COMP 6448 - Week 3

Security Engineering Masterclass

Vulnerabilities:

- Vulnerabilities exist because developers make mistakes.
- Budget constraints for developers.
- Majority of attackers have little or much money to spend. We want to win the easy targets.

2017	10	2007	2004
Injection	Injection	Cross-Site Scripting (XSS)	Unvalidated Input
Broken Authentication	Broken Authentication and Session Management	Injection Flaws	Broken Access Control
Sensitive Data Exposure	Cross-Site Scripting (XSS)	Broken Authentication and Session Management	Malicious File Execution	Broken Authentication and Session Management
XML External Entities (XXE)	Insecure Direct Object References	Insecure Direct Object References	Insecure Direct Object Reference	Cross Site Scripting
Broken Access Control	Security Misconfiguration	Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	Buffer Overflow
Security Misconfiguration	Sensitive Data Exposure	Security Misconfiguration	Information Leakage and Improper Error Handling	Injection Flaws
Cross-Site Scripting (XSS)	Missing Function Level Access Control	Insecure Cryptographic Storage	Broken Authentication and Session Management	Improper Error Handling
Insecure Deserialization	Cross-Site Request Forgery (CSRF)	Failure to Restrict URL Access	Insecure Cryptographic Storage	Insecure Storage
Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities	Insufficient Transport Layer Protection	Insecure Communications	Application Denial of Service
Insufficient Logging & Monitoring	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Failure to Restrict URL Access	Insecure Configuration Management

- Finding vulnerabilities is good, but fixing it or creating a tool to identify it is great.
- OWASP Juice Shop has a nice guide on doing SQLi.

CTF:

- File information/inspector will give some nice photo metadata
- Stenograph
- Signal?
- I love my dog

We get 10000s of SOC alerts each day. How do we find the vulnerable things?

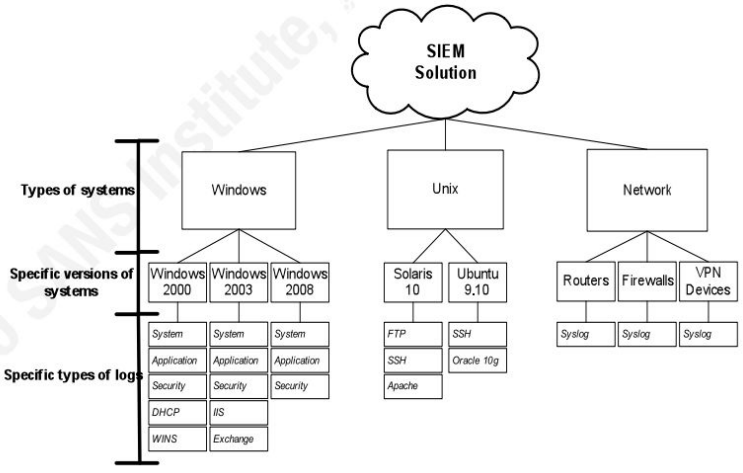
- We need to address issues within 72 hours.
- Challenge is to reduce time in triaging alerts.

Forensics Tools:

- Strings: Will look inside binary files and try to gather readable strings.
- Exiftool: A metadata extractor for photos, videos and audio.
- Binwalk: Can find hidden files inside zip files. `binwalk -e file.zip`
- Hex dump tool: Go find one on the web
- Steghide: Can reveal hidden messages in files. `steghide extract -sf`
- File: Can reveal what type of file is, regardless of the extension.

Information Security Management (ISM) Reading:

- Log Management Process:
  - User request
  - System response
  - Write system log
  - Write l… system
  - Correla… data. Generate alert.
  - System… alerts.
- Barriers to effe…
  - To mal… able, it must address the Five W's.
  - A basi… que of determining when the event occurred, who was involve… where did it take place and why it happened.
  - E.g. A poor example of SIEM is a failed logon event where the issue is identified (what) but the IP address of the username who attempted to login as not adequately answered (who).
  - Be wary of SIEM software that claims tens of thousands of events per seconde.
    - E.g. a firewall with one rule set to filter for a single service is much faster than a firewall set to filter thousands of rules where multiple nested groups exist in each rule.
  - In most instances SIEM correlation is a scheduled task and note performed as every new event is collected by the system.
    - E.g. Fraudulent ATM activity would take approximately 300 seconds to identify given the traffic and maybe another 60 seconds for a guard to go to the ATMs, by which time the user has already completed a transaction and left.
  - The data must actually be good for the SIEM system to work. Garbage in, garbage out.
  - Also need to manage the amount of data that goes through. Too much data will lead to poor performance.
- Dissecting use cases:
  - Take a top-down bottom up middle out approach.
    - Top down:



      - Group similar systems in each level of the tree.
      - The assign transport methods for each. In this case log files reside on the Windows and UNIX systems which must be read and sent to the SIEM solution.

- Bottom up:
  - Refers to the flow of information.
  - Each piece of information in a log file, such as an IP address is [illegible]ta point.
  - [illegible] is made up of one or more data points.

Lo	
Lo	
Lo	
Log verbosity level	
Log size average	
Log type	
Data points	
Application name	
Application version	
Operating System	
Rotation frequency	Real-time, hourly, daily, etc
Log standard defined	Link to the operating procedure

- Middle out:
  - Take the data points from the bottom up phase and match them to use cases across the different systems found in the enterprise.