



Abusing, & Exploiting DHCP

By James Hemmings

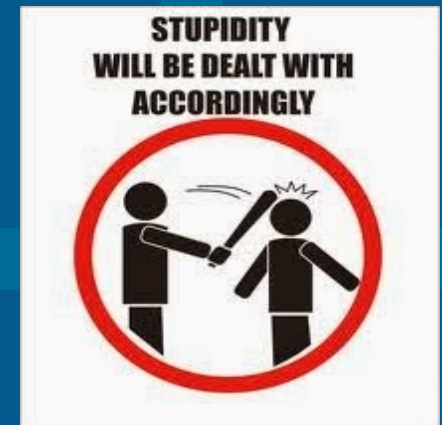
About me

- James Hemmings
- Ethical Hacking 1st Year Student
- 1st Year Ethical Hacking Class Representative
- Previously employed as IT Technician
- Huge passion for all things Linux, and information security

32444245304354

Disclaimer

- **DO NOT BE STUPID**
 - Using the contents of these slides on a public network, and/or business network WILL get you into trouble
 - I take no responsibility for misuse of the content in these slides
 - TL;DR
 - Test this in a lab environment, not anywhere else :)



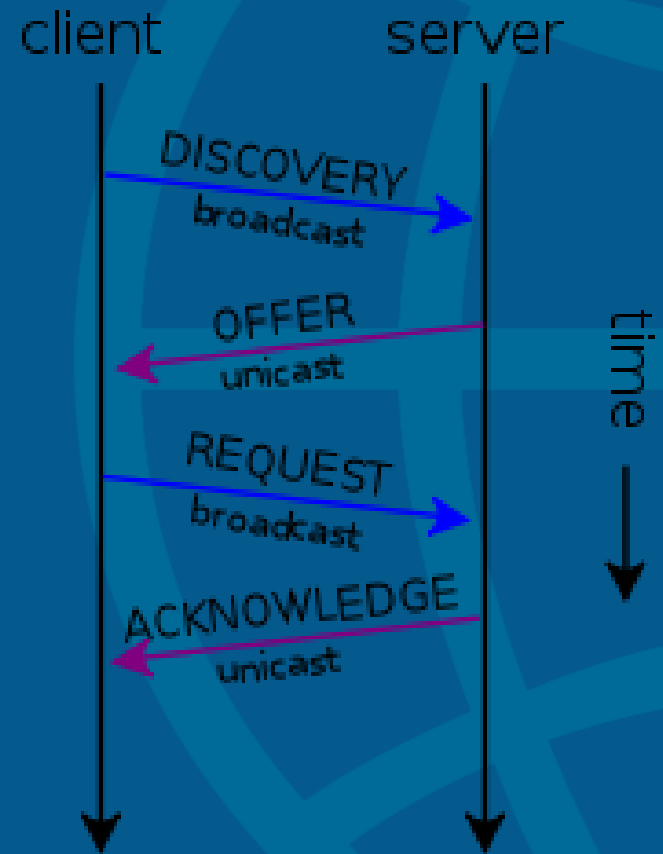
Agenda

- About Me
- Agenda
- What is DHCP
- DHCP Server
- Proof Of Concept
- Tools
- Demo
- Commands
- What else can we do?
- Counter Measures
- Q & A

32444245304354

What is DHCP (1/2)

- Dynamic Host Configuration Protocol
- Assigns dynamic IP address's to clients on a network
- Client: UDP Port 68



What is DHCP (2/2)

R1_to_R2.cap [Wireshark 1.6.7]

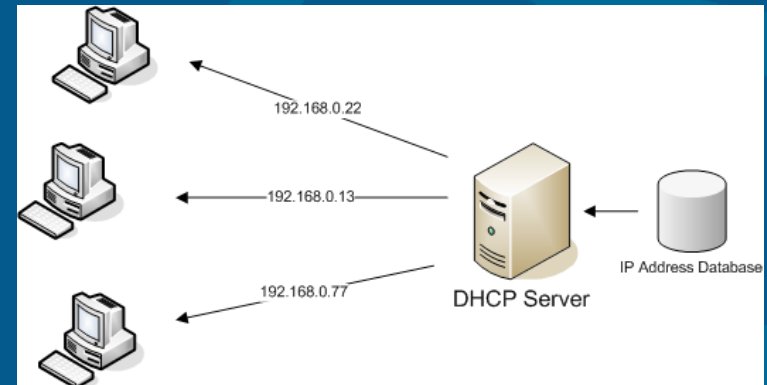
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
103	433.584154	0.0.0.0	255.255.255.255	DHCP	618	DHCP Discover - Transaction ID 0x225d
105	435.579178	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x225d
106	435.585370	0.0.0.0	255.255.255.255	DHCP	618	DHCP Request - Transaction ID 0x225d
107	435.587536	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x225d

DHCP Server (1/2)

- DHCP Server can be configured on Windows/Linux ect
- Server assigns dynamic IP for period of 8 days (LAN), & 8 hours (WiFi)
- Server: UDP Port 67



The screenshot shows the Windows DHCP console for the scope "192.168.0.0". The "Address Leases" tab is selected, displaying a table of active leases.

