DHCP - Rogue DHCP

Historique

<Intemporel>

Description

Rogue DHCP server attacks are gaining popularity but can be mitigated. The hacker sets up a rogue DHCP server and creates an IP address conflict by broadcasting a duplicate IP address. Hackers infiltrate a network by attacking the wireless router, which they do with ARP poisoning in order to inject rogue packets into the stream of data being processed by the router. This ingenious hack gives hackers continuous access to networks via proxy servers and spam mailers, making it difficult for IT professionals to stop or even detect a cyber attack from happening. The hacker then listens for incoming connections and selectively responds with malicious messages such as fake authentication requests or viruses that play havoc on unsuspecting users' devices.

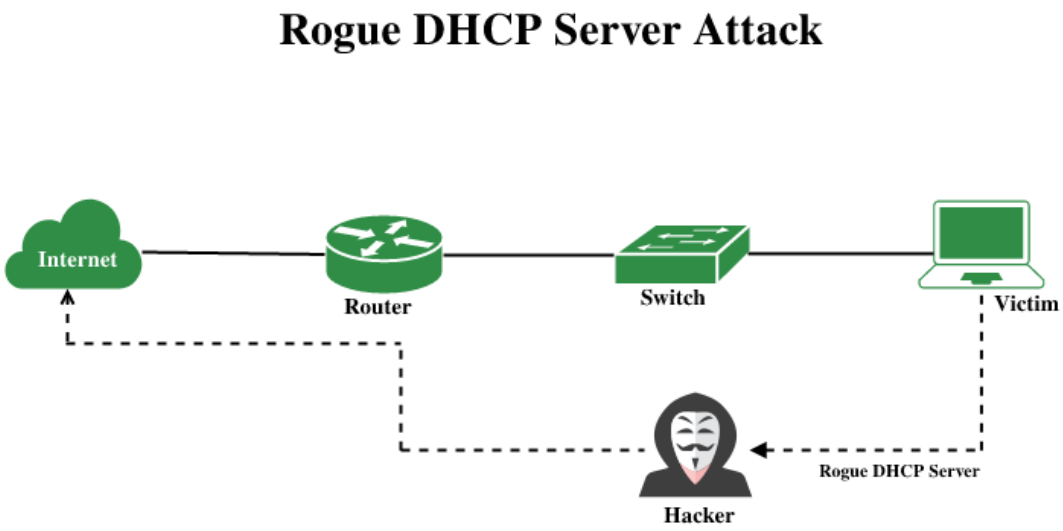
Rogue DHCP Server Attack:

The hacker sets up a rogue DHCP server and creates an IP address conflict by broadcasting a duplicate IP address. Hackers infiltrate a network by attacking the wireless router, which they do with ARP poisoning in order to inject rogue packets into the stream of data being processed by the router. This ingenious hack gives hackers continuous access to networks via proxy servers and spam mailers, making it difficult for IT professionals to stop or even detect a cyber attack from happening. The hacker then listens for incoming connections and selectively responds with malicious messages such as fake authentication requests or viruses that play havoc on unsuspecting users' devices.

Rogue DHCP server attacks are gaining popularity but can be mitigated. The hacker sets up a rogue DHCP server and creates an IP address conflict by broadcasting a duplicate IP address. The

hacker will then try to get computers to connect to the rogue device instead of the router. Once that’s accomplished, the hacker can do just about anything he wants, ranging from stealing information to installing malicious software on your computer in order to control it remotely. A government official speaking at a recent press conference said that Iran had set up fake wireless networks in countries like Iraq and Afghanistan, so they could monitor communications easily while people were using Wi-Fi hotspots.

Schéma



Prevention:

- Always use trusted WLAN hotspots.
- Enable MAC filtering/SSID broadcast on your wireless network as much as possible. This will help prevent your network from being accessed by unwanted users.

- Update the firmware and applications whenever a security update is available for them (especially firmware). This will close loopholes and patch vulnerabilities in your wireless network that hackers can exploit to gain access to your devices or the corporate network behind them.
- Turn off file sharing (CIFS/SMB) on your wireless bridges, routers, etc.
- Log and monitor all ingress/egress traffic.
- Log all DHCP lease events on your wireless network.
- If the rogue DHCP server is accessed from inside the network, then restrict the IP addresses that have access to your DHCP server and/or reset the MAC address on your router/firewall, so it only accepts packets from that specific MAC address as an authorized device that is allowed to connect to your network (stateful packet inspection).
- Change default passwords (always choose a complex password) for your wireless equipment such as routers, access points, etc.
- Enable Secure NAT on the Router or Firewall in order to prevent unwanted users from accessing internal servers behind it

Important points:

- The hacker will first use an attack on the wireless router with MAC address spoofing and ARP poisoning.
- The hacker will then try to get computers to connect to the rogue device instead of the router. Once that's accomplished, the hacker can do just about anything, ranging from stealing information to installing malicious software on your computer in order to control it remotely. This can include:
  -Stealing data -Downloading/Uploading viruses -Spyware -Hacking into your computer -Conducting man-in-the-middle attacks against you.
- Hackers use fake websites (often phishing) in order to get users to log in to their accounts illegally with their social security numbers and passwords.

Conclusion:

Rogue DHCP server attacks can result in a great deal of damage to your network and the organization. Whether it's sensitive data or just unwanted visitors, you need to take this seriously and make sure you have secure access control strategies in place.

Sources

[What is Rogue DHCP Server Attack? - GeeksforGeeks]

Revision #1
Created 2026-09-08 06:51:09 UTC by Olivier
Updated 2026-09-08 06:54:01 UTC by Olivier