Network Security Assessment Report

I. Introduction

The purpose of this report to conduct a comprehensive scan of the home network, including all connected devices such as routers, computers, smartphones and other IoT devices. This is done in order to identify any potential security vulnerabilities, such as open ports, default passwords and outdated firmware. In an era where digital threats are becoming increasingly sophisticated, ensuring the security of personal networks is paramount for protecting sensitive information and preventing unauthorised access.

II. Methodology

Tools Used:

1. Ifconfig: displays information about all active network interface
2. Nmap: Used for port scanning and identifying services running on devices
3. Metasploit: Used for exploiting known vulnerabilities for penetration testing
4. Nikto: Used for scanning web servers to detect outdated software and potentially dangerous files/script
5. Arp: Used for discovering active IP addresses in the local network

Procedures:

1. External IP Identification: Utilized online services such as "whatismyip.com" to determine the external IP address of the network
2. Nmap Scanning: Conducted scans using Nmap to identify open ports on the network's devices and any services that were running on these ports
3. Metasploit Utilization: Utilized Metasploit for further investigation into potential vulnerabilities discovered during the Nmap scan
4. Nikto Web Server Analysis: Ran Nikto against identified web servers to uncover common misconfigurations, outdated software, and other vulnerabilities
5. Arp Network Mapping: Performed ARP scanning to list all the devices connected to the local network, including hardware addresses

III. Findings

1. External IP address of router
    - IP Discovery: The external IP address was identified using online IP lookup services (https://www.whatismyip.com/). The router IP's address was found to be: 130.208.24.1 and my personal computer's IP address was found to be: 130.208.26.47.
    - Admin Login Review: The router's admin login was examined and found to be secured by a password, and not the default credentials, which is a positive security measure.

2. Local Network Scan
    - Device Detection: Multiple devices including personal computers, smartphones were detected.

- Open Ports: Open ports such as 22 (SSH), 80 (HTTP), and 443 (HTTPS) were found, which could be entry points for attackers if not properly secured.
- Open Port Analysis: Several devices had open ports that are known to be used by common services, but the presence of services like Telnet on some devices posed a potential security risk due to the unencrypted nature of the protocol.

3. Port Scan Results

Target Host: The port scan was conducted on the host with the IP address 130.208.24.1.
Open Ports: The scan revealed several open TCP ports on the target host:

- Port 22 (SSH): Open, running Cisco SSH 1.25 (protocol 2.0).
- Port 23 (Telnet): Open, identified as Cisco router Telnet service.
- Port 80 (HTTP): Open, running an OpenResty web app server, which is a web platform based on nginx.
- Port 443 (HTTPS): Open, also running an OpenResty web app server.
- Port 830: Open, service not identified.

4. Service Identification

- Secure Shell (SSH) on Port 22: The SSH service is using version 1.25, which may indicate a specific range of Cisco devices. It's essential to ensure this service is updated and properly configured, as SSH is commonly targeted for brute force attacks.
- Telnet on Port 23: The presence of an open Telnet port is unusual due to the unencrypted nature of Telnet communication, which could allow for credential sniffing. It is generally recommended to disable Telnet in favor of SSH.
- HTTP and HTTPS on Ports 80 and 443: Both ports are serving web applications via OpenResty. It's important to regularly update such web servers and check for misconfigurations that could lead to vulnerabilities.
- Unidentified Service on Port 830: This port did not return a recognizable service during the scan. Further investigation is needed to determine the service running on this port and assess its security posture.

5. Device Information

The scan detected that the target device is a Cisco router with an IOS operating system. This information can be used to check against known vulnerabilities specific to the device's make and model.

IV. Discussion

- Unauthorized Access: The presence of SSH and Telnet services indicates potential channels for unauthorized access. Secure configuration and strong authentication mechanisms are required to prevent such access.
- Data Exposure: Unencrypted services like Telnet could lead to sensitive information being exposed over the network.
- Web Server Exploits: Given that HTTP and HTTPS services are running, there may be web application vulnerabilities that could be exploited. Regular application scanning and updates are recommended.

VI. Recommendations

Based on the findings of this scan, the following actions are recommended:

- Close unnecessary open ports
- Update router and device firmware
- Change default passwords
- Regular Monitoring: Establish a routine for regular network scans and updates.
- Telnet Service Review: It is advisable to disable the Telnet service due to its unsecured communication protocol and replace it with SSH, which offers encrypted communication.
- Port 830 Investigation: Further investigation into the unidentified service running on port 830 is needed to understand its purpose and to secure it appropriately.

