T1 Solutions

Q1. You have been tasked with designing an anti malware for a malware that runs in background and continuously encrypts the files and then asks for a ransom to decrypt. Discuss the design of this anti malware. What all heuristics/static/dynamic signs you will look for discovering such a malware. Explain each of these signs in detail.

Ans A malware that encrypts files is commonly known as ransomware. Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Design:

Heuristics that can be used to detect ransomware: [1 mark]

- Random bit generations
- File extension change
- Rapid deletion of files

Static Analysis : [1 mark]

- Presence of parallel and fast encryption logic.
- Presence of certain strings such as bitcoin/BTC
- Presence of certain strings such as cryptowallet addresses

Dynamic Analysis: [1 mark]

- Upon running the alleged malware in a sandbox it should start encrypting the files.
- The malware tries to contact a server to upload the encryption key

Depending on the individual point presented by the students and how they interconnect them to design an anti-malware [1 mark]

Q2. Given a network based spreading worm. Explain what all damage that such a worm can do on a corporate network. Which features does a worm exploit to spread laterally? Compare a worm with a Trojan, what is the basic differentiating characteristic between them? Identify the loopholes that each of them exploit to attack.

Ans: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behavior will continue

Explain what all damage that such a worm can do on a corporate network. [1 mark]

Once a worm gets into a corporate network then it has free hand to spread throughout the network since usually the firewalls filter external traffic only and internal ports are unguarded. The damage that can be done ranges from simple bandwidth congestion to specific tasks that may be coded in the worm's payload.

Which features does a worm exploit to spread laterally? [1 mark]

Worms spread by exploiting vulnerabilities, such as buffer overflow. They have builtin network exploits using which they replicate from computer to computer in a network.

Compare a worm with a Trojan, what is the basic differentiating characteristic between them? Identify the loopholes that each of them exploit to attack. [2 mark]

A worm is a class of software called malware that has the ability to self-replicate and spread across a network. A worm is like a computer program that exploits security vulnerabilities such as security failures in a system to gain access to the system. A Trojan, on the other hand, is a type of malicious code that infects your computer system by disguising itself as a useful program while hiding its true malicious intent. Worms replicate themselves typically using networking protocols to explore a system's local network and begin to spread when they find potential systems to infect. They do not have to piggy back into a software program to cause damage. A Trojan, on the other hand, hides inside an innocent-looking

email or program to mislead the users of its true purpose. Unlike a worm, a Trojan does not self-replicate; it is a hidden piece of code.

Q3. A parasitic virus adds itself to a given executable. Show how such a virus infects files. You are supposed to list the steps (in a pseudoalgorithm form) that such a malware takes.
Ans:
A Parasitic Virus, also known as a file virus, is spread by attaching itself to executable programs. When a program infected with a parasitic virus is opened, the virus code runs. To hide, the virus passes control back to the original program. Your computer sees the virus as part of the program you were trying to run and gives it the same rights. These rights allow the virus to copy itself, install itself in memory, or make changes to your computer.

a) The virus is executed
b) The virus looks for other files in the file system and makes a list of suitable files.
c) The virus selects one files and proceeds to infect it
d) The virus compresses the original code
e) Next the virus adds itself to the original file in such a manner that whenever the infected file is executed first the virus will be executed and then the control will be passed to the original code.
f) To hide the infection any methods can be used such as compression
g) To prevent reinfection any marking technique can be used such as padding, modification of date timestamp etc.

Allot marks based on steps written, novelty and overall functioning.

Q 4 Consider following security breaches and answer which the principle of computer security is targeted. Suggest some prevention techniques for following breaches.

a) Veteran's Administration (VA) incident: 26.5 million discharged veterans' records, including name, SSN & date of birth, stolen from the home of an employee who "improperly took the material home."
b) In July 2020, hackers gained access to 130 private and corporate Twitter accounts with at least a million followers each.
c) Suppose an attacker makes an entry in the wrong health record (misfiling) and has the potential of significant consequences.
d) Suppose, the sender sends the message and later denies.

