

NPT (Network Penetration Testing)

A Project Report for Industrial Internship
In the partial fulfillment for the award of the degree of

RACHITA CHAKRABORTY.

B.Tech

In the

Department OF **COMPUTER SCIENCE & BUSINESS SYSTEMS**

NARULA INSTITUTE OF TECHNOLOGY



At

Ardent Computech Pvt. Ltd.



CERTIFICATE FROM SUPERVISOR

This is to certify that the student “Rachita Chakraborty” have successfully completed the project titled "**NPT(Network Penetration Testing)**" under my supervision during the period from “**5th July 2024**” to “**2nd August 2024**” which is in partial fulfillment of requirements for the award of the **B.Tech** degree and submitted to the Department of COMPUTER SCIENCE AND BUSINESS SYSTEMS in Narula Institute of Technology .

Signature of the Supervisor

Date: 05/07/2024

Name of the Project Supervisor: **Dipon Mondal**

ACKNOWLEDGEMENT

The achievement that is associated with the successful completion of any task would be incomplete without mentioning the names of those people whose endless cooperation made it possible. Their constant guidance and encouragement made all our efforts successful.

We take this opportunity to express our deep gratitude towards our project mentor, **Dipon Mondal** for giving such valuable suggestions, guidance and encouragement during the development of this project work.

Last but not the least we are grateful to all the faculty members of Ardent Computech Pvt. Ltd. for their support.

Content Table

S.L. no.	PARTICULARS	PAGE NO.
1.	What is Cyber Security?	05
2.	Why Cyber Security?	06
3.	What is Ethical Hacking?	07
4.	What is NPT in Cyber Security?	08
5.	Why is NPT crucial in Cyber Security?	09
6.	Careers in Cyber Security.	10
7.	Pros & Cons of NPT.	11
8.	Task	12 - 19
9.	Conclusion	20
10.	References	21

1. What is Cyber Security?

Cyber Security refers to the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Key Components of Cyber Security

1. **Network Security:** Protecting the integrity, confidentiality, and availability of data as it is transmitted across or accessed through network systems.
2. **Application Security:** Keeping software and devices free of threats. A compromised application could provide access to the data it is designed to protect. Security begins at the design stage, well before a program or device is deployed.
3. **Information Security:** Protecting the privacy and integrity of data, both in storage and in transit.
4. **Operational Security:** Includes the processes and decisions for handling and protecting data assets. This encompasses the permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared.
5. **Disaster Recovery and Business Continuity:** Defining how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
6. **End-User Education:** Addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, avoid plugging in unidentified USB drives, and various other important lessons is vital for the security of any organization.

2. Why Cyber Security?

- **Protecting Sensitive Data:** Cyber security is crucial for protecting sensitive data, including personal information, financial records, intellectual property, and confidential business information. Unauthorized access to this data can lead to identity theft, financial loss, and damage to reputation.
- **Preventing Cyber Attacks:** The rise of sophisticated cyber attacks, such as phishing, ransomware, and malware, highlights the need for robust cyber security measures. These attacks can disrupt operations, steal data, and cause significant financial and reputational damage.
- **Safeguarding Financial Assets:** Cyber attacks can have a direct financial impact on organizations, leading to theft of funds, financial fraud, and costly recovery efforts. Implementing strong cyber security measures helps safeguard financial assets and reduces the risk of financial loss.
- **Defending Against Emerging Threats:** The cyber threat landscape is constantly evolving, with new and more sophisticated threats emerging regularly. Staying ahead of these threats requires continuous improvement of cyber security measures, including regular updates, patch management, and employee training.
- **Protecting National Security:** Cyber security is also critical at a national level. Protecting critical infrastructure, such as power grids, communication networks, and financial systems, from cyber attacks is essential for national security and public safety.
- **Reducing Risk and Liability:** Implementing strong cyber security measures reduces the risk of data breaches and cyber incidents, thereby minimizing potential legal and financial liabilities. It also helps protect against the costs associated with incident response, legal fees, and regulatory fines.

By understanding and implementing effective cyber security practices, organizations can protect their data, maintain customer trust, comply with regulations, and ensure long-term business success in an increasingly digital world.

3. What is Ethical Hacking?

Ethical hacking, also known as penetration testing or white-hat hacking, is the practice of intentionally probing systems, networks, and applications to identify and fix security vulnerabilities. Unlike malicious hackers (black-hat hackers), ethical hackers are authorized and legal, working with the permission of the system owner.

Types of Hackers –

- White Hat Hacker
- Black Hat Hacker
- Grey Hat Hacker

Importance of Ethical Hacking

- **Identifying Vulnerabilities:** Ethical hacking helps organizations discover security weaknesses before malicious hackers can exploit them.
- **Improving Security Posture:** Provides actionable insights and recommendations to enhance overall security measures.
- **Compliance and Regulation:** Assists organizations in meeting regulatory requirements and industry standards for data protection.
- **Building Trust:** Demonstrates a commitment to security, which builds trust with customers and stakeholders.

