Defensive Security 1 (INFO70243)

Assignment 4

Pen Testing Assignment

Uthaya Krishnan
Id : 991805820
Sheridan College

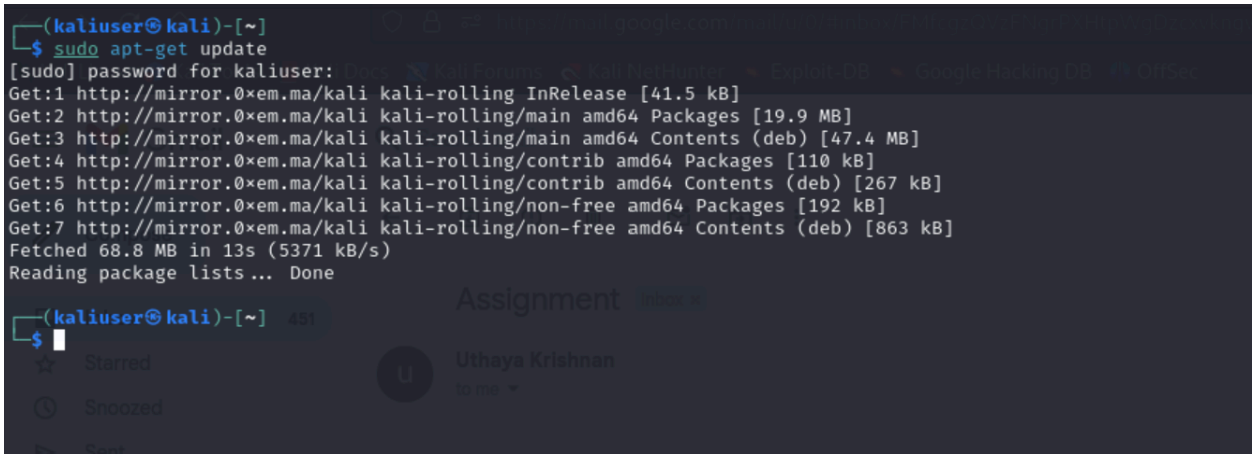
Vulnerability assessment with Nessus

Objective :

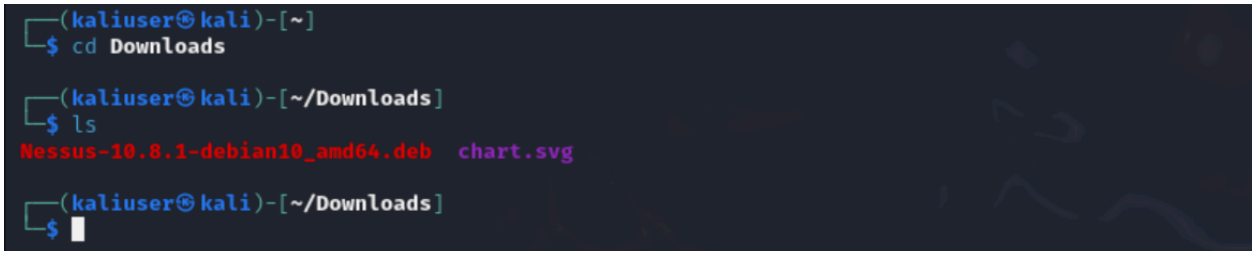
To perform a vulnerability assessment using the Nessus tool. The objective is the process of setting up Nessus on a Linux system, conducting a network vulnerability scan, and generating a report based on the findings.

Pre-lab configuration

Task1: Updating Linux Machine (kali Linux used here)



