CyberSecurity Lab Report: Phishing Attack Simulation Using the Social-Engineer Toolkit (SET) | ARP Spoofing Attacks | NTLMv2 Hash Stealing and Cracking in a LAN Network Setup

Mark DAKROUB[M], **Mohamed Amine BELKHALIFA**[M] **and Saibou KEITA**[S]

[1]*Dsti School Of Engineering*
[1]*CyberSecurity Project*
[1]*Applied MSc in Data Engineering for Artificial Intelligence*

Professor Adel KHALDI - Fundamentals of Cyber Security Practices

Abstract—In our current digital advancement and the use of AI tools and technologies, hackers today became very expert in using their knowledge to exploit systems, assets and valuable information. One of the well known initial strategies being used is "Information Gathering" which uses "DNS Analysis" to gather information about the assets. Phishing is also a cyber crime methodologies used after DNS Analysis, in which web applications , emails. telephone, text messages, banking details, credit card details and credentials are all targeted. Phishing is mainly a form of online identify theft. Phishers usually use Social Engineering as a way to steal the victim's personal data and account details. This study will give a comprehensive and Demo Lab of how these attacks are performed, and will also discuss ways and recommendation to protect yourself from future identity and credentials theft.

Keywords—*VmWare, Pshishing, Credentials, Kali, Windows*

1. Introduction

Phishing is a cyber crime activity in which hackers attempt to extract crucial information such as banking and credit card details and credentials by targeting the victim as a trustworthy entity in an electronic communication. Phishing comes in various ways; it can be from a popular Web application site, advertisements, auction sites, and online payment processes. Phishing sites and emails links are usually infected with malware. In email Email hacking, the hacker sends a link via email to the victim regarding banking or personal information, when the user clicks on the link and fills in the details, all personal information and credentials are automatically sent to the attacker's host machine. In the image below, we have how phishing is done:

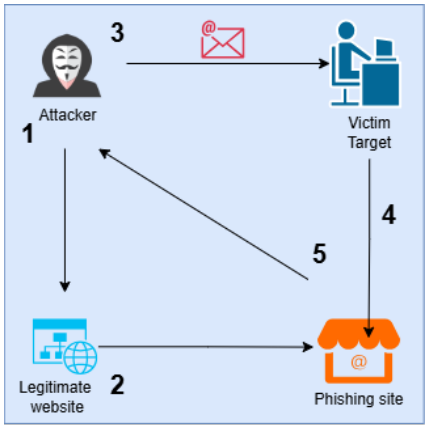

Figure 1. Phishing steps

1. The attacker chooses a suitable website to clone.
2. The attacker clones the web application.
3. The attacker sends the web application.
4. The victim clicks on the link and enters their credentials.
5. The victim's credentials are sent to the attacker's host machine.

Phishing always starts with an email invitation or a link wrapped in a logo or a symbol, any communication type is harnessed to complete the process. The message is made in a way to reveal itself as a trust worthy entity, if the victim is fooled, his credentials will be exposed. Sometimes malware also comes in a form of downloading a malicious code into the victim's turing machine.

2. Objectives

Phishing attacks have emerged as one of the insidious threats to information security. These attacks exploit human psychology by exploiting the deception to trick humans into giving out their credentials and financial details. This study contains a lab, which aims to provide hands-on experience in simulating a phishing attack using the Social-Engineering Toolkit (SET) within a controlled environment. By understanding the mechanics of such attacks, cybersecurity professionals can better anticipate the potential threats and readers can learn more about how to protect themselves. The main objectives of this lab is:

- **Comprehension**: To understand the principles and methodologies underlying phishing attacks.
- **Tool Utilization**: gaining proficiency in using the Social Engineer Toolkit (SET) for creating realistic phishing scenarios.
- **Execution**: carrying out a credential harvesting attack within a controlled lab environment.
- **Analysis**: evaluating the efficiency of the attack and understand the implications of such security breaches.
- **Mitigation Strategies**: proposing strategies for preventing phishing attacks incidents.

3. Background

3.1. Understanding Phishing

Phishing is a form of cyber crime that utilizes social engineering, the attacker reveals himself as a trustworthy entity to deceive individuals into giving away their confidential credentials and information. These attacks often involve fraudulent emails, websites and luring victims into providing sensitive data.

3.2. The Social-Engineer Toolkit (SET)

The (SET) Social Engineering Tool, is an open source tool written in python, designed to perform deceptive tasks against humans. Understanding the functionality and application of SET is crucial for cybersecurity professionals, as it provides insights into how attackers deploy their deceptive phishing campaigns, enabling defenders to perceive sooner threats and take proper measurements and counter-attack such threats.

