www.wordlyknowledge.uz Volume: 3, Issue: 1, 2023

TYPES OF NETWORK ATTACKS

Sugdiyona Ilkhomjon qizi Mamadalieva

Fergana branch of the Tashkent University of Information Technologies, master's student, Fergana region, Buvayda district, Soy-Buyi street 4

ibrohimovasugdiyona98@gmail.com

Nilufar Kakhramonovna Abdulkhamidova

Fergana branch of the Tashkent University of Information Technologies, master's student, Fergana region, Kuvasay, A.Navai st. 128-45

softmint27@gmail.com

Ziyoda Umidjon qizi Toxirjonova

Fergana branch of the Tashkent University of Information Technologies, bachelor's degree Kuvasoi city, A. Kadiri 5-16, Fergana region

ziyodaxontohirjonova@gmail.com

Annotation: Network attacks are attempts to gain unauthorized access to, disrupt, or disable computer networks or systems. Attackers may target networks for a variety of reasons, including stealing data, extorting money, or simply causing damage.
Keywords: Network attack, cyberattacks, HTTP floods, Denial of service (DoS), Phishing, DNS poisoning, Reflection attack, SQL injection, botnet, Cross-site scripting (XSS), vulnerability

Inrtoduction:A network attack is any attempt to gain unauthorized access to, disrupt, or disable a computer network or system. Attackers may target networks for a variety of reasons, including stealing data, extorting money, or simply causing damage.
A denial-of-service (DoS) attack is a type of cyberattack that attempts to make a computer or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. DoS attacks achieve this by overwhelming the target with traffic, or sending it information that triggers a crash. They are one of the most common types of cyberattacks and can be launched by anyone with an internet connection.

Main part

Volume-based attacks: These attacks flood the target with traffic, making it unable to handle legitimate requests. Common examples of volume-based attacks include ICMP floods, SYN floods, and UDP floods.

Application-layer attacks: These attacks exploit vulnerabilities in specific applications or operating systems to cause them to crash or become unresponsive. Common examples of application-layer attacks include HTTP floods and DNS floods. Examples of DoS attacks.

An attacker floods a web server with HTTP requests, making it unable to respond to legitimate requests.

An attacker floods a DNS server with DNS queries, making it unable to resolve domain names.

An attacker sends a large number of ICMP packets to a network, making it unable to handle legitimate traffic.

An attacker exploits a vulnerability in an operating system to cause it to crash.

www.wordlyknowledge.uz Volume: 3, Issue: 1, 2023

Organizations should also have a plan in place for responding to DoS attacks. This plan should include steps for identifying and mitigating attacks, as well as steps for communicating with customers and employees during an attack.
By taking these steps, organizations can help to protect themselves from DoS attacks and minimize the impact of an attack if it does occur. A distributed denial-of-service (DDoS) attack is a type of cyberattack in which the attacker floods a target server or network with traffic from multiple sources, making it unavailable to legitimate users. DDoS attacks can be launched using a variety of methods, including botnets and reflection attacks.

Botnets are networks of compromised computers that can be controlled by the attacker. The attacker can use the botnet to send a large number of requests to the target server or network, overwhelming it and making it unavailable to legitimate users.Reflection attacks exploit vulnerabilities in network protocols to amplify the amount of traffic that is sent to the target. For example, an attacker might send a large number of UDP packets to a DNS server with a forged source IP address of the target server. The DNS server will then respond to the packets, sending the traffic to the target server.

Man-in-the-middle attacks (MitM) is a type of cyberattack in which the attacker intercepts communication between two parties and impersonates one of them. This allows the attacker to steal data or modify communications without the knowledge of either party.

MitM attacks can be launched using a variety of methods, including:
ARP spoofing: ARP spoofing is a technique in which the attacker sends fake ARP messages to the victim's computer. This causes the victim's computer to send traffic to the attacker's computer instead of the intended destination;
DNS poisoning: DNS poisoning is a technique in which the attacker changes the DNS records for a domain name. This causes the victim's computer to resolve the domain name to the attacker's computer instead of the legitimate server;
SSL interception: SSL interception is a technique in which the attacker intercepts SSL traffic between the victim's computer and a website. This allows the attacker to decrypt the traffic and steal sensitive data, such as passwords and credit card numbers.

