10/30/2024

Task 1: Introduction to Network Security Basics

Submitted by:-

Ahatesham Mopagar

THE RED USER

Introduction

During my time as a Cyber Security Intern at The Red Users, I was immersed in the dynamic and ever evolving field of cybersecurity. Throughout my tasks, I developed a foundational understanding of network security and web applicat ion security, learning to identify and mitigate common vulnerabilities.

In the first task, I delved into the fundamentals of network security. I explored various network threats, such as viruses, worms, trojans, and phishing attacks, understanding how they operate and how to defend against them. By setting up a simple network environment and configuring security measures like firewalls and encryption, I gained hands on experience in protecting a network from unauthorized access. Additionally, Ilearned to monitor network traffic using Wireshark, identifying different types of traffic and recognizing suspicious activity. This task provided me with a solid foundation in network security, equipping me with the skills needed to secure small networks and detect potential threats.

Objective

The objective of Task 1 was to understand the basics of network security by learning about different types of network threats and implementing basic security measures. This task aimed to equip me with foundational knowledge and practical skills in securing a small network environment. By exploring various network threats, setting up a secure network, monitoring traffic, and reflecting on best practices, I developed a solid understanding of how to protect networks from unauthorized access and detect potential security threats.

This hands-on experience laid the ground work for more advanced security concepts and techniques, preparing me to tackle complex security challenges in the future.

Tools:

1. **Firewall (Windows Defender Firewall):**
    - Enabled and configured to block unauthorized access and protect the network.
2. **Wireshark:**
    - Utilized to capture and analyze network traffic.
    - Identified different types of traffic such as HTTP, DNS, and others.

Methods:

1. **Research and Summarize Network Threats:**
    - Explored various network threats including viruses, worms, trojan, and phishing attacks.
    - Understood how these threats operate and the basic security concepts to defend against them.
2. **Set Up Network Environment:**
    - Configured a simple network environment with a router and connected devices.
    - Implemented basic security configurations like changing default passwords and enabling network encryption (WPA2/WPA3).
3. **Enable and Configure Firewall:**
    - Set up Windows Defender Firewall to block unauthorized access.
    - Applied security rules to restrict access to network resources.
4. **Monitor Network Traffic with Wireshark:**
    - Captured network traffic to identify various types of traffic and their significance.
    - Analyzed the captured traffic to spot unusual or suspicious activity that might indicate a security threat.

Network Threats:

Network threats are malicious activities that target computer systems connected to a network. These threats can compromise data security, disrupt operations, and cause financial loss.

Some common types of network threats include:

1. Viruses
2. Worms
3. Trojans

1. Viruses

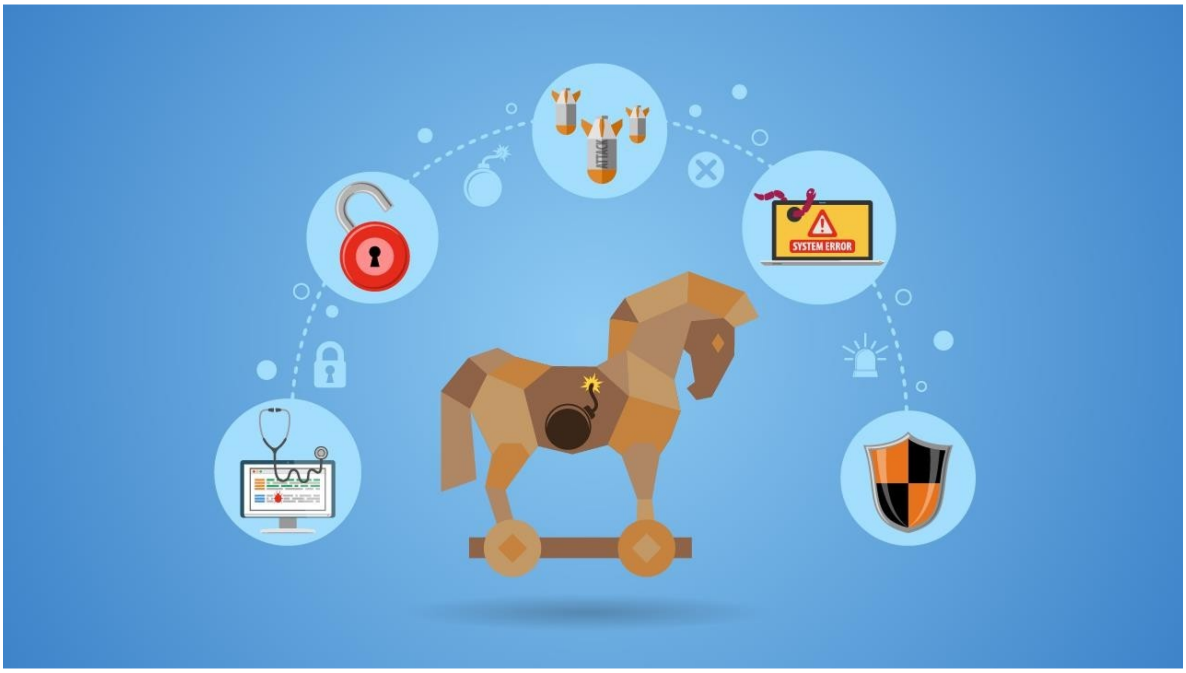
Viruses are self-replicating malicious programs that attach themselves to other executable files. When an infected file is executed, the virus spreads to other files and systems on the network. Viruses can damage files, corrupt data, and slow down system performance.

2. **Worms**

Worms are self-propagating malware that can replicate themselves without requiring a host program. They often exploit vulnerabilities in network protocols to spread rapidly across a network, consuming bandwidth and system resources.

3. **Trojans**

Trojans are malicious programs disguised as legitimate software. They often trick users into downloading and executing them, after which they can install malware, steal data, or take control of the infected system.

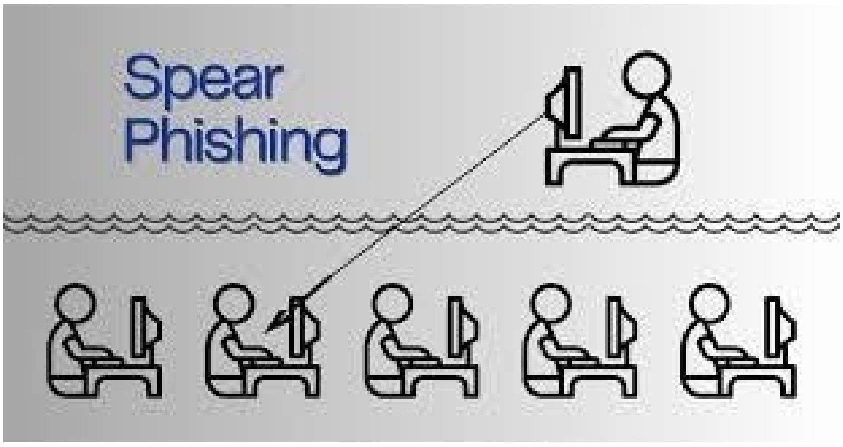


Phishing Attacks

Phishing attacks are attempts to deceive users into disclosing sensitive information, such as passwords or credit card details. Phishing emails often appear to be from legitimate sources, such as banks or online retailers, and may contain links to malicious websites or attachments.

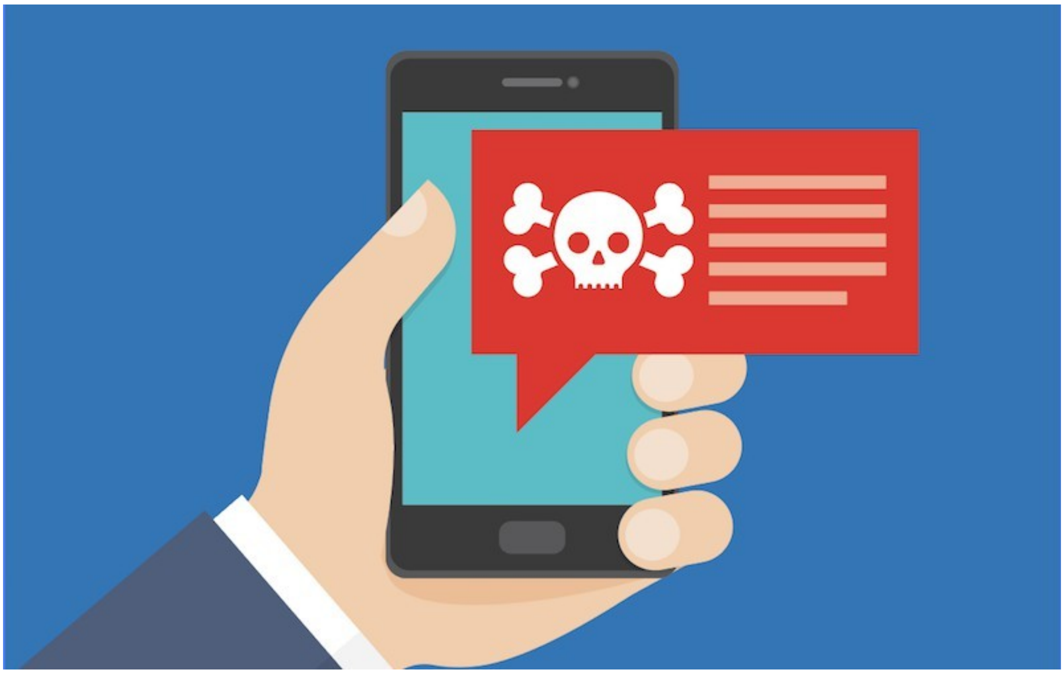
Types of Phishing:

- **Spear Phishing:** Targeted attacks that use personal information to make the emails appear more convincing.



- **Whaling:** Phishing attacks targeting high-profile individuals, such as CEOs or executives.

- **Smishing:** Phishing attacks that use text messages to deceive victims.



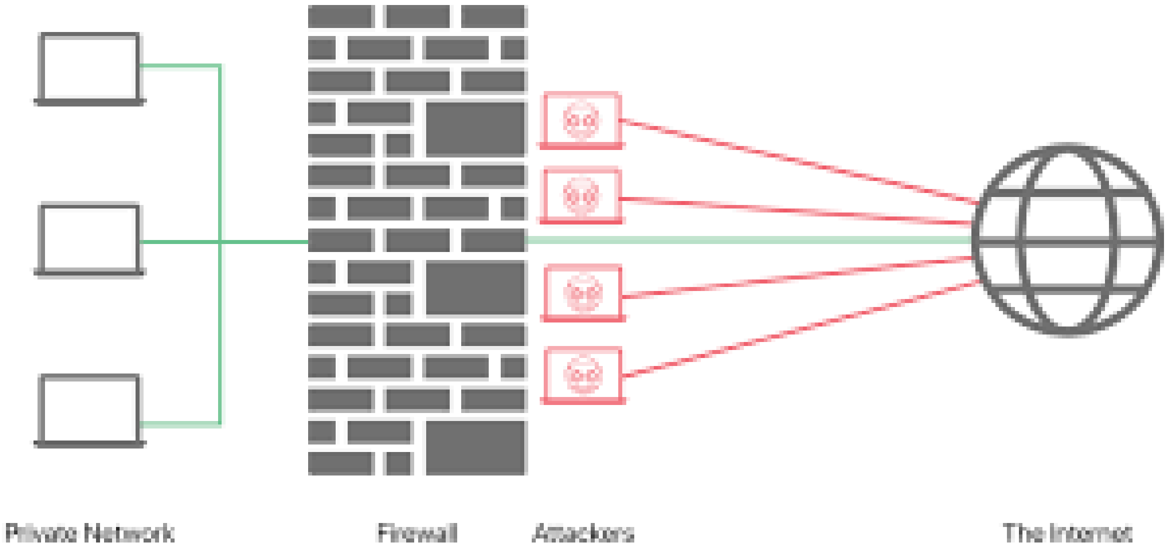
- **Vishing:** Phishing attacks that use voice calls to deceive victims.

Protecting Against Network Threats

- **Keep software up to date**
- **Use strong passwords**
- **Be cautious of suspicious emails**
- **Use antivirus and antimalware software**
- **Back up important data**
- **Educate users**

Firewalls

Firewalls are network security devices that act as a barrier between a trusted network (e.g., your internal network) and an untrusted network (e.g., the internet). They monitor and filter incoming and outgoing network traffic, preventing unauthorized access and attacks. Firewalls can be hardware-based appliances or software-based programs.



