

The University of Akron

IdeaExchange@UAkron

Williams Honors College, Honors Research
Projects

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

Spring 2023

Defense of a Small Network

Isabella Adkins
ija9@uakron.edu

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



Part of the [Digital Communications and Networking Commons](#), [Information Security Commons](#), [OS and Networks Commons](#), and the [Other Computer Sciences Commons](#)

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

Recommended Citation

Adkins, Isabella, "Defense of a Small Network" (2023). *Williams Honors College, Honors Research Projects*. 1674.

https://ideaexchange.uakron.edu/honors_research_projects/1674

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

Simulating a Small Office Network for Penetration Testing

Isabella Adkins

The University of Akron

CISS 491: Senior Cybersecurity Project

Dr. John Nicholas

March 27, 2023

Abstract

The following report contains the complete documentation, including analysis, description, and testing for the project: Simulating a Small Office Network For Penetration Testing. The testing documentation proves the project is working as proposed, as well as demoing the attacks used against the network. The analysis and description provide insight on replicating the project, as well as a general overview.

Contents

Cybersecurity Project Proposal	4
Progress Journals	11
Project Analysis	18
Project Description	22
Testing Documentation	47
References	124

Cybersecurity Project Proposal

Isabella Adkins

01/11/2023

Spring 2023

Project Name: Simulating a Small Office Network for Penetration Testing

Project Description:

This project will consist of the design and implementation of three routers, one switch, a server for file sharing, and three end hosts with Fedora OS. The network will consist of three subnets, and a firewall will be implemented to keep outside threats from the Fedora OS devices. This network will be completely simulated within the GNS3 software, and OS licenses purchased from Cisco. The three routers will represent three different departments within the company: legal, accounting, and HR. These devices will all be on the same 10.13.0.0/16 network/subnet. The network will be secured to align with industry standards; such as disabling unused ports, and encrypting plaintext passwords. Once the network is secure, a Windows machine simulating Kali Linux will be used in an attempt to penetrate the network. During penetration testing, tools like nmap and metasploit will be used to gain information about the network, as well as to try and discover vulnerabilities to gain access to the network. Kali Linux will also be used in an attempt to get a phishing email to an end host on the network.

Required Equipment:

- (1) Lenovo Legion Laptop (Equipped to run GNS3 + VirtualBox)
- (1) GNS3 Software
- (1) Cisco Router Licensing
- (1) VirtualBox VM Software
- (3) Fedora OS VMs
- (1) Kali Linux VM

Budget:

Item	Expected Cost	Total
Licensing	\$150	\$150

Detailed Objectives:**1. Research**

- a. Using GNS3 Software with Cisco Licensing
 - i. Adding Devices to GNS3
 - ii. Implementing Fedora OS within GNS3 software
 - iii. Implementing a file sharing server within GNS3
- b. Using an external Kali Linux machine to connect to GNS3 software
 - i. Using an instance of Kali within GNS3
 - ii. Using an external instance of Kali to connect to GNS3
- c. Troubleshooting with GNS3 software
 - i. Issues with connecting Cisco devices
 - ii. Issues with using VirtualBox
 - iii. Issues with using Kali
- d. Command line commands for routers
 - i. Setting up snort spam filter to catch phishing emails
- e. Configuring File Sharing server with encryption for extra data protection

2. Design

- a. Network Topology and Addressing
 - i. Router 1 (R1-Leg)
 - ii. Router 2 (R2-Acct)
 - iii. Router 3 (R3-HR)
 - iv. Switch 1 (Sw1)
 - v. File Sharing Server (Serv1)
 - vi. Fedora OS (PC1)
 - vii. Fedora OS (PC2)

viii. Fedora OS (PC3)

Device Name	Interface	IP Address	Subnet Mask
R1-Leg	G0/1	10.13.1.1	255.255.255.0
R1-Leg	S0/0/1	10.13.5.1	255.255.255.0
R2-Acct	G0/1	10.13.2.1	255.255.255.0
R2-Acct	S0/0/1	10.13.5.2	255.255.255.0
R2-Acct	S0/0/2	10.13.6.1	255.255.255.0
R3-HR	G0/1	10.13.4.1	255.255.255.0
R3-HR	S0/0/1	10.13.6.2	255.255.255.0
Sw1	Fas0/1	10.13.2.2	255.255.255.0
Serv1	Fas0/1	10.13.4.3	255.255.255.0
PC1-Fed	Fas0/1	10.13.1.2	255.255.255.0
PC2-Fed	Fas0/1	10.13.2.3	255.255.255.0
PC3-Fed	Fas0/1	10.13.4.4	255.255.255.0

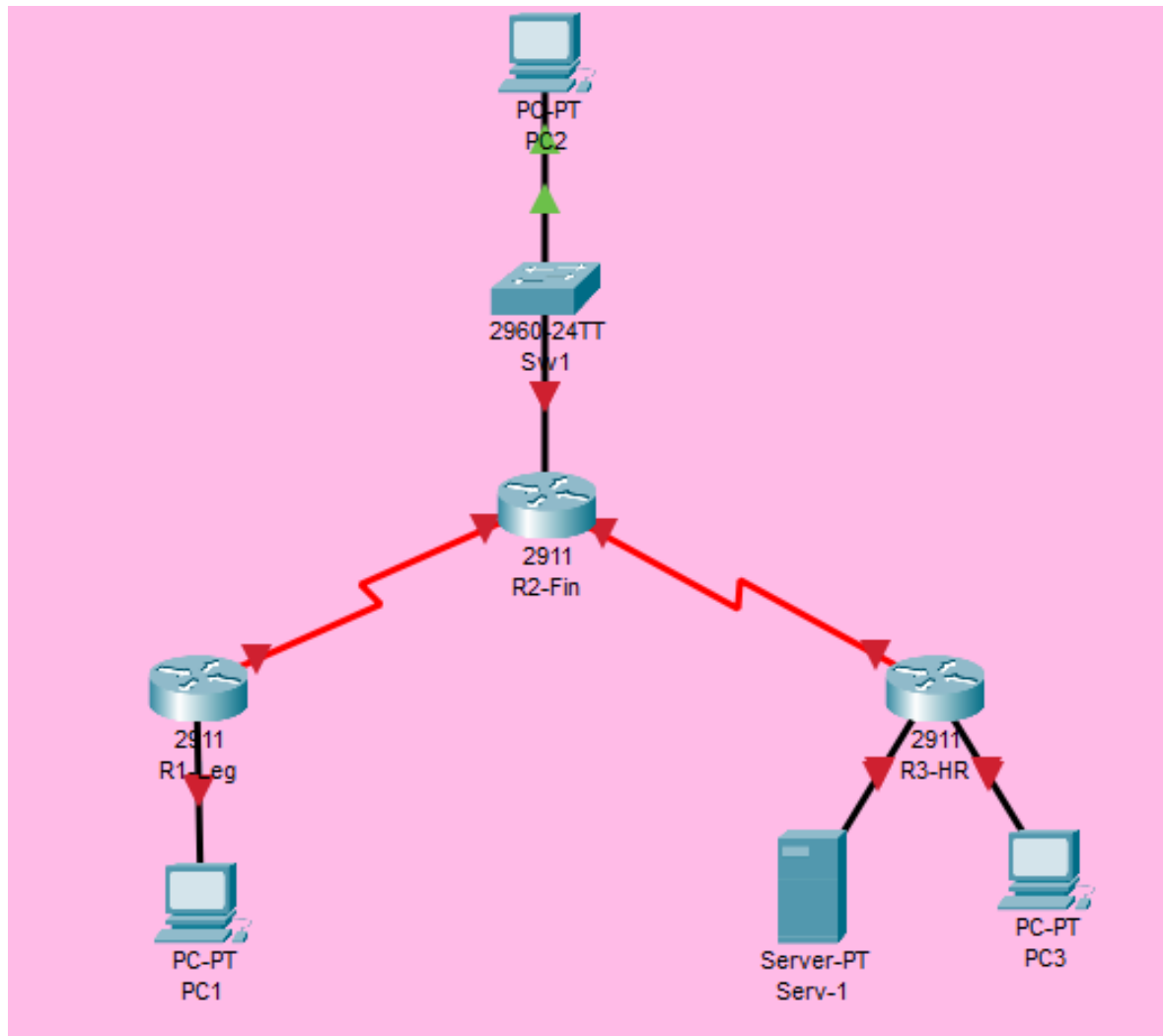


Figure 1.1 - Sample Topology created in Cisco Packet Tracer

3. Implementation

- a. Configure R1-Leg
 - i. Set IP Address/Subnet Mask
 - ii. Configure routing (RIPv2)
 - iii. Set passwords (enable/secret)
 - iv. Set up filter for spam emails
 - v. Configure ACL to prevent any traffic from outside the company network from reaching Leg segment
- b. Configure R2-Acct
 - i. Set IP Address/Subnet Mask

- ii. Configure routing (RIPv2)
- iii. Set passwords (enable/secret)
- iv. Configure ACL to prevent any traffic from outside the company network from reaching Acct segment
- c. Configure R3-HR
 - i. Set IP Address/Subnet Mask
 - ii. Configure routing (RIPv2)
 - iii. Set passwords (enable/secret)
 - iv. Configure firewall to prevent any traffic from outside the company network from reaching HR segment
- d. Configure Sw1
 - i. Set IP Address/Subnet Mask
 - ii. Set passwords (enable/secret)
 - iii. Disable unused interfaces/ports
- e. Configure Serv1
 - i. Setup for file sharing across network
- f. Configure PC1-Fed
 - i. Configure IP Address/Subnet Mask
 - ii. Configure access to file sharing server
- g. Configure PC2-Fed
 - i. Configure IP Address/Subnet Mask
 - ii. Configure access to file sharing server
- h. Configure PC3-Fed
 - i. Configure IP Address/Subnet Mask
 - ii. Configure access to file sharing server

4. Testing

- a. Ensure connectivity via ICMP Pings
 - i. PC1 to PC2, PC3
 - ii. PC2 to PC1, PC3
 - iii. PC3 to PC1, PC2

- b. Ensure PCs can access shared files on Serv1
 - i. Create File on each PC and upload to server
 - ii. Have PCs access shared files/save edits
- c. Reconnaissance using nmap
- d. Use metasploit to locate any vulnerabilities that can be used to gain access to file server
- e. Configure phishing email toolkit/send email to users

5. Documentation

- a. Configurations for all listed devices
- b. Troubleshooting for any issues
 - i. Connection failures
 - ii. File sharing issues
- c. Reconnaissance results
 - i. Network information
 - ii. Specific host information
- d. Metasploit results
 - i. Successful?
 - ii. Able to find any vulnerabilities
 - iii. Able to use any vulnerabilities
 - iv. How to fix the potential vulnerabilities
- e. Phishing results
 - i. Creation of email
 - ii. Sending of email/rejection of email
 - iii. Email reached end host through preventative measures
 - iv. How to reinforce measures if successful to prevent more phishing
- f. Analysis of completed project
- g. Testing procedures/proof
- h. Weekly progress Journals
- i. References

Estimated Time:

<i>Research</i>	<i>Design</i>	<i>Implementation</i>	<i>Testing</i>	<i>Documentation</i>	<i>Total</i>
10 hrs.	15 hrs.	15 hrs.	10 hrs.	10 hrs.	60 hrs.

Progress Journals

Isabella Adkins

Summary - Week Ending: 3/27/23

Date	Start Time	End Time	Description	Total
3/20	7:00 PM	8:00 PM	ACLs/Documentation	1 Hr
3/21	11:00 AM	3:00 PM	ACLs/Router Security/Documentation	4 Hrs
3/22	7:00 PM	9:00 PM	Kali tests	2 Hrs
3/23	10:00 AM	10:00 PM	(Had breaks) Kali tests/Documentation	9 Hrs
3/24	10:00 AM	12:00 PM	Documentation	2 Hrs
3/26	12:30 PM	6:30 PM	Documentation	6 Hrs

Weekly Total Hours	24 Hours
Total Hours To Date	65 Hours 45 Minutes

Journal Details

- 3/20 - Created APA formatted templates for completing documentation. Worked on testing and implementation of ACLs for routers within the network.
- 3/21 - Correcting ACLs for denying SMTP traffic, setting up enable/secret passwords, disabling unused interfaces on routers, creating banner messages, installing Kali Linux VM Virtual machine, creating reference documentation
- 3/22 - Connecting Kali to topology (ran into some issues)
- 3/23 - Connecting Kali to topology, performing ethical hacking tests
- 3/24 - Documentation (Power Point, Notes, etc)
- 3/26 - Documentation (Analysis, Description, Testing) FINISHED EVERYTHING!!!

Isabella Adkins**Summary - Week Ending: 3/19/23**

Date	Start Time	End Time	Description	Total
3/13	4:00 PM	9:00 PM	Fixing FTP/GNS3 topology	5 Hrs
3/14	7:00 PM	9:00 PM	Fixing FTP/GNS3 topology	2 Hrs
3/15	2:30 PM	4:00 PM	GNS3 Topology/Ping Tests	1 Hr 30 Mins
3/16	2:00 PM	5:00 PM	Switch configs/FTP Server	3 Hrs
3/17	11:45 AM	5:15 PM	Switch/Router Security Configs/FTP Server	5 Hrs 30 Mins

Weekly Total Hours	17 Hours
Total Hours To Date	41 Hours 45 Minutes

Journal Details

- 3/13 - Accidentally deleted config, had to restart topology, reinstall new Fedora VMs for creation of filesharing server.
- 3/14 - Configuring FTP on Fedora Server, adding fixed VMs to topology, gns3 marketplace appliance configuration
- 3/15 - Adding VMs to topology, connecting them to ports, sample ping tests. FTP server configurations
- 3/16 - FTP Users and test files added, configuring switch, ping tests
- 3/17 - Adding test FTP documents, making sure VMs can access documents, switch configs (enable/secret password, port security), router configs (trying to make ACLs)

Isabella Adkins**Summary - Week Ending: 3/12/23**

Date	Start Time	End Time	Description	Total
3/6	2:40 PM	3:15 PM	Adding Server/Switch to Topology	35 Min
3/8	3:30 PM	6:30 PM	Configurations/Documentation	3 Hrs.
3/9	10:30 PM	11:40 PM	Configuration/Documentation	1 Hr 10 Min
3/11	11:30 AM	3:00 PM	Configurations/Installation	3 Hrs 30 Min
3/12	3:00 PM	5:30 PM	Configurations/Installations	2 Hrs 30 Min

Weekly Total Hours	10 Hours 45 Minutes
Total Hours To Date	24 Hours 45 Minutes

Journal Details

- 3/6 - Worked on adding templates to GNS3 with Personal Labs image for switch. Getting ftp server from GNS3 marketplace and adding to topology
- 3/8 - Assigning IPs, adding routers to topology, troubleshooting issues, documenting commands used, setting up Fedora VMs.
- 3/9 - Assigned IPs to Fedora device, connecting and cabling routers to fedora, some ping tests
- 3/11 - Assigned IPs to Fedora Device, Switch, cabled network, ping tests. Trying to get FTP server in GNS3 and functional.
- 3/12 - Tested IPs, working on implementing FTP server

Isabella Adkins**Summary - Week Ending: 3/5/23**

Date	Start Time	End Time	Description	Total
2/28	8:00 PM	11:30 PM	Software installations/troubleshooting	3.5
3/1	1:00 PM	2:00 PM	GNS3 Prep	1
3/2	5:00 PM	7:00 PM	GNS3 Installation/Images Upload	2

Weekly Total Hours	6.5
Total Hours To Date	14

Journal Details

- 2/28 - Ran into issue with localhost connecting, and also mismatch between GNS3 VM version and GNS3 version. Trouble everywhere, reinstalled, restarted multiple times, had to reinstall and lose all my progress, added a bunch of useless exceptions to firewall, went into settings so main server is not the GNS3 VM (maybe).
- 3/1 - Reinstall GNS3, finally figured out firewall issue (working now), uploaded ISO images from Cisco personal labs
- 3/2 - Uploaded ISO images, using Solar Putty Window for testing configs

Isabella Adkins**Summary - Week Ending: 2/26/23**

Date	Start Time	End Time	Description	Total
2/25	4:00 PM	6:00 PM	GNS3 Configurations	2
2/26	5:00 PM	6:00 PM	Router Testing/Configurations	1

Weekly Total Hours	3
Total Hours To Date	7.5

Journal Details

- 2/25 - Tested various features of GNS3, tested sample configurations and saving file
- 2/26 - Tested additional GNS3 configs/settings, tested router configs.

Isabella Adkins**Summary - Week Ending: 2/19/23**

Date	Start Time	End Time	Description	Total
2/16/23	7:00 PM	9:00 PM	Research/Installation	2
2/18/23	2:00 PM	3:30 PM	Research/Installation	1.5

Weekly Total Hours	2.5
Total Hours To Date	4.5

Journal Details

- 2/16 - Researched Cisco licensing options, purchased 200 dollar personal package, installed python, installed VM Ware
- 2/18 - Installed ISO files into gns3, test configurations with SolarWinds PutTy window, updated fedora oracle box

Isabella Adkins**Summary - Week Ending: 2/12/23**

Date	Start Time	End Time	Description	Total
2/7/23	3:00 PM	4:00 PM	Research	1
2/8/23	5:00 PM	6:00 PM	Research	1

Weekly Total Hours	2 Hours
Total Hours To Date	2 Hours

Journal Details

- 2/7 - Researched Cisco licensing/options
- 2/8 - Researched Cisco licensing, and compatibility with GNS3

Project Analysis

GNS3 was the software used to simulate the network and host the routers. In the initial configuration, there was an issue where the additional GNS3 VM (Used to divert some of the processing power and put less strain on the host computer), was not being recognized. This was solved by redownloading GNS3. After this second installation, there was another issue where the VM was not connecting. This was because of a known bug that the GNS3 software was shipped with, that many other users encountered. This was patched by downloading GNS3 for the third time, from GitHub. After this third installation, GNS3 worked as intended, and was able to be used to simulate the network and complete the project.

R1-Leg was configured to connect to the Fedora VM Cap-Leg-1, and keep it on the subnet 10.13.1.0/24. R1-Leg was also configured to connect to R2-Fin via 10.13.5.0/24. Standard security measures such as creating long passwords with a variety of characters, disabling unused ports, adding a banner as a legal protection, and enabling brute-force attack protection by having a login timeout if too many incorrect attempts are used. The router was configured and works as proposed, passing packets and being able to ping out. At the end of the configurations, the Kali machine was connected to represent an internal attack, and used the subnet 10.13.8.0/24. From there, the penetration tests were carried out.

R2-Fin was configured to connect to the switch Sw-1, and keep it on the subnet 10.13.2.0/24. R2-Fin was also configured to connect to R1-Leg via 10.13.5.0/24. R2-Fin was also configured to connect to R3-HR via 10.13.6.0/24. Standard security measures such as creating long passwords with a variety of characters, disabling unused ports,

adding a banner as a legal protection, and enabling brute-force attack protection by having a login timeout if too many incorrect attempts are used. The router was configured and works as proposed, passing packets and being able to ping out.

R3-HR was configured to connect to the Fedora VM Cap-HR-1, and keep it on the subnet 10.13.4.0/24. R3-HR was also configured to connect to the FTP server Cap-FTP-Serv-1, using the subnet 10.13.7.0/24. R3-HR was also configured to connect to R2-Fin via 10.13.6.0/24. Standard security measures such as creating long passwords with a variety of characters, disabling unused ports, adding a banner as a legal protection, and enabling brute-force attack protection by having a login timeout if too many incorrect attempts are used. The router was configured and works as proposed, passing packets and being able to ping out.

Sw-1 was configured to connect between R2-Fin, and the Fedora VM Cap-Fin-1 on the subnet 10.13.2.0/24. The two ports in use were added to VLAN 10, while all other ports were added to VLAN 30, and shut down as a security measure. Secure passwords were added, and there was a login timeout to prevent any brute-force attacks. The switch was configured and works as proposed, being able to pass packets and ping outwards.

Cap-Leg-1 was a Fedora VM running Fedora 37. This was simulated with an ISO image through VMWare software, and then implemented into the GNS3 topology. The IP address was manually configured to be static and 10.13.1.2/24. The device was then configured to be able to access the FTP server. No issues were found in the creation of the VM, or the implementation of the VM.

Cap-Fin-1 was a Fedora VM running Fedora 37. This was simulated with an ISO image through VMWare software, and then implemented into the GNS3 topology. The IP address was manually configured to be static and 10.13.2.4/24. The device was then configured to be able to access the FTP server. No issues were found in the creation of the VM, or the implementation of the VM.

Cap-HR-1 was a Fedora VM running Fedora 37. This was simulated with an ISO image through VMWare software, and then implemented into the GNS3 topology. The IP address was manually configured to be static and 10.13.4.2/24. The device was then configured to be able to access the FTP server. No issues were found in the creation of the VM, or the implementation of the VM.

Cap-FTP-Serv-1 was a Fedora Server VM running Fedora 37. This was simulated with an ISO image through VMWare software, and then implemented into the GNS3 topology. The IP address was manually configured to be static and 10.13.7.2/24. The device was then configured to be able to act as an FTP server. On this FTP server, three “profiles” were created for each of the three other Fedora VMs. An additional subnet had to be created in order for the FTP server to be able to work, which deviated from the proposal. No other issues were found in the implementation of the VM.

The Kali machine was a simulated image running through OracleBox software, implemented into the GNS3 topology. One major issue that occurred initially was Kali, when simulated through VMWare was not able to be implemented into the topology. A solution was found by downloading the Kali “appliance” from the GNS3 marketplace, and running an image of Kali through there. After those steps were taken, Kali was successfully implemented into the network, and the tools Nmap, the Social Engineer’s

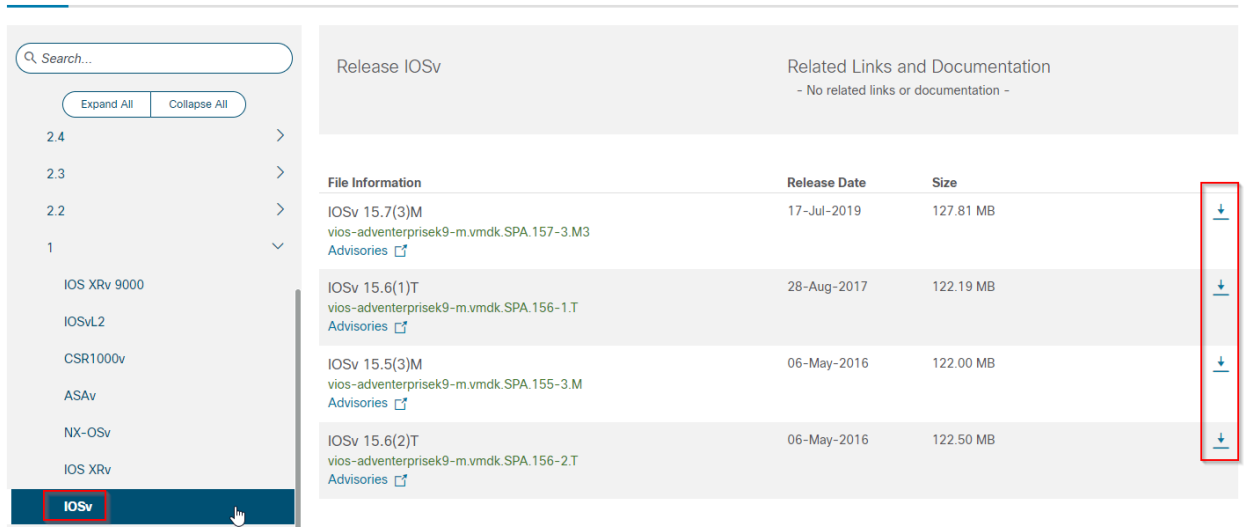
Toolkit, and Metasploit were all used to gain information and attempt to penetrate the network.

Project Description

Acquiring Router Images

1. Navigate to The Cisco Learning Network Store and purchase 'Cisco Modeling Labs - Personal' for \$199.00
2. Navigate to Cisco Downloads and download the files located under the 'ISOv' tab

Software Download



Search...

Expand All Collapse All

2.4 >
2.3 >
2.2 >
1 >

IOS XRv 9000
IOSvL2
CSR1000v
ASAv
NX-OSv
IOS XRv

IOSv

Release IOSv

Related Links and Documentation
- No related links or documentation -

File Information	Release Date	Size	
IOSv 15.7(3)M vios-adventerprisek9-m.vmdk.SPA.157-3.M3 Advisories	17-Jul-2019	127.81 MB	↓
IOSv 15.6(1)T vios-adventerprisek9-m.vmdk.SPA.156-1.T Advisories	28-Aug-2017	122.19 MB	↓
IOSv 15.5(3)M vios-adventerprisek9-m.vmdk.SPA.155-3.M Advisories	06-May-2016	122.00 MB	↓
IOSv 15.6(2)T vios-adventerprisek9-m.vmdk.SPA.156-2.T Advisories	06-May-2016	122.50 MB	↓

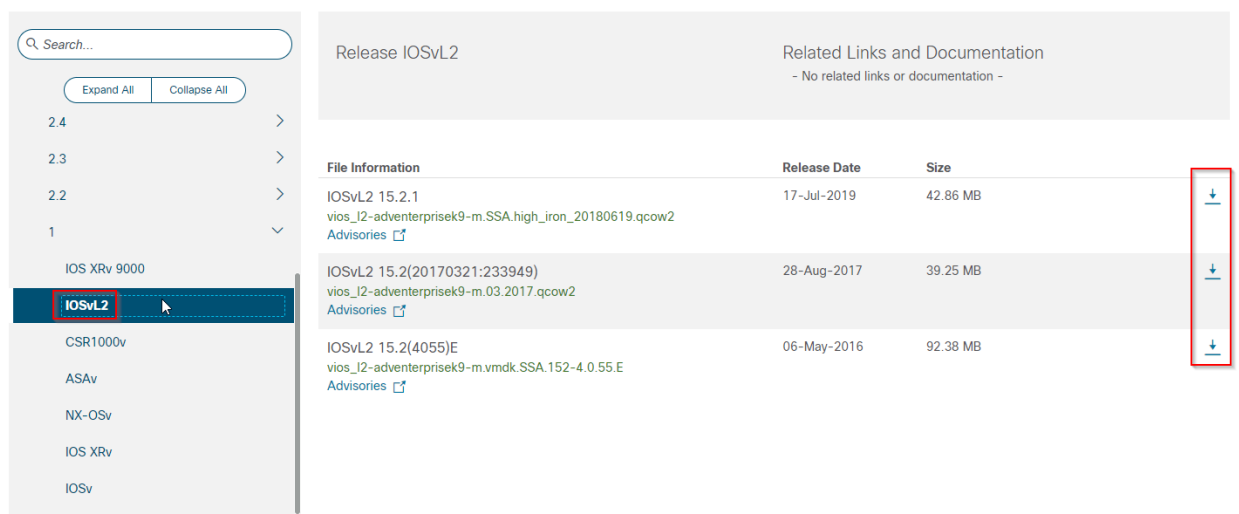
Figure 1.1 - Download page for Router Images

3. Save the images, and refer to **Adding Images to GNS3** for instructions on adding routers to the topology

Acquiring Switch Images

1. Navigate to The Cisco Learning Network Store and purchase 'Cisco Modeling Labs - Personal' for \$199.00
2. Navigate to Cisco Downloads and download the files located under the 'ISOvL2' tab

Software Download



Search...

