Répás Sándor, PhD hallgató
Hálózati és hálózatbiztonsági tanácsadó
E-mail: repa@ahol.com

Aktív hálózati eszközök támadása és védekezési lehetőségek

Rezümé:

Egyre nagyobb szerephez jutnak az adatátviteli hálózatok, melyek működéséhez elengedhetetlenek az adatkeretek és adatcsomagok továbbítását végző aktív hálózati eszközök, ezért kiemelt fontosságúvá vált ezen hálózati eszközök biztonságos működésének megvalósítása. A következőkben a kapcsoló[1] és útválasztó[2] hálózati eszközök alapvető működését, majd a működési síkokat mutatom be. Mindhárom sík esetében bemutatásra kerülnek lehetséges támadási módszerek, valamint olyan ajánlások is ismertetésre kerülnek, melyek segítséget nyújthatnak az adott támadás elleni védekezésben.

Kulcsszavak: biztonság, hálózat, hálózati eszközök, infrastruktúra, router, switch, támadás, védekezés

Bevezetés

Az élet minden területén előfordulnak a különböző célú távközlési és adatátviteli hálózatok, melyek segítségével nyújtott szolgáltatások mindennapi tevékenységünk szerves részévé váltak. Napjainkban a távközlési hálózatok működése egyre nagyobb mértékben IP alapokra helyeződik át. Az IP[3] konvergencia folyamata jól megfigyelhető a VOIP[4], valamint az IPTV[5] alkalmazások térnyerésével is. Eközben folyamatosan zajlik az áttérés az Ethernetre, mely már a WAN[6] alkalmazásokban is egyre inkább kiszorítja a hagyományos megoldásokat, mint amilyen az SDH[7] is. Kijelenthető, hogy a közeljövő telekommunikációja során alkalmazott átviteli hálózatok kialakítása szinte kizárólag Ethernet, IP, QoS[8] együttes alkalmazásával fog megvalósulni.

Az Etherneten és IP-n alapuló hálózatok nélkülözhetetlen aktív eszközei az OSI[9] 2-es rétegében[10] működő kapcsolók, valamint a 3-as rétegben[11] dolgozó útválasztók. A megbízható átvitel biztosítása érdekében kiemelt fontosságúvá vált ezen eszközök biztonsága, lehetséges támadási lehetőségeik, és a támadások elleni védekezési módszerek megismerése. A következőkben bemutatom a hálózati eszközök működését, működési síkjait, az egyes síkokra jellemző néhány lehetséges támadási lehetőséget, valamint az ellenük használható védekezési megoldásokat.

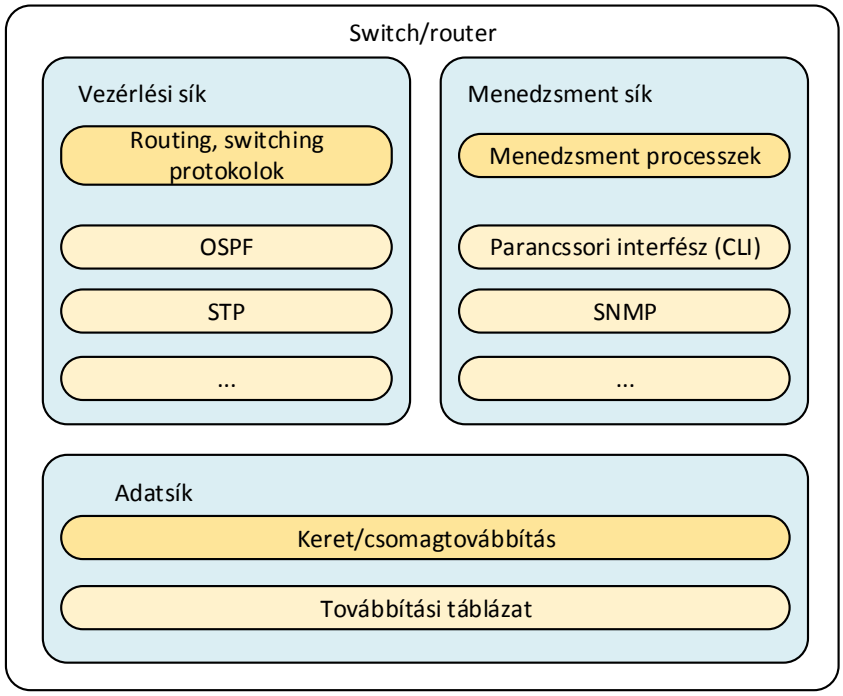
[1] Ethernet swich, switch
[2] IP router, router
[3] Internet Protocol
[4] Voice over IP
[5] Internet Protocol television
[6] Wide Area Network
[7] Synchronous Digital Hierarchy
[8] Quality of Service
[9] Open Systems Interconnection
[10] Adatkapcsolati réteg, Data-Link layer
[11] Hálózati réteg, Network layer

