Instrukcja 2

Symulacja ataków odmowy usługi (DoS/DDoS)

Słowa kluczowe
Hping3, DoS, DDoS, Analiza ruchu, Wireshark

Literatura
1. **Daniel Graham**, *Etyczny hacking. Praktyczne wprowadzenie do hackingu*

Potrzebne narzędzia
- system operacyjny **Microsoft Windows 10 / Microsoft Windows 11**
- system **Kali Linux**
- **Wireshark**
- środowisko wirtualizacji (VM), np. Oracle VM VirtualBox lub VMware Workstation.

I. Narzędzie hping3

Narzędzie sieciowe `hping3` umożliwiające wysyłanie niestandardowych pakietów TCP/IP oraz analizę odpowiedzi systemu docelowego, podobnie jak w przypadku programu ping, który wykorzystuje komunikaty ICMP.

Program obsługuje m.in. fragmentację pakietów, dowolną zawartość i rozmiar pakietów, a także umożliwia przesyłanie danych przy użyciu obsługiwanych protokołów.

Za pomocą `hping3` można wykonać między innymi:

- testowanie reguł zapory sieciowej (firewalla),
- zaawansowane skanowanie portów,
- testowanie wydajności sieci przy użyciu różnych protokołów oraz rozmiarów pakietów,
- wykrywanie ścieżki MTU,
- zdalne pobieranie odcisku palca systemu operacyjnego (fingerprinting),
- audyt stosu TCP/IP,
- analizę oraz symulację różnych typów ataków sieciowych.

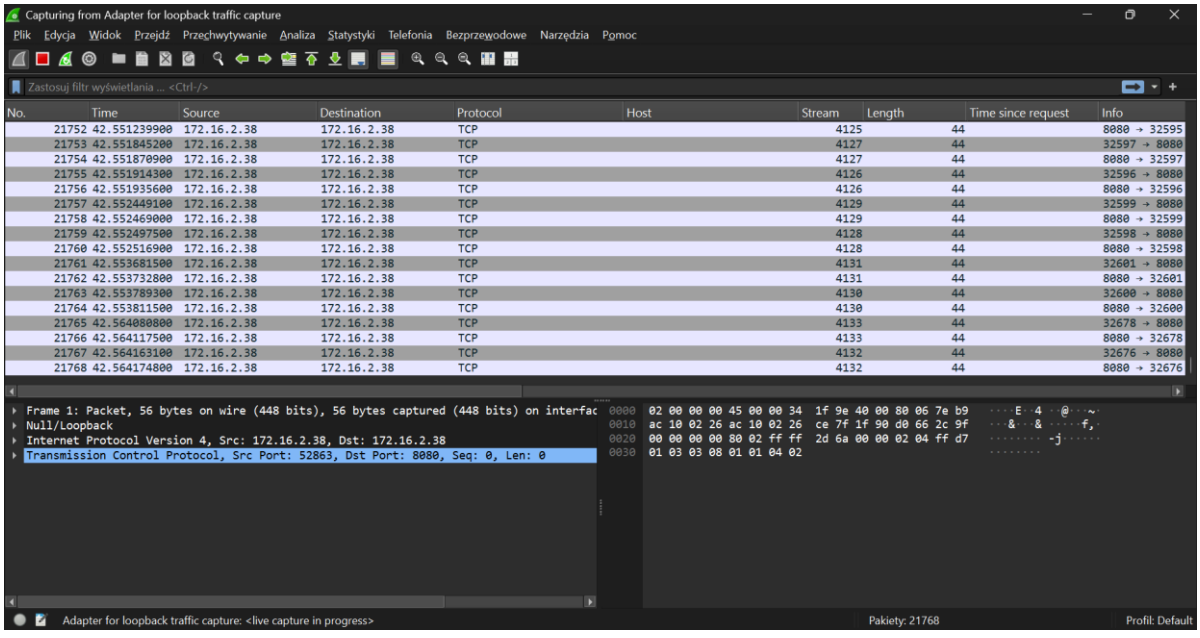
1. W systemie Windows upewnij się, że program Wireshark nasłuchuje na odpowiednim interfejsie sieciowym.

