# *IT Security (420-F30-HR)*

# *Lab 08 – Endpoint Security*

Date assigned: Tuesday, March 25

Date Due: Friday, March 28, 8am

**Objectives:**

Learn:

1. Understand Endpoint Security concerns and vectors
2. Endpoint Security Defenses and Counter measures

# Microsoft Defender for Endpoint

## Research Microsoft recommendations on securing Windows endpoints Read [this](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide)

## What is Defender for Endpoint? What devices does it protect?

## Microsoft Defender for Endpoint is an endpoint security platform designed to prevent, detect, investigate, and respond to threats. It provides threat and vulnerability management, attack surface reduction, endpoint detection and response (EDR) and automated investigation/remediation.

## What is the asset discovery? Why is this done and how frequently? What is an “unmanaged” device?

Asset discovery is the process of identifying all devices connected to a network. It ensures visibility over all endpoints to detect potential threats or gaps in coverage. This is done continuously or at regular intervals. An unmanaged device is a device connected to the network, but it is not enrolled in an endpoint management system – meaning it is not being monitored, controlled, or protected.

## What is Attack Surface Reduction (ASR)? Provide some example of ASR behaviours. What of the NIST CSF functions does this map onto?

Attack Surface Reduction (ASR) is a feature that minimizes the paths attackers can use to gain entry or move laterally within a system.

Examples include:

* Blocking Office apps from creating child processes
* Blocking untrusted scripts or executables from running
* Preventing credential stealing by blocking credential dumping behavior. ASR maps onto the "Protect" function of the NIST Cybersecurity Framework (CSF)

## What is the EDR (Endpoint and Detection Response) feature? Which of the NIST CSF functions does this map onto?

EDR is a cybersecurity technology that continuously monitors endpoints for evidence of threats and performs automatic actions to help mitigate them.

Detect & response

## Explain the AI features used in to investigate and fix things at scale.

Automatically analyzing alerts and correlating incidents

Running automated playbooks to contain or remediate threats.

Providing recommendations and taking actions (e.g., isolating devices or removing malware)

These features allow large-scale, rapid response without requiring constant manual intervention.

# Microsoft Enterprise-wide DLP

As part of Microsoft 365 suite:

## What is Data Loss Prevention (DLP) and how does it work? ([link](https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp))

DLP detects sensitive items by using deep content analysis. It prevents unintentional or unauthorized sharing of sensitive information. It works by scanning content for pattern or types of data that is sensitive and enforces policies such as warnings, blocking, or encrypting the data before it leaves the org.

## What are some examples of sensitive information that a DLP can scan for?

* Credit cards
* SIN
* Health records
* Bank account info
* Passport or driver license numbers
* Custom keywords

## What are some examples of possible responses the DLP can do once triggered?

* Show a warning to the user
* Block the content from being shared
* Report the incident
* Auto-encrypta the document or email
* Log the activity for auditing

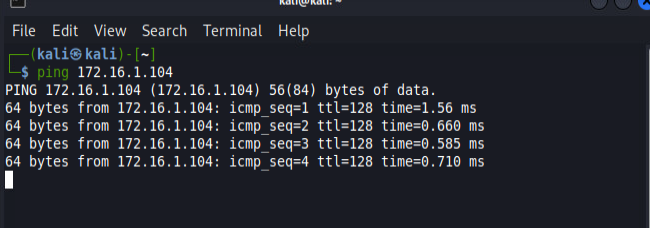
## Where are some possible locations for DLP policies to be applied?

* Exchange Online (emails)
* SharePoint Online (documents)
* OneDrive for Business
* Microsoft Teams
* Endpoint devices (Windows, macOS)