4. Lab Environment Setup

- **Environment**: VM-Ware PRO, hosting the VMs.
- **Attacker Machine VM**: Kali Linux 2023.3.
- **Target Machine VM**: Windows 7 operating system.
- **Network**: Local Area Network (LAN) with IP range.

5. Methodology

5.1. Virtual Lab Deployment Guide

5.1.1. Prerequisites

- VMware Workstation Pro installed.

- Importing the VMs.
- Admin privileges.

5.1.2. Installing the VMware Workstation Pro

1. Download the installer for VMware Workstation Pro from the official VMware website: VMware Workstation Pro – Free for Personal Use.
2. During installation on the Windows OS, ensure that Windows Hypervisor Platform (WHP) is enabled.

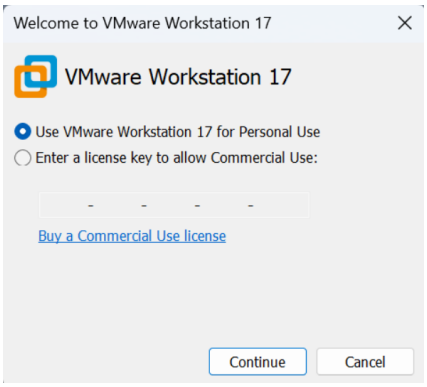

Figure 2. Your image caption here

5.1.3. Creating a VM directory

1. create a folder to organize the VMs.
2. The folder will serve as the root storage location for the configurations files of the VM.

5.1.4. Configuring VMware Workstation

1. Launch the VM workstation.
2. Go to:
   - `Edit` → `Preferences` → `Workspace`
   - Set the default location for the VM.
3. Updating the NAT DHCP lease time:
   - Navigate to: `Edit` → `Virtual Network Editor`
   - Click on change Settings.
   - Select `VMnet8 (NAT)` from the list.
   - Click `DHCP Settings`.
   - Set both `Default Lease Time` and `Maximum Lease Time` to 63 days.
   - Then click `apply` and then `ok` to save changes.

Below figures are the configurations:

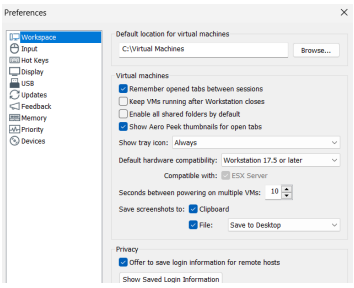

Figure 3. Default location

5.2. Downloading Virtual Machine Images

5.2.1. Kali Linux Attacker VM

Download the Kali Linux VMware image,standard build from the official site: https://www.kali.org/get-kali/kali-virtual-machines

- Choose the **VMware format**.
- Download the **ZIP archive**.

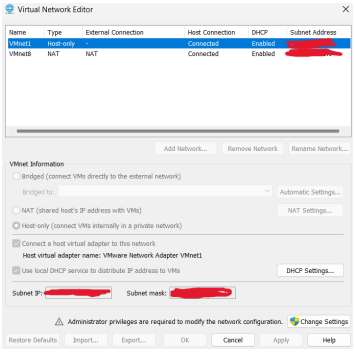

Figure 4. NAT Settings 1

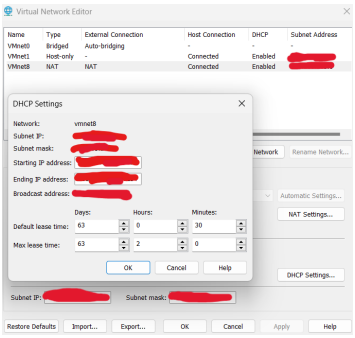

Figure 5. NAT Settings 2

5.2.2. Windows 7 Victim VM

Download the Windows 7 VM from the following OneDrive link: Windows 7 VM (OneDrive)

- This file is typically in `.ova` (Open Virtualization Archive) format.

5.3. Organizing and Importing the VMs

- Extract the VM Kali file and import it to the default location.
- Do the same with the Windows .ova file.

5.4. Optimizing the VM's configurations

- Go to both VM's configuration settings.
- Configure the RAM and CPU
- Apply the settings and close the configuration window.

