Hacker Tools, Techniques, Exploits, and Incident Handling

Duration : 5 Days

- Live Windows examination
- Network investigation
- Memory investigation
- Malware investigation

Topics

Incident Response

- Common incident response mistakes
- Incident goals and milestones
- Post-incident activities

Digital Investigations

- Asking and answering the right questions
- Pivoting during an investigation
- Taking notes and writing reports
- Artifact and event-based timelines

Live Examination

- How to start, even with minimal information
- Examining a live environment
- Identifying abnormal activity

Digital Evidence

- Understanding what digital evidence is and how to collect it
- The role and elements of a chain of custody
- How to collect digital evidence

Network Investigations

- Analyzing packet captures using tcpdump
- Web proxy logs

Memory Investigations

- How to investigate memory images using the Volatility framework

Malware Investigations

- Basic approaches for investigating malware
- Best practices for working with malware

Monitoring the enIntroducing the MITRE ATT&CK Framework

- Attacker evolution and the network for tool, technique, and practice (TTP) mapping
- Using the MITRE ATT&CK Framework for smarter adversary assessment
- How we integrate SEC504 with the MITRE ATT&CK Framework

Reconnaissance

- What does your network reveal?
- Are you leaking too much information?
- Using certificate transparency for pre-production server identification
- Domain Name System harvesting
- Data gathering from job postings, websites, and government databases
- Identifying publicly compromised accounts
- FOCA for metadata analysis
- Aggregate OSINT data collection with SpiderFoot
- Mastering SHODAN searches for target discovery

Scanning

- Learn the techniques attackers use to enumerate your networks
- Locating and attacking personal and enterprise Wi-Fi
- Identifying and exploiting proprietary wireless systems
- Port scanning: small and large-scale enumeration tasks
- Quick and effective intel collection from web servers
- Characterizing network targets by OS, service, patch level
- Vulnerability scanning and finding prioritization

Enumerating Windows Active Directory Targets

- Windows Active Directory domain enumeration with BloodHound, SharpView
- Windows Command and Control with PowerShell Empire
- Operating system bridging from Linux to Windows targets
- Defending against SMB attacks with sophisticated Windows networking features
- Understanding SMB security features through Windows Server 2019

Defense Spotlight: DeepBlueCLI

- Using PowerShell to enumerate Windows systems
- Fast and effective Windows event log analysis
- Leveraging PowerShell output modifiers for reporting, analysis
- Characterizing common Windows scans and attacks against Windows servers

- Environment using snapshot and continuous recording tools

Exercises

- Online password guessing attacks with Hydra
- Defense Spotlight: Password guessing attack analysis with Elastic Stack
- Effective password cracking using Hashcat and John the Ripper
- Defense Spotlight: Domain Password Exposure Analysis with DPAT
- Data exfiltration, scanning, and pivoting with Netcat

Topics

Password Attacks

- How attackers bypass account lockout policies
- Choosing a target protocol for password guessing attacks
- Techniques for choosing password lists
- How attackers reuse compromise password lists against your organization
- Techniques for password cracking
- Recommendations for password cracking in your organization

Defense Spotlight: Log Analysis with Elastic Stack (formerly ELK)

- Establishing a lightweight log analysis system with Elasticsearch, Logstack, Beats, and Kibana
- Understanding Linux and UNIX authentication logging data
- Configuring Filebeat for simple log ingestion
- Using Kibana to identify password attack events
- Customizing Kibana visualization for effective threat hunting

Understanding Password Hashes

- Hashing algorithms, processes, and problems
- Understanding Windows hashing function through Windows Server 2019
- Password hash function strength and quality metrics
- Extracting Windows domain password hashes using built-in tools
- Getting password hashes from Windows 10 systems
- Decoding UNIX and Linux password hashes
- Mitigating GPU-based cracking: PBKDF2, bcrypt, and scrypt

Password Cracking Attacks

- John the Ripper: single, wordlist, incremental, and external cracking modes
- Cracking hashes with Hashcat: straight and combinator attacks
- Effective hash computation using mask attacks
- Breaking user password selection weaknesses with Hashcat rules
- Three simple strategies for defeating password cracking

