WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

KURS WSTĘPNY: ATAKI W SIECIACH KOMPUTEROWYCH

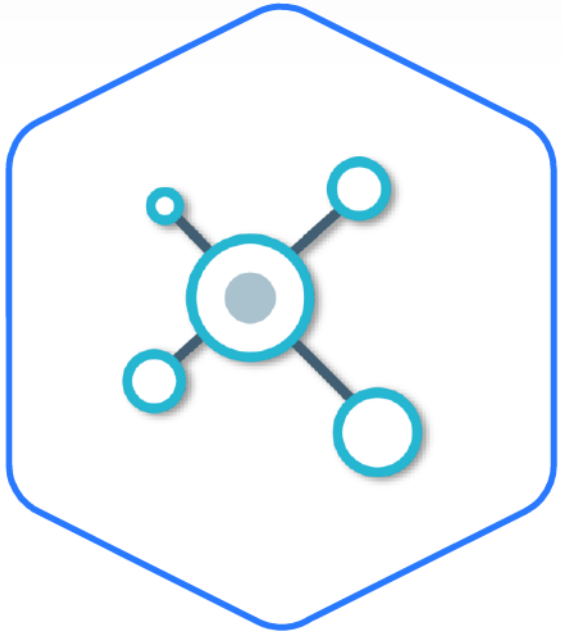
ZARYS WYKŁADU

Dowiesz się o prostocie ataków sieciowych, możliwościach manipulowania urządzeniami i infrastrukturą sieciową oraz ich uszkadzania.
Zapoznasz się z rodzajami i narzędziami ataków sieciowych.

- Warunki i koncepcje ataków sieciowych
- Ataki typu „Na ścieżce” (On-Path)
- Ataki typu DoS/DDoS
- Ataki na sieci bezprzewodowe

WARUNKI I KONCEPCJE ATAKÓW SIECIOWYCH

PRZEGLĄD ATAKÓW SIECIOWYCH



- Manipulowanie infrastrukturą sieciową lub jej uszkodzenie.
- Przechwytywanie poufnych informacji (On-Path)
- Odmowa usługi (Denial of Service - DoS)

CELE ATAKÓW SIECIOWYCH

Servers

Security Devices

Networking Equipment

Endpoint Devices

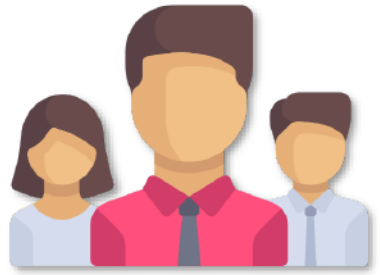
TYPOWE ATAKI SIECIOWE

Niektóre z dobrze znanych typów ataków sieciowych, które można przeprowadzić na różne usługi

Sniffing	Aktywne lub pasywne przechwytywanie ruchu sieciowego
IP Spoofing	Podszywanie się pod inny adres IP
MAC Spoofing	Podszywanie się pod inny adres MAC
DNS Poisoning	Manipulowanie informacjami w rekordach DNS
Name Resolution Poisoning	Pozyskiwanie poświadczeń użytkowników za pośrednictwem sfałszowanych domen sieciowych

ATAKI TYPU „NA ŚCIEŻCE” (ON-PATH)

PRZEGLĄD ATAKÓW ON-PATH



- Wykonywane w celu podglądania ruchu sieciowego
- Można wdrażać aktywnie lub pasywnie
- Istnieją dedykowane narzędzia i metody On-Path
- Przekierowuje ruch atakowanej maszyny
  do maszyny kontrolowanej przez atakującego

ATAKI ON-PATH

Powódź MAC
Przełącznik wysyła wszystkie odebrane pakiety do wszystkich urządzeń w sieci.

Zatruwanie ARP i zatruwanie DNS
Podszywanie się pod urządzenie końcowe lub router w celu podsłuchiwania ruchu sieciowego.

ARP

Polecenie służy do przeglądania odwzorowania adresów IP/MAC

Używane do uzasadnionych celów (rozwiązywania problemów)

Może pomóc w identyfikacji ataków On-Path

Command Prompt

```
C:\>arp -a

Interface: 192.168.50.4 --- 0x7
  Internet Address      Physical Address      Type
  192.168.50.1          28-80-88-36-d6-68     dynamic
  192.168.50.2          88-51-fb-25-67-d3     dynamic
  192.168.50.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ĆWICZENIE

