**Opção 1:**

**Remote code execution Server**

Criar SMTP server (Exim Servers)

default TCP port 25 (Exim Vulnerability)

Code & Command execution em servers vulneráveis: roubo e extração de informação sensível a esse servidor

**(The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of a buffer)**

<https://www.bleepingcomputer.com/news/security/millions-of-exim-mail-servers-exposed-to-zero-day-rce-attacks/>

**Opção 2:**

**ARP Spoofing**

1. The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices⁠—let’s say these are a workstation and a router.
2. The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send out forged ARP responses.
3. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker’s MAC address. This fools both router and workstation to connect to the attacker’s machine, instead of to each other.
4. The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
5. The attacker is now secretly in the middle of all communications.

the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS

**Tutorial de como executar:** [**https://tutorialedge.net/security/arp-spoofing-for-mitm-attack-tutorial/**](https://tutorialedge.net/security/arp-spoofing-for-mitm-attack-tutorial/)

**https://www.tutorialspoint.com/ethical\_hacking/ethical\_hacking\_arp\_poisoning.htm**

**Plano C:**

**DNS Tunneling**

1. The attacker registers a domain, such as badsite.com. The domain’s name server points to the attacker’s server, where a tunneling malware program is installed.
2. The attacker infects a computer, which often sits behind a company’s firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers.
3. The DNS resolver routes the query to the attacker’s command-and-control server, where the tunneling program is installed. A connection is now established between the victim and the attacker through the DNS resolver. This tunnel can be used to exfiltrate data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker’s computer.