Capstone Proposal

Samuel Roa

Neumont College of Computer Science

Capstone Proposal

Corey Burk

12/04/2024

Table of Contents

Table of Contents

[Table of Contents 2](#_Toc187018743)

[Capstone Abstract 3](#_Toc187018744)

[Project Description 4](#_Toc187018745)

[Building and Defending against Command and Control (C2) Servers 4](#_Toc187018746)

[Project Scope 6](#_Toc187018747)

[Project Technologies 7](#_Toc187018748)

[Skills and Technologies to be implemented in this project 7](#_Toc187018749)

[New Skills and Technologies 8](#_Toc187018750)

[Project Features 10](#_Toc187018751)

[Project Phase Breakdown 11](#_Toc187018752)

[Project Deliverables 14](#_Toc187018753)

[Project Milestones 15](#_Toc187018754)

[Project Timeline and First Two-Week Breakdown. 16](#_Toc187018755)

[References and Research Links 18](#_Toc187018756)

Capstone Abstract

My Capstone project aims to explore and mitigate cyber threats stemming from Command and Control (C2) servers and botnet operations by creating a simulated cyber-attack and defense environment. This project will include deploying a C2 Server to manage a botnet and launch controlled attacks against a simulated enterprise infrastructure I create. I will ensure this testing environment is isolated and contained by beginning the project using a fully isolated virtual network and then switching over to a physical LAN connection that I will create using the Switches in the server room. I will ensure this LAN network is isolated from all other machines by not connecting it to the internet, assigning only static IPs without a Default Gateway, and creating a custom subnet. All network traffic will be monitored. This infrastructure will consist of a Windows 2022 server hosting a web page using IIS and virtual machines via Hyper-V and a Rocky Linux server running a separate website. Additionally, this infrastructure will be created using Dell PowerEdge blade servers that I borrow from the Neumont Student Server Room. The goal of the first phase of this project is to analyze the attack, network traffic patterns, and system vulnerabilities that the C2 server exploits. I will be using Tools such as Splunk, Snort, and Wireshark to capture, monitor, and analyze network packets to document the behavior of malicious communications and their impact on networks.

Following the first phase, the second phase of the project will shift the focus to developing and incorporating defensive strategies to protect against these attacks. I will be capitalizing on the data I collected in the first phase, implementing various security measures, and adopting network intrusion detection and prevention systems to fortify the infrastructure. I will oversee the effectiveness of these defenses through a series of similar attacks explained in the first phase, intending to identify and mitigate vulnerabilities. Overall, this project aims to provide a comprehensive understanding of C2 server operations, enhance my skills in cybersecurity defense, and grow my understanding of real-world scenarios. These defense and documentation tools will be used on a VM (Virtual Machine) with Kali Linux

Project Description

## Building and Defending against Command and Control (C2) Servers

My project will oversee the lifecycle of a cyberattack through a Command and Control (C2) server and a botnet, with an emphasis on offensive and defensive strategies. My primary objective is to gain a greater understanding of how attackers deploy and utilize C2 servers to control botnets, and how to defend against those attacks in a control environment that I deploy.

The project will begin with research behind several open-source botnets such as BlackNET, UBoat, DarkC0ders Net, and BYOB. Once I decide on a C2 Server and botnet, I will begin deployment. This Botnet will be used to launch simulated attacks on a self-hosted infrastructure consisting of

* + Windows Server 2022 hosting multiple virtual machines (VMs) via Hyper-V
  + A Rocky Linux server hosting a website

Once I have completed the setup of the infrastructure, I will deploy a controlled attack to compromise the various systems I created within the network. During this phase of the project, I will be collecting network data using the following:

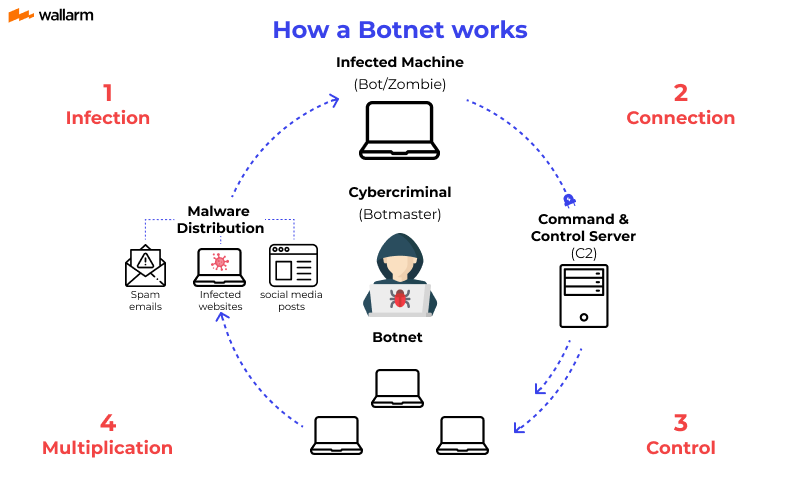
* + - Splunk for log aggregation and threat detection
    - Snort for real-time intrusion detection
    - Wireshark for network packet analysis

The data I collect will provide insight into the communication patterns, payloads, and network anomalies associated with botnet activities.

