MY RECENT CYBERSECURITY PROJECT: Vulnerability Assessment & SIEM Integration with MITRE ATT&CK Mapping and Remediation (Nmap, Nessus, Splunk)

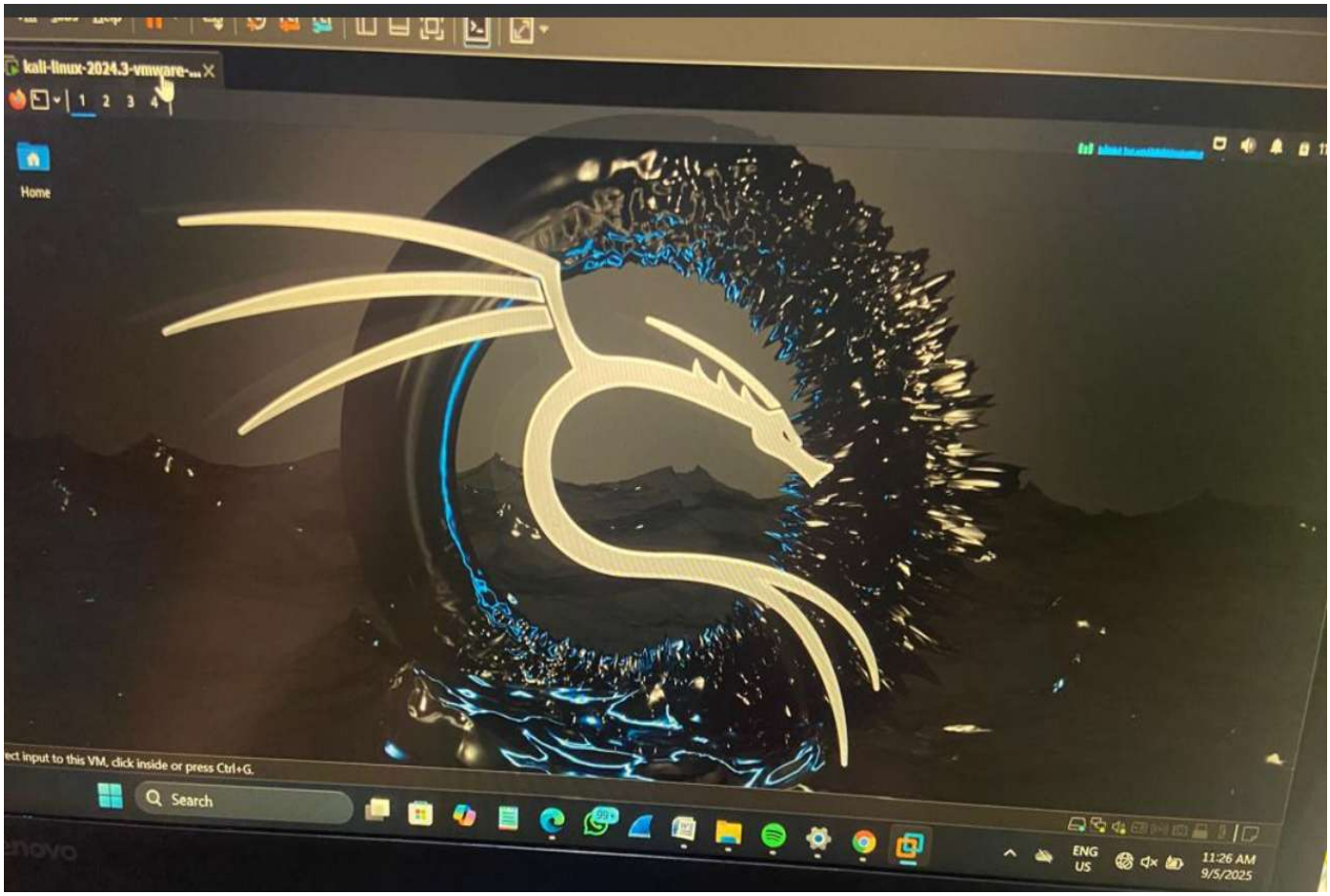
I'm excited to share my recent hands on cybersecurity project.

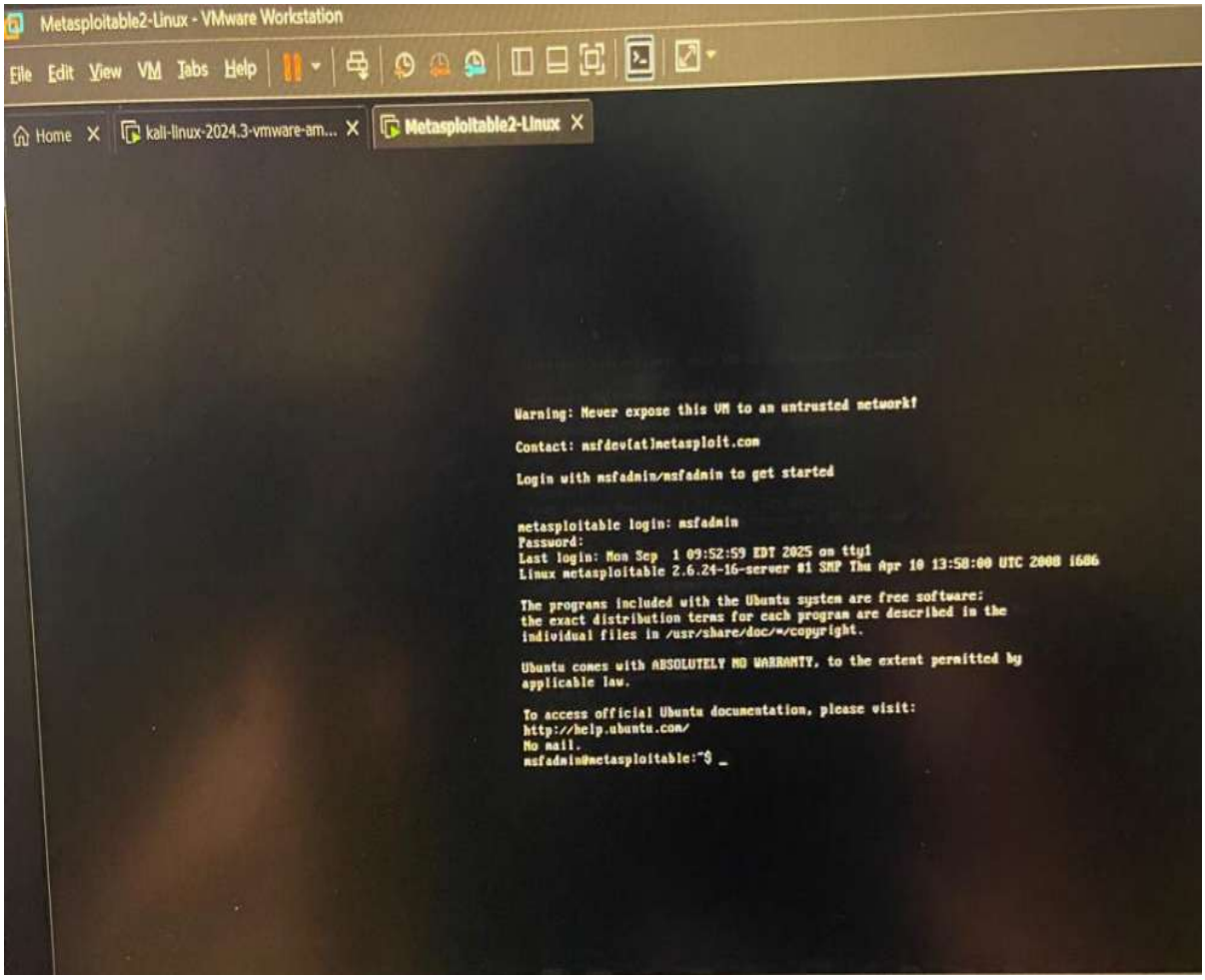
Project Overview: This project simulates a real SOC analyst workflow: scanning a vulnerable machine (Metasploitable 2) with Nmap and Nessus, ingesting findings into Splunk, mapping results to MITRE ATT&CK techniques, and providing remediation recommendations. The goal was to practice vulnerability management, threat detection, and reporting.

