CS695 – Lab 2

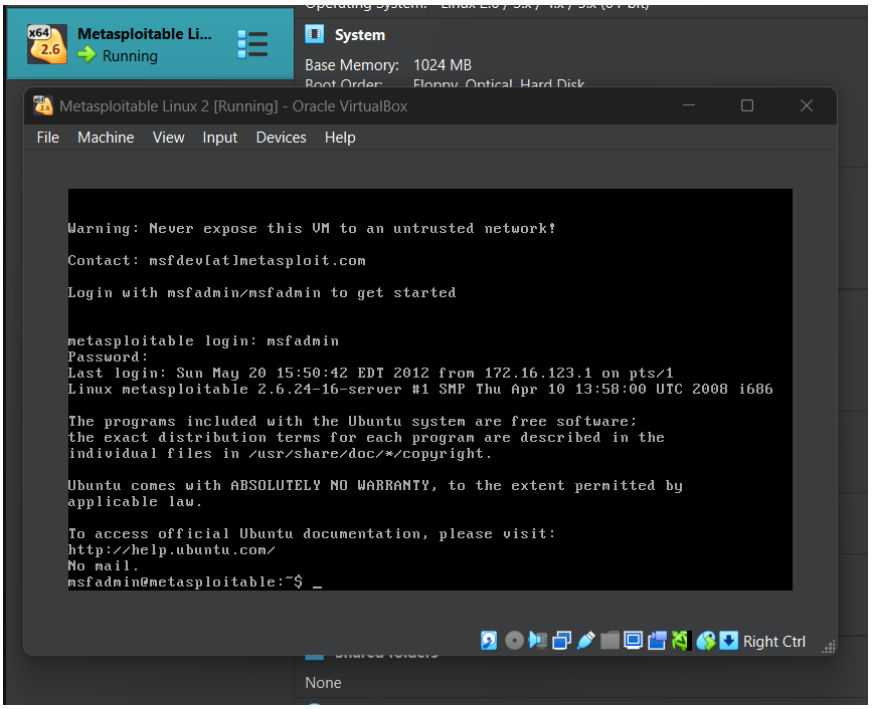
Probing and Vulnerability Scanning

Ryan Christopher

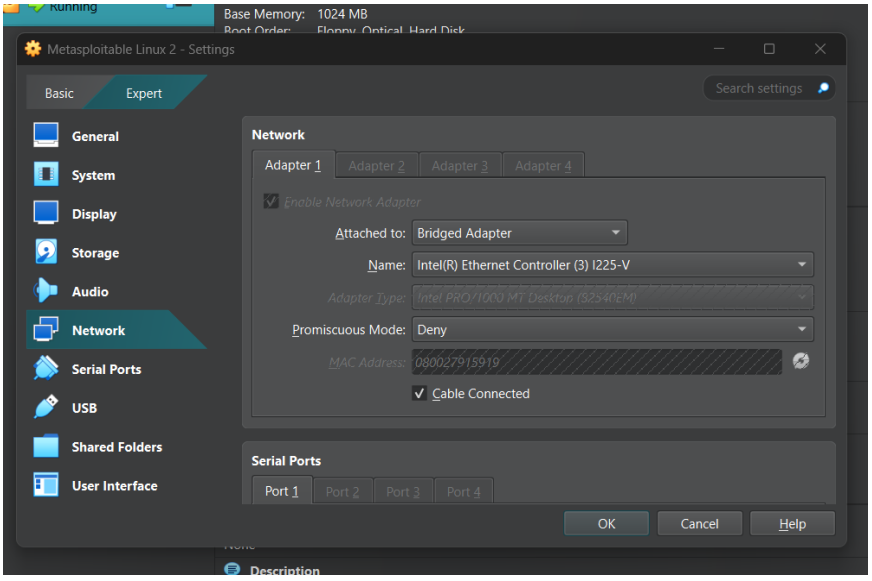
Table of Contents:

Lab Preparation – Load Metasploitable 2 Linux into VM

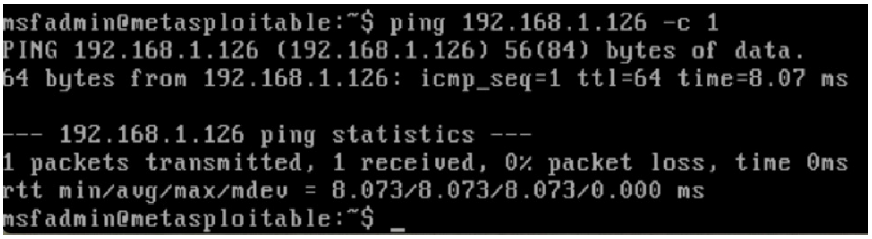
7)



8)

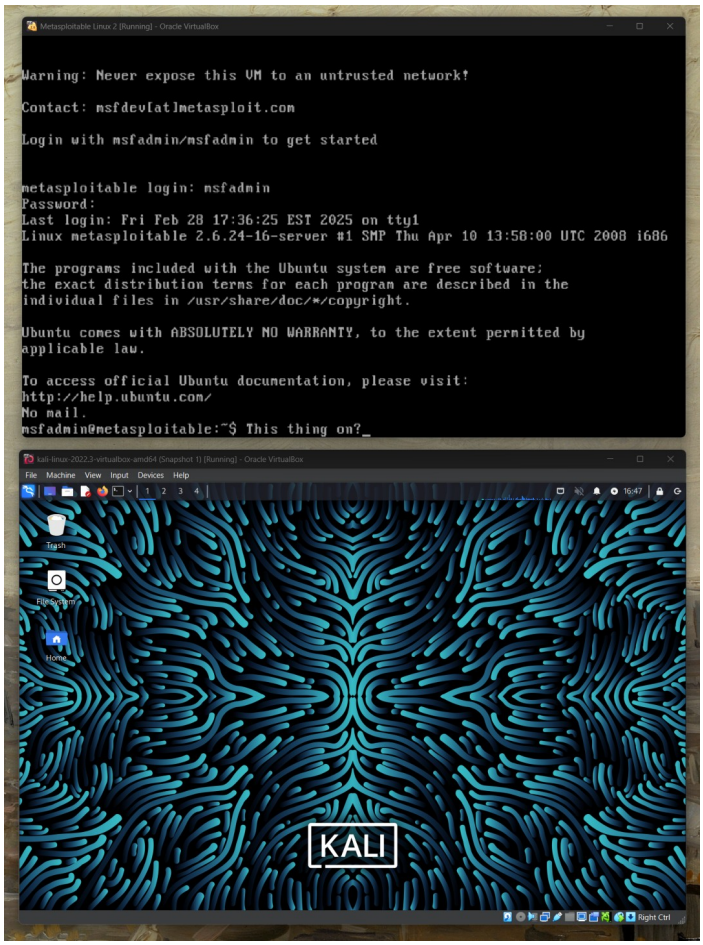


9) The IP for Metasploitable 2 is 192.168.1.125 and the IP for Kali is 192.168.1.126:

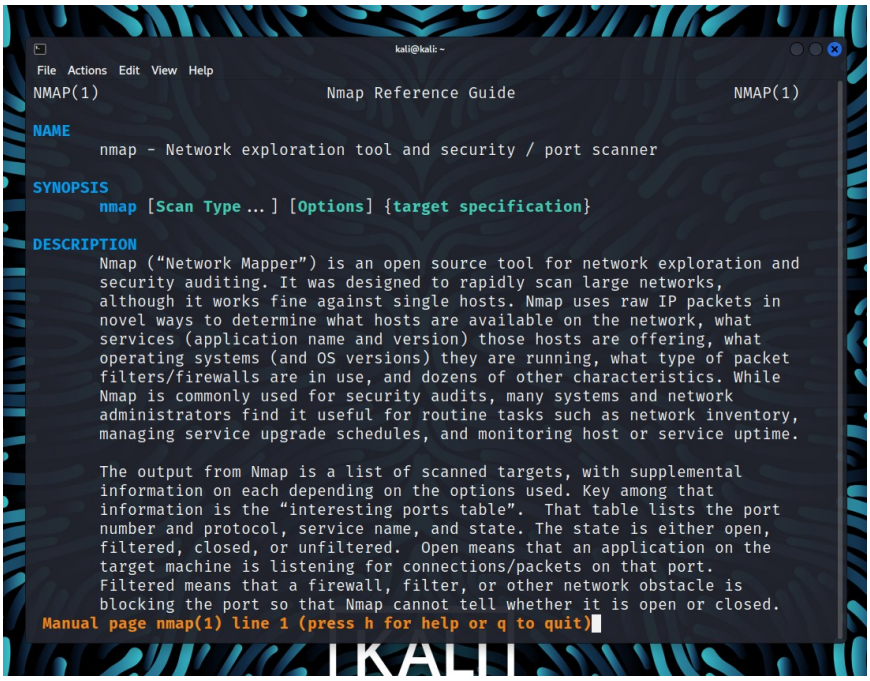


Part 1 – Using Nmap to Probe

1)



2)



3)

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ /usr/sbin/ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.126  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::76a5:d7d7:8d7e:d7f2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 1155  bytes 70791 (69.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1042  bytes 64900 (63.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$
```

4)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 23:38 EST
Nmap scan report for 192.168.1.125
Host is up (0.00059s latency).
MAC Address: 08:00:27:91:59:19 (PCS Systemtechnik/Oracle VirtualBox virtual NI
C)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

5)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.1.125/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 23:41 EST
Nmap scan report for 192.168.1.1
Host is up (0.00065s latency).
MAC Address: 54:07:7D:18:CE:5C (Netgear)
Nmap scan report for 192.168.1.4
Host is up (0.015s latency).
MAC Address: 14:7D:DA:0B:AB:03 (Apple)
Nmap scan report for 192.168.1.8
Host is up (0.00024s latency).
MAC Address: 04:42:1A:E6:58:EC (ASUSTek Computer)
Nmap scan report for 192.168.1.10
Host is up (0.038s latency).
MAC Address: 84:90:0A:63:61:16 (Arcadyan)
Nmap scan report for 192.168.1.11
Host is up (0.14s latency).
MAC Address: 80:60:B7:0C:30:9C (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.1.33
Host is up (0.11s latency).
MAC Address: F8:B9:5A:D2:E4:4E (LG Innotek)
Nmap scan report for 192.168.1.60
Host is up (0.19s latency).
MAC Address: 2A:E0:C2:19:90:4B (Unknown)
Nmap scan report for 192.168.1.105
Host is up (0.11s latency).
MAC Address: 8C:86:1E:B7:4A:4E (Apple)
Nmap scan report for 192.168.1.125
Host is up (0.00098s latency).
MAC Address: 08:00:27:91:59:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC
)
Nmap scan report for 192.168.1.126
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 3.38 seconds
```

6)

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 23:43 EST
Nmap scan report for 192.168.1.125
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:91:59:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC
)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 23:45 EST
Nmap scan report for 192.168.1.125
Host is up (0.00080s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:91:59:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-1000 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 23:45 EST
Nmap scan report for 192.168.1.125
Host is up (0.0026s latency).
Not shown: 988 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:91:59:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

┌──(kali㉿kali)-[~]
└─$
```

7)

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 23:47 EST
Nmap scan report for 192.168.1.125
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:91:59:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.28 seconds

┌──(kali㉿kali)-[~]
└─$
```

8)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 23:50 EST
Nmap scan report for 192.168.1.125
Host is up (0.00063s latency).
Not shown: 977 closed tcp ports (reset)
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        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
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
MAC Address: 08:00:27:91:59:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: U
nix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.12 seconds

