

Task 1

Task 1 :Scan Your Local Network for Open Ports

1.Install Nmap from official website.



I complete installation

2.Find your local IP range (e.g., 192.168.1.0/24).

```
C:\WINDOWS\system32\ x + ~
C:\Users\Asus>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::127a:499d:be32:7d77%21
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
```

3.Run: *nmap -sS 192.168.1.0/24* to perform TCP SYN scan.

```
Not shown: 994 closed ports
PORT      STATE      SERVICE
135/tcp   open       msrpc
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
514/tcp   filtered  shell
902/tcp   open       iss-realsure
912/tcp   open       apex-mesh
```

4.Note down IP addresses and open ports found.

Yes I note down

5.Optionally analyze packet capture with Wireshark.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help					
Filter:		Expression... Clear Apply			
No.	Time	Source	Destination	Protocol	Length
1038	40.422312	192.168.1.77	173.194.33.1	TCP	54
1039	40.659611	fe80::bdca:e67b:5eb7:1ff02::c		SSDP	201
1040	41.550320	192.168.1.77	207.8.65.23	HTTP	51
1041	41.580992	207.8.65.23	192.168.1.77	TCP	60
1042	42.051665	192.168.1.76	239.255.255.250	UDP	50
1043	42.104199	Actionte_d8:a3:88	Msi_74:82:e6	ARP	60
1044	42.104226	Msi_74:82:e6	Actionte_d8:a3:88	ARP	40
1045	42.119803	192.168.1.74	239.255.255.250	UDP	56
1046	42.910321	192.168.1.77	74.125.53.125	Jabber />	51
1047	42.929318	74.125.53.125	192.168.1.77	TCP	60
1048	43.659423	fe80::bdca:e67b:5eb7:1ff02::c		SSDP	201
1049	45.052365	192.168.1.76	239.255.255.250	UDP	50
1050	45.121318	192.168.1.74	239.255.255.250	UDP	56
1051	45.418680	192.168.1.77	72.165.61.176	UDP	120
1052	46.659410	fe80::bdca:e67b:5eb7:1ff02::c		SSDP	201
<div> <div>III</div> </div>					
<div> <div>+</div> Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) </div>					
<div> <div>+</div> Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:0 </div>					
<div> <div>+</div> Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239. </div>					
<div> <div>+</div> Internet Group Management Protocol </div>					

6. Research common services running on those ports.

Yes I notes few protocol in show above

7. Identify potential security risks from open ports.

Show any port are risk provide to system or not

If yes → close, block, or secure it.

8. Save scan results as a text or HTML file.

Name	Filter
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
IPX only	ipx
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80 25}

Task 2: Analyze a Phishing Email Sample

1. Obtain a sample phishing email (many free samples online).

From: **GlobalPay** <VT@globalpay.com>  Hide
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

1 Attachment, 7 KB

Save ▼

Quick Look

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc



[update2816.html \(7 KB\)](#)

2. Examine sender's email address for spoofing.

Delivered-To: david@example.com
Received: by 10.76.84.202 with SMTP id d10csp3498721oab;
Fri, 07 Feb 2014 03:47:15 -0700 (MST)
X-Received: by 10.152.35.5 with SMTP id h5mr9284714lab.49.1391765235143;
Fri, 07 Feb 2014 03:47:15 -0700 (MST)
Return-Path: <VT@globalpay.com>
Received: from mail.fakeglobalpay.com (unknown [203.0.113.42])
by mx.example.com with ESMTP id abc123xyz456
for <david@example.com>;
Fri, 07 Feb 2014 03:47:02 -0700 (MST)
Authentication-Results: mx.example.com;
spf=fail (example.com: domain of VT@globalpay.com does not designate
dkim=fail header.i=@globalpay.com;
dmarc=fail (p=REJECT) header.from=globalpay.com
From: GlobalPay <VT@globalpay.com>
To: David
Subject: Restore your account
Date: Fri, 07 Feb 2014 03:47:02 -0700
Message-ID: <20140207034702.VT12345@globalpay.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="phishing-boundary"
Content-Disposition: inline
X-Mailer: PhishMailer 1.0

3. Check email headers for discrepancies (using online header analyzer).

Delivery Information

- ✖ DMARC Compliant
- ✔ SPF Alignment
- ✖ SPF Authenticated
- ✖ DKIM Alignment
- ✖ DKIM Authenticated

