

The University of Akron

IdeaExchange@UAkron

Williams Honors College, Honors Research
Projects

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

Spring 2020

Gaming LAN setup with Local and Remote Access and Downloads

Ethelyn Tran
gmt17@zips.uakron.edu

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



Part of the [Information Security Commons](#), [OS and Networks Commons](#), and the [Systems Architecture 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

Tran, Ethelyn, "Gaming LAN setup with Local and Remote Access and Downloads" (2020). *Williams Honors College, Honors Research Projects*. 1074.

https://ideaexchange.uakron.edu/honors_research_projects/1074

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.

Gaming LAN setup with Local and Remote Access and Downloads

The University of Akron

Computer Information System (CIS): Senior Project
2440:491 – 001

Honors Project Sponsor:

Dr. J. Nicholas

Honors Project Reader:

Professor S. Smith
Professor M. Haines

Honors Faculty Advisor:

Advisor S. Hoge

Ethelyn Tran

13 April 2020

CIS: Senior Project

2440:491-001



Project Plan

Ethelyn Tran

Part I of VII

Project Proposal

Project Name:

Gaming LAN Setup with Local and Remote Access and Downloads

Team Member(s):

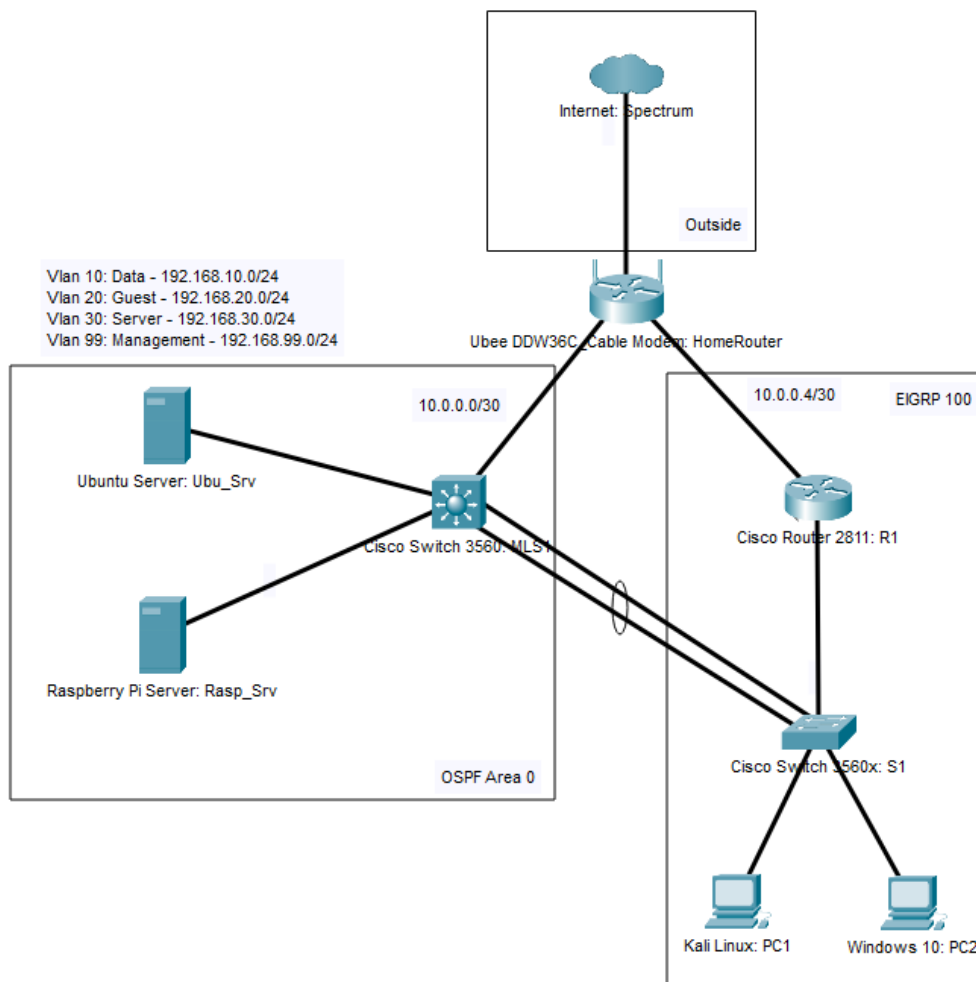
Ethelyn Tran

Project Summary:

The Gaming LAN Setup project aims to design and implement a functioning, hardened network that could be utilized locally and remotely to allow users to join or host gaming servers of choice. Users will have the ability to securely log into the internal network to join a session or download files via web interface. The hardened network will allow the designated user to take a management position in order to perform penetration testing and discover vulnerabilities to guard against possible hostile, online gamers.

Topology:

The topology was created using Cisco Packet Tracer. The cable modem, the router, the switches, and the end devices will be physical. Only the Ubuntu server (Ubu-Srv) end device will be virtual, using Oracle VM VirtualBox

**Location of Work:**

- Lab work will be set up at home in Akron, Ohio

Proposal Description

The goal for this project is to create a Gaming LAN setup that acts as a functioning, hardened network which could be utilized locally and remotely. The objective is to create a foundation network setup that can be built upon for customizable gaming servers. The secure network will include features that would allow users to securely login into a web interface to access listed sessions or personalized servers and to be able to download related files securely.

Gamers, playing multiplayer games, would often encounter a lack of resource to play with their friends in a private environment without the concern of random players joining in, especially hostile gamers. This setup would give home users opportunities to host their own servers and have all the necessary information to create a personalized community. In addition, one user may take a management or admin position to adjust the varying level of security, monitor the network, discover vulnerabilities and troubleshoot when necessary.

The home local area network (LAN) will be connected to the “outside” internet via Ubee Cable Modem Home Router provided by the Internet Service Provider (ISP) Spectrum. The network will further be divided into two area networks by a Cisco Multilayer Switch 3560 and a Cisco Router 2811 to securely separate the servers and end devices. The end devices could connect locally with a Cisco Switch 3560x. Layer 3 will be implemented with the best security practices to include their respectively routing protocols, NAT, IPSec Tunneling, ACLs and remote access. Along with the best security practices, Layer 2 will have VLAN, redundancy and priority protocol.

An Ubuntu server, hosting a very secure file transfer protocol daemon (VSFTPD), and a Raspbian Server, hosting a web interface, will be connected to the Cisco Multilayer Switch 3560. Moreover, The Raspbian server will be hosting Pi-Hole as a Domain Name System (DNS)

sinkhole in conjunction with hosting the Apache Server with NGINX for the front-end web interface. Through this, local and remote hosts may connect to the web interface and enter their respective login credentials to access information. The end device “PC1” will be operating in Kali Linux, a Debian OS, as a management or administration host. The admin role will be capable of accessing both servers with elevated privileges, using networking monitoring tools such as NMAP and Wireshark and using vulnerability scanners like OpenVAS. Kali Linux, equipped by open-source tools, will be performing penetration testing such as with John the Ripper tool and a denial-of-service (DoS) simulation.

As with most of information technology and security projects, the research required consists of ensuring the design and implementation are compatible and will function seamlessly between different vendors to work as intended. Although many tools are designed to work with many systems and applications, bugs and incompatibility issues may still occur whether it is in the lower hardware level or all the way up to the specific tools and applications, disrupting the topology. The project will predictably have errors to troubleshoot that will require further research into the resolution or workarounds. The overall project will be documented to include all stages of implementations, discoveries of errors and troubleshooting methods.

The project proposal undertook two (2) weeks of review before meeting the final approval of a Honors Project Sponsor, two Readers and a Faculty Advisor prior to being submitted online to the Williams Honors College for review and approval as well. Anticipated to take approximately 170 hours to complete to include everything from research, documentation binder to the presentation, the project is scheduled to be completed within nine (9) weeks before being submitted for evaluations by the Honors Project Sponsor. The Honors Project will not only advance my discipline but also be included to The University of Akron’s institutional repository

to contribute to higher learning. Afterwards, the project will be presented in a classroom setting with an audience of mostly student peers. The presentation will showcase my objectives, implementation of design, a video demonstration. The Honors Project Sponsor, the two readers and the Honors Faculty Advisor will be present to review my performance.

As the Cybersecurity major within the College of Applied Science & Technology (CAST) has just been recently introduced to the University of Akron, this senior project, along with other student peers' senior projects, will set a precedent for future senior project courses within the Computer Information System (CIS) curriculum. Set to graduate with both CIS: Cisco Networking and CIS: Cybersecurity major, this Honors Project will incorporate in depth learning of both networking skills and interlaced with the cybersecurity perspective. Having the opportunity to take a CIS Senior Project course as part of the overall curriculum, the Honors Senior Project will demonstrate not only what was learned but the capability of being able to apply skills to make real-world connections by engaging various scenarios. Not only will this project will act as a refresh learning strategy but will also afford the opportunity to showcase accumulated skills and to practice for future career projects.

Equipment:

- a. (1) Ubee DDW36C Cable Modem
- b. (1) Cisco 2811
- c. (1) Cisco Multilayer Switch 3560 with PoE
- d. (1) Cisco Switch 3560x with PoE
- e. (1) Microsoft Surface Pro
 - a. Windows 10
- f. (1) Toshiba Laptop
 - a. USB Persistent Kali Linux
- g. (1) Raspberry Pi 3
 - a. Raspbian OS
- h. (1) Desktop PC
 - a. Oracle VM Virtual Box: Ubuntu Server

Detailed Objectives:1) Research:

- a. Encryption standard and method of user's credentials
- b. Hosting Apache Server to include NGINX
- c. Web server's basic access authentication
- d. Implementation of Raspbian OS and integration of VSTFP
- e. Common exploits within HTML and TCP/IP Layer 4: Application
- f. Penetration testing tools: OpenVAS, John the Ripper
- g. Network monitoring tools: Pi-Hole, NMAP, Wireshark

2) Design:

- a. Topology:
 - i. Ensure physical and logical connections
 - ii. Ensure wiring and hardware reliability
 - iii. Ensure updated hardware and software versions
- b. Network Layout:
 - i. IP Address Layout
 - Spectrum provided public IP address
 - Cable Modem to MLS1: 10.0.0.0/30 255.255.255.252
 - Cable Modem to R1: 10.0.0.4/30 255.255.255.252
 - VLAN 10: Data – 192.168.10.0/24 255.255.255.0
 - VLAN 20: Guest – 192.168.20.0/24 255.255.255.0
 - VLAN 30: Server – 192.168.30.0/24 255.255.255.0
 - VLAN 99: Management – 192.168.99.0/24 255.255.255.0

- 3) Implementation:
 - a. Implement Spectrum Cable Modem
 - i. NAT Translation
 - ii. DHCP Server
 - iii. NTP Services
 - iv. Port-Forwarding Services
 - v. SSID and Security Password
 - b. Router: R1
 - i. Best practice security management
 - ii. EIGRP Routing Protocols
 - iii. IPSec Tunneling
 - iv. FHRP: HSRP
 - v. ACLs
 - c. Multilayer Switch: MLS1
 - i. Best practice security management
 - ii. OSPF Routing Protocols
 - iii. IPSec Tunneling
 - iv. FHRP: HSRP
 - v. ACLs
 - vi. VLAN Implementation
 - d. Cisco Switch
 - i. Best practice security management
 - ii. Remote Access
 - iii. VLAN Implementation
 - e. Ubuntu Server
 - i. Remote Access
 - ii. Identity/User management
 - iii. VSFTP
 - iv. Encryption exploitation
 - f. Raspberry Server
 - i. Remote Access
 - ii. Identity/User management
 - iii. HTML web interface
 - iv. Pi-Hole
 - g. PC Kali Linux
 - i. Penetration software & tools
 - ii. Management user privilege

4) Testing:

- a. Network Configuration
 - i. Ensure connectivity
 - Ping
 - Trace Route
 - Show interface details
 - ii. Routing Protocols
 - IP Route
 - Redundancy
 - Routing Priority
 - VLAN security
 - IPSec Tunneling
 - iii. Switching Security
 - VLAN security
 - Port security
- b. Server's Web Interface
 - i. Online access to web interface front
 - ii. Encryption of credential information
- c. Penetration Tools & Software
 - i. Remote connection locally and remotely
 - ii. OpenVAS, John the Ripper
 - iii. Pi-Hole, NMAP, Wireshark
 - iv. HTML and Session Management Exploitation
 - v. Privilege separation exploitation

5) Documentation:

- a. Project Plan
- b. Project Analysis
- c. Project Description
- d. Project Presentation
 - i. Description & Purpose
 - ii. Overview of Physical and Logical Topology
 - Routing Setup
 - Ubuntu Server Setup
 - Raspberry Pi Setup
 - Web interface overview
 - End user devices description
 - iii. Penetration Testing & Exploitation Overview
- e. Project Weekly Journals
- f. Research Reference

6) Time Estimates (In Hours):

Estimated Times:

Research	Design	Installation	Configuration	Testing	Documentation	Total
40	10	20	30	20	50	170

7) Estimated Cost:

Cable Modem, end devices and wiring in this project is already available. End

Devices includes Raspberry Pi, Ubuntu Server, Kali Linux and Windows 10 PC

Modular devices are available with the used Cisco router and Cisco switches that

will be purchased from a friend.

DEVICE	COST
Cisco Router 2811	~\$50
Cisco Multilayer Switch 3560 with PoE	~\$50
Cisco Switch 3560x with PoE	~\$50
TOTAL:	~\$150

CIS: Senior Project

2440:491-001



Project Analysis

Ethelyn Tran

Part II of VII

Project Analysis

The proposed project functioned as given with most of the planned features with minor adjustments. With Spectrum's Ubee Cable Modem, the home router acted as the gateway router to the outside internet. By default, the cable modem was setup to act as the Dynamic Host Configuration Protocol (DHCP) server. Due to the limitation of the home router and with user agreement with the Internet Service Provider (ISP), Spectrum, the DHCP private IP address range were limited by the number of customer-premises equipment (CPE) entry points. The DHCP option was limited to just one set of subnet range. Thus, the topology was unable to obtain the various listed subnets as intended. Instead, subnet ranges such as the Server's subnet with VLAN 30 was changed from 192.168.30.0/24 to 192.168.3.0/24. Network Address Translation (NAT) was performed on the ISP side, so NAT was unable to be configured on the client side and onto the overall router topology as intended, hindering the implementation of ACLs rule for outside and for inside. Network Time Protocol (NTP) service worked as intended as baseline for the topology. IPsec Tunneling was also limited and was unable to be configured due the lack of VPN passthrough support. Diagnosis that was researched recommend contacting ISP for ISP-side configuration. The home router was configured to be Wi-Fi home router as well with an SSID and WPA2-PSK key and encryption for local users.

Cisco Router: R1 was configured with EIGRP 100 routing as the Multilayer Switch MLS1 was configured with OSPF as the main Area 0. With limited DHCP range, the Router's interface fa0/2 that is connected to the home router was changed from 10.0.0.4/30 to 192.168.0.4/30. Similarly, interface fa0/1 of MLS1's logical address was changed from 10.0.0.0/30 to 192.168.0.8/30. Extended ACLs rules were assigned. All three devices supported the VLAN implementation, along with Trunking protocol. S1 Trunking layer 2 EtherChannel

performed with load-balancing with MLS1, utilizing Hot Standby Router Protocol (HSRP). Static IP address were assigned to both Servers to the interfaces

Adding persistence to Kali Live in a USB flash drive not only posed an issue for legacy devices that does not support EUFI boot up but also the issue of system space to accommodate the large sets of apt-get update and apt-get upgrade. When the dpkg available memory for apt-get was filled, a clean install would be required for the Kali Linux system. Due to a few misconfiguration and bugs, repository downloads for applications such as OpenVAS will not trigger the background update. A manual download and apt-get update --fix-missing would be required. Equipped with John the Ripper, a password software cracker, Kali USB can perform penetration testing. OpenVAS by Greenbone, a vulnerability scanner was installed to monitor for any issues on the backend of the network and assess the severity of each issue

Ubu_Srv was set to have a Local group, a Remote group and one admin user to manage the system. This difference permits the admin to assess each logins and timestamp for future diagnosis. An VSFTP server was installed and configured to allow internal access with the localhost IP address, which is 192.168.3.10/24 and external access with the public IP address assigned by the ISP. Home router was configured to set port-forwarding with 192.168.3.10 with port 20-21 for FTP, allowing external users to be directed. Due to issues with Windows 10 OS built-in firewall, command line does not support passive FTP traffic, such as the case when connecting to the FTP server the external public IPv4 address.

Rasp_Srv was set to host the Pi-hole, a DNS "Blackhole" service and the web interface hosting server. Pi-hole was installed and host through lighttpd with a web interface admin for easier accessibility. Apache2 was installed and set to host with port 80 and port 443. Port-forwarding was also applied at the router to redirect Port 80 and 443 traffic to the IP address

192.168.3.20/24. HTML file was created, along with supporting files such .js and .css files and replaced the default index file. Subsequently, basic security authentication was applied to the site before entry. Htpasswd file was created for users' credentials to work in conjunction with Basic Auth functionality

Greenbone OpenVAS was installed, and the web graphical interface was created. Vulnerability scans were performed and assessed towards the severity of each entry. Acting as filter for ads and traffic database, Pi-hole was installed, and the web graphical interface was created as well. Pi-hole can be set to make queries about any sites or any users visiting and generating traffic. The home router was set to relay DNS traffic to the Pi-hole database. Wireshark, a network packet analyzer, came pre-installed and was used to demonstrate the HTML exploit of the basic security authentication methodology. John the Ripper, a password cracking feature, came pre-installed in Kali Linux. As John the Ripper performed brute force attacks to uncover the hash or encryption of a password entry, the process would take hours and would be heavy on the CPU resources. The Kali's root password was temporarily set to "123" to demonstrate the test.

Noting that with the current events of the Covid-19 lockdown, there were minor issues and delays with sporadic internet connection disruption and power outages that caused unforeseen setbacks. However, majority of the functionalities worked as installed and intended; however, most of the device and application come as an open-source services, and open-source services tend to have software bugs. The most time-consuming process was diagnosing the issues through understanding the bugs, researching and testing various methods to see which works with the current device setup.

CIS: Senior Project

2440:491-001

Project Presentation

Ethelyn Tran
Part III of VII

Project Presentation

Gaming LAN Setup
A Secured LAN with Local and Remote Access and Downloads

Computer Information System (CIS): Senior Project
2440:491 – 001

Ethelyn Tran Spring 2020 – 13 April 2020

1

Introduction

Honors Project Sponsor
Dr. J. Nicholas

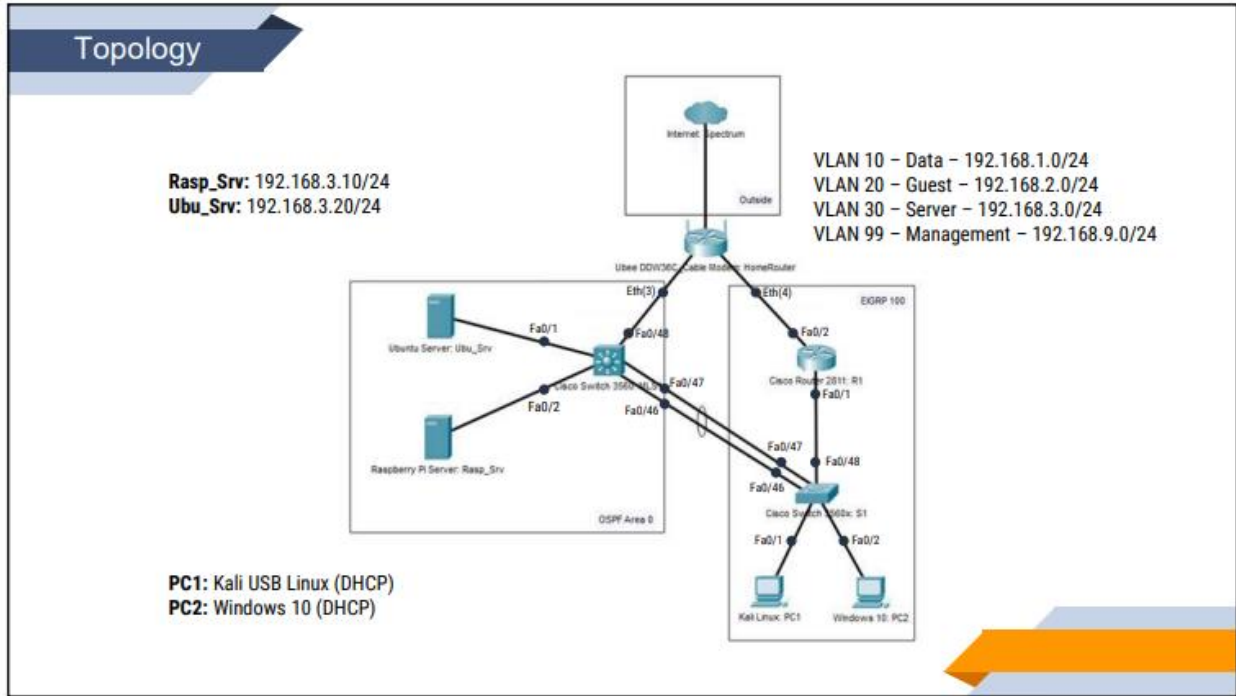
Honors Faculty Advisor
Advisor S. Hoge

Honors Project Reader
Professor M. Haines
Professor S. Smith

Summary:

- Functioning and easy to manage local-area network (LAN)
- Secure web interface to act as a hub
- Secure file transfer to exchange files
- Applications to configure and monitor the overall network
- Tools to assess vulnerabilities

2



3

📌 Layer 3 and Layer 2 Networking

Cisco Equipment	ISP Spectrum
<ul style="list-style-type: none"> > R1 Router: <ul style="list-style-type: none"> - EIGRP Routing Protocol - ACLs > S1 Switch: <ul style="list-style-type: none"> - VLANs Separation - Priority & Redundancy > MLS1 Multilayer Switch: <ul style="list-style-type: none"> - OSPF Routing Protocol - ACLs 	<ul style="list-style-type: none"> > Ubee Cable Modem: <ul style="list-style-type: none"> - DHCP Server - NTP Services - Port-Forwarding Services - WI-FI SSID

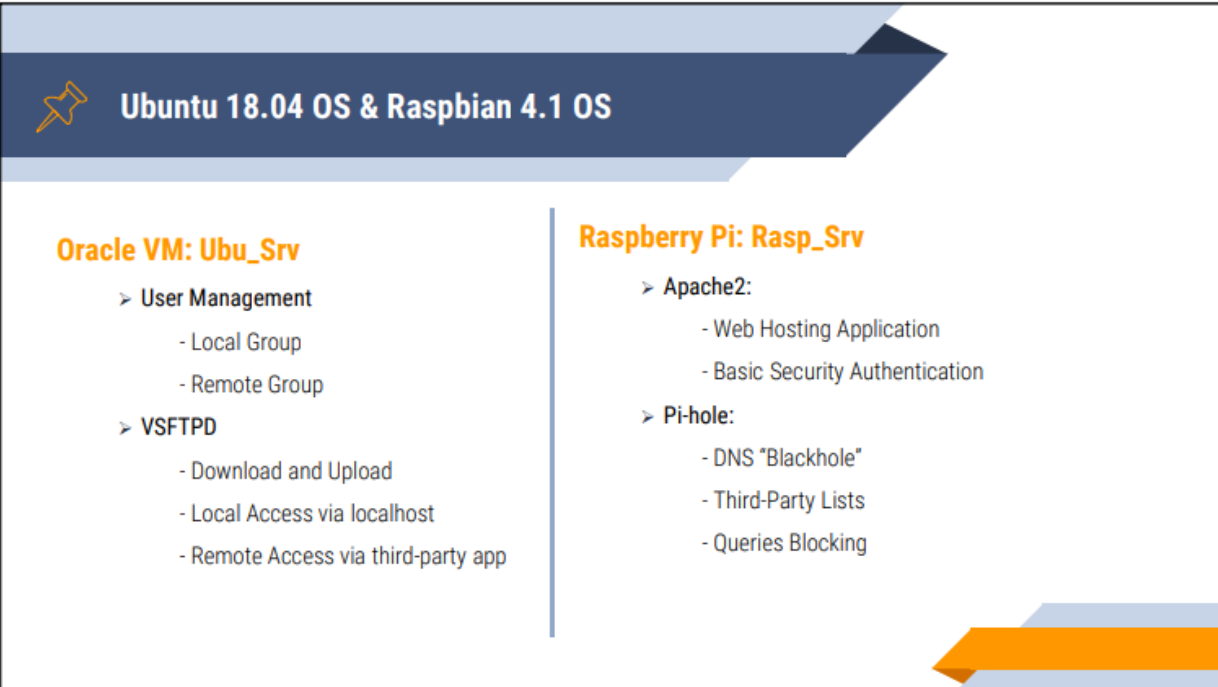
4



Kali Persistence USB + Windows 10

- Kali Persistence USB**
 - Local and Remote User
 - GreenBone Security Manager:
 - OpenVAS
 - Wireshark
 - John the Ripper
- Toshiba - Windows 10 OS**
 - Local User
 - Windows Defender & Firewall
 - Network Management
 - Feature Testing

