

**Name:** Scott Moskal

**Week:** One (1/31 – 2/4)

Day of the week	Start time	End Time	Description	Total Hours
Monday (1/31)	12:30 PM	2:30 PM	Honors Signatures	2 Hours
Tuesday (2/1)	1:30 PM	2:30 PM	Received Signature	1 Hour
Wednesday (2/2)	2:30 PM	5:30 PM	Wireless Setup	3 Hours
Thursday (2/3)	2:30 PM	12:00 AM	Basic Network Configurations	9.5 Hours
Friday (2/4)	2:00 PM	5:00 PM	Switch Configuration	3 Hours
				Weekly Total: 18.5 Hours

**Details by Day:**

**Monday:**

- Received permission to use Project Proposal for Honors Proposal
- Began asking for signatures from four readers

**Tuesday:**

- Received first signature for Honors Project, Sponsor

**Wednesday:**

- Configured the wireless section of the network
  - o Set the IP address for the wireless network to 10.1.1.0/29
  - o Set the router IP to 10.1.1.1
  - o Set the IP for the WAN port of the router to 172.16.1.2
  - o Connected both the Acer Laptop and the HP laptop to the network

- Changed the default username and password

## **Thursday:**

- Set up both Ubiquiti routers
  - Changed the default passwords, as usernames cannot be changed for admin accounts
  - Followed basic setup instructions to give each port an IP address
  - Both routers were given IP addresses for all three ports, two for connectivity and one for management
  - Established two networks between the devices, 172.16.1.0/30 for communication between the wireless router and router 1, and 172.16.3.0/30 for communication between Router 1 and Router 2
    - Router 1 eth1: 172.16.1.1/30
    - Router 1 eth2: 172.16.3.1/30
    - Router 2 eth1: 172.16.3.2/30
    - Router 2 eth0: 192.168.1.1/29
  - Firewall rules were created by default when setting up the networks on the routers.
  - Adjusted the firewall rules to allow traffic through the devices rather than drop traffic.
  - Added static routes to each router for communication
    - Router 1 used both Router 2 and the Wireless router for access to each network

- Router 2 used Router 1 for a next hop to all networks with no direct connection
- Set VLAN 10 and VLAN 20 on Router 2 to port eth0
  - Eth0.10: 192.168.10.1/29
  - Eth0.20: 192.168.20.1/29
- Troubleshoot connectivity issues between devices

## **Friday**

- Configured the Netgear switch
  - Changed the default password
  - Set the static route to 192.168.1.2 for management
  - Set eth1 to VLAN 10
  - Set eth2 to VLAN 20
  - Set eth5 to be the trunk port
- Configured the Beelink Desktop to run on VLAN 10 with an IP address of 192.168.10.3/29
- Verified communication between devices on the VLAN.

**Name:** Scott Moskal

**Week:** Two (2/7 - 2/11)

Day of the week	Start time	End Time	Description	Total Hours
Tuesday	2:00 PM	10: 00 PM	General failure of installation	8 Hours
Wednesday	12:00 PM	5:00 PM	Installation of OS and firmware	5 Hours
Thursday	11:00 AM	12:00 PM	Configure FTP Server on OpenMediaVault	1 Hour
Friday	8:00 PM	8:30 PM	File creation for Acer FTP client	30 minutes
				Total: 14.5 Hours

**Details by Day:**

**Tuesday**

- Attempted installation of FileZilla FTP Client on BeeLink Desktop
- Attempted installation of vsftpd server on BeeLink Desktop
- Removal of defective FTP servers and all related packages
- Installation of Wine on the BeeLink Desktop
- Attempted installation of FileZilla FTP Server for Windows
- Genral failure to configure the FTP server over Wine
- Failure to install OpenMediaVault on the Raspberry Pi with the initial configuration
- Installation of FileZilla Client of the Acer Laptop

**Wednesday**

- Procurement of a MicroSD card reader
- Installation of Raspian OS Lite onto the Raspberry Pi

