FOR508.1: Advanced Incident Response & Threat Hunting

• Real Incident Response Tactics
• Preparation: Key tools, techniques, and procedures that an incident response team needs to respond properly to intrusions
• Identification/Scoping: Proper scoping of an incident and detecting all compromised systems in the enterprise
• Containment/Intelligence Development: Restricting access, monitoring, and learning about the adversary in order to develop threat intelligence
• Eradication/Remediation: Determining and executing key steps that must be taken to help stop the current incident
• Recovery: Recording of the threat intelligence to be used in the event of a similar adversary returning to the enterprise
• Avoiding "Whack-A-Mole" Incident Response: Going beyond immediate eradication without proper incident scoping/containment
• Threat Hunting
• Hunting versus Reactive Response
• Intelligence-Driven Incident Response
• Building a Continuous Incident Response/Threat Hunting Capability
• Forensic Analysis versus Threat Hunting across endpoints
• Threat Hunt Team Roles
• ATT&CK - MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK(TM))
• Threat Hunting in the Enterprise
• Identification of Compromised Systems
• Finding Active and Dormant Malware
• Digitally Signed Malware
• Malware Characteristics
• Common Hiding Mechanisms
• Finding Evil by Understanding Normal
• Understanding Common Windows Services and Processes
• svchost.exe Abuse
• Incident Response and Hunting across Endpoints
• WMIC & PowerShell
• Incident Response and Hunting Endpoint Collection with Kansa
• Malware Defense Evasion and Identification
• Service Hijacking/Replacement
• Frequent Compilation
• Binary Padding
• Packing/Armoring
• Dormant Malware
• Signing Code with Valid Cert

• Anti-Forensics/Timestomping
• Malware Persistence Identification
• AutoStart Locations, RunKeys
• Service Creation/Replacement
• Service Failure Recovery
• Scheduled Tasks
• DLL Hijacking
• WMI Event Consumers
• More Advanced - Local Group Policy, MS Office Add-In, or BIOS Flashing
• Investigating WMI-Based Attacks
• WMI Overview
• WMI Attacks Across the Kill Chain
• Auditing the WMI Repository
• WMI File System and Registry Residue
• Command-Line Analysis and WMI Logs
• WMI Process Anomalies

FOR508.2: Intrusion Analysis

• Stealing and Utilization of Legitimate Credentials
o Pass the Hash
o Single Sign On (SSO) Dumping using Mimikatz
o Token Stealing
o Cached Credentials
o LSA Secrets
o Kerberos Attacks
o NTDS.DIT theft
• Advanced Evidence of Execution Detection
o Attacker Tactics, Techniques, and Procedures (TTPs) overserved through process execution
o Prefetch Recovery and Analysis
o Application Compatibility Cache (ShimCache)
o Amcache Registry Examination
• Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs)
o Compromising Credentials Techniques
o Remote Desktop Services Misuse
o Windows Admin Share Abuse
o PsExec Utilization
o Windows Remote Management Tool Techniques
o PowerShell Remoting/WMIC Hacking
o Vulnerability Exploitation
• Log Analysis for Incident Responders and Hunters
o Profiling Account Usage and Logons
o Tracking and Hunting Lateral Movement
o Identifying Suspicious Services
o Detecting Rogue Application Installation
o Finding Malware Execution and Process Tracking

o Capturing Command Lines and Scripts
o Powershell Transcript and ScriptBlock Logging
o PowerShell Script Obfuscation
o WMI Activity Logging
o Anti-Forensics and Event Log Clearing

FOR508.3: Memory Forensics in Incident Response & Threat Hunting

• Remote and Enterprise Incident Response
o Remote Endpoint Access in the Enterprise
o RemoteEndpoint Host-based Analysis
o Scalable Host-based Analysis (one analyst examining 1,000 systems) and Data Stacking
o Remote Memory Analysis
• Triage and Enpoint Detection and Reponse (EDR)
o Endpoint Triage Collection
o EDR Capabilities and Challenges
o EDR and Memory Forensics
• Memory Acquisition
o Acquisition of System Memory from both Windows 32/64 Bit Systems
o Hibernation and Pagefile Memory Extraction and Conversion
o Virtual Machine Memory Acquisition
o Memory changes in Windows 10
o Windows 10 Virtual Secure Mode
• Memory Forensics Analysis Process for Response and Hunting
o Identify Rogue Processes
o Analyze Process DLLs and Handles
o Review Network Artifacts
o Look for Evidence of Code Injection
o Check for Signs of a Rootkit
o Acquire Suspicious Processes and Drivers
• Memory Forensics Examinations
o Live Memory Forensics
o Advanced Memory Analysis with Volatility
o Webshell Detection Via Process Tree Analysis
o Code Injection, Malware, and Rootkit Hunting in Memory
o WMI and PowerShell Processes
o Extract Typed Adversary Command Lines
o Investigate Windows Services
o Hunting Malware Using Comparison Baseline Systems
o Find and Dump Cached Files from RAM
• Memory Analysis Tools
o Volatility
o Rekall & Google Rapid Response
o Comae Windows Memory Toolkit