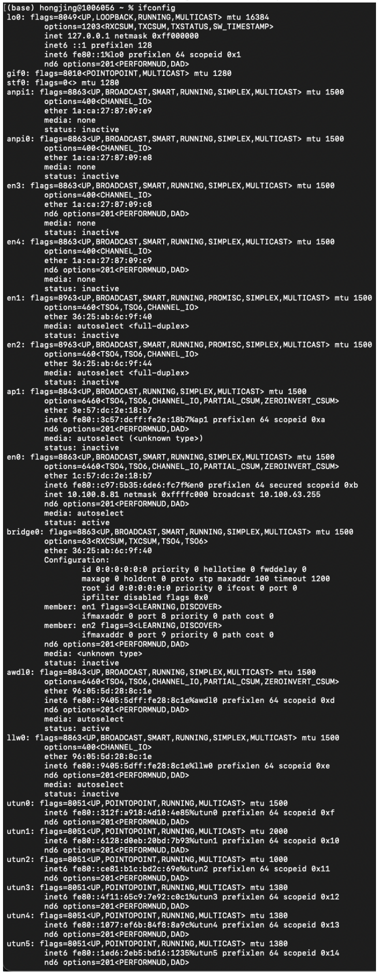
VII. Conclusion

Conducting regular network security scans is crucial for:

- Identifying and mitigating vulnerabilities before they can be exploited
- Ensuring that all devices are updated and secured against known threats
- Protecting sensitive personal and professional information from unauthorised access
- Maintaining the overall health and security of the home network

