Threat management and cybersecurity Resources

Key contributors:
Devon Brown
Daniel Garza
Candan Martin

April/26/2022

Executive Summary

The purpose of this project is to test the efficiency of detecting vulnerabilities using OpenVAS, Nessus, and Metasploit. We used 3 different operating systems Metasploitable, Fedora, and CentOS to test the efficiency of our vulnerability assessment tools. We used Metasploitable for its numerable vulnerabilities as our baseline least secure system. We used Fedora because it is used to host servers so we wanted to see how secure the system would be. We used CentOS because it is widely used by scientists, so we wanted to compare its security to Fedora and Metasploitable. Candan will be using Nessus, Devon will be using OpenVAS, and Daniel will be using Metasploit.

We focused on Metasploitable because we knew that we would be able to find vulnerabilities so, we wanted to compare how effective Nessus, OpenVAS, and Metasploit would be on an insecure system. This was done so we can understand how the vulnerability assessments tools worked, how they would display the vulnerabilities, and how this software would provide solutions when vulnerabilities were found.

<u>These are the results that we got:</u>

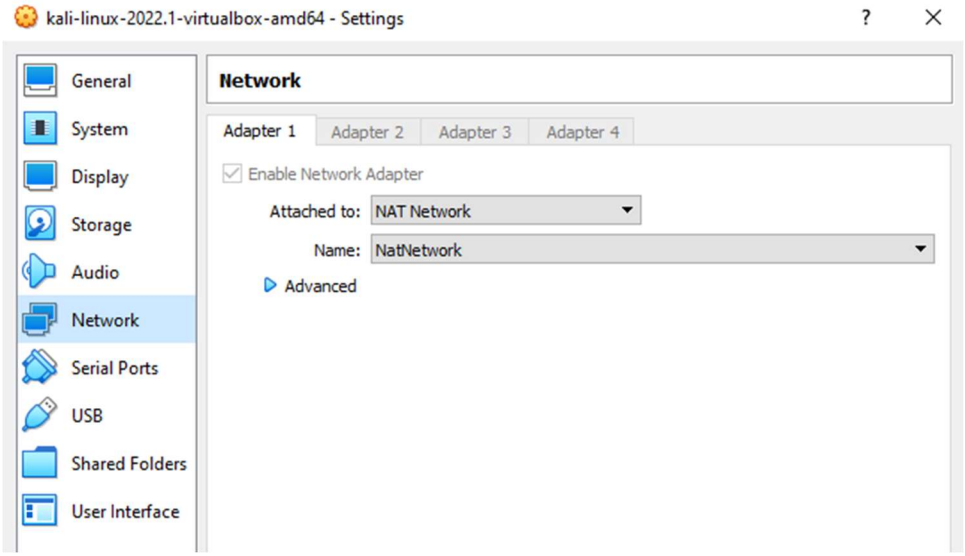
OpenVAS:

Intro: Devon used OpenVAS to scan metasploitable using its ip and find any vulnerabilities. Next, Devon located the reports page and exported a xml of the report.

Experimental Procedure:

It consists of 11 steps

1. Set-up NAT Network within planned VMs. Connect VMs to NAT network



2. Download and configure OpenVAS on Kali Linux

Use command : sudo apt-get update

sudo apt-get dist-upgrade

3. Start target OS and run command ifconfig to get the ip address.

4. ping target ip within kali to make sure they are connected on NAT Network.

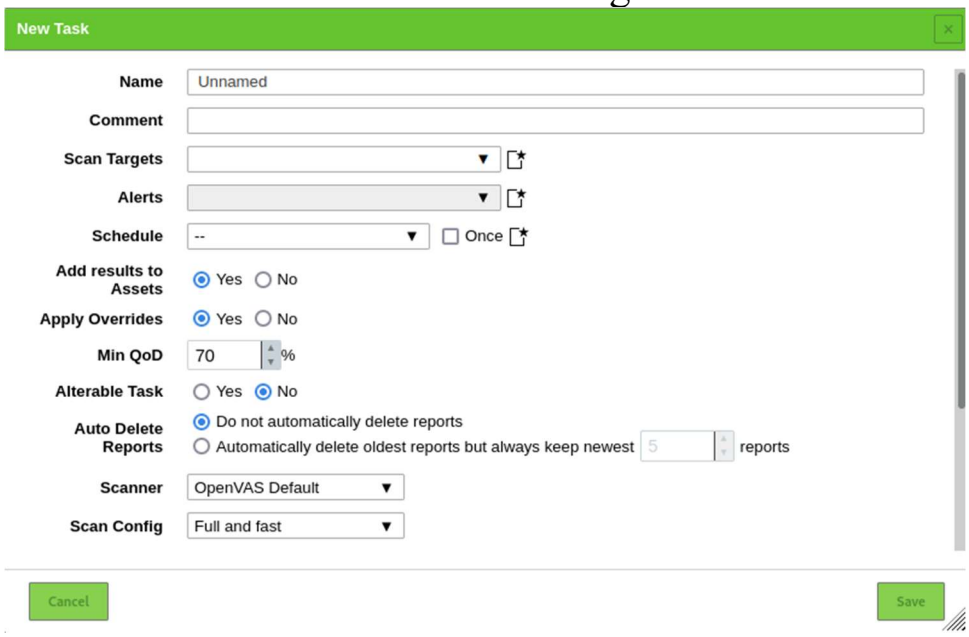
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.139.132                                          130 ×
PING 192.168.139.132 (192.168.139.132) 56(84) bytes of data.
64 bytes from 192.168.139.132: icmp_seq=1 ttl=64 time=15.5 ms
64 bytes from 192.168.139.132: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 192.168.139.132: icmp_seq=3 ttl=64 time=1.79 ms
64 bytes from 192.168.139.132: icmp_seq=4 ttl=64 time=1.47 ms
64 bytes from 192.168.139.132: icmp_seq=5 ttl=64 time=1.32 ms
64 bytes from 192.168.139.132: icmp_seq=6 ttl=64 time=1.80 ms
```

5. Get password from initial configuration and start OpenVAS. Start OpenVAS with sudo gvm-start.

```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-start
[*] Please wait for the GVM / OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● greenbone-security-assistant.service - Greenbone Security Assistant (gsad)
     Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)
     Active: active (running) since Fri 2021-02-12 12:24:11 UTC; 43ms ago
       Docs: man:gsad(8)
             https://www.greenbone.net
    Process: 33117 ExecStart=/usr/sbin/gsad --listen=127.0.0.1 --port=9392 (code=exited, status=0/SUCCESS)
   Main PID: 33118 (gsad)
      Tasks: 1 (limit: 4546)
     Memory: 1.7M
     CGroup: /system.slice/greenbone-security-assistant.service
             └─33118 /usr/sbin/gsad --listen=127.0.0.1 --port=9392