┌──(kali㉿kali)-[~]
└─$
```

Part 1 Questions:

1) What is a network mask? How do you use it to determine the IP address range of your LAN?

A network mask is a 32-bit digits in the form of 4 octets that identifies the network address and the host address of an IP address. This is done by converting the IP address and the netmask into their binary octets. The section of the binary representation of the IP address shares the same position as the 1's in the netmask is the network address, whereas the section that overlaps with 0's is the host address. With this, the range of a LAN can be determined by setting the host binary values to 0 to find the first possible address and all of the host binary values to 1 to find the last possible address.

2) 3 vulnerabilities rated as "high" for Linux 2.6.9 – 2.6.33:

1: Return value not checked – "artswrapper in aRts, when running setuid root on Linux 2.6.0 or later versions, does not check the return value of the setuid function call, which allows local users to gain root privileges by causing setuid to fail, which prevents artsd from dropping privileges."

If a bad actor knows that a return value is not checked, they can write malicious code that forces setuid to fail and gain root privileges for an unsuspecting user or for their own user if they are able to remotely control the device. This would then make the bad actor able to have a higher level of control and access to the system than the system intended.

2: Linux kernel does not properly handle page faults – "The Linux kernel 2.6.9 before 2.6.9-67 in Red Hat Enterprise Linux (RHEL) 4 on Itanium (ia64) does not properly handle page faults during NUMA memory access, which allows local users to cause a denial of sevice (panic) via invalid arguments to set_mempolicy in an MPOL_BIND operation."

If a user downloads malware that knows of this vulnerability, their system could held ransom and be made unusable through panic that would be forced through page faults on NUMA memory access.

3: Vulnerability in apk-tools that can result in Remote Code Execution – "Alpine Linux versions prior to 2.6.10, 2.7.6, and 2.10.1 contains a Other/Unknown vulnerability in apk-tools (Alpine Linux's package manager) that can result in Remote Code Execution. This attack appears to be exploitable via a specially crafted APK-file that can cause apk to write arbitrary data to an attacker-specified file, due to bus in handling long link target name and the way a regular file is extracted."

By allowing remote code execution to occur, this vulnerability has a strong ability to compromise the security of the system. If an APK-file that appears legitimate contains the instructions needed to write to another file on the targeted system.

3) 3 Vulnerabilities rated as “high” for MySQL 5.0.51a:

1: Backdoor in vsftpd 2.3.4 – “vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.”

This vulnerability was listed as “high” in CVSS 2.0 and “critical” in CVSS 3.x, and is due to the nature of a backdoor allowing unauthorized access to a system through the port that is opened by vsftpd.

2: SQL injection vulnerability in ProFTPD 1.3.1 – “SQL injection vulnerability in ProFTPD Server 1.3.1 through 1.3.2rc2 allows remote attackers to execute arbitrary SQL commands via a “%” (percent) character in the username, which introduces a “” (single quote) character during variable substitution by mod_sql.”

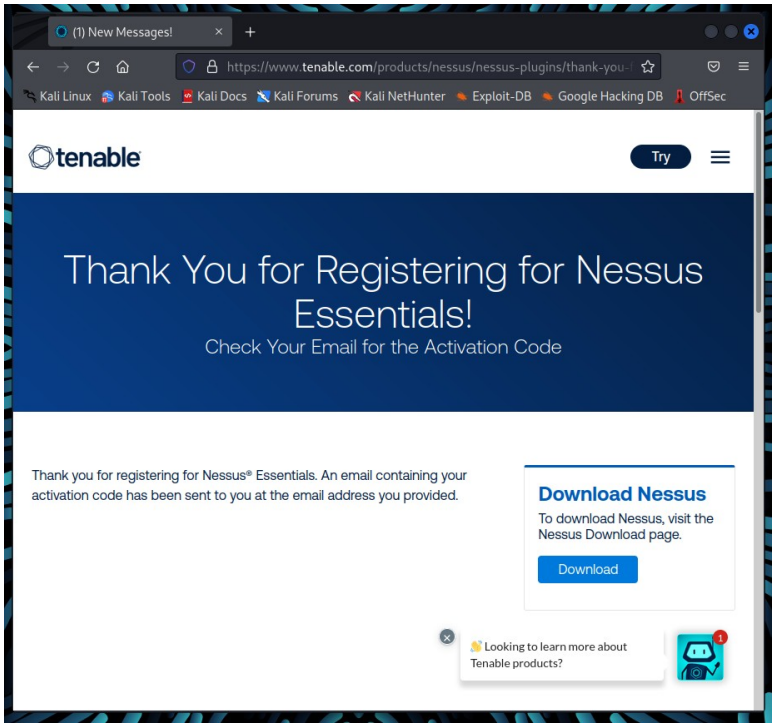
A SQL injection vulnerability when exploited can result in important/sensitive data being accessed and modified on the target system.

3: Linux telnetd allows remote attackers to bypass authentication – “telnet daemon (telnetd) from the Linux netkit package before netkit-telnet-0.16 allows remote attackers to bypass authentication when telnetd is running with the -L command line option.”

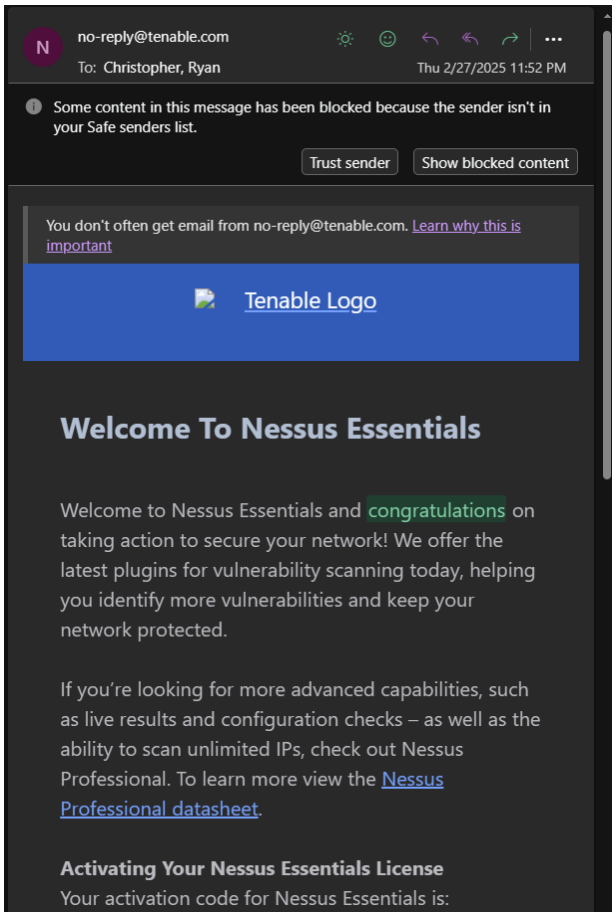
If authentication is bypassed, a remote attacker that successfully exploits this vulnerability would gain immediate access to the target system, making the data that is normally protected fully accessible.

Part 2 – Using Nessus to Scan Vulnerabilities

1)



2)



3)

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  lab1  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Nessus-10.8.3-ubuntu1604_amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$
```

4)

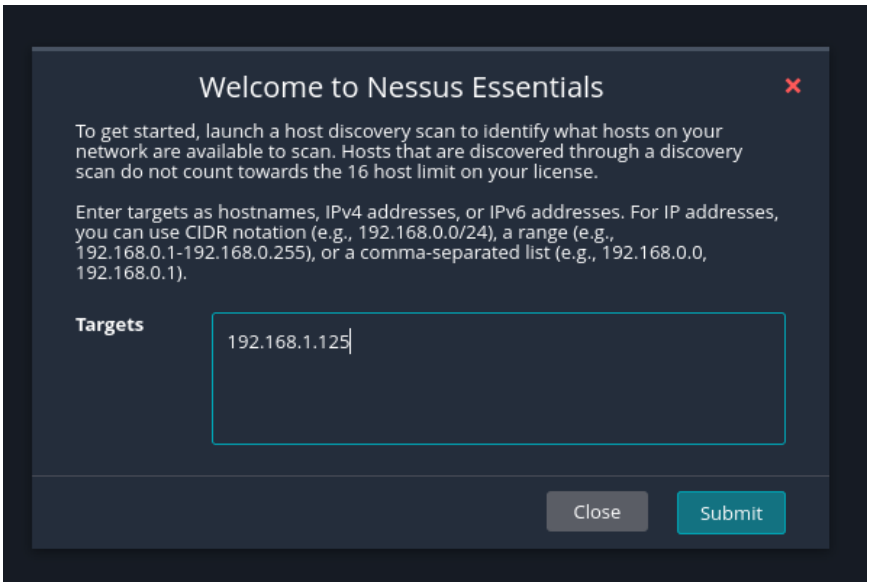
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i ~/Downloads/Nessus-10.8.3-ubuntu1604_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 342013 files and directories currently installed.)
Preparing to unpack .../Nessus-10.8.3-ubuntu1604_amd64.deb ...
```

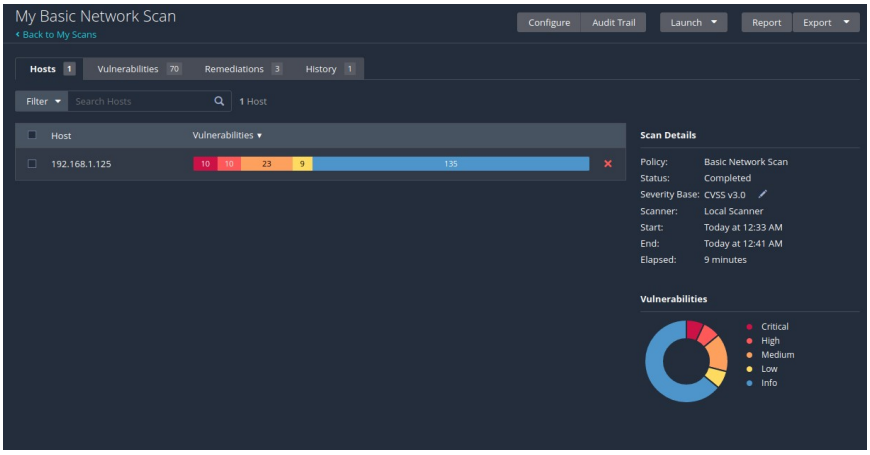
5)

