HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Szabó Tibor
szabo.tibor@nbsz.gov.hu

CDP (CISCO DISCOVERY PROTOCOL) TÁMADÁS

Absztrakt

Korábbi cikkemben érintőlegesen ismertettem néhány, közismertebb Layer 2[1] szintű hálózatbiztonsági problémát és támadási formát, melyre érdemes odafigyelni mind a tervezési szakaszban, mind az implementálás során, amikor hálózatok és hálózatvédelmi berendezések topológiájának kialakítása folyik és a konfigurációk véglegesítésre kerülnek az eszközökben. [16] Az említett támadási formák közül ebben a cikkben magára a CDP (Cisco[2] Discovery Protocol) támadásra és annak megértésére koncentrálok – elhagyva azokat a technikai részleteket, melyek nem közvetlenül tartoznak a tárgyhoz.

In my previous article I presented some of most common Layer 2 level network security issues and attack method, which are worth paying attention. When planning and implementing the networks and network security equipment and finalizing the configuration we should pay attention in every stage. [16] I'm focusing now on the attack method of CDP (Cisco Discovery Protocol) – I avoid mentioning those technical details, which are not directly relevant to the issue in this article.

Kulcsszavak: *CDP, layer 2, memória túlcsordulás, sebezhetőség, Yersinia, ~ CDP, layer 2, memory overflow, vulnerability, Yersinia*

[1] Adatkapcsolati réteg az OSI modellben.
[2] A világ vezető hálózati eszköz gyártója.

1. BEVEZETÉS

Napjainkra az internet szolgáltatók országos lefedettséget biztosítanak, mindemellett az információ igény és a sávszélesség növekedése egyre csökkentette ár/sávszélesség arány értékét, mely elérhetőbbé tette a vállalatok, kisvállalatok és az egyének számára is a világhálóhoz való hozzáférés igénybe vételét. Ma már a szolgáltatás hozzáférési pontra csatlakozó egyedi végpontokat nagyvállalatokhoz hasonlóan kisvállalatoknál és egyéni vállalkozásoknál is felváltják a kisebb-nagyobb magánhálózatok, melyek az alkalmazottak részére is elérhetővé teszik a lokális adatbázisokat, számítógépes erőforrásokat és az internet szolgáltatást. Ellenben a hálózatok építése során viszonylag keveset foglalkozunk a biztonsággal és elég gyakran az eszközök alapbeállításával megelégszünk.

Korábbi cikkemben érintőlegesen ismertettem néhány, közismertebb Layer 2 szintű hálózatbiztonsági problémát, melyre érdemes odafigyelni mind a tervezési szakaszban, mind az implementálás során, amikor hálózatok és hálózatvédelmi berendezések topológiájának kialakítása folyik és a konfigurációk véglegesítésre kerülnek az eszközökben. [16] Az említett támadási formák közül ebben a cikkben magára a CDP (Cisco Discovery Protocol) támadásra és annak megértésére koncentrálok – elhagyva azokat a technikai részleteket, melyek nem közvetlenül tartoznak a tárgyhoz.

2. A CDP PROTOKOLL INFORMÁCIÓI

A CDP (Cisco Discovery Protocol) a Cisco által szabadalmaztatott protokoll az OSI Layer 2 szintjén, mely szinte minden Cisco által gyártott eszközön működik. [1], [3] Természetesen a Cisco berendezések széleskörű elterjedésének hatására voltak gyártók, melyek szintén alkalmazták ezt a protokollt a hálózatban való együttműködés megkönnyítése érdekében. Ilyen gyártó volt a HP (Hewlett Packard) is, mely a Procurve 2500 sorozatú switch[3] eszközeiben implementálta ezt a képességet. [2]

A legtöbb Cisco switch és router[4] (útválasztó) berendezésen alapértelmezetten engedélyezve van a CDP funkció, aminek segítségével a közvetlenül egymáshoz csatlakozó eszközök felderíthetik egymást, megtudhatják egymás konfigurációs beállításait és a hibaelhárítás gyorsabban és szakszerűbben végrehajtható.

