Ochrona danych i systemów
Milestone 3 + live demo

Temat 1: Aktywny Firewall

Skład zespołu:

- Alicja Uzar
- Daniel Mynarski
- Dominik Wróbel

Plan prezentacji

1. Podsumowanie prac
2. Omówienie algorytmu uwzględniającego czas i priorytet ataku
    2.1. Tabela priorytetów ataków
3. Omówienie zestawu testów
    3.1. TCP Port Scanning
    3.2. UDP Port Scanning
    3.3. ICMP Flood
    3.4. LAND Attack
    3.5. UDP Flood
    3.6. Ping of Death
4. Omówienie teoretyczne live demo - studium przypadku
5. Live demo

Podsumowanie prac

Milestone 1

- Architektura
- Plan, harmonogram, narzędzia

01 IV 2020

Milestone 3

- Algorytm blokowania uwzględniający czas / priorytet
- Zestaw testów
- Dokumentacja

24 V 2020

11 III 2020
Start projektu

22 IV 2020

Milestone 2

- Snort, skrypty, iptables
- Przeprowadzenie ataku z obroną

27 V 2020
Zakończenie projektu

Omówienie algorytmu uwzględniającego czas i priorytet

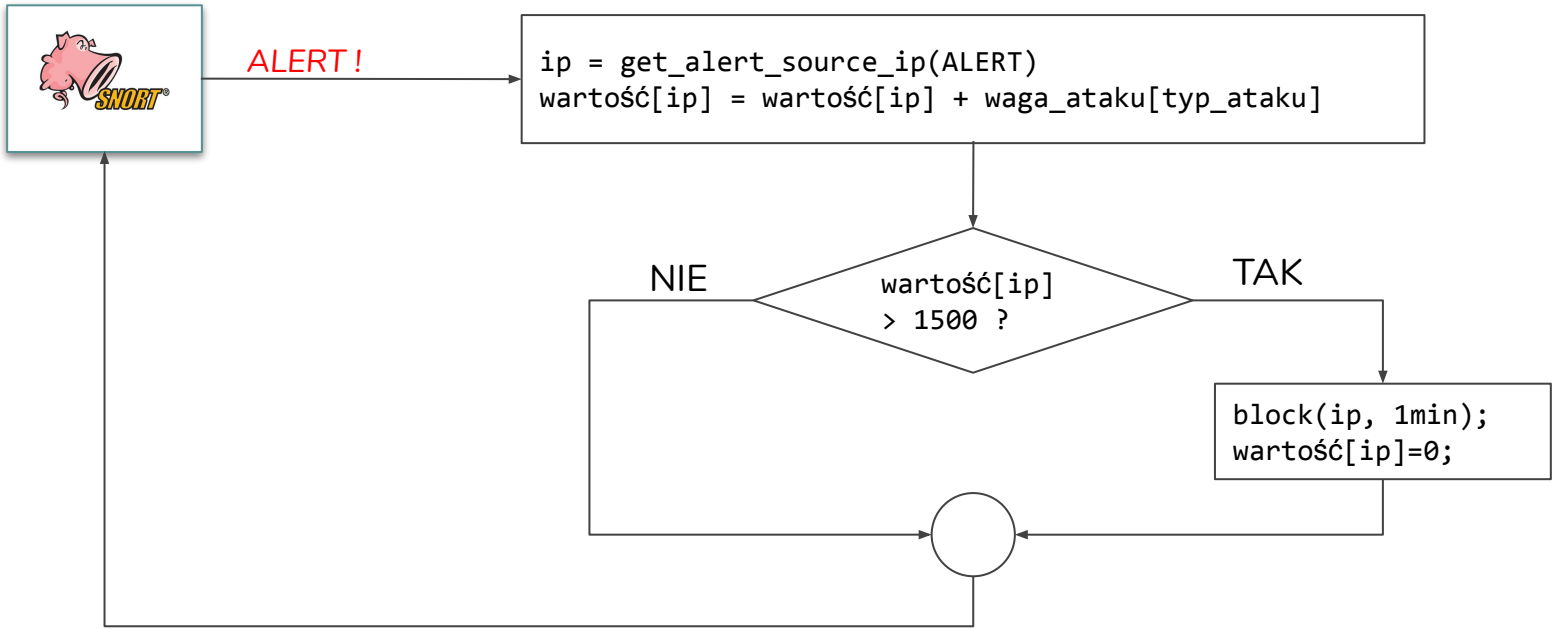


Tabela priorytetów ataków TODO

Kategoria ataku	Atak / Alert	Priorytet	Wartość liczbowa
PORT SCANNING	TCP Port Scanning	LOW	30
	UDP Port Scanning	LOW	30
	....	...	...
DoS WARNING - DoS POSSIBLE	ICMP Flood Alert Possible	MEDIUM	750
	...	...	...
DoS DETECTED	ICMP Flood	HIGH	1500
	Ping of Death	HIGH	1500
	...	...	...

Test 1.1 - TCP Port Scanning

- Opis: Atak polegający na sprawdzeniu dostępnych portów i działających serwisów w protokole TCP na atakowanym hoście.

