ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Πληροφορικής

Εργασία Μαθήματος

"Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων"

Τίτλος Εργασίας	***Understanding Cyber Threats: Human Factors and Defense Strategies***
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Ανδριανόπουλος Βασίλειος 2303
	Τσαντίλας Αλέξανδρος 2344
	Γιώργος Τσουτσουλιανούδης 2347
Ημερομηνία παράδοσης	25/2/2024

Contents

Introduction

Hackers, ubiquitous in the cybersecurity landscape, possess diverse psychological profiles influencing their motivations for cyber attacks. These motivations, ranging from curiosity and recognition-seeking to ideological convictions and financial incentives, intricately shape hackers' decision-making processes and target selection strategies. Understanding the psychological underpinnings of hackers is vital for cybersecurity stakeholders to develop effective defense
mechanisms against cyber threats.

Profiles

Novices

Novices are known for their abilities and limited social interactions. They often delve into hacking due to curiosity or a lack of interests lacking the expertise for more advanced attacks. Their inspiration usually comes from guides, tutorials or forums where they find vulnerabilities and attempt basic exploits motivated more by a desire to learn than any harmful motives. With an understanding of hacking basics novices form a mostly harmless part of the cybersecurity world often gaining knowledge through trial and error.

Cyberpunks

Individuals thrive in underground communities, building relationships and using their skills to gather information from others. May use existing codes/scripts but with some modifications or write their own ones. They have abilities and are driven by the excitement of

rebellion and exploration. Their actions are fueled by a sense of adventure especially when they stumble upon vulnerabilities or engage in hacks, for entertainment. Unrestricted by guidelines, these cyber enthusiasts embody the essence of hacking culture, often testing limits and questioning societal standards through their digital escapades.

Insiders

Individuals with insider access tap into the resources of an organization usually driven by incentives or personal grievances (revenge). Usually they are disgruntled current or ex-employees who abuse their access to get what they want. Their social skills range widely, often focusing on cultivating connections in spaces. Factors that spur them into action include having information about weaknesses within the organization or feeling discontented leading to activities such as stealing data or speaking out about misconduct. Working discreetly within settings insiders present a risk as they can exploit internal weaknesses, for personal benefit or to uncover unethical behavior.

Old Guards

Old Guards are hackers who do not hack for malicious reasons but show little concern for personal privacy. They usually use customized codes/scripts/penetration testing tools to reveal vulnerabilities in existing systems. Though not harmful their activities can occasionally cross lines as they value exploration and testing over respecting privacy rights. These individuals represent a mix of hacking principles and a relaxed attitude, towards privacy standards. These individuals represent a mix of hacking principles and a relaxed attitude, towards privacy standards.

Professionals

Skilled individuals use their level expertise and tools to engage in hacking for financial profit and to enhance their professional standing. They move within both networks and more mainstream professional communities, motivated by attractive opportunities and intricate problems. Their motivations are sparked by targets and the rise of technologies driving them to seek out complex cyber exploits. Operating at the cutting edge of cybercrime these skilled individuals present a challenge utilizing their knowledge and resources to coordinate cyber activities aimed at achieving financial or strategic benefits.

Hacktivists

Hacktivists combine their abilities with deep beliefs utilizing hacking as a means of advocating for political or social causes. Their drive for transformation is fueled by events linked to their mission or perceived unfairness. Although skilled in internet activism they may encounter difficulties in face to face interactions. Motivated by a passion for advocacy, hacktivists question. Support various movements through impactful online activities sometimes blurring the boundaries, between virtual demonstrations and unlawful cyber behavior.

Nation States

Nation States, driven by financial gain, revenge, or ideology, exhibit high extraversion and assertiveness. They are highly trained and extremely skilled hackers who work directly or indirectly for one government to destabilize, disrupt, and destroy the systems and networks of a nation or government. Their attention to detail is evident in their planned and sophisticated cyber assaults. Their conscientiousness is reflected in a meticulous, staged approach to sophisticated attacks. Socially, they are adaptable to building virtual relationships within the hacking community and may be talkative in conveying state-sponsored goals. Their manipulation is strategic, aimed at achieving geopolitical objectives through electronic means.

Students

Students possess abilities and motivations often fueled by curiosity and a desire for learning. They participate in hacking as a means of exploration spurred by the discovery of vulnerabilities during their coursework and school projects. Despite the absence of industry ties they add to the richness of hacking practices through their spirit of experimentation and quest for findings. Positioned at the forefront of cybersecurity knowledge students serve as a presence in the hacking community guided by a sense of wonder and an eagerness to understand the changing landscape of cyber threats.

