VIT UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING

Chapter 1: ETHICAL HACKING

By
Dr. Ravi Verma

About System Hacking

- The term system can be anything, either a desktop, laptop or tablet, etc. When the term "System Hacking" comes into play, it usually means the art of hacking a computer using tools and techniques. 'How to hack a system or computer?' is probably one of the most frequently asked questions by most Internet users and hacking enthusiasts. So here's a brief idea of what and how system hacking plays a significant role to doom the target.

What is System Hacking ?

- System hacking is a vast subject that consists of hacking the different software-based technological systems such as laptops, desktops, etc. System hacking is defined as the compromise of computer systems and software to access the target computer and steal or misuse their sensitive information. Here the malicious hacker exploits the weaknesses in a computer system or network to gain unauthorized access to its data or take illegal advantage.

How hacker will perform Hacking ?

- A hacker can hack the computer system because the hacker knows the actual work of computer systems and software inside the system. For this, a hacker has information about the systems, networking, and knowledge of other areas related to computer science. Anyone who is using a computer and is connected to the internet is susceptible to malicious hackers' threats. These online villains generally use viruses, malware, Trojans, worms, phishing techniques, email spamming, social engineering, exploit operating system vulnerabilities, or port vulnerabilities to access any victim's system.

What after Hacking System ?

- When your PC gets connected to the internet, the hacker may execute the malware on your PC and quietly transmits the personal, financial, and essential information without your knowing consent. These hackers can blackmail the victim for the money by stealing that sensitive information from your computer, which you don't want to reveal. After compromising the victim's system, the hacker can do these following things:

What after Hacking System ? Cont..

- Ruin the victim's data by deleting the files.
- Steal files and folders.
- Hijack victim's username and password.
- Steal money and credit card details while the victim is doing e-marketing or online transaction.
- Sell victim's information to third parties who may use this information for illicit purposes.
- Create traffic to shut down your website.
- Get access to the servers and manipulate the files, programs, etc.

Linux Hacking

- Now to hack a Linux-based computer system and get access to a password protected Linux system, we have to know Linux's basic file structure. As we know, Linux is considered to be the most secure OS to be hacked or cracked, but in the world of Hacking, nothing is 100% secured.
- Hackers usually use the following techniques to hack the Windows system.
- Hack Linux using the SHADOW file.
- Another technique commonly used by hackers is to bypass the user password option in Linux.
- In another technique, the hacker detects the bug on Linux distribution and tries to take advantage of it.

Window Hacking

The user password of Windows OS, which appears after the Windows starts logging in, lets users protect the computer from getting unauthorized access. Choosing a strong password of more than eight digits is an excellent practice. Henceforth you can protect your files and folders from the hands of malicious users. There are several tricks and techniques to crack a windows password. But, from the hacker's point of view, if you can use social engineer your victim and find a Windows computer open, you can easily modify the existing password and give a new password that will be unaware of the victim or the owner of the computer.

Precautions against System Hacking

- The following are the precautionary points you should know to protect from system hacking or computer hacking:
- Use extreme caution while entering chatrooms or dealing with chatrooms' users online.
- Continuously check for the accuracy of the personal account.
- Carefully deal with friends' requests from online social networking sites and emails.
- Don't open or click unnecessary emails from strangers or unknown senders.

Point to keep in mind to protect system from hacking

- Use both way firewall and keep updating.
- Update the OS for better patches.
- Avoid questionable websites.
- Use Internet Security Antivirus and Anti-malware software protection with definition updates.
- Increase the browser security settings.
- Download the required software from trusted sites only.
- Practice using safe email protocols such as SSL, SMTPS, etc.

Point to keep in mind to protect system from hacking Cont..

- Check whether the sites are HTTPS or not for better secured online services and transactions.
- Immediately delete those messages which you suspect to be spam.
- Try to use genuine software(s) and not the pirated ones because the pirated ones could be reverse-engineered. Hackers can attach monitoring or malicious tools and programs with the software.

Session Hijacking

- The importance of security is on the rise as digital innovation explodes. And as organizations launch more applications and evolve existing ones, the application attack surface grows. This provides cyber criminals with a greater opportunity to exploit application vulnerabilities. The threat is real: Verizon finds that 43% of data breaches are linked to application vulnerabilities.

Session Hijacking Cont..