Expand All Collapse All

2.4 >
2.3 >
2.2 >
1 >
IOS XRv 9000
IOSvL2
CSR1000v
ASAv
NX-OSv
IOS XRv
IOSv

Release IOSvL2

Related Links and Documentation
- No related links or documentation -

File Information	Release Date	Size
IOSvL2 15.2.1 vios_l2-adventerprisek9-m.SSA.high_iron_20180619.qcow2 Advisories	17-Jul-2019	42.86 MB
IOSvL2 15.2(20170321:233949) vios_l2-adventerprisek9-m.03.2017.qcow2 Advisories	28-Aug-2017	39.25 MB
IOSvL2 15.2(4055)E vios_l2-adventerprisek9-m.vmdk.SSA.152-4.0.55.E Advisories	06-May-2016	92.38 MB

Figure 1.1 - Download page for Switch images

3. Save the images, and refer to **Adding Images to GNS3** for instructions on adding switches to the topology

Adding Images to GNS3

1. Navigate to the GNS3 Marketplace and download the following two appliances:
 - a. Cisco IOSv
 - b. Cisco IOSvL2
2. Open the GNS3 application and navigate to the project/click 'Create New Project'
3. Click on 'File' and then select 'Import appliance'

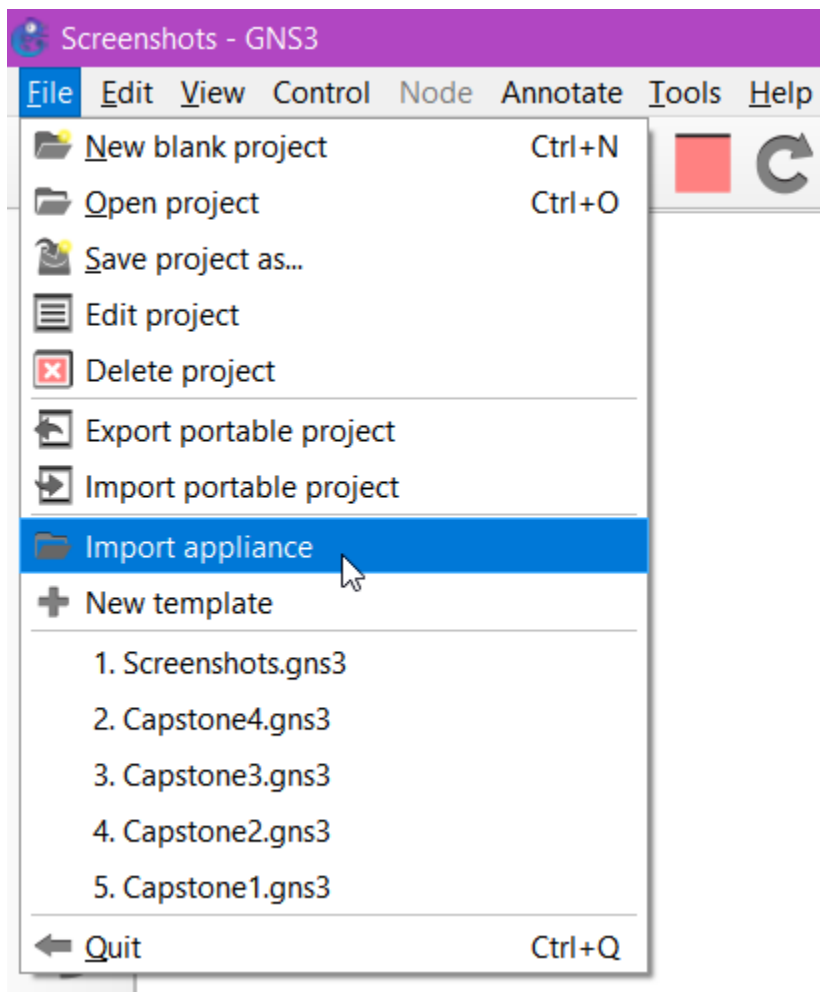


Figure 1.1 - Importing Appliance Menu

4. Select the GNS3 Appliance image (Either IOSv or IOSvL2), then click 'Open'
5. Select 'Install the application on the GNS3 VM' when prompted, then click 'Next'
6. The Qemu menu will auto-populate, click 'Next'

- When prompted, select the version that includes the previously downloaded IOSv file, and click 'Next'

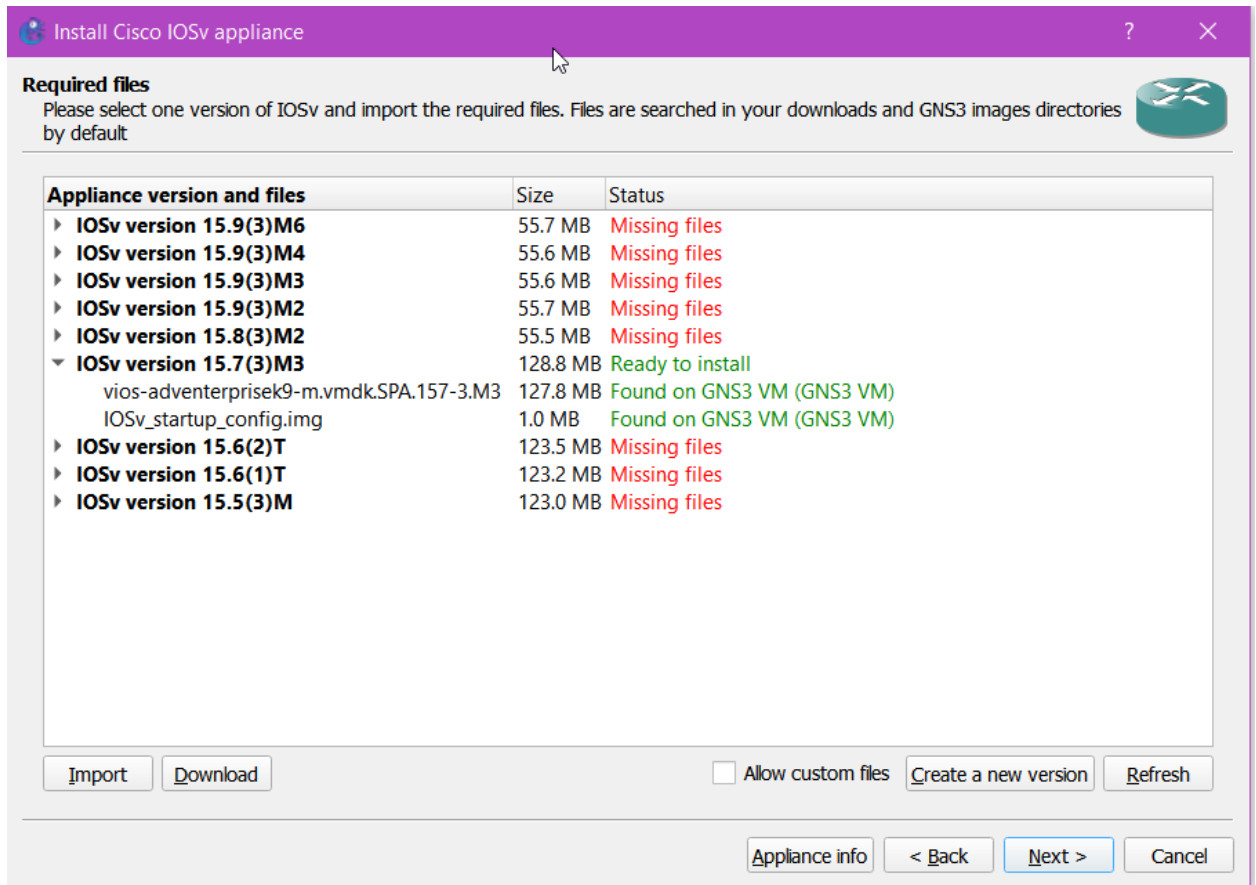


Figure 1.2 - Adding Personal Labs to GNS3

- When prompted, click 'Yes' to install the appliance, and then click 'Finish'
- From the GNS3 Topology Page, navigate to the devices tab, and then click and drag the newly added device to the topology

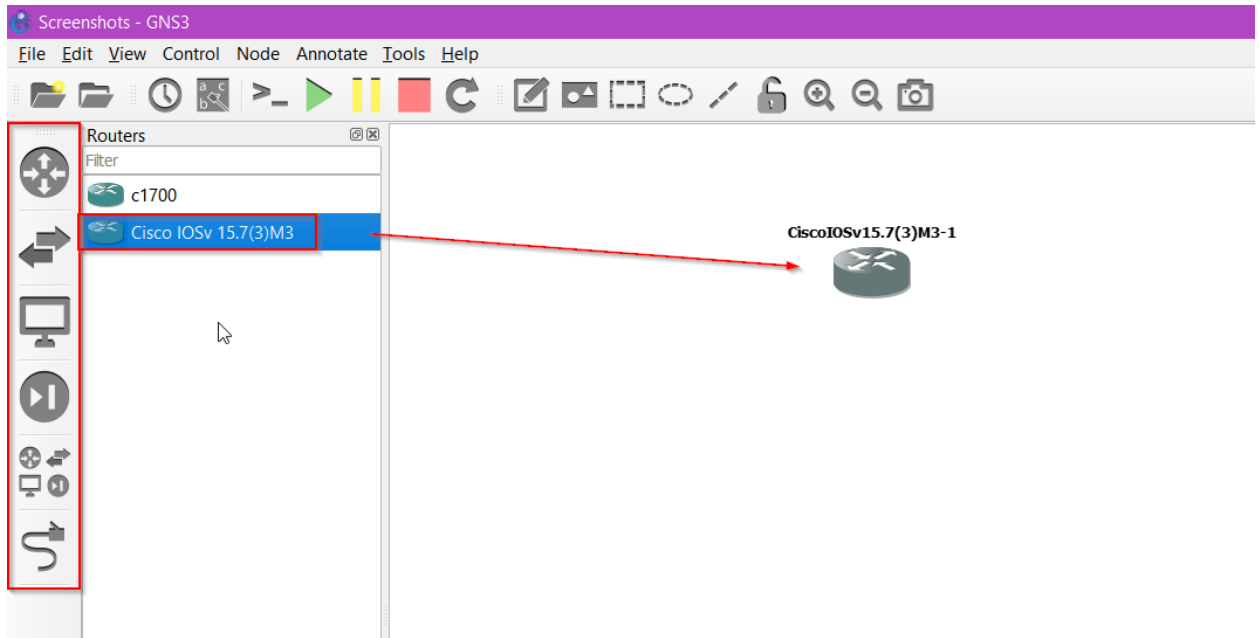


Figure 1.3 - Adding device to topology

10. Repeat steps 3-9 until all router/switch images have been successful added to the topology

Adding Virtual Machines to GNS3

1. Navigate to the 'End Devices' tab and select 'New Template', then select 'Manually create a new template'

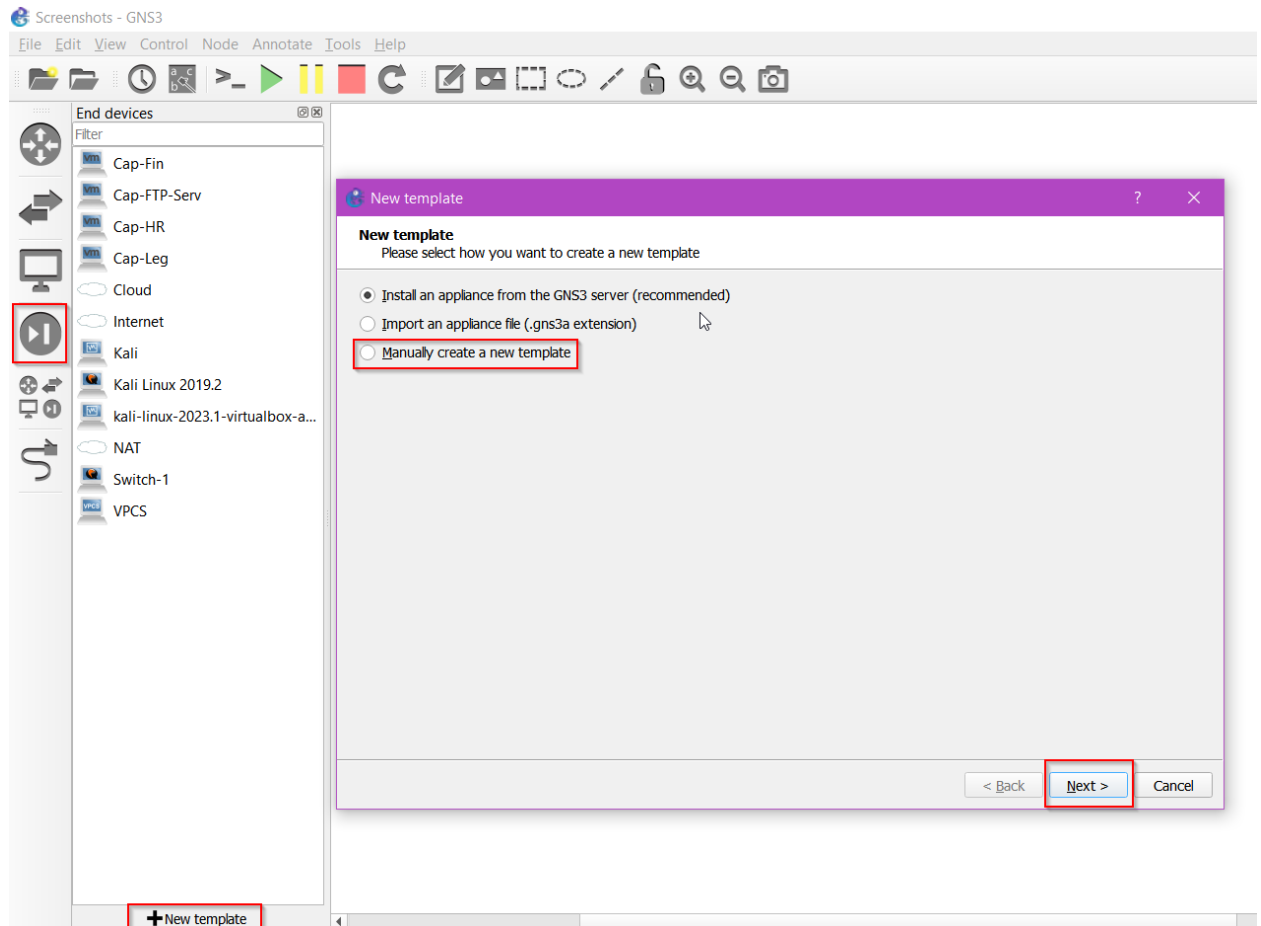


Figure 1.1 - Adding VM to GNS3

2. Select 'VMware VMs' and 'New' and then select the Virtual Machine you wish to add

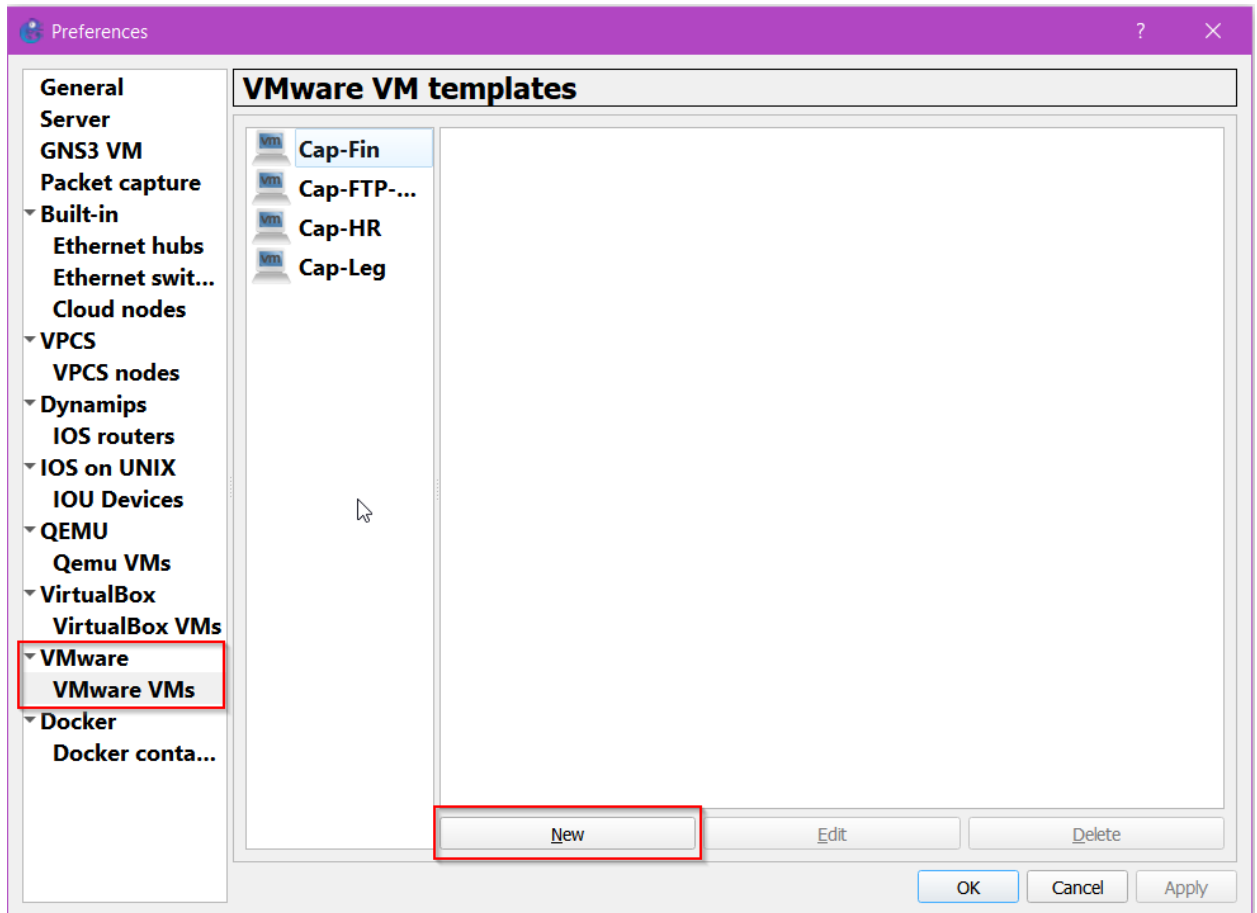


Figure 1.2 - Adding VM to GNS3

3. Select 'Run this VM on my computer' and then select the VM you wish to import.
Then click 'Finish'
4. From the 'End Devices' menu, click and drag the newly added VM to the topology page.
5. Repeat steps 1-4 until all VMs have been added to the topology

Configuring Router 1

1. From the GNS3 Topology, right-click the router to be configured and select 'Console' - a PuTTY terminal window will open
2. Apply the following commands to secure the router to the specifications of 'Simulating a Small Office Network for Penetration Testing'
 - a. Hostname R1-Leg
 - b. No ip domain-lookup
 - c. No banner incoming
 - d. No banner login
 - e. Int range g0/3
 - i. Shutdown
 - f. Int g0/2
 - i. Ip address 10.13.8.1 255.255.255.0
 - ii. No shutdown
 - g. Int g0/1
 - i. Ip address 10.13.5.1 255.255.255.0
 - ii. No shutdown
 - h. Int g0/0
 - i. Ip address 10.13.1.1 255.255.255.0
 - ii. No shutdown
 - i. Router rip
 - i. Version 2
 - ii. Network 10.0.0.0

- j. Ip access-list extended 101
 - i. Remark For stopping external email traffic
 - ii. Deny tcp any any eq smtp
 - iii. Deny tcp any any eq smtp log
 - iv. Permit icmp any any
 - v. Permit tcp any any
- k. Int g0/0
 - i. Ip access-group 101 out
- l. Line con 0
 - i. Password Sfp&df12023!
 - ii. Login
- m. Enable secret SSfp&df12023!
- n. Line vty 0 15
 - i. Password Secur3Pa55!
 - ii. Login
- o. Service password-encryption
- p. Banner motd #AUTHORIZED USERS ONLY - UNAUTHORIZED USERS
WILL BE HUNTED BY THE LAW!#
- q. Login block-for 120 attempts 2 within 60
- r. Login on-failure
- s. Copy running-config startup-config

Configuring Router 2

3. From the GNS3 Topology, right-click the router to be configured and select 'Console' - a PuTTY terminal window will open
4. Apply the following commands to secure the router to the specifications of 'Simulating a Small Office Network for Penetration Testing'
 - a. Hostname R2-Fin
 - b. No ip domain-lookup
 - c. No banner incoming
 - d. No banner login
 - e. Int g0/1
 - i. Ip address 10.13.5.2 255.255.255.0
 - ii. No shutdown
 - f. Int g0/0
 - i. Ip address 10.13.2.1 255.255.255.0
 - ii. No shutdown
 - g. Int g0/2
 - i. Ip address 10.13.6.1 255.255.255.0
 - ii. No shutdown
 - h. Int g0/3
 - i. shutdown
 - j. Router rip
 - i. Version 2
 - ii. Network 10.0.0.0

- k. Ip access-list extended 102
 - i. Remark For stopping external email traffic
 - ii. Deny tcp any any eq smtp
 - iii. Deny tcp any any eq smtp log
 - iv. Permit icmp any any
 - v. Permit tcp any any
- l. Int g0/0
 - i. Ip access-group 102 out
- m. Line con 0
 - i. Password Sfp&df12023!
 - ii. Login
- n. Enable secret SSfp&df12023!
- o. Line vty 0 15
 - i. Password Secur3Pa55!
 - ii. Login
- p. Service password-encryption
- q. Banner motd #AUTHORIZED USERS ONLY - UNAUTHORIZED USERS
WILL BE HUNTED BY THE LAW!#
- r. Login block-for 120 attempts 2 within 60
- s. Login on-failure
- t. Copy running-config startup-config

Configuring Router 3

5. From the GNS3 Topology, right-click the router to be configured and select 'Console' - a PuTTY terminal window will open
6. Apply the following commands to secure the router to the specifications of 'Simulating a Small Office Network for Penetration Testing'
 - a. Hostname R3-HR
 - b. No ip domain-lookup
 - c. No banner incoming
 - d. No banner login
 - e. Int g0/1
 - i. Ip address 10.13.7.1 255.255.255.0
 - ii. No shutdown
 - f. Int g0/0
 - i. Ip address 10.13.4.1 255.255.255.0
 - ii. No shutdown
 - g. Int g0/2
 - i. Ip address 10.13.6.2 255.255.255.0
 - ii. No shutdown
 - h. Int g0/3
 - i. shutdown
 - i. Router rip
 - i. Version 2
 - ii. Network 10.0.0.0

- j. Ip access-list extended 103
 - i. Remark For stopping external email traffic
 - ii. Deny tcp any any eq smtp
 - iii. Deny tcp any any eq smtp log
 - iv. Permit icmp any any
 - v. Permit tcp any any
- k. Int g0/0
 - i. Ip access-group 103 out
- l. Line con 0
 - i. Password Sfp&df12023!
 - ii. Login
- m. Enable secret SSfp&df12023!
- n. Line vty 0 15
 - i. Password Secur3Pa55!
 - ii. Login
- o. Service password-encryption
- p. Banner motd #AUTHORIZED USERS ONLY - UNAUTHORIZED USERS
WILL BE HUNTED BY THE LAW!#
- q. Login block-for 120 attempts 2 within 60
- r. Login on-failure
- s. Copy running-config startup-config

Configuring the Switch

7. From the GNS3 Topology, right-click the router to be configured and select 'Console' - a PuTTY terminal window will open
8. Apply the following commands to secure the router to the specifications of 'Simulating a Small Office Network for Penetration Testing'
 - a. Hostname Sw-1
 - b. No ip domain-lookup
 - c. Line con 0
 - i. Password Sfp&df12023!
 - d. Enable secret SSfp&df12023!
 - e. Line vty 0 15
 - i. Password Secur3Pa55!
 - ii. Login
 - f. Banner motd #AUTHORIZED USERS ONLY - UNAUTHORIZED USERS
WILL BE HUNTED BY THE LAW!#
 - g. Service password-encryption
 - h. Vlan 10
 - i. Name Traffic
 - i. Vlan 30
 - i. Name Unused
 - j. Int vlan 10
 - i. Ip address 10.13.2.2 255.255.255.0
 - ii. No shutdown

- k. Int g0/0-1
 - i. Switchport mode access
 - ii. Switchport access vlan 10
- l. Int range g0/2-3
 - i. Switchport mode access
 - ii. Switchport access vlan 30
- m. Int range g1/0-3
 - i. Switchport mode access
 - ii. Switchport access vlan 30
- n. Int range g2/0-3
 - i. Switchport mode access
 - ii. Switchport access vlan 30
- o. Int range g3/1-3
 - i. Switchport mode access
 - ii. Switchport access vlan 30
- p. Copy running-config startup-config

Configuring Cap-Leg-1 VM

1. *Optional* install FileZila from applications store
2. Navigate to 'Network Settings' from the Fedora Desktop
3. Click on the gear icon next to the network adapter
4. Apply the following
 - a. IP Address - 10.13.1.2
 - b. Subnet Mask - 255.255.255.0
 - c. Default Gateway - 10.13.1.1
5. Click 'Apply' and restart the virtual machine to ensure the configurations save/are updated

Configuring Cap-Fin-1 VM

1. *Optional* install FileZila from applications store
2. Navigate to 'Network Settings' from the Fedora Desktop
3. Click on the gear icon next to the network adapter
4. Apply the following
 - a. IP Address - 10.13.2.4
 - b. Subnet Mask - 255.255.255.0
 - c. Default Gateway - 10.13.2.1
5. Click 'Apply' and restart the virtual machine to ensure the configurations save/are updated

Configuring Cap-HR-1 VM

1. *Optional* install FileZila from applications store
2. Navigate to 'Network Settings' from the Fedora Desktop
3. Click on the gear icon next to the network adapter
4. Apply the following
 - a. IP Address - 10.13.4.2
 - b. Subnet Mask - 255.255.255.0
 - c. Default Gateway - 10.13.4.1
5. Click 'Apply' and restart the virtual machine to ensure the configurations save/are updated

Configuring FTP-Serv-1

1. Enter the following commands to configure the FTP Server
 - a. Sudo apt install vsftpd
 - b. sudo systemctl start vsftpd
 - c. sudo systemctl enable vsftpd
2. Uncomment the following from the /etc/vsftpd.conf file
 - a. sudo nano /etc/vsftpd.conf
 - i. Anonymous_enable=NO
 - ii. local_enable=YES
 - iii. write_enable=YES
 - iv. userlist_enable=YES
 - v. userlist_file=/etc/vsftpd/vsftpd.userlist
 - vi. userlist_deny=NO
 - b. sudo service vsftpd restart
3. Enter the following commands to continue configuring the FTP Server
 - a. Sudo passwd root FTPServadminpa55!
 - b. sudo nmcli connection modify 'eth0' IPv4.address 10.13.7.2
255.255.255.0
 - c. sudo nmcli connection modify 'eth0' IPv4.gateway 10.13.7.1
 - d. usermod Legal -a -G wheel
 - i. Sudo passwd Legal Legal
 - e. Usermod Fin -a -G wheel
 - i. Sudo passwd Fin Fin
 - f. Usermod HR -a -G wheel

- i. Sudo passwd HR HR
 - g. Vi /etc/vsftpd/vsftpd.userlist
 - h. echo "Legal" | sudo tee -a /etc/vsftpd/vsftpd.userlist
 - i. echo "Fin" | sudo tee -a /etc/vsftpd/vsftpd.userlist
 - j. echo "HR" | sudo tee -a /etc/vsftpd/vsftpd.userlist
4. Login as Legal
- a. Mkdir FTP
 - b. **Create Sample documents using command 'vi FILENAME'
5. Login as Fin
- a. Mkdir FTP
 - b. **Create Sample documents using command 'vi FILENAME'
6. Login as HR
- a. Mkdir FTP
 - b. **Create Sample documents using command 'vi FILENAME'

Adding Kai to GNS3

1. Download ISO image of Kali Linux from kali.com for VIRTUALBOX



Figure 1.1 - Download page for Kali Linux

2. Navigate to the GNS3 Marketplace and download the following appliance
 - a. Kali Linux
3. Refer to **Adding Images to GNS3** to install Kali and add it to the topology
4. Update the network settings to the following:
 - a. IP address - 10.13.8.1
 - b. Subnetmask - 255.255.255.0
 - c. Default Gateway 10.13.8.1
5. Kali comes equipped with a variety of pentesting tools; to fully replicate Simulating a Small Office Network for Penetration Testing, open the following:

- a. Metasploit
 - b. Social Engineer's Toolkit
 - c. Terminal window and enter nmap commands
6. For further instructions on penetration testing - view **Adkins - 491_001 - Testing Documentation Nmap Documentation, Metasploit Documentation, and Social Engineer's Toolkit Documentation**

Testing Documentation

Routing Table

The following is the complete routing table for the project:

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
R1-Leg	G0/0	10.13.1.1	255.255.255.0	
R1-Leg	G0/1	10.13.5.1	255.255.255.0	
R1-Leg	G0/2	10.13.8.1	255.255.255.0	
Cap-Leg-1	Eth0	10.13.1.2	255.255.255.0	10.13.1.1
Kali	Eth0	10.13.8.3	255.255.255.0	10.13.8.1
R2-Fin	G0/0	10.13.2.1	255.255.255.0	
R2-Fin	G0/1	10.13.5.2	255.255.255.0	
R2-Fin	G0/2	10.13.6.1	255.255.255.0	
Sw-1	Vlan 10	10.13.2.2	255.255.255.0	10.13.2.1
Cap-Fin-1	Eth0	10.13.2.4	255.255.255.0	10.13.2.1
R3-HR	G0/0	10.13.7.1	255.255.255.0	
R3-HR	G0/1	10.13.4.1	255.255.255.0	
R3-HR	G0/2	10.13.6.2	255.255.255.0	
Cap-FTP-Serv-1	Eth0	10.13.7.2	255.255.255.0	10.13.7.1
Cap-HR-1	Eth0	10.13.4.2	255.255.255.0	10.13.4.1

Table 1.1 - Routing Table

As seen in the table above, the device name, the interface it is connected through, the IP address, the Subnet Mask, and the default gateway (if present) has all been included.

