Evasion Techniques and Breaching Defenses

Offensive Security
# Table of Contents

1. Evasion Techniques and Breaching Defenses: General Course Information
   1.1 About The PEN-300 Course
   1.2 Provided Material
      1.2.1 PEN-300 Course Materials
      1.2.2 Access to the Internal VPN Lab Network
      1.2.3 The Offensive Security Student Forum
      1.2.4 Live Support and RocketChat
      1.2.5 OSEP Exam Attempt
   1.3 Overall Strategies for Approaching the Course
      1.3.1 Welcome and Course Information Emails
      1.3.2 Course Materials
      1.3.3 Course Exercises
   1.4 About the PEN-300 VPN Labs
      1.4.1 Control Panel
      1.4.2 Reverts
      1.4.3 Client Machines
      1.4.4 Kali Virtual Machine
      1.4.5 Lab Behavior and Lab Restrictions
   1.5 About the OSEP Exam
   1.6 Wrapping Up

2. Operating System and Programming Theory
   2.1 Programming Theory
      2.1.1 Programming Language Level
      2.1.2 Programming Concepts
   2.2 Windows Concepts
      2.2.1 Windows On Windows
      2.2.2 Win32 APIs
      2.2.3 Windows Registry
   2.3 Wrapping Up

3. Client Side Code Execution With Office
   3.1 Will You Be My Dropper
      3.1.1 Staged vs Non-staged Payloads
      3.1.2 Building Our Droppers
      3.1.3 HTML Smuggling
3.2 Phishing with Microsoft Office
   3.2.1 Installing Microsoft Office
   3.2.2 Introduction to VBA
   3.2.3 Let PowerShell Help Us
3.3 Keeping Up Appearances
   3.3.1 Phishing PreTexting
   3.3.2 The Old Switcheroo
3.4 Executing Shellcode in Word Memory
   3.4.1 Calling Win32 APIs from VBA
   3.4.2 VBA Shellcode Runner
3.5 PowerShell Shellcode Runner
   3.5.1 Calling Win32 APIs from PowerShell
   3.5.2 Porting Shellcode Runner to PowerShell
3.6 Keep That PowerShell in Memory
   3.6.1 Add-Type Compilation
   3.6.2 Leveraging UnsafeNativeMethods
   3.6.3 DelegateType Reflection
   3.6.4 Reflection Shellcode Runner in PowerShell
3.7 Talking To The Proxy
   3.7.1 PowerShell Proxy-Aware Communication
   3.7.2 Fiddling With The User-Agent
   3.7.3 Give Me A SYSTEM Proxy
3.8 Wrapping Up
4 Client Side Code Execution With Windows Script Host
   4.1 Creating a Basic Dropper in Jscript
      4.1.1 Execution of Jscript on Windows
      4.1.2 Jscript Meterpreter Dropper
   4.2 Jscript and C#
      4.2.1 Introduction to Visual Studio
      4.2.2 DotNetToJscript
      4.2.3 Win32 API Calls From C#
      4.2.4 Shellcode Runner in C#
      4.2.5 Jscript Shellcode Runner
      4.2.6 SharpShooter
   4.3 In-memory PowerShell Revisited
4.3.1 Reflective Load

4.4 Wrapping Up

5 Process Injection and Migration

5.1 Finding a Home for Our Shellcode
   5.1.1 Process Injection and Migration Theory
   5.1.2 Process Injection in C#

5.2 DLL Injection
   5.2.1 DLL Injection Theory
   5.2.2 DLL Injection with C#

5.3 Reflective DLL Injection
   5.3.1 Reflective DLL Injection Theory
   5.3.2 Reflective DLL Injection in PowerShell

5.4 Process Hollowing
   5.4.1 Process Hollowing Theory
   5.4.2 Process Hollowing in C#

5.5 Wrapping Up

6 Introduction to Antivirus Evasion

6.1 Antivirus Software Overview

6.2 Simulating the Target Environment

6.3 Locating Signatures in Files

6.4 Bypassing Antivirus with Metasploit
   6.4.1 Metasploit Encoders
   6.4.2 Metasploit Encryptors

6.5 Bypassing Antivirus with C#
   6.5.1 C# Shellcode Runner vs Antivirus
   6.5.2 Encrypting the C# Shellcode Runner

6.6 Messing with Our Behavior
   6.6.1 Simple Sleep Timers
   6.6.2 Non-emulated APIs

6.7 Office Please Bypass Antivirus
   6.7.1 Bypassing Antivirus in VBA
   6.7.2 Stomping On Microsoft Word

6.8 Hiding PowerShell Inside VBA
   6.8.1 Detection of PowerShell Shellcode Runner
   6.8.2 Dechaining with WMI
6.8.3 Obfuscating VBA

