Detecting Incidents Part 1

INFO-6081 – Monitoring & Incident Response

FANSHAWE

Learning Outcomes

- Event Classification
- Incident Classification Categories
- Detecting Incidents
- Indicators of Compromise
- False Positives
- Intrusion Detection and Prevention Systems
- Incident Decision Making

Event Classification

- NIST definitions:
  - **Event**
    - any observable occurrence in a system or network
  - **Adverse Event**
    - an event with negative consequences
- When an adverse event becomes a threat to the ongoing operation of an organization, it is classified as an incident
- Incident classification is responsible for determining which adverse events are potential incidents (candidates)

Event Classification Sources

- Some of the sources used for event classification include:
  - Intrusion Detection and Prevention Systems (IDPS)
  - Security Information and Event Management (SIEM)
  - Antivirus and Antispam Software
  - File Integrity Checking Software
  - Operating system, Service and Application Logs
  - Network Device Logs
  - People

Incident Classification Categories

- Some broad categories in which incidents can occur include:
  - Denial of Service
  - Malicious Code
  - Unauthorized Access
  - Inappropriate Usage
  - Multiple Component

Detecting Incidents

- Many incident types result in some form of disruption of service
  - Unfortunately, service disruptions can occur even when no malicious compromise is present
- To classify potential incidents before they occur, the following terms are used:
  - **Indicator** (aka indicator of compromise)
    - A sign that an adverse event is underway and could become an incident
  - **Precursor**
    - A sign that an event currently occurring may signal a future incident

Possible Indicators of Compromise

- **Presence of Unfamiliar Files**
  - Unfamiliar files appear, or files appear in an unusual location
- **Presence of Unknown Programs or Processes**
  - Strange or unknown programs appear in the process list, or a user receives a User Account Control elevation prompt from an unknown application
- **Unusual Consumption of Resources**
  - Unexplained spikes in resource usage
- **Unusual System Crashes**
  - A system hangs, reboots or crashes more than is normal

Probable Indicators of Compromise

- **Activities at Unexpected Times**
  - Resource usage is higher than expected baseline
- **Presence of Unexpected New Accounts**
  - New accounts added to a system that have no journal of creation
- **Reported Attacks**
  - A user reports that they have been the victim of an attack
- **Notification from IDPS**
  - An adverse event is detected by scanning the network traffic

Definite Indicators of Compromise

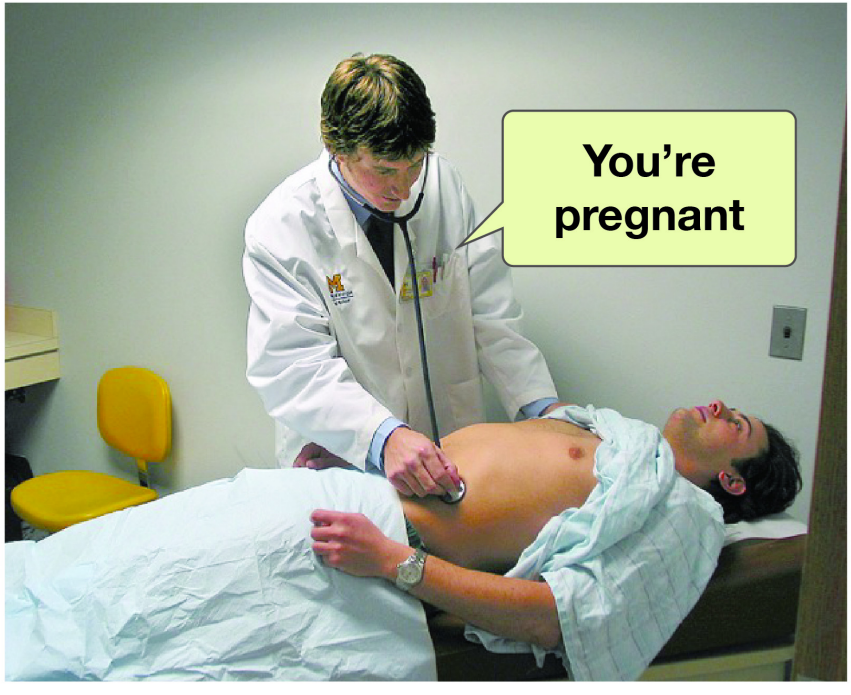
- **Use of Dormant Accounts**
  - Resource accounts or disabled user accounts
- **Changes to Logs**
  - System logs appear different from those of a backup
- **Presence of Hacker Tools**
  - Tools that can be used to compromise a system found on a host
  - Potentially the result of a penetration test
- **Notifications from a Partner or Peer**
  - Another organization reports an attack originating from your systems
- **Notification by Hacker**
  - An extortion attempt from a hacker, or corporate assets defaced

Identifying Real Incidents

- Each organization will create a process that is used to collect and evaluate incident candidates
- Some choose to have an “incident centre”
- Most organizations struggle with false-positives and event noise, which is an event that does not rise to the level of incident
- By its nature incident handling will generate false-positives and event noise, but with experience and system tuning, the rates of these events can be kept to a manageable level

False Positives

Type I error
(false positive)



Type II error
(false negative)

False Positives

Common sources of false-positive events:

- **Placement**
  - An IDPS that is placed outside of a firewall boundary is likely to see a large number of attempted attacks
  - Many of these may be filtered by the firewall
- **Policy**
  - Some tools used for network operations may produce signatures that are classified as attack signatures
- **Lack of Awareness**
  - Users may not be aware of policy limitations, or fail to interpret them correctly

Detecting Incidents
End of Part 1

INFO-6081 – Monitoring & Incident Response

FANSHAWE

Detecting Incidents Part 2

INFO-6081 – Monitoring & Incident Response

FANSHAWE

Intrusion Detection and Prevention Systems

- Intrusion Detection and Prevention Systems are systems that are used to determine if the network resources are used according to organizational policy
- An intrusion is a type of attack that serves to gain unauthorized access to a system or disrupt the normal operations of the network
- IDPS produce alerts when an intrusion is detected, and IPS can perform actions on the offending traffic

Intrusion Detection and Prevention Systems

In addition its primary function, IDPS can be used for the following purposes:

- **Identifying security policy problems**
  - Duplicating firewall rulesets can alert to a failure in firewall filtering
- **Documenting the existing threat to an organization**
  - IDPS logs can identify the frequency and characteristics of an attack
- **Deterring individuals from violating security policies**
  - If users know that they are being monitored, they are less likely to commit policy violations

Incident Decision Making

When analyzing and validating events to determine which should be classified as an incident, consider the following:

- **Profile Networks and Systems**
  - Measure the characteristics of expected activity so that changes can be easily identified
- **Understand Normal Behaviors**
  - Know what normal behavior is, so that abnormal behavior can be easily recognized

Incident Decision Making

- **Use Centralized Logging and Create a Log Retention Policy**
  - Centralized logging can help prevent an attacker from “covering their tracks”
- **Perform Event Correlation**
  - Correlating events across multiple hosts provide a more detailed picture of the actions the intruder
- **Keep All Host Clocks Synchronized**
  - Use NTP to synchronize clocks with a trusted time source

Incident Decision Making

- **Maintain and Use a Knowledge Base of Information**
  - Information about previous incidents and responses can be quickly accessed in times of need
- **Use Internet Search Engines for Research**
  - Use the knowledge and experience of thousands of professionals that share their experiences online
- **Run Packet Sniffers to Collect Additional Data**
  - Full content data can aid when determining what actions an intruder took

Incident Decision Making

- **Consider Filtering the Data**
  - Helps to prevent information overload
- **Consider Experience as Being Irreplaceable**
  - An experienced incident handler can usually identify the significance of an event faster than a novice
- **Create a Diagnosis Matrix for Less Experienced Staff**
  - Quick reference guides for less experienced handlers ensure that a potential incident is not overlooked

Incident Decision Making

- **Seek Assistance From Others**
  - If the team is unable to determine the full cause and nature of an incident, they should consult with internal or external resources to ensure it is contained and eradicated
  - Internal resources should be experts in dealing with the systems in question
  - External resources may have encountered the same or similar situations in the past

Detect Compromised Software

- Systems that monitor the network, servers or other components can themselves be compromised
- On such systems, it is important to verify the integrity of the host providing the service
- A separate HIDPS sensor located on the IDPS host can monitor the host and alert to any potential intrusion

Watch for Unexpected Behavior

- Notify users that monitoring is in use
- Investigate alerts from network and systems alert mechanisms and error reports
- Review performance metrics and compare results to baselines
- Identify unexpected, unusual or suspicious traffic
- Identify unexpected, unusual or suspicious user activity
- Conduct periodic network mapping
- Perform periodic vulnerability scanning to detect know vulnerabilities

Watch for Unexpected Behavior

- Use HIDS to monitor systems for suspicious file activity or filesystem changes
- Investigate unauthorized hardware attached to computers
- Inspect physical resources for signs of unauthorized activity

Summary

- When an adverse event becomes a threat to the ongoing operation of an organization, it is classified as an incident
- Incidents can be classified into some of the following categories: DoS, Malicious Code, Unauthorized Access, etc.
- Potential incidents are referred to in terms of indicators or precursors
- False positives are a reality of inspection and systems should be trained to minimize their occurrences
- IDPS can be used to feed event data and prove compliance
- Many systems and data sources are used to make a decision about potential incidents

Detecting Incidents
End of Lesson 4

INFO-6081 – Monitoring & Incident Response

FANSHAWE

References

- Bejtlich, R. (2013). Chapter 4: Distributed Deployment. In The practice of network security monitoring understanding incident detection and response. San Francisco: No Starch Press.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. doi: 10.6028/nist.sp.800-61r2
- Grance, T., Kent, K. A., & Kim, B. (2004). Computer security incident handling guide. Computer Security Incident Handling Guide. doi: 10.6028/nist.sp.800-61

References

- Price, P., Jhangiani, R., & Chiang, I.-C. A. (2015). *Research methods in psychology*. Retrieved from https://opentextbc.ca/researchmethods/
- Scarfone, K. A., & Mell, P. M. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). doi: 10.6028/nist.sp.800-94
- Security Onion Solutions. (2020). Security Onion: Security Onion Documentation. Evans, GA: Author.

References

- Whitman, M. E., Mattord, H. J., & Green, A. (2014). Chapter 5: Incident Response: Detection and Decision Making. Principles of incident response and disaster recovery (2nd ed.). Australia: Course Technology Cengage Learning.