<Name Omitted>

CS5155 – Lab 3 Report

Setup:

* Download Security Onion & Pcap file
* Use security onion Setup wizard utility
* Use tcpreplay to replay given pcap file to eth0 (chosen for the interface)

Full command used: sudo tcpreplay -ieth0 -M10 ./Desktop/lab3.pcap

Given Data:

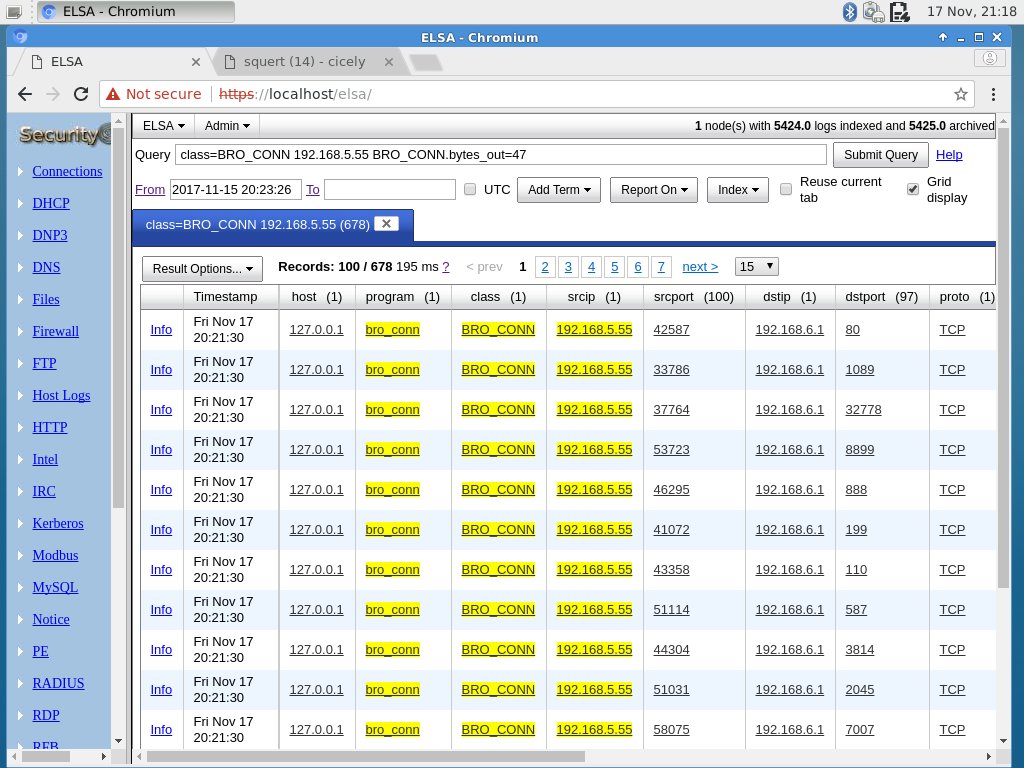
* All data within Pcap file
* Company address range (192.168.6.0/24)
* Gateway address (192.168.6.1)
* Suspicious IP address (192.168.5.55)
* Information that there is only one attacker and only one victim

Phases of Cyber Kill Chain:

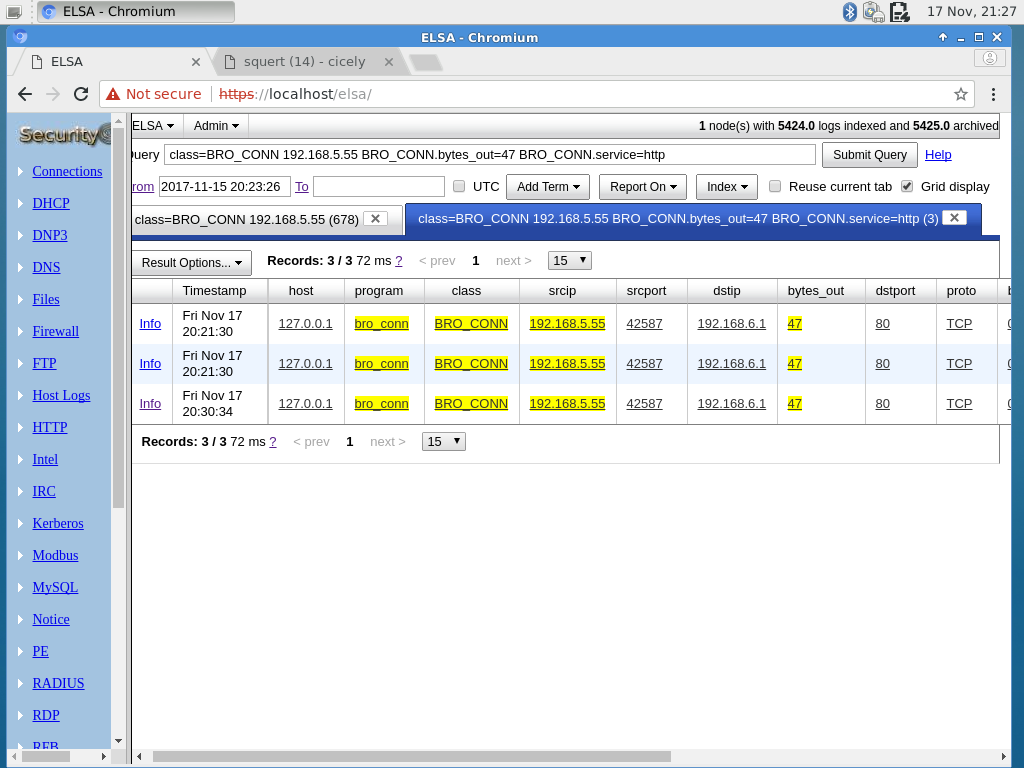
1. Reconnaissance

For reconnaissance, the attacker gathered names of employees off of the company website.