2-es és 3-as rétegben működő hálózati eszközök működése

Az 1. ábra egy aktív hálózati eszköz (kapcsoló, vagy útválasztó, switch vagy router) különböző síkjait mutatja be. A switchek és routerek legfontosabb feladata az IP csomagot[12] tartalmazó Ethernet keret[13] megfelelő irányba történő továbbítása. A továbbításhoz elsődlegesen a célállomás címére van szükség, mely adatkapcsolati rétegben a fizikai cím (MAC[14]), míg hálózati rétegben a logikai (IP) cím. Ez a továbbítás történik meg az adatsíkon.

A hálózati eszközök működéséhez azonban még rengeteg más információ is szükséges. Ezeket az információkat a vezérlési síkon működő szolgáltatások, protokollok biztosítják. Ilyenek lehetnek például switchek esetében a VLAN[15]-ok dinamikus menedzselését biztosító protokollok, vagy a kapcsolótáblát karbantartó szolgáltatások, míg routerek esetében a különböző útválasztási protokollok[16].

A hálózati eszközök beállítását, működésének módosítását, valamint folyamatos felügyeletét a menedzsment sík segítségével lehet megoldani. Itt állíthatjuk be például, hogy ki léphet be az adott eszközre, de itt kérdezhető le az eszköz pillanatnyi terheltsége is.



1. ábra: Kapcsolók és útválasztók működési síkjai
Forrás: Saját készítésű ábra

Míg az adatsíkon a keretek/csomagok továbbítása történik, addig a vezérlési- és a menedzsment sík esetében a keretek/csomagok forrása, vagy célállomása az adott hálózati eszköz is lehet. Az elsőre példa egy IP csomag továbbítása, míg a második esetre egy a routernek címzett SNMP[17] lekérdezés.

A bemutatott támadások, elterjedtségük miatt Cisco[18] eszközökön kerülnek bemutatásra, de a legtöbb esetben más gyártók eszközein is alkalmazhatóak.

[12] IP packet
[13] Ethernet frame
[14] Media Access Control
[15] Virtual Local Area Network
[16] Routing protocol
[17] Simple Network Management Protocol
[18] Cisco Systems, Inc, www.cisco.com

Menedzsment sík támadások

Jelszó helyreállítás[19]

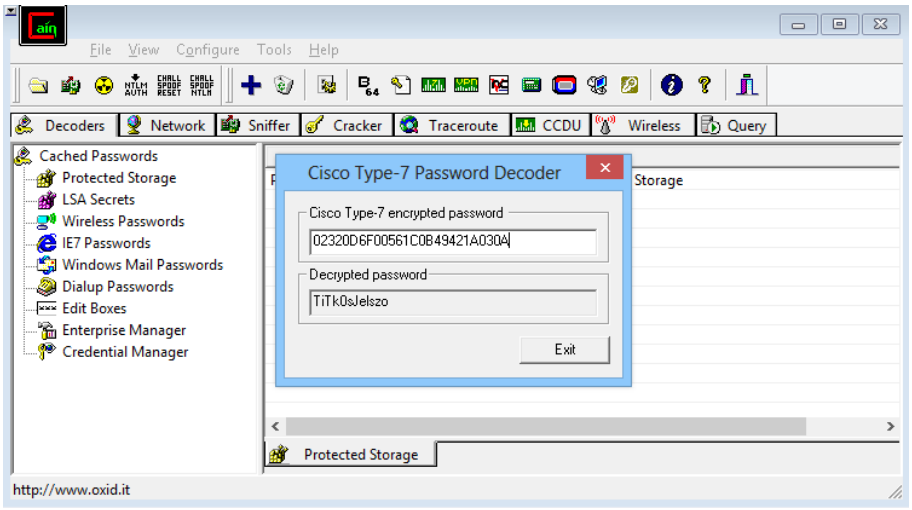
A legtöbb menedzselhető hálózati eszköz rendelkezik konzol port csatlakozóval, melyen keresztül a kezdeti beállítások, vagy szükség esetén, a hálózaton kívülről történő menedzsment[20] végezhető el. A Cisco[21] eszközök a konzol porton alapértelmezetten lehetővé teszik, a hitelesítési folyamat megkerülését, melynek eredeti célja, hogy a jelszó elfelejtése esetén is konfigurálhassuk eszközünket.

