Experiment Number:8

Aim: Study **Nmap** installation and it's use with different options to scan open ports, perform **OS fingerprinting**, do a **ping** scan, **tcp** port scan, **udp** port scan,.. etc

Date of Performance: 23-9-2020

Date of Submission: 27-9-2020

Grade:

Sign:

Name :

Bhagyashri Nitin Patil

Roll Number: 50

Scan Ports using Nmap

1. Scan with Hostname

- nmap kaliLinux

```
bhagyashri@kaliLinux:~$ nmap kaliLinux
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:00 EDT
Nmap scan report for kaliLinux (127.0.1.1)
Host is up (0.000082s latency).
All 1000 scanned ports on kaliLinux (127.0.1.1) are closed
```

- nmap www.google.com

```
bhagyashri@kaliLinux:~$ nmap www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:01 EDT
Nmap scan report for www.google.com (216.58.200.132)
Host is up (0.28s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:805::2004
rDNS record for 216.58.200.132: maa05s10-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

2. Scan with ip address

- nmap 216.58.200.132

```
bhagyashri@kaliLinux:~$ nmap 216.58.200.132
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:03 EDT
Nmap scan report for maa05s10-in-f4.1e100.net (216.58.200.132)
Host is up (0.24s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 66.24 seconds
```


3. Scan using -v option [To get more details]

- nmap -v google.com

```
bhagyashri@kaliLinux:~$ nmap -v google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:06 EDT
Initiating Ping Scan at 09:06
Scanning google.com (172.217.167.174) [2 ports]
Completed Ping Scan at 09:06, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:06
Completed Parallel DNS resolution of 1 host. at 09:06, 0.06s elapsed
Initiating Connect Scan at 09:06
Scanning google.com (172.217.167.174) [1000 ports]
Discovered open port 443/tcp on 172.217.167.174
Discovered open port 80/tcp on 172.217.167.174
Connect Scan Timing: About 60.95% done; ETC: 09:07 (0:00:30 remaining)
Completed Connect Scan at 09:07, 65.81s elapsed (1000 total ports)
Nmap scan report for google.com (172.217.167.174)
Host is up (0.17s latency).
Other addresses for google.com (not scanned): 2404:6800:4007:80a::200e
rDNS record for 172.217.167.174: bom12s01-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 66.07 seconds
```

4. Scan multiple hosts with ip address

- nmap 192.168.0.101 192.168.0.102 192.168.0.103

```
bhagyashri@kaliLinux:~$ nmap 192.168.0.101 192.168.0.102 192.168.0.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:09 EDT
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.09 seconds
```


5. Scan multiple hosts with host names

- nmap google.com amazon.com flipkart.com

```
bhagyashri@kaliLinux:~$ nmap google.com amazon.com flipkart.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:10 EDT
Nmap scan report for google.com (172.217.31.206)
Host is up (0.19s latency).
Other addresses for google.com (not scanned): 2404:6800:4007:80a::200e
rDNS record for 172.217.31.206: maa03s28-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for amazon.com (205.251.242.103)
Host is up (0.43s latency).
Other addresses for amazon.com (not scanned): 176.32.103.205 176.32.98.166
rDNS record for 205.251.242.103: s3-console-us-standard.console.aws.amazon.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for flipkart.com (163.53.78.110)
Host is up (0.38s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 3 IP addresses (3 hosts up) scanned in 186.41 seconds
```

6. Scan a whole subnet

- nmap 192.168.0.* [* means all]

```
bhagyashri@kaliLinux:~$ nmap 192.168.0.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:19 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 103.44 seconds
```


7. Scan Multiple Servers using last octet of IP address

- nmap 192.168.0.101,102,103,104

```
bhagyashri@kaliLinux:~$ nmap 192.168.0.101,102,103,104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:31 EDT
Nmap done: 4 IP addresses (0 hosts up) scanned in 3.04 seconds
bhagyashri@kaliLinux:~$
```

8. Scan list of Hosts from a file

- cat Filescan.txt

```
bhagyashri@kaliLinux:~$ cat Filescan.txt
172.217.166.46
216.58.200.132
```

- nmap -iL Filescan.txt

```
bhagyashri@kaliLinux:~$ nmap -iL Filescan.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 09:58 EDT
Nmap scan report for bom07s18-in-f14.1e100.net (172.217.166.46)
Host is up (0.22s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for maa05s10-in-f4.1e100.net (216.58.200.132)
Host is up (0.37s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 140.47 seconds
```


9. Scan an IP Address Range

- nmap -v 192.168.0.101-105

