CIST 3381: Information Assurance & Security

Spring 2022

Pen-testing Application Experience Proposal

* **Your Name:** Michael Chillemi
* **What you want to do after graduation:**

I want to be a red team penetration tester.

1. Propose at least three choices for the application (open-source applications) you’d like to work on. We will meet and finalize one on which you will work during the semester.

*Note: Some applications cannot be used as your primary application, including recon applications, steganography applications, and password cracker, NMap / Zenmap, Nessus, Wireshark, Maltego.*

Pen-Testing Application Choice - 1

* **Application name + URL**

BeEF

[https://beefproject.com/#:~:text=BeEF%20is%20short%20for%20The,focuses%20on%20the%20web%20browser.&text=BeEF%20will%20hook%20one%20or,from%20within%20the%20browser%20context](https://beefproject.com/" \l ":~:text=BeEF is short for The,focuses on the web browser.&text=BeEF will hook one or,from within the browser context).

* **Application Purpose**

Beef is a browser exploitation framework. It is a pen testing tool that focuses on web browsers. From within the browser context, BeEF will hook one or more web browsers and utilize them as beachheads for launching directed command modules and other assaults on the system.

* **Project Scenario & goal (including how / for what purpose you will use the application for)**

The purpose I will use this application is to use a web browser to activate various tools on a targets computer. Ex: getting log in credentials, webcam shots and many more.

* **Why are you interested in this application?**

I am interested in this topic because people use browsers every day. Also I have always been curious how to use web browsers to gather information about a target. To hopefully learn how they work and how to identify a similar tool if faced with it in the future.

Pen-Testing Application Choice - 2

* **Application name+ URL**

Metasploit Payloads reverse shell scipts

https://docs.rapid7.com/metasploit/working-with-payloads

* **Application Purpose**

The purpose is to get the target to download and open the reverse power shell script in order to get access to the targets computer.

* **Project Scenario & goal (including how / for what purpose you will use the application for)**

Creating a basic webpage with a download link for the user to download the payload once downloaded the target is going to run it giving full access to the attacker.

* **Why are you interested in this application?**

I am interested in this application because metasploit is very interesting and useful tool used in pen testing. Also using reverse power shell script to gain access to a computer has always been a interest of mine.

Pen-Testing Application Choice - 3

* **Application name+ URL**

Aircrack-ng

https://www.aircrack-ng.org/

* **Application Purpose**

The purpose of this application is to access how secure a wifi network is. You can use this tool to monitor packets and export to text files to do further investigation. It can also run attacks like replay attacks, de-authentication, and fake access points.

* **Project Scenario & goal (including how / for what purpose you will use the application for)**

Using aircrack-ng to hack into a WiFi network to be able to obtain the WiFi password.

* **Why are you interested in this application?**

As I started to get into Cyber security one of my many interest was being able to find passwords from WiFi networks without knowing the password.