Acropolis Institute of Technology & Research, Indore

Department of Computer Science & Information Technology

EVALUATION OF INTERNSHIP REPORT

B.Tech: III Year

Report

Nmap Utility Command

Submitted to -

Prof. Nidhi Nigam

Submitted by -

Jessica Chouhan
0827CI201087
CSIT-2

Department of Computer Science & Information Technology
AITR, Indore

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

Certificate

Certified that training work entitled "*Cyber Security*" is a bonafied work carried out after sixth semester by "*Jessica Chouhan*" in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from "*Prof. Nidhi Nigam (CEH certified)*" Acropolis Institute of Technology and Research during the academic year 2022-23.

Name and Sign of Training Coordinator *Name & Sign of Internship Coordinator*

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

<u>ACKNOWLEDGEMENT</u>

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training coordinator, *Prof. Nidhi Nigam (CEH certified)* , CSIT Department, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by him/her. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

Name – Jessica Chouhan
Enrollment No. – 0827CI201087

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

INDEX

Introduction to Technology Undertaken
(Cyber Security)

Cyber security is currently one of the fastest growing and most in-demand industries in terms of employment opportunities. There are several reasons for this quicker-than-average growth across nearly every type of cyber security career. This includes the fact that cyber attacks are increasing at an unprecedented rate, and the malicious actors behind these infiltrations are continuously coming up with new attack strategies.

Often, all that stands between an organization and a full-scale, damaging data breach are internal cyber security professionals and the tactics they put in place for protection. Beyond just guarding against unauthorized access, these cyber security professionals are also responsible for maintaining continuous uptime of the organization’s most crucial IT assets while supporting these platforms’ top-notch performance for end users.

The types of cyber security jobs available in today’s market are multi-disciplinary and touch every department of the business. Organizations from enterprises and small businesses to government agencies now need highly trained and knowledgeable IT and cyber security personnel to guard against attacks and support the technologies that underpin daily operations.

In today's digital world, cybersecurity has become an essential part of every company's strategy for sustainability, security, and growth. As businesses grow, the demand for cybersecurity talent will only continue to grow in 2023 and beyond.

Cyber security is a growing industry that is still in need of skilled professionals. The global cyber security market is expected to grow from $170 billion in 2017 to $202 billion in 2023.

The demand for cyber security jobs has risen significantly over the past few years. More than 1 million cyber security jobs will be available by 2023, but less than 400,000 cybersecurity professionals will be trained by then. Cyber security is an ever-growing industry. It is projected to grow by 11% in 2023 and by 20% in 2025. This is a fast-paced career with a median salary of $81,000.

Objectives

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

1. Protect the confidentiality of data.
2. Preserve the integrity of data.
3. Promote the availability of data for authorized users.

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the **AIC (Availability, Integrity, and Confidentiality)** triad to avoid the confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

The CIA criteria are one that most of the organizations and companies use when they have installed a new application, creates a database or when guaranteeing access to some data. For data to be completely secure, all of these security goals must come into effect. These are security policies that all work together, and therefore it can be wrong to overlook one policy.

1. Confidentiality

Confidentiality is roughly equivalent to privacy and avoids the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content. It prevents essential information from reaching the wrong people while making sure that the right people can get it. Data encryption is a good example to ensure confidentiality.

2. Integrity

Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not be altered in an unauthorized way, and that source of the information is genuine.

3. Availability

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Project undertaken

(Nmap Utility Commands using cmd)

Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. It is a globally recognized tool mostly used by networking experts and penetration testers to find services, hosts, and open ports on a computer network. Network mapper allows its users to discover which devices are running on the network, find vulnerabilities, and detect installed services.

Nmap Commands

1. Scan a Range of IP Address

To scan the entire CIDR(classless inter-domain routing) range of IP addresses, you can use this command.

Command: nmap <IP range>

2. Port Scanning

Nmap is the best port scanning tool. Performing port scans will provide you with details about port services and states. It scan a specific port or entire port range.

