hakin9

Útoky na druhou vrstvu síťového modelu OSI

Alfredo Andrés, David Barroso

Pod lupou

Útoky na druhou vrstvu síťového modelu OSI

Alfredo Andrés, David Barroso

stupeň obtížnosti

Zabezpečení druhé vrstvy modelu OSI podceňuje celá řada společností a proto při zjišťování bezpečnosti sítě bývá právě tato vrstva nejslabším článkem. Její zabezpečení bývá často zcela opomíjeno, jelikož útoků na druhou vrstvu modelu OSI není mnoho. Úspěšný útok na tuto vrstvu však může být stejně nebezpečný jako všechny útoky na ostatní vrstvy modelu OSI.

Vrstva datových spojů patří mezi nejméně zabezpečené a často opomíjené prvky sítí. Často se stává, že administrátoři jednoduše připojí switche, nastaví je a dál se o ně již nestarají. Testy průniků (pen-testing) pak často odhalí switche, které používají zranitelné verze systému IOS a které nejsou nijak chráněny. Administrátoři se často také domnívají, že implementace virtuální sítě VLAN zabrání útočníkům před vniknutím. Ochranu pomocí architektury sítě VLAN lze však zdolat, a proto mohou být útoky vyšších vrstev vedeny i napříč sítěmi VLAN.

Výhodou druhé vrstvy modelu OSI je fakt, že pakety spojové vrstvy nemohou být přeneseny sítěmi nad protokolem IP, například přes Internet. Všechny útoky lze tedy vést pouze z vnitřních sítí. Statistiky však hovoří jasně, útoky z vnitřní sítě mohou být stejně nebezpečné jako útoky zvenčí. Navíc bychom si měli uvědomit, že útočník z vnější sítě, který projde přes bránu firewall a dostane se do zóny DMZ, může pomocí útoků na druhou vrstvu modelu OSI zónu DMZ opustit a zaútočit na celou síť. Zaměřme se nyní na obvykle zranitelná místa spojové vrstvy, povězme si, jak mohou být útočníkem zneužity, a co můžeme učinit pro ochranu svého zařízení. Později uvedené příklady se vztahují k zařízení společnosti Cisco, ovšem některé lze využít i k ochraně zařízení od jiných výrobců.

Většinu uváděných postřehů a dat jsme získali od autorů nástroje Yersinia, kteří je sepsali při studiu a vývoji tohoto nástroje. Někdy nebylo možné získat oficiální informace nebo veřejně přístupný kód, proto jsou některá pozorování založena na studiu chování nikoliv na uveřejněných standardech.

Z tohoto článku se naučíte...

- specifikace protokolů druhé vrstvy modelu OSI: STP, CDP, DTP, IEEE 802.1Q, VTP,
- jak probíhají útoky proti těmto protokolům,
- jak před těmito útoky ochránit systém,
- jak používat nástroj Yersinia, který je užitečný pro administrátory a pen-testery (testery průniků).

Měl byste vědět...

- měli byste mít základní znalosti druhé vrstvy modelu OSI,
- měli byste být obeznámeni s technologií společnosti Cisco.

Sedm vrstev modelu OSI

Model OSI (*Open Systems Interconnection*) byl navržen v roce 1977, aby se stal standardem pro vzájemnou komunikaci mezi zařízeními od různých výrobců. Tento model definuje několik vrstev spojených s přenosem dat, od nejnižší (fyzické) až po nejvyšší (aplikační) vrstvu. Mezi jednotlivými vrstvami existuje silná závislost, například hlavičky jednotlivých protokolů se přidávají při přechodu z nižší do vyšší vrstvy modelu OSI. Sedm vrstev modelu OSI tvoří:

- 1. vrstva – fyzická vrstva: provádí správu (a řízení) komunikace na síťovém kanálu,
- 2. vrstva – spojová vrstva: umožňuje doručení datových bloků,
- 3. vrstva – síťová vrstva: zodpovídá za směrování datových paketů,
- 4. vrstva – transportní vrstva: zodpovídá za spolehlivé doručení dat (bez chyb),
- 5. vrstva – relační vrstva: umožňuje řídit komunikaci mezi aplikacemi,
- 6. vrstva – prezentační vrstva: usnadňuje přenos dat v daném datovém formátu mezi aplikacemi, řadí prezentační data,
- 7. vrstva – aplikační vrstva: umožňuje aplikacím přístup k modelu OSI (k síti).

Protokol STP (Spanning Tree Protocol)

Protokol STP zabraňuje vzniku cyklů v síti během propojování síťových prvků. Protokol zaručuje, aby mezi dvěma zařízeními existovala pouze jediná cesta. Každý paket protokolu STP se nazývá BPDU (*Bridge Protocol Data Unit*) a identifikujeme jej podle jeho formátu: paket podle standardu IEEE 802.3 s hlavičkou podle standardu 802.2 a cílovou adresou MAC 01:80:C2:00:00:00 (viz Obrázek 1).

Existují dva typy paketů BPDU: konfigurační paket (*Configuration*) a paket TCN (*Topology Change Notification*). První typ se odesílá pravidelně, zatímco druhý se odesílá po zjištění síťové změny (například otevření/uzavření portu). Podrobnější informace o protokolu STP naleznete ve standardu IEEE Standard 802.1D (viz sekce *Na Internetu*).

Útoky

Hlavní vadou protokolu STP je nedostatečná autentizace a řízení. Každé zařízení, každá osoba nebo útočník může odeslat paket BPDU a pracovat s protokolem.

Abychom porozuměli útokům, musíme znát formát paketu *Configuration* BPDU (viz Obrázek 2):

- *PID* (2 bajty): protokol, vždy nabývá hodnoty 0,
- *Version* (1 bajt): verze protokolu STP, může nabývat hodnot nula (protokol STP), jedna (protokol RSTP nebo tři (protokol MSTP),
- *Message type* (1 bajt): typ paketu BPDU: configuration (0x00) nebo TCN (0x80),
- *Flags* (1 bajt): slouží pro nastavení portů (užitečné pro protokol RSTP) a částečně také pro upozornění na změnu v topologii,
- *Root ID* (8 bajtů): ID kořenového zařízení,
- *Root path cost* (4 bajty): cena cesty ke kořenovému zařízení,
- *Bridge ID* (8 bajtů): ID odesílatele paketu BPDU,
- *Port ID* (2 bajty): číslo portu (IEEE nebo Cisco STP BPDU), ze kterého byl paket BPDU odeslán,
- *Message age* (2 bajty): doba, která uplynula od odeslání konfigurační zprávy, na které je tento paket založen,
- *Maximum age* (2 bajty): čas, kdy by měla být tato konfigurační zpráva vymazána,
- *Hello time* (2 bajty): čas, který uplynul mezi dvěma konfiguračními pakety BPDU,

Nástroj Yersinia

Ke spuštění útoků na vrstvu datových spojů využijeme nástroj Yersinia od autorů tohoto článku. Nástroj Yersinia je přenositelný – napsaný v jazyku C (pomocí knihoven libpcap a libnet) a vícevláknový (podporuje více uživatelů a více souběžných útoků). Nástroj můžeme využít k analýze, editaci a sledování síťových paketů nebo dokonce k uložení síťového provozu ve formátu pcap.
Nejnovější verze nástroje Yersinia (0.5.5.2) podporuje následující protokoly:

