Evasion Techniques and Breaching Defenses

Learning Module	Learning Units
Evasion Techniques and Breaching Defenses: General Course Information	About The PEN-300 Course
	Provided Material
	Overall Strategies for Approaching the Course
	About the PEN-300 VPN Labs
	About the OSEP Exam
	Wrapping Up
Operating System and Programming Theory	Programming Theory
	Operating System and Programming Theory
	Client Side Code Execution With Office
Client Side Code Execution With Office	Will You Be My Dropper

	Phishing with Microsoft Office
	Keeping Up Appearances
	Executing Shellcode in Word Memory
	PowerShell Shellcode Runner
	Keep That PowerShell in Memory
	Talking To The Proxy
	Wrapping Up
Client Side Code Execution With Windows Script Host	Creating a Basic Dropper in Jscript
	Jscript and C#
	In-memory PowerShell Revisited
	Wrapping Up
Process Injection and Migration	Finding a Home for Our Shellcode

	DLL Injection
	Reflective DLL Injection
	Process Hollowing
	Wrapping Up
Introduction to Antivirus Evasion	Antivirus Software Overview
	Simulating the Target Environment
	Locating Signatures in Files
	Bypassing Antivirus with Metasploit
	Bypassing Antivirus with C#
	Messing with Our Behavior
	Office Please Bypass Antivirus
	Hiding PowerShell Inside VBA
	Wrapping Up
Advanced Antivirus Evasion	Intel Architecture and Windows 10
	Antimalware Scan Interface
	Bypassing AMSI With Reflection in PowerShell
	Wrecking AMSI in PowerShell
	UAC Bypass vs Microsoft Defender

	Bypassing AMSI in JScript
	Wrapping Up
Application Whitelisting	Application Whitelisting Theory and Setup
	Basic Bypasses
	Bypassing AppLocker with PowerShell
	Bypassing AppLocker with C#
	Bypassing AppLocker with JScript
	Wrapping Up
Bypassing Network Filters	DNS Filters
	Web Proxies
	IDS and IPS Sensors
	Full Packet Capture Devices
	HTTPS Inspection
	Domain Fronting
	DNS Tunneling
	Wrapping Up
Linux Post-Exploitation	User Configuration Files
	Bypassing AV

	Shared Libraries
	Wrapping Up
Kiosk Breakouts	Kiosk Enumeration
	Command Execution
	Post-Exploitation
	Privilege Escalation
	Windows Kiosk Breakout Techniques
	Wrapping Up
Windows Credentials	Local Windows Credentials
	Access Tokens
	3 Kerberos and Domain Credentials
	Processing Credentials Offline
	Wrapping Up
Windows Lateral Movement	Remote Desktop Protocol
	Fileless Lateral Movement

	Wrapping Up
Linux Lateral Movement	Lateral Movement with SSH
	DevOps
	Kerberos on Linux
	Wrapping Up
Microsoft SQL Attacks	MS SQL in Active Directory
	MS SQL Escalation
	Linked SQL Servers
	Wrapping Up
Active Directory Exploitation	AD Object Security Permissions
	Kerberos Delegation
	Active Directory Forest Theory
	Burning Down the Forest
	Going Beyond the Forest

	Compromising an Additional Forest
	Wrapping Up
Combining the Pieces	Enumeration and Shell
	Attacking Delegation
	Owning the Domain
	Wrapping Up
Trying Harder: The Labs	Real Life Simulations
	Wrapping Up