Types of Firewalls

1. Packet Filtering Firewalls
2. Stateful Inspection Firewalls
3. Application Firewalls

1. Packet Filtering Firewalls

These firewalls examine individual network packets based on their headers (source and destination IP addresses, ports, protocols). They allow or block traffic based on predefined rules.

How they work:

- Examine each packet's header information.
- Compare the header information against a set of rules.
- If the packet matches a rule, it is allowed or blocked accordingly.

Example: A rule could be configured to allow all incoming traffic on port 80 (HTTP) but block all traffic on port 23 (Telnet).

2. Stateful Inspection Firewalls

These firewalls keep track of the state of network connections, allowing them to make more informed decisions about which packets to allow or block.

How they work:

- Maintain a state table that records the status of active connections.
- Examine packets in the context of their connection state.
- Allow or block packets based on the connection state and predefined rules.

Example: A stateful inspection firewall might allow a packet to initiate a TCP connection, but block subsequent packets from the same source if they don't follow the expected sequence.

3. Application Firewalls

These firewalls inspect the content of network traffic at the application layer (e.g., HTTP, FTP). They can provide more granular control over network access, blocking specific types of applications or content.

How they work:

- Examine the content of network packets, not just the headers.
- Can identify and block malicious content, such as viruses, malware, or unauthorized access attempts.

Example: An application firewall could block access to certain websites or prevent the download of specific file types.

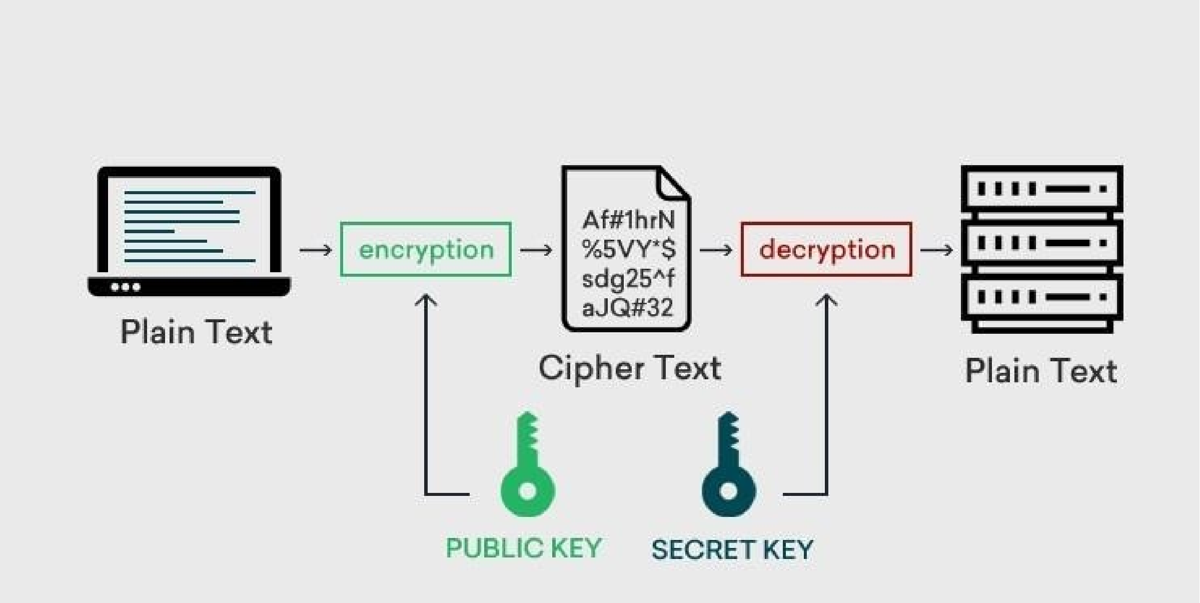
Benefits of Using Firewalls

- **Prevent unauthorized access:** Firewalls can block malicious traffic from entering a network.

- **Protect against attacks:** Firewalls can help defend against various types of attacks, such as viruses, worms, and DDoS attacks.
- **Enforce security policies:** Firewalls can be used to enforce network security policies, such as restricting access to certain websites or applications.
- **Improve network performance:** Firewalls can help improve network performance by blocking unnecessary traffic.

Encryption

Encryption is the process of converting plain text (readable data) into ciphertext (unreadable data) using a cryptographic algorithm. This makes it difficult for unauthorized individuals to access and understand the data. Encryption is a fundamental tool for protecting sensitive information, such as personal data, financial transactions, and intellectual property.



Key Concepts

- **Plaintext:** The original, readable data.
- **Ciphertext:** The encrypted data.
- **Encryption Algorithm:** The mathematical function used to convert plaintext into ciphertext.
- **Encryption Key:** A secret value used by the encryption algorithm to perform the transformation.

Types of Encryption

1. Symmetric Encryption
2. Asymmetric Encryption
3. Hybrid Encryption

1. **Symmetric Encryption**

- **How it works:** Uses the same key for both encryption and decryption.

- **Advantages:** Faster and more efficient than asymmetric encryption, suitable for large amounts of data.
- **Disadvantages:** Requires a secure method for exchanging the encryption key.

2. Asymmetric Encryption

- **How it works:** Uses different keys for encryption and decryption. One key is public, while the other is private.
- **Advantages:** Does not require a secure method for exchanging the encryption key, suitable for digital signatures and key exchange.
- **Disadvantages:** Slower and less efficient than symmetric encryption, not suitable for encrypting large amounts of data.

3. Hybrid Encryption

- **How it works:** Combines symmetric and asymmetric encryption for improved performance and security.
- **Advantages:** Provides the best of both worlds: fast encryption and decryption with secure key exchange.
- **Disadvantages:** Requires more complex implementation.

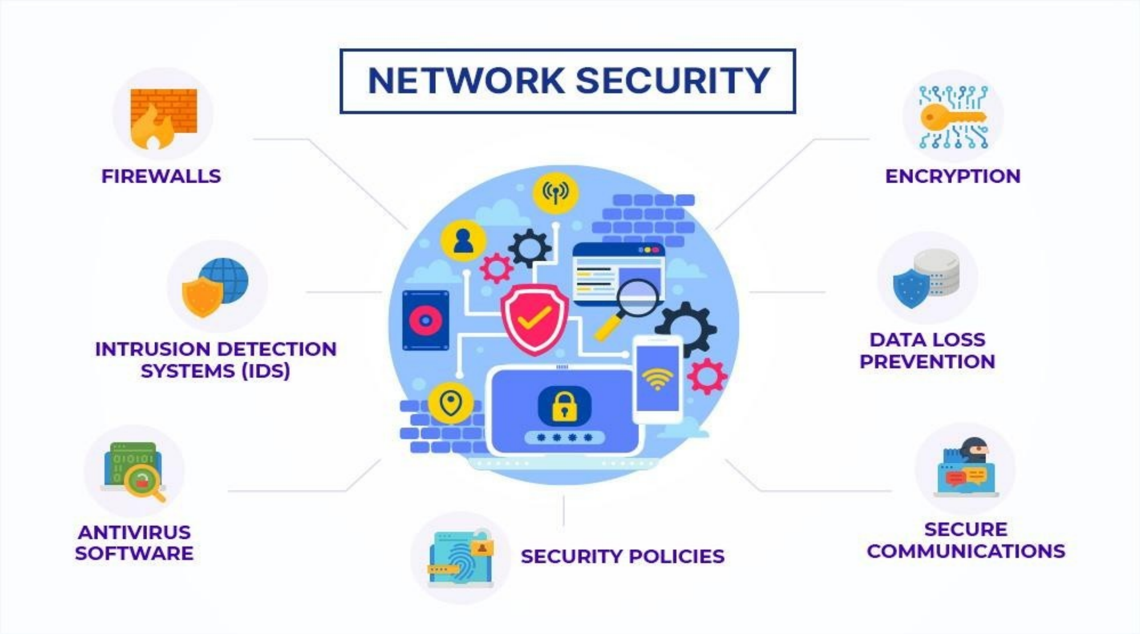
Encryption Modes

- **Electronic Codebook (ECB):** Encrypts each block of plaintext independently.
- **Cipher Block Chaining (CBC):** Encrypts each block of plaintext based on the previous block.
- **Counter Mode (CTR):** Generates a pseudo-random nonce for each block and XORs it with the plaintext.
- **Galois/Counter Mode (GCM):** Provides both encryption and authentication.

Secure Network Configurations

A secure network configuration involves implementing various security measures to protect a network from unauthorized access and attacks.

Here are some key considerations:



1. Physical Security
2. Strong Authentication
3. Access Controls
4. Patch Management
5. Intrusion Detection and Prevention Systems (IDPS)
6. Virtual Private Networks (VPNs)
7. Security Awareness Training

1. **Physical Security**

- **Physical access control:** Restrict physical access to network equipment and data centres.
- **Environmental controls:** Implement measures to protect equipment from environmental hazards (e.g., temperature, humidity, power outages).

2. **Strong Authentication**

- **Multi-factor authentication (MFA):** Require users to provide two or more factors of authentication (e.g., something they know, something they have, something they are).

- **Password policies:** Enforce strong password policies, including requiring a combination of uppercase and lowercase letters, numbers, and special characters.

3. **Access Controls**

- **Role-based access control (RBAC):** Assign permissions based on a user's role or job function.
- **Attribute-based access control (ABAC):** Assign permissions based on a user's attributes (e.g., department, location).

4. Patch Management

- **Regular updates:** Apply security patches and updates to software to address vulnerabilities.
- **Vulnerability scanning:** Use vulnerability scanning tools to identify and prioritize vulnerabilities.

5. **Intrusion Detection and Prevention Systems (IDPS)**

- **Network-based IDPS:** Monitor network traffic for signs of malicious activity.
- **Host-based IDPS:** Monitor system activity for signs of compromise.

6. **Virtual Private Networks (VPNs)**

- **Encryption:** Encrypt data transmitted over the internet to protect it from eavesdropping.
- **Tunneling:** Create a secure tunnel between two networks.

7. **Security Awareness Training**

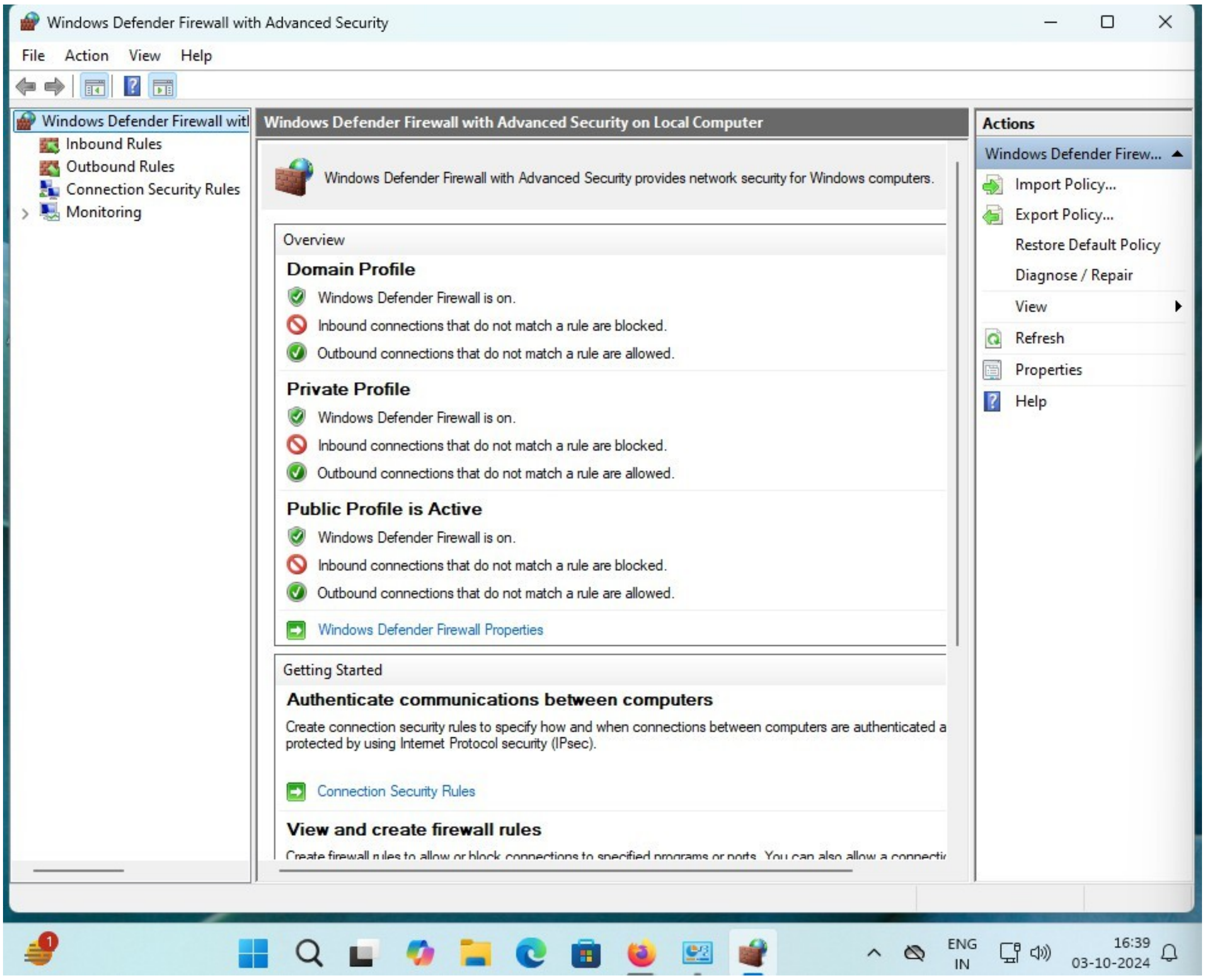
- **Educate users:** Teach users about security best practices, such as strong password management, phishing prevention, and recognizing suspicious activity.
- **Phishing simulations:** Conduct phishing simulations to test users' awareness and identify training gaps.

