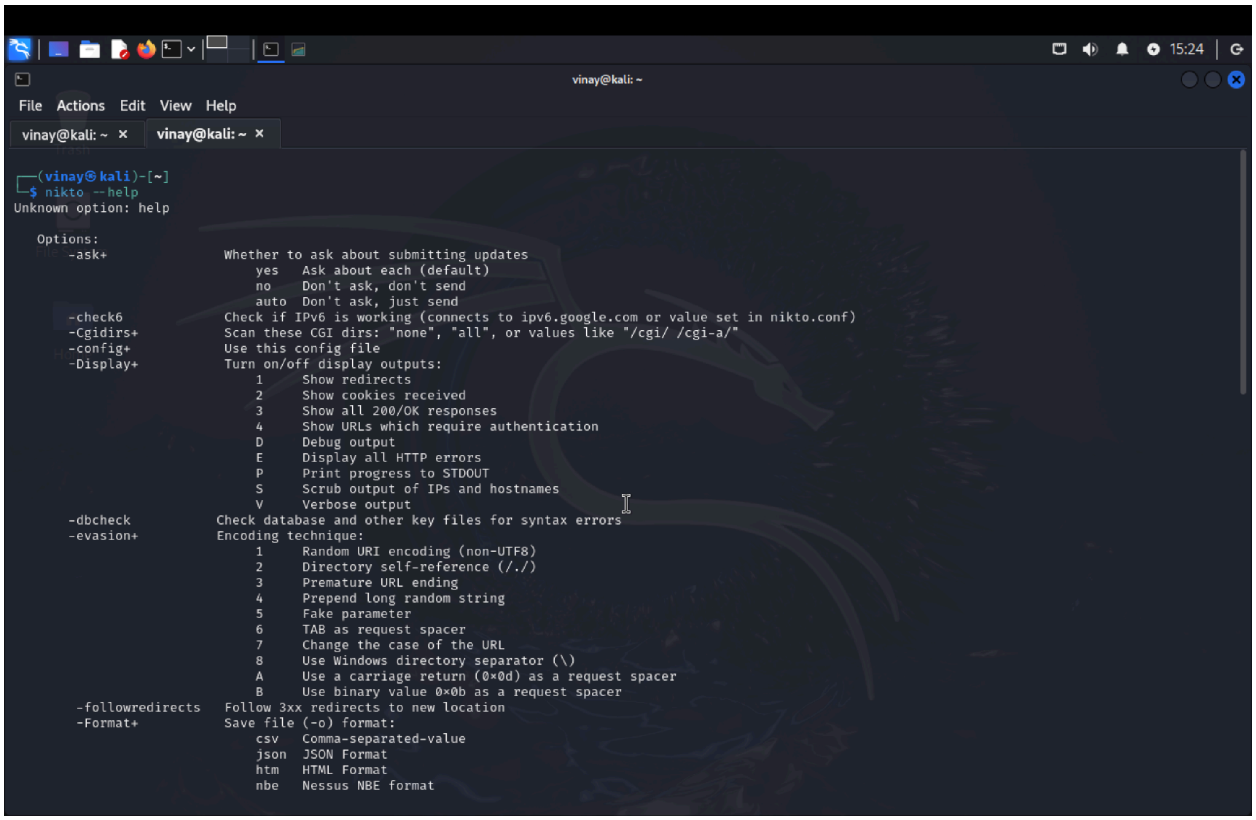
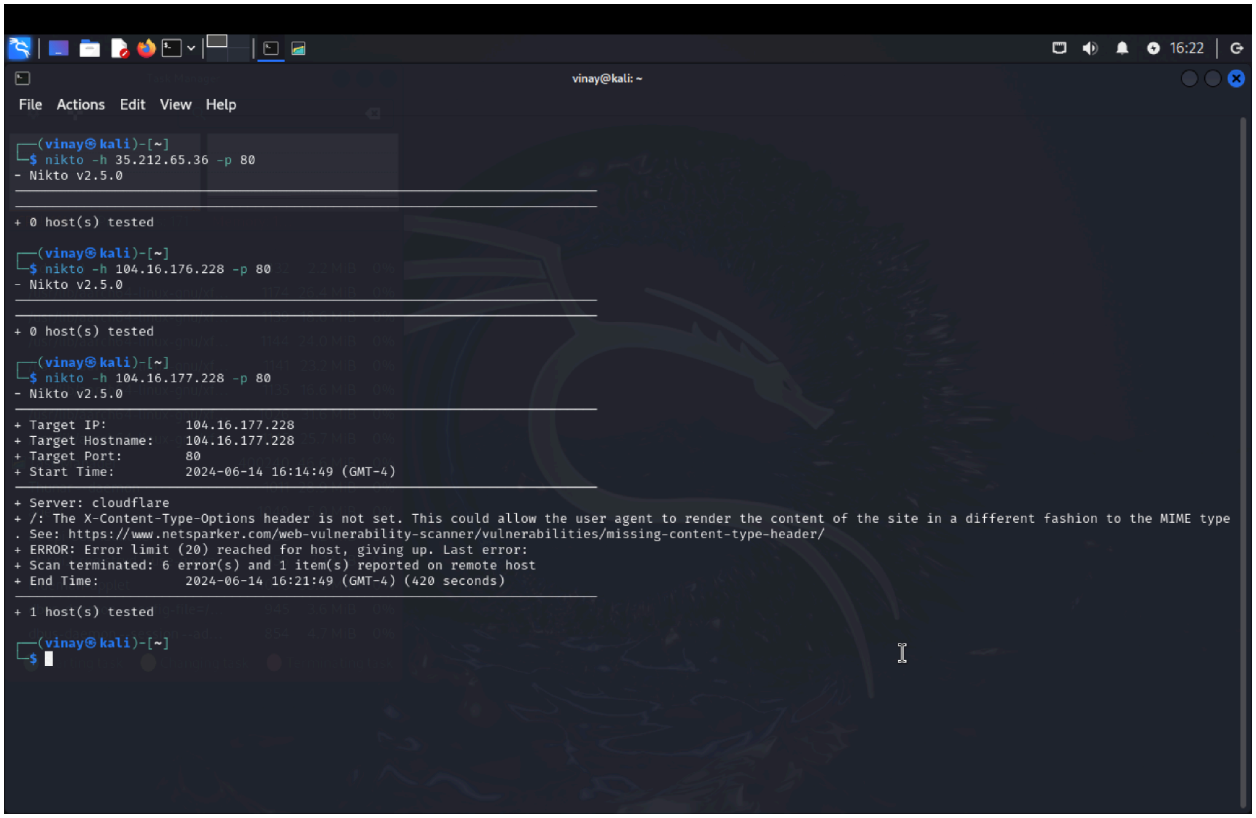
In Phase 2 of the penetration test, we will use tools to find and connect to the target hosts, so we can discover possible ways to attack the system. We will collect information about usernames, group names, hostnames, network shares, services, IP tables, routing tables, service settings, audit configurations, application details, banners, SNMP details, and DNS details. Before the real test, we will practice using these tools in the lab environment at Artemis Company. The tools we will use are:

