NAME: Mark Lopes

Roll NO: 9913

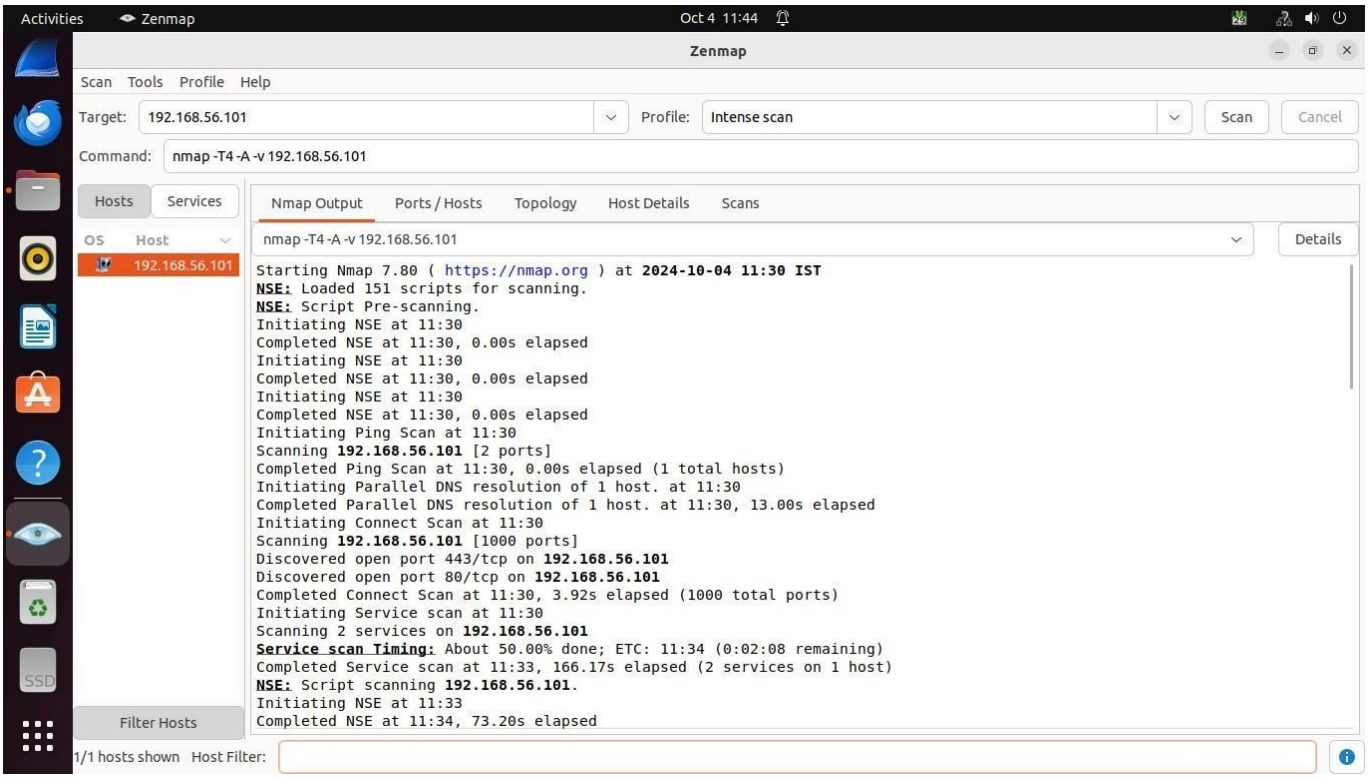
COMP: A

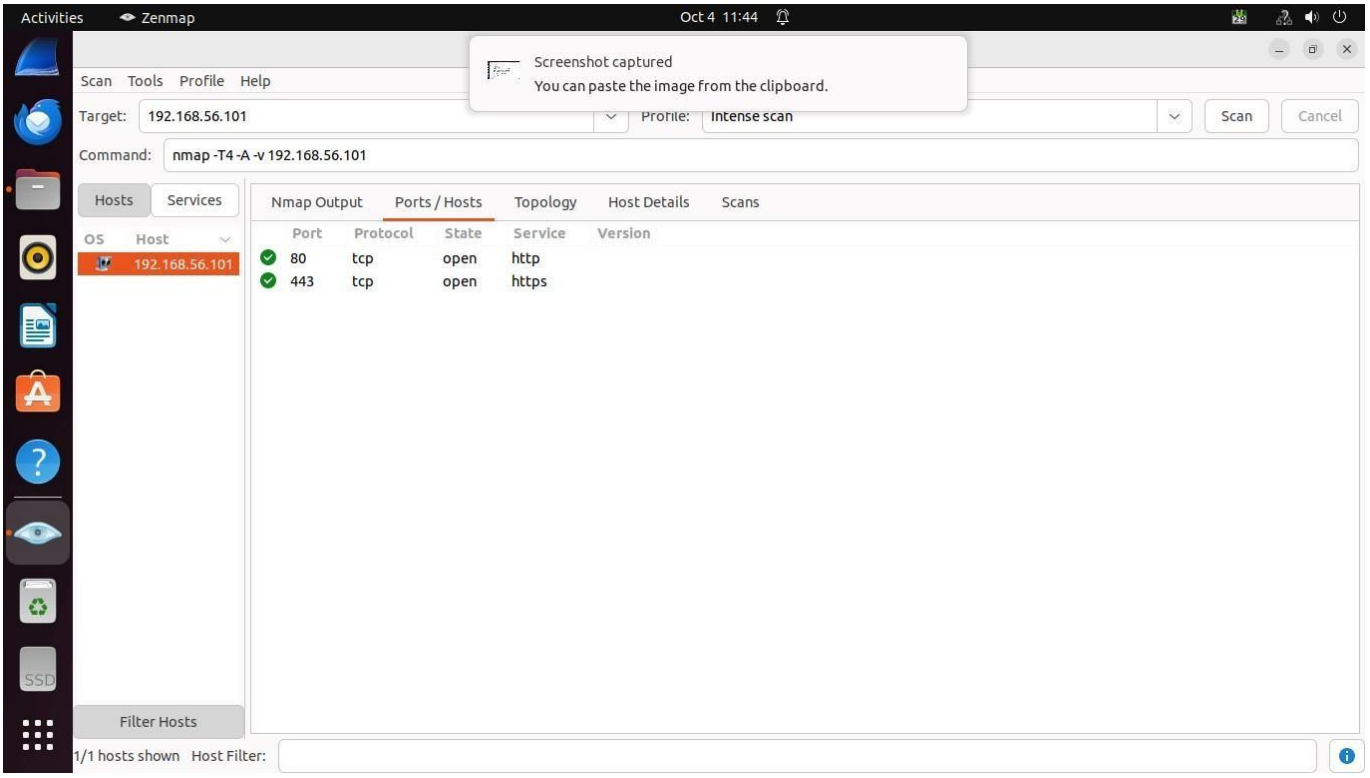