Defense Spotlight: Domain Password Auditing

- Enumerating Windows domain settings with simple PowerShell one-line scripts
- Characterizing systemic behavior in user password selection
- Identifying bad password offenders in your organization
- Mitigating password sharing in Windows domains

- • Metasploit Attack and Analysis
- Software Update Browser Exploitation
- System Resource Utilization Database Analysis
- Command Injection Attack
- Cross Site Scripting Attack
- SQL Injection Attack
- SQL Injection Log Analysis

Topics

Using Metasploit for System Compromise

- Using the Metasploit framework for specific attack goals
- Matching exploits with reconnaissance data
- Deploying Metasploit Meterpreter Command & Control
- Identifying Metasploit exploit artifacts on the system and network

Drive-By and Watering Hole Attacks

- Examining the browser attack surface
- Identifying browser vulnerabilities with JavaScript
- Code-executing Microsoft Office attacks
- Backdooring legitimate code with attacker payloads

Defense Spotlight: System Resource Usage Monitor (SRUM)

- Assessing attacker activity with Windows 10 app history
- Extracting useful data from the protected SRUM database
- Converting raw SRUM data to useful post-exploit analysis

Web Application Attacks

- Account harvesting for user enumeration
- Command injection attacks for web server remote command injection
- SQL Injection: Manipulating back-end databases
- Session Cloning: Grabbing other users' web sessions
- Cross-Site Scripting: Manipulating victim browser sessions

Defense Spotlight: Effective Web Server Log Analysis

- Using Elastic Stack (ELK) tools for post-attack log analysis
- Configuring Filebeat for web server log consumption
- Using the Kibana Query Language (KQL) to identify custom web attacks
- Hunting for common SQL Injection attack signatures
- Decoding obfuscated attack signatures with CyberChef

- Endpoint Security Bypass

  - Evading EDR analysis with executable manipulation: ghostwriting
  - Manipulating Windows Defender for attack signature disclosure
  - Using LOLBAS to evade application whitelisting
  - Adapting Metasploit payloads on protected platforms

Pivoting and Lateral Movement

- Pivoting from initial compromise to internal networks
- Effective port forwarding with Meterpreter payloads
- Leveraging compromised hosts for internal network scanning, exploitation
- Windows netsh and attacker internal network access

Privileged Insider Network Attacks

- Leveraging initial access for network attacks
- Deploying packet sniffers, MITM attack tools
- Native packet capture on compromised Windows hosts
- Abusing weak protocols: DNS, HTTP
- Network service impersonation attacks with Flamingo
- Abusing Windows name resolution for password disclosure

Covering Tracks

- Maintaining access by manipulating compromised hosts
- Editing log files on Linux and Windows systems
- Hiding data in Windows ADS
- Network persistence through hidden Command & Control

Defense Spotlight: Real Intelligence Threat Analytics (RITA)

- Characterizing advanced Command & Control activity over the network
- Capturing and processing network data with Zeek
- Network threat hunting: beacons, long connections, strobes, and DNS analysis

Post-Exploitation Data Collection

- Harvesting passwords from compromised Linux hosts
- Password dumping with Mimikatz and EDR bypass
- Defeating Windows and macOS password managers

- Windows keystroke logging attacks
- Data exfiltration over blended network protocols

Where To Go From Here

- Techniques for solving the problem of needing time for study
- Understanding the Forgetting Curve dilemma
- Techniques for developing long-term retention from what you have learned
- Building study strategies for certification, applying your knowledge

- •

Hands-on Analysis

  - Exploiting user password misuse
  - Completing scanning, reconnaissance analysis
  - Using OSINT resources to collect information about a target network
  - Matching reconnaissance data with public exploits
  - Privilege escalation on Linux and Windows systems
  - Exploiting common Windows Domain vulnerabilities
  - Pillaging data on compromised systems
  - Pivoting from initial compromise to internal network access
  - Identifying attacker artifacts following a network compromise