Research Report on Common Network Security Threats

Author – Akanksha Mane

Date – 22nd November 2025

Abstract

This report presents a detailed and structured examination of major network security threats, focusing on prevalent attack vectors such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Man-in-the-Middle (MITM) attacks, and various spoofing-based techniques. Each threat is analysed in terms of how it operates, the vulnerabilities it targets, and the mechanisms attackers use to exploit network weaknesses. The report also explores the broader impacts of these threats from technical disruptions such as network outages and data interception to significant business consequences including financial loss, service downtime, and reputational harm.

Real-world examples and notable case studies are incorporated to highlight the practical relevance of each threat and illustrate how inadequate defenses have led to major incidents across industries. In addition, the document outlines proven mitigation strategies that organizations can adopt, ranging from robust encryption practices and traffic filtering to proper authentication mechanisms and proactive monitoring.

To address the evolving nature of the threat landscape, the report discusses current trends such as the rise of botnet-driven attacks, automation in cyber exploitation, and the growing complexity of hybrid network environments. It concludes by presenting a structured defensive model based on the People–Process–Technology (PPT) framework, offering organizations a balanced and holistic approach to enhancing their network security posture. Designed for both technical professionals and general readers, this research report aims to provide clarity, academic rigor, and practical insight into defending modern networks against emerging threats.

Table of Content

INTRODUCTION

As organizations continue to digitize their operations and depend heavily on interconnected networks, safeguarding network infrastructures has become a critical priority. Modern businesses rely on seamless communication between systems, users, and devices, making networks the backbone of almost every operational process. However, this heavy reliance also exposes organizations to a wide range of security threats that target weaknesses in communication channels, network protocols, endpoint devices, and even user behavior.

Network security threats have evolved in both scale and sophistication. Attackers now employ automated tools, botnets, and advanced techniques to exploit vulnerabilities, intercept sensitive information, or disrupt services. Consequences can include unauthorized access, large-scale data breaches, prolonged downtime, reputational damage, and significant financial losses. Even a single overlooked vulnerability in a network can create opportunities for adversaries to infiltrate critical systems or manipulate data.

This report provides a comprehensive overview of the most prevalent network security threats encountered today, explaining how they operate, the vectors they use, and the harm they inflict on organizations. Additionally, it examines real-world incidents to illustrate the practical impact of these attacks and discusses effective, industry-approved mitigation strategies. By understanding these threats in depth, organizations can enhance their defenses, reduce risk exposure, and build a more resilient network security posture suitable for today's evolving digital environment.

COMMON NETWORK SECURITY THREATS

2.1. DENIAL-OF-SERVICE (DOS/DDOS) ATTACKS

What it is:

A Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack is a deliberate attempt to make a network service, application, or system unavailable to legitimate users by overwhelming it with excessive traffic or resource-intensive requests. While a DoS attack is launched from a single machine, a DDoS attack leverages hundreds or thousands of compromised devices often part of a botnet to amplify the impact.

How it works:

1. Target Selection:
   The attacker chooses a vulnerable system such as a web server, application endpoint, or network component that supports critical services.
2. Traffic Generation:
   In a DoS attack, the attacker directly sends a rapid stream of packets or requests from one machine.
   In a DDoS attack, the attacker first compromises multiple devices (e.g., IoT devices, personal computers) and forms a botnet. These devices are then remotely controlled to send massive amounts of traffic simultaneously.
3. Resource Exhaustion:
   The targeted system becomes overloaded as its CPU, memory, bandwidth, or connection limits are consumed. This prevents it from processing legitimate requests.
4. Service Disruption:
   As system resources deplete, the service becomes slow, unresponsive, or fully unavailable, leading to operational downtime.

Impact:

DoS/DDoS attacks can severely affect organizations by:

- Rendering critical services inaccessible to users
- Causing operational downtime and disrupted business processes
- Generating significant financial losses, especially for online platforms
- Damaging an organization's reputation due to loss of customer trust
- Forcing costly recovery efforts and infrastructure upgrades

Real world example:

One of the most notable incidents occurred in 2016, when the DNS provider Dyn was hit by a massive DDoS attack executed through the Mirai botnet, which consisted largely of compromised

IoT devices. The attack disrupted major online services including Twitter, Netflix, Reddit, Spotify, and GitHub, affecting millions of users globally.

