Practical Malware Analysis

Chapter 0/1 Quiz

Chapter 0

1. Explain the differences between Basic Static, Advanced Static, Basic Dynamic, and Advanced Dynamic Analysis.

2. Match each type of malware to its description below

Botnet	Malware that infects a machine and then uses the machine to send spam, generating income for attackers that sell spam-sending services
Downloader	Malicious code designed to conceal the existence of other code, usually paired with other malware and difficult to detect
Information-stealing Malware	Malicious code that exists only to download other malicious code, commonly installed upon accessing a system
Launcher	Malicious code that can copy itself to infect additional devices
Rootkit	Allows an attacker remote access to a system and receives instructions from a command and control server
Scareware	Malware that collects data from a victim’s device and sends it to an attacker, typically to gain banking credentials or PII
Spam-sending Malware	Malicious program used to launch other malicious programs, usually via non-traditional techniques to ensure stealth
Worm or Virus	Malware designed to frighten a user into buying something via error messages, notifications, etc

Chapter 1

1. What are two ways that Antivirus software identifies malicious files?

2. Explain the differences between hashing, encryption, and encoding.

3. What are the differences between static, runtime, and dynamic linking and how does each affect what information appears in a PE header?

4. Match each of the following common Dynamic-link Libraries to its description below

Kernel32.dll	Contains all of the user-interface components, such as buttons, scroll bars, and components for controlling and responding to user interaction
Advapi32.dll	The interface to the Windows kernel, used to access functions not normally available to Windows programs
User32.dll	Contains functions for displaying and manipulating graphics
Gdi32.dll	Contains functions for connecting to a network or performing network-related tasks
Ntdll.dll	Contains core functionality, such as access to and manipulation of memory, files, and hardware
WSock32.dll or Ws2_32.dll	Contains higher-level networking functions that implement protocols such as FTP, HTTP, and NTP
Wininet.dll	Provides access to advanced core Windows components such as the Service Manager and Registry

5. Which of the following pieces of information are stored in a PE header? (Check all that apply)

- ❏ Resources
- ❏ Section sizes
- ❏ Compile time
- ❏ Section names
- ❏ Exports
- ❏ Subsystem
- ❏ Imports

6. What are at least three things that indicate that an executable is packed?

7. Match the following common PE section names to their descriptions below

.text	Contains information for relocation of library files
.rdata	Contains the executable code
.data	Sometimes present, stores the export function information
.idata	Stores resources needed by the executable
.edata	Stores global data accessed throughout the program
.pdata	Holds read-only data that is globally accessible within the program
.rsrc	Sometimes preset, stores the import function information
.reloc	Present only in 64-bit executables and stores exception-handling information

Bonus: Explain what the MSVCRT Dynamic-link Library is used for