Exploiting Software

HAKING

Vol.2 No.7
Issue 07/2012(11) ISSN: 1733-7186

SamuraiWTF Toolkit

BURP SUITE AUTOMATIC ATTACKS

MALWARE

MEMORY LEVELS GATE MITIGATION

W3PENETRATION TESTING LAB SETUP GUIDEAF

WEBSENSE

ANTI-ROOTKITS IN THE ERA OF CYBER WARS

PLUS

TRY TO IMPROVE OUR FIRST LINE OF SECURITY: PASSWORD CONSTRUCTION AND MANAGEMENT

HOW TO PROTECT BEFORE SECURITY INCIDENTS CAUSED BY INHERITED VULNERABILITIES OF HUMAN NATURE: PICKING UP MUSHROOMS IN THE RAIN FOREST – SOCIAL ENGINEERING INFORMATION GATHERING

eLearnSecurity
Forging security professionals

PENETRATION TESTING PROFESSIONAL v.2

Online Penetration Testing Course

www.elearnsecurity.com

- 2400+ interactive slides
- 9 hours video training material
- 100% hands-on with Hera Labs
- Extremely in depth and thorough contents
- Leads to Hands-on ECPPT certification
- 3 Knowledge domains
- Web application penetration testing
- Network penetration testing
- System security and Exploit Development
- Lifetime access to course material

Now the most Hands-On course on Penetration Testing :

Coliseum Web Application Security Lab

- 14 real world vulnerable websites
- User-exclusive sand-boxed access to labs
- Multiplatform : PHP, MySQL, MS SQL Server
- Practice OWASP Top 10
- Web app analysis, XSS, SQLi, LFI/RFI, CSRF
- Get inline help if you get stuck

Hera Penetration Testing Virtual Lab

- VPN access from your own Attack box
- User-exclusive, non-shared access to labs
- Guided Exploitation Walkthrough
- Windows Servers, BSD, Linux, Firewalls, IDS's
- Different Labs with Different Network topologies
- On-demand: No Activation, No Expiration

www.elearnsecurity.com

HEY! TEACHER!

LEAVE THEM KIDS ALONE!

THE MOST ADVANCED COURSE ON PENETRATION TESTING

IS SELF-PACED!

WWW.ELEARNSECURITY.COM

Exploiting Software
team

Editor in Chief: Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Managing Editor: Natalia Boniewicz
natalia.boniewicz@hakin9.org

Editorial Advisory Board: Rebecca Wynn, Matt Jonkman, Donald Iverson, Michael Munt, Gary S. Milefsky, Julian Evans, Aby Rao

Proofreaders: Michael Munt, Rebecca Wynn, Elliott Bujan, Bob Folden, Steve Hodge, Jonathan Edwards, Steven Atcheson, Robert Wood

Top Betatesters: Nick Baronian, Rebecca Wynn, Rodrigo Rubira Branco, Chris Brereton, Gerardo Iglesias Galvan, Jeff rey Smith, Robert Wood, Nana Onumah, Rissone Ruggero, Inaki Rodriguez

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 Expoiting Software magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@hakin9.org

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Dear Readers,

In this issue we are going to introduce to you the best of the open source and free tools that focuses on assessing and exploiting web applications: the Samurai WTF Toolkit. In the article Diving Through SamuraiWTF Toolkit written by Manjul Verma we will we dive through Samurai-WTF to understand what really it contains. In the article Penetration Testing LAB Setup Guide

Jeremiah Brott will teach us how to create your own penetration testing laboratory. In the article Malware, a cyber threat increasingly difficult to contain Pierluigi Paganini will talk about the worst cyber threat that daily evolve with the capacity to hit every sector without distinction. If you want to know why Burp Suite provides a powerful set of tools that not only perform automated scanning that can provide the tester with an overview of how the Web application handles security challenges, but also provide the ability to perform powerful, targeted attacks, read the article Burp Suite Automating Attacks written by Ric Messier. In the article Memory Levels Gate Mitigation

Amr Thabet will introduce us two created by him Modes (normal and high modes) to stop any way to bypass the mitigation and solutions for any incompatibility problem you could face. In the article Anti-Rootkits in the Era of Cyber Wars Igor Korkin will show us his method of stealth detection based on dynamic bit signature is described. In the article Web Filtering with Websense. To be or not to be filtered: that is the dilemma Abdy Martinez will show us a method of stealth detection based on dynamic bit signature is described. To understand why most organizations still rely on traditional passwords and will continue to do so for many years read the article Password Construction and Management written by Gaurav Kumar. And finally read about the inherited vulnerabilities of human nature in the article Picking Up Mushrooms in the Rain Forest – Social Engineering Information Gathering written by Vlad Styran. Enjoy the reading!

.

Natalia Boniewicz
& Hakin9 Team

Get prepared.

We are Expanding Security, a Pen Testing and Training Company. We've been preventing deer-in-headlights look since 2006. We offer Pen Testing services plus our Live On Line training classes for ISSMP, ISSAP, CISSP, and Certified Ethical Hacker. We give you online access to materials wherever you are.

You need to keep your job secure, your business strong, and your staff on top of the game. See how good and fun training can be. Our courses are current to changing technology, and our training is the fastest, easiest way to master the relevant data you need NOW.

Sign up for our free weekly PainPill and come to a free class.
http://www.expandingsecurity.com/PainPill

...with Freedom, Responsibility, and Security for All ™
www.ExpandingSecurity.com

ATTACK PATTERN

8 Malware, a cyber threat increasingly difficult to contain

BY PIERLUIGI PAGANINI

Why despite all the countermeasures implemented by security firms the agents continue to make claim victims? Which are the most feared agents? When we speak about malware we introduce one of the worst cyber threat that daily evolve with the capacity to hit every sector without distinction.

16 Burp Suite Automating Attacks

BY RIC MESSIER

As new security measures are constantly being created in an attempt to protect websites, so are the threats and attacks that are designed to bypass these security measures. Burp Suite is a software program that can help accomplish these goals without paying the sometimes unaffordable prices of commercial Web application testing tools. Burp Suite provides a powerful set of tools that not only perform automated scanning that can provide the tester with an overview of how the Web application handles security challenges, but also provide the ability to perform powerful, targeted attacks.

22 Memory Levels Gate Mitigation

BY AMR THABET

Return Oriented Programming is a very powerful technique and very similar to the applications' normal flow. You don't have any way to stop the application and watch for ROPs. Memory Levels Gate (MLG) is a method to solve this problem. It gives you a supervision of your sensitive kernel APIs that could convert any normal buffer in the stack into a ghost that could play with the whole OS. The idea gives you a gate (using the NX or XD flag that are used in DEP) to control the calls to your kernel APIs and checking for ROPs. But your security checks(that detect ROP) could lead to one of two other ghosts: 1. Easy to bypass or 2. Incompatibility. It's hard to find the optimum design for your security checks. So, the author created two Modes (normal and high modes) to stop any way to bypass the mitigation and solutions for any incompatibility problem you could face.

DEFENSE PATTERN

26 Anti-Rootkits in the Era of Cyber Wars

BY IGOR KORKIN

In the last two years, information security issues have been front and center within various news sources. Some of the major issues that have been covered in the media included Stuxnet, Duqu, and Flame. By learning of these tools and their capabilities, it is important to think about what could be next. This article is intended to provide a concept of information security system design, particularly for stealth detection. The author's method of stealth detection based on dynamic bit signature is described.

30 Web Filtering with Websense. To be or not to be filtered: that is the dilemma

BY ABDY MARTINEZ

If you asked IT people about the importance of Web Filtering, the first thing they would say is: to save bandwidth. And sometimes, the bandwidth limitation is the primary reason that an organization decide to obtain this kind of solution. But network performance is just one of the reasons that we should consider to implement this technique in our organizations. In this article, you will learn what is Web filtering, how it works, Websense solution, and basic considerations when you are choosing your Web filtering solution.

34 Password Construction and Management

BY GAURAV KUMAR

Passwords are our first line of security. In the era of defense-indepth, gone are the days of simply installing a firewall, antivirus, and spam filter. Although these technologies can act as a defense against the common hacker and threat, if credentials to a network are intercepted, these devices are useless.Although alternative technologies for authentication, such as biometrics, smartcards, and one-time passwords, are available for all popular operating systems, most organizations still rely on traditional passwords and will continue to do so for many years.

PENETRATION TESTING

38 Diving Through SamuraiWTF Toolkit
BY MANJUL VERMA
The Samurai Web Testing Framework is a live Ubuntu Linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focuses on assessing and exploiting web applications. In this article, we dive through Samurai-WTF to understand what really it contains.

60 Penetration Testing LAB Setup Guide
BY JEREMIAH BROTT
This penetration testing guide has been created with a few things in mind. One being the attacks are designed from attacker with internal access into the network being penetrated. Future guides will extend upon this document bringing more advanced network setups and unique vulnerabilities. After setting up this LAB environment, you will have the ability to exploit issues from the following categories: mis-configured Services and Applications, Backdoors planted into software, unintentional Backdoors, Weak Passwords, Web Applications, plus much more, how much can you find?

SOCIAL ENGINEERING

66 Picking Up Mushrooms in the Rain Forest – Social Engineering Information Gathering
BY VLAD STYRAN
Social Engineering is a field of information security industry that is both known and unknown to general public. On the one hand, there is a number of world known social engineers, from both the dark and the bright side of the trade, whose adventures are captured in numerous movies and memoires. While on the other hand social engineering is one of the topics that are full of speculation and uneducated claims, including those in the media, and that sadly turns social engineering into some kind of a gray area. In the meanwhile, social engineering infiltrates a substantial part of computer security operations. To name few, Security Awareness, despite its arguable efficiency, is the set of information security controls directed to decrease the probability and potential impact of security incidents caused by inherited vulnerabilities of human nature.

Malware,

a cyber threat increasingly difficult to contain

The article propose a view on the malware world proposing statistics related to diffusion trend and explaining which are main actors responsible for the spread of malicious agents. Why despite all the countermeasures implemented by security firms the agents continue to make claim victims? Which are the most feared agents? The article tries to reply to these and other questions based on objective data provided by the principal security company operate in the sector.

When we speak about malware we introduce one of the worst cyber threat that daily evolve with the capacity to hit every sector without distinction. The world "malware" is really generic, we refer in fact a heterogeneous family of malicious software designed with the purpose to disrupt computer operation, gather sensitive information, or gain unauthorized access to victims systems with very different scopes.

Sample of malware type are computer viruses, worms, trojan, spyware, ramsonware, adware and rootkits, each of them characterized by an unprecedented growth linked to rapidly changing of the technological context supported by the increased use of internet and the explosion of mobile services.

The large extension of network like internet and the impressive diffusion of social networks have advantaged the spread of malicious software, it is to be considered a natural process, to give an idea of what we have observed in the recent years consider that in the last couple of years the release rate of malicious code and of other unwanted programs was greater of the one related to previous 20 years, it's amazing!

The malware analysis is became an essential component of the security sector, security firms have introduced specific sentinel over the main networks to gather information on every suspect activities that could threaten systems security.

The work is really hard because the malware today have reached a level of sophistication really high, in many cases for their development are engaged teams of experts that work for elude of the principal alerting system, and unfortunately it is happened that some virus or trojan have been discovered years later their diffusion with serious consequences.

How does work the global detection network for malware analysis?

The principal security firms have deployed on the networks thousands of probes used to analyze the traffic and not only, billions email messages and Web requests are processed daily in dedicated data centers, the gathered information are put in relation with data acquired through an antifraud community of enterprises, law enforcement advisor and consumers feedback, only in this way it is possible to detect incoming cyber threat just in time. When user download it's last antivirus update or anti-rootkit tool he must be aware of the great works that experts do every day without interruption, because malware don't' know holidays.

A very interesting part of the precious works done could be appreciated reading the periodical reports that company provides, a precious sources that inform on the incoming threat and related risks.

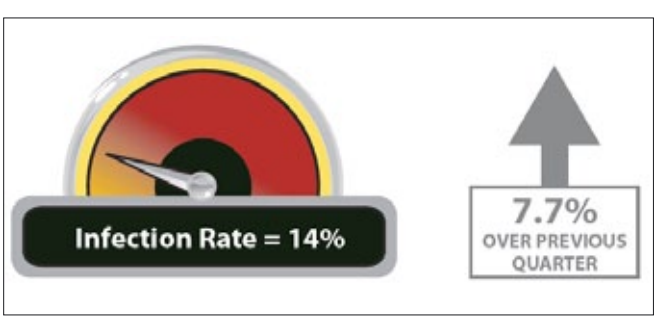


Figure 1. *Kindsight Security Report – Percentage of home network infected Q2 2012*

All the data proposed by different analysis of the phenomenon demonstrate a sensible increase of malware diffusion despite the awareness of the cyber threat and the counter measures implemented by private and government entities.

According the data provided by Kindsight Security, the a majority-owned subsidiary of Alcatel-Lucent, around 14 percent of home networks were infected with malware in the period between April and June 2012 (Figure 1).

One of the main vector to spread the malicious agents is still the email, unsuspecting users are daily hijacked on infected website that compromise their machines with various type of malware.

According the proposed statistics 9 percent of residential households were infected by high-threat malware, such as a botnet, rootkit, or a banking Trojan, meanwhile approximately 6 percent were infected with moderate-threat malware such as spyware, browser hijackers, and adware.

Of course in many cases user's machine is compromised by several malware.

The report dedicates a specific session to the botnets and in particular to ZeroAccess botnet which grew to over 1.2 million nodes over the second quarter, a figure that could give an idea on the rapidity of the infection diffusion of these agents (Figure 2).

Another primary source of information on the evolution of malware, and more in general of any cyber threat diffusion, related the fights against malware diffusion are the reports and bulletins provided by security firm Symantec. In the last issue of Symantec "Internet Security Threat Report" has been reported an increase respect last year result of a surge in polymorphic malware attacks, particularly from those found in Web attack kits and socially engineered attacks using email-borne malware.

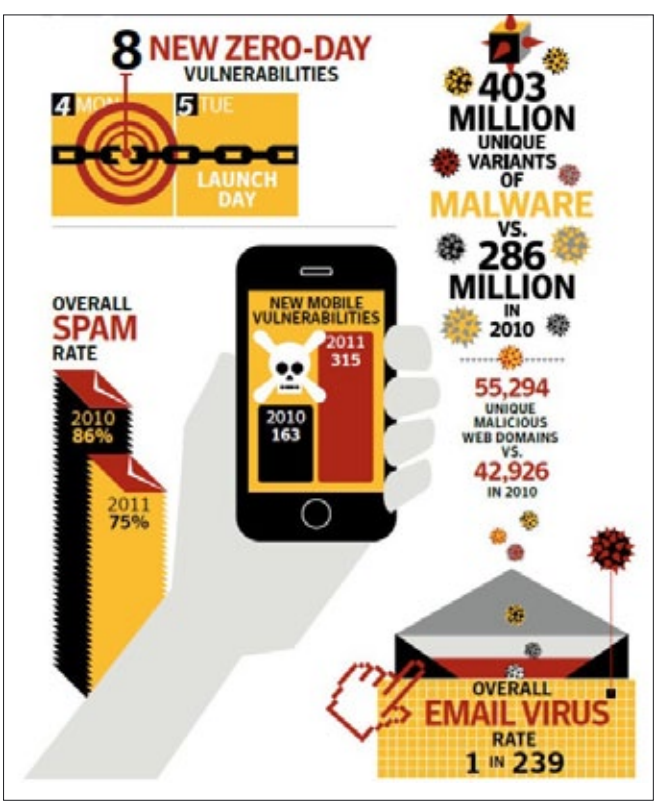


Figure 2. *Symanted Security Threat Report 2011*

The report giver great emphasis to the increasing of the number of zero day vulnerabilities exploited with a rate of 8 new vulnerabilities per day. Zero-day vulnerabilities represent a serious problem for system security, they are unknown and represents privileged way to avoid security defense of any type of architecture.

Particularly efficient are malicious agent that exploit zero-day vulnerabilities because they could operate being detected also for a long period. According the Symantec data it has been registered an increase of unique variants of malware 140% respect 2010, passing from 286 million of variants to 403 million that confirm the worrying trend.

Malware impact on private and government sectors

We can surely note that malware impact any sector of today society, there is no differences between private business and government affairs, both are very vulnerable to cyber attacks conducted using malicious agents. What is changed in the last couple of years is the awareness that this cyber threat could be used also in military sector. In the last years we have read a lot on the concept of cyber weapon, powerful malware that are used in covert military operation, to compromise enemy's system.

The possibility to exploit enemy system using a malicious source code is considerable an old idea on which many states have made great investments, but only recently with the massive introduction of technology in everything surround us and the large diffusion of networked systems have made practicable the offensive.

The Stuxnet case has demonstrated how much powerful could be a cyber weapon and how high is the interest of the governments in the design and development of a malware that is able to interfere with the processes of a critical infrastructure such as a nuclear plant or a telecommunication system.

In a government and military sectors the use of malware is increased in a sensible way, after Stuxnet security company have detected other dangerous instances of malware, Duqu, Flame and Mahdi, malicious agent technologically advanced that have been developed with state sponsored project

and that mainly have offensive and cyber espionage purposes.

Why a government is interested in the development of a malware for offensive purposes?

- First, the disclosure of such agents is silenced for the nature of the vulnerabilities that are exploited. The study of new zero-day vulnerability provides a real advantage to those who attack and the related risks of failure of operations is minimal. We consider that attacks perpetrated in this way, because of the anonymous nature of the offense, allow you to circumvent the approval by the world community to a military offensive.
- The costs involved in developing solutions such as that at issue are relatively low compared to other conventional weapons.
- The choice of cyber weapon allows those who use the solution to remain anonymous until military strategies deem it appropriate. The main strategies that use of such malware are mainly aimed at:
  - Probing the technological capabilities of the enemy. The ability of an agent to infect enemy structures is symptomatic of inadequate cyber defense strategy that may suggest additional military options.
  - Undermine those that are considered critical structures whose operation depends on the opponent's vital functions of the governmental structure of a country.
- No doubt regarding the efficacy of these weapons. Events have proved that they are offensive weapons designed with the intent to infect opposing structures. The cyber weapons can be designed to hit specific targets while minimizing the noise related the usage of the weapon that can result in causing the discovery. The vector of infection can be of various kinds, such as a common USB support, being able to hit a very large number of targets in a small time interval.
- Another significant factor is the ability to predict and to observe the development of a cyber weapon by agencies intelligence. In a classical context the development of a conventional weapon can be easily identified through intelligence operations on the ground and via satellite observations can be easily identified a garrison used to develop military systems. The development of a cyber weapon is rather difficult to locate and thus hinder, even a private home may be suitable for the purpose.

As we have seen the use of malware is becoming very frequent in cyber attacks and cyber espionage campaign but the most evident impact of malware diffusion is without doubt registered in private sectors.

Large organizations register every year billions of dollars of loss related cyber attacks operated using malware, data leaks represents for the businesses one of the primary concerns. Malware could infect computer and entire networks causing serious damage to the productive level of the company. A malware infection could cause the loss of intellectual property or company secrets that could compromise the existence of the business, a malware could also infect production control systems with serious repercussion.

Small business is in my opinion the sector most exposed, small companies due the global crisis have made cost cutting also on security perspective opening the door in many cases to malware and other cyber threat. Lack of resources, reduced budgets and low awareness on cyber threat represents the key factors of a worrying scenario.

Malware diffusion

Security experts have identified various schemes for malware diffusion, of course the mail channel is represented by internet, let's think to millions of unaware users that daily are infecting simply visiting a compromised web site. The categories of web sites mainly impacted by this type of attack are Blogs & Web communications, Hosting/Personal hosted sites, Business/Economy, Shopping and Education & Reference.

One of the of the most subtle and effective mode of infection is the "Drive-by attacks", internet users are infected just visiting a compromised website, victims are hijacked on infected websites with very common attack techniques such as 'clickjacking' or 'likejacking' that deceives the users inducing them to watch a video or simply expressing its pleasure regarding a specific topic using "I like" function.

But the way of malware diffusion are infinite, let's think to the diffusion on internet of exploit toolkits which allow creation new malware without specific technical capabilities, this peculiarity has facilitated the rapid adoption and diffusion of the attack kits in the criminal world that have intercepted the growing demand in a millionaire business, a phenomenon that continues in its inexorable rise.

The principal channel to spread malware is, according the different security firms, the email. During the last year the number of malicious email is increased targeting mainly large company but also governments and no profit organizations. The in-

fection schema very simple, malicious emails contain infected file as attachment that exploit a vulnerability in the target system, in many targeted attacks to circumvent the user the content of the mail appears legitimate and try to catch the attention of the victim.

In alternative way the email could contains a reference to a compromised web site that host malware able to infect user's machine.

Using a similar schema for example in Syria and in Tibet governments have spread agents to political persecute opponents tracing their activities and take the remote control of their machine to steal documents and precious information.

But malware could also be diffused through the social networks platforms, they represents digital squares where millions of users exchange videos, images and links, an ideal scenario for the diffusion of malicious code. During the last year with the impressive growth of social network we have also observed the increase of the number of malware propagated using the popular social platforms. Millions of user always connected and with low awareness on the cyber threats are ideal victims for cybercrime that once again uses malware to exploit user's vulnerabilities. In the social networking the fundamental factor is use of social engineering techniques to circumvent users that most often are redirected on compromised web sites through the sharing of "malicious hyperlink".

Due the importance of social networks, mine of information, they represent a privileged target for cyber criminals that intend implements new fraud schema and governments that try to spread malware with cyber espionage purpose. Recently the experts of Trusteer firm have discovered a new variant Zeus malware responsible for a series of attacks against principal internet service providers. The variant carried out attacks using the P2P network architecture targeting users of Facebook, Hotmail and Yahoo and Google Mail. Zeus Trojan is born as an agent able to steal banking information by logging keystrokes and form grabbing, it is spread mainly through phishing and drive-by downloads schemes.

The malware variant that hit Facebook uses a web injection mechanism to propose to the victims a special price reduced of 20% for purchases made with Visa or MasterCard debit card using their Facebook account. The scam promises in fact that after registering debit card information, the victim will earn cash back when they purchase Facebook points. Of course to the user is proposed a form for the registration of debit card info

that is equivalent to a legitimate one also in term of proposed layout

Who is responsible for malware diffusion?

Use of malware is really frequent for different purposes, cybercrime, cyber warfare, hacktivism, governments monitoring and surveillance.

The criminal organizations are very active in the development and diffusion of malware, is known that this kind of crime is very profitable and often go unpunished due lack in current regulation in many country of the world. Criminal gangs have discovered how much lucrative is the cybercrime and how reduced are the possibility to be legally pursued. Computer crime by its nature has placed in the cyberspace with direct effects on the real world, but due this characteristic, its persecution is virtually impossible for the absence of globally shared regulations against this type of illicit.

Main use of malware made by cyber criminals are Malware could be used in different fraud patterns, mainly their use is to steal user sensible information like banking credentials. The diffusion could happen through several channels like social networking, mail spamming, visiting infecting host or hijacking web navigation. The common factor is the identity theft of the user for fraudulent activity. During the last weeks we have assisted to the rapid diffusion of new generations of Ransomware demonstrating that the use of malware could be adapted for different model of cybercrimes.

Ransomware is a type of malware which restricts access to the computer resources of the victim demanding the payment of a ransom for the removal of the restrictions. To prevent the access to the resources the malware encrypt files of infected machine.

Cybercrime is not only the sector that adopts malware for its purposes, one of the most interesting usage is related to cyber warfare. Borrowing definition of “cyber weapon” provided by security experts Thomas Rid and Peter McBurney :

“a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings“

we can immediately think to the effect of a computer malware targeted against a strategic objective such as a critical infrastructure.

Over the years many cyber weapons have been identified as described the most famous of which is the virus Stuxnet, for its development is common opinion that has been involved, by US and Israel Governments, a pool of high specialists. The reality is more complex, the future for malware in cyber warfare scenario is made of dedicated platform used to create multiform and modular agent that could target specific objectives simply including new components. We are facing with open projects that evolve with the need and in function with specific targets present new offensive features.

Kaspersky’s director of global research & analysis, Costin Raiu, discovered with his team the existence of a common platform to build the malwares Duqu and Stuxnet, that they named “Tilded platform” because many of the files in agents have names beginning with the tilde symbol “~” and the letter “d.””. What is really interesting is that the researcher is convinced that the same framework has been also used to create at least three other pieces of malware confirming the existence of a “factory” platform that Costin Raiu defined using the following statement:

“It’s like a Lego set. You can assemble the components into anything: a robot or a house or a tank,”

But malware could be also the next option of group of hacktivist such as Anonymous. During the last couple of years we have witnessed the escalation of operations conducted by the Anonymous group, the hacker group that is expressing a social dissent through cyber attacks.

Is common conviction that the group use only DDoS attacks for its operations, but the collective is changing and some security experts believe that they are also exploring other options such as malware deployment. The purposes of malware usage maybe be different, malicious software could be used to attack strategic objectives with targeted campaign and also to conduct cyber espionage operations. Also DDoS attacks could be automated infecting machines of the victims or simply hosting a malware on a website that redirect the attacks against the chosen targets.

Another regrettable usage of malware is monitoring and controlling, typically implemented by governments and intelligence agencies. In most cases virus and trojan have been used to infect computer used to attack dissident, opponents and political oppositions. The purpose is to track their operation on the web, gather sensible information and localize them. In many cases the use of malware has made possible the capture of the victims and their ruthless suppression.

During the Syrian repression the government has discovered that dissidents were using program such as Skype to communicate, so it has used the

same channel to spread the backdoor "Xtreme RAT", a malware that belong to the Remote Access Tool category really simple to retrieve on line at a low price (Full version Price: €100 EUR).

Cyber espionage malware, a global nightmare

Malware once were used primarily to destroy the victim's PC, but the scenario has completely changed today.

We have seen that cyber criminals, governments, and groups of hacktivists, with different purposes, tend to lean toward the spread of malicious agents that have the capacity to infiltrate the targets be silently stealing from them the most information. Profit, Power, Protest the main motivations behind the attacks, that are radically changing user's approach to the web and the their perception of security.

We usually blame China but recent events have shown that it is common practice to use malware with these purposes, but China is not the only nations involved in similar attacks, let's consider for example United States and researches to develop cyber weapon that are able to infiltrate sensitive networks to steal information. The project Olympic Games is the evidence of the effort spent in this new form of offense, and other valid examples of malware used with cyber espionage purpose are Duqu and Flame both developed to gather sensible information from Iranian Government.

A recent study on cyber-espionage has demonstrated that more than 200 families of malware have been designed and used to spy on government and corporate representatives.

We have assisted to the diffusion of new agents that works in botnet architectures, in similar way to the ones used by cybercrime for massive attacks, but that are specifically developed for selected targets that resulting to have a minor dimension.

The study reveals that more than 1,100 domain were used in the attacks, in particular the experts have traced the botnet used analyzing the traffic produced, the Sinkholing, a consolidated technique used by many security firms,

Sinkholing is a technique that researchers use to redirect the identification of the malicious C&C server to their own analysis server. With this methods researcher design a map of the botnet and of the control center identifying the type and numbers of final attacks.

Attacks have the primary intent to steal classified information from government agencies or trade secrets from corporations and the situation could be extremely dangerous for the economy of a company and of the overall country.

With similar attacks governments and business try to reduce the technological gap with their competitors, it's clear how much diffused is the phenomenon.

The cybercrime is not watching, it has increased focus in targeting individuals and organizations of

TABLE 2: MOBILE THREAT STATISTICS BY TYPE, 2004-2011

	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL
Adware									-
Application								5	5
Backdoor							3		3
Garbage			8						8
Hack-Tool							4	8	12
Monitoring-Tool							1	15	16
Riskware			1		1	8	1	10	21
Spyware			5	15	6		2	5	33
Trojan	11	105	160	23	13	24	47	141	524
Trojan-Downloader								1	1
Virus	14	19	17	6					56
Worm				2	8	6	22		38
	25	124	191	46	28	38	80	185	717

Figure 3. *F-Secure – Mobile Threat Report*

all sizes to steal financial information, in particular under pressure has made the small businesses too vulnerable to cyber attacks.

The Trend Micro has reported a sensible increase of focused attacks respect previous quarter (27%), around 142 million threats which were blocked from infecting small businesses but also large companies have been hit by the crime as happened for the IXSHE campaign.

Cyber espionage represents a serious cyber threat, and government agencies are defining best practices to reduce the risk of exposure to the attacks.

NIST has recently released the public comment release of Draft Special Publication 800-83 (SP) Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

Malware is considered the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.

This publication provides recommendations for improving an organization's malware incident prevention measures. It also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones.

Which future for malware?

The data collected on the malware diffusion let us think that new sophisticated agents will be developed in the short term, most of them able to exploit also 0-days vulnerabilities.

We must expect that governments and intelligence agencies will make large use of malicious computer program to infiltrate enemy network and steal sensible information, we are in the cyber era and this is the new way to fight. The conflict are moving from the ordinary world in the cyber space, new powerful cyber weapon could be designed to attacks critical infrastructure and left in the wild to spread it self-making serious damages.

One of the most critical aspect in fact is the ability of malware developer to follow the evolution of their creation, there is the concrete risk that virus and rootkit are reverse engineered to create new aggressive agent that could be freely sold to best bidder.

Another trend that create great concern is related to the botnet diffusion and evolution, the traditional techniques used to detect and decapitate the malicious structure are becoming obsolete due the introduction of new sophisticated structure. Let's think to P2P botnet or to botnet that doesn't need the traditional presence of Command and Control server, characteristic that make hard their detection.

Factors like the massive diffusion of mobile devices and the integration of new services, such as banking and communication, in social networking platform are creating the right condition for the diffusion of malicious cyber threats. Consider also the increasing attention of ordinary crime in cyber fraud, a business relatively secure that will attract capitals in cybercrime areas, new groups of hackers and specialist could sell their services to the crime with unpredictable consequences.

To give an idea on how much attractive is the mobile technology for malware developer let's give a look to the Mobile Threat Report released by security firms F-Secure that warns of a dramatic increase in malware targeting mobile devices, especially Androind OS based. The following table reports interesting statistics on mobile threats discovered between 2004 and 2011, showing an impressive growth grouped by malware type (Figure 3).

According the report "In Q1 2011, 10 new families and variants were discovered. A year later, this number has nearly quadrupled with 37 new families and variants discovered in Q1 2012 alone," the report states."

Conclusions

All this data show a situation can only worsen in the next future, to mitigate the risks related to malware diffusion it's necessary to increase the level of awareness especially for those sectors more exposed such as mobile and social networking.

To contain the raise of malware diffusion each country must create a proper response team that involve exponents of private industry and government agencies, this team must cooperate on global scale exchanging information and working to the definition of regulation globally recognized to provide stiff penalties for cyber criminals.

PIERLUIGI PAGANINI

Pierluigi Paganini has a Bachelor in Computer Science Engineering IT, majoring in Computer Security and Hacking techniques. Security expert with over 20 years experience in the field. Certified Ethical Hacker at EC Council in London. Actually he is Company Operation Director for Bit4Id, Researcher, Security Evangelist, Security Analyst and Freelance Writer. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to found the security blog „Security Affairs".

Security Affairs (http://securityaffairs.co/wordpress)

Email : pierluigi.paganini@securityaffairs.co

inj3ct0r

if you'll hacked us
we'll pay you 10K $
http://1337day.com/

Exploit database separated by exploit type
(local, remote, DoS, Poc, etc.)

Burp Suite Automating Attacks

As new security measures are constantly being created in an attempt to protect websites, so are the threats and attacks that are designed to bypass these security measures.