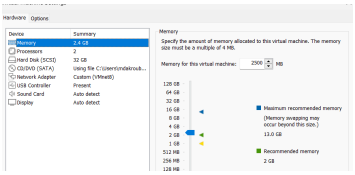

Figure 6. Configurations

6. Attack Execution

6.1. Launching SET

In order to use the Phishing toolkit, we first have to access the Kali Linux main menu, and the navigate to exploitation tools and select the Social Engineering Toolkit (SET). This framework is mainly used for simulating social engineering attacks. Once selected, a new terminal window will pop up. The system will prompt the user to enter their password, this step is crucial to provide permission for SET to function properly. The toolkit then load its main interface, offering a range of options for deploying phishing attacks.

After execution, the social engineering toolkit SET will launch an interactive terminal with operational categories

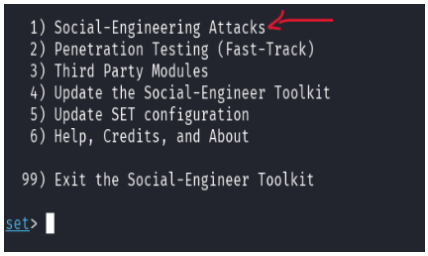

Figure 7. setoolkit options

We will be focusing on Social Engineering Attacks module. This option enables the creation of phishing websites to harvest login credentials.

After our first selection, the toolkit will present a new set of choices. our main option to choose is Website Attack Vectors, this option will provide us with various techniques for conducting the attacks.
I

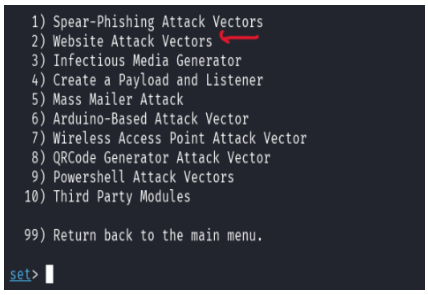

Figure 8. Website attack vectors

In this option, we'll be using the Credential Harvester Attack method, which will help us to clone a any legitimate login page, this will enable us to trick the victim to enter his credentials. This method is mainly effective in phishing simulations as it mimics real-world attack strategies.

Figure 9. Credentials Harvesting

6.2. Cloning the Target Website

This options offers us different approaches to create the ground basis for the phishing attack. The first method will allow the SET toolkit to import a list of pre-created or pre-defined websites which can be directly used for an attack. This option is mainly used for demonstration and testing purposes.

The second method will offer a better flexibility which will enable the attacker to choose a specific website that the victim visits regularly. SET will clone the website's HTML and allow the attacker to embed credential harvesting mechanism with the code in the cloned interface. this option is useful for personalized attacks.

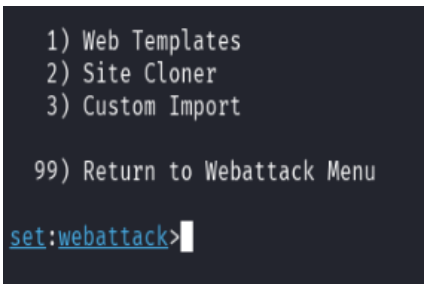

Figure 10. Site Cloner

The third option allows the user to import a custom-built website which includes basic HTML format file, this option is more suitable for advanced attackers who can customize their own website.

For our today's attack, we'll use the second option –> Site Cloner. This method will enable cloning any specified website to create a realistic phishing scenario.

6.3. Setting the IP Address

Following our next step, Kali's command line will prompt for the IP Address for the attacker's host machine. This will is required so that the harvested credentials can be harvested credentials can be sent to the attacker's host machine. In order to obtain the IP address, a separate terminal window should be opened, and the command "Ip a" can be excuted to display the network configuration details.

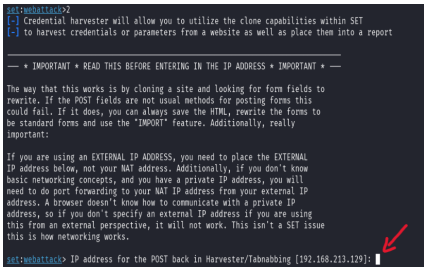

Figure 11. IP Address

6.4. Cloning and Hosting the Site

After obtaining the IP address, the next step involves specifying the target web application to be cloned.

Figure 12. Cloning configuration

The chosen URL is the official login Facebook's page. SET then replicates the web page template and turns it into a phishing link. This cloned page is hosted locally on the attacker's Kali machine and is automatically configured to send any harvested credentials to the specified IP address.

Figure 13. Cloning configuration (continued)

6.5. Victim's Interaction

During the cloning process, the specified website's structure is cloned and a local web server is automatically launched on the attacker's

host machine. The server will remain active waiting for it's victim to insert his credentials. Once the victim accesses the phishing link and enters his credentials. The information is captured and logged in real-time.

