Pentesting a Storage Network

Scott Moskal

College of Engineering and Polymer Science, University of Akron

CIS Senior Cybersecurity Project

Dr. John Nicholas

January 31, 2022

Project Description:

A small storage network will be designed with two wired routers, one wireless router, a switch, two laptops, a desktop, and a Raspberry Pi. Both laptops will be connected to the wireless router. The HP laptop will run Parrot OS and the Acer laptop will run Windows 11. The wireless router will be connected to the second router via port eth0. The eth2 port on the second router will be connected to eth1 port of the third router. The third router will be connected to the eth0 port of the Netgear switch. The switch will have two VLANs. VLAN 10 will be connected to the BeeLink desktop computer running Kali Linux. The desktop will also be used as an FTP server. VLAN 20 will be connected to the Raspberry Pi running OpenMediaVault. The Raspberry Pi will act as a NAS server. The three tools used for pentesting will be nmap, OpenVAS, and Wireshark. Nmap will be used to discover IP addresses and opened ports on the network. OpenVAS will be used to discover advanced vulnerabilities within the network. Wireshark will be used to capture unencrypted traffic traversing the network. The HP laptop will use Metasploit and bettercap. Metasploit will be used in an attempt to gain unauthorized access to the FTP server. Bettercap will be used in an attempt to execute a man-in-the-middle attack against the Acer Laptop. The BeeLink Desktop will use aircrack-ng. Aircrack-ng will be used in an attempt to crack the WPA encryption key on the wireless router.

Equipment

2x Ubiquiti EdgeRouter Lite-3

- Router 1: 18E829BF0532
- Router 2: 18E829B9F85C

1x Netgear Switch (GS108PE)

- Switch 3UJB0C5CA21A5

1x TP-Link 3000Mbps Wireless N Router (TP-WR841N)

- Router 2149622019187

1x HP Pavillion x360 Laptop with Parrot OS

1x Acer Laptop with Windows 11

1x BeeLink T4 Pro Micro PC with Kali Linux

1x Raspberry Pi 1GB with OpenMediaVault

Software

Windows 11

- FileZilla FTP Client

Kali Linux

- FileZilla FTP Server
- Aircrack-ng

Parrot OS

- Nmap
- OpenVAS/Greenbone
- Wireshark
- Metasploit
- bettercap

OpenMediaVault

Objectives

1) Research
    a. TP-Link Wireless N Router Web Portal
        i. What routing protocols can be configured?
        ii. Which routing protocols will be used?
        iii. What are the hardening techniques?
    b. Ubiquiti EdgeRouter WEB graphical user interface (GUI)
        i. What routing protocols can be configured?
        ii. Which routing protocols will be used?
        iii. What are the hardening techniques?
    c. Netgear Switch
        i. What security features can the switch use?
        ii. How are VLANs implemented?
        iii. How many VLANs can be used?
        iv. How is a trunk port created?
    d. FileZilla FTP Server and Client
        i. What is the software?
        ii. How can documents be shared via FTP be protected?
        iii. Does the software have any security features?
    e. OpenVAS/Greenbone
        i. What is the tool?
        ii. What vulnerabilities can be found on the network?

f. Nmap
    i. What is the tool?
    ii. What vulnerabilities can be found on the network?
    iii. What commands will be used?
g. Wireshark
    i. What is the tool?
    ii. What information can be found within the packets shared across the network?
    iii. What security vulnerabilities can be determined from the information within the packets?
h. bettercap
    i. What is the tool?
    ii. What attacks is the tool capable of performing?
    iii. How many targets can the tool attack?
    iv. Can the tool be used in tandem with other tools?
i. Aircrack-ng
    i. What is the tool?
    ii. What information does the tool reveal about wireless devices?
    iii. What commands are used?
    iv. Can the tool detect remote routers?
j. Metasploit
    i. What is the tool?
    ii. What information can be revealed with the tool?

iii. Can the tool target an FTP server and how?

iv. What commands will be used?

