Fall 2023

Small Business Office Network

Michael Gerome
mdg111@uakron.edu

CIS Senior Cybersecurity Project Spring 2023

Michael Gerome

College Engineering and Polymer Science, University of Akron

CISS-491-801 CIS Senior Cybersecurity Project

John B. Nicholas, PhD

March 26, 2023

Project Name:

Small Business Office Network

Project Description:

This project proposal describes a network of a small business setting up an office network. The network will have basic security configured and the IT department will run penetration tests on the network to find vulnerabilities. After the tests are performed and the results are documented the network will be further secured in accordance with the results of the tests. There will be four departments configured in the network separated by VLANs: Management (VLAN99), HR (VLAN48), Sales (VLAN24), and IT (VLAN36). The Management department will be placed in the 192.168.99.0/24 network, the HR department will be placed in the 192.168.48.0/24 network, the sales department will be placed in the 172.20.24.0/24 network, and the IT department will be placed in the 10.30.36.0/24 network. The three routers will be connected with /30 networks in accordance with the addressing table. The departments are placed on separate networks to allow the IT department to control what traffic can pass from one department to another. Once the networks are configured and connectivity is confirmed and documented the IT department will begin by performing a network scan on a Kali Linux machine using the Nmap tool. Then the IT department will use the Kali Linux tools Legion and Nikto to gather vulnerability information from the network. The Medusa Tool will also be used to attempt to crack login credentials on the routers in the network.

Location of Work:

The network will be emulated using GNS3 on a personal laptop.

Equipment Used:

- 3x Cisco CSR1000v 17.03 Routers
- 5x CiscoIOSvL2 Switches
- 8x Windows 10 Desktops
- 1 Kali Linux Laptop

Detailed Objective:

1. Research
    a. Confirm configuration of Router-on-a-stick and inter VLAN routing.
    b. Network scanning with the Nmap tool.
    c. Vulnerability scanning with Kali Linux tools.
        i. How to operate Legion.
        ii. How to operate Nikto.
    d. Password cracking attempt with Medusa Tool in Kali Linux.
    e. Configuration and topology layout for devices in network.
2. Design
    a. Deploy devices in GNS3 following the network topology shown below.
    b. The devices and their interfaces will be given static IP addresses following the according the address table shown below:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router 1	Gi1.48	192.168.48.1	255.255.255.0	NA
	Gi1.99	192.168.99.1	255.255.255.0	
	Gi2	10.10.1.1	255.255.255.252	
	Gi3	10.10.3.1	255.255.255.252	
Router 2	Gi01.24	172.20.24.1	255.255.255.0	NA

	Gi2	10.10.1.2	255.255.255.252	
	Gi3	10.10.2.1	255.255.255.252	
Router 3	Gi1.36	10.30.36.1	255.255.255.0	NA
	Gi2	10.10.3.2	255.255.255.252	
	Gi3	10.10.2.2	255.255.255.252	
Switch 1	VLAN 1	192.168.48.2	255.255.255.0	192.168.48.1
Switch 2	VLAN 1	192.168.48.3	255.255.255.0	192.168.48.1
Switch 3	VLAN 1	192.168.99.2	255.255.255.0	192.168.99.1
Switch 4	VLAN 1	10.30.36.2	255.255.255.0	10.30.36.1
Switch 5	VLAN 1	172.20.24.2	255.255.255.0	172.20.24.1
PC1	NIC1	192.168.48.4	255.255.255.0	192.168.48.1
PC2	NIC1	192.168.48.5	255.255.255.0	192.168.48.1
PC3	NIC1	192.168.99.4	255.255.255.0	192.168.99.1
PC4	NIC1	192.168.99.5	255.255.255.0	192.168.99.1
PC5	NIC1	172.20.24.3	255.255.255.0	172.20.24.1
PC6	NIC1	172.20.24.4	255.255.255.0	172.20.24.1
PC7	NIC1	172.20.24.5	255.255.255.0	172.20.24.1
PC8	NIC1	10.30.36.3	255.255.255.0	10.30.36.1
Laptop1	eth0	10.30.36.4	255.255.255.0	10.30.36.1

c. The network will use EIGRP for routing between routers.

d. Each network will be on a separate VLAN.

i. Router 1 will be connected to the Management VLAN (VLAN 99) and the HR VLAN (VLAN 48). The connection between Switch 2 and Router 1 will be configured with sub interfaces for Router-on-a-stick inter VLAN routing.

ii. Router 2 will be connected to the Sales department on VLAN 24.

iii. Router 3 will be connected to the IT department on VLAN 36.

e. All unused ports on all routers and switches will be disabled.

f. ACLs will be configured on all routers to fulfill network needs (ACL commands shown in implementation section):

i. Router 1:

1. Management and HR departments will be able to reach the Sales and IT desktop.
2. No access to Pen testing laptop from Management or HR department.
3. Any traffic directed outside the networks in the addressing table will be denied.

ii. Router 2:

1. The sales department will be able to reach the IT person's Desktop but not the Pen testing laptop.
2. They should also be able to contact the management and HR network.
3. Any traffic directed outside the networks in the addressing table will be denied.

iii. Router 3:

1. Kali Linux laptop will be able to have access to all devices in network.

2. IT department will be able to access Management and Sales departments.

g. STP will be configured on switch 1, switch 2, and switch 3 in order to prevent network loops.

3. Implementation

a. Deploying devices and connecting them with ethernet cables.

i. This is done virtually in GNS3 following the design of the network topology shown below.

b. Assign static IP addresses to each device according to the addressing table.

i. Router and switch IP addresses will be configured through the CLI

ii. The Windows and Kali Linux device will be configured through the settings in the GUI.

c. Configure basic initial configuration on routers and switches:

i. Configure the device name.

ii. Configure time on devices.

iii. Secure user EXEC mode by setting strong password on line console 0 and require login.

iv. Configure SSH access on routers and switches in network for remote management.

1. Configure a hostname for the device.
2. Configure a domain name for device.
3. Create a crypto key for device

4. Generate a username and password for a user with administrator privilege.
5. On the vty lines configure ssh to be the method for login.

v. Secure privileged EXEC mode by configuring a strong password

vi. Secure all passwords in the config file by employing password encryption.

vii. Provide legal notification by creating a “message of the day” banner to warn against unauthorized access to the device.

viii. Configure the management SVI by configuring interface VLAN 1 of the switches with IP addresses according to the addressing table.

ix. Configure default Gateway on the switches.

d. Configure VLANs on switches, configure router-on-a-stick configuration on Router 1, and assign switch interfaces to VLANs.
    i. VLAN 99: Management
    ii. VLAN 24: Sales
    iii. VLAN 36: IT
    iv. VLAN 48: HR
    v. VLAN 75: Unused-Interfaces
e. Configure STP on switch 1, switch 2, and switch 3 to prevent network loops.
    i. Use the spanning-tree command and available options to configure.
f. Configure EIGRP routing on routers in global config mode:
g. Implement Layer 2 Security
    i. Shutdown all unused ports on switches and assign them to VLAN 75

ii. On all trunk ports on switch 1, switch 2, and switch 3 disable automatic trunking.

iii. On access ports on switch 4 and switch 5 implement port security to prevent MAC address table attacks.

h. Implement router security:

i. Configure log messages to have timestamps:

1. service timestamps log datetime

ii. Prevent brute force login attacks by limiting the number of login attempts that can be attempted within a couple of minutes. Log all login attempts to monitor device access.

iii. Enable IOS Image Resilience Feature:

1. secure boot-image

iv. Configure local AAA with strong password:

i. Implement ACLs on Routers to follow rules in the design section.

4. Testing

a. Perform ping tests on various networks to others to confirm expected connectivity.

b. Perform network scanning with Nmap.

i. Discover what is visible to Nmap and what services are running on devices in the network.

ii. Document results of test.

c. Vulnerability scanning with Legion.

i. Find potential vulnerabilities with Legion tool on network.

ii. Implement solutions for vulnerability if possible.

iii. Document the vulnerability and the solutions.

d. After fixing vulnerability run another vulnerability scan with Nikto.

i. Confirm if the same vulnerabilities appear and if fixed vulnerabilities are gone.

ii. Implement solutions to new vulnerabilities if possible.

iii. Document the results and solutions to new vulnerabilities.

e. Password cracking attempt on devices with Medusa.

i. Attempt to crack various login credentials of devices throughout the network with Medusa tool.

ii. Document the results and replace passwords if needed.

5. Documentation

a. Project Plan

b. Project Analysis

c. Project Description

i. Configuration of all devices through the implementation stage.

d. Testing Documentation

i. Successful and failed ping attempts.

1. Reason and solution of failed pings

ii. Information found with Nmap.

1. Open ports and solutions.

iii. Use of Legion and vulnerabilities discovered with tool.

1. Steps taking to mitigate vulnerabilities.

iv. Use of Nikto and vulnerabilities discovered with tool.

1. Steps taking to mitigate vulnerabilities.

v. Password cracking attempt with Medusa.

1. Details on how to conduct attack.

2. Details on the results of the attack.

e. Project Weekly Journals

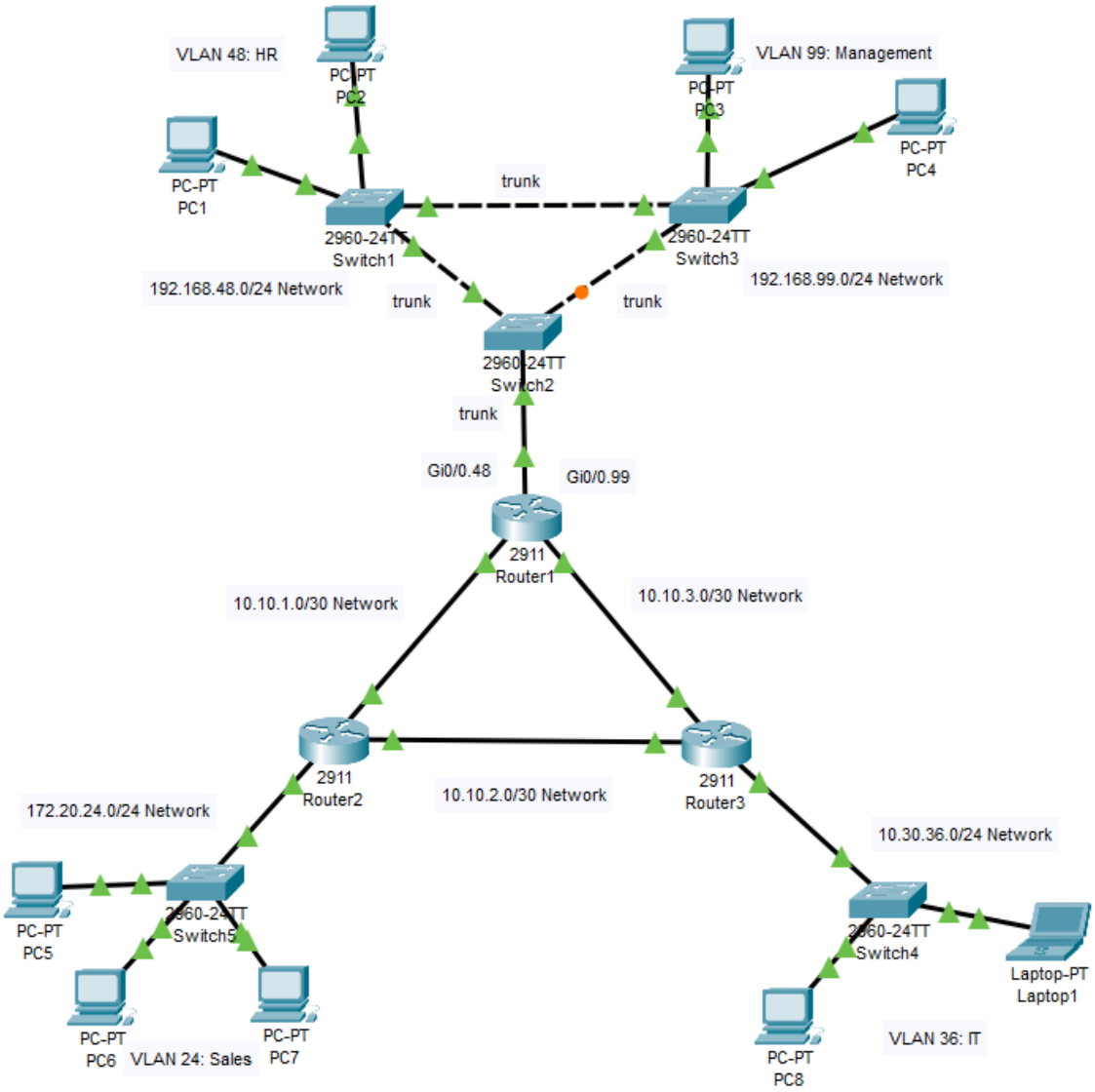
f. Research References

Time Estimate:

Research	Design	Implementation	Testing	Documentation	Total
20 Hours	10 Hours	15 Hours	20 Hours	15 Hours	80 Hours

Budget or Cost Estimate:

GNS3 is a free software however the IOS images of the devices need to be purchased and imported. A pack of Cisco device images can be found at (https://dynamips.store/product/gns3-cisco-images-downlaod/) for $56.


VLAN 48: HR
PC-PT
PC2
VLAN 99: Management
PC-PT
PC3
PC-PT
PC4
PC-PT
PC1
trunk
2960-24TT
Switch1
2960-24TT
Switch3
192.168.48.0/24 Network
trunk
trunk
192.168.99.0/24 Network
2960-24TT
Switch2
trunk
Gi0/0.48
Gi0/0.99
2911
Router1
10.10.1.0/30 Network
10.10.3.0/30 Network
2911
Router2
10.10.2.0/30 Network
2911
Router3
172.20.24.0/24 Network
10.30.36.0/24 Network
PC-PT
PC5
2960-24TT
Switch5
2960-24TT
Switch4
Laptop-PT
Laptop1
PC-PT
PC6
VLAN 24: Sales
PC-PT
PC7
PC-PT
PC8
VLAN 36: IT

Project Analysis

Overall, the process of completing the project was a success. There were a few minor configuration mistakes on devices and changes that needed to be made to the testing plan, but these issues did not impact the success of the project. The network layout chosen in this project is meant to depict a small office network with different departments. This network is isolated from the Internet and is solely meant for internal use. The following section will summarize the configurations made to the different devices in the network and what role they play.

The routers on the network are present to allow interconnectivity between the departments and to monitor and control the network traffic that travels between them. There are three routers in the network, Router1 connects to the 192.168.48.0/24 and 192.168.99.0/24 subnets and is the default gateway. Router2 is the default gateway of the 172.20.24.0/24 subnet and Router3 is the default gateway for the 10.30.36.0/24 subnet. Each router also has strong passwords set for the user EXEC mode, privileged EXEC mode, and SSH connections. The routers are also configured with a local AAA server increased security which requires a username and password to enter the terminal of the router. The routing protocol Enhanced Interior Gateway Routing Protocol (EIGRP) is used to connect the routers and allow them to communicate with each other. Interface Gi1 on Router1 is configured with two subinterfaces, Gi1.48 and Gi1.99 which allows for router-on-a-stick configuration. This allows for the two VLANs connected to Router1 to communicate. When initially configured the encapsulation dot1q was not set on interface Gi1.99 and therefore connectivity was not possible at the time. This caused much confusion when trying to troubleshoot the issue however it was eventually fixed.

In order to enhance the security of the routers login attempts on all connections are limited to five failed login attempts within one minute. This protects the routers against brute-force password attacks. This was proven in the testing portion of the project as a brute-force password attack was unsuccessful because of this configuration. Finally, access control lists (ACLs) were configured on the routers to limit what departments other departments can communicate with.

The switches in the network are present to connect the end devices to the routers. They are configured with VLANs to allow different departments of this small business to be separated for each other in the network. There are five switches present in the network topology. They are all configured with the default gateway of the network they are in and have the SVI Vlan1 configured with an IP address. Just as with the routers in the network the switches have passwords configured for the user EXEC mode, privileged EXEC mode, and SSH connections. Each switch is configured with five VLANs which represent the different departments. Switch1, Switch2, and Switch3 are responsible for VLAN 48 (HR) and VLAN 99 (Management). Switch4 is connected to devices in VLAN 36 (IT) and Switch5 is connected devices in VLAN 24 (Sales). Switch1, Switch2, and Switch3 have spanning tree protocol (STP) configured on them since the three switches are all connected. STP determines the best path to the destination and send the packet only out that direction. This helped prevent network loops where packets get caught traveling between switches in a loop.

In order to increase the security of the switches in the network all the unused interfaces where assigned to a separate VLAN and all turned to administratively down. Next the trunking links which allow the different VLANs to communicate are configured to disable automatic DTP trunking negotiations. This means that the switch will ignore incoming DTP frames which are

attempting to connect to the switch. The port security of the switches is configured to limit MAC addresses on systems and disable the port if an external MAC address attempts to assign itself to the switch. This configuration helps to prevent any form of MAC address attack on the switches.

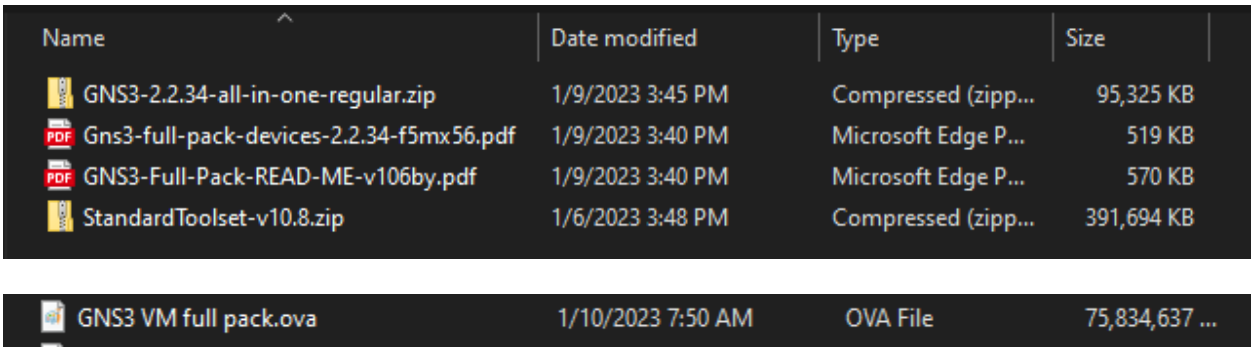
There are two types of end devices in the network topology, Windows 10 computers and a Kali Linux laptop. The windows computers are present solely for the purpose of host to target within the network. Each windows computer is configured with an IP address as laid out in the addressing table. This is done through the Network & Internet settings on each device. Initial attempts to ping the end devices result in no response. After researching possible reasons for this issue, it was discovered that this was due to the windows firewall blocking the ICMP packets from reach the device. This was fixed by using the command prompt to add a rule to the firewall allowing the ICMP packets through to the system. The Kali Linux laptop is used in this project as the penetration testing device. When first configured the OS needed to be installed in order to allow the device to keep changes made to it after being used. Once set up, the machine had many built-in tools for penetration testing and vulnerability scanning.

These tools were used in the testing phase of the project. Once the desired connectivity between devices was confirmed Kali Linux was used to determine what information was visible from within the network. Nmap was used as a reconnaissance to discover devices in the network and their IP address. Nmap was also used to determine what TCP ports were open on each device. Next the Legion tool was used to scan the network for host and vulnerabilities. Unfortunately, due to the fact that the network design does not involve being connected to the internet the laptop was unable to retrieve information from the online vulnerability databases. However, the tool is still able to run a wide-variety of tools and scripts to gather additional information. Finally, the medusa tool was used to attempt to brute-force attack the password for

the SSH connection on Router3. However due to the security configuration done this attack was unsuccessful.

Project Description

This project was performed using the GNS3 software within a software package found at the following URL: (https://dynamips.store/product/gns3-cisco-images-downlaod/). After purchasing the package of Cisco IOS, download all the files received via email which are shown below.



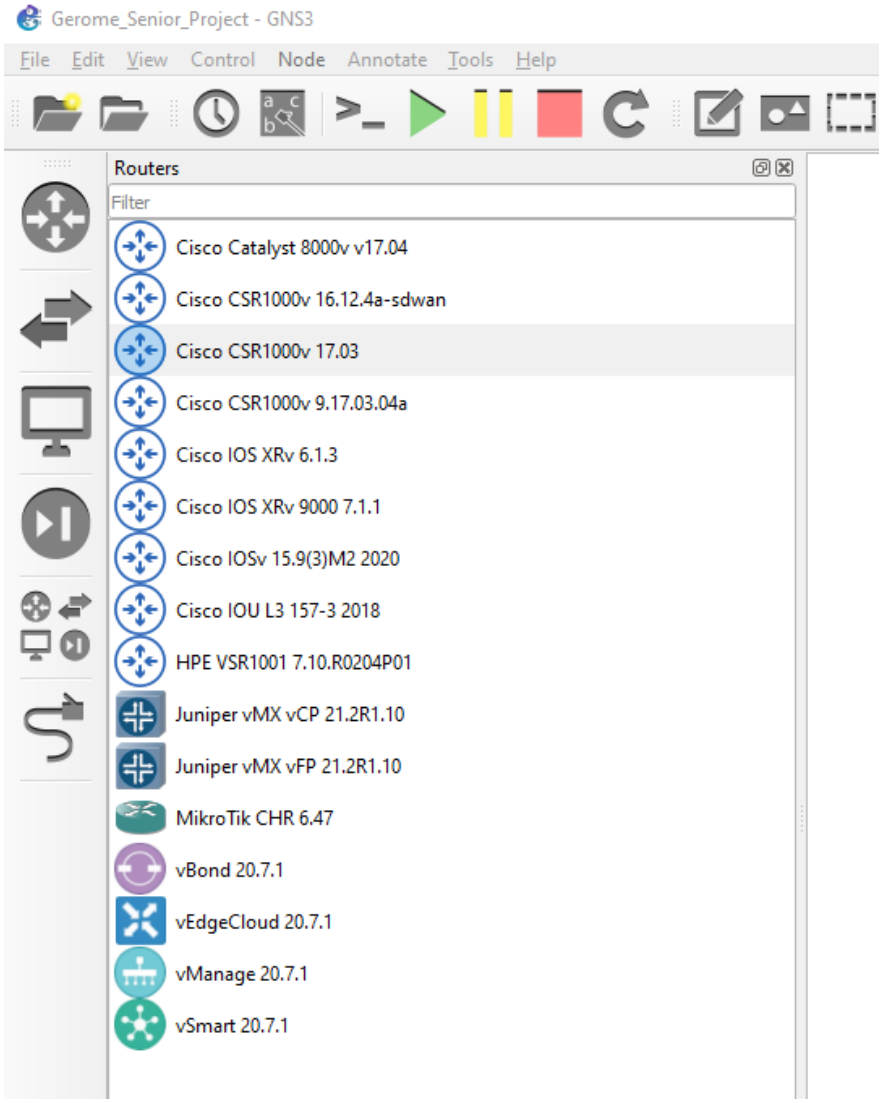
Name	Date modified	Type	Size
GNS3-2.2.34-all-in-one-regular.zip	1/9/2023 3:45 PM	Compressed (zipp...	95,325 KB
Gns3-full-pack-devices-2.2.34-f5mx56.pdf	1/9/2023 3:40 PM	Microsoft Edge P...	519 KB
GNS3-Full-Pack-READ-ME-v106by.pdf	1/9/2023 3:40 PM	Microsoft Edge P...	570 KB
StandardToolset-v10.8.zip	1/6/2023 3:48 PM	Compressed (zipp...	391,694 KB

GNS3 VM full pack.ova	1/10/2023 7:50 AM	OVA File	75,834,637 ...

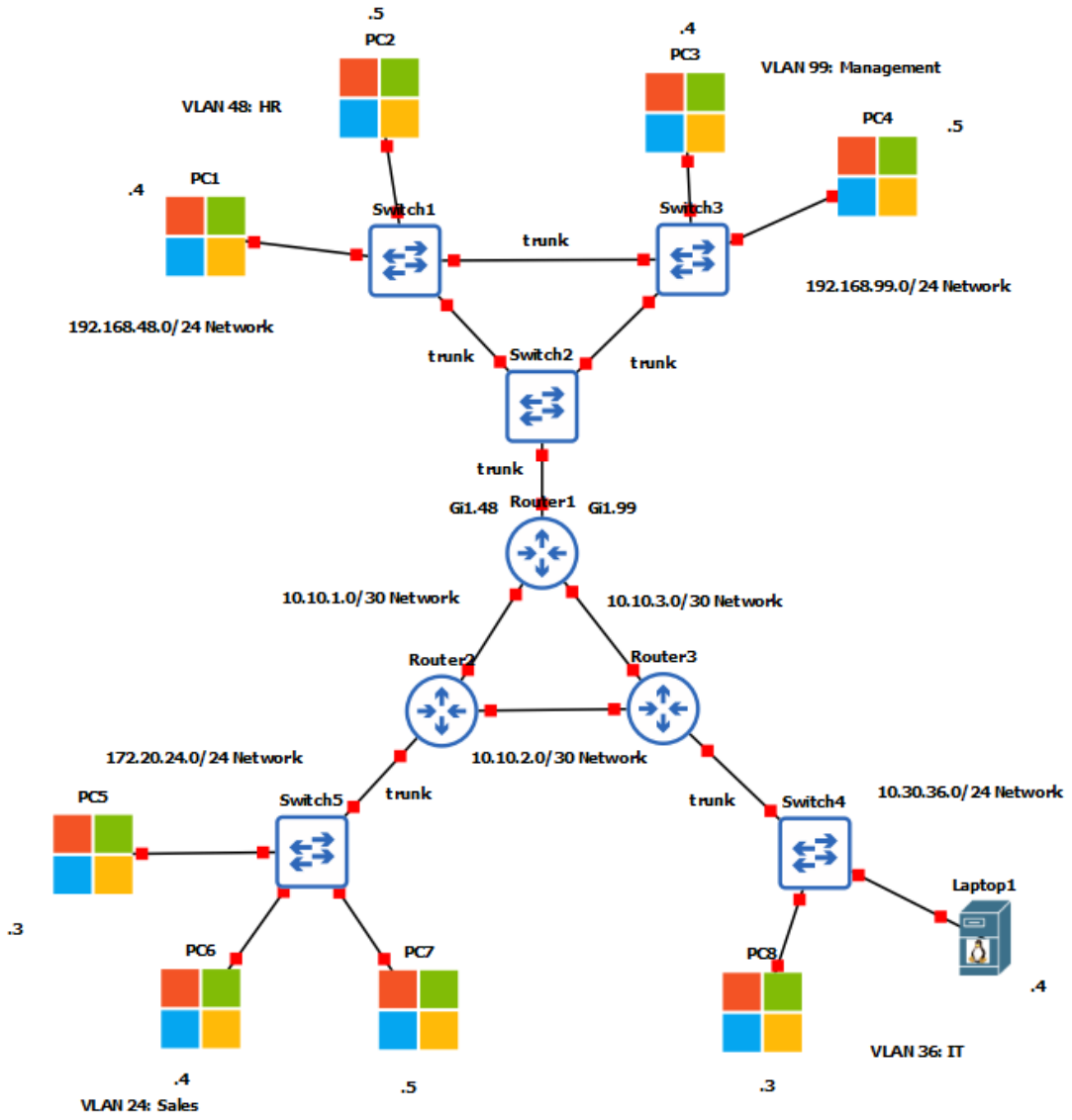
The .ova file contains all the devices used in this project. Use this file to create a virtual machine using the hypervisor of choice. Follow the directions in the READ ME file to install GNS3 and the VM. The “Gns3-full-pack-devices-2.2.34-f5mx56.pdf” file contains the default usernames and passwords for some of the devices in the pack.