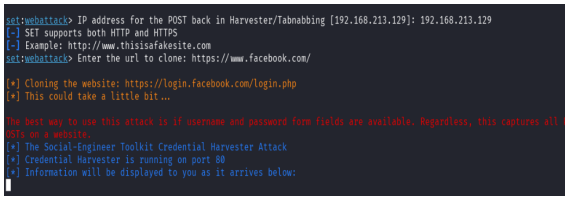

Figure 14. Local server launched

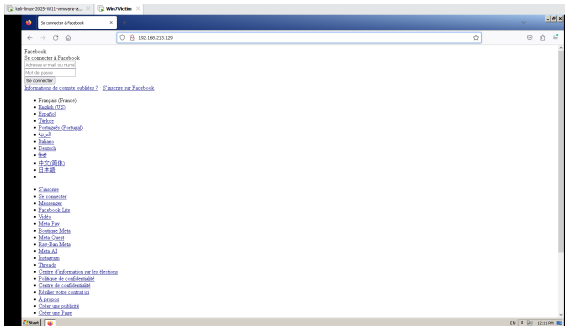

Figure 15. Phishing website

7. Results

7.1. Phishing output

Below we can see the result after the victim has clicked on the web application and inserted his credentials. After the whole process is completed, the setoolkit will create an XML report containing all the information and the credentials.

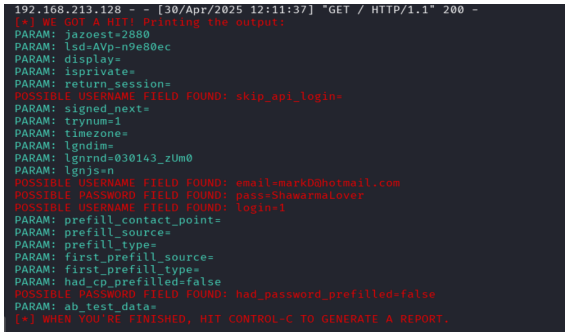

Figure 16. Phishing website

The XML report contains configuration details, such as the selected attack vector, the IP address, the cloned website URL and the harvested credentials of the victim. The credentials includes banking details, username, passwords and credit card serial numbers. The XML format is used in order to ensure the data is well structured and can be parsed for further analysis.

7.2. Output as report

An important information about accessing the XML report, when attempting to access the report as a standard user, Kali will deny your access because the setoolkit is mainly executed with elevated privileges using sudo. All files generated from the setoolkit are typically owned by the root user, and the operating system enforces access control to prevent non-root users from modifying or viewing the files.

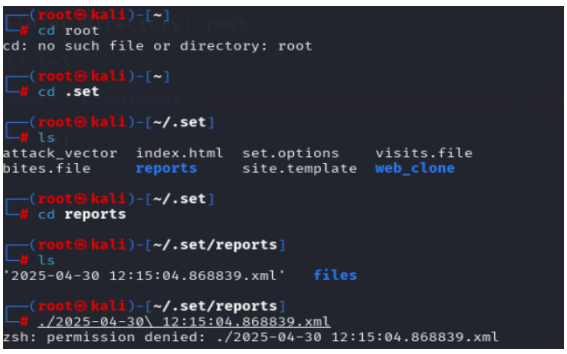

Figure 17. Accessing report

After switching to root user obtaining the admin privileges, accessing the XML report becomes available. The report contains detailed information about phishing sessions with date and time of the attack, the phishing URL and the harvested credentials.

Figure 18. root-user report

8. Analysis and Key Observations

The experiment we conducted demonstrates how easily phishing attacks can target both public and private users. With the increasing availability of open-source tools—combined with the growing influence of artificial intelligence—such attacks are becoming more frequent and sophisticated. The success of the phishing attack did not rely solely on system vulnerabilities, but primarily on psychological manipulation, particularly the user's sense of trust.

Key Observations:

- **User Trust:** The study shows that users are more inclined to trust websites that appear familiar and legitimate. This tendency significantly increases their vulnerability to phishing attacks, especially when the cloned site convincingly mimics a trusted platform.
- **Tool Accessibility:** Social engineering tools such as SET lower the barrier to entry for executing advanced phishing campaigns. The widespread availability of such tools highlights the urgent need for increased public awareness and user education about preventive security measures.
- **Network Vulnerabilities:** The success of the attack was enabled by the fact that both virtual machines were operating within the same Local Area Network (LAN). This scenario emphasizes the importance of implementing access controls, network segmentation, and traffic monitoring to detect and prevent internal threats.

