PENTESTING ON DATA CENTER

AND NMAP TOOL

A REPORT

Submitted by

CH DHEERAJ
[RA2111030010182]

Under the Guidance of

Dr. D. Deepika

Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING
with specialization in CYBER SECURITY

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603203

APRIL 2024

COLLEGE OF ENGINEERING & TECHNOLOGY SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report **“Pentesting On Datacenter and N MAP Tool”** is the bonafide work of “**CH Dheeraj**” of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE	SIGNATURE
Dr. D. Deepika	Dr. Annapurani Panaiyappan K
Assistant Professor	Professor and Head
Networking and Communications	Networking and Communications

CASE STUDY ON “Pentesting On Data Center And Nmap Tool”

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester : III/VI

Report Title **:** Pentesting on Data Center and NMAP Tool

Course Faculty **:** Dr. D. Deepika

Student Name **:** CH DHEERAJ[RA2111030010182]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

Introduction

In today's digital landscape, safeguarding sensitive data is a top priority for organizations across all industries. ABC Corporation, a leading data management provider, is taking proactive measures to ensure the security and integrity of its data center infrastructure by undergoing a comprehensive penetration testing initiative. This strategic move is designed to assess the existing security protocols and identify potential vulnerabilities that could be exploited by malicious actors.

Penetration testing, also known as ethical hacking, involves simulating cyberattacks on a company's systems to uncover weaknesses that may exist within the network, servers, and applications. The primary objective of this initiative is to rigorously evaluate the data center's security posture, providing a thorough examination of its resilience against potential threats such as unauthorized access, data breaches, and cyberattacks.

Through this process, ABC Corporation aims to gain valuable insights into its current security measures and identify areas for improvement. The findings from the penetration testing will be used to propose targeted mitigation strategies, strengthening the data center's defenses and enhancing the overall protection of its data and systems.

By investing in a robust penetration testing initiative, ABC Corporation demonstrates its commitment to maintaining a secure data environment for its customers and stakeholders. This proactive approach not only helps the organization stay ahead of emerging threats but also fosters trust and confidence in its ability to safeguard critical data. As a result, the corporation can continue to deliver high-quality data management services with the assurance of a fortified security posture.

Scope

The penetration testing initiative encompasses the entire data center infrastructure of ABC Corporation. This includes:

1. Network Components: All network devices such as routers, switches, firewalls, load balancers, and other network infrastructure that connects and supports data center operations.

2. Servers and Systems: All servers and systems running within the data center, including web servers, application servers, database servers, and other specialized systems.

3. Applications: All applications hosted in the data center, including those used internally by ABC Corporation and those offered to customers or partners.

4. Storage and Backup Systems: All data storage devices, including SANs (Storage Area Networks), NAS (Network-Attached Storage), and backup systems.

5. Access Controls and Policies: User access controls, policies, and procedures related to data center operations, including user authentication and authorization mechanisms.

6. Physical Security: The physical security measures in place at the data center, such as surveillance, access control, and environmental controls.

7. Data Protection and Privacy: How data is handled and protected within the data center, including encryption, data retention, and privacy policies.

Objective

The objective of the penetration testing initiative is to:

1. Identify Vulnerabilities: Conduct a comprehensive assessment to identify any vulnerabilities in the data center infrastructure, including network, systems, applications, storage, and physical security.

2. Assess Risk: Evaluate the potential impact and likelihood of exploitation of identified vulnerabilities to assess the overall risk to ABC Corporation's data center.

3. Propose Mitigation Strategies: Recommend actionable strategies to mitigate the identified vulnerabilities and enhance the data center's security posture.

4. Ensure Compliance: Verify that the data center infrastructure aligns with relevant industry standards and regulatory requirements related to data security and privacy.

5. Enhance Incident Response: Provide insights to improve ABC Corporation's incident response capabilities in the event of a security breach.

6. Strengthen Security Posture: Strengthen ABC Corporation's overall security posture by addressing weaknesses and reinforcing existing security measures.

By conducting this penetration testing initiative, ABC Corporation aims to ensure the robustness of its data center infrastructure and protect its data assets from potential threats and breaches.

About the tool and the application chosen

Tool: N MAP

Nmap (Network Mapper) is a powerful, open-source network scanning and security auditing tool that is widely used by network administrators, cybersecurity professionals, and IT experts. It helps discover hosts and services on a network, providing information about the network's structure, devices, and their potential vulnerabilities.

Host Discovery: Nmap can identify live hosts on a network, checking which ones are up and running.

Port Scanning: Nmap scans network ports (TCP/UDP) on a host to determine which ports are open and what services are running on them.

Service Version Detection: Nmap can determine the version of the services running on a host's open ports, which is useful for identifying outdated or potentially vulnerable services.

Operating System Detection: Nmap can detect the operating system (OS) running on a host by analyzing the characteristics of the network packets sent and received.

