Foundational Security Operations and Defensive Analysis

Learning Module	Learning Units	Learning Objectives
Attacker Methodology	The Network as a Whole	• Gain a basic understanding of an enterprise network's DMZ
		• Learn about deployment environments
		• Understand the difference between core and edge network devices
		• Study virtual private networks and remote sites
	The Lockheed-Martin Cyber Kill-Chain	• Learn the parts of the Lockheed-Martin Cyber Kill-Chain
		• Apply the Kill-Chain to malware that performed cryptomining
		• Apply the Kill-Chain to three iterations of ransomware
	MITRE ATT&CK Framework	• Learn the classifications of the MITRE ATT&CK Framework
		• Review a case study of OilRig campaigns with MITRE ATT&CK principles
		• Review a case study of APT3 campaigns with MITRE ATT&CK principles
		• Review a case study of APT28 campaigns with MITRE ATT&CK principles
Windows Endpoint Introduction	Windows Processes	• Gain a basic understanding of programs running within Windows
		• Learn about Windows Services and their relationship with processes
		• Review the common states of Windows

		Services
	Windows Registry	• Review the configuration structure of the Windows Registry
		• Learn about the key-value pair relationship within the Windows Registry
		• Understand the value types and formats for Windows Registry keys
	Command Prompt, VBScript, and PowerShell	• Review the non-graphical means of interacting with Windows
		• Build batch scripts used for the command prompt to run local commands
		• Write a Visual Basic Script for collecting operating system
		• Build custom PowerShell functions
	Programming on Windows	• Review the Component Object Model in Windows
		• Learn about the development of the .NET Framework and .NET Core
	Windows Event Log	• Gain a basic understanding of Windows Event logs and sources
		• Review several Windows Event logs using the Windows Event Viewer
		• Use PowerShell to query Windows Event logs
	Empowering the Logs	• Gain a basic understanding of System Monitor (Sysmon)
		• Review Sysmon events using the Windows Event Viewer
		• Review Sysmon events using PowerShell
		• Use PowerShell Core in Kali Linux to query event logs remotely

Windows Server Side Attacks	Credential Abuse	• Learn about the Windows Security Account Manager
		• Learn about Windows Authentication
		• Understand the concept of suspicious login activity
		• Evaluate the behavior of brute-force login activity
	Web Application Attacks	• Learn about the configuration of Internet Information Services (IIS) in Windows
		• Evaluate logging artifacts of local file inclusion for attacking web servers
		• Evaluate logging artifacts of command injection and file upload for attacking web servers
	Binary Exploitation	• Learn about binary attacks through buffer overflows, and the artifacts they create
		• Study the use of Windows Defender Exploit Guard and how it protects against binary exploitation
		• Evaluate logging artifacts generated by the Windows Defender Exploit Guard
Windows Client Side Attacks	Attacking Microsoft Office	• Review social engineering and spearphishing techniques
		• Evaluate the use of Microsoft Office products to deploy phishing attacks
		• Review logging artifacts generated from a phishing attack
	Monitoring Windows PowerShell	• Gain a basic understanding of extended PowerShell logging capabilities
		• Understand the use of PowerShell module logging
		• Understand the use of PowerShell script block logging

		• Understand the use of PowerShell transcription
		• Review PowerShell logging artifacts generated from a phishing attack
		• Learn about PowerShell obfuscation and deobfuscation
Windows Privilege Escalation	Privilege Escalation Introduction	• Gain a basic understanding of Windows integrity levels and enumeration
		• Learn about Windows' User Account Control (UAC)
		• Evaluate a UAC bypass technique and the logging artifacts it creates
	Escalations to SYSTEM	• Perform an elevation using UAC Bypass and review the logging artifacts created
		• Learn about service permissions for privilege escalation along with relevant logging artifacts
		• Learn about unquoted service paths for privilege escalation along with logging artifacts
Linux Endpoint Introduction	Linux Applications and Daemons	• Understand what Linux daemons are
		• Understand the Syslog Framework components
		• Understand how the syslog and the journal daemon work together
		• Understand Linux web logging
	Automating the Defensive Analysis	• Understand how scripting can aid log analysis
		• Understand how to scale further scripting with DevOps tools
		• Understand how to put together what we learned in a real-life hunting scenario