```
bhagyashri@kaliLinux:~$ nmap -v 192.168.0.101-105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 10:09 EDT
Initiating Ping Scan at 10:09
Scanning 5 hosts [2 ports/host]
Completed Ping Scan at 10:09, 3.01s elapsed (5 total hosts)
Nmap scan report for 192.168.0.101 [host down]
Nmap scan report for 192.168.0.102 [host down]
Nmap scan report for 192.168.0.103 [host down]
Nmap scan report for 192.168.0.104 [host down]
Nmap scan report for 192.168.0.105 [host down]
Read data files from: /usr/bin/../share/nmap
Nmap done: 5 IP addresses (0 hosts up) scanned in 3.08 seconds
```

10. Scan network excluding Remote Hosts

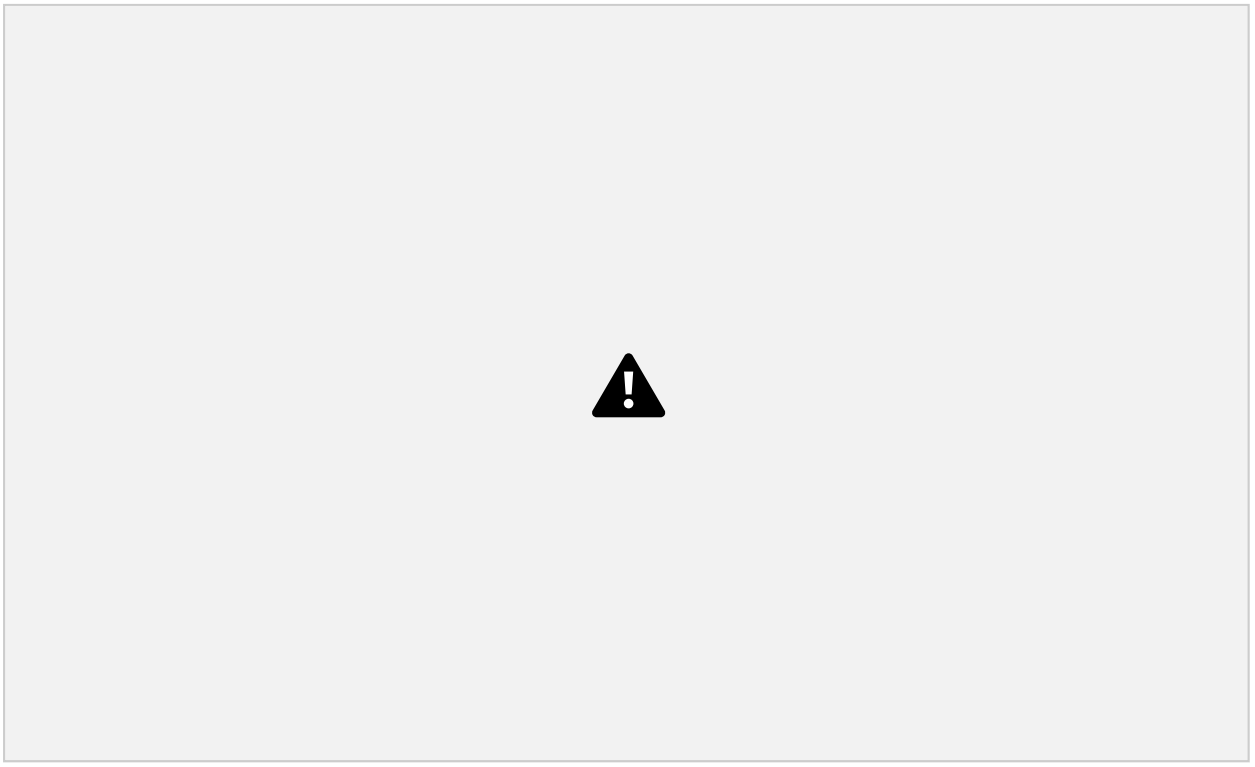
- nmap 192.168.0.* --exclude 192.168.0.100

