XFLOW RESEARCH

DHCP Starvation and Prevention Techniques:

Dec 21, 2023

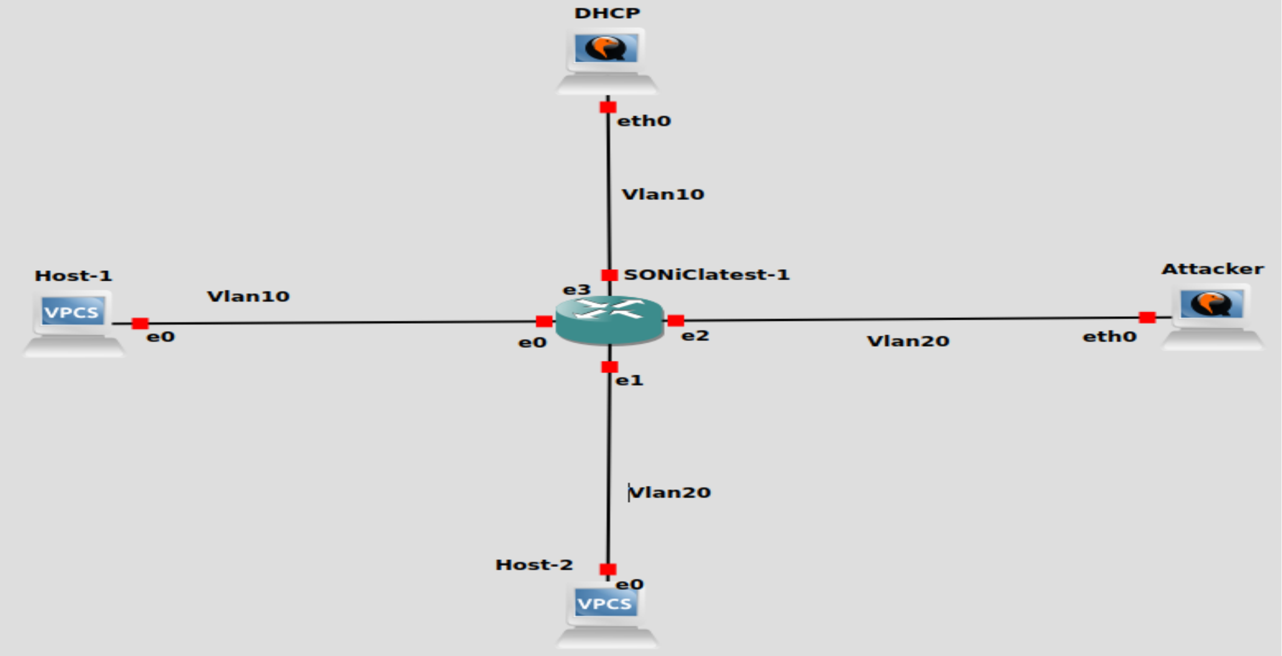
Dynamic Host Configuration Protocol (DHCP) is a vital component in network management, automating the assignment of IP addresses and related configuration information to devices. However, with its importance comes the potential for abuse. DHCP starvation attacks pose a significant threat to network stability by depleting the available IP address pool and disrupting network operations.

DHCP Starvation: A Stealthy Threat

In a DHCP starvation attack, malicious actors flood the DHCP server with a barrage of DHCP requests, overwhelming the server's capacity to respond promptly. By doing so, attackers aim to exhaust the available IP address pool, causing legitimate devices to be denied access to the network. This can lead to network downtime, connectivity issues, and a potential security breach as unauthorized devices may gain access

Anatomy of DHCP Starvation Attack

To illustrate this threat, consider the following topology , where an attacker exploits vulnerabilities in the DHCP protocol to flood the server with requests, creating chaos within the network. Attack code is given in the reference link below.



Prevention Techniques: Binding Table As a Shield

To fortify the network against DHCP starvation attacks, implementing preventive measures is crucial. One effective technique involves the use of binding tables in DHCP relays to restrict the impact of the attack on untrusted ports.

Binding Table: Guardian of DHCP

A binding table is a record-keeping mechanism that associates IP addresses with corresponding MAC addresses, Lease(sec), Type, Vlan and Interface. By incorporating binding tables into DHCP relays on the network, administrators gain the ability to filter and control DHCP requests, thwarting malicious attempts to exhaust the IP address pool.

DHCP switch
sari cheezn
iptable rule
input
screen shot
behavior in a para graph

Reference

https://github.com/yoelbassin/DHCP-starvation/blob/main/dhcpStarvation.py