Security Measures Implemented

The security measures implemented on the Windows virtual machine (VM) using Windows Defender Firewall to prevent unauthorized access, particularly in an environment running VMware with both Windows and Kali Linux VMs.

Enabling Windows Defender Firewall

- **Action**: The Windows Defender Firewall was enabled for both private and public network settings.
- **Reason**: Enabling the firewall provides a basic layer of protection against unauthorized access and potential threats from both internal and
  external sources. It helps control traffic based on defined rules.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated a protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connectic

Configuration of Inbound and Outbound Rules

- **Action**: Customized inbound and outbound rules were created to block specific ports and applications based on security needs.
- **Reason**:
  - **Inbound Rules**: By blocking unauthorized ports or applications, the risk of exploitation from external sources is minimized. This prevents unauthorized access to services running on the VM.
  - **Outbound Rules**: These rules restrict applications from sending data out of the network, helping to prevent data leakage or communication with potentially harmful external servers.

Allowing Specific Programs

- **Action**: Specific applications necessary for operation were explicitly allowed through the firewall.
- **Reason**: This ensures that only trusted applications have the ability to communicate over the network, reducing the attack surface.

Configuration of Network Profile Settings

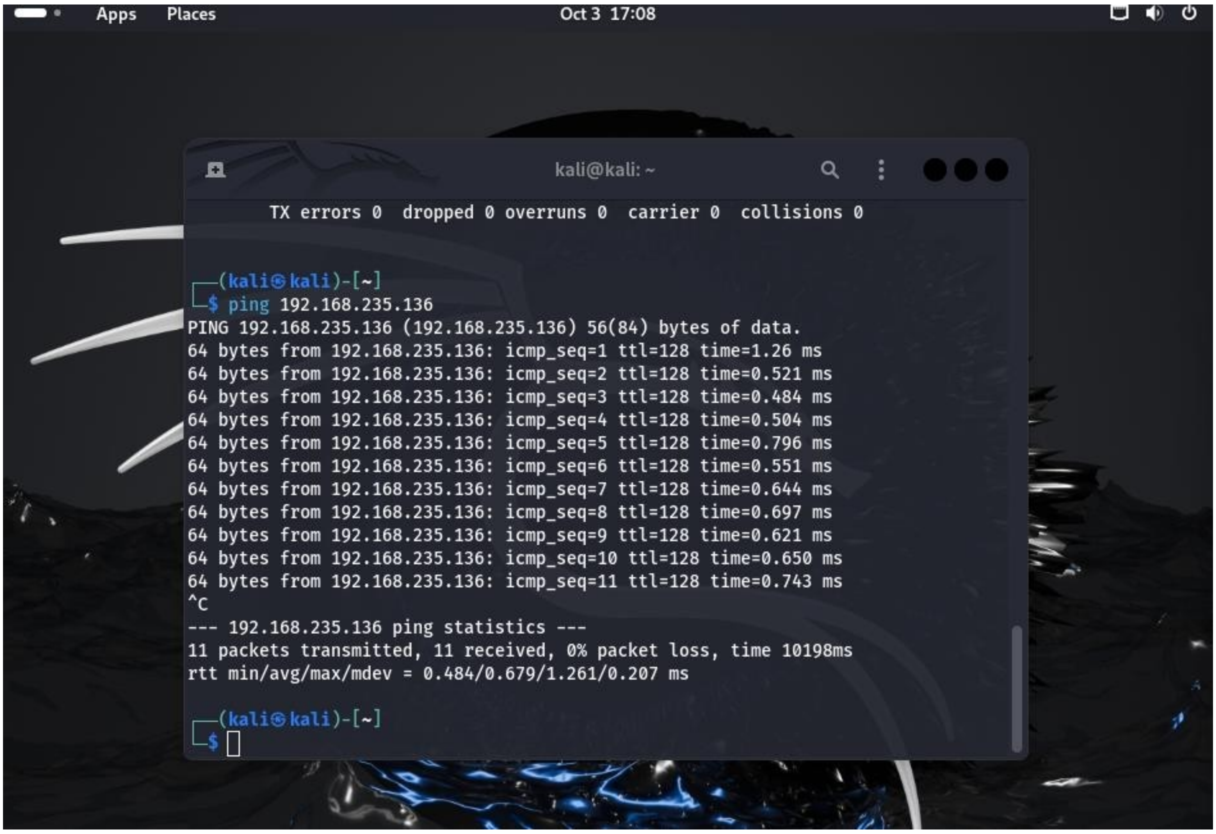
- **Action**: The Windows VM's network profile was set to either Private or Public based on its usage scenario.
- **Reason**: Different profiles apply different firewall rules, allowing for more granular control of traffic based on the network environment.

For example, a public profile would enforce stricter rules to safeguard against external threats.

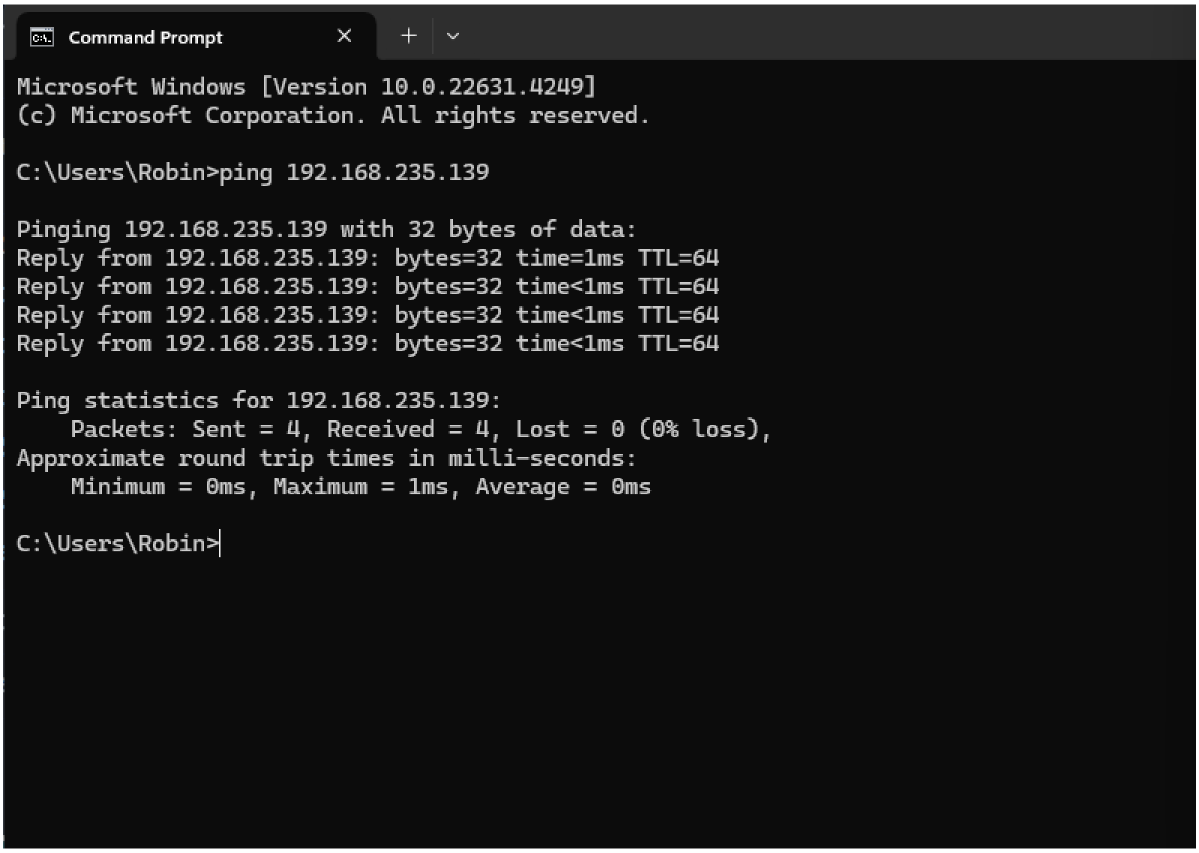
Testing Firewall Configuration

- **Action**: Access tests were performed using Kali Linux to ensure the firewall rules were functioning as intended.
- **Reason**: Regular testing ensures that the implemented rules effectively block unauthorized access and that no unintended vulnerabilities exist.

Firewall Devender Turn: ON

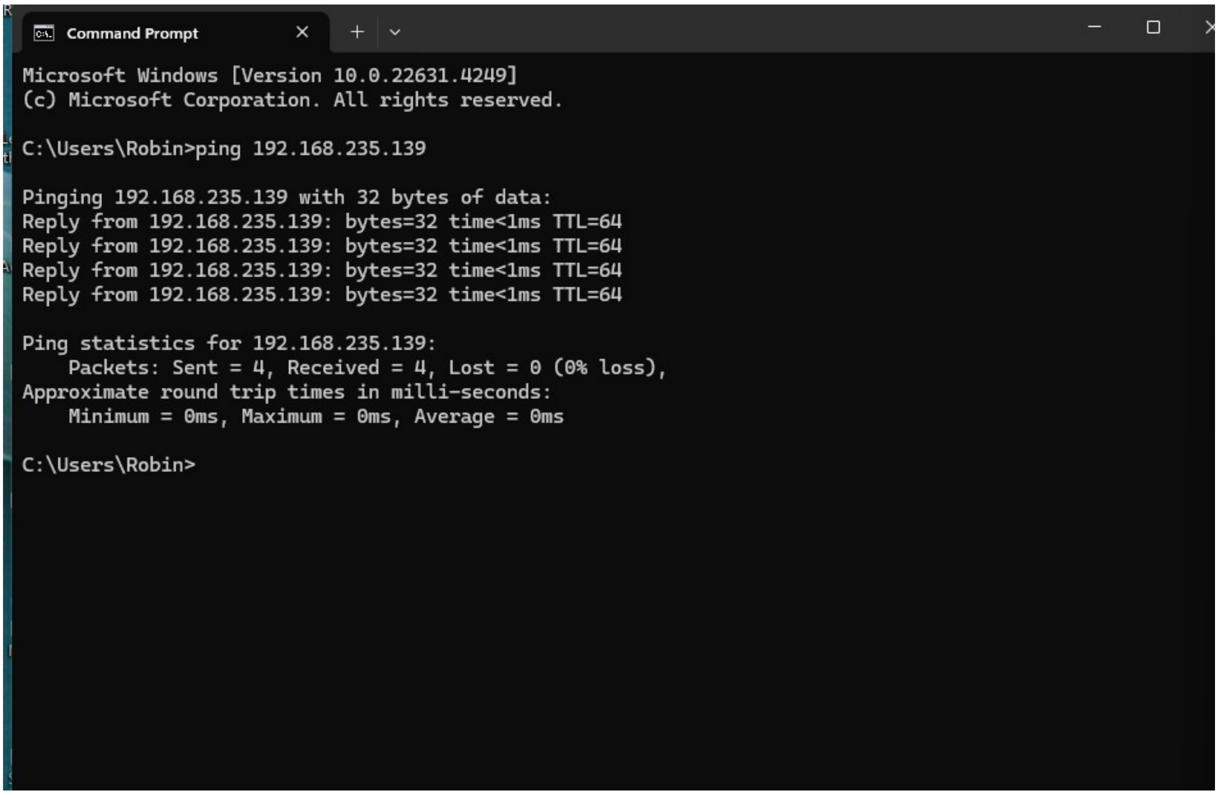


```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ ping 192.168.235.136
PING 192.168.235.136 (192.168.235.136) 56(84) bytes of data.
64 bytes from 192.168.235.136: icmp_seq=1 ttl=128 time=1.26 ms
64 bytes from 192.168.235.136: icmp_seq=2 ttl=128 time=0.521 ms
64 bytes from 192.168.235.136: icmp_seq=3 ttl=128 time=0.484 ms
64 bytes from 192.168.235.136: icmp_seq=4 ttl=128 time=0.504 ms
64 bytes from 192.168.235.136: icmp_seq=5 ttl=128 time=0.796 ms
64 bytes from 192.168.235.136: icmp_seq=6 ttl=128 time=0.551 ms
64 bytes from 192.168.235.136: icmp_seq=7 ttl=128 time=0.644 ms
64 bytes from 192.168.235.136: icmp_seq=8 ttl=128 time=0.697 ms
64 bytes from 192.168.235.136: icmp_seq=9 ttl=128 time=0.621 ms
64 bytes from 192.168.235.136: icmp_seq=10 ttl=128 time=0.650 ms
64 bytes from 192.168.235.136: icmp_seq=11 ttl=128 time=0.743 ms
^C
--- 192.168.235.136 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10198ms
rtt min/avg/max/mdev = 0.484/0.679/1.261/0.207 ms

┌──(kali㉿kali)-[~]
└─$ 
```



```
Microsoft Windows [Version 10.0.22631.4249]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robin>ping 192.168.235.139

Pinging 192.168.235.139 with 32 bytes of data:
Reply from 192.168.235.139: bytes=32 time=1ms TTL=64
Reply from 192.168.235.139: bytes=32 time<1ms TTL=64
Reply from 192.168.235.139: bytes=32 time<1ms TTL=64
Reply from 192.168.235.139: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.235.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Robin>
```

