Florida Institute of Technology

Harris Institute for Assured Information

Project Report

Secure Data Coms & Networks

CYB 5290

Dr. Abdullah Aydeger

BY

Aeshah Zarraa and Kajolben Gajjar

DNS Security Attacks and Defensive Approaches Against Them

Introduction

Security assaults are harmful acts by cybercriminals to exploit vulnerabilities in computer systems, networks, or applications. These vulnerabilities might allow the attackers to take control of the targeted system, network, or application. These assaults can have significant repercussions, such as data theft, financial resources loss, and an organization's reputation tarnishing. The following is a list of frequent forms of security breaches:

Malware Attacks: Malware is software that is designed to cause damage to computer systems. Some examples of malware include viruses, Trojan horses, and spyware. Malware is software that may be used for various nefarious purposes, including the theft of data, the destruction of systems, and the creation of backdoors via which hackers can access confidential information.

Phishing Attacks: Phishing attacks are a type of social engineering assault that includes pretending to be a reliable organization to deceive consumers into giving critical information. Emails, SMS messages, and bogus websites are all common vectors for the transmission of phishing attempts.

Denial of Service: Attacks known as denial of service (DoS) are carried out to flood a network or system with so much traffic that it becomes unreachable to those who are authorized to use it. These assaults can be carried out in a variety of ways, including through the use of botnets.

Man in the Middle: Attacks known as "Man in the Middle" (MitM) entail intercepting and modifying communications that are taking place between two parties to steal information or carry out other harmful operations. Attacks known as man-in-the-middle can be carried out using packet sniffing and ARP spoofing.

Attacks on passwords: A password attack is any effort to obtain unauthorized access to a system or account by guessing the user's password or stealing it. These assaults can be carried out in several ways, including phishing, brute force, and other methods.

SQL Injection Attacks: SQL injection attacks exploit online application weaknesses to obtain unauthorized access to a database. SQL injection attacks are also known as SQL injection attacks. These assaults can be utilized to steal data, change data, or carry out various other criminal activities.

What is CIA

Confidentiality, Integrity, and Availability are the pillars upon which information security is founded, and they are sometimes abbreviated as "CIA" in cybersecurity. These guiding concepts are utilized in formulating efficient security policies and controls, which shield sensitive data and systems against unauthorized access, alteration, and deletion.

Confidentiality: The shielding of sensitive information from exposure or access by unauthorized parties is what is meant by the term "confidentiality." This can be accomplished by implementing access restrictions, encryption, and other security measures.

Integrity: The guarantee that information is correct and has not been altered or tampered with in an unauthorized manner is what the term "integrity" means and relates to the assurance in question. The application of data validation strategies, such as checksums or digital signatures, is one method that may be used to accomplish this goal.

Availability: The capacity to retrieve and use information or resources at the opportune moment is what we mean when discussing availability. This could be accomplished by using

redundancy, backup systems, and contingency planning.
These three tenets, when put together, allow businesses to guarantee the safety of their data and systems against various cyber dangers, such as computer hacking, malware, and other forms of online assaults.

Attacks to Focus on this Research

In this research, we focused on the following attacks:

1. DNS cache Poisoning
2. Distributed Reflection Denial of Service – TCP SYN Flood
3. DNS hijacking
4. Random Subdomain Attack

We research these attacks sequentially and analyze how they are executed and what pillar of the CIA model they hit.

1. DNS cache Poisoning

To understand this attack, it is necessary to understand what DNS (Domain Name Server) is and how it works. The abbreviation "DNS" refers to the Domain Name System, which is a system that converts domain names that are readable by humans, such as "www.example.com," into the numeric Internet Protocol (IP) addresses that computers use to identify one another on the internet, such as "192.0.2.1."
When a user enters a domain name into their web browser, the browser requests a DNS resolver, which then looks for the IP address associated with that domain name in a hierarchical directory system of DNS servers. When the resolver finds it, the browser notifies the user that it has located the IP address. The IP address is then sent back to the user's browser by the DNS resolver after it has been located. The user's browser may then use the IP address to connect with the web server hosting the website that is connected with the domain name.
Without the Domain Name System (DNS), internet users would have to commit the numerical IP addresses of every website they want to access to memory, which would be impractical and time-consuming. DNS is an essential component of the internet's underlying infrastructure.

