Heimdall IDS

Heimdall IDS je IDS provozující detekci a mitigaci záplavových útoků v sítích LAN.

Heimadall IDS využívá knihovnu paramiko (https://github.com/paramiko/paramiko). Licence pro tuto knihovnu lze nalézt v adresáři licences. Instalace knihovny paramiko je možná z příkazové řádky příkazem: `pip3 install paramiko`. V případě problému s pip je potřeba zadat příkaz: `sudo apt install python3-pip` a zopakovat předchozí příkaz.

Program byl vytvořen v rámci bakalářské práce o detekci a mitigaci záplavových útoků.

Funkce Heimdall IDS:

- Detekce záplavových útoků (4 metody)
- ARP Scan
- Učící modul
- Připojení přes SSH do Mikrotik směrovače

Požadavky a použití

Směrovač by měl zrcadlit veškerý provoz na rozhraní s IDS. Příklad nastavení Mikrotik směrovače (rozhraní ether3 a ether4 bude kopírováno na ether2):

```
/interface ethernet switch
set switch1 mirror-source=none mirror-target=ether2
/interface ethernet switch rule
add mirror=yes ports=ether3,ether4 switch=switch1
```

Systém s IDS by měl mít nastavené své připojené rozhraní jako promiskuitní. V OS Linux toho lze dosáhnout příkazem:

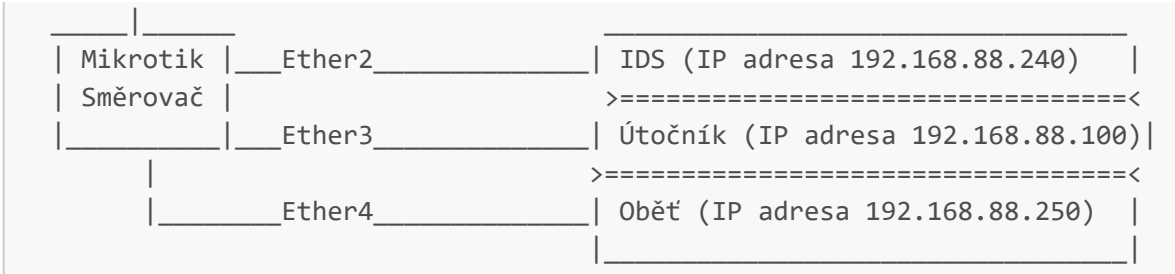
```
sudo ip link set eth0 promisc on
```

Samotný program je spouštěn z příkazové řádky ve formátu:

```
sudo python3 main.py ARGUMENTS
```

- IDS byl testován na této topologii:

```
  Internet
     |
     | Ether1           Síť 192.168.88.0/24
```



Detekční modul

- Povolením tohoto modulu je umožněna detekce záplavových DDoS útoků. Pokud nastane útok, je vypsán log do konzole a současně je uložen do souboru heimdall_logs.log

Metody

- Heimdall disponuje 4 metodami detekce:

1. SYN Flood metoda

- Metoda rozhoduje o vyhlášení poplachu na základě poměru mezi SYN a ACK TCP segmenty
- Při běžné komunikaci jsou SYN zprávy využity jen při úvodním 3-Way-Handshake. ACK zprávy jsou využity taktéž při tomto ustanovení spojení, ale na rozdíl od SYN zpráv jsou použity i při potvrzování příchozích zpráv.
- Pokud bude množství SYN zpráv větší než ACK zpráv, je velká pravděpodobnost, že se jedná o útok.
- Pravidlo pro rozhodování tedy zní, že pokud je poměr SYN/ACK větší než daný limit je vyhlášen poplach

2. UDP Flood metoda

- Metoda sleduje množství UDP zpráv za časový interval
- Pokud je množství větší než limit, je vyhlášen poplach

3. ICMP Flood metoda

- Metoda sleduje množství ICMP zpráv za časový interval
- Pokud je množství větší než limit, je vyhlášen útok

4. Komplexní metoda

- Metoda je založena na principu, že komunikace probíhá po vlnách
- Komplexní metoda sleduje množství všech paketů za časový interval
- Hodnoty množství jsou ukádány do seznamu a je zkoumáno, kolik z nich překračuje hodnotu tzv. Danger Zone
- Pokud je v seznamu více než polovina hodnot v Danger Zone, je vyhlášen poplach

```
|
|      _ _
|‚‚‚ _| ‚| ‚| ‚‚‚‚‚‚‚‚‚‚‚‚‚‚‚‚ Hranice Danger Zone
|   | | | |_
|  _| | | | |_     _
|_| | | | | | |_ _| |_
|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_> Čas


Záplavový útok

Množství paketů
^
|
|    _ _ _ _ _ _ _ _
|‚‚‚| ‚| ‚| ‚| ‚| ‚| ‚| ‚| ‚| ‚‚‚‚‚‚ Hranice Danger Zone
|   | | | | | | | | | |
|  _| | | | | | | | | |
|_| | | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_> Čas
```