STEPS TAKEN:

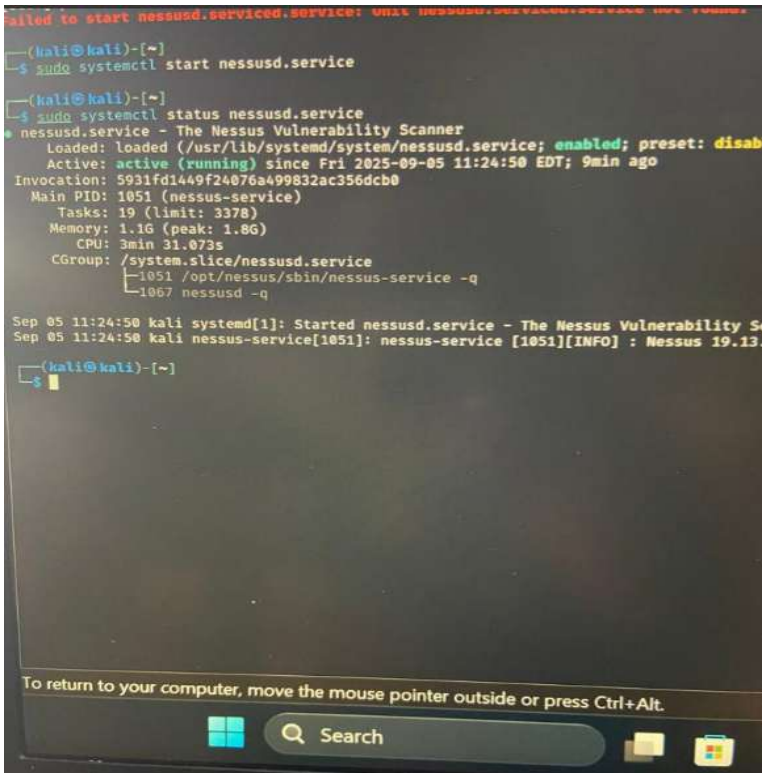
1. Set up the lab, installed kali Linux, deployed metasploitable as target machine, installed Nessus Essentials on Kali Linux, Installed Splunk Enterprise on my host machine (windows)
2. Ran **Nmap scans on Metasploitable** to identify open ports and services.
3. Used **Nessus** to perform authenticated and unauthenticated scans on metasploitable.
4. Exported Nessus results for ingestion to splunk in windows using shared folder in linux
5. Wrote Python scripts to convert .nessus file and .xml file to CSV files for easier analysis in Splunk.
6. Built Splunk dashboards showing **Top CVEs, open ports, and severity levels.**
7. Mapped key vulnerabilities to **MITRE ATT&CK techniques**
8. Suggested **remediation** for high-severity CVEs.

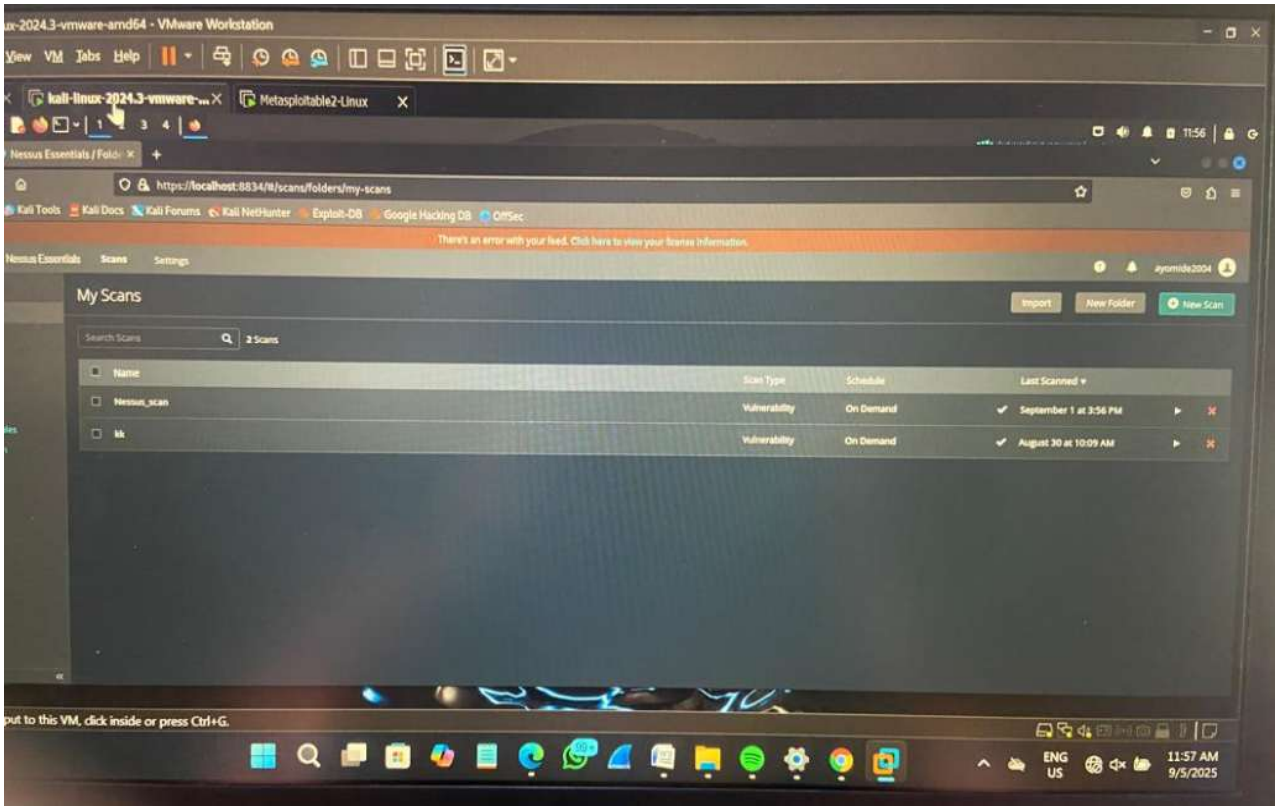
Step 1: The first thing I did was to get my kali Linux and my target machine which is metasploitable ready.