FOR508.4: Timeline Analysis

• Timeline Analysis Overview
o Timeline Benefits
o Prerequisite Knowledge
o Finding the Pivot Point
o Timeline Context Clues
o Timeline Analysis Process
• Memory Analysis Timeline Creation
o Memory Timelining
• Filesystem Timeline Creation and Analysis
o MACB Meaning by Filesystem
o Windows Time Rules (File Copy versus File Move)
o Filesystem Timeline Creation Using Sleuthkit and fls
o Bodyfile Analysis and Filtering Using the mactime Tool
• Super Timeline Creation and Analysis
o Super Timeline Artifact Rules
o Program Execution, File Knowledge, File Opening, File Deletion
o Timeline Creation with log2timeline/Plaso
o log2timeline Input Modules
o log2timeline Output Modules
o Filtering the Super Timeline Using psort
o Targeted Super Timeline Creation
o Automated Super Timeline Creation
o Super Tmeline Analysis
o Volume Shadow Copy Timelining

FOR508.5: Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics Detection

• Cyber Threat Intelligence
o Importance of Cyber Threat Intelligence
o Understanding the "Kill Chain"
o Threat Intelligence Creation and Use During Incident Response and Threat Hunting
o Creation of Indicators of Compromise
o Incident Response Team Life-Cycle Overview
• Malware and Anti-Forensic Detection
o NTFS Filesystem Analysis
o Master File Table (MFT) Critical Areas
o NTFS System Files
o NTFS Metadata Attributes ($Standard_Information, $Filename, $Data)
o Rules of Windows Timestamps for $StdInfo and $Filename
o Timestomp detection via NTFS Timestamp Analysis
o Resident versus Nonresident Files
o Hidden data in Alternate Data Streams
o Finding Wiped/Deleted Files using Directory Listings and the $I30 file
o Filesystem Flight Recorders: Transaction Logging and the $Logfile and $UsnJrnl
o What Happens When Data Is Deleted from an NTFS Filesystem?

• Anti-Forensic Detection Methodologies
o MFT Anomalies
o Timeline Anomalies
o Deleted File
o Deleted Registry Keys
o File Wiping
o Adjusting Timestamps
• Identifying Compromised Hosts without Active Malware
o Rapid Data Triage Analysis
o Cyber Threat Intelligence and Indicators of Compromise Searching
o Evidence of Persistence
o Super-timeline Examination
o Packing/Entropy/Executable Anomaly/Density Checks
o System Logs
o Memory Analysis
o Malware Identification

FOR508.6: The APT Threat Group Incident Response Challenge

•The Intrusion Forensic Challenge will ask each incident response team to analyze multiple systems in an enterprise network with many endpoints.
•During the challenge, each incident response team will be asked to answer key questions and address critical issues in the different categories listed below, just as they would during a real breach in their organizations:
IDENTIFICATION AND SCOPING:
1. How and when did the APT group breach our network?
2. List all compromised systems by IP address and specific evidence of compromise.
3. When and how did the attackers first laterally move to each system?
CONTAINMENT AND THREAT INTELLIGENCE GATHERING:
4. How and when did the attackers obtain domain administrator credentials?
5. Once on other systems, what did the attackers look for on each system?
6. Find extracted email from executive accounts and perform damage assessment.
7. Determine what was stolen: Recover any archives exfiltrated, find encoding passwords, and extract the contents to verify extracted data.
8. Collect and list all malware used in the attack.
9. Develop and present security intelligence and host and network based indicators of compromise describing attacker tradecraft.
REMEDIATION AND RECOVERY:
10. What level of account compromised occurred. Is a full password reset required during remediation?
11. Based on the attacker techniques and tools discovered during the incident, what are the recommended steps to remediate and recover from this incident?
a. What systems need to be rebuilt?
b. What IP addresses need to be blocked?
c. What countermeasures should we deploy to slow or stop these attackers if they come back?
d. What recommendations would you make to detect these intruders in our network again?