Az egyes eszköztípusok jelszó törlési folyamata eltérhet egymástól, melyek pontos ismertetése elérhető a gyártó honlapján [5]. A folyamat segítségével jelszó nélkül hozzáférhetünk az eszköz konfigurációjához, mely tartalmazhat jelszavakat, és titkosítási kulcsokat is. Csak kismértékben nehezíti a támadó dolgát, ha ezek az információk elkódolva kerültek tárolásra[22], mert az interneten számos alkalmazás elérhető, mely az ilyen formátumú jelszavak visszaállítását végzi. Erre a célra jól használható eszköz az ingyenesen elérhető Cain & Abel [12]. A 2. ábra mutatja a konfigurációnak az NVRAM[23]-ban található konfigurációs állomány részletét, mely egy felhasználó jelszavát tartalmazza elkódolva, míg a 3. ábra a jelszó visszaalakítását mutatja be.

```
username testuser password 7 02320D6F00561C0B49421A030A
```

2. ábra: Felhasználó és elkódolt jelszava CISCO IOS konfigurációjában
Forrás: Saját készítésű ábra

A támadás elleni leghatékonyabb védekezési módszer a megfelelő fizikai biztonság biztosítása az eszköz részére. Ahogy láttuk nem hatásos a `service password-encryption` parancs kiadása, de a secret-ek alkalmazása sem lehetséges olyan esetekben, amikor a hálózati eszköznek visszaalakítható formátumban kell tárolni a jelszót, titkosítási kulcsot. Növelheti a biztonságot a password recovery funkció letiltása a `no service password-recovery` konfigurációs beállítás alkalmazásával.



3. ábra: Jelszó visszafejtése Cain & Abel segítségével
Forrás: Saját készítésű ábra

[19] Password recovery
[20] Out of band management
[21] De más gyártók is. Például Juniper
[22] Ez elérhető a `service password-encryption` konfigurációs parancs segítségével.
[23] Non-volatile random-access memory. A CISCO eszközök ebben a memóriában tárolják az indításkor betöltődő konfigurációs beállításokat.

SNMP

Az SNMP protokoll elterjedten használt a különböző hálózati eszközök távoli, automatikus menedzselésére. Az SNMP-nek három verziója létezik[24], melyekből egyedül a 3-as támogatja a felhasználók egyedi azonosítását és a titkosítást. Egyszerűsége miatt, biztonsági hátrányai ellenére jelenleg is elterjedten alkalmazzák 2C verzióját. Az SNMP v1 és v2c azonosításra az úgynevezett community stringet alkalmazza, melynek alapértéke a legtöbb gyártó esetében `PUBLIC` a csak olvasási műveletekre és `PRIVATE` az írási műveletekre [13]. Nagyon sok esetben az üzemeltetők nem változtatják meg az alapértelmezett beállításokat, és nem is tesznek semmilyen korlátozást az SNMP lekérdezésekre. Az SNMP segítségével az eszközről, annak típusától, és SNMP támogatásától függően rengeteg információ megtudható[25]. A 4. ábra egy Linuxon elindított SNMP lekérdezést, és néhány fontosabb sort mutat be az érkezett válaszból[26].

```
user@NS1:~$ snmpwalk -v 2c -c PUBLIC 10.200.63.1
SNMPv2-MIB::sysDescr.0 = STRING: RouterOS RB433AH
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.14988.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1686692400) 195 days, 5:15:24.00
SNMPv2-MIB::sysContact.0 = STRING: root@domain.hu
SNMPv2-MIB::sysName.0 = STRING: Central-router
SNMPv2-MIB::sysLocation.0 = STRING: III.emelet
SNMPv2-MIB::sysServices.0 = INTEGER: 78
…
RFC1213-MIB::ipRouteNextHop.0.0.0.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.3.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.100.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.101.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.102.0 = IpAddress: 10.240.4.17
RFC1213-MIB::ipRouteNextHop.10.0.103.0 = IpAddress: 10.240.4.17
```

4. ábra: SNMP lekérdezés snmpwalk paranccsal

Forrás: Saját készítésű ábra

A lekérdezések előtt, az elérhető SNMP eszközöket pedig az `nmap`[27] parancs, vagy más portscan[28] alkalmazás segítségével fedezhetjük fel. Ehhez a nyitott 161-es UDP[29] portok keresése szükséges.

Hálózati eszköz túlterhelés SNMP segítségével

Az SNMP kérések feldolgozása és a megfelelő válasz elküldése a legtöbb hálózati eszközön nagy terhelést idéz elő. Az 5. ábra mutatja, ahogyan az előzőleg bemutatott parancs (4. ábra) hatására egy router processzorán 30%-os terheltség keletkezik.

[24] SNMPv1, SNMPv2c, SNMPv3

[25] Például: az eszköz típusa, mióta működik, hőmérséklete, szabad memóriája, útválasztó táblája.