Scripting Engine (NSE): Nmap includes a scripting engine that allows users to write custom scripts for more complex scans and vulnerability assessments.

Vulnerability Scanning: By using NSE scripts, Nmap can identify common vulnerabilities in network services.

Flexible and Customizable: Nmap offers a wide range of options and configurations, allowing users to customize scans according to their needs. Output Formats: Nmap supports various output formats such as plain text, XML, and Grepable, making it easy to integrate with other tools and scripts.

Network Mapping and Visualization: Nmap can map out network topologies and visualize them in different formats, helping users understand the structure and interconnections in a network.

Stealth Scanning: Nmap offers different scanning techniques such as SYN scan, FIN scan, and others to perform scans stealthily and avoid detection.

Application Chosen: Pentesting on Datacenter

In the context of a penetration testing initiative at ABC Corporation, utilizing the Nmap tool can provide crucial insights into the security of the company's data center infrastructure. Nmap (Network Mapper) is a powerful open-source network scanning tool used to discover hosts and services on a computer network, which can play a significant role in identifying potential vulnerabilities in the data center's security posture.

1. Network Discovery: Nmap can help identify all active devices and hosts on the data center's network. This includes servers, routers, switches, and other network devices. This discovery phase is essential to understand the scope and architecture of the network.

2. Port Scanning: Nmap allows penetration testers to scan for open ports on the network's hosts. By identifying open ports, testers can determine which services and applications are running on each host, as these are potential entry points for attackers.

3. Service Enumeration: Nmap can go beyond just listing open ports; it can also identify the services running on those ports and the versions of the software being used. This information can reveal outdated or unpatched services that may be vulnerable to known exploits.

4. Vulnerability Assessment: Nmap can be integrated with scripts and other tools such as NSE (Nmap Scripting Engine) to automate the process of identifying vulnerabilities in the network. These scripts can be used to detect specific security issues such as insecure configurations, outdated software, and misconfigurations.

5. Reporting and Analysis: The data collected through Nmap scans can be analyzed to generate comprehensive reports on the security status of the data center's infrastructure. These reports can then guide decision-making for implementing mitigation strategies.

6. Ongoing Monitoring: After initial penetration testing, Nmap can be used for ongoing monitoring of the network to detect any new vulnerabilities or changes in the network's security posture.

In summary, Nmap plays a critical role in assessing and enhancing the security of ABC Corporation's data center infrastructure by providing a thorough analysis of the network's hosts, services, and potential vulnerabilities. This information is vital for developing effective mitigation strategies and ensuring the security of the data center.

ADVANTAGES:

Comprehensive Network Discovery: Nmap can identify all active hosts on a network, providing a complete overview of the network topology. This includes identifying servers, devices, and network components.

Port Scanning and Service Enumeration: Nmap can scan for open ports and identify the services running on those ports, along with their versions. This helps in pinpointing potential vulnerabilities due to outdated software or insecure services.

Flexible and Customizable: Nmap supports a variety of scanning techniques and options, such as TCP and UDP scans, SYN and ACK scans, and stealth scans. These options allow testers to customize their scans according to the specific needs of the penetration testing initiative.

Integration with Nmap Scripting Engine (NSE): Nmap's scripting engine allows for automation and customization of security checks. NSE scripts can detect specific vulnerabilities, security misconfigurations, and even perform advanced checks like brute-force attacks.

Cross-Platform Compatibility: Nmap is compatible with multiple operating systems, including Linux, Windows, and macOS, making it a versatile tool for use in different network environments.

Performance Optimization: Nmap offers various options for optimizing performance, such as parallel scanning and adjusting scan speeds. This is useful for efficiently scanning large and complex networks.

Free and Open-Source: As an open-source tool, Nmap is freely available to anyone. This makes it a cost-effective option for companies like ABC Corporation to leverage in their penetration testing initiatives.

Reporting and Data Export: Nmap can generate detailed reports of scan results, including exporting data in formats such as XML for further analysis. This data can be useful for documenting findings and guiding mitigation strategies.

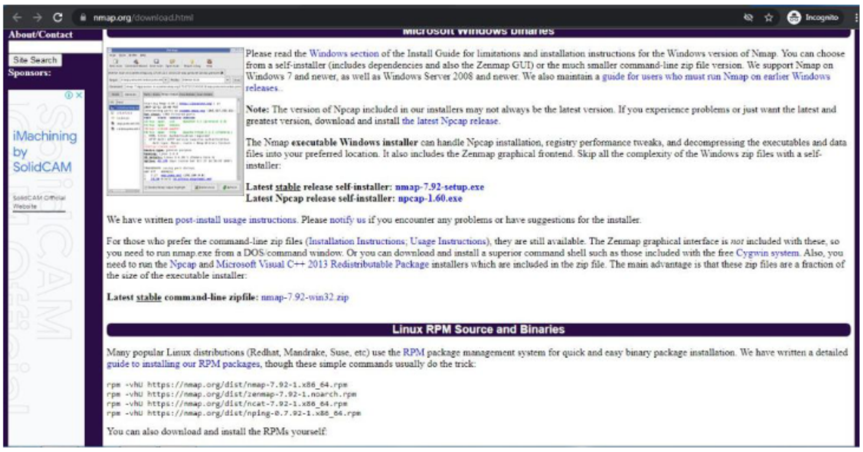
Security Awareness and Training: Using Nmap in penetration testing helps security teams stay up-to-date with the latest threats and vulnerabilities, fostering a culture of security awareness and continuous learning.