Five phase of Ethical Hacking –

4. The Reconnaissance Phase.
5. The Scanning Phase.
6. The Gaining Access Phase.
7. The Maintaining Access Phase.
8. The Covering of Tracks Phase.

4. What is NPT?

Network Penetration Testing (NPT) is a systematic process used to evaluate the security of a computer network by simulating an attack from malicious outsiders (e.g., hackers) and insiders (e.g., employees). The goal is to identify vulnerabilities that could be exploited to gain unauthorized access to network resources.

How Network Penetration Testing Works

Network Penetration Testing involves simulating attacks on a network to identify vulnerabilities. Ethical hackers, also known as penetration testers, use a variety of tools and techniques to probe the network for weaknesses. They attempt to exploit these vulnerabilities to gain unauthorized access, test the effectiveness of security measures, and evaluate the potential impact of a breach.

Penetration testers follow a methodical approach, which typically includes planning, reconnaissance, scanning, exploitation, and reporting. They gather information about the network, identify potential entry points, attempt to exploit vulnerabilities, and document their findings. The results are then used to recommend improvements and strengthen the network's security posture.

Network Penetration Testing is a critical practice for maintaining robust network security. By simulating real-world attacks, it helps organizations identify and address vulnerabilities, ensuring that their networks are well-protected against potential threats. Regular penetration testing is essential for staying ahead of evolving cyber threats and maintaining a strong security posture.

5. Why is NPT crucial in Cyber Security?

Network Penetration Testing (NPT) involves simulating attacks on a network to discover vulnerabilities before malicious hackers can exploit them. By evaluating the security of a network through ethical hacking techniques, NPT helps organizations identify and address weaknesses in their defenses.

1. **Identifies Vulnerabilities:** NPT helps uncover hidden vulnerabilities in network infrastructure, such as unpatched systems or misconfigured settings, before they can be exploited by cybercriminals. By finding and addressing these vulnerabilities early, organizations can prevent potential breaches and minimize the risk of data loss or system compromise.
2. **Enhances Security Posture:** The insights gained from NPT provide actionable recommendations to bolster network security. This includes improving firewall configurations, updating security policies, and enhancing monitoring systems.
3. **Ensures Compliance:** Many industries are subject to strict regulations regarding data protection and network security. NPT helps organizations meet these compliance requirements by demonstrating due diligence in identifying and addressing potential security risks.
4. **Protects Sensitive Information:** As cyber attacks increasingly target sensitive data, including personal, financial, and proprietary information, NPT is essential for protecting this valuable information from unauthorized access or theft.
5. **Improves Incident Response:** NPT helps organizations develop and refine their incident response plans by identifying potential attack vectors and understanding how to respond effectively to different types of threats.
6. **Facilitates Continuous Improvement:** Cyber threats are constantly evolving, and NPT provides a mechanism for ongoing assessment of network security. Regular testing ensures that security measures remain effective against new and emerging threats.

Network Penetration Testing is a vital component of a comprehensive cyber security strategy. By proactively identifying and addressing vulnerabilities, enhancing security measures, ensuring regulatory compliance, and protecting sensitive data, NPT plays a crucial role in safeguarding networks against cyber threats. Regular NPT is essential for maintaining a strong security posture and staying ahead of evolving cyber threats.

6. Careers in Cyber Security

As the need arises for secure and reliable computer infrastructure, software and networks, so does the demand for professionals to fill cybersecurity positions. Cybersecurity professionals play an integral role in protecting the privacy and confidentiality of sensitive data and personal information from cyberattacks and other prominent threats.

Cybersecurity Engineer: *Average Annual Salary:* About \$102,000

Career Overview: Cyber Security Engineers assess an organization's security needs, assisting with establishing standards and best practices. These professionals design, implement and maintain secure solutions to protect an organization's data, networks and systems against cyberattacks, hackers and other threats. They conduct tests to identify vulnerabilities in networks and systems, respond to security breaches and ensure all defences are up to date.

Information Security Analyst: *Average Annual Salary:* About \$78,000

Career Overview: Information Security Analysis protect an organization's computer networks, systems and databases from cyberattacks, data breaches and other threats. These professionals monitor information networks and computer infrastructure to identify vulnerabilities in digital security systems and secure sensitive information and data.

Information Security Manager: *Average Annual Salary:* Around \$126,000

Career Overview: Cybersecurity managers are responsible for securing an organization's computer networks and systems and protecting organizations from cyberattacks, hackers, viruses, malware and other threats. These professionals carry out security measures, update current security systems and conduct regular audits to ensure compliance with relevant regulations.

Information Technology Support Technician: *Average Annual Salary:* Around \$51,000

Career Overview: Information technology support technicians provide in-person and remote technical support to clients who need help setting up, maintaining and troubleshooting computer software and hardware problems. These professionals serve as the primary point of contact when a problem arises.