Command: nmap -p <numeric value> <IP>

3. Ping Scan Using Nmap

This is one of the most popular and easiest Nmap commands for host detection. If you are interested in knowing which hosts are running in your network, you should use this command. It also provides the option to find out multiple hosts or any specific host. This command returns the IP address and MAC address of available hosts but provides no information about ports.

Command: Nmap -sP <target>

4. Saving the Nmap Scan Output to a File

Security tool Nmap has become a crucial tool in the cyber security field. And Nmap allows its users to export or save scan results into the text file or XML.

Command: nmap -oN output.txt example.com (This command will export Nmap scan into a text file)

nmap -oX output.xml example.com (This command will save the output of Nmap scanning in XML)

5. Most Popular Ports Scanning

It scan the fixed number of most popular ports.In order to apply this command you have to use the "–top-ports" option with a specific numeric value. This option gives you the ability to scan top ports. However, in Nmap, you also have the option to select the number of top ports to scan. This command allows users to get better and faster results.

Command: nmap –top-ports <numeric value> <IP address/Domain>

6. Display Open Ports

It detect open ports.Finding open ports (target ports that respond to UDP/TCP/SCTP requests) can be the first step to protecting and hacking any network. And if you only want to find ports you can connect to, then this command can be really useful to you.

Command: nmap — open<IP address/domain name>

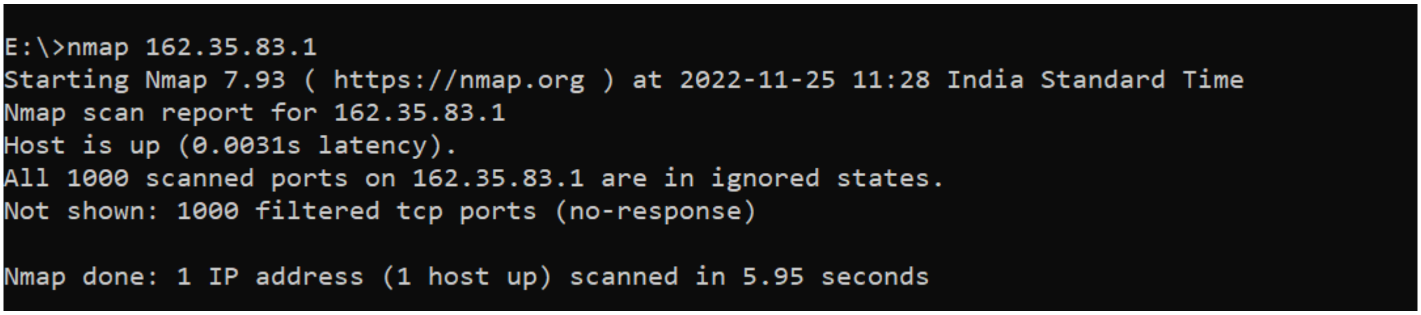
7. Service Version Detection

Nmap has a database of more than 2000 services and associated ports for example– SSH(port 22) and HTTP (port 80). So while doing network inventories if you want to know which versions are running, you can use the Nmap version detection (-sV) command. Knowing the exact version number can be really helpful while finding which exploits your server is vulnerable to.