Task3 : Verifying the downloads folder for Nessus tool installer



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
```

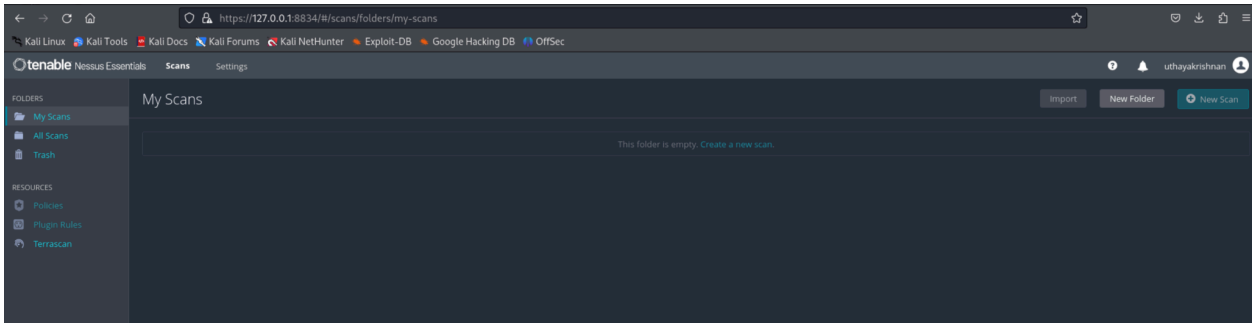
Task 5: Check the status of the service with “systemctl” command

```
┌──(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: inactive (dead)

┌──(kaliuser㉿kali)-[~/Downloads]
└─$
```

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)

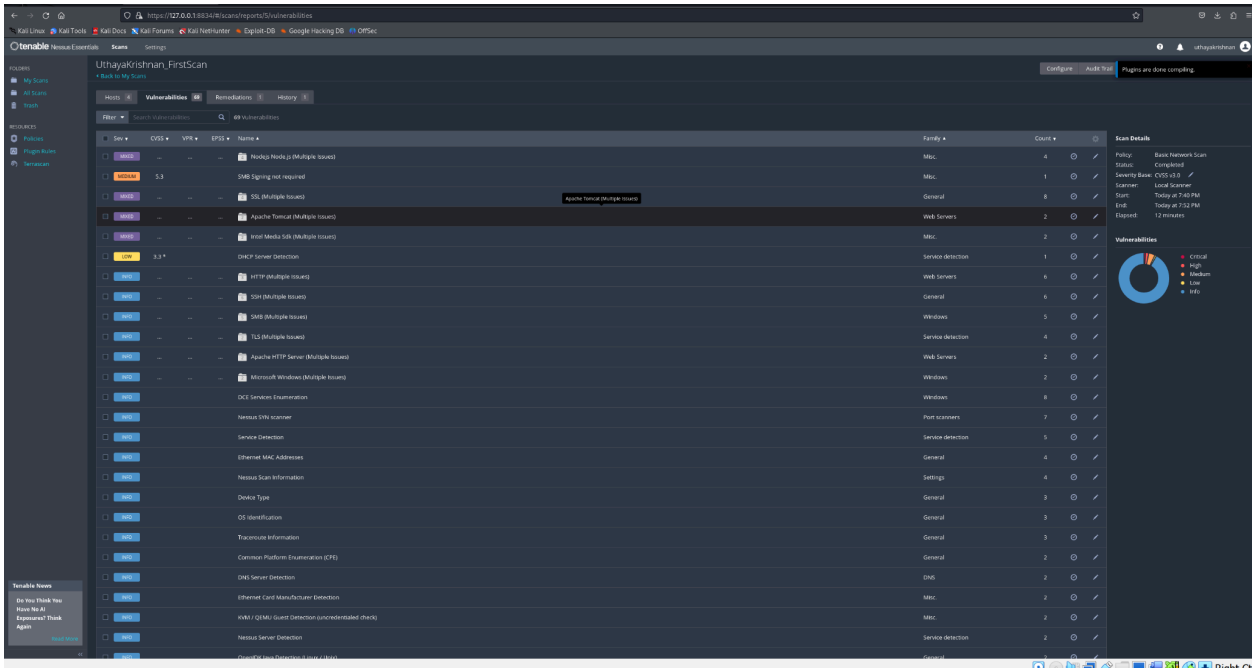
```
┌──(kaliuser㉿kali)-[~/Downloads]
└─$ sudo ifconfig -a
[sudo] password for kaliuser:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.7  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:febb:f7ef  prefixlen 64  scopeid 0x20<link>
        ether 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 0x10<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



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.