LIVE Demo: Hacking with SIEMS

Eric Knight, MIS, CISSP, CISM, CEH
Senior Knowledge Engineer
LogRhythm, Inc.
eric.knight@logrhythm.com

Introduction

- This is a LIVE DEMONSTRATION of using Security Information and Event Managers to diagnose cases of:
  - Following a terminated user's activities
  - Worm outbreaks
  - Dissecting a suspected breach

- SIEM Forensics are capable of spotting illicit activities by:
  - Collecting log and event data from networked devices
  - Reducing the logs to relevant details
  - Enrichment of the information to add human understandable context
  - Classify logs and events to help determine significance
  - Correlate logs and events to identify important conditions

Worm Outbreak – What we expect

- Expected behavior of worms:
  - Propagates typically with a known vulnerability on common open network services
  - Often detected by anti-virus software packages, but may infect a system without signatures recently updated.
  - Replaces or modifies system files
  - Contacts a command and control system on the Internet
  - Sends spam
  - Sends denial of service attacks
  - Attempts to infect other machines

Worm Outbreak Procedures

- We've been instructed to investigate a possible malware outbreak where Bob from Sales (bob-notebook) plugged his computer into the office network after letting his kids use it gaming over the weekend.
- Procedures:
  - See if Bob's system appears infected
  - See what systems Bob's computer has communicated with
  - See if any other systems are behaving like Bob's system
  - See if Bob's computer has been sending spam

Worm Outbreak – Lessons Learned

- Investigation summary:
  - Three systems infected
- Lessons learned:
  - No single log or source of logs was able to show the "big picture"
  - Not much time required to spot other infections
  - Do not trust log data from compromised hosts
- Systems providing critical information: Intrusion Detection, Netflows, Firewall, Anti-Virus.

Hostile Termination – What we expect

- Ex-Employee has access to a number of systems
  - There may be shared or test accounts known to this person
  - “Valuable” information may be deleted, modified, or copied

Hostile Termination Procedures

- We've been instructed to investigate if an employee suspected of an unspecified illegal activity that lead to their termination performed any activities on the network after termination. This activity was initiated by the company's out-processing policy.
- Procedures:
  - Check perimeter devices for evidence of Mr. X's remote authentications
  - Locate files Mr. X accessed

Hostile Termination– Lessons Learned

- Investigation summary:
  - Mr. X used a shared account to access the network from home on multiple occasions.
  - Free wi-fi was used to steal important documents using an old service account.
- Lessons learned:
  - History of usage can contain details useful for spotting a trespass by ex-employees
  - Criminals often make little slip-ups with technology that helps spot even sneaky activities
- Systems providing critical information: Outlook, VPN, Audit Logs

Breach – What we expect

- Hack attempt was made to compromise a host to gain control
- Intruder had to locate and gain access to the critical information
- Critical information is transferred out of the organization

Breach - Procedures

- Company CFO was contacted regarding strange activities to employee bank accounts, all of which seem to be associated with direct deposit records. Determine if this breach happened at your company or by the bank.
- Investigate activities involving the data
- Investigate anything affecting the computer
- Locate the source of the breach
- Locate where the data was sent to

Breach – Summary

- Investigation summary:
  - Hacker broke in from Prague, CZ to the web server
  - Used a hole in the DMZ to access a database on the internal network
  - Probably installed a keylogger or sniffer to capture dbadmin's password
  - Logged into systems until they located the accounting server
  - Transferred the vital employee file to the database server
  - Transferred the file to computer in Prague.
- Lessons learned:
  - Records can be so detailed that they lose their importance in volume.
  - Possible to identify attacks without the majority of security features (Anti-Virus, Firewall, Intrusion Prevention, and File Integrity Monitoring.)
- Systems providing critical information: authentication logs, audit logs, network traffic flow data, access logs.

Conclusion

- SIEMs simplify investigations and accelerate discovery
- All three investigations involved logs that came from multiple systems
- Security and authentication systems were not the only places where useful information was gathered
- Information (or lack of) from a single source cannot always be trusted

Q&A

COMPLY. SECURE. OPTIMIZE.