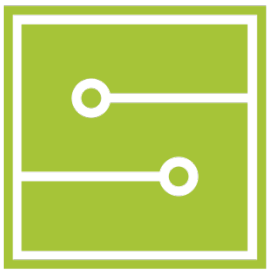
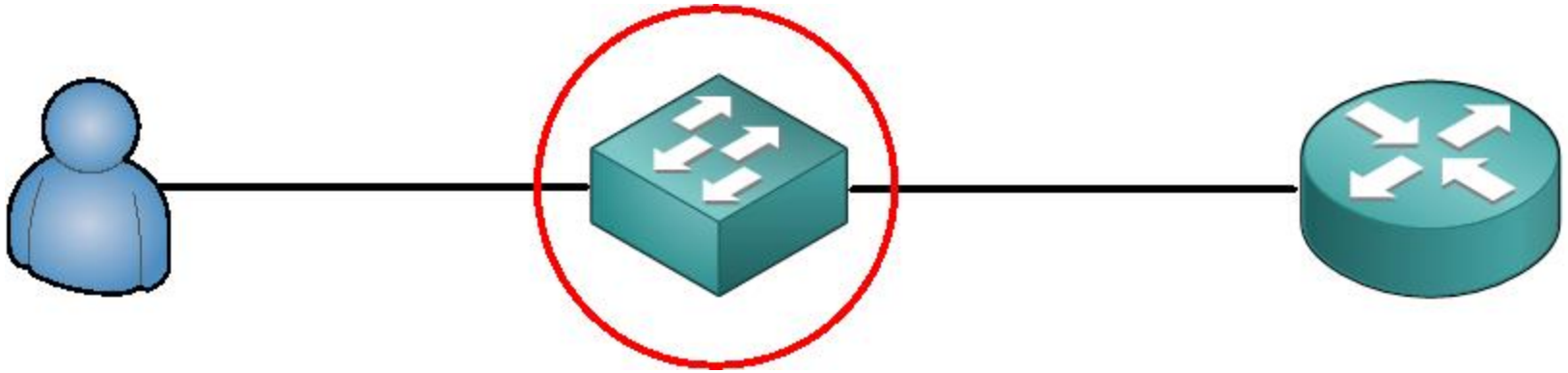


Simonyi Károly Szakkollégium

(IPv6) First Hop Security

Szummer Mihály
<szummer.mihaly@simonyi.bme.hu>

First Hop



Problémák

- 1. Router (default gateway) hijack/DoS
- 2. IP cím lopás
- 3. IP cím hamisítás

IPv4

IPv4: Router hijack/DoS – DHCP Snooping

- MAC – IPv4 – VLAN – Interface adatbázis előállítása
- DHCP szerver üzenetek szűrése (pl. DHCP Offer)

- sw(config)#ip dhcp snooping vlan 1

- És ha nincs DHCP?
- sw(config)#ip source binding 0000.1111.2222 vlan 10 2.2.2.2 interface Gi1/1

IPv4: IP cím lopás – Dynamic ARP Inspection

- A DHCP Snooping adatbázisnak nem megfelelő ARP üzenetek szűrése az üzenetben szereplő IP-MAC alapján.

- sw(config)#ip arp inspection vlan 1

IPv4: cím hamisítás – IP Source Guard

- A DHCP Snooping adatbázisnak nem megfelelő IP csomagok szűrése forrás cím alapján.

- sw(config-if)#ip verify source vlan dhcp-snooping

IPv6

IPv6

- #1: Router Advertisement Guard
- #2: IPv6 Snooping
  - IPv6 ND Inspection
  - IPv6 Address Glean
- ##: DHCPv6 Guard
- #3: IPv6 Source Guard

Router Advertisement Guard

- Router Advertisement-ek szűrése különböző feltételek alapján (forrás, prefix, preference, flag-ek, hop-limit)
- Korábbi megoldások: Port ACL, RA-guard lite
- **RA-guard**

- L2-es szeparálás (VLAN, PVLAN)

Router Advertisement Guard

RA-guard lite:
sw(config-if)#ipv6 nd raguard

RA-guard:
sw(config)#ipv6 nd raguard policy MYPOLICY
sw(config-nd-raguard)#device-role host ! device-role router
sw(config-nd-raguard)#match ra prefix-list MYPREFIX

sw(config-if)#ipv6 nd raguard attach-policy MYPOLICY
vagy
sw(config)#vlan configuration 10
sw(config-vlan-config)#ipv6 nd raguard attach-policy MYPOLICY

IPv6 Snooping

- Address Glean
- NDP Inspection

IPv6 Address Glean

- IPv6 bindig table: IPv6-MAC-Interface-VLAN

- ND üzenetekből => IPv6 binding table
- DHCP üzenetekből => IPv6 binding table

- És ha statikus?
  - ipv6 neighbor binding vlan 10 fe80::20 interface gi1/1 aabb.ccdd.eeff

IPv6 Address Glean

- sw(config)#ipv6 snooping policy SnPol
- sw(config)#vlan configuration 10
- sw(config-vlan-config)#ipv6 snooping attach-policy SnPol

NDP Inspection

- ND üzenetek ellenőrzése, kezelése és szűrése az IPv6-MAC összerendelés alapján.

- DAD, cím feloldás, …

- (config)#ipv6 nd inspection policy NDPI
- (config-nd-inspection)#validate source-mac
- (config-if)#ipv6 nd inspection attach-policy NDPI

DHCPv6 Guard

- DHCPv6 szerver üzenetek (advertisement, reply) szűrése

- DHCPv6 Guard:
  - sw(config)#vlan configuration 10
  - sw(config)#ipv6 dhcp guard

- Uplink?
  - sw(config)#ipv6 dhcp guard policy UPLINK
  - sw(config-dhcp-guard)#device-role server
  - Sw(config-if)#ipv6 dhcp guard attach-policy UPLINK

IPv6 Source Guard

- Szűri az IPv6 binding table-nek megfeleő IPv6 csomagokat azok forrás címe alapján.

- sw(config)#ipv6 source-guard policy SG_Pol
- sw(config-sisf-sourceguard)#deny global-autoconf
- sw(config-sisf-sourceguard)#permit link-local
- sw(config-if)#ipv6 source-guard attach-policy SG_Pol

Merre tovább?

- SeND
- Destination Guard
- uRPF

- ciscolive365.com:
  - BRKSEC-2003 - IPv6 Security Threats and Mitigations
  - BRKSEC-3003 - Advanced IPv6 Security: Securing LinkOperations at the First Hop
  - BRKSEC-2202 - Understanding and Preventing Layer 2 Attacks in IPv4 and IPv6 networks

Öf. + ?

szummer.mihaly@simonyi.bme.hu

home.sch.bme.hu/~smz/nws2013/