Understanding DHCP Starvation Attack and Protecting Your Network with DHCP Snooping

Introduction

The Dynamic Host Configuration Protocol (DHCP) plays a vital role in modern networks by dynamically distributing network configuration settings to connected devices. While it simplifies network management, it is also vulnerable to specific types of attacks, such as the **DHCP Starvation Attack**. This article provides an in-depth explanation of DHCP, the DHCP Starvation Attack, and how to secure your network using **DHCP Snooping**.

1 What is DHCP ?

DHCP, or **Dynamic Host Configuration Protocol**, is a protocol responsible for distributing network settings to devices automatically. These settings include :

- **IP Address :** Assigns unique addresses to devices.
- **Subnet Mask :** Defines the network boundary.

- **Default Gateway :** Specifies the router for network communication.
- **DNS Server :** Provides the addresses of domain name servers.

How DHCP Works

The DHCP process consists of four main steps :

1. **Discover :** The client sends a DHCP Discover message to locate an available DHCP server.
2. **Offer :** The server responds with an offer containing an IP address and network configuration.
3. **Request :** The client requests the offered configuration from the server.
4. **Acknowledge :** The server acknowledges and completes the process by assigning the configuration.

2 What is a DHCP Starvation Attack ?

A **DHCP Starvation Attack** aims to exhaust all available IP addresses in the DHCP server's pool, preventing legitimate devices from obtaining an IP address.

How the Attack Works

1. The attacker uses tools (e.g., Kali Linux utilities) to send a flood of DHCP Discover requests with **fake MAC addresses**.
2. The DHCP server assigns all available IP addresses in its pool to these fake devices.

3. Legitimate devices cannot obtain IP addresses and are isolated from the network, often defaulting to APIPA addresses (`169.254.x.x`) without gateway or DNS functionality.

Related DHCP Attacks

- **DHCP Starvation Attack :** Exhausts IP addresses in the pool.
- **Rogue DHCP Attack :** An attacker sets up a fake DHCP server to distribute incorrect network settings.
- **DHCP Spoofing :** The attacker impersonates a DHCP server using tools like Ettercap.

3 Protecting Your Network with DHCP Snooping

DHCP Snooping is a feature available on managed switches that provides protection against DHCP-based attacks. It achieves this by :

- Preventing unauthorized devices from running a rogue DHCP server.
- Safeguarding the DHCP server from IP exhaustion caused by DHCP Starvation Attacks.

Steps to Enable DHCP Snooping

Here are the configuration steps to enable DHCP Snooping on a Cisco switch :

1. **Enable DHCP Snooping :**

```
(config)# ip dhcp snooping
```

2. **Specify VLANs to Protect :**

```
(config)# ip dhcp snooping vlan 1
```

3. **Mark Trusted Ports :** Identify ports connected to the DHCP server as trusted :

```
(config)# int f0/1
(config-if)# ip dhcp snooping trust
```

4. **Configure Untrusted Ports :** Define other ports as untrusted and limit the number of DHCP requests to prevent abuse :

```
(config)# int range f0/2 - 24
(config-if)# ip dhcp snooping limit rate 4
```

What Happens When DHCP Snooping is Active ?

When DHCP Snooping is enabled :

- Unauthorized devices attempting to send excessive DHCP Discover requests will have their ports shut down (Error Disabled State).
- Legitimate devices can obtain IP addresses without disruption.

4 Benefits of DHCP Snooping

- **Enhanced Security :** Blocks unauthorized devices and rogue DHCP servers.
- **IP Management :** Prevents IP exhaustion by ensuring efficient allocation.
- **Network Stability :** Protects critical infrastructure from malicious attacks.

Conclusion

The DHCP Starvation Attack is a serious threat that can disrupt network operations by isolating legitimate devices. However, by implementing **DHCP Snooping**, network administrators can effectively safeguard their infrastructure against such attacks. This feature not only ensures a stable and secure network but also enhances overall operational efficiency. Proactively deploying tools like DHCP Snooping is essential to maintaining a resilient and secure network environment.