**GLBP & HSRP Attacks**

## FHRP Hijacking Overview

### Insights into FHRP

FHRP is designed to provide network robustness by merging multiple routers into a single virtual unit, thereby enhancing load distribution and fault tolerance. Cisco Systems introduced prominent protocols in this suite, such as GLBP and HSRP.

### GLBP Protocol Insights

Cisco's creation, GLBP, functions on the TCP/IP stack, utilizing UDP on port 3222 for communication. Routers in a GLBP group exchange "hello" packets at 3-second intervals. If a router fails to send these packets for 10 seconds, it is presumed to be offline. However, these timers are not fixed and can be modified.

### GLBP Operations and Load Distribution

GLBP stands out by enabling load distribution across routers using a single virtual IP coupled with multiple virtual MAC addresses. In a GLBP group, every router is involved in packet forwarding. Unlike HSRP/VRRP, GLBP offers genuine load balancing through several mechanisms:

* **Host-Dependent Load Balancing:** Maintains consistent AVF MAC address assignment to a host, essential for stable NAT configurations.
* **Round-Robin Load Balancing:** The default approach, alternating AVF MAC address assignment among requesting hosts.
* **Weighted Round-Robin Load Balancing:** Distributes load based on predefined "Weight" metrics.

### Key Components and Terminologies in GLBP

* **AVG (Active Virtual Gateway):** The main router, responsible for allocating MAC addresses to peer routers.
* **AVF (Active Virtual Forwarder):** A router designated to manage network traffic.
* **GLBP Priority:** A metric that determines the AVG, starting at a default of 100 and ranging between 1 and 255.
* **GLBP Weight:** Reflects the current load on a router, adjustable either manually or through Object Tracking.
* **GLBP Virtual IP Address:** Serves as the network's default gateway for all connected devices.

For interactions, GLBP employs the reserved multicast address 224.0.0.102 and UDP port 3222. Routers transmit "hello" packets at 3-second intervals, and are considered non-operational if a packet is missed over a 10-second duration.

### GLBP Attack Mechanism

An attacker can become the primary router by sending a GLBP packet with the highest priority value (255). This can lead to DoS or MITM attacks, allowing traffic interception or redirection.

### Executing a GLBP Attack with Loki

[Loki](https://github.com/raizo62/loki_on_kali) can perform a GLBP attack by injecting a packet with priority and weight set to 255. Pre-attack steps involve gathering information like the virtual IP address, authentication presence, and router priority values using tools like Wireshark.

Attack Steps:

1. Switch to promiscuous mode and enable IP forwarding.
2. Identify the target router and retrieve its IP.
3. Generate a Gratuitous ARP.
4. Inject a malicious GLBP packet, impersonating the AVG.
5. Assign a secondary IP address to the attacker's network interface, mirroring the GLBP virtual IP.
6. Implement SNAT for complete traffic visibility.
7. Adjust routing to ensure continued internet access through the original AVG router.

By following these steps, the attacker positions themselves as a "man in the middle," capable of intercepting and analyzing network traffic, including unencrypted or sensitive data.

For demonstration, here are the required command snippets:

# Enable promiscuous mode and IP forwarding

sudo ip link set eth0 promisc on

sudo sysctl -w net.ipv4.ip\_forward=1

# Configure secondary IP and SNAT

sudo ifconfig eth0:1 10.10.100.254 netmask 255.255.255.0

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Adjust routing

sudo route del default

sudo route add -net 0.0.0.0 netmask 0.0.0.0 gw 10.10.100.100

Monitoring and intercepting traffic can be done using net-creds.py or similar tools to capture and analyze data flowing through the compromised network.

### Passive Explanation of HSRP Hijacking with Command Details

#### Overview of HSRP (Hot Standby Router/Redundancy Protocol)

HSRP is a Cisco proprietary protocol designed for network gateway redundancy. It allows the configuration of multiple physical routers into a single logical unit with a shared IP address. This logical unit is managed by a primary router responsible for directing traffic. Unlike GLBP, which uses metrics like priority and weight for load balancing, HSRP relies on a single active router for traffic management.

#### Roles and Terminology in HSRP

* **HSRP Active Router**: The device acting as the gateway, managing traffic flow.
* **HSRP Standby Router**: A backup router, ready to take over if the active router fails.
* **HSRP Group**: A set of routers collaborating to form a single resilient virtual router.
* **HSRP MAC Address**: A virtual MAC address assigned to the logical router in the HSRP setup.
* **HSRP Virtual IP Address**: The virtual IP address of the HSRP group, acting as the default gateway for connected devices.

#### HSRP Versions

HSRP comes in two versions, HSRPv1 and HSRPv2, differing mainly in group capacity, multicast IP usage, and virtual MAC address structure. The protocol utilizes specific multicast IP addresses for service information exchange, with Hello packets sent every 3 seconds. A router is presumed inactive if no packet is received within a 10-second interval.

#### HSRP Attack Mechanism

HSRP attacks involve forcibly taking over the Active Router's role by injecting a maximum priority value. This can lead to a Man-In-The-Middle (MITM) attack. Essential pre-attack steps include gathering data about the HSRP setup, which can be done using Wireshark for traffic analysis.

#### Steps for Bypassing HSRP Authentication

1. Save the network traffic containing HSRP data as a .pcap file.

tcpdump -w hsrp\_traffic.pcap

1. Extract MD5 hashes from the .pcap file using hsrp2john.py.

python2 hsrp2john.py hsrp\_traffic.pcap > hsrp\_hashes

1. Crack the MD5 hashes using John the Ripper.

john --wordlist=mywordlist.txt hsrp\_hashes

**Executing HSRP Injection with Loki**

1. Launch Loki to identify HSRP advertisements.
2. Set the network interface to promiscuous mode and enable IP forwarding.

sudo ip link set eth0 promisc on

sudo sysctl -w net.ipv4.ip\_forward=1

1. Use Loki to target the specific router, input the cracked HSRP password, and perform necessary configurations to impersonate the Active Router.
2. After gaining the Active Router role, configure your network interface and IP tables to intercept the legitimate traffic.

sudo ifconfig eth0:1 10.10.100.254 netmask 255.255.255.0

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

1. Modify the routing table to route traffic through the former Active Router.

sudo route del default

sudo route add -net 0.0.0.0 netmask 0.0.0.0 gw 10.10.100.100

1. Use net-creds.py or a similar utility to capture credentials from the intercepted traffic.

sudo python2 net-creds.py -i eth0

Executing these steps places the attacker in a position to intercept and manipulate traffic, similar to the procedure for GLBP hijacking. This highlights the vulnerability in redundancy protocols like HSRP and the need for robust security measures.

## References

* <https://medium.com/@in9uz/cisco-nightmare-pentesting-cisco-networks-like-a-devil-f4032eb437b9>