BATCH : C

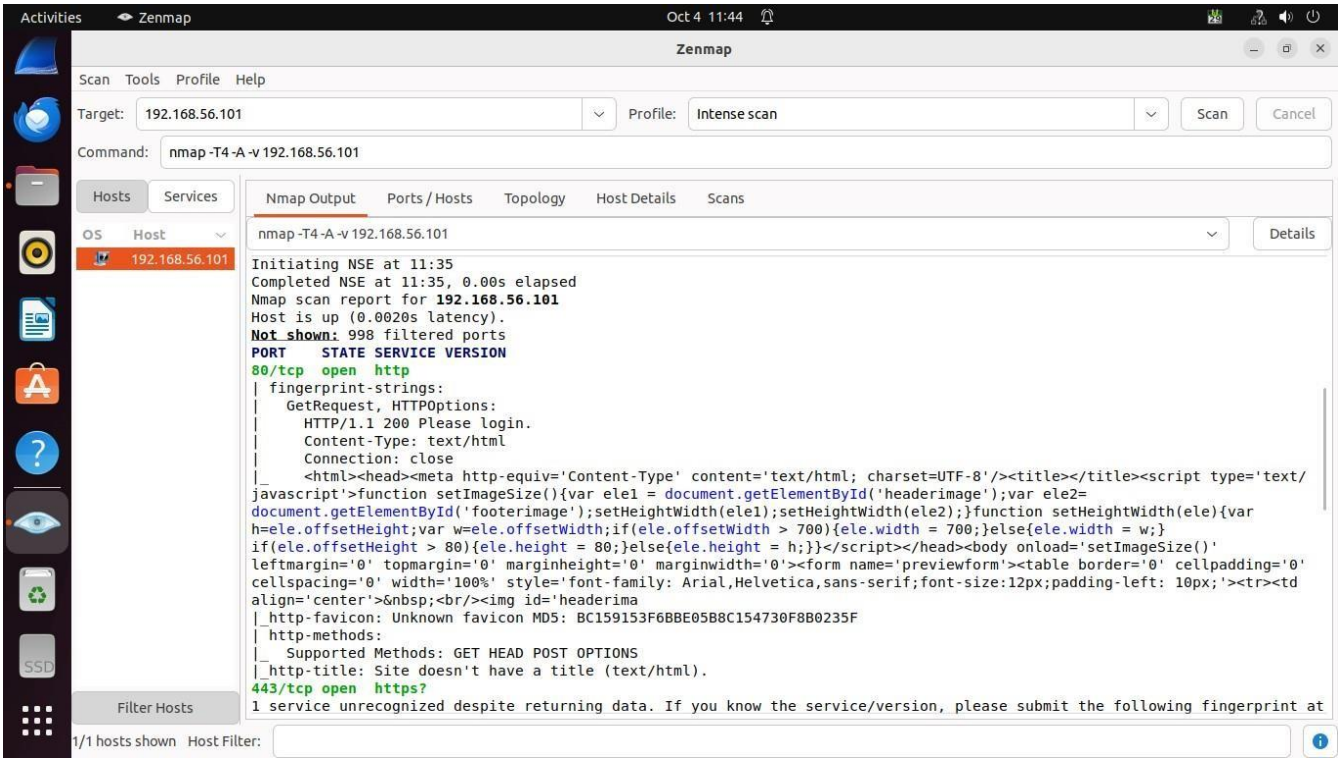
EXPERIMENT NO.4

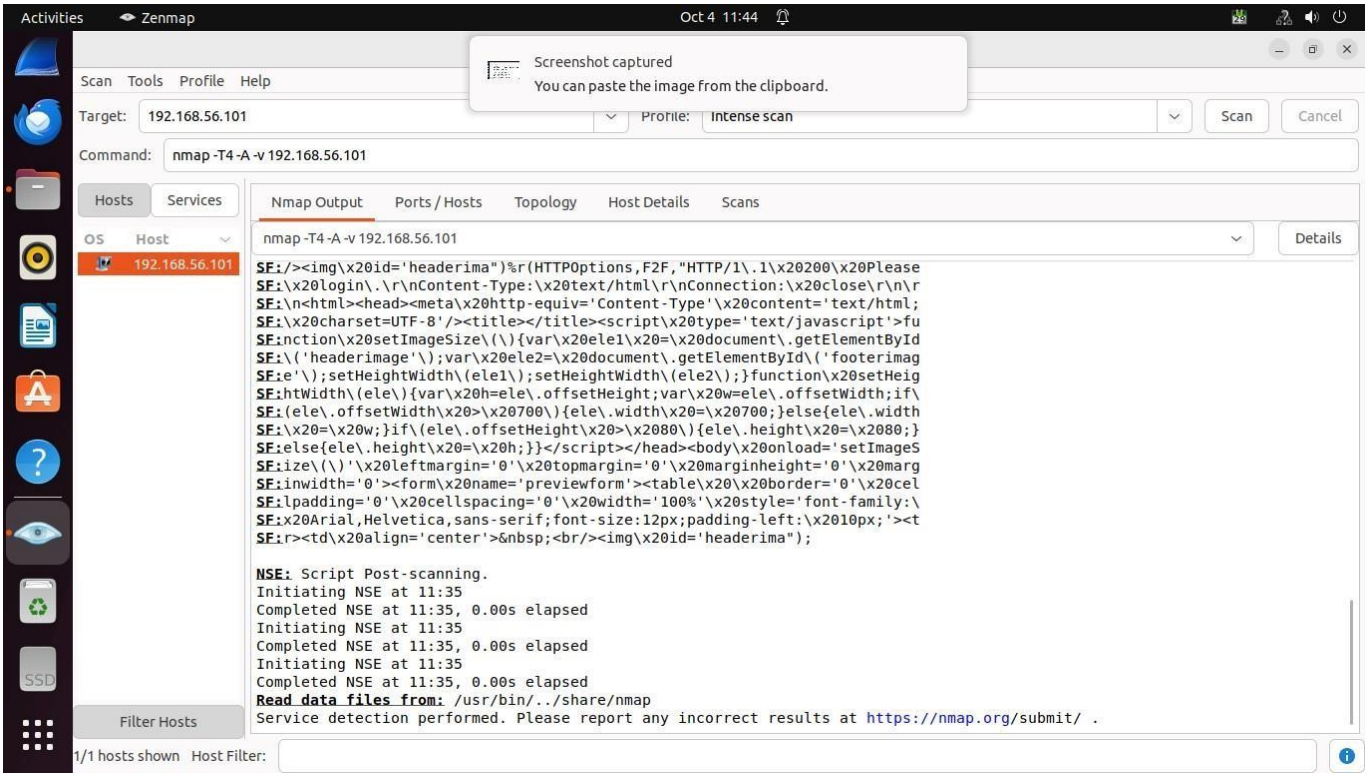
