

Defensive Security 1 (INF070243)

Assignment 4

Pen Testing Assignment



Uthaya Krishnan
Id : 991805820
Sheridan College

Vulnerability assessment with Nessus

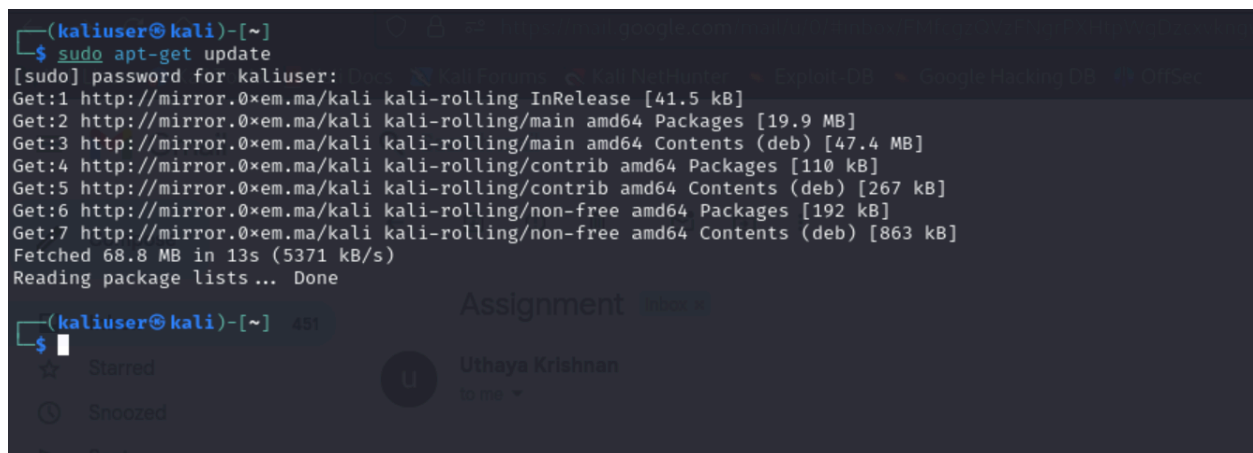
Objective :

To perform a vulnerability assessment using the Nessus tool. The objective is the process of setting up Nessus on a Linux system, conducting a network vulnerability scan, and generating a report based on the findings.

Pre-lab configuration

Task1: Updating Linux Machine (kali Linux used here)

```
(kaliuser@kali)-[~]
$ sudo apt-get update
[sudo] password for kaliuser:
Get:1 http://mirror.0xem.ma/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.0xem.ma/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:3 http://mirror.0xem.ma/kali kali-rolling/main amd64 Contents (deb) [47.4 MB]
Get:4 http://mirror.0xem.ma/kali kali-rolling/contrib amd64 Packages [110 kB]
Get:5 http://mirror.0xem.ma/kali kali-rolling/contrib amd64 Contents (deb) [267 kB]
Get:6 http://mirror.0xem.ma/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://mirror.0xem.ma/kali kali-rolling/non-free amd64 Contents (deb) [863 kB]
Fetched 68.8 MB in 13s (5371 kB/s)
Reading package lists... Done
```

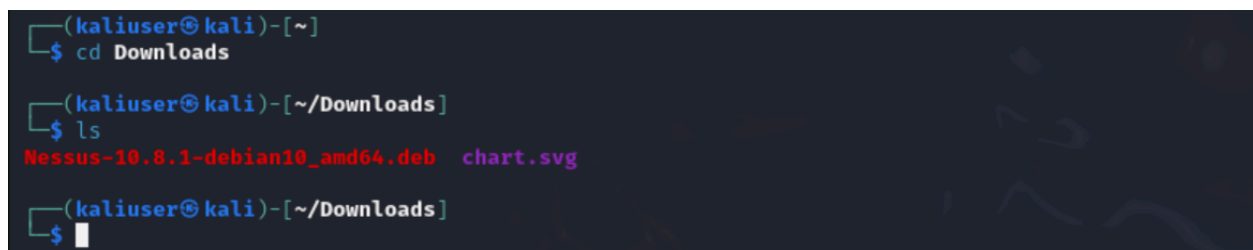


Task3 : Verifying the downloads folder for Nessus tool installer

```
(kaliuser@kali)-[~]
$ cd Downloads

(kaliuser@kali)-[~/Downloads]
$ ls
Nessus-10.8.1-debian10_amd64.deb  chart.svg

(kaliuser@kali)-[~/Downloads]
$
```



