JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Detecting, Preventing, and Responding to Reconnaissance

THREAT MANAGEMENT

Detecting, Preventing, and Responding to Reconnaissance

- Successful reconnaissance doesn't always mean a successful attack, but we want to limit the damage that could occur as much as possible

- We utilize the same technique to limit both casual and directed reconnaissance

Detecting Recon: Overview

- Monitoring must occur at connection points between two network zones

- Perform data collection so you can analyze the data at a later time

Detecting Recon: Data Sources

- Network traffic analysis using IDS, IPS, HIDS, NIDS, firewalls, and other security devices
- Packet analysis
- Protocol analysis
- Traffic and flow analysis
- Device and system logs
- Port and vulnerability scans
- Security Information and Event Management Logs

- If you outsource your services, you might have to relay on your SaaS or PaaS provider to detect it for you…

Detecting Recon: Data Analysis

- Anomaly Analysis
  - What is different about this? What's not normal?
- Trend Analysis
  - Helps to identify future problems based on past
  - Example: Traffic congestion
- Signature Analysis
  - Fingerprint or hash used to detect threats
- Heuristic or Behavioral Analysis
  - Detects threats based on behavior
  - Useful to detect unknown threats
- Manual Analysis
  - Human expertise is used to analyze the data

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Preventing Passive Recon

- Control the information your release
- Blacklist system that are abusing your services
- Use CAPTCHAs to prevent scripts and bots
- Utilize third-party registration for domains/Ips
- Set rate limits for lookups and searches
- Avoid publishing zone files, if possible
- Educate your users about social media risks

Preventing Active Recon

- Employ network defenses
- Limit external exposure of services and know your forward facing footprint
- Utilize an IPS to limit or stop probes/scans
- Utilize monitoring and alert systems based on signature, behavior, or anomaly