GAZI UNIVERSITY

ENGINEERING FACULTY

COMPUTER ENGINEERING

CENG482 INTRODUCTION TO COMPUTER SECURITY

Gamze AKSU – 171180005

Assignment-4

MARCH 2022

CONTENTS

Page

CONTENTS 1

1. SECURITY TESTING 2

1.1. Types of Security Testing 2

1.2. Test for Mobile Phone 3

1.3. Test for My Mobile Phone 4

2. BRAIN HACKING 5

3. CYBER WEAPONS 5

3.1. Virus 5

3.2. Worm 5

3.3. Trojan 6

3.4. Exploits 6

3.6. Phishing 6

4. CYBER WARFARE 6

4.1. Types of Cyberwarfare 7

4.2. Examples of Cyberwarfare Attacks 8

REFERENCES 9

1. SECURITY TESTING

Security testing is a type of software testing. It is done to protect the system from threat actors. It is applied to eliminate vulnerabilities in an application. Security vulnerabilities are exposed. It aims to ensure that there is no vulnerability for any threat that may come from threat actors. It is done so that malicious people do not get any information about any company. With this test, situations that may result in loss of information, money and reputation can be prevented.

1.1. Types of Security Testing

There are seven different types of security tests in Security Testing according to the Open Source Security Testing methodology manual [1]. These seven different types of security testing are described below.

1. **Vulnerability Scanning:** A vulnerability scan is a scan for known vulnerabilities. Each of the known vulnerabilities has a different signature. There are applications developed for scanning these signatures. Vulnerability scanning using these applications is called.
2. **Security Scanning:** It is applied to prevent weaknesses that may occur in the network and the system. First, weaknesses in the network and the system are identified. Then, these weaknesses are tried to be eliminated in order to reduce the risks that may occur. Two different security scans can be done as Manual scan and Automatic scan.
3. **Penetration Testing:** Penetration testing can also be viewed as a simulation. Within the scope of this test, before the threat actors, white hat people act as threat actors and test the system if there is a security vulnerability in the system. Later, the security vulnerabilities found are tried to be closed.
4. **Risk Assessment:** It is the analysis of security risks. A classification is made on the risks that can be seen in the organization. In this context, risks are classified with expressions such as low, medium and high. After the identified risks are classified, the necessary controls and measures are applied for these risks.
5. **Security Auditing:** It is an internal inspection for applications and operating systems for security vulnerabilities and flaws. An example of this is the examination of each line of code one by one.
6. **Ethical Hacking:** It is the testing of software within the company. Experts try to hack the company's software. The purpose of this hacking is to reveal security vulnerabilities in the system, as in other tests.

7. **Posture Assessment:** It is applied to show the general stance of the company. Firstly, the Security Scanning, Ethical Hacking and Risk Assessment tests are combined. It is then shown as an average posture of the company against threats.

1.2. Testing Types for Mobile Devices

There are three main types of testing for testing mobile devices. These are Unit Testing, Factory Testing, Certification Testing. Using reference [2], these tests are explained below.

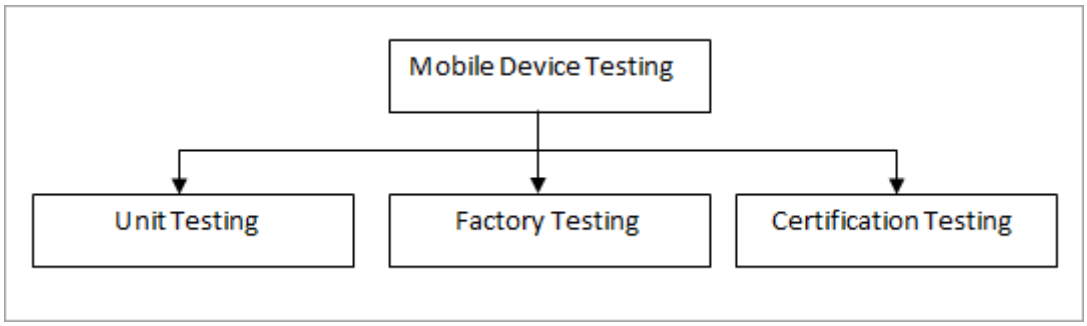

Figure 1: Mobile Device Testing

1. **Unit Testing:** Unit testing is performed by the software or hardware developers themselves. Within the scope of this test, each developed part is tested one by one.
2. **Factory Testing:** Factory testing is testing a device that leaves the factory. It is done to make sure that nothing bad happened to the hardware inside the device during assembly and that it works correctly. Hardware components of the device and applications on the device are tested in every possible way. Some of the tests that can be performed as part of factory testing are described below.
    - **Mobile Application Testing:** These are tests related to the operation of applications in the mobile device. Operations such as installation and removal of the application on the device, and the proper functioning of the installed application are tested.
    - **Hardware Testing:** It is the testing of hardware components inside the mobile device. Hardware components are tested to see if they work. For example, the operation of the on-off button and the touch screen or the suitability of the sim card slot are tested within the scope of this test.
    - **Battery (charging) Testing:** It is testing the battery of the mobile device. Check if the battery is working as it should. For example, the charging and discharging times of the battery are tested within the scope of this test.
    - **Network Testing:** It is tested whether the device can connect to networks such as 3G, 4G Wi-Fi that needs to be connected to communicate with other devices, or how

it reacts when it encounters a problem. For example, the response of the device when the connection is slow or the network connection is lost.

