Assignment 5

New Attempt

- Due Oct 22, 2024 by 11:59pm
- Points 100
- Submitting a file upload
- File Types pdf

Due: Tuesday, October 20, 2024 (11:59 PM). Please submit your assignment on Canvas as a PDF.

DNS Spoofing and Social Engineering

In this assignment, you will learn how to perform DNS spoofing. Then you implement a social engineering scenario, and eventually, you integrate DNS spoofing and social engineering to have a more complete attack. You use bettercap for doing DNS spoofing and Social Engineering Toolkit to perform social engineering.

DNS Spoofing

Domain Name Server (DNS) spoofing (a.k.a. DNS poisoning) is a type of attack in which an attacker alters the DNS records so that the victim is redirected to a fraudulent website that resembles the original one.

After a successful DNS spoofing, the attacker can take advantage of users' trust in different ways for malicious objectives. For instance, users may be asked to login into (what they believe to be) their account, giving the attacker the opportunity to access their sensitive information. It is common that malicious websites to install worms or viruses on the user's system which means the attacker will potentially have access to the victim's computer for a long term.

Methods for executing a DNS spoofing attack include:

1. Man In The Middle Attack (MITM)
2. DNS Server Compromise

In this assignment, we use MITM to perform DNS spoofing.

Social Engineering

Social engineering is the term used for a range of attacks that use psychological manipulation aiming at fooling users to reveal their sensitive information by making security mistakes. In a social engineering attack, an attacker first investigates the victim in order to acquire various background information. Then the attacker proceeds to gain the victim's trust to behave according to the attacker's interest.

Setup

For this assignment, we need the following VMs: Router, Kali Linux, Windows 7. Kali Linux is used as an attacker and Windows 7 VM is the target machine. In Kali, you need to have bettercap installed. Furthermore, you will need Wireshark which is already preinstalled in Kali. Lastly, you also need the Social Engineering Toolkit (SET) which is already preinstalled in Kali. You can access SET using the command `setoolkit`.

1 The dns.spoof Module (35%)

In this task, we are going to explore the dns.spoof module of bettercap. This module replies to DNS queries with spoofed responses. You are going to create a sample website in Kali and redirect the user to it using DNS spoofing.

In order to perform DNS spoofing, you need to establish a MITM attack on the victim machine. Also, you need to enable apache2 in order to be able to serve a website in Kali (command to enable: `service apache2 start`).

Task 1 (5 %): Create a sample HTML file in Kali and place it under `/var/www/html` with a name `index.html`. Report the screenshot of the website you created as it appears from the target machine.

Task 2 (10 %) Now use the dns.spoof module of bettercap to attack the target machine and redirect requests to facebool.com (facebool is not a typo) to the attacker's IP. Report the commands you used in order to perform the attack.

Task 3 (5 %): Report a screenshot by visiting facebool.com from the target machine.

Task 4 (15 %): Explain how the dns.spoof module works under the hood in terms of packet inspection.

2 The Social Engineering Toolkit (SET) (35%)

The Social-Engineer Toolkit is an open-source tool for social engineering. In this task, you will be introduced to the social engineering toolkit and more specifically the harvester credentials method which is a method for cloning a website (usually to acquire the login credentials of the user).

Task 5 (5 %): Run `setoolkit` and find the proper option in order to perform the attack by cloning a website's login form. You can choose the website you prefer to clone. Report the commands needed to perform the website cloning attack.

From the target machine visit the attacker's IP and verify that you can see the cloned website. Then, try to login to the website.

Task 6 (5 %): Report a screenshot of the cloned webpage created by the cloning attack.

Task 7 (5 %): According to your opinion what does the `setoolkit` do under the hood when it performs the harvester's credential attack?

Task 8 (10 %): Select another module of SET (of your choice) other than harvester's credentials and perform a social engineering attack. What module did you choose? Explain your result.

Task 9 (10 %): Discuss the role of social media platforms in modern social engineering attacks. Define 2 or more scenarios where an attacker uses Social media to gather more information on a target.

3 Combining dns.spoof with SET (30%)

In this task, we are going to explore the dns.spoof module of bettercap in combination with the Social Engineering toolkit.

Use the command `setoolkit` to generate a clone credentials harvester website to clone a login form of a website of your choice (e.g **https://twitter.com/login (https://twitter.com/login)**). After cloning the website the tool creates a website under your machine's IP address. Visit your machine's local IP address in order to verify it is working. Enter a username and a password and check if `setoolkit` “grabbed” the information from the form.

After successfully cloning the website we are going to perform a DNS attack on the target machine and have our cloned website to be displayed when a specific domain name is visited from the target machine. Set the proper options and start the dns.spoof module in order to redirect requests to twiter.com (twiter.com is not a typo) to the attacker’s IP address similar to what you did in Task 1.

Verify that the dns.spoof works. Now change the dns.spoof name from twiter.com to a website that you have previously visited (you may have to restart dns.spoof module). Visit that website from the victim's machine.

Task 10 (5 %): Why DNS spoofing doesn’t work on previously visited websites?

Task 11 (10 %): The user in the target machine (victim) can help the attacker to complete the failed DNS spoofing (see task 12). Explain how this can happen.

Task 12 (5 %): Explain how DNS over HTTPS (DoH) and DNS over TLS (DoT) work and discuss how they can prevent DNS spoofing attacks.

Task 13 (5 %): Explain how DNSSEC can be used to prevent DNS spoofing attacks.

Task 14 (5 %): Explain how else you could prevent DNS spoofing attacks.