```
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner


┌──(kali㉿kali)-[~/Downloads]
└─$
```

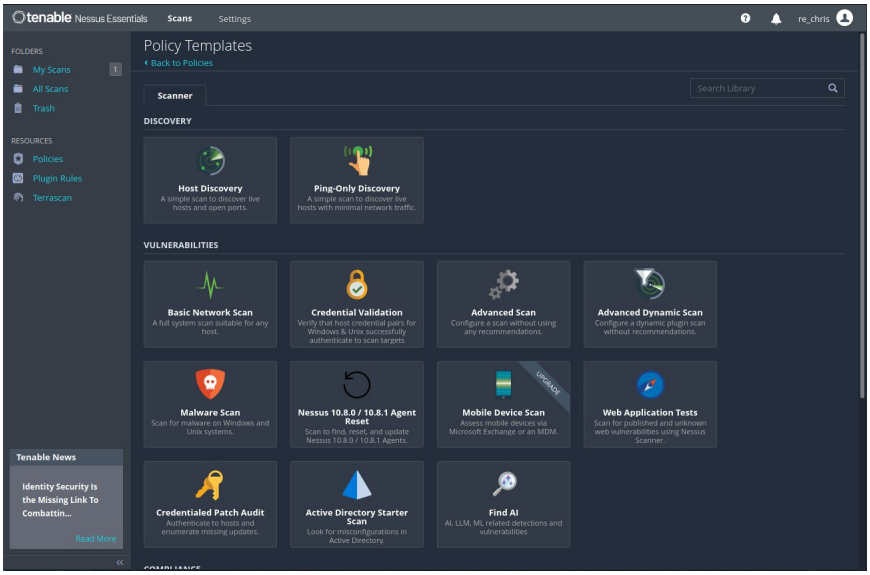
```
┌──(kali㉿kali)-[~/Downloads]
└─$ /bin/systemctl start nessusd.service