Once the first phase is complete, I will begin the second phase of the project, which will oversee me creating defensive measures implemented based on that analysis of the first attack. All network data collected, and defensive measures implemented will be done using a Kali Linux VM (Virtual Machine) The defenses that I will include are as follows:

* + - Network segmentation
    - Intrusion Detection and Prevention Systems
    - Creating a Firewall and implementing firewall rules and endpoint protections.

A second wave of attacks will be deployed to evaluate the effectiveness of the defenses. I plan on repeating attacks to defend as best as I can with new technologies and strategies I learn against these attacks. Finally, the project will conclude with a report documenting the attacks, network traffic analysis, defensive strategies used, and lessons learned.



Project Scope

My capstone project will showcase both offensive and defensive cybersecurity techniques by simulating a real-world botnet attack using a Command and Control (C2) Server. My goal for this project is to build a practical infrastructure by getting as close as I can to an enterprise infrastructure, deploying a botnet, learning how to execute controlled attacks, and developing defenses against these attacks to mitigate the impact of the attacks. I will showcase my technical skills by creating an infrastructure comprised of Windows Server 2022, Rocky Linux Server, Kali Linux VM (Virtual Machine), PFsense VM, and a Botnet deployment. Throughout the project, I will keep detailed logs to track the botnet behavior, attack vectors, defense effectiveness, and improvement. I will be creating a final report summarizing my findings throughout this project including an analysis of botnet behavior, network traffic patterns, successful defense strategies, and any recommendations for improving security in a real-world environment.

Although ambitious, I believe my project is reasonable within the scope of 200 man-hours being split between 10 weeks at a pace of 20 hours per week. This project scope is designed to provide hands-on experience with cybersecurity and information systems tools and techniques, with an emphasis on understanding and defending against botnet attacks in a real-world simulation.

Project Technologies

## Skills and Technologies to be implemented in this project

My capstone project will require the usage of several technologies, some new to me and some I’ve used in previous cases. The Technologies I plan on leveraging are as follows:

1. **Hyper-V**
   1. Hyper-V provides a virtualization platform to create and manage virtual machines (VMs) on a Windows server
2. **Windows Server 2022**
   1. The primary purpose of this technology is to serve as the main server operating system (OS) for hosting the virtual machines and provide the infrastructure for the project using the Dell PowerEdge Blades from the Neumont Student Server Room
3. **Rocky Linux**
   1. The purpose of this technology is to serve as a secondary web server that will be used in the simulated attacks against the botnet.
4. **Botnet Framework**
   1. This technology is the botnet itself, managed by the C2 server, this will be what performs the attacks
5. **Splunk**
   1. This technology will serve as a tool for log aggregation and analysis. It will also be used for detecting and monitoring the attacks
6. **Snort**
   1. Snort serves as an intrusion detection and prevention system (IDPS) for identifying malicious activity in network traffic.
7. **Wireshark**
   1. Wireshark is a network protocol analyzer. This will be used to capture and inspect packets sent by the botnet
8. **Firewalls** 
   1. I plan on using Windows Firewall, iptables on Linux, and pfsense. These network security tools will be used to block unauthorized access during the defense phase of this project.
9. **Endpoint Detection and Response (EDR)**
   1. I plan on using open-source endpoint detection and response to protect individual VMs from botnet infections and attacks
10. **OpenVPN**
    1. I plan on using OpenVPN to take advantage of working on this project remotely, though I won’t be directly setting it up since it already exists in the Neumont Student Server Room environment, I will take advantage of it already being set up with the network for the blades for my project.
11. **Kali Linux**
    1. I plan on deploying a Kali Linux virtual machine to host the SIEM used and to capture network data. If time allows it, I also want to spend time researching and using tools that have come preinstalled on Kali that prove useful for this project.