Mitigation:

Organizations employ several measures to reduce the risk and impact of DoS/DDoS attacks:

- Rate Limiting: Restricts the number of requests a user or IP address can send.
- DDoS Protection Services: Cloud-based tools like Cloudflare, AWS Shield, and Akamai can detect and absorb attack traffic.
- Firewalls and Intrusion Prevention Systems: Block suspicious or malformed packets before they reach internal systems.
- Traffic Filtering and Anomaly Detection: Identifies unusual spikes in traffic and automatically reroutes or drops malicious flows.
- Redundancy and Load Balancing: Distribute traffic across multiple servers to avoid single points of failure.

2.2. MAN-IN-THE-MIDDLE ATTACKS

What it is:

A Man-in-the-Middle (MITM) attack occurs when an attacker secretly intercepts, monitors, or alters communication between two parties without their knowledge. The attacker positions themselves between the sender and receiver, gaining access to sensitive information or manipulating data while maintaining the appearance of a legitimate connection.

How it works:

1. Interception of Traffic:
   The attacker intercepts communication channels, often exploiting insecure networks such as public Wi-Fi, unencrypted HTTP connections, or compromised routers.
2. Data Capture or Modification:
   Once the traffic is intercepted, the attacker can monitor sensitive information such as login credentials, credit card numbers, or personal data or modify messages before forwarding them to the intended recipient.
3. Impersonation:
   Advanced MITM attacks involve impersonating one or both parties to extract confidential information or trick users into executing malicious actions, such as transferring funds or installing malware.

Impact:

MITM attacks can have serious consequences for both individuals and organizations, including:

- Theft of sensitive data such as passwords, financial information, or personal records
- Session hijacking, allowing attackers to access accounts and resources without authorization
- Financial fraud and unauthorized transactions
- Loss of trust and reputational damage for organizations hosting compromised systems

Real world example:

A common scenario occurs on public Wi-Fi networks, where attackers set up rogue hotspots or exploit unsecured networks to eavesdrop on user communications. Users connecting to these networks can have their login credentials, emails, and other sensitive data captured without their knowledge.

Mitigation:

- Encryption (TLS/SSL): Ensures that data transmitted between client and server is encrypted and cannot be read or modified in transit.

- Virtual Private Networks (VPNs): Protect communication by tunneling traffic securely, even over untrusted networks.
- Secure Wi-Fi Configurations: Avoid using open networks; implement WPA3 encryption and strong authentication on private networks.
- Multi-Factor Authentication (MFA): Reduces the impact of stolen credentials by requiring additional verification steps.
- Certificate Pinning and HTTPS: Prevents attackers from impersonating legitimate websites using forged certificates.

2.3. SPOOFING ATTACKS

What it is:

Spoofing attacks occur when an attacker masquerades as a legitimate device, user, or system in order to deceive network devices, applications, or end users. Common forms include IP spoofing, DNS spoofing, email spoofing, and ARP spoofing, each targeting different communication layers to gain unauthorized access, intercept data, or redirect traffic.

How it works:

1. Crafting a Fake Identity**:**
   The attacker forges identifiers such as IP addresses, domain names, MAC addresses, or email headers to make malicious communications appear legitimate.
2. Exploiting Trust Mechanisms:
   Once the fake identity is accepted by the network or users, the attacker can bypass security controls, redirect traffic, or manipulate data in transit. For example, DNS spoofing can redirect users to malicious websites, while email spoofing can deliver phishing messages that appear to come from trusted sources.
3. Execution of Malicious Actions:
   The attacker may gain unauthorized access to systems, capture sensitive information, inject malware, or perform further attacks like session hijacking and credential theft.

Impact:

- Unauthorized access to restricted systems or sensitive data
- Redirection of users to malicious websites, enabling phishing and malware deployment
- Interception and theft of confidential communications and credentials
- Compromised trust in organizational communications, leading to reputational damage

Real world example:

In 2013, the Target Corporation data breach partially involved email spoofing as part of the initial attack vector. Attackers sent phishing emails to employees of a third-party vendor, which appeared to come from legitimate sources. This allowed the attackers to gain access to Target's network indirectly. Once inside, they leveraged spoofed credentials and access privileges to exfiltrate sensitive customer payment information, affecting over 40 million credit and debit card accounts.
Similarly, DNS spoofing attacks have been widely reported in the past decade, where attackers redirected users trying to access legitimate banking or e-commerce websites to fake versions designed to steal login credentials and financial data.