Header Name	Header Value
Delivered-To	david@example.com
X-Received	by 10.152.35.5 with SMTP id h5mr9284714lab.49.1391765235143; Fri, 07 Feb 2014 03:47:15 -0700 (MST)
Return-Path	<VT@globalpay.com>
Authentication-Results	mx.example.com; spf=fail (example.com: domain of VT@globalpay.com does not designate 203.0.113.42 as permitted sender) smtp.mailfrom=VT@globalpay.com; dkim=fail header.i=@globalpay.com; dmarc=fail (p=REJECT) header.from=globalpay.com
From	GlobalPay <VT@globalpay.com>
To	David
Subject	Restore your account
Date	Fri, 07 Feb 2014 03:47:02 -0700
Message-ID	<20140207034702.VT12345@globalpay.com>
MIME-Version	1.0
Content-Type	multipart/mixed; boundary="phishing-boundary"
Content-Disposition	inline
X-Mailer	PhishMailer 1.0

4. Identify suspicious links or attachments.

<https://tinyurl.com/mhswfafx>

5. Look for urgent or threatening language in the email body.

<https://www.virustotal.com>

It checks if the URL is malicious.

6. Note any mismatched URLs (hover to see real link).

- "Account suspended"
- "Pay now or lose access"
- "Immediate action required"

7. Verify presence of spelling or grammar errors.

- Broken English
- Spelling errors

- *Misused punctuation*

8. Summarize phishing traits found in the email.

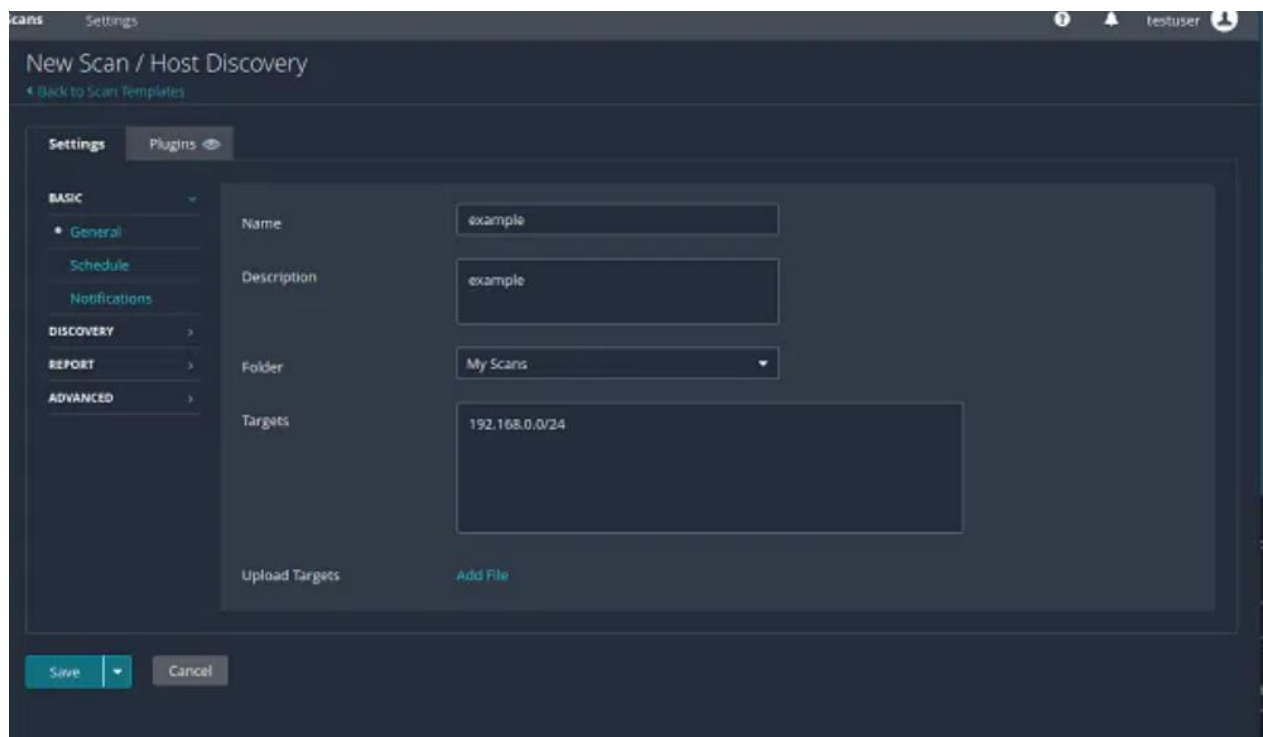
- **Fake Sender Address:**
- From: security@apple-support.com → looks like Apple, but not real.
- **Spoofed Links:**
- Link: <http://apple.secure-login-update.com> (not real Apple site)
- **Header Analysis:**
- SPF: fail
- DKIM: not signed
- **Urgent Language:**
- “Your account will be locked in 24 hours.”
- **Spelling/Grammar Errors:**
- “acount” instead of “account”
- “safely verify you information”
- **Suspicious Attachment:**
- Invoice.html → may contain malicious code

Task 3: Perform a Basic Vulnerability Scan on Your PC.