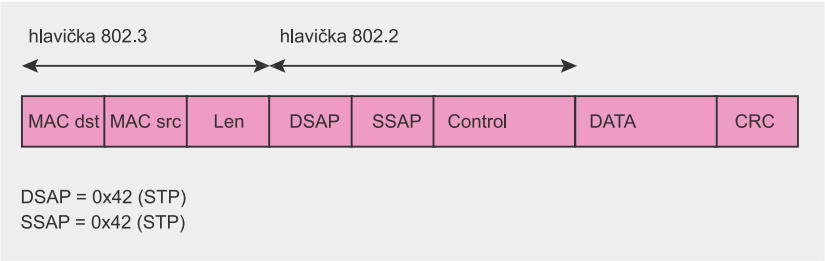
- *Spanning Tree Protocol* (STP),
- *Cisco Discovery Protocol* (CDP),
- *Dynamic Trunking Protocol* (DTP),
- *Dynamic Host Configuration Protocol* (DHCP),
- *Hot Standby Router Protocol* (HSRP),
- IEEE 802.1Q,
- *Inter-Switch Link Protocol* (ISL),
- *VLAN Trunking Protocol* (VTP).

Nástroj Yersinia může pracovat v některém ze tří hlavních režimů:

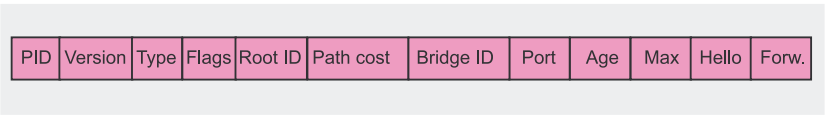
- režim příkazového řádku: lze využít k vedení útoků ad-hoc – tento režim byl implementován, aby bylo možné využít nástroje Yersinia ve skriptech,
- režim síťový démon: umožňuje využít nástroj Yersinia ze vzdáleného umístění – knihovna CLI se podobá knihovně využívané zařízeními společnosti Cisco,
- režim GUI: napsaný pomocí balíku ncurses.

Všechny popisované útoky jsme spustili v režimu GUI, i když mohou být spuštěny i v ostatních režimech. Chcete-li zjistit, jaké funkce nástroj Yersinia nabízí, stiskněte po jeho spuštění v režimu GUI klávesu [*h*] (`yersinia -I`). Poznámka: ke spuštění vyžaduje režim GUI velké množství řádků a sloupců – pokud tedy režim selže, zkuste maximalizovat okno terminálu.

Nástroj Yersinia zahrnuje také útoky na protokoly jiných vrstev modelu OSI (například HSRP, DHCP), ovšem my se zaměříme pouze na funkce spojené s druhou vrstvou. Název nástroje byl odvozen od jména bakterie, která byla v Evropě původcem středověkého *moru* – *Yersinia pestis*.



Obrázek 1. *Struktura paketu BPDU*



Obrázek 2. *Struktura paketu Configuration BPDU*

- *Forward delay* (2 bajty): prodleva, kterou by měly zachovat mosty po změně topologie sítě, ale před přechodem do jiného stavu.

Základní funkce protokolu STP jsou: volba kořenového zařízení a výpočet cesty přes všechna zařízení, které tvoří kostru grafu. Volby kořenového zařízení se zpočátku účastní všechna zařízení. Jako kořenové zařízení se vybere zařízení s nejnižším identifikačním číslem (ID). Když po zvolení kořenového zařízení dojde ke změně v síti, cesty se přepočítají. Pokud se odpojí současný kořenový uzel nebo se připojí uzel s nižším identifikačním číslem, provádí se volba znovu.

Praktické použití

Podívejme se na tři možné útoky na protokol STP. První dva představují útoky typu DoS (*Denial of Service*). Oba útoky donutí síťová zařízení nad protokolem STP přepočítat síťové cesty. Tím vzniká nestabilita sítě, protože každý switch spotřebuje při přepočtu cesty procesorový čas a paměť. Tyto útoky mohou současně způsobit zdání cyklů v síti. V nejhorším případě může dojít k pádu celé sítě a opakovanému rozesílání duplikovaných paketů, které síť zahlcují a způsobí její nefunkčnost.

Princip útoků tohoto typu je celkem jednoduchý. Útoky jsou založeny na zasílání tisíců paketů BPDU (v případě prvního útoku – paketů *Configuration* BPDU a v druhém případě – paketů TCN) s náhodně generovanou adresou MAC (a dalšími poli paketu *Configuration* BPDU, například *Bridge ID*). Útoky předstírají, že se k síti připojuje tisíce nových zařízení, které se chtějí podílet na protokolu STP. Není divu, že vzniká zmatek.

Oba útoky – *sending conf BPDUs* a *sending tcn BPDUs* – můžeme provést pomocí nástroje Yersinia (chcete-li zvolit typ útoku, stiskněte v režimu GUI klávesu [*x*]). Odezvu switche zobrazují Výpisy 1 a 2.

Třetí útok předstírá, že získal roli kořenového uzlu protokolu STP. Útok nejprve zachytí paket BPDU, který obsahuje ID kořenového uzlu. Potom se nastaví systém útoku. Útok vystupuje jako nové síťové zařízení, které se chce připojit k protokolu STP a má nižší ID než současný kořenový uzel. Identifikační číslo nového kořenového uzlu se získá odečtením jedničky od ID skutečného uzlu. Jednotlivá ID se tedy příliš neliší a administrátor nemůže letmým pohledem rozdíl zjistit.

Důsledkem tohoto útoku je nestabilita sítě. Musíme si uvědomit, že když účastníci sítě zjistí, že v síti došlo ke změně, odesílají kořenovému zařízení potvrzení (TCN). Po obdržení potvrzení odešle kořenové zařízení paket *Configuration* BPDU s bitem změny nastaveným na hodnotu 1 (pole *Flags*), aby si všechna zařízení přepočítala cesty. Pokud byl útok úspěšný, zahazuje nové, falešné kořenové zařízení pakety TCN od

Dekódování paketů

I když dekódování a sledování paketů protokolů druhé vrstvy umožňuje i nástroj Yersinia, můžeme pro tyto funkce využít jiné nástroje, například nástroj tcpdump nebo Ethereal. Pro zachytávání paketů protokolu STP spustíme nástroj Ethereal s těmito parametry:

```
# ethereal -f stp
```

Výpis 1. *Následky útoku typu DoS, který zasílá pakety Configuration BPDU*

```
01:20:26: STP: VLAN0001 heard root 32768-d1bf.6d60.097b on Fa0/8
01:20:26: STP: VLAN0001 heard root 32768-9ac6.0f72.7118 on Fa0/8
01:20:26: STP: VLAN0001 heard root 32768-85a3.3662.43dc on Fa0/8
01:20:26: STP: VLAN0001 heard root 32768-3d84.bc1c.918e on Fa0/8
01:20:26: STP: VLAN0001 heard root 32768-b2e2.1a12.dbb4 on Fa0/8
```