Ans- For each section, 0.5 marks for answer and 0.5 for preventive measures[at least 2 measures].
a) Confidentiality
Ensure proper physical security of electronic and physical sensitive data wherever it lives.

- Lock down workstations and laptops as a deterrent.
- Secure your area, files and portable equipment before leaving them unattended.
- Don't leave papers, computers or other electronic devices visible in an empty car or house.
- Shred sensitive paper records before disposing of them.
- Don't leave sensitive information lying around unprotected, including on printers, fax machines, copiers, or in storage.
- Laptops should be secured at all times. Keep it with you or lock it up securely before you step away -- and make sure it is locked to or in something permanent.
- Use extra security measures for portable devices (including laptop computers) and portable electronic media containing sensitive or critical info: Encryption, Extra physical security,Even portable devices and media with encrypted PII must have strict physical security.
- Securely delete personal and sensitive information when it is no longer needed for business purposes.

b) Authentication

- Use good, cryptic passwords that are difficult to guess, and keep them secure

- Never share or reveal your passwords, even to people or organizations you trust
- Use different passwords for work and non-work accounts.
- Have a unique password for each account.
- Change initial and temporary passwords, and password resets, as soon as possible whenever possible. These tend to be less secure.

c) Integrity
- Backup files on regular basis to prevent data loss
- Avoid file theft and unauthorized access protecting data with encryption
- Securely delete data and sanitize supports after intended lifecycle
- Verify data integrity to detect modification
- Safely share, synchronize, attach, and upload files

d) Non-Repudiation
- Using secure envelopes and digital signatures.

Q 5. As a security engineer, you have been given a task to build a system that implements both Bell Lapadula and Biba strict Integrity Models. Is it possible especially when a subject would have "high" privilege for BLP and "high" integrity for Biba, and an object that such subjects can access have "higher" classification level in BLP and "higher" integrity level in Biba ("higher" dominates "high"). Start your answer with either 'Yes' or 'No' followed by explanation. Also suggest is there any security model that provides above security requirement.
Ans- In the given question,

i(s) = high i(o) = higher
l(s) = high l(o) = higher

"higher" dominates “high"

This situation is discussed in two conditions. 1) For high < higher and 2)For high = higher.
[1 Marks for identifying two conditions]

Case 1: For high < higher, it is not possible for this situation. The explanation is as follows
[1 Mark for Case 1]

- If s wants to read o, according to the ssc of bell-lapadula model, $l(o) \leq l(s)$ does not comply with the condition of the example.
- If s wants to write o, according to the Biba strict integrity model, $i(o) \leq i(s)$ does not comply with the condition of the example.
- If s wants to append o, the analysis is the same as write as it does not comply with Biba model.
- We assume $S \subseteq O$, if s wants to execute o, according to Biba model, $i(o) \leq i(s)$ does not comply with the condition in example.

Case 2: For high = higher, it is possible for this situation. The explanation is as follows
[1 Mark for Case 2]

- We can hold both Bell-Lapadula and Biba models because the security level and integrity level is the same for subject and object. Both models can satisfy their conditions only when the security level and integrity level is the same.

[1 Mark for suggesting briefing alternative model]

Alternative model to suggest is Chinese wall model. “The Chinese Wall Security Policy” is an authoritative voice in the information security realm. It is essentially an access control policy that addresses a very specific security issue: conflict of interest. It aims to protect the confidentiality and, through extension, the integrity of a set of data, by mandating rules around its access and availability. Data sets in this model could be any one of the following three types

- Objects – This is the same as the objects of the Bell-LaPadula model and is essentially the ungrouped basic units of information
- Company Dataset – This is the collection of all objects belonging to a single organization or company
- Conflict of Interest Class – This is a collection of companies that are in competition with each other