1. Install OpenVAS or Nessus Essentials.



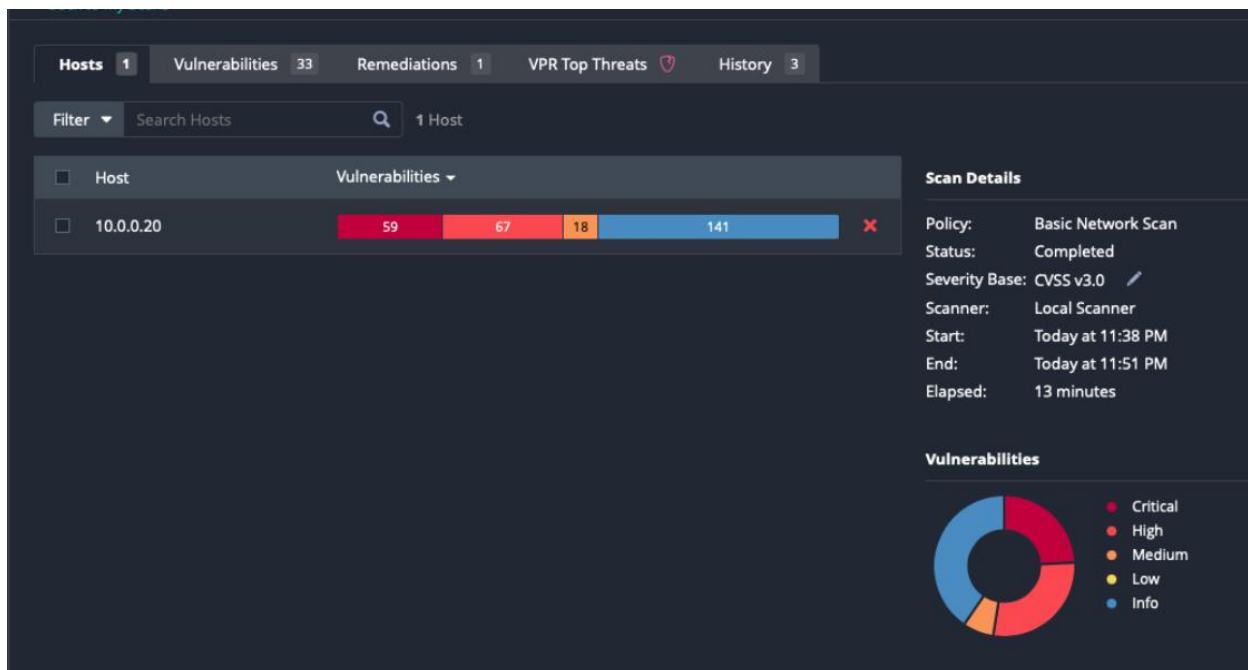
2. Set up scan target as your local machine IP or localhost



3.Start a full vulnerability scan.

4.Wait for scan to complete (may take 30-60 mins).

5.Review the report for vulnerabilities and severity



6.Research simple fixes or mitigations for found vulnerabilities.

Description

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

Solution

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4169

Output

```
Nessus received a 350 response from sending the following unauthenticated request :  
SITE CPFR /etc/passwd
```

Severity: Critical
ID: 84215
Version: 1.10
Type: remote
Family: FTP
Published: June 16, 2015
Modified: March 27, 2020

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Functional
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

7.Document the most critical vulnerabilities.

FileEditView

Description:

The system has Server Message Block version 1 (SMBv1) protocol enabled. SMBv1 is an outdated file-sharing protocol that is vulnerable to remote code execution (RCE) attacks. Notably, it was exploited in the WannaCry ransomware attack.