Ping Tests: Cap-Leg-1

The Fedora VM named Cap-Leg-1, a part of the 10.13.1.0/24 subnet, was configured with the IP address 10.13.1.2/24. To show that the device had ping connectivity, the ping command was issued from the terminal on the Cap-Leg-1 VM to the three other end devices in the network: Cap-Fin-1, Cap-HR-1, and Cap-FTP-Serv-1. The below screenshots show the output of the successful ping commands.

Command: Ping 10.13.2.4: Cap-Fin-1

```
[cap-leg@fedora ~]$ ping 10.13.2.4
PING 10.13.2.4 (10.13.2.4) 56(84) bytes of data.
64 bytes from 10.13.2.4: icmp_seq=1 ttl=62 time=10.0 ms
64 bytes from 10.13.2.4: icmp_seq=2 ttl=62 time=8.52 ms
64 bytes from 10.13.2.4: icmp_seq=3 ttl=62 time=8.40 ms
64 bytes from 10.13.2.4: icmp_seq=4 ttl=62 time=10.1 ms
^C
--- 10.13.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 8.399/9.267/10.114/0.811 ms
[cap-leg@fedora ~]$
```

Figure 1.1 - Output of ping to Cap-Fin-1

Command: Ping 10.13.4.2: Cap-HR-1

```
[cap-leg@fedora ~]$ ping 10.13.4.2
PING 10.13.4.2 (10.13.4.2) 56(84) bytes of data.
64 bytes from 10.13.4.2: icmp_seq=1 ttl=61 time=6.78 ms
64 bytes from 10.13.4.2: icmp_seq=2 ttl=61 time=5.73 ms
64 bytes from 10.13.4.2: icmp_seq=3 ttl=61 time=7.43 ms
64 bytes from 10.13.4.2: icmp_seq=4 ttl=61 time=7.67 ms
^C
--- 10.13.4.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 5.730/6.903/7.669/0.750 ms
[cap-leg@fedora ~]$
```

Figure 1.2 - Output of ping to Cap-HR-1

Command: Ping 10.13.7.2: Cap-FTP-Serv-1

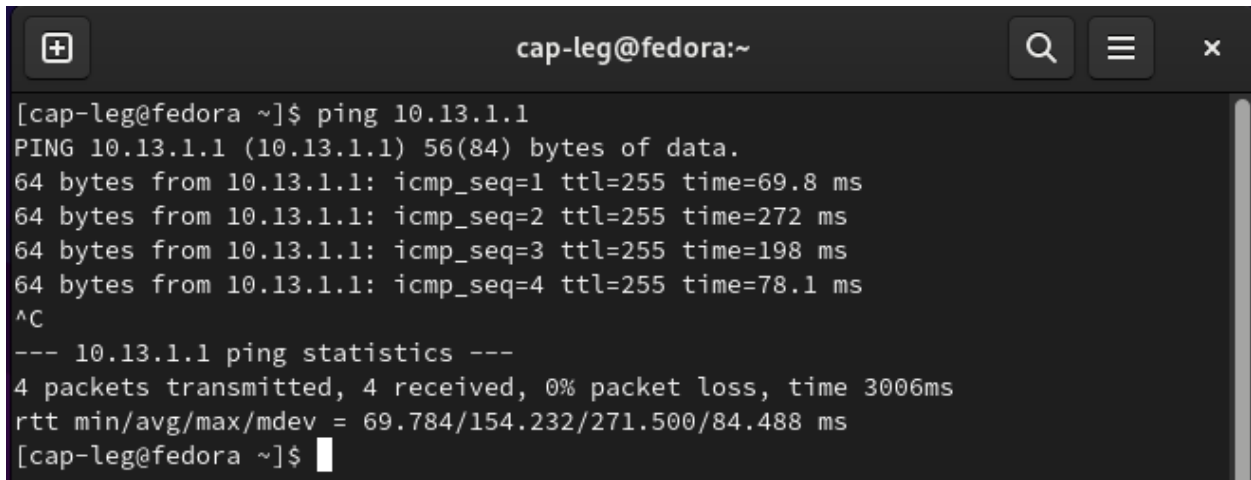
```
[cap-leg@fedora ~]$ ping 10.13.7.2
PING 10.13.7.2 (10.13.7.2) 56(84) bytes of data.
64 bytes from 10.13.7.2: icmp_seq=1 ttl=61 time=5.69 ms
64 bytes from 10.13.7.2: icmp_seq=2 ttl=61 time=7.60 ms
64 bytes from 10.13.7.2: icmp_seq=3 ttl=61 time=6.67 ms
64 bytes from 10.13.7.2: icmp_seq=4 ttl=61 time=7.33 ms
^C
--- 10.13.7.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 5.689/6.821/7.604/0.736 ms
[cap-leg@fedora ~]$
```

Figure 1.3 - Output of ping to Cap-FTP-Serv-1

As seen in the screenshots, the command was issued and on the terminal window, the results are: 64 bytes from *destination*, as well as the ICMP sequence number, the time to live, and the time it took for the ping to reach. At the bottom, the statistics show all 4 packets were received, none were lost, and statistics about the time it took to send the pings.

In addition to the ping tests sent to the other Fedora VMs, the ping command was also issued to the interfaces of the routers and the switch across the network to verify connectivity. The results of the ping tests can be seen in the screenshots below.

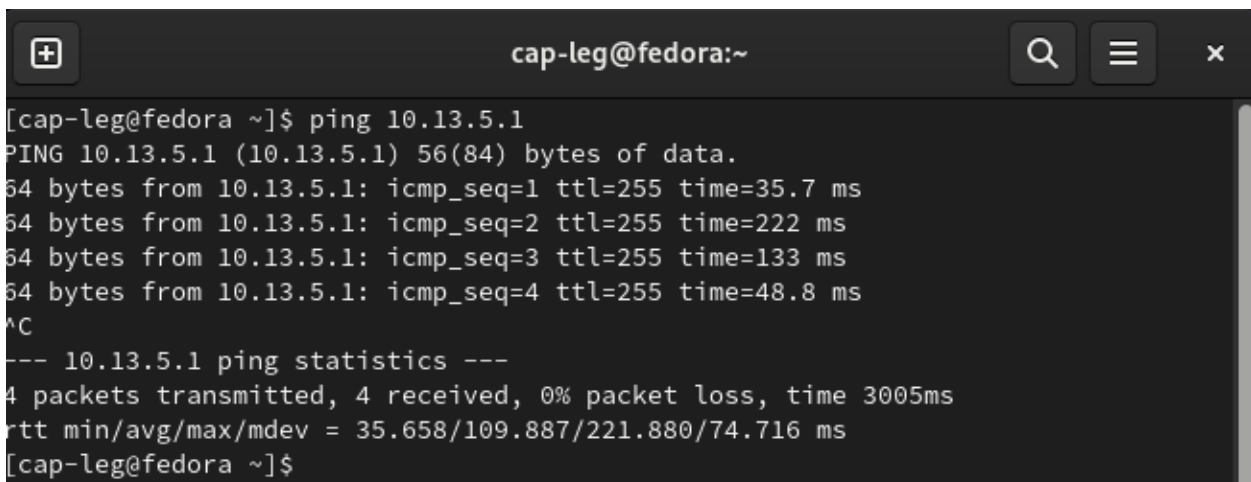
Command: Ping 10.13.1.1: R1-Leg G0/0

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.1.1. The output displays four successful ping attempts with varying response times and a summary statistics block at the bottom.

```
[cap-leg@fedora ~]$ ping 10.13.1.1
PING 10.13.1.1 (10.13.1.1) 56(84) bytes of data.
64 bytes from 10.13.1.1: icmp_seq=1 ttl=255 time=69.8 ms
64 bytes from 10.13.1.1: icmp_seq=2 ttl=255 time=272 ms
64 bytes from 10.13.1.1: icmp_seq=3 ttl=255 time=198 ms
64 bytes from 10.13.1.1: icmp_seq=4 ttl=255 time=78.1 ms
^C
--- 10.13.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 69.784/154.232/271.500/84.488 ms
[cap-leg@fedora ~]$
```

Figure 1.4 - Output of ping to R1-Leg: Interface G0/0

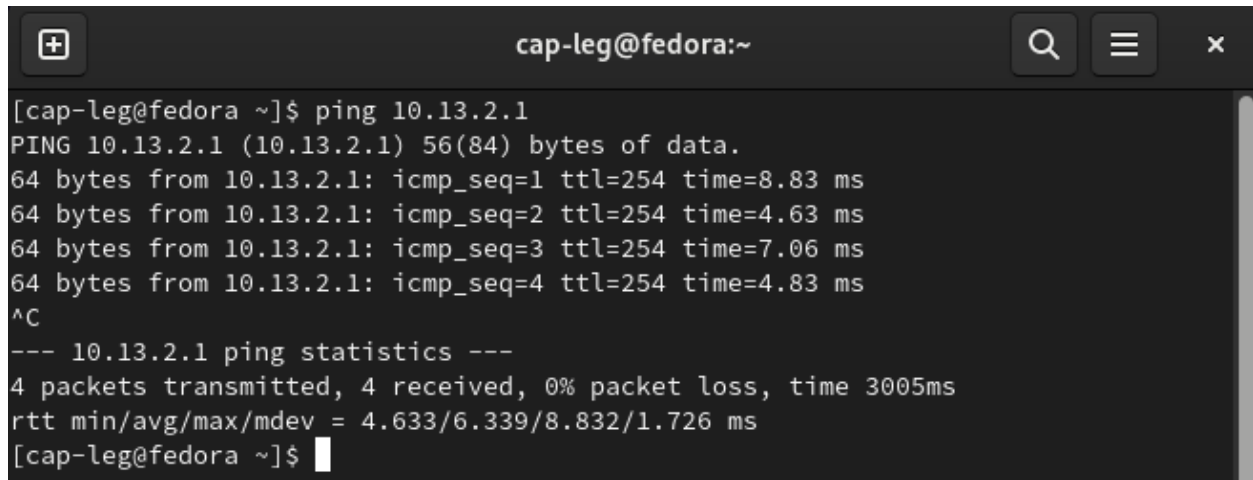
Command: Ping 10.13.5.1: R1-Leg G0/1

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.5.1. The output displays four successful ping attempts with varying response times and a summary statistics block at the bottom.

```
[cap-leg@fedora ~]$ ping 10.13.5.1
PING 10.13.5.1 (10.13.5.1) 56(84) bytes of data.
64 bytes from 10.13.5.1: icmp_seq=1 ttl=255 time=35.7 ms
64 bytes from 10.13.5.1: icmp_seq=2 ttl=255 time=222 ms
64 bytes from 10.13.5.1: icmp_seq=3 ttl=255 time=133 ms
64 bytes from 10.13.5.1: icmp_seq=4 ttl=255 time=48.8 ms
^C
--- 10.13.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 35.658/109.887/221.880/74.716 ms
[cap-leg@fedora ~]$
```

Figure 1.5 - Output of ping to R1-Leg: Interface G0/1

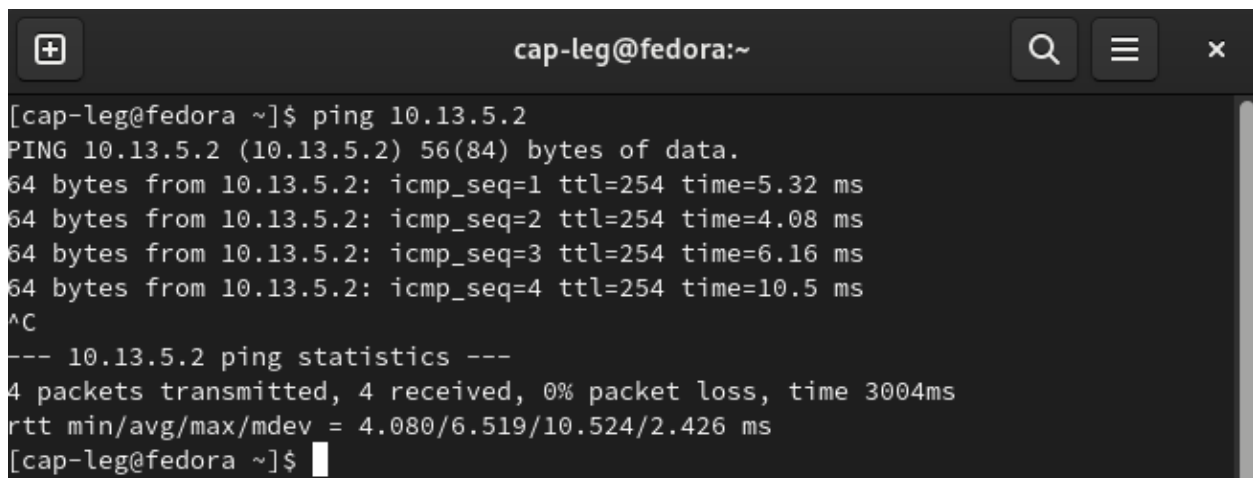
Command: Ping 10.13.2.1: R2-Fin G0/0

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.2.1. The output displays four successful ping attempts with varying round-trip times (8.83 ms, 4.63 ms, 7.06 ms, 4.83 ms) and a summary of ping statistics: 4 packets transmitted, 4 received, 0% packet loss, and a total time of 3005ms. The RTT statistics are: min/avg/max/mdev = 4.633/6.339/8.832/1.726 ms.

```
[cap-leg@fedora ~]$ ping 10.13.2.1
PING 10.13.2.1 (10.13.2.1) 56(84) bytes of data.
64 bytes from 10.13.2.1: icmp_seq=1 ttl=254 time=8.83 ms
64 bytes from 10.13.2.1: icmp_seq=2 ttl=254 time=4.63 ms
64 bytes from 10.13.2.1: icmp_seq=3 ttl=254 time=7.06 ms
64 bytes from 10.13.2.1: icmp_seq=4 ttl=254 time=4.83 ms
^C
--- 10.13.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 4.633/6.339/8.832/1.726 ms
[cap-leg@fedora ~]$
```

Figure 1.6 - Output of ping to R2-Fin: Interface G0/0

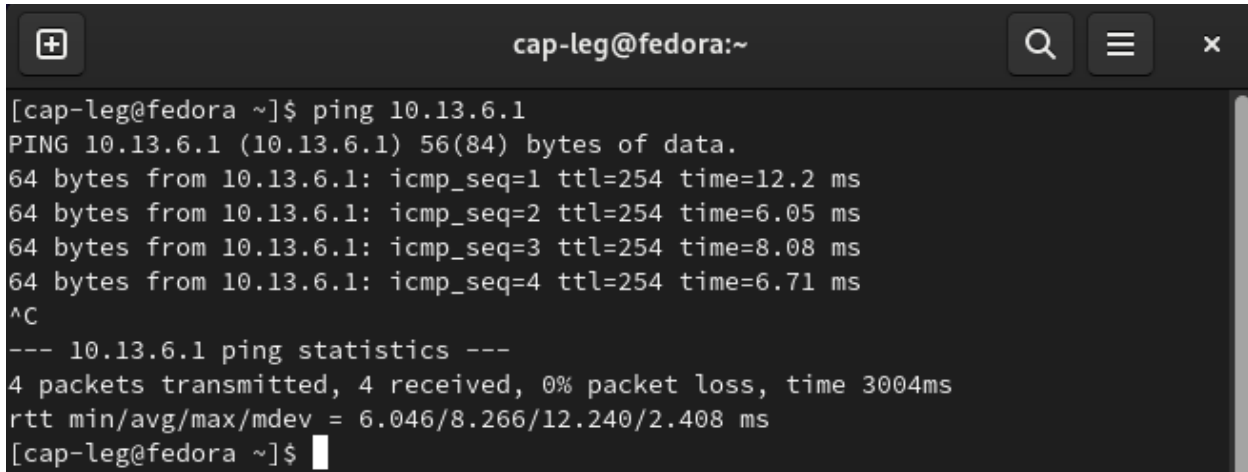
Command: Ping 10.13.5.2: R2-Fin G0/1

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.5.2. The output displays four successful ping attempts with round-trip times of 5.32 ms, 4.08 ms, 6.16 ms, and 10.5 ms. A summary of ping statistics shows 4 packets transmitted, 4 received, 0% packet loss, and a total time of 3004ms. The RTT statistics are: min/avg/max/mdev = 4.080/6.519/10.524/2.426 ms.

```
[cap-leg@fedora ~]$ ping 10.13.5.2
PING 10.13.5.2 (10.13.5.2) 56(84) bytes of data.
64 bytes from 10.13.5.2: icmp_seq=1 ttl=254 time=5.32 ms
64 bytes from 10.13.5.2: icmp_seq=2 ttl=254 time=4.08 ms
64 bytes from 10.13.5.2: icmp_seq=3 ttl=254 time=6.16 ms
64 bytes from 10.13.5.2: icmp_seq=4 ttl=254 time=10.5 ms
^C
--- 10.13.5.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 4.080/6.519/10.524/2.426 ms
[cap-leg@fedora ~]$
```

Figure 1.7 - Output of ping to R2-Fin: Interface G0/1

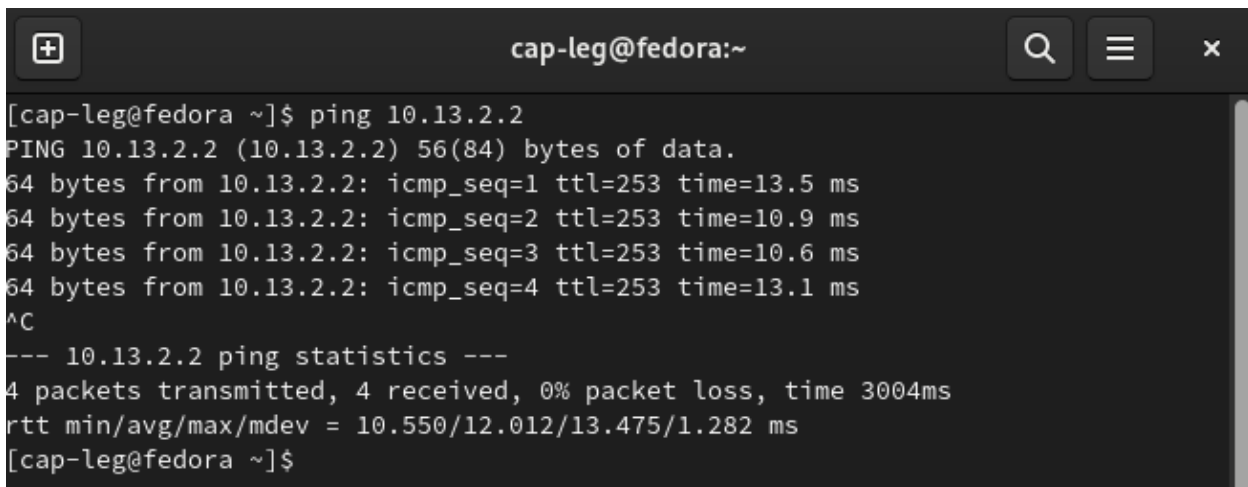
Command: Ping 10.13.6.1: R2-Fin G0/2

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.6.1. The output displays four successful ping attempts with varying response times and a summary of ping statistics. The window includes standard Linux terminal window controls like search, menu, and close buttons.

```
[cap-leg@fedora ~]$ ping 10.13.6.1
PING 10.13.6.1 (10.13.6.1) 56(84) bytes of data.
64 bytes from 10.13.6.1: icmp_seq=1 ttl=254 time=12.2 ms
64 bytes from 10.13.6.1: icmp_seq=2 ttl=254 time=6.05 ms
64 bytes from 10.13.6.1: icmp_seq=3 ttl=254 time=8.08 ms
64 bytes from 10.13.6.1: icmp_seq=4 ttl=254 time=6.71 ms
^C
--- 10.13.6.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 6.046/8.266/12.240/2.408 ms
[cap-leg@fedora ~]$
```

Figure 1.8 - Output of ping to R2-Fin: Interface G0/2

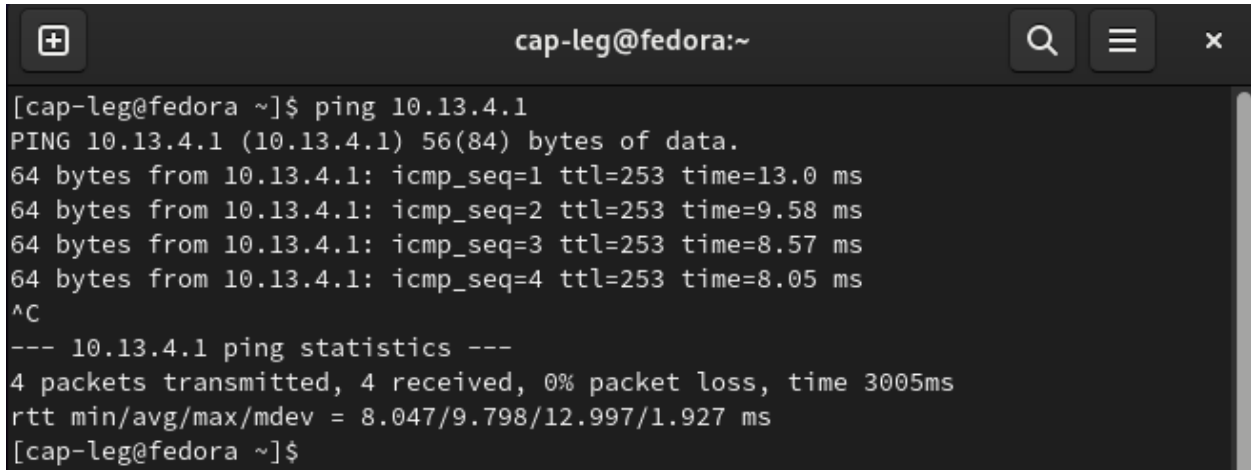
Command: Ping 10.13.2.2: Sw-1

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.2.2. The output displays four successful ping attempts with varying response times and a summary of ping statistics. The window includes standard Linux terminal window controls like search, menu, and close buttons.

```
[cap-leg@fedora ~]$ ping 10.13.2.2
PING 10.13.2.2 (10.13.2.2) 56(84) bytes of data.
64 bytes from 10.13.2.2: icmp_seq=1 ttl=253 time=13.5 ms
64 bytes from 10.13.2.2: icmp_seq=2 ttl=253 time=10.9 ms
64 bytes from 10.13.2.2: icmp_seq=3 ttl=253 time=10.6 ms
64 bytes from 10.13.2.2: icmp_seq=4 ttl=253 time=13.1 ms
^C
--- 10.13.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 10.550/12.012/13.475/1.282 ms
[cap-leg@fedora ~]$
```

Figure 1.9 - Output of ping to Sw-1

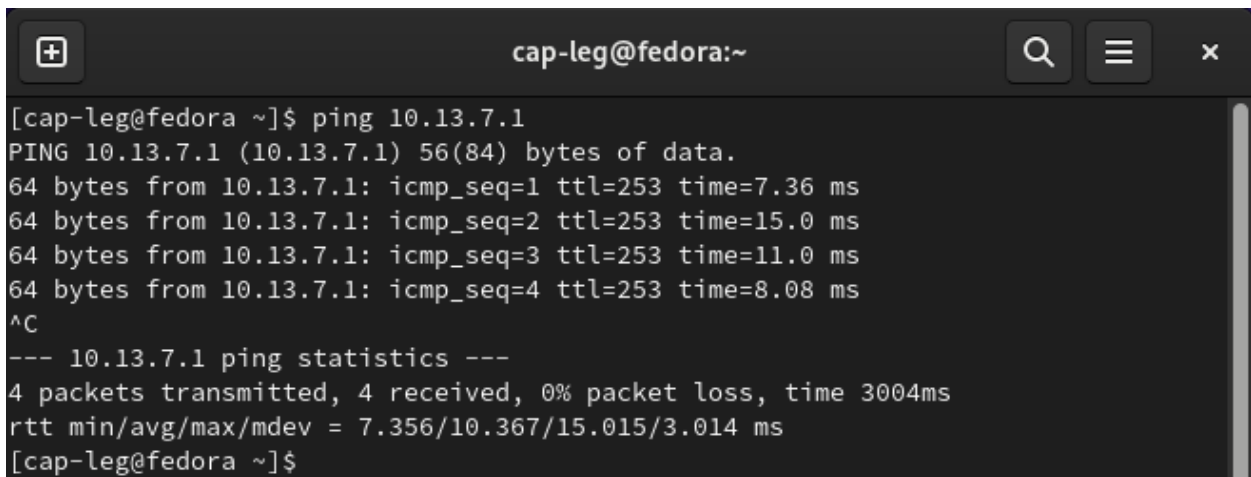
Command: Ping 10.13.4.1: R3-HR G0/0

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.4.1. The output shows four successful ping requests with varying response times and a summary of ping statistics.

```
[cap-leg@fedora ~]$ ping 10.13.4.1
PING 10.13.4.1 (10.13.4.1) 56(84) bytes of data.
64 bytes from 10.13.4.1: icmp_seq=1 ttl=253 time=13.0 ms
64 bytes from 10.13.4.1: icmp_seq=2 ttl=253 time=9.58 ms
64 bytes from 10.13.4.1: icmp_seq=3 ttl=253 time=8.57 ms
64 bytes from 10.13.4.1: icmp_seq=4 ttl=253 time=8.05 ms
^C
--- 10.13.4.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 8.047/9.798/12.997/1.927 ms
[cap-leg@fedora ~]$
```

Figure 1.10 - Output of ping to R3-HR: Interface G0/0

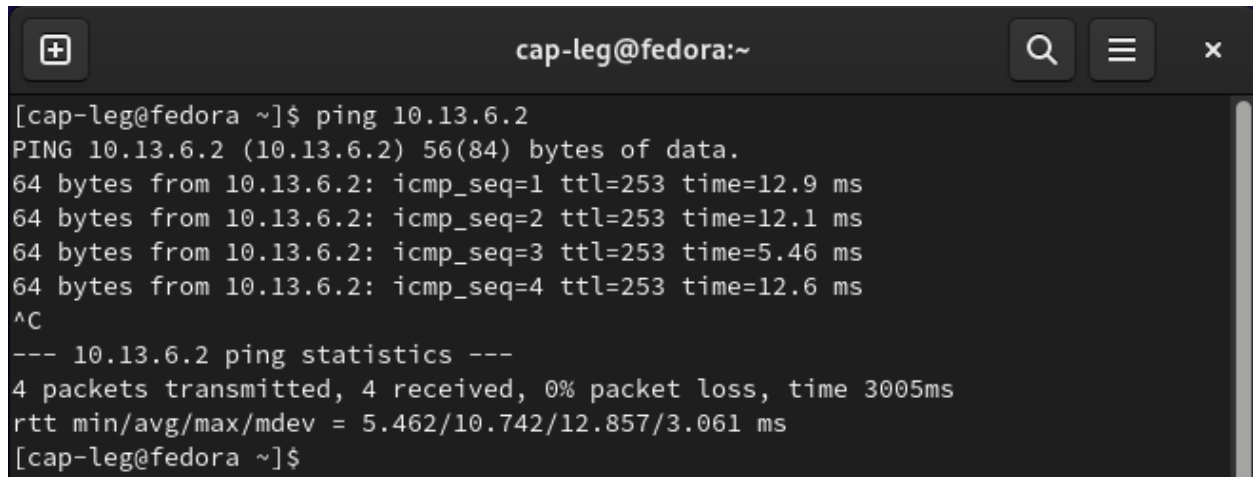
Command: Ping 10.13.7.1: R3-HR G0/1

A terminal window titled 'cap-leg@fedora:~' showing the output of a ping command to 10.13.7.1. The output shows four successful ping requests with varying response times and a summary of ping statistics.

```
[cap-leg@fedora ~]$ ping 10.13.7.1
PING 10.13.7.1 (10.13.7.1) 56(84) bytes of data.
64 bytes from 10.13.7.1: icmp_seq=1 ttl=253 time=7.36 ms
64 bytes from 10.13.7.1: icmp_seq=2 ttl=253 time=15.0 ms
64 bytes from 10.13.7.1: icmp_seq=3 ttl=253 time=11.0 ms
64 bytes from 10.13.7.1: icmp_seq=4 ttl=253 time=8.08 ms
^C
--- 10.13.7.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 7.356/10.367/15.015/3.014 ms
[cap-leg@fedora ~]$
```

Figure 1.11 - Output of ping to R3-HR: Interface G0/1

Command: Ping 10.13.6.2: R3-HR G0/2

A terminal window titled 'cap-leg@fedora:~' with search, menu, and close buttons. The terminal shows the execution of a ping command to 10.13.6.2. The output displays four successful ping attempts with varying response times and a final summary showing 0% packet loss.

```
[cap-leg@fedora ~]$ ping 10.13.6.2
PING 10.13.6.2 (10.13.6.2) 56(84) bytes of data:
64 bytes from 10.13.6.2: icmp_seq=1 ttl=253 time=12.9 ms
64 bytes from 10.13.6.2: icmp_seq=2 ttl=253 time=12.1 ms
64 bytes from 10.13.6.2: icmp_seq=3 ttl=253 time=5.46 ms
64 bytes from 10.13.6.2: icmp_seq=4 ttl=253 time=12.6 ms
^C
--- 10.13.6.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 5.462/10.742/12.857/3.061 ms
[cap-leg@fedora ~]$
```

Figure 1.12 - Output of ping to R3-HR: Interface G0/2

The above ping tests are all successful with no packet loss, indicating connectivity.