Výpis 2. *Následky útoku typu DoS, který zasílá pakety TCN BPDU*

```
01:35:39: STP: VLAN0001 Topology Change rcvd on Fa0/8
01:35:39: STP: VLAN0001 Topology Change rcvd on Fa0/8
01:35:39: STP: VLAN0001 Topology Change rcvd on Fa0/8
01:35:39: STP: VLAN0001 Topology Change rcvd on Fa0/8
01:35:39: STP: VLAN0001 Topology Change rcvd on Fa0/8
```

Výpis 3. *Následky útoku Claiming Root Role*

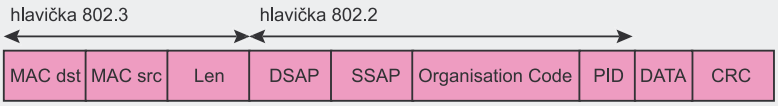
```
01:58:48: STP: VLAN0001 heard root 32769-000e.84d4.2280 on Fa0/8
01:58:48:     supersedes 32769-000e.84d5.2280
01:58:48: STP: VLAN0001 new root is 32769, 000e.84d4.2280 on port Fa0/8, cost 19
```

switchů. Žádný switch tedy neprovede přepočítání cesty. Postupně tak dojde k poškození síťové struktury.

Ke spuštění útoku pomocí nástroje Yersinia musíme nejprve stisknout klávesu [*d*], abychom paket BPDU naplnili výchozími hodnotami, potom spustíme útok *Claiming Root Role* (stiskněte klávesu [*x*] a zvolte čtvrtý útok). Tento útok je tvořen dvěma fázemi. Nejprve odposlechneme paket configuration BPDU, abychom zjistili ID kořene, a potom každých *hello time* sekund odešleme nový, podvržený paket configuration BPDU. Reakce switche je zobrazena na Výpisu 3.

Identifikační číslo (ID) původního kořene bylo 32769-000e.84d5.2280, zatímco nové číslo má hodnotu 32769-000e.84d4.2280. Pokud si identifikační číslo kořene pečlivě prohlédneme, zjistíme, že patnáctý znak je nyní číslo 4 místo původního čísla 5. Naše virtuální zařízení má tedy nižší ID a proto bylo zvoleno jako nový kořen protokolu STP.

Existují ještě další způsoby útoků na protokol STP, některé implementuje i nástroj Yersinia. Uveďme si například metodu *Causing Eternal Root Elections* – odesílají se pakety s nižšími a nižšími identifikačními čísly, volba kořene tedy nikdy nekončí a v síti dochází ke všeobecnému chaosu. Další útok se nazývá *Claiming Root Role with MiTM*, což je útok typu *Man-in-the-Middle*. Vyzkoušet můžeme také útok *Claiming Other Role*, který představuje pokus o vystupování jako libovolný další uzel – útok *Claiming Other Role* představuje *prokázání principu* (*proof-of-concept*), nemá žádné negativní důsledky.



DSAP = 0xAA (SNAP)
SSAP = 0xAA (SNAP)
Organisation Code = 0x00000C (Cisco)
PID = 0x2000 (CDP)

Obrázek 3. *Struktura paketu protokolu CDP*

Obrázek 4. *Pole paketu protokolu CDP*

Protiopatření

Chce-li administrátor zabránit útokům na zařízení od společnosti Cisco, měl by:

- vypnout protokol STP, pokud jeho použití není nezbytně nutné,
- využít rozšíření *Spanning Tree Portfast BPDU Guard Enhancement* a *Spanning Tree Protocol Root Guard Enhancement* (viz sekce *Na Internetu*).

Protokol CDP (Cisco Discovery Protocol)

CDP je protokol chráněný autorskými právy společnosti Cisco. Umožňuje vzájemnou komunikaci mezi různými síťovými zařízeními společnosti Cisco. Ostatní výrobci však protokol mohou také používat, pokud si ovšem technologii zakoupí (což udělala například společnost Hewlett-Packard).

Paket protokolu CDP nejsnáze určíte sledováním těchto rysů: paket standardu IEEE 802.3 s hlavičkou SNAP standardu 802.2 a cílovou adresou MAC pro všesměrové vysílání 01:00:0C:CC:CC:CC (viz Obrázek 3).Paket protokolu CDP obsahuje zajímavé informace o vlastnostech zařízení, které zasílá paket. Mezi tyto informace patří například:

- název zařízení,
- model,
- verze systému IOS,
- adresa IP (adres může být více),
- doména VTP,
- vlastnosti zařízení (switch, router, most apod.).

Tato data, která jsou opakovaně odesílána každým zařízením společnosti Cisco, nabízejí velmi užitečné informace, které lze využít při pozdějších útocích. Implicitně bývá podpora protokolu CDP zapnuta a informace se odesílají každých 180 sekund (každé 3 minuty).

Útoky

Pro odeslání ani přijímání paketů protokolu CDP není vyžadována autentizace. Data paketu bývají navíc odeslána jako prostý text. Tento fakt velmi usnadňuje vedení útoků. Navíc je formát protokolu CDP vysvětlen na webových stránkách společnosti Cisco (viz sekce *Na Internetu*). Paket protokolu CDP tvoří následující pole (viz Obrázek 4):

- *Version* (1 bajt): udávaná verze protokolu CDP, obvykle nabývá hodnoty jedna nebo dvě,
- *TTL* (1 bajt) – *Time To Live*: životnost paketu protokolu CDP,
- *Checksum* (2 bajty): ověření platnosti paketu,
- *TLV* (proměnlivá délka) – Sada polí *Type*, *Length*, *Value*. Pole

Tabulka 1. *Příklady záznamů pole TLV*

Obsah pole TLV	Typ	Délka	Hodnota
0001 0008 7a61 7065	*Device ID* (0x0001)	8 (0x0008) (dva bajty pro typ, dva bajty pro délku a čtyři bajty pro hodnotu)	*zape* (0x7a 0x61 0x70 0x65)
000b 0005 01	*Duplex type* (0x000b)	5 (0x0005) (dva bajty pro typ, dva bajty pro délku a jeden bajt pro hodnotu)	0x01 (Full Duplex)

Výpis 4. *Důsledky útoku typu DoS na protokol CDP*

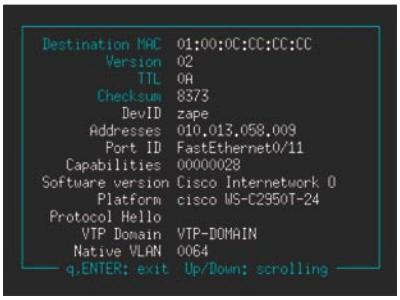
```
# show cdp neighbours
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
2EEEWWW          Gig 0/1           253                    yersinia  Eth 0
ZCCCUU9          Gig 0/1           250        T S I r     yersinia  Eth 0
J222FFX          Gig 0/1           249        R T         yersinia  Eth 0
WAAASS6          Gig 0/1           240        R B I r     yersinia  Eth 0
2IIWWWE          Gig 0/1           249        T B H I     yersinia  Eth 0
K333FFX          Gig 0/1           234        R T         yersinia  Eth 0
TBBBOO7          Gig 0/1           252        B H r       yersinia  Eth 0
3KKYKYY          Gig 0/1           250        R B H       yersinia  Eth 0
TBBBPP7          Gig 0/1           252        S H I r     yersinia  Eth 0
```

TLV obsahuje vlastní data, která představuje seznam záznamů pole TLV, každý záznam má tento formát: *Type* (2 bajty) – typ popisovaných dat (např. *Device ID*, *Address*, *Port ID*), *Length* (2 bajty) – délka pole TLV a *Value* (proměnlivá délka) – vlastní hodnota (seznam příkladů záznamů pole TLV naleznete v Tabulce 1, nástroj Yersinia znázorňující hodnoty pole TLV ukázkového paketu je zobrazen na Obrázku 5).