Affected Operating Systems:

- Windows 7
- Windows 8.1
- Windows Server 2008
- Windows Server 2012

Impact:

If SMBv1 is not disabled, attackers can:

- Remotely execute code
- Spread malware like worms/ransomware
- Compromise multiple systems over the network

Evidence Found:

- Port 445 detected as open
- SMB version 1.0 confirmed active by Nessus

Remediation:

To disable SMBv1 on Windows:

PowerShell Command:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

Additional Tips:

- Restart the system after running the command
- Confirm by checking SMB status:
Get-SmbServerConfiguration | Select EnableSMB1Protocol

Final Note:

Disabling SMBv1 is a critical step in hardening your system against modern cyber threats. Always prefer SMBv2 or SMBv3 for secure file sharing.

8.Take screenshots of the scan results.

Filter

Search Vulnerabilities

15 Vulnerabilities

<input type="checkbox"/>	Sev	Score	Name	Family	Count		
<input type="checkbox"/>	MEDIUM	5.3	SMB Signing ...	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	...	SMB (M...	Windows	6	🔄	✎
<input type="checkbox"/>	INFO		DCE Services ...	Windows	9	🔄	✎
<input type="checkbox"/>	INFO		Nessus SYN s...	Port scanners	3	🔄	✎
<input type="checkbox"/>	INFO		Common Pla...	General	1	🔄	✎
<input type="checkbox"/>	INFO		Device Type	General	1	🔄	✎
<input type="checkbox"/>	INFO		Ethernet MA...	General	1	🔄	✎
<input type="checkbox"/>	INFO		ICMP Timest...	General	1	🔄	✎
<input type="checkbox"/>	INFO		Link-Local M...	Service detection	1	🔄	✎
<input type="checkbox"/>	INFO		Nessus Scan ...	Settings	1	🔄	✎
<input type="checkbox"/>	INFO		OS Identificat...	General	1	🔄	✎
<input type="checkbox"/>	INFO		OS Security P...	Settings	1	🔄	✎
<input type="checkbox"/>	INFO		Target Crede...	Settings	1	🔄	✎

