Javonnie Rutherford

Lab 04: Network Forensics

Contents

[Introduction 2](#_Toc163121951)

[What I Know and How I’m Approaching This 2](#_Toc163121952)

[Finding the Bad Guys IP Address and MAC Address 3](#_Toc163121953)

[But Who Is 192.168.15.4? 4](#_Toc163121954)

[Conclusion 4](#_Toc163121955)

[Bibliography 4](#_Toc163121956)

# Introduction

* In this lab, I will be using Network Forensics to find the student harassing Professor Lily Tuckrige. The professor has received multiple threatening messages from an anonymous user. Luckily, we do know two things: the list of students in the class and a packet capture of the port we suspect the harasser is using.

# What I Know and How I’m Approaching This

* The first message came from the IP address 140.247.62.34, which is a dorm room and houses three female students. Students don’t have access to the Wi-Fi and only have access to the ethernet port, so someone in that room installed their own router. “So, it must be someone in that room, right? Since they installed the router?” Unfortunately, no. For whatever reason, they didn’t put a password on their Wi-Fi, so anyone could access it.
* The second message was posted to willselfdestruct.com and was another harassing email. This will be the one I focus more on.
  + I know that the message had to have been posted onto that website. So, if I can either:
    - A. Find the website IP for the website willselfdestruct.com, I’ll know the IP address responsible for sending the message.
    - B. Reconstruct or analyze files for key words like “hate”, “teaching”, and “hide”, since they are unique words. The reason this step works is because [www.willselfdestruct.com](http://www.willselfdestruct.com) runs on HTTP and not HTTPS, meaning everything posted to that website is in plaintext.
  + I’ll know the device that is sending the messages.

# Finding the Bad Guys IP Address and MAC Address

* I decided to follow my second train of thought, by looking for the key words. However, as I uploaded the pcap to Network Miner, I noticed the Messages tab with only two hits on it and voila! I found the Bad Guys IP address and the two websites used for anonymous messages.

A screenshot of a computer

Description automatically generated

* Next, to find the MAC address, I navigate to the Hosts tab and find the source host IP address (192.168.15.4).

A screenshot of a computer

Description automatically generated

# But Who Is 192.168.15.4?

* To do this, I went to the credentials tab in hopes of their email being leaked in some login effort since they used HTTP very often. Unfortunately, 192.168.15.4 has visited every website known to man, so it did take some time scrolling through before I found it.

A screenshot of a computer

Description automatically generated

* Eventually, I end up finding a [jcoachj@gmail.com](mailto:jcoachj@gmail.com) email, which when compared to the students, aligns with a student named Johnny Coach. Case Solved!

# Conclusion

* This was an amazing lab that really highlights the differences between Wireshark and Network Miner. From a Digital Forensics point of view, Network Miner takes this by a country mile. I loved how easy it made this lab by offering file reconstruction, leaked credentials, and the hosts tab that provides all relevant information on the host in one place. This lab was absolutely doable using Wireshark, but I could not imagine how much harder it must’ve been.

# Bibliography

**No citations this go around!**