Petty Thieves

Petty thieves typically have basic, to moderate abilities and are often driven by motives for quick financial rewards. Their social interactions may be. They could find social situations challenging. They are inclined to target opportunities and vulnerable individuals engaging in activities like data theft or straightforward scams for personal gain. In their approach they employ methods such as trojans and are easily accessible online. To obtain information, like credit card or bank account details.

Digital Pirates

People known as Digital Pirates have some knowledge. They are usually active in online piracy groups. Their main driving forces include a desire for items and a rebellious attitude towards authority, which can sometimes make it challenging for them to interact socially in settings. Factors that prompt their actions include the release of content and crackdowns on piracy leading them to engage in activities like sharing or distributing software and media. Their strategy typically involves either directly or indirectly obtaining copyrighted material. Then making it available thus contributing to the availability of unauthorized copies, on various digital platforms.

Crowdsourcers

Crowdsourcing participants work together in communities combining technical abilities and resources. They are driven by a shared goal of problem solving and building their reputation feeling at ease, in environments. They get involved when invited to join or faced with community challenges coming together to uncover weaknesses or tackle issues. Their approach involves collaborating and sharing expertise for activities, like creating software or overseeing botnets sometimes pursuing questionable objectives using unconventional means.

Crime Facilitators

Individuals known as Crime Facilitators possess moderate abilities and engage in underground markets, where they establish trust to aid criminal operations. Driven by motives and the allure of opportunities they may demonstrate manipulative behaviors. Factors that prompt their actions include prospects and the demand for goods or services leading them to engage in activities like selling stolen information or offering cybercrime services. Their approach involves equipping cybercriminals, with tools and technical expertise enabling them to execute attacks and thereby bolstering criminal operations in the digital sphere.

Cross site Scripting

Introduction

Cross-Site Scripting (XSS) stands as a recognized web attack wherein malicious web code, typically in script form, is transmitted or executed through the victim's web browser using their web applications. This execution can potentially filter personal information, pilfer user cookies for identity hijacking during fraudulent sessions, providing attackers with the opportunity to steal sensitive data or even gain control over specific devices. XSS accounts for 40% of attack attempts, followed by SQL injection (SQLi) at 24%, a 7% incidence of a cross-section attack, a 4% occurrence of local file inclusion (LFI), and the least prevalent being distributed denial of service (DDoS) at 3%.

Vulnerabilities

XSS commonly takes place under the following circumstances:

- Unreliable data is capable of being input into a web application.
- The web application dynamically generates this untrusted data.
- A user visits the website, which has been created through a web browser infected with a malicious XSS script, previously contaminated by the untrusted data.
- An XSS script sent by a server is executed within a web page, operating within the same domain context as the web server.

Another important factor is that JavaScript has become an integral and commonplace element of the internet. Consequently, to expedite and simplify development, numerous web applications depend on JavaScript libraries to avoid duplicating efforts. Regrettably, a considerable number of these JavaScript libraries contain vulnerabilities, necessitating the update to their most recent versions.

Presently, the majority of web applications utilize cookies to preserve the session status with the user, meaning that cookies are dispatched subsequent to user authentication (session cookie). Subsequent logins do not require additional authentication, as the validated cookies are solely checked to authorize the new request. While this authentication feature enhances user experience, it also renders cookies susceptible to attacks since they are generated by websites and contain limited data that can be transmitted between a sender and a receiver. Based on users' browsing patterns, cookies can identify individuals by storing their website activity history, allowing for the delivery of more tailored content in line with their preferences. For instance, upon a user's initial visit to a webpage, a cookie is stored on their device. Upon subsequent visits, the website's server requests the same cookie to update it with new site configurations, resulting in a highly personalized user experience.

Techniques

As per the existing literature, three categories of attacks are identified: *persistent XSS*, *non-persistent XSS*, and *Document Object Model (DOM) XSS*.

Vulnerabilities are identified not only in the software and hardware but also in the users, particularly developers, who form an integral part of any computing environment. XSS attacks exploit deficiencies in mechanisms for filtering and validating input fields within web

forms. This exploitation enables the transmission and execution of malicious scripts stored as instructions in text files. These scripts are interpreted line by line in real-time during execution.

The distinction among the three types of attacks lies specifically in the location of their execution. Direct and indirect XSS attacks take place on the server side, whereas DOM XSS occurs independently on the client side (web browser) without any intervention from the server. As the code can originate on the server side, it becomes the responsibility of the application developer to safeguard against these attacks, irrespective of the specific type of XSS vulnerability. Another differentiating factor among the attacks is the timing and location of their execution. In the case of the first two, malicious codes are injected during the processing of requests originating from entries programmed through HTML. In contrast, with DOM XSS, the malicious code is directly injected into the application during its execution on the client.