11. Find nmap version

- nmap -v

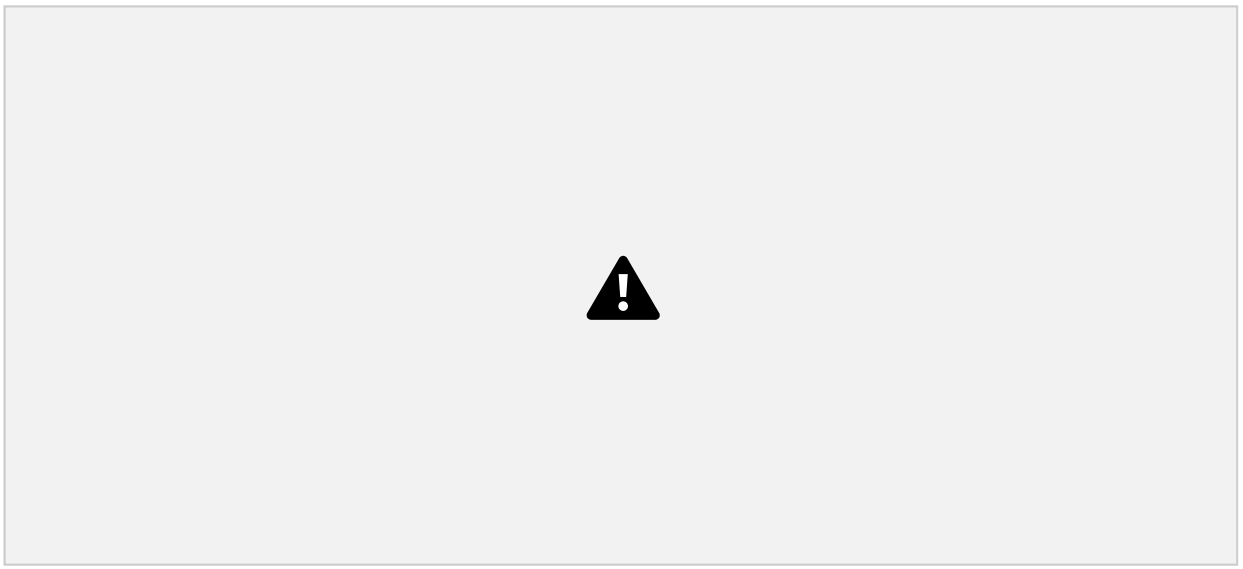
12. Scan OS information and Traceroute

- nmap -A google.com



13. Enable OS detection with Nmap

- nmap -O google.com



CNS (Roll_50)

14. Scan a Host to Detect Firewall

- nmap -sA 192.168.0.101

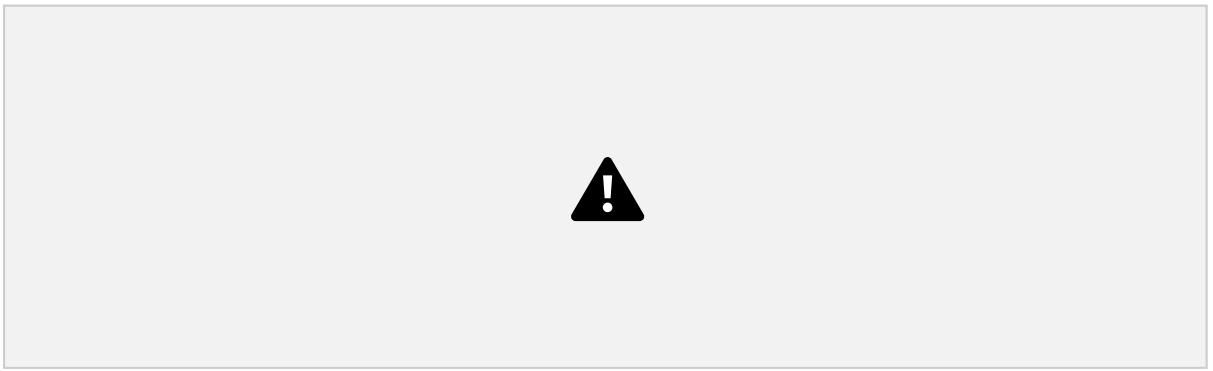
15. Scan a Host to to check its protected by Firewall • nmap -PN 192.168.0.1

16. Scan a Find out Live hosts in a Network

- nmap -sP 192.168.0.*

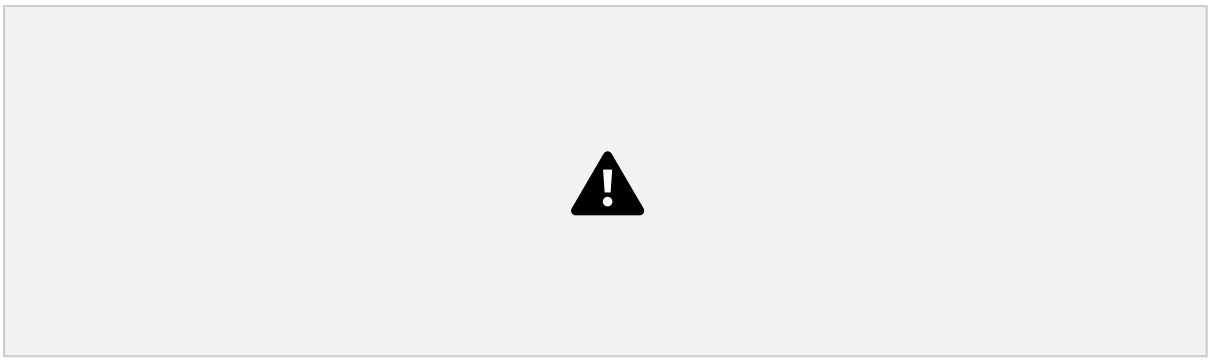
17. Perform a Fast Scan

- nmap -F 172.217.166.46



18. Scan Ports consecutively

- nmap -r 172.217.166.46



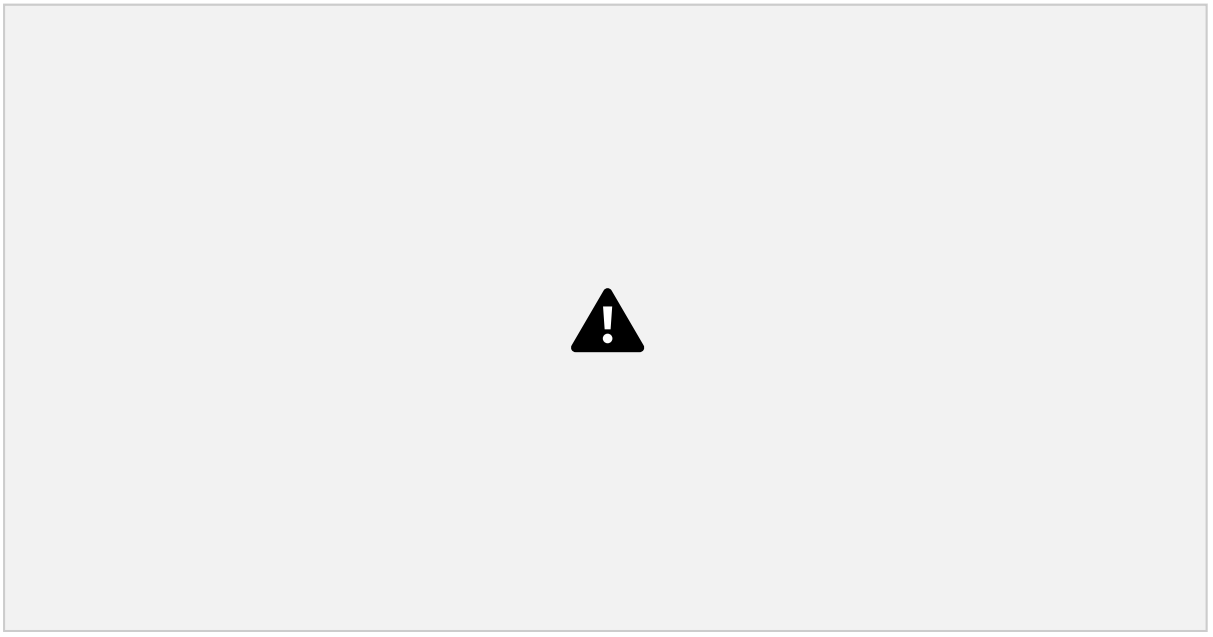
19. Scan a For specific port