Tool installation procedure

Installing Nmap on Windows

Follow the below steps to install Nmap on Windows:

Step 1: Visit the official website using the URL https://nmap.org/download.html on any web browser the click on **nmap-7.92-setup.exe**. Downloading of this executable file will start soon. It is a 21.8 MB file so it will take some minutes.



Microsoft Windows Binaries

Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install the latest Npcap release.

The Nmap **executable Windows installer** can handle Npcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

Latest stable release self-installer: nmap-7.92-setup.exe
Latest Npcap release self-installer: npcap-1.60.exe

We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files (Installation Instructions; Usage Instructions), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install a superior command shell such as those included with the free Cygwin system. Also, you need to run the Npcap and Microsoft Visual C++ 2013 Redistributable Package installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

Latest stable command-line zipfile: nmap-7.92-win32.zip

Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the RPM package management system for quick and easy binary package installation. We have written a detailed guide to installing our RPM packages, though these simple commands usually do the trick:

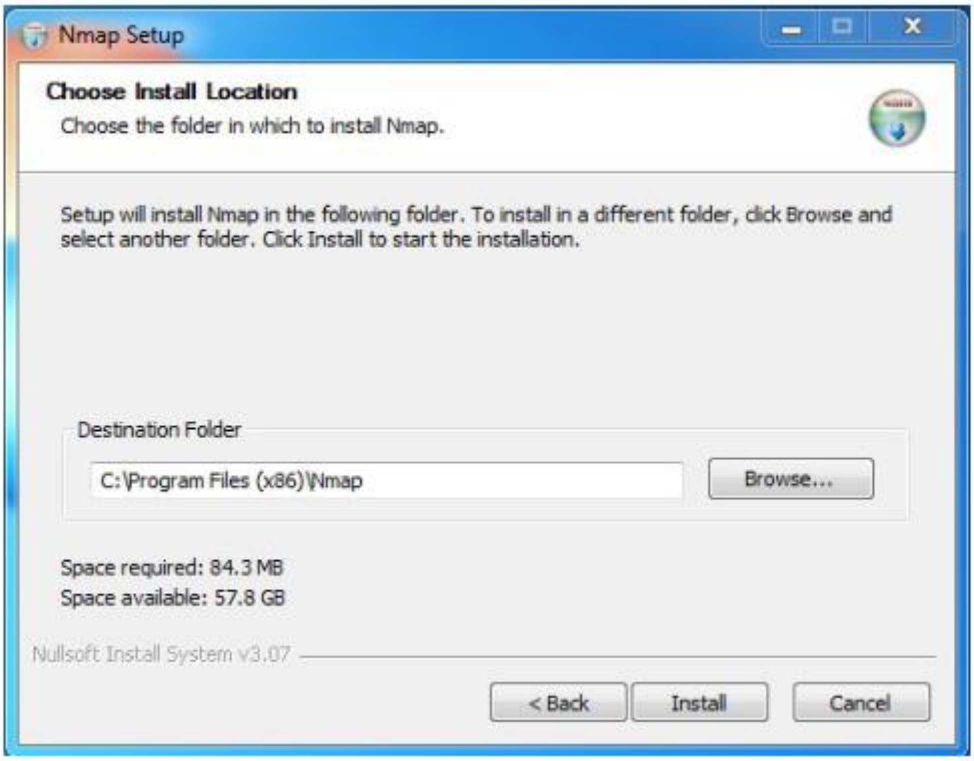
```
rpm -vhU https://nmap.org/dist/nmap-7.92-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.92-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.92-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.92-1.x86_64.rpm
```

You can also download and install the RPMs yourself:

Step 2: Now check for the executable file in downloads in your system and run it.

Step 3: It will prompt confirmation to make changes to your system. Click on **Yes**.

Step 4: The next screen will be of License Agreement, click on I Agree.
Step 5: Next screen is of choosing components, all components are already marked so don’t change anything just click on the Next button.
Step 6: In this step, we choose the installation location of Nmap. By default, it uses the C drive but you can change it into another drive that will have sufficient memory space for installation. It requires 84.3 MB of memory space.



Nmap Setup

Choose Install Location

Choose the folder in which to install Nmap.

Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files (x86)\Nmap

Space required: 84.3 MB

Space available: 57.8 GB

Nullsoft Install System v3.07

Step 7: After this installation process it will take a few minutes to complete the installation.

Step 8: Npcap installation will also occur with it, the screen of License Agreement will appear, click on I Agree.

Step 9: Next screen is of installation options don't change anything and click on the Install button.

Step 10: After this installation process it will take a few minutes to complete the installation.

Step 11: After completion of installation click on the Next button.

Step 12: Click on the Finish button to finish the installation of Npcap.

Step 13: After completion of the installation of Nmap click on Next button.

Step 14: Screen for creating shortcut will appear, click on Next button.

Step 15: Click on the Finish button to finish the installation of Nmap.

Step 16: Nmap is successfully installed on the system and an icon is created on the desktop.

Step 17: Run the software and see the interface.

Steps of ethical hacking that you have done on your application using the chosen tool

N MAP on Datacenter on an application:

1. Reconnaissance:

- Gather information about the application to understand its architecture, technology stack, and potential vulnerabilities.

2. Enumeration:

- Exploiting the identified open ports, hackers use tools like N-MAP or Nessus or OpenVAS to conduct service enumeration and detect potential vulnerabilities.
- They identify outdated software versions, misconfigurations, and weak security controls that could be exploited.

3. Exploitation:

- Leveraging the information obtained from reconnaissance and enumeration phases, hackers exploit known vulnerabilities in ABC Corporation's network infrastructure and applications.
- Hackers craft convincing phishing emails targeting ABC Corporation's employees, enticing them to click on malicious links or download attachments.

4. Post-Exploitation:

- Once initial access is gained, hackers escalate their privileges within the network by exploiting misconfigurations or vulnerabilities in operating systems and applications.

- They exploit weaknesses in access control mechanisms or insecure default configurations to gain administrative privileges.

5. Data-Exfilteration:

- Having established a significant presence within the network, hackers identify and exfiltrate sensitive data, including customer records, financial information, and proprietary software.
- They use tools like Cobalt Strike or Mimikatz to harvest credentials, escalate privileges, and exfiltrate data stealthily.

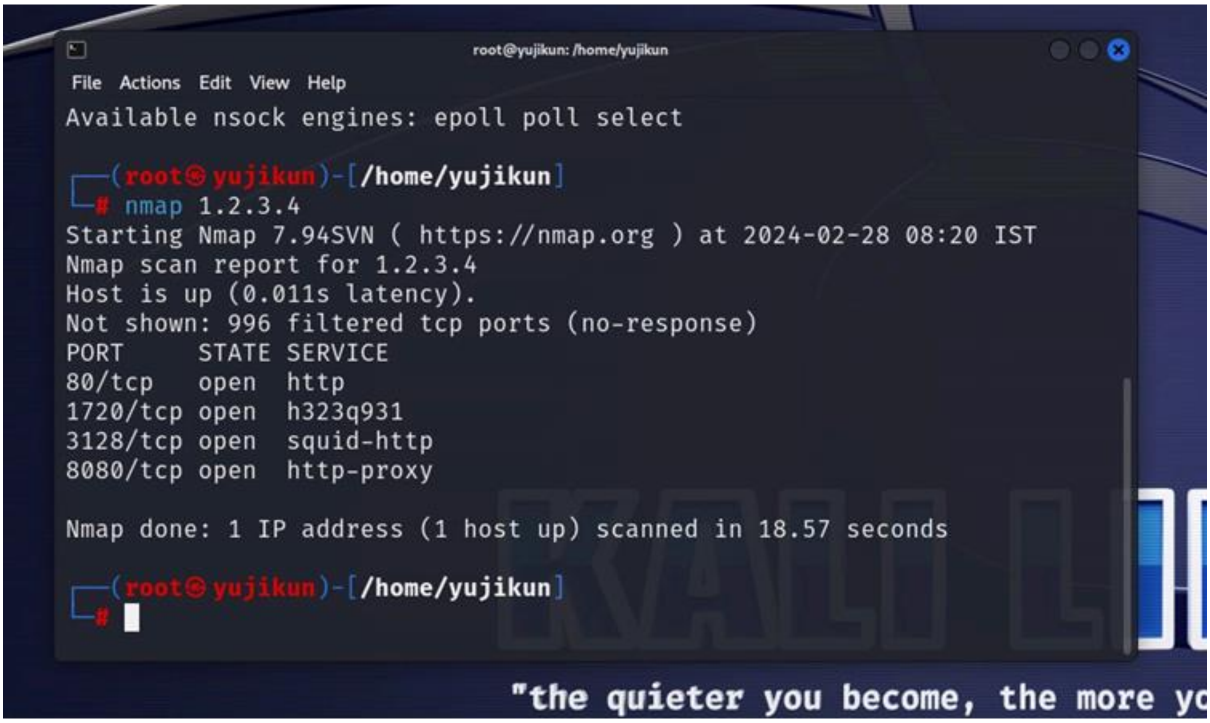
6. Mitigation Measures:

- Implement robust network segmentation to limit lateral movement.
- Regularly update and patch all software and systems to address known vulnerabilities.
- Enforce strong password policies and multi-factor authentication to prevent unauthorized access.

