Network traffic analysis

Saturday, December 9, 2023 5:18 PM

NTA = examine network traffic to characterize common ports / protocols used

- establish baseline
- monitor / respond to threats
- greatest possible insight to network

detect anomalies and help w/ meeting security guidelines

collecting real-time traffic

setting baseline for day-2-day network comms

identifying and analyzing traffic from nonstandard ports, hosts, errors

errors

detecting malware on the wire

past incidents

Required skills and knowledge

TCP/IP stack and OSI model

how networking traffic and host applications interact

Basic networking concepts

understand what types of traffic we will see at each stage

Common ports and protocols

helps when spotting abnormal behavior

Concepts of IP packets and sublayers

understand how TCP/UDP comm

Protocol transport encapsulation

Protocol transport encapsulation

each layer encapsulates the previous

Environment and equipment

- tcpdump
- Tshark = cli of wireshark
- Wireshark
- NGrep = grep for network packets
  HTTP/ FTP Host
- tcpick = cli packet sniffer for tracking and reassembling TCP streams
- network taps = Taps; taking copies of network traffic and sending to another place for analysis
  can put packet back on wire as if nothing changed

- networking span ports = copy from L2 → L3 devices during egress or ingress processing and send back to collection point

  port is often mirrored

- Elastic stack – colmination of tools that can take data from many sources, ingest data visualize it to enable searching and analysis

- SIEMS

Berkeley packet filter BPF – raw interface to read/write from data-link layer

NTA workflow

1. Ingest traffic

   capture filters

capture traffic

2. Reduce noise by filtering

2. Analyze and explore

look at specific hosts, protocols, etc.

- encrypted?
- unauth access?
- abnormal host comms?

4. Detect root issue

- errors?
- benign or malicious?
- IDS/IPS

5. Fix and monitor