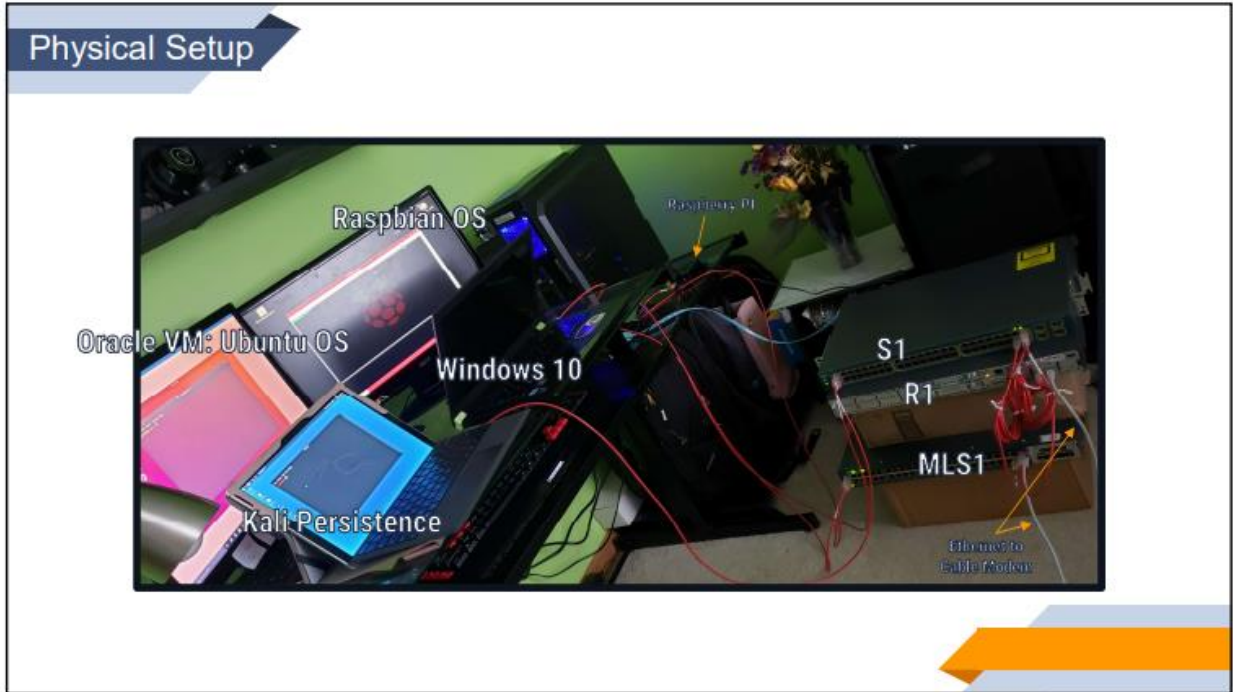
5



Ubuntu 18.04 OS & Raspbian 4.1 OS

- Oracle VM: Ubu_Srv**
 - User Management
 - Local Group
 - Remote Group
 - VSFTPD
 - Download and Upload
 - Local Access via localhost
 - Remote Access via third-party app
- Raspberry Pi: Rasp_Srv**
 - Apache2:
 - Web Hosting Application
 - Basic Security Authentication
 - Pi-hole:
 - DNS "Blackhole"
 - Third-Party Lists
 - Queries Blocking

6



7

Cable Modem Routers Role & Limitations

Setup
DHCP
DHCPv6
LAN IPv6
DNS
Static Lease
Backup
Time

DHCP

DHCP Server Yes No

Starting Address Set

Private Starting Address 192.168.0.2 (2-254) Number of CPEs 0

Public Starting Address 0.0.0.0 (2-254) Number of CPEs 0

Lease Time 86400

Apply

Network Address Translation (NAT)

- Backend Public IP to Private IP
- DHCP Service "CPE" limitation and range

R1 & MLS1

- Limited Routing Capabilities

8

Ubu_Srv – VSFTP Service

User List

- Users permitted to access to VSFTP in vsftpd.userlist_file=/etc/vsftpd.userlist
- Users have individual FTP upload directory

Upload & Download

- Users permitted to read and write through each respective user's directory with Chmod
- Users can read, write, execute while group can read and execute files

Port-Forwarding

- Home router port forwarded external IP address to 192.168.3.10
- Port 20-21 permitted for FTP along with 10000:10100 for other return port

9

VSFTP

FTP with PC2 Windows 10 OS

```

Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.


C:\Users\E>ftp 192.168.3.10
Connected to 192.168.3.10.
228 "Welcome to Project E's FTP service"
200 Always in UTF8 mode.
User (192.168.3.10:(none)): Garen
331 Please specify the password.
Password:
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1001 1004 8980 Apr 07 03:26 examples.desktop
dr-xr-x--- 3 1001 1004 4096 Apr 09 01:24 ftp
226 Directory send OK.
                
```

Windows Command Line Ftp 192.168.3.10

```

ftp> 130 bytes received in 0.01Seconds 21.00kbytes/sec.
ftp> cd ftp
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-x--- 2 1001 1004 4096 Apr 09 21:29 upload
226 Directory send OK.
ftp> 67 bytes received in 0.00Seconds 22.33kbytes/sec.
ftp> cd upload
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1001 1004 59 Apr 09 21:29 CustomGameFile
-rw-r--r-- 1 0 0 59 Apr 09 21:08 TestFile.txt
226 Directory send OK.
ftp> 145 bytes received in 0.01Seconds 26.71kbytes/sec.
ftp>
                
```

10



Rasp_Srv – Web Interface

HTML Front Page

- Web front acts as a hub for local and remote users to visit for information
- Front page is constructed by .html, .js, spam.js, and .css

Basic Security Authentication

- Local and remote users requires authentication prior to entering the website
- Users have individual FTP upload directory

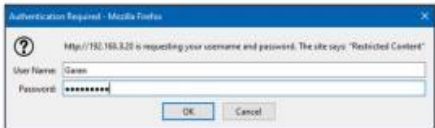
Port-Forwarding

- Home router will redirect External IP Address to 192.168.3.20
- The forwarding reroutes port 80 for HTTP and 443 for HTTPS


11

Web-Front

Local Security Authentication
PC2 Windows 10 OS with
http://192.168.3.20:80





Remote Security Authentication
4G Cellular Network – S9 with
http://PublicIPv4Address:80


12

Vulnerability Scans




OpenVAS

- Acts as vulnerability scanner
- Capable of scanning every node on the network
- Displays vulnerability reports based on severity of class
- Slow to deliver vulnerability reports
- False positive on small severity



Pi-hole

- Acts as a relay Domain Name Server (DNS)
- Routes traffic into database to be queried
- Match against third-party's blocklists
- Device will not automatically choose Pi-hole as the DNS
- Manually update lists



Wireshark


- Acts as a detailed packet analyzer
- Organizes packets by IP, ports, protocols and layered data
- Too noisy

13

Scans

Greenbone Security Manager: OpenVAS

PC1 Kali Persistence USB



Results (125 of 154)

Results by Severity Class (Total: 125)

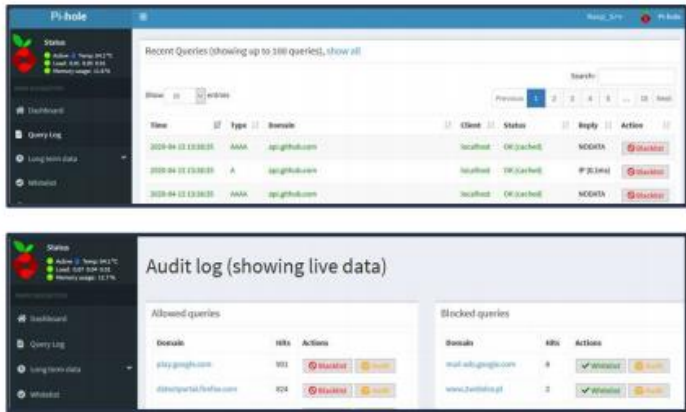
- Medium
- Low
- Long

Vulnerability

Vulnerability	Severity
CPE Inventory	0.0 (Low)
SSL/TLS: Certificate Expired	0.0 (Low)
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites	0.0 (Low)
HTTP Security Headers Detection	0.0 (Low)
SSL/TLS: Report Supported Cipher Suites	0.0 (Low)
SSL/TLS: Report Non-Weak Cipher Suites	0.0 (Low)
SSL/TLS: Certificate - Self-Signed Certificate Detection	0.0 (Low)

Pi-hole: DNS "Blackhole"

Rasp_Srv Raspberry PI



Pi-hole

Recent Queries (showing up to 100 queries, show all)

Time	Type	Domain	Client	Status	Reply	Action
2020-04-02 13:30:35	AAAA	apple-github.com	localhost	OK (cached)	NODATA	🛑 Block
2020-04-02 13:30:35	A	apple-github.com	localhost	OK (cached)	P (2144)	🛑 Block
2020-04-02 13:30:35	AAAA	apple-github.com	localhost	OK (cached)	NODATA	🛑 Block

Audit log (showing live data)

Domain	Hits	Actions
apple-github.com	303	🛑 Block 🗑️ Whitelist
apple-partners.github.com	624	🛑 Block 🗑️ Whitelist

14

Penetration Testing

John the Ripper

- Password cracking open-source software
- Specify format of file, hash of the file, location of the file
- Uses brute force which is heavy on CPU

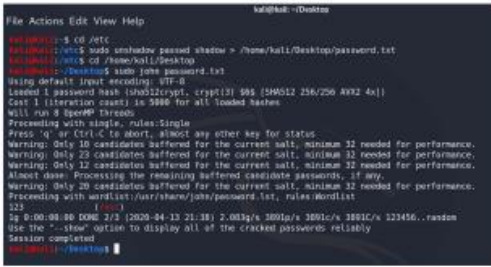
HTML Exploitation

- Basic authentication eliminates cookies, session identifiers and login pages
- Uses HTTP Header that can easily be captured by any packet analyzer such as Nmap and Wireshark
- Basic Auth is encoded in Base64 in transit

15

Pent Testing


John the Ripper: PC1 Kali Persistence USB



```


kali@kali:~/Desktop
File Actions Edit View Help
root@kali:~# cd /etc
root@kali:~/etc# ls
root@kali:~/etc# cd /home/kali/Desktop
root@kali:~/Desktop# pwd
/home/kali/Desktop
root@kali:~/Desktop# ls -la
total 12
-rw-rw-r-- 1 root root 4096 Nov 12 12:12 john_password.txt
root@kali:~/Desktop# cat john_password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $B$1256/256/4932/4x)
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 SpeedTests
Proceeding with single, rules=Single
Press 'q' if Ctrl-C is abort, almost any other key for status:
Warning: Only 10 candidates buffered for the current salt, minimum 32 needed for performance.
Warning: Only 22 candidates buffered for the current salt, minimum 32 needed for performance.
Warning: Only 32 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done. Processing the remaining buffered candidate passwords, if any.
Warning: Only 20 candidates buffered for the current salt, minimum 32 needed for performance.
Proceeding with wordlist (/usr/share/john/password.lst), rules=wordlist
22
ig 0:00:00.00 DOM 2/3 (2020-04-13 21:18) 2.083g/s 3891p/s 3891c/s 3891C/A 123456..random
Use the --show option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
    
```

HTML Exploitation with Wireshark PC1 Kali Persistence USB



```

TCP 192.168.1.100 -> 192.168.1.1 [ACK] Seq=65535 Win=65535 Len=0
TCP 192.168.1.1 -> 192.168.1.100 [ACK] Seq=65535 Win=65535 Len=0
TCP 192.168.1.100 -> 192.168.1.1 [ACK] Seq=65535 Win=65535 Len=0
HTTP 192.168.1.100 -> 192.168.1.1 [POST] Content-Length: 100
HTTP 192.168.1.1 -> 192.168.1.100 [200 OK]
    
```



```

Authorization: Basic Qm9keSjDm45Tm93Z3V1MTZl | base64 -d
Garen:League123
    
```

Authorization is encoded based on Base64

16

References

- Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham: Elsevier Inc.
- Batard, P. (2020, February 29). Create Bootable USB Drives the Easy Way. Retrieved from Rufus: <https://rufus.ie/>
- Canonical Ltd. (2018, April 26th). Download Ubuntu Desktop. Retrieved from Ubuntu: <https://ubuntu.com/download/desktop>
- Cezar, M. (2018, April 20). How to Synchronize Time with NTP in Linux. Retrieved from TecMint: <https://www.tecmint.com/synchronize-time-with-ntp-in-linux/>
- Charles, K. (2020, February 14). Setting up the root account on Kali 2020 . Retrieved from Security Boulevard: <https://securityboulevard.com/2020/02/setting-up-the-root-account-on-kali-2020/>
- dookie. (2017, November 15). Configuring and Tuning OpenVAS in Kali Linux. Retrieved from Kali by Offensive Security: <https://www.kali.org/tutorials/configuring-and-tuning-openvas-in-kali-linux/>
- From, R., & Frahm, E. (2015). *Implementing Cisco IP Switch Networks (SWITCH) Foundation Learning Guide*. Indianapolis: Cisco Press.
- g0tm1k. (2020, February 22). Adding Persistence to a Kali Linux "Live" USB Drive. Retrieved from Kali: <https://www.kali.org/docs/usb/kali-linux-live-usb-persistence/>
- Greenbone Networks GmbH. (2020). *openvas Package Description*. Retrieved from Kali Tools: <https://tools.kali.org/vulnerability-analysis/openvas>
- Hughes, J. (2020, March 12). Setting up an Apache Web Server on a Raspberry Pi. Retrieved from Raspberry Pi: <https://www.raspberrypi.org/documentation/remote-access/web-server/apache.md>
- Infrabot, A. (2019, May 22). PasswordBasicAuth. Retrieved from Confluence Apache: <https://cwiki.apache.org/confluence/display/httpd/PasswordBasicAuth>

17

References

- Linuxize. (2019, March 19). How to Setup FTP Server with VSFTPD on Ubuntu 18.04. Retrieved from Linuxize: <https://linuxize.com/post/how-to-setup-ftp-server-with-vsftpd-on-ubuntu-18-04/>
- Microsoft Corporation. (2017, May 02). Disabling Secure Boot. Retrieved from Microsoft Docs: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/disabling-secure-boot>
- MiniTool. (2020). MiniTool Partition Wizard Free 12. Retrieved from Partition Wizard: <https://www.partitionwizard.com/free-partition-manager.html>
- Offensive Security. (2020, January 28). Kali Linux Downloads. Retrieved from Kali by Offensive Security: <https://www.kali.org/downloads/>
- Oracle Corporation. (2020, February 19). Download VirtualBox. Retrieved from Virtual Box: <https://www.virtualbox.org/wiki/Downloads>
- PI-Hole. (2019, May 18). Pi-hole: Network-wide Ad Blocking. Retrieved from Pi-hole: <https://pi-hole.net/>
- Raspberry Pi Foundation. (2020, February 13). Raspbian. Retrieved from Raspberry Pi: <https://www.raspberrypi.org/downloads/raspbian/>
- Simpson, M., Backman, K., & Corley, J. (2017). *Hands-On Ethical Hacking and Network Defense*. Boston: Cengage Learning.
- Soyinka, W. (2016). *Linux Administration: A Beginner's Guide*. New York: McGraw-Hill Education.
- Teare, D., Vachon, B., & Graziani, R. (2015). *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide*. Indianapolis: Cisco Press.
- W3 Resources. (2020, February 26). User management. Retrieved from W3Resources: <https://www.w3resource.com/linux-system-administration/user-management.php>
- XECDesign. (2020, February 14). NOOBS. Retrieved from Raspberry Pi: <https://www.raspberrypi.org/documentation/installation/noobs.md>

18



CIS: Senior Project
2440:491-001

Project Description

Ethelyn Tran
Part IV of VII

Project Description

Table of Contents

Description – Testing – Weekly Journals

1.	Windows 10 Operating System (OS): PC2	15
1.1.	Windows Update	15
1.2.	Windows 10 Version	16
1.3.	Windows Defender: A Built-In Security Service.....	16
1.4.	Firewall & Network Protection	17
1.5.	Device Name	18
1.6.	Network Connectivity	19
2.	Kali Linux OS: PC1.....	20
2.1.	Kali Linux Install	20
2.2.	USB Drive Format	20
2.3.	Bootable USB Partition.....	21
2.4.	Kali Linux Persistence Boot Up.....	23
2.5.	Kali Linux Root User and System Updates	24
2.6.	Open Vulnerability Assessment Scanner (OpenVAS) Application.....	25
3.	Oracle VM's Ubuntu GUI: Ubu_Srv.....	27
3.1.	Oracle Virtual Machine (VM) Virtual Box Install.....	27
3.2.	Virtual Ubuntu OS Setup	29
3.3.	VM Ubuntu Desktop Install	32
3.4.	Ubuntu Desktop System Update	35
3.5.	Network Configuration	35
3.6.	Users and Groups	37
3.7.	User Home Directory Privileges	39
3.8.	Password Policies	41
4.	Ubu_Srv – Very Secure File Transfer Protocol Daemon (VSFTPD)	42
4.1.	VSFTP Installation.....	42
4.2.	VSFTP Setup and Configuration.....	42
4.3.	VSFTP Users and Directory.....	44

4.4.	VSFTP Sample Files	45
5.	Raspbian OS: Rasp_Srv.....	47
5.1.	Raspbian Operating System (OS) Installation	47
5.2.	System Configuration - Time zone and Root Password	48
5.3.	Network Configuration	49
5.4.	Pi-hole Installation	50
5.5.	Pi-hole Setup	52
6.	Rasp_Srv – Web Hosting	54
6.1.	Apache Server Installation	54
6.2.	Apache HTML Setup	54
6.3.	Basic Access Authentication Implementation.....	60
7.	Layer 2 Cisco Switch: S1	62
7.1.	Device Setup	62
7.2.	VLAN Implementation	63
7.3.	Interface Configuration	64
8.	Layer 3 Multilayer Switch: MLS1.....	66
8.1.	Device Setup	66
8.2.	VLAN Implementation	67
8.3.	Interface Configuration	67
8.4.	Hot Standby Router Protocol (HSRP).....	69
8.5.	Open Shortest Path first (OSPF) Routing Protocol.....	69
8.6.	Access Control Lists (ACLs)	69
9.	Layer 3 Router: R1	71
9.1.	Basic Setup.....	71
9.2.	VLAN Implementation	72
9.3.	Interface Configuration	72
9.4.	Hot Standby Router Protocol (HSRP).....	73
9.5.	Enhanced Interior Gateway Routing Protocol (EIGRP)	73
9.6.	Access Control Lists (ACLs)	74
10.	Spectrum Cable Modem: Ubee DDQ36C / Home Router.....	75
10.1.	Secure Admin Login.....	75

10.2.	Dynamic Host Configuration Protocol (DHCP) Server	76
10.3.	Dynamic Domain Name Server (DDNS) Services.....	76
10.4.	Network Time Protocol (NTP) Services	77
10.5.	Port-Forwarding Services	78
10.6.	Service Set Identifier (SSID) and Password.....	79
1.	Server Functionality with PC2 Windows 10 OS	82
1.1.	Rasp_Srv – Web Server with Security Authentication	82
1.2.	Ubu_Srv – File Transfer Program (FTP) with Security Access.....	83
2.	Vulnerability Management	85
2.1.	OpenVAS Vulnerability Scan	85
2.2.	Pi-hole Management	86
3.	Penetration Testing – PC1: Kali Linux USB.....	88
3.1.	John the Ripper: Password Cracking Software	88
3.2.	HTML Exploitation.....	88
4.	Network Connectivity – Diagnosis.....	91
4.1.	End Users and Equipment Connectivity	91
4.2.	Interface Details	92
4.3.	Routing Protocols.....	92
1.	Weekly Report: February 3rd – February 9th	95
2.	Weekly Report: February 10th – February 16th.....	96
3.	Weekly Report: February 17th – February 23rd	97
4.	Weekly Report: February 24th – March 1st	98
5.	Weekly Report: March 2nd – March 8th.....	99
6.	Weekly Report: March 16th – March 22nd.....	100
7.	Weekly Report: March 23rd – March 29th	101
8.	Weekly Report: March 30th – April 5th.....	102
9.	Weekly Report: April 6th – April 12th.....	103
10.	Estimation of Time	104

Project Description

The project is implemented from end devices to routing equipment in reference to the topology. Each device includes a description of the goal and purpose. When applicable, an entry begins with the hardware information and the installation process. Best security practices, configurations and various functioning programs will be explained according to their respective devices. An understanding of these processes allows the administrator to build and maintain the system.

1. Windows 10 Operating System (OS): PC2

Operating on a Microsoft Surface Pro (5th Gen) laptop, Windows 10 Home 64-bit OS comes pre-installed when device was purchased. Windows OS requires Windows updates to ensure that any known bugs and security vulnerability are patched. Additional local built-in user security will be applied.

1.1. Windows Update

- 1) To navigate to Windows Update, click the Windows “Start” button
- 2) In the search box, type “Windows Update settings” and press Enter to display the Windows Update window
- 3) Click “Check for Updates” to initiate



Figure 1.1 Windows Update

- 4) If Windows requires an update, click “Restart Now” to install and apply the new update. The OS will restart

1.2. Windows 10 Version

- 1) To check for an update on Windows version, click Windows “Start” button
- 2) Type “Windows Update settings” into the search bar.
- 3) On the Windows update window, click “Download and install now” for any feature and security updates



Figure 1.2 Windows Version Update

- 4) Click “Restart now” to apply the newly downloaded updates. The OS will restart.

1.3. Windows Defender: A Built-In Security Service

- 1) Click Windows “Start” button.
- 2) Type and enter “Windows Security” in the search box. Windows Security window will be displayed

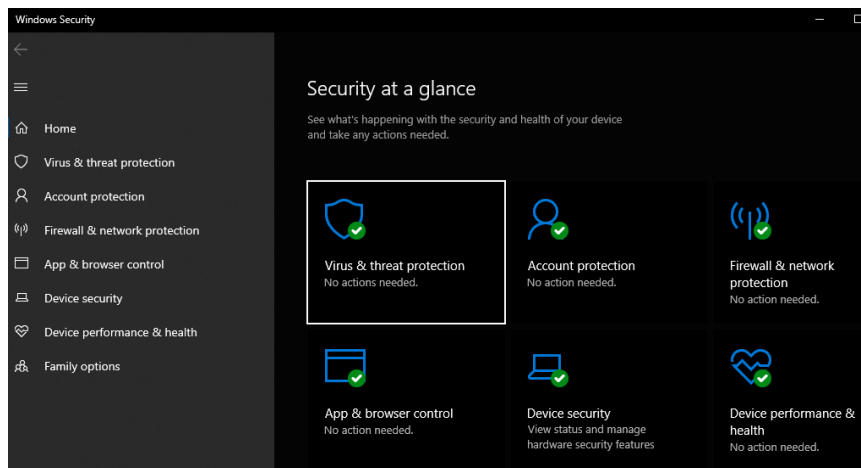


Figure 1.3 Windows Security Display

- 3) Click on “Virus & threat protection”
- 4) If the device does not have any third-party anti-virus software, click on “Manage settings” under the header Virus & threat protection settings



Figure 1.4 Virus & Threat Protection Options

- 5) Switch the button under the header Real-time protection to “On”
- 6) Switch the button under the header Cloud-delivered protection to “On”
- 7) Switch the button under the header Automatic sample submission to “On”
- 8) Switch the button under the header Tamper Protection to “On”
- 9) On the upper left corner, click on the return arrow to navigate back to the previous page
- 10) Under the header Virus & threat protection updates, click “Check for updates”
- 11) Proceed to click on “Check for updates” again when Protection Updates windows is displayed

1.4. Firewall & Network Protection

- 1) On the left navigation pane, select Firewall & network protection
- 2) If header Domain network is not already on, click “Turn on”
- 3) If header Private network is not already on, click “Turn on”
- 4) If header Public network is not already on, click “Turn on”

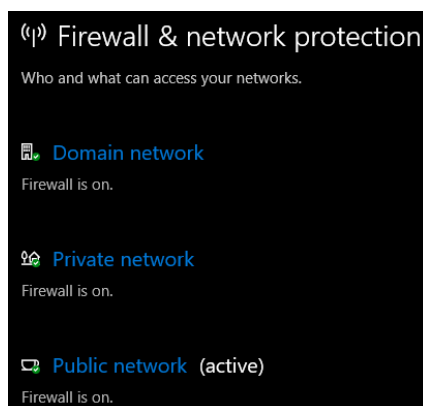


Figure 1.5 Firewall & Network Protection Options

- 5) Click on “Advanced Setting” on the same window.
- 6) Enter Administration password when prompted
- 7) The Windows Defender Firewall with Advanced Security window will launch. On the left navigation tree, click on “Inbound Rules” under Windows Defender Firewall with Advanced Security on Local Computer
- 8) Under the Inbound Rules panel, locate the two entries of “File Transfer Program” and click to launch Properties

* *Note:* Under Firewall, one entry File Transfer Program rule is for UDP and the other is for TCP

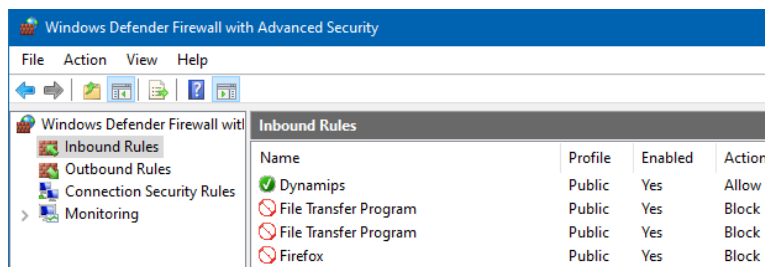


Figure 1.6 File Transfer Program (FTP) in Windows Defender Firewall

- 9) Under the Action header, permit the connection by click on the “Allow the connection button”
- 10) Click Apply to confirm the changes and exit the Properties window
- 11) Repeat for the other “File Transfer Program” entry.
- 12) Exit the Advanced Security window
- 13) Exit the Windows Security window

1.5. Device Name

- 1) Click on the Windows “Start” button
- 2) In the search bar, type in “Device Specification.” Press enter for the Setting window to be displayed.
- 3) Click “Rename this PC”
- 4) Rename the device its to “PC2” in accordance with the topology when prompted

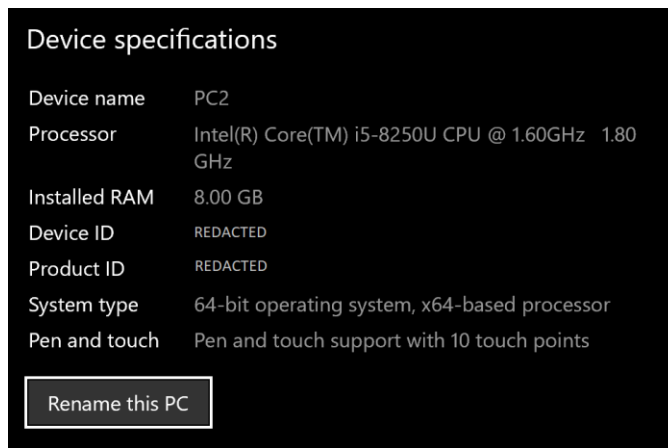


Figure 1.7 Device Specification and Information

- 5) When prompted, click “Restart now” to apply changes

1.6. Network Connectivity

- 1) Click on the Windows “Start” button
- 2) In the search bar, type in “Network Status” to launch the Network Status window
- 3) Click “Change connection properties” under the Network status header
- 4) Under the IP settings, ensure that the IP assignment field is set to “Automatic (DHCP)”



Figure 1.8 IP Assignment: DHCP

2. Kali Linux OS: PC1

Using a SanDisk Cruzer-Fit 16GB flash drive, Kali Linux OS persistence will be added onto the USB drive. Kali OS: PC1 will be acting as end device user with administrator elevated privilege and will perform penetration testing, along with vulnerability scanning. Rufus 3.9 software will be used to create the persistence. The Kali Live USB drive is formatted as FAT32, making the drive a UEFI-only booting USB live media. If not already available, each application will be installed and updated.