By implementing these mitigation measures, ABC Corporation can significantly reduce the risk of a successful penetration attack and safeguard its data center infrastructure from potential threats

Screenshots of the implementation

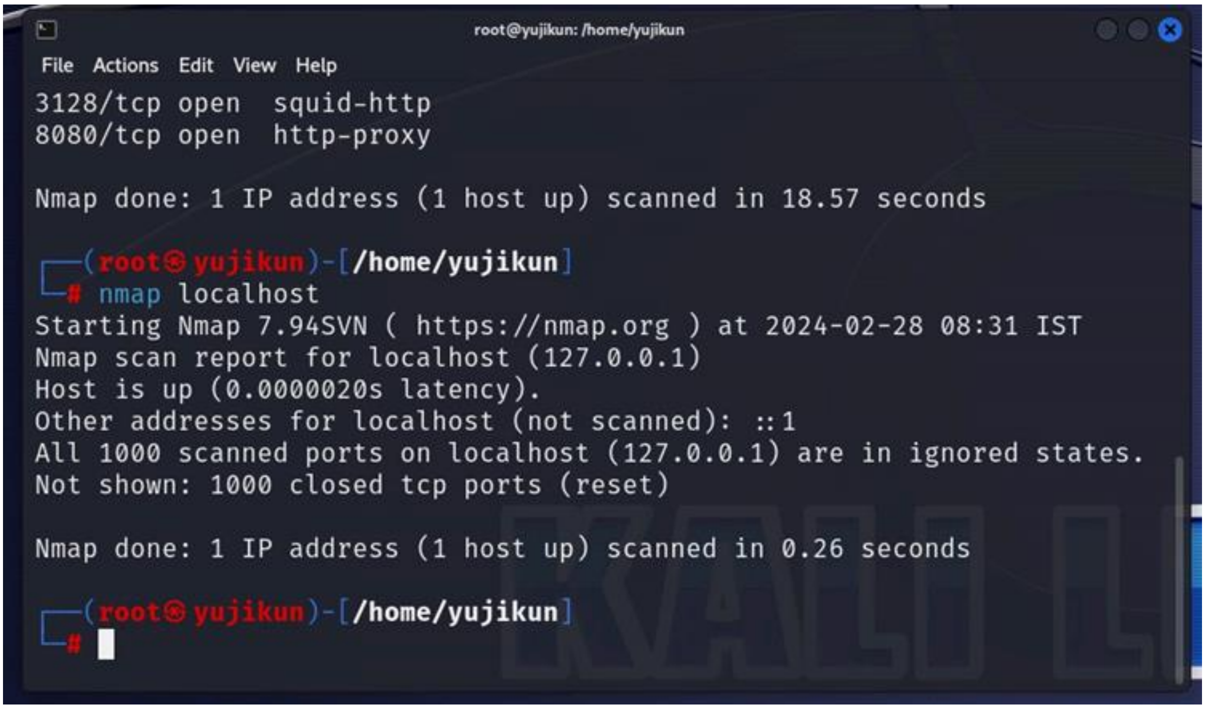
1)to scan a target using nmap :



root@yujikun: /home/yujikun
File Actions Edit View Help
"the quieter you become, the more yo