Network Engineer: *Average Annual Salary:* Around \$81,000

Career Overview: A network engineer sets up and maintains networks within an organization or between organizations. These professionals maintain and improve the efficiency of current computer networks, which typically include wide area networks, local area networks, intranet and extranet. They may also design and implement new network solutions.

Systems Administrator: *Average Annual Salary:* Around \$68,000

Career Overview: System administrators offer technical support services focused on servers and computer systems. These professionals are often the first point of contact within IT departments when technical issues arise. They ensure an organization's computer systems are functioning smoothly.

7. Pros & Cons of NPT

Advantages of Penetration Testing

1. **Early Detection of Vulnerabilities:** Penetration testing allows for the detection and correction of vulnerabilities before they are exploited by cybercriminals. This helps strengthen security by addressing potential weaknesses before they become a major problem.
2. **Improved Response to Attacks:** By identifying weaknesses, penetration testing helps organizations develop response plans for potential attacks. This enables quick and coordinated action in the event of a security breach.
3. **Strengthening Security Mechanisms:** Penetration testing highlights gaps in security mechanisms, prompting organizations to enhance their defences and adopt better security practices.
4. **Validation of Fixes:** After addressing vulnerabilities, penetration testing helps validate the effectiveness of the implemented patches, ensuring that security measures are adequate.

Limitations of Penetration Testing


1. **No Guarantee of Comprehensive Coverage:** Penetration testing does not guarantee the discovery of all vulnerabilities. Testers may miss some issues, meaning an application may appear secure but still have undetected vulnerabilities.
2. **Costs and Resources:** Penetration testing can be costly and time-consuming, requiring resources to be reasonably applied. Organizations must balance the benefits of increased security with the associated costs.
3. **Interpretation of Results:** The penetration testing results can be complex and require expertise to interpret correctly. Organizations must have qualified professionals to analyse the results and take appropriate actions.
4. **Timing of Discovery:** Penetration testing does not guarantee that discovered vulnerabilities will be patched promptly. Some organizations may delay applying patches, leaving an opportunity for attackers.

In summary, while penetration testing is a crucial component of a comprehensive cybersecurity strategy, it is not without its challenges. Organizations should carefully weigh the advantages and disadvantages and use penetration testing in conjunction with other security measures to create a layered defense against cyber threats.

8.Task – 1

Using nmap: Nmap (Network Mapper) is a powerful and versatile open-source tool used for network discovery and security auditing. Developed by Gordon Lyon (also known by his pseudonym Fyodor), Nmap is widely used by network administrators, security professionals, and even hackers to assess network security and map network topology.

First, I opened Kali Linux root terminal with the password.



```

root@kali: /home/kali
File Actions Edit View Help
Currently scanning: 192.168.3.0/16 | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

IP          At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.0.1  a4:2a:95:26:11:c4   1      60  D-Link International
192.168.0.115 08:00:27:76:ee:16   1      60  PCS Systemtechnik GmbH
192.168.0.169 84:7b:57:bd:62:0e   1      60  Intel Corporate

(root@kali)~/home/kali
# nmap -O 192.168.0.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 10:34 EDT
Nmap scan report for dlinkrouter.local (192.168.0.1)
Host is up (0.0052s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https
1900/tcp  open  upnp
4443/tcp  open  pharos
4445/tcp  open  upnotifyp
MAC Address: A4:2A:95:26:11:C4 (D-Link International)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V7.94SVNWE=4XD-B/4XOT=53KCT=1XCU=39892XPV=YKDS=1KDC=DRG=YYM=A42A95
OS:XTM=66AF9179KP=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1KISR=101NTI=ZKCI=IKII
OS=IKTS=7)SEQ(SP=104%GCD=1KISR=102NTI=ZKCI=IKII=IKTS=7)SEQ(SP=104%GCD=1KIS
OS=R=103NTI=ZKCI=IKII=IKTS=7)SEQ(SP=106%GCD=1KISR=103NTI=ZKCI=IKII=IKTS=7)J0
OS:PS(O1=M5B4S111N4XQ2=M5B4S111N4XQ3=M5B4S111N4XQ4=M5B4S111N4XQ5=M5B4S
OS:T11N4XQ6=M5B4S111)WIN(W1=3890XW2=3890XW3=3890XW4=3890XW5=3890XW6=3890)E
OS:CN(R=YKDF=YKT=40XW=3908XO=M5B4NNSNW4KCC=YXQ=)T1(R=YKDF=YKT=40XW=0XA=5%F
OS=ASURD=0XQ=)T2(R=N)T3(R=N)T4(R=YKDF=YKT=40XW=0XS=AXA=ZNF=R2Q=MRD=0XQ=)T5
OS:(R=YKDF=YKT=40XW=0XS=ZKA=5%F=ARXQ=3RD=0XQ=)T6(R=YKDF=YKT=40XW=0XS=AXA=Z
OS:XF=R2Q=MRD=0XQ=)T7(R=N)U1(R=YKDF=NKT=40XPL=164XUN=0XRIPL=GXRID=GXRIPLCK=
OS:GXRUCK=GXRU=GX)IE(R=YKDF=NKT=40XCD=5)

Network Distance: 1 hop

Nmap scan report for 192.168.0.115
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
  