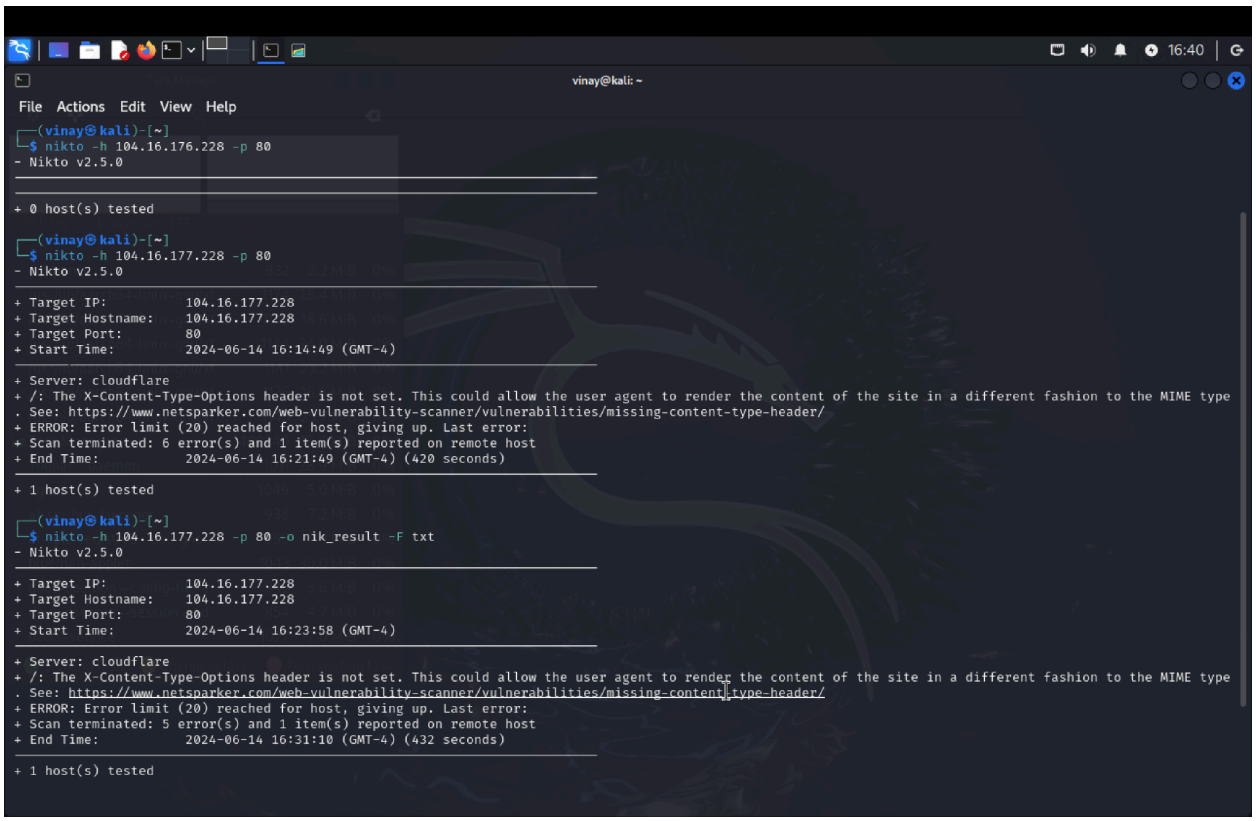
Tool 1:NIKTO:

The NIKTO tool is a computer program that helps to find security vulnerabilities on websites or web servers. It works by scanning the website's code and configuration settings to identify potential weaknesses that hackers could exploit. Once these vulnerabilities are identified, website owners can take steps to fix them and make their website more secure. Using the NIKTO tool can help protect sensitive information and prevent cyber attacks.

Website owners should regularly use the NIKTO tool to ensure their website is secure from potential threats. By running regular scans with the NIKTO tool, they can stay one step ahead of hackers and protect their website and user data. It is important to address any vulnerabilities identified by the NIKTO tool promptly to maintain a safe and secure online presence. By using tools like NIKTO, website owners can proactively protect their websites against cybersecurity threats.



