<date that the hw is uploaded>

Introduction to cyber security 156360

semester a 2020-2021

hw # \_6\_

machon tal english speakers

|  |  |
| --- | --- |
| Teudat zehut | Student Name |
| 209927128 | Tamar Harizy |
| 006798775 | Gila Odes |

**Question 1 – 1988 worm**

**a. What kind of malware was it? (Explain why it is categorized in this way)**

The malware of this attack was that of a worm as a worm is a complete harmful program that can duplicate itself and run independently on a computer without a host code to attach itself too. This was the case with this specific attack as it was released on the internet and every computer it connected to and replicated itself and continued its destructive behavior of overloading each system. This worm attack was an attack on resources as in many cases the internet and systems on computers became so clogged that the stopped functioning.

**b. What 3 vulnerabilities it exploited? For each one: i. What kind of vulnerability is it? ii. How it can be fixed?**

The first vulnerability was that found in the fingered functionality (and other comparative string methods like strcpy and get methods) of the program which is supposed to be there to allow the system to verify users and get relevant information about a specific user. This process is supposed to be a background process of the system and not other users. However, the system did not guard against buffer overflow attacks and was vulnerable in that way. This could be fixed by ensuring to add buffer protection – namely if they were to develop variables that accept values for bounds on their program-supplied buffer arguments as a check; and all servers should check for unchecked uses of original variable calls – comparing them with the new replacement variables.

Another vulnerability lied in the system using sendmail which has a functionality that it can begin a conversation with the remote mailer to decide who to send the mail to, what the mail should say and other information. Although very useful the worm exploited the inbuilt weakness that when in debug mode the worm could send the sendmail commands instead of information and the sendmail (assuming it is information) executed it. The best fix would be to develop another system that achieves the same end result and disuse sendmail (because often disabling of debug mode hinders system performance and does not have an effective security assurance).

Thirdly, another found vulnerability was that the worm was able to effectively and quickly decrypt user passwords as the passwords were stored in a publicly readable file (meaning anyone could read the contents – hence the hackers knew the actual passwords and just needed to work on the decryption of them). One could fix this vulnerability by having a shadowed file for passwords with limited access that does not allow public viewing of the files contenets.