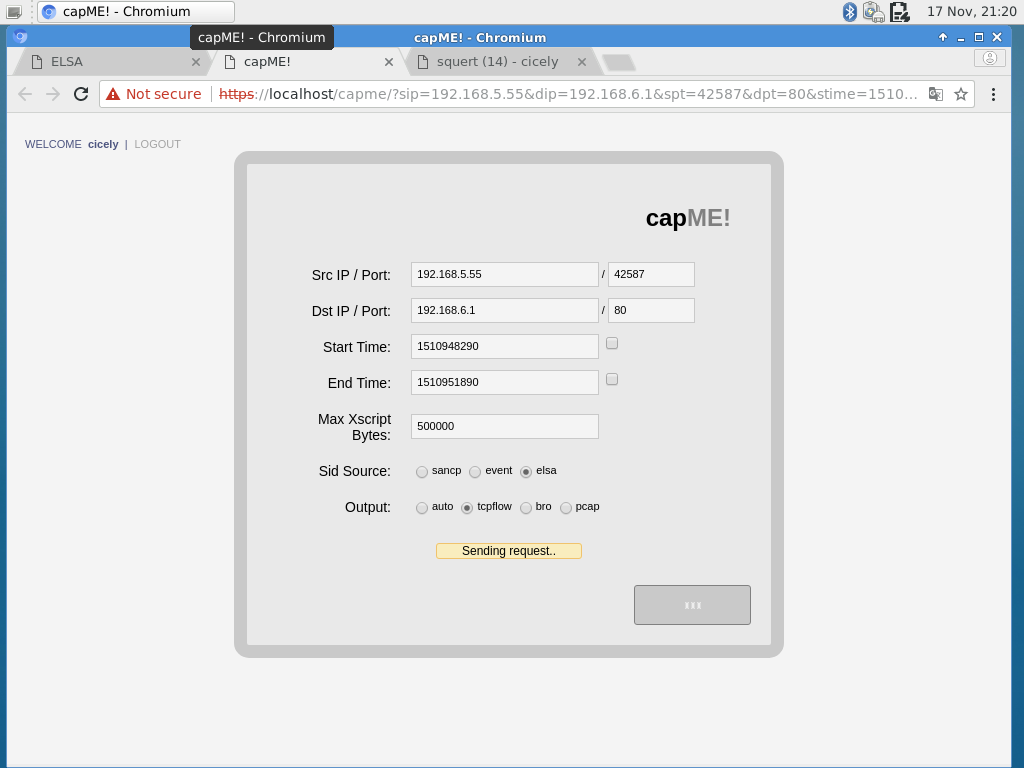
In order to determine this, I performed the following actions:

* + Using ELSA, I checked the bro conn logs for connections involving the suspicious IP address (192.168.5.55)

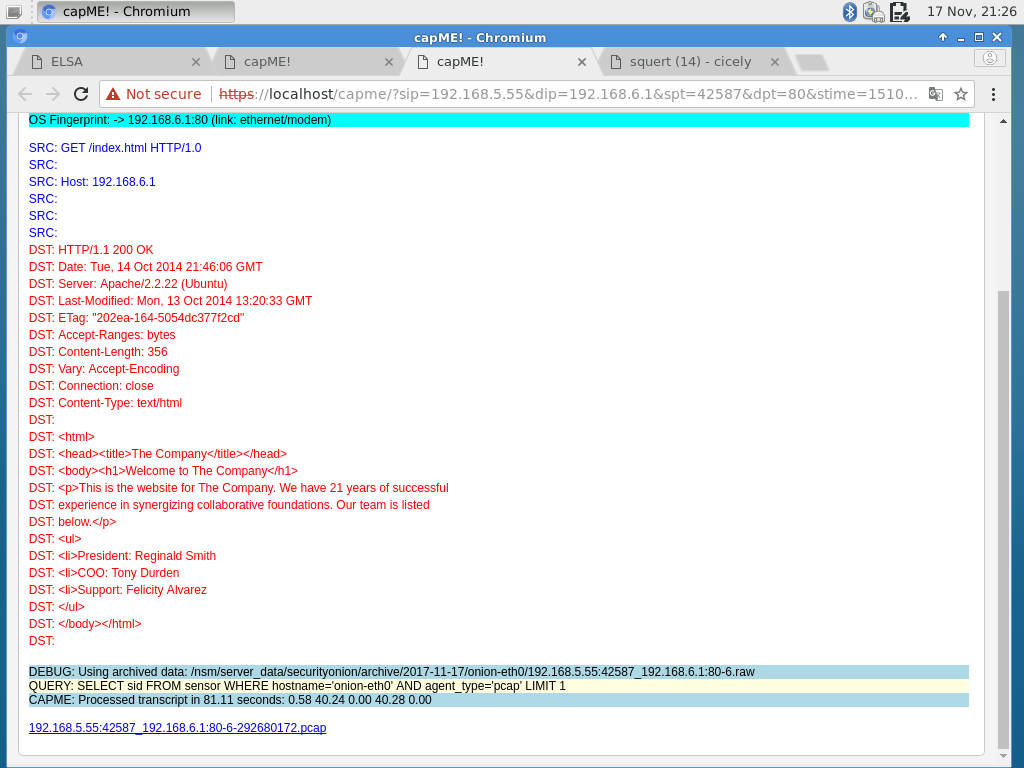
*Connections with suspicious IP (192.168.5.55) in bro\_conn logs.*

* + Using the information that 192.168.5.55 connected with the gateway (192.168.6.1) many times, I concluded that the information gathered probably was from somewhere public facing.
  + From there, I concluded that the information was probably gathered from a public facing website, which would be hosted via http or https and checked for connections via port 80 with the gateway. Within this search, there was a connection that had 47 bytes out. I chose to investigate that connection further.

*Connections from suspicious IP to gateway via port 80 that had bytes out.*

* + I used one of the instances with 47 bytes and sent eh log to ‘capMe!’, allowing me to see the transferred data.

*Sending the log to capMe!*.

* + The data from the tcpflow indicated that the attacker had connected to the company’s home page and could have gotten the names of employees from there.

