Name: Sudharshiya Ganesan

Student Id: 20232004

Course: MCA1 Cyber technician

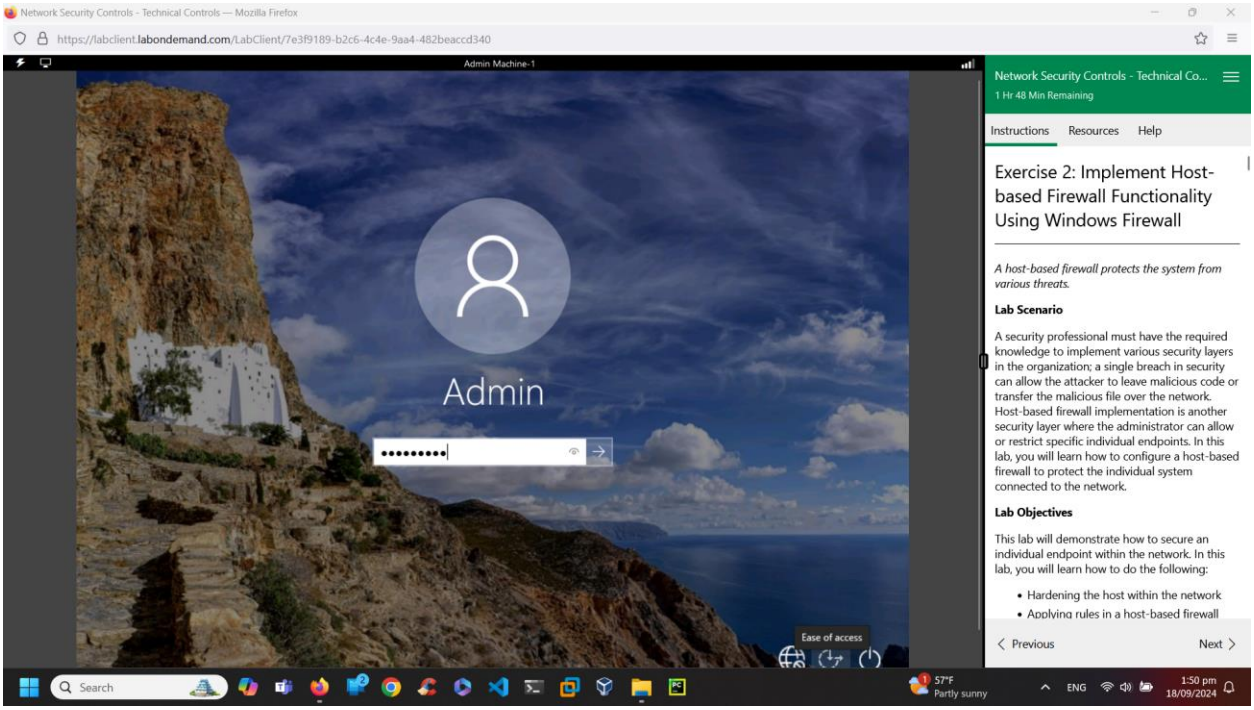
1. **Ilab Module no. and name:** 7. Network Security controls- Technical controls

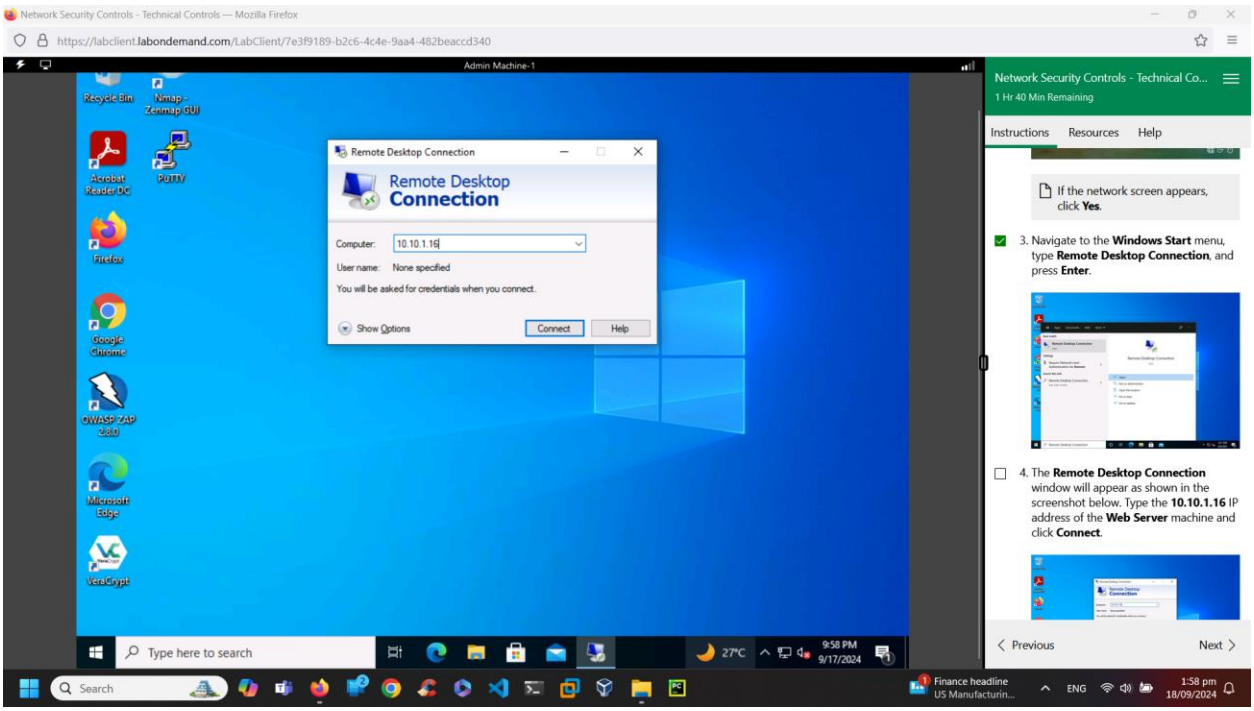
   Exercise no. and name: 2, Implement Host-based Firewall Functionality Using Windows Firewall

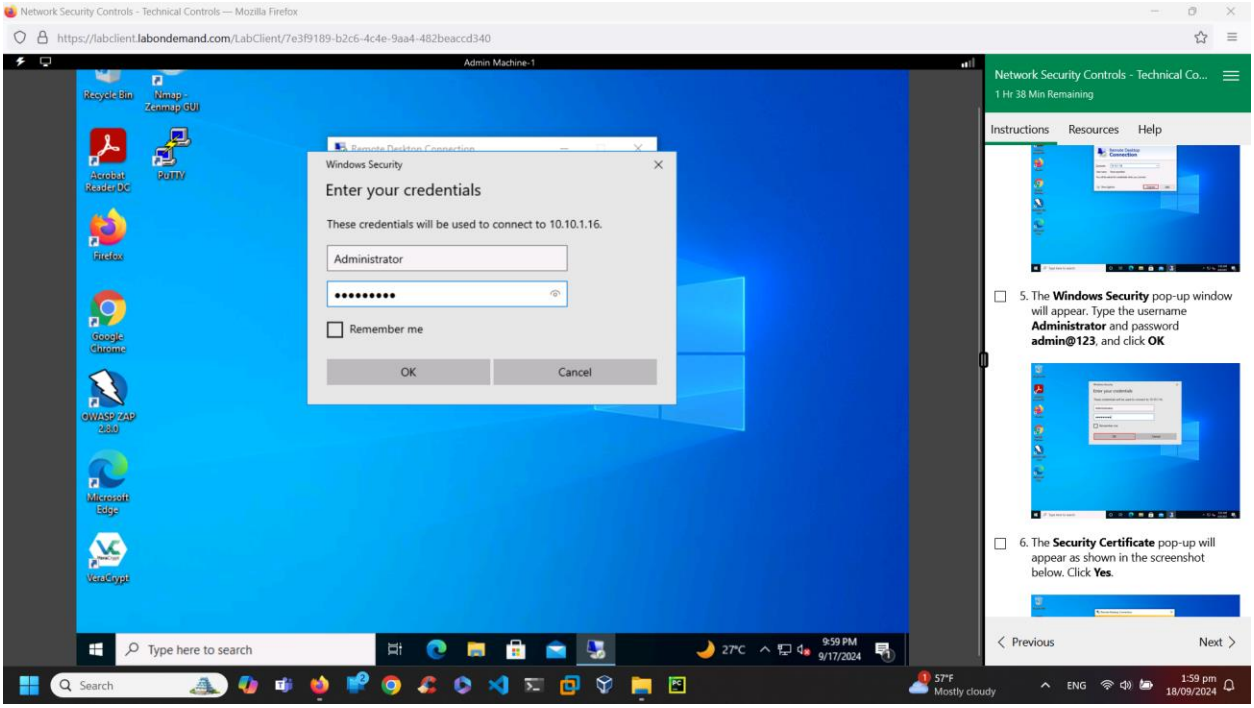
   Performed Date: 18/09/2024

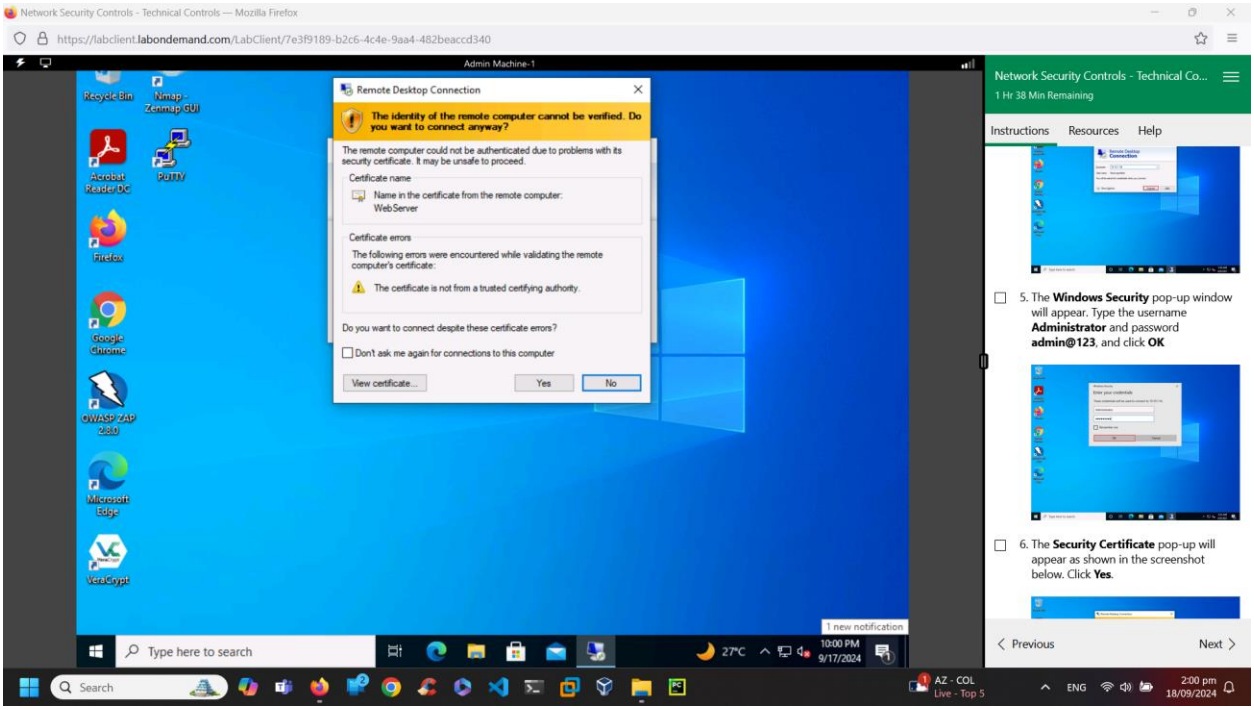
Summary:

This lab demonstrates the use of Remote Desktop connection by entering IP address of Web Server to establish the connection from Admin Machine1 to Web Server. It also asks for enter credentials which authenticate and authorize to make a remote access. If you want to stop RDP access. Go to control panel-system and security-Advanced security to set the inbound rules. Here RDP and FTP services were blocked to restrict remote access from other devices.




Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Recycle Bin
Nmap - Zenmap GUI
Acrobat Reader DC
PuTTY
Firefox
Google Chrome
OWASP ZAP 2.8.0
Microsoft Edge
VeraCrypt
Remote Desktop Connection
Remote Desktop Connection
Computer: 10.10.1.16
User name: None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help
Type here to search
27°C
9:58 PM
9/17/2024
Search
Finance headline
US Manufacturin...
ENG
1:58 pm
18/09/2024
Network Security Controls - Technical Co...
1 Hr 40 Min Remaining
Instructions
Resources
Help
If the network screen appears, click Yes.
3. Navigate to the Windows Start menu, type Remote Desktop Connection, and press Enter.
4. The Remote Desktop Connection window will appear as shown in the screenshot below. Type the 10.10.1.16 IP address of the Web Server machine and click Connect.
Previous
Next


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Windows Security
Enter your credentials
These credentials will be used to connect to 10.10.1.16.
Administrator
Remember me
OK
Cancel
Network Security Controls - Technical Co...
1 Hr 38 Min Remaining
Instructions
Resources
Help
5. The Windows Security pop-up window will appear. Type the username Administrator and password admin@123, and click OK.
6. The Security Certificate pop-up will appear as shown in the screenshot below. Click Yes.
Previous
Next


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
WebServer
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
Network Security Controls - Technical Co...
1 Hr 38 Min Remaining
Instructions
Resources
Help
5. The Windows Security pop-up window will appear. Type the username Administrator and password admin@123, and click OK.
6. The Security Certificate pop-up will appear as shown in the screenshot below. Click Yes.
Previous
Next

Network Security Controls - Technical Controls — Mozilla Firefox

https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340

Web Server

Control Panel

Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
View event logs

Network and Internet
View network status and tasks

Hardware
View devices and printers
Add a device

Programs
Uninstall a program
Turn Windows features on or off

User Accounts
Change account type

Appearance and Personalization
Change the theme

Clock, Language, and Region
Add a language
Change input methods
Set the time and date
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

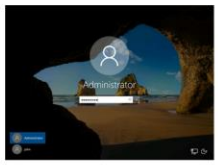
Java Update Available
A new version of Java is ready to be installed.
Click here to continue.
Java Update Checker

7:07 PM
9/17/2024

Network Security Controls - Technical Co...
1 Hr 31 Min Remaining

Instructions | Resources | Help

- [x] 11. If already logged in as **Administrator** user, skip below step.
- [x] 12. By default, the **Administrator** account is selected. Click T admin@123 and press **Enter** to login.



- [x] 13. Open **Control Panel**.
- [x] 14. Click the **System and Security** option.

Previous | Next

Search

USD/JPY -0.57%

ENG

2:07 pm
18/09/2024

Network Security Controls - Technical Controls — Mozilla Firefox

https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340

Web Server

System and Security

Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance and Personalization
Clock, Language, and Region
Ease of Access

Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings | Troubleshoot common computer problems

Windows Firewall
Check firewall status | Allow an app through Windows Firewall

System
View amount of RAM and processor speed | Allow remote access
Launch remote assistance | See the name of this computer

Power Options
Change what the power buttons do | Change when the computer sleeps

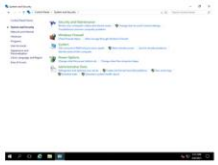
Administrative Tools
Defragment and optimize your drives | Create and format hard disk partitions
View event logs | Schedule tasks | Generate a system health report

7:08 PM
9/17/2024

Network Security Controls - Technical Co...
1 Hr 30 Min Remaining

Instructions | Resources | Help

- [ ] 15. The **System and Security** windows will appear. Click **Windows Firewall**.



- [ ] 16. The **Windows Firewall** window opens. Click **Use recommended settings**.

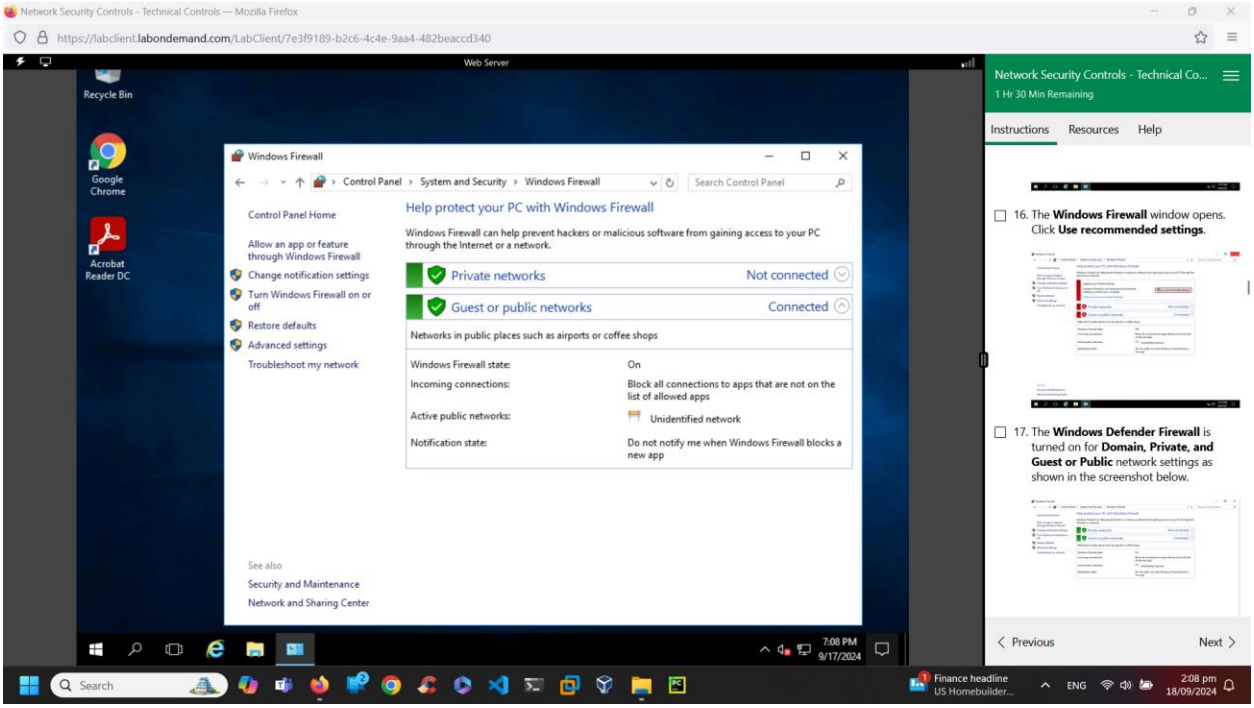
Previous | Next

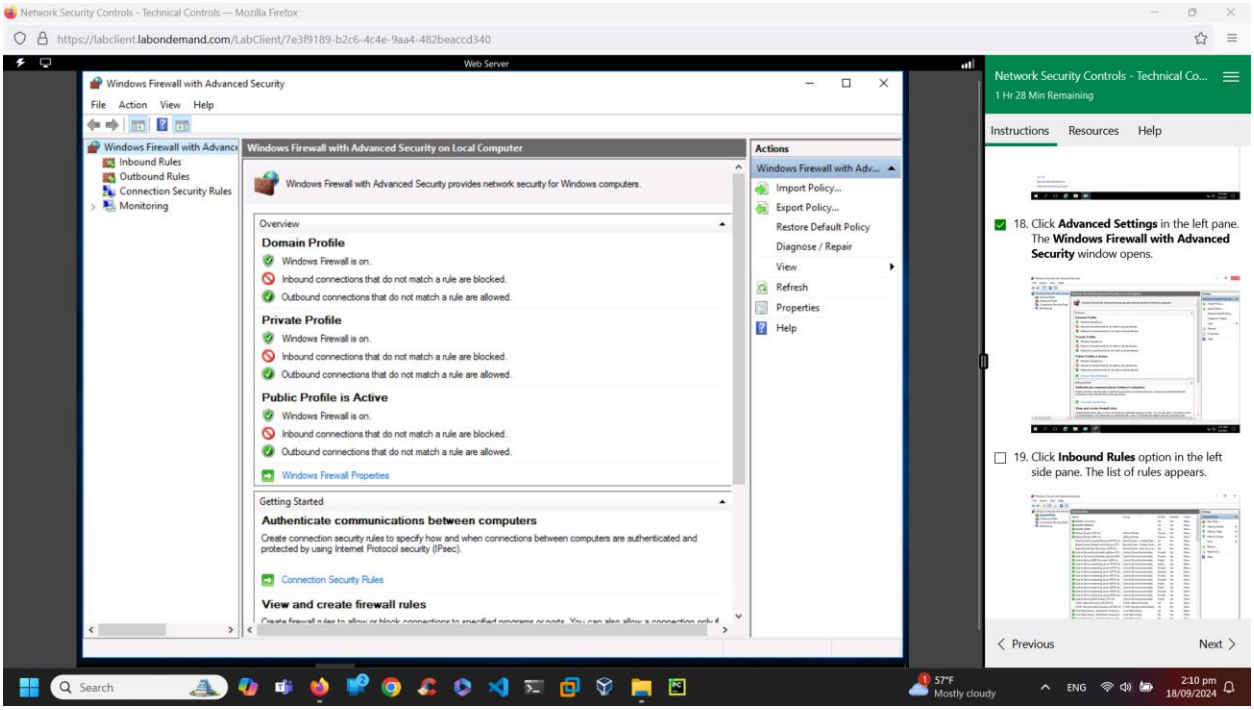
Search

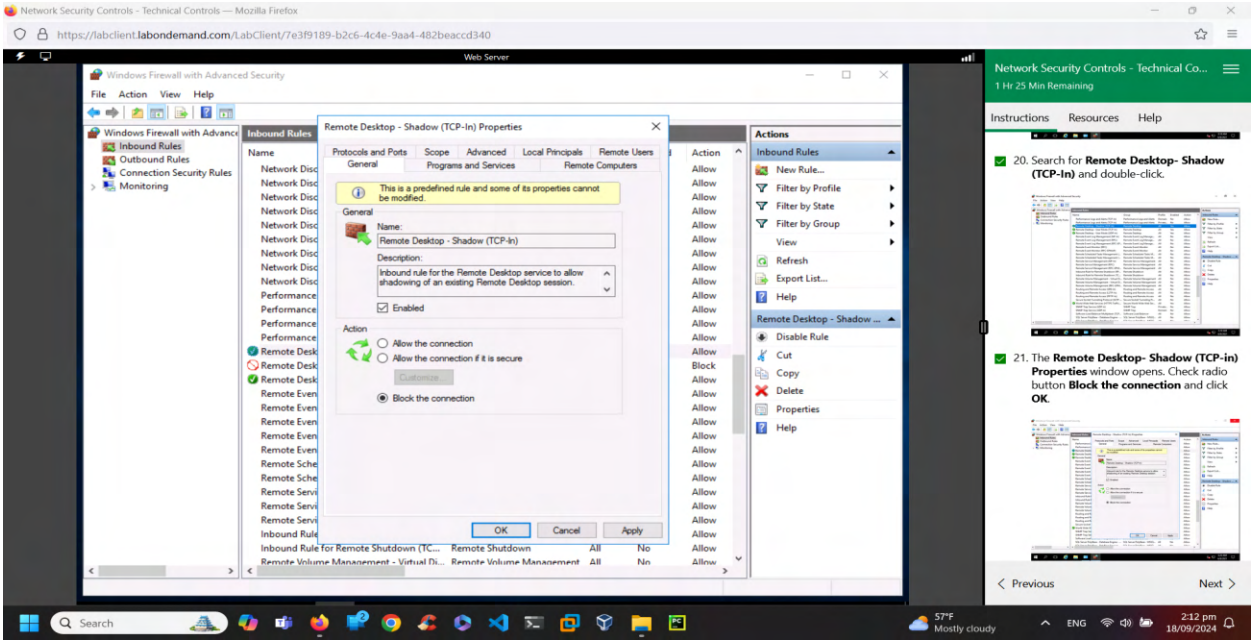
USD/JPY -0.57%

ENG

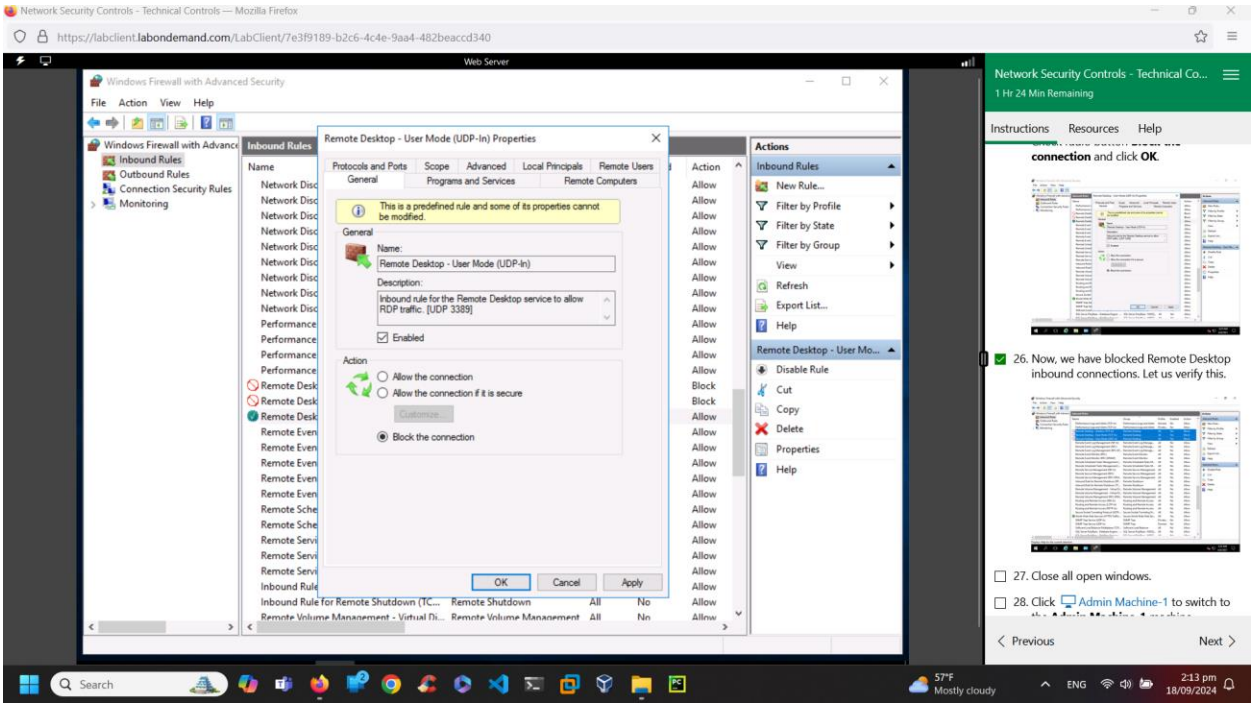
2:08 pm
18/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Recycle Bin
Google Chrome
Acrobat Reader DC
Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active public networks: Unidentified network
Notification state: Do not notify me when Windows Firewall blocks a new app
See also
Security and Maintenance
Network and Sharing Center
7:08 PM
9/17/2024
Search
Finance headline
US Homebuilder...
ENG
2:08 pm
18/09/2024
Network Security Controls - Technical Co...
1 Hr 30 Min Remaining
Instructions
Resources
Help
16. The Windows Firewall window opens. Click Use recommended settings.
17. The Windows Defender Firewall is turned on for Domain, Private, and Guest or Public network settings as shown in the screenshot below.
Previous
Next

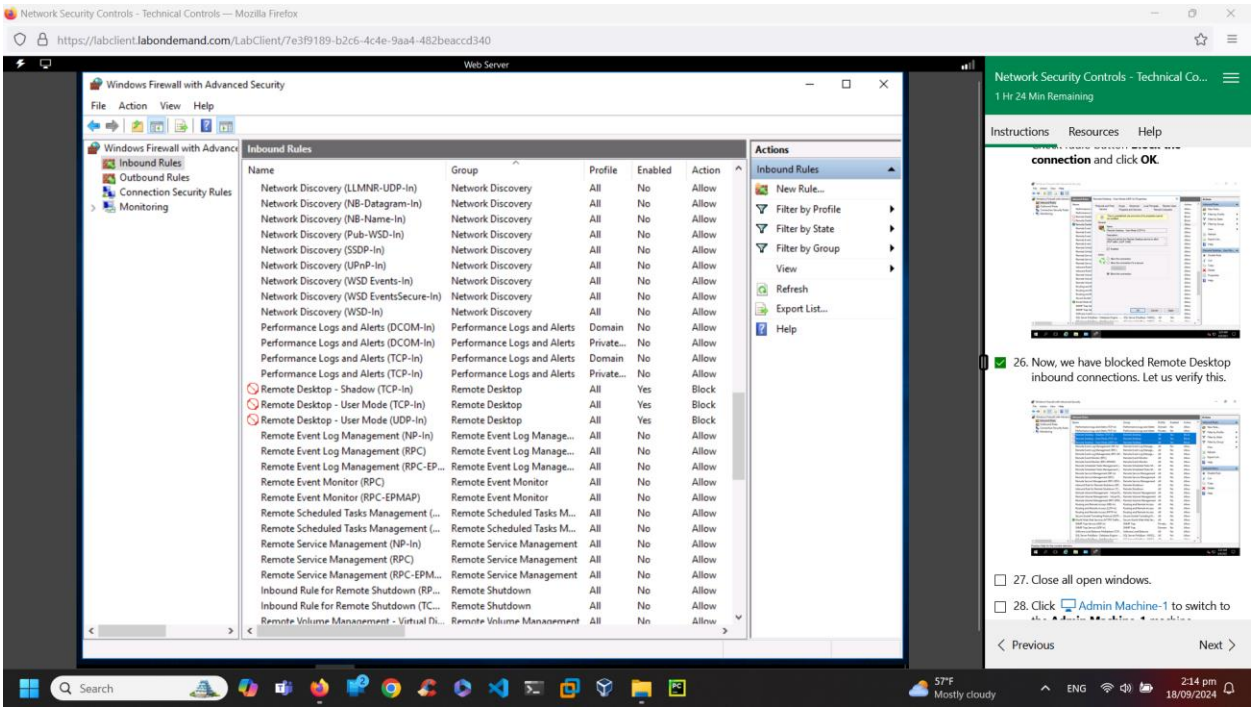

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Actions
Windows Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
57°F
Mostly cloudy
Search
ENG
2:10 pm
18/09/2024
Network Security Controls - Technical Co...
1 Hr 28 Min Remaining
Instructions
Resources
Help
18. Click Advanced Settings in the left pane. The Windows Firewall with Advanced Security window opens.
19. Click Inbound Rules option in the left side pane. The list of rules appears.
Previous
Next

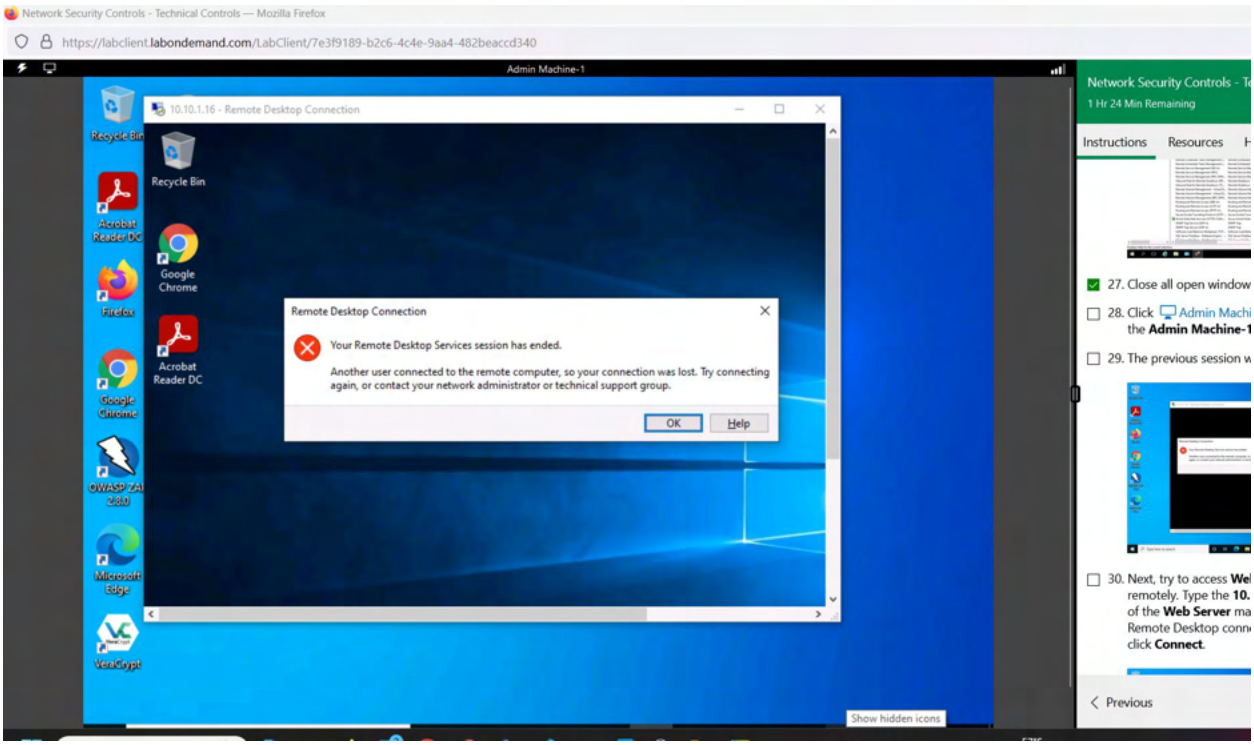


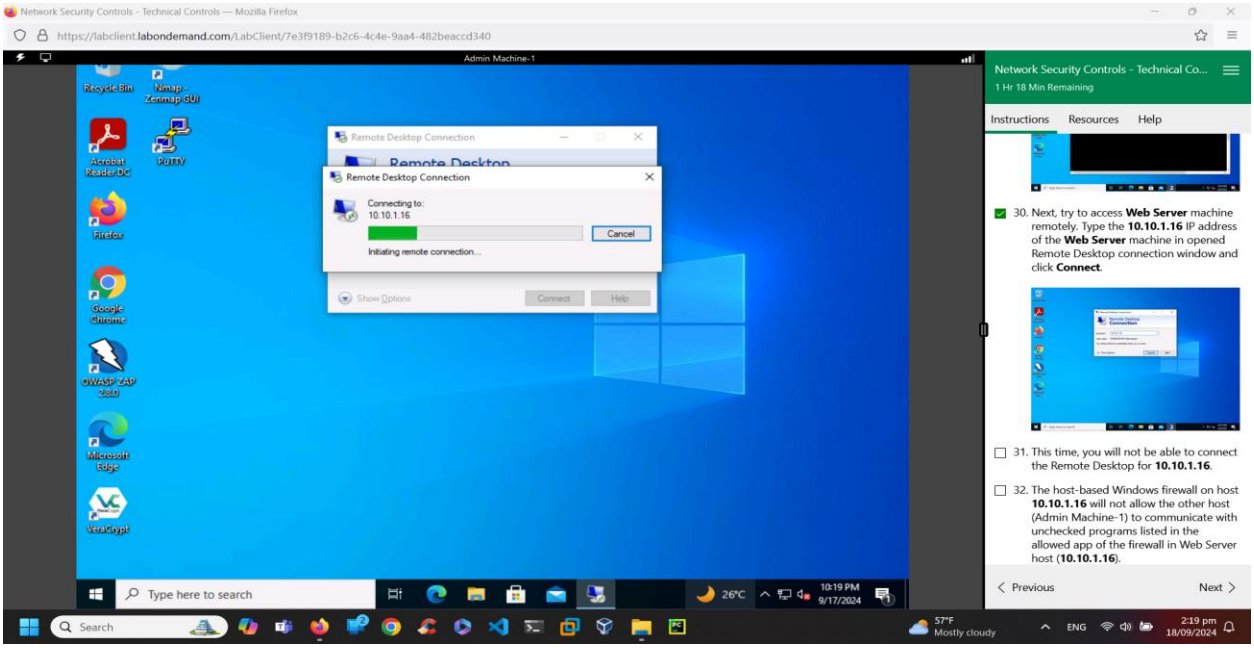
Step 10: Search for Remote desktop user mode tcp in and Remote desktop user mode udp in, and double click to block the connection.

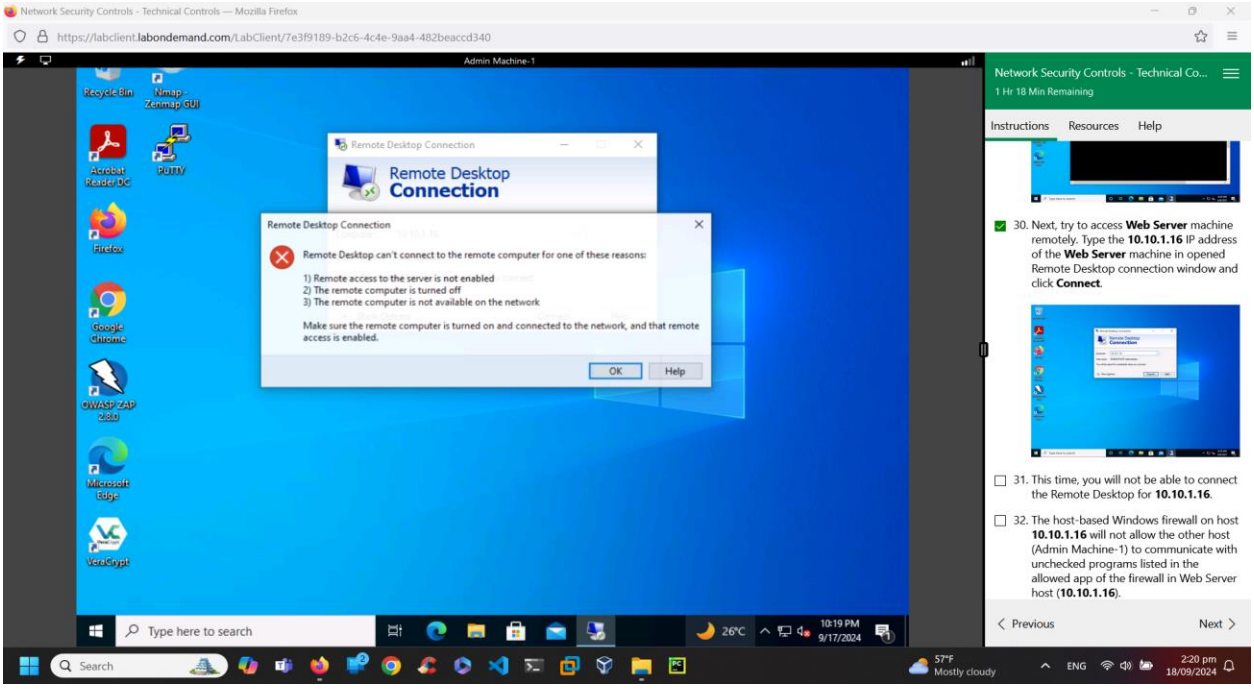

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Remote Desktop - User Mode (UDP-In) Properties
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
General
Programs and Services
Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
Remote Desktop - User Mode (UDP-In)
Description:
Inbound rule for the Remote Desktop service to allow RDP traffic. [UDP 3389]
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK
Cancel
Apply
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Remote Desktop - User Mo...
Disable Rule
Cut
Copy
Delete
Properties
Help
Network Security Controls - Technical Co...
1 Hr 24 Min Remaining
Instructions
Resources
Help
connection and click OK.
26. Now, we have blocked Remote Desktop inbound connections. Let us verify this.
27. Close all open windows.
28. Click Admin Machine-1 to switch to
Previous
Next
Search
57°F
Mostly cloudy
ENG
2:13 pm
18/09/2024

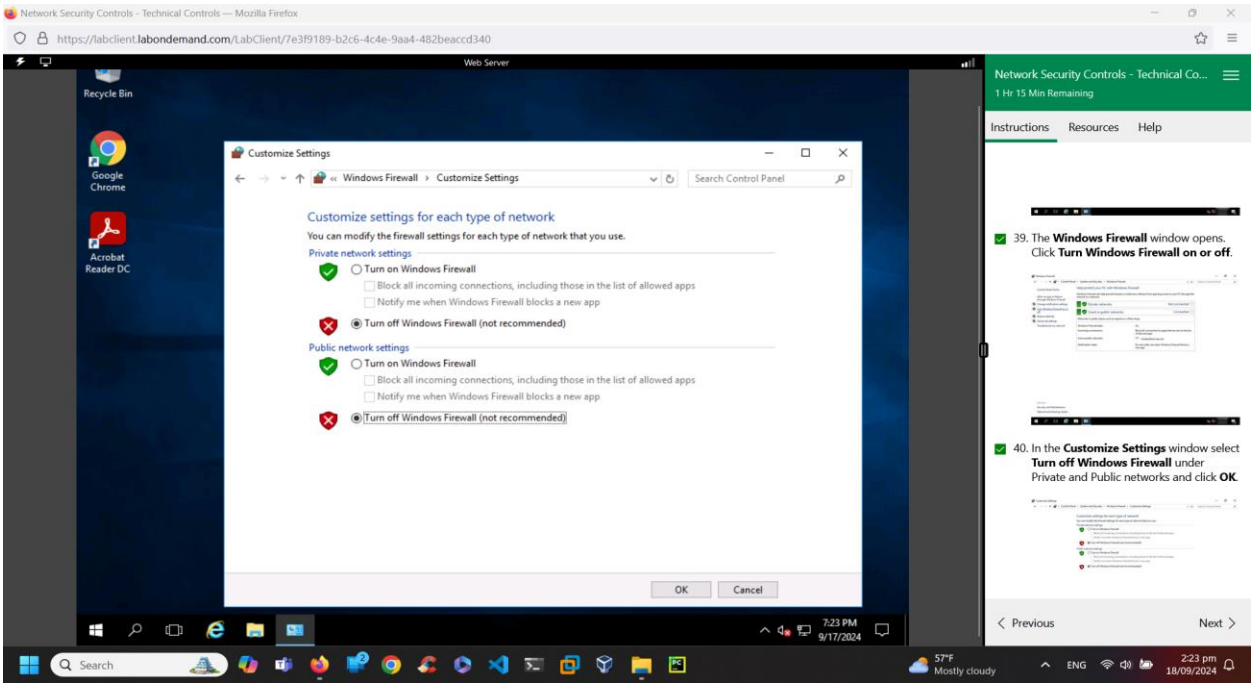
•

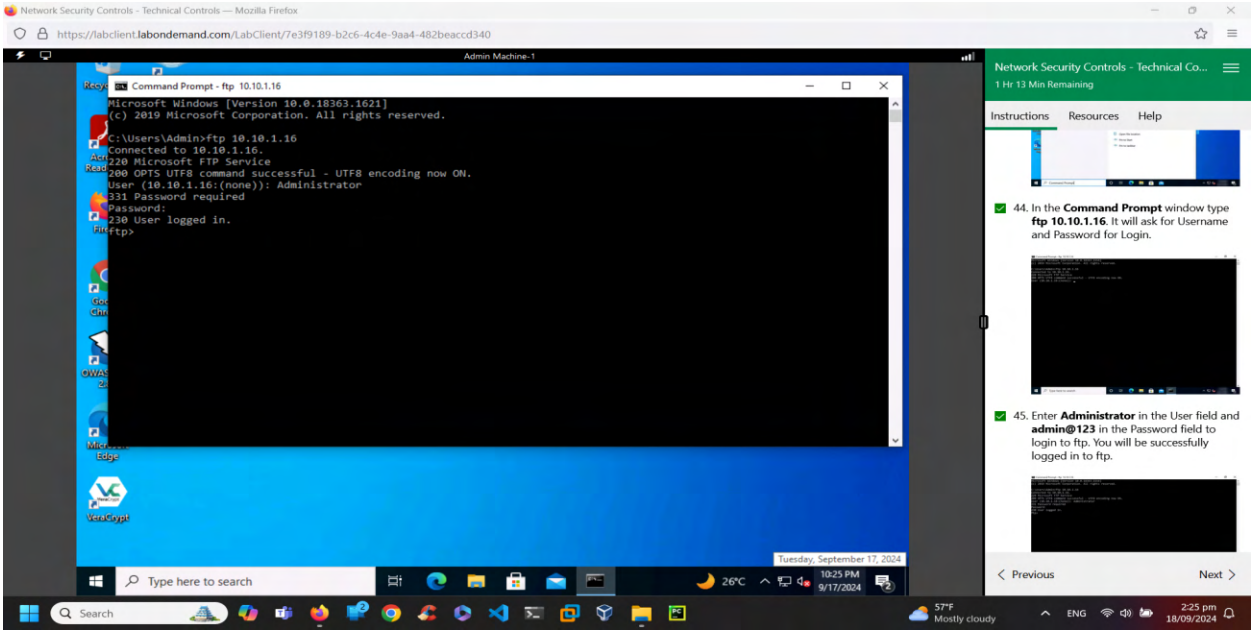

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Name
Group
Profile
Enabled
Action
Network Discovery (LLMNR-UDP-In)
Network Discovery (NB-Datagram-In)
Network Discovery (NB-Name-In)
Network Discovery (Pub-WSD-In)
Network Discovery (SSDP-In)
Network Discovery (UPnP-In)
Network Discovery (WSD Events-In)
Network Discovery (WSD EventsSecure-In)
Network Discovery (WSD-In)
Performance Logs and Alerts (DCOM-In)
Performance Logs and Alerts (TCP-In)
Remote Desktop - Shadow (TCP-In)
Remote Desktop - User Mode (TCP-In)
Remote Desktop - User Mode (UDP-In)
Remote Event Log Management (NP-In)
Remote Event Log Management (RPC)
Remote Event Log Management (RPC-EP...
Remote Event Monitor (RPC)
Remote Event Monitor (RPC-EPMAP)
Remote Scheduled Tasks Management (...
Remote Service Management (NP-In)
Remote Service Management (RPC)
Remote Service Management (RPC-EPM...
Inbound Rule for Remote Shutdown (RP...
Inbound Rule for Remote Shutdown (TC...
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Network Security Controls - Technical Co...
1 Hr 24 Min Remaining
Instructions
Resources
Help
connection and click OK.
26. Now, we have blocked Remote Desktop inbound connections. Let us verify this.
27. Close all open windows.
28. Click Admin Machine-1 to switch to
Previous
Next
Search
57°F
Mostly cloudy
ENG
2:14 pm
18/09/2024

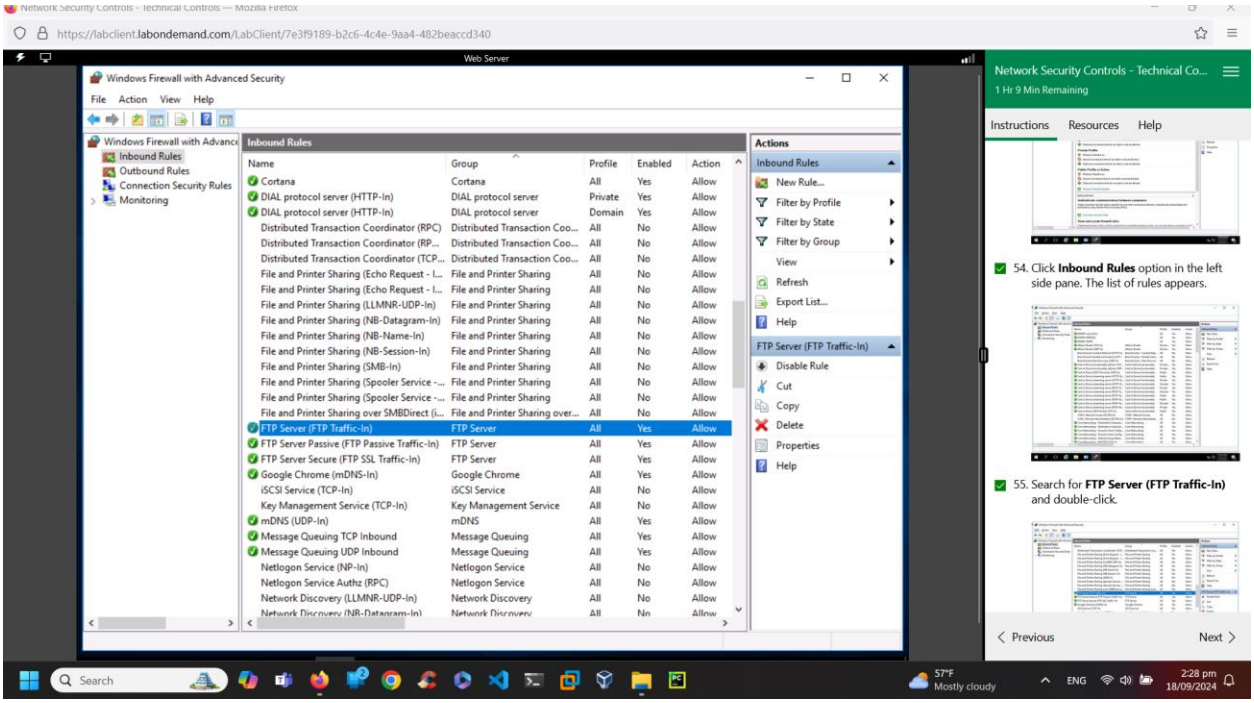

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
10.10.1.16 - Remote Desktop Connection
Recycle Bin
Acrobat Reader DC
Google Chrome
Firefox
OWASP ZAP 2.8.0
Microsoft Edge
VeraCrypt
Remote Desktop Connection
Your Remote Desktop Services session has ended.
Another user connected to the remote computer, so your connection was lost. Try connecting again, or contact your network administrator or technical support group.
OK
Help
Show hidden icons
Network Security Controls - T
1 Hr 24 Min Remaining
Instructions
Resources
27. Close all open window
28. Click Admin Machi the Admin Machine-1
29. The previous session w
30. Next, try to access Wel remotely. Type the 10. of the Web Server ma Remote Desktop conn click Connect.
Previous

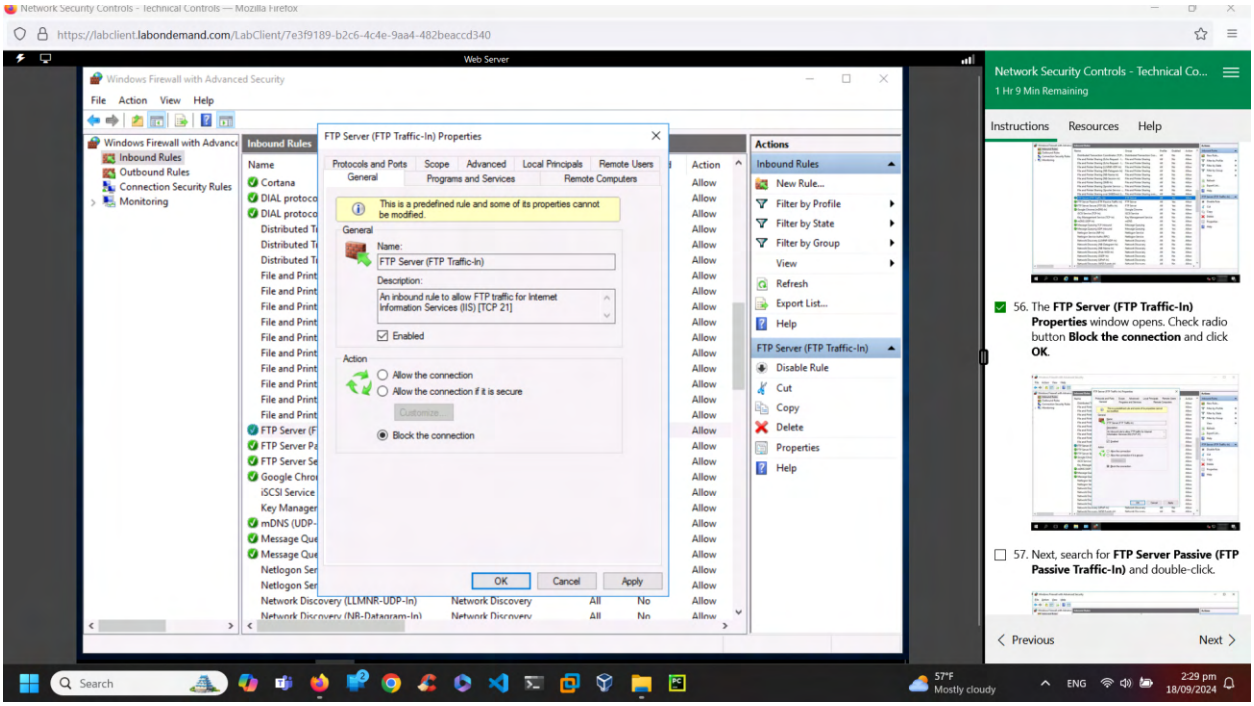

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Recycle Bin
Nmap - Zenmap GUI
Acrobat Reader DC
PuTTY
Firefox
Google Chrome
OWASP ZAP 2.8.0
Microsoft Edge
VeraCrypt
Remote Desktop Connection
Connecting to: 10.10.1.16
Initiating remote connection...
Cancel
Show Options
Connect
Help
Type here to search
26°C
10:19 PM 9/17/2024
Search
57°F Mostly cloudy
ENG
2:19 pm 18/09/2024
Network Security Controls - Technical Co...
1 Hr 18 Min Remaining
Instructions
Resources
Help
30. Next, try to access Web Server machine remotely. Type the 10.10.1.16 IP address of the Web Server machine in opened Remote Desktop connection window and click Connect.
31. This time, you will not be able to connect the Remote Desktop for 10.10.1.16.
32. The host-based Windows firewall on host 10.10.1.16 will not allow the other host (Admin Machine-1) to communicate with unchecked programs listed in the allowed app of the firewall in Web Server host (10.10.1.16).
Previous
Next

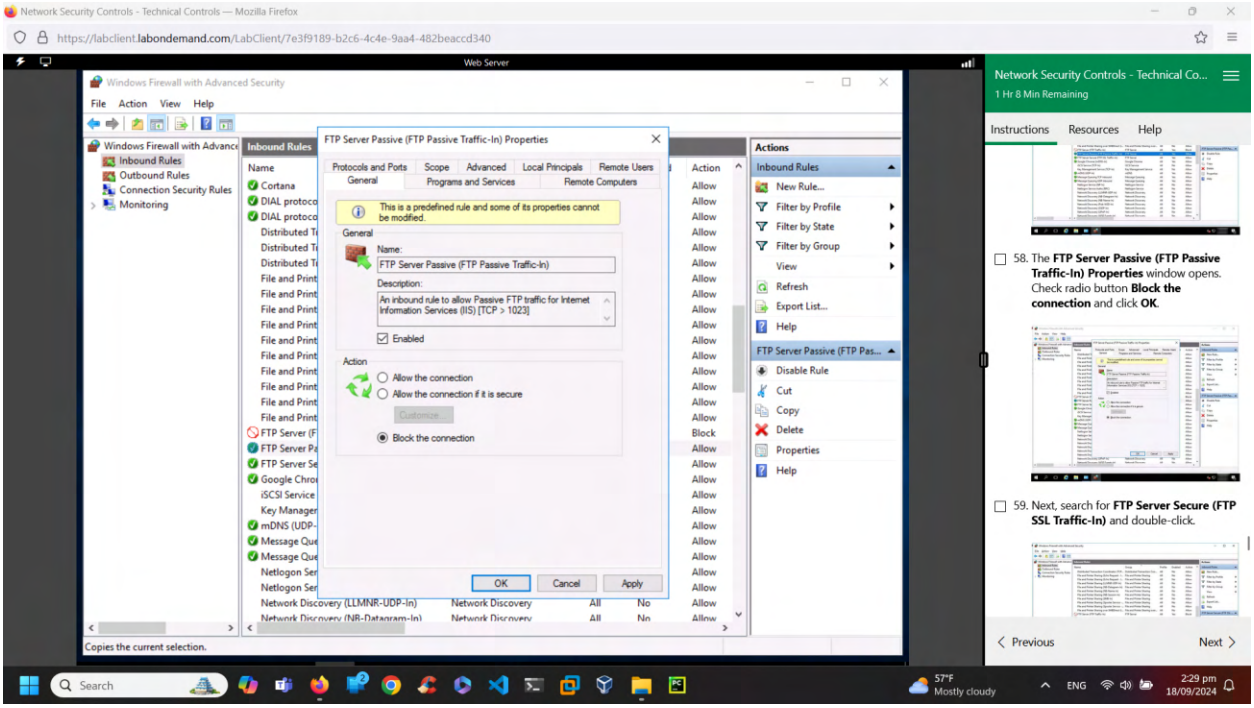

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Remote Desktop Connection
Remote Desktop Connection
Remote Desktop can't connect to the remote computer for one of these reasons:
1) Remote access to the server is not enabled
2) The remote computer is turned off
3) The remote computer is not available on the network
Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.
OK
Help
Type here to search
10:19 PM
9/17/2024
Network Security Controls - Technical Co...
1 Hr 18 Min Remaining
Instructions
Resources
Help
30. Next, try to access Web Server machine remotely. Type the 10.10.1.16 IP address of the Web Server machine in opened Remote Desktop connection window and click Connect.
31. This time, you will not be able to connect the Remote Desktop for 10.10.1.16.
32. The host-based Windows firewall on host 10.10.1.16 will not allow the other host (Admin Machine-1) to communicate with unchecked programs listed in the allowed app of the firewall in Web Server host (10.10.1.16).
Previous
Next
57°F
Mostly cloudy
ENG
2:20 pm
18/09/2024