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 10:50 PM

End: Today at 10:53 PM

Elapsed: 3 minutes

Vulnerabilities

● Critical

● High

● Medium

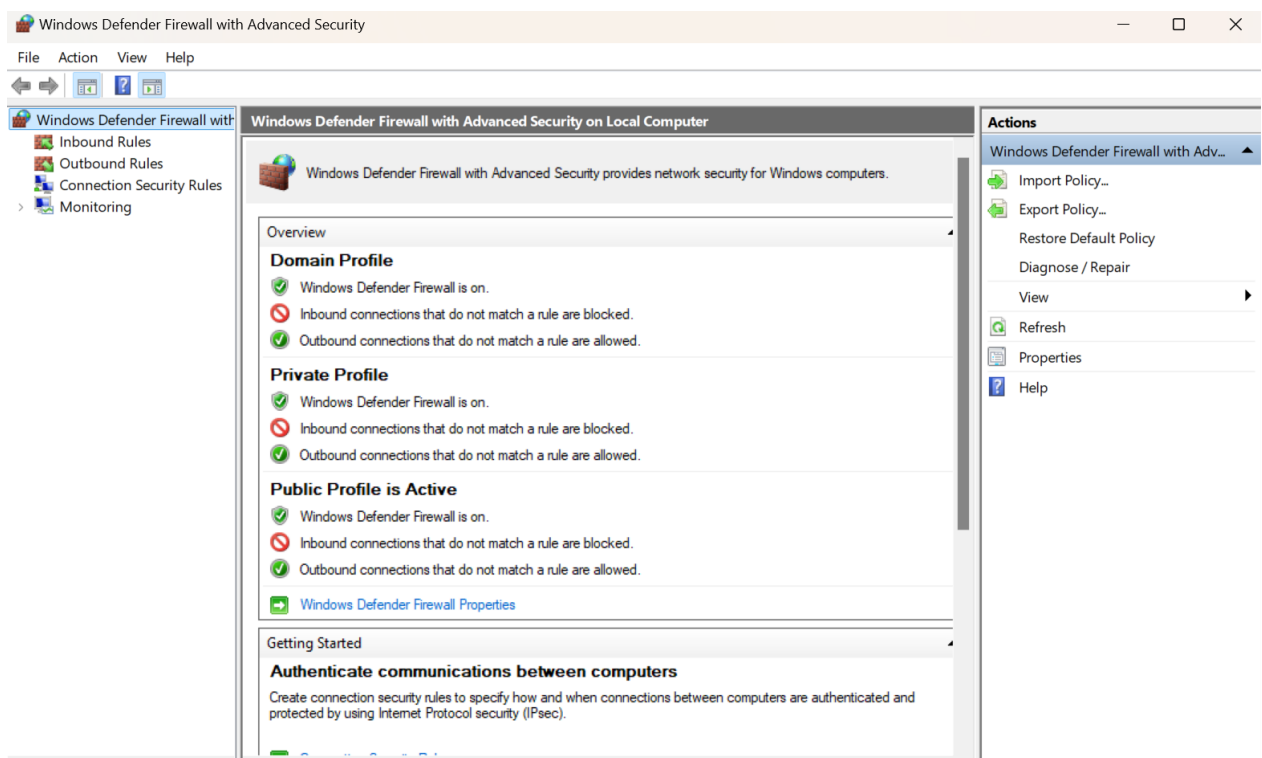
● Low

● Info

Task 4: *Setup and Use a Firewall on Windows/Linux*

1. Open firewall configuration tool (Windows Firewall or terminal for UFW).

2. List current firewall rules.



3. Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP
☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports
☒ Specific local ports:

Example: 80, 443, 5000-5010

4. Test the rule by attempting to connect to that port locally or remotely.

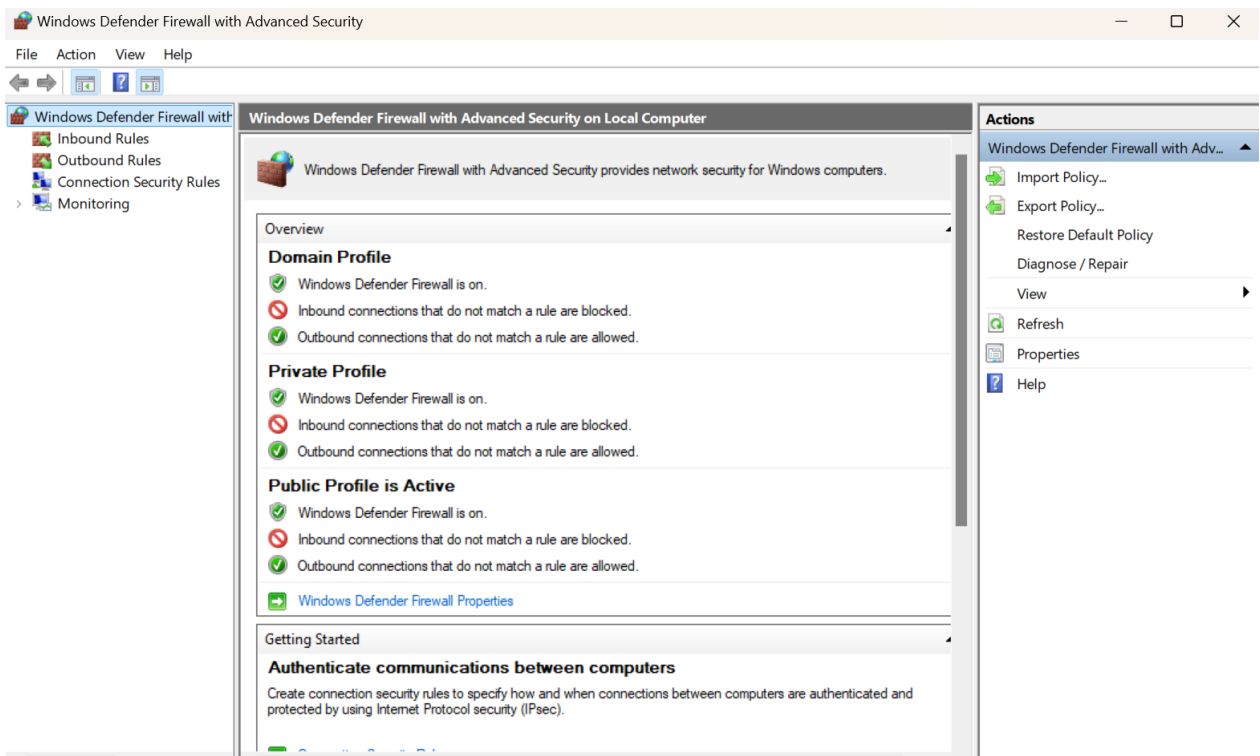
```
TCP 127.0.0.1:49706 127.0.0.1:49707 ESTABLISHED 6212
TCP 127.0.0.1:49707 127.0.0.1:49706 ESTABLISHED 6212
TCP 127.0.0.1:49723 127.0.0.1:49724 ESTABLISHED 6212
TCP 127.0.0.1:49724 127.0.0.1:49723 ESTABLISHED 6212
TCP 192.168.111.1:139 0.0.0.0:0 LISTENING 4
TCP 192.168.213.186:139 0.0.0.0:0 LISTENING 4
TCP 192.168.226.1:139 0.0.0.0:0 LISTENING 4
TCP [::]:135 [::]:0 LISTENING 1324
TCP [::]:445 [::]:0 LISTENING 4
TCP [::]:7680 [::]:0 LISTENING 13620
TCP [::]:8834 [::]:0 LISTENING 6212
TCP [::]:49664 [::]:0 LISTENING 656
TCP [::]:49665 [::]:0 LISTENING 992
TCP [::]:49666 [::]:0 LISTENING 1344
TCP [::]:49667 [::]:0 LISTENING 2084
TCP [::]:49668 [::]:0 LISTENING 3508
TCP [::]:49672 [::]:0 LISTENING 892
```

