Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 6, No.1, June : 2025

A COMPREHENSIVE ANALYSIS OF NETWORK SECURITY ATTACKS

T C Swetha Priya, Assistant Professor, Department of Information Technology, Stanley College of Engineering and Technology for Women, Hyderabad, Telangana, India.
Ala Lahari, Student, Department of Information Technology, Stanley College of Engineering and Technology for Women, Hyderabad, Telangana, India.
D Deepika, Student, Department of Information Technology, Stanley College of Engineering and Technology for Women, Hyderabad, Telangana, India.

ABSTRACT:
Software development has reached incredible heights during the evolution of digital platforms, on the spectrum of interconnectivity, thereby accentuating the necessity of network security for people, organizations, and governments. The ongoing cyberattacks are ever increasing in sophistication, exploiting all sorts of vulnerabilities through the infrastructure networks to steal sensitive data, disrupt services, and inflict system or reputation losses. Some of the primary threats to network security are malware, phishing, denial-of-service (DoS) and distributed denial-of-service (DDoS), man-in-the-middle (MitM), ransomware, SQL injection, and zero-day. Extortion, espionage, cyber warfare, and sabotage often color the motives behind these attacks. The attack methodologies include brute forcing, social engineering, botnet-driven disruptions, and advanced persistent threats. Moreover, network weaknesses are further exploited through attacks against network protocols, authentication systems, and user behavior. Emerging threats posed by IoT-based vulnerabilities, cloud security, and supply chain attacks further complicate the security environment. A clear understanding of these techniques and their associated objectives aids the effort to combat these attacks and serve as the natural protection against risks, threat modeling, and enhancing cybersecurity within an ever-interconnected digital environment.
Keywords: Network security, cyber-attacks, phishing, SQL injection, IoT vulnerabilities.

INTRODUCTION:

In the age of digitization, network security becomes an imperative for the protection of sensitive data and for preserving the integrity of communication systems. Organizations and individuals live under constant threat day by day for additional cyberattacks from which confidentiality, integrity, and availability could be breached due to the growing reliance on internet-connected devices. Network security involves various strategies, policies, and technologies meant to prevent unauthorized access, data breach, or even malicious activities involving the network infrastructure against such threats. At the foundation comes user authorization-the combination of usernames and passwords. But look! There are many other layers one must delve into with the mesmerizing evolution in cyber threats-the firewalls, intrusion detection systems (IDS), and many more besides. Firewalls enhance access control policies to deny entry to unauthorized users, allowing them to exploit vulnerabilities within the network, while IDS and antivirus software provide avenues for damage control against malware-viruses, worms, and trojans.

The rapid rise of the internet comes with the ability for much personal, corporate, and governmental information to be easily shared within cross-border networks. Network security thus becomes an urgent necessity. Cybercriminals attack intellectual property, financial transaction information, and government secrets at other levels through denial-of-service (DoS), phishing, or advanced persistent threats. To ensure adequate security for network infrastructure mechanisms, one must continue research into many areas within and outside encryption techniques to advanced mechanisms in detecting threats.This research paper covers network security attacks by looking into their historical development, vulnerabilities in the architecture of the internet, types of cyber threats, and existing security mechanisms. It also looks into the latest advancements in security hardware and software

which in turn give hints to new trends as well as challenges to be faced in the future in the area of network security.

REVIEW OF LITERATURE:

Mohan V. Pawar [a], J. Anuradha [b](2015):

Network security has become all the more important with the rapid expansion of computer networks and internet technologies, especially in mobile ad hoc networks (MANETs), wherein decentralized nodes are more susceptible to attacks. Malicious nodes will selfishly disrupt network performance and maintain their own resources. To counter such threats, researchers address the CIA core security principles and, with the aid of models like security vectors, assess and improve security. Attacks such as black hole, gray hole, wormhole, and denial of service emphasize the importance of suitable and adaptive security policies for MANETs (Pawar & Anuradha, 2015).

Natarajan Meghanathan (2014):

This chapter focuses on two major topics in network security. It examines classical network attacks whereby session hijacks, man-in-the-middle attacks, DNS attacks, and distributed denial of service (DDoS) attacks have been employed for the exploitation of vulnerabilities in computer networks. In so doing, it considers the countermeasures that have emerged over a period of time against such threats, inclusive of technical as well as procedural solutions. The chapter then goes on to elaborate on modern network security controls, typically describing within this section those most adopted protocols and standards such as IPSec, Kerberos, SSH, TLS, VPNs, firewalls, and S/MIME. These mechanisms act as a major front against the threats today on the networks by preventing, detecting, and responding to a security breach, while not forgetting about establishing a trusted path for communications, securing the exchange of data, and controlling access to data (Meghanathan, 2014).

Yuchong Li [a] [b], Qinghui Liu [c] (November 2021):

In today's digital age, cyberspace delivers the infrastructure for economic, commercial, cultural, social, and governmental activities in most sectors of society involving individuals, private enterprises, NGOs, and state institutions, hence being the primary platform. Such purposes bring about increasing reliance on electronic and wireless communication technologies, where an increasing threat of cyber-attacks has become a vital concern of the world. In both private companies and government agencies across the globe, threats are imposed upon them on the basis of financial, political, or military implications. Cyber-attacks take the form of computer viruses or corporate espionage or exploit several other attack vectors with the intent of disrupting systems or stealing valuable information. These attacks may severely jeopardize the financial interests of an organization or torture a nation's national security. In reaction, organizations have adopted countless cybersecurity practices and technologies to protect their data and reduce consequential damages. Cybersecurity measures nowadays are seen to shift focus from damage control to the constant monitoring and expert updating of IT systems to keep ahead of active threats while identifying weak infrastructures and increasing their resilience (Li & Liu, 2021).