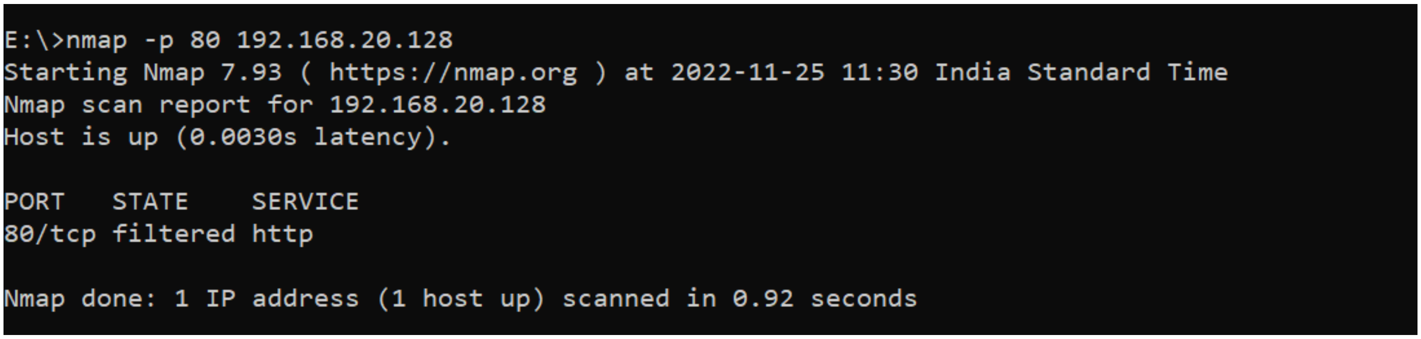
Command: nmap -sV<IP>

Screenshots of Project and Certificates

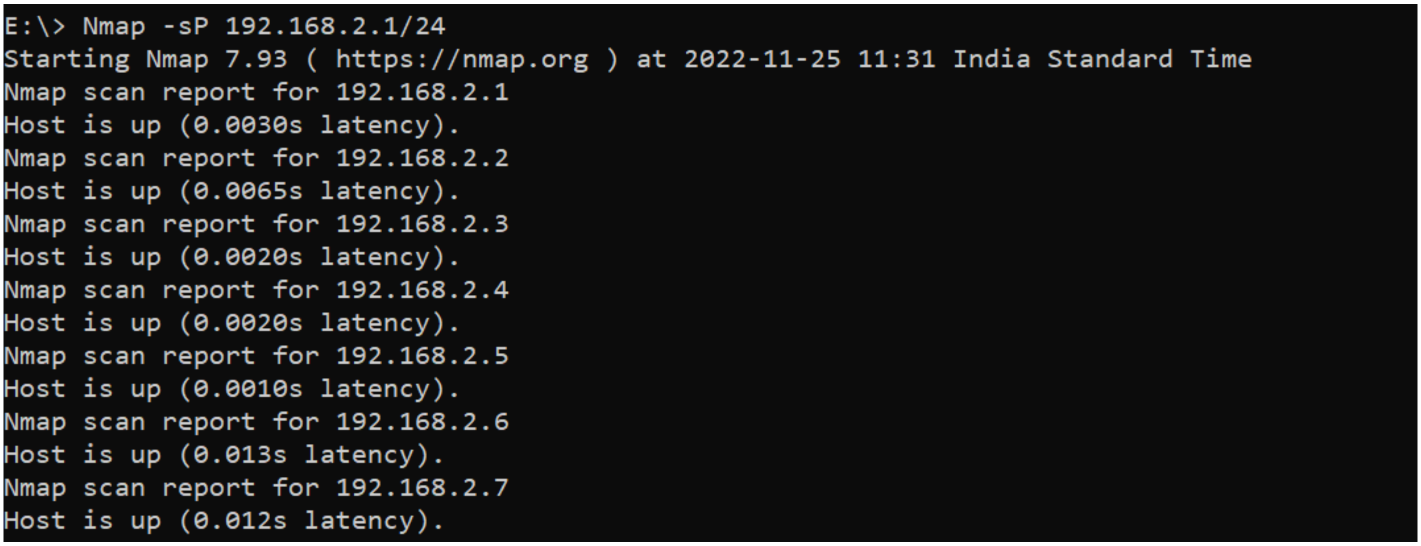
- **Project screenshots :-**



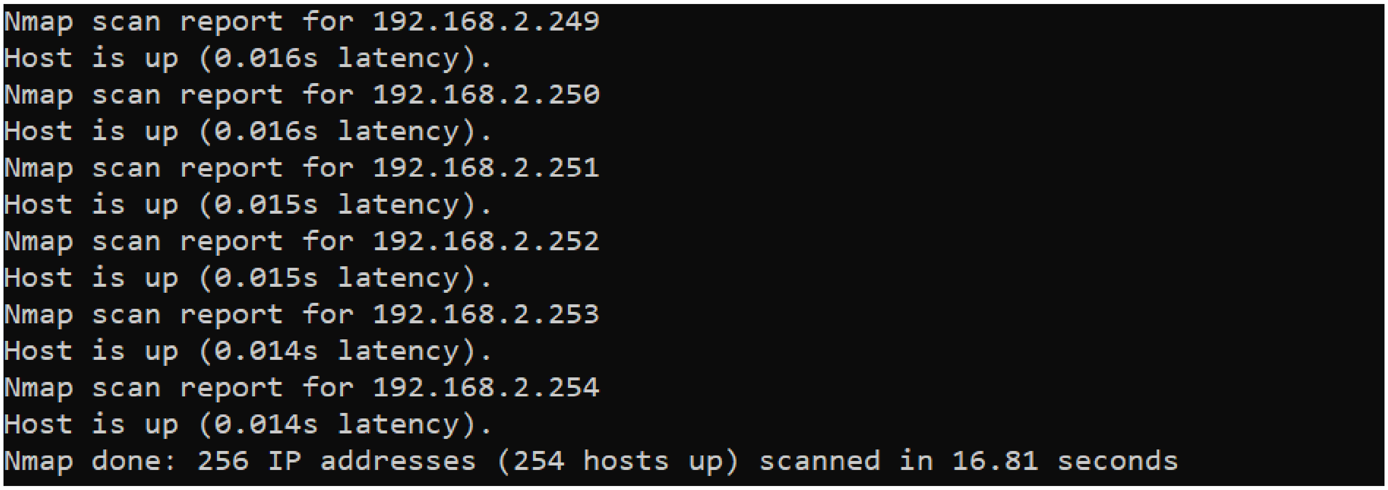
```
E:\>nmap 162.35.83.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:28 India Standard Time
Nmap scan report for 162.35.83.1
Host is up (0.0031s latency).
All 1000 scanned ports on 162.35.83.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.95 seconds
```