Firewall Devender Turn: OFF



```
Microsoft Windows [Version 10.0.22631.4249]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robin>ping 192.168.235.139

Pinging 192.168.235.139 with 32 bytes of data:
Reply from 192.168.235.139: bytes=32 time<1ms TTL=64
Reply from 192.168.235.139: bytes=32 time<1ms TTL=64
Reply from 192.168.235.139: bytes=32 time<1ms TTL=64
Reply from 192.168.235.139: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.235.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Robin>
```

Monitoring Firewall Activity

- **Action**: Regular monitoring of firewall logs and settings was established.
- **Reason**: Continuous monitoring allows for the identification of any suspicious activity or potential breaches, enabling timely responses to
- security incidents.

Changing Default Passwords

Reason: Changing default passwords mitigates the risk of unauthorized access. Strong, unique passwords are critical for securing accounts against brute-force attacks.

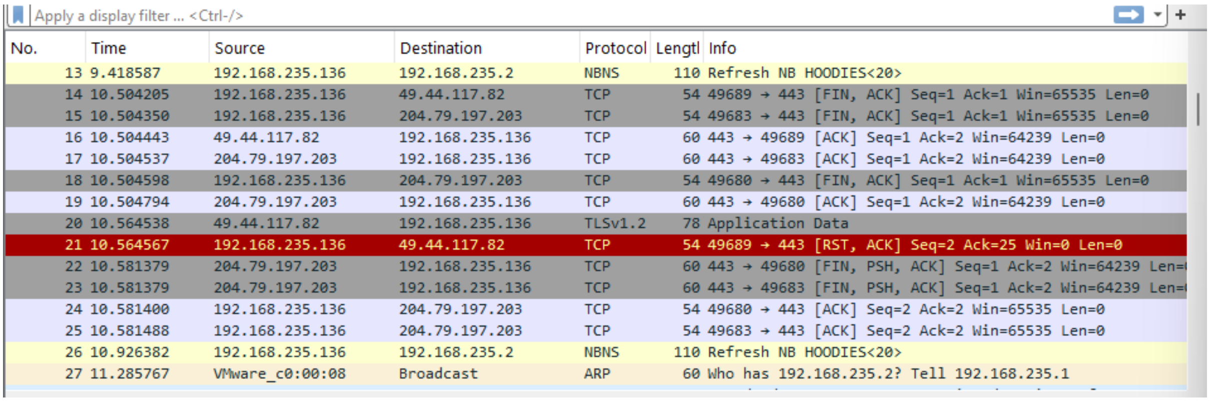
Enabling Network Encryption (WPA2/WPA3)

Reason: Accessing the router settings is necessary to modify the security settings of the wireless network.

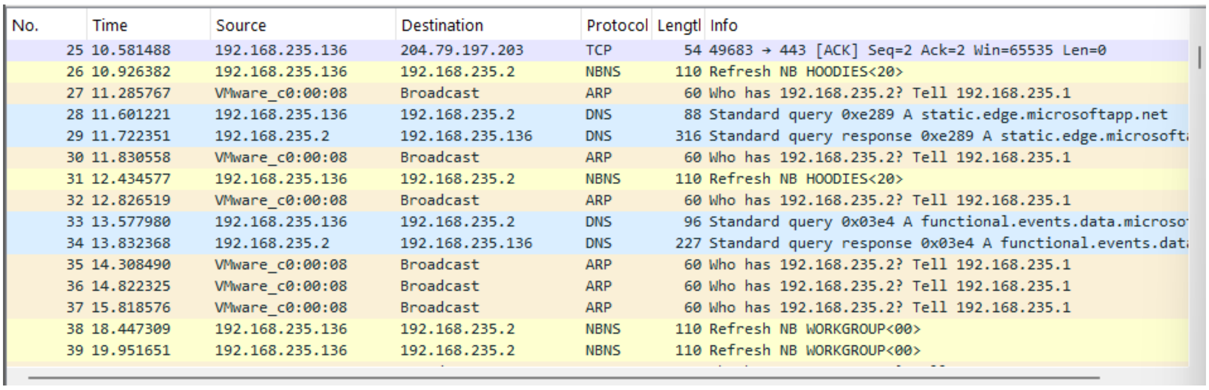
Changing Wi-Fi Security Settings

Reason: Enabling WPA2/WPA3 encryption ensures that data transmitted over the wireless network is secured, protecting it from eavesdropping and unauthorized access.

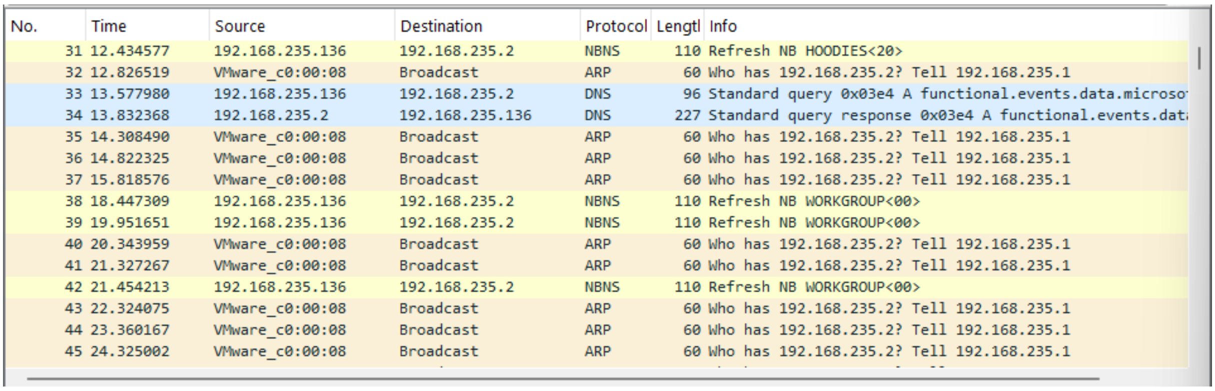
Network Traffic:



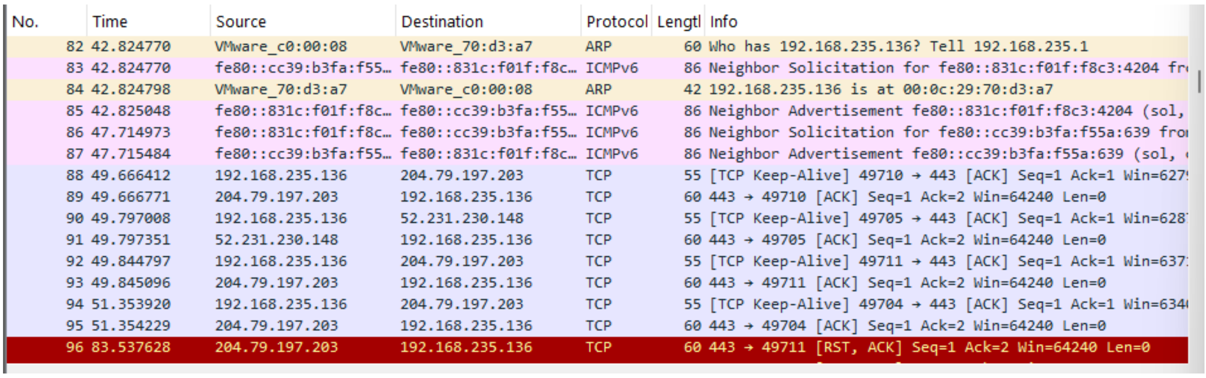
No.	Time	Source	Destination	Protocol	Lengtl	Info
13	9.418587	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB HOODIES<20>
14	10.504205	192.168.235.136	49.44.117.82	TCP	54	49689 → 443 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
15	10.504350	192.168.235.136	204.79.197.203	TCP	54	49683 → 443 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
16	10.504443	49.44.117.82	192.168.235.136	TCP	60	443 → 49689 [ACK] Seq=1 Ack=2 Win=64239 Len=0
17	10.504537	204.79.197.203	192.168.235.136	TCP	60	443 → 49683 [ACK] Seq=1 Ack=2 Win=64239 Len=0
18	10.504598	192.168.235.136	204.79.197.203	TCP	54	49680 → 443 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
19	10.504794	204.79.197.203	192.168.235.136	TCP	60	443 → 49680 [ACK] Seq=1 Ack=2 Win=64239 Len=0
20	10.564538	49.44.117.82	192.168.235.136	TLSv1.2	78	Application Data
21	10.564567	192.168.235.136	49.44.117.82	TCP	54	49689 → 443 [RST, ACK] Seq=2 Ack=25 Win=0 Len=0
22	10.581379	204.79.197.203	192.168.235.136	TCP	60	443 → 49680 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=
23	10.581379	204.79.197.203	192.168.235.136	TCP	60	443 → 49683 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=
24	10.581400	192.168.235.136	204.79.197.203	TCP	54	49680 → 443 [ACK] Seq=2 Ack=2 Win=65535 Len=0
25	10.581488	192.168.235.136	204.79.197.203	TCP	54	49683 → 443 [ACK] Seq=2 Ack=2 Win=65535 Len=0
26	10.926382	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB HOODIES<20>
27	11.285767	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1



