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

Disclaimer

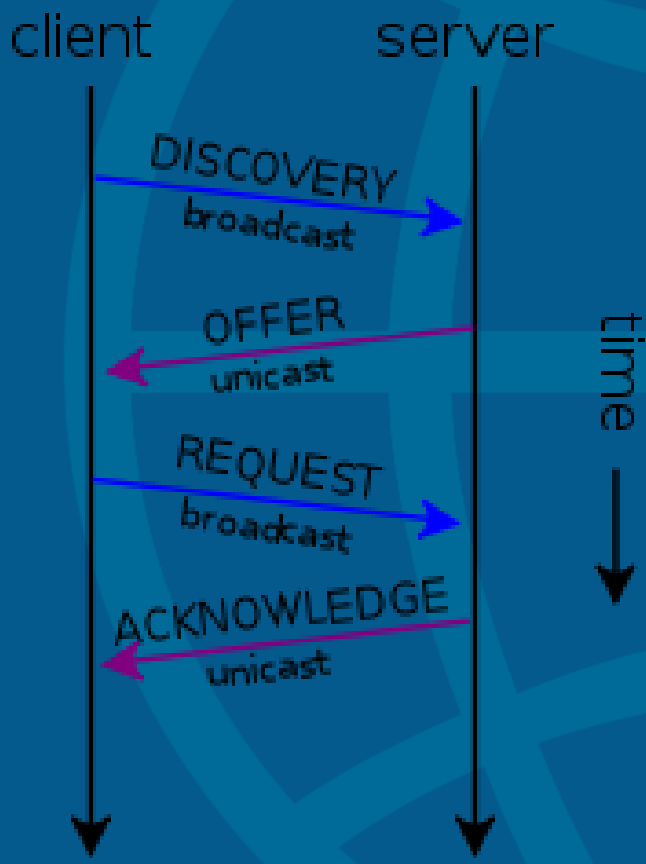
- **DO NOT BE STUPID**
  - Using the contents of these slides on a public network, and/or business network WILL get you into trouble
  - I take no responsibility for misuse of the content in these slides
  - TL;DR
    - Test this in a lab environment, not anywhere else :)

Agenda

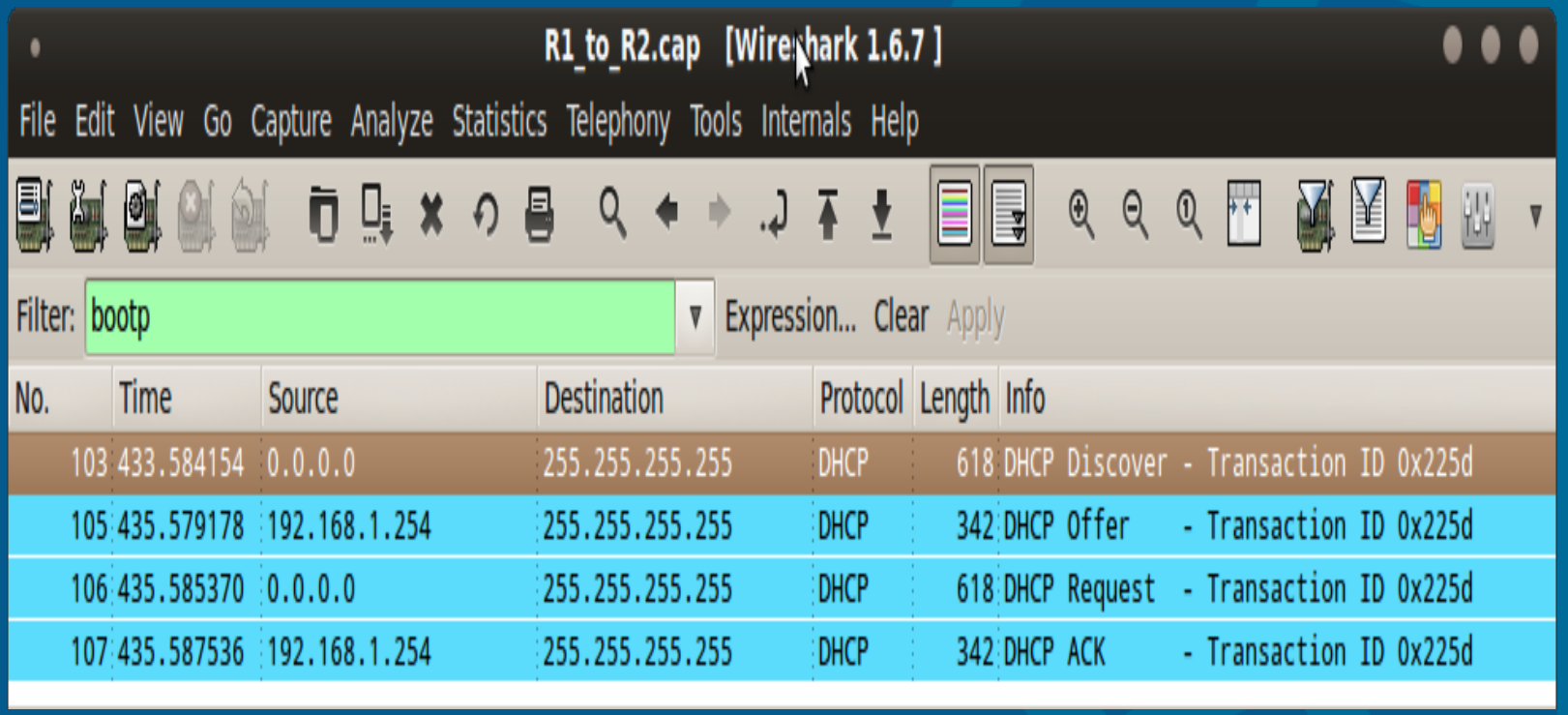
- About Me
- Agenda
- What is DHCP
- DHCP Server
- Proof Of Concept
- Tools
- Demo
- Commands
- What else can we do?
- Counter Measures
- Q & A