Nézzük meg, milyen információkat tartalmaz egy router memóriája a hozzá közvetlenül csatlakozó CDP üzenetekből a „show cdp neighbors” utasítással:

```
Router_4#sho cdp neighbors

   Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                     S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Router3             Ser 1          120           R        2500      Ser 0
Router1             Eth 1          180           R        2500      Eth 0
Switch1             Eth 0          240           S        1900      2
```

A tárolt CDP üzenetek között szerepel:

- Device ID: a szomszédos eszköz neve.
- Local Intrfce: a helyi router eszközünk kapcsolódási pontjának típusa és száma, amin keresztül a CDP üzenet érkezik.

[3] Olyan számítógépes hálózatban alkalmazott aktív eszköz, mely összekapcsolja a hálózati eszközöket.

[4] Olyan útválasztó eszköz, mely továbbítja az adatcsomagokat a számítógépes hálózatok között. A router egy vagy több adatvonallal csatlakozik. a különböző hálózatokhoz.

- Holdtme: CDP üzenetek tárolásának ideje másodpercben.
- Capability: a szomszédos eszköz router vagy switch.
- Platform: a szomszédos eszköz típusa.
- Port ID: a szomszédos eszköz csatlakozási pontjának típusa és száma, amiről a CDP üzenet érkezik.

Kérdezzük le a szomszédos Router1 eszköz adatait kissé részletesebben a „show cdp entry Router1" paranccsal: [4]

```
Router_4#sho cdp entry Router1
   -------------------------

   Device ID: Router1
   Entry address(es):
    IP address: 10.0.10.2
   Platform: cisco 2500, Capabilities: Router
   Interface: Ethernet1,  Port ID (outgoing port): Ethernet0
   Holdtime : 180 sec

   Version:
   Cisco Internetwork Operating System Software
   IOS (tm) 2500 Software (2500-JS-L), Version 11.2(15)
   RELEASED SOFTWARE (fcl)
   Copyright (c) 1986-1998 by Cisco Systems, Inc.
   Compiled Mon 06-Jul-98 22:22 by tmullins
```

A tárolt CDP üzenetek között szerepel:

- Device ID: a szomszédos eszköz neve.
- Entry address (es): a szomszédos eszköz IP címe.
- Platform: a szomszédos eszköz típusa.
- Capabilities: a szomszédos eszköz router vagy switch.
- Interface: a helyi router eszközünk kapcsolódási pontjának típusa és száma, amin keresztül a CDP üzenet érkezik.
- Port ID: a szomszédos eszköz csatlakozási pontjának típusa és száma, amiről a CDP üzenet érkezik.
- Holdtme: CDP üzenetek tárolásának ideje másodpercben.
- Version: a szomszédos eszközön futó szoftver (OS) típusa.

A CDP információk un. multicast[5] üzenetekkel vannak szétküldve periódikusan a hálózat adatkapcsolati rétegén, ezért az útválasztók (router) ezeket már nem terjesztik tovább más hálózatok felé. A megérkező multicast üzenetek az egyes eszközök helyi CDP adatbázisát frissítik. A periódikusság mértékét az időzítések (timer) segítségével lehet beállítani, melyek meghatározzák, hogy:

- milyen gyakran (update timer) kell szétküldeni a CDP információkat és
- mennyi ideig (holdtime) kell tárolni a megkapott CDP üzenetet.

[5] Olyan kommunikációs forma, melyben egy adó és több vevő egy közös csatornán információt cserél. Ilyen például a hangközvetítés.

Nézzünk az időzítésekre egy példát lekérdezve „show cdp” paranccsal egy router adatait:

```
Router_4#show cdp
  Global CDP information:
          Sending CDP packets every 60 seconds
          Sending a holdtime value of 180 seconds
```

