Brady Venneman

DHCP Snooping Lab

4/17/2024

The most valuable feature of this lab was the hands-on experience with configuring DHCP snooping to mitigate man-in-the-middle and DHCP starvation attacks. By setting up a rogue DHCP server and observing how DHCP snooping prevents it from assigning IPs, the lab provided a clear understanding of how this security feature protects a network. In preparation for this lab, I reviewed the concepts of DHCP servers, DHCP snooping, and the different types of DHCP attacks. This helped me understand the purpose of each configuration step. For future labs, I would consider creating a more detailed outline of the steps involved and researching any specific commands or configurations beforehand. This would allow me to be more efficient and focus on understanding the underlying concepts during the lab itself.

This experience solidified my understanding of DHCP snooping and its role in network security. I learned how to configure a switch to differentiate between trusted and untrusted DHCP sources, limit the rate of DHCP packets, and ensure that clients receive valid IP addresses from the legitimate DHCP server. For someone preparing for this lab for the first time, I would recommend familiarizing themselves with DHCP basics, DHCP snooping concepts, and the commands used for configuration. It would also be helpful to understand the different types of DHCP attacks that DHCP snooping mitigates.

1.1: A DHCP server automatically assigns IP addresses, subnet masks, default gateways, and other configuration parameters to devices on a network. It does this by responding to DHCP requests broadcast by devices seeking an IP address.

1.2: 192.168.123.1

1.4: 192.168.123.2. it was serviced from the gateway 192.168.123.253

2.1:

2.2: A screenshot of a computer

Description automatically generated

2.3: A man-in-the-middle attack is a cyberattack where the attacker secretly relays and potentially alters communication between two parties who believe they are talking directly to each other. The attacker intercepts data flowing between the victim and the legitimate source, allowing them to steal information or manipulate the data.

3.1: limits the rate of incoming DHCP packets to 10 per second. This helps mitigate DHCP starvation attacks where an attacker floods the network with DHCP requests, overwhelming the legitimate DHCP server and preventing clients from obtaining valid IP addresses.

3.4: A screen shot of a computer

Description automatically generated

3.5: displays the snooping configuration, with the trusted and untrusted ports

3.6: A DHCP starvation attack is a denial-of-service attack where the attacker floods the network with DHCP requests, overwhelming the legitimate DHCP server and preventing clients from obtaining valid IP addresses.