



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ

DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

MAC FLOODING ÚTOK

THESIS TITLE

SEMESTRÁLNÍ PROJEKT

TERM PROJECT

AUTOR PRÁCE

AUTHOR

DANIEL OLEARČIN

VEDOUCÍ PRÁCE

SUPERVISOR

PAVEL OČENÁŠEK, Mgr. Ing. Ph.D.

BRNO 2021

Abstrakt

Cielom práce bolo zistiť ako funguje MAC flooding útok, čo sa snažíme docieľiť a ako na to.

Abstract

The aim of the work was to find out how the MAC flooding attack works, what we are trying to achieve and how to do it.

Klíčová slova

MAC flooding útok

Keywords

MAC flooding attack

Citace

OLEARČIN, Daniel. *MAC flooding útok*. Brno, 2021. Semestrální projekt. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Pavel Očenášek, Mgr. Ing. Ph.D.

MAC flooding útok

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....

Daniel Olearčín

2. května 2021

Obsah

1	Úvod	2
1.1	Čo je to MAC flooding útok	2
2	Ochrana	3
2.1	Ako sa vyhnúť MAC flooding útoku	3
2.1.1	Obmedzenie portu	3
2.1.2	Statické priradenie MAC adresy	3
2.1.3	Zakázať zbytočné porty	3
2.1.4	Vyvarovať sa pripojeniam s rôznych zariadení	3
2.1.5	Záver ochrany	3
3	Útok	4
3.1	Ako realizovať MAC flooding útok	4
4	Zhrnutie MAC flooding útoku	6
4.1	Čo sa dá dosiahnuť	6

Kapitola 1

Úvod

1.1 Čo je to MAC flooding útok

MAC flooding je útok, ktorým sa dá manipulovať správanie switcha tak, aby bolo možné odpočúvať prevádzku, ktorá cez neho prechádza.

MAC flooding využíva zraniteľnosť, ktorá vyplýva zo základnej funkcionality switcha. Switch si zaznamenáva do tzv. CAM tabuľky MAC adresy zariadení, ktoré cez neho komunikujú a porty, z ktorých mu dané MAC adresy prichádzajú. Na základe tejto tabuľky sa switch rozhoduje, ktorým portom pošle prevádzku.

Zraniteľnosť spočíva v tom, že veľkosť tejto tabuľky je obmedzená. Akonáhle sa táto tabuľka naplní, nebude si mať kam zapisovať MAC adresy nových zariadení, ktoré sa pokúšajú o komunikáciu.

Následne sa switch začne voči tejto komunikácii správať ako ethernetový HUB, čiže ju začne preposielať na všetky fyzické porty. Útočník môže túto komunikáciu ľahko odchytiť a analyzovať jej obsah napríklad vo Wiresharku. Viac viz [2].

Kapitola 2

Ochrana

2.1 Ako sa vyhnúť MAC flooding útoku

Je dôležité, aby sme vždy podnikli kroky k ochrane nášho vybavenia. Našťastie máme nástroje a funkcie, pomocou ktorých môžeme zabrániť vstupu votrelcov a trpieť útoky, ktoré ohrozujú naše systémy. Ochrany osobných údajov a bezpečnosť sú veľmi dôležité faktory a musia byť vždy v bezpečí. Musíme vedieť, že tieto funkcie nie sú k dispozícii u všetkých sieťových prepínačov, ale sú k dispozícii u tých, ktoré sa všeobecne používajú v spoločnostiach.

2.1.1 Obmedzenie portu

Jednou z týchto charakteristík je obmedzenie počtu MAC adries, ktoré bude schopný zistiť na každom portu. Týmto spôsobom, akonáhle dosiahne maximum, zahodí všetky neznáme. Tým sa zabráni MAC Flooding útok, ktorý sme vysvetlili.

2.1.2 Statické priradenie MAC adresy

Môžeme sa tiež rozhodnúť nakonfigurovať prepínač staticky, priradiť iba MAC adresy. To nám umožňuje spracovávať iba pakety z určitých adries MAC.

