- SEC504.1: Incident Response and Cyber Investigations

  Incident Response

  - Case study: Argous Corporation compromise
  - Dynamic Approach to Incident Response
  - Investigative analysis: Examining incident evidence

  Digital Investigations

  - Techniques for digital investigation
  - Establishing an incident timeline
  - Investigation efficiency: Data reduction

  Live Examination

  - Identifying suspicious Windows processes
  - Correlating network and persistence activity
  - Enumerating Windows auto-start extensibility points
  - Leveraging Sysinternals for live Windows examinations

  Network Investigations

  - Identifying compromised host beaconing with proxy server logs
  - Filtering network activity to identify indicators of compromise
  - Assessing encrypted network traffic with multiple data sources
  - Building the incident timeline

  Memory Investigations

  - Collecting volatile memory from a compromised host
  - Conducting offline analysis of attacker persistence
  - Using Volatility to inspect attacker malware

  Malware Investigations

  - Assessing attacker malware in a custom test environment
  - Using snapshot and continuous recording tools
  - Inspecting malware actions with RegShot and Procmon
  - Identifying malicious code on Windows

  Cloud Investigations

  - Steps for conducting a cloud security incident investigation

- Essential cloud logging assets for incident response
- Data collection and isolation for compromise assessment
- Applying cloud recovery and remediation following an incident
- Complete cloud compromise incident response walkthrough

Bootcamp: Linux Olympics

- Building command line skills at your own pace
- Working with Linux file systems and permissions
- Using JQ to parse and filter JSON data
- Using file parsing tools, including grep, cut, and awk
- Linux compromise incident response walkthrough

SEC504.2: Recon, Scanning, and Enumeration Attacks

MITRE ATT&CK Framework Introduction

- Using ATT&CK to guide an incident response investigation
- Staying current with changing attack techniques
- Leveraging ATT&CK for threat intelligence

Open-Source Intelligence

- Enumerating targets without being detected
- Host identification through domain and public certificate authority data
- User account compromise assessment
- Automating open-source intelligence collection with SpiderFoot

DNS Interrogation

- Mining public DNS servers for organization data
- Automating host enumeration with dns-brute
- DNS server log inspection for attack identification
- Creative host identification using manual and automated tools

Website Reconnaissance

- Information-gathering from public websites
- Parsing Exchangeable Image File Format (EXIF) data from public documents
- Optimizing search engine reconnaissance interrogation
- Abstracting attack identification using public sources
- Limiting website-sensitive data disclosure

Network and Host Scanning with Nmap

- Host enumeration and discovery with Nmap

- Internal and external network mapping and visualization
- Minimizing network activity to avoid detection
- Deep host assessment with Nmap Scripting Engine tools

Cloud Spotlight: Cloud Scanning

Enumerating shadow cloud targets

- Accelerating scans with Masscan
- Walkthrough: Scanning Amazon Web Services for target discovery
- Attributing cloud hosts to a target organization
- Visual representation of identified targets with EyeWitness

Server Message Block (SMB) Sessions

- Understanding Windows SMB: Essential skill development
- Identifying SMB attacks against Windows
- Using built-in tools for SMB password guessing attacks
- Enumerating Windows domains using SharpView and BloodHound
- Understanding SMB security features

Defense Spotlight: DeepBlueCLI

- Identifying attacks using Windows Event Logs
- Differentiating attacks from false positives
- Remote host assessment for compromise identification
- Tips for fast assessment to begin incident analysis

SEC504.3: Password and Access Attacks

Password Attacks

- Password attack trifecta: Guessing, spray, and credential stuffing
- Techniques for bypassing password attack defenses
- Understanding real-world authentication attacks

Understanding Password Hashes

- Weaknesses in Windows password hash formats
- Collecting password hashes in Windows, Linux, and cloud targets
- Mitigating GPU-based password cracking with scrypt and Argon2

Password Cracking

- Recovering passwords from hashes with John the Ripper and Hashcat
- Accelerating password cracking with GPUs and cloud assets

- Effective cracking with password policy masks
- Multi-factor authentication and password cracking implications

Defense Spotlight: Domain Password Audit Tool (DPAT)