- nmap -p 80 google.com

CNS (Roll_50)

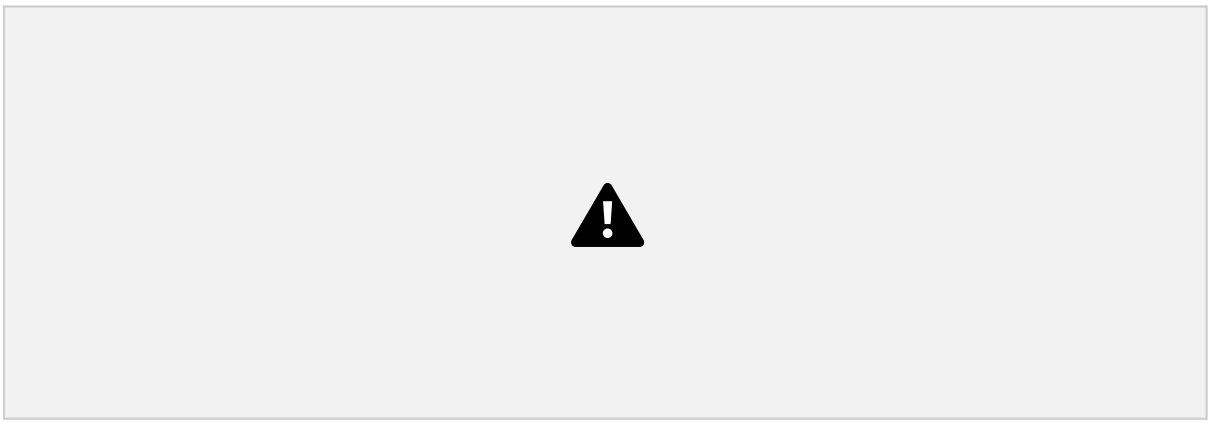
20. Scan Host interfaces and Routes

- nmap -ifList



21. Scan a TCP Port

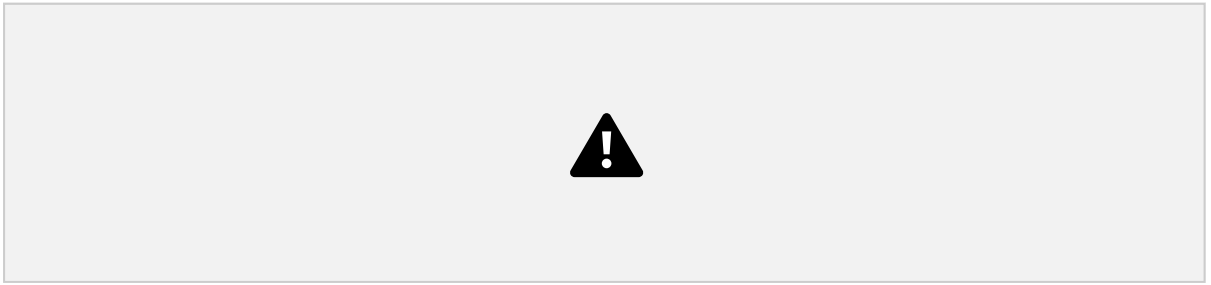
- nmap -p T:8888,80 www.amzon.com



CNS (Roll_50)

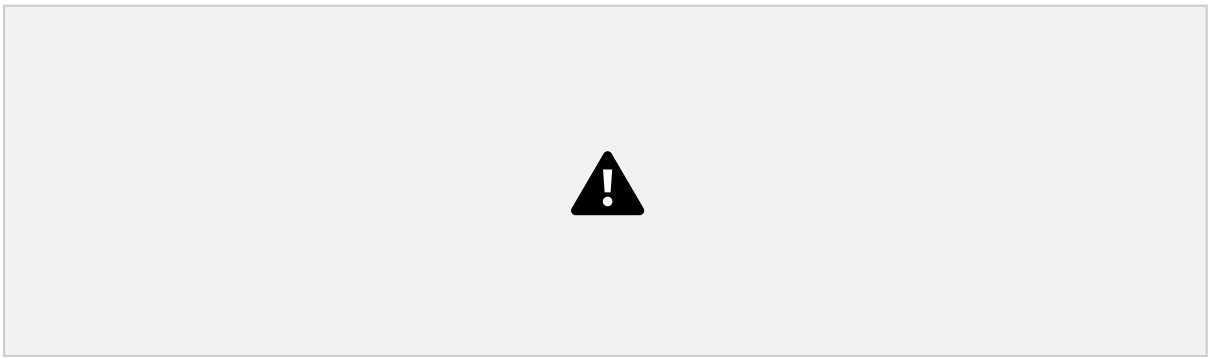
22. Scan a UDP Port

- nmap -sU 53 amzon.com



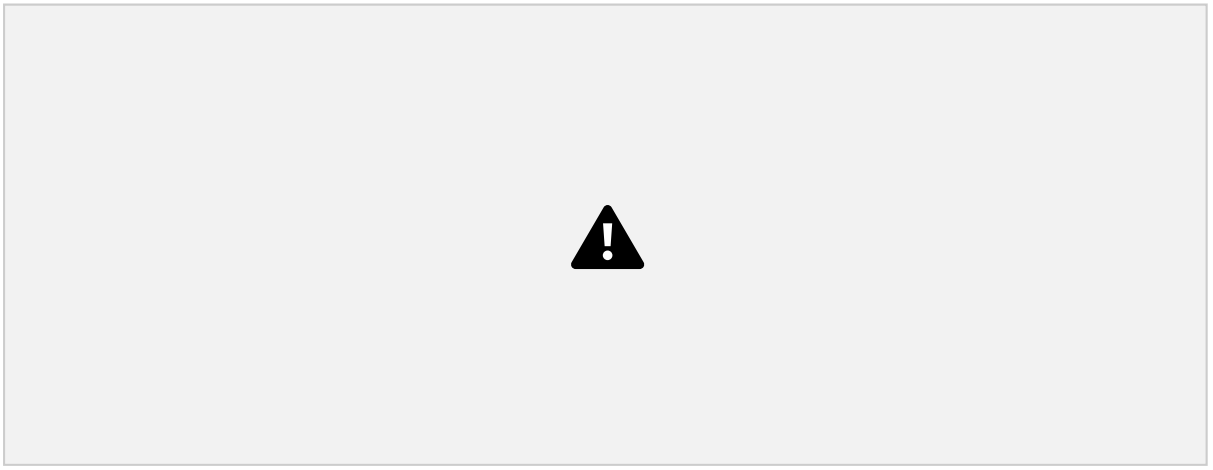
23. Scan Multiple Ports

- nmap -p 80,443 127.0.1.1



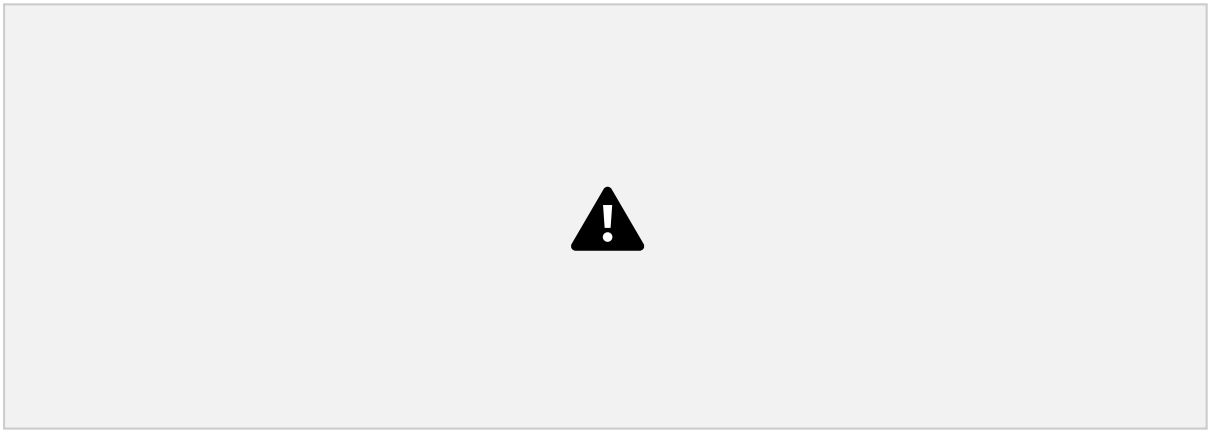
24. Scan remote hosts using TCP ACK(PA) & TCP Syn(PS)

- nmap -PS google.com



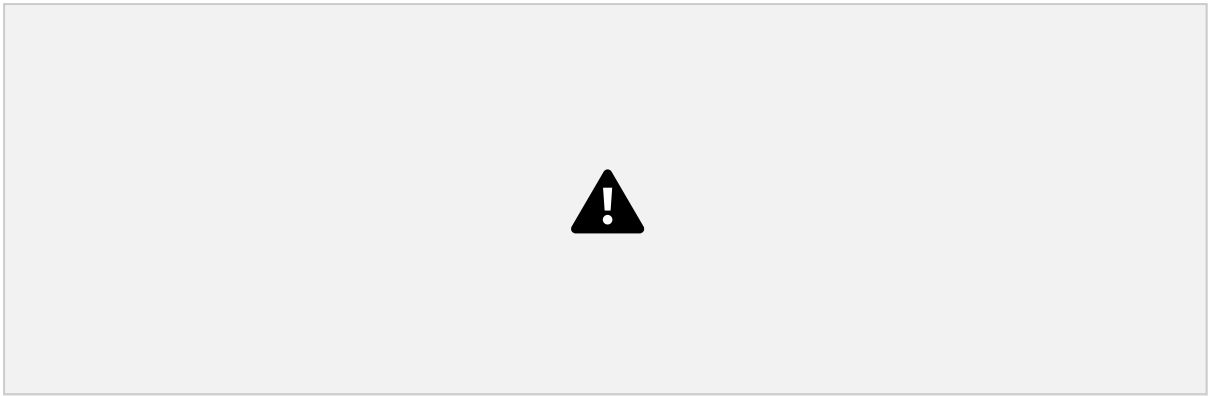
25. Scan remote hosts for specific ports with using TCP Syn

- nmap -PA -p 22,80 172.217.166.46