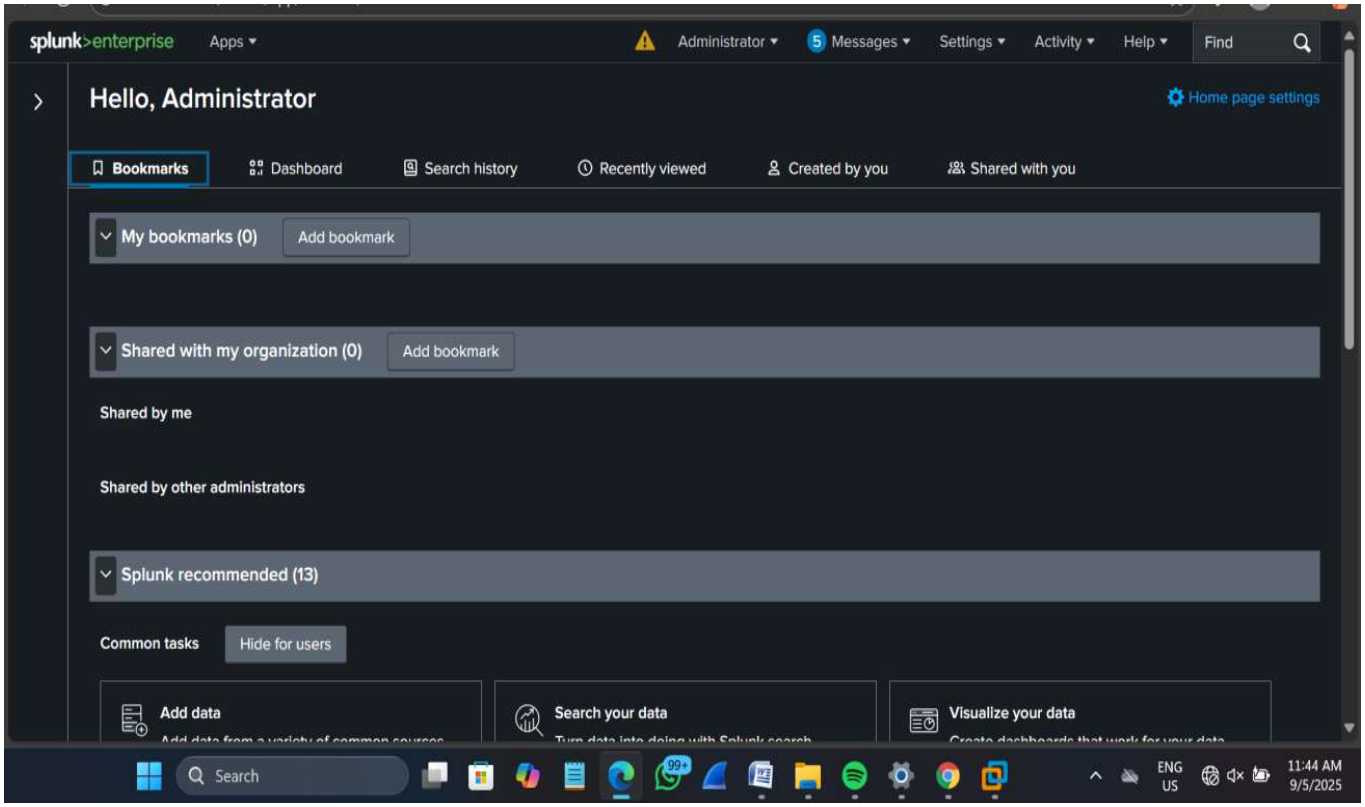




Then set up my nessus and splunk as well







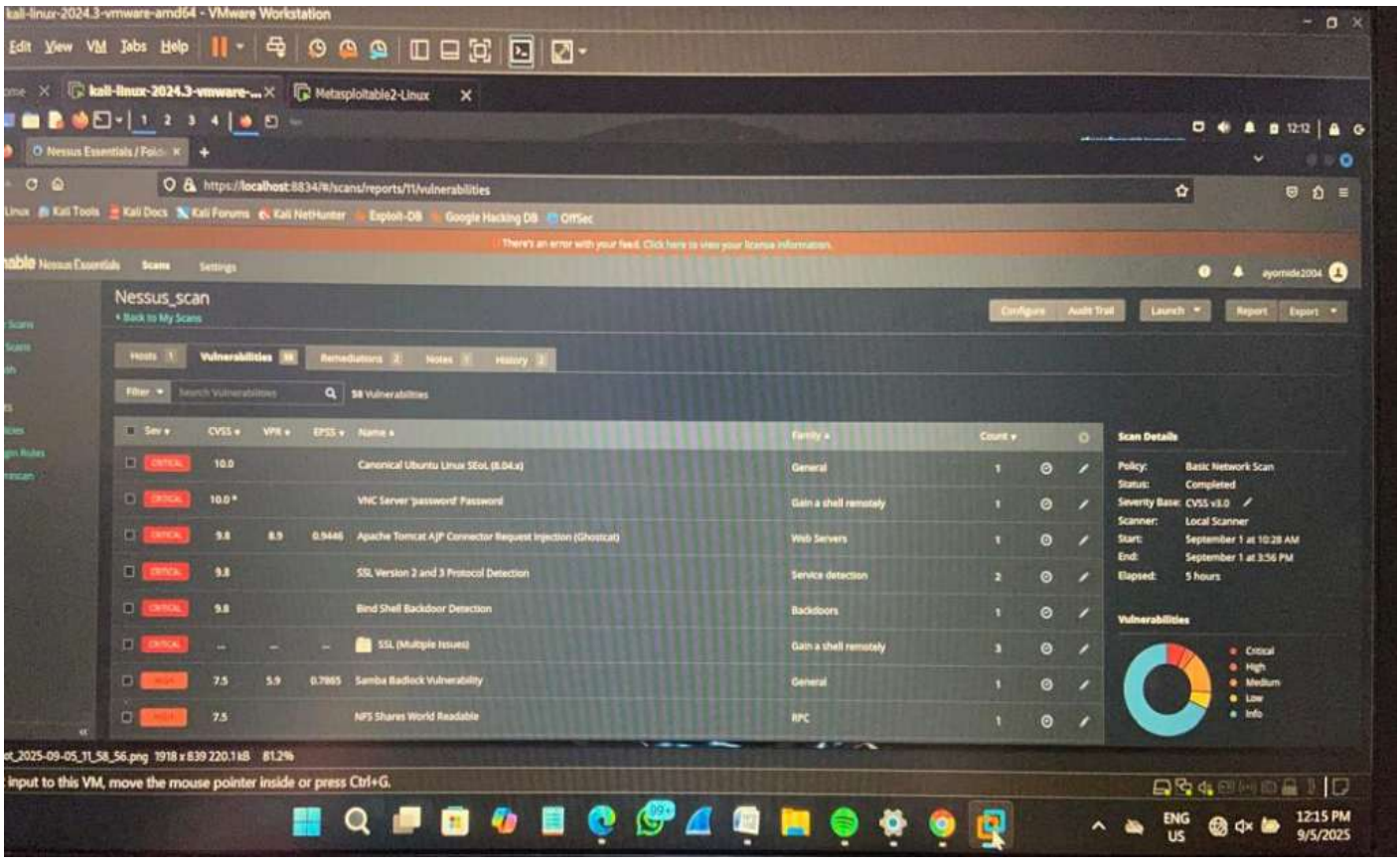
Step 2

Reconnaissance Using Nmap: Ran nmap scan on Metasploitable's Ip to identify open ports and services

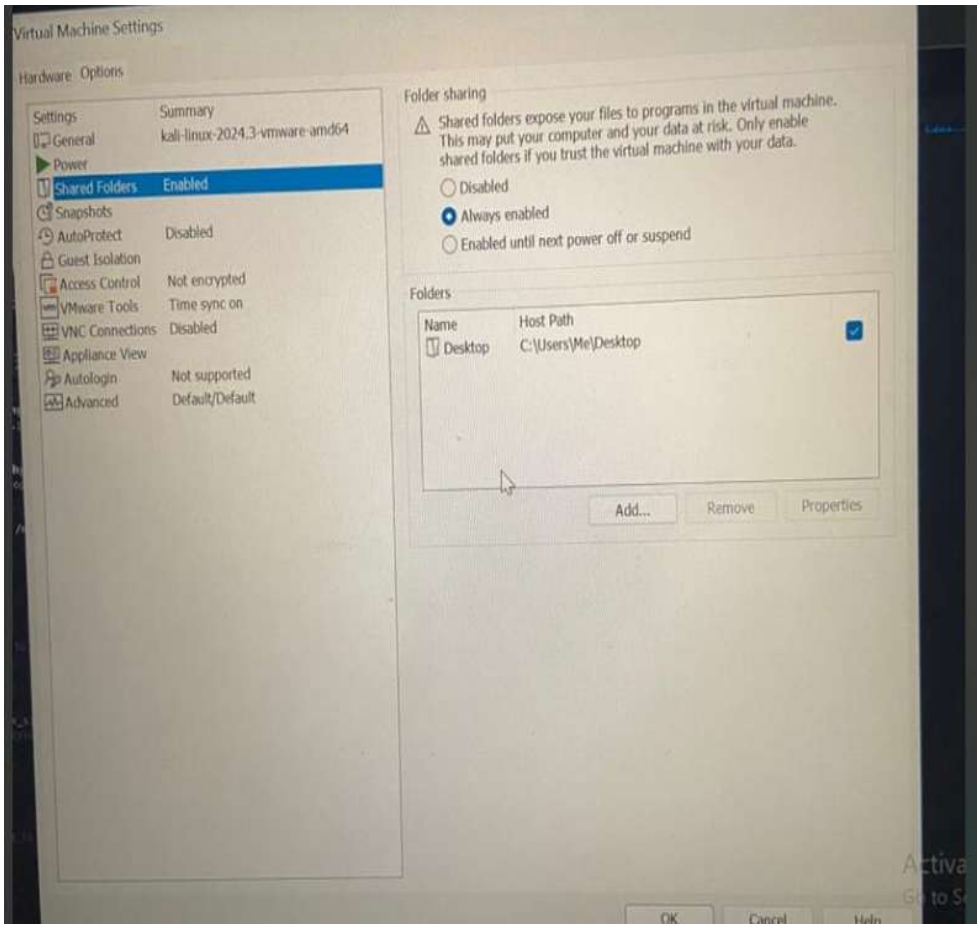
Note: I checked the ip address using ifconfig

