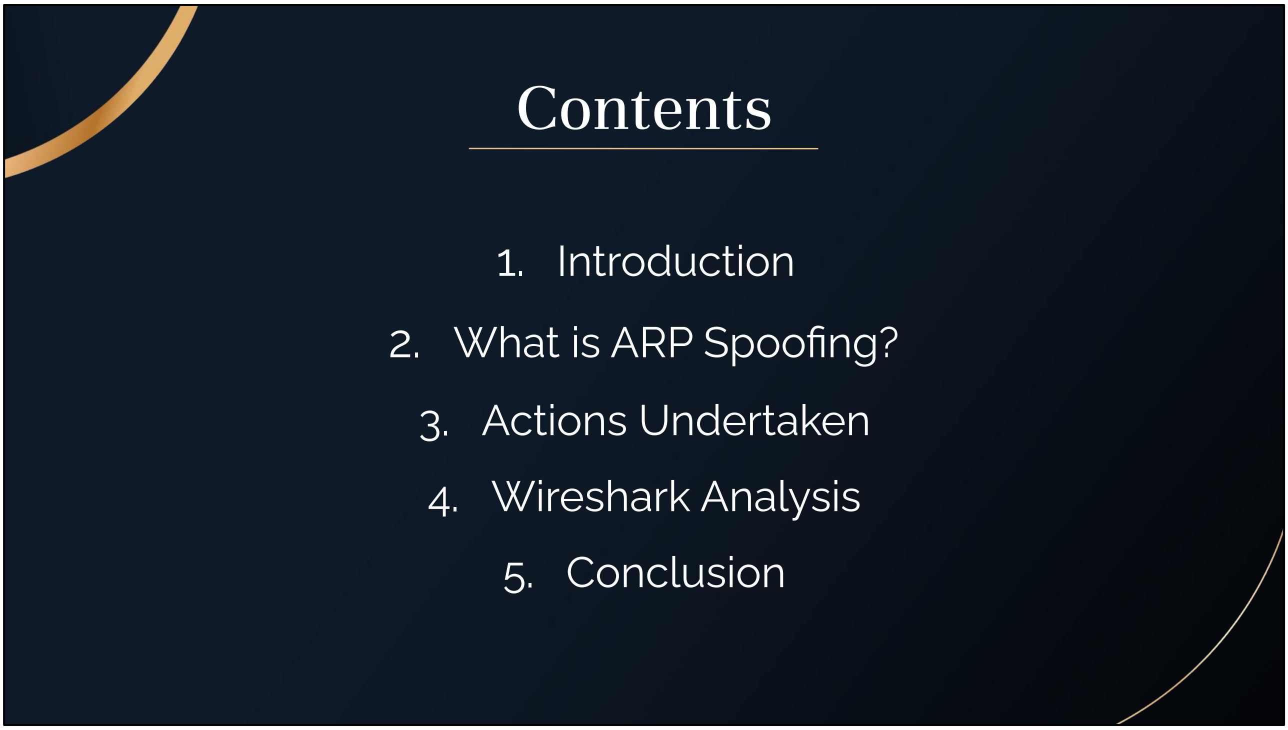
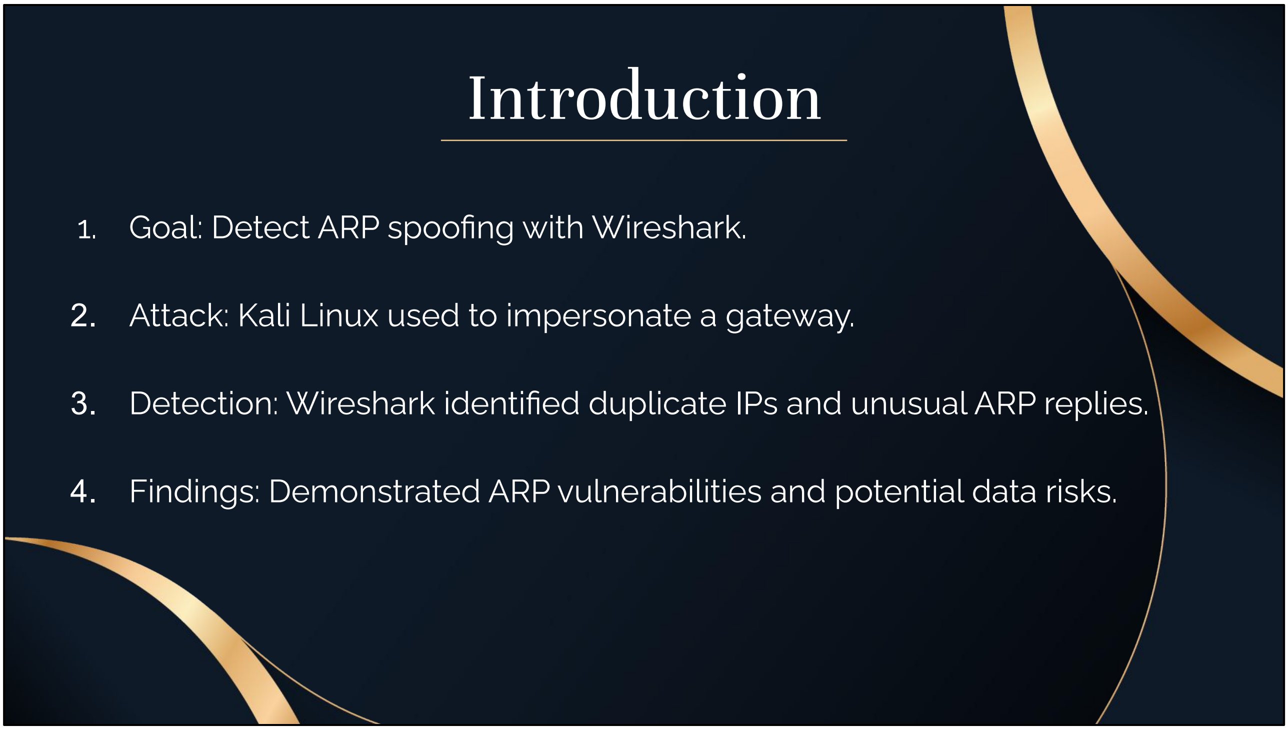
ARP Spoofing Attack in Wireshark