┌──(kali㉿kali)-[~/Downloads]
└─$
```

6-12)

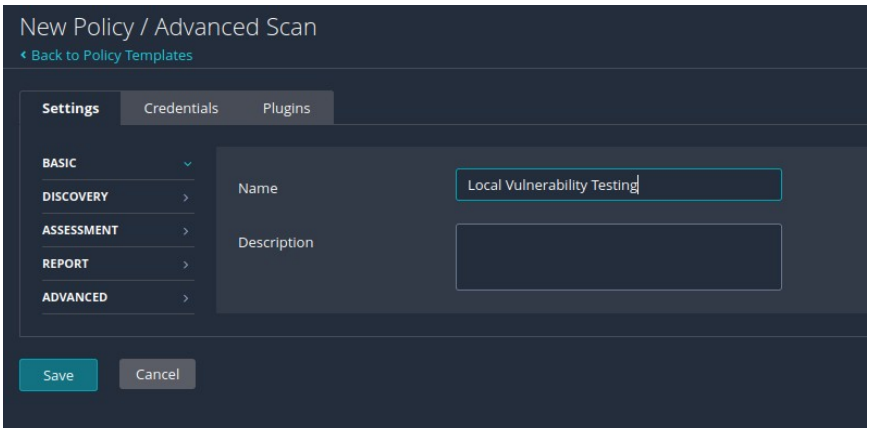



My Basic Network Scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 70
Remediations 3
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.1.125
10
10
23
9
135
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:33 AM
End: Today at 12:41 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

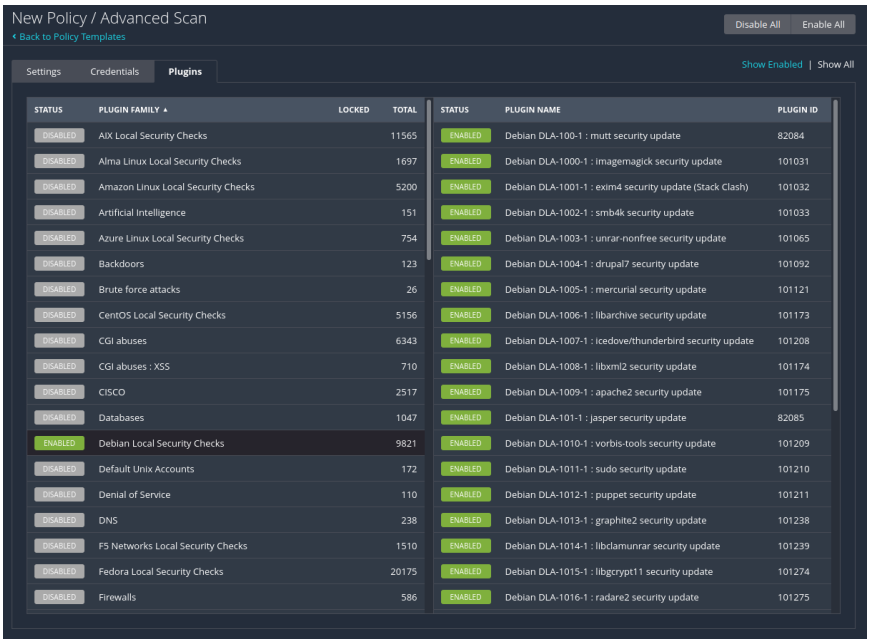
13)


tenable Nessus Essentials
Scans
Settings
re_chris
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Identity Security Is the Missing Link To Combattin...
Read More
Policy Templates
Back to Policies
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Active Directory Starter Scan
Look for misconfigurations in Active Directory.
Find AI
AI, LLM, ML related detections and vulnerabilities

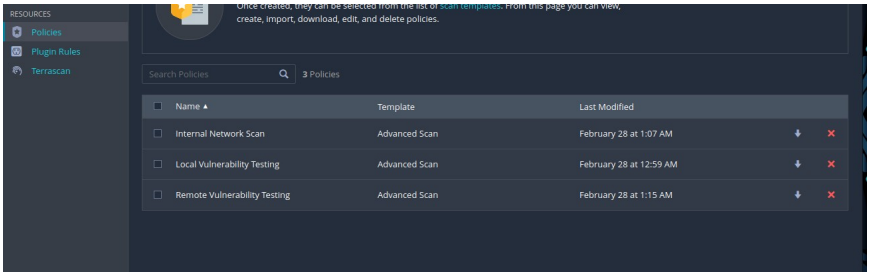
14)


New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Local Vulnerability Testing
Description
Save
Cancel

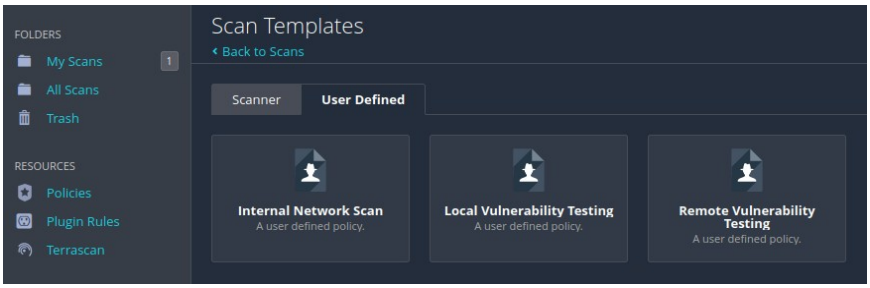
15)


New Policy / Advanced Scan
Back to Policy Templates
Disable All
Enable All
Settings
Credentials
Plugins
Show Enabled | Show All
STATUS PLUGIN FAMILY LOCKED TOTAL
DISABLED AIX Local Security Checks 11565
DISABLED Alma Linux Local Security Checks 1697
DISABLED Amazon Linux Local Security Checks 5200
DISABLED Artificial Intelligence 151
DISABLED Azure Linux Local Security Checks 754
DISABLED Backdoors 123
DISABLED Brute force attacks 26
DISABLED CentOS Local Security Checks 5156
DISABLED CGI abuses 6343
DISABLED CGI abuses : XSS 710
DISABLED CISCO 2517
DISABLED Databases 1047
ENABLED Debian Local Security Checks 9821
DISABLED Default Unix Accounts 172
DISABLED Denial of Service 110
DISABLED DNS 238
DISABLED F5 Networks Local Security Checks 1510
DISABLED Fedora Local Security Checks 20175
DISABLED Firewalls 586
STATUS PLUGIN NAME PLUGIN ID
ENABLED Debian DLA-100-1 : mutt security update 82084
ENABLED Debian DLA-1000-1 : imagemagick security update 101031
ENABLED Debian DLA-1001-1 : exim4 security update (Stack Clash) 101032
ENABLED Debian DLA-1002-1 : smb4k security update 101033
ENABLED Debian DLA-1003-1 : unrar-nonfree security update 101065
ENABLED Debian DLA-1004-1 : drupal7 security update 101092
ENABLED Debian DLA-1005-1 : mercurial security update 101121
ENABLED Debian DLA-1006-1 : libarchive security update 101173
ENABLED Debian DLA-1007-1 : icedove/thunderbird security update 101208
ENABLED Debian DLA-1008-1 : libxml2 security update 101174
ENABLED Debian DLA-1009-1 : apache2 security update 101175
ENABLED Debian DLA-101-1 : jasper security update 82085
ENABLED Debian DLA-1010-1 : vorbis-tools security update 101209
ENABLED Debian DLA-1011-1 : sudo security update 101210
ENABLED Debian DLA-1012-1 : puppet security update 101211
ENABLED Debian DLA-1013-1 : graphite2 security update 101238
ENABLED Debian DLA-1014-1 : libclamunrar security update 101239
ENABLED Debian DLA-1015-1 : libgcrypt11 security update 101274
ENABLED Debian DLA-1016-1 : radare2 security update 101275

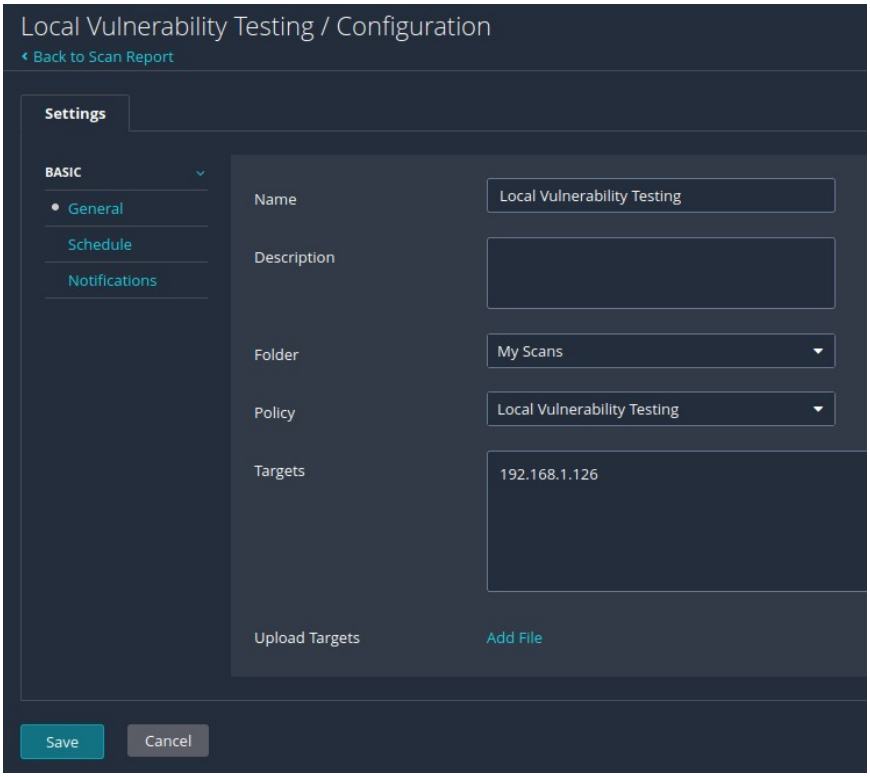
16)

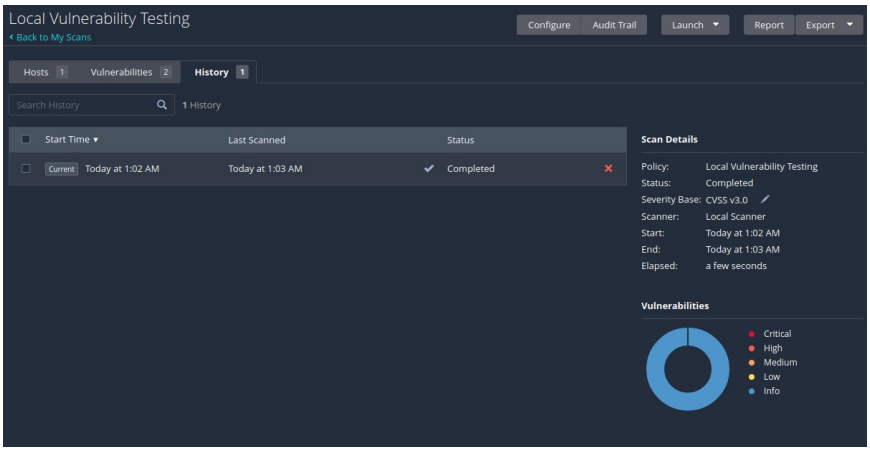

RESOURCES
Policies
Plugin Rules
Terrascan