AIM: Perform network discovery using discovery tools (eg. Nmap, mrtg)

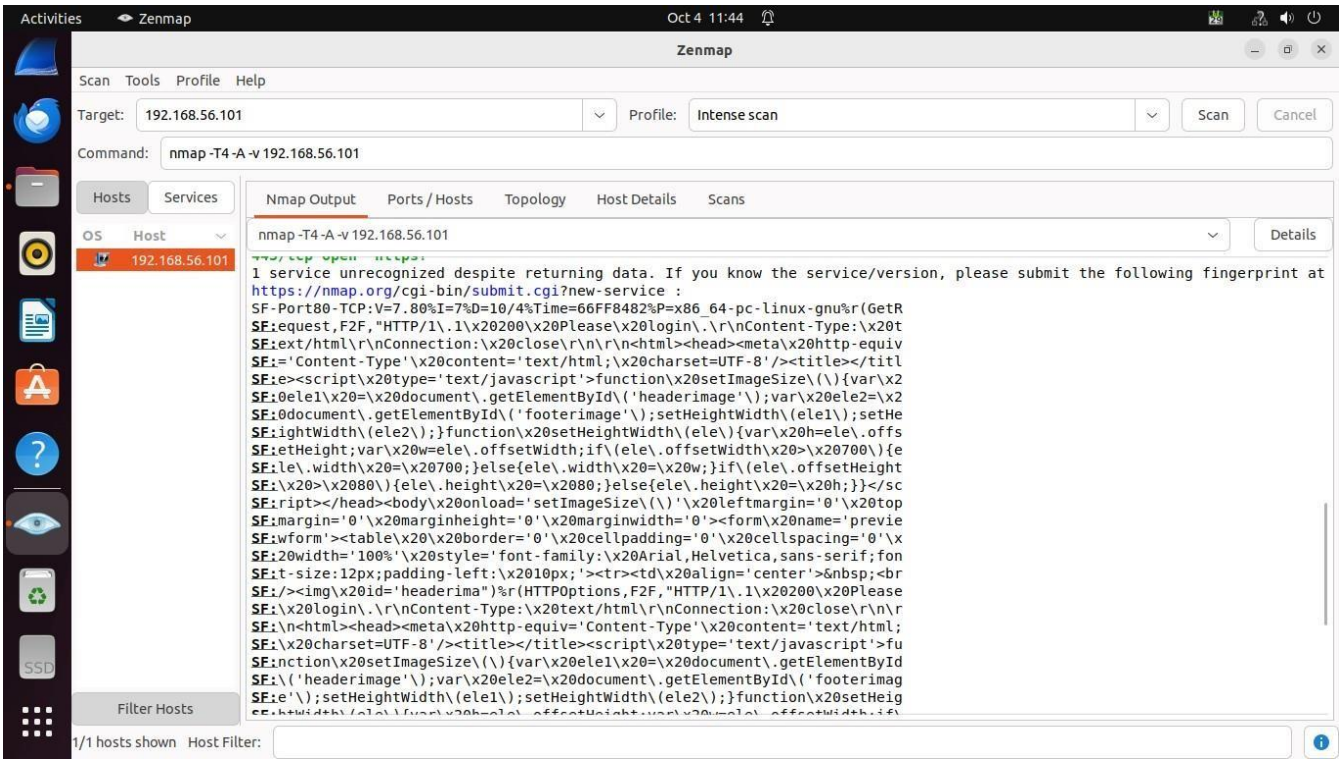
Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also knownby his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.




