Virus

Computer virus is a piece of malicious code or software program that is able to infect a target system and then make copies of itself on other local computers

1. Worms : The largest difference is that worms are not attached to a computer program. They exist independently on the host system, and they often take advantage of network resources to spread to other hosts on the network they have compromised
2. Keylogger : to log the keystrokes of the user who has been infected. This is absolutely disastrous for the target user, because an attacker will be able to record and view every single key that the target types on their host system. This includes usernames and passwords, Google searches, private instant messaging conversations, and even payment card data
3. Rootkits : extremely dangerous because they serve to edit background processes in an effort to hide the malicious activities of an attacker. This will help viruses, keyloggers, and other malicious code exist for extended periods of time without detection on the target system
4. Trojan virus : extremely problematic because they can be slipped into innocent-looking applications and they are very hard to detect without the right security software

Virus Attack

1. Code Red : This attack relied heavily on an exploit found in the code that left servers vulnerable to a buffer overflow issue in an older version of code.very difficult to detect because it had the ability to run solely in memory(RAM)
2. Sasser : took advantage of a buffer overflow vulnerability that caused target systems to crash. And impossible to reboot your computer without removing the power cable and it caused many computers to crash completely
3. Zeus : a Trojan horse created to infect Windows machines in an effort to force them to carry out varying procedures that were deemed to be criminal activity
4. I Love You : 10% of every computer connected to the Internet at the time was infected with this virus
5. Melissa : virus was an infected text document that was uploaded to the alt.sex Usenet group with the appearance of being a collection of usernames and passwords for subscription and membership-only pornographic websites.virus would look at the first 50 addresses in the infected host's email address book and start sending those addresses emails.
6. Conficker Worm : created a botnet (a group of infected computers networked together) of more than 9 million different hosts that harmed governmental agencies, large enterprises, and simple individual users alike.
7. MyDoom : one of the fastest email worms to infect masses of computers, appearance of an email error. After a user had clicked on the "error" to view the problem the worm would send copies of itself to people found in the email address book of the infected system (38 billion$)

8. Stuxnet : political background as it is thought to have been created by the Israeli Defense Force in conjunction with the American government, goal to obstruct the initiatives of the Iranians to create nuclear weapons
9. Crypto Locker : Trojan horse that infected Windows machines, and the goal was to ransom target computers in exchange for money
10. Flashback : used infected websites to inject faulty JavaScript code into the host browser, and it made infected Mac hosts part of a botnet.

Ethical Considerations

1. Black hat hacker (Bad guys) : type of nefarious Internet user who exploits weaknesses in computing systems for personal gain or in order to disrupt an organization's information systems to cause them harm.
2. White hat hacker (good guys) : find potential security flaws and correct the errors so the black hat hackers can't break a system and use penetration testing tools and footprinting methods to identify disastrous security flaws on the organization's network and information infrastructure and patch them before they become a problem that would cost the organization obscene amounts of money.

Networking Fundamentals : OSI Model (Open Systems Interconnection)

1. Application – A computer application that creates data such as an email or instant messaging program
2. Presentation – The method of encoding data, such as ASCII text
3. Session – TCP ports (FTP, POP, HTTP, HTTPS, etc.)
4. Transport – TCP or UDP connections (among others)
5. Network – IP addresses and packets
6. Data-Link – MAC addresses and frames
7. Physical – ones and zeros (bits) transmitted across a cable

IP Addressing Essentials : number that serves as a unique identifier that helps computers differentiate between hosts connected to their network

Consist of four numbers ranging from 0-255 that are separated by periods

Consists of 2 portions : Network portion and host portion

1. Subnet Masks : determines how much of the IP address defines a network and how much of the address identifies a host on that network subnet

1. 255.0.0.0 (/8) – 8 bits (the first octet) define the network portion of the address.

2. 255. 255.0.0 (/16) – 16 bits (the first two octets) define the network portion of the address.

3. 255. 255. 255.0 (/24) – 24 bits (the first three octets) define the network portion of the address.

4. 255. 255. 255. 255 (/32) – This subnet mask indicates a host address. It does not indicate a network subnet.