Part 1: Topology Setup & IP Address Configuration

Once properly downloaded and the virtual machine is started, devices will appear in the GNS3 software. Remember after each part to save the running configurations to the startup-config file on the routers and switches in the network using the copy command:



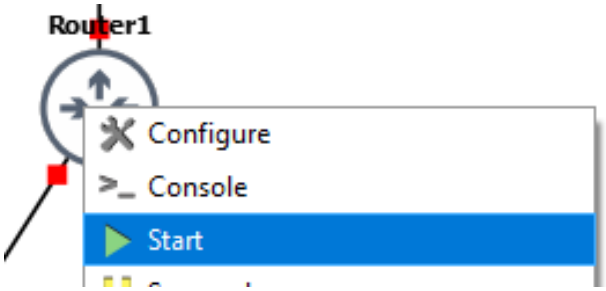
1. Begin by placing devices in accordance with the Project Plan and connect the devices with links on the interfaces specified in the addressing table.



2. Change the display name of the devices as shown above by double clicking on the shown name.

3. Start the routers by right-clicking on them and selecting “Start”

4. Right-click the device again and select “Console” and wait for the startup sequence to complete.



5. When prompted type “no” to exit the Auto install script.

```
No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console

Autoinstall trying DHCPv4 on GigabitEthernet1,GigabitEthernet2,GigabitEthernet3


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no
```

6. Enter global configuration mode by typing the following commands. This will work on all routers and switches used:

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

7. Assign static IP addresses to router interfaces according to the addressing table (ignore interface Gi1 on Router 1 for now this will be configured later) using the following commands:

```
Router(config)#interface GigabitEthernet2
Router(config-if)#ip add
Router(config-if)#ip address 10.10.1.1 255.255.255.252
Router(config-if)#no shutdown
```

8. Once all the interfaces are configured with IP addresses exit global configuration mode and save the device configuration to startup-config:

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

9. Check the configuration of the interfaces to confirm all IP addresses are assigned with the "show ip interface brief" command:

Router1

```
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES unset  administratively down down
GigabitEthernet2       10.10.1.1       YES manual up                    up
GigabitEthernet3       10.10.3.1       YES manual up                    up
GigabitEthernet4       unassigned      YES unset  administratively down down
```

Router2

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       172.20.24.1     YES manual up                    up
GigabitEthernet2       10.10.1.2       YES manual up                    up
GigabitEthernet3       10.10.2.1       YES manual up                    up
GigabitEthernet4       unassigned      YES unset  administratively down down
```

Router3

```
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.30.36.1      YES manual up                    up
GigabitEthernet2       10.10.3.2       YES manual up                    up
GigabitEthernet3       10.10.2.2       YES manual up                    up
GigabitEthernet4       unassigned      YES unset  administratively down down
Router#
```

10. Now perform the same commands on the switches in the network to assign IP addresses to their VLAN 1 interface:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip addre
*Mar 22 17:42:34.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
Switch(config-if)#ip address 192.168.48.2 255.255.255.0
Switch(config-if)#no shutdown
```

11. Also configure the default gateway on the switches in accordance with the addressing table. These addresses point towards an interface on the routers:

```
Switch(config)#ip default-gateway 192.168.48.1
```

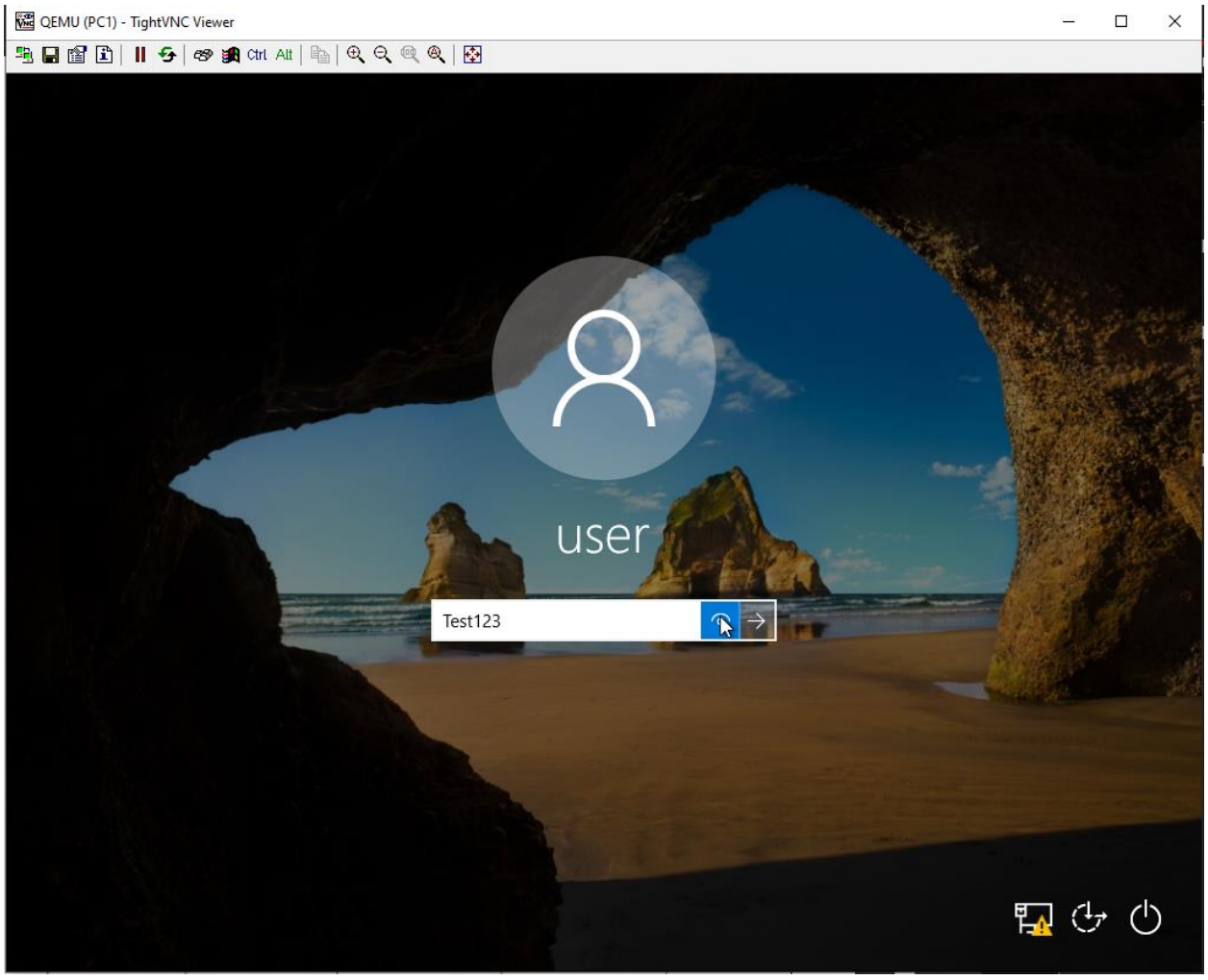
12. Once configured save the configuration with the following command:

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 3409 bytes to 1571 bytes[OK]
Switch#
*Mar 22 17:48:35.212: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Mar 22 17:48:35.886: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch#
```

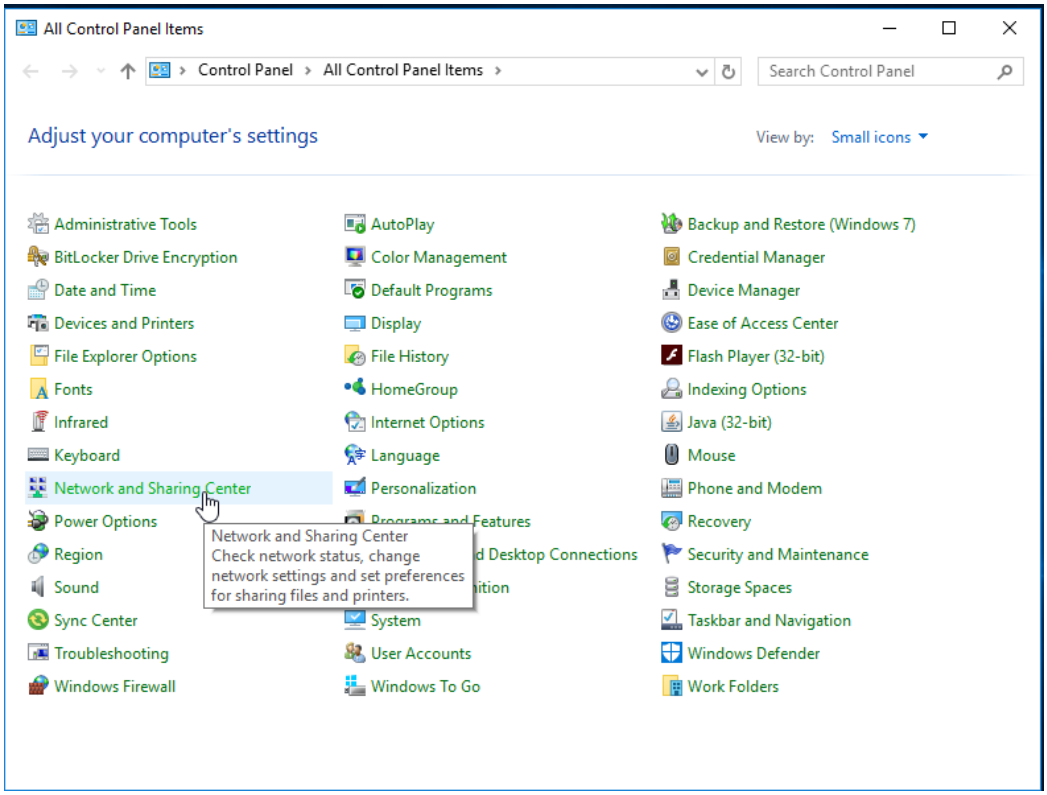
13. Confirm the IP address was configured correctly by using the following command:

```
Switch#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Vlan1                  172.20.24.2     YES manual up                    up
Switch#
```

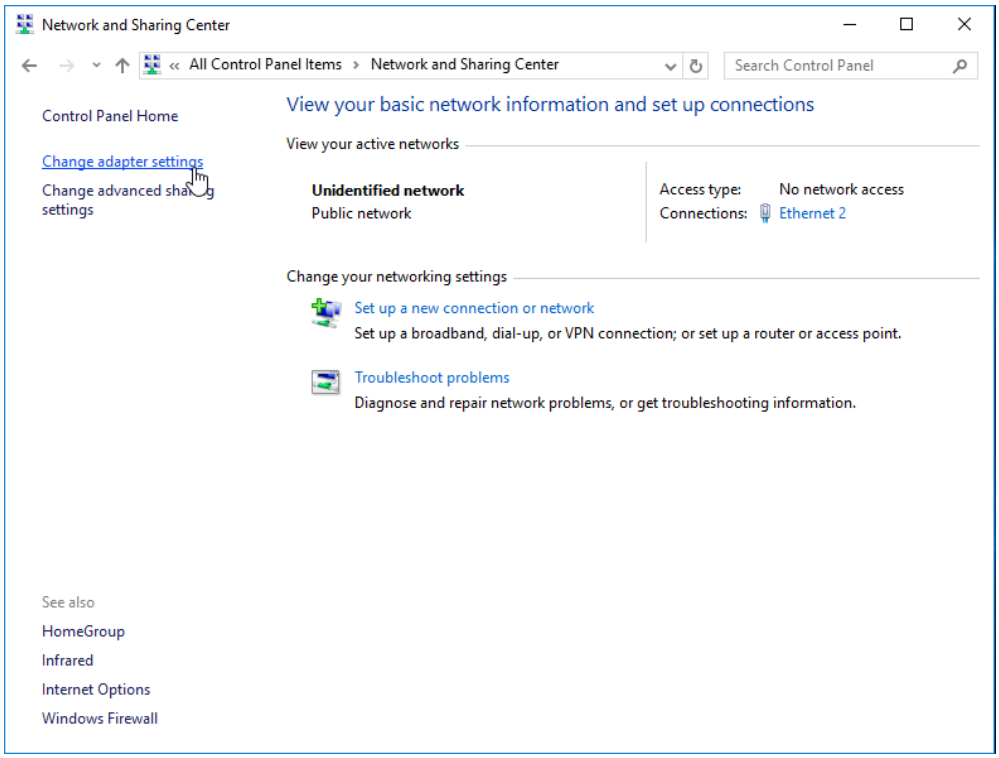
14. Now start the Windows computers by right-clicking on the device and selecting “Start”. Then right-click again and select “Console.”
15. Once the device is started-up there will be a login screen. The device will automatically log into the “user” user with a default password of “Test123”.



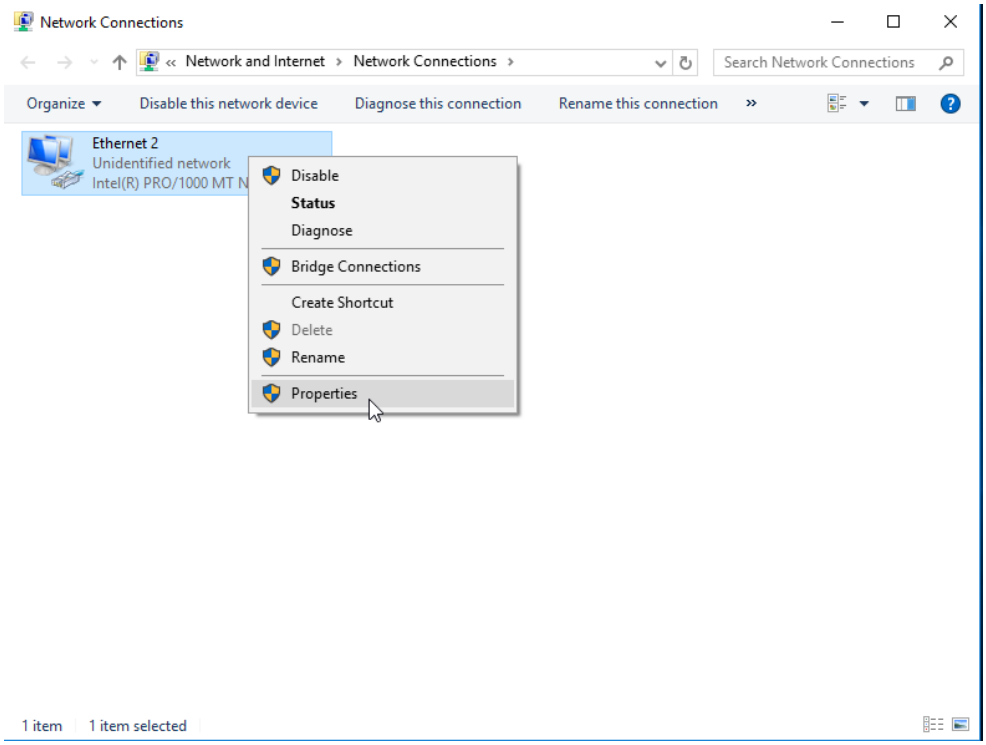
16. Open the Control Panel and select the Network and Sharing Center.



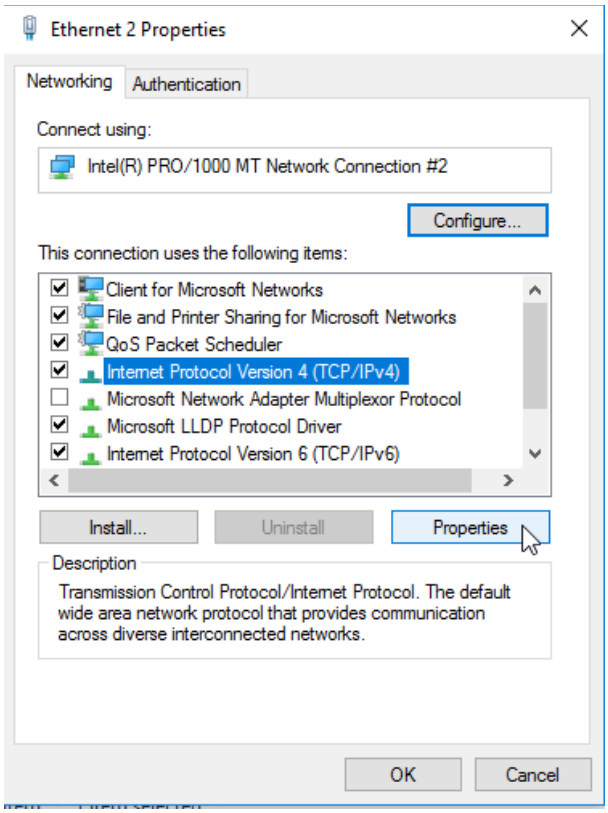
17. Select Change adapter settings.



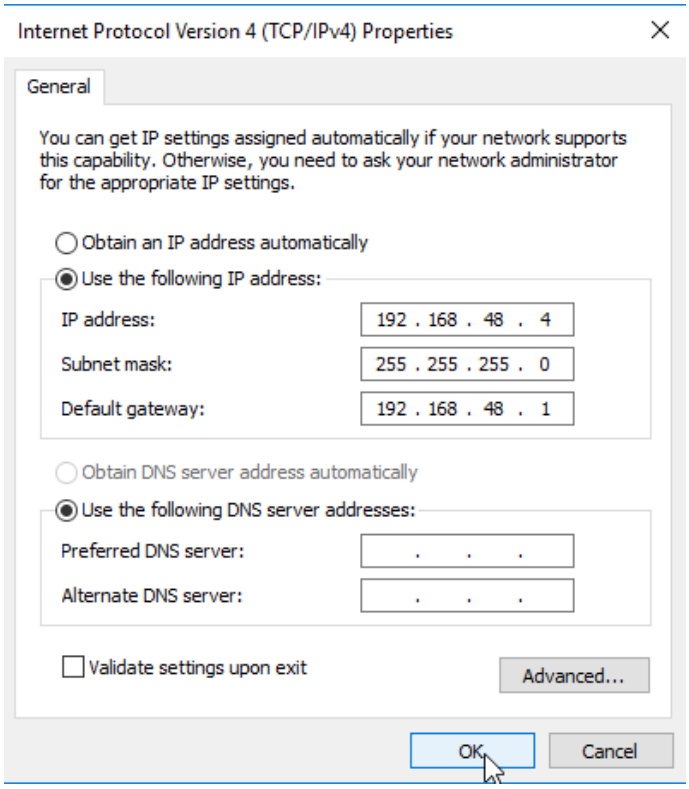
18. Right-click on the network adapter and select Properties.



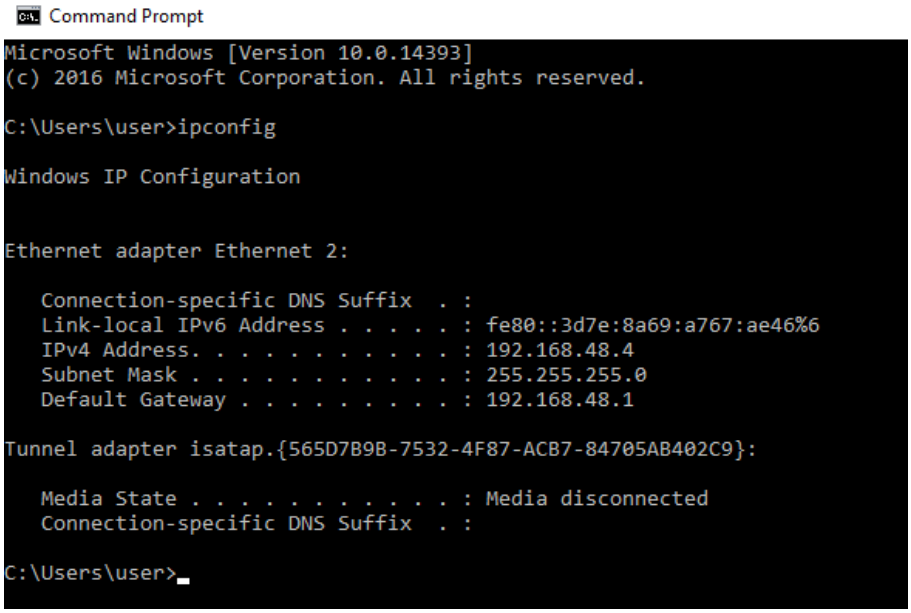
19. Select the Internet Protocol Version 4 (TCP/IPv4) and then select the Properties button.



20. Select Use the following IP address and enter the IP address, subnet mask, and default gateway according to the addressing table. Then select OK.



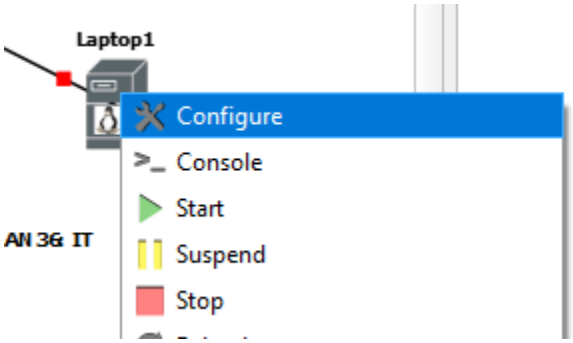
21. Then open the Command Prompt and use the “ipconfig” command to confirm the IP address changed.



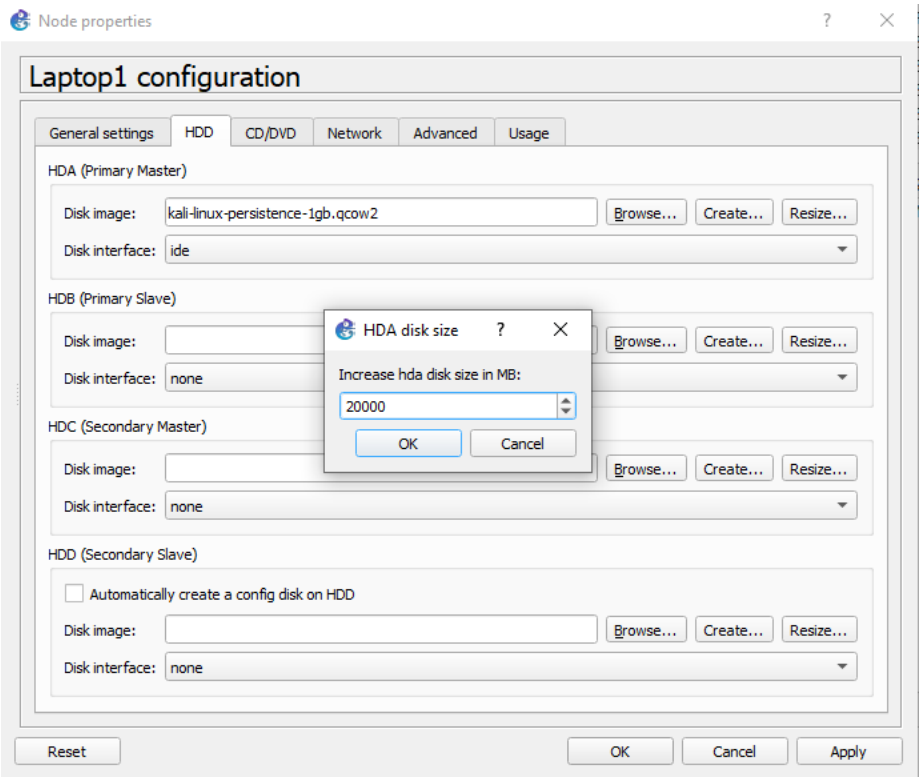
22. Repeat this process for the rest of the Windows 10 devices in the network.

23. Once finished with the windows computer start the Kali Linux Laptop and open the console.

24. Right-click on Laptop1 and select Configure:



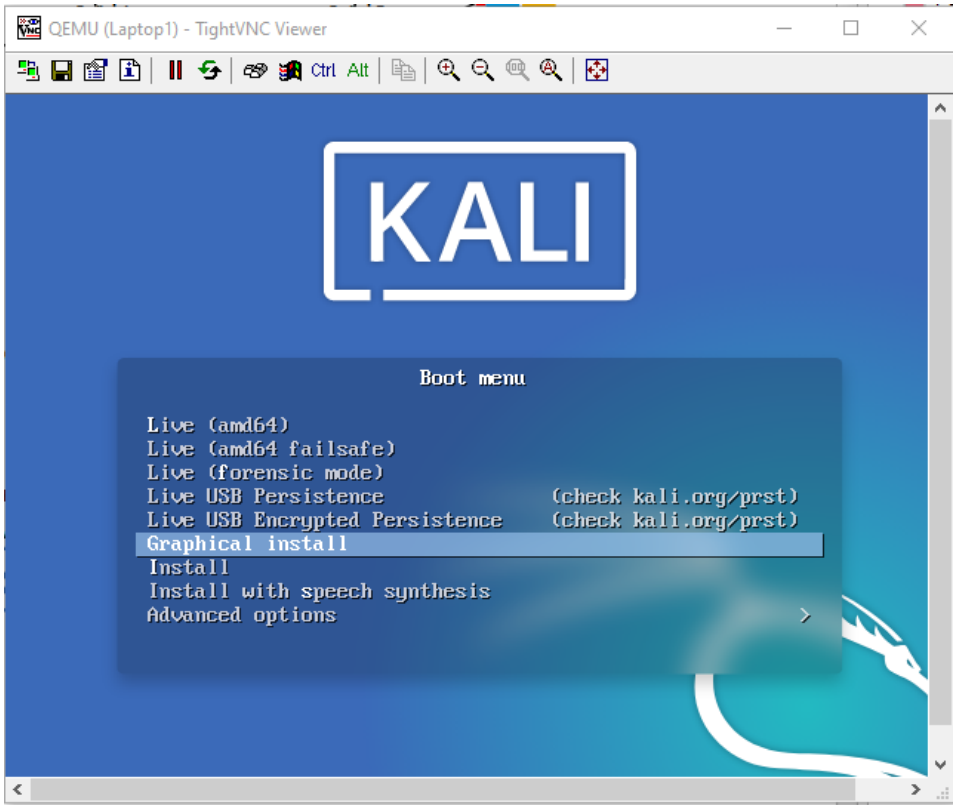
25. Select “Resize…” on the HAD (Primary Master) HDD and enter 20,000 for the MB size



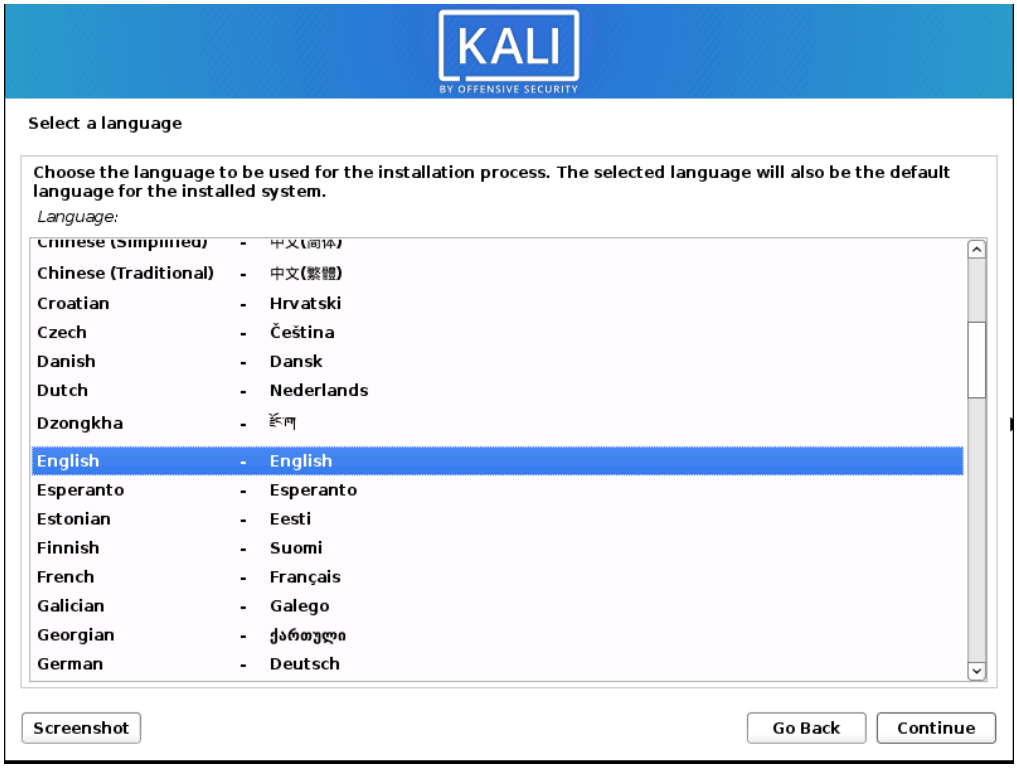
26. Select “OK” then “Apply” and close the window.

27. Start Laptop1 and open the Console connection.

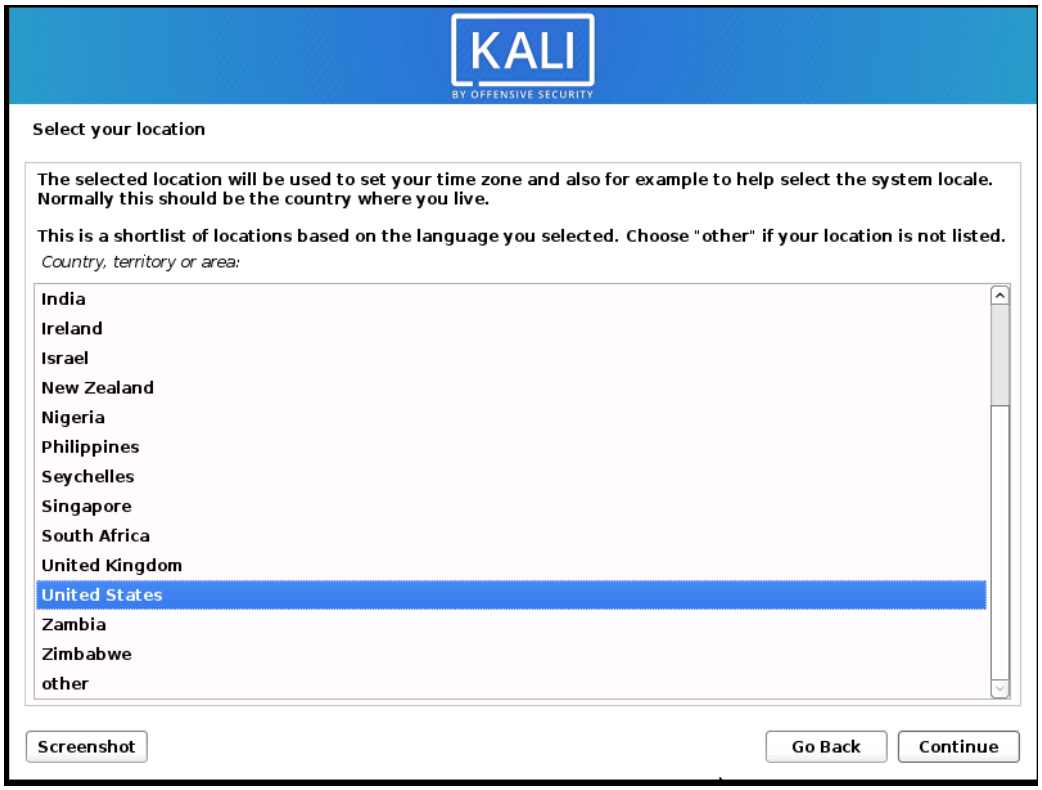
28. In the Boot menu press enter on “Graphical Install.”



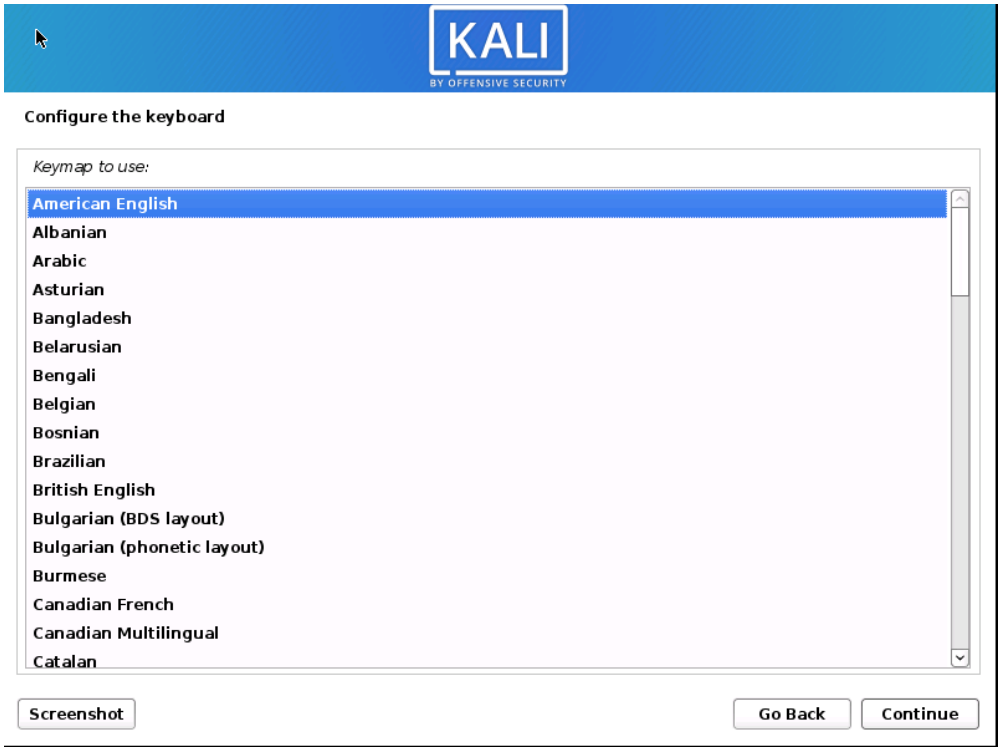
29. Select English as language of choice:



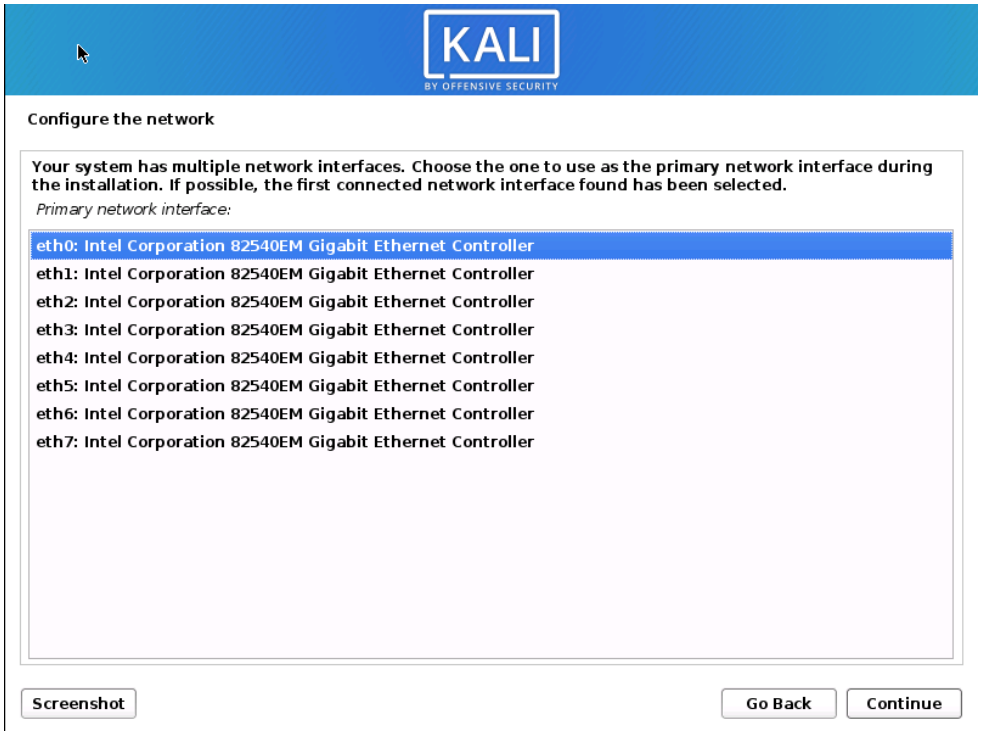
30. Select United States as the location:



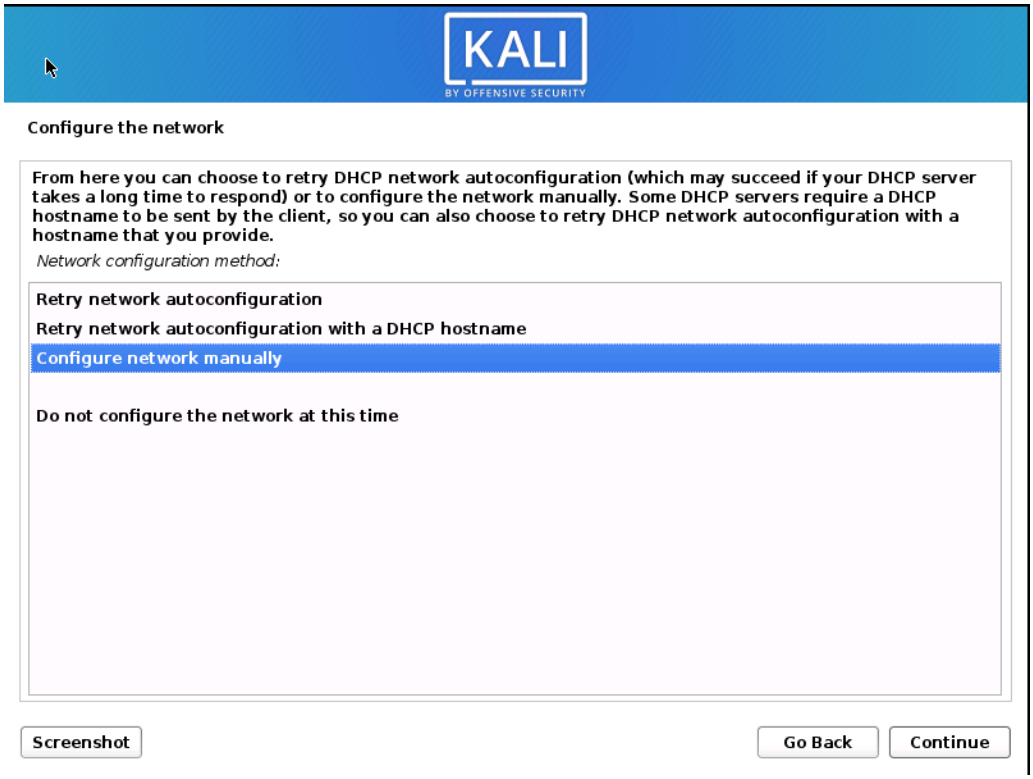
31. Select “American English” for keyboard layout:



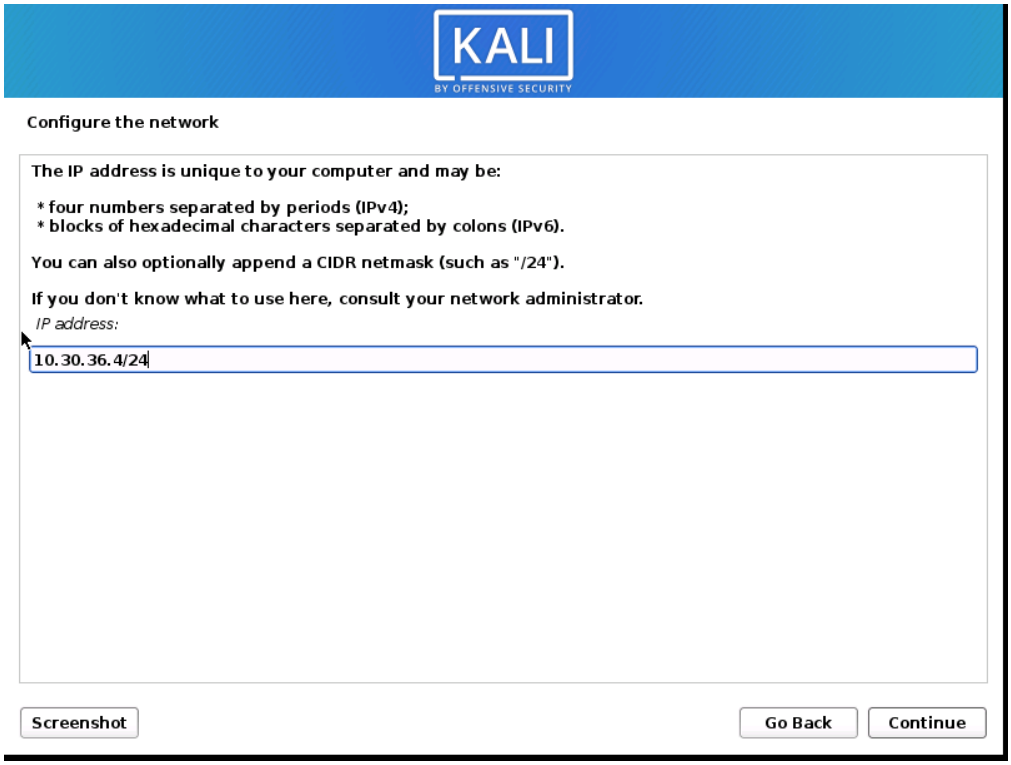
32. The device will then attempt to confiure network settings using DHCP but it will fail. It will then prompt to manually confiure the network. Select eth0 when prompted:



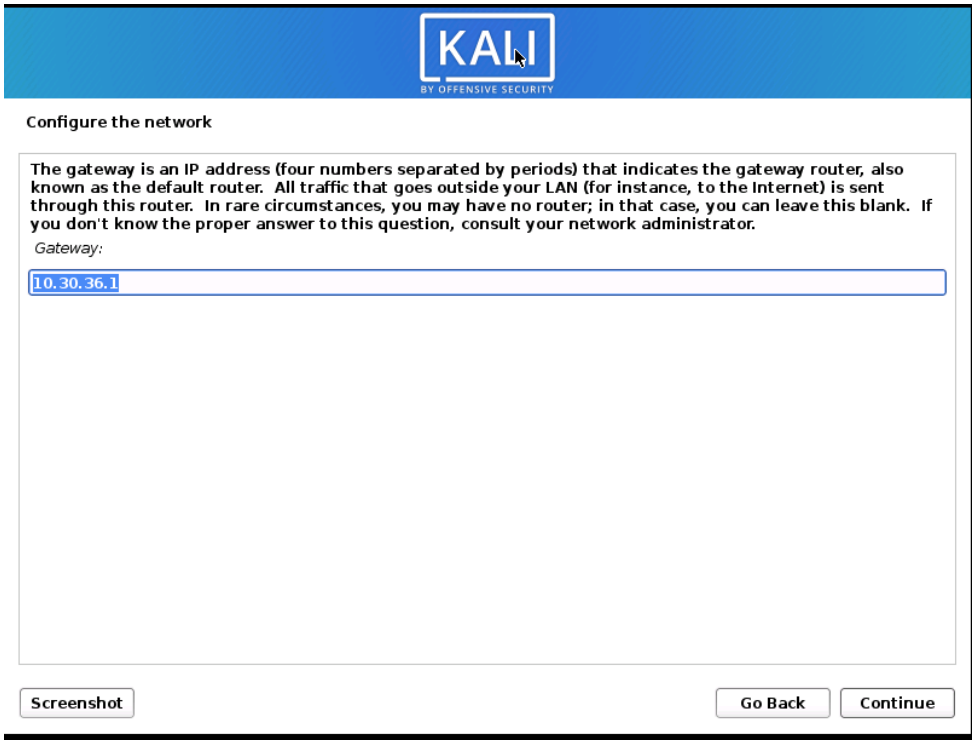
33. Select “Configure network manually”:



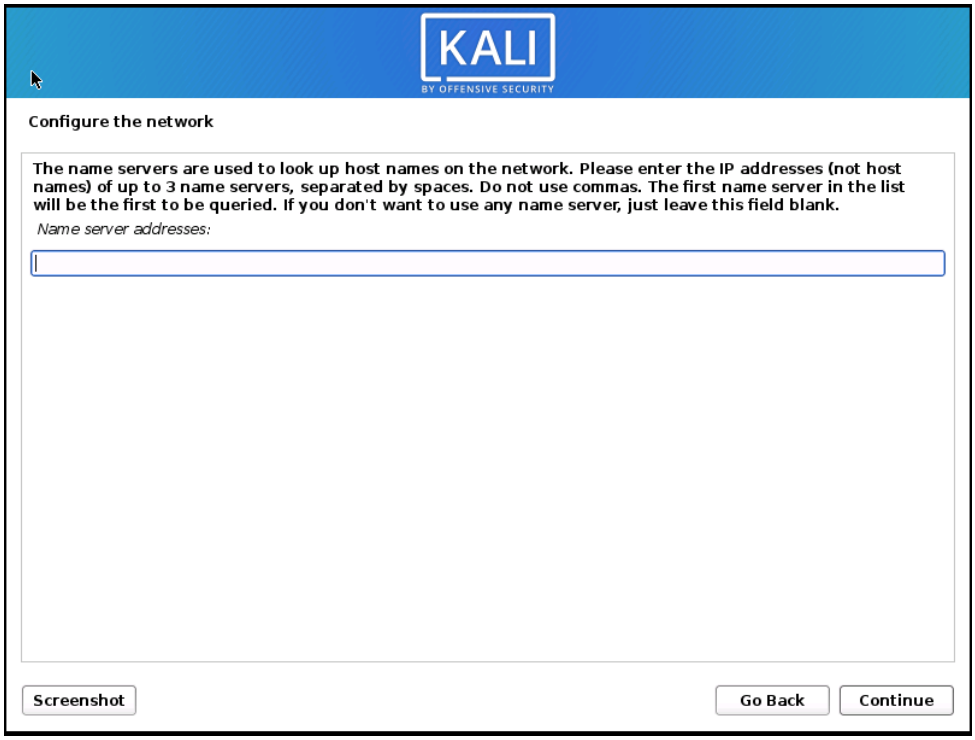
34. Enter the IP address for Laptop1:



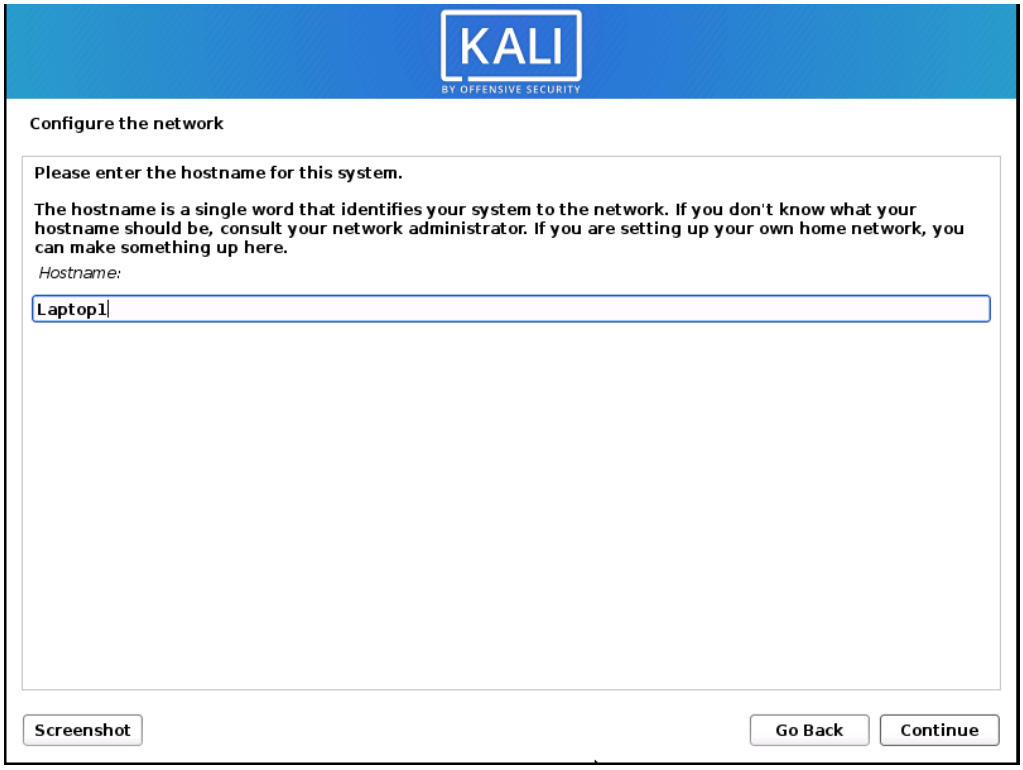
35. The default gateway will be automatically populated on the next page. Select Continue:



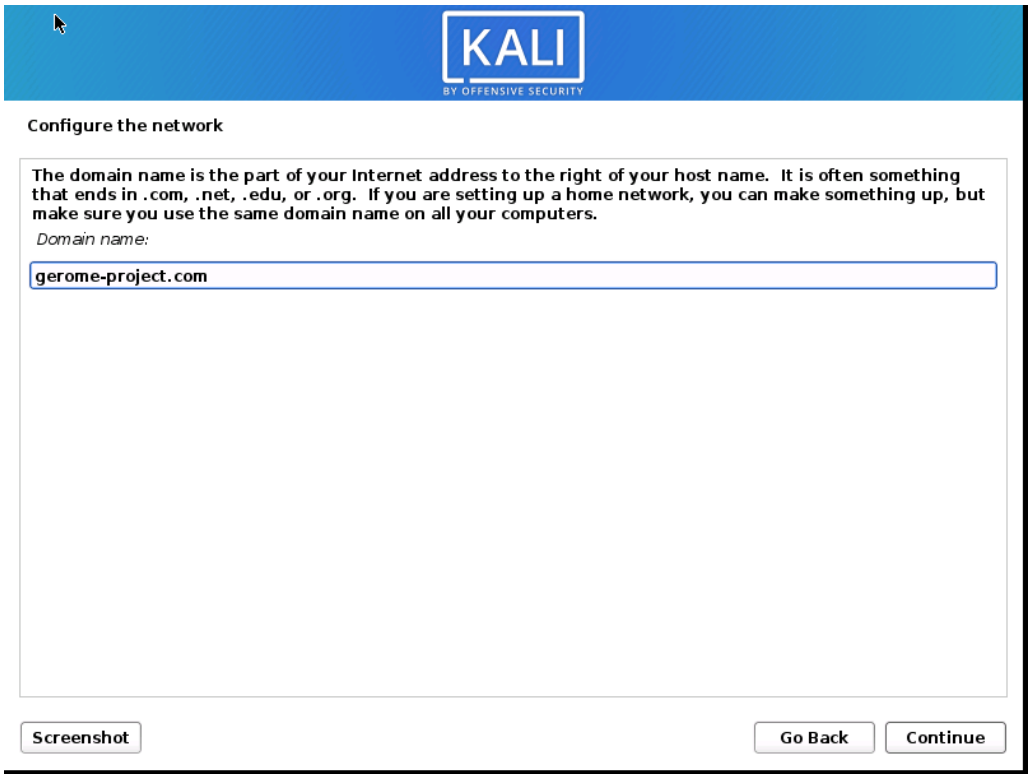
36. The next page asked for a DNS server but since the network doesn't have one leave the field blank:



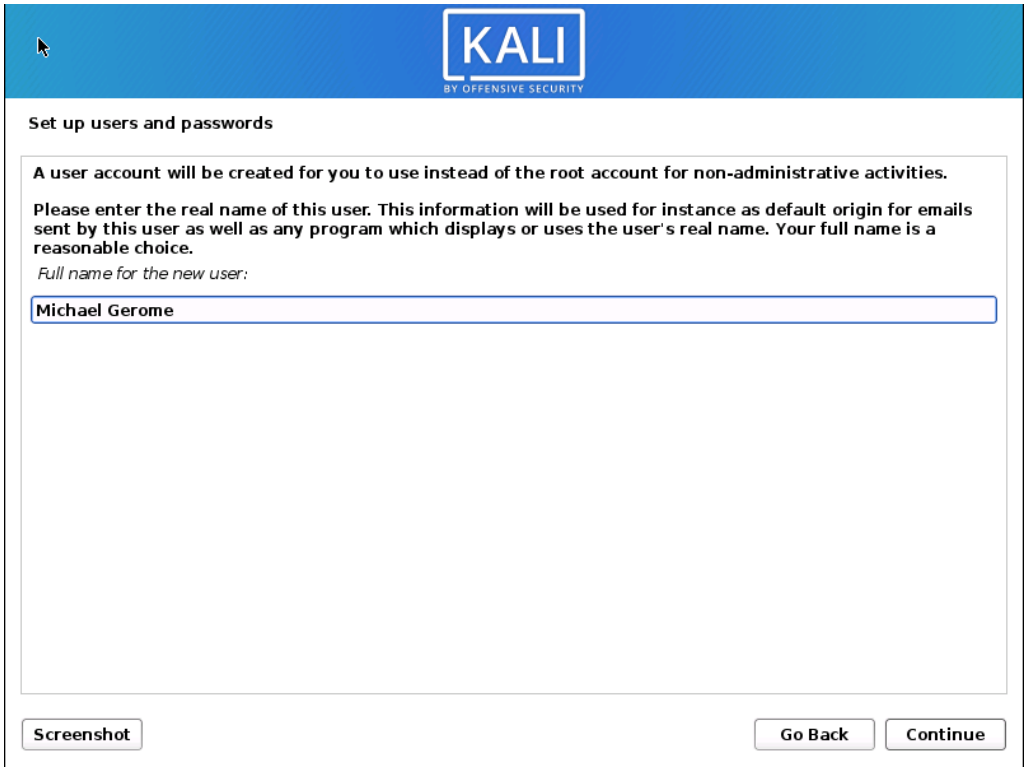
37. The system will then ask for a hostname, use Laptop1 as the hostname:



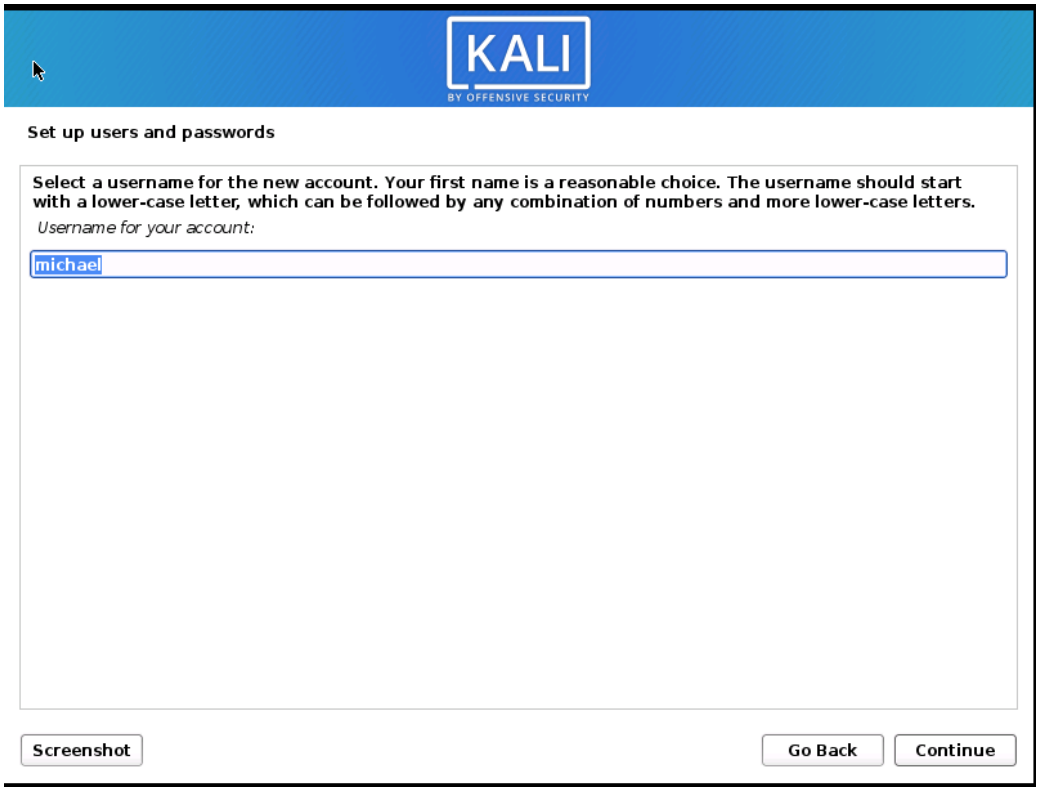
38. Enter the domain name gerome-project.com when prompted:



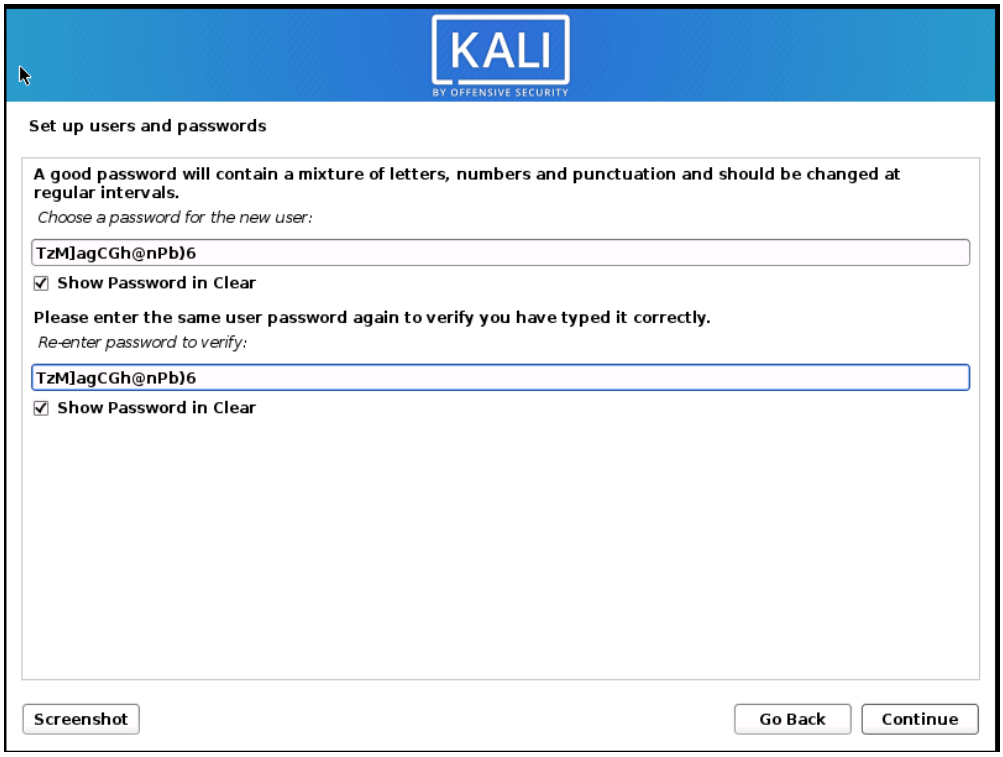
39. Enter a name for the user account:



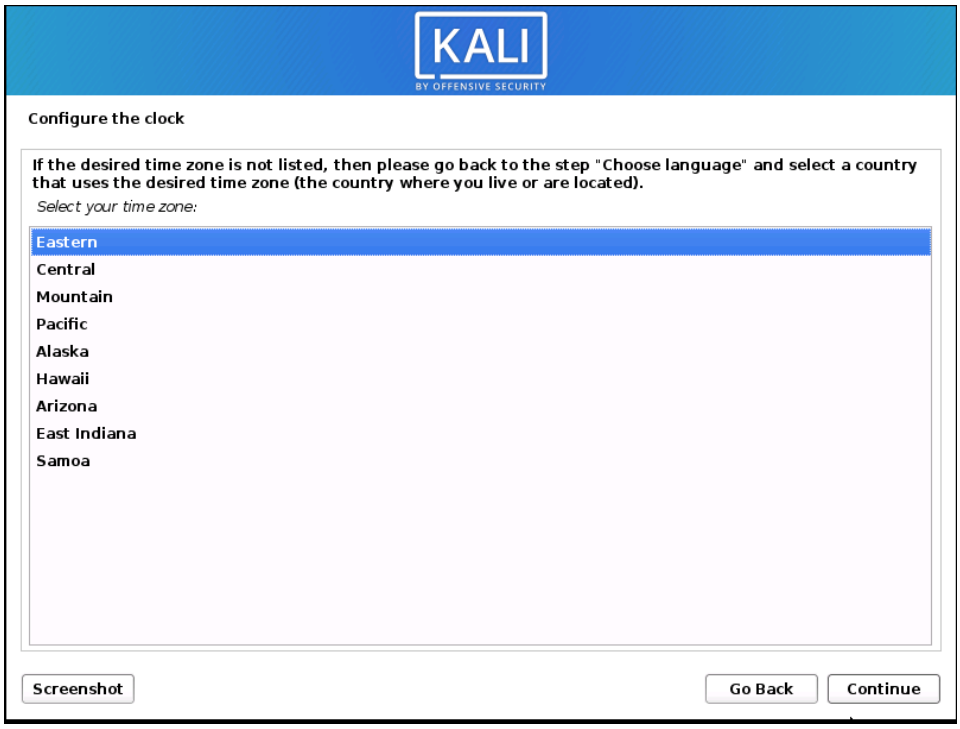
40. Keep the defualt username given for the account:



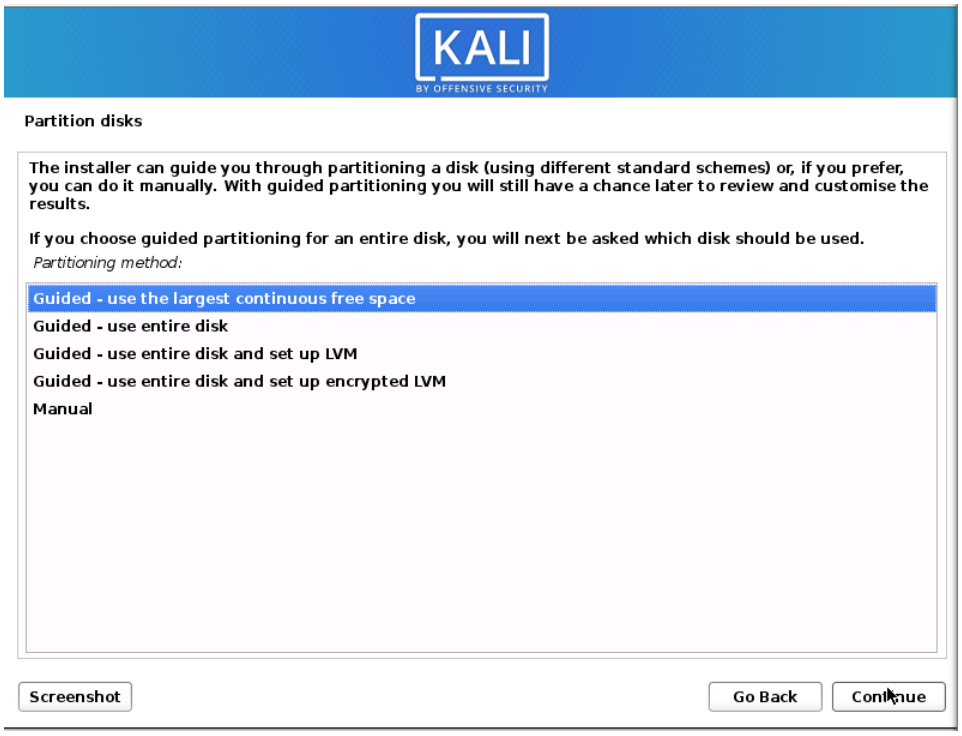
41. Enter a strong password for the device, for this project the password “TzM]agCGh@nPb)6” will be used:



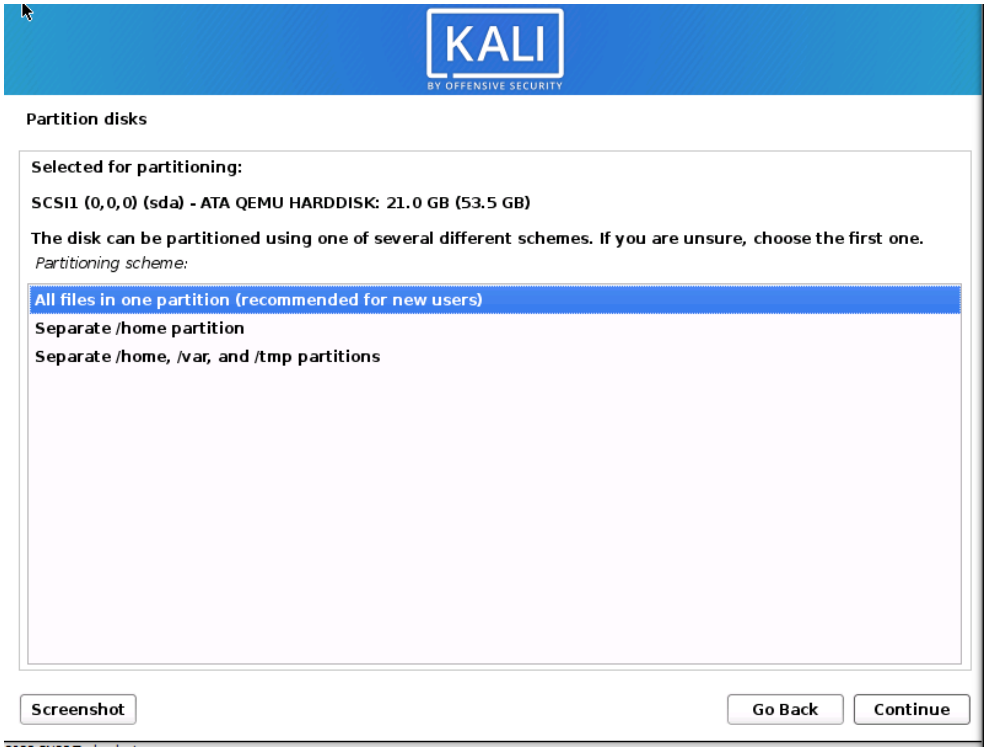
42. Select Eastern as the time zone:



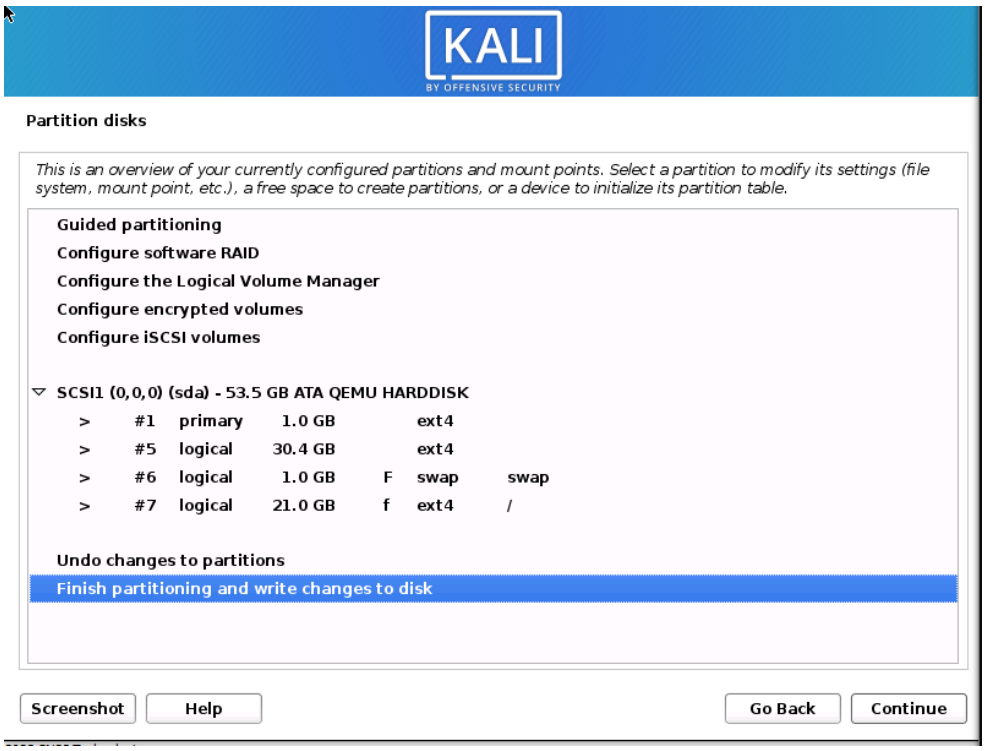
43. When asked how to partition the disk select the “Guided – use the largest continuous free space” option:



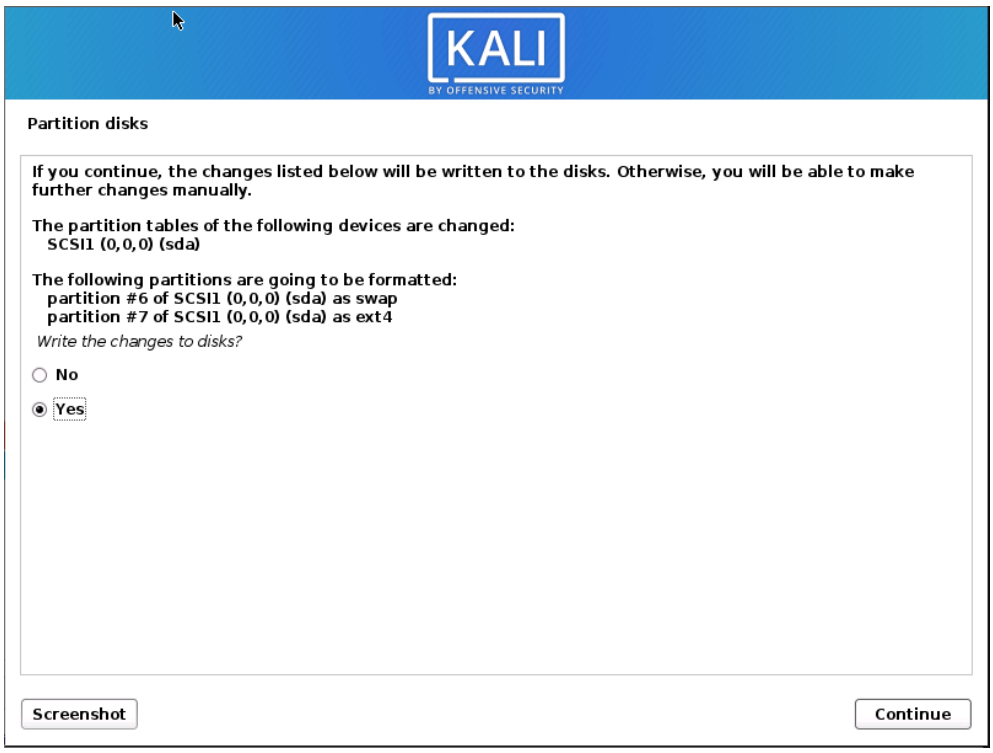
44. Select the “All files in one partition (recommended for new users)” option:



45. Select “Finish partitioning and write changes to disk”:

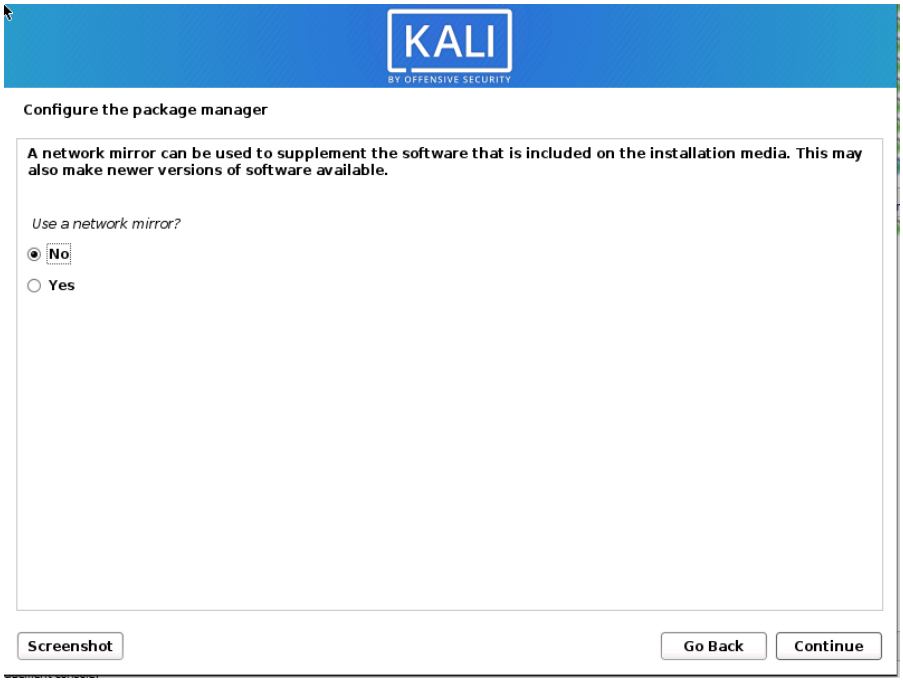


46. Select Yes to making changes to the disks:

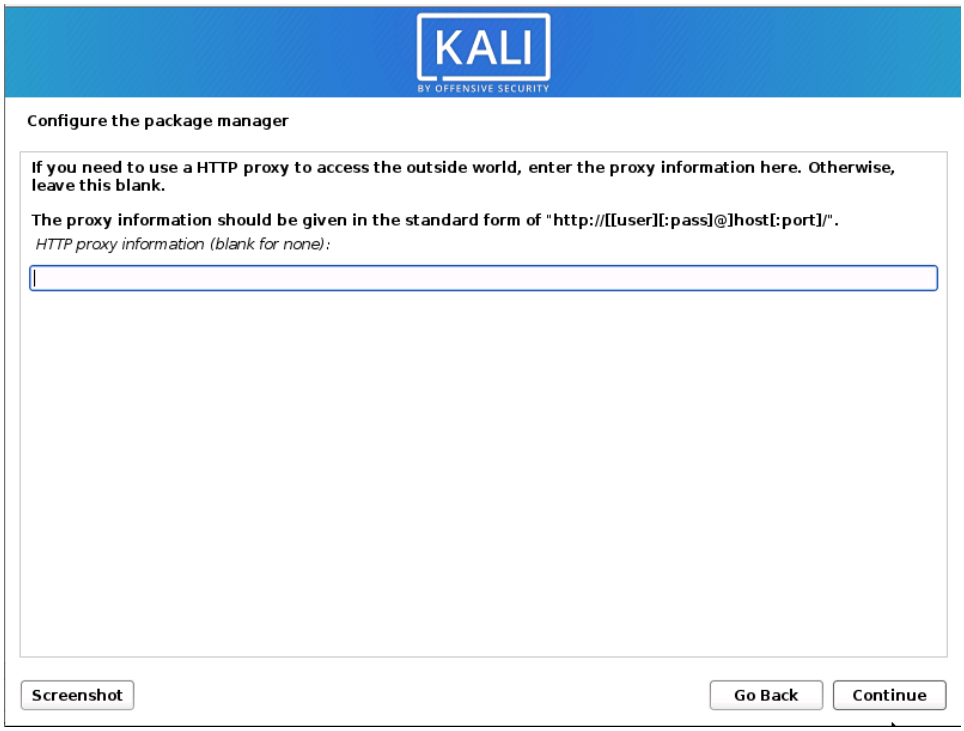


47. Now the machine will begin installing the system.

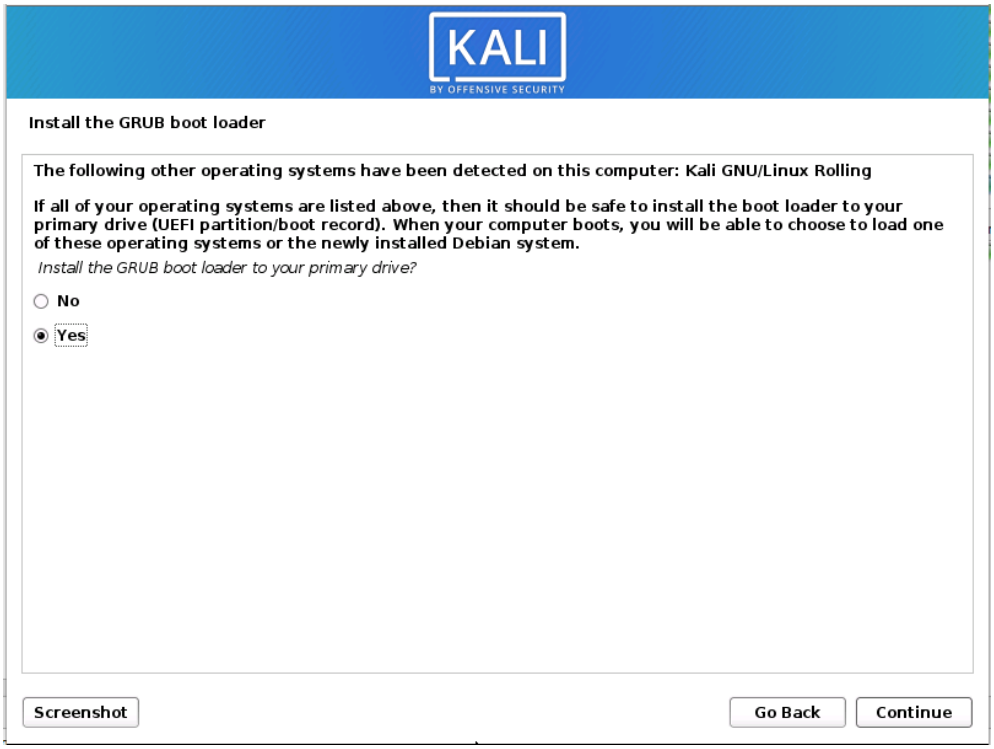
48. Select “No” to using a network mirror:



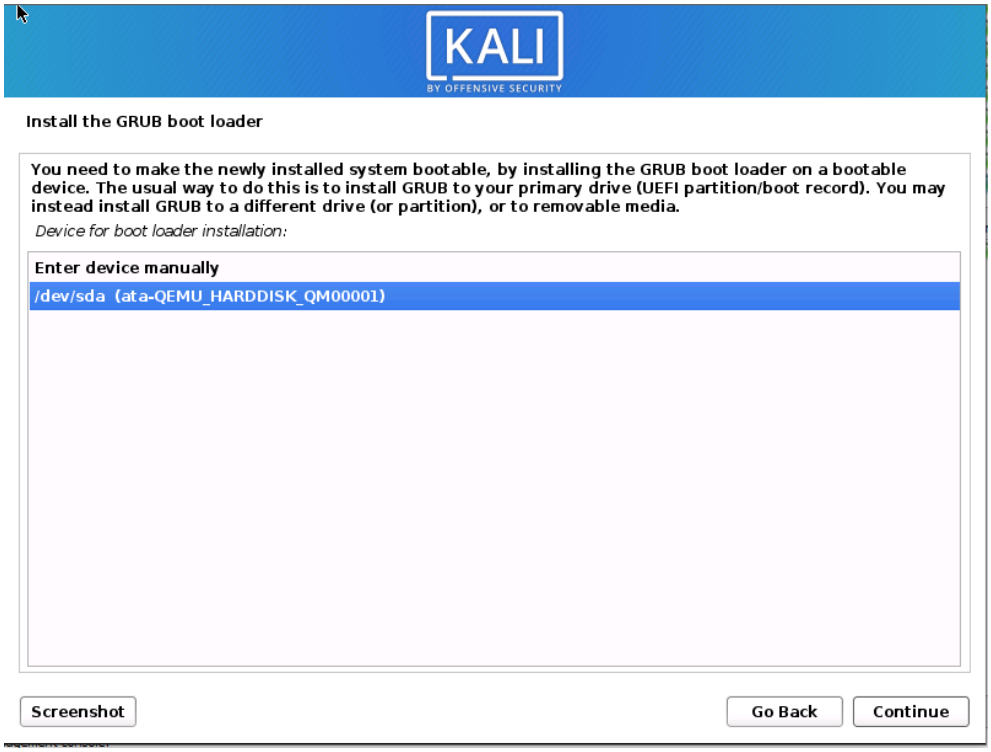
49. Leave the HTTP proxy information field blank:



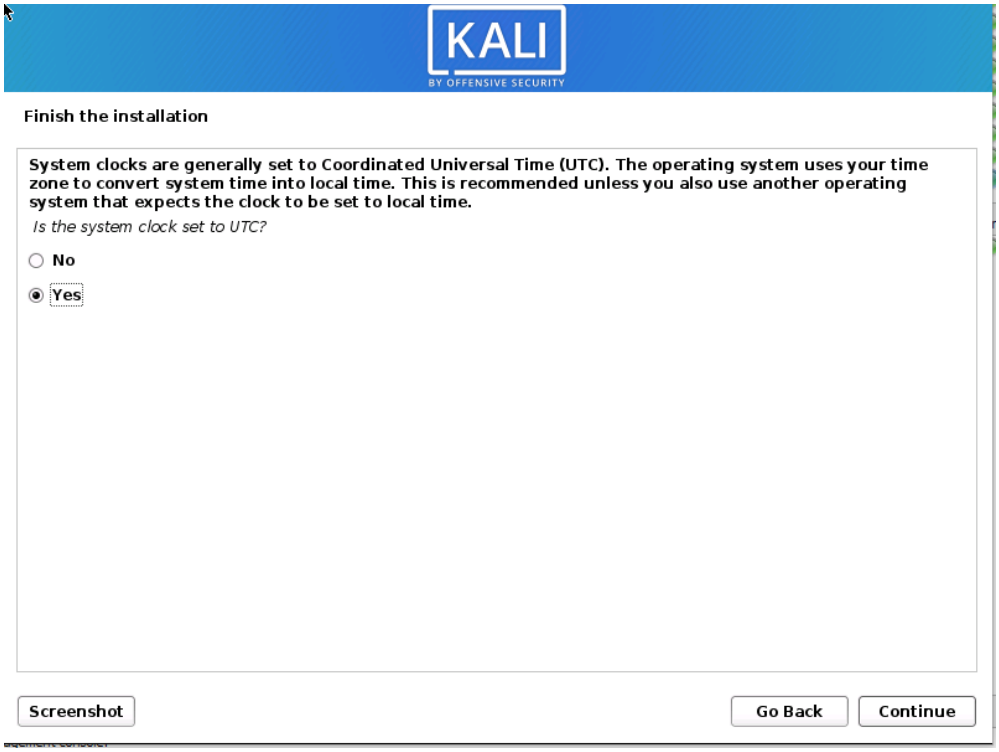
50. Install the GRUB boot loader to the primary drive:



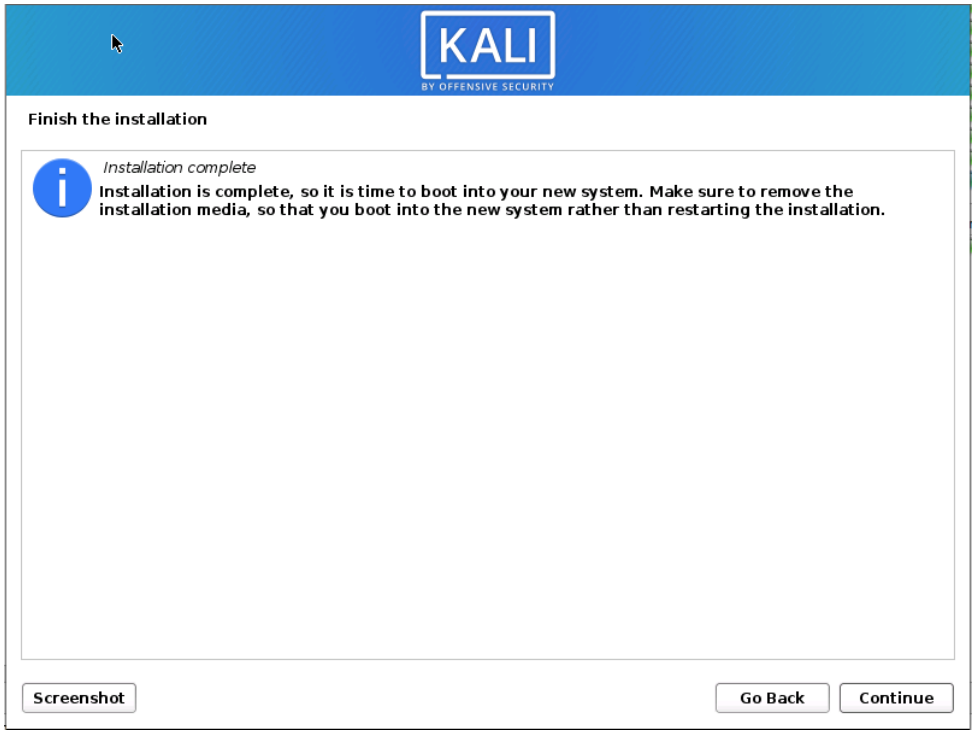
51. Select the /dev/sda disk as the location to install the GRUB boot loader:



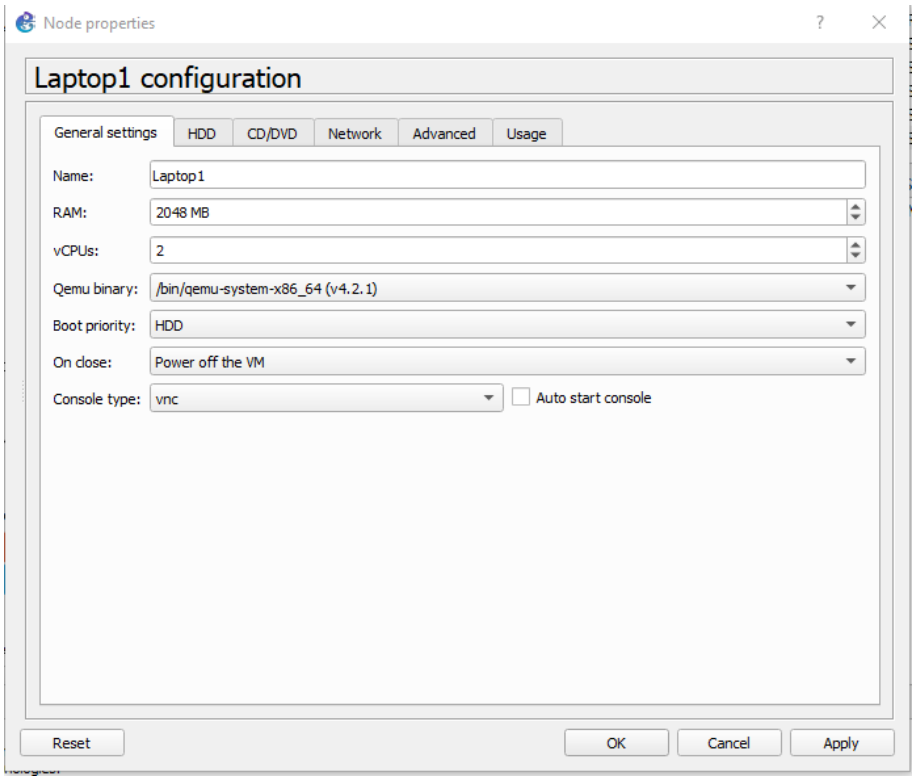
52. Select “Yes” for setting the clock to use Coordinated Universal Time (UTC):



53. Once the installation is complete select continue:



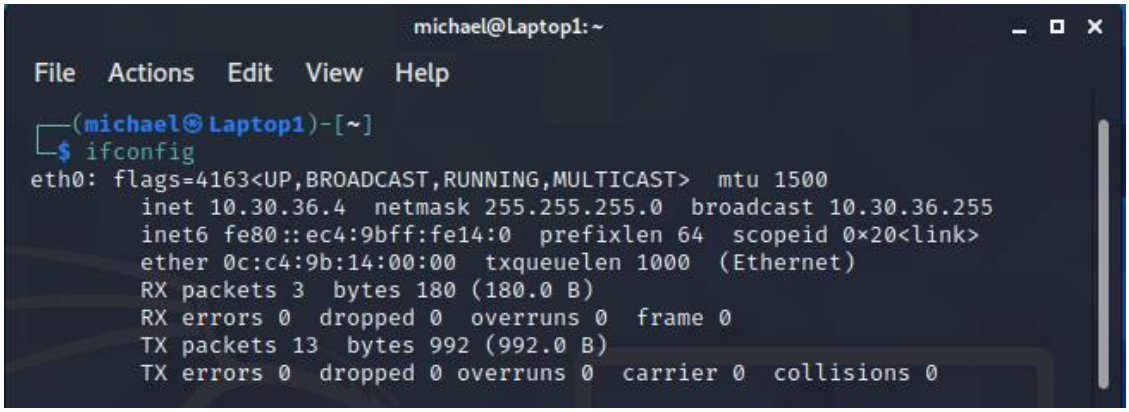
54. Once the process finishes and the boot menu reappears, shutdown the laptop and right-click on the icon and select “Configure”. Change the “Boot priority” option to HDD to have the laptop boot from the hard drive which is where the Linux OS was just installed.



55. Click “OK” and start the laptop.

56. Log into the user account created during the installation process.

57. Open the terminal and issue the “ifconfig” command to check the network adapter configuration:



Part 2: Initial Configuration

In this part of the configuration basic initial configuration will be performed on the routers and switches in the network.

1. First configure the hostname of the devices according to the addressing table by using the "hostname" command:

```
Router(config)#hostname Router1
Router1(config)#
```

2. Configure the clock so that it is displaying the correct time zone (eastern standard time):

```
Router1(config)#clock timezone EST -5
Router1(config)#
```

3. Secure user EXEC mode by setting strong password online console 0 and require login. Assign passwords according to the password table below:

Device	Console	Username	Password
Router1	User EXEC mode	NA	MBBreAR3me
	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	9wNLw2CDgR
	Local AAA	AAAadmin	tfgVZ0FK=Q
Router2	User EXEC mode	NA	MBBreAR3me
	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	9wNLw2CDgR
	Local AAA	AAAadmin	tfgVZ0FK=Q

Router3	User EXEC mode	NA	MBBreAR3me
	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	badpassword
	Local AAA	AAAadmin	tfgVZ0FK=Q
Switch1	User EXEC mode	NA	MBBreAR3me
	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	9wNLw2CDgR
Switch2	User EXEC mode	NA	MBBreAR3me
	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	9wNLw2CDgR
Switch3	User EXEC mode	NA	MBBreAR3me
	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	9wNLw2CDgR
Switch4	User EXEC mode	NA	MBBreAR3me
	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	9wNLw2CDgR
	User EXEC mode	NA	MBBreAR3me

Switch5	Privileged EXEC mode	NA	TdFzU8gXmn
	SSH	remoteadmin	9wNLw2CDgR

4. Secure user EXEC mode using the following commands:

```
Router1(config)#line console 0
Router1(config-line)#password MBBreAR3me
Router1(config-line)#login
Router1(config-line)#
```

5. Configure SSH on the device to enable remote management using the following commands (set the SSH password on Router 3 to “badpassword” for testing purposes):

```
Router1(config)#hostname Router1
Router1(config)#ip domain name gerome-project.com
Router1(config)#crypto key generate rsa
% You already have RSA keys defined named Router1.gerome-project.com.
% Do you really want to replace them? [yes/no]: yes
Choose the size of the key modulus in the range of 512 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [1024]:
*Mar 22 21:04:51.682: %CRYPTO_ENGINE-5-KEY_DELETED: A key named Router1.gerome-project.com has been removed from key storage
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

Router1(config)#
*Mar 22 21:04:55.200: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named Router1.gerome-project.com has been generated or imported by crypto-engine
Router1(config)#username
Router1(config)#username remoteadmin pr
Router1(config)#username remoteadmin privilege 15 se
Router1(config)#username remoteadmin privilege 15 se?
secret  serial-number

Router1(config)#username remoteadmin privilege 15 secr
Router1(config)#username remoteadmin privilege 15 secret 9wNLw2CDgR
Router1(config)#line vty 0 4
Router1(config-line)#transport input ssh
Router1(config-line)#login local
Router1(config-line)#exit
Router1(config)#
```

6. Secure privileged EXEC mode by setting a password on that console line:

```
Router1(config)#enable secret TdFzU8gXmn
```

7. Secure these passwords by using the password-encryption command and configure and minimum password length of ten characters:

```
Router1(config)#service password-encryption
Router1(config)#security pass
Router1(config)#security passwords min-
Router1(config)#security passwords min-length 10
```

8. Configure a legal notification to those logging in warning against unauthorized access to the machine and the repercussions for doing so:

```
Router1(config)#banner motd "Unauthorized access to this machine is prohibited$
```

9. Repeat these commands on the other routers and switches on the network making changes according to the addressing and password tables, as necessary.

Part 3: VLAN & Router-on-a-stick Configuration

1. To configure VLANs of switches use the following commands. Configure the five VLANs laid out in the proposal:

```
Switch1(config)#vlan 24
Switch1(config-vlan)#name Sales
Switch1(config-vlan)#exit
Switch1(config)#vlan 36
Switch1(config-vlan)#name IT
Switch1(config-vlan)#exit
Switch1(config)#vlan 48
Switch1(config-vlan)#name HR
Switch1(config-vlan)#exit
Switch1(config)#vlan 75
Switch1(config-vlan)#name Unused-Interfaces
Switch1(config-vlan)#exit
Switch1(config)#vlan 99
Switch1(config-vlan)#name Management
Switch1(config-vlan)#exit
Switch1(config)#
```

2. Assign the interfaces connected to end devices to access mode and to VLANs:

```
Switch1(config)#int gigabitEthernet0/2
Switch1(config-if)#switch
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 48
Switch1(config-if)#exit
Switch1(config)#int gig
Switch1(config)#int gigabitEthernet0/3
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 48
Switch1(config-if)#exit
```

3. Configure trunk ports on switches that are labeled as trunk links on the topology.

```
Switch1(config)#int gi
Switch1(config)#int gigabitEthernet 0/0
Switch1(config-if)#switchport trunk enc
Switch1(config-if)#switchport trunk encapsulation d
Switch1(config-if)#switchport trunk encapsulation dot1q
Switch1(config-if)#swit
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#
```

4. On Router1 configure the subinterfaces of Gi1 using the following commands:

```
Router1(config)#int Gi1.48
Router1(config-subif)#encapsulation dot1q 48
Router1(config-subif)#ip address 192.168.48.1 255.255.255.0
Router1(config-subif)#exit
Router1(config)#int Gi1.99
Router1(config-subif)#encapsulation dot1q 99
Router1(config-subif)#ip address 192.168.99.1 255.255.255.0
Router1(config-subif)#exit
Router1(config)#int Gi1
Router1(config-if)#no shutdown
Router1(config-if)#
*Mar 22 23:28:57.359: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state to up
*Mar 22 23:28:58.359: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1, changed state to up
Router1(config-if)#exit
Router1(config)#exit
Router1#show ip i
*Mar 22 23:29:17.620: %SYS-5-CONFIG_I: Configured from console by consolent br
Router1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  up                    up
GigabitEthernet1.48    192.168.48.1    YES manual up                    up
GigabitEthernet1.99    192.168.99.1    YES manual up                    up
GigabitEthernet2       10.10.1.1       YES NVRAM  up                    up
GigabitEthernet3       10.10.3.1       YES NVRAM  up                    up
GigabitEthernet4       unassigned      YES NVRAM  administratively down down
Router1#
```

As shown with the show command at the bottom the subinterfaces have been configured.

5. At this point VLAN encapsulation should be done on Router2 and Router3 on the Gi1 interface. Use the following commands on the respective routers:

```
Router2(config)#int Gi1
Router2(config-if)#no ip add
Router2(config-if)#int Gi1.24
Router2(config-subif)#encap
Router2(config-subif)#encapsulation d
Router2(config-subif)#encapsulation dot1Q 24
Router2(config-subif)#ip addr
Router2(config-subif)#ip address 172.20.24.1 255.255.255.0
Router2(config-subif)#no shut
Router2(config-subif)#end
```

```
Router3(config)#int Gi1
Router3(config-if)#no ip address
Router3(config-if)#int Gi1.36
Router3(config-subif)#enca
Router3(config-subif)#encapsulation dot1q 36
Router3(config-subif)#encapsulation dot1q 36 n
Router3(config-subif)#encapsulation dot1q 36 native ?
  <cr>  <cr>

Router3(config-subif)#encapsulation dot1q 36 native
Router3(config-subif)#ip address 10.30.36.1 255.255.255.0
Router3(config-subif)#no shut
```

Part 4: STP Configuration

1. In order to prevent network loops between Switch1, Switch2, and Switch3 spanning tree protocol (STP) will be configured on these switches. Switch2 will be used as the root bridge for the protocol. On Switch2 issue the following commands to configure the switch:

```
Switch2(config)#spanning-tree vlan 24,36,48,99
Switch2(config)#spanning-tree vlan 24,36,48,99 ?
  forward-time  Set the forward delay for the spanning tree
  hello-time    Set the hello interval for the spanning tree
  max-age       Set the max age interval for the spanning tree
  priority      Set the bridge priority for the spanning tree
  root          Configure switch as root
  <cr>

Switch2(config)#spanning-tree vlan 24,36,48,99 root primary
Switch2(config)#spanning-tree mode pvst
Switch2(config)#
```

   The first command enables STP on the listed VLANs, the second command makes Switch2 the primary root switch, and the thirs command set the spanning tree mode to PVST.

2. Now perform the following commands on Switch1 and Switch3 which will be configured as secondary switches:

```
Switch1(config)#spanning-tree vlan 24,36,48,99
Switch1(config)#spanning-tree vlan 24,36,48,99 root ?
  primary    Configure this switch as primary root for this spanning tree
  secondary  Configure switch as secondary root

Switch1(config)#spanning-tree vlan 24,36,48,99 root se
Switch1(config)#spanning-tree vlan 24,36,48,99 root secondary
Switch1(config)#sp
Switch1(config)#spanning-tree m
Switch1(config)#spanning-tree mode pvst
```

3. On the interfaces which are connected to end devices on the switch issue the following commands to help protect the network against STP attacks:

```
Switch1(config)#int range g0/2-3
Switch1(config-if-range)#spa
Switch1(config-if-range)#spanning-tree ?
  bpdufilter     Don't send or receive BPDUs on this interface
  bpduguard      Don't accept BPDUs on this interface
  cost           Change an interface's spanning tree port path cost
  guard          Change an interface's spanning tree guard mode
  link-type      Specify a link type for spanning tree protocol use
  mst            Multiple spanning tree
  port-priority  Change an interface's spanning tree port priority
  portfast       Portfast options for the interface
  vlan           VLAN Switch Spanning Tree

Switch1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast will be configured in 2 interfaces due to the range command
 but will only have effect when the interfaces are in a non-trunking mode.
Switch1(config-if-range)#spanning-tree bpduguard enable
```

4. To verify that STP was configured correctly use the “show spanning-tree” command to view the configuration on the switches:

```
Switch2#show spann
Switch2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0c0c.d487.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0c0c.d487.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
```

Switch2 has correctly been labeled the root bridge.