Shahrulniza Musa David J. Parish(July 2007):

The job of analyzing huge volumes of communication network security data has a variety of challenges, which at times require an advanced form of auxiliary tools for efficient exploration and interpretation. Research has shown that data visualization is an analysis tool that lends itself to an expedited and intuitive understanding of complex alert information. In response, a prototype software was developed to visualize the network security alerts through an easier interface, based on the documented requirements of network security analysts, as highlighted by the literature. This tool offers multiple 3D projections of alert data, with functionalities such as filtering, drill-down, and variable-speed playback. It further utilizes a classification tree algorithm to relay if the alerts are false or true. With real-time visual monitoring, situational awareness is enhanced. Some case studies have shown the positive usefulness of the prototype for effective network security analysis and decision-making

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 6, No.1, June : 2025

ATTACKS IN NETWORK SECURITY :

Malware - Based Attacks:

Malware is an abbreviation of malicious software whose types are designed to prevent, cause damage, or access computer systems without authorization. Some of the most common types of attacks using malware will be discussed below at length.

i.Malware

Malware covers any software that has been deliberately designed to perform malicious acts on a computer system, such as stealing confidential information, disrupting its operations, or gaining illegitimate access. It is an umbrella term, which covers the entire range of categories of different malicious programs, such as viruses, worms, trojan horses, ransomware, spyware, and others. The main aim or objective of malware is to take advantage of the vulnerabilities in the system and use them in favor of the attacker [1].

ii.Virus

A computer virus is the type of malware that advertently associates with genuine programs or files so that it can clone itself and expand to other apartments when acting on the infected program. As with the common types of viruses, they produce highly damaging actions like data corruption, disruption of services, or keystroke logging. They do not reproduce by themselves but need the action of users, which is usually the execution of the host program [2].

iii.Worm

Worms are an example of self-replicating malware that, in the absence of user action, can spread independently over networks. They differ from viruses in that they do not attach to a host program but propagate by exploiting flaws in operating systems or applications. With high possibilities, a worm can bring about serious damage, including consumption of bandwidth, server overload, and ease in delivering other malicious payloads [3].

iv.Botnet

A botnet is the network of compromised computers or zombies/bots that are managed by a remote intruder. Most of the time, the networks are used for coordinated great attacks, for instance, a Distributed Denial of Service (DDoS), spamming or sending spam emails, and mining cryptocurrency illegally. Botnets are highly destructive because they can use so many systems for performing evil activities at the same time [6].

v.Rootkit

The rootkit is a special type of malware, which is designed to achieve unauthorized root or administrative access to the system while hiding itself from view. Rootkits try to achieve this by modifying the operating system or by installing themselves at a low level to hide malicious processes, files, or system data. Most rootkits are difficult to detect and remove, making them effective tools for attackers wanting persistent access to compromised systems [12].

vi. Trojan Horses

Trojan horses, or trojans, represent malicious rogue programs that impersonate some legitimate software intended to trick unsuspecting users into installing them [14]. Once executed, trojans can do all sorts of nasty things, like create back doors for unauthorized access, take data, or download other malware. They do not self-replicate like viruses and worms but infiltrate systems through social engineering [18].

vii. Ransomware

Ransomware infects end-users computer systems and encrypts its files or locks people out from accessing their systems demanding ransom to allow access again [19]. The effect of this type of attack can be very disastrous at the individual as well as organizational level, resulting in the loss of data and

a direct major financial blow. Phishing emails, the downloading of items, or even system vulnerabilities often deliver ransomware [26].

DENIAL-OF-SERVICE(DoS) DISTRIBUTED DENIAL-OF-SERVICE ATTACKS:

The Denial of Service (DoS) attack ultimately results in the system not being accessible to its intended users anymore because it simply opens the doors to superfluous requests pouring in, thus exhausting resources and, eventually, denying service to important conventional users. This could involve service disruption of a serious scale and potential financial loss [12]. In other words, DoS can be carried out by using different techniques like:

i. Vulnerability Attack: where a weakness or flaw present in the software or hardware of the system is taken advantage of [13]. An attacker sends inputs that are malformed or unexpected in order to crash the system or degrade its performance, for instance, a buffer overflow vulnerability may make the system [4].

ii. Bandwidth Flooding: Attackers flood a network with traffic meant for the target domain until bandwidth is consumed completely, never leaving room for even legitimate traffic and thus denying access to the server [3]. Common techniques used for flooding with bandwidth include sending them large volumes of ICMP or UDP packets [12].

iii. Connection Flooding: Attackers, here, create a large number of half-open or fully open TCP connections to the target system that burn away connection table resources of the target system [3]. This can make resources required for handling legitimate connections become inadequately exhausted, hence denying services. A widely known type of connection flooding attack is TCP-syn flooding [12].

DISTRIBUTED DENIAL-OF-SERVICE ATTACK(DDoS):

A Distributed Denial-of-Service (DDoS) attack is a worldwide version of a flooding Denial-of-Service (DoS) attack. A flooding Denial-of-Service attack serves as the best definition of a DDoS attack. In a flooding denial-of-service attack, the attacker needs a higher bandwidth attack to maximize the potential damage [12].