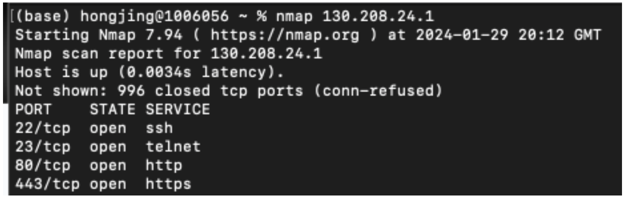
VIII. Appendices

1. Ifconfig to display all active network interface



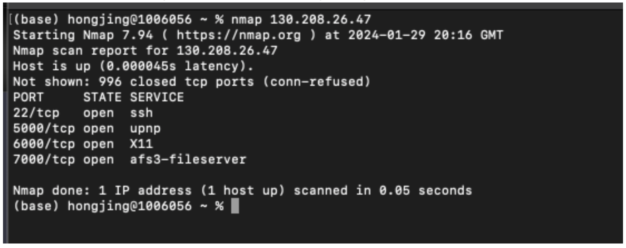
```
(base) hongjing@1006056 ~ % ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
	options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
	inet 127.0.0.1 netmask 0xff000000
	inet6 ::1 prefixlen 128
	inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
	nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=400<CHANNEL_IO>
	ether 1a:ca:27:87:09:e9
	media: none
	status: inactive
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=400<CHANNEL_IO>
	ether 1a:ca:27:87:09:e8
	media: none
	status: inactive
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=400<CHANNEL_IO>
	ether 1a:ca:27:87:09:c8
	nd6 options=201<PERFORMNUD,DAD>
	media: none
	status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=400<CHANNEL_IO>
	ether 1a:ca:27:87:09:c9
	nd6 options=201<PERFORMNUD,DAD>
	media: none
	status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
	options=460<TSO4,TSO6,CHANNEL_IO>
	ether 36:25:ab:6c:9f:40
	media: autoselect <full-duplex>
	status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
	options=460<TSO4,TSO6,CHANNEL_IO>
	ether 36:25:ab:6c:9f:44
	media: autoselect <full-duplex>
	status: inactive
ap1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
	ether 3e:57:dc:2e:18:b7
	inet6 fe80::3c57:dcff:fe2e:18b7%ap1 prefixlen 64 scopeid 0xa
	nd6 options=201<PERFORMNUD,DAD>
	media: autoselect (<unknown type>)
	status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
	ether 1c:57:dc:2e:18:b7
	inet6 fe80::c97:5b35:6de6:fc7f%en0 prefixlen 64 secured scopeid 0xb
	inet 10.100.8.81 netmask 0xffffc000 broadcast 10.100.63.255
	nd6 options=201<PERFORMNUD,DAD>
	media: autoselect
	status: active
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=63<RXCSUM,TXCSUM,TSO4,TSO6>
	ether 36:25:ab:6c:9f:40
	Configuration:
		id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
		maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
		root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
		ipfilter disabled flags 0x0
	member: en1 flags=3<LEARNING,DISCOVER>
	        ifmaxaddr 0 port 8 priority 0 path cost 0
	member: en2 flags=3<LEARNING,DISCOVER>
	        ifmaxaddr 0 port 9 priority 0 path cost 0
	nd6 options=201<PERFORMNUD,DAD>
	media: <unknown type>
	status: inactive
awdl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
	ether 96:05:5d:28:8c:1e
	inet6 fe80::9405:5dff:fe28:8c1e%awdl0 prefixlen 64 scopeid 0xd
	nd6 options=201<PERFORMNUD,DAD>
	media: autoselect
	status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
	options=400<CHANNEL_IO>
	ether 96:05:5d:28:8c:1e
	inet6 fe80::9405:5dff:fe28:8c1e%llw0 prefixlen 64 scopeid 0xe
	nd6 options=201<PERFORMNUD,DAD>
	media: autoselect
	status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
	inet6 fe80::312f:a918:4d10:4e85%utun0 prefixlen 64 scopeid 0xf
	nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
	inet6 fe80::6128:d0eb:20bd:7b93%utun1 prefixlen 64 scopeid 0x10
	nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
	inet6 fe80::ce81:b1c:bd2c:69e%utun2 prefixlen 64 scopeid 0x11
	nd6 options=201<PERFORMNUD,DAD>
utun3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
	inet6 fe80::4f11:65c9:7e92:c0c1%utun3 prefixlen 64 scopeid 0x12
	nd6 options=201<PERFORMNUD,DAD>
utun4: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
	inet6 fe80::1077:ef6b:84f8:8a9c%utun4 prefixlen 64 scopeid 0x13
	nd6 options=201<PERFORMNUD,DAD>
utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
	inet6 fe80::1ed6:2eb5:bd16:1235%utun5 prefixlen 64 scopeid 0x14
	nd6 options=201<PERFORMNUD,DAD>
```

2. Nmap scan for router



```
(base) hongjing@1006056 ~ % nmap 130.208.24.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 20:12 GMT
Nmap scan report for 130.208.24.1
Host is up (0.0034s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
```

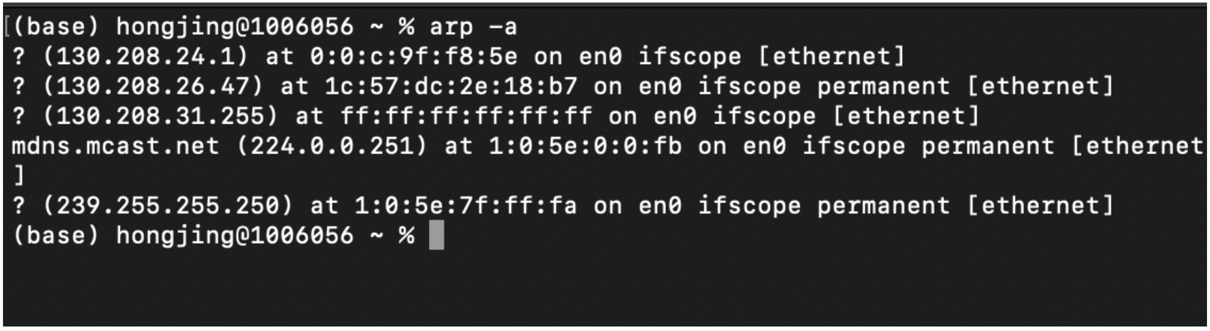
3. Nmap scan for laptop



```
(base) hongjing@1006056 ~ % nmap 130.208.26.47
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 20:16 GMT
Nmap scan report for 130.208.26.47
Host is up (0.000045s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp
6000/tcp open  X11
7000/tcp open  afs3-fileserver

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
(base) hongjing@1006056 ~ %
```