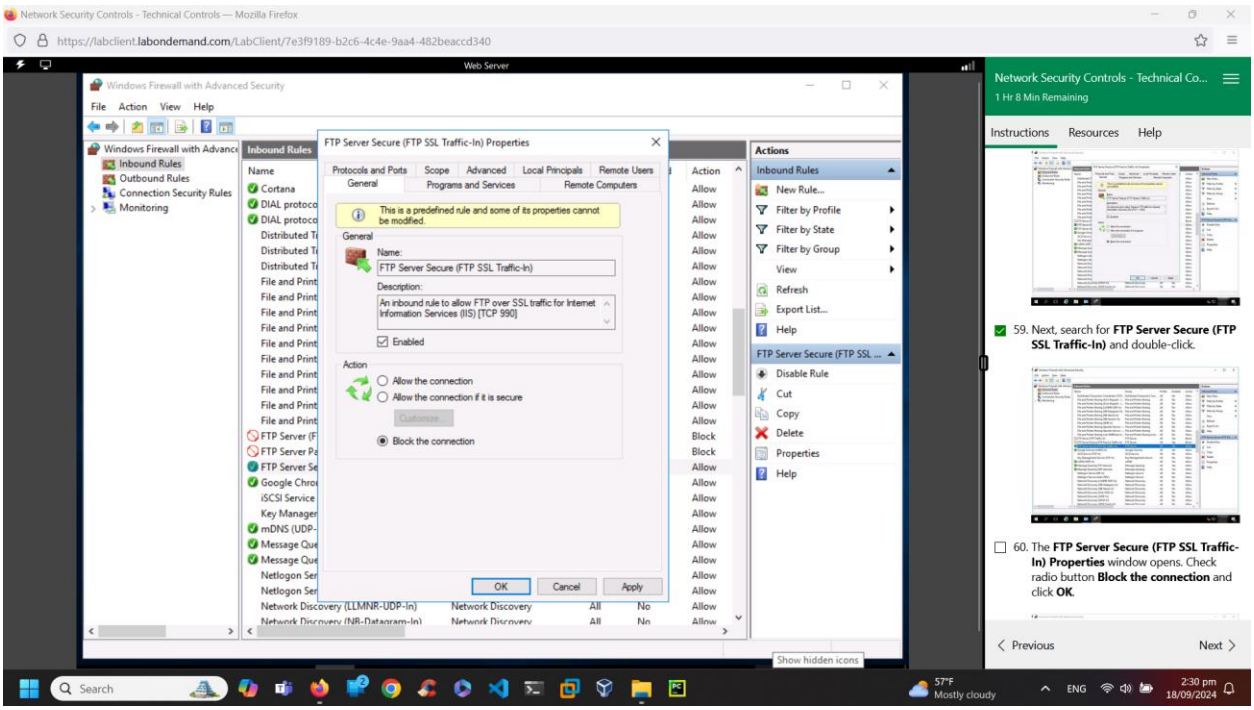

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Customize Settings
Windows Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
Public network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
OK
Cancel
7:23 PM
9/17/2024
Network Security Controls - Technical Co...
1 Hr 15 Min Remaining
Instructions
Resources
Help
39. The Windows Firewall window opens. Click Turn Windows Firewall on or off.
40. In the Customize Settings window select Turn off Windows Firewall under Private and Public networks and click OK.
Previous
Next
57°F
Mostly cloudy
ENG
2:23 pm
18/09/2024

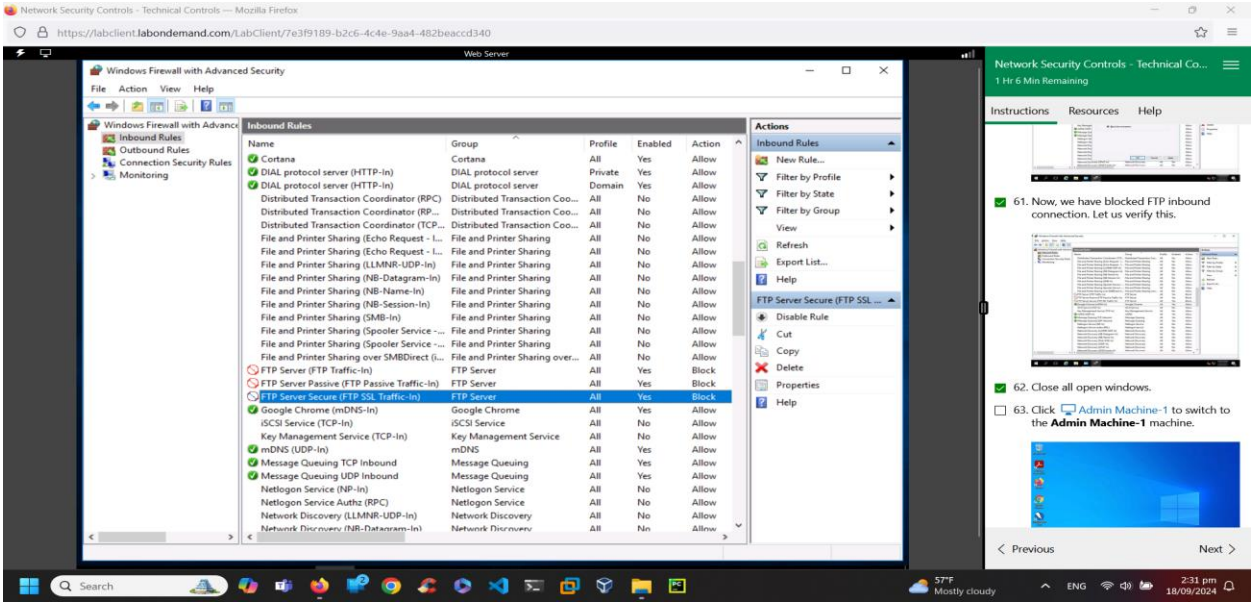

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Command Prompt - ftp 10.10.1.16
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>ftp 10.10.1.16
Connected to 10.10.1.16.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.1.16:(none)): Administrator
331 Password required
Password:
230 User logged in.
ftp>
Type here to search
Tuesday, September 17, 2024
10:25 PM
9/17/2024
Network Security Controls - Technical Co...
1 Hr 13 Min Remaining
Instructions
Resources
Help
44. In the Command Prompt window type ftp 10.10.1.16. It will ask for Username and Password for Login.
45. Enter Administrator in the User field and admin@123 in the Password field to login to ftp. You will be successfully logged in to ftp.
Previous
Next
Search
57°F
Mostly cloudy
ENG
2:25 pm
18/09/2024

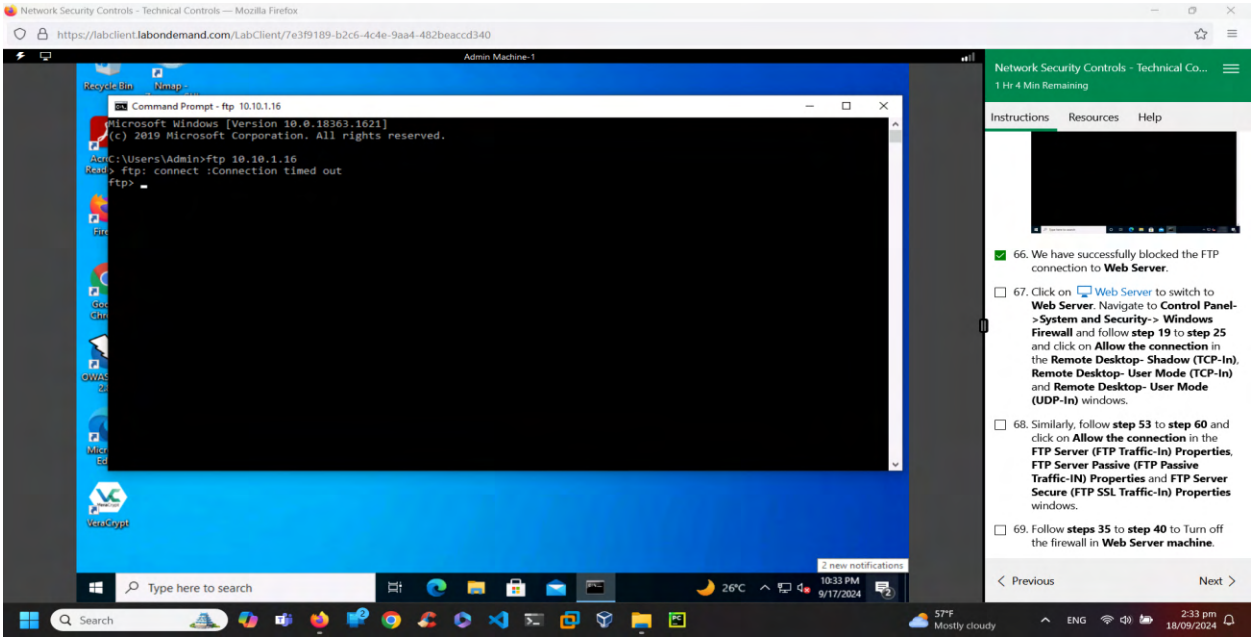

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action
Cortana Cortana All Yes Allow
DIAL protocol server (HTTP-In) DIAL protocol server Private Yes Allow
DIAL protocol server (HTTP-In) DIAL protocol server Domain Yes Allow
Distributed Transaction Coordinator (RPC) Distributed Transaction Coo... All No Allow
Distributed Transaction Coordinator (RP... Distributed Transaction Coo... All No Allow
Distributed Transaction Coordinator (TCP... Distributed Transaction Coo... All No Allow
File and Printer Sharing (Echo Request - I... File and Printer Sharing All No Allow
File and Printer Sharing (Echo Request - I... File and Printer Sharing All No Allow
File and Printer Sharing (LLMNR-UDP-In) File and Printer Sharing All No Allow
File and Printer Sharing (NB-Datagram-In) File and Printer Sharing All No Allow
File and Printer Sharing (NB-Name-In) File and Printer Sharing All No Allow
File and Printer Sharing (NB-Session-In) File and Printer Sharing All No Allow
File and Printer Sharing (SMB-In) File and Printer Sharing All No Allow
File and Printer Sharing (Spooler Service -... File and Printer Sharing All No Allow
File and Printer Sharing (Spooler Service -... File and Printer Sharing All No Allow
File and Printer Sharing over SMBDirect (i... File and Printer Sharing over... All No Allow
FTP Server (FTP Traffic-In) FTP Server All Yes Allow
FTP Server Passive (FTP Passive Traffic-In) FTP Server All Yes Allow
FTP Server Secure (FTP SSL Traffic-In) FTP Server All Yes Allow
Google Chrome (mDNS-In) Google Chrome All Yes Allow
iSCSI Service (TCP-In) iSCSI Service All No Allow
Key Management Service (TCP-In) Key Management Service All No Allow
mDNS (UDP-In) mDNS All Yes Allow
Message Queuing TCP Inbound Message Queuing All Yes Allow
Message Queuing UDP Inbound Message Queuing All Yes Allow
Netlogon Service (NP-In) Netlogon Service All No Allow
Netlogon Service Authz (RPC) Netlogon Service All No Allow
Network Discovery (LLMNR-UDP-In) Network Discovery All No Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
FTP Server (FTP Traffic-In)
Disable Rule
Cut
Copy
Delete
Properties
Help
Network Security Controls - Technical Co...
1 Hr 9 Min Remaining
Instructions Resources Help
54. Click Inbound Rules option in the left side pane. The list of rules appears.
55. Search for FTP Server (FTP Traffic-In) and double-click.
Previous Next
Search
57°F Mostly cloudy
ENG
2:28 pm 18/09/2024

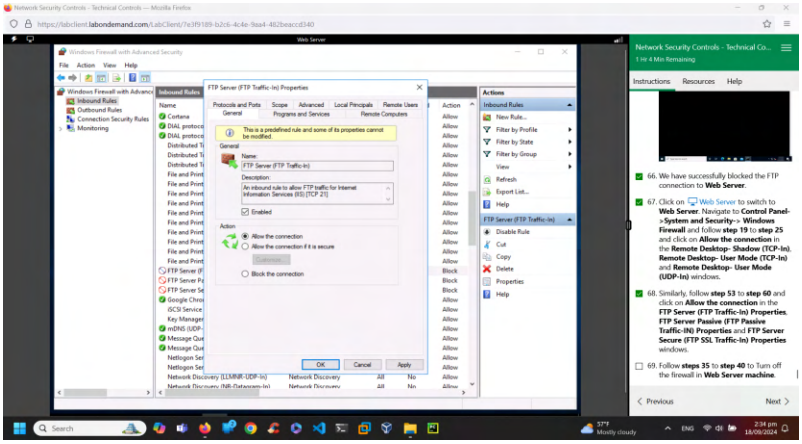

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
FTP Server (FTP Traffic-In) Properties
Protocols and Ports Scope Advanced Local Principals Remote Users
General Programs and Services Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
FTP Server (FTP Traffic-In)
Description:
An inbound rule to allow FTP traffic for Internet Information Services (IIS) [TCP 21]
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK Cancel Apply
Network Security Controls - Technical Co...
1 Hr 9 Min Remaining
Instructions Resources Help
56. The FTP Server (FTP Traffic-In) Properties window opens. Check radio button Block the connection and click OK.
57. Next, search for FTP Server Passive (FTP Passive Traffic-In) and double-click.
Previous Next
Search
57°F Mostly cloudy
ENG
2:29 pm 18/09/2024

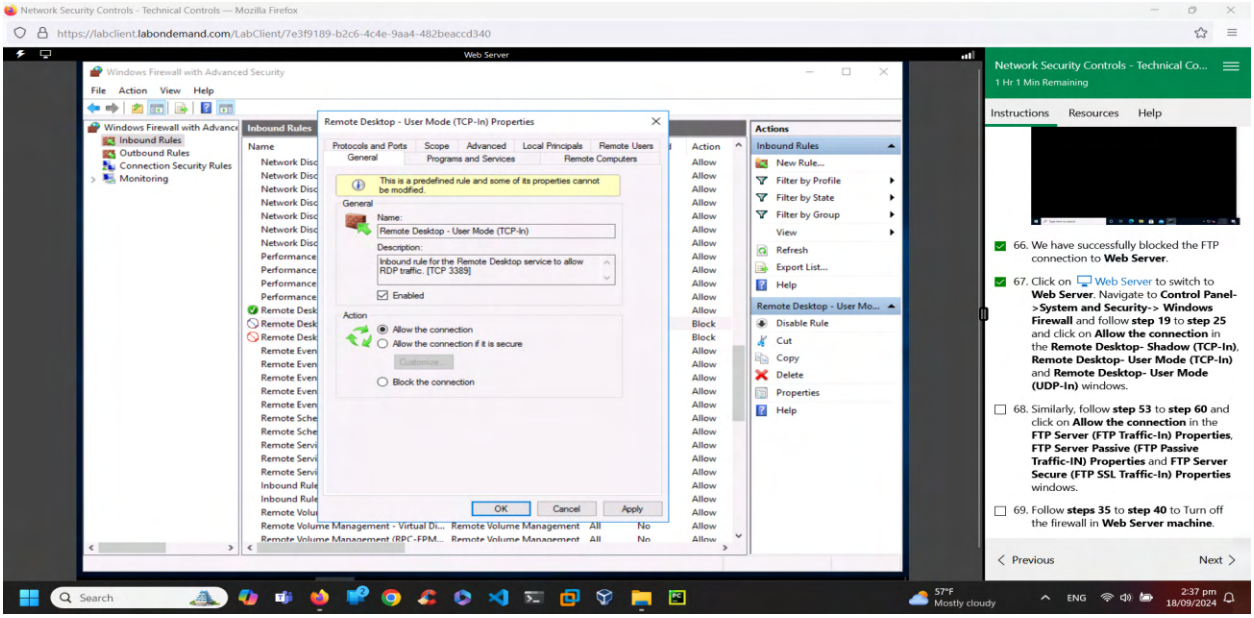

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
FTP Server Passive (FTP Passive Traffic-In) Properties
Protocols and Ports Scope Advanced Local Principals Remote Users
General Programs and Services Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
FTP Server Passive (FTP Passive Traffic-In)
Description:
An inbound rule to allow Passive FTP traffic for Internet Information Services (IIS) [TCP > 1023]
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK Cancel Apply
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
FTP Server Passive (FTP Pas...
Disable Rule
Cut
Copy
Delete
Properties
Help
Copies the current selection.
Network Security Controls - Technical Co...
1 Hr 8 Min Remaining
Instructions Resources Help
58. The FTP Server Passive (FTP Passive Traffic-In) Properties window opens. Check radio button Block the connection and click OK.
59. Next, search for FTP Server Secure (FTP SSL Traffic-In) and double-click.
Previous
Next
Search
57°F Mostly cloudy
ENG
2:29 pm 18/09/2024

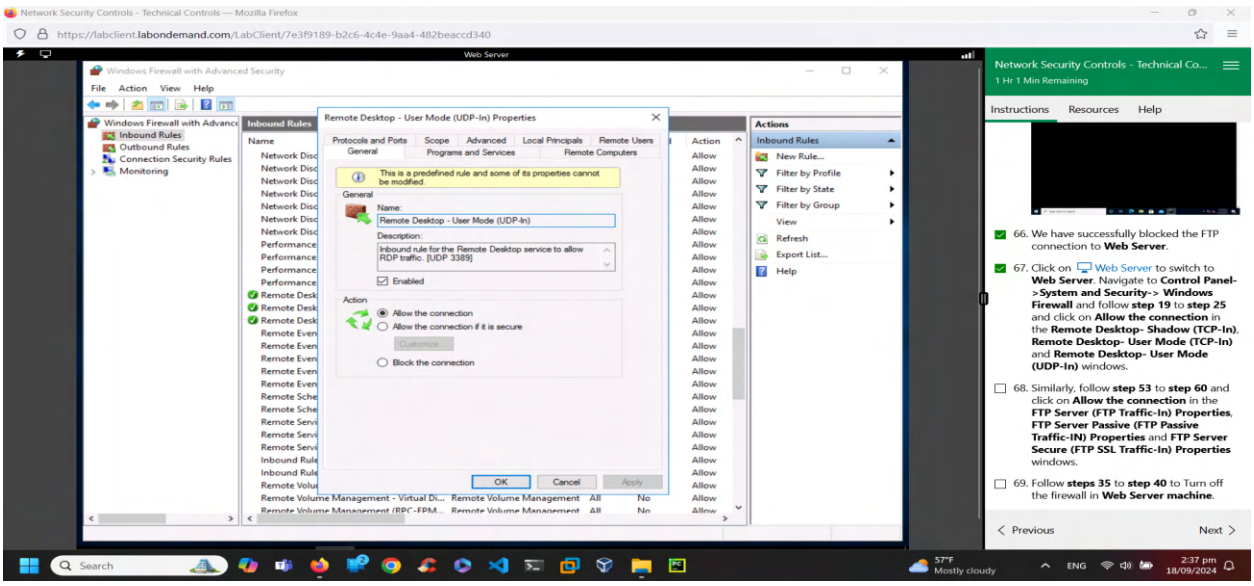

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
FTP Server Secure (FTP SSL Traffic-In) Properties
Protocols and Ports Scope Advanced Local Principals Remote Users
General Programs and Services Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
FTP Server Secure (FTP SSL Traffic-In)
Description:
An inbound rule to allow FTP over SSL traffic for Internet Information Services (IIS) [TCP 990]
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK Cancel Apply
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
FTP Server Secure (FTP SSL ...
Disable Rule
Cut
Copy
Delete
Properties
Help
Show hidden icons
Network Security Controls - Technical Co...
1 Hr 8 Min Remaining
Instructions Resources Help
59. Next, search for FTP Server Secure (FTP SSL Traffic-In) and double-click.
60. The FTP Server Secure (FTP SSL Traffic-In) Properties window opens. Check radio button Block the connection and click OK.
Previous
Next
Search
57°F Mostly cloudy
ENG
2:30 pm 18/09/2024

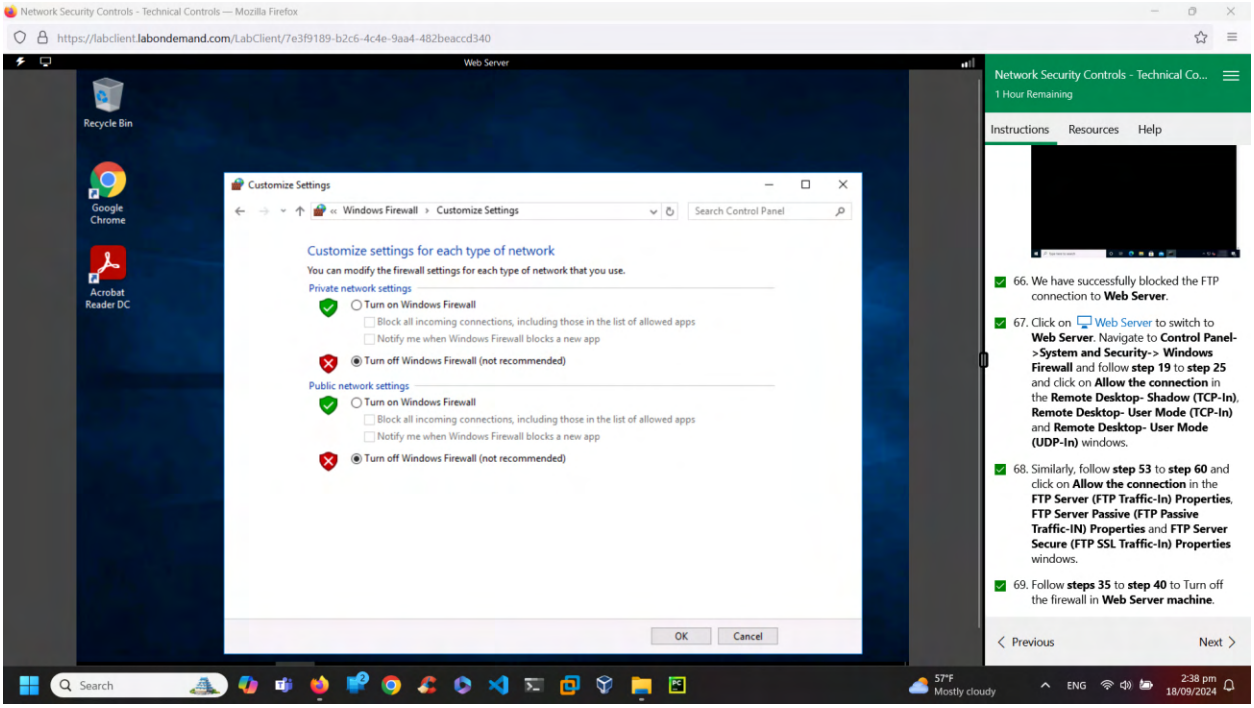

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Name Group Profile Enabled Action
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
FTP Server Secure (FTP SSL ...
Disable Rule
Cut
Copy
Delete
Properties
Help
Network Security Controls - Technical Co...
1 Hr 6 Min Remaining
Instructions Resources Help
61. Now, we have blocked FTP inbound connection. Let us verify this.
62. Close all open windows.
63. Click Admin Machine-1 to switch to the Admin Machine-1 machine.
Previous
Next
Search
57°F
Mostly cloudy
ENG
2:31 pm
18/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Recycle Bin
Nmap -
Command Prompt - ftp 10.10.1.16
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>ftp 10.10.1.16
ftp: connect :Connection timed out
ftp>
VeraCrypt
Type here to search
2 new notifications
10:33 PM
9/17/2024
26°C
Network Security Controls - Technical Co...
1 Hr 4 Min Remaining
Instructions Resources Help
66. We have successfully blocked the FTP connection to Web Server.
67. Click on Web Server to switch to Web Server. Navigate to Control Panel->System and Security-> Windows Firewall and follow step 19 to step 25 and click on Allow the connection in the Remote Desktop- Shadow (TCP-In), Remote Desktop- User Mode (TCP-In) and Remote Desktop- User Mode (UDP-In) windows.
68. Similarly, follow step 53 to step 60 and click on Allow the connection in the FTP Server (FTP Traffic-In) Properties, FTP Server Passive (FTP Passive Traffic-IN) Properties and FTP Server Secure (FTP SSL Traffic-In) Properties windows.
69. Follow steps 35 to step 40 to Turn off the firewall in Web Server machine.
Previous
Next
Search
57°F
Mostly cloudy
ENG
2:33 pm
18/09/2024




Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Remote Desktop - User Mode (TCP-In) Properties
Protocols and Ports Scope Advanced Local Principals Remote Users
General Programs and Services Remote Computers
This is a predefined rule and some of its properties cannot be modified.
Name: Remote Desktop - User Mode (TCP-In)
Description: Inbound rule for the Remote Desktop service to allow RDP traffic. [TCP 3389]
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK Cancel Apply
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Remote Desktop - User Mo...
Disable Rule
Cut
Copy
Delete
Properties
Help
Network Security Controls - Technical Co...
1 Hr 1 Min Remaining
Instructions Resources Help
66. We have successfully blocked the FTP connection to Web Server.
67. Click on Web Server to switch to Web Server. Navigate to Control Panel->System and Security-> Windows Firewall and follow step 19 to step 25 and click on Allow the connection in the Remote Desktop- Shadow (TCP-In), Remote Desktop- User Mode (TCP-In) and Remote Desktop- User Mode (UDP-In) windows.
68. Similarly, follow step 53 to step 60 and click on Allow the connection in the FTP Server (FTP Traffic-In) Properties, FTP Server Passive (FTP Passive Traffic-IN) Properties and FTP Server Secure (FTP SSL Traffic-In) Properties windows.
69. Follow steps 35 to step 40 to Turn off the firewall in Web Server machine.
Previous Next
Search
57°F Mostly cloudy
ENG
2:37 pm 18/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Web Server
Windows Firewall with Advanced Security
File Action View Help
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Remote Desktop - User Mode (UDP-In) Properties
Protocols and Ports Scope Advanced Local Principals Remote Users
General Programs and Services Remote Computers
This is a predefined rule and some of its properties cannot be modified.
Name: Remote Desktop - User Mode (UDP-In)
Description: Inbound rule for the Remote Desktop service to allow RDP traffic. [UDP 3389]
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK Cancel Apply
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Network Security Controls - Technical Co...
1 Hr 1 Min Remaining
Instructions Resources Help
66. We have successfully blocked the FTP connection to Web Server.
67. Click on Web Server to switch to Web Server. Navigate to Control Panel->System and Security-> Windows Firewall and follow step 19 to step 25 and click on Allow the connection in the Remote Desktop- Shadow (TCP-In), Remote Desktop- User Mode (TCP-In) and Remote Desktop- User Mode (UDP-In) windows.
68. Similarly, follow step 53 to step 60 and click on Allow the connection in the FTP Server (FTP Traffic-In) Properties, FTP Server Passive (FTP Passive Traffic-IN) Properties and FTP Server Secure (FTP SSL Traffic-In) Properties windows.
69. Follow steps 35 to step 40 to Turn off the firewall in Web Server machine.
Previous Next
Search
57°F Mostly cloudy
ENG
2:37 pm 18/09/2024



Report:

The Host based Windows firewall is a security method which protects incoming and outgoing traffic with proper protection layer of authentication using credentials when any device wants to communicate with the other. Here I have learnt to use Windows firewall and set inbound rules, remote desktop application and FTP in command prompt and understand their functions. This method of secure connection is to ensure only trusted and necessary traffic is permitted.

As a cyber technician, Windows firewall setting comes under risk management and risk mitigate technique.

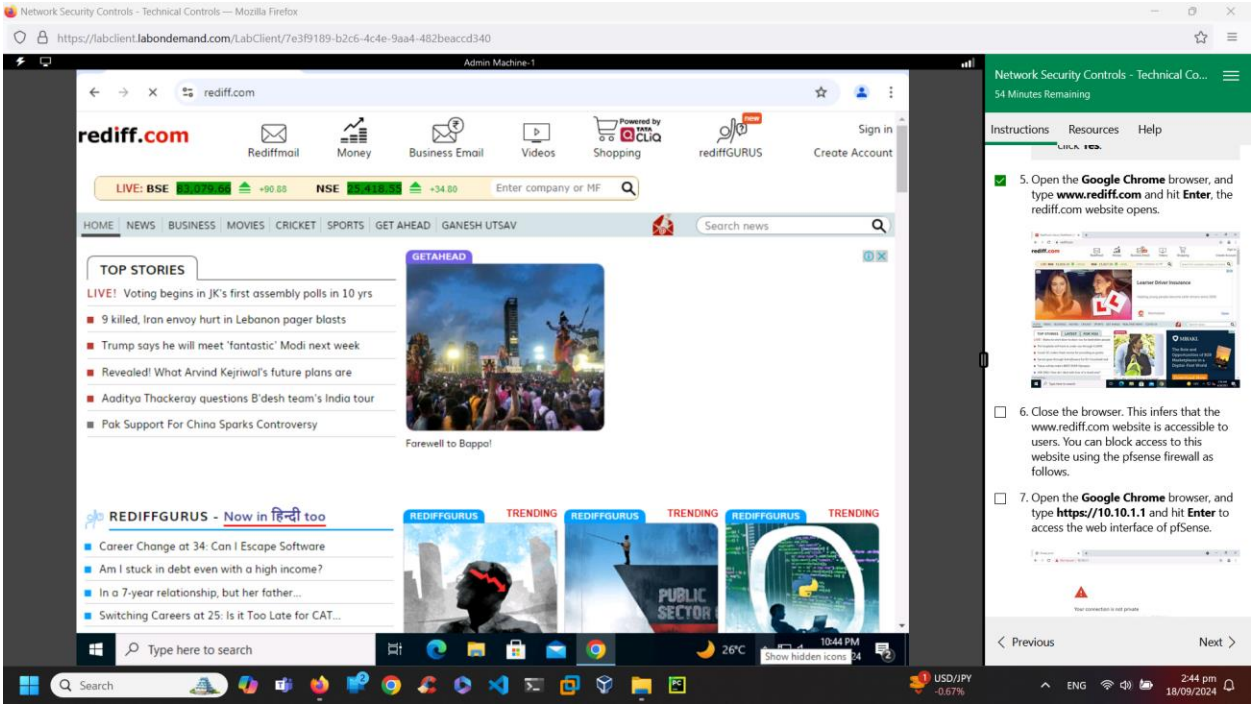
2. **Ilab Module no. and name:** 7. Network Security controls- Technical controls

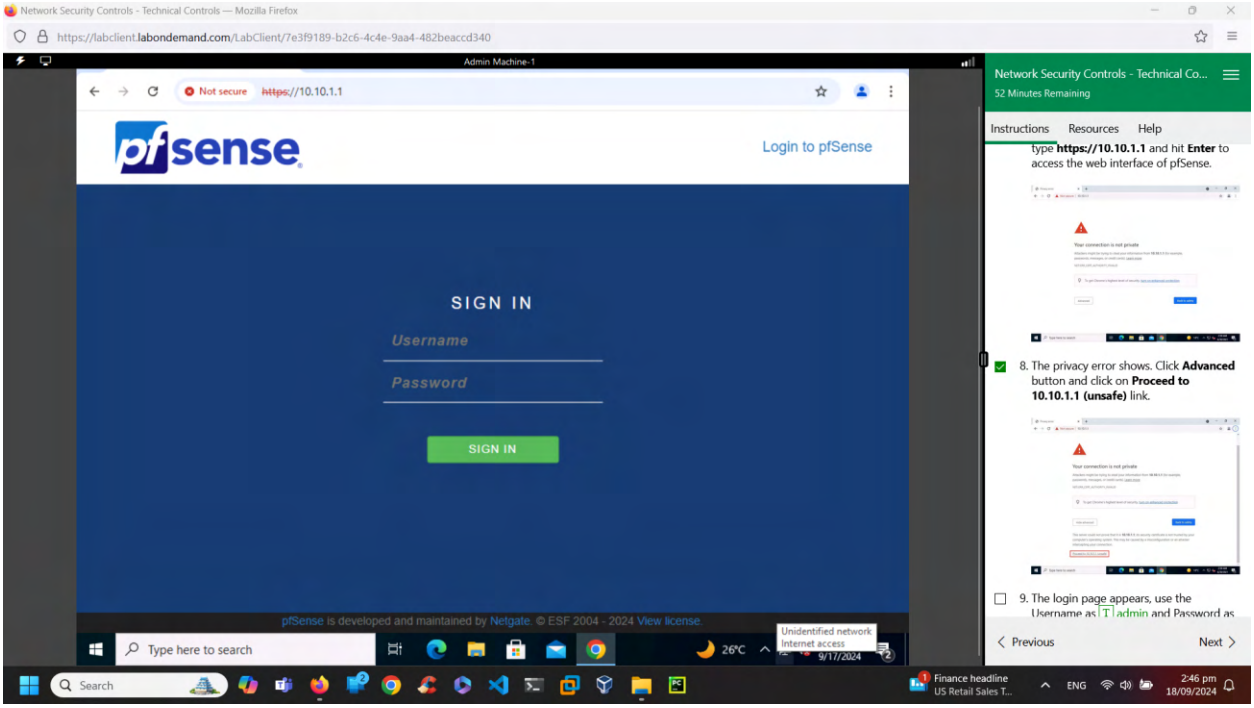
Exercise no. and name: 3, Implement Network-Based Firewall Functionality Block Unwanted Website Access using pfSense Firewall

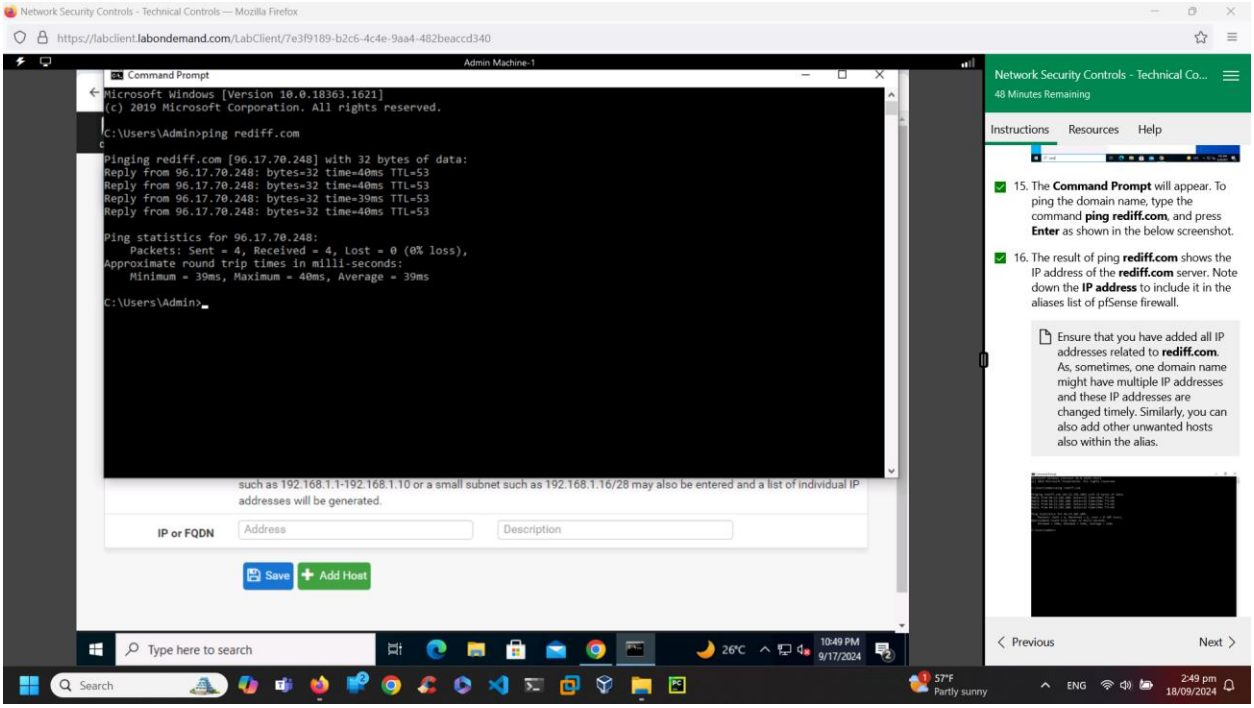
Performed Date: 18/09/2024

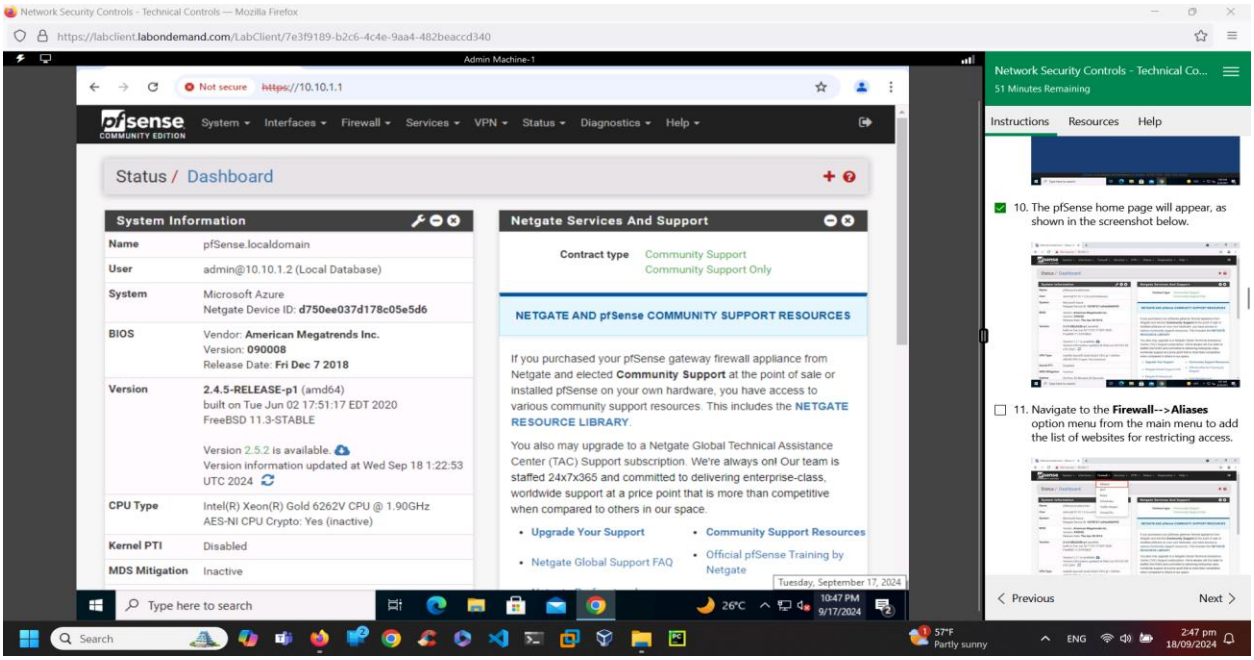
Summary:

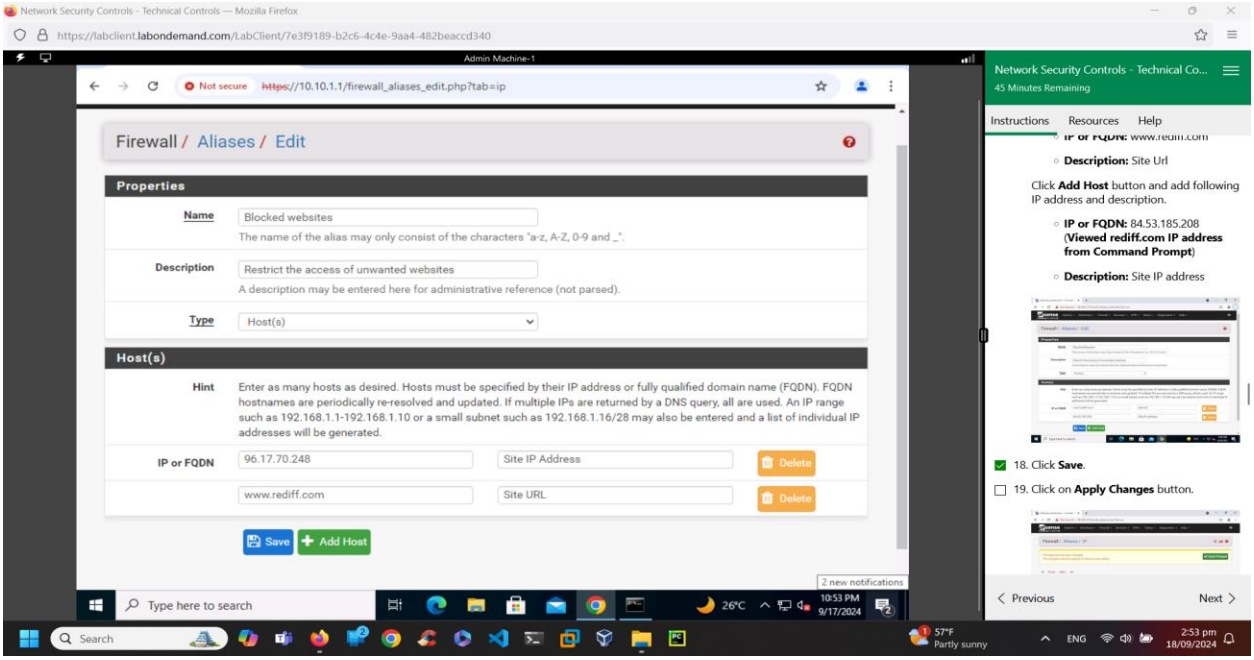
This lab demonstrates how pfsense is used to set firewall aliases and set rules and policy to block unwanted websites with their IP addresses. It changes the firewall policy and restart it to make the changes in the device.

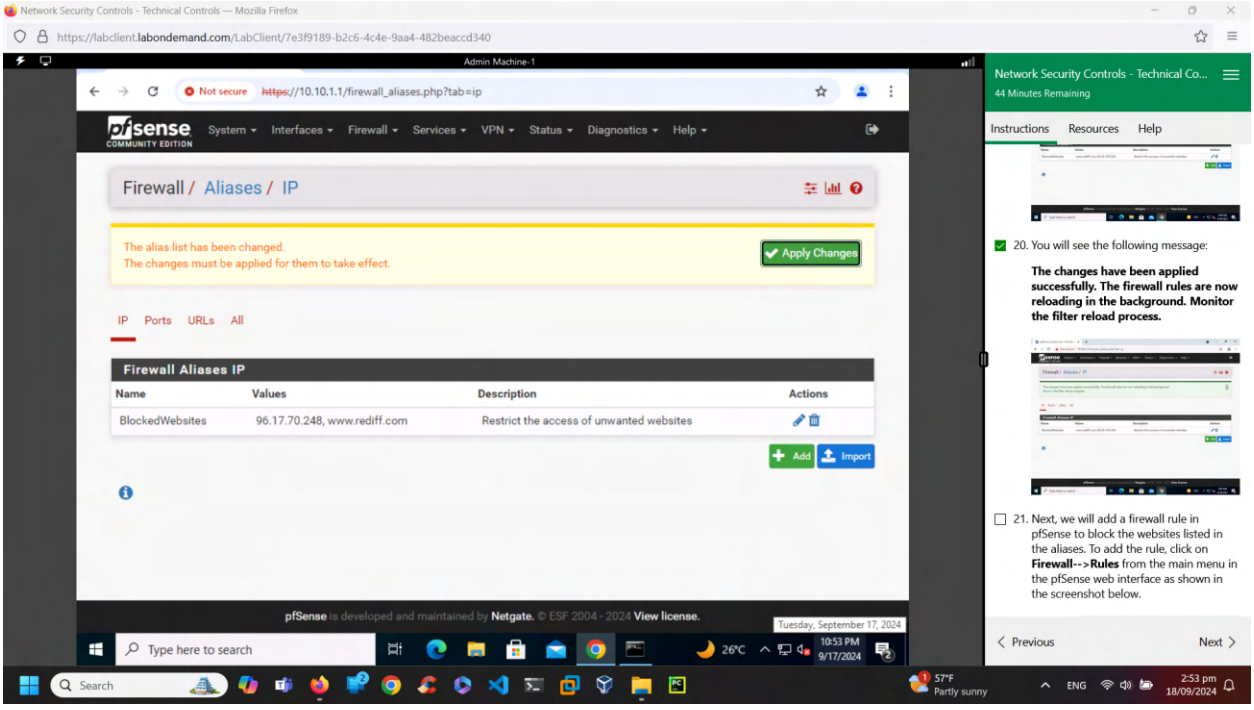

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
rediff.com
rediff.com
Rediffmail
Money
Business Email
Videos
Shopping
rediffGURUS
Sign in
Create Account
LIVE: BSE 83,079.66 +90.88 NSE 25,418.55 +34.80
Enter company or MF
HOME | NEWS | BUSINESS | MOVIES | CRICKET | SPORTS | GET AHEAD | GANESH UTSAV
Search news
TOP STORIES
LIVE! Voting begins in JK's first assembly polls in 10 yrs
9 killed, Iran envoy hurt in Lebanon pager blasts
Trump says he will meet 'fantastic' Modi next week
Revealed! What Arvind Kejriwal's future plans are
Aaditya Thackeray questions B'desh team's India tour
Pak Support For China Sparks Controversy
GETAHEAD
Farewell to Bappa!
REDIFFGURUS - Now in हिन्दी too
Career Change at 34: Can I Escape Software
Am I stuck in debt even with a high income?
In a 7-year relationship, but her father...
Switching Careers at 25: Is it Too Late for CAT...
REDIFFGURUS TRENDING
REDIFFGURUS TRENDING
REDIFFGURUS TRENDING
Type here to search
26°C
10:44 PM
Show hidden icons
Search
USD/JPY -0.67%
ENG
2:44 pm 18/09/2024
Network Security Controls - Technical Co...
54 Minutes Remaining
Instructions
Resources
Help
5. Open the Google Chrome browser, and type www.rediff.com and hit Enter, the rediff.com website opens.
6. Close the browser. This infers that the www.rediff.com website is accessible to users. You can block access to this website using the pfsense firewall as follows.
7. Open the Google Chrome browser, and type https://10.10.1.1 and hit Enter to access the web interface of pfSense.
Previous
Next

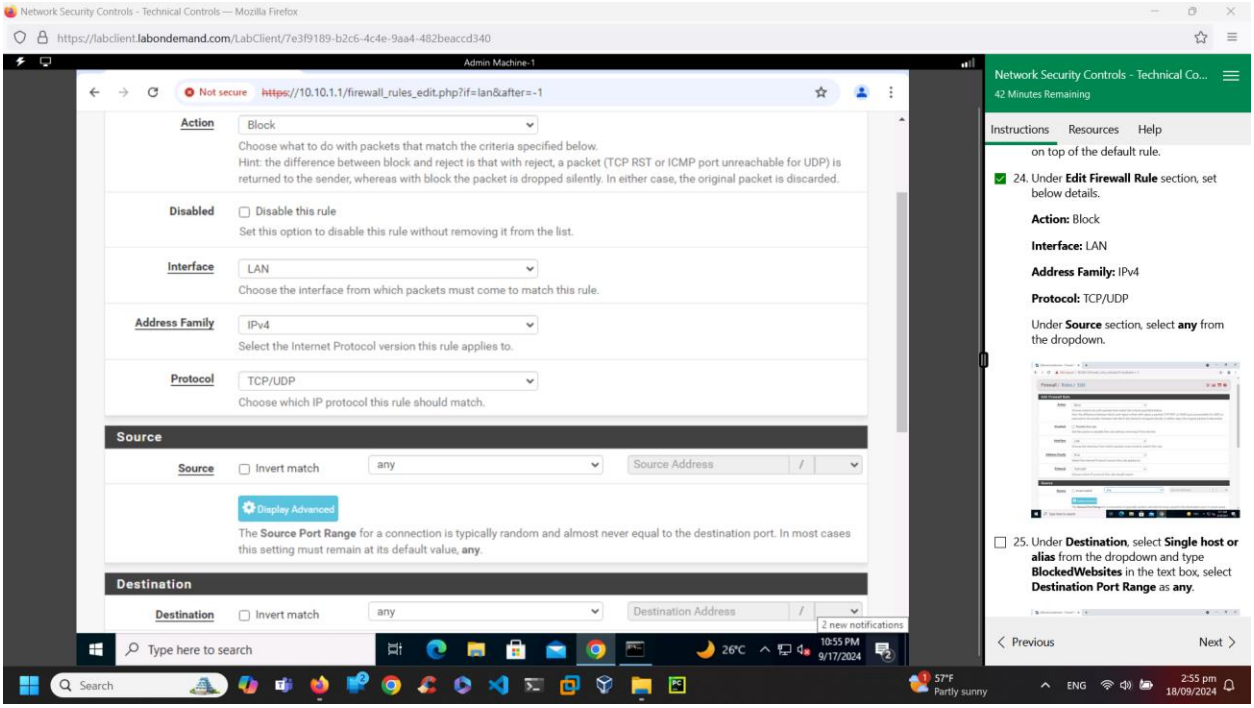

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Not secure https://10.10.1.1
pfsense
Login to pfSense
SIGN IN
Username
Password
SIGN IN
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Type here to search
26°C
Unidentified network
Internet access
9/17/2024
Search
Finance headline US Retail Sales T...
ENG
2:46 pm 18/09/2024
Network Security Controls - Technical Co...
52 Minutes Remaining
Instructions
Resources
Help
type https://10.10.1.1 and hit Enter to access the web interface of pfSense.
8. The privacy error shows. Click Advanced button and click on Proceed to 10.10.1.1 (unsafe) link.
9. The login page appears, use the Username as admin and Password as
Previous
Next

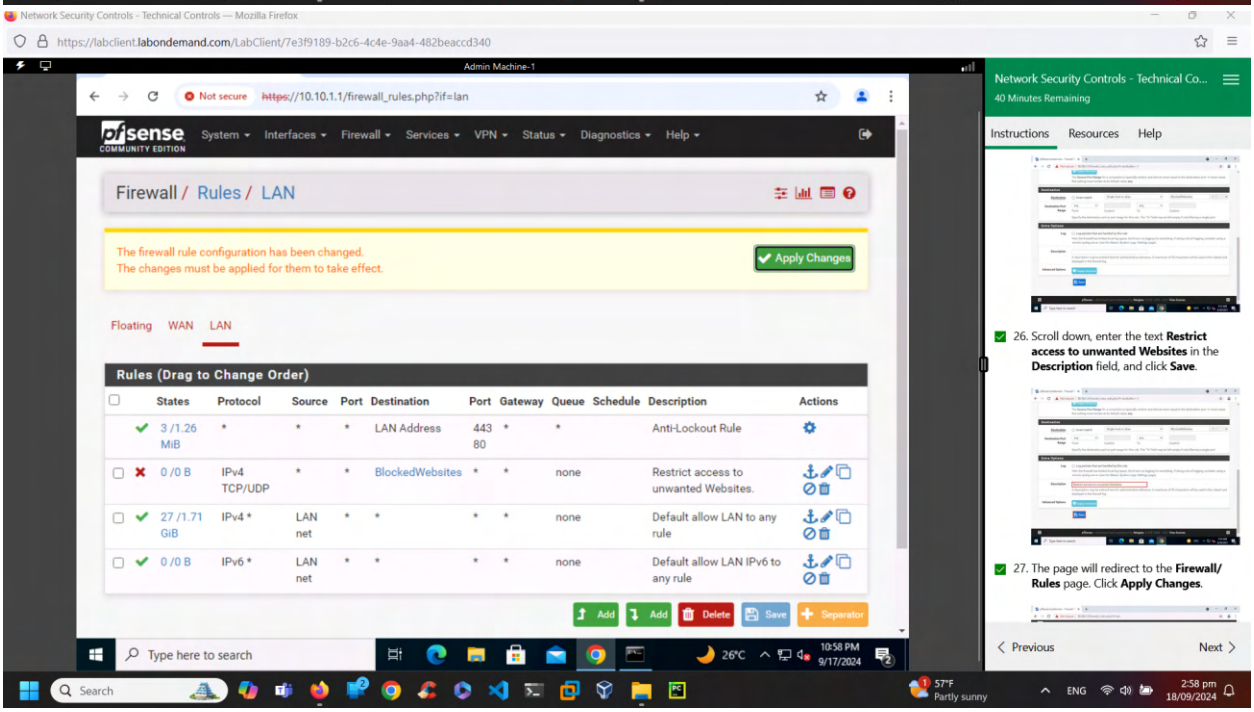

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Command Prompt
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>ping rediff.com
Pinging rediff.com [96.17.70.248] with 32 bytes of data:
Reply from 96.17.70.248: bytes=32 time=40ms TTL=53
Reply from 96.17.70.248: bytes=32 time=40ms TTL=53
Reply from 96.17.70.248: bytes=32 time=39ms TTL=53
Reply from 96.17.70.248: bytes=32 time=40ms TTL=53
Ping statistics for 96.17.70.248:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 39ms, Maximum = 40ms, Average = 39ms
C:\Users\Admin>
such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.
IP or FQDN
Address
Description
Save
Add Host
Network Security Controls - Technical Co...
48 Minutes Remaining
Instructions
Resources
Help
15. The Command Prompt will appear. To ping the domain name, type the command ping rediff.com, and press Enter as shown in the below screenshot.
16. The result of ping rediff.com shows the IP address of the rediff.com server. Note down the IP address to include it in the aliases list of pfSense firewall.
Ensure that you have added all IP addresses related to rediff.com. As, sometimes, one domain name might have multiple IP addresses and these IP addresses are changed timely. Similarly, you can also add other unwanted hosts also within the alias.
Previous
Next
Type here to search
26°C
10:49 PM
9/17/2024
Search
57°F
Partly sunny
ENG
2:49 pm
18/09/2024

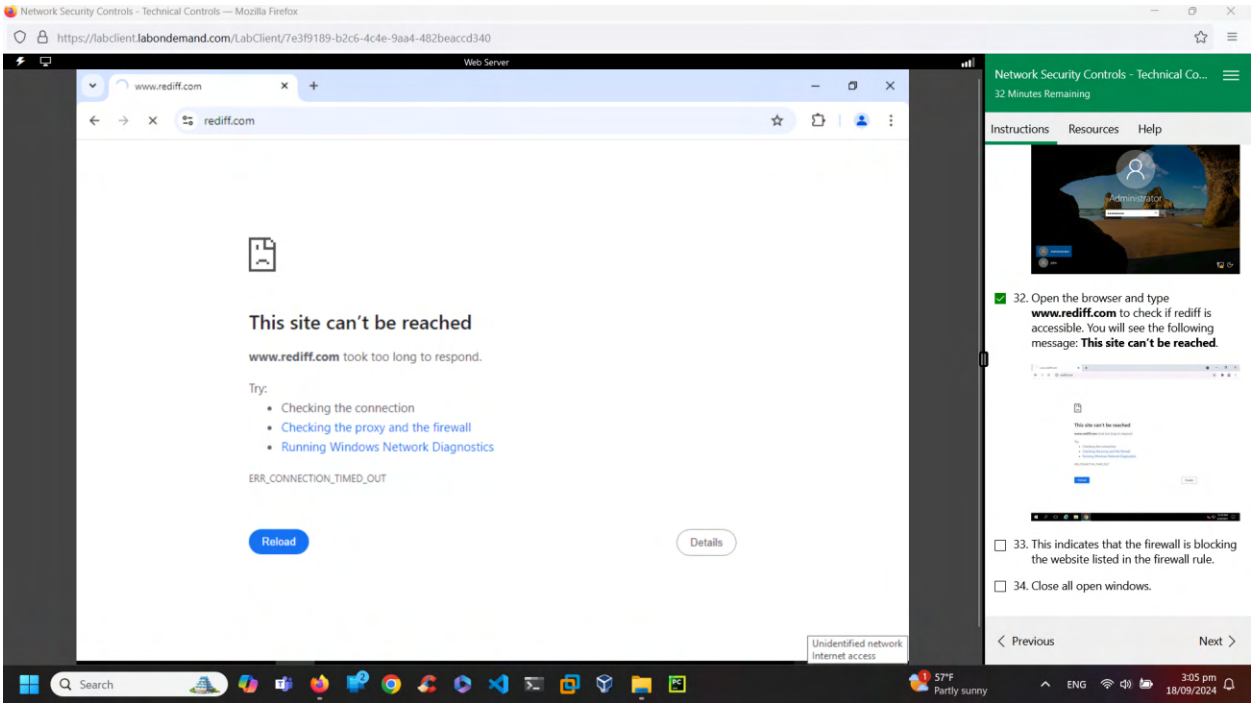

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Not secure https://10.10.1.1
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name pfSense.localdomain
User admin@10.10.1.2 (Local Database)
System Microsoft Azure
Netgate Device ID: d750ee037d178c05e5d6
BIOS Vendor: American Megatrends Inc.
Version: 090008
Release Date: Fri Dec 7 2018
Version 2.4.5-RELEASE-p1 (amd64)
built on Tue Jun 02 17:51:17 EDT 2020
FreeBSD 11.3-STABLE
Version 2.5.2 is available.
Version information updated at Wed Sep 18 1:22:53 UTC 2024
CPU Type Intel(R) Xeon(R) Gold 6262V CPU @ 1.90GHz
AES-NI CPU Crypto: Yes (inactive)
Kernel PTI Disabled
MDS Mitigation Inactive
Netgate Services And Support
Contract type Community Support
Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Upgrade Your Support
Community Support Resources
Netgate Global Support FAQ
Official pfSense Training by Netgate
Tuesday, September 17, 2024
Network Security Controls - Technical Co...
51 Minutes Remaining
Instructions
Resources
Help
10. The pfSense home page will appear, as shown in the screenshot below.
11. Navigate to the Firewall-->Aliases option menu from the main menu to add the list of websites for restricting access.
Previous
Next
Type here to search
26°C
10:47 PM
9/17/2024
Search
57°F
Partly sunny
ENG
2:47 pm
18/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Not secure https://10.10.1.1/firewall_aliases_edit.php?tab=ip
Firewall / Aliases / Edit
Properties
Name
Blocked websites
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description
Restrict the access of unwanted websites
A description may be entered here for administrative reference (not parsed).
Type
Host(s)
Host(s)
Hint
Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.
IP or FQDN
96.17.70.248
Site IP Address
Delete
www.rediff.com
Site URL
Delete
Save
Add Host
2 new notifications
Type here to search
26°C
10:53 PM
9/17/2024
Network Security Controls - Technical Co...
45 Minutes Remaining
Instructions
Resources
Help
Description: Site Url
Click Add Host button and add following IP address and description.
IP or FQDN: 84.53.185.208 (Viewed rediff.com IP address from Command Prompt)
Description: Site IP address
18. Click Save.
19. Click on Apply Changes button.
Previous
Next
Search
57°F
Partly sunny
ENG
2:53 pm
18/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Not secure https://10.10.1.1/firewall_aliases.php?tab=ip
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Aliases / IP
The alias list has been changed.
The changes must be applied for them to take effect.
Apply Changes
IP
Ports
URLs
All
Firewall Aliases IP
Name
Values
Description
Actions
BlockedWebsites
96.17.70.248, www.rediff.com
Restrict the access of unwanted websites
Add
Import
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Tuesday, September 17, 2024
Type here to search
26°C
10:53 PM
9/17/2024
Network Security Controls - Technical Co...
44 Minutes Remaining
Instructions
Resources
Help
20. You will see the following message:
The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload process.
21. Next, we will add a firewall rule in pfSense to block the websites listed in the aliases. To add the rule, click on Firewall-->Rules from the main menu in the pfSense web interface as shown in the screenshot below.
Previous
Next
Search
57°F
Partly sunny
ENG
2:53 pm
18/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Not secure https://10.10.1.1/firewall_rules_edit.php?if=lan&after=-1
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP/UDP
Choose which IP protocol this rule should match.
Source
Source
Invert match
any
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
2 new notifications
Type here to search
26°C
10:55 PM
9/17/2024
Network Security Controls - Technical Co...
42 Minutes Remaining
Instructions
Resources
Help
on top of the default rule.
24. Under Edit Firewall Rule section, set below details.
Action: Block
Interface: LAN
Address Family: IPv4
Protocol: TCP/UDP
Under Source section, select any from the dropdown.
25. Under Destination, select Single host or alias from the dropdown and type BlockedWebsites in the text box, select Destination Port Range as any.
Previous
Next
Search
57°F
Partly sunny
ENG
2:55 pm
18/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/7e3f9189-b2c6-4c4e-9aa4-482beaccd340
Admin Machine-1
Not secure https://10.10.1.1/firewall_rules.php?if=lan
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
3 /1.26 MiB
*
*
*
LAN Address
443 80
*
*
Anti-Lockout Rule
0 /0 B
IPv4 TCP/UDP
*
*
BlockedWebsites
*
*
none
Restrict access to unwanted Websites.
27 /1.71 GiB
IPv4 *
LAN net
*
*
*
*
none
Default allow LAN to any rule
0 /0 B
IPv6 *
LAN net
*
*
*
*
none
Default allow LAN IPv6 to any rule
Add
Add
Delete
Save
Separator
Type here to search
26°C
10:58 PM
9/17/2024
Network Security Controls - Technical Co...
40 Minutes Remaining
Instructions
Resources
Help
26. Scroll down, enter the text Restrict access to unwanted Websites in the Description field, and click Save.
27. The page will redirect to the Firewall/ Rules page. Click Apply Changes.
Previous
Next
Search
57°F
Partly sunny
ENG
2:58 pm
18/09/2024



Report:

Pfsense controls inbound and outbound rules using custom rules and helps to block access to malicious domains which reduce the probability of phishing attacks and helps the organization to be more productive, secure, less traffic by avoiding the employees to access unwanted websites. As a cyber technician, I have learnt to set a firewall policy/rule using pfsense which helps me to maintain a secure network.

