GAZI UNIVERSITY

FACULTY OF ENGINEERING – COMPUTER ENGINEERING

171180010 – Cansu AYTEN

CENG482 INTRODUCTION TO COMPUTER SECURITY

HOMEWORK 4

MARCH 2022

CONTENTS

1. SECURITY TESTING

Security testing checks for vulnerabilities or risks in a software application. In this way, it is tested whether the system is vulnerable to attacks by malicious people. After vulnerabilities and risks are identified, attacks can be prevented by resolving problems by developers. With the prevention of attacks, losses such as information, data, money, or reputation of institutions, organizations, or persons that may be attacked can be prevented. With this test, as a result of any attack, the assets of the system or the people who own the system are protected from malicious use, or the system is protected from becoming inoperable.

There are seven types of tests within the scope of security testing. These are vulnerability scanning, security scanning, penetration testing, risk assessment, security auditing, ethical hacking and posture assessment [1].

1. Vulnerability scanning is a process by which a software automatically scans for vulnerabilities that can be exploited by attackers. There are known vulnerability signatures. The software application is checked by using these signatures in the scanning process.
2. Security scanning includes the automatic or manual detection of security vulnerabilities in the network and system. It then offers solutions to reduce the risks arising from these security vulnerabilities.
3. Penetration testing tests how the system will be affected in an attack by malicious people. For this, an attack simulation is made. Thus, potential vulnerabilities in the system are tested and the system is analyzed.
4. Risk assessment is a type of test that includes the analysis of observed security risks and the measures that can be taken against these risks. This test includes levels of risk. There are three levels of risk: high, medium, and low.
5. Security auditing is the audit of the security of the information system in line with some criteria. In this test, lines of code are examined and checked.
6. Ethical hacking is a test method involving the act of unauthorized access to a system, hacking a system. In this test, the actions of malicious people are applied. It relies on the detection of vulnerabilities by experts before attackers can discover and exploit security vulnerabilities in the system.
7. Posture assessment is a combination of security scanning, ethical hacking, and risk assessment methods. Indicates the status of the organization on security.

2. MOBILE DEVICE TESTING

Mobile devices are tools that make people's life significantly easier and enable them to perform most operations in a practical way. For this reason, it is expected that mobile devices will work correctly, fulfill the expected functions, that is, be of good quality. Mobile Device Testing is carried out to check whether the software and hardware of mobile devices perform the required functions. There are three types of mobile device testing. These are Unit Testing, Factory Testing and Certification Testing [2].

1. Unit Testing: It is a method in which the hardware and software of the device are tested piece by piece by the developers.
2. Factory Testing: It is the process of testing the hardware parts in possible ways to prevent problems that may occur due to defective manufacture or assembly. This process is done by company personnel. Apart from the hardware parts, the tests of the applications installed in the device are also performed. Factory testing includes tests such as mobile application testing, hardware testing, battery (charging) testing, network testing, protocol testing, mobile games testing, mobile software compatibility testing.
    - Mobile Application Testing: Operations such as installing and uninstalling applications on the mobile device, and whether the application works as expected are tested.
    - Hardware Testing: It is the process of testing mobile device hardware. Examples of these hardware are an on-off button or a touch screen.
    - Battery (charging) Testing: It includes testing of battery performance conditions such as charging the battery, the battery running out in the expected time or speed.
    - Network Testing: Includes testing of features such as 3G, 4G, Wi-Fi, etc. of the mobile device. For example, the response of the device in case of a slow connection, the response of the device in case of network disconnection, and how easily the device can connect when an existing network is found are tested.
    - Protocol Testing: It is a method that tests the structure of packets sent over the network using protocol testing tools.
    - Mobile Games Testing: The difference from Mobile Application testing is that it uses an automated, systematic, and well-structured approach.
    - Mobile Software Compatibility Testing: It tests mobile device software for conflicts using specific tools.

3. Certification Testing: In order for the device to be put on the market, it must meet certain requirements and be certified. An example of these requirements is that the device should not negatively affect human health and be suitable for use. Once such requirements are met, the device is certified to indicate that the device is suitable for sale.

There are other features that should be considered when testing mobile devices. One of them is the geography where the people who will use the mobile device live. It should be tested whether the mobile device works correctly in the conditions of this geography (temperature, pressure, etc.). Another is that tests are required to check that the equipment such as USB port, headphone port, or display is working properly even when the device is on the move or in harsh conditions. Finally, it is necessary to test that all applications that can be installed on the device are supported by the device [2].

Since my phone has passed these tests, which should be done before purchasing, it can perform its expected functions. Applications can be downloaded and uninstalled correctly and work as expected within the scope of applications I have downloaded. There are no problems that I have observed in hardware parts such as the phone screen, volume keys, power keys. The battery can be charged and it can be used for a long time.