- Password cracking as a defense opportunity with the DPAT
- Collecting Windows domain hashes for security analysis
- Identifying systemic vulnerabilities in password selection
- Safely reporting on password selection faults

Cloud Spotlight: Insecure Storage

- Case study: Cloud bucket storage exposure
- Understanding cloud storage for Amazon Web Services, Azure, and Google Compute
- Discovering insecure bucket storage
- Walkthrough: Insecure storage to website persistence compromise
- Identifying insecure cloud storage access

Multi-purpose Netcat

- Internal data transfer to evade monitoring controls
- Pivoting and lateral movement
- Listener and reverse TCP backdoors on Linux and Windows
- Detailed look at attacker post-compromise techniques

SEC504.4: Public-Facing and Drive-By Attacks

Metasploit Framework

- Using Metasploit to identify, configure, and deliver exploits
- Selecting payloads that grant access while evading defenses
- Establishing and using Command & Control (C2) victim access
- Identifying Metasploit and Meterpreter fingerprints for incident response

Drive-By Attacks

- Phishing and malicious Microsoft Office files
- Leveraging a watering hole to attack victim browsers
- Case study: Control system attack through watering hole forum compromise
- Building extensible payloads for effective attacks
- Customizing exploits for defense bypass

Defense Spotlight: System Resource Usage Monitor

- Leveraging Windows diagnostics for incident response

- Assessing incident network activity using built-in Windows data
- Case study: Data theft and terminated employee workstation analysis

Command Injection

- Compromising websites with command injection
- Walkthrough: Falsimentis community service website attack
- Applying command injection in non-website targets
- Attack access enumeration through command injection
- Auditing web applications for command injection flaws

Cross-Site Scripting (XSS)

- Exploiting victim browsers through server flaws
- Classifying XSS types for opportunistic or target attacks
- Cookie theft, password harvesting, and camera/microphone capture attacks
- Using content security policies (CSP) to stop XSS

SQL Injection

- Understanding SQL constructs and developer errors
- Extracting data through SQL injection
- Using Sqlmap to automate vulnerability discovery
- SQL injection against cloud databases: Relational Database Service (RDS), Spanner, Azure SQL

Cloud Spotlight: SSRF and IMDS Attacks

- Identifying server-side request forgery vulnerabilities
- Understanding common requests vs. server-side requests
- Walkthrough: Falsimentis federated SSO attack
- Obtaining cloud keys through IMDS attacks

SEC504.5: Evasion and Post-Exploitation Attacks

Endpoint Security Bypass

- Applying ghostwriting to evade signature detection
- Evading application safelist controls
- Using signed executables to evade endpoint controls
- Getting the most value from Endpoint Detection and Response (EDR) platforms

Pivoting and Lateral Movement

- Using Metasploit features for lateral movement
- Attacker detection evasion through pivoting

- Using Linux and Windows features for advanced exploitation
- Command & Control (C2) for privileged internal access

Hijacking Attacks

- Exploiting privileged LAN access
- Attacking default Windows vulnerable protocols
- Password harvesting on the LAN

Covering Tracks

- Hiding collected data on Windows and Linux
- Log editing techniques for both simple and complex log formats
- Building tamper-proof logging platforms

Establishing Persistence

- Exploiting Windows Silent Process Exit
- Windows Management Instrumentation (WMI) Event Subscription persistence techniques
- Exploiting Windows Active Directory: Golden Ticket attacks
- Web shell access and multi-platform persistence
- Cloud keys and backdoor accounts in Azure, Amazon Web Services, and Google Compute

Defense Spotlight: Real Intelligence Threat Analytics

- Threat hunting through network analysis
- Identifying beacons and C2 on your network
- Characterizing network oddities: Long connections
- Catching DNS exfiltration and access attacks

Data Collection

- Linux and Windows post-exploitation password harvesting
- Evading detection controls: Mimikatz
- Attacking password managers on Windows and macOS
- Keystroke logging attacks

Cloud Spotlight: Cloud Post-Exploitation

- Privilege enumeration and escalation in cloud environments
- Identifying stealthy backdoors in Azure
- Using cloud attack frameworks: Pacu and GCP PrivEsc
- Case study: Access to database dumping in Google Compute
- Built-in tools for data access: Microsoft 365 Compliance Search

