Unit-2

Black Hat Hackers

Like all hackers, black hat hackers usually have extensive knowledge about breaking into computer networks and bypassing security protocols. They are also responsible for writing malware, which is a method used to gain access to these systems. Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime. Black hat hackers can range from amateurs getting their feet wet by spreading malware, to experienced hackers that aim to steal data, specifically financial information, personal information and login credentials. Not only do black hat hackers seek to steal data, they also seek to modify or destroy data as well Black hats fit the widely-held stereotype that hackers are criminals performing illegal activities for personal gain and attacking others. They're the computer criminals. A black-hat hacker who finds a new, "zero-day" security vulnerability would sell it to criminal organizations on the black market or use it to compromise computer systems Media portrayals of black-hat hackers may be accompanied by silly stock photos like the below one, which is intended as a parody

White Hat Hackers

White hat hackers choose to use their powers for good rather than evil Also known as "ethical hackers," white hat hackers can sometimes be paid employees or contractors working for companies as security specialists that attempt to find security holes via hacking (White hat hackers employ the same methods of hacking as black hats, with one exception they do it with permission from the owner of the system first, which makes the process completely legal. White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies. There are even courses, training, conferences and certifications for ethical hacking

For example, many white-hat hackers are employed to test an organization’s computer security systems The organization authorizes the white-hat hacker to attempt to compromise their systems. The white-hat hacker uses their knowledge of computer security systems to compromise the organization's systems, just as a black hat hacker would. However, instead of using their access to steal from the organization or vandalize its systems, the white-hat hacker reports back to the organization and informs them of how they gained access, allowing the organization to improve their defenses. This is known as "penetration testing." and it's one example of an activity performed by white-hat hackers. A white hat hacker who finds a security vulnerability would disclose it to the developer, allowing them to patch their product and improve its security before it's compromised. Various organizations pay "bounties" or award prizes for revealing such discovered vulnerabilities, compensating white hats for their work

Grey Hat Hackers

As in life, there are grey areas that are neither black nor white. Grey hat hackers are a blend of both black hat and white hat activities. Often, grey hat hackers will look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the issue. If the owner does not respond or comply, then sometimes the hackers will post the newly found exploit online for the world see. These types of hackers are not inherently malicious with their intentions; they're just looking to get something out of their discoveries for themselves. Usually, grey hat hackers will not exploit the found vulnerabilities. However, this type of backing is still considered illegal because the hacker did not receive permission from the owner prior to attempting to attack the system. Although the word hacker tends to evoke negative connotations when referred to, it is important to remember that all hackers are not created equal. If we didn't have white hat hackers diligently seeking out threats and vulnerabilities before the black hats can find them, then there would probably be a lot more activity involving cybercriminals exploiting vulnerabilities and collecting sensitive data than is now there

For example, a black hat hacker would compromise a computer system without permission. stealing the data inside for their own personal gain or vandalizing the system. A white-hat hacker would ask for permission before testing the system's security and alert the organization after compromising it: A gray-hat hacker might attempt to compromise a computer system without permission, informing the organization after the fact and allowing them to fix the problem. While the gray-hat hacker didn't use their access for bad purposes, they compromised and discovered a security system without permission, which is illegal. If a gray-hat hacker flaw in a piece of software or on a website, they may disclose the flaw publically instead of privately disclosing the flaw to the organization and giving them time to fix it. They wouldn't take advantage of the flaw for their own personal gain - that would be black-hunt behavior -- but the public disclosure could cause damage as black-hat hackers tried to take advantage of the flu before it was fixed.

Ethical hacking different from Security Audits and Digital Forensics

Ethical hacking - which encompasses formal and methodical penetration testing white hat hacking, and vulnerability testing involves the same tools, tricks, and techniques that criminal hackers use, but with one major difference: Ethical hacking is performed with the target's permission in a professional setting. The intent of ethical hacking is to discover vulnerabilities from a malicious attacker's viewpoint to better secure systems. Ethical hacking is part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

Ethical hacking versus audits

Many people confuse ethical hacking with security auditing, but there are big differences. Security auditing involves comparing a company's security policies to what's actually taking place. The intent of security auditing is to validate that security controls exist - typically using a risk-based approach. Auditing often involves reviewing business processes and in many cases, might not be very technical. Not all audits are this high-level, but the majority are quite simplistic. Conversely, ethical hacking focuses on vulnerabilities that can be exploited It validates that security controls do not exist or are ineffective at best. Ethical hacking can be both highly technical and nontechnical, and although you do use a formal methodology, it tends to be a bit less structured than formal auditing. If auditing continues to take place in your organization. you might consider integrating ethical hacking techniques into your IT audit program. They complement one another really well.