create, import, download, edit, and delete policies.
Search Policies
3 Policies
Name
Template
Last Modified
Internal Network Scan
Advanced Scan
February 28 at 1:07 AM
Local Vulnerability Testing
Advanced Scan
February 28 at 12:59 AM
Remote Vulnerability Testing
Advanced Scan
February 28 at 1:15 AM

17)

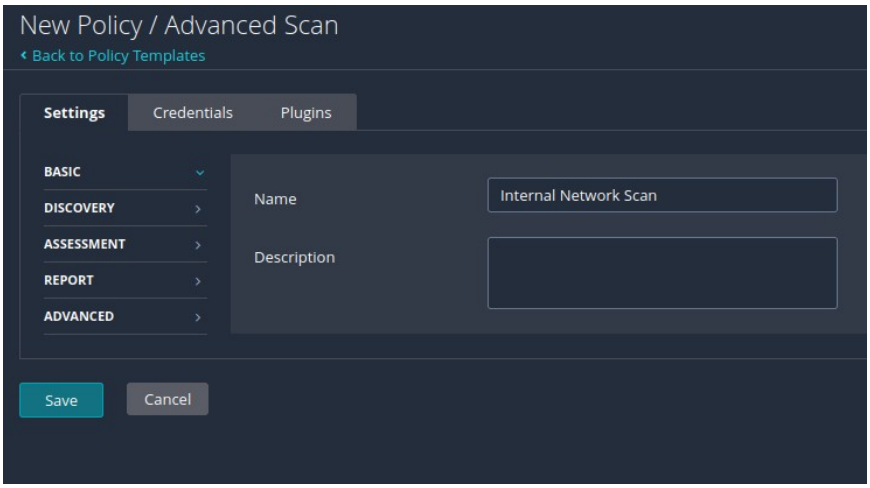

FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Scan Templates
Back to Scans
Scanner
User Defined
Internal Network Scan
A user defined policy.
Local Vulnerability Testing
A user defined policy.
Remote Vulnerability Testing
A user defined policy.

18)

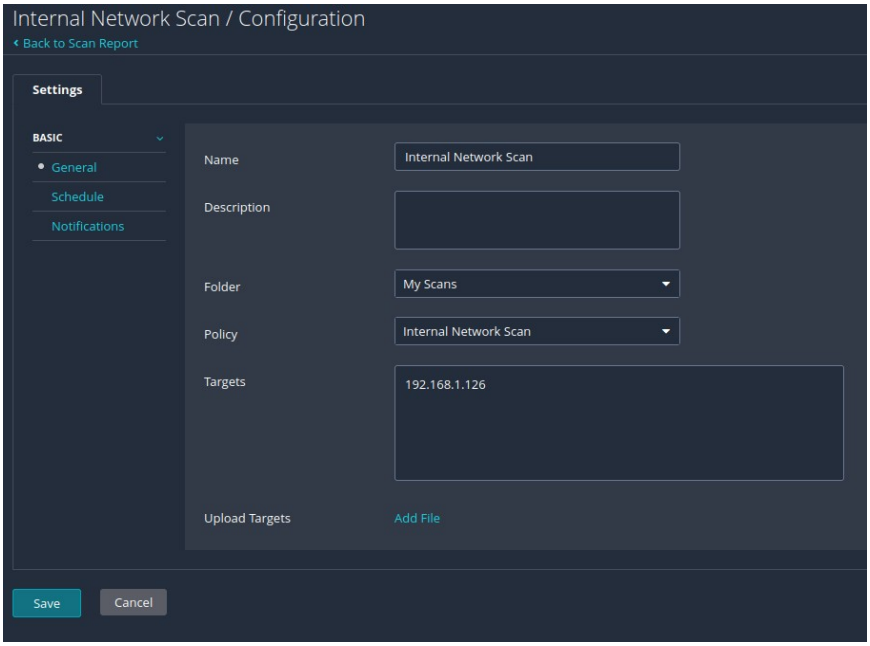

Local Vulnerability Testing / Configuration
Back to Scan Report
Settings
BASIC
General
Schedule
Notifications
Name
Local Vulnerability Testing
Description
Folder
My Scans
Policy
Local Vulnerability Testing
Targets
192.168.1.126
Upload Targets
Add File
Save
Cancel

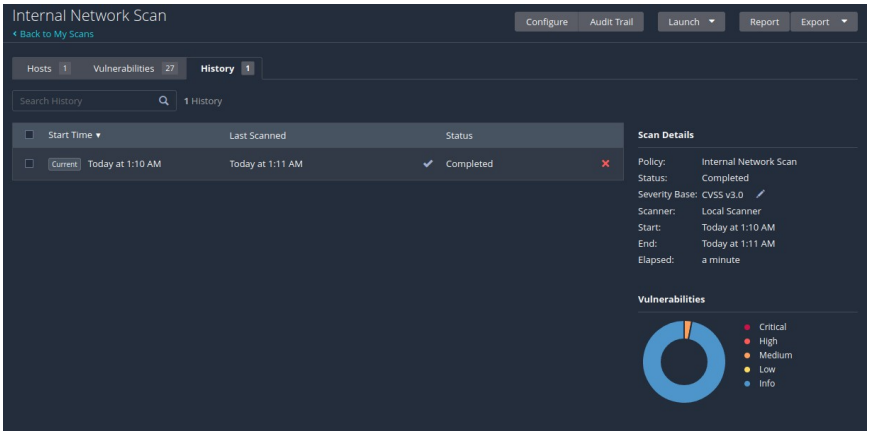

Local Vulnerability Testing
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 2
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 1:02 AM
Today at 1:03 AM
Completed
Scan Details
Policy: Local Vulnerability Testing
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:02 AM
End: Today at 1:03 AM
Elapsed: a few seconds
Vulnerabilities
Critical
High
Medium
Low
Info

19)

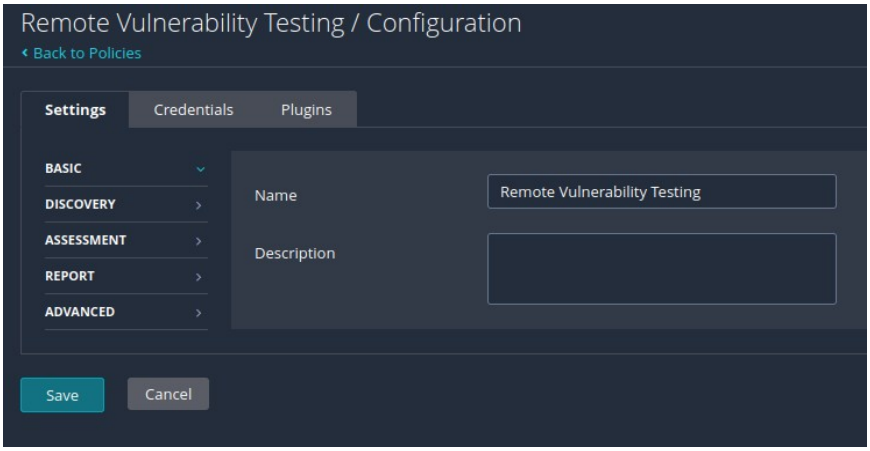

New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Internal Network Scan
Description
Save
Cancel

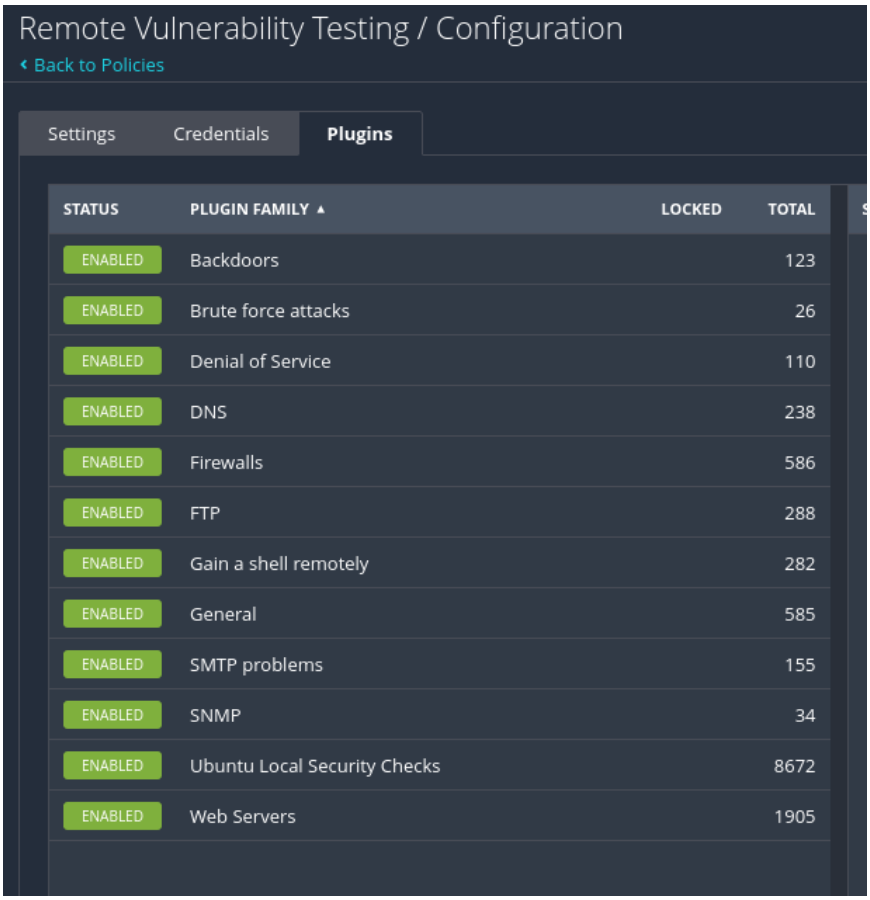

Internal Network Scan / Configuration
Back to Policies
Settings
Credentials
Plugins
STATUS
PLUGIN FAMILY
LOCKED
TOTAL
ENABLED CISCO 2517
ENABLED Default Unix Accounts 172
ENABLED DNS 238
ENABLED Firewalls 586
ENABLED FTP 288
ENABLED Gain a shell remotely 282
ENABLED General 585
ENABLED Netware 14
ENABLED Peer-To-Peer File Sharing 109
ENABLED Service detection 634
ENABLED Settings 123
ENABLED SMTP problems 155
ENABLED SNMP 34

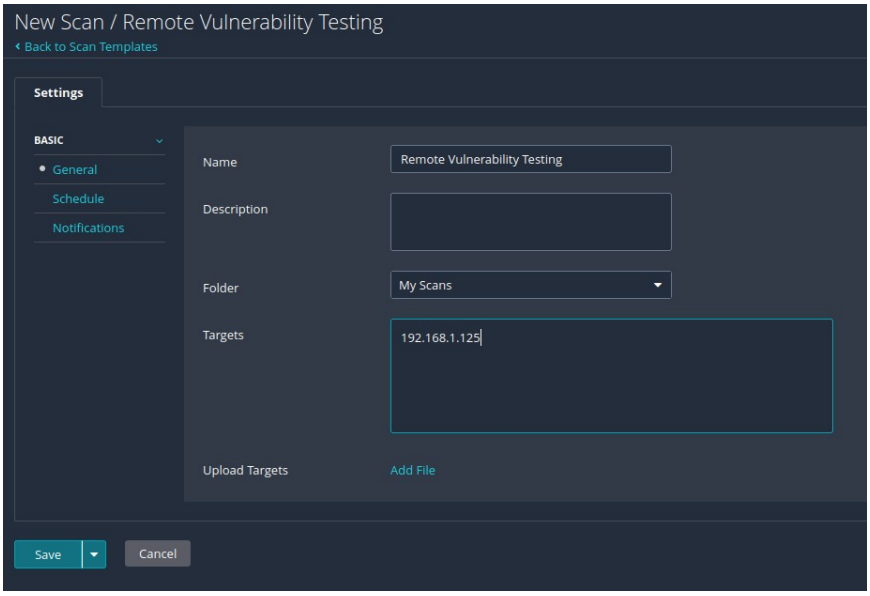

Internal Network Scan / Configuration
Back to Scan Report
Settings
BASIC
General
Schedule
Notifications
Name
Internal Network Scan
Description
Folder
My Scans
Policy
Internal Network Scan
Targets
192.168.1.126
Upload Targets
Add File
Save
Cancel

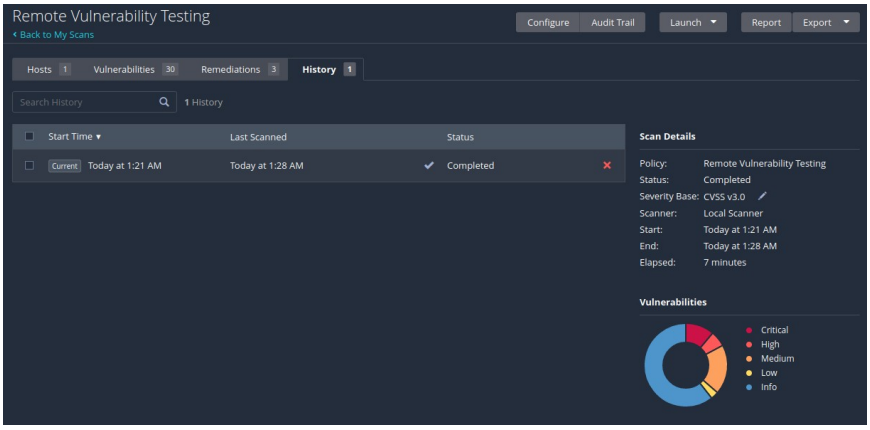

Internal Network Scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 27
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 1:10 AM
Today at 1:11 AM
Completed
Scan Details
Policy: Internal Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:10 AM
End: Today at 1:11 AM
Elapsed: a minute
Vulnerabilities
Critical
High
Medium
Low
Info

20)


Remote Vulnerability Testing / Configuration
Back to Policies
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Remote Vulnerability Testing
Description
Save
Cancel


Remote Vulnerability Testing / Configuration
Back to Policies
Settings
Credentials
Plugins
STATUS
PLUGIN FAMILY
LOCKED
TOTAL
ENABLED Backdoors 123
ENABLED Brute force attacks 26
ENABLED Denial of Service 110
ENABLED DNS 238
ENABLED Firewalls 586
ENABLED FTP 288
ENABLED Gain a shell remotely 282
ENABLED General 585
ENABLED SMTP problems 155
ENABLED SNMP 34
ENABLED Ubuntu Local Security Checks 8672