Feb 12 12:24:11 kali systemd[1]: Starting Greenbone Security Assistant (gsad)...
Feb 12 12:24:11 kali gsad[33117]: Oops, secure memory pool already initialized
Feb 12 12:24:11 kali systemd[1]: Started Greenbone Security Assistant (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; vendor preset: disabled)
     Active: active (running) since Fri 2021-02-12 12:24:06 UTC; 5s ago
       Docs: man:gvmd(8)
    Process: 33071 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock (code=exited, status=0/SUCCESS)
   Main PID: 33073 (gvmd)
      Tasks: 2 (limit: 4546)
     Memory: 3.1M
     CGroup: /system.slice/gvmd.service
```

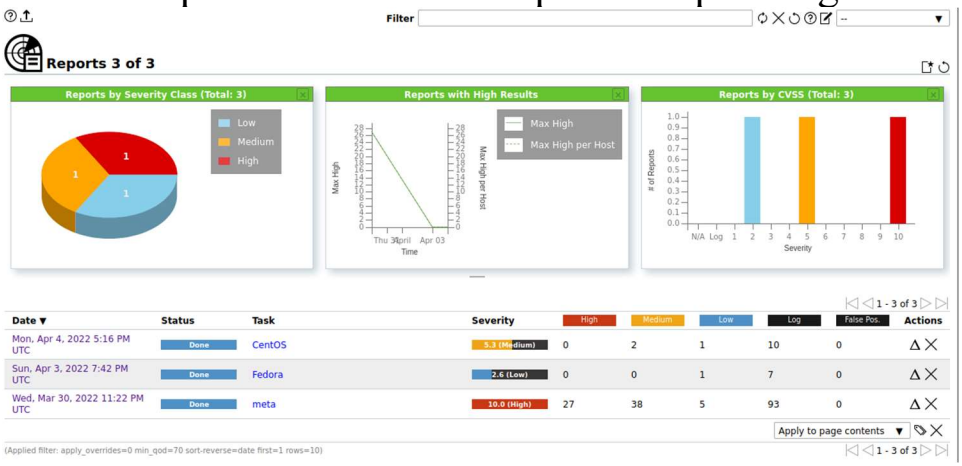
6.Login with admin and the provided password.

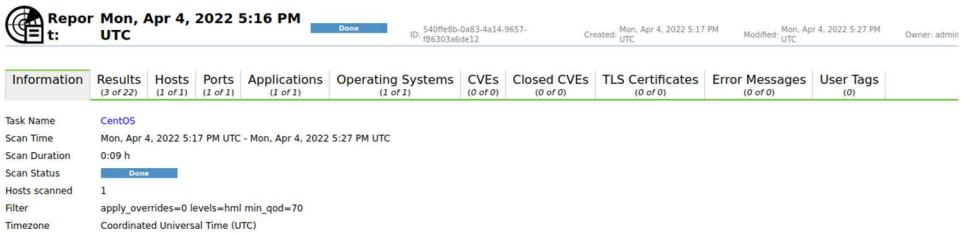
7. Select new task and enter the target OS details.



8. save task then click the arrow to run a scan.

9. Go to reports and select the specific report to get details on the scan.





10. Download report for the OS scan and upload onto GIthub
11. repeat steps 3-4 and 7-10 for each target OS

OpenVAS Report Results:

Metasploitable

Fedora

CentOS

Full Report on Git-Hub. Go to the links on the ***Project Management*** *page*

Nessus:

Intro:

Candan used the Nessus vulnerability assessment tool to scan Metasploitable's IP address and identify vulnerabilities in Metasploitable's operating system. After scan, Nessus provided insight on the vulnerabilities found and Candan generated it's general report

Experimental Procedure:

- It consists of 11 steps

Step 1.

Use ifconfig command in Metasploitable to identify IP address for metasplotable. Fig 1.1

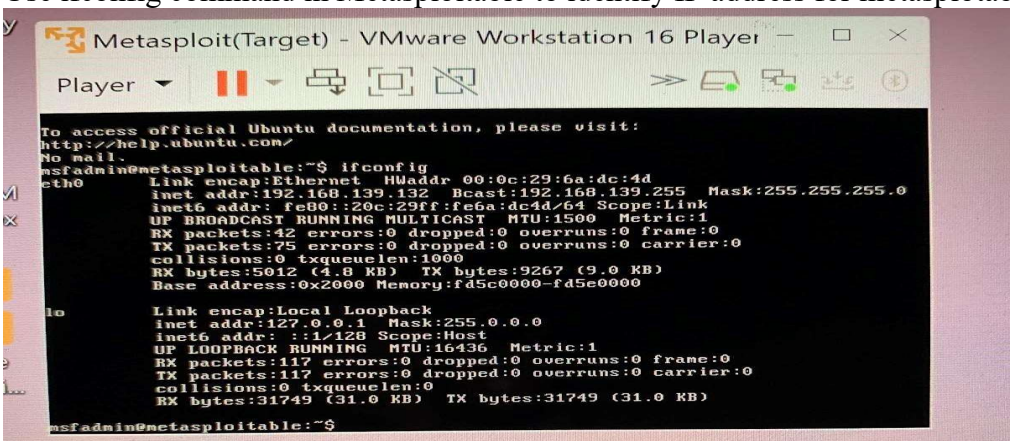


Fig 1.1

Metasploitable ip address is displayed

Step 2:

Open Kali Linux terminal and use command "ping " to check for a connection from metasploitable our target machine. Fig 1.2

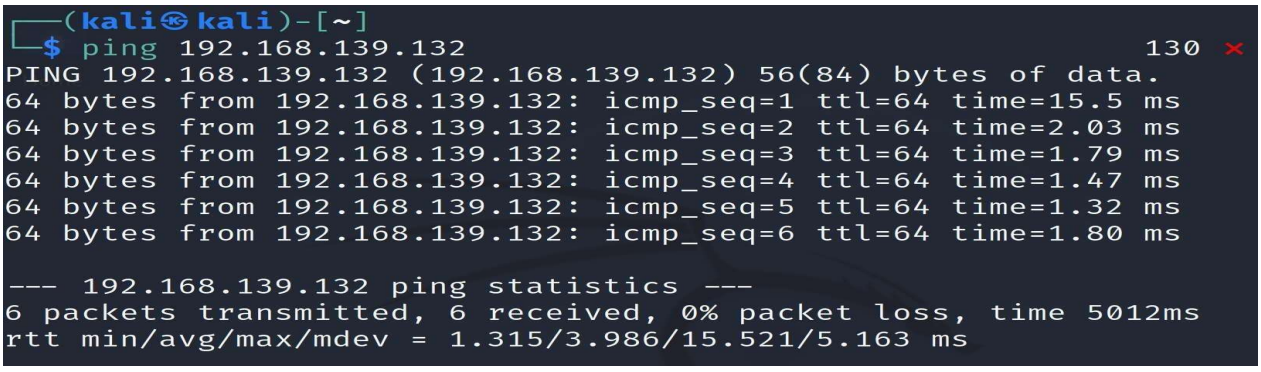


Fig 1.2

Step 3.

Open the Nessus application in the Kali Linux VM.

Step 4.

Perform a scan with Nessus on the target VM. Provide screenshots and explain thoroughly each step.

Step 5.

Selected Basic Network Scan. Fig 1.3

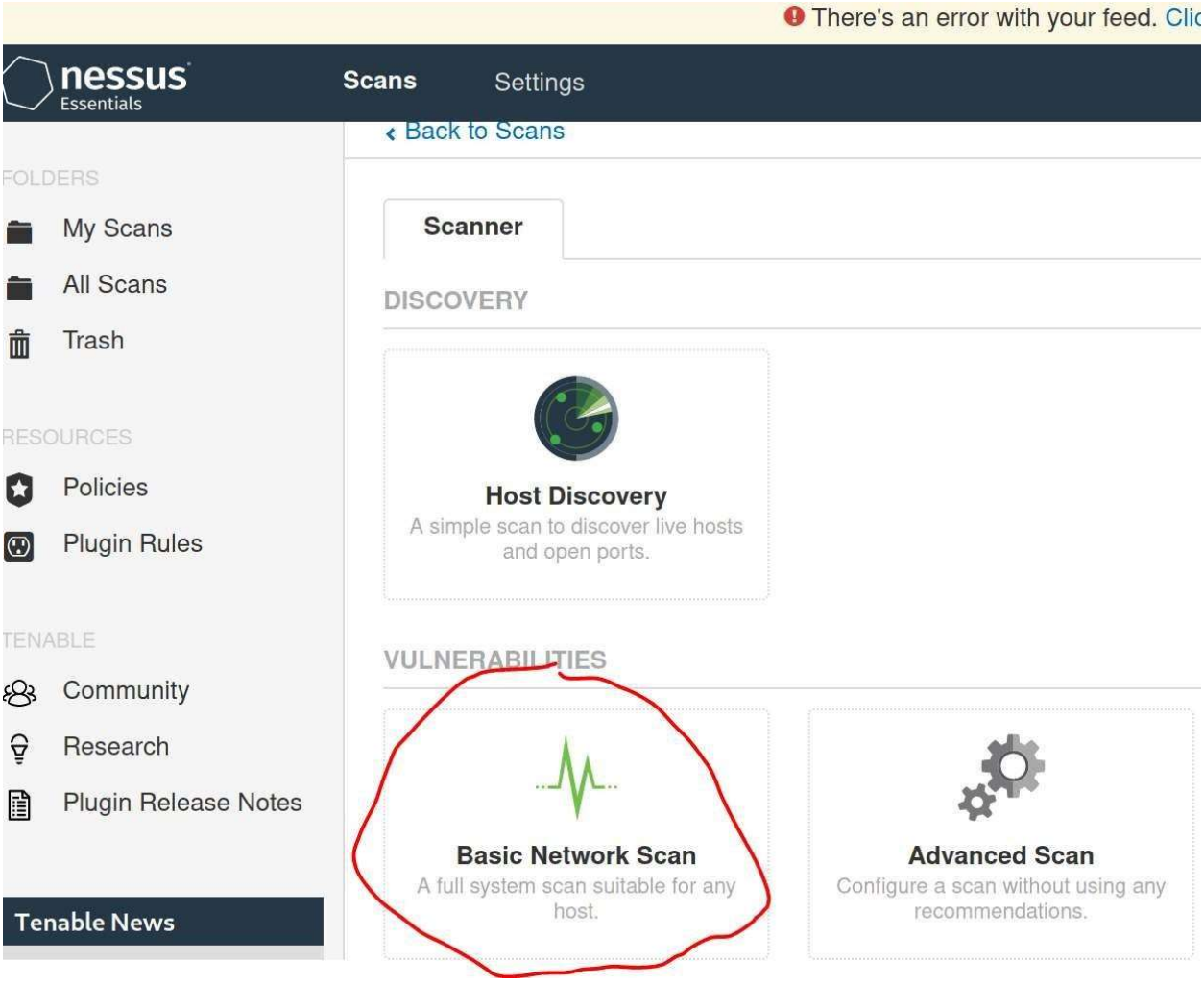


Fig 1.3

Step 6.

Name the target OS. Make a description of target. Input target IP address into “Targets”. Save the scan. Fig 1.4

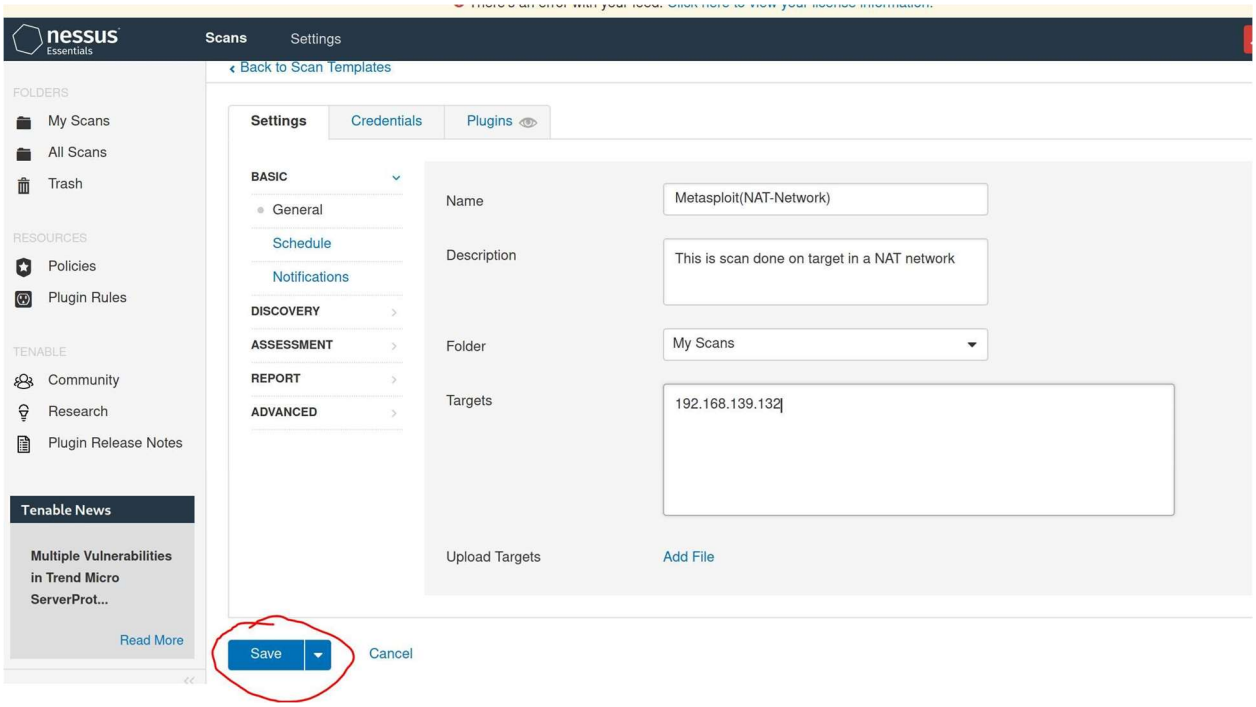


Fig 1.4

Step 7.

Find scan that was created and select the play button to launch scan. This will tell Nessus to start the scan on the target OS(Metasploitable). Fig 1.5