# Windows Host Firewall

## In the VDI environment. Startup configuration1, all machines.

## From Kalibox, ping the WinServerBox.

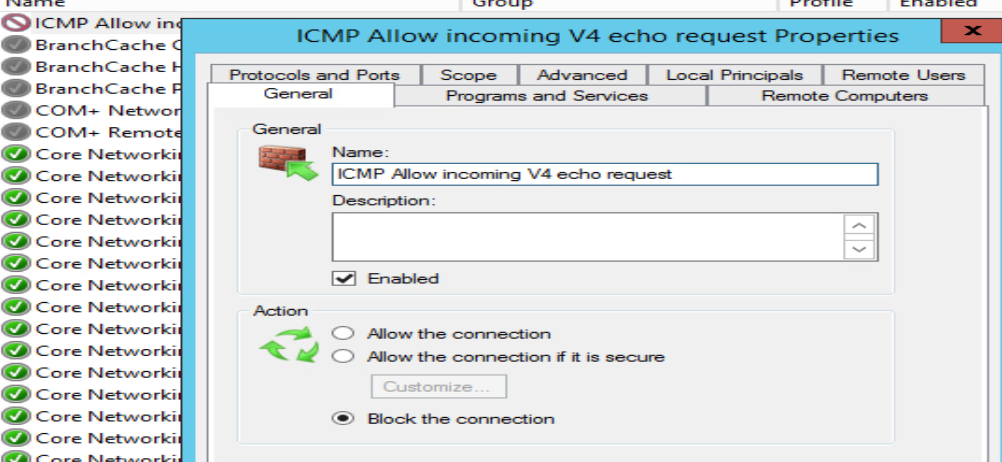


## Log onto the WinServerBox. Open the Windows Firewall with Advanced Security tool. Turn on the firewall for the private and public profile. This makes sure that the firewall is running, even on public or private networks.

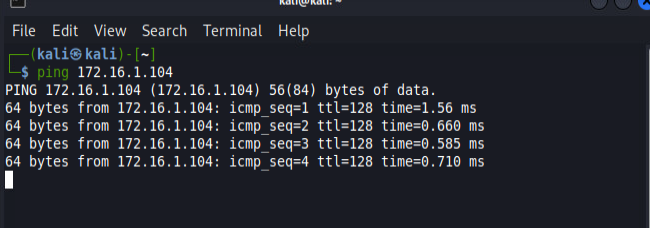
## A screenshot of a computer AI-generated content may be incorrect.

## Change the firewall rule to not respond to pings (ICMP Echo, inbound rule).

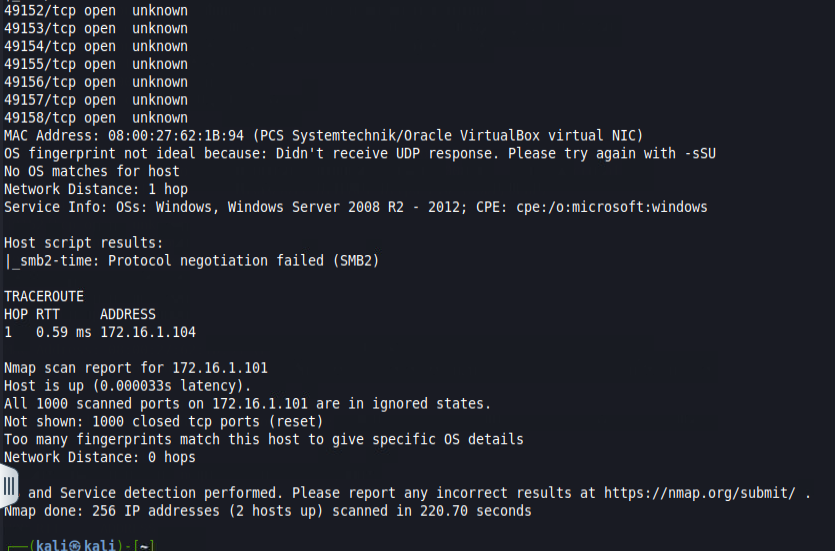
Hint: ping is an ICMP Echo request.



## Ping WinServerBox from KaliBox



## From KaliBox run “nmap -A 172.16.1.0/24”. Is WinServerBox discoverable?



## Change the rule to allow pings on WinServerBox. Confirm the pings work.

## 

## What’s the pros vs cons of blocking the pings?

Pros:

* Reduces visibility to attackers performing network reconnaissance
* Helps mitigate basic scanning tools (e.g., ping, nmap)

Cons:

* Can interfere with legitimate troubleshooting
* May cause false assumptions that a machine is offline

**Marking Scheme**

|  |  |
| --- | --- |
|  | **Out of** |
|  |  |
| **Part A: Defender for Endpoint** |  |
| What | 2 |
| Asset Discovery | 2 |
| ASR | 2 |
| EDR | 2 |
| AI | 2 |
|  |  |
| **Part B: DLP** |  |
| Def’n explanation | 4 |
| Info examples | 2 |
| Possible responses | 5 |
| Locations | 4 |
|  |  |
| **Part C: Host Firewall** |  |
| Ping works | 2 |
| Firewall started and configured | 2 |
| No more pings | 2 |
| Nmap observation | 2 |
| Restore ping function | 2 |
| conclusion | 2 |
|  |  |
| **Crossword** | 10 |