9. Recommendations

A comprehensive and an effective security approach is needed in order to reduce the risk of phishing attacks. The below strategies are recommended to strengthen the user awareness, technical preventions:

9.1. User Security Literacy:

The most well known strategy to secure yourself and prevent any future attacks by being knowledgeable in security trainings. Big organizations should always implement continuous training and conduct simulated phishing campaigns to increase user awareness. These trainings can help identify any possible future phishing signs such as suspicious emails, attachments and links.

9.2. MFA: Multi Factor authentication

: Adding an additional layer of security is crucial for users to provide a better form of verification when accessing their accounts and systems. When credentials are stolen, attackers will not have the ability to enter the account if they do not possess the device which contains the MFA security, hardware security key or any biometric data. This approach will prevent the attacker from accessing any account or process any unauthorized event in any successful phishing attempt.

9.3. Email Filtering

: Adding a filtering option in the email will prevent phishing emails from reaching end users. These strategies can leverage the use of machine learning, fraud detection and threat intelligence to identify and quantine any suspicious emails.

9.4. Secure Browsing:

It's better to take cautious approaches when checking websites, always enable the HTTPS encryption and avoid entering eny unfamiliar websites. Most organizations provide security plugins for the browser to warn the users when visit any penitential malicious web applications.

9.5. Network traffic monitoring:

Some security measures can be deployed to increase the security settings in networks, such as IPS - Intrusion Prevention Systems, this tool is deployed to monitor network traffic for suspicious activities. This tool powerful in detecting anomalies and block suspicious traffic in real time. This tool can help organizations identify threats early, early prevention measures can be taken to prevent security breaches from escalating.

10. ARP Spoofing Attacks

10.1. Introduction to ARP Spoofing Attacks

An Address Resolution Protocol (ARP) spoofing attack is a type of man-in-the-middle (MITM) cyberattack that exploits weaknesses in the ARP protocol, a fundamental component of local area networks (LANs). ARP is responsible for mapping dynamic IP addresses to physical MAC addresses, enabling devices to communicate on a network.

In an ARP spoofing attack, a malicious actor (using Kali Linux in our scenario) sends forged ARP messages to the local network. These messages falsely associate the attacker's MAC address with the IP address of a legitimate device, such as the network gateway (a router). This redirects traffic intended for the victim through the attacker's machine, allowing them to:

- Intercept Data: Capture sensitive information (e.g., login credentials, emails, or financial details).
- Modify Traffic: Alter data packets or inject malicious conten (malware).
- Disrupt Connectivity: Cause denial-of-service (DoS) by blocking or flooding the victim's connection.

This attack is particularly dangerous because it operates at the data link layer (Layer 2 of the OSI model), bypassing many traditional security measures like firewalls. For the Windows 10 victim, the attack may go unnoticed unless advanced network monitoring or encryption (HTTPS, VPNs) is in place.

10.2. What is Ettercap and How it Works for ARP Poisoning

Ettercap is a comprehensive, open-source network security tool designed for man-in-the-middle (MITM) attacks, packet sniffing, and network analysis (Documentation Link). ARP poisoning with Ettercap involves tricking the victim (Windows 10) and the gateway (e.g., router) into believing the attacker's machine (Kali) is the legitimate intermediary. Here's a breakdown:

1. **Network Scanning**
   (a) Ettercap scans the local network to identify devices and their IP/MAC addresses.
   (b) It detects the gateway (router) and the target victim (Windows 10).
2. **ARP Cache Poisoning**
   (a) Ettercap sends forged ARP replies to:
      i. The victim, claiming the attacker's MAC address belongs to the gateway.
      ii. The gateway, claiming the attacker's MAC address belongs to the victim.
   (b) This redirects all traffic between the victim and gateway through the attacker's machine.
3. **MITM Attack Execution**
   (a) Once the ARP tables are poisoned, Ettercap can:
      i. Sniff Traffic: Capture unencrypted data (e.g., HTTP, FTP, DNS queries).
      ii. Modify Packets: Inject malicious code or alter content in transit.
      iii. Session Hijack: Steal cookies or login sessions.

10.3. ARP Poisoning Attack Simulation

10.4. First, we have to get the victim's IP address and the default Gateway.

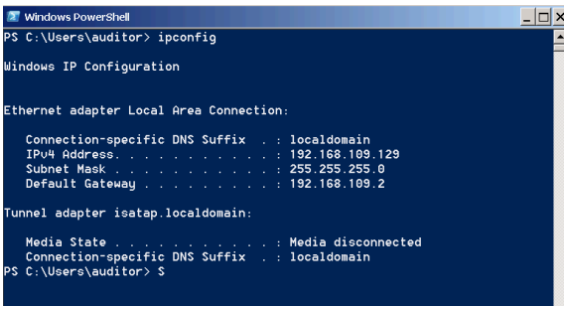

Figure 19. Victim's IP Address

10.4.1. Let's also display the arp cache table

As we can see, so far , the arp cache looks legitimate and contains the IP and the MAC address of the real Gateway which is the router in our case.

