**Ethical Hacking**

**Homework3**

1. **What is Malware? Mention the different usages of Malware.**

Malware is short for malicious software. Malware is something which tends to cause some behavior change wanted by the attacker. It might be a file or code which is supposed to steal or infect or conduct some behavior change in the system which attacker wants to cause in the system.

Malware can be a simple mail, on which we click and then a piece of code or software is placed in our system and the network gaps are being monitored by someone else in the world. Information of all kinds is being leaked using those network gaps.

Attackers use Malware in various levels of attack, for example to leave a trace in the system when attacked can be considered as Malware if its existence causes some constant disturbance in the system.

1. **Describe differences between viruses, trojan horses and worms.**

**Virus:**

1. A computer program or software that connects to another program or computer to destroy a computer system is known as a virus. When a virus-infected computer application is started, it does certain actions, such removing a file from the computer system. Remote control is not possible for viruses.

2. Exe files are used to launch viruses.

3. Information modification is a virus' primary goal.

**Trojan horses:**

1. Unlike viruses and worms, Trojan Horse does not replicate itself. It is a covert piece of code that steals the user's vital information. The e-mail ID and password, for instance, are observed by Trojan horse software when entered a web browser for logging.

2. Trojan horses run through programs and perceive themselves as useful software.

3. Information theft is the Trojan horse's primary goal.

**Worms:**

1. While worms are a type of computer software like viruses, they do not alter the program. It keeps reproducing itself, slowing down the computer system. Worms can be managed remotely.

2. Worms exploit system flaws to spread.

3. Worms' primary goal is to consume system resources.

1. **Describe the differences between botnets, trapdoor/backdoor and rootkits.**

**Botnets:**

A network of computers that have been infected with malware and are controlled by a single attacking party is known as a botnet (short for "robot network"). A bot is any machine that the bot-herder is in control of. The attacking party can control every computer in its botnet at once to execute a coordinated illegal operation from a single central location. A botnet's size (many are made up of millions of bots) allows an attacker to carry out extensive operations that would have been impossible with malware in the past. Infected devices can receive updates and alter their behavior instantly since botnets are constantly under the control of a remote attacker.

Uses the vast size of the botnet, for instance, to flood a target network or server with requests, making it unreachable to the users for whom it was designed. DDoS attacks target organizations with the intention of extorting money in exchange for stopping the attack or for personal or political reasons.

**Trapdoor/backdoor:**

A covert method of controlling a computer. Back doors, often known as "trap doors," are access points installed into software by the original creator who has remote or local access to the computer. For instance, a back door in an application would let someone activate either the software's visible or secret features. Access to all computer system operations would be possible through a back door in the operating system.

An uploader, which is a PHP script that enables the attackers to upload whatever or anything they want, was by far the most prevalent sort of backdoor discovered in 2021. Anyone with the proper URL path, arguments, and (rarely) access credentials can upload any files they wish to the web server thanks to these malicious files.

**Rootkits:**

A malicious software package known as a rootkit is made to grant unauthorized access to a computer or other software. Rootkits are difficult to spot and might hide their presence on a compromised system. Rootkit virus is used by hackers to remotely enter your computer, control it, and steal data.

Because the hacker has privileged access to system files and system processes, rootkits may also appear to be legitimate, much to how fileless malware leverages legal programs without leaving a trace. Rootkits cause your computer to deceive both you and occasionally antivirus and security applications.

1. **Describe the differences between spyware and adware.**

Spyware is software created to monitor every aspect of your computer usage; from the programs you use to the websites you visit.

Adware are programs that display a variety of offers and advertising, frequently in response to the websites you visit. These advertisements stand apart from pop-up windows that show up when visiting particular websites.

The following signs of spyware or adware infection on your computer:

There might be a lot more pop-up ads than usual.

You could visit unexpected websites using your web browser.

Your computer can appear slow or become unstable (repeatedly freezing or crashing).

On your system, network traffic may rise.

How to stop spyware/adware infection

When viewing a website, pause before clicking any links that appear in pop-up windows. Consider your decision before clicking on the adorable animation that you were instructed to view in an email.

Consider your options before downloading and installing the "free" game, screensaver, or other application you just came across online.

Please carefully read the license agreement before installing any program. Do not accept an agreement if something is unclear or if you do not comprehend it. The license may expressly or indirectly say that the spyware or adware is present in the software you are installing.

1. **How can you detect and remove rootkits? Why is it hard to do so?**

A rootkit is a sneaky computer program made to grant privileged access to a computer on an ongoing basis while actively concealing its existence. The words "root" and "kit" are combined to form the term "rootkit." Initially, a rootkit was a group of applications that provided network or computer administrator-level access. On Unix and Linux systems, the admin account is called "Root," while "kit" refers to the software parts that make up the tool. The majority of malware in use today, including Trojans, worms, and viruses, hides its existence and operations from users and other system processes by using rootkits.

Rootkits are tough to find. There are no commercially available tools that can detect and get rid of all rootkits, both known and unknown. There are several methods for searching for a rootkit on a compromised PC. Behavioral-based detection techniques, such as watching for unusual computer system behavior, signature scanning, and memory dump analysis are also available. Rebuilding the compromised system from scratch is frequently the only way to remove a rootkit.

Many rootkits infiltrate computer systems by attaching themselves to trusted applications or viruses. By keeping your system patched against known vulnerabilities, you can protect it from rootkits. Updated virus definitions are also a part of this, along with fixes for your OS and applications. Never open email attachments or accept files from unidentified sources. Read the end-user license agreements thoroughly before installing any software.