Countermeasures

Modern web frameworks help reduce XSS vulnerabilities by promoting good security practices such as templating and auto-escaping. XSS attacks require attackers to insert and execute malicious content on a webpage, emphasizing the need to protect all variables in a web application through validation and proper escaping. This practice, known as perfect injection resistance, is facilitated by frameworks, although no framework is entirely flawless, and security gaps may still exist. Output encoding and HTML sanitization are effective measures to address these gaps, with output encoding recommended for displaying user-entered data verbatim and HTML sanitization used when users need to author HTML, preserving intended functionality while preventing XSS attacks.

A Web Application Firewall (WAF) is a security solution that acts as a protective barrier for web applications against malicious activities such as SQL injection and cross-site scripting attacks. It monitors and filters incoming HTTP traffic, enforcing security policies to detect and block threats, thus enhancing the overall security of the application.

Content Security Policy (CSP) is a security measure that protects against cross-site scripting (XSS) and code injection attacks by controlling the sources from which content can be loaded on web pages. It allows administrators to define and enforce policies that restrict the execution of certain content or scripts to trusted sources, reducing the risk of security vulnerabilities. Implemented through HTTP headers or HTML markup, CSP enhances web application security by preventing unauthorized access to sensitive data.

Man in the middle attacks

Introduction

There are two primary types of man-in-the-middle attacks: standard MITM attacks, where a malicious user intercepts direct communication between parties, and MITC attacks, which involve intercepting communication between a user and cloud services. In an MITM attack, the attacker intercepts and manipulates data exchanged between a service provider and the user, posing as the user to steal credentials and financial data. MITC attacks exploit vulnerabilities in cloud synchronization token systems, allowing attackers to impersonate cloud services and manipulate tokens for unauthorized access. MITM attacks typically involve interception and decryption, exploiting vulnerabilities in unsecured Wi-Fi routers. MITB attacks, a variant, inject malware into the victim's browser to collect sensitive data.

Techniques

MITM attacks encompass several methods:

- Spoofing-based MITM involves intercepting communication between hosts through spoofing attacks, controlling data without hosts' awareness.
- SSL/TLS MITM involves inserting into the communication channel between victims, establishing separate SSL connections, and relaying messages without detection to record or modify data.
- BGP MITM hijacks IP addresses to route traffic through the attacker's Autonomous Station (AS) for manipulation.

- False Base Station (FBS)-based MITM forces victims to connect to a fake Base Transceiver Station (BTS) for traffic manipulation.

Vulnerabilities

Weak Authentication: Systems with weak or easily guessable authentication methods can be compromised, allowing attackers to gain unauthorized access to communication channels.

Lack of Encryption: Communication channels that transmit data without encryption are vulnerable to interception and manipulation by attackers.

Unsecured Wi-Fi Networks: Public Wi-Fi networks lacking proper encryption or authentication measures are susceptible to MITM attacks, as attackers can eavesdrop on traffic passing through the network.

DNS Spoofing: Manipulation of DNS responses to redirect users to malicious websites allows attackers to intercept and modify communication between users and legitimate services.

ARP Spoofing: By spoofing ARP (Address Resolution Protocol) messages, attackers can associate their MAC address with the IP address of another device on the network, leading to interception and manipulation of traffic.

SSL Stripping: Exploiting vulnerabilities in websites or applications to downgrade HTTPS connections to HTTP allows attackers to intercept and view plaintext communication.

Countermeasures

S-ARP is an extension of ARP that utilizes public-key cryptography to authenticate ARP Replies. Upon network entry, hosts generate public and private key pairs, sending them along with signed certificates to the Authoritative Key Distributor (AKD). This cryptographic

approach allows any party to verify the legitimacy of transmitted requests, effectively preventing ARP spoofing attacks.

Dynamic ARP Inspection (DAI) is a security feature implemented by certain switches to protect networks from ARP spoofing-based MITM attacks. DAI ensures that only legitimate ARP Requests and Responses are forwarded within the network. By monitoring the validity of received ARP packets against a trusted (IP, MAC) mapping database, Ethernet switches can effectively prevent unauthorized ARP activity, enhancing network security.

Force SSL/TLS connection solutions enforce the use of SSL/TLS connections between communicating parties. ISAN-HTTPSEnforcer utilizes JavaScript API to redirect users to HTTPS, but the initial connection may still be insecure, potentially vulnerable to SSL/TLS MITM attacks if JavaScript API calls are stripped from response packets or if JavaScript is disabled. HTTP Strict Transport Security (HSTS) is a similar solution where websites can mandate SSL/TLS connections by attaching a special header in response packets, instructing browsers to establish HTTPS connections for specified sub-domains.

