Homework Assignment 5: Endpoint Vulnerabilities, Attacks, and Defenses

Provide clear explanations in your own words and include examples where possible.

1. What is the difference between blocking ransomware and locking ransomware?

2. Why is ransomware considered a major threat to endpoint devices?

3. Explain the function of a keylogger. How can it be implemented in both software and hardware?

4. What is a remote access Trojan (RAT), and how does it differ from a standard Trojan?

5. Describe how a fileless virus operates and why it is more difficult to detect than a file-based virus.

6. What is a botnet, and how are bots used in coordinated cyberattacks?

7. Compare a logic bomb, a rootkit, and a backdoor in terms of how they sidestep endpoint defenses.

8. List three Indicators of Attack (IoAs) that could signal a potential security breach and explain each.

9. What makes locking ransomware infections via USB drives especially dangerous in organizational settings?

10. Define a buffer overflow and explain how it can be exploited by attackers.

11. How does a cross-site scripting (XSS) attack work, and what is the main weakness it exploits?

12. Explain the difference between CSRF (Cross-Site Request Forgery) and SSRF (Server-Side Request Forgery) attacks.

13. What is a replay attack and how can it compromise digital identity?

14. Describe the roles of antivirus software, HIDS, and EDR tools in protecting endpoint systems.

15. What is the purpose of application allow lists and sandboxing in operating system protections?