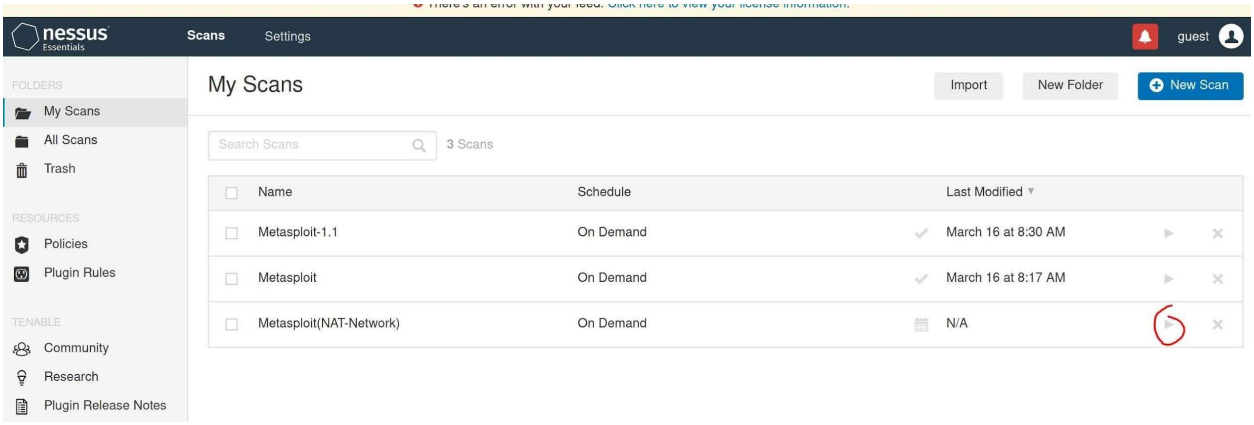


Fig 1.5

Step 8.

Wait for the scan to complete. Fig 1.6

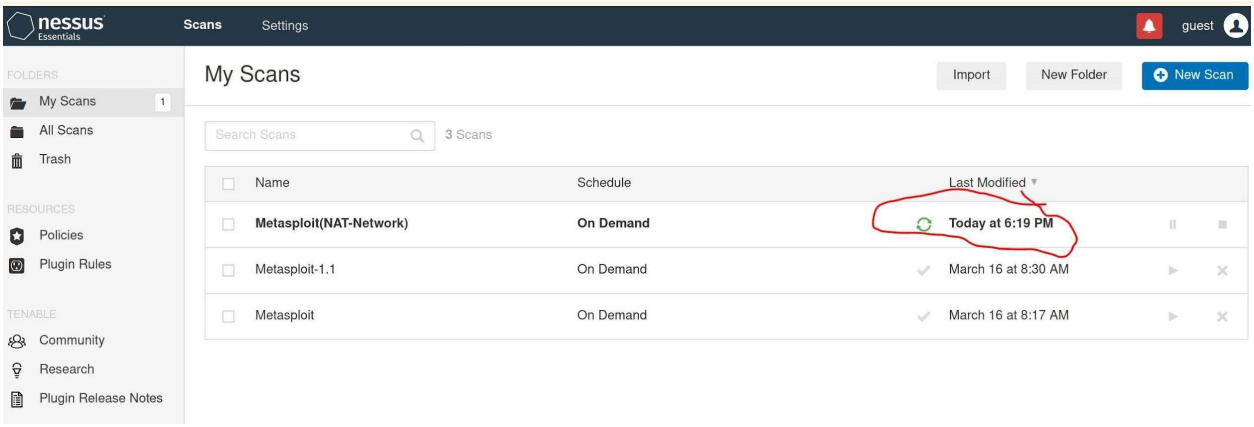


Fig 1.6

Step 9.

Click on the Metasploit(NAT-Network) file created to view the scan

Step 10.

Select the vulnerabilities tab to view vulnerabilities found. Fig 1.7

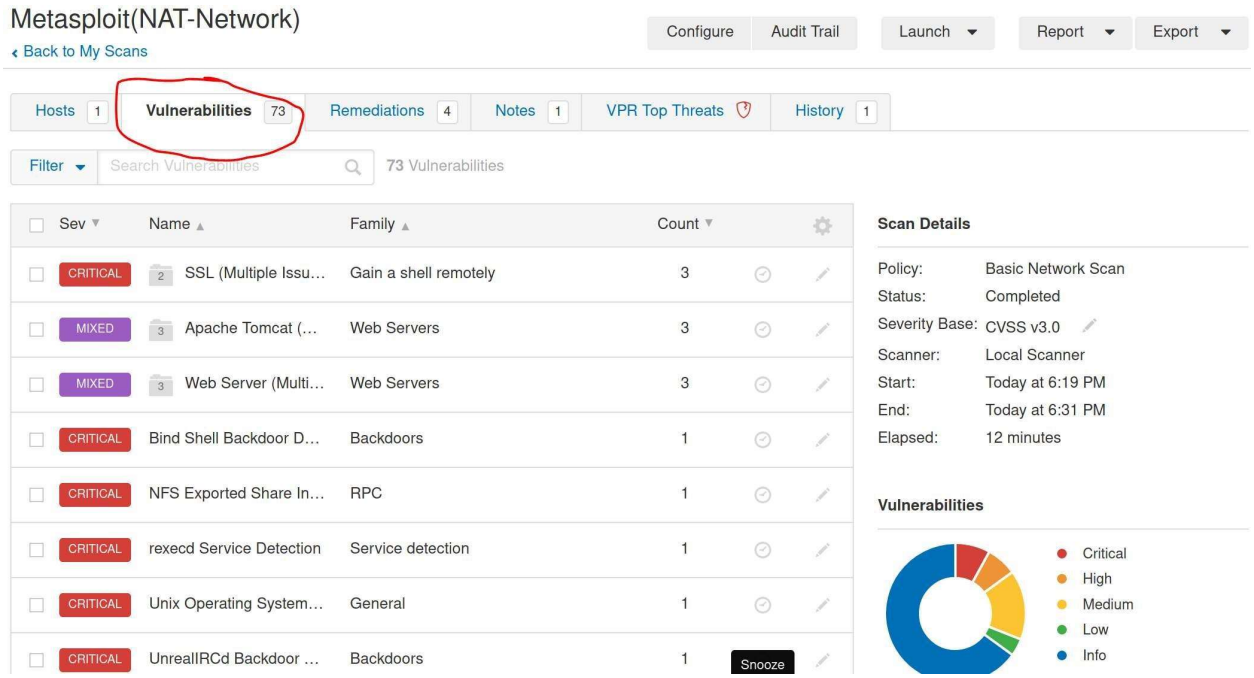


Fig 1.7

Step 11.

Download the generated report from Nessus. Select Report□PDF and then generate with the default Executive summary selected. Fig 1.8

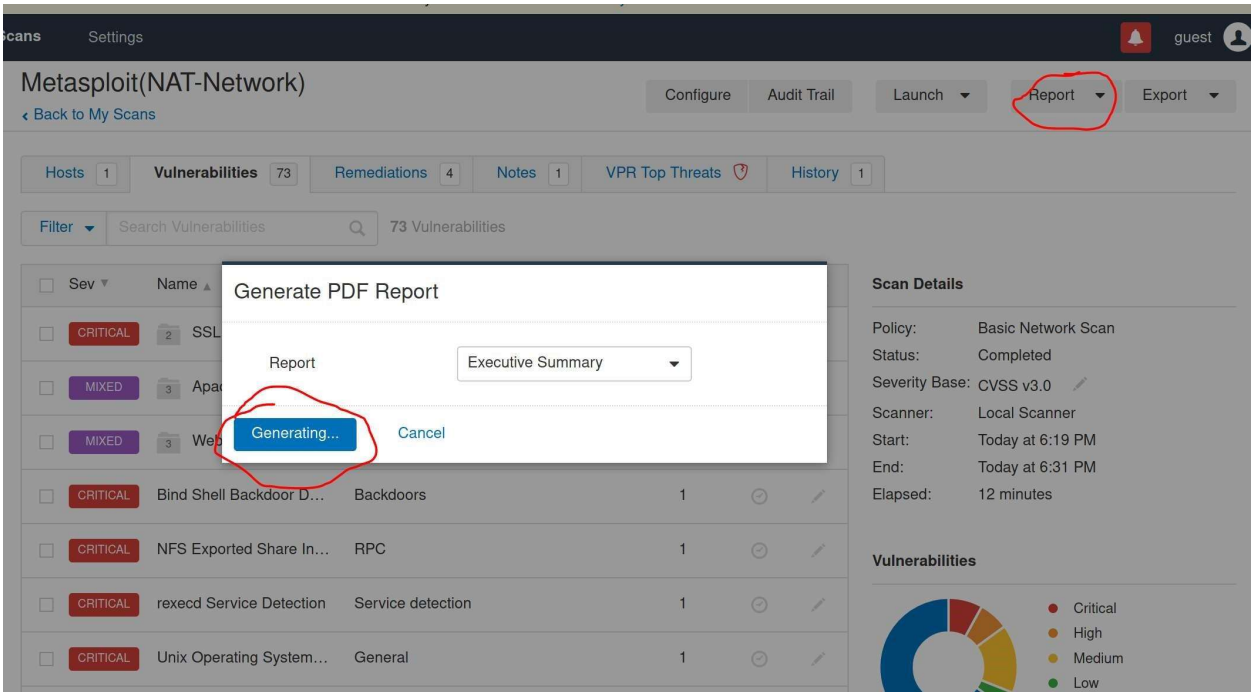
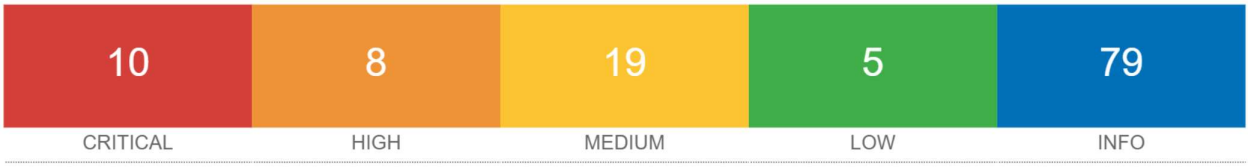

Scans
Settings
guest
Metasploit(NAT-Network)
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 73
Remediations 4
Notes 1
VPR Top Threats
History 1
Filter
Search Vulnerabilities
73 Vulnerabilities
Sev
Name
Generate PDF Report
Report
Executive Summary
Generating...
Cancel
CRITICAL
SSL
MIXED
MIXED
CRITICAL
Bind Shell Backdoor D…
Backdoors
1
CRITICAL
NFS Exported Share In…
RPC
1
CRITICAL
rexecd Service Detection
Service detection
1
CRITICAL
Unix Operating System…
General
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:19 PM
End: Today at 6:31 PM
Elapsed: 12 minutes
Vulnerabilities
Critical
High
Medium
Low

Fig 1.8

Nessus Report Results:

Metasploitable

192.168.139.132



CentOS

192.168.139.136

Fedora

192.168.139.133

*Full Report on Git-Hub. Go to the links on the **Project Management** page*

Metasploit:

First released in 2003, Metasploit is widely known as one of the most impactful Vulnerability Assessment Scanners(VAS). Like many other open source softwares, it was subject to the creation of many front-end GUIs. One such GUI, Armitage, was released in 2015. Armitage is useful in that it heightens ease of use in Metasploit and provides a user friendly platform for new users to launch from.

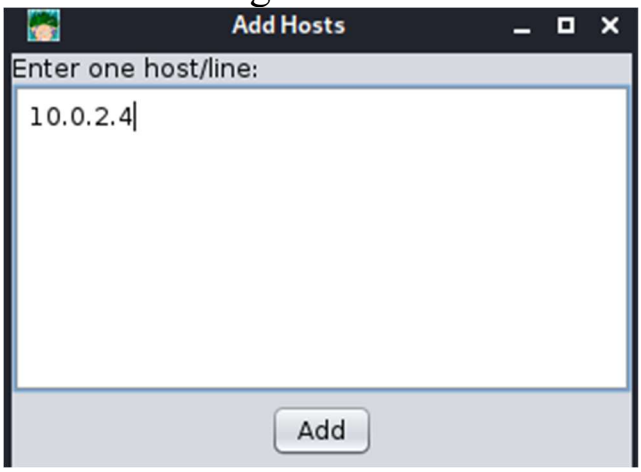
The process consists of 5 steps. The following screenshots depict an Armitage scan of a Metasploitable machine on the same NAT Network.

Step 1. Ensure that target and host machines are on NAT network

Step 2. Determine IP of target machine

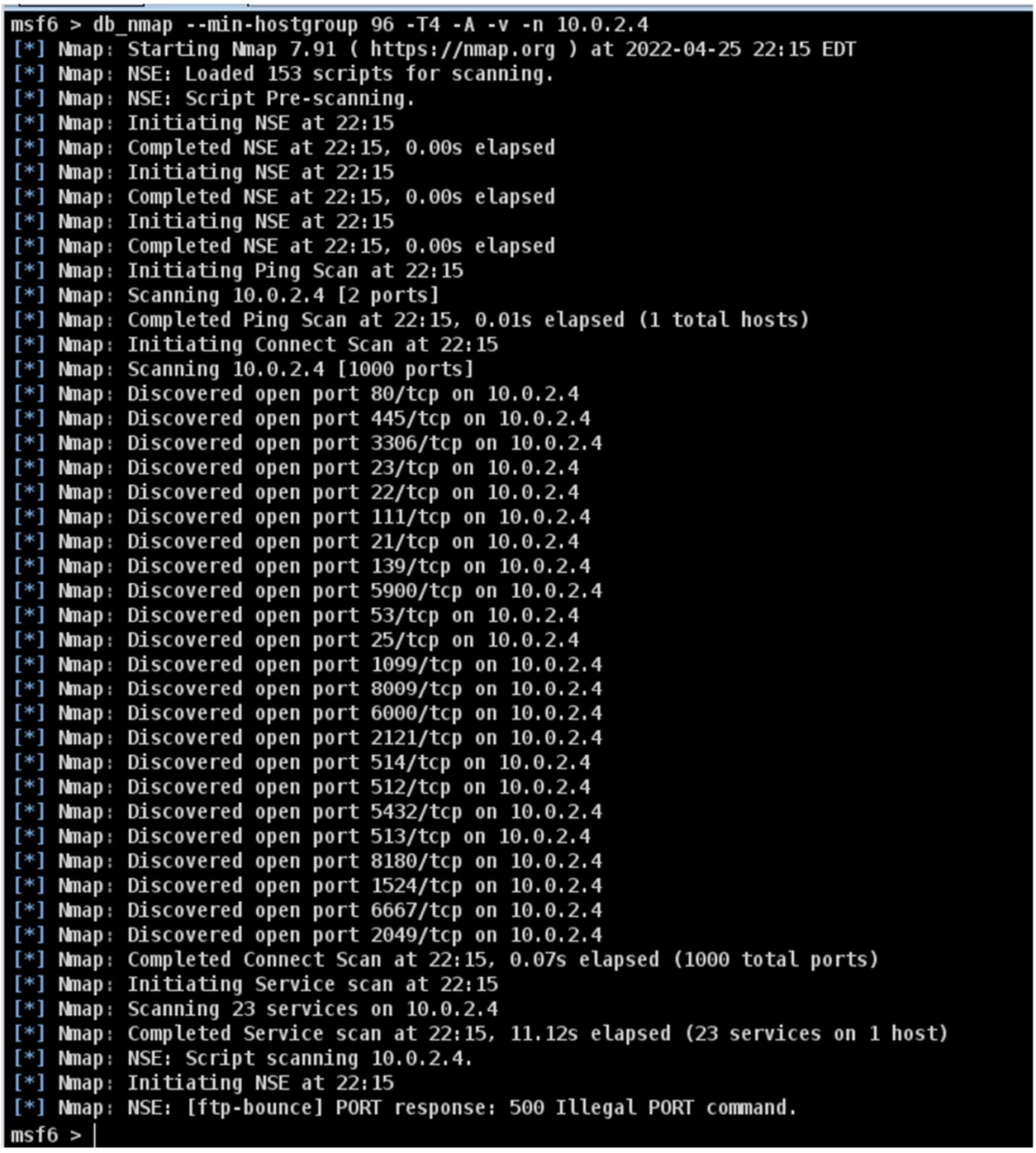
```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:a2:5c:81 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fea2:5c81/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Step 3. Open Armitage, select “connect” then “yes” to start msfdb. Add host to Armitage.