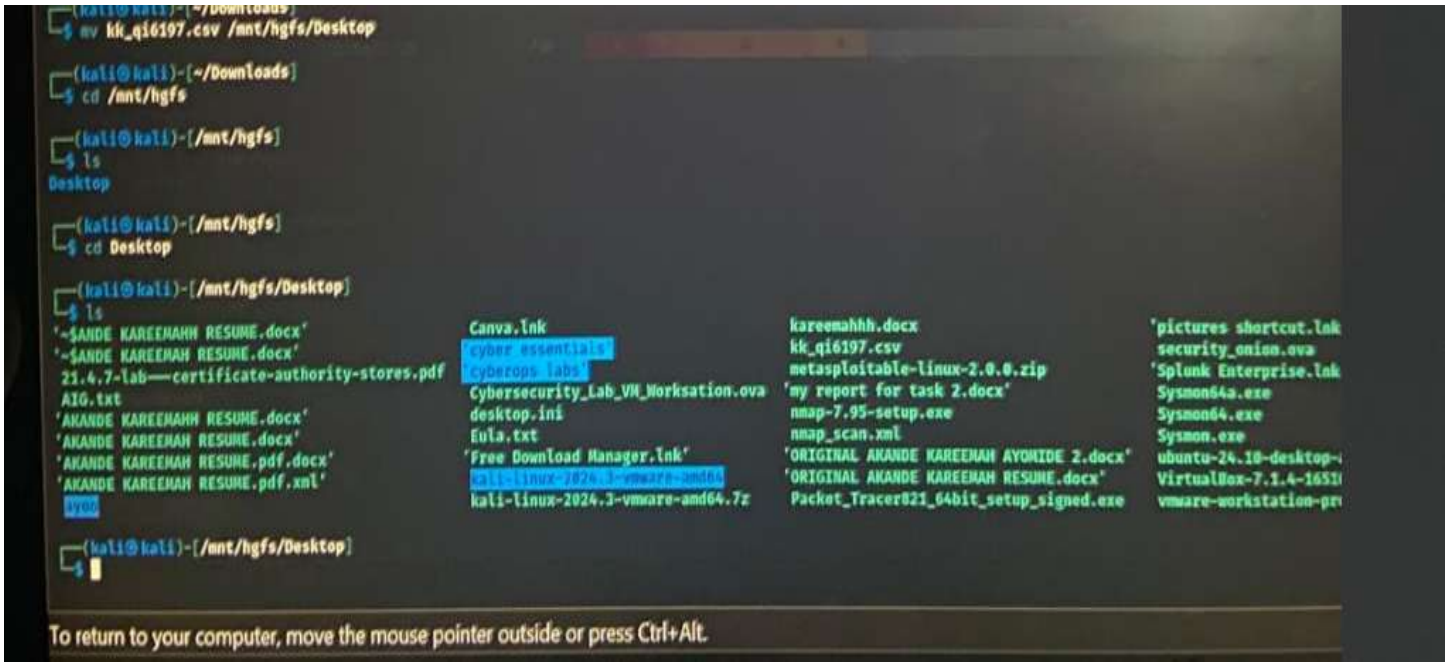
```
File Edit View VM Tabs Help
Metasploitable2-Linux   kali-linux-2024.3-vmware-...
File Actions Edit View Help
└─$ sudo nmap -sS -sV -P  80 -T4 192.168.61.128 -OX /mnt/hgfs/Desktop/nmap_scan.xml
Unknown argument to -O.
QUITTING!

┌──(kali㉿kali)-[/mnt/hgfs]
└─$ sudo nmap -sS -sV -P  80 -T4 192.168.61.128 -oX /mnt/hgfs/Desktop/nmap_scan.xml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-29 01:05 EDT
Nmap scan report for 192.168.61.128
Host is up (0.0070s latency).
Not shown: 977 filtered tcp ports (no-response)
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  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:l

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (1 host up) scanned in 178.43 seconds

┌──(kali㉿kali)-[/mnt/hgfs]
└─$ cd downloads
cd: no such file or directory: downloads

┌──(kali㉿kali)-[/mnt/hgfs]
└─$ cd Downloads
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

Step 3: used **Nessus** to perform authenticated and unauthenticated scans on metasploitable.



Step 4: Exported Nessus results for ingestion to splunk in windows using shared folder in linux.



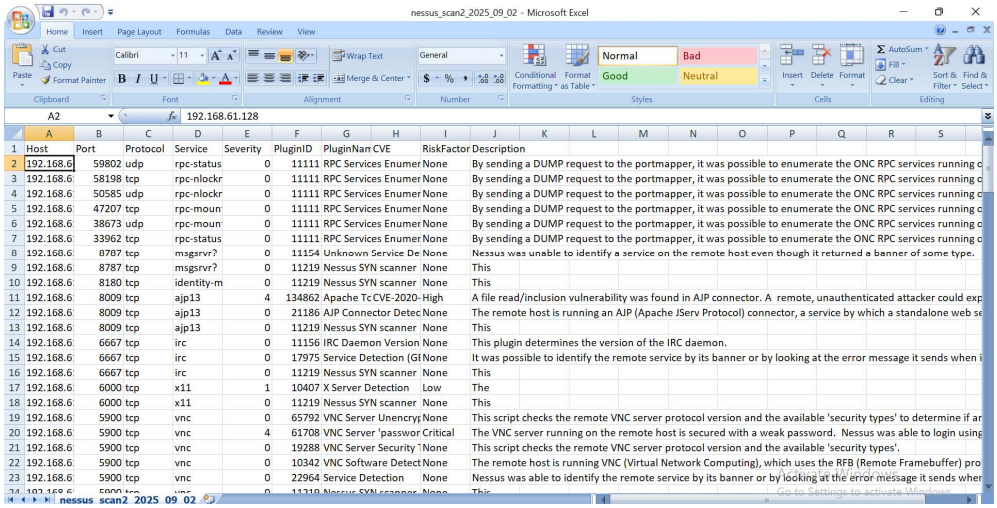


STEP 5:

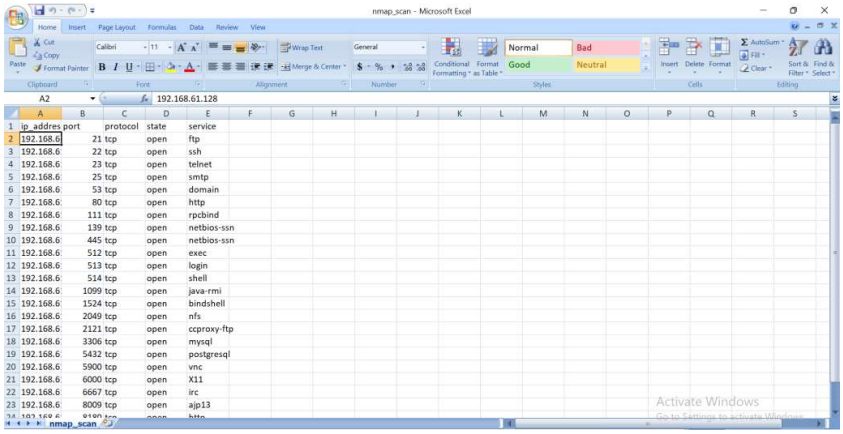
Wrote Python scripts to convert .nessus file and .xml file to CSV files for easier analysis in Splunk

```
File  Edit  View
root = tree.getroot()

# Open CSV for writing
with open(output_file, "w", newline="", encoding="utf-8") as csvfile:
    writer = csv.writer(csvfile)
    writer.writerow([
        "Host", "Port", "Protocol", "Service",
        "Severity", "PluginID", "PluginName",
        "CVE", "RiskFactor", "Description"
    ])