As a result, the number of available attacks and threats continue to grow at a rapid rate. Due to the fact that there are many different ways to test a website for vulnerabilities that may allow for these attacks to be successful, automated testing is sometimes a necessity. Burp Suite is a software program that can help accomplish these goals without paying the sometimes unaffordable prices of commercial Web application testing tools. There are two versions of Burp Suite available; the free edition and the professional edition. The list of features can be vie-wed at *http://portswigger.net/burp/download.html*. While there are other free tools available, Burp Suite is packed

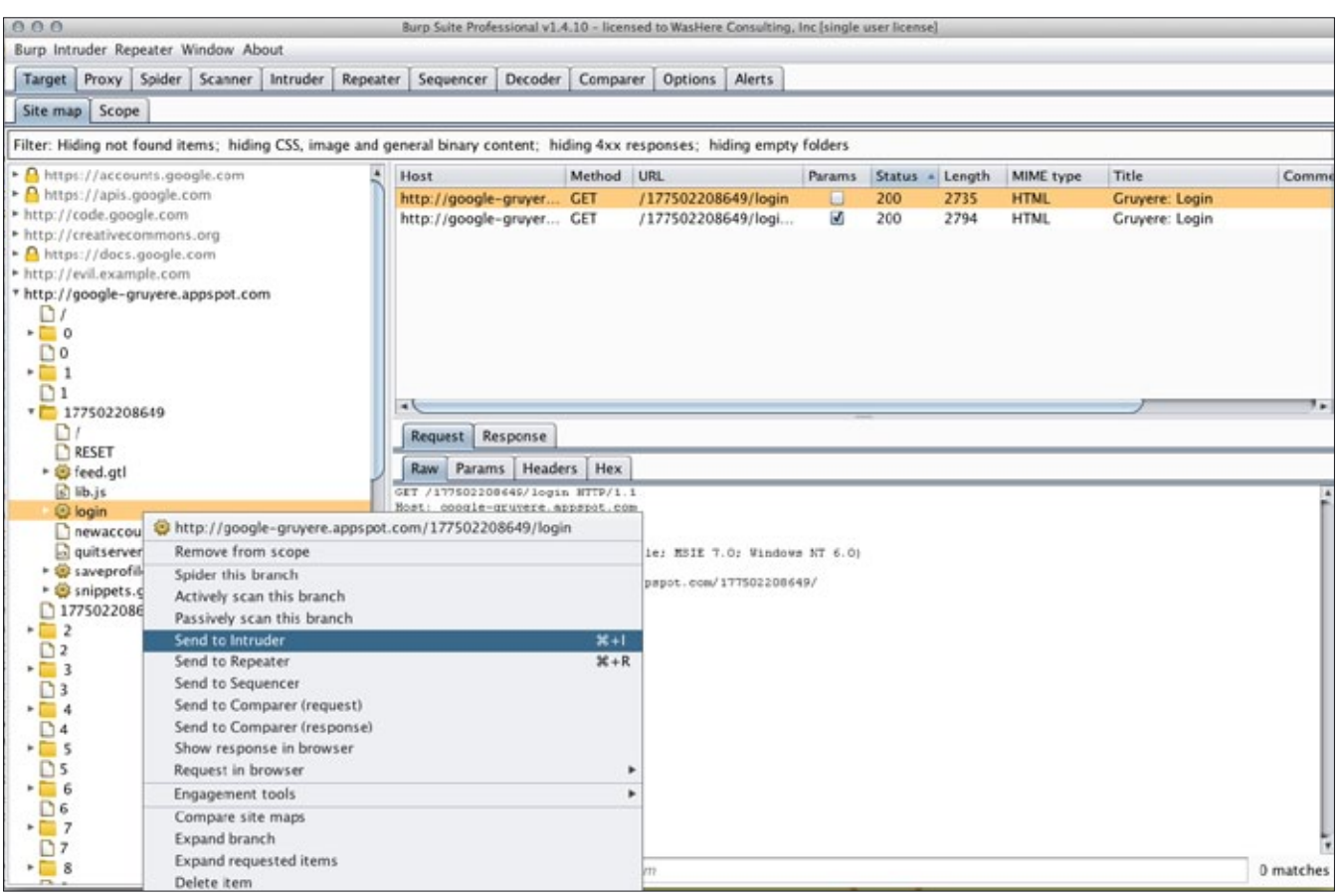


Figure 1. *Sending Request to Intruder*

with features that can make Web application testing much easier. For the purposes of this demonstration, Google's Gruyere will be used as the target Web site. Gruyere is designed to have a number of vulnerabilities which makes it useful learning and demonstration platform.

Brute Forcing Logins

Web applications that allow user input will usually have an authentication process before granting access to that user. While testing a website to determine if an attacker can obtain username and passwords, the tester usually starts by probing the site for credentials. *Most testers will have precompiled lists of usernames and passwords that will be used to test the website. A useful functionality of Burp Suite is that a tester can input these lists of credentials without manually entering each credential set.*

In order to test for usernames and passwords, the Intruder function of Burp Suite will be used. The easiest way to start is by performing a spider on the site to get a list of all the pages. From the list of pages, the request where the login information is submitted will be visible in the results. In Gruyere, for example, the login page is located at google-gruyere.appspot.com. The returned request is below:

```
GET /177502208649/login?uid=foo&pw=foo HTTP/1.1
Host: google-gruyere.appspot.com
Accept: */*
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0;
                Windows NT 6.0)
Connection: close
Referer: http://google-gruyere.appspot.com/
                177502208649/login
Cookie: GRUYERE_ID=177502208649
```

In the request line are URL parameters. This is where the tester will want to make changes. In order to perform this function, the request will be sent to the Intruder of Burp Suite. This will put the

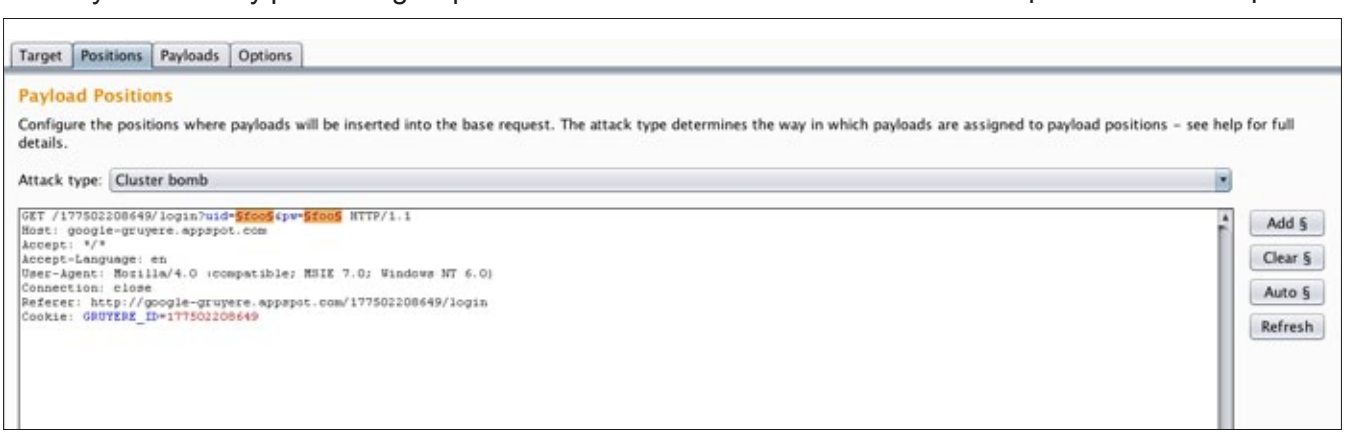


Figure 2. *Payload Fields*

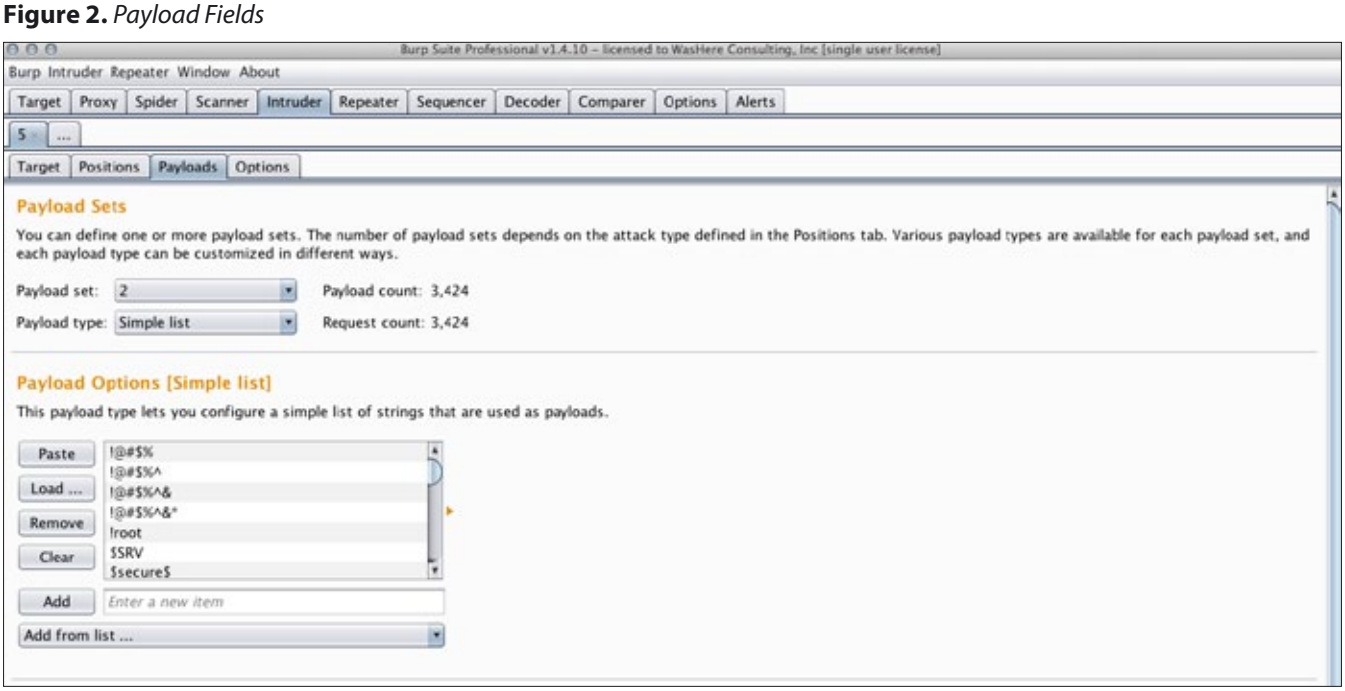


Figure 3. *Password list selected for second field*

request into another tab in Burp Suite and select the portions of the HTTP that it believes can be manipulated with Intruder (Figure 1).

Once the request is sent to the Intruder window, the tester can start selecting the types of manipulations that will be used. Burp Suite uses payloads to indicate which sections of the message are going to be altered. Depending on the attack type, the tester can use a variety of payloads.

While viewing the Intruder window, the target will be shown. Burp will fill in the necessary data based on the target that was used in the spider from where the HTTP message was selected. At this point, the tester can make changes to the target. In the positions tab, the tester will see the selected payloads and can choose to either add them or remove them. In the example above, the user, the password and the cookie are all selected as payloads. One huge advantage regarding the flexibility that Burp offers is that if the tester had written their own Web server, for example, they could use Burp's Intruder to perform fuzzing and anomaly testing against their web server to learn how it handles invalid input. While Burp will automatically select parameters and data handled by the Web application, the tester can just as easily manipulate data handled by the Web server itself. Any piece of data in the HTTP sent to the server can be manipulated by Burp by putting payload selections around what areas should be changed (as seen Figure 2). As mentioned above, Burp offers different types of attacks depending on how many payloads you have. The types of attacks offered are as follows:

Sniper

A sniper attack takes one defined set of payloads and runs through each payload position individually. For example, if the tester has an HTTP request that has two fields they were trying to inject payloads into, the first payload would be injected into the first field on the first request. The second request (the first payload) would be injected into the second field. This will generate p X f requests, where p is the number of payloads and f is the number of fields.

Battering Ram

A battering ram attack has one set of payloads in use. Instead of only making a change to one field at a time, each field gets manipulated on each request. The first field would be populated with the first payload. The second field would also be populated with the first payload. The second request would see both fields populated with the second payload. The total number of requests would be the number of payloads.

Pitchfork

With pitchfork, the user has multiple payload types and multiple fields. The first field would be popu-

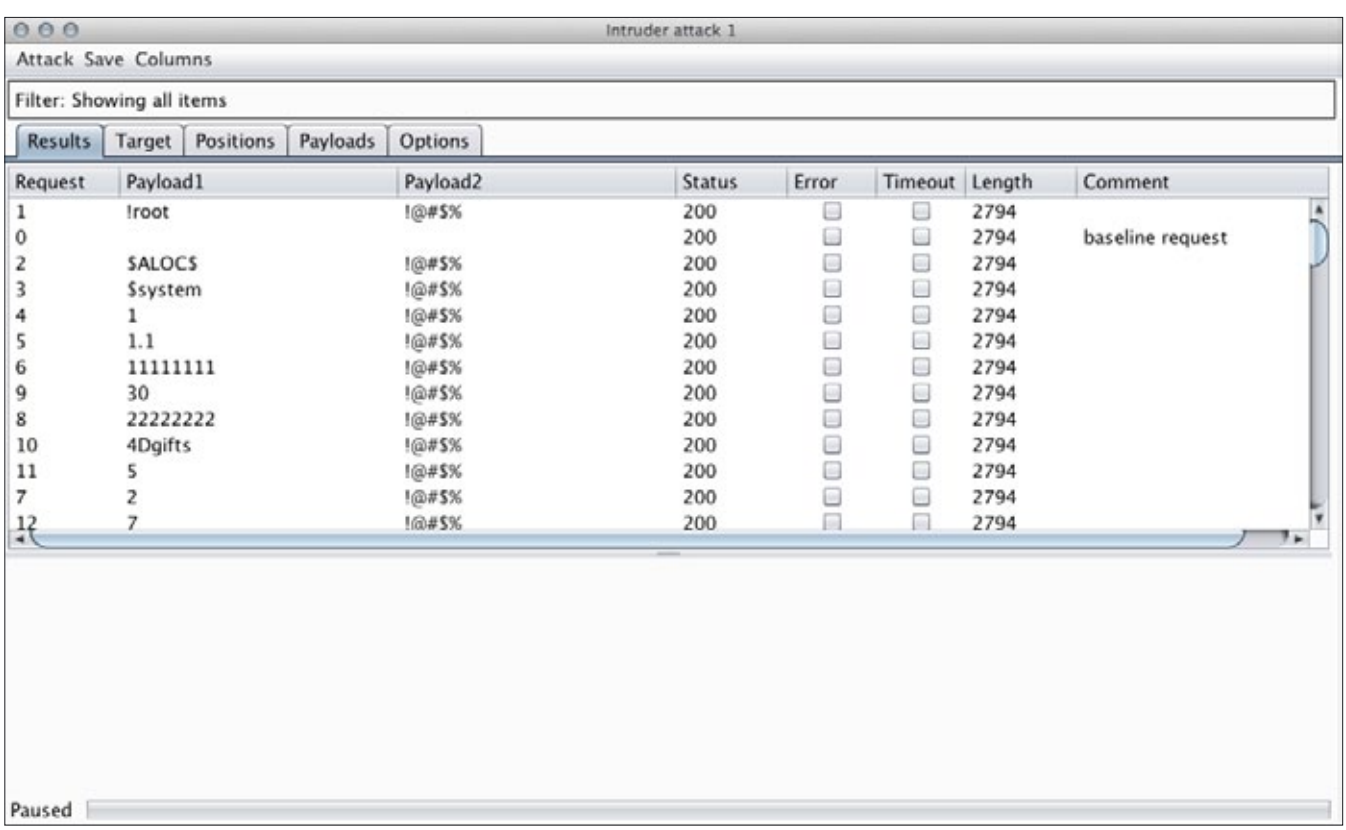


Figure 4. *Intruder attack*

lated with the first payload from the first payload source. The second field would be populated with the first payload from the second payload source. In the second request, both fields would get the second payload from their respective payload sources. The number of requests is the smallest number of payloads in one of the payload sources.

Cluster bomb

A cluster bomb similar to the battering ram but has multiple payload sources as well as multiple fields that can be manipulated. The best example here is a username and password. The tester wants to check every password against every username so the first request you would populate the first field with the first payload from the first payload source. The second field would get the first payload from the second payload source. The tester would repeat this process through all payloads in the second source (in this example, the password file) before moving on to the next payload from the first payload source. As a result, the number of payloads multiplies from all of the sources together to determine the number of requests that are generated; a username file with 4 entries and a password file with 5 entries would generate 20 total requests.

Another benefit that Burp offers is allowing the automation of payload creation. There are a number of payloads that are built in to Burp. Additional data can be added to any payload so the tester can use the built in payloads as a starting point and then create their own custom payloads. While there are a number of usernames and passwords built in to Burp, the list is more of a starting point so it is always recommended that the tester provide their own lists (Figure 3).

On the Payloads tab, select the payload set (which payload field that the tester created in their HTTP request they want to add data to). In this example scenario, a simple list for both Payload sets is going to be used. In the first payload set, choose "Add from list" and select "usernames". In the second payload set, repeat the same process but select "passwords". This example will use a Cluster bomb attack because there are two different payload types and two different payload fields and all of the entries in the second payload set against each entry in the first payload set will be tested.

Once all of the fields set have been configured with the type of data, the attack can be performed. Burp will perform the oftentimes tedious task of testing the data against the Web server as well as logging the responses for future indication as to which set of data worked and achieved the wanted results. As seen Figure 4, when starting the attack, a window is opened that shows each request with the data in each payload and the HTTP status code that was received in response to the request.

In order to provide even more flexibility, the tester can create rule sets to further modify the payload data sets. The tester could, for example, have a set of data that was stored in upper case and the user

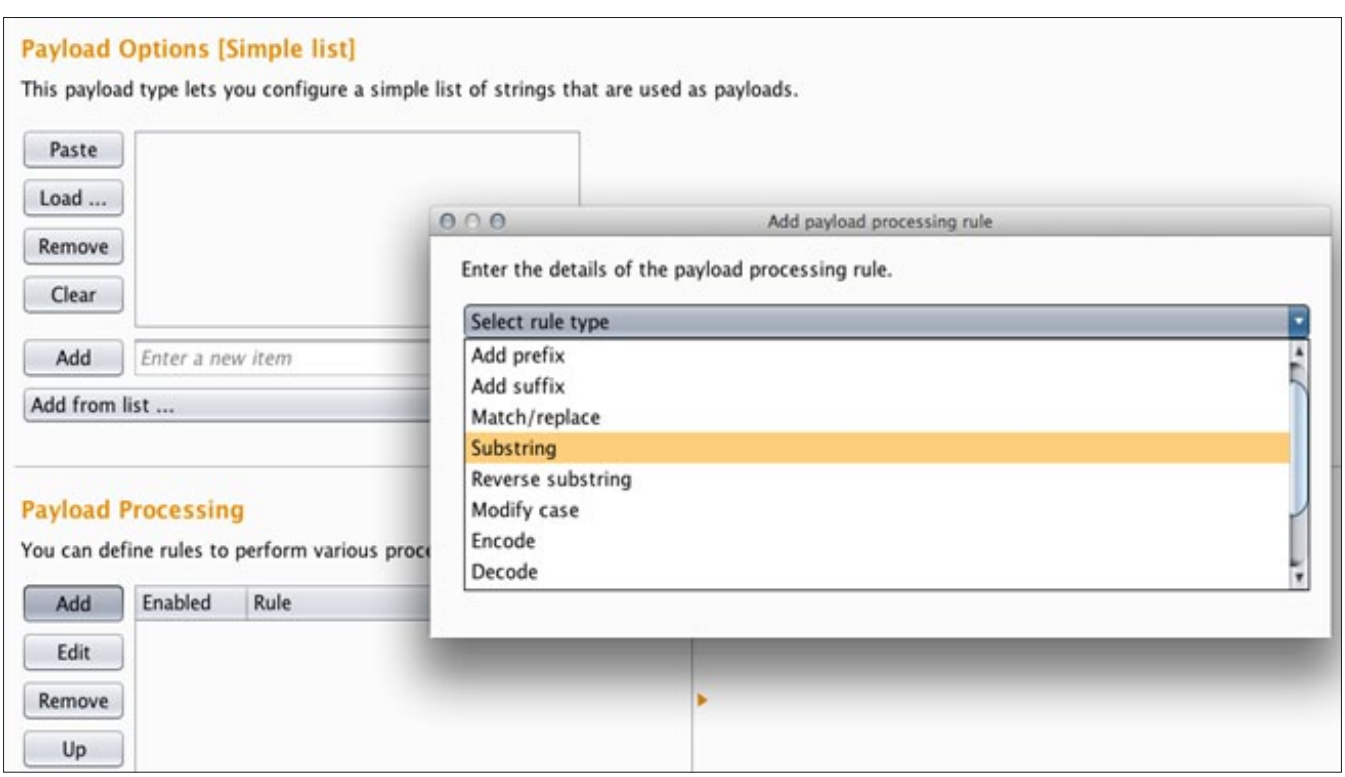


Figure 5. *Modifying payloads*

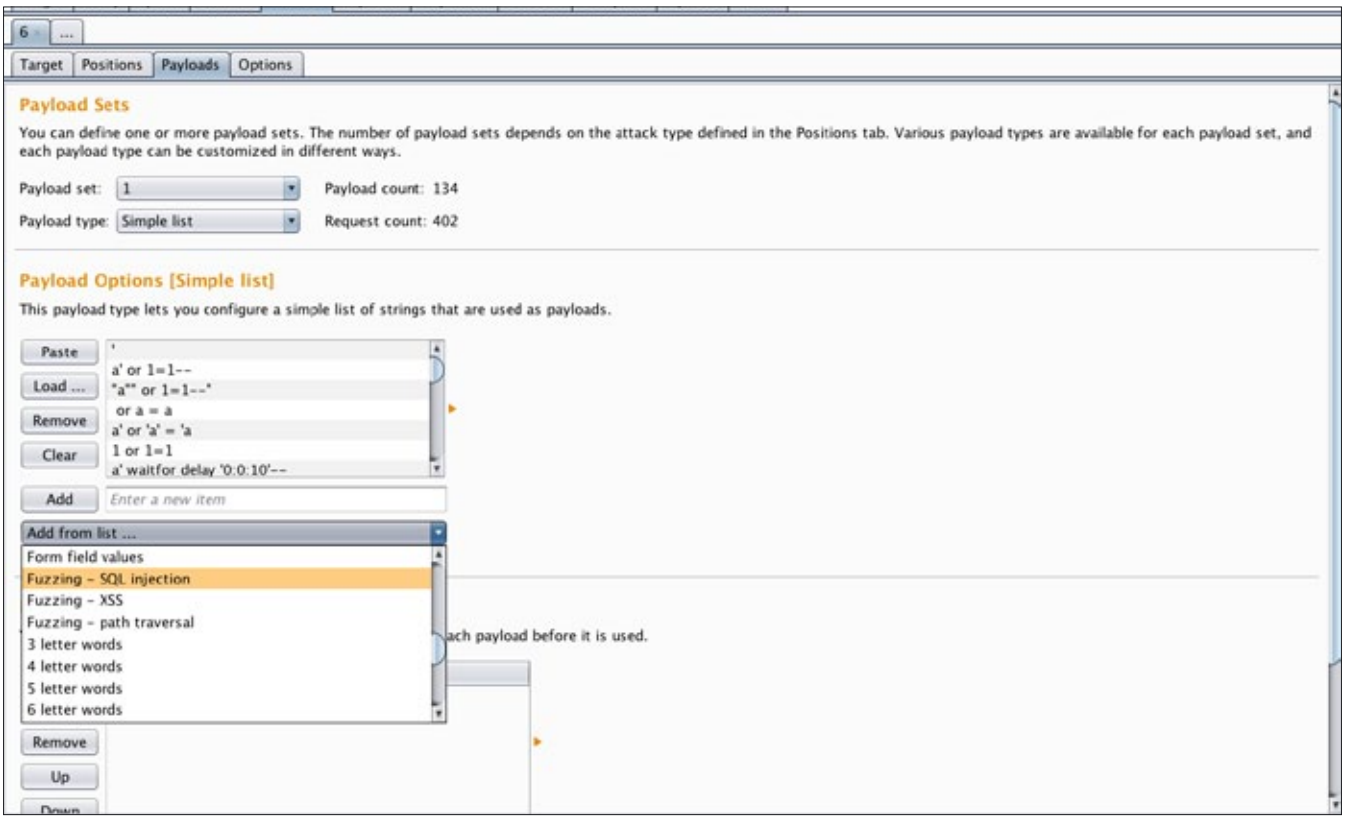


Figure 6. *Selecting SQL Injection attack*

could take that set of data and create a set of rules to manipulate the case to be lower or mixed case. This would allow the tester to generate one set of data and then make changes as needed, i.e. usernames and/or passwords case sensitivity (Figure 5).

XSS and SQL Injection

Burp Suite also allows password cracking much easier by taking the tedium out of multiple guesses and by tracking responses automatically for future reference. Due to the fact that SQL Injection and *Cross-Site Scripting* (XSS) attacks require numerous fields to be tested and checked, as well as checking the responses to determine if the attack was successful, the testing process can become quite tedious. Burp is useful while testing for these ever popular attacks by providing the ability to perform these attacks in an automated fashion.

To test for SQL Injection and XSS attacks, the tester would again use the Intruder functionality. This testing is performed in a similar process that was used for the username and password guessing attack. The first step is to send an HTTP request to the Intruder. At this point, changes to the fields that are going to be attacked can be made; depending on what the tester believes may be injectable. The only difference is when the payload is selected, "Fuzzing – SQL Injection" is going to be selected from the list. As shown Figure 6, there is also a selection for XSS attacks in the list as well. Once the appropriate payload sources for each field have been selected, the attack can begin. Burp will run through all of the payloads and indicate which responses reported useful information. The tester can review each request and response as necessary to determine whether it worked.

Conclusion

Burp Suite provides a powerful set of tools that not only perform automated scanning that can provide the tester with an overview of how the Web application handles security challenges, but also provide the ability to perform powerful, targeted attacks. Although only certain functions of Burp were explored in this demonstration, the techniques that were explained in this article can help speed up the tedious portions that are present in the Web Application testing process.

RIC MESSIER

Ric Messier is a security consultant who operates a small business, WasHere Consulting, Inc. (www.washere.com), helping customers with their security and networking challenges. Ric has a video training on Ethical Hacking coming out soon with Infinite Skills (www.infiniteskills.com). He also teaches graduate and undergraduate college courses in networking and information security at Brandeis University and Champlain College.

HACKTIVITY

The IT Security Festival in Central and Eastern Europe

October 12-13, 2012. MOM Cultural Center, Budapest

THE LARGEST IT SECURITY FESTIVAL IN CENTRAL AND EASTERN EUROPE WILL BE HELD AGAIN! Real festival mood, peresentations, workshops, games, hardware hacking, lockpicking, big friday party and 1000+ hackers from all over the world!!!

Keynote Speaker:

Jeff Bardin, USA

Jeff is the Chief Intelligence Officer for Treadstone 71. In 2007, he was awarded the RSA Conference award for Excellence in the Field of Security Practices. He is the most respected expert in the field of cyber crime, cyber terrorism, cyber inteligence.
This talk covers the cyber intelligence lifecycle including examples of denial and deception. Open source intelligence (OSINT) is a critical aspect of asymmetric cyber warfare. It is part of the mosaic defense and one practiced as a method of unrestricted warfare. Methods of cyber espionage, sock puppet creation, infiltration, data collection and analysis are covered. Case studies on creating your own personas while using OSINT tools will be discussed.

...and who can you look forward to?

ZOLTÁN BALÁZS / HUNGARY --- Zombie browsers, spiced with rootkit extensions
ALEXANDER POLJAKOV / RUSSIA --- Top 10 SAP vulnerabilities and attacks
JOE MCCRAY / USA --- The Evolution of Pentesting High Security Environments
ANDRÁS KABAI / HUNGARY --- Hunting and exploiting bugs in kernel drivers
ALEXANDER KORNBRUST / GERMANY --- Self Defending Database
VIVEK RAMACHANDRAN / INDIA --- Malicious Wi-Fi Routers for Fun and Profit
MIROSLAV STAMPAR / CROATIA --- Spot the Web Vulnerability
BOLDIZSÁR BENCSÁTH / HUNGARY --- Duqu, Flame, Gauss malware analysis experiences
SHAY CHEN / ISRAEL --- Diviner the new OWASP ZAP extension

PAYPASS VULNERABILITIES | HSRP INSECURITIES | „CHIP-TWEET” | TRACING MOBILE PHONES
ALTERNATIVE USAGE OF PKI DEVICES | LOCKPICKING 2.0 | ALTERNATIVE INTERNET
USB = UNIVERSAL SECURITY BUG | iOS SECURITY | ANDROID SECURITY | NAT ATTACK
BROWSER BASED ATTACKS | DIGIPASS INSTRUMENTATION | SECURITY CODE REVIEW
GEEK GIRLS | ELITE SOCIAL NETWORKS CROOKS | AV INSECURITIES

AND WHAT ELSE?!

Hello Workshops. Jump from theory to practice: **Hello Injection** **Hello CA** **Hello Code Review**
Hardware hacking / Lockpicking (non-destructivelock-opening) workshop and Urban Warrior competition / **24 hours - Hacker road reloaded.** Get prepared. Never experienced any similar game. Form a team, with a good hacker, a good lockpicker, a good social engineer.

Tickets are available until 20th of September with 10% discount on www.hacktivity.com

Full price for adults: 68 EUR / for companies: 150 EUR / Cheap hotels offering also there!

Special packages:
2 days ticket & 2 nights in a hotel*** 199 EUR
2 days ticket & 2 nights in a hotel**** 299 EUR
packages.hacktivity.com

Sponsors:

Further information and registration: www.hacktivity.com

Deloitte. | CCC THINK VALUE. | biztributor | WEBSHARK | ARUBA networks | ADNOVUM | FORTINET | HAKIN9 All About IT Security | asc

Memory Levels Gate Mitigation

Recently, software vulnerabilities have become a primary attack vector. Zero-day exploits threats have arisen, and becoming well-known and very effective attacks.

Searching for vulnerabilities and fixing them didn't stop hackers discovering vulnerabilities or prevent these threats. The runtime mitigations or 2nd line of defense becomes the only solution to prevent from these threats and decrease the chances to write a successful exploit for the discovered vulnerabilities.

The DEP, ASLR, EAF and other mitigations raise the security levels, decreasing the chance to write reliable exploits, but still hackers have ways to bypass them. Hackers created The *Return Oriented Programming* (ROP) technique to bypass these defenses.

Security Researchers created mitigations to stop ROP like ROP Defender and Windows 8 mitigation. Some of them bypassed these protections with heap play or returnless ROP or *jump oriented programming* (JOP).

In this research, I'm going to raise the security level more stopping the hackers from using the ROP or JOP techniques using a runtime mitigation based on DEP. This is my research in Bluehat Prize Contest 2011

The Problem

- Very similar to normal application flow.
- Doesn't use only the "ret" at the end of functions, but it can return to the middle of an instruction.
- Controlling the Memory Management APIs will not defeat ROP Attacks because they could use a 100% ROP shellcode.
- It could also use pop/jmp instead of "ret" instructions.
- You don't have a way to stop the execution of the application in the middle to analyze the stack calls or the execution flows

The Previous Solutions:

Although the ROP is very similar to the normal application flow, it has one main difference. The return oriented programming returns to APIs or returns to functions. They use the returns instead of calls and they can return to a place that didn't call it. Using this difference, most of security mitigations can detect what are normal calls and what's the ROP.

The Solutions could be categorized in 3 Types:

Binary Mitigations

This type of Mitigation is based on modifying the binary of the executable files … like adding checks before "ret" instructions, or reconstructing the code to prevent including a working gadget.

Some solutions are based on defending the "ret" instruction at the end of every function and its return address. You don't defend against ROP attacks … you defend against buffer overflow attacks, you do like "/GS", because ROP Attacks don't depend on the "ret" instructions at the end of functions … but they depend on the "0xC3" byte that's equivalent to "ret" inside an instruction, or like "mov ax,0453455C3" as it includes "0xC3" opcode.

The Binary Mitigations are very powerful if they are inside a compiler but can you force the vendor to use it? or in binary modification tools but they will be risky if these applications don't really contain bugs.

Sandboxing Mitigations

It's a good solution to use sandboxes but it will slow the application more and more

API Hooking

Using API Hooking maybe the best way because it could prevent the application from using your PC's resources and it's very near to the caller… but it contains problems:

- You need to Hook all API Functions with all internal APIs (like hooking Zw Functions and all above APIs in ntdll and Kernel32.dll)
- He could return after the API Hook (pass the first 5 bytes for example from the API)
- UserMode solutions could be bypassed, because he could return after the checks so he could bypass the idea.
- Could use SysEnter directly
- Could do like the check do (if the call is not ROP, it will set a variable, the ROP can use gadgets to set this variable itself)
- Need to be studied in Muli-Threaded Applications

Also, if the Kernel Mode solution is far away from the ROP Attacks, it can't examine the call stacks or it couldn't be near to the ROP calling the API.

The Advantage of this solution that it's very fast compared to the other solutions and it can be used without lowering performance.

The Solution

This solution is a mix between API Hooking and Sandboxing; powerful as normal API Hooking preventing ROP Attacks and nearly all bypassing techniques, without affecting performance like sandboxing.

This Mitigation uses API Hooking preventing the execution of whole executable pages inside system DLLs (ntdll, kernel32 and could be more) by removing the executable flag from its pages so it hooks all APIs by default preventing calling after the Hooking call at the beginning of the Function.

Also, it does all the checks in the kernel-mode and then switches the executable flag from the normal application to the system DLLs to check the return after the API finishes.

The Memory Levels Gate Concept

The concept of a Memory Levels Gate is to create a gate between two places in memory named "Levels". The first Level is the Kernel level (Level = 1) and it contains the kernel32.dll and ntdll.dll. And the 2nd Level is the User Level (Level = 0) and it contains all executable places in memory except kernel32 and ntdll.dll.

This Gate will stop the application and do some checks to be sure it calls to the 2nd level using normal calls and that no ROPs are discovered. After that, it accepts the call the 2nd Level giveing the application a Ticket to return with it. This Ticket is the return address.

When returning. The Application must return using the Ticket it took and return to the return address that it was previously called from to this level.

To create this gate, while running in the User Level we will set all executable pages in the Kernel Level to be not executable and the same while running in the Kernel Level. And when the application is accepted to call to 2nd Level, the Gate will set the 2nd Level to be executable and the 1st Level to be non-executable. With this trick, we will stop the application and watch the stack and detect ROPs.

The Practical Implementation

To implement this idea, you should write a device driver hooks the IDT (0) or hooking the exceptions of page faults (or execute a non-executable page) and this device driver does the checks and then saves the return address in a dynamic array of Tickets.

This device driver should work with SEH hooking LoadLibraryA and set the code section to be non-executable. It should hook the memory allocation and protection functions (in the kernel); searching for any page that will become executable. It should remove the PAGE_EXECUTABLE flag and write the address of this page and the number of pages in the executable places of the User Level.

For the security checking, you can write your own checks to detect the ROP while calling or returning using this gate.

The Security Checks

The problem that I faced while creating the security checks for detecting the ROP is that I'm between two things could make the idea un-implementable: "easy to bypass" and "incompatibility". I created these security checks to give you solutions to fix any incompatibility you could face. The Checks are:

- TheEip is inside the executable places of this Level. Like: If it's a call from User Level to Kernel Level, you should check the call-to-address to determine if it's really inside the executable places at the Kernel Level.
- Determine if the Return Address or [esp] is pointing to place inside the code section of any loaded module.

