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 — **DANIEL OLEARČIN**
AUTHOR

VEDOUCÍ PRÁCE — **PAVEL OČENÁŠEK, Mgr. Ing. Ph.D.**
SUPERVISOR

BRNO 2021

Abstrakt

Cieľom práce bolo zistiť ako funguje MAC flooding útok, čo sa snažíme docieliť 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 Olearčin

2. května 2021

Obsah

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 prichádzjú. 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

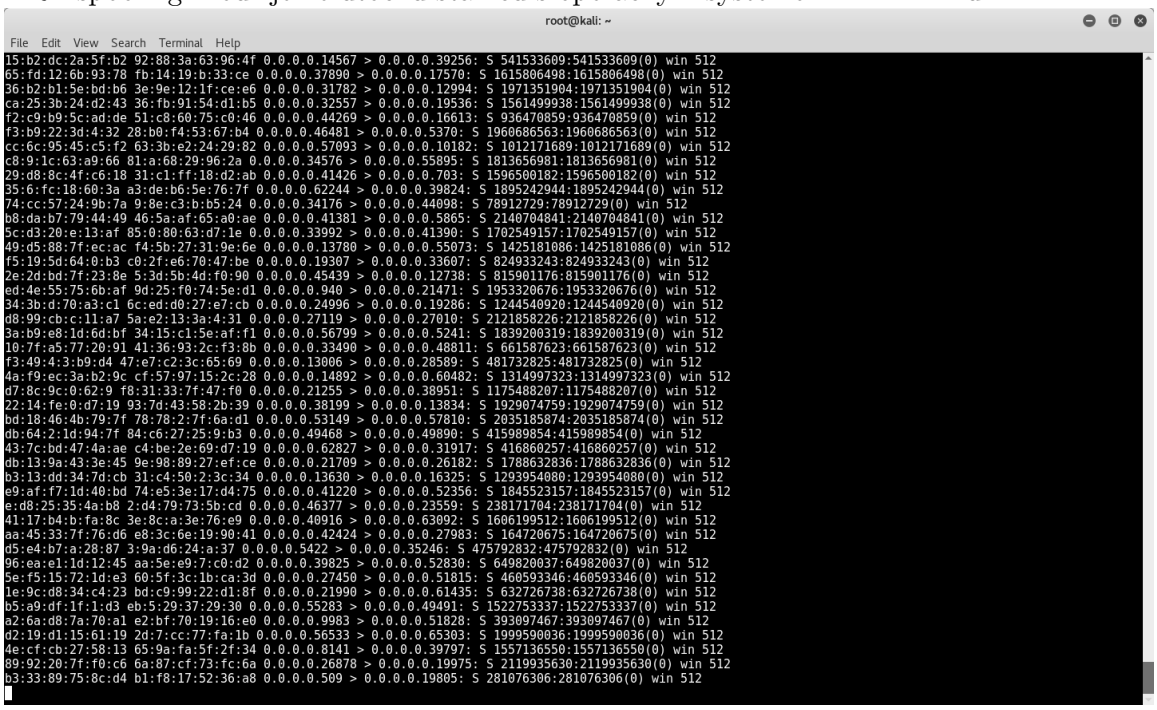
Nakoniec, ako vidíme, útoky MAC Flooding môžu poškodiť zabezpečenia našich sieťových prepínačov. Je dôležité, aby sme vždy podnikli kroky, aby sme zabránili problémom, ktoré nakoniec ovplyvní celú sieť. Videli sme niekoľko základných tipov, ktoré môžeme vziať do úvahy, aby sme zabránili útokom. Viac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



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 podhodených 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 maju 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/