Name : Patel Dhruv Nirmalkumar
Email : dhruvpatel.00700@gmail.com
Phone : 9426176903
Task : 10

Firewall Concepts and Principles

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predefined rules.
In Windows, this is handled by **Windows Defender Firewall with Advanced Security (WFAS)**.
WFAS is a **stateful, host-based firewall**.

Core Concepts

Concept	Description
Stateful Filtering	WFAS tracks active connections. If an outbound connection is allowed, the related inbound response traffic is automatically permitted. No extra inbound rule is needed.
Network Profiles	Windows Firewall supports **Domain**, **Private**, and **Public** profiles. Each profile can have different rules depending on the network environment.
Inbound / Outbound Rules	Inbound rules control traffic coming to the system. Outbound rules control traffic leaving the system. By default, outbound traffic is allowed and inbound traffic is blocked unless explicitly permitted.

Firewall Configuration and Rules

The firewall is configured to allow only required inbound services while keeping all other inbound traffic blocked by default.

Configuration Using PowerShell

Action	PowerShell Command	Purpose
Allow SSH (Port 22)	New-NetFirewallRule -DisplayName "Allow SSH Inbound" -Direction Inbound -LocalPort 22 -Protocol TCP -Action Allow	Enables secure remote administration
Allow HTTP (Port 80)	New-NetFirewallRule -DisplayName "Allow HTTP Inbound" -Direction Inbound -LocalPort 80 -Protocol TCP -Action Allow	Allows inbound web traffic
Deny Other Inbound Traffic	*(Default policy)*	Blocks all unsolicited inbound connections

---

Configuration Using netsh advfirewall

Allow SSH (Port 22)

netsh advfirewall firewall add rule name="Allow SSH Inbound" dir=in action=allow protocol=TCP localport=22

Allow HTTP (Port 80)

netsh advfirewall firewall add rule name="Allow HTTP Inbound" dir=in action=allow protocol=TCP localport=80

Final Ruleset Summary

Rule Name	Direction	Protocol	Local Port	Action	Purpose
Allow SSH Inbound	Inbound	TCP	22	Allow	Remote Management
Allow HTTP Inbound	Inbound	TCP	80	Allow	Web Server Access
Default Inbound Policy	Inbound	All	All	Block	Deny all other unsolicited traffic

---

Testing, Logging, and IP Blocking

Test Connectivity

Test Scenario	Tool	Expected Result
Allowed Port (80)	Test-NetConnection -Port 80 or telnet localhost 80	Connection succeeds or is refused (if no service), but does not time out
Denied Port (8080)	Test-NetConnection -Port 8080 or telnet localhost 8080	Connection fails or times out

Enable and Observe Firewall Logs

Firewall logging is disabled by default and must be enabled manually.

PowerShell Command to Enable Logging

```
Set-NetFirewallProfile `
 -Profile Public `
 -LogFileName "%systemroot%\system32\LogFiles\Firewall\pfirewall.log" `
 -LogBlocked True `
 -LogSuccessful True
```

Log Details

- Log file location: C:\Windows\System32\LogFiles\Firewall\pfirewall.log
- Blocked traffic entries: DROP
- Allowed traffic entries: ACCEPT

Block a Malicious IP Address

To block a known malicious IP (example: 192.0.2.1), create a specific inbound block rule.

```
New-NetFirewallRule `
 -DisplayName "Block Malicious IP 192.0.2.1" `
 -Direction Inbound `
 -Action Block `
 -RemoteAddress 192.0.2.1
```

Note:
WFAS prioritizes block rules over allow rules, so the traffic is dropped immediately.

Documentation and Impact Explanation

Rule Documentation

This document provides complete firewall documentation, including:

- Firewall concepts and principles
- PowerShell and netsh configuration commands
- Connectivity testing procedures
- Firewall logging configuration
- Malicious IP blocking techniques

Impact Analysis

Impact Area	Description
Security Posture	A strong default-deny inbound policy significantly reduces the attack surface. Only SSH and HTTP are exposed.
Operational Efficiency	Stateful filtering allows normal outbound activity without disruption while enforcing strict inbound control.
Threat Intelligence	Firewall logs help detect scanning attempts and suspicious traffic patterns for proactive defense.
System Management	PowerShell-based rule management enables quick response to new security threats and operational needs.