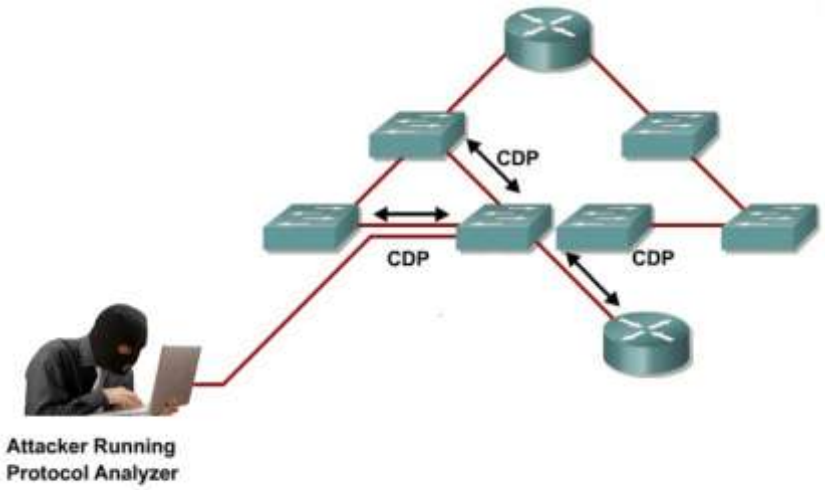
3. A CDP TÁMADÁS

A CDP támadás sajátosságainak egyszerűbb értelmezhetősége kedvéért érdemes felbontani azt két részre:

- memória túlcsordulást okozó módszerre és
- információszerzési módszerre.

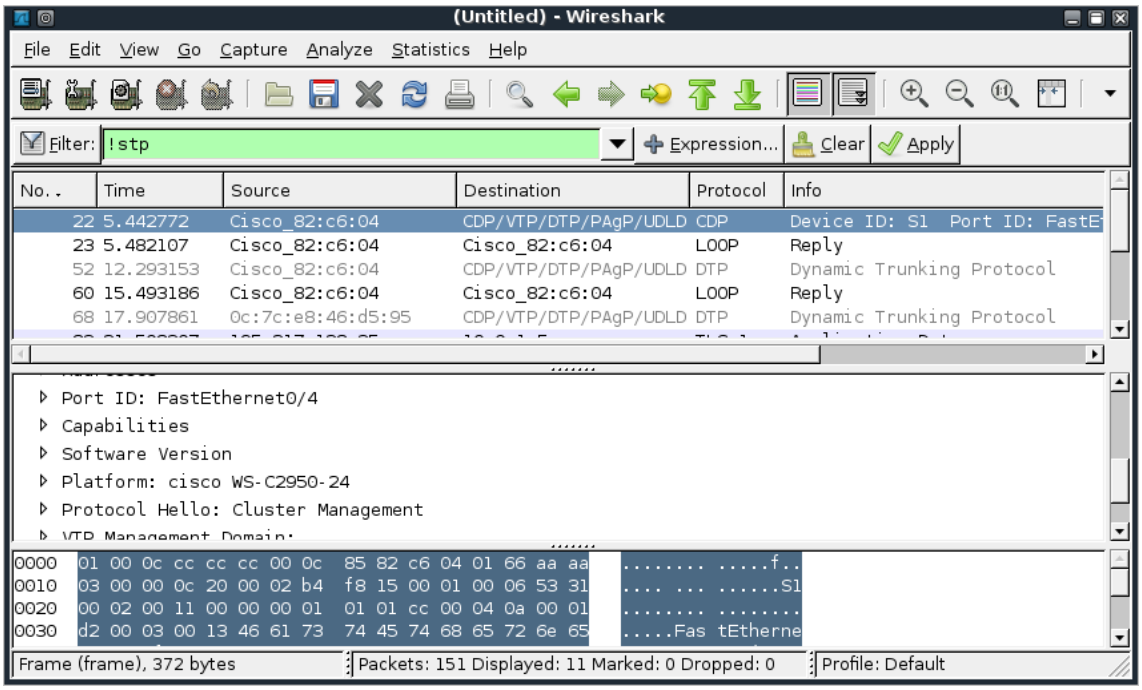
A memória túlcsordulást okozó módszer azt használja ki, hogy az eszközök memória allokációs képességei gyengék, ezáltal az eszközben futó, egyes folyamatok hajlamosak a másiknak a memória területére ráírni adatokat. Az inkoherens adatok értelmezésekor abnormális működés vagy teljes leállás következik be, amit hamis CDP csomagok hálózatba történő tömeges küldésével lehet elérni egyes hálózati elemeknél. [14]

Az információszerzési módszer azt használja ki, hogy a CDP üzenetek nincsenek titkosítva, ezért könnyen értelmezhetővé válik bárki számára, aki a hálózatra felcsatlakozva (vezetékkel vagy vezeték nélkül) passzívan monitorozza az IP forgalmat. (1. ábra).