In DDoS attacks, the attacker compromises as many systems as he/she can and uses malicious software called daemons to control these systems [5]. These compromised systems are termed as "bots" and together form a large network known as "botnet". These bots are inactive and will wait until the attacker has identified a viable target [6].

The attacker now uses a command and control (C2) program to issue a command to all the bots that are part of their attack [5]. Directing everybody will command all bots to attack the intended victim through flooding DoS. Dispersed hosts not only magnify the total effect of the attack but also complicate the efforts to trace its source [12].

MAN-IN-THE-MIDDLE ATTACK :

i. Man-in-the-Middle

Man-in-the-Middle attacks take place when a hacker secretly infiltrates and manipulates communication between two parties who believe they are directly connected. The attacker sets up two different encrypted channels - one with each party - allowing them to eavesdrop on communication, modify it, and even inject malicious data into it. Examples of typical MitM attacks are ARP spoofing, DNS spoofing, and SSL stripping. They are typically perpetrated for credential theft, financial fraud, or espionage [2]. To prevent organizations from becoming victims of such attacks, SSL/TLS encryption, certificate validation, and strong authentication mechanisms should be used.

ii. Packet Sniffing

Packet sniffing is passive-type attack in which an attacker watches traffic on a network to capture highly sensitive data like passwords, authentication tokens, and financial details. Packet sniffing becomes highly vulnerable and leads to the stealing of private information by making use of public

exposed Wi-Fi networks since the data has been transmitted without encryption. Cybercriminals break into network packets and extract important information using programs like Wireshark, Tcpdump, and Ettercap [31]. The preventive measures against packet sniffing include enforcing end-to-end encryption (SSL/TLS, VPNs), WPA3 secured Wi-Fi, and disallowing unnecessary packet broadcasting. If an attacker takes an active role in manipulating the network traffic, for example, by using ARP spoofing methods to intercept packets between two devices, then an attack is classified as a MitM or a Man in the Middle attack [2].

iii. Session Hijacking

Session Hijacking occurs when an attacker assumes the control of a session of an authorized user by capturing or guessing the session identifier. An attacker who has obtained a session token can impersonate the user and perform unauthorized actions. Common techniques used for web session hijacking are Session Sidejacking, Session Fixation, and Cross-Site Scripting (XSS) [15]. This type of attack proves to be successful mostly on the websites, where session tokens are sent in clear text or stored insecurely. In order to prevent Session Hijacking, HTTPS should be enforced for secure communication, HTTP-only cookies should be utilized in the organization, session expiration mechanisms should be enabled, and Multi-Factor Authentication (MFA) should be implemented. It is **MitM** if the attacker intercepts session cookies in transit using sniffing techniques [2].

SPOOFING ATTACKS:

i.IP Spoofing

IP Spoofing is a method that fakes the source IP address in the packets which makes the attacker impersonates a trusted device. This method is generally used in Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, which can flood a target system with a barrage of malicious traffic coming from hundreds or thousands of spoofed IP addresses [2]. Some attackers also rely on IP spoofing techniques to bypass security controls and gain unauthorized access to networks. An example of a well-known attack of IP spoofing is a Smurf Attack, where an attacker sends several ICMP requests with a forged source address, causing the victim's system to be drenched in excessive responses. Packet filtering, ingress and egress filtering, and IPSEC-based authentication could be the immediate prevention measures against this threat.

ii. DNS Spoofing

DNS Spoofing or DNS Cache Poisoning is an attack in which the attacker inserts false DNS records into the cache of a server so that this user is really directed to malicious rather than genuine websites. DNS spoofing usually excels in phishing schemes, free data distribution through malware, and espionage [2]. Some attack methods include fast flux, Man-in-the-Middle DNS attacks, and cache poisoning. Effective countermeasures include DNSSEC (Domain Name System Security Extensions), secure recursive DNS resolvers, and regular cache flushing.

AUTHENTICIATION ATTACKS:

i. Exhaustive Brute-Force Attacks

An exhaustive brute-force attack is the advanced method to crack the password where every possible formation of the password is attempted until the right combination is reached. In this case, success is guaranteed but can take an appalling length of time. By way of illustration, an eight-character password, having 95 characters, yields a possible 7 quadrillion combinations. Assuming that an individual can make 10,000 guesses in one second, it would take approximately 22,875 years to crack that password. In the case of 1,000 servers working on this, it will still take way above 22 years.

The exponential nature of password complexity makes length of paramount importance in any security system. A four-character password possesses around 81 million combinations, which can be cracked within under two hours at that rate. However, extending the length to eight characters pushes the time into an entirely impractical range [31].

In contrast, for optimization, hackers implement tools like John the Ripper, which first takes on blunt force to the passwords by trying the dictionary attacks: attacking the common words and phrases, then giving up on them and trying real brute force techniques and this tool is one of the people in cyber-security testing.

ii. Password Attacks :

Password attacks encompass different types of approaches used to obtain or decode user passwords for unauthorized use and access to the specified systems and data. Examples of such attacks include brute-force and dictionary attacks where individual attempts are made at every possible combination and circumstantial use of a compiled list of potential passwords respectively. The efficiency of these forms of attack relies heavily on the targeted password's complexity and strength. Weakly or commonly used passwords are particularly open to attack underscoring the need for a robust password policy and the implementation of multi-factors for authentication mechanisms [31].