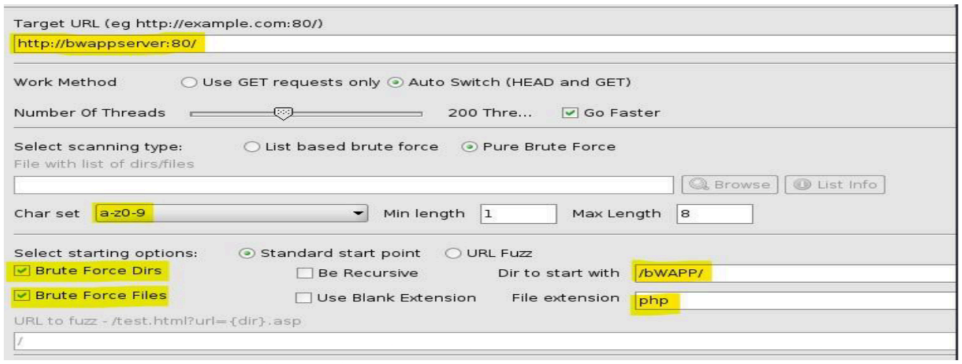

16:22
vinay@kali: ~
File Actions Edit View Help
(vinay㉿kali)-[~]
$ nikto -h 35.212.65.36 -p 80
- Nikto v2.5.0
+ 0 host(s) tested
(vinay㉿kali)-[~]
$ nikto -h 104.16.176.228 -p 80
- Nikto v2.5.0
+ 0 host(s) tested
(vinay㉿kali)-[~]
$ nikto -h 104.16.177.228 -p 80
- Nikto v2.5.0
+ Target IP: 104.16.177.228
+ Target Hostname: 104.16.177.228
+ Target Port: 80
+ Start Time: 2024-06-14 16:14:49 (GMT-4)
+ Server: cloudflare
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 6 error(s) and 1 item(s) reported on remote host
+ End Time: 2024-06-14 16:21:49 (GMT-4) (420 seconds)
+ 1 host(s) tested
(vinay㉿kali)-[~]
$

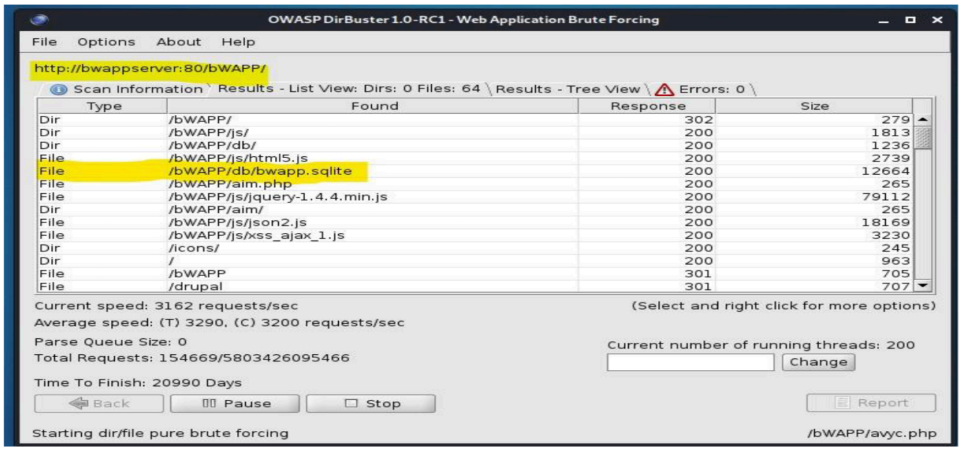

16:40
vinay@kali: ~
File Actions Edit View Help
(vinay㉿kali)-[~]
$ nikto -h 104.16.176.228 -p 80
- Nikto v2.5.0
+ 0 host(s) tested
(vinay㉿kali)-[~]
$ nikto -h 104.16.177.228 -p 80
- Nikto v2.5.0
+ Target IP: 104.16.177.228
+ Target Hostname: 104.16.177.228
+ Target Port: 80
+ Start Time: 2024-06-14 16:14:49 (GMT-4)
+ Server: cloudflare
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 6 error(s) and 1 item(s) reported on remote host
+ End Time: 2024-06-14 16:21:49 (GMT-4) (420 seconds)
+ 1 host(s) tested
(vinay㉿kali)-[~]
$ nikto -h 104.16.177.228 -p 80 -o nik_result -F txt
- Nikto v2.5.0
+ Target IP: 104.16.177.228
+ Target Hostname: 104.16.177.228
+ Target Port: 80
+ Start Time: 2024-06-14 16:23:58 (GMT-4)
+ Server: cloudflare
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 5 error(s) and 1 item(s) reported on remote host
+ End Time: 2024-06-14 16:31:10 (GMT-4) (432 seconds)
+ 1 host(s) tested

Tool2: Dirbuster

The DirBuster tool is a helpful software used by cybersecurity experts to find hidden directories on websites. It works by scanning a website and looking for directories that may not be easily visible to the public. This tool is important because it helps identify potential security risks and vulnerabilities on a website, allowing the website owner to fix them before they can be exploited by hackers. By using DirBuster, cybersecurity professionals can strengthen the overall security of a website and protect it from potential cyber attacks.

One of the key features of the DirBuster tool is its ability to automate the process of directory discovery, saving time and effort for cybersecurity professionals. With just a few clicks, users can scan a website and quickly uncover hidden directories that may pose a security threat. This automated process not only speeds up the security analysis of a website but also ensures that no potentially vulnerable directories are overlooked. Overall, DirBuster is a valuable tool in the cybersecurity toolbox, helping professionals proactively identify and address website vulnerabilities.





Tool3:Nmap

Nmap enumeration is a method used to discover and analyze information about computer networks. It helps identify open ports, services, and potential vulnerabilities in a network. By sending specific packets to target devices, Nmap gathers data on how they are configured and what services they are running. This information can help network administrators and security professionals understand the layout of a network and assess its security posture. Nmap enumeration is a valuable tool for strengthening network defenses and preventing unauthorized access.

When conducting Nmap enumeration, it is important to have permission from the network owner to avoid violating any laws or policies. Ethical use of Nmap involves respecting privacy and confidentiality while assessing network security. It is crucial to document and analyze the results of Nmap scans carefully to make informed decisions about improving network security. By employing Nmap enumeration responsibly, organizations can enhance their cybersecurity measures and protect sensitive data from potential threats.