## New Skills and Technologies

To further develop my understanding of cybersecurity and information systems, I will focus on learning these new tools:

1. **Botnet Framework:**
   1. I have not used this type of technology before so learning it will prove to be a challenging task, but it is a crucial one for this project. I will learn how to create, deploy, and launch successful attacks with a botnet controlled by a C2 Server.
2. **Splunk:**
   1. A good chunk of this project is simply capturing data and understanding the attacks from the botnet. Splunk is a SIEM technology that I have used before but never managed to get working so I am excited to work with this for my project. If I am not able to configure Splunk within the first 2-3 weeks of this project I plan on pivoting to another SIEM solution like ELK Stack or Graylog.
3. **Snort:**
   1. Snort will play as an IDPS for this project. I have never touched nor deployed an IDPS myself so learning how to implement this will prove great for my career as it is a crucial technology used in both the cybersecurity and Information systems fields.
4. **Endpoint Detection and Response** 
   1. Like my previous point, this is not something I have experimented with before, but I am excited to be researching this and implementing it in my project.

Project Features

The purpose of my capstone project is to have a complete, fully set-up 2 Server infrastructure consisting of Server 1 being the C2 Server hosting the botnet and Server 2 being the testing infrastructure that I use to practice botnet attacks. Both servers will be using Windows Server 2022 as the main OS, and I will create the necessary VMs I need for this project.

I will be using the Neumont Student Server Room to create my infrastructure using the switches provided and 2 Dell PowerEdge Blades.

I will be using OpenVPN to work on this project from home with a remote connection.

To ensure the safety of this botnet not affecting the server room I will begin with a fully isolated virtual network and then move over to a physical LAN consisting of a private subnet completely isolated from the internet to ensure the attack doesn’t affect other systems.

Project Phase Breakdown

**Preparation and Creation Phase:**

**Necessary Research**

* Before I can begin creating any servers or infrastructure, I have to know what I’m doing which is why I will begin by watching any helpful videos I can find and reading any documentation available on BYOB (the botnet I plan on using), Splunk, Snort, Wireshark, OSSEC, and PFsense. I do plan on skimming research on Windows Server 2022, Hyper-V, and Rocky Linux; since I have used these before I won’t use up too much time on researching these, but I will do some research on things they offer that I might’ve not used in the past just to refresh my mind on these technologies.
* My **Deliverable** for this phase will be a documentation of research I conducted during this phase. I plan on uploading all my findings on my [GitHub Page](https://github.com/sroa18).
* During this phase, I also plan on creating a diagram of the infrastructure that I plan on creating for this project. This diagram will serve as a blueprint, and I will use it as a comparison to see the contrast between the beginning of this project and the final product.

**Creation of Infrastructure**

* Using the research, I gathered and the diagram I created from the previous phase, this phase will focus on beginning the creation of the project. Using two Dell PowerEdge Blades from the Student Server Room, I will begin by loading both servers with Windows Server 2022. One server will be used to host the C2 Server, the botnet, and the dummy machines to use as bots. The second server will host a Windows IIS Web Server, A Rock Linux VM that hosts a Web Server, A PFSense VM, and a Kali Linux VM. I will also use this time to create and document the network I will use for this project, starting with the virtual network and then switching over to the physical LAN network.

**Project Phase Breakdown (Cont.)**

**Testing Phase:**

**First Attack:**

* Once I complete the creation of the infrastructure and ensure all systems can communicate with each other I will begin testing the Botnet. During this time, I will troubleshoot any issues that arise, document all network data transmitted, and document how to use the botnet. I will also record the first successful usage of the bot for my presentation to compare it to the second attack.
* After a successful attack I will document how long it took for the botnet to disable the systems and the services they run.

**Second Attack:**

* After the first successful attack I will immediately begin restoring the servers that were affected by the attack and document the restoration, document the data that was transmitted during the attack, and review how it was used to see what I can learn from it for the defense phase.
* Once I feel I have reviewed all information presented to me from the first attack I will begin implementing defenses based on what I’ve learned. This time will also be used to handle all troubleshooting that may have arisen from this point.
* After all defense tools have been implemented, I will begin a second round of testing/attacking using the botnet. I will also record this round to compare it with the first round. All network data captured will be documented.

**Project Phase Breakdown (Cont.)**

**Final Phase:**

* This phase includes a potential third round of testing depending on how long it takes me to get there and testing of new tools that Kali Linux provides that I did not include on the main list.
* Additionally, I will use this phase to create a final documentation serving as a review of everything I have documented and learned throughout this project, highlighting what went right and wrong, and will be used to compare the first diagrams with the final diagram.
* The final part of this project will be to create the final presentation, this will also be where I decide to attempt a live demonstration of the project or opt to use the videos, I recorded in the previous steps depending on whether the project works after the two, potentially three attacks. I will create a loose script that I will practice for the presentation and prepare for possible questions.