3. BRAIN-HACKING

Brain hacking is the application of methods that affect a person's mind, thoughts, functions, cognitive processes. It is a technology that can know a person better than himself. So it can be dangerous. Devices that allow computers to communicate directly with the brain have been developed. For example, EEG headsets, which are devices that can record sensitive nerve signals, can measure and record emotions or reactions in a situation. By analyzing it, this information can be used in marketing or product designs. A group of experts and scientists conducted a study aiming to steal information from users through devices that allow computers to communicate directly with the brain. With this study, users' bank information, address, etc. have access to such information [3].

The device developed by the company called Neuralink, which develops brain-machine interfaces owned by Elon Musk, has been tested on monkeys. Then the company applied to test the device on humans. Their device is based on controlling a computer with the brain [4].

4. CYBER WEAPONS

4.1 Virus

Viruses are structures that enter the computer through an application beyond the control of the user of the computer, can replicate themselves, spread to other files, and run themselves. Viruses added to the executable file change the way the computer and programs work when this file is run. Programs cannot function properly or are damaged due to viruses. Security vulnerabilities are exploited when creating viruses [5].

4.2 Worm

Computer worms are self-executing structures that can enter the computer via a network connection or a file beyond the control of the user, reproduce themselves, spread to other computers and servers. Unlike viruses, it does not require an executable file to run. After entering the system, it can spread rapidly to low-defense servers or computers on a network by exploiting security vulnerabilities [6].

4.3 Trojan

A malware Trojan or Trojan Horse hides its true purpose and enters the system as if it were a reliable program or file. The system is affected by installing this software. After entering the system, it does not try to replicate itself or spread to other files. It causes many bad results such as taking control of the system, changing-stealing data, downloading, and running other malicious software [7].

4.4 Exploit

It is a program that creates problems in the system by taking advantage of vulnerabilities and code errors in software or system. For example, it is used in processes such as unauthorized access to the system, creating an authorized user in the system, increasing the authority of a user or changing the authorization status, deactivating a system, and in this way harms the systems. There are three types of exploits. These are Remote Exploit, Local Exploit, and Client Side Exploit. Remote Exploit is a type of exploit that accesses the system over a local or digital network. Local Exploit is inside the system and can access the privileges of users who are authorized in the system. Client Side Exploit accesses the system over a network. But users need to enable it [8].

4.5 Key Logger Software

It is a type of attack in which keyboard activities and sensitive information can be recorded from keystrokes. This software downloads any program or file to the computer with them while they are being downloaded. As a result, the password entered using the keyboard

keys, credit card number, etc. such information is saved to a file with the keylogger software. The fact that this recorded file is captured by malicious people means that attackers can access the information. Apart from that, there are some cases where keylogger software is not illegal. Companies can use this software to monitor employee activities. Families with children can likewise use it to monitor children's activities. There are some suggestions to remove or protect keylogger software. A program or file should not be downloaded from unknown sources. Programs considered harmful should be removed. A virtual keyboard should be used for online banking transactions. There must be security software that protects the computer [9].

4.6 Phishing

Phishing is a type of attack in which attackers aim to steal the victim's important information (password, identity information, etc.) by sending innocent and reliable-looking e-mails. If the victim interacts with harmful links or harmful files in such e-mails, the system owned by the victim can be hijacked by attackers. Malicious e-mails contain misleading writing or links that appear to be reliable. Examples of these writing or links are confirmation of personal information, links to a payment, a suspicious login attempt or activity. If the user interacts with them, sensitive information such as passwords, credit card numbers, etc. can be stolen. In order to be protected from this attack, attention should be paid to who sent the e-mail and the subject of the e-mail. A clear e-mail address and error-free subject writing are required. Do not click on suspicious links. No sensitive information should be shared via emails. The password used for e-mail and other account passwords must be different. Multi-factor authentication should be used. The computer must have security software. And many such measures can be taken [10].

5. CYBER WARFARE

Cyber warfare occurs as a result of cyber attacks by a state against an enemy nation or state. The purpose of these attacks is to damage or destroy the computer systems of the attacked state, to weaken that country and to harm its national interests. A series of actions taken for this purpose are described as attacks, but these actions have not been clarified by the experts. In cyber warfare, weapons are used as in real wars. Weapons used in cyber warfare are called cyber weapons. Such as viruses, phishing, computer worms softwares that can damage critical systems and render them inoperable, DDoS attacks that prevent users from accessing systems or computer networks, rendering these systems inoperable, data theft, spyware that can steal

information that endanger national security, or cyber espionage actions can be shown cyber warfare. [11,12].

5.1 Types of Cyber Warfare Attacks

In cyber warfare, the aim is to harm or weaken the country by damaging or destroying critical systems of a country. Persons can be assigned to detect security vulnerabilities in systems in a country. An attack can be made if any security vulnerabilities are found. In this assignment, seven types of cyber attacks will be discussed. These are espionage, sabotage, denial-of-service (DoS) attacks, electrical power grid, propaganda attacks, economic disruption, and surprise attacks. [11].