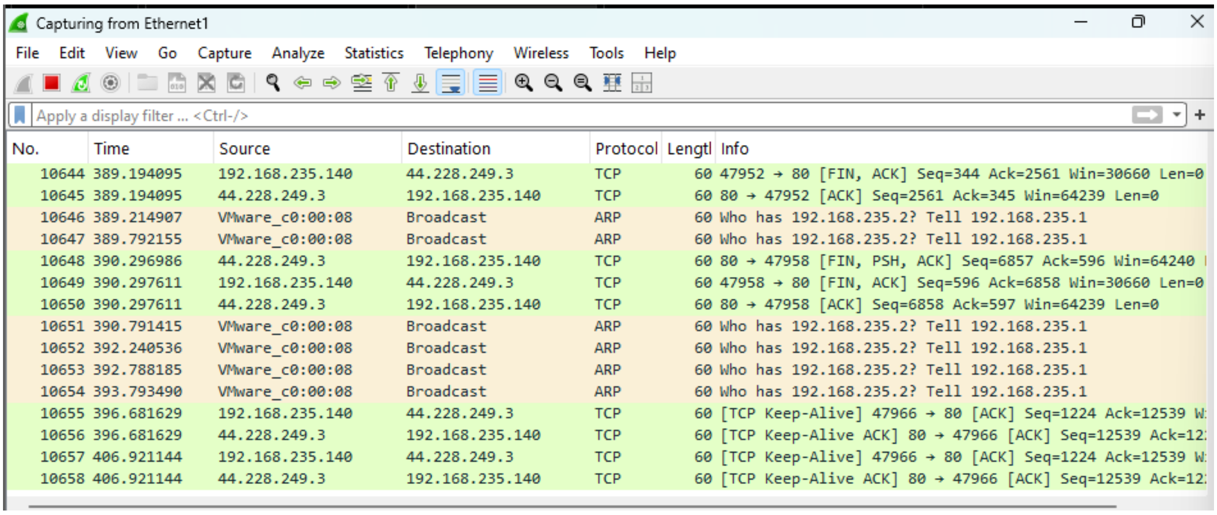
No.	Time	Source	Destination	Protocol	Lengtl	Info
25	10.581488	192.168.235.136	204.79.197.203	TCP	54	49683 → 443 [ACK] Seq=2 Ack=2 Win=65535 Len=0
26	10.926382	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB HOODIES<20>
27	11.285767	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
28	11.601221	192.168.235.136	192.168.235.2	DNS	88	Standard query 0xe289 A static.edge.microsoftapp.net
29	11.722351	192.168.235.2	192.168.235.136	DNS	316	Standard query response 0xe289 A static.edge.microsofta
30	11.830558	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
31	12.434577	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB HOODIES<20>
32	12.826519	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
33	13.577980	192.168.235.136	192.168.235.2	DNS	96	Standard query 0x03e4 A functional.events.data.microso
34	13.832368	192.168.235.2	192.168.235.136	DNS	227	Standard query response 0x03e4 A functional.events.data
35	14.308490	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
36	14.822325	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
37	15.818576	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
38	18.447309	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB WORKGROUP<00>
39	19.951651	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB WORKGROUP<00>



No.	Time	Source	Destination	Protocol	Lengtl	Info
31	12.434577	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB HOODIES<20>
32	12.826519	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
33	13.577980	192.168.235.136	192.168.235.2	DNS	96	Standard query 0x03e4 A functional.events.data.microso
34	13.832368	192.168.235.2	192.168.235.136	DNS	227	Standard query response 0x03e4 A functional.events.data
35	14.308490	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
36	14.822325	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
37	15.818576	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
38	18.447309	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB WORKGROUP<00>
39	19.951651	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB WORKGROUP<00>
40	20.343959	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
41	21.327267	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
42	21.454213	192.168.235.136	192.168.235.2	NBNS	110	Refresh NB WORKGROUP<00>
43	22.324075	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
44	23.360167	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1
45	24.325002	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.235.2? Tell 192.168.235.1

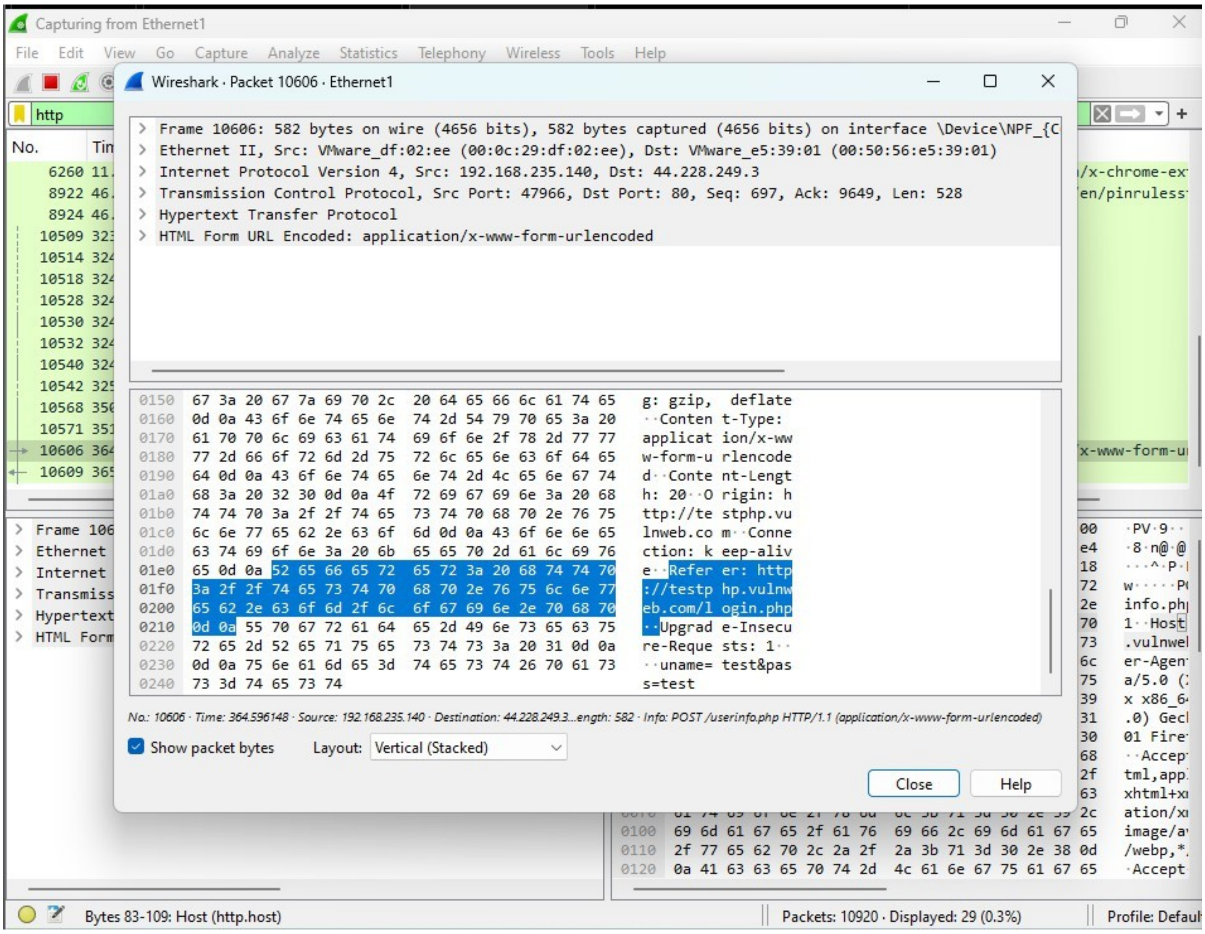


No.	Time	Source	Destination	Protocol	Lengtl	Info
82	42.824770	VMware_c0:00:08	VMware_70:d3:a7	ARP	60	Who has 192.168.235.136? Tell 192.168.235.1
83	42.824770	fe80::cc39:b3fa:f55…	fe80::831c:f01f:f8c…	ICMPv6	86	Neighbor Solicitation for fe80::831c:f01f:f8c3:4204 fr
84	42.824798	VMware_70:d3:a7	VMware_c0:00:08	ARP	42	192.168.235.136 is at 00:0c:29:70:d3:a7
85	42.825048	fe80::831c:f01f:f8c…	fe80::cc39:b3fa:f55…	ICMPv6	86	Neighbor Advertisement fe80::831c:f01f:f8c3:4204 (sol,
86	47.714973	fe80::831c:f01f:f8c…	fe80::cc39:b3fa:f55…	ICMPv6	86	Neighbor Solicitation for fe80::cc39:b3fa:f55a:639 fro
87	47.715484	fe80::cc39:b3fa:f55…	fe80::831c:f01f:f8c…	ICMPv6	86	Neighbor Advertisement fe80::cc39:b3fa:f55a:639 (sol,
88	49.666412	192.168.235.136	204.79.197.203	TCP	55	[TCP Keep-Alive] 49710 → 443 [ACK] Seq=1 Ack=1 Win=627
89	49.666771	204.79.197.203	192.168.235.136	TCP	60	443 → 49710 [ACK] Seq=1 Ack=2 Win=64240 Len=0
90	49.797008	192.168.235.136	52.231.230.148	TCP	55	[TCP Keep-Alive] 49705 → 443 [ACK] Seq=1 Ack=1 Win=628
91	49.797351	52.231.230.148	192.168.235.136	TCP	60	443 → 49705 [ACK] Seq=1 Ack=2 Win=64240 Len=0
92	49.844797	192.168.235.136	204.79.197.203	TCP	55	[TCP Keep-Alive] 49711 → 443 [ACK] Seq=1 Ack=1 Win=637
93	49.845096	204.79.197.203	192.168.235.136	TCP	60	443 → 49711 [ACK] Seq=1 Ack=2 Win=64240 Len=0
94	51.353920	192.168.235.136	204.79.197.203	TCP	55	[TCP Keep-Alive] 49704 → 443 [ACK] Seq=1 Ack=1 Win=634
95	51.354229	204.79.197.203	192.168.235.136	TCP	60	443 → 49704 [ACK] Seq=1 Ack=2 Win=64240 Len=0
96	83.537628	204.79.197.203	192.168.235.136	TCP	60	443 → 49711 [RST, ACK] Seq=1 Ack=2 Win=64240 Len=0



Capturing from Ethernet1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Lengtl Info
10644 389.194095 192.168.235.140  44.228.249.3     TCP      60 47952 → 80 [FIN, ACK] Seq=344 Ack=2561 Win=30660 Len=0
10645 389.194095 44.228.249.3     192.168.235.140  TCP      60 80 → 47952 [ACK] Seq=2561 Ack=345 Win=64239 Len=0
10646 389.214907 VMware_c0:00:08  Broadcast        ARP      60 Who has 192.168.235.2? Tell 192.168.235.1
10647 389.792155 VMware_c0:00:08  Broadcast        ARP      60 Who has 192.168.235.2? Tell 192.168.235.1
10648 390.296986 44.228.249.3     192.168.235.140  TCP      60 80 → 47958 [FIN, PSH, ACK] Seq=6857 Ack=596 Win=64240
10649 390.297611 192.168.235.140  44.228.249.3     TCP      60 47958 → 80 [FIN, ACK] Seq=596 Ack=6858 Win=30660 Len=0
10650 390.297611 44.228.249.3     192.168.235.140  TCP      60 80 → 47958 [ACK] Seq=6858 Ack=597 Win=64239 Len=0
10651 390.791415 VMware_c0:00:08  Broadcast        ARP      60 Who has 192.168.235.2? Tell 192.168.235.1
10652 392.240536 VMware_c0:00:08  Broadcast        ARP      60 Who has 192.168.235.2? Tell 192.168.235.1
10653 392.788185 VMware_c0:00:08  Broadcast        ARP      60 Who has 192.168.235.2? Tell 192.168.235.1
10654 393.793490 VMware_c0:00:08  Broadcast        ARP      60 Who has 192.168.235.2? Tell 192.168.235.1
10655 396.681629 192.168.235.140  44.228.249.3     TCP      60 [TCP Keep-Alive] 47966 → 80 [ACK] Seq=1224 Ack=12539 W
10656 396.681629 44.228.249.3     192.168.235.140  TCP      60 [TCP Keep-Alive ACK] 80 → 47966 [ACK] Seq=12539 Ack=12
10657 406.921144 192.168.235.140  44.228.249.3     TCP      60 [TCP Keep-Alive] 47966 → 80 [ACK] Seq=1224 Ack=12539 W
10658 406.921144 44.228.249.3     192.168.235.140  TCP      60 [TCP Keep-Alive ACK] 80 → 47966 [ACK] Seq=12539 Ack=12
```



Capturing from Ethernet1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 10606 · Ethernet1