2.1.3 Zakázať zbytočné porty

Neexistuje ani lepšia bezpečnostná bariéra ako zakázať tie porty, ktoré nepoužívame. Týmto spôsobom by možný útočník nemohol nájsť spôsob, ako ich zaplaviť a získať tak informácie.

2.1.4 Vyvarovať sa pripojeniam s rôznych zariadení

Ďalšou možnosťou, ktorú musíme zlepšiť zabezpečenie a vyhnúť sa tak problémom s nasýtením MAC adries, zabrániť mu v prijímaní nových pripojení z iných zariadení.

2.1.5 Záver ochrany

Nakoniec, ako vidíme, útoky MAC Flooding môžu poškodiť zabezpečenia našich sieťových prepínačov. Je dôležité, aby sme vždy podnikli kroky, aby sme zabránili problémom, ktoré nakoniec ovplyvní celú sieť. Videli sme niekoľko základných tipov, ktoré môžeme vziať do úvahy, aby sme zabránili útokom. Viac viz [1]

Kapitola 3

Útok

3.1 Ako realizovať MAC flooding útok

Na zahájenie útoku MAC flooding použijeme nástroj MACOF, ktorý je súčasťou balíčku DSNIFF. Jeho súčasťou je napríklad aj nástroj ARPSPOOF, ktorý sa používa pri útoku ARP spoofing. Použijeme útočnú stanicu s operačným systémom KALI Linux.

```
root@kali: ~  
File Edit View Search Terminal Help  
15:b2:dc:2a:5f:b2 92:88:3a:63:96:4f 0.0.0.0.14567 > 0.0.0.0.39256: S 541533609:541533609(0) win 512  
65:fd:12:6b:93:78 fb:14:19:b:33:ce 0.0.0.0.37890 > 0.0.0.0.17570: S 1615806498:1615806498(0) win 512  
36:b2:b1:5e:bd:b6 3e:9e:12:1f:ce:e6 0.0.0.0.31782 > 0.0.0.0.12994: S 1971351904:1971351904(0) win 512  
ca:25:3b:24:d2:43 36:fb:91:54:d1:b5 0.0.0.0.32557 > 0.0.0.0.19536: S 1561499938:1561499938(0) win 512  
f2:e9:b9:5c:ad:de 51:c8:60:75:c0:46 0.0.0.0.44269 > 0.0.0.0.16613: S 936470859:936470859(0) win 512  
f3:b9:22:3d:4:32 28:b8:74:53:67:b4 0.0.0.0.46481 > 0.0.0.0.5370: S 1960686563:1960686563(0) win 512  
cc:6c:95:45:c5:f2 63:3b:e2:24:29:82 0.0.0.0.57093 > 0.0.0.0.10182: S 1012171689:1012171689(0) win 512  
c8:9:1c:63:a9:66 81:a:68:29:96:2a 0.0.0.0.34576 > 0.0.0.0.55895: S 1813656981:1813656981(0) win 512  
29:d8:8c:4f:c6:18 31:c1:ff:18:d2:ab 0.0.0.0.41426 > 0.0.0.0.703: S 1596500182:1596500182(0) win 512  
35:6:fc:18:60:3a a3:de:b6:5e:76:7f 0.0.0.0.62244 > 0.0.0.0.39824: S 1895242944:1895242944(0) win 512  
74:cc:57:24:9b:7a 9:8e:c3:b:5:24 0.0.0.0.34176 > 0.0.0.0.44098: S 78912729:78912729(0) win 512  
b8:da:b7:79:44:49 46:5a:af:65:a0:ae 0.0.0.0.41381 > 0.0.0.0.5865: S 2140704841:2140704841(0) win 512  
5c:d3:28:e:13:af 85:0:80:63:d7:1e 0.0.0.0.33992 > 0.0.0.0.41390: S 1702549157:1702549157(0) win 512  
49:05:88:7f:ec:ac f4:5b:27:31:9e:6e 0.0.0.0.13780 > 0.0.0.0.55073: S 1425181086:1425181086(0) win 512  
f5:19:5d:64:0:b3 c0:2f:e0:70:47:be 0.0.0.0.10307 > 0.0.0.0.33607: S 824933243:824933243(0) win 512  
2e:2d:bd:7f:23:8e 5:3d:5b:4d:f0:90 0.0.0.0.45439 > 0.0.0.0.12738: S 815901176:815901176(0) win 512  
ed:e4:55:75:6b:af 9d:25:f0:74:5e:d1 0.0.0.0.940 > 0.0.0.0.21471: S 1953320676:1953320676(0) win 512  