1. ábra. CDP üzenetek monitorozása

A következő ábra azt szemlélteti, hogy mit láthat a támadó az IP forgalom monitorozása közben a közismert Wireshark – ingyenes hálózati forgalomanalizáló szoftver – kezelő felületén. (2. ábra)



2. ábra. Wireshark felülete [5]

A forgalom passzív monitorozásán kívül egy másik lehetséges megoldás a támadó számára, ha aktívan, saját számítógépéről hamis CDP üzeneteket küld szét a hálózatban, amire a közvetlenül csatlakozó Cisco eszközök a protokoll szabályai szerint válaszolnak. A fentiekben részletezett információk, melyeket az eszközök egymás között cserélnek, sok olyan értékes adatot tartalmaznak, amelyek hasznosak a támadó számára. Nézzük ezeket sorban egy-egy példával illusztrálva, hogy mire használhatóak fel az egyes adatok.

A *szomszédos eszköz IP címe*[6] (Entry address) alapján lehetősége van a támadónak leszűkíteni azt a tartományt, amire a későbbiekben koncentrálnia kell. Vegyük például a privát címeket (3. ábra), amik a LAN hálózatok címkiosztására vannak fenntartva:

Tartomány kezdete	Tartomány vége	Címek száma
10.0.0.0	10.255.255.255	16 777 216
172.16.0.0	172.31.255.255	1 048 576
192.168.0.0	192.168.255.255	65 536

3. ábra. Privát címek

A címek számában az egyes értékek közötti (alulról felfelé haladva) 16 szoros szorzó elég nagy érték, ha figyelembe vesszük, hogy egy automata biztonsági szkenner (mint pl.: nmap, Nessus) jelentős időt (több perc) tud eltölteni egy adott hálózati címen lévő eszköz biztonsági réseinek felderítésében. Amennyiben csak egy kisebb IP tartományra kell koncentrálni, akkor jelentős időt lehet megtakarítani, mindazonáltal kevesebb idő is elég a hálózati elemek sérülékenységeinek felderítéséhez.

Az *eszköz fajtája* (router vagy switch) további támpontot ad a hálózati topológia felderítéséhez, mivel a router eszközöket általában olyan helyre építik be, ahol különböző IP címtartományba eső hálózatokat, különböző protokollokat és/vagy csatlakozási felületeket alkalmaznak a hálózatban. A router egyik speciális funkciója a hálózati átjáró (gateway), melynél könnyen feltételezhető, hogy egy másik más IP cím tartománnyal rendelkező hálózat is létezik a közvetlenül láthatón kívül.

[6] Internet protokoll cím egy olyan numerikus jelölés, mely minden eszközhöz hozzá van rendelve a számítógépes hálózatban.

A *hálózati elem típusa* (Platform. pl.:WS-C2950-24) és a rajta futó operációs rendszer *verzió száma* (Version. pl.: 12.1(12c)EA1) alapján meghatározható, hogy feltártak-e korábban sérülékenységet az eszközön, aminek kiaknázásával hathatós támadás indítható a hálózati elem ellen. A meghatározást megkönnyíti, hogy az interneten sok olyan adatbázis található ma már, ahol összegyűjtik, rendszerezik és publikálják az eszközök és rendszerek sérülékenységeit. Egy közismert, sérülékenységekkel foglalkozó internetes honlap (www.securiteam.com) adatbázisából lekérdezhetőek a „Cisco" sérülékenységek, aminek eredményeként 922 különböző bejegyzést (2013. 02. 08) kapunk. Ez tovább szűkíthető a „Cisco ios" kérdéssel magára az operációs rendszerek sebezhetőségeire. Ekkor a felsorolás már csak 223 elemből áll, amik között sok figyelemre méltó található aktív támadás szempontjából.

Az eszköz konkrét típusa és sérülékenysége alapján kiválaszthatóvá válik az a módszer, amivel a támadó elérheti célját. Ki kell hangsúlyozni, hogy e célok között nem csak a számítógépes rendszerekhez való jogosultság megszerzése, az adatbázisokból történő információk kiszivárogtatása állhat, hanem a – ma már egyre gyakoribb – szolgáltatások vagy a hálózat megbénítása és elérhetetlenné tétele is. Széles körben ismert, hogy pont ez volt a cél 2007-ben Észtországban, ahol naponta bankok, médiacégek és kormányhivatalok szerverei voltak elérhetetlenek – többhetes támadássorozat alatt – órákon keresztül. Könnyen belátható mindenki számára, hogy ezzel a módszerrel hasonló mértékű károkat lehet okozni bárhol a világon a kritikus infrastruktúrákban annak ellenére, hogy jól képzett, professzionális informatikusok megtettek mindent a védelmi rendszerek képességeinek maximális szintre hozásában. Ennek a legegyszerűbb magyarázata az, hogy a rendszerek építésénél gyakran hagyatkozunk mások által gyártott berendezésekre és szoftverekre, melyeknek sérülékenységei ismeretlenek az adott pillanatban a védelmi rendszer szakértő építői számára.

