<https://chatgpt.com/c/8a567d7c-210d-4b7f-8589-5059ae33e319>

1. What is DHCP starvation attack and how is it done?

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign IP addresses to devices on a network. DHCP starvation is a type of denial-of-service (DoS) attack where the attacker exhausts the available pool of IP addresses in the DHCP server, preventing legitimate users from obtaining IP addresses and connecting to the network.

**How DHCP Starvation Works:**

1. **Attack Initiation:** The attacker uses a tool or script to send a large number of DHCP discovery requests to the DHCP server.
2. **Fake MAC Addresses:** Each request is sent with a different, often randomly generated, MAC address. This tricks the DHCP server into thinking that each request is coming from a different device.
3. **IP Address Exhaustion:** The DHCP server assigns an IP address from its pool to each fake MAC address. As the number of requests increases, the available IP addresses are quickly exhausted.
4. **Denial of Service:** Once the pool of IP addresses is depleted, legitimate devices on the network are unable to obtain an IP address. As a result, they cannot connect to the network or access network resources.

**Tools for DHCP Starvation:**

* **Yersinia:** A network security tool that can perform various network attacks, including DHCP starvation.
* **dhcpx:** A specific tool designed to send multiple DHCP requests with random MAC addresses.

**Prevention and Mitigation:**

1. **DHCP Snooping:** This feature is available on many network switches and can help prevent DHCP starvation by allowing only trusted ports to send DHCP requests.
2. **IP Address Filtering:** Configuring the DHCP server to allocate IP addresses only to known and trusted MAC addresses.
3. **Rate Limiting:** Implementing rate limiting on DHCP requests to prevent a flood of requests from exhausting the IP address pool.
4. **Network Segmentation:** Dividing the network into smaller segments or subnets can limit the impact of a DHCP starvation attack to a smaller portion of the network.
5. **Monitoring and Alerts:** Regularly monitoring DHCP logs and setting up alerts for suspicious activity can help in early detection of DHCP starvation attacks.

By understanding DHCP starvation and implementing appropriate security measures, network administrators can protect their networks from such attacks and ensure continuous availability of network services.

1. Give example

**Network Setup:**

* A company has a network with a DHCP server that assigns IP addresses from a pool of 192.168.1.2 to 192.168.1.254.
* There are around 100 employees who connect to the network using various devices such as laptops, smartphones, and tablets.

**Attack Execution:**

1. **Preparation:**
   * The attacker gains access to the network, either by connecting directly to the network or by compromising a device on the network.
   * The attacker has a laptop with Kali Linux installed, which includes tools for performing DHCP starvation attacks.
2. **Launching the Attack:**
   * The attacker opens a terminal on Kali Linux and uses a tool like **Yersinia** or **dhcpstarv** to start the DHCP starvation attack.
   * Using Yersinia, the attacker runs the following command to open the interactive mode:

css

Copy code

yersinia -I

* + In the Yersinia interactive interface, the attacker selects the DHCP attack module and starts sending a flood of DHCP discovery packets with fake MAC addresses.
  + Alternatively, using a simple script or another tool, the attacker could execute:

css

Copy code

dhcpstarv -i eth0

(Here, eth0 is the network interface connected to the target network.)

1. **Effect of the Attack:**
   * The DHCP server receives a large number of DHCP discovery requests, each with a different fake MAC address.
   * The DHCP server starts allocating IP addresses to these fake MAC addresses, depleting the pool of available IP addresses.
   * Legitimate users trying to connect to the network are unable to obtain an IP address because the pool is exhausted.
2. **Impact:**
   * Employees report that they are unable to connect to the network.
   * Network administrators notice an unusual number of IP addresses being assigned in the DHCP server logs.
   * The network becomes unusable for legitimate users, causing a denial of service.

**Detection and Mitigation:**

* **Detection:**
  + Network administrators check the DHCP server logs and see a large number of IP addresses assigned to suspicious or random MAC addresses.
  + Network monitoring tools alert administrators about the abnormal rate of DHCP requests.
* **Mitigation:**
  + Enable DHCP snooping on network switches to filter and block untrusted DHCP requests.
  + Implement rate limiting on DHCP requests to prevent a flood of requests from a single source.
  + Configure the DHCP server to allocate IP addresses only to known and trusted MAC addresses.
  + Segment the network to isolate the impact of the attack.

By following these detection and mitigation steps, network administrators can respond to the DHCP starvation attack and restore normal network functionality.