Jestliže známe formát paketu, můžeme se zasíláním podvržený paket protokolu CDP vydávat za síťové zařízení. Zranitelnost vůči útokům typu DoS na starší verze systému IOS společnosti Cisco odhalil FX z týmu Phenoelit (viz sekce *Na Internetu*). Pokud odešleme velké množství paketů protokolu CDP s různými identifikačními čísly (vystupujeme jako různá síťová zařízení), zahltíme paměť zařízení. Tím dojde ke zhroucení zařízení, které musí být kvůli správné funkci restartováno. Podobný útok tedy může způsobit odpojení síťového segmentu nebo, jestliže útočník napadne router, odpojení přístupu k Internetu až do restartu zařízení.

Praktické použití

Připojíme-li se k síti, která obsahuje zařízení podporující protokol CDP, režim GUI rychle zobrazí režimy



Obrázek 5. *Pole TLV ukázkového paketu zobrazeného pomocí nástroje Yersinia*

těchto zařízení. První útok na protokol CDP založíme na výše zmíněném zranitelném místě. Pro útok tohoto typu již další informace nepotřebujeme. V grafickém uživatelském rozhraní nástroje Yersinia v režimu CDP stiskněte klávesu [*x*] a zvolte útok *flooding CDP table*. Důsledek útoku je zobrazen na Výpisu 4 a záznamy switche na Výpisu 5.

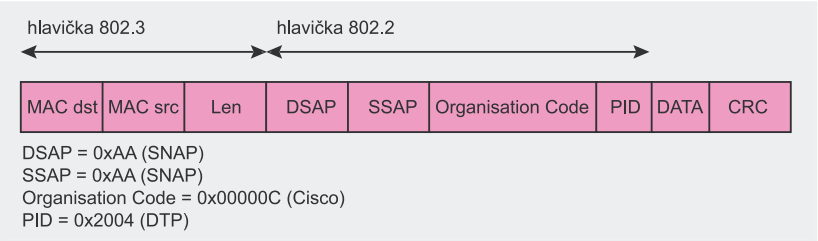
Nástroj Yersinia zahrnuje také další útok, který umožňuje sestavit virtuální zařízení od společnosti Cisco. Při kontrole zařízení sousedících s jedním z reálných zařízení se administrátorovi v konzoli zobrazí všechna podvržená virtuální zařízení. Tento útok nemá kromě rozčílení síťového administrátora (administrátor bude jistě chtít zjistit, jaká nová

Výpis 5. *Důsledky útoku typu DoS na protokol CDP – záznamy ze switche*

```
00:06:08: %SYS-2-MALLOCFAIL: Memory allocation of 224 bytes failed from 0x800118D0, alignment 0
Pool: Processor  Free: 0  Cause: Not enough free memory
Alternate Pool: I/O  Free: 32  Cause: Not enough free memory
-Process= "CDP Protocol", ipl= 0, pid= 26
-Traceback= 801DFC30 801E1DD8 800118D8 80011218 801D932C 801D9318
00:06:08:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:09:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:10:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:11:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:12:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:13:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:14:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:15:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:16:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:17:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:18:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:19:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:20:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:21:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:22:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:23:  ../src-calhoun/strata_stats.c at line 137: can't not push event list
00:06:38: %SYS-2-MALLOCFAIL: Memory allocation of 140 bytes failed from 0x801E28BC, alignment 0
Pool: Processor  Free: 0  Cause: Not enough free memory
Alternate Pool: I/O  Free: 32  Cause: Not enough free memory
```

Co je to sdružování portů

V oblasti telekomunikací představuje termín *sdružený port* linku, která umožní přenést mezi dvěma výměnami dat současně více než jeden hlasový nebo datový kanál. V síti lze sdružený port sestavit mezi dvěma switchi. Sdružování portů umožňuje odesílat data z několika virtuálních sítí VLAN pomocí stejné fyzické linky.



Obrázek 6. *Struktura paketu protokolu DTP*

Obrázek 7. *Struktura paketu protokolu DTP (bez hlaviček protokolu Ethernet)*

zařízení se připojila k síti) žádné negativní důsledky.

Protiopatření

Jediným účinným opatřením, jak zabránit útokům proti protokolu CDP, je vypnout podporu protokolu pomocí příkazu `no cdp run`.

Protokol DTP (Dynamic Trunking Protocol)

DTP je protokol chráněný autorskými právy společnosti Cisco, který podporuje sdružené porty (trunk, viz sekce *Co je to sdružování portů*) mezi switchi pracujícími nad druhou vrstvou modelu OSI. Pakety protokolu DTP mívají cílovou adresu MAC nastavenu na hodnotu 01:00:0C:CC:CC:CC a rámec dle standardu IEEE 802.3 s hlavičkou SNAP dle standardu 802.2 (viz Obrázek 6). Protokol DTP je dostupný pro většinu switchů společnosti Cisco kromě modelů XL.

Podpora protokolu DTP bývá v zařízeních společnosti Cisco implicitně zapnuta a připravena k vyjednávání se všemi porty switche. Abychom však mohli sdružený port sestavit, musíme vědět, jak vyjednávání probíhá. Specifikace protokolu DTP je však chráněným vlastnictvím společnosti Cisco (není veřejná), což pochopení procesu značně znesnadňuje. Aby tedy autoři článku pochopili formát protokolu DTP, museli provést takzvaný reverse engineering síťového provozu mezi dvěma switchi.

Protokol DTP zajišťuje aktivaci sdruženého portu i typ zapouzdření nutný k odeslání i přijetí dat prostřednictvím daného portu. Nejběžnější zapouzdření definuje specifikace protokolu IEEE 802.1Q, který podporuje většina switchů společnosti Cisco. Specifikace IEEE 802.1Q je veřejný standard. Použít lze na druhou stranu také protokol ISL, který je chráněn autorskými právy společnosti Cisco a je podporován nejvyšší třídou zařízení společnosti Cisco. Hlavním důvodem zapouzdření je nutnost značkovat pakety podle jejich odpovídající virtuální sítě VLAN. Zapouzdření dat tedy switchům usnadňuje rozhodnutí, kam paket odeslat.

Útoky

Protokol DTP nepoužívá autentizaci odesílatele a, jak jsme již zmínili, je implicitně zapnut na všech portech. Jedinou potíží tedy bude vyjednat spojení pomocí protokolu DTP. Pokud se nám to podaří, budeme mít přístup do ostatních virtuálních sítí VLAN. Abychom dojednání spojení pochopili, musíme nejprve pochopit formát paketu protokolu DTP (viz Obrázek 7):

- *Domain* (32 bajtů): textový řetězec ve formátu ASCII podle domény protokolu VTP,
- *Status* (1 bajt): zobrazuje stav portu: *on*, *off*, *desirable* nebo *auto*; výchozí nastavení: *desirable* – můžeme začít s vyjednáváním na protokolu DTP,
- *Type* (1 bajt): podporovaný typ zapouzdření: *ISL*, *802.1Q*, *negotiated* (protokol ISL nebo 802.1Q) nebo *native*,
- *Neighbor-ID* (6 bajtů): identifikace zařízení, které paket odesílá; obvykle adresa MAC portu.

