V2.4.6 - quiz - Logic Bombs and Rootkits

Amanda Success (Period 9) (replace with your information)
Monday December 25, 2023
Seat 99 (Grade level 13)
Cyber Capstone

0. What is a keylogger?
A. A hardware device used to encrypt keyboard inputs
B. A software program that tracks and logs keystrokes on a victim's keyboard
C. A security measure used to protect against malware attacks
D. A physical keyboard layout designed to prevent keylogging
___ <- Type answer here

1. What is a logic bomb?
A. A type of malware that encrypts sensitive data on a computer system.
B. A piece of code that waits for specific conditions to be met before executing.
C. A hardware device used to trigger system failures.
D. A security measure designed to prevent unauthorized access to computer networks.
___ <- Type answer here

2. What are triggers in the context of logic bombs?
A. Hardware components used to activate the logic bomb.
B. Specific events or conditions that cause the logic bomb to execute.
C. Encryption keys used to decrypt data encrypted by the logic bomb.
D. Security measures used to detect and neutralize logic bombs.
___ <- Type answer here

3. What are time bombs?
A. Logic bombs that detonate after a certain amount of time has passed.
B. Logic bombs that detonate when triggered by specific events.
C. Hardware devices used to activate logic bombs.
D. Encryption keys used to decrypt data encrypted by logic bombs.
___ <- Type answer here

4. Who is likely to install a logic bomb as an insider threat?
A. A cybersecurity expert hired to protect the company's network.
B. A disgruntled employee with privileged access to computer systems.
C. An external hacker attempting to breach the company's security.
D. A competitor trying to sabotage the company's operations.
___ <- Type answer here

5. Why are logic bombs hard to identify?
A. They are large and easily detectable by antivirus software.
B. They are activated randomly without specific triggers.
C. They are stealthy by nature and remain inactive until triggered.
D. They only affect outdated computer systems.
___ <- Type answer here

6. What is a recommended defense against logic bombs?
A. Disabling all antivirus software to prevent detection.
B. Regularly updating the operating system and patching vulnerabilities.
C. Ignoring scheduled tasks and system backups.
D. Using weak passwords to deter logic bomb activation.
___ <- Type answer here

7. What is a rootkit?
A. A type of malware that provides administrative access to a computer while concealing its presence.
B. A type of malware that targets only Linux/Unix systems.
C. A hardware component used to enhance computer performance.
D. A software tool used by system administrators to enhance system security.
___ <- Type answer here

8. What is the main role of a rootkit?
A. To enhance computer performance.
B. To alter system files and conceal its presence to avoid detection.
C. To provide additional security features to the operating system.
D. To detect and remove other malware from the computer.
___ <- Type answer here

9. Why are rootkits difficult to detect?
A. Because they only target outdated operating systems.
B. Because they activate after the operating system boots up.
C. Because they alter system files and data reports to avoid detection.
D. Because they are only installed on Linux/Unix systems.
___ <- Type answer here

10. How do rootkits block some antivirus software?
A. By encrypting system files.
B. By activating before the operating system boots up.
C. By disabling the computer's firewall.
D. By uninstalling the antivirus software.
___ <- Type answer here

11. What type of rootkit overwrites the firmware of the system's BIOS?
A. Bootkit
B. Kernel rootkit
C. Firmware rootkit
D. Driver rootkit
___ <- Type answer here

12. What is the purpose of Secure Boot in defending against rootkits?
A. To prevent unauthorized access to computer hardware.
B. To detect tampering with boot loaders and key operating system files.
C. To enhance computer performance.
D. To encrypt system files and data reports.
___ <- Type answer here

13. Which operating system was targeted by the Machiavelli rootkit?
A. Linux
B. Windows
C. Mac OS X
D. Android
___ <- Type answer here

14. What is Stuxnet?
A. The first known rootkit for industrial control systems (ICS).
B. A hardware component used to enhance computer performance.
C. A type of malware that targets Linux/Unix systems.
___ <- Type answer here

D. A software tool used by system administrators to enhance system security.