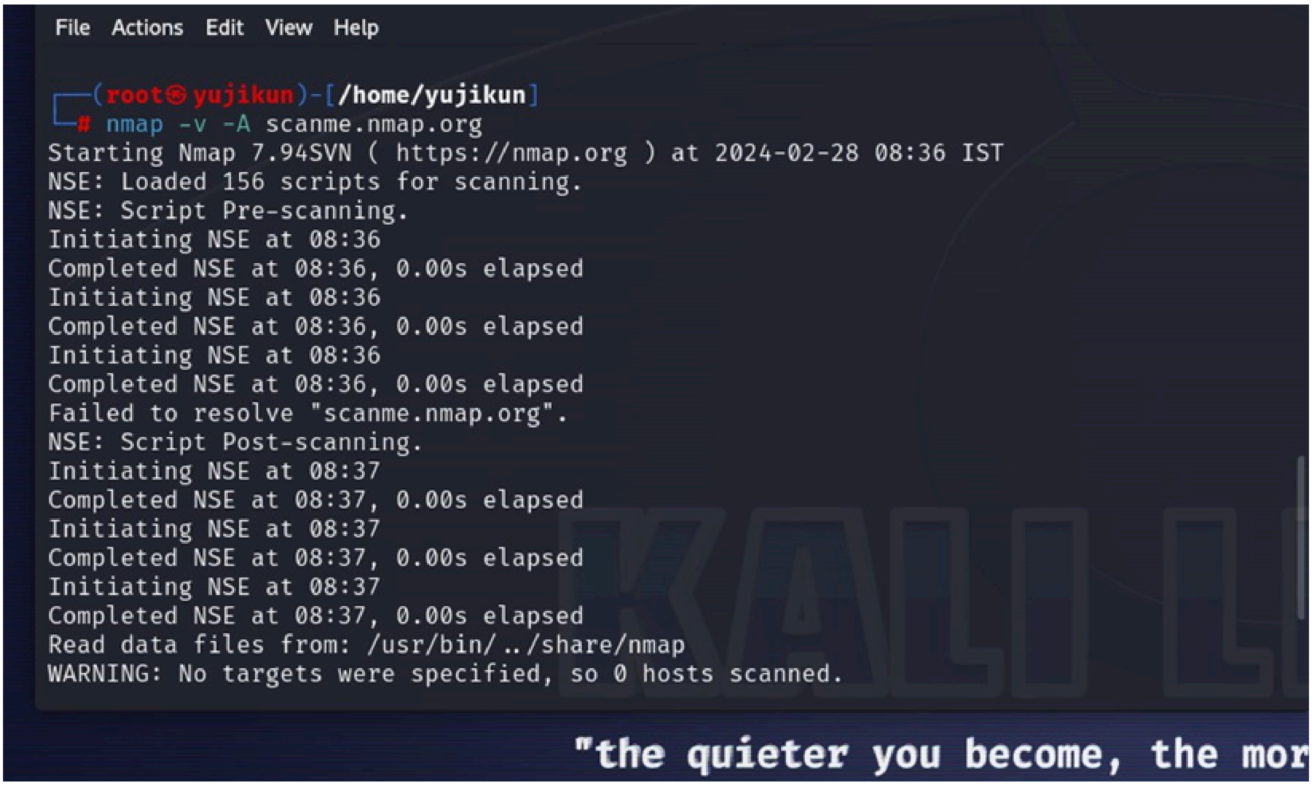
```
Available nsock engines: epoll poll select

┌──(root㉿yujikun)-[/home/yujikun]
└─# nmap 1.2.3.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 08:20 IST
Nmap scan report for 1.2.3.4
Host is up (0.011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
1720/tcp open  h323q931
3128/tcp open  squid-http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 18.57 seconds

┌──(root㉿yujikun)-[/home/yujikun]
└─# 
```

2)nmap scan on a local host

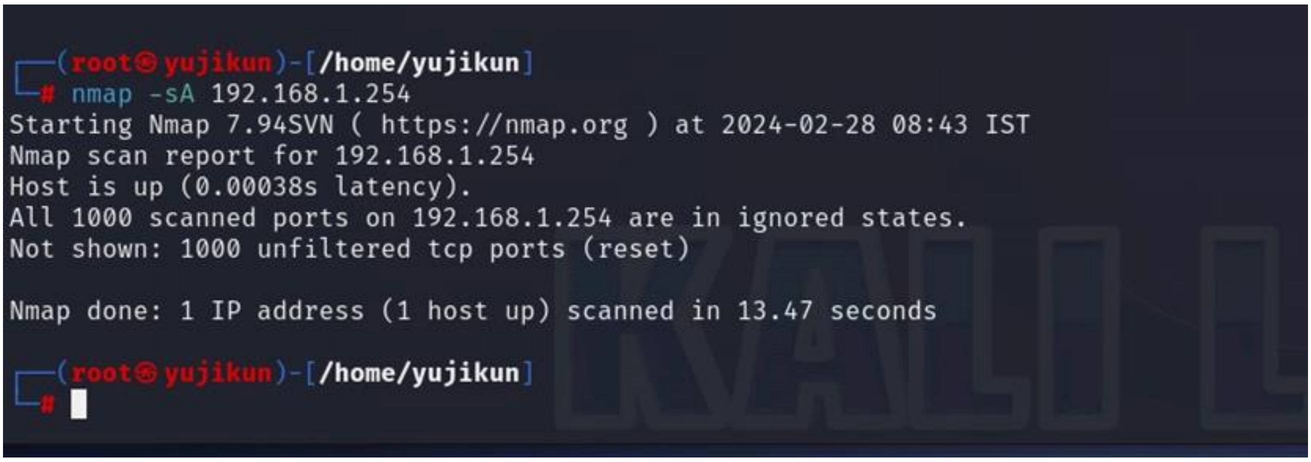


```
3128/tcp open  squid-http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 18.57 seconds

┌──(root㉿yujikun)-[/home/yujikun]
└─# nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 08:31 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(root㉿yujikun)-[/home/yujikun]
└─# 
```