2. W systemie Kali Linux uruchom atak `SYN Flood`:

```
sudo hping3 -e 'Twój_Nr_Indeksu' -d 120 -S -w 64 -p 8080 --flood --rand-source IP_OFIARY
```

- `-e '[tekst]'`: Dodaje własny podpis (signature) do pakietu.
- `-d 120`: Rozmiar danych w pakiecie (120 bajtów).
- `-S`: Ustawienie flagi SYN.
- `-w 64`: Rozmiar okna TCP.
- `-p 8080`: Port docelowy (serwer HTTP).
- `--flood`: Wysyłanie pakietów z maksymalną prędkością (brak czekania na odpowiedzi).
- `--rand-source`: Generowanie losowych adresów źródłowych (ukrywa atakującego).

3. Wróć do programu Wireshark.



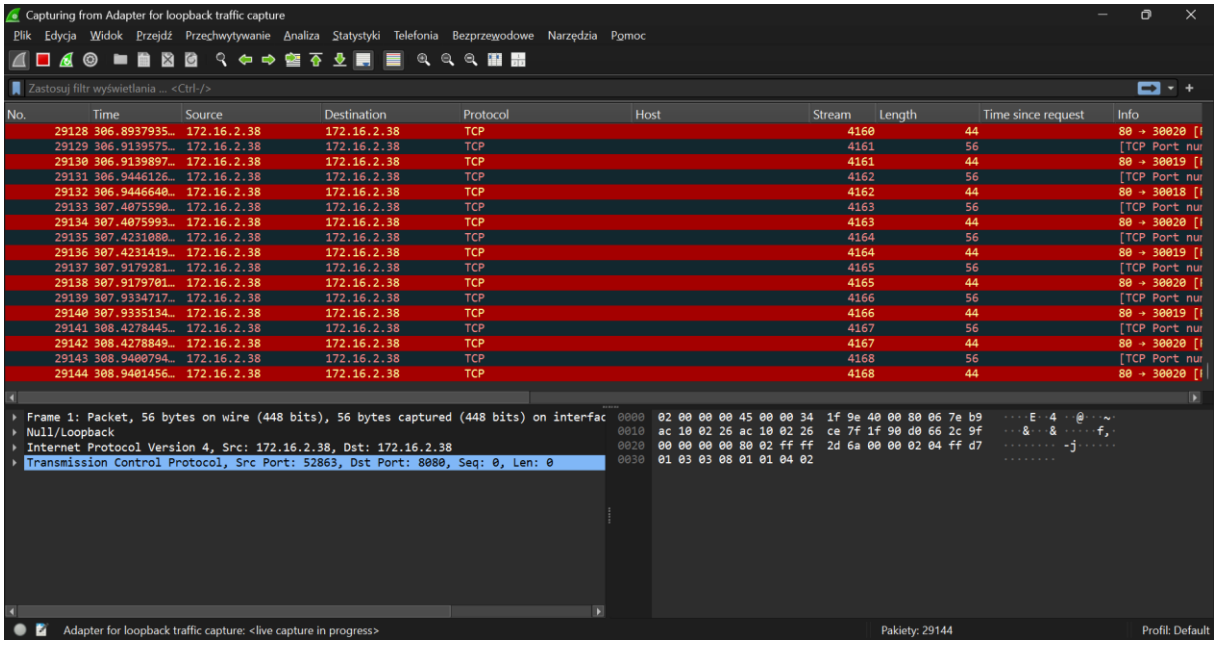
Powinieneś zauważyć skutki ataku w postaci znacznego wzrostu ruchu sieciowego, który może powodować zwiększone obciążenie systemu Windows. W niektórych przypadkach komputer może zacząć pracować głośniej z powodu zwiększonego wykorzystania zasobów.

4. Wróć do terminala w Kali Linux i zatrzymaj atak, używając kombinacji klawiszy `Ctrl + C`

5. W systemie Kali Linux uruchom polecenie:

```
sudo hping3 -S -p 80 IP_OFIARY -a IP_OFIARY
```

6. Wróć do programu Wireshark.



W tym przypadku pakiet jest wysyłany do maszyny docelowej z identycznym adresem źródłowym i docelowym, co jest charakterystyczne dla ataku typu LAND Attack.

7. Wróć do terminala i zatrzymaj działanie programu kombinacją klawiszy: `Ctrl + C`