There are a number of things that organizations can do to protect themselves from DDoS and MitM attacks, including:

Use a firewall and intrusion detection system (IDS): A firewall and IDS can help to block malicious traffic from reaching the target network.

Use a content delivery network (CDN): A CDN can help to distribute traffic across multiple servers, making it more difficult for attackers to overwhelm a single server.
Implement load balancing: Load balancing can help to distribute traffic across multiple servers so that no single server is overloaded.

Use strong encryption: Strong encryption can help to protect data from being stolen even if it is intercepted by an attacker.

Educate employees about cybersecurity best practices: Employees should be educated about how to identify and avoid DDoS and MitM attacks.
Phishing attacks are attempts to trick users into revealing sensitive information, such as passwords or credit card numbers. Phishing attacks are often carried out via email or social media. The attacker may send a fake email that appears to be from a legitimate company, such as a bank or credit card company. The email may ask the user to click on a link or open an attachment. If the user does so, they will be taken to a fake website that looks like the real website of the company. The attacker can then steal the user's sensitive information when they enter it into the fake website.
Malware attacks involve infecting devices with malware, such as viruses, worms, or Trojans. Malware can be used to steal data, damage systems, or disrupt operations. Malware can be

www.wordlyknowledge.uz Volume: 3, Issue: 1, 2023

spread in a variety of ways, such as through email attachments, infected websites, and removable media.

Examples of phishing attacks

Here are some examples of phishing attacks:

An attacker sends an email that appears to be from a bank, asking the user to click on a link to reset their password. The link takes the user to a fake website that looks like the real website of the bank. When the user enters their password into the fake website, the attacker steals it.

An attacker sends an email that appears to be from a social media company, asking the user to click on a link to confirm their account information. The link takes the user to a fake website that looks like the real website of the social media company. When the user enters their account information into the fake website, the attacker steals it.

Examples of malware attacks

Here are some examples of malware attacks:

• A user opens an email attachment that contains a virus. The virus infects the user's computer and steals their personal information.

• A user visits a website that is infected with a worm. The worm infects the user's computer and spreads to other computers on the network.

A user inserts a USB drive into their computer that is infected with a Trojan horse. The Trojan horse gives the attacker control over the user's computer. How to protect against phishing attacks and malware attacks.

There are a number of things that users can do to protect themselves from phishing attacks and malware attacks, including: Be suspicious of unsolicited emails and attachments. Do not click on links or open attachments in emails from unknown senders.

Keep your software up to date. Software updates often include security patches that can help to protect against known vulnerabilities. Use antivirus software. Antivirus software can help to detect and remove malware from your computer.

Be careful about what websites you visit. Avoid visiting websites that are known to be malicious or that have a bad reputation. Be careful about what files you download. Only download files from trusted sources.

By taking these steps, users can help to protect themselves from phishing attacks and malware attacks. A zero-day attack is a type of cyberattack that exploits a vulnerability in software that is not yet known to the software vendor. This makes zero-day attacks very dangerous because there is no patch available to fix the vulnerability. Zero-day attacks are often carried out by state-sponsored actors or sophisticated criminal groups. These attackers have the resources and expertise to develop and launch zero-day attacks.

Examples of zero-day attacks, there are some examples of zero-day attacks:

In 2010, the Stuxnet virus was used to attack Iranian nuclear facilities. Stuxnet exploited a vulnerability in the SCADA software that is used to control industrial processes. In 2013, the Heartbleed bug was discovered. Heartbleed was a vulnerability in the OpenSSL cryptographic library that is used by many websites and other software applications. Heartbleed allowed attackers to steal data from servers that were running OpenSSL. In 2017, the WannaCry ransomware attack affected over 230,000 computers in 150 countries. WannaCry exploited a vulnerability in the Windows operating system. How to protect against zero-day attacks. There is no foolproof way to protect against zero-day attacks. However, there are a number of things that organizations can do to reduce their risk, including:Keep software up to date: Software vendors often release security patches to fix known vulnerabilities. It is important to install these patches as soon as they are available.Use a firewall and intrusion detection system (IDS): A firewall and IDS can help to block malicious traffic from reaching the target network. Implement security

