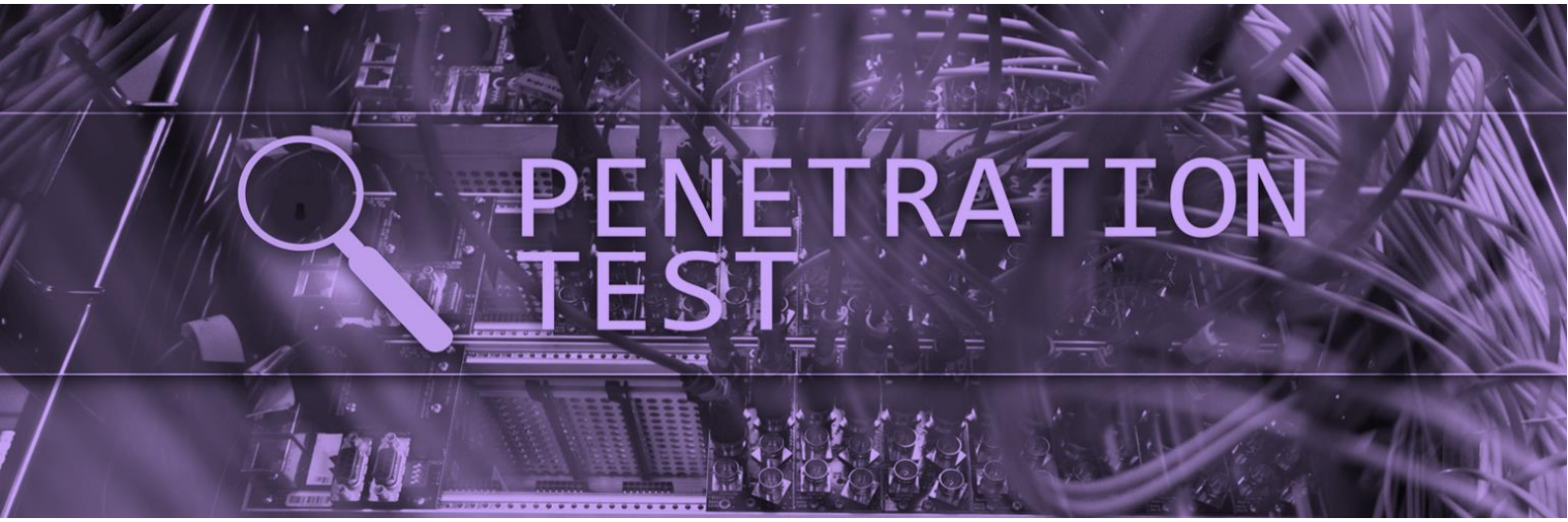
LIFARS
your digital world, secured

Case Study–
NAC bypass & ARP spoofing



To ensure the effectiveness of our client's security implementations LIFARS frequently conducts penetration tests evaluating their systems can hold up to real world scenarios and stay resilient. Our cyber resiliency experts deliver calculated attacks against systems the same way black hat hackers.

In December, our client requested that LIFARS Pen Testing Team perform an internal black box penetration test as part of a due diligence exercise. The client, an international financial organization with over 10000 employees and 500 IPv4 addresses, understands the risks they face on a daily basis and the importance of meeting compliance standards. Therefore, this client requested an external black box penetration test on their network.

The intent of this assessment was to identify weaknesses in the company's internet facing infrastructure and to detail how these vulnerabilities could impact the organization.

Therefore, the team used ARP poisoning as a main target for mounting other attacks, such as Man-in-the-middle (MiTM). This security testing effort was conducted with emphasis on the actual state of the systems examined and no documentation to the client was provided.

Note: All information in this case study has been modified to maintain confidentiality of our client

PENETRATION TESTING PHASES

There are various methodologies and approaches that can be used during penetration testing. LIFARS Pen Testing Team, follows the Penetration Testing Execution Standard (PTES) as the basis for penetration testing execution. The main phases of PTES are listed below.

