## August 2024 Hackbright Capstone Project

### Week 1: Investigation Phase

During the investigation phase I spent time thinking about what project I wanted to tackle for the capstone project. I spent time weighing out the pro’s and con’s for each of the main starter ideas listed on the project start page. Throughout class sessions this week I watched over a few YouTube videos to get some additional ideas and information on relevant technical topics. I eventually settled upon two different projects for the capstone which was discussed in detail in my AUG. 2024 Capstone Planning document. Essentially one project proposal was to create a fictional company where I could create a virtual network myself and design improvements to the network and attempt some security modifications. With this project I would complete the setup of the network, organize the layout of the network (displayed with a topography map), implement firewall settings, implement automated updates, use an IDS, implement secure user settings, and essentially audit the network for security. The second project selection was to simply program an application that would help with file integrity monitoring using PowerShell and some sort of hashing algorithm (SHA-512) to create an alert should any changes be made to a dedicated file within a file storage system.

By the end of the week and after a discussion with an instructor I decided it would be best to create a virtual network and create some detailed security features within that network.

### Week 2: Start up phase

During this week I spent a lot of time working on Microsoft Azure and reading about and setting up most of the components for the virtual environment I wanted for my lab. I established a free trial, and had several virtual machines set up and was working on ensuring that everything would be properly networked. Towards the end of the week however, I noticed that with all the features I would be setting up in Azure that I would end up having to create a subscription to some features and would end up being charged. At this point I mad the decision to change course and create a virtual network within virtual box .

So to complete the week, I rebooted virtual box, and started to download all the required ISO’s that would be used throughout the course of this project. During this week I downloaded:

* Microsoft Windows 10
* Kali Linux
* Metasploit
* Microsoft Server 2019
* OpnSense

I created virtual client systems for each product and downloaded an exact duplicate copy of OpnSense to create a failover firewall situation for the network.

### WEEK 3/4: IMPLEMENTATION PHASE

These two weeks really were the meat and the potatoes of the entire project as I spent most of my time setting up the new installs of Server 2019, Kali, and OpnSense.

* I established a Virtual WAN IP (10.0.2.254/24) used a DHCP provided address by an ISP of (10.0.2.0/24).
* I created a Master OpnSense firewall with an IP address 10.200.200.251/24 and since the two firewalls would be syncing over a separate network the master had a sync address of 10.0.0.1)with a skew = 0.
* I created a failover OpnSense firewall with an IP address of 10.200.200.252/24 with a sync address of 10.0.0.1 and a skew = 100.
* Virtual LAN IP address: 10.200.200.254/24
* I then assigned all of the different Clients running on the network their own IP address, allowing DHCP on active directory.
* Having a separate network between the two firewalls allowed for them to communicate and synchronize rules between each other, so that rules applied to the master firewall would also affect the linked firewall.

A computer network diagram with words

Description automatically generated

(Initial Top End Network Topography)

A screenshot of a computer

Description automatically generated

(OpnSense Firewall Commands and Setup)

Network Configuration:

|  |  |
| --- | --- |
| Network Device | IP Address |
| Kali Linux | 10.200.200.10 |
| Win Server 2019 | 10.200.200.13 |
| Windows 10 | 10.200.200.20 |
| LAN | 10.200.200.254 |
| Outside Metasploit | 10.0.2.10 |

Active Directory

* I did a fresh install of active directory on the network, and deployed a new forest with a root domain of corp.xyz.com. All client PC’s would be linked to this domain over the network.
* During this time I determined that my fictional company would be a travel agency with dozens of users on a network, but for the purpose of this project I would only be creating a few users on the network using one Windows 10 client. (Due to power constraints within VB)
* I created new user accounts on active directory:

|  |  |
| --- | --- |
| USER | Category |
| Master yoda | **Account Manager** |
| Mace Windu | **Travel Agent** |
| george lucas | Accountant |
| Obi Wan | Travel Agent |
| Ani Skywalker | Customer Service |
| Duchess satine | Travel Agent |