DDoS Attacks

Introduction

A Denial of Service (DoS) attack involves an individual or a group attempting to disable an online service. This poses significant risks, particularly for companies like Amazon and eBay, heavily dependent on uninterrupted online operations for their business. In recent history, there have been notable large-scale attacks on prominent internet sites prompting extensive efforts to develop mechanisms for detecting and mitigating such attacks. The largest DDoS attack recorded occurred in September 2017 when Google services were targeted, reaching a magnitude of 2.54 Tbps. Google Cloud made this attack public in October 2020. The assailants utilized spoofed packets sent to 180,000 web servers, causing them to respond to Google. Notably, this incident was part of a series, as the attackers had executed multiple DDoS attacks on Google's infrastructure in the preceding six months.

Although the inception of denial of service attacks, facilitated by tools automating network setup and attack launches, dates back to around 1998, various forms of these attacks have been employed. Generally, DoS attacks can be categorized into three types:

Exploiting vulnerabilities or implementation bugs in the software of a service to bring it down.
Utilizing all available resources on the target machine.
Consuming all the bandwidth accessible to the victim machine. The third type is commonly referred to as bandwidth attacks.

Vulnerabilities

The internet was initially designed with a focus on functionality rather than security. The widely used TCP/IP protocol suite, fundamental for data communication, operates under the assumption that all participating hosts have no malicious intent. The internet infrastructure lacks built-in security measures to shield hosts from potential threats posed by other hosts failing to regulate their behavior. For instance, the TCP protocol expects hosts to reduce packet transmission rates upon detecting congestion-related packet losses. However, a host neglecting these conditions can easily overwhelm intermediate links to the destination.

This design leaves the internet susceptible to various denial-of-service (DDoS) attacks. Several internet features contribute to the vulnerability of DDoS attacks:

- *Dependency on Internet Security:* DDoS attacks often originate from compromised hosts. Regardless of the security measures on a specific host, it becomes vulnerable to DoS attacks if there are insecure hosts in the internet that can be exploited for launching such attacks.

- *Tracing Difficulties:* The TCP/IP protocol, used throughout the internet, operates on a connectionless IP protocol. Routing decisions are made at each step based on

destination addresses, making it challenging to trace attacks back to their source. IP spoofing, where attackers create packets with incorrect source IP addresses, adds to the difficulty of identifying the true source of an attack.

- *Limited Resources:* The interconnected hosts and networks within the internet have finite resources such as bandwidth, processing power, and storage capacities. Denial-of-service attacks target these resources, and even if the attack doesn't completely shut down the victim, it can exhaust resources, diminish service quality, and lead to significant financial losses for service providers.

- *Target-Rich Environment:* The internet is described as a "target-rich environment" due to the numerous hosts and networks with vulnerabilities that can be exploited for gaining control. Attackers can easily compromise a large number of hosts, using them as a launching pad for Distributed Denial of Service (DDoS) attacks.

- *System Vulnerability:* Breaking networking infrastructure and protocols is often easier than developing them. Many internet hosts, including intermediate routers, expect specific packet formats and traffic behavior. The lack of foresight regarding malicious usage during the software design phase can lead to unexpected behavior in network systems, such as routers allocating memory buffers while waiting for datagram fragments, which can be exploited with malformed fragments indicating large or negative offsets.

Techniques

Hence, to initiate a DDoS attack, the attacker must undergo the following stages:

- *Compromising Hosts and Deployment:* The attacker identifies vulnerable hosts through network scanning, exploits known vulnerabilities to compromise systems, and deploys software on them, transforming them into agents or handlers in the

attack network. The process may include a propagation step, where compromised hosts recursively engage in scanning, exploitation, and deployment. In the early stages of DDoS technology, attackers manually executed all four steps, but automation has progressively become more prevalent. Notably, the T0rnkit toolkit was among the pioneering DDoS tools to automate scanning, exploitation, and deployment.

- *Propagation Techniques:* DDoS tools utilize sophisticated self-propagation techniques, with advancements in propagation methodologies that include central chain propagation, back chaining propagation, and autonomous propagation. In central chain propagation, the attack toolkit is duplicated from a central server to the newly compromised host through transfer protocols like HTTP, FTP, or RCP after successfully compromising a host. Back chaining propagation involves copying the attack toolkit from the attacking host to the compromised host. Autonomous propagation is exhibited by certain worms, like the Morris worm of 1988 and the Code Red worm, wherein attack instructions are embedded directly into the code, enabling rapid dissemination without the need for external file transfers.

- *Establishing Communication Channels:* As the DDoS network expands, maintaining control becomes challenging. Handlers aid communication with agents, typically listening for commands on well-known ports. Agents and handlers communicate through various channels, making it challenging to detect DDoS tools. Techniques like encryption and IRC channels are utilized, enhancing the complexity of communication and avoiding detection.

- *Launching the DDoS Attack:* With the DDoS network in place and communication infrastructure established between agents and handlers, the attacker issues commands to agents to initiate packet transmission to the victim host. Agents aim to send unusual data packets (e.g., TCP floods, ICMP floods, UDP floods) to maximize disruption.

