DNS Poisoning Attack

M.Tech ICT(ML)
Dhirubhai Ambani Institute of Information and Communication Technology

Supervisor: Prof. Anish Mathuria
Jigar Shekhat-202211004
Rutvik Prajapati-202211053

May 11, 2023

1 Purpose of the Project

The purpose of a DNS poisoning project is to investigate and analyze the potential vulnerabilities and security risks related to Domain Name System (DNS) poisoning, also known as DNS cache poisoning or DNS spoofing. DNS poisoning occurs when an attacker manipulates the DNS cache of a domain name server, redirecting legitimate traffic to a fraudulent website or server. This type of attack can be used to steal sensitive information, such as login credentials, financial data, or personal information.

The main goal of a DNS poisoning project is to identify and assess the effectiveness of various techniques for detecting, preventing, and mitigating DNS poisoning attacks. This can involve conducting experiments to simulate different attack scenarios and evaluating the performance of different security measures, such as DNSSEC (DNS Security Extensions), firewalls, intrusion detection systems, and network monitoring tools. The results of such a project can help organizations and individuals better understand the risks of DNS poisoning and take proactive measures to protect their networks and systems against these types of attacks.

2 Expected Outcome

1. **Website redirection:** The attacker can redirect users who attempt to access a legitimate website to a fraudulent website that they control. This can be done to steal sensitive information, such as login credentials, financial data, or personal information.

2. **Malware distribution:** The attacker can use DNS poisoning to redirect users to websites that contain malware or malicious software. This can allow the attacker to gain control over the user's device, steal information, or use the device to launch further attacks.

3. **Denial of service:** The attacker can use DNS poisoning to disrupt the normal operation of a website or network by redirecting legitimate traffic to non-existent servers or websites. This can prevent legitimate users from accessing the website or network and can cause damage to the reputation of the affected organization.
4. **Reputation damage:** A successful DNS poisoning attack can damage the reputation of the affected organization by causing users to lose trust in its online services and by causing financial losses due to fraudulent activities.
5. **Reputation damage:** A successful DNS poisoning attack can damage the reputation of the affected organization by causing users to lose trust in its online services and by causing financial losses due to fraudulent activities.
6. **Loss of revenue:** DNS poisoning attacks can result in loss of revenue for affected organizations, especially if customers lose trust in their online services or if sensitive information is stolen as a result of the attack.

3 Background Study

DNS poisoning, also known as DNS cache poisoning or DNS spoofing, is a type of cyber attack that targets the DNS infrastructure. DNS is a critical component of the internet that translates domain names into IP addresses that computers use to communicate with each other. DNS poisoning attacks occur when an attacker manipulates the DNS cache of a domain name server, redirecting legitimate traffic to a fraudulent website or server. DNS poisoning attacks can be carried out in various ways, such as by intercepting and modifying DNS responses, or by injecting fake DNS queries into the network. Once an attacker is able to poison the DNS cache of a target server, they can redirect users to a malicious website or server that they control. This can allow them to steal sensitive information, distribute malware, or launch further attacks.
DNS poisoning attacks can have serious consequences for organizations, including reputational damage, loss of revenue, and legal liability. They can also be difficult to detect and prevent, especially if attackers use sophisticated techniques to evade detection.
To mitigate the risk of DNS poisoning attacks, organizations can implement various security measures, such as implementing DNSSEC (DNS Security Extensions) to ensure the authenticity of DNS responses, using firewalls and intrusion detection systems to monitor network traffic, and regularly updating and patching software and hardware components. Additionally, organizations can provide training and awareness programs to employees and end-users to help them recognize and avoid phishing and social engineering attacks that may be used to initiate DNS poisoning attacks[1].

4 Working Steps

1. **Preparation and Configuring**
   by booting up Kali Linux, whether it's a Virtual Machine (VM), a native boot, or

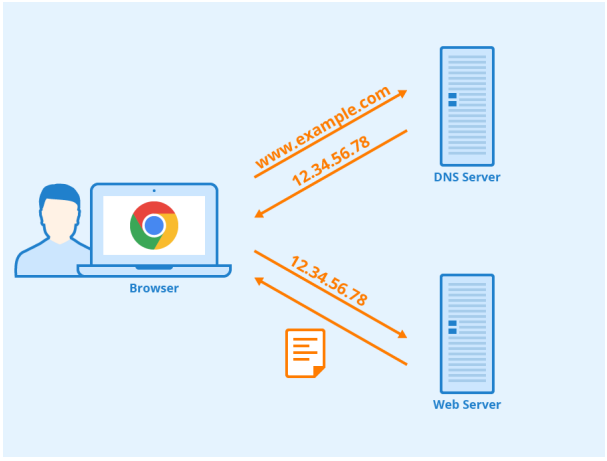

Figure 1: Use of DNS

a dual boot. We boot up kali linux in our VM. Kali Linux has an ettercap tool for our project which can be helpful in ARP poisoning on the target machine and default gateway.
After that, We edited the Ettercap configuration file (/etc/ettercap/etter.conf) and make uid and gid zero in that file. we also removed both the # signs below where it says "if you use iptables".