- The Eip must point to an API in the import table of the calling module or a function that was gotten by GetProcAddress in this module (the accepted addresses could be saved in kernel mode and checks run to determine if the Eip is one of them).
- The return address (RetAddr or [esp]) is pointing to an instruction after a "CALL [disp32]" (check if (RetAddr – 6)>0xFF 0x15) and check if this call really points to this "Eip" or this API.
- If this call is relative … check to determine if it points to "JMP DWORD PTR [disp32]"
- If the call is "CALL REG", check to determine if there's any "ret" or ret-like instructions very near to it (5-6 bytes) and "ret" (10-15 bytes).
- If a "ret" or a "ret-like" object is very near to the "CALL REG", check if the previous instruction is "movREG, APIxxx". If yes, accept only the calls to APIxxx.
- Because there are known applications that have these type of instructions ("CALL REG" and very near to it "ret" or ret-like instructions), to avoid Incompatibility, you have two solutions:
  - Saves the places (that contain these sequences of instructions) on every application and which API it should call to.
  - Do various checks on the stack and the frequency of ret or ret-like instructions that the return addresses point to. Check on the stack for ROP like return addresses.
- Check if [ESP -4] (the previously popped dword) is not equal to the Eip or not pointing to a "JMP" and there's no "jmp" very near to it (Optional – semi unimportant)

That's the security checks that I designed to stop the ROP. It should detect all types of ROP. You can perform more checks on the stack and frequency of return addresses very near to "ret" or ret-like instructions, but you need to make it as optimized as you can.

For SYSENTER

For the "SYSENTER" instruction, you should accept it (for Kernel APIs' SSDT index) while the application is in Level =1 (Kernel Level) and you must not accept it from the User Level.

For Multi-Threaded Applications

For Multi-Threaded Applications, the process is a bit complicated. To make them run without problems, you should run only one thread and suspend the others while running in the kernel level.

If the thread becomes waiting (for an Object or something), you should lower the Level to the User Level and resume the threads again

If thisThread becomes ready, you should raise the level again and suspend all threads and then, resume this thread.

If this thread becomes ready and there's another thread running in Kernel-Level, the ready thread should be suspended until the other thread in the Kernel-Level finishes the kernel usage and then, resume the ready thread again.

You can improve the idea for the multi-threaded applications. I don't have much knowledge to cover all the side effects, but Microsoft could deal with this.

The Advantages

- This Mitigation will make the use of Return Oriented Programming or return-to-libc too hard if not impossible to use in Windows. It detects all known types of ROP and stops them before playing with your system.
- This Mitigation gives you a complete supervision of your Kernel APIs and the ability to write any check that could give you a higher level of security. You can add more than "Kernel32" and "ntdll" to the Kernel-Level

The Disadvantages

- It will decrease the performance with many page faults (but it will be handled in the Kernel-Mode … so you could optimize the performance) and many checks on every call.
- It has side effects on Multi-Threading applications.
- Could lead to incompatibility (you could fix this problem with the solutions that I wrote)

The Prototype

The Files

The prototype contains two files:

- VulnApp.exe: This executable file contains two applications: The Vulnerable Application and the Executer application that runs the Vulnerable Application with or without the MLG Mitigation and gives it the exploit buffer that triggers the vulnerability of the Vulnerable Application and overwrite the return address
- MemLevelGate.dll: this dll file contains the mitigation application.

The Concept:

This Prototype is a proof-of-concept application. It describes the idea in action in a very simple way and applies the mitigation in a very simple shape.

This prototype uses SEH instead of a kernel-mode device driver and it creates a gate between these:

- Kernel Level: and it contains the user32.dll only (as the Vunlerable Application and the Exploit will try to use MessageBoxA and you will determine how it detects ROP and the real call).
- User Level: it contains only the VulnApp.exe module.

Also, I decided to use The READ flag instead of EXECUTE flag to make the prototype compatible with all windows versions and to all Process settings (you don't need to run the process on custom setting or run it with EMET).

It applies some of the security checks described in section 6. It detects ROPs and writes to the console the result and terminates the application.

Conclusion

As I said, Return Oriented Programming is a very powerful technique and very similar to the applications' normal flow. You don't have any way to stop the application and watch for ROPs.

Memory Levels Gate (MLG) is a method to solve this problem. It gives you a supervision of your sensitive kernel APIs that could convert any normal buffer in the stack into a ghost that could play with the whole OS. The idea gives you a gate (using the NX or XD flag that are used in DEP) to control the calls to your kernel APIs and checking for ROPs.

But your security checks(that detect ROP) could lead to one of two other ghosts: 1. Easy to bypass or 2. Incompatibility. It's hard to find the optimum design for your security checks. So, I created two Modes (normal and high modes) to stop any way to bypass the mitigation and solutions for any incompatibility problem you could face.

Also, the mitigation could lower the performance or become very complex to code. So, as I said, it's related to how much you could pay for security and what's other solutions you could use to stop the ROP (if you have others) and the cost of every solution (performance and complexity) and what you could choose to rise your security.

AMR THABET

I'm a Freelancer Malware Researcher and Penetration Tester recently graduated from Alexandria University faculty of engineering. I'm the Author of Pokas x86 Emulator, a speaker in Cairo Security Camp 2010 and a speaker in Athcon Security Conference 2011 in Athens, Greece. You can find more about me in my website: http://www.amrthabet.co.cc.

Anti-Rootkits in the Era of Cyber Wars

This article describes the design of a detection system of hidden objects in modern situations. It describes various trends of virus attacks, analyzes potential virus attacks targets and mentions the statistics from the US laws and McAfee reports.

This article is intended to provide a concept of information security system design, particularly for stealth detection. The author's method of stealth detection based on dynamic bit signature is described.

In the last two years, information security issues have been front and center within various news sources. Some of the major issues that have been covered in the media included Stuxnet, Duqu, and Flame. By learning of these tools and their capabilities, it is important to think about what could be next.

An article written by David E. Sanger titled "Obama Order Sped Up Wave of Cyber-attacks Against Iran" was published in "New York Times" on July 1, 2012. This article mentioned the Stuxnet worm that hit Iran's nuclear facilities was cooperative work of the United States and Israel.

A few weeks later, on July 19, 2012, an article titled "US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say" was published in The Washington Post that included information about the authors of the "Flame" virus.

As shown, special services of one country was able to remotely disable industrial, civil and military infrastructure of another country. This infrastructure is now managed by SCADA automated systems, security aspects of which will be covered in the article.

Scada And Cnc Systems

Speaking of cyber wars, we cannot avoid the topic of SCADA.

When mentioning cyber wars, the topic of SCADA (*Supervisory Control and Data Acquisition*) systems cannot be ignored. SCADA is the result of evolutionary development of control systems. SCADA is software that controls various technical processes. It is used in all major control systems from air-conditioning systems in business centers and water treatment systems to oil pipelines and transportation control systems on a large scale.

Due to the specific use and operation complexity of SCADA systems, it is difficult to test them as thoroughly as other systems and as a result, may contain more vulnerabilities. It is often seen that any system that is widely used, attacks are created to target those systems, especially if those systems are known to be easily exploitable. These two facts make SCADA systems easy targets.

In the United States Federal law S.773 – Cybersecurity Act of 2009 in part SEC. 2. FINDINGS, in paragraph 4 it is defined that:

"More than 85% of all critical infrastructures are in private hands. Cyber threats for government information systems and critical infrastructures are evolving and growing"; and

"(4) With more than 85 percent of the Nation's critical infrastructure owned and operated by the private sector, it is vital that the public and private sectors cooperate to protect this strategic national asset".

In paragraph 9, Paul Kurtz stated:

"the United States is unprepared to respond to a 'cyber-Katrina' and that a massive cyber disruption could

have a cascading, long-term impact without adequate co-ordination between government and the private sector".

According to the 2011 report, "In the Dark Crucial Industries Confront Cyberattacks", prepared by Stewart Baker, Natalia Filipiak and Katrina Timlin from McAfee it is stated that:

"among 200 heads of mission-critical facilities in 14 countries, 80% of them are faced with large-scale cyber-attacks, while 25% were even subject to extortion by the attackers. 30% of companies are not ready for such attacks, while 40% think they will be aimed by hackers next year."

The article, "SCADA hack talk canceled after US, Siemens request" prepared by Elinor Mills for *cnet.com* reported that:

"a report on how to hack SCADA systems was canceled by request of Siemens representative, According to an expert it was 'due to a lack of possibility for Siemens to cope with existing security threats'. Two researchers say they canceled a talk at a security conference today on how to attack critical infrastructure systems, after U.S. cybersecurity and Siemens representatives asked them not to discuss their work publicly."

In connection with the ability to control CNC machines remotely via Ethernet or Wifi-connections, new information security threats need to be solved.

Potential Targets Of Virus Exposure

Before proposing an action plan, it is important to analyze potential targets of viruses' impact.

A virus can affect the following components of the automated system:

- User data – working documents and multimedia data can be damaged or deleted
- Software – operating system and applications operation can be disrupted: both popular software packages like Microsoft Office, and specialized software such as Mathcad and Matlab.
- Hardware – both primary equipment, such as motherboard and hard drive and peripheral equipment, such as a printer, lathe with CNC, etc. can be put out of action. For example, the virus Stuxnet affected PLC-controllers of SCADA-systems made by Siemens.
- Telecommunication infrastructure – interaction between network nodes can be disrupted, and network equipment can be disabled.
- User – well-being and health can be harmed by using low-frequency waves from internal loudspeaker of system unit.

Why Can't Viruses Be Stopped?

There are three main reasons:

Vulnerability of perimeter protection

It is extremely difficult to prevent virus writers from obtaining corporate versions of commonly used protection systems. This allows for virus writers to study and analyze how the systems work and where they are vulnerable. With that said, repeated testing of viruses and changing its operation algorithm or obfuscations code, can ensure that the protection system will not detect the virus, so it is ready to use.

Virus writers use both steganography and technical stealth techniques, which do not allow detection of a malicious object heuristically. Hackers bypassed validation of digital signatures of drivers using this technique (Stuxnet used certificates of Realtek and JMicron, and Flame uses certificates of Microsoft itself (2718704)). The result was "Microsoft Driver Signing" system does not fully meet new challenges.

Lack of appropriate pre-emptive work in business companies

It is often not profitable for businesses to invest funds to projects that do not return a profit.

An example of this is hardware virtualization. Hardware virtualization can help protect systems against malware and other malicious software; however, companies oftentimes do not want to invest in virtualization software because they do not see a dramatic return. In Symantec Endpoint Protection 12.1 hypervisors a detection module has been embedded, and McAfee DeepDefender is based on a hypervisor. Unfortunately, only a few companies have taken this into account.

Complexity of advanced viruses' analysis

Experts of antivirus companies, even after receiving virus samples, cannot always study them fast enough to completely stop an infection. Due to the nature of viruses, until they have been created, there is no fix for them. Therefore, in the instance of Stuxnet virus, fixes took several months. The Flame virus, being much more complicated, may take much longer to study. This does not even be-

gin to mention what is out there that has not yet been detected.

The mixture of sophisticated viruses that cannot be stopped and vulnerable systems that are impossible to defend is quite alarming.

The Proposed Approach For Detection

Pursue a preemptive tactic

Any weapon can become obsolete especially in the world of information security. At present, we see that virus technologies are improving faster than antivirus vendors can respond.

It is necessary to create a rootkit lab to test and analyze rootkits to determine how to current "undetectable" rootkits could be detectable using security measures.

Use as unique and varied approaches to virus detection as possible

The creation of viruses is usually associated with issues of their hiding in the OS. To ensure detection of hidden objects, it is necessary to develop new and unique ways of detection, regardless of the concealment method the virus is using.

Below is a method of detection of concealment in Windows OS.

After starting a process, a number of structures corresponding to this process are created in memory. They include structures EPROCESS, ETHREAD, and structures of handles. They are joined in a list. Drivers structures and are in kernel memory, while service structures are in user mode memory of the SERVICES.EXE process (Figure 1).

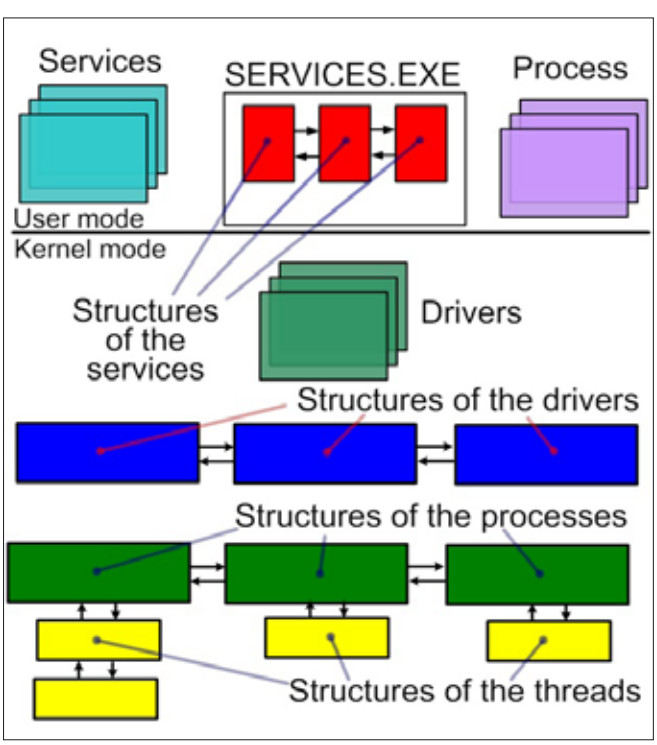


Figure 1. *Process, threads, drivers and services structures in OS Windows*

Standard OS tools collect information on running processes by passing through the list of EPROCESS structures and while using links between the structures.

As a way of hiding a classical method "DKOM" will be used. This method involves changing pointers of neighboring ERPROCESS structures (Figure 2).

For detection of concealment, it is necessary to obtain a list of processes on the basis of other list since ERPROCESS is already broken at this point.

Popular anti-rootkits use multiple lists, and, if anomalies are detected, they indicate that there is concealment. However, for the purpose of resistance to anti-rootkits, virus writers may remove corresponding structures from other lists.

The essence of the proposed method of detection is to search memory structures "similar" to EPROCESS structures without taking into account links between them (Figure 3).

To detect hidden process, the following operations need to be performed:

- Create a *dynamic bit signature* (DBS) of the process structure as a template, which "fits" to all EPROCESS structures loaded into memory.
- Search for match of some part of memory with the received by the DBS with the help of probabilistic test. The search is conducted through analyzed memory; and as a result a list of processes (author's list) is received.
- Compare the author's list with a list of processes obtained by standard means of the OS. If you find that in the author list there are processes that are not in the list obtained by regular means, it is concluded that these processes are hidden.

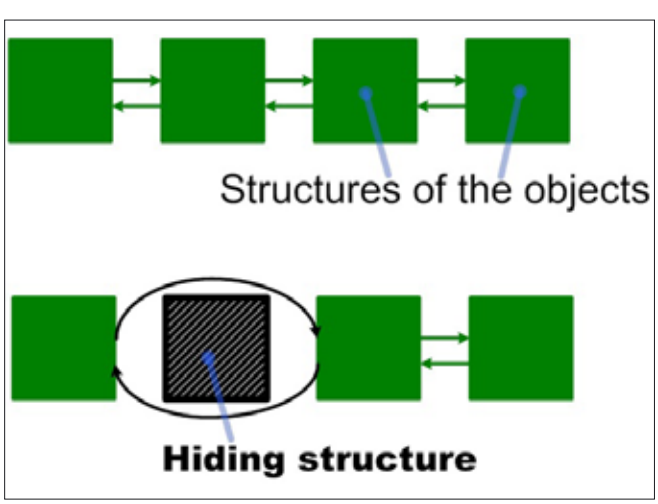


Figure 2. *Sample of hiding objects*

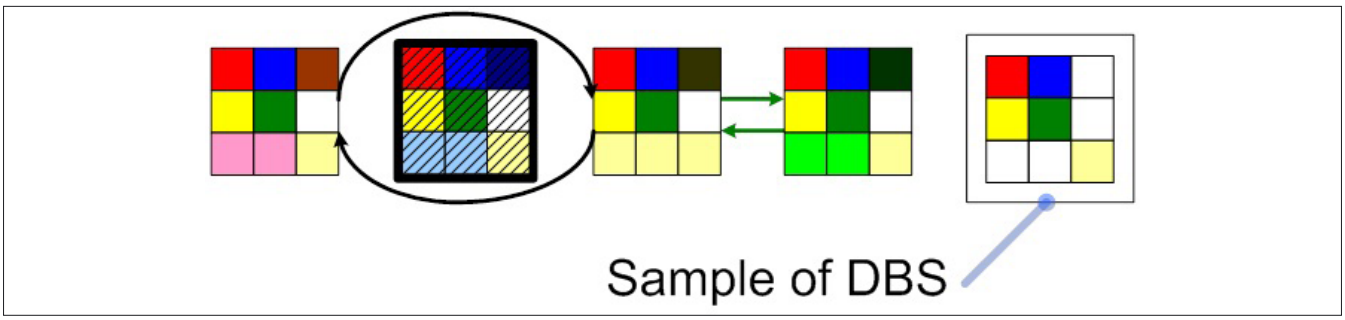


Figure 3. *A list of objects structures and a sample of dynamic bit signature*

It is necessary to perform the following steps to create the DBS:

- To pass through the list of existing structures of EPROCESS and compare them bitwise.
- When a match of a specific bit in all structures is found, it is necessary to save the value of this bit and the offset.
- Perform steps 1 and 2 in a loop for all bits of EPROCESS structures. As a result to get DBS process structure.

When searching for "similar" fragments of memory 80-90% of the template structure match is enough. This method of hidden processes detection on basis of DBS has several advantages:

- Due to the fact that EPROCESS structure template contains about 300 significant bits, practical probability of false operation is equal to zero, while probabilistic verification can detect even deliberately altered structures;
- The DBS does not use any Windows functions to get the final list of objects and, therefore, it is much more difficult to resist it. The result of the method cannot be changed by interception or modification of kernel structures;
- DBS provides portability of the method, because structures of EPROCESS have changed in different OS and service packs.

The idea of signatures is not new. Andreas Schuster from Deutsche Telekom AG Group Security suggested an approach of static signatures for process detection in the paper "Searching for Processes and Threads in Microsoft Windows Memory Dumps". His signatures depend on version of OS Windows while DBS does not need to be aware of this.

Counteraction to detection is possible, but only by resetting all fields of chosen structure, which leads to disruption of the system – BSOD.

DBS provides a portable way on all 32-bit OS Windows, and to detect hidden objects in 64-bit OS Windows you only need minimal changes in the source code.

The method of detection is prompt, since it does not require viral activity, for example, working with file system, registry, or network. This method certainly does not solve all problems of hidden software, but its regular use provides control of hidden processes absence, which is a lot.

- Continuous development and improvement.

It is necessary to carefully monitor publications regarding new and advanced computer technologies, operating systems and their protection controls. It is necessary to hire experts, to provide training, and actively participate in professional conferences.

Using the three steps outlined above will help build a detection system, which is technically very difficult to resist.

IGOR KORKIN

Igor Korkin – Ph.D., a specialist in information security. He works at Moscow Engineering Physics Institute, training post-graduate students and supervising students. Has been engaged in rootkit technologies for over 5 years, the author of more than 10 scientific papers, winner of the "Hackers versus Forensic on Forum "Positive Hack Days 2012" in Moscow, Russia. Author's publications can be followed on his website at sites.google.com/site/igorkorkin.

Web Filtering with Websense

To be or not to be filtered: that is the dilemma

Websense is my new "toy" in my security arsenal. But there were things that I started to ask myself about it. Especially, when you setup a security profile and then came people requesting permissions for sites that they consider "indispensable" for the duties. So, to be or not to be filtered… That is what I am going to share with you: my dilemma. Is it a formula for a good web filtering? Let see it.

In this article, you will learn what is Web filtering, how it works, Websense solution, and basic considerations when you are choosing your Web filtering solution. Enjoy the reading!

What is Web Filtering?

Web filtering, also called content filtering on Web, is a group of methods or techniques used by enterprises to prevent computer users from accessing inappropriate web sites. Also it is used to prevent access of known malware hosts and a way to prevent an inappropriate use of the organization limited bandwidth.

It is well-known that the primary reason for organization insecurity is the internal employee. For that reason, Web filtering should protect against what is being sent out from the computer. With the number of blogs, wikis and personal storage sites, a company's web filtering solution must be able to inspect outbound content to make sure company data is not being lost.

Why it is so important?

If you asked IT people about the importance of Web Filtering, the first thing they would say is: to save bandwidth. And sometimes, the bandwidth limitation is the primary reason that an organization decide to obtain this kind of solution.

But network performance is just one of the reasons that we should consider to implement this technique in our organizations.

- Enhance Employee Productivity: Without a Web filter, employees could waste time surfing for things that have nothing to do with your jobs. Spending time doing things on the Internet that they shouldn't be.
- Avoid Legal Liability: Keep in mind that the most common way employees misuse the Internet is to surf porn. Imagine the co-worker accessing this type of content, that depending of the country is considered illegal, and a colleague is offended by that action results in lawsuit against the company. This is too delicate.
- Improve Network Performance: As we discuss previously, some co-workers download tons of content like videos, music, streaming media that saturate network resources. Here appears the famous question… the network is too slow, why?

Websense… what is that?

In the market there is a good quantity of options of what to choose when you decide to implement a Web filter, from commercial expensive product to free Open Source options.

Figure 1. *Websense Logo*

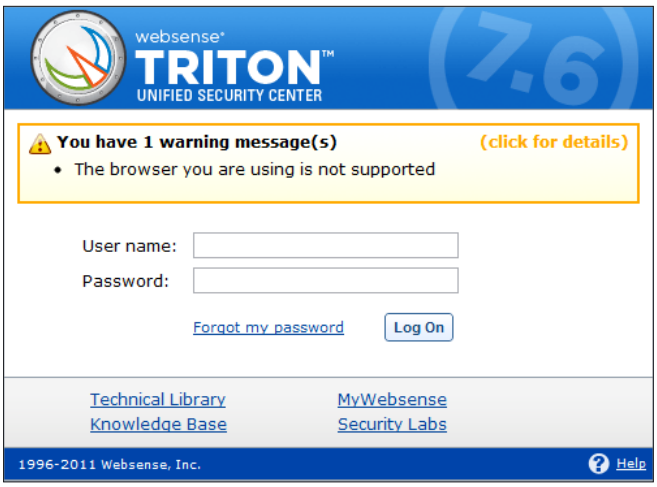


Figure 2. *Websense login window*

Here we are going to review Websense, founded by Phil Trubey in 1994.

From Wikipedia, "Websense is a San Diego-based company specializing in web filtering software. Their software is used by customers, including companies, schools and libraries, to protect their networks from spyware, prevent students from viewing sexual or other inappropriate content, discourage employees from spending time browsing webpages instead of working, and similar purposes".

Apart from web filtering, Websense provides software-based, appliance-based and cloud-based email security, and data loss-prevention technology (Figure 1).

Websense is software that shows a complete picture of who is using the network, how the network is being used and when the network is being used. Websense allows network administrators to block access to web pages and other protocols based on categories.

Also, it tracks individual internet usage for the purpose of reporting on any browsing deviating from the standards set by the policies, and its reports can be sorted by category, URL, application, user, workstation, dates, and more.

How it works?

I have the opportunity to work with a stand-alone product where Websense software detects the client's Internet request, and then queries the Filtering Service to determine whether the request should be blocked or permitted.

But also Websense can be an integrated environment with your firewall, proxy server, caching application, or network appliance.

When a client requests a website, Websense identifies which policy currently applies, and which categories have the Block, Confirm, or Quota action applied by that policy.

Clients can be computers or networks. Or if you configure Websense software to communicate with a supported directory service, that is amazing and functional, clients can also be users, groups and domains/organizational units.

Websense also permits filtering protocols other than HTTP, such as those used by instant messaging, streaming media, and file sharing applications (Figure 2).

Are there exceptions to the rules?

Filtering rules are typically set by the IT department. Depending on the filtering plan, it may be possible for different computer users to have different levels of internet access. Here comes the dilemma: keep it simple or do granular filter rules?

Web filters can often cause problems by blocking sites they shouldn't be blocking that could af-

Figure 3. *Websense main window*

fect business processes. Keep in mind that your design should be in line with business goals. Your best weapon: organizational security policies.

Beware… first define your security policies to establish which websites can be accessed and which cannot. An acceptable user policy or internet usage policy should be in place before implementing web filtering. Then, only then, apply software to help you with that filtering necessity (Figure 3).

Remember that Web filtering is meant to help enforce existing security policies. Employees should already have a clear knowledge of what is allowed before monitoring and filtering of web access is implemented.

A little bit of happiness… quota action

One of the options offered by Websense that makes my co-workers a little bit happy is the quota action. But what is that?

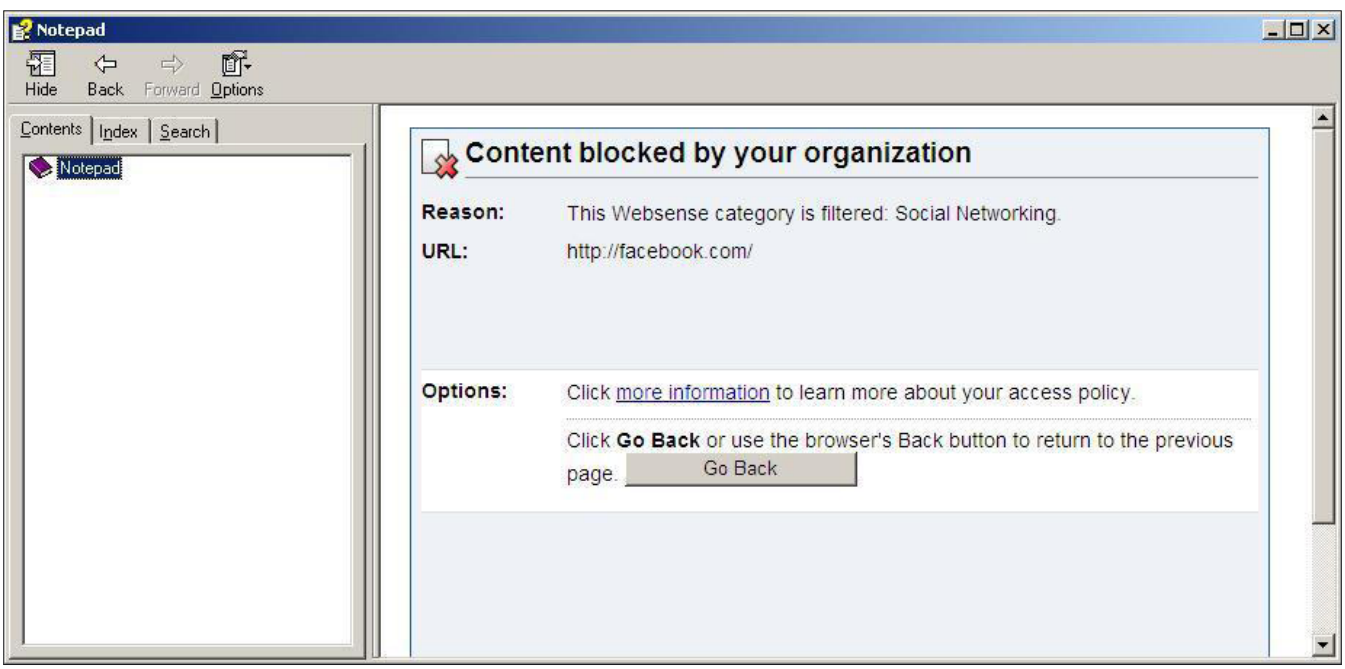


Figure 4. *"Content blocked by your organization" Websense message*

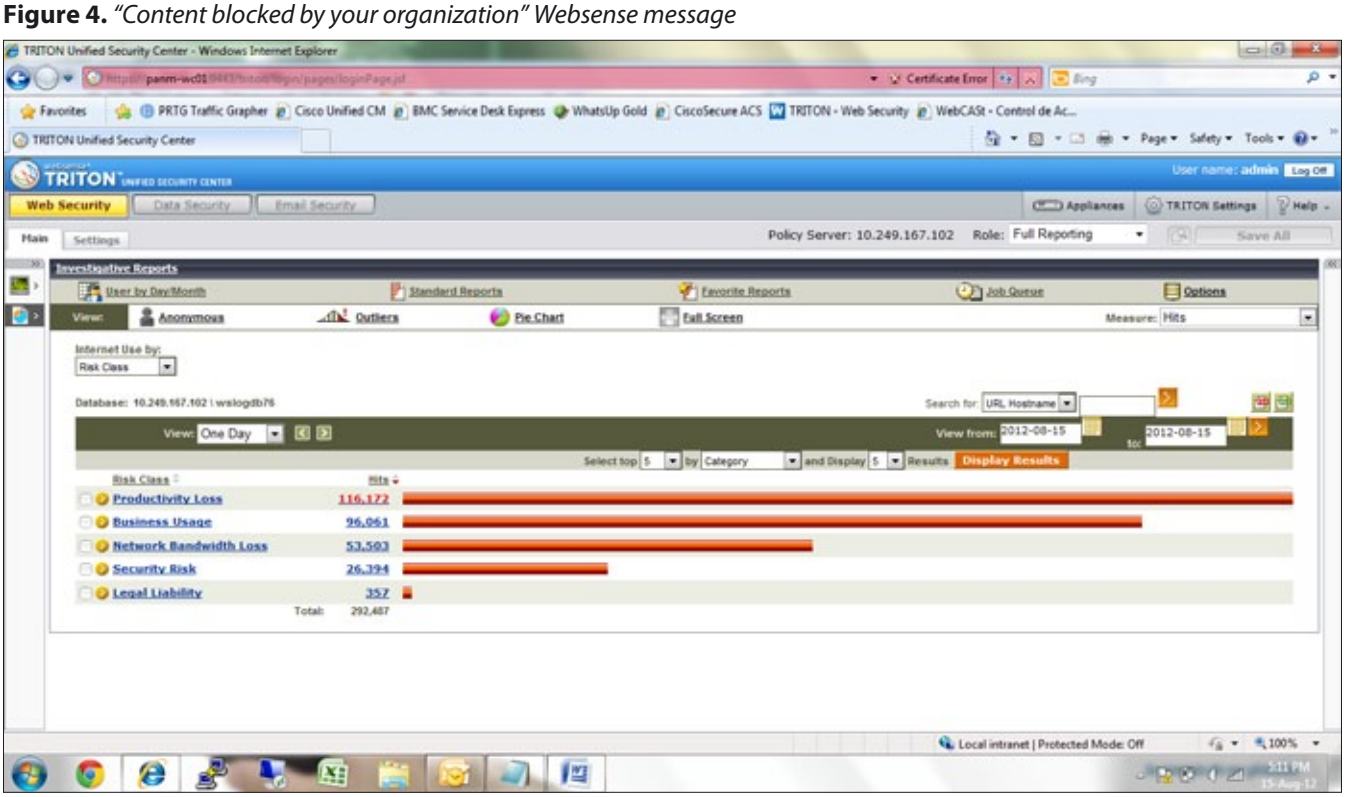


Figure 5. *Websense reporting*

Defined by Websense, it is an option that "gives employees access to sites in selected categories for a limited amount of time each day".

Quotas give you control over how much time your employees spend on personal surfing and what URL categories they are accessing.

"When a user requests a site in a quota-limited category, a block message presents the option to view the site using quota time. Clicking Use Quota Time starts a quota session, during which the user can view sites in any quota category, as well as view permitted sites and sites classified under Miscellaneous/Uncategorized in the Master Database. After the quota session ends, requesting another site in a quota category results in another quota block message. If quota time remains, the user can start a new quota session. If no time remains, the user can click Go Back to return to the previous page."

Quota time is "billed" on a daily basis per user. So, once it is used up, clients must wait until the next day to access sites in quota categories. To change the amount of default quota time, use the following path: *Server > Settings > Common Filtering*.

Are you asking if it is possible to bypass Websense?

Let me be honest with you… it's quite difficult to bypass Websense. The have a huge database of bypassing websites. Websense looks for trends like these and locks them down daily. But if you want to try it's ok. Let me tell you how to do it (it could be useful with other Web filters).

Cross your fingers to find a proxy or circumvention site that hasn't been blocked. That is the key step. Sites such as *https://www.proxy.org* offer a way to bypass Websense by using a secure connection. You can access the proxy web site, and then access blocked sites through that.

Type the URL you want to go to in the box on the site. The way this works is that the proxy avoidance site is hosted on a non-filtered connection. The page is routed through that connection to your computer.

Choosing an appropriate Web filtering solution

It is true that there exists other solutions than Websense, so let me lists some basic elements that you should consider when you want to select a Web filtering solution.

First, remember that the orchestra masters are the security policies. So, the features of the filter should match to the company's needs.

References

- *http://en.wikipedia.org/wiki/Content_filtering*
- *http://www.netsentron.com/forum/content-filter-why/*
- *http://www.futuresoft.com/products/ifilter/ifilter_7.0_whitesheet.pdf*
- *http://www.wikihow.com/Bypass-Websense*

Also, it is necessary to consider that the implementation should not impact business operations and network infrastructure, including the use of Active Directory. The filtering solution should easily be integrated.

The solution should permit granular policies; the web filtering solution should allow the company to control web access for individual users. If the company has telecommuting users, the web filtering solution should control web use of these users.

Finally, consider reporting capabilities and configuration tools of the web filtering solutions. And the maintenance procedures of the database, that is the core information of the Web filtering solution (Figure 5).

Don't forget to select a Web filtering solution that handles proxy sites and filter HTTPS protocol.

Conclusions

As you see… everything depends on the situation. It is important to understand the business requirements and define security policies before you decide to implement a Web filtering solution.