How DNS Protocol Works

The Domain Name System (DNS) protocol is a decentralized network that operates hierarchically to translate domain names into IP addresses. The following is a condensed explanation of how it operates:
A domain name is entered into the user's web browser by the user.

- A DNS query is sent from the browser to the user's local DNS resolver, which the user's internet service provider almost always provides. (ISP).
- The browser then answers if the local DNS resolver has a cached record of the IP address corresponding to the domain name in question. If this is not the case, a query is sent to one of the root DNS servers.

- Following the completion of the request, the root DNS server will provide a reference to a top-level domain (TLD) DNS server.
- In its response to the request, the TLD server refers to the authoritative DNS server responsible for the domain name being queried.
- The authoritative DNS server answers the request, which provides the corresponding IP address for the domain name.
- The local DNS resolver saves the IP address in the browser's cache, delivering it to the browser. The browser then makes a connection with the web server that is hosting the website.

This procedure can take anywhere from a few milliseconds to several seconds to complete, depending on several factors, including the speed of the user's internet connection, the responsiveness of the DNS servers involved, and the complexity of the domain name that is being requested. DNS also supports various additional features, including caching, load balancing, and security measures such as DNSSEC (DNS Security Extensions), which are all designed to defend against malicious assaults.

DNS Cache Poisoning Attack on DNS Protocol

DNS cache poisoning is a cyber assault known as DNS spoofing or DNS hijacking. In this type of cyber-attack, an attacker manipulates the DNS cache of a DNS server to divert traffic that would typically go to a real domain name to a malicious website. The attacker can achieve this by delivering erroneous DNS information to the resolver. The DNS resolver will then cache the erroneous information and serve it to subsequent users who request the same domain name.

The following is a simplified illustration of how an attack that involves poisoning the DNS cache may work:

- An attacker initiates a DNS query for a valid domain name, such as www.example.com, and transmits it to a DNS resolver.
- An attacker will transmit a spoofed DNS response packet before the DNS resolver can react. This packet will contain bogus information, such as a different IP address linked with www.example.com.
- Any other user who requests www.example.com will be sent to the malicious website operated by the attacker since the DNS resolver will have cached the bogus information and served it to them.

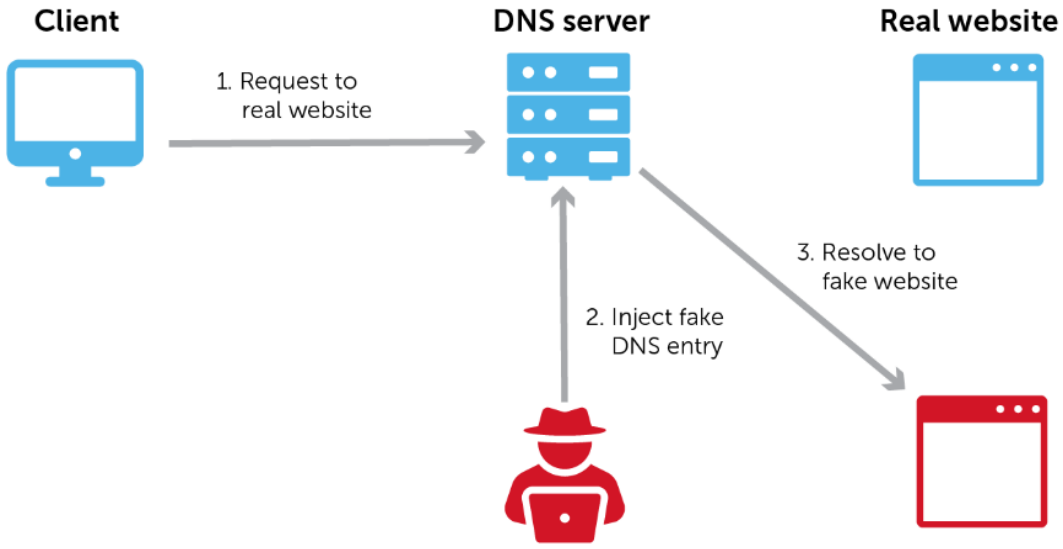

Figure 1: A simple scenario of DNS Cache Poisoning

Ettercap Tool for Cache Poisoning

Ettercap is a popular open-source application for evaluating network security and conducting research. Cache poisoning attacks are one of its many characteristics, and it can also perform many other useful functions.

