Module 3: Assignment

3-1: Biological and File-Based Viruses

The word virus comes from Latin, meaning a slimy liquid, poison, or poisonous secretion. In late Middle English, it was used for the venom of a snake. The word later evolved from the discharge to the substances within the body that caused the infectious diseases that produced the discharge. In 1799, Edward Jenner published his discovery that the cowpox virus could actually be used as a vaccine against smallpox. As biological science continued to advance, the word "virus" became even more specific when referring to tiny infectious agents—even smaller than bacteria—that replicate in living cells. This new field of virology exploded in the 1930s when electronic microscopes allowed scientists to see viruses for the first time. since then, scientists have continued to identify and name new biological viruses. Combating viruses by developing vaccines has many parallels to how malicious file-based viruses are identified and removed from a computer. using the Internet, research these two types of viruses and find the similarities between combating biological and computer viruses.

- *Write a one-to-two-paragraph summary of your research.*

3-2: Living-off-the-land Binaries (lolBins)

Fileless viruses take advantage of native services and processes that are part of the OS to avoid detection and carry out their attacks. These native services used in a file-less virus are called living-off-the-land binaries (lolbins). Use the Internet to research file-less viruses and lolbins.

- When did file-less viruses first appear?
- How do they compare with file-based viruses?
- What are the defenses against file-less viruses?

Write a one-page paper on your research.

3-3: Infamous logic Bombs

Search the Internet for examples of logic bombs. Select four logic bombs and write a report about them.

- Who was responsible?
- When did the bombs go off?
- What was the damage?
- What was the penalty for the person responsible?
- Did the organization make any changes after the attack?
- How can they be prevented?

Provide your understanding of the above questions.

3-4: Cybersecurity AI

The use of AI in cybersecurity is growing rapidly. Use the Internet to research the latest developments in cybersecurity AI.

- How does it work?
- What platforms are using it?
- What are some examples of it?
- How is it being improved?
- How can adversarial AI attacks be defended against?

Write a one-page paper of what you have learned.

Module 4: Assignment

4-1: AV Comparison

Select four antivirus products, one of which is a free product, and compare their features.

- Create a table that lists the features.
- How do they compare with the AV software you currently use?
- Which would you recommend to others? Why?

Create a report on your research.

4-2: Threat Maps

Locate four online cybersecurity threat maps. Compare their real-time results.

- Why are these results different?
- What type of information do they provide?
- How easy or hard are they to use?
- How could they be used?
- How should they not be used?
- What are the strengths?
- What are the weaknesses?
- What recommendations would you make for improving host security?

Write a one-page paper on your analysis.

4-3: Application Patch Management

Select four third-party applications (not OSs) that you frequently use.

- How does each of them address patch management?

Visit their websites to determine how they alert users to new vulnerabilities.

- Are the patch management systems adequate?
- Should patch management be required of all third-party applications?
- What are the advantages?
- What are the disadvantages?

Write a one-page paper on your finding.

Module 5: Assignment

5-1: Unified endpoint Management tools

Use the Internet to identify and compare three different unified endpoint management tools.

- Create a table that lists their various features.
- Which of the tools would you recommend for a small business with 10 employees who use smartphones but has a single person managing IT services? Why?

Provide your understanding of the above questions

5-2: Enterprise deployment Model comparison

Research the different enterprise deployment models listed in Table 5-3, page 133 from the textbook.

- Create a detailed table listing their typical features.
- How they are used, and their advantages and disadvantages to both the enterprise as well as to the employee.
- Which of them is the most secure option?
- Which is the least secure option?
- Which of them is most advantageous for the enterprise?
- Which would you prefer to use?
- Which would you recommend for your school or place of employment? Why?

Create a one-paragraph summary along with your table.