The basic packet attack types favored by DDoS tools include TCP floods, ICMP floods, and UDP floods. While the tools have evolved in scanning, exploitation, propagation, and agent-handler communication sophistication, the attack payload, including TCP, ICMP, and UDP floods, has remained largely unchanged due to its sustained effectiveness.Notably, recent attacks have employed lethal and potent amplification techniques, utilizing DNS, NTP (Network Time Protocol), or SNMP (Simple Network Management Protocol), enabling rapid escalation to substantial attack intensities.

Countermeasures

Load balancing is a straightforward strategy that empowers network providers to enhance the available bandwidth for essential connections, safeguarding them against disruptions in the face of an attack. An extra layer of protection involves replicating servers to compensate if some become compromised during a DDoS attack.

Honeypots function as closely monitored network decoys with various purposes, such as diverting attackers from more valuable machines, offering early alerts on emerging attack trends, and enabling thorough examination of adversaries during and after honeypot exploitation. The effectiveness of honeypots relies on the engagement of hackers since any interaction with these decoys is inherently unauthorized, adhering to the concept that legitimate users should not be utilizing or engaging with them.

Phishing Attacks

Introduction

Phishing remains a significant worry as numerous internet users are deceived by it. This type of attack, known as social engineering, involves a phisher enticing users to divulge sensitive information by deceitfully leveraging the identity of a reputable organization or entity in a systematic manner, aimed at fostering trust in the deceptive message and ultimately disclosing the victim's confidential data to the attacker.

Vulnerabilities

The human factor represents a vulnerability to phishing attacks due to the susceptibility of individuals to social engineering tactics. Meanwhile, the SMTP protocol's lack of robust authentication and encryption mechanisms exposes email communications to spoofing and interception, facilitating the delivery of phishing emails. It is essential to address both the human and technical aspects of these vulnerabilities to effectively mitigate the risks posed by phishing attacks. This includes implementing security awareness training for users to recognize phishing attempts and implementing secure email protocols and authentication mechanisms to protect against email spoofing and interception.

Techniques

In this context, we have categorized five types of phishing distribution methods that facilitate the propagation of phishing attacks: email, online social networks (OSNs), short message service (SMS), instant messenger (IM), and blogs.

4.1. *Email*

Crafting a deceptive email message with the intent of coaxing users into revealing their credentials is a common phishing technique. According to a PhishMe report, a staggering 91% of cyber-attacks originate from fraudulent emails. The primary reasons individuals fall victim to these emails include curiosity (13.7%), fear (13.4%), and urgency (13.2%), followed by award incentives, entertainment, and opportunity. Avanan's phishing report reveals that 1 in every 99 emails is a phishing attempt using fake links or malicious attachments. The report also highlights that 83% of individuals worldwide have received phishing emails, leading to disruptions such as reduced productivity (67%), loss of

proprietary data (54%), and reputation damage (50%). The FBI reports a loss of $1.2 billion in 2018 due to Business Email Account Compromise (BEC) in the USA.

4.2. *Online Social Networks (OSNs)*

Users often follow people they trust on OSN websites and join interest groups, but OSNs pose significant threats to user privacy by exposing personal information publicly. Attackers may exploit OSN platforms to execute phishing attacks, often by posting malicious links related to sales or offers. Research by Kaspersky Lab indicates that 22% of phishing frauds on the Internet target Facebook users. Additionally, Dimensional Research found that 39% of users believe OSNs are the primary source of social engineering attacks.

4.3. *Short Message Services (SMS)*

In SMS phishing, also known as Smishing, users receive SMS messages containing links to malicious webpages or fraudulent mobile applications. Studies show that SMS has an open rate of 98%, significantly higher than the 28–33% open rate for emails. Furthermore, the response rate for SMS is 39% higher than that for emails.

4.4. *Instant Messenger (IM)*

Similar to fake emails, fraudulent instant messages, such as those on WhatsApp and Facebook Messenger, may include phishing webpage URLs or attachments. These attachments often infect IM software or install malicious software on the user's system. Attackers may also attempt to gather credentials by posing as trustworthy individuals.

4.5. *Blogs and Forums*

Phishers may manually post messages on web forums containing fake links or thread content. Attackers may share links to fake web pages on popular blogs or forums visited by numerous users daily. These links may be disguised as award-winning notifications, fake registrations, fake online sales, software updates, and more.

Countermeasures

Implementing Multi-Factor Authentication (MFA) stands as a robust defense against phishing attacks. MFA requires users to provide multiple forms of verification, typically something they know (like a password) and something they have (such as a code sent to their mobile device). This additional layer of security significantly reduces the risk of unauthorized access, even if a phishing attack successfully steals the user's password. By requiring multiple factors for authentication, MFA helps mitigate the effectiveness of phishing attempts, as attackers would need more than just the user's password to gain access to their accounts.

