Windows User Mode Exploit Development (OSED) Syllabus

Learning Module	Learning Units
Windows User Mode Exploit Development: General Course Information	About the EXP-301 Course
	Provided Materials
	Overall Strategies for Approaching the Course
	About the EXP-301 VPN Labs
	About the OSED Exam
	Wrapping Up
WinDbg and x86 Architecture	Introduction to x86 Architecture
	Introduction to Windows Debugger
	Accessing and Manipulating Memory from WinDbg
	Controlling the Program Execution in WinDbg
	Additional WinDbg Features
	Wrapping Up

Exploiting Stack Overflows	Stack Overflows Introduction
	Installing the Sync Breeze Application
	Crashing the Sync Breeze Application
	Win32 Buffer Overflow Exploitation
	Wrapping Up
Exploiting SEH Overflows	Installing the Sync Breeze Application
	Crashing Sync Breeze
	Analyzing the Crash in WinDbg
	Introduction to Structured Exception Handling
	Structured Exception Handler Overflows
	Wrapping Up
Introduction to IDA Pro	IDA Pro 101

	Working with IDA Pro
	Wrapping Up
Overcoming Space Restrictions: Egghunters	Crashing the Savant Web Server
	Analyzing the Crash in WinDbg
	Detecting Bad Characters
	Gaining Code Execution
	Finding Alternative Places to Store Large Buffers
	Finding our Buffer - The Egghunter Approach
	Improving the Egghunter Portability Using SEH
	Wrapping Up

Creating Custom Shellcode	Calling Conventions on x86
	The System Call Problem
	Finding kernel32.dll
	Resolving Symbols
	NULL-Free Position-Independent Shellcode (PIC)
	Reverse Shell
	Wrapping Up
Reverse Engineering for Bugs	Installation and Enumeration
	Interacting with Tivoli Storage Manager
	Reverse Engineering the Protocol
	Digging Deeper to Find More Bugs

	Wrapping Up
Stack Overflows and DEP Bypass	Data Execution Prevention
	Return Oriented Programming
	Gadget Selection
	Bypassing DEP
	Wrapping Up
Stack Overflows and ASLR Bypass	ASLR Introduction
	Finding Hidden Gems
	Expanding our Exploit (ASLR Bypass)
	Bypassing DEP with WriteProcessMemory
	Wrapping Up

Format String Specifier Attack Part I	Format String Attacks
	Attacking IBM Tivoli FastBackServer
	Reading the Event Log
	Bypassing ASLR with Format Strings
	Wrapping Up
Format String Specifier Attack Part II	Write Primitive with Format Strings
	Overwriting EIP with Format Strings
	Locating Storage Space

	Getting Code Execution
	Wrapping Up
Trying Harder: The Labs	Challenge 1
	Challenge 2
	Challenge 3
	Wrapping Up