[26] A lekérdezésre adott válasz több mint 4200 sort tartalmazott, így csak a fontosabbak kerültek az ábrába.

[27] https://nmap.org/

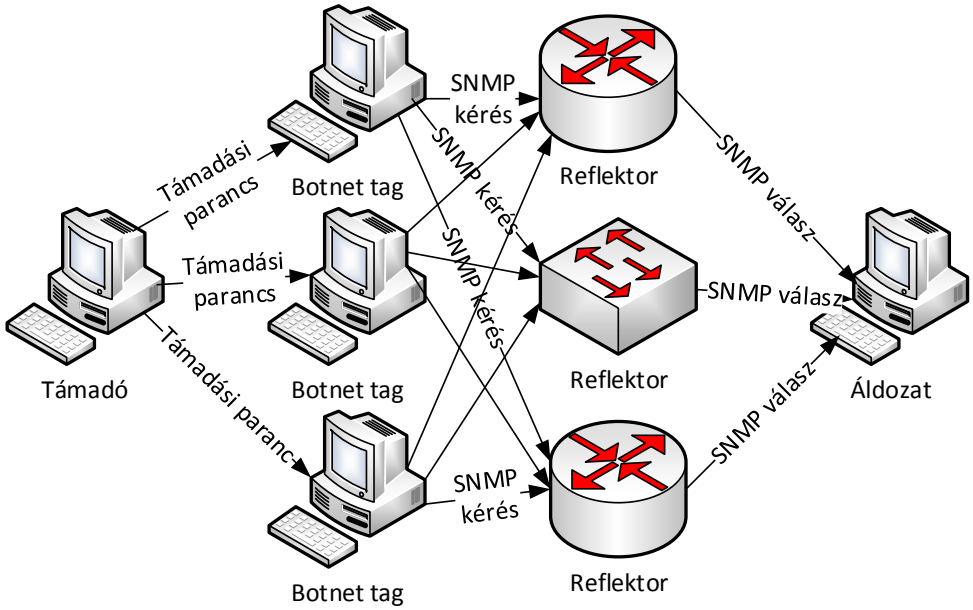
[28] A vizsgált hálózatra csatlakozó eszközön nyitott portokat, ezáltal elérhető hálózati szolgáltatásokat kereső alkalmazás.

[29] User Datagram Protocol, felhasználói datagram protokoll

```
[admin@Central-router] > system resource print
                   uptime: 27w6d5h27m34s
                  version: 6.29
               build-time: May/27/2015 11:19:36
             free-memory: 94.0MiB
            total-memory: 128.0MiB
                     cpu: MIPS 24Kc V7.4
               cpu-count: 1
           cpu-frequency: 680MHz
                cpu-load: 30%
          free-hdd-space: 49.2MiB
         total-hdd-space: 64.0MiB
 write-sect-since-reboot: 914547
        write-sect-total: 13383449
              bad-blocks: 0%
       architecture-name: mipsbe
              board-name: RB433AH
                platform: MikroTik
```

5. ábra: Router terhelése snmpwalk parancs hatására
Forrás: Saját készítésű ábra

Az SNMP-nek a hálózati eszközt terhelő tulajdonságát kiválóan lehet alkalmazni DDoS[30] támadások kivitelezésére, melyek során a támadott eszközt kell elárasztani SNMP kérésekkel. Ez a támadás a legtöbb esetben akkor is hatékonynak bizonyul, ha a támadó nem ismeri a megfelelő communityt, mert a hálózati eszköznek akkor is fel kell dolgoznia a beérkezett kéréseket. A támadás kivitelezése nagyon egyszerű, valamint az interneten is rengeteg eszköz található meg kivitelezéséhez (Például: [2]).



6. ábra: SNMP-t támogató hálózati eszközök segítségével felerősített DDoS támadás
Forrás: Saját készítésű ábra

SNMP segítségével felerősített támadás[31]

A támadás a hálózati eszközöket a forgalom növelésére használja, oly módon, hogy az áldozat IP címét megadva forrás címként SNMP kéréseket küld hálózati eszközök részére. Az

[30] Distributed Denial of Service, elosztott túlterheléses szolgáltatás megtagadás
[31] SNMP Reflected Amplification DDoS Attack

elküldött SNMP kérések kicsik, azonban célzottan olyan adatokat kérdeznek le, melyek nagy válaszokat generálnak. Így a támadó részére csak kis sávszélességet igénnyel a támadás kivitelezése, míg az áldozat irányába sokszoros forgalmat képes generálni a módszer alkalmazása. A támadást a 6. ábra szemlélteti. A támadásról és az ellene történő védekezésről bővebb információk találhatóak a BITAG kiadványában [3], míg egy támadásra alkalmazható egyszerű program letölthető az ERNW GmbH oldaláról [11].