34:3b:d:70:a3:c1 6c:ed:d0:27:e7:cb 0.0.0.0.24996 > 0.0.0.0.19286: S 1244540920:1244540920(0) win 512  
d8:99:cb:c:11:a7 5a:e2:13:3a:4:31 0.0.0.0.27119 > 0.0.0.0.27010: S 2121858226:2121858226(0) win 512  
3a:b9:e8:1d:6d:bf 34:15:c1:5e:af:f1 0.0.0.0.56799 > 0.0.0.0.5241: S 1839200319:1839200319(0) win 512  
10:7f:a5:77:20:91 41:36:93:2c:f3:8b 0.0.0.0.33490 > 0.0.0.0.48811: S 661587623:661587623(0) win 512  
f3:49:4:3:b9:d4 47:e7:c2:3c:65:69 0.0.0.0.13006 > 0.0.0.0.28589: S 481732825:481732825(0) win 512  
4a:f9:ec:3a:b2:9c cf:57:97:15:2c:28 0.0.0.0.14892 > 0.0.0.0.60482: S 1314997323:1314997323(0) win 512  
d7:8c:9e:0:62:9 f8:31:33:7f:47:f0 0.0.0.0.21255 > 0.0.0.0.38951: S 1175480207:1175480207(0) win 512  
22:14:fe:0:d7:19 93:7d:43:58:2b:39 0.0.0.0.38199 > 0.0.0.0.13834: S 1929074759:1929074759(0) win 512  
bd:18:46:4b:79:7f 78:78:2:7f:6a:d1 0.0.0.0.53149 > 0.0.0.0.57810: S 2035185874:2035185874(0) win 512  
db:64:2:1d:94:7f 84:c6:27:25:9:b3 0.0.0.0.49468 > 0.0.0.0.49890: S 415989854:415989854(0) win 512  
43:7c:bd:47:4a:ae c4:be:26:69:d7:19 0.0.0.0.62827 > 0.0.0.0.31917: S 416860257:416860257(0) win 512  
db:13:9a:43:3e:45 9e:98:89:27:ef:ce 0.0.0.0.21709 > 0.0.0.0.26182: S 1788632836:1788632836(0) win 512  
b3:13:dd:34:7d:cb 31:c4:50:2:3c:34 0.0.0.0.13630 > 0.0.0.0.16325: S 1293954080:1293954080(0) win 512  
e9:af:f7:1d:40:bd 74:e5:3c:17:d4:75 0.0.0.0.41220 > 0.0.0.0.52356: S 1845523157:1845523157(0) win 512  
e:d8:25:35:4a:b8 2:d4:79:73:5b:cd 0.0.0.0.46377 > 0.0.0.0.23559: S 238171704:238171704(0) win 512  
41:17:b4:b:fa:8c 3e:8c:a:3e:76:e9 0.0.0.0.40916 > 0.0.0.0.63892: S 1606199512:1606199512(0) win 512  
ba:45:33:7f:76:d0 e8:3c:6e:19:90:41 0.0.0.0.42424 > 0.0.0.0.27983: S 164720675:164720675(0) win 512  
d5:e4:b7:a:28:87 3:9a:d6:24:a:37 0.0.0.0.5422 > 0.0.0.0.35246: S 475792832:475792832(0) win 512  
96:ea:e1:1d:12:45 aa:5e:e9:7:c0:d2 0.0.0.0.39825 > 0.0.0.0.52830: S 649820037:649820037(0) win 512  
5e:f5:15:72:1d:e3 60:5f:3c:1b:ca:3d 0.0.0.0.27450 > 0.0.0.0.51815: S 460593346:460593346(0) win 512  
1e:9c:d8:34:c4:23 bd:c9:99:22:d1:8f 0.0.0.0.21990 > 0.0.0.0.61435: S 632726738:632726738(0) win 512  
b5:a9:df:1f:1:d3 eb:5:29:37:29:30 0.0.0.0.55283 > 0.0.0.0.49491: S 1522753337:1522753337(0) win 512  
a2:6a:d8:7a:70:a1 e2:bf:70:19:16:e0 0.0.0.0.9983 > 0.0.0.0.51828: S 393097467:393097467(0) win 512  
d2:19:d1:15:61:19 2d:7:cc:77:fa:1b 0.0.0.0.56533 > 0.0.0.0.65303: S 1999590036:1999590036(0) win 512  
4e:cf:cb:27:58:13 65:9a:fa:5f:2f:34 0.0.0.0.8141 > 0.0.0.0.39797: S 1557136550:1557136550(0) win 512  
09:92:2b:7f:f0:c0 6a:87:cf:73:fc:6a 0.0.0.0.26878 > 0.0.0.0.19975: S 2119935630:2119935630(0) win 512  
b3:33:09:75:8c:d4 b1:f8:17:52:36:a8 0.0.0.0.509 > 0.0.0.0.19805: S 281076306:281076306(0) win 512
```