It is not filter just for filter, or permit just for permit. As we learn in this article there are certain reasons to implement a Web filter and parameters necessary to consider when you are choosing and then configuring your Web filtering solution.

ABDY MARTÍNEZ

Abdy Martínez, Telecommunications Administrator at AES Panama, is specialized in Network / Information Security and Forensics.

CCNA Security, CompTIA Security+ (2011 objectives) and CCDA certified.

Password

Construction and Management

Passwords are our first line of security. In the era of defense-in-depth, gone are the days of simply installing a firewall, antivirus, and spam filter. Although these technologies can act as a defense against the common hacker and threat, if credentials to a network are intercepted, these devices are useless.

Many security incidents and data breaches originate from lack of adequate password construction and management policies.

Executive Summary

At the heart of compliance, (SOX, PCI, PIPEDA, or HIPAA), is access management and authentication. And at the heart of authentication are User IDs and Passwords. For example, the section 404 of the Sarbanes-Oxley Act of 2002 requires a publicly-held company's auditor to attest to, and report on, management's assessment of its internal controls. All internal controls are futile if the password for the system containing the final report is compromised.

Recent regulatory controls over businesses that process credit cards, store confidential information for individuals, or are listed on the stock market require that passwords are stored in a controlled environment with restricted access to only the people that need it. That said, having a strong password construction and management standard goes far beyond meeting regulatory controls.

Key Considerations

Although alternative technologies for authentication, such as biometrics, smartcards, and one-time passwords, are available for all popular operating systems, most organizations still rely on traditional passwords and will continue to do so for many years. Therefore, it is very important that organizations define and enforce password policies for their systems that include mandating the use of strong passwords. Strong passwords meet a number of requirements for complexity – including length and character categories – that make passwords more difficult for attackers to determine. Establishing strong password policies for your organization can help prevent attackers from impersonating users and can thereby help prevent the loss, exposure, or corruption of sensitive information.

Strong password policies can be enforced on the domain controller or on a stand-alone computer depending on if the organization uses computers as a part of the domain or as independent machines. Most organizations have computers connect to the domain so that the security policies, etc., can be centrally managed. A strong password policy can be defined on the domain controller. Once an appropriate password policy has been configured, users in your organization will only be able to create passwords that meet the criteria defined in the aforementioned password policy. But before a company implements password policies, they must first identify what settings are relevant in their environment. Once that is determined, the following points will make sure that our password security is enforced:

"Establishing strong password policies for your organization can help prevent attackers from impersonating users and can thereby help prevent the loss, exposure, or corruption of sensitive information."

Complexity is the best policy

A non-complex password containing a word that exists in a dictionary could be compromised within

a matter of a couple seconds. Hackers can now leverage extremely fast processing powers to "brute force" even the most complex passwords. Although they can be cracked, complex passwords should contain so of the following characteristics in an effort to deter a hacker from cracking their password:

- English uppercase characters (A – Z)
- English lowercase characters (a – z)
- Base 10 digits (0 – 9)
- Non-alphanumeric (For example: !, $, #, or %)
- Unicode characters

Is a complex password alone enough?
Although the complexity of a password is important, there are still many other settings that should be considered while creating a password policy.

Password History
Enforce password history determines the number of unique new passwords a user must use before an old password can be reused.

Password Age
Maximum password age determines how many days a password can be used before the user is required to change it. Setting this value too low can cause a frustration for your users; setting it too high or disabling it gives potential attackers more time to determine passwords. For most organizations, set this value to 45 days.

Minimum password age determines how many days a user must keep new passwords before they can change them. This setting is designed to work with the "enforce password history" setting, so that users cannot quickly reset their passwords the required number of times and then change back to their old passwords. The value of this setting can be between 0 and 999; if it is set to 0, users can immediately change new passwords. It is recommended that you set this value to at least 5 days.

Password Length
Minimum password length determines how short passwords can be. Most operating systems support passwords up to 28 characters. If it is set to 0, users are allowed to have blank passwords, so it should never be set to 0. It is recommended that this setting be set this value to 8 characters.

People are the weakest link
A company might have the most sophisticated perimeter security mechanisms and the most robust password construction and management protocols, but if a trained social engineer can obtain a username and password from an employee, all of those devices are useless.

> *"All Passwords can be cracked if there is enough time."*

Historically, efforts on password mechanisms have focused mainly on technical issues. Only in recent years has the security community recognized that user behavior plays a part in many security failures, and that policies alone may not be sufficient to ensure correct user behavior. The most beneficial way for a company to thwart this security concern is to train their employees through awareness. Security awareness training covering password security and making users aware of social engineering has proven to work really well.

In most organizations, users cannot be forced to comply; rather, they have to be persuaded to do so. Ultimately, the mechanisms themselves, policies, tutorials, training and the general discourse have to be designed with their persuasive power in mind.

Managing privileged passwords (Keys to the castle)
Privileged passwords are rightly called 'keys to the castle' as they permit the users to get virtually unlimited access and full controls to the IT resources such as servers, databases, network devices and IT applications. It is increasingly becoming evident that managing privileged passwords with multiple layers of security is in the best interest of the organization. The most common practices that leads to improper management of privileged passwords are:

> *"Policies alone may not be sufficient to ensure correct user behavior."*

- Assignment of a common password to multiple privileged accounts for ease of use.
- Assigning non-expiring passwords for admin accounts.
- Hard-coded passwords enabling application-to-application communication.
- If an administrator leaves, he/she goes out with the password that is less likely to be changed.

The most practical way to manage privileged passwords is "atomization." Privileged Password Management solutions act as the alternative for

the traditional, inefficient and insecure password management processes. Some of the preventive, detective, and corrective actions these products may perform are:

- Password storage in encrypted repository.
- Access to the repository is enforced based on least access privilege, need to know, and segregation of duties. A Unix administrator is now only able to obtain the password for the Unix box and not the windows box.
- Passwords are automatically changed after a predefined interval of time, assigning a strong and complex password. Insiders can no longer make guesses.
- Real time audit reporting and alerting. All password access activities are completely audited and exceptions reported.

Some of these solutions might add real value to your password management efforts.

Password Self-Serve Utility

Some organizations are increasingly using and advocating self-service portals for users to reset their own passwords; so much so that password resetting authority has been removed from the conventional helpdesk role. Password self-serve can not only reduce the helpdesk cost but also eliminate password compromise as a result of an attacker impersonating a legitimate user. Key advantages of a password self-serve utility are:

- Users can reset passwords themselves.
- Users can unlock their accounts.
- Provides secure channel of resetting user accounts via pre-enrolled security questions.
- Makes users more productive.
- Reduces burden on the helpdesk.
- Saves helpdesk cost.
- Ability to log on user password change request activity.

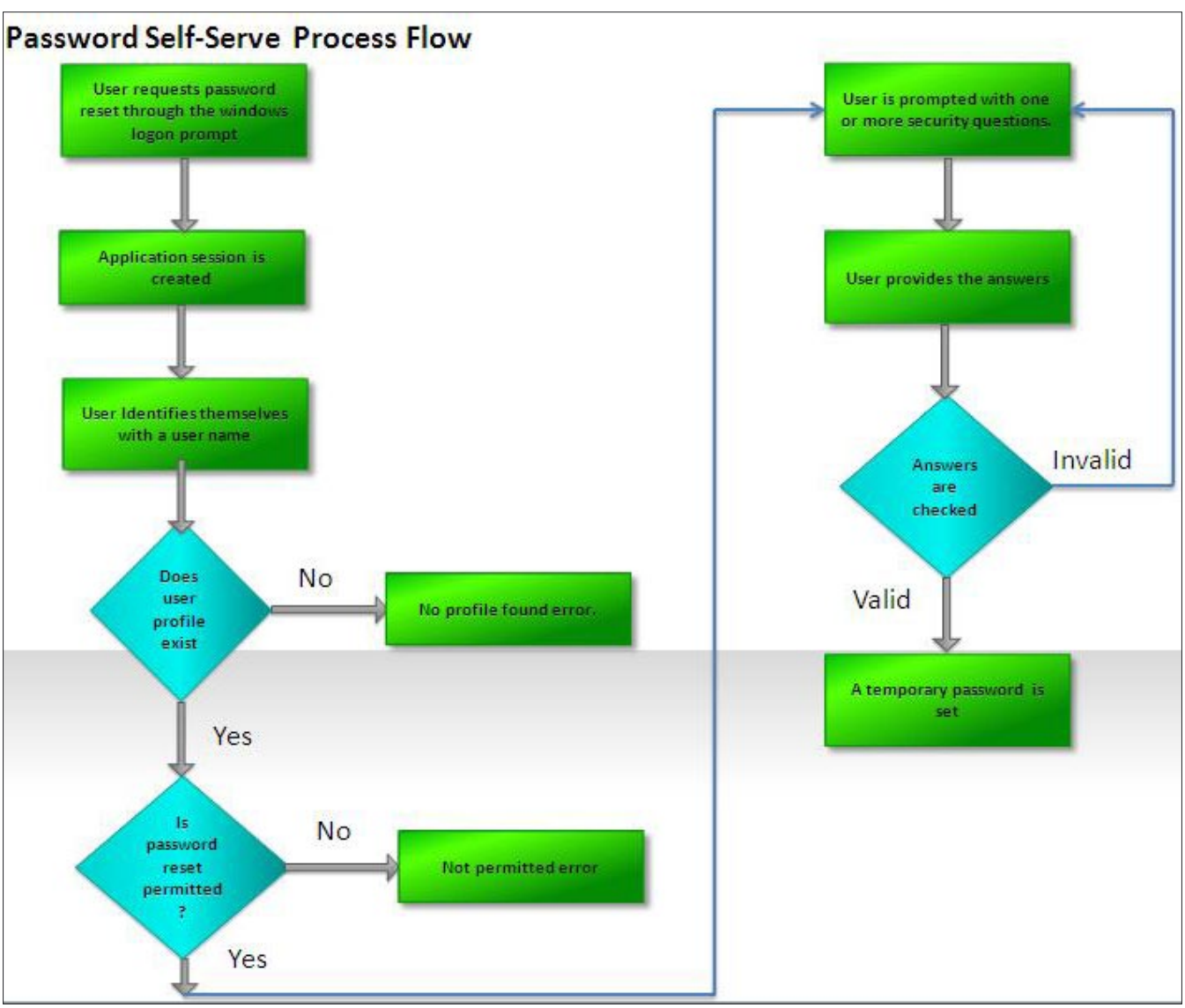


Figure 1. *Password Self-Serve Process Flow*

How does password self-serve work?
Users who need their passwords reset launch a self-serve application from an interface tied to the

> *"Password self-serve can not only reduce the helpdesk cost but also eliminate password compromise as a result of an attacker impersonating a legitimate user."*

windows logon screen. The self-service application then communicates with the password authority to request the password reset. In order to obtain a new password, the user will have to identify and authenticate them by answering one or more security questions that were enrolled in the application beforehand. Other methods of authentication, such as a hardware security key or biometrics may also be used but will result in increased cost and complexity. The following diagram explains the process flow of the password self-serve mechanism: Figure 1.

Recommendations

- Recognize that effective password construction and management is your first line of security.
- Enforce a strong password construction policy on your domain. Once such a policy is enforced, there is minimal monitoring involved. Users just cannot create a password that does not meet your minimum requirements as defined in the policy.
- Protect privileged passwords (a.k.a. 'keys to the castle') with layered security. Consider investing in privileged password management solutions.
- Consider password self-serve solutions. This will immediately reduce helpdesk costs and make employees more effective.
- Last, but not the least, awareness is the key. Modifying employees' behavior towards keeping passwords secure goes a long way.

Bottom Line
Gaining unauthorized access to data by obtaining, or guessing, passwords is an age-old and extremely effective technique; thus, an understanding of passwords, their uses, and techniques for password management is crucial.

GAURAV KUMAR

Diving Through SamuraiWTF Toolkit

The Samurai Web Testing Framework is a live Ubuntu Linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focuses on assessing and exploiting web applications.

The increase in information sharing through social networking and business adoption of the Web as a means of doing business and delivering services, today most businesses rely on web sites to deliver and server their customers, partners and stakeholders. And, websites are often attacked directly by the hackers for various reasons like gaining access to web application where they have direct access to confidential back-end data or compromise the corporate network or the end-users accessing the website etc.

As a result, this reminds industry of paying attention to web security and related threats in addition to the security of the underlying computer network and operating systems.

Defining the typical threat to web application could be, Cross-Site Scripting (XSS); SQL Injection; Brute force attacks; Dictionary attacks; Cookie replay attacks; Credential theft; Session Hijacking; Session Replay; Man in the Middle; Query string manipulation; Form field manipulation; Cookie manipulation; HTTP header manipulation etc. and many more; which typically result from flawed cod-

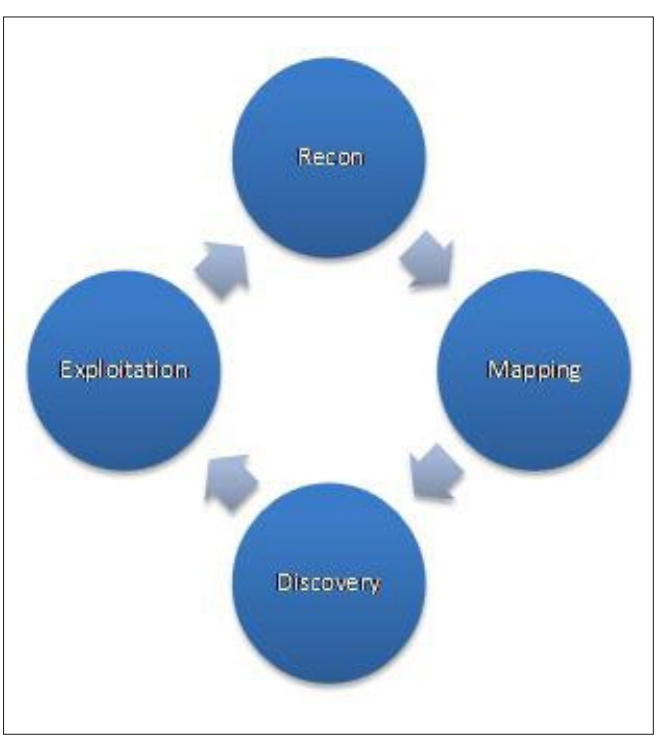


Figure 1. *Recon, Exploitation, Mapping and Discovery*

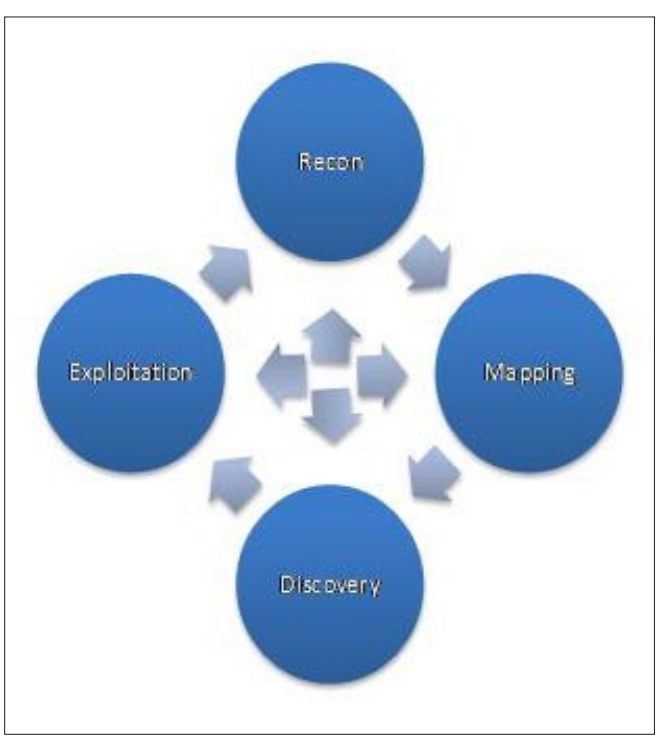


Figure 2. *Methodology in Real Life*

ing, and failure to sanitize input to and output from the web application.

Typically for setting up a web penetration testing tool in the testing environment requires appropriate selection of tool, downloading and building of the tool on desired operating system and finally configuring to use. The effort and time required in building solutions encompassing web penetration testing tools is just incomparable with what we get with SamuraiWTF..

Samurai Web Testing Framework, in short called SamuraiWTF focuses on tools most appropriate to web penetration testing required for a web penetration tester. This toolkit ships with rich number of open source pre-configured tools utilized under different stages of penetration testing. The latest release of SamuraiWTF is SamuraiWTF-2.0rc5, download available at *http://sourceforge.net/projects/samurai/files*.

Further in this article, we dive through SamuraiWTF to understand what really it contains.

Orchestration of SamuraiWTF

The point, I need to highlight in SamuraiWTF2.0, listing of penetration testing tools in a methodical manner which you would find more organized. All the listing of tools follows what suites most as standard pen testing methodology.

Figure 3. *Recon*

Figure 4. *Mapping*

SamuraiWTF 's orchestration of penetration testing tools pursues standard methodology as described here. The formal Methodology (as Figure 2):

- A simple methodology of penetration testing containing four steps like
  - Recon: Gathering information from external sources about your target. The tools listed under this method are (as Figure 3)
  - Mapping: Learning about the target app from a user's AND a developer's perspective. The tools listed under this method are (as Figure 4)
  - Discovery: Learning the app from an attacker's perspective. The tools listed under this method are (as Figure 5)

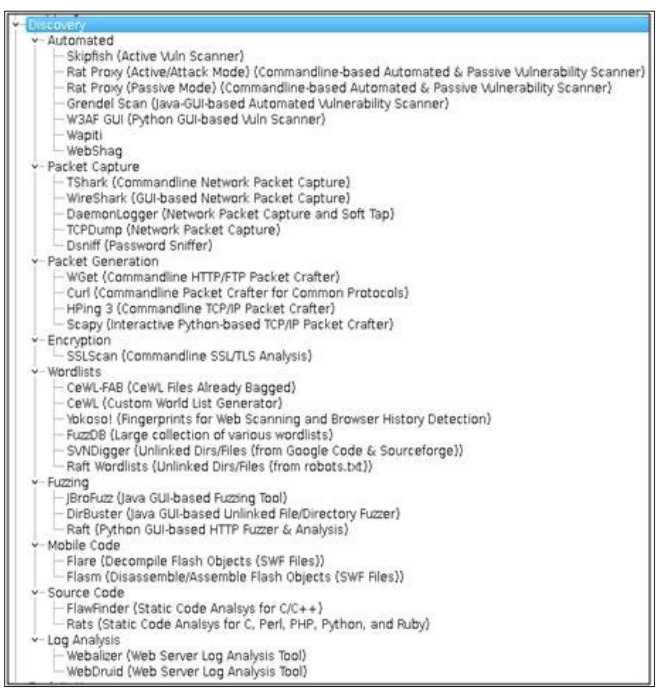


Figure 5. *Exploitation*

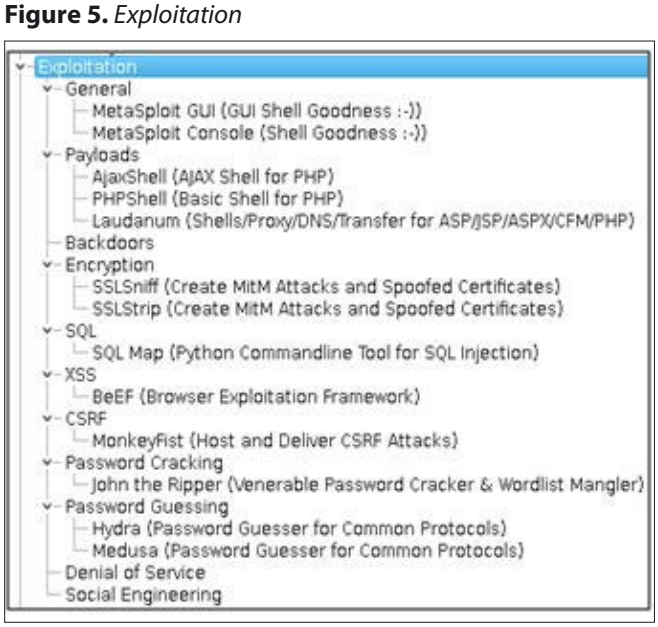


Figure 6. *The tools*

  - Exploitation: Attempting to measure the true risk of discovered vulnerabilities. The tools listed under this method are (as Figure 6)
- Also, Successful exploitation often leads to new functionality to map and a second layer of vulnerabilities to discover

But, Methodology in Real Life (as Figure 2):

- We still follow the overall clockwise flow, but we often move back and forth between processes
- Trick is to keep focused and progressing through the steps

Figure 7. *Samurain names*

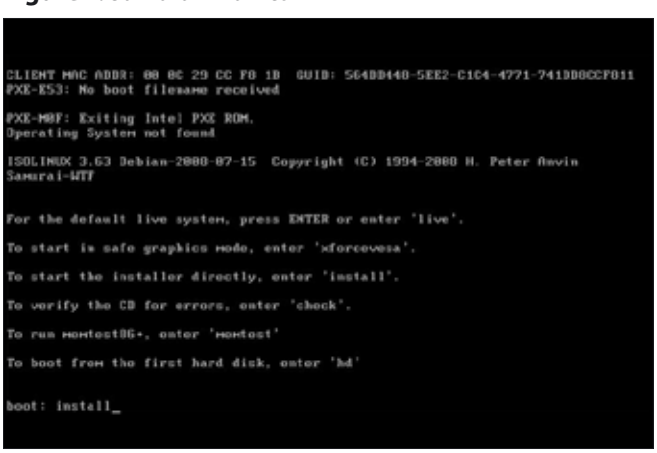


Figure 8. *Typing „install" at boot menu*

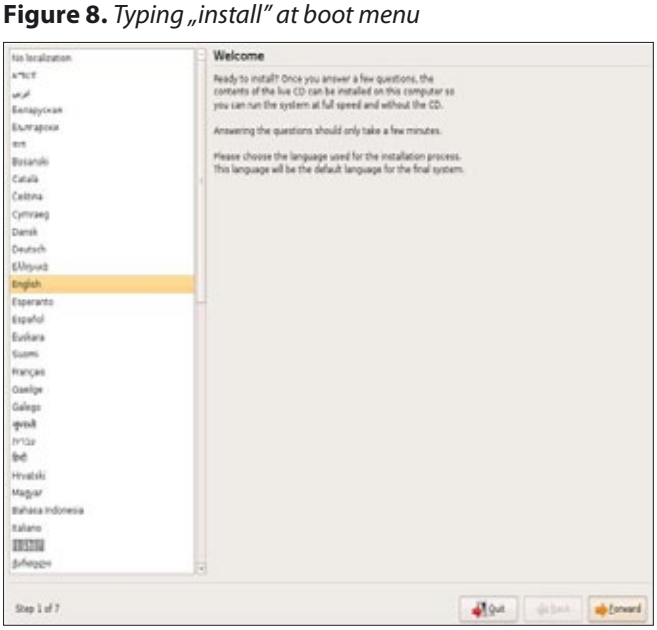


Figure 9. *Selecting your location*

Samurai WTF Installation

Installer of SamuraiWTF is available in "iso" and "Virtual Machine" file format which can be downloaded from *http://sourceforge.net/projects/samurai/files/*, latest version is SamuraiWTF2.0 branch (as Figure 7)

SamuraiWTF releases: Figure 7.

Now, we are stepping to start SamuraiWTF installation on Physical and Virtual machines.

You can use any of below described installation method based on availability and suitability of testing environment resources and/or convenient.

To login to SamuraiWTF, you can use

```
Username: samurai
Password: samurai
```

Installation 1: "iso" Image File on Physical Machine

Version: samurai-0.9.9

Download: *http://sourceforge.net/projects/samurai/files/samurai/samurai-0.9.9/samurai-0.9.9.iso/download.*

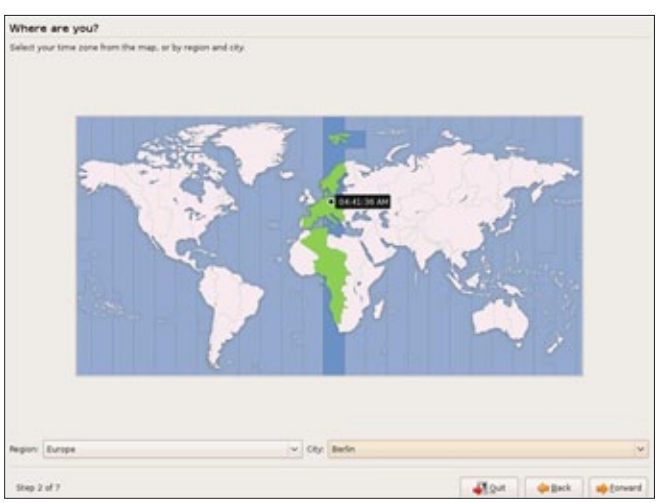


Figure 10. *Selecting your time zone*

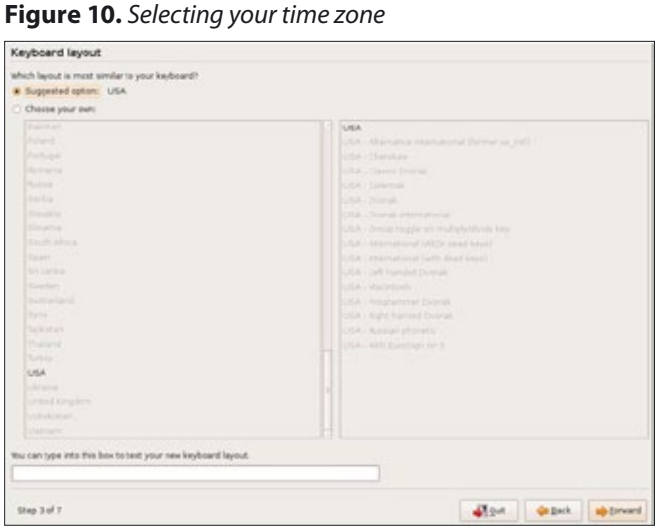


Figure 11. *Selecting your keyboard layout*

Pre-requisite: 1. Burn samurai-0.9.9.iso image file on DVD, 2. Aware of basic steps of Linux installation.

In this installation method we will be installing SamuraiWTF on physical hard disk. Now, here are the steps for installation of "iso" image on a Physical Machine.

Step 1
Power on your machine, insert samurai-0.9.9.iso bootable DVD.

Step 2
At boot prompt, type any of below option and hit enter key

- live: For default live system i.e. boot through DVD
- xforcevesa: To start in safe graphics mode
- install: To start installer directly
- check: To verify the "CD/DVD" for errors
- memtest: To run memory test
- hd: Boot from the hard disk

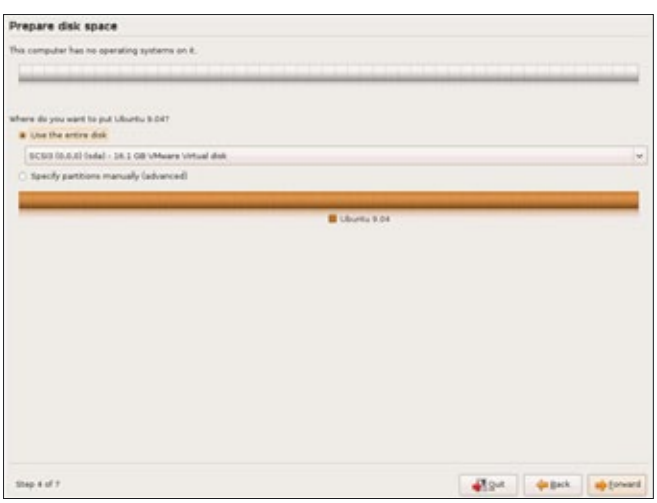


Figure 12. *Selecting whole disc for installation*

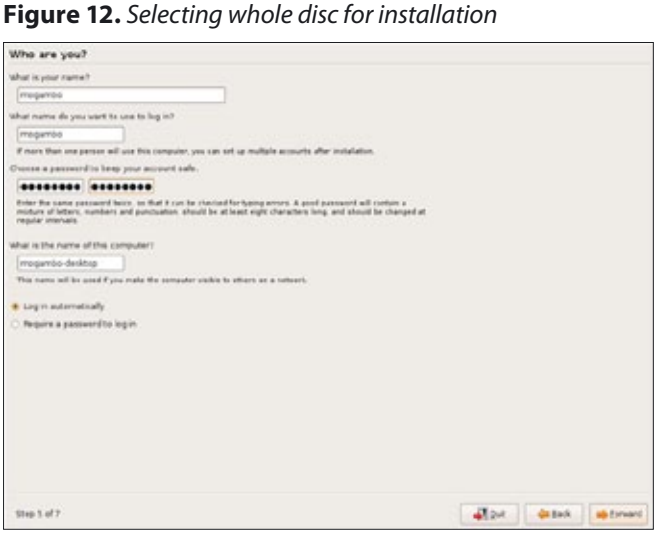


Figure 13. *Creating your user details*

Step 3
Type "install" at boot menu (as Figure 8) and pres enter key.

Step 4
Ubuntu Linux installation starts and seeks answer of few questions from you.

Step 5
Select your location (as Figure 9) and press Forward button.

Step 6
Select your time zone and press Forward button (as Figure 10).

Step 7
Select your keyboard layout and press Forward button (as Figure 11).

Step 8
Here we need to provide disk space for installation. You could also select manual partition by selecting radio button "Specify partitions manually (Advance)" but I am selecting whole disk for installation (as Figure 12) and press Forward button.

Figure 14. *Veryfying all the details*

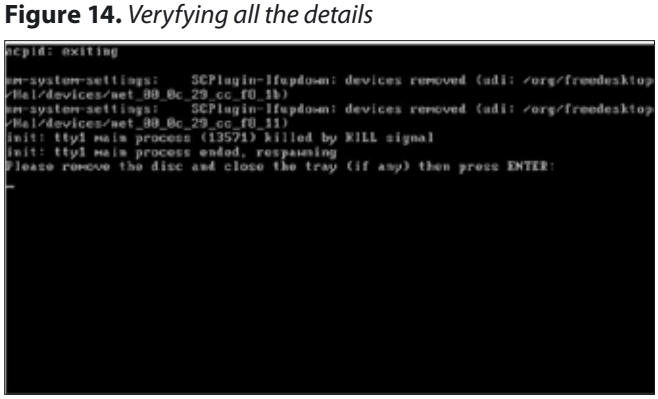


Figure 15. *Rebooting the system*

Step 9
Create your user details and select option whether you want to be authenticated while login or log-in automatically (as Figure 13) and press Forward button.

Step 10
Finally verify all the details (as Figure 14) you entered and press Install button if you wish to continue or you can abort the installation by selecting Quit button or go back to modify details if any. I selected Install.

Step 11
Wait for few minutes and you will see progress bar shows you installation status.

Step 12
After installation is completed, you are asked to remove disc (DVD) and press enter button to reboot the system (as Figure 15).

Figure 16. *Your Samurai WTF*

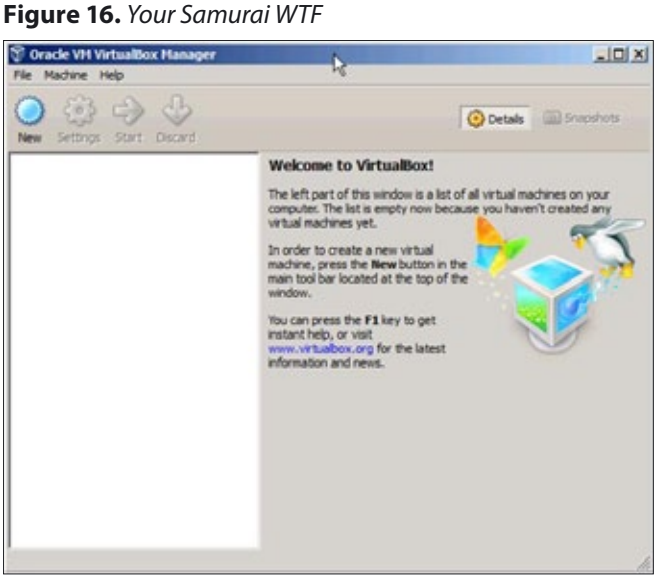


Figure 17. *Launching Oracle VM VirtualBox on Windows machine*

After reboot, here appears your SamuraiWTF (Figure 16) and you all set to rock with Samurai-WTF !!!

Installation 2:
Virtual Image File on Oracle VM VirtualBox
Version: samuraiWTF-2.0rc1
Download: *http://sourceforge.net/projects/samurai/files/SamuraiWTF%202.0%20Branch/samurai-WTF-2.0rc1.zip/download*

A Quick Overview of Oracle VM VirtualBox
VirtualBox is a cross-platform virtualization application for x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. This is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. For more details visit site: *https://www.virtualbox.org/*.

Figure 18. *Launchung „Create New Virtual Machine Wizard"*

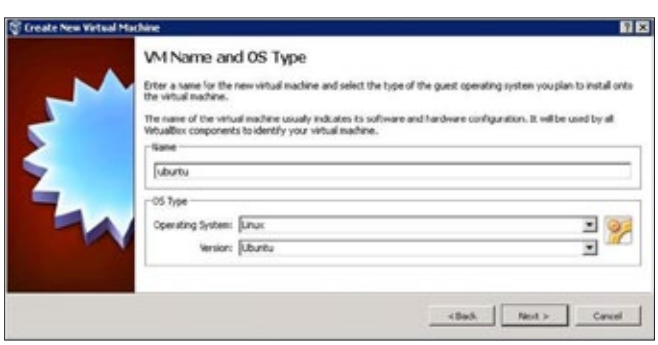


Figure 19. *Selecting the type of operating system*

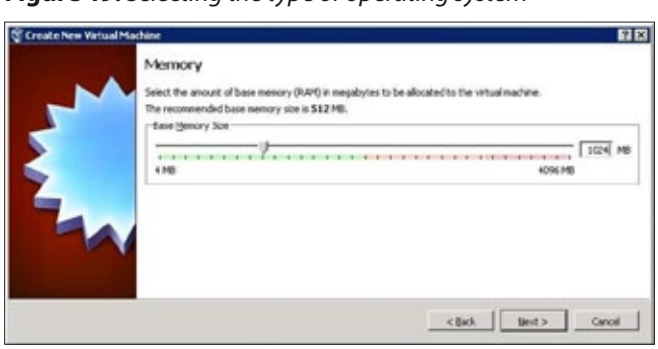


Figure 20. *Selecting Virtual Machine's memory*

To download Oracle VM VirtualBox visit site: *https://www.virtualbox.org/wiki/Downloads.*

For instance, I do have Oracle VM VirtualBox, version 4.1.2r73507 on my Windows Vista & Windows2008r2 host machines.