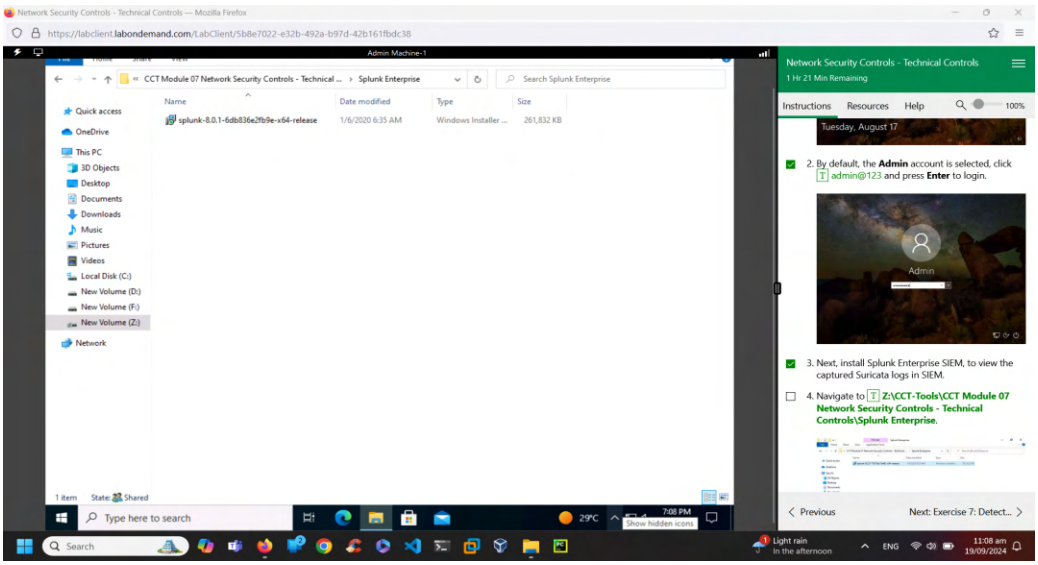
3. **Ilab Module no. and name:** 7. Network Security controls- Technical controls

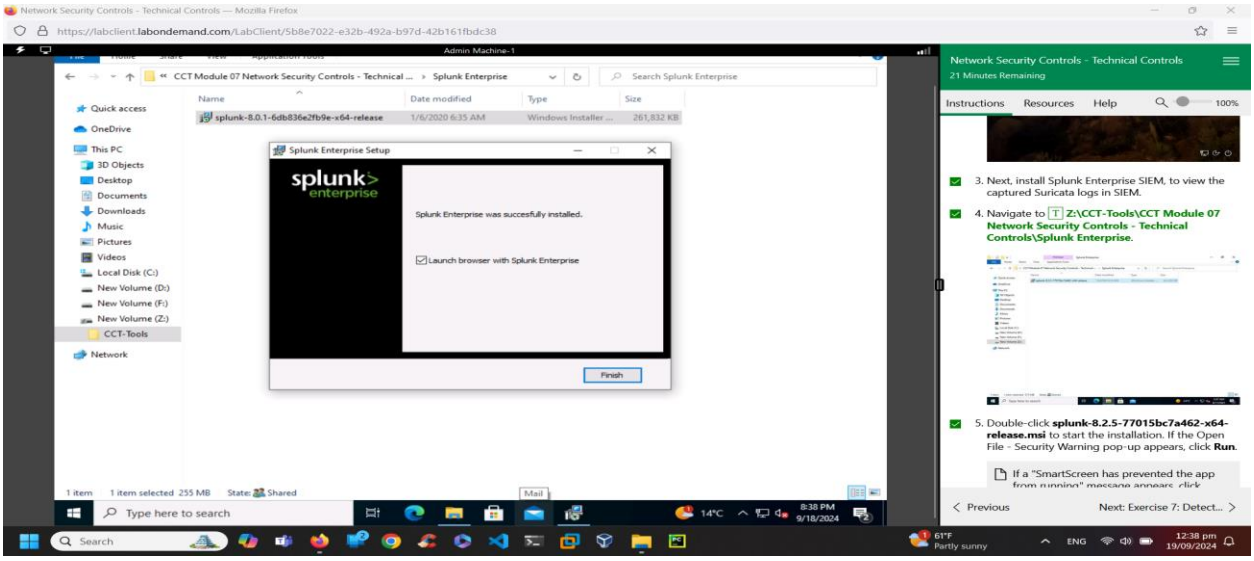
   Exercise no. and name: 3, Implement Network-based IDS Function using Suricata IDS

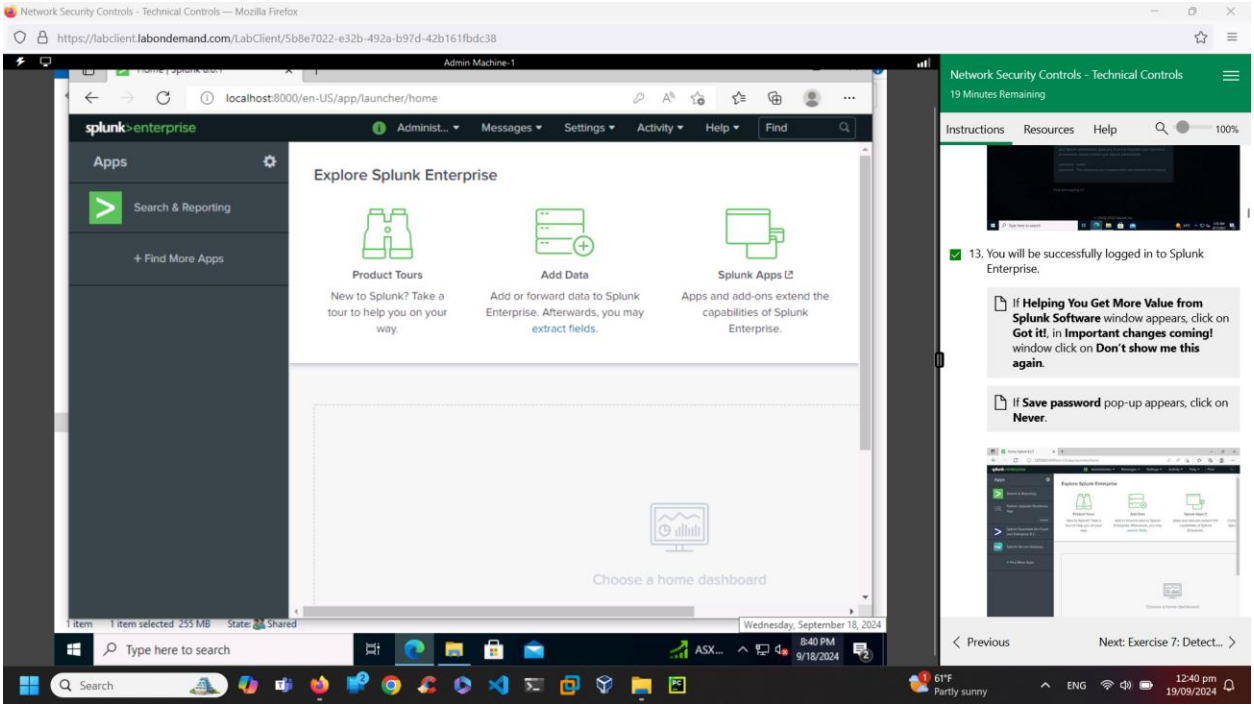
   Performed Date: 19/09/2024 and 20/09/2024

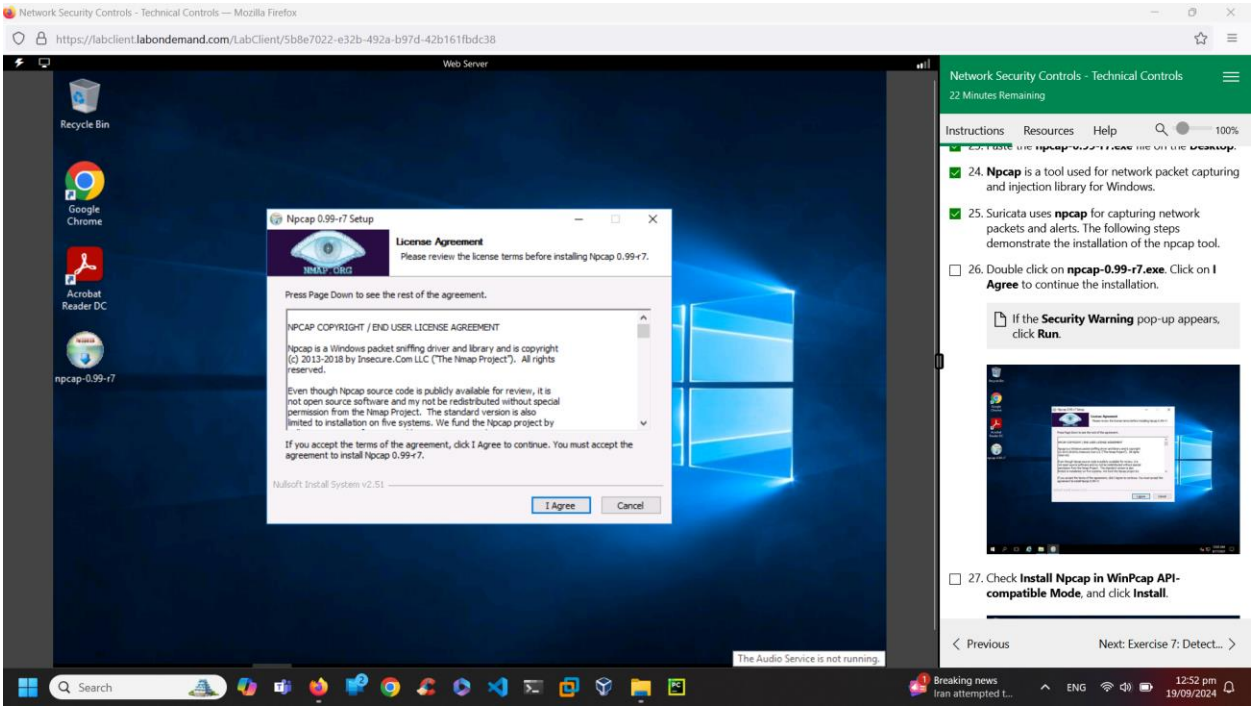
Summary:

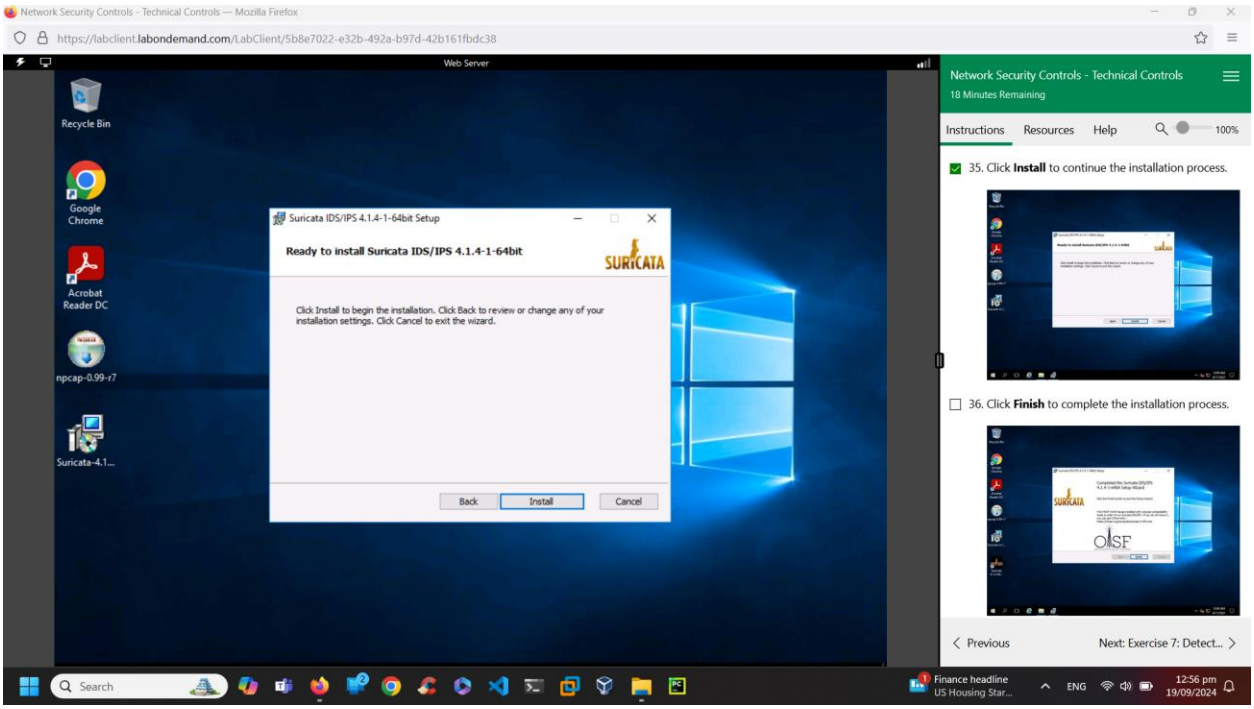
This lab demonstrates the installation of Splunk enterprise with Splunk universal forwarder. We also use Suricata IDS and npcap to log the data in fast log which integrates with Splunk to list the alerts, vulnerabilities and threats. It also involves some changes in the existing config file and create few new config files, run files and log files.

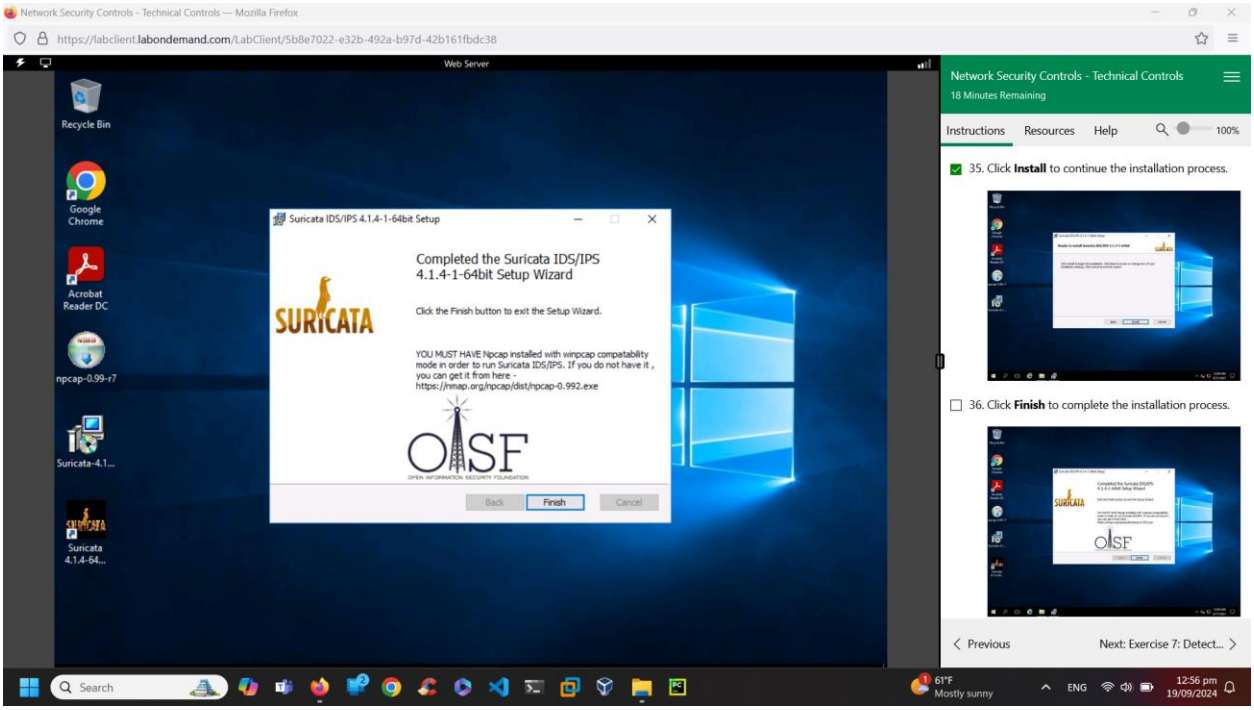

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Admin Machine-1
CCT Module 07 Network Security Controls - Technical ... › Splunk Enterprise
Search Splunk Enterprise
Name
Date modified
Type
Size
splunk-8.0.1-6db836e2fb9e-x64-release
1/6/2020 6:35 AM
Windows Installer ...
261,832 KB
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
New Volume (F:)
New Volume (Z:)
Network
1 item
State: Shared
Type here to search
29°C
7:08 PM
Show hidden icons
Search
Light rain
In the afternoon
ENG
11:08 am
19/09/2024
Network Security Controls - Technical Controls
1 Hr 21 Min Remaining
Instructions
Resources
Help
100%
Tuesday, August 17
2. By default, the Admin account is selected, click admin@123 and press Enter to login.
Admin
3. Next, install Splunk Enterprise SIEM, to view the captured Suricata logs in SIEM.
4. Navigate to Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Splunk Enterprise.
Previous
Next: Exercise 7: Detect...

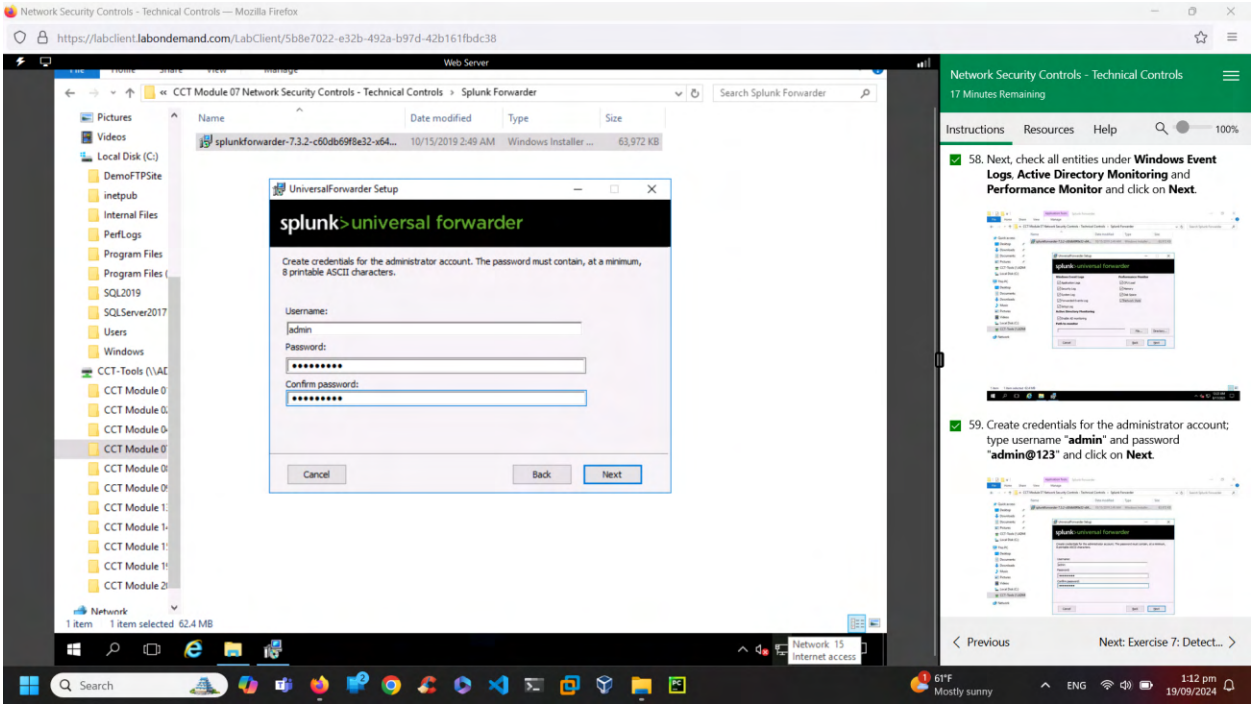

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Admin Machine-1
CCT Module 07 Network Security Controls - Technical ... › Splunk Enterprise
Search Splunk Enterprise
Name
Date modified
Type
Size
splunk-8.0.1-6db836e2fb9e-x64-release
1/6/2020 6:35 AM
Windows Installer ...
261,832 KB
Splunk Enterprise Setup
splunk> enterprise
Splunk Enterprise was succesfully installed.
Launch browser with Splunk Enterprise
Finish
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
New Volume (F:)
New Volume (Z:)
CCT-Tools
Network
1 item
1 item selected 255 MB
State: Shared
Mail
Type here to search
14°C
8:38 PM
9/18/2024
Search
61°F
Partly sunny
ENG
12:38 pm
19/09/2024
Network Security Controls - Technical Controls
21 Minutes Remaining
Instructions
Resources
Help
100%
3. Next, install Splunk Enterprise SIEM, to view the captured Suricata logs in SIEM.
4. Navigate to Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Splunk Enterprise.
5. Double-click splunk-8.2.5-77015bc7a462-x64-release.msi to start the installation. If the Open File - Security Warning pop-up appears, click Run.
If a "SmartScreen has prevented the app
Previous
Next: Exercise 7: Detect...

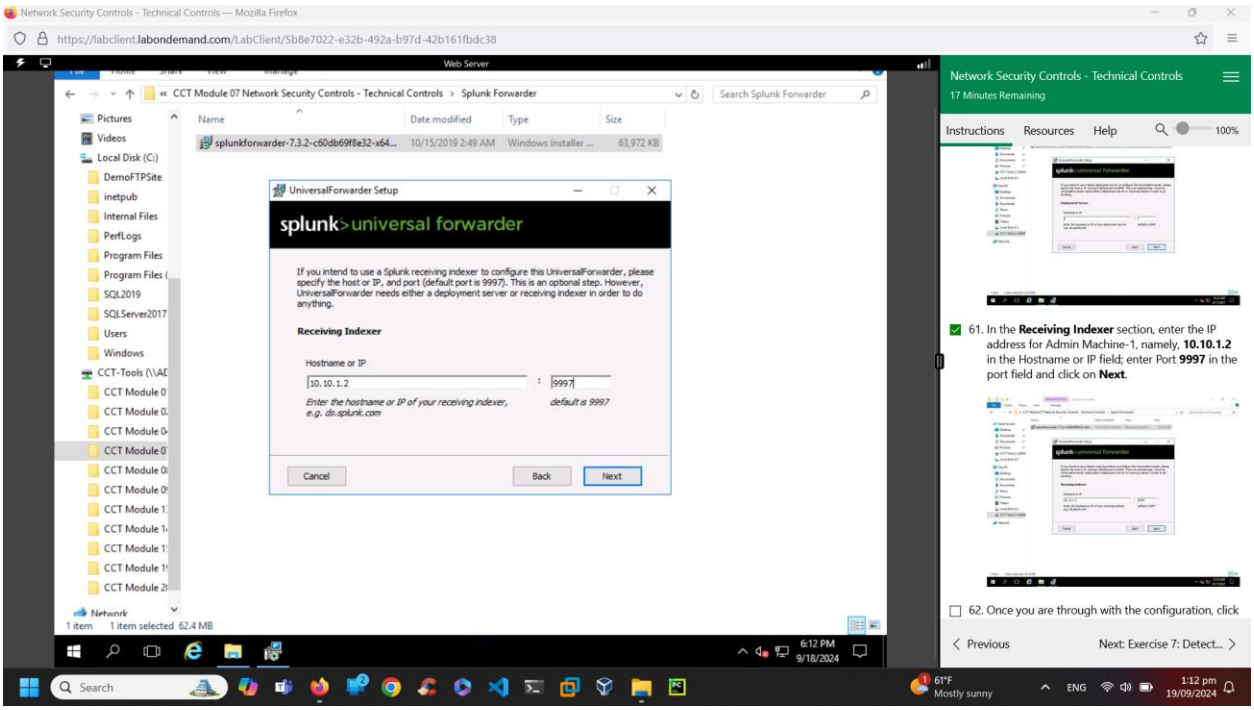

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Admin Machine-1
localhost:8000/en-US/app/launcher/home
splunk>enterprise
Administ...
Messages
Settings
Activity
Help
Find
Apps
Search & Reporting
+ Find More Apps
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.
Choose a home dashboard
Wednesday, September 18, 2024
Type here to search
8:40 PM
9/18/2024
Search
61°F
Partly sunny
ENG
12:40 pm
19/09/2024
Network Security Controls - Technical Controls
19 Minutes Remaining
Instructions
Resources
Help
100%
13. You will be successfully logged in to Splunk Enterprise.
If Helping You Get More Value from Splunk Software window appears, click on Got it!, in Important changes coming! window click on Don't show me this again.
If Save password pop-up appears, click on Never.
Previous
Next: Exercise 7: Detect...


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Web Server
Recycle Bin
Google Chrome
Acrobat Reader DC
npcap-0.99-r7
Npcap 0.99-r7 Setup
License Agreement
Please review the license terms before installing Npcap 0.99-r7.
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2018 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.
Even though Npcap source code is publicly available for review, it is not open source software and my not be redistributed without special permission from the Nmap Project. The standard version is also limited to installation on five systems. We fund the Npcap project by
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 0.99-r7.
Nullsoft Install System v2.51
I Agree
Cancel
The Audio Service is not running.
Search
Breaking news
Iran attempted t...
ENG
12:52 pm
19/09/2024
Network Security Controls - Technical Controls
22 Minutes Remaining
Instructions
Resources
Help
100%
24. Npcap is a tool used for network packet capturing and injection library for Windows.
25. Suricata uses npcap for capturing network packets and alerts. The following steps demonstrate the installation of the npcap tool.
26. Double click on npcap-0.99-r7.exe. Click on I Agree to continue the installation.
If the Security Warning pop-up appears, click Run.
27. Check Install Npcap in WinPcap API-compatible Mode, and click Install.
Previous
Next: Exercise 7: Detect...


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Web Server
Recycle Bin
Google Chrome
Acrobat Reader DC
npcap-0.99-r7
Suricata-4.1...
Suricata IDS/IPS 4.1.4-1-64bit Setup
Ready to install Suricata IDS/IPS 4.1.4-1-64bit
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel
Search
Finance headline
US Housing Star...
ENG
12:56 pm
19/09/2024
Network Security Controls - Technical Controls
18 Minutes Remaining
Instructions
Resources
Help
100%
35. Click Install to continue the installation process.
36. Click Finish to complete the installation process.
Previous
Next: Exercise 7: Detect...


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Web Server
Recycle Bin
Google Chrome
Acrobat Reader DC
npcap-0.99-r7
Suricata-4.1...
Suricata 4.1.4-64...
Suricata IDS/IPS 4.1.4-1-64bit Setup
Completed the Suricata IDS/IPS 4.1.4-1-64bit Setup Wizard
Click the Finish button to exit the Setup Wizard.
YOU MUST HAVE Npcap installed with winpcap compatability mode in order to run Suricata IDS/IPS. If you do not have it , you can get it from here - https://nmap.org/npcap/dist/npcap-0.992.exe
Back
Finish
Cancel
Search
61°F
Mostly sunny
ENG
12:56 pm
19/09/2024
Network Security Controls - Technical Controls
18 Minutes Remaining
Instructions
Resources
Help
100%
35. Click Install to continue the installation process.
36. Click Finish to complete the installation process.
Previous
Next: Exercise 7: Detect...


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Web Server
« CCT Module 07 Network Security Controls - Technical Controls › Splunk Forwarder
Search Splunk Forwarder
Name
Date modified
Type
Size
splunkforwarder-7.3.2-c60db69f8e32-x64...
10/15/2019 2:49 AM
Windows Installer ...
63,972 KB
UniversalForwarder Setup
splunk>universal forwarder
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.
Username:
admin
Password:
Confirm password:
Cancel
Back
Next
1 item
1 item selected 62.4 MB
Network 15
Internet access
Network Security Controls - Technical Controls
17 Minutes Remaining
Instructions
Resources
Help
100%
58. Next, check all entities under Windows Event Logs, Active Directory Monitoring and Performance Monitor and click on Next.
59. Create credentials for the administrator account; type username "admin" and password "admin@123" and click on Next.
Previous
Next: Exercise 7: Detect...
Search
61°F
Mostly sunny
ENG
1:12 pm
19/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Web Server
« CCT Module 07 Network Security Controls - Technical Controls › Splunk Forwarder
Search Splunk Forwarder
Name
Date modified
Type
Size
splunkforwarder-7.3.2-c60db69f8e32-x64...
10/15/2019 2:49 AM
Windows Installer ...
63,972 KB
UniversalForwarder Setup
splunk>universal forwarder
If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.
Receiving Indexer
Hostname or IP
10.10.1.2
9997
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com
default is 9997
Cancel
Back
Next
1 item
1 item selected 62.4 MB
6:12 PM
9/18/2024
Network Security Controls - Technical Controls
17 Minutes Remaining
Instructions
Resources
Help
100%
61. In the Receiving Indexer section, enter the IP address for Admin Machine-1, namely, 10.10.1.2 in the Hostname or IP field; enter Port 9997 in the port field and click on Next.
62. Once you are through with the configuration, click
Previous
Next: Exercise 7: Detect...
Search
61°F
Mostly sunny
ENG
1:12 pm
19/09/2024

Network Security Controls - Technical Controls — Mozilla Firefox

https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38

Web Server

Services

File Action View Help

Service Control

Windows is attempting to stop the following service on Local Computer...

SplunkForwarder Service

Close

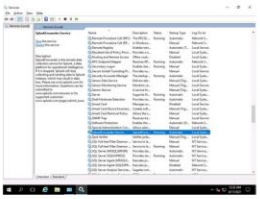
Activate Windows
Go to Settings to activate Windows.

Network Security Controls - Technical Controls

8 Minutes Remaining

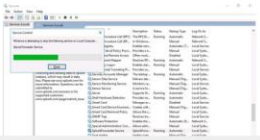
Instructions Resources Help 100%

opens, search for **SplunkForwarder Service**.



☐ 77. Click on **SplunkForwarder Service**, and then **Restart** the service.

If an error occurs while restarting, click **Start** again.



Previous Next: Exercise 7: Detect...

Search

61°F Mostly sunny

ENG 1:28 pm 19/09/2024

Network Security Controls - Technical Controls — Mozilla Firefox

https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38

Web Server

Recycle Bin

Administrator: C:\Windows\system32\cmd.exe - suricata.exe -c suricata.yaml -i 10.10.1.16

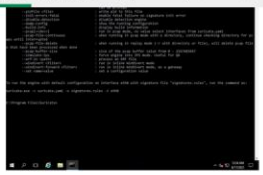
```
        --dump-config                   : show the running configuration
        --build-info                    : display build information
        --pcap[=<dev>]                  : run in pcap mode, no value select interfaces from suricata.yaml
        --pcap-file-continuous          : when running in pcap mode with a directory, continue checking directory f
or pcaps until interrupted
        --pcap-file-delete              : when running in replay mode (-r with directory or file), will delete pcap
files that have been processed when done
        --pcap-buffer-size              : size of the pcap buffer value from 0 - 2147483647
        --simulate-ips                  : force engine into IPS mode. Useful for QA
        --erf-in <path>                 : process an ERF file
        --windivert <filter>            : run in inline WinDivert mode
        --windivert-forward <filter>    : run in inline WinDivert mode, as a gateway
        --set name=value                : set a configuration value


To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command a
s:

suricata.exe -c suricata.yaml -s signatures.rules -i eth0


C:\Program Files\Suricata>suricata.exe -c suricata.yaml -i 10.10.1.16
18/9/2024 -- 18:31:08 - <Info> - Running as service: no
18/9/2024 -- 18:31:08 - <Info> - translated 10.10.1.16 to pcap device \Device\NPF_{4145D27B-2359-4013-9F71-D0D908E70D6A}

18/9/2024 -- 18:31:08 - <Notice> - This is Suricata version 4.1.4 RELEASE
18/9/2024 -- 18:31:08 - <Warning> - [ERRCODE: SC_ERR_NIC_OFFLOADING(284)] - NIC offloading on \Device\NPF_{4145D27B-2359
-4013-9F71-D0D908E70D6A}: Checksum IPv4 Rx: 0 Tx: 0 IPv6 Rx: 1 Tx: 1 LSOv1 IPv4: 0 LSOv2 IPv4: 0 IPv6: 0
18/9/2024 -- 18:31:08 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
```

Activate Windows
Go to Settings to activate Windows.

Network Security Controls - Technical Controls

5 Minutes Remaining

Instructions Resources Help 100%



☑ 80. Type the **suricata.exe -c suricata.yaml -i 10.10.1.16** command to run Suricata for capturing network traffic, and press **Enter**.

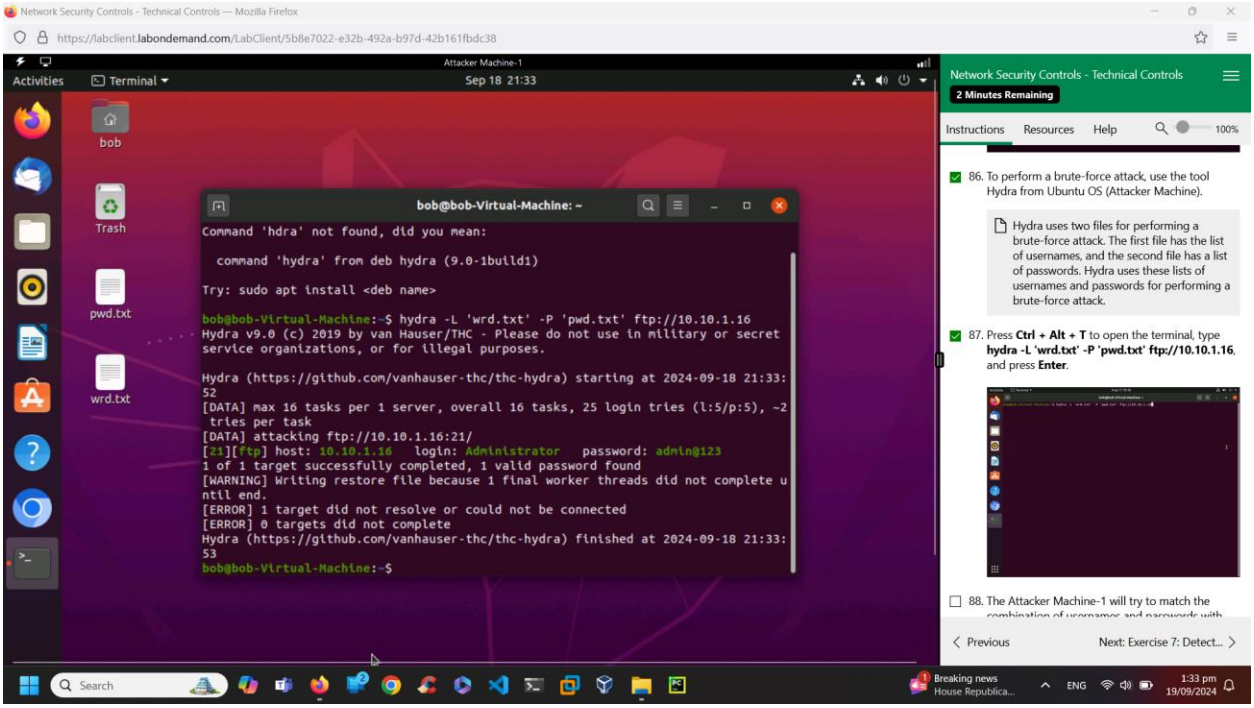
☑ 81. The Suricata engine will start. Leave the command prompt open and Suricata running.

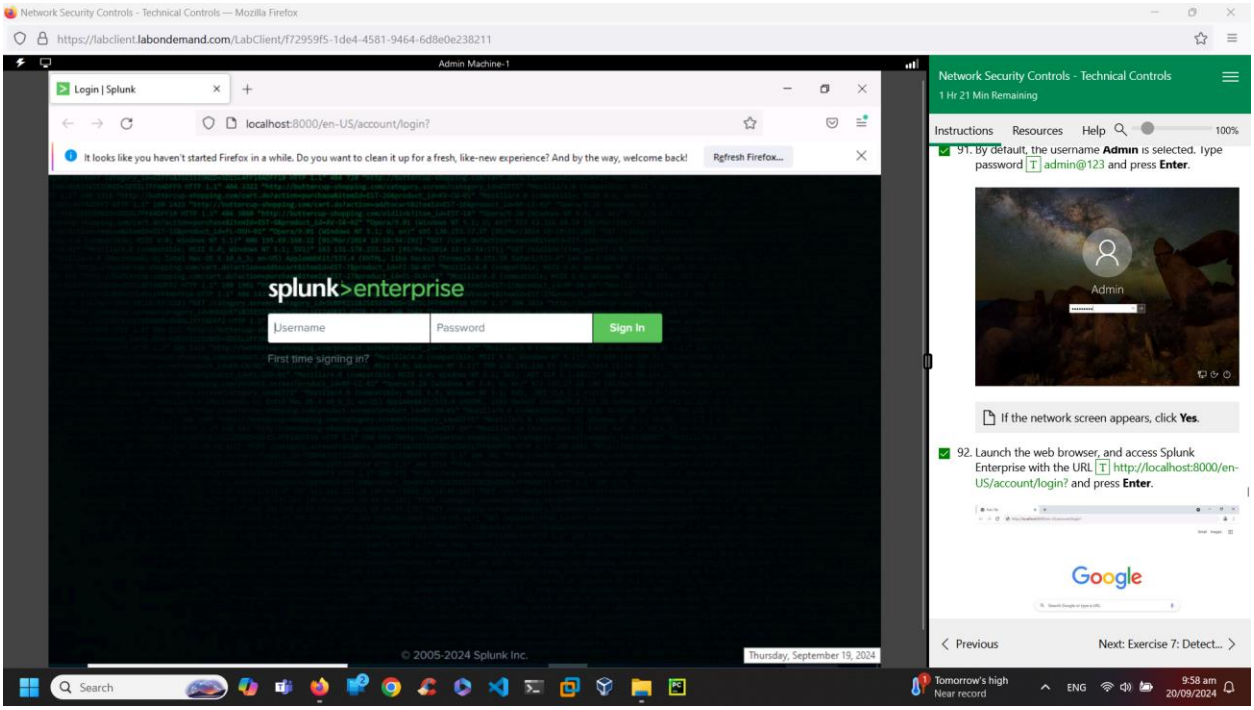
Previous Next: Exercise 7: Detect...

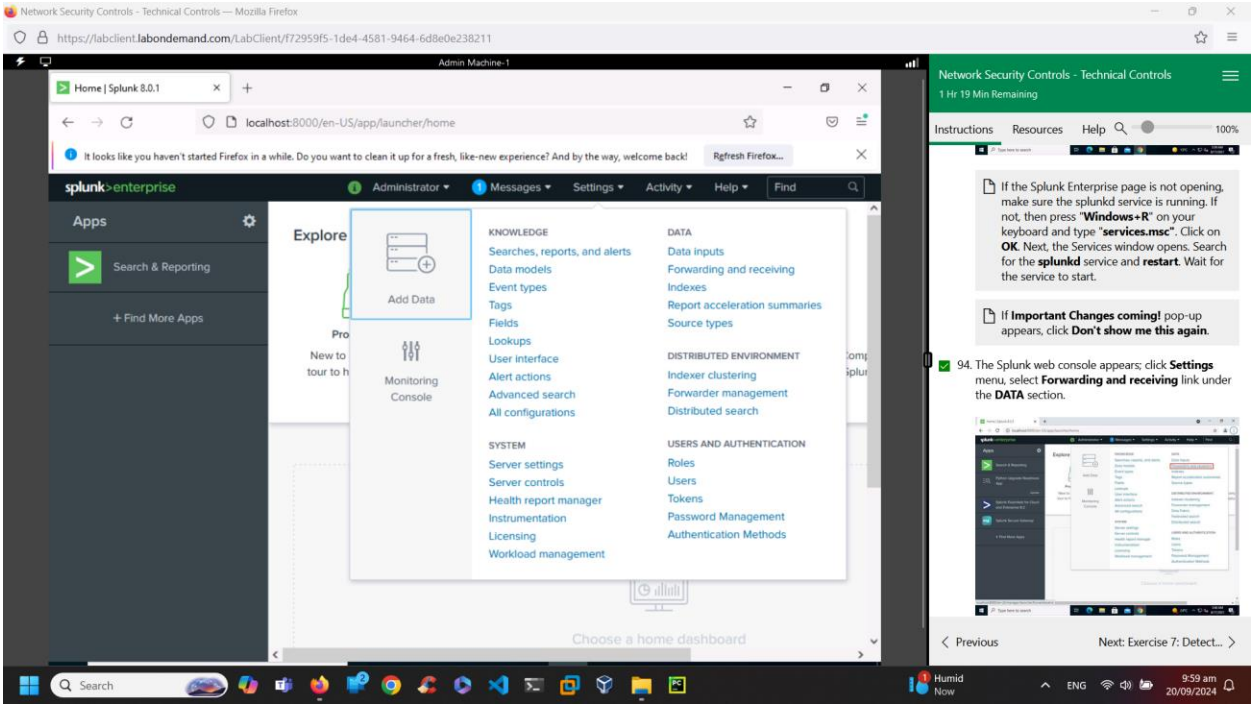
Search

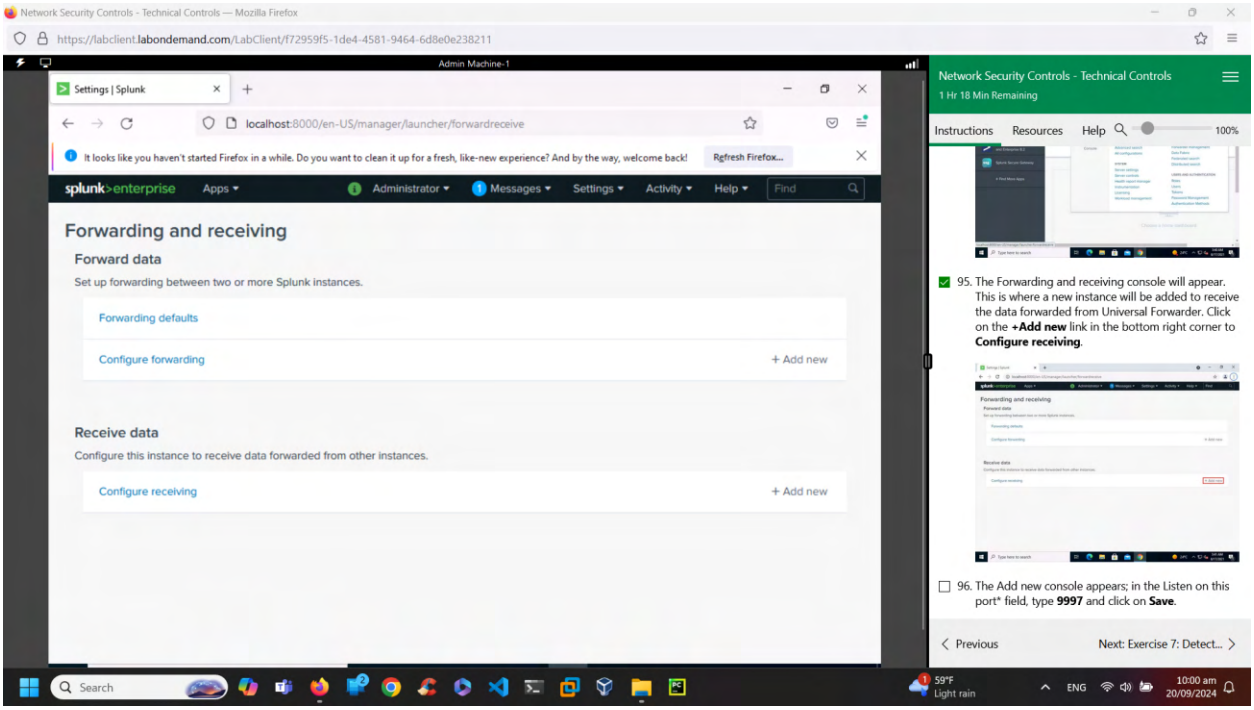
62°F Mostly sunny

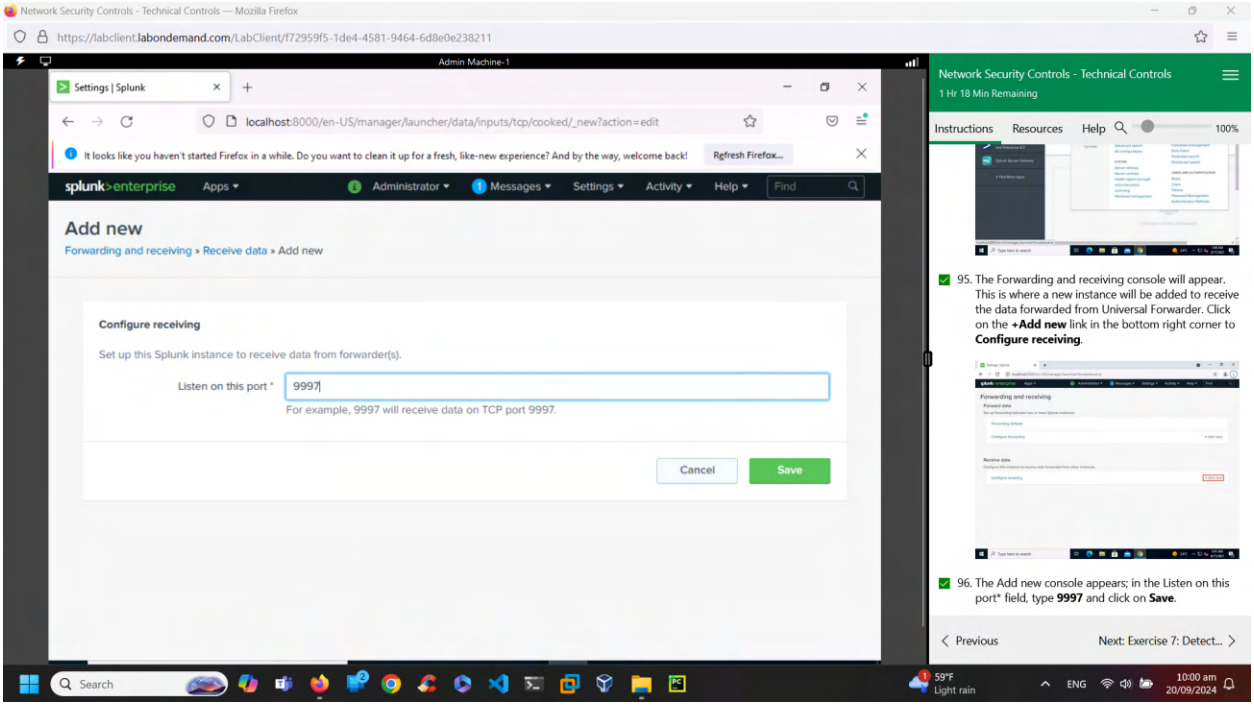
ENG 1:31 pm 19/09/2024

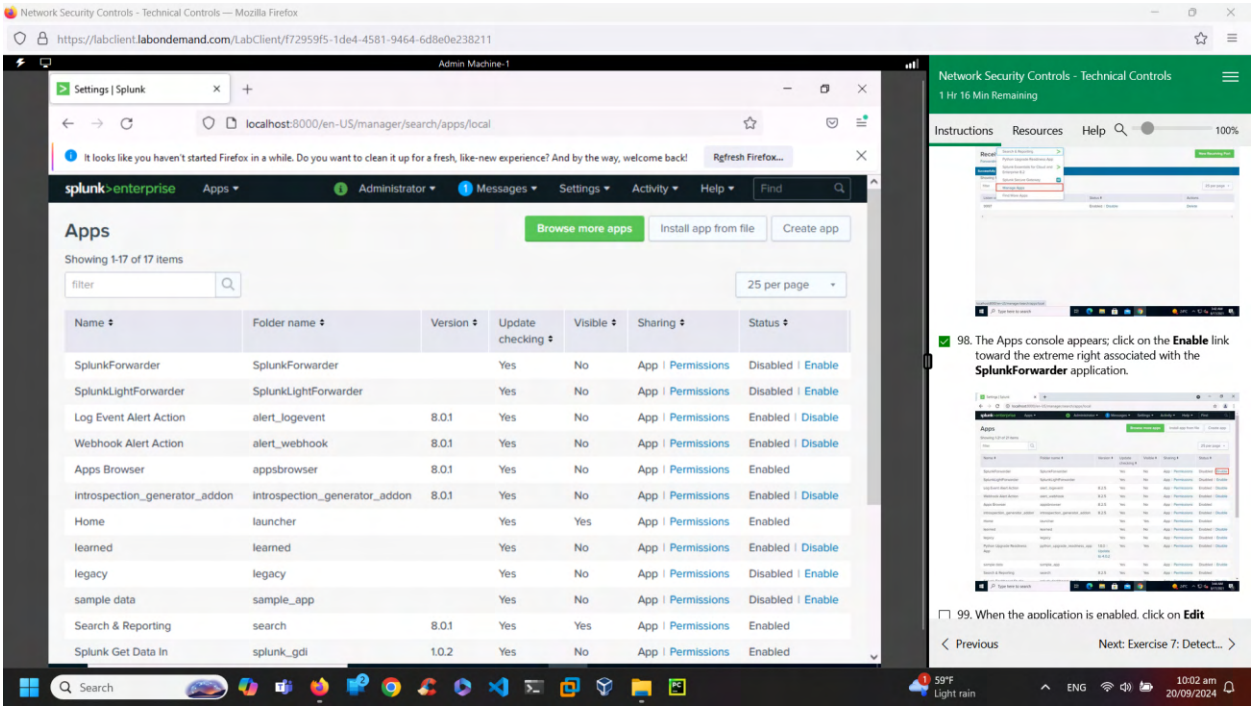

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/5b8e7022-e32b-492a-b97d-42b161fbdc38
Attacker Machine-1
Activities
Terminal
Sep 18 21:33
bob
Trash
pwd.txt
wrd.txt
bob@bob-Virtual-Machine: ~
Command 'hdra' not found, did you mean:
command 'hydra' from deb hydra (9.0-1build1)
Try: sudo apt install <deb name>
bob@bob-Virtual-Machine:~$ hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-18 21:33:52
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://10.10.1.16:21/
[21][ftp] host: 10.10.1.16 login: Administrator password: admin@123
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-18 21:33:53
bob@bob-Virtual-Machine:~$
Network Security Controls - Technical Controls
2 Minutes Remaining
Instructions
Resources
Help
100%
86. To perform a brute-force attack, use the tool Hydra from Ubuntu OS (Attacker Machine).
Hydra uses two files for performing a brute-force attack. The first file has the list of usernames, and the second file has a list of passwords. Hydra uses these lists of usernames and passwords for performing a brute-force attack.
87. Press Ctrl + Alt + T to open the terminal, type hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16, and press Enter.
88. The Attacker Machine-1 will try to match the
Previous
Next: Exercise 7: Detect...
Search
Breaking news
House Republica...
ENG
1:33 pm
19/09/2024

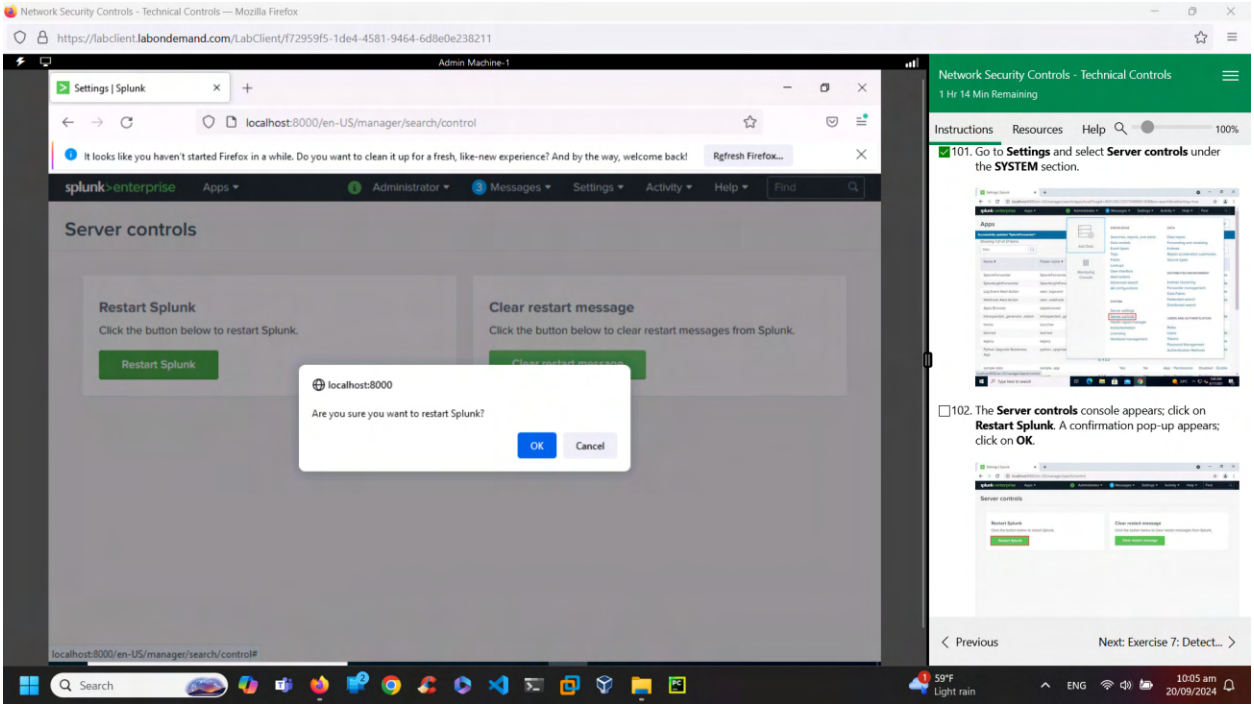

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Login | Splunk
localhost:8000/en-US/account/login?
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
splunk>enterprise
Username
Password
Sign In
First time signing in?
© 2005-2024 Splunk Inc.
Thursday, September 19, 2024
Network Security Controls - Technical Controls
1 Hr 21 Min Remaining
Instructions
Resources
Help
100%
91. By default, the username Admin is selected. Type password admin@123 and press Enter.
Admin
If the network screen appears, click Yes.
92. Launch the web browser, and access Splunk Enterprise with the URL http://localhost:8000/en-US/account/login? and press Enter.
Google
Previous
Next: Exercise 7: Detect...
Search
Tomorrow's high
Near record
ENG
9:58 am
20/09/2024

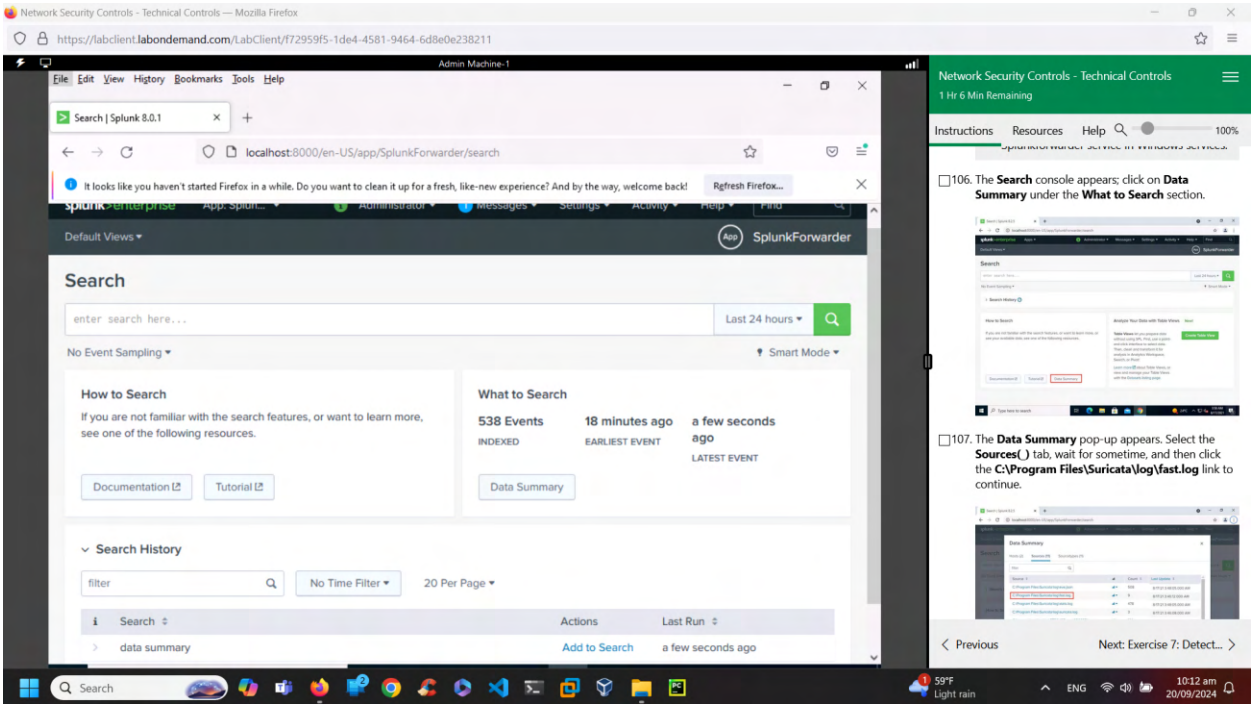

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Home | Splunk 8.0.1
localhost:8000/en-US/app/launcher/home
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
splunk>enterprise
Administrator
Messages
Settings
Activity
Help
Find
Apps
Search & Reporting
+ Find More Apps
Explore
Add Data
Monitoring Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
SYSTEM
Server settings
Server controls
Health report manager
Instrumentation
Licensing
Workload management
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password Management
Authentication Methods
Choose a home dashboard
Search
Humid
Now
ENG
9:59 am
20/09/2024
Network Security Controls - Technical Controls
1 Hr 19 Min Remaining
Instructions
Resources
Help
100%
If the Splunk Enterprise page is not opening, make sure the splunkd service is running. If not, then press "Windows+R" on your keyboard and type "services.msc". Click on OK. Next, the Services window opens. Search for the splunkd service and restart. Wait for the service to start.
If Important Changes coming! pop-up appears, click Don't show me this again.
94. The Splunk web console appears; click Settings menu, select Forwarding and receiving link under the DATA section.
Previous
Next: Exercise 7: Detect...