2) Design

a. All devices and routes will use static IPs.

b. All unused ports on the switch will be disabled.

c. The administrative network will use a router-on-a-stick configuration with two VLANs.

d. Addressing scheme:

i. Wireless Network: 10.1.1.0/29

ii. Wireless Router to Wired Router A: 172.16.1.0/30

iii. Wired Router A to Wired Router B: 172.16.3.0/30

iv. VLAN 10: 192.168.10.0/29

v. VLAN 20: 192.168.20.0/29

vi. More information will be included in the table and topology design below.

3) Implementation

a. TP-Link 3000Mbps Wireless N Router

i. Configure the IP address according to the address table.

ii. Set the wireless LAN address to be static.

iii. Set the wired WAN address to be static.

iv. Enable WPA/WPA2.

v. Change the default username and password.

vi. Configure the firewall rules.

b. Configure EdgeRouter 1

i. Configure the IP address according to the address table.
ii. Set the IP address on eth1 to be static.
iii. Set the IP address on eth2 to be static.
iv. Change the default username and password.
v. Configure and enable the firewall rules.

c. Configure EdgeRouter 2
    i. Configure the IP address according to the address table.
    ii. Enable trunking and port forwarding on port eth0.
    iii. Change the default username and password.
    iv. Set up router-on-a-stick for port eth0.
    v. Connect eth0 to Netgear switch.
    vi. Configure the firewall rules.
    vii. Disable all unused ports.

d. Configure Netgear GS108PE
    i. Configure the IP address according to address table.
    ii. Disable all unused ports.
    iii. Create VLAN 10 on port eth1.
    iv. Create VLAN 20 on port eth2.
    v. Enable Auto-DoS prevention.

e. Configure Raspberry Pi
    i. Install OpenMediaVault.
    ii. Configure the static IP address according to address table.
    iii. Update the OS and software.

iv. Protect the device with a strong password.

v. Set up a NAS specified for FTP.

vi. Enable protection services for files.

f. Configure BeeLink T4 Pro

i. Configure the static IP address according to the address table.

ii. Update the OS and software.

iii. Download FileZilla FTP Server.

iv. Configure the FTP server with strong passwords.

v. Enable document protection features.

vi. Update aircrack-ng.

g. Configure HP Pavilion x360

i. Configure the static IP address according to the address table.

ii. Update the OS and software.

iii. Update OpenVAS/Greenbone with the latest vulnerabilities.

iv. Update Metasploit.

h. Acer Laptop

i. Configure the static IP address according to the routing table.

ii. Update the OS and software.

iii. Download the FileZilla Client.

4) Testing

a. Ping all IP addresses to verify connectivity across the network.

b. Create a mix of open and password-protected files to store on the network.

c. Nmap

i. Scan the network for other hosts.
ii. Find vulnerabilities in the network that relate to open ports.
iii. Identify the end devices that are using port 21 for file sharing.

d. OpenVAS
    i. Scan the administrative portion of the network for vulnerabilities.
    ii. Scan the wireless portion of the network for vulnerabilities.

e. Wireshark
    i. Capture packets travelling across the network for encrypted and unencrypted credentials.
    ii. Capture different packet types to reveal information related to different protocols.

f. Metasploit
    i. Identify the FTP server on the network.
    ii. Attempt to gain access using a password attack.

g. Aircrack-ng
    i. Identify the network interface of the desktop computer used to detect wireless signals.
    ii. Identify the MAC address of the wireless router.
    iii. Attempt to expose the WPA encryption key using a brute force attack.

h. Bettercap
    i. Sniff packets sent between the TP-Link Wireless N Router and the Acer Laptop.
    ii. Attempt a man-in-the-middle attack against the Acer Laptop.

5) Documentation
    a. Project Plan
    b. Project Analysis
    c. Project Description
        i. Network Topology and Addressing Scheme
        ii. Firewall configuration
        iii. Switch configuration
        iv. HP Pavilion x360 configuration
        v. BeeLink T4 Pro configuration
        vi. Raspberry Pi configuration
        vii. Acer Laptop configuration
        viii. Nmap configuration
        ix. OpenVAS/Greenbone configuration
        x. Wireshark configuration
        xi. Metasploit configuration
        xii. Aircrack-ng configuration
        xiii. bettercap configuration
    d. Testing documentation
    e. Project weekly journals
    f. Research References

Table 1

Time Estimate (In Hours)

Research	Design	Implementation	Testing	Documentation	Total
20	30	30	25	30	135

Budget and Costs

All equipment is already owned or is being borrowed free of charge. All software to be downloaded is free and open-source.