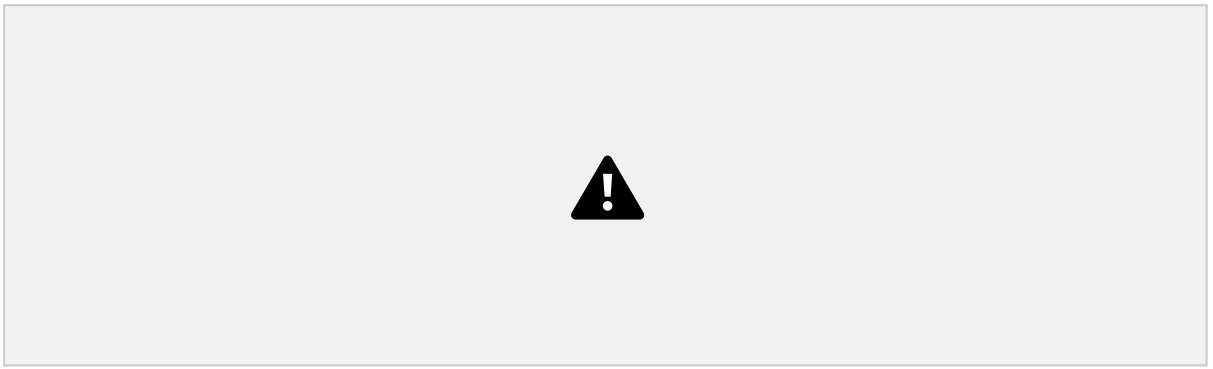
26. Perform a stealthy scan

- nmap -sS 172.217.166.46



27. Check most commonly used Ports with TCP Syn

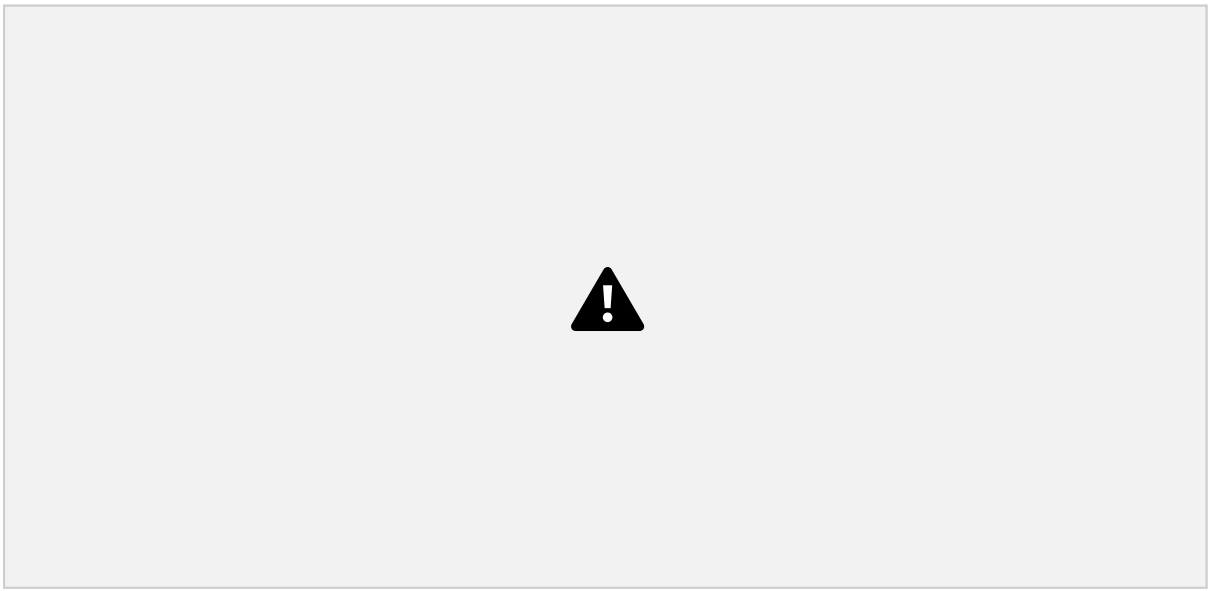
- nmap -sT 172.217.166.46



28. Scan Perform a TCP null scan to fool a firewall

- nmap -sN 163.53.78.110

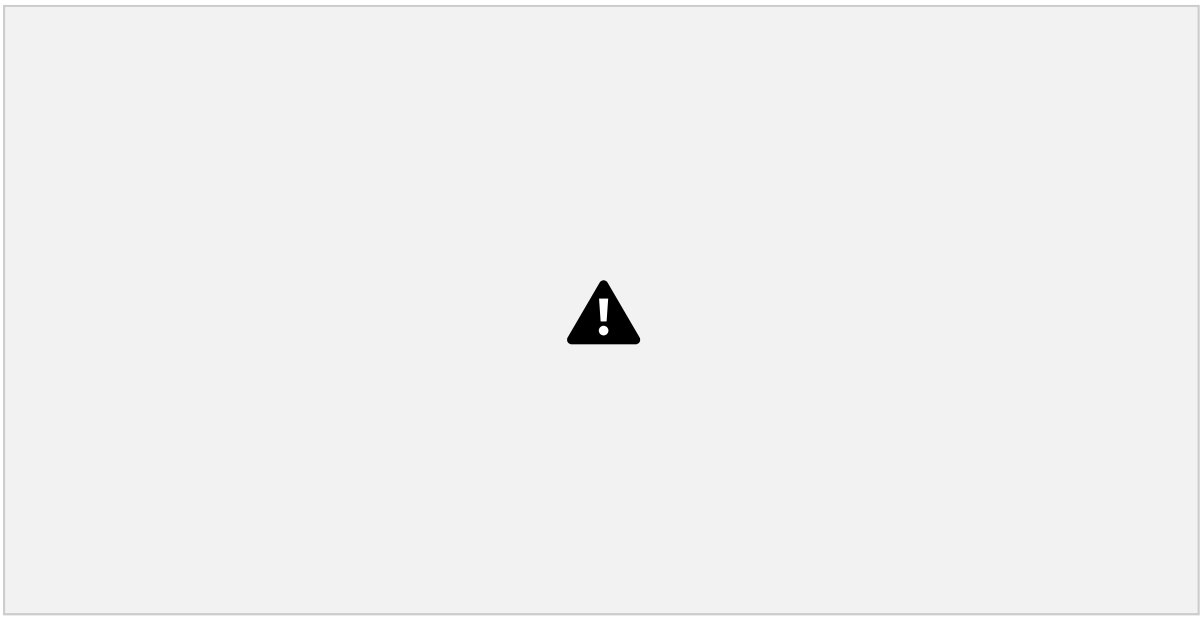
29. Scan the most popular ports



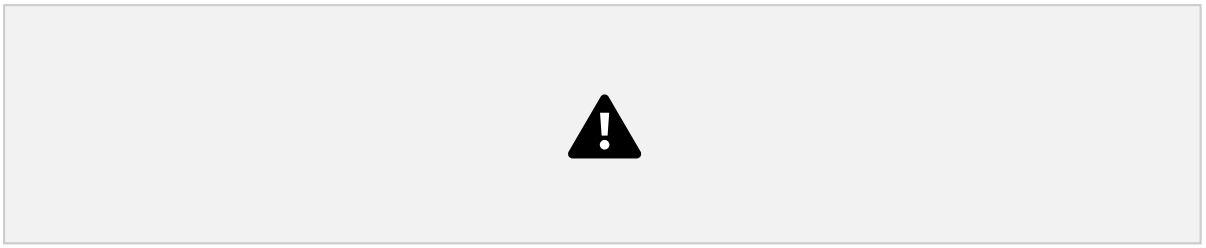
ZENMAP

Zenmap Installation Steps

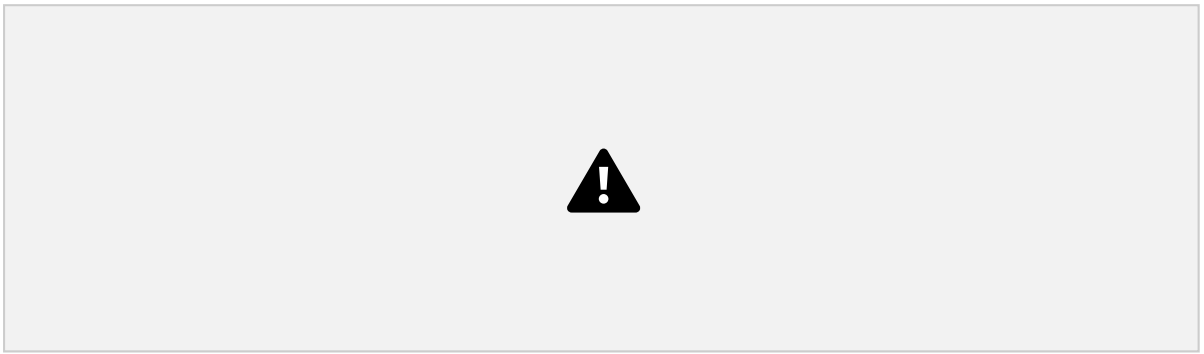
1. Go to nmap.org website and click on zenmap rpm file as shown:



2. Run command : sudo alien ‘zenmap-7.80-1.noarch .rpm’

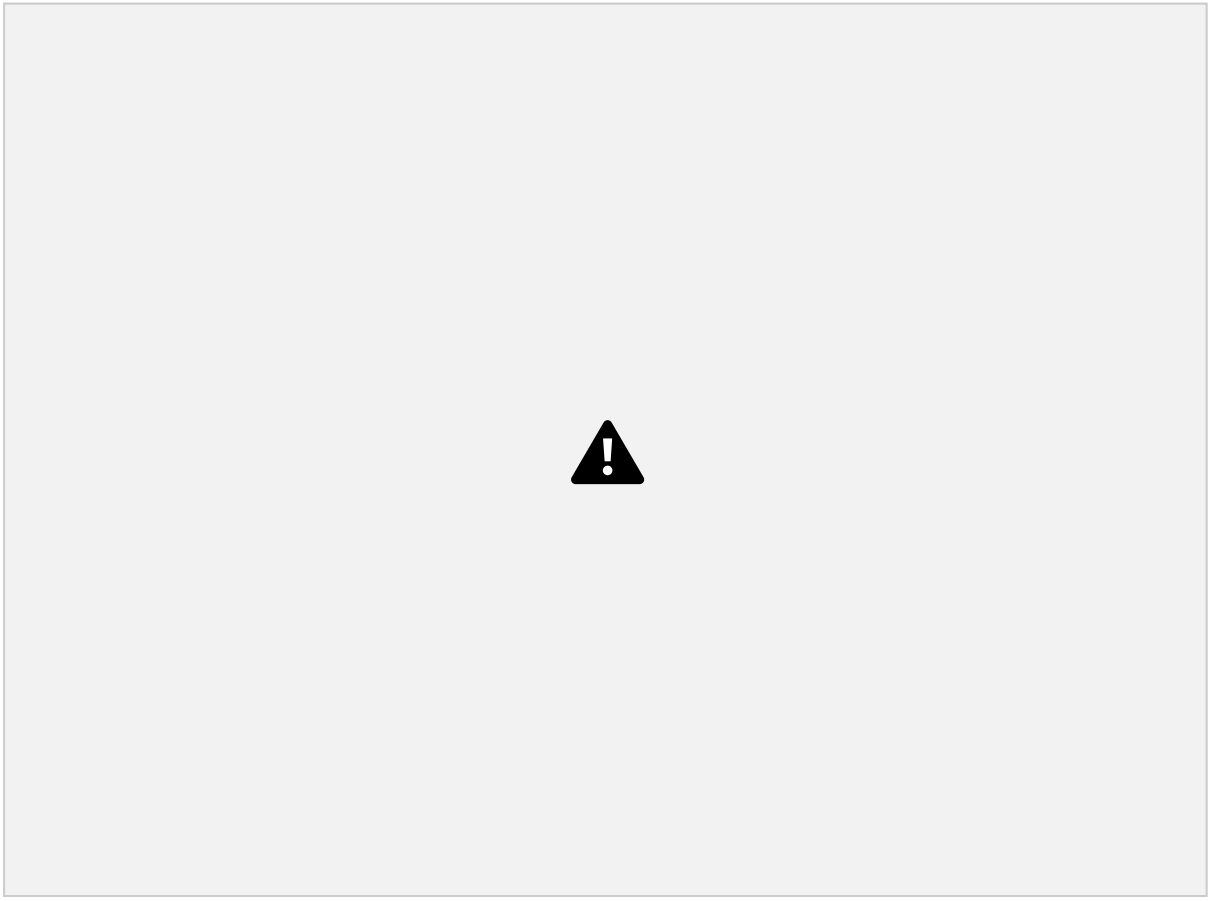


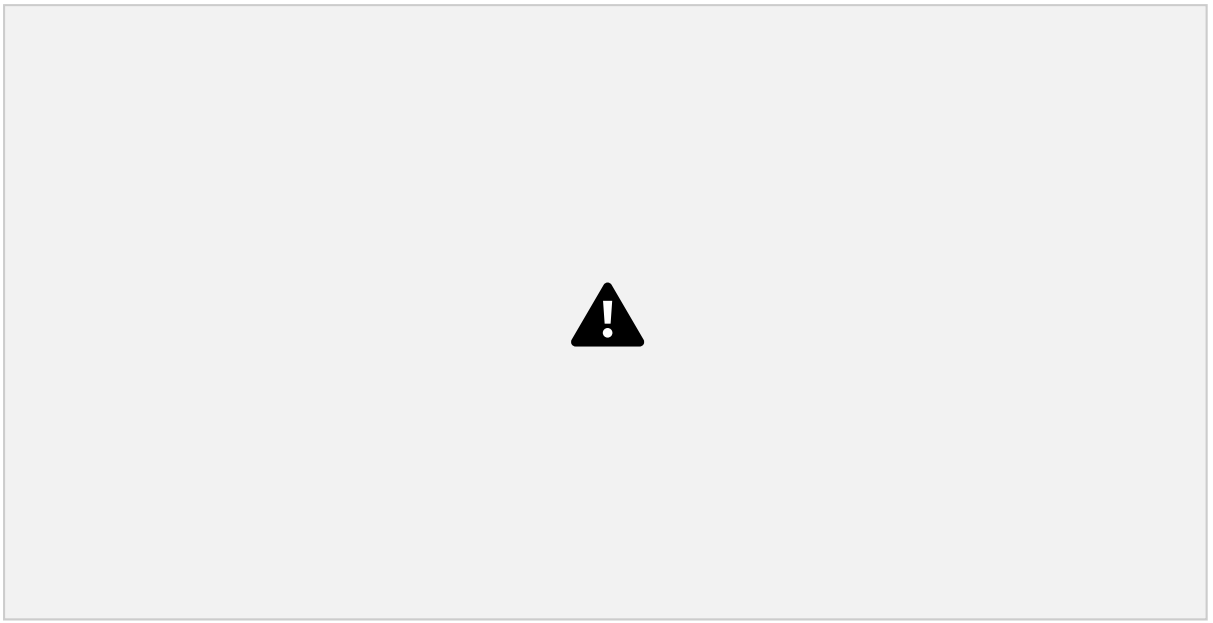