```

Then I used to command 'netdiscover' to fetch the information about all the active hosts under a network,

And used 'nmap -O 192.168.0.*' to detect all the operating systems active under the network 192.168.0.

```
File Actions Edit View Help
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8000/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:76:EE:16 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for Rachita (192.168.0.169)
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdaapi
MAC Address: 84:7B:57:0D:62:0E (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 11110|2022|Phone|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (97%), Microsoft Windows 10 (92%), Microsoft Windows Server 2022 (91%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows Server 2008 SP1 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for kali (192.168.0.174)
Host is up (0.000068s latency).
All 1000 scanned ports on kali (192.168.0.174) are in ignored states.
```

Here, we got our target OS which is running on Linux 2.6.X with the allotted IP 192.168.0.115

```
File Actions Edit View Help
Nmap done: 256 IP addresses (4 hosts up) scanned in 23.56 seconds

root@kali:~/kali
root@kali:~/kali# nmap -A 192.168.0.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 18:45 EDT
Nmap scan report for 192.168.0.115
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.0.174
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outs
ide US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2024-08-04T14:46:24+00:00; 0s from scanner time.
sslv2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain      ISC BIND 9.4.2
|_dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
```

I searched ‘nmap -A 192.168.0.115’ to fetch all the information about the target system to know all possible vulnerabilities.


```
File Actions Edit View Help
root@kali: /home/kali

|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|11/tcp open  rpcbind 2 (RPC #10000)
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 43484/udp mountd