Mitigation:

To defend against spoofing attacks, organizations should implement multiple layers of protection:

- Strong Authentication Mechanisms: Use multi-factor authentication (MFA) and robust credential verification to ensure only legitimate users gain access.
- DNS Security Extensions (DNSSEC): Validates DNS responses to prevent redirection to malicious domains.
- Digital Signatures and Certificates: Ensure the authenticity and integrity of emails, software, and communications.
- Network Access Controls: Implement packet filtering, ARP inspection, and IP address verification to detect and block forged network traffic.
- User Awareness and Training: Educate users to recognize suspicious emails, websites, and network behaviors.

2.4. PHISHING & SOCIAL ENGINEERING

What it is:

Phishing and social engineering attacks involve deceptive communication strategies designed to manipulate individuals into divulging sensitive information or performing actions that compromise security. Unlike purely technical attacks, these exploits rely on human psychology, trust, and behavior to bypass security mechanisms. Common forms include email phishing, SMS phishing (smishing), voice phishing (vishing), and other targeted social engineering campaigns.

How it works:

1. Crafting Malicious Communication:
   Attackers create emails, messages, or calls that appear legitimate, often mimicking trusted organizations, colleagues, or service providers. The messages may contain urgent requests, threats, or enticing offers to provoke an immediate response.
2. Luring the Victim:
   Victims are tricked into clicking links, downloading attachments, or entering login credentials into counterfeit websites. Sophisticated attacks may use personalized information to increase credibility (spear-phishing).
3. Exploitation:
   Once the victim interacts with the phishing attempt, attackers may:
   - Steal credentials for corporate accounts, banking, or email
   - Install malware, spyware, or ransomware on the victim's device
   - Gain unauthorized access to sensitive networks and systems

Impact:

Phishing and social engineering attacks can cause extensive damage, including:

- Credential theft leading to account compromise
- Unauthorized access to confidential organizational data
- Financial loss through fraudulent transactions
- Propagation of malware, ransomware, or further attacks within a network
- Erosion of trust and reputational harm for both individuals and organizations

Real world example:

In 2017, the Google Docs phishing campaign targeted Gmail users worldwide. Attackers sent seemingly legitimate Google Docs invitations that, when clicked, requested access to users' Google accounts. Thousands of users unknowingly granted access, allowing attackers to steal personal

information and propagate the attack through contact lists, demonstrating how quickly social engineering can scale.

Mitigation:

Organizations can significantly reduce the risk of phishing and social engineering through a combination of technical and human-centered strategies:

- Awareness Training: Educate employees to recognize suspicious emails, links, attachments, and requests.
- Email Filtering and Anti-Phishing Tools: Implement spam filters, domain verification, and advanced threat detection solutions.
- Multi-Factor Authentication (MFA): Even if credentials are compromised, MFA adds an additional layer of protection.
- Regular Simulated Phishing Exercises: Reinforce training by testing users' ability to detect phishing attempts.
- Incident Response Procedures: Establish clear reporting channels for suspected phishing or social engineering attempts.

2.5. RANSOMWARE

What it is:

Ransomware is a type of malicious software designed to deny users access to critical data, applications, or entire systems by encrypting files or locking devices. The attacker then demands a ransom typically in cryptocurrency in exchange for providing the decryption key. Ransomware attacks can target individuals, small businesses, or large organizations, often causing significant operational and financial disruption.

How it works:

1. Infection Vector:
   Ransomware often infiltrates systems via phishing emails, malicious attachments, drive-by downloads from compromised websites, or through exploitation of unpatched vulnerabilities in software and network services.
2. Encryption of Data:
   Once executed, the malware scans the system for files, encrypts them using strong cryptographic algorithms, and prevents the user from accessing them. Some ransomware variants can also spread laterally across a network, infecting shared drives and connected systems.
3. Ransom Demand:
   After encryption, a ransom note is displayed, instructing victims on how to pay the attacker usually in Bitcoin or other cryptocurrencies to obtain the decryption key. Attackers may also threaten data leaks if payment is not made, adding pressure for victims to comply.