6.9 Wrapping Up

7 Advanced Antivirus Evasion

7.1 Intel Architecture and Windows 10
7.1.1 WinDbg Introduction

7.2 Antimalware Scan Interface
7.2.1 Understanding AMSI
7.2.2 Hooking with Frida

7.3 Bypassing AMSI With Reflection in PowerShell
7.3.1 What Context Mom?
7.3.2 Attacking Initialization

7.4 Wrecking AMSI in PowerShell
7.4.1 Understanding the Assembly Flow
7.4.2 Patching the Internals

7.5 UAC Bypass vs Microsoft Defender
7.5.1 FodHelper UAC Bypass
7.5.2 Improving Fodhelper

7.6 Bypassing AMSI in JScript
7.6.1 Detecting the AMSI API Flow
7.6.2 Is That Your Registry Key?
7.6.3 I Am My Own Executable

7.7 Wrapping Up

8 Application Whitelisting

8.1 Application Whitelisting Theory and Setup
8.1.1 Application Whitelisting Theory
8.1.2 AppLocker Setup and Rules

8.2 Basic Bypasses
8.2.1 Trusted Folders
8.2.2 Bypass With DLLs
8.2.3 Alternate Data Streams
8.2.4 Third Party Execution

8.3 Bypassing AppLocker with PowerShell
8.3.1 PowerShell Constrained Language Mode
8.3.2 Custom Runspaces
8.3.3 PowerShell CLM Bypass
8.3.4 Reflective Injection Returns
8.4 Bypassing AppLocker with C#
  8.4.1 Locating a Target
  8.4.2 Reverse Engineering for Load
  8.4.3 Give Me Code Exec
  8.4.4 Invoking the Target Part 1
  8.4.5 Invoking the Target Part 2
8.5 Bypassing AppLocker with JScript
  8.5.1 JScript and MSHTA
  8.5.2 XSL Transform
8.6 Wrapping Up
9 Bypassing Network Filters
  9.1 DNS Filters
    9.1.2 Dealing with DNS Filters
  9.2 Web Proxies
    9.2.1 Bypassing Web Proxies
  9.3 IDS and IPS Sensors
    9.3.1 Case Study: Bypassing Norton HIPS with Custom Certificates
  9.4 Full Packet Capture Devices
  9.5 HTTPS Inspection
  9.6 Domain Fronting
    9.6.1 Domain Fronting with Azure CDN
    9.6.2 Domain Fronting in the Lab
  9.7 DNS Tunneling
    9.7.1 How DNS Tunneling Works
    9.7.2 DNS Tunneling with dnscat2
  9.8 Wrapping Up
10 Linux Post-Exploitation
  10.1 User Configuration Files
    10.1.1 VIM Config Simple Backdoor
    10.1.2 VIM Config Simple Keylogger
  10.2 Bypassing AV
    10.2.1 Kaspersky Endpoint Security
    10.2.2 Antiscan.me
  10.3 Shared Libraries
10.3.1 How Shared Libraries Work on Linux
10.3.2 Shared Library Hijacking via LD_LIBRARY_PATH
10.3.3 Exploitation via LD_PRELOAD
10.4 Wrapping Up

11 Kiosk Breakouts
11.1 Kiosk Enumeration
  11.1.1 Kiosk Browser Enumeration
11.2 Command Execution
  11.2.1 Exploring the Filesystem
  11.2.2 Leveraging Firefox Profiles
  11.2.3 Enumerating System Information
  11.2.4 Scratching the Surface
11.3 Post-Exploitation
  11.3.1 Simulating an Interactive Shell
11.4 Privilege Escalation
  11.4.1 Thinking Outside the Box
  11.4.2 Root Shell at the Top of the Hour
  11.4.3 Getting Root Terminal Access
11.5 Windows Kiosk Breakout Techniques
11.6 Wrapping Up