CRYPTOGRAPHIC ATTACKS:

i. Key Compromise Attack

A compromised key attack is one in which the attacker forcefully attempts to get access to the cryptographic key in order to decrypt sensitive information, develop digital signatures, or impersonate a legitimate entity. Such attacks can take place, for example, due to lack in key management of keys, malfunctions in the key generation algorithms, or even through physical theft of the key. The possible damage that can occur by the compromised key is broad; it ranges from unauthorized data access to financial fraud and a fall in public confidence on secure channels of communication. One of the methods for reducing these risks is preparing and putting in place robust key management protocols, updating and changing keys regularly, and securing the keys in hardware security modules [32].

ii. Birthday Attack

It is a probability theory application that allows an in-depth study into hash collisions using less brute destruction, especially in the birthday phenomenon. The vastness of the paradox, as applied to two individuals in a crowd of 23, shows that they both have a 50% likelihood of sharing a birth date. In other words, in hashing terms, if the function outputs a certain (fixed) number of possibilities, then an attacker can, with approximately 50% chances, find two different inputs that produce the same hash (collision) after around 2^(n/2) trials, n being the bit length of the hash output [32]. The threat identification is specific to digital signatures and certificates since this yield abnormal forgery due to hash collisions. Ways of mitigating against birthday attacks include; usage of hash functions with sufficiently large output sizes to maintain the compute effort against finding collisions infeasible for an attacker.

The methods used by cybercriminals to manipulate users into providing confidential information or doing activities that compromise security are grouped into such attacks as phishing and social engineering. These attacks apply human psychology or social manipulation rather than technological vulnerabilities, which makes them so very devious. Below follows an overview of various kinds of such attacks with the support of findings from research articles [32].

PHISHING ATTACK :

i. Phishing

Normally, phishing consists of attackers impersonating bank officials or other trustworthy entities in order to deceive victims into divulging sensitive information such as usernames, passwords, or credit card numbers. It is usually carried out through emails, messages, or spoofed websites designed to very closely resemble legitimate ones. Oftentimes, the success of the phishing attack depends upon the urgency or trust generated by the attackers in motivating the victims to act without careful

consideration [32]. According to research, phishing continues to be a threat because it is one of the least expensive yet most effective means of attack.

ii. Whale-Phishing Attacks

Whaling attacks are directed against high-profile individuals within an organization When dealing with CEOs, CFOs, or other executives, these attacks are highly personalized, and they involve extensive research that allows for the creation of convincing messages aimed at making the correspondence appear legitimate and pertinent to the victim's professional role. The objective is to trick the executive into approving a financial transaction or divulging sensitive information or access to secure systems. Given the potential for immensely high rewards, whaling attacks are very carefully planned and executed. Studies carry evidence that the personalized nature of whaling nevertheless makes it a serious threat, as traditional security mechanisms may not detect those attacks easily [32].

iii. The Crime of Spear-Phishing

Spear-phishing is a targeted form of phishing that focuses on a designated individual or a specified organization. Unlike generic phishing attempts, spear-phishing attempts involve personalized messages that are often based on information gathered from social-network profiles, professional-network sites, or previous communication. This personalization increases the chance of the victim's trust in the message, with possible compliance with the requests of the attackers. Typically used for several purposes, including infiltrating an organization network, stealing intellectual property, or conducting financial fraud, studies have highlighted that due to its tailored approach, spear-phishing has a better success rate than widely used phishing campaigns [32].

SOCIAL ENGINEERING ATTACK:

Social engineering refers to phishing social engineering encompasses the many manipulative techniques designed to exploit human cognitive biases and behaviors so as to gain unauthorized access to systems or information [2]. Phishing is one of the most prevalent forms of social engineering, but others include pretexting (creating a fabricated scenario to steal information) baiting (offering an enticing reward for lure up victims), and tailgating (where an unauthorized person follows an authorized person) [4]. These attacks capitalize on the human factors of trust, fear, greed, or desire to help, thereby rendering non-technical defenses ineffective on their own [1]. Therefore, research points out that unless the psychological underpinnings of social engineering are understood, the design and implementation of countermeasures-as security training and awareness-will suffer [5].

WEB ATTACKS AND APPLICATION-LEVEL ATTACKS:

i.SQL Injection

SQL Injection (SQLi) entails an abuse of input fields when an attacker inputs strings of SQL queries from outside considering it part of a database end-user query and may result in unauthorized data access, manipulation, or even deletion [3]. It can be used in the login page, search bars, as well as API requests [9]. There are types of attacks through which one can perform SQL injection: union based, error based, and hard-to-get blind SQL injections. To avoid being prone to such injections, prepared statements should be used, validation of inputs, as well as restricting database permissions [6].

ii.URL Interpretation

URL Interpretation Attacks are attacks based on fraudulent manipulation of a URL to gain access to a resource, redirect a user, or exploit directory traversal vulnerabilities. URL parameters can be manipulated, open redirects can be exploited by attackers, or access to restricted files can also be gained through path traversal techniques. Mitigation steps for developers include validating and cleansing inputs to URLs, implementing access controls, and URL encoding to avoid unauthorized access [7].

iii. Cross-Site Scripting (XSS) Attacks

Cross-Site Scripting, or XSS for short, is an attack against the web application, wherein malicious script is injected into the web application, and it gets executed by the user's browsers, which then could use the script to steal cookies, deface the web sites, or redirect the users [2]. There are three types of XSS: stored XSS, reflected XSS, and DOM-based XSS, the last being executed through the manipulation of the webpage's DOM. Some possible defense strategies include input sanitization, implementation of Content Security Policy (CSP), and cookie protection through the use of HTTP-only and Secure flags [8].