Step 4. Click on Hosts>NMAP Scan> Intense Scan. Repeat step 4 with different scanning tools.

Results:



```
[*] Nmap: Completed NSE at 22:15, 8.68s elapsed
[*] Nmap: Initiating NSE at 22:15
[*] Nmap: Completed NSE at 22:15, 0.22s elapsed
[*] Nmap: Initiating NSE at 22:15
[*] Nmap: Completed NSE at 22:15, 0.00s elapsed
[*] Nmap: Nmap scan report for 10.0.2.4
[*] Nmap: Host is up (0.0019s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
[*] Nmap: | ftp-syst:
[*] Nmap: |   STAT:
[*] Nmap: | FTP server status:
[*] Nmap: |      Connected to 10.0.2.15
[*] Nmap: |      Logged in as ftp
[*] Nmap: |      TYPE: ASCII
[*] Nmap: |      No session bandwidth limit
[*] Nmap: |      Session timeout in seconds is 300
[*] Nmap: |      Control connection is plain text
[*] Nmap: |      Data connections will be plain text
[*] Nmap: |      vsFTPd 2.3.4 - secure, fast, stable
[*] Nmap: |_End of status
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
[*] Nmap: |_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: |_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
[*] Nmap: | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
[*] Nmap: | Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
[*] Nmap: | Public Key type: rsa
[*] Nmap: | Public Key bits: 1024
[*] Nmap: | Signature Algorithm: sha1WithRSAEncryption
[*] Nmap: | Not valid before: 2010-03-17T14:07:45
[*] Nmap: | Not valid after:  2010-04-16T14:07:45
[*] Nmap: | MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
[*] Nmap: |_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
[*] Nmap: |_ssl-date: 2022-04-26T02:15:58+00:00; 0s from scanner time.
[*] Nmap: | sslv2:
[*] Nmap: |   SSLv2 supported
[*] Nmap: |   ciphers:
[*] Nmap: |     SSL2_DES_192_EDE3_CBC_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
msf6 >
```

```
[*] Nmap: |     SSL2_RC4_128_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_WITH_MD5
[*] Nmap: |     SSL2_RC4_128_EXPORT40_WITH_MD5
[*] Nmap: |_    SSL2_DES_64_CBC_WITH_MD5
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: | dns-nsid:
[*] Nmap: |_  bind.version: 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: | http-methods:
[*] Nmap: |_  Supported Methods: GET HEAD POST OPTIONS
[*] Nmap: |_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
[*] Nmap: |_http-title: Metasploitable2 - Linux
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
[*] Nmap: | rpcinfo:
[*] Nmap: |   program version    port/proto  service
[*] Nmap: |   100000  2            111/tcp   rpcbind
[*] Nmap: |   100000  2            111/udp   rpcbind
[*] Nmap: |   100003  2,3,4       2049/tcp   nfs
[*] Nmap: |   100003  2,3,4       2049/udp   nfs
[*] Nmap: |   100005  1,2,3      41295/tcp   mountd
[*] Nmap: |   100005  1,2,3      58154/udp   mountd
[*] Nmap: |   100021  1,3,4      36110/udp   nlockmgr
[*] Nmap: |   100021  1,3,4      51525/tcp   nlockmgr
[*] Nmap: |   100024  1          41585/udp   status
[*] Nmap: |_  100024  1          47410/tcp   status
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
[*] Nmap: 512/tcp  open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp  open  login       OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp  open  tcpwrapped
[*] Nmap: 1099/tcp open  java-rmi    GNU Classpath grmiregistry
[*] Nmap: 1524/tcp open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: | mysql-info:
[*] Nmap: |   Protocol: 10
[*] Nmap: |   Version: 5.0.51a-3ubuntu5
[*] Nmap: |   Thread ID: 10
[*] Nmap: |   Capabilities flags: 43564
[*] Nmap: |   Some Capabilities: SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsTransactions, SupportsCompression, Support41Auth, Speaks41ProtocolNew, LongColumnFlag
[*] Nmap: |   Status: Autocommit
[*] Nmap: |_  Salt: %AZ~.g=9D-R7Y<`PP!OK
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
msf6 >
```

```
[*] Nmap: | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
[*] Nmap: | Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
[*] Nmap: | Public Key type: rsa
[*] Nmap: | Public Key bits: 1024
[*] Nmap: | Signature Algorithm: sha1WithRSAEncryption
[*] Nmap: | Not valid before: 2010-03-17T14:07:45
[*] Nmap: | Not valid after:  2010-04-16T14:07:45
[*] Nmap: | MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
[*] Nmap: |_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
[*] Nmap: |_ssl-date: 2022-04-26T02:15:58+00:00; 0s from scanner time.
[*] Nmap: 5900/tcp open  vnc         VNC (protocol 3.3)
[*] Nmap: | vnc-info:
[*] Nmap: |   Protocol version: 3.3
[*] Nmap: |   Security types:
[*] Nmap: |_    VNC Authentication (2)
[*] Nmap: 6000/tcp open  X11         (access denied)
[*] Nmap: 6667/tcp open  irc         UnrealIRCd
[*] Nmap: | irc-info:
[*] Nmap: |   users: 1
[*] Nmap: |   servers: 1
[*] Nmap: |   lusers: 1
[*] Nmap: |   lservers: 0
[*] Nmap: |   server: irc.Metasploitable.LAN
[*] Nmap: |   version: Unreal3.2.8.1. irc.Metasploitable.LAN
[*] Nmap: |   uptime: 0 days, 0:08:43
[*] Nmap: |   source ident: nmap
[*] Nmap: |   source host: C29CBC04.EB72D3BE.7B559A54.IP
[*] Nmap: |_  error: Closing Link: bjedmzlbp[10.0.2.15] (Quit: bjedmzlbp)
[*] Nmap: 8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: |_ajp-methods: Failed to get a valid response for the OPTION request
[*] Nmap: 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: |_http-favicon: Apache Tomcat
[*] Nmap: | http-methods:
[*] Nmap: |_  Supported Methods: GET HEAD POST OPTIONS
[*] Nmap: |_http-server-header: Apache-Coyote/1.1
[*] Nmap: |_http-title: Apache Tomcat/5.5
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: 1h00m00s, deviation: 2h00m01s, median: 0s
[*] Nmap: | nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
[*] Nmap: | Names:
[*] Nmap: |   METASPLOITABLE<00>   Flags: <unique><active>
[*] Nmap: |   METASPLOITABLE<03>   Flags: <unique><active>
[*] Nmap: |   METASPLOITABLE<20>   Flags: <unique><active>
[*] Nmap: |   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
msf6 >
```

```
[*] Nmap: |_  error: Closing Link: bjedmzlbp[10.0.2.15] (Quit: bjedmzlbp)
[*] Nmap: 8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: |_ajp-methods: Failed to get a valid response for the OPTION request
[*] Nmap: 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: |_http-favicon: Apache Tomcat
[*] Nmap: | http-methods:
[*] Nmap: |_  Supported Methods: GET HEAD POST OPTIONS
[*] Nmap: |_http-server-header: Apache-Coyote/1.1
[*] Nmap: |_http-title: Apache Tomcat/5.5
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: 1h00m00s, deviation: 2h00m01s, median: 0s
[*] Nmap: | nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
[*] Nmap: | Names:
[*] Nmap: |   METASPLOITABLE<00>   Flags: <unique><active>
[*] Nmap: |   METASPLOITABLE<03>   Flags: <unique><active>
[*] Nmap: |   METASPLOITABLE<20>   Flags: <unique><active>
[*] Nmap: |   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
[*] Nmap: |   WORKGROUP<00>        Flags: <group><active>
[*] Nmap: |   WORKGROUP<1d>        Flags: <unique><active>
[*] Nmap: |_  WORKGROUP<1e>        Flags: <group><active>
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: |   Computer name: metasploitable
[*] Nmap: |   NetBIOS computer name:
[*] Nmap: |   Domain name: localdomain
[*] Nmap: |   FQDN: metasploitable.localdomain
[*] Nmap: |_  System time: 2022-04-25T22:15:51-04:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: |_smb2-time: Protocol negotiation failed (SMB2)
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 22:15
[*] Nmap: Completed NSE at 22:15, 0.00s elapsed
[*] Nmap: Initiating NSE at 22:15
[*] Nmap: Completed NSE at 22:15, 0.00s elapsed
[*] Nmap: Initiating NSE at 22:15
[*] Nmap: Completed NSE at 22:15, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 21.74 seconds
```