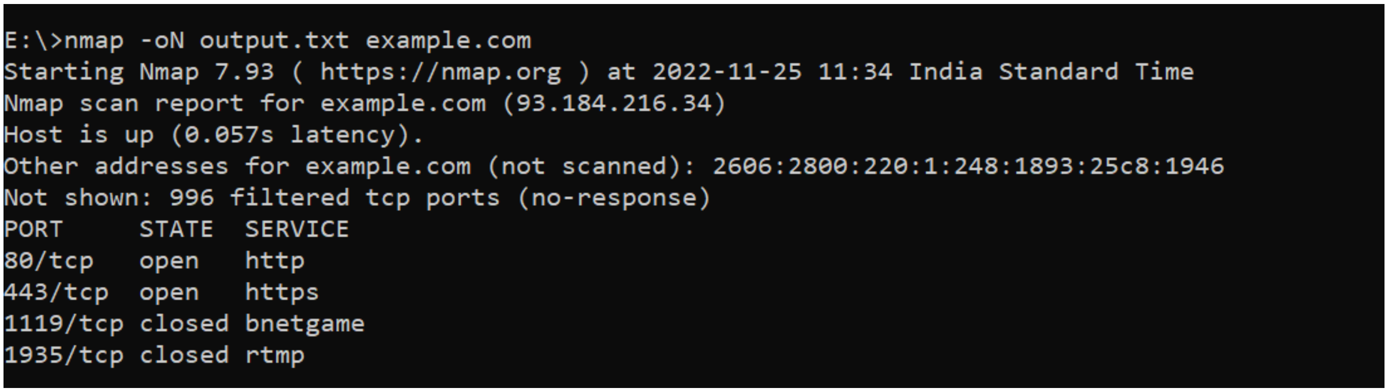
```
E:\>nmap -p 80 192.168.20.128
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:30 India Standard Time
Nmap scan report for 192.168.20.128
Host is up (0.0030s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```



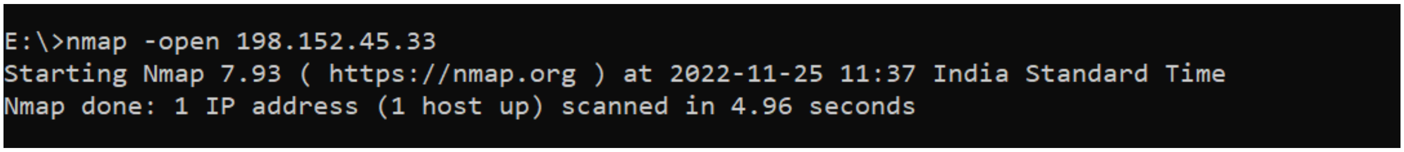
```
E:\> Nmap -sP 192.168.2.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:31 India Standard Time
Nmap scan report for 192.168.2.1
Host is up (0.0030s latency).
Nmap scan report for 192.168.2.2
Host is up (0.0065s latency).
Nmap scan report for 192.168.2.3
Host is up (0.0020s latency).
Nmap scan report for 192.168.2.4
Host is up (0.0020s latency).