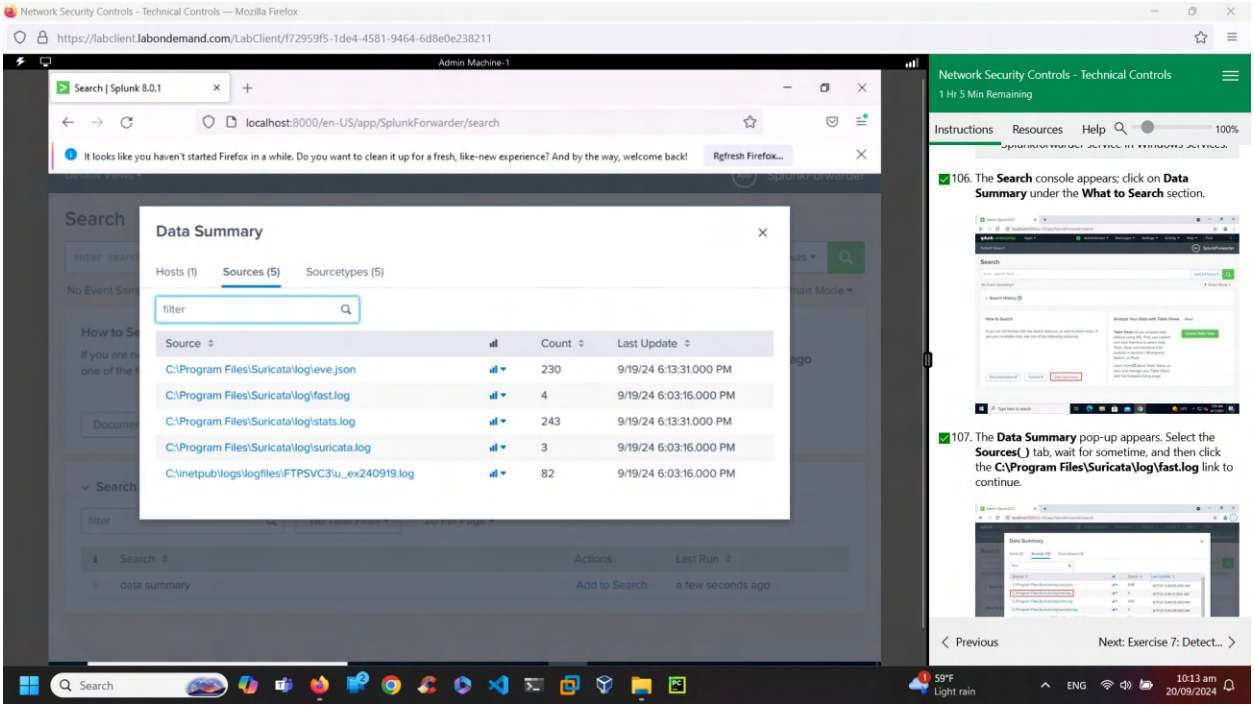

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Settings | Splunk
localhost:8000/en-US/manager/launcher/forwardreceive
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Forwarding and receiving
Forward data
Set up forwarding between two or more Splunk instances.
Forwarding defaults
Configure forwarding
+ Add new
Receive data
Configure this instance to receive data forwarded from other instances.
Configure receiving
+ Add new
Search
59°F
Light rain
ENG
10:00 am
20/09/2024
Network Security Controls - Technical Controls
1 Hr 18 Min Remaining
Instructions
Resources
Help
100%
95. The Forwarding and receiving console will appear. This is where a new instance will be added to receive the data forwarded from Universal Forwarder. Click on the +Add new link in the bottom right corner to Configure receiving.
96. The Add new console appears; in the Listen on this port* field, type 9997 and click on Save.
Previous
Next: Exercise 7: Detect...

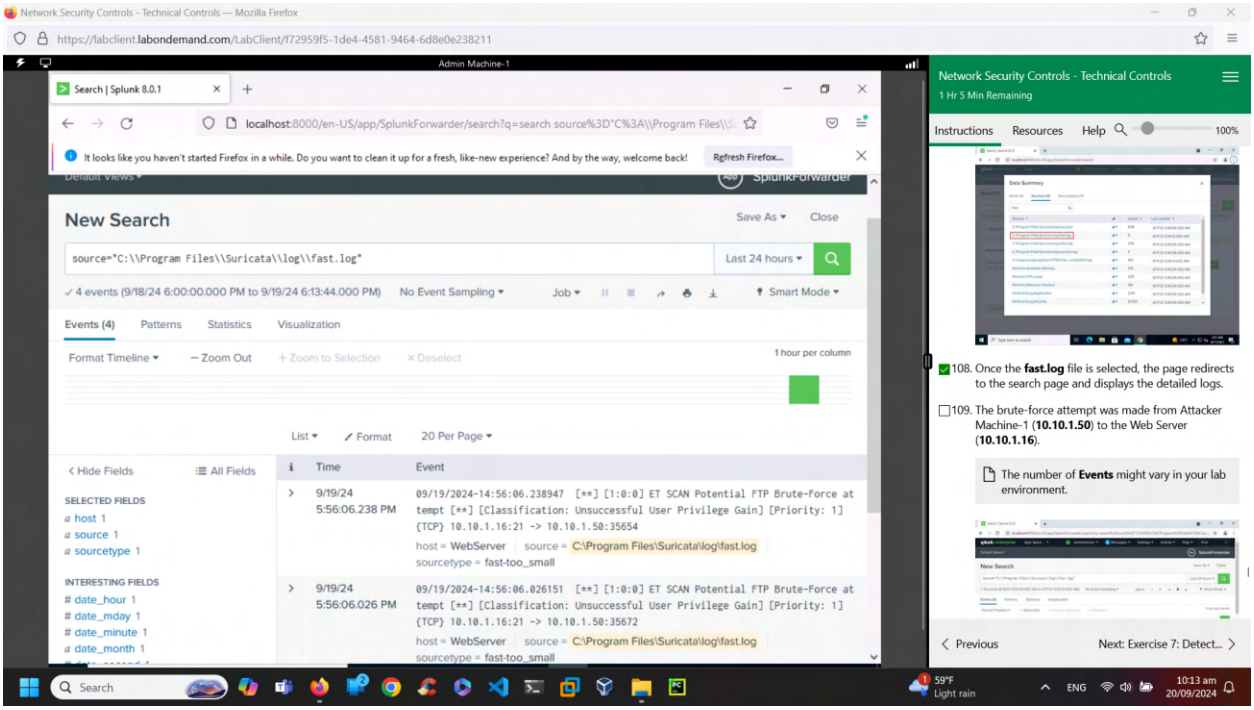

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Settings | Splunk
localhost:8000/en-US/manager/launcher/data/inputs/tcp/cooked/_new?action=edit
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add new
Forwarding and receiving » Receive data » Add new
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).
Listen on this port *
9997
For example, 9997 will receive data on TCP port 9997.
Cancel
Save
Network Security Controls - Technical Controls
1 Hr 18 Min Remaining
Instructions
Resources
Help
100%
95. The Forwarding and receiving console will appear. This is where a new instance will be added to receive the data forwarded from Universal Forwarder. Click on the +Add new link in the bottom right corner to Configure receiving.
96. The Add new console appears; in the Listen on this port* field, type 9997 and click on Save.
Previous
Next: Exercise 7: Detect...
Search
59°F
Light rain
ENG
10:00 am
20/09/2024

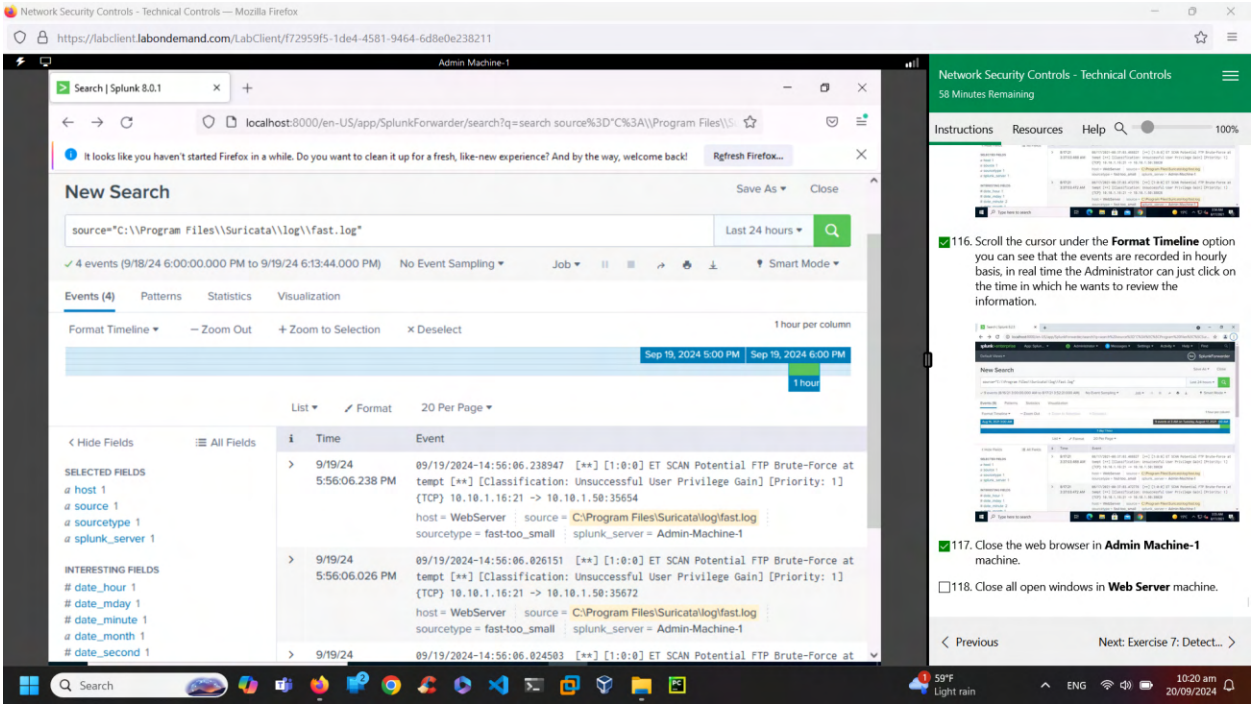

Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Settings | Splunk
localhost:8000/en-US/manager/search/apps/local
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Browse more apps
Install app from file
Create app
Showing 1-17 of 17 items
filter
25 per page
Name
Folder name
Version
Update checking
Visible
Sharing
Status
SplunkForwarder | SplunkForwarder | | Yes | No | App | Permissions | Disabled | Enable
SplunkLightForwarder | SplunkLightForwarder | | Yes | No | App | Permissions | Disabled | Enable
Log Event Alert Action | alert_logevent | 8.0.1 | Yes | No | App | Permissions | Enabled | Disable
Webhook Alert Action | alert_webhook | 8.0.1 | Yes | No | App | Permissions | Enabled | Disable
Apps Browser | appsbrowser | 8.0.1 | Yes | No | App | Permissions | Enabled
introspection_generator_addon | introspection_generator_addon | 8.0.1 | Yes | No | App | Permissions | Enabled | Disable
Home | launcher | | Yes | Yes | App | Permissions | Enabled
learned | learned | | Yes | No | App | Permissions | Enabled | Disable
legacy | legacy | | Yes | No | App | Permissions | Disabled | Enable
sample data | sample_app | | Yes | No | App | Permissions | Disabled | Enable
Search & Reporting | search | 8.0.1 | Yes | Yes | App | Permissions | Enabled
Splunk Get Data In | splunk_gdi | 1.0.2 | Yes | No | App | Permissions | Enabled
Network Security Controls - Technical Controls
1 Hr 16 Min Remaining
Instructions
Resources
Help
100%
98. The Apps console appears; click on the Enable link toward the extreme right associated with the SplunkForwarder application.
99. When the application is enabled, click on Edit
Previous
Next: Exercise 7: Detect...
Search
59°F
Light rain
ENG
10:02 am
20/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Settings | Splunk
localhost:8000/en-US/manager/search/control
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Server controls
Restart Splunk
Click the button below to restart Splunk.
Restart Splunk
Clear restart message
Click the button below to clear restart messages from Splunk.
localhost:8000
Are you sure you want to restart Splunk?
OK
Cancel
localhost:8000/en-US/manager/search/control#
Search
59°F
Light rain
ENG
10:05 am
20/09/2024
Network Security Controls - Technical Controls
1 Hr 14 Min Remaining
Instructions
Resources
Help
100%
101. Go to Settings and select Server controls under the SYSTEM section.
102. The Server controls console appears; click on Restart Splunk. A confirmation pop-up appears; click on OK.
Previous
Next: Exercise 7: Detect...


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
File Edit View History Bookmarks Tools Help
Search | Splunk 8.0.1
localhost:8000/en-US/app/SplunkForwarder/search
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Default Views
SplunkForwarder
Search
enter search here...
Last 24 hours
No Event Sampling
Smart Mode
How to Search
If you are not familiar with the search features, or want to learn more, see one of the following resources.
Documentation
Tutorial
What to Search
538 Events
INDEXED
18 minutes ago
EARLIEST EVENT
a few seconds ago
LATEST EVENT
Data Summary
Search History
filter
No Time Filter
20 Per Page
Search
Actions
Last Run
data summary
Add to Search
a few seconds ago
Search
59°F
Light rain
ENG
10:12 am
20/09/2024
Network Security Controls - Technical Controls
1 Hr 6 Min Remaining
Instructions
Resources
Help
100%
106. The Search console appears; click on Data Summary under the What to Search section.
107. The Data Summary pop-up appears. Select the Sources(_) tab, wait for sometime, and then click the C:\Program Files\Suricata\log\fast.log link to continue.
Previous
Next: Exercise 7: Detect...


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Search | Splunk 8.0.1
localhost:8000/en-US/app/SplunkForwarder/search
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Data Summary
Hosts (1)
Sources (5)
Sourcetypes (5)
filter
Source
Count
Last Update
C:\Program Files\Suricata\log\eve.json 230 9/19/24 6:13:31.000 PM
C:\Program Files\Suricata\log\fast.log 4 9/19/24 6:03:16.000 PM
C:\Program Files\Suricata\log\stats.log 243 9/19/24 6:13:31.000 PM
C:\Program Files\Suricata\log\suricata.log 3 9/19/24 6:03:16.000 PM
C:\inetpub\logs\logfiles\FTPSVC3\u_ex240919.log 82 9/19/24 6:03:16.000 PM
Network Security Controls - Technical Controls
1 Hr 5 Min Remaining
Instructions
Resources
Help
100%
106. The Search console appears; click on Data Summary under the What to Search section.
107. The Data Summary pop-up appears. Select the Sources(_) tab, wait for sometime, and then click the C:\Program Files\Suricata\log\fast.log link to continue.
Previous
Next: Exercise 7: Detect...
Search
59°F Light rain
ENG
10:13 am 20/09/2024


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Search | Splunk 8.0.1
localhost:8000/en-US/app/SplunkForwarder/search?q=search source%3D"C%3A\\Program Files\\S
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
New Search
Save As
Close
source="C:\\Program Files\\Suricata\\log\\fast.log"
Last 24 hours
4 events (9/18/24 6:00:00.000 PM to 9/19/24 6:13:44.000 PM)
No Event Sampling
Job
Smart Mode
Events (4)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
date_month 1
9/19/24 5:56:06.238 PM
09/19/2024-14:56:06.238947 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:35654
host = WebServer source = C:\Program Files\Suricata\log\fast.log
sourcetype = fast-too_small
9/19/24 5:56:06.026 PM
09/19/2024-14:56:06.026151 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:35672
host = WebServer source = C:\Program Files\Suricata\log\fast.log
sourcetype = fast-too_small
Network Security Controls - Technical Controls
1 Hr 5 Min Remaining
Instructions
Resources
Help
100%
108. Once the fast.log file is selected, the page redirects to the search page and displays the detailed logs.
109. The brute-force attempt was made from Attacker Machine-1 (10.10.1.50) to the Web Server (10.10.1.16).
The number of Events might vary in your lab environment.
Previous
Next: Exercise 7: Detect...
Search
59°F Light rain
ENG
10:13 am 20/09/2024



Report:

The tools like Suricata IDS/IPS, npcap, Splunk are used to monitor, protect and analyze network activities and events. It analyzes the attack patterns and find it as a brute force attack in the lab scenario. Suricata sends the alerts to Splunk via fast log file. SIEM like Splunk is used to detect, respond, analyse the events and works in integration with IDS/IPS tools for better performance. Npcap is used to capture the network packets in windows.

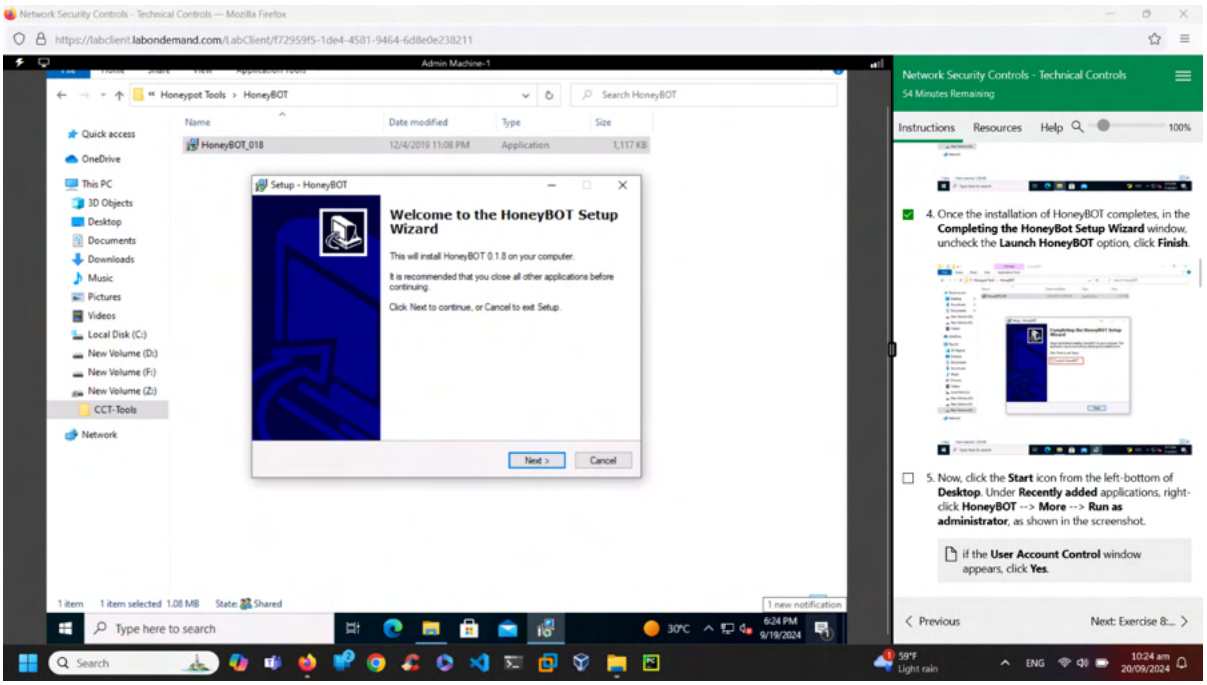
As a Cyber technician, IDS/IPS, SIEM are the important tools and strategies to monitor network traffic, detect security threats and block malicious activities

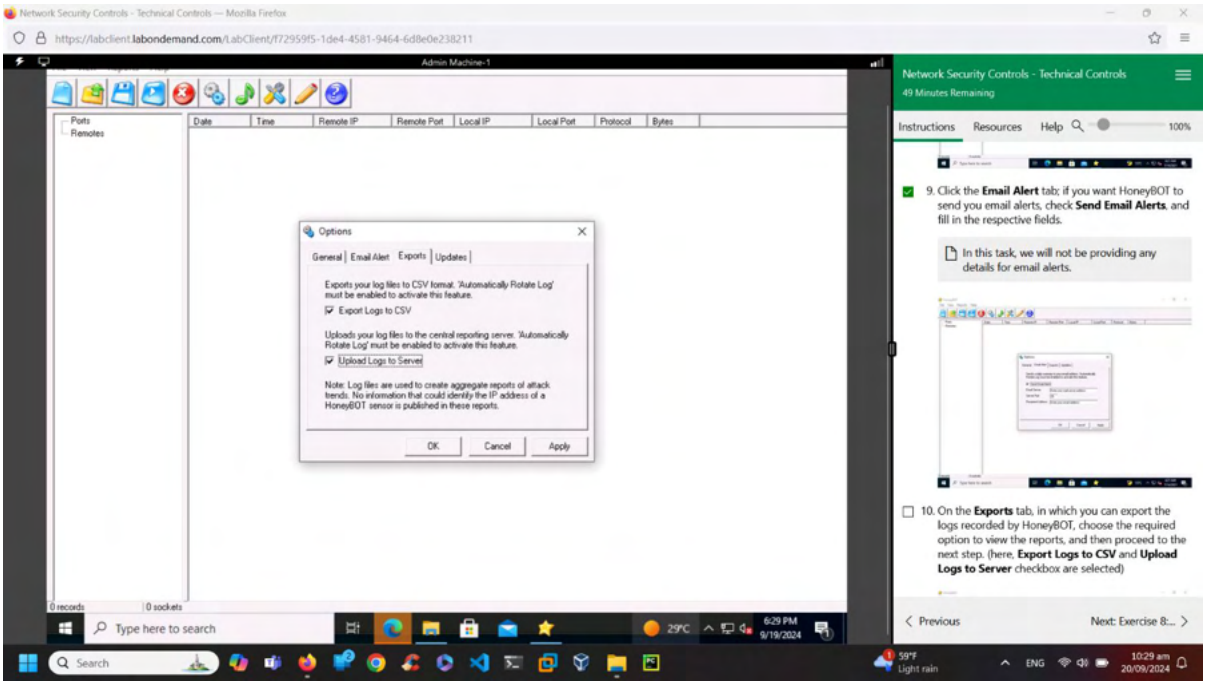
4. **Ilab Module no. and name:** 7. Network Security controls- Technical controls

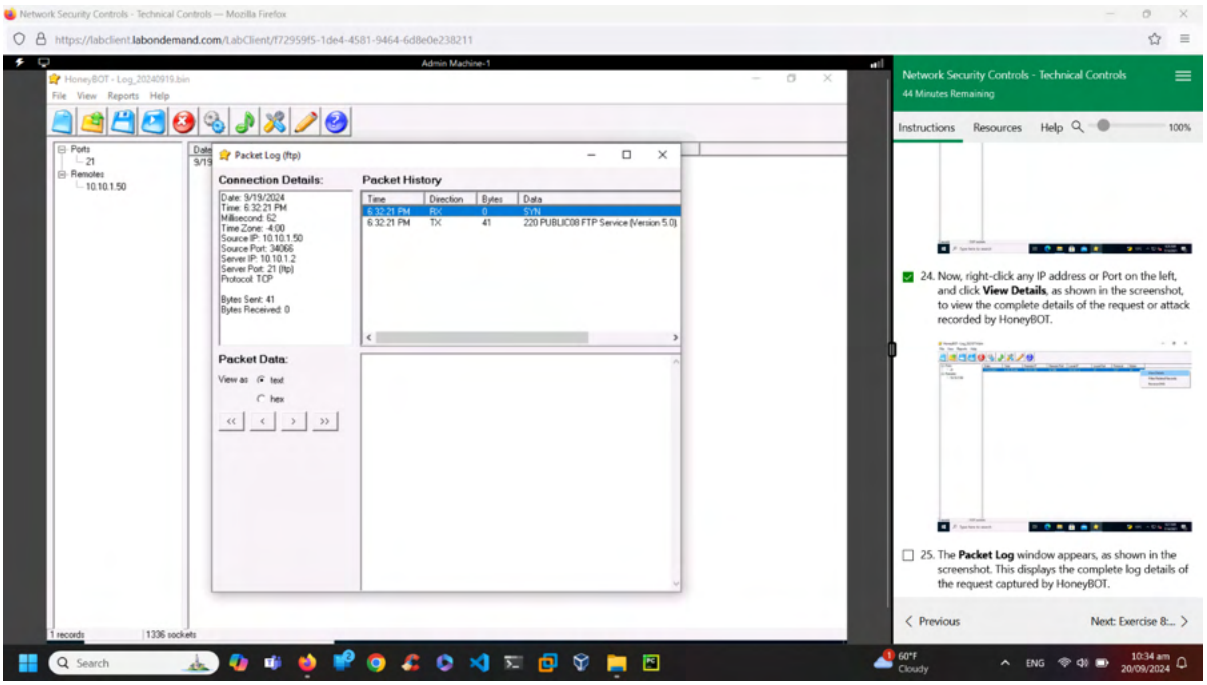
   Exercise no. and name: 7, Detect Malicious Network Traffic using HoneyBOT
   Performed Date: 19/09/2024 and 20/09/2024

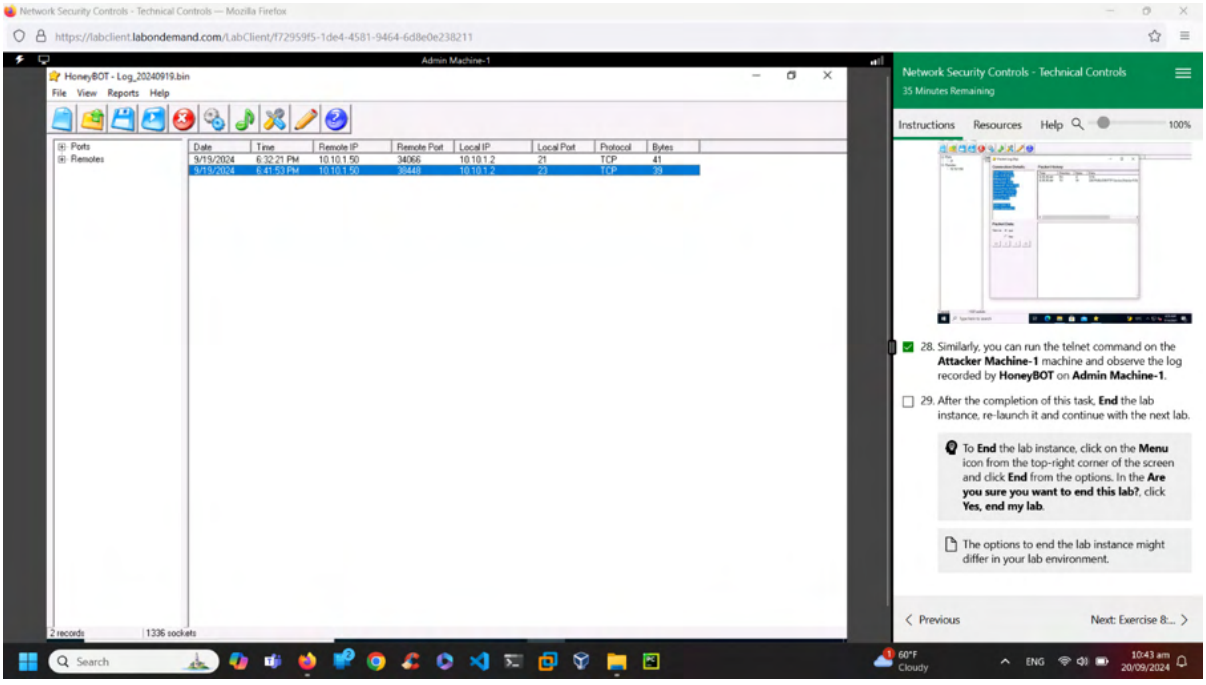
Summary:

This lab involves installation of HoneyBOT, involves configuring it with email alerts, export the log files in Admin Machine1. Once it is done, trying to access Admin Machine1 from attacker machine using port number 21(FTP) and 23(Telnet) using terminal. The logs are collected with Ip addresses, port numbers and some other details as shown in the screenshots.


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Honeypot Tools › HoneyBOT
Search HoneyBOT
Name
Date modified
Type
Size
HoneyBOT_018
12/4/2019 11:08 PM
Application
1,117 KB
Setup - HoneyBOT
Welcome to the HoneyBOT Setup Wizard
This will install HoneyBOT 0.1.8 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel
Network Security Controls - Technical Controls
54 Minutes Remaining
Instructions
Resources
Help
100%
4. Once the installation of HoneyBOT completes, in the Completing the HoneyBot Setup Wizard window, uncheck the Launch HoneyBOT option, click Finish.
5. Now, click the Start icon from the left-bottom of Desktop. Under Recently added applications, right-click HoneyBOT --> More --> Run as administrator, as shown in the screenshot.
if the User Account Control window appears, click Yes.
Previous
Next: Exercise 8:...


Network Security Controls - Technical Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/f72959f5-1de4-4581-9464-6d8e0e238211
Admin Machine-1
Ports
Remotes
Date
Time
Remote IP
Remote Port
Local IP
Local Port
Protocol
Bytes
Options
General
Email Alert
Exports
Updates
Export Logs to CSV
Upload Logs to Server
OK
Cancel
Apply
Network Security Controls - Technical Controls
49 Minutes Remaining
Instructions
Resources
Help
100%
9. Click the Email Alert tab; if you want HoneyBOT to send you email alerts, check Send Email Alerts, and fill in the respective fields.
In this task, we will not be providing any details for email alerts.
10. On the Exports tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (here, Export Logs to CSV and Upload Logs to Server checkbox are selected)
Previous
Next: Exercise 8:...





Report:

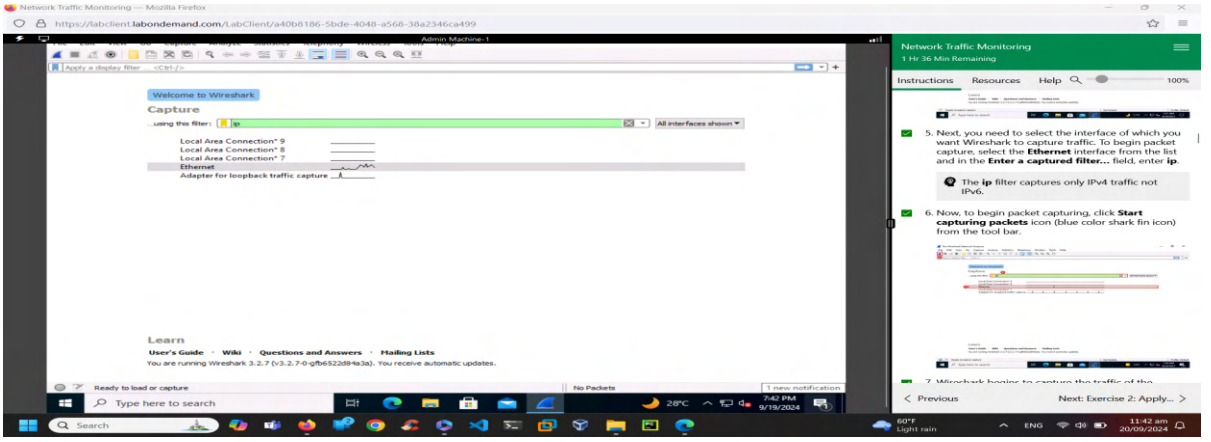
As a cyber technician, it helps me to understand how deployment of HoneyBOT in a network logs unauthorized access attempts with attacker's IP address details and how immediate alertness through email enhances live security. So, it shows the gaps in the network security and makes me to understand stronger access controls and firewall rules are required to mitigate them.

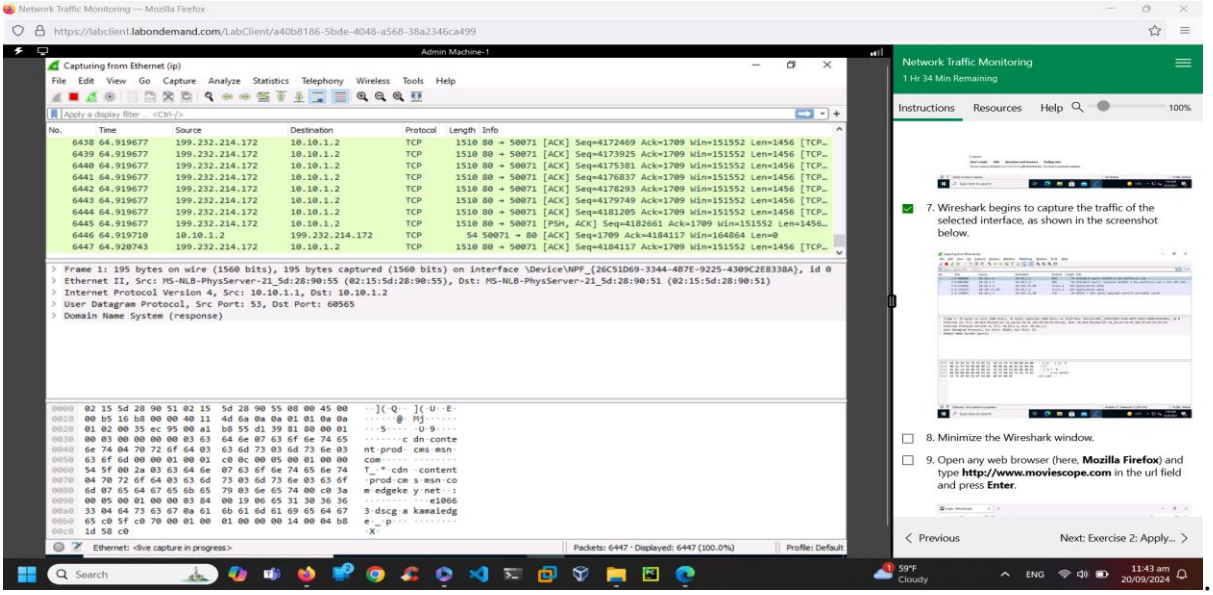
5. **Ilab Module no. and name:** 17. Network Traffic Monitoring

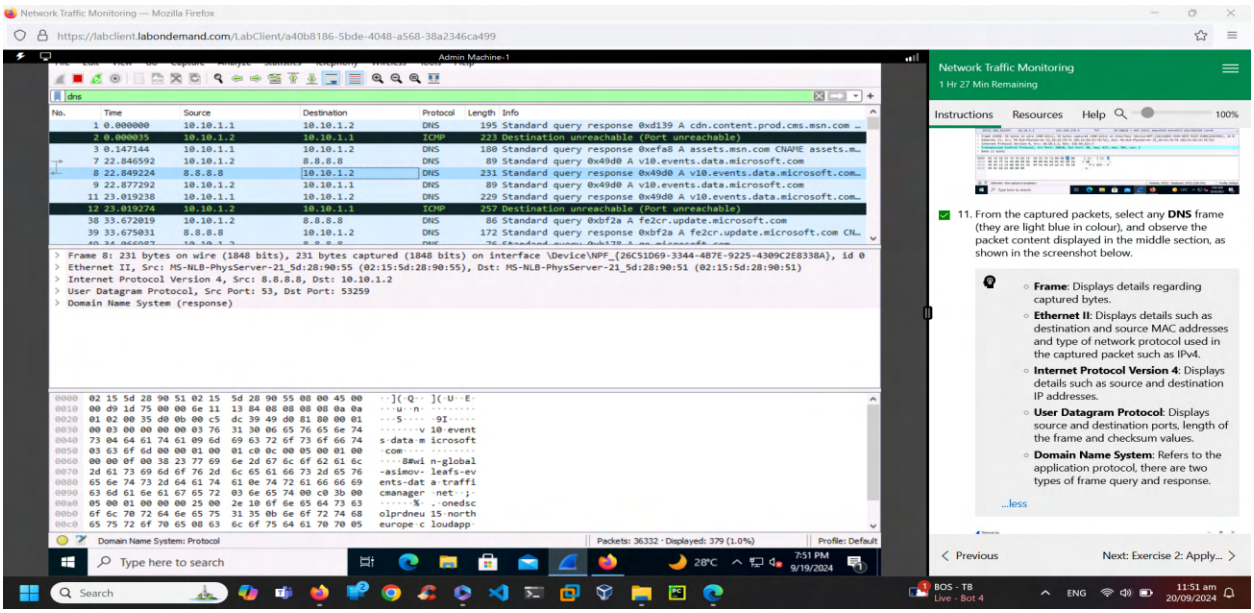
   Exercise no. and name: 1 Intercept Network Traffic using Wireshark and tcpdump
   Performed Date: 20/09/2024

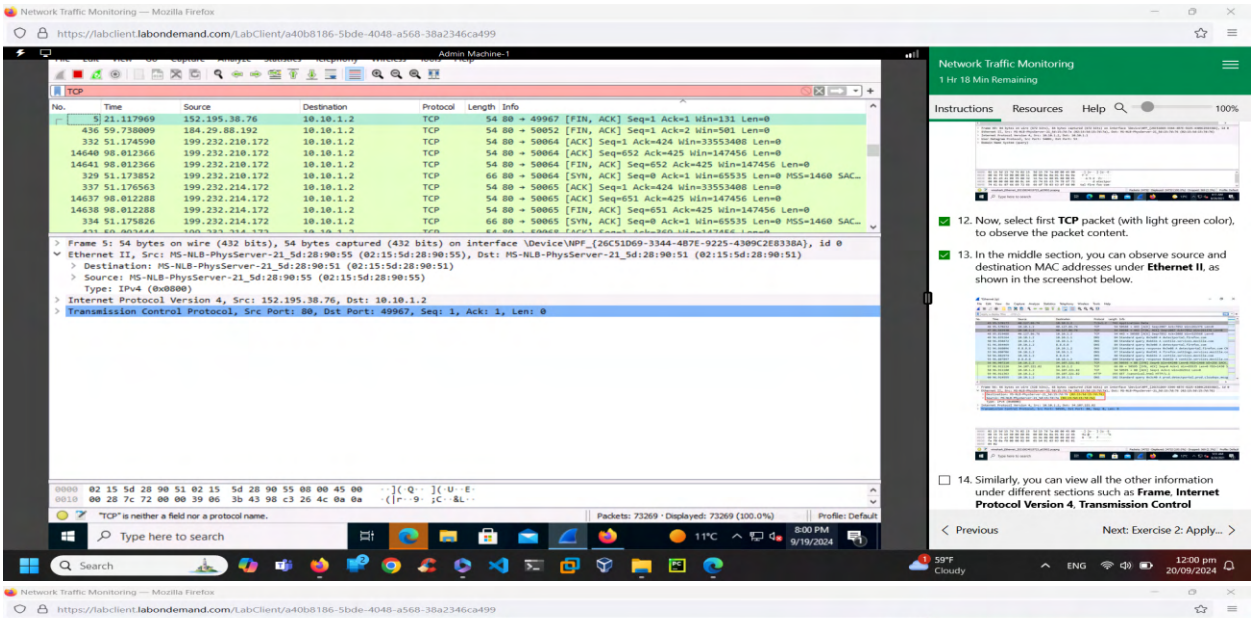
Summary:

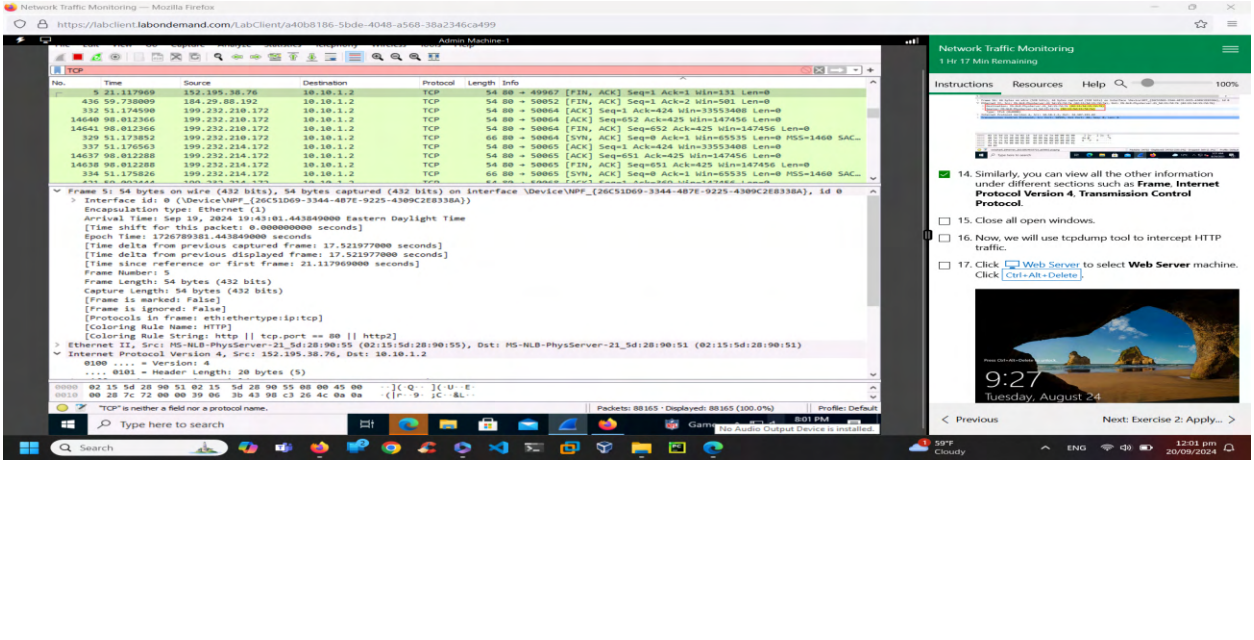
This lab involves intercepting Wireshark of different protocols (light blue-TCP, light green-UDP) from Admin machine1 through Ethernet0, capture packets and logging the details of entering into the website Moviescope. Web Server machine to enable basic authentication in IIS from server manager and disable Anonymous authentication. But practically windows authentication is the safest one. Used tcpdump commands from attacker machine in order to listen webserver machine and retrieve login credential because of unencrypted http packets and even with SSH protocol using Diffie-Hellmen key exchange to retrieve SSH client key because of no SSL certificate

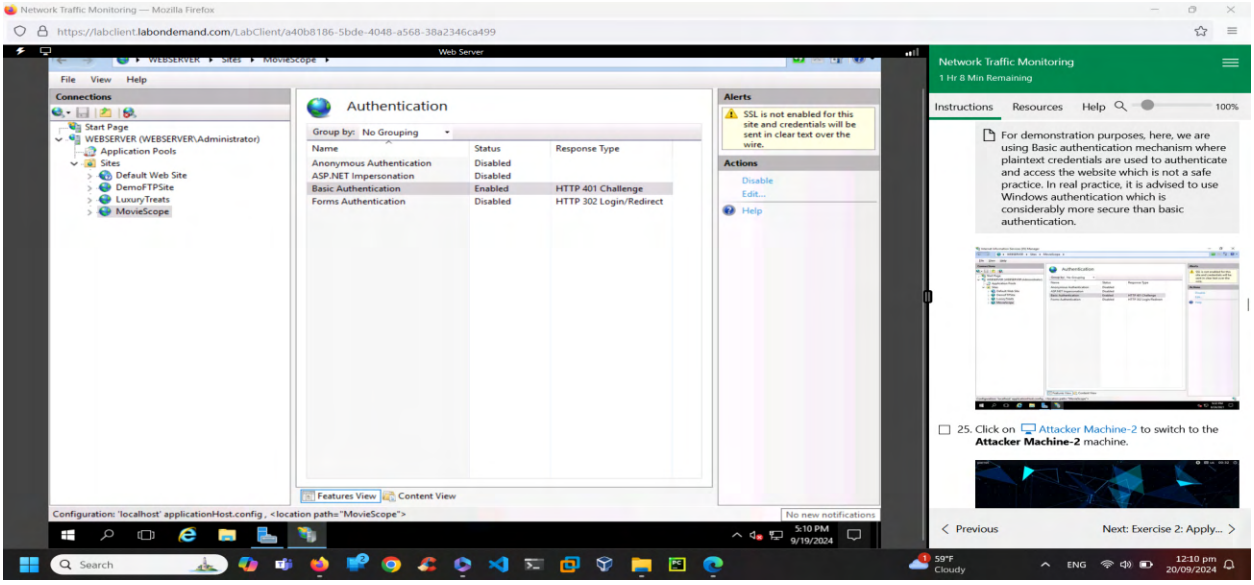


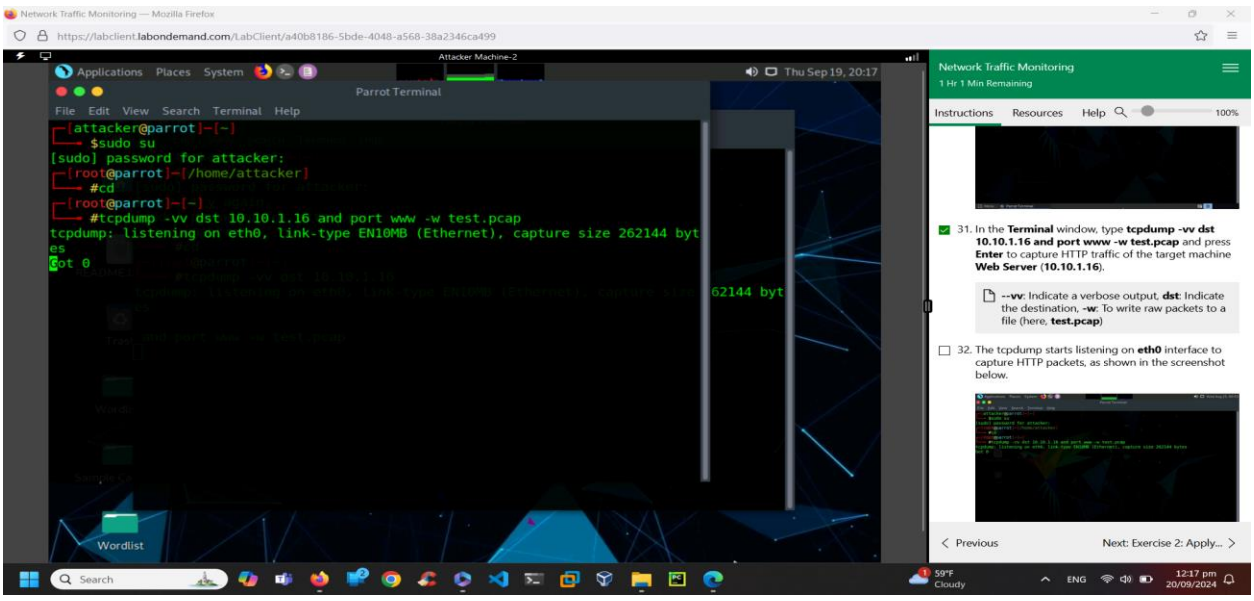



Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Admin Machine-1
dns
Network Traffic Monitoring
1 Hr 27 Min Remaining
Instructions
Resources
Help
100%
11. From the captured packets, select any DNS frame (they are light blue in colour), and observe the packet content displayed in the middle section, as shown in the screenshot below.
Frame: Displays details regarding captured bytes.
Ethernet II: Displays details such as destination and source MAC addresses and type of network protocol used in the captured packet such as IPv4.
Internet Protocol Version 4: Displays details such as source and destination IP addresses.
User Datagram Protocol: Displays source and destination ports, length of the frame and checksum values.
Domain Name System: Refers to the application protocol, there are two types of frame query and response.
...less
Previous
Next: Exercise 2: Apply...


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Admin Machine-1
TCP
Network Traffic Monitoring
1 Hr 18 Min Remaining
Instructions
Resources
Help
100%
12. Now, select first TCP packet (with light green color), to observe the packet content.
13. In the middle section, you can observe source and destination MAC addresses under Ethernet II, as shown in the screenshot below.
14. Similarly, you can view all the other information under different sections such as Frame, Internet Protocol Version 4, Transmission Control
Previous
Next: Exercise 2: Apply...


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Admin Machine-1
TCP
Network Traffic Monitoring
1 Hr 17 Min Remaining
Instructions
Resources
Help
100%
14. Similarly, you can view all the other information under different sections such as Frame, Internet Protocol Version 4, Transmission Control Protocol.
15. Close all open windows.
16. Now, we will use tcpdump tool to intercept HTTP traffic.
17. Click Web Server to select Web Server machine. Click Ctrl+Alt+Delete.
9:27
Tuesday, August 24
Previous
Next: Exercise 2: Apply...


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Web Server
File View Help
Connections
Start Page
WEBSERVER (WEBSERVER\Administrator)
Application Pools
Sites
Default Web Site
DemoFTPSite
LuxuryTreats
MovieScope
Authentication
Group by: No Grouping
Name
Status
Response Type
Anonymous Authentication
Disabled
ASP.NET Impersonation
Disabled
Basic Authentication
Enabled
HTTP 401 Challenge
Forms Authentication
Disabled
HTTP 302 Login/Redirect
Alerts
SSL is not enabled for this site and credentials will be sent in clear text over the wire.
Actions
Disable
Edit...
Help
Features View
Content View
Configuration: 'localhost' applicationHost.config , <location path="MovieScope">
No new notifications
5:10 PM
9/19/2024
Search
59°F
Cloudy
ENG
12:10 pm
20/09/2024
Network Traffic Monitoring
1 Hr 8 Min Remaining
Instructions
Resources
Help
100%
For demonstration purposes, here, we are using Basic authentication mechanism where plaintext credentials are used to authenticate and access the website which is not a safe practice. In real practice, it is advised to use Windows authentication which is considerably more secure than basic authentication.
25. Click on Attacker Machine-2 to switch to the Attacker Machine-2 machine.
Previous
Next: Exercise 2: Apply...


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:17
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#tcpdump -vv dst 10.10.1.16 and port www -w test.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
Got 0
62144 byt
Wordlist
Search
59°F
Cloudy
ENG
12:17 pm
20/09/2024
Network Traffic Monitoring
1 Hr 1 Min Remaining
Instructions
Resources
Help
100%
31. In the Terminal window, type tcpdump -vv dst 10.10.1.16 and port www -w test.pcap and press Enter to capture HTTP traffic of the target machine Web Server (10.10.1.16).
--vv: Indicate a verbose output, dst: Indicate the destination, -w: To write raw packets to a file (here, test.pcap)
32. The tcpdump starts listening on eth0 interface to capture HTTP packets, as shown in the screenshot below.
Previous
Next: Exercise 2: Apply...

Network Traffic Monitoring — Mozilla Firefox

https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499

Attacker Machine-2

Parrot Terminal

test.pcap (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000308	10.10.1.13	10.10.1.16	HTTP	390	GET / HTTP/1.1
9	48.666362	10.10.1.13	10.10.1.16	HTTP	445	GET / HTTP/1.1
11	50.545065	10.10.1.13	10.10.1.16	HTTP	421	GET /css/common...
18	50.546955	10.10.1.13	10.10.1.16	HTTP	419	GET /css/grid.cs...
19	50.546994	10.10.1.13	10.10.1.16	HTTP	420	GET /css/style.c...
20	50.547026	10.10.1.13	10.10.1.16	HTTP	431	GET /css/style-r...
24	50.560441	10.10.1.13	10.10.1.16	HTTP	407	GET /js/moderniz...
26	50.560552	10.10.1.13	10.10.1.16	HTTP	404	GET /js/script.j...
35	51.317668	10.10.1.13	10.10.1.16	HTTP	418	GET /images/logo...

```
Transmission Control Protocol, Src Port: 52682, Dst Port: 80, Seq: 325, Ack: 1510, Len: 379
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: www.moviescope.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Authorization: Basic QWRtaW5pc3RyYXRvcjphZG1pbkAxMjM=\r\n
    Credentials: Administrator:admin@123
  \r\n
  [Full request URI: http://www.moviescope.com/]
  [HTTP request 2/5]
  [Prev request in frame: 3]
  [Next request in frame: 11]
```

```
0040  c5 b9 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /  HTTP/1.1
```

Credentials (http.authbasic) Packets: 127 · Displayed: 25 (19.7%) Profile: Default

Click to switch to "Workspace 4"

Menu | Parrot Terminal | Parrot Terminal | Mozilla Firefox | Login - MovieSc... | (as superuser)

Search

59°F Cloudy ENG 12:26 pm 20/09/2024

Network Traffic Monitoring

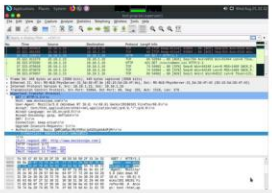
52 Minutes Remaining

Instructions Resources Help 100%

- [x] 41. Click to select any **HTTP** message with **GET** request.
- [x] 42. From the middle-pane, expand **Hypertext Transfer Protocol** node. Under **Hypertext Transfer Protocol** node, expand **Authorization** node.