By George Knowles-Bacon



Contents

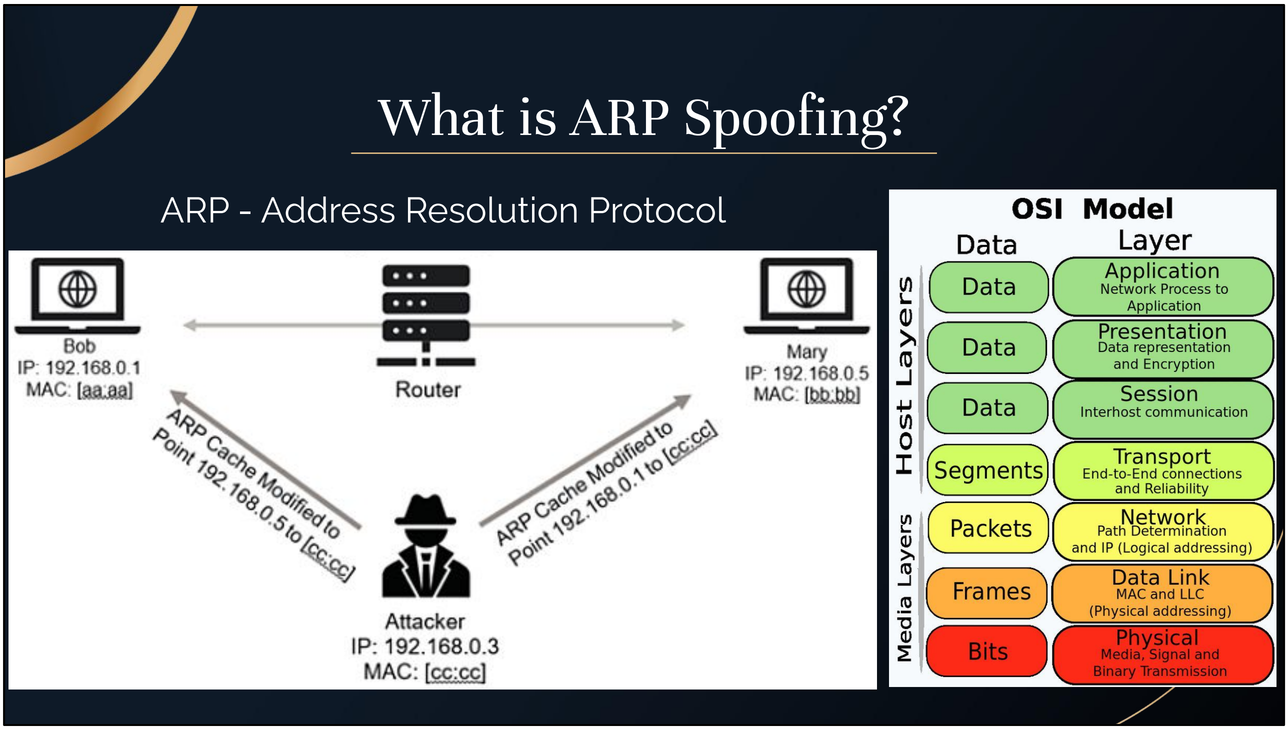
1. Introduction
2. What is ARP Spoofing?
3. Actions Undertaken
4. Wireshark Analysis
5. Conclusion



Introduction

1. Goal: Detect ARP spoofing with Wireshark.
2. Attack: Kali Linux used to impersonate a gateway.
3. Detection: Wireshark identified duplicate IPs and unusual ARP replies.
4. Findings: Demonstrated ARP vulnerabilities and potential data risks.

1. The objective was to identify signs of ARP spoofing, where a malicious device impersonates a legitimate network device (like a gateway) to intercept traffic.
2. Kali Linux was used to launch an ARP spoofing attack, where it sent fake ARP packets to the Windows 7 VM, making it believe Kali was the network gateway.
3. Wireshark captured unusual network activity, such as duplicate IP addresses and inconsistent ARP replies, indicating that ARP spoofing was occurring.
4. The results showed that ARP-based attacks can compromise network security, leading to risks like data interception, session hijacking, and unauthorized access.



What is ARP Spoofing?

ARP - Address Resolution Protocol

OSI Model

	Data	Layer
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data representation and Encryption
	Data	Session Interhost communication
	Segments	Transport End-to-End connections and Reliability
Media Layers	Packets	Network Path Determination and IP (Logical addressing)
	Frames	Data Link MAC and LLC (Physical addressing)
	Bits	Physical Media, Signal and Binary Transmission

Lets begin with - ARP stands for Address Resolution Protocol. It is a crucial networking protocol that maps IP addresses (Layer 3) to MAC addresses (Layer 2) within a local area network (LAN), enabling devices to communicate effectively.

ARP spoofing attacks, is also known as ARP poisoning. It involves an attacker sending false ARP messages to associate their MAC address with a legitimate IP address, leading to various malicious activities like man-in-the-middle attacks, session hijacking, and denial-of-service. Over 50% of local network attacks involve ARP spoofing.