Because a rootkit may be able to undermine the tools used to detect it, rootkit detection is challenging. Utilizing a different, trustworthy operating system, behavioral-based techniques, signature scanning, difference scanning, and memory dump analysis are some detection strategies.

1. **What is ransomware and who hits by it? Why is there such a boom in ransomware?**

A form of virus known as ransomware prohibits or restricts users' access to their systems, either by locking the system's screen or by encrypting the users' files, in exchange for a ransom.

Ransomware may reach a computer using a variety of methods. Phishing spam is one of the most popular distribution methods; these attachments get to the victim in an email pretending to be a file they can trust. They can hijack the victim's computer once they have been downloaded and opened, especially if they include social engineering techniques built in that persuade victims to grant administrator access. Other, more aggressive ransomware variants, like NotPetya, bypass user trickery by taking advantage of security flaws to infect machines.

Attackers can choose which companies to use ransomware on in many ways. Attackers may choose to target universities because they frequently have fewer security teams and a dispersed user base that shares files frequently, making it simpler to get past their defenses.

Particularly susceptible to ransomware—and paying the ransom—are certain markets. Hospitals and other medical facilities are frequent targets for high-profile ransomware attacks because attackers know that, when lives are truly on the line, these institutions are more inclined to pay a little ransom to solve the issue. According to estimates, healthcare organizations are the target of 45 percent of ransomware assaults, and 85 percent of malware infections at these organizations are ransomware. Another alluring sector? The financial services industry is where the money is, as famously said by Willie Sutton. A ransomware attack was launched against 90 percent of financial institutions in 2017.

**7. Describe the steps for ransomware incident handling.**

Managing ransom incidents can be done by maintaining some checkpoints, such as:

1. Can you stop it right away? Get moving.

2. Got a back-up? restore data

3. Are there recovery tools? restore data.

4. No? Ransom, Pay/Loss

**8. How can you recover files once you are attacked by ransomware? Should businesses pay the ransom or take preventive cybersecurity measures?**

Forensic technique

Recover files using free tools

1. Kaspersky

2. Trend Micro

No More Ransom

Commercial services

To pay or not to pay

Dilemma

Cybersecurity guards against unauthorized access to and compromise of sensitive data, including customer information and trade secrets. Many rules and data protection legislation also impose strict requirements on businesses, including the implementation of cybersecurity programs. Following cybersecurity precautions is excellent practice for any company organizations, as opposed to paying a ransom.

**9. What are the symptoms of Malware infections?**

1. The system sluggish

2. Memory usage issues

3. Unusual programs and files executing

4. Strange computer actions

**10. How many ways the virus can attach to a program? Describe the parts of a virus code**

A virus can attach itself as a piece of code or a file from the original source. The virus source mimics the original source, and it will wait for the source to be activated before spreading.

By seizing control of the source and running at the beginning and end of the original source, virus sources even attempt to replace the events in the original source.

Three parts of the virus code:

Infection mechanism: The virus spreads by replicating its original source, according to the infection process.

Trigger: While the viral source is waiting for the primary source to start up so that it can run on the primary source.

Payload: Once the virus has begun to operate, depending on the virus kind, it begins to gather all data pertaining to the beginning and end of the original source while manipulating all sensitive data.

**11. How can you classify the viruses based on target and concealment strategy?**

Considering the target:

Boot sector infector: A boot sector infector is a form of malware that attacks the Master Boot Record (MBR) of a hard drive or the boot partition of a computer system. The virus runs dangerous code during startup and before security software may be run.

File infectors: These corrupt program files, including those from utilities, games, and apps. They frequently reside in memory, which means that after being run they continue to operate and can infect more programs.

Macro Virus: A macro virus is a type of computer virus that is built in the same macro language that is used to construct applications like Microsoft Word and Excel. It does not rely on the operating system and is focused on software applications (OS). Any computer running any OS, including Windows, macOS, and Linux, can be infected as a result.

Considering the concealment strategy:

Encrypted Virus: In the past five years, computer malware known as "encrypted viruses" has emerged as a significant danger to multinational corporations. A computer virus or malware that has the ability to encrypt its payload in order to hinder detection is referred to as an encrypted virus.

Stealth Virus: A computer virus that employs many strategies to evade detection by antivirus software is known as a stealth virus. Its name is derived from the word "stealth," which refers to a strategy for carrying out a task without drawing attention to it.

Polymorphic viruses are sophisticated file-infecting agents that may alter copies of themselves to evade detection while keeping the same fundamental functions after each infection. Polymorphic viruses encrypt their codes and utilize various encryption keys every time, varying their physical file makeup after each infection.

Metamorphic Virus: A virus that has the ability to translate, change, and rewrite its own code is said to be metamorphic. It is regarded as the most contagious computer virus, and if it isn't swiftly identified, it can seriously harm a machine.

**12. Describe various ways the viruses can be detected by virus scanners.**

In order to find Trojans, spyware, and other malicious software distributed by criminals, the virus scanner uses signatures. These are typically analogous to the thorough profiles that a virus scanner, which functions somewhat like an electronic sheriff, uses to check the files on a computer.

If something strange occurs to the system, create logs, and use the code or checksum to determine the updates.

Keep an eye out for any odd patterns, such as skipping or adding the first and last instructions in the payload of the system.