*Representation of the data sent for homepage that includes employee names.*

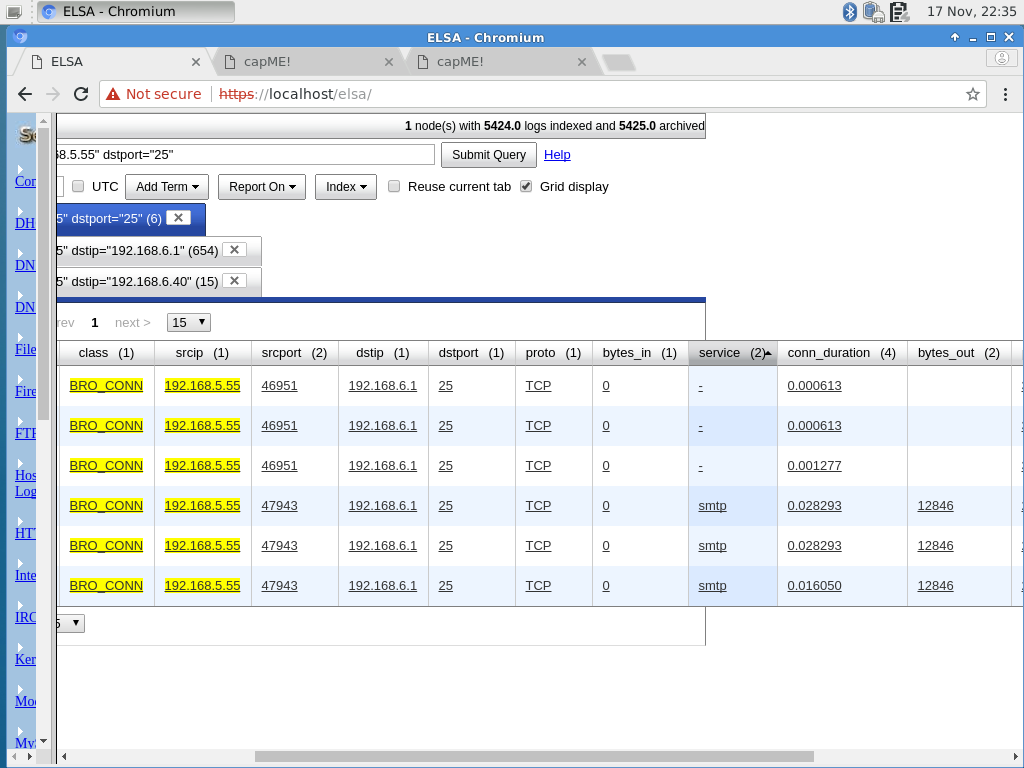
1. Weaponization

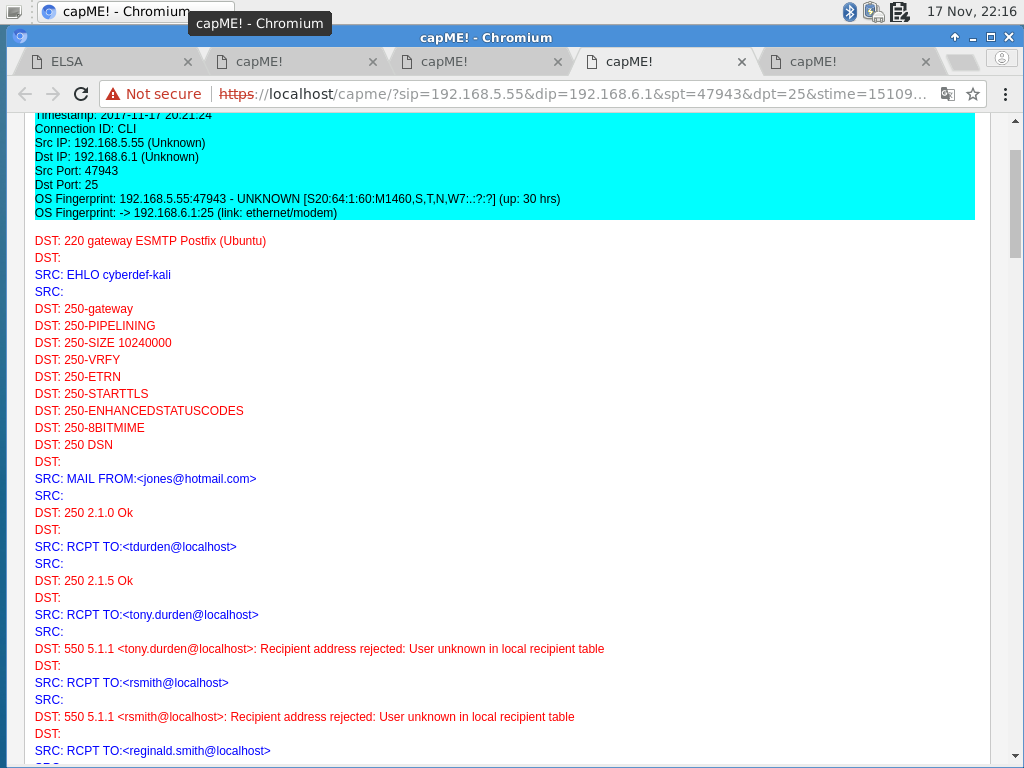
As for the weaponization phase, the attacker used an infected PDF and JavaScript in order to gain a back door into the victim’s computer. A more thorough explanation of how the PDF is in the ‘Exploitation’ section (4). This deduction was a result of investigating the other steps of the cyber kill chain.