```
> Frame 10606: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface \Device\NPF_{C
> Ethernet II, Src: VMware_df:02:ee (00:0c:29:df:02:ee), Dst: VMware_e5:39:01 (00:50:56:e5:39:01)
> Internet Protocol Version 4, Src: 192.168.235.140, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 47966, Dst Port: 80, Seq: 697, Ack: 9649, Len: 528
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0150  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0160  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type:
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
0180  77 2d 66 6f 72 6d 2d 75  72 6c 65 6e 63 6f 64 65   w-form-u rlencode
0190  64 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   d··Conte nt-Lengt
01a0  68 3a 20 32 30 0d 0a 4f  72 69 67 69 6e 3a 20 68   h: 20··O rigin: h
01b0  74 74 70 3a 2f 2f 74 65  73 74 70 68 70 2e 76 75   ttp://te stphp.vu
01c0  6c 6e 77 65 62 2e 63 6f  6d 0d 0a 43 6f 6e 6e 65   lnweb.co m··Conne
01d0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
01e0  65 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   e··Refer er: http
01f0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
0200  65 62 2e 63 6f 6d 2f 6c  6f 67 69 6e 2e 70 68 70   eb.com/l ogin.php
0210  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0220  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
0230  0d 0a 75 6e 61 6d 65 3d  74 65 73 74 26 70 61 73   ··uname= test&pas
0240  73 3d 74 65 73 74                                  s=test
```

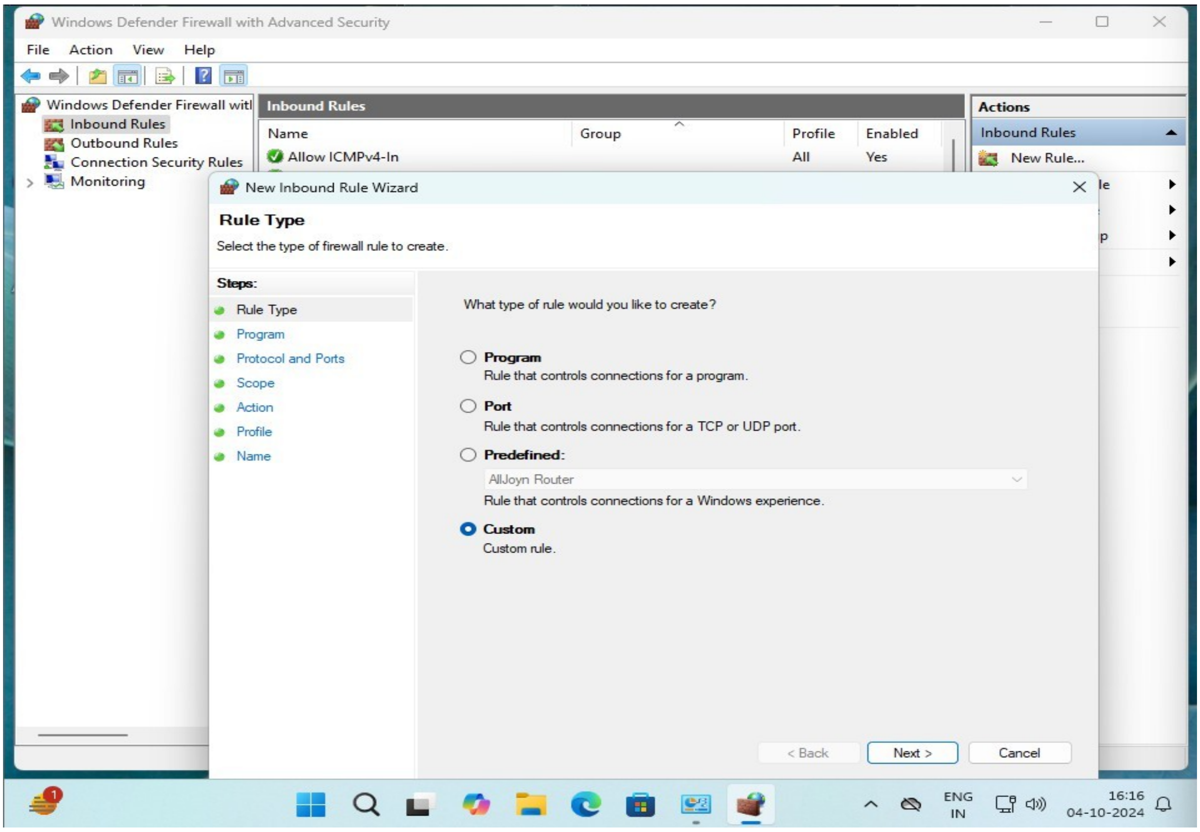
No.: 10606 · Time: 364.596148 · Source: 192.168.235.140 · Destination: 44.228.249.3...ength: 582 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

☑ Show packet bytes Layout: Vertical (Stacked)

Bytes 83-109: Host (http.host) Packets: 10920 · Displayed: 29 (0.3%) Profile: Defaul

Implementing Security Measures

Configure Rule Type



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

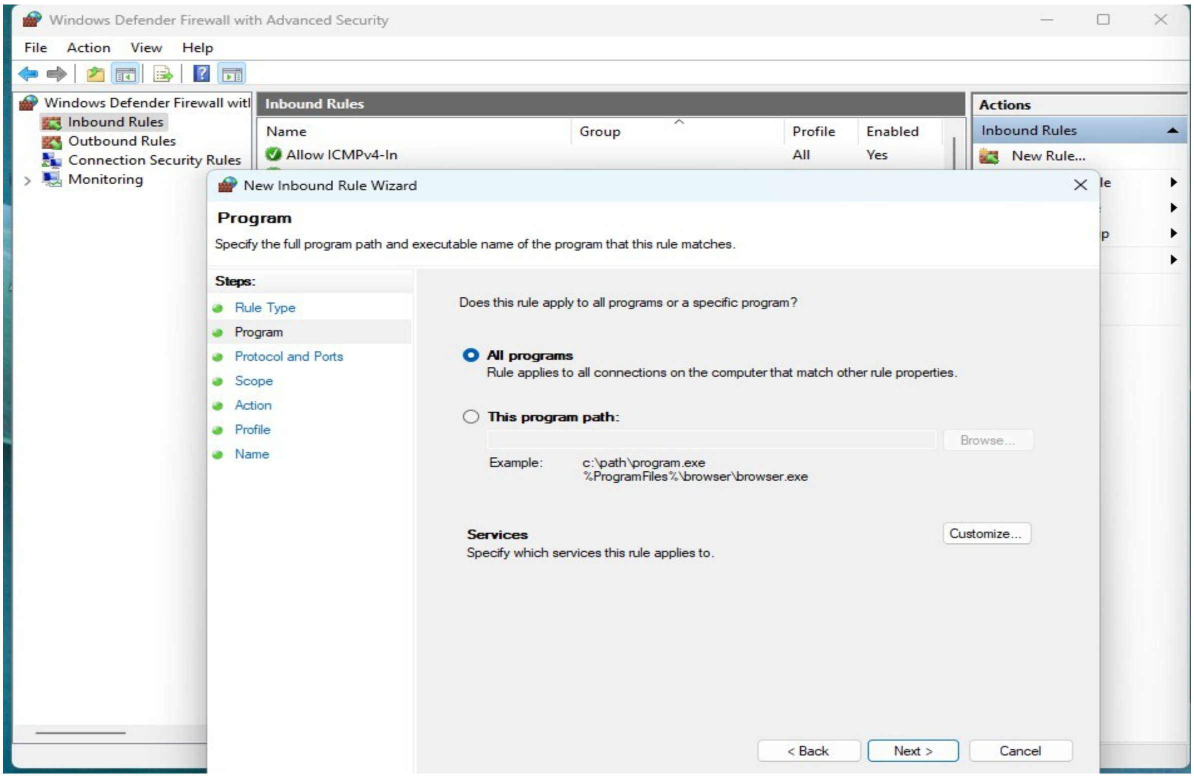
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

< Back | Next > | Cancel

Specify Program


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled
Allow ICMPv4-In All Yes
Actions
Inbound Rules
New Rule...

New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

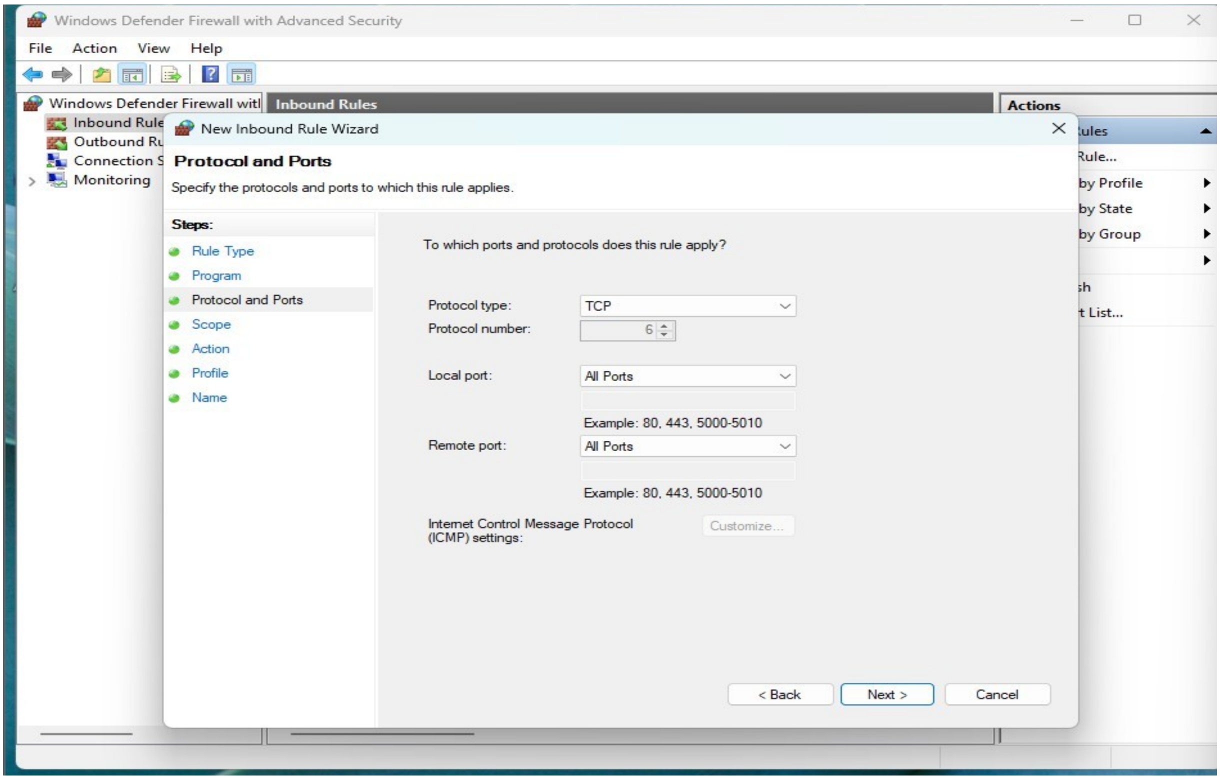
● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.
Customize...

< Back | Next > | Cancel

Configure Protocol and Ports



Protocol and Ports

Specify the protocols and ports to which this rule applies.

To which ports and protocols does this rule apply?

Protocol type: TCP

Protocol number: 6

Local port: All Ports

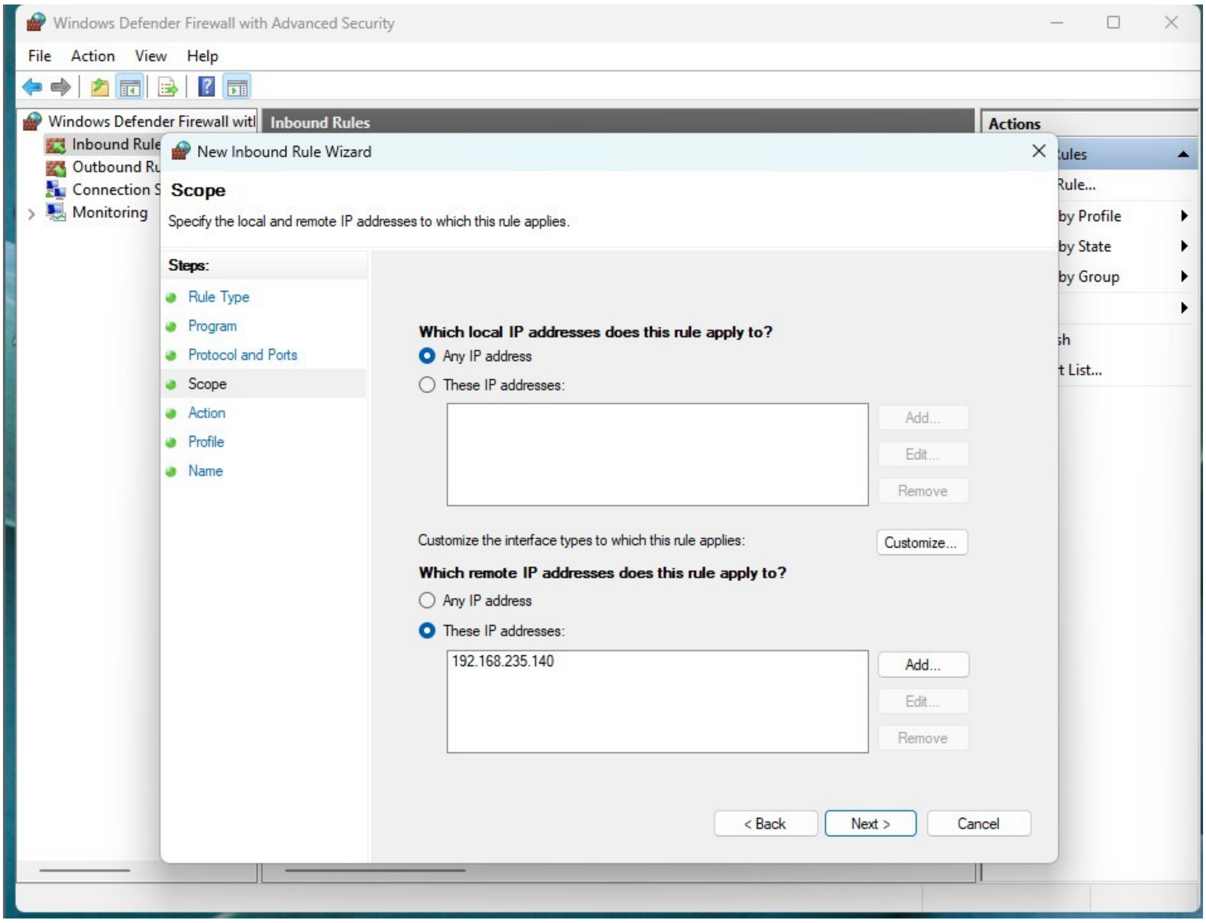
Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

Configure Scope



Scope

Specify the local and remote IP addresses to which this rule applies.

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

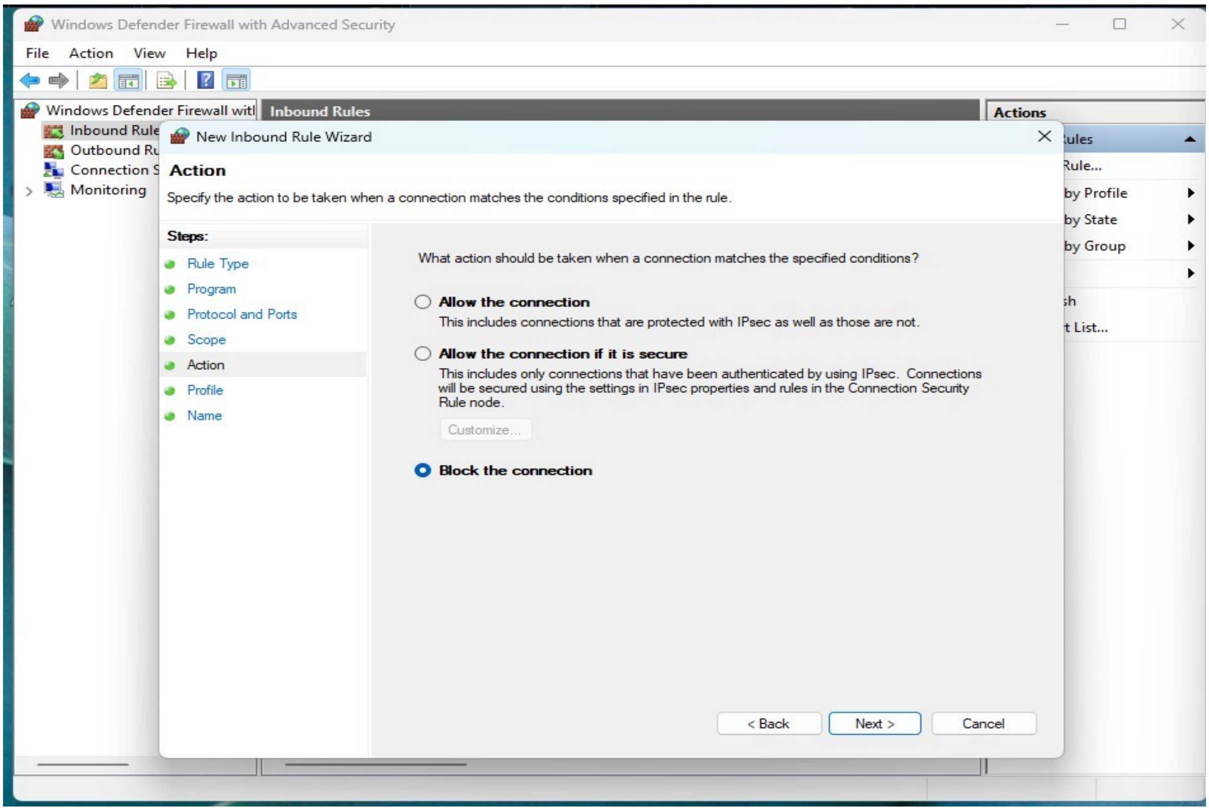
Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

192.168.235.140

Configure Action



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

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

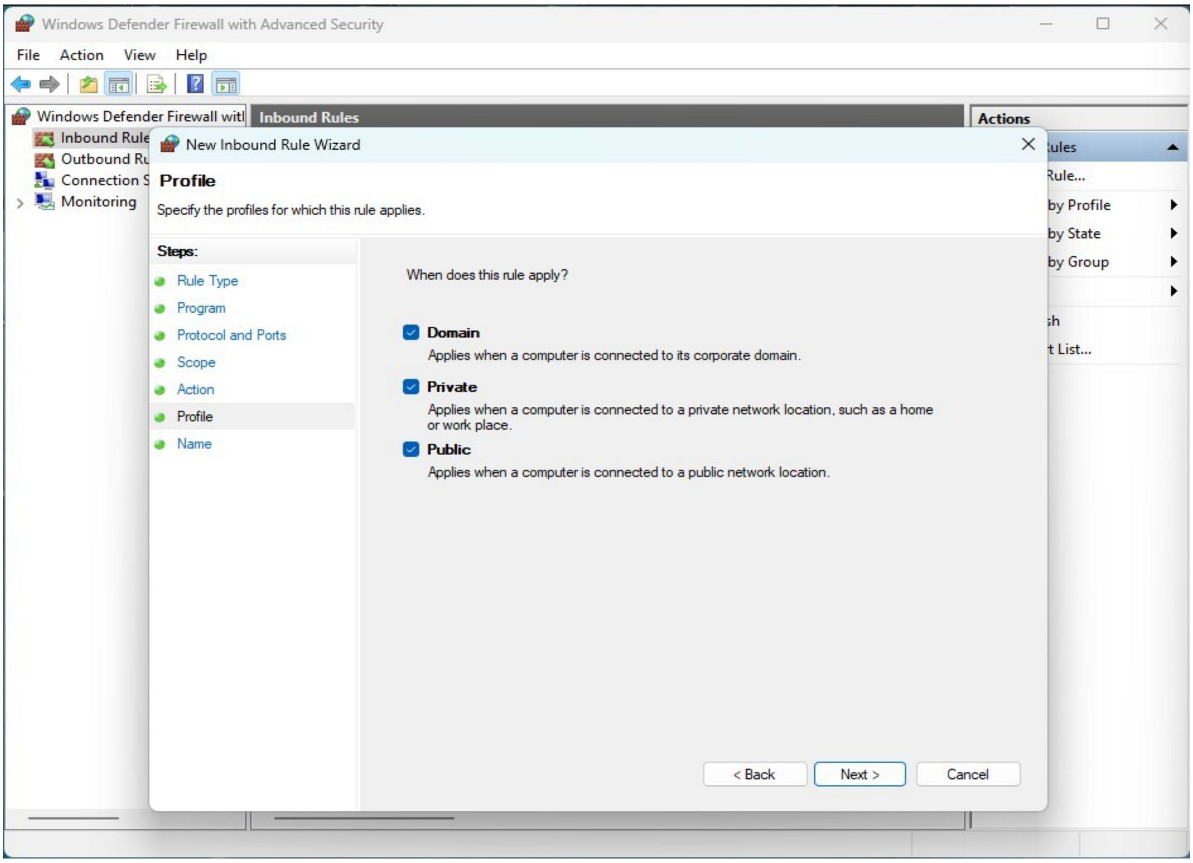
What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

Configure Profile



Profile

Specify the profiles for which this rule applies.

Steps:

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

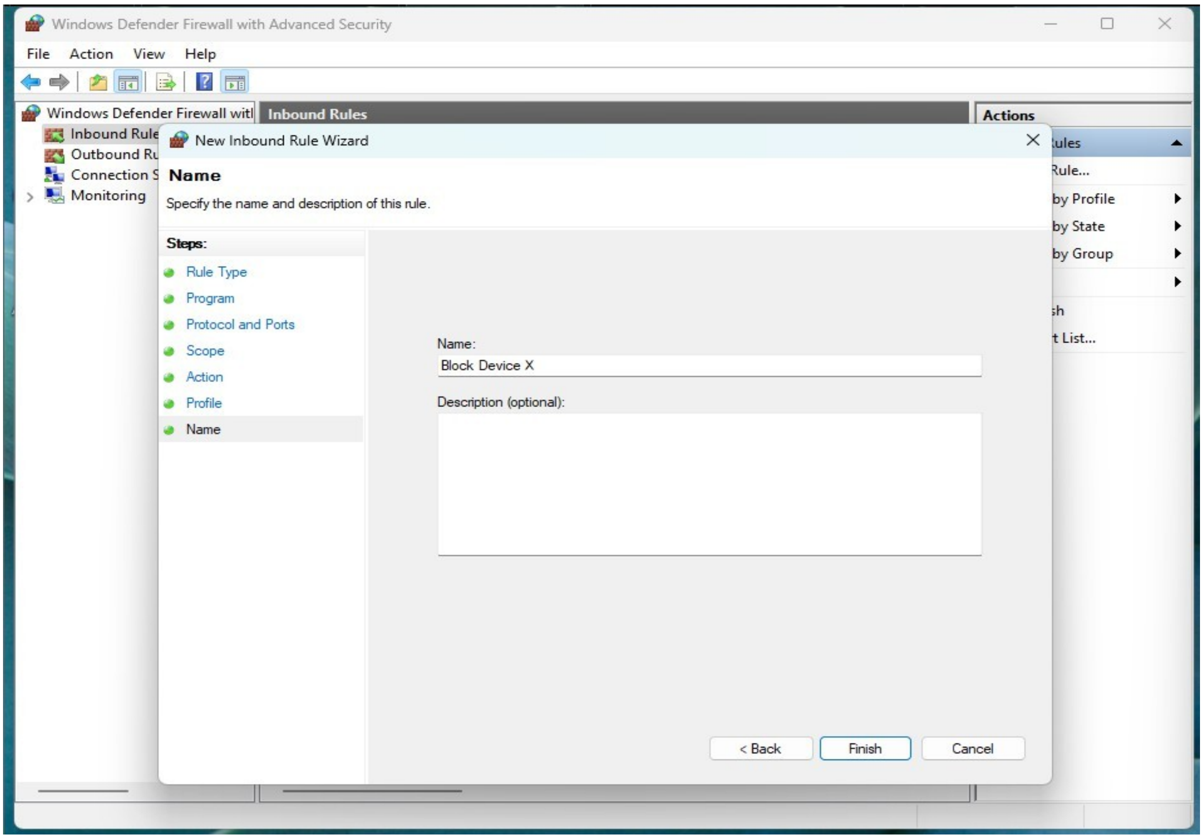
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

Name the Rule



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

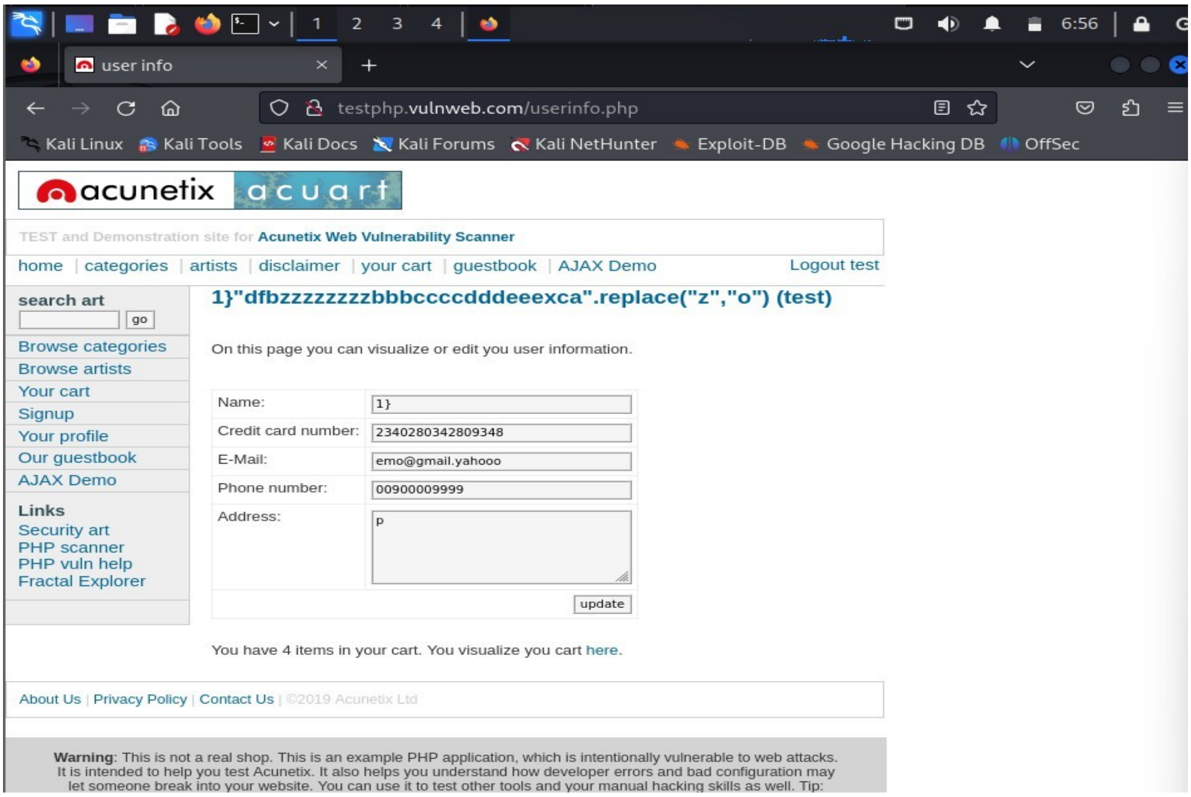
Steps:

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

Name: Block Device X

Description (optional):

After Blocking



testphp.vulnweb.com/userinfo.php

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

1}"dfbzzzzzzzzbbbccccdddeeexca".replace("z","o") (test)

On this page you can visualize or edit you user information.

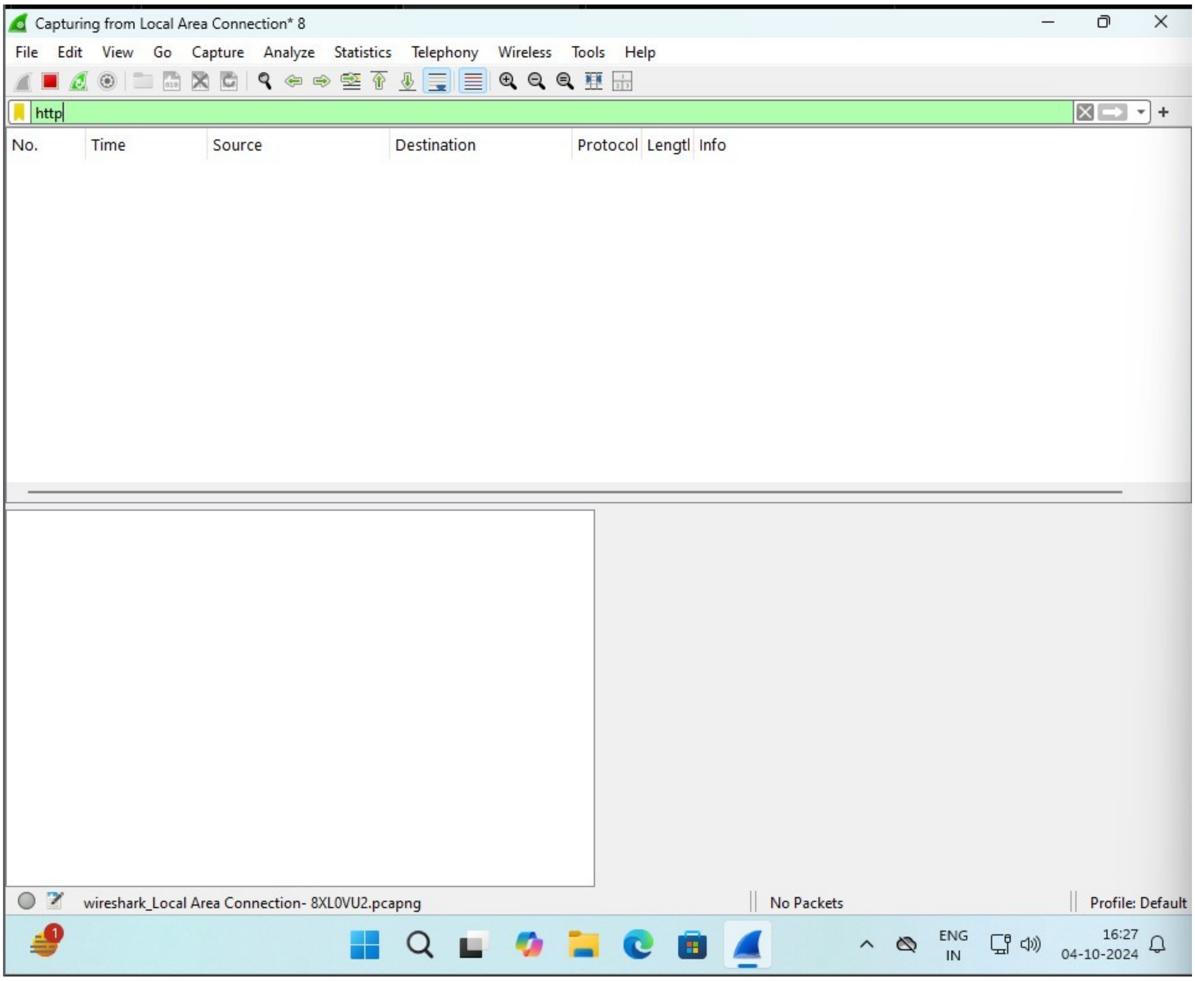
Name:	1}
Credit card number:	2340280342809348