Client IP Address	Name	Lease Expires
192.168.0.12	ASUS-LAPTOP.scri...	10/1/20
192.168.0.13	HP160-V32-03.ex...	10/2/20
192.168.0.14	XMPL-WIN7-05.ex...	9/30/20
192.168.0.24	FERRARI-WIN7.scr...	9/30/20
192.168.0.101	HP160-WIN7-02.e...	9/29/20
192.168.0.103	Gateway-Win7.scr...	10/2/20
192.168.0.104	HP160-WIN7-01.e...	9/29/20
192.168.0.105	HP160-XP-04.EXA...	10/1/20
192.168.0.198	TIVO-240000090...	9/30/20
192.168.0.199	TIVO-240000080...	9/30/20

DHCP Server (2/2)

- DHCP is unauthenticated, and responds to DHCPDISCOVER messages
- Checks IP Pool for already leased address's based on MAC address of client/pool
- Well, lets spam DHCPDISCOVER messages.
- However...
- This would cause an MAC conflict, thus the need for mac spoofing is present

Proof Of Concept (1/2)



- Attacker sends spoofed MAC address's in the DHCPDISCOVER packets repeatedly until the entire IP pool is exhausted
- Then a gratuitous ARP is sent to the LAN, knocking all windows systems offline (Sorry Linux)
- Rouge DHCP server if running, will then send new IP's to clients

Proof Of Concept (2/2)

- Once the DHCP pool has all leases taken away, we can setup a rogue DHCP server to perform a MiTM attack
- We can set the DHCP options for the gateway to the Kali Linux machine.
- Then launch an attack with SSLStrip, or ettercap
- Or plain old wireshark!

Tools

- Pig.py – Command line driven
- Yersinia – GUI driven
- DHCPStarv – Command line driven
- Scapy – Manual command line attacks
- Metasploit Rouge DHCP – command line driven, launches listening rouge DHCP server

Demo

Environment:

Windows Server 2008 R2 – DHCP/AD Server

Hostname: server.bobcorp.local

IP: 192.168.187.10

Windows 7 Ultimate – Client

Hostname: Lab1VM.bobcorp.local

IP: Dynamic

Kali Linux - Attacker

Hostname: kali.bobcorp.local

IP: Dynamic

32444245304354

Commands

- DHCP Starvation Attack
 - `Pig.py -d eth0`
- Metasploit Rouge DHCP Server
 - `Msfconsole`
 - `Use auxiliary/server/dhcp`
 - `Show options`
- (Set options to correct router, netmask, dns, server ip, & pool range)

What else can we do?

Tftpd64: Settings

GLOBAL | TFTP | DHCP | SYSLOG

DHCP Pool definition

IP pool start address: 10.10.10.2

Size of pool: 200

Lease (minutes): 2880

Boot File:

DHCP Options

Def. router (Opt 3): 10.10.10.1

Mask (Opt 1): 255.255.255.0

DNS Servers (Opt 6):

WINS server (Opt 44):

NTP server (Opt 42):

SIP server (Opt 120):

Domain Name (15):

Additional Option: 114 {} { ignored.}; echo 'foo'

DHCP Settings

☒ Ping address before assignation

☐ Persistent leases

☐ Double answer if relay detected

☒ Bind DHCP to this address: 10.10.10.1

OK Default Help Cancel

```
geoff@sl_linux_gdw:/lib/dhcpd/dhcpd-hooks$ sudo /etc/rc.d/rc.inet1 eth0_restar
t
Polling for DHCP server on interface eth0:
dhcpd[3287]: version 6.0.5 starting
dhcpd[3287]: eth0: soliciting an IPv6 router
dhcpd[3287]: eth0: soliciting a DHCP lease
dhcpd[3287]: eth0: offered 10.10.10.4 from 10.10.10.1
dhcpd[3287]: eth0: leased 10.10.10.4 for 172800 seconds
dhcpd[3287]: eth0: adding host route to 10.10.10.4 via 127.0.0.1
dhcpd[3287]: eth0: adding route to 10.10.10.0/24
dhcpd[3287]: eth0: adding default route via 10.10.10.1
'foo'
dhcpd[3287]: forked to background, child pid 3317
geoff@sl_linux_gdw:/lib/dhcpd/dhcpd-hooks$
```

[110404.447634] usb 2-2.1: Product: Virtual Bluetooth Adapter



Counter Measures

- DHCP Snooping
 - Enable this on switch to prevent rouge DHCP servers, by blocking all messages from none-trusted DHCP servers
- Port Security
 - Prevents DHCP starvation attacks by triggering a violation if more than specified mac address's on port is reached.
- Dynamic ARP Inspection
 - Prevents current ARP attacks

Thank you.

Any questions?

Contact Me:

james@hemmings.pw

[@MrJamesHemmings](#)

[linkedin.com/in/jhemmings](https://www.linkedin.com/in/jhemmings)

32444245304354