Ping Tests: Cap-Fin-1

The Fedora VM named Cap-Fin-1, a part of the 10.13.2.0/24 subnet, was configured with the IP address 10.13.2.2/24. To show that the device had ping connectivity, the ping command was issued from the terminal on the Cap-Fin-1 VM to the three other end devices in the network: Cap-Leg-1, Cap-HR-1, and Cap-FTP-Serv-1. The below screenshots show the output of the successful ping commands.

Command: Ping 10.13.1.2: Cap-Leg-1

```
[cap-fin@fedora ~]$ ping 10.13.1.2
PING 10.13.1.2 (10.13.1.2) 56(84) bytes of data.
64 bytes from 10.13.1.2: icmp_seq=1 ttl=62 time=12.8 ms
64 bytes from 10.13.1.2: icmp_seq=2 ttl=62 time=9.52 ms
64 bytes from 10.13.1.2: icmp_seq=3 ttl=62 time=12.5 ms
64 bytes from 10.13.1.2: icmp_seq=4 ttl=62 time=12.4 ms
^C
--- 10.13.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 9.523/11.799/12.790/1.322 ms
```

Figure 2.1 - Output of ping to Cap-Leg-1

Command: Ping 10.13.4.2: Cap-HR-1

```
[cap-fin@fedora ~]$ ping 10.13.4.2
PING 10.13.4.2 (10.13.4.2) 56(84) bytes of data.
64 bytes from 10.13.4.2: icmp_seq=1 ttl=62 time=21.0 ms
64 bytes from 10.13.4.2: icmp_seq=2 ttl=62 time=107 ms
64 bytes from 10.13.4.2: icmp_seq=3 ttl=62 time=10.5 ms
64 bytes from 10.13.4.2: icmp_seq=4 ttl=62 time=12.4 ms
^C
--- 10.13.4.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 10.513/37.658/106.775/40.099 ms
```

Figure 2.2 - Output of ping to Cap-HR-1

Command: Ping 10.13.7.2: Cap-FTP-Serv-1

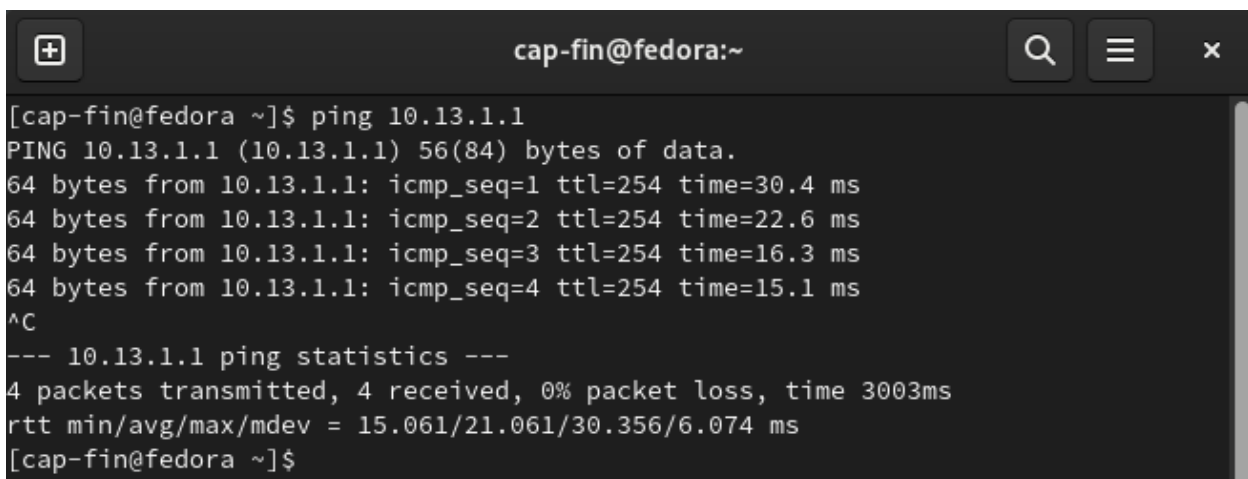
```
[cap-fin@fedora ~]$ ping 10.13.7.2
PING 10.13.7.2 (10.13.7.2) 56(84) bytes of data.
64 bytes from 10.13.7.2: icmp_seq=1 ttl=62 time=14.8 ms
64 bytes from 10.13.7.2: icmp_seq=2 ttl=62 time=15.3 ms
64 bytes from 10.13.7.2: icmp_seq=3 ttl=62 time=12.4 ms
64 bytes from 10.13.7.2: icmp_seq=4 ttl=62 time=17.2 ms
^C
--- 10.13.7.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 12.398/14.945/17.226/1.721 ms
[cap-fin@fedora ~]$
```

Figure 2.3 - Output of ping to Cap-FTP-Serv-1

The pings are all successful with no lost packets meaning network connectivity was obtained.

In addition to the above ping tests, the ping command was also issued to the router and switch interfaces within the network. The below screenshots verify this.

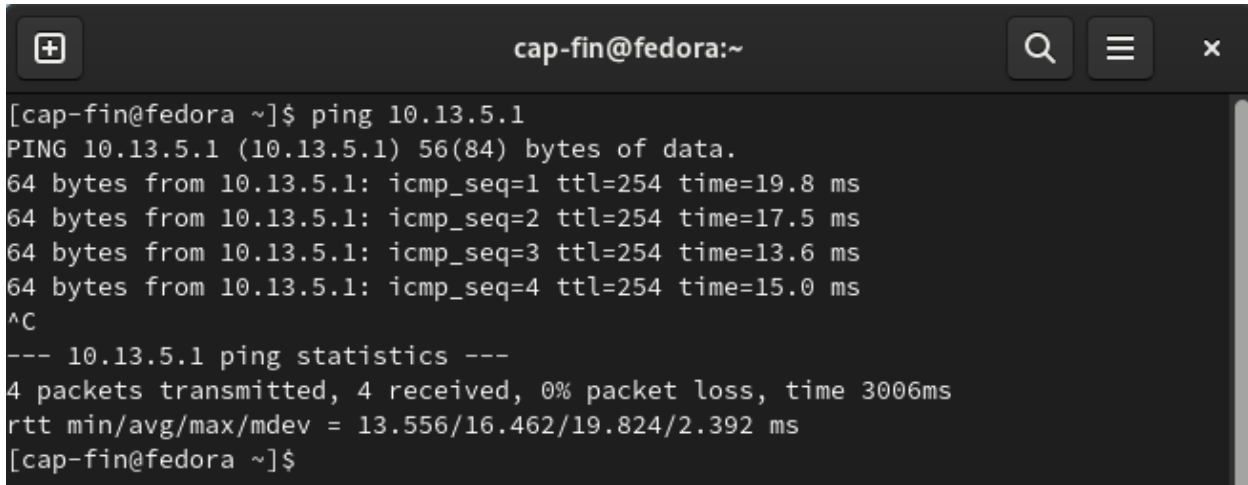
Command: Ping 10.13.1.1: R1-Leg - Interface G0/0



```
cap-fin@fedora:~
[cap-fin@fedora ~]$ ping 10.13.1.1
PING 10.13.1.1 (10.13.1.1) 56(84) bytes of data.
64 bytes from 10.13.1.1: icmp_seq=1 ttl=254 time=30.4 ms
64 bytes from 10.13.1.1: icmp_seq=2 ttl=254 time=22.6 ms
64 bytes from 10.13.1.1: icmp_seq=3 ttl=254 time=16.3 ms
64 bytes from 10.13.1.1: icmp_seq=4 ttl=254 time=15.1 ms
^C
--- 10.13.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 15.061/21.061/30.356/6.074 ms
[cap-fin@fedora ~]$
```

Figure 2.4 - Output of ping to R1-Leg: Interface G0/0

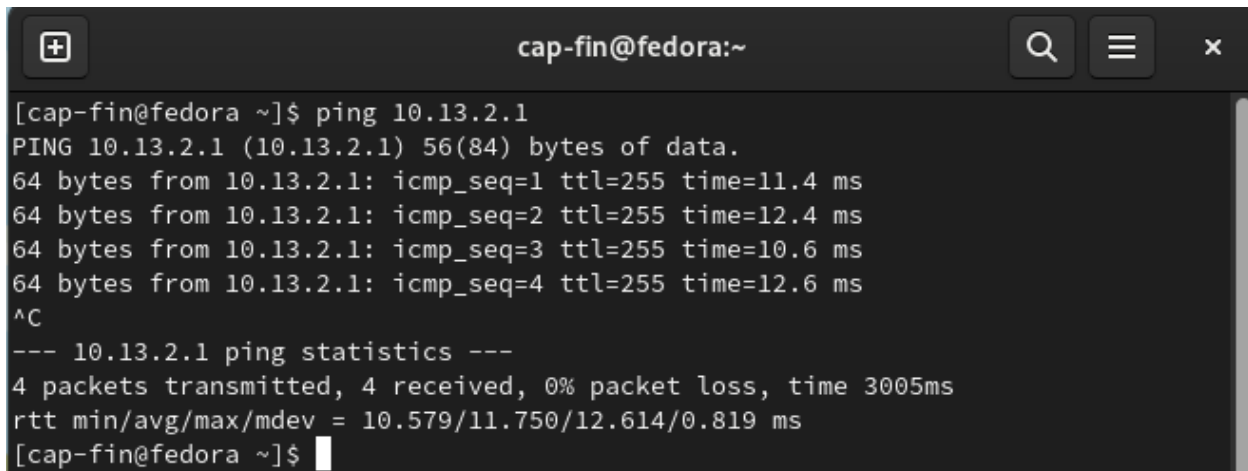
Command: Ping 10.13.5.1: R1-Leg - Interface G0/1

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.5.1. The output displays four successful ping requests with varying response times and a summary statistics block at the bottom.

```
[cap-fin@fedora ~]$ ping 10.13.5.1
PING 10.13.5.1 (10.13.5.1) 56(84) bytes of data.
64 bytes from 10.13.5.1: icmp_seq=1 ttl=254 time=19.8 ms
64 bytes from 10.13.5.1: icmp_seq=2 ttl=254 time=17.5 ms
64 bytes from 10.13.5.1: icmp_seq=3 ttl=254 time=13.6 ms
64 bytes from 10.13.5.1: icmp_seq=4 ttl=254 time=15.0 ms
^C
--- 10.13.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 13.556/16.462/19.824/2.392 ms
[cap-fin@fedora ~]$
```

Figure 2.5 - Output of ping to R1-Leg: Interface G0/1

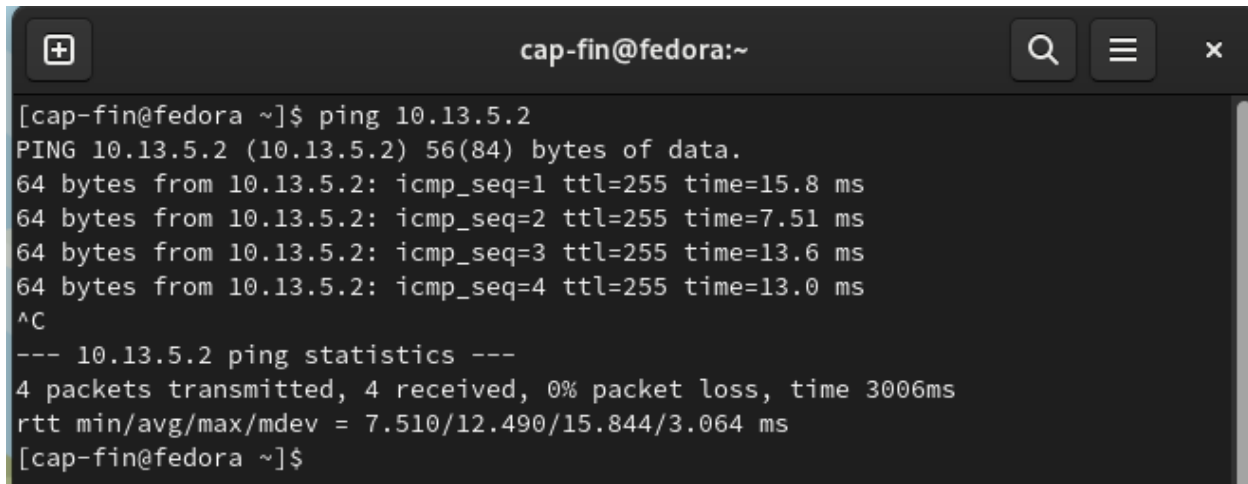
Command: Ping 10.13.2.1: R2-Fin - Interface G0/0

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.2.1. The output displays four successful ping requests with varying response times and a summary statistics block at the bottom.

```
[cap-fin@fedora ~]$ ping 10.13.2.1
PING 10.13.2.1 (10.13.2.1) 56(84) bytes of data.
64 bytes from 10.13.2.1: icmp_seq=1 ttl=255 time=11.4 ms
64 bytes from 10.13.2.1: icmp_seq=2 ttl=255 time=12.4 ms
64 bytes from 10.13.2.1: icmp_seq=3 ttl=255 time=10.6 ms
64 bytes from 10.13.2.1: icmp_seq=4 ttl=255 time=12.6 ms
^C
--- 10.13.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 10.579/11.750/12.614/0.819 ms
[cap-fin@fedora ~]$
```

Figure 2.6 - Output of ping to R2-Fin: Interface G0/0

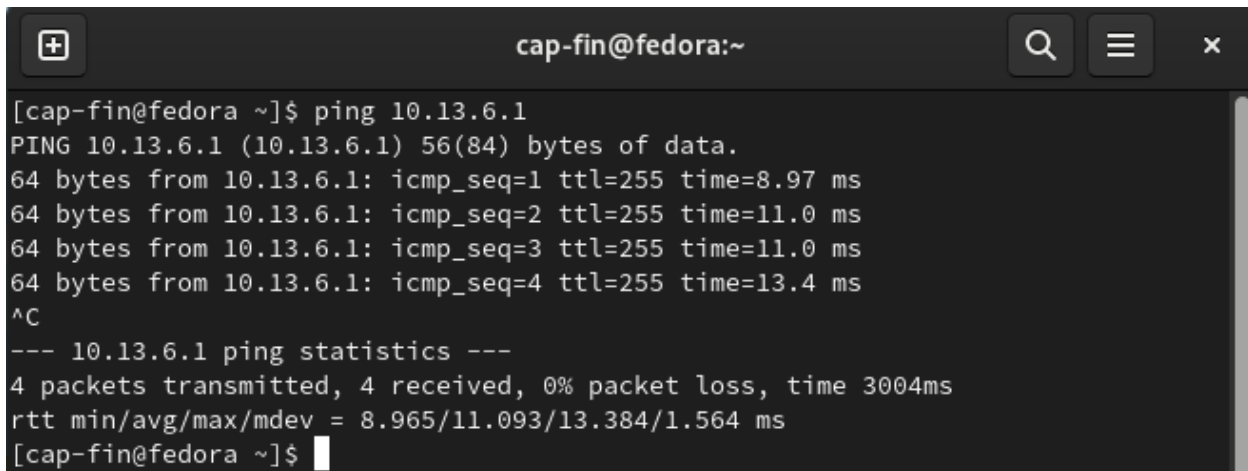
Command: Ping 10.13.5.3: R2-Fin - Interface G0/1

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.5.2. The output includes four successful ping attempts with varying response times and a summary statistics block.

```
[cap-fin@fedora ~]$ ping 10.13.5.2
PING 10.13.5.2 (10.13.5.2) 56(84) bytes of data.
64 bytes from 10.13.5.2: icmp_seq=1 ttl=255 time=15.8 ms
64 bytes from 10.13.5.2: icmp_seq=2 ttl=255 time=7.51 ms
64 bytes from 10.13.5.2: icmp_seq=3 ttl=255 time=13.6 ms
64 bytes from 10.13.5.2: icmp_seq=4 ttl=255 time=13.0 ms
^C
--- 10.13.5.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 7.510/12.490/15.844/3.064 ms
[cap-fin@fedora ~]$
```

Figure 2.7 - Output of ping to R2-Fin: Interface G0/1

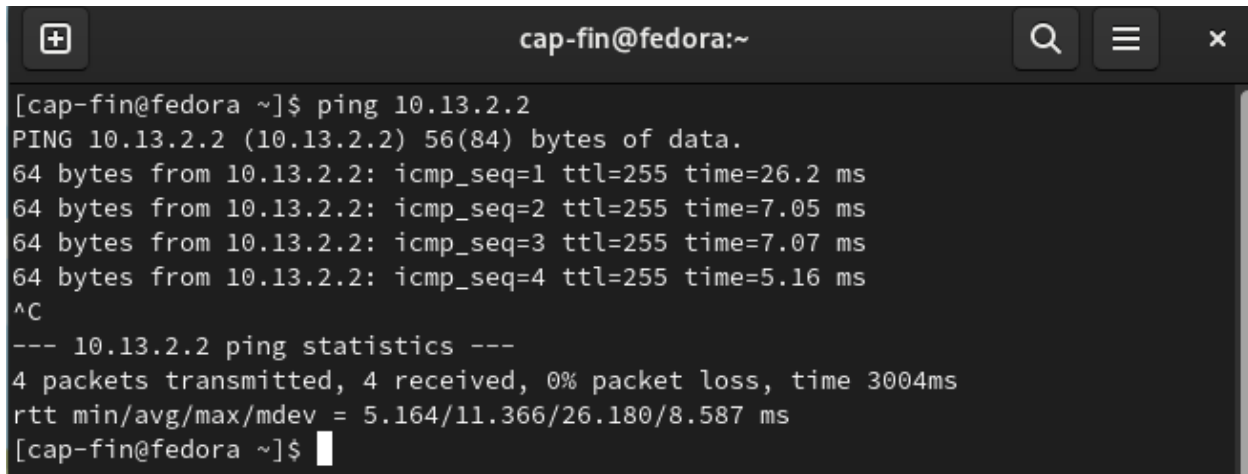
Command: Ping 10.13.2.1: R2-Fin - Interface G0/2

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.6.1. The output includes four successful ping attempts with varying response times and a summary statistics block.

```
[cap-fin@fedora ~]$ ping 10.13.6.1
PING 10.13.6.1 (10.13.6.1) 56(84) bytes of data.
64 bytes from 10.13.6.1: icmp_seq=1 ttl=255 time=8.97 ms
64 bytes from 10.13.6.1: icmp_seq=2 ttl=255 time=11.0 ms
64 bytes from 10.13.6.1: icmp_seq=3 ttl=255 time=11.0 ms
64 bytes from 10.13.6.1: icmp_seq=4 ttl=255 time=13.4 ms
^C
--- 10.13.6.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 8.965/11.093/13.384/1.564 ms
[cap-fin@fedora ~]$
```

Figure 2.8 - Output of ping to R2-Fin: Interface G0/2

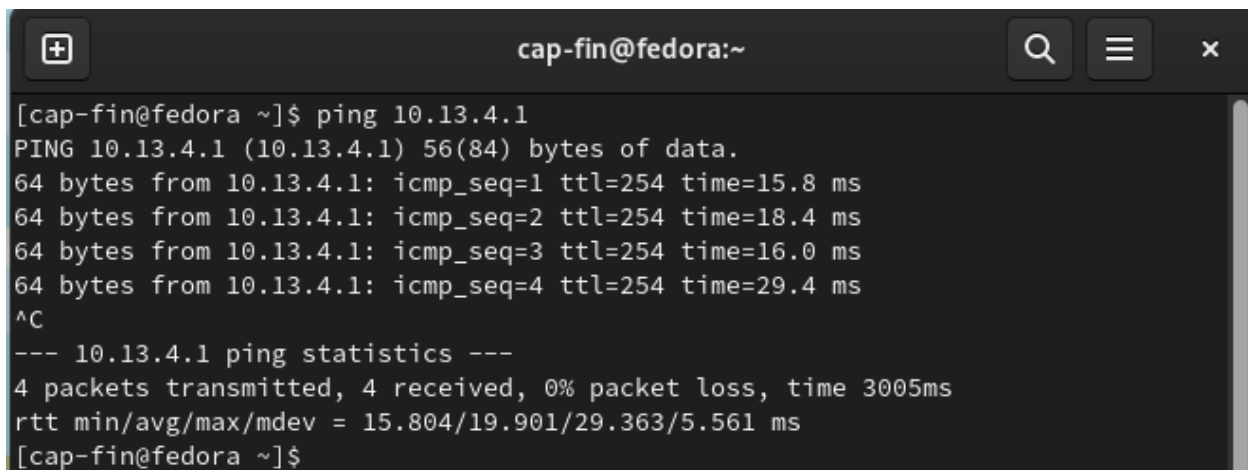
Command: Ping 10.13.2.2: Sw-1

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.2.2. The output includes four successful ping requests with varying response times and a summary statistics block.

```
[cap-fin@fedora ~]$ ping 10.13.2.2
PING 10.13.2.2 (10.13.2.2) 56(84) bytes of data.
64 bytes from 10.13.2.2: icmp_seq=1 ttl=255 time=26.2 ms
64 bytes from 10.13.2.2: icmp_seq=2 ttl=255 time=7.05 ms
64 bytes from 10.13.2.2: icmp_seq=3 ttl=255 time=7.07 ms
64 bytes from 10.13.2.2: icmp_seq=4 ttl=255 time=5.16 ms
^C
--- 10.13.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 5.164/11.366/26.180/8.587 ms
[cap-fin@fedora ~]$
```

Figure 2.9 - Output of ping to Sw-1

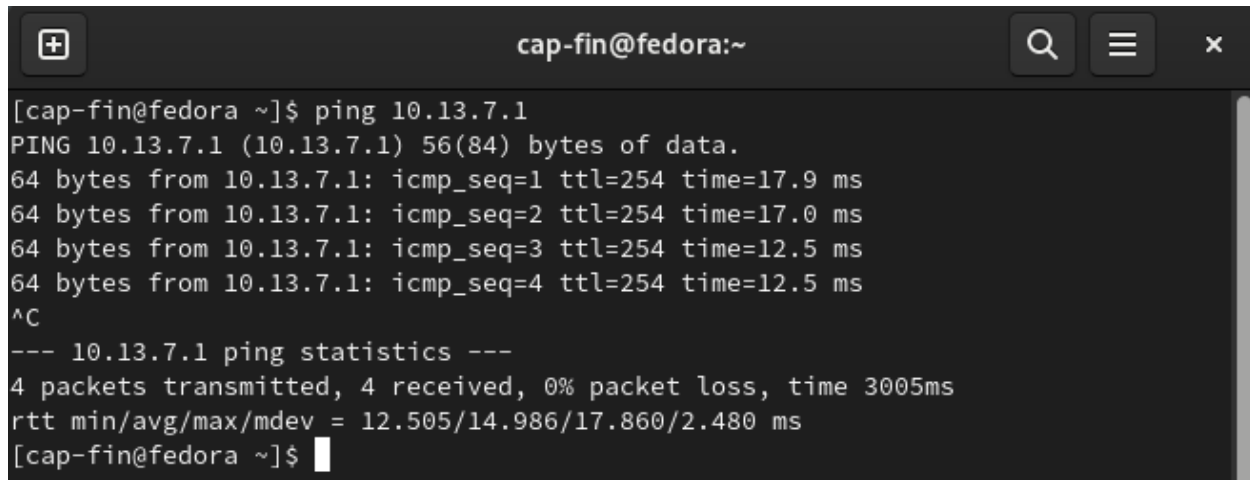
Command: Ping 10.13.4.1: R3-HR - Interface G0/0

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.4.1. The output includes four successful ping requests with varying response times and a summary statistics block.

```
[cap-fin@fedora ~]$ ping 10.13.4.1
PING 10.13.4.1 (10.13.4.1) 56(84) bytes of data.
64 bytes from 10.13.4.1: icmp_seq=1 ttl=254 time=15.8 ms
64 bytes from 10.13.4.1: icmp_seq=2 ttl=254 time=18.4 ms
64 bytes from 10.13.4.1: icmp_seq=3 ttl=254 time=16.0 ms
64 bytes from 10.13.4.1: icmp_seq=4 ttl=254 time=29.4 ms
^C
--- 10.13.4.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 15.804/19.901/29.363/5.561 ms
[cap-fin@fedora ~]$
```

Figure 2.10 - Output of ping to R3-HR: Interface G0/0

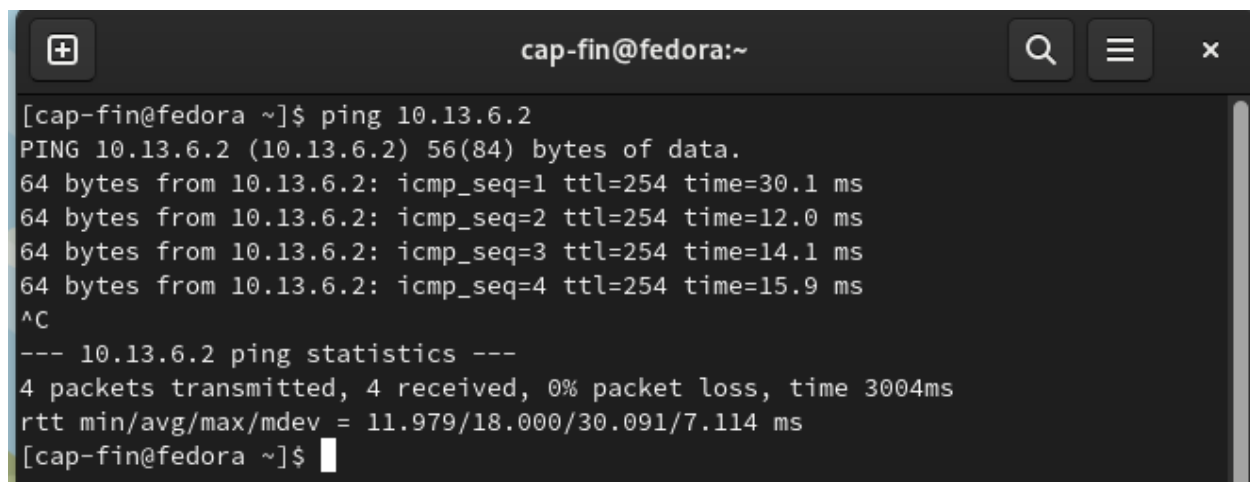
Command: Ping 10.13.7.1: R3-HR - Interface G0/1

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.7.1. The output displays four successful ping requests with varying response times and a summary statistics block indicating 0% packet loss.

```
[cap-fin@fedora ~]$ ping 10.13.7.1
PING 10.13.7.1 (10.13.7.1) 56(84) bytes of data.
64 bytes from 10.13.7.1: icmp_seq=1 ttl=254 time=17.9 ms
64 bytes from 10.13.7.1: icmp_seq=2 ttl=254 time=17.0 ms
64 bytes from 10.13.7.1: icmp_seq=3 ttl=254 time=12.5 ms
64 bytes from 10.13.7.1: icmp_seq=4 ttl=254 time=12.5 ms
^C
--- 10.13.7.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 12.505/14.986/17.860/2.480 ms
[cap-fin@fedora ~]$
```

Figure 2.11 - Output of ping to R3-HR: Interface G0/1

Command: Ping 10.13.6.2: R3-HR - Interface G0/2

A terminal window titled 'cap-fin@fedora:~' showing the output of a ping command to 10.13.6.2. The output displays four successful ping requests with varying response times and a summary statistics block indicating 0% packet loss.

```
[cap-fin@fedora ~]$ ping 10.13.6.2
PING 10.13.6.2 (10.13.6.2) 56(84) bytes of data.
64 bytes from 10.13.6.2: icmp_seq=1 ttl=254 time=30.1 ms
64 bytes from 10.13.6.2: icmp_seq=2 ttl=254 time=12.0 ms
64 bytes from 10.13.6.2: icmp_seq=3 ttl=254 time=14.1 ms
64 bytes from 10.13.6.2: icmp_seq=4 ttl=254 time=15.9 ms
^C
--- 10.13.6.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 11.979/18.000/30.091/7.114 ms
[cap-fin@fedora ~]$
```

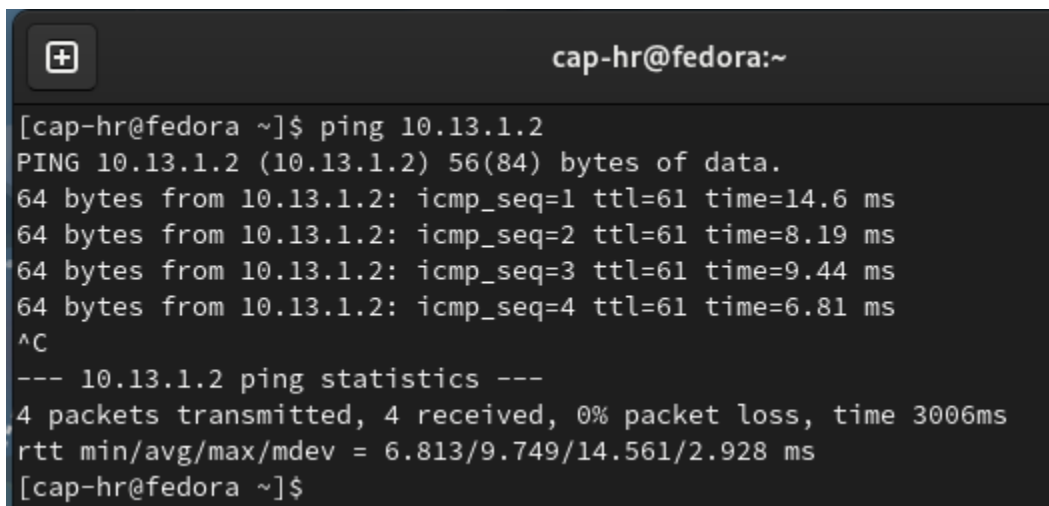
Figure 2.12 - Output of ping to R3-HR: Interface G0/2

As shown in the screenshots, there are no lost packets, and all of the ping tests are successful, indicating connectivity.