Artificial neural networks and Bayesian filters leverage probabilistic methods to effectively differentiate between spam and legitimate emails. By training these algorithms on large datasets of labeled email samples, they can learn to accurately identify spam emails based on the underlying patterns and characteristics present in the data. This allows for robust and adaptive spam filtering systems that can continuously evolve to combat new and emerging spamming techniques.

SQL Injection Attacks

Introduction

SQL Injection attacks pose a significant threat to the security of web applications and databases. As one of the most prevalent forms of cyber-attacks, SQL Injection exploits vulnerabilities in the code to manipulate a database, potentially leading to unauthorized access, data breaches, and even the compromise of an entire system.

Vulnerabilities

Insufficient Input Validation

Web applications often accept user input for queries without adequate validation. If this input is not properly sanitized, attackers can inject malicious SQL code, taking advantage of the system's vulnerability.

Poorly Configured Permissions

In some cases, databases are configured with overly permissive user permissions, allowing attackers to execute unauthorized commands and access sensitive information.

Outdated Software

Failure to keep software, including database management systems and web applications, updated with the latest security patches can create vulnerabilities that attackers exploit through SQL Injection.

Techniques

Classic SQL injection

Attackers insert malicious SQL statements into input fields, manipulating the original query to gain unauthorized access or retrieve sensitive data.

Union-based SQL Injection

By leveraging the UNION SQL operator, attackers can combine the results of the original query with their own crafted query, potentially revealing sensitive information from other database tables.

Blind SQL Injection

In situations where the application does not display database errors, attackers use Boolean-based or time-based techniques to infer information about the database structure and contents without direct feedback.

Time-Based Blind SQL Injection

Attackers exploit delays in the application's response to infer whether specific conditions are true or false, gradually extracting information about the database.

Countermeasures

Input Validation and Parameterized Queries

Developers must validate and sanitize all user input to prevent malicious SQL code injection. Parameterized queries, using prepared statements and stored procedures, can effectively separate user input from SQL code, reducing the risk of injection.

Least Privilege PrincipleImplement the principle of least privilege, ensuring that database users have only the minimum required permissions. This limits the potential damage an attacker can cause even if they successfully inject malicious SQL code.

Regular Software Updates

Keeping all software components, including databases and web applications, up to date with the latest security patches is crucial to closing potential vulnerabilities exploited by attackers.

Web Application Firewalls (WAFs)

Employing WAFs can add an additional layer of defense by monitoring and filtering HTTP traffic between a web application and the Internet. WAFs can detect and block SQL Injection attempts, mitigating the risk of successful attacks.

Advanced Persistent Threats (APTs)

Introduction

Advanced Persistent Threats (APTs) have emerged as a formidable and sophisticated method of cyber attacks. Unlike conventional cyber threats, APTs are characterized by their prolonged, targeted, and covert nature. These attacks are meticulously planned, leveraging advanced techniques to infiltrate systems, compromise sensitive data, and maintain a persistent presence within a network.

Vulnerabilities

Human Element

APTs often exploit the weakest link in any security system—the human factor. Social engineering techniques, such as phishing emails, are commonly used to deceive individuals into divulging sensitive information or executing malicious actions.

Outdated Software and Systems

Legacy software and systems with outdated security patches provide fertile ground for APTs. Attackers exploit known vulnerabilities in these systems to gain unauthorized access and establish a persistent foothold.

Inadequate Security Protocols

Weak or inadequate security protocols, including poor access controls, weak passwords, and insufficient network segmentation, create entry points for APTs. Attackers capitalize on these weaknesses to move laterally within a network.

Supply Chain Weaknesses

APT actors may infiltrate an organization's supply chain, targeting third-party vendors or service providers. This approach allows attackers to compromise systems indirectly, often bypassing the primary target's defenses.

Techniques

Spear Phishing

APTs often commence with targeted spear-phishing campaigns. These campaigns involve crafting personalized and convincing messages to trick specific individuals into disclosing sensitive information or downloading malicious attachments.

Zero-Day Exploits

APTs leverage zero-day vulnerabilities, exploiting flaws in software or hardware that are unknown to the vendor. This provides attackers with an advantage, as security teams are unaware of the vulnerability until an attack occurs.

Fileless Malware

APTs often employ fileless malware that resides in system memory, making detection challenging. This technique allows attackers to operate stealthily, avoiding traditional antivirus solutions that rely on file scanning.

Watering Hole Attacks

APT actors compromise websites frequented by their targets, injecting malicious code into these sites. When the targeted individuals visit the compromised site, their systems become infected, allowing attackers to establish a presence within the network.