Impact:

Ransomware attacks can have severe consequences for organizations and individuals:

- Permanent data loss if backups are unavailable or compromised
- Operational downtime affecting productivity, revenue, and service delivery
- Financial loss through ransom payments, system restoration, and legal penalties
- Reputational damage and loss of customer trust
- Potential secondary attacks, such as data exfiltration or regulatory fines for breaches

Real world example:

The WannaCry attack in 2017 was one of the most widespread ransomware outbreaks in history. Exploiting the SMB vulnerability MS17-010 in Windows systems, WannaCry infected hundreds of thousands of devices across over 150 countries. Organizations including the UK National Health Service (NHS), FedEx, and Telefónica experienced significant service disruptions and financial losses. Despite Microsoft releasing a patch before the attack, many systems remained unpatched, highlighting the critical importance of timely updates in ransomware prevention.

Mitigation:

To defend against ransomware, organizations should adopt a layered approach:

- Regular Backups: Maintain offline and redundant backups to ensure recovery without paying ransom.
- Endpoint Security: Use antivirus, anti-malware, and behavior-based detection solutions to block and quarantine ransomware.
- Timely Patching: Regularly update operating systems, applications, and network devices to close exploitable vulnerabilities.
- Network Segmentation: Limit lateral movement by isolating critical systems and sensitive data.
- User Awareness: Train employees to recognize phishing emails, suspicious links, and unsafe downloads.
- Incident Response Plans: Establish clear procedures for containing infections, restoring systems, and reporting incidents to authorities.

2.6. ARP POISONING

What it is:

ARP Poisoning, also known as ARP Spoofing, is a network-based attack in which an adversary manipulates the Address Resolution Protocol (ARP) tables of devices on a local network. By corrupting these tables, the attacker tricks systems into associating the attacker's MAC address with the IP address of another legitimate device. This allows the adversary to intercept, monitor, or modify network traffic flowing between connected hosts.

How it works:

1. Sending Forged ARP Replies:
   The attacker broadcasts fake ARP reply packets across the network, claiming that their own MAC address corresponds to the IP address of a legitimate device such as a router or another host. Since ARP is inherently trust-based and lacks authentication, devices typically accept and store this false information without verification.
2. Poisoned ARP Cache:
   The victim device updates its ARP cache with the attacker's spoofed information. As a result, any data intended for the legitimate device is mistakenly sent to the attacker's machine.
3. Traffic Interception or Redirection:
   Once positioned in the communication path, the attacker can:
   - Passively eavesdrop on sensitive data
   - Modify packets before forwarding them
   - Inject malicious payloads
   - Launch Man-in-the-Middle (MITM) attacks
   - Disrupt communication entirely by dropping packets

Impact:

ARP Poisoning can cause significant security and operational issues within a local network, including:

- Unauthorized interception of sensitive information such as login credentials, financial data, or session cookies
- Full-scale MITM attacks enabling manipulation of traffic
- Impersonation of devices or services
- Loss of data integrity and confidentiality
- Facilitation of additional attacks such as session hijacking or DNS spoofing

Real world example:

Although ARP Poisoning typically occurs inside local networks and is less publicized than large-scale cyberattacks, it is frequently observed in environments like public Wi-Fi networks, corporate LANs, and educational institutions. For instance, attackers on unsecured public hotspots have successfully used ARP spoofing tools such as Ettercap or Cain & Abel to capture credentials from unsuspecting users, demonstrating how easily local traffic can be compromised without proper network protections.

Mitigation:

Organizations can reduce the risk of ARP Poisoning through a combination of technical controls and network security configurations:

- Static ARP Entries: Assign fixed ARP mappings for critical systems such as gateways and servers to prevent unauthorized changes.
- Dynamic ARP Inspection (DAI): Enable DAI on switches to verify ARP packets against trusted sources before forwarding them.
- Port Security: Restrict MAC address changes and limit the number of devices that can connect to a switch port.
- VLAN Segmentation: Separate critical systems and sensitive departments into distinct VLANs to minimize exposure.
- Encryption: Use HTTPS, TLS, VPNs, and other encryption mechanisms to protect data, even if intercepted.
- Monitoring Tools: Deploy intrusion detection systems (IDS) to identify unusual ARP traffic patterns or anomalies.