Nézzünk egy-két konkrét példát sérülékenységekre:

1. A Cisco 6400 NRP2 modul Telnet sebezhetősége (dokumentálva: Cisco bug ID CSCdt65960) biztosítja a támadó részére, hogy jelszó nélkül lépjen be az eszköz kezelőfelületére, ha a jelszó eddig még nem volt beállítva. Amennyiben az üzemeltető úgy helyezi üzembe az eszközt, hogy ezt a jelszót nem állította be korábban, akkor a támadó hozzá tud férni az eszközhöz telnet protokoll segítségével a hálózaton keresztül 12.1(05)DC01 vagy annál korábbi Cisco IOS verzió esetén. [6], [7]
2. A Cisco IOS software Telnet opció kezelési sebezhetősége (dokumentálva: Cisco bug ID CSCdm70743) alapján a támadó – kereskedelmi forgalomban vagy ingyenes elérhető – informatikai biztonsági rések automatikus feltárására alkalmas szoftvercsomag alkalmazásával a Cisco router újraindulását éri el, miközben bizonyos UNIX alapú rendszerek specifikált sérülékenységeinek (Telnet ENVIRON option) jelenlétét teszteli. Mielőtt a router jelezné, hogy elfogadja a jelzett opciót váratlanul újraindul, miközben a hozzá csatlakozó infrastrukturális elemek természetesen elérhetetlenek lesznek. A hiba érinti az alábbiakban felsorolt eszközöket bizonyos (11.3AA, 12.0(2)…12.0(6) és – egyes verzió számú – 12.0(7)) Cisco operációs rendszerek esetén:
    a) AS5200, AS5300, és AS5800 sorozatú hálózati beléptető szerver,
    b) 3660, 7100, 7200 és 7500 sorozatú router,
    c) uBR7200 kábel modem végződtető router,
    d) SC3640 rendszer vezérlő a hálózati beléptető szerverek részére,
    e) AS5800-as sorozatú Voice Gateway,
    f) AccessPath LS-3, TS-3, és VS-3 integrált beléptető rendszerek különböző szolgáltatásokhoz. [8], [9]

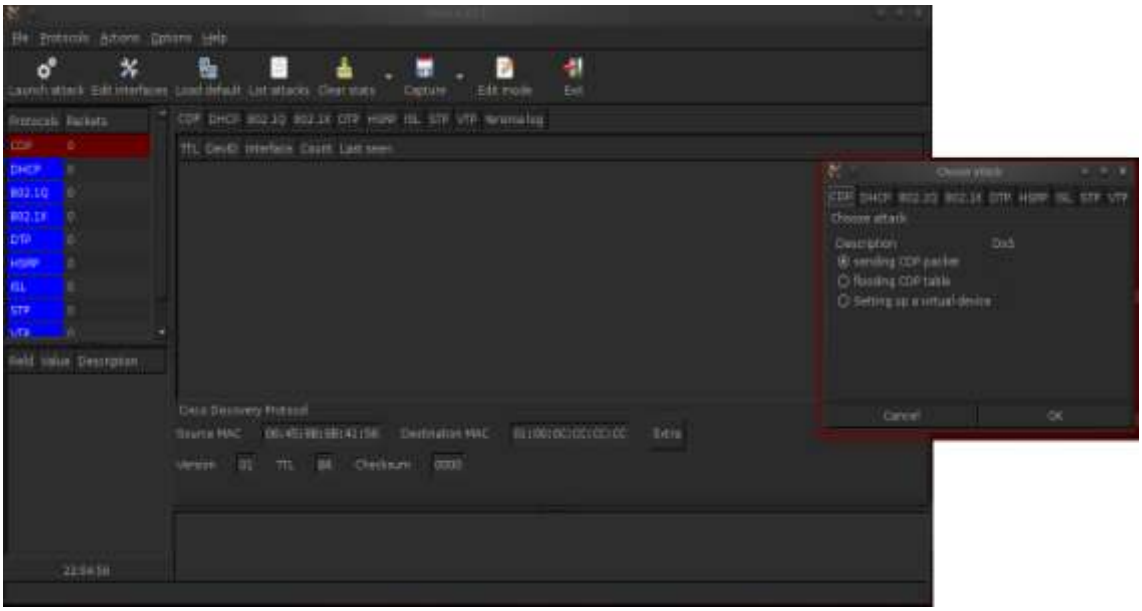
A felsorolt hálózati elemek számossága arra utal, hogy „szinte” független volt a platformtól az operációs rendszer kódjában található hiba, amit a gyártó az újabb verziók kiadásakor megismételt.