5. Add rule to allow SSH (port 22) if on Linux.

```
ubuntu@linuxopsys:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22 ALLOW IN Anywhere
22 (v6) ALLOW IN Anywhere (v6)
```

6. Remove the test block rule to restore original state.



Go back to **Inbound Rules**, find `Block Telnet`, right-click → **Delete**

7. Document commands or GUI steps used.

Blocked TCP port 23 using Windows Firewall Advanced Settings

8. Summarize how firewall filters traffic

Windows Firewall **filters** traffic based on **rules**: allow/block specific **ports**, **IPs**, **apps**, etc.

Task 5: *Capture and Analyze Network Traffic Using Wireshark.*

1. Install Wireshark.



2. Start capturing on your active network interface.

3. Browse a website or ping a server to generate traffic

4. Stop capture after a minute.

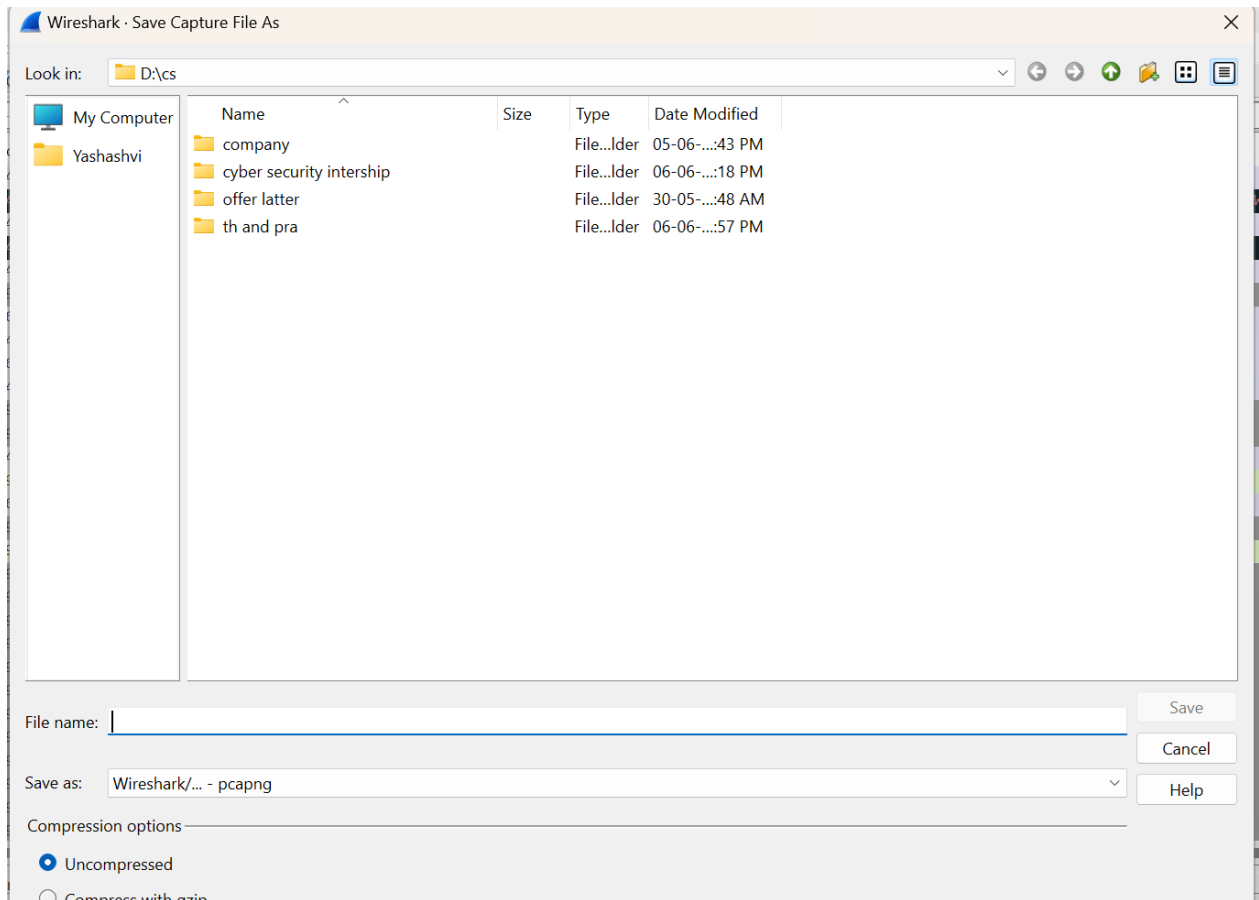
5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help					
Filter:		Expression... Clear Apply			
No.	Time	Source	Destination	Protocol	Length
1038	40.422312	192.168.1.77	173.194.33.1	TCP	54
1039	40.659611	fe80::bdca:e67b:5eb7:1ff02::c		SSDP	201
1040	41.550320	192.168.1.77	207.8.65.23	HTTP	51
1041	41.580992	207.8.65.23	192.168.1.77	TCP	60
1042	42.051665	192.168.1.76	239.255.255.250	UDP	50
1043	42.104199	Actionte_d8:a3:88	Msi_74:82:e6	ARP	60
1044	42.104226	Msi_74:82:e6	Actionte_d8:a3:88	ARP	40
1045	42.119803	192.168.1.74	239.255.255.250	UDP	56
1046	42.910321	192.168.1.77	74.125.53.125	Jabber />	51
1047	42.929318	74.125.53.125	192.168.1.77	TCP	60
1048	43.659423	fe80::bdca:e67b:5eb7:1ff02::c		SSDP	201
1049	45.052365	192.168.1.76	239.255.255.250	UDP	50
1050	45.121318	192.168.1.74	239.255.255.250	UDP	56
1051	45.418680	192.168.1.77	72.165.61.176	UDP	120
1052	46.659410	fe80::bdca:e67b:5eb7:1ff02::c		SSDP	201
<div> <div></div> <div>1000</div> </div>					
<div> <div>+</div> Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) </div> <div> <div>+</div> Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:0 </div> <div> <div>+</div> Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239. </div> <div> <div>+</div> Internet Group Management Protocol </div>					