CROSS CUTTING IMPACTS & TRENDS

The landscape of network security threats is constantly evolving, shaped by technological advancements, attacker sophistication, and expanding organizational infrastructures. Several overarching trends influence how network attacks are executed, detected, and mitigated**.**

A. Increased Automation in Attacks:
Modern attackers increasingly rely on automated tools and exploit kits to identify and compromise vulnerable systems at scale. Automated scanning allows adversaries to probe thousands of targets simultaneously, significantly reducing the time between vulnerability disclosure and exploitation. Botnets, AI-driven attack frameworks, and self-propagating malware enable attacks to operate continuously and autonomously, increasing both the speed and breadth of compromise.

B. Rise of Targeted Multi-Vector Attacks:
Threat actors are moving beyond single-point attacks, leveraging multiple vectors simultaneously to maximize impact. For example, a cybercriminal might combine phishing emails, DDoS disruption, and malware injection into a coordinated attack on a target organization. These multi-vector campaigns increase the likelihood of success, bypass traditional security controls, and often require more sophisticated detection and response strategies.

C. Growing Exploitation of Cloud and IoT:
As organizations increasingly adopt cloud services and deploy Internet of Things (IoT) devices, the attack surface expands dramatically. Cloud misconfigurations, weak authentication, and insecure APIs are increasingly exploited by attackers, while IoT devices often lack strong security controls, leaving them vulnerable to hijacking and lateral network movement. These trends demand adaptive security measures, including continuous monitoring, identity and access management, and automated patching, to protect diverse and distributed infrastructures.

D. Implications:
These trends underscore the need for proactive and holistic defense strategies. Organizations must adopt automated threat detection, maintain strong patch management practices, implement multi-layered security controls, and continuously update risk assessments to keep pace with evolving attack methods. Failure to adapt can result in faster, more sophisticated compromises that are harder to detect and remediate.

GENERAL MITIGATION FRAMEWORK (PEOPLE – PROCESS – TECHNOLOGY)

A comprehensive approach to network security relies on a balanced integration of people, processes, and technology. Each component plays a critical role in identifying, preventing, and responding to threats effectively.

A. People

Human awareness and competency are essential in mitigating security risks. Employees should be trained to recognize suspicious activity, phishing attempts, and other social engineering tactics. Regular security awareness programs and targeted training sessions help cultivate a security-conscious culture, reducing the likelihood of accidental breaches. Clear role definitions and accountability ensure that responsibilities for monitoring, patching, and incident response are well understood and executed consistently.

B. Process

Structured processes provide the foundation for systematic security management. This includes the development and enforcement of security policies, standard operating procedures (SOPs), and incident response plans. Continuous monitoring, vulnerability assessments, and periodic audits ensure compliance with regulatory frameworks and organizational standards. Well-defined escalation procedures and patch management cycles help maintain operational continuity while minimizing exposure to emerging threats.

C. Technology

Modern tools and technologies serve as the first line of defense against network attacks. Firewalls and intrusion detection/prevention systems (IDS/IPS) help block malicious traffic and detect suspicious activity. Encryption protects data in transit and at rest, while access controls and multi-factor authentication ensure that only authorized users can access sensitive systems. Additionally, endpoint protection, SIEM platforms, and automated threat intelligence integration enhance detection and response capabilities, allowing organizations to respond to threats in real time.

D. Integration of PPT Framework:

When people, processes, and technology work together cohesively, organizations can create a resilient security posture capable of preventing, detecting, and responding to network threats efficiently. For example, trained personnel can leverage monitoring tools effectively, policies ensure proper escalation and reporting, and technology enforces protections and automates defenses, forming a unified, proactive security ecosystem.