- **Protocol Testing:** In the protocol test, the structure of the packets sent is tested. Protocol testing tools are used to implement this test.
- **Mobile Software Compatibility Testing:** In Mobile Software Compatibility Testing, the compatibility of the applications in the device with each other is tested. Tools have been developed for the implementation of this test. It is a non-functional type of test.

3. **Certification Testing:** Certification testing is based on testing the standards that the mobile device must comply with for release. The standards that must be complied with, such as the compatibility of the device with other devices and the extent of the damage to the users, are tested. After the mobile device passes these tests, it obtains a certificate.

1.3. Testing for My Mobile Phone

In order to test my phone, the tests in title 1.2. Testing Types for Mobile Devices must be performed. These tests are already done before the phone is in my hands. So I won't be performing Unit Testing and Certification Testing myself. I'm just going to run some of the Factory Testing. The results of the tests performed are shown in the table below.

Types of Testing	Pass/Fail
Mobile Application Testing	Pass
Hardware Testing	Pass
Battery (charging) Testing	Pass
Network Testing	Not tested.
Protocol Testing	Not tested.
Mobile Software Compatibility Testing	Pass

Table 1: Factory Testing Results

2. BRAIN HACKING

With the development of brain-machine interfaces, devices that can be connected to the brain have been developed. As a result of hacking these devices, people's medical information and personal information such as home addresses and credit card passwords can be stolen without their knowledge. Just as other devices are protected, devices that directly connect to this brain and process brain signals must also be protected. Some scientists and developers have worked to hack these devices. And some of these works have been successful. For example, a device based on mind-controlling games was hacked and some personal information of the user was stolen. In another example, a cybersecurity expert hacked an EEG headset. [3]

Using a brain-machine interface, brain signals and tools such as prosthetic arms and wheelchairs are provided. As a result of processing these brain signals, crimes such as causing physical harm to others can be committed.

3. CYBER WEAPONS

3.1. Virus

A computer virus is a program that secretly affects the operation of the computer without the user's consent and knowledge. Viruses usually require a host program. They cannot exist on their own and are followed by a piece of software. The software must be run for the virus to be active. In order for the virus to be transmitted, there must be security vulnerabilities and social engineering attacks must be carried out. [4]

3.2. Worm

Unlike viruses, computer worms are programs that can exist on their own and can replicate themselves. It uses vulnerabilities in the target device to propagate itself. With the seized machine, other machines are scanned and the machines with the vulnerabilities are also infected. In this way, it begins to multiply exponentially. Worms damage the system by consuming bandwidth even with just scanning. [5]

3.3. Trojan

Trojans are malware that tries to enter the victim's computer undetected. Unlike viruses and worms, they do not try to reproduce themselves after they enter unnoticed. Once inside the victim's computer, it can be used for malicious purposes such as deleting data, blocking data, changing data, copying data, and reducing the performance of the computer or network. Ransomware is also usually carried out using a Trojan. [6][7]

3.4. Exploits

They are programs that try to harm the system by taking advantage of computer, software or system vulnerabilities. With exploits, operations such as requesting unauthorized access, creating an authorized user and deactivating the system can be performed. In general, exploits can be examined under three different headings in terms of communicating with the system. [8]

1. Remote Exploit: They communicate with the system over the local network or the internet.
2. Local Exploit: They are designed for vulnerabilities in the system.
3. Client Side Exploit: In this type of exploit, access is made over the network like remote exploit, but it also needs user interaction.