- One of the vulnerability attack vectors that cyber criminals find fruitful is session hijacking. Searching for small windows of opportunity, hackers use advanced breaching techniques, that are also known as cookie hijacking. The ability to tap in and monitor activity for the duration of a session can prove dangerous, especially in the case of highly sensitive information. Hackers can do this by squeezing in unnoticed, possibly taking over, and eventually kicking users out of the session.

What Is a Session

- Though it seems like a complicated ENGAGEMENT of systems and networks, a computer's ability to communicate with a website comes from one single source. This source is known as the Transmission Control Protocol/Internet Protocol or TCP/IP. Certain limitations in TCP/IP are the reason it is vulnerable to attack. In an attempt to decrease the potential for attack, layers are added on top of TCP/IP in the hopes of stopping attacks long before they reach the core.

What Is a Session Cont..

- Sessions refer to the time in which two systems are in communications with one another. Common systematic communications include computer-to-computer and client-to-server. From login to logout, information entered throughout the duration of communications is prone to storage depending on cookie settings. These cookies collect and store useful information for future logins. PHP scripts are the culprit behind this credential storage, with their unmatched connectivity properties that have revolutionized webpage interactions.

What Is Session Hijacking

- When a session is hijacked, attackers slip in unnoticed and are able to monitor all activity taking place for the duration. Every session is marked with a session cookie, which reports back to the server. If an attacker obtains a session cookie, the session ID or session key is put at risk. With a session ID, hackers can input information into their own browser that is recognized by the server as the original connection.

What Is Session Hijacking

- Larger corporations use cookies differently to enhance efficiency. Their single sign-on (SSO) systems collect information from several authenticated users at a time. A successful hijacking session puts all of these accounts at risk, as well as other applications connected within the system. When full access to accounts is achieved, servers cannot tell the difference and permit all activities without suspicion.

What Is Session Hijacking

- With full access to an SSO, hackers have a huge database of information at their disposal. Information at risk includes personally identifiable information (PII), sensitive company details, among other data types. With access to these details, hackers have the ability to wreak havoc in multiple ways. Stopping application attacks before they start is the best way to combat session hijacking, accentuating the importance of understanding how session hijacking works and the potential damage attacks can cause.

Types of Vulnerabilities Exploited in Session Hijacking Attacks

- Experienced hackers know that several application vulnerability options exist when it comes to session hijacking. Using advanced session hijacking techniques and a basis of vast programming knowledge, bad actors can decide which session hijacking method is best for the account or information they wish to exploit. Things like the exact pathway they will use to gain access and the chosen IP address come into play when selecting the best and most robust option.

Cross-Site Scripting Vulnerabilities

- Cross-site scripting (XSS) vulnerabilities are the most popular attack vector used during a session takeover. Hackers look for XSS vulnerabilities in applications, injecting client-side scripts. Most typically, JavaScript is used and embedded into webpages. This newly written script will cause the browser to act as coded when loading a faulty page. If safeguards or application security tools are not in place, the loaded page provides hackers with sensitive information needed to uncover the session key. The most likely execution is in the form of email, one with the name and/or logo of a reputable company. Though it may seem legitimate, links within the email lead to malicious websites.

Session Side-Jacking Vulnerabilities

- Session side-jacking likely comes to mind for many when session hijacking is mentioned. Hackers use packet sniffing to observe network activity. It requires the hacker to actively jump in after users have logged in successfully. This is especially dangerous for sites that use secure sockets layer/transport layer security (SSL/TLS) encryption for logging in, which allows impersonation of accounts if the session key is successfully acquired. Insecure Wi-Fi hotspots are a popular area that cyber criminals target with session side-jacking attacks, as they give them the option to set up their own access points for executing man-in-the-middle-attacks.

Session Fixation Vulnerabilities

- Bad actors often create malicious links that lead to fake websites—session fixation attacks. They do this hoping that users will click on them without a second thought. By clicking on the wrong link, users could provide cyber criminals access to session keys by leading them to a vulnerable server. If hackers pay close attention to detail, they can create a page that mimics that of a well-known company, and in turn, make it more difficult for users to spot suspicious or insecure activity. Once a user clicks on a link, a valid login form appears prompting users to log in. After their credentials are entered, attackers use the session key that is disclosed to take over the session.