Now remember, ARP Spoofing happens at Layer 2 the Data Link Layer of the OSI model.

We need to understand why the protocol sends requests - ARP cache stores a table of IP addresses to MAC addresses for devices on a local network (Like an address book).
When a device needs to send data, it checks the ARP cache for the destination MAC address. If not found, it sends an ARP request to discover it. This process improves network efficiency by reducing the need for repeated address lookups.

Normal ARP works by helping devices on a LAN find out which MAC address belongs to which IP address.

When one computer wants to talk to another, it sends an ARP request asking, "Who

has this IP address?"
The correct device responds with an ARP reply, saying "That IP address belongs to this MAC address."

During ARP Spoofing (the attack) - A hacker tricks devices into sending data to the wrong MAC address. Therefore, the attacker sends fake ARP replies on the network. These fake replies tell victims that "The attacker's MAC address belongs to the router's IP address."

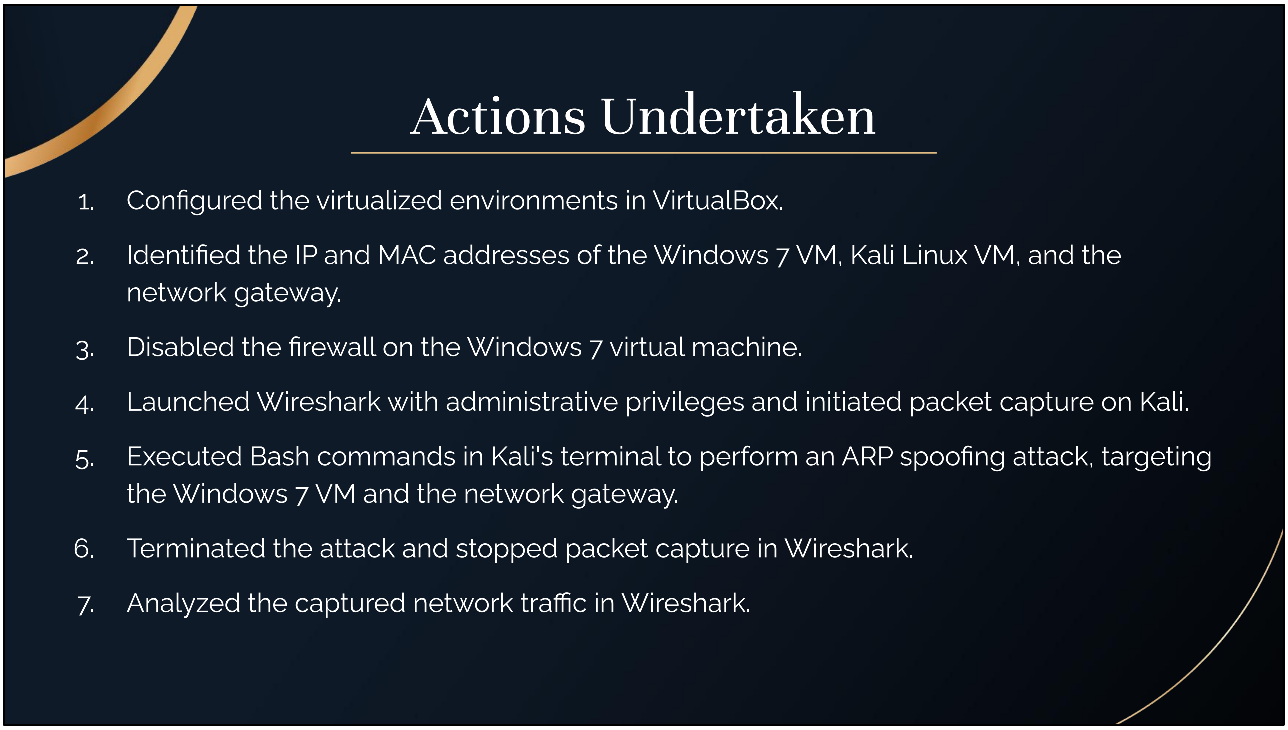
So instead of sending traffic to the real router, the victims unknowingly send data to the attacker first. The attacker can therefore, Intercept and read the data, Modify the data before sending it to the real router (Man-in-the-Middle attack), Completely block the victim's connection (Denial of Service - DoS) or do them all at once

Speed & Detection

It can take Seconds to minutes to spoof with tools like arpspoof or etterCAP. However, if no monitoring tools are in place it could take Hours to days for the spoof to be detected.