Ettercap may carry out cache poisoning attacks through the spoofing method known as Address Resolution Protocol (ARP). On a local network, ARP is a protocol utilized to map a physical address, also known as a MAC address, to a logical address, also known as an IP address. Ettercap can manipulate the DNS cache and redirect traffic to a malicious server by spoofing the ARP tables of both the victim and the gateway. This causes the DNS cache to return the IP address of the attacker's server for the requested domain name.

The phishing assault, session hijacking attack, and man-in-the-middle attack are just a few examples of attacks that may be carried out with Ettercap's cache-poisoning capability. However, it is essential to remember that assaults, including poisoning caches, are against the law and can have severe repercussions. Because of this, it should only be utilised for morally justifiable reasons, such as evaluating the safety of one's network or with the express agreement of the network's owner.

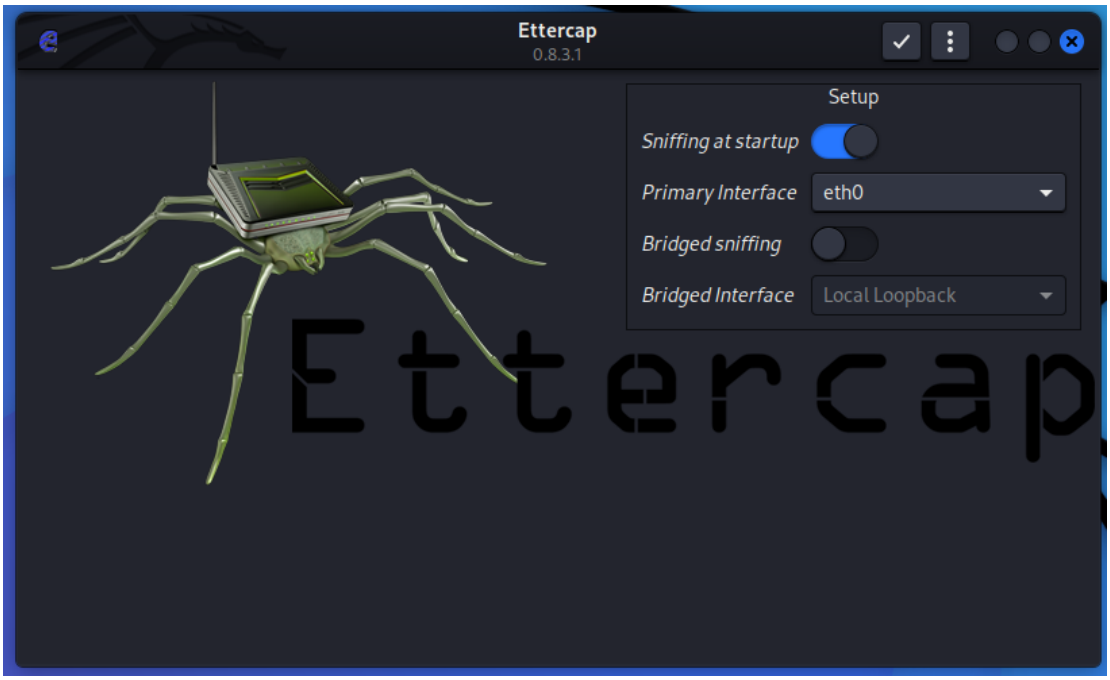

Figure 2: Ettercap Tool for Cache Poisoning

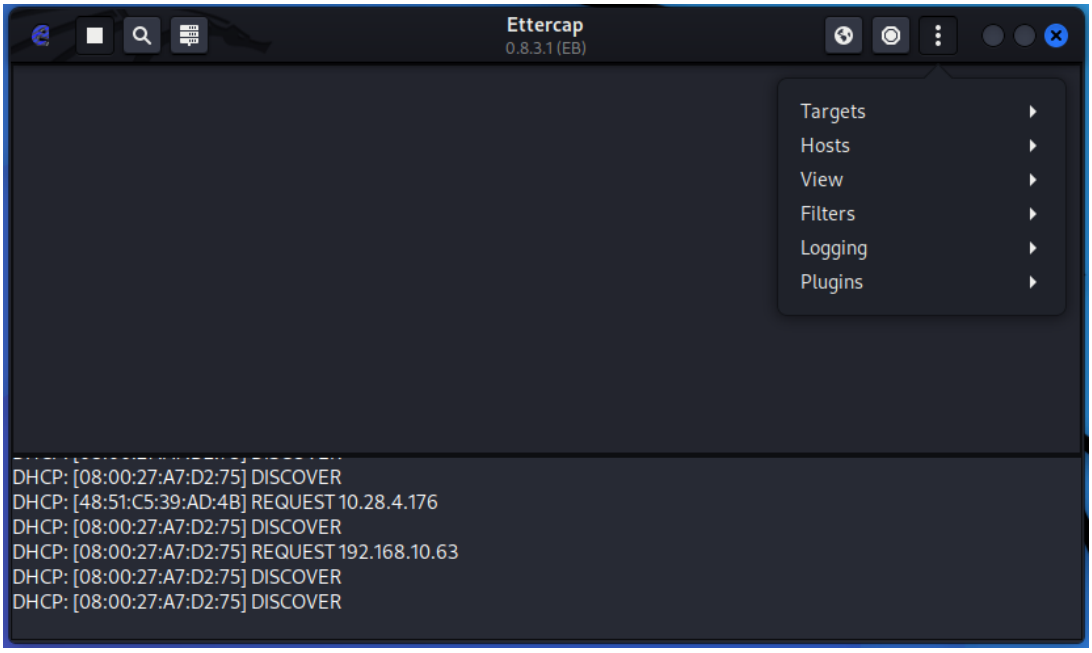

Figure 3: Select Plugins Options from the Option Menu