    # Loop through hosts
    for report_host in root.findall(".//ReportHost"):
        host = report_host.get("name")

        # Loop through vulnerabilities
        for report_item in report_host.findall("ReportItem"):
            port = report_item.get("port")
            protocol = report_item.get("protocol")
            service = report_item.get("svc_name")
            severity = report_item.get("severity")
            plugin_id = report_item.get("pluginID")
            plugin_name = report_item.get("pluginName")
            risk_factor = report_item.findtext("risk_factor", default="")
            description = report_item.findtext("description", default="")
            cve = ",".join([c.text for c in report_item.findall("cve")])

            writer.writerow([
                host, port, protocol, service,
                severity, plugin_id, plugin_name,
                cve, risk_factor, description
            ])

print(f"[+] Done! Results saved to {output_file}")
```

```
File  Edit  View

import csv
import xml.etree.ElementTree as ET

# Open your Nmap scan file
tree = ET.parse("nmap_scan.xml")
root = tree.getroot()

# Prepare CSV file
with open("nmap_scan.csv", "w", newline="") as csvfile:
    writer = csv.writer(csvfile)
    writer.writerow(["ip_address", "port", "protocol", "state", "service"])

    for host in root.findall("host"):
        ip_elem = host.find("address")
        if ip_elem is not None:
            ip_address = ip_elem.get("addr")
        else:
            continue

        for port in host.findall(".//port"):
            portid = port.get("portid")
            protocol = port.get("protocol")
            state = port.find("state").get("state")
            service_elem = port.find("service")
            service = service_elem.get("name") if service_elem is not None else ""