  If you do not see Authorization node in the first block of HTTP packets then select HTTP GET packet from a different block of HTTP packets.

- [x] 43. You can observe that the credentials are displayed because the HTTP packets are unencrypted which makes them vulnerable to packet sniffing. Close the **Wireshark** window.



Previous Next: Exercise 2: Apply...

Network Traffic Monitoring — Mozilla Firefox

https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499

Attacker Machine-2

Applications Places System Thu Sep 19, 20:30

Parrot Terminal

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #ssh sam@10.10.1.79
The authenticity of host '10.10.1.79 (10.10.1.79)' can't be established.
ECDSA key fingerprint is SHA256:RMB43/oUEthHrOcnTw6n0Us6WVfle2H1iaDhtuuXGa8.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Search

59°F Cloudy ENG 12:30 pm 20/09/2024

Network Traffic Monitoring

48 Minutes Remaining

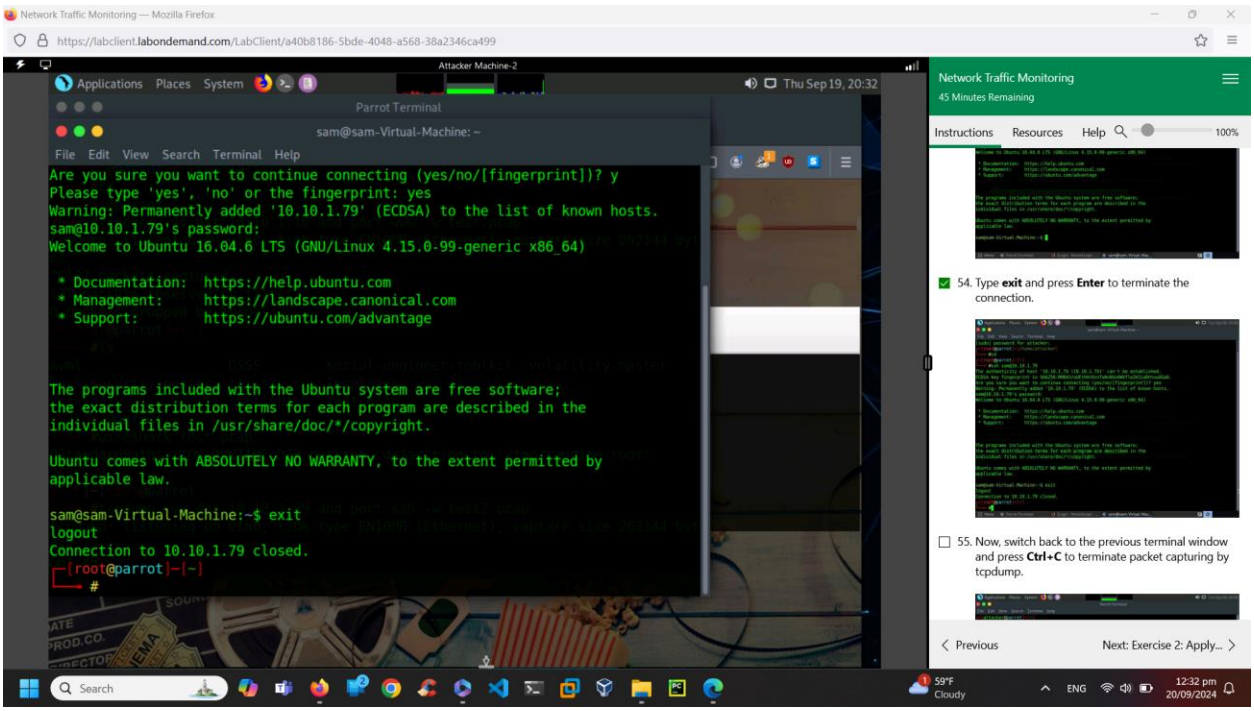
Instructions Resources Help 100%

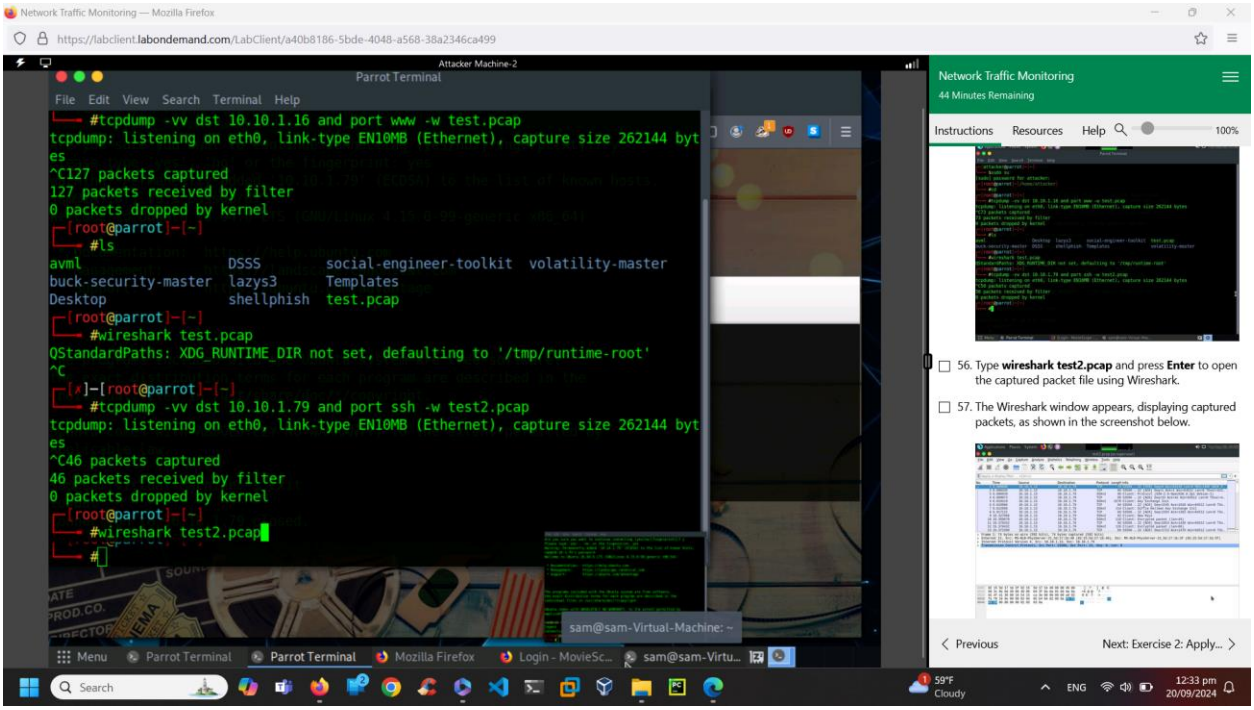
- [x] 51. Type **ssh sam@10.10.1.79** and press **Enter** to establish SSH connection with **Admin Machine-2**.

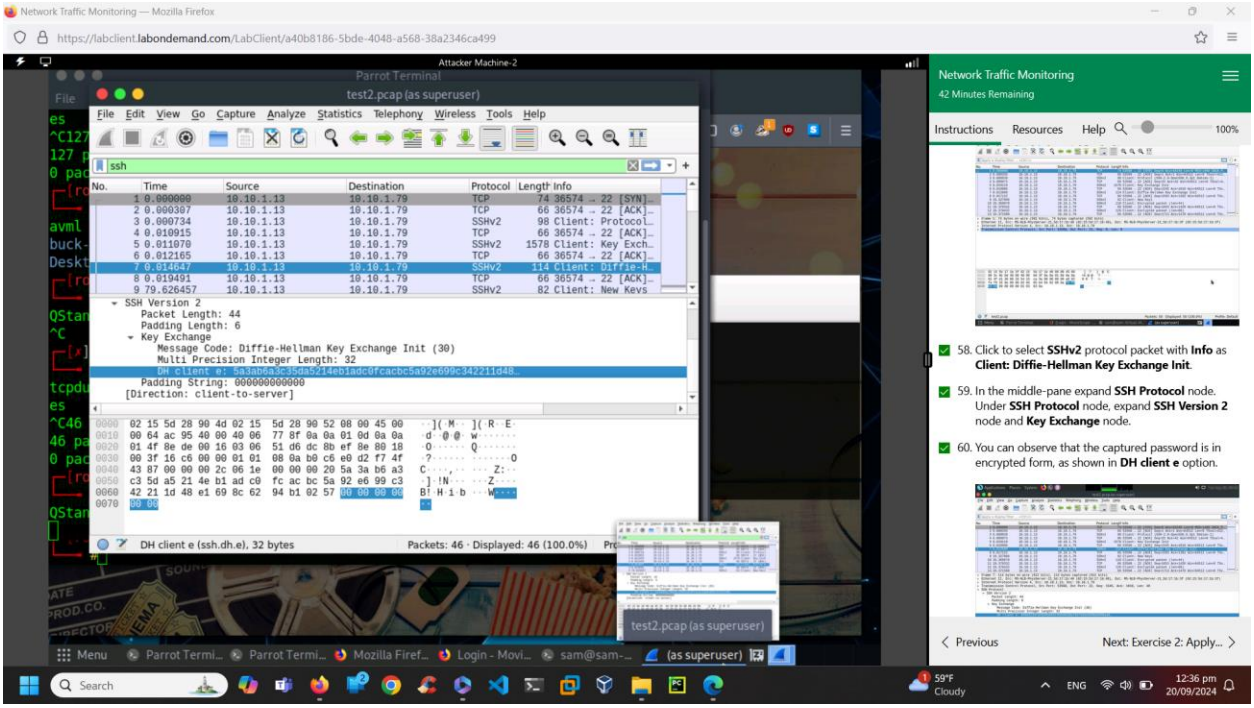
  If connection attempt prompt appears, type **yes** and press **Enter**.

- [ ] 52. In the **password** field, type **admin@123** and press **Enter**.
- [ ] 53. You can observe that a remote connection has been established, as shown in the screenshot below.

Previous Next: Exercise 2: Apply...


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:32
Parrot Terminal
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.1.79' (ECDSA) to the list of known hosts.
sam@10.10.1.79's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-99-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
sam@sam-Virtual-Machine:~$ exit
logout
Connection to 10.10.1.79 closed.
┌[root@parrot]-[~]
└── #
Network Traffic Monitoring
45 Minutes Remaining
Instructions Resources Help 100%
54. Type exit and press Enter to terminate the connection.
55. Now, switch back to the previous terminal window and press Ctrl+C to terminate packet capturing by tcpdump.
Previous
Next: Exercise 2: Apply...
Search
59°F Cloudy
ENG
12:32 pm 20/09/2024


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Parrot Terminal
File Edit View Search Terminal Help
└── #tcpdump -vv dst 10.10.1.16 and port www -w test.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C127 packets captured
127 packets received by filter
0 packets dropped by kernel
┌[root@parrot]-[~]
└── #ls
avml DSSS social-engineer-toolkit volatility-master
buck-security-master lazys3 Templates
Desktop shellphish test.pcap
┌[root@parrot]-[~]
└── #wireshark test.pcap
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
^C
┌[✗]-[root@parrot]-[~]
└── #tcpdump -vv dst 10.10.1.79 and port ssh -w test2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C46 packets captured
46 packets received by filter
0 packets dropped by kernel
┌[root@parrot]-[~]
└── #wireshark test2.pcap
└── #
sam@sam-Virtual-Machine: ~
Menu Parrot Terminal Parrot Terminal Mozilla Firefox Login - MovieSc... sam@sam-Virtu...
Network Traffic Monitoring
44 Minutes Remaining
Instructions Resources Help 100%
56. Type wireshark test2.pcap and press Enter to open the captured packet file using Wireshark.
57. The Wireshark window appears, displaying captured packets, as shown in the screenshot below.
Previous
Next: Exercise 2: Apply...
Search
59°F Cloudy
ENG
12:33 pm 20/09/2024



Report:

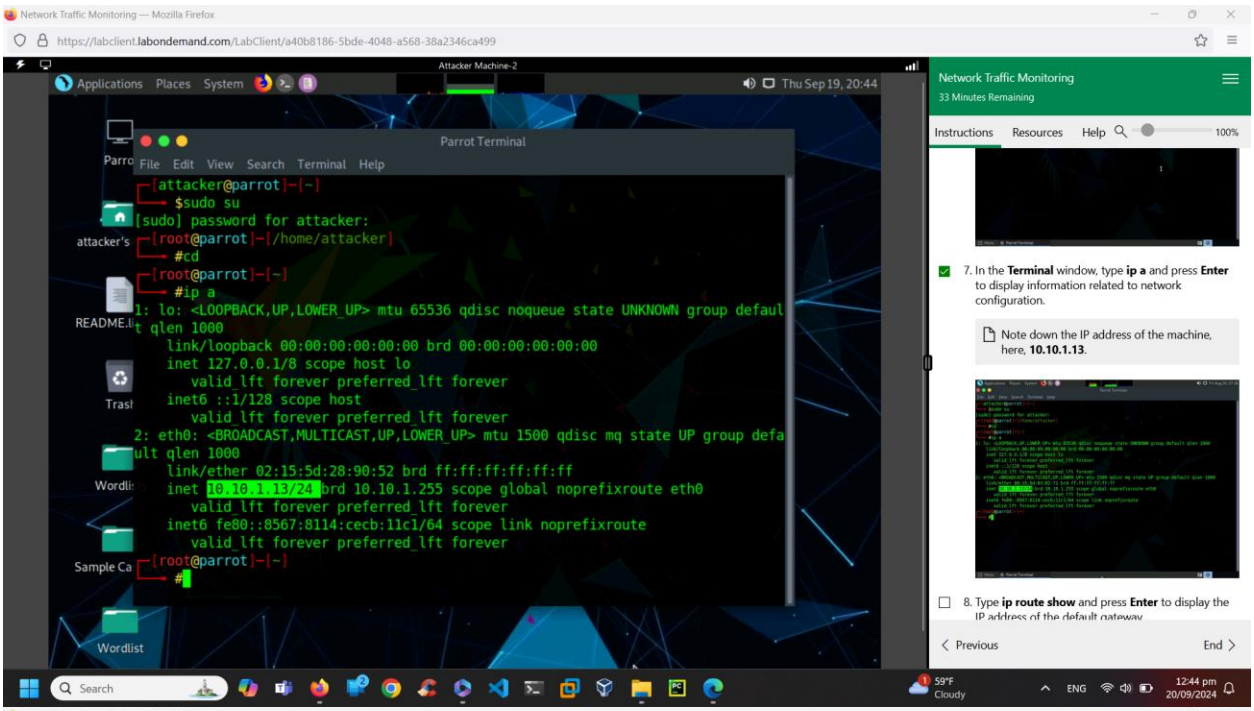
As a cyber technician, we are using incident response tools like Wireshark and tcpdump. I have experienced basic authentication is not secured enough to fill the gaps in the security. We need Multi factor authentication or Windows authentication in the network for a secure environment. It also made me to understand why SSL/TLS should be implemented.

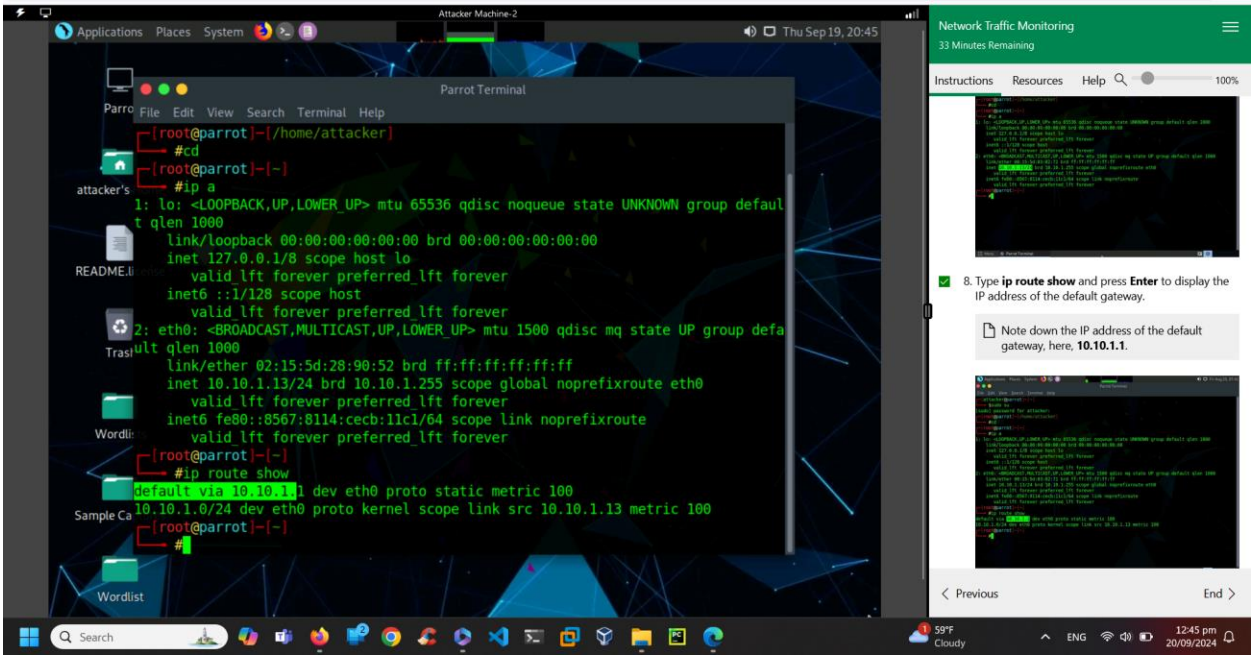
6. **Ilab Module no. and name:** 17. Network Traffic Monitoring
   Exercise no. and name: 4 Scan Network to Identify Hosts in the Local Network
   Performed Date: 20/09/2024

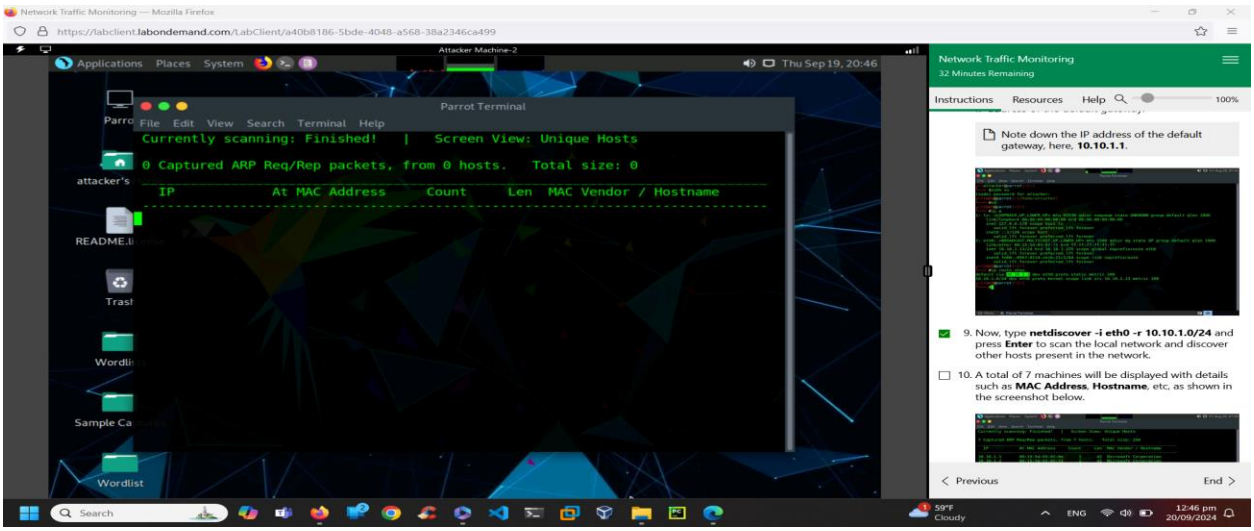
Summary:

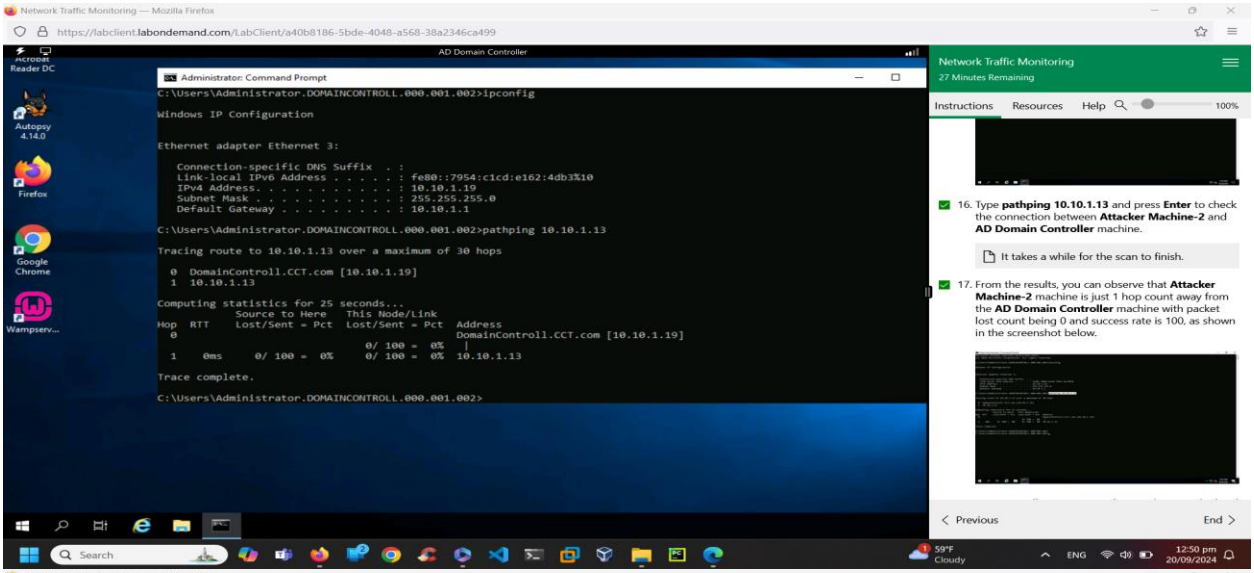
This lab demonstrates of using Nmap in attacker machine and how the commands in Mate terminal retrieve data of ports (Open/closed/number of ports), MAC addresses (known and unknown hosts) and protocol used. It also helps to check traceroute between attacker machine and AD domain controller. I also used different Nmap extensions to get required data as shown in the screenshots below.

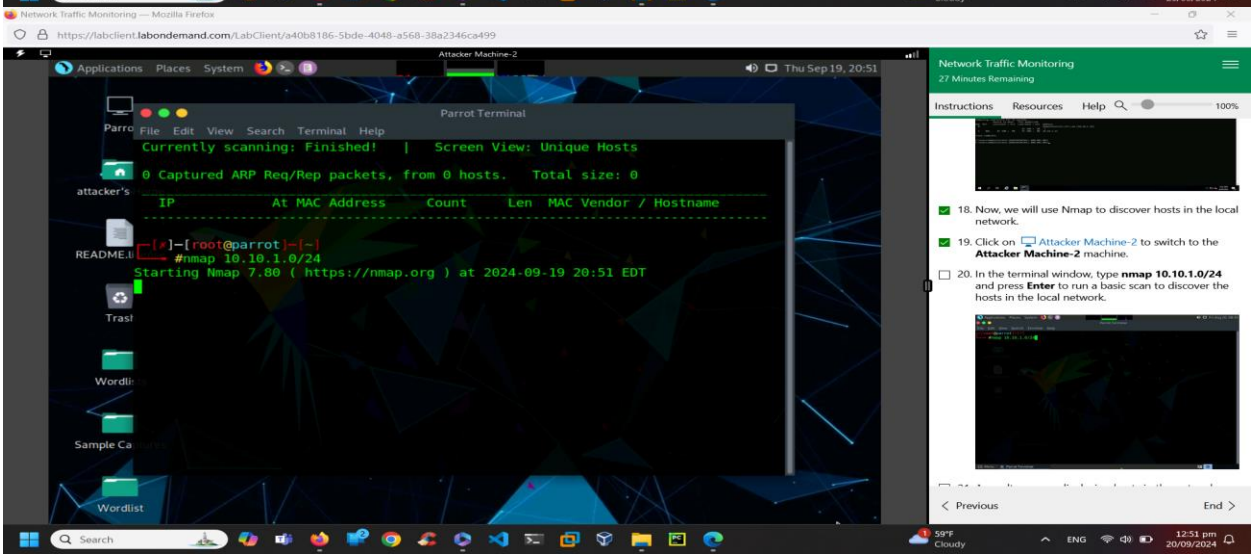
Screenshots:

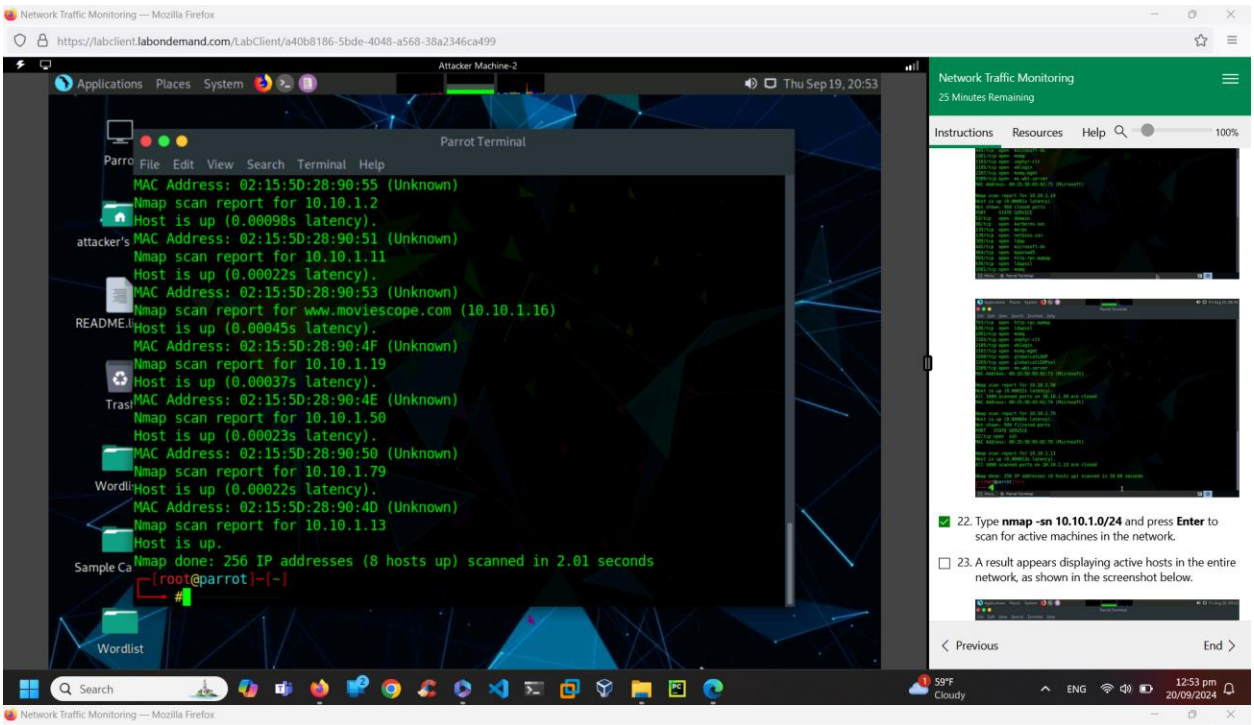

Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:44
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 02:15:5d:28:90:52 brd ff:ff:ff:ff:ff:ff
inet 10.10.1.13/24 brd 10.10.1.255 scope global noprefixroute eth0
valid_lft forever preferred_lft forever
inet6 fe80::8567:8114:cecb:11c1/64 scope link noprefixroute
valid_lft forever preferred_lft forever
[root@parrot]~[~]
#
Wordlist
Search
59°F Cloudy
ENG
12:44 pm 20/09/2024
Network Traffic Monitoring
33 Minutes Remaining
Instructions Resources Help 100%
7. In the Terminal window, type ip a and press Enter to display information related to network configuration.
Note down the IP address of the machine, here, 10.10.1.13.
8. Type ip route show and press Enter to display the IP address of the default gateway
Previous End

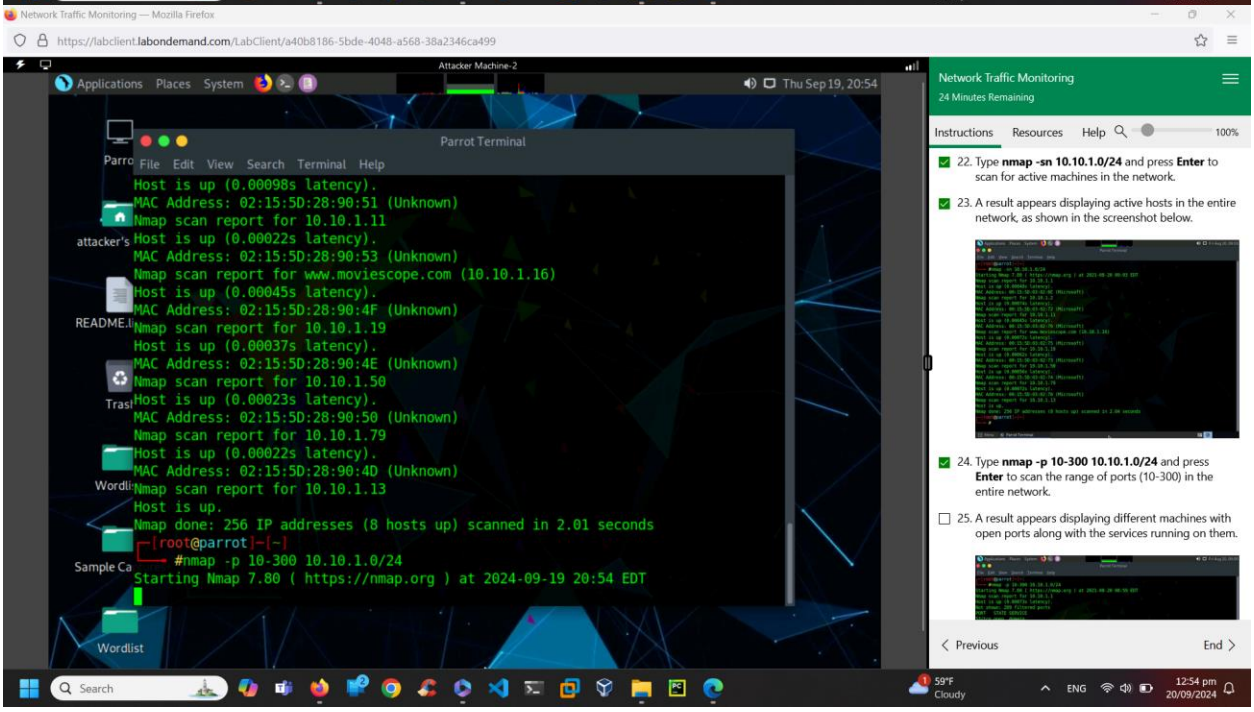

Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:45
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 02:15:5d:28:90:52 brd ff:ff:ff:ff:ff:ff
inet 10.10.1.13/24 brd 10.10.1.255 scope global noprefixroute eth0
valid_lft forever preferred_lft forever
inet6 fe80::8567:8114:cecb:11c1/64 scope link noprefixroute
valid_lft forever preferred_lft forever
[root@parrot]~[~]
#ip route show
default via 10.10.1.1 dev eth0 proto static metric 100
10.10.1.0/24 dev eth0 proto kernel scope link src 10.10.1.13 metric 100
[root@parrot]~[~]
#
Wordlist
Search
59°F Cloudy
ENG
12:45 pm 20/09/2024
Network Traffic Monitoring
33 Minutes Remaining
Instructions Resources Help 100%
8. Type ip route show and press Enter to display the IP address of the default gateway.
Note down the IP address of the default gateway, here, 10.10.1.1.
Previous End


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:46
Parrot Terminal
File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
0 Captured ARP Req/Rep packets, from 0 hosts. Total size: 0
IP At MAC Address Count Len MAC Vendor / Hostname
attacker's
README.li
Trasl
Wordli
Sample Ca
Wordlist
Search
59°F Cloudy
ENG
12:46 pm 20/09/2024
Network Traffic Monitoring
32 Minutes Remaining
Instructions Resources Help 100%
Note down the IP address of the default gateway, here, 10.10.1.1.
9. Now, type netdiscover -i eth0 -r 10.10.1.0/24 and press Enter to scan the local network and discover other hosts present in the network.
10. A total of 7 machines will be displayed with details such as MAC Address, Hostname, etc, as shown in the screenshot below.
< Previous
End >


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
AD Domain Controller
Administrator: Command Prompt
C:\Users\Administrator.DOMAINCONTROLL.000.001.002>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 3:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::7954:c1cd:e162:4db3%10
IPv4 Address. . . . . : 10.10.1.19
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.1.1
C:\Users\Administrator.DOMAINCONTROLL.000.001.002>pathping 10.10.1.13
Tracing route to 10.10.1.13 over a maximum of 30 hops
0 DomainControll.CCT.com [10.10.1.19]
1 10.10.1.13
Computing statistics for 25 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 DomainControll.CCT.com [10.10.1.19]
0/ 100 = 0% |
1 0ms 0/ 100 = 0% 0/ 100 = 0% 10.10.1.13
Trace complete.
C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
Autopsy 4.14.0
Firefox
Google Chrome
Wampserv...
Search
59°F Cloudy
ENG
12:50 pm 20/09/2024
Network Traffic Monitoring
27 Minutes Remaining
Instructions Resources Help 100%
16. Type pathping 10.10.1.13 and press Enter to check the connection between Attacker Machine-2 and AD Domain Controller machine.
It takes a while for the scan to finish.
17. From the results, you can observe that Attacker Machine-2 machine is just 1 hop count away from the AD Domain Controller machine with packet lost count being 0 and success rate is 100, as shown in the screenshot below.
< Previous
End >


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:51
Parrot Terminal
File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
0 Captured ARP Req/Rep packets, from 0 hosts. Total size: 0
IP At MAC Address Count Len MAC Vendor / Hostname
attacker's
README.li
[root@parrot]~[~]
#nmap 10.10.1.0/24
Starting Nmap 7.80 (https://nmap.org) at 2024-09-19 20:51 EDT
Trasl
Wordli
Sample Ca
Wordlist
Search
59°F Cloudy
ENG
12:51 pm 20/09/2024
Network Traffic Monitoring
27 Minutes Remaining
Instructions Resources Help 100%
18. Now, we will use Nmap to discover hosts in the local network.
19. Click on Attacker Machine-2 to switch to the Attacker Machine-2 machine.
20. In the terminal window, type nmap 10.10.1.0/24 and press Enter to run a basic scan to discover the hosts in the local network.
< Previous
End >


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:53
Parrot Terminal
File Edit View Search Terminal Help
MAC Address: 02:15:5D:28:90:55 (Unknown)
Nmap scan report for 10.10.1.2
Host is up (0.00098s latency).
MAC Address: 02:15:5D:28:90:51 (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00022s latency).
MAC Address: 02:15:5D:28:90:53 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.16)
Host is up (0.00045s latency).
MAC Address: 02:15:5D:28:90:4F (Unknown)
Nmap scan report for 10.10.1.19
Host is up (0.00037s latency).
MAC Address: 02:15:5D:28:90:4E (Unknown)
Nmap scan report for 10.10.1.50
Host is up (0.00023s latency).
MAC Address: 02:15:5D:28:90:50 (Unknown)
Nmap scan report for 10.10.1.79
Host is up (0.00022s latency).
MAC Address: 02:15:5D:28:90:4D (Unknown)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.01 seconds
[root@parrot]~[~]
#
Wordlist
Search
59°F Cloudy
ENG
12:53 pm 20/09/2024
Network Traffic Monitoring
25 Minutes Remaining
Instructions Resources Help 100%
22. Type nmap -sn 10.10.1.0/24 and press Enter to scan for active machines in the network.
23. A result appears displaying active hosts in the entire network, as shown in the screenshot below.
Previous End


Network Traffic Monitoring — Mozilla Firefox
https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499
Attacker Machine-2
Applications Places System
Thu Sep 19, 20:54
Parrot Terminal
File Edit View Search Terminal Help
Host is up (0.00098s latency).
MAC Address: 02:15:5D:28:90:51 (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00022s latency).
MAC Address: 02:15:5D:28:90:53 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.16)
Host is up (0.00045s latency).
MAC Address: 02:15:5D:28:90:4F (Unknown)
Nmap scan report for 10.10.1.19
Host is up (0.00037s latency).
MAC Address: 02:15:5D:28:90:4E (Unknown)
Nmap scan report for 10.10.1.50
Host is up (0.00023s latency).
MAC Address: 02:15:5D:28:90:50 (Unknown)
Nmap scan report for 10.10.1.79
Host is up (0.00022s latency).
MAC Address: 02:15:5D:28:90:4D (Unknown)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.01 seconds
[root@parrot]~[~]
#nmap -p 10-300 10.10.1.0/24
Starting Nmap 7.80 (https://nmap.org) at 2024-09-19 20:54 EDT
Wordlist
Search
59°F Cloudy
ENG
12:54 pm 20/09/2024
Network Traffic Monitoring
24 Minutes Remaining
Instructions Resources Help 100%
22. Type nmap -sn 10.10.1.0/24 and press Enter to scan for active machines in the network.
23. A result appears displaying active hosts in the entire network, as shown in the screenshot below.
24. Type nmap -p 10-300 10.10.1.0/24 and press Enter to scan the range of ports (10-300) in the entire network.
25. A result appears displaying different machines with open ports along with the services running on them.
Previous End

Network Traffic Monitoring — Mozilla Firefox

https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499

Attacker Machine-2

Applications Places System Thu Sep 19, 20:54

Parrot Terminal

File Edit View Search Terminal Help

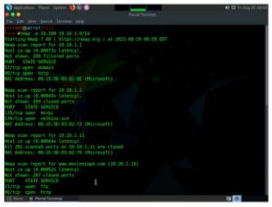
```
88/tcp  open  kerberos-sec
135/tcp open  msrpc
139/tcp open  netbios-ssn
MAC Address: 02:15:5D:28:90:4E (Unknown)

Nmap scan report for 10.10.1.50
Host is up (0.00022s latency).
All 291 scanned ports on 10.10.1.50 are closed
MAC Address: 02:15:5D:28:90:50 (Unknown)

Nmap scan report for 10.10.1.79
Host is up (0.00025s latency).
Not shown: 290 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:15:5D:28:90:4D (Unknown)

Nmap scan report for 10.10.1.13
Host is up (0.0000060s latency).
All 291 scanned ports on 10.10.1.13 are closed

Nmap done: 256 IP addresses (8 hosts up) scanned in 6.78 seconds
┌──[root@parrot]─[~]
└──╼ #
```

Network Traffic Monitoring

24 Minutes Remaining

Instructions Resources Help 100%

- [x] 24. Type **nmap -p 10-300 10.10.1.0/24** and press **Enter** to scan the range of ports (10-300) in the entire network.
- [x] 25. A result appears displaying different machines with open ports along with the services running on them.



- [ ] 26. Type **nmap --top-port 20 10.10.1.0/24** and press **Enter** to scan for the twenty most common ports.
- [ ] 27. A result appears displaying different top 20 ports along with status as open/close/filtered, as shown in the screenshot below.

Previous End

Search 59°F Cloudy ENG 12:54 pm 20/09/2024

Network Traffic Monitoring — Mozilla Firefox

https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499

Attacker Machine-2

Applications Places System Thu Sep 19, 20:55

Parrot Terminal

File Edit View Search Terminal Help

```
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
Nmap scan report for 10.10.1.13
Host is up (0.0000060s latency).
All 291 scanned ports on 10.10.1.13 are closed

Nmap done: 256 IP addresses (8 hosts up) scanned in 6.78 seconds
┌──[root@parrot]─[~]
└──╼ #nmap --top-port 20 10.10.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-19 20:55 EDT
```

Network Traffic Monitoring

23 Minutes Remaining

Instructions Resources Help 100%

- [x] 24. Type **nmap -p 10-300 10.10.1.0/24** and press **Enter** to scan the range of ports (10-300) in the entire network.
- [x] 25. A result appears displaying different machines with open ports along with the services running on them.

- [x] 26. Type **nmap --top-port 20 10.10.1.0/24** and press **Enter** to scan for the twenty most common ports.
- [ ] 27. A result appears displaying different top 20 ports along with status as open/close/filtered, as shown in the screenshot below.

Previous End

Search 59°F Cloudy ENG 12:55 pm 20/09/2024

Network Traffic Monitoring — Mozilla Firefox

https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499

Attacker Machine-2

Applications Places System Thu Sep 19, 20:55

Parrot Terminal

File Edit View Search Terminal Help

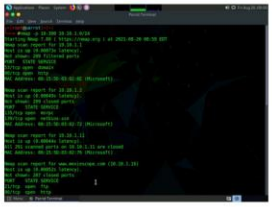
```
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
53/tcp   closed domain
80/tcp   closed http
110/tcp  closed pop3
111/tcp  closed rpcbind
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
143/tcp  closed imap
443/tcp  closed https
445/tcp  closed microsoft-ds
993/tcp  closed imaps
995/tcp  closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy

Nmap done: 256 IP addresses (8 hosts up) scanned in 3.65 seconds
┌──[root@parrot]─[~]
└──╼ #
```

Network Traffic Monitoring

23 Minutes Remaining

Instructions Resources Help 100%

- [x] 24. Type **nmap -p 10-300 10.10.1.0/24** and press **Enter** to scan the range of ports (10-300) in the entire network.
- [x] 25. A result appears displaying different machines with open ports along with the services running on them.



- [x] 26. Type **nmap --top-port 20 10.10.1.0/24** and press **Enter** to scan for the twenty most common ports.
- [ ] 27. A result appears displaying different top 20 ports along with status as open/close/filtered, as shown in the screenshot below.

Previous End

Search 59°F Cloudy ENG 12:55 pm 20/09/2024

Network Traffic Monitoring — Mozilla Firefox

https://labclient.labondemand.com/LabClient/a40b8186-5bde-4048-a568-38a2346ca499

Attacker Machine-2

Applications Places System Thu Sep 19, 20:57

Parrot Terminal

File Edit View Search Terminal Help

```
Host is up (0.00038s latency).
MAC Address: 02:15:5D:28:90:51 (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00023s latency).
MAC Address: 02:15:5D:28:90:53 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.16)
Host is up (0.00018s latency).
MAC Address: 02:15:5D:28:90:4F (Unknown)
Nmap scan report for 10.10.1.19
Host is up (0.00047s latency).
MAC Address: 02:15:5D:28:90:4E (Unknown)
Nmap scan report for 10.10.1.50
Host is up (0.00043s latency).
MAC Address: 02:15:5D:28:90:50 (Unknown)
Nmap scan report for 10.10.1.79
Host is up (0.00030s latency).
MAC Address: 02:15:5D:28:90:4D (Unknown)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.01 seconds
┌──[root@parrot]─[~]
└──╼ #nmap -A 10.10.1.19
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-19 20:57 EDT
```

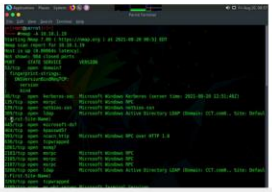
Network Traffic Monitoring

21 Minutes Remaining

Instructions Resources Help 100%

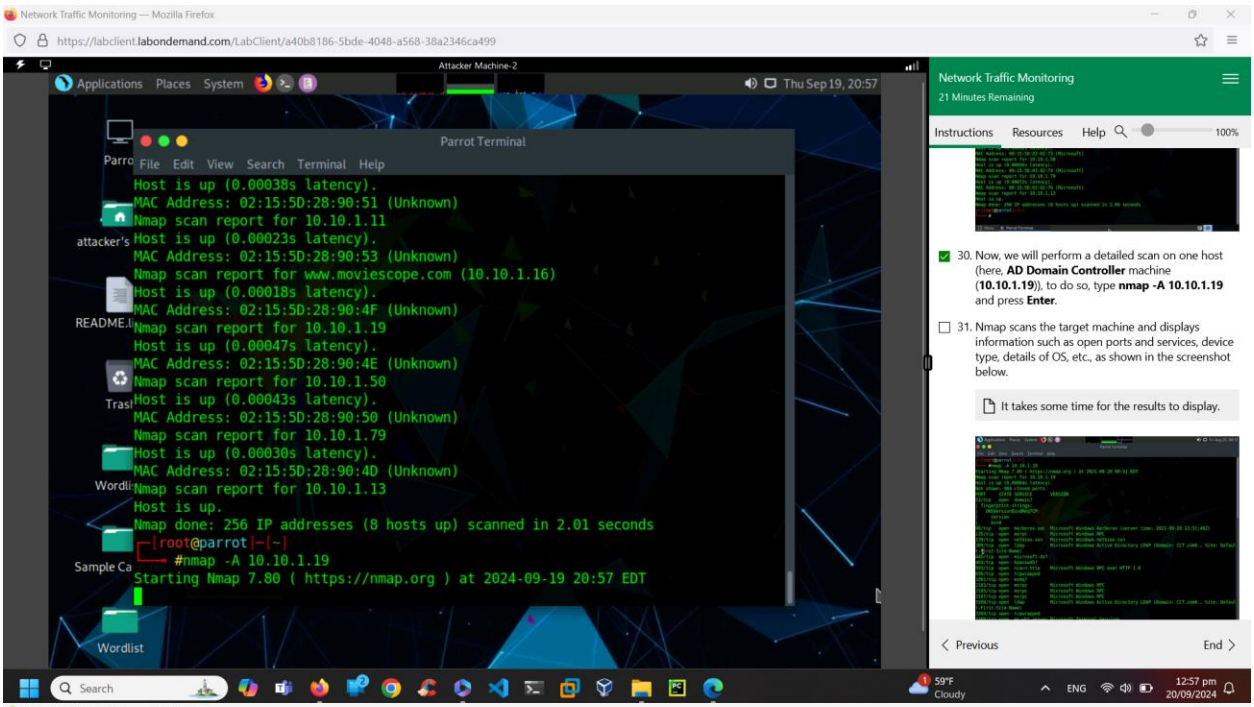
- [x] 30. Now, we will perform a detailed scan on one host (here, **AD Domain Controller** machine (**10.10.1.19**)), to do so, type **nmap -A 10.10.1.19** and press **Enter**.
- [ ] 31. Nmap scans the target machine and displays information such as open ports and services, device type, details of OS, etc., as shown in the screenshot below.

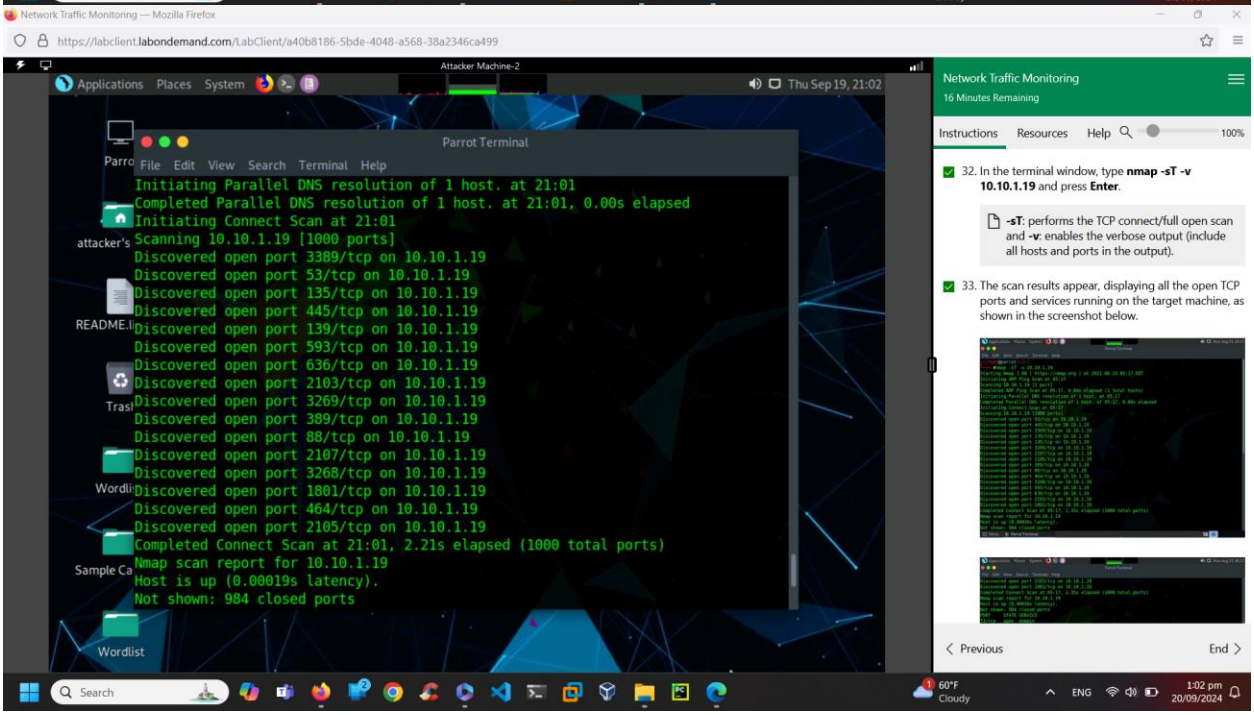
It takes some time for the results to display.



Previous End

Search 59°F Cloudy ENG 12:57 pm 20/09/2024





Report:

As a cyber technician, the purpose of this exercise is to understand different type of scanning and perform network scanning using Nmap which identifies active hosts, open ports and services running on a network. Identifying potential weakness in the network is the critical task in this exercise.

7. **Ilab Module no. and name:** 9. Application security

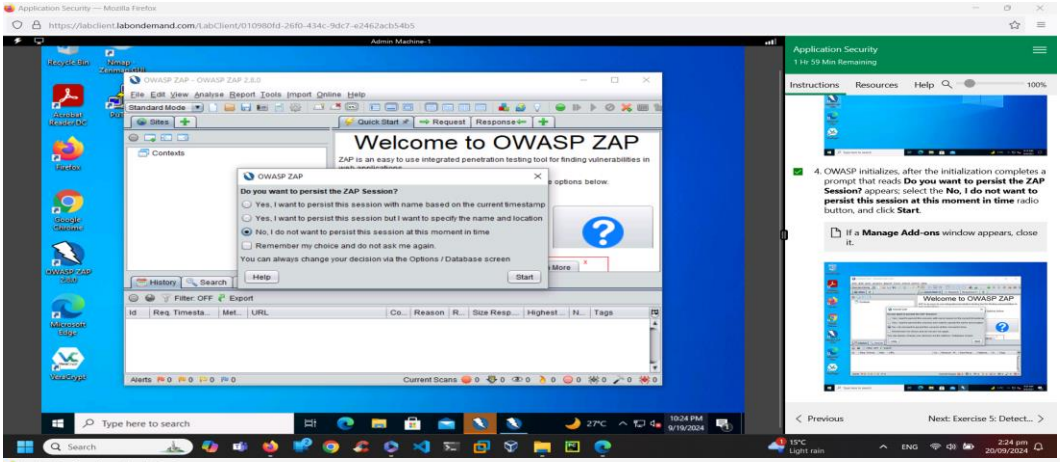
Exercise no. and name: 4 Detect Web Application Vulnerabilities using OWASP ZAP

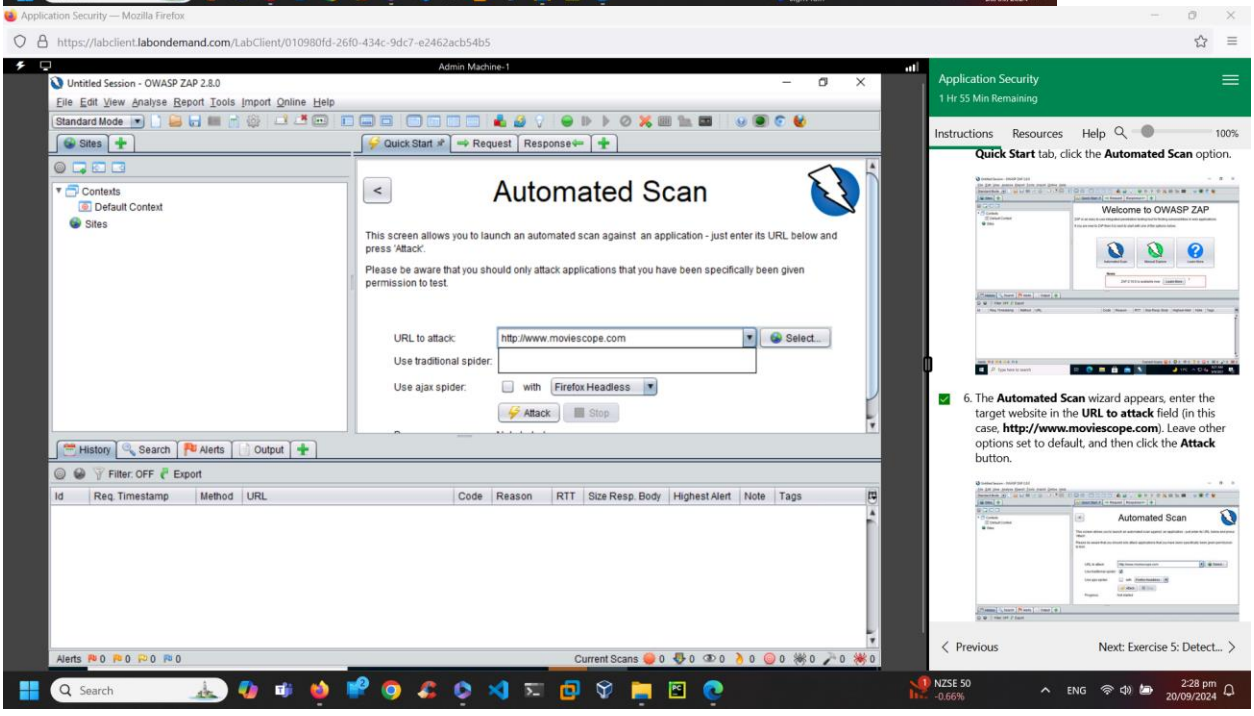
Performed Date: 20/09/2024

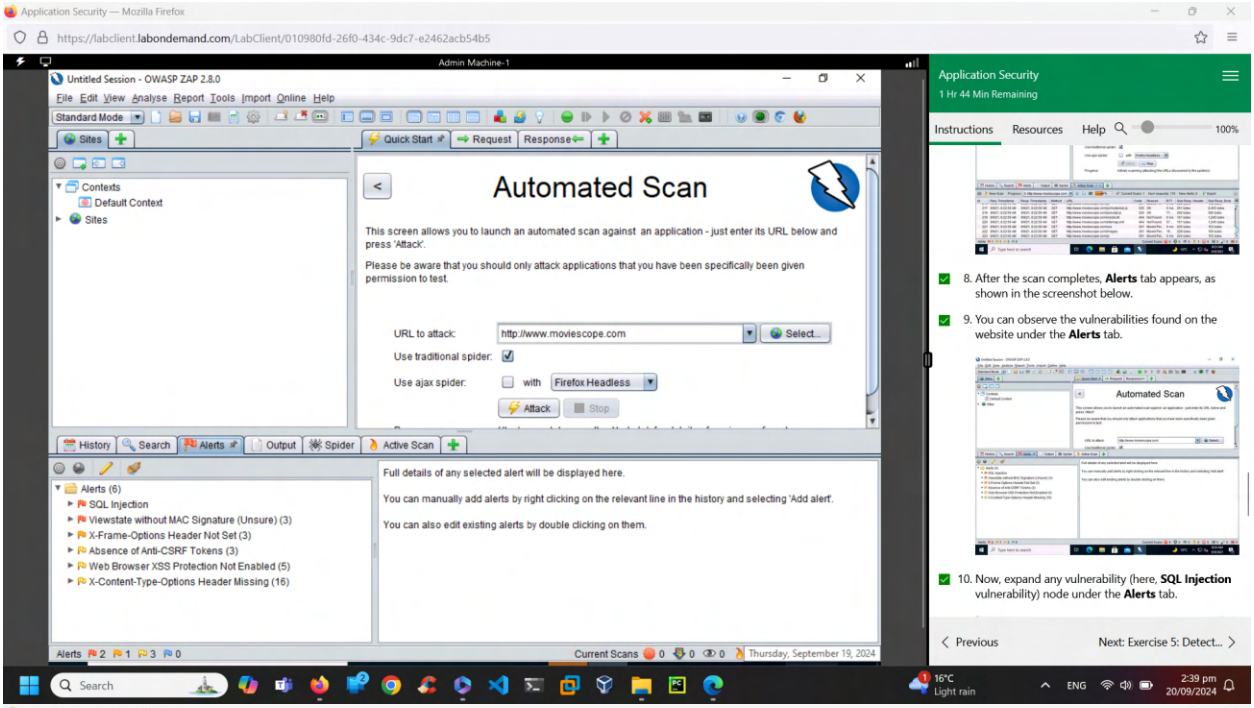
Summary:

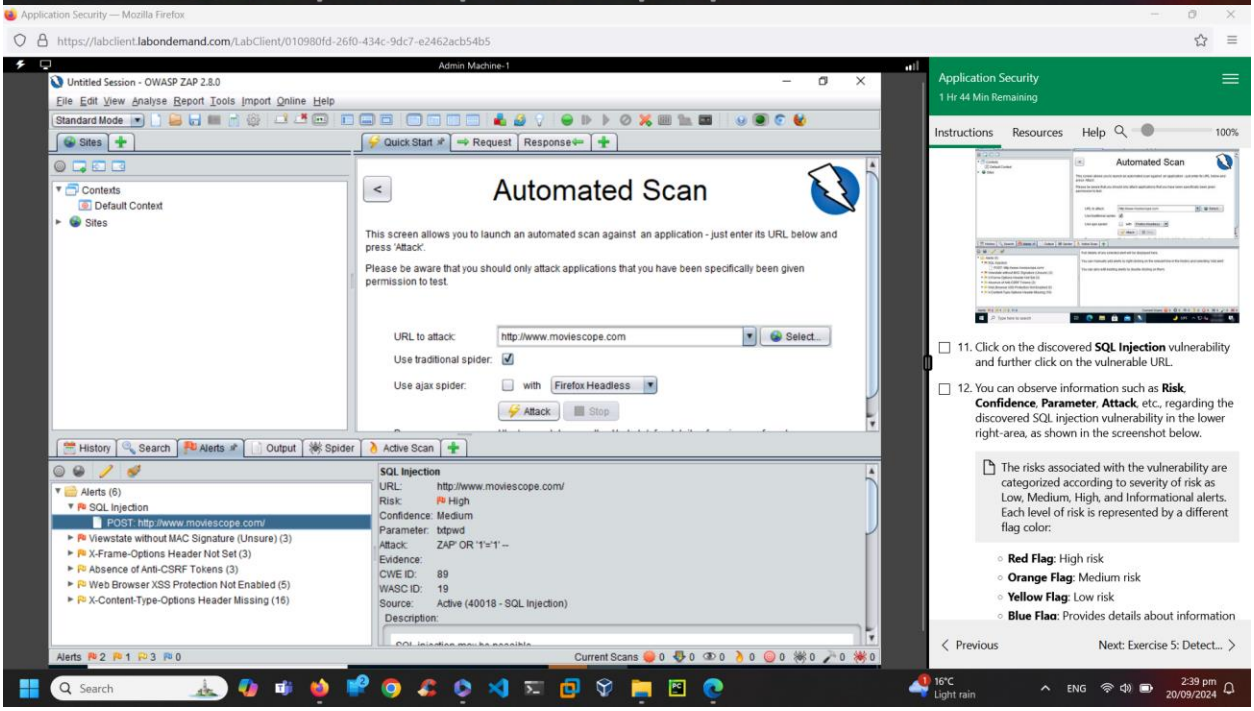
Installing OWASP ZAP to scan for vulnerabilities in the website movie scope.com. We can type any URL to check for the weakness in the application. It shows the alerts with the details of risk matrix like high risk and low risk by assessing the effect of the threat. The screenshots are shown to capture the fields of the alerts in OWASP.

