**Unit 4 Lab: Analyzing Network Traffic to Create a Baseline Definition**

Desmond Hughes

Purdue University Global

IT262 Certified Ethical Hacking I

Cheryl Waters

July 31, 2022

Graphical user interface, text

Description automatically generatedA screenshot of a computer

Description automatically generated with medium confidenceGraphical user interface

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface, text, application, Word

Description automatically generatedGraphical user interface, application, Word

Description automatically generatedText

Description automatically generatedGraphical user interface, text, application, chat or text message

Description automatically generatedGraphical user interface

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generatedGraphical user interface

Description automatically generated

Step 2: Packet Captures review and/or analysis IP (Internet Protocol). Packet Captures also known as libpcap keep networks protected when they are working safely and effectively and often used by network administrators so that they can examine security threats in network traffic. When information or data is breached or has been attacked packet captures can help with the investigation finding the problem. In the hands of hackers, it can be used to hack and steal data and information. Packet Capture can intercept data packets crossing computer networks that is then later stored.

Some ways Packet Capture can help prevent attacks from hackers and data breaches are incident response, keeps an eye on network traffic, and being saved for further analysis. Incident response is used when hackers breach the data and try to cover their tracks the hacker will not be able to unsend the packets that a network as traversed. Doing this can also trace the path of the hackers, and can also see signs when data is being transferred out of the network. Network traffic is the data moving through a computer network, and packet capture looks through network traffic more thoroughly than you can get in other monitoring solutions. Packet captures being able to be saved for further analysis is a good feature because with it being saved it can be reviewed by an analyst. Also, with this feature it can be saved even if it’s multiple hours of data.

Reference

Grimmick, R. (2021). Packet Capture: What is it and What You Need to Know. Retrieved 1 August 2022, from <https://www.varonis.com/blog/packet-capture>