Hunting Malware Across the Enterprise – 2 days (12 hours)

Objective: To identify security preparedness gaps due to indications of malware or APT compromises, or security architecture deficiencies.

Description: This course of instruction will demonstrate the methodology to conduct a Security Audit of enterprise computers. Host and Network Operating and File System artifacts will be identified and their significance to related examination techniques explained. The results of the Security Audit will be interpreted in order to evaluate the enterprise (and host-level) Security Architecture according to common regulatory and operating/best practices criteria. Software tools and related examination techniques will be provided, including:

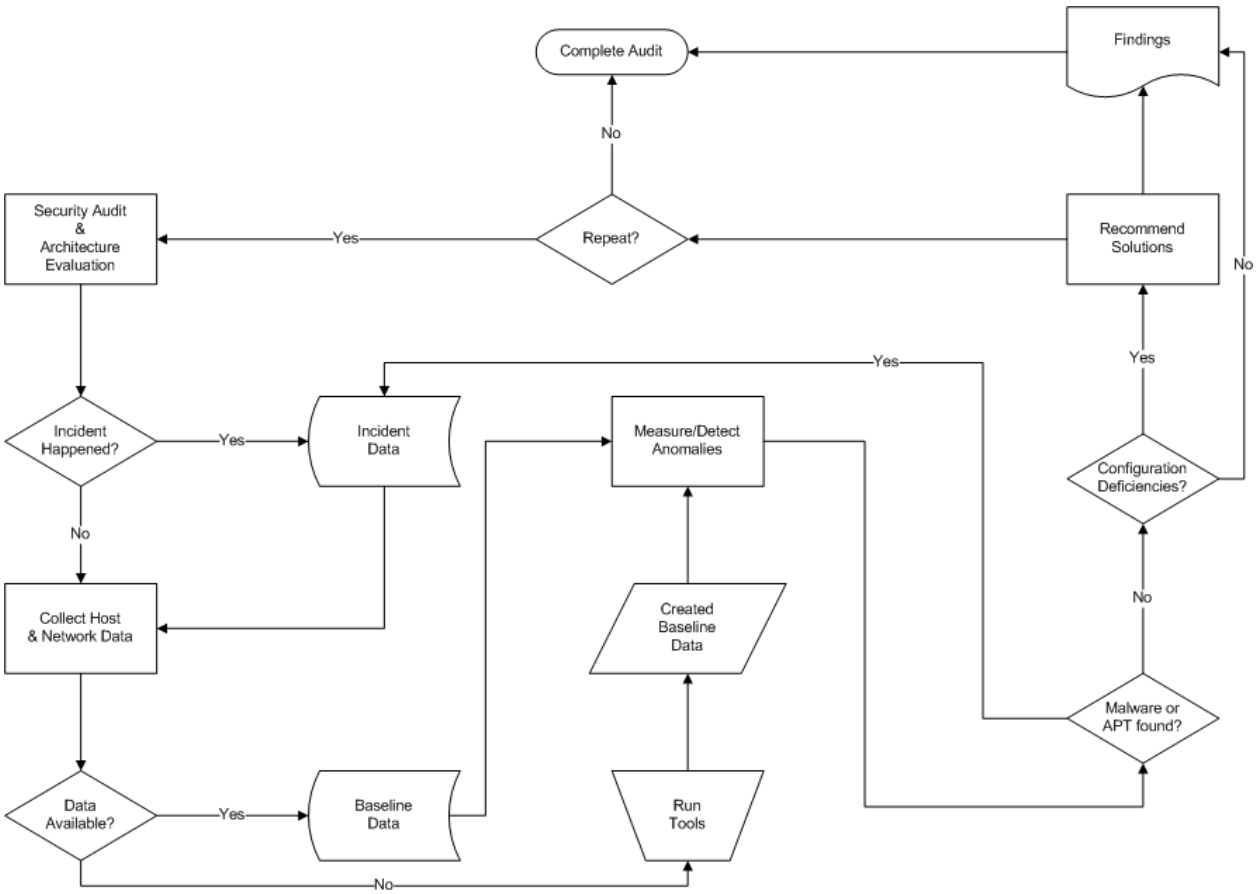
1. Host and Network security artifacts discovery (logs, samples, traces etc.)
2. File and Operating System baseline definition and anomaly detection
3. Network communications anomaly detection
4. Correlation and frequency analysis of audit data
5. Scheduling, coordination and repetition of audit
6. Audit tools and automation
7. Recognizing indicators of infection, compromise, and APT
8. Recommended response procedures to threat types (botnet, PWS, Infostealers, Trojans etc.)
9. Evaluating Host and Network security configuration
    a. Collect and load security artifacts for analysis (logs, configurations, tools output etc.)
    b. Perform analysis (communications, credentials usage, and host activities)
    c. Triage results by threat(s) detected
    d. Further examination of high-priority findings
    e. Security architecture compliance (Perimeter and Network controls, Events Correlation, User Access Controls, Antivirus/Antimalware, Data Leakage Prevention, Configuration Change Management, User Awareness, Honeypots, Threat Intelligence etc.)
10. Documenting findings and recommending security architecture remediation and user training

Required Experience: Windows/Linux system administration
Understanding of TCP/IP and network services
- NetBIOS/SMB
- HTTP/HTTPS
- FTP

