Purple Team Tactics & Kill Chain Defenses

Duration: 40 hrs

Module 1: Introduction to Purple Teaming & Cyber Kill Chain

- Understanding the Red Team, Blue Team, and Purple Team Roles
- Cyber Kill Chain and MITRE ATT&CK Framework
- Adversary Emulation and Threat-Informed Defense
- Importance of Collaboration Between Offense and Defense

Module 2: Setting Up a Purple Team Lab

- Configuring an Isolated Testing Environment
- Deploying SIEM and EDR Solutions
- Installing Free and Open-Source Attack Emulation Tools
- Ensuring Legal and Ethical Considerations in Testing

Module 3: Reconnaissance & Threat Intelligence Collection

- OSINT Techniques for Threat Actor Profiling
- Passive vs. Active Reconnaissance Strategies
- Analyzing Threat Feeds and IOCs (AlienVault OTX, OpenCTI)
- Automating Recon with SpiderFoot and Recon-ng

Module 4: Weaponization & Initial Access Tactics

- Common Attack Vectors Used by Advanced Adversaries
- Exploit Development and Payload Creation
- Weaponizing Office Documents and LNK Files
- Simulating Initial Access with Atomic Red Team

Module 5: Execution & Privilege Escalation

- Fileless Malware & Living Off the Land Binaries
- Windows and Linux Privilege Escalation Techniques
- Abusing Misconfigured Services and Sudo Exploits
- Exploit Defense Evasion with Obfuscation Techniques

Module 6: Persistence & Defense Evasion

- Creating Scheduled Tasks and Registry Persistence

- Leveraging Rootkits and Hidden Services
- Bypassing Antivirus and EDR
- Detecting and Mitigating Persistence Mechanisms

Module 7: Credential Access & Lateral Movement

- Dumping Hashes and Credentials
- Pass-the-Hash and Pass-the-Ticket Attacks
- Lateral Movement via Remote Execution
- Detecting and Preventing Credential Theft

Module 8: Exfiltration & Impact

- Data Exfiltration Over Covert Channels
- Ransomware Simulations and Data Wiping Techniques
- Identifying and Responding to Data Breach Indicators
- Implementing Data Loss Prevention (DLP) Controls

Module 9: Threat Hunting & Incident Response

- Proactive Threat Hunting with Sigma, YARA, and Velociraptor
- Analyzing Windows Event Logs for Attack Traces
- Host and Network Forensics with Volatility and Suricata
- Containment and Remediation Strategies

Module 10: Building a Threat-Informed Defense Strategy

- Mapping Defense Tactics to the MITRE ATT&CK Framework
- Developing an Effective Detection and Response Playbook
- Enhancing SIEM Rules and Threat Intelligence Integration
- Measuring and Improving Purple Team Effectiveness

Module 11: Reporting & Lessons Learned

- Documenting Findings and Attack Simulations
- Creating Actionable Defense Recommendations
- Running Purple Team Tabletop Exercises
- Continuous Improvement Through Red and Blue Team Feedback