APPLICATION-LEVEL ATTACKS:

i.Web Attacks

Web Attacks include brute force attacks, session hijacking, CSRF (Cross Site Request Forgery), or directory traversal as threats to web applications [6]. These threats target the weaknesses authentication, weaknesses in session management, and insecure web components. In Security, one needs to deploy authentication methods and apply rate limiting to reduce reliance upon and security threats to session handling methods.

ii. Code Execution

Code Execution Attack is a situation in which an attacker exploits vulnerabilities in web applications to run arbitrary code on a target system. The most common of these include Remote Code Execution (RCE), command injection, and insecure deserialization [9]. These attacks are capable of bringing the system to its knees by compromising the entire system. Preventive measures have strict input validation, enforce the principle of least privilege, and apply security patches regularly [12].

UNAUTHORIZED ACCESS ATTACK :

Unauthorized access is when individuals have entered systems, networks, or data with no authority whatsoever. This can happen due to exploitation of some existing system vulnerabilities, misconfigurations, or poor authentication mechanisms [7]. A recent study further emphasizes the miss-configured systems and unpatched software vulnerabilities as the most prominent points of unauthorized access and insists that strong security measures be put in place to avoid any such breach [5].

INSIDER ATTACK :

Insider threats are threats by individual employees who usually harm the organization by engaging in most of the harmful activities they are initiated with a means of accessing the organization's systems and data. These types of threats can also potentially destroy a lot, e.g., intellectual property theft, sabotage, and exposure of sensitive information [2]. A systematic literature review on insider threats categorizes types of insiders, levels of access to infrastructures, motivations that lead to a particular attack, and methods that the attackers would use to carry out the attack. The research notes the inherent challenges in detecting insider threats and why there is a need for more advanced detection and prevention strategies [10].

iii. Mitigation Strategies

Comprehensive security measures must be initiated to combat the unauthorized access and learning of an insider.

a. Robust Access Control Mechanisms: Implementing Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to ensure that only authorized individuals have access to sensitive data.

b. Regular System Audits and Monitoring: Continually monitoring and auditing the systems to identify and respond to unauthorized activities.

c. Employee Training and Awareness: Educating employees about security policies, what threats may occur, and appropriate personal precautions to avoid the risk of inadvertent insider threats.

d. Advanced Threat Detection Systems: Using machine-learning tools and behavior analysis to detect unusual activities that an insider would indicate.
By implementing these strategies, organizations have an arsenal of weapons to fight against unauthorized and insider threats and therefore ensure the safety of their assets and important information [11].

ADVANCED PERSISTENT THREATS (APT) AND LATERAL MOVEMENTS:
Advanced persistent threats are sustained and targeted cyber-attacks where the intruder would gain access to a network and remain undetected for months or years; such activities are highly organized, intending to perpetrate intelligence property theft, activity monitoring, or operational disruption [13]. A generalized assessment of research on APT attribution insists on the complexities associated with the accomplishment of pinpointing the perpetrators behind such attacks; thus, the need for improved detection and attribution methodologies.

LATERAL MOVEMENT:
Lateral movements employ techniques via which attackers traverse through a network after an initial compromise to escalate privileges and access sensitive assets; in doing so, they often use a process called "pivoting," changing the use of the compromised system as a foothold to explore and exploit other systems within the network [15]. A systematic survey of lateral movement detection establishes the difficulty to distinguish malicious activities from legitimate administrative actions, thus calling for the intervention of more advanced intrusion detection systems to check typical patterns of such movements [14].
ROUTING ATTACKS
Routing attacks are very well planned and organized attacks by a set of hackers often into or disrupts the smooth functioning of routing protocols. As a result, the routing messages leave such packets lost denied services or simply are found directed to wrong places [16].
i. **Black Hole Attack:**
In a black hole attack, a malicious node claims falsely to have the shortest path to the destination in the route discovery phase. Once it becomes part of the route, it takes in all data packets while causing denial of service. This scenario is particularly bad in Mobile Ad Hoc Networks (MANETs) where topology of the network is dynamic and decentralized [17].
ii. Rushing Attack:
The rushing attack is one that strikes during route discovery in networks. The attacker will forward the requests of route packets very quickly such that all legitimate requests drown out. This will enable such a malicious node to become part of many routes and then can injure other routes. Such an attack is very difficult to detect as it just manipulates the routing process without showing obvious symptoms [16].
iii. Byzantine Attack:
Byzantine attacks made nodes compromised behave maliciously or erratically, for example, creating routing loops or forwarding along suboptimal paths, to disrupt services in the network. These attacks turn out to be complicated, as the malignant behavior might be detectable and mitigated because it generates legitimate issues on the network [18].