Ping Tests: Cap-HR-1

The Fedora VM named Cap-HR-1, a part of the 10.13.4.0/24 subnet, was configured with the IP address 10.13.4.2/24. To show that the device had ping connectivity, the ping command was issued from the terminal on the Cap-HR-1 VM to the three other end devices in the network: Cap-Leg-1, Cap-Fin-1, and Cap-FTP-Serv-1. The below screenshots show the output of the successful ping commands.

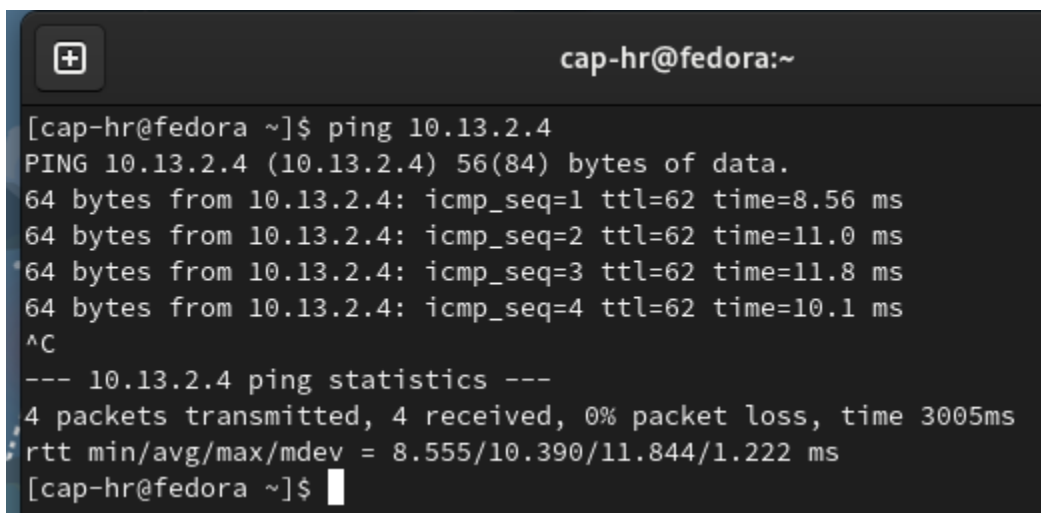
Command: Ping 10.13.1.2: Cap-Leg-1

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.1.2. The output shows four successful pings with varying response times and a summary statistics block.

```
cap-hr@fedora:~$ ping 10.13.1.2
PING 10.13.1.2 (10.13.1.2) 56(84) bytes of data.
64 bytes from 10.13.1.2: icmp_seq=1 ttl=61 time=14.6 ms
64 bytes from 10.13.1.2: icmp_seq=2 ttl=61 time=8.19 ms
64 bytes from 10.13.1.2: icmp_seq=3 ttl=61 time=9.44 ms
64 bytes from 10.13.1.2: icmp_seq=4 ttl=61 time=6.81 ms
^C
--- 10.13.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 6.813/9.749/14.561/2.928 ms
cap-hr@fedora ~]$
```

Figure 3.1 - Output of ping to Cap-Leg-1

Command: Ping 10.13.2.4: Cap-Fin-1

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.2.4. The output shows four successful pings with varying response times and a summary statistics block.

```
cap-hr@fedora:~$ ping 10.13.2.4
PING 10.13.2.4 (10.13.2.4) 56(84) bytes of data.
64 bytes from 10.13.2.4: icmp_seq=1 ttl=62 time=8.56 ms
64 bytes from 10.13.2.4: icmp_seq=2 ttl=62 time=11.0 ms
64 bytes from 10.13.2.4: icmp_seq=3 ttl=62 time=11.8 ms
64 bytes from 10.13.2.4: icmp_seq=4 ttl=62 time=10.1 ms
^C
--- 10.13.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 8.555/10.390/11.844/1.222 ms
cap-hr@fedora ~]$
```

Figure 3.2 - Output of ping to Cap-Fin-1

Command: Ping 10.13.7.2: Cap-FTP-Serv-1

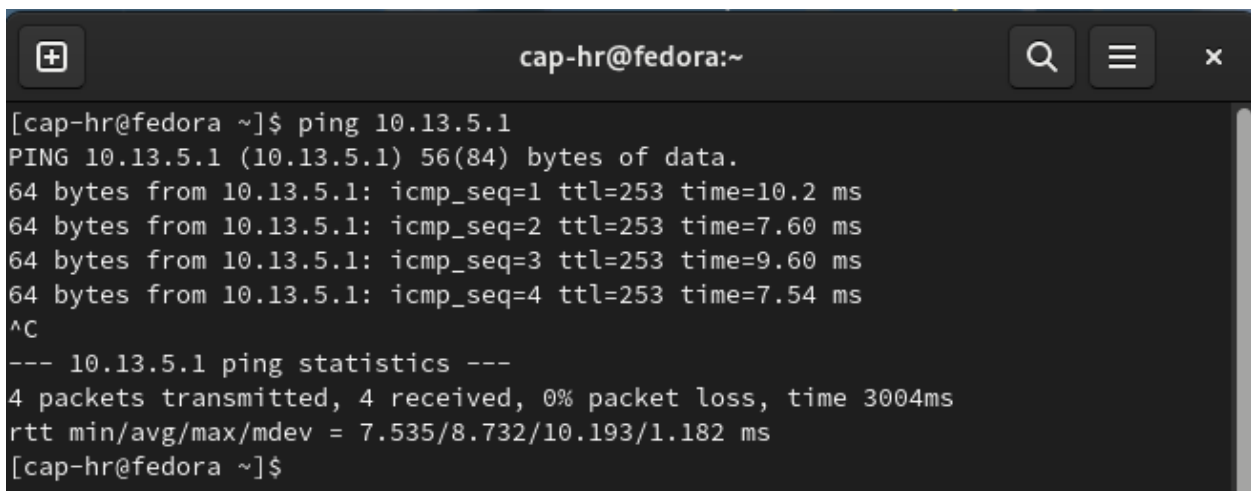
```
[cap-hr@fedora ~]$ ping 10.13.7.2
PING 10.13.7.2 (10.13.7.2) 56(84) bytes of data.
64 bytes from 10.13.7.2: icmp_seq=1 ttl=63 time=2.91 ms
64 bytes from 10.13.7.2: icmp_seq=2 ttl=63 time=1.95 ms
64 bytes from 10.13.7.2: icmp_seq=3 ttl=63 time=3.17 ms
64 bytes from 10.13.7.2: icmp_seq=4 ttl=63 time=2.75 ms
^C
--- 10.13.7.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.948/2.696/3.172/0.457 ms
[cap-hr@fedora ~]$
```

Figure 3.3 - Output of ping to Cap-FTP-Serv-1

The pings are all successful with no lost packets meaning network connectivity was obtained.

In addition to the above ping tests, the ping command was also issued to the router and switch interfaces within the network. The below screenshots verify this.

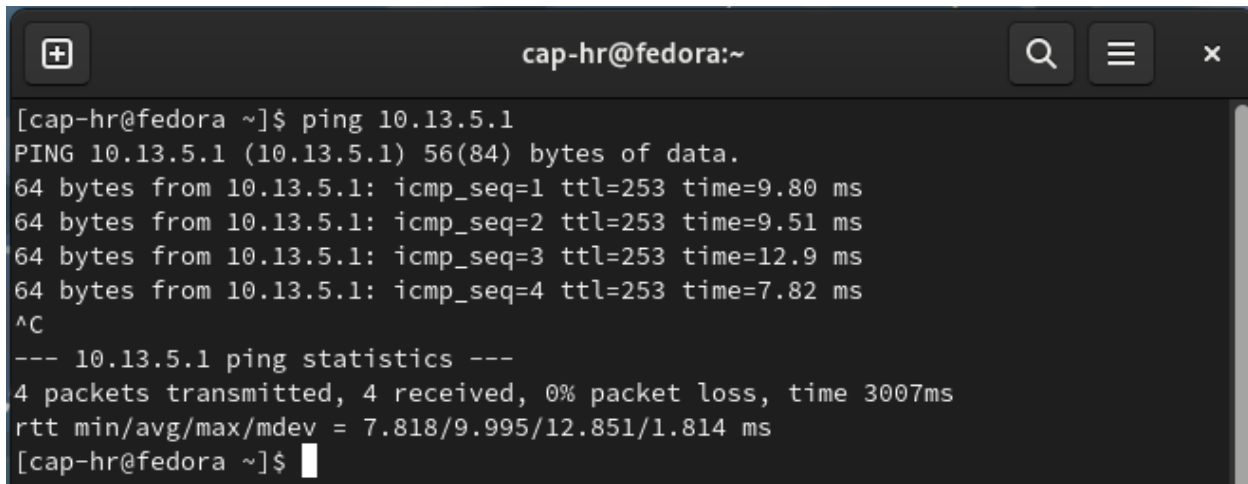
Command: Ping 10.13.5.1: R1-Leg - Interface G0/0



```
cap-hr@fedora:~
[cap-hr@fedora ~]$ ping 10.13.5.1
PING 10.13.5.1 (10.13.5.1) 56(84) bytes of data.
64 bytes from 10.13.5.1: icmp_seq=1 ttl=253 time=10.2 ms
64 bytes from 10.13.5.1: icmp_seq=2 ttl=253 time=7.60 ms
64 bytes from 10.13.5.1: icmp_seq=3 ttl=253 time=9.60 ms
64 bytes from 10.13.5.1: icmp_seq=4 ttl=253 time=7.54 ms
^C
--- 10.13.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 7.535/8.732/10.193/1.182 ms
[cap-hr@fedora ~]$
```

Figure 3.4 - Output of ping to R1-Leg: Interface G0/0

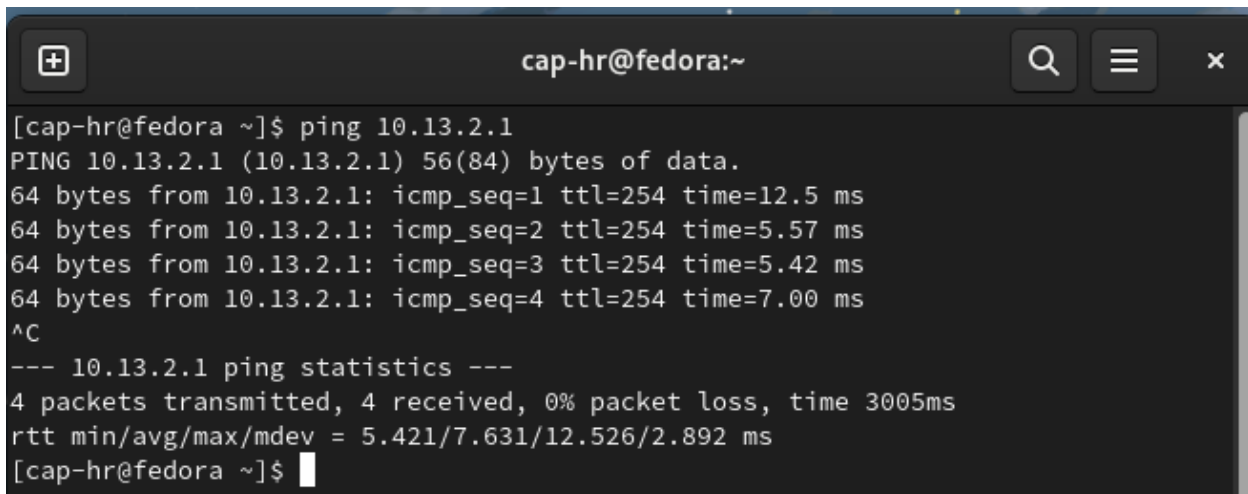
Command: Ping 10.13.5.1: R1-Leg - Interface G0/1

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.5.1. The output includes four successful ping attempts with varying response times and a summary statistics block.

```
[cap-hr@fedora ~]$ ping 10.13.5.1
PING 10.13.5.1 (10.13.5.1) 56(84) bytes of data.
64 bytes from 10.13.5.1: icmp_seq=1 ttl=253 time=9.80 ms
64 bytes from 10.13.5.1: icmp_seq=2 ttl=253 time=9.51 ms
64 bytes from 10.13.5.1: icmp_seq=3 ttl=253 time=12.9 ms
64 bytes from 10.13.5.1: icmp_seq=4 ttl=253 time=7.82 ms
^C
--- 10.13.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 7.818/9.995/12.851/1.814 ms
[cap-hr@fedora ~]$
```

Figure 3.5 - Output of ping command to R1-Leg: Interface G0/1

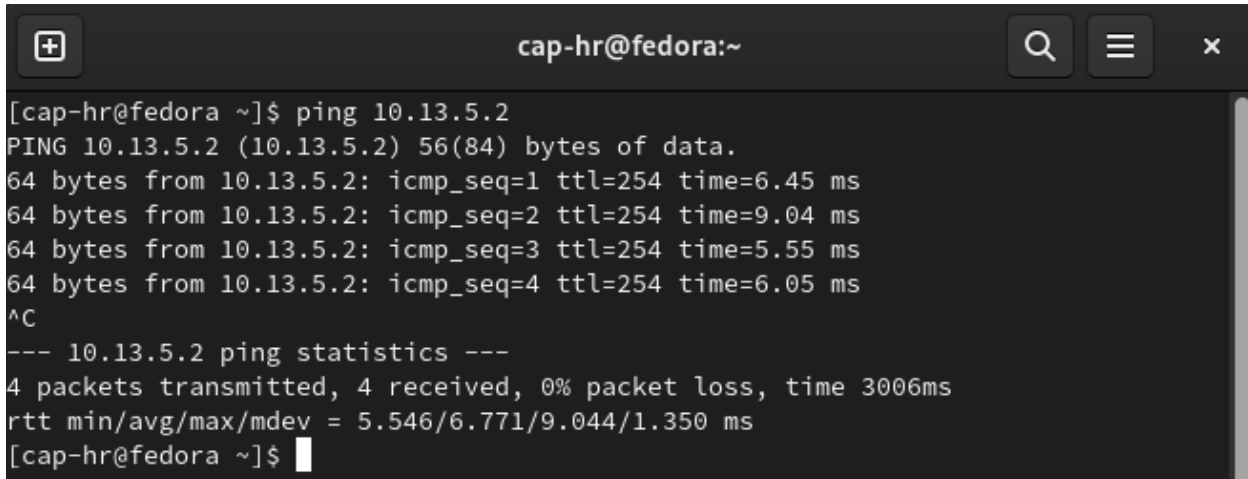
Command: Ping 10.13.2.1: R2-Fin - Interface G0/0

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.2.1. The output includes four successful ping attempts with varying response times and a summary statistics block.

```
[cap-hr@fedora ~]$ ping 10.13.2.1
PING 10.13.2.1 (10.13.2.1) 56(84) bytes of data.
64 bytes from 10.13.2.1: icmp_seq=1 ttl=254 time=12.5 ms
64 bytes from 10.13.2.1: icmp_seq=2 ttl=254 time=5.57 ms
64 bytes from 10.13.2.1: icmp_seq=3 ttl=254 time=5.42 ms
64 bytes from 10.13.2.1: icmp_seq=4 ttl=254 time=7.00 ms
^C
--- 10.13.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 5.421/7.631/12.526/2.892 ms
[cap-hr@fedora ~]$
```

Figure 3.6 - Output of ping command to R2-Fin: Interface G0/0

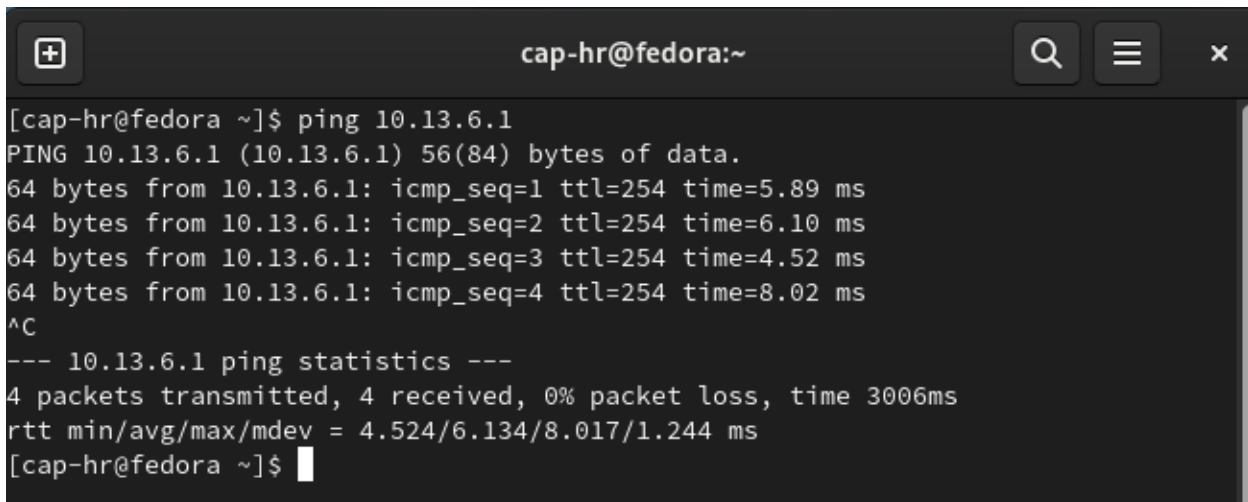
Command: Ping 10.13.5.2: R2-Fin - Interface G0/1

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.5.2. The output includes four successful ping attempts with varying response times and a summary of ping statistics.

```
[cap-hr@fedora ~]$ ping 10.13.5.2
PING 10.13.5.2 (10.13.5.2) 56(84) bytes of data.
64 bytes from 10.13.5.2: icmp_seq=1 ttl=254 time=6.45 ms
64 bytes from 10.13.5.2: icmp_seq=2 ttl=254 time=9.04 ms
64 bytes from 10.13.5.2: icmp_seq=3 ttl=254 time=5.55 ms
64 bytes from 10.13.5.2: icmp_seq=4 ttl=254 time=6.05 ms
^C
--- 10.13.5.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 5.546/6.771/9.044/1.350 ms
[cap-hr@fedora ~]$
```

Figure 3.7 - Output of ping command to R2-Fin: Interface G0/1

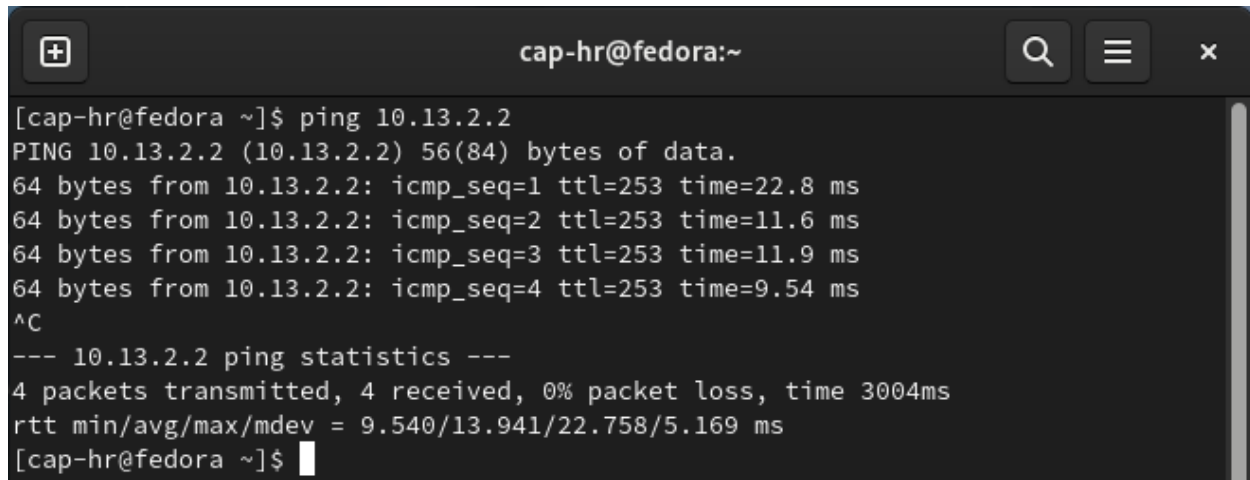
Command: Ping 10.13.6.1: R2-Fin - Interface G0/2

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.6.1. The output includes four successful ping attempts with varying response times and a summary of ping statistics.

```
[cap-hr@fedora ~]$ ping 10.13.6.1
PING 10.13.6.1 (10.13.6.1) 56(84) bytes of data.
64 bytes from 10.13.6.1: icmp_seq=1 ttl=254 time=5.89 ms
64 bytes from 10.13.6.1: icmp_seq=2 ttl=254 time=6.10 ms
64 bytes from 10.13.6.1: icmp_seq=3 ttl=254 time=4.52 ms
64 bytes from 10.13.6.1: icmp_seq=4 ttl=254 time=8.02 ms
^C
--- 10.13.6.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 4.524/6.134/8.017/1.244 ms
[cap-hr@fedora ~]$
```

Figure 3.8 - Output of ping command to R2-Fin: interface G0/2

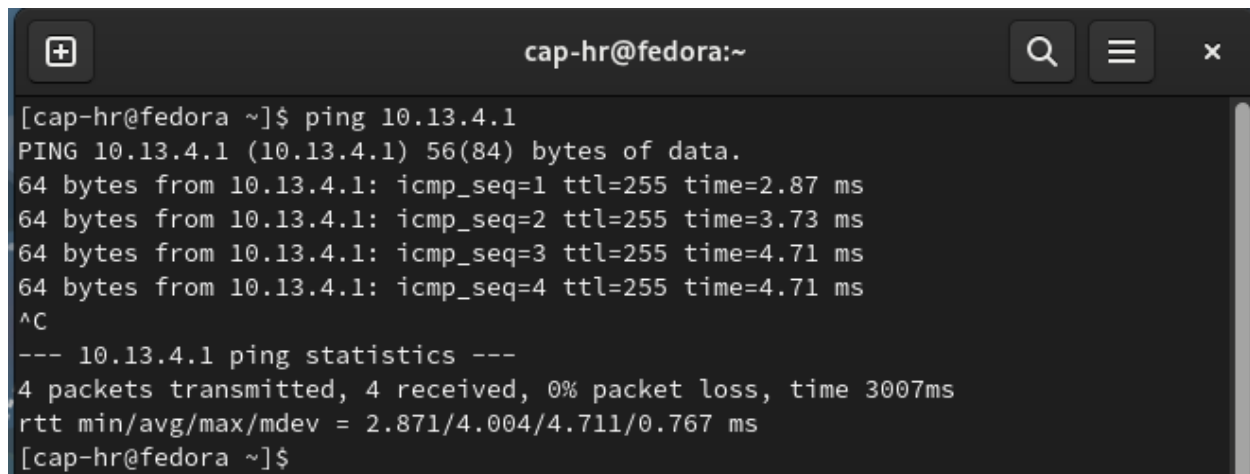
Command: Ping 10.13.2.2: Sw-1

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.2.2. The output includes four successful ping attempts with varying response times and a summary statistics block.

```
[cap-hr@fedora ~]$ ping 10.13.2.2
PING 10.13.2.2 (10.13.2.2) 56(84) bytes of data:
64 bytes from 10.13.2.2: icmp_seq=1 ttl=253 time=22.8 ms
64 bytes from 10.13.2.2: icmp_seq=2 ttl=253 time=11.6 ms
64 bytes from 10.13.2.2: icmp_seq=3 ttl=253 time=11.9 ms
64 bytes from 10.13.2.2: icmp_seq=4 ttl=253 time=9.54 ms
^C
--- 10.13.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 9.540/13.941/22.758/5.169 ms
[cap-hr@fedora ~]$
```

Figure 3.9 - Output of ping command to Sw-1

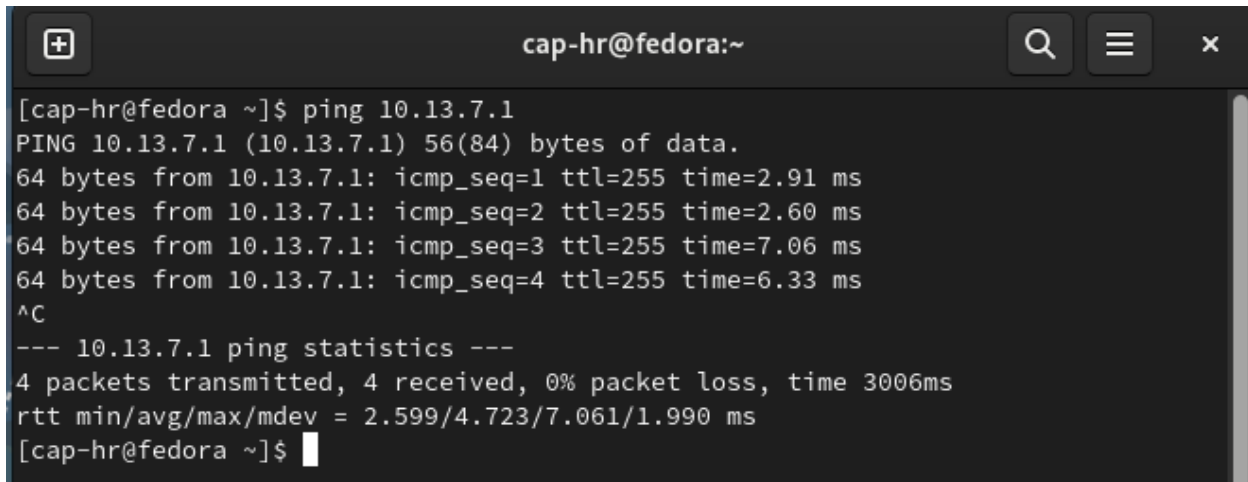
Command: Ping 10.13.6.1: R3-HR - Interface G0/0

