Matthew Wilson

Dr. Ali Zarafshani

CSCE 4560.002 Group 12

3 December 2022

Matthew Wilson Project Report Contribution

What is Beef? Beef is a tool in Kali Linux that facilitates phishing attacks meant for penetration testing. Beef generates a link that, when clicked, hooks a victim's browser. This hook gives the attacker a large amount of information about the victim's computer and gives the attacker control over the victim's browser. Once the hook is set, the attacker knows the victim's operating system, IP address, browser type, browser extensions, and more. The attacker can also make pop-ups appear on the victim's screen, turn on the victim's webcam, redirect the victim to another site, and more. This information and control over the victim's browser allows the attacker to perform very convincing spear phishing.

The purpose of using Beef in this project is to expand on the demonstration of Beef from the lecture. There are two methods for deploying Beef, hosting locally or on a server. Hosting locally is easier to use, has more customizability, and can be hosted on the attacker's machine, but the attacker is limited to attacking other machines on their local network. Hosting on a server allows for attacking any machine with an internet connection and a browser, but hosting on a server costs money, makes tracking the attacker easier, and the attacker has much less customizability.

Hosting locally requires a machine running Kali Linux OS with Beef-xss installed. This version of Beef makes a script and generates a line of html code for embedding the script into any html file. For a spear phishing attack, an attacker places the line of code into any html file,

sends that file to a victim, the victim opens the file in the browser, and the script runs and embeds the hook into the browser. From there, the attacker can perform further phishing or reconnaissance using the various tools in Beef. The script works only on the local network since the html file with the Beef hook script is not attached to a domain and can not connect to the internet.

Hosting over a server requires a hosting service that has a machine that can run Beef. I use a service called Linode. Linode allowed me to create an instance of a linux machine that was specialized towards running Beef. This allows an attacker to attack any computer connected to the internet since Linode hosts the Beef machine on the internet. However, Linode costs money, has limits on how much data can be processed, and can track the attacker. Changing the website that has the hook script is difficult using Linode and requires a large amount of configuration. It is more practical to use the hook webpage that Beef provides in conjunction with Linode. This method of using Beef is better suited for large scale phishing and not for spear phishing.

If I was to perform an attack using Beef, I would target a group of victims on the same local network with a spear phishing attack. I would use the local method to stay more anonymous and grant me more control over the attack. I gain access to a machine that is on the same local network as my victims. Use a flash drive with bootable Kali Linux image to boot the machine to Kali. Next, I run Beef and email my website to the victims. The email needs to look authentic and enticing for the victims to click the link provided. I am assuming only a small percentage of the victims will click the link. Those who click on the link will have their browser open and the hook embedded into it. From there, I perform reconnaissance to find which victim has the data I want or is the easiest to infiltrate. I redirect the victim I chose to my fake website

saying their password needs to be updated and that they need to input their current login info. Once they submit the login, I have successfully stolen their login information using Beef.