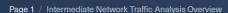
## INTERMEDIATE NETWORK TRAFFIC ANALYSIS



## **Intermediate Network Traffic Analysis Overview**

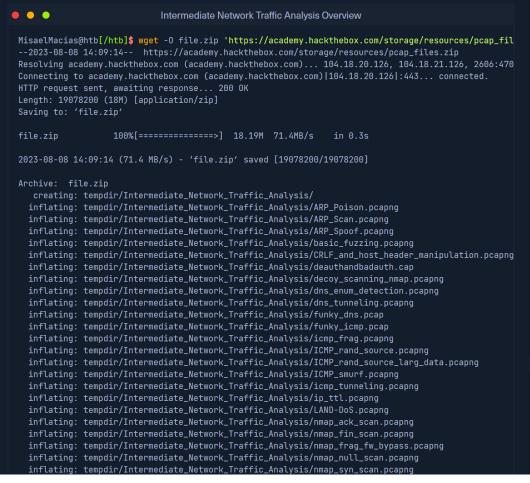
The importance of mastering network traffic analysis in our fast-paced, constantly evolving, and intricate network environments cannot be overstated. Confronted with an overwhelming volume of traffic traversing our network infrastructure, it can feel daunting. Our potential to feel ill-equipped or even overwhelmed is an inherent challenge we must overcome.

In this module, our focus will be on an extensive set of attacks that span crucial components of our network infrastructure. We will delve into attacks that take place on the link layer, the IP layer, and the transport and network layers. Our exploration will even encompass attacks that target the application layer. The goal is to discern patterns and trends within these attacks. Recognizing these patterns equips us with the essential skills to detect and respond to these threats in an efficacious manner.

Further, we will discuss additional skills to augment our abilities. We will touch upon anomaly detection techniques, delve into facets of log analysis, and investigate some Indicators of Compromise (IOCs). This comprehensive approach not only bolsters our capacity for proactive threat identification but also enhances our reactive measures. Ultimately, this will empower us to identify, report, and respond to threats more effectively and within a shorter time frame.

**Note**: For participating in this module and completing the hands-on exercises, please download pcap\_files.zip from the Resources section (upper right corner).

You can download and uncompress pcaps. zip to a directory named pcaps inside Pwnbox as follows.



Resources **Table of Contents** Introduction Link Layer Attacks ARP Spoofing & Abnormality Detection ARP Scanning & Denial-of-Service 802.11 Denial-of-Service Roque Access Point & Evil-Twin **Attacks Detecting Network Abnormalities** Fragmentation Attacks Fig. 19 Source & Destination Spoofing Attacks IP Time-to-Live Attacks TCP Handshake Abnormalities TCP Connection Resets & Hijacking **ICMP Tunneling Application Layer Attacks** 6 HTTP/HTTPs Service Strange HTTP Headers Cross-Site Scripting (XSS) & Code Injection Detection SSL Renegotiation Attacks Peculiar DNS Traffic Strange Telnet & UDP Connections Skills Assessment Skills Assessment My Workstation

OFFLINE