Countermeasures

User Education and Awareness

Organizations should prioritize educating employees about the risks associated with APTs, emphasizing the importance of recognizing and reporting suspicious activities, especially in emails and other communication channels.

Implementing Robust Access Controls

Organizations should enforce strong access controls, including multi-factor authentication and the principle of least privilege. Limiting user access reduces the attack surface and impedes lateral movement.

Continuous Monitoring and Threat Detection

Deploying advanced threat detection solutions and continuously monitoring network traffic can help identify APTs early in their lifecycle. Behavioral analysis and anomaly detection play a critical role in spotting unusual activities.

Incident Response Planning

Developing and regularly testing an incident response plan enables organizations to respond swiftly and effectively when an APT is detected. This includes isolating affected systems, conducting forensic analysis, and implementing remediation measures.

Regular Software Updates

Keeping software and systems up to date with the latest security patches is crucial. Regular updates help mitigate the risk of APTs exploiting known vulnerabilities in outdated software.

Zero-Day Exploits

Introduction

Zero-day exploits represent a unique class of cyber threats. These exploits target undisclosed vulnerabilities in software, hardware, or firmware, catching organizations off guard and leaving them vulnerable to sophisticated attacks.

Vulnerabilities

Zero-day exploits leverage vulnerabilities in software or hardware that are unknown to the developers or vendors. These vulnerabilities often result from coding errors, design flaws, or unforeseen interactions within a system. Cybercriminals and state-sponsored actors actively seek these undisclosed weaknesses to gain unauthorized access, exfiltrate sensitive information, or execute malicious activities without fear of immediate detection.

Techniques

Malware Injection

Zero-day exploits commonly involve the injection of malware into targeted systems. Malicious code can be introduced through infected files, email attachments, or compromised websites, exploiting vulnerabilities to establish a foothold within the system.

Drive-by Downloads

Attackers may exploit zero-day vulnerabilities through drive-by downloads, wherein users unknowingly download malicious content while visiting compromised websites. These downloads often occur without user interaction, making them particularly challenging to detect.

Phishing and Social Engineering

Zero-day exploits may be incorporated into phishing campaigns, where attackers manipulate users into revealing sensitive information or executing actions that facilitate the exploit. Social engineering techniques play a pivotal role in deceiving individuals and organizations.

Watering Hole Attacks

Cybercriminals may compromise websites frequented by their target audience, turning them into "watering holes." By exploiting zero-day vulnerabilities, attackers can infect visitors' systems, targeting a specific user demographic or industry.

Countermeasures

Patch management

Regularly updating and patching software and critical systems is a good practice to defend against zero-day exploits. Developers and vendors must promptly release patches addressing newly discovered vulnerabilities, and organizations should prioritize timely application of these updates.

Network Segmentation

Employing network segmentation can contain the impact of a zero-day exploit by isolating compromised segments from the rest of the network. This strategy limits lateral movement and prevents widespread damage.

User Education and Awareness

Educating users about phishing tactics, social engineering, and safe online practices is vital in preventing zero-day exploits. Empowering individuals to recognize and report suspicious activities adds an additional layer of defense.

Behavioral Analytics

Implementing behavioral analytics and anomaly detection tools can enhance the ability to identify suspicious activities indicative of a zero-day exploit. By monitoring user behavior and network traffic, organizations can detect deviations from normal patterns.

DNS tunneling

Introduction

Attackers constantly seek innovative methods to infiltrate networks and exfiltrate sensitive data. One such method gaining prominence is DNS tunneling attacks. DNS (Domain Name System) tunneling provides a covert channel for cybercriminals to bypass traditional security measures, posing a significant threat to organizations and their digital assets.

Vulnerabilities

Inadequate Monitoring

Traditional security solutions may not effectively monitor DNS traffic, allowing malicious activities to go unnoticed.

Encryption

Attackers often encrypt their payloads within DNS requests, making it challenging for conventional security tools to detect and analyze the malicious content.

Diverse Attack Vectors

DNS tunneling can be executed through various attack vectors, including malware, malicious scripts, or compromised applications, increasing the difficulty of detection.

Techniques

Covert Communication

Attackers use DNS queries and responses to encode and transmit data covertly, disguising malicious activities within seemingly legitimate DNS traffic.

Data Exfiltration

Malicious actors exploit DNS tunnels to exfiltrate sensitive information from compromised networks, evading traditional detection mechanisms.

Command and Control (C2) Servers

DNS tunnels serve as communication channels between compromised systems and external C2 servers, allowing attackers to remotely control infected endpoints.

Domain Generation Algorithms (DGAs)

Attackers employ DGAs to dynamically generate domain names, making it challenging for security solutions to block malicious communications based on static domain blacklists.