Védekezési lehetőségek

A legjobb megoldás az SNMP által használt 161-es UDP portot szűrőlistával védeni a hálózati eszközön, valamint a már évekkel ezelőtt elavult régebbi SNMP verziók helyett SNMPv3 alkalmazása. A gyártók is nagyon sokat tehetnének a biztonság növelése érdekében, ha a leszállított eszközök alapértelmezetten nem engedélyeznék az SNMP működését. A CISCO weblapján részletes segítség található az SNMP biztonságos beállításához [6].

Vezérlési sík támadások

OSPF[32]

A routerek az IP csomagok továbbítását alapesetben a routing tábla alapján végzik. Ennek a táblának a karbantartását a legkisebb hálózatoktól eltekintve érdemes dinamikus routing protokollokra bízni, mint amilyen az OSPF is. Az OSPF az egyik legnépszerűbb, nem gyártó függő, kapcsolatállapot alapú útválasztási protokoll[33].

- Hálózat felderítése

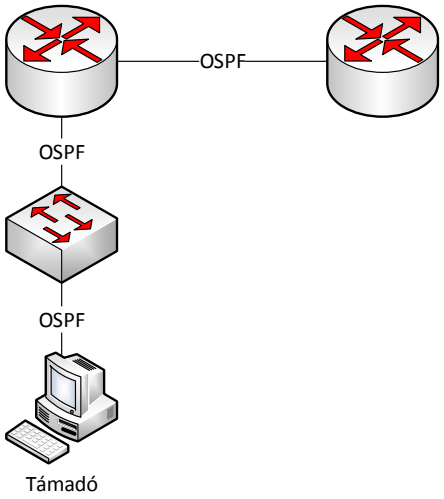
Az OSPF működéséből fakadóan az egyes OSPF routerek a teljes hálózat[34] felépítését ismerik. Ez az információ pedig nagyon jól használható a további támadások előkészítéséhez. Az egyes OSPF protokollt használó routerek az OSPF kommunikáció során multicast címzés segítségével, 3 féle hitelesítés alkalmazásával kommunikálhatnak [7]. A hitelesítés lehetséges típusait az 1. táblázat tartalmazza.

AuthType	Description
0	Null authentication
1	Simple password
2	Cryptographic authentication

1. táblázat: OSPF lehetséges hitelesítés típusai
Forrás: RFC 2328

A 0 és 1-es típus esetében a támadónak mindössze annyi a feladata, hogy néhány OSPF csomag elfogása után, az azokban található információk[35] felhasználásával beállított OSPF protokollt támogató routerrel (például Quagga segítségével [8]) csatalakozik a hálózathoz, majd rövid időn belül a hálózat teljes routing táblája megjelenik routerében. A gyakorlatban nagyon sokszor előfordul, hogy a hálózati eszközöket felügyelő szakember az eszközök beállítása során nem figyel arra, hogy az OSPF csomagok csak az útválasztók közötti interfészeken forduljanak elő, így a támadás egy asztali számítógépről is egyszerűen kivitelezhető (7. ábra).

[32] Open Shortest Path First
[33] Link-state routing protocol
[34] Több terület (area) esetében valójában csak a saját area felépítését.
[35] Például: area, hello interval.



7. ábra: OSPF-et használó hálózat támadása
Forrás: Saját készítésű ábra

A 2-es típusú hitelesítés MD5 kivonat[36] alkalmazását jelenti, mely elavultsága miatt, napjainkra már könnyen feltörhető. Ilyen esetben néhány csomag elfogása után, azokból az MD5 kulcs előállítható az interneten elérhető programok valamelyikével [9].

- Forgalom elterelése

Ha már az OSPF routerek elhiszik a támadó eszközről, hogy az is egy jogosult OSPF router, úgy nem nehéz feladat, a többi routert megtévesztve, azoknak hamis útvonalakat továbbítva a forgalom más irányba terelése, majd lehallgatása. Ennek a feladatnak az elvégzésére is található az interneten néhány eszköz [10].

