DYNAMIC HOST CONFIGURATION PROTOCOL VULNERABILITIES

A.L. Smeer, A.S. Sunil Lal, E.S. Belousova

Dynamic Host Configuration Protocol (DHCP) is a network protocol which is used on UDP/IP networks. A DHCP Server dynamically assigns an IP-address and other network configuration parameters to each device in a network, so that they can communicate with other networks.

A pair of vulnerabilities in the DHCP client in Windows 10 and Windows Server 2019 allows attackers to execute code remotely, according to researchers at security firm Positive Technologies [1]. An attacker configures a DHCP server on their computer. Then the attacker waits for a vulnerable Windows 10 computer to ask for a renewal of IP address lease, which usually happens every few hours. By sending this invalid response, the attacker can obtain the rights of an anonymous user on the victim computer. It provides a useful entry point for continued escalation by pairing with other vulnerabilities. Nominally, attackers must be on the same network as the targeted system, though for organizations where DHCP Relay is used to use external DHCP servers, this limitation can be bypassed.

The aim of the work is to research DHCP vulnerability in Cisco Packet Tracer.

Based on simulation we can highlight the following features of DHCP vulnerability exploiting. Attacker introduces a new system (the laptop) in the network and then requests an IP-address, as the DHCP protocol will assign an IP-address automatically. Then attacker can see that an IP-address has been assigned to his device and he can change the MAC-address of this device, because the DHCP-server detects it as another device, i. e. a new device. So, it gets assigned a new IP address. In other words, attacker does MAC-spoofing attack. So, the DHCP pool of the server will be exhausted, the server will not respond to clients messages and it will simply drop clients replies. In this case, the attacker configures his device as DHCP-server. It receives the clients message and responds to it by giving IP-addresses, the IP-address of the DNS server and the default router. Replacing the default gateway attacker will cause all traffic to pass through his device, which will allow the attacker to get personal data of users. Spoofing a DNS server (DNS-spoofing) will result in users being given a nonreal IP-address of real web resources, which can be used for extortion.

In the continuation of our work, recommendations for protecting corporate networks from the vulnerability of the DHCP protocol will be compiled and tested.

Literature

1. Sanders, J. Windows 10 DHCP vulnerability allows for remote code execution [Electronic resource]. – 2021. – Access mode: https://www.techrepublic.com/article/windows-10-dhcp-vulnerability-allows-for-remote-code-execution/ – Date of access: 30.03.2021.