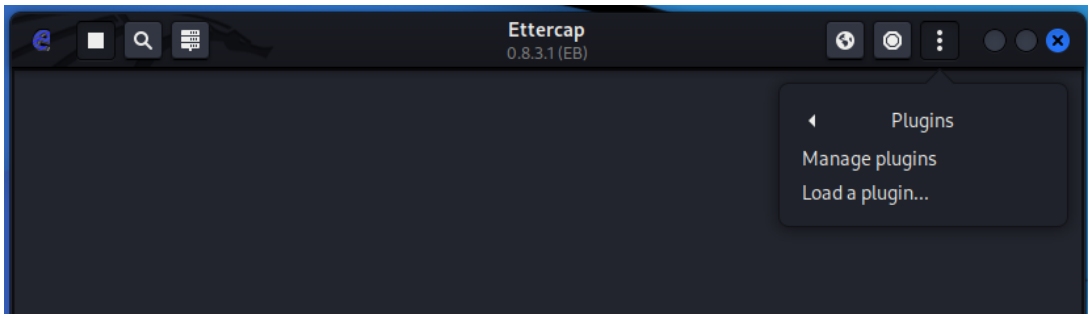

Figure 4: Select the "Load a Plugin" Option

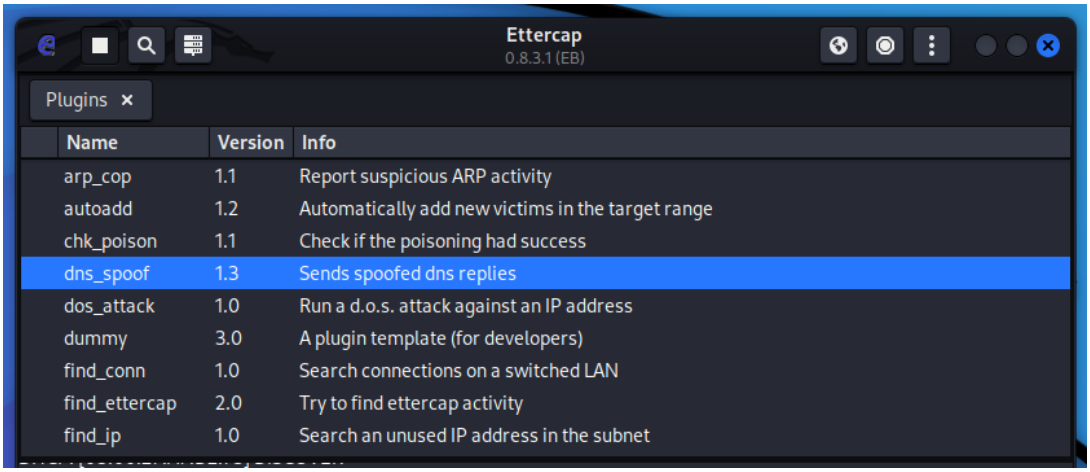

Figure 5: Select the 'dns_spoof' plugin to launch the attack

2. Distributed Reflection Denial of Service – TCP SYN Flood

The term "Distributed Reflection Denial of Service," or "DRDoS," refers to a sort of cyber assault in which an attacker takes use of the capability of reflective services to increase the volume of traffic that is sent towards a target system or network. The attack consists of sending requests to many susceptible servers, which then reply to the target by sending considerably bigger answers back to the target. This overwhelms the target's network infrastructure, ultimately making the network unreachable to legitimate users.

To send requests to reflecting servers during a DRDoS assault, it is common practice to use a botnet, which is a network of computers that have been hacked and are under the attacker's control. DNS servers, NTP servers, SNMP servers, and other similar services might fall under the category of reflecting servers. These servers react to inquiries with far more comprehensive answers than the initial question. The attacker will submit a forged request to the reflective server, making it look like the request originated from the target system. This will cause the server to provide a substantially bigger answer to the target.

TCP SYN Flood

The TCP SYN flood attack is a denial-of-service assault (DoS attack) in which an attacker delivers a flood of TCP SYN packets to a target system, overloading that system's capacity to react to genuine requests for service.

A client establishes a TCP connection by sending an SYN packet to the server; the server then sends an SYN-ACK packet in response. Finally, the client sends an ACK packet to confirm the connection. This procedure is known as the three-way handshake. An attacker launches an SYN flood assault on a target system by sending many SYN packets with a spoofed source IP address. This prompts the target system to send SYN-ACK packets to the spoofed IP address to validate the connection. The target system continues to wait for the last ACK packet to complete the connection since the attacker does not deliver it. However, the target system eventually surpasses its maximum limit for half-open connections, which results in a denial of service.