Při vyjednávání na protokolu DTP mezi zařízeními společnosti Cisco se nejprve odešlou tři pakety (v intervalu jeden paket za sekundu), které představují stav sdružování portů a požadovaný typ zapouzdření. Následně se paket protokolu DTP odesílá každých 30 sekund. Nástroj Yersinia toto chování implementuje pomocí samostatného vlákna. Abychom mohli podle potřeby změnit stav zařízení, musíme sledovat stav ostatních zařízení. To vyřešíme pomocí cyklu, který přijímá pakety protokolu DTP. Nástroj Yersinia změní stav protokolu DTP podle druhého zařízení již po několika testech.

Výpis 6. *Stav sítě VLAN před útokem*

```
zipi# sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/24
                                                Gi0/1, Gi0/2
100  Office                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
200  Internet                         active    Fa0/20, Fa0/21, Fa0/22, Fa0/23
```

Výpis 7. *Stav portu protokolu DTP získaný z konzole switche*

```
zipi# sh dtp int Fa0/10
DTP information for FastEthernet0/10:
  TOS/TAS/TNS:                              ACCESS/DESIRABLE/ACCESS
  TOT/TAT/TNT:                              NATIVE/802.1Q/802.1Q
  Neighbor address 1:                       000000000000
  Neighbor address 2:                       000000000000
```

Výpis 8. *Stav portů po útoku*

```
zipi# sh dtp int fa0/10
DTP information for FastEthernet0/10:
  TOS/TAS/TNS:                              TRUNK/DESIRABLE/TRUNK
  TOT/TAT/TNT:                              802.1Q/802.1Q/802.1Q
  Neighbor address 1:                       666666666666
  Neighbor address 2:                       000000000000
```

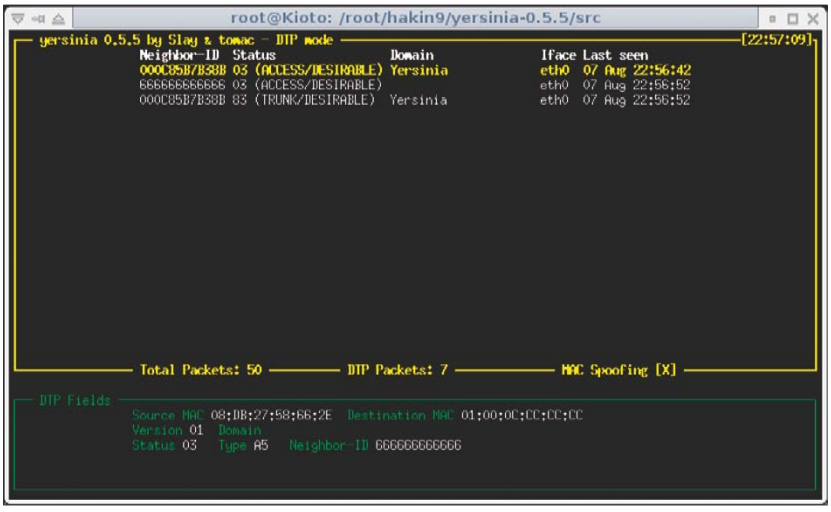
Výpis 9. *Porty přidělené síti VLAN po útoku*

```
zipi# sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/24
                                                Gi0/1, Gi0/2
100  Office                           active    Fa0/11, Fa0/12, Fa0/13
200  Internet                         active    Fa0/20, Fa0/21, Fa0/22, Fa0/23
```

Praktické použití

Ukažme si, jak probíhá útok vedený proti switchi Catalyst 2950T se systémem IOS verze 12.1.(22) EA3. Název hostitele byl nastaven na *zipi*. Zařízení obsahuje dvě virtuální sítě: *Office* (porty Fa0/10, Fa0/11, Fa0/12 a Fa0/13) a *Internet* (porty Fa0/20, Fa0/21, Fa0/22 a Fa0/23). Doménu protokolu VTP změníme na *Yersinia*. Ostatním parametrům ponecháme výchozí hodnoty. Stav sítě VLAN před útokem zobrazuje Výpis 6.

V režimu GUI nástroje Yersinia zvolte okno s protokolem DTP. Pokud vaše síť využívá protokol DTP, zobrazí se jeho data do 30 sekund. Stav portu protokolu DTP zjistíme také z konzole switche: číslo portu je Fa0/10 a stav je výchozí (viz Výpis 7).



Obrázek 8. *Důsledky útoku na protokol DTP*

Pomocí klávesy [*d*] naplníme pole ve spodní části okna výchozími hodnotami. Klávesa [*e*] nám umožní změnit obsah pole *Neighbor-ID* a vložit hodnotu 666666666666. Editaci ukončíme stiskem klávesy [*return*].

Pomocí klávesy [*x*] se přepneme do okna s útoky a vybereme útok *enabling trunking*. Stav portu protokolu DTP se změní na *TRUNKING* a pole *Neighbor address 1* bude obsahovat naše ID (viz Výpis 8). Pokud se navíc jako před chvílí podíváme na porty sítí VLAN, zjistíme, že port Fa0/10 již není v seznamu sítí VLAN (viz Výpis 9). V hlavním okně nástroje Yersinia jsou zobrazeny nové pakety; pakety podvržené nástrojem Yersinia mají v poli *Neighbor-ID* uvedenu hodnotu 666666666666 (viz Obrázek 8). Nyní již můžeme vést útoky proti protokolům 802.1Q a VTP. A co je zajímavější, můžeme se chovat jako skutečný switch, který umožňuje sniffing sítě VLAN (z jiných sítí VLAN, než ke které jsme připojeni).

Protiopatření

Jediné proveditelné opatření proti útokům na protokol DTP představuje vypnutí podpory automatického sdružování portů pomocí příkazu `switchport mode access`. Chce-li však poté administrátor nastavit nový sdružený port, je nucen zapnout podporu sdružování portů ručně (ručně nastavit switch).

Protokol IEEE 802.1Q

Protokol IEEE 802.1Q je veřejnou specifikací. Jeho specifikace popisuje formát paketů, které procházejí sdružovanými linkami. Právě kvůli otevřené povaze specifikace byl tento standard přijat většinou výrobců a běžně se využívá pro sdružování portů. Není ovšem jediný. Většina výrobců implementuje také svá vlastní řešení. Společnost Cisco využívá například svůj vlastní patentovaný protokol ISL (*Inter-Switch Link*).

Když switch přijme rámec, přidá značku protokolu 802.1Q (4 bajty),

přepočítá hodnotu pole FCS (*Frame Check Sequence*) a upravený paket odešle na sdruženou linku. Pole přidaná protokolem 802.1Q do rámce protokolu Ethernet_II zobrazuje Obrázek 9. Pole VID představuje síť VLAN, pro kterou je paket určen. Pole nabývá hodnot v rozsahu od 0 do 4 096. Pokud vytvoříme sdruženou linku a switch podporuje protokol 802.1Q, můžeme teoreticky odesílat pakety mezi různými sítěmi VLAN.