1. Espionage: It is the process of obtaining the information and secrets of a country in a secret manner. Before this information is obtained, attacks are made to damage computer systems. Examples of these attacks are botnet or phishing.
2. Sabotage: With attacks that sabotage critical systems of a state, the national security of that state is endangered. Information belonging to that state can be stolen or destroyed by hostile states. Apart from this, information stealing or breach of confidentiality may also occur due to the presence of spies belonging to enemy states in the state or due to careless employees within the state.
3. Denial-of-service (DoS) Attacks: These are attacks that make the system inoperable by constantly sending multiple requests to a system and forcing them to process those requests. Since these attacks will prevent access to systems, important operations can be blocked and systems can be disrupted.
4. Electrical Power Grid: One of the attacks that can damage infrastructure, disrupt communication, and damage critical systems is attacking power grids.
5. Propaganda Attacks: These are the attacks made with the aim of spreading lies or spreading shameful truths in order to break the trust of the citizens of the target country in the country and attract them to their side. In this way, people living in the target country or citizens of that country are tried to be directed.
6. Economic Disruption: It is an attack on the networks of economy-related organizations in order to prevent people living in the target country from accessing money when they need it or to steal money. Banks can be given as examples of these institutions.
7. Surprise Attacks: It is a type of unexpected (surprise) attack during a hybrid war, in order to weaken the enemy state and make a physical attack.

5.2 Examples of Cyber Warfare Operations

There are many examples in history for cyber wars. Below are four examples of cyber warfare [11,12].

- **Bronze Soldier (2007)**

  Estonia moved the Bronze Soldier statue associated with the Soviet Union to a military cemetery. After this incident, Estonia was cyber-attacked. The traffic of websites, banks, and media outlets in Estonia has become so intense that they have become inoperable.

- **The Stuxnet Worm (2010)**

  Stuxnet is malware that attacks the Iranian nuclear program. With this software, one of the most complex software in history, Iran's data acquisition and supervisory systems were targeted. This worm, which damaged Iran's nuclear work, spread through Universal Serial Bus devices.

- **Edward Snowden (2013)**

  Edward Snowden is a former Central Intelligence Agency (CIA) employee who disclosed classified information pertaining to the National Security Agency's cyber surveillance system.

- **Sony Pictures (2014)**

  After the release of the movie "The Interview", which contains negative events about North Korean leader Kim Jong-Un, a cyber attack was carried out on Sony Pictures. According to the FBI, the analysis of the software used in the attack showed that this software resembled the malware of the North Koreans.

5.3 Combating Cyber Warfare

There is not yet an international law that regulates the use of cyber weapons. However, the Cooperative Cyber Defense Center of Excellence has published a guide that includes explanations about when cyber attacks do not recognize the rules of law and how countries should respond to it. This guide is called Tallinn Manual [11].

Simulations or exercises can be carried out to determine the readiness of a country for cyber warfare. In this way, vulnerabilities and defense deficiencies are revealed and resolved. Apart from that, protecting critical systems and learning how to act and act quickly in case of a cyber attack are among the benefits that the exercises bring to the country. [11].

REFERENCES

1. Hamilton, T. (2022). What is Security Testing? Types with Example. https://www.guru99.com/what-is-security-testing.html
2. Mobile Device Testing: An In-Depth Tutorial On Mobile Testing. (2022). https://www.softwaretestinghelp.com/mobile-device-testing-tutorial/
3. Cybersecurity to Guard Against Brain Hacking. (2020). https://www.bbvaopenmind.com/en/technology/digital-world/cybersecurity-to-guard-against-brain-hacking/
4. Elon Musk to show off working brain-hacking device. (2020). https://www.bbc.com/news/technology-53921596
5. Computer virus. (2022). *Wikipedia* https://en.wikipedia.org/wiki/Computer_virus
6. Computer worm. (2022). *Wikipedia* https://en.wikipedia.org/wiki/Computer_worm
7. Trojan horse (computing). (2022) . *Wikipedia* https://en.wikipedia.org/wiki/Trojan_horse_(computing)
8. Exploit Nedir ? (2020). https://bbsteknoloji.com/exploit-nedir/
9. Demystifying a Keylogger – How They Monitor What You Type and What You Can Do About It? (2019). https://home.sophos.com/en-us/security-news/2019/what-is-a-keylogger
10. Johnson, D. (2020). Phishing: How To Protect Yourself When Working Remotely https://www.bluehost.com/blog/phishing-how-to-protect-yourself-when-working-remotely/?utm_source=google&utm_medium=genericsearch&gclid=Cj0KCQjw_4-SBhCgARIsAAlegrX1sWRZz82LCGEvNGhrWE9EscCPYDMpJrSYaRvgBR67H2_sLULftXoaAhyWEALw_wcB&gclsrc=aw.ds
11. Cyber Warfare. (n.d.) https://www.imperva.com/learn/application-security/cyber-warfare/
12. Hanna, K. T. Ferguson, K. Rosecrance, L. (2021). cyberwarfare. https://www.techtarget.com/searchsecurity/definition/cyberwarfare