3. Run command : sudo dbkg -I zenmap_7.80-2_all.deb



Scan Ports using Zenmap (GUI)

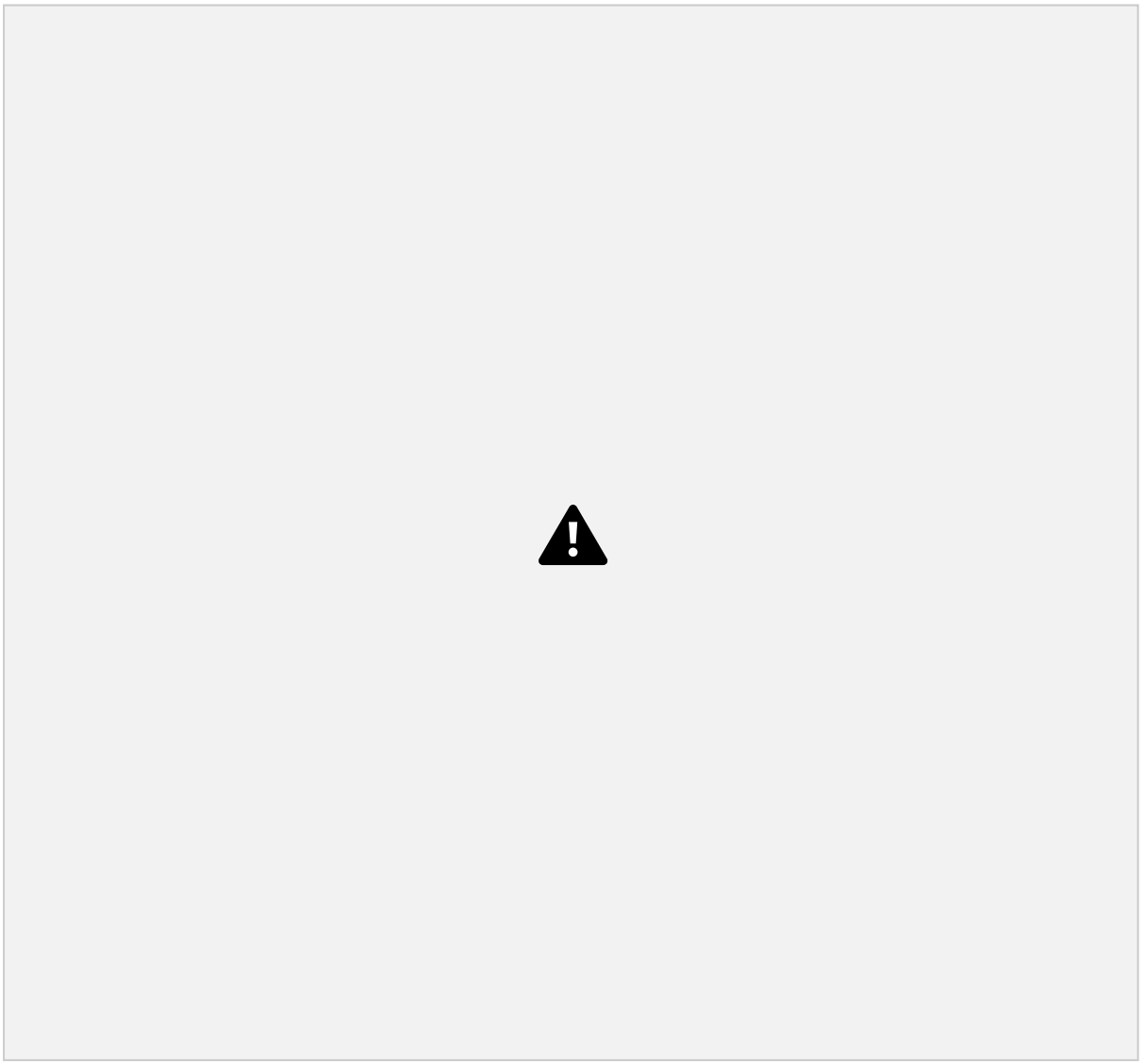
1. Scan multiple hosts with host names

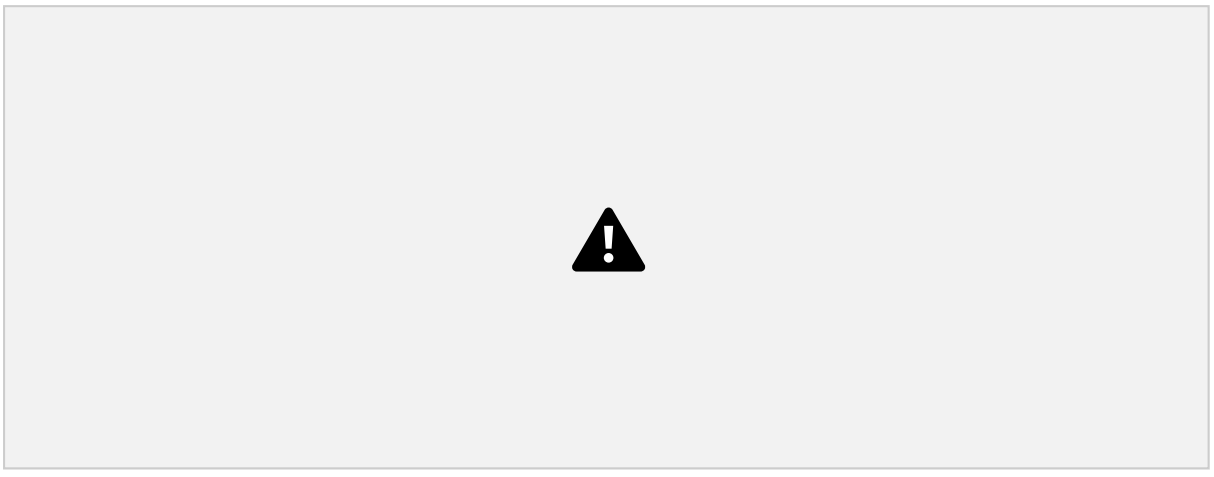




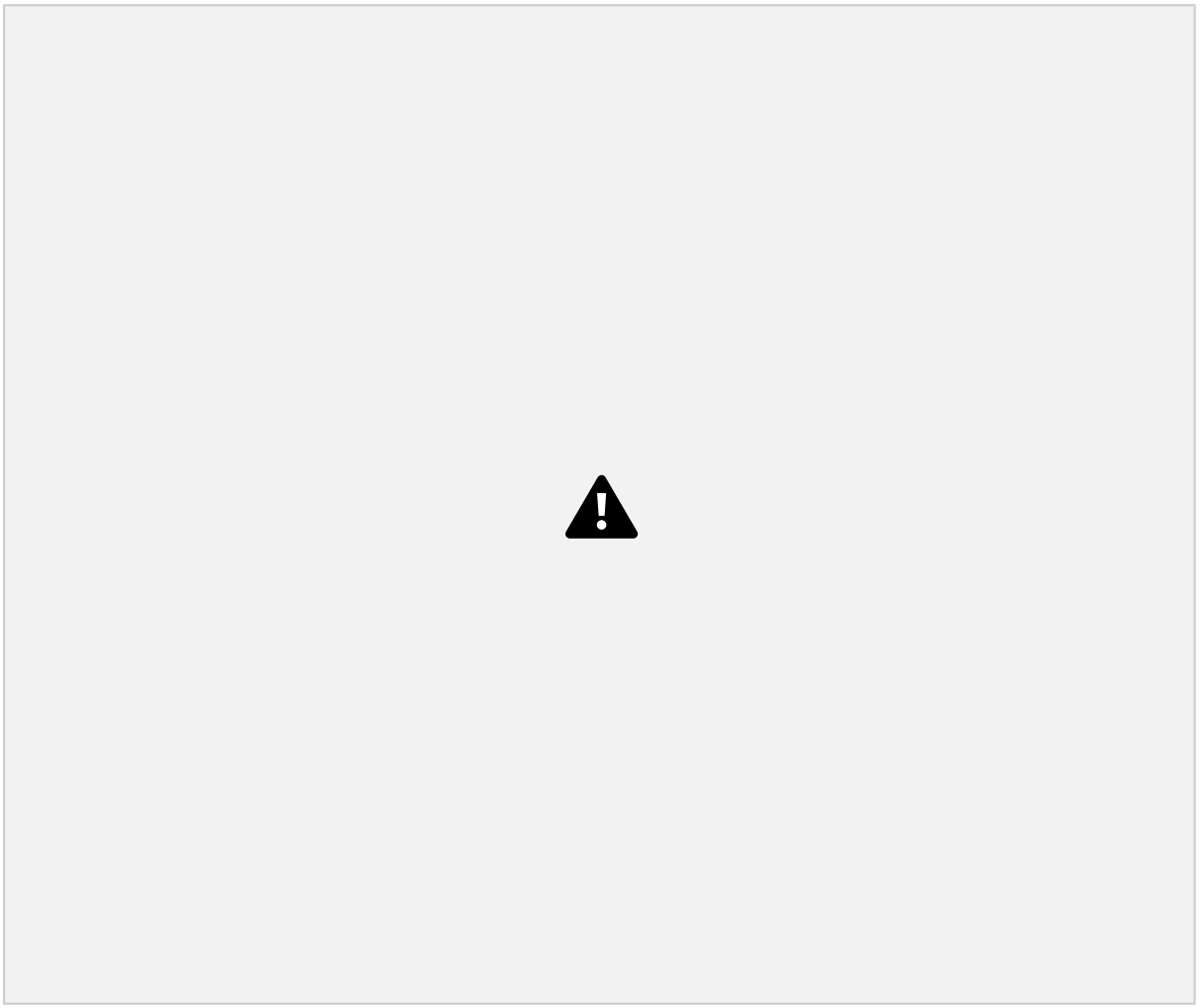
CNS (Roll_50)

2. Scan an IP Address Range

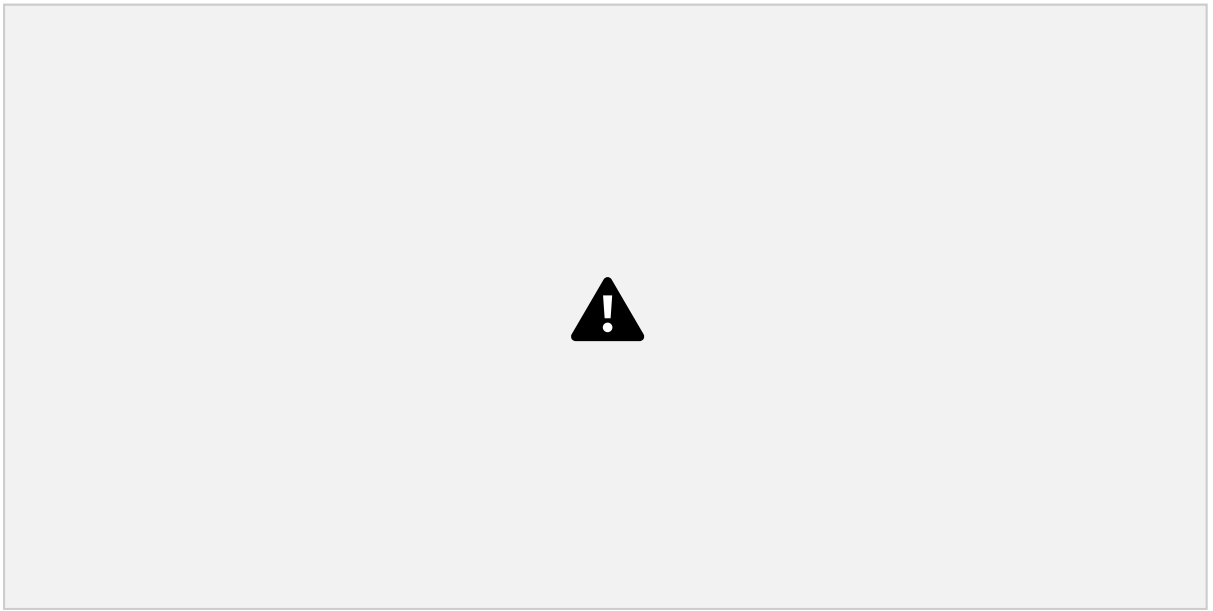


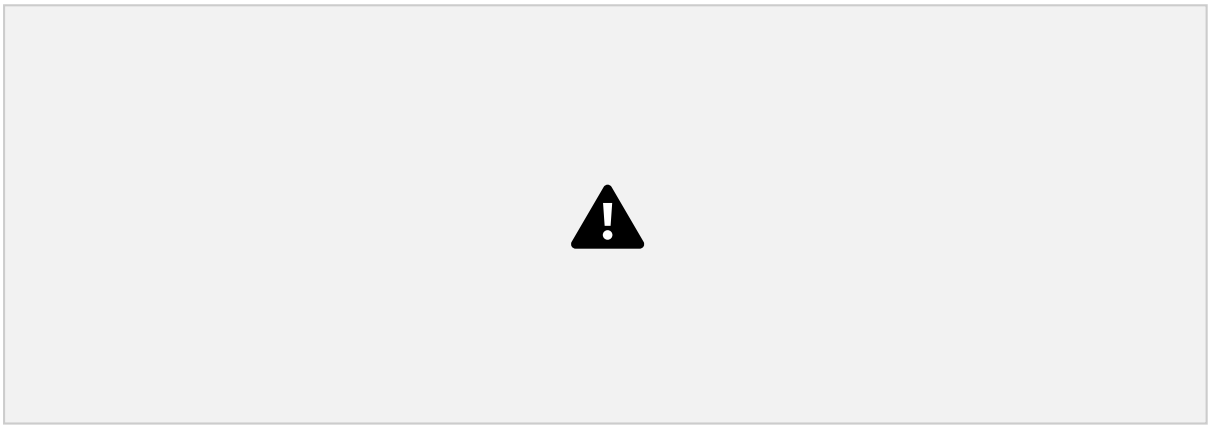


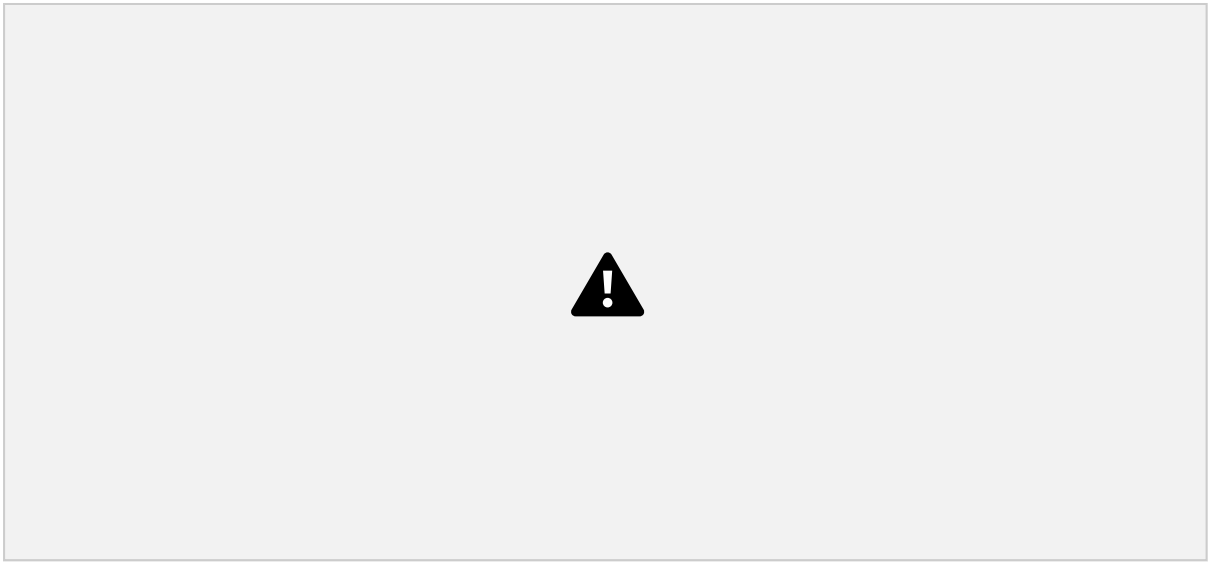
CNS (Roll_50)



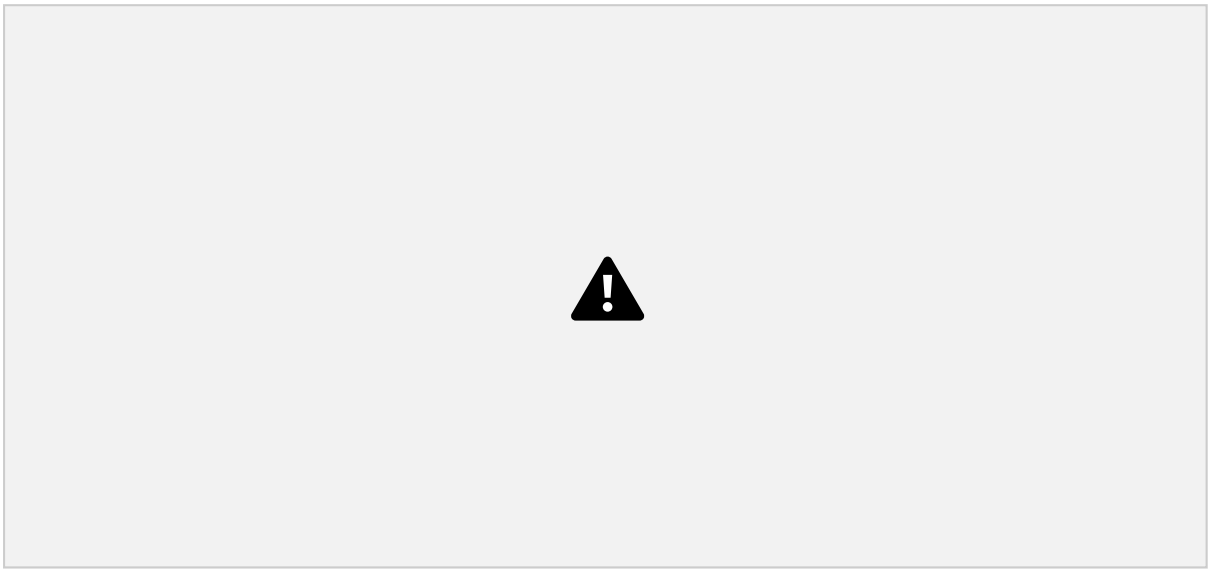
3. Scan a For specific port

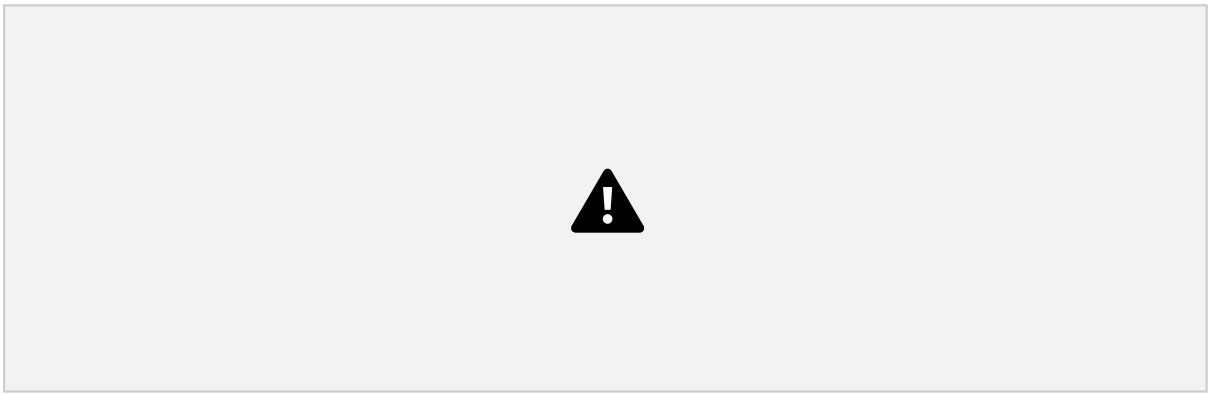




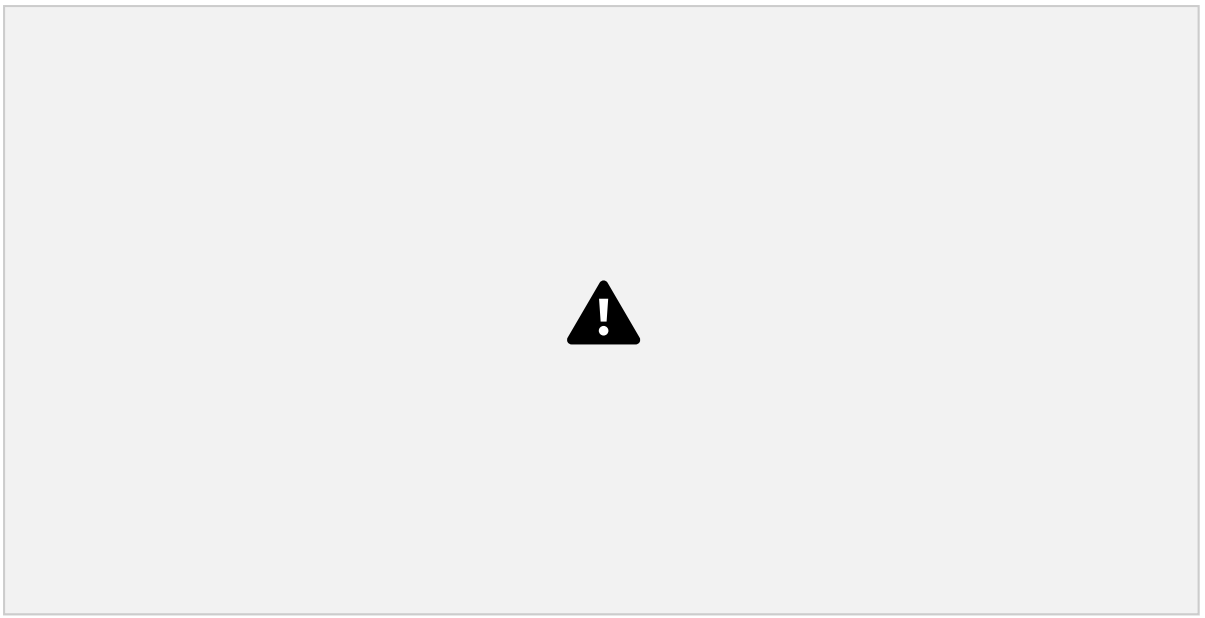


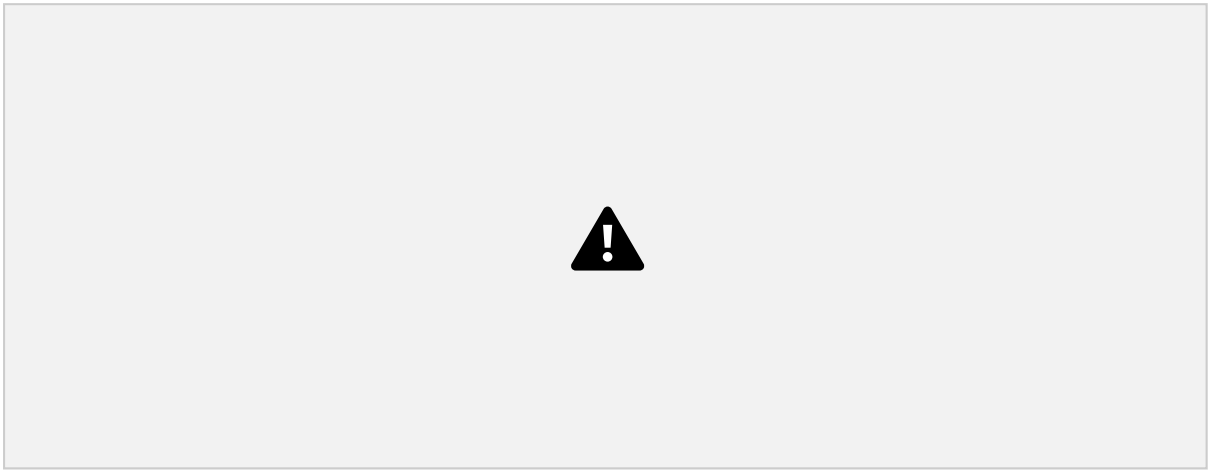
4. Scan a TCP Port

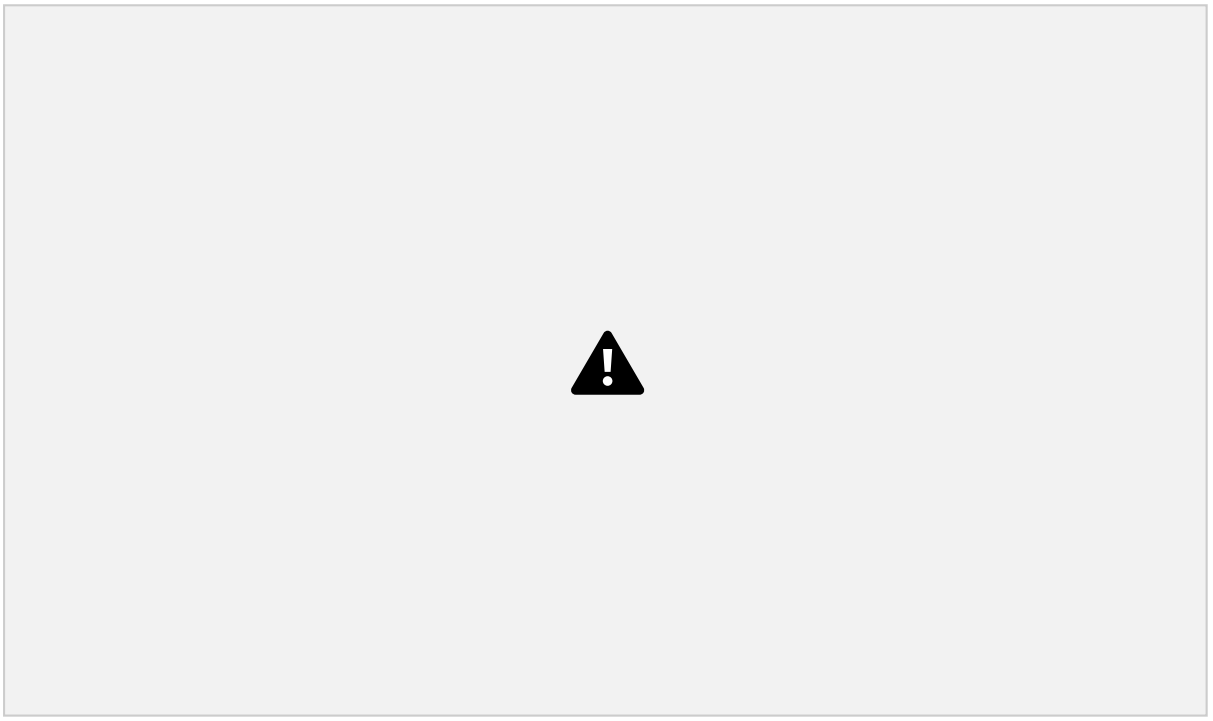


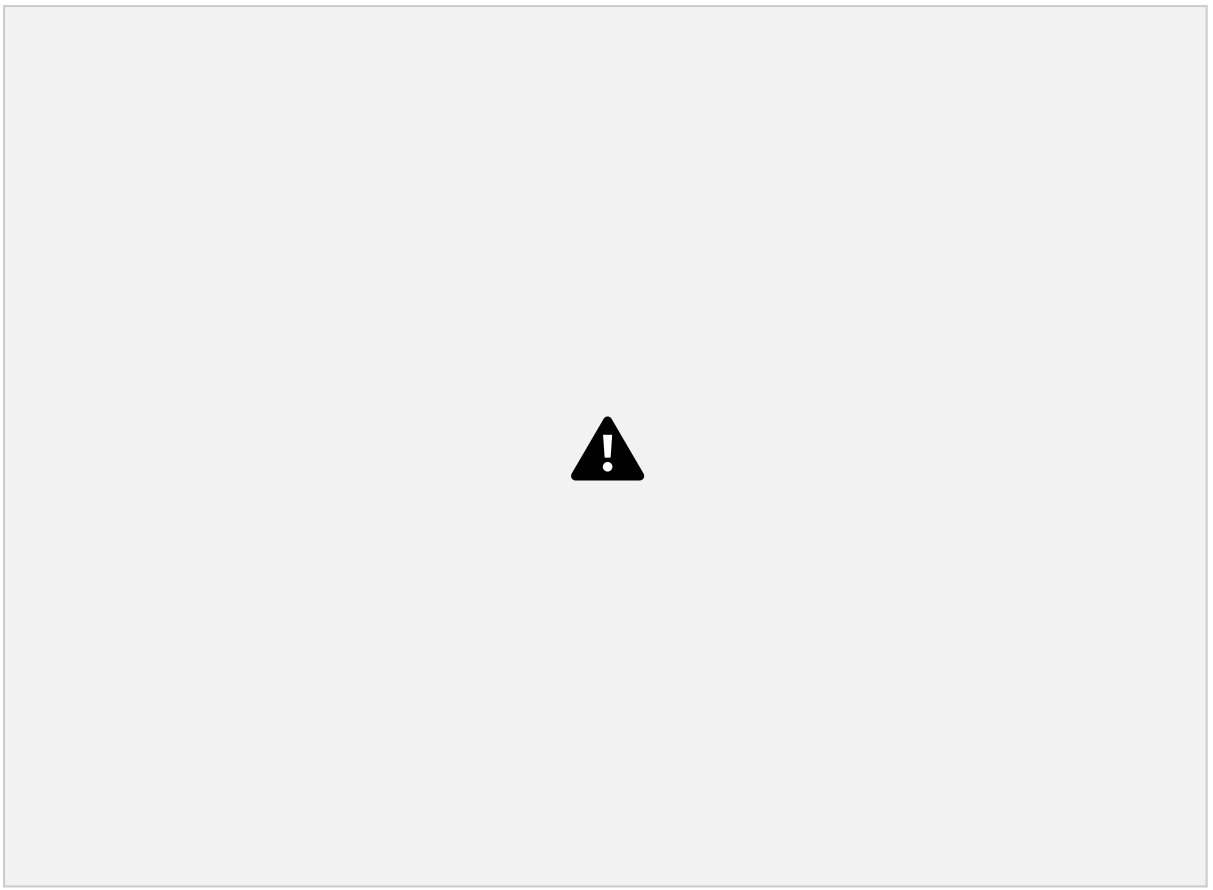