            writer.writerow([ip_address, portid, protocol, state, service])
```



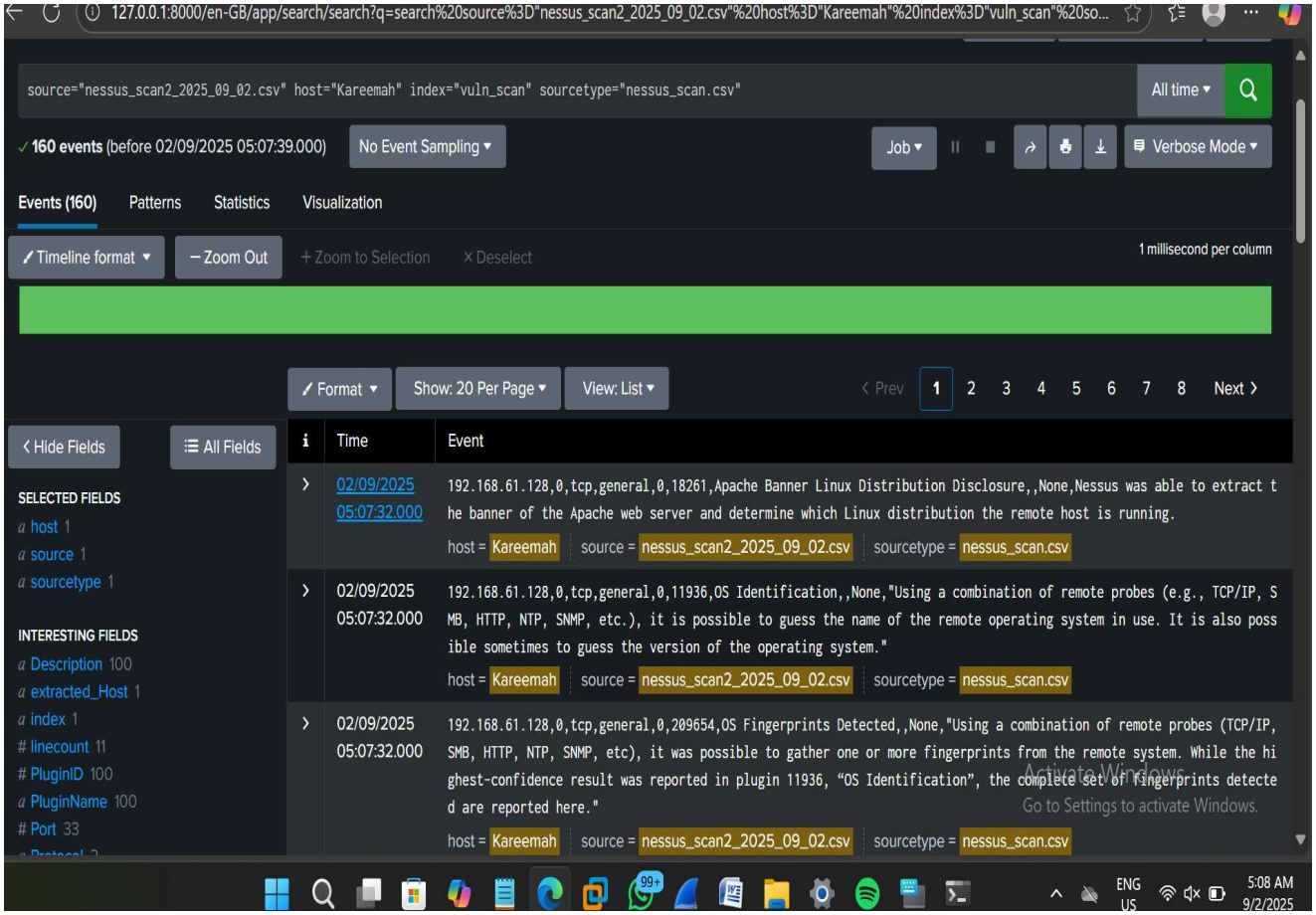
Host	Port	Protocol	Service	Severity	PluginID	PluginName	CVE	RiskFactor	Description
192.168.6	59802	udp	rpc-status	0	11111	RPC Services Enumer		None	By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running c
192.168.6	58198	tcp	rpc-nlockr	0	11111	RPC Services Enumer		None	By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running c
192.168.6	50585	udp	rpc-nlockr	0	11111	RPC Services Enumer		None	By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running c
192.168.6	47207	tcp	rpc-moun	0	11111	RPC Services Enumer		None	By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running c
192.168.6	38673	udp	rpc-moun	0	11111	RPC Services Enumer		None	By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running c
192.168.6	33962	tcp	rpc-status	0	11111	RPC Services Enumer		None	By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running c
192.168.6	8787	tcp	msgsrvr?	0	11154	Unknown Service De		None	Nessus was unable to identify a service on the remote host even though it returned a banner of some type.
192.168.6	8787	tcp	msgsrvr?	0	11219	Nessus SYN scanner		None	This
192.168.6	8180	tcp	identity-m	0	11219	Nessus SYN scanner		None	This
192.168.6	8009	tcp	ajp13	4	134862	Apache Tc	CVE-2020-	High	A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exp
192.168.6	8009	tcp	ajp13	0	21186	AJP Connector Detec		None	The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web se
192.168.6	8009	tcp	ajp13	0	11219	Nessus SYN scanner		None	This
192.168.6	6667	tcp	irc	0	11156	IRC Daemon Version		None	This plugin determines the version of the IRC daemon.
192.168.6	6667	tcp	irc	0	17975	Service Detection (GI		None	It was possible to identify the remote service by its banner or by looking at the error message it sends when i
192.168.6	6667	tcp	irc	0	11219	Nessus SYN scanner		None	This
192.168.6	6000	tcp	x11	1	10407	X Server Detection		Low	The
192.168.6	6000	tcp	x11	0	11219	Nessus SYN scanner		None	This
192.168.6	5900	tcp	vnc	0	65792	VNC Server Unencryp		None	This script checks the remote VNC server protocol version and the available 'security types' to determine if ar
192.168.6	5900	tcp	vnc	4	61708	VNC Server 'passwor		Critical	The VNC server running on the remote host is secured with a weak password. Nessus was able to login using
192.168.6	5900	tcp	vnc	0	19288	VNC Server Security		None	This script checks the remote VNC server protocol version and the available 'security types'.
192.168.6	5900	tcp	vnc	0	10342	VNC Software Detect		None	The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) pro
192.168.6	5900	tcp	vnc	0	22964	Service Detection		None	Nessus was able to identify the remote service by its banner or by looking at the error message it sends wher

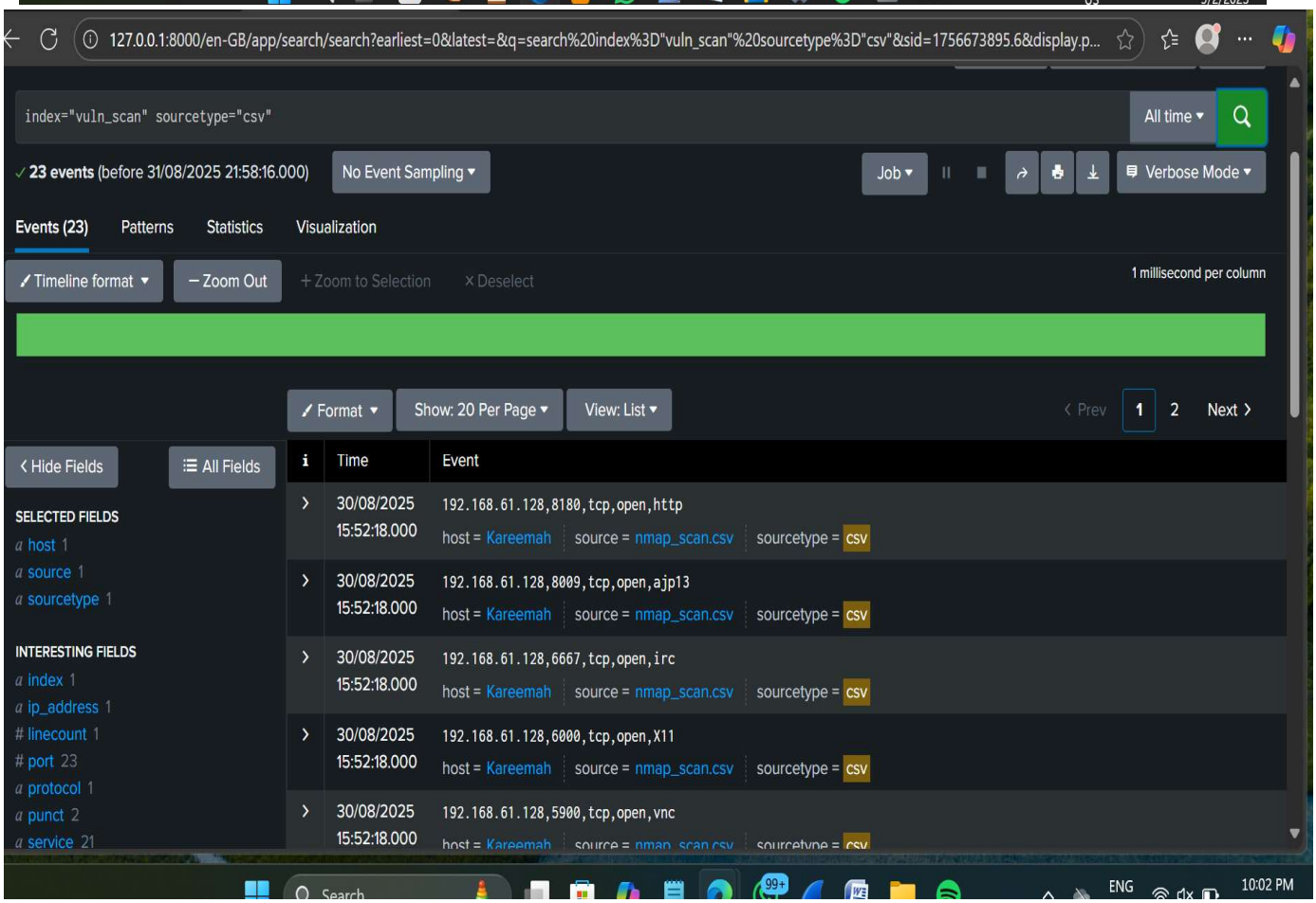


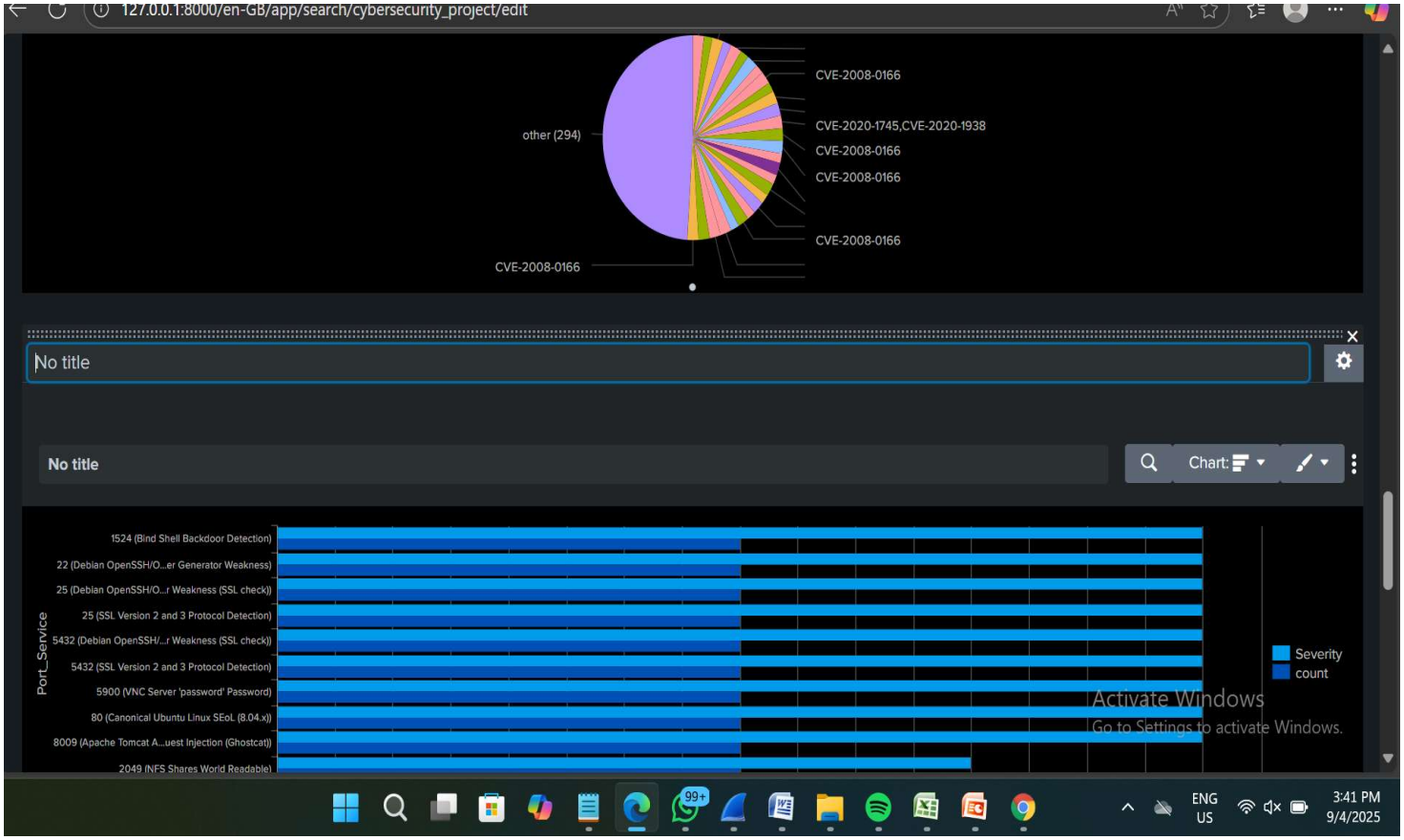
ip_addres	port	protocol	state	service
192.168.6	21	tcp	open	ftp
192.168.6	22	tcp	open	ssh
192.168.6	23	tcp	open	telnet
192.168.6	25	tcp	open	smtp
192.168.6	53	tcp	open	domain
192.168.6	80	tcp	open	http
192.168.6	111	tcp	open	rpcbind
192.168.6	139	tcp	open	netbios-ssn
192.168.6	445	tcp	open	netbios-ssn
192.168.6	512	tcp	open	exec
192.168.6	513	tcp	open	login
192.168.6	514	tcp	open	shell
192.168.6	1099	tcp	open	java-rmi
192.168.6	1524	tcp	open	bindshell
192.168.6	2049	tcp	open	nfs
192.168.6	2121	tcp	open	ccproxy-ftp
192.168.6	3306	tcp	open	mysql
192.168.6	5432	tcp	open	postgresql
192.168.6	5900	tcp	open	vnc
