OffSec

# SOC-200 OSDA

*Security Operations and Defensive Analysis*

SOC-200 (Security Operations and Defensive Analysis) is a defensive-minded course covering the foundations of defending networks and systems against cyber threats. The course will focus on developing techniques for easily parsing and analyzing logs, which can be performed at scale. This more manual approach ensures a better understanding of how logs and artifacts are generated and how they can be queried in both Windows and Linux environments. Along the way, learners will develop an understanding of network security incidents and detection techniques.

| | |
|---|---|
| Attack Methodology Introduction | Build a foundation for understanding attacker behaviors and how to anticipate their moves in penetration testing engagements |
| Windows Endpoint Introduction | Discover common vulnerabilities in Windows endpoints and the attack vectors adversaries use to target them |
| Windows Server-Side Attacks | Learn methods commonly used to exploit critical services and vulnerabilities on compromised Windows servers |
| Windows Client-Side Attacks | Analyze browser-based attacks, vulnerabilities in software, and social engineering techniques attackers use to compromise user-facing sides of Windows systems |
| Windows Privilege Escalation | Exploit misconfigurations, software flaws, and zero-day vulnerabilities to increase your level of network control |
| Windows Persistence | Explore file system persistence, registry modifications, scheduled tasks, and other methods to retain the upper hand on attackers trying to stay hidden on compromised Windows systems |
| Linux Endpoint Introduction | Get familiar with common attack vectors used to target Linux endpoints, their security mechanisms, and potential vulnerabilities |
| Linux Server-Side Attacks | Understand how adversaries compromise Linux servers through privilege escalation methods, service exploits, and configuration weaknesses |
| Network Detections | Refine your evasion strategies by using firewalls, intrusion detection systems, and other tools to identify malicious activities |
| Antivirus Alerts and Evasion | Use advanced methods for evading antivirus solutions and minimize your digital footprint with techniques like payload obfuscation and exploit customization |
| Network Evasion and Tunneling | Avoid being detected by defensive technologies while making lateral network moves using covert communication methods and tunneling techniques |

| | |
|---|---|
| Active Directory Enumeration | Uncover potential attack paths with methods and tools that gather information about Active Directory's structure, users, groups, and permissions |
| Windows Lateral Movement | Leverage compromised credentials, remote execution, and network pivoting to expand control in Windows environments post-exploit |
| Active Directory Persistence | Explore hidden accounts, service manipulation, and other methods of blending into network fabrics using the same techniques as attackers |
| SIEM Part One | Building an ELK SIEM: Get hands-on with setting up a SIEM solution using the ELK stack (Elasticsearch, Logstash, and Kibana). Learn how to install, configure, and integrate these components to start collecting and analyzing security logs |
| SIEM Part Two | Operationalizing Your SIEM: Discover how to effectively manage and use your ELK SIEM deployment. Learn to collect logs from various sources, normalize data, create insightful dashboards, and set up alerts to proactively detect a security incident |