IE2052 – Advanced Networking Technology

2nd Year 2nd Semester

Assignment 01 – Individual

Contents

Physical Security Vulnerabilities

- Only those with permission may enter some restricted portions of SLIIT. The doors may be opened by giving fingerprint authentication. But someone who isn't permitted can follow someone who is to that safe place. It is referred to as tailgating [1].

Figure 1: Fingerprint Authentication

- On the tables in the administration center, there can be documents with sensitive information, such as login passwords for the workstations. Such information is accessible to students who visit that location for a good cause. Occasionally, with the aid of the student, the information could reach the incorrect persons.

- There are several computer laboratories at SLIIT. They are equipped with priceless machineries like computers and other associated gadgets. These laboratories' doors may be stolen if they were left unsecured.

Figure 2: Computer Lab

- Students can attempt to vandalize college property [2].

- It would be a major catastrophe if both the administration and the students did not care about what they were doing and what was occurring on campus.

Suggest solutions to detect and correct physical security vulnerabilities.

- CCTV cameras should be installed so that it would be simpler to identify students or employees who are tailgating and that they can keep an eye on those who are following them.

- Keeping confidential records at a location that is out of the reach of visitors, such as students.

- While the labs are not used, they are kept secured and CCTV cameras are installed to monitor who enters if the doors are left open.

- Conducting workshops to raise awareness of potential campus hazards, followed by a deliberate performance of scenarios to gauge how students and staff would behave and react to them.

- Installation of sensors in restricted locations that will go off when someone enters a certain area without authorization such as a student.

Figure 3: CCTV

Logical Security Vulnerabilities

- If an external device is infected with a virus and linked to a computer in a lab there is a chance that harmful software might be loaded by that device. If the system was not started with a virus defense it will be challenging to get rid of it [3].

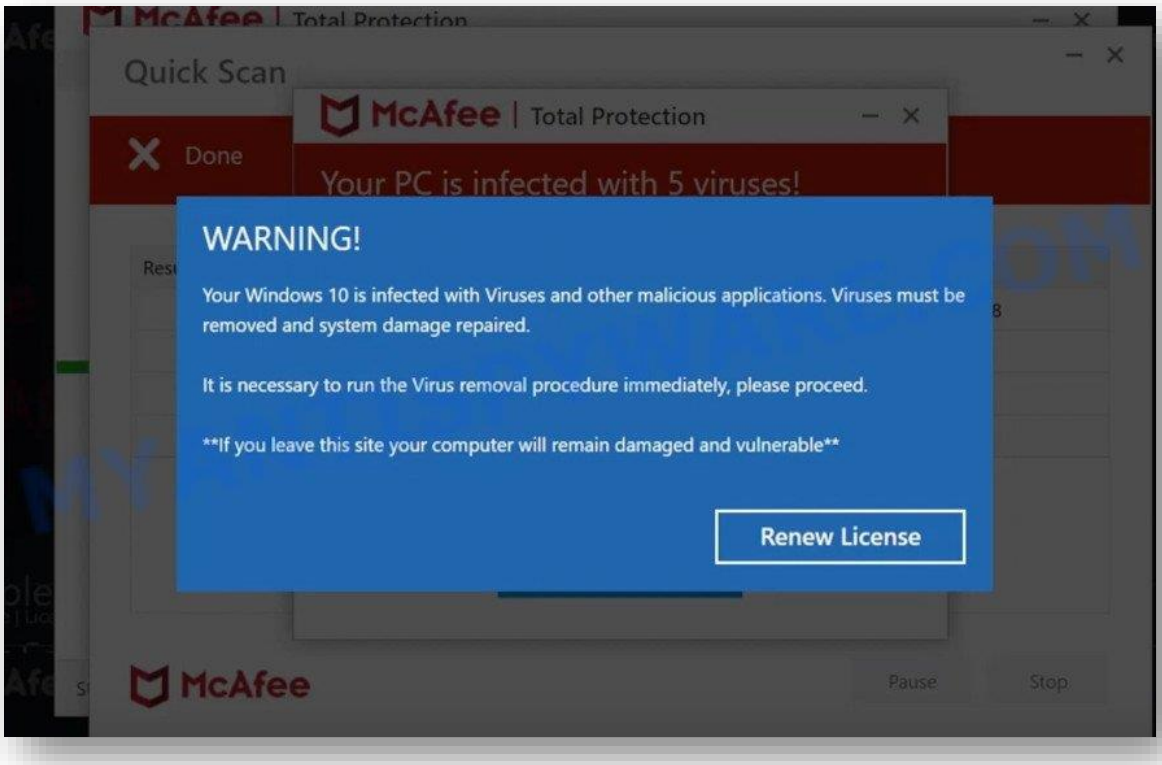

Figure 4: PC Protected Warning Message

- at the servers on campus there is sensitive information including student and professor information as well as student test results. The administration may not be able to utilize these data again if they are altered or corrupted by an unauthorized individual.

- Students may connect to other websites during the lab sessions which might allow them to download unapproved applications to the server and click on numerous URLs.