-> nmap -sn 192.168.134.0/24

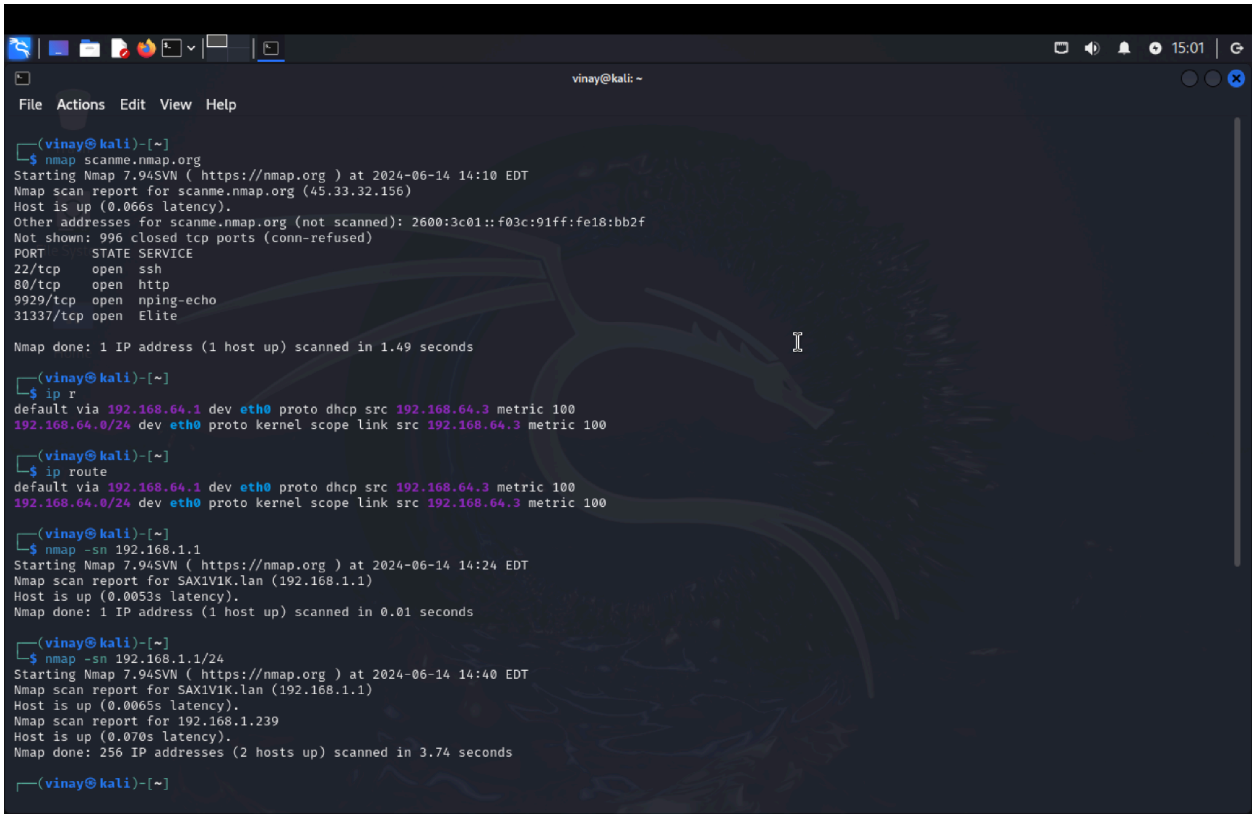
Ping sweep the network (pinging range of IP addresses)