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.4.1. The output includes four successful ping attempts with very low response times and a summary statistics block.

```
[cap-hr@fedora ~]$ ping 10.13.4.1
PING 10.13.4.1 (10.13.4.1) 56(84) bytes of data:
64 bytes from 10.13.4.1: icmp_seq=1 ttl=255 time=2.87 ms
64 bytes from 10.13.4.1: icmp_seq=2 ttl=255 time=3.73 ms
64 bytes from 10.13.4.1: icmp_seq=3 ttl=255 time=4.71 ms
64 bytes from 10.13.4.1: icmp_seq=4 ttl=255 time=4.71 ms
^C
--- 10.13.4.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.871/4.004/4.711/0.767 ms
[cap-hr@fedora ~]$
```

Figure 3.10 - Output of ping command to R3-HR: Interface G0/0

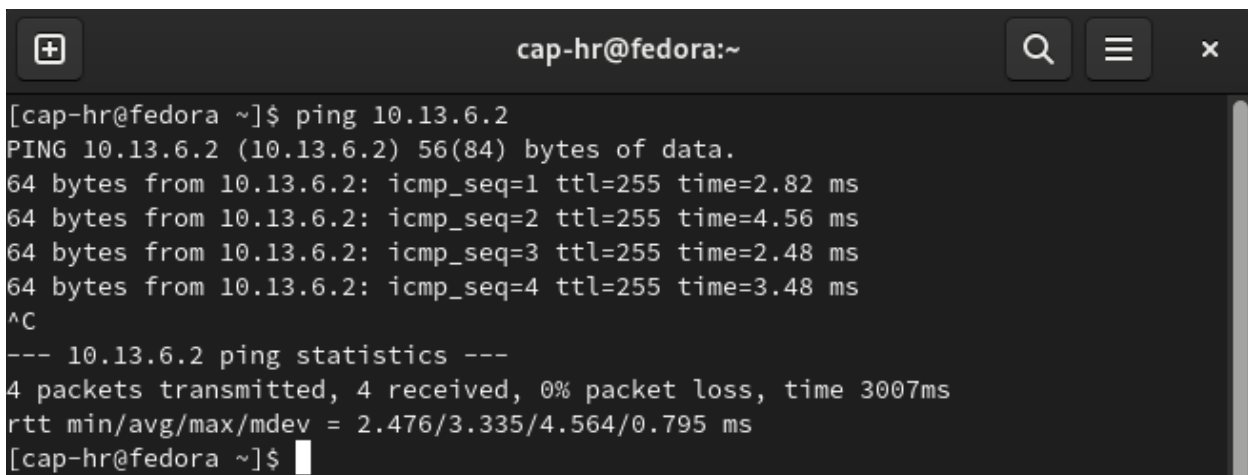
Command: Ping 10.13.7.1: R3-HR - Interface G0/1

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.7.1. The output displays four successful ping attempts with varying response times and a summary statistics block at the bottom.

```
[cap-hr@fedora ~]$ ping 10.13.7.1
PING 10.13.7.1 (10.13.7.1) 56(84) bytes of data.
64 bytes from 10.13.7.1: icmp_seq=1 ttl=255 time=2.91 ms
64 bytes from 10.13.7.1: icmp_seq=2 ttl=255 time=2.60 ms
64 bytes from 10.13.7.1: icmp_seq=3 ttl=255 time=7.06 ms
64 bytes from 10.13.7.1: icmp_seq=4 ttl=255 time=6.33 ms
^C
--- 10.13.7.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.599/4.723/7.061/1.990 ms
[cap-hr@fedora ~]$
```

Figure 3.11 - Output of ping command to R3-HR: Interface G0/1

Command: Ping 10.13.6.2: R3-HR - Interface G0/2

A terminal window titled 'cap-hr@fedora:~' showing the output of a ping command to 10.13.6.2. The output displays four successful ping attempts with varying response times and a summary statistics block at the bottom.

```
[cap-hr@fedora ~]$ ping 10.13.6.2
PING 10.13.6.2 (10.13.6.2) 56(84) bytes of data.
64 bytes from 10.13.6.2: icmp_seq=1 ttl=255 time=2.82 ms
64 bytes from 10.13.6.2: icmp_seq=2 ttl=255 time=4.56 ms
64 bytes from 10.13.6.2: icmp_seq=3 ttl=255 time=2.48 ms
64 bytes from 10.13.6.2: icmp_seq=4 ttl=255 time=3.48 ms
^C
--- 10.13.6.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.476/3.335/4.564/0.795 ms
[cap-hr@fedora ~]$
```

Figure 3.12 - Output of ping command to R3-HR: Interface G0/2

The ping tests are successful, with no lost packets meaning connectivity was achieved.

Ping Tests: Cap-FTP-Serv-1

The Fedora VM named Cap-FTP-Serv-1, a part of the 10.13.7.0/24 subnet, was configured with the IP address 10.13.7.2/24. To show that the device had ping connectivity, the ping command was issued from the terminal on the Cap-FTP-Serv-1 VM to the three other end devices in the network: Cap-Leg-1, Cap-Fin-1, and Cap-HR-1. The below screenshots show the output of the successful ping commands.

Command: Ping 10.13.1.2: Cap-Leg-1

```
[root@FTPServ ~]# ping 10.13.1.2
PING 10.13.1.2 (10.13.1.2) 56(84) bytes of data.
64 bytes from 10.13.1.2: icmp_seq=1 ttl=61 time=94.6 ms
64 bytes from 10.13.1.2: icmp_seq=2 ttl=61 time=6.80 ms
64 bytes from 10.13.1.2: icmp_seq=3 ttl=61 time=8.23 ms
64 bytes from 10.13.1.2: icmp_seq=4 ttl=61 time=5.57 ms
^C
--- 10.13.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 5.574/28.812/94.644/38.019 ms
[root@FTPServ ~]# Serv-Fin
```

Figure 4.1 - Output of ping to Cap-Leg-1

Command: Ping 10.13.2.4: Cap-Fin-1

```
[root@FTPServ ~]# ping 10.13.2.4
PING 10.13.2.4 (10.13.2.4) 56(84) bytes of data.
64 bytes from 10.13.2.4: icmp_seq=1 ttl=62 time=192 ms
64 bytes from 10.13.2.4: icmp_seq=2 ttl=62 time=12.0 ms
64 bytes from 10.13.2.4: icmp_seq=3 ttl=62 time=12.3 ms
64 bytes from 10.13.2.4: icmp_seq=4 ttl=62 time=8.20 ms
^C
--- 10.13.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 8.199/56.050/191.756/78.366 ms
```

Figure 4.2 - Output of ping to Cap-Fin-1

Command: Ping 10.13.4.2: Cap-HR-1

```
[root@FTPServ ~]# ping 10.13.4.2
PING 10.13.4.2 (10.13.4.2) 56(84) bytes of data.
64 bytes from 10.13.4.2: icmp_seq=1 ttl=63 time=137 ms
64 bytes from 10.13.4.2: icmp_seq=2 ttl=63 time=2.13 ms
64 bytes from 10.13.4.2: icmp_seq=3 ttl=63 time=21.9 ms
64 bytes from 10.13.4.2: icmp_seq=4 ttl=63 time=2.58 ms
^C
--- 10.13.4.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 2.132/40.852/136.750/55.941 ms
```

Figure 4.3 - Output of ping to Cap-HR-1

The pings are all successful with no lost packets meaning network connectivity was obtained.

In addition to the ping tests sent to the other Fedora VMs, the ping command was also issued to the interfaces of the routers and the switch across the network to verify connectivity. The results of the ping tests can be seen in the screenshots below.

Command: Ping 10.13.1.1: R1-Leg - Interface G0/0

```
[root@FTPServ ~]# ping 10.13.1.1
PING 10.13.1.1 (10.13.1.1) 56(84) bytes of data.
64 bytes from 10.13.1.1: icmp_seq=1 ttl=253 time=17.1 ms
64 bytes from 10.13.1.1: icmp_seq=2 ttl=253 time=11.1 ms
64 bytes from 10.13.1.1: icmp_seq=3 ttl=253 time=9.53 ms
64 bytes from 10.13.1.1: icmp_seq=4 ttl=253 time=13.5 ms
^C
--- 10.13.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 9.525/12.823/17.120/2.863 ms
[root@FTPServ ~]#
```

Figure 4.4 - Output of ping command to R1-Leg: Interface G0/0

Command: Ping 10.13.5.1: R1-Leg - Interface G0/1

```
[root@FTPServ ~]# ping 10.13.5.1
PING 10.13.5.1 (10.13.5.1) 56(84) bytes of data.
64 bytes from 10.13.5.1: icmp_seq=1 ttl=253 time=14.9 ms
64 bytes from 10.13.5.1: icmp_seq=2 ttl=253 time=16.1 ms
64 bytes from 10.13.5.1: icmp_seq=3 ttl=253 time=5.90 ms
64 bytes from 10.13.5.1: icmp_seq=4 ttl=253 time=9.02 ms
^C
--- 10.13.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 5.899/11.461/16.055/4.172 ms
[root@FTPServ ~]# _
```

Figure 4.5 - Output of ping command to R1-Leg: Interface G0/1

Command: Ping 10.13.2.1: R2-Fin - Interface G0/0

```
[root@FTPServ ~]# ping 10.13.2.1
PING 10.13.2.1 (10.13.2.1) 56(84) bytes of data.
64 bytes from 10.13.2.1: icmp_seq=1 ttl=254 time=15.5 ms
64 bytes from 10.13.2.1: icmp_seq=2 ttl=254 time=5.14 ms
64 bytes from 10.13.2.1: icmp_seq=3 ttl=254 time=7.25 ms
64 bytes from 10.13.2.1: icmp_seq=4 ttl=254 time=10.7 ms
^C
--- 10.13.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 5.137/9.635/15.485/3.911 ms
[root@FTPServ ~]# _
```

Figure 4.6 - Output of ping command to R2-Fin: Interface G0/0

Command: Ping 10.13.5.2: R2-Fin - Interface G0/1

```
[root@FTPServ ~]# ping 10.13.5.2
PING 10.13.5.2 (10.13.5.2) 56(84) bytes of data.
64 bytes from 10.13.5.2: icmp_seq=1 ttl=254 time=13.3 ms
64 bytes from 10.13.5.2: icmp_seq=2 ttl=254 time=7.12 ms
64 bytes from 10.13.5.2: icmp_seq=3 ttl=254 time=10.5 ms
64 bytes from 10.13.5.2: icmp_seq=4 ttl=254 time=3.60 ms
^C
--- 10.13.5.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 3.600/8.622/13.286/3.630 ms
[root@FTPServ ~]# _
```

Figure 4.7 - Output of ping command to R2-Fin: Interface G0/1

Command: Ping 10.13.6.1: R2-Fin - Interface G0/2

```
[root@FTPServ ~]# ping 10.13.6.1
PING 10.13.6.1 (10.13.6.1) 56(84) bytes of data.
64 bytes from 10.13.6.1: icmp_seq=1 ttl=254 time=12.7 ms
64 bytes from 10.13.6.1: icmp_seq=2 ttl=254 time=11.7 ms
64 bytes from 10.13.6.1: icmp_seq=3 ttl=254 time=4.29 ms
64 bytes from 10.13.6.1: icmp_seq=4 ttl=254 time=5.60 ms
^C
--- 10.13.6.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 4.290/8.568/12.697/3.670 ms
[root@FTPServ ~]#
```

Figure 4.8 - Output of ping command to R2-Fin: Interface G0/2

Command: Ping 10.13.2.2: Sw-1

```
[root@FTPServ ~]# ping 10.13.2.2
PING 10.13.2.2 (10.13.2.2) 56(84) bytes of data.
64 bytes from 10.13.2.2: icmp_seq=1 ttl=253 time=13.2 ms
64 bytes from 10.13.2.2: icmp_seq=2 ttl=253 time=9.51 ms
64 bytes from 10.13.2.2: icmp_seq=3 ttl=253 time=10.0 ms
64 bytes from 10.13.2.2: icmp_seq=4 ttl=253 time=8.08 ms
^C
--- 10.13.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 8.079/10.200/13.180/1.863 ms
[root@FTPServ ~]# _
```

Figure 4.9 - Output of ping command to Sw-1

Command: Ping 10.13.4.1: R3-HR - Interface G0/0

```
[root@FTPServ ~]# ping 10.13.4.1
PING 10.13.4.1 (10.13.4.1) 56(84) bytes of data.
64 bytes from 10.13.4.1: icmp_seq=1 ttl=255 time=3.37 ms
64 bytes from 10.13.4.1: icmp_seq=2 ttl=255 time=2.53 ms
64 bytes from 10.13.4.1: icmp_seq=3 ttl=255 time=2.60 ms
64 bytes from 10.13.4.1: icmp_seq=4 ttl=255 time=11.5 ms
^C
--- 10.13.4.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.533/5.009/11.537/3.783 ms
[root@FTPServ ~]# _
```

Figure 4.10 - Output of ping command to R3-HR: Interface G0/0

Command: Ping 10.13.7.1: R3-HR - Interface G0/1

```
[root@FTPServ ~]# ping 10.13.7.1
PING 10.13.7.1 (10.13.7.1) 56(84) bytes of data.
64 bytes from 10.13.7.1: icmp_seq=1 ttl=255 time=3.28 ms
64 bytes from 10.13.7.1: icmp_seq=2 ttl=255 time=2.64 ms
64 bytes from 10.13.7.1: icmp_seq=3 ttl=255 time=3.12 ms
64 bytes from 10.13.7.1: icmp_seq=4 ttl=255 time=3.59 ms
^C
--- 10.13.7.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.639/3.156/3.587/0.342 ms
[root@FTPServ ~]# _
```

Figure 4.11 - Output of ping command to R3-HR: Interface G0/1

Command: Ping 10.13.6.2: R3-HR - Interface G0/2

```
[root@FTPServ ~]# ping 10.13.6.2
PING 10.13.6.2 (10.13.6.2) 56(84) bytes of data.
64 bytes from 10.13.6.2: icmp_seq=1 ttl=255 time=7.20 ms
64 bytes from 10.13.6.2: icmp_seq=2 ttl=255 time=2.60 ms
64 bytes from 10.13.6.2: icmp_seq=3 ttl=255 time=2.62 ms
64 bytes from 10.13.6.2: icmp_seq=4 ttl=255 time=2.99 ms
^C
--- 10.13.6.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.603/3.855/7.203/1.938 ms
[root@FTPServ ~]#
```

Figure 4.12 - Output of ping command to R3-HR: Interface G0/2

The pings are all successful, and connectivity is verified.

FTP Server Access: Cap-Leg-1

For ease of documentation, the GUI application FileZilla will be used to demonstrate the FTP server properties.

First, the connection to the FTP server is established by typing `ftp://10.13.7.2` and logging in with the username `Legal` and the password `Legal`. The notification states that the directory listing of `/FTP` is successful.

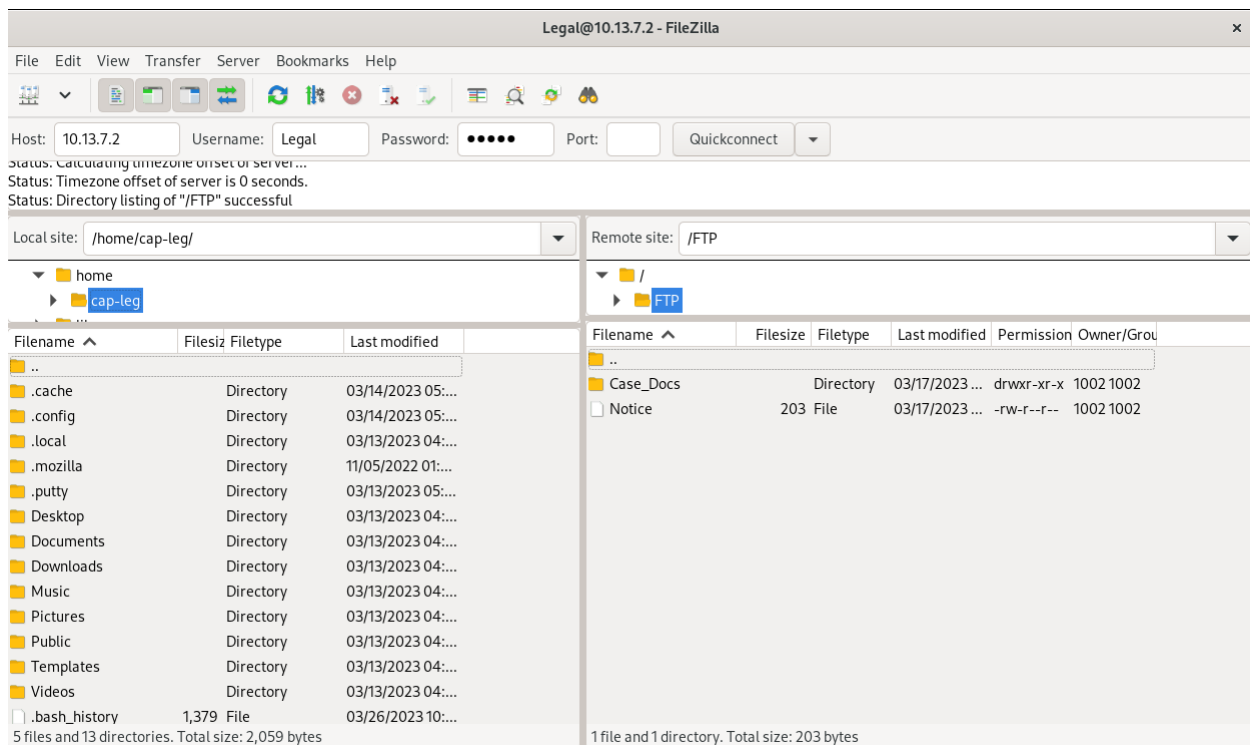


Figure 5.1 - FileZilla FTP Connection

After selecting the document 'Notice', click and drag it to the `/home/cap-leg/` directory.

The file transfer is successful.

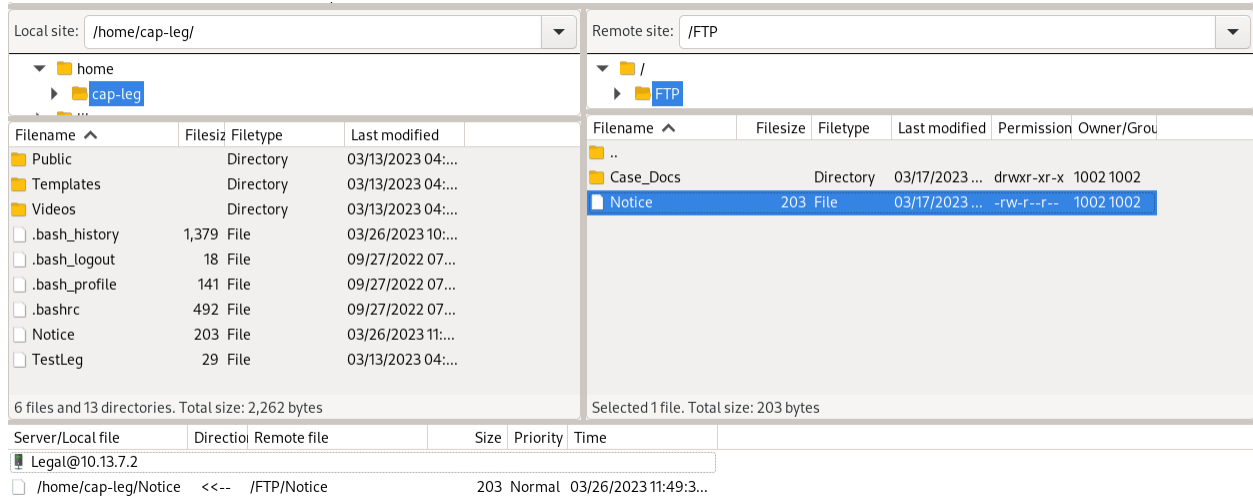


Figure 5.2 - Successful transfer from Server to Host

By Selecting the document 'TestLeg', and clicking and dragging it to the rightmost /FTP directory, the file is uploaded.

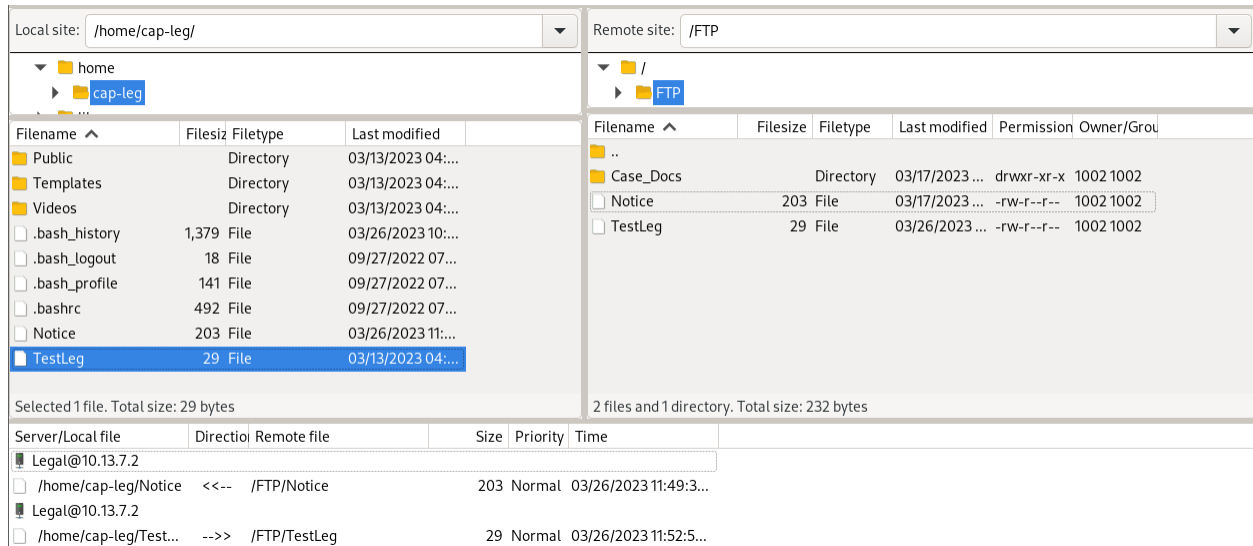


Figure 5.3 - Successful transfer from Host to Server

The transfer notification at the bottom and the new file in the directory demonstrates the file transfer was successful.

FTP Server Access: Cap-Fin-1

For ease of documentation, the GUI application FileZilla will be used to demonstrate the FTP server properties.

First, the connection to the FTP server is established by typing *ftp://10.13.7.2* and logging in with the username *Fin* and the password *Fin*. The notification states that the directory listing of /FTP is successful.

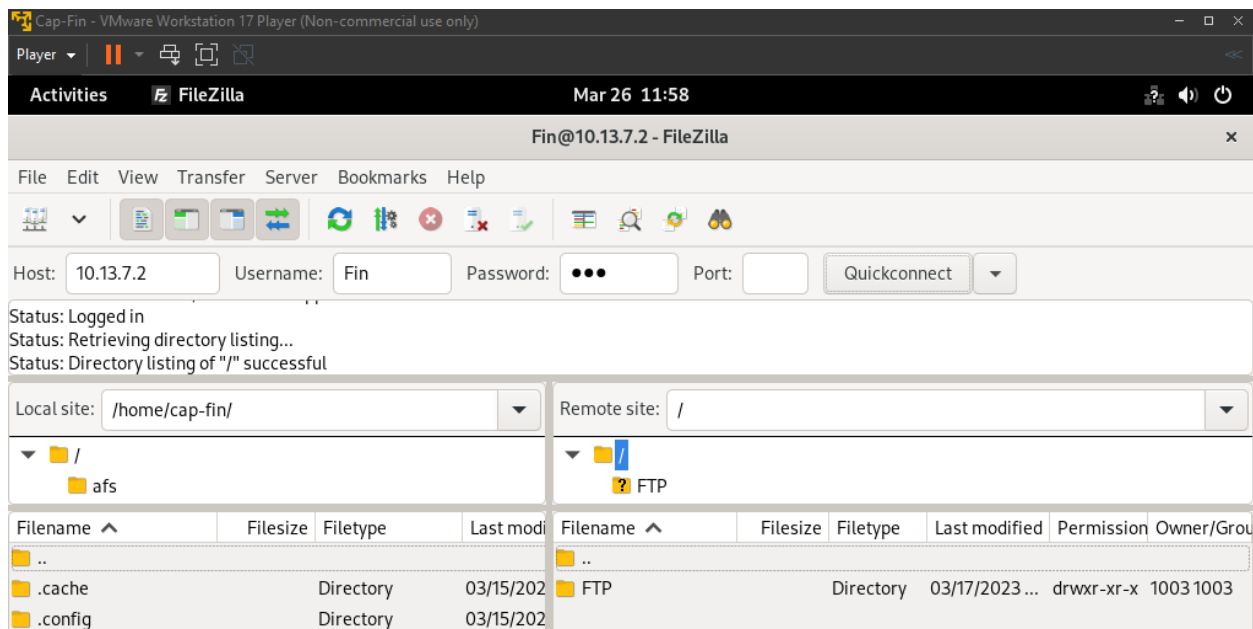


Figure 6.1 - FileZilla FTP Connection

After selecting the document 'Manager_Salary', click and drag it to the /home/cap-fin/ directory. The file transfer is successful.

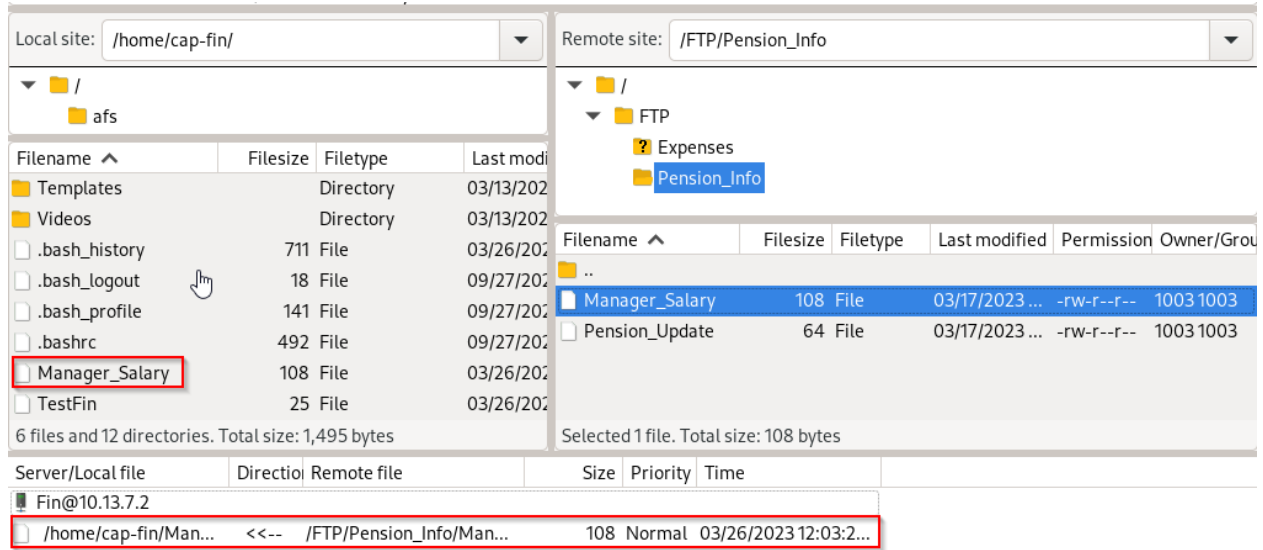


Figure 6.2 - Successful Server to Host FTP transfer

By Selecting the document 'TestFin', and clicking and dragging it to the rightmost /FTP directory, the file is uploaded. The transfer is successful, and the document is now accessible on the server.