- The PCs in a lab can be logged into by a variety of individuals. Just the student's accounts are accessible to them. They will however get access and be able to read the information that should only be seen by staff if they learned the PC's login details from the staff member's account [4].

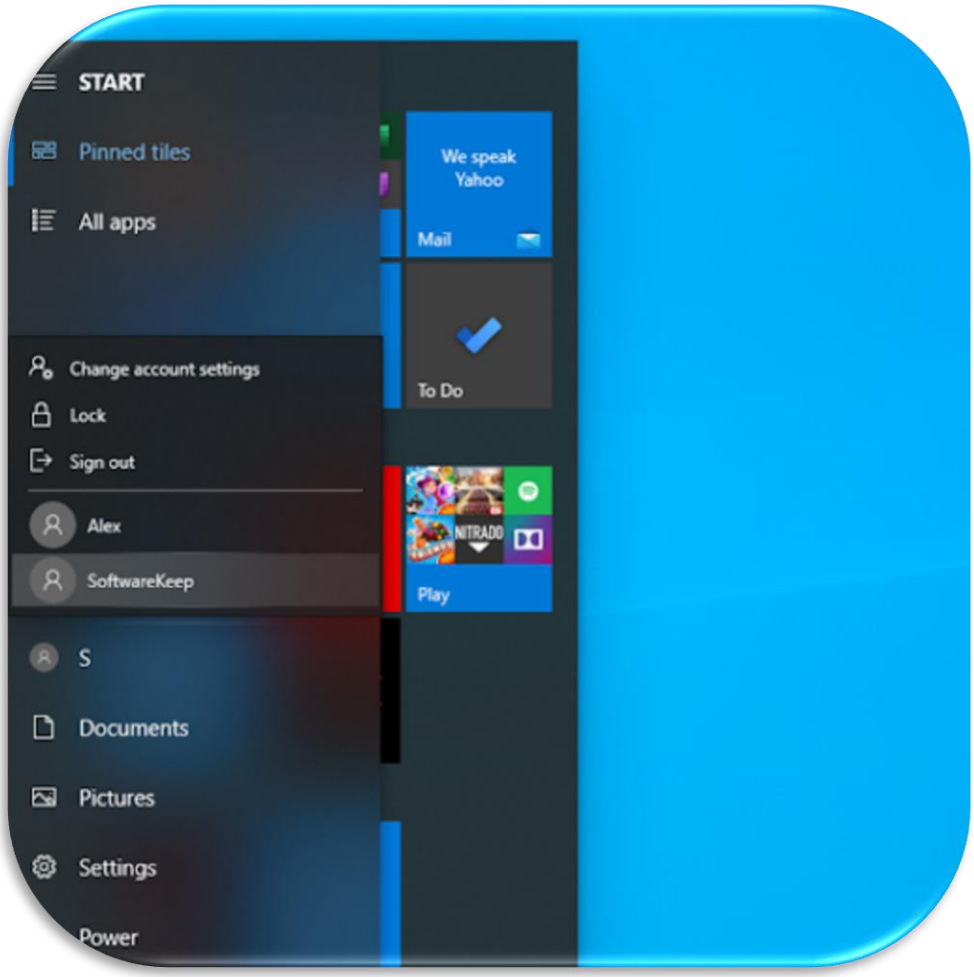

Figure 5: PC login Details

- Students at SLIIT who are pursuing degrees in cyber security are aware of how to decipher passwords. Students may gain access to private information if they are successful in brute–forcing the password of a system used by the administration.