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0

2. Two Special Network Addresses :
   Network Address - defines an entire network Eg : 192.168.1.0.
   Broadcast Address - send information to every host residing on that network at the same time Eg : 192.168.1.255.
3. MAC Addresses (Media Access Control) : layer 2 addresses, and they are globally unique. Each MAC address is contained on the network card of your computer, and it is composed of twelve hexadecimal digits (0-9, A, B, C, D, E, F) which total 48 bits in length. The following is an example of a MAC address: - B8EE:6525:7EA6
   The first half of the address – the first 6 digits – indicate the OUI (Organizationally Unique Identifier)
4. ARP (Address Resolution Protocol) : network protocol that binds layer 2 addresses to layer 3 addresses, information is constantly changing every time you take your laptop or mobile device to a new wireless network, and this information is critical to facilitating types of attacks such as a man in the middle attack.
5. Ports and Firewalls : -Port 80: HTTP (Hyper Text Transfer Protocol – used for web browsing and web pages)
   -Port 20/21: FTP (File Transfer Protocol – used to download files remotely)
   -Port 22: SSH (Secure SHell – used to remotely run command line procedures)
   -Port 53: DNS (Domain Name System – used to bind IP addresses to URLs)
   -Port 547: DHCP Server (Dynamic Host Configuration Protocol – automatic IP address assignment)
   -Port 443: HTTPS (Hyper Text Transfer Protocol Secure – encrypted HTTP)
   Firewall : permit or deny traffic to a network, can prevent hackers from making connections on specified ports to protect the local network

   Command Prompt - ipconfig

   <u>Hackers Toolbelt</u>

   1. Vulnerability scanners - we'll take a look at one called OpenVAS later in this book
      help white hat hackers find potential security holes in their computing systems to plug up the security holes before a black hat hacker could find a way to penetrate the system
      Pros of Vulnerability Scanners: -Help make systems more secure by identifying weaknesses that an administrator or security expert can then address and take care of -Mitigates the risk of hackers taking advantage of a system
      Cons of Vulnerability Scanners: -Sometimes they are not perfect and have the potential to miss the latest system vulnerabilities -They rely partially on a database of vulnerabilities

that needs to be continuously updated -Hackers can take advantage of them to find ways to break into a system

2. Port scanners – we'll also see how to use a port scanner called NMAP
   software utility that can be used to determine which ports a host is accepting connections on
3. Layer 4 Scanners : look for minute details in the operation of layer 4 protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) to find weaknesses in hosts
4. Packet sniffers – this software listens to and records all of the information flowing over your network, and we'll use one later for a man-in-the-middle attack -demonstration invaluable tools that are able to capture, store, and display all of the information that is flowing over a cable or transmission medium such as a wireless interface. By using a packet sniffer, you'll be able to see in great detail all of the conversations that computers are having with each other. You can see connection attempts, file transfers, and even Google searches.
5. Password crackers – these tools are used to uncover the password to a system
   gain unauthorized access to computer systems

Features of NMAP

1. Ping Sweeps : identify active machines on a given subnet, used to determine if two hosts have an end-to-end connection
2. ability to identify the operating systems that active hosts are using, will be able to tell you the model of device a host is using
3. goal is to find what port(s) are open on a whole subnet or a single host.

Metasploit is a vulnerability framework that is huge in the hacking and network penetration world
Their functions :
-show options – lists available options to configure Metasploit
-set rhost 192.168.1.3 – sets the remote host (target) of an attack to 192.168.1.3
-set lhost 192.168.1.2 – sets the attacking local host of an attack to 192.168.1.2
-set rport 80 – sets the port number of the target host to 80
-set lport 53 – sets the local port of the attacker to 53
-set payload [PAYLOAD] – allows a user to execute a given payload
-unset rhost – removes a remote host's IP address
-unset lhost – removes a local attacking host's IP address
-exploit [EXPLOIT] – allows an attacker to execute a given exploit
-back – returns a user to the initial Metasploit screen
-sessions –l – displays active sessions

-sessions –i [ID] – goes to an active section where [ID] is a numeric value taken from the previous command

Metasploit

1. terminology used in Metasploit such as payloads, exploits, listening, Metasploit interfaces, and have a general understanding of the database concept before moving forward.
2. Payloads refer to sections of executable code that can be delivered to a target.
3. Exploitation, on the other hand, simply means taking advantage of a known system vulnerability by using Metasploit
4. Listening means that Metasploit is collecting and analyzing network traffic that matches certain criteria, much like a packet sniffer such as Wireshark.
5. The database is one of the features of this software that makes it so powerful, and you can save vast amounts of data you collect about different networks within the database. Not only will it help you organize the information you collect, but you can actually run commands on entries found in the database to ease the automation process.

