SIEM Applications: Security Onion and Gravwell

November 1, 2023

Group 29

Updates

- Gravwell Demo scheduled for November 14th
- Testing report assignment in progress
- Security Onion Installation
- Questions on Faculty Design Review Presentation?
- Gravwell Installation

Security Onion Applications

- Att&ck navigator
  - Provides a link to be able to access the matrix
  - Can color code and annotate the matrix
  - Also has a default layer named playbook that allows users to see the playbook coverage in the context of the Att&ck framework
  - Can right-click a specific technique within the Att&ck framework and view your related plays in security onion
- Grid
  - Can check the status of all nodes in the grid
  - Can view
    - How long node has been online
    - Number of events per second
    - Connection status
    - Process status
    - Description
- PCAP
  - Allows access to full packet capture
  - Can search for a packet stream that meets certain criteria
  - Can view the payload data if needed
  - Can send all visible packet data to CyberChef
  - Can download full PCAP file

Security Onion Installation

- Manager Node has been installed on the VM
  - Email: isugridsiem@gmail.com
  - Password: icpslab@123
- The configuration has recommended using static IPs as opposed to DHCP
- The nodes require another NIC to sniff traffic and one for the manager node

Gravwell Installation

- Self hosted on-prem with 13.9 GB/day data ingestion
- Unlimited: ingester endpoints, retention, search count and automations.
- Community Ed: Requires at least 4GB of RAM and 2CPU cores.
- Currently working on installation guide on ubuntu-SIEMMaster-2-Gravell.
- Obtain Gravwell license for even for CE edition.
- In our case install Gravwell using Debian package.
- Verify firewall rules to allow flow in ports: TLS Ingest Port: TCP 4024, Indexer Control Port: TCP 9404

Gravwell Kits (i.e. applications)

- Zeek: can do semantic analysis on network traffic, detecting protocols and extracting as much information as possible.
- NetFlow: Another network analysis tool specializing in DNS.
- IPFIX: Allows us to quickly identify network flows, filter on ports, or generally monitor the behavior of aggregate flows.
- Grok: The grok program is a great tool for parsing log data and program output. You can match any number of complex patterns on any number of inputs (processes and files) and have custom reactions.