2.1. Kali Linux Install

- 1) On any internet browser, enter “<https://www.kali.org/downloads/>” on the search address bar
- 2) Click on “Kali Linux 64-Bit (Live)” under the “Image Name” column
- 3) When prompted, confirm download. In this case, “kali-linux-2020.1b-live-amd64.iso” is downloaded

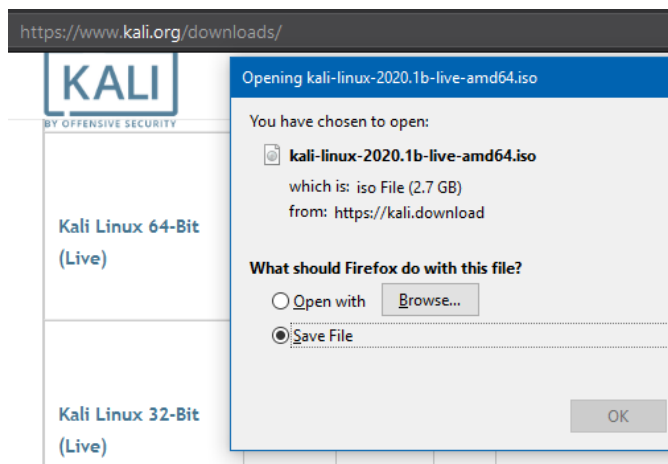


Figure 2.1 Kali Live Linux ISO

2.2. USB Drive Format

- 1) Insert the physical SanDisk Cruzer-Fit 16GB flash drive into the USB port of the PC
- 2) Click the Windows “Start” button
- 3) Type and enter “File Explorer” into the search bar. The default “This PC” file explorer will appear

- 4) Windows automatically mounts the USB drive to a drive letter. Identify the drive letter. In this case, the USB drive is mounted to (E:). Right-clicked on the USB drive (E:)
- 5) Select “Format...” and the “Format USB Drive (E:)” prompt will appear
- 6) Select the File system’s drop menu to FAT32
- 7) Type in “PC1” onto the Volume label bar
- 8) Uncheck the Quick Format option

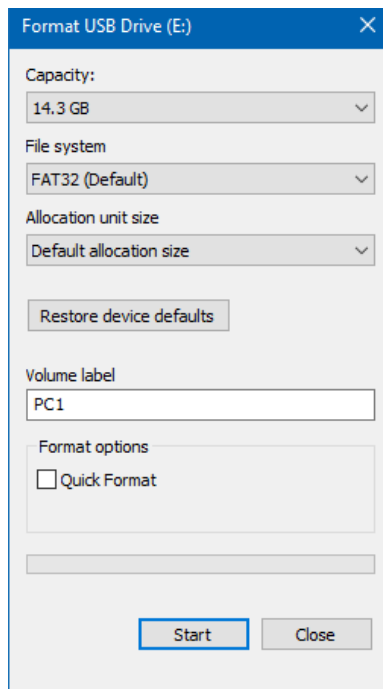


Figure 2.2 PC1 USB Drive Format

- 9) Press Start to begin

2.3. Bootable USB Partition

- 1) On the search address bar of any internet browser, type and navigate to “<https://rufus.ie/>”
- 2) Under the Download header, select on the latest version of Rufus tool
- 3) When prompted, confirm the installation. In this case, “rufus-3.9.exe” is downloaded

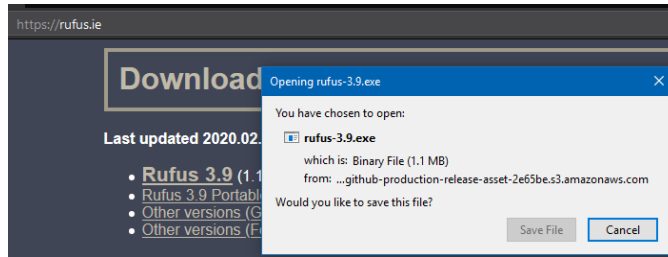


Figure 2.3 Rufus' Download Page

- 4) Navigate to the folder that contains the newly downloaded “rufus-3.9.exe”
- 5) Click on the file to run the executable. The Rufus program window will appear.
- 6) For Device, select “PC1 (E:) [16 GB]”
- 7) For Boot selection, click SELECT. Open windows will appear.
- 8) Navigate to the Kali Linux ISO and select “kali-linux-2020.1b-live-amd64” ISO to open
- 9) Under Persistent partition size, select the slider bar to 8GB or type in “8” in the bar next to the slider
- 10) Under the Volume Label, type in “PC1 Kali”
- 11) Under File system, select “FAT32 (Default)” in the drop-down menu

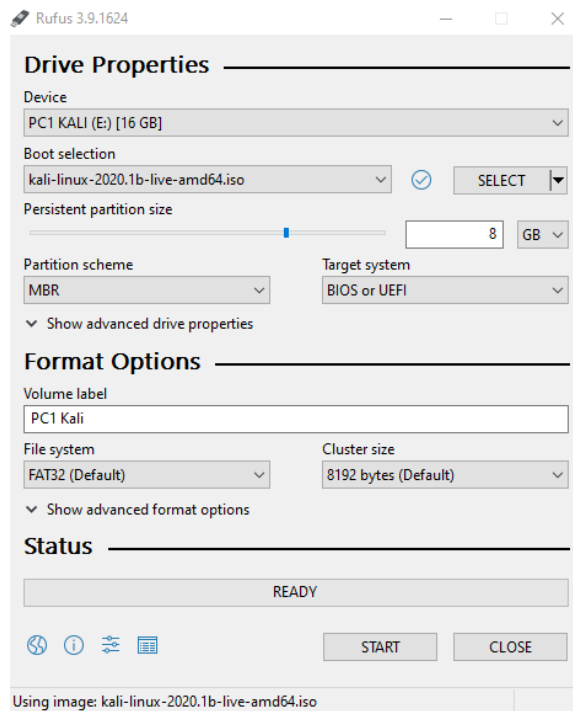


Figure 2.4 Rufus Program Selections

- 12) Click START to begin
- 13) Rufus program prompt a warning to destroy all data on the current device, click OK to proceed
- 14) Upon completion, click Close to conclude the program

2.4. Kali Linux Persistence Boot Up

- 1) Click on Windows “Start” button
- 2) Click on the gear icon, “Settings” and Windows Settings will launch
- 3) Select “Update & Security” to launch Windows Update
- 4) On the left navigation pane, click on “Recovery”
- 5) Under the header Advanced startup, click “Restart now”

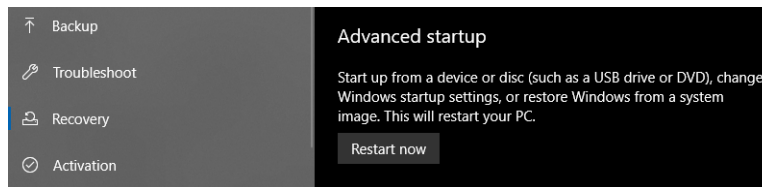


Figure 2.5 Recovery and Advanced Startup Settings

- 6) The host machine will reboot into a setting screen
- 7) Under the Choose an option header, click on “Troubleshoot”
- 8) Under the Troubleshoot header, click on “Advanced Option”
- 9) Under the Advanced option header, click on “UEFI Firmware Settings”
- 10) Click “Restart” to be booted into the UEFI BIOS screen
- 11) With the arrow keys, navigate the top tabs to the boot security. In this case, navigate to the “Boot” tab
- 12) With the arrow keys, navigate to “Secure Boot” and select disable
- 13) Return to the navigation tabs and navigate to the “Exit” tab
- 14) Confirm with “Y” to save and exit the BIOS menu
- 15) The computer will reboot
- 16) Upon bootup, enter the Boot Menu. In this case, enter F12 to enter the menu
- 17) Select the option to boot to the PC1 Kali Live USB drive
- 18) When the Kali Linux Boot Menu appear, navigate down to “Live system (persistence, check kali.org/prst).” Press Enter to boot



Figure 2.6 Kali Linux Boot Menu

2.5. Kali Linux Root User and System Updates

- 1) With Kali Linux GUI, click on the Kali Linux Icon on the upper left corner to display the start menu
- 2) Click or type in "Terminal Emulator"
- 3) Enter the command "sudo su" to enter root user
- 4) Enter the command "passwd root" to set the root user's password
- 5) Enter "2020KaLiRoPa!!" twice to confirm

* *Note:* Administration password is recommended to be at least 14 character in length with a mixture of uppercase and lowercase letter and special characters

* *Note:* The root password is a paraphrase of the year 2020, and the phrase "Kali Live Root Password"

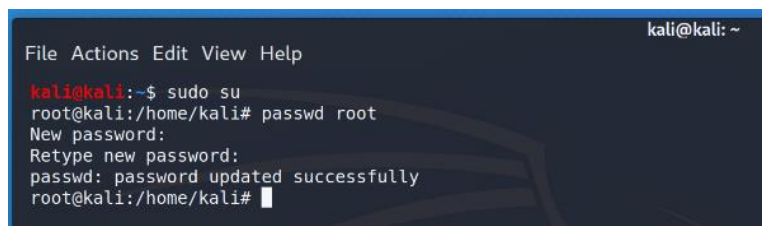


Figure 2.7 Root User and Password

- 6) In order to retrieve the repository to update Kali OS, the system time has to be synchronized. In the terminal, type in “sudo apt-get install ntpdate”
- 7) Enter “Y” to confirm the installation of the Network Time Protocol (NTP)
- 8) Type in “sudo ntpdate in.pool.ntp.org” and press Enter to set NTP server
- 9) Enter the command “sudo apt-get update” to update any listed files
- 10) Enter the command “sudo apt-get upgrade”
- 11) Enter “Y” to confirm the upgrade process

2.6. Open Vulnerability Assessment Scanner (OpenVAS) Application

- 1) With Kali Linux GUI, click on the Kali Linux Icon on the upper left corner to display the start menu
- 2) Click or type in “Terminal Emulator” and press Enter
- 3) In the terminal, type in “sudo apt-get install openvas” to initiate the download of the Greenbone Network’s OpenVAS application
- 4) Enter the root password to continue
- 5) Type “Y” and press enter to confirm
- 6) After the installation, type in “sudo openvas-setup” to initiate setup
- 7) Once the setup is completed, OpenVAS will launch in a web browser
 - * *Note:* If OpenVAS did not launch, open any web browser and type in “127.0.0.1:9392” into the web address bar
- 8) Return to the terminal, copy the password generated for admin user

```
Apr 08 08:35:28 kali systemd[1]: Starting Open Vulnerability Assessment System Manager Daemon...
Apr 08 08:35:28 kali systemd[1]: openvas-manager.service: Can't open PID file /run/openvasmd.pid
Apr 08 08:35:31 kali systemd[1]: Started Open Vulnerability Assessment System Manager Daemon.

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...

[>] Checking for admin user
[*] Creating admin user
User created with password '2c19fad4-58e1-492b-b6cd-921d2061d6a0'.

[+] Done
kali@kali:~$
kali@kali:~$
```

Figure 2.8 OpenVAS Admin Generated Password

- 9) Ensure compatibility between Kali Linux and OpenVAS, create a directory by typing “mkdir /var/lib/openvas/gnupg/”
- 10) In the Greenbone OpenVAS window, enter “admin” for the username
- 11) Enter the generated password, “2c19fad4-58e1-492b-b6cd-921d2061d6a0”

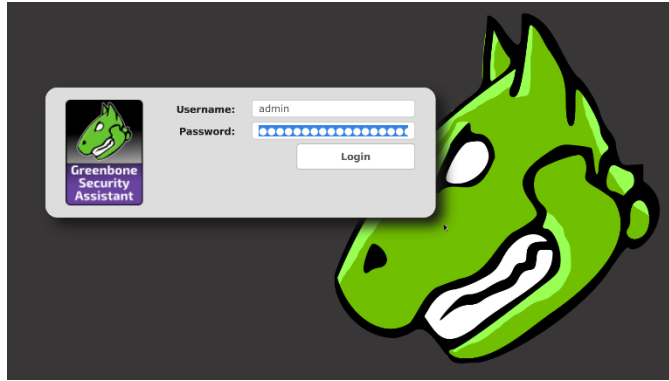


Figure 2.9 Greenbone Security Assistant's OpenVAS Login Screen

- 12) Once logged into the dashboard, hover over “Administration” on the top navigation bar, and click on “Users”
- 13) On the only entry of user, click “Edit User” under the Actions column
- 14) Once the Edit User window launches, click the “New Password” button and enter a new password. In this case, “2020KaLiRoPa!!”

* *Note:* Recommended to have a different password for every admin account

Figure 2.10 OpenVAS's New Admin Password

- 15) Logout of OpenVAS and close the web browser
 - 16) Return to the terminal, type in “sudo greenbone-certdata-sync” and press enter to sync Comprehensive Error Rate Testing (CERT) database into OpenVAS
 - 17) Type in “sudo greenbone-scapedata-sync” and press enter to update and sync Security Content Automation Protocol (SCAP) data
 - 18) To stop OpenVAS running in the background, type in “Sudo openvas-stop”
 - 19) To start OpenVAS, type in “sudo openvas-start”
-

3. Oracle VM's Ubuntu GUI: Ubu_Srv

Using the Oracle VM VirtualBox, the Unix distribution of Ubuntu Desktop 18.04 LTS will be installed. With the Ubuntu Desktop distribution, a user graphical interface (GUI) will be available for use. Each entry begins with the installation process of the respective application, followed by recommended system configurations. Running in a virtual environment, the bridged adapter setting simulates the Ubuntu Desktop as a physical network connection. As Ubuntu Desktop will act as VSFTP server, a static IP address will be assigned. Network connectivity and logical setup are required prior to VSFTP application install. Within the newly installed Ubuntu VM, users will be created, and recommended security practices will be applied.

3.1. Oracle Virtual Machine (VM) Virtual Box Install

- 1) On any internet browser, navigate to “<https://www.virtualbox.org/>” on the web address search bar
- 2) Click “Download VirtualBox 6.4” right on the front page
- 3) Under the header VirtualBox 6.1.4 platform packages, click “Windows hosts” to initiate installation

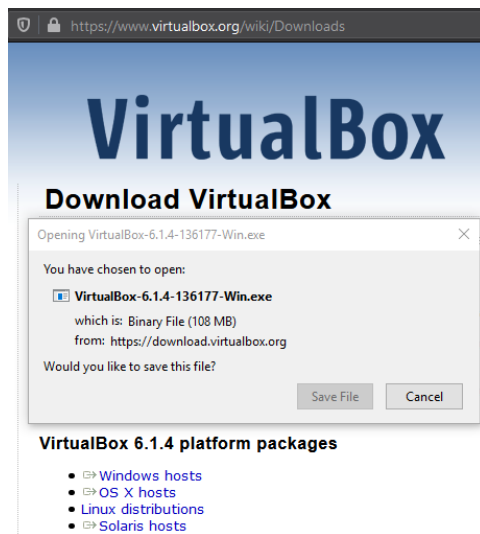


Figure 3.1 Oracle's VirtualBox Download Page

- 4) In this case, “VirtualBox-6.1.4-136177-Win” executable is downloaded
- 5) Within the same web page and under the header VirtualBox 6.1.4 Oracle VM VirtualBox Extension Pack, click on “All supported platforms” to install the extension pack

- 6) In this case, “Oracle_VM_VirtualBox_Extension_Pack-6.1.4.vbox-extpack” is downloaded
- 7) Navigate to the folder that contains the “VirtualBox-6.1.4-136177-Win.exe”
Click to begin the installation.
- 8) Once the Setup Wizard prompt appear, click to Next to continue
- 9) By default, all the features are set to install. Click Next on the Custom Setup section twice

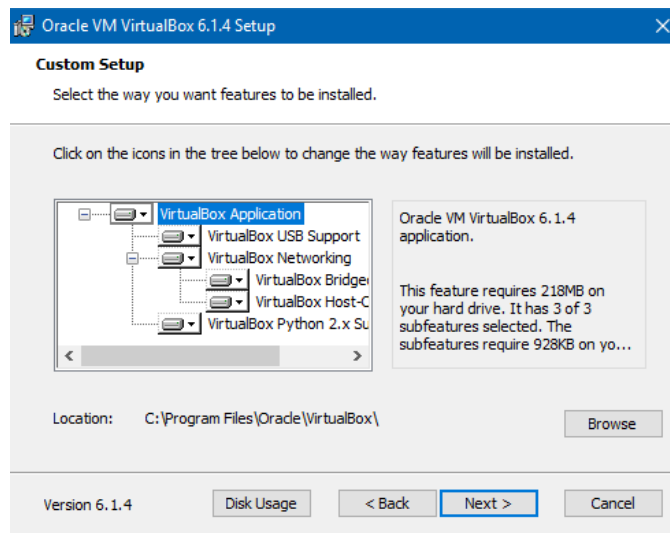


Figure 3.2 Features selected to be installed by default on Custom Setup

- 10) On the warning prompt that the network connection will be reset, click Yes to confirm
- 11) Click Install to begin the installation
- 12) Set Oracle VM VirtualBox 6.1.4 to start after installation. Click Finish when installation completes
- 13) Locate the “Oracle_VM_VirtualBox_Extension_Pack-6.1.4.vbox-extpack” file. Click open to begin the install of the extension pack
- 14) A VirtualBox – Question prompt will appear. Confirm the installation of the extension pack by clicking Install
- 15) Read and click I Agree to the VirtualBox License
- 16) Once the extension pack is installed, click OK.
- 17) Exit the program

3.2. Virtual Ubuntu OS Setup

- 1) On any internet browser, insert “https://ubuntu.com/download/desktop” into the web address search bar and press enter
- 2) Next to Ubuntu 18.04.4 LTS, click the Download button
- 3) When prompted, save the file to desired location

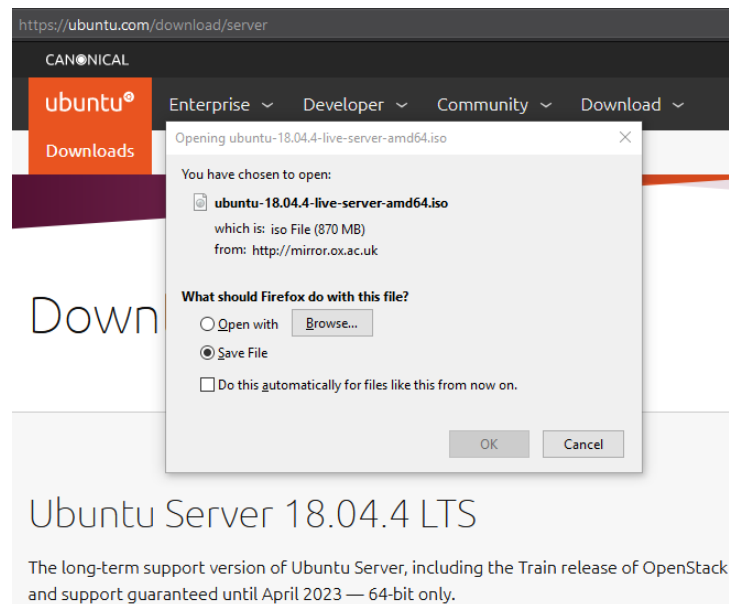
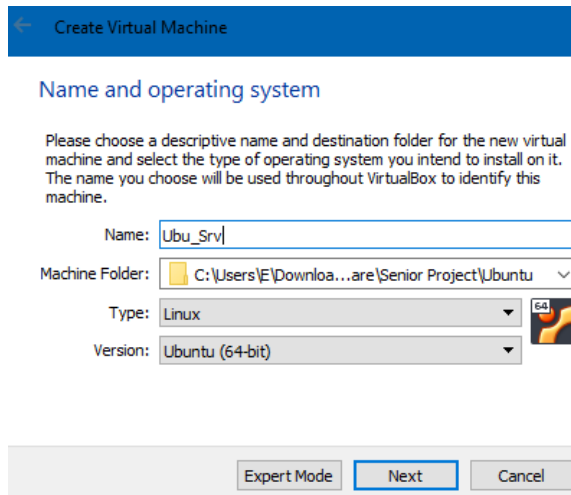


Figure 3.3 Canonical's Ubuntu Desktop Download Page

- 4) In this case, "ubuntu-18.04.4-desktop-amd64" ISO is downloaded
- 5) To open Oracle VM VirtualBox, click Windows "Start" button
- 6) In the search box, type in "Oracle VM VirtualBox" and press enter to launch the program
- 7) Click "New" on the top navigation bar. The Name and operating system will launch
- 8) For the Name field, enter "Ubu_Srv" according to the topology
- 9) For the Machine Folder field, select the desired location to save the operating system
- 10) For the Type field, select "Linux" in the drop-down menu
- 11) For the Version field, select "Ubuntu (64-bit)" in the drop-down menu



The screenshot shows the 'Create Virtual Machine' wizard in Oracle VM VirtualBox Manager. The title bar reads 'Create Virtual Machine'. The main heading is 'Name and operating system'. Below this, there is a paragraph of instructions: 'Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.' The form contains the following fields: 'Name' with the text 'Ubu_Srv', 'Machine Folder' with a folder icon and the path 'C:\Users\E\Downlo...are\Senior Project\Ubuntu', 'Type' with a dropdown menu set to 'Linux' and a small Linux logo icon, and 'Version' with a dropdown menu set to 'Ubuntu (64-bit)'. At the bottom of the form are three buttons: 'Expert Mode', 'Next' (which is highlighted with a blue border), and 'Cancel'.

Figure 3.4 Operating System Identification

- 12) Click Next to proceed to the Memory size section
- 13) Enter “4096” for MB field. Click Next
- 14) At the Hard disk section, select the “Create a virtual hard disk now” button.
Click Create to confirm
- 15) At the Hard disk file type window, select the “VDI (VirtualBox Disk Image)” button. Click Next to proceed
- 16) At the Storage on physical hard disk section, select the “Fixed size” button.
Click Next to continue
- 17) At the File location and size section, enter “20.00” within the GB field. Click Create to proceed
- 18) Once the program returns to the main Oracle VM VirtualBox Manager, select “Ubu_Srv” to highlight the program
- 19) Click “Settings” on the top navigation bar. The Ubu_Srv – Settings window will launch
- 20) Click “System” on the left navigation pane
- 21) Click on the Processor tab
- 22) Change the “Processor(s)” into “4”

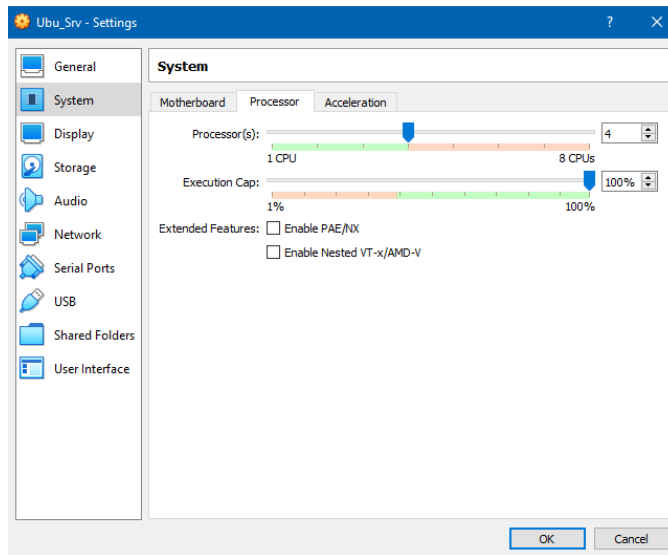


Figure 3.5 Processor System Setting

23) Click “Display” on the left navigation pane

24) Maximized the “Video Memory” to “128MB” under the Screen tab

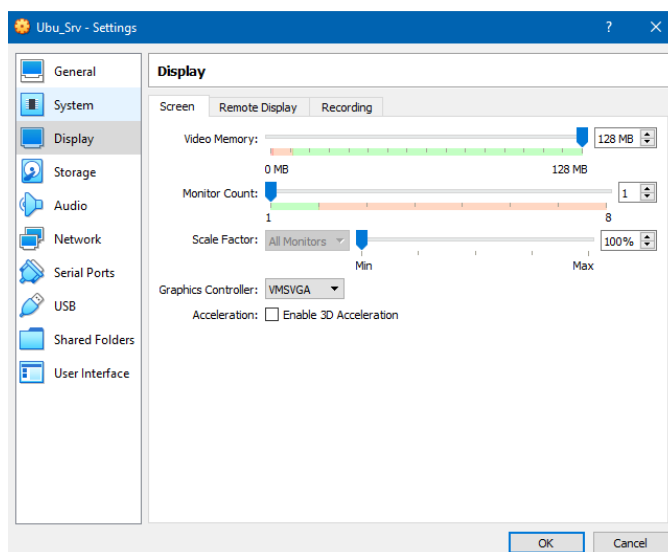


Figure 3.6 Display Screen Setting

25) Click “Network” on the left navigation pane

26) Under the Adapter 1 tab, select “Bridged Adapter” from the Attached to field

27) Collapsed the Advanced field to show additional setting

28) From the drop-down menu of the Adapter Type field, change the setting to “Allow All”