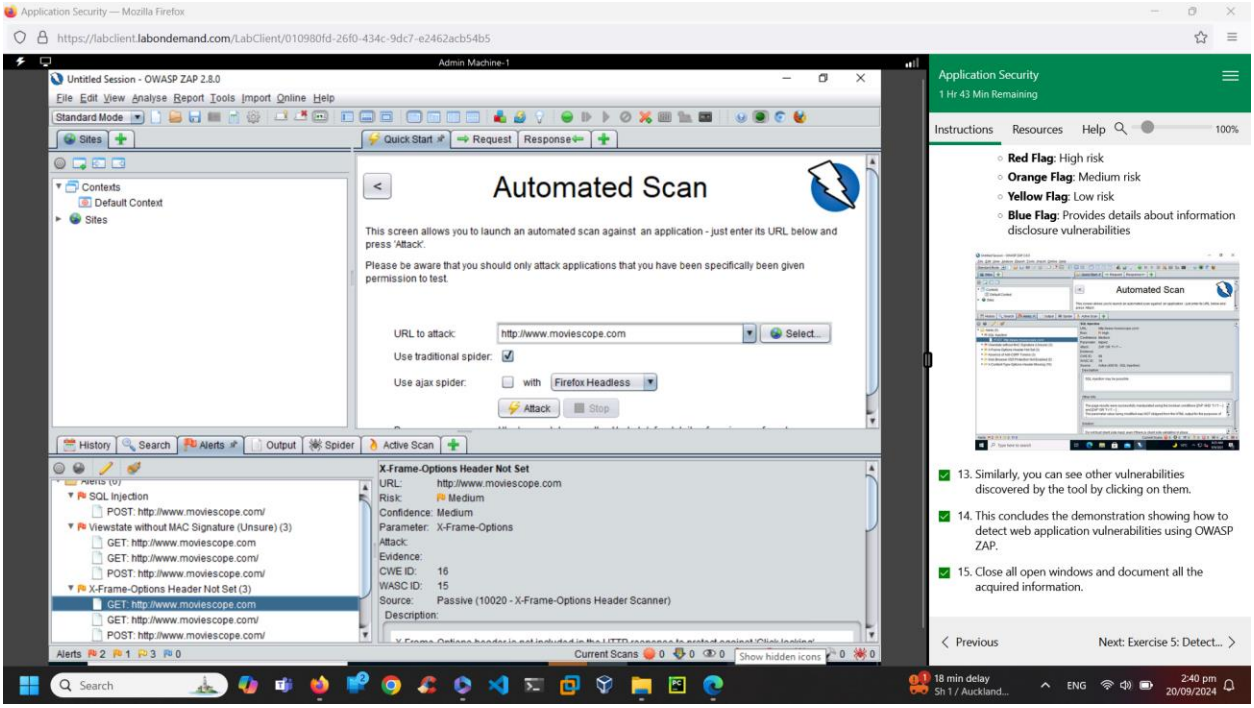
Screenshots:






Application Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/010980fd-26f0-434c-9dc7-e2462acb54b5
Admin Machine-1
Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://www.moviescope.com
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
History
Search
Alerts
Output
Spider
Active Scan
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts (6)
SQL Injection
Viewstate without MAC Signature (Unsure) (3)
X-Frame-Options Header Not Set (3)
Absence of Anti-CSRF Tokens (3)
Web Browser XSS Protection Not Enabled (5)
X-Content-Type-Options Header Missing (16)
Alerts 2 1 3 0
Current Scans 0 0 0 0
Thursday, September 19, 2024
Search
16°C
Light rain
ENG
2:39 pm
20/09/2024
Application Security
1 Hr 44 Min Remaining
Instructions
Resources
Help
100%
8. After the scan completes, Alerts tab appears, as shown in the screenshot below.
9. You can observe the vulnerabilities found on the website under the Alerts tab.
10. Now, expand any vulnerability (here, SQL Injection vulnerability) node under the Alerts tab.
Previous
Next: Exercise 5: Detect...


Application Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/010980fd-26f0-434c-9dc7-e2462acb54b5
Admin Machine-1
Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://www.moviescope.com
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
History
Search
Alerts
Output
Spider
Active Scan
Alerts (6)
SQL Injection
POST: http://www.moviescope.com/
Viewstate without MAC Signature (Unsure) (3)
X-Frame-Options Header Not Set (3)
Absence of Anti-CSRF Tokens (3)
Web Browser XSS Protection Not Enabled (5)
X-Content-Type-Options Header Missing (16)
SQL Injection
URL: http://www.moviescope.com/
Risk: High
Confidence: Medium
Parameter: btpwd
Attack: ZAP' OR '1'='1' --
Evidence:
CWE ID: 89
WASC ID: 19
Source: Active (40018 - SQL Injection)
Description:
Alerts 2 1 3 0
Current Scans 0 0 0 0 0 0 0 0 0
Search
16°C
Light rain
ENG
2:39 pm
20/09/2024
Application Security
1 Hr 44 Min Remaining
Instructions
Resources
Help
100%
11. Click on the discovered SQL Injection vulnerability and further click on the vulnerable URL.
12. You can observe information such as Risk, Confidence, Parameter, Attack, etc., regarding the discovered SQL injection vulnerability in the lower right-area, as shown in the screenshot below.
The risks associated with the vulnerability are categorized according to severity of risk as Low, Medium, High, and Informational alerts. Each level of risk is represented by a different flag color:
Red Flag: High risk
Orange Flag: Medium risk
Yellow Flag: Low risk
Blue Flag: Provides details about information
Previous
Next: Exercise 5: Detect...



Report:

As a cyber technician, I understood how continuous scanning of the website with OWASP.ZAP helps to identify, assess the vulnerabilities and list out the threats. A critical SQL injection was detected in one of the application's input fields, it could lead to unauthorised access and data loss. It also listed insecure http header or no header alerts. Understanding of different real time threats, their effects, their categorisation helps to mitigate them in order of high priority to reduce the impact of the threat.

8. **Ilab Module no. and name:** 5. Network Security-Administrative controls

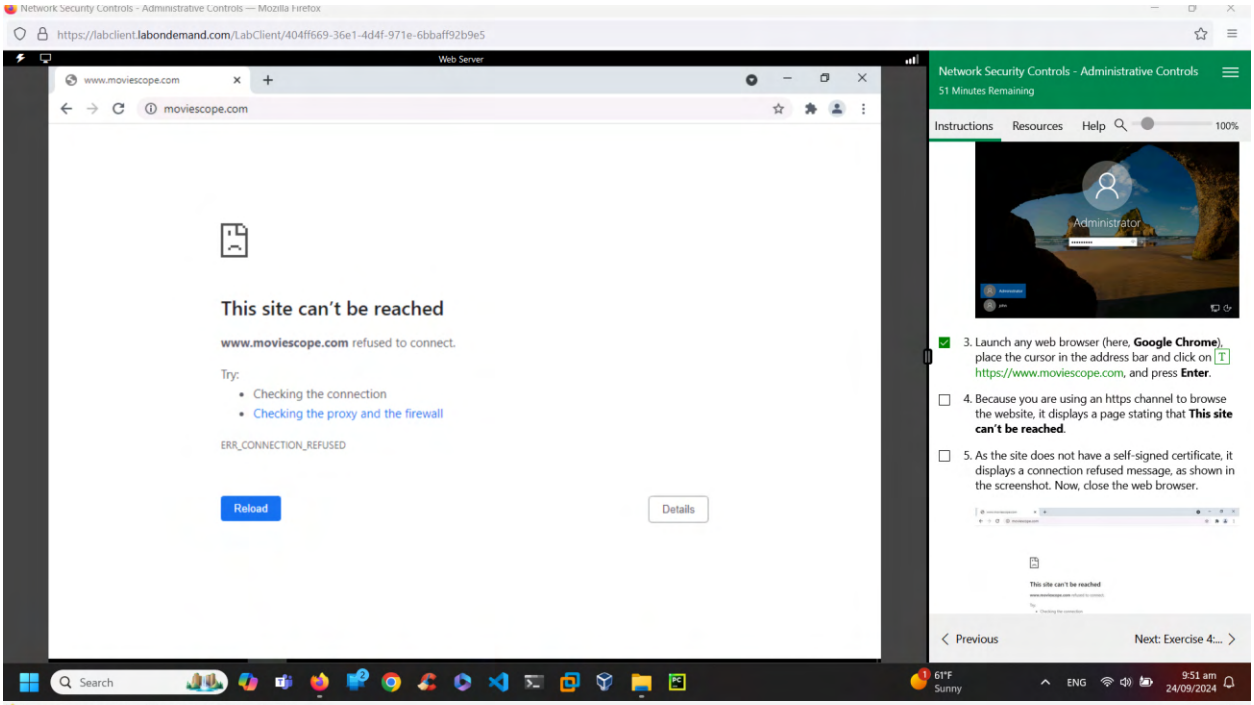
   Exercise no. and name: 3 Implement a Secure Network Policy

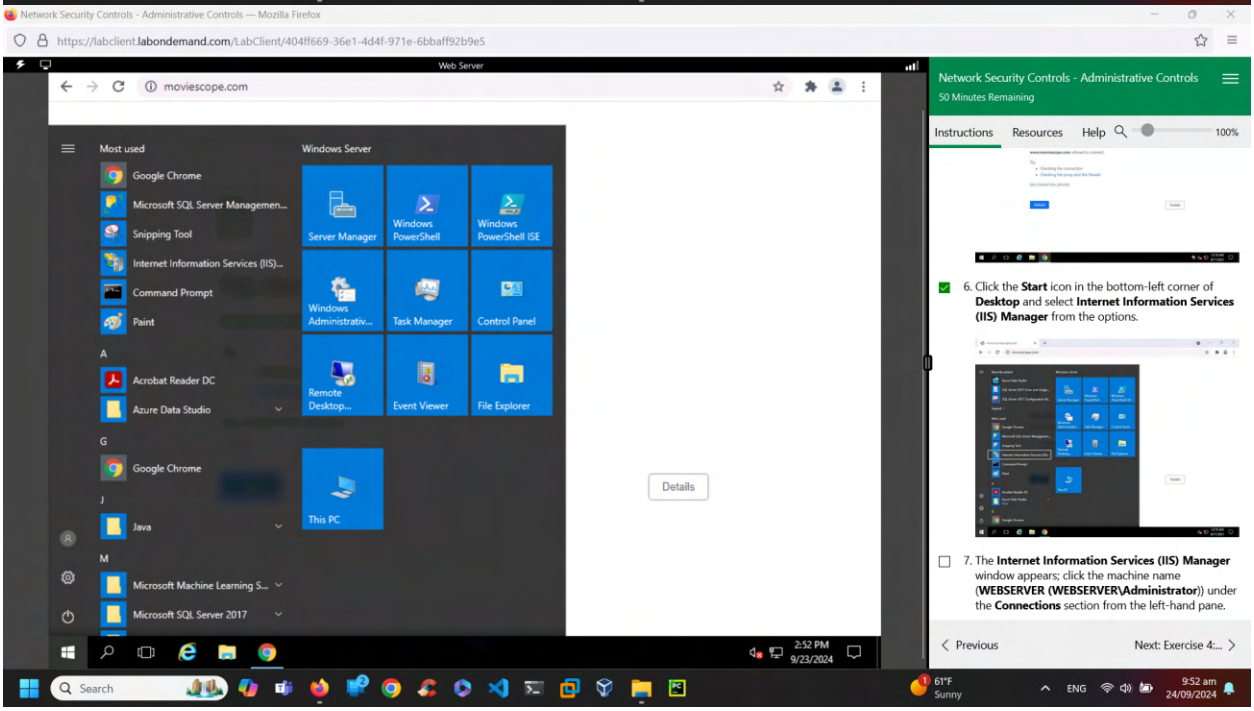
   Performed Date: 24/09/2024

Summary:

This lab demonstrates how to create a self-signed certificate in the IIS for the site moviescope. Use site binding to add https 443 port to the website to make a secure connection and in the authentication enables basic authentication method to enable extra layer of protection.

Screenshots:


Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
www.moviescope.com
moviescope.com
This site can't be reached
www.moviescope.com refused to connect.
Try:
Checking the connection
Checking the proxy and the firewall
ERR_CONNECTION_REFUSED
Reload
Details
Network Security Controls - Administrative Controls
51 Minutes Remaining
Instructions
Resources
Help
100%
Administrator
3. Launch any web browser (here, Google Chrome), place the cursor in the address bar and click on https://www.moviescope.com, and press Enter.
4. Because you are using an https channel to browse the website, it displays a page stating that This site can't be reached.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Now, close the web browser.
Previous
Next: Exercise 4:...
Search
61°F
Sunny
ENG
9:51 am
24/09/2024


Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
moviescope.com
Most used
Google Chrome
Microsoft SQL Server Managemen...
Snipping Tool
Internet Information Services (IIS)...
Command Prompt
Paint
Acrobat Reader DC
Azure Data Studio
Java
Microsoft Machine Learning S...
Microsoft SQL Server 2017
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
This PC
Details
2:52 PM
9/23/2024
Network Security Controls - Administrative Controls
50 Minutes Remaining
Instructions
Resources
Help
100%
6. Click the Start icon in the bottom-left corner of Desktop and select Internet Information Services (IIS) Manager from the options.
7. The Internet Information Services (IIS) Manager window appears; click the machine name (WEBSERVER (WEBSERVER\Administrator)) under the Connections section from the left-hand pane.
Previous
Next: Exercise 4:...
Search
61°F
Sunny
ENG
9:52 am
24/09/2024

Network Security Controls - Administrative Controls — Mozilla Firefox

https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5

Web Server

Start Page

File View Help

Connections

Start Page

WEBSERVER (WEBSERVER\Adi

Microsoft

Internet Information Services 10

Application Server Manager

Recent connections

Name Server

WEBSERVER localhost

Connection tasks

Connect to localhost

Connect to a server...

Connect to a site...

Connect to an application...

Online resources

IIS News and Information

IIS Downloads

IIS Forums

TechNet

MSDN

ASP.NET News

Microsoft Web Platform

IIS News Enable IIS News

IIS News is disabled, click the Enable IIS News link to get the most recent online news.

Ready

Monday, September 23, 2024

2:52 PM 9/23/2024

Search

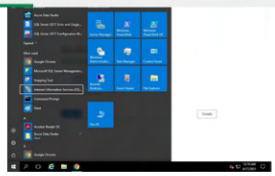
61°F Sunny

ENG 9:52 am 24/09/2024

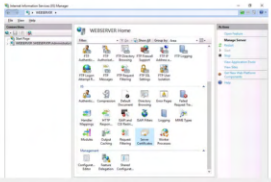
Network Security Controls - Administrative Controls

50 Minutes Remaining

Instructions Resources Help 100%



- [x] 7. The **Internet Information Services (IIS) Manager** window appears; click the machine name (**WEBSERVER (WEBSERVER\Administrator)**) under the **Connections** section from the left-hand pane.
- [ ] 8. In **WEBSERVER Home**, double-click **Server Certificates** in the **IIS** section.



Previous Next: Exercise 4:...

Network Security Controls — Mozilla Firefox

https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5

Web Server

WEBSERVER

File View Help

Connections

Start Page

WEBSERVER (WEBSERVER\Adi

Application Pools

Sites

WEBSERVER Home

Filter: Go Show All Group by: Area

Controls

FTP

FTP Authentic... FTP Authorizat... FTP Directory Browsing FTP Firewall Support FTP IP Address a... FTP Logging FTP Logon Attempt R...

FTP Messages FTP Request Filtering FTP SSL Settings FTP User Isolation

IIS

Authentic... Compression Default Document Directory Browsing Error Pages Failed Request Tra... Handler Mappings

HTTP Respon... ISAPI and CGI Restri... ISAPI Filters Logging MIME Types Modules Output Caching

Request Filtering Server Certificates Worker Processes

Management

Features View Content View

Actions

Open Feature

Manage Server

Restart

Start

Stop

View Application Pools

View Sites

Get New Web Platform Components

Help

Ready

2:53 PM 9/23/2024

Search

61°F Sunny

ENG 9:53 am 24/09/2024

Network Security Controls - Administrative Controls

49 Minutes Remaining

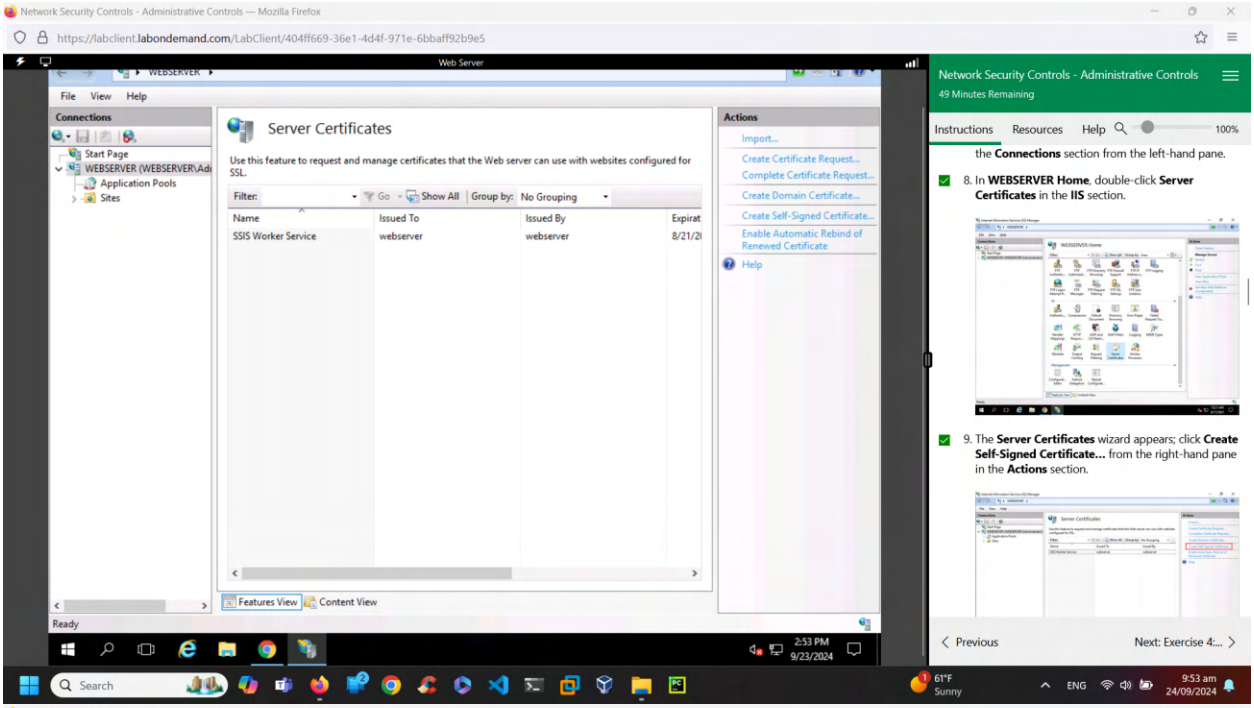
Instructions Resources Help 100%

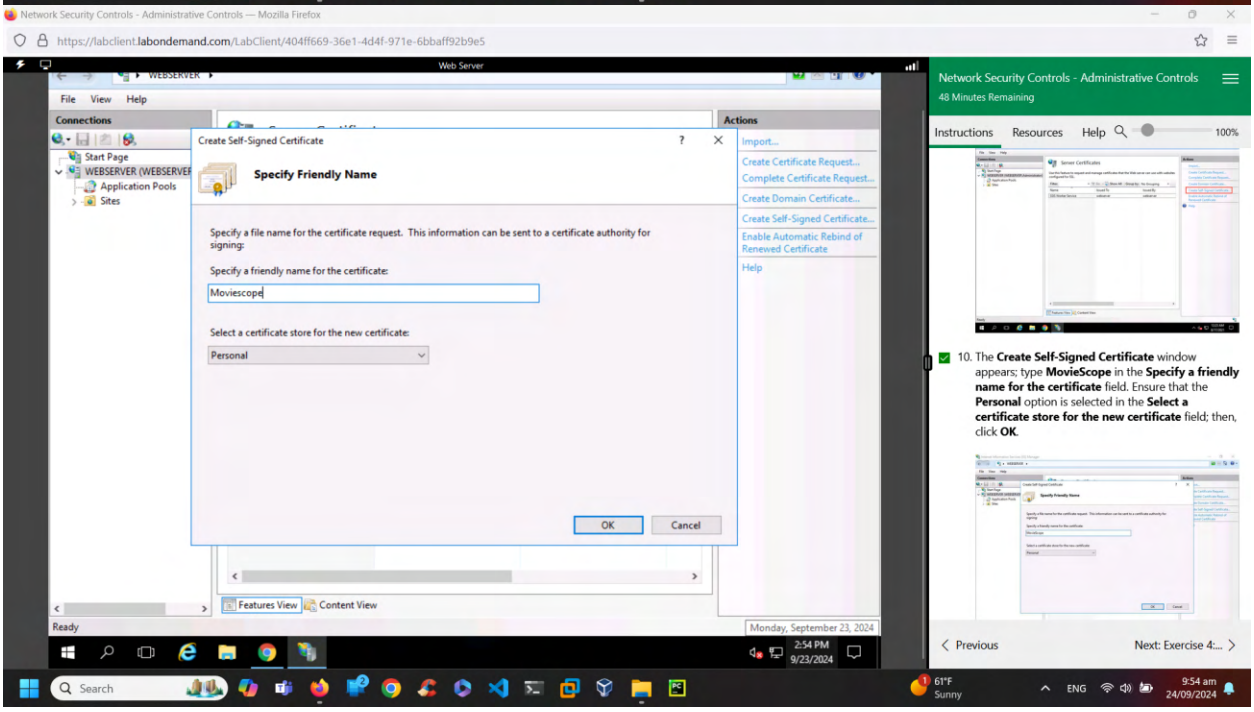
the **Connections** section from the left-hand pane.

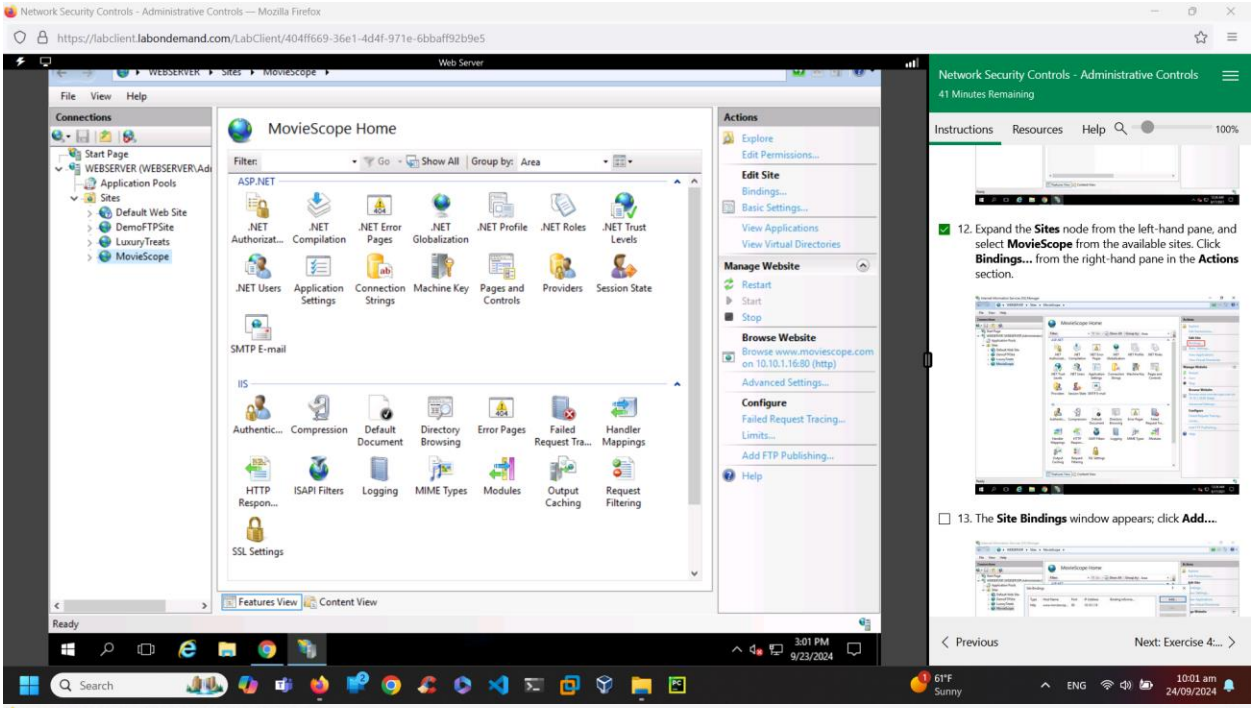
- [x] 8. In **WEBSERVER Home**, double-click **Server Certificates** in the **IIS** section.

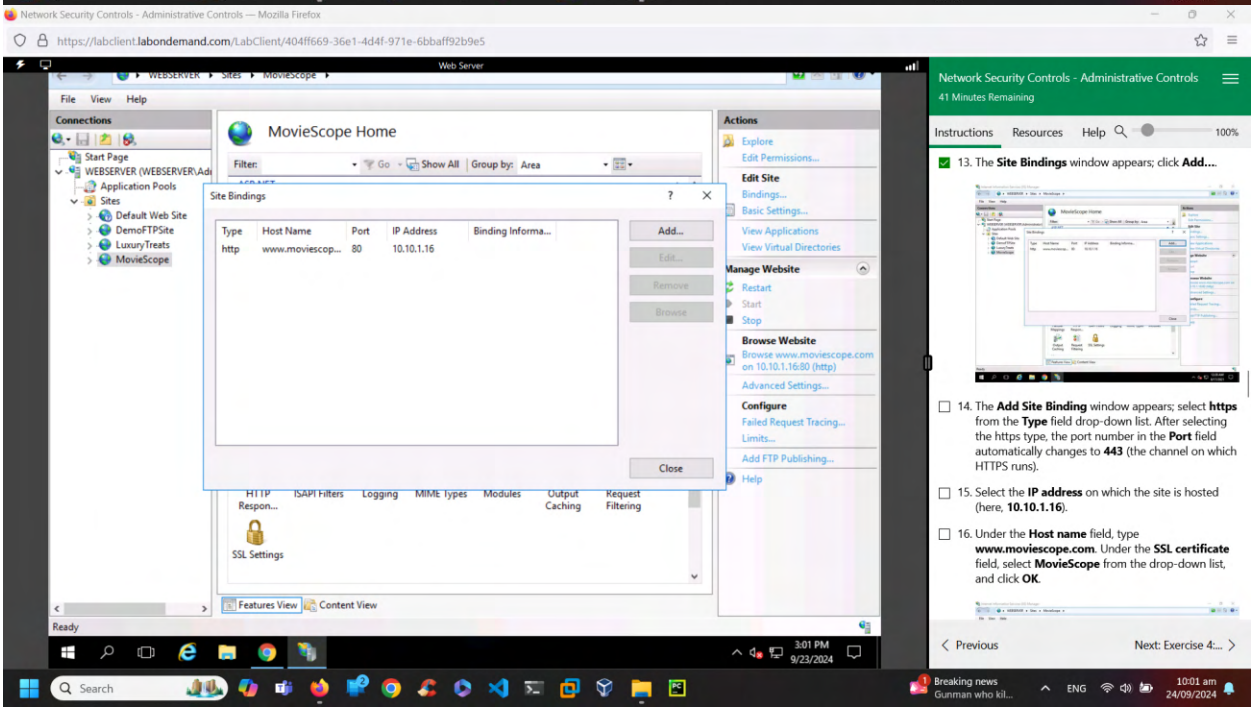
- [x] 9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.

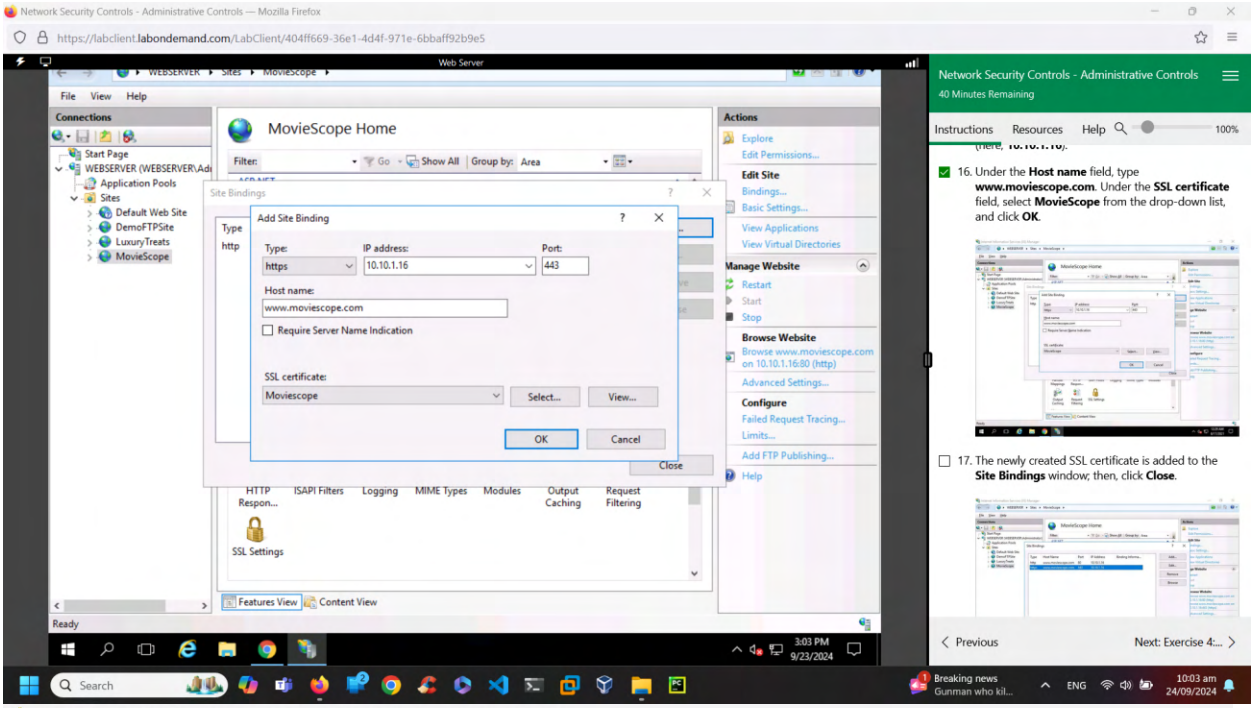
Previous Next: Exercise 4:...


Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
File View Help
Connections
Start Page
WEBSERVER (WEBSERVER\Ad
Application Pools
Sites
Server Certificates
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.
Filter:
Go
Show All
Group by: No Grouping
Name
Issued To
Issued By
Expirat
SSIS Worker Service
webserver
webserver
8/21/2
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
2:53 PM
9/23/2024
Network Security Controls - Administrative Controls
49 Minutes Remaining
Instructions
Resources
Help
100%
the Connections section from the left-hand pane.
8. In WEBSERVER Home, double-click Server Certificates in the IIS section.
9. The Server Certificates wizard appears; click Create Self-Signed Certificate... from the right-hand pane in the Actions section.
Previous
Next: Exercise 4:...
Search
61°F
Sunny
ENG
9:53 am
24/09/2024

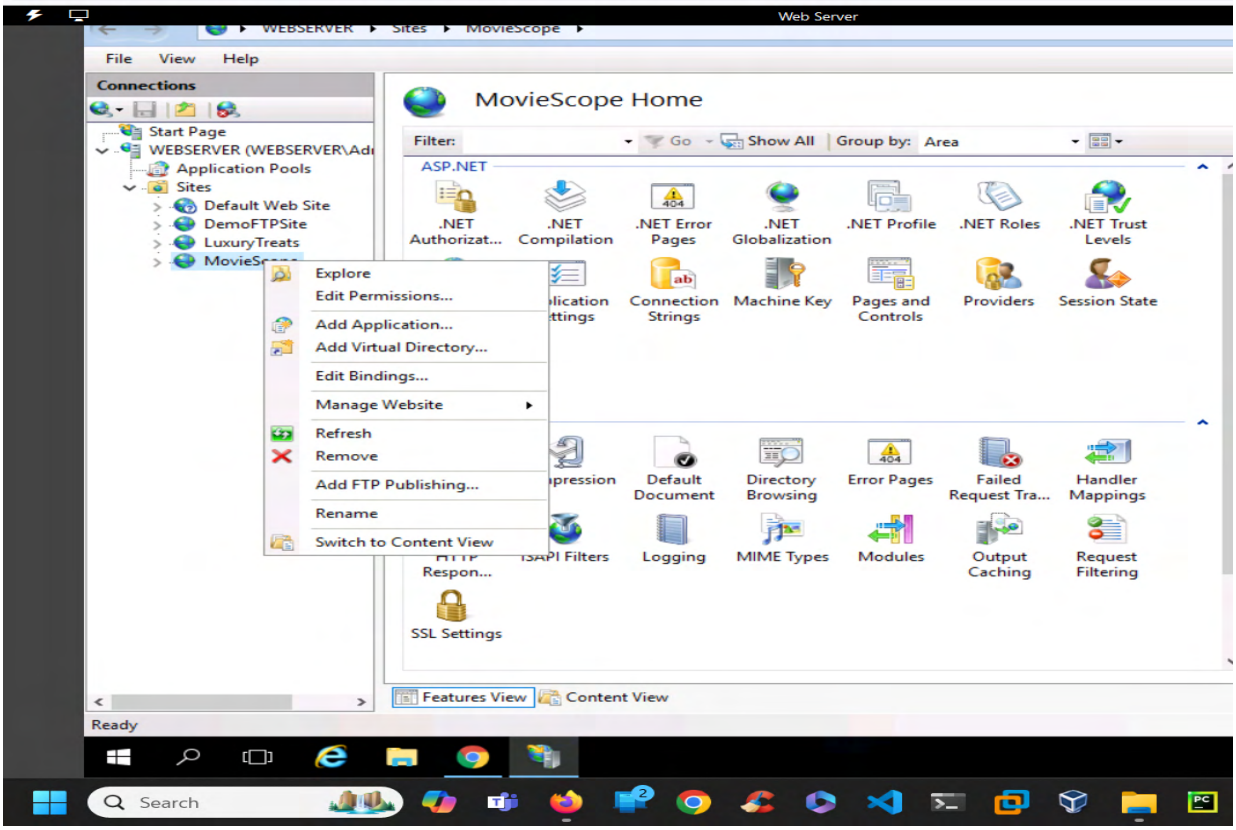

Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
File View Help
Connections
Start Page
WEBSERVER (WEBSERVER
Application Pools
Sites
Create Self-Signed Certificate
Specify Friendly Name
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:
Specify a friendly name for the certificate:
Moviescope
Select a certificate store for the new certificate:
Personal
OK
Cancel
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
Monday, September 23, 2024
2:54 PM
9/23/2024
Network Security Controls - Administrative Controls
48 Minutes Remaining
Instructions
Resources
Help
100%
10. The Create Self-Signed Certificate window appears; type MovieScope in the Specify a friendly name for the certificate field. Ensure that the Personal option is selected in the Select a certificate store for the new certificate field; then, click OK.
Previous
Next: Exercise 4:...
Search
61°F
Sunny
ENG
9:54 am
24/09/2024

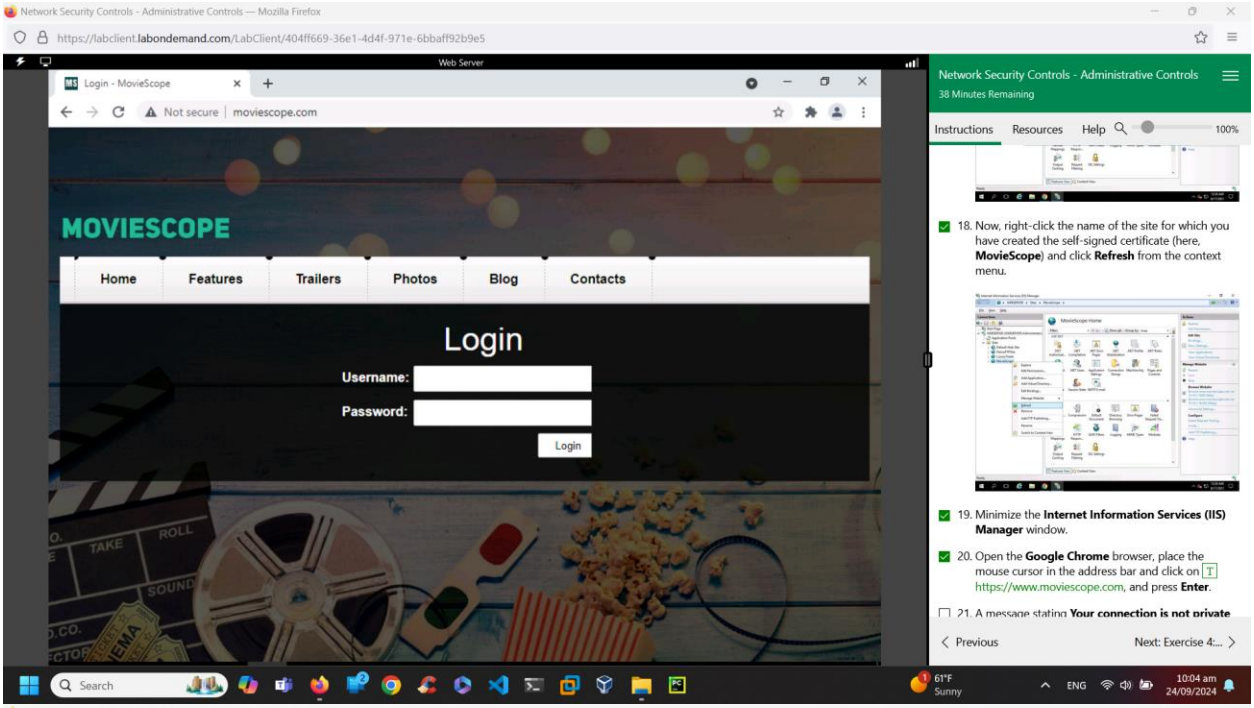

Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
File View Help
Connections
Start Page
WEBSERVER (WEBSERVER\Adi
Application Pools
Sites
Default Web Site
DemoFTPSite
LuxuryTreats
MovieScope
MovieScope Home
Filter:
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
.NET Trust Levels
.NET Users
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Respon...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Features View
Content View
Ready
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse www.moviescope.com on 10.10.1.16:80 (http)
Advanced Settings...
Configure
Failed Request Tracing...
Limits...
Add FTP Publishing...
Help
3:01 PM
9/23/2024
Network Security Controls - Administrative Controls
41 Minutes Remaining
Instructions
Resources
Help
100%
12. Expand the Sites node from the left-hand pane, and select MovieScope from the available sites. Click Bindings... from the right-hand pane in the Actions section.
13. The Site Bindings window appears; click Add...
Previous
Next: Exercise 4:...
Search
61°F
Sunny
ENG
10:01 am
24/09/2024

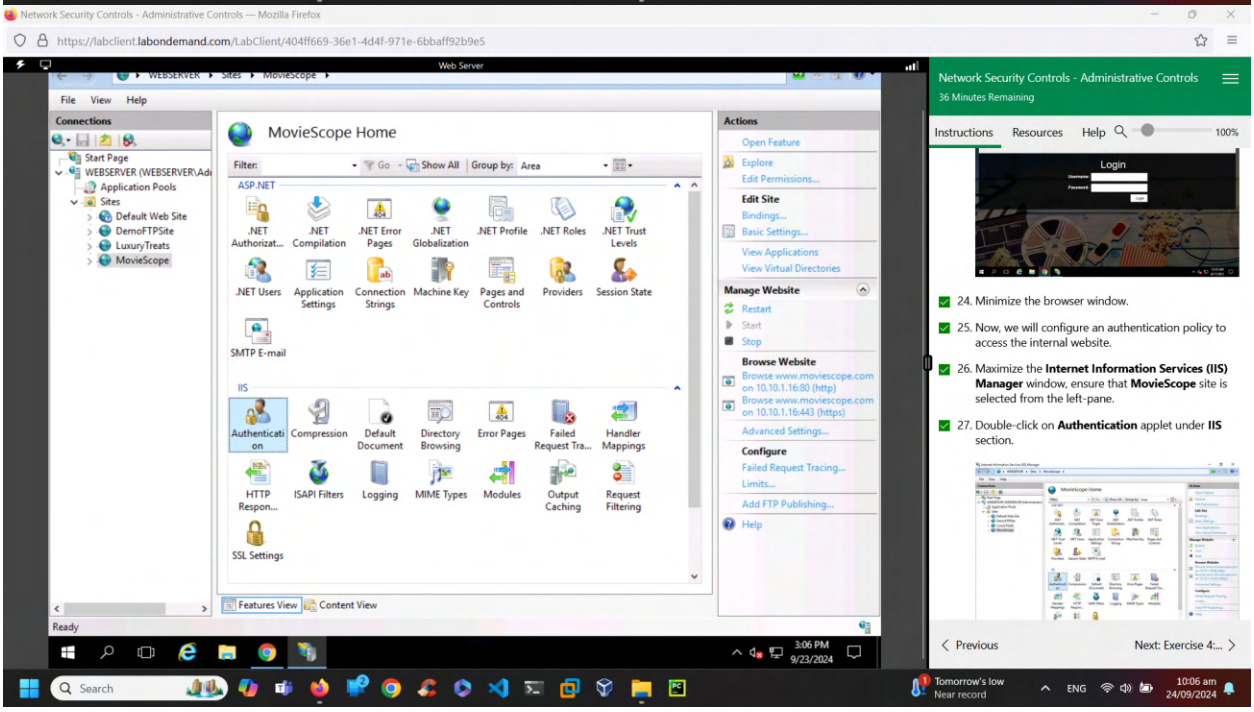

Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
File View Help
Connections
Start Page
WEBSERVER (WEBSERVER\Adi
Application Pools
Sites
Default Web Site
DemoFTPSite
LuxuryTreats
MovieScope
MovieScope Home
Filter:
Show All
Group by: Area
Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
http
www.moviescop...
80
10.10.1.16
Add...
Edit...
Remove
Browse
Close
HTTP Respon...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Features View
Content View
Ready
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse www.moviescope.com on 10.10.1.16:80 (http)
Advanced Settings...
Configure
Failed Request Tracing...
Limits...
Add FTP Publishing...
Help
3:01 PM
9/23/2024
Network Security Controls - Administrative Controls
41 Minutes Remaining
Instructions
Resources
Help
100%
13. The Site Bindings window appears; click Add...
14. The Add Site Binding window appears; select https from the Type field drop-down list. After selecting the https type, the port number in the Port field automatically changes to 443 (the channel on which HTTPS runs).
15. Select the IP address on which the site is hosted (here, 10.10.1.16).
16. Under the Host name field, type www.moviescope.com. Under the SSL certificate field, select MovieScope from the drop-down list, and click OK.
Previous
Next: Exercise 4:...
Search
Breaking news
Gunman who kil...
ENG
10:01 am
24/09/2024

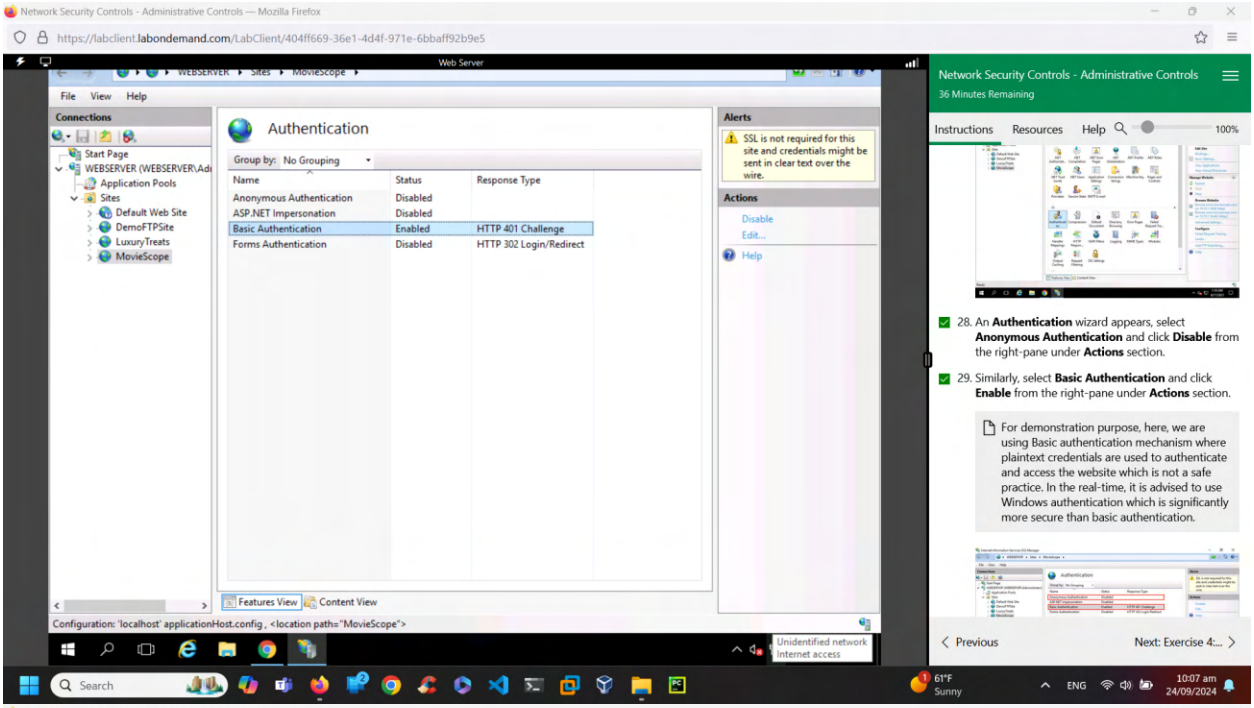


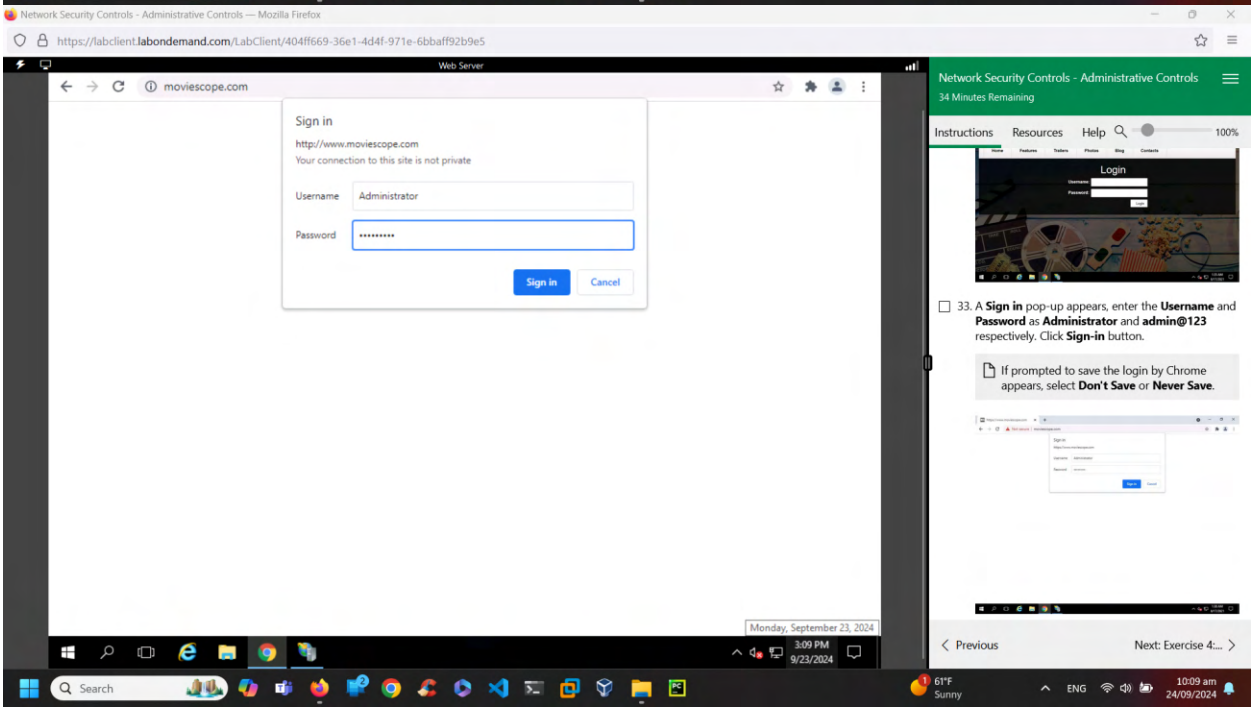
Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5

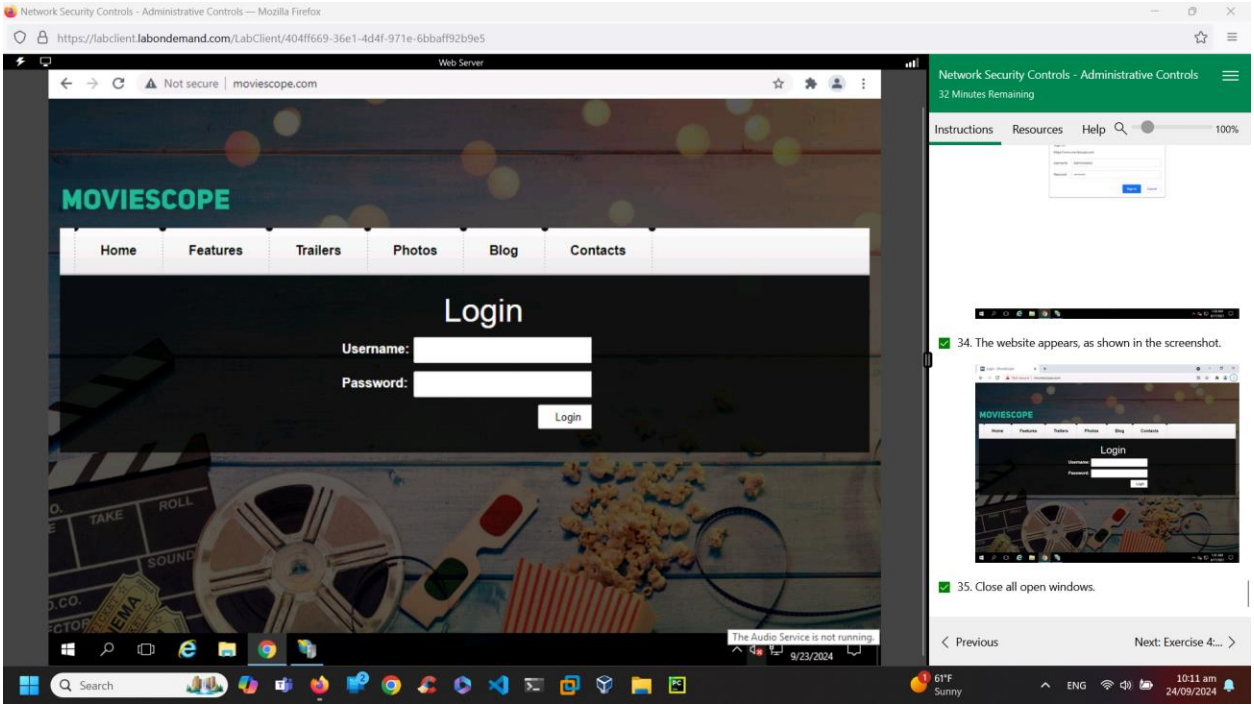



Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
Login - MovieScope
Not secure | moviescope.com
MOVIESCOPE
Home
Features
Trailers
Photos
Blog
Contacts
Login
Username:
Password:
Login
Network Security Controls - Administrative Controls
38 Minutes Remaining
Instructions
Resources
Help
100%
18. Now, right-click the name of the site for which you have created the self-signed certificate (here, MovieScope) and click Refresh from the context menu.
19. Minimize the Internet Information Services (IIS) Manager window.
20. Open the Google Chrome browser, place the mouse cursor in the address bar and click on https://www.moviescope.com, and press Enter.
21. A message stating Your connection is not private
Previous
Next: Exercise 4:...
Search
61°F
Sunny
ENG
10:04 am
24/09/2024


Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
File View Help
Connections
Start Page
WEBSERVER (WEBSERVER\Ad
Application Pools
Sites
Default Web Site
DemoFTPSite
LuxuryTreats
MovieScope
MovieScope Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
.NET Trust Levels
.NET Users
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
Authenticati on
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Respon...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Features View
Content View
Ready
Actions
Open Feature
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse www.moviescope.com on 10.10.1.16:80 (http)
Browse www.moviescope.com on 10.10.1.16:443 (https)
Advanced Settings...
Configure
Failed Request Tracing...
Limits...
Add FTP Publishing...
Help
3:06 PM
9/23/2024
Network Security Controls - Administrative Controls
36 Minutes Remaining
Instructions
Resources
Help
100%
Login
24. Minimize the browser window.
25. Now, we will configure an authentication policy to access the internal website.
26. Maximize the Internet Information Services (IIS) Manager window, ensure that MovieScope site is selected from the left-pane.
27. Double-click on Authentication applet under IIS section.
Previous
Next: Exercise 4:...
Search
Tomorrow's low
Near record
ENG
10:06 am
24/09/2024


Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
File View Help
Connections
Start Page
WEBSERVER (WEBSERVER\Adi
Application Pools
Sites
Default Web Site
DemoFTPSite
LuxuryTreats
MovieScope
Authentication
Group by: No Grouping
Name Status Response Type
Anonymous Authentication Disabled
ASP.NET Impersonation Disabled
Basic Authentication Enabled HTTP 401 Challenge
Forms Authentication Disabled HTTP 302 Login/Redirect
Alerts
SSL is not required for this site and credentials might be sent in clear text over the wire.
Actions
Disable
Edit...
Help
Features View
Content View
Configuration: 'localhost' applicationHost.config , <location path="MovieScope">
Unidentified network
Internet access
Search
61°F
Sunny
ENG
10:07 am
24/09/2024
Network Security Controls - Administrative Controls
36 Minutes Remaining
Instructions
Resources
Help
100%
28. An Authentication wizard appears, select Anonymous Authentication and click Disable from the right-pane under Actions section.
29. Similarly, select Basic Authentication and click Enable from the right-pane under Actions section.
For demonstration purpose, here, we are using Basic authentication mechanism where plaintext credentials are used to authenticate and access the website which is not a safe practice. In the real-time, it is advised to use Windows authentication which is significantly more secure than basic authentication.
Previous
Next: Exercise 4:...