Activities
Zenmap
Oct 4 11:44
Screenshot captured
You can paste the image from the clipboard.
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.56.101
Hosts
Services
OS Host
192.168.56.101
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port Protocol State Service Version
80 tcp open http
443 tcp open https
Filter Hosts
1/1 hosts shown Host Filter:


Activities
Zenmap
Oct 4 11:44
Zenmap
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.56.101
Hosts
Services
OS Host
192.168.56.101
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.56.101
Details
Initiating NSE at 11:35
Completed NSE at 11:35, 0.00s elapsed
Nmap scan report for 192.168.56.101
Host is up (0.0020s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http
| fingerprint-strings:
| GetRequest, HTTPOptions:
| HTTP/1.1 200 Please login.
| Content-Type: text/html
| Connection: close
|_ <html><head><meta http-equiv='Content-Type' content='text/html; charset=UTF-8'/><title></title><script type='text/
javascript'>function setImageSize(){var ele1 = document.getElementById('headerimage');var ele2=
document.getElementById('footerimage');setHeightWidth(ele1);setHeightWidth(ele2);}function setHeightWidth(ele){var
h=ele.offsetHeight;var w=ele.offsetWidth;if(ele.offsetWidth > 700){ele.width = 700;}else{ele.width = w;}
if(ele.offsetHeight > 80){ele.height = 80;}else{ele.height = h;}}</script></head><body onload='setImageSize()'
leftmargin='0' topmargin='0' marginheight='0' marginwidth='0'><form name='previewform'><table border='0' cellpadding='0'
cellspacing='0' width='100%' style='font-family: Arial,Helvetica,sans-serif;font-size:12px;padding-left: 10px;'><tr><td
align='center'>
<img id='headerima
|_http-favicon: Unknown favicon MD5: BC159153F6BBE05B8C154730F8B0235F
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
443/tcp open https?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
Filter Hosts
1/1 hosts shown Host Filter:





CONCLUSION: We have explored various methods for scanning ports, with Nmap standing out as a robust network scanning tool developed by Gordon Lyon. It works by sending specialized packets and interpreting the responses to map network structures. Nmap's strength lies in its ability to adjust to varying network conditions, supported by an active community. In addition to determining host availability and port status, it can also detect

operating systems, service versions, uptime, device types, and firewalls, making it an all-encompassing solution for network discovery and security evaluations.