2. **ARP poisoning**
After configuring that file, We had done ARP poisoning on target 1 and target 2 in ettercap. Target 1 is Victim Machine and Target 2 is Default gateway.

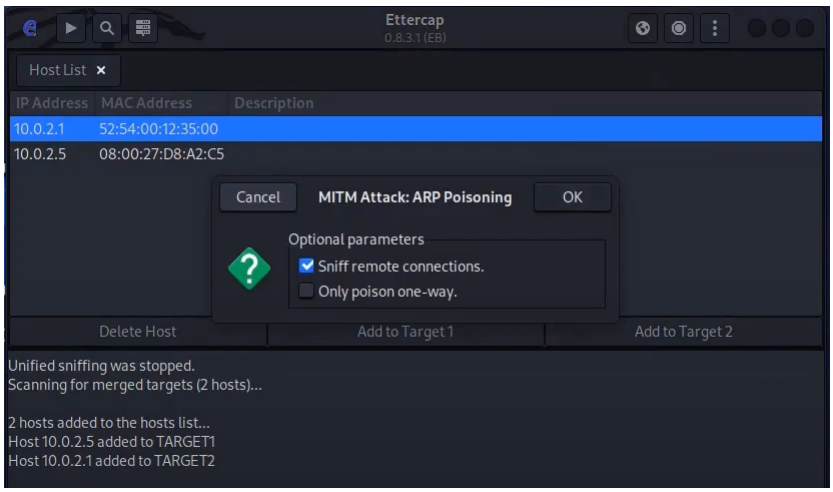

Figure 2: ARP poisoning

3. **Action**
   After ARP poisoning, We perform dns spoofing which is given in the manage plugin in Ettercap.

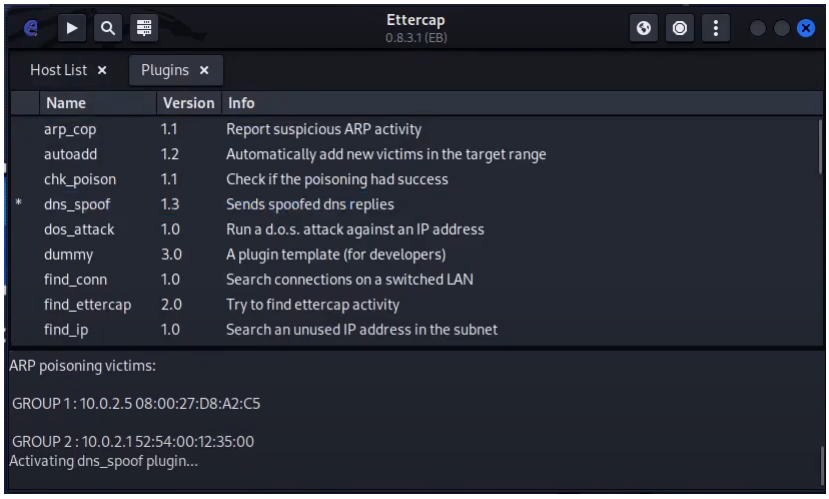

Figure 3: DNS spoof

We also perform DNS spoofing via python. In that, We write code in Python language with help of scapy module. By that code, We can spoof the DNS.

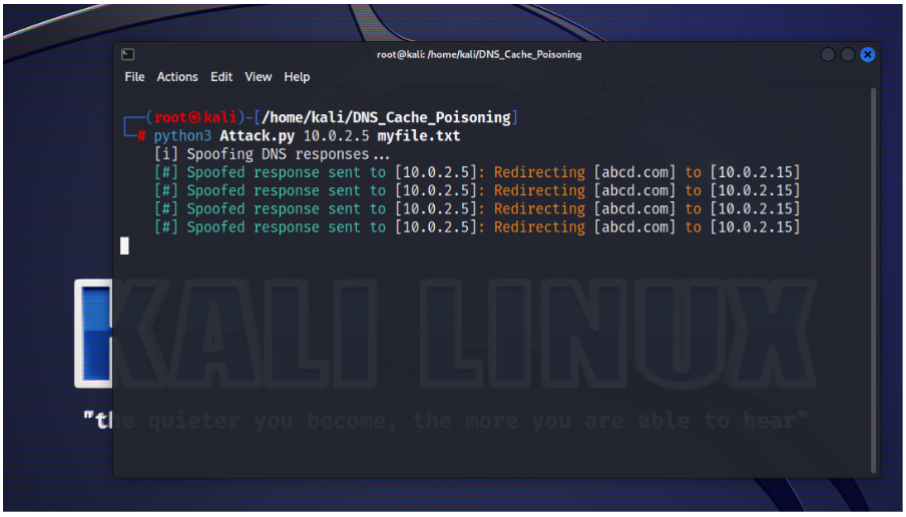

Figure 4: Python-scapy code

5 Real-World Examples of DNS Poisoning

- On January 26, 2015, a hacker group managed to redirect visitors of the Malaysia Airlines (MAS) official website to another site displaying malicious content.
- April 2018, a major DNS cache poisoning attack compromised Amazon's DNS servers, redirecting users to malicious websites.
- November 2011, a large-scale attack on ISPs in Brazil rerouted traffic from popular sites (including Google, Gmail, and Hotmail) to a web page that installs malicious Java applets.
- December 2009, hackers redirect traffic from Twitter to their own website.

MAS was right. Their own hardware/servers were not actually "hacked". Instead, they had fallen victim to a hack attack that indirectly affected them.

6 Prevention

1. **Client-Side Prevention**
   - Keep your Antivirus/Anti-malware apps "Cooking and Up-to-Date"
   - If you have the possibility, browse the internet via a Virtual Machine
   - Don't download suspicious files. If you insist, do it through a "sandboxed apps" or a Virtual Machine
   - Use a respected DNS Server and a reputable ISP
   - Always double-check websites you visit (check if there is HTTPS encryption)
   - Flush computer DNS cache as well as DNS cache stored in the route

   Additional long-term prevention:
   - Virtual Private Network (VPN): A service that encrypts all the internet traffic going to and from a device and routes it through an intermediary server in a location of the user's choosing.
   - Encrypted DNS: Apps that encrypt DNS traffic between the user and an OpenDNS nameserver (similar to how SSL encrypts traffic to websites that use HTTPS).
2. **Security mechanisms developed for DNS server operators**
   - UDP Source Port Randomization (UDP SPR): What this does is setting the UDP source port randomly, so an attacker would have to guess both the transaction ID and the source port in a short time window - which is usually not feasible (2^{32}).

- DNS Security Extensions (DNSSEC): It is a protocol designed to create a unique cryptographic signature and store it alongside other DNS records. Thus, DNSSEC provides DNS with an additional methods of verification by digitally signing the DNS information. This is done on all levels of the DNS Resolution process [2][4].

3. **DNS Poisoning Detection** Detecting DNS poisoning attacks can be challenging, as attackers may use sophisticated techniques to evade detection[3]. However, there are several methods that organizations can use to detect DNS poisoning attacks, including:

   - Monitoring DNS traffic: Organizations can monitor DNS traffic on their network to detect any anomalies or suspicious activity, such as unexpected DNS responses, unusually high traffic volume, or patterns of requests that do not align with normal traffic.
   - Using DNS monitoring tools: There are various DNS monitoring tools available that can help organizations detect DNS poisoning attacks. These tools analyze DNS traffic and use machine learning algorithms to identify patterns and anomalies that may indicate an attack.
   - Monitoring network logs: Organizations can monitor network logs to detect any suspicious activity, such as unusual DNS queries or requests from unfamiliar IP addresses.
   - Conducting penetration testing: Organizations can conduct regular penetration testing to identify vulnerabilities in their DNS infrastructure and test the effectiveness of their security measures in detecting and preventing DNS poisoning attacks.

7 Observation:

We had to be connected to their LAN in order to carry out the DNS poisoning assault. As a result, this is the limitation we have. We found that DNS poisoning attacks can be challenging, as attackers may use various techniques to evade detection. However, there are several indicators that can suggest that a DNS poisoning attack may be occurring:

- Unexpected website redirection
- Unusual network traffic
- Inconsistent DNS responses
- DNSSEC validation failure

If any of these symptoms are recognized, poisoning the DNS will be extremely difficult.

8 Conclusion

As you can see, DNS is crucial to the operation of websites and online services on a daily basis. Unfortunately, attackers may perceive it as an appealing chance to compromise your networks. This is why it is critical to monitor your DNS servers and traffic. We must exercise caution when using the Internet.
If the victim lacks awareness and does not use any prevention strategy. As a result, the attacker may easily poison the DNS for that victim and successfully reroute any website on the victim's system.

9 Future Work

We performed DNS poisoning on a target that was in the same area network as us. In the future, we can attempt a target that is not on the same network.

References

[1] Fatemah Alharbi, Yuchen Zhou, Feng Qian, Zhiyun Qian, and Nael Abu-Ghazaleh. Dns poisoning of operating system caches: Attacks and mitigations. *IEEE Transactions on Dependable and Secure Computing*, 19(4):2851–2863, 2022.

[2] Artem A Maksutov, Ilya A Cherepanov, and Maksim S Alekseev. Detection and prevention of dns spoofing attacks. In *2017 Siberian Symposium on Data Science and Engineering (SSDSE)*, pages 84–87. IEEE, 2017.

[3] Yasuo Musashi, Masaya Kumagai, Shinichiro Kubota, and Kenichi Sugitani. Detection of kaminsky dns cache poisoning attack. In *2011 4th International Conference on Intelligent Networks and Intelligent Systems*, pages 121–124. IEEE, 2011.

[4] Jonathan Trostle, Bill Van Besien, and Ashish Pujari. Protecting against dns cache poisoning attacks. In *2010 6th IEEE Workshop on Secure Network Protocols*, pages 25–30. IEEE, 2010.