TRAFFIC MANIPULATION ATTACKS:
i. Replay Attack:
Here, a replay attack would be one where the adversary intercepts valid data transmissions and gets them retransmitted to achieve illicit results. The attackers, by simply replaying legitimate messages, can either breach security and gain access or corrupt the operations of the network. Such an attack exploits [19].

ii. Location Disclosure Attack:
In a location disclosure attack, the adversary will try to learn the physical location of nodes in a network by analyzing routing messages and traffic patterns from which a user could be determined, entailing privacy breach attacks. These are significantly serious attacks in situations where anonymity of nodes is critical in a network [20].

iii. Network Monitoring:
That is what network monitoring means: monitoring a network at intervals in order to discover irregularities, monitor performance, and ensure security. Techniques include pattern analysis of traffic, packet inspection, and network flow monitoring. Well-functioned monitoring could help identify and/or mitigate the various attacks, help manage P2P traffic, and maintain overall health in a network environment [21].

iv. Peer to Peer Traffic:
P2P networks are those regular networks in which nodes share resources from anywhere around them, usually to allow users to share files, stream, or do distributed computing. Although P2P applications give their benefits such as poorly resource distribution or redundancy, P2P applications can also lead to worse situations such as increased bandwidth usage and challenges in traffic management. Identifying and managing P2P traffic becomes the prerequisite of efficiency in a network with a value for security [22].

EXPLOITATION AND VULNERABILITY-BASED ATTACKS

i. Buffer Overflow :
A buffer overflow happens when a program writes too much data into a buffer so that the adjacent memory corrupts. An attacker can employ an exploit to execute arbitrary code or crash the whole system. Despite all possible mitigations against buffer overflows, they remain a major security problem [23].

ii. Drive-by Attacks :
A drive-by download happens when a user unintentionally downloads malicious code by merely visiting a compromised website. After exploiting such a weakness in a web browser or web browser plugin, no additional action is needed by the user except for making a visit. Use of hardening and update of security measures, for example, software updates and using security plugins should ultimately help give protection against this kind of attack. Thus, it becomes important to study these attack types with proper countermeasures that can be used for the mitigation of exploited systems against vulnerability-based attacks [24].

VULNERABILITY-BASED ATTACK :

i.Vulnerability Scanners :
Tools that find security holes in systems, networks, and applications are called vulnerability scanners. It analyzes known vulnerabilities such as buffer overflows by checking software configuration and analyzing source code. By establishing periods of regular utilization for these applications, you can stay ahead of the curve in a proactive security management approach so that potential threats can be remedied before they are exploited [25].

EAVESDROPPING ATTACKS :

i. Eavesdropping Attacks :
Unauthorized entry into private and personal communications makes eavesdropping attacks a really serious threat to information across multiple networks.

Forms of Eavesdropping Attacks :
a. Passive Eavesdropping: It's when one person listens in but doesn't alter the conversation. The result is that it's very difficult to prove the act.

b. Active Eavesdropping: These are devious types of attacks, where an individual alters information within the whole stream of communication and may lead to attacks or breaches of data.

Eavesdropping in Wireless Networks :

Because of these features, a wireless network is most susceptible to eavesdropping. The researchers mentioned, eavesdroppers can have a field day depending on several parameters like node density and channel conditions, the likelihood of intercepting the communication can be improved. Model had been proposed to assess the eavesdropper's category, so as to improve the design of secured wireless communication protocols [27].

ADVANCED EAVESDROPPING TECHNIQUES:

Accelerometer-Based Sound Eavesdropping: Using this technique, attackers can re-create sounds heard on the loudspeaker of the device by analyzing corresponding low-frequency accelerometer signal patterns, even though they don't have access to the microphone. The achieved model employs conditional Generative Adversarial Networks (cGANs) to sharpen the quality of the reconstruction and highlight potential weaknesses in how sensor data is handled by devices [29]. Model Inversion Eavesdropping in Semantic Communication Systems: In contrast, the interception of signals and inversion of model data could lead to recovery of the original messages by attackers [31]. This technique represents a major breach in personal integrity, and it promises to become serious as semantic communication systems become increasingly established [32].

DETECTION AND MITIGATION STRATEGIES:

Some of the strategies suggested to combat eavesdropping attacks are the following:

Physical Layer Security Measures: Such measures would include using machine learning algorithms such as Support Vector Machines (SVMs) to detect active eavesdropping at the physical layer in the form of anomaly detection. This method mainly analyzes some features of the signal instead of the behavioral patterns between the transmission and reception links. Privacy-Preserving State Estimation: For example, in a networked system, the provisions for data perturbation and schedule transmission can be used against eavesdroppers to infer secret information in system data. These kinds of methods target certain information obfuscation and make things more complex for attackers to derive anything of value. Knowing and understanding the different types of eavesdropping and having efficient detection and prevention strategies are vital measures that will help in securing sensitive communications over a wide variety of networks [32].

COMPARISON OF NETWORK SECURITY ATTACKS:

S. No.	Attack Name	Introduction	Application/Target	Challenges	Mitigation Techniques
1	**Malware**	.Software's with malicious intent that can damage an infrastructural system or steal data.	Computers, networks, mobile devices.	Detection and elimination become difficult.	Use antivirus, keep systems updated, avoid suspicious files.