Nmap scan report for 192.168.2.5
Host is up (0.0010s latency).
Nmap scan report for 192.168.2.6
Host is up (0.013s latency).
Nmap scan report for 192.168.2.7
Host is up (0.012s latency).
```



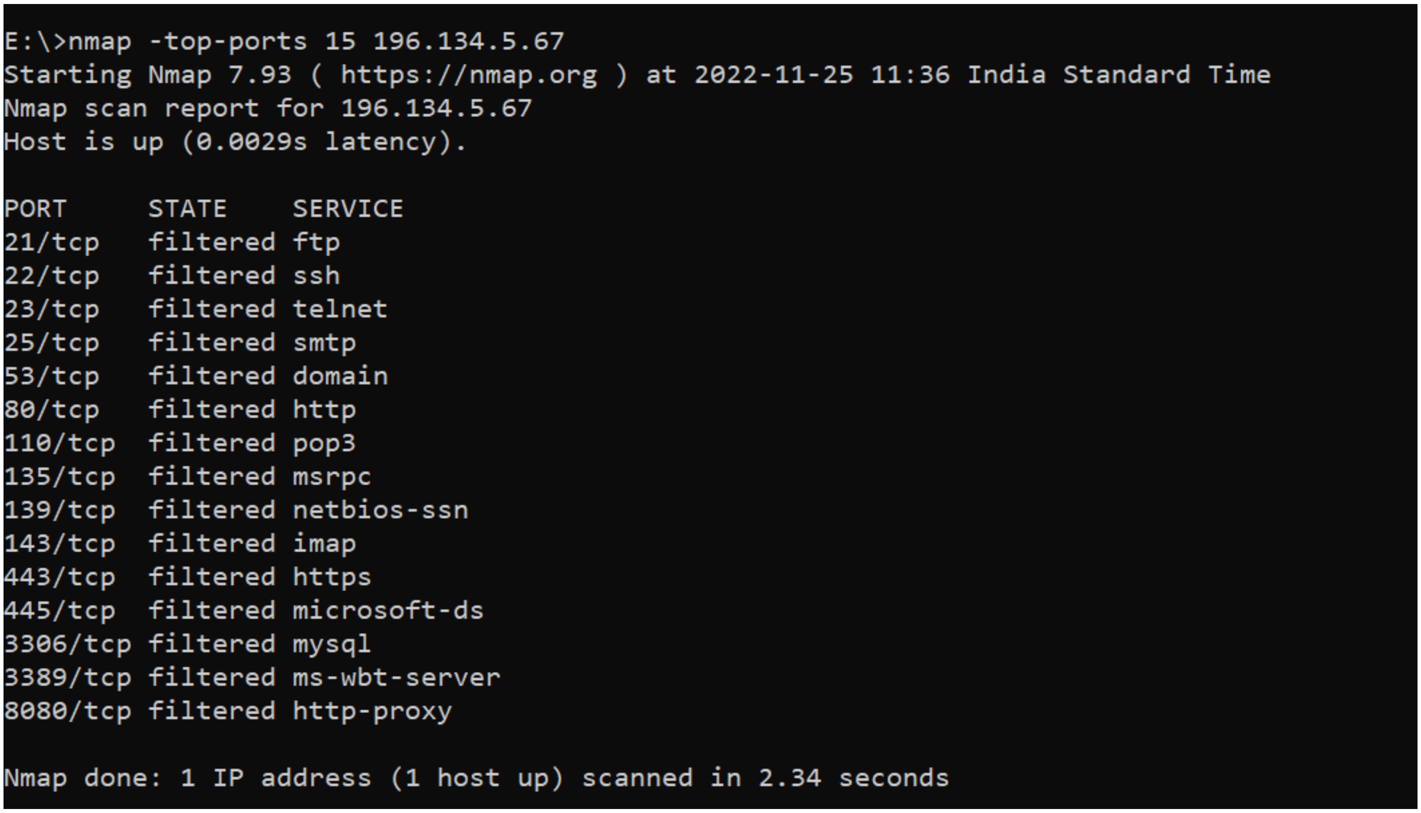
```
Nmap scan report for 192.168.2.249
Host is up (0.016s latency).
Nmap scan report for 192.168.2.250
Host is up (0.016s latency).
Nmap scan report for 192.168.2.251
Host is up (0.015s latency).
Nmap scan report for 192.168.2.252
Host is up (0.015s latency).
Nmap scan report for 192.168.2.253
Host is up (0.014s latency).
Nmap scan report for 192.168.2.254
Host is up (0.014s latency).
Nmap done: 256 IP addresses (254 hosts up) scanned in 16.81 seconds
```