www.wordlyknowledge.uz Volume: 3, Issue: 1, 2023

controls: Security controls, such as access control lists and data encryption, can help to protect data from being accessed or stolen by unauthorized individuals. Educate employees about cybersecurity best practices: Employees should be educated about how to identify and avoid zero-day attacks. By taking these steps, organizations can help to reduce their risk of being affected by a zero-day attack.
Additional safety guidelines, there are some additional safety guidelines that organizations can follow to protect themselves from zero-day attacks:Use sandboxing: Sandboxing can be used to isolate software from the rest of the system. This can help to prevent zero-day attacks from spreading to other parts of the system.Use a web application firewall (WAF): A WAF can help to protect websites from zero-day attacks.Monitor network traffic for suspicious activity: Organizations can monitor network traffic for suspicious activity to identify potential zero-day attacks. In conclusion , imagine a network as a vast prairie, with servers and data centers scattered across it like homesteads. Attackers are like bandits and outlaws, roaming the prairie in search of easy targets. They may use brute force to break into servers, or they may use more sophisticated methods, such as social engineering or zero-day attacks.

Defenders are like sheriffs and marshals, trying to keep the peace and protect the homesteads. They use firewalls, intrusion detection systems, and other security measures to keep attackers at bay. But attackers are always looking for new ways to get around these defenses. The battle between attackers and defenders is never-ending, and it is only getting more intense. As technology evolves, so too do the tools and techniques used by both sides. As a result, network attacks are becoming more sophisticated and more dangerous. According to above paragraphs,in the future, network attacks will become so sophisticated that they will be indistinguishable from natural disasters. Attackers will be able to exploit vulnerabilities in the critical infrastructure that powers our society, such as the power grid and the transportation system. These attacks could cause widespread disruption and chaos.

Referens:

1. Lundberg, S., “VLAN Hopping”, “Advanced LAN Technologie” 1-8., 2014.
2. Abdur Rahman, Md. F., Kamal, P., “Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm”, “International Journal of Advancements in Technology”,Vol. 5, 1-10., 2014.
3. Bruschi, D., Ornaghi, A., Rosti, E. (2013). “S-ARP: A Secure Address Resolution Protocol”, “Italian Dept. of Education and Research F.I.R.S.T. Project”, 1-9.
4. Prasad, B., K., M., Reddy, A., R., M., Venugopal R., K., “DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey”, “Global Journal of Computer Science and Technology: E Network, Web & Security”, Vol. 14, 1-19., 2014.
5. Choudhary, Kavita, Meenaksh, and Shilpa. Smurf Attacks: Attacks Using ICMP (2011): 1-3, 2011.
6. Duany, Z., Yuan, X., Chandrashekar, J., “Controlling IP Spoong Based DDoS Attacks Through Inter-Domain Packet Filters”, “IEEE INFOCOM 2006”, Vol. 5, 1-30, 2006.
7. Mirkovic, J., Jevtic, N., Reiher, P., “A Practical IP Spoofing Defense through Route-Based Fltering”, 1-14, 2005.
8. Geneiatakis, D., Vrakas, N., Lambrinoudakis, C. (2009). “ Utilizing Bloom Filters for Detecting Flooding Attacks against SIP Based Services”, “Computer security”, 1-14.
9. Maj, S. P., Veal, D., Makasiranondh, W. (2010). “Using State Model Diagrams to Manage Secure Layer 2 Switches”, “International Journal of Computer Science and Network Security”, Vol. 10, 1-4.
10. Prasad, B., K., M., Reddy, A., R., M., Venugopal R., K. (2014). “DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey”, “Global Journal of Computer Science and Technology: E Network, Web & Security”, Vol. 14, 1-19.

www.wordlyknowledge.uz Volume: 3, Issue: 1, 2023

11. Karabade, A., Daş, R., "Analysis of the Data Link and Network Layer Attacks and Defence Mechanisms", The Third International Symposium on Digital Forensics and Security (ISDFS 2015), 11-12 May, 2015, Gazi University, Ankara.
12. Gtakhbayar, N., Battulga, D., Sodbileg, Sh. (2012). "Classification of Artificial Intelligence IDS for Smurf Attack", "International Journal of Artificial Intelligence & Applications (IJAIA)", Vol. 3, 1-5.
13. Alomar, E., Gupta, B., B., Ppayah, S., K. (2012). "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", 1-6.
14. Elleithy, K., M.(2011). "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", "Systemics, Cybernetics and Informatics", Vol. 3, 1-6