DHCP Starvation Using Python/Scapy

1.0 Objective

DHCP Starvation Attack is when an attacker binds all usable IP addresses on a DHCP server and performs a Denial of Service on the network. We will be performing this attack on the external router **rtr**. Do not perform this attack on **int-rtr** as results may vary.

Rather than completing the entire DHCP handshake/protocol, we will be stepping in to the last portion by sending a request from a spoofed MAC address and receiving a DHCP ACK back from the router to confirm a 24hr binding to a bogus MAC address. This will need to be done per IP address in the range of 10.10.111.100 - 10.10.111.200

2.0 Lab Setup

Power-on **ONLY** the router **rtr** and no other virtual machine. If **rtr** is not in its default configuration, i.e. you modified it at some point, re-image it. Log in to the router (user = root, password = badpassword). Navigate to the directory **/var/lib/dhcp3/.** Using nano or vim, edit the DHCP leases files: **dhcpd.leases** and **dhcpd.leases~**

Delete all the entries found in these files but not the files themselves or the header (first few lines). This will remove any static or old IP/MAC bindings pre-configured in the router.

You must **REBOOT rtr** using the reboot command. If for any reason in the future you need to edit these files again **you must reboot the router each and every time** for the effects to take place. Once rebooted check to make sure the files have no entries. (You may leave one IP/MAC binding for the Backtrack 5 machine if you so choose.)

3.1 Part A

After you have deleted the entries in the router power on the backtrack5 machine.

Using SCAPY and Python create a script that will 'starve' the DHCP IP address pool (10.10.111.100 - 10.10.111.200).

Hints:
* You only need to complete the last 2 steps of the DHCP protocol in order to bind an IP address so review the DHCP protocol steps.

** If you are getting ACK's for certain IP addresses and not others: check to see if the leases file has a static entry for that IP, make sure all other machines are off as well.

*** If you are getting ACK's for certain IP addresses and not others: packets get dropped on a LAN all the time. Since this is NOT a connection-oriented protocol there is no

automatic retransmission of dropped DHCP packets. The router may drop them due to processing delays or network congestion etc. Keep track of which IP addresses are actually being ACK'd using either wireshark/tcpdump or your script could have a scapy feature for this. It's acceptable if you need to run your script multiple times and/or request specific IP addresses for dropped packets. Also try adding a time delay into your script to allow time for the router to process/respond as well as being able to watch the network traffic at human speeds.

3.2 Part B

Finally, turn on the windows XP machine. Once it's started up open **cmd.exe** and type **ipconfig** to see that the XP machine is unable to get an IP address from the DHCP server. (The IP address and subnetmask should be 0.0.0.0). If you have a routable IP address use the command **ipconfig/release.** The IP address may have been cached in your VM from a previous boot.

Type **ipconfig/renew** to try to get an IP address from the router. You should eventually receive a message saying that the request has timed out. This means the attack was successful.

Occasionally you may encounter a host that has somehow assigned itself an IP address in the 169.254.0.0/16 range. This is a particularly common symptom of Windows machines that have been configured for DHCP but for whatever reason are unable to contact a DHCP server. When a host fails to dynamically acquire an address, it can optionally assign itself a *link-local IPv4 address* in accordance with RFC 3927. Microsoft's term for this is Automatic Private Internet Protocol Addressing (APIPA).

Hints:
* If the XP machine still gets an IP address try using the command: **ipconfig/release** which sends a DHCP message to the router letting it know that IP address is now free. If this does not work you will need to remove the entry manually in the leases file in the router and reboot the router.

** Check the leases file(s) in the router to ensure you've actually bound all the available IP addresses.

4.0 What to Submit

Write a lab report describing your activities and including the following details:

- [50 pts] Your scapy/python script or script(s) to accomplish the attack.
- [20 pts] Your dhcp.leases file from the router with all the bound IP addresses before and after your attack (full screenshot acceptable).
- [15 pts] Screenshots of the victim machine being unable to obtain an IP address.
- [15 pts] Screen shots of your wireshark capture.
- Include any other screenshots or steps in the process you feel like including to demonstrate how your attack works.