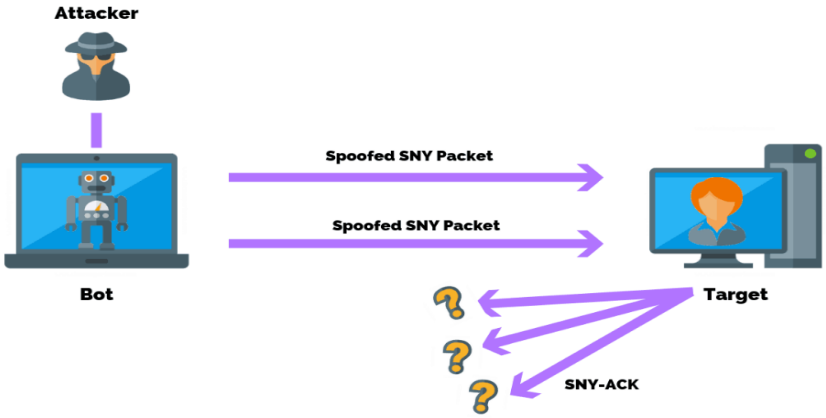

Figure 6: TCP Syn Flood Attack on Target Machine Using a Bot

Tool for SYN Flood Attack

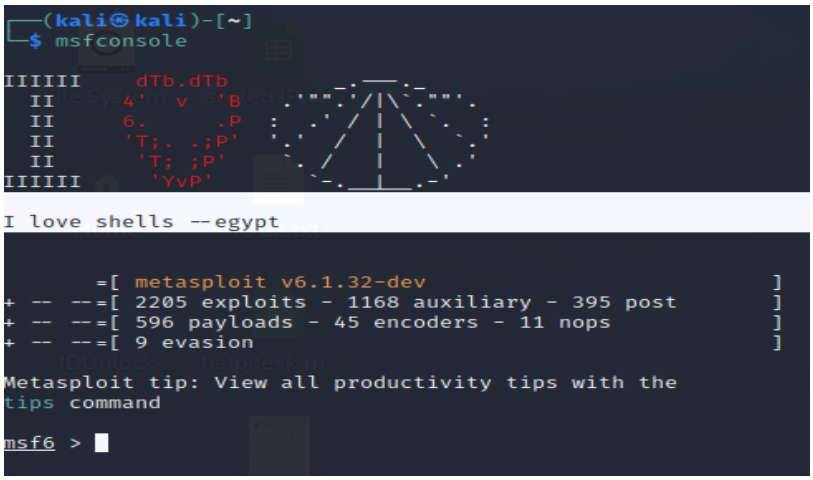

Figure 7: Starting of Metasploit framework Console

Figure 8: Search for SYN Flood Attack Module

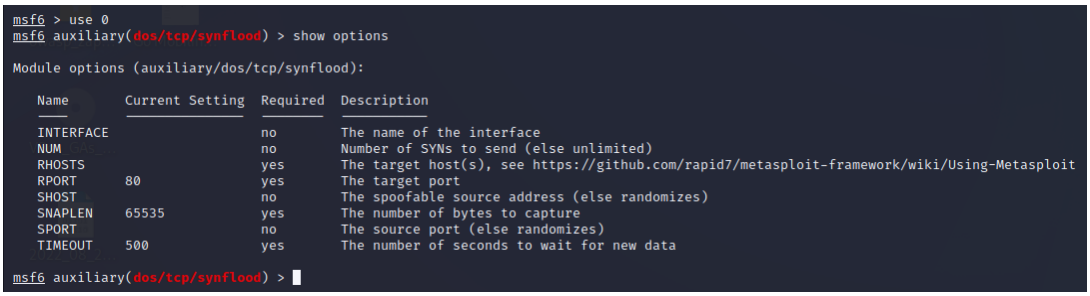

Figure 9: Set the Options of the Module to Launch SYN Flood Attack

3. Random Subdomain Attacks

A random sub-domain assault is a cyber-attack involving the creation of a large number of sub-domains under a valid domain name and the subsequent use of those sub-domains to conduct malicious attacks. This type of attack is known as domain name hijacking. This attack intends to circumvent standard security measures such as firewalls and intrusion detection systems by using subdomains that are not typically monitored or restricted. This may be accomplished using a domain name system (DNS) poisoning technique.

The attacker in a random sub-domain attack will construct sub-domains using random sequences of characters, such as "asdf.mydomain.com" or "qwer.mydomain.com," amongst other possible examples. The attacker might use an automated process to generate hundreds or thousands of these sub-domains in a concise amount of time. After the sub-domains have been formed, the attacker can utilize them to host phishing websites, malware downloads, and other harmful material.