Ako vidíme, zaplnili sme celú CAM tabuľku a switch si už nemá kam zapisovať nové vstupy.

```
SW1-NETVEL#show mac address-table count

Mac Entries for Vlan 1:
-----
Dynamic Address Count   : 8190
Static Address Count    : 0
Total Mac Addresses     : 8190

Total Mac Address Space Available: 0
```

Keď si pozrieme tabuľku s MAC adresami, môžeme vidieť množstvo podhodnotených vstupov, ktoré prišli z portu fa0/1 od našej útočnej stanice.

```
SW1-NETVEL#show mac address-table
Mac Address Table
-----
Vlan      Mac Address      Type      Ports
-----
All       0014.6986.9400    STATIC    CPU
All       0100.0ccc.cccc    STATIC    CPU
All       0100.0ccc.cccd    STATIC    CPU
All       0100.0cdd.dddd    STATIC    CPU
1         0009.625d.b633    DYNAMIC    Fa0/1
1         000a.c611.c949    DYNAMIC    Fa0/1
1         0012.f943.04b8    DYNAMIC    Fa0/1
1         0027.e040.387d    DYNAMIC    Fa0/1
1         0033.4534.bec9    DYNAMIC    Fa0/1
1         0036.8d66.9928    DYNAMIC    Fa0/1
1         0037.6f3c.ecec    DYNAMIC    Fa0/1
1         003d.7b3b.c2c6    DYNAMIC    Fa0/1
1         003e.3c5a.8095    DYNAMIC    Fa0/1
1         0040.4833.29e5    DYNAMIC    Fa0/1
1         0058.c805.558f    DYNAMIC    Fa0/1
1         005a.3e18.7b80    DYNAMIC    Fa0/1
1         005b.5b12.3c04    DYNAMIC    Fa0/1
1         005c.e478.6c36    DYNAMIC    Fa0/1
1         005e.1d36.c3bd    DYNAMIC    Fa0/1
--More--
```


Kapitola 4

Zhrnutie MAC flooding útoku

4.1 Čo sa dá dosiahnuť

Pri MAC flooding útoku dochádza k zaplneniu switcha a následne môže dôjsť k odpočúvaniu komunikácie útočníkom. V prítomnej dobe už sa to nestáva často pretože switche ktoré sa kupujú už majú zabudovanú obranu proti takýmto typom útokov. Veľmi veľa som pochopil o tomto útoku v tomto videu takže odporúčam tým ktorých to zaujíma pozrieť.

https://www.youtube.com/watch?v=54kfAXpQtWo&ab_channel=ProfessorMesser

Literatura

- [1] Co je MAC Flooding Attack a co dělat, aby se tomu zabránilo. [online], [upravené: 2020-09-20]. Dostupné z: <https://itigic.com/cs/mac-flooding-attack-and-what-to-do-to-prevent-it/>
- [2] MAC FLOODING A PORT SECURITY – ÚTOK NA SWITCH A AKO SA BRÁNIŤ. [online], [upravené: 2018-03-19]. Dostupné z: <https://netvel.sk/mac-flooding-attack-port-security/>