Project Deliverables

**Project Outcomes:**

**Server 1:**

By the end of this project the first machine will serve to have a fully functional C2 server, hosted with Windows Server 2022, with an operational botnet that can attack the second machine without causing any damage outside of the private LAN I set up.

**Server 2:**

By the end of this project, the second machine will be running Windows Server 2022, running a web server using IIS, and running 3 VMs consisting of PFSense, Kali Linux, and Rocky Linux, with an additional web server running off Rocky Linux. This machine will be properly defended using information learned from the attacks of the first machine, using PFsense as a firewall, OSSEC or Splunk as the SIEM, Snort, and Wireshark.

**Documentation:**

I plan on creating extensive documentation throughout this whole process to record my findings on each aspect and create a review of the project at the end at the end, record what I have learned, record comparisons from the beginning of the project to the final product, and upload all my findings to my [GitHub.](https://github.com/sroa18) This documentation will also include all the diagrams I created at the beginning to build this project I will create a final diagram of the existing diagram and compare it. Finally, I will create a detailed set-up guide that is intended to serve as a low-along if anyone wishes to recreate this project.

Project Milestones

1. Begin documentation and conduct final research for the project and create a diagram for the creation of the project.
2. Both servers are created, and Windows Server 2022 is installed and running properly on both
3. The first server has C2 Server and Botnet up and running. The second Server has IIS Webserver created and Necessary VMs created. A fully isolated virtual network is created to conduct connectivity testing.
4. The network is switched over to a physical LAN once the first server has been proven to be completely isolated from the internet. A private subnet with static IPs has been created.
5. Launch the first successful attack, documenting all data transmitted while also recording the attack for demonstration.
6. Restore the effected server from the previous attack and begin creating necessary defenses for the next attack.
7. Launch a second attack, recording this attack for demonstration and comparison. Document all data transmitted and differences between the first and second attacks.
8. Create a final documentation serving as a review of everything I have documented and learned throughout this project.
9. Create a step-by-step guide on the project for anyone who wants to recreate it.

Project Timeline and First Two-Week Breakdown.

|  |  |  |
| --- | --- | --- |
| Week | Milestone | Estimated time to complete |
| 1 | Necessary Research/ Creation of Documentation/Creating Diagrams  Uploading all findings to GitHub with continual updates. | 15 Hours |
| 2-3 | Creating both Servers running Windows Server 2022 and creating a Virtual Network. Loading the first server with BYOB Botnet and testing to see if it works. If BYOB does not work after troubleshooting, pivot to different botnets or potentially create my own. Once the botnet is created, isolated from the internet, and once it’s proven safe move over to physical LAN. Once the botnet is created, load the second server with the necessary VMs and create web servers using IIS and Rocky Linux. Deploy Wireshark and snort to record network data transmitted. | 55 Hours |
| 4-5 | Launch the First attack. Troubleshooting any issues as they arise. Once I record a successful first attack, I will review the data transmitted, attack recording, and create extensive documentation breaking down what happened, and use the information I learned to know what kind of defenses I’ll need. Will also restore the second machine from the effects of the first attack. All information will be documented and updated on GitHub | 40 Hours |
| 6-7 | Launch a second attack, troubleshooting any issues that arise. Once a second attack is successful and recorded, I will review the new data that was transmitted and compare it to the first attack emphasizing the importance of the defenses used. All information will be documented and updated on GitHub | 40 Hours |
| 8-9 | If the time allows it, I will use the information used from both attacks and tools from Kali Linux to defend from a third round of attacks. This attack will also be recorded and documented. If not, I will use this time to continue troubleshooting and potentially switch from Splunk to OSSEC. Will create final documentation that will emphasize a review of the project and attempt to restore the servers for a live demonstration. Will create a set-by-step guide. | 30 Hours |
| 10 | This will be the time that I use to create practice presentations and finalize my presentation. I will practice a script and prepare myself for questions. By this point, I will have decided if I will use the recorded attacks for demonstration or conduct a live demonstration. | 20 Hours |

References and Research Links

[Botnet Link](https://github.com/malwaredllc/byob)

[Hyper-V](https://learn.microsoft.com/en-us/virtualization/)

[Windows Server 2022](https://learn.microsoft.com/en-us/windows-server/)

[Rocky Linux](https://rockylinux.org/)

[Splunk](https://docs.splunk.com/Documentation)

[Snort](https://www.snort.org/documents)

[WireShark](https://www.wireshark.org/docs/)

[OSSEC](https://www.ossec.net/docs/)

[PFsense](https://docs.netgate.com/pfsense/en/latest/index.html)