Step 5. After scans, select “Find Attacks”. Armitage automatically selects attacks that target vulnerabilities found in scan. Alternatively, one can select a “Hail Mary” attack. WARNING: This option is not subtle whatsoever and does not allow one to select hosts.

Metasploitable Report Results:

Metasploitable does not have a generate report tool

Recommendations:

Based on our results, we recommend OpenVAS and Nessus for detecting vulnerabilities in an operating system because both are easy to use and provide details on vulnerabilities detected in a structured manner. These 2 vulnerability assessment systems are best for providing insight into the vulnerabilities we have in our chosen operating systems.

The details Nessus provides on vulnerability systems include how to patch vulnerability and vulnerability numbers that can be identified online for solutions to vulnerability.

What makes OpenVAS stand out is its user interface. It is very simple to navigate. Learning how to scan is very easy and, learning how to exploit is simple as it tells you all about how to do it.

Vulnerability Scaling:

Nessus:
Nessus scales its vulnerability as Critical, High, Medium, and Low. These are based on CVSS which is based on how easily a vulnerability can be exploited.

OpenVAS:
OpenVAS ranks vulnerability a high, medium, and low. IT is based on CVSS that is ranked on how easily a vulnerability can be exploited.

Metasploit:
On the other hand, we would recommend Metasploit for learning how to use VASs because Metasploit provides the framework for several different VASs. It also gives the user an insight to using NMAP by displaying the commands used when running specific tools.

Project Milestones:

Milestone 1

- Proposal

Description:

Our team will brainstorm a topic to implement in our project and present our project idea to our professor Gonzalo.

Milestone 2

- Develop a plan for the team project

Description:

Our team hosts a meeting at UIW to discuss what we will need to do for our project and layout a plan on how we should work on the project.

Our team concluded that we would

1st. Identify different vulnerability Assessment software's we would use.

2nd. Identify Operating Systems to scan for vulnerabilities.

3rd. We need to set up a NAT configuration to create an isolated environment.

4th. Set up the attacker OS and target OS, run software to scan OS, record steps to use software, generate a report, and upload our work into our group GitHub repository.

5th. Set up tasks for team members on our Trello account to show the progress of the team.

Milestone 3

- Identify Software and Operating Systems for operation.

Description:

Our team decided to use Nessus, Openvas, and Metasploit to scan the operating systems Fedora, CentOS, and Metasploitable.

Milestone 4

- Develop a network for virtual machines.

Description:

Our team configured our VMS to a NAT configuration to isolate them from our home networks.

Milestone 5

- Execute Software on Operating Systems within the network.

Description:

Our Team will install our assigned vulnerability assessment scanners onto our personal computers kali Linux virtual machine.

Candan will install Nessus, Devon will install OpenVAS and, Daniel will install Metasploit.

All team members will install the OS's Metasploitable, Fedora, and CentOS onto their own virtual machines configured to a NAT network.

Using our virtual kali Linux machine, each member will use their assigned software to scan for vulnerabilities on target operating systems Fedora, CentOS, and Metasploitable.

Milestone 6

- Record, analyze, and then discuss with the team on data.

Description:

Our team will take snapshots of the steps used to execute our vulnerability assessment software in a word document.

Our team will generate vulnerability reports from the software and uploaded to the teams GitHub repository of the group.

Meet with the team to discuss which software was most effective and what operating system was most secure.

Milestone 7

- Create a Slide presentation
- Submit Final Report

Description:

Create a presentation of our project to present to our class.

Revise the initial report and submit a final report of the project.

Current Status of Project:

The project is complete and software has been used to scan three operating systems for vulnerabilities.