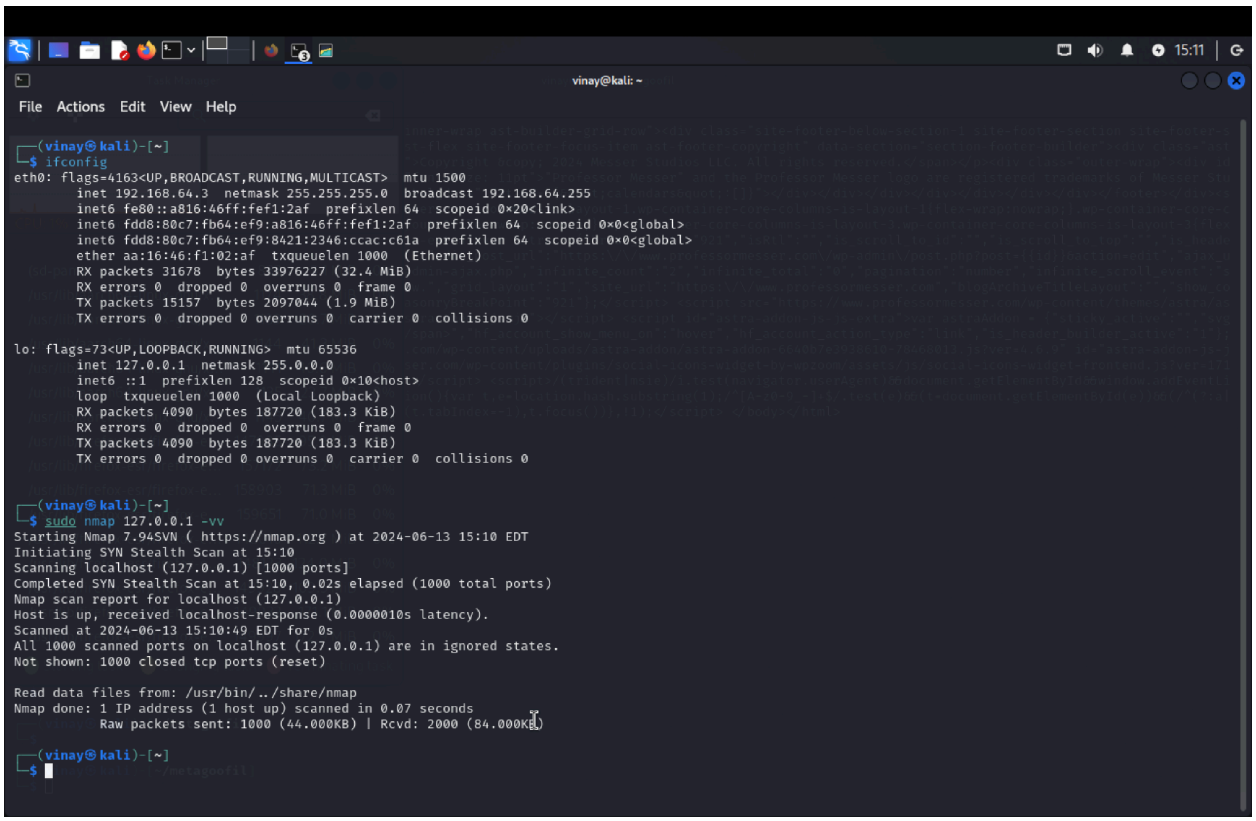
-> nmap -p -sV 192.168.134.0/24

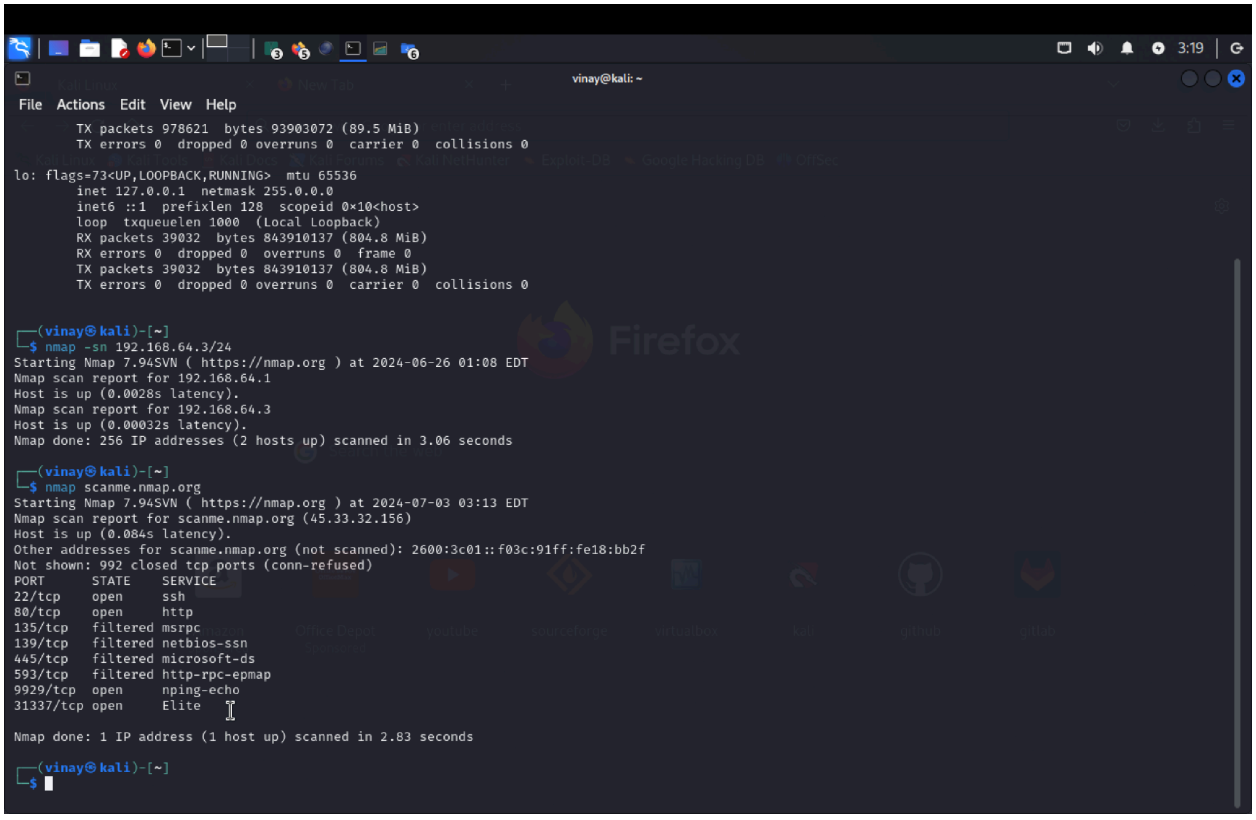
Full TCP port scan with service version detection

