Objectives:
Mitigate attacks based on DHCP rogue servers.

Intro:
ChurchBells Inc. is having connectivity issues and needs your help.

The Scenario:
According to the reports, some user PCs within the company are having connectivity issues. What has puzzled ChurchBells Helpdesk staff is that the PCs having trouble are not always the same, they seem to be randomly affected.

According to the reports, the affected PCs are not able to communicate with parts of the network.

As shown in the topology below, ChurchBells Inc. has a very simple network. It relies on a router (CBR1) to route traffic between the internal devices and the outside world (the Internet) by performing NAT before sending packets out to the Internet as RFC 1918 IP addresses are used within ChurchBells’ network.

CBR1 also plays an important role as the DHCP server of the network and thus, it is CBR1’s responsibility to hand out IP addresses and IP configurations.

The user PCs and network devices connect to CBR1 via Cisco switch.

Topology:
Step 1 – Verifying users’ PCs

Once you get to ChurchBells’ office, you decide first to take a look at the user PCs. You ask for a PC which is currently experiencing the problem and a Helpdesk representative shows it to you. A quick inspection reveals that the PC has the wrong IP configuration. More specifically, the PC is connected to 192.168.10.0/24 but has IP information belonging to a different network.

Just to be sure, you try to release and renew the IP configuration via DHCP on the affected PC. Since that specific PC is running a version of MS Windows XP, you issue the following commands from a MS Windows command shell window:

C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix : 
    IP Address. . . . . . . . . . . . . .: 0.0.0.0
    Subnet Mask . . . . . . . . . . . . .: 0.0.0.0
    Default Gateway . . . . . . . . . :

C:\>

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix : 
    IP Address. . . . . . . . . . . . . .: 10.15.20.146
    Subnet Mask . . . . . . . . . . . . .: 255.255.255.0
    Default Gateway . . . . . . . . . : 10.15.20.1

As shown above, even after a release and renew the PC still acquires the wrong IP information. This explains why it is not able to communicate properly. Since it was configured to learn IP information from a DHCP server (CBR1) you decide to go check CBR’s configuration.
Step 2 – Verifying CBR1

You connect your laptop to CBR1’s console port and check the router configuration. Everything looks good. Below is the relevant portion of CBR1’s configuration:

```plaintext
ip dhcp pool CB_POOL
    network 192.168.10.0 255.255.255.0
    default-router 192.168.10.1
    dns-server 24.25.5.150 24.25.5.149
    domain-name cbr-inc.com

interface Serial0/1
    ip address dhcp
    ip nat outside
    ip virtual-reassembly
    no cdp enable

interface FastEthernet0/1
    ip address 192.168.10.1 255.255.255.0
    ip nat inside
    ip virtual-reassembly

ip nat inside source list INTERNS interface Serial0/1 overload

ip access-list standard INTERNS
    permit 192.168.10.0 0.0.0.255
```

Surprisingly, CBR1 has no flaws in its configuration. The only DHCP pool defined was properly configured and CBR1’s interfaces have correct IP addresses configured. You check the cables and the switch configuration without finding any problem. Since nothing wrong was found either in CBR1, in the switch or the cabling and some PCs are still learning wrong information via DHCP, chances are a second DHCP server is running within ChurchBells’ network.
Step 3 – Searching for a rogue DHCP Server

You suspect there is a rogue DHCP server active within ChurchBells’ network and you decide to investigate to be sure.

A rogue DHCP server on a network is a DHCP server which is not under the administrative control of the network staff. It is usually a network device such as a modem or a router connected to the network by a user who is unaware of the consequences, though it can also be knowingly used for network attacks.

A rogue DHCP server can be very dangerous. The DHCP protocol, as many other network protocols, was written with no security concerns. No authentication or authorization takes place during an exchange between a DHCP server and a DHCP client, so the server has no way of knowing if the client requesting the address is a legitimate client on the network, and the client has no way of knowing if the server that assigned the address is a legitimate DHCP server. The presence of rogue clients and servers on your network can create all kinds of problems.

For example, a rogue DHCP server could provide legitimate clients with bogus TCP/IP information that prevents the clients from communicating on the network. A denial of service (DoS) condition then results, and users are unable to connect to network resources to perform their work. A rogue DHCP server could simply be set up by gaining physical access to your network through social engineering and plugging in a laptop configured as a DHCP server.