12 Windows Credentials
12.1 Local Windows Credentials
  12.1.1 SAM Database
  12.1.2 Hardening the Local Administrator Account
12.2 Access Tokens
  12.2.1 Access Token Theory
  12.2.2 Elevation with Impersonation
  12.2.3 Fun with Incognito
12.3 Kerberos and Domain Credentials
  12.3.1 Kerberos Authentication
  12.3.2 Mimikatz
12.4 Processing Credentials Offline
  12.4.1 Memory Dump
  12.4.2 MiniDumpWriteDump
12.5 Wrapping Up
13 Windows Lateral Movement

13.1 Remote Desktop Protocol
   13.1.1 Lateral Movement with RDP
   13.1.2 Reverse RDP Proxying with Metasploit
   13.1.3 Reverse RDP Proxying with Chisel
   13.1.4 RDP as a Console
   13.1.5 Stealing Clear Text Credentials from RDP

13.2 Fileless Lateral Movement
   13.2.1 Authentication and Execution Theory
   13.2.2 Implementing Fileless Lateral Movement in C#

13.3 Wrapping Up

14 Linux Lateral Movement

14.1 Lateral Movement with SSH
   14.1.1 SSH Keys
   14.1.2 SSH Persistence
   14.1.3 SSH Hijacking with ControlMaster
   14.1.4 SSH Hijacking Using SSH-Agent and SSH Agent Forwarding

14.2 DevOps
   14.2.1 Introduction to Ansible
   14.2.2 Enumerating Ansible
   14.2.3 Ad-hoc Commands
   14.2.4 Ansible Playbooks
   14.2.5 Exploiting Playbooks for Ansible Credentials
   14.2.6 Weak Permissions on Ansible Playbooks
   14.2.7 Sensitive Data Leakage via Ansible Modules
   14.2.8 Introduction to Artifactory
   14.2.9 Artifactory Enumeration
   14.2.10 Compromising Artifactory Backups
   14.2.11 Compromising Artifactory’s Database
   14.2.12 Adding a Secondary Artifactory Admin Account

14.3 Kerberos on Linux
   14.3.1 General Introduction to Kerberos on Linux
   14.3.2 Stealing Keytab Files
   14.3.3 Attacking Using Credential Cache Files
   14.3.4 Using Kerberos with Impacket
## 14.4 Wrapping Up

## 15 Microsoft SQL Attacks

### 15.1 MS SQL in Active Directory
- 15.1.1 MS SQL Enumeration
- 15.1.2 MS SQL Authentication
- 15.1.3 UNC Path Injection
- 15.1.4 Relay My Hash

### 15.2 MS SQL Escalation
- 15.2.1 Privilege Escalation
- 15.2.2 Getting Code Execution
- 15.2.3 Custom Assemblies

### 15.3 Linked SQL Servers
- 15.3.1 Follow the Link
- 15.3.2 Come Home To Me

### 15.4 Wrapping Up

## 16 Active Directory Exploitation

### 16.1 AD Object Security Permissions
- 16.1.1 Object Permission Theory
- 16.1.2 Abusing GenericAll
- 16.1.3 Abusing WriteDACL

### 16.2 Kerberos Delegation
- 16.2.1 Unconstrained Delegation
- 16.2.2 I Am a Domain Controller
- 16.2.3 Constrained Delegation
- 16.2.4 Resource-Based Constrained Delegation

### 16.3 Active Directory Forest Theory
- 16.3.1 Active Directory Trust in a Forest
- 16.3.2 Enumeration in the Forest

### 16.4 Burning Down the Forest
- 16.4.1 Owning the Forest with Extra SIDs
- 16.4.2 Owning the Forest with Printers

### 16.5 Going Beyond the Forest
- 16.5.1 Active Directory Trust Between Forests
- 16.5.2 Enumeration Beyond the Forest

### 16.6 Compromising an Additional Forest
16.6.1 Show Me Your Extra SID
16.6.2 Linked SQL Servers in the Forest
16.7 Wrapping Up

17 Combining the Pieces
17.1 Enumeration and Shell
   17.1.1 Initial Enumeration
   17.1.2 Gaining an Initial Foothold
   17.1.3 Post Exploitation Enumeration
17.2 Attacking Delegation
   17.2.1 Privilege Escalation on web01
   17.2.2 Getting the Hash
   17.2.3 Delegate My Ticket
17.3 Own the Domain
   17.3.1 Lateral Movement
   17.3.2 Becoming Domain Admin
17.4 Wrapping Up

18 Trying Harder: The Labs
18.1 Real Life Simulations
18.2 Wrapping Up