Next Steps:

- Present project and submit onto Canvas assignments page

Expected Outcomes:

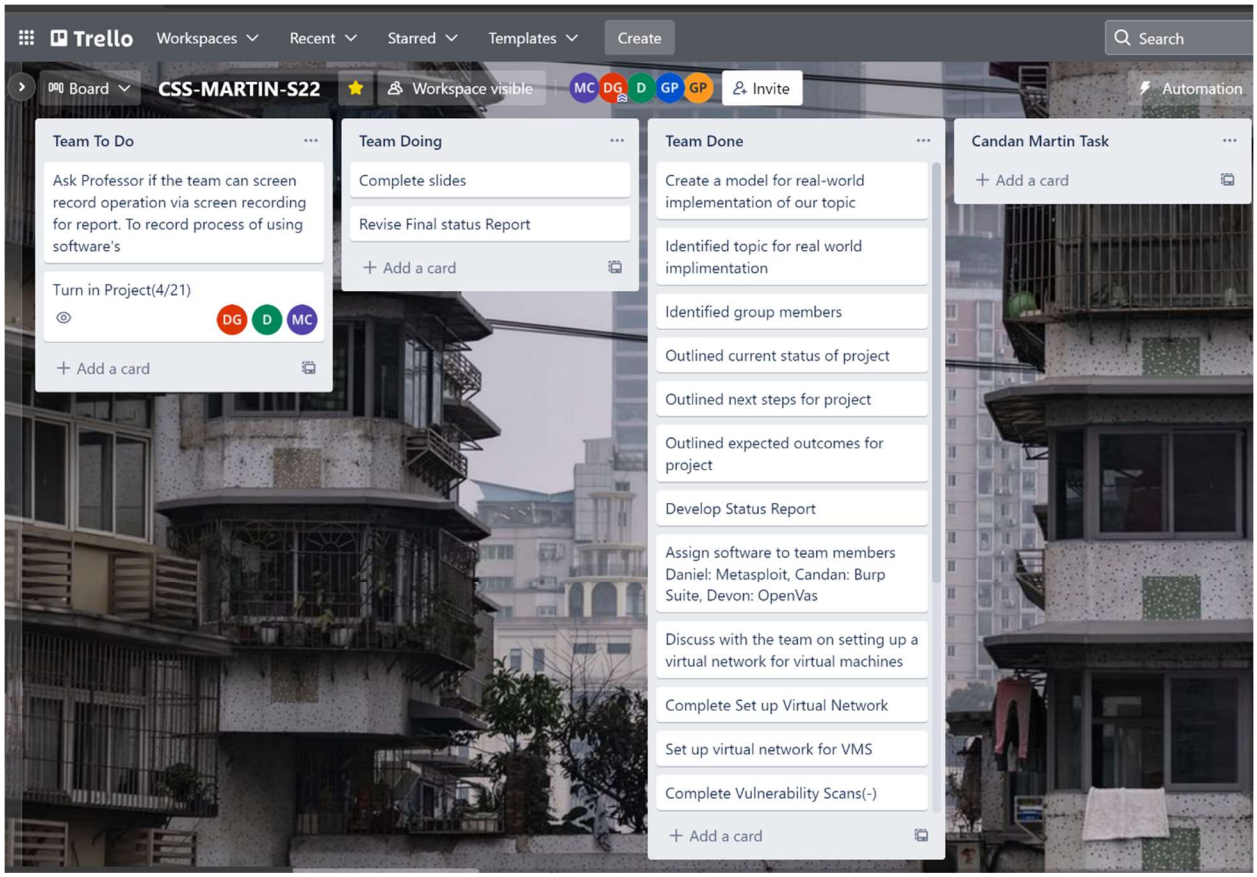
- Have a model that can be used to identify the most effective Vulnerability assessment scanners.
- Identify the most effective and useful vulnerability scanner.

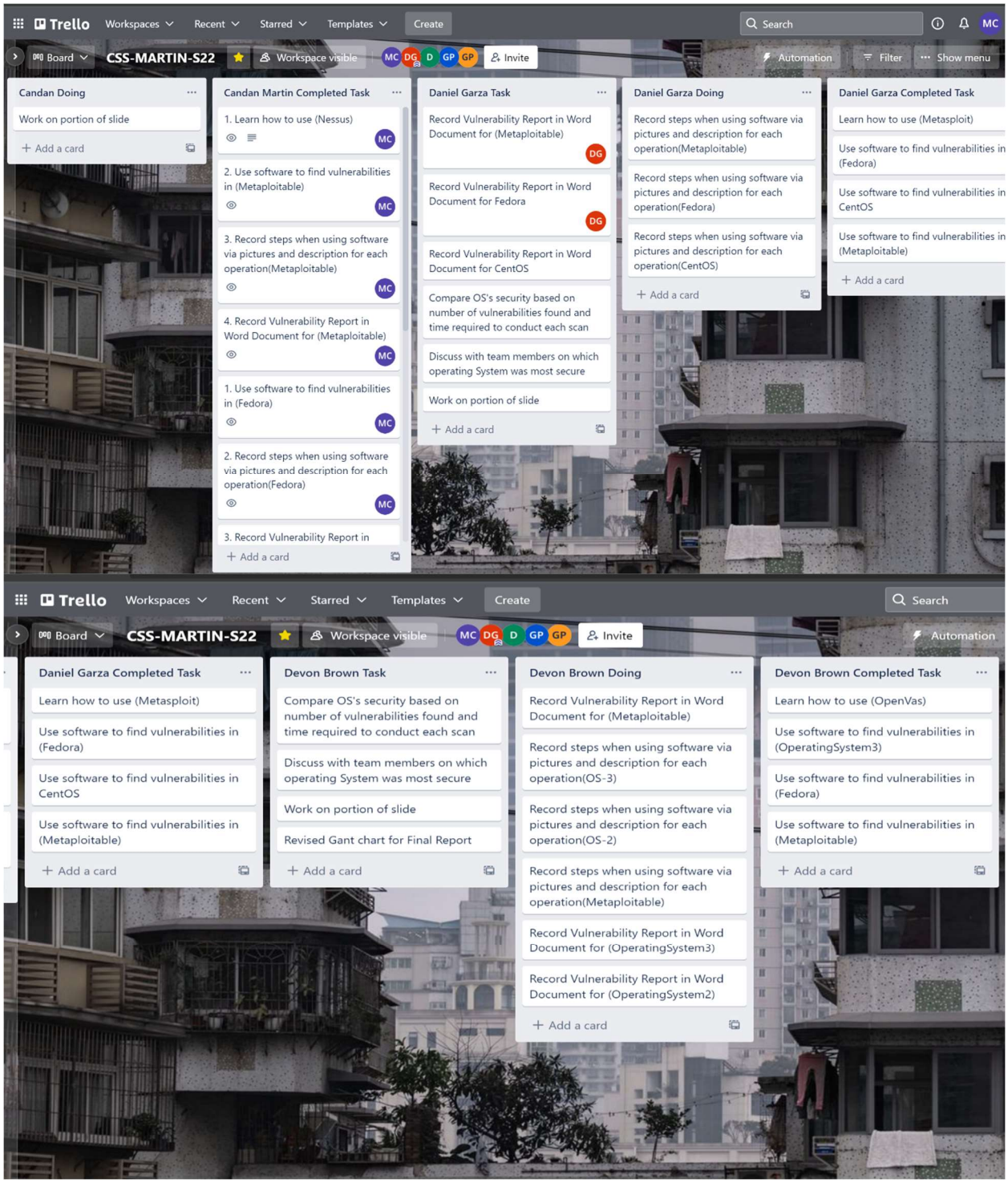
Deliverables

Deliverable 1.

Add member tasks in Trello Account-Link in table of contents.

Fig. 2.1




Trello
Workspaces
Recent
Starred
Templates
Create
Search
Board
CSS-MARTIN-S22
Workspace visible
Invite
Automation
Filter
Show menu
Candan Doing
Work on portion of slide
Add a card
Candan Martin Completed Task
1. Learn how to use (Nessus)
2. Use software to find vulnerabilities in (Metaploitable)
3. Record steps when using software via pictures and description for each operation(Metaploitable)
4. Record Vulnerability Report in Word Document for (Metaploitable)
1. Use software to find vulnerabilities in (Fedora)
2. Record steps when using software via pictures and description for each operation(Fedora)
3. Record Vulnerability Report in
Daniel Garza Task
Record Vulnerability Report in Word Document for (Metaploitable)
Record Vulnerability Report in Word Document for Fedora
Record Vulnerability Report in Word Document for CentOS
Compare OS's security based on number of vulnerabilities found and time required to conduct each scan
Discuss with team members on which operating System was most secure
Work on portion of slide
Daniel Garza Doing
Record steps when using software via pictures and description for each operation(Metaploitable)
Record steps when using software via pictures and description for each operation(Fedora)
Record steps when using software via pictures and description for each operation(CentOS)
Daniel Garza Completed Task
Learn how to use (Metasploit)
Use software to find vulnerabilities in (Fedora)
Use software to find vulnerabilities in CentOS
Use software to find vulnerabilities in (Metaploitable)
Trello
Workspaces
Recent
Starred
Templates
Create
Search
Board
CSS-MARTIN-S22
Workspace visible
Invite
Automation
Daniel Garza Completed Task
Learn how to use (Metasploit)
Use software to find vulnerabilities in (Fedora)
Use software to find vulnerabilities in CentOS
Use software to find vulnerabilities in (Metaploitable)
Devon Brown Task
Compare OS's security based on number of vulnerabilities found and time required to conduct each scan
Discuss with team members on which operating System was most secure
Work on portion of slide
Revised Gant chart for Final Report
Devon Brown Doing
Record Vulnerability Report in Word Document for (Metaploitable)
Record steps when using software via pictures and description for each operation(OS-3)
Record steps when using software via pictures and description for each operation(OS-2)
Record steps when using software via pictures and description for each operation(Metaploitable)
Record Vulnerability Report in Word Document for (OperatingSystem3)
Record Vulnerability Report in Word Document for (OperatingSystem2)
Devon Brown Completed Task
Learn how to use (OpenVas)
Use software to find vulnerabilities in (OperatingSystem3)
Use software to find vulnerabilities in (Fedora)
Use software to find vulnerabilities in (Metaploitable)