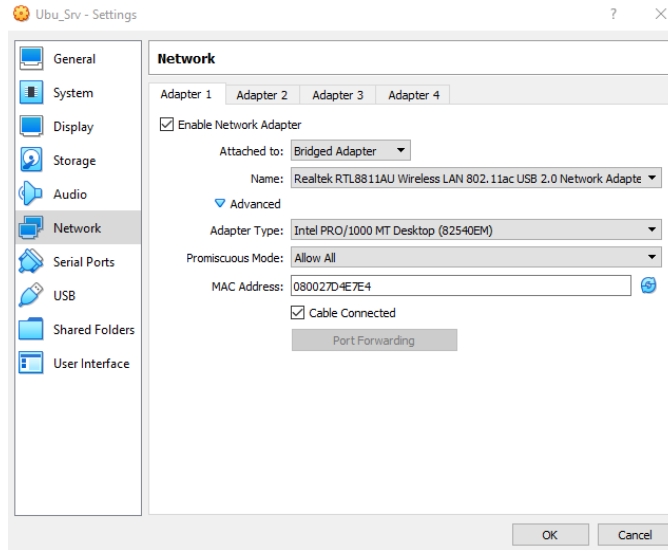


Figure 3.7 Adapter 1 Network Setting

29) Click OK to conclude the Settings

3.3. VM Ubuntu Desktop Install

- 1) With Ubu_Srv highlighted on Oracle VM VirtualBox Manager, click “Start” on the top navigation bar to launch
- 2) At the Select start-up disk window, navigate to where the “ubuntu-18.04.4-desktop-amd64” ISO

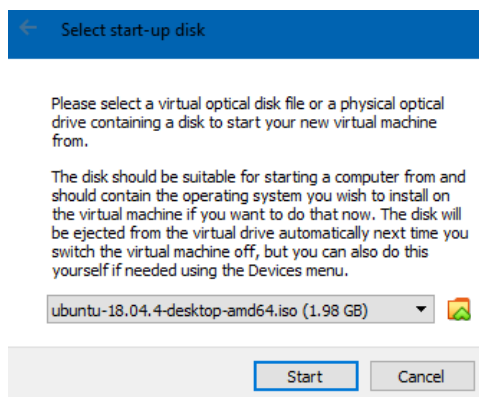


Figure 3.8 Ubuntu ISO Selected

- 3) Click Start to begin
- 4) At the install window, select “English” on the left pane and click “Install Ubuntu” on the right pane



Figure 3.9 Initial Install Window of Ubuntu Desktop

- 5) At the Keyboard layout section, select “English (US)” at the left and the right list
- 6) Click Continue to proceed to the Updates and other software section
- 7) Select the “Normal installation” button
- 8) Check both “Download updates while installing Ubuntu” and “Install third-party software for graphics and Wi-Fi hardware and additional media formats” checkboxes

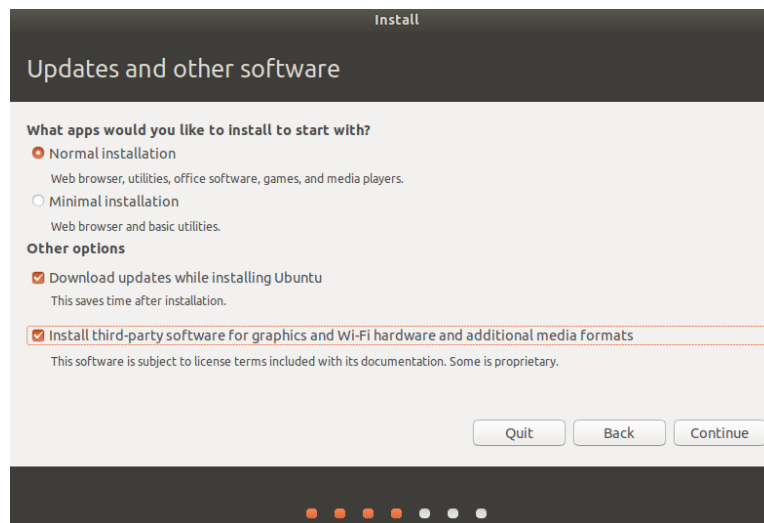
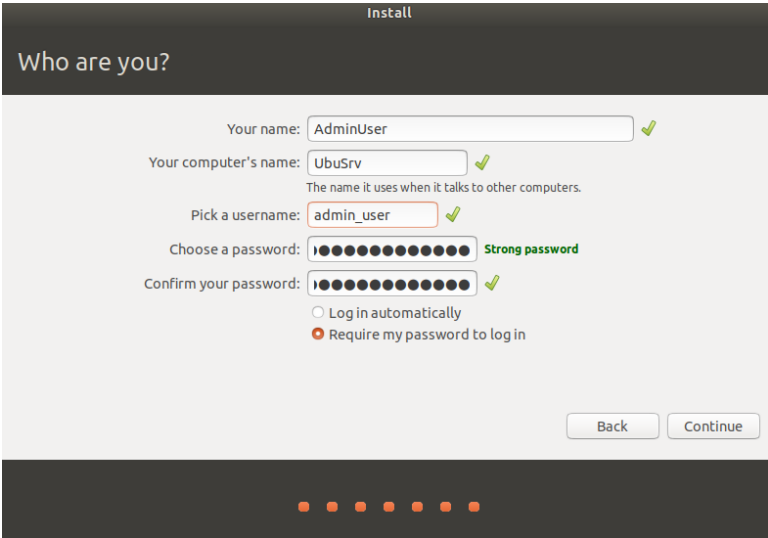


Figure 3.10 Initial Updates and Other Software Option

- 9) Click Continue to go to the Installation type section
- 10) Select the “Erase disk and install Ubuntu” option

- 11) Click Install Now and click Continue at the prompt to confirm selections
- 12) Type “New York” to select Eastern Daylight Time (GMT-4) for the system time
- 13) Click Continue to proceed to user
- 14) Enter “AdminUser” for Your name field
- 15) Enter “UbuSrv” for Your computer’s name field
 - * *Note:* Ubuntu Desktop does not permit special character
- 16) Enter “admin_user” for Pick a username field
- 17) Enter “20ThIsThAdPa20!” for the Choose a password field and for the Confirm your password field
 - * *Note:* Administration password is recommended to be at least 14 character in length with a mixture of Uppercase and lowercase letter and special characters
 - * *Note:* The admin password is a paraphrase of the year 2020, and the phrase “This Is The Admin Password”
- 18) Select “Require my password to log in” button



The screenshot shows the 'Who are you?' screen during Ubuntu installation. The title bar says 'Install'. The main heading is 'Who are you?'. There are five input fields, each with a green checkmark to its right: 'Your name: AdminUser', 'Your computer's name: UbuSrv', 'Pick a username: admin_user', 'Choose a password: [masked] Strong password', and 'Confirm your password: [masked]'. Below the password fields are two radio buttons: 'Log in automatically' (unselected) and 'Require my password to log in' (selected). At the bottom right are 'Back' and 'Continue' buttons. At the very bottom, there is a progress indicator consisting of five orange dots.

Figure 3.11 First User and Device Information

- 19) Click Continue to finish
- 20) After the installation is completed, click Restart Now to complete the process

3.4. Ubuntu Desktop System Update

- 1) When Ubuntu Desktop have boot up completely, click on “Show Application” icon on the left navigation panel
- 2) Type “Terminal” the search bar. Click Enter to launch the terminal application
- 3) Enter “sudo apt-get update” into the command line
- 4) Enter admin_user’s password to confirm the command
- 5) Enter “sudo apt-get upgrade” into the command line
- 6) Enter “Y” to continue the process

```

admin_user@UbuSrv: ~
File Edit View Search Terminal Help
Get:30 http://us.archive.ubuntu.com/ubuntu bionic-backports/universe ar
Fetched 6,726 kB in 2s (2,749 kB/s)
Reading package lists... Done
admin_user@UbuSrv:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer req
 libwayland-egl1-mesa
Use 'sudo apt autoremove' to remove it.
The following packages have been kept back:
 fwupd fwupdate fwupdate-signed linux-generic-hwe-18.04 linux-headers
The following packages will be upgraded:
 apport apport-gtk bluez bluez-cups bluez-obexd bsutils cpp-7 dmidecc
 gir1.2-ibus-1.0 gir1.2-javascriptcoregtk-4.0 gir1.2-nm-1.0 gir1.2-wel
 libasound2 libasound2-data libblkid1 libbluetooth3 libcc1-0 libdrm-ar
 libdrm-nouveau2 libdrm-radeon1 libdrm2 libegl-mesa0 libegl1-mesa libe
 libgcc1 libgd3 libgl1-mesa-dri libgl1-mesa-glx libglapi-mesa libglb2
 libglx-mesa0 libgomp1 libibus-1.0-5 libicu60 libjavascriptcoregtk-4.0
 libnss-systemd libpam-systemd libsgutils2-2 libsmartcols1 libsqlite3
 libwayland-client0 libwayland-cursor0 libwayland-egl1 libwayland-egl
 libxatracker2 libxml2 linux-base linux-firmware mount network-manage
 python3-apport python3-pill python3-problem-report python3-renderpm py
 rsync systemd systemd-sysv unattended-upgrades util-linux uuid-runti
 xserver-xephyr xwayland xxd
96 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
Need to get 0 B/209 MB of archives.
After this operation, 6,204 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y

```

Figure 3.12 Apt-Get Upgrade Command

3.5. Network Configuration

- 1) In the Terminal, type in “Sudo apt install net-tools,” allowing the use of “ifconfig...” commands
- 2) Type in the command “ifconfig -a” to view the ethernet connections. Confirm that ethernet connection is “enp0s3”

```

admin_user@UbuSrv: ~
File Edit View Search Terminal Help
admin_user@UbuSrv:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.17 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::ec57:d015:76eb:dbaa prefixlen 64 scopeid 0x20<link>
    inet6 2607:fcc8:9b04:4c00:d882:844a:aeca:25f0 prefixlen 64 scopeid 0x0<global>
    inet6 2607:fcc8:9b04:4c00::6 prefixlen 128 scopeid 0x0<global>
    inet6 2607:fcc8:9b04:4c00:c4bf:4e6c:c:8b18 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:d4:e7:e4 txqueuelen 1000 (Ethernet)
    RX packets 14282 bytes 18961445 (18.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4769 bytes 500999 (500.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 668 bytes 52525 (52.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 668 bytes 52525 (52.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

admin_user@UbuSrv:~$

```

Figure 3.13 Network Information with Ifconfig

- 3) Shut down the ethernet connection with “sudo ifconfig enp0s3 down”
- 4) Enter admin’s password when prompted
- 5) Navigate to the network directory with “cd /etc/network”
- 6) Back up the “interfaces” file by entering “sudo cp interfaces interfaces.backup”
- 7) As “interfaces” file is a read-only file, enter “sudo chmod 740 interfaces” to allow admin to read and write into the file
- 8) Enter “sudo gedit interfaces” to launch the built-in text editor, Gedit
- 9) Navigate to the bottom of the last text line, add an empty line with Enter
- 10) Add the comment “# The primary network interface”
- 11) In the next line, add “auto enp0s3”
- 12) In the next line, type in “iface enp0s3 inet static”
- 13) In the next line, type in “address 192.168.30.10”
- 14) In the next line, type in “netmask 255.255.255.0”

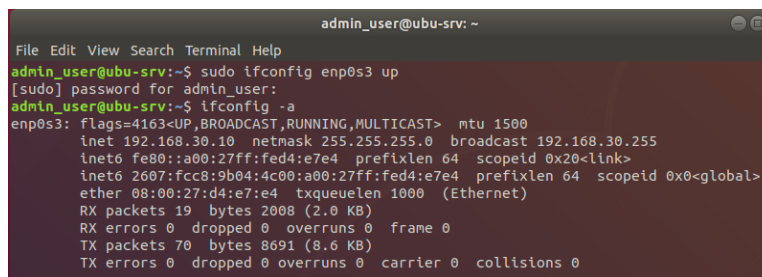
```

Open  interfaces  Save  /etc/network
1 # interfaces(5) file used by ifup(8) and ifdown(8)
2 auto lo
3 iface lo inet loopback
4
5 # The primary network interfaces
6 auto enp0s3
7 iface enp0s3 inet static
8 address 192.168.30.10
9 netmask 255.255.255.0
10

```

Figure 3.14 Interfaces File Configuration

- 15) Click Save before exiting the text editor and returning to the terminal
- 16) Reboot the Ubuntu Desktop in order for changes to take effect. Type in the terminal, “sudo reboot”
- 17) After the reboot, click on “Show Application” icon on the left navigation panel
- 18) Type “Terminal” the search bar. Click Enter to launch the terminal application
- 19) Enter “sudo ifconfig enp0s3 up” into the command line
- 20) Enter admin’s password when prompted
- 21) Type in “ifconfig -a” into the terminal to confirm changes



```

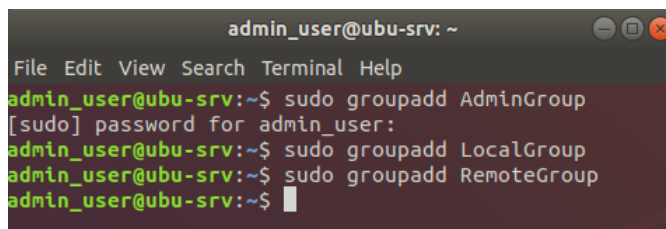
admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo ifconfig enp0s3 up
[sudo] password for admin_user:
admin_user@ubu-srv:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.30.10 netmask 255.255.255.0 broadcast 192.168.30.255
inet6 fe80::a00:27ff:fed4:e7e4 prefixlen 64 scopeid 0x20<link>
inet6 2607:fcc8:9b04:4c00:a00:27ff:fed4:e7e4 prefixlen 64 scopeid 0x0<global>
ether 08:00:27:d4:e7:e4 txqueuelen 1000 (Ethernet)
RX packets 19 bytes 2008 (2.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 70 bytes 8691 (8.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 3.15 Static IP Address Configuration

3.6. Users and Groups

- 1) In the terminal, type “sudo groupadd *groupname*.” Press Enter
 - * *Note:* The group name serves as title to which group a user belongs.
- 2) Enter admin’s password when prompted
- 3) Enter the following each individual line:
 - a. “sudo groupadd LocalGroup”
 - b. “sudo groupadd RemoteGroup”
 - c. “sudo groupadd AdminGroup”



```

admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo groupadd AdminGroup
[sudo] password for admin_user:
admin_user@ubu-srv:~$ sudo groupadd LocalGroup
admin_user@ubu-srv:~$ sudo groupadd RemoteGroup
admin_user@ubu-srv:~$ █

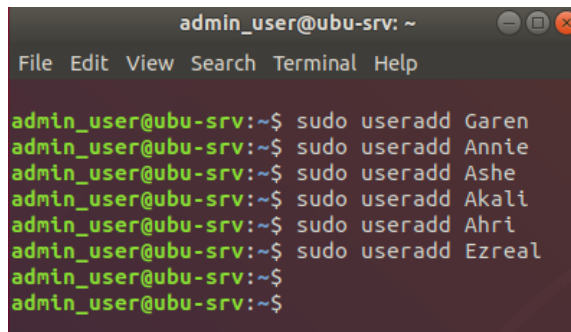
```

Figure 3.16 Groupadd Command

- 4) In the terminal, type “sudo useradd *username*.” Press Enter
- 5) Enter admin’s password when prompted

* *Note:* The username serves as user's name to logins

- 6) Enter the following in each individual line:
 - a. "sudo useradd Garen"
 - b. "sudo useradd Annie"
 - c. "sudo useradd Ashe"
 - d. "sudo useradd Akali"
 - e. "sudo useradd Ahri"
 - f. "sudo useradd Ezreal"



```
admin_user@ubu-srv: ~
File Edit View Search Terminal Help

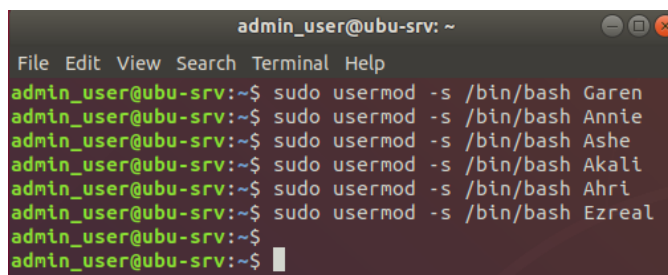
admin_user@ubu-srv:~$ sudo useradd Garen
admin_user@ubu-srv:~$ sudo useradd Annie
admin_user@ubu-srv:~$ sudo useradd Ashe
admin_user@ubu-srv:~$ sudo useradd Akali
admin_user@ubu-srv:~$ sudo useradd Ahri
admin_user@ubu-srv:~$ sudo useradd Ezreal
admin_user@ubu-srv:~$
admin_user@ubu-srv:~$
```

Figure 3.17 Useradd Command

- 7) In the terminal, type "sudo usermod -s /bin/bash *username*." Press Enter

* *Note:* User's login shell is not Bourne Shell by default

- 8) Enter admin's password when prompted
- 9) Enter the following in each individual line:
 - a. "sudo usermod -s /bin/bash Garen"
 - b. "sudo usermod -s /bin/bash Annie"
 - c. "sudo usermod -s /bin/bash Ashe"
 - d. "sudo usermod -s /bin/bash Akali"
 - e. "sudo usermod -s /bin/bash Ahri"
 - f. "sudo usermod -s /bin/bash Ezreal"



```
admin_user@ubu-srv: ~
File Edit View Search Terminal Help

admin_user@ubu-srv:~$ sudo usermod -s /bin/bash Garen
admin_user@ubu-srv:~$ sudo usermod -s /bin/bash Annie
admin_user@ubu-srv:~$ sudo usermod -s /bin/bash Ashe
admin_user@ubu-srv:~$ sudo usermod -s /bin/bash Akali
admin_user@ubu-srv:~$ sudo usermod -s /bin/bash Ahri
admin_user@ubu-srv:~$ sudo usermod -s /bin/bash Ezreal
admin_user@ubu-srv:~$
admin_user@ubu-srv:~$
```

Figure 3.18 Usermod Command

10) In the terminal, type “sudo passwd *username*.” Press Enter

11) Type in the user’s new password. Press Enter

* *Note:* The recommended password length for a user is at least eight (8) characters

```
admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo passwd Garen
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
admin_user@ubu-srv:~$
```

Figure 3.19 Passwd Command

12) The following is the chart of all user added:

Group	User	Password
AdminGroup	admin_user	20ThIsThAdPa20!
LocalGroup	Garen	League123
LocalGroup	Annie	League123
LocalGroup	Ashe	League123
RemoteGroup	Akali	Legend456
RemoteGroup	Ahri	Legend456
RemoteGroup	Ezreal	Legend456

Figure 3.20 User’s Group Chart

13) In the terminal, type “sudo usermod -a -G *groupname username*.” Press Enter.

14) Enter the username into the group according to Figure 3.20

```
admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo usermod -a -G AdminGroup admin_user
admin_user@ubu-srv:~$ sudo usermod -a -G LocalGroup Garen
admin_user@ubu-srv:~$ sudo usermod -a -G LocalGroup Annie
admin_user@ubu-srv:~$ sudo usermod -a -G LocalGroup Ashe
admin_user@ubu-srv:~$ sudo usermod -a -G RemoteGroup Akali
admin_user@ubu-srv:~$ sudo usermod -a -G RemoteGroup Ahri
admin_user@ubu-srv:~$ sudo usermod -a -G RemoteGroup Ezreal
admin_user@ubu-srv:~$
```

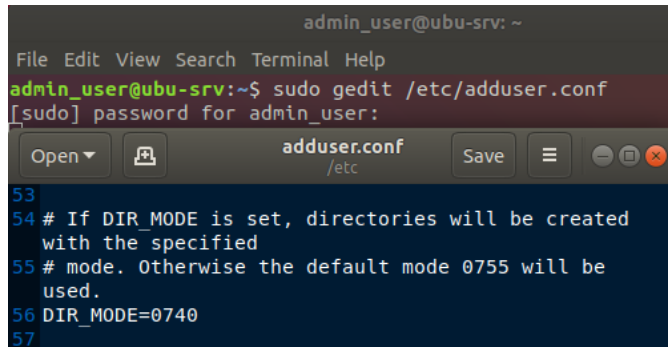
Figure 3.21 Usermod into Groups Command

3.7. User Home Directory Privileges

- 1) In the terminal, type in “sudo gedit /etc/adduser.conf”
- 2) Enter Admin’s password when prompted

- 3) Once the adduser.conf launch in Gedit, navigate down and change the line “DIR_MODE=0770” to “DIR_MODE=0740”

* *Note:* Any subsequent directory will be created with the permission 0740 (drwxr-----)



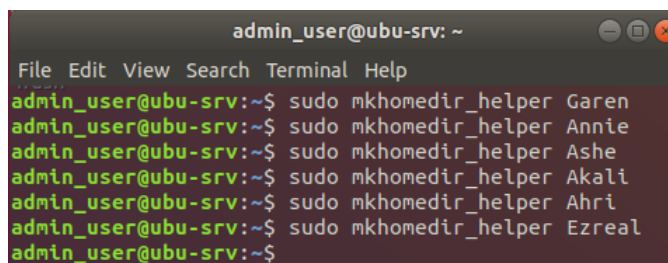
```
admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo gedit /etc/adduser.conf
[sudo] password for admin_user:
Open adduser.conf Save
/etc
53
54 # If DIR_MODE is set, directories will be created
with the specified
55 # mode. Otherwise the default mode 0755 will be
used.
56 DIR_MODE=0740
57
```

Figure 3.22 DIR_MODE Configuration

- 4) Click save and exit adduser.conf
- 5) In the terminal, type “sudo mkhomedir_helper username.” Press Enter.

* *Note:* New users does not have a home directory by default

- 6) Enter the following in each individual line:
 - a. sudo mkhomedir_helper Garen
 - b. sudo mkhomedir_helper Annie
 - c. sudo mkhomedir_helper Ashe
 - d. sudo mkhomedir_helper Akali
 - e. sudo mkhomedir_helper Ahri
 - f. sudo mkhomedir_helper Ezreal



```
admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo mkhomedir_helper Garen
admin_user@ubu-srv:~$ sudo mkhomedir_helper Annie
admin_user@ubu-srv:~$ sudo mkhomedir_helper Ashe
admin_user@ubu-srv:~$ sudo mkhomedir_helper Akali
admin_user@ubu-srv:~$ sudo mkhomedir_helper Ahri
admin_user@ubu-srv:~$ sudo mkhomedir_helper Ezreal
admin_user@ubu-srv:~$
```

Figure 3.23 Mkhomedir_helper Command

- 7) Confirm user’s home directory permissions by typing “ls -ld /home/Garen”

3.8. Password Policies

- 1) In the terminal, type in “cd /etc/pam.d” and type in “ls -a” to view all available file
- 2) Type in “sudo gedit common-password”
- 3) Locate the password line, starting with “password [success=1 default=ignore]. Type in “minlen=8” at the end of the line to enforce password length to be at least 8 characters long

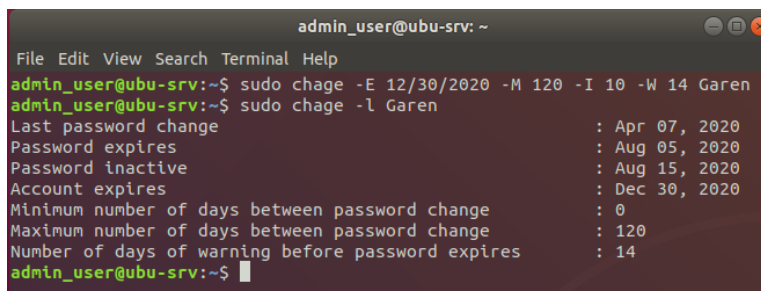
```

23
24 # here are the per-package modules (the "Primary" block)
25 password [success=1 default=ignore] pam_unix.so obscure sha512 minlen=8
26

```

Figure 3.24 Minimum Password Length

- 4) Click save and exit the text editor
- 5) The following is the password requirements:
 - a. -E : 12/30/2020 = Explicit expiration date in MM/DD/YYYY
 - b. -M : 120 = Maximum password age in days
 - c. -I : 10 = Inactivity period before expiration in days
 - d. -W : 14 = Warning time period before password expiration in days
- 6) In the terminal, type in “sudo chage -E 12/30/2020 -M 120 -I 10 -W 14 *username.*” Type in for each user



```

admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo chage -E 12/30/2020 -M 120 -I 10 -W 14 Garen
admin_user@ubu-srv:~$ sudo chage -l Garen
Last password change           : Apr 07, 2020
Password expires                : Aug 05, 2020
Password inactive              : Aug 15, 2020
Account expires                 : Dec 30, 2020
Minimum number of days between password change : 0
Maximum number of days between password change : 120
Number of days of warning before password expires : 14
admin_user@ubu-srv:~$

```

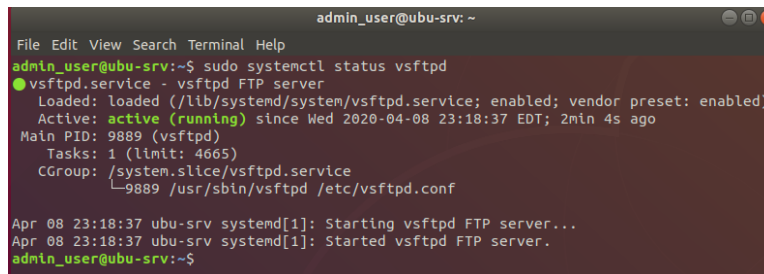
Figure 2.25 Password Policy for Each User

- 7) Confirm changes by typing “sudo chage -l *username*” to view each user information
-

4. Ubu Srv – Very Secure File Transfer Protocol Daemon (VSFTPD)

4.1. VSFTP Installation

- 1) On the Ubuntu Desktop GUI, click on “Show Application” on the lower left corner.
- 2) Type in the search bar, “Terminal” and press Enter to launch the terminal window
- 3) In terminal line, type in “sudo apt install vsftpd” and press enter to execute
- 4) Enter the admin’s password when prompted
- 5) After the installation, type in “sudo systemctl status vsftpd” and press enter to verify the installation

A terminal window titled 'admin_user@ubu-srv: ~' showing the command 'sudo systemctl status vsftpd' and its output. The output indicates that the vsftpd service is active and running. The terminal text is as follows:

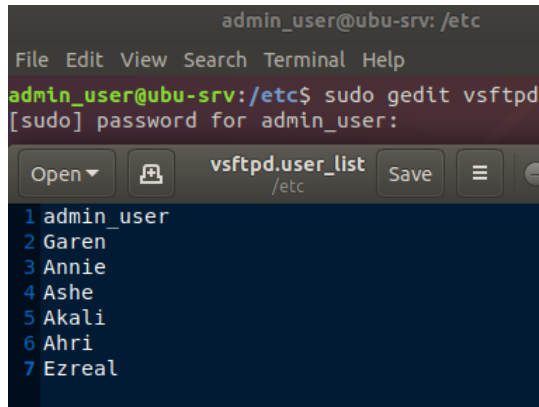
```
admin_user@ubu-srv: ~  
File Edit View Search Terminal Help  
admin_user@ubu-srv:~$ sudo systemctl status vsftpd  
● vsftpd.service - vsftpd FTP server  
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)  
   Active: active (running) since Wed 2020-04-08 23:18:37 EDT; 2min 4s ago  
 Main PID: 9889 (vsftpd)  
    Tasks: 1 (limit: 4665)  
   CGroup: /system.slice/vsftpd.service  
           └─9889 /usr/sbin/vsftpd /etc/vsftpd.conf  
  
Apr 08 23:18:37 ubu-srv systemd[1]: Starting vsftpd FTP server...  
Apr 08 23:18:37 ubu-srv systemd[1]: Started vsftpd FTP server.  
admin_user@ubu-srv:~$
```

Figure 4.1 VSFTPD Status Check

4.2. VSFTP Setup and Configuration

- 1) In the terminal, open the configuration file by entering “sudo gedit /etc/vsftpd.conf”
- 2) Once the text editor window launches, ensure that each line is as following:
 - a. “anonymous_enable=NO”
 - b. “local_enable=YES”
- 3) Locate the comment, “#write_enable=YES” and delete the comment marker “#”, so the setting will be listed as “write_enable=YES”
- 4) In order to allow only certain users to access, type the following at the end of the file:
 - a. “userlist_enable=YES”
 - b. “userlist_file=/etc/vsftpd.user_list”
 - c. “userlist_deny=NO”

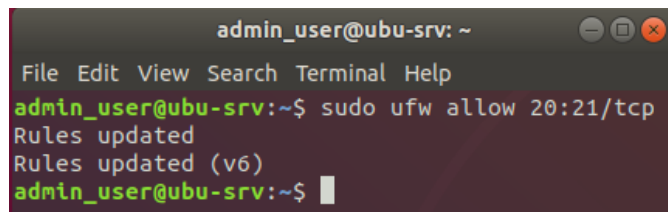
- 5) Save the file in the Gedit text editor and exit
- 6) In the terminal, type “cd /etc/” to navigate to the directory
- 7) To create the user file, enter “sudo gedit vsftpd.user_list”
- 8) Once the text editor launch, enter each user’s name one per line.