Figure 20. ARP Cache Table

10.4.2. The attacker's IP address

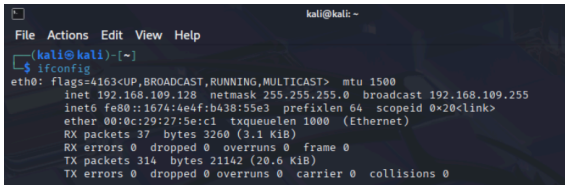

Figure 21. Attacker's IP Address

10.4.3. Now let's open Ettercap and list the hosts available on our network, using Scan for Hosts

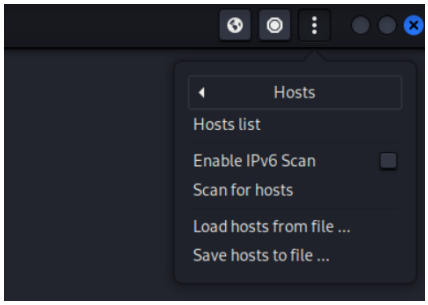

Figure 22. Scanning for Hosts

10.4.4. Hosts added to the list

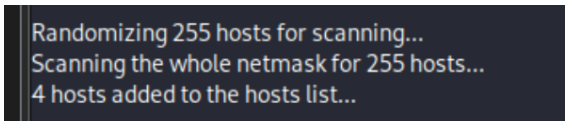

Figure 23. Added Lists 1

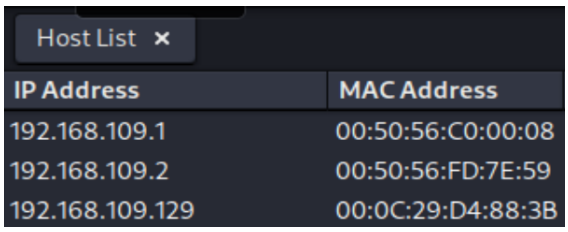

Figure 24. Added Lists 2

We successfully listed the victim's and the Gateway IPs. Now we add them to Target number 1 and 2 respectively.

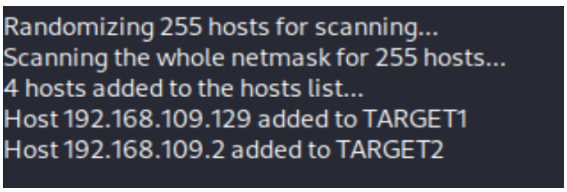

Figure 25. Victim's Gateway

10.4.5. Then, let's choose ARP Poisoning as our Man in the middle attack.

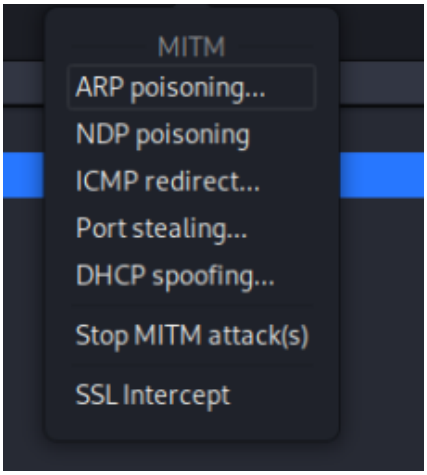

Figure 26. Choosing ARP Poisoning

And the attack starts:

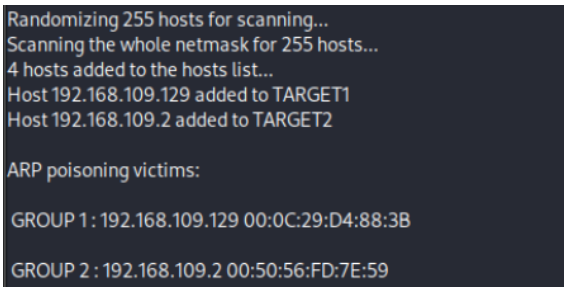

Figure 27. Attack Launched

10.4.6. Let's open Wireshark to see if the ARP packets have started

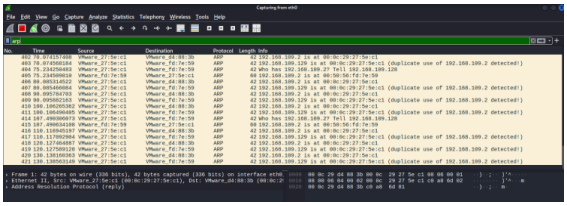

Figure 28. Wireshark

10.4.7. Now, let's check again the ARP cache table on our victim machine

Figure 29. e ARP cache table on our victim machine

As you can see, the default gateway now has the MAC address of the attacker machine which ends with c1 as we saw earlier.