Pre-requisite: 1. Minimum 15GB of free disk space 2.Oracle VM VirtualBox on your host machine.

Now here are the steps for installation of SamuraiWTF's virtual image on virtual disk using "Oracle VM VirtualBox"

Step 1
Installation of Oracle VM VirtualBox on Windows machine (Windows 2008R2)

- Copy or download executable of Oracle VM VirtualBox to local hard drive
- Double click VirtualBox installer exe file and follow the installation wizard, it's as simple as any other windows installer
- Launch Oracle VM VirtualBox on Windows machine (as Figure 17)

Step 2
Copy file samuraiWTF-2.0rc1.zip on local hard drive and the extract the same.

Step 3
Launch "Create New Virtual Machine Wizard" to create new Virtual Machine by selecting New in toolbar (as Figure 18) and press Next button.

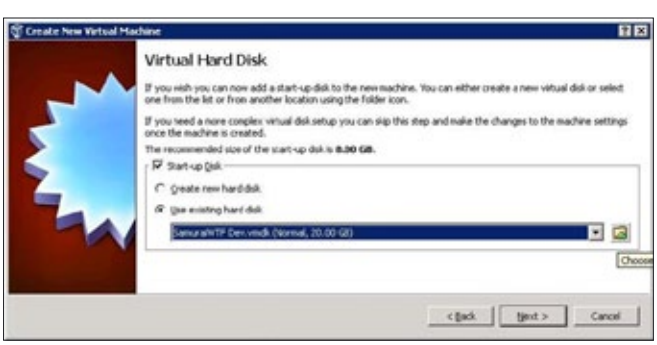


Figure 21. *Confirming*

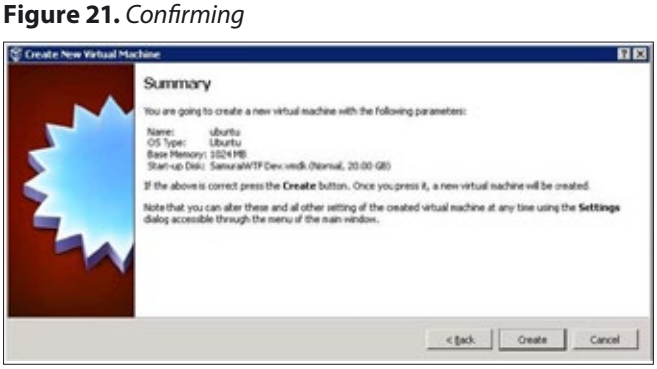


Figure 22. *Veryfying final Summary window*

Step 4
Enter below details in name field of virtual machine and select the type of operating system (as Figure 19) and press Next button.

- Name: ubuntu
- Operating System: Linux
- Version: ubuntu

Step 5
Select Virtual Machine's memory as per your requirement, I selected 1024MB (as Figure 20).

Step 6
In Virtual hard disk wizard

- Ensure "Start-up Disk" is checked
- Select option "Use existing hard disk"
- Locate and select Samurai virtual hard disk file i.e. vmdk file on your local hard drive (what is extracted in Step 2) by selecting folder icon

Finally confirm, your Virtual hard disk wizard looks like same as Figure 21 and then press Next button.

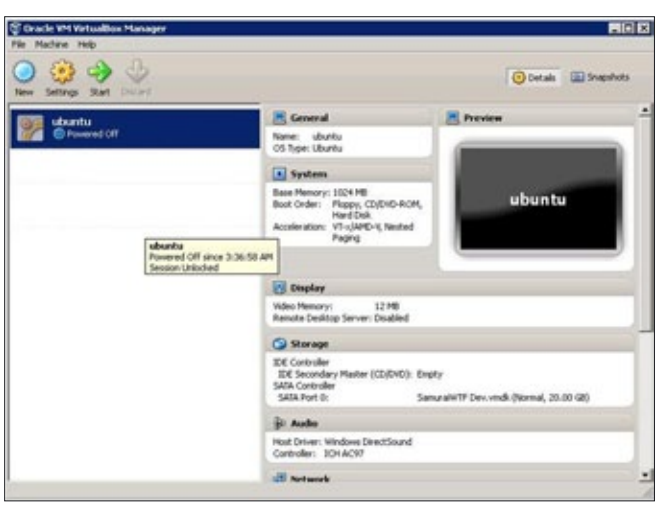


Figure 23. *Samurai successfully in „Oracle VM VirtualBox"*

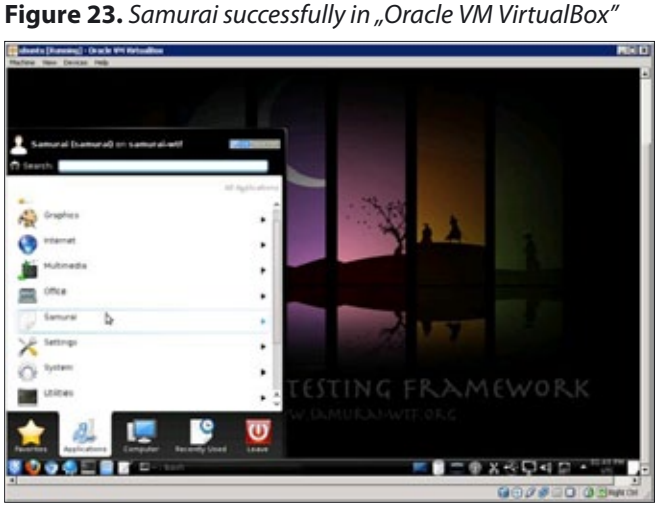


Figure 24. *Samurai WTF*

Step 7
Verify final Summary window (Figure 22) and if all correct then press Create button.

Step 8
Samurai is successfully in "Oracle VM VirtualBox" (as Figure 23).

Now, select start button (green colored arrow) in toolbar in Figure 23 and here appears your SamuraiWTF (Figure 24) and you all set to rock with SamuraiWTF !!!

Installation 3: "iso" Image File on Virtual Machine

Version: samurai-0.9.9
Download: *http://sourceforge.net/projects/samurai/files/samurai/samurai-0.9.9/samurai-0.9.9.iso/download*
Pre-requisite: 1. copy samurai-0.9.9.iso image file on your hard-disk, 2. VMware Player, Workstation, or Fusion

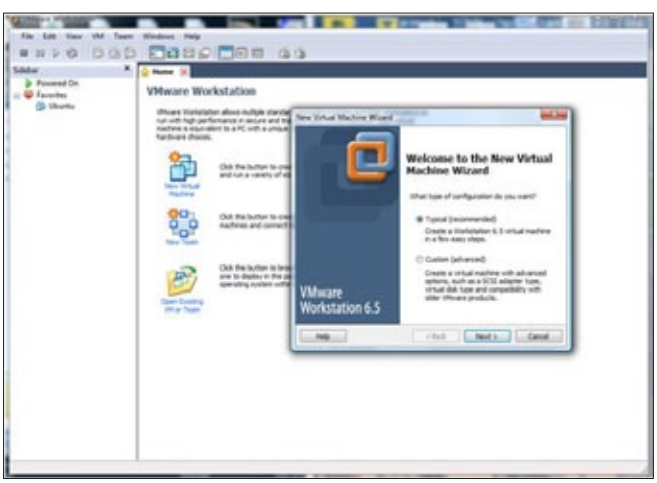


Figure 25. *Selecting radio button*

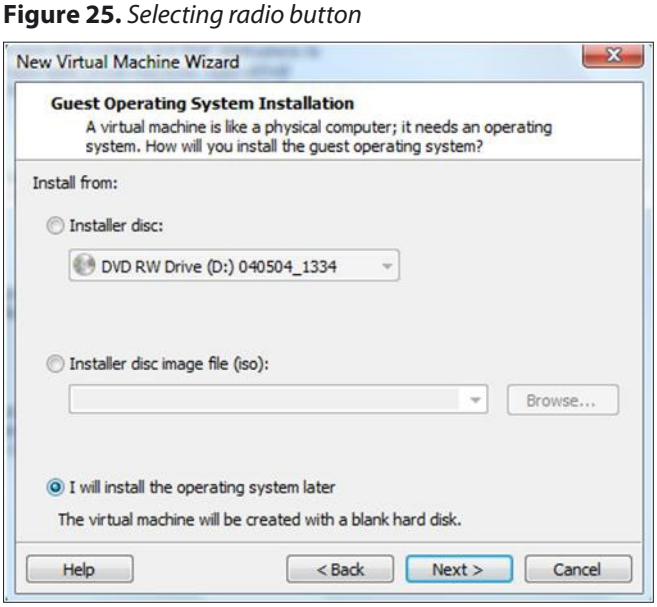


Figure 26. *Selecting Guest Operating System Installation*

In this installation method we will be setting up SamuraiWTF on Virtual Machine without disk. This is quick way to get started with SamuraiWTF if don't want "iso" file to be installed. Now, here are the steps to follow for booting SamuraiWTF iso file through VMware Player, Workstation, or Fusion. The example presented here was performed on VMware Workstation 6.5.

Step 1
Launch VMware workstation and select New Virtual Machine, would launch New Virtual Machine Wizard. Select radio button "Typical (recommended)" (as Figure 25) and press Next button.

Step 2
In "Select Guest Operating System Installation" window select radio button "I will install operating

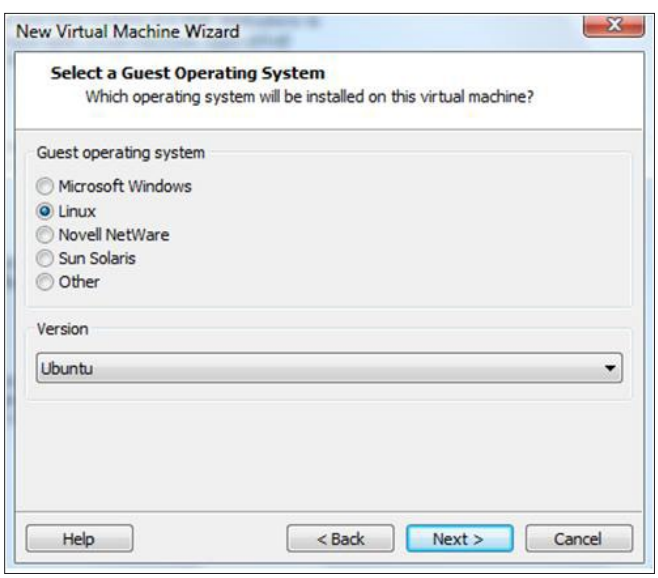


Figure 27. *Selecting radio button Linux as guest operating system and version as Ubuntu*

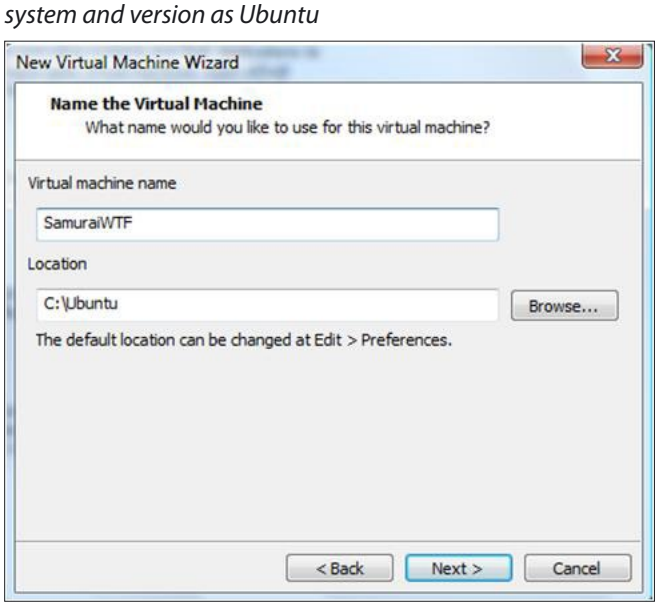


Figure 28. *Entering VM name and location*

system later" as (as Figure 26) and press Next button.

Step 3
In "Select Guest Operating System window", select radio button Linux as guest operating system and version as Ubuntu (as Figure 27) and press Next button.

Step4
Enter VM name and location to store files in Name the Virtual Machine window (as Figure 28) and press Next button.

Step 5
Select disk capacity in Specify Disk Capacity window (as Figure 29) and press Next button.

Step 6
Finally, verify the summary window (as Figure 30) and press Finish button to complete virtual machine creation. Also, you could check option "Power on this virtual machine after creation" if you want Virtual Machine to be powered on automatically after pressing Finish button.

Step7
Next, edit virtual machine settings and supply SamuraiWTF's "iso" image file location in CD/DVD device option (as Figure 31).

Now, power on the virtual machine and here appears your SamuraiWTF (Figure 32) and you all set to rock with SamuraiWTF !!!

Explaining Targets

>Applications>Samurai>Targets.

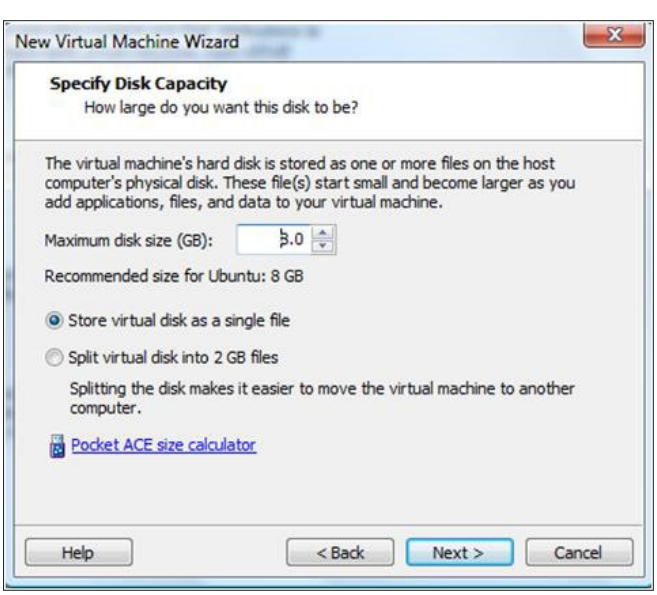


Figure 29. *Selecting Disc Capacity window*

The Samurai's preinstalled targets are vulnerable web applications; a web security professional would require testing their skills and tools in a legal environment. Assaulting these targets using SamuraiWTF's preinstalled penetration testing tools, a security professional understands various web security threats. Also, becomes expert on how to discover and exploit the vulnerability in a web application.

From the list of available targets (as Figure 33), few targets are only available on SamuraiWTF but remaining publically available.

The idea here is to know about these pre-configured SamuraiWTF's targets and its notable features where penetration testers can carry out various pen tests to improve their knowledge on

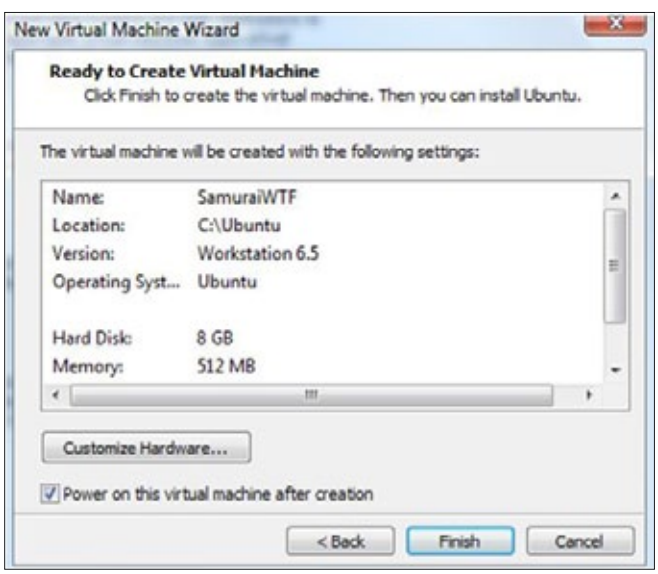


Figure 30. *Veryfying the summary window*

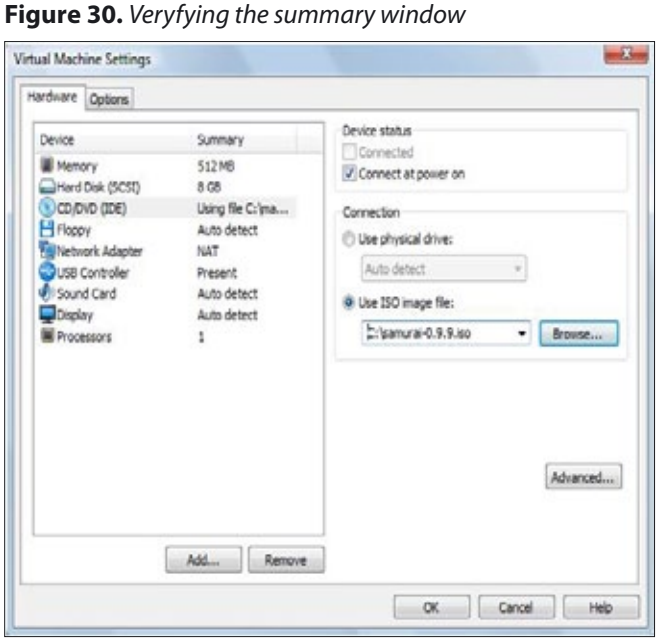


Figure 31. *Edit virtual machine settings and supplying SamuraiWTF's "iso" image file location in CD/DVD device option*

vulnerabilities and exploitation.

In Samuai WTF Virtual Machine go to: >Damn Vulnerable Web App (DVWA) (PHP-based with Multiple Security Levels and PHPIDS).

Clicking here or manually entering URL http://dvwa or https://dvwa in Samurai's Firefox browser would launch DVWA application (as Figure 34).

Introduction

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

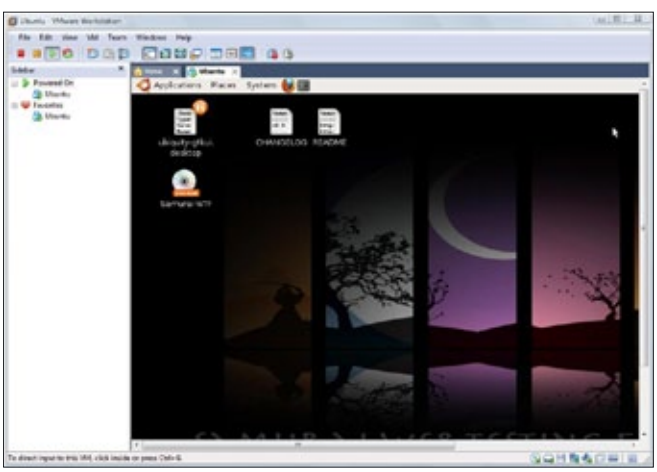


Figure 32. *Powering on the virtual machine*

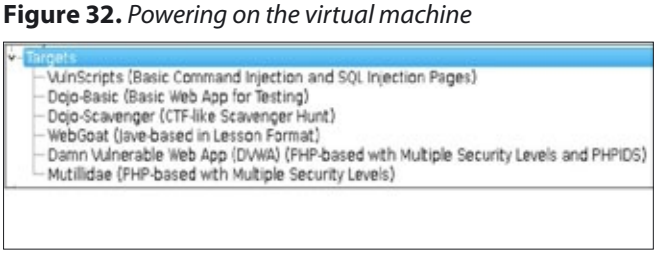


Figure 33. *list of available targets*

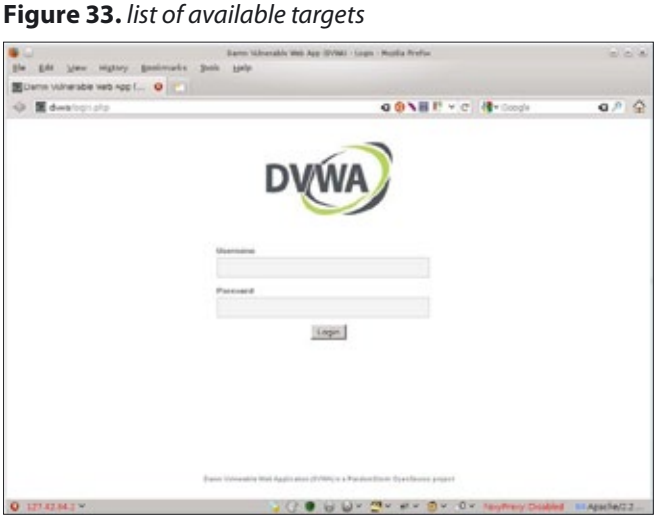


Figure 34. *launching DVWA application*

Login DVWA

```
User: admin
Password: password
```

Hitting Login button will show up DVWA home page (as Figure 35). Now, your DVWA target is all set.

Important Features

- Login Brute Force
  (mainly used for guessing passwords and bypassing access control)
- Command Execution
  (mainly used to execute command remotely)
- SQL Injection
  (mainly used for attacking database using website)
- XSS Stored(Persistent)/Reflected

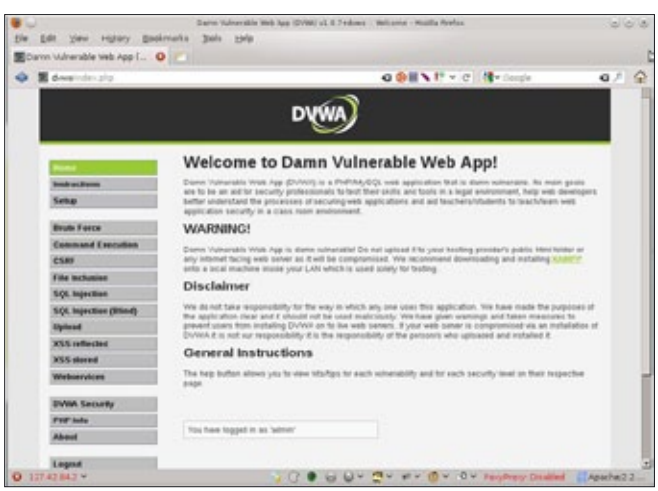


Figure 35. *Hitting Login button will show up DVWA home page*

Figure 36. *Choose a vulnerability page*

(or Non-Persistent) (mainly used by attackers to inject client side script into Web pages viewed by other users)
- CSRF
  (transmission of unauthorized commands from a user that the website trusts)
- PHP-IDS
  (finding intrusion data coming from client to php web application)

And lot more…

WebSite
http://sourceforge.net/projects/dvwa.

>Dojo-Basic (PHP-based with Multiple Security Levels and PHPIDS).

Clicking here or manually entering URL *http://dojo-basic* in Samurai's Firefox browser would launch Dojo-Basic application (as Figure 36).

Introduction
The Samurai Dojo-Basic application implements the OWASP Top 10 vulnerabilities in PHP/MySQL, and does it in such a way that it is easy to demonstrate common attacks. The primary goal of this project is to understand how vulnerability works.

You can go to OWASP Top 10 website (*https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*) to read about the vulnerability, then choose a vulnerability page from the "Vuln List" link in the "Pentester Help" menu on the left (in Figure 36). Finally, try to discover and exploit the vulnerability.

When you exploit the vulnerability which is you think you found a bug in this application, that's the feature.

Figure 37. *Clicking "Register" link in "Core Controls" menuon left pane of webpage*

Login Dojo-Basic
You have to register, See the Steps!!!

```
User:
Password:
```

Step 1
Launching Registration page

- Click "Register" link in "Core Controls" menu on left pane of webpage (Figure 36)
- It shows up registration page (as Figure 37)

Step2: Create Login Account
Enter login details like username, password & signature and submit the details. You receive confirmation message "Account Made" for successful user registration.

For example, created user (as Figure 38)

```
Username: mogamboo
Password: HappyMogamboo
Signature: Mogambo kush hua!!!
```

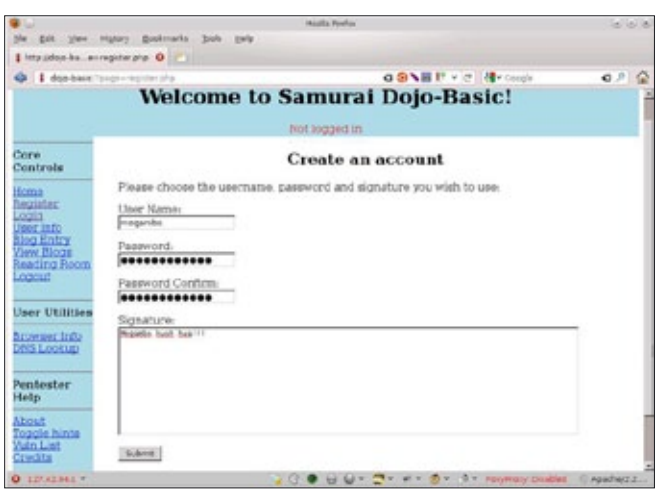


Figure 38. *Showing up registration page*

Figure 39. *Logging*

Step3: Login with User Credentials
Click “Login” link in “Core Controls” menu on left pane of webpage and enter login credentials. You have logged in NOW!!! (as Figure 39).

Important Features

- Mapped to OWASP Top 10, 2010
- Very simple web app designed for beginner and intermediate level web pentesters

WebSite
No website as currently only available on SamuraiWTF.

>Mutillidae (PHP-based with Multiple Security Levels).

Clicking here or manually entering URL http://mutillidae in Samurai’s Firefox browser would launch Mutillidae application (as Figure 40)

Introduction
Mutillidae is a free, open source web application provided to allow security enthusiast to pen-test and hack a web application. It contains dozens of vulnerabilities and hints to help the user exploit them; providing an easy-to-use web hacking environment deliberately designed to be used as a hack-lab for security enthusiast, classroom labs, and vulnerability assessment tool targets.

Mutillidae has been used in graduate security courses, in corporate web sec training courses, and as an "assess the assessor" target for vulnerability software.

Login Mutillidae
You have to register, See the Steps!!!

```
User:
Password:
```

Step1: Launching Registration page

- Click “Login/Register” link in top menu of webpage
- Again click on link “Don’t have an account? Please register here”, would show up registration page (as Figure 41)

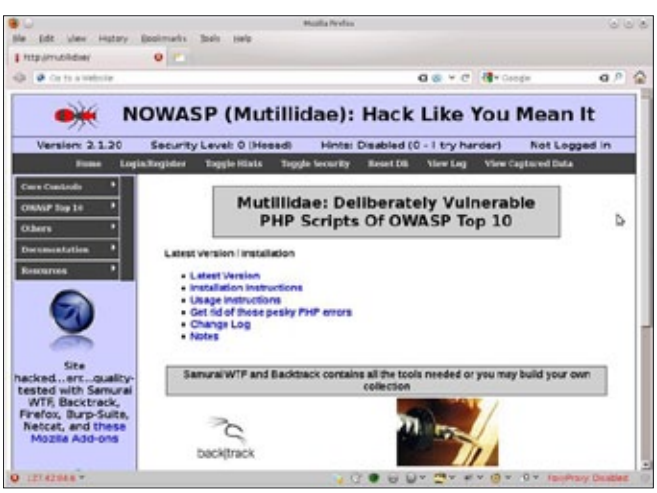


Figure 40. *Launching Mutillidae application*

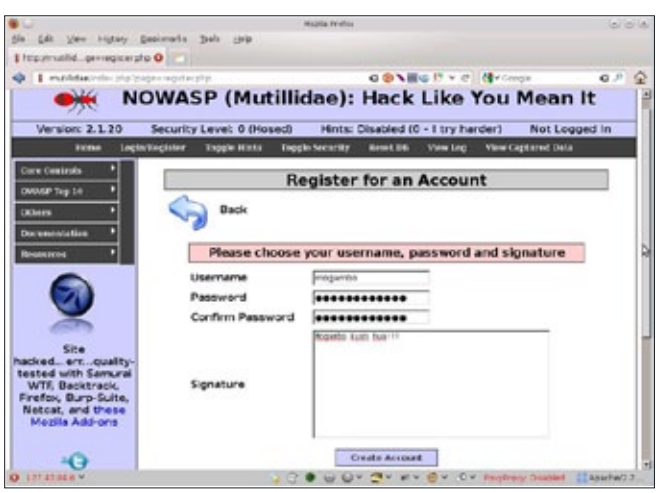


Figure 42. *Creating an account*

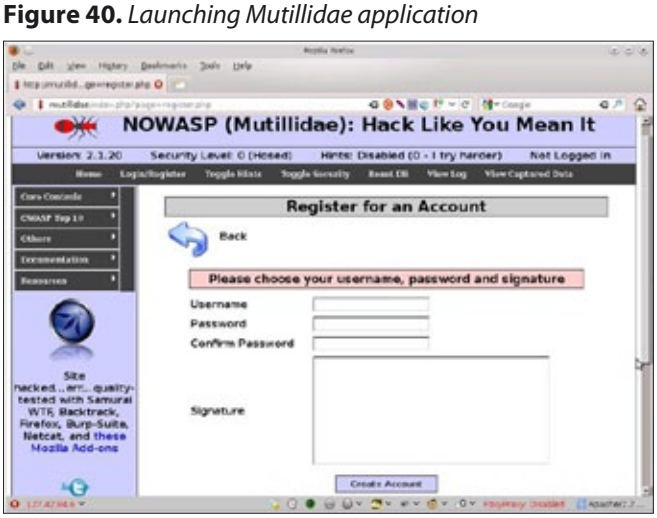


Figure 41. *Registration page*

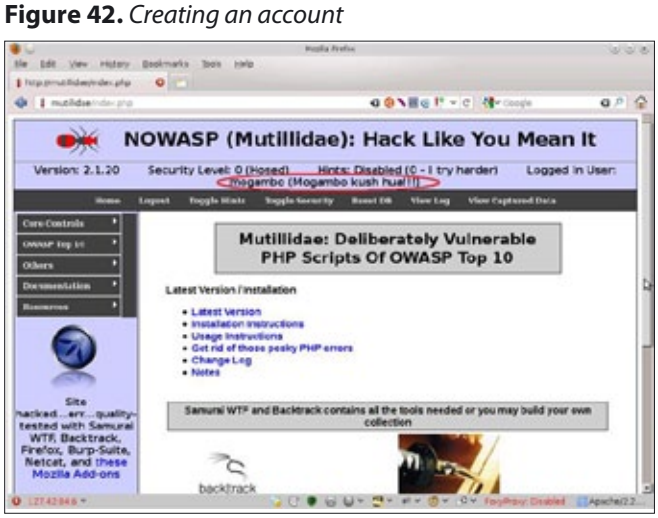


Figure 43. *User “mogambo” logged in successfully*

Step2: Create Login Account
Enter login details like username, password & signature in webpage and create an account.
For example, created user (as Figure 42)

```
Username: mogamboo
Password: HappyMogamboo
Signature: Mogambo kush hua!!!
```

You receive confirmation message

Account created for mogambo. 1 rows inserted.

on web page.

Step3: Login with User Credentials
Click Click "Login/Register" link in top menu of webpage and enter login credentials. You have logged in NOW!!!(as Figure 43). Red color circled in Figure 43 shows user "mogambo" logged in successfully.

Important Features

- Contains all of the vulnerabilities from the OWASP Top 10
- cross-site scripting
- sql, html, javascript injection
- response-splitting
- clickjacking
- forms-caching

And, lot more…

WebSite
http://www.irongeek.com/i.php?page=mutillidae/mutillidae-deliberately-vulnerable-php-owasp-top-10.

>WebGoat (Java-based in Lesson Format)
Clicking here or manually entering URL http://webgoat or *http://webgoat:8080/webgoat/attack* in Samurai's Firefox browser would launch WebGoat application (as Figure 44) and seek authentication

Introduction
WebGoat is a deliberately insecure J2EE web application maintained by OWASP (*Open Web Application Security Project*) designed to teach web application security lessons. The primary goal of the WebGoat project is to create an interactive teaching environment for web application security.

Login WebGoat

```
User: guest
Password: guest
```

Enter login details and press Ok button in WebGoat authentication window, would show up WebGoat home page (as Figure 45). You are all set to start web goat application by clicking "Start WebGoat" command button.

