DHCP Assaults

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

Against the assault of laughter, nothing can stand.

-Mark Twain

DHCP Attacks

What is DHCP?

Client-server protocol

Server role

Provides address configurations to DHCP-enabled clients

Avoid duplation and fat-finger mistakes

Tedious input

How DHCP Works

DHCP client broadcasts a DHCPDISCOVER

DHCP-relay agent captures the client request and unicasts it to available servers

DHCP server unicasts DHCPOFFER/ADVERTISE

Relay agent broadcasts DHCPOFFER/ADVERTISE

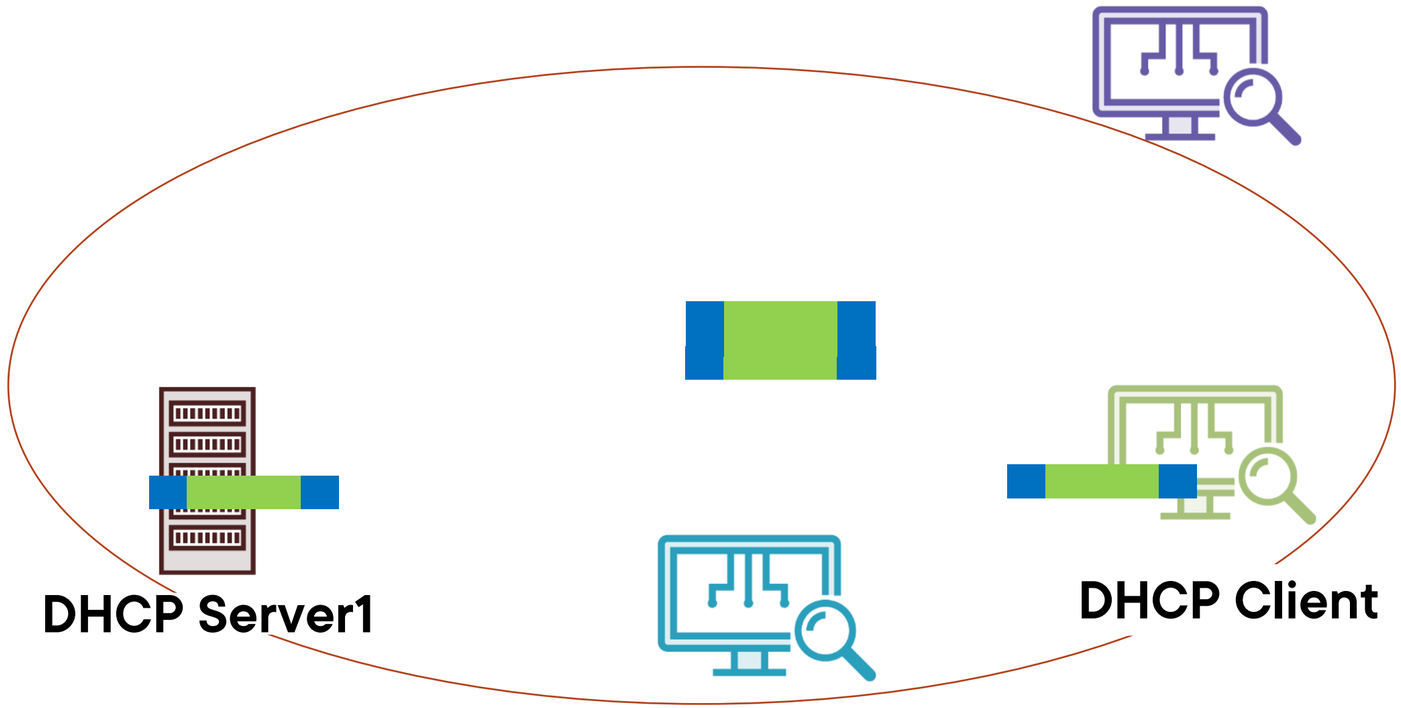
The client broadcasts DHCPREQUEST/REQUEST

DHCP server sends a unicast DHCPACK/REPLY with the IP configuration and information

```
IPv4 Address. . . . . . . . . . . : 10.10.10.35(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Monday, February 1, 2016 1:38:54 PM
Lease Expires . . . . . . . . . . : Friday, February 5, 2016 3:38:56 PM
Default Gateway . . . . . . . . . : 10.10.10.1
DHCP Server . . . . . . . . . . . : 10.10.10.151
DHCPv6 IAID . . . . . . . . . . . : 168321134
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1D-F1-6B-12-08-60-6E-75-5C-6D
DNS Servers . . . . . . . . . . . : 10.10.10.151
```