What is DHCP (1/2)

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

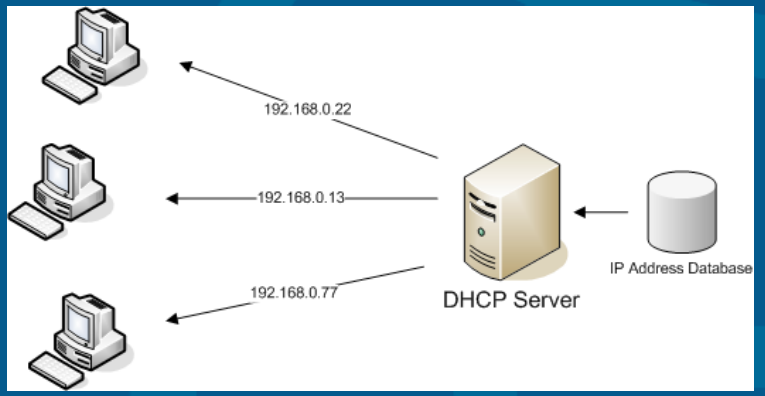


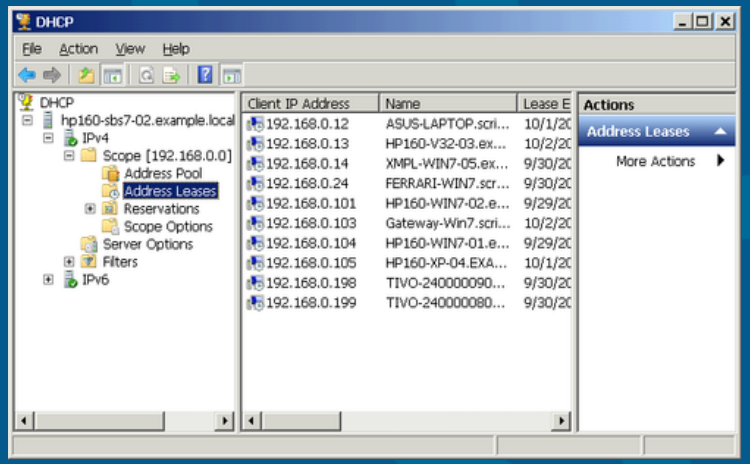
What is DHCP (2/2)



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





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

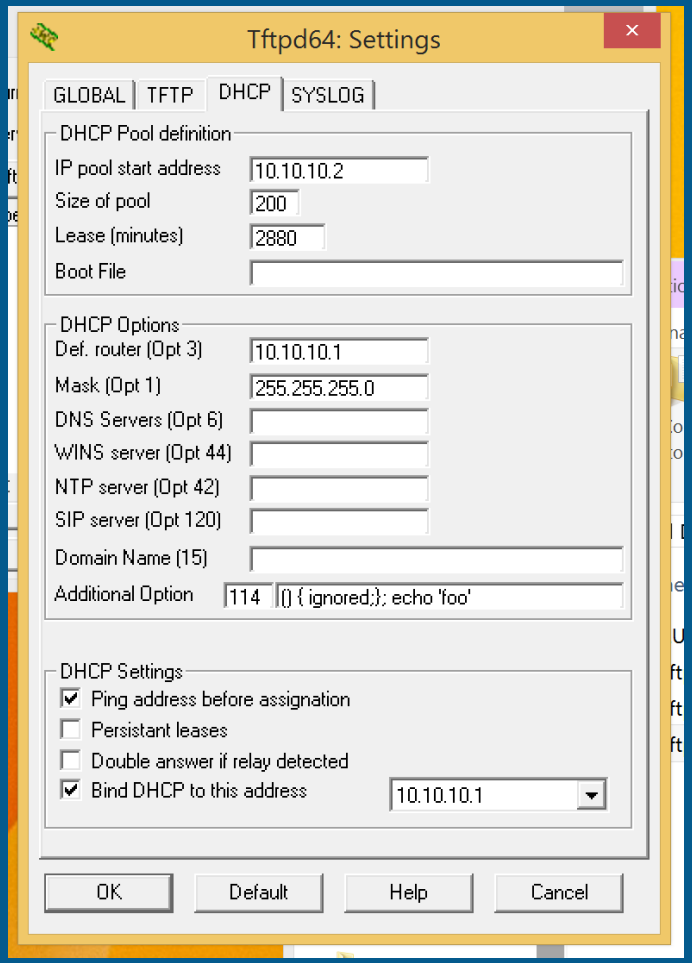
Hostname: kali.bobcorp.local

IP: Dynamic

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?




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