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

KEY FINDINGS

While conducting the penetration test, we discovered that the client network had implemented Network access control (NAC). This solution is often used on corporate networks to prevent unauthorized hosts from accessing internally systems and services.

Bypassing Network Access Control

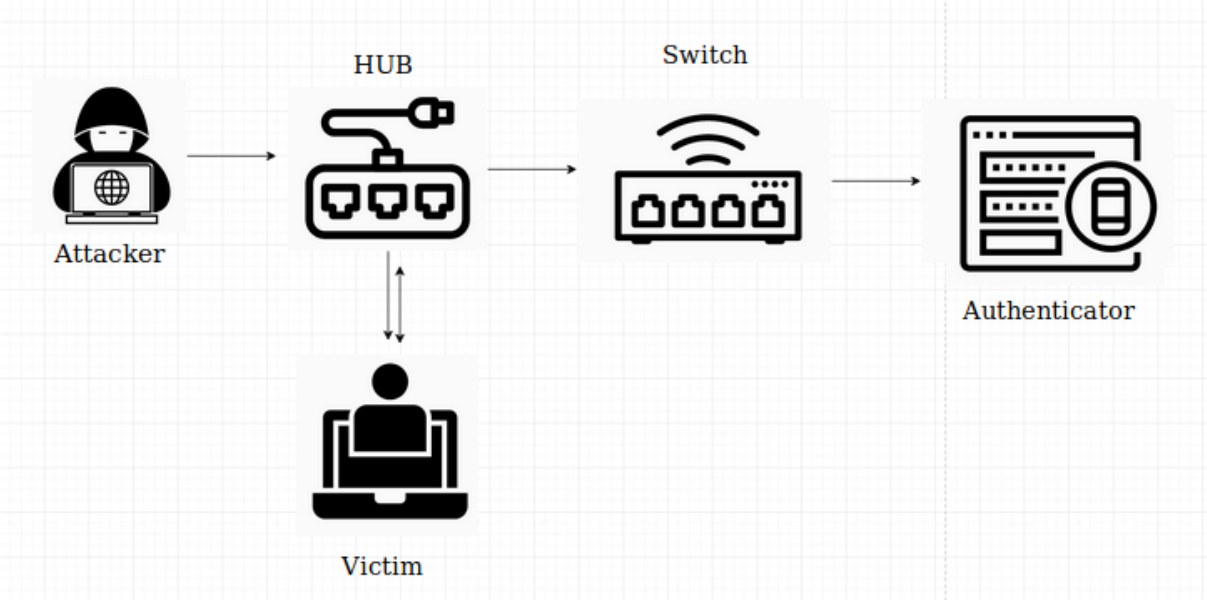


Figure 1 NAC Bypass scheme (incogbyte.github.io)

Hardware Used

100 Mb Hub – multiport repeater and PoE injector

Steps to reproduce NAC bypass:

1. First, we had to find an authenticated host and connect it to our hub. As we have PoE injector, we can also connect to VoIP Phone and PC.

