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.

Intermediate Network Traffic Analysis Overview

```
MisaelMacias@htb[/htb]$ wget -O file.zip 'https://academy.hackthebox.com/storage/resources/pcap_fil
--2023-08-08 14:09:14--  https://academy.hackthebox.com/storage/resources/pcap_files.zip
Resolving academy.hackthebox.com (academy.hackthebox.com)... 104.18.20.126, 104.18.21.126, 2606:470
Connecting to academy.hackthebox.com (academy.hackthebox.com)|104.18.20.126|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19078200 (18M) [application/zip]
Saving to: 'file.zip'

file.zip           100%[===============>]  18.19M  71.4MB/s    in 0.3s

2023-08-08 14:09:14 (71.4 MB/s) - 'file.zip' saved [19078200/19078200]

Archive:  file.zip
   creating: tempdir/Intermediate_Network_Traffic_Analysis/
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/ARP_Poison.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/ARP_Scan.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/ARP_Spoof.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/basic_fuzzing.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/CRLF_and_host_header_manipulation.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/deauthandbadauth.cap
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/decoy_scanning_nmap.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/dns_enum_detection.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/dns_tunneling.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/funky_dns.pcap
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/funky_icmp.pcap
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/icmp_frag.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/ICMP_rand_source.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/ICMP_rand_source_larg_data.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/ICMP_smurf.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/icmp_tunneling.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/ip_ttl.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/LAND-DoS.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/nmap_ack_scan.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/nmap_fin_scan.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/nmap_frag_fw_bypass.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/nmap_null_scan.pcapng
  inflating: tempdir/Intermediate_Network_Traffic_Analysis/nmap_syn_scan.pcapng
```

Resources

Table of Contents

My Workstation

OFFLINE

```
inflating: tempdir/Intermediate_Network_Traffic_Analysis/nmap_xmas_scan.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/number_fuzzing.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/rogueap.cap
inflating: tempdir/Intermediate_Network_Traffic_Analysis/RST_Attack.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/SSL_renegotiation_edited.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/SSL_renegotiation_original.pcap
inflating: tempdir/Intermediate_Network_Traffic_Analysis/TCP-hijacking.pcap
inflating: tempdir/Intermediate_Network_Traffic_Analysis/TCP_rand_source_attacks.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/telnet_tunneling_23.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/telnet_tunneling_9999.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/telnet_tunneling_ipv6.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/udp_tunneling.pcapng
inflating: tempdir/Intermediate_Network_Traffic_Analysis/XSS_Simple.pcapng
```

Start Instance

∞ / 1 spawns left

Next

Mark Complete & Next

Powered by HACKTHEBOX