DHCP attackes

Resources:

https://cs-coe.iisc.ac.in/wp-content/uploads/2020/08/Attacks-and-Mitigation-Techniques.pdf

https://pentera.io/blog/dhcp-spoofing-101/

DHCP spoofing attack methods

Needless to say, the DHCP protocol is a powerful network configuration tool that can simplify life for network administrators. The problem arises when unsuspecting network administrators are not well aware of all that makes the DHCP protocol susceptible to attack. By default, the DHCP protocol uses no form of authentication and is sent on broadcast, so potentially any device on the network could receive and possibly tamper with the messages. Let's consider what could happen if an attacker were to combine attacks – for example, DHCP starvation and Rogue DHCP – to launch a Man-In-The-Middle attack (MITM).

DHCP Starvation Attack

In a DHCP starvation attack, an attacker sends the DHCP server multiple DHCP-REQUEST messages with spoofed source MAC addresses within a short time span in order to deplete the server's pool of available IP addresses and prevent a race condition. The "starved" DHCP server will not respond to new DHCP requests until a new address becomes available. A DHCP starvation attack sets the stage for the attacker to pass himself off as the DHCP server and send out spoofed messages to trick other clients on the network.

How Does a DHCP Starvation Attack Work?

In a DHCP Starvation attack, a hostile actor sends a ton of bogus DISCOVER packets until the DHCP server thinks they've expended their available pool. Clients looking for IP addresses find that there are no IP addresses for them, and they're denied service. Additionally, they may look for a different DHCP server, one which the hostile actor may provide. And using a hostile or dummy IP address,

that hostile actor can now read all the traffic that client sends and receives.

In a hostile environment, where we have a malicious machine running some kind of a tool like Yersinia, there could be a machine that sends DHCP DISCOVER packets. This malicious client doesn't send a handful – it sends hundreds and hundreds of malicious DISCOVER packets using bogus, made-up MAC addresses as the source MAC address for each request.

If the DHCP server responds to each of these bogus DHCP DISCOVER packets, the entire IP address pool could be depleted, and that DHCP server could believe it has no more IP addresses to offer to valid DHCP requests.

Once a DHCP server has no more IP addresses to offer, typically the next thing to happen would be for the attacker to bring in their own DHCP server. This rogue DHCP server then begins handing out IP addresses.

The benefit of that to the attacker is that if a bogus DHCP server is handing out IP addresses, including default DNS and gateway information, clients who use those IP addresses and start to use that default gateway can now be routed through the attacker's machine. That's all that a hostile actor needs to perform a man-in-the-middle (MITM) attack.

Rogue DHCP attack

Now the attacker can set up his own rogue DHCP server, listen for incoming broadcast requests, and send out spoofed responses with malicious configurations. Usually, the attacker will aim to set himself as the DNS server and default gateway for the clients. The attacker will open port 53 on his machine for DNS activity, so that every DNS resolution request will reach his machine, allowing him to choose when to answer with his own hostname.