- Védekezés

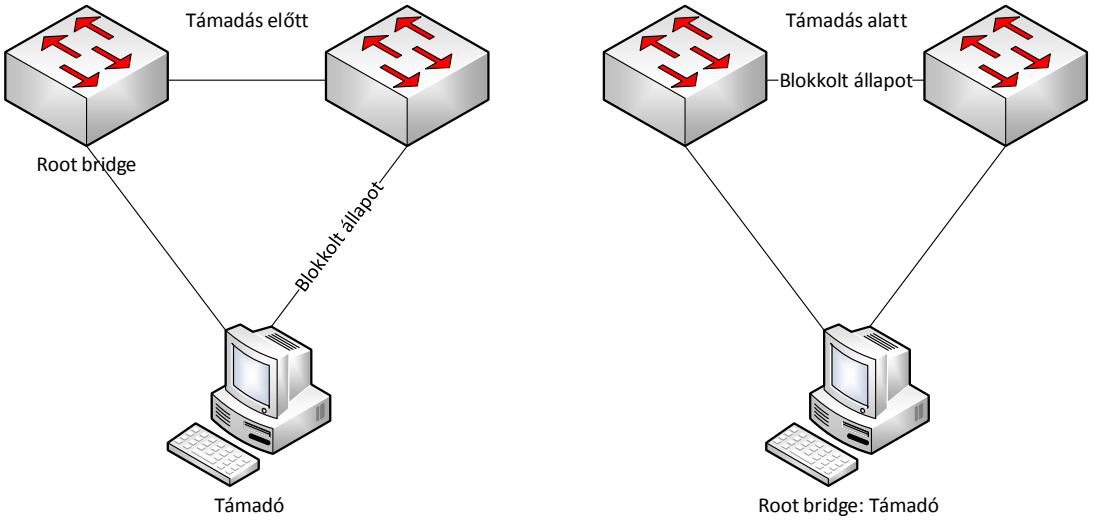
Az OSPF támadások kivédésére korlátozottan alkalmazható az OSPF forgalom korlátozása a routerek közti interfészekre a `passive-interface`, vagy a `passive-interface default` OSPF konfigurációs parancs [4], és az MD5 hitelesítés együttes alkalmazása. A teljes körű védelmet azonban csak az IPsec[37] alkalmazásával érhetjük el.

STP[38] manipuláció

Az OSI modell 2-es rétegében megvalósított redundanciához került kifejlesztésre az STP protokoll. Segítségével, a különböző problémákat[39] okozó hurkok kialakulása nélkül biztosítható a redundancia, mellyel a hálózatkiesések csökkenthetők. Az STP működése során elsődlegesen a bridge[40] prioritást veszi figyelembe, így ennek manipulálásával a forgalom eltéríthető, majd megfigyelhető (8. ábra). Erre a célra például az interneten elérhető Yersinia [1] alkalmazható.

A támadás elleni védekezés, Cisco eszközökön a BPDU Guard, BPDU Filtering, vagy a Root Guard alkalmazásával lehetséges [14].

[36] MD5 digest
[37] Internet Protocol Security
[38] Spanning Tree Protocol
[39] Például: broadcast storm
[40] Hálózatokat L2-es szinten összekötő eszköz

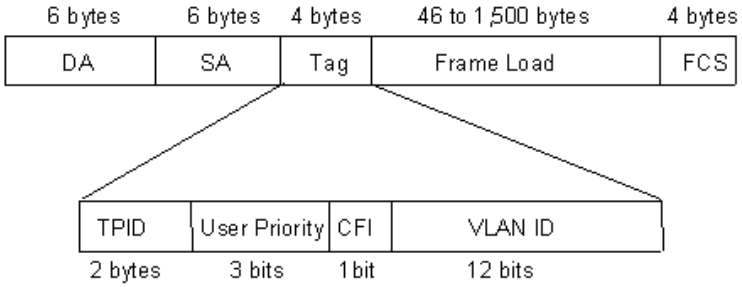


8. ábra: Forgalom elterelés STP alkalmazásával
Forrás: Saját készítésű ábra

Adatsík támadások

VLAN ugrás kettős jelölés[41] alkalmazásával

A 802.1Q [15] segítségével történő VLAN kialakítása során az Ethernet keretbe 4 byte beszúrása történik, melyből 12 bit azonosítja a VLAN-t (9. ábra).