* I grouped the users according to their category, “travel agents”, “accountants”, “account manager”, etc. Using these groups I defined different permissions for data access on the network and different permissions such as remote log-in depending on job description.
* I created a policy for everyone for password security rules, creating a script to force password changes every 30 to 90 days, depending on how complex the user made the password. While I enacted a complex password policy users with more complex passwords would not have to change their passwords as often.
* I added multi-factor authentication, a second best layer of security for the network.
* I adjust and enforced password history, maximum password and minimum password ages, minimum password length, and Kerberos policy.
* I Implemented the concept of the least privilege model so that simple user accounts only have access to the data and information that they need to get their work completed. Account managers (role-based) had slightly elevated levels of permissions to manage their employees effectively and have access to more files. Examples of Group Policy Management set up:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

OpnSense Firewall

* For the firewalls it was all about setting up the syncing process and the virtual network between the two firewalls. After setting up the backup firewall and the master, implementing periodic updates, and establishing the CARP protocol and the skew differential I performed a quick test using ping on the windows 10 system to ensure that if one of the firewalls went down, the other firewall was still functioning with the same settings and would continue to work. I set up a continuous ping from three different command prompt sessions to the primary network IP address, the Master address and the backup firewall address. I then shut down the primary firewall. During this test I witnessed the ping to the master firewall “time-out” over and over again until reboot was completed. I also briefly witnessed a “time-out” on the network itself until the secondary firewall kicked in and took control. With a successful test, I knew that I had created redundancy for the first line of defense over the network.
* I also activated the IDS feature within the firewall and created a custom rule in Kali to upload to the firewall to capture and alert for an NMAP scan. (First type of scan indicating a potential network recon/attack).

A screenshot of a computer

Description automatically generated

Breakdown of the rule:

Action: Alerting or Dropping

Protocol: TCP

$home\_net , placeholder for our home network 10.200.200.254/24. (Any TCP traffic that comes from home network on any port in the direction of 10.200.200.254 will generate message “ Possible…”)

USE NMAP to test this.

Flow of traffic : stateless, it hasn’t been established yet.

Flags: S Syn stealth scan, syn request to server, never complete the 3 way handshake.

Count 50, seconds: 1 : 50 syn requests at once in 1 second it will trigger the rule, and create an alert.

SID : signature ID

A screen shot of a computer code

Description automatically generated

* After creating the rule, I downloaded FileZilla, and used it to transfer the .rules, and .xmp onto the server.
* I knew the tool worked correctly when I saw my custom rule populate in the downloads tab on OpnSense. I enabled the rule and applied it so it would then show up in the rules tab, enabling the rule so it was running on the firewall.

A screenshot of a computer

Description automatically generated

* I tested the firewall by hoping onto my Metasploit and Kali machines and sending a “sudo nmap -sS -Pn –top-ports 500 10.200.200.254” command to scan to the network IP address.



-sS: Syn Scan

-Pn: Host not responding; still continue with scan.

-- top-ports 500

Ip address: the firewall.

* After initiating the scan under the alerts tab were several new alerts that had been populated showing that the firewall had successfully detected and alerted to the probe.
* I downloaded a plug-in called ZenArmor and activated some of its free security features including their powerful proxy tools to help with some content control traffic over the firewall, blocking most access to gun websites, dating websites, sites with violence and gore, and a few other specific websites I did not want crew members accessing. I left access to social media sites as I figured some travel agents might find advertising on them beneficial.
* To demonstrate that the proxy worked correctly I logged in with the account manager on a Windows 10 machine and had him go to Tinder, a dating website over the network. His attempt was unsuccessful and the website was correctly blocked.
* I then created a firmware and software update schedule to ensure that the firewall would be protected from the latest threats.
* I created multi-factor authentication for access to the firewalls management interface.
* In a genuine productive environment, I would set the firewall to default deny traffic, explicitly allowing traffic for what the business needs are.
* In larger networks I would consider segmentation. In this network there is simply redundancy for the firewalls.
* I ensured that the firewall was using NAT to obscure all internal IP addresses.
* I ensured that protective measures on the firewall were set to detect and protect against DoS attacks.
* I disabled all unnecessary ports on the firewall to ensure protection.

### Week 5: Finishing Touches/Project Completion

During this week I ensured that everything across the virtual network was working properly. I went back over all the test and demos that I had done before and repeated them, recording each individual test with OBS video software. I then worked on putting together my power point presentation and incorporated my demo clips into the PowerPoint presentation. During this week I worked on narrowing down the timing of the presentation and cutting some of the more unnecessary information from the presentation to get as close as I could to the 5:00 minute mark. I reviewed the presentation with an instructor and wrapped up production, finalizing the capstone project by the end of the week.