1. Delivery

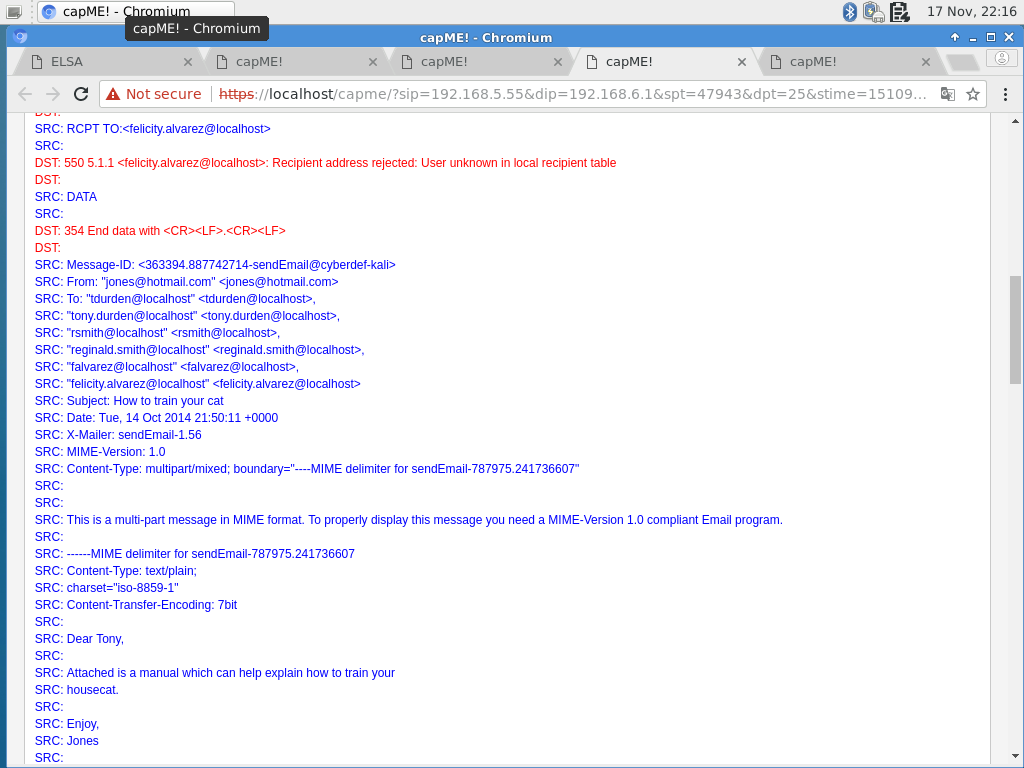
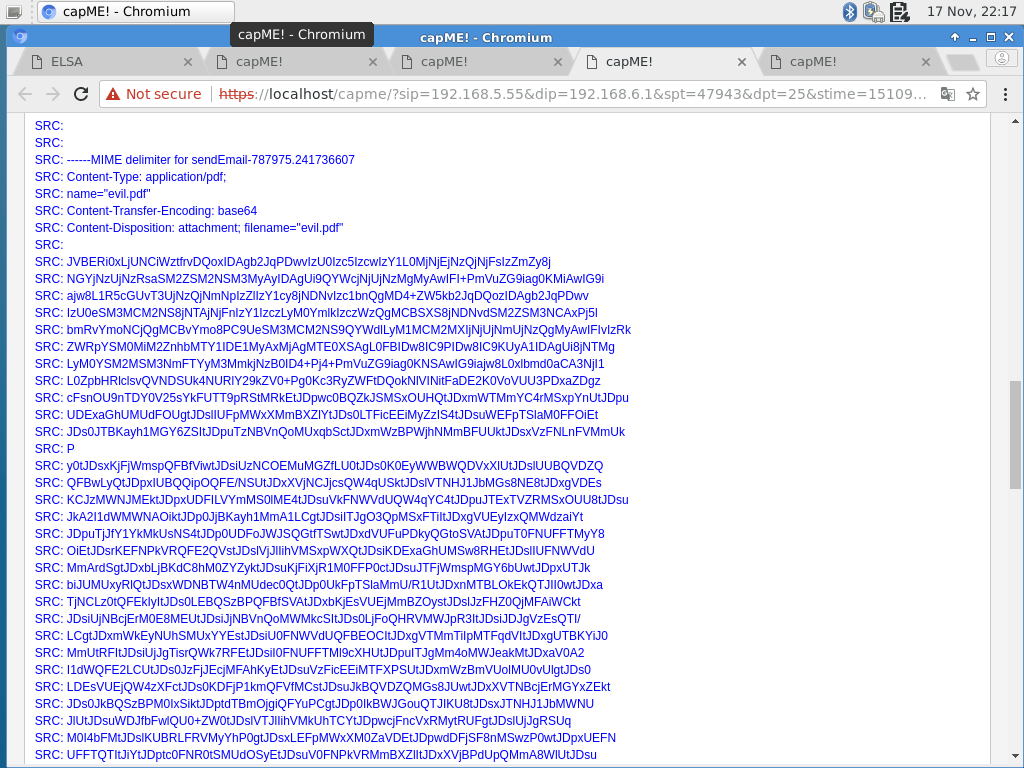
To deliver the infected file, the attacker used an email with a variety of guessed email addresses (derived from the email domain and combinations of the collected employee names). In order to determine this, I used the following steps:

* + Using the malicious address as the source IP and the gateway address as the destination IP, I started a search through the bro\_conn logs using ELSA.
  + From there, I decided that email was the most likely point of access and filtered the list by various common email ports as the destination port. I found that port 25 was successful and looks at one of the logs that used the smtp service and had a large number of ‘bytes out’ (12843)

*ELSA with malicious source IP, company gateway as the destination IP, and an E-mail destination port (port 25).*

* + From there, I looked at the logs with ‘capMe!’ and discovered the sent e-mail with PDF attachment.

*Beginning of malicious e-mail where attacker attempts to guess various e-mail addresses.*

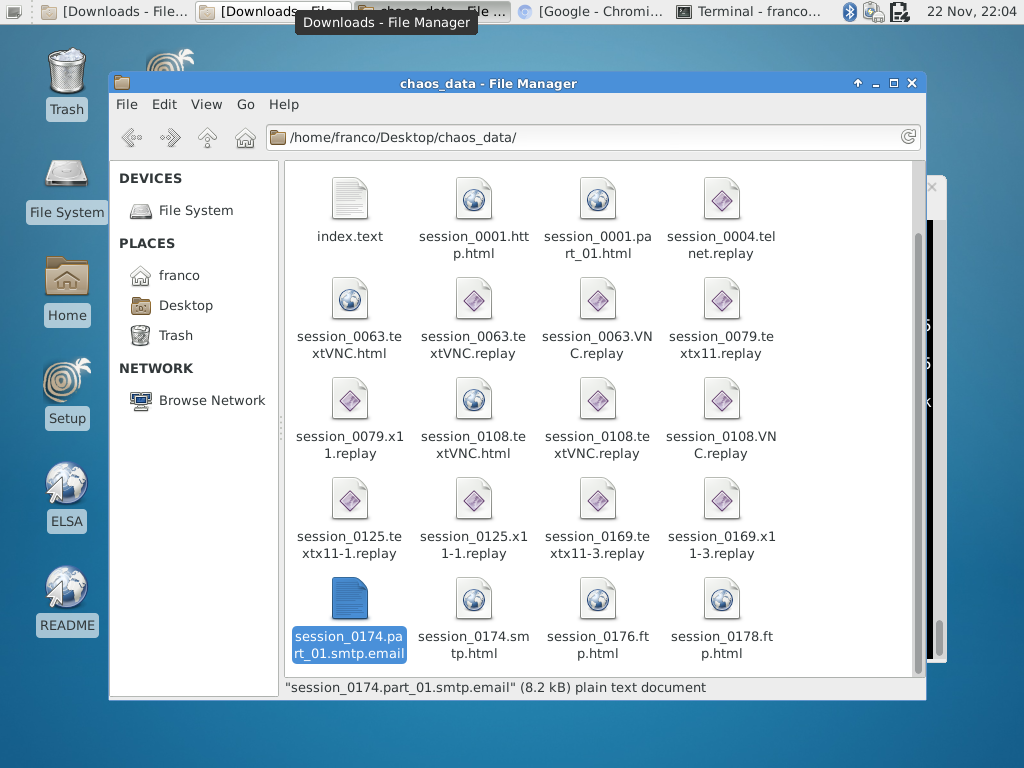
*E-mail with generic, friendly message.*