Network Security Controls - Administrative Controls — Mozilla Firefox
https://labclient.labondemand.com/LabClient/404ff669-36e1-4d4f-971e-6bbaff92b9e5
Web Server
moviescope.com
Sign in
http://www.moviescope.com
Your connection to this site is not private
Username Administrator
Password
Sign in
Cancel
Monday, September 23, 2024
3:09 PM
9/23/2024
Search
61°F
Sunny
ENG
10:09 am
24/09/2024
Network Security Controls - Administrative Controls
34 Minutes Remaining
Instructions
Resources
Help
100%
Login
33. A Sign in pop-up appears, enter the Username and Password as Administrator and admin@123 respectively. Click Sign-in button.
If prompted to save the login by Chrome appears, select Don't Save or Never Save.
Previous
Next: Exercise 4:...



Reports:

As a cyber technician, implementing an SSL certificate ensures a secure connection between the server and clients. If the document/data is encrypted, it is protected in all stage like data in rest, data in transit and data in state. It also redirects insecure http to https, ensuring all the connections are secured.

9. **Ilab Module no. and name:** 15. Data Security

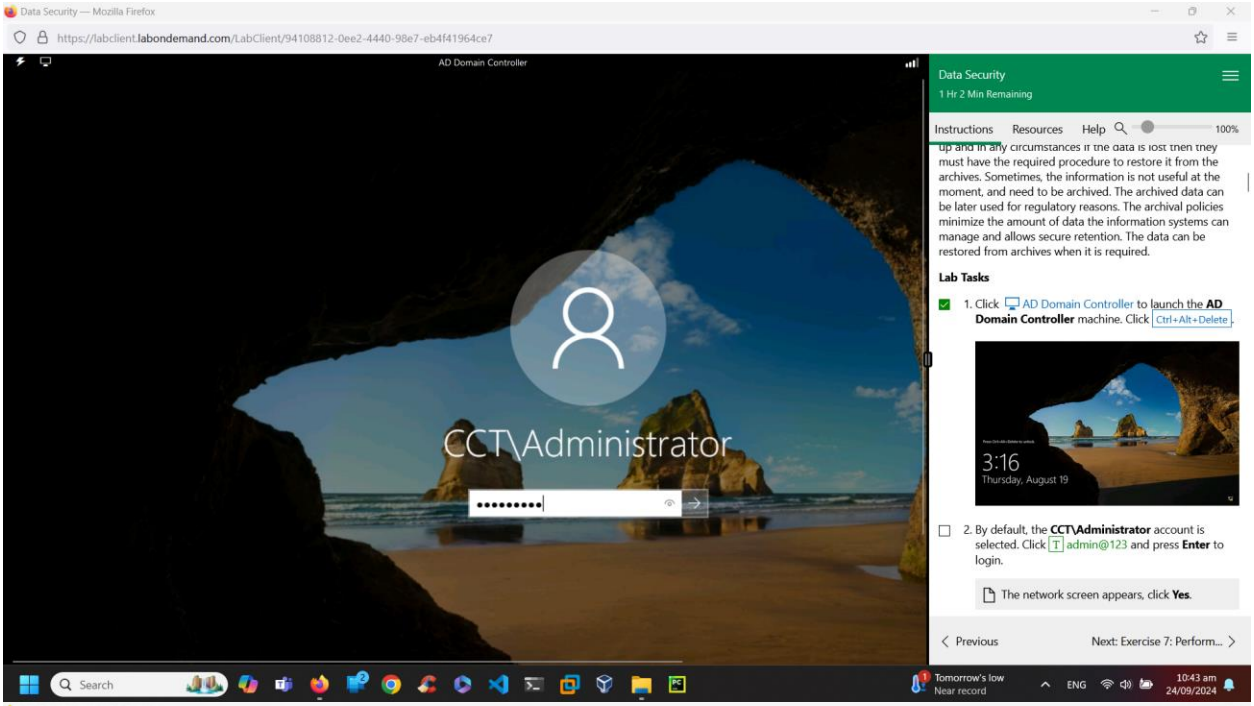
   Exercise no. and name: 6 Back Up and Restore Data in Windows

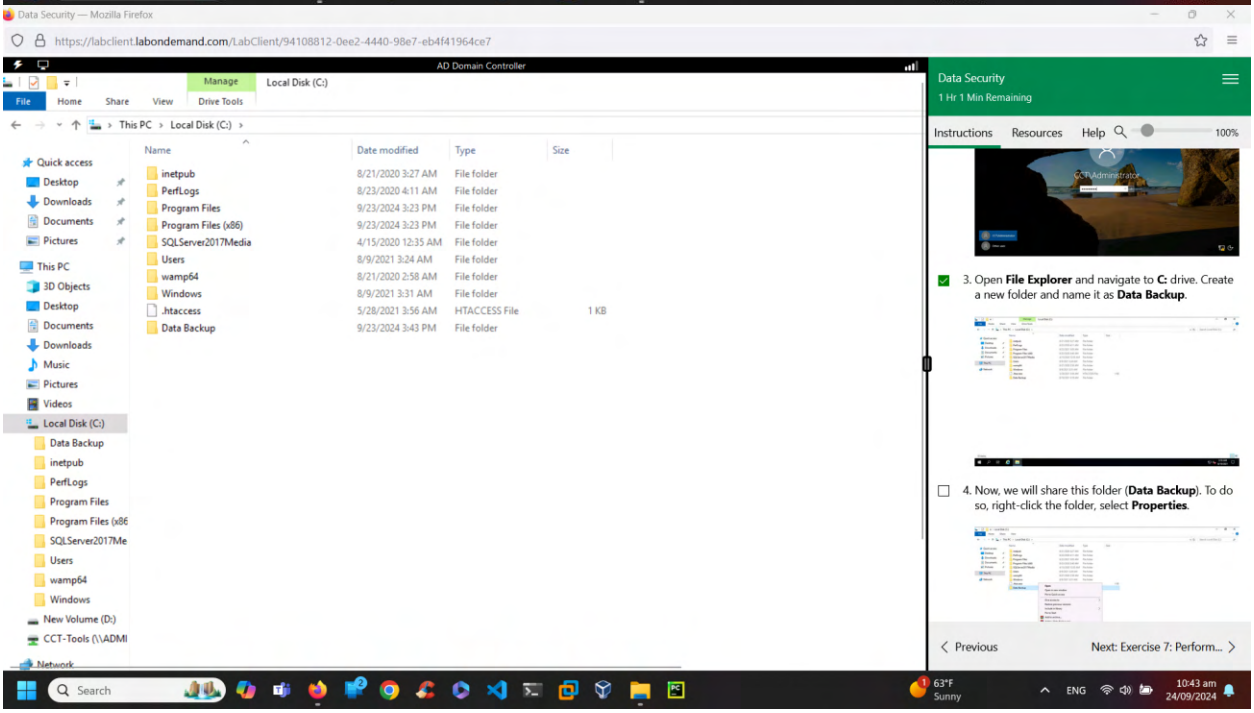
   Performed Date: 24/09/2024

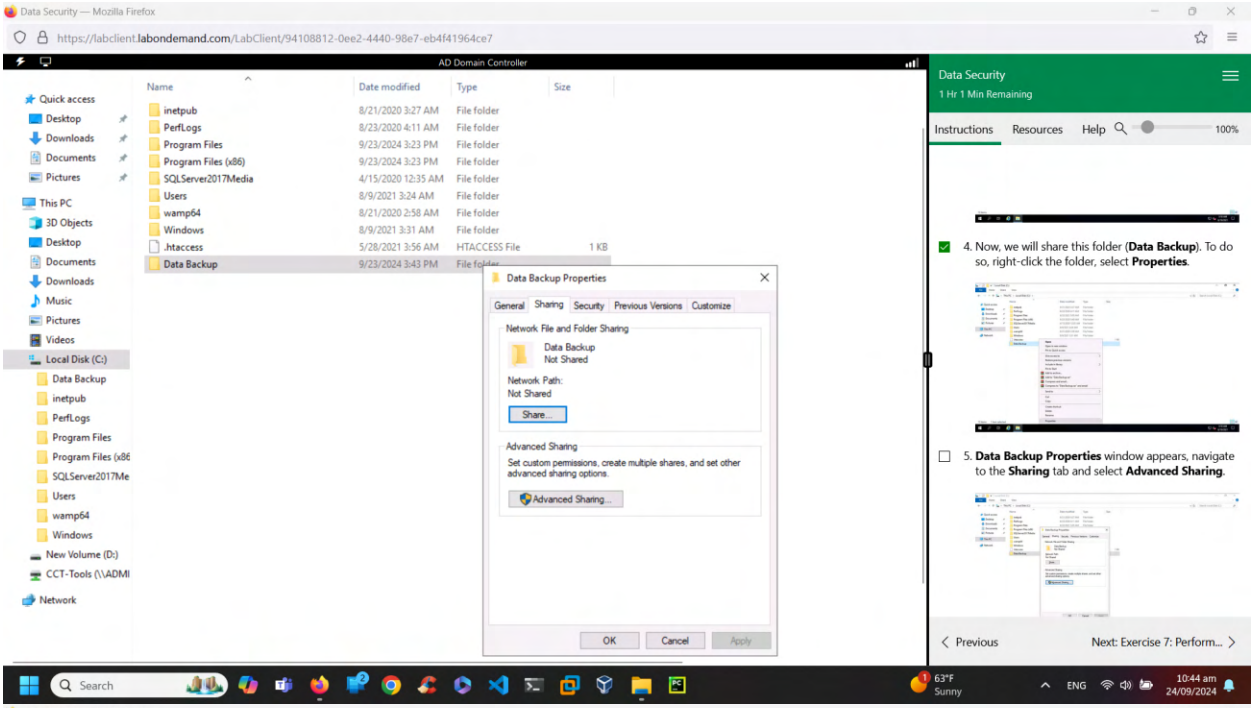
Summary:

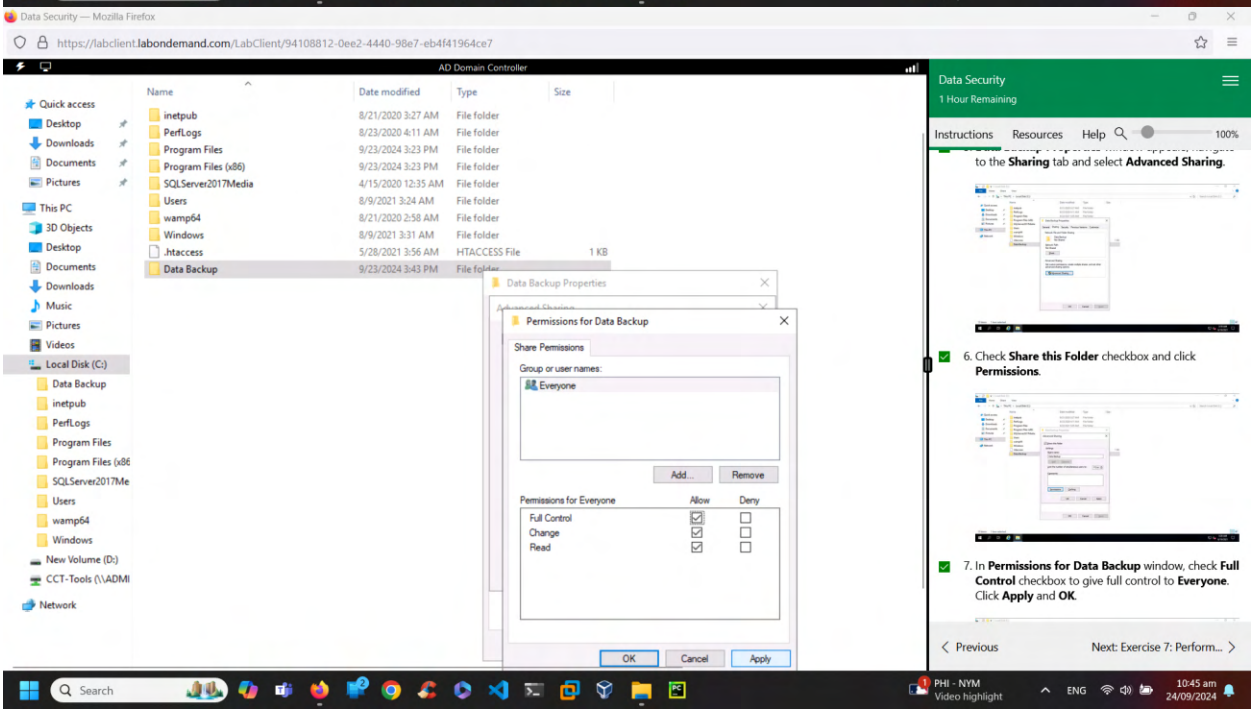
The lab demonstrates how to back up the data in a destination folder using Server manager tools. It also shows if the internal files folder is deleted, step by steps to retrieve the data using recovery wizard which fetches the files and stored in a folder called data recovered.

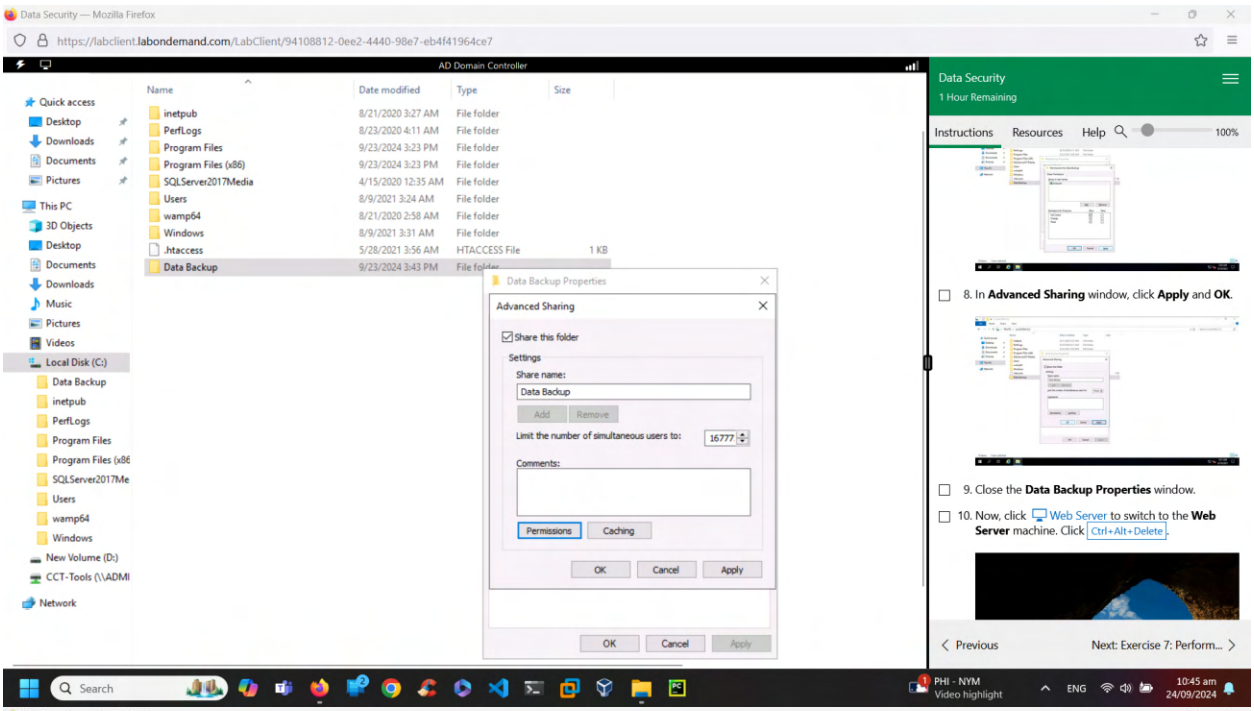
Screenshots:

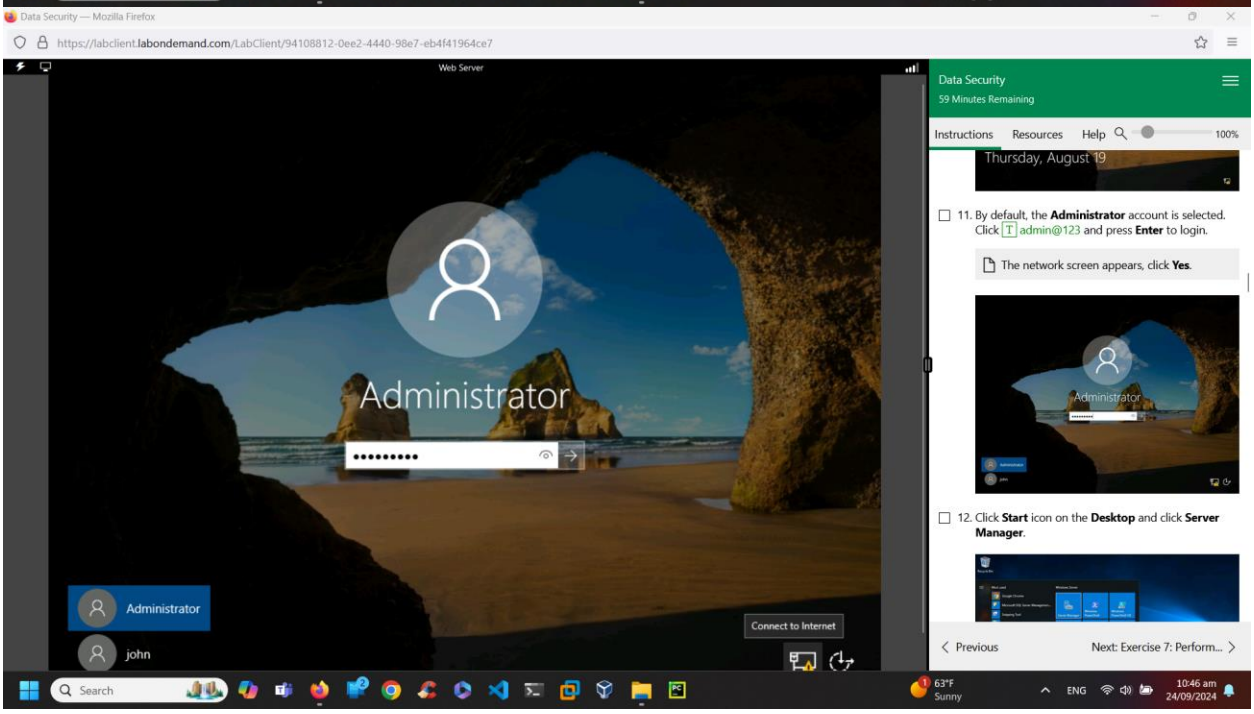

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
AD Domain Controller
CCT\Administrator
Data Security
1 Hr 2 Min Remaining
Instructions
Resources
Help
100%
must have the required procedure to restore it from the archives. Sometimes, the information is not useful at the moment, and need to be archived. The archived data can be later used for regulatory reasons. The archival policies minimize the amount of data the information systems can manage and allows secure retention. The data can be restored from archives when it is required.
Lab Tasks
1. Click AD Domain Controller to launch the AD Domain Controller machine. Click Ctrl+Alt+Delete.
3:16
Thursday, August 19
2. By default, the CCT\Administrator account is selected. Click admin@123 and press Enter to login.
The network screen appears, click Yes.
Previous
Next: Exercise 7: Perform...
Search
Tomorrow's low
Near record
ENG
10:43 am
24/09/2024

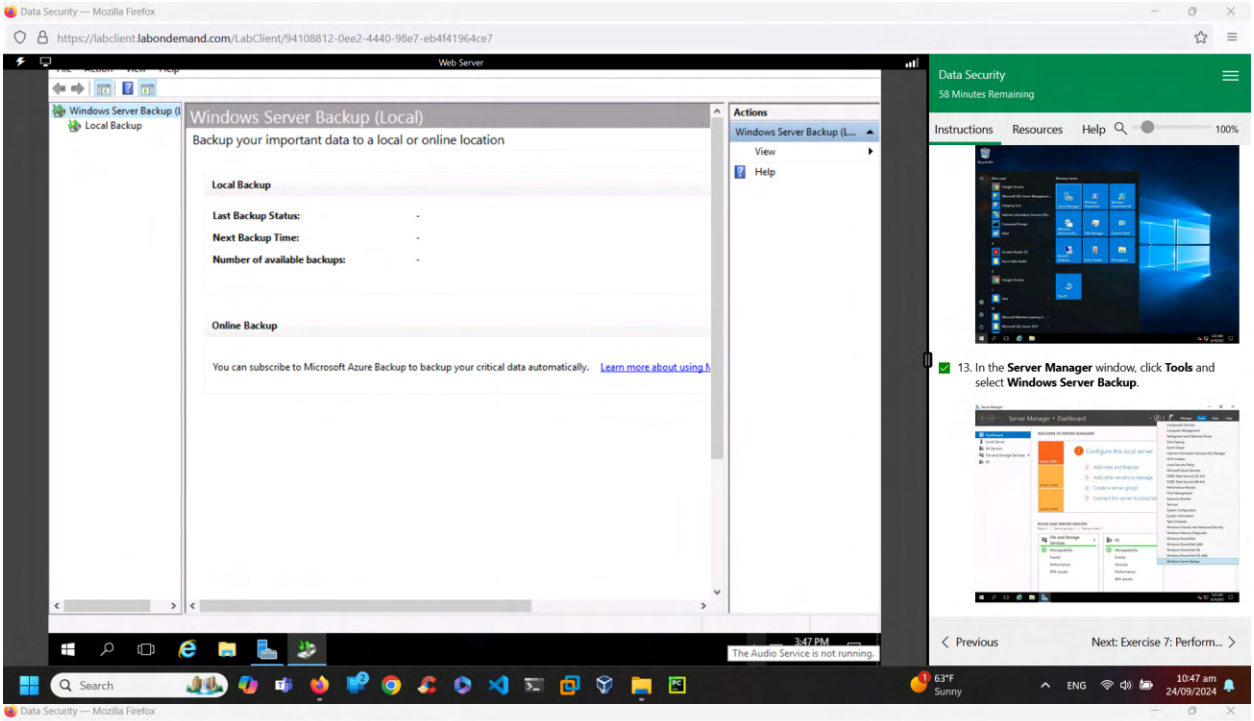

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
AD Domain Controller
Manage
Local Disk (C:)
File
Home
Share
View
Drive Tools
This PC › Local Disk (C:) ›
Quick access
Desktop
Downloads
Documents
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Data Backup
inetpub
PerfLogs
Program Files
Program Files (x86)
SQLServer2017Me
Users
wamp64
Windows
New Volume (D:)
CCT-Tools (\\ADMI
Network
Name
Date modified
Type
Size
inetpub 8/21/2020 3:27 AM File folder
PerfLogs 8/23/2020 4:11 AM File folder
Program Files 9/23/2024 3:23 PM File folder
Program Files (x86) 9/23/2024 3:23 PM File folder
SQLServer2017Media 4/15/2020 12:35 AM File folder
Users 8/9/2021 3:24 AM File folder
wamp64 8/21/2020 2:58 AM File folder
Windows 8/9/2021 3:31 AM File folder
.htaccess 5/28/2021 3:56 AM HTACCESS File 1 KB
Data Backup 9/23/2024 3:43 PM File folder
Data Security
1 Hr 1 Min Remaining
Instructions
Resources
Help
100%
3. Open File Explorer and navigate to C: drive. Create a new folder and name it as Data Backup.
4. Now, we will share this folder (Data Backup). To do so, right-click the folder, select Properties.
Previous
Next: Exercise 7: Perform...
Search
63°F
Sunny
ENG
10:43 am
24/09/2024

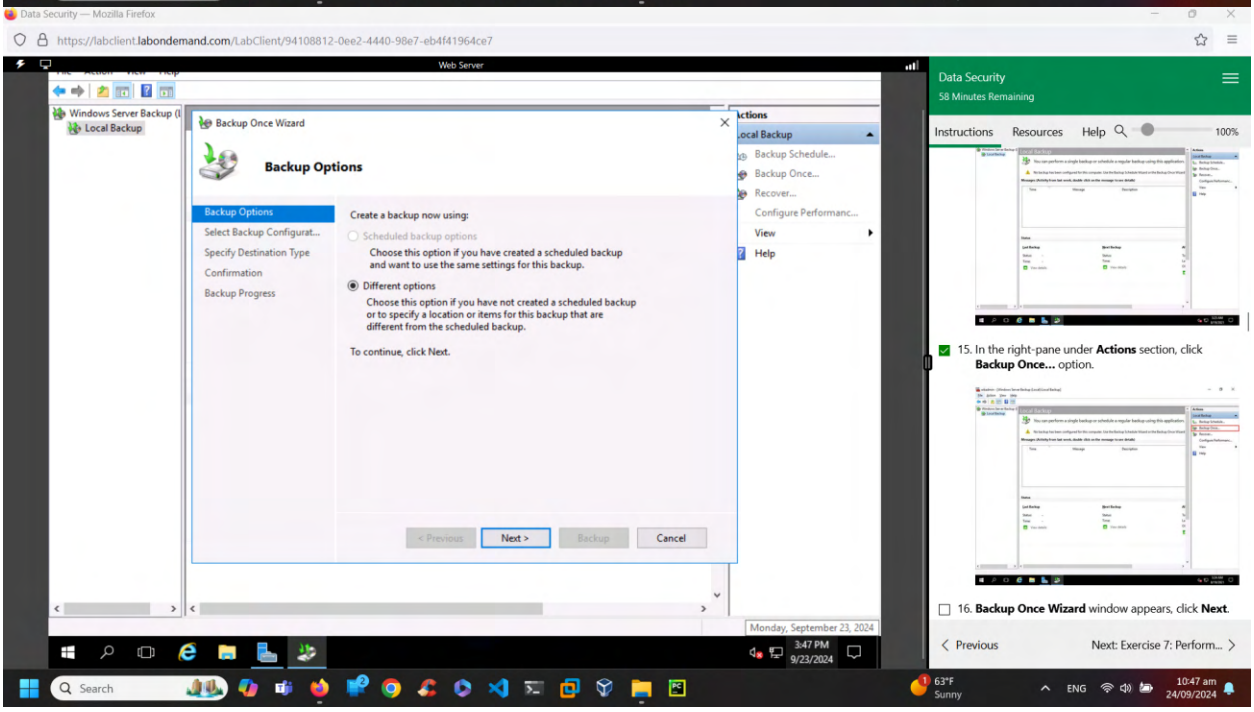

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
AD Domain Controller
Data Backup Properties
General Sharing Security Previous Versions Customize
Network File and Folder Sharing
Data Backup
Not Shared
Network Path:
Not Shared
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
OK Cancel Apply
Data Security
1 Hr 1 Min Remaining
Instructions Resources Help 100%
4. Now, we will share this folder (Data Backup). To do so, right-click the folder, select Properties.
5. Data Backup Properties window appears, navigate to the Sharing tab and select Advanced Sharing.
Previous
Next: Exercise 7: Perform...
Search
63°F Sunny
ENG
10:44 am 24/09/2024

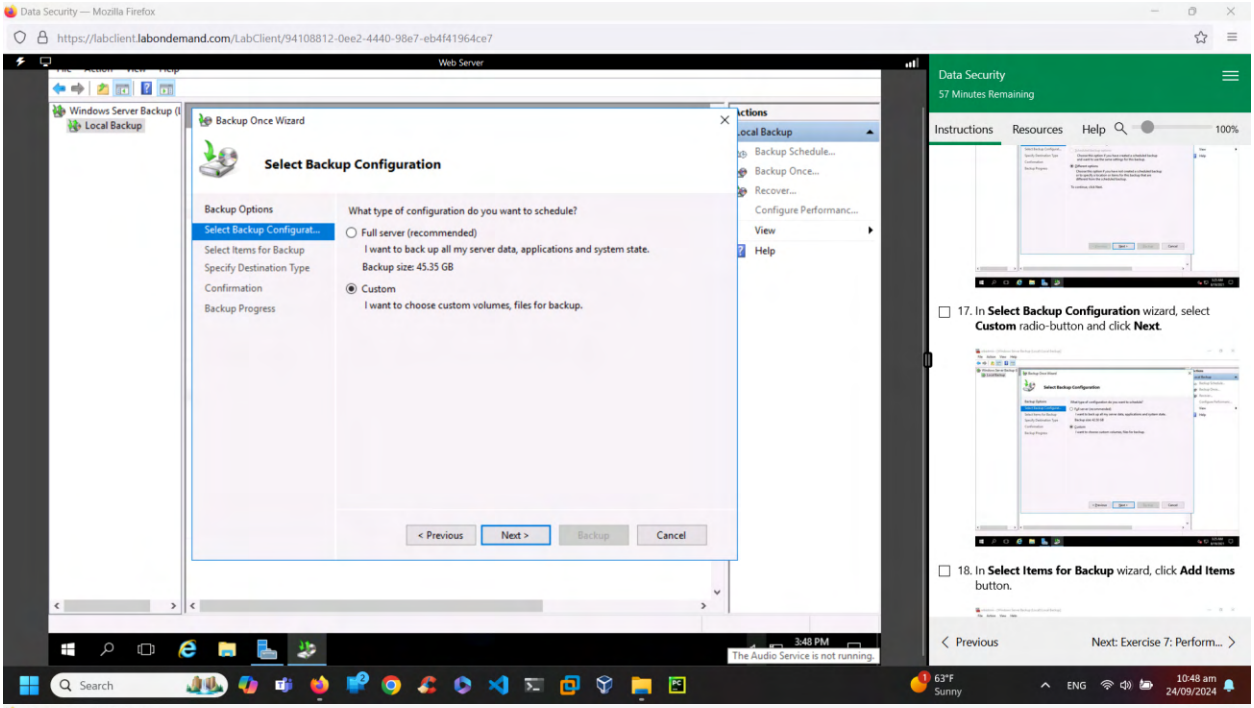

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
AD Domain Controller
Permissions for Data Backup
Share Permissions
Group or user names:
Everyone
Add... Remove
Permissions for Everyone Allow Deny
Full Control
Change
Read
OK Cancel Apply
Data Security
1 Hour Remaining
Instructions Resources Help 100%
to the Sharing tab and select Advanced Sharing.
6. Check Share this Folder checkbox and click Permissions.
7. In Permissions for Data Backup window, check Full Control checkbox to give full control to Everyone. Click Apply and OK.
Previous
Next: Exercise 7: Perform...
Search
PHI - NYM Video highlight
ENG
10:45 am 24/09/2024

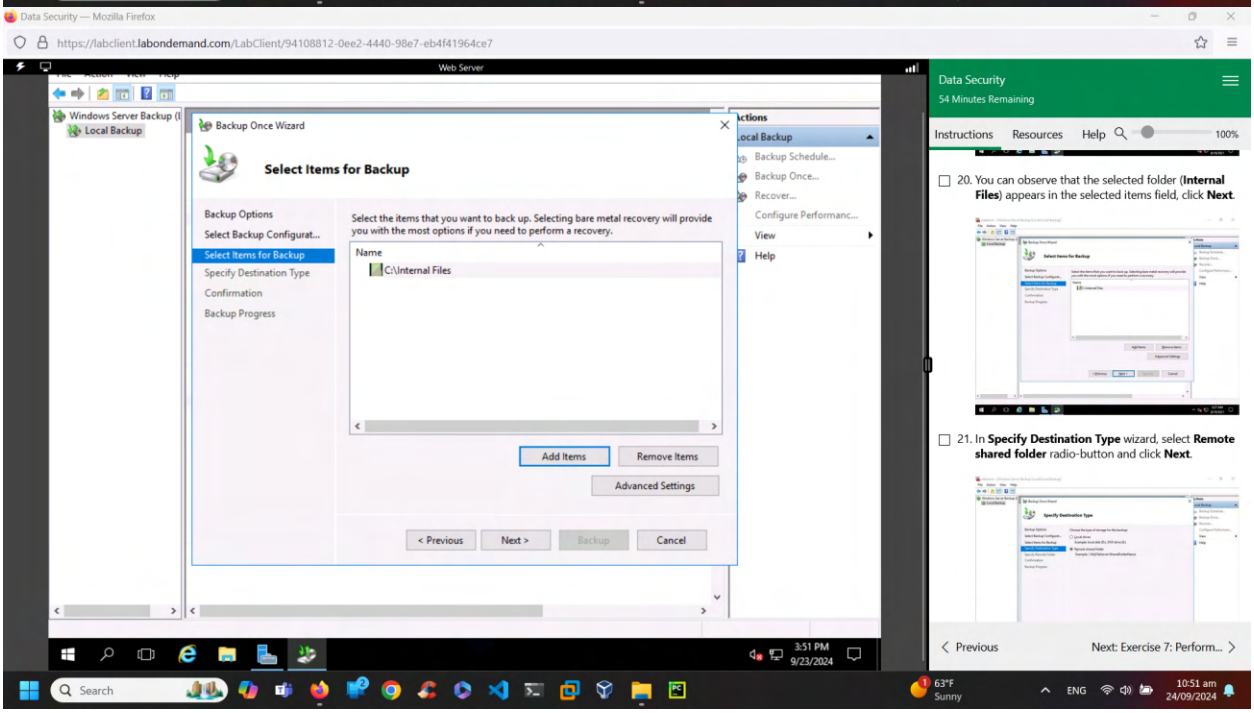

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
AD Domain Controller
Data Backup Properties
Advanced Sharing
Share this folder
Settings
Share name:
Data Backup
Add
Remove
Limit the number of simultaneous users to:
16777
Comments:
Permissions
Caching
OK
Cancel
Apply
Data Security
1 Hour Remaining
Instructions
Resources
Help
100%
8. In Advanced Sharing window, click Apply and OK.
9. Close the Data Backup Properties window.
10. Now, click Web Server to switch to the Web Server machine. Click Ctrl+Alt+Delete.
Previous
Next: Exercise 7: Perform...
Search
PHI - NYM
Video highlight
ENG
10:45 am
24/09/2024

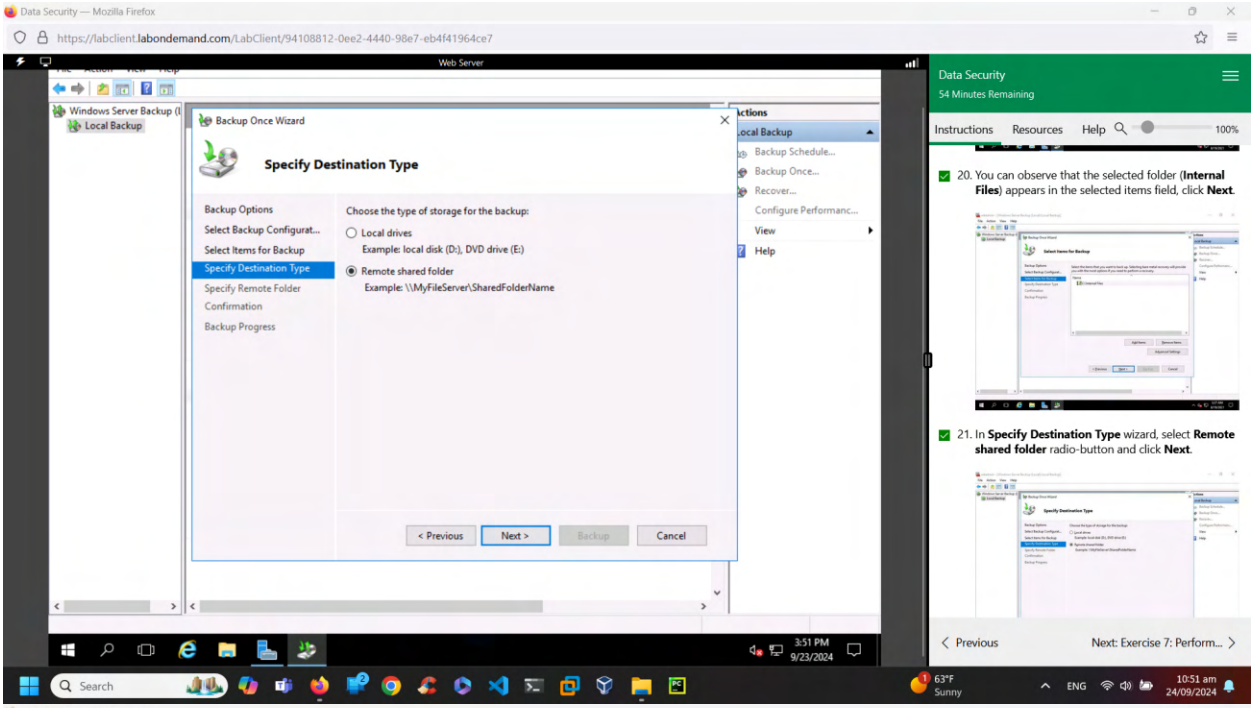

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Administrator
Administrator
john
Connect to Internet
Data Security
59 Minutes Remaining
Instructions
Resources
Help
100%
Thursday, August 19
11. By default, the Administrator account is selected. Click admin@123 and press Enter to login.
The network screen appears, click Yes.
12. Click Start icon on the Desktop and click Server Manager.
Previous
Next: Exercise 7: Perform...
Search
63°F
Sunny
ENG
10:46 am
24/09/2024

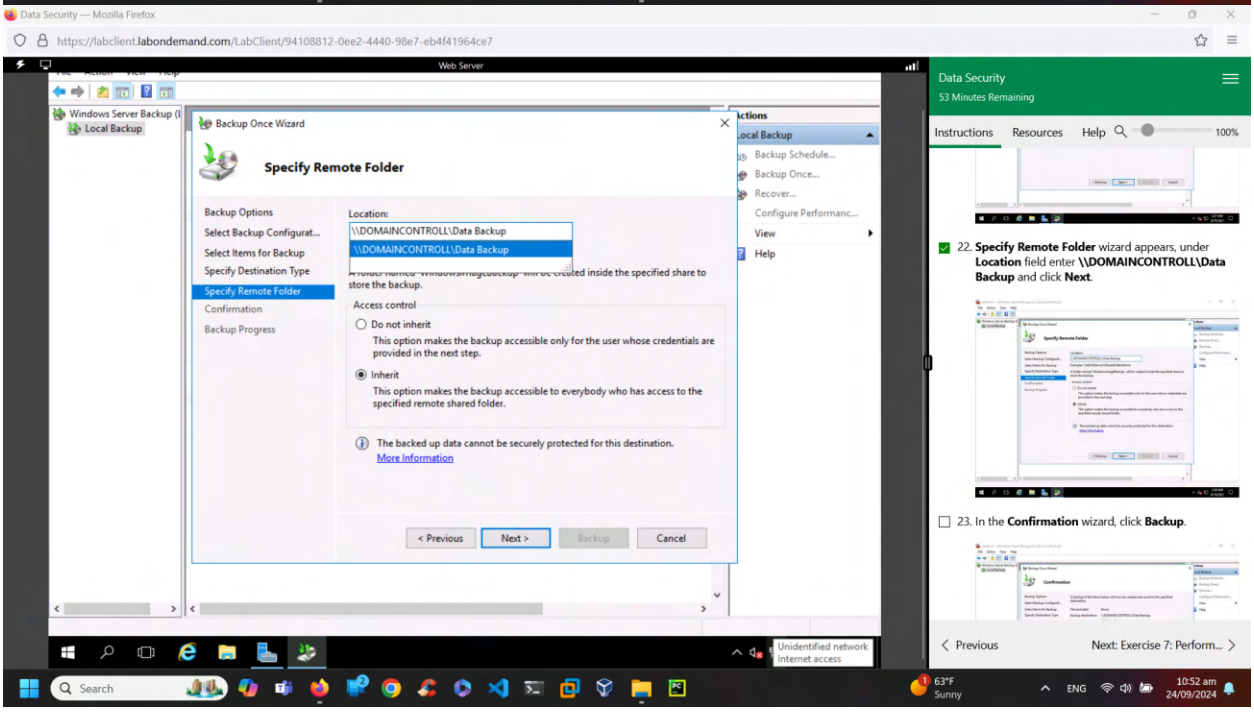

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Windows Server Backup (Local)
Backup your important data to a local or online location
Local Backup
Last Backup Status:
Next Backup Time:
Number of available backups:
Online Backup
You can subscribe to Microsoft Azure Backup to backup your critical data automatically.
Actions
Windows Server Backup (L...
View
Help
The Audio Service is not running.
Data Security
58 Minutes Remaining
Instructions
Resources
Help
100%
13. In the Server Manager window, click Tools and select Windows Server Backup.
Previous
Next: Exercise 7: Perform...
Search
63°F
Sunny
ENG
10:47 am
24/09/2024

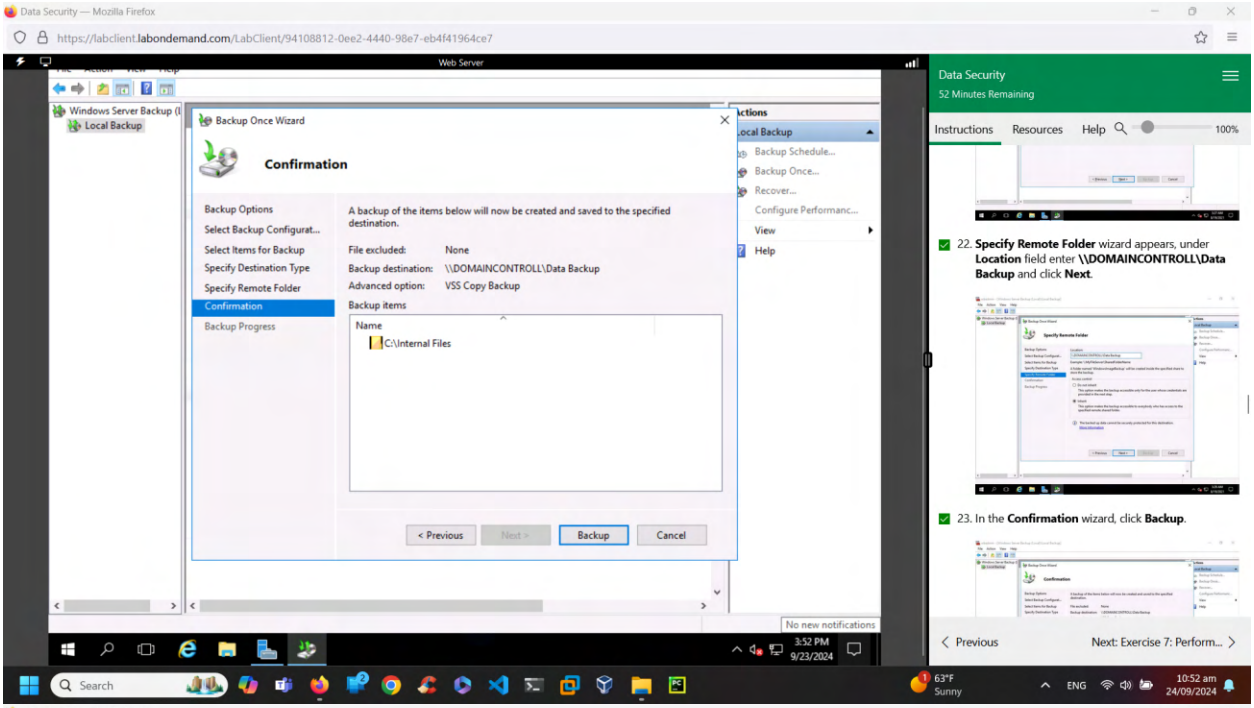

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Backup Options
Backup Options
Select Backup Configurat...
Specify Destination Type
Confirmation
Backup Progress
Create a backup now using:
Scheduled backup options
Choose this option if you have created a scheduled backup and want to use the same settings for this backup.
Different options
Choose this option if you have not created a scheduled backup or to specify a location or items for this backup that are different from the scheduled backup.
To continue, click Next.
< Previous
Next >
Backup
Cancel
Backup Schedule...
Backup Once...
Recover...
Configure Performanc...
View
Help
Monday, September 23, 2024
3:47 PM
9/23/2024
Data Security
58 Minutes Remaining
Instructions
Resources
Help
100%
15. In the right-pane under Actions section, click Backup Once... option.
16. Backup Once Wizard window appears, click Next.
Previous
Next: Exercise 7: Perform...
Search
63°F
Sunny
ENG
10:47 am
24/09/2024

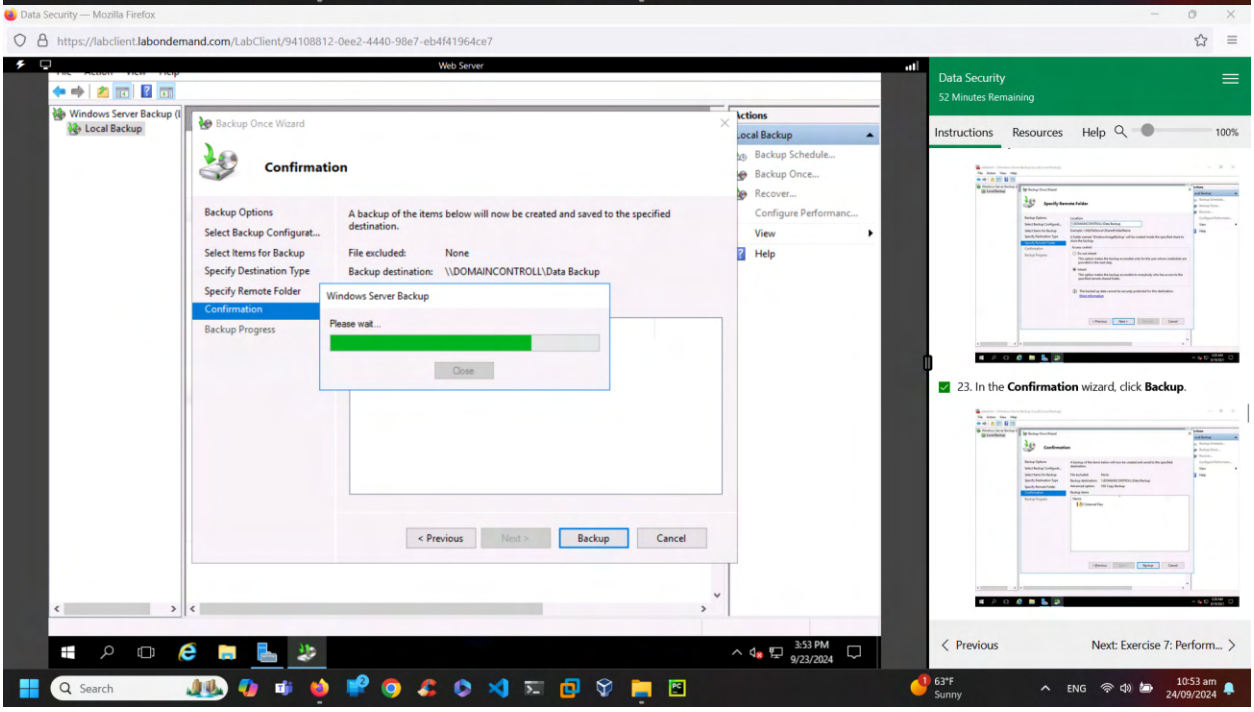

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Select Backup Configuration
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Confirmation
Backup Progress
What type of configuration do you want to schedule?
Full server (recommended)
I want to back up all my server data, applications and system state.
Backup size: 45.35 GB
Custom
I want to choose custom volumes, files for backup.
< Previous
Next >
Backup
Cancel
Windows Server Backup (L
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performanc...
View
Help
3:48 PM
The Audio Service is not running.
Search
63°F
Sunny
ENG
10:48 am
24/09/2024
Data Security
57 Minutes Remaining
Instructions
Resources
Help
100%
17. In Select Backup Configuration wizard, select Custom radio-button and click Next.
18. In Select Items for Backup wizard, click Add Items button.
Previous
Next: Exercise 7: Perform...

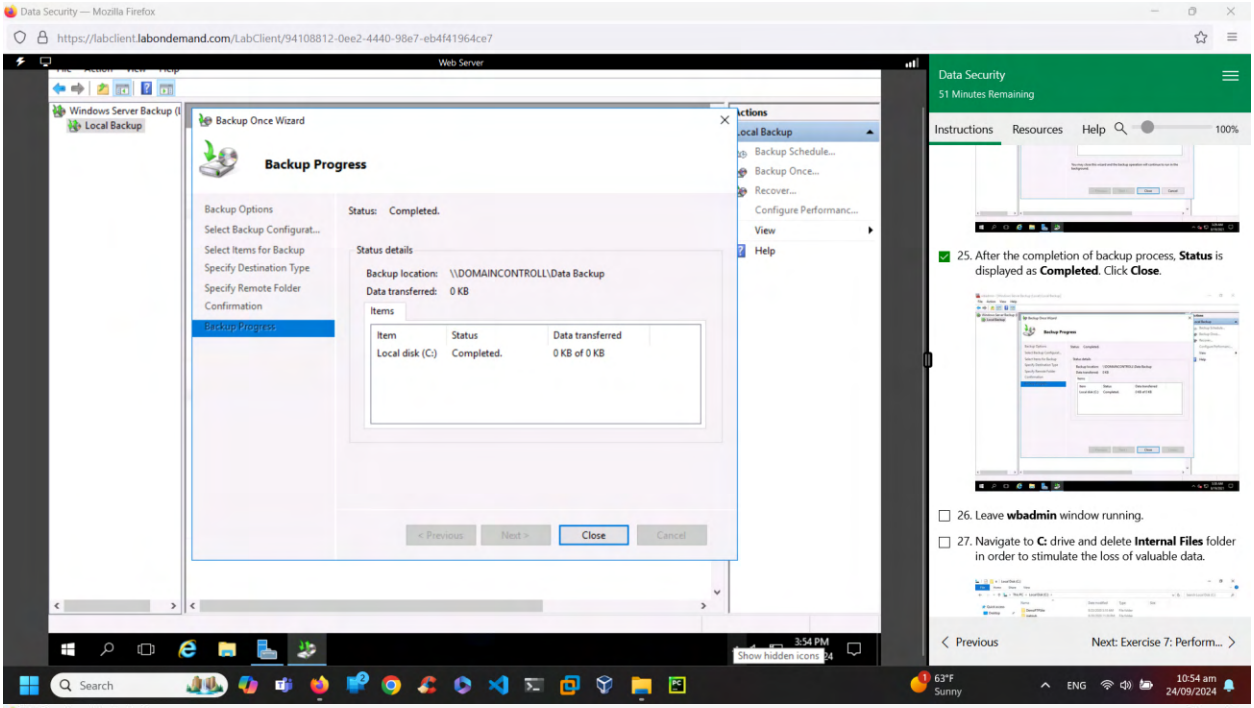

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Select Items for Backup
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Confirmation
Backup Progress
Select the items that you want to back up. Selecting bare metal recovery will provide you with the most options if you need to perform a recovery.
Name
C:\Internal Files
Add Items
Remove Items
Advanced Settings
< Previous
Next >
Backup
Cancel
Windows Server Backup (L
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performanc...
View
Help
3:51 PM
9/23/2024
Search
63°F
Sunny
ENG
10:51 am
24/09/2024
Data Security
54 Minutes Remaining
Instructions
Resources
Help
100%
20. You can observe that the selected folder (Internal Files) appears in the selected items field, click Next.
21. In Specify Destination Type wizard, select Remote shared folder radio-button and click Next.
Previous
Next: Exercise 7: Perform...

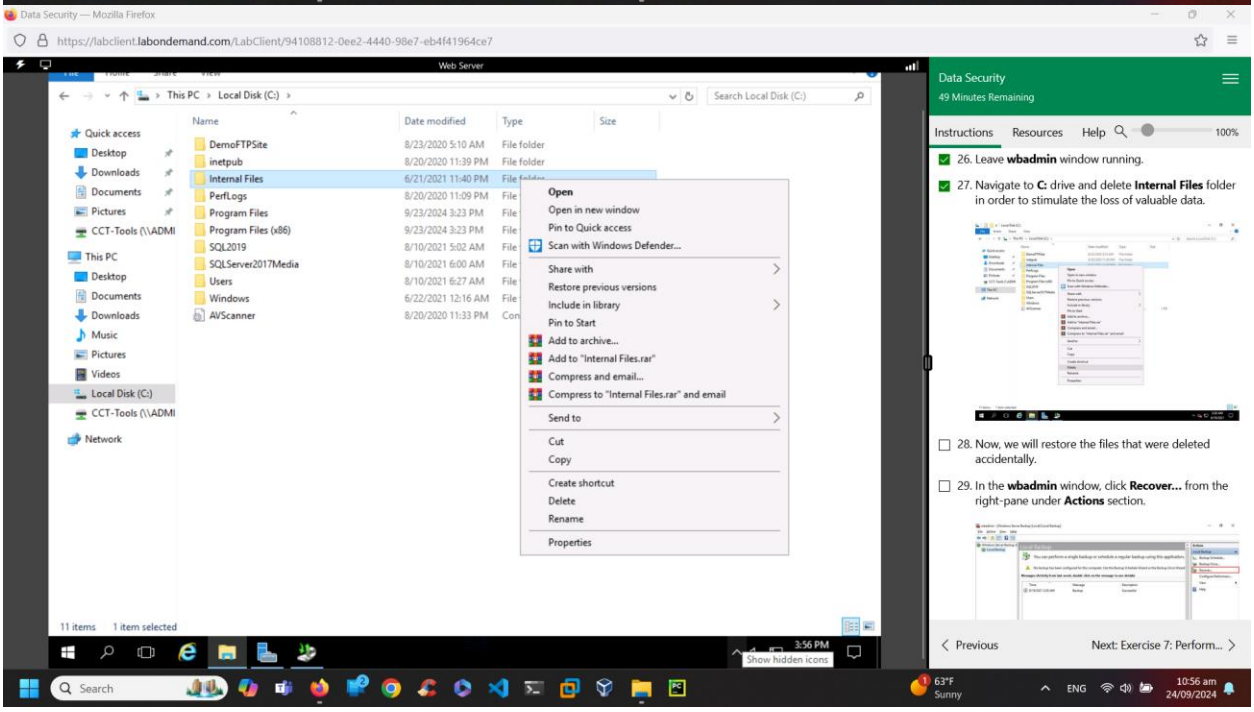

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Specify Destination Type
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Specify Remote Folder
Confirmation
Backup Progress
Choose the type of storage for the backup:
Local drives
Example: local disk (D:), DVD drive (E:)
Remote shared folder
Example: \\MyFileServer\SharedFolderName
< Previous
Next >
Backup
Cancel
Data Security
54 Minutes Remaining
Instructions
Resources
Help
100%
20. You can observe that the selected folder (Internal Files) appears in the selected items field, click Next.
21. In Specify Destination Type wizard, select Remote shared folder radio-button and click Next.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Specify Remote Folder
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Specify Remote Folder
Confirmation
Backup Progress
Location:
\\DOMAINCONTROLL\Data Backup
\\DOMAINCONTROLL\Data Backup
store the backup.
Access control
Do not inherit
This option makes the backup accessible only for the user whose credentials are provided in the next step.
Inherit
This option makes the backup accessible to everybody who has access to the specified remote shared folder.
The backed up data cannot be securely protected for this destination.
More Information
< Previous
Next >
Backup
Cancel
Data Security
53 Minutes Remaining
Instructions
Resources
Help
100%
22. Specify Remote Folder wizard appears, under Location field enter \\DOMAINCONTROLL\Data Backup and click Next.
23. In the Confirmation wizard, click Backup.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Confirmation
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Specify Remote Folder
Confirmation
Backup Progress
A backup of the items below will now be created and saved to the specified destination.
File excluded: None
Backup destination: \\DOMAINCONTROLL\Data Backup
Advanced option: VSS Copy Backup
Backup items
Name
C:\Internal Files
< Previous
Next >
Backup
Cancel
Data Security
52 Minutes Remaining
Instructions
Resources
Help
100%
22. Specify Remote Folder wizard appears, under Location field enter \\DOMAINCONTROLL\Data Backup and click Next.
23. In the Confirmation wizard, click Backup.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Confirmation
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Specify Remote Folder
Confirmation
Backup Progress
A backup of the items below will now be created and saved to the specified destination.
File excluded: None
Backup destination: \\DOMAINCONTROLL\Data Backup
Windows Server Backup
Please wait...
Close
< Previous
Next >
Backup
Cancel
Data Security
52 Minutes Remaining
Instructions
Resources
Help
100%
23. In the Confirmation wizard, click Backup.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Backup Once Wizard
Backup Progress
Backup Options
Select Backup Configurat...
Select Items for Backup
Specify Destination Type
Specify Remote Folder
Confirmation
Backup Progress
Status: Completed.
Status details
Backup location: \\DOMAINCONTROLL\Data Backup
Data transferred: 0 KB
Items
Item
Status
Data transferred
Local disk (C:)
Completed.
0 KB of 0 KB
< Previous
Next >
Close
Cancel
Backup Schedule...
Backup Once...
Recover...
Configure Performanc...
View
Help
Show hidden icons
3:54 PM
Search
63°F
Sunny
ENG
10:54 am
24/09/2024
Data Security
51 Minutes Remaining
Instructions
Resources
Help
100%
25. After the completion of backup process, Status is displayed as Completed. Click Close.
26. Leave wbadmin window running.
27. Navigate to C: drive and delete Internal Files folder in order to stimulate the loss of valuable data.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
This PC > Local Disk (C:) >
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
CCT-Tools (\\ADMI
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CCT-Tools (\\ADMI
Network
Name
Date modified
Type
Size
DemoFTPSite
8/23/2020 5:10 AM
File folder
inetpub
8/20/2020 11:39 PM
File folder
Internal Files
6/21/2021 11:40 PM
PerfLogs
8/20/2020 11:09 PM
Program Files
9/23/2024 3:23 PM
Program Files (x86)
9/23/2024 3:23 PM
SQL2019
8/10/2021 5:02 AM
SQLServer2017Media
8/10/2021 6:00 AM
Users
8/10/2021 6:27 AM
Windows
6/22/2021 12:16 AM
AVScanner
8/20/2020 11:33 PM
Open
Open in new window
Pin to Quick access
Scan with Windows Defender...
Share with
Restore previous versions
Include in library
Pin to Start
Add to archive...
Add to "Internal Files.rar"
Compress and email...
Compress to "Internal Files.rar" and email
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
11 items
1 item selected
Show hidden icons
3:56 PM
Search
63°F
Sunny
ENG
10:56 am
24/09/2024
Data Security
49 Minutes Remaining
Instructions
Resources
Help
100%
26. Leave wbadmin window running.
27. Navigate to C: drive and delete Internal Files folder in order to stimulate the loss of valuable data.
28. Now, we will restore the files that were deleted accidentally.
29. In the wbadmin window, click Recover... from the right-pane under Actions section.
Previous
Next: Exercise 7: Perform...