Policy Considerations

If you choose to make ethical hacking an important part of your business risk management program, you really need to have a documented security testing policy. Such a policy outlines the type of ethical hacking that is done which systems (such as servers, web applications, laptops, and so on are tested, and how often the testing is performed

You might also consider creating a security standards document that outlines the specific security testing tools that are used and specific dates your systems are tested each year you might list standard testing dates, such as once per quarter for external systems and biannual tests for internal systems - whatever works for your business

Compliance and regulatory concerns

Your own internal policies might dictate how management views security testing, but you also need to consider the state, federal, and global laws and regulations that affect your business. Many of the federal laws and regulations in the US. - such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (TECH) Act, Gramm-Leach-Bliley Act (LBA), North American Electric Reliability Corp Corporation industry Data Security Standard (PCI DSS) security evaluations. Related

(NERC) CIP requirements, and Payment Card require strong security controls and consistent international laws such as the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the European Union Data Protection Directive, and Japan's Personal Information Protection Act (JPIPA) are no different Incorporating your ethical hacking tests into these compliance requirements is a great way to meet the state and federal regulations and beef up your overall privacy and security program

Signing NDA

A non-disclosure agreement (NDA), also known as a confidentiality agreement (CA). confidential disclosure agreement (CDA), proprietary information agreement (PIA) or secrecy agreement (SA) is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties. Doctor-patient confidentiality (physician-patient privilege), attorney-client privilege, priest-penitent privilege, bank-client confidentiality, and Kickback agreements are examples, often not enshrined in a written contract between the parties. It is a contract through which the parties - agree not to disclose information covered by the agreement. An NDA creates a confidential -- relationship between the parties, typically to protect any type of confidential and proprietary information or trade secrets. As such, an NDA protects non-public business information. Like all contracts, they cannot be enforced if the contracted activities are felonies. NDAS are commonly signed when two companies, individuals, or other entities are considering doing business and need to understand the processes used in each other's business for the purpose of evaluating the potential business relationship. NDAs can be "mutual". meaning both parties are restricted in their use of the materials provided, or they can restrict the use of material by a single party. An employee can be required to sign an NDA or NDA-like agreement with an employer, protecting trade secrets. In fact, some employment agreements include a clause restricting employees' use and dissemination of company-owned confidential information. In legal disputes resolved by settlement, the parties often sign a confidentiality agreement relating to the terms of the settlement.

In some cases, employees who are dismissed following their complaints about unacceptable practice, or discrimination against and harassment of themselves, may be paid compensation subject to an NDA forbidding them from disclosing the events complained about. Such conditions in an NDA may not be enforceable in law, although they may intimidate the former employee into silence.

General types

A non-disclosure agreement (NDA) may be classified as unilateral, bilateral, or multilateral:

- **Unilateral**
A unilateral NDA involves two parties where only one party anticipates disclosing certain information to the other party and requires that the information be protected from further disclosure for some reason

- **Bilateral**
A bilateral NDA involves two parties where both parties anticipate disclosing information to one another that each intends to protect from further disclosure. This type of NDA is common when businesses are considering some kind of joint venture or merger When presented with a unilateral NDA, some parties may insist upon a bilateral NDA, even though they anticipate that only one of the parties will disclose information under the NDA This approach is intended to incentivize the drafter to make the provisions in the NDA more "fair and balanced" by introducing the possibility that a receiving party would later become a disclosing party or vice versa, which is not an entirely uncommon occurrence

- **Multilateral**

A multilateral NDA invokes three or more parties where at least one of the parties anticipates disclosing information to the other parties and requires that the information be protected from further disclosure. This type of NDA eliminates the need for separate unilateral or bilateral NDAs between only two parties. A multilateral NDA can be advantageous because the parties involved review, execute, and implement just one agreement. However, this advantage can be offset by more complex negotiations that may be required for the parties involved to reach a unanimous consensus on a multilateral agreement.

Things You Should Consider Before Signing

Look for broad and vague language:

Who analyzes an NDA, make sure the definitions of proprietary and confidential information are thoroughly defined. Be skeptical of broad and Vague language that opts to unreasonably limit your ability to discuss and divulge information. Make sure to exclude these four categories of information from your NDA in order to better protect yourself

a. Publicly available information
b. Information you already possess or may acquire on your own
c. Information you can prove you learned of independent of the protected information provided for under the NDA
d. Information received by a 3rd party source

Understand the document's scope:
Reflect on what the NDA is asking you to keep confidential and for how long. What must you do to keep the information secret? What type of information are you prohibited from disclosing? How long after your departure are you expected to keep the information private?

The consequences of breaching it:
Be wary of unusually extreme or unfair punishments for breaching the NDA. Weigh the proportionality of punishment to the breach, and if the punishment far outweighs the breach, refrain from signing. You should also make sure the NDA isn't heavily in favor of one party, Steer clear of an NDA that imposes responsibility on you for breaches by third parties, including your coworkers and other employees, without a similar provision to balance.

The timing of your John Hancock: Consideration, a bargained for exchange of value between parties, is a basic element of all contracts. You will likely be asked to sign your NDA at the before you begin work, where your employment suffices as standalone consideration. The issue arises once you are asked to sign an NDA after starting your job You may be entitled to "fresh" consideration, as most stave require "new" and "fresh consideration where an employee is asked to sign an NDA after commencing work Your "fresh" consideration may come in the form of a promotion additional vacation days, a bonus, or various other employee benefits

Liquidated damages: Run, and don't look back. An NDA containing a liquidated damages provision entitles your employer to a specified amount of damages paid to them without ever having to prove you were the direct cause. Most liquidated damages provisions are oppressive and contrary to public policy. Don't gift your employer an automatic recovery for something you may not have even done.