```
admin_user@ubu-srv: /etc
File Edit View Search Terminal Help
admin_user@ubu-srv: /etc$ sudo gedit vsftpd.
[sudo] password for admin_user:
Open vsftpd.user_list /etc Save
1 admin_user
2 Garen
3 Annie
4 Ashe
5 Akali
6 Ahri
7 Ezreal
```

Figure 4.2 Vsftpd.user_list File

- 9) Click save and exit the text editor
- 10) In the terminal, restart FTP service by entering “sudo systemctl restart vsftpd”
- 11) Using Ubuntu’s built-in firewall, UncomplicatedFirewall (UFW) will be configured to permit FTP. In the terminal “sudo ufw allow 20:21/tcp”
* Note: FTP command port is 21, and FTP data port is 20



```
admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv: ~$ sudo ufw allow 20:21/tcp
Rules updated
Rules updated (v6)
admin_user@ubu-srv: ~$
```

Figure 4.3 UncomplicatedFirewall (UFW) FTP rule

- 12) After the confirmation, disable the firewall with “sudo ufw disable”
- 13) Restart the firewall service by typing “sudo ufw enable”
- 14) Check the status of the firewall by entering “sudo ufw status

```

admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo ufw disable
Firewall stopped and disabled on system startup
admin_user@ubu-srv:~$ sudo ufw enable
Firewall is active and enabled on system startup
admin_user@ubu-srv:~$ sudo ufw status
Status: active

To Action From
--
20:21/tcp ALLOW Anywhere
20:21/tcp (v6) ALLOW Anywhere (v6)

admin_user@ubu-srv:~$ █

```

Figure 4.4 UncomplicatedFirewall (UFW) Status

4.3. VSFTP Users and Directory

- 1) Users may have an FTP directory tree to upload file and access the file remotely. In the terminal, type “sudo mkdir -p /home/user/ftp/upload”
 - * Note: The *user* is the users that has been created in Ubuntu and permitted to utilized FTP in vsftpd.user_list
- 2) After the directory has been created, set the FTP directory to only be able to Read and Execute, “sudo chmod 550 /home/user/ftp”
 - * Note: chmod 550, permits Owner and Group to Read and Execute listed as r-xr-x---
- 3) To allow user to upload and write file into the Upload folder, enter “sudo chmod 750 /home/user/ftp/upload”
 - * Note: chmod 750, permits the Owner to Read, Write and Execute and the Group to Read and Execute listed as rwxr-x---
- 4) To give ownership to users, type in “sudo chown -R user: /home/user/ftp” and press enter
 - * Note: Each user will have ownership recursively on each respective FTP directory

```

admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo mkdir -p /home/Garen/ftp/upload
[sudo] password for admin_user:
admin_user@ubu-srv:~$ sudo chmod 550 /home/Garen/ftp
admin_user@ubu-srv:~$ sudo chmod 750 /home/Garen/ftp/upload
admin_user@ubu-srv:~$ sudo chown -R Garen: /home/Garen/ftp
admin_user@ubu-srv:~$ █

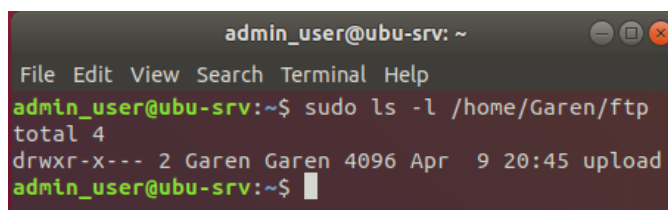
```

Figure 4.5 User's Respective FTP Directory

- 5) To confirm the changes to the file, type “sudo ls -l /home/user/ftp”
- 6) Repeat for each user to have each user’s respective FTP directory

4.4. VSFTP Sample Files

- 1) To begin adding files available to download via FTP as an admin, admin must navigate to the user’s directory. In the terminal, type and enter “sudo su” to enter root user
- 2) Type in “cd /home/user/ftp/uploads” and press Enter to navigate to the directory



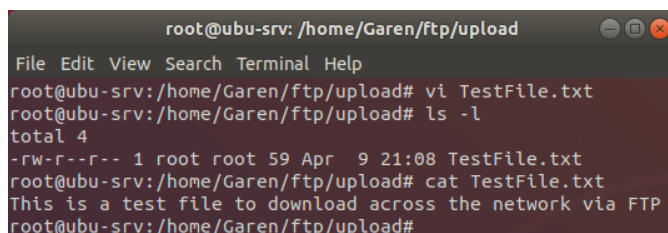
```

admin_user@ubu-srv: ~
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ sudo ls -l /home/Garen/ftp
total 4
drwxr-x-- 2 Garen Garen 4096 Apr  9 20:45 upload
admin_user@ubu-srv:~$

```

Figure 4.6 User’s FTP Upload Directory

- 3) Enter “vi TestFile.txt” to create the file and begin editing
- 4) Once vi launches, press ESC on the keyboard and then the letter “i” to begin typing into the file
- 5) Type a generic description. In this case, type “This is a test file to download across the network via FTP”
- 6) Press ESC and “:wq” to write to the file and exit
- 7) Confirm the existence of the file by typing “ls -l”



```

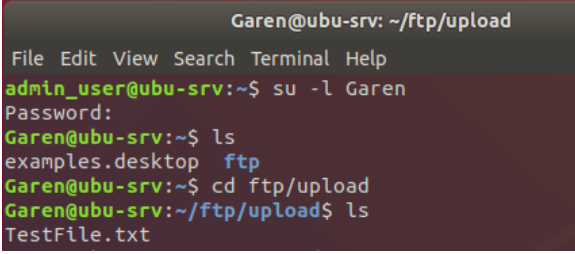
root@ubu-srv: /home/Garen/ftp/upload
File Edit View Search Terminal Help
root@ubu-srv:/home/Garen/ftp/upload# vi TestFile.txt
root@ubu-srv:/home/Garen/ftp/upload# ls -l
total 4
-rw-r--r-- 1 root root 59 Apr  9 21:08 TestFile.txt
root@ubu-srv:/home/Garen/ftp/upload# cat TestFile.txt
This is a test file to download across the network via FTP
root@ubu-srv:/home/Garen/ftp/upload#

```

Figure 4.7 Test File for FTP by Root

- 8) Type “exit” to return from root user to admin_user
- 9) To begin adding files available to download via user, type and enter “su -l user”
- 10) Enter the user’s password to enter user’s login shell

11) To navigate to the uploads folder, type and enter in “cd ftp/uploads”



```
Garen@ubu-srv: ~/ftp/upload
File Edit View Search Terminal Help
admin_user@ubu-srv:~$ su -l Garen
Password:
Garen@ubu-srv:~$ ls
examples.desktop  ftp
Garen@ubu-srv:~$ cd ftp/upload
Garen@ubu-srv:~/ftp/upload$ ls
TestFile.txt
```

Figure 4.8 Test File for FTP by User

12) Type and enter “vi CustomGameFile”

13) Once the vi text editor launches, press “i” to begin typing into the file

14) In this case, type “This is a custom game file that can be downloaded over ftp”

15) Press ESC and “:wq” to write and quit the file

16) Enter “logout” in the terminal to logout of the user’s login shell

5. Raspbian OS: Rasp_Srv

Using a Raspberry Pi 3 Model B+ 32GB, Raspbian v4.19 Operating System, dubbed Raspbian Jessie, is installed using NOOBS v2.7, including recommended system configurations. The Raspberry Pi 3 Model B+ comes with a microSD card that is pre-installed with NOOBS, an operating system installer. Apache Application is installed onto Raspbian OS to be used as a web server application. As the Raspberry Pi will act as web hosting server, a static IP address will be assigned. Network connectivity and logical setup are required prior to Pi-hole application and Apache Server installation.

5.1. Raspbian Operating System (OS) Installation

- 1) After the physical setup, “NOOBS v2.7 – Built: Mar 14 2018” will launch as the first application and window.
- 2) At the bottom of the window, select the language (l) to “English (US)” at the drop-down menu
- 3) Select the keyboard (9) to “us” from the drop-down menu
- 4) Tick the Raspbian (RECOMMENDED) checkbox
- 5) Click “Install (i)” to begin the installation

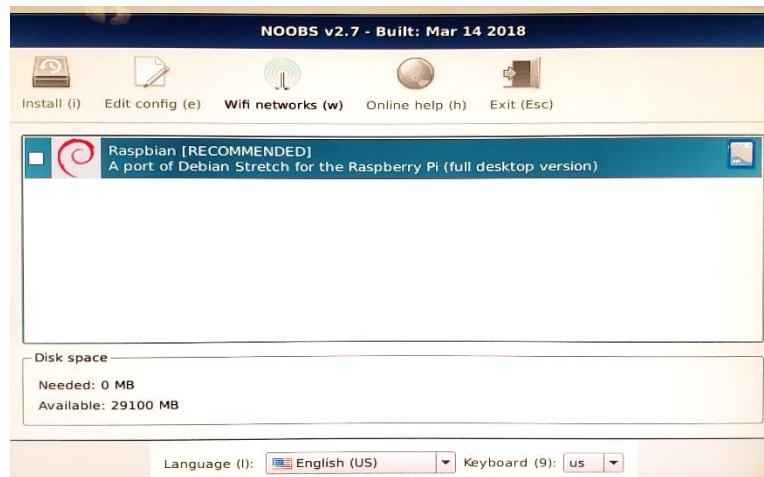


Figure 5.1 NOOBS OS Installer

- 6) On the prompt, click “Yes” to confirm the overwriting of the current drive data and installation
- 7) After the installation process of the OS, a prompt to inform the success of installation will appear. Click “OK” to continue

5.2. System Configuration - Time zone and Root Password

- 1) Once the OS completely bootup, click on the “Application Menu” on the upper left corner the taskbar
- 2) Navigate to “Accessories” to display another menu next to it
- 3) Click on “Terminal” to launch the terminal window for Raspbian
- 4) In the terminal, type “sudo raspi-config” to launch the Raspberry Pi Software Configuration Tool (raspi-config) window
- 5) Navigate down to option “4 Localisation Options” and press Enter

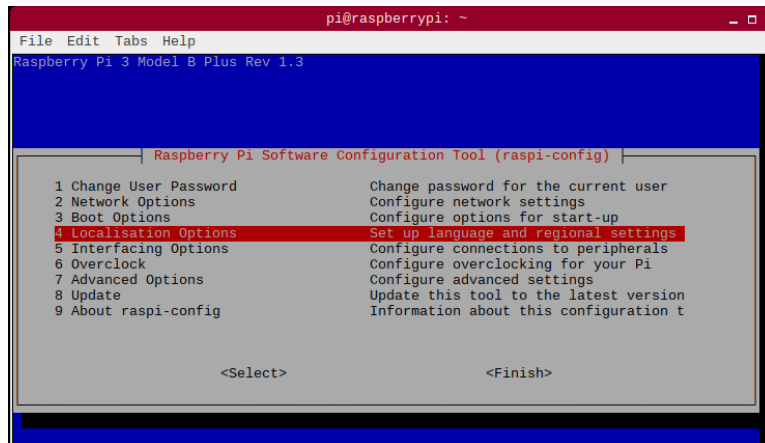
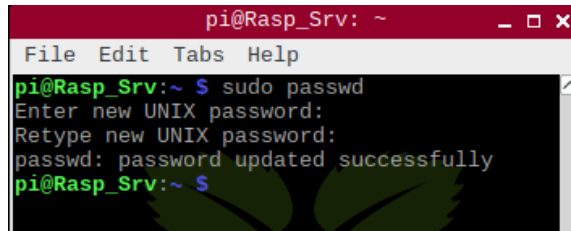


Figure 5.2 Raspberry Pi Software Configuration Tool

- 6) Navigate down to option “I2 Change Timezone” and press Enter
- 7) In the Configuring Tzdata window and under the Geographic area header, navigate down to “US” and press Enter
- 8) Under the Time zone header, navigate down to “Eastern” and press Enter
- 9) Navigate down to Finish to apply the settings and to return to the terminal
- 10) In the terminal type “sudo passwd” to change current user password
 - * Note: The default password for the user “Pi” is “raspberry”
- 11) Enter “!LoRaBePi2020!” twice with confirmation
 - * Note: The password is a paraphrase of “Love Rasp Berry Pi” and year 2020



```

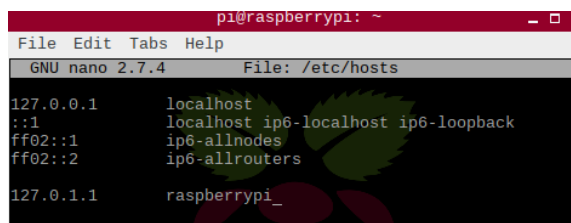
pi@Rasp_Srv: ~
File Edit Tabs Help
pi@Rasp_Srv:~ $ sudo passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
pi@Rasp_Srv:~ $

```

Figure 5.3 Current User Password Change

5.3. Network Configuration

- 1) To change the host name, type “sudo nano /etc/hostname” in the terminal
- 2) Once nano launches, change the hostname from “raspberrypi” to “Rasp_Srv”
- 3) Press “CTRL+X” on the keyboard and press “Y” to save to write to file
- 4) In the terminal, type “sudo nano /etc/hosts” and press enter
- 5) Change “raspberrypi” to “Rasp_Srv”



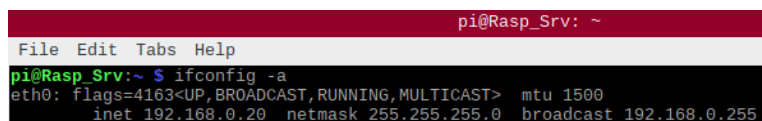
```

pi@raspberrypi: ~
File Edit Tabs Help
GNU nano 2.7.4 File: /etc/hosts
127.0.0.1    localhost
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
127.0.1.1   raspberrypi_

```

Figure 5.4 Hostname Change in /etc/hosts

- 6) Press “CTRL+X” on the keyboard and press “Y” to save to write to file
- 7) In the terminal, enter “reboot” to apply recently changed hostname
- 8) Once the OS reboots, click on the “Application Menu” on the upper left corner the taskbar
- 9) Navigate to “Accessories” to display another menu next to it
- 10) Click on “Terminal” to launch the terminal window
- 11) In the terminal, type “ifconfig -a” to view all available interface and to confirm the name of the wired connection. In this case, “eth0” is the wired connection



```

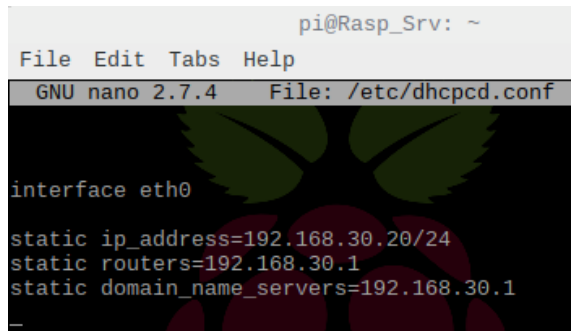
pi@Rasp_Srv: ~
File Edit Tabs Help
pi@Rasp_Srv:~ $ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 192.168.0.20 netmask 255.255.255.0 broadcast 192.168.0.255

```

Figure 5.5 Ifconfig Command

- 12) In the terminal type “sudo nano /etc/dhcpd.conf” to launch the text editor

- 13) Navigate to the end of the file and add a section for eth0 by typing “interface eth0”
- 14) Below the line, add “static ip_address=192.168.30.20/24”
- 15) Press Enter and add “static routers=192.168.30.1”
- 16) Add the final line, “domain_name_servers=192.168.30.1”



```

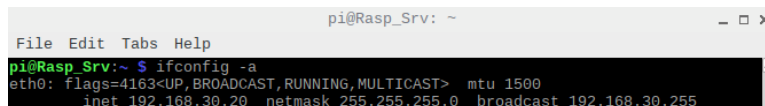
pi@Rasp_Srv: ~
File Edit Tabs Help
GNU nano 2.7.4 File: /etc/dhcpd.conf

interface eth0
static ip_address=192.168.30.20/24
static routers=192.168.30.1
static domain_name_servers=192.168.30.1

```

Figure 5.6 Static IP Configuration in /etc/dhcpd.conf

- 17) Enter CTRL+X and press “Y” to save the file and exit
- 18) In the terminal, type in “sudo reboot” to apply the changes
- 19) Once the OS reboots, click on the “Application Menu” on the upper left corner the taskbar
- 20) Navigate to “Accessories” to display another menu next to it
- 21) Click on “Terminal”
- 22) In the terminal, type in “ifconfig -a” to confirm the changes



```

pi@Rasp_Srv: ~
File Edit Tabs Help
pi@Rasp_Srv:~$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.30.20 netmask 255.255.255.0 broadcast 192.168.30.255

```

Figure 5.7 New Changes in Ifconfig Command

5.4. Pi-hole Installation

- 1) In the terminal, type in “sudo curl -sSL https://install.pi-hole.net | bash” and allow the program to do the checking
- 2) The Pi-hole Automated Installer window will launch in terminal, click “Ok” to confirm that the Pi-hole will apply network-wide
- 3) Click “Ok” to confirm the warning that the Pi-hole will act as a server that will need a static IP address
- 4) Tick all third-party vendors. Click “Ok” to proceed

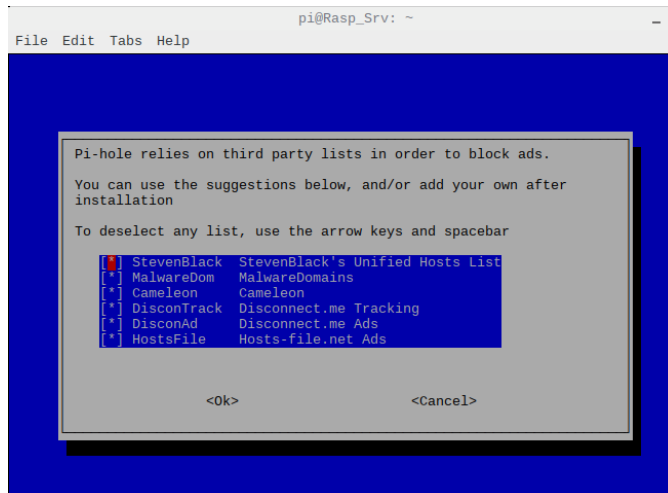


Figure 5.8 Ad-blocking from Third Party Lists

- 5) Select only “IPv4 Block ads over IPv4.” Click “Ok” to continue
- 6) On the Static IP Address, click “Yes” to confirm that system’s static IP address is “192.168.30.20/24” and the default gateway is “192.168.30.1”
- 7) Click “Ok” to proceed through the warning that the router may still conflict and assign out the IP address if not manually configured in the router
- 8) Tick “On (Recommended)” to install the web admin interface that is accessible with a web browser. Click “Ok” to proceed
- 9) Tick “On (Recommended)” to install the web server (lighttpd) to let the device host the application. Click “Ok” to proceed
- 10) Tick “On (Recommended)” to confirm to log queries. Click “Ok” to proceed
- 11) Tick “0 Show everything option” for the privacy mode for Faster Than Light (FTL) engine. FTL permit the ability to view web queries

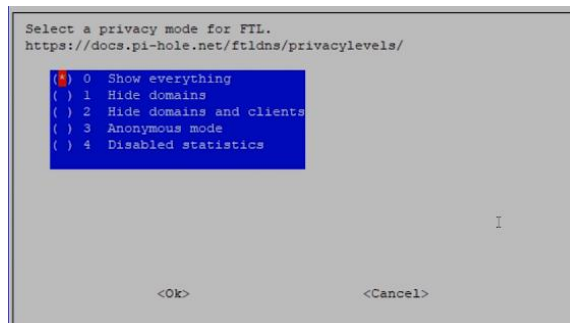


Figure 5.9 Privacy Mode for FTL

- 12) After the package configuration finishes the installation, the Installation Complete dialogue will appear. Confirm and record the following:
- IPv4 address is “192.168.30.20”
 - Web interface is “http://pi.hole/admin” or “http://192.168.30.20/admin”
 - Admin Login: “PwAvg0zV”

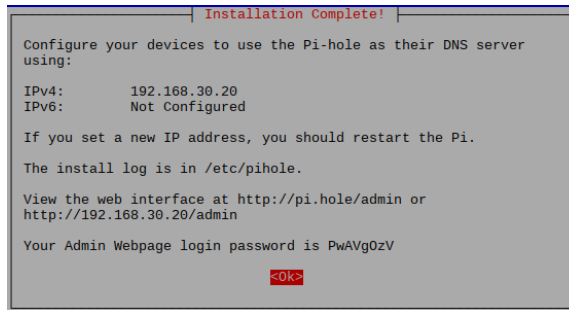


Figure 5.10 Admin Webpage Credentials

- 13) Click “Ok” to proceed back to the terminal

5.5. Pi-hole Setup

- Pi-Hole Admin’s password may only be changed in the terminal. In the terminal, type “sudo pihole -a -p”
- Enter “!LoRaBePiHo20!” twice with confirmation
 - * Note: The password is a paraphrase of “Love Rasp Berry Pi Hole” and year 2020

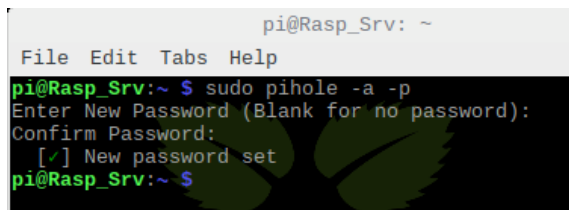


Figure 5.11 Pi-hole Login Credentials

- On any web browser, type and enter “http://pi.hole/admin” or “http://192.168.30.20/admin”
- On the left panel, click “Login” to enter the login page for admins

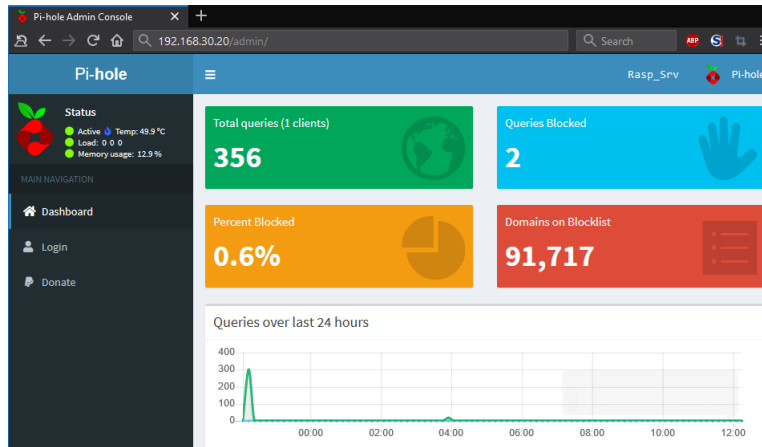


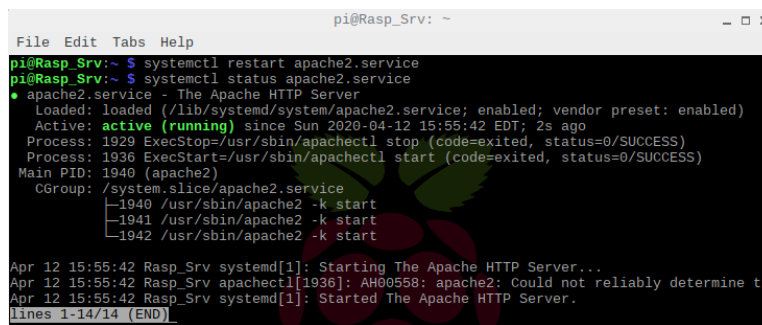
Figure 5.12 Pi-hole Dashboard

- 5) In the password field, enter “!LoRaBePiHo20” to enter the detailed dashboard
 - 6) Logout and exit application once dashboard have been reviewed. Pi-hole will continue to run in the background
-

6. Rasp Srv – Web Hosting

6.1. Apache Server Installation

- 1) Click on the “Application Menu” on the upper left corner the taskbar
- 2) Navigate to “Accessories” to display another menu next to it
- 3) Click on “Terminal” to launch the terminal window for Raspbian
- 4) Type and enter “sudo apt install apache2 -y”
- 5) Enter admin password when prompted
- 6) Type and enter “systemctl status apache2.service” after the installation has been completed
- 7) Enter the password for the current user when a new window prompt appears. In this case, enter “!LoRaBePiHo20!” for current user “Pi”
- 8) Type and enter “systemctl status apache2.service” to check the current status



```

pi@Rasp_Srv:~$ systemctl restart apache2.service
pi@Rasp_Srv:~$ systemctl status apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2020-04-12 15:55:42 EDT; 2s ago
     Process: 1929 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
     Process: 1936 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 1940 (apache2)
   OSGroup: /system.slice/apache2.service
            └─1940 /usr/sbin/apache2 -k start
               └─1941 /usr/sbin/apache2 -k start
                  └─1942 /usr/sbin/apache2 -k start

Apr 12 15:55:42 Rasp_Srv systemd[1]: Starting The Apache HTTP Server...
Apr 12 15:55:42 Rasp_Srv apachectl[1936]: AH00558: apache2: Could not reliably determine t
Apr 12 15:55:42 Rasp_Srv systemd[1]: Started The Apache HTTP Server.
lines 1-14/14 (END)

```

Figure 6.1 Apache2.Service Status

6.2. Apache HTML Setup

- 1) Using notepad++ in Windows 10, a HyperText Markup Language (HTML) file is created along with Cascading Style Sheets (CSS) to support the page
 - * *Note:* Using notepad++ in Windows 10 OS is done for simplicity
 - a. The following is the HTML code:

```

<!DOCTYPE html>
<html>

<head>
<!--
  CIS Senior Projects
  2440:491-001
  Dr. Nicholas

  Raspbian-Apache Web Front
  Author: Ethelyn Tran

```

Date: 13 April 2020

Filename: Front.htm

Supporting files: modernizr-1.5.js, fronstyles.css, Banner.jpg
-->

```

<meta charset="UTF-8" />
<title>Project E's Gaming Hub</title>
<script src="modernizr-1.5.js"></script>

<link href="frontstyles.css" rel="stylesheet" />
<script src="spam.js" type="text/javascript"></script>
  <script type="text/javascript">
    function showEM(userName,emServer) {
      /* The showEM() function displays a link to the user's
         e-mail address. The text of the user and e-mail server
         names are entered in reverse order to thwart e-mail
         harvesters.