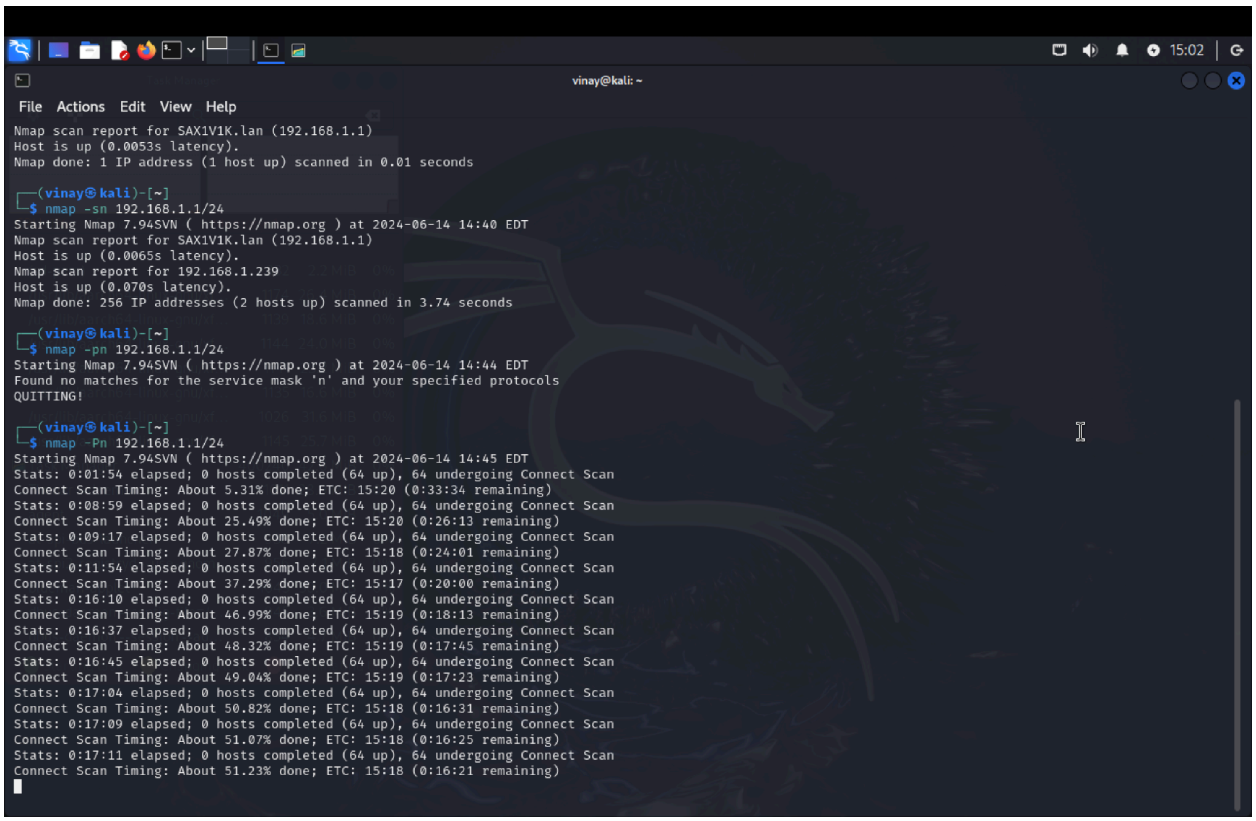
-> nmap -v -A -T4 192.168.134.0/24

Aggressive scan (-A) with faster speed (-T4). Aggressive scan is a combination of OS detection -O), version scanning (-sV) and script scanning (-sC). The Nmap Scripting Engine (NSE) scripts have associated categories (safe, intrusive, malware, backdoor, version, discovery, and vulnerability).


15:01
vinay@kali: ~
File Actions Edit View Help
┌──(vinay㉿kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-14 14:10 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.066s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
┌──(vinay㉿kali)-[~]
└─$ ip r
default via 192.168.64.1 dev eth0 proto dhcp src 192.168.64.3 metric 100
192.168.64.0/24 dev eth0 proto kernel scope link src 192.168.64.3 metric 100
┌──(vinay㉿kali)-[~]
└─$ ip route
default via 192.168.64.1 dev eth0 proto dhcp src 192.168.64.3 metric 100
192.168.64.0/24 dev eth0 proto kernel scope link src 192.168.64.3 metric 100
┌──(vinay㉿kali)-[~]
└─$ nmap -sn 192.168.1.1
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-14 14:24 EDT
Nmap scan report for SAX1V1K.lan (192.168.1.1)
Host is up (0.0053s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
┌──(vinay㉿kali)-[~]
└─$ nmap -sn 192.168.1.1/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-14 14:40 EDT
Nmap scan report for SAX1V1K.lan (192.168.1.1)
Host is up (0.0065s latency).
Nmap scan report for 192.168.1.239
Host is up (0.070s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.74 seconds
┌──(vinay㉿kali)-[~]


15:11
vinay@kali: ~
File Actions Edit View Help
┌──(vinay㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.64.3 netmask 255.255.255.0 broadcast 192.168.64.255
inet6 fe80::a816:46ff:fef1:2af prefixlen 64 scopeid 0×20<link>
inet6 fdd8:80c7:fb64:ef9:a816:46ff:fef1:2af prefixlen 64 scopeid 0×0<global>
inet6 fdd8:80c7:fb64:ef9:8421:2346:ccac:c61a prefixlen 64 scopeid 0×0<global>
ether aa:16:46:f1:02:af txqueuelen 1000 (Ethernet)
RX packets 31678 bytes 33976227 (32.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 15157 bytes 2097044 (1.9 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4090 bytes 187720 (183.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4090 bytes 187720 (183.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(vinay㉿kali)-[~]
└─$ sudo nmap 127.0.0.1 -vv
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-13 15:10 EDT
Initiating SYN Stealth Scan at 15:10
Scanning localhost (127.0.0.1) [1000 ports]
Completed SYN Stealth Scan at 15:10, 0.02s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.0000010s latency).
Scanned at 2024-06-13 15:10:49 EDT for 0s
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2000 (84.000KB)
┌──(vinay㉿kali)-[~]
└─$