VirtualBox Kali Linux
10.0.2.4/24

nmap -sT 10.0.2.15

Snort + VirtualBox
Ubuntu
10.0.2.15/24

```
alert tcp any any -> 10.0.2.15 any (msg:"TCP PORT SCAN ALERT"; detection_filter:track
by_src, count 990, seconds 1; sid:1000003; rev:1;)
```

Test 1.2 - UDP Port Scanning

- Opis: Atak polegający na sprawdzeniu dostępnych portów i działających serwisów w protokole UDP na atakowanym hoście.

VirtualBox Kali Linux
10.0.2.4/24

*nmap -sU -v -p *
7,19,37,53,67,68,69,137,138,161,162,514,520,
33434 10.0.2.15

Snort + VirtualBox
Ubuntu
10.0.2.15/24

```
alert udp any any -> 10.0.2.15 any (msg:"UDP PORT SCAN ALERT"; detection_filter:track
by_src, count 20, seconds 1; sid:1000004; rev:1;)
```

Test 2.1 - ICMP Flood

- Opis: Atak polegający na wysłaniu do systemu ofiary ogromnej liczby pakietów ICMP. System ofiary będzie zmuszony odpowiadać wieloma pakietami ICMP, stając się w końcu nieosiągalnym dla innych klientów

hping3 -1 -V -c 1000 --flood 10.0.2.15

VirtualBox Kali Linux
10.0.2.4/24

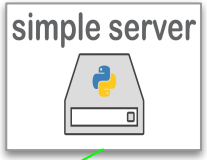
Snort + VirtualBox Ubuntu
10.0.2.15/24

```
alert icmp any any -> 10.0.2.15 any (msg:"ICMP FLOOD ALERT"; detection_filter:track
by_dst, count 500, seconds 1; sid:1000007; rev:1;)
```

Test 2.2 - LAND Attack

- Opis: Atak polegający na wysłaniu na otwarty port hosta złośliwego pakietu. Pakiet zawiera adres docelowy i adres do odpowiedzi ustawiony na ten sam adres, który jest adresem hosta-ofiary. W efekcie host odpowiada w nieskończoność sam do siebie.

hping3 -V -c 1 -d 100 -S -p 80 -s 80 -k -a 10.0.2.15 10.0.2.15



VirtualBox Kali Linux
10.0.2.4/24

Snort + VirtualBox Ubuntu
10.0.2.15/24 + server
localhost:8080

```
pip install simple_http_server # przed uruchomieniem SNORT
sudo python -m SimpleHTTPServer 80
```

```
alert tcp any any -> 10.0.2.15 80 (msg:"LAND ATTACK ALERT"; sameip; flags:S; sid:
1000005; rev:1;)
```

Test 2.3 - UDP Flood

- Opis: Atak polegający na wysłaniu na otwarty port UDP ogromnej liczby pakietów. System ofiary będzie zmuszony odpowiadać wieloma pakietami ICMP, stając się w końcu nieosiągalnym dla innych klientów.

hping3 -2 -V -c 100 -d 100 -S -p 21 --flood 10.0.2.15

VirtualBox Kali Linux
10.0.2.4/24

Snort + VirtualBox Ubuntu
10.0.2.15/24

```
alert udp any any -> 10.0.2.15 21 (msg:"UDP FLOOD ALERT"; detection_filter:track by_dst,
count 75, seconds 1; sid:1000006; rev:1;)
```

Test 2.4 - Ping of Death

- Opis: Atak na system polegający na wysłaniu zapytania ping (*ICMP Echo Request*) w pakiecie o rozmiarze większym niż 65 535 bajtów. Może to spowodować awarię atakowanego systemu lub zawieszenie działającej na nim aplikacji.

hping3 -i u10000 -1 -d 51000 -c 4 10.0.2.15

VirtualBox Kali Linux
10.0.2.4/24

Snort + VirtualBox Ubuntu
10.0.2.15/24

```
alert icmp any any -> 10.0.2.15 any (msg:"PING OF DEATH ALERT"; dsize:>50000; itype: 8;
icode:0; detection_filter:track by_src, count 1, seconds 1; sid:1000008; rev:1;)
```

Omówienie live demo - studium przypadku

VirtualBox
Kali Linux
10.0.2.4/24

sudo nmap -sT 10.0.2.15

TCP PORT SCAN ALERT: x10

10.0.2.4/24: 0 + 10*30 = 300

Test connection: ping 10.0.2.15

sudo nmap -sU -v -p \
7,19,37,53,67,68,69,137,138,161,162,514,520,33434 10.0.2.15

UDP PORT SCAN ALERT: x14

10.0.2.4/24: 300 + 14*30 = 720

Test connection: ping 10.0.2.15

sudo hping3 -i u100 -1 -c 101 10.0.2.15

ICMP FLOOD POSSIBLE: x1

10.0.2.4/24: 720 + 750 = 1470

Test connection: ping 10.0.2.15

sudo hping3 -i u100 -1 -c 101 10.0.2.15

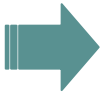
ICMP FLOOD POSSIBLE: x1

10.0.2.4/24: 1470 + 750 >= 1500
BLOCK IP !

Test connection: ping 10.0.2.15

Snort +
VirtualBox
Ubuntu
10.0.2.15/24

Dziękujemy za uwagę



Live demo