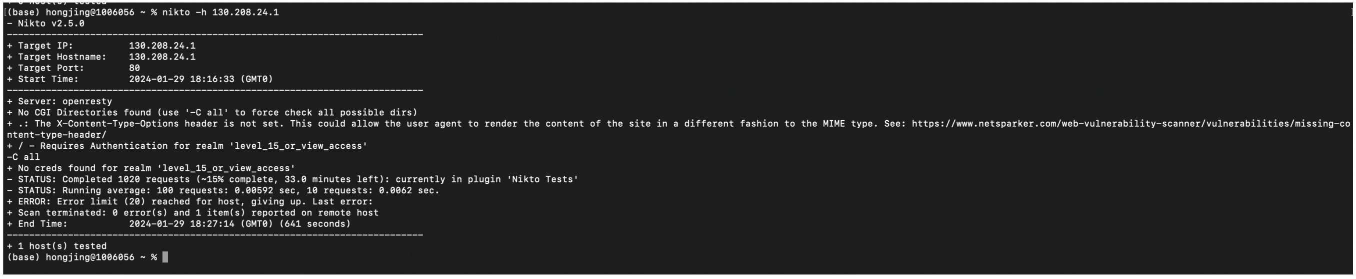
4. Arp -a to show ARP table of my machine



```
(base) hongjing@1006056 ~ % arp -a
? (130.208.24.1) at 0:0:c:9f:f8:5e on en0 ifscope [ethernet]
? (130.208.26.47) at 1c:57:dc:2e:18:b7 on en0 ifscope permanent [ethernet]
? (130.208.31.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet
]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
(base) hongjing@1006056 ~ %
```

The output of the arp -a command shows the ARP (Address Resolution Protocol) table of my machine. This table maps IP addresses to their corresponding physical MAC (Media Access Control) addresses on the local network.

5. Using `nikto -h 130.208.24.1`



```
(base) hongjing@1006056 ~ % nikto -h 130.208.24.1
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          130.208.24.1
+ Target Hostname:    130.208.24.1
+ Target Port:        80
+ Start Time:         2024-01-29 18:16:33 (GMT0)
---------------------------------------------------------------------------
+ Server: openresty
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ .: 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-co
ntent-type-header/
+ / - Requires Authentication for realm 'level_15_or_view_access'
-C all
+ No creds found for realm 'level_15_or_view_access'
- STATUS: Completed 1020 requests (~15% complete, 33.0 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.00592 sec, 10 requests: 0.0062 sec.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 1 item(s) reported on remote host
+ End Time:           2024-01-29 18:27:14 (GMT0) (641 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
(base) hongjing@1006056 ~ %
```

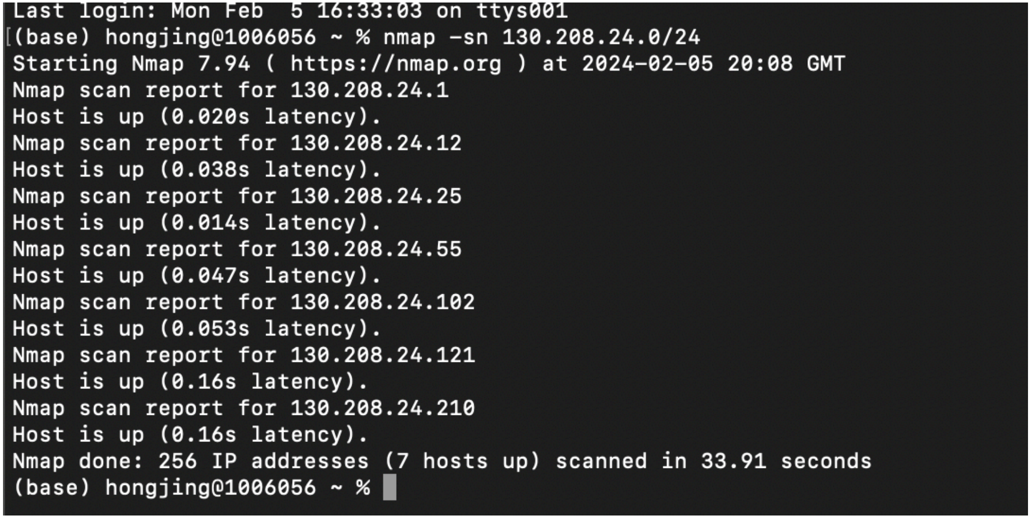
Nikto Scan Final Output Analysis

- Server Type: openresty, which is a full-fledged web platform based on nginx.
- No Common Gateway Interface (CGI) directories were found. This is generally positive from a security standpoint as CGI scripts can be a source of vulnerabilities if not properly managed.
- Missing X-Content-Type-Options Header: The server lacks the X-Content-Type-Options header with the nosniff value. This security header prevents the browser from interpreting files differently than the server's declared content type, which can protect against certain types of attacks, like MIME type confusion.
- Authentication Required: The root path / requires authentication within the realm 'level_15_or_view_access'. This implies some level of access control.