3.5. Phishing

Phishing attack is a type of internet scam. It is one of the oldest and most effective attacks in internet history. In this attack, e-mails are generally sent to the victim's e-mail account that will attract their attention. This e-mail may contain discounts and gifts. Sometimes, with social engineering, the close circle of the victim is learned and an e-mail is arranged accordingly. In this way, the victim is closer to clicking the links in the email. When the victim clicks on the link in the e-mail, the victim's information can be stolen by directing them to fake sites such as fake social media and bank sites. Additionally, the victim's device can be infected with malicious software with the harmful files sent as an attachment in the e-mail. [9]

4. CYBER WARFARE

Cyber-attacks against nation states are called cyber warfare. It is intended to inflict critical damage. Examples include cyberattacks that can damage government and civilian infrastructures, disrupt critical systems, and even cause loss of life. But which cyberattacks would be called cyberwarfare is a question. It is not entirely clear which actions will be cybercrime and which will be cyberwar. [10]

4.1. Types of Cyberwarfare

With the growth of the Internet, the vulnerabilities of nation-states are also increasing. Although works are carried out to close these vulnerabilities, it is not possible to completely cover the vulnerabilities. There are three main types of cyber warfare attacks by cybercriminals who exploit these vulnerabilities. [11]

1. **Destabilization:** Cybercriminals attack states over critical structures. Assets such as transportation systems, banking systems, electricity networks, water resources, dams and hospitals can be given as examples of critical structures. The destabilization of these structures can have significant consequences.
2. **Sabotage:** A government's computer systems are sabotaged to support traditional warfare. States should identify risks to be prepared for this situation. Enemies and terrorists can steal or destroy government information. For example, military information can be stolen by hacking the military database. In addition, hackers can crack down on vital government intelligence and threaten national security.
3. **Data theft:** Data is always important. To obtain data and information, hackers hack systems and ultimately can use the data they get as they wish. The data can first be used for intelligence. However, if it cannot be used for intelligence, it can be used to demand ransom or create chaos in the country. They may even want to simply destroy the data.

The three main types of cyber warfare described here are described under seven headings in the resource [10]. These are as follows:

1. Espionage
2. Sabotage
3. Denial-of-service (DoS) Attacks
4. Electrical Power Grid
5. Propaganda Attacks
6. Economic Disruption
7. Surprise Attacks

4.2. Examples of Cyberwarfare Attacks

- **Stuxnet:** Stuxnet is a worm type of malware. It was developed to attack the Iranian nuclear program. It spread with Universal Serial Bus devices. Iranian supervisory control and data acquisition systems were targeted.
- **Sony Pictures Hack:** Sony released a movie that vilified North Korean leader Kim Jong Un, and after that, a cyberattack on Sony Pictures company took place. As a result of the researches, it was determined that the attack was similar to the attacks of North Korean hackers.
- **Bronze Soldier:** In 2007, the Estonian government moved a statue called the Bronze Soldier from the capital to a military cemetery. After that, the Estonian government suffered massive cyber-attacks. Estonian government websites, media outlets and banks were locked with intense DoS attacks.
- **Enemies of Qatar:** Elliott Broidy, an American Republican fundraiser, sued the Qatari government. The case alleged that the Qataris saw Elliott Broidy as an obstacle to improving their position. That's why they're trying to steal and leak Elliott Broidy's emails and discredit him, Elliott Broidy said.

REFERENCES

1. Hamilton, T. (2022). What is Security Testing? Types with Example. Retrieved from https://www.guru99.com/what-is-security-testing.html
2. Software Testing Help. (2022). Mobile Device Testing: An In-Depth Tutorial On Mobile Testing. Retrieved from https://www.softwaretestinghelp.com/mobile-device-testing-tutorial/
3. OpenMindBBVA. (2020). Cybersecurity to Guard Against Brain Hacking https://www.bbvaopenmind.com/en/technology/digital-world/cybersecurity-to-guard-against-brain-hacking/
4. Wikipedia contributors. (2022, March 11). Computer virus. In *Wikipedia, The Free Encyclopedia*. Retrieved 19:01, March 29, 2022, from https://en.wikipedia.org/wiki/Computer_virus
5. Wikipedia contributors. (2022, March 28). Computer worm. In *Wikipedia, The Free Encyclopedia*. Retrieved 19:02, March 29, 2022, from https://en.wikipedia.org/wiki/Computer_worm
6. Wikipedia contributors. (2022, February 26). Trojan horse (computing). In *Wikipedia, The Free Encyclopedia*. Retrieved 19:02, March 29, 2022, from https://en.wikipedia.org/wiki/Trojan_horse_(computing)
7. Kaspersky. (n.d.). Trojan atı nedir ve ne gibi zararlar verebilir? Retrieved from https://www.kaspersky.com.tr/resource-center/threats/trojans
8. Yüksektepeli, O. (2013). Exploit Nedir? Retrieved from https://www.mshowto.org/exploit-nedir.html
9. İstanbul Bilgi Üniversitesi. (n.d.). Phishing Saldırısı. Retrieved from https://it.bilgi.edu.tr/tr/guvenlik/phishing/
10. İmperva. (n.d.). Cyber Warfare. Retrieved from https://www.imperva.com/learn/application-security/cyber-warfare/
11. Hanna, K. Ferguson, K. Rosencrance, L. (2021). Cyberwarfare. Retrieved from https://www.techtarget.com/searchsecurity/definition/cyberwarfare