Útoky

Abychom mohli protokol 802.1Q využít, musíme vytvořit sdružený port. V předchozím oddíle jsme se naučili, jak zapnout podporu sdružených portů nad protokolem DTP a také jak určit, že zapouzdření proběhne pomocí protokolu 802.1Q. Předpokládejme, že byla sdružená linka sestavena na odpovídajícím portu.

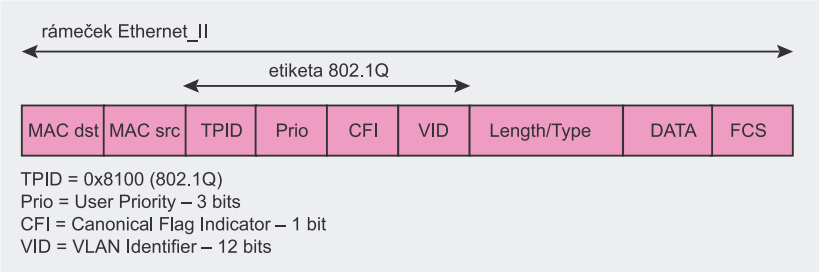
Útoky proti protokolu 802.1Q můžeme rozdělit do dvou kategorií:

- odesílání rámců protokolu 802.1Q na cizí sítě VLAN,
- využití dvakrát zapouzdřených rámců protokolu 802.1Q – útok tohoto typu přidává do původního rámce dvě značky. Když switch odstraní první značku, jako cílové místo se použije síť VLAN uvedená ve druhé značce.

Praktické použití

Nejprve pomocí nástroje Yersinia zkusíme odeslat dvakrát zapouzdřené rámce protokolu 802.1Q. Pole v okně protokolu 802.1Q naplníme výchozími hodnotami (klávesa [*d*]) a přepneme se do editačního režimu (klávesa [*e*]). Hodnotu v poli *Source MAC* změníme na 66:66:66:66:66:66, hodnotu v poli *VLAN* na 16 a hodnotu v poli *VLAN2* na 1. Nakonec editační režim opustíme ([*return*]). Nyní se pomocí klávesy [*x*]přesuneme do okna s útoky a zvolíme útok *sending 802.1Q double enc. packet*.

K odesílání paketů *ICMP Echo Request* s textem *YERSINIA* využívá nástroj Yersinia protokol 802.1Q. Paket dekódovaný pomocí nástroje Ethereal zobrazuje Výpis 10 (ně-



Obrázek 9. *Pole přidaná přidaná do rámce protokolu Ethernet_II protokolem 802.1Q*

Výpis 10. *Paket ICMP Echo Request nástroje Yersinia dekódovaný pomocí nástroje Ethereal*

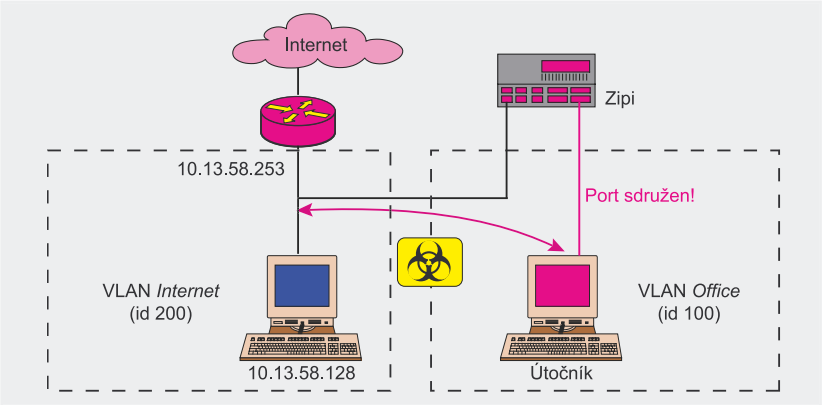
```
Ethernet II, Src: 66:66:66:66:66:66, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source: 66:66:66:66:66:66 (66:66:66:66:66:66)
    Type: 802.1Q Virtual LAN (0x8100)
802.1q Virtual LAN
    111. .... .... .... = Priority: 7
    ...0 .... .... .... = CFI: 0
    .... 0000 0001 0000 = ID: 16
    Type: 802.1Q Virtual LAN (0x8100)
802.1q Virtual LAN
    111. .... .... .... = Priority: 7
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0001 = ID: 1
    Type: IP (0x0800)
Internet Protocol, Src Addr: 10.0.0.1 (10.0.0.1), ↩
      Dst Addr: 255.255.255.255 (255.255.255.255)
    Protocol: ICMP (0x01)
    Source: 10.0.0.1 (10.0.0.1)
    Destination: 255.255.255.255 (255.255.255.255)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Checksum: 0xb953 (correct)
    Identifier: 0x0042
    Sequence number: 00:42
    Data (8 bytes)
0000  59 45 52 53 49 4e 49 41                          YERSINIA
```

která pole byla kvůli srozumitelnosti vynechána). Názorně vidíme, že jsme odeslali dvakrát zapouzdřený rámec protokolu 802.1Q – nejprve pro síť VLAN 16 a následně pro síť VLAN 1.

Uvedený útok slouží pouze pro demonstraci, že je možné přeposílat síťový provoz do jiné sítě (jedná se o takzvaný *VLAN-hopping*). Aplikovat však můžeme i pokročilejší útoky například útok typu *Man-in-the-Middle*.

Výpis 11. *Nastavení sítě VLAN pro vedení útoku*

```
zipi# sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/24
                                                Gi0/1, Gi0/2
100  Office                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
200  Internet                         active    Fa0/20, Fa0/21, Fa0/22, Fa0/23
```



Obrázek 10. *Mapa sítě nad protokolem 802.1Q*

Budoucí verze nástroje Yersinia budou mít implementovány i tyto útoky.

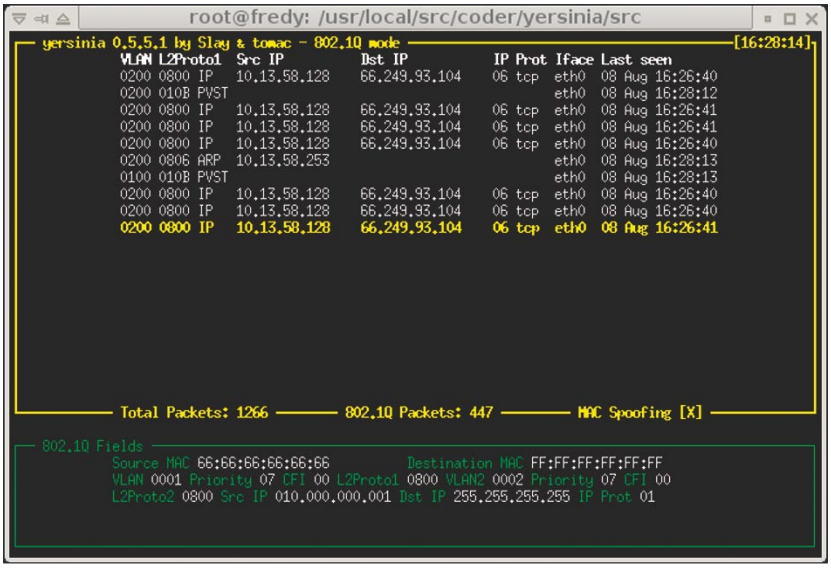
Další útok vyžaduje poněkud složitější nastavení. Představme si, že máme switch nazvaný *zipi* se systémem IOS 12.1(22) EA3 a dvě sítě VLAN: *Office* (porty Fa0/10, Fa0/11, Fa0/12 a Fa0/13) a *Internet* (Fa0/20, Fa0/21, Fa0/22 a Fa0/23) (viz Výpis 11). Doménu protokolu VTP změníme na *Yersinia*. Ostatní proměnné ponecháme beze změny.