A CDP támadás eszköze

Amennyiben a támadó kevésbé akar fáradozni a hálózaton áramló IP csomagok – Wireshark programmal történő – monoton és esetenként kimerítő analizálásával, és drága szabadidejét szeretné más, ennél nagyobb kihívást jelentő támadási vektorok alkalmazásával tölteni, akkor számára kézenfekvő, hogy a CDP támadás kivitelezésére az egyik, széles körben ismert, *Yersinia* – ingyenesen letölthető – szoftvert fogja fegyvertárából elővenni.

A Yersinia egy speciális keretrendszer, mely Layer 2 szintű támadások végrehajtására lett kialakítva. Létezik parancssoros, interaktív karakteres és – ma még csökkentett funkciókkal rendelkező – grafikus felületű változata is. Az alkalmazás CDP menü pontja további funkciókat kínál:

- CDP csomagok küldésére a hálózatba,
- a szomszédos Cisco eszköz CDP táblájának elárasztására és
- virtuális eszköz létrehozására. (4. ábra)



4. ábra. A Yersinia grafikus felülete

A keretrendszer emellett lehetőséget biztosít támadások és penetrációs vizsgálatok végrehajtására különböző protokollok (VTP[7], ISL[8], HSRP[9], DHCP[10], DTP[11], STP[12], IEEE 802.1Q[13] és IEEE 802.1X[14]) esetén, melyek részletes – és egyben érdekességekben bővelkedő – kifejtése messze túlmutat a cikk keretein. [10]

[7] VLAN Trunking Protocol
[8] Inter-Switch Link Protocol
[9] Hot Standby Router Protocol
[10] Dynamic Host Configuration Protocol
[11] Dynamic Trunking Protocol
[12] Spanning Tree Protocol
[13] Hálózati szabvány Virtual LAN-ok számára. [11]
[14] Szabvány Port alapú hálózat hozzáférés vezérlésekről. [12]

4. VÉDEKEZÉS CDP TÁMADÁS ELLEN

A CDP támadások módszerétől függően a Cisco különböző védekezési eljárást, módszert javasolt és/vagy új, javított operációs rendszereket készített. Memória túlcsordulást okozó probléma esetén a gyártó – saját szempontjából – a legkézenfekvőbb megoldást javasolta: meg kell szüntetni a CDP funkciót az egész eszközön „no cdp run" utasítással. Amennyiben a helyi hálózati adminisztrátoroknak továbbra is szüksége van erre a funkcióra, akkor csak bizonyos (számítógép farmok felé vagy internet szolgáltató felé néző) csatlakozási felületeken kell megszüntetni „no cdp enable/set cdp disable" utasítással a CDP csomagok további áramlását.

Természetesen lehetnek olyan esetek, amikor ez utóbbi javaslatot sem lehet elfogadni – ekkor kell a hálózati eszközünk operációs rendszerét lecserélni az alábbiakban felsorolt vagy annál újabb verzióra: [13], [15]

- 12.2(3.6)B
- 12.2(4.1)S
- 12.2(3.6)PB
- 12.2(3.6)T
- 12.1(10.1)
- 12.2(3.6)

5. ÖSSZEGZÉS

Jelen cikk célja leginkább a figyelem felkeltése volt, mivel egyre gyakrabban tapasztalható, hogy a rohamosan fejlődő (pl.: átvitel-technikai sávszélesség, szolgáltatás) igényeket kielégíteni kívánó informatikai menedzsmentnek csak arra marad ideje – mind vállalati, mind állami szektorban egyaránt – a fejlesztés és kivitelezés „szélviharában", hogy a rendszermérnökökkel közösen épphogy üzembe helyezze határidőre a hálózati elemeket. Ennek többnyire az az eredménye, hogy a biztonsági kérdésekre már nem jut elég idő és a router valamint a switch eszközök többnyire gyári (default) beállításokkal és némi alapkonfigurálás után kezdik továbbítani az első biteket. Ez érvényes a hálózatvédelmi eszközök nagy részére is.