Defense & Prevention

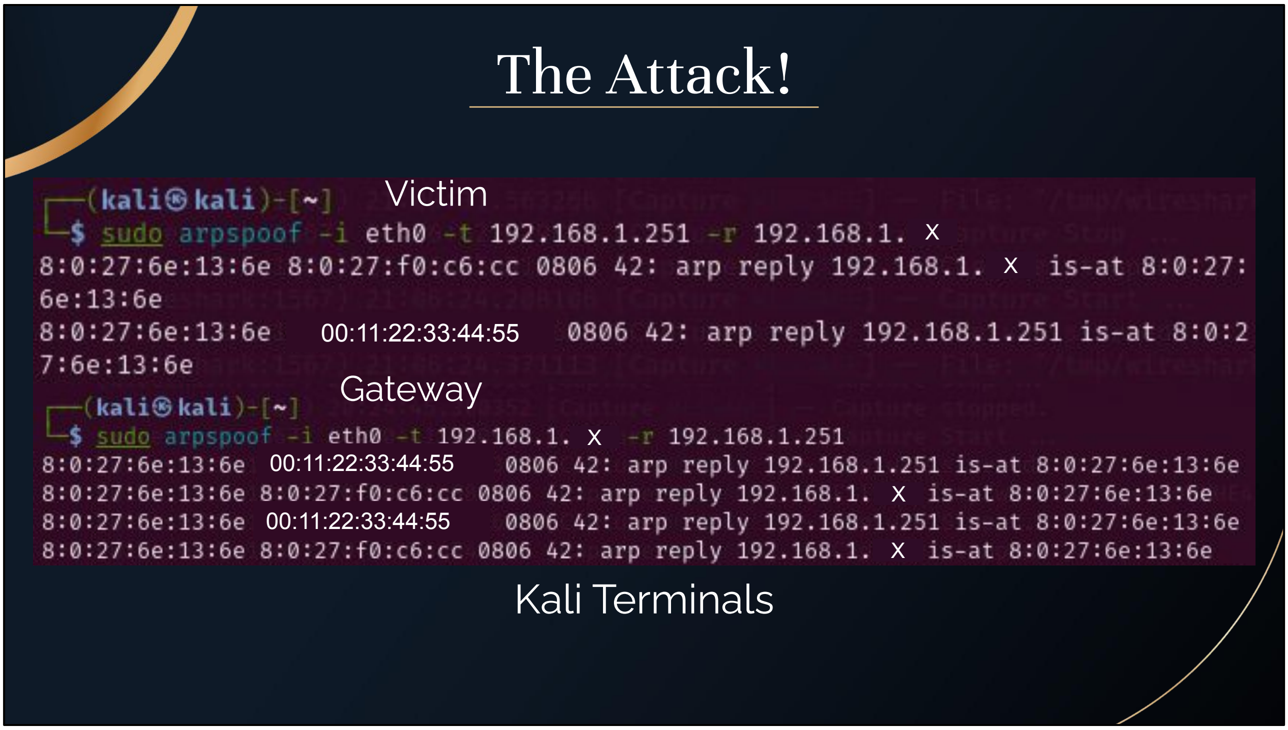
Static ARP entries – Blocks 90% of attacks.
Dynamic ARP Inspection (DAI) – Stops nearly 100% of spoofing on managed switches.
VPNs & HTTPS – Protect sensitive data even if spoofing occurs.



Actions Undertaken

1. Configured the virtualized environments in VirtualBox.
2. Identified the IP and MAC addresses of the Windows 7 VM, Kali Linux VM, and the network gateway.
3. Disabled the firewall on the Windows 7 virtual machine.
4. Launched Wireshark with administrative privileges and initiated packet capture on Kali.
5. Executed Bash commands in Kali's terminal to perform an ARP spoofing attack, targeting the Windows 7 VM and the network gateway.
6. Terminated the attack and stopped packet capture in Wireshark.
7. Analyzed the captured network traffic in Wireshark.

1. I set up a Windows 7 VM and configured both Windows 7 and Kali to use a Bridged Adapter in VirtualBox.
2. Running ipconfig in win7 and ifconfig in kali I found the ip and mac addresses for both machines and the gateway in both
3. When Kali couldn't ping the target, I suspected the firewall was blocking traffic. Disabling it allowed all ARP packets through, revealing the attack process.
4. I then launched Wireshark as admin using: - sudo wireshark
5. See next slides
6. See next slides



The Attack!

Victim

```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -t 192.168.1.251 -r 192.168.1. X
8:0:27:6e:13:6e 8:0:27:f0:c6:cc 0806 42: arp reply 192.168.1. X  is-at 8:0:27:
6e:13:6e
8:0:27:6e:13:6e    00:11:22:33:44:55    0806 42: arp reply 192.168.1.251 is-at 8:0:2
7:6e:13:6e
```

Gateway

```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -t 192.168.1. X  -r 192.168.1.251
8:0:27:6e:13:6e  00:11:22:33:44:55    0806 42: arp reply 192.168.1.251 is-at 8:0:27:6e:13:6e
8:0:27:6e:13:6e 8:0:27:f0:c6:cc 0806 42: arp reply 192.168.1.  X  is-at 8:0:27:6e:13:6e
8:0:27:6e:13:6e  00:11:22:33:44:55    0806 42: arp reply 192.168.1.251 is-at 8:0:27:6e:13:6e
8:0:27:6e:13:6e 8:0:27:f0:c6:cc 0806 42: arp reply 192.168.1.  X  is-at 8:0:27:6e:13:6e
```