- Error Limit Reached: The scan reached the error limit set for the host and therefore terminated early. This could be due to various reasons like network issues, server configuration causing errors, or defensive measures from the server.

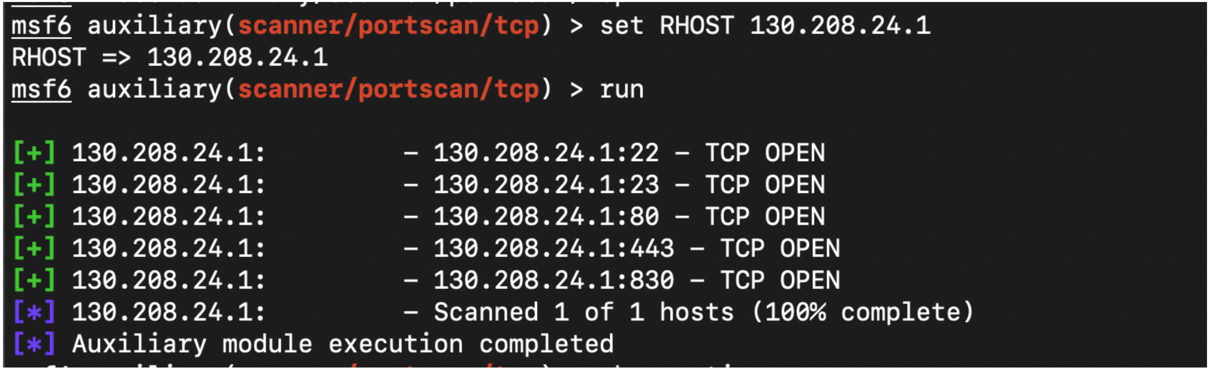
6. Using nmap -sn 130.208.24.0/24

This command will ping every IP in the 130.208.24.0 to 130.208.24.255 range to see which ones respond. The output will list the IPs of all devices that respond to the ping. The -sn flag will perform a ping scan to discover hosts without performing port scans.



```
Last login: Mon Feb  5 16:33:03 on ttys001
[(base) hongjing@1006056 ~ % nmap -sn 130.208.24.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 20:08 GMT
Nmap scan report for 130.208.24.1
Host is up (0.020s latency).
Nmap scan report for 130.208.24.12
Host is up (0.038s latency).
Nmap scan report for 130.208.24.25
Host is up (0.014s latency).
Nmap scan report for 130.208.24.55
Host is up (0.047s latency).
Nmap scan report for 130.208.24.102
Host is up (0.053s latency).
Nmap scan report for 130.208.24.121
Host is up (0.16s latency).
Nmap scan report for 130.208.24.210
Host is up (0.16s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 33.91 seconds
(base) hongjing@1006056 ~ %
```