Familiarity with Windows/Linux and Network logs
Basic SQL (MSSQL/SQLITE/MYSQL) programming
Understanding of forensic procedures (network and host – disk/memory)

Required Tools/Equipment: Laptop computer with Windows O/S and Administrator Rights
Internet access
MSSQL or MYSQL and related GUI (MSSQL Studio, RazorSQL etc.)
VMWare Workstation

Workflow:



Methodology:

- Leverage **tools** for efficiency of effort
  - Windows/Unix Operating System tools
  - Third-party utilities
  - SQL databases
- Leverage **intelligence** for efficiency of scale
  - Threat Intelligence (reputation, history etc.)
  - SQL correlation of artifacts (discovery/frequency)
  - Vendor Intelligence (malware analytics etc.)
  - Experience (botnets/APT/crimeware research)

Sample Workplan:

Security Audit	
	1. Coordinate with client to determine scope of audit (# of computers)
	2. Deliver script to facilitate host artifacts collection a. MFT or Dir /a /s %SystemDrive% b. Netstat c. DNS Cache d. Registry Keys e. Scheduled Tasks f. Antivirus logs
	3. Coordinate with client for network logs collection (as available) a. Proxy b. Firewall c. Intrusion Detection System d. Data Leakage Prevention System e. DNS f. Active Directory g. Antivirus Enterprise Console h. AntiMalware
	4. Collect host artifacts and logs in central storage location for processing
	5. Parse and load logs into SQL database for analysis
	6. Load blacklists (network and files) into SQL database to facilitate analysis
	7. Run SQL analysis: a. Network communications correlation with blacklist to identify known malicious actors i. Host Netstat & DNS Cache ii. Proxy / Firewall / IDS / DLP / DNS / AntiMalware b. Network communications frequency analysis to identify potential beaconing or unknown channels for investigation i. Host Netstat & DNS Cache ii. Proxy / Firewall / IDS / DLP / DNS / AntiMalware

	c. Extract all unique IP and DNS addresses and compare with Threat Intelligence to determine reputation of addresses d. Host correlation with blacklist (files) to identify known malicious content i. MFT ii. Registry Keys iii. Scheduled Tasks iv. Antivirus Logs e. Query directories of MFT for binaries for investigation i. %\TEMP\% ii. %\Temporary Internet Files\% iii. %\Recycler\% iv. %\Application Data\% f. Match Operating System binaries with cache folders to identify anomalous binaries for investigation g. Match Operating System binary names with Whitelist to identify anomalous binaries for investigation h. Match Registry Keys binary names with Whitelist to identify anomalous binaries for investigation i. Extract filepath and filenames from Antivirus logs to query as a list against all MFT entries – to identify lingering infections j. Query any services running from a location other than %system32% or %Program Files% - from Registry Keys k. Query any scheduled tasks running from a location other than %system32% or %Program Files% - from Registry Keys l. Query all %.rdp and %.bmc filepaths to document User Profiles and dates/times of usage m. Perform other queries as useful
	8. Based on results of SQL analysis, identify any computers that require further investigation and collect the following artifacts: a. Windows Event Logs b. NTUSER.DAT files c. Internet History files

	d. Memory Image e. Quarantined Virus files
	9. Examine additional data to determine if lingering infections exist, or indicators of APT exist. a. If infections then collect and submit malware samples to Antivirus vendor for pattern updates, then deploy update and verify that the infection is cleaned. b. If indicators of APT exist (anomalous File System usage or Operating System configurations, or unusual User Profile activity), then obtain forensic disk images of each computer to perform forensic investigation.
	10. Identify additional specific artifacts (addresses, filenames, dates of interest, Registry Keys, processes and resources, and Scheduled Tasks) and re-query the SQL database to ensure all compromised computers have been identified.
	11. Document findings including evidence of infection or compromise, and recommendations to reconfigure (or update) host or network services.
	12. Report findings and recommendations.

Security Architecture Evaluation	
	1. Deliver script to facilitate host artifacts collection a. SysInfo b. MSInfo32
	2. Coordinate with client to deliver configurations of: (note if any do not exist) a. Firewall b. Intrusion Detection System c. Data Leakage Prevention d. Active Directory e. Proxy f. DNS (internal/external) g. DHCP h. Antimalware i. Host UAC/ACL j. Network Storage UAC/ACL

	k. Honeypots
	3. Coordinate with client to deliver audit report from Antivirus Enterprise Console: a. Patterns in use b. Frameworks in use c. Compliance (include organizational definition) d. Console Logs (detections etc.)
	4. Perform differential analysis of configurations data to identify anomalous or dissimilar builds, versions, policies, or services: a. Network Devices b. Host Operating Systems c. Host File System UAC/ACL's
	5. Assess compliance (actual vs. reported) of Enterprise Antivirus protection
	6. Review Antivirus detections history to identify underperforming patterns or persistent infections, and potential compromise vectors
	7. Assess removable media policies and UAC controls
	8. Contrast AntiMalware and Antivirus Logs to identify gaps in detections, and/or underperforming patterns or policies
	9. Conduct tests: a. External network web services penetration b. External/Internal network scanning (services and ports) c. Phishing (attachment and/or link) d. USB drops
	10. Document and present results, including remediation recommendations a. Host services configuration b. Network services configuration c. Security Architecture services configuration d. User Awareness and Training