Kali Terminals

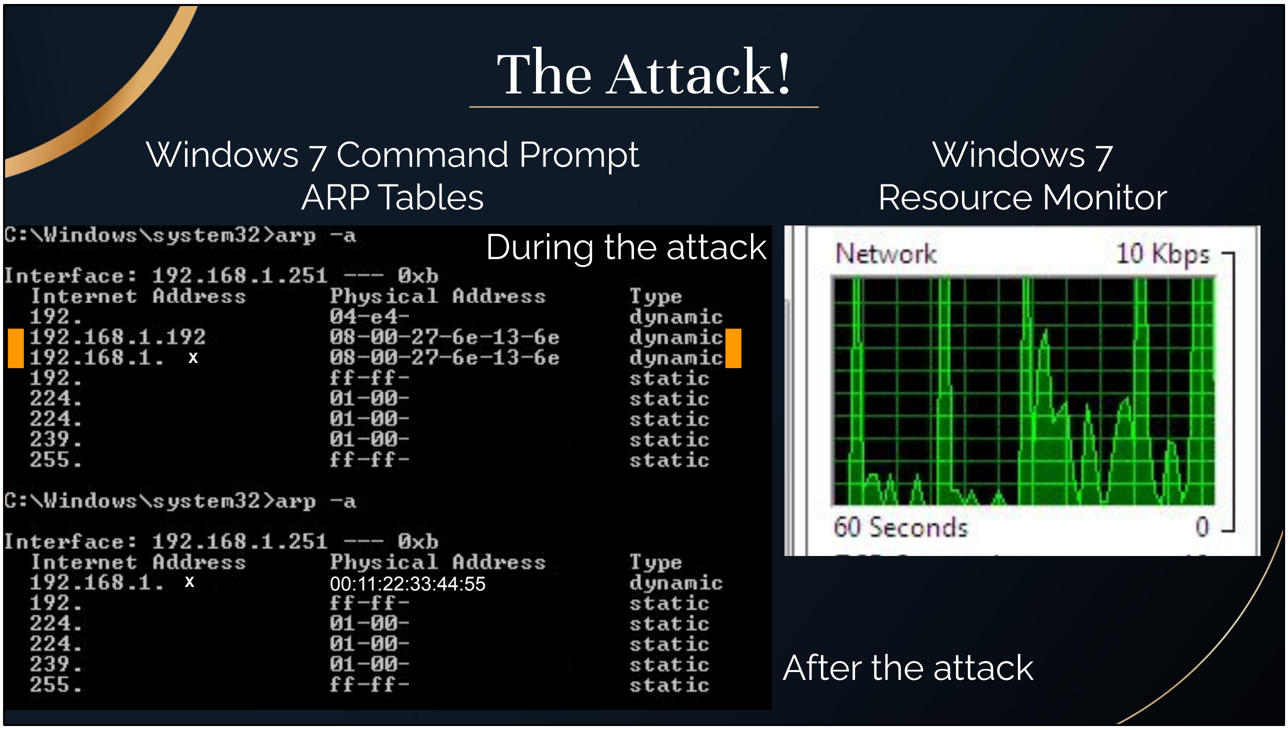
Kali Linux is the attacker

Here you can see I used two separate terminals to run the bash commands to trigger the attack which I did for around 15 minutes. Then I pressed ctrl + c to terminate the running commands. Let’s explain what the commands mean:

- sudo: Runs the command with superuser (root) privileges.
- arpspoof: The tool used to send fake ARP (Address Resolution Protocol) messages. -
- -i eth0: Specifies the network interface (eth0).
- -t 192.168.1.251: Target device (victim's IP address).
- -r 192.168.1.X: Gateway (router) IP address.
-
- This command spoofs the ARP table of the victim (192.168.1.251), making it believe that the attacker's MAC address is the gateway (192.168.1.X).
- As a result, the victim will send its traffic through the attacker's machine.
-
- Similar to the first command but in reverse.
- -t 192.168.1.X: Targets the gateway (router).
- -r 192.168.1.251: Spoofs the victim's IP.
-

  This spoofs the ARP table of the router, making it believe the attacker's MAC address is the victim (192.168.1.251). Now, both the victim and the gateway

- are sending packets through the attacker.
-
- The attacker is using the arpspoof command to trick two devices on the network (the victim and the gateway/router) into thinking the attacker's computer is the legitimate communication partner.



The Attack!

Windows 7 Command Prompt
ARP Tables

During the attack

```
C:\Windows\system32>arp -a

Interface: 192.168.1.251 --- 0xb
  Internet Address      Physical Address      Type
  192.                  04-e4-                dynamic
  192.168.1.192         08-00-27-6e-13-6e     dynamic
  192.168.1.  x         08-00-27-6e-13-6e     dynamic
  192.                  ff-ff-                static
  224.                  01-00-                static
  224.                  01-00-                static
  239.                  01-00-                static
  255.                  ff-ff-                static

C:\Windows\system32>arp -a

Interface: 192.168.1.251 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.  x         00:11:22:33:44:55     dynamic
  192.                  ff-ff-                static
  224.                  01-00-                static
  224.                  01-00-                static
  239.                  01-00-                static
  255.                  ff-ff-                static
```