5. Scan multiple Ports



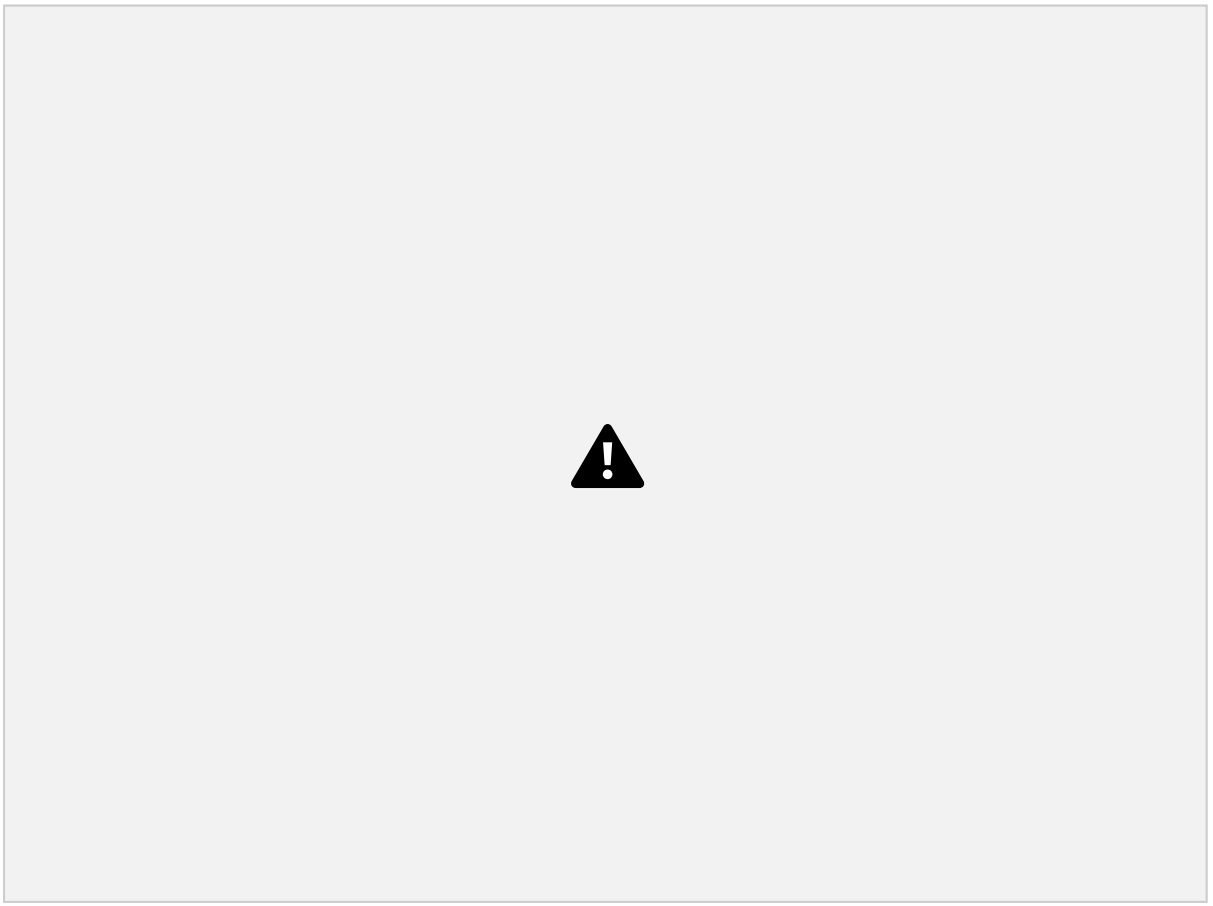


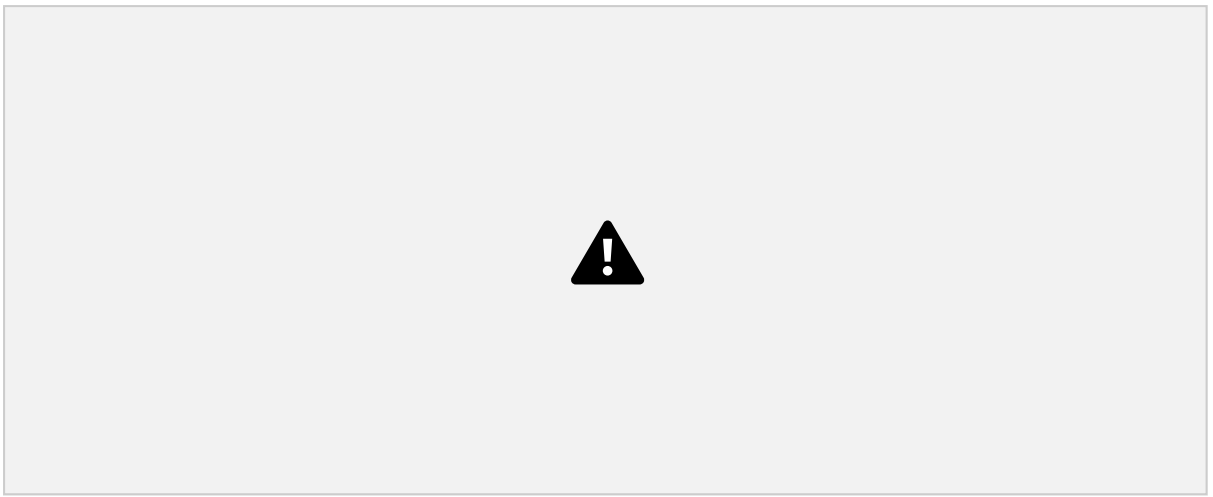




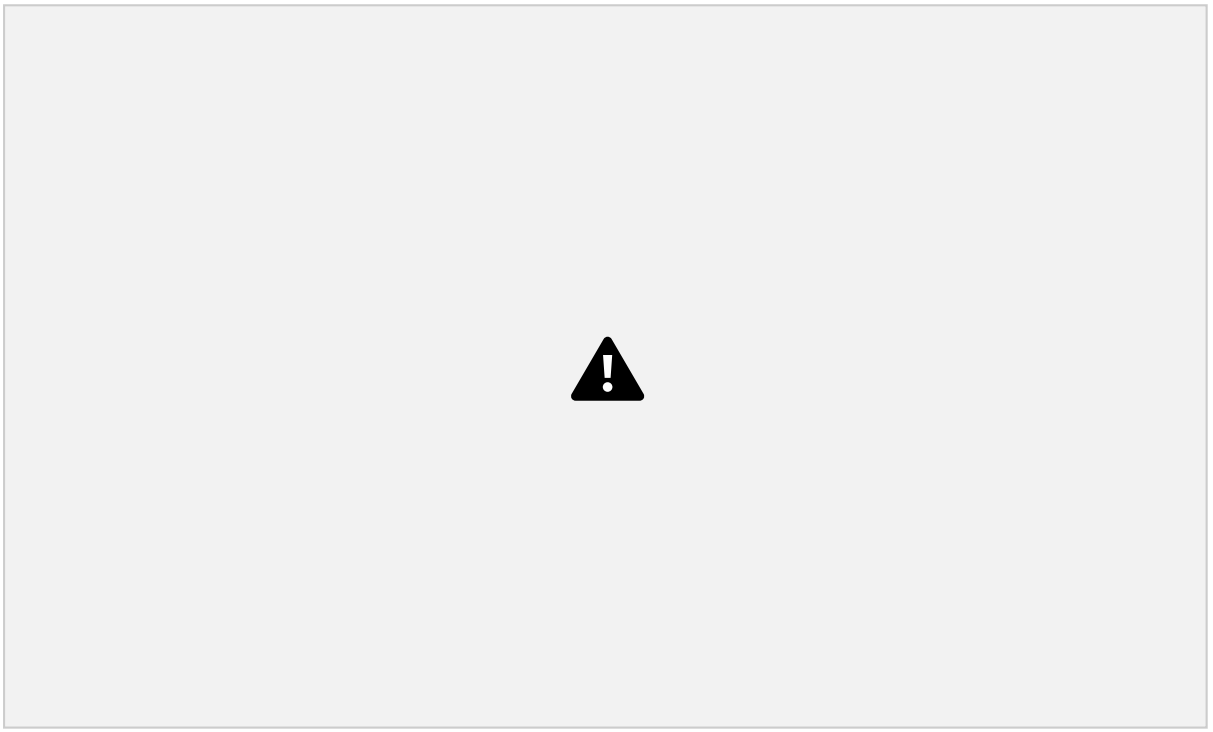
CNS (Roll_50)

6. Perform a Fast Scan

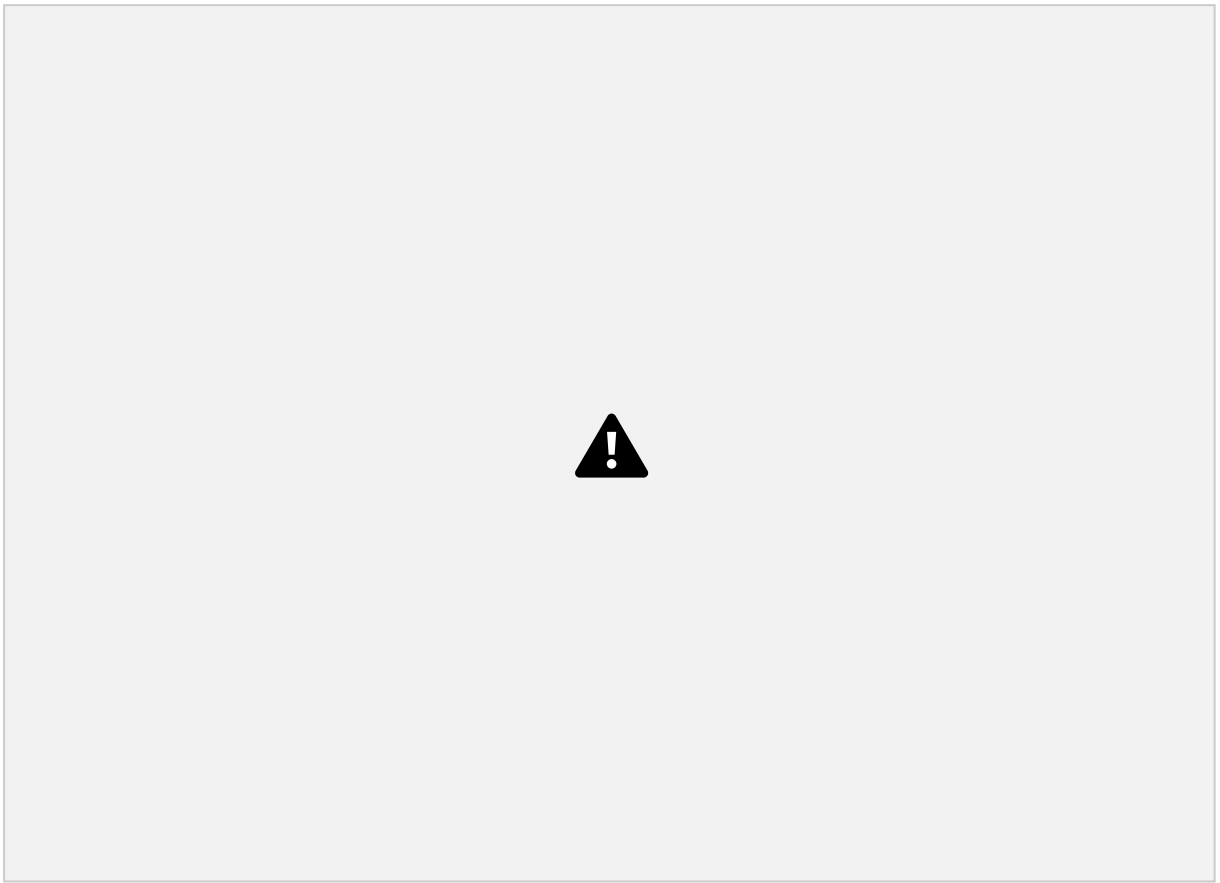


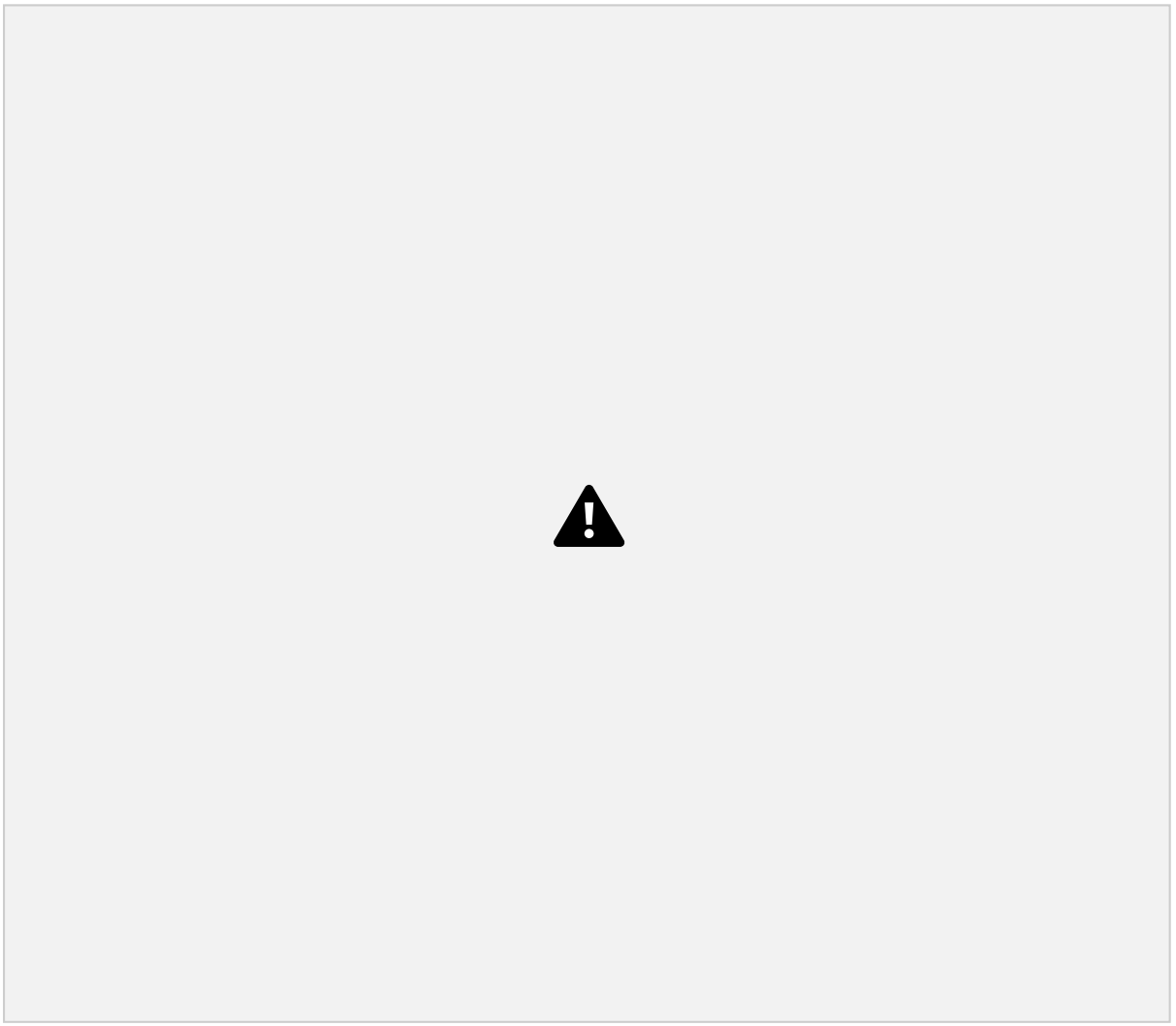


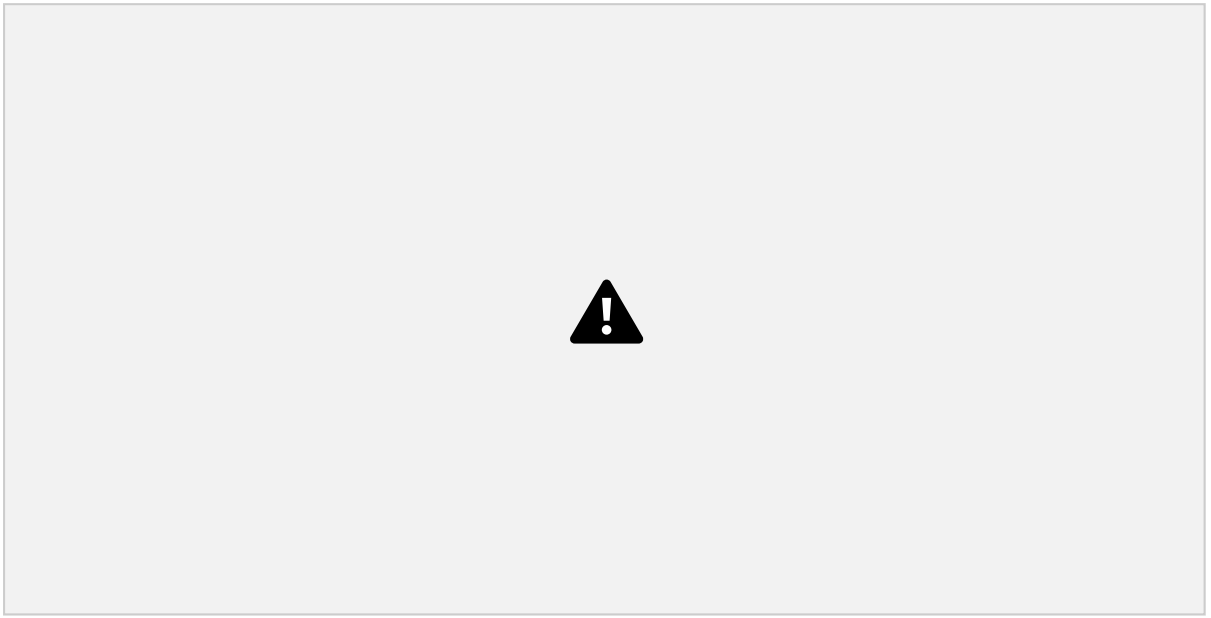
CNS (Roll_50)



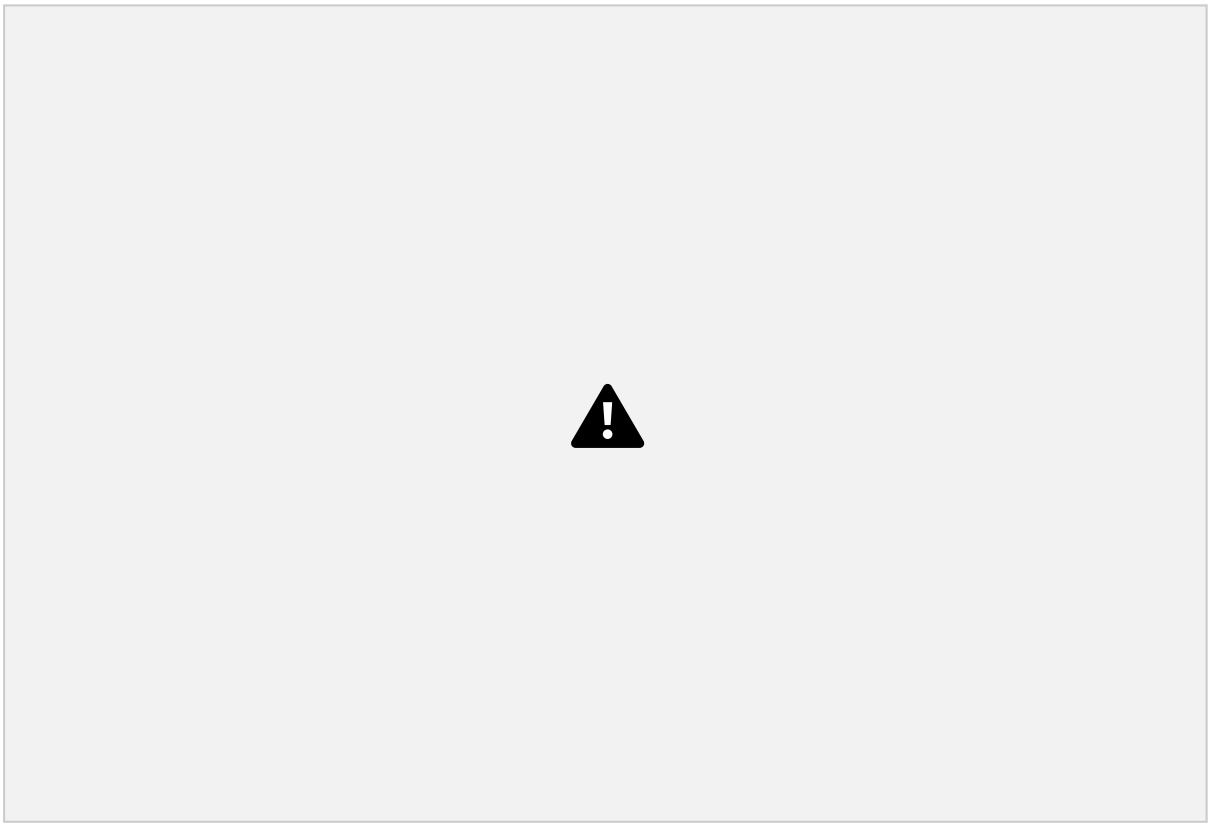
7. Scan Network ports by Network Range



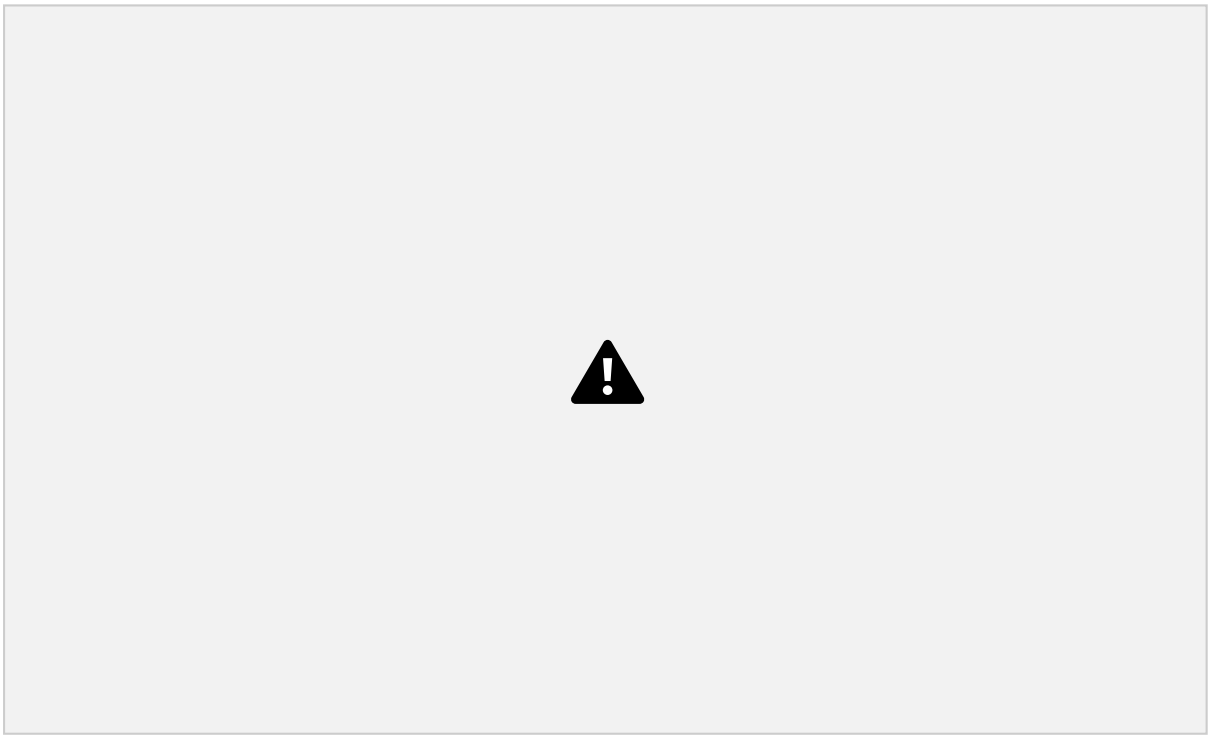


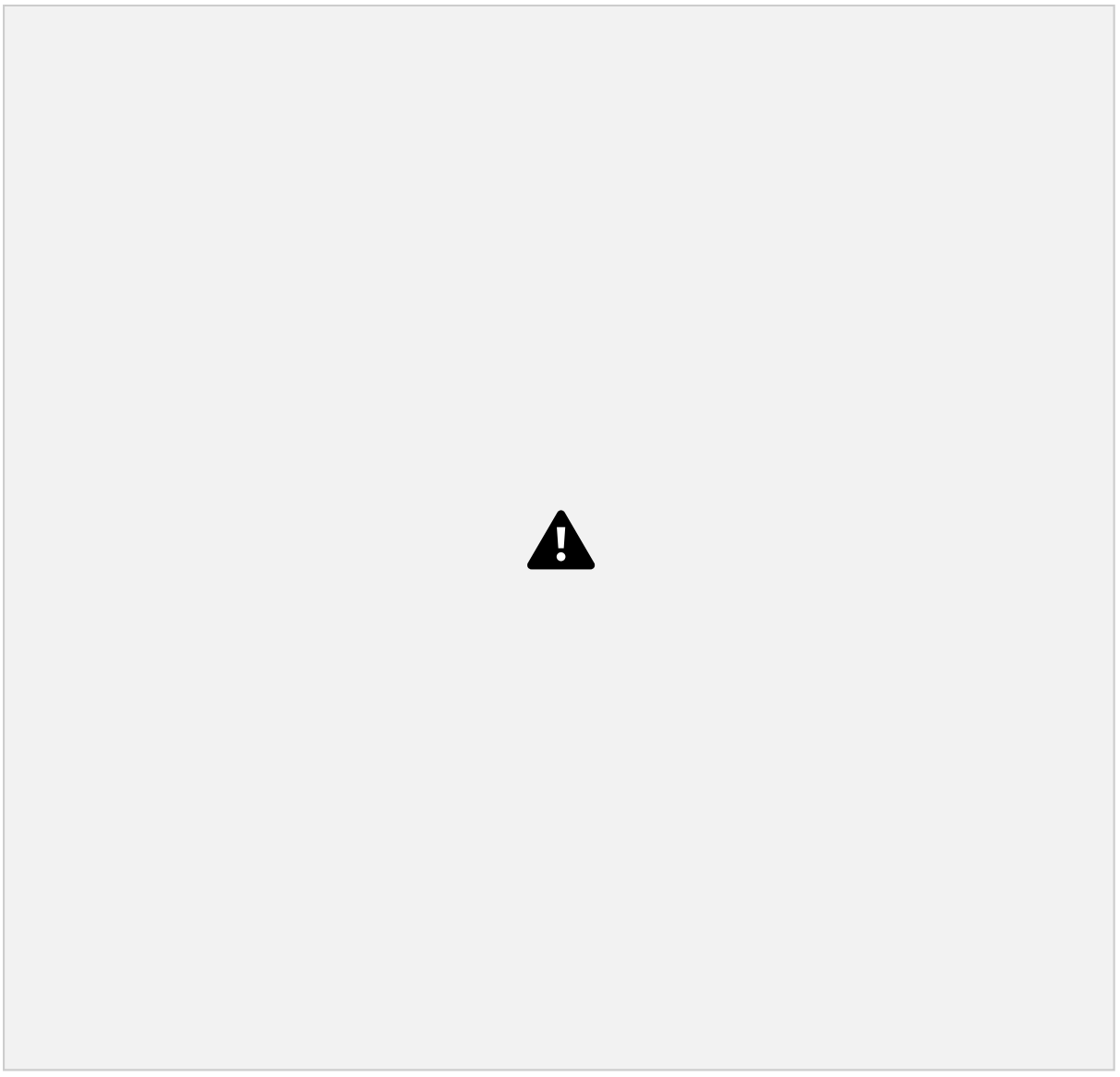


CNS (Roll_50)

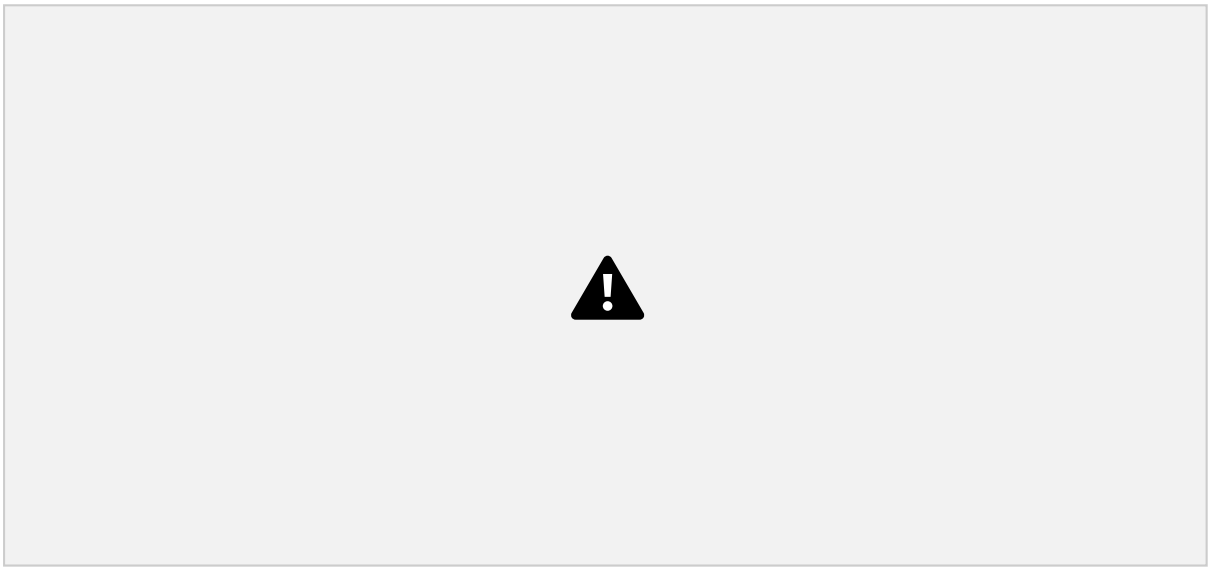


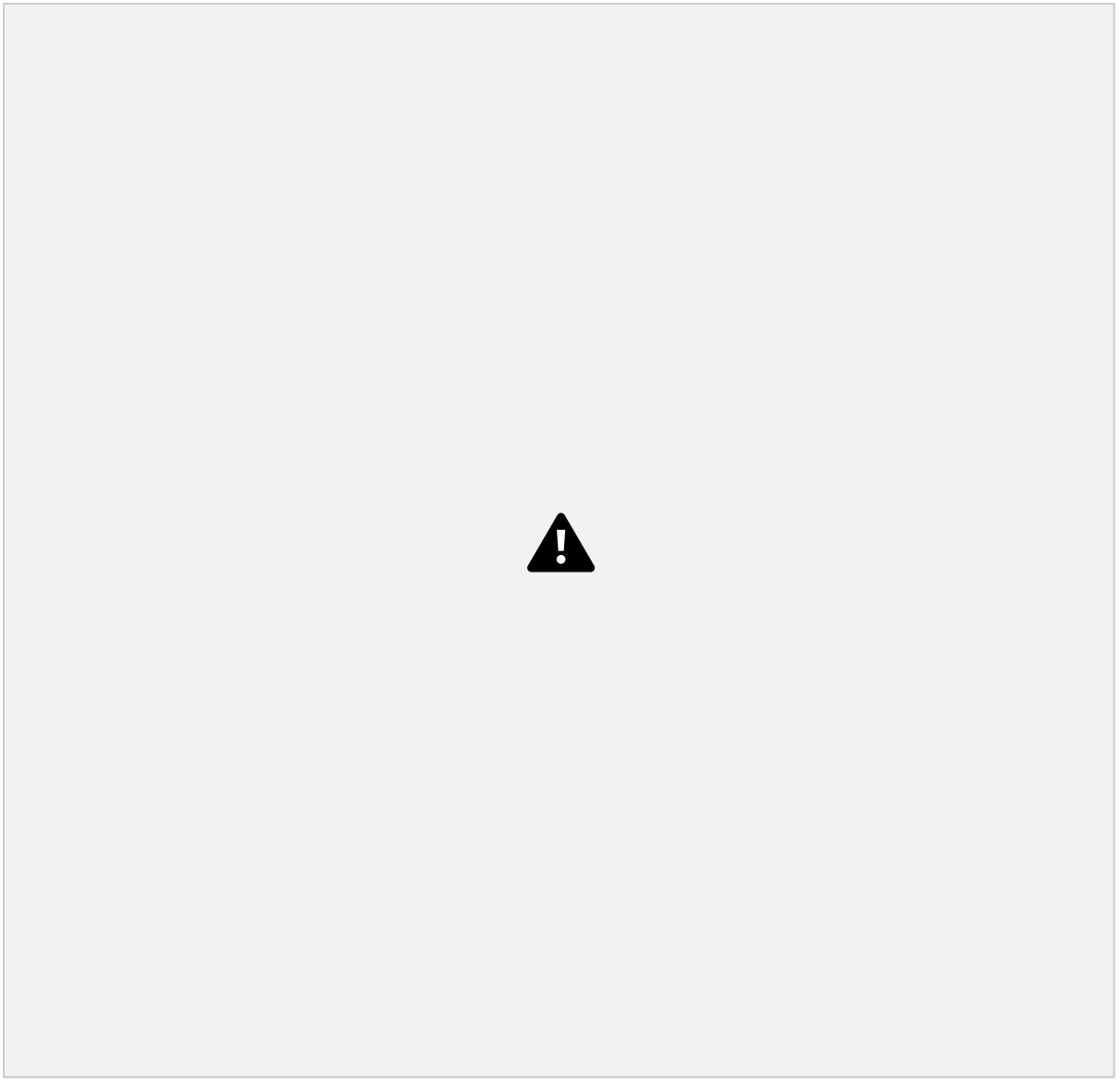
8. Enable OS detection with Nmap





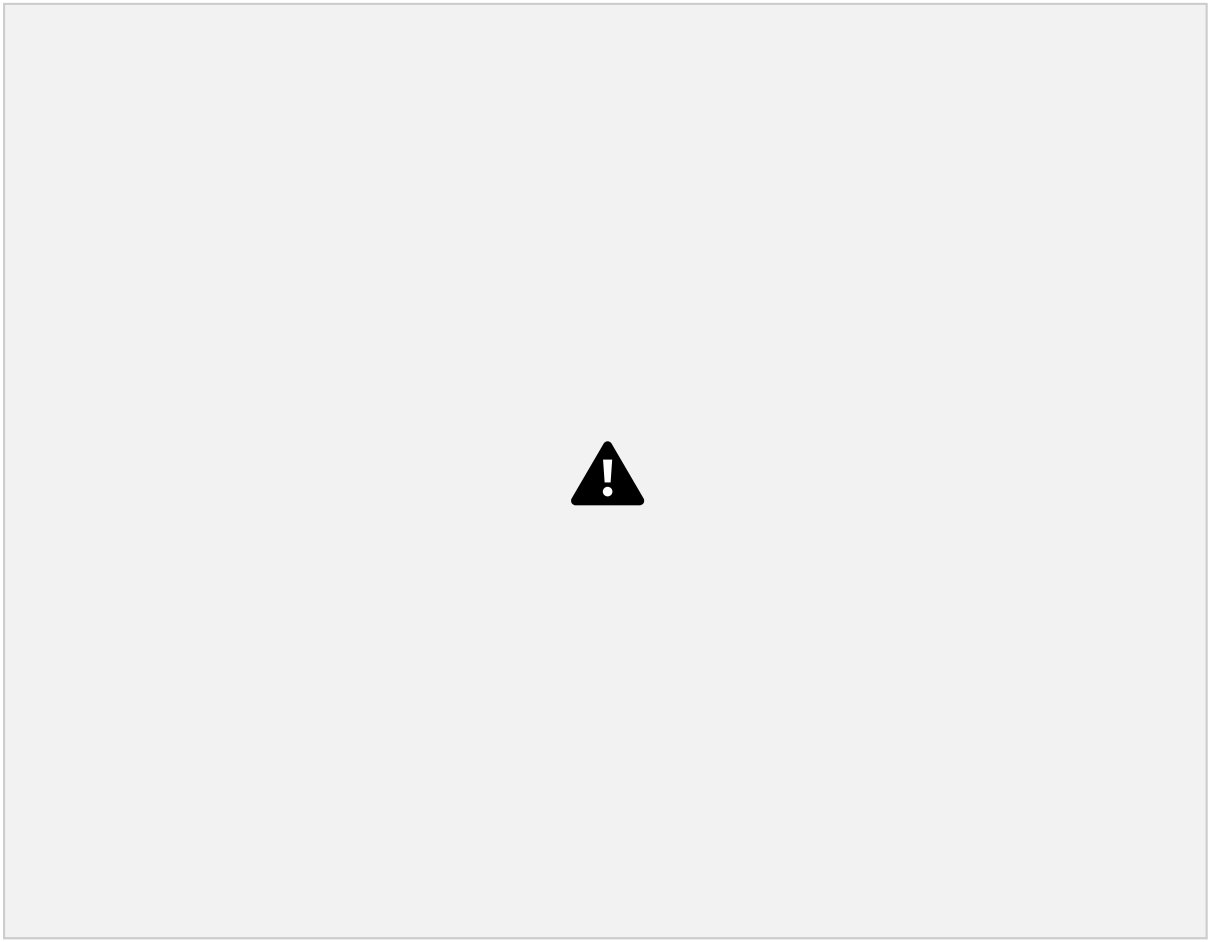