*Malicious attachment on e-mail.*

* + From this, it can also be determined that the victim was located at IP address 192.168.6.40 based on the traffic, connections, and e-mail that was actually sent.

1. Exploitation

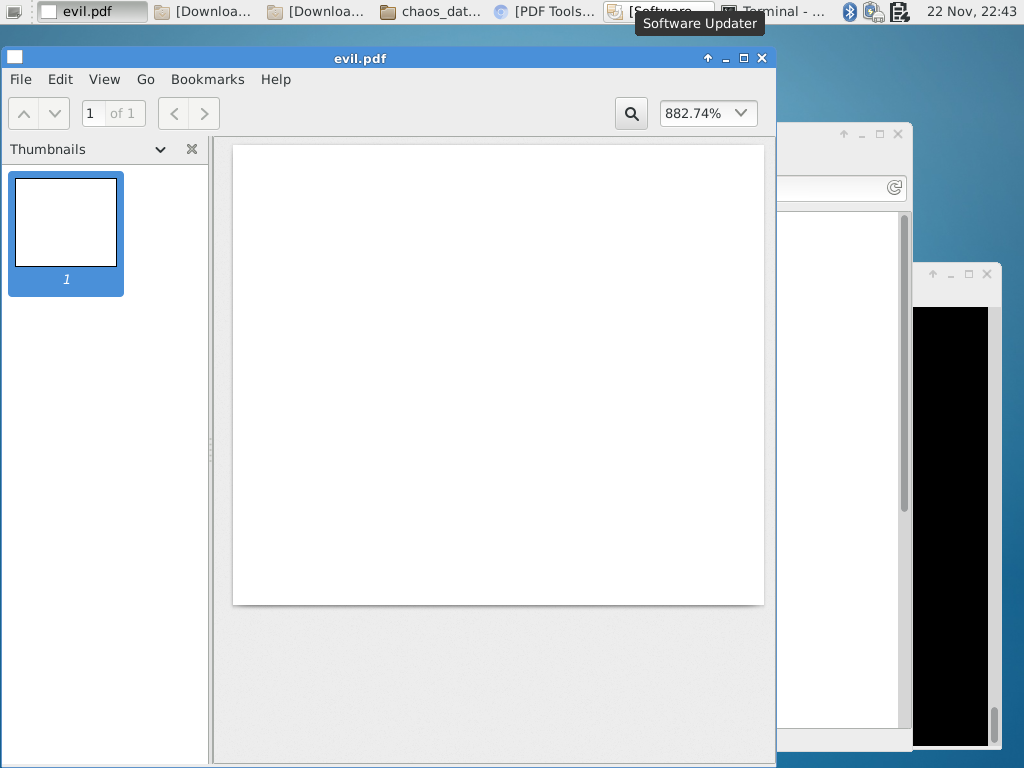
The attacker exploited a vulnerability with PDFs and how JavaScript can be embedded in them. They used obfuscated Javascript delivered in a malicious PDF.

* + To look at the file, the first step was to take the pcap file, create a new folder for a collection of data about the file, and use the chaosreader program to retrieve details from it. Using the command chaosreader ./lab3.pcap, I retrieved a variety of data about the pcap file. This data included the email sent to the victim.

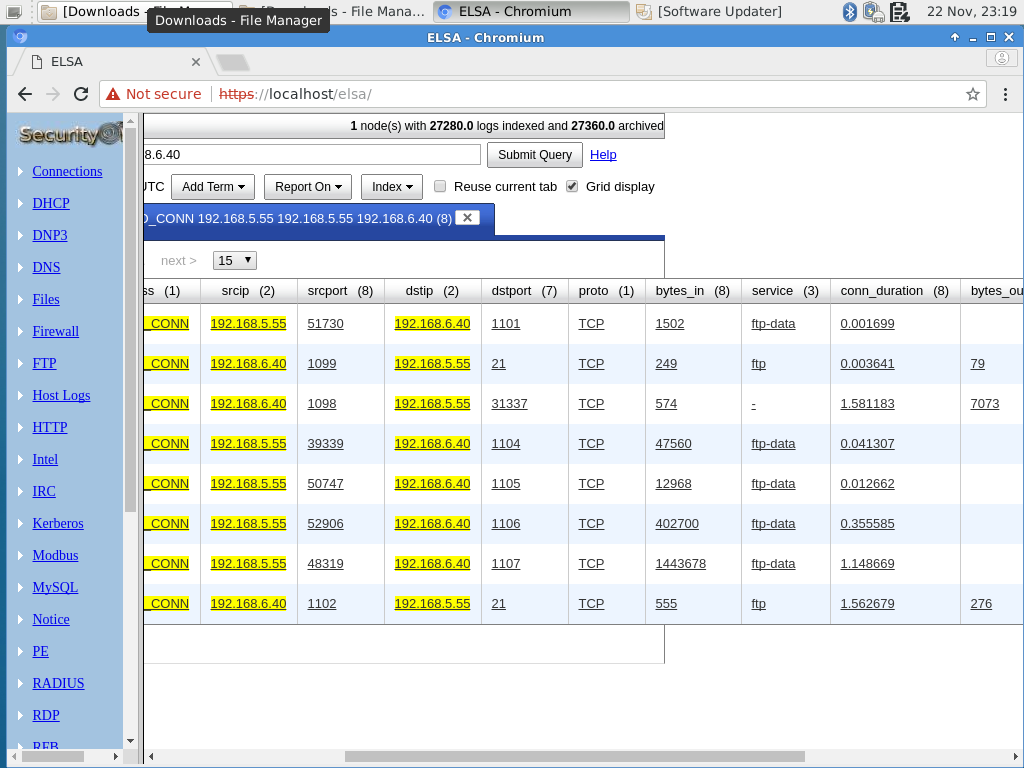
*Data created using chaosreader, including the email file.*