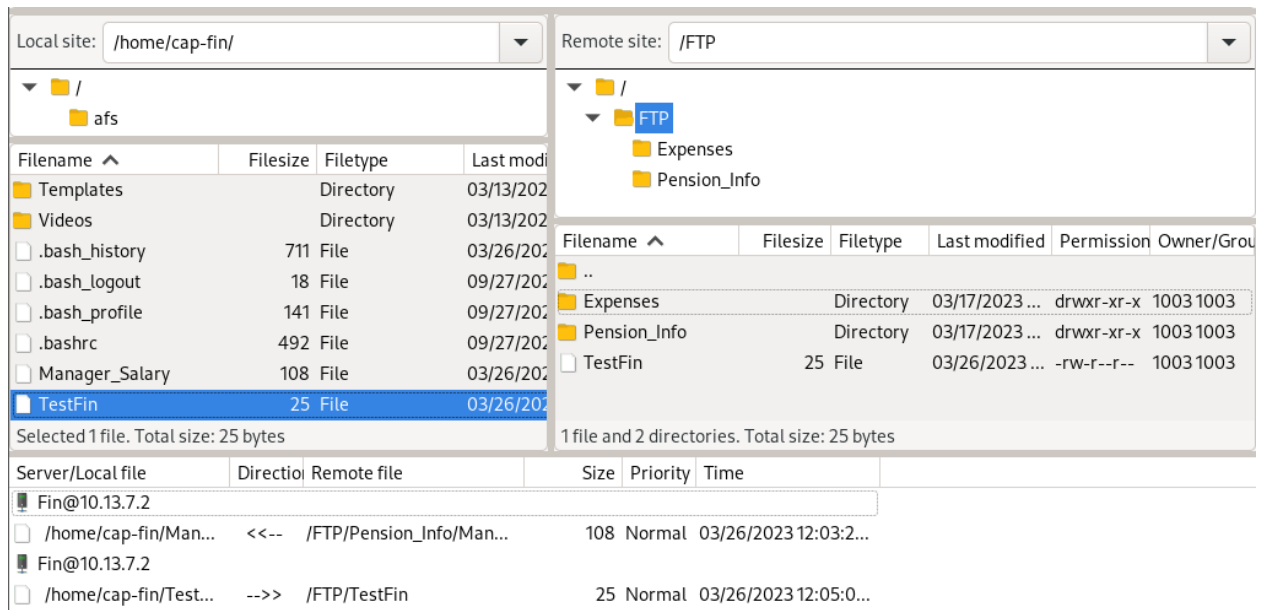


Figure 6.3 - Successful Host to Server FTP transfer

FTP Server Access: Cap-HR-1

For ease of documentation, the GUI application FileZilla will be used to demonstrate the FTP server properties.

First, the connection to the FTP server is established by typing `ftp://10.13.7.2` and logging in with the username `HR` and the password `HR`. The notification states that the directory listing of `/FTP` is successful.

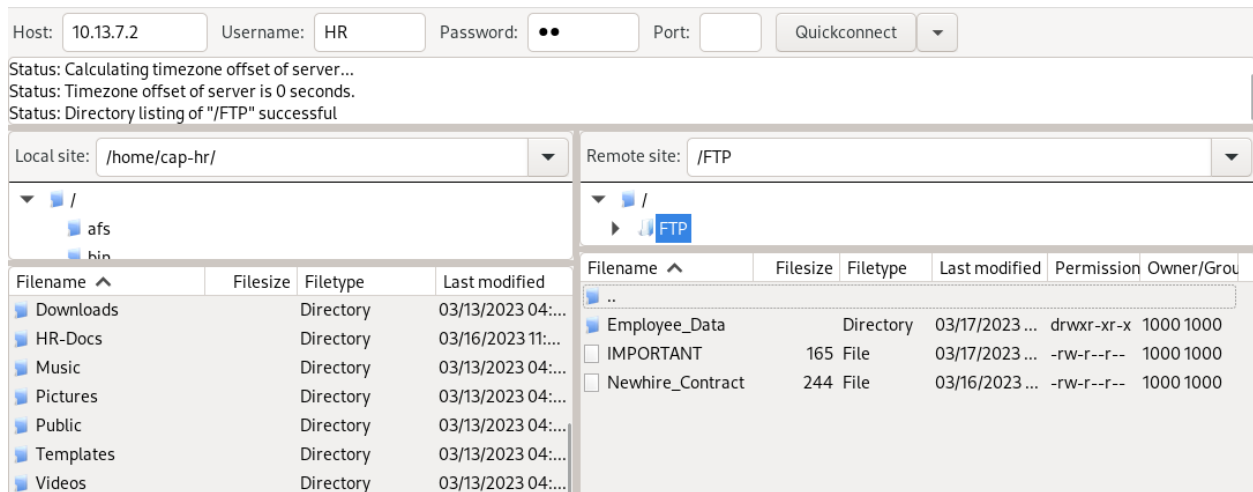


Figure 7.1 - FileZilla FTP Connection

After selecting the document 'Newhire_Contract', click and drag it to the `/home/cap-hr/` directory. The file transfer is successful.

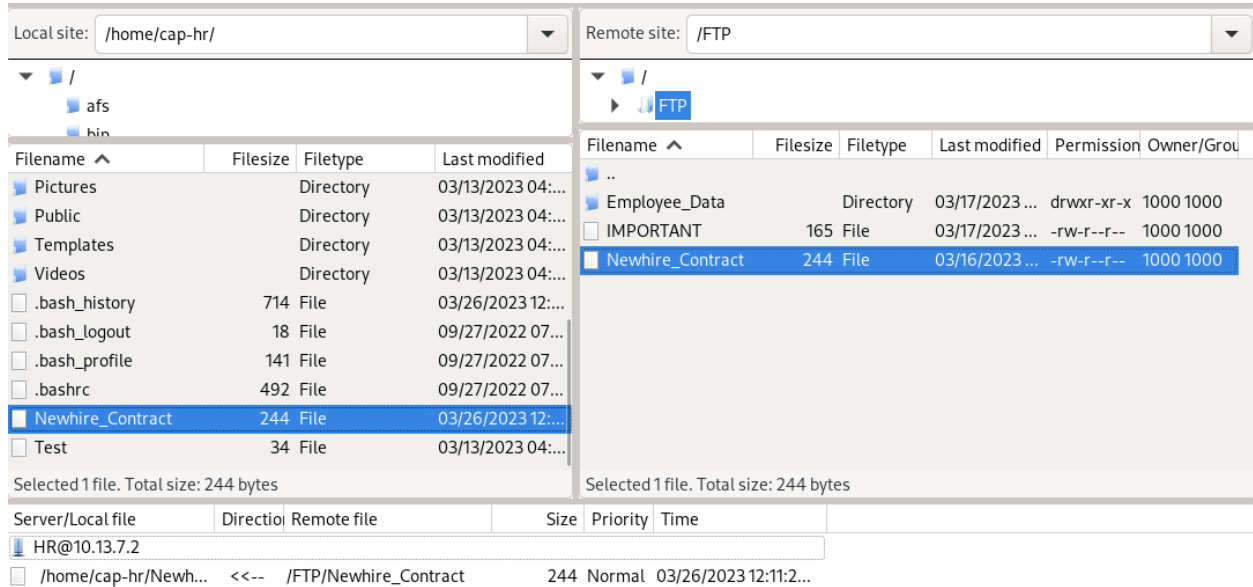


Figure 7.2 - Successful Server to Host FTP transfer

By Selecting the document ‘Test’, and clicking and dragging it to the rightmost /FTP directory, the file is uploaded. The transfer is successful, and the document is now accessible on the server.

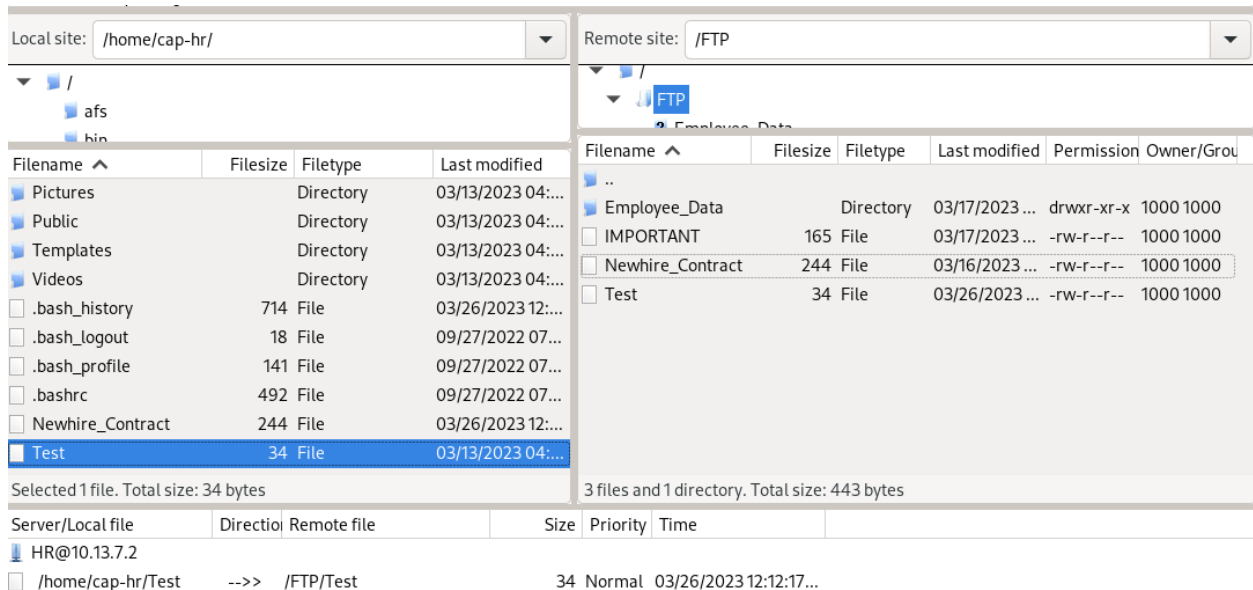


Figure 7.3 - Successful Host to Server FTP transfer

Show IP Route: R1-Leg

The command 'sh ip route' was issued on R1-Leg to provide the routing table for R1-Leg. The screenshot below demonstrates the results of the command below.

```

R1-Leg#sh 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
       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
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.13.1.0/24 is directly connected, GigabitEthernet0/0
L       10.13.1.1/32 is directly connected, GigabitEthernet0/0
R       10.13.2.0/24 [120/1] via 10.13.5.2, 00:00:16, GigabitEthernet0/1
R       10.13.4.0/24 [120/2] via 10.13.5.2, 00:00:16, GigabitEthernet0/1
C       10.13.5.0/24 is directly connected, GigabitEthernet0/1
L       10.13.5.1/32 is directly connected, GigabitEthernet0/1
R       10.13.6.0/24 [120/1] via 10.13.5.2, 00:00:16, GigabitEthernet0/1
R       10.13.7.0/24 [120/2] via 10.13.5.2, 00:00:16, GigabitEthernet0/1
R1-Leg#

```

Figure 8.1 - Output of 'sh ip route' command

The codes are listed out and the subnets for the network are listed as well. There are two connected routes, 10.13.5.0/24 (The connection to R2) and, 10.13.1.0/24 (The connection to the fedora VM). In addition to this, the command lists the two locally connected routes, both ending in .1, which is 10.13.1.1 and 10.13.5.1. Lastly, there are 4 RIP routes, which are shared from the other routers, and are the remaining network segments.

Show IP Route: R2-Fin

The command 'sh ip route' was issued on R2-Fin to provide the routing table for R2-Fin.

The screenshot below demonstrates the results of the command below.

```
R2-Fin#sh 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
       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
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
R    10.13.1.0/24 [120/1] via 10.13.5.1, 00:00:05, GigabitEthernet0/1
C    10.13.2.0/24 is directly connected, GigabitEthernet0/0
L    10.13.2.1/32 is directly connected, GigabitEthernet0/0
R    10.13.4.0/24 [120/1] via 10.13.6.2, 00:00:13, GigabitEthernet0/2
C    10.13.5.0/24 is directly connected, GigabitEthernet0/1
L    10.13.5.2/32 is directly connected, GigabitEthernet0/1
C    10.13.6.0/24 is directly connected, GigabitEthernet0/2
L    10.13.6.1/32 is directly connected, GigabitEthernet0/2
R    10.13.7.0/24 [120/1] via 10.13.6.2, 00:00:13, GigabitEthernet0/2
R2-Fin#
```

Figure 9.1 - Output of 'sh ip route' command

The codes are listed out and the subnets for the network are listed as well. There are three connected routes, 10.13.2.0/24 (The connection to Sw-1), 10.13.5.0/24 (The connection to R1), and 10.13.6.0/24 (The connection to R3). The command lists the three locally connected routes, two ending in .1, and one ending in .2. These are the connections to Sw-1, R3, and R1 respectively. Lastly, there are 3 RIP routes, which are shared from the other routers, and are the remaining network segments.

Show IP Route: R3-HR

The command 'sh ip route' was issued on R3-HR to provide the routing table for R3-HR.

The screenshot below demonstrates the results of the command below.

```
R3-HR#sh 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
       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
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
R    10.13.1.0/24 [120/2] via 10.13.6.1, 00:00:04, GigabitEthernet0/2
R    10.13.2.0/24 [120/1] via 10.13.6.1, 00:00:04, GigabitEthernet0/2
C    10.13.4.0/24 is directly connected, GigabitEthernet0/0
L    10.13.4.1/32 is directly connected, GigabitEthernet0/0
R    10.13.5.0/24 [120/1] via 10.13.6.1, 00:00:04, GigabitEthernet0/2
C    10.13.6.0/24 is directly connected, GigabitEthernet0/2
L    10.13.6.2/32 is directly connected, GigabitEthernet0/2
C    10.13.7.0/24 is directly connected, GigabitEthernet0/1
L    10.13.7.1/32 is directly connected, GigabitEthernet0/1
R3-HR#
```

Figure 10.1 - Output of the 'sh ip route' command

The codes are listed out and the subnets for the network are listed as well. There are three connected routes, 10.13.4.0/24 (The connection to the VM), 10.13.6.0/24 (The connection to R2), and 10.13.7.0/24 (The connection to the FTP server). The command lists the three locally connected routes, two ending in .1, and one ending in .2. These are the connections to Cap-HR-1, Cap-FTP-Serv-1, and R2 respectively. Lastly, there are 3 RIP routes, which are shared from the other routers, and are the remaining network segments.

Show IP Access-List: R1-Leg

To verify the created access list, the 'sh ip access-list' command was issued from R1-Leg.

```
R1-Leg#sh ip access-list
Extended IP access list 101
 10 deny tcp any any eq smtp log
 20 permit icmp any any (28 matches)
 30 permit tcp any any
Extended IP access list sl_def_acl
 10 deny tcp any any eq telnet log
 20 deny tcp any any eq www log
 30 deny tcp any any eq 22 log
 40 permit ip any any log
R1-Leg#
```

Figure 11.1 - Output of 'sh ip access-list' on R1-Leg

There are two extended IP access-lists: 101 which was manually created, and has 1 deny statement blocking SMTP traffic, and 2 permit statements, allowing ICMP traffic and other tcp traffic. This was applied to interface G0/0, outbound.

The second extended IP access-list, sl_def_acl, was manually added by the Cisco router, and is the "secure login default ACL". This is automatically added by the Cisco IOS, but was not applied to any interfaces.

Show IP Access-List: R2-Fin

To verify the created access list, the 'sh ip access-list' command was issued from R2-Fin.

```
R2-Fin#sh ip access-list
Extended IP access list 102
 10 deny tcp any any eq smtp log
 20 permit icmp any any (32 matches)
 30 permit tcp any any
Extended IP access list sl_def_acl
 10 deny tcp any any eq telnet log
 20 deny tcp any any eq www log
 30 deny tcp any any eq 22 log
 40 permit ip any any log
R2-Fin#
```

Figure 12.1 - Output of 'sh ip access-list' command on R2-Fin

There are two extended IP access-lists: 102 which was manually created, and has 1 deny statement blocking SMTP traffic, and 2 permit statements, allowing ICMP traffic and other tcp traffic. This was applied to interface G0/0, outbound.

The second extended IP access-list, sl_def_acl, was manually added by the Cisco router, and is the "secure login default ACL". This is automatically added by the Cisco IOS, but was not applied to any interfaces.

Show IP Access-List: R3-HR

To verify the created access list, the 'sh ip access-list' command was issued from R3-HR.

```
R3-HR#sh ip access-list
Extended IP access list 103
 10 deny tcp any any eq smtp log
 20 permit icmp any any (28 matches)
 30 permit tcp any any
Extended IP access list sl_def_acl
 10 deny tcp any any eq telnet log
 20 deny tcp any any eq www log
 30 deny tcp any any eq 22 log
 40 permit ip any any log
R3-HR#
```

Figure 13.1 - Output of 'sh ip access-list' command on R3-HR

There are two extended IP access-lists: 104 which was manually created, and has 1 deny statement blocking SMTP traffic, and 2 permit statements, allowing ICMP traffic and other tcp traffic. This was applied to interface G0/0, outbound.

The second extended IP access-list, sl_def_acl, was manually added by the Cisco router, and is the "secure login default ACL". This is automatically added by the Cisco IOS, but was not applied to any interfaces.

Show Run: R1-Leg

The following is the output of the 'Sh run' command for R1-Leg, and demonstrates all of the commands and security measures taken. The default Cisco banners were left in to prove the ISO images are officially licensed by Cisco.

```
R1-Leg#sh run
```

```
Building configuration...
```

```
Current configuration : 3789 bytes
```

```
!
```

```
version 15.7
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname R1-Leg
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
enable secret 5 $1$Wor1$2YYGy8ciscOehwq7Khq6i/
```

```
!
```

```
no aaa new-model
```

```
!
```

```
!
```

```
!
```

```
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
!
!
!
!
no ip domain lookup
ip cef
login block-for 120 attempts 2 within 60
login on-failure log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
```

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

!

!

!

interface GigabitEthernet0/0

ip address 10.13.1.1 255.255.255.0

ip access-group 101 out

duplex auto

speed auto

media-type rj45

!

interface GigabitEthernet0/1

ip address 10.13.5.1 255.255.255.0

duplex auto

```
speed auto
media-type rj45
!
interface GigabitEthernet0/2
ip address 10.13.8.1 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
!
router rip
version 2
network 10.0.0.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
ipv6 ioam timestamp
```

!

!

access-list 101 remark For denying email traffic

access-list 101 deny tcp any any eq smtp log

access-list 101 permit icmp any any

access-list 101 permit tcp any any

!

control-plane

!

banner exec ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *

* education. IOSv is provided as-is and is not supported by Cisco's *

* Technical Advisory Center. Any use or disclosure, in whole or in part, *

* of the IOSv Software or Documentation to any third party for any *

* purposes is expressly prohibited except as otherwise authorized by *

* Cisco in writing. *

*****^C

banner incoming ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *

* education. IOSv is provided as-is and is not supported by Cisco's *

* Technical Advisory Center. Any use or disclosure, in whole or in part, *

* of the IOSv Software or Documentation to any third party for any *

* purposes is expressly prohibited except as otherwise authorized by *

* Cisco in writing. *

*****^C

banner login ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *
 * education. IOSv is provided as-is and is not supported by Cisco's *
 * Technical Advisory Center. Any use or disclosure, in whole or in part, *
 * of the IOSv Software or Documentation to any third party for any *
 * purposes is expressly prohibited except as otherwise authorized by *
 * Cisco in writing. *

*****^C

```
banner motd ^CAUTHORIZED USERS ONLY - UNAUTHORIZED USERS WILL BE HUNTED BY THE
LAW!^C
```

```
!
```

```
line con 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
password 7 113A1F1551160D00567A797769
```

```
logging synchronous
```

```
login
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
password 7 0538030C345E1D3918504253
```

```
login
```

```
transport input none
```

```
line vty 5 9
```

```
password 7 04680E051A331F7E084C5056
```

```
login
```

transport input none

line vty 10 15

password 7 012003074E19553F20191B48

login

transport input none

!

no scheduler allocate

!

end

R1-Leg#

Show Run: R2-Fin

The following is the output of the 'Sh run' command for R2-Fin, and demonstrates all of the commands and security measures taken. The default Cisco banners were left in to prove the ISO images are officially licensed by Cisco.

```
R2-Fin#sh run
```

```
Building configuration...
```

```
Current configuration : 3720 bytes
```

```
!
```

```
version 15.7
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname R2-Fin
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
enable secret 5 $1$cln9$fKo/1tt/HThkUi8hjsVZ1
```

```
!
```

```
no aaa new-model
```

```
!
```

```
!
```

```
!
```

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

!

!

!

!

!

no ip icmp rate-limit unreachable

!

!

!

!

!

!

no ip domain lookup

ip cef

login block-for 120 attempts 2 within 60

login on-failure log

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

!

!

!

interface GigabitEthernet0/0

ip address 10.13.2.1 255.255.255.0

ip access-group 102 out

duplex auto

speed auto

media-type rj45

!

interface GigabitEthernet0/1

ip address 10.13.5.2 255.255.255.0

duplex auto

```
speed auto
media-type rj45
!
interface GigabitEthernet0/2
ip address 10.13.6.1 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
!
router rip
version 2
network 10.0.0.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
ipv6 ioam timestamp
```

!

!

access-list 102 remark For stopping external email traffic

access-list 102 deny tcp any any eq smtp log

access-list 102 permit icmp any any

access-list 102 permit tcp any any

!

control-plane

!

banner exec ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *

* education. IOSv is provided as-is and is not supported by Cisco's *

* Technical Advisory Center. Any use or disclosure, in whole or in part, *

* of the IOSv Software or Documentation to any third party for any *

* purposes is expressly prohibited except as otherwise authorized by *

* Cisco in writing. *

*****^C

banner incoming ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *

* education. IOSv is provided as-is and is not supported by Cisco's *

* Technical Advisory Center. Any use or disclosure, in whole or in part, *

* of the IOSv Software or Documentation to any third party for any *

* purposes is expressly prohibited except as otherwise authorized by *

* Cisco in writing. *

*****^C

banner login ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *
 * education. IOSv is provided as-is and is not supported by Cisco's *
 * Technical Advisory Center. Any use or disclosure, in whole or in part, *
 * of the IOSv Software or Documentation to any third party for any *
 * purposes is expressly prohibited except as otherwise authorized by *
 * Cisco in writing. *

*****^C

banner motd ^CAUTHORIZED USERS ONLY - UNAUTHORIZED USERS WILL BE HUNTED BY THE L
 AW!^C

!

line con 0

exec-timeout 0 0

privilege level 15

password 7 08124A5E4F1D031B405B5E576B

logging synchronous

login

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

line vty 0 4

password 7 15210E0F1138781429666063

login

transport input none

line vty 5 15

password 7 06350A22595C5A290442474A

login

transport input none

!

no scheduler allocate

!

end

R2-Fin#

Show Run: R3-HR

The following is the output of the 'Sh run' command for R3-HR, and demonstrates all of the commands and security measures taken. The default Cisco banners were left in to prove the ISO images are officially licensed by Cisco.

```
R3-HR#sh run
```

```
Building configuration...
```

```
Current configuration : 3719 bytes
```

```
!
```

```
version 15.7
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname R3-HR
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
enable secret 5 $1$wZ1O$CPjyGcQmq/jOT5ld2.iBX1
```

```
!
```

```
no aaa new-model
```

```
!
```

```
!
```

```
!
```


mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

!

!

!

!

!

no ip icmp rate-limit unreachable

!

!

!

!

!

!

no ip domain lookup

ip cef

login block-for 120 attempts 2 within 60

login on-failure log

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

!

```
redundancy
```

```
!
```

```
no cdp log mismatch duplex
```

```
!
```

```
ip tcp synwait-time 5
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
interface GigabitEthernet0/0
```

```
ip address 10.13.4.1 255.255.255.0
```

```
ip access-group 103 out
```

```
duplex auto
```

```
speed auto
```

```
media-type rj45
```

```
!
```

```
interface GigabitEthernet0/1
```

```
ip address 10.13.7.1 255.255.255.0
```

```
duplex auto
```

```
speed auto
media-type rj45
!
interface GigabitEthernet0/2
ip address 10.13.6.2 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
!
router rip
version 2
network 10.0.0.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
ipv6 ioam timestamp
```

!

!

access-list 103 remark For stopping external email traffic

access-list 103 deny tcp any any eq smtp log

access-list 103 permit icmp any any

access-list 103 permit tcp any any

!

control-plane

!

banner exec ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *

*****^C

banner incoming ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *

*****^C

banner login ^C

FINAL PROJECT

100

* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *

*****^C

```
banner motd ^CAUTHORIZED USERS ONLY - UNAUTHORIZED USERS WILL BE HUNTED BY THE  
LAW!^C
```

```
!
```

```
line con 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
password 7 15210D1C422E2D287A63677152
```

```
logging synchronous
```

```
login
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
password 7 097F4B0A0C1744220A59516B
```

```
login
```

```
transport input none
```

```
line vty 5 15
```

```
password 7 113A1C060200583C057F7E65
```

```
login
```

FINAL PROJECT
101

transport input none

!

no scheduler allocate

!

end

R3-HR#

FINAL PROJECT

102

Show Run: Sw-1

The following is the output of the 'Sh run' command for Sw-1, and demonstrates all of the commands and security measures taken. The default Cisco banners were left in to prove the ISO images are officially licensed by Cisco.

```
Sw1#sh run
```

```
Building configuration...
```

```
Current configuration : 4854 bytes
```

```
!
```

```
! Last configuration change at 17:14:44 UTC Sun Mar 26 2023
```

```
!
```

```
version 15.2
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
service compress-config
```

```
!
```

```
hostname Sw1
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
enable secret 5 $1$UXun$hpOHhmQpRYRtoD9cfo5j91
```

```
!
```

```
no aaa new-model
```

FINAL PROJECT

103

!

!

!

!

!

!

!

!

no ip domain-lookup

ip cef

no ipv6 cef

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

!

!

!

!

!

!

!

!

!

!

!

FINAL PROJECT

104

!

!

!

```
interface GigabitEthernet0/0
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
negotiation auto
```

!

```
interface GigabitEthernet0/1
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
negotiation auto
```

!

```
interface GigabitEthernet0/2
```

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

!

```
interface GigabitEthernet0/3
```

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

!

```
interface GigabitEthernet1/0
```

```
switchport access vlan 30
```

```
switchport mode access
```

FINAL PROJECT

105

shutdown

negotiation auto

!

interface GigabitEthernet1/1

switchport access vlan 30

switchport mode access

shutdown

negotiation auto

!

interface GigabitEthernet1/2

switchport access vlan 30

switchport mode access

shutdown

negotiation auto

!

interface GigabitEthernet1/3

switchport access vlan 30

switchport mode access

shutdown

negotiation auto

!

interface GigabitEthernet2/0

switchport access vlan 30

switchport mode access

shutdown

negotiation auto

!

interface GigabitEthernet2/1

FINAL PROJECT

106

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

```
!
```

```
interface GigabitEthernet2/2
```

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

```
!
```

```
interface GigabitEthernet2/3
```

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

```
!
```

```
interface GigabitEthernet3/0
```

```
no switchport
```

```
no ip address
```

```
shutdown
```

```
negotiation auto
```

```
!
```

```
interface GigabitEthernet3/1
```

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

FINAL PROJECT

107

!

```
interface GigabitEthernet3/2
```

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

!

```
interface GigabitEthernet3/3
```

```
switchport access vlan 30
```

```
switchport mode access
```

```
shutdown
```

```
negotiation auto
```

!

```
interface Vlan1
```

```
no ip address
```

!

```
interface Vlan2
```

```
no ip address
```

```
shutdown
```

!

```
interface Vlan10
```

```
ip address 10.13.2.2 255.255.255.0
```

!

```
interface Vlan30
```

```
no ip address
```

```
shutdown
```

!

```
interface Group-Async0
```

FINAL PROJECT

108

physical-layer async

no ip address

encapsulation slip

!

router rip

version 2

network 10.0.0.0

!

ip default-gateway 10.13.2.1

ip forward-protocol nd

!

ip http server

!

ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr

ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr

!

!

!

!

!

!

control-plane

!

banner exec ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *

* education. IOSv is provided as-is and is not supported by Cisco's *

* Technical Advisory Center. Any use or disclosure, in whole or in part, *

FINAL PROJECT

109

* of the IOSv Software or Documentation to any third party for any *

* purposes is expressly prohibited except as otherwise authorized by *

* Cisco in writing. *

*****^C

banner incoming ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *

* education. IOSv is provided as-is and is not supported by Cisco's *

* Technical Advisory Center. Any use or disclosure, in whole or in part, *

* of the IOSv Software or Documentation to any third party for any *

* purposes is expressly prohibited except as otherwise authorized by *

* Cisco in writing. *

*****^C

banner login ^C

* IOSv is strictly limited to use for evaluation, demonstration and IOS *

* education. IOSv is provided as-is and is not supported by Cisco's *

* Technical Advisory Center. Any use or disclosure, in whole or in part, *

* of the IOSv Software or Documentation to any third party for any *

* purposes is expressly prohibited except as otherwise authorized by *

* Cisco in writing. *

*****^C

banner motd ^CAUTHORIZED USERS ONLY - UNAUTHORIZED USERS WILL BE HUNTED BY THE

LAW!^C

!

line con 0

password 7 107D0F09431314075E54787865

login

FINAL PROJECT

110

line aux 0

line vty 0 4

password 7 122A001407195F342B7E7169

login

line vty 5 15

password 7 023501581E145C114D1B5C58

login

!