- Assessing your cloud deployment for vulnerabilities

Where to Go from Here

- Tips for developing long-term recall and memory retention
- Applying spaced repetition theory using Anki
- Staying motivated and finding time for skill development
- Recommendations for passing your certification exam

SANS SEC560

- 1: Comprehensive Pen Test Planning, Scoping, and Recon
- The Mindset of the Professional Pen Tester
- Building a World-Class Pen Test Infrastructure
- Creating Effective Pen Test Scopes and Rules of Engagement
- Detailed Recon Using the Latest Tools
- Mining Search Engine Results
- Reconnaissance of the Target Organization, Infrastructure, and Users
- Automating Reconnaissance with Spiderfoot
- 2: In Depth Scanning
- Tips for Awesome Scanning
- Tcpdump for the Pen Tester
- Nmap In-Depth: The Nmap Scripting Engine
- Version Scanning with Nmap
- Identifying insecurities in Windows with GhostPack Seatbelt
- False-Positive Reduction
- Netcat for the Pen Tester
- Initial Access
- Password Guessing, Spraying, and Credential Stuffing
- 3: Exploitation
- Comprehensive Metasploit Coverage with Exploits, Stagers, and Stages
- Strategies and Tactics for Anti-Virus Evasion and Application Control Bypass
- In-Depth Meterpreter Analysis, Hands-On
- Implementing Port Forwarding Relays for Merciless Pivots
- How to Leverage PowerShell Empire to Plunder a Target Environment
- Lateral Movement with WMI and SC
- 4: Password Attacks and Merciless Pivoting
- Password Attack Tips
- Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems
- Pivoting through Target Environments
- Extracting Hashes and Passwords from Memory with Mimikatz Kiwi
- PowerShell’s Amazing Post-Exploitation Capabilities
- Tips for Effective Reporting
- 5: Domain Domination and Azure Annihilation
- Kerberos Authentication Protocol
- Poisoning Multicast Name Resolution with Responder

- Domain Mapping and Exploitation with Bloodhound
- Effective Domain Privilege Escalation
- Persistent Administrative Domain Access
- Azure Authentication Principles and Attacks
- Azure AD Integration with On-Premise Domain
- Azure Applications and Attack Strategies
- 6: Penetration Test and Capture-the-Flag Workshop

SANS SEC542

- 1: Introduction and Information Gathering
- Overview of the web from a penetration tester's perspective
- Web application assessment methodologies
- The penetration tester's toolkit
- WHOIS and DNS reconnaissance
- Open source intelligence (OSINT)
- The HTTP protocol
- Secure Sockets Layer (SSL) configurations and weaknesses
- Interception Proxies
- Proxying SSL through BurpSuite Pro and Zed Attack Proxy
- Heartbleed exploitation
- SEC 542.2: Configuration, Identity, and Authentication Testing
- Target profiling
- Collecting server information
- Logging and Monitoring
- Learning tools to spider a website
- Analyzing website contents
- Brute forcing unlinked files and directories
- Fuzzing
- Web authentication mechanisms
- Username harvesting and password guessing
- Burp Intruder
- SEC 542.3: Injection
- Session management and attacks
- Authentication and authorization bypass
- Mutillidae
- Command Injection
- Directory traversal
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Insecure Deserialization
- SQL injection
- Blind SQL injection
- Error-based SQL injection
- Exploiting SQL injection
- SQL injection tools: sqlmap

- SEC 542.4: JavaScript and XS
- XML External Entity (XXE)
- Cross-Site Scripting (XSS)
- Browser Exploitation Framework (BeEF)
- AJAX
- XML and JSON
- Document Object Model (DOM)
- API attacks
- Data attacks
- SEC 542.5: CSRF, Logic Flaws, and Advanced Tools
- Cross-Site Request Forgery (CSRF)
- Python for web app penetration testing
- WPScan
- ExploitDB
- BurpSuite Pro scanner
- Metasploit
- When tools fail
- Business of Penetration Testing
- SEC 542.6: Capture the Flag