- Installation of OpenMediaVault over the Raspian OS Lite operating system
- Changing of the administrator password for strength

### **Thursday**

- Activation of the FTP server system built into OpenMediaVault
- Creation of users dedicated to each approved user of the server
  - o Creation of the Acer user for access from the Acer Laptop
  - o Creation of the BeeLink user for access from the BeeLink Desktop
- Creation of a new file system for the shared folders using a SanDisk Ultra 32 GB USB drive
- Creation of folders for each user
  - o FTP files for Acer for the Acer Laptop
  - o FTP files for BeeLink for the BeeLink Desktop
- Adjusting of permissions for each user as desired for each folder
  - o Read/Write access for Acer, Read access for BeeLink on FTP files for Acer
  - o Read/Write access for BeeLink, Read access for Acer on FTP files for BeeLink
- Successful testing of connection using FileZilla Client on the Acer Laptop
- Received two of the necessary four signatures for the Honors Proposal
- Received permission from four readers of the Honors project

### **Friday**

- Creation of files for storage on the FTP client for the Acer Laptop
  - o Creation of a document, presentation, and spreadsheet
- Set a password for the spreadsheet file saved in the FTP client for the Acer Laptop

**Name:** Scott Moskal

**Week:** Three (2/14 – 2/19)

Day of the week	Start time	End Time	Description	Total Hours
Monday	10:00 AM	11:00 AM	Submitted Honors Proposal	1 Hour
Wednesday	5:00 PM	8:00 PM	Connection Troubleshootings	3 Hours
Thursday	6:00 PM	10:00 PM	Connection Troubleshootings	4 Hours
Saturday	2:00 PM	9:00 PM	New network devices and full connectivity	7 Hours
				Total: 14 Hours

**Details by Day:**

**Monday:**

- Submitted Honors Proposal documents with all signatures prepared

**Wednesday:**

- Attempted to reform ping issues from wired side of the network (VLANs, switch, and routers) to the wireless side
  - o Adjusted firewall rules to allow ICMP traffic through on port 1
  - o Adjusted the routing table for more access on the wireless LAN
- Procured a new wireless router to replace the persistent issues with the old one
- Experienced the same issues and attempted to troubleshoot ping issues
- Failed to resolve issues
- Readjusted the scope of the project, turning the wireless router into a wireless access point connected to a physical router

## **Thursday**

- Procurement of a physical router
- Configured basic networking specifications similar to the original router used (same IP addresses, same routing table, same static routes)
- Similar issues related to those mentioned above (issues were uniform across TP-Link routers)

## **Saturday**

- Procurement of different physical router, a third Ubiquiti Edgerouter Lite, from the same source as the first two
- Configured with basic network parameters, as mentioned above
- Adjusted firewall rules to allow ping traffic to pass through
- Created a DHCP server to statically assign an IP address based on the MAC address of a device, as defined by the address pool
  - o 10.1.1.2 for the Acer Laptop
  - o 10.1.1.5 for the HP laptop
  - o 10.1.1.6 for the wireless access point
- Reconfigured the new wireless router for AP management
- Created new usernames and passwords for each device, using a mix of both characters and numbers (for security reasons, the exact passwords will not be mentioned)

## Equipment Change

- Old equipment
  - TP-Link TL-WR841N
- New Equipment
  - Ubiquiti Edgerouter Lite (used as the router)
  - TP-Link TL-WR940N
- Extra peripheral equipment not mentioned in proposal
  - Sandisk Ultra 32GB flash drive (for use on the Raspberry Pi server as a file system)
  - MicroSD card reader (for installing Raspian OS onto the MircoSD card the Raspberry Pi uses)



**Name:** Scott Moskal

**Week:** Four (2/21 – 2/26)

Day of the week	Start time	End Time	Description	Total Hours
Monday	12:00 PM	5:00 PM	Execution of pentesting	5 Hours
Tuesday	11:00 AM	5:00 PM	Finishing pentests and exploits	6 Hours
Thursday	3:00 PM	5:00 PM	Screenshots for proof	2 Hours
				<b>Total: 13 Hours</b>