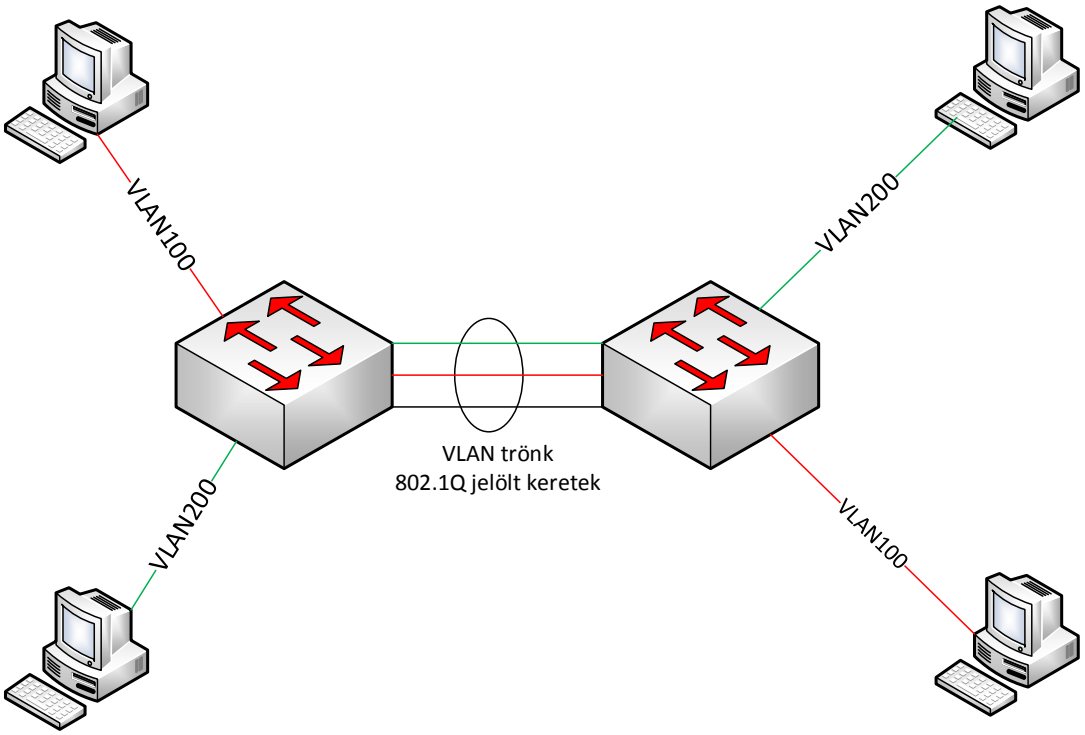


9. ábra: Ethernet keret VLAN jelölése
Forrás: H3C Group Holding Ltd. in: h3c.com (letöltve: 2016. október 26.)

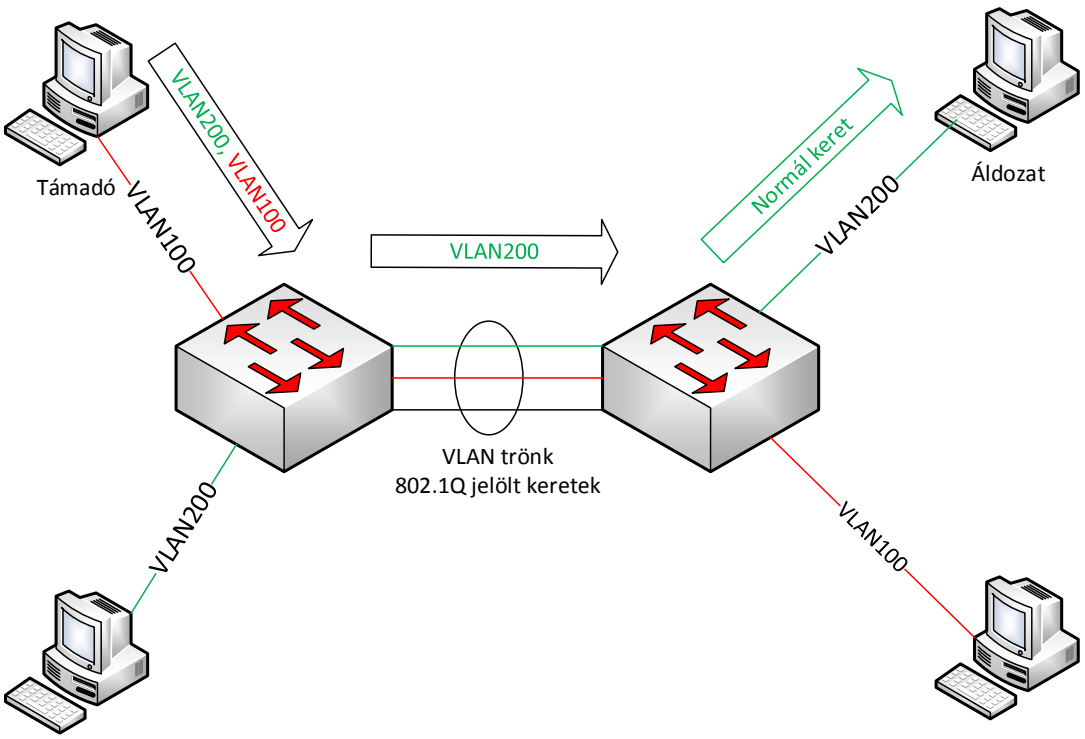
Normál működés esetén, a hozzáférési porton érkező jelöletlen keretet, mielőtt a switch egy trunk[42] portján kiküldené, ellátja a megfelelő VLAN jelöléssel. Ezt a jelölést a fogadó switch eltávolítja, majd a keretben lévő információ és a kapcsolási táblázata alapján kiküldi a megfelelő porton (10. ábra). A dupla jelölés alkalmazása során a hozzáférési porton lévő eszköz már VLAN jelöléssel duplán ellátott keretet küld a swicth felé, amely értelmezi és eltávolítja a külső keretet, majd annak figyelembevételével végzi a továbbítást, míg belső keret megmarad (11. ábra).