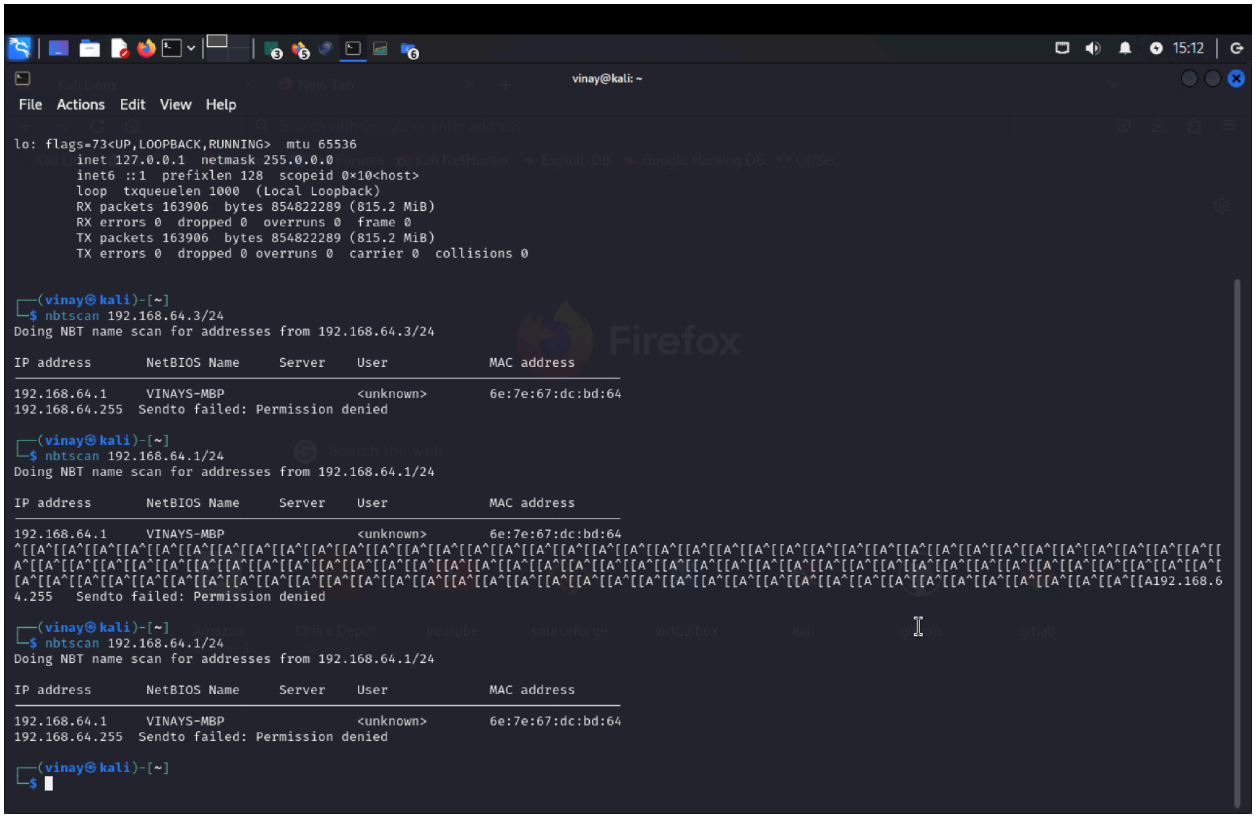

3:19
vinay@kali: ~
File Actions Edit View Help
TX packets 978621 bytes 93903072 (89.5 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 39032 bytes 843910137 (804.8 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 39032 bytes 843910137 (804.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(vinay㉿kali)-[~]
$ nmap -sn 192.168.64.3/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-26 01:08 EDT
Nmap scan report for 192.168.64.1
Host is up (0.0028s latency).
Nmap scan report for 192.168.64.3
Host is up (0.00032s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.06 seconds
(vinay㉿kali)-[~]
$ nmap scanme.nmap.org
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-03 03:13 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.084s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
(vinay㉿kali)-[~]
$