Windows 7
Resource Monitor

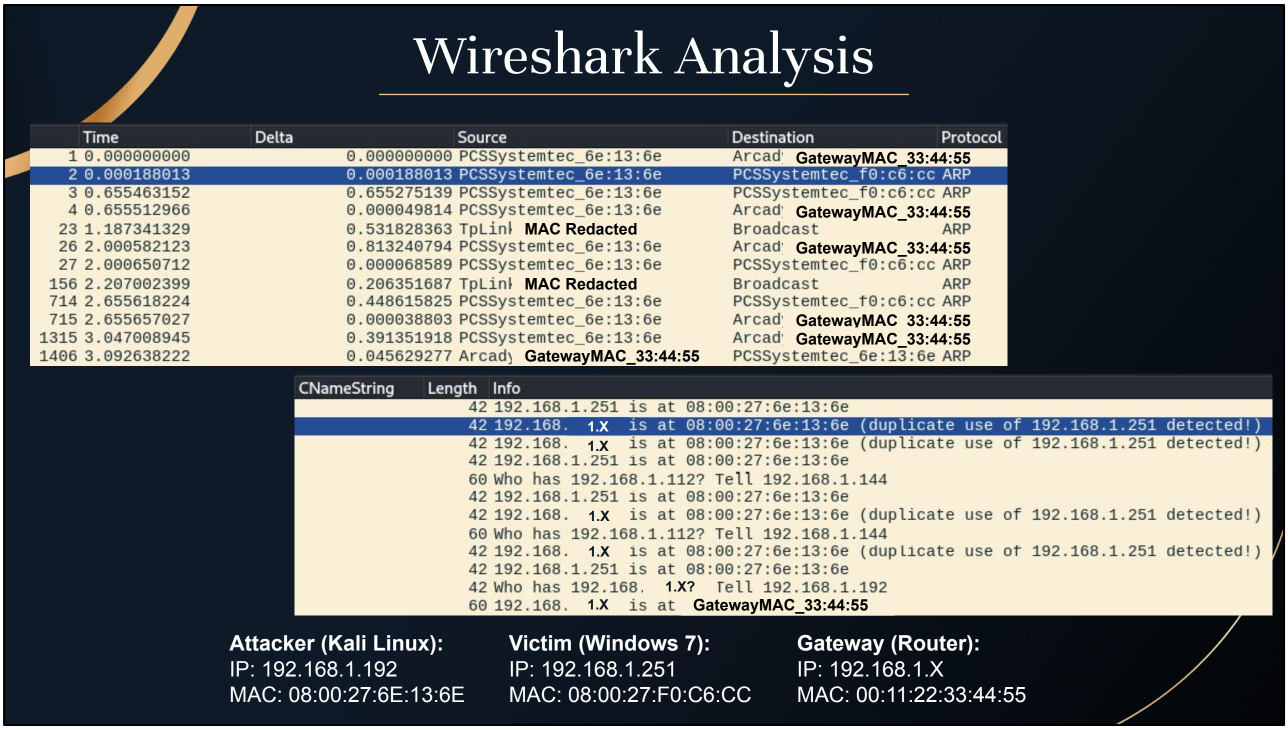
After the attack

Victim's computer (Windows 7)

- The Windows 7 computer is being tricked into sending data to the attacker instead of the real router.
- The Command Prompt (arp -a) shows changes in MAC addresses, proving the attack is working.
- Static ARP entries are manually configured mappings of IP addresses to MAC addresses, ensuring reliable communication by preventing dynamic ARP entries from overwriting or aging out, and are useful for troubleshooting, security, and specific network configuration

Network Disruption & Traffic Monitoring

- The Windows 7 Resource Monitor shows network activity spikes, caused by intercepted or rerouted traffic.



Wireshark Analysis

```
     Time                      Delta                   Source                    Destination                Protocol
   1 0.000000000               0.000000000 PCSSystemtec_6e:13:6e     Arcad  GatewayMAC_33:44:55
   2 0.000188013               0.000188013 PCSSystemtec_6e:13:6e     PCSSystemtec_f0:c6:cc ARP
   3 0.655463152               0.655275139 PCSSystemtec_6e:13:6e     PCSSystemtec_f0:c6:cc ARP
   4 0.655512966               0.000049814 PCSSystemtec_6e:13:6e     Arcad  GatewayMAC_33:44:55
  23 1.187341329               0.531828363 TpLin  MAC Redacted       Broadcast             ARP
  26 2.000582123               0.813240794 PCSSystemtec_6e:13:6e     Arcad  GatewayMAC_33:44:55
  27 2.000650712               0.000068589 PCSSystemtec_6e:13:6e     PCSSystemtec_f0:c6:cc ARP
 156 2.207002399               0.206351687 TpLin  MAC Redacted       Broadcast             ARP
 714 2.655618224               0.448615825 PCSSystemtec_6e:13:6e     PCSSystemtec_f0:c6:cc ARP
 715 2.655657027               0.000038803 PCSSystemtec_6e:13:6e     Arcad  GatewayMAC 33:44:55
1315 3.047008945               0.391351918 PCSSystemtec_6e:13:6e     Arcad  GatewayMAC_33:44:55
1406 3.092638222               0.045629277 Arcad  GatewayMAC_33:44:55   PCSSystemtec_6e:13:6e ARP
```

```
CNameString    Length  Info
                    42 192.168.1.251 is at 08:00:27:6e:13:6e
                    42 192.168.  1.X  is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.251 detected!)
                    42 192.168.  1.X  is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.251 detected!)
                    42 192.168.1.251 is at 08:00:27:6e:13:6e
                    60 Who has 192.168.1.112? Tell 192.168.1.144
                    42 192.168.1.251 is at 08:00:27:6e:13:6e
                    42 192.168.  1.X  is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.251 detected!)
                    60 Who has 192.168.1.112? Tell 192.168.1.144
                    42 192.168.  1.X  is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.251 detected!)
                    42 192.168.1.251 is at 08:00:27:6e:13:6e
                    42 Who has 192.168.  1.X?  Tell 192.168.1.192
                    60 192.168.  1.X  is at  GatewayMAC_33:44:55
```

Attacker (Kali Linux):
IP: 192.168.1.192
MAC: 08:00:27:6E:13:6E

Victim (Windows 7):
IP: 192.168.1.251
MAC: 08:00:27:F0:C6:CC

Gateway (Router):
IP: 192.168.1.X
MAC: 00:11:22:33:44:55

Here we analyse an ARP spoofing attack using Wireshark. This screenshot provides evidence of ARP poisoning.

- I used the filter ‘arp’ to see all the ARP requests and replies you can also use other filters.

Looking at the capture, we see multiple ARP packets where the same IP address is associated with different MAC addresses. This is a clear indication of ARP spoofing."

- 192.168.1.251 (which belongs to the victim, Windows 7) is falsely claimed by the attacker.
- 192.168.1.X (the gateway) is also being spoofed.
- This results in network confusion, where traffic meant for the victim or gateway is redirected through the attacker.

Key Evidence in the Capture
Now, let’s focus on specific details in the packet capture.