You can negotiate: It never hurts to ask, and companies are much more likely to allow changes to surprise or last-minute NDAS With any functional contract, there should be a balance between parties. Ask for clarifications, and spell out any concerns you have about the provisions or terms of the agreement

Go with your gut: If something in the NDA seems suspicious, it probably is. Having an attorney check over your contract and NDA now may seem like an inconvenience, but is a fraction of the cost and hassle you could suffer later on down the road. A few dollars now, could save you years of hardship, stress, and even a lawsuit. Also, if the NDA seems overly oppressive or suspicious, there is nothing wrong with scrapping the NDA altogether and walking away

Vulnerability Assessment and Penetration Testing

Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately. A vulnerability assessment process that is intended to identify threats and the risks they pose typically involves the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report. Organizations of any size, or even individuals who face an increased risk of cyber-attacks, can benefit from some form of vulnerability assessment, but large enterprises and other types of organizations that are subject to ongoing attacks will benefit most from vulnerability analysis. Because security vulnerabilities can enable hackers to access IT systems and applications, it is essential for enterprises to identify and remediate weaknesses before they can be exploited. A comprehensive vulnerability assessment along with a management program can help companies improve the security of their systems.

Importance of vulnerability assessments

A vulnerability assessment provides an organization with information on the security weaknesses in its environment and provides direction on how to assess the risks associated with those weaknesses and evolving threats. This process offers the organization a better understanding of its assets, security flaws and overall risk, reducing the likelihood that a cybercriminal will breach its systems and catch the business off guard.

Types of vulnerability assessments

Vulnerability assessments depend on discovering different types of system or network vulnerabilities, which means the assessment process includes using a variety of tools, scanners and methodologies to identify vulnerabilities, threats and risks.

Some of the different types of vulnerability assessment scans include the following:

Network-based scans
are used to identify possible network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.

Host-based scans are used to locate and Identify vulnerabilities in servers, workstations or other network hosts. This type of scan usually examines ports and services that may also be visible to network-based scans, but it offers greater visibility into the configuration settings and patch history of scanned systems.

Wireless network scans of an organization's Wi-Fi networks usually focus on points of attack in the wireless network infrastructure In addition to identifying rogue access points, a wireless network scan can also validate that a company's network is securely configured.

Application scans can be used to test websites in order to detect known software vulnerabilities and erroneous configurations in network or web applications

Database scans can be used to identify the weak points in a database so as to prevent malicious attacks, such as SQL injection attacks

Vulnerability assessments vs penetration tests

A vulnerability assessment often includes a penetration testing component to identify vulnerabilities in an organization's personnel, procedures or processes that might not be detectable with network or system scans. The process is sometimes referred to as vulnerability assessment penetration testing, or VAPT, However, penetration testing is not sufficient as a complete vulnerability assessment and is, in fact, a separate process A vulnerability assessment aims to uncover vulnerabilities in a network and recommend the appropriate mitigation or remedi or remediation to reduce or remove the risks

- A vulnerability assessment uses automated network security scarıning tools: The results are listed in the vulnerability assessment report, which focuses on providing enterprises with a list of vulnerabilities that need to be fixed, without evaluating specific attack goals or scenarios

- Organizations should employ vulnerability testing on a regular basis to ensure the security of their networks, particularly when changes are made, eg: services are added, new equipment is installed or ports are opened.

- In contrast, penetration testing involves identifying vulnerabilities in a network, and it attempts to exploit them to attack the system. Although sometimes carried out in concert with vulnerability assessments, the primary aim of penetration testing is to check whether a vulnerability really exists and to prove that exploiting it can damage the application or network.

- While a vulnerability assessment is usually automated to cover a wide variety of unpatched vulnerabilities, penetration testing generally combines automated and manual techniques to help testers delve further into the vulnerabilities and exploit them to gain access to the network in a controlled environment

Black-Box Penetration Testing

In a black-box engagement, the consultant does not have access to any internal information and is not granted internal access to the client's applications or network. It is the job of the consultant to perform all reconnaissance to obtain the sensitive knowledge needed to proceed. which places them in a role as close to the typical attacker as possible. This type of testing is the most realistic, but also requires a great deal of time and has the greatest potential to overlook a vulnerability that exists within the internal part of a network or application. A real life attacker does not have any time constraints and can take months to develop an attack plan waiting for the right opportunity. In addition, there are many defensive tools that exist within networks to help prevent an existing vulnerability from being exploited. Even new web browsers have settings that can circumvent an attack, but the weakness in an application may still exist, and all that is required to exploit the vulnerability is a variation of setting or a connection from a different browser version just because a configuration prevents the vulnerability from being found or exploited does not necessarily mean the vulnerability does not exist or is actually being mitigated, it only means that some outside force is buffering the result. This can result in a very dangerous outcome and a false sense of security that may be exploited at a later time by someone who has more time to explore this attack surface more greatly

Grey-Box Penetration Testing

An engagement that allows a higher level of access and increased internal knowledge falls into the category of gray-box testing Comparatively, a black-box tester begins the engagement from a strict external viewpoint attempting to get in, while the gray box tester has already been granted some internal access and knowledge that may come in the form of lower-level credentials, application logic flow charts, or network infrastructure maps. Gray box testing can simulate an attacker that has already penetrated the perimeter and has some form of internal access to the network. By providing some form of background to the security consultants undertaking the assessment, it helps to create a more efficient and streamlined approach. This saves on the time and money) spent on the reconnaissance phase, allowing the consultants to focus their efforts on exploiting potential vulnerabilities in higher risk systems rather than attempting to discover where these systems may be found.