Task 4: Install the Nessus into the box using “sudo dpkg -i” command

```
(kaliuser@kali)~[~/Downloads]
$ sudo dpkg -i Nessus-10.8.1-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 391438 files and directories currently installed.)
Preparing to unpack Nessus-10.8.1-debian10_amd64.deb ...
Unpacking nessus (10.8.1) ...
Setting up nessus (10.8.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
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
```

Task: Vulnerability as
Pre-lab configuration
1) Make sure you
2) Check your in
3) Update your t
4) You need to h
school's one o
Lab
1) Use any web t
<https://www.>
code
This is the pag
address in ord
your email ad
2) Then go to th
[your-operatin](#)
8 / Kali Linux
favorite Linux
3) Open up a ter
1 mark
4) Use your own
install Nessus
it" is the comm
5) Check the stat
status" (take
6) Now start the
screenshot) -
7) Now go back t
web interface
port for the w

Task 5: Check the status of the service with “systemctl” command

```
(kaliuser@kali)~[~/Downloads]
$ sudo systemctl status nessusd
o nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: inactive (dead)

(kaliuser@kali)~[~/Downloads]
$
```

box(Metas
terminal at
eth0 interf
record you

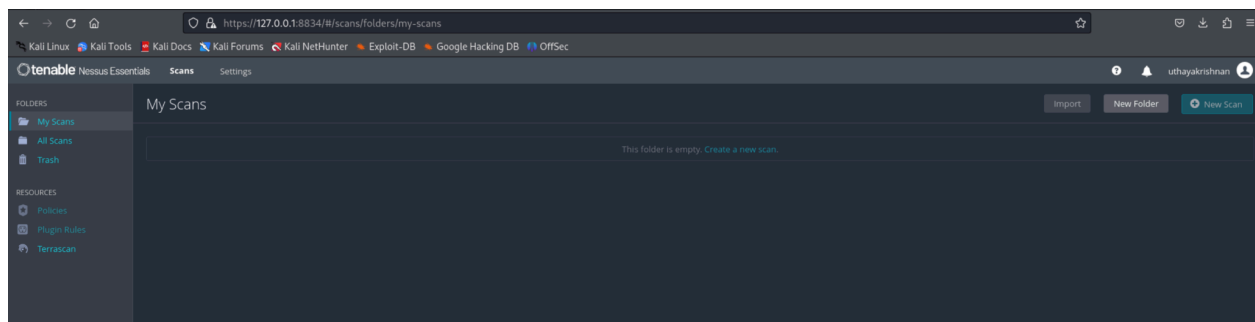
Task 6: Start the Nessus service

```
(kaliuser@kali)-[~/Downloads]
$ sudo systemctl start nessusd

(kaliuser@kali)-[~/Downloads]
$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sun 2024-08-11 19:18:47 EDT; 50s ago
     Main PID: 33718 (nessus-service)
        Tasks: 15 (limit: 4084)
      Memory: 111.9M (peak: 112.2M)
         CPU: 36.547s
       CGroup: /system.slice/nessusd.service
              └─33718 /opt/nessus/sbin/nessus-service -q
                 └─33721 nessusd -q

Aug 11 19:18:47 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Aug 11 19:18:49 kali nessus-service[33721]: Cached 0 plugin libs in 14msec
Aug 11 19:18:49 kali nessus-service[33721]: Cached 0 plugin libs in 0msec
```