!

end

Sw1#

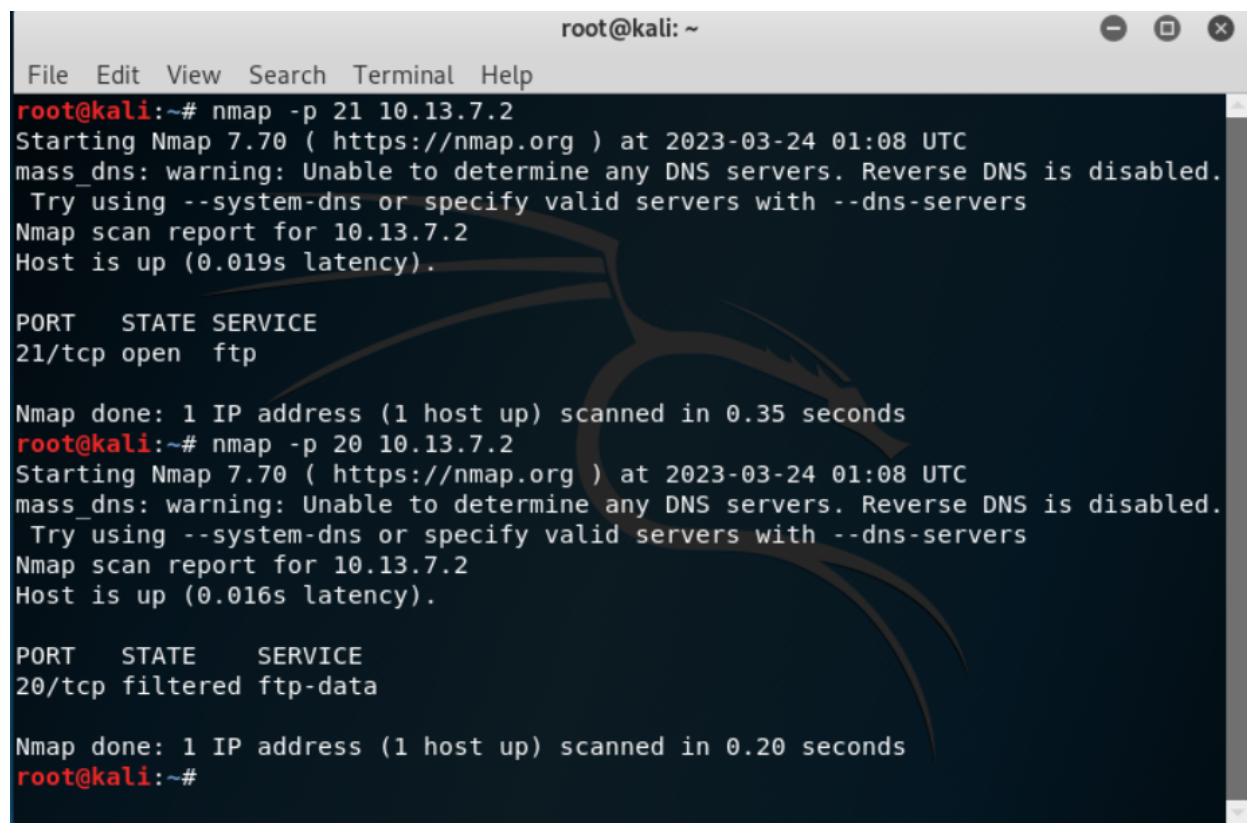
Nmap Documentation

With the Kali Linux machine, the following commands were issued from the terminal:

```
nmap -p 20 10.13.7.2
```

```
nmap -p 21 10.13.7.2
```

These commands would perform a scan of port 20 and 21 for the end host 10.13.7.2, Cap-FTP-Serv-1. The screenshots below show the output of the commands.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 21 10.13.7.2
Starting Nmap 7.70 ( https://nmap.org ) at 2023-03-24 01:08 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.13.7.2
Host is up (0.019s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@kali:~# nmap -p 20 10.13.7.2
Starting Nmap 7.70 ( https://nmap.org ) at 2023-03-24 01:08 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.13.7.2
Host is up (0.016s latency).

PORT      STATE  SERVICE
20/tcp    filtered ftp-data

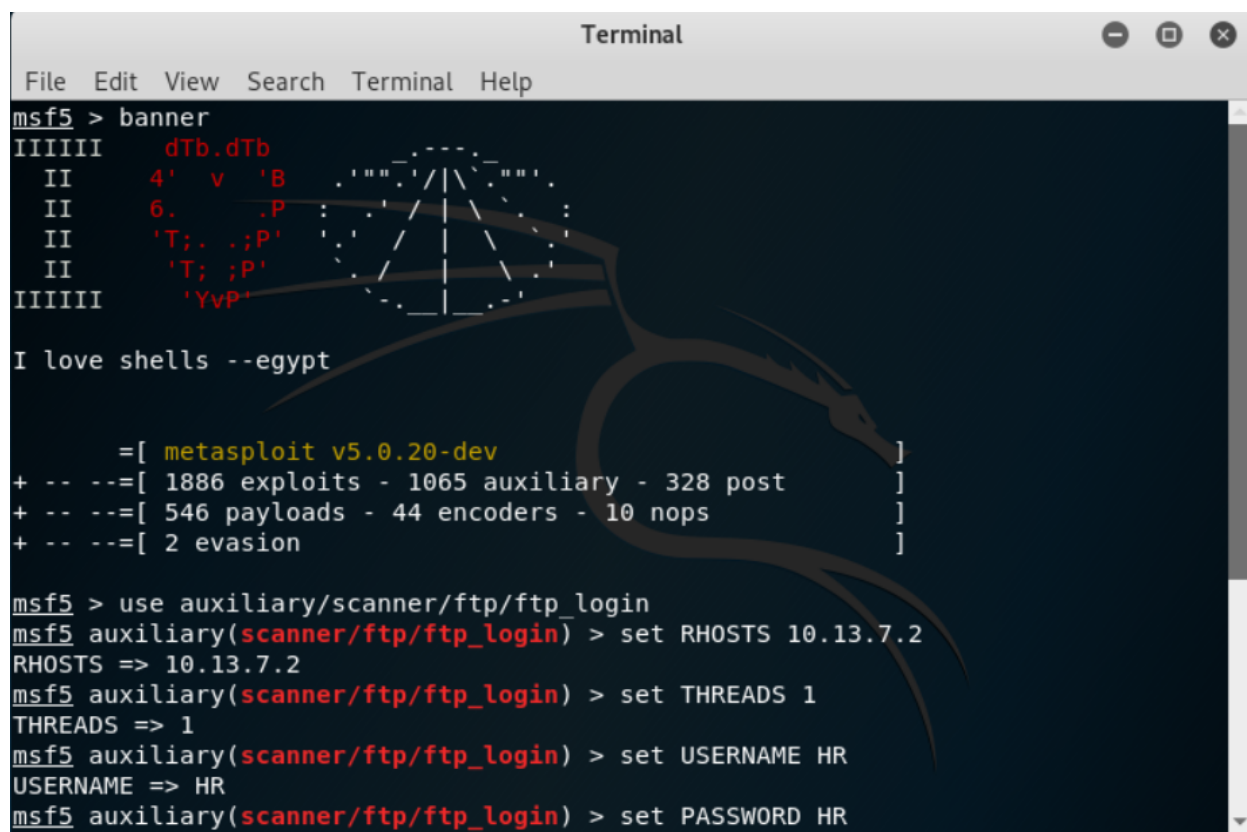
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@kali:~#
```

Figure 18.1 - Output of nmap command

As seen in the screenshot, when scanning port 21, it is revealed to be open, and providing the standard ftp service. When scanning port 20, it is listed as filtered, which means there could be a firewall, or other blocking method in place preventing nmap from getting the exact status of the port.

Metasploit Documentation

With the Kali machine, from the msfconsole, or metasploit was used to perform two actions against the FTP server. The actions of the commands are in the screenshots below.

A screenshot of a terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the Metasploit banner, which includes ASCII art and the text "I love shells --egypt". Below the banner, the terminal displays the output of the 'banner' command, showing the Metasploit version (v5.0.20-dev) and a summary of available exploits, auxiliary modules, payloads, encoders, nops, and evasion techniques. The terminal then shows the user entering the 'use auxiliary/scanner/ftp/ftp_login' command, followed by setting 'RHOSTS' to '10.13.7.2', 'THREADS' to '1', 'USERNAME' to 'HR', and 'PASSWORD' to 'HR'.

```
msf5 > banner
IIIIII  dTb.dTb
  II    4' v 'B
  II    6. .P
  II    'T; . ;P'
  II    'T; ;P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v5.0.20-dev ]
+ -- --=[ 1886 exploits - 1065 auxiliary - 328 post ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops ]
+ -- --=[ 2 evasion ]

msf5 > use auxiliary/scanner/ftp/ftp_login
msf5 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 10.13.7.2
RHOSTS => 10.13.7.2
msf5 auxiliary(scanner/ftp/ftp_login) > set THREADS 1
THREADS => 1
msf5 auxiliary(scanner/ftp/ftp_login) > set USERNAME HR
USERNAME => HR
msf5 auxiliary(scanner/ftp/ftp_login) > set PASSWORD HR
```

Figure 19.1 - Output of metasploit terminal

```
msf5 auxiliary(scanner/ftp/ftp_login) > set PASSWORD HR
PASSWORD => HR
msf5 auxiliary(scanner/ftp/ftp_login) > set VERBOSE false
VERBOSE => false
msf5 auxiliary(scanner/ftp/ftp_login) > ruf
^CInterrupt: use the 'exit' command to quit
msf5 auxiliary(scanner/ftp/ftp_login) > run

[*] 10.13.7.2:21 - 10.13.7.2:21 - Starting FTP login sweep
[+] 10.13.7.2:21 - 10.13.7.2:21 - Login Successful: HR:HR
[*] 10.13.7.2:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_login) > █
```

Figure 19.2 - Output of metasploit terminal

```
Terminal
File Edit View Search Terminal Help
msf5 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.13.7.2
RHOSTS => 10.13.7.2
msf5 auxiliary(scanner/ftp/ftp_version) > set THREADS 1
THREADS => 1
msf5 auxiliary(scanner/ftp/ftp_version) > run

[+] 10.13.7.2:21 - FTP Banner: '220 (vsFTPd 3.0.5)\x0d\x0a'
[*] 10.13.7.2:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_version) > █
```

Figure 19.3 - Output of metasploit terminal

As seen in the first two screenshots, the metasploit command: *use auxiliary/scanner/ftp/ftp_login* was entered, which allows metasploit to attempt to login to a known FTP server. The *RHOSTS* command was used to set the target for the FTP Login. The *THREADS* command was used to specify the processing power that should be devoted to completing the command. The *USERNAME* and *PASSWORD* commands were used to enter in the credentials that would be used when metasploit attempted the login. *VERBOSE False* was to turn off the verbose mode. The *RUN* command was used to start the login process. After the *run* command is entered, there is a successful login attempt of the FTP server by metasploit.

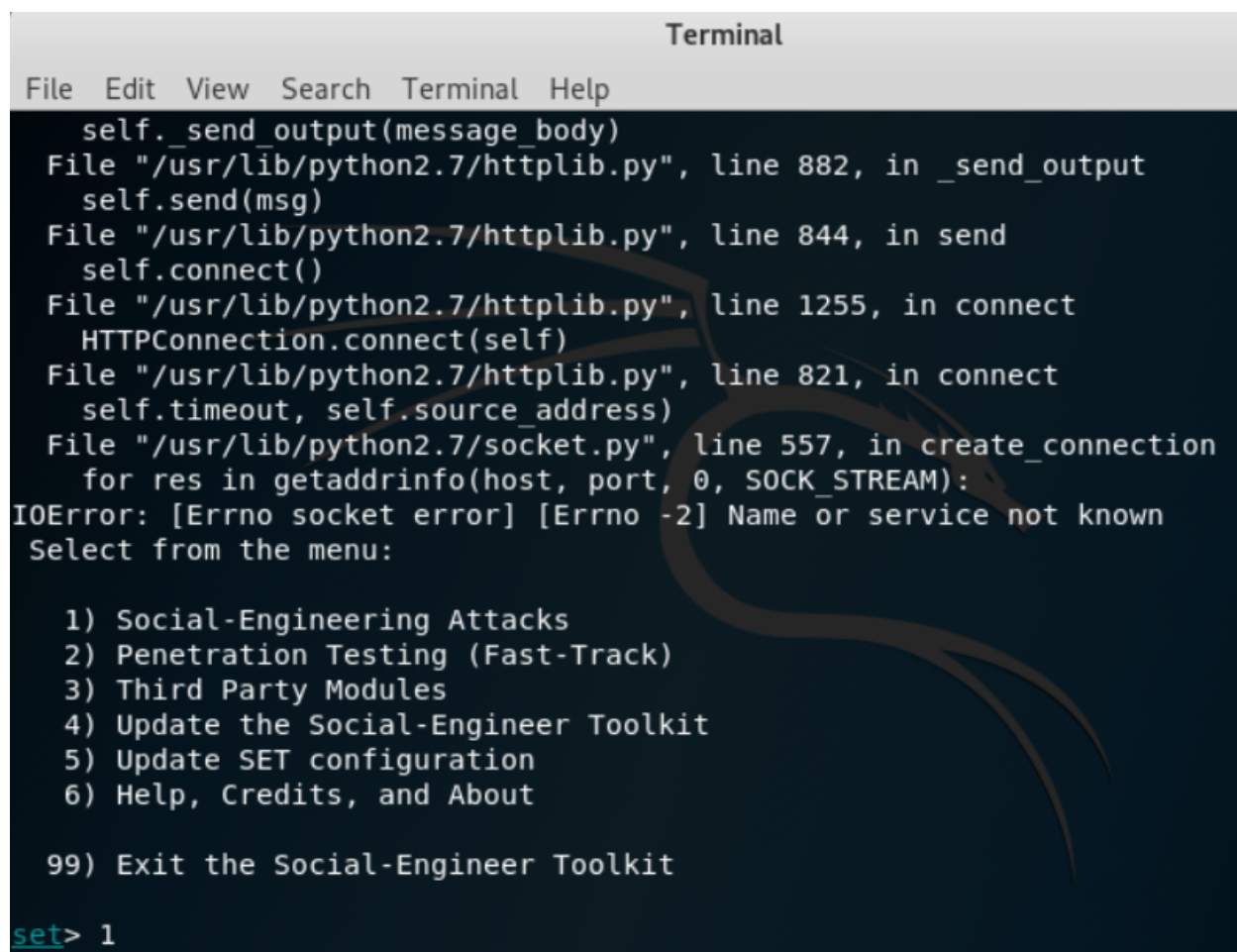
FINAL PROJECT

114

The last screenshot uses the command *use auxiliary/scanner/ftp/ftp_version* and is used to gather the version of a specified FTP server. The RHOSTS is set to 10.13.7.2, the THREADS are set to 1, and the command is run. The returned version is vsFTPd 3.0.5.

Social Engineer's Toolkit Documentation

The Social Engineer's Toolkit (SET) was used to attempt to create a phishing email template that would be used. After SET is opened in a terminal window, option 1, Social-Engineering Attacks is entered.

A terminal window titled "Terminal" with a menu bar containing "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows a series of Python stack trace lines: "self._send_output(message_body)", "File "/usr/lib/python2.7/httplib.py", line 882, in _send_output", "self.send(msg)", "File "/usr/lib/python2.7/httplib.py", line 844, in send", "self.connect()", "File "/usr/lib/python2.7/httplib.py", line 1255, in connect", "HTTPConnection.connect(self)", "File "/usr/lib/python2.7/httplib.py", line 821, in connect", "self.timeout, self.source_address)", "File "/usr/lib/python2.7/socket.py", line 557, in create_connection", "for res in getaddrinfo(host, port, 0, SOCK_STREAM):", "IOError: [Errno socket error] [Errno -2] Name or service not known". Below the error, it says "Select from the menu:" followed by a numbered list: "1) Social-Engineering Attacks", "2) Penetration Testing (Fast-Track)", "3) Third Party Modules", "4) Update the Social-Engineer Toolkit", "5) Update SET configuration", "6) Help, Credits, and About", and "99) Exit the Social-Engineer Toolkit". At the bottom, the prompt "set> 1" is visible.

```
Terminal
File Edit View Search Terminal Help
self._send_output(message_body)
File "/usr/lib/python2.7/httplib.py", line 882, in _send_output
self.send(msg)
File "/usr/lib/python2.7/httplib.py", line 844, in send
self.connect()
File "/usr/lib/python2.7/httplib.py", line 1255, in connect
HTTPConnection.connect(self)
File "/usr/lib/python2.7/httplib.py", line 821, in connect
self.timeout, self.source_address)
File "/usr/lib/python2.7/socket.py", line 557, in create_connection
for res in getaddrinfo(host, port, 0, SOCK_STREAM):
IOError: [Errno socket error] [Errno -2] Name or service not known
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

Figure 20.1 - Output of SET terminal

On the next menu, option 5, Mass Mailer Attack, is selected.

```
Terminal
File Edit View Search Terminal Help
File "/usr/lib/python2.7/httplib.py", line 1255, in connect
  HTTPConnection.connect(self)
File "/usr/lib/python2.7/httplib.py", line 821, in connect
  self.timeout, self.source_address)
File "/usr/lib/python2.7/socket.py", line 557, in create_connection
  for res in getaddrinfo(host, port, 0, SOCK_STREAM):
IOError: [Errno socket error] [Errno -2] Name or service not known
Select from the menu:

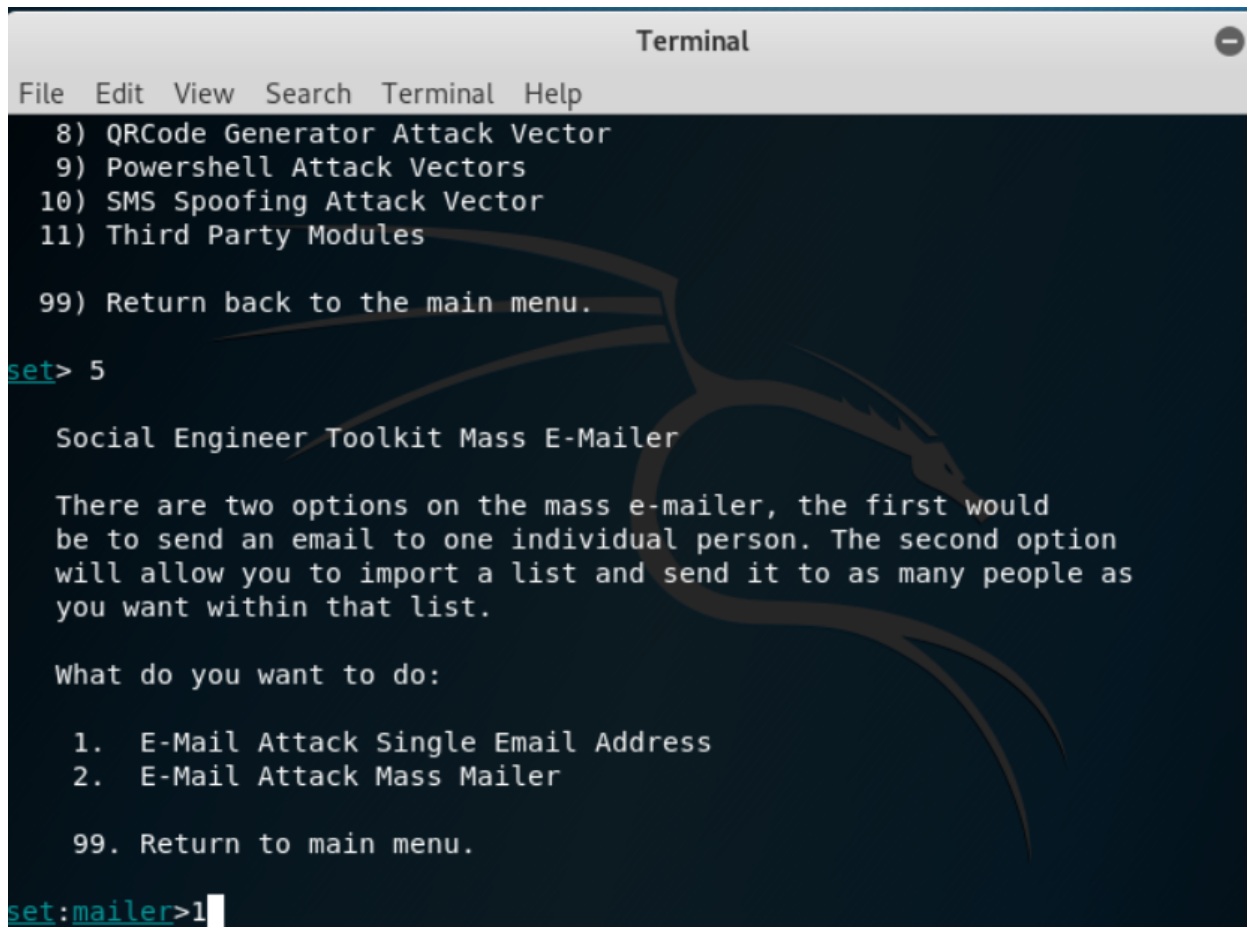
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 5
```

Figure 20.2 - Output of SET terminal

On the next menu, option 1, Email Attack Single Email Address is selected.



```
Terminal
File Edit View Search Terminal Help
 8) QRCode Generator Attack Vector
 9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.
set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

 1. E-Mail Attack Single Email Address
 2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
```

Figure 20.3 - Output of SET terminal

On the next menu, the following email address is entered: Legal@internal.com.

```
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
set:phishing> Send email to:Legal@internal.com
```

Figure 20.4 - Output of SET terminal

On the next menu, option 2, Use your own server or open relay, is selected.

```
set:mailer>1
set:phishing> Send email to:Legal@internal.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>2
```

Figure 20.5 - Output of SET terminal

On the next menu, the 'from address' is entered as HR@interna1.com.

```
set:mailer>1
set:phishing> Send email to:Legal@internal.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):HR@internal.com
```

Figure 20.6 - Output of SET terminal

On the next menu, the 'FROM NAME the user will see' is entered as HR@internal.com.

```
set:mailer>1
set:phishing> Send email to:Legal@internal.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):HR@internal.com
set:phishing> The FROM NAME the user will see:HR@internal.com
```

Figure 20.7 - Output of SET terminal

On the next menu, the SMTP email server is entered as smtp.mailserver.com.

```
set:phishing>2
set:phishing> From address (ex: moo@example.com):HR@internal.com
set:phishing> The FROM NAME the user will see:HR@internal.com
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smtp.mailserver.com
```

Figure 20.8 - Output of SET terminal

On the next menu, the port number is entered as 25, the message will be flagged with high priority, no file or inline file is attached, and the email subject and message is created in plaintext. END is entered to signify the end of the message.

```
set:phishing>2
set:phishing> From address (ex: moo@example.com):HR@internal.com
set:phishing> The FROM NAME the user will see:HR@internal.com
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smtp.mailserver.com
set:phishing> Port number for the SMTP server [25]:25
set:phishing> Flag this message/s as high priority? [yes|no]:y
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Thanks!
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:
Thank you for all that you do!
Next line of the body: Click the link for a suprise!
```

Figure 20.9 - Output of SET terminal

All of the above steps were taken and the email would be sent if there was a functioning SMTP server. The email would be sent to the end user, but stopped by the ACLs on the routers preventing traffic from port 25 from reaching end users.

References

- Academy , C. (2023). Software Download. Retrieved March 21, 2023, from <https://software.cisco.com/download/home/286290254/type/286290305/release/OSvL2>
- Beasts 4, S. (2022). *Vsftpd.conf(5) - linux man page*. vsftpd.conf(5): config file for vsftpd - Linux man page. Retrieved March 21, 2023, from <https://linux.die.net/man/5/vsftpd.conf>
- Cerda, A. (2021, December 25). Cannot load the GNS3 VM dialog: Not dialog: Not connected to the Controller. Retrieved February 28, 2023, from <https://www.youtube.com/watch?v=4DfAqROpoz8>
- Cisco Academy . (2023). *Cisco Modeling Labs - Personal*. Cisco Modeling Labs - Personal - The Cisco Learning Network Store. Retrieved February 15, 2023, from <https://learningnetworkstore.cisco.com/cisco-modeling-labs-personal/cisco-modeling-labs-personal/CML-PERSONAL.html>
- Courses, D. (2012, February 28). *Standard Access List (ACL) for the CISCO CCNA - Part 1*. YouTube. Retrieved March 20, 2023, from <https://www.youtube.com/watch?v=4PPUvRj2PvM>
- Direction, N. (2023, March 3). *CML Installation*. Network Direction. Retrieved February 15, 2023, from <https://networkdirection.net/articles/cml/cml-installation/>
- Foxdk, & Pontifexludaeacus. (2019). *R/GNS3 - buying Cisco Virl Images*. r/gns3 - Buying Cisco VIRT images. Retrieved January 25, 2023, from https://www.reddit.com/r/gns3/comments/bbnamz/buying_cisco_virl_images/
- Gene, N. (2021, January 12). *Setting up the GNS3 VM server*. Nstudy. Retrieved February 28, 2023, from <https://www.n-study.com/en/how-to-use-gns3/gns3-vm-server-setup/>
- GNS3, G. H. (2023, February 28). *Releases · GNS3/GNS3-gui*. Version 2.2.38. Retrieved March 1, 2023, from <https://github.com/GNS3/gns3-gui/releases>
- GNS3. (2022, December 3). *[vmware] unable to create Nio Ethernet for bridge ethernet0.vnet · issue #840 · GNS3/GNS3-gui*. Unable to Create NIO Ethernet Bridge. Retrieved March 11, 2023, from <https://github.com/GNS3/gns3-gui/issues/840>

- Hope, C. (2023, March 5). *How to use FTP from a command line*. Computer Hope. Retrieved March 13, 2023, from <https://www.computerhope.com/issues/ch001246.htm>
- Kovačević, A. (2022, October 21). *How to use the linux FTP command*. Knowledge Base by phoenixNAP. Retrieved March 13, 2023, from <https://phoenixnap.com/kb/linux-ftp>
- Nagori, A. I. (2021). How to configure a static IP address on Fedora? Retrieved March 14, 2023, from <https://linuxhint.com/configure-static-ip-address-fedora/>
- NetworkingNotes, C. (2022, July 18). *How to add, install or import IOS in GNS3*. ComputerNetworkingNotes. Retrieved February 15, 2023, from <https://www.computernetworkingnotes.com/ccna-study-guide/how-to-add-install-or-import-ios-in-gns3.html>
- Patel, V., & Bhatt, K. (2021, September 20). *Download gns3 ios image: How to install*. Download GNS3 iOS Image | How to Install. Retrieved February 18, 2023, from <https://devsjournal.com/download-gns3-ios-image.html>
- Sec, O. (2019, November 1). *Scanner FTP auxiliary modules - metasploit unleashed*. OffSec. Retrieved March 23, 2023, from <https://www.offsec.com/metasploit-unleashed/scanner-ftp-auxiliary-modules/>
- Server, U. (2023, February 24). *FTP Server*. Ubuntu. Retrieved March 21, 2023, from <https://ubuntu.com/server/docs/service-ftp>
- Simic, S. (2022, December 7). *How to install and configure FTP server on ubuntu with vsftpd*. Knowledge Base. Retrieved March 12, 2023, from <https://phoenixnap.com/kb/install-ftp-server-on-ubuntu-vsftpd>
- Systems, C. (2020). *CML Installation Guide*. Cisco Developer. Retrieved February 15, 2023, from <https://developer.cisco.com/docs/modeling-labs/#!cml-installation-guide>
- Tshepang, blong. (2011, January 17). *How to make Fedora User a sudoer?* Unix & Linux Stack Exchange. Retrieved March 20, 2023, from <https://unix.stackexchange.com/questions/4405/how-to-make-fedora-user-a-sudoer>
- Upravnik. (2023, February 14). *Configuring ripv2*. Study CCNA. Retrieved March 9, 2023, from <https://study-ccna.com/configuring-ripv2/>

FINAL PROJECT

123

Willins, O. (2019, August 24). *SL_DEF_ACL ?* Cisco Community. Retrieved March 23, 2023, from <https://community.cisco.com/t5/other-security-subjects/sl-def-acl/td-p/224967>

Xuan Nguyen, N. (2022, April 2). *How to setup FTP server with vsftpd*. ATA Learning. Retrieved March 16, 2023, from <https://adamtheautomator.com/vsftpd>