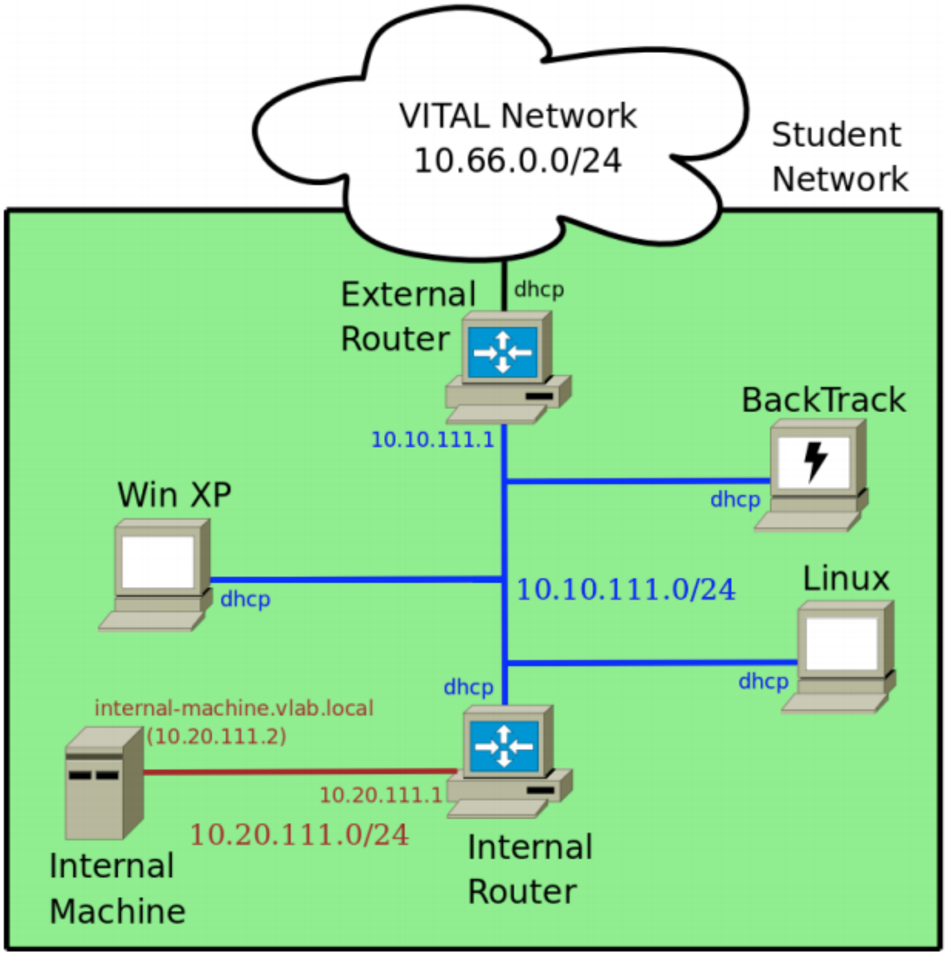
1.0 Objective

DHCP Starvation Attack is when an attacker binds all usable IP addresses on a DHCP server and perform a Denial of Service on the network. This attack is perfoemed on the external router rtr.. 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

Following is the diagram of the VMs used in the implementation of this lab (Note: Not all VMs may be used in this particular implementation.)



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 deleted the entries have been deleted in the router, power on the backtrack5 machine. Save the SCAPY and Python script that will 'starve' the DHCP IP address pool (10.10.111.100 - 10.10.111.200).

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).