Malware Installation Vulnerabilities

- Another vulnerability initiated by clicking links is malware code installation. Malware is defined as any type of software created to damage a network, computer, or server. Bad apples with development skills generate this software and hide it in the form of a clickable link. If clicked, a download of the software begins immediately. Typical actions include scanning of web-based traffic hunting for session cookies along the way and access to local storage. Local storage, also known as the “cookie jar,” is a playground for attackers, providing direct access to the user’s cookie file.

What Hackers Can Do with Session Hijacking

- Active monitoring is just the tip of the iceberg for session hijacking. Cyber criminals using session hijacking can completely take over a system, both at the network and application level. When hackers get access to an SSO, multiple applications are at risk. Cookie storage in SSO stores credentials used for all applications, including those with sensitive personal information. Entering directly into the server, attackers are essentially invisible during and after an application session. Then, long after users log out, hackers can create specific modifications to the server for future logins.

What Hackers Can Do with Session Hijacking

- Neither users nor larger corporations may know they’re victims of session hijacking until it is too late. Hijackers can silently track and monitor any activity, waiting for the right time to cause harm. This puts both financial and personal information at risk for both individuals and corporations. As both parties turn to applications for a more convenient way of doing things, the need to enhance their security rises.

How to Prevent Session Hijacking

- Just like with most methods of protection, prevention is key. Stopping breaches before they can begin requires constant monitoring and updating of malware. Most of the time, ethical hackers attempt to point out vulnerabilities in servers in the hope of providing companies and individuals a sense of security. For the time being, session hijacking poses a large threat due to its exploitation of fundamental activities executed by the vast majority of web applications.
- Apart from basic safe surfing rules while on the web, both individuals and cybersecurity teams can reduce their risk of a hijacked session in a few ways. As the use of applications increases, shielded practices are key both during and after use.

Use HTTP Headers to Tighten Up Security

- One iron-clad security system works by adding a few extra lines of code to the beginning of application scripts. For example, an X-XSS protection header stops malicious code in its tracks. There are thousands of headers out there, some approved by the Internet Engineering Task Force (IETF).

HTTP to HTTPS Redirects

- For proper SSL/TLS encryption of all traffic during a session, it is best to use HTTPS, or more specifically, HSTS (HTTP Strict Transport Security). Unlike its four-letter counterpart (HTTP), HTTPS makes interception of plaintext session ID impossible even if they are monitoring activity. It also guarantees that all connections are encrypted, thus increasing the difficulty of session takeover. Embedding an HSTS header enforces applications to only connect to HTTPS and will redirect any HTTP activity.

Embedding RASP

- Runtime application self-protection (RASP) embeds security instrumentation within the application it is protecting. This enables it to spot attacks on vulnerabilities and block them in real time. RASP can be thought of as a weapon used by applications to shield itself. From the time a session begins, it works to monitor activity, including data requests and application-to-system solicitations.

Modify Caching

- Though caching works wonders for performance, it can put a damper on security. When using applications, sensitive information is stored in the browser's cache. If access to the computer is not limited to one sole user, anyone can access sensitive information. It could be as easy as hitting the "back" button, depending on the settings that are enabled. Further, disabling caching can become tedious, especially for those who are in and out of applications all day. That said, this could be an option only for those applications with confidential information.

Keeping Applications Secure from Session Hijacking

- The threat that session hijacking imposes is substantial. Digital transformation is pushing companies to employ more online databases to handle the burgeoning amount of data that is now used by existing and growing numbers of new applications. Data breaches can be a huge risk exposure, providing cyber criminals with access to numerous accounts.
- Session hijacking attacks target a long list of application vulnerabilities, and when their exploitation is successful, bad actors can slip into a session unnoticed, sometimes detected too late. As a matter of fact, the average time it takes to notice an attack (dwell time) is about 95 days. Imagine what attackers can do with full access to accounts for such a long time. Because of its potential to cause irrefutable damage, session hijacking is on the long list of things security and operations teams need to heed.

Keeping Applications Secure from Session Hijacking

- Today, most security measures focus on prevention, causing security teams to try and think ahead of hackers. It is becoming an inexorable cycle where both sides are successful time and time again. Legacy application security solutions that rely on penetration testing and application scanning simply cannot scale to support the modern software development life cycle (SDLC). Unable to keep up with SDLC, legacy application security approaches miss true vulnerabilities, generate large numbers of false positives, and incur growing security debt. Instead, organizations need to seek out application security that uses instrumentation to embed security within software and delivers continuous testing of software in development and monitoring of software once it is in production.

Question Please?

THANK YOU