Linux Server-Side Attacks	Credential Abuse	• Understand suspicious logins and how to detect them in logs
		• Understand brute-force password attacks and their log footprints
	Web Application Attacks	• Understand command injection attacks and their log footprint and detections
		• Understand SQL injection attacks and their log footprint and detections
Linux Privilege Escalation	User-side privilege escalation attack detections	• Understand how Linux privileges works
		• Understand how to detect privilege escalation attacks on user's configuration files
	System-side privilege escalation attack detections	• Understand how Linux privileges works
		• Understand how to detect privilege escalation attacks on user's configuration files
Windows Persistence	Persistence on Disk	• Understand and recognize Persisting via Windows Service
		• Understand and recognize Persisting via Scheduled Tasks
		• Understand and recognize Persisting by DLL-Sideloading/Hijacking
	Persistence in Registry	• Understand Using Run Keys
		• Understand Using Winlogon Helper
Network Detections	Intrusion Detection Systems	• Understand theory and methodologies behind IPS and IDS
		• Understand Snort rule syntax
		• Learn how to craft basic Snort rules
	Detecting Attacks	• Learn how to detect known vulnerabilities with Snort rules

		• Learn how to detect novel vulnerabilities with Snort rules
	Detecting C2 Infrastructure	• Understand the components of a C2 framework
		• Learn how to detect a well-known C2 communication through Snort rule sets
Antivirus Detections	Antivirus Basics	• Understand an Overview of Antivirus
		• Understand Signature-Based Detection
		• Understand Heuristic and Behavioral-Based Detection
	Antimalware Scan Interface (AMSI)	• Understand the basics of AMSI
		• Understand how attackers bypass AMSI
Active Directory Enumeration	Abusing Lightweight Directory Access Protocol	• Understand LDAP
		• Interact with LDAP
		• Enumerate Active Directory with PowerView
	Detecting Active Directory Enumeration	• Audit Object Access
		• Perform Baseline Monitoring
		• Use Honey Tokens
Network Evasion and Tunneling	Network Segmentation	• Understand the concept of network segmentation
		• Learn the benefits of network segmentation
		• Understand possible methods of implementing network segmentation in an enterprise
	Detecting Egress Busting	• Understanding the concept of egress filtering

		• Understanding an iptables firewall setup and application of egress filtering
		• Evaluate an "egress busting" technique and the logging artifacts it creates
	Port Forwarding and Tunneling	• Understand the concept of tunneling and port forwarding
		• Learn how attackers use it to compromise additional machines in the network
		• Understand the possible methods and tools attackers use to tunnel into the network and how to detect them
Windows Lateral Movement	Windows Authentication	• Understanding Pass the Hash
		• Understanding Brute Forcing Domain Credentials
		• Understanding Terminal Services
	Abusing Kerberos Tickets	• Understanding Pass the Ticket
		• Understanding Kerberoasting
Active Directory Persistence	Keeping Domain Access	• Understanding Domain Group Memberships
		• Understanding Domain User Modifications
		• Understanding Golden Tickets
SIEM Part One: Intro to ELK	Log Management Introduction	• Understand SIEM Concepts
		• Learn about the ELK Stack
		• Use ELK Integrations with OSQuery
	ELK Security	• Understand Rules and Alerts
		• Understand Timelines and Cases
SIEM Part Two: Combining the Logs	Phase One: Web Server Initial Access	• Detect enumeration and command injection

		• Implement Phase One detection rules
	Phase Two: Lateral Movement to Application Server	• Discover brute forcing and authentication
		• Create Phase Two detection rules
	Phase Three: Persistence and Privilege Escalation on Application Server	• Understand persistence and privilege escalation
		• Build Phase Three detection rules
	Phase Four: Perform Actions on the Domain Controller	• Identify dumping the AD database
		• Create Phase Four detection rules