How DHCP Works

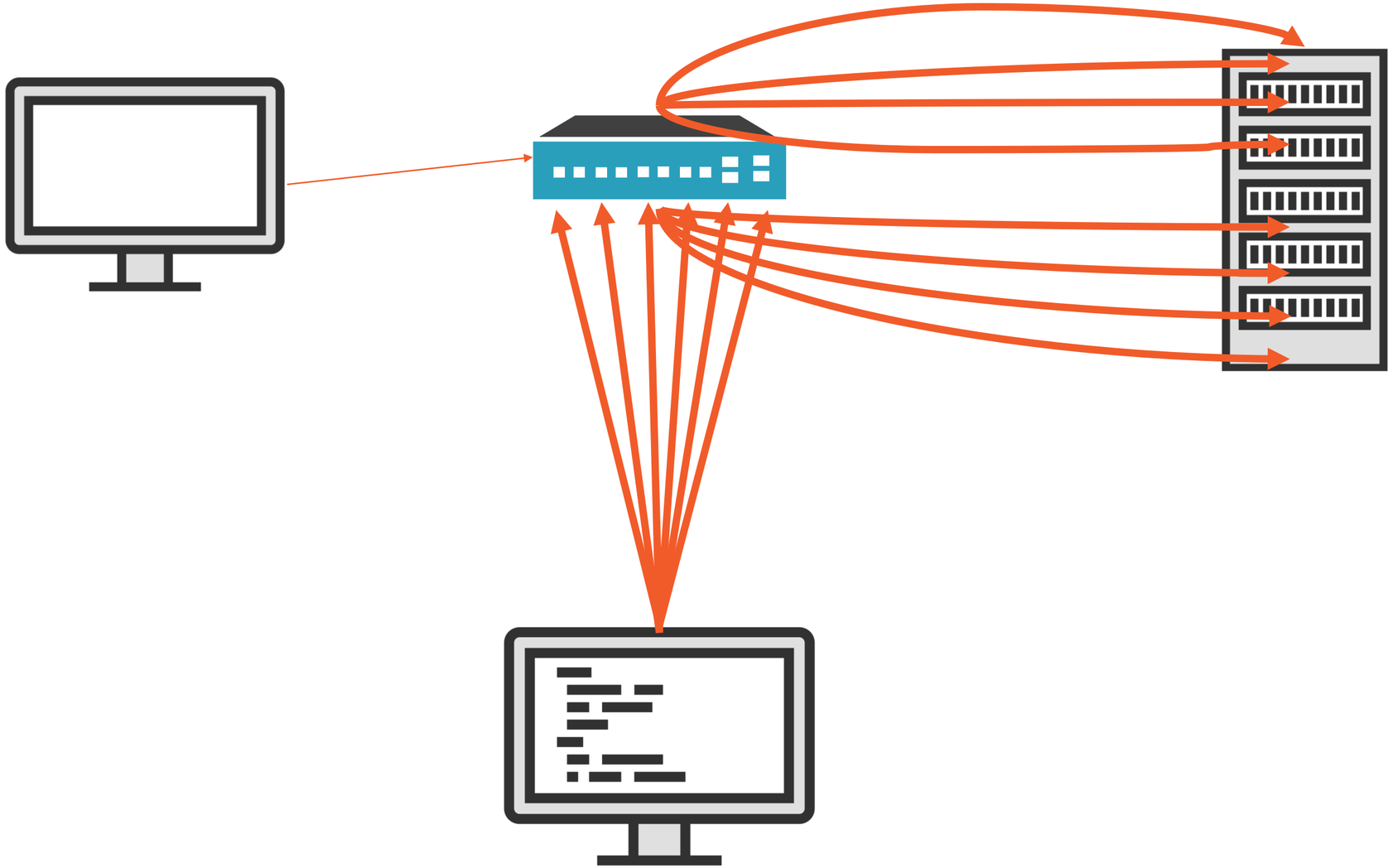
1. **DHCP client broadcasts a DHCPDISCOVER**
2. **DHCP servers broadcast a DHCPOFFER**
3. **DHCP client broadcasts a DHCPREQUEST**
4. **DHCP Server1 broadcasts a DHCPACK**




```
IPv4 Address. . . . . . . . . . . : 10.10.10.35(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Monday, February 1, 2016 1:38:54 PM
Lease Expires . . . . . . . . . . : Friday, February 5, 2016 3:38:56 PM
Default Gateway . . . . . . . . . : 10.10.10.1
DHCP Server . . . . . . . . . . . : 10.10.10.151
DHCPv6 IAID . . . . . . . . . . . : 168321134
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1D-F1-6B-12-08-60-6E-75-5C-6D
DNS Servers . . . . . . . . . . . : 10.10.10.151
```

DHCP Starvation Attack

DHCP Starvation Attack



Corp Scope
~~192.168.0.1~~
~~192.168.0.2~~
~~192.168.0.3~~
~~192.168.0.4~~
|
|
~~192.168.0.254~~

DHCP Starvation Attack Tools

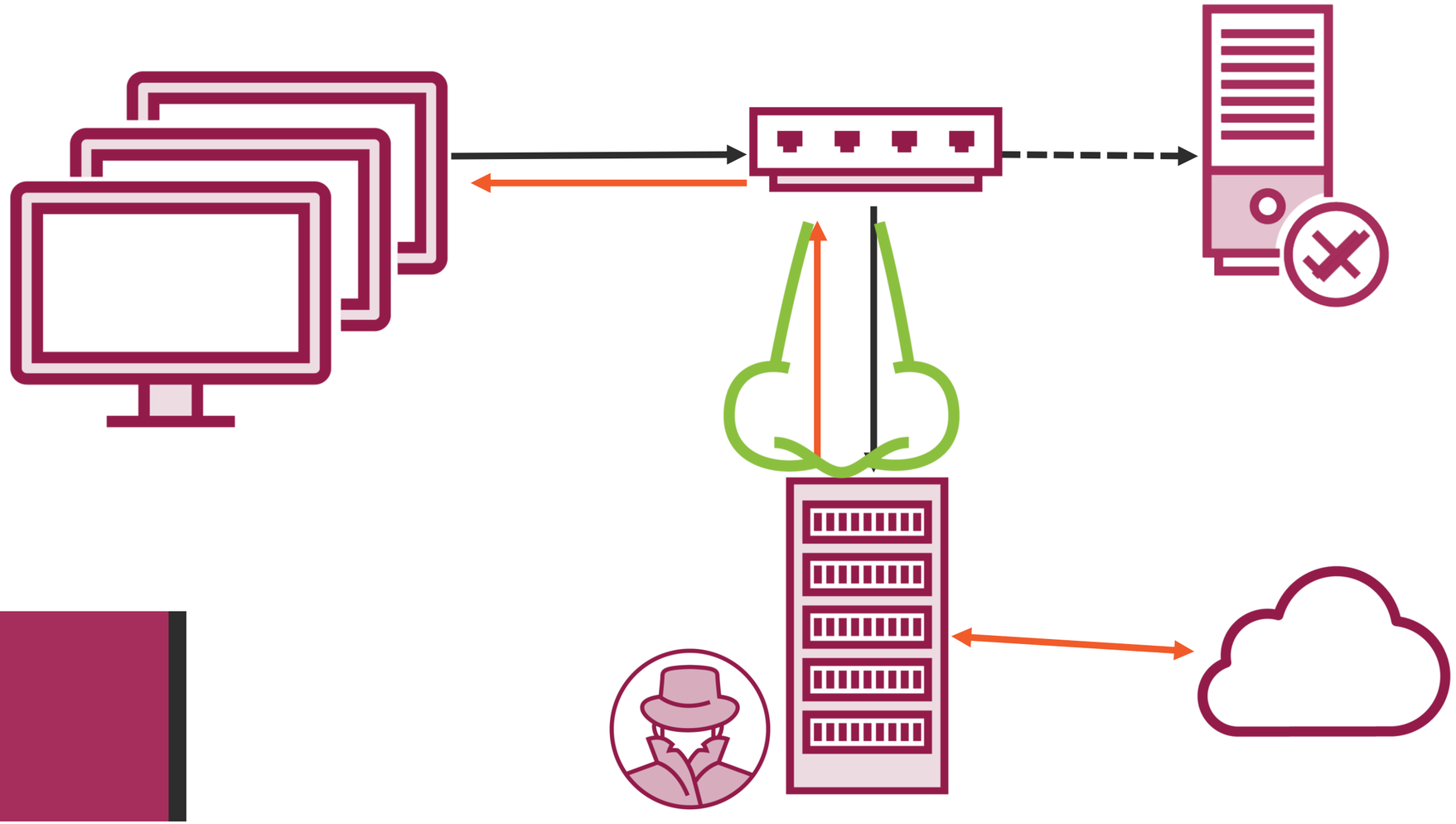
- **Yersinia**
- **Hyenae**
- **dhcpstarv**
- **Gobbler**
- **DHCPig**

Demo

DHCP Starvation with Yersinia

Rogue Attack

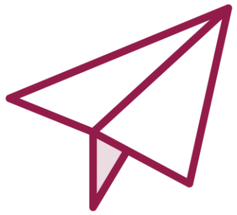
What if?



Key Rogue Attack Learnings

Works in conjunction with the DHCP starvation attack

Attacker sets up a rogue DHCP server and responds to DHCP requests with bogus IP addresses



Attacker sends a TCP/IP setting to the user after kicking them out from the genuine server

Demo

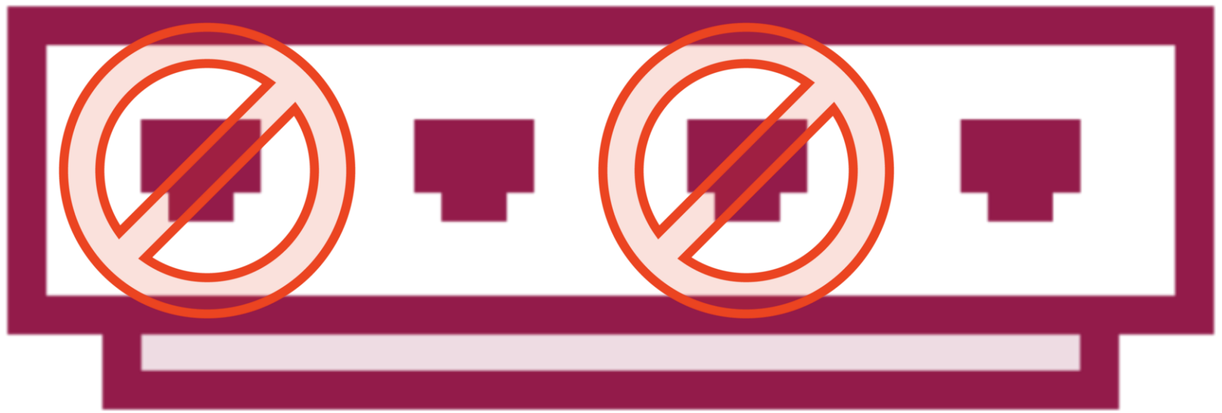
Setting up a DHCP rouge server

Defense Methods

Stopping Attacks

How do we stop a DHCP Starvation Attack?

Enable port security
-Sets a max number of MAC addresses



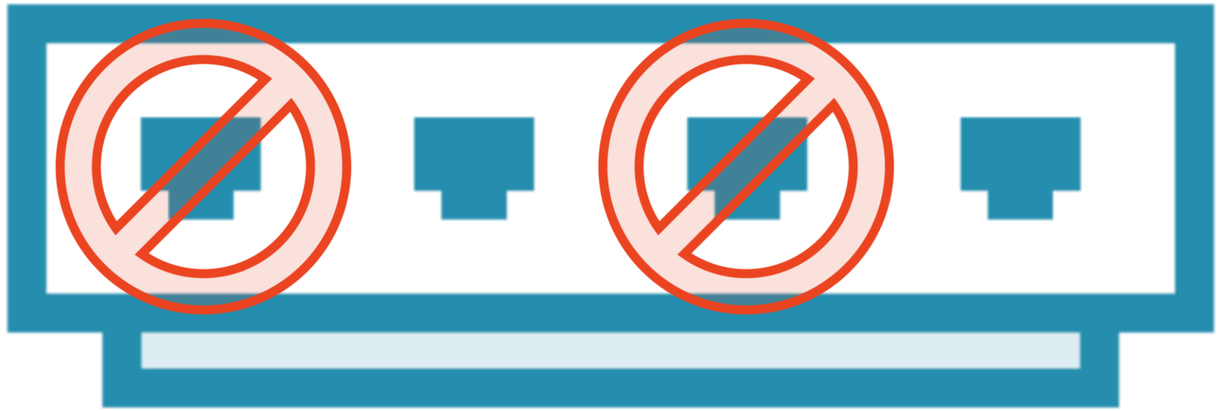
IOS Settings

```
switchport port-security

switchport port-security maximum 1

switchport port-security violations restrict

switchport port-security aging time 2

switchport port-security aging type inactivity
```

Stopping Attacks

How do we stop a Rogue Attack?

DHCP Snooping
-Stops ports from responding to DHCP offers



Microsoft Windows

Authorized DHCP in AD

Learning Check

Learning Check

- DHCPDISCOVER
- Starvation attack
- Rogue attack
- DHCP snooping
- switchport port-security

Up Next:
Understanding ARP Poisoning Attacks