A hálózati eszközök gyártói hasonló időprésben vannak az új eszközök mihamarabbi piacra bocsátása miatt, ezért a fejlesztéskor a programkódokban lévő hibák felkutatására és kiszűrésére már nem marad elegendő idő. A szoftverhibák és sérülékenységek előbb vagy utóbb felszínre kerülnek, amiket a támadók kihasználnak terveik végrehajtásához. Mindazok ellenére, hogy a gyártók elismerik eszközeik hibáit, nyilvántartják azokat és gondoskodnak a javításról, még a későbbiekben szembesülhetünk újabb, esetleg korábban nem létező hibákkal is.

Nyilvánvaló, hogy a CDP támadhatósága elég régi keletű, egy kis odafigyeléssel védhető, ellenben most is léteznek sérülékenységek, ami rávilágít arra, hogy az eszközök alkotói ma is tévedhetnek, tehát létezhetnek olyan hibák, amiket mi nem, viszont a támadó ismerhet. Ebből kifolyólag különösen figyelmet kell fordítani a kritikus infrastruktúrák hálózatvédelmi eszközrendszerének kialakítására és a hálózati forgalom elemzésére.

Felhasznált irodalom:

[1] Cisco Discovery Protocol, Posted on July 6, 2011: http://ciscoskills.net/2011/07/06/cisco-discovery-protocol/ (2013.02.05.)

[2] ProCurveSwitch2500Series: http://www.hp.com/rnd/pdfs/datasheets/switch_2500_series.pdf (2013.02.04.)

[3] Using Cisco Discovery Protocol, First Published: February 1, 1995, Last Updated: August 12, 2010: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.pdf (2013.02.05.)

[4] Cisco Discovery Protocol: http://netcert.tripod.com/ccna/switches/cdp.html (2013.02.05.)

[5] Bobs Double Penetration Adventure - Part 2: http://synjunkie.blogspot.hu/2009_10_01_archive.html (2013.02.05.)

[6] Cisco 6400 NRP2 Telnet Vulnerability: http://www.securiteam.com/securitynews/5GP0D204KA.html (2013.02.03.)

[7] Cisco 6400 NRP2 Telnet Vulnerability, Revision 1.0, For Public Release 2001 June 14 15:00 UTC (GMT): http://www.cisco.com/en/US/products/csa/cisco-sa-20010614-nrp2-telnet.html (2013.02.03.)

[8] Cisco IOS Software TELNET Option Handling Vulnerability, Advisory ID: cisco-sa-20000420-ios-telnet, Revision 1.0, For Public Release 2000 April 20 13:00 UTC (GMT): http://www.cisco.com/en/US/products/csa/cisco-sa-20000420-ios-telnet.html (2013.02.03.)

[9] Cisco IOS Software TELNET Option Handling Vulnerability: http://www.securiteam.com/securitynews/5AQ0G000GI.html (2013.02.03.)

[10] Yersinia: http://www.yersinia.net/doc.htm (2013.02.03.)

[11] Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks, IEEE Standard for Local and metropolitan area networks, 31 August 2011 — http://standards.ieee.org/getieee802/download/802.1Q-2011.pdf (2013.02.04.)

[12] Port-Based Network Access Control, IEEE Standard for Local and metropolitan area networks 5 February 2010: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf (2013.02.04.)

[13] Sean Convery, Cisco Systems: Hacking Layer 2: Fun with Ethernet switches http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf (2013.01.18.)

[14] Yusuf Bhaiji Understanding, Preventing, and Defending Against Layer 2 Attacks 2009: http://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf (2013.02.16.)

[15] Cisco's Response to the CDP Issue, Document ID: 13621, For Public Release 2001 October 10: http://www.cisco.com/application/pdf/paws/13621/cdp_issue.pdf (2013.02.18.)

[16] Szabó Tibor: „Network security problems on Layer 2”