Important Features
A lesson based approach with currently over 30 lessons, including those dealing with the following issues:

- Cross-site Scripting (XSS)
- Access Control
- Thread Safety
- Hidden Form Field Manipulation
- Parameter Manipulation
- Weak Session Cookies
- Blind/Numeric/String SQL Injection
- Web Services

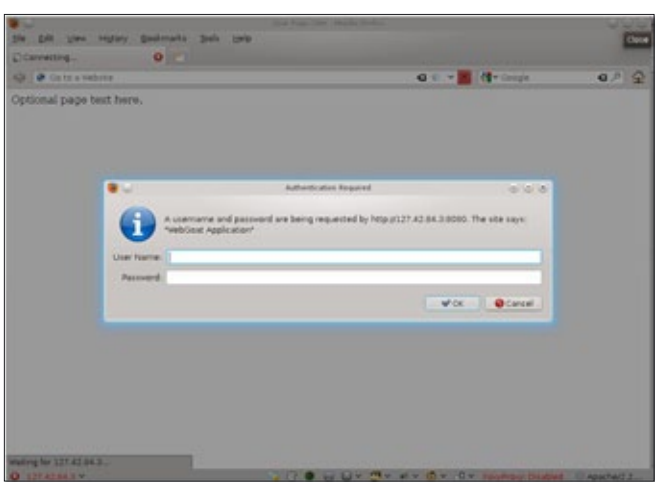


Figure 44. *WebGoat application*

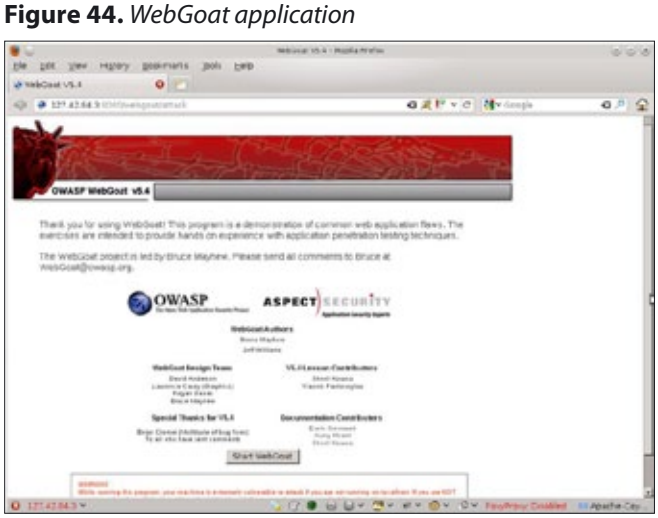


Figure 45. *Web-Goat home page*

- Fail Open Authentication
- Dangers of HTML Comments

And, lot more…

WebSite
https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project.

SamuraiWTF Arsenal

There are over 100 tools, extensions and scripts are bundled within SamuraiWTF. It would require comprehensive effort to explain all of these tools, extension and scripts. This article focuses on some of the web penetration testing tools methodically categorized under recon, mapping, discovery and exploitation.

All the examples, screenshots shown in this article here onwards are performed on "samurai-WTF-2.0rc1" virtual image on Oracle VM Virtual Box.

Nikto
(>Applications>Samurai>Mapping>Finger Printing) (Clicking here launches Nikto as Figure 46)

Nikto is an Open Source (GPL) web server scanner tool which tests web servers for dangerous files/CGIs, outdated server software and other problems. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Essentially, it is a web server assessment tool which is designed to find various default and insecure files, configurations and programs on any type of web server.

How Nikto works?
Nikto is command line based web scanner. Running command "nikto –h" shows all the options present (as Figure 47) where most of options are self explained. Some of Nikto options are:

-Display
Control the output that Nikto shows. Use the reference number or letter to specify the type.

Multiple may be used. By default only some basic information about the target and vulnerabilities is shown. Using the *-Display* parameter can produce more information for debugging issues.

- 1 – Show redirects. This will display all requests which elicit a "redirect" response from the server.
- 2 – Show cookies received. This will display all cookies that were sent by the remote host.
- 3 – Show all 200/OK responses. This will show all responses which elicit an "okay" (200) response from the server. This could be useful for debugging.

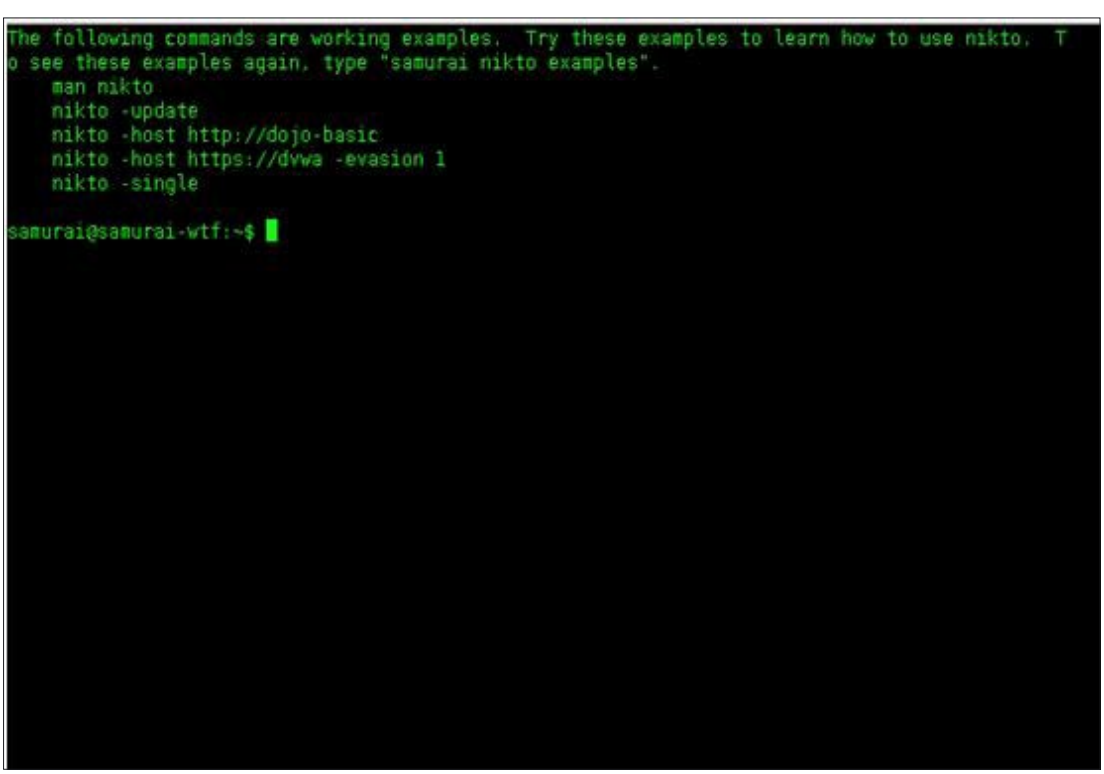


Figure 46. *Launching Nikto*

- 4 – Show URLs which require authentication. This will show all responses which elicit an "authorization required" header.
- D – Debug Output. Show debug output, which shows the verbose output and extra information such as variable content.
- E – Display all HTTP errors. Show details for any HTTP error encountered.
- P – Print progress to STDOUT. Show status report to STDOUT during testing (interval set in nikto.conf).
- V – Verbose Output. Show verbose output, which typically shows where Nikto is during program execution.
- E – Error Output. Display all HTTP and communications errors, which show a lot of output on some servers.

-Format
Save the output file specified with -o (-output) option in this format. If not specified, the default will be taken from the file extension specified in the -output option. Valid formats are:

- csv – a comma-seperated list
- htm – an HTML report
- msf – log to Metasploit
- txt – a text report
- xml – an XML report

-id
ID and password to use for host Basic host authentication. Format is "id:password".

-mutate
A mutation will cause Nikto to combine tests or attempt to guess values. These techniques may cause a tremendous amount of tests to be launched against the target. Use the reference number to specify the type, multiple may be combined.

- Test all files with all root directories. This takes each test and splits it into a list of files and directories. A scan list is then created by combining each file with each directory.
- Guess for password file names. Takes a list of common password file names (such as "passwd", "pass", "password") and file extensions ("txt", "pwd", "bak", etc.) and builds a list of files to check for.
- Enumerate user names via Apache (/~user type requests). Exploit a misconfiguration with Apache UserDir setups which allows valid user names to be discovered. This will attempt to brute-force guess user names. A file of known users can also be supplied by supplying the file name in the -mutate-options parameter.
- Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests). Exploit a flaw

```
Option host requires an argument

       -config+            Use this config file
       -Cgidirs+           scan these CGI dirs: 'none', 'all', or values like "/cgi/ /cgi-a/"
       -dbcheck            check database and other key files for syntax errors
       -Display+           Turn on/off display outputs
       -evasion+           ids evasion technique
       -Format+            save file (-o) format
       -host+              target host
       -Help               Extended help information
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -mutate+            Guess additional file names
       -mutate-options+    Provide extra information for mutations
       -output+            Write output to this file
       -nocache            Disables the URI cache
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -port+              Port to use (default 80)
       -Plugins+           List of plugins to run (default: ALL)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Single             Single request mode
       -timeout+           Timeout (default 2 seconds)
       -Tuning+            Scan tuning
       -update             Update databases and plugins from CIRT.net
       -vhost+             Virtual host (for Host header)
       -Version            Print plugin and database versions
               + requires a value

       Note: This is the short help output. Use -H for full help.

   samurai@samurai-wtf:~$
```

Figure 47. *All the options present*

in cgiwrap which allows valid user names to be discovered. This will attempt to brute-force guess user names. A file of known users can also be supplied by supplying the file name in the *-mutate-options* parameter.
- Attempt to brute force sub-domain names. This will attempt to brute force know domain names, it will assume the given host (without a www) is the parent domain.
- Attempt to brute directory names. This is the only mutate option that requires a file to be passed in the *-mutate-options* parameter. It will use the given file to attempt to guess directory names. Lists of common directories may be found in the OWASP DirBuster project (*https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project*)

-mutate-options
Provide extra information for mutates, e.g. a dictionary file.

-output
Write output to the file specified. The format used will be taken from the file extension. This can be over-ridden by using the -Format option.

For '-Format msf' the output option takes special meaning. It should contain the password and location of the Metasploit RPC service. For example, it may look like: `-o msf:<password>@http://localhost:55553/RPC2`.

-Single
Perform a single request to a target server. Nikto will prompt for all options which can be specified, and then report the detailed output. Single request mode is designed to perform a solitary request against the target. This is useful to confirm a test result using the same resources Nikto used during a scan. The single option allows manual setting of most variables used by Nikto and LibWhisker, and upon completion will display both the request and the result of the operation.

-Tuning
Tuning options will control the test that Nikto will use against a target. By default, all tests are performed. If any options are specified, only those tests will be performed. If the "x" option is used, it will reverse the logic and exclude only those tests. Use the reference number or letter to specify the type, multiple may be used:

- 0 – File Upload
- 1 – Interesting File / Seen in logs
- 2 – Misconfiguration / Default File
- 3 – Information Disclosure
- 4 – Injection (XSS/Script/HTML)
- 5 – Remote File Retrieval – Inside Web Root
- 6 – Denial of Service
- 7 – Remote File Retrieval – Server Wide
- 8 – Command Execution / Remote Shell
- 9 – SQL Injection
- a – Authentication Bypass
- b – Software Identification
- c – Remote Source Inclusion
- x – Reverse Tuning Options (i.e., include all except specified)

The given string will be parsed from left to right, any x characters will apply to all characters to the right of the character.

Basic Testing using Nikto
The most basic Nikto scan requires simply a host to target, since port 80 is assumed if none is specified. The host can either be an IP or a hostname of a machine, and is specified using the *-h* (*-host*) option. This will scan the IP 192.168.0.1 on TCP port 80:

```
samurai@samurai-wtf:~$ nikto -h 192.168.0.1
```

To check on a different port, specify the port number with the *-p* (*-port*) option. This will scan the IP 192.168.0.1 on TCP port 443:

```
samurai@samurai-wtf:~$ nikto -h 192.168.0.1 -p 443
```

Hosts, ports and protocols may also be specified by using a full URL syntax, and it will be scanned:

```
samurai@samurai-wtf:~$ nikto -h
                  https://192.168.0.1:443/
```

There is no need to specify that port 443 may be SSL, as Nikto will first test regular HTTP and if that fails, HTTPS. If you are sure it is an SSL server, specifying *-s* (*-ssl*) will speed up the test.

```
samurai@samurai-wtf:~$ nikto -h 192.168.0.1 -p 443
                  -ssl
```

More complex tests can be performed using the *-mutate* parameter. This can produce extra tests, some of which may be provided with extra parameters through the *-mutate-options* parameter. For example, using *-mutate* 3, with or without a file at-

tempts to brute force usernames if the web server allows ~user URIs:

```
samurai@samurai-wtf:~$ nikto -h 192.168.0.1
-mutate 3 -mutate-options user-list.txt
```

Multiple Port Testing using Nikto

Nikto can scan multiple ports in the same scanning session. To test more than one port on the same host, specify the list of ports in the *-p* (*-port*) option. Ports can be specified as a range (i.e., 80-90), or as a comma-delimited list, (i.e., 80,88,90). This will scan the host on ports 80, 88 and 443.

```
samurai@samurai-wtf:~$ nikto -h 192.168.0.1 -p
                  80,88,443
```

Nikto behind a Proxy

If the machine running Nikto only has access to the target host (or update server) via an HTTP proxy, the test can still be performed. There are two ways to use a proxy with Nikto, via the nikto.conf file or directly on the command line.

To use the nikto.conf file, set the PROXY* variables, and then execute Nikto with the -useproxy option. All connections will be relayed through the HTTP proxy specified in the configuration file.

```
samurai@samurai-wtf:~$ nikto -h localhost -p 80
                  -useproxy
```

To set the proxy on the command line, use the -useproxy option with the proxy set as the argument, for example:

```
samurai@samurai-wtf:~$ nikto -h localhost
                  -useproxy http://localhost:8080/
```

Updating Nikto

Nikto can be automatically updated, assuming you have Internet connectivity from the host Nikto is installed on. To update to the latest plugins and databases, simply run Nikto with the -update command.

```
samurai@samurai-wtf:~$ nikto -update
```

If updates are required, you will see a list of the files downloaded:

```
samurai@samurai-wtf:~$ nikto -update
+ Retrieving 'nikto_core.plugin'
+ Retrieving 'CHANGES.txt'
```

Updates may also be manually downloaded from *http://www.cirt.net/.*

Integration Nikto with Nessus

Nessus (*http://www.nessus.org/nessus/*) can be configured to automatically launch Nikto when it finds a web server. Ensure Nikto works properly, that *nikto.pl* is in the PATH, and that nikto.nasl is present in the Nessus install. Run 'nessusd -R' and then restart nessusd.

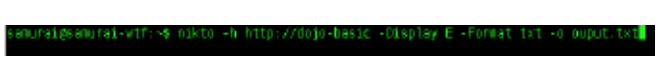
See *http://blog.tenablesecurity.com/2008/09/using-nessus-to.html* for detailed instructions.

Web server assessment using Nikto

The idea here is to find all http errors in target web application and store the output in txt file format. To do so, follow steps.

Step 1

Type nikto command to scan target http://dojo-basic



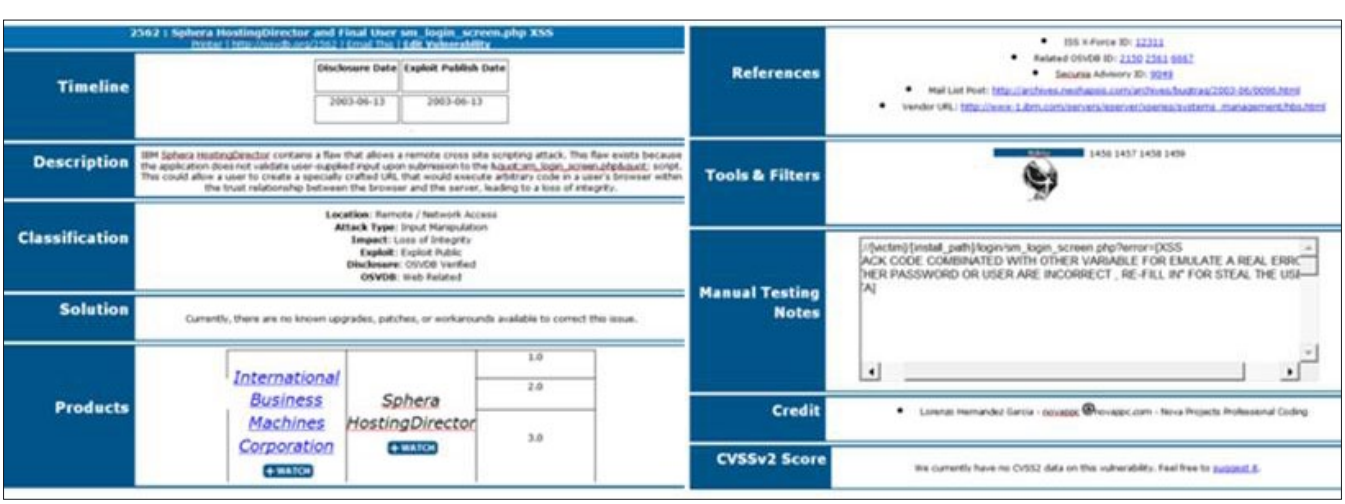


Figure 48. *Errors in the target web application*

Step 2

The output of the command shows many errors in the target web application (as Figure 48).

You could see many OSVDB (Open Source Vulnerability Database) errors are reported in this execution. For OSVDB errors, you could further take reference from website *http://osvdb.org/.*

For example:

Analyzing, one of OSVDB error of Nikto-Picture-03, the error OSVDB-2562 reports as “vulnerable to Cross Site Scripting (XSS)”. Figure 49 shows complete details, impact and available solution of this reported error OSVDB-256. This information could be fetched by making quick search on OSBDB ID on home page on website *http://osvdb.org/.*

For a penetration tester this information helps to necessary steps and make appropriate decision on security posture of the hosted web application.

Summary

Here, we have successfully used Nikto to launch web scan on a web site which reported many OSVDB (Open Source Vulnerability Database) errors like XSS and other error as well.

Not every error is a security problem, though most are. Sometimes, there are some items that are "info only" type errors that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server.

Nikto helps penetration tester to perform comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers.

Burp Suite Free

(>Applications>Samurai>Mapping>Interception) (Clicking here launches Burp Suite Free as Figure 49)

Burp Suite is an integrated platform for attacking web applications. It contains a variety of tools with numerous interfaces between them designed to facilitate and speed up the process of attacking an application.

A commercial version also exists which adds an automated vulnerability scanner and extended attack tool.

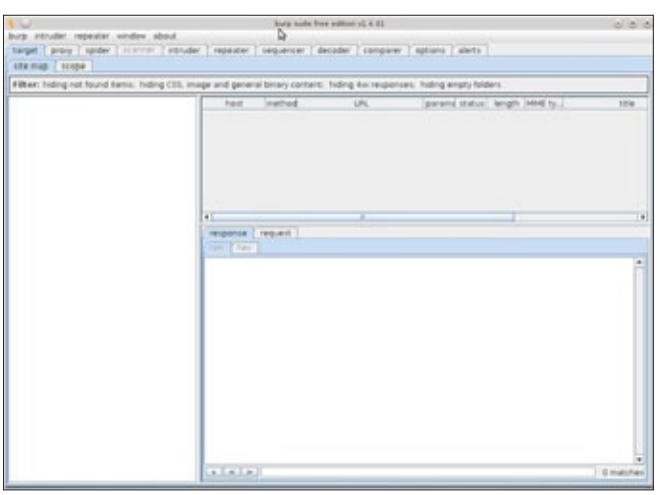


Figure 49. *launching Burp Suite Free*

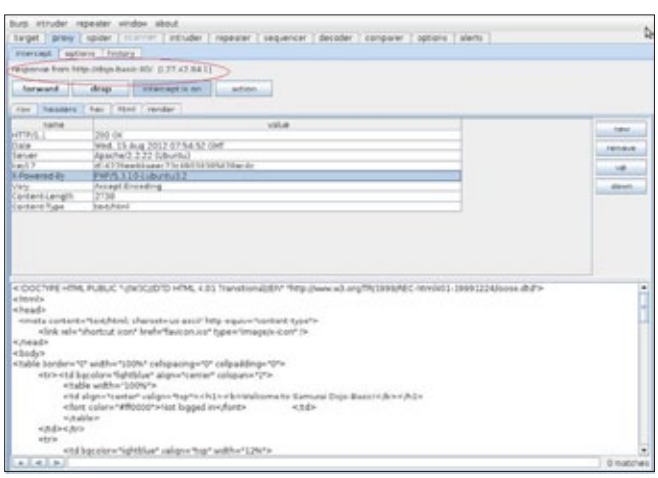


Figure 51. *Launching http://dojo-basic web site which got intercepted*

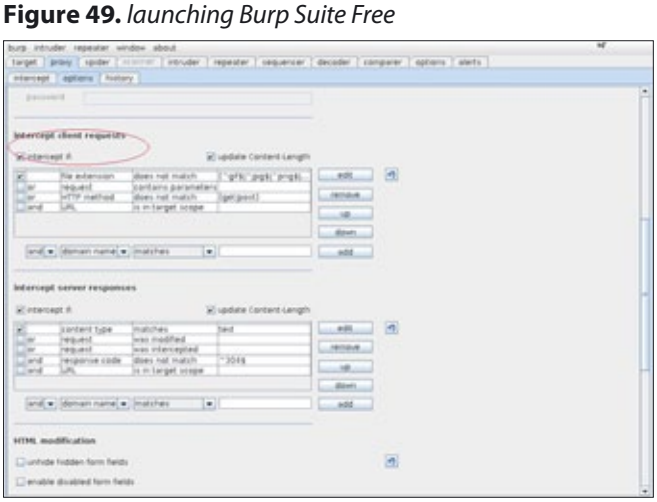


Figure 50. *Enabling the check box next to „intercept if*

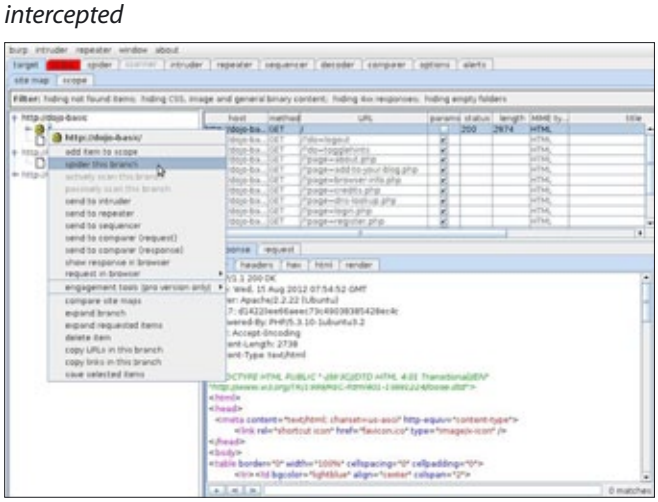


Figure 52. *Choosing the „spider this host/branch”*

Burp Suite Free contains the following key components:

Burp Proxy
An intercepting HTTP/S proxy server which operates as a man-in-the-middle between the end browser and the target web application, allowing you to intercept, inspect and modify the raw traffic passing in both directions.
By modifying browser requests in various malicious ways, Burp Proxy can be used to perform attacks such as SQL injection, cookie subversion, privilege escalation, session hijacking, directory traversal and buffer overflows.

Note
Interception has been disabled by default in SamuraiWTF, re-enable same to function.

Step1: Re-enable proxy
To re-enable, go to the Proxy Options tab, under "intercept client requests", and enable the check box next to "intercept if:" (as Figure 50). [Look at the red color circled highlighted portion].

Step2: Using Burp Proxy
When Burp Proxy is launched, the HTTP/S proxy service is started automatically on port 8080 of the loopback interface only. To start using Burp Proxy, simply configure your browser to use a proxy server on 127.0.0.1:8080, and begin browsing.

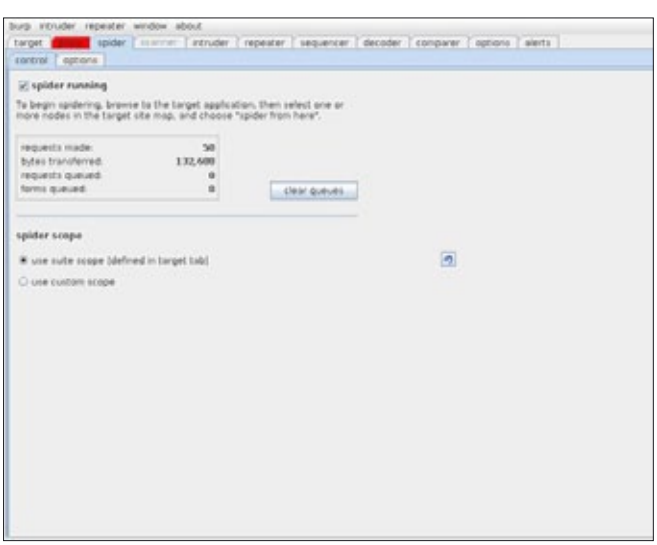


Figure 53. *Control tab*

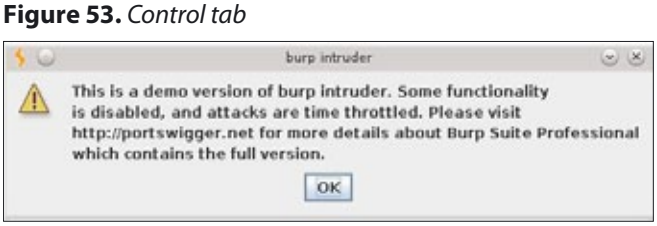


Figure 54. *Alert message*

For example, I configured 127.0.0.1:8080 proxy information in my Samurai's WTF Firefox browser and launched *http://dojo-basic* web site which got intercepted (as Figure 51).

Burp Spider
An intelligent application-aware web spider which allows complete enumeration of an application's content and functionality.
Burp Spider maps a target application by following hyperlinks found within HTML and JavaScript, submitting forms, and using other clues such as directory listings, source code comments.
Burp Spider enables you to obtain a detailed understanding of how a web application works, avoiding the time-consuming and unreliable task of manually following links, submitting forms and scouring HTML source code.
Potentially vulnerable application functions can be quickly identified, allowing you to check for specific vulnerabilities such as SQL injection and directory traversal.

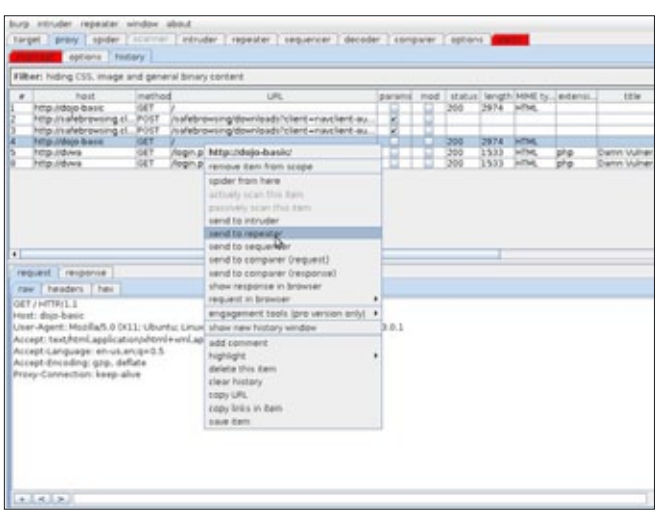


Figure 55. *Selecting target http://dojo-basic*

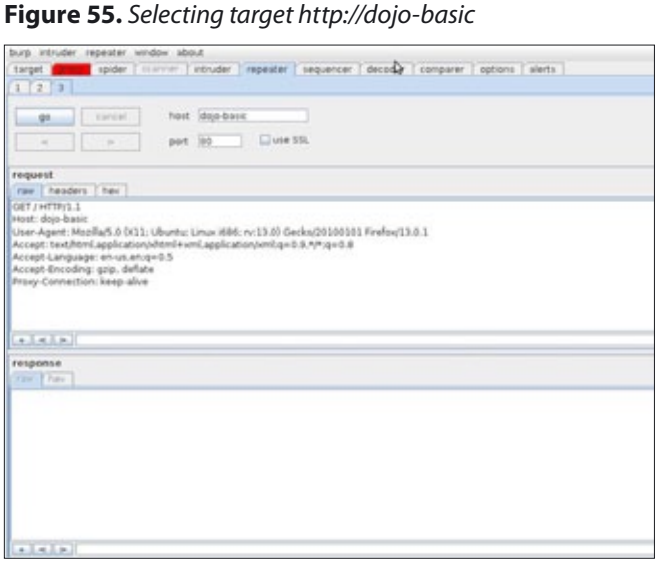


Figure 56. *Request and response windows*

Using Burp Spider

To use Burp Spider against an application requires two simple steps:

Step 1

With your browser configured to use Burp Proxy as its proxy server, browse to the target application. For example, browse target web application http://dojo-basic.

Step 2

Go to the site map in the "target" tab, and select the host(s) and directories where the target application resides. Choose the "spider this host/branch" option from the context menu (as Figure 52).

Step 3

This Control tab is used to start and stop Burp Spider, monitor its progress, and define the spidering scope. For example, spidering target http://dojo-basic and progress can be seen in control tab as Figure 53.

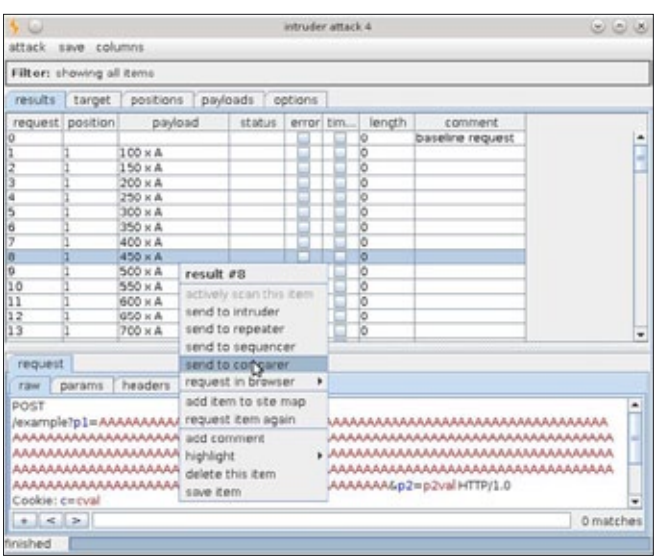


Figure 57. *Passing intruder attack to comparer*

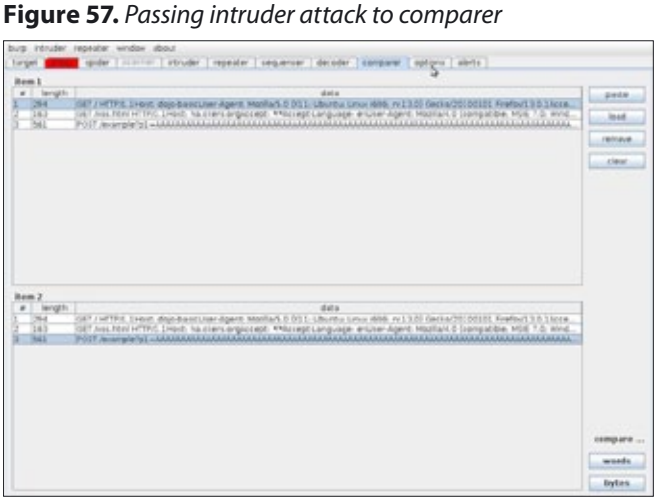


Figure 58. *Two tables in the main panel*

Burp Intruder

A highly configurable tool for automating customized attacks against web applications, such as enumerating identifiers, harvesting useful data, and fuzzing for common vulnerabilities. Burp Intruder is crippled in Free version and shows alert message as Figure 54 while start the attack.

Burp Repeater

Burp Repeater is a tool for manually modifying and reissuing individual HTTP requests, and analyzing their responses. It is best used in conjunction with the other Burp Suite tools. For example, you can send a request to Repeater from the target site map, from the Burp Proxy browsing history, or from the results of a Burp Intruder attack, and manually adjust the request to fine-tune an attack or probe for vulnerabilities. Here using repeater from browsing history and selecting target http://dojo-basic (as Figure 55).

When you send a request to Repeater from another tool, that request gets its own tab. Each tab has its own request and response windows as Figure 56.

Burp Sequencer

A tool for analyzing the quality of randomness in an application's session tokens or other important data items which are intended to be unpredictable. In the context of web applications, the sampled data will typically consist of session tokens, anti-XSRF nonces, or other items on whose unpredictability the application depends for its security.

Burp Decoder

Burp Decoder is a simple tool for transforming encoded data into its canonical form, or for transforming raw data into various encoded and hashed forms. It is capable of intelligently recognizing several encoding formats using heuristic techniques.

To start using Burp Decoder, you can simply type or paste some data into the main panel. In a typical situation, however, you will identify some "interesting" data in the course of using one of the other Burp tools, and you can use the "send to decoder" option to automatically load the relevant information into the tool.

Burp Comparer

Burp Comparer is a simple tool for performing a comparison (a visual "diff") between any two items of data. In the context of attacking a web application, this requirement will typically arise when you want to quickly identify the differences between two application responses (for example, between

two responses received in the course of a Burp Intruder attack, or between responses to a failed login using valid and invalid usernames), or between two application requests (for example, to identify the different request parameters that give rise to different behavior).

To perform a comparison between items of data, you can paste them into Burp Comparer, or load them from file. However, the easiest method is typically to pass the interesting requests or responses directly to Comparer from any of the other Burp tools. For example, passing intruder attack to Comparer as Figure 57.

When items of data have been loaded into Burp Comparer, they appear within the two tables in the main panel (Figure 58).

W3AF GUI

(>Applications>Samurai>Discovery>Automated) (Clicking here launches w3af as Figure 59)

W3AF (short for web application attack and audit framework) is an open-source web application security scanner. This is a complete environment for auditing and attacking web applications. And, this environment provides a solid platform for web vulnerability assessments and penetration tests.

Start W3AF GUI

Executing command

```
samurai@samurai-wtf:~$ w3af_gui &
```

would launch W3AF-GUI (as Figure 59).