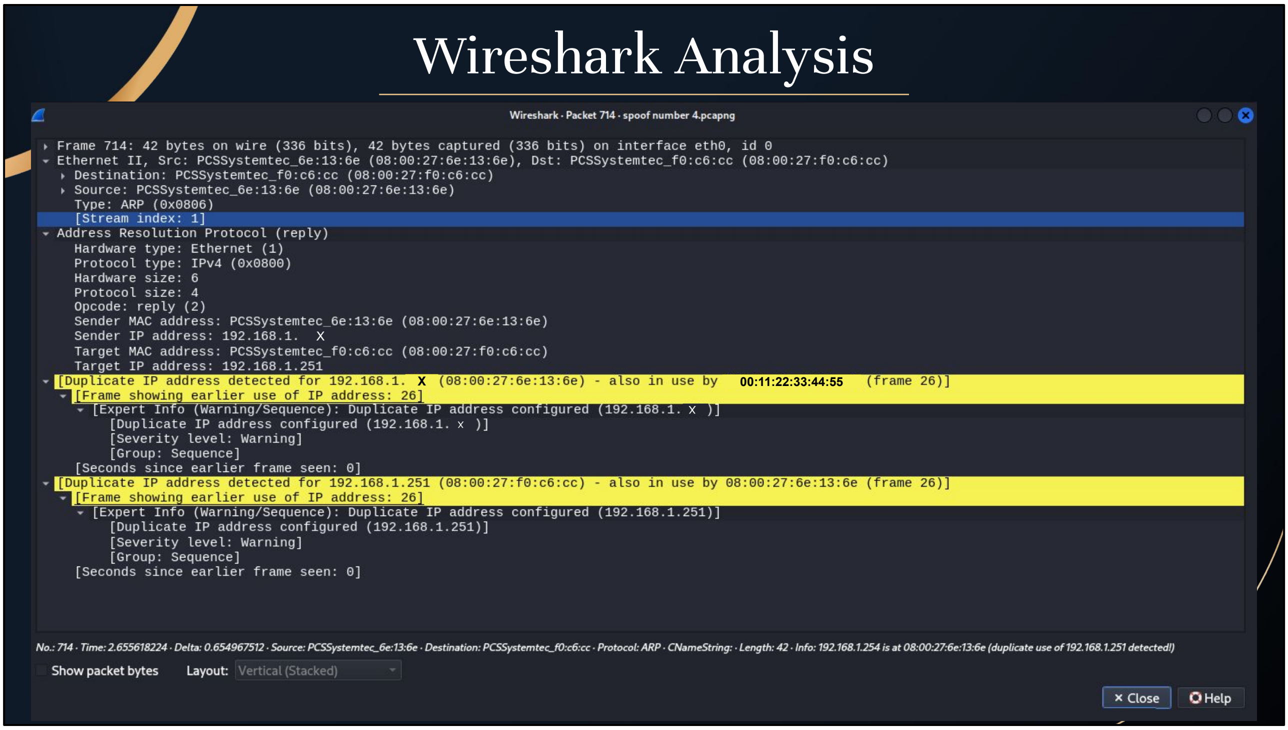
- The source MAC address 08:00:27:6E:13:6E appears frequently, falsely responding as both 192.168.1.251 and 192.168.1.X.
- Wireshark flags “Duplicate use of 192.168.1.251 detected”, confirming the presence of conflicting ARP replies.
- Some packets ask “Who has 192.168.1.X?”, meaning devices are trying to resolve the gateway’s IP but are getting manipulated responses.

- Sensitive data theft – The attacker can intercept usernames, passwords, or personal information.
- Denial of Service (DoS) – The network may become unreliable if devices keep losing connection.
- Session Hijacking – The attacker could take over active network sessions by injecting malicious data.

Evidence from Wireshark Capture

Key Observations:

1. Duplicate IP Conflict Detected:
    - Wireshark flags duplicate usage of 192.168.1.251, indicating a spoofing attempt.
2. ARP Replies from the Attacker (08:00:27:6E:13:6E):
    - Claims that 192.168.1.251 belongs to its MAC address.
    - Misleads other devices into sending packets to the attacker instead of the real victim.
3. Frequent ARP Broadcasts & Who-has Requests:
    - ARP packets targeting the gateway and other devices, indicating possible further poisoning attempts.



Wireshark Analysis

Wireshark · Packet 714 · spoof number 4.pcapng

```
▸ Frame 714: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▾ Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e), Dst: PCSSystemtec_f0:c6:cc (08:00:27:f0:c6:cc)
  ▸ Destination: PCSSystemtec_f0:c6:cc (08:00:27:f0:c6:cc)
  ▸ Source: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
    Type: ARP (0x0806)
    [Stream index: 1]
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PCSSystemtec_6e:13:6e (08:00:27:6e:13:6e)
    Sender IP address: 192.168.1.  X
    Target MAC address: PCSSystemtec_f0:c6:cc (08:00:27:f0:c6:cc)
    Target IP address: 192.168.1.251
▾ [Duplicate IP address detected for 192.168.1.  X  (08:00:27:6e:13:6e) - also in use by   00:11:22:33:44:55   (frame 26)]
  ▾ [Frame showing earlier use of IP address: 26]
    ▾ [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.1. x  )]
        [Duplicate IP address configured (192.168.1. x  )]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 0]
▾ [Duplicate IP address detected for 192.168.1.251 (08:00:27:f0:c6:cc) - also in use by 08:00:27:6e:13:6e (frame 26)]
  ▾ [Frame showing earlier use of IP address: 26]
    ▾ [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.1.251)]
        [Duplicate IP address configured (192.168.1.251)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 0]
```

No.: 714 · Time: 2.655618224 · Delta: 0.654967512 · Source: PCSSystemtec_6e:13:6e · Destination: PCSSystemtec_f0:c6:cc · Protocol: ARP · CNameString: · Length: 42 · Info: 192.168.1.254 is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.251 detected!)