RECOMMENDATIONS & BEST PRACTICES CHECKLIST

To defend against the growing spectrum of network security threats, organizations should implement a proactive, multi-layered strategy that combines technology, process, and user awareness. The following recommendations provide a practical framework for enhancing security posture:

A. Regular Patching and Updates:
Timely updates and patching of operating systems, applications, and network devices are critical to close vulnerabilities before attackers exploit them. Organizations should maintain an up-to-date inventory of assets, prioritize patches based on risk and severity, and deploy updates consistently across all endpoints, servers, and network components. Automated patch management tools can streamline this process while minimizing human error.

B. Deploy Intrusion Detection and Prevention Systems (IDS/IPS):
Implementing IDS/IPS solutions helps monitor network traffic for signs of suspicious activity, including known attack patterns and anomalous behavior. These systems can alert security teams in real time or automatically block malicious traffic, providing an essential layer of defense against DoS/DDoS attacks, malware propagation, and unauthorized access attempts.

C. Strong Authentication Policies:
Enforcing robust authentication mechanisms, such as multi-factor authentication (MFA), complex password policies, and role-based access controls (RBAC), reduces the risk of unauthorized access even if credentials are compromised. Regular audits of user accounts and privileges ensure that access rights are aligned with current roles and responsibilities.

D. Continuous Monitoring & Logging:
Real-time monitoring of network traffic, system logs, and security alerts allows organizations to detect threats early, investigate anomalies, and respond quickly to incidents. Centralized logging and Security Information and Event Management (SIEM) platforms provide visibility across complex infrastructures, enabling correlation of events, trend analysis, and faster incident response.

CONCLUSION

Understanding network security threats is critical for organizations to build resilient, reliable, and secure systems. The ever-evolving landscape of cyberattacks including DoS/DDoS, Man-in-the-Middle attacks, spoofing, phishing, ransomware, and ARP poisoning demonstrates that both technical vulnerabilities and human factors must be addressed to prevent compromise.

A proactive approach that integrates preventive controls, continuous monitoring, and structured security frameworks enables organizations to reduce the likelihood and impact of attacks. Preventive measures, such as patch management, strong authentication, encryption, and network segmentation, close exploitable gaps, while monitoring and logging provide real-time visibility into anomalous behavior, enabling rapid detection and response.

Implementing a People–Process–Technology (PPT) framework ensures that security responsibilities are clearly assigned, processes are standardized and auditable, and technology enforces consistent protections across the network. Additionally, ongoing user training, vulnerability assessments, and incident response planning strengthen organizational readiness against both conventional and advanced threats.

In conclusion, a holistic, multi-layered network security strategy not only mitigates immediate risks but also enhances long-term operational resilience. Organizations that combine awareness, policy-driven processes, and advanced security technologies are better equipped to defend against evolving threats, protect sensitive data, and maintain trust with customers, stakeholders, and regulatory authorities.

REFERENCES

- NIST Special Publication 800-61 Rev. 2. (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2
- NIST Special Publication 800-115. (2008). *Technical Guide to Information Security Testing and Assessment*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-115/final
- MITRE ATT&CK® Framework. (2025). *A knowledge base of adversary tactics and techniques*. MITRE Corporation. https://attack.mitre.org/
- OWASP Foundation. (2023). *Top Ten and Network Security Guidance*. Open Web Application Security Project. https://owasp.org/
- ENISA. (2024). *ENISA Threat Landscape — Annual Report*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/
- Verizon. (2024). *Data Breach Investigations Report (DBIR) 2024*. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/
- Cisco Systems, Inc. (2024). *Cisco Annual Cybersecurity Report: Network Threats and DDoS Trends*. Cisco. https://www.cisco.com/c/en/us/products/security/
- Cloudflare, Inc. (2024). *DDoS Threat Reports and Mitigation Guidance*. Cloudflare Blog and Research. https://www.cloudflare.com/learning/ddos/
- Akamai Technologies. (2024). *State of the Internet / Security — DDoS and Web Application Attack Trends*. Akamai. https://www.akamai.com/
- Palo Alto Networks — Unit 42. (2024). *Threat Intelligence Reports on Network Exploits and MITM Techniques*. Unit 42 Research. https://unit42.paloaltonetworks.com/
- SANS Institute. (2023). *Network Security Monitoring, Detection, and Incident Response Guidance*. SANS Reading Room. https://www.sans.org/