```
E:\>nmap -oN output.txt example.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:34 India Standard Time
Nmap scan report for example.com (93.184.216.34)
Host is up (0.057s latency).
Other addresses for example.com (not scanned): 2606:2800:220:1:248:1893:25c8:1946
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1119/tcp closed bnetgame
1935/tcp closed rtmp
```

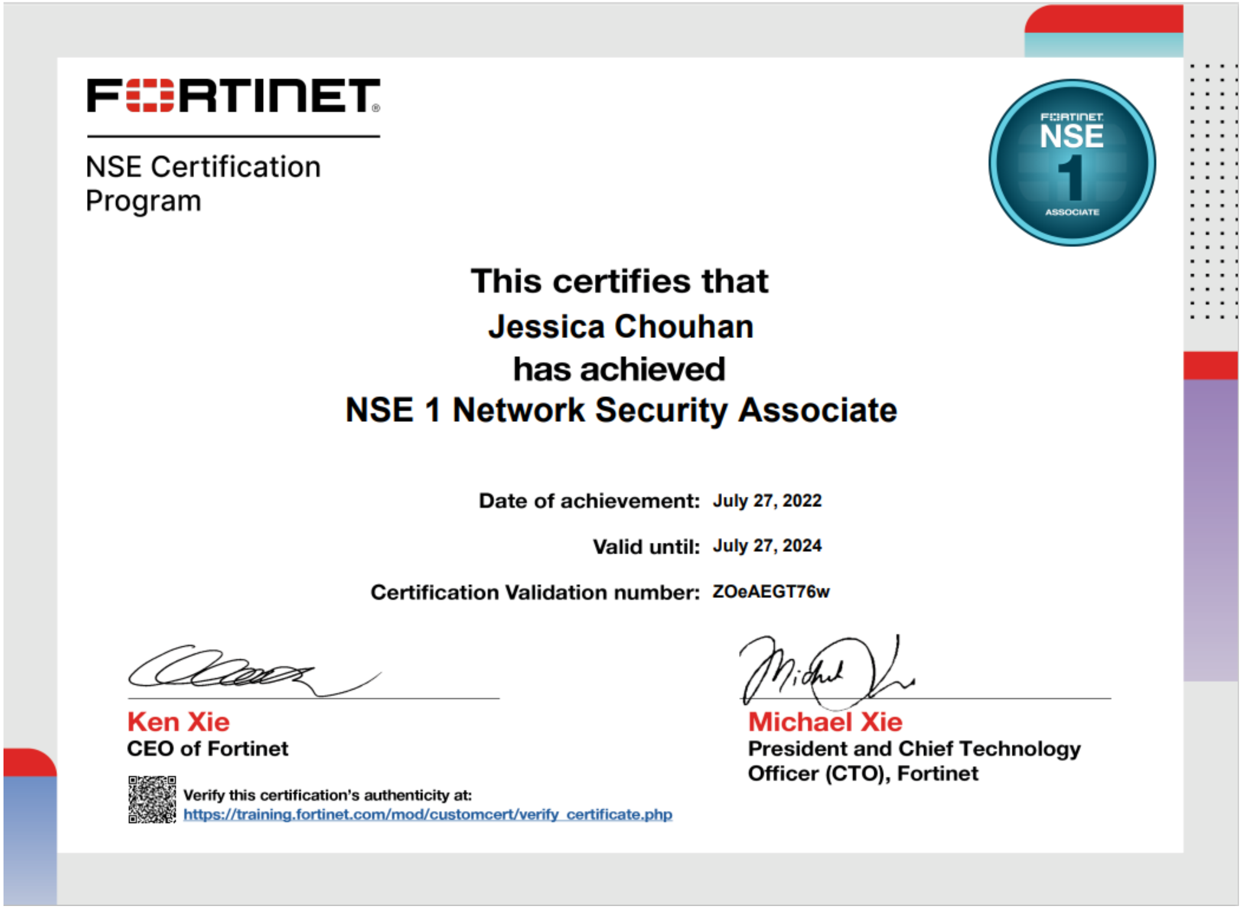