```
VLAN0075
  Spanning tree enabled protocol ieee
  Root ID    Priority    32843
             Address     0c0c.d487.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32843  (priority 32768 sys-id-ext 75)
             Address     0c0c.d487.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    P2p
Gi0/1               Desg FWD 4         128.2    P2p
Gi0/2               Desg FWD 4         128.3    P2p



VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    24675
             Address     0c0c.d487.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24675  (priority 24576 sys-id-ext 99)
             Address     0c0c.d487.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    P2p
Gi0/1               Desg FWD 4         128.2    P2p
Gi0/2               Desg FWD 4         128.3    P2p
```

The four VLANs listed in the commands also appear in the output of the show command.

Part 5: EIGRP Configuration

The EIGRP routing protocol will be configured on the three routers to allow the three sections of the network to communicate with each other. Use the following commands on each of the three routers:

1. Router 1:

```
Router1(config)#router eigrp 50
Router1(config-router)#network 192.168.48.0 0.0.0.255
Router1(config-router)#network 192.168.99.0 0.0.0.255
Router1(config-router)#network 10.10.1.0 0.0.0.3
Router1(config-router)#network 10.10.3.0 0.0.0.3
```

2. Router 2:

```
Router2(config)#router eigrp 50
Router2(config-router)#network 172.20.24.0 0.0.0.255
Router2(config-router)#network 10.10.1.0 0.0.0.3
Router2(config-router)#ne
*Mar 23 17:56:40.696: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: Neighbor 10.10.1.1 (GigabitEthernet2) is up: new adjacen
Router2(config-router)#network 10.10.2.0 0.0.0.3
Router2(config-router)#
```

3. Router 3:

```
Router3(config)#router eigrp 50
Router3(config-router)#network 10.30.36.0 0.0.0.255
Router3(config-router)#network 10.10.3.0 0.0.0.3
Router3(config-router)#
*Mar 23 17:58:33.446: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: Neighbor 10.10.3.1 (GigabitEthernet2) is up: new adjacency
Router3(config-router)#network 10.10.2.0 0.0.0.3
Router3(config-router)#
*Mar 23 17:58:53.276: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: Neighbor 10.10.2.1 (GigabitEthernet3) is up: new adjacency
Router3(config-router)#
```

4. As the configuration was performed on each router, log messages are sent stating new adjacencies have formed with the other routers. To verify the configuration of the routing protocol use the “show ip route” command

```
Router1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C        10.10.1.0/30 is directly connected, GigabitEthernet2
L        10.10.1.1/32 is directly connected, GigabitEthernet2
D        10.10.2.0/30 [90/3072] via 10.10.3.2, 00:02:55, GigabitEthernet3
                      [90/3072] via 10.10.1.2, 00:02:55, GigabitEthernet2
C        10.10.3.0/30 is directly connected, GigabitEthernet3
L        10.10.3.1/32 is directly connected, GigabitEthernet3
D        10.30.36.0/24 [90/3072] via 10.10.3.2, 00:02:48, GigabitEthernet3
      172.20.0.0/24 is subnetted, 1 subnets
D        172.20.24.0 [90/3072] via 10.10.1.2, 00:02:53, GigabitEthernet2
      192.168.48.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.48.0/24 is directly connected, GigabitEthernet1.48
L        192.168.48.1/32 is directly connected, GigabitEthernet1.48
      192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.99.0/24 is directly connected, GigabitEthernet1.99
L        192.168.99.1/32 is directly connected, GigabitEthernet1.99
Router1#
```

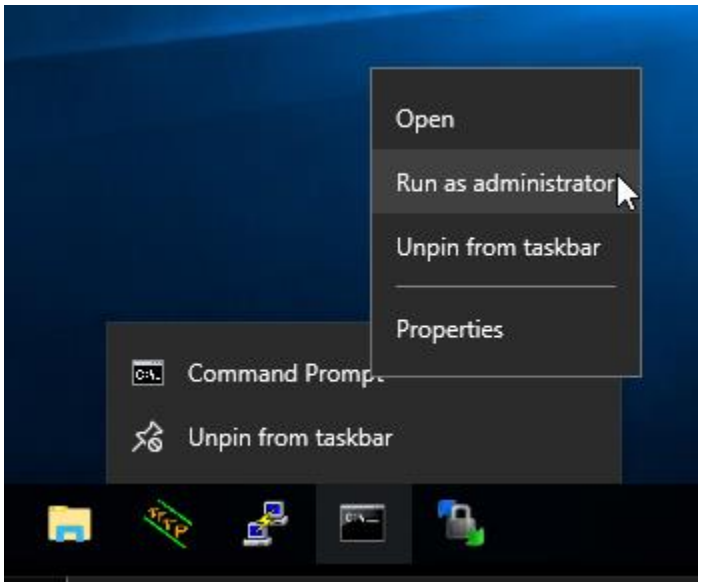
```
Router2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C        10.10.1.0/30 is directly connected, GigabitEthernet2
L        10.10.1.2/32 is directly connected, GigabitEthernet2
C        10.10.2.0/30 is directly connected, GigabitEthernet3
L        10.10.2.1/32 is directly connected, GigabitEthernet3
D        10.10.3.0/30 [90/3072] via 10.10.2.2, 00:02:55, GigabitEthernet3
                      [90/3072] via 10.10.1.1, 00:02:55, GigabitEthernet2
D        10.30.36.0/24 [90/3072] via 10.10.2.2, 00:02:55, GigabitEthernet3
      172.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.20.24.0/24 is directly connected, GigabitEthernet1
L        172.20.24.1/32 is directly connected, GigabitEthernet1
D     192.168.48.0/24 [90/3072] via 10.10.1.1, 00:02:55, GigabitEthernet2
D     192.168.99.0/24 [90/3072] via 10.10.1.1, 00:02:55, GigabitEthernet2
Router2#
```

```
Router3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
D        10.10.1.0/30 [90/3072] via 10.10.3.1, 00:03:04, GigabitEthernet2
                      [90/3072] via 10.10.2.1, 00:03:04, GigabitEthernet3
C        10.10.2.0/30 is directly connected, GigabitEthernet3
L        10.10.2.2/32 is directly connected, GigabitEthernet3
C        10.10.3.0/30 is directly connected, GigabitEthernet2
L        10.10.3.2/32 is directly connected, GigabitEthernet2
C        10.30.36.0/24 is directly connected, GigabitEthernet1
L        10.30.36.1/32 is directly connected, GigabitEthernet1
      172.20.0.0/24 is subnetted, 1 subnets
D        172.20.24.0 [90/3072] via 10.10.2.1, 00:03:04, GigabitEthernet3
D     192.168.48.0/24 [90/3072] via 10.10.3.1, 00:03:04, GigabitEthernet2
D     192.168.99.0/24 [90/3072] via 10.10.3.1, 00:03:04, GigabitEthernet2
Router3#
```

These screenshots show the routing table of each of the routers. The routes labeled with the letter D are the routes that EIGRP received from the adjacent routers. Each router now has a route to the other subnets on the network.

The Windows 10 computers by default do not accept ping attempts so that will need to be enabled with the following steps:

1. On each Windows machine open the command prompt as an administrator:



2. Enter the following command to create a firewall rule to allow ICMP echo requests from other devices:

```
C:\Windows\system32>netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=
in action=allow
Ok.


C:\Windows\system32>
```

3. Test connectivity by sending pings from different end devices to other devices. The screenshots below show that devices from each subnet are able to get responses from the target of their pings. Once all devices are able to ping each other, save the configuration of all routers and switches then move on to the next section:

QEMU (PC1) - TightVNC Viewer

Administrator: Command Prompt

```
Pinging 192.168.99.5 with 32 bytes of data:
Reply from 192.168.99.5: bytes=32 time=18ms TTL=127
Reply from 192.168.99.5: bytes=32 time=17ms TTL=127
Reply from 192.168.99.5: bytes=32 time=17ms TTL=127
Reply from 192.168.99.5: bytes=32 time=24ms TTL=127

Ping statistics for 192.168.99.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 24ms, Average = 19ms

C:\Windows\system32>ping 172.20.24.4

Pinging 172.20.24.4 with 32 bytes of data:
Reply from 172.20.24.4: bytes=32 time=17ms TTL=126
Reply from 172.20.24.4: bytes=32 time=13ms TTL=126
Reply from 172.20.24.4: bytes=32 time=11ms TTL=126
Reply from 172.20.24.4: bytes=32 time=12ms TTL=126

Ping statistics for 172.20.24.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 17ms, Average = 13ms

C:\Windows\system32>ping 10.30.36.3

Pinging 10.30.36.3 with 32 bytes of data:
Reply from 10.30.36.3: bytes=32 time=17ms TTL=126
Reply from 10.30.36.3: bytes=32 time=15ms TTL=126
Reply from 10.30.36.3: bytes=32 time=14ms TTL=126
Reply from 10.30.36.3: bytes=32 time=18ms TTL=126

Ping statistics for 10.30.36.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 18ms, Average = 16ms
```

QEMU (PC3) - TightVNC Viewer

Administrator: Command Prompt

```
C:\Windows\system32>ping 192.168.48.5

Pinging 192.168.48.5 with 32 bytes of data:
Reply from 192.168.48.5: bytes=32 time=30ms TTL=127
Reply from 192.168.48.5: bytes=32 time=18ms TTL=127
Reply from 192.168.48.5: bytes=32 time=15ms TTL=127
Reply from 192.168.48.5: bytes=32 time=13ms TTL=127

Ping statistics for 192.168.48.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 30ms, Average = 19ms

C:\Windows\system32>ping 172.20.24.5

Pinging 172.20.24.5 with 32 bytes of data:
Reply from 172.20.24.5: bytes=32 time=15ms TTL=126
Reply from 172.20.24.5: bytes=32 time=12ms TTL=126
Reply from 172.20.24.5: bytes=32 time=9ms TTL=126
Reply from 172.20.24.5: bytes=32 time=8ms TTL=126

Ping statistics for 172.20.24.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 15ms, Average = 11ms

C:\Windows\system32>ping 10.30.36.4

Pinging 10.30.36.4 with 32 bytes of data:
Reply from 10.30.36.4: bytes=32 time=11ms TTL=62
Reply from 10.30.36.4: bytes=32 time=15ms TTL=62
Reply from 10.30.36.4: bytes=32 time=11ms TTL=62
Reply from 10.30.36.4: bytes=32 time=13ms TTL=62

Ping statistics for 10.30.36.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 15ms, Average = 12ms
```

QEMU (PC5) - TightVNC Viewer

Administrator: Command Prompt

```
C:\Windows\system32>ping 192.168.48.4

Pinging 192.168.48.4 with 32 bytes of data:
Reply from 192.168.48.4: bytes=32 time=16ms TTL=126
Reply from 192.168.48.4: bytes=32 time=17ms TTL=126
Reply from 192.168.48.4: bytes=32 time=12ms TTL=126
Reply from 192.168.48.4: bytes=32 time=15ms TTL=126

Ping statistics for 192.168.48.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 17ms, Average = 15ms

C:\Windows\system32>ping 192.168.99.4

Pinging 192.168.99.4 with 32 bytes of data:
Reply from 192.168.99.4: bytes=32 time=24ms TTL=126
Reply from 192.168.99.4: bytes=32 time=10ms TTL=126
Reply from 192.168.99.4: bytes=32 time=14ms TTL=126
Reply from 192.168.99.4: bytes=32 time=17ms TTL=126

Ping statistics for 192.168.99.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 24ms, Average = 16ms

C:\Windows\system32>ping 10.30.36.4

Pinging 10.30.36.4 with 32 bytes of data:
Reply from 10.30.36.4: bytes=32 time=9ms TTL=62
Reply from 10.30.36.4: bytes=32 time=6ms TTL=62
Reply from 10.30.36.4: bytes=32 time=12ms TTL=62
Reply from 10.30.36.4: bytes=32 time=9ms TTL=62

Ping statistics for 10.30.36.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 12ms, Average = 9ms
```

```
┌──(michael㉿Laptop1)-[~]
└─$ ping 192.168.48.5
PING 192.168.48.5 (192.168.48.5) 56(84) bytes of data.
64 bytes from 192.168.48.5: icmp_seq=1 ttl=126 time=15.7 ms
64 bytes from 192.168.48.5: icmp_seq=2 ttl=126 time=11.6 ms
64 bytes from 192.168.48.5: icmp_seq=3 ttl=126 time=18.4 ms
64 bytes from 192.168.48.5: icmp_seq=4 ttl=126 time=15.1 ms
64 bytes from 192.168.48.5: icmp_seq=5 ttl=126 time=8.85 ms
^C
--- 192.168.48.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 8.849/13.937/18.414/3.346 ms

┌──(michael㉿Laptop1)-[~]
└─$ ping 192.168.99.4
PING 192.168.99.4 (192.168.99.4) 56(84) bytes of data.
64 bytes from 192.168.99.4: icmp_seq=1 ttl=126 time=13.4 ms
64 bytes from 192.168.99.4: icmp_seq=2 ttl=126 time=17.5 ms
64 bytes from 192.168.99.4: icmp_seq=3 ttl=126 time=18.0 ms
^C
--- 192.168.99.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 13.350/16.299/18.005/2.093 ms

┌──(michael㉿Laptop1)-[~]
└─$ ping 172.20.24.3
PING 172.20.24.3 (172.20.24.3) 56(84) bytes of data.
64 bytes from 172.20.24.3: icmp_seq=1 ttl=126 time=9.01 ms
64 bytes from 172.20.24.3: icmp_seq=2 ttl=126 time=7.44 ms
64 bytes from 172.20.24.3: icmp_seq=3 ttl=126 time=6.13 ms
^C
--- 172.20.24.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.132/7.526/9.009/1.176 ms
```

Part 6: Router and Switch Security Configuration

This section involves using commands to help increase the security of the routers and switches in the network. For layer two security on the switches, the unused ports will be placed in a separate vlan and shutdown, the trunking ports will have autotrunking disabled, and the port-security command will be used to harden the device. The routers will be configured with Denial-of-Service (DoS) attack protection, IOS image resilience, and local Authentication, Authorization and Accounting (AAA) on all routers.

1. First open the console on each switch and enter priviledged EXEC mode. Enter the "show ip int brief" command and view the results. Now enter global configuration mode and move to the interfaces which are not in use. Assign these interfaces to VLAN 75 and use the shutdown command on them. Perform these commands on each of the switches.

```
Switch1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Vlan1                  192.168.48.2    YES NVRAM  up                    up
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#int range Gi1/0-3,Gi2/0-3,Gi3/0-3
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 75
Switch1(config-if-range)#shutdown
Switch1(config-if-range)#
*Mar 25 03:04:03.923: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively down
*Mar 25 03:04:03.987: %LINK-5-CHANGED: Interface GigabitEthernet1/1, changed state to administratively down
*Mar 25 03:04:04.048: %LINK-5-CHANGED: Interface GigabitEthernet1/2, changed state to administratively down
*Mar 25 03:04:04.088: %LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to administratively down
*Mar 25 03:04:04.181: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Mar 25 03:04:04.236: %LINK-5-CHANGED: Interface GigabitEthernet2/1, changed state to administratively down
*Mar 25 03:04:04.277: %LINK-5-CHANGED: Interface GigabitEthernet2/2, changed state to administratively down
*Mar 25 03:04:04.311: %LINK-5-CHANGED: Interface GigabitEthernet2/3, changed state to administratively down
*Mar 25 03:04:04.345: %LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to administratively down
*Mar 25 03:04:04.395: %LINK-5-CHANGED: Interface GigabitEthernet3/1, changed state to administratively down
*Mar 25 03:04:04.442: %LINK-5-CHANGED: Interface GigabitEthernet3/2, changed state to administratively down
*Mar 25 03:04:04.478: %LINK-5-CHANGED: Interface GigabitEthernet3/3, changed state to administratively down
Switch1(config-if-range)#
```

2. Next on all interfaces connected to links labeled trunk on the topology use the following command to disable automatic DTP trunking neogotiations:

```
Switch1(config)#int range Gi0/0-1
Switch1(config-if-range)#switch
Switch1(config-if-range)#switchport none
Switch1(config-if-range)#switchport nonegotiate
Switch1(config-if-range)#
```

3. The following commands will enable port-security options on the switch. This section will configure MAC address rules to limit one MAC address per interface and restrict the interface if additional MAC addresses are attempting to assign themselves. Issue the following commands on Switch4 and Switch5 on interfaces connected to end devices:

```
Switch5(config)#int range Gi0/1-3
Switch5(config-if-range)#switchport port
Switch5(config-if-range)#switchport port-security mac
Switch5(config-if-range)#switchport port-security mac-address sticky
Switch5(config-if-range)#switchport port-security max
Switch5(config-if-range)#switchport port-security maximum 1
Switch5(config-if-range)#switchport port-security violation restrict
Switch5(config-if-range)#
```

4. Next open the router console on the three routers and issue the following command. This command will configure the router to tag log messages with timestamps with the correct time:

```
Router1(config)#service timestamps log datetime localtime year
```

5. In order to prevent a DoS attack the routers need to be configured to limit login attempts onto the device. Issue the following commands on each router to limit login attempts to five failed attempts in 60 seconds. Also configure the router to log all successful and failed login attempts. These logs can be seen with the “show login” command.

```
Router1(config)#login block-for 120 attempts 5 within 60
Router1(config)#login delay 5
Router1(config)#login on-success log
Router1(config)#login on-failure log
Router1(config)#
```

6. Next local AAA will be configured on each switch to make log-ons more secure. Follow the following steps to configure AAA on the device:

```
Router1(config)#username AAAadmin algorithm-type scrypt secret tfgVZ0FK=Q
Router1(config)#aaa new-model
Router1(config)#aaa authentication login default local-case enable
Router1(config)#aaa authentication login AAAlogin local-case
Router1(config)#aaa local authentication attempts max-fail 5
Router1(config)#line vty
% Incomplete command.

Router1(config)#line vty 0 4
Router1(config-line)#login authentication AAAlogin
Router1(config-line)#
```

7. The last configuration for the routers in this section involves creating access control lists (ACLs) to control the flow of network traffic. As laid out in the project plan, each router has its own set of rules that it will enforce using ACLs.

    g. Router 1:

        i. Management and HR departments will be able to reach the Sales, the IT desktop, and each other.

        ii. No access to Pen testing laptop from Management or HR department.

        iii. Any traffic directed outside the networks in the addressing table will be denied.

```
Router1(config)#ip access-list extended HRACL
Router1(config-ext-nacl)#$92.168.48.0 0.0.0.255 172.20.24.0 0.0.0.255 log
Router1(config-ext-nacl)#deny ip 192.168.48.0 0.0.0.255 10.30.36.4 0.0.0.0 log
Router1(config-ext-nacl)#deny ip 192.168.48.0 0.0.0.255 any log
Router1(config-ext-nacl)#exit
Router1(config)#int Gi1.48
Router1(config-subif)#ip acces
Router1(config-subif)#ip access-group HRACL in
```

```
Router1(config-ext-nacl)#15 permit ip 192.168.48.0 0.0.0.255 192.168.99.0 0.0.$
```

```
Router1(config-ext-nacl)#25 permit ip 192.168.48.0 0.0.0.255 10.30.36.0 0.0.0.$
```

```
Router1(config)#ip access-list extended ManagementACL
Router1(config-ext-nacl)#$92.168.99.0 0.0.0.255 172.20.24.0 0.0.0.255 log
Router1(config-ext-nacl)#b.
Router1(config-ext-nacl)#deny ip 192.168.99.0 0.0.0.255 10.30.36.4 0.0.0.0 log
Router1(config-ext-nacl)#c.
Router1(config-ext-nacl)#deny ip 192.168.99.0 0.0.0.255 any log
Router1(config-ext-nacl)#exit
Router1(config)#int Gi1.99
Router1(config-subif)#ip acc
Router1(config-subif)#ip access-group ManagementACL in
```

```
Router1(config-ext-nacl)#15 permit ip  192.168.99.0 0.0.0.255 192.168.48.0 0.0$
```

```
Router1(config-ext-nacl)#25 permit ip 192.168.99.0 0.0.0.255 10.30.36.0 0.0.0.$
```

h. Router 2:

i. The sales department will be able to reach the IT person's Desktop but not the Pen testing laptop.

ii. They should also be able to contact the management and HR network.

iii. Any traffic directed outside the networks in the addressing table will be denied.

```
Router2(config)#ip access-list extended SalesACL
Router2(config-ext-nacl)#$72.20.24.0 0.0.0.255 192.168.99.0 0.0.0.255 log
Router2(config-ext-nacl)#permit ip 172.20.24.0 0.0.0.255 192.168.48.0 0.0.0.25$
Router2(config-ext-nacl)#deny ip 172.20.24.0 0.0.0.255 10.30.36.4 0.0.0.0 log
Router2(config-ext-nacl)#permit ip 172.20.24.0 0.0.0.255 10.30.36.0 0.0.0.255 $
Router2(config-ext-nacl)#deny ip 172.20.24.0 0.0.0.255 any log
Router2(config-ext-nacl)#exit
Router2(config)#int Gi1.24
Router2(config-subif)#ip access-group SalesACL in
Router2(config-subif)#
```

i. Router 3:

i. Kali Linux laptop will be able to have access to all devices in network.

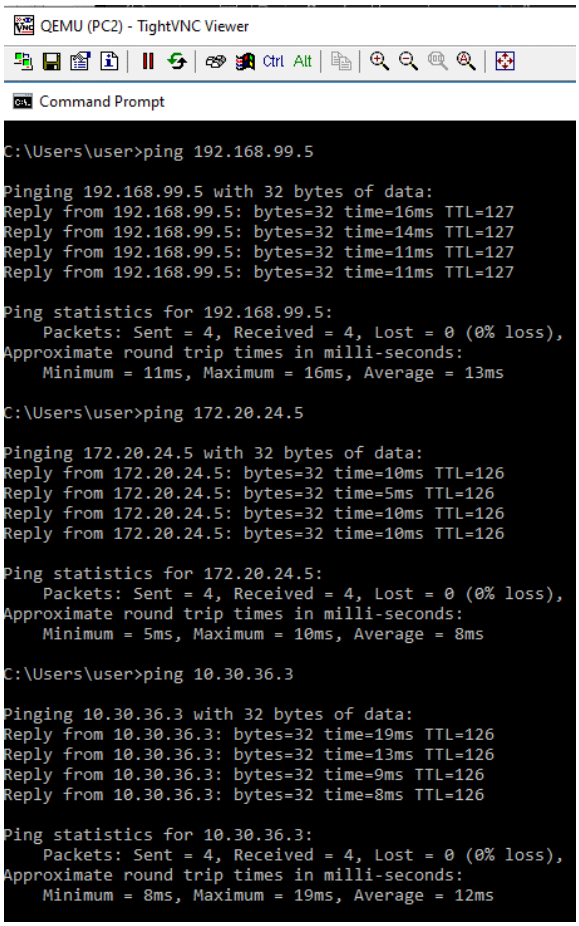
ii. IT department will be able to access Management and Sales departments.

```
Router3(config)#ip access-list extended ITACL
Router3(config-ext-nacl)#permit ip 10.30.36.3 0.0.0.0 any
Router3(config-ext-nacl)#permit ip 10.30.36.0 0.0.0.255 192.168.99.0 0.0.0.255$
Router3(config-ext-nacl)#permit ip 10.30.36.0 0.0.0.255 172.20.24.0 0.0.0.255 $
Router3(config-ext-nacl)#deny ip 10.30.36.0 0.0.0.255 any log
Router3(config-ext-nacl)#exit
Router3(config)#int Gi1.36
Router3(config-subif)#ip access
Router3(config-subif)#ip access-group ITACL in
```

An error was made in the first entry in this ACL. Enter the ACL configuration mode and issue the following commands to fix.

```
Router3(config-ext-nacl)#no 10
Router3(config-ext-nacl)#10 permit ip host 10.30.36.4 any log
Router3(config-ext-nacl)#end
```

8. The last step involves testing the ACLs by attempting to ping each network again. Now that ACLs are filtering traffic some networks will need be available to others. Proper connectivity is explained below:
    a. HR Subnet:
        i. The HR subnet should be able to reach the management and sales departments, as well as the desktop in the IT department.



ii. The HR subnet should not be able to ping the Kali Linux laptop in the IT department:

```
C:\Users\user>ping 10.30.36.4

Pinging 10.30.36.4 with 32 bytes of data:
Reply from 192.168.48.1: Destination net unreachable.
Reply from 192.168.48.1: Destination net unreachable.
Reply from 192.168.48.1: Destination net unreachable.
Reply from 192.168.48.1: Destination net unreachable.

Ping statistics for 10.30.36.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

b. Management Subnet:

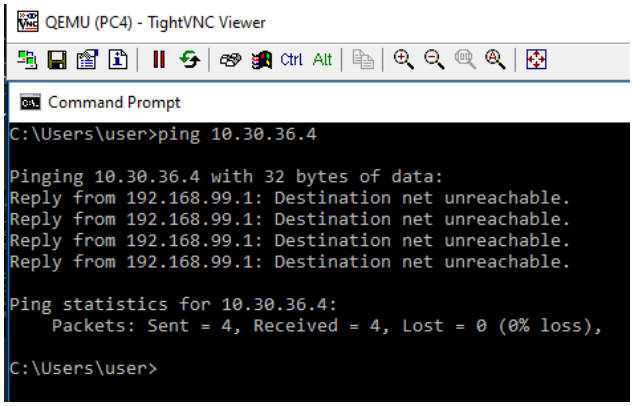
i. The management subnet should be able to reach the HR and sales departments, as well as the desktop in the IT department.

QEMU (PC4) - TightVNC Viewer

Command Prompt

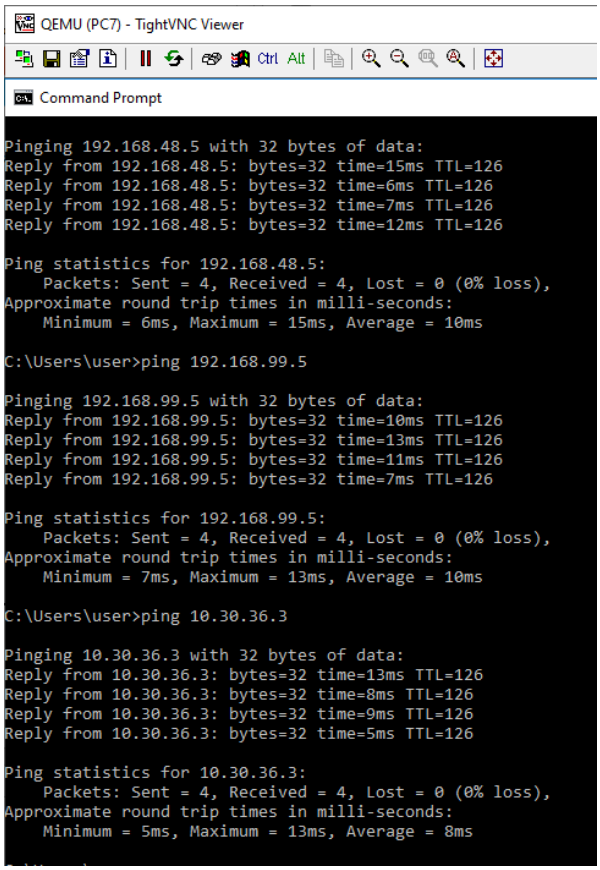
```
    Minimum = 9ms, Maximum = 11ms, Average = 10ms

C:\Users\user>ping 192.168.48.5

Pinging 192.168.48.5 with 32 bytes of data:
Reply from 192.168.48.5: bytes=32 time=10ms TTL=127
Reply from 192.168.48.5: bytes=32 time=9ms TTL=127
Reply from 192.168.48.5: bytes=32 time=9ms TTL=127
Reply from 192.168.48.5: bytes=32 time=9ms TTL=127

Ping statistics for 192.168.48.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms

C:\Users\user>ping 172.20.24.5

Pinging 172.20.24.5 with 32 bytes of data:
Reply from 172.20.24.5: bytes=32 time=12ms TTL=126
Reply from 172.20.24.5: bytes=32 time=10ms TTL=126
Reply from 172.20.24.5: bytes=32 time=11ms TTL=126
Reply from 172.20.24.5: bytes=32 time=8ms TTL=126

Ping statistics for 172.20.24.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 12ms, Average = 10ms

C:\Users\user>ping 10.30.36.3

Pinging 10.30.36.3 with 32 bytes of data:
Reply from 10.30.36.3: bytes=32 time=10ms TTL=126
Reply from 10.30.36.3: bytes=32 time=8ms TTL=126
Reply from 10.30.36.3: bytes=32 time=9ms TTL=126
Reply from 10.30.36.3: bytes=32 time=13ms TTL=126

Ping statistics for 10.30.36.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 13ms, Average = 10ms
```

ii. The management subnet should not be able to ping the Kali Linux laptop in the IT department.