W3AF Plug-ins

The w3af plug-ins does all the magic i.e. finding the vulnerabilities and exploiting them. W3AF had three core types of plug-ins: discovery, audit and exploit but the complete list of plug-ins types is:

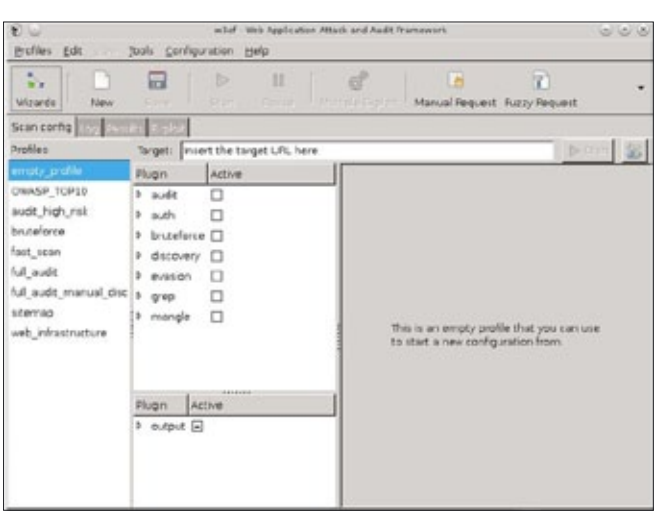


Figure 59. *Launching w3af*

- Discovery: find new points of injection that are later used by audit plug-ins to find vulnerabilities
- Audit: find vulnerabilities after feeding discovery plug-in result
- Grep: analyze HTTP requests and responses that are initiated by other plug-ins and identify vulnerabilities on that traffic; for example, a grep plug-in will find a comment on the HTML body that has the word “password” inside it and generate a vulnerability baseExploit: abusing the vulnerabilities found in the audit phase and return something useful to the user (remote shell, SQL table dump, a proxy, etc)
- Output: This is the way the framework and the plug-ins communicate with the user. Output plug-ins saves the data to a text or html file. Debugging information is also sent to the output plug-ins and can be saved for analysis.
- Mangle: allows modification of requests and responses based on regular expressions, think “sed (stream editor) for the web”.
- Bruteforce: will bruteforce logins. These plugins are part of the discovery phase.
- Evasion: try to evade simple intrusion detection rules

Important Note

Due to stability and consistency issues, it’s better not to enable all plug-ins.

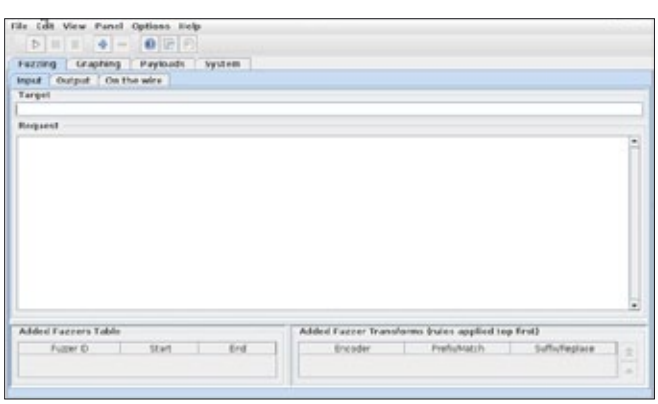


Figure 60. *Launching JBroFuzz*

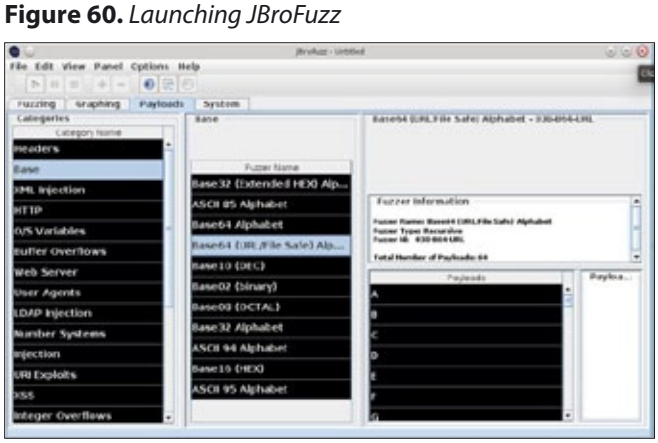


Figure 61. *Tool JBroFuzz*

Starting a Scan

To start W3AF GUI scan, you could use an existing profile from the profile list of W3AF main window which is pre-configured with the required plug-ins. Next, all you have to do is supply target and start the scan. Or, you could create custom profile by selecting desired plug-ins and output format and supplying the target. Also, you could use wizard of toolbar of W3AF main window to create a custom profile to launch scan on your target.

The Output

All the w3af's output is managed by the output plug-ins. Each output plug-in will write in a different format (txt, html, etc), for example the textFile plugin writes all output to the output-w3af.txt file by default. The configuration of output file format is done by checking/unchecking output plug-in of W3AF main window.

JBroFuzz

(>Applications>Samurai>Discovery>Fuzzing)
(Clicking here launches JBroFuzz as Figure 60)

A fuzzer is a program and fuzzing is a software testing technique which injects automatically invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks.

To conduct web application fuzzing, you can automatically send a large number / volume of HTTP Requests including invalid, unexpected and random data like urls, forms, user-generated content, RPC requests etc. to a website, to test its input validation capabilities. Tool JBroFuzz (as Figure 60) is GUI based Java application used for web application fuzzing.

Introduction

JBroFuzz is a web application fuzzer for requests being made over HTTP or HTTPS and offers web protocol fuzzing capabilities. This generates requests, puts them on the wire and records the corresponding responses received back. It does not attempt to identify if a particular site is vulnerable or not; this requires further human analysis.

However, certain payloads included in fuzzers that can be used to generate requests (e.g. XSS) are crafted to attempt to successfully exploit flaws. Such flaws represent previously known vulnerabilities for web applications. JBroFuzz groups fuzzers with their corresponding payloads into a number of categories, depending on previously known vulnerabilities.

Thus, the human analyst would have to select the fuzzers to use in order to test against a particular set of vulnerabilities and review the results in order to recognize if exploitation succeeded or not.

Figure 62. *"Open URL Location" window*

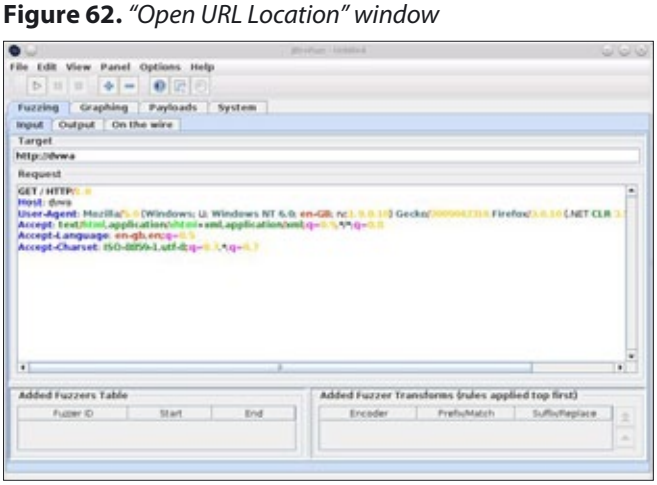


Figure 63. *Fuzzing tab*

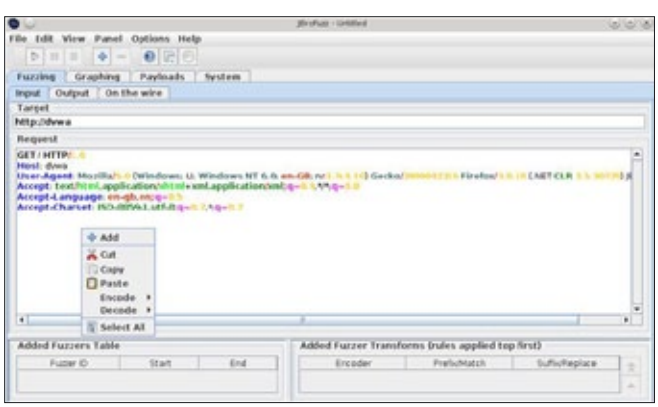


Figure 64. *"Add a Fuzzer" window*

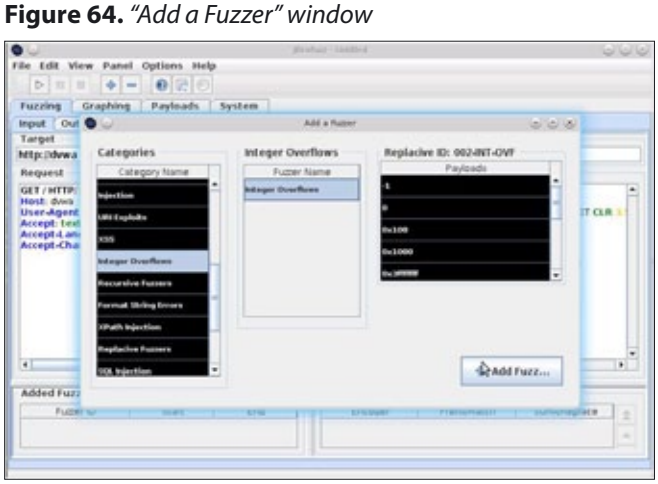


Figure 65. *Selecting "Integer Overflows"*

The components of JBroFuzz are presented into tabs are:

Fuzzing
The fuzzing tab is the main tab of JBroFuzz, responsible for all fuzzing operations performed over the network. Depending on the fuzzer payloads selected, it creates the malformed data for each request, puts it on the wire and writes the response to a file.

Graphing
The graphing tab is responsible for graphing (in a variety of forms) the responses received while fuzzing. This tab can offer a clear indication of a response that is different than the rest received, an indication of further examination being required.

Payloads
The payloads tab is a collection of fuzzers with their corresponding payloads that can be used while fuzzing. Payloads are added to the request in the fuzzing tab; a more clear view of what payloads are available, how they are grouped and what properties each fuzzer has can be seen in this tab.

System
The system tab represents the logging console of JBroFuzz at runtime. Here you can access java runtime information, see any errors that might occur and also track operation in terms of events being logged.

How JBroFuzz Works?

Before we launch a fuzzing attack against a target we should know what payload we are selecting from the list. You could see all the available payloads in Payload tab of JBroFuzz, which looks like Figure 61.

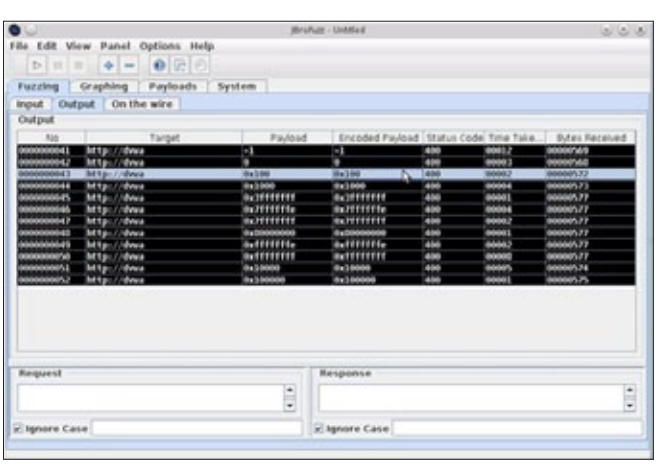


Figure 66. *Output of this fuzzing*

Now, here describing how to set a payload and launch fuzzing attack against a target. All these has to be done in Fuzzing tab.

The 'Fuzzing' tab is where you craft your request message to a particular host. Once that is in place, you can select any part of the request and proceed into adding any number of payloads

Step1: Selecting target and creating request header
In the Fuzzing tab,

- Enter target in the target field. Here, I am using SamuraiWTF's target http://dvwa
- To entry to request field, press [ctrl + L] in the target field, "Open URL Location" window as Figure 62 would appear; select request as required
- Now, your Fuzzing tab look like Figure 63

Step2: Setting up payload and launching the attack

- In the request field of Fuzzing tab, right click and select Add as Figure 64, will show up "Add a Fuzzer" window
- In the category, select fuzzer and payload. For example, I selected "Integer Overflows" as Figure 65
- The fuzzer will be added in the "Added Fuzzers Table" in the bottom of the "Fuzzing" tab
- And, finally hit the start button in the tool bar to launch the attack

Step3: The Output
Go to the "Output" tab to analyze the execution and its response. Output of this fuzzing is shown in Figure 66. For further analysis, select and right click row in the output table and view detailed report.

MANJUL VERMA | A CERTIFIED ETHICAL HACKER

13 years of IT experience in Switching, Routing, Firewalling and Network & Application Security. Experience and expertise includes vulnerability assessment, ethical hacking, peripheral and internal network security, application security, wireless security & evasion of Firewall/IDS/IPS. Currently, employed as Network and Security Architect in PPS R&D division of HP (Hewlett-Packard), Bangalore, India. Prior to HP, served Novell Software, Nevis Networks, Juniper Networks and couple of other startup companies. Email: manjulkverma@gmail.com

Penetration Testing LAB Setup Guide

Internal Attacker – Beginner version

This guide assumes a few things...

- You have installed Backtrack before and you are familiar with using VirtualBox.
- You like breaking stuff!

This penetration testing guide has been created with a few things in mind. One being the reader is a beginner in the field of penetration testing. Two being the attacks are designed from attacker with internal access into the network being penetrated. Future guides will extend upon this document bringing more advanced network setups and unique vulnerabilities.

After setting up this LAB environment, you will have the ability to exploit issues from the following categories:

- Mis-configured Services and Applications
- Backdoors planted into software
- Unintentional Backdoors
- Weak Passwords
- Web Applications
- Plus lots more, how much can you find?

Whysetup a LAB?

Penetration testing is a skill that takes practice to be perfect. In order to be good at it, you must have lots of practice and experience. Unfortunately hacking into computers or the networks that they live on in most cases is illegal. This is where a penetration testing lab comes into value. This LAB should never be used in any sort of publically accessible or production network, it has been made vulnerable intentionally ;)

LAB Setup

Prerequisites

Before getting started, you will need to have installed a working copy of VirtualBox.

VirtualBox: *www.virtualbox.org/wiki/Downloads*.

Along with copies of the following files from the awesome projects below:

- BackTrack R2: *http://www.backtrack-linux.org/downloads/*
- PfSense 2.0.1: *http://www.pfsense.org/mirror.php?section=downloads*

I used: pfSense-2.0.1-RELEASE-i386.iso.gz – *http://files.chi.pfsense.org/mirror/downloads/pfSense-2.0.1-RELEASE-i386.iso.gz*.

- Metasploitable 2: *http://sourceforge.net/projects/metasploitable/files/Metasploitable2/*
- Kioptrix – Level 1: *http://www.kioptrix.com/blog/*

To keep things neat and tidy, create a folder somewhere to place all the above files in. The inside of this folder create a *VirtualMachines* folder. Here you can store the extracted images, as well

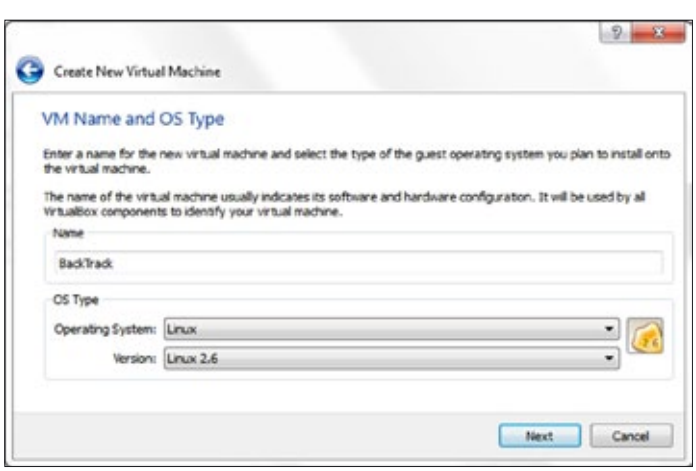


Figure 1. *Creating the BackTrack Virtual Machine*

as virtual disk you will be creating for BackTrack and PfSense installs. You will obviously need a pretty beefy machine in order to run all of the above machines virtually. At a bare minimal, only the following are required to be running. If you follow the exact guide, you will need at least 4GB ram minimum to allocate to all instances.

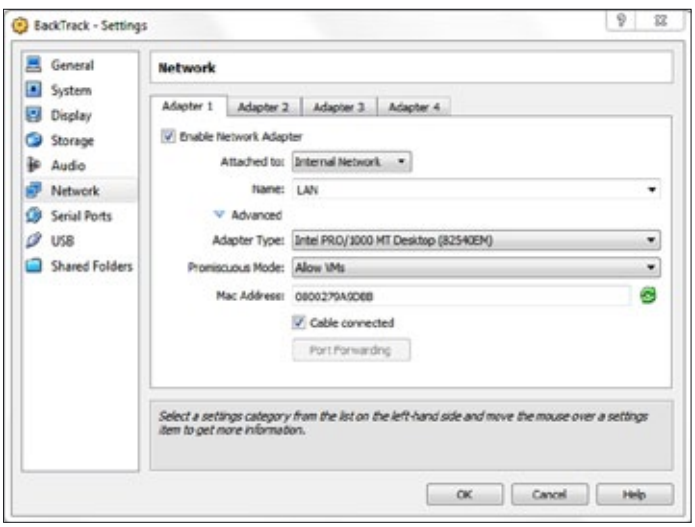


Figure 2. *Configuring the private LAN segment*

Figure 3. *Installing BackTrack to Disk*

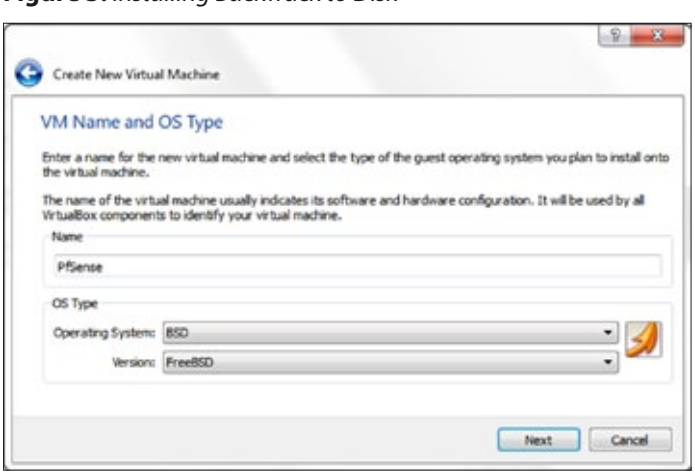


Figure 4. *Creating the PfSense Virtual Machine*

- PfSense
- BackTrack
- Metasploitable 2 and/or Kioptrix – Level 1

LAB System Requirements

4GB of system ram for allocation to Virtual Instances. You can potentially get away with using less, though 4 is recommended.

20.0 GB hard drive space – *15.4 GB* without keeping archives and ISO files.

LAB Setup – Creating VirtualBox Instances

BackTrack

Create a new machine in VirtualBox for BackTrack – R2.
Name: BackTrack
Operating System: Linux
Memory: 512MB minimal – I used 1024MB.
Startup Disk: 15.00 GB minimal

- When creating the instance for BackTrack, you will need a minimal of 512mb of ram for this instance (Figure 1).
- Edit the Network settings of *Adapter 1* to match the following settings.

  NOTE

  While in the configuration, write down the instances MAC Address.

  Attached to: Internal Network
  Name: LAN
  Promiscuous Mode: Allow VMs
  MAC Address: Figure 2.
- Once the instance has been created, start the instance and then proceed to install BackTrack to the virtual disk that has just been created (Figure 3).

PfSense

Create another machine in VirtualBox for *PfSense 2.0.1*.
Operating System: FreeBSD
Memory: 512MB
Startup Disk: 5.00 GB minimal – you *should* not need over 10GB max (Figure 4).

NOTE

This instance will require a bit more configuration on the network adapter side of things.

Installation & Network Configuration

Edit the settings for this instance, and then add a new network card, then configure each interface to match the following settings (Figure 5 and Figure 6).

Adapter 1	Adapter 2
Attached to: Bridged Adapter *Promiscuous Mode*: Allow VMs *Advanced Menu*: *Adapter Type*: PCnet-PCI II	*Attached to*: Internal Network *Name*: LAN *Promiscuous Mode*: Allow VMs *Advanced Menu*: *Adapter Type*: PCnet-PCI II

- Make sure to set *Adapter Type to PCnet-PCI II*, or things will not work correctly.
- Once the instance has been created, start it up and install *PfSense*.
  - Upon booting press 1 to continue with the start-up.
  - At the prompt, press I to proceed with the installation. Once prompted, use the following options in order.
    - Accept these settings.
    - Quick/Easy Install
    - OK
    - Symmetric multiprocessing kernel
    - Reboot PfSense.

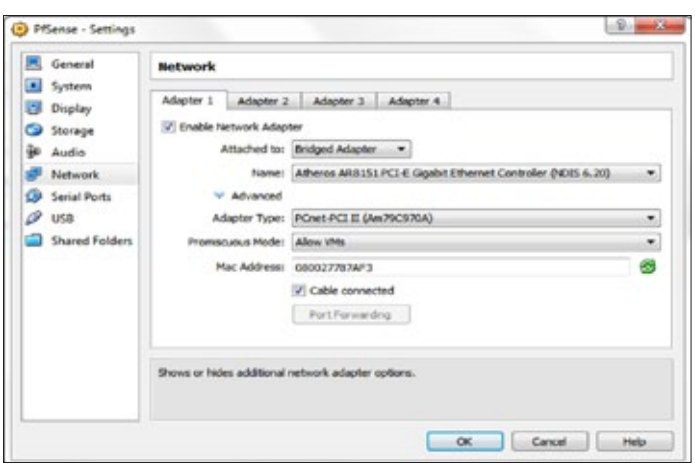


Figure 5. *Tweaking the PfSense Network Adapter*

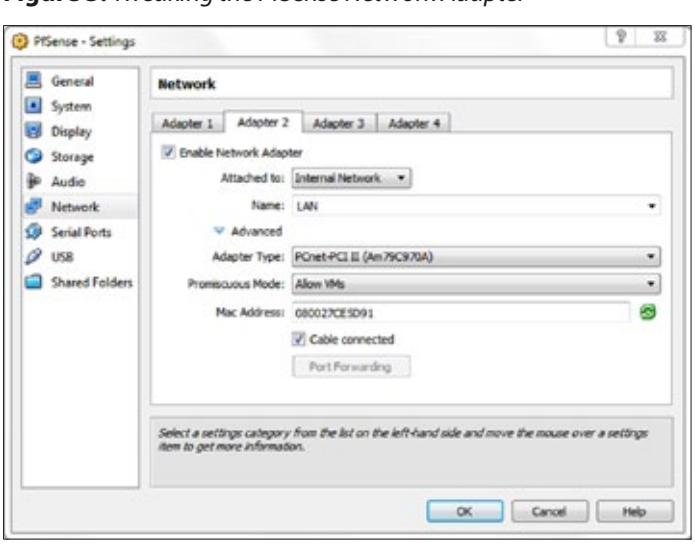


Figure 6. *Enabling a LAN segement on PfSense*

- After PfSense reboots, you will be prompted with the option to create VLANs. Type *n* and then hit *Enter* to continue.
  - Once at the '*Enter the WAN interface prompt type the WLAN1 interface'.* Type in *le0*, and press *Enter*
  - You will now be prompted to specify the *LAN* interface. Type in *le1*, and press *Enter.*
  - To continue press *Enter* again and then *y* when prompted to continue.
  - PfSense should now be installed.
- Once PfSense has been installed, you will need to set the *IP Address* of the *LAN* interface.
  - From the PfSense console select *option 2* 'Set interface(s) IP address'.
  - At the Enter the number of the interface you wish to configure: prompt, type *2* to choose the *LAN* interface.
  - When prompted, use the following *IP Address*: 192.168.12.1
  - Use 24 at the 'LAN IPv4 subnet bit count prompt'.
  - Type *y* at the prompt when asked if you would like to enable the DHCP server on LAN.
  - When asked to provide the starting address range, use the following *starting IP Address*: 192.168.12.50
  - You will then be asked to specify the *ending IP Address* for the DHCP range. Use the following IP Address: 192.168.12.100.
  - Type *y* when asked to enable web configuration.

At this point PfSense should be handing out addresses within: *192.168.12.50-192.168.12.100* range.

NOTE
To confirm DHCP is working properly, reboot the BackTrack instance and verify that it now has an address within the range specified above.

LAB Setup – Vulnerable Machines

What is a penetration testing LAB without things to exploit?

A boring networking lab ;)

For the beginner version of this guide, we will be using some freely available projects purposely built for penetrating. In this guide we will be using Metasploitable 2, provided by the metasploit project, and Kioptrix – Level 1 provided by *kioptrix.com*.

Metasploitable 2
The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download from Sourceforge.net and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMware, VirtualBox, and other common virtualization platforms.

Kioptrix – Level 1
Kioptrix VM Image's are easy challenges. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games is to learn the basic tools and techniques in vulnerability assessment and exploitation. There is more ways than one to successfully complete the challenges.

Metasploitable 2

- Create a new VBox Instance for Metasploitable 2 using the following options.
  Name: Metasploitable 2
  OS Type: Linux 2.6
  Memory: 512
  Startup Disk: Metasploitable.vmdk (Normal, 8.00 GB)
  NOTE
  Make sure you are selecting the *Use existing hard disk* option: then browse to the Metasploitable.vmdk file that was downloaded earlier.
- Once the instance has been created, you will need to change some settings on *Adapter 1* in the Network settings. From the Network section.

Go to *Adapter 1* and change the following options.
Attached to: Internal Network
Name: LAN

NOTE
Under the Advanced menu, take note of the MAC address. You will need it later.

Kioptrix – Level 1

- Create a new VBox Instance for *Kioptrix – Level 1* using the following options.
  Name: Kioptrix VM Level 1
  OS Type: Other Linux
  Memory: 256
  Startup Disk: Kioptrix Level 1.vmdk (Normal, 3.00 GB)
  NOTE
  Make sure you are selecting the *Use existing hard disk* option: The Kioptrix Level 1.vmdk file can be found within the download.
- Once the instance has been created, you will need to change some settings on Adapter 1 in the Network settings. From the Network section.

Go to *Adapter 1* and change the following options.
Attached to: Internal Network
Name: LAN

NOTE
Under the Advanced menu, take note of the MAC address. You will need it later.

PfSense Setup

Configuration
Now that PfSense has been setup in a default state, and confirmed to be handing out DHCP addresses properly. We can now begin configuration of PfSense by accessing it via the web interface from the BackTrack machine using Firefox.

To access the PfSense web interface, open the following URL in Firefox: *http://192.168.12.1*.

The default username is: *admin* and the default password is: *pfsense*.

Login to the web interface and follow the prompts through the guided wizard to complete installation. Nothing needs to be changed at this point, other than verifying the settings you have specified earlier.

Once the PfSense setup has finalized, reload the web interface to get to the main configuration view.

Extra Packages (optional)
A few *optional* packages can be installed.

These packages will not be used in this guide, though they will in the *External Attacker – Intermediate* version of this guide.

- From the PfSense interface, go to *System->Packages*.
  Then Install *Proxy Server with mod_security* by clicking the + icon next to the listing.
- Once installed, go back to *System->Packages*.
  Then install *snort*.

SNMP Setup (optional)
Since this is a penetration testing guide for beginners, let's start out by making the firewall itself a lit-

tle bit vulnerable. This will make something simple and easy to test out SNMP enumeration attacks or vulnerability scanners.

- From the PfSense web interface, go to *Services->SNMP*.
- Next to the *SNMP Daemon* section, check off *Enable*. Then *save* the settings.

PfSense – DHCP

Now that PfSense has been setup and configured, you can now make use of the MAC Addresses you have taken note off earlier when creating the vulnerable lab machines.

Vulnerable machines – Static Reservations

- Open up the PfSense web interface. Then go to *Services->DHCP Server*.
  - Verify that the range specified is the same range specified you have specified earlier in this guide during the PfSense setup.
    NOTE
    This never seems to be the same range as specified on the console initially.
- Scroll to the bottom and add a new Static Reservation for the Metasploitable 2 and Kioptrix instances. Using the MAC addresses you wrote down.

Metasploitable2	Kioptrix – Level 1:
MAC Address: (the one you wrote down) *IP Address*: 192.168.12.20 *Hostname*: metasploitable2 *Description*: metasploitable2	*MAC Address*: (the one you wrote down) *IP Address*: 192.168.12.30 Hostname: kioptrixl1 Description: kioptrix – level 1

- Once the above reservations have been created, you can now *save & apply* the settings to PfSense.
- Verify the configuration by restarting each vulnerable instance.

To simplify the setup, you can edit the `/etc/hosts` file on the BackTrack machine, adding the following entries:

```
192.168.12.20  metasploitable2
192.168.12.30  kioprtrixl1
```

Virtual Lab Layout & Diagrams

Virtual Box Layout

Figure 7.

Virtual Network Diagram

External Subnet: DHCP Assigned
Internal Subnet: 192.168.12.0/24

Firewall: Internal: 192.168.12.1 External: DHCP Assigned
BackTrack / Attacker: Internal: 192.168.12.x/24
Metasploitable2: Internal: 192.168.12.20
Kioptrixl1: Internal: 192.168.12.30
Figure 8.

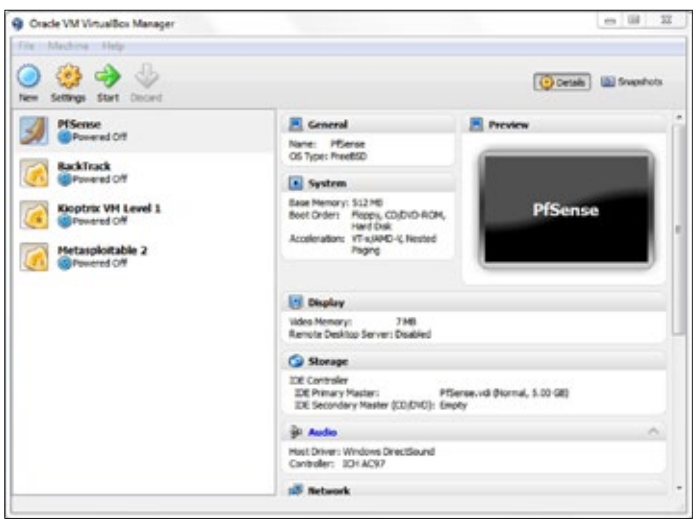


Figure 7. *LAB setup overview*

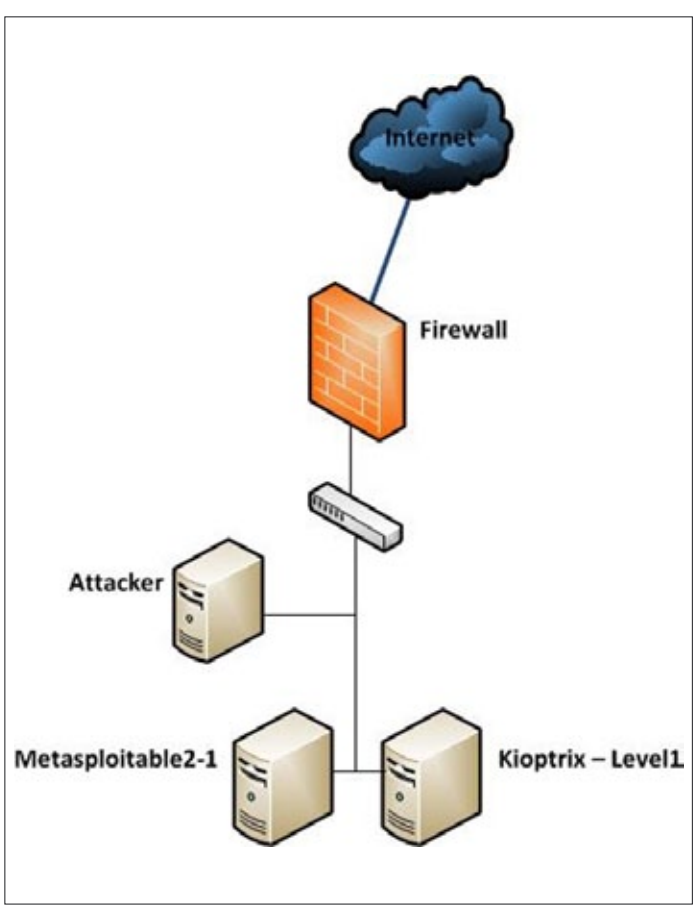


Figure 8. *Logical LAB network diagram*

Conclusion

Once everything has been started, you should now be ready to start testing out your skills in the newly created penetration testing LAB. Keep in mind this LAB has been designed with access from an internal attacker's perspective. From the BackTrack machine you can now start exploring the *192.168.12.0/24* network. Have fun!

If you have any questions or issues with the above instructions, please let me know. As this is an initial release, so expect some bugs or un-documented features to come up ;D

If you are completely clueless after following this guide, have a look at the following exploitation guides.

Exploitation Guides

If you are truly a beginner, this will help you out along the way. If not, carry on and start hacking…

Metasploitable 2 Exploitability Guide: https://community.rapid7.com/docs/DOC-1875.

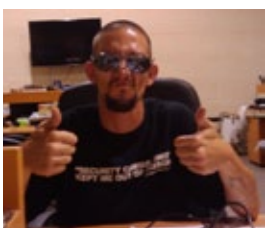
As always, Hackers do it with all sorts of characters…

Syntax Guide

Below is a reference point for syntax and highlighting used throughout this guide.

- *Information* – Denotes required information.
- *command* – Reference to a system command, normally not required to be run by the user for the instructions unless stated otherwise.
- *command* – Reference to a system command to be ran by the user as part of the instructions.
- *Something*: something – Reference to an option in the GUI application.
- *Action* – Denotes some action to be performed with the current GUI application.
- *File name* – Specifies a file name.

