Overview

This project simulates a cyberattack designed to steal confidential data and payment information from users engaging in e-transactions over unprotected networks. The attack utilizes a proxy webpage disguised as a legitimate website to trick users into entering their credentials, which are then captured by the attacker. The attack is executed through ARP spoofing to position the attacker between the client and server, followed by DNS spoofing to redirect the user to a malicious site controlled by the attacker.

The primary goal of the simulation is to gain insight into how cyberattacks like this exploit network vulnerabilities to retrieve sensitive user information such as usernames, passwords, and financial details, which can later be used to access banking accounts or social media profiles. For demonstration purposes, the attack replicates the Amazon login page, but it could also mimic other popular platforms like Gmail or Bank of America.

The simulation explores how such attacks can be conducted in person by targeting users in upscale locations such as cafes or libraries, where people might knowingly or unknowingly access unsecured networks. It also examines the use of phishing emails that appear as legitimate banking notices or shipping confirmations, enabling attackers to remotely target individuals from similar high-income demographics.

Objectives

- Analyze the vulnerabilities in network security that allow attackers to steal confidential data such as usernames, passwords, and payment information.
- Simulate the login page of trusted websites (e.g., Google Accounts, Amazon, Bank of America) to study the effectiveness of openly-accessible and automated phishing and spoofing techniques.
- Understand and demonstrate the role of social engineering and network spoofing methods, such as ARP and DNS spoofing, in compromising user security.

Technologies Used

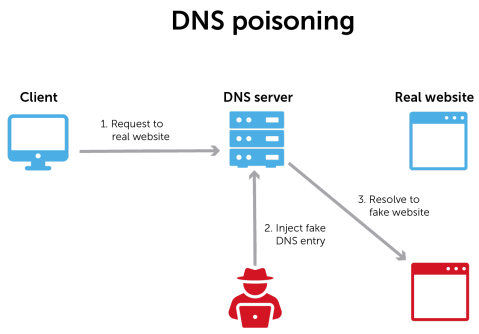
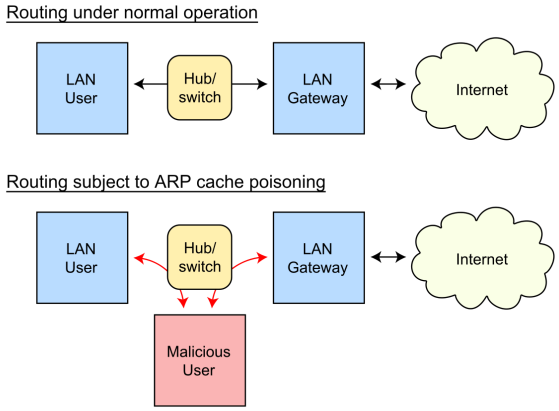
- Kali Linux: Tools like Ettercap and DNSchef for spoofing.
- Wireshark: For network traffic analysis.
- HTML/CSS: Used to create a cloned website for phishing.

Attack Methodology

1. ARP Spoofing: Insert the attacker into the network between the client and the server.
2. DNS Spoofing: Redirect traffic from the victim to a malicious website.
3. Website Cloning: Create a convincing copy of trusted sites like Amazon or Bank of America to phish for credentials.

4. Phishing Emails: Use social engineering techniques to enhance the likelihood of victims falling for the fake site.

Walkthrough

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Source: https://bluecatnetworks.com/blog/what-is-dns-poisoning-how-to-prevent-it/</td>
<td>Source: https://en.wikipedia.org/wiki/ARP_spoofing</td>
</tr>
</table>

We're using **A** to refer to steps performed by the attacker and **V** for the victim. The following instructions are based on a YouTube tutorial on using Ettercap for DNS and ARP spoofing:

1. **[A]** Open PowerShell and type ipconfig to find your IP address. This will help verify if Ettercap is working in the subsequent steps.
2. **[A]** In PowerShell, start the Apache web server by typing sudo service apache2 start and enter your sudo password. Apache is a free, open-source web server software that hosts a server capable of accepting HTTP requests.
3. **[V]** On the victim's laptop, open a browser and enter the attacker's IP address to check if it displays the default Apache web page. Next, modify the default page to look like the phishing site you intend to use.
4. **[A]** In PowerShell, navigate to the directory containing the default web page by typing cd /var/www/html and list the files with ls -l.
5. **[A]** Locate the index.html file. Type sudo mv index.html index-old.html to rename the current file, and then type sudo vi index.html to begin editing the malicious site.
6. **[V]** Reload the IP in the browser to verify if the site's appearance has changed.
7. **[A]** Navigate to the Ettercap configuration directory by typing cd /etc/ettercap. We will edit two files: etter.conf and etter.dns to configure Ettercap.
8. **[A]** Open etter.conf with sudo vi etter.conf and change ec_uid and ec_gid to 0. Then, locate the OS-specific section for Linux by typing /Linux and uncomment (remove the # from) all lines within this section.

9. **[A]** Open etter.dns with sudo vi etter.dns and add the following lines at the bottom:

    sitename.com A [Attacker's IP]

    *.sitename.com A [Attacker's IP]

    www.sitename.com PTR [Attacker's IP]

10. **[V]** Enter sitename.com in the browser to check if the site now reflects the changes.
11. **[A]** Move on to the ARP poisoning step to position the attacker between the victim and the network. Open Ettercap, select targets, and add the victim as Target 1 and the default gateway as Target 2.
12. **[A]** In Ettercap, go to the menu (three dots) > Plugins > Manage Plugins > and activate dns_spoof.
13. **[V]** Visit http://sitename.com. Since HTTP traffic is unencrypted, Ettercap will capture any form elements sent by the victim for the attacker to review.

Future Additions

1. **Customization of Phishing Emails:** The website will collect data about targeted individuals, such as their interests or recent purchasing activity. This information will enable attackers to craft personalized phishing emails that are more likely to succeed.
2. **Machine Learning Techniques:** Integrating machine learning can enhance the success rate of attacks by analyzing user behavior from previous attacks and using this data to predict responses. For instance, machine learning algorithms can determine the optimal time to send phishing emails or identify which social engineering tactics are most effective.
3. **Advanced Social Engineering:** Attackers may employ more sophisticated social engineering techniques to gain users' trust and access the website. For example, they could set up a fake customer service hotline and respond to user calls, providing reassurance that the website is legitimate.

References

1. "DNS Spoofing Attacks." *YouTube*, https://www.youtube.com/watch?v=g-XZpTxusS8.
2. "ARP Poisoning." *YouTube*, https://www.youtube.com/watch?v=A7nih6SANYs.
3. "ARP Spoofing with arpspoof - MITM." *YouTube*, https://www.youtube.com/watch?v=8SIP36Fym7U.
4. "Ettercap Tutorial." *YouTube*, https://www.youtube.com/watch?v=0yxI6izcs5g.
5. Nancy John. "Using SET Tool Kit to Perform Website Cloning in Kali Linux." *Medium*, https://medium.com/@nancyjohn_95536/using-set-tool-kit-to-perform-website-cloning-in-kali-linux-67fa01c92af9.