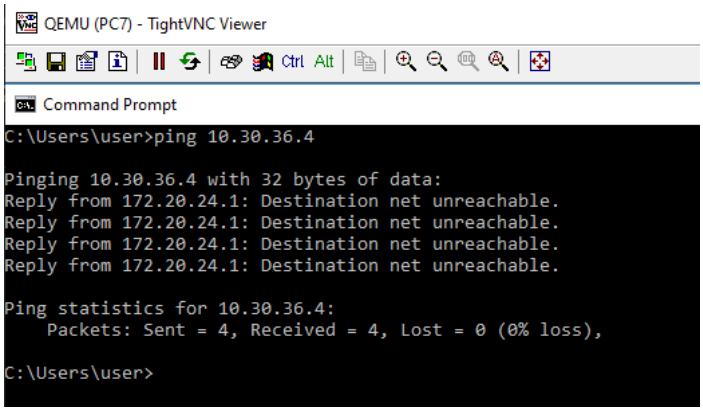


c. Sales Subnet:

i. The sales subnet should be able to reach the management and HR departments, as well as the IT desktop.

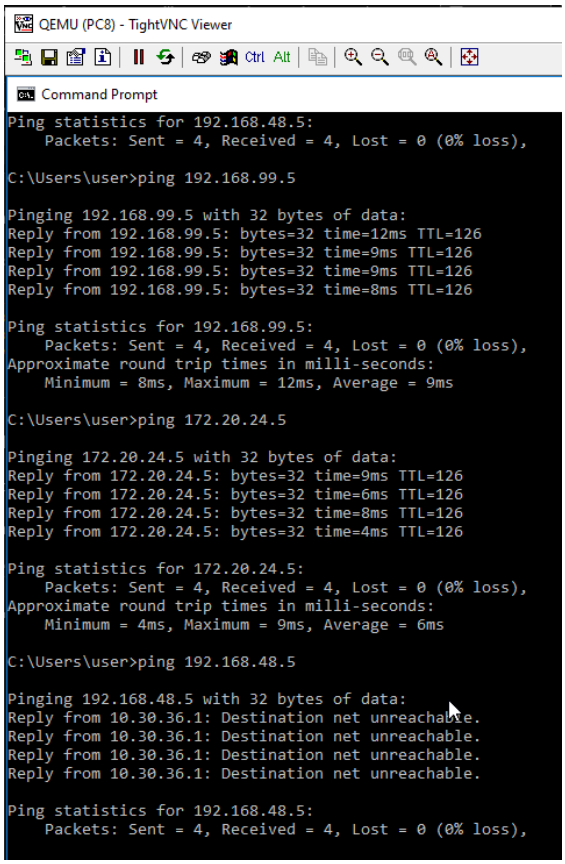


ii. The sales department should not be able to reach the IT Linux Laptop.

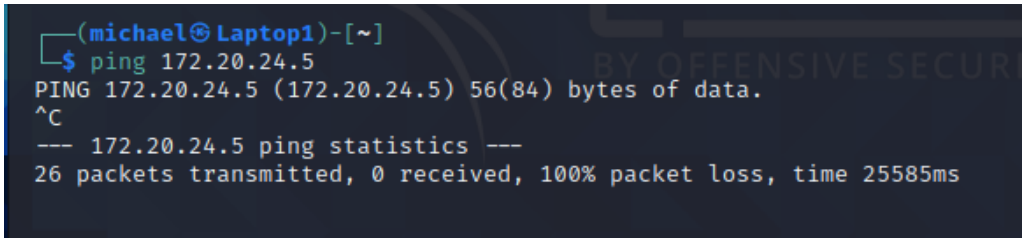


d. IT Subnet:

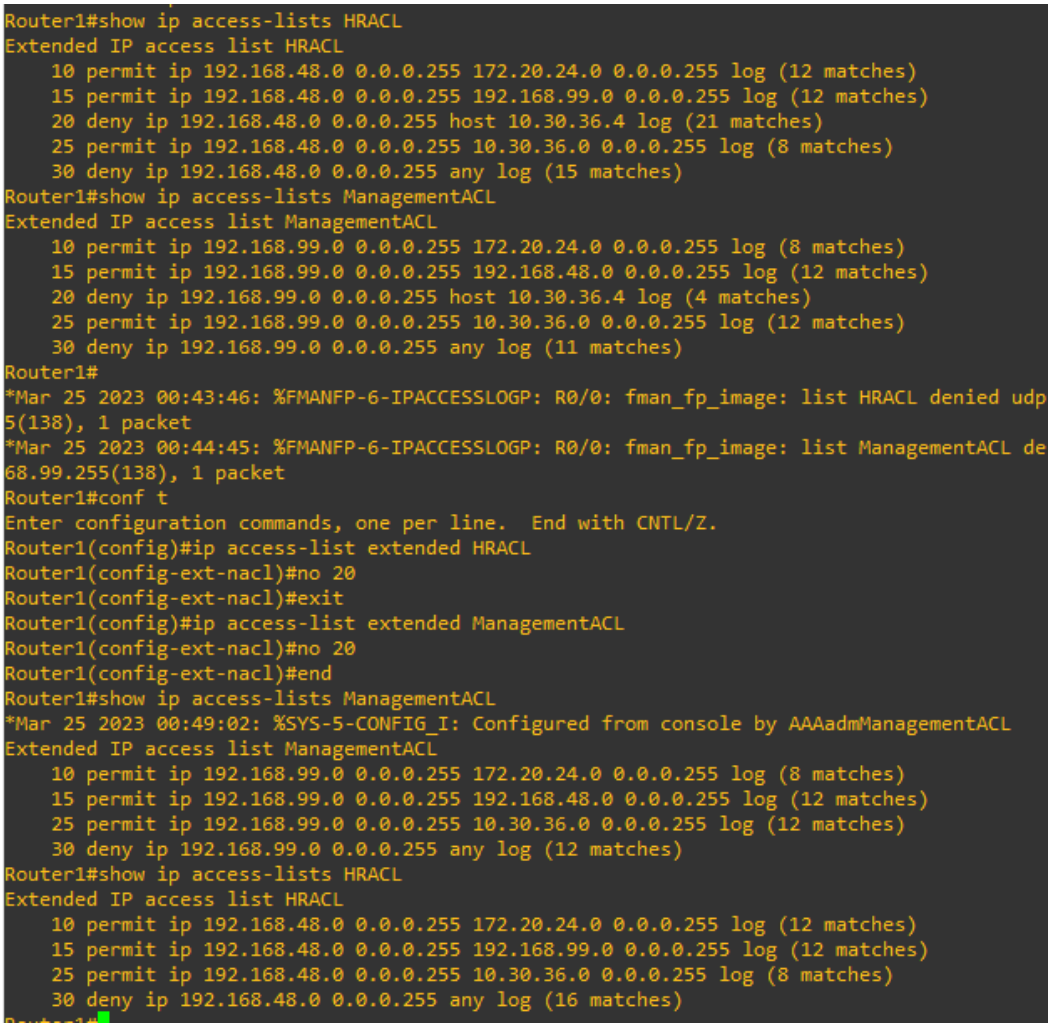
i. The IT subnet has different permissions for the end devices. The IT desktop should be able to reach the sales and management departments but not the HR department.



ii. The Kali Linux laptop should be able to ping all departments. However testing reveals that since the ACLs on the routers block traffic to the Laptop it does not receive responses to pings:



iii. In order to fix this issue the following commands, this will delete the entery which is causing the issue:



```
Router2#show ip access-lists
Extended IP access list SalesACL
    10 permit ip 172.20.24.0 0.0.0.255 192.168.99.0 0.0.0.255 log (8 matches)
    20 permit ip 172.20.24.0 0.0.0.255 192.168.48.0 0.0.0.255 log (12 matches)
    30 deny ip 172.20.24.0 0.0.0.255 host 10.30.36.4 log (46 matches)
    40 permit ip 172.20.24.0 0.0.0.255 10.30.36.0 0.0.0.255 log (12 matches)
    50 deny ip 172.20.24.0 0.0.0.255 any log (11 matches)
Extended IP access list meraki-fqdn-dns
Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet
    20 deny tcp any any eq www
    30 deny tcp any any eq 22
    40 permit ip any any
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#ip access-list extended SalesACL
Router2(config-ext-nacl)#no 30
Router2(config-ext-nacl)#end
Router2#show ip access-lists
*Mar 25 2023 00:51:21: %SYS-5-CONFIG_I: Configured from console by AAAadmin on console
Extended IP access list SalesACL
    10 permit ip 172.20.24.0 0.0.0.255 192.168.99.0 0.0.0.255 log (8 matches)
    20 permit ip 172.20.24.0 0.0.0.255 192.168.48.0 0.0.0.255 log (12 matches)
    40 permit ip 172.20.24.0 0.0.0.255 10.30.36.0 0.0.0.255 log (12 matches)
    50 deny ip 172.20.24.0 0.0.0.255 any log (11 matches)
Extended IP access list meraki-fqdn-dns
Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet
    20 deny tcp any any eq www
    30 deny tcp any any eq 22
    40 permit ip any any
Router2#
```

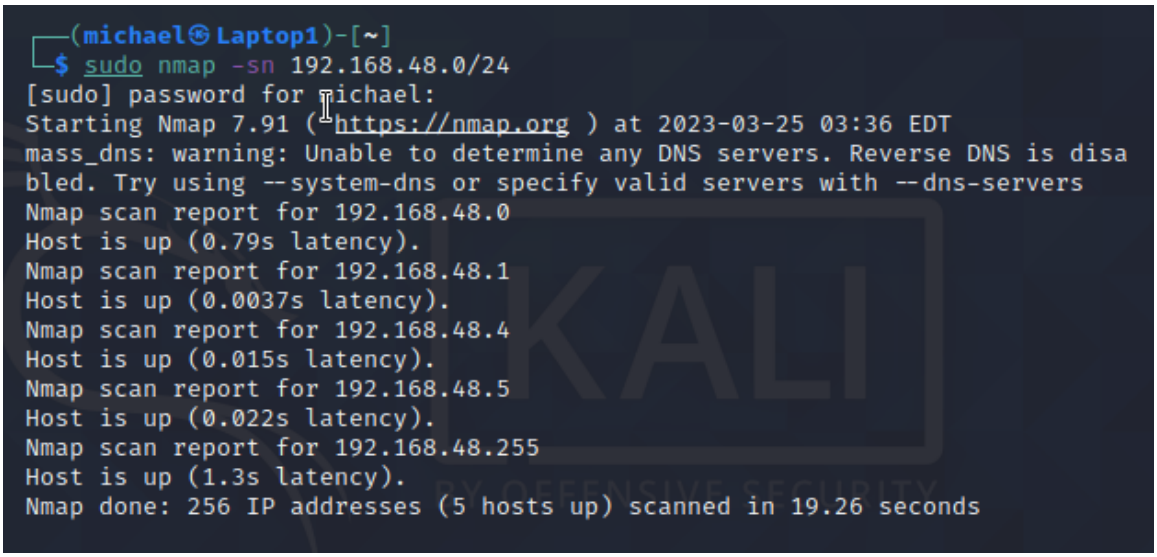
iv. Now the Kali Linux Laptop is able to ping the other devices.

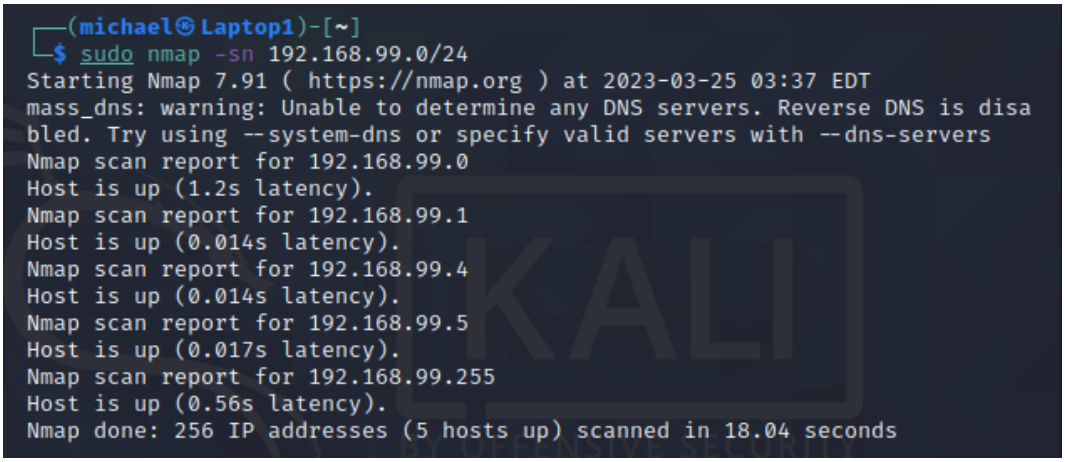
```
┌──(michael㉿Laptop1)-[~]
└─$ ping 172.20.24.5
PING 172.20.24.5 (172.20.24.5) 56(84) bytes of data.
64 bytes from 172.20.24.5: icmp_seq=1 ttl=126 time=15.8 ms
64 bytes from 172.20.24.5: icmp_seq=2 ttl=126 time=9.07 ms
64 bytes from 172.20.24.5: icmp_seq=3 ttl=126 time=8.18 ms
64 bytes from 172.20.24.5: icmp_seq=4 ttl=126 time=5.75 ms
^C
--- 172.20.24.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 5.745/9.692/15.772/3.715 ms

┌──(michael㉿Laptop1)-[~]
└─$ ping 192.168.48.5
PING 192.168.48.5 (192.168.48.5) 56(84) bytes of data.
64 bytes from 192.168.48.5: icmp_seq=1 ttl=126 time=10.3 ms
64 bytes from 192.168.48.5: icmp_seq=2 ttl=126 time=9.05 ms
64 bytes from 192.168.48.5: icmp_seq=3 ttl=126 time=8.11 ms
64 bytes from 192.168.48.5: icmp_seq=4 ttl=126 time=7.49 ms
^C
--- 192.168.48.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 7.488/8.739/10.306/1.061 ms

┌──(michael㉿Laptop1)-[~]
└─$ ping 192.168.99.5
PING 192.168.99.5 (192.168.99.5) 56(84) bytes of data.
64 bytes from 192.168.99.5: icmp_seq=1 ttl=126 time=10.2 ms
64 bytes from 192.168.99.5: icmp_seq=2 ttl=126 time=9.56 ms
64 bytes from 192.168.99.5: icmp_seq=3 ttl=126 time=7.74 ms
^C
--- 192.168.99.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.742/9.162/10.182/1.035 ms
```

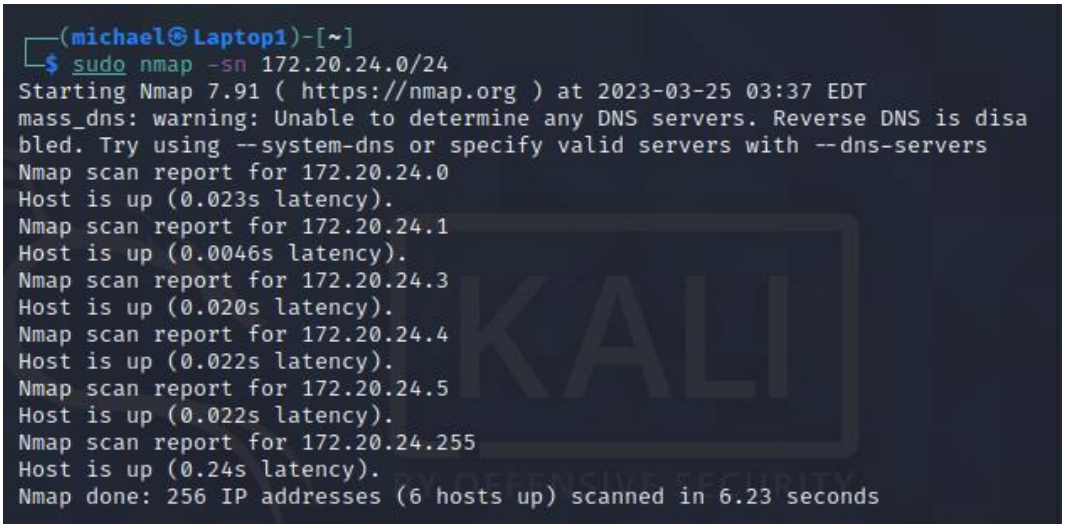
Project Testing Documentation

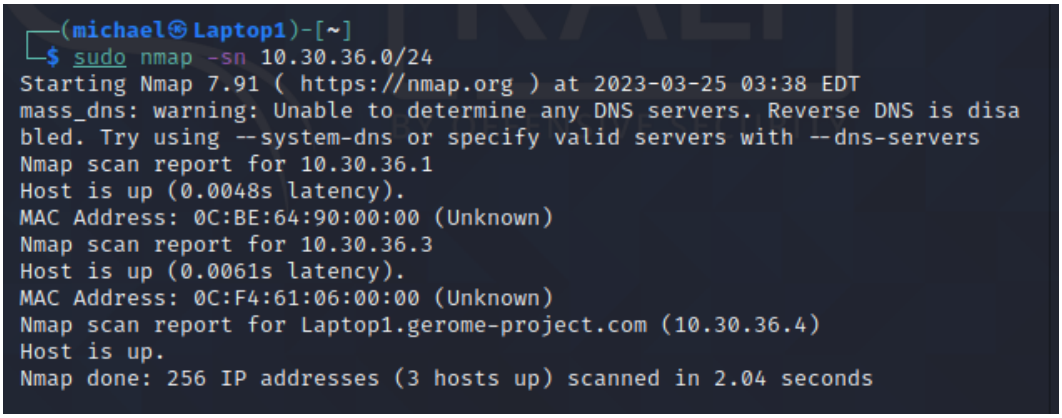
This section of the project consists of performing various tests on parts of the network to discover any problems and vulnerabilities. At the end of the project description section the ping command was used from each network and proper connectivity has occurred. The first test to be performed on the network will be performing reconnaissance on the network using the Nmap tool. This will involve three different scans on each subnet: a TCP SYN scan, a TCP FIN scan, and a ping sweep scan.

1. Make sure all devices are turn on in the network and open the Linux console.
2. Open the terminal and enter the following command to perform a ping scan on the network segment. A ping scan is where Nmap pings all IP addresses requested to check who responds. The “nmap -sn” command is used to perform the ping scan.









The above scans show that all of the end devices and router interfaces are visible to Nmap through pings. This information can be used later when deciding on a target for future action.

3. The next type of scan to be performed is a TCP SYN scan. This scan option is the most popular due to its high-speed and its relatively unobtrusive and stealthy nature. The command to perform a TCP SYN scan is “nmap -sS”:

```
└─$ sudo nmap -sS 192.168.99.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-25 03:48 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
bled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.99.0
Host is up (0.025s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
179/tcp closed bgp
443/tcp open   https
646/tcp closed ldp

Nmap scan report for 192.168.99.1
Host is up (0.0057s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.99.4
Host is up (0.017s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 192.168.99.5
Host is up (0.026s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 192.168.99.255
Host is up (0.036s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
179/tcp closed bgp
443/tcp open   https
646/tcp closed ldp
```

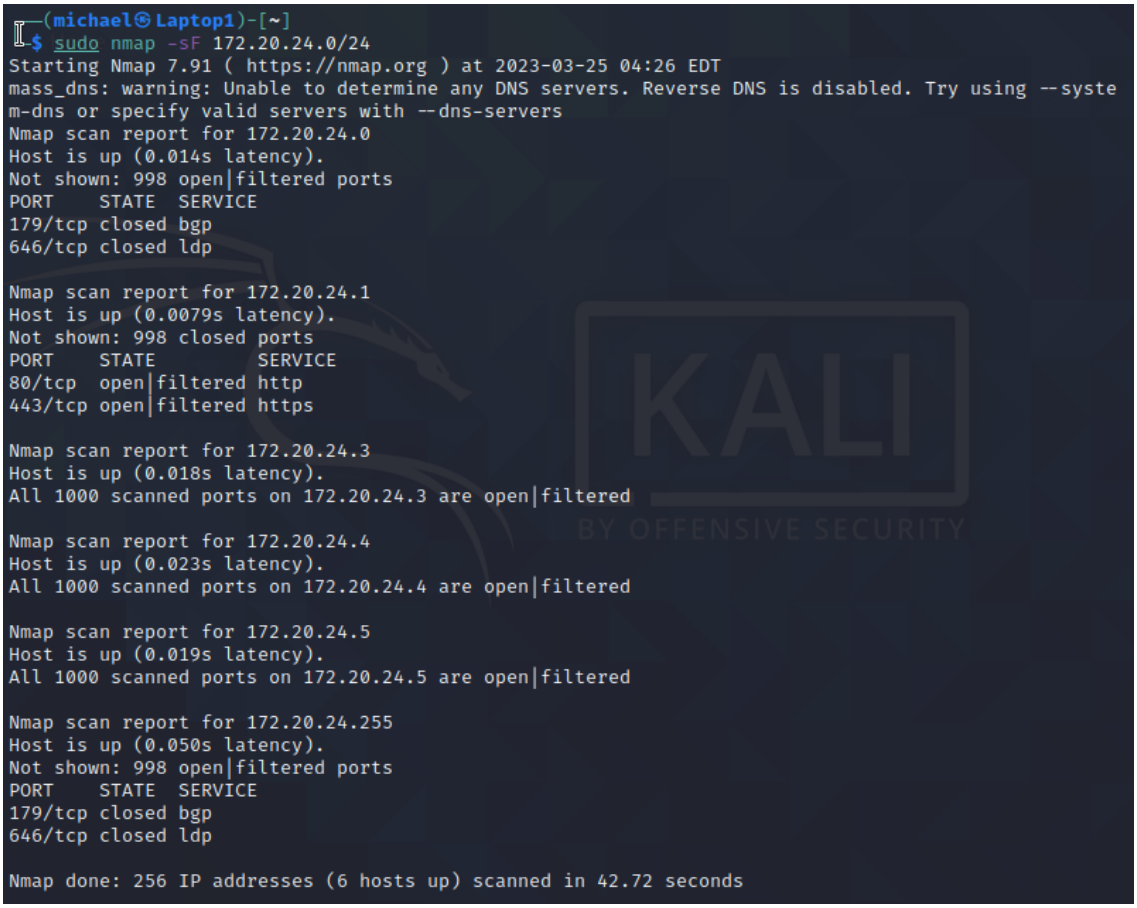
```
└─$ sudo nmap -sS 172.20.24.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-25 03:49 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
bled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.20.24.0
Host is up (0.015s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
179/tcp closed bgp
443/tcp open   https
646/tcp closed ldp

Nmap scan report for 172.20.24.1
Host is up (0.0059s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for 172.20.24.3
Host is up (0.015s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.20.24.4
Host is up (0.027s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.20.24.5
Host is up (0.015s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.20.24.255
Host is up (0.0086s latency).
```

This scan discovers a few new pieces of information. First is the list of TCP ports which are open on the devices in the network. The routers in each subnet have three TCP ports open which are ports 22 (SSH), 80 (HTTP), and 443 (HTTPS). The Windows 10 computers all have port 3389 open which is reserved for the Remote Desktop Protocol (RDP). Finally, it is shown that the Kali Linux Laptop has no open TCP ports.