2	**Virus**	A class of malware that attaches to files and spreads once the infected files are opened.	Personal and corporate computers.	User action is needed to propagate, but can lead to data corruption.	Install antivirus, avoid downloading unknown files.
3	**Worm**	. A self-replicating type of malware that spreads without user interaction.	Networked systems, IoT devices.	Consumes bandwidth, can damage a lot very fast.	Use firewalls, patch vulnerabilities, monitor network traffic.
4	**Botnet**	A collection of manipulated devices manipulated remotely.	Used for DDoS attacks, spamming, and cybercrime.	Very stealthy as to detection as it works quietly.	Implement intrusion detection, use strong authentication.
5	**Rootkit**	You get so deep in the system that you gain permanent access.	Servers, corporate networks.	Quite difficult to detect and remove.	Use rootkit scanners, enable secure boot.
6	**Trojan Horse**	.It's like normal software; however, it has malicious codes behind it.	Individual users, businesses.	Can establish hidden entries, can steal data	Avoid downloading from untrusted sources, use security software.
7	**Ransom ware**	An application that coaxes the user to pay ransom to decode files.	Critical business data, hospitals, institutions.	Loss of data, extorts money.	Regular backups, avoid clicking on unknown links.
8	**DoS Attack**	.Excessively using a system to cause denial of service to legitimate users.	Websites, servers, networks.	Breaks service and causes financial loss.	Use rate limiting, DDoS protection tools.
9	**DDoS Attack**	Multiple systems used, for amplification of a DoS attack.	Large-scale websites, online services.	Havoc difficulty because of volume.	Cloud-based mitigation, traffic filtering.

10	**Man-in-the-Middle**	The attacker intercept communication between two parties.	Online transactions, VoIP calls.	Eavesdropping and data manipulation.	Use end-to-end encryption, secure connections (HTTPS).
11	**IP Spoofing**	The attacker forged an IP address for imitational purposes as to really have a trusted device.	Network communicatio ns, firewalls.	Causes DoS/DDoS.	Packet filtering, network authentication.
12	**DNS Spoofing**	Changes the DNS responses to steer users towards malicious websites	Web browsing, email services.	Turns into phishing and malware infections.	Use DNSSEC, verify website URLs.
13	**Packet Sniffing**	Hoards the traffic from networks to steal sensitive data.	Public Wi-Fi, corporate networks.	Can compromise personal and financial data.	Use VPN, encrypt network traffic.
14	**Session Hijackin g**	Appropriates a session from a legitimate user.	Web applications, banking systems.	Identity theft, data breaches.	Use HTTPS, session timeouts, multi-factor authentication.
16	**Whale-Phishing**	Targets high-profile individuals like executives.	Corporate email, financial data.	Can lead to major data breaches.	Cybersecurity awareness, verification of communications.
15	**Phishing**	Fraudulent emails or websites trick users into revealing credentials.	Email services, social media.	Hard to detect, exploits human psychology.	Spam filters, user education, two-factor authentication.
16	**Whale-Phishing**	Targets high-profile individuals who are like executives.	Corporate email, financial data.	This can lead to significant data breaches.	Cybersecurity awareness, verification of communications.

17	**Spear-Phishing**	A certifiable individual can be targeted in a spear-phishing maneuver.	Corporate executives, government officials.	Very targeted attacks.	Verify sender identity, educate users.
18	**SQL Injection**	Hacks into databases using malicious SQL queries and manipulates them.	Web applications, login systems.	Can get sensitive user data.	Use parameterized queries, input validation.
19	**Cross-Site Scripting (XSS)**	Injects malicious scripts into websites.	User-generated content websites, forums.	Can steal cookies, impersonate users.	Use content security policies, sanitize inputs.
20	**Web Attacks**	Exploits the vulnerabilities of web applications.	Online portals, e-commerce sites.	Data leaks, service interruption.	Regular security testing, secure coding practices.
21	**Brute Force Attack**	He tries the guess of one password combination after another and stops once a success has been achieved.	Login systems, encrypted data.	Incredibly time-consuming, but will do the job in the case of weak passwords.	Use strong passwords, limit login attempts.
22	**Password Attacks**	Numerous methods exist to steal or crack passwords.	Online accounts, corporate systems.	Weak passwords make it that much easier for the attacker.	Enforce password complexity, two-factor authentication.
23	**Compromised-Key Attack**	Cryptographic keys have been stolen and then used to gain access into the system.	Encrypted communication, SSL/TLS.	This can lead to large-scale data breaches.	Use key rotation, secure key storage.
24	**Birthday Attack**	Makes cracks in the cryptographic security by exploiting hash function collisions.	Digital signatures, cryptographic applications.	Reduces the amount of work for an attack.	Use strong cryptographic algorithms.

25	**Insider Threats**	Using internal attack employees and/or contractors.	Corporate networks, data centers.	Very hard to detect because they have legitimate access.	Monitor user behavior, restrict access.
26	**Advanced Persistent Threat (APT)**	Discovery of long-term cyber espionage by state-sponsored or organized groups.	Government, large enterprises.	Highly sophisticated, difficult to prevent.	Network segmentation, continuous monitoring.
27	**Black Hole Attack**	It simply discards network traffic to blackout communications.	Wireless and mobile networks.	Causes network outages, data loss.	Use secure routing protocols, monitor network anomalies.
28	**Buffer Overflow**	Exploits memory vulnerabilities to execute malicious code.	Applications, operating systems.	System crashes, unauthorized access may result.	Bounds checking, secure coding.
29	**Vulnerability Scanners**	Cries for automated tools to scan for security weaknesses.	Web applications, servers.	Could be used by attackers and defenders alike.	Regular security audits, patch management.
30	**Eavesdropping Attacks**	Intercepting data when it's being transmitted.	Wireless networks, VoIP calls.	Sensitive communication has been compromised.	Encrypt communications, use secure protocols.