192.168.6	6000	tcp	open	X11
192.168.6	6667	tcp	open	irc
192.168.6	8009	tcp	open	ajp13

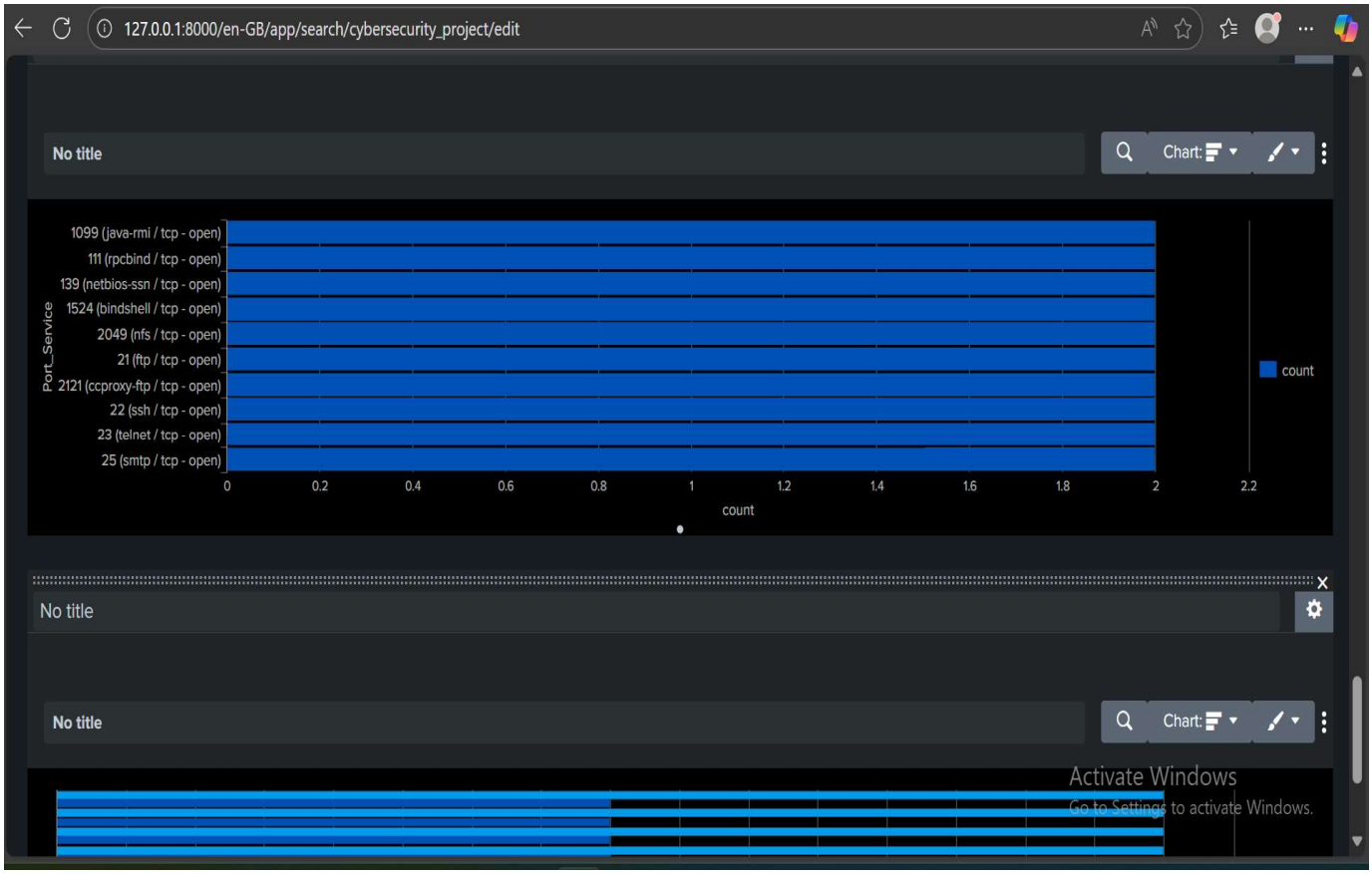
STEP 6:

Built Splunk dashboards showing **Top CVEs, open ports, and severity levels.**

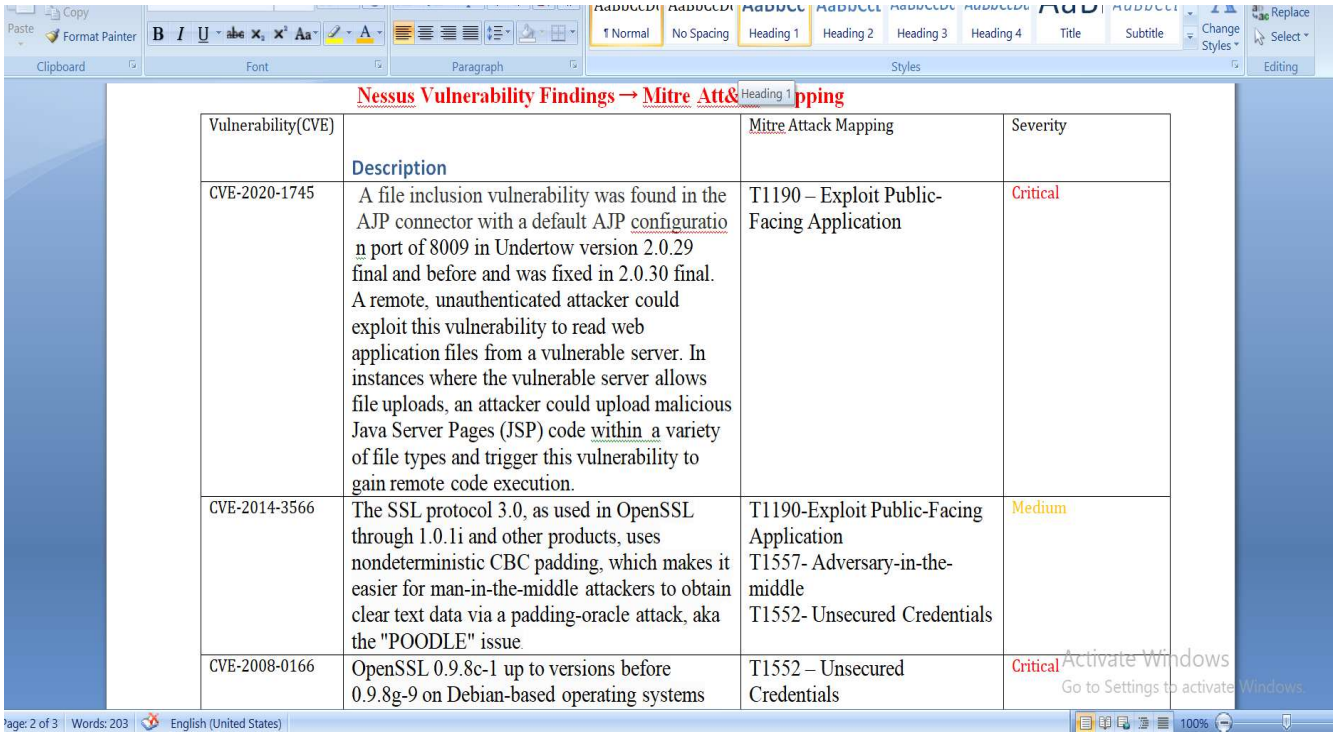

127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"nessus_scan2_2025_09_02.csv"%20host%3D"Kareemah"%20index%3D"vuln_scan"%20so...
source="nessus_scan2_2025_09_02.csv" host="Kareemah" index="vuln_scan" sourcetype="nessus_scan.csv"
All time
✓ 160 events (before 02/09/2025 05:07:39.000)
No Event Sampling
Job
Verbose Mode
Events (160)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Prev 1 2 3 4 5 6 7 8 Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Description 100
a extracted_Host 1
a index 1
linecount 11
PluginID 100
a PluginName 100
Port 33
Time
Event
02/09/2025 05:07:32.000
192.168.61.128,0,tcp,general,0,18261,Apache Banner Linux Distribution Disclosure,,None,Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.
host = Kareemah source = nessus_scan2_2025_09_02.csv sourcetype = nessus_scan.csv
02/09/2025 05:07:32.000
192.168.61.128,0,tcp,general,0,11936,OS Identification,,None,"Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system."
host = Kareemah source = nessus_scan2_2025_09_02.csv sourcetype = nessus_scan.csv
02/09/2025 05:07:32.000
192.168.61.128,0,tcp,general,0,209654,OS Fingerprints Detected,,None,"Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here."
host = Kareemah source = nessus_scan2_2025_09_02.csv sourcetype = nessus_scan.csv
Activate Windows
Go to Settings to activate Windows.
ENG US
5:08 AM 9/2/2025


127.0.0.1:8000/en-GB/app/search/search?earliest=0&latest=&q=search%20index%3D"vuln_scan"%20sourcetype%3D"csv"&sid=1756673895.6&display.p...
index="vuln_scan" sourcetype="csv"
All time
✓ 23 events (before 31/08/2025 21:58:16.000)
No Event Sampling
Job
Verbose Mode
Events (23)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Prev 1 2 Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a index 1
a ip_address 1
linecount 1
port 23
a protocol 1
a punct 2
a service 21
Time
Event
30/08/2025 15:52:18.000
192.168.61.128,8180,tcp,open,http
host = Kareemah source = nmap_scan.csv sourcetype = csv
30/08/2025 15:52:18.000
192.168.61.128,8009,tcp,open,ajp13
host = Kareemah source = nmap_scan.csv sourcetype = csv
30/08/2025 15:52:18.000
192.168.61.128,6667,tcp,open,irc
host = Kareemah source = nmap_scan.csv sourcetype = csv
30/08/2025 15:52:18.000
192.168.61.128,6000,tcp,open,X11
host = Kareemah source = nmap_scan.csv sourcetype = csv
30/08/2025 15:52:18.000
192.168.61.128,5900,tcp,open,vnc
host = Kareemah source = nmap_scan.csv sourcetype = csv
Search
ENG
10:02 PM


127.0.0.1:8000/en-GB/app/search/cybersecurity_project/edit
other (294)
CVE-2008-0166
CVE-2020-1745,CVE-2020-1938
CVE-2008-0166
CVE-2008-0166
CVE-2008-0166
CVE-2008-0166
No title
No title
Chart:
1524 (Bind Shell Backdoor Detection)
22 (Debian OpenSSH/O...er Generator Weakness)
25 (Debian OpenSSH/O...r Weakness (SSL check))
25 (SSL Version 2 and 3 Protocol Detection)
5432 (Debian OpenSSH/...r Weakness (SSL check))
5432 (SSL Version 2 and 3 Protocol Detection)
5900 (VNC Server 'password' Password)
80 (Canonical Ubuntu Linux SEoL (8.04.x))
8009 (Apache Tomcat A...uest Injection (Ghostcat))
2049 (NFS Shares World Readable)
Port_Service
Severity
count
Activate Windows
Go to Settings to activate Windows.
ENG
US
3:41 PM
9/4/2025


127.0.0.1:8000/en-GB/app/search/cybersecurity_project/edit
No title
Chart:
1099 (java-rmi / tcp - open)