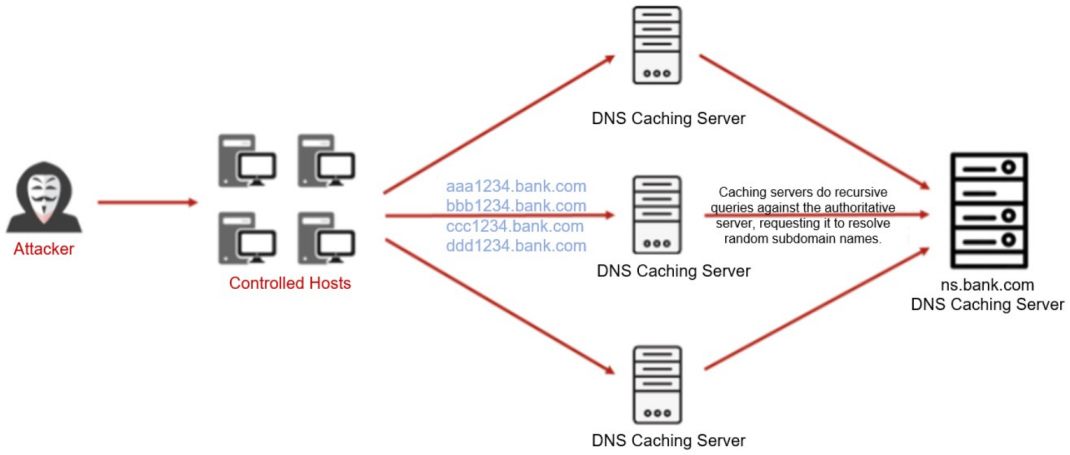

Figure 10: A Scenario of a random sub-domain Attack

Assuming an adversary intends to launch an assault on the authoritative server of a bank, which is located at ns.bank.com, by sending a high number of requests to fictitious subdomains:
aaa1234.bank.com
bbb1234.bank.com
ccc1234.bank.com
ddd1234.bank.com
...
Step 1: The attacker tells the controlled hosts it has under its control to submit a large number of DNS lookup queries to illegitimate subdomains to the DNS cache servers of an Internet service provider.
Step 2: Once the requests have been received, the DNS caching servers will do a DNS lookup, during which they will search the local DNS records. When the servers discover that none of their local records matches, they will iteratively query the authoritative server.
Step 3: DNS query requests from various DNS cache servers are flooded to the server considered to be authoritative.
Step 4: The DNS caching servers and the authoritative server each get a significant number of requests, which increases the volume of network traffic that may exceed the bandwidth limit. In addition, the servers might get so congested that they fail.

Mitigation Steps for DNS attacks:

1. DNS cache Poisoning:

- Use a trustworthy DNS resolver: Make use of a DNS resolver from a dependable supplier with a track record of security and dependability.
- Update your devices and software: Install updates frequently to fix any possible vulnerabilities in your system or program.

- Use DNSSEC: DNSSEC is an authentication and integrity checking extension for the DNS protocol. You can ensure that the DNS data you receive is legitimate and unaltered by turning on DNSSEC.

1. Distributed Reflection Denial of Service – TCP SYN Flood:

- Network-level security measures can be set in place to detect and stop malicious traffic before it reaches its targeted server. These measures include firewalls and routers.
- Use anti-DDoS services: Anti-DDoS services can filter out malicious traffic or reroute it to a different network to automatically detect and neutralize attacks in real-time.
- Configure rate-limiting: Servers can be made to accept a maximum number of incoming TCP SYN requests from a single IP address in order to reduce the quantity of incoming traffic.
- Keep software up to date: Stay current on security patches and upgrades for software and systems. By doing this, known vulnerabilities that attackers might use in DRDoS assaults can be addressed.

1. DNS hijacking:

- Use secure DNS servers: Use trustworthy, secure DNS servers instead of open or public DNS servers, which are more susceptible to attacks.
- Establish two-factor authentication: To prevent unwanted access to the DNS server, implement two-factor authentication for DNS accounts.
- Observe DNS traffic: Keep an eye on DNS logs and traffic to spot any odd behavior or suspicious DNS requests.
- Maintain software updates: To ensure that known vulnerabilities are fixed, maintain software and system upgrades with security patches.

1. Random Subdomain Attack:

- Implement subdomain filtering: Subdomain filtering should be used to prevent or restrict access to unidentified or suspect subdomains.
- Use SSL/TLS certificates: Encrypt all data sent between the client and the server using Secure Socket Layer (SSL) or Transport Layer Security (TLS) certificates to stop hackers from intercepting or altering the data.
- Use domain reputation-based services: Use domain reputation-based services that can instantly assess the reputation of domains and subdomains in order to identify and restrict harmful subdomains.
- Use Intrusion Detection System: Utilize an intrusion detection system (IDS) to identify suspicious activity and abnormal behavior and stop additional attacks.

Conclusion:
In conclusion, DNS attacks are becoming more common and sophisticated and can have significant consequences for both individuals and companies.
Overall, in order to protect their DNS infrastructure and maintain the privacy and security of internet users, companies and people must continue to be cautious and proactive in putting the mitigation measures into action. By doing this, DNS attacks can be made less likely to occur, have less of an effect, and can even be stopped in their tracks.

References:

- Rapid7, "What is a malware attack?," 2023. [Online]. Available: https://www.rapid7.com/fundamentals/malware attacks/#:~:text=A%20malware%20attack%20is%20a,command%20and%20control%2C%20and%2 [Accessed 11 04 2023].
- CloudFlare, "What is a phishing attack?," 11 04 2023. [Online]. Available: https://www.cloudflare.com/learning/access-management/phishing-attack/
- CloudFlare, "What is a denial-of-service (DoS) attack?," 11 04 2023. [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
- Rapid7, "Man in the Middle (MITM) Attacks," 11 04 2023. [Online]. Available: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/
- Understanding DNS attacks: Identifying and patching vulnerabilities | Snyk
- Four major DNS attack types and how to mitigate them – BlueCat Networks