|_100005 1,2,3 55755/tcp mountd
|_100021 1,3,4 33392/tcp nlockmgr
|_100021 1,3,4 52380/udp nlockmgr
|_100024 1 39963/tcp status
|_100024 1 43602/udp status
|139/tcp open  netbios-ssn Samba smbD 3.X - 4.X (workgroup: WORKGROUP)
|445/tcp open  netbios-ssn Samba smbD 3.0.20-Debian (workgroup: WORKGROUP)
|512/tcp open  exec?
|513/tcp open  login OpenBSD or Solaris rlogind
|514/tcp open  shell?
|_fingerprint-strings:
|_NULL:
|_ Couldn't get address for your host (kali)
|1099/tcp open  java-rmi GNU classpath gwiregistry
|1524/tcp open  bindshell Metasploitable root shell
|2049/tcp open  nfs 2-4 (RPC #100003)
|2121/tcp open  ftp ProFTPD 1.3.1
|3306/tcp open  mysql MySQL 5.0.51a-3ubuntu5
|_mysql-info:
|_Protocol: 10
|_Version: 5.0.51a-3ubuntu5
|_Thread ID: 8
|_Capabilities flags: 43566
|_Some Capabilities: SupportsCompression, Support41Auth, ConnectWithDatabase, SupportsTransactions, SwitchToSSLAfterHandshake,
|_Speaks41ProtocolNew, LongColumnFlag
|_Status: Autocommit
|_Ssl: (g06_j5-Xlv-x7TgRPC;
|5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-08-04T14:46:24+00:00; 0s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outs
|_de US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|5900/tcp open  vnc VNC (protocol 3.3)
|_vnc-info:
|_Protocol version: 3.3
|_Security types:
|_VNC Authentication (2)
|6000/tcp open  X11 (access denied)
```

```
File Actions Edit View Help
root@kali: /home/kali

|_users: 1
|_lservers: 0
|_server: irc.Metasploitable.LAN
|_version: Unreal3.2.8.1. irc.Metasploitable.LAN
|_uptime: 0 days, 0:23:05
|_source ident: nmap
|_source host: Test-8025C80A
|_error: Closing link: xosqmskur[kali] (Quit: xosqmskur)
|8009/tcp open  ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
|8100/tcp open  http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
|_SF-Port514-TCP:V=7.945VNMI=7KD=8/4&Time=66AF93F6&P=x86_64-pc-linux-gnu&R(N
|_SF:ULL,28,"x01Couldn'tx20getx20addressx20forx20yourx20hostx20(kali
|_SF:)\n");
|_MAC Address: 08:00:27:76:EE:16 (Oracle VirtualBox virtual NIC)
|_Device type: general purpose
|_Running: Linux 2.6.X