2. After that, we connected to the hub, and start intercepting ARP frames to identify the valid host MAC address.

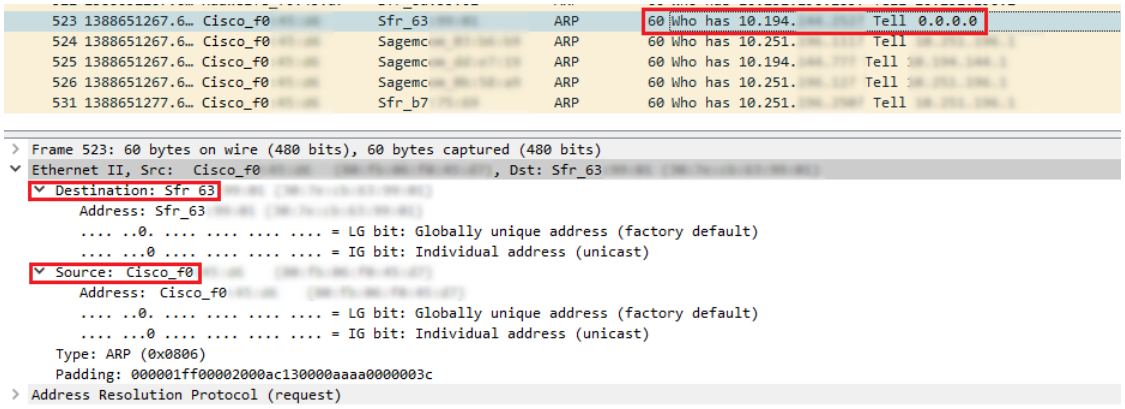


Figure 2 IP & MAC address of the victim

3. At this point, we can connect the hub to the switch, and we wait for Victim authentication.

4. After successful authentication, we cloned the valid MAC and IP address and connect to HUB. Now the switch does not recognize the difference between the attacker and the PC client.

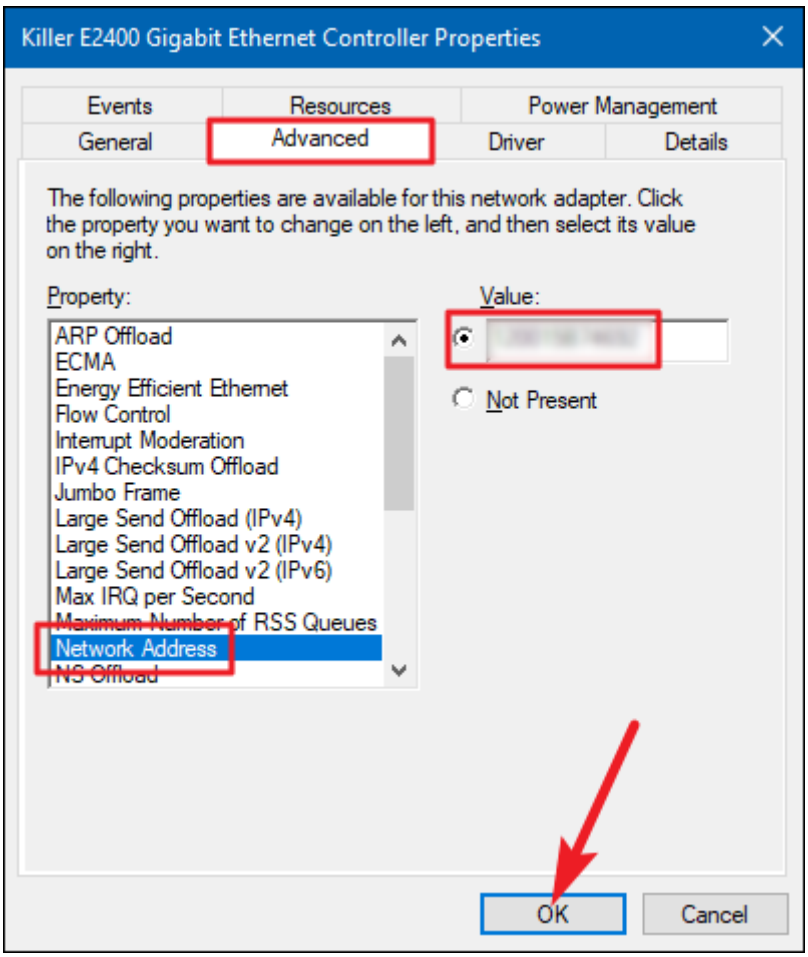


Figure 3 MAC address change

ARP Spoofing

ARP poisoning is when an attacker sends false ARP messages over a local area network to link an attacker's MAC address with the IP address of a legitimate computer or server on the network.

Once the attacker's MAC address is linked to an authentic IP address, the attacker can receive anything directed to the legitimate MAC address. As a result, the attacker can make an Man-in-the-middle attack (MiTM).