Another scenario might involve an attacker compromising a client computer on your network and installing software that repeatedly requests new IP addresses using spoofed MAC addresses until the entire pool of addresses in your DHCP server's scope is leased. When this happens, legitimate clients that boot onto the network cannot acquire an address and again users are unable to access the network and cannot do their work.

A more serious attack takes place when an attacker modifies the server to assign incorrect DNS settings to clients. While the client would still be able to access the network (making it hard for the user to detect a problem) all DNS queries would be redirected to rogue or hijacked DNS servers. This bogus DNS server could then redirect clients to hostile websites, designed to imitate financial institutions websites as banks or credit cards. The user, led to believe such websites were authentic, would end up exposing very sensitive information.

As a last example, an attacker could modify the server to assign the address of the attacker's own machine as the default gateway, which results in outbound client traffic being redirected to the attacker's machine, which captures and reads the traffic and forwards it to the real default gateway. The result is exposure of sensitive business information without users even being aware of what is happening.
Question

If a client receives more than one DCHPOFFER packet, which one does it take?

**Answer:** The client will most likely take the first offer presented to it, with a few exceptions. Usually, in situations like that, the rogue DHCP server located among the DHCP clients (one of the user PCs running a DHCP server) is picked by the clients because it is “closer” than the valid DHCP server.

You explain your suspicions to the Helpdesk staff and learn from them that a new computer was added to the network. It has Linux running on it and according to them the problems started more or less at the same time they added that computer to the network. Upon your request, you are taken to that specific computer by the Helpdesk team.

You plug your own laptop into ChurchBells’ network and start Wireshark, a traffic analyzer software. With Wireshark running on your laptop, you release/renew the IP address information once more in the affected PC.

On the traffic analyzer output window you can see that two DHCP servers responded to the request: CBR1 and an unidentified server.

You login to the Linux box and find DHCP running on it. To quickly ensure whether or not the new installed Linux box is the source of the problem, you unplug its network cable and release/renew the IP configuration in the same user PC used before. Once more the traffic analyzer running on your laptop shows DHCP responses but only from CBR1 this time. You repeat the test a few times to ensure no rogue DHCP servers are answering clients’ requests and ask the helpdesk team to “clean up” the Linux machine before reconnecting it to the network.

Even though the problem is solved, you decide to take some security measures to prevent rogue DHCP servers to connect to the network in the future. You decide to configure a Cisco proprietary protocol in the switch called **DHCP Snooping**.

**DHCP Snooping** is a Cisco proprietary feature that provides a higher level of DHCP security by defining trusted and untrusted ports and “looking into” DHCP packets while they cross the switch. Ports where legal DHCP servers are not expected (as ports connected to hosts, printers, etc) are tagged as “untrusted” while switch ports connected to legal DHCP servers are tagged as “trusted”. Since there is no reason for a host to send DCHPOFFER and/or DHCPACK messages, DHCP Snooping watches every DHCP message crossing the switch. If a DCHPOFFER or a DHCPACK is detected coming from a host (untrusted port), the switch will discard the message. Such messages are only forwarded if they come from trusted ports.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.
Note: DHCP Snooping has more features than mentioned here. For instance, it is able to check the frame source MAC address to ensure it is the same MAC address listed within the DHCP packet field to avoid DHCP DoS. For more information about DHCP Snooping, check:


You connect to the switch’s console port and configure DHCP snooping in VLAN 10 – the only VLAN used by ChurchBells’ network. The commands are listed below for future reference.

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw1(config)# ip dhcp snooping
Sw1(config)# ip dhcp snooping vlan 10
Sw1(config)# ip dhcp snooping information option
Sw1(config-if)# ip dhcp snooping trust
Sw1(config-if)# ip dhcp snooping limit rate 100
Sw1(config)# end
Sw1# show ip dhcp snooping
DHCP Snooping is configured on the following VLANs:
  10
Insertion of option 82 information is enabled.
<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet2/1</td>
<td>yes</td>
<td>10</td>
</tr>
<tr>
<td>FastEthernet2/2</td>
<td>yes</td>
<td>none</td>
</tr>
<tr>
<td>FastEthernet3/1</td>
<td>no</td>
<td>20</td>
</tr>
</tbody>
</table>
Sw1#