|_OS CPE: cpe:/o:linux:linux_kernel:2.6
|_OS details: Linux 2.6.9 - 2.6.33
|_Network Distance: 1 hop
|_Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-os-discovery:
|_OS: Unix (Samba 3.0.20-Debian)
|_Computer name: metasploitable
|_NetBIOS computer name:
|_Domain name: localdomain
|_FQDN: metasploitable.localdomain
|_System time: 2024-08-04T10:46:17-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-security-mode:
|_account_used: guest
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s

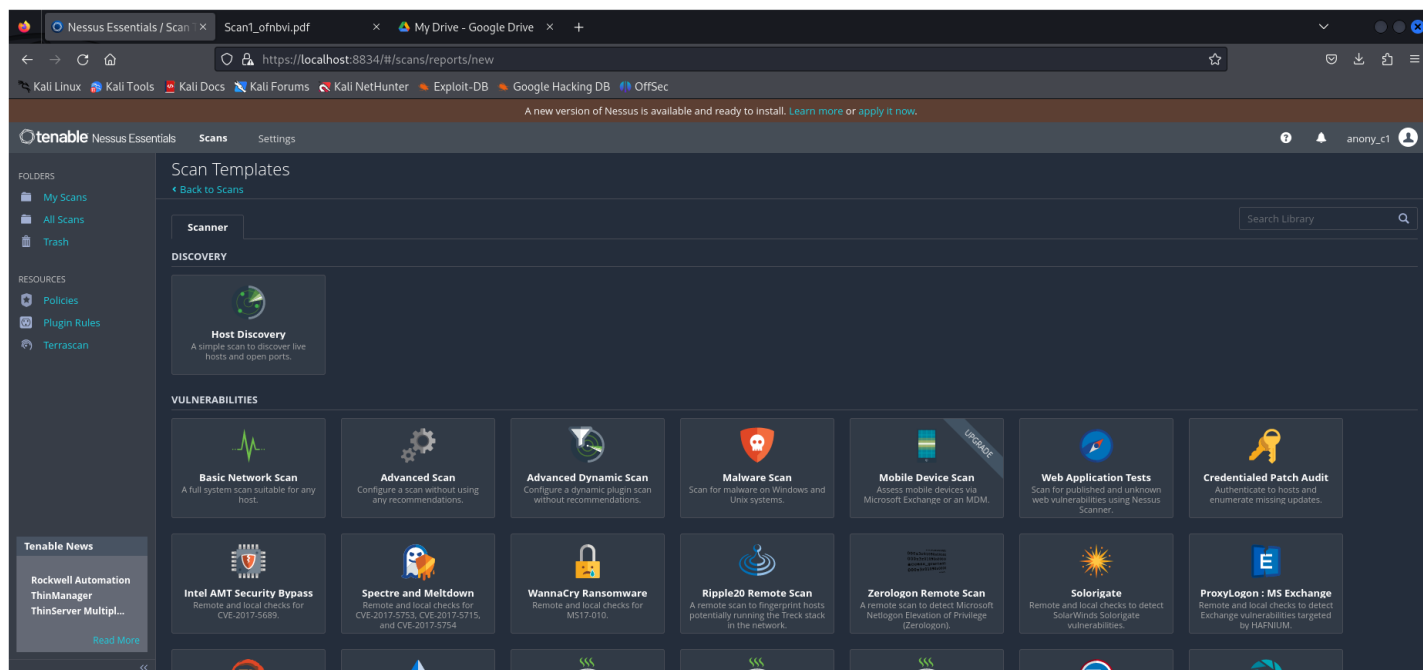
TRACEROUTE
HOP RTT ADDRESS
1 3.34 ms 192.168.0.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

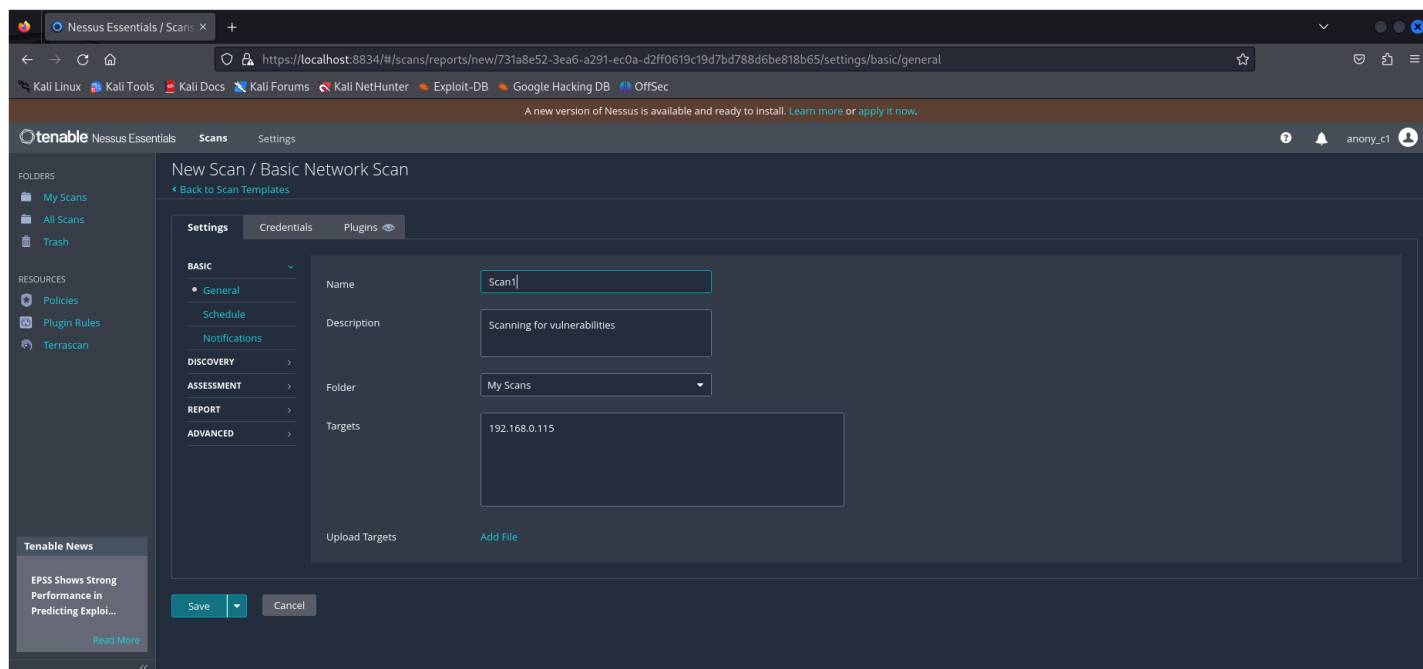
Here, so many critical open ports (port number 21-ftp, 22-ssh, 23-telnet, 25-fmtip etc.) were detected by nmap which can possibly be attacked by other systems.

Using Nessus: Nessus, developed by Tenable, Inc., is a popular vulnerability scanner used to detect security weaknesses, & compliance issues in systems and networks. It provides comprehensive assessments & detailed reports to help prioritize and address critical vulnerabilities.

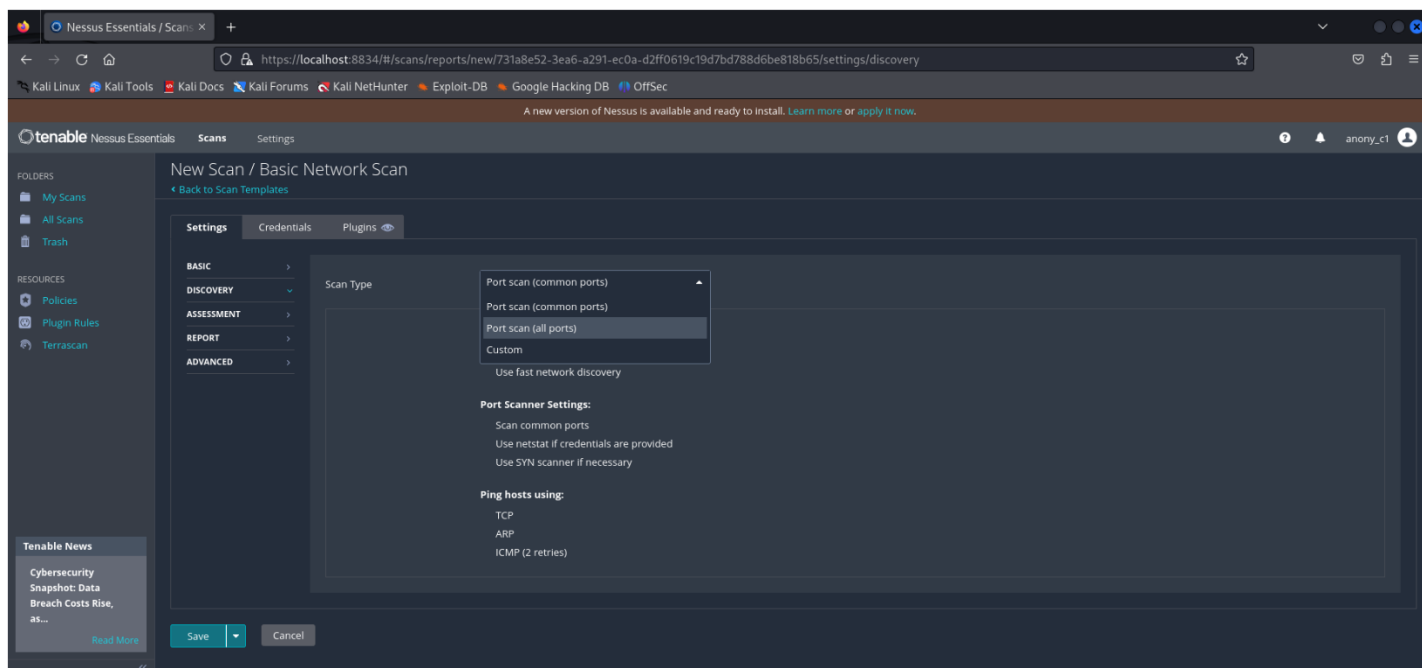
First, I launched Nessus clicked on 'New Scan' and opened 'Basic Network Scan'.



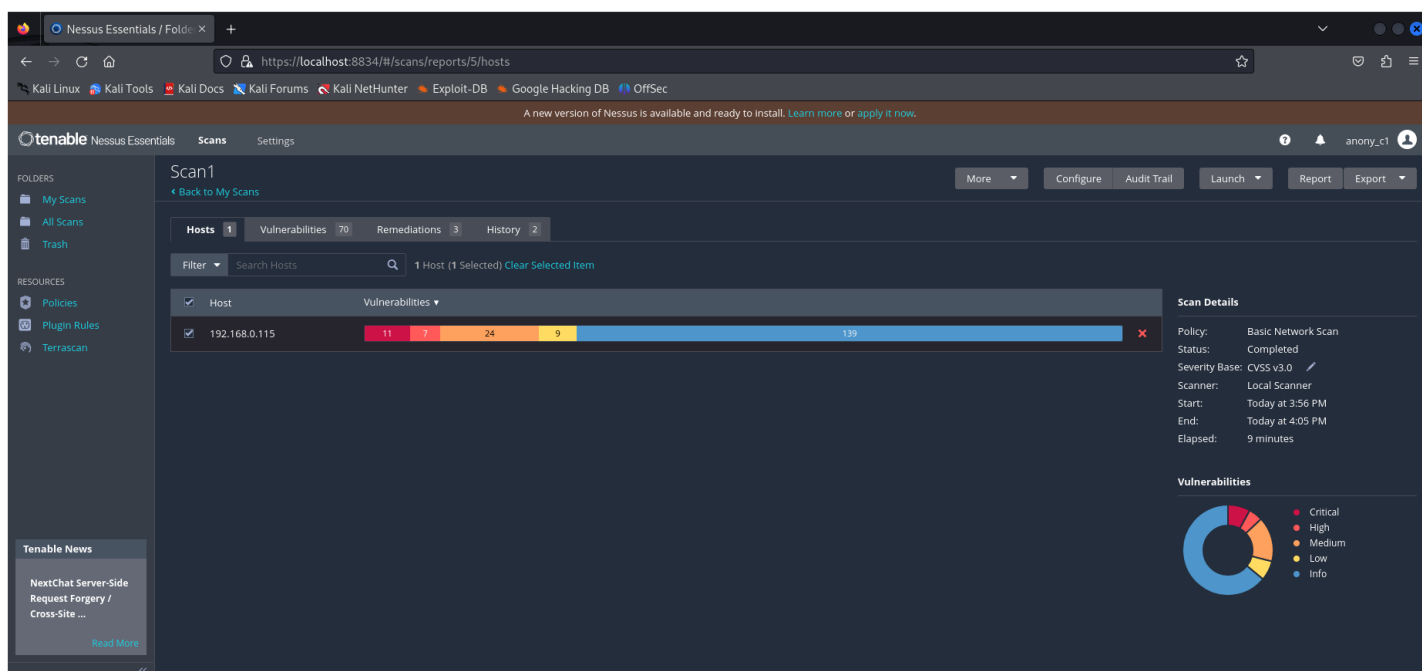
Then I gave the scan name 'Scan1' and provided scan description, Folder to save the scan & the target IP 192.168.0.115



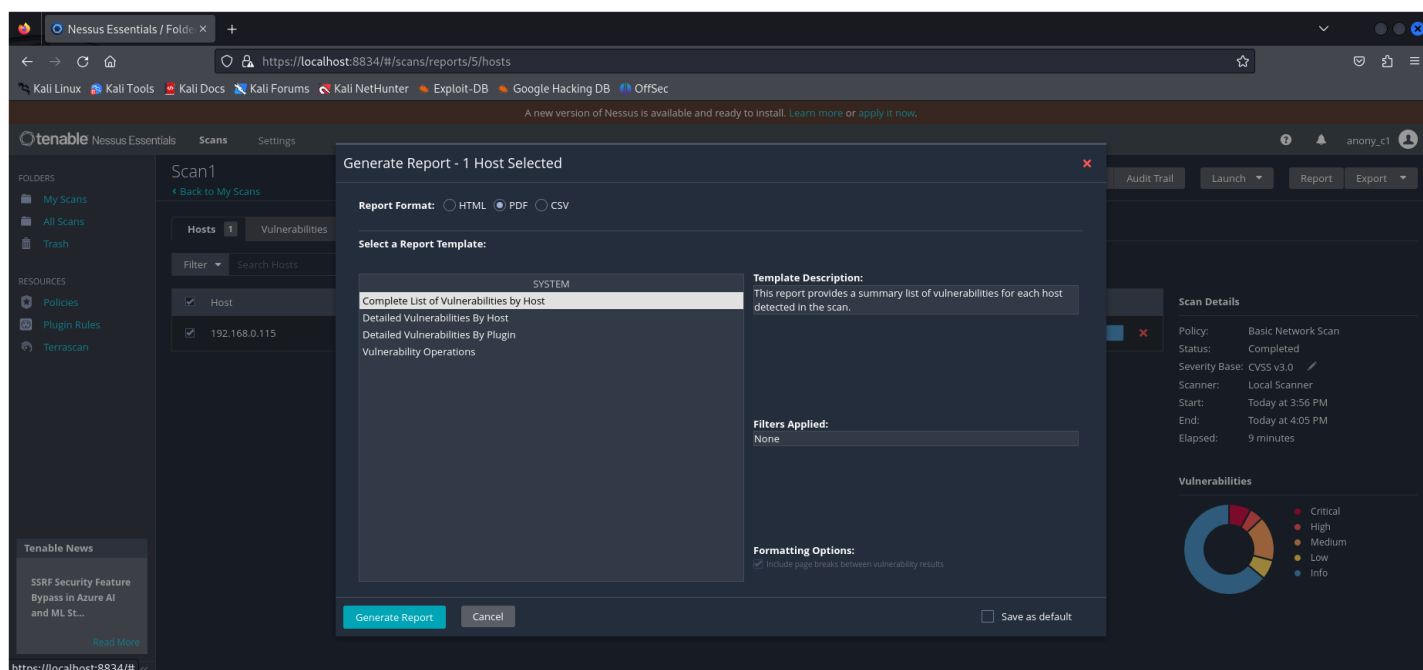
I changed the Scan Type from 'Port Scan (Common Ports)' to 'Port Scan (All Ports)' in the 'Discovery' Option.



After launching the target IP scan, Scan1, it takes a few minutes to generate the scan result and then gives a brief result of the vulnerabilities.



Then I clicked on 'Report' option to generate the report in .pdf format and selected the option 'Complete List of Vulnerabilities by Host'.



Here are the detailed report of the vulnerabilities scanned by Nessus.



Scan1

Report generated by Tenable Nessus™

Mon, 05 Aug 2024 16:05:22 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.0.115