A támadás csak nem megfelelően konfigurált, vagy elavult swicthek alkalmazása esetén kivitelezhető[43], ráadásul csak egyirányú forgalomtovábbításra alkalmas. Ha azonban két külön VLAN-ban szereplő számítógépen telepítésre került a VLAN ugrásra alkalmas program, úgy a módszer használható a VLAN-ok közti kétirányú kommunikáció biztosítására, a VLAN izoláció kikerülésére, mely sok esetben biztonsági meggondolások miatt van tiltva.

[41] VLAN hopping by double tagging
[42] Olyan port, melyen egyszerre több VLAN forgalma kerül továbbításra, oly módon, hogy az egyes Ethernet keretek jelölve vannak, hogy mely VLAN-hoz tartoznak.
[43] Vannak azonban más VLAN ugrási módszerek.



10. ábra: 802.1Q VLAN hálózat kialakítása
Forrás: Saját készítésű ábra



11. ábra: VLAN ugrás kettős jelöléssel
Forrás: Saját készítésű ábra

Összegzés

Az adatátviteli hálózatok nélkülözhetetlen elemei, a kapcsolók és az útválasztók elleni támadási lehetőségek nagyon sokfélék, azonban szinte minden esetben lehetséges védekezési módszerek is rendelkezésre állnak. Fontos, hogy már a hálózat tervezése, majd kiépítése során a biztonság kiemelt szempontként kerüljön figyelembe vételre. Később pedig a hálózatüzemeltetők is kísérjék figyelemmel a nyilvánosságra kerülő támadási és védekezési módszereket, melyeket folyamatosan implementáljanak a felügyeletükre bízott hálózatban.

Irodalomjegyzék:

1. Barroso, DAVID és Andrés ALFREDO: Yersinia, http://www.yersinia.net/index.htm, letöltve: 2016. október 26.
2. Bechtsoudis, ANESTIS: Simple SNMP Bulk Request Denial Of Service Tool, in: https://packetstormsecurity.com/files/116126/Simple-SNMP-Bulk-Request-Denial-Of-Service-Tool.html, letöltve: 2016. október 26.
3. Broadband Internet Technical Advisory Group: SNMP Reflected Amplification DDoS Attack Mitigation, in: http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf, letöltve: 2016. október 26.
4. Bryant, CHRIS: OSPF And Passive Interfaces, http://www.mcmcse.com/cisco/guides/ospf_and_passive_interfaces.shtml, letöltve: 2016. október 26.
5. Cisco Systems, Inc: Password Recovery Procedures, in: http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/6130-index.html, letöltve: 2016. október 26.
6. Cisco Systems, Inc: Securing Simple Network Management Protocol, in: http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/20370-snmpsecurity-20370.html, letöltve: 2016. október 26.
7. John, MOY: RFC 2328 - OSPF Version 2, in: https://www.ietf.org/rfc/rfc2328.txt, letöltve: 2016. október 26.
8. Lamparter, DAVID et al: Quagga Routing Suite, http://www.nongnu.org/quagga/, letöltve: 2016. október 26.
9. Mannay, FOEH: Offline Attack on MD5 keys in captured OSPF packets, http://networkingbodges.blogspot.hu/2013/10/offline-attack-on-md5-keys-in-captured.html, letöltve: 2016. október 26.
10. Mende, DANIEL: Loki, https://c0decafe.de/loki.html, letöltve: 2016. október 26.
11. Mende, DANIEL: snmpattack.pl, in: https://www.ernw.de/download/snmpattack.pl, letöltve: 2016. október 26.
12. Montoro, MASSIMILIANO: Oxid.it Cain & Abel, http://www.oxid.it/cain.html, letöltve: 2016. október 26.
13. Reigle, GARY A: SNMP Community Strings, https://www.giac.org/paper/gcih/44/default-snmp-community-strings-set-public-private/100366, letöltve: 2016. október 26.
14. Semperboni, FABIO: How to protect against BPDU attack, http://www.ciscozine.com/how-to-protect-against-bpdu-attack/, letöltve: 2016. október 26.
15. The Institute of Electrical and Electronics Engineers, Inc: 802.1Q - Virtual LANs, http://www.ieee802.org/1/pages/802.1Q.html, letöltve: 2016. október 26.