CONCLUSION :

Network security threats impact individuals, corporations, and governments alike because they thrive on exploiting the weaknesses present within digital infrastructures. These threats continue to increase in complexity-from malware-inflicted intrusions to denial-of-service disruptions to very detailed phishing techniques. Attackers use exploits such as SQL injection, session hijacking, and DNS spoofing to gain unauthorized access, steal data, or disturb normal functioning. As cyber threats advance, organizations must take a multilayer approach to security. This involves strong authentication protocols, timely security updates, intrusion detection systems, and employee awareness. Encryption and secure network configuration also help minimize risks. Efforts in cybersecurity must maintain the focus on new threats and appropriate countermeasures, thereby producing a field-ready defense mechanism against dynamic attacks. Individuals and organizations may prevent most below-surface cyberattacks and protect sensitive data through proactive measures combined with sophisticated security procedures.

REFERENCES :

[1]. Pawar, Mohan V., and J. Anuradha. "Network security and types of attacks in network." ***Procedia Computer Science*** **48 (2015).**

[2]. **Meghanathan, Natarajan. "Network security: Attacks and controls."** ***Network Security Technologies: Design and Applications*****. IGI Global, 2014.**
[3]. **Yuchong Li, Qinghui Liu. "Cybersecurity and Digital Transformation: An Evolving Relationship."** ***Journal of Information Security and Applications*****, Volume 59, November 2021, 102842.**
[4]. **Shahrulniza Musa, David J. Parish. "Visualization of network security data: A case study."** ***Computers & Security*****, Volume 26, Issue 5, July 2007, Pages 351-359.**
[5]. **Wang, X., & Yu, H. (2005). A generalized birthday attack.** ***Lecture Notes in Computer Science*****, 3494.**
[6]. **Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms.** ***ACM SIGCOMM Computer Communication Review*****, 34(2).**
[7]. **Kumar, R., & Tripathi, R. (2021). Distributed Denial-of-Service (DDoS) attacks and defense mechanisms in different web-enabled computing platforms: Challenges, issues, and future directions of research.** ***Frontiers in Computer Science*****.**
[8]. **Alshamrani, A., & Alwan, M. (2020). Phishing attacks in social engineering: A review.** ***International Journal of Computer Applications*****.**
[9]. **Stuttard, D., & Pinto, M. (2011).** ***The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*****. Wiley.**
[10]. **Kirda, E., Kruegel, C., Vigna, G., & Jovanovic, N. (2006). Static detection of cross-site scripting vulnerabilities. In** ***Proceedings of the 2006 IEEE International Conference on Software Engineering*****.**
[11]. **Halfond, W. G. J., Viegas, J., & Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. In** ***Proceedings of the IEEE International Symposium on Secure Software Engineering*****.**
[12]. **Cowan, C., Wagle, P., Pu, C., Beattie, S., & Walpole, J. (2000). Buffer overflows: Attacks and defenses for the vulnerability of the decade. In** ***Proceedings of the DARPA Information Survivability Conference and Exposition*****. IEEE.**
[13]. **Argentieri, G. (2023). Forensic analysis of peer-to-peer network traffic using Wireshark.** ***Sule Lamido University Journal of Science and Technology*****.**
[14]. **Mills, G. A., Pomary, P., Togo, E., & Sowah, R. A. (2022). Artificial neural network-based detection and management of P2P traffic in networks.** ***Journal of Network and Systems Management.***
[15]. **Agrawal, S. (2015). Approach for detecting black hole attack in MANETs.** ***International Journal of Computer Applications*****.**
[16]. **Almomani, A., & Gupta, B. B. (2016). A survey of phishing email filtering techniques.** ***IEEE Communications Surveys & Tutorials*****.**
[17]. **Armin, J., Thompson, B., & Creese, S. (2015). Countering cyber threats: Context-based security.** ***IEEE Security & Privacy*****.**
[18]. **Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems, and tools.** ***IEEE Communications Surveys & Tutorials*****.**
[19]. **Böhme, R., & Moore, T. (2012). The economics of information security.** ***Science*****.**
[20]. **Choi, H., Lee, H., & Kim, H. (2012). Botnet detection by monitoring group activities in DNS traffic.** ***Computer & Security*****.**
[21]. **Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.** ***Future Generation Computer Systems*****.**
[22]. **Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications.** ***IEEE Symposium on Security and Privacy*****.**
[23]. **Gope, P., & Hwang, T. (2016). BSN-Care: A secure IoT-based modern healthcare system using body sensor network.** ***IEEE Sensors Journal*****.**

[24]. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2020). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*.

[25]. He, W., & Da Xu, L. (2015). A state-of-the-art survey of cloud manufacturing. *International Journal of Computer Integrated Manufacturing*.

[26]. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*.

[27]. Li, J., Li, X., Chen, X., Lee, P. P., & Lou, W. (2015). A hybrid cloud approach for secure authorized deduplication. *IEEE Transactions on Parallel and Distributed Systems*.

[28]. Mohurle, S., & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*.

[29]. Osborn, S. L., Sandhu, R., & Munawer, Q. (2000). Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System*.

[30]. Reddy, K. S., & Reddy, R. R. (2017). A comprehensive study of cybercrime in India. *International Journal of Advanced Research in Computer Engineering & Technology*.

[31]. Sabillon, R., Cavaller, V., Cano, J., & Serra, M. (2016). Cyber security governance: A component of all the aspects of cybersecurity. *Journal of Information Security*.

[32]. **Zimba, A., & Wang, Y. (2019). Cybercrime: A threat to cyber security. *International Journal of Computer Applications*.**