Vulnerabilities by Host

192.168.0.115



Vulnerabilities

Total: 116

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.0817	32314	Debian OpenSSH/OpenSSL Package Random Number Ge Weakness
CRITICAL	10.0*	5.1	0.0817	32321	Debian OpenSSH/OpenSSL Package Random Number Ge Weakness (SSL check)
CRITICAL	10.0*	5.9	0.015	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	0.6495	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0234	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0323	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection
HIGH	7.5*	5.9	0.015	10245	rsh Service Detection
MEDIUM	6.5	4.4	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate

192.168.0.115

4

MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	0.9727	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.0031	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	0.9524	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obs and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0054	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	4.0	0.0465	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	0.0114	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9483	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (Logjam)
LOW	3.7	3.6	0.1227	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	2.9	0.9736	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	2.9	0.9736	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supp (Logjam)
LOW	3.4	5.1	0.9749	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	-	10407	X Server Detection
INFO	N/A	-	-	10223	RPC portmapper Service Detection

192.168.0.115

5

INFO	N/A	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11156	IRC Daemon Version Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	10719	MySQL Server Detection

192.168.0.115

6

INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported

192.168.0.115

7

INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosur

192.168.0.115

8

INFO	N/A	-	-	52703	vsftpd Detection
------	-----	---	---	-------	------------------

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.115

9

There are mentioned all the vulnerabilities detected by Nessus with risk level – critical, high. medium & low with other info. These vulnerabilities can be exploited by attackers & are harmful for the system, so fast actions are required to fix these vulnerabilities.

Here the Network Penetration Testing of the target device with the IP 192.168.0.115 is completed.

Conclusion

In summary, cybersecurity is essential for safeguarding digital information in an increasingly interconnected world, where sophisticated threats pose significant risks to data integrity, confidentiality, and availability. Network Penetration Testing (NPT), along with ethical hacking, plays a vital role in this domain by proactively identifying and addressing vulnerabilities before they can be exploited. These practices not only enhance overall security but also assist organizations in meeting compliance standards and protecting against potential breaches. As the need for skilled cybersecurity professionals grows, a career in this field offers promising opportunities to contribute to a secure digital environment. Embracing comprehensive security measures and continuous learning is crucial for effectively defending our digital infrastructure.

This project has significantly expanded my knowledge by providing a deeper understanding of key cybersecurity concepts, such as the importance of protecting digital information, the role of ethical hacking, and the critical function of Network Penetration Testing (NPT). Through researching these topics, I have gained insights into how proactive security measures help identify and address vulnerabilities, enhance organizational defenses, and ensure compliance. Additionally, exploring career opportunities in cybersecurity has highlighted the growing demand for skilled professionals and the importance of ongoing learning in this rapidly evolving field.

References

- GeeksforGeeks
- Youtube
- Wikipedia
- Kali Linux
- Metasploitable