□ Show packet bytes   Layout: Vertical (Stacked)

- Here is the expanded view of the packet 714 which reveals an ARP poisoning attack in progress.
- Wireshark identifies 192.168.1.251 and 192.168.1.X as being used by multiple MAC addresses.
- This is an indication of ARP spoofing, where the attacker is claiming to be both the victim and the gateway.
- As a result, network traffic intended for legitimate devices is redirected to the attacker.

In ARP Replies

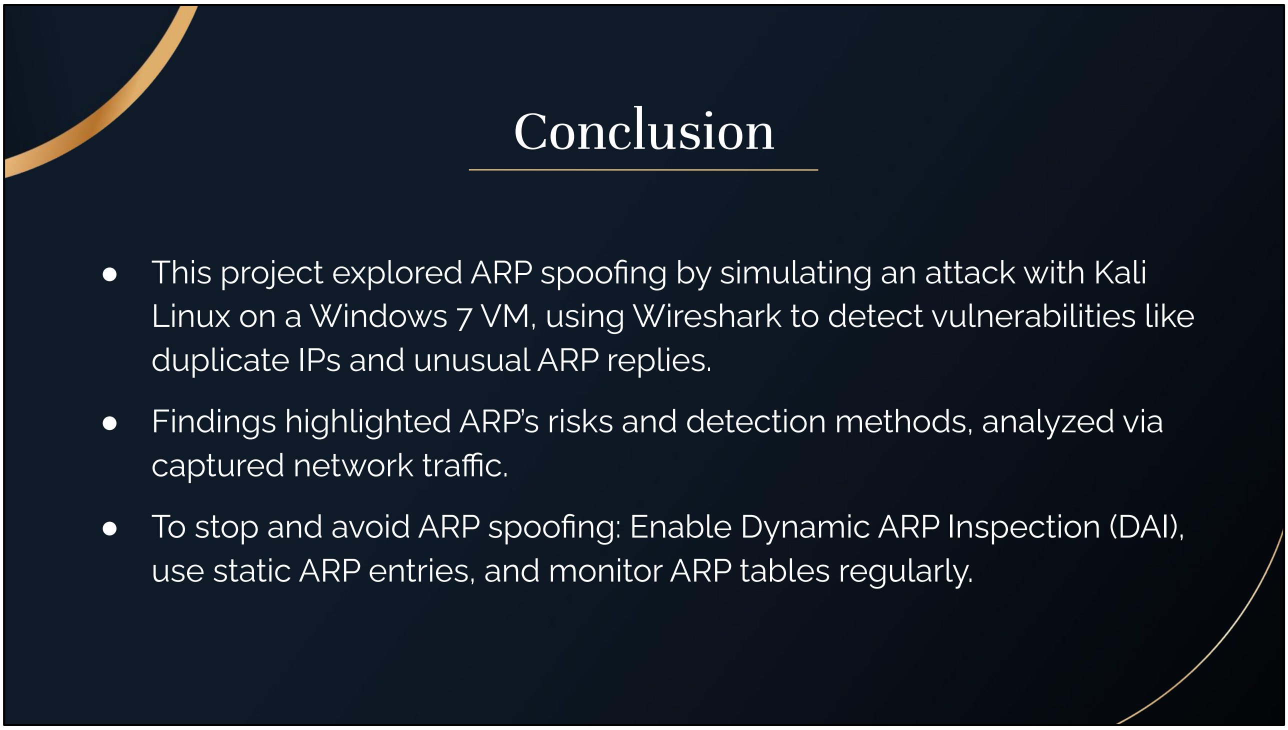
- The attacker's MAC 08:00:27:6E:13:6E is falsely claiming ownership of:
  - 192.168.1.251 (Victim)
  - 192.168.1.X (Gateway)
- This allows the attacker to intercept and manipulate network traffic.

Frame 26 – Initial Spoofing Attempt

- Wireshark traces the first occurrence of duplicate IP usage back to Frame 26.
- This means the attack began at this frame, and all subsequent packets reflect the impact of ARP poisoning.

Here is where you would find and see the Impact of a full Attack by being able to view Sensitive data such as passwords and usernames.

- The attacker successfully impersonated both the victim and the gateway.
- Proper network security measures can help detect and mitigate these threats.



Conclusion

- This project explored ARP spoofing by simulating an attack with Kali Linux on a Windows 7 VM, using Wireshark to detect vulnerabilities like duplicate IPs and unusual ARP replies.
- Findings highlighted ARP's risks and detection methods, analyzed via captured network traffic.
- To stop and avoid ARP spoofing: Enable Dynamic ARP Inspection (DAI), use static ARP entries, and monitor ARP tables regularly.

To summarise, I examined ARP spoofing, a cyberattack in which an attacker manipulates ARP tables to intercept or alter network traffic.

Using a virtualized environment with Windows 7 and Kali Linux, I executed an ARP spoofing attack and conducted a packet analysis in Wireshark.

The findings highlighted key indicators such as duplicate IP addresses and irregular ARP replies, demonstrating the vulnerabilities embedded in the ARP protocol.

To prevent ARP spoofing, organizations should implement Dynamic ARP Inspection, use static ARP entries, and monitor ARP tables (arp -a which I do recommend everyone to try and keep an eye on). Encrypting communications with HTTPS, SSH, or VPNs further reduces risks.

Understanding and mitigating ARP spoofing is essential for maintaining secure networks.

And Thank You for Being SPOOFED!