CNS (Roll_50)

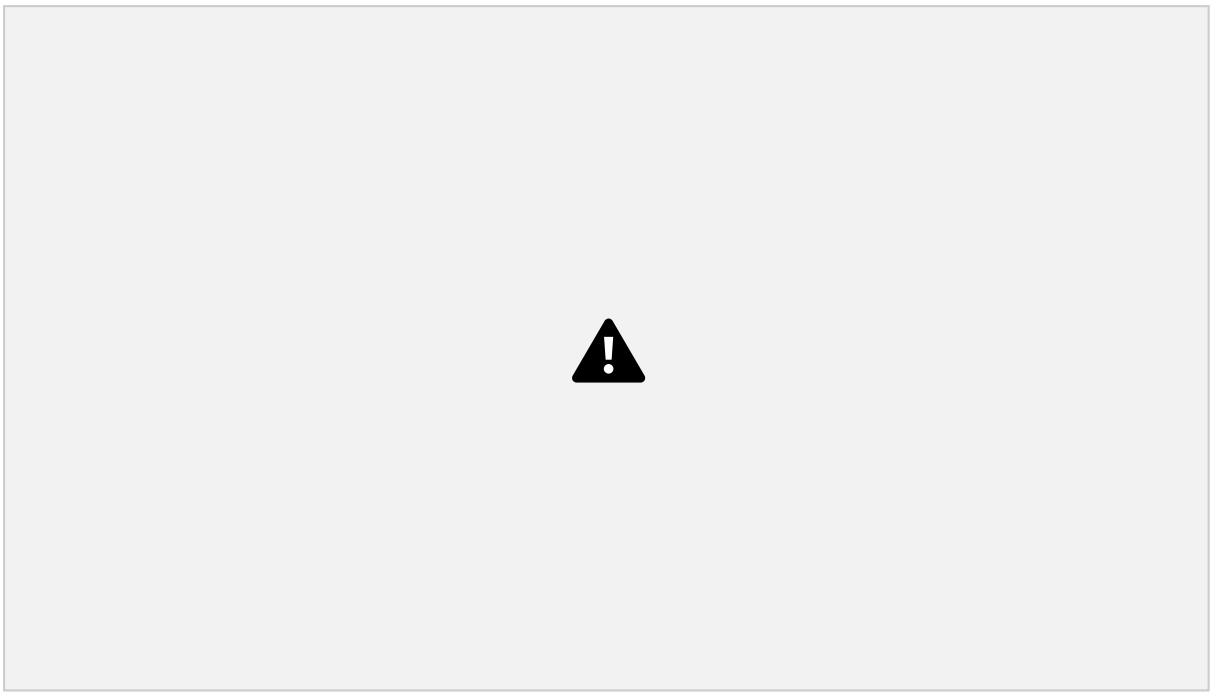


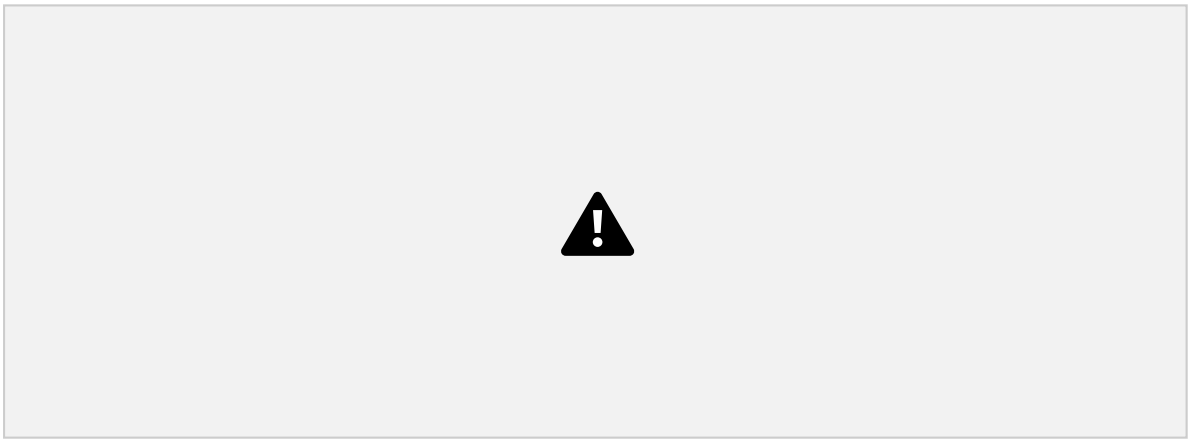


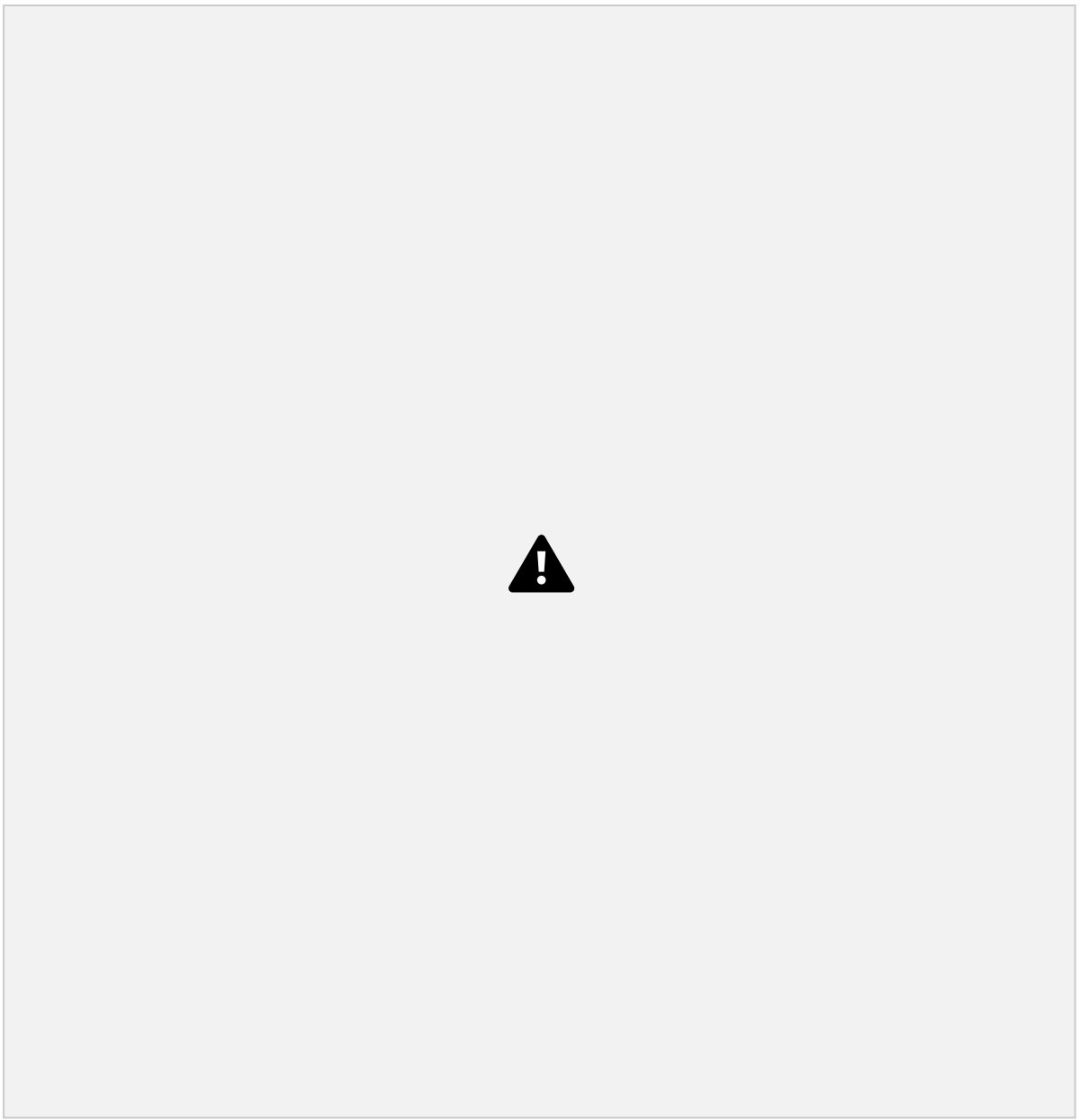
CNS (Roll_50)

9. Scan OS information and Traceroute in details

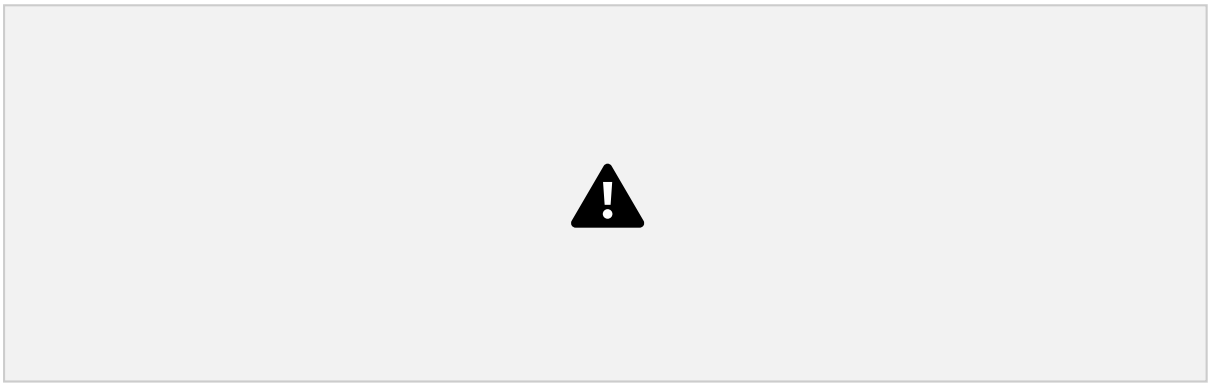


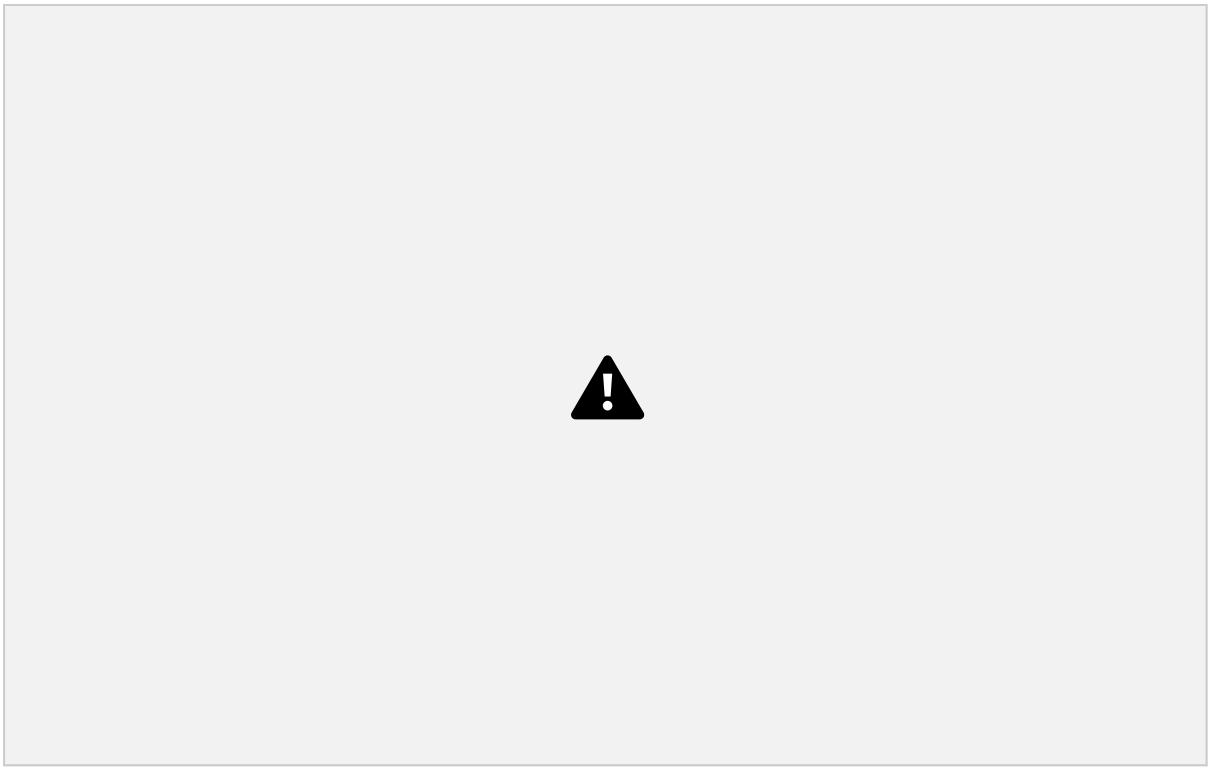




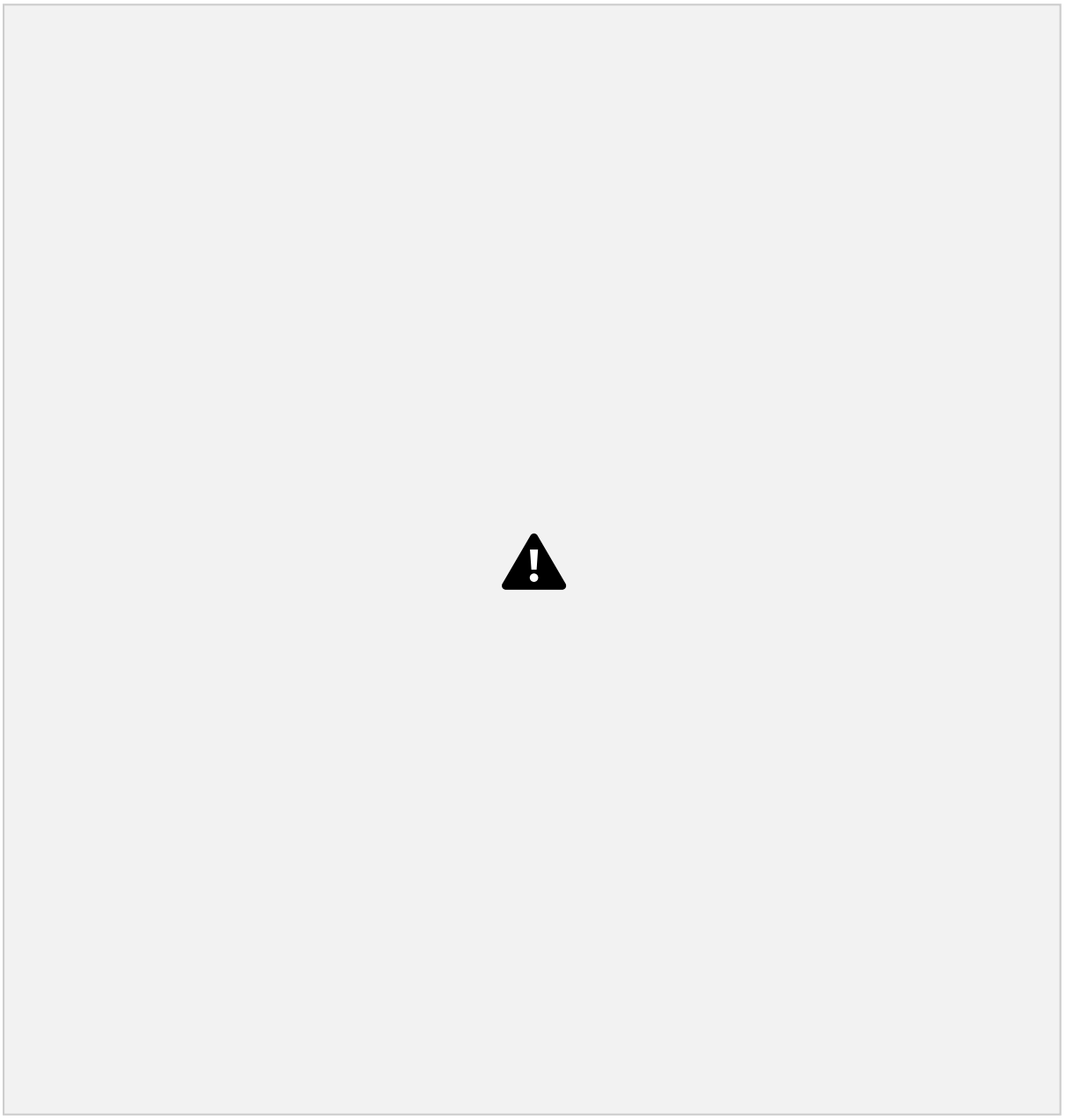


CNS (Roll_50)



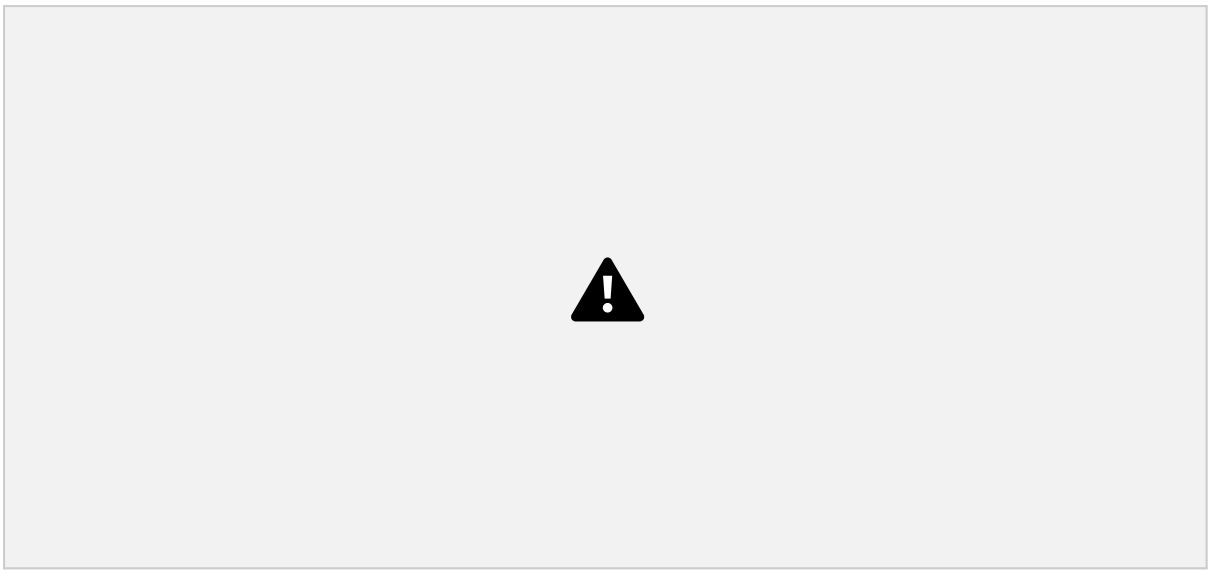


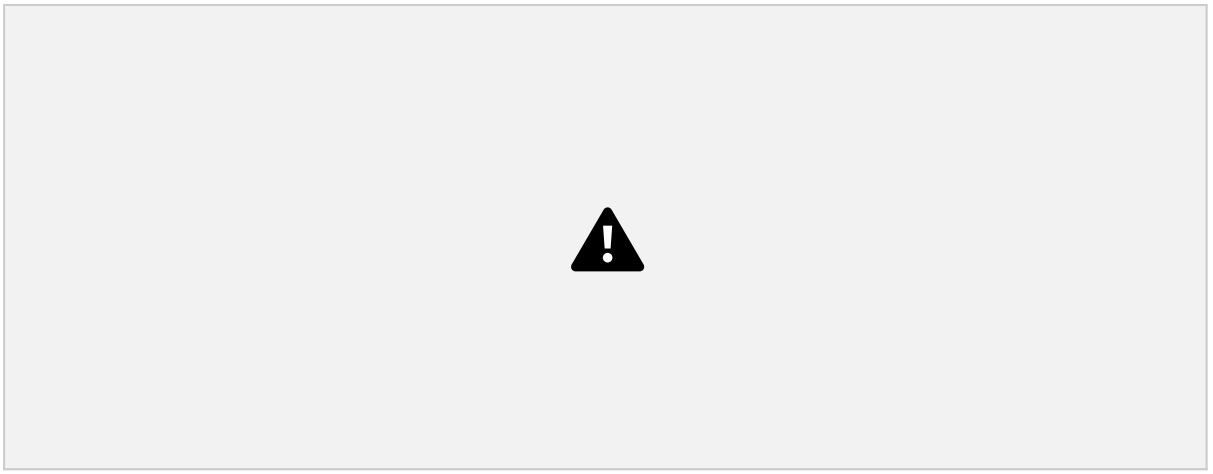
CNS (Roll_50)

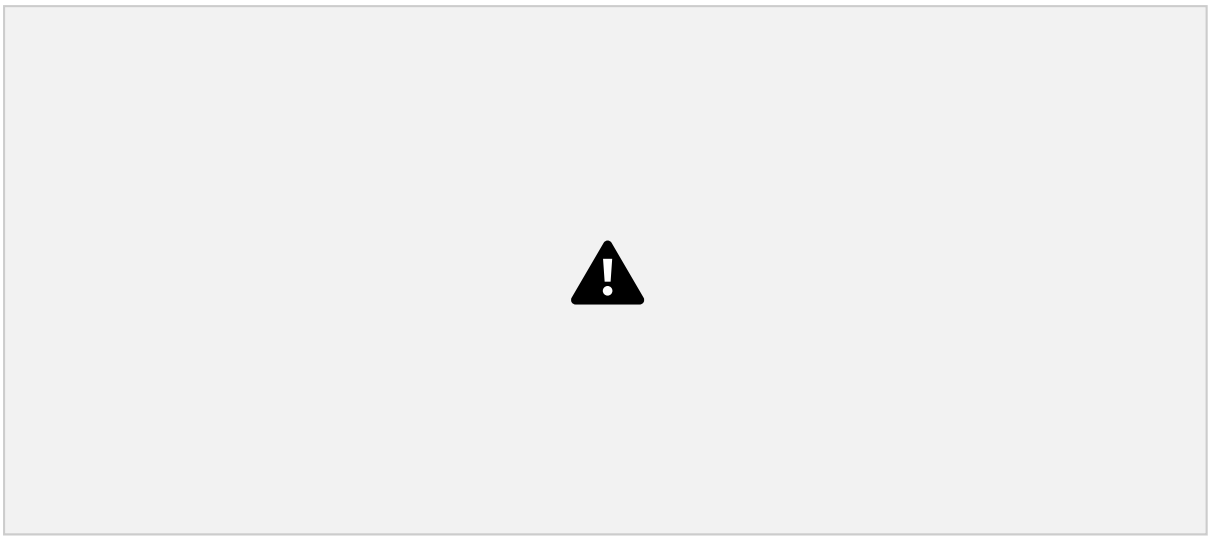


CNS (Roll_50)

10. Perform a stealthy scan

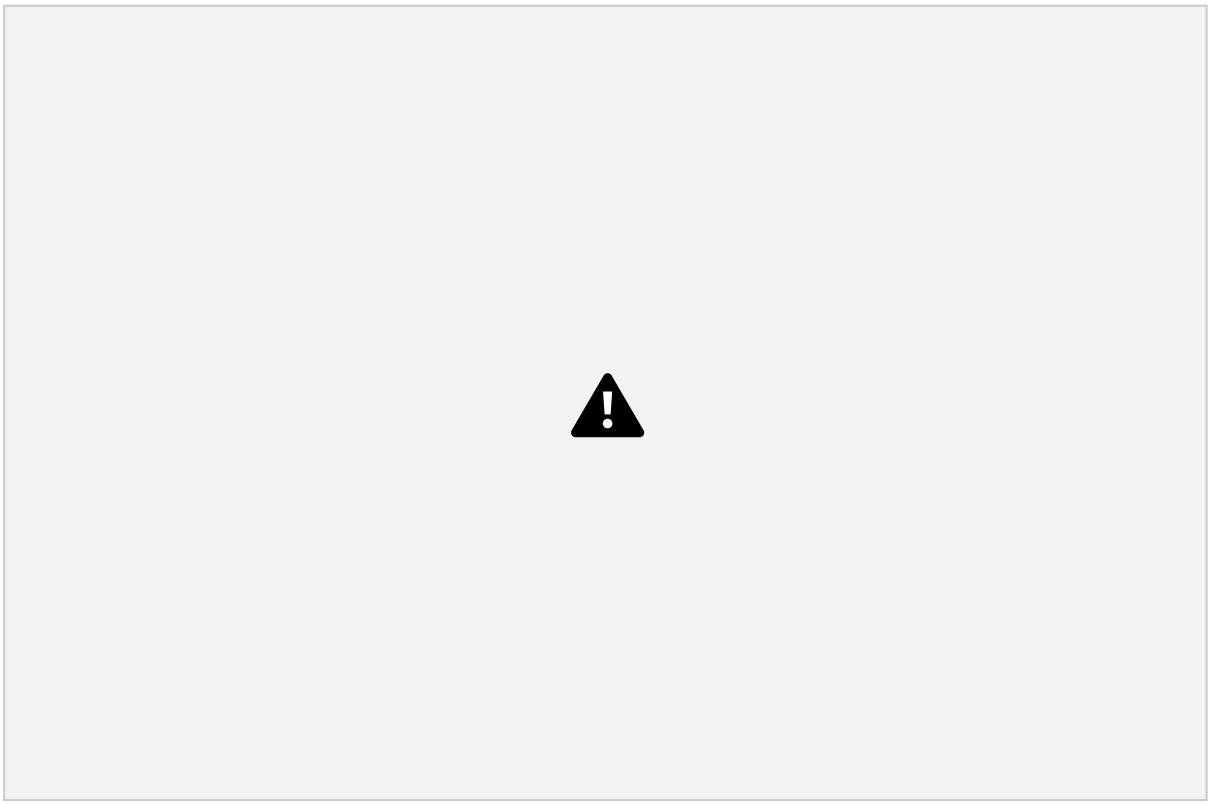


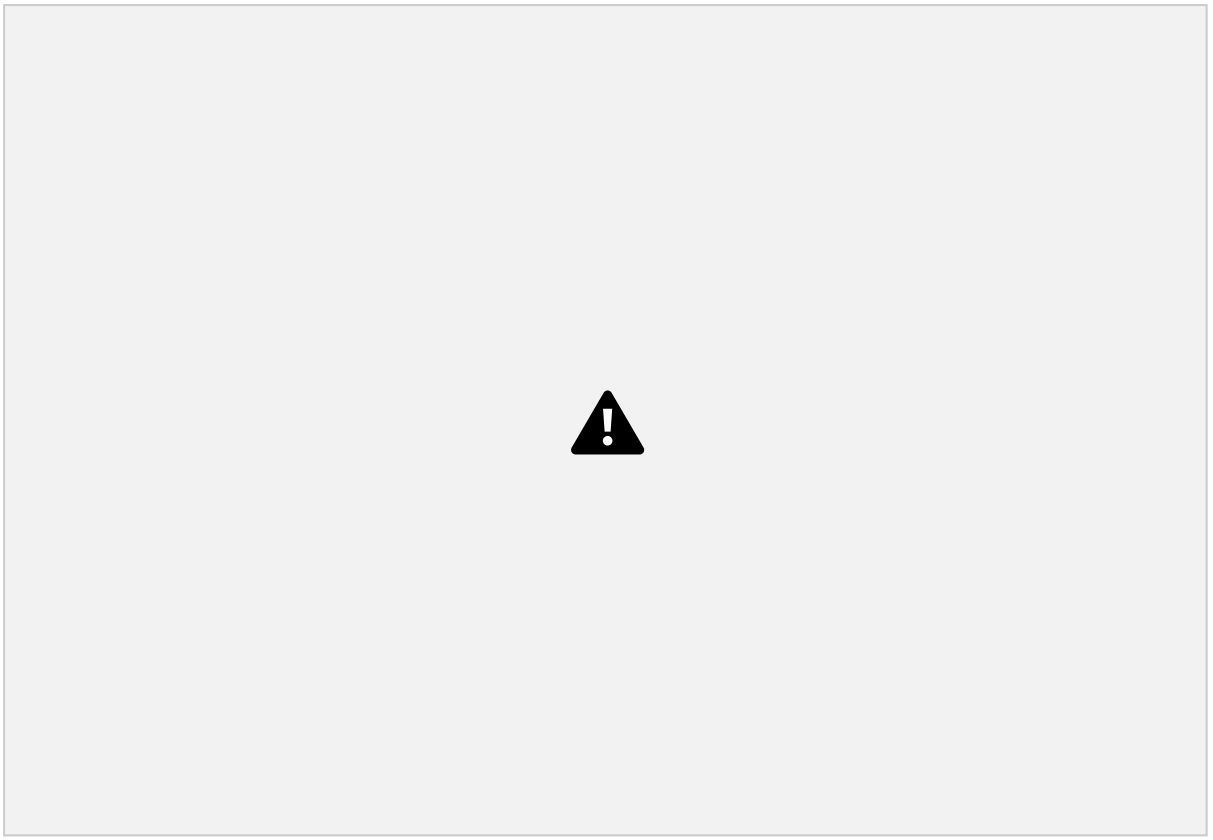




CNS (Roll_50)

11. Check most commonly used Ports with TCP Syn





CNS (Roll_50)