E-Mail:	emo@gmail.yahooo
Phone number:	00900009999
Address:	p

You have 4 items in your cart. You visualize you cart here.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip:

Not capturing Any Packet



Capturing from Local Area Connection* 8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Lengtl	Info

wireshark_Local Area Connection- 8XL0VU2.pcapng

No Packets

Profile: Default

Basic Security Measures and Their Role in Network Protection

Network security is paramount in today's digital age, where threats are evolving rapidly. Implementing basic security measures can significantly enhance the protection of your network.

Some of the key measures and how they contribute to network security:

1. Strong Passwords:

- **Why it matters:** Weak passwords are a common entry point for unauthorized access.
- **How it helps:** Using complex, unique passwords with a combination of uppercase and lowercase letters, numbers, and symbols makes it significantly harder for attackers to guess or brute-force them.

2. Regular Updates:

- **Why it matters:** Software vulnerabilities are constantly discovered and patched.
- **How it helps:** Keeping operating systems, applications, and firmware up- to-date ensures that known security holes are addressed, reducing the risk of exploitation.

3. Firewall:

- **Why it matters:** A firewall acts as a gatekeeper, controlling network traffic.
- **How it helps:** By filtering incoming and outgoing data, a firewall can block malicious attempts to access your network. It can also restrict access to certain websites or services.

4. Antivirus and Anti-Malware:

- **Why it matters:** Malware, such as viruses, worms, and ransomware, can cause significant damage to a network.

- **How it helps:** Antivirus and anti-malware software scans files and network traffic for malicious code, detecting and removing threats before they can harm your system.

5. Two-Factor Authentication (2FA):

- **Why it matters:** Even if a password is compromised, 2FA adds an extra layer of protection.
- **How it helps:** 2FA requires a second form of verification, such as a code sent to a mobile device or a security token, in addition to a password. This makes it much more difficult for unauthorized users to gain access.

6. Employee Training:

- **Why it matters:** Human error is a significant security risk.
- **How it helps:** Educating employees about security best practices, such as recognizing phishing attempts and avoiding clicking on suspicious links, can help prevent accidental breaches.

7. Network Segmentation:

- **Why it matters:** Isolating sensitive systems and data can limit the impact of a breach.
- **How it helps:** By dividing a network into smaller, segmented networks, it becomes more difficult for an attacker to move laterally and access critical resources.

Additional Security Measures for Larger, More Complex Networks.

As networks grow in size and complexity, the need for more robust security measures becomes increasingly important.

Here are some additional considerations:

1. Intrusion Detection and Prevention Systems (IDPS):

- **Purpose:** Detect and prevent unauthorized access or malicious activity within a network.
- **How it helps:** IDPS systems monitor network traffic for suspicious patterns and anomalies, alerting administrators to potential threats in real-time.

2. Data Loss Prevention (DLP):

- **Purpose:** Protect sensitive data from unauthorized access, use, or disclosure.
- **How it helps:** DLP solutions monitor data flows within a network, identifying and blocking attempts to transfer or copy confidential information outside the organization.

3. Security Information and Event Management (SIEM):

- **Purpose:** Centralize and correlate security events from various sources.
- **How it helps:** SIEM systems provide a comprehensive view of network activity, enabling administrators to identify security threats, investigate incidents, and respond effectively.