Obrázek 10 znázorňuje strukturu sítě. Zařízení útočníka je připojeno k síti VLAN 100 (*Office*) na portu Fa0/10. K síti VLAN 200 (*Internet*) je připojen počítač se systémem Windows a adresou IP 10.13.58.128. Na Obrázku 10 také vidíme, že zařízení ze sítě VLAN *Internet* mají přístup k Internetu pomocí routeru s adresou IP 10.13.58.253, zatímco síť VLAN *Office* přístup k Internetu nemá.

Pokusíme se přistoupit k datům odesílaným z počítače se systémem Windows, který je umístěn v síti VLAN *Internet*. K tomu použijeme útok *sending 802.1Q arp poisoning*. Nejprve ovšem musíme podle návodu z předchozího oddílu vytvořit a vyjednat sdruženou linku. Před započetím útoku bychom měli ověřit, že záznam v tabulce protokolu ARP systému Windows (adresa IP 10.13.58.128) pro adresu IP 10.13.58.253 (router pro Internet) obsahuje skutečnou adresu MAC routeru.

Nyní otevřeme okno protokolu 802.1Q. Uvidíme pravděpodobně pakety směrované na adresu MAC pro všesměrové nebo skupinové vysílání. Tyto pakety se rozesílají na všechny porty sítě VLAN (v našem případě na všechny porty sítě VLAN 200, tedy sítě VLAN *Internet*) a také na všechny porty s vyjednaným sdružováním (například náš port). Všechna pole naplníme výchozími hodnotami a přesuneme se do editačního režimu, abychom mohli změnit hodnotu v poli *Source MAC* na 66:66:66:66:66:66. Nyní se přesuneme do okna s útoky a zvolíme útok *sending 802.1Q arp poisoning*. Tento útok vyžaduje zadání několika parametrů, proto se zobrazí nové okno s následujícími poli:

- *IP to poison*: adresa IP, kterou chceme nahradit, v našem případě tedy: 10.13.58.253 (router pro Internet),
- *IP VLAN*: identifikátor sítě VLAN, na kterou chceme odeslat pakety, v našem případě: 200 (síť VLAN *Internet*),
- *ARP IP Source*: tato adresa IP se použije ke zjištění adresy MAC routeru pro Internet; adresa musí odpovídat stejné síti VLAN jako adresa IP z pole *IP to poison*, ale nesmí být obsazena; použijme např. adresu 10.13.58.66.



Obrázek 11. *Důsledek útoku na protokol 802.1Q*

Nyní můžeme útok spustit. Pokud půjde vše podle plánu, uvidíme v tabulce ARP počítače se systémem Windows (10.13.58.128) adresu MAC 66:66:66:66:66:66 a v okně nástroje Yersinia se zobrazí více informací (viz Obrázek 11).

Pokusme se nyní zjistit, co vlastně nástroj Yersinia provádí:

- Pomocí podvržených paketů protokolu ARP hledá adresu MAC internetového routeru.
- Když útok zjistí adresu MAC routeru pro Internet, spustí se vlákno, které odesílá každou sekundu jeden paket *ARP reply*. Tím se poškodí tabulka ARP systému Windows – nastaví se falešná adresa MAC pro adresu IP 10.13.58.128 (internetový router): 66:66:66:66:66:66.

Nástroj Yersinia tak získá všechna data, která počítač se systémem Win-

Co je to doména protokolu VTP

Doména protokolu VTP je textový řetězec formátu ASCII sdílený všemi switchi, které náleží do stejné skupiny nebo jednoho celku. Tento řetězec se vkládá do všech paketů protokolu VTP. Doménu nalezneme také v některých polích protokolu CDP. Stejný textový řetězec obsahuje dokonce i doména protokolu DTP.

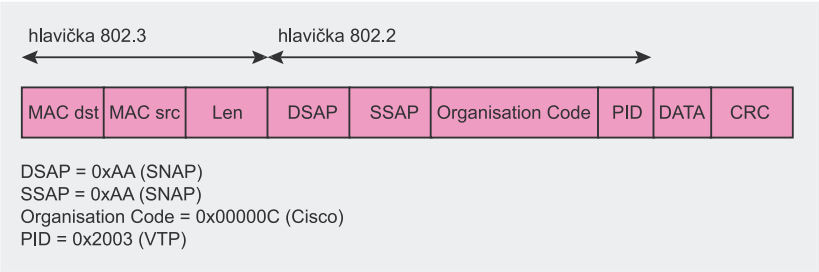
dows (adresa IP 10.13.58.128) odešle na Internet. Yersinia data přepíše a přepošle do zdrojové sítě VLAN (*Internet* VLAN, ID 200), tentokrát ovšem data směřují na správnou adresu MAC routeru pro Internet (adresa IP 10.13.58.253). Pokud bychom chtěli síťová data uložit, stačí stisknout klávesu [*s*]. Data budou uložena ve formátu pcap. Nyní můžeme pouze doufat, že vlastník počítače nepoužívá hesla ve formátu prostého textu.

Protiopatření

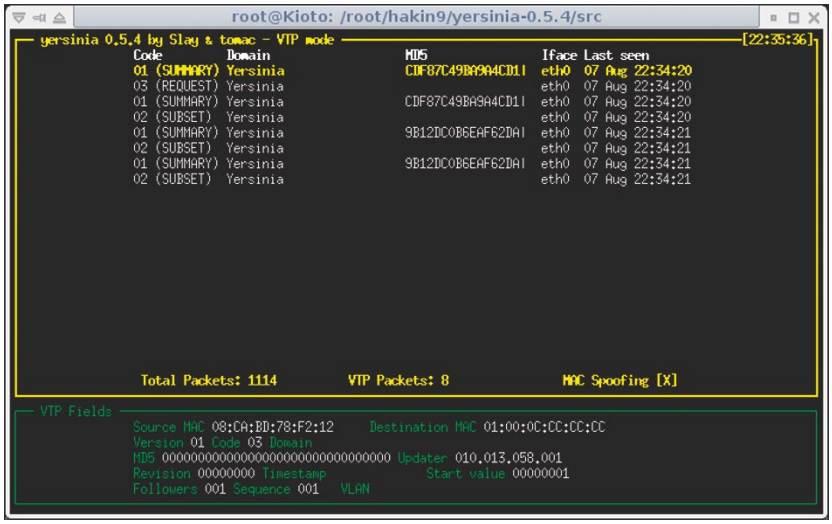
Ochrana proti útokům na protokol IEEE 802.1Q spočívá, stejně jako v případě útoků na protokol DTP, ve vypnutí podpory automatického sdružování portů.

