SEC560.1: Comprehensive Pen Test Planning, Scoping, and Recon

• Tour of the SANS Slingshot Penetration Testing Virtual Machine
• Formulating an Effective Scope and Rules of Engagement
• Document Metadata Treasure Hunt
• Utilizing Recon-ng to Plunder DNS for Useful Information

SEC560.2: In-Depth Scanning

• Getting the Most Out of Nmap
• OS Fingerprinting and Version Scanning In-Depth
• The Nmap Scripting Engine
• The Nessus Vulnerability Scanner
• Netcat for the Pen Tester
• PowerShell for the Pen Tester

SEC560.3: Exploitation

• Client-Side Attacks with Metasploit
• Exploiting Network Services and Leveraging the Meterpreter
• Evading Anti-Virus Tools with the Veil Framework
• Metasploit Databases and Tool Integration
• Port Pivoting Relays
• Leveraging PowerShell Empire for Post Exploitation
• Creating Malicious Services and Leveraging the Wonderful WMIC Toolset

SEC560.4: Password Attacks and Merciless Pivoting

• Password Guessing and Spraying with THC-Hydra
• Metasploit Psexec, Hash Dumping and Mimikatz Kiwi Credential Harvesting
• Pivoting with Metasploit and SSH
• Password Cracking with John the Ripper and Hashcat
• Sniffing and Cracking Windows Authentication Exchanges
• Metasploit Pivoting and Mimikatz Kiwi for Credential Harvesting

SEC560.5: Domain Domination and Web App Pen Testing

• Kerberos Attacks
• Attacking Nearby Clients with Responder
• Domain Mapping and Exploitation with Bloodhound
• Effective Domain Privilege Escalation
• Domain Dominance
• Using the ZAP Proxy to Manipulate Custom Web Applications

• Leveraging Command Injection Flaws
• Exploiting SQL Injection Flaws to Gain Shell Access of Web Targets

SEC560.6: Penetration Testing Workshop

• Kerberos authentication protocol
• Poisoning multicast name resolution with Responder
• Domain Mapping and Exploitation with Bloodhound
• Effective Domain Privilege Escalation
• Persisting administrative domain access
• Using the ZAP Proxy to Manipulate Custom Web Applications
• Maximizing Effectiveness of Command Injection Testing
• Data Plundering with SQL Injection
• Leveraging SQL Injection to Perform Command Injection