4. The final scan to be performed is a TCP FIN scan. A TCP FIN scan is when Nmap sends a packet with the FIN flag set which is used to close a connection. If the port is closed it will return a RST packet which may give additional information.

```
┌──(michael㉿Laptop1)-[~]
└─$ sudo nmap -sF 192.168.48.0/24                                                    130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-25 04:21 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syste
m-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.48.0
Host is up (0.0062s latency).
Not shown: 998 open|filtered ports
PORT    STATE  SERVICE
179/tcp closed bgp
646/tcp closed ldp

Nmap scan report for 192.168.48.1
Host is up (0.0041s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
80/tcp  open|filtered http
443/tcp open|filtered https

Nmap scan report for 192.168.48.4
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.48.4 are open|filtered

Nmap scan report for 192.168.48.5
Host is up (0.019s latency).
All 1000 scanned ports on 192.168.48.5 are open|filtered

Nmap scan report for 192.168.48.255
Host is up (0.041s latency).
Not shown: 998 open|filtered ports
PORT    STATE  SERVICE
179/tcp closed bgp
646/tcp closed ldp

Nmap done: 256 IP addresses (5 hosts up) scanned in 38.45 seconds
```

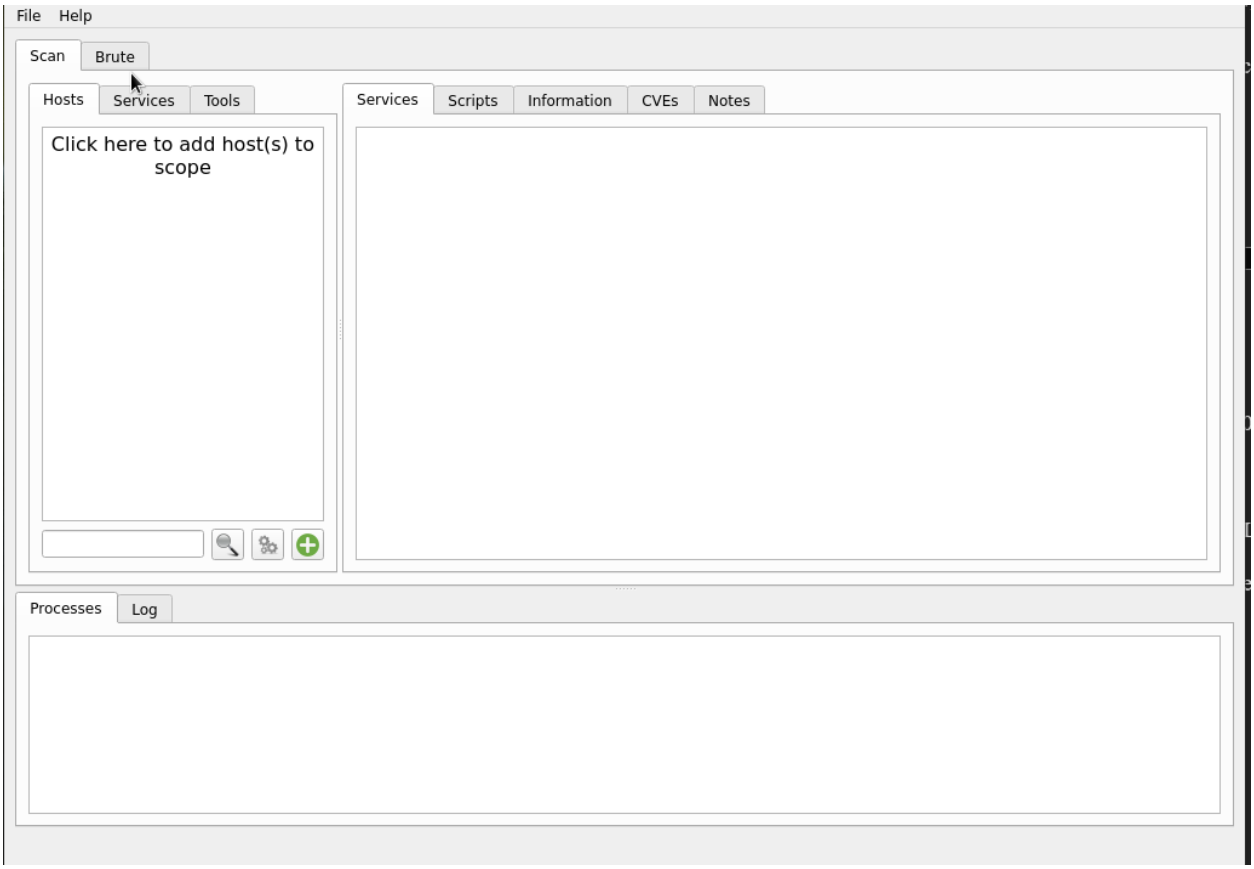
```
┌──(michael㉿Laptop1)-[~]
└─$ sudo nmap -sF 192.168.99.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-25 04:25 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syste
m-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.99.0
Host is up (0.053s latency).
Not shown: 998 open|filtered ports
PORT    STATE  SERVICE
179/tcp closed bgp
646/tcp closed ldp

Nmap scan report for 192.168.99.1
Host is up (0.0044s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
80/tcp  open|filtered http
443/tcp open|filtered https

Nmap scan report for 192.168.99.4
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.99.4 are open|filtered

Nmap scan report for 192.168.99.5
Host is up (0.025s latency).
All 1000 scanned ports on 192.168.99.5 are open|filtered

Nmap scan report for 192.168.99.255
Host is up (0.013s latency).
Not shown: 998 open|filtered ports
PORT    STATE  SERVICE
179/tcp closed bgp
646/tcp closed ldp

Nmap done: 256 IP addresses (5 hosts up) scanned in 35.68 seconds
```



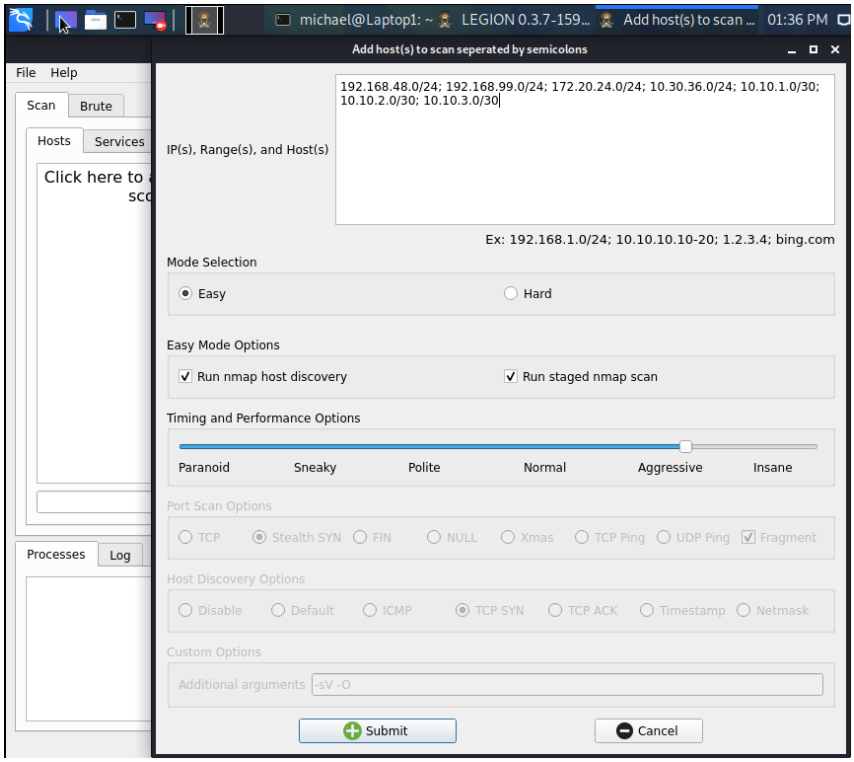
The FIN scan gave a clearer picture of the state of the ports on the devices. First on the end devices we see that the Windows computers have all 1000 scanned ports in the “open

| filtered" state. We also see the port 80 and 443 are set in the "open | filtered" state on the router interface.

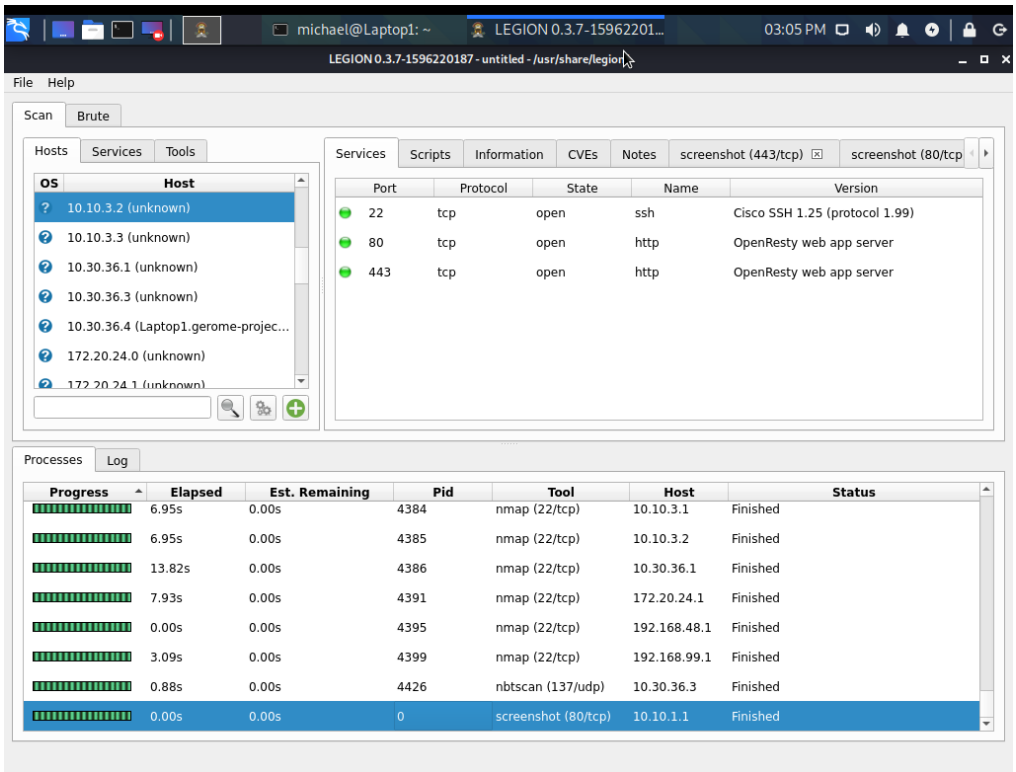
5. The next test for the network uses the Legion tool on Kali Linux to scan for vulnerabilities on devices within the network. To open the tool, issue the command "sudo legion" into the Linux terminal.



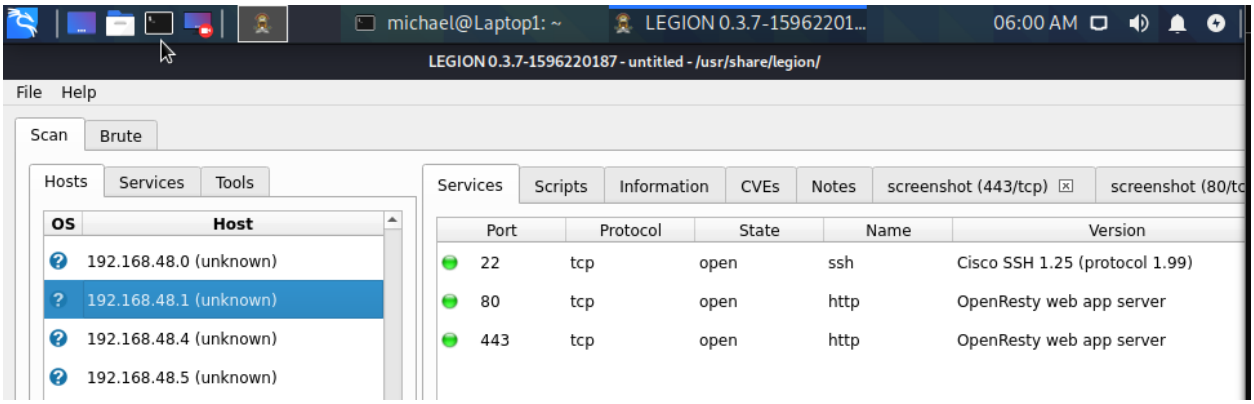
6. Select "Click here to add host(s) to scope" and add the IP addresses that were discovered with the Nmap scans and then select "Submit":



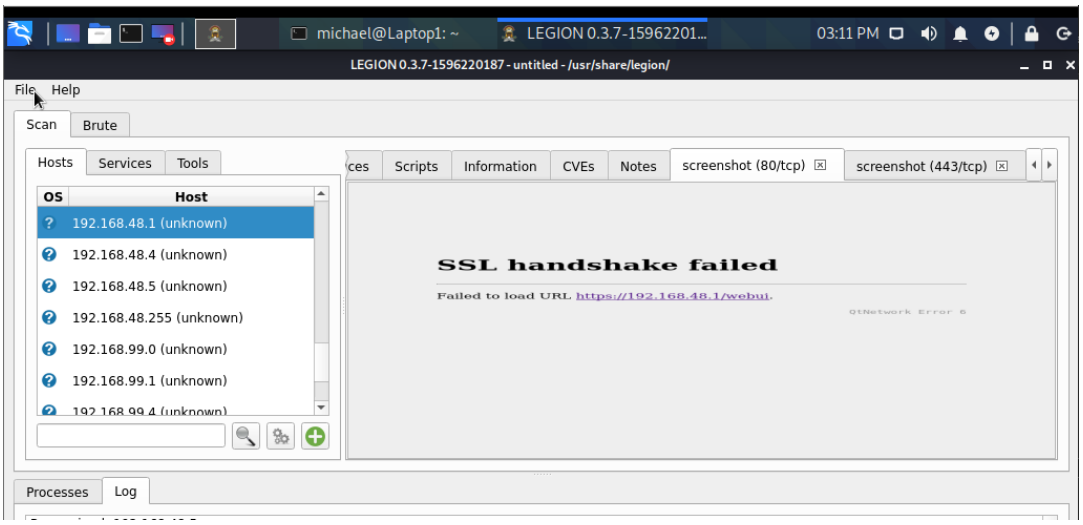
7. Once the scan is complete the left side of the screen will populate with discovered IP addresses.



8. The Legion tool is able to collect a wide-variety of information from the hosts it detects. Since the devices on the network aren't running many services there is not too much information available. Selecting the Router1 host at 192.168.48.1, it shows there are three services running on the device.

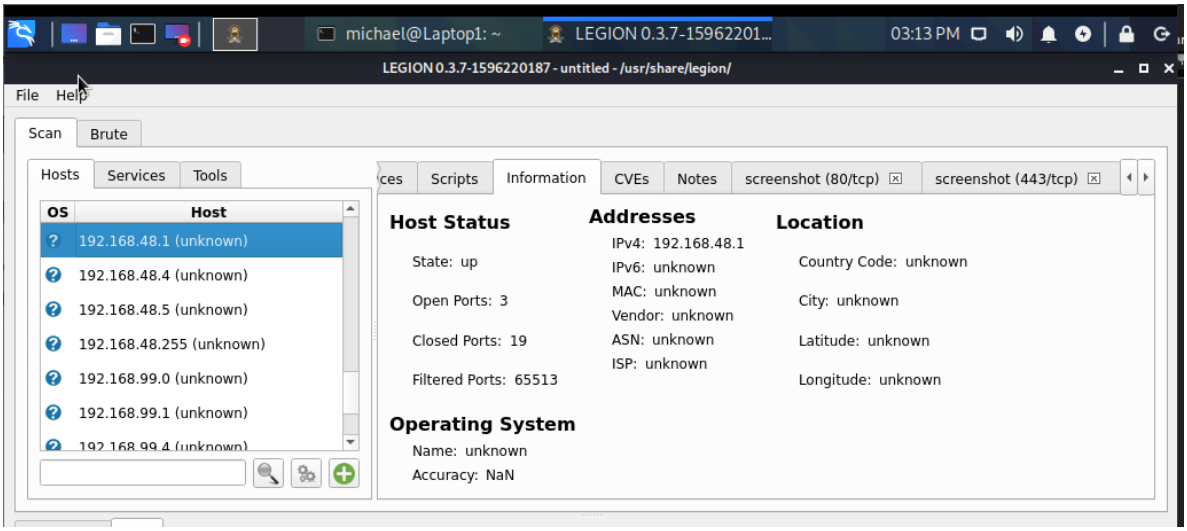


9. Once Legion detects hosts on a network and the services they are running it is able to run other applications to perform different tasks on them. For example, most devices on the network have ports 80 which hosts HTTP and 443 which hosts HTTPS open on them. Legion attempts to connect to these services and collect a screenshot of the results. Since these protocols are not configured on any devices in the network Legion returns the following results:



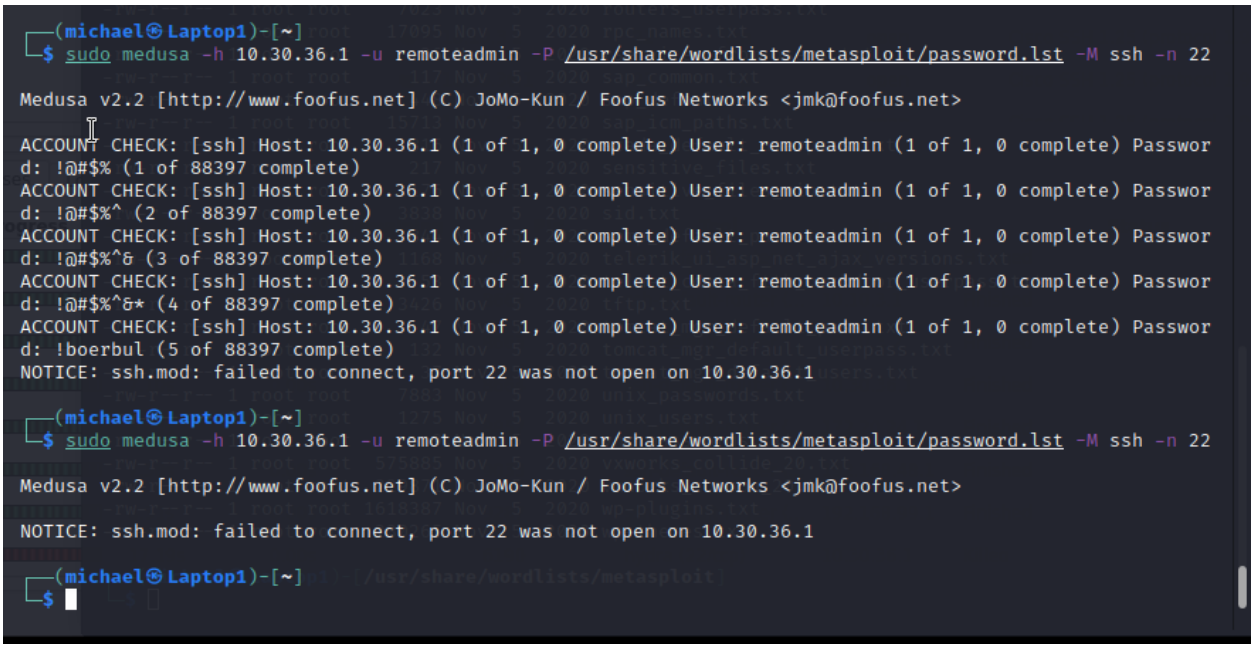
The SSL handshake occurs when a server and client establish the secret keys with which they communicate. Since the none of the devices are configured with as a web server this handshake automatically fails.

10. Legion will also compile all information gathered on a device in the information tab. The screenshot below shows that the host 192.168.48.1 has three open ports and 19 closed ports:



11. Legion is also able to view device configuration for vulnerabilities based on information from online databases. Legion is a powerful tool with a wide-variety of tools of which it can use. However, the current network is not connected to the outside internet so Legion is unable to retrieve this information. Since the network is isolated from the Internet the vulnerability scanners are unable to access vulnerability databases on the Internet. This means that these vulnerability scanning tools act as an advanced reconnaissance tool used to view what information is visible from within the network.
12. The last test to be performed will be a password cracking attempt using various techniques to attempt to gain access to one of the devices on the network. This test will

assume that the username “remoteadmin” will be used in attempts to crack passwords. This was configured on Router3 during SSH configuration. During this test the medusa tool will be used to attempt to find the password for SSH connections to devices. This test will also use a text file containing a list of over 80 thousand possible passwords. When the medusa tool is used on the host it begins at the start of the list but after the 5th attempt it was unable to connect to the device. This is because when the routers were being configured, a limit of five failed login attempts within 60 seconds was set. Since more than five attempts were made on the connection the port shut down for two minutes. This has greatly increased the protection of the routers against brute-force password attacks. Since the attacker can only attempt five passwords every two minutes, a list of 88397 passwords will take just around 24 days to go through the whole list.



Project Weekly Journals

Name: Michael Gerome

Week of 2/6/23 – 2/12/2023

Date	Start Time	End Time	Description	Total Hours
2/11/23	10:00am	1:30pm	Downloaded and Setup GNS3	3.5 Hours
				Total Hours to Date: 3.5 Hours

Journal Details:

2/11/23

- Downloaded GNS3 from gns3.com on personal laptop.
- Purchased and downloaded .ova file for GNS3 virtual machine from (https://dynamips.store/product/gns3-cisco-images-downlaod/). This provided a package of IOS images of Cisco routers, switches, and various end devices.
- Download the VMware hypervisor from vmware.com and configured the GNS3 virtual machine (VM) for use with the GNS3 application.
- Confirmed connectivity between VM and GNS3 application and the ability to place devices in emulation software.

Name: Michael Gerome

Week of 2/13/23 – 2/19/2023

Date	Start Time	End Time	Description	Total Hours
2/18/23	10:00am	2pm	Began Basic Configuration of Devices	4 Hours

Total Hours to Date: 7.5 Hours

Journal Details:

2/11/23

- Placed all devices into GNS3 in accordance with the Project Plan Topology
- Configured initial configuration on devices including the following:
    - IP addresses, subnet masks, and default gateways
    - Hostnames
    - Passwords for privileged EXEC mode and global configuration mode

Name: Michael Gerome

Week of 2/20/23 – 2/26/2023

Date	Start Time	End Time	Description	Total Hours

Total Hours to Date: 7.5 Hours

Journal Details:

- Due to work load in other classes this week no work was done on the project this week will continue to work on project next week.

Name: Michael Gerome

Week of 2/27/23 – 3/5/2023

Date	Start Time	End Time	Description	Total Hours
3/5/2023	6pm	11pm	Continued with configuration of devices.	5 Hours

Total Hours to Date: 12.5 Hours

Journal Details:

- Configured VLANs on devices and set up EIGRP between subnets.
- Configured Layer 2 security commands on switches.
- Started to configure router security.
- Configured STP on three switches.

Name: Michael Gerome

Week of 3/6/23 – 3/12/23

Date	Start Time	End Time	Description	Total Hours
3/8/2023	4pm	6pm	Continued with configuration of devices.	2 Hours
3/10/2023	11am	4pm	Set up Kali Linux machine and configured Windows PCs	5 Hours
3/11/2023	4pm	8pm	Worked on project Documentation	4 Hours

Total Hours to Date: 23.5 Hours

Journal Details:

- Configured Windows computers to allow ICMP echo requests for connectivity testing.
- Set up Kali Linux laptop and verified connectivity to network.
- Began research on Kali Linux tools for testing.
- Began testing by using Nmap.
- Worked on documentation for project

Name: Michael Gerome

Week of 3/13/23 – 3/19/23

Date	Start Time	End Time	Description	Total Hours
3/15/2023	4pm	8pm	Performed scan with Legion and looked at options	4 Hours
3/17/2023	11am	4pm	Researched on how to use medusa and performed brute-force attack	2.5 Hours
3/18/2023	4pm	8pm	Worked on project Documentation	4 Hours
				Total Hours to Date: 34 Hours

Journal Details:

- Researched how to use Legion and Medusa
- Performed scan with Legion and explored options
- Used Medusa to conduct brute-force password attack
- Continued working on project documentation

Name: Michael Gerome

Week of 3/13/23 – 3/19/23

Date	Start Time	End Time	Description	Total Hours
3/24/2023	11am	8pm	Finalized documentation, wrote project analysis	9 Hours
3/26/2023	5pm	8pm	Made project presentation and practiced	3 hours

Total Hours to Date: 46Hours

Journal Details:

- Finished work on project
- Worked on and finished project documentation
- Made project presentation

References

Allen, R. (2022, May 23). *How to allow Ping in windows firewall (client or server OS)*. Active Directory Pro. Retrieved March 26, 2023, from https://activedirectorypro.com/allow-ping-windows-firewall/

Catalyst Digital Building Series Switch Hardware Installation Guide - Product Overview [cisco catalyst digital building series switches]. Cisco. (2017, August 18). Retrieved March 26, 2023, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_digital_building_series_switches/hardware/install/b-cdb-hig/b-cdb-hig_chapter_01.html

Cisco. (2017, May 7). *Clock commands on Cisco IOS XR software*. Cisco. Retrieved March 26, 2023, from https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r3-9/system_management/command/reference/yr39xr12k_chapter4.html#wp748744425

Concepts and configuration of The spanning tree protocol. Section. (n.d.). Retrieved March 26, 2023, from https://www.section.io/engineering-education/concepts-and-configuration-of-stp/

Configuring switches with vlans¶. pfSense® software Configuration Recipes - Configuring Switches with VLANs | pfSense Documentation. (n.d.). Retrieved March 26, 2023, from https://docs.netgate.com/pfsense/en/latest/recipes/switch-vlan-configuration.html#:~:text=Most%20switches%20have%20a%20means,be%20configured%20on%20any%20ports.&text=The%20port%20to%20which%20the,possible%20VLANs%20on%20the%20interface.

GeeksforGeeks. (2020, December 2). *Password cracking with Medusa in linux*. GeeksforGeeks. Retrieved March 26, 2023, from https://www.geeksforgeeks.org/password-cracking-with-medusa-in-linux/

Glenn, W. (2020, December 15). *How to allow Pings (ICMP echo requests) through your windows firewall*. How. Retrieved March 26, 2023, from https://www.howtogeek.com/1153/allow-pings-icmp-echo-request-through-your-windows-vista-firewall/

Interface whose encapsulation is auto can not be configured to Trunk. PeteNetLive. (2021, March 4). Retrieved March 26, 2023, from https://www.petenetlive.com/kb/article/0001167

Messina, G. (2021, July 19). *Kali Linux: Top 5 tools for password attacks*. Infosec Resources. Retrieved March 26, 2023, from https://resources.infosecinstitute.com/topic/kali-linux-top-5-tools-for-password-attacks/

Network reconnaissance using NMAP - one stop solution. GoLinuxCloud. (2021, December 27). Retrieved March 26, 2023, from https://www.golinuxcloud.com/network-reconnaissance-using-nmap/

Pederstuen, E. (2021, February 12). *Cisco sub-interface config in packet tracer*. YouTube. Retrieved March 26, 2023, from https://www.youtube.com/watch?v=b1JaMlRCjK8&ab_channel=ErikPederstuen

Router on a stick approach - cisco configuration. Grandmetric. (2022, December 22). Retrieved March 26, 2023, from https://www.grandmetric.com/knowledge-base/design_and_configure/router-on-a-stick-approach-cisco-configuration/

Spanning tree protocol (STP) configuration. Grandmetric. (2022, December 22). Retrieved March 26, 2023, from https://www.grandmetric.com/knowledge-base/design_and_configure/spanning-tree-protocol-stp-configuration/