Figure 1

Network Topology

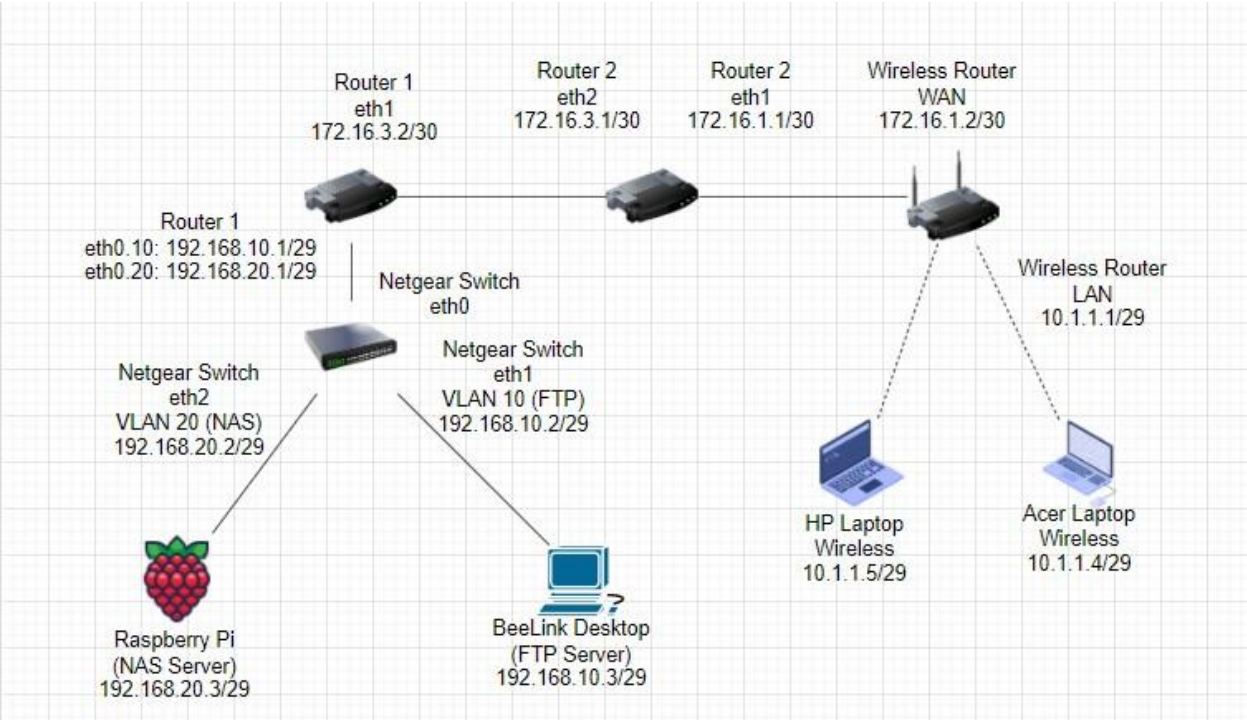

Table 2

IP Table

Device	Port	IP Address	Subnet Mask	Default Gateway	LAN/WAN
Wireless Router	WiFi	10.1.1.1	255.255.255.248	N/A	LAN
	WAN	172.16.1.2	255.255.255.252	N/A	WAN
Wired Router 2	Eth1	172.16.1.1	255.255.255.252	N/A	WAN
	Eth2	172.16.3.1	255.255.255.252	N/A	WAN
Wired Router 1	Eth0	172.16.3.2	255.255.255.252	N/A	WAN
	Eth1	192.168.10.1	255.255.255.248	N/A	LAN
		192.168.20.1	255.255.255.248	N/A	LAN
Switch	Eth1	192.168.10.2	255.255.255.248	192.168.10.1	LAN
	Eth2	192.168.20.2	255.255.255.248	192.168.20.1	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