Task 9: Logged into the Nessus web portal to check the site is up



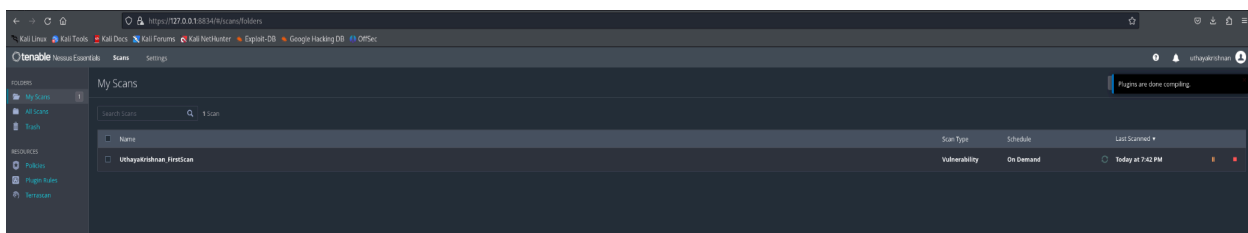
Task 10: Network Interface of the target machine (kali Linux)

```
(kaliuser@kali)-[~/Downloads]
$ sudo ifconfig -a
[sudo] password for kaliuser:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.7 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:febb:f7ef prefixlen 64 scopeid 0<x20<link>
    ether 08:00:27:bb:f7:ef txqueuelen 1000 (Ethernet)
    RX packets 491063 bytes 722773661 (689.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 44471 bytes 7556436 (7.2 MiB)
    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<x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 25284 bytes 10782636 (10.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25284 bytes 10782636 (10.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kaliuser@kali)-[~/Downloads]
$
```

Task 14: Start the scan against target IP 10.0.2.0/24



Task 15: The list of Hosts that are scanned



The list of Vulnerabilities found as a result of scan

Critical and High severity vulnerabilities found in the Host 10.0.2.7

The screenshot shows the 'Uthayakrishnan_FirstScan' interface with the 'Vulnerabilities' tab active. The table lists the following vulnerabilities found on host 10.0.2.7:

Severity	CVEs	VPR	EPSS	Name	Family	Count
Critical				Node.js Node.js (Multiple Issues)	Node.js	4
Critical	5.3			SMB Signing not required	MS-SCN	1
Critical				SSL (Multiple Issues)	General	8
Critical				Apache Tomcat (Multiple Issues)	Web Servers	2
Critical				Intel Media SDK (Multiple Issues)	MS-SCN	2
High	3.3.1			DHCP Server Detection	Service Detection	1
High				HTTP (Multiple Issues)	Web Servers	6
High				SQL (Multiple Issues)	General	6
High				SSH (Multiple Issues)	Windows	5
High				TLS (Multiple Issues)	Service Detection	4
High				Apache HTTP Server (Multiple Issues)	Web Servers	2
High				Microsoft Windows (Multiple Issues)	Windows	2
High				OSCE Services Enumeration	Windows	8
High				Nessus SSH Scanner	Port Scanners	7
High				Service Detection	Service Detection	5
High				Ethernet MAC Addresses	General	4
High				Nessus Scan Information	Settings	4
High				Device Type	General	3
High				OS Identification	General	3
High				Transcode Information	General	3
High				Common Platform Enumeration (CPE)	General	2
High				DNS Server Detection	DNS	2
High				Ethernet Card Manufacturer Detection	MS-SCN	2
High				IPv6 / QoS (Guard Detection unimplemented checks)	MS-SCN	2
High				Nessus Server Detection	Service Detection	2
High				OpenSSH (Multiple Issues)	General	2

Conclusion

The penetration test conducted on this environment has revealed several vulnerabilities that could potentially be exploited by malicious actors. Among these, critical vulnerabilities include insecure configurations, lack of encryption, and outdated software were identified as the most critical.

In addition to the high-severity issues, a number of medium and low-severity vulnerabilities were also discovered, indicating opportunities for further strengthening the security posture of the environment.

These weaknesses could lead to unauthorized access, data breaches, or service disruptions if left unaddressed.