ENABLED Web Servers 1905


New Scan / Remote Vulnerability Testing
Back to Scan Templates
Settings
BASIC
General
Schedule
Notifications
Name
Remote Vulnerability Testing
Description
Folder
My Scans
Targets
192.168.1.125
Upload Targets
Add File
Save
Cancel


Remote Vulnerability Testing
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 30
Remediations 3
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 1:21 AM
Today at 1:28 AM
Completed
Scan Details
Policy: Remote Vulnerability Testing
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:21 AM
End: Today at 1:28 AM
Elapsed: 7 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

Part 2 Questions

1) Compare the reports from step 12 and step 20, and state your findings.

The “Basic Network Scan” from step 12 shows a total of 120 vulnerabilities. Of the 120 vulnerabilities, 8 are critical, 8 are high, and 18 are medium. The “Remote Vulnerability Testing” scan from step 20 shows a total of 63 vulnerabilities, of which there are 7 critical, 4 high, and 12 medium. From these two reports, it seems that Metasploitable 2 Linux is especially vulnerable when it comes to remote access, as the only critical vulnerability found in the “Basic Network Scan” and not in the “Remote Vulnerability Testing” is “SSL Version 2 and 3 Protocol Detection.” While I was initially surprised by this overlap, it began to make sense as Metasploitable 2 Linux is purposefully designed to be vulnerable to attacks and most attacks have to occur over a network.

2) Compare the reports from step 18 and step 19, and state your findings.

From the “Local Vulnerability Testing” and “Internal Network Scan” results, it is not surprising to see that Kali Linux has no critical or high vulnerabilities, and only 1 medium in the “Internal Network Scan” report which is “SSL Certificate Cannot Be Trusted.” Since Kali Linux has such an emphasis on security, the lack of vulnerabilities is expected. In the “Internal Network Scan” report, the other 35 vulnerabilities are all in the “info” severity which seems unavoidable as a device connected to a network. Most of the “info” vulnerabilities seem related to accessible information like the device type, hostname, running processes information, and connection information.

Reflection

a) What is the purpose of the lab in your own words?

To me, this lab was meant for us to become exposed to the practice of fingerprinting and scanning devices other than our own on a network. While we had 2 virtual machines running, almost all of the information for both machines was done on Kali using the IP address of Metasploitable 2. The interactions we did with Nmap got us information via fingerprinting on the Metasploitable 2 machine such as it's operating system, the versions of different software it has, and the ports it has open, while our use of Nessus gave us full reports on the vulnerabilities each of the two systems had.

b) What did you learn? Did you achieve the objectives?