```
E:\>nmap -open 198.152.45.33
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:37 India Standard Time
Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
```



```
E:\>nmap -top-ports 15 196.134.5.67
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-25 11:36 India Standard Time
Nmap scan report for 196.134.5.67
Host is up (0.0029s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.34 seconds
```

- **Certificate :-**



FORTINET

NSE Certification
Program

FORTINET
NSE
1
ASSOCIATE

This certifies that
Jessica Chouhan
has achieved
NSE 1 Network Security Associate

Date of achievement: July 27, 2022

Valid until: July 27, 2024

Certification Validation number: ZOeAEGT76w

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

Github Links (Project/certificate)

Project – https://github.com/Jessica-0103/EOI-Project

Certificate- https://github.com/Jessica-0103/EOI-Project/blob/main/NSE_1_Certification.pdf

Conclusion

As threats and protection measures continue to become more complex and sophisticated, it’s important for employers to find candidates with in-depth knowledge into cyber security and other highly relevant areas. In this way, while a bachelor’s degree may suffice for some types of cyber security careers, the most attractive candidates are those who hold master’s degrees.

Those interested in these or other types of cyber security careers can put themselves on the path to employment by obtaining a high-level degree. The Online Cybersecurity, Master of Science program at the University of Nevada at Reno provides students with the skills, experience and expertise they need to pursue an array of exciting and high-compensating cyber security careers.