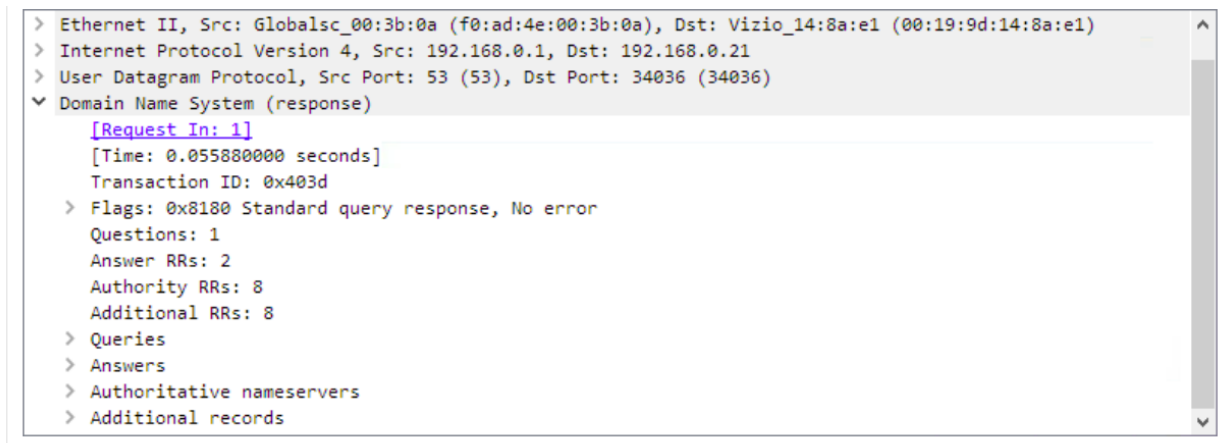
6. Identify at least 3 different protocols in the capture.

http,ssdp,arp

7. Export the capture as a .pcap file.



8. Summarize your findings and packet details



Task 6 : Create a Strong Password and Evaluate Its Strength

1. Create multiple passwords with varying complexity.

2. Use uppercase, lowercase, numbers, symbols, and length variations.

<i>Password</i>	<i>Description</i>
<i>hello123</i>	<i>Simple lowercase + numbers</i>
<i>Hello123</i>	<i>Added uppercase</i>
<i>Hello@123</i>	<i>Added special symbol</i>
<i>H3lL0@2025!</i>	<i>Mixed complex + longer</i>
<i>A\$tr0n0mY!@#</i>	<i>Strong password with symbols</i>
<i>qwerty</i>	<i>Common weak password</i>
<i>P@ssw0rd</i>	<i>Looks strong, but commonly used</i>

3. Test each password on password strength checker.

<https://password.kaspersky.com>

<https://howsecureismypassword.net>

4.Note scores and feedback from the tool.