In full honesty, I did not realize you could run multiple virtual machines at the same time. So at the very beginning I learned that you can run Metasploitable 2 and Kali at the same time! In terms of network mapping and scanning, I learned how to fingerprint devices on a network using Nmap along with what kind of information is available when you are fingerprinting a device. I was aware that the operating system is available to see, however what surprised me was seeing a full list of the ports that are open along with what specific version of software a device on the network is running, such as ssh, telnet, and MySQL. I also learned how to use Nessus for performing scans and generating a report of vulnerabilities found on a target IP address. I believe that I achieved the objectives of the lab, and am already planning on running scans on some of my personal devices to see what kinds of information I can now gather.

c) From the defense point of view, why is it important to close unused services/ports and patch your system/software in a timely manner?

Unused services and ports along with unpatched systems and software pose as a massive threat to the security of a device. Ports that are open serve as a potential way into the system from an outside device on the network that can easily be avoided by closing the services and/or ports when not being used. Out of date systems and software serve as possibilities for a system to become compromised as time goes on since bad actors will work with outdated or unpatched software to discover vulnerabilities and develop methods to exploit said vulnerabilities. By updating your operating system and applications regularly, the identified vulnerabilities are fixed, lowering the risk of your system being compromised.

d) Is this lab hard or easy? Are the lab instructions clear?

While time consuming, this lab was not overly difficult due to the instructions being clear and concise. There was a slight learning curve to using Nessus as I had never used the software before, however once I became familiar with the UI and the different menus presented I was able to run the scans fairly easily.

e) What do you think about the tools used? What worked? What didn't? Are there other better alternatives?

What surprised me the most was how not technically demanding the tools used in this lab are. Nmap required using the terminal, but it's commands are not overly difficult and we are able to gain more information that I though with few to none additional parameters. The same goes for Nessus, where the only information needed was the IP address of a target system. I had always assumed these tools would have a high barrier to entry, but to my surprise they all worked as intended with a lower learning curve than expected. From what I have seen, there are alternatives to both Nmap and Nessus, however I don't see a particular reason to use the alternatives as they don't appear to offer "better" results, just different methods to gain the same information.

f) Other feedback

I very much enjoyed this lab, it seemed to be a well thought out introduction to what Metasploitable 2 Linux, Nmap, and Nessus are as well as how to start using Nmap and Nessus as the tools they are. I am hoping that we get to use Nmap and Nessus more in depth as I'm guessing we have only scratched the surface of their functionality.