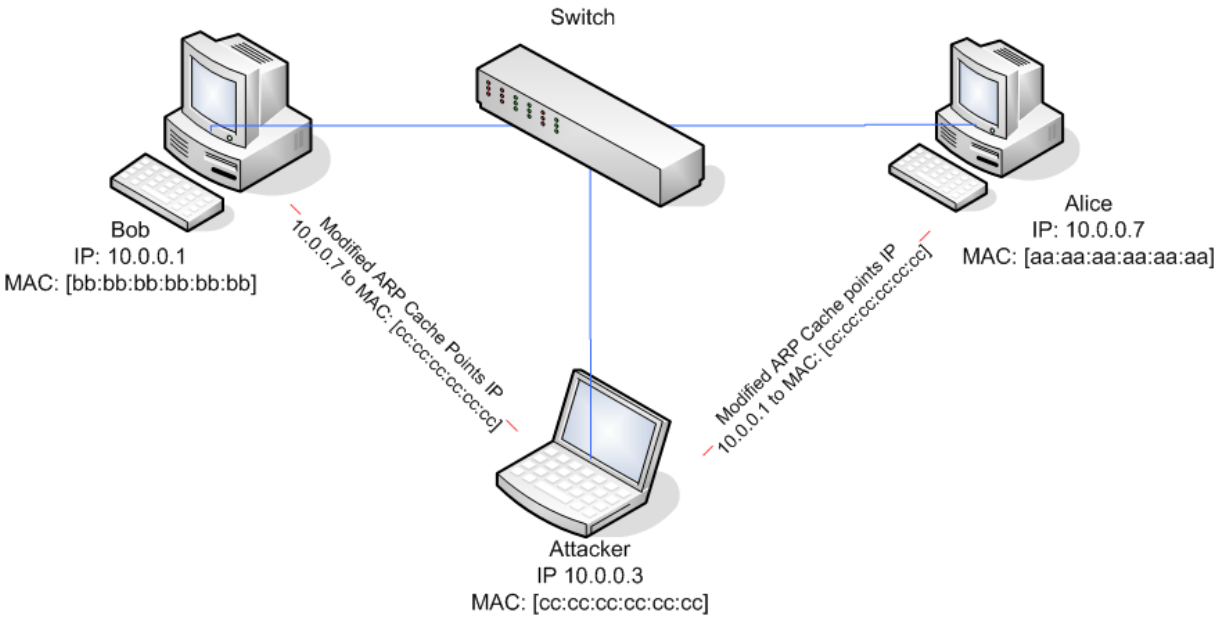
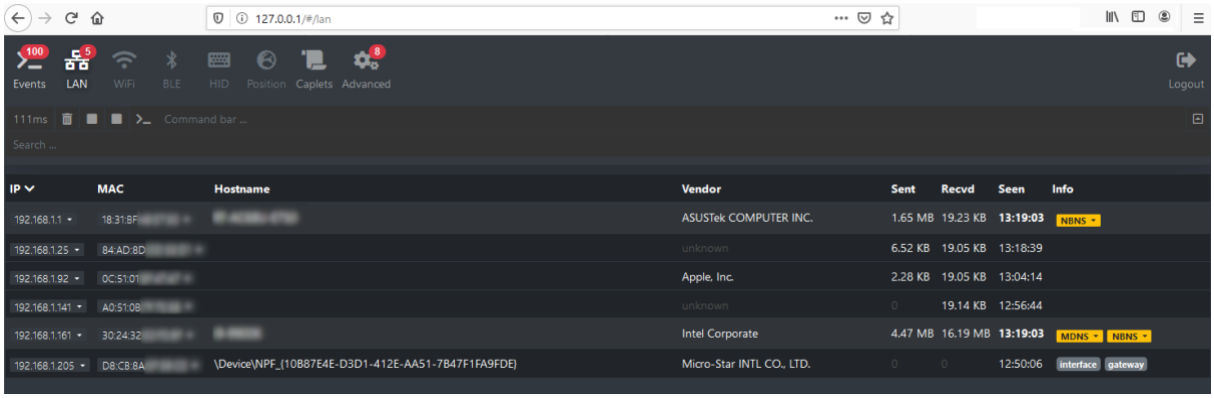


Figure 4 Representation of ARP spoofing

We have used bettercap on Windows to launch an ARP spoofing attack.

