Lab Assignment: Research Writing on Endpoint Security

Instructions

Choose any THREE of the following prompts. Write 2–3 well-organized paragraphs per prompt. Cite at least one credible source for each response (e.g., academic articles, security vendor reports, threat intelligence feeds, or news coverage of breaches).

Research Writing Prompts (Choose 3)

1. **Ransomware in the Real World**
   Research a recent ransomware attack that impacted an organization (e.g., healthcare, education, or local government). What type of ransomware was used? What damage was done and how did the organization respond?
2. **Keyloggers and Spyware in Modern Espionage**
   Explore how keyloggers or spyware have been used in cyberespionage. Provide an example of a real campaign or breach and explain what was targeted and how the malware operated.
3. **Botnets and Distributed Attacks**
   Investigate a well-known botnet (e.g., Mirai, Emotet, TrickBot). How did it work? What was the scale of the attack, and how was the botnet eventually disrupted?
4. **Fileless Malware Techniques**
   Define fileless malware and describe a recent example. How did it evade detection? What tools or processes were leveraged to carry out the attack?
5. **Indicators of Attack (IoAs) in Action**
   Identify a breach where IoAs played a critical role in detection or post-incident analysis. Which indicators were observed and how did they help defenders understand or contain the attack?
6. **Application-Level Vulnerabilities**
   Choose a recent web application attack (e.g., SQL injection, XSS, CSRF). What was the vulnerability and how was it exploited? What security practices could have prevented it?
7. **Endpoint Protection Comparison**
   Compare at least two endpoint protection tools (e.g., traditional antivirus vs. EDR). What features set them apart? Which would be more effective in a modern enterprise and why?
8. **Patch Management and Exploits**
   Discuss a security incident that occurred due to unpatched software. What vulnerabilities were exploited? What lessons were learned about patch management?