Basic Metasploit Commands :msfconsole
-show options – lists available options to configure Metasploit
-set rhost 192.168.1.3 – sets the remote host (target) of an attack to 192.168.1.3
-set lhost 192.168.1.2 – sets the attacking local host of an attack to 192.168.1.2
-set rport 80 – sets the port number of the target host to 80
-set lport 53 – sets the local port of the attacker to 53
-set payload [PAYLOAD] – allows a user to execute a given payload
-unset rhost – removes a remote host's IP address
-unset lhost – removes a local attacking host's IP address
-exploit [EXPLOIT] – allows an attacker to execute a given exploit
-back – returns a user to the initial Metasploit screen
-sessions –l – displays active sessions
-sessions –i [ID] – goes to an active section where [ID] is a numeric value taken from the previous command

Wireless Password Hacking
The two easiest encryption standards to crack into are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access)
Web-Based Vulnerabilities : SQLi (SQL Injection) and XSS (Cross-Site Scripting) attacks (common)

1. SQL (Structured Query Language) is a high level language that is used to communicate with databases. It helps application developers and websites insert, update, and delete information in

databases, and some of the queries are extremely powerful. For example, with one SQL command you could add one entry to a database or even delete all of the entries within an entire database.

2. your name, street address, zip code, country, phone number, and payment card details - this data is then “plugged in” to SQL code running in the background to properly store the data in a database.
3. If the developer made an error in their code that doesn’t properly sanitize the data, a hacker could insert (i.e. inject) text into the web form field that completely changes the operation of the SQL statement. By placing SQL code into the web form, the attacker has the ability to disrupt the database because their text and characters would be plugged directly into the SQL commands
4. Using these types of injection techniques, hackers can do the following: - Delete sensitive information - Escalate their privileges in the website - Create new administrative accounts - Steal usernames and passwords - Steal payment card data - Garner complete control over a database
5. Cross-Site Scripting Techniques (XSS) : XSS is a much more flexible technique and it can be used to inject malicious code into a user’s web browser or even take over a session between a client and a server. To top it all off, a hacker doesn’t need to manually initiate the attack. Instead, it can all be carried out automatically.

OpenVAS, or the Open Vulnerability Assessment system is a great tool for both black hat and white hat hackers alike.
OpenVAS is really a collection of programs that work together to facilitate testing procedures that are cataloged in a massive database of listed exploits – much like the Metasploit database.

Social engineering is a technique frequently used by sophisticated hackers to gain access to networks, and you need to have a solid understanding of these techniques to protect yourself from their black hat endeavors.

1. An Email from a Trusted Party : Don’t offer up your credentials to anyone, and I mean anyone, including your close friends. Unfortunately, hackers have been able to expand their access to a network after successfully hacking a computer by duping users on the attacked PC’s email list into forfeiting more information. By using an email account from the computer they hacked, the hacker is able to take advantage of the trust relationship between the person they are emailing and the person they have hacked.
2. A False Request for Help Sometimes : hackers will send messages that appear to be from a legitimate company that claim they are responding to a request that you never made. Often they will imitate a large and reputable corporation with thousands upon thousands of users to increase their chance of success. If you never requested aid from them, you need to avoid that email like the plague. The real problem here is the scenario where you do use a product or service from the company they are imitating, though.

3. Baiting Targets : Any baiting scheme is going to revolve around the appearance that the attacker is offering something of value. Many times you will see these types of social engineering attacks in pop-up ads or on torrent websites. The bait is frequently a free book, movie, or game that the target thinks is legitimate when in reality, it is a link to malicious code. Unfortunately, some of these offers look very real – they can take the form of a hot deal in a classified ad or a deal found in an Internet marketplace or false e-commerce site.

Man-In-The-Middle Attacks : extremely dangerous for end users because a successful attack will allow a hacker to view all of the data that a user is sending over the network. If the user is setting up a connection to a VPN server, the hacker will be able to capture their key to decipher their encrypted messages. In addition, the hacker will be able to see all of the websites the user visits as well as steal information such as usernames, passwords, and even payment card data.

Protecting Yourself from Hackers :

1. Software Updates
2. Change Default Usernames and Passwords
3. Use Strong Passwords (passwords should not be related to you)
4. Properly Configure Your Firewalls : Firewalls are a critical part of any security solution designed to protect users from hackers, and you need to make sure that your firewall is configured correctly
5. Antivirus and Antimalware Software Solutions
6. Using VPNs : VPN (Virtual Private Network) is essentially a service that encrypts all data communications between two endpoints – effectively making it impossible for a hacker, governmental agency, or petty Internet crook to unscramble and decipher the data.
7. Backing Up Your Data
8. Web Browser Security