**Details by Day:**

**Monday:**

- Began series of pentests on the network with nmap
  - o Executed nmap to discovering devices on the wireless network
  - o Executed nmap to identify open ports on the devices present on the wireless network
  - o Executed nmap on both VLANS to discover devices and open ports on each identified device
- Performed a network analysis with Wireshark
  - o Connected the Acer laptop to the FTP server
  - o Captured unencrypted traffic of login using Wireshark, displaying the username and password
  - o Captured encrypted traffic of login attempts to the wireless access point and the router connected to the wireless network
- Began performing OpenVAS vulnerability scan on both VLANS

- Moved the scans to the BeeLink desktop due to installation issues on the HP laptop
- Installed OpenVAS on the BeeLink desktop on Kali Linux
- Initiated a scan on VLAN 10 and recorded the results
- Initiated a scan on VLAN 20 and recorded the results

## **Tuesday**

- Initiated a scan on the wireless network and recorded the results
- Began an attack on the FTP server using Metasploit
  - Specified the parameters that Metasploit would use, including the scanning tool, the text file for usernames, and the text file for passwords
  - Failed to login with the tool
  - Failed to login with several subsequent attempts, each using a different password list
- Began an attack using Aircrack-ng
  - Scanned the network to discover the wireless access point on the network
  - Captured a handshake initiated between AP and a device attempting to connect to it
  - Used the captured handshake in conjunction with the password file saved in Kali Linux to attempt a crack
  - Failed to discover the encryption key using Aircrack-ng
- Began a man-in-the-middle attack using bettercap

- Specified the gateway to be used in the attack and the victim of the attack being the Acer Laptop
- Successfully changed the MAC address of the HP laptop to be the same as the default gateway of the network
- Successfully captured traffic for every attempt the Acer Laptop attempted to communicate with the network

## **Thursday**

- Initiated ping tests for all end devices to ping all other devices within the network for screenshots
  - Successfully pinged all devices in communication with the HP Laptop
  - Successfully pinged all devices in communication with the Acer Laptop
  - Successfully pinged all devices in communication with the BeeLink Desktop
  - Successfully pinged all devices in communication with the Raspberry Pi
  - Took screenshots of all successful tests for the testing documentation

**Name:** Scott Moskal

**Week:** Five (2/28 – 3/04)

Day of the week	Start time	End Time	Description	Total Hours
Wednesday	2:00 PM	8:00 PM	Begin Documentation	6 Hours
Thursday	2:00 PM	5:00 PM	Continue Documentation	3 Hours
Friday	12:00 PM	1:00 PM	Continue Documentation	1 Hour
				<b>Total: 10 Hours</b>

**Details by Day:**

**Wednesday**

- Began writing the Project Description
  - o Included title page and introduction to the project, including all necessary information as laid out within the project proposal.
  - o Updated the topology to reflect changes made since submission of the proposal.
  - o Began writing on network configurations for the routers.

**Thursday**

- Continued writing the Project Description
  - o Configuration of Router 0 completed
  - o Configuration of the TP-Link Access Point completed

**Friday**

- Continued writing the Project Description
  - o Configuration of Router 1 completed
  - o Configuration of Router 2 completed
  - o Configuration of the Switch completed
  - o Completion of physical connections made between devices.

**Miscellaneous changes and updates not mentioned previously**

- The Switch must have its own IP address for proper connection and communication
- The VLAN ports on the switch cannot be given IP addresses. Rather, the ports can only have a VLAN ID attached. Therefore, the IP scheme will have minor updates.
- Due to connectivity issues, the laptops and TP-Link Access Point will have their addresses assigned using a static DHCP address, rather than being manually entered.