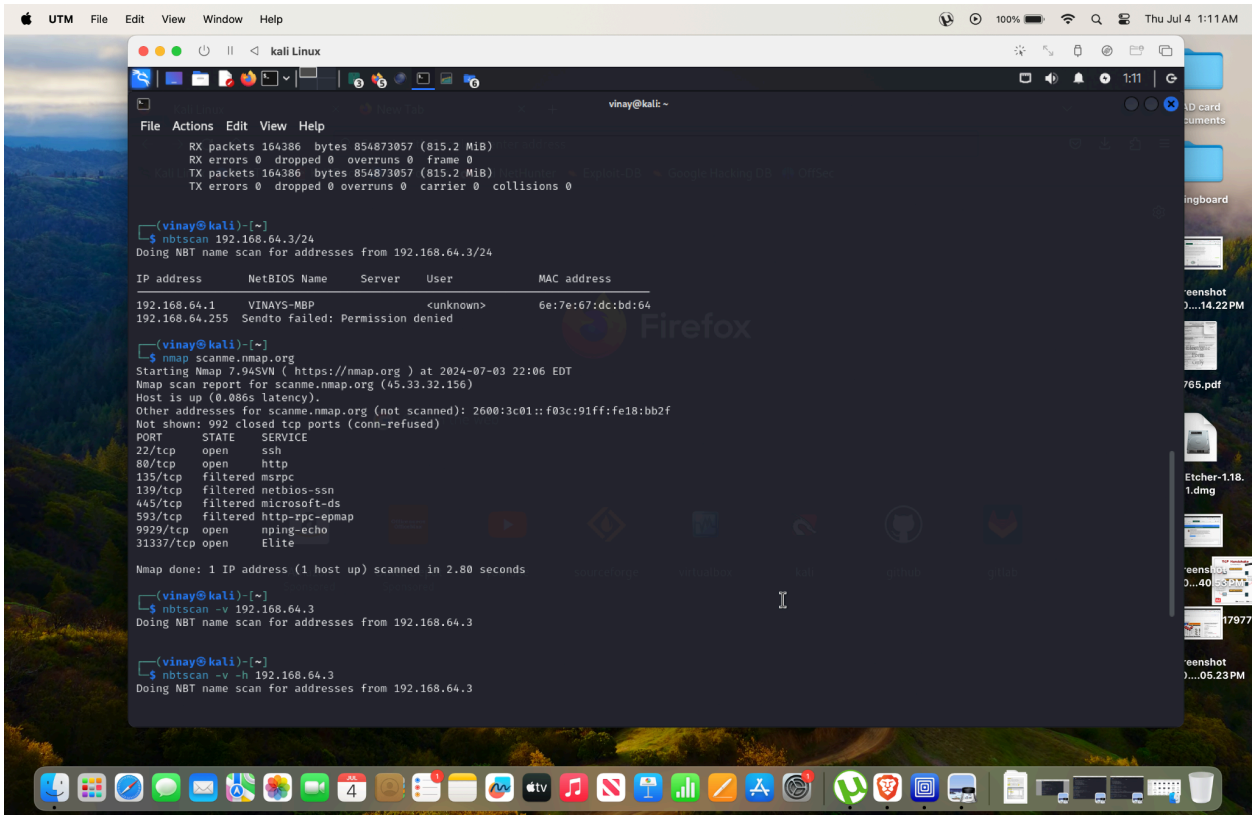

15:02
vinay@kali: ~
File Actions Edit View Help
Nmap scan report for SAX1V1K.lan (192.168.1.1)
Host is up (0.0053s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
(vinay㉿kali)-[~]
$ nmap -sn 192.168.1.1/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-14 14:40 EDT
Nmap scan report for SAX1V1K.lan (192.168.1.1)
Host is up (0.0065s latency).
Nmap scan report for 192.168.1.239
Host is up (0.070s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.74 seconds
(vinay㉿kali)-[~]
$ nmap -pn 192.168.1.1/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-14 14:44 EDT
Found no matches for the service mask 'n' and your specified protocols
QUITTING!
(vinay㉿kali)-[~]
$ nmap -Pn 192.168.1.1/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-14 14:45 EDT
Stats: 0:01:54 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 5.31% done; ETC: 15:20 (0:33:34 remaining)
Stats: 0:08:59 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 25.49% done; ETC: 15:20 (0:26:13 remaining)
Stats: 0:09:17 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 27.87% done; ETC: 15:18 (0:24:01 remaining)
Stats: 0:11:54 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 37.29% done; ETC: 15:17 (0:20:00 remaining)
Stats: 0:16:10 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 46.99% done; ETC: 15:19 (0:18:13 remaining)
Stats: 0:16:37 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 48.32% done; ETC: 15:19 (0:17:45 remaining)
Stats: 0:16:45 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 49.04% done; ETC: 15:19 (0:17:23 remaining)
Stats: 0:17:04 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 50.82% done; ETC: 15:18 (0:16:31 remaining)
Stats: 0:17:09 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 51.07% done; ETC: 15:18 (0:16:25 remaining)
Stats: 0:17:11 elapsed; 0 hosts completed (64 up), 64 undergoing Connect Scan
Connect Scan Timing: About 51.23% done; ETC: 15:18 (0:16:21 remaining)

Tool 5:NbtScan:-

"Nbtscan" is a computer program used to scan networks and identify devices connected to them. It works by sending out messages to devices on the network and waiting for responses. Once a response is received, nbtscan collects information about the device, such as its IP address and hostname. This information can be useful for network administrators to monitor and manage their networks effectively.

Network administrators can use nbtscan to quickly identify and locate devices on their network, which can help them troubleshoot any connectivity issues. By knowing which devices are connected to the network, administrators can also ensure that unauthorized devices are not accessing sensitive information. Overall, nbtscan is a valuable tool for maintaining the security and efficiency of a network.


15:12
vinay@kali: ~
File Actions Edit View Help
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 163906 bytes 854822289 (815.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 163906 bytes 854822289 (815.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(vinay㉿kali)-[~]
$ nbtscan 192.168.64.3/24
Doing NBT name scan for addresses from 192.168.64.3/24
IP address NetBIOS Name Server User MAC address
192.168.64.1 VINAYS-MBP <unknown> 6e:7e:67:dc:bd:64
192.168.64.255 Sendto failed: Permission denied
(vinay㉿kali)-[~]
$ nbtscan 192.168.64.1/24
Doing NBT name scan for addresses from 192.168.64.1/24
IP address NetBIOS Name Server User MAC address
192.168.64.1 VINAYS-MBP <unknown> 6e:7e:67:dc:bd:64
192.168.64.255 Sendto failed: Permission denied
(vinay㉿kali)-[~]
$ nbtscan 192.168.64.1/24
Doing NBT name scan for addresses from 192.168.64.1/24
IP address NetBIOS Name Server User MAC address
192.168.64.1 VINAYS-MBP <unknown> 6e:7e:67:dc:bd:64
192.168.64.255 Sendto failed: Permission denied
(vinay㉿kali)-[~]
$


UTM File Edit View Window Help
Thu Jul 4 1:11 AM
kali Linux
vinay@kali: ~
File Actions Edit View Help
RX packets 164386 bytes 854873057 (815.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 164386 bytes 854873057 (815.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(vinay㉿kali)-[~]
$ nbtscan 192.168.64.3/24
Doing NBT name scan for addresses from 192.168.64.3/24
IP address NetBIOS Name Server User MAC address
192.168.64.1 VINAYS-MBP <unknown> 6e:7e:67:dc:bd:64
192.168.64.255 Sendto failed: Permission denied
(vinay㉿kali)-[~]
$ nmap scanme.nmap.org
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-03 22:06 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.086s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
(vinay㉿kali)-[~]
$ nbtscan -v 192.168.64.3
Doing NBT name scan for addresses from 192.168.64.3
(vinay㉿kali)-[~]
$ nbtscan -v -h 192.168.64.3
Doing NBT name scan for addresses from 192.168.64.3

Tool5: Dns (domain name service) is mainly intended as a hierarchical decentralized service. Any resource connected to the network that has the primary function is referred to as a distributed naming scheme. The use of ip addresses to hostnames is a common practice. Dns enumeration reveals some of the record types that are not identified by the database. The following are the points: Records with the start of authority (soa) that contain important information about a domain containing important data. A record that contains ip addresses. Nameserver (ns) records that contain information about the nameservers. Smtp mail exchanger (mx) records.

The process of dns enumeration involves the process of transferring zone transfer requests to the enumerator. Dns primary server pretending to be a client.. The pentester can use DNS enumeration to evaluate the results of the requests which will reveal confidential domain records. DNS enumeration was performed using dnsrecon on the private network in the lab. Dnsrecon wasused on the http://winserver.artemisdev.com which is redirected to https://artemisdev.000webhostapp.com . The diagrams below show SOA records, the NS records, and the CNAME records and the corresponding IP address.