3)when protected by firewall , nmap to scan the protected target

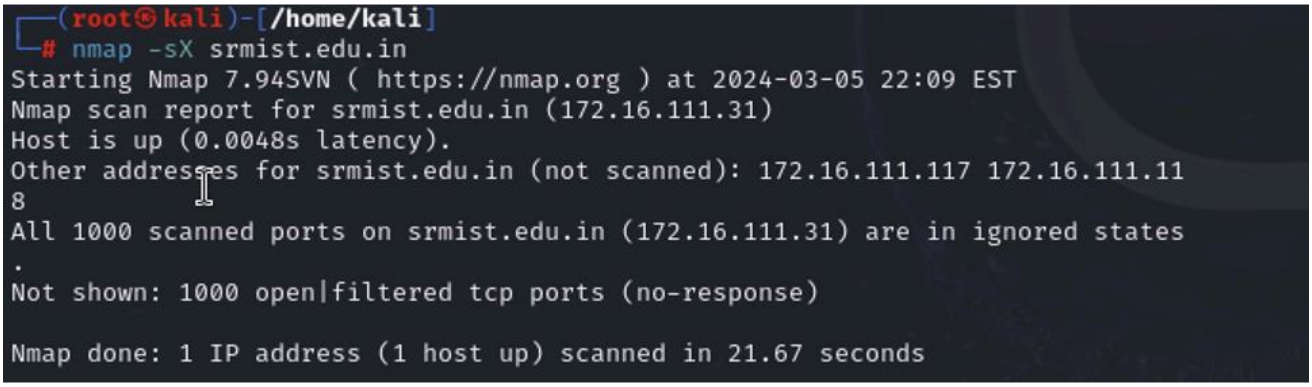


```
┌──(root㉿yujikun)-[/home/yujikun]
└─# nmap -v -A scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 08:36 IST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:36
Completed NSE at 08:36, 0.00s elapsed
Initiating NSE at 08:36
Completed NSE at 08:36, 0.00s elapsed
Initiating NSE at 08:36
Completed NSE at 08:36, 0.00s elapsed
Failed to resolve "scanme.nmap.org".
NSE: Script Post-scanning.
Initiating NSE at 08:37
Completed NSE at 08:37, 0.00s elapsed
Initiating NSE at 08:37
Completed NSE at 08:37, 0.00s elapsed
Initiating NSE at 08:37
Completed NSE at 08:37, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
```



```
┌──(root㉿yujikun)-[/home/yujikun]
└─# nmap -sA 192.168.1.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 08:43 IST
Nmap scan report for 192.168.1.254
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.1.254 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds

┌──(root㉿yujikun)-[/home/yujikun]
└─#
```