Struktura detekčního logu

- Informace o útocích jsou, jak už bylo zmíněno, ukládány v podobě logu do souboru a vypsány do konzole
- Struktura logu je následující:

1. Část udává informaci o času detekce útoku
2. Část udává informaci o typu útoku
3. Část udává informaci o hodnotě parametru, podle něhož byl útok detekován
4. Část udává IP adresu útočníka
5. Část udává MAC adresu útočníka

- Za útočníka je určen uživatel, který vyprodukoval nejvíce škodlivých zpráv
- Příklad logu:

```
Mon Mar 22 14:57:38 2021; UDP Flood; 9; 00:50:56:C0:00:08; 192.168.133.1
```

Nastavení

Povolení metod

```
# Enable SYN Method
-d syn
# Enable UDP Method
-d udp
```

```
# Enable ICMP Method
-d icmp
# Enable Complex Method
-d complex
# Enable several Methods
-d syn,udp,icmp
# Enable all Methods
-d all
```

Časovače

- Časovače udávají hodnotu intervalů detekce [sekundy]

```
-t syn-5
# change several timers for methods
-t syn-5,udp-11
```

Rules

- Pravidla udávají limity počtu zpráv pro jednotlivé metody [pakety/host]

```
# change rule for one method
-r syn-2
# change rules for several methods
-r syn-2,complex-100
```

Minimální parametry pro umožnění běhu detekčního modulu

- Detekční modul může provádět svou činnost jen v případě, že je mu znám počet hostů v síti
- Tuto informaci může získat z předaného argumentu nebo od modulu ARP Scan
- Počet hostů je udáván bez započítání IDS a Mikrotik směrovače

Příklad nastavení

```
# first example
sudo main.py -d all -r syn-0.3,udp-100 -t complex-5 --number_of_hosts 5
#second  example
sudo python3 main.py -d syn,udp -s 192.168.1.0/24
```

ARP Scan

- Modul k mapování sítě využívající ARP dotazy
- Pokud host na ARP dotaz odpoví, je v IDS označen jako UP, pokud ne je DOWN

- Pokud známý host neodpoví, neznamená to, že je ihned z tabulky hostů IDS odstraněn. Je odstraněn až vyprší limit, během kterého může odpovět na ARP žádost.
- Při současném běhu s detekčním modulem umožňuje IDS měnit dynamicky pravidla podle počtů hostů v síti
- Scan lze využít i bez současného běhu ostatních modulů
- Informace o hostech jsou prezentovány v pravidelných intervalech v konzoli a v případě objevení nového hosta je uložen log do souboru s logy

Log modulu ARP Scan

- Log udává informace o nověh hostu v síti
- Struktura logu:

1. Část udává informaci o času objevení hosta
2. Část udává informaci o tom, že se jedná o log modulu ARP Scan
3. Část udává informaci o rozhraní Mikrotik směrovače, ke kterému je host připojen
4. Část udává MAC adresu nového hosta
5. Část udává IP adresu nového hosta

- Příklad logu:

```
Mon Mar 22 14:57:38 2021; New Host; ether3; 00:50:56:C0:00:08; 192.168.133.135
```

Povolení modulu ARP Scan

```
#format -s NETWORK/MASK
# in solo mode
sudo python3 main.py -s 192.168.133.0/24
# together with Detection Module
sudo python3 main.py -d syn,udp -s 192.168.1.0/24
```

Učící modul

- Modul je určený pro ulehčení nastavování pravidel detekčního modulu
- Učící modul v daném čase sleduje provoz sítě a na jeho základě stanoví hodnoty pravidel pro jednotlivé detekční metody
- Modul může být pouze povolen v případě současného využití s detekčním modulem

Povolení Učícího modulu

```
# format is -l TIME_FOR_LEARNING_IN SECONDS
sudo python3 main.py -d all -l 120
```

SSH modul

- Modul slouží pro komunikaci mezi IDS a Mikrotik směrovačem
- Je zde využita knihovna paramiko
- Při běhu s detekčním modulem umožňuje shození portu útočníka v případě detekce útoku
- Při běhu s modulem ARP Scan poskytuje IDS informace o rozhraních, ke kterým jsou hosti připojeni
- Modul je možné povolit jen v případě současného běhu s detekčním modulem nebo modulem ARP Scan

Povodelní SSH modulu

```
# format is -c IP,USERNAME -i SAFE_INTERFACE1,SAFE_INTERFACE2,...
sudo python3 main.py -d all -l 120 -c 192.168.1.1,admin -i ether0
```

Testované nastavení

```
sudo python -d all -r syn-0.8,udp-10418,icmp-16,complex-1903 -c 192.168.88.1,admin
-s 192.168.88.0/24
```

Testované útoky

```
# SYN Flood Attack
hping3 -S --flood  192.168.88.250
# UDP Flood Attack
hping3 --flood  --udp 192.168.88.250
# ICMP Flood Attack
hping3 --flood -1 192.168.88.250
# PUSH and ACK Flood Attack
hping3 --flood -PA 192.168.88.250
```