* + From there, my next goal was to extract the PDF from the e-mail file. I decided to do this using the ‘mpack’ package, so first I installed the package using the command ‘sudo apt-get install mpack’.
  + I used the ‘munpack’ command to unpack the email and retrieve the file with command ‘munpack ./session\_0174.part\_01.smtp.email’ and it extracted the file ‘evil.pdf’ into the directory.
  + It is easy to tell that the extracted PDF file is malicious from the fact that

1. The PDF is blank upon opening it.
2. The PDF contains obfuscated JavaScript. This can be clearly seen when opening the PDF in a text editor

*Blank PDF file.*

1. Installation

The JavaScript within the PDF allowed a backdoor into the system by allowing the attacker to have access via ftp. At this point, it is easy to ascertain that the victim is 192.168.6.40 because the attacker makes connections with only the gateway and that IP address.

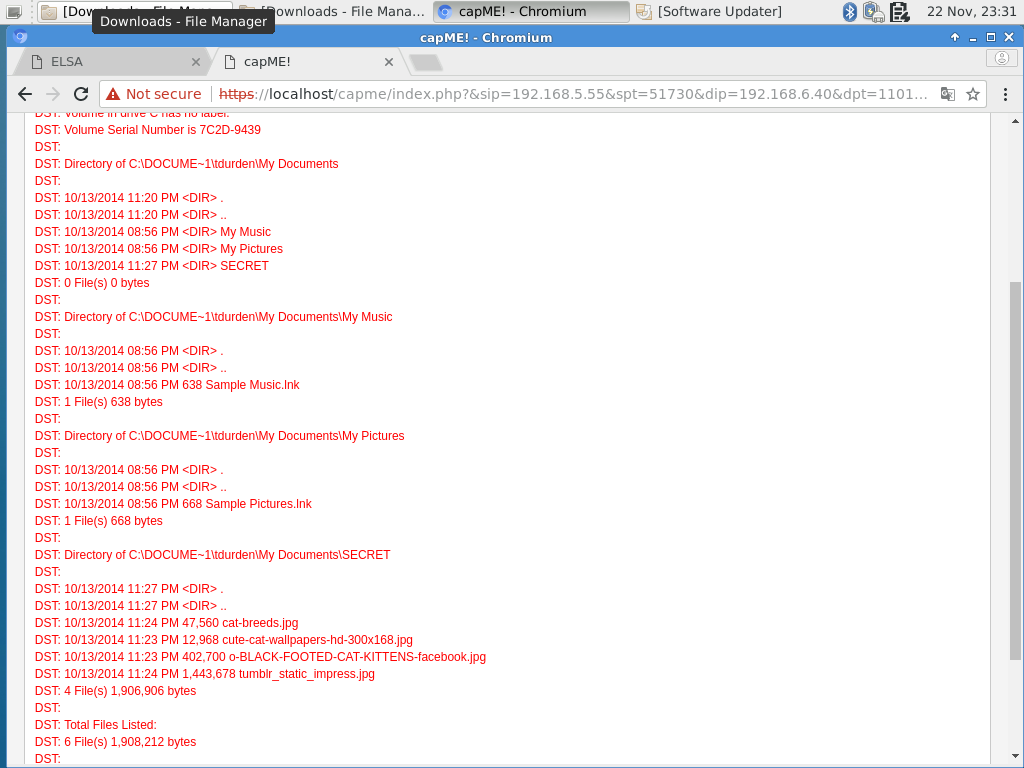
*FTP communication between host and victim.*

1. Command & Control

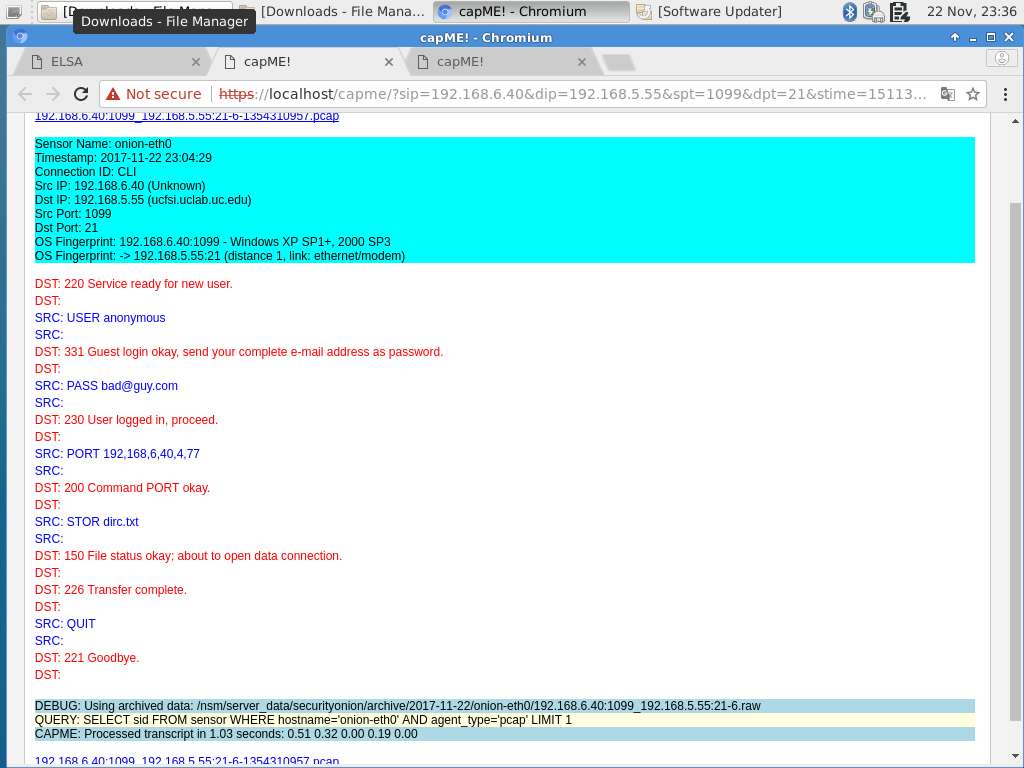
After the malware was installed, the attacker could control the user’s computer via a backdoor. From there, they can control the user’s computer as they like.