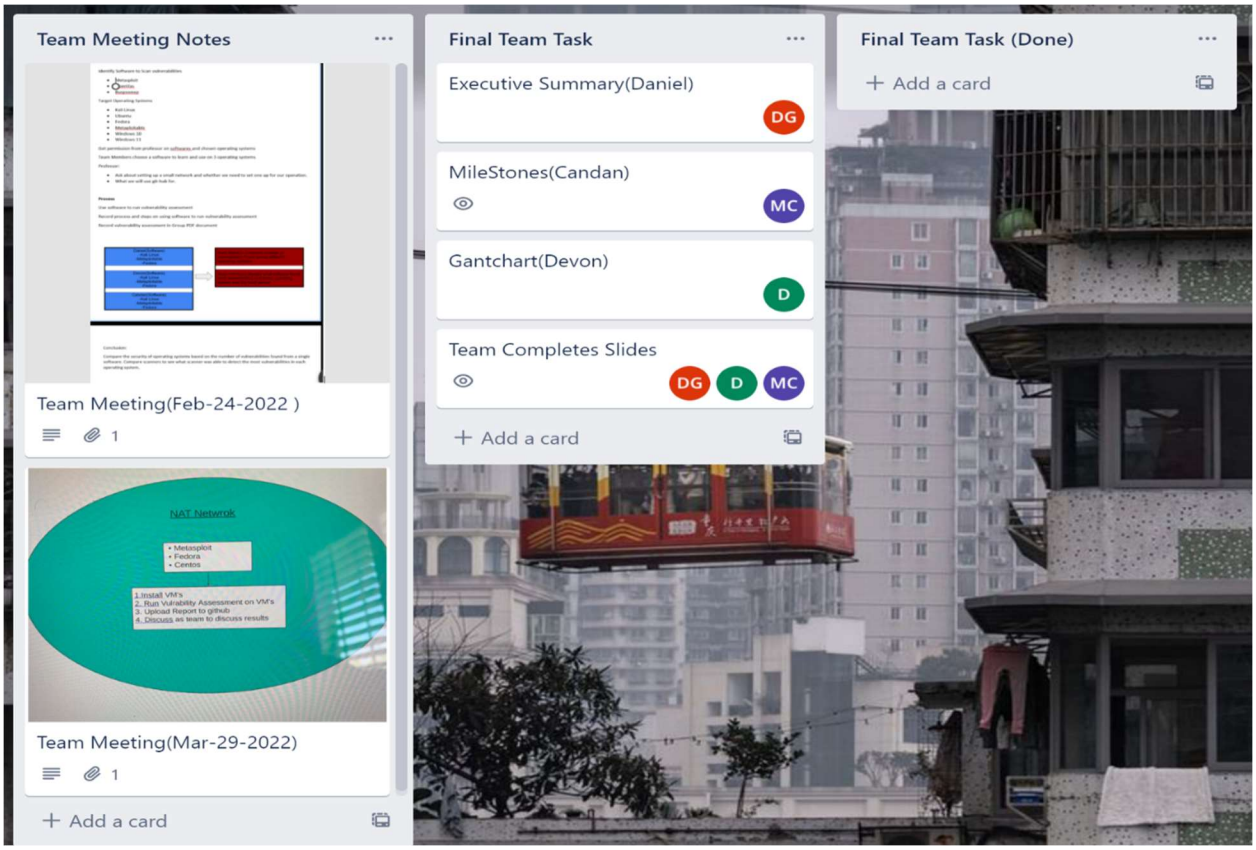


Fig. 2.1

Deliverable 2.

Documents showing how we used software and our generated reports were uploaded to team GitHub-Link in table of contents

Fig. 2.2

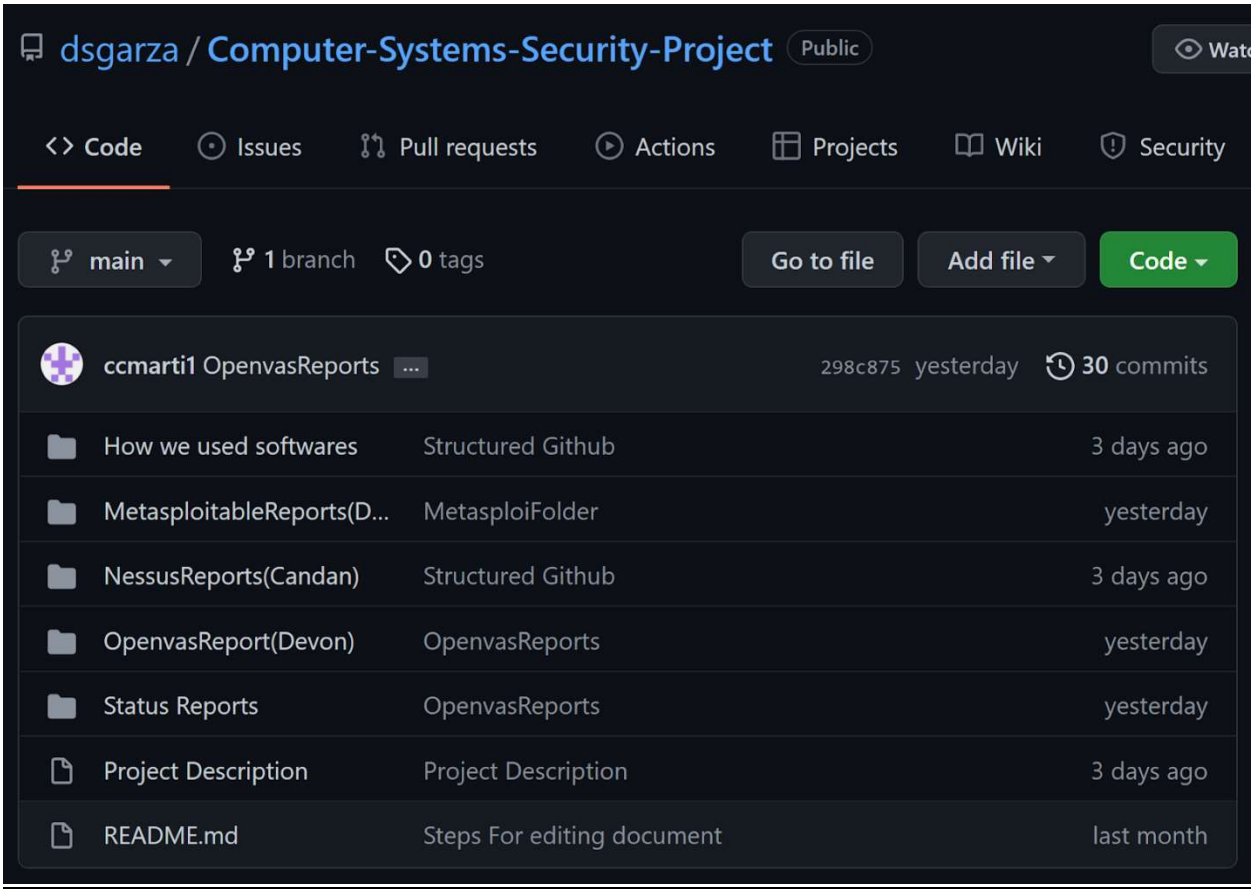


Fig. 2.2

Deliverable 3.

Presentation Slide Made Fig. 2.3

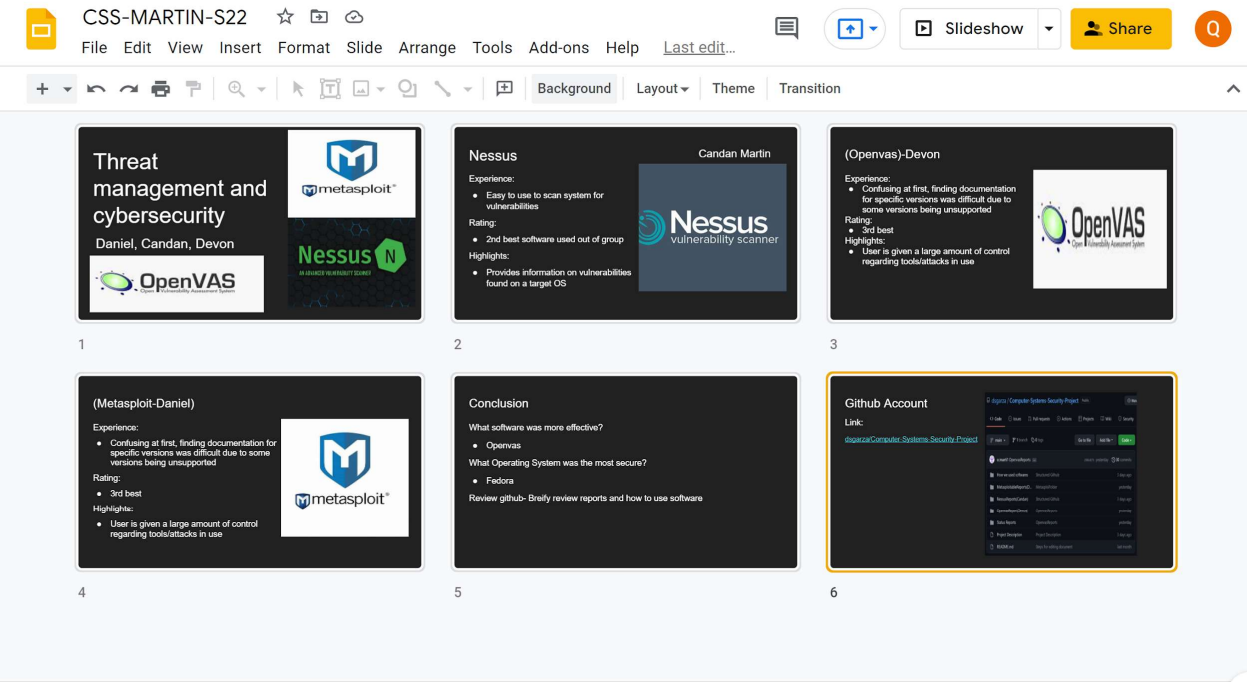


Fig. 2.3

Deliverable 4.

Initial visual display of how we will execute our project. Fig. 2.4

Changes made to design:

1. Burp suite has been changed to Nessus. Burp suite was miss-spelled as burpsweep.
2. Target Operating Systems changed to Metasploitable, Fedora, CentOS.