White Box Penetration Testing

The final category of testing is called white-box testing, which allows the security consultant to have complete open access to applications and systems. This allows consultants to view source code and be granted high-level privilege accounts to the network. The purpose of white-box testing is to identify potential weaknesses in various areas such as logical vulnerabilities, potential security exposures, security misconfigurations, poorly written development code, and lack-of-defensive measures. This type of assessment is more comprehensive, as both internal and external vulnerabilities are evaluated from a "behind the scenes" point of view that is not available to typical attackers. Combining the knowledge of experienced security consultants with a proven systematic track record of implementing tools to perform both dynamic analysis (e.g. fuzzing) and static analysis (eg. code review) provides an inclusive testing methodology to help identify all potential components that may be areas of concern.

CONTENTS

- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration

SCANNING NETWORKS

What is scanning technique?

Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization. Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication, or weak encryption algorithm. So a pen-tester and ethical hacker list down all such vulnerabilities found in an organization's network.

Scanning is of three types:

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Objectives of Network Scanning:

- To discover live hosts/computer, IP address, and open ports of the victim
- To discover services that are running on a host computer
- To discover the Operating System and system architecture of the target
- To discover and deal with vulnerabilities in Live hosts.

Scanning Methodologies

- Hackers and Pen-testers check for Live systems
- Check for open ports
- Scanning beyond IDS (Intrusion Detection System)

Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform Banner grabbing attacks. This information may be used by intruders hackers to portray the lists of applicable exploits.
-Scan for vulnerability
-Prepare Proxies

Port Scanning

It is a conventional technique used by penetration testers and hackers to search for open doors from where hackers can get access to any organization's system. During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and topology of the targeted organization. Once the hacker fetches the IP address of the victim organization by scanning TCP and UDP ports, the hacker maps the network of this organization under his/her grab. Amap is a tool to perform port scanning.

CP/IP handshake

Before moving to the scanning techniques, we have to understand the 3-way TCP/IP handshaking process. Handshaking in computer term means the automated process used to set dynamic parameters of a communication channel between two entities taking the use or some protocols. Here, TCP (Transmission Control Protocol) and IP (Internet Protocol) met the two protocols used for handshaking between a client and a server, Here first the client sends synchronization packet for establishing a connection, and the server listens to and responds with SYK/ACK Packet to the client. The client again responds to the server by sending an ACK packet. Here SYN deriotes synchronize, which is used to initialize connections between the client and the server in the form of packets ACK denotes acknowledgment which is used to establish a connection between two hosts

Scanning techniques mainly used:

- **SYNScan:** SYN scan or stealth doesn't complete the TCP three-way handshake technique. A hacker sends an SYN packet to the victim, and if an SYN/ACK frame is received back then the target would complete the connection and the port is in a position to listen. If an RST is retrieved from the target, it is assumed that the port is closed or not activated. SYN stealth scan is advantageous because a few IDS systems log this as an attack or connection attempt

- **XMASScan** send a packet which contains URG (urgent). FIN (finish) and PSH (push) flags. If there exists an open port, there will be no response: but if the port is closed, the target responds with an RST/ACK packet. (RST-reset).

- **FINScan:** A FIN scan is similar to an XMAS scan except that it sends a packet with Just the FIN (finish) flag and no URG or PSH flags. FIN scan receives the same response and has the same limitations as XMAS scans.

- **IDLEScan:** An IDLE scan uses a spoofed/hoax IP to send SYN packet to the target by determining port scan response and IP header sequence number. Depending on the response of the scan, the port is determined, whether open or closed

- **Inverse TCP Flag Scan:** Here, the attacker sends TCP probe packets with a TCP flag(FIN, URG PSH) or with no flags If there is no response, then it indicates that the port is open and RST means the port is closed
- **ACK Flag Probe Scan:** Here the attacker sends TCP probe packets where an ACK flag is set to a remote device which then analyzes the header information (TTL and WINDOW field). The RST packet signifies whether the port is open or closed. This scan is also used to check the target's/victim's filtering system

Vulnerability Scanning

It is the proactive identification of vulnerabilities of the system within a network in an automated manner, to determine whether the system can be exploited or threatened. In this case, the computer should have to be connected to the internet

Tools and Steps Used

If a hacker wants to perform ICMP (Internet Control Message Protocol) scanning, it can be done manually.

The steps are

- Open Windows OS
- Press Win+R (Run) buttons in combination
- In the Run, type- cmd

- Type the command: ping IP Address or type: ping DomainName

Tools that can are used to scan networks and ports are:

Nmap: to extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems, and OS versions . Angry IP Scanner, scans for systems available in a given input range,

Hping 2/Hiping3: are command line packet crafting and network scanning tools used for TCP/IP protocols.

Superscan: is another powerful tool developed by Mcafee, which is a TCp port scanner, also used for pinging.

ZenMap: is another very powerful Graphical user interface (Gl) tool to detect the type of OS, OS version, ping sweep, port scanning, etc Net Scan Tool Suite Pack is a collection of different types of tools which can perform a port scan. flooding, webrippers, mass emailers, and This tool is trial version but paid versions are also available

Wireshark and Omnipeak are two powerful and famous tools which listen to network traffic and acts as a network analyzer

Names of other famous tools for PCs are Advanced Port Scanner, Net Tools, MegaPing. CurrPorts, PRTG Network Monitor, SoftPerfect Network Scanner, Network Inventory Explorer, etc.