Data Security — Mozilla Firefox

https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7

Web Server

Windows Server Backup (I

Local Backup

Local Backup

You can perform a single backup or schedule a regular backup using this application.

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard

Messages (Activity from last week, double click on the message to see details)

Time	Message	Description
9/23/2024 3:53 PM	Backup	Successful

Status

Last Backup

Status: Successful

Time: 9/23/2024 3:53 PM

View details

Next Backup

Status: Not scheduled

Time: -

View details

Actions

Local Backup

Backup Schedule...

Backup Once...

Recover...

Configure Performanc...

View

Help

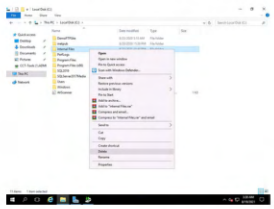
3:57 PM
9/23/2024

Data Security

48 Minutes Remaining

Instructions Resources Help 100%

- [x] 26. Leave **wbadmin** window running.
- [x] 27. Navigate to **C:** drive and delete **Internal Files** folder in order to stimulate the loss of valuable data.



- [x] 28. Now, we will restore the files that were deleted accidentally.
- [ ] 29. In the **wbadmin** window, click **Recover...** from the right-pane under **Actions** section.

Previous Next: Exercise 7: Perform...

Data Security — Mozilla Firefox

https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7

Web Server

Windows Server Backu

Local Backup

Recovery Wizard

Getting Started

Getting Started
Specify Location Type
Select Backup Location
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress

You can use this wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.

Where is the backup stored that you want to use for the recovery?

- This server (WEBSERVER)
- A backup stored on another location

To continue, click Next.

< Previous Next > Recover Cancel

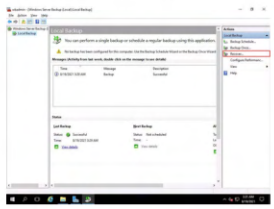
3:58 PM
9/23/2024

Data Security

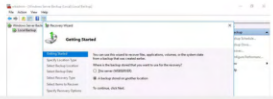
47 Minutes Remaining

Instructions Resources Help 100%

- [x] 28. Now, we will restore the files that were deleted accidentally.
- [x] 29. In the **wbadmin** window, click **Recover...** from the right-pane under **Actions** section.



- [ ] 30. **Getting Started** wizard appears, select **A backup stored on another location** radio-button and click **Next**.



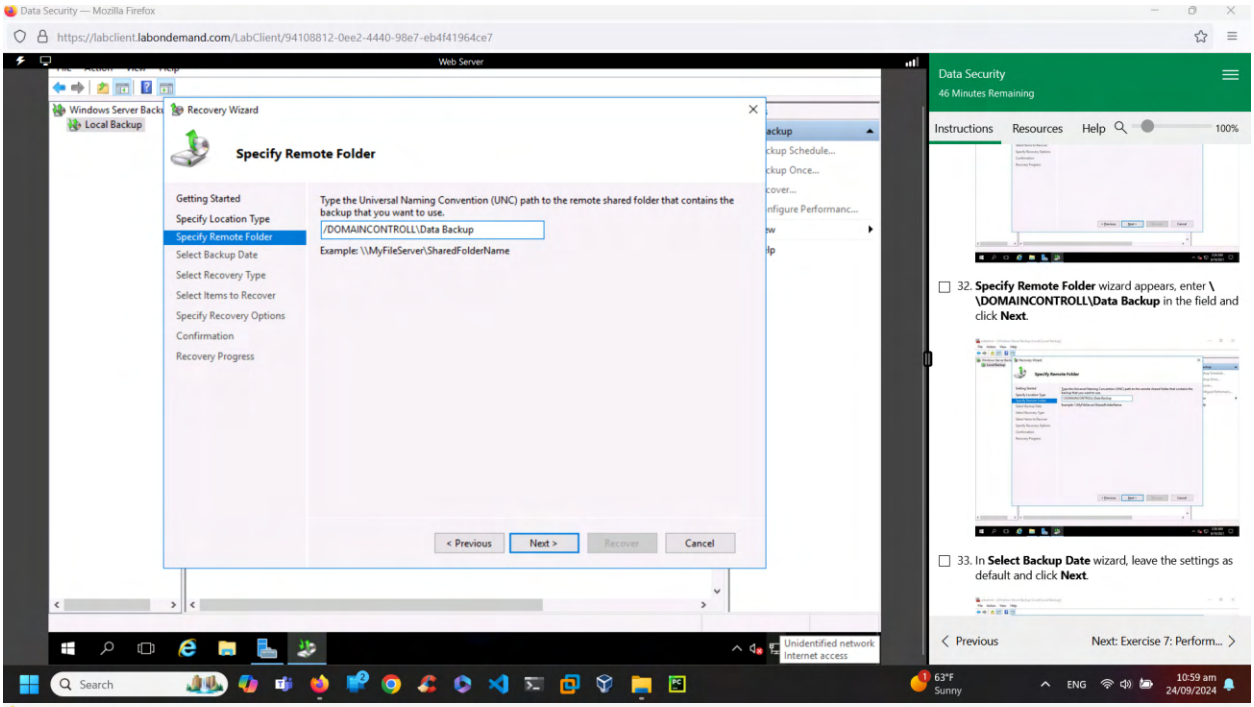
Previous Next: Exercise 7: Perform...

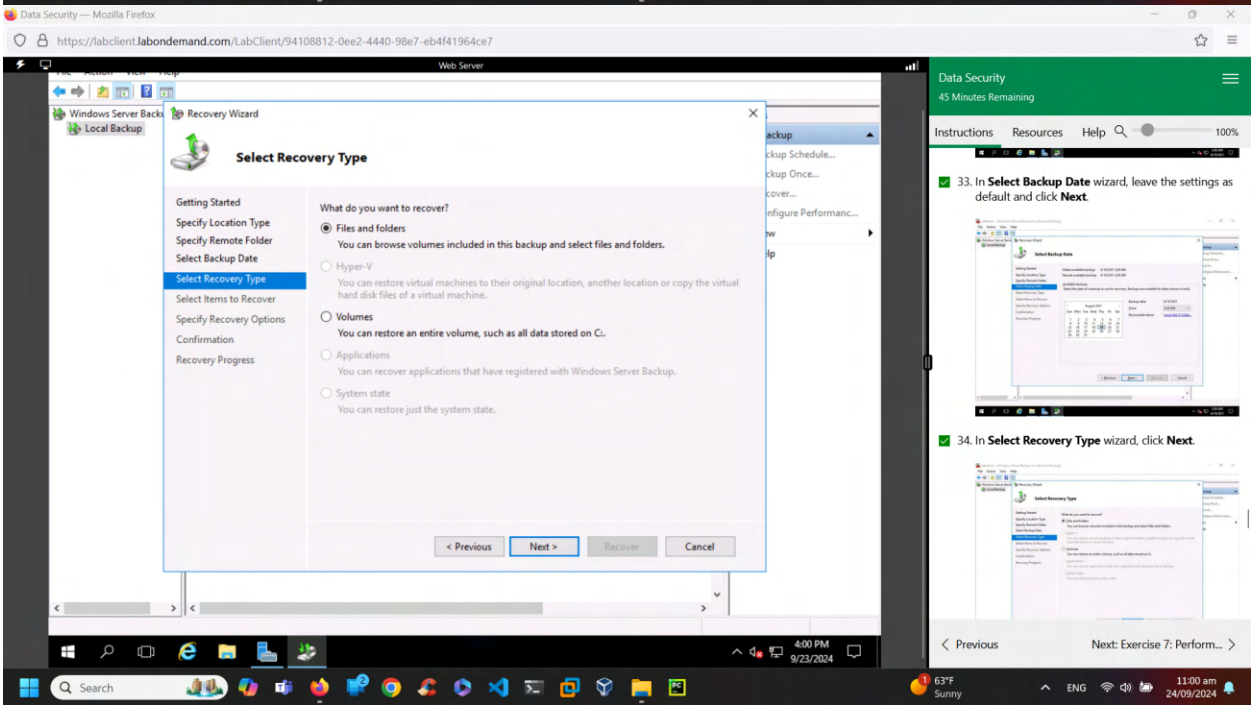
Search

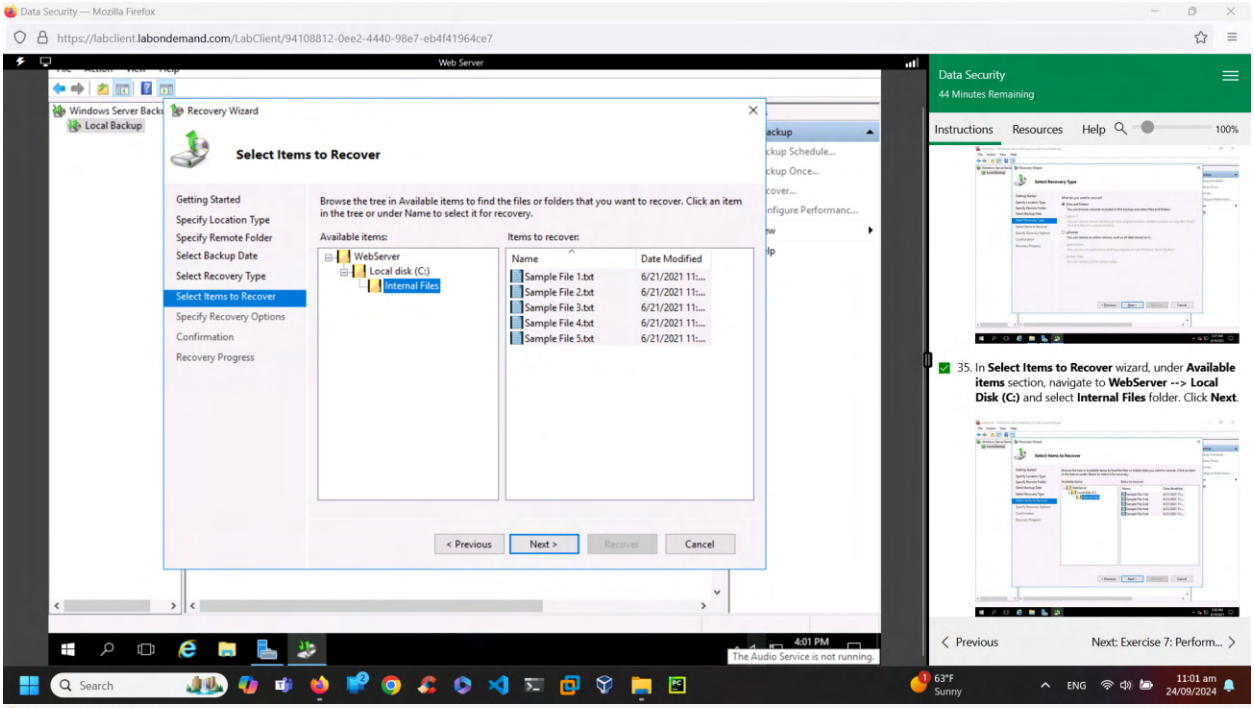
63°F Sunny

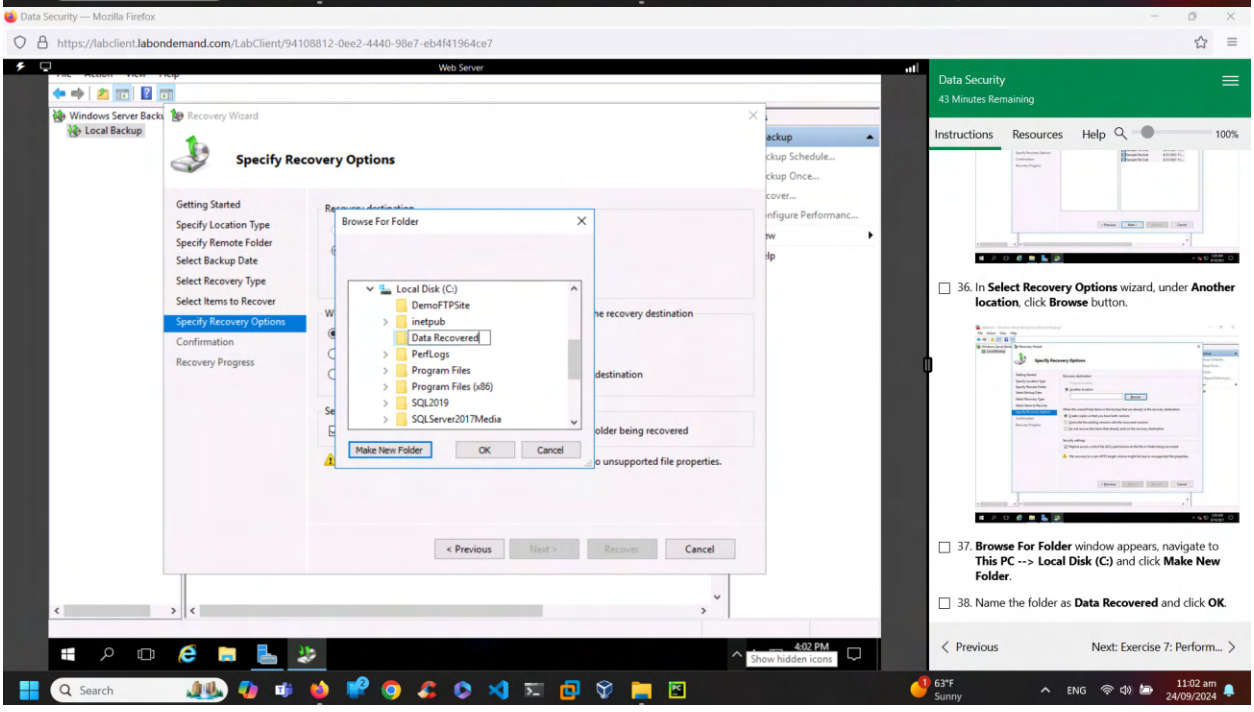
ENG

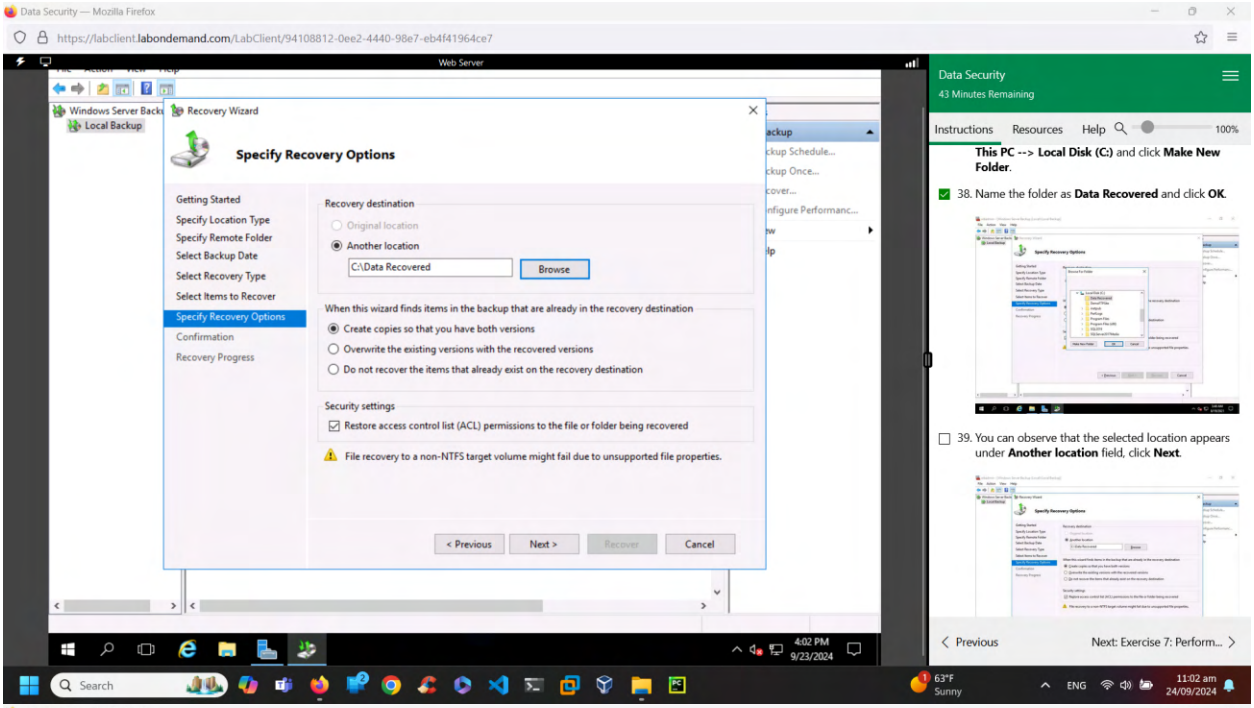
10:58 am
24/09/2024

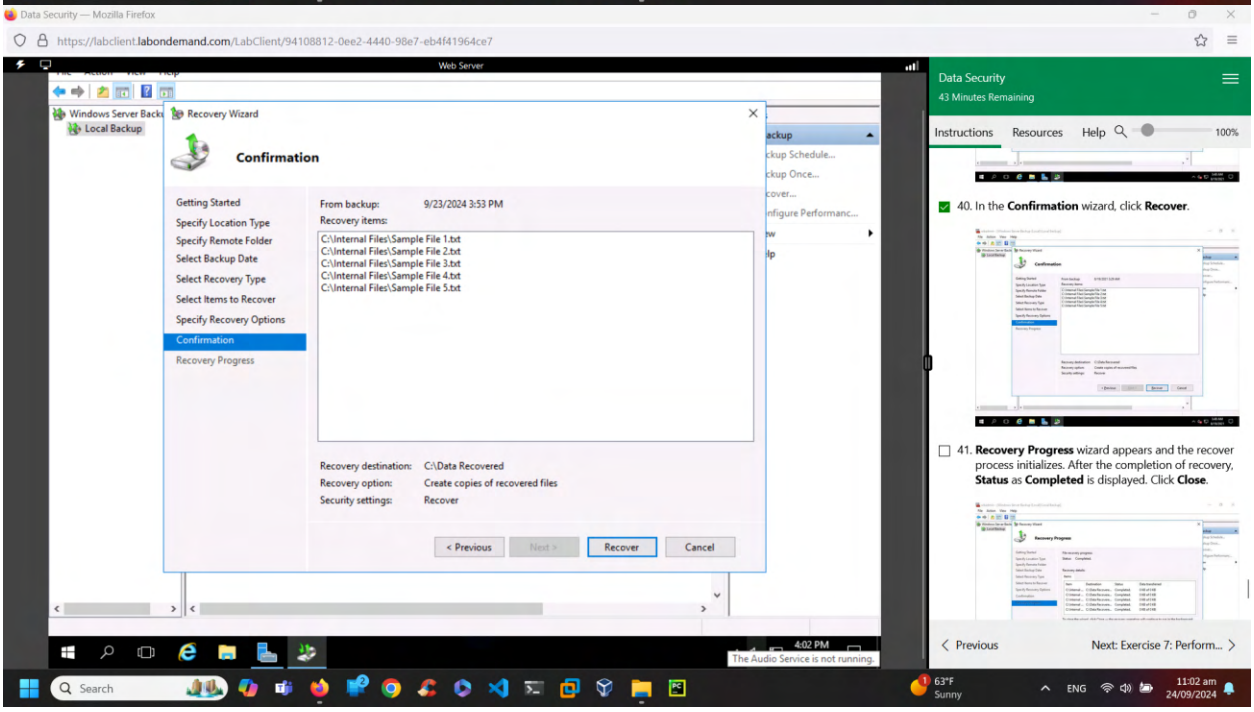

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Recovery Wizard
Specify Remote Folder
Getting Started
Specify Location Type
Specify Remote Folder
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
Type the Universal Naming Convention (UNC) path to the remote shared folder that contains the backup that you want to use.
/DOMAINCONTROLL\Data Backup
Example: \\MyFileServer\SharedFolderName
< Previous
Next >
Recover
Cancel
Data Security
46 Minutes Remaining
Instructions
Resources
Help
100%
32. Specify Remote Folder wizard appears, enter \ \DOMAINCONTROLL\Data Backup in the field and click Next.
33. In Select Backup Date wizard, leave the settings as default and click Next.
Previous
Next: Exercise 7: Perform...
Search
63°F
Sunny
ENG
10:59 am
24/09/2024

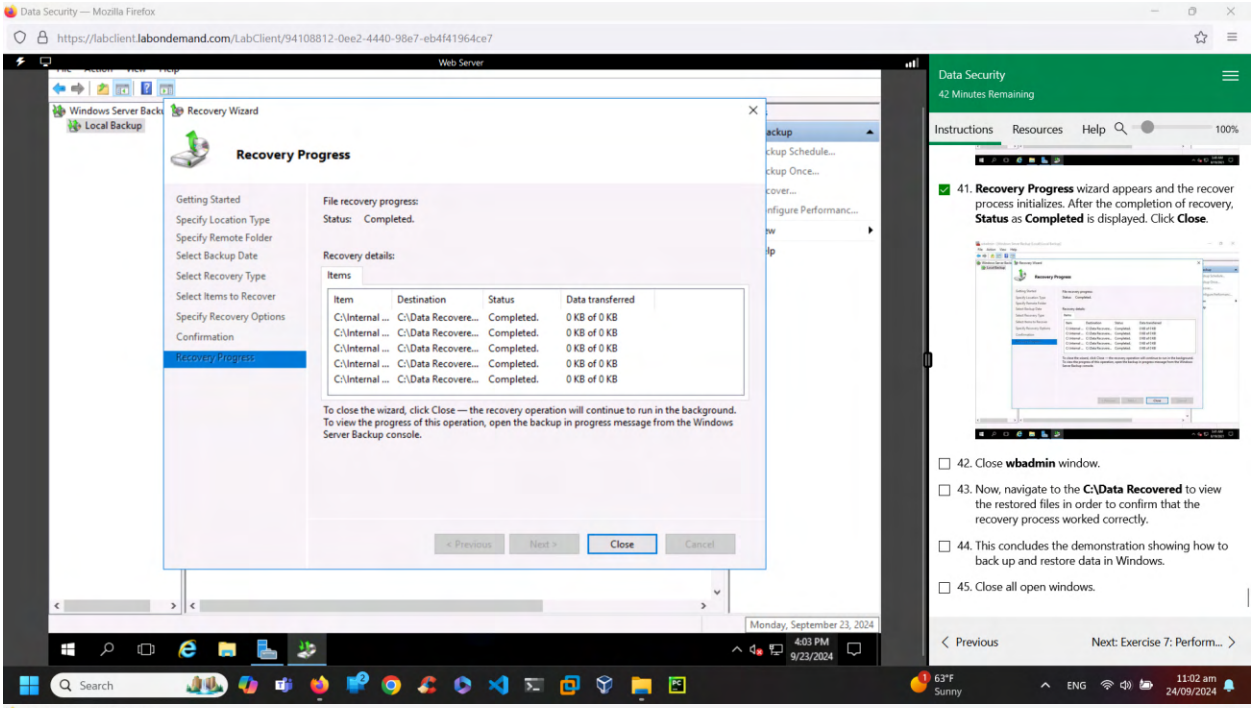

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Recovery Wizard
Select Recovery Type
Getting Started
Specify Location Type
Specify Remote Folder
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
What do you want to recover?
Files and folders
You can browse volumes included in this backup and select files and folders.
Hyper-V
You can restore virtual machines to their original location, another location or copy the virtual hard disk files of a virtual machine.
Volumes
You can restore an entire volume, such as all data stored on C:.
Applications
You can recover applications that have registered with Windows Server Backup.
System state
You can restore just the system state.
< Previous
Next >
Recover
Cancel
Data Security
45 Minutes Remaining
Instructions
Resources
Help
100%
33. In Select Backup Date wizard, leave the settings as default and click Next.
34. In Select Recovery Type wizard, click Next.
Previous
Next: Exercise 7: Perform...
Search
63°F
Sunny
ENG
11:00 am
24/09/2024

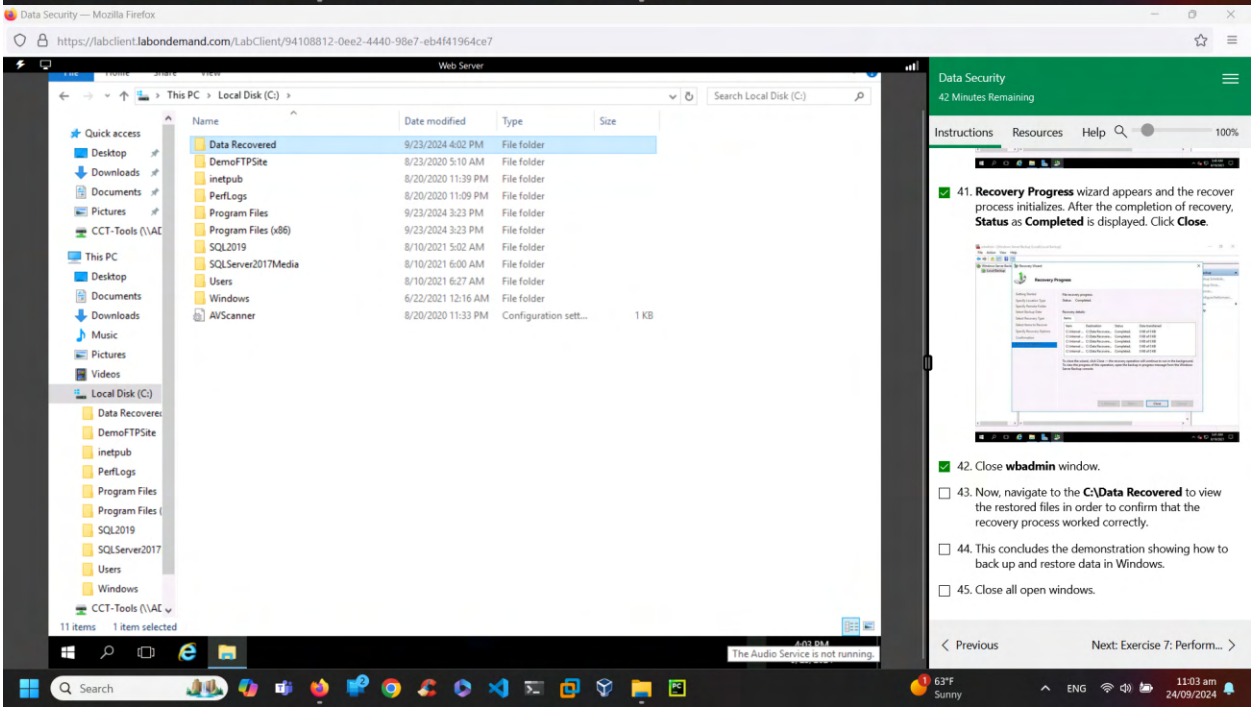

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Recovery Wizard
Select Items to Recover
Getting Started
Specify Location Type
Specify Remote Folder
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
Browse the tree in Available items to find the files or folders that you want to recover. Click an item in the tree or under Name to select it for recovery.
Available items:
Items to recover:
WebServer
Local disk (C:)
Internal Files
Name
Date Modified
Sample File 1.txt 6/21/2021 11:...
Sample File 2.txt 6/21/2021 11:...
Sample File 3.txt 6/21/2021 11:...
Sample File 4.txt 6/21/2021 11:...
Sample File 5.txt 6/21/2021 11:...
< Previous
Next >
Recover
Cancel
The Audio Service is not running.
Data Security
44 Minutes Remaining
Instructions
Resources
Help
100%
35. In Select Items to Recover wizard, under Available items section, navigate to WebServer --> Local Disk (C:) and select Internal Files folder. Click Next.
Previous
Next: Exercise 7: Perform...

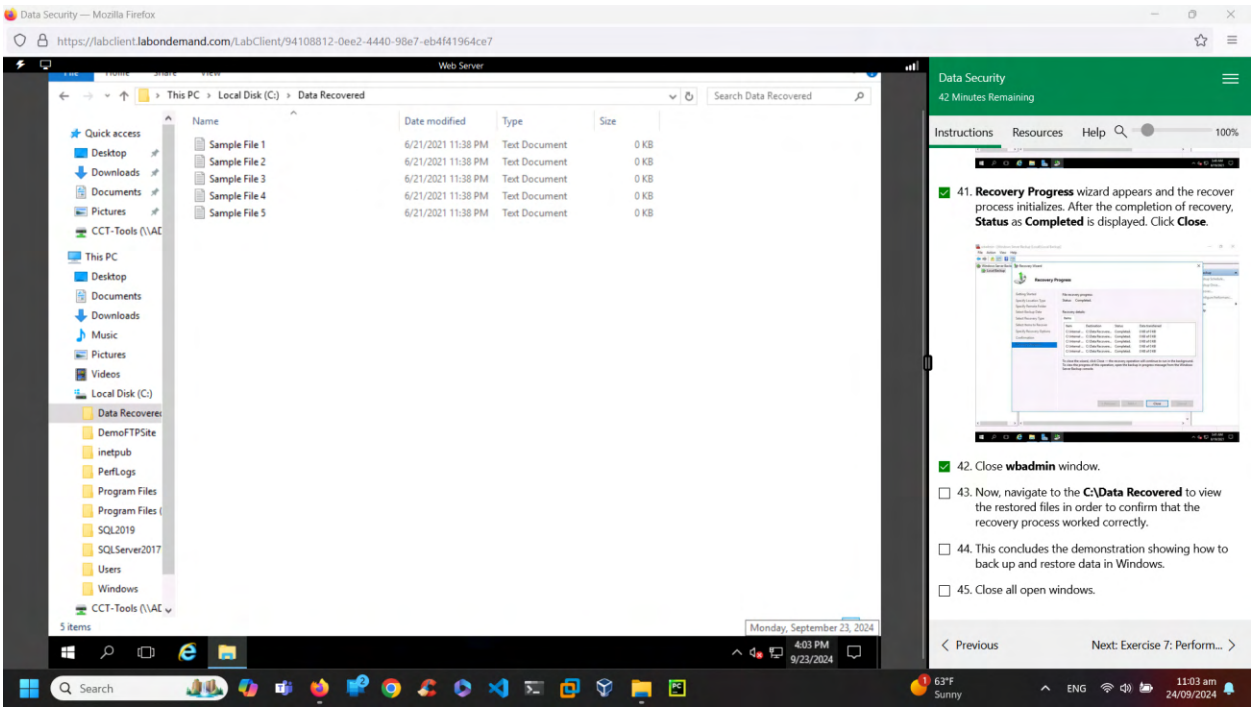

Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Recovery Wizard
Specify Recovery Options
Getting Started
Specify Location Type
Specify Remote Folder
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
Browse For Folder
Local Disk (C:)
DemoFTPSite
inetpub
Data Recovered
PerfLogs
Program Files
Program Files (x86)
SQL2019
SQLServer2017Media
Make New Folder
OK
Cancel
< Previous
Next >
Recover
Cancel
Show hidden icons
Data Security
43 Minutes Remaining
Instructions
Resources
Help
100%
36. In Select Recovery Options wizard, under Another location, click Browse button.
37. Browse For Folder window appears, navigate to This PC --> Local Disk (C:) and click Make New Folder.
38. Name the folder as Data Recovered and click OK.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Recovery Wizard
Specify Recovery Options
Getting Started
Specify Location Type
Specify Remote Folder
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
Recovery destination
Original location
Another location
C:\Data Recovered
Browse
When this wizard finds items in the backup that are already in the recovery destination
Create copies so that you have both versions
Overwrite the existing versions with the recovered versions
Do not recover the items that already exist on the recovery destination
Security settings
Restore access control list (ACL) permissions to the file or folder being recovered
File recovery to a non-NTFS target volume might fail due to unsupported file properties.
< Previous
Next >
Recover
Cancel
Data Security
43 Minutes Remaining
Instructions
Resources
Help
100%
This PC --> Local Disk (C:) and click Make New Folder.
38. Name the folder as Data Recovered and click OK.
39. You can observe that the selected location appears under Another location field, click Next.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Recovery Wizard
Confirmation
Getting Started
Specify Location Type
Specify Remote Folder
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
From backup: 9/23/2024 3:53 PM
Recovery items:
C:\Internal Files\Sample File 1.txt
C:\Internal Files\Sample File 2.txt
C:\Internal Files\Sample File 3.txt
C:\Internal Files\Sample File 4.txt
C:\Internal Files\Sample File 5.txt
Recovery destination: C:\Data Recovered
Recovery option: Create copies of recovered files
Security settings: Recover
< Previous
Next >
Recover
Cancel
The Audio Service is not running.
Data Security
43 Minutes Remaining
Instructions
Resources
Help
100%
40. In the Confirmation wizard, click Recover.
41. Recovery Progress wizard appears and the recover process initializes. After the completion of recovery, Status as Completed is displayed. Click Close.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
Recovery Wizard
Recovery Progress
Getting Started
Specify Location Type
Specify Remote Folder
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
File recovery progress:
Status: Completed.
Recovery details:
Items
Item
Destination
Status
Data transferred
C:\Internal ...
C:\Data Recovere...
Completed.
0 KB of 0 KB
To close the wizard, click Close — the recovery operation will continue to run in the background. To view the progress of this operation, open the backup in progress message from the Windows Server Backup console.
< Previous
Next >
Close
Cancel
Monday, September 23, 2024
4:03 PM
9/23/2024
Search
63°F
Sunny
ENG
11:02 am
24/09/2024
Data Security
42 Minutes Remaining
Instructions
Resources
Help
100%
41. Recovery Progress wizard appears and the recover process initializes. After the completion of recovery, Status as Completed is displayed. Click Close.
42. Close wbadmin window.
43. Now, navigate to the C:\Data Recovered to view the restored files in order to confirm that the recovery process worked correctly.
44. This concludes the demonstration showing how to back up and restore data in Windows.
45. Close all open windows.
Previous
Next: Exercise 7: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Web Server
This PC > Local Disk (C:) >
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Music
Videos
Local Disk (C:)
Name
Date modified
Type
Size
Data Recovered
DemoFTPSite
inetpub
PerfLogs
Program Files
Program Files (x86)
SQL2019
SQLServer2017Media
Users
Windows
AVScanner
9/23/2024 4:02 PM
8/23/2020 5:10 AM
8/20/2020 11:39 PM
8/20/2020 11:09 PM
9/23/2024 3:23 PM
9/23/2024 3:23 PM
8/10/2021 5:02 AM
8/10/2021 6:00 AM
8/10/2021 6:27 AM
6/22/2021 12:16 AM
8/20/2020 11:33 PM
File folder
Configuration sett...
1 KB
11 items
1 item selected
The Audio Service is not running.
Search
63°F
Sunny
ENG
11:03 am
24/09/2024
Data Security
42 Minutes Remaining
Instructions
Resources
Help
100%
41. Recovery Progress wizard appears and the recover process initializes. After the completion of recovery, Status as Completed is displayed. Click Close.
42. Close wbadmin window.
43. Now, navigate to the C:\Data Recovered to view the restored files in order to confirm that the recovery process worked correctly.
44. This concludes the demonstration showing how to back up and restore data in Windows.
45. Close all open windows.
Previous
Next: Exercise 7: Perform...



Reports:

Implementing backup and restore strategies in Server Manager as a Cyber Technician ensures quick recovery during any cyber incidents or hardware failure. In case of disaster, if the downtime is less, it helps to continue the business after some time.

10. **Ilab Module no. and name:** 15. Data Security

    Exercise no. and name: 3 Implement Built-in File System-level Encryption on Windows

    Performed Date: 24/09/2024

Summary:

This lab demonstrates how file encryption EFS is done using advanced attributes in the properties of the file. It also demonstrates how the file can be encrypted, ciphered in command prompt and ciphered.exe overwrites with Zeroes and random numbers in the screesnhots shown below.

Screenshots:

Data Security — Mozilla Firefox

https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7

Admin Machine-1

User Account Control

Do you want to allow this app to make changes to your device?

Windows Command Processor

Verified publisher: Microsoft Windows

Show more details

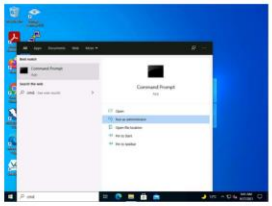
Yes No

Data Security

1 Hr 25 Min Remaining

Instructions Resources Help 100%

from the right-pane, select **Run as administrator** option.



7. **User Account Control** window appears, click **Yes** to proceed.
8. Switch to the **Command Prompt** window. In the **Command Prompt**, type **cipher /e "C:\Users\Admin\Desktop\Test.txt"** and press **Enter**.

/e: Specifies encryption of a file or a directory.

Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its

Previous Next: Exercise 4: Perform...

Search

61°F Sunny ENG 10:20 am 24/09/2024

Data Security — Mozilla Firefox

https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7

Admin Machine-1

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher /e "C:\Users\Admin\Desktop\Test.txt"
```

Microsoft Edge

VeraCrypt

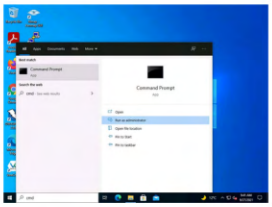
Monday, September 23, 2024

Data Security

1 Hr 23 Min Remaining

Instructions Resources Help 100%

from the right-pane, select **Run as administrator** option.



7. **User Account Control** window appears, click **Yes** to proceed.
8. Switch to the **Command Prompt** window. In the **Command Prompt**, type **cipher /e "C:\Users\Admin\Desktop\Test.txt"** and press **Enter**.

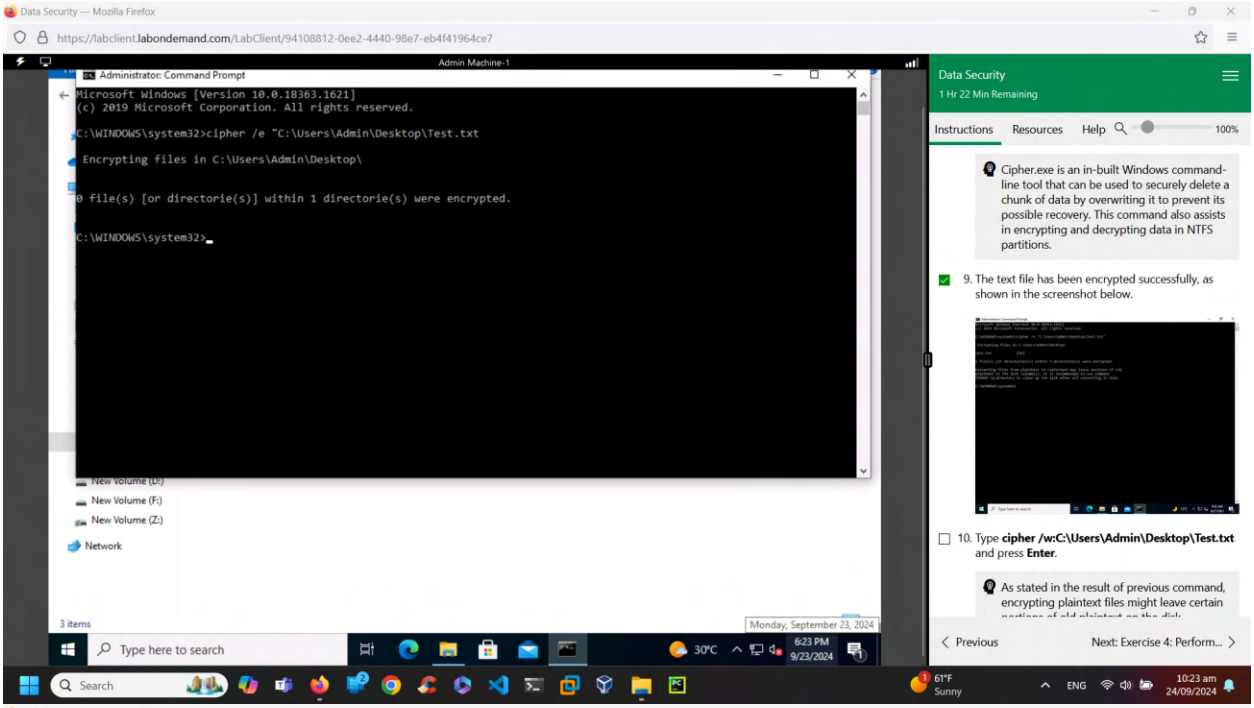
/e: Specifies encryption of a file or a directory.

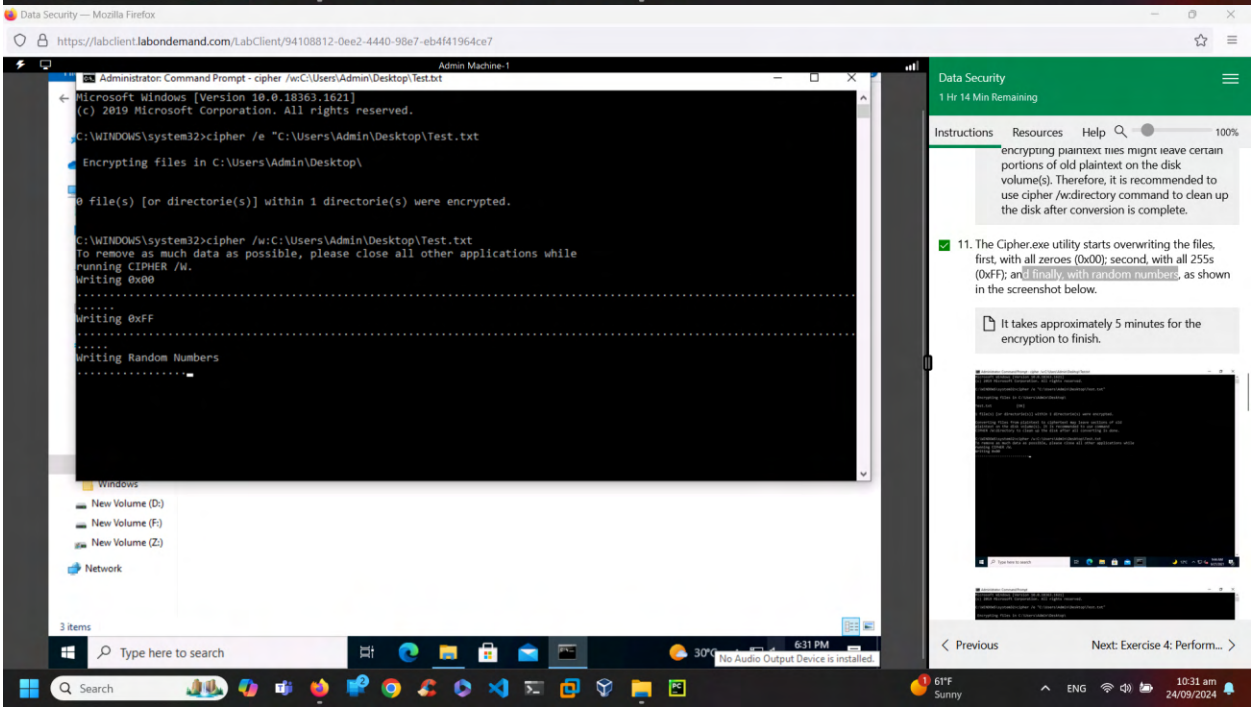
Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its

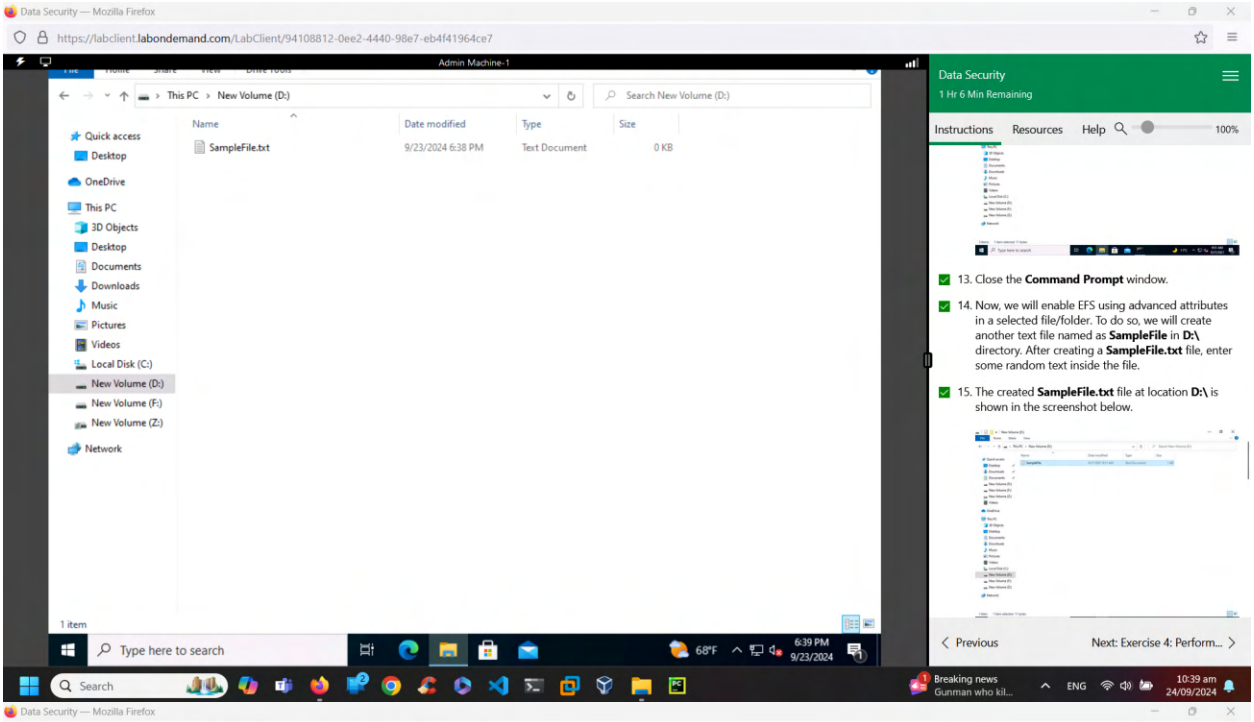
Previous Next: Exercise 4: Perform...

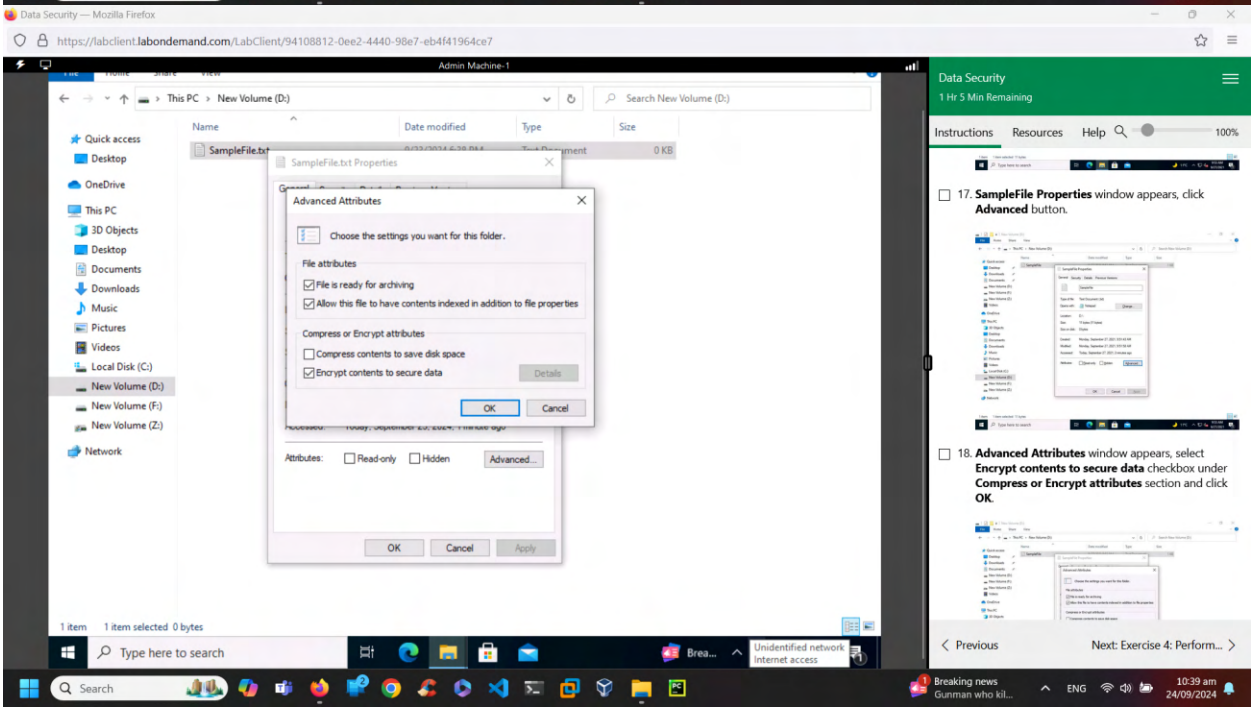
Search

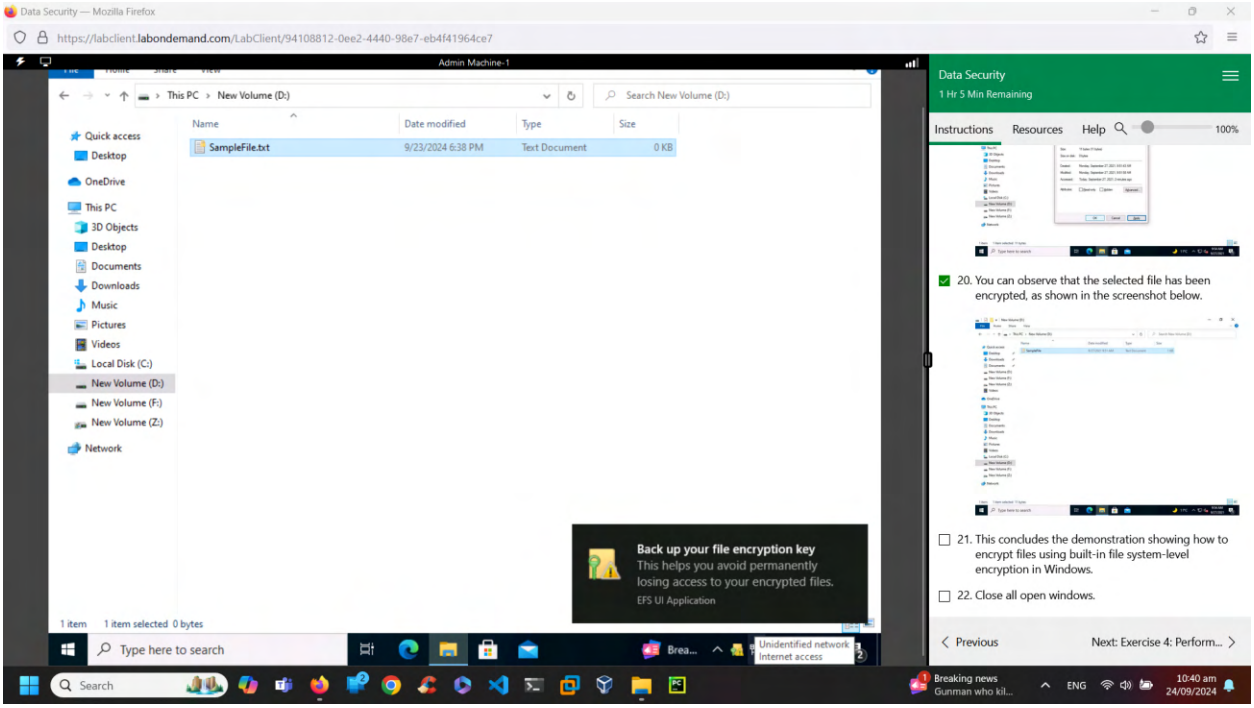
61°F Sunny ENG 10:22 am 24/09/2024


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Admin Machine-1
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>cipher /e "C:\Users\Admin\Desktop\Test.txt
Encrypting files in C:\Users\Admin\Desktop\
0 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.
C:\WINDOWS\system32>
New Volume (F:)
New Volume (Z:)
Network
3 items
Monday, September 23, 2024
Type here to search
6:23 PM
9/23/2024
Search
61°F
Sunny
ENG
10:23 am
24/09/2024
Data Security
1 Hr 22 Min Remaining
Instructions
Resources
Help
100%
Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.
9. The text file has been encrypted successfully, as shown in the screenshot below.
10. Type cipher /w:C:\Users\Admin\Desktop\Test.txt and press Enter.
As stated in the result of previous command, encrypting plaintext files might leave certain
Previous
Next: Exercise 4: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Admin Machine-1
Administrator: Command Prompt - cipher /w:C:\Users\Admin\Desktop\Test.txt
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>cipher /e "C:\Users\Admin\Desktop\Test.txt
Encrypting files in C:\Users\Admin\Desktop\
0 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.
C:\WINDOWS\system32>cipher /w:C:\Users\Admin\Desktop\Test.txt
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
Writing 0xFF
Writing Random Numbers
Windows
New Volume (D:)
New Volume (F:)
New Volume (Z:)
Network
3 items
Type here to search
6:31 PM
No Audio Output Device is installed.
Search
61°F
Sunny
ENG
10:31 am
24/09/2024
Data Security
1 Hr 14 Min Remaining
Instructions
Resources
Help
100%
encrypting plaintext files might leave certain portions of old plaintext on the disk volume(s). Therefore, it is recommended to use cipher /w:directory command to clean up the disk after conversion is complete.
11. The Cipher.exe utility starts overwriting the files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot below.
It takes approximately 5 minutes for the encryption to finish.
Previous
Next: Exercise 4: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Admin Machine-1
This PC › New Volume (D:)
Search New Volume (D:)
Name
Date modified
Type
Size
SampleFile.txt
9/23/2024 6:38 PM
Text Document
0 KB
Quick access
Desktop
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
New Volume (F:)
New Volume (Z:)
Network
1 item
Type here to search
68°F
6:39 PM
9/23/2024
Search
Breaking news
Gunman who kil...
ENG
10:39 am
24/09/2024
Data Security
1 Hr 6 Min Remaining
Instructions
Resources
Help
100%
13. Close the Command Prompt window.
14. Now, we will enable EFS using advanced attributes in a selected file/folder. To do so, we will create another text file named as SampleFile in D:\ directory. After creating a SampleFile.txt file, enter some random text inside the file.
15. The created SampleFile.txt file at location D:\ is shown in the screenshot below.
Previous
Next: Exercise 4: Perform...


Data Security — Mozilla Firefox
https://labclient.labondemand.com/LabClient/94108812-0ee2-4440-98e7-eb4f41964ce7
Admin Machine-1
This PC › New Volume (D:)
Search New Volume (D:)
Name
Date modified
Type
Size
SampleFile.txt
0 KB
SampleFile.txt Properties
Advanced Attributes
Choose the settings you want for this folder.
File attributes
File is ready for archiving
Allow this file to have contents indexed in addition to file properties
Compress or Encrypt attributes
Compress contents to save disk space
Encrypt contents to secure data
Details
OK
Cancel
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply
1 item
1 item selected 0 bytes
Type here to search
Unidentified network
Internet access
Search
Breaking news
Gunman who kil...
ENG
10:39 am
24/09/2024
Data Security
1 Hr 5 Min Remaining
Instructions
Resources
Help
100%
17. SampleFile Properties window appears, click Advanced button.
18. Advanced Attributes window appears, select Encrypt contents to secure data checkbox under Compress or Encrypt attributes section and click OK.
Previous
Next: Exercise 4: Perform...



Reports:

As a cyber technician, we are responsible for the data security, maintaining compliance like GDPR, HIPAA to avoid penalty and maintain organization's reputation. It can be done on the folders, sub-folders and files rather than full disk encryption.