JEREMIAH BROTT



Jeremiah currently holds a lead role with Access2Networks Toronto as an Information Security Consultant. In addition to holding numerous certifications, Jeremiah is also the professor for Malicious Code – Design & Defense along with Ethical Hacking at Sheridan Institute for the Applied Information Sciences System Security degree program. Hacker's do it with all sorts of characters… www.IHackedThisBox.com

Picking Up

Mushrooms in the Rain Forest
Social Engineering Information Gathering

Social Engineering is a field of information security industry that is both known and unknown to general public. On the one hand, there is a number of world known social engineers, from both the dark and the bright side of the trade, whose adventures are captured in numerous movies and memoires.

While on the other hand social engineering is one of the topics that are full of speculation and uneducated claims, including those in the media, and that sadly turns social engineering into some kind of a gray area.

In the meanwhile, social engineering infiltrates a substantial part of computer security operations. To name few, Security Awareness, despite its arguable efficiency, is the set of information security controls directed to decrease the probability and potential impact of security incidents caused by inherited vulnerabilities of human nature. Also, social engineering vector, or as we often call it Social Channel, is an integral part of a robust penetration test according to every modern methodology in this field. Not to mention the variety of human factor threats facilitated by the ubiquity of the Internet, such as phishing, 419 scam, email and social networks spam and so on and so forth.

Obviously enough, knowing all this does not make any one of us a (Anti) Social Engineering expert. For several decades now we (and by 'we' I mean information security professionals) have known that 'human factor' is the cause of something around 80% security threats and did almost nothing to deal with that. While network channel of attack keeps increasing the difficulty of its exploitability, social engineering tricks work as they used to for Kevin Mitnick and Frank Abagnale. And sometimes even better (or worse, depending on your perspective) because there are many times more people targets accessible by the attackers nowadays.

So, what can we do? Many things, in fact. First of all, if Social Engineering threats constitute a significant threat to your business, revise your business model. Can you remove people component from it? I guess, no. Then, you have to change or educate people and that is the hard part.

As I said, people are inherently vulnerable because… they are people. People are willing to talk, trust, and share to each other and that is both to our benefit as a species and disadvantage as individuals. It may seem funny, but all the things that helped us develop the society can be used in malicious purpose by immoral individuals.

The complete course of action that may increase your resistance to Social Engineering attacks would take a book to briefly describe and I am going to recommend some of existing books in the end of this article. As a quick start I recommend to conduct an audit and learn from it. For some using audit techniques in the beginning of information security program may seem unnatural, but think about it: can we start any improvement without sufficient knowledge of our current state? I strongly doubt it. In this article we'll discuss some aspects of social engineering penetration testing, in particular information gathering. There is a very small chance of successfully assessing security when it works. Instead, usually it takes a hard time of trying to break it. And there unlikely is a field in pentesting that is more sensitive to proper information gathering than social engineering audit.

So, let's start with a threat model. Roughly speaking, there is a target or 'mark' that is our goal in a pentest. Most of the time it's all about getting sensitive information important enough to be further leveraged in order to get and maintain access to IT systems, or alternatively be used directly in

order to demonstrate risk to the client's business. The mark can be also an action by individual (e.g. personnel) that can facilitate the attack: influencing guards to grant access us to restricted area, or making a person click malicious link or open uber-APT-dropping email attachment can be another goal. Keeping all the SE methods and techniques out for the time being, there is one thing lack of which renders all that SE 'dark art' useless: Information. Gathering sufficient amount of information is vital in a pentest, and the type of information we are looking for strongly depends on what result we want to achieve.

In the course of this article, let's assume that our goal is to contact some of the client's employees and present them with email with our 'special' attachment, or a link to some crafted or cloned website. While the former is often used in order to gain access to the client's network, the latter is a tool of choice for credentials harvesting. So, it seems like we need some email addresses, right? First thing that comes to mind is, of course, using a search engine such as Google. Unfortunately almost all of them are doing a good job of keeping this type of data not that easy to find. Try to search for some sort of email yourself and you will see that the regular approach works pretty well when you are searching for a specific email, but fails miserably once you try to find some new, unknown emails in a specific domain. So, what can we do to search for *usernames@client.com*?

Sure thing, there are some tools for that. First, look at theHarvester, an easy to use information gathering tool. Fire up your BackTrack and find it in `/pentest/enumeration/theharvester/theHarvester.py`. The tool takes many options, the most important of which are *what* to search for and *where*: `-d` and `-b` options respectively (Listing 1).

Let's type some demo commands to show its power. In line with some other information, the command `./theHarvester.py -b all -d hakin9.org` will also show this section: Listing 2.

While this is a relatively modest list of emails, I hope that's enough to show you theHarvester's power and simplicity. Next, let's think for a while about some other places we can find emails. Remember what a regular email looks like: it's either *fistname.lastname@client.com*, or *flastname@client.com*, or *firstnamel@client.com*. There are, of course, some companies that put more effort to obscure the real email of their staff behind some sort of *firlastn@client.com* by putting together pieces of first and last names of various lengths. But those cases are rare, so forget about it for

Listing 1. *Running theHarvester*

```
noroot@bt:/pentest/enumeration/theharvester$ ./theHarvester.py

Usage: theharvester options

       -d: Domain to search or company name
       -b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles,people123,jigsaw,all)
       -s: Start in result number X (default 0)
       -v: Verify host name via dns resolution and search for virtual hosts
       -f: Save the results into an HTML and XML file
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 to 50 results,
          -h: use SHODAN database to query discovered hosts
            google 100 to 100, and pgp doesn't use this option)

Examples:./theharvester.py -d microsoft.com -l 500 -b google
         ./theharvester.py -d microsoft.com -b pgp
         ./theharvester.py -d microsoft -l 200 -b linkedin

noroot@bt:/pentest/enumeration/theharvester$
```

now. In general, emails can be obtained from employees' names, period. And where can we find those names? Of course, on social networks.

The social network of choice here is, of course, LinkedIn. Despite its recent security issues, LI remains a serious business communication tool and not only for recruiting as some people may think. Even with 'basic' account you can dig a lot of client's employees there: just search for a company name and export the results form browser to an HTML file. After that, apply your knowledge of the client's naming convention: how the real 'human' names are transformed to usernames by their IT administrators. Few minutes of grep'ing and regexp magic, and here you are with your list of *potential* usernames. I say potential, because at this point it's your 'educated guesses' of usernames, nothing more. To use it effectively, you should verify it and the question is 'how'?

For this purpose Social Engineers have three good friends: VRFY, EXPN and RCPT. These are the commands of SMTP protocol that makes our rare emails cross the Internet in the flow of constant spam load. They do the following: VRFY literally verifies a given email or username, EXPN expands mailing lists, end RCPT admits that the recipient's email is correct in the course of SMTP conversation. While the latter is vital for email systems functioning properly, the former two should not be used, especially on the Internet facing email servers, so called MXs. And the main reason why is that having access to these commands in the client's domain we can easily verify every single guess we made about their usernames and emails. All these actions are easily automated by any `netcat` flavor and a scripting language like Perl or Python: Listing 3. Yeah, see ya. Thanks for making my day. As you can see, even a small organizations leek all sort of contact information to the public. And the main reason is because almost none or of them treats this type of information with due respect. But Social Engineers do.

Listing 2. *theHarvester output*

```
[+] Emails found:
------------------
grzegorz.tabaka@hakin9.org
andrzej.kuca@hakin9.org
ireneusz.pogroszewski@hakin9.org
ewa.dudzic@hakin9.org
patrycja.przybylowicz@hakin9.org
karolina.lesinska@hakin9.org
en@hakin9.org
monika.drygulska@hakin9.org
magda.b@hakin9.org
robert.zadrozny@hakin9.org
newsletteren@hakin9.org
hakin9@hakin9.org
romanp@hakin9.org
tonid@hakin9.org
en@hakin9.org
```

Listing 3. *Using SMTP VRFY command*

```
noroot@bt:~$ ncat mail.client.com 25
220 mail.client.com ESMTP; Wed, 12 Aug 2012 00:00:00 +0200
VRFY accounting
250 Yeah, I know that one.  He (or she) is Accounting Department <accounting@client.com>.
VRFY vpupkin

quit
221 See ya in cyberspace
```

Another place to search for contact details is… your client's website. And I don't mean those contacts on 'About' page which you should have found in very beginning. Instead, search for some office documents and PDF files. For that use a Google 'dork' of this kind: `site:hakin9.org filetype:pdf` and you can combine various file types joining them by OR keyword. There are always such files, because your client's business should use some documents. And documents usually contain Metadata.

Metadata's definition is tricky: it's data about data. Roughly speaking, it is not what's contained within the document, although that information can also be very interesting, but rather what are the properties of the document itself. These properties might be document's name, location, revision number, size, or, and that is of most interest to us, its author. Document's author usually is the operating system username that created it, which leads us to a new contact to verify and then send our emails. All this data can be seen in the document's properties once it's downloaded from the website, however doing this manually is kind of boring. And since the metadata has its value, it should come with no surprise that there is a tool for its collection.

Meet FOCA: the ultimate metadata mining tool. It searches websites for documents that contain metadata and then downloads them, parses them for information, and then categorizes and correlates what it's found. Along with contact information, there are more sweets for you: the types and versions of software by which the documents have been created. You can download FOCA following a short registration process on its website *http://www.informatica64.com/foca.aspx*.

So, let's start FOCA and create a sample project using `docstoc.com` domain website. The first thing you will see is the search windows. You can choose from one to three of supported search engines there and also limit the search to specific types of documents. Although I believe it's a good idea to always search with and for all of them, let's start with `Google`, `.pdf` and `.doc(x)` for now. As of the time of this writing, FOCA found 10 PDF files at hakin9.org website, so let's download them. Click the right mouse button at any document URL and choose "Download All". Downloading all PDF files from a website may take a while, then click it again and choose "Extract All Metadata". Warning: be careful with the files you're downloading, because running malicious PDFs in vulnerable software may cause all sorts of harm (Figure 1).

Once you've downloaded all the documents and extracted metadata from them, you will see that the tree of parameters in the left pane of FOCA's windows is now populated with various values, including usernames and types and versions of soft-

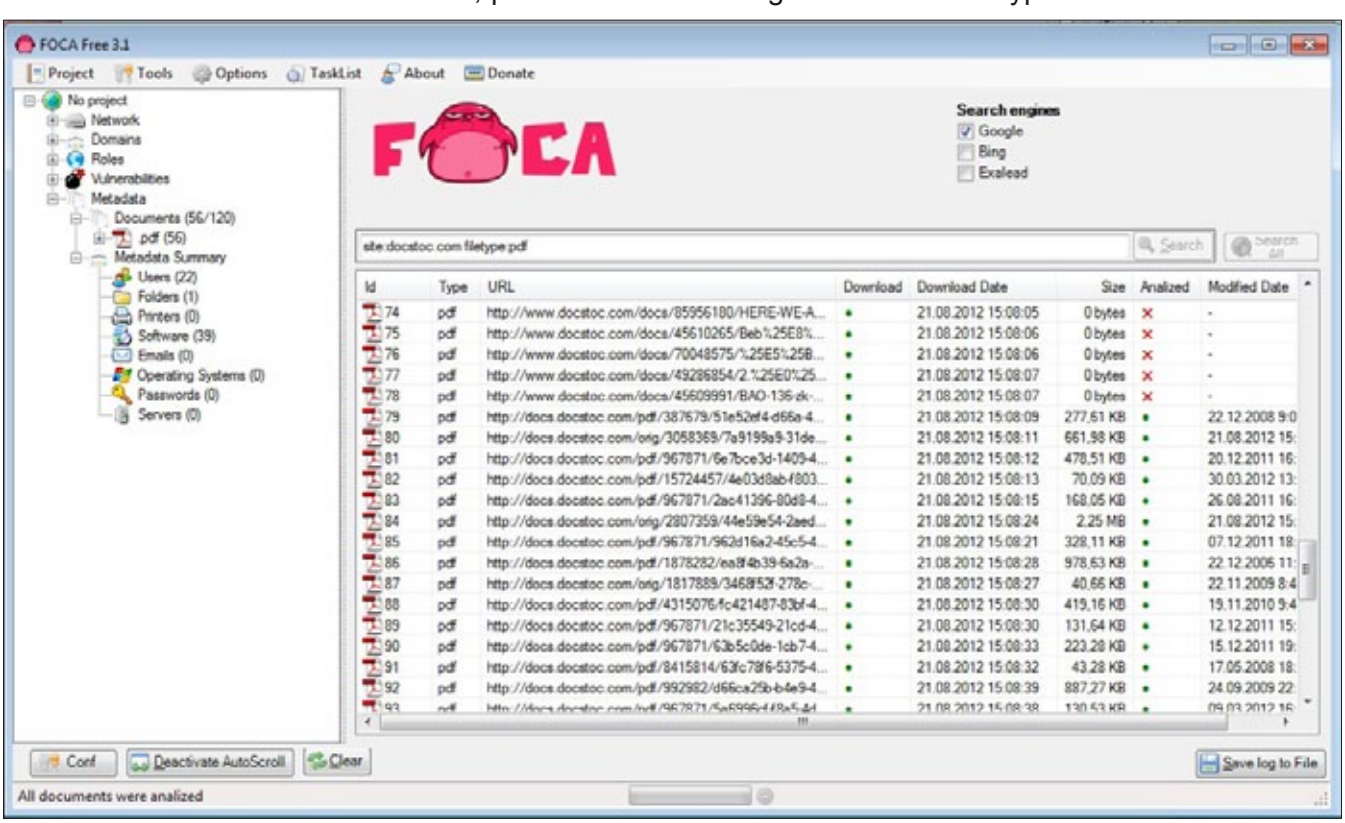


Figure 1. *The list of downloaded and analyzed documents in FOCA*

ware packages used to create the files. All this information is linked to the original files, so you can always find which user created what and by what software. Now you can go search for some folks still using Office XP and Adobe Reader 8.

Of course, it is completely up to us what amount of metadata leaks in the documents we create. Windows users can remove any detail of all of them at once just by opening the document's file properties, going to 'Details' tab and clicking 'Remove Properties and Personal Information' (Figure 2).

Unfortunately, things are not that simple for OpenOffice users and on Linux, but you can find the way to remove metadata by researching this topic yourself. If you are concerned about the security implications of metadata leakage in the corporate world (and I assume that you already are) you may also search online for some commercial-grade gateway-like software products.

The next piece of software I want to show you has become an irreplaceable tool in the pentesters' arsenal and Social Engineers are not the exception. Cool guys at Paterva created Maltego for our fun and profit. To describe what it does I will use one word: Magic. Of course, any IT magical trick has a piece of prominent technology behind it, in this case it's an outstanding extendable information correlation engine, but anyway, Magic is the

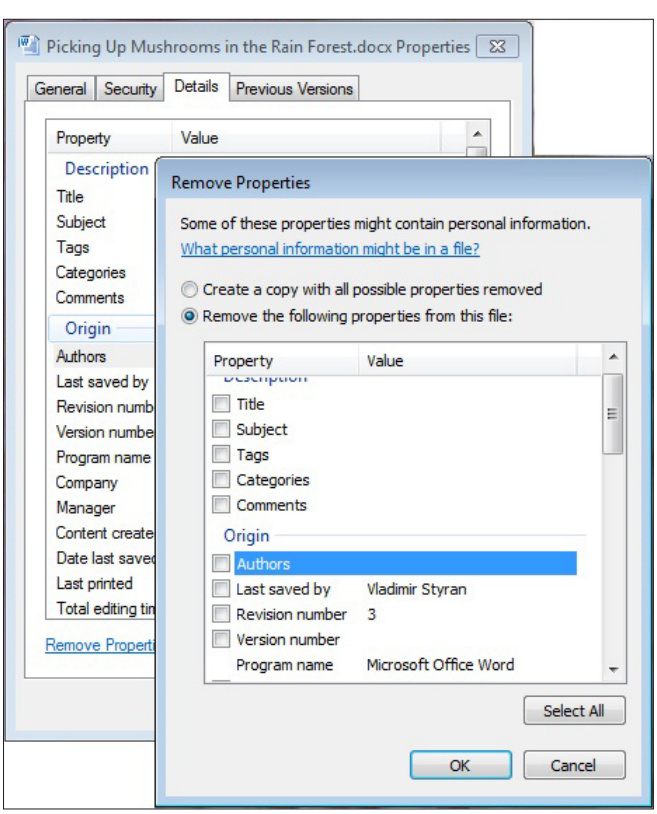


Figure 2. *Edit or remove metadata from document files in Windows*

right word. You can download a Community Edition version of Maltego here *https://www.paterva.com/web5/client/community.php*, it also comes with the latest version of BackTrack. To start using Maltego you have to register on community website and resolve a captcha in its user interface once in a while. That is to remind you that you should definitely buy a fool version once you decide to use Maltego for your pentesting engagements.

Alright, let's start Maltego and create a new graph. Maltego calls its projects 'graphs' and you will soon know why (Figure 3).

At the left pane of the GUI you can see a list of various types of information you can insert into the graph. Think of these objects as 'nodes'. Once put into the graph, every node can be 'transformed' into another type of object by a predefined transformation – either executed remotely on a server or located locally at your hard drive. At the picture above you can see the list of transforms available for an email address. Start playing with Maltego using your personal information and trying to transform it to something else and I am sure you will be surprised with the results.

As you can see, Maltego does little that could not be performed manually otherwise. Remember those VRFY scripts we made earlier? They totally can replace 'Verify email address exists [SMTP]' transform on emails. Theoretically, all these transforms could be done by hands through searching the Internet and finding relationships between different pieces of data. But given Maltego's ease of use and intuitive approach to information search and correlation I cannot imagine my life without it any more.

Although execution of Social Engineering attacks is somewhat beyond the topic of this article, I cannot miss a chance to give you some guidance on it. Let's assume that I wrote this article for a reason and at this point you have gathered a list of valid email addresses of the client you have an engagement with. Let's also assume that you have an explicit written permission to perform Social Engineering audit of your client's organizational security controls and employee awareness. And it would also be great to ensure that your client have notified their employees that an audit may take place. (Yes, I know, that's hard, but we cannot stay within ethical boundaries without all these precautions). In a situation like this you may start sending your emails and that is another area for automation.

Social-Engineer Toolkit is your friend for that. SET comes with BackTrack or can be downloaded from its developer's website *https://www.trusted-*

sec.com/. Dave 'Rel1k' Kennedy brought it to us so we can use that mighty tool to conduct an array of various SE attack scenarios. To run it `cd` to its work directory `/petntest/exploit/set` and start it as root: `sudo ./set`.

SET has a structured text-based interface organized as a tree of menus. Since we decided to work on two specific types of attacks (sending links and attachments) let's check out what can SET help us with in this regard (Figure 4).

By choosing '1) Social-Engineering Attacks' menu item, you will see that first available options are exactly what we needed: '1) Spear-Phishing' and '2) Website' attack vectors. Spear-phishing lets us conduct either mass or directed email attacks with predefined email templates and recipients lists. SET has strong integration with Metasploit in order to handle the results of your attacks. Try to proceed with configuring a spear-phishing attack and you will see that there is a wide choice of payloads to attach to your email. Payloads can be configured to start and run various kinds of remote shells including Meterpreter, and there is a flexible configuration for how your shells should ring back home. From my experience, Java or PDF payload with Meterpreter reverse HTTPS shell works almost all the time. After choosing payload options, SET sends your emails and starts Metasploit reverse connection handler for you. All you have to do now is just sit and wait for Meterpreter sessions finding their way home. Be careful: since most social engineering attacks have extremely high success rate, your reverse handler may hang or crash under the DoS. Just kidding.

Alright, what about credentials harvesting? Don't erase all those email addresses, we'll need them. Run Social-Engineer Toolkit once again and choose '1) Social-Engineering Attacks', then '2) Website Attack Vectors'. Then choose attack method, Java Applet is my favorite for this vector, but you choose '2) Credential Harvester'. SET can start a web server for you and populate it either with a predefined template or a cloned site. Although cloned sites are extremely useful for social engineering attacks, they often cannot be used due to complexity of modern web applications. In these cases, when the website has a dynamic structure or its URL contains some personalized part that cannot be guessed by site cloner script, you will find Web Templates approach very useful. But for now choose '2) Site Cloner' and clone some well-known website such as Twitter or Facebook. Social-Engineer Toolkit will now

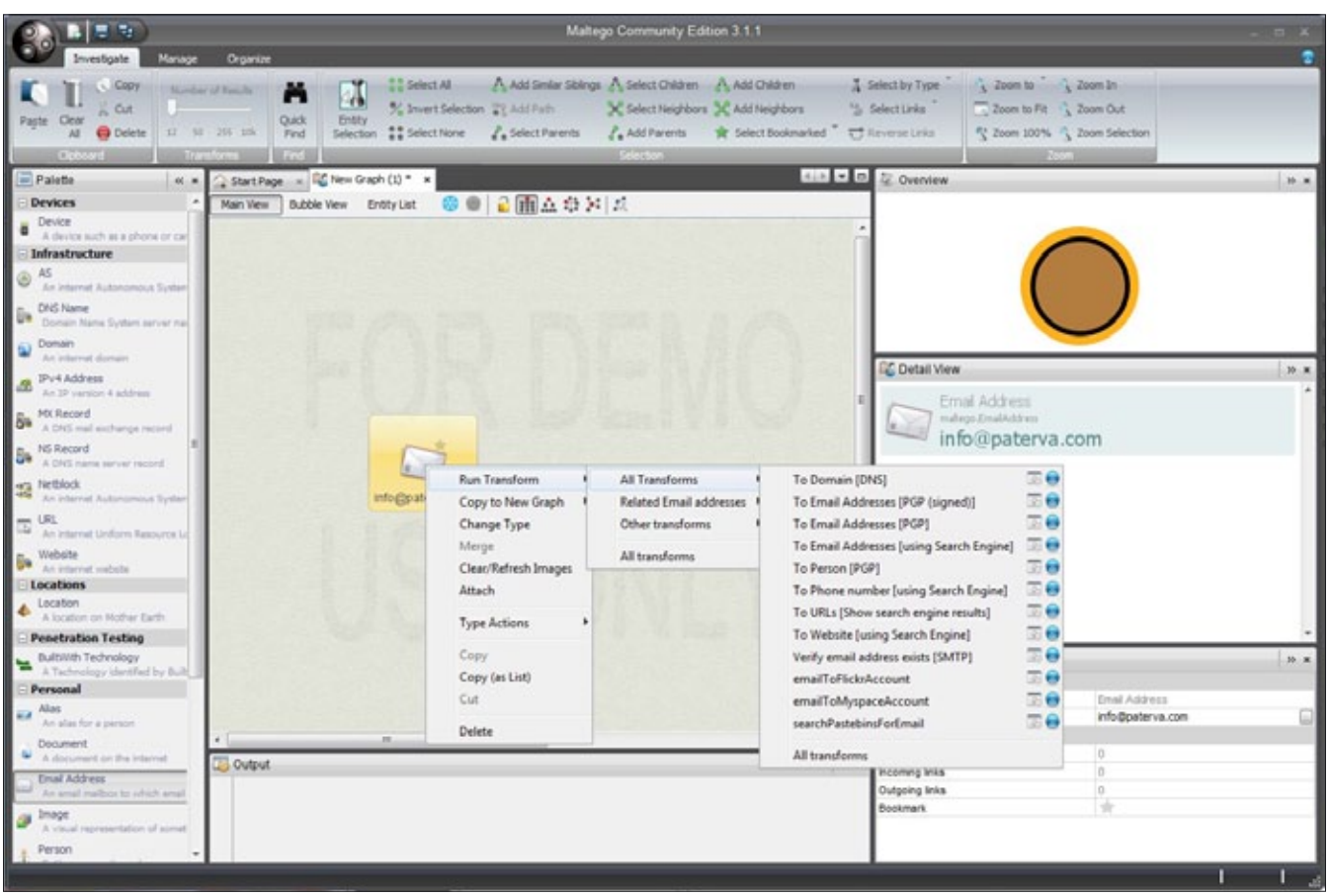


Figure 3. *The list of Maltego transforms available for an email address*

clone and start the website for you and you can direct your browser to http://localhost to see the exact copy of cloned website. Type some gibberish to sign-in form and submit it then go back to SET still running on background. As you can see, your browser is automatically redirected to the true cloned site, and your login credentials are showed in SET. Impressive, huh?Once again, as in the case with Maltego, you can see that this entire juicy staff can be done manually with little knowledge of any scripting language. But it would take so much time to automate social engineering attacks with such level of usability. So next time you meet Dave, buy him a beer. But be careful and don't hug him!

As you can see from above, there is a nice set of tools that can be used during a social engineering audit. Take them and put them to good use. I hope that information in this article can help you assess and increase security awareness of your colleagues and customers. But there is one more thing I want to stress here.

Remember that you assess security, e.g. processes that help people and organizations manage the risk. Thus processes are the ones to blame here once you accomplish a huge success during the audit and indicate the ease of obtaining critical information or running a shell on a critical system. Many organizations do not understand that in this case processes fail, not people. And the cases when people pay for the lack of organization's commitment to security are not rare.

As a security auditor, you should always remember that firing a person who 'clicked the link' is the stupidest action to take since this person is probably the most security aware employee when the audit ends and you present the report. So, first educate your customer in regard of the things said and then try to keep your results unbiased and remove all personal details from the report before sending it to your customer. These are things that save your karma and let you sleep at night.

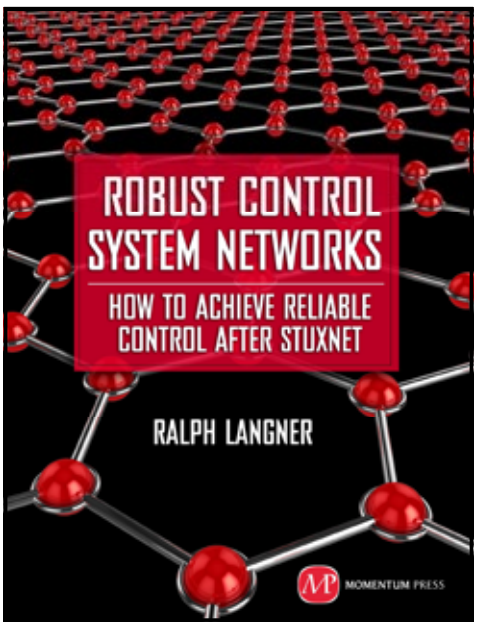
As a conclusion, as promised, let me present you with some direction for further research on the topic of Social Engineering. In this article we discussed the very technical part of the trade that constitutes a very small portion of social engineering knowledge. To know more, use an outstanding Social Engineering Framework at *http://www.social-engineer.org* and listen to its monthly podcast. Also, there is a great book written by Chris Hadnagy, the founder of social-engineer.org, called 'Social Engineering, the Art of Human Hacking' which I strongly recommend once you decide to know more on the topic.

Figure 4. *Social-Engineer Toolkit main menu*

VLAD STYRAN

Vlad Styran is a security professional focusing on security audits and penetration tests for last 5 years. Vlad has 11 years of experience in implementing security systems, building information security management systems, and conducting large scale security audits. Currently Vlad holds position of Lead Security Consultant in a large Ukrainian professional IT services company BMS Consulting. Vlad writes a blog on information security (http://securegalaxy.blogspot.com) and is a co-host of security podcast Securit13 (http://secuirt13.libsyn.com). He is certified with CISSP, CISA, CEH, ISO27001LA, SCSA, CCNA and others.

MOMENTUM PRESS



From the researcher who was one of the first to identify and analyze the infamous industrial control system malware "Stuxnet," comes a book that takes a new, radical approach to making Industrial control systems safe from such cyber attacks: design the controls systems themselves to be "robust."

Ralph Langner started a software and consulting company in the industrial IT sector. Over the last decade, this same company, Langner Communications, became a leading European consultancy for control system security in the private sector. The author received worldwide recognition as the first researcher to technically, tactically, and strategically analyze the Stuxnet malware.

www.momentumpress.net
222 E. 46th Street, #203
New York, NY 10017

Do You Want to Become a Cyber Security Expert?

OR ADVANCE YOUR IT SECURITY CAREER?

- Cyber Security has one of the largest market shares in IT
- Government & Compliance Regulations are more and more enforced
- Gartner Group predicts unprecedented growth and need in Cyber Security
- Skilled Cyber Security Experts are in ever more demand

THE CYBER 51 EXPERT COACHING FORUM

- Individual 1-on-1 Mentoring on Ethical Hacking, Penetration Testing and IT Security
- Networking with other community members and moderators
- Access to a wealth of tools and information not found on public domain
- Permanent Job & Contract offers, Webinars and much more!

YOUR BENEFITS

- Become an Ethical Hacker / Penetration Tester with 1-on-1 mentoring
- Learn at your own pace at a fraction of the cost of regular courses

CYBER 51 COACHING FORUM

CYBER SECURITY FORUM

CONTENT:

1. General Topics
2. Service Assessment
3. Ethical Hacking
4. Cyber Threats
5. Mitigating Cyber Threats
6. Penetration Testing

CYBER 51 INSTRUCTORS

OUR CERTIFICATION LEVELS:

- Certified Ethical Hacker (C|EH)
- Forensic Investigator (C|HFI)
- Certified Security Analyst (ECSA)
- Licensed Penetration Tester (C|LPT)
- Network Security Admin (ENSA)
- ISC Consortium (CISSP)

FEATURES

ADDITIONAL FEATURES:

- 1-on-1 Coaching
- Trainers with Years of Experience
- Wealth of Tools
- Webinars
- Networking with other members
- Contract & Perm. Job Opportunities

WHY CYBER 51?

- Learn whenever you want to
- Dedicated 1-on-1 Coaching
- Information you will not find on public boards
- All Mentors work as Senior Security Consultants
- Frequent updates
- Great Value for money

CYBER 51
A PURE CYBER SECURITY NETWORK

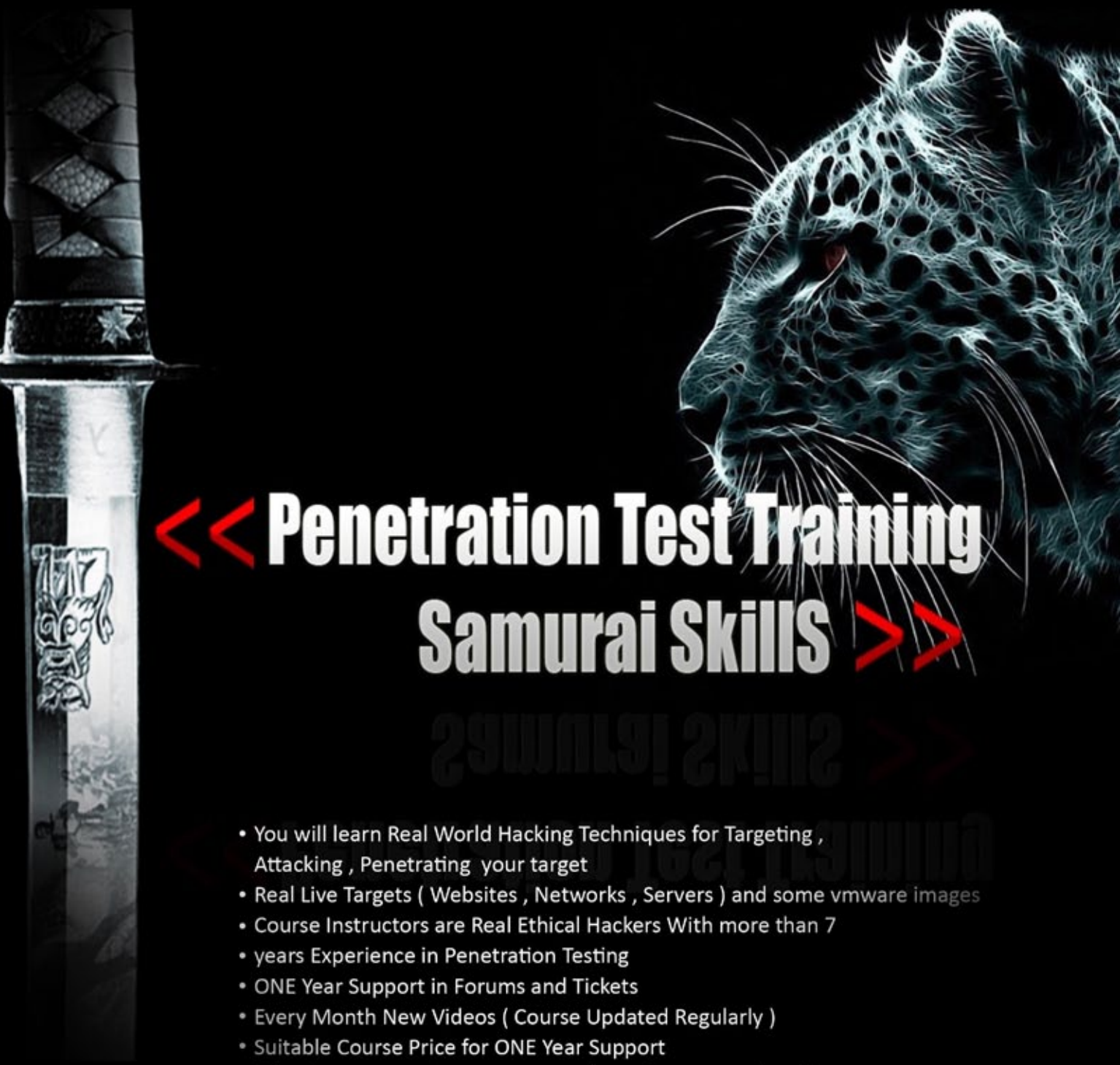
CONTACT US TODAY

CYBER 51 LIMITED, 176 THE FAIRWAY, SOUTH RUISLIP, HA4 0SH, MIDDLESEX, UNITED KINGDOM

EMAIL: INFO@CYBER51.COM

WEB: WWW.CYBER51.COM

CODENAME:
SAMURAI SKILLS COURSE



<< Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time , any where)
- Our Course is Totally Different from Other Courses (new Techniques)