There are various other scanners available free and inbuilt in Kali Linux OS.
Tools and software that are used in mobiles as scanners include the names such as Umit Network Scanner, Fing. IP network Scanner. PortDroid network Analysis. Panm IP Scanner. Nessus Vulnerability Scanner. Shadow Sec Scanner, etc

Countermeasures against Scanning

- Configure firewalls and IDS to detect and block probes.
- Use custom rules to lock down the network and block unwanted ports
- Run port Scanning tools to determine whether the firewall accurately detects the port scanning activities
- Security Experts should ensure the proper configuration of anti-scanners and anti spoofing rules
- Security experts of an organization must also ensure that the IDS, routers, and firewall firmware are updated to their latest releases

Enumeration

Enumeration and its Types

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system.

In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target.

The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase

Types of information enumerated by intruders:

- Network Resource and shares
- Users and Groups
- Routing tables
- Auditing and Service settings Machine names
- Applications and banners

- SNMP and DNS details

Techniques for Enumeration

- Extracting user names using email ID's
- Extract information using the default password
- Brute Force Active Directory
- Extract user names using SNMP
- Extract user groups from Windows
- Extract information using DNS Zone transfer

Services and Port to Enumerate

- TCP 53: DNS Zone transfer
- TCP 135: Microsoft RPC Endpoint Mapper
- TCP 137. NetBIOS Name Service
- TCP 139: NetBIOS session Service (SMB over NetBIOS)
- TCP 445: SMB over TCP (Direct Host)
- UDP 161: SNMP
- TCP/UDP 389: LDAP
- TCP/UDP 3368: Global Catalog Service
- TCP 25: Simple Mail Transfer Protocol (SMTP)

TYPES OF ATTACKS

CONTENTS

1. Keystroke Logging
2. Denial of Service / DOS DDOS)
3. Waterhole Attack
4. Brute Force
5. Phishing
6. Fake WAP
7. Eavesdropping
8. Man-in-the-middle
9. Session Hijacking
10. Clickjacking
11. Cookie Theft
12. URL Obfuscation
13. Buffer Overflow
14. DNS Poisoning
15. ARP Poisoning
16. Identity Theft
17. IOT Attacks
18. BOTS and BOTNETS

Keystroke Logging:

Keystroke logging, often referred to as key logging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A key logger can be either software or hardware. While the programs themselves are legal, with many of them being designed to allow employers to oversee the use of their computers, keyloggers are most often used for stealing passwords and other confidential information. Key logging can also be used to study human-computer interaction. Numerous key logging methods exist: they range from hardware and software-based approaches to acoustic analysis.

Applications of Keystroke Logging

Wireless keyboard and mouse sniffers:

These passive sniffers collect packets of data being transferred from a wireless keyboard and its receiver. As encryption may be used to secure the wireless communications between the two devices this may need to be cracked beforehand if the transmissions are to be read. In some cases, this enables an attacker to type arbitrary commands into a victim's computer.

Keyboard overlays: Criminals have been known to use keyboard overlays on ATMs to capture people's PINS. Each key press is registered by the keyboard of the ATM as well as the criminal's keypad that is placed over it. The device is designed to look like an integrated part of the machine so that bank customers are unaware of its presence.

Electromagnetic emissions: It is possible to capture the electromagnetic emissions of a wired keyboard from up to 20 meters (66 ft.) away, without being physically wired to it. In 2009, Swiss researchers tested 11 different USB, PS/2 and laptop keyboards in a semi-anechoic chamber and found them all vulnerable primarily because of the prohibitive cost of adding shielding during manufacture The researchers used wide band receiver to tune into the specific frequency of the emissions radiated from the keyboards.

Optical surveillance Optical surveillance, while not a keylogger in the classical sense, is nonetheless an approach that can be used to capture passwords or PINS A strategically placed camera, such as a hidden surveillance camera at an ATM, can allow a criminal to watch a PIN or password being entered 1922

Physical evidence: For a keypad that is used only to enter a security code, the keys which are in actual use will have evidence of use from many fingerprints A passcode
of four digits, if the four digits in question are known. is reduced from 10.000 possibilities to just 24 possibilities (10 versus #

factorial of 4), These could then be used on separate occasions for a manual "brute force attack”

Smartphone sensors: Researchers have demonstrated that it is possible to capture the keystrokes of nearby computer keyboards using only the commodity accelerometer found in smartphones. The attack is made possible by smartphone near a keyboard on the same desk. The smartphone's placing a accelerometer can then detect the vibrations created by typing on the keyboard and then translate this raw accelerometer signal into readable sentences with as much as 80 percent accuracy The technique involves working through probability by detecting pairs of keystrokes, rather than individual keys. It models: keyboard events in pairs and then works out whether the pair of keys pressed is on the left or the right side of the keyboard and whether they are close together or far apart on the QWERTY keyboard. Once it has worked this out, it compares the results to a preloaded dictionary where each word has been broken down in the same way. Similar techniques have also been shown to be effective at capturing keystrokes on touchscreen keyboards while in some cases, in combination with gyroscope or with the ambient light sensor

Denial of Service (DOS / DDOS)

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop shop the attack simply by blocking a single source,

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a making it for legitimate customers to enter, thus disrupting trade

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.