        */

      userName = stringReverse(userName); // reverse the text of the userName parameter
      emServer = stringReverse(emServer); // reverse the text of the emServer parameter
      var emLink = userName + "@" + emServer; // combine the text of userName and emServer
      document.write("<a href= 'mailto:' + emLink + " ' ' >");
      document.write(emLink); document.write("</a>");
    }
  </script>
</head>
<body>
  <header></header>

  <nav class="vertical">
    <h1>Links</h1>
    <ul>
      <li><a href="#">About the Group</a></li>
      <li><a href="#">Gaming Channels</a></li>
      <li><a href="#">Internal Downloads</a></li>
      <li><a href="#">External Downloads</a></li>
    </ul>
  </nav>

  <section>
    <h1><strong>Main Announcement</strong></h1>
    <h4>This is a sample page to test out Rasp_Srv - Apache's Web Server</h4>
    <table border="1" cellpadding="5" cellspacing="0">
      <tr>
        <th>Faculty Member</th>
        <th>Role</th>
        <th>EMail</th>
      </tr>
      <tr>
        <td>Dr. John Nicholas</td>
        <td>Honors Project Sponsor</td>
        <td>
          <script type="text/javascript">showEM("nj","ude.norkau");</script>
        </td>
      </tr>
      <tr>
        <td>Professor Stanley Smith</td>
        <td>Reader</td>
        <td>
          <script type="text/javascript">showEM("htimshs","ude.norkau");</script>
        </td>
      </tr>
      <tr>
        <td>Professor Michael Haines</td>
        <td>Reader</td>
        <td>
          <script type="text/javascript"> showEM("42hwm","ude.norkau"); </script>
        </td>
      </tr>
    </table>
  </section>

```



```

        </td>
      </tr>
      <tr>
        <td>Advisor Sarah Hoge</td>
        <td>Honors Faculty Advisor</td>
        <td>
          <script type="text/javascript"> showEM("egohsm","ude.norkau");</script>
        </td>
      </tr>
    </table>
  </section>

  <footer>
    <address>
      <b>The University of Akron</b>
      <b>&#8226;</b>
      <b>Ethelyn Tran</b>
      <b>&#8226;</b>
      <script type="text/javascript"> showEM("71tmg","ude.norkau");
    </address>
  </footer>
</body>
</html>

```

b. The following is the CSS code for frontstyles.css:

```

/*
  Filename: frontstyles.css
  This file contains styles used in the front.html file.
*/
/* Display HTML5 structural elements as blocks */

article, aside, figure, figcaption, footer, hgroup, header,
section, nav {
display: block;
}

/* Set the default page element styles */
body * {
font-family: Verdana, Geneva, sans-serif;
font-size: 100%;
font-weight: inherit;
line-height: 1.2em;
list-style: none;
margin: 0px;
padding: 0px;
text-decoration: none;
vertical-align: baseline;
}

/* Body Styles */
body {
font-family: Verdana, Geneva, sans-serif;
font-weight: normal;
margin: 0px auto;
width: 1000px;
background-color: Black;
}

/* Header styles */
header {
background-color: rgb(0,6,43);
border-bottom: 1px solid blue;
margin-bottom: 0px;
}

nav {
background-color: white;
border: 1px solid green;
float: left;
width: 250px;
}

```

```
}  
  
nav ul {  
  margin: 10px;  
  
}  
  
nav ul li {  
  font-size: 14px;  
}  
  
nav ul li a {  
  display: block;  
  text-decoration: none;  
  color: black;  
  margin: 5px 0px;  
}  
  
nav ul li a:hover {  
  color: white;  
  background-color: rgb(0,150,0);  
}  
  
nav h1 {  
  background-color: rgb(0,150,0);  
  color: white;  
  display: block;  
  font-weight: bold;  
  letter-spacing: 3px;  
  text-align: center;  
  width: 100%;  
}  
  
section {  
  float: left;  
  margin-left: 35px;  
}  
  
section h1 {  
  color: white;  
  font-size: 24px;  
  font-weight: bold;  
  letter-spacing: 4px;  
  margin-bottom: 10px;  
  margin-top: 10px;  
}  
  
section h4 {  
  color: white;  
  font-size: 14px;  
  letter-spacing: 2px;  
  margin-bottom: 9px;  
  margin-top: 10px;  
}  
  
table {  
  border: 1px solid blue;  
  font-size: 14px;  
  margin-top: 0px;  
  margin-bottom: 20px;  
  width: 700px;  
}  
  
th {  
  background-color: rgb(0,7,196);  
  color: white;  
  font-weight: normal;  
  letter-spacing: 2px;  
  padding: 5px;  
}
```

```

td {
  vertical-align: top;
  background-color: white;
  padding: 5px;
}

td a {
  text-decoration: none;
}

td a:link {
  color: black;
  text-decoration: underline;
}

td a:hover {
  color: blue;
  text-decoration: underline;
}

td a:visited {
  color: purple;
  text-decoration: underline;
}

address {
  border-top: 1px solid blue;
  clear: left;
  padding-top: 10px;
  font-size: 10px;
  font-style: normal;
  text-align: center;
}

address b {
  color: white;
  margin-left: 10px;
  margin-right: 10px;
}

address a:link {
  color: white;
  text-decoration: underline;
}

address a:hover {
  color: blue;
  text-decoration: underline;
}

address a:visited {
  color: purple;
  text-decoration: underline;
}

```

- c. The following is the code for Spam.js for email links to be protected from harvesting

```

/*
  Function List:
  stringReverse
  Used to reverse the order of characters in a text string
*/

function stringReverse(textString) {
  if (!textString) return "";
  var revString="";
  for (i = textString.length-1; i>=0; i--)

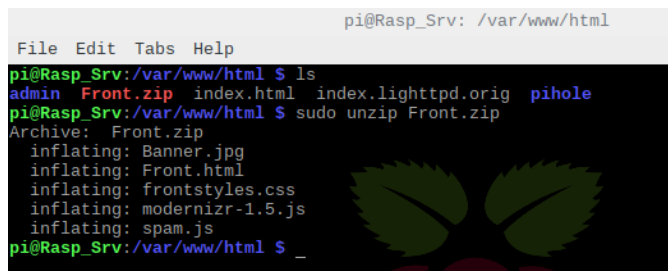
```

```

    revString+=textString.charAt(i)
return revString;
}

```

- 2) After transferring the html code to the Raspbian OS, navigate to the download file. In the terminal of the Raspbian OS, type and enter “cd Downloads”
- 3) Type and enter “ls” to view the existing file. In this case, the html is compressed into a zip file named “Front.zip”
- 4) Type and enter “sudo mv Front.zip /var/www/html” to move the zip file into the directory Apache launches HTML files
- 5) Navigate to the directory by entering “cd /var/www/html”
- 6) Type and enter “ls” to confirm the newly moved “Front.zip” file
- 7) Unzip the file by entering “sudo unzip Front.zip”



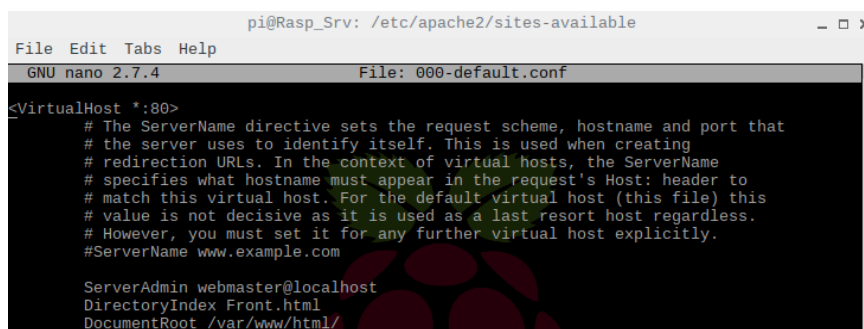
```

pi@Rasp_Srv: /var/www/html
File Edit Tabs Help
pi@Rasp_Srv:/var/www/html $ ls
admin Front.zip index.html index.lighttpd.orig pihole
pi@Rasp_Srv:/var/www/html $ sudo unzip Front.zip
Archive: Front.zip
  inflating: Banner.jpg
  inflating: Front.html
  inflating: frontstyles.css
  inflating: modernizr-1.5.js
  inflating: spam.js
pi@Rasp_Srv:/var/www/html $ _

```

Figure 6.2 Unzipping Front.html

- 8) Remove the original HTML file by typing “sudo rm index.html”
- 9) Type and enter “cd /etc/apache2/sites-available/” to navigate to the Apache’s site configuration
- 10) Type and enter “sudo nano 000-default-conf” to edit the configuration file
- 11) After the 000-default-conf launches in the text-editor, locate the line “DocumentRoot /var/www/html”
- 12) Above that line, add “DirectoryIndex Front.html” to direct default page to Front.html



```

pi@Rasp_Srv: /etc/apache2/sites-available
File Edit Tabs Help
GNU nano 2.7.4 File: 000-default.conf
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DirectoryIndex Front.html
DocumentRoot /var/www/html/

```

Figure 6.3 Apache Default Directory Index

13) Press CTRL+X and click “Y” to write into the file and exit the file

6.3. Basic Access Authentication Implementation

- 1) In the terminal, type and enter “mkdir /etc/htpasswd” to make a directory dedicated to users and the user’s respective password
- 2) Create the htpasswd’s hidden folder and add the user by typing “sudo htpasswd -c /etc/htpasswd/.htpasswd username”
 - * *Note:* username will be in respect to the users in Ubuntu OS
- 3) Enter the password twice to confirm the user’s password. In this case, for user “Garen”, the password is “League123” in respect to Ubuntu OS

```

pi@Rasp_Srv: /etc/htpasswd
File Edit Tabs Help
pi@Rasp_Srv:/etc/htpasswd $ sudo rmdir .htpasswd
pi@Rasp_Srv:/etc/htpasswd $ sudo htpasswd -c /etc/htpasswd/.htpasswd Garen
New password:
Re-type new password:
Adding password for user Garen
pi@Rasp_Srv:/etc/htpasswd $
pi@Rasp_Srv:/etc/htpasswd $
    
```

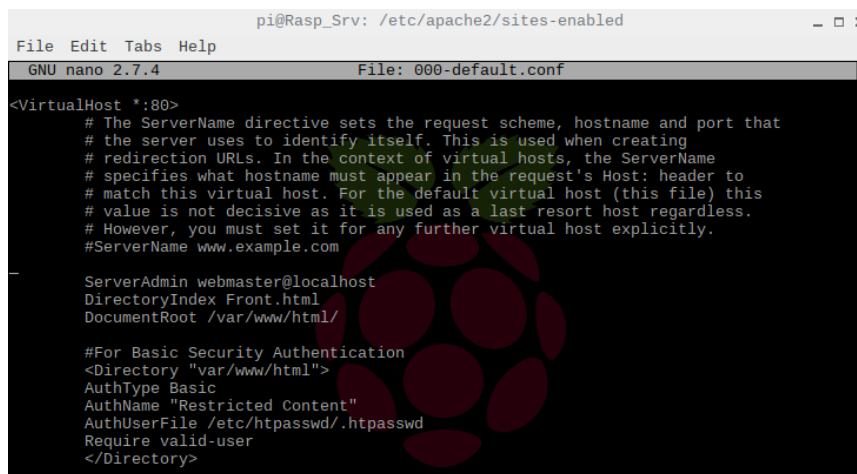
Figure 6.4 Htpasswd Created with User

- 4) For subsequent users, omit the option “-c” of creating the hidden file by typing “sudo htpasswd /etc/htpasswd/.htpasswd username”
 - a. Perform for the following user:

User	Password
Garen	League123
Annie	League123
Ashe	League123
Akali	Legend456
Ahri	Legend456
Ezreal	Legend456

- 5) Type and enter “cd” to the main directory
- 6) Navigate to the Apache configuration file by entering “cd /etc/apache2/sites-enabled/”
- 7) Type and enter “ls” to view the current files in the directory
- 8) To edit the configuration file, type and enter “sudo nano 000-default.conf”

- 9) Once the file editor launches, add the following lines underneath the line “DocumentRoot /var/www/html”
 - a. # For Basic Security Authentication
 - b. <Directory “var/www/html”>
 - c. AuthType Basic
 - d. AuthName “Restricted Content”
 - e. AuthUserFile /etc/htpasswd/.htpasswd
 - f. Require valid-user
 - g. </Directory>



```
pi@Rasp_Srv: /etc/apache2/sites-enabled
File Edit Tabs Help
GNU nano 2.7.4 File: 000-default.conf
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DirectoryIndex Front.html
DocumentRoot /var/www/html/