1. Actions on Objectives

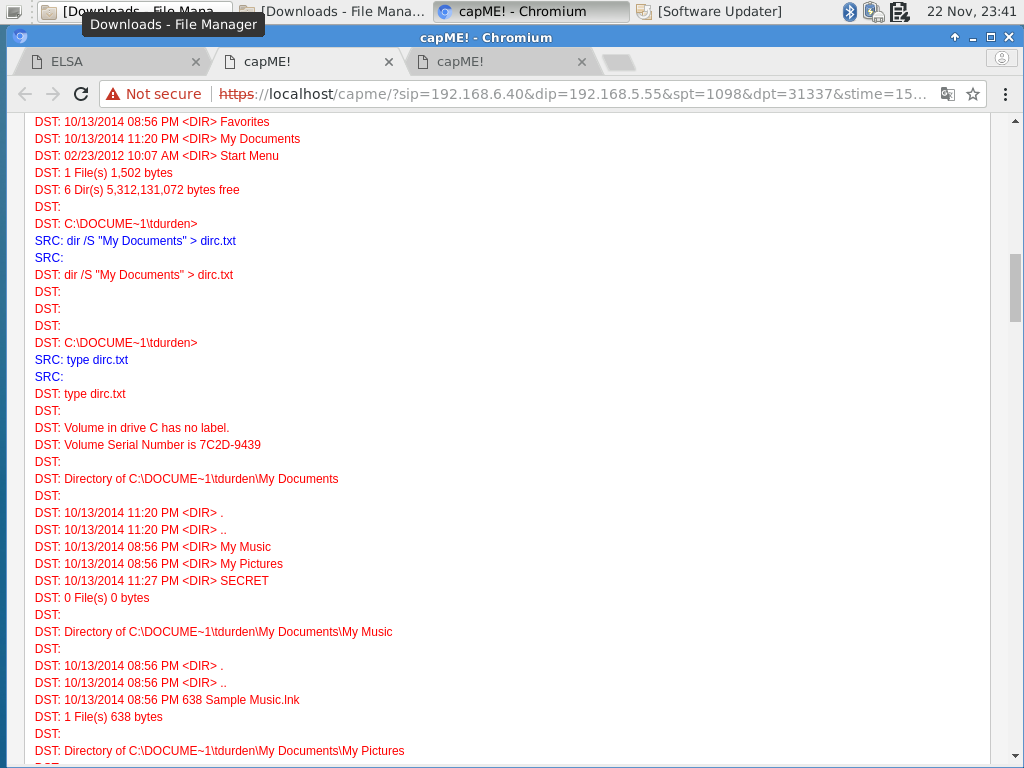
The attacker collects data from the victim via these steps:

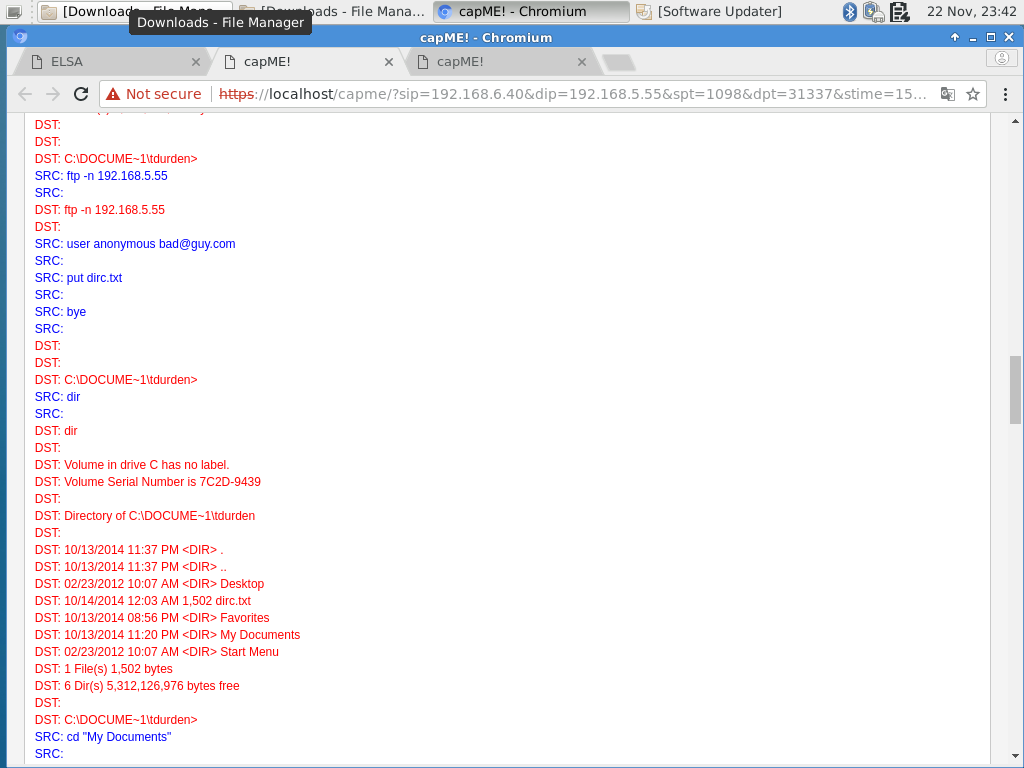
* + First, the attacker searched through the user’s directories.

