**WIRELESS SURVEY/PHISHING**

Adrian Varela

WTAMU

CIDM 6341-70: Current Issues In Cybersecurity

Professor Murray Jennex

February 04, 2023

WIRELESS SURVEY

WHAT DID YOU DO

When conducting the Wireshark activity, I was able to download a packet tracing application through the internet utilizing a Mac OS. Through this download I had to read the instructions and download Install ChmodBPF.pkg for the installation of Wireshark. When finally installed I then waited for the application to download the local interfaces. This gave time for the application to access the router for the packet tracing to begin. When starting the application, I chose what destination I wanted to access which was the en0, the Ethernet network interface.

WHAT WERE THE RESULTS

I accessed the Ethernet network interface the results gave me more information than I could imagine. As I accessed the packets traced through Wireshark it gave me information ranging from source to destination to the protocol. I noticed the background color was broken down through the protocol. I first thought that dark backgrounds meant that the files were vulnerable but, I found it to be due to the protocol. When viewing all this information I found that each protocol was broken down to common types such as TCP, ARP, DNS, ICMPv6 and one protocol I was not familiar with MDNS. There were many more protocols and the break down showed the length as well as specific information in the info column. The info column broke down the frame, ethernet, IPV, and detailed information on the protocol. When using Wireshark, you find out a lot of information that you may not want someone to find out.

WHAT DID YOU LEARN

I learned a plethora of information when using Wireshark. Wireshark can be used for packet tracing to see how your information is vulnerable. The great part of the system I learned was that it can be user friendly. This can break down how you want the information color-coded, how you want it displayed by column and even in what order. This information also displayed what information can be broadcasted. This information depicted what IP address the source came from and where they wanted the destination.

As I explored more of Wireshark, I found that you could access even more information through the analyze, statistics and capture options. Each option gave more in-depth exploration of what you were searching. If you as a user did not want to view all of the protocols or information you could use these broken down to each category. The capture in Wireshark showed real time packets and you had the option of stopping at any point. Through the use of all this information you really see how vulnerable you are to hackers.

PHISHING

WHAT DID YOU DO

The exercises for phishing gave great insight on what to depict when it comes to phishing from malicious hackers. The SonicWall exercise started by giving you the option of using a fake name and email to play the receiver of the messages. After inputting your information, you then had to choose whether the email sent to you was phishing like a malicious user or legitimate with 10 questions. When going through the OpenDNS phishing quiz I again had the opportunity to depict whether the access for online websites were phishing or not with 14 sites.

WHAT WERE THE RESULTS

The results for SonicWall were a total of 9 out of 10 questions were answered correctly. The website gave you the option to learn why each answer was answered correctly or incorrectly. The website also gave you the opportunity to receive your answers through your legitimate email. When doing the OpenDNS Phishing quiz I scored 13 out of 14 websites correctly. The results gave you the option of finding out why your answer was correct or incorrect again. They also tied back to why these sites were used because of the popularity of the site.

WHAT DID YOU LEARN

When using both websites I learned that complacency was my biggest issue. When going through the questions each one got repetitive to where I thought I knew what I was doing for each website. This mistake could have been one out of the 90 percent of companies that receive phishing attacks that work. When I discovered why I missed the questions it was the little things such as spelling errors or even the website https protocol. These little items can help protect any company and the information stored within that company.