SEC504.1: Incident Handling Step-by-Step and Computer Crime Investigation

Topics

Preparation

- Building an incident response kit
- Identifying your core incident response team
- Instrumentation of the site and system

Identification

- Signs of an incident
- First steps
- Chain of custody
- Detecting and reacting to insider threats

Containment

- Documentation strategies: video and audio
- Containment and quarantine
- Pull the network cable, switch and site
- Identifying and isolating the trust model

Eradication

- Evaluating whether a backup is compromised
- Total rebuild of the Operating System
- Moving to a new architecture

Recovery

- Who makes the determination to return to production?
- Monitoring to system
- Expect an increase in attacks

Special Actions for Responding to Different Types of Incidents

- Espionage
- Inappropriate use

Incident Record-keeping

- Pre-built forms
- Legal acceptability

Incident Follow-up

- Lessons learned meeting
- Changes in process for the future

SEC504.2: Computer and Network Hacker Exploits – Part 1

Topics

Reconnaissance

- What does your network reveal?
- Are you leaking too much information?
- Using forward and reverse Whois lookups, ARIN, RIPE, and APNIC
- Domain Name System harvesting
- Data gathering from job postings, websites, and government databases
- Recon-ing
- Pushpin
- Identifying publicly compromised accounts
- Maltego
- FOCA for metadata analysis
- Aggregate OSINT data collection with SpiderFoot

Scanning

- Locating and attacking personal and enterprise Wi-Fi
- Identifying and exploiting proprietary wireless systems
- Rubber Duckie attacks to steal Wi-Fi profiles
- War dialing with War-VOX for renegade modems and unsecure phones
- Port scanning: Traditional, stealth, and blind scanning
- Active and passive operating system fingerprinting
- Determining firewall filtering rules
- Vulnerability scanning using Nessus and other tools
- Distributing scanning using cloud agents for blacklist evasion

Intrusion Detection System (IDS) Evasion

- Foiling IDS at the network level
- Foiling IDS at the application level: Exploiting the rich syntax of computer languages
- Web Attack IDS evasion tactics
- Bypassing IDS/IPS with TCP obfuscation techniques

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

SEC504.3: Computer and Network Hacker Exploits – Part 2

Topics

Physical-layer Attacks

- Clandestine exploitation of exposed USB ports
- Simple network impersonation for credential recovery
- Hijacking password libraries with cold boot recovery tools

Gathering and Parsing Packets

- Active sniffing: ARP cache poisoning and DNS injection
- Bettercap
- Responder
- LLMNR poisoning
- WPAD attacks
- DNS cache poisoning: Redirecting traffic on the Internet
- Using and abusing Netcat, including backdoors and insidious relays
- IP address spoofing variations
- Encryption dodging and downgrade attacks

Operating System and Application-level Attacks

- Buffer overflows in-depth
- The Metasploit exploitation framework
- AV and application whitelisting bypass techniques

Netcat: The Attacker's Best Friend

- Transferring files, creating backdoors, and shoveling shell
- Netcat relays to obscure the source of an attack
- Replay attacks

Endpoint Security Bypass

- How attackers use creative office document macro attacks
- Detection bypass with Veil, Magic Unicorn
- Putting PowerShell to work as an attack tool
- AV evasion with Ghostwriting
- Attack tool transfiguration with native binaries

SEC504.4: Computer and Network Hacker Exploits – Part 3

Topics

Password Cracking

- Password cracking with John the Ripper
- Hashcat mask attacks
- Modern Windows Pass-the-Hash attacks
- Rainbow Tables
- Password guessing and spraying attacks

Web Application Attacks

- Account harvesting
- SQL Injection: Manipulating back-end databases
- Session cloning: Grabbing other users' web sessions
- Cross-site scripting

Denial-of-Service Attacks

- Distributed Denial of Service: Pulsing zombies and reflected attacks
- Local Denial of Service

SEC504.5: Computer and Network Hacker Exploits – Part 4

Topics

Maintaining Access

- Backdoors: Using Poison Ivy, VNC, Ghost RAT, and other popular beasts
- Trojan horse backdoors: A nasty combo
- Rootkits: Substituting binary executables with nasty variations
- Kernel-level Rootkits: Attacking the heart of the Operating System (Rooty, Avatar, and Alureon)

Covering the Tracks

- File and directory camouflage and hiding
- Log file editing on Windows and Unix
- Accounting entry editing: UTMP, WTMP, shell histories, etc.
- Covert channels over HTTP, ICMP, TCP, and other protocols
- Sniffing backdoors and how they can really mess up your investigations unless you are aware of them
- Steganography: Hiding data in images, music, binaries, or any other file type
- Memory analysis of an attack

Putting It All Together

- Specific scenarios showing how attackers use a variety of tools together
- Analyzing scenarios based on real-world attacks
- Learning from the mistakes of other organizations
- Where to go for the latest attack info and trends

SEC504.6: Hacker Tools Workshop

Topics

Hands-on Analysis

- Nmap port scanner
- Nessus vulnerability scanner
- Network mapping
- Netcat: File transfer, backdoors, and relays
- Microsoft Windows network enumeration and attack
- More Metasploit
- Exploitation using built in OS commands
- Privilege escalation
- Advanced pivoting techniques