*Attacker searching through directories.*

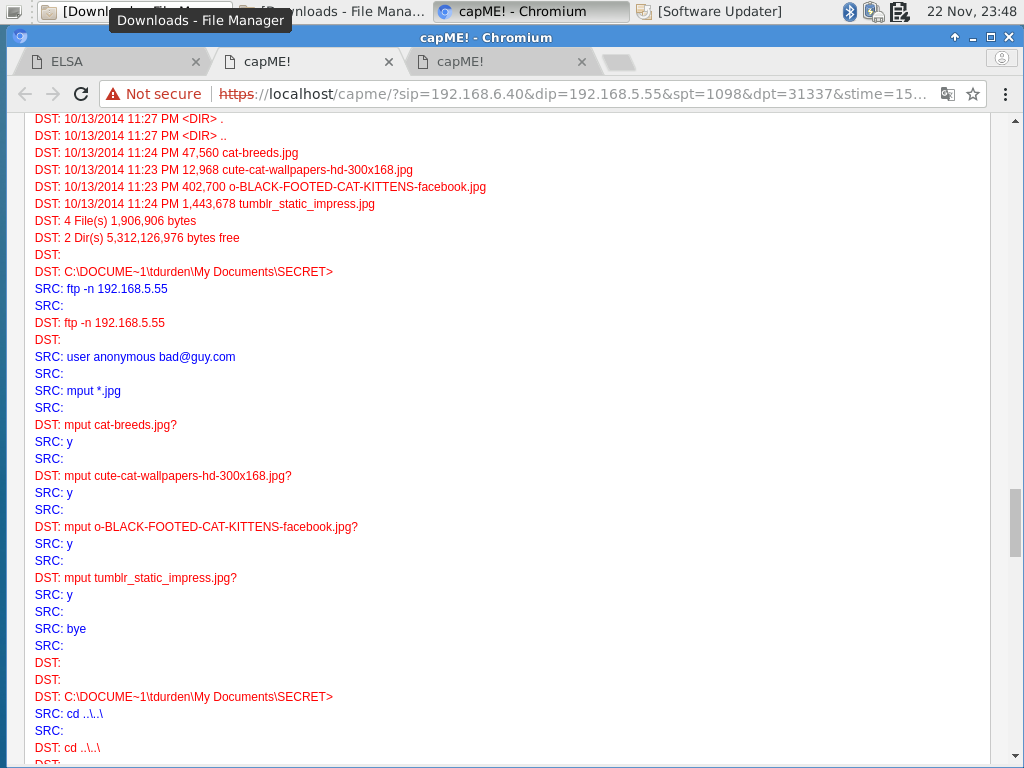
* + Then, the attacker added themselves as a new user and transferred a new file to the victim’s computer.

*Attacker adding themselves as a user.*

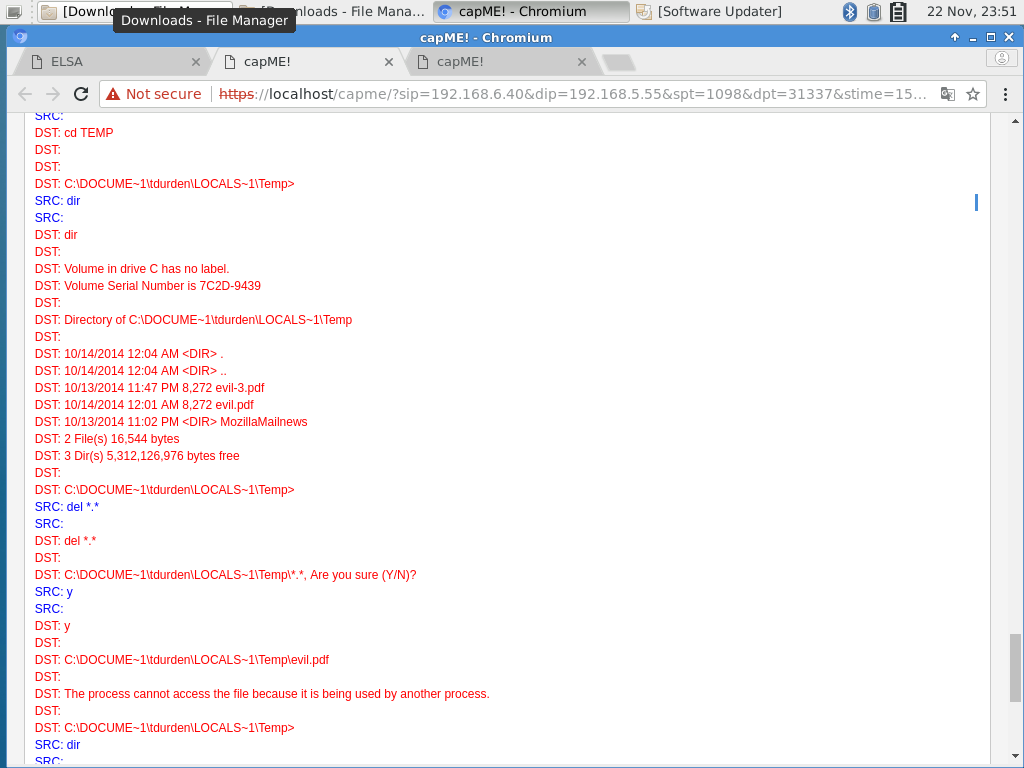
* + The attacker adds data to the file and sends it to themselves to better understand the user’s directory structure.

*Collecting directory data.*

*Sending file with directory data to self.*

* + The attacker then takes some of the victim’s files.

*Attacker collecting files.*

* + **Then, the attacker deletes the malicious pdf from the user’s computer.

*Attacker covering tracks by deleting malicious .pdf fart.*

Final Results:

* Attacker IP = 192.168.5.55
* Victim IP = 192.168.6.40
* Attacker’s weapon of choice – malicious pdf file (evil.pdf)
* Attacker’s goal – collection of files from victim’s computer:
  + cat-breeds.jpg
  + cute-cat-wallpapers-hd-300x168.jpg
  + o-BLACK-FOOTED-CAT-KITTENS-facebook.jpg
  + ttumblr\_static\_impress.jpg

The attacker successfully infiltrated the victim’s computer and stole files from him by using a backdoor implanted via malicious JavaScript in a PDF.