Project Proposal

PREFORMING A VUNERABILITY

ASSEMENT ON A SECURED NETWORK

MATHIAS SOVINE

UNIVERSITY OF ARKON

SPRING 2021

Project Description:

A computer network will be built using 3 routers, 1 switch, and 4 computers. The network will be used to simulate the connections between an at home office and the internet. The network will be divided into 3 sub-networks. The routers will be secured using methods like access control lists, changing default admin passwords, and network encryption. The switch will be secured using methods like switchport security and setting access passwords. Once the network is secured, three penetration testing techniques and three exploits will be performed on the network. The results of the exploits and penetration testing techniques will be documented. The home office subnet or a device within the home office subnet will be the target of all attacks within the network. One attack will be launched from PC 1 from another subnet and attempt to harvest router login credentials of a user on the home office subnet. Another attack involves a packet sniffing a transferred file from a client (PC 3) to a server (PC 2) sent using the File Transfer Protocol (FTP). The final attack will involves creating a backdoor on PC-3, using Metasploit, and running post exploitation attacks from PC-4.

Network Equipment:

Network PC	**Brand/Model**	**Build**	**Operating System**	**Network Connection**
PC 1	Lenovo Yoga	Laptop	Kali Linux Boot	USB Ethernet Adapter
PC 2	Dell	Tower	Windows 10	Ethernet port
PC 3	Sony Vaio	Laptop	Windows 7	Ethernet port
PC 4	HP	Tower	Kali Linux Boot	Ethernet port

Network Router	**Brand**	**Model**	**# of Ports**
Router A	Linksys	N600 Wi-FI Router E2500	4 LAN & 1 WAN
Router B	TP-Link	AC1900v6	4 LAN & 1 WAN
Router C	Cisco	Series 1921	2 Ethernet Ports

Network Switch	**Brand**	**Model**	**# of Ports**

Switch 1	Cisco	2940 Series	8

Detail Objective:

1.) Design

a. Addressing scheme for network.

i. The home-office subnet will have a router on a stick structure with two VLANs: WORK(10) and PLAY(20).

ii. Across the subnets the NAT and RIPv2 protocols and static routes will be used for routing network traffic.

iii. All network interfaces will use static addressing.

Addressing Table			
Device	**Interface**	**IP Address**	**Subnet Mask**
Router A	LAN Port 2	172.18.0.1	255.255.255.0
	WAN	10.0.0.1	255.255.255.252
Router B	LAN Port 2	10.0.0.5	255.255.255.252
	WAN	10.0.0.2	255.255.255.252
Router C	G0/0	10.0.0.6	255.255.255.252
	G0/1.10 - VLAN 10	192.168.10.1	255.255.255.0
	G0/1.20 - VLAN 20	192.168.20.1	255.255.255.0
PC-1	Ethernet Port	172.18.0.20	255.255.255.0
PC-2	Ethernet Port	192.168.10.2	255.255.255.0
PC-3	Ethernet Port	192.168.10.3	255.255.255.0
PC-4	Ethernet Port	192.168.20.4	255.255.255.0

Switch Configuration		
VLAN	**PORT**	**Connected Device and Interface**
10	F0/1	PC-2: Ethernet Port
10	F0/2	PC-3: Ethernet Port
20	F0/3	PC-4: Ethernet Port

Trunk	F0/8	Router C: G0/0

b. Network connections and subnets will be displayed in the topology within this document.

2.) Configurations of Network Devices

a. All port connections will be made using ethernet cables.

b. Configure Subnet 1

i. Router A

1. Change default router access password.
2. Change router name to Router A.
3. Set the LAN port 2 and the WAN port IP addresses according to addressing table.
4. Enable RIP – this undoes NAT configuration.
5. Enable IPv4 SPI Firewall Protection.

ii. Configure PC-1

1. Configure static IP address for Kali Linux Boot according to the addressing table.
2. Update and upgrade all software packages.

iii. Ping Router A from PC-1 to ensure connection.

c. Configure Subnet 2

i. Configure Router B

1. Change default router access password.
2. Configure the LAN port 2 and the WAN port IP addresses according to addressing table.
3. Set operation mode to Router.
4. Enable NAT and NAT Boost.
5. Create a static route for traffic from Subnet 1 to the Home Office Subnet.
6. Configure security settings.
    a. Enable SPI Firewall.
    b. Enable DoS protection

i. Set ICMP-FLOOD ATTACK Filtering to Middle.
ii. Set UDP-FLOOD ATTACK Filtering to Middle.
iii. Set TCP-SYN-FLOOD ATTACK Filtering to Middle.

7. Enable Traffic Statistics.

d. Configure Home Office Subnet
   i. Configure Router C
      1. Change hostname to RouterC.
      2. Assign the privileged level secret.
      3. Create message of the day: Authorized Users Only!!!
      4. Configure interface G0/0:
         a. int g0/0
         b. ip address 10.0.0.6 255.255.255.252
         c. no shutdown
      5. Configure interface G0/1:
         a. int g0/1
         b. no shutdown
         c. int g0/1.10
         d. encapsulation dot1q 10
         e. ip address 192.168.10.1 255.255.255.0
         f. int g0/1.20
         g. encapsulation dot1q 20
         h. ip address 192.168.20.1 255.255.255.0

      6. Configure default route exiting through the g0/0 interface.
      7. Configure an inbound extended ACL on the G0/0 interface to allow HTTP, HTTPS, and ICMP traffic.
      8. Configure an inbound extended ACL on the G0/1.10 interface to allow all traffic.