Steps to reproduce ARP spoofing attack:

1. We need to scan the network for all hosts, using module **net.recon** and **net.probe**.

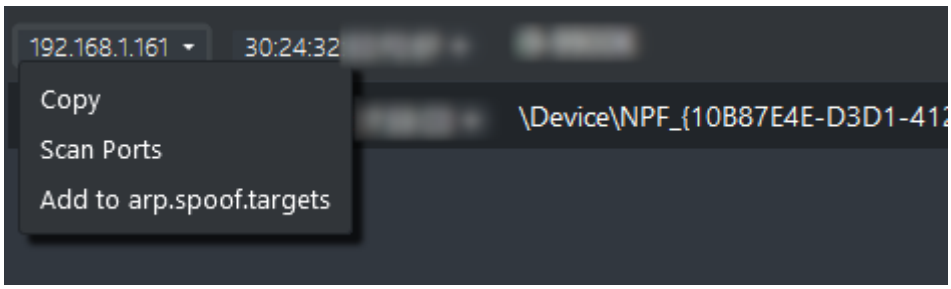


2. With this newly obtained set of hosts, we can choose which specific host we want to target. We can either use the console command or the GUI to execute this.

   From the console command we can type in the cmdlet:

   `Set arp.spoof.targets TARGET  IP`

   From the GUI we can go to the IP address on the left corner, in this case it is *192.168.1.161*. From the pull down menu, we can then choose *add to arp.spoof.targets*



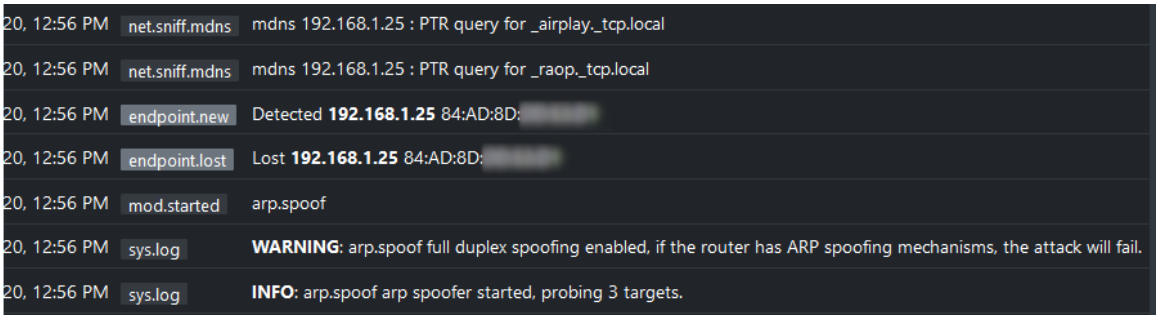
3. Before starting the ARP spoofing module, we need to start **net.sniff** . We can either use the console command or the GUI to execute this.

   From the console command we type in the following cmdlet:

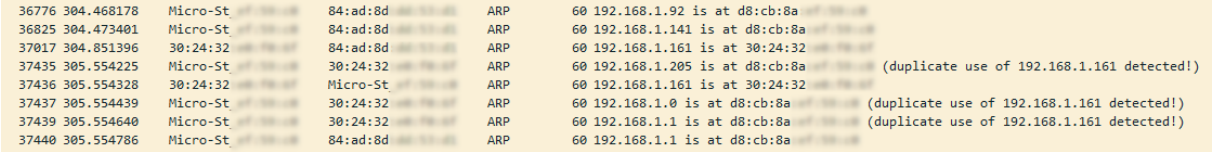
   `net.sniff on`

   From the GUI we can go to: Advanced -> net.sniff -> net.sniff.on

We have now successfully launched ARP spoofing:



Verification of ARP spoofing using Wireshark:



CONCLUSION

With ARP spoofing & Man-in-the-Middle (MiTM) attack we were able to sniff user login data and critical password hashes. These attacks were only successful because we were able to bypass NAC.

REPORTING

Key issues listed in this case study, and many others, were put into the final report. The issues were identified at risk levels: low, medium, high and critical. The executive summary provided a brief summary of vulnerabilities discovered during this assessment broken down by category. Many of these issues were presented graphically with recommendations given for resolution of each.