4. Network Access Control (NAC):

- **Purpose:** Enforce network access policies based on user identity, device health, and network location.
- **How it helps:** NAC solutions ensure that only authorized devices and users can access the network, reducing the risk of unauthorized access and malware infections.

5. Vulnerability Scanning:

- **Purpose:** Identify and assess vulnerabilities in network devices and applications.
- **How it helps:** Vulnerability scanning tools help organizations prioritize remediation efforts and reduce the risk of exploitation.

6. Security Auditing and Penetration Testing:

- **Purpose:** Evaluate the effectiveness of security measures and identify potential weaknesses.
- **How it helps:** Regular security audits and penetration testing can help organizations uncover vulnerabilities that may have been missed by other security controls.

7. Incident Response Planning:

- **Purpose:** Prepare for and respond to security incidents in a timely and effective manner.
- **How it helps:** A well-defined incident response plan can help minimize the impact of a security breach and restore normal operations quickly.

8. Cloud Security:

- **Purpose:** Protect data and applications hosted in the cloud.
- **How it helps:** Cloud security measures, such as encryption, access controls, and vulnerability management, are essential for safeguarding sensitive information stored in cloud environments.

Challenge:

- Initially, it was overwhelming to grasp the vast array of network threats such as viruses, worms, trojans, and phishing attacks.
- Configuring a virtual lab with a router and connected devices was initially complex, particularly ensuring all components communicated effectively.
- Understanding the various firewall settings and rules required to block unauthorized access was difficult.
- Interpreting the data captured by Wireshark was initially confusing due to the volume and complexity of network traffic.
- Differentiating between normal and suspicious traffic was challenging, given the diverse nature of network activity.
- Considering additional security measures for larger networks and educating others on network security was challenging due to the broader scope.

Overcome:

- I tackled this by breaking down the research into manageable sections, f ocusing on one threat at a time. I used reputable sources like cybersecuri ty blogs, academic papers, and official documentation to gain a clear und erstanding of each threat.
- I followed step-by-step guides and tutorials on setting up virtual networks. When I encountered issues, I sought help from online forums and community support, which provided solutions and best practices.
- I referred to detailed documentation and online resources specific to Windows Defender Firewall. Experimenting with different configurations and observing their effects helped solidify my understanding.
- I used online tutorials and guides to understand the basics of Wireshark. By focusing on identifying common protocols (like HTTP and DNS) and gradually moving to more complex analyses, I improved my traffic analysis skills.
- I read case studies and examples of malicious traffic patterns. By

compari ng these examples with my captured data, I learned to spot anomalies th at might indicate a security threat.

Here's a short paragraph on how to educate others about network security:

I would use clear, relatable examples that highlight the potential consequences of neglecting online safety.

For instance, I could explain how a compromised password can lead to identity theft or financial loss. Additionally, I would emphasize the importance of practicing safe browsing habits, such as avoiding suspicious links and being cautious about sharing personal information online. By using simple language and real-world scenarios, I aim to empower individuals to take proactive steps to protect themselves and their digital assets.