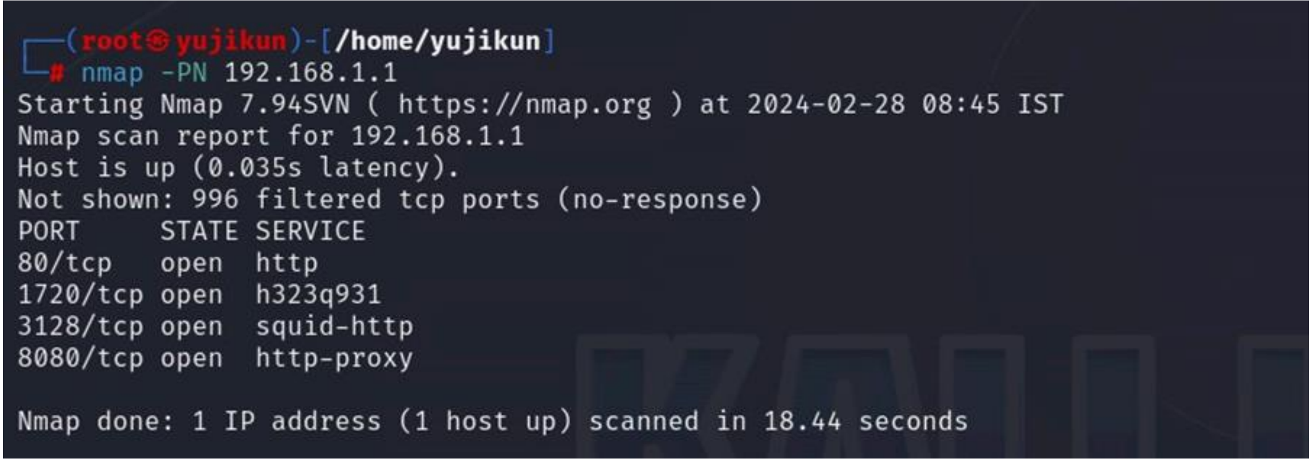
4)N MAP -SX



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sX srmist.edu.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 22:09 EST
Nmap scan report for srmist.edu.in (172.16.111.31)
Host is up (0.0048s latency).
Other addresses for srmist.edu.in (not scanned): 172.16.111.117 172.16.111.11
8
All 1000 scanned ports on srmist.edu.in (172.16.111.31) are in ignored states
.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.67 seconds
```

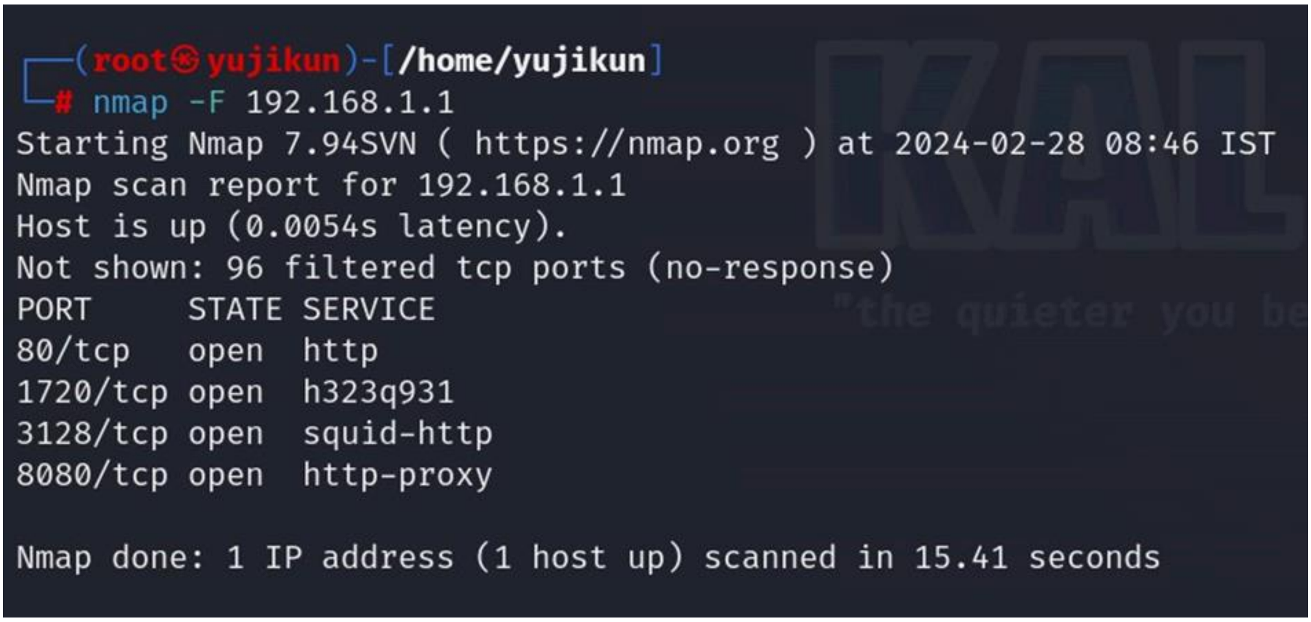
The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

5) host protected by firewall, nmap command to scan the host



```
┌──(root㉿yujikun)-[/home/yujikun]
└─# nmap -PN 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 08:45 IST
Nmap scan report for 192.168.1.1
Host is up (0.035s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
1720/tcp open  h323q931
3128/tcp open  squid-http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 18.44 seconds
```

6)for fast Scan



```
┌──(root㉿yujikun)-[/home/yujikun]
└─# nmap -F 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 08:46 IST
Nmap scan report for 192.168.1.1
Host is up (0.0054s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
1720/tcp open  h323q931
3128/tcp open  squid-http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
```

Conclusion

TIn summary, ABC Corporation's decision to undertake a penetration testing initiative is a proactive and strategic move to ensure the security of its data center infrastructure. By simulating potential cyber threats and attacks, the corporation aims to identify and assess vulnerabilities within its data center environment. The primary goal of this initiative is to uncover weak points in the security architecture that could be exploited by malicious actors, thereby allowing the company to address these issues before they result in data breaches or other security incidents.

The penetration testing process will provide ABC Corporation with a comprehensive analysis of its current security posture, highlighting areas where security controls and defenses can be enhanced. This may include vulnerabilities in network configurations, server setups, application security, data storage, and access controls. Additionally, the testing may reveal potential gaps in the organization's incident response and recovery capabilities.

Once vulnerabilities are identified, ABC Corporation can leverage the findings to develop and implement targeted mitigation strategies. This could involve updating software and hardware, patching vulnerabilities, reconfiguring network and security settings, and enhancing security policies and procedures. By taking these steps, the company can significantly reduce its risk exposure and better

In conclusion, this penetration testing initiative is a vital and beneficial endeavor for ABC Corporation. It empowers the organization to proactively strengthen its security measures and ensure the ongoing safety and integrity of its data center infrastructure.

References

https://www.geeksforgeeks.org/how-to-install-nmap-on-windows/

https://nmap.org/book/inst-windows.html

https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/