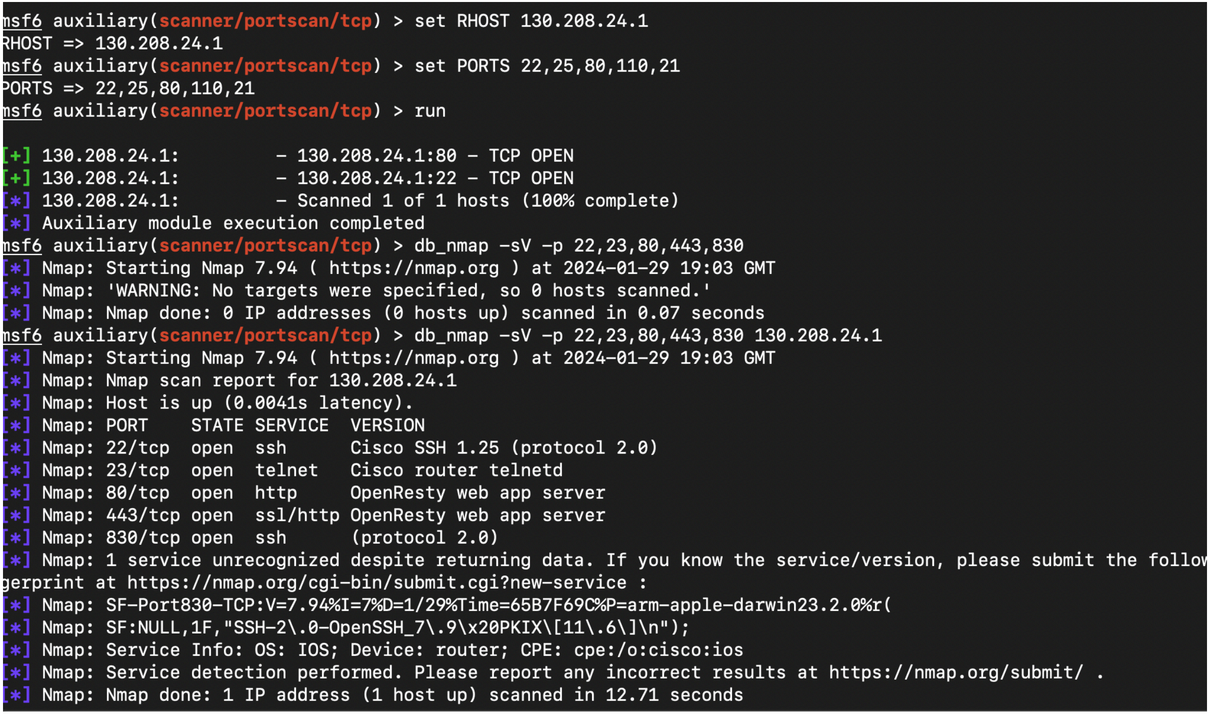
7. Using Metasploit
    - Launch Metasploit using msfconsole
    - Activate the port scanner module
    - use auxiliary/scanner/portscan/tcp
    - configure RHOSTS with the IP of the router and run



```
msf6 auxiliary(scanner/portscan/tcp) > set RHOST 130.208.24.1
RHOST => 130.208.24.1
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 130.208.24.1:         - 130.208.24.1:22 - TCP OPEN
[+] 130.208.24.1:         - 130.208.24.1:23 - TCP OPEN
[+] 130.208.24.1:         - 130.208.24.1:80 - TCP OPEN
[+] 130.208.24.1:         - 130.208.24.1:443 - TCP OPEN
[+] 130.208.24.1:         - 130.208.24.1:830 - TCP OPEN
[*] 130.208.24.1:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Once we’ve established a clear picture of the available ports, we can begin enumerating them in order to observe and locate the operating services, as well as their versions.



```
msf6 auxiliary(scanner/portscan/tcp) > set RHOST 130.208.24.1
RHOST => 130.208.24.1
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21
PORTS => 22,25,80,110,21
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 130.208.24.1:         - 130.208.24.1:80 - TCP OPEN
[+] 130.208.24.1:         - 130.208.24.1:22 - TCP OPEN
[*] 130.208.24.1:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > db_nmap -sV -p 22,23,80,443,830
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 19:03 GMT
[*] Nmap: 'WARNING: No targets were specified, so 0 hosts scanned.'
[*] Nmap: Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds
msf6 auxiliary(scanner/portscan/tcp) > db_nmap -sV -p 22,23,80,443,830 130.208.24.1
[*] Nmap: Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 19:03 GMT
[*] Nmap: Nmap scan report for 130.208.24.1
[*] Nmap: Host is up (0.0041s latency).
[*] Nmap: PORT    STATE SERVICE  VERSION
[*] Nmap: 22/tcp  open  ssh      Cisco SSH 1.25 (protocol 2.0)
[*] Nmap: 23/tcp  open  telnet   Cisco router telnetd
[*] Nmap: 80/tcp  open  http     OpenResty web app server
[*] Nmap: 443/tcp open  ssl/http OpenResty web app server
[*] Nmap: 830/tcp open  ssh      (protocol 2.0)
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the follow
gerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port830-TCP:V=7.94%I=7%D=1/29%Time=65B7F69C%P=arm-apple-darwin23.2.0%r(
[*] Nmap: SF:NULL,1F,"SSH-2\.0-OpenSSH_7\.9\x20PKIX\[11\.6\]\n");
[*] Nmap: Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 12.71 seconds
```