#For Basic Security Authentication
<Directory "var/www/html">
AuthType Basic
AuthName "Restricted Content"
AuthUserFile /etc/htpasswd/.htpasswd
Require valid-user
</Directory>
```

Figure 6.5 Authentication Type Basic Entry

- 10) Click CTRL+X and click “Y” to write to the file and exit
 - 11) In the terminal, type in “sudo systemctl restart apache2.service” to restart the overall Apache2 services
 - 12) Type and enter “sudo systemctl status apache2.service” to confirm that the Apache2 application is running and active
-

7. Layer 2 Cisco Switch: S1

Utilizing Cisco 3560 Series Switch, the Layer 2 network device is named “S1” and is implemented three Virtual Local-Area Networks (VLANs) to include a Data VLAN reserved for local users, a Guest VLAN reserved for visiting local users, and a Management VLAN reserved for management to connect to for diagnosis. The rest of the ethernet ports is implemented with basic security practices.

Interface	VLAN / Device	IPv4 Address Range
Fa0/1 – Fa0/10	Data – VLAN 10	192.168.1.0-192.168.1.255 255.255.255.0
Fa0/11 – Fa0/20	Guest – VLAN 20	192.168.2.0-192.168.2.255 255.255.255.0
Fa0/21 – Fa0/45	Shutdown	-
Fa0/46 – Fa0/47	MLS1	-
Fa0/48	R1 – Int VLAN 1	192.168.0.2 255.255.255.0
G0/1 – G0/2	Management – VLAN 99	192.168.9.0-192.168.9.255 255.255.255.0

7.1. Device Setup

- 1) In the terminal emulator, type and enter “enable” to enter the Privileged EXEC mode
- 2) Type “write erase” and press enter to begin the process of clearing any previous configuration to default factory setting
- 3) Press Enter to continue
- 4) After the clearing process, type and enter “reload” to reboot device
- 5) Press Enter to confirm

- 6) Once the device reloads, type and enter “enable” to enter the Privileged EXEC mode
- 7) Type in “configure terminal” to enter Global Configuration mode
- 8) Type in “hostname S1”

- 9) Type in “enable secret *password*” to set the Global Configuration encrypted password. In this case, the password is “ProjectE01!”swi
- 10) Type in “line con 0” to configure console line
- 11) Type in “password *password*” to set the console line password. In this case, the password to enter by console is “Project20!”
- 12) Type in “login” to apply during login
- 13) Type in “line vty 0 15” to configure Telnet and SSH virtual line
- 14) Type in “password *password*” to set the console line password. In this case, the password to enter by console is “Project04!”
- 15) Type in “login” to apply during login
- 16) Type in “Transport input all” to permit both Telnet and SSH

- 17) Enter “service password-encryption” to encrypt every password listed in the running-configuration

7.2. VLAN Implementation

- 1) Within the Global Configuration, type in “vlan 10” to create VLAN 10
- 2) Type in “name Data” to name VLAN 10
- 3) Type in “vlan 20” to create VLAN 20
- 4) Type in “name Guest” to name VLAN 20
- 5) Type in “vlan 30” to create VLAN 30
- 6) Type in “name Server” to name VLAN 30
- 7) Type in “vlan 99” to create VLAN 99
- 8) Type in “name Management” to name VLAN 99
- 9) Type in “vlan 88” to create VLAN 88
- 10) Type in “name Native” to name VLAN 88

- 11) Enter “Interface VLAN 5” to create the virtual interface for the L2 Switch
- 12) Enter “ip address 192.168.1.5 255.255.255.0”
- 13) To return to previous mode, enter “exit”
- 14) Enter “ip default-gateway 192.168.1.1 255.255.255.0”

7.3. Interface Configuration

- 1) Type in “Interface range fa0/1-10” to enter the configuration setting of the range of Fast Ethernet 0/1 to Fast Ethernet 0/10
- 2) Type in “switchport mode access” to assign the port to access for data traffic
- 3) Type in “switchport access vlan 10” to assign the port for VLAN 10
- 4) Type in “no shutdown” to ensure connectivity
- 5) Enter in “Interface range fa0/11-20”
- 6) Enter in “switchport mode access”
- 7) Enter in “switchport access vlan 20”
- 8) Enter in “no shutdown”
- 9) Enter in “Interface range g0/1-2” to enter the configuration of the range of Gigabit Ethernet ports
- 10) Enter in “switchport mode access”
- 11) Enter in “switchport access vlan 99”
- 12) Enter in “no shutdown”
- 13) Type and enter “interface range fa0/21-45, g0/3-4” to address unused interface
- 14) Type and enter “shutdown” to administrative shut down the ports
- 15) Exit the configuration mode by entering “exit”

- 16) To configure EtherChannel, type in “interface port-channel 1” to create a logical channel
- 17) Return to the previous mode again with “exit”
- 18) In the terminal, type in “interface range fa0/46-48” to enter the configuration of all trunk ports
- 19) Enter “channel-group 1 mode on” which forces connection without negotiating for all the links
- 20) Return by entering “exit”
- 21) Type and enter “interface port-channel 1” to enter the logical EtherChannel”
- 22) Enter in “switchport trunk encapsulation dot1q” to negotiate the ports to dot1q
- 23) Enter in “switchport mode trunk” to assign the ports as trunks

- 24) Enter in “switchport trunk native vlan 88” to assign VLAN traffic to be directed into the trunk
 - 25) Enter in “switchport trunk allowed vlan 10,20,30,99” to permit traffic through trunk
 - 26) To save the current configuration, type and enter in “copy running-configuration startup-configuration”
-

8. Layer 3 Multilayer Switch: MLS1

Using Cisco Multilayer Switch 3560 Series, the equipment will function as a multilayer switching Layer 3 Equipment. The L3 Switch will serve as the default gateway to the static Rasp_Srv and Ubu_Srv. The MLS1 will operate on the OSPF routing protocol and is connected to the Cable Modem router. MLS1 will also serve as router for redundancy failure should R1 fail for the local users. Basic ACLs implementation will be applied. IPsec Tunneling will not be configured due to home modem router's VPN passthrough limitation

Interface	VLAN / Device	IPv4 Address Range
Fa0/1 – Fa0/10	Server – VLAN 30	192.168.3.0-192.168.3.255 255.255.255.0
Fa0/11 – Fa0/45	Shutdown	-
Fa0/46 – Fa0/47	S1	-
Fa0/48	Cable Modem	192.168.0.8-192.168.0.11 255.255.255.252

8.1. Device Setup

- 1) In the terminal emulator, type and enter “enable” to enter the Privileged EXEC mode
- 2) Type “write erase” and press enter to begin the process of clearing any previous configuration to default factory setting
- 3) Press Enter to continue
- 4) After the clearing process, type and enter “reload” to reboot device
- 5) Press Enter to confirm

- 6) Once the device reloads, type and enter “enable”
- 7) Type in “configure terminal” to enter Global Configuration mode
- 8) Type in “hostname MLS1”
- 9) Type in “enable secret *password*” to set the Global Configuration encrypted password. In this case, the password is “ProjectE01!”
- 10) Type in “line con 0” to configure console line

- 11) Type in “password *password*” to set the console line password. In this case, the password to enter by console is “Project20!”
- 12) Type in “login” to apply during login
- 13) Type in “line vty 0 15” to configure Telnet and SSH virtual line
- 14) Type in “password *password*” to set the console line password. In this case, the password to enter by console is “Project04!”
- 15) Type in “login” to apply during login
- 16) Type in “Transport input all” to permit both Telnet and SSH
- 17) Enter “service password-encryption” to encrypt every password listed in the running-configuration

8.2. VLAN Implementation

- 1) Within the Global Configuration, type in “vlan 10” to create VLAN 10
- 2) Type in “name Data” to name VLAN 10
- 3) Directly type in “vlan 20” to create VLAN 20
- 4) Type in “name Guest” to name VLAN 20
- 5) Type in “vlan 30” to create VLAN 30
- 6) Type in “name Server” to name VLAN 30
- 7) Type in “vlan 99” to create VLAN 99
- 8) Type in “name Management” to name VLAN 99
- 9) Type in “vlan 88” to create VLAN 88
- 10) Type in “name Native” to name VLAN 88
- 11) Type in the exit once finish

8.3. Interface Configuration

- 1) To enter the configuration setting of the range of Fast Ethernet 0/1 to Fast Ethernet 0/10, enter in “Interface range fa0/1-10”
- 2) Type in “switchport mode access” to assign the port to access for data traffic
- 3) Type in “switchport access vlan 30” to assign the port for VLAN 30
- 4) Type in “no shutdown” to ensure connectivity
- 5) Type and enter “interface range fa0/11-45” to address unused interface

- 6) Type and enter “shutdown” to administrative shut down the ports
- 7) Return to the previous configuration mode with “exit”

- 8) To create the logical channel interface with “interface port-channel 1”
- 9) Enter “exit”
- 10) Type in “interface range fa0/46-48” to enter the configuration of all trunk ports
- 11) Type and enter “channel-group 1”
- 12) Type and enter “exit” to return
- 13) Create the sub-interfaces within the logical interface by typing “interface port-channel 1.10”
- 14) Type and enter “encapsulation dot1q 10”
- 15) Enter “ip address 192.168.1.2 255.255.255.0”
- 16) Return by typing “exit”
- 17) Continue with other sub-interfaces with “interface port-channel 1.20”
- 18) Type and enter “encapsulation dot1q 20”
- 19) Enter “ip address 192.168.2.2 255.255.255.0”
- 20) Return by typing “exit”
- 21) Enter in “interface port-channel 1.30”
- 22) Type and enter “encapsulation dot1q 30”
- 23) Enter “ip address 192.168.3.2 255.255.255.0”
- 24) Return by typing “exit”
- 25) Enter in “interface port-channel 1.99”
- 26) Type and enter “encapsulation dot1q 99”
- 27) Enter “ip address 192.168.9.2 255.255.255.0”
- 28) Return by typing “exit”
- 29) Enter in “interface port-channel 1.88”
- 30) Type and enter “encapsulation dot1q 88”
- 31) Enter “ip address 192.168.8.2 255.255.255.0”
- 32) Return by typing “exit”

8.4. Hot Standby Router Protocol (HSRP)

- 1) In the terminal, type and enter “interface range Fa0/46-47”
- 2) Enable the protocol with “standby version 2”
- 3) Add “standby 10 preempt” after enabling the protocol
- 4) Assign the interfaces with “standby 10 priority 100”
** Note: MLS1 will act as the standby routing device with the priority 100 being lower than R1’s higher priority of 110*
- 5) Then, assign the standby group with “standby 10 ip 192.168.1.10”
- 6) Enter “exit” to return to the Global Configuration mode

8.5. Open Shortest Path first (OSPF) Routing Protocol

- 1) In the terminal’s Global Configuration mode, type and enter “router ospf 1” to enable and initiate the routing protocol configuration
- 2) Include the area 0 that connects to the Cable modem with “network 192.168.0.8 0.0.0.3 area 0”
** Note: Wildcard mask of the range is required to identify the subnet range of the network*
- 3) Include the internal area by typing “network 192.168.30.0 0.0.0.255 area 0”
- 4) Enter “exit” to return to the Global Config mode
- 5) Allow a static route for hosts to exit the area with “ip route 0.0.0.0 0.0.0.0 interface fa0/48”
** Note: The static route allows the static route with all available in the routing table with the exit interface*

8.6. Access Control Lists (ACLs)

- 1) To ensure that only known internal user can ping the network equipment, enter the following, “ip access-list extended 102”
- 2) After entering the access list number 102, enter a rule to deny Guest telnetting into the device “5 deny tcp 192.168.2.1 0.0.0.255 any eq telnet”
- 3) Enter a rule to permit local Data hosts to telnet into the devices, “10 permit tcp 192.168.0.1 0.0.0.255 any eq telnet”

- 4) Enter a rule to permit Management hosts to telnet into the devices, “15 permit tcp 192.168.9.1 0.0.0.255 any eq telnet”
 - 5) Enter “20 deny tcp any any eq telnet” to deny every host that is not within the internal network
 - 6) Type “25 permit icmp 192.168.0.1 0.0.15.255 any” to permit internal network subnet to ping at any destination
 - 7) Enter “30 deny icmp any any” to block all icmp traffic from other subnet to any destination host within the network
 - 8) With just one ACL implementation, a deny all will be implicitly applied. Type and enter “access-list permit ip any any” to allow other traffic flow
 - 9) To save the current configuration, type and enter in “copy running-configuration startup-configuration”
-

9. Layer 3 Router: R1

Using Cisco Router 2811 Series, the equipment will function as a standard Layer 3 router named R1. R1 router will serve as the default gateway for host PC1 and PC2 with the higher priority for traffic. EIGRP will be configured to be connected to the Cable Modem router. Basic inter-VLAN routing and ACLs implementation will be applied. IPsec Tunneling will not be configured due to home modem router's VPN passthrough limitation

Interface	VLAN / Device	IPv4 Address Range
F0/1	S1	192.168.1.0 – 192.168.9.0 255.255.255.0
Fa0/2	Cable Modem	192.168.0.4 – 192.168.0.7 255.255.255.0

9.1. Basic Setup

- 1) To enter the Privileged EXEC mode, type and enter “enable” in the terminal emulator
- 2) Type “write erase” and press enter to begin the process of clearing any previous configuration to default factory setting
- 3) Press Enter to continue
- 4) After the clearing process, type and enter “reload” to reboot device
- 5) Press Enter to confirm

- 6) Once the device reloads and prompts, type and enter “enable”
- 7) To enter Global Configuration mode, type in “configure terminal”
- 8) Type in “hostname *devicename*” to set the device's name. In this case, enter “hostname R1”
- 9) Enter in “enable secret *password*” to set the Global Configuration encrypted password. In this case, use the password “ProjectE01!”
- 10) Type in “line con 0” to configure console line
- 11) Type in “password *password*” to set the console line password. “password Project20!” will be used
- 12) Type in “login” to apply during login

- 13) To configure Telnet and SSH virtual line, type in “line vty 0 5”
- 14) Type in “password *password*” to set the console line password. In this case, enter “password Project04!” to set the password
- 15) To apply for the login, enter in “login”
- 16) To permit both Telnet and SSH, enter in “Transport input all”
- 17) To encrypt every password listed in the running-configuration, enter “service password-encryption”

9.2. VLAN Implementation

- 1) Within the same Global Configuration mode and to create VLAN 10, type in “vlan 10”
- 2) To name VLAN 10, enter “name Data”
- 3) To create VLAN 20, type in “vlan 20”
- 4) To name VLAN 20, enter “name Guest”
- 5) To create VLAN 30, type in “vlan 30”
- 6) To name VLAN 30, enter “name Server”
- 7) To create VLAN 99, type in “vlan 99”
- 8) To name VLAN 99, enter “name Management”
- 9) To create VLAN 88, type in “vlan 88”
- 10) To name VLAN 88, enter “name Native”
- 11) To exit and return, type and enter “exit”

9.3. Interface Configuration

- 1) To enter the configuration of Fast Ethernet 0/2, type in “interface fa0/2”
- 2) To assign the interface an IP Address, enter in “ip address 192.168.0.6 255.255.255.0”
- 3) To ensure connectivity, enter in “no shutdown”
- 4) To create the sub-interfaces within the logical interface by typing “interface fa0/1.10”
- 5) Type and enter “encapsulation dot1q 10”
- 6) Enter in “ip address 192.168.1.1 255.255.255.0”

- 7) Return by typing “exit”
- 8) To continue creating other sub-interfaces, enter in “interface fa0/1.20”
- 9) Type and enter “encapsulation dot1q 20”
- 10) Enter in “ip address 192.168.2.1 255.255.255.0”
- 11) Return by typing “exit”
- 12) Enter in “interface fa0/1.30”
- 13) Type and enter “encapsulation dot1q 30”
- 14) Enter in “ip address 192.168.3.1 255.255.255.0”
- 15) Return by typing “exit”
- 16) Enter in “interface fa0/1.99”
- 17) Type and enter “encapsulation dot1q 99”
- 18) Enter in “ip address 192.168.9.1 255.255.255.0”
- 19) Return by typing “exit”
- 20) Enter in “interface fa0/1.88”
- 21) Type and enter “encapsulation dot1q 88”
- 22) Enter in “ip address 192.168.9.1 255.255.255.0”
- 23) Return by typing “exit”
- 24) To configure the overall interface Fast Ethernet 0/1, enter in “interface fa0/1”
- 25) To ensure functionality, enter in “no shutdown”
- 26) Enter in “exit” to return to the previous mode

9.4. Hot Standby Router Protocol (HSRP)

- 1) Within in the Global Configuration mode, type and enter in “interface Fa0/1”
- 2) Enable the protocol with “standby version 2”
- 3) After enabling protocol, add “standby 10 preempt” after the previous command
- 4) Assign the interfaces with “standby 10 priority 110”
 - * *Note:* R1 will act as the main routing device with the priority 110
- 5) Assign the standby group with “standby 10 ip 192.168.1.10”
- 6) Enter “exit” to return to the Global Configuration mode

9.5. Enhanced Interior Gateway Routing Protocol (EIGRP)

- 1) Within the same Global Configuration mode and to enable EIGRP, enter in “router eigrp 100”
- 2) With EIGRP automatically summarizing routes, enter in “no auto-summary” to manually add in each network to ensure that all connected devices are accounted for security
- 3) Add “network 192.168.0.4 0.0.0.3” for connection to the Cable Modem
- 4) Add each internal network by entering “network 192.168.1.0 0.0.0.255”
- 5) Add “network 192.168.2.0 0.0.0.255” after the previous command
- 6) Add “network 192.168.3.0 0.0.0.255”
- 7) Enter in “network 192.168.9.0 0.0.0.255” to add any host within in Management VLAN

9.6. Access Control Lists (ACLs)

- 1) To begin the ACLs set, enter in “ip access-list extended 101”
 - 2) To deny Guest telnetting into any device with “5 deny tcp 192.168.2.1 0.0.0.255 any eq telnet”
 - 3) To permit Data hosts to telnet into any device, “10 permit tcp 192.168.0.1 0.0.0.255 any eq telnet”
 - 4) To permit Management hosts to telnet into any devices, “15 permit tcp 192.168.9.1 0.0.0.255 any eq telnet”
 - 5) Enter “20 deny tcp any any eq telnet” to deny unlisted subnets
 - 6) To permit internal subnet to ping at any destination, enter in “25 permit icmp 192.168.0.1 0.0.15.255 any”
 - 7) To block all ICMP traffic from other subnet to any destination IP, enter in “30 deny icmp any any”
 - 8) With the implicit deny all, type and enter “access-list permit ip any any” to allow other traffic flow
 - 9) To save the current configuration, type and enter in “copy running-configuration startup-configuration”
-

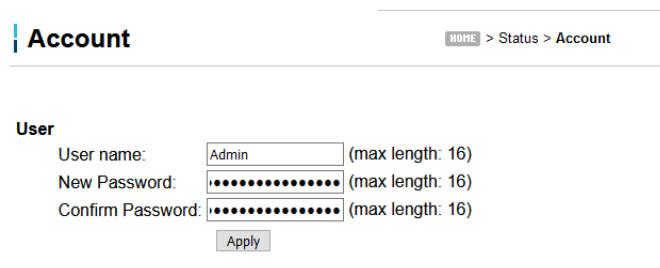
10.Spectrum Cable Modem: Ubee DDQ36C / Home Router

Ubee DDQ36C Cable Modem is the home router provided by Internet Service Provider (ISP) Spectrum, acting as the gateway router between the local network and the internet. The cable modem is configured to support four wired connections and dual channel wireless connections with secure administrative privileges. By default, Network Address Translation (NAT) is performed by the ISP side and is not available to configure. Dynamic Host Configuration Protocol (DHCP) is configured to permit a singular IPv4 range. As part of the Term of Service and User Agreement with the ISP, features such as NAT and extended DHCP range cannot be configured. Domain Name Service (DNS) is enabled for Pi-hole to filter through queries

10.1. Secure Admin Login

- 1) To configure wireless without a console cable, a web browser can be used to access the home router. In any web browser, type in “http://192.168.0.1”
- 2) On the left panel, click “Login” to enter the cable modem software information page
- 3) On the Status navigation panel on the left, click “Account”
- 4) Under the Account header, enter the “Admin” on the User name field
- 5) Enter the admin’s password for both New Password and Confirm Password field. In this case, the password is set to “04HoRoAdPa202!”

* *Note:* The recommended minimum password length for admin users is 14 characters. In this case, the password is a paraphrase of “April”, “Home Router Admin Password” and the abbreviation of year “2020”



The screenshot shows the 'Account' page of the home router portal. At the top left, there is a vertical bar with the word 'Account' in bold. To the right of this bar, there is a breadcrumb trail: 'HOME > Status > Account'. Below the breadcrumb trail, there is a section titled 'User' with three input fields: 'User name:' containing 'Admin', 'New Password:' with 16 dots, and 'Confirm Password:' with 16 dots. Each field has '(max length: 16)' to its right. Below the input fields is an 'Apply' button.

Figure 10.1 Account Credentials to Home Router Portal

- 6) Click “Apply” to confirm changes

10.2. Dynamic Host Configuration Protocol (DHCP) Server

- 1) On the top navigation bar, click the “Basic” tab on the top navigation panel
- 2) Click on DHCP on the left navigation panel

The screenshot displays the DHCP configuration page in a router's web interface. The top navigation bar includes tabs for Status, Basic, Advanced, Firewall, Parental Control, Wireless, MoCA, and Logout. The left sidebar lists various configuration options: Setup, DHCP, DHCPv6, LAN IPv6, DDNS, Static Lease, Backup, and Time. The main content area is titled 'DHCP' and shows the following settings:

- DHCP Server: Yes No
- Starting Address Set:
 - Private Starting Address: 192.168.0.2 (2-254) Number of CPES: 0
 - Public Starting Address: 0.0.0.0 (2-254) Number of CPES: 0
- Lease Time: 86400

An 'Apply' button is located at the bottom of the configuration area.

Figure 10.2 Basic Tab with DHCP Configuration

- 3) For DHCP Server, click the “Yes” button
- 4) Click on the button to set the setting to use the DHCP service for “Private” addresses
- 5) Enter the range of Private IP address that the DHCP server will distribute. In this case, the Private Starting Address is 192.168.0.2 up to 192.168.15.255
 - * Note: Current configuration did not permit more than the given range of IP address. Out of range comes back with “One or more error occurred while processing.” Different router or ISP agreement may differ
- 6) Click “Apply” to confirm the changes

10.3. Dynamic Domain Name Server (DDNS) Services

- 1) Navigate to the “Advanced” tab on the top navigation bar
- 2) Through Options, tick the box next to “DNS Relay” to enable
- 3) Navigate back to the “Basic” tab
- 4) Click on “DDNS” on the left navigation bar

DDNS

HOME > Basic > DDNS

DDNS Service:

User Name:

Password:

Host Name:

IP Address: **Redacted**

Status: DDNS service is not enabled.

Figure 10.3 DDNS Options

- 5) In the User Name field, enter the Pi-hole credential. In this case, the username is “admin”
- 6) Enter the Pi-hole admin’s password. In this case, enter “!LoRaBePiHo20!”
- 7) For the Host Name field, redirect to the Raspberry Pi’s static IPv4 address. In this case, enter “192.168.3.20”
- 8) Click “Apply” to continue

10.4. Network Time Protocol (NTP) Services

- 1) Under the same tab, click on “Time” on the left navigation panel
- 2) Click on the button to enable Simple Network Time Protocol (SNTP)
- 3) Enter three different Time Server for each field. In this case, “clock.via.net,” “ntp.nasa.gov,” and “tick.ucla.edu” are listed
 - * *Note:* Time servers are hosted by various third-party vendor. Several NTP servers can be provided by “NIST Internet Time Servers” and “ntppool.org”
- 4) Set the Timezone Offset to “-5” Hours to account for Daylight Savings in Eastern Standard Time

Time

Enable SNTP Yes No

Time Server 1

Time Server 2

Time Server 3

Timezone Offset Hours Minutes

Figure 10.4 NTP Time Servers

- 5) Click “Apply” to confirm

10.5. Port-Forwarding Services

- 1) On the top navigation panel, click on the “Advanced” tab
- 2) On the left navigation panel, click on “Forwarding” section
- 3) Click “Create IPv4” button
- 4) In the Local IP field, enter the local IPv4 address. In this case, “192.168.3.20” for the Apache Web Server Application on the Rasp_Srv
- 5) In the port fields, permit the start and end ports to be 80 and 443
 - * *Note:* Port 80 is the HyperText Transfer Protocol (HTTP) port, and port 443 is the HyperText Transfer Protocol Secure (HTTPS) port
- 6) Select “TCP” on the drop-down menu for the Protocol field
- 7) Select “On” on the drop-down menu for the Enabled filed
- 8) Click “Apply” to add the entry
- 9) Click “Create IPv4” button again
- 10) In the Local IP field, enter the local IPv4 address. In this case, “192.168.3.10” for the FTP server on the Ubu_Srv
- 11) In the port fields, permit the start and end ports to be 20 and 21
 - * *Note:* Port 20 is the active FTP data port and port 21 is the FTP service
- 12) Select “TCP” on the drop-down menu for the Protocol field
- 13) Select “On” on the drop-down menu for the Enabled filed
- 14) Click “Apply” to add the entry

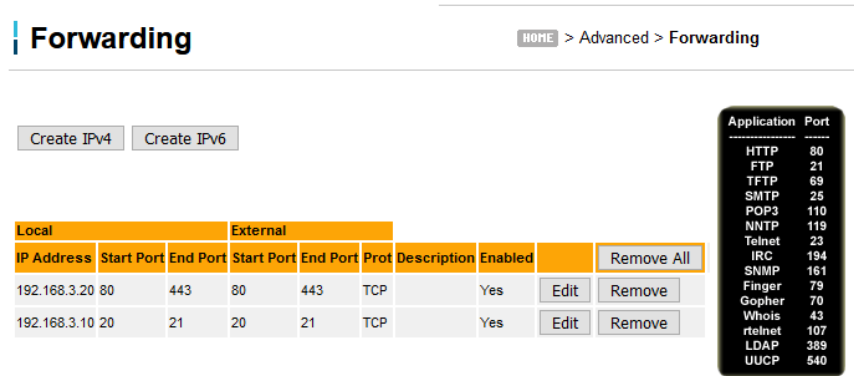


Figure 10.5 Port-Forwarding Entries

10.6. Service Set Identifier (SSID) and Password

- 1) On the top navigation panel, click on the “Wireless” tab to configure Wi-Fi settings
- 2) On the left navigation panel, click on “2.4G Hz” channel
- 3) Under the channel header, click on “Primary Network” section
- 4) Select “Enabled” in the drop-down menu for Primary Network field
- 5) For the Network Name (SSID) field, enter any desire name for easy identification over wireless scanning
- 6) Select “On” in the drop-down menu for Broadcast SSID field
- 7) Select “Mixed (11b/g/n)” in the drop-down menu for Wireless Mode
- 8) Select “Enabled” for the WPA2-PSK field in the drop-down menu to confirm the Pre-Shared Key (PSK) as the highest available protected access on the cable modem
- 9) For the WPA/WPA2 Encryption field, select “AES” as the WPA2-PSK is based on Advanced Encryption Standard (AES) cipher
- 10) Enter the password for the wireless connection in the “WPA Pre-Shared Key” field
- 11) Click “Apply” to confirm changes to bring 2.4G Hz channel up

Primary Network

MAC-ID: Redacted

Primary Network Enabled ▾

Network Name (SSID) Redacted

Broadcast SSID On ▾

Wireless Mode Mixed (11b/g/n) ▾

WPA Disabled ▾

WPA-PSK Disabled ▾

WPA2 Disabled ▾

WPA2-PSK Enabled ▾

WPA/WPA2 Encryption AES ▾

WPA Pre-Shared Key *****

Show Key

Figure 10.6 2.4G Hz Wireless Settings

- 12) On the left navigation panel, click on “5G Hz” channel
- 13) Click on “Primary Network” section
- 14) Select “Enabled” for the Primary Network field

- 15) For the Network Name (SSID) field, enter any desire name for easy identification over wireless scanning to differentiate from the 2.4G Hz channel
 - 16) Select “On” for the Broadcast SSID field
 - 17) Select “Mixed (11b/g/n)” for the Wireless Mode
 - 18) Select “Enabled” for the WPA2-PSK field
 - 19) Select “AES” as the WPA/WPA2 Encryption field
 - 20) Enter the password in the “WPA Pre-Shared Key” field
 - 21) Click “Apply” to confirm the new changes
-

CIS: Senior Project
2440:491-001

Testing Documentation

Ethelyn Tran
Part V of VII

Testing Documentation

The testing documentation demonstrates the network connectivity and functionalities of various devices. The documentation will also include vulnerability scans and penetration testing from certain device where applicable. Each entry includes a description of purpose and intended goal. The testing documentation will also notate possible issues encountered during setup. An understanding of the testing of each functionality allows the administrator to assess and diagnose the system as well as maintain the system's functionality

1. Server Functionality with PC2 Windows 10 OS

1.1. Rasp_Srv – Web Server with Security Authentication

- 1) To confirm the active Apache2 server, type and enter “systemctl status apache2.service” in the terminal
- 2) Open any internet web browser, and navigate to the address bar
- 3) Type and enter the Rasp_Srv's localhost address with “http://192.168.3.20:80/” with port 80 for HTTP

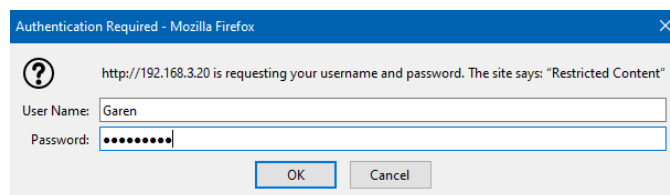


Figure 1.1 Authentication Required Prompt

- 4) The website will prompt the user for credentials to enter the “Restricted Content” In this case, the user “Garen” and the password “League123” are used
- 5) Click “OK” to enter the credentials and to load the front interface

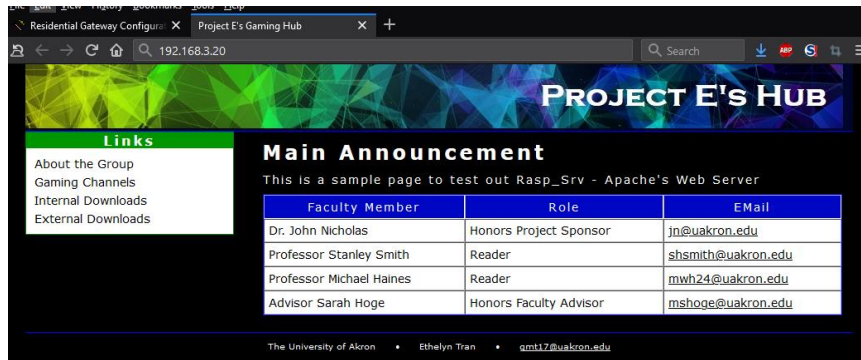


Figure 1.2 Website Front Page

- 6) Similar for remote users, open any web browser and type in “http://ExternalIPAddress:80”
- 7) The user will be prompted with the same requirement for authentication

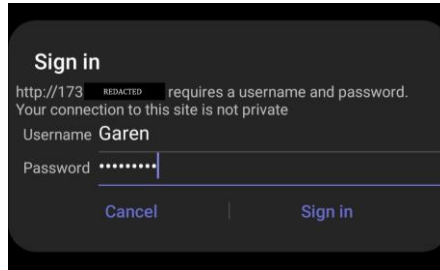


Figure 1.3 External IP's Authentication Prompt

1.2. Ubu_Srv – File Transfer Program (FTP) with Security Access

- 1) Click on the Windows “Start” button on the lower left task bar
- 2) In the search bar, type “CMD” for Windows OS 10 command line
- 3) In the prompt, enter the protocol and the FTP server’s static IP address with “ftp 192.168.3.10”
- 4) The designated banner will be issued and prompted for the username. In this case, enter “Garen” for the user
- 5) Enter the password for the user “League123”
- 6) To navigate directory, enter “dir” or “dir /ftp/upload” to review the FTP upload folder

```
Command Prompt
Microsoft Windows [Version 10.0.18363.752]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\E>ftp 192.168.3.10
Connected to 192.168.3.10.
220 "Welcome to Project E's FTP service"
200 Always in UTF8 mode.
User (192.168.3.10:(none)): Garen
331 Please specify the password.
Password:
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 1001  1004    8980 Apr 07 03:26 examples.desktop
dr-xr-x---  3 1001  1004   4096 Apr 09 01:24 ftp
226 Directory send OK.
ftp: 138 bytes received in 0.01Seconds 23.00Kbytes/sec.
ftp> cd ftp
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-x---  2 1001  1004   4096 Apr 09 21:29 upload
226 Directory send OK.
ftp: 67 bytes received in 0.00Seconds 22.33Kbytes/sec.
ftp> cd upload
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--  1 1001  1004    59 Apr 09 21:29 CustomGameFile
-rw-r--r--  1 0     0      59 Apr 09 21:08 TestFile.txt
226 Directory send OK.
```

Figure 1.4 FTP into Localhost

- 7) To download file, type and enter “get CustomGameFile” to retrieve the file into the current user’s directory
 - 8) The FTP setting prevents users to utilize commands such as “sudo,” “chmod” and “mv/cp” to avoid tampering and privilege exploitation
-

2. Vulnerability Management

2.1. OpenVAS Vulnerability Scan

- 1) In any web browser, enter “https://127.0.0.1:9392” to enter the web interface of Greenbone Security Assistant
- 2) Enter your admin credential as set up. In this case “admin” for the user. “2020KaLiRoPa!!” for the password
- 3) On the upper left corner, there is a star button to click “Add a New”
- 4) Fill in the necessary field to be able identify the user’s computer and ensure that the credential matches for an SSH connection. In this case, the Ubu_Srv was enlisted with “admin_user” and the password for “20ThIsThAdPa20!”
- 5) Click “Submit” once finished
- 6) To set the “New Target,” open “Targets” under the Configuration tab
- 7) On the upper left corner, there is a blue icon that says Add a New Target
- 8) Set the host field to 192.168.3.10
- 9) Set the required to port 22 for SSH protocol
- 10) Click “Submit” to continue
- 11) Under the Scan Management tab, choose “Tasks”
- 12) On the right corner, select a white button that indicates “Add a New Scan Task”
- 13) Enter the necessary field of “Name” and “Scan Target”
**Note: User have the option to change the Scan Config to simply Discovery of the target to a Deep Scan of the target’s vulnerability.*
- 14) Locate the listing for the newly created task, click the “play” button to begin
- 15) On the upper right corner, set the page to refresh every 30s to see the targets’ progress
- 16) After the scan finishes, on the right of the selected scans are various button. Among them includes a view button and export. The report of the vulnerability to could be in CSV file or a text file
- 17) Navigate back to the main dashboard to view various severity line

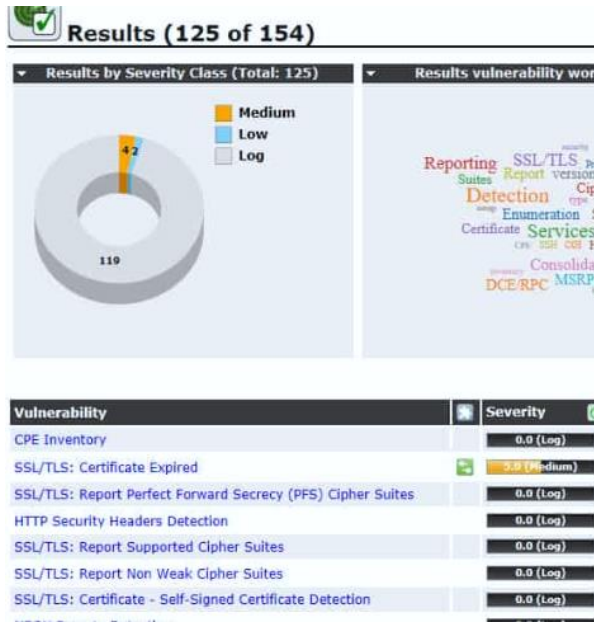


Figure 2.1 OpenVAS Dashboard after Vulnerability Scan

2.2. Pi-hole Management

- 1) Pi-hole DNS functions on the background and as soon as the system boots up.
- 2) Enter the web admin interface with “http://pi.hole/admin” and login with the set credentials. In this case, the username is “admin” and “!LoRaBePiHo20!”
- 3) Navigate to the “Tools” tab on the left navigation panel to confirm live data and functionality of the pi-hole in the background

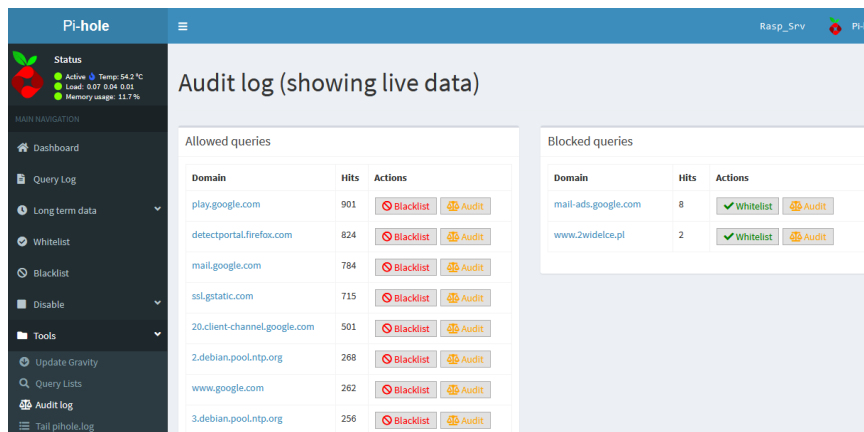


Figure 2.2 Pi-hole Audit Logs

- 4) Navigate to “Settings” on the left panel to set specific blacklist and system configuration settings

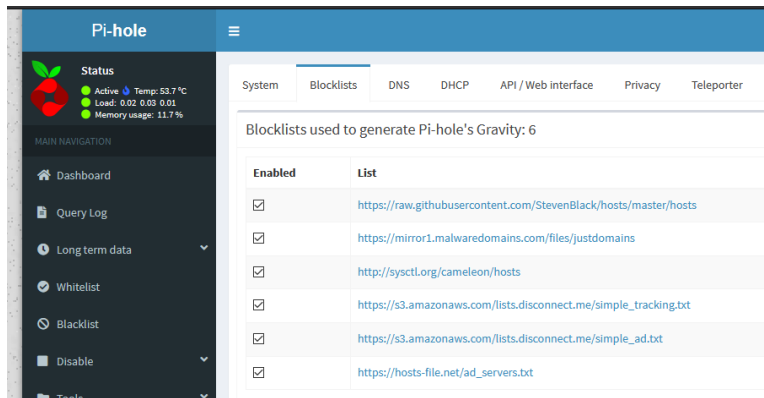


Figure 2.3 Pi-hole Setting

- 5) Blocklist sites are automatically generated by third-party vendor. Devices are able to send network traffic query with DNS relay to the Pi-hole
- 6) Timestamped, status, domain and client can be pinpoint by each queries in the front client end and backend of the servers

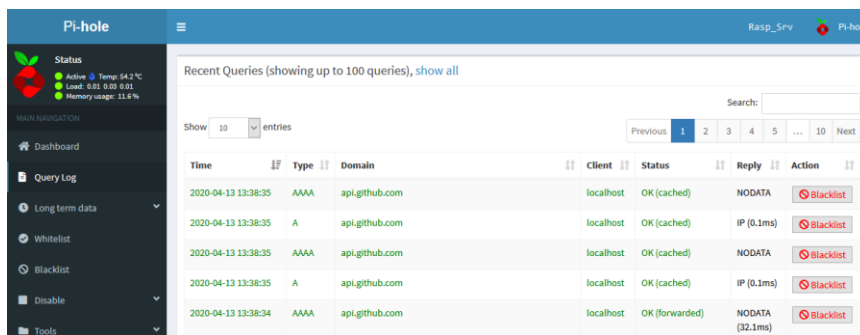


Figure 2.4 Pi-hole Recent Queries

3. Penetration Testing – PC1: Kali Linux USB

3.1. John the Ripper: Password Cracking Software

- 1) John the Ripper utilizes brute-force method to crack password. The process can become extensive in terms of CPU usage and time consumption on resources depending on the complexity of the password
- 2) To test the functionality of the “John” command, the root password has been changed from “2020KaLiRoPa!!” to “123”
- 3) In the terminal, type “sudo passwd root” and press enter
- 4) Enter the new root password “123” twice to confirm
- 5) To start the hash logging and cracking password, navigate to the /etc/ directory with “cd /etc”
- 6) Type and enter “sudo unshadow passwd shadow > /home/kali/Desktop/password.txt.” The feature takes the /etc/passwd user directory file and the encrypted /etc/shadow containing the users’ password and append together in a new file named “password.txt”
- 7) Navigate to the Desktop directory with “cd /home/kali/Desktop”
- 8) Type and enter “sudo john password.txt” to begin loading the hashes, search within wordlists and crack the password