Protokol VTP (VLAN Trunking Protocol)

VTP je patentovaný protokol společnosti Cisco, který slouží pro centralizovanou správu sítí VLAN. Pokud síť nastavujeme pomocí switche, můžeme příslušné informace (název sítě VLAN a identifikátor) nastavit automaticky u všech switchů, které jsou ve stejné doméně (viz sekce *Co je to doména protokolu VTP*).Pakety protokolu VTP obsahují rámec dle protokolu IEEE 802.3 s hlavičkou SNAP podle protokolu 802.2 (viz Obrázek 12) a odesílají se na adresu MAC pro všesměrové vysílání 01:00:0C:CC:CC:CC.



Obrázek 12. *Struktura paketu protokolu VTP*



Obrázek 13. *Důsledky útoku na protokol VTP*

Existují čtyři typy paketů protokolu VTP:

- *Summary advertisement – SUMMARY.* Podobný jako paket *Hello*; odesílá se každých 5 minut,
- *Advertisement request – REQUEST.* Využívá se pro zasílání dotazů,
- *Subset advertisement – SUBSET,* Datový paket s popisy sítě VLAN.
- *Join – JOIN.*

Výpis 12. *Úspěšný útok – odebrání sítě VLAN*

```
zipi# sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/24
                                                Gi0/1, Gi0/2
100  Office                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
```

Útoky

Ačkoliv protokol VTP podporuje použití hesel, standardně není tato podpora zapnuta. Hash MD5 se však uvnitř paketu *SUMMARY* uvádí vždy. Tento haš spočítáme podle nastavení sítě VLAN, hesla (pokud je použito) a dalších polí.

Paket *SUMMARY* se standardně odesílá každých 5 minut. Vezmeme-li v úvahu fakt, že útoky na protokol VTP vyžadují data získaná z těchto paketů, zjistíme, že útok nesmí trvat déle než 5 minut.

Nástroj Yersinia implementuje hned několik útoků na protokol VTP. Zaměřme se na dva nejvýznamnější: přidání (adding) a odebrání (deleting) sítě VLAN. Abychom mohli tyto útoky provést, musíme učinit následující kroky:

- získat data protokolu VTP; nejsnáze tato data získáme přijetím paketu *SUMMARY,*
- odeslat paket *REQUEST,* pomocí kterého získáme seznam sítí VLAN,

- upravit sítě VLAN získané v předchozím kroku,
- pomocí paketů *SUMMARY* a *SUBSET* odeslat nové nastavení sítě VLAN.

Praktické použití

Konfiguraci pro ukázkový útok ponecháme stejnou jako v předchozím oddíle: dvě sítě VLAN: *Office* (ID 100) a *Internet* (ID 200). Útok je zaměřen na odstranění sítě VLAN *Internet* (ID 200). Nástroj Yersinia umístíme na port Fa0/13.

Nyní se přesuneme do okna protokolu VTP, pole naplníme výchozími hodnotami a spustíme útok *deleting one vlan*. Nástroj Yersinia se dotáže na identifikátor odebírané sítě. V našem případě má identifikátor sítě hodnotu 200. Za několik minut se bude hlavní okno nástroje Yersinia podobat oknu na Obrázku 13. Byl-li útok úspěšný, nebude v konzoli switche uvedena síť VLAN 200 (viz Výpis 12).

Důsledky smazání sítě VLAN mohou být různé. Testy ukazují, že všechna zařízení připojená k portu smazané sítě VLAN, budou odpojena. Čtenáři si mohou vyzkoušet následující pokus. Zkuste nastavit počítač, aby opakoval příkaz ping na hostitele v této síti VLAN (například na výchozí bránu). Potom síť VLAN smažte. Zjistíte, že nástroj ping již nepřijímá žádnou odezvu. Když však síť VLAN znovu připojíte (samozřejmě pomocí nástroje Yersinia), začne nástroj ping opět fungovat.

Protiopatření

Podobně jako v předchozích dvou oddílech je opět nejefektivnějším protiopatřením vypnutí podpory automatického sdružování portů. Tentokrát však můžeme k ochraně sítě využít heslo protokolu VTP.

Shrnutí

V tomto článku jsme hovořili pouze o několika protokolech nad druhou vrstvou modelu OSI a o nejběžnějších útocích. Z příkladů jasně vyplývá, že pokud při konfiguraci sítě nevezmeme v úvahu možná rizika, může se druhá vrstva modelu OSI stát terčem závažných útoků. Většina protokolů je zranitelných a pozor bychom si tedy měli dát zvláště při jejich správě a administraci. ●

O autorech

David Barroso se specializuje na odstraňování důsledků útoků a síťovou bezpečnost. V současnosti pracuje ve španělské společnosti S21sec, která se zabývá zabezpečením. David se rovněž hodně angažuje v celosvětovém společenství pro bezpečnost, které píše články, odborná pojednání a vyvíjí nové bezpečnostní nástroje.

Alfredo Andrés již několik let pracuje v bezpečnostní sféře a pro iniciativu Open Source vyvíjí nástroje a záplaty. Také Alfredo pracuje ve společnosti S21sec, kde řídí skupinu pen-testerů.

Oba autoři prezentovali nástroj Yersinia na konferenci BlackHat Europe 2005. Během přednášky o jednom z protokolů testovaných nástrojem Yersinia (uvedeny byly také specifika zařízení společnosti Cisco) prezentovali útoky typu zero-day a odhalili vývoj nástroje Yersinia.

V Síti

- *http://yersinia.sourceforge.net/* – domovská stránka nástroje Yersinia,
- *http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf* – prezentace Seana Converyho o útocích na druhou vrstvu protokolu OSI,

Spanning Tree Protocol

- *http://www.javvin.com/protocolSTP.html* – webová stránka o protokolu STP (*Spanning Tree Protocol*),
- *http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/frames.htm#xtocid61* – formát paketu BPDU,
- *http://www.cisco.com/warp/public/473/146.html* – článek *Understanding Rapid Spanning Tree Protocol (802.1w)*,
- *http://www.cisco.com/warp/public/473/17.html* – článek *Understanding Spanning-Tree Protocol Topology Changes*,
- *http://www.cisco.com/warp/public/473/65.html* – článek věnovaný rozšíření *Spanning Tree Portfast BPDU Guard Enhancement*,
- *http://www.cisco.com/warp/public/473/74.html* – článek věnovaný rozšíření *Spanning Tree Protocol Root Guard Enhancement*.

Cisco Discovery Protocol

- *http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/frames.htm#xtocid12* – formát paketu protokolu CDP,
- *http://www.phenoelit.de/stuff/CiscoCDP.txt* – doporučení týmu Phenoelit ohledně zranitelnosti protokolu CDP systému IOS.

Dynamic Trunking Protocol

- *http://www.netcraftsmen.net/welcher/papers/switchvtp.html* – článek *Switching: Trunks and Dynamic Trunking Protocol (DTP)*.

IEEE 802.1Q

- *http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf* – standard IEEE 802.1Q ve formátu PDF.

VLAN Trunking Protocol

- *http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/frames.htm#xtocid31* – formát rámce protokolu VTP.