

Forum:[Hack Forums](#)

Thread: [DHCP Rogue Server](#)

Archive - September 2, 2010, 10:21 am

Setting up a Rogue DHCP Server is one technique that an attacker can use to gain access to network traffic. This is achieved by spoofing responses that would normally be sent by an authorised DHCP server. The authorised DHCP server will also reply to the client DHCP requests, but if the rogue device is closer (less hops) to the client, its reply to the client may arrive first.

[img]http://www.hakipedia.com/images/RogueDHCPattack.png[/img]

Severity

Moderately High.
Exploit Likelihood

Moderate.
Description

A rogue DHCP server is a DHCP server set up on a network by an attacker, or by an unaware user, and is not under the control of network administrators. An accidental rogue device is commonly a modem with DHCP capabilities which a user has attached to the network unaware of the consequences of doing so. Rogue DHCP servers are also commonly used by attackers for the purpose of network attacks such as Man in the Middle, Sniffing, and Reconnaissance attacks.

Man in the Middle Attacks

Man in the Middle DHCP attacks can be used to forge network resources. The Rogue DHCP reply will offer an IP address and information that may designate the attackers machine as the default gateway or Domain Name System (DNS) server. If the attacker is designated default gateway, any clients with addresses assigned from the Rogue DHCP Server will forward packets to the attacking device, which may in turn send them to the desired destination, or possibly elsewhere. If the attacker also designates it's own Rogue DNS Server(s), they may design phishing websites to obtain other confidential information, such as credit card details and passwords.

Attack Vector

[img]http://www.hakipedia.com/images/RogueDHCP.png[/img]

The Yersinia Rogue DHCP attack panel

Yersinia is a GNU/Linux framework that takes advantage of some of the weaknesses in different network protocols. It can be used for analyzing and testing deployed networks and systems. To use Yersinia for a Rogue DHCP Server, the following steps may be followed:

1. Start Yersinia via the command line by typing: yersinia -l.
2. Select a NIC you wish to use by pressing "i".
3. Load DHCP mode by pressing the "g" key, then select DHCP mode.
 1. Press the "x" button to open the attacks menu.
 2. Press "2" to create the Rogue DHCP server.

4. Set the parameters to match your Rogue DHCP server and press Enter.
5. Use Wireshark or similar tool to sniff all packets.

Mitigation

Cisco Catalyst switches can eradicate Rogue DHCP Server attacks using DHCP Snooping.

To enable DHCP Snooping on a Cisco IOS switch, follow these steps:

```
switch(config)# ip dhcp snooping
!Enables DHCP Snooping globally!
switch(config)# ip dhcp snooping vlan {,}
!Enables DHCP Snooping for Specific VLANs!
switch(config-if)# ip dhcp snooping trust
!Sets the interface to trusted state; can then pass DHCP replies!
switch(config-if)# ip dhcp snooping limit rate
!Sets rate limit for DHCP Snooping!
```

These attackers are known as "man-in-the-middle" attacks, and they may go virtually undetected if the intruder intercepts the data flow through the network, and forwards the packets off to their original destination as requested.

Regards,
Archive