Denial-of-service attacks are characterized by an explicit attempt by attackers to prevent legitimate use of a service. There are two general forms of DoS attacks, those that crash services and those that flood services. The most serious attacks are distributed

Distributed DoS

A distributed denial-of-service (DDoS) is a large-scale DoS attack where the perpetrator uses more than one unique IP address, often from thousands of hosts infected with malware. distributed denial of service attack typically involves more than around 3-5 nodes on different networks: fewer nodes may qualify as a DoS attack but is not a DDoS attack. Since the incoming traffic flooding the victim originates from different sources, may be impossible to stop the attack simply by using ingress filtering also makes it difficult to distinguish legitimate user traffic from attack traffic when spread across multiple points of origin. As an alternative or augmentation of a DDoS attacks may involve forging of IP sender addresses further complicating identifying and defeating the attack

Method of attack

An application layer DDoS attack is done mainly for specific targeted purposes, including disrupting transactions and access to databases. It requires fewer resources than network layer attacks but often accompanies them. An attack may be disguised to look like legitimate traffic, except it targets specific application packets or functions The attack on the application layer can disrupt services such as the retrieval of information or search functions on a website

Advanced persistent Dos

An advanced persistent DoS (APDOS) is associated with an advanced persistent threat and requires specialized DDoS mitigation. These attacks can persist for weeks, the longest continuous period noted so far lasted 38 days. This attack involved approximately 50+ petabytes of malicious traffic.

Attackers in this scenario may tactically switch between several targets to create a diversion to evade defensive DDoS countermeasures but all the while eventually concentrating the main thrust of the attack onto a single victim. In this scenario, attackers with continuous access to several very powerful network resources are capable of sustaining a prolonged campaign generating enormous levels of un-amplified DDoS traffic

APDoS attacks are characterized by:

- Advanced Reconnaissance
- Tactical Execution
- Explicit Motivation
- Large Computing Capacity
- Simultaneous Multi-Threaded OSI Layer Attacks

Waterhole Attack

Watering hole is a computer attack strategy, in which the victim is of a particular group in this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group becomes infected. Hacks looking for specific information may only attack users coming from a specific IP address. This also makes the hacks harder to detect and research The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.

Defense Techniques

Websites are often infected through zero-day vulnerabilities on browsers or other software. A defense against known vulnerabilities is to apply the latest software patches to remove the vulnerability that allowed the site to be infected. This is assisted by users to ensure that all of their software is running the latest version. An additional defense is for companies to monitor their websites and networks and then block traffic if malicious content is detected.

Process of Waterhole Attack

A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment. The name watering hole attack is inspired by predators in the natural world who lurk near watering holes, looking for opportunities to attack desired prey In a watering hole attack, the predator lurks near niche websites popular with the target prey looking for opportunities to infect the websites with malware or mal-vertisements that will make the target vulnerable.

Watering hole attacks, which tend to focus on legitimate, popular websites, are a derivative of pivot attacks, which target one thing to get at another. In a watering hole attack the attacker first profiles its targets who are typically employees of large enterprises, human rights groups or government offices -- to determine the type of websites they frequent. The attacker then looks for vulnerabilities in the websites and injects malicious JavaScript or HTML code that redirects the target to a separate site where the malware is hosted. This compromised website is now ready to infect the target with the injected malware upon access.

While watering hole attacks are uncommon, they pose a considerable threat since they are difficult to detect and typically target high-security organizations through their low-security employees, business partners, connected vendors or an unsecured wireless network.

Brute Force

Brute Force Attack can be defined as the way to gain access over a website or a web server by successive repetitive attempts of various password combinations. This is done to capture the data of the user such as USERID, pin, etc, in brute force software to generate consecutive password strengths a software will also be developed with the given data. This is also done by introducing malicious software with the help of bots on the target site. This attack is mostly done by cyber-crime people to gain personal or secure data for their own purpose.
There are two categories in Brute Force Attacks.

- White Hat Hacking
- Black Hat Hacking

White Hat Hacking:
People who hack computers or servers or any other source for a good cause is called White Hat Hackers. Basically, white hat hackers hack systems to check the vulnerability of the system or software or application.

Black Hat Hacking:
People who hack computers or servers or any other source for a bad cause are called as black hat hackers. Basically black hat hackers hack systems to steal sensitive data from the system or software or application. The work of the white hat hackers is to save sensitive data from black hat hackers. White hat hackers

find the vulnerability of the system or software or application and solve issues.

Types of Brute Force Attack

The main purpose of this attack is to have access to personal and secure information. The methods to try are also many. Let us now discuss them There are mainly two types of brute force attacks they are:

- Directory guessing brute force attack
- Password guessing brute force attack

Directory Guessing Brute Force Attack

The probability of these attacks is more on websites and web servers, for this they use the directories/folders which are rarely used or hidden and then try to personalize them

Password Guessing Brute Force Attack

Password guessing attacks are most common in websites and web servers. In this, the attackers use vectors or software to compromise websites which involves trying multiple combinations of user id and password until they find one with the right data. Once entered they can compromise the site with phishing or malicious software: Most attacks are done by using the most commonly used user id and password combinations.

They also manipulate the data related to the website to easily grab the details

Purpose

Purpose of a brute force attack is to gain access to a software or website or mobile application or any other source. The word brute force itself states that it is a force attack to gain access to a software or website or any other source. Using Brute Force Attack we can find usernames and passwords of the users forcibly

How can the Brute Force Attack Happen?