```

kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali:~$ cd /etc
kali@kali:/etc$ sudo unshadow passwd shadow > /home/kali/Desktop/password.txt
kali@kali:/etc$ cd /home/kali/Desktop
kali@kali:~/Desktop$ sudo john password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 10 candidates buffered for the current salt, minimum 32 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 32 needed for performance.
Warning: Only 12 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 20 candidates buffered for the current salt, minimum 32 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123
(root)
1g 0:00:00:00 DONE 2/3 (2020-04-13 21:38) 2.083g/s 3891p/s 3891c/s 3891C/s 123456..random
Use the "--show" option to display all of the cracked passwords reliably
Session completed
kali@kali:~/Desktop$

```

Figure 3.1 John Command with Root Password

3.2. HTML Exploitation

- 1) In Kali linux, click on the top left corner to open the menu to “Applications”
- 2) Type and enter “Wireshark” to launch the packet analyzer.

- 3) At the upper left corner, click the shark fin icon to “Start” the listening and recording process of packet of files traversing in the current system
- 4) Click on the top left corner to open the menu to “Applications”
- 5) Open any web browser of choice and enter “http://192.168.3.20:80”
- 6) Once the web loads, a prompt will appear asking for credentials for the “restricted content”
- 7) Enter any user’s credentials. In this case user “Garen” and the password “League123” is entered
- 8) The main “Front.html” page will load normally
- 9) Return to the Wireshark application, and click the red button to “Stop” the recording packets
- 10) On the filter address bar, type in “ip.addr == 192.168.3.20 && tcp.port == 80” and press enter
- 11) Locate the entry with “GET / favicon.ico HTTP/1.1>” In this case, frame 491 was examined

Protocol	Length	Info
TCP	1514	http(80) -> 36768 [ACK] Seq=35932 Ack=660 Win=34816 Len=1448 TSval=1944114 TSecr=532819584 [T...
TCP	66	36768 -> http(80) [ACK] Seq=660 Ack=37380 Win=90240 Len=0 TSval=532819592 TSecr=1944114
TCP	1514	http(80) -> 36768 [ACK] Seq=37380 Ack=660 Win=34816 Len=1448 TSval=1944114 TSecr=532819584 [T...
TCP	66	36768 -> http(80) [ACK] Seq=660 Ack=38828 Win=93056 Len=0 TSval=532819592 TSecr=1944114
HTTP	480	HTTP/1.1 200 OK (JPEG JFIF image)
TCP	66	36768 -> http(80) [ACK] Seq=660 Ack=39242 Win=96000 Len=0 TSval=532819592 TSecr=1944114
HTTP	361	GET /favicon.ico HTTP/1.1
HTTP	560	HTTP/1.1 404 Not Found (text/html)
TCP	66	36768 -> http(80) [ACK] Seq=955 Ack=39736 Win=98944 Len=0 TSval=532819823 TSecr=1944137
TCP	66	http(80) -> 36770 [FIN, ACK] Seq=951 Ack=312 Win=31872 Len=0 TSval=1944587 TSecr=532819568
TCP	66	http(80) -> 36766 [FIN, ACK] Seq=15208 Ack=684 Win=34816 Len=0 TSval=1944587 TSecr=532819569

Figure 4.2 GET HTTP 1.1 Frame

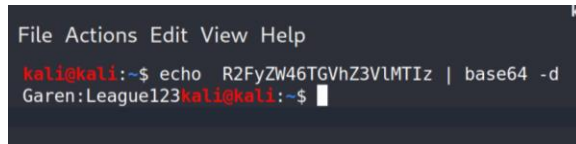
- 12) Navigate to the “HyperText Transfer Protocol” and expand the section
- 13) Locate the line “Authorization: Basic....”
- 14) Copy the encoded line that followed “Authorization: Basic”

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
<User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0>
Accept: image/webp,*/*\r\n
<Accept: image/webp,*/*\r\n>
Accept-Language: en-US,en;q=0.5\r\n
<Accept-Language: en-US,en;q=0.5\r\n>
Accept-Encoding: gzip, deflate\r\n
<Accept-Encoding: gzip, deflate\r\n>
DNT: 1\r\n
Authorization: Basic R2FyZW46TGZhZ3VlMTIz\r\n
<Authorization: Basic R2FyZW46TGZhZ3VlMTIz\r\n>
Connection: keep-alive\r\n
<Connection: keep-alive\r\n>
\r\n
```

Figure 3.3 Authorization Basic Line

- 15) Launch the Terminal Emulator

- 16) Type and enter “echo R2FyZW45TGZhZ3VlMTIz | base64 -d” in the terminal

A terminal window with a dark background. The menu bar at the top shows 'File Actions Edit View Help'. The prompt is 'kali@kali:~\$'. The command entered is 'echo R2FyZW46TGZhZ3VlMTIz | base64 -d'. The output is 'Garen:League123kali@kali:~\$'.

```
File Actions Edit View Help
kali@kali:~$ echo R2FyZW46TGZhZ3VlMTIz | base64 -d
Garen:League123kali@kali:~$
```

Figure 3.4 Decoding Base64

- 17) Although basic_auth does not use session managements, login windows or cookies that are vulnerable to SQL injections and session exploitation, the feature encode users' credentials in Base64 that is obtainable by any user listening into the network packet traffic
-

4. Network Connectivity – Diagnosis

4.1. End Users and Equipment Connectivity

All show commands and the following commands can be entered in the Privileged Exec Commands denoted by “#” which can be entered into with “enable.” Pinging and using Traceroute are the two methods to confirm the connectivity of devices and the directions of each packet through the topology. Pinging is the process of sending Internet Control Message Protocol (ICMP) echo to the listed end device and expect an “echo” in return. Apart from inspecting the actual physical equipment for any unplugged wires or damaged equipment, the recommended troubleshooting technique is to inspect from bottom-up, starting with the malfunctioning end device to all the way up to the routing protocols

- 1) Ping and or use Traceroute to ping neighboring end devices such as between PC1 and PC2 to assess the VLAN implementation, including the switchport trunk, and Switch S1 proper functionality
 - a. **PC1#** ping 192.168.1.10
 - b. **PC2#** traceroute 192.168.1.5
- 2) Tracing the step to the default gateway is a step to ensure that VLAN have been assigned the correct configuration in respect to their device’s VLAN. As both PC1 and PC2 are part of the same VLAN, both should be able to ping their default gateway. Similarly, both servers should be able to ping each other and the default gateway as both devices share in VLAN 30 – Server
 - a. **PC1#** traceroute 192.168.1.1
 - b. **Rasp_Srv#** traceroute 192.168.3.1
- 3) To ensure the connectivity of the topology and that all VLANs implemented correctly, the devices should be able to ping between routers and switches. Traceroute can monitor the hops each packet takes to arrive to destination. The logical and priority assignment designate that PC1 will hop to S1 before utilizing the EtherChannel to get to MLS1 before sending the packet to the Ubu_Srv (192.168.3.10/24).
 - a. **PC1#** traceroute 192.168.3.10

4.2. Interface Details

Interfaces diagnosis are crucial to identifying which VLAN each logical port is connected to and what is the function of each interface. VLAN implementation separates the interfaces logically and virtually. Ensuring the VLAN are designated correctly to each port is the first step to the bottom to up diagnosis approach. VLAN trunking are also crucial to permit the various virtual and logical traffic with a specific VLAN to be permitted and separated

- 1) To have an overview of all the VLAN available, which interface belongs to which VLAN and even if the interface appears to be assigned to a VLAN, enter the following:
 - a. **MLS1# Show Vlan Brief**
 - b. **MLS1# Show Interface Switchport**
- 2) Each interface has the physical statistics the input and output traffic and the logical assignment the interface was given. Interface will show the status of the interface signifying whether it is administratively down, or another configuration is conflicting. Ensure the status of each assigned VLAN and connection links
 - a. **MLS1# Show IP Interface**
 - b. **MLS1# Show Interface trunk**
 - c. **MLS1# Show Interface Port-Channel 1 switchport**

4.3. Routing Protocols

Routing protocols are not heavily relied on the given topology as the Cable Modem does not accept the routing protocols given, and both Layer 3 devices are not connected to each other to redistribute between OSPF and EIGRP routing protocols. However, if they routing protocols are configured correct in each respective device, both devices can scalable to another router to be connected to each device bearing the same routing protocols. The topology is designed with redundancy that should R1 fail, PC1 and PC2 can still use the EtherChannel connected to the MLS1 to the outside network

- 1) To review the EtherChannel connection along with FHRP priority, enter the following the command. The command will allow the user to ensure the “Active” state, along with hello packets being sent
 - a. **MLS1#** show standby
- 2) As OSPF is indicated by O, EIGRP is indicated by an E in the overall routing topology. However, with the circumstances, each router does not have neighboring routers to share the same routing protocols. This feature will be available if and when the admin adds another routing device as a scalability feature. A static routing protocol had been added as a wild card to be able to direct any traffic out with the symbol of S*
 - a. **MLS1#** Show IP Route
 - b. **R1#** Show IP Traffic
- 3) Respectively, each routing protocols allows the users to monitor for statistic and review configuration accordingly. Viewing the OSPF neighbor, the command will show the state to be “FULL/BDR” identifying the neighboring ID with the interface. In this case, however, there are no other neighboring area, so the routing list will only include a “C” for direct connection
 - a. **MLS1#** Show IP OSPF neighbor
 - b. **MLS1#** Show IP OSPF database
 - c. **R1#** Show EIGRP topology
 - d. **R1#** Show EIGRP traffic
- 4) ACLs implementation has an implicit deny all as the first ACLs rule is entered in. Routing will check ACLs rules in order by number. In this case, Extended IP access list are applied with access-list from 5 to 30. The following show commands:
 - a. **MLS1#** Show IP Access-lists
 - b. **R1#** Show IP Access-lists *access-list-number*

CIS: Senior Project

2440:491-001

Weekly Project Journals

Ethelyn Tran
Part VI of VII

1. Weekly Report: February 3rd – February 9th

Summary

Date	Start Time	End Time	Description	Total Hours
2/05/2020	14:00	16:00	Start Documentation; Install/Update of Operating Systems (OS)	2
2/07/2020	10:00	12:00	Install/Update of OS; Test End Device	3
			Total Hours This Week	5
			Total Hours to Date	5

Journal Details

2/05/2020

- Documentation Binder:
 - Purchased of binder, creation of cover page, added Table of Contents
- Operating Systems Updates:
 - Microsoft Surface Pro: Windows 10
 - USB SanDisk 16GB: Kali Linux Persistent

2/07/2020

- Tested End Devices & Continuation of Operating Systems (OS) Updates:
 - Dell Inspiron Laptop for USB Persistent Kali Linux died during testing***
 - Replaced with another laptop: Toshiba R845-S80 laptop
 - Oracle VM VirtualBox update
 - Implementation of Ubuntu Desktop to include Graphic User Interface
 - Raspberry Pi 3 Model B testing
 - Raspbian OS implementation

2/09/2020

- Purchased the Cisco router, multilayer switch and switch with POE from a friend with all the necessary cablings

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

2. Weekly Report: February 10th – February 16th

Summary

Date	Start Time	End Time	Description	Total Hours
2/10/2020	12:00	15:00	Completed	3
2/12/2020	12:00	14:00	Tested Cisco lab equipment	2
			Total Hours This Week	5
			Total Hours to Date	10

Journal Details

2/10/2020

- Researched, installed and explored Raspbian OS on Raspberry Pi 3
- Completed USB Kali Linux Persistent drive
- Installed Wireshark
- Researched Apache Server – NGINX
- Updated Ubuntu Server and added users for testing

2/12/2020

- Tested each Cisco equipment (Cisco 2811, Cisco MLS 3560 and Cisco 3560x) and all the cabling
- Reset each Cisco equipment to default configuration

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

3. Weekly Report: February 17th – February 23rd

Summary

Date	Start Time	End Time	Description	Total Hours
2/18/2020	12:00	17:00	Pi-Hole and Apache Server researching, implementation & testing	5
2/20/2020	10:00	16:00	VSFTPD research & implementation; Documentation Update	6
			Total Hours This Week	11
			Total Hours to Date	21

Journal Details

2/18/2020

- Wrapped up Cisco equipment to reset to default configurations
- Researched and completed installation on Pi-Hole on Raspbian OS
- Performed initial testing of Pi-Hole's various capability
- Researched Apache Server integrations and began implementation into Raspbian OS

2/20/2020

- Troubleshoot Apache Server integration into Raspbian OS to allow local access and prep for remote access
- Researched and began installation of VSFTPD
- Intermission: organized documentation to ensure detailed and consistent formatting

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

4. Weekly Report: February 24th – March 1st

Summary

Date	Start Time	End Time	Description	Total Hours
2/25/2020	15:00	18:00	Finish up VSFTPD & start the design of web interface	3
2/27/2020	12:00	19:00	Continue Web interface design & research of access authentication	7
2/28/2020	09:00	14:00	Troubleshoot Apache server and integration of authentication	5
			Total Hours This Week	15
			Total Hours to Date	36

Journal Details

2/25/2020

- Completed installation of VSFTPD and creation of sample files
- Began design of web interface

2/27/2020

- Continue design of web interface
- Research implementation of a web server's basic access authentication
- Design and implementation of a basic access authentication
- Troubleshoot Apache server and authentication process

2/28/2020

- Intermission: documentation updates
- Continue troubleshooting authentication process
- Research how to integrate VSFTPD and Apache Server

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

5. Weekly Report: March 2nd – March 8th

Summary

Date	Start Time	End Time	Description	Total Hours
3/03/2020	15:00	18:00	Update documentation; implement authentication process	3
3/05/2020	15:00	21:00	Finish authentication process; research integration between server	6
3/06/2020	09:00	15:00	Fill in small details; adjust documentation for consistency; setup L2 connections	6
			Total Hours This Week	15
			Total Hours to Date	51

Journal Details

3/03/2020

- Caught up on documentation details and updates
- Implemented basic access authentication

3/05/2020

- Finished the implementation of basic access authentication
- Filled in users' basic information and privilege level
- Researched integration of VSFTPD in between servers

3/06/2020

- Filled in details within the FTP server
- Adjusted documentation for consistency
- Connected physical connection within Layer 2 and including L3 Multilayer Switch

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

6. Weekly Report: March 16th – March 22nd

Summary

Date	Start Time	End Time	Description	Total Hours
3/8-15/2020			Progress had to be reset due to unforeseen circumstances	11
3/17/2020	0:00	9:00	Updated documentation; implemented L2 devices' configuration and security practices	9
3/18/2020	0:00	7:00	Finished VLAN implementations; applied and troubleshoot L3 routing protocols	7
3/21/2020	7:00	3:00	Configured ACLs and IPsec tunneling; updated documentations	6
			Total Hours This Week	33
			Total Hours to Date	84

Journal Details

3/15/2020

- During the week, sporadic power outages and internet connectivity disruption kept either resetting unsaved progress or corrupting files. Reset L2 and L3 equipment for a clean reconfiguration. Troubleshoot for corrupted files and data loss

3/17/2020

- Experienced internet speed at 10-20mbps sporadically***
- Completed physical connections between L2 and L3, except to the ISP modem router
- Implemented HSRP and FHRP within L2
- Researched and configured best security practice for L2 and VLAN security
- Redo and organized documentation to reflect a cohesive procedure

3/18/2020

- Completed VLAN implementation for L3 for MLS and R1 including best practices
- Configured OSPF and EIGRP within L3 devices
- Troubleshoot OSPF and EIGRP such as connectivity issues and zone issues
- Implement best security practices and ACLs

3/21/2020

- Experienced a power outage***
- Diagnosed configurations within Cisco equipment and online servers
 - Configurations and changes appear intact for the most part after diagnosis
- Troubleshoot connectivity issues with ACLs
- Research and created IPsec Tunneling
- Added steps into the documentation

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

7. Weekly Report: March 23rd – March 29th

Summary

Date	Start Time	End Time	Description	Total Hours
3/23/2020	8:00	4:00	Updated documentation; troubleshoot routing protocols; redo ACLs	6
3/24/2020	12:00	4:00	Troubleshoot IPsec Tunneling; performed routine maintenance and documentation updates	4
			Total Hours This Week	10
			Total Hours to Date	94

Journal Details

3/23/2020

- Intermission: Documentation Updates
- Reconfigured OSPF and EIGRP connectivity issues
- Research on Best Practices with ACLs
- Redo and tested ACLs to reflect changes

3/24/2020

- Intermission: Document Updates
- Research and troubleshoot IPsec Tunneling
- Performed routine updates on Kali Linux OS, Ubuntu OS, Windows 10 OS

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

8. Weekly Report: March 30th – April 5th

Summary

Date	Start Time	End Time	Description	Total Hours
3/31/2020	12:00	15:00	Troubleshoot the remaining network issue; documentation updates	3
4/02/2020	12:00	19:00	Researched and performed scans and runs with tools available	7
4/04/2020	8:00	11:00	Performed a scan and documentation updates	3
			Total Hours This Week	13
			Total Hours to Date	107

Journal Details

3/31/2020

- Troubleshoot IPsec tunneling
- Tested network traffic between routing protocols
- Documentation Updates

4/02/2020

- Installed OpenVAS and performed a vulnerability scan
- Researched and performed a run with John the Ripper software
- Researched DDoS tools available
- Document Updates

4/04/2020

- Installed Nmap feature and performed network mapping
- Documentation Updates

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

9. Weekly Report: April 6th – April 12th

Summary

Date	Start Time	End Time	Description	Total Hours
04/07/2020	12:00	17:00	Tested network equipment; project analysis updates	5
04/09/2020	9:00	11:00	Tested server functionalities; documentation updates	4
04/11/2020	12:00	17:00	Finalized documentation; draft presentation	5
			Total Hours This Week	14
			Total Hours to Date	121

Journal Details

04/07/2020

- Tested network equipment functionalities
- Testing Documentation and Reference update
- Project Analysis overview and update

04/09/2020

- Tested server functionalities
- Testing Documentation updates

04/11/2020

- Draft Presentation PowerPoint
- Documentation finalization and binder organization

Team Meetings

Date	Start Time	End Time	Description	Total Hours
N/A	N/A	N/A	N/A	0
			Total Hours	0

10. Estimation of Time**Project Proposal – Time Estimates (In Hours):**

Estimated Times:

Research	Design	Installation	Configuration	Testing	Documentation	Total
40	10	20	30	20	50	170

Actual Time Estimates (In Hours):

Actual Times:

Research	Design	Installation	Configuration	Testing	Documentation	Total
17	10	12	33	24	25	121

CIS: Senior Project

2440:491-001

Research References

Ethelyn Tran
Part VII of VII

References

- Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham: Elsevier Inc.
- Batard, P. (2020, February 29). *Create Bootable USB Drives the Easy Way*. Retrieved from Rufus: <https://rufus.ie/>
- Canonical Ltd. (2018, April 26th). *Download Ubuntu Desktop*. Retrieved from Ubuntu: <https://ubuntu.com/download/desktop>
- Cezar, M. (2018, April 20). *How to Synchronize Time with NTP in Linux*. Retrieved from TecMint: <https://www.tecmint.com/synchronize-time-with-ntp-in-linux/>
- Charles, K. (2020, February 14). *Setting up the root account on Kali 2020* . Retrieved from Security Boulevard: <https://securityboulevard.com/2020/02/setting-up-the-root-account-on-kali-2020/>
- dookie. (2017, November 15). *Configuring and Tuning OpenVAS in Kali Linux*. Retrieved from Kali by Offensive Security: <https://www.kali.org/tutorials/configuring-and-tuning-openvas-in-kali-linux/>
- Froom, R., & Frahim, E. (2015). *Implementing Cisco IP Switch Networks (SWITCH) Foundation Learning Guide*. Indianapolis: Cisco Press.
- g0tmi1k. (2020, February 22). *Adding Persistence to a Kali Linux "Live" USB Drive*. Retrieved from Kali: <https://www.kali.org/docs/usb/kali-linux-live-usb-persistence/>
- Greenbone Networks GmbH. (2020). *openvas Package Description*. Retrieved from Kali Tools: <https://tools.kali.org/vulnerability-analysis/openvas>
- Hughes, J. (2020, March 12). *Setting up an Apache Web Server on a Raspberry Pi*. Retrieved from Raspberry Pi: <https://www.raspberrypi.org/documentation/remote-access/web-server/apache.md>
- Infrabot, A. (2019, May 22). *PasswordBasicAuth*. Retrieved from Confluence Apache: <https://cwiki.apache.org/confluence/display/httpd/PasswordBasicAuth>

- Linuxize. (2019, March 19). *How to Setup FTP Server with VSFTPD on Ubuntu 18.04*. Retrieved from Linuxize: <https://linuxize.com/post/how-to-setup-ftp-server-with-vsftpd-on-ubuntu-18-04/>
- Microsoft Corporation. (2017, May 02). *Disabling Secure Boot*. Retrieved from Microsoft Docs: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/disabling-secure-boot>
- MiniTool. (2020). *MiniTool Partition Wizard Free 12*. Retrieved from Partition Wizard: <https://www.partitionwizard.com/free-partition-manager.html>
- Offensive Security. (2020, January 28). *Kali Linux Downloads*. Retrieved from Kali by Offensive Security: <https://www.kali.org/downloads/>
- Oracle Corporation. (2020, February 19). *Download VirtualBox*. Retrieved from Virtual Box: <https://www.virtualbox.org/wiki/Downloads>
- Pi-Hole. (2019, May 18). *Pi-hole: Network-wide Ad Blocking*. Retrieved from Pi-hole: <https://pi-hole.net/>
- Raspberry Pi Foundation. (2020, February 13). *Raspbian*. Retrieved from Raspberry Pi: <https://www.raspberrypi.org/downloads/raspbian/>
- Simpson, M., Backman, K., & Corley, J. (2017). *Hands-On Ethical Hacking and Network Defense*. Boston: Cengage Learning.
- Soyinka, W. (2016). *Linux Administration: A Beginner's Guide*. New York: McGraw-Hill Education.
- Teare, D., Vachon, B., & Graziani, R. (2015). *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide*. Indianapolis: Cisco Press.
- W3 Resources. (2020, February 26). *User management*. Retrieved from W3Resources: <https://www.w3resource.com/linux-system-administration/user-management.php>
- XECDesign. (2020, February 14). *NOOBS*. Retrieved from Raspberry Pi: <https://www.raspberrypi.org/documentation/installation/noobs.md>