This means that the attacker has tricked the victim (Windows 10) and the gateway (the router) into believing the attacker's machine (Kali) is the legitimate intermediary.

Now the attacker can execute one of the attacks listed above, let's test traffic sniffing while the ARP cache table is poisoned.

The victim navigates to http://testphp.vulnweb.com/login.php to log in. *This website uses HTTP and is intended for demonstration purposes only.*

Figure 30. demonstration purposes

10.4.8. And let's go back to the attacker machine and see the intercepted traffic.

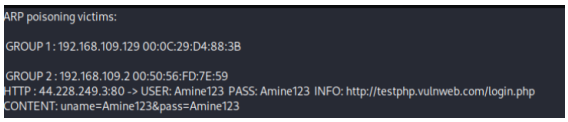

Figure 31. attacker machine and see the intercepted traffic

As shown, Ettercap intercepted the HTTP request and got the login credentials.

10.5. Risks and Detection

Signs of ARP Spoofing:

- Unusual network slowdowns.
- Duplicate IP-MAC entries in the ARP table (check using `arp -a` on Windows or `arp -vn` on Linux).

Detection Tools:

- **Wireshark:** Monitor ARP packets for anomalies.
- **XArp:** Actively detects ARP spoofing attempts.

11. NTLMv2 Hash Stealing and Cracking in a LAN Network Setup

This presentation outlines a demonstration of NTLMv2 hash stealing and password cracking in a controlled lab environment, showing how authentication credentials can be captured and compromised in a LAN local network.

Lab environment setup configuration:

- **Attacker Machine:** Kali Linux 2025 (Penetration Testing Distribution)
- **Target Machine:** Windows 7
- **Network Configuration:** Both machines connected to the same local network
- **Attack Scenario:** Man-in-the-middle attack to capture and crack authentication hashes.

11.1. Step 1: Initialize environment

The lab begins with both machines powered on VMware and connected to the same network. The Windows 7 machine represents a typical user workstation while Kali linux serves as the attacker's platform with pre-installed penetration testing tools.

11.2. Step 2: Deploying responder on Kali linux

Responder is executed on the Kali linux machine using the bash command: sudo responder -I eth1 -v

This launches Responder in verbose mode on the `eth1` network interface. Responder works by:

- Setting up rogue authentication servers
- Listening for all `LLMNR`, `NBT-NS`, and `mDNS` requests on the network
- Responding to these requests to capture authentication attempts

Figure 32. Setting up rogue authentication servers

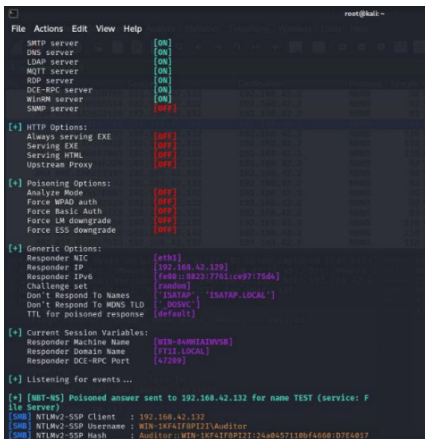

Figure 33. Setting up rogue authentication servers

11.3. Step 3: Triggering authentication on Windows 7

On the Windows 7 machine, an SMB authentication attempt is triggered by:

1. Opening Windows Explorer
2. Entering `\\test` in the address bar and pressing *Enter*

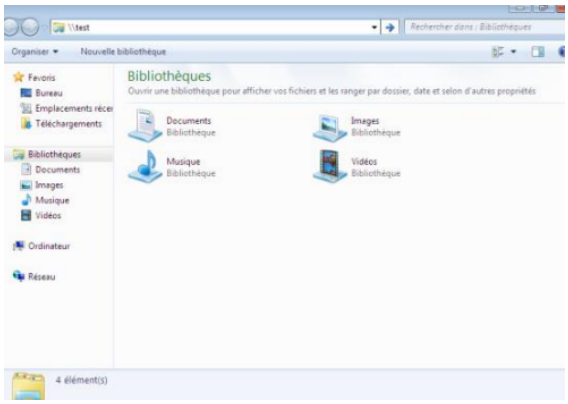

Figure 34. SMB authentication

This action causes Windows to attempt to connect to a non existent server, triggering LLMNR / NBT-NS name resolution requests 1.