To successfully accomplish a brute force attack we need to find a vulnerability and we need to implement our attacks to crack the password protected website or application or server or any other source. Many basic and dynamic websites or servers or applications will be hacked on a regular basis to steal sensitive data.

The Motive behind a Brute Force Attack

The motive behind a brute force attack is stealing sensitive data and making money out of it which is really bad. Stealing sensitive data can lead a company to the loss or can even lead a whole country into the problem. People became smart and people are able to hack some highly secured websites and applications like NASA, Facebook. Twitter etc.

What to do after a Brute Force Attack

If someone steals sensitive data from your software or website or server, first find the vulnerability on your server or system or application and solve it and then start tracing the IP address of the hacker who stole the data from your server or application. Check any other vulnerabilities are present on your site where you can enter into your site forcibly Better to take preventions and securities before getting hacked.

Phishing and Fake WAP

Phishing is a type of Social Engineering attack that aims to obtain sensitive information including the bank account number, usernames, passwords, and credit card details. It is mostly done by sending fake emails that appear to have come from a legitimate source, or it can be in the form of Phishing. The recipient is mostly manipulated to click a malicious link that can install malware or access sensitive information. Or it can simply be a case of website link that redirects the recipient to a malicious website in order to obtain login credentials

Common Features of Phishing Emails:

It will have an eye-catching subject such as "Congratulations! You've won an iPhone"

It will reflect a sense of urgency so that the recipient doesn't get enough time to re think and make a mistake in the hurry that can later benefit the attackers

It will have attachments that make no sense with respect to that email

Threats of Phishing:

Almost all kinds of Internet theft is possible through Phishing. It can be very dangerous if the received malicious link is being clicked. It can:

- Redirect to a website used for malicious purposes.
- Install malware or Ransom ware to the PC.
- Steal confidential data of the Internet users such as credit card information
- Steal the identity of the users for the purpose of Identity theft

Preventive Measures:

The first and foremost thing that I recommend is to go through the email thoroughly. The attackers make tiny mistakes which often get skipped while reading. Re-check the spellings, the source and the subject before taking any further step.

- Computer security tools should be in updated form.
- Never open suspicious email attachments

- Never click on suspicious email links
- Don't provide confidential information via email. over phone or text messages
- Don't post your personal data, like your vacation plans, or your address or phone number, publicly on social media.

Eavesdropping

Eavesdropping is secretly or stealthily listening to the private conversation or communications of others without their consent. Network eavesdropping is a network layer attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information. This type of network attack is generally one of the most effective as a lack of encryption services are used.
It is also linked to the collection of metadata.

Eavesdropping is an unauthorized digital communication, real-time interception of a private communication, such as phone calls, instant message, video conference or fax transmission As simple we can explain, it is the act of intercepting digital communication between two
points as part of Sniffing.

Cyber attackers can sniff the network and get the record output of sensitive data from insecure networks. The packets are encrypted, but it can view by using some cryptographic tools and able to intercept for getting private information such as your password, credit card details from the unsecured website that does not use SSL encryption

Methods

Data sniffing in the context of network security, corresponds to theft or interception of data by capturing the network traffic using a sniffer. When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer

Using a sniffer application, an attacker can analyze the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network

Sniffing attacks can be compared to a tapping of phone wires and getting to know about the conversation, and for this reason, it is also referred to as wiretapping applied to computer networks. Using sniffing tools, attackers can sniff sensitive information from a network, including Email traffic (SMTP, POP, IMAP traffic), Web traffic (HTTP, FTP traffic (Telnet authentication, FTP Passwords, SMB, NFS) and many more.

The Packet Sniffer utility usually sniffs the network data without making any modifications in the network's packets. Packet sniffers can just watch, display, and log the traffic, and this information can be accessed by the attacker

Man-In-The-Middle Attack

Man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Eavesdropping is one of the examples of man-in-the-middle attacks, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances.
For example, an attacker within reception range of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle.

Impact of Eavesdropping Attack

By using someone's bank account info to make unauthorized purchases or to transfer money to the cybercriminal account. By stealing a person's identity, in terms of their private information including Social security numbers (SSN), Home address, etc. Eavesdropping attack is generally performed by black hat hackers. However, government security agencies have also been connected.

Prevention

To prevent Eavesdropping network attacks, do not use applications that are using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred.

- Use Top VPN (Virtual Private Networks) to secure your network. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted.

- Use Internet Security software instead of Antivirus solutions. It can protect you from Network threat activities.

- Do not use Public Wi-Fi network

URL Obfuscation

An obfuscated URL is a web address that has been obscured or concealed and has been made to imitate the original URL of a legitimate website. It is done to make users access a spoof website rather than the intended destination. Obfuscated URLs are one of the many phishing attacks that can fool Internet users. The spoof site is often an identical clone of the original one in order to fool users into divulging login and other personal information An obfuscated URL is also called a hyperlink trick. Attackers usually use a common misspelling technique where they misspell a domain name to trick users into visiting. These obfuscated URL be a cause of malware entering a user's computers stem, URL obfuscation is used together with spamming, redirecting users using a misleading URL that leads to a malicious site URLs are strings of text that identify web resources such as websites or any kind of Internet server, so an obfuscated URL shows up as a meaningless query string to users. This hides the real address of the linked site when the user hovers over the link. URL obfuscation is not always used for phishing or cross-site scripting, but it is also used by legitimate websites to hide the true URL of certain pages so that they cannot be accessed directly by the users or allow certain procedures to be bypassed, It is also used as an anti-hacking procedure. This is termed as security through obscurity E.g:

Instead of clicking on PayPal.com, the hacker creates a fake website link which is called as PayPals.com

Buffer Overflow

A buffer is a temporary area for data storage. When more data gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding. In a buffer overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user, for example, the data could trigger a response that damages files, changes data or unveils private information. Attackers would use a buffer-overflow exploit to take advantage of a program that is waiting on a user's input.