Identify Software to Scan vulnerabilities

- Metasploit
- OpenVas
- Burpsweep

Target Operating Systems

- Kali Linux
- Ubuntu
- Fedora
- Metaploitable
- Windows 10
- Windows 11

Get permission from professor on softwares and chosen operating systems

Team Members choose a software to learn and use on 3 operating systems

Professor:

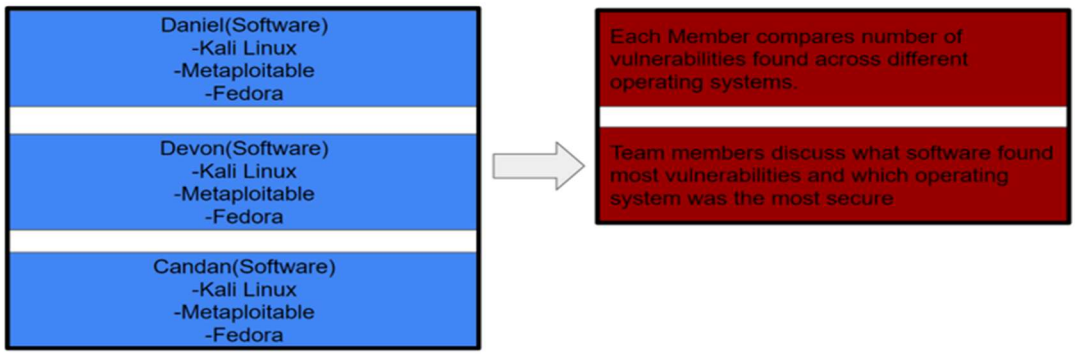
- Ask about setting up a small network and whether we need to set one up for our operation.
- What we will use git-hub for.

Process

Use software to run vulnerability assessment

Record process and steps on using software to run vulnerability assessment

Record vulnerability assessment in Group PDF document



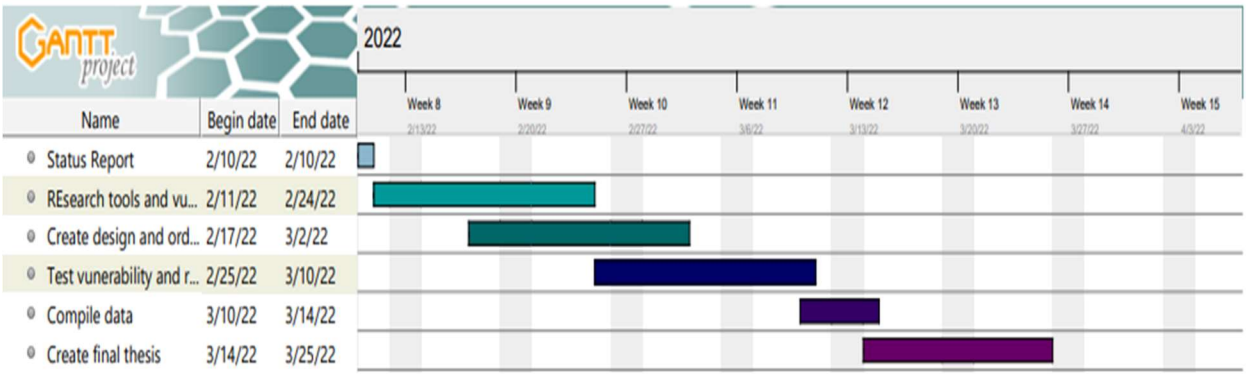
Conclusion:

Compare the security of operating systems based on the number of vulnerabilities found from a single software. Compare scanners to see what scanner was able to detect the most vulnerabilities in each operating system.

Fig. 2.4

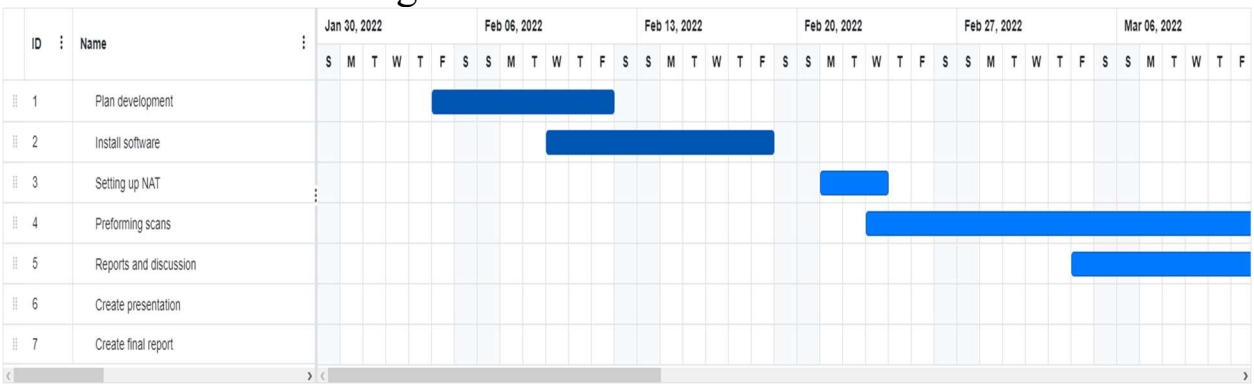
Deliverable 5.

Initial Gantt Chart Fig. 2.5



Deliverable 6.

Revised Gantt Chart Fig. 2.6



Professional Accomplishments

1. Learn to work in a collaborative environment in a team.
2. Development of skills in project management and constructing a plan to implement a task given. Our task given was implementing the topic our team chose.

Individually

Candan:

1. Learned how to use Nessus to scan operating systems.
2. Learned how to structure plans for project implementation and collaborate with the team for ideas.
3. Learned how to configure NAT network.

Daniel:

1. Learned how to use Armitage software.
2. Learned how to work Unix/Linux operating systems efficiently.
3. Learned time/project management.

Devon:

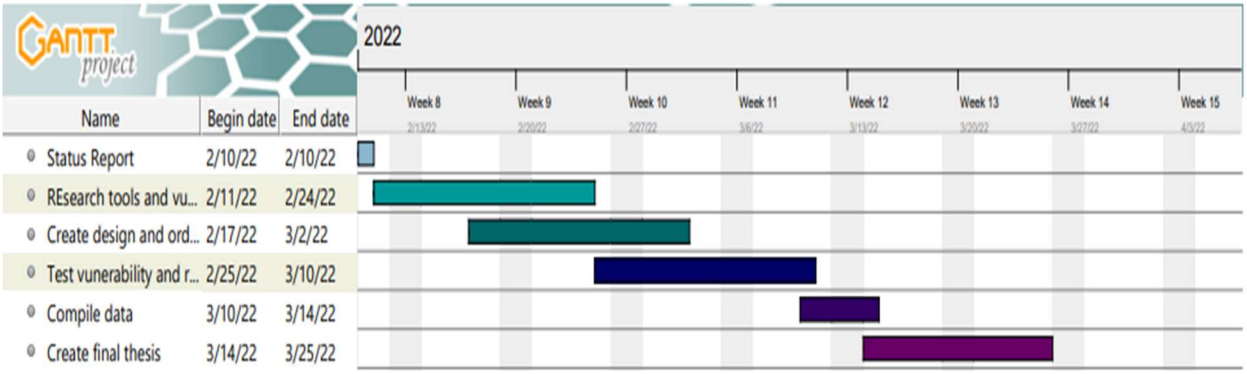
1. Learned how to configure and use OpenVAS

2. Learned how to find and exploit vulnerabilities on Operating Systems.
3. Learn how to create a Gantt Chart

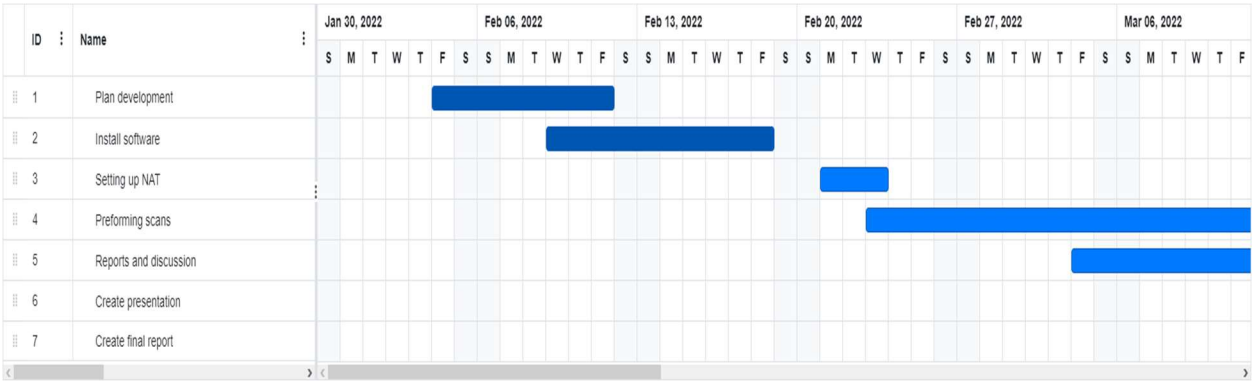
Project Schedule Management

Gantt chart

- Initial Gantt Chart



- Revised Gantt Chart



Links

Github:

https://github.com/dsgarza/Computer-Systems-Security-Project.git

Description:

Contains all results and materials used in the project.

Trello:

https://trello.com/b/D8nc0ssm/comp-sys-sec-project#

Description:

This is where the team planned and tracked its progress on the project.

Credits Page

Executive Summary

Contributors: Daniel and Candan

- OpenVAS Results
- OpenVas Generated Report

  Contributors: Devon
- Nessus Results
- Nessus Generated Report

  Contributors: Candan
- Metasploit Results
- Metasploit Generated Report

  Contributors: Daniel
- Recommendations

  Contributors: Devon, Daniel and Candan

Project Milestones

Contributors: Candan

- Current Status of Project
- Next Steps
- Expected Outcomes

  Contributors: Candan

Deliverables

Contributors: Candan

Professional Accomplishments

Contributors: Devon, Daniel and Candan

- Candan Professional Accomplishments
- Daniel Professional Accomplishments
- Devon Professional Accomplishments

Project Schedule Management

Contributors: Devon and Candan

- Gant Chart

  Contributors: Devon
- Links

  Contributors: Candan

Credits Page

Contributors: Candan

Table of Contents

Contributors: Candan

Table of Contents