УДК 004.056

RELEVANCE OF HSRP SECURITY

Milanka I.Yu., Volotka V.S.
Scientific Supervisor - Senior Lecturer Volotka V.S.
Kharkiv National University of Radio Electronics, Faculty of Infocommunication,
Kharkiv, Ukraine
e-mail: ihor.milanka@nure.ua.

Currently, there are a lot of threats that can disrupt the proper functioning of information and communication systems and lead to their denial of service. If this happens, any company risks significant material and reputational losses. That is why it is so important to constantly develop new and more advanced methods of protecting information and communication systems, which can help increase the level of fault tolerance of corporate networks in relation to external influence from third parties and sources.

The FHRP (First Hop Redundancy Protocol) family of protocols is a crucial element in the topology of any organization's network and significantly impacts its security level [1]. In the context of security, the role of the FHRP family of protocols includes:

- Ensuring network continuity (fault tolerance);
- Performing load balancing to effectively distribute network resources and prevent equipment overload;
- Protection against attacks aimed at network service disruption (e.g., DoS and DDoS);
- Organizing the process of network traffic authentication and filtering.

The main advantage of the HSRP (Hot Standby Router Protocol) protocol (as well as all other protocols in the FHRP family) is that if the active router fails and the standby router takes its place, the network continues to serve subscribers during this process, and user devices do not disconnect from it. This is because all devices in the HSRP group are configured with identical virtual IP and MAC addresses. Despite being used for providing fault-tolerant routing within a corporate network, the HSRP protocol also has its own vulnerabilities [2].

These vulnerabilities can be exploited through the following types of attacks:

- Traffic interception attack;
- Spoofing attack;
- Denial of Service (DoS) attack targeting router overload with traffic;
- Password retrieval attack targeting router passwords compromise;
- Attack on HSRP v1 protocol.

Each of the mentioned attacks is utilized by malicious actors to exploit the most common vulnerabilities of the HSRP protocol. The "Traffic interception" attack aims to intercept HSRP packets transmitted between routers of the same group openly. The "Spoofing" attack allows attackers to forge HSRP packets in a way that they will transmit compromised virtual IP addresses and the desired priority values to routers. This attack can lead to destabilization of the corporate network operation and enable the attacker to designate a rogue router as "active" by altering priority values for all legitimate network devices. Through a DoS attack, the attacker can overload routers and disrupt the operation of the entire network. The DoS attack is executed by sending a large number of false HSRP packets to the network devices configured with the HSRP protocol.

The "Password retrieval" attack targets routers configured with the HSRP protocol to intercept authentication passwords and gain unauthorized access to the configuration of network devices.

The last type of attack is associated with vulnerabilities in the HSRP v1 protocol. In the first version of HSRP, it is possible to spoof HSRP packets and perform a DoS attack. As a rule, it is generally recommended not to use the first version of the HSRP protocol [3].

To ensure the necessary level of security for the HSRP, the following methods can be utilized:

1. Use of HSRP v2: deploying the second version of the HSRP protocol is recommended as it offers more advanced security mechanisms compared to HSRP v1.
2. Authentication of HSRP packets.
3. Filtering HSRP traffic: configure HSRP traffic filtering on network equipment to only allow HSRP traffic from trusted sources, thereby mitigating vulnerabilities associated with adding rogue routers to the HSRP group (e.g., "Traffic interception" and "Spoofing" attacks).
4. Restrict access to HSRP configuration: minimize unauthorized dissemination of HSRP technical information beyond the corporate network and among unauthorized individuals.
5. Encryption of traffic: organize encryption of HSRP traffic by creating and configuring a dedicated VPN topology utilizing the Internet Protocol Security (IPSec) protocol.
6. Monitoring: set up a monitoring system to track suspicious activity propagated through HSRP traffic and alert information security experts or system administrators about potential network attacks. Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) are often used for network monitoring.
7. Software updates.
8. Physical access control.
9. Employee training.

The aforementioned methods will significantly enhance the security level of the HSRP and the corporate network as a whole. It is important to remember, however, that all the described protection methods are not guarantees of complete network and HSRP protocol security. Security is an ongoing process that requires continuous monitoring, adaptation to emerging threats, and implementation of additional measures as needed.

References:

1. Barney N., Lutkevich B. What is Network Security? 2022. URL: https://www.techtarget.com/searchnetworking/definition/network-security.

2. HSRP MD5 Authentication. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/fhp-hsrp-md5.pdf.

3. 10 Common Internet Security Threats and How to Avoid Them. URL: https://velecor.com/10-common-internet-security-threats-and-how-to-avoid-them/.