9. Configure an inbound extended ACL on the G0/1.20 interface to allow FTP traffic designated for the WORK VLAN and allow all traffic to other networks.

ii. Configure Switch 1
    1. Change hostname to Switch1.
    2. Assign the privileged level secret.
    3. Create message of the day: Authorized Users Only!!!
    4. Configure interfaces f0/1 and f0/2:
        a. No shutdown
        b. Switchport mode access
        c. Switchport access VLAN 10
        d. Switchport port-security maximum 1
        e. Switchport port-security mac-address sticky
    5. Configure interface f0/3:
        a. No shutdown
        b. Switchport mode access
        c. Switchport access VLAN 20
        d. Switchport port-security maximum 1
        e. Switchport port-security mac-address sticky
    6. Configure interface f0/:8
        a. No shutdown
        b. Switchport mode trunk
        c. Switchport trunk allowed VLAN 10
        d. Switchport trunk allowed VLAN 20
        e. Switchport trunk native VLAN 90
    7. Shutdown all unused interfaces

iii. Configure PC-2, PC-3, and PC-4 with the static IP addresses as shown in the addressing table.

iv. Configure the PCs' firewall to allow ICMP traffic.
    1. Download and install Filezilla Server on PC-2.
        a. Configure Filezilla server to listen on port 800.

b. Configure users and groups.
c. Create a directory to share across the network.
d. Configure PC-2 firewall for FTP rule.
e. Configure router to forward FTP traffic.

2. Download and install Filezilla Client on PC-3 and PC-4.
3. Connect PC-3 and PC-4 to PC-2 through configured Filezilla Client software.
4. Test FTP connection by transferring a text file from PC-3 and PC-4 to PC-2.

3.) Test Network Configuration
   a. Ping PC-1 from PC-2, PC-3, and PC-4.
   b. Ping PC-4 from PC-1 and PC-2.
   c. Record results of ping test. Analyze and correct network configurations if ping tests return negative.

4.) Pen-Test Network
   a. Preform reconnaissance using nmap on PC-1.
      i. Scan for hosts on VLANs WORK and PLAY using a Ping Scan:
         1. WORK: nmap -sn 192.168.10.0/24
         2. PLAY: nmap -sn 192.168.20.0/24
      ii. Scan for open ports on VLANs WORK and PLAY using reported IP addresses.
         1. WORK: nmap 192.168.10.1-3
         2. PLAY: nmap 192.168.20.4
      iii. Record a list of open ports and hosts within the Home Office subnet.
      iv. Explain the vulnerabilities of this test.

   b. Run a vulnerability scan using OpenVAS.
      i. Download and install OpenVAS on PC-1 and PC-2.
      ii. Run an OpenVas scan on VLAN WORK and VLAN PLAY from PC-1.
         1. Record the list of vulnerabilities for each PC.

2. Report and list solutions for vulnerabilities with 8.0 severity or higher.

iii. Run an OpenVas scan on VLAN WORK from PC-2.
1. Record the list of vulnerabilities for each PC.
2. Report and list solutions for vulnerabilities with 8.0 severity or higher.

iv. Document the differences in recorded vulnerabilities between PC-1 and PC-2's reports.

v. Explain the vulnerabilities that the OpenVas exposes.

c. Use a Phishing Email to test network users.

i. Use a phishing attack to gain graphical router login access for Router B.
1. geomont789@gmail.com to receive phishing email.
2. mvicor451@gmail.com to send phishing email.

5.) Exploit Network

a. Phishing Email Attack

i. Run a nmap scan of Router B from PC-1 to find the graphical router access interface.

ii. Use the wget command to download web files from Router B.

iii. Edit the created index.html file using HTML and PHP to mimic Router B's login page.

iv. Use Setoolkit on PC-1 to harvest credentials for Router B login.
1. sudo setoolkit
2. 1 – Social-Engineering Attack
3. 2 – Website Attack Vectors
4. 3 – Credential Harvester Attack Method
5. 3 – Custom Import
6. Set custom webpage to the edited index.html file.

v. Send a phishing email to geomont789@gmail.com on PC-3 about needing to login to the router with a phishing link to the index.html file.

vi. Collect login credentials from the geomont789@gmail.com login.

vii. Login to router from PC-1 using credentials.

   b. Windows 7 Exploit
      i. Run msfconsole and create a payload with msfvenom on PC-4.
      ii. Send payload to FTP server.
      iii. Send a request to PC-3 user to download the file from the FTP server.
      iv. Use open meterpreter shell to run post exploitation commands.
      v. Send copies of important files on PC-3 back to the PC-4.
   c. Man-in-the-middle Attack
      i. Using Wireshark on PC-3 capture a plain-text document traveling over FTP between PC-4 and PC-2.
      ii. Use information within the plain-text document to exploit the user of PC-4.
6. Secure Network
   a. Harden network security to prevent the pen-testing techniques from being used on the network.
      i. Set Home Office subnet devices to block pings from outside of the network.
      ii. Write a phishing email detection training document.
   b. Harden network security to prevent vulnerabilities revealed by OpenVas scan and exploits.
      i. Write report on how to send a document over ftp securely.
      ii. Download AVG on PC-3 to help prevent further downloads of malicious files.
7. Documentation
   a. Project Description
   b. Network Equipment
   c. Detail Objective
      i. Addressing scheme for network.
      ii. Configurations of Network Devices
      iii. Test Network Configuration
      iv. Pen-Test Network
      v. Exploit Network

vi. Secure Network
vii. Documentation

d. Time Estimate
e. Budget Estimate
f. Topology

Time Estimate (In Hours):

Research	Design	Implementation	Testing	Documentation	Total
20	**5**	**20**	**5**	**25**	**75**

Budget Estimate:

The needed extra equipment for this proposal will cost $120. The software being used is opensource or previously purchased.

Topology:

View Image on next page.

Network Topology