<i>Password</i>	<i>Time to Crack (approx)</i>	<i>Feedback</i>
<i>hello123</i>	<i>Few seconds</i>	<i>Too simple</i>
<i>Hello123</i>	<i>2 minutes</i>	<i>Better, but still weak</i>
<i>Hello@123</i>	<i>20 minutes</i>	<i>Acceptable, not very strong</i>
<i>H3lL0@2025!</i>	<i>Centuries</i>	<i>Very strong</i>
<i>A\$tr0n0mY!@#</i>	<i>Billions of years</i>	<i>Excellent password</i>
<i>qwerty</i>	<i>Instant</i>	<i>Extremely weak</i>

5. Identify best practices for creating strong passwords.

- *Long (at least 12+ characters)*
- *Uses uppercase + lowercase + numbers + symbols*
- *Avoid common patterns (like 123, password, qwerty)*
- *Not based on dictionary words*
- *Not reused on multiple sites*

6. Write down tips learned from the evaluation.

- *Use random phrases or passphrases (e.g., Sun\$etRun@2025!)*
- *Replace letters with symbols or numbers (like o → 0, a → @)*
- *Use password managers to generate/store strong passwords*
- *Don't write passwords on paper*

7. Research common password attacks (brute force, dictionary).

<i>Attack Type</i>	<i>Description</i>
<i>Brute Force</i>	<i>Tries every combination (slow but effective)</i>
<i>Dictionary Attack</i>	<i>Uses a list of common words/passwords</i>
<i>Phishing</i>	<i>Tricks user into revealing password</i>
<i>Credential Stuffing</i>	<i>Reuses leaked passwords on other sites</i>

8. Summarize how password complexity affects security..

Simple passwords (like hello123) are cracked in seconds using brute force or dictionary attacks.

Complex passwords (like A\$tr0n0mY!@#) resist brute force because of longer length and randomness.

Using common passwords, even with symbols (P@ssw0rd), is risky. Attackers guess them easily.

The more unique and random, the better.

Task 7: Identify and Remove Suspicious Browser Extensions

Question 1:

Did you open the extension page in your browser?

Open Extension Page:

Chrome → Type: chrome://extensions/

Firefox → Type: about:addons

Press Enter

Answer:

Yes, I opened the extensions page by typing the URL and pressing Enter.

Question 2:

Is there any extension you don't remember installing?

Check All Installed Extensions:

Look at the names of all extensions.

Do you use them? Do you remember installing them?

Answer:

I recognize all extensions OR I found some unknown extensions.

Question 3:

Does any extension ask for too much access or have bad reviews?

Check Extension Details:

Click on "Details" or the extension name.

Check permissions (e.g., read all site data).

Search the name on Google and check reviews.

Answer:

*Some extensions ask for too much access or have bad reviews
OR All extensions look safe.*

Question 4:

Did you remove any extensions that looked suspicious or unnecessary?

Remove Suspicious or Unused Extensions:

Click "Remove" or "Delete".

Remove suspicious, unused, or poorly rated extensions.

Answer:

*I removed extensions that looked suspicious or unnecessary
OR I kept all because they were safe.*

Question 5:

Did your browser feel faster or safer after restarting?

Restart Your Browser:

Close all browser windows.

Open your browser again.

Answer:

The browser feels faster and safer OR No difference noticed yet.

Task 8 :Identify and Remove Suspicious Browser Extensions

- 1.Choose a reputable free VPN service and sign up.*
- 2.Download and install the VPN client.*
- 3.Connect to a VPN server (choose closest or any location).*
- 4.Verify your IP address has changed (use whatismyipaddress.com).*
- 5.Browse a website to confirm traffic is encrypted.*
- 6.Disconnect VPN and compare browsing speed and IP.*
- 7.Research VPN encryption and privacy features.*
- 8.Write a summary on VPN benefits and limitations.*