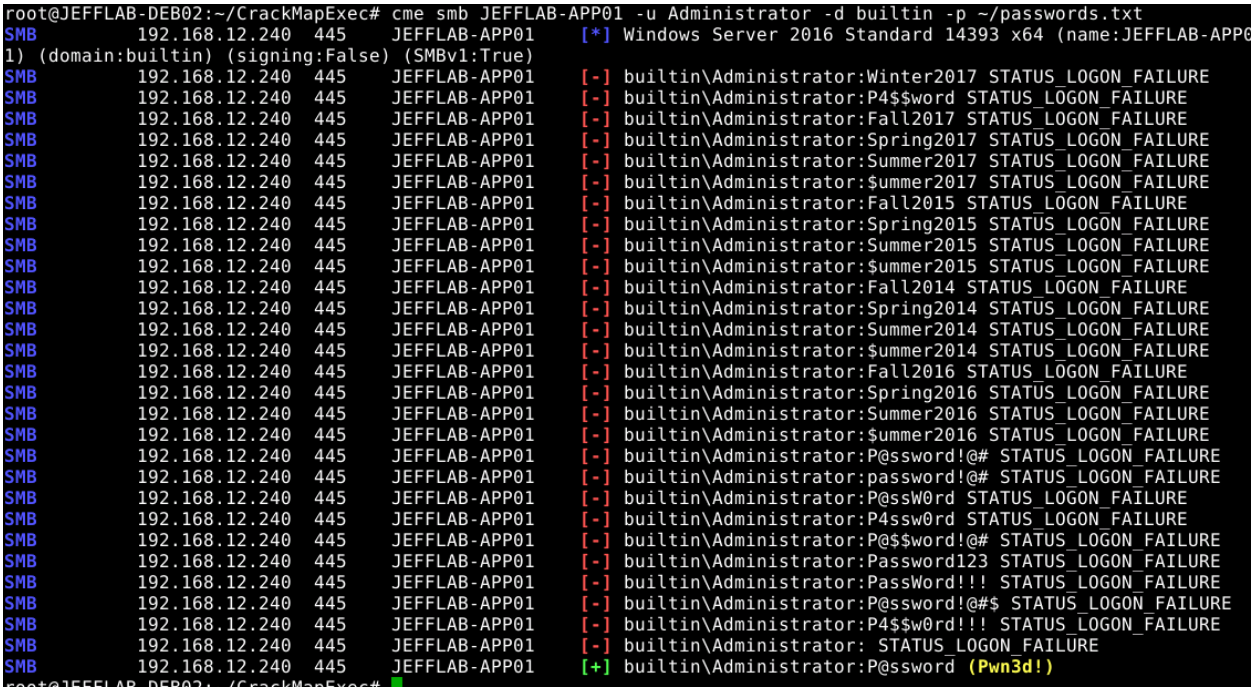

Figure 6: Password Hacking

Suggest solutions to detect and correct logical security vulnerabilities.

- Installation of virus detection software on all campus-owned servers.
- Utilizing two-factor authentication while accessing a system to guarantee data security.
- Preserving a copy of your most crucial and private data.
- Employing intrusion detection or prevention technologies can assist shield servers from assaults like Daniel of service.
- Prohibiting kids from visiting any websites and requiring them to double-check links before clicking on them.

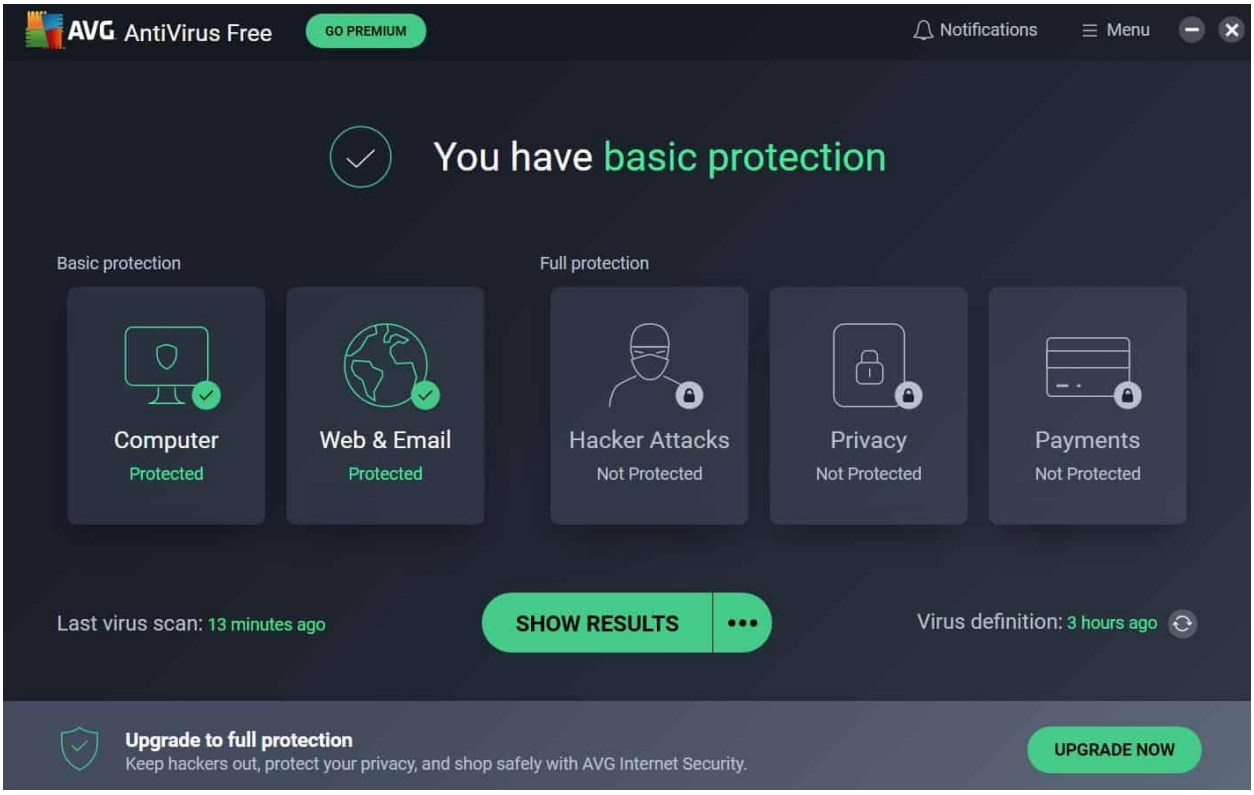

Figure 7: Virus Gard Installation

References

[1] SLIIT, "Providing authentication by fingerprints".

[2] SLIIT, "damage campus premises".

[3] SLIIT, " external device is connected to a PC machine in a lab".

[4] SLIIT, "in the lab PCs students can login only the student's account".