Rogue DHCP server discovery

I Googled rogue IP addresses, and reviewed: https://community.spiceworks.com/topic/1895432-how-to-detect-a-rogue-dhcp-server-in-a-lan, it gave the following which helps for Windows.

Windows

Jon Sellors Oct 28, 2016 at 12:46 AM
Hi,

If you want to find the rogue server, you need to find its IP address and its hardware address. The 2nd address will help you identify where the server is physically on the network. Do this from one of the affected PCs at the command prompt:

Type "ipconfig/all" (without the quotes and press ENTER. Scroll up to where you can see these lines (about 15 lines down):

Lease Obtained. . . . . : 24 October 2016 09:03:38
Lease Expires . . . . : 31 October 2016 08:59:46
Default Gateway . . . . : 192.168.100.254
DHCP Server . . . . : 192.168.100.10

The last 2 entries will probably be different for you. We need to focus on the address for "DHCP Server".

Then type "arp-a" in the command prompt.

Look down the list until you find the same IP address as the DHCP server. Ax example will look like this:

Interface: 192.168.100.46 --- 0xb
  Internet Address   Physical Address   Type
  192.168.100.5   00-08-9b-f2-5b-62   dynamic
  192.168.100.10   00-15-5d-64-3c-01   dynamic
  192.168.100.11   00-15-5d-64-3c-0b   dynamic
  192.168.100.254   b0-b2-dc-70-c9-70   dynamic
  192.168.100.255   ff-ff-ff-ff-ff-ff   static
  224.0.0.1   01-00-5e-00-00-01   static
  224.0.0.22   01-00-5e-00-00-16   static
  224.0.0.251   01-00-5e-00-00-fb   static
  224.0.0.252   01-00-5e-00-00-fc   static
  239.255.255.250   01-00-5e-7f-ff-fa   static
  255.255.255.255   ff-ff-ff-ff-ff-ff   static

We are interested in the hardware address which is the number in the 2nd column:

192.168.100.10   00-15-5d-64-3c-01   dynamic

Now google the first part of this number ie 00-15-5d

This will give you the manufacturer of the "bad" DHCP server.

Try this on your own PC to get the hardware address just to confirm your theory of a rogue DHCP server.

Macintosh and Linux

BTWarp- a works on Linux, andipconfig/all ispossibly replaced byifconfig–a on Linux (although I see nothing about leases in the man page). If you have sudo access then maybe the following will help:

[root@pinger cottrell]# dhclient -d -nw eth0
Internet Systems Consortium DHCP Client 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:50:56:be:ee:30
Sending on LPF/eth0/00:50:56:be:ee:30
Sending on Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4 (xid=0x4d00071d)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8 (xid=0x4d00071d)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 11 (xid=0x4d00071d)

<snip>

```
The follwing works on some systems:

sudo nmap --script broadcast-dhcp-discover -e eth0
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2016-08-16 09:25 UTC
Pre-scan script results:
| broadcast-dhcp-discover:
|   IP Offered: 192.168.14.67
|   DHCP Message Type: DHCPOFFER
|   Server Identifier: 192.168.14.1
|   IP Address Lease Time: 0 days, 0:05:00
|   Subnet Mask: 255.255.255.0
|   Router: 192.168.14.1
|   Domain Name Server: 193.190.127.150
|   Domain Name: maas
|   Broadcast Address: 192.168.14.255
|_  NTP Servers: 91.189.91.157, 91.189.89.199, 91.189.94.4, 91.189.89.198
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.27 sec
```

However at SLAC on pinger I got:

[root@pinger cottrell]# sudo nmap --script broadcast-dhcp-discover -e eth0

Starting Nmap 5.51 (http://nmap.org) at 2017-10-30 11:20 PDT
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:576: 'broadcast-dhcp-discover' did not match a category, filename, or directory
stack traceback:
[C]: in function 'error'
/usr/share/nmap/nse_main.lua:576: in function 'get_chosen_scripts'
/usr/share/nmap/nse_main.lua:1006: in main chunk
[C]: ?

QUITTING!