There are two types of buffer overflows

- Stack-based
- Heap-based

Heap-based, which are difficult to execute and the least common of the two attack an application Hooding the memory space reserved for a program Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack memory space used to store user input.

A buffer overflow, or buffer overrun, is a common software coding mistake that an attacker could exploit to gain access to your system. This error occurs when there is more data buffer than it can handle, causing data to overflow into adjacent storage. This vulnerability can cause a system crush or worse, create an entry point for a cyber-attack.

Definition of a Buffer Overflow

A buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle. The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space. This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions.

Many programming languages are prone to buffer overflow attacks. However, the extent of such attacks varies depending on the language used to write the vulnerable program. For instance, code written in Perl and JavaScript is generally not susceptible to buffer overflow However, a buffer overflow in a program written in C, C++, FORTRAN or Assembly could allow the attacker to fully compromise the targeted system Cyber Criminals exploit buffer overflow problems to alter the execution path of the application by overwriting parts of its memory. Coding errors are typically the cause of buffer overflow.

DNS Poisoning

DNS Poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in the substitution of false IP addresses at the DNS level where web addresses are converted into numeric IP addresses, It allows an attacker to replace IP address entries for a target site on a given DNS server with IP address of the server controls. An attacker can create fake DNS entries for the server which may contain malicious content with the same name,

Defenses against DNS Poisoning

As an ethical hacker, your work could very likely put you in a position of prevention rather than pen testing. Here are defenses against the attacks:

- Use a hardware-switched network for the most sensitive portions of your network in an effort to isolate traffic to a single segment or collision domain
- Implement IP DHCP Snooping on switches to prevent ARP poisoning and spoofing attacks
- Implement policies to prevent promiscuous mode on network adapters.
- Be careful when deploying wireless access points, knowing that all traffic on wireless network is subject to sniffing
- Encrypt your sensitive traffic using an encryption protocol such as SSH or IPsec
- Port security is used by switches that have the ability to be programmed to allow only specific MAC addresses to send and receive data on each porn.
- IPV6 has security benefits and options that IPv4 does not have.
- Replacing protocols such as FTP and Telnet with SSH is an effective defense against sniffing. If SSH is not a viable solution, consider protecting older legacy protocols with IPsec
- Virtual Private Networks (VPNs) can provide an effective defense against sniffing due to their encryption aspect.
- SSL is a great defense along with IPsec.

ARP Poisoning

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines MAC addresses. ARP Poisoning is also known as ARP Spoofing.

Here is how ARP works

When one machine needs to communicate with another, it looks up its ARP table
If the MAC address is not found in the table, the ARP request is broadcasted over the network.
All machines on the network will compare this IP address to MAC address .
If one of the machines in the network identifies this address, then it will respond to the ARP_request with its IP and MAC address.
The requesting computer will store the address pair in its ARP table and communication will take place.

What is ARP Spoofing?

ARP packets can be forged to send data to the attacker's machine
ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch
The switch is set in forwarding mode and after the ARP table is flooded with spoofed ARP responses, the attackers can sniff all network packets.
Attackers flood a target computer ARP cache with forged entries, which is also known as poisoning. ARP poisoning uses Man-in-the-Middle access to poison the network

BOTs and BOTNETS

A botnet is a collection of internet connected devices infected by malware that allow hackers to control them. Cyber criminals use botnets to instigate betnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft and DDOS attacks. A botnet is a number of Internet connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack). steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or malicious connotation

How does a botnet attack work?

Botnet owners can have access to several thousand computers at a time and can command them to carry out malicious activities Cybercriminals initially gain access to these devices by using special Trojan viruses to attack the computers' security systems, before implementing command and control software to criable them to carry out malicious activities on a large scale. These activities can be automated to encourage as many simultaneous attacks as possible.

Different types of botnet attacks can include:

- Distributed Denial of Service (DDoS) attacks that cause unplanned application downtime
- Validating lists of leaked credentials leading to account takeovers
- Web application attacks to steal data
- Providing an attacker access to a device and its connection to a network
- In other cases, cybercriminals will sell access to the botnet network, sometimes known as a "zombie" network, so that other cybercriminals can make use of the network for their own malicious activities, such as activating a spam campaign.

How many bots are in a botnet?

The number of bots will vary from botnet to botnet and depends on the ability of the botnet owner to infect unprotected devices.

How can I protect myself against a botnet attack?

It is important to understand that a botnet is just a collection of Internet connected devices under the command and control of a botnet owner. As such, a botnet can be used to launch different types of attacks, each of which may require a different type of protection.

PS: The Botnet attacks an also be used in Client-Server Model Attacks und Peer-to-Peer Attacks