111 (rpcbind / tcp - open)
139 (netbios-ssn / tcp - open)
1524 (bindshell / tcp - open)
2049 (nfs / tcp - open)
21 (ftp / tcp - open)
2121 (ccproxy-ftp / tcp - open)
22 (ssh / tcp - open)
23 (telnet / tcp - open)
25 (smtp / tcp - open)
Port_Service
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2
2.2
count
count
No title
No title
Chart:
Activate Windows
Go to Settings to activate Windows.

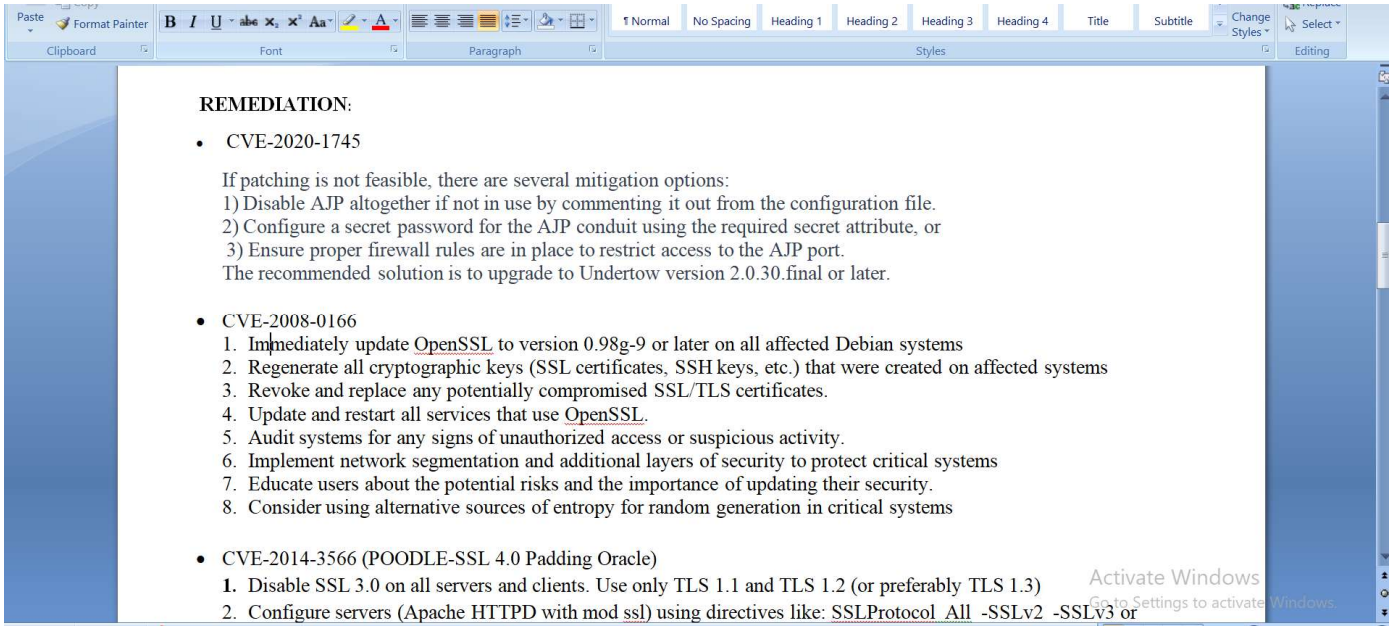
STEP 7: Mapped key vulnerabilities to **MITRE ATT&CK techniques**



Nessus Vulnerability Findings → Mitre Att&ck Mapping

Vulnerability(CVE)	Description	Mitre Attack Mapping	Severity
CVE-2020-1745	A file inclusion vulnerability was found in the AJP connector with a default AJP configuration port of 8009 in Undertow version 2.0.29 final and before and was fixed in 2.0.30 final. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious Java Server Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution.	T1190 – Exploit Public-Facing Application	Critical
CVE-2014-3566	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain clear text data via a padding-oracle attack, aka the "POODLE" issue.	T1190-Exploit Public-Facing Application T1557- Adversary-in-the-middle T1552- Unsecured Credentials	Medium
CVE-2008-0166	OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems	T1552 – Unsecured Credentials	Critical

STEP 8: Suggested **remediation** for high-severity CVEs.



REMEDIATION:

- CVE-2020-1745

  If patching is not feasible, there are several mitigation options:
  1) Disable AJP altogether if not in use by commenting it out from the configuration file.
  2) Configure a secret password for the AJP conduit using the required secret attribute, or
  3) Ensure proper firewall rules are in place to restrict access to the AJP port.
  The recommended solution is to upgrade to Undertow version 2.0.30.final or later.

- CVE-2008-0166
  1. Immediately update OpenSSL to version 0.98g-9 or later on all affected Debian systems
  2. Regenerate all cryptographic keys (SSL certificates, SSH keys, etc.) that were created on affected systems
  3. Revoke and replace any potentially compromised SSL/TLS certificates.
  4. Update and restart all services that use OpenSSL.
  5. Audit systems for any signs of unauthorized access or suspicious activity.
  6. Implement network segmentation and additional layers of security to protect critical systems
  7. Educate users about the potential risks and the importance of updating their security.
  8. Consider using alternative sources of entropy for random generation in critical systems

- CVE-2014-3566 (POODLE-SSL 4.0 Padding Oracle)
  1. Disable SSL 3.0 on all servers and clients. Use only TLS 1.1 and TLS 1.2 (or preferably TLS 1.3)
  2. Configure servers (Apache HTTPD with mod ssl) using directives like: SSLProtocol All -SSLv2 -SSLv3 or

This project successfully simulated a real-world **SOC Analyst workflow**, starting from reconnaissance to vulnerability detection, analysis, and remediation. Using **Nmap**, I identified open ports and services on the target machine. With **Nessus**, I performed a vulnerability scan that revealed multiple high-risk CVEs, which were then mapped to the **MITRE ATT&CK framework** to understand how adversaries could exploit them. Finally, results were ingested into **Splunk**, where dashboards were built to visualize top vulnerabilities.

This project emphasized the critical SOC responsibility of turning raw vulnerability data into **actionable intelligence** for decision-makers.