Countermeasures

Deep Packet Inspection

Employ deep packet inspection to analyze DNS traffic for anomalies, including irregular payload sizes, unusual patterns, or suspicious content.

Behavioral Analysis

Implement behavioral analysis to identify deviations from normal DNS traffic behavior, helping detect and prevent anomalous activities associated with DNS tunneling.

DNS Filtering

Use DNS filtering services and maintain updated blacklists to block known malicious domains and prevent communication with malicious C2 servers.

Regular Monitoring and Auditing

Regularly monitor DNS traffic, conduct audits, and analyze logs to identify unusual patterns or unexpected changes, enabling prompt response to potential threats.

Encryption and Authentication

Implement DNSSEC (DNS Security Extensions) to add an additional layer of security, ensuring the authenticity and integrity of DNS data, and consider encrypting DNS traffic to protect against eavesdropping.

Attacker Category	**Type of Attack**	**Response Tactics**
Novices	Phishing, SQL Injection Attacks, DDoS	User education, email filtering, multi-factor authentication
Cyberpunks	DDoS, Cross-site Scripting (XSS), Phishing	Traffic filtering, DDoS mitigation services,CSP
Insiders	Supply Chain Attacks, Advanced Persistent Threats (APTs)	Employee monitoring, access controls, supplier vetting
Old Guards	Zero-Day Exploits, APTs	Patch management, vulnerability scanning
Professionals	APTs, SQL Injection Attacks, Zero-Day Exploits	Intrusion detection systems, threat intelligence

Hacktivists	SQL Injection Attacks, DDoS, XSS	Web application firewalls, code reviews,CSP
Nation States	APTs, Zero-Day Exploits, Cross-site Scripting (XSS)	Cybersecurity alliances, diplomatic measures
Students	DNS Tunneling, SQL Injection Attacks, cross-site scripting (XSS)	Network monitoring, anomaly detection
Petty Thieves	Phishing, DDoS, SQL Injection Attacks	User education, email filtering, legal action
Digital Pirates	DDoS, Supply Chain Attacks, APTs	Digital rights management, legal action
Crowdsourcers	APTs, DDoS, Cross-site Scripting (XSS)	Cybersecurity awareness, monitoring crowd activities
Crime Facilitators	Supply Chain Attacks, SQL Injection Attacks	Collaborative threat intelligence, legal action

Citations

[1] Despina Polemi, Kitty Kioskli(2020): A Socio-Technical Approach to Cyber Risk Assessment

[2] Nicholas Kolokotronis, Stavros Shiaeles(2021) :Cyber-Security Threats, Actors, and Dynamic Mitigation

[3] Ankit Kumar Jain & B. B. Gupta (2021): A survey of phishing attack techniques, defence mechanisms and open research challenges, Enterprise Information Systems

[4] Zaroo, P., 2002. A survey of DDoS attacks and some DDoS defence mechanisms. Advanced Information Assurance

[5] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defence mechanisms: classification and state-of-the-art. Computer Networks

[6] Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications

[7] Sadeghian, A., Zamani, M., & Abdullah, S. M. (2013). A Taxonomy of SQL Injection Attacks. 2013 International Conference on Informatics and Creative Multimedia.

[8] Mokube, I., & Adams, M. (2007). Honeypots. Proceedings of the 45th Annual Southeast Regional Conference

[9] Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2019). Cross-Site Scripting (XSS) Attacks And Mitigation: A Survey. Computer Networks

[10] Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. IEEE Communications Surveys & Tutorials

[11] Chen, J., & Guo, C. (2006). Online Detection and Prevention of Phishing Attacks. 2006 First International Conference on Communications and Networking in China.

[12] Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. Information Systems Research:

[13] Samuel Chng, Han Yu Lu, Ayush Kumar, David Yau (March 2022): Hacker types, motivations and strategies: A comprehensive framework

[14] B Landreth: Out of the Inner Circle - A Hacker's Guide to Computer Security

[15] Richard Barber (February 2001): Hackers Profiled — Who Are They and What Are Their Motivations?

[16] Marcus K. Rogers(9 November 2005): A two-dimensional circumplex approach to the development of a hacker taxonomy

[17] Marcus K. Rogers (January 2010): The Psyche of Cybercriminals: A Psycho-Social Perspective

[18] Meyers, C A; Powers, S S; Faissol, D M, (2009): Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches

[19] Sara L.N. Hald, Jens M. Pedersen(2012): An updated taxonomy for characterizing hackers according to their threat properties

[20] Charlette Donalds. Kweku-Muata Osei-Bryson: A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction

[21] Ryan Seebruck(2015): A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model

[22] Caroline Moeckel(2019): Examining and Constructing Attacker Categorisations, an Experimental Typology for Digital Banking

[23] Nineta Polemi(2020): Psychosocial Approach to Cyber Threat Intelligence