**Name:** Scott Moskal

**Week:** Six (3/7 – 3/11)

Day of the week	Start time	End Time	Description	Total Hours
Wednesday	2:00 PM	6:00 PM	Documentation	4 Hours
Thursday	10:00 PM	2:00 PM	Documentation	4 Hours
Friday	2:30 PM	6:00 PM	Documentation	3.5 Hours
				<b>Total: 11.5 Hours</b>

**Details by Day:**

**Wednesday**

- Continued writing documentation, focusing on the end devices on the network.
  - o Finished writing the configuration of the Acer Laptop.
  - o Finished writing the configuration of the HP Laptop.
  - o Finished writing the configuration of the BeeLink Desktop.
  - o Began writing the configuration of the Raspberry Pi.

**Thursday**

- Continued writing documentation, focusing on the pentesting of the network.
  - o Finished writing the configuration of the Raspberry Pi.
  - o Finished documentation on how to use nmap.
  - o Finished documentation on how to use Wireshark.
  - o Began documentation on how to use OpenVAS.

**Friday**

- Continued writing documentation, focusing on the exploits used against the network.

- Finished documentation on how to use OpenVAS.
- Finished documentation on how to use Metasploit.
- Finished documentation on how to use Aircrack-ng.
- Finished documentation on how to use bettercap.

**Name:** Scott Moskal

**Week:** Seven (3/14 – 3/18)

Day of the week	Start time	End Time	Description	Total Hours
Monday	6:00 PM	10:00 PM	Documentation	4 Hours
Tuesday	10:00 AM	4:00 PM	Documentation	6 Hours
Wednesday	12:00 PM	2:00 PM	Documentation	2 Hours
Thursday	2:00 PM	5:00 PM	Documentation	3 Hours
				<b>Total: 15 Hours</b>

**Details by Day:**

**Monday**

- Continued writing project description.
  - o Finished documentation regarding security measures made for the network.
  - o Documented fixes for every vulnerability found by OpenVAS.
  - o Began documentation on the Appendix.

**Tuesday**

- Continued documentation on Project Description, Project Analysis, and Testing Documentation.
  - o Finished documentation in the Appendix, including installation instructions for software on different operating systems and supplemental instructions for setting and finding IP schemes.
  - o Began Testing Documentation.
  - o Finished verifying network connections in the Testing Documentation.
  - o Began documentation on the Project Analysis on device configuration.



## **Wednesday**

- Continued documentation on Project Analysis and Testing Documentation
  - Explained the methodologies behind the penetration tests and the exploits in the Project Analysis.
  - Explained problems and solutions in the Project Analysis.
  - Began explaining the routing tables in the Testing Documentation.

## **Thursday**

- Continued documentation for Testing Documentation and Project Description
  - Began adding pictures to the Testing Documentation and Project Description.

**Name:** Scott Moskal

**Week:** Eight (3/28 – 4/3)

Day of the week	Start time	End Time	Description	Total Hours
Tuesday	7:00 PM	9:00 PM	Documentation	2 Hours
Wednesday	7:00 PM	9:00 PM	Documentation	2 Hours
Thursday	7:00 PM	9:00 PM	Documentation	2 Hours
Friday	7:00 PM	9:00 PM	Documentation	2 Hours
Saturday	7:00 PM	9:00 PM	Documentation	2 Hours
Sunday	7:00 PM	9:00 PM	Documentation	2 Hours
				<b>Total: 12 Hours</b>

**Details by Day:**

**Tuesday**

- Continued putting images into all documentation

**Wednesday**

- Began work on PowerPoint Presentation
- Finished the first ten slides
- Included general setup of all devices
- Included finished topology and IP scheme table

**Thursday**

- Finished all slides with no video content
- Included penetration testing tools
- Included exploits attempted against the network
- Included all problems experienced and the fixes to solve them

**Friday**

- Included video and photographic proof of project

### **Saturday**

- Performed extra work to ensure quality in all documentation

### **Sunday**

- Finished looking over all documentation
- Submitted all work for grading