11.4. Step 4: Capturing all NTLMv2 Hashes from Windows

When the Windows 7 machine attempts to connect to the non-existent `\\test` share:

1. It broadcasts a name resolution request.
2. Responder responds, pretending to be the requested server.
3. Windows 7 automatically attempts to authenticate.
4. Responder captures the NTLMv2 authentication hash during this process.

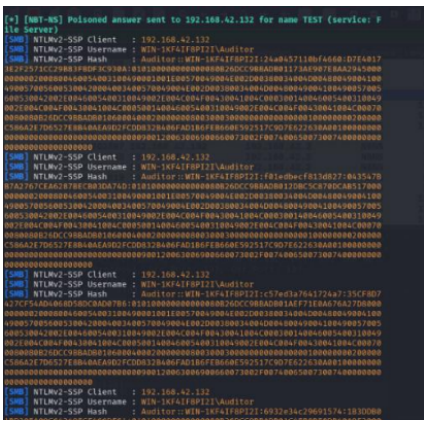

Figure 35. Machine attempts to connect to the non existent test share

The hash contains the username and an encrypted version of the password that can be attacked using password cracking tools.

11.5. Step 5: Viewing Captured Hashes

To verify the captured hashes, we list the Responder logs directory bash command: ls/usr/share/responder/logs.

Manual command to put hashes: vi hashes.txt after you have copied the NTLMv2 hash from the responder, paste this corner and them to quit :q! and press enter. This is area who this displays all captured hash files, confirming the successful interception of authentication attempts 2.

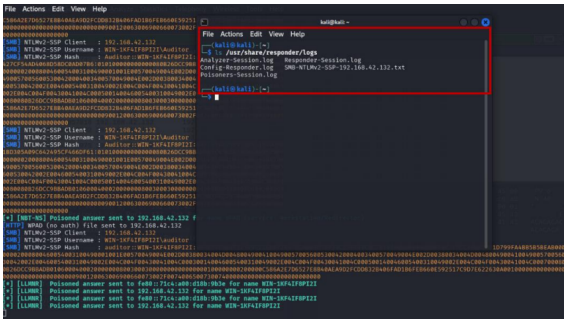

Figure 36. The captured hash files

11.6. Step 6: Examining Hash Contents

The hash file can be viewed using bash command line: cat /usr/share/responder/logs/SMB-NTLMv2-SSP-192.168.42.132.txt

This reveals the captured NTLMv2 hash containing:

- Username (`auditor`)
- Domain information
- Encrypted password challenge-response data

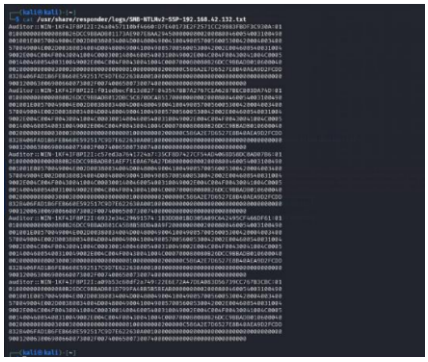

Figure 37. captured NTLMv2 hash

11.7. Step 7: Cracking the Password

John the Ripper is used to crack the captured hash: john/usr/share/responder/logs/SMB-NTLMv2-SSP-192.168.42.132.txt

This reveals the captured NTLMv2 hash containing:

- Username (`auditor`)
- Domain information
- Encrypted password challenge-response data

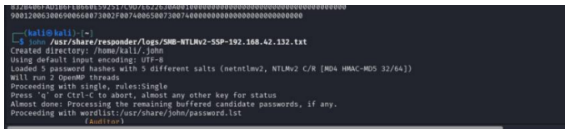

Figure 38. Password cracking process 1

Figure 39. Password cracking process 2

12. Security Implications

This is the demonstration feedback:

- How easily authentication credentials can be compromised on unsecured networks
- The vulnerability of the NTLM authentication protocol
- The importance of secure network configurations and modern authentication protocols

Here are some ways to reduce the impact:

- Disable LLMNR and NBT-NS in network settings
- Implement SMB signing
- Use strong, complex passwords
- Deploy modern authentication protocols like Kerberos
- Segment networks properly with access controls
- Monitor networks for suspicious activities like rogue authentication servers