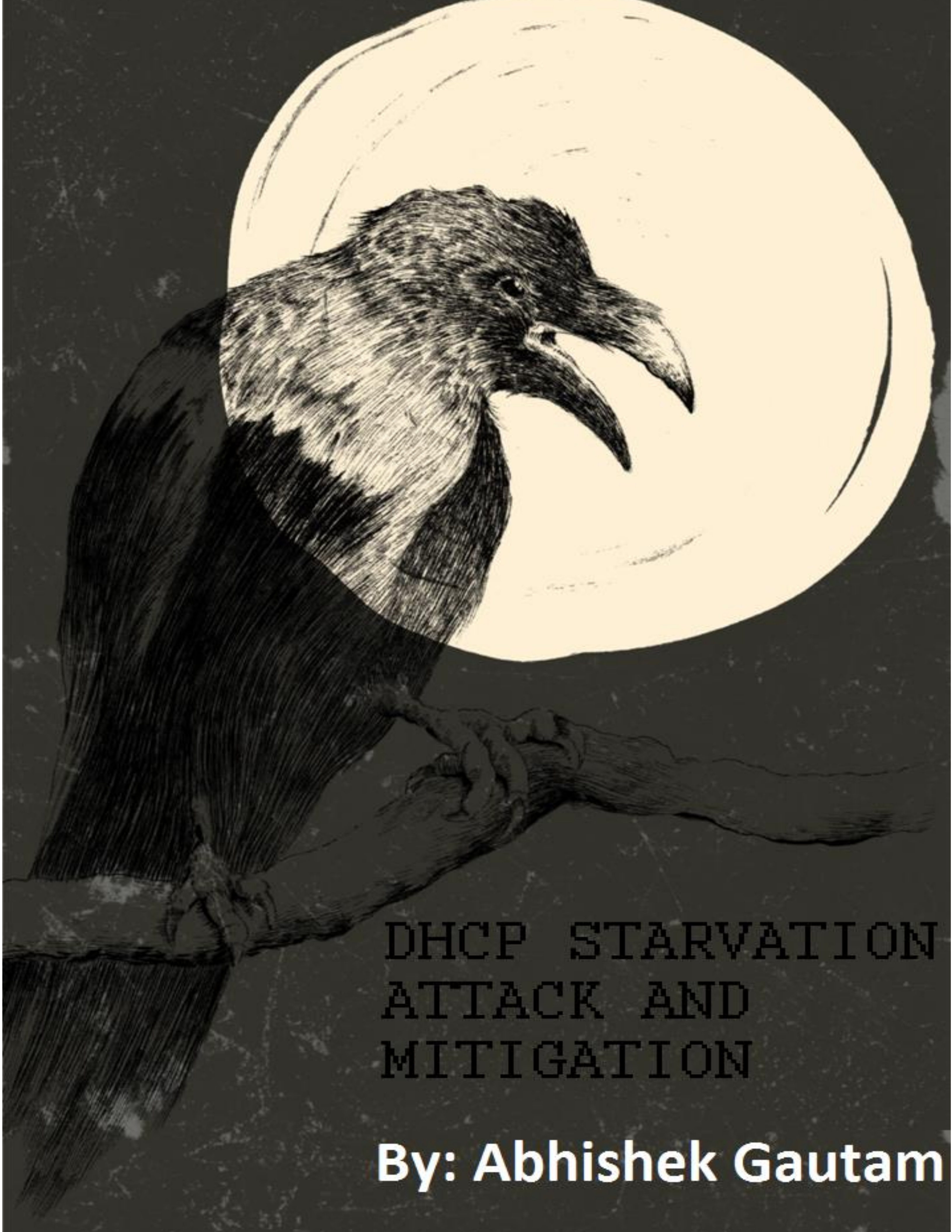


DHCP STARVATION ATTACK AND MITIGATION

By: Abhishek Gautam

DHCP STARVATION ATTACK

Requirement

Kali Linux or BT5

Tools: Gobbler/Yersinia/Metaspliot

A Network Router.

*Tip*GNS3 can be used for router simulation.

How this attack works?

For understanding how this attack works we need to first understand what dhcp is and what are it's functionality.

DHCP stands for ***dynamic host configuration protocol*.**

It assigns 3 thing to a new user making connection with the network:

1> An unique network ip

2> A Default Gateway

3> A subnet mask

All these are allocated dynamically to a user. Now each router has a capacity of allocating IPs to different devices

This Capacity of Allocating the IPs depends on the hardware plus the subnet mask it is using.

First the person connecting to a network send **DHCP Discover packets** to the router.

If ips are avilable then DHCP SERVER send **DHCP Offer packets**.

But in this attack we send multiple broadcast multiple discover packets continuously with random spoofed mac address and all ips get exhausted from the ip table. This is a simple **resource starvation attack** just like a synchronization (SYN) flood attack.

Attack are designed to **deplete all of the addresses within the DHCP scope on a particular segment**. Subsequently, a legitimate user is denied an IP address requested via DHCP and thus is not able to access the network.

What is the key principle behind this attack :

It works by broadcasting vast numbers of DHCP requests with spoofed MAC addresses simultaneously.

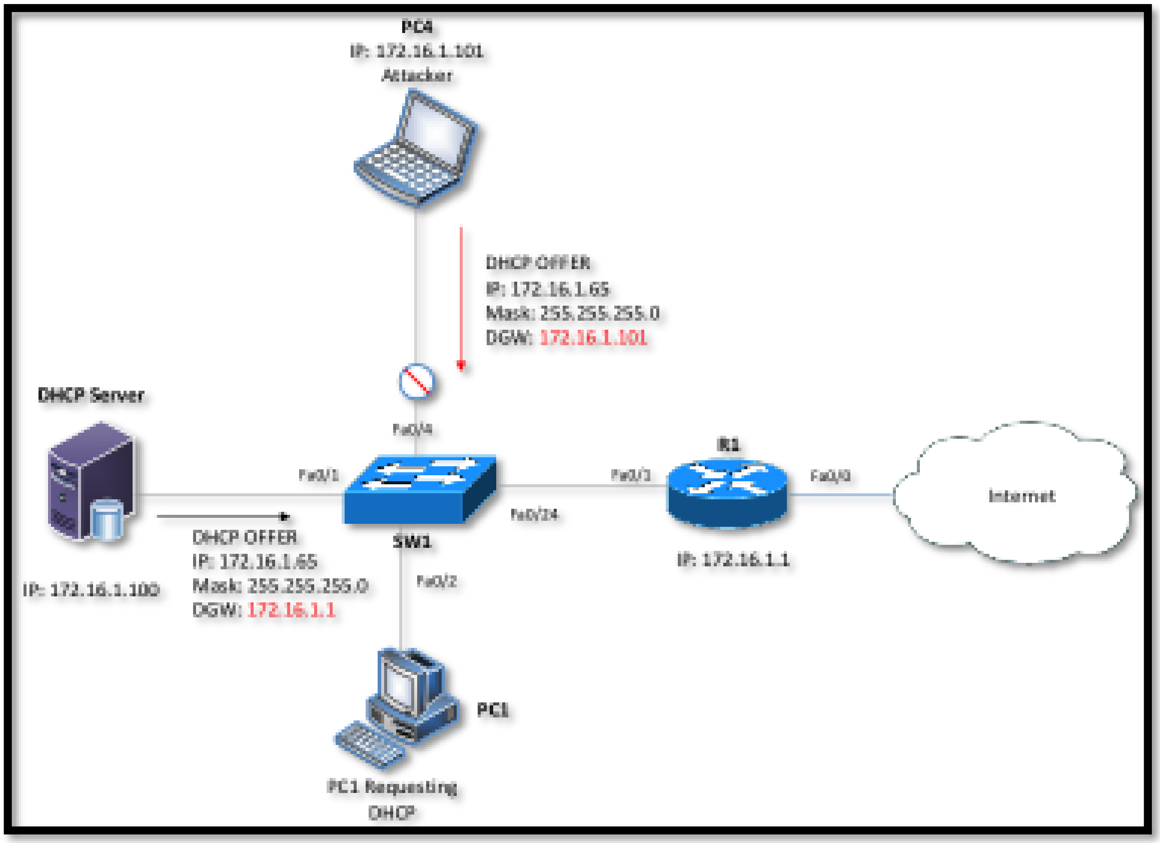
For what purpose we can use this attack?

DHCP starvation may be purely a **DoS(Denial of servic) mechanism** or may be used in conjunction with a **malicious rogue server attack** to redirect traffic to a malicious computer ready to intercept traffic.

Rogue DHCP Server

A rogue DHCP server is a DHCP server set up on a network by an attacker, or by an unaware user, and is not under the control of network administrators. An accidental rogue device is commonly a modem or home wireless router with DHCP capabilities which a user has attached to the network unaware of the consequences of doing so. Rogue DHCP servers are also commonly used by attackers for the purpose of network attacks such as Man in the Middle, Sniffing, and Reconnaissance attacks.

By placing a rogue DHCP server on the network, a network attacker can provide clients with addresses and other network information. Because DHCP responses typically include default gateway and Domain Name System (DNS) server information, network attackers can supply their own system as the default gateway and DNS server resulting in a man-in-the-middle attack (Figure 1).



Man in the Middle DHCP attacks can be used to forge network resources. The Rogue DHCP reply will offer an IP address and information that may designate the attacker’s machine as the default gateway or Domain Name System (DNS) server. If the attacker is designated default gateway, any clients with addresses assigned from the Rogue DHCP Server will forward packets to the attacking device, which may in turn send them to the desired destination, or possibly elsewhere. If the attacker also designates its own Rogue DNS Server(s), they may design phishing websites to obtain other confidential information, such as credit card details and passwords.

How to perform this attack?

Step1: Open terminal type "**yersinia -G**" it will open graphical version of yersinia.

Step2: Click on '**Launch Attack**'.

Step3: Select the tab 'DHCP' and check the second box '**sending DISCOVER packet**' and press **OK**.

Within seconds, hundreds of DHCP requests will be sent and the router will be busy handling all our requests and won't be able to handle IP addresses to genuine users.

How to stop the attack?

Step1: Click on **'List attack'** and then **'cancel all attacks'**.

Mitigation

There are two ways to secure it

1>port security

2>dhcp scooping

1>Port Security:

It is recommended that you set the port secuirty to 1 so that at max only one mac address on a switch port.

if you have VoIP in your network this could cause it to go down so you can change it accordingly:

switchport port-security maximum 5

There's often no tangible reason why a switch port should ever allow more than one MAC address on a switch port.

If someone tried to launch Yersinia on a port-security enabled switch, it would immediately **put the port in a secure-shutdown state.** The port would immediately turn off which protects the switch and alerts you that some butt munch on your network is trying to take you down but the problem here is that a **tool** called **DhcpStarv** can be used to **bypass the port securi**ty and we should never apply port security on **WLCs(wireless Lan controllers).**

2>DHCP Snooping:

DHCP snooping is a **DHCP security feature** that provides network security by **filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database**, which is also referred to as a **DHCP snooping binding table.**

DHCP snooping is a **Cisco Catalyst switch feature** that determines **which switch ports can respond to DHCP requests**. Ports are **identified as trusted and**

untrusted. Trusted ports can source all DHCP messages, while untrusted ports can source requests only. Trusted ports host a DHCP server or can be an uplink toward the DHCP server. If a rogue device on an untrusted port attempts to send a DHCP response packet in to the network, the port is shut down. This feature can be coupled with DHCP option 82, in which switch information, such as the port ID of the DHCP request, can be inserted into the DHCP request packet.

Untrusted ports are those not explicitly configured as trusted. A DHCP binding table is built for untrusted ports. Each entry contains the client MAC address, IP address, lease time, binding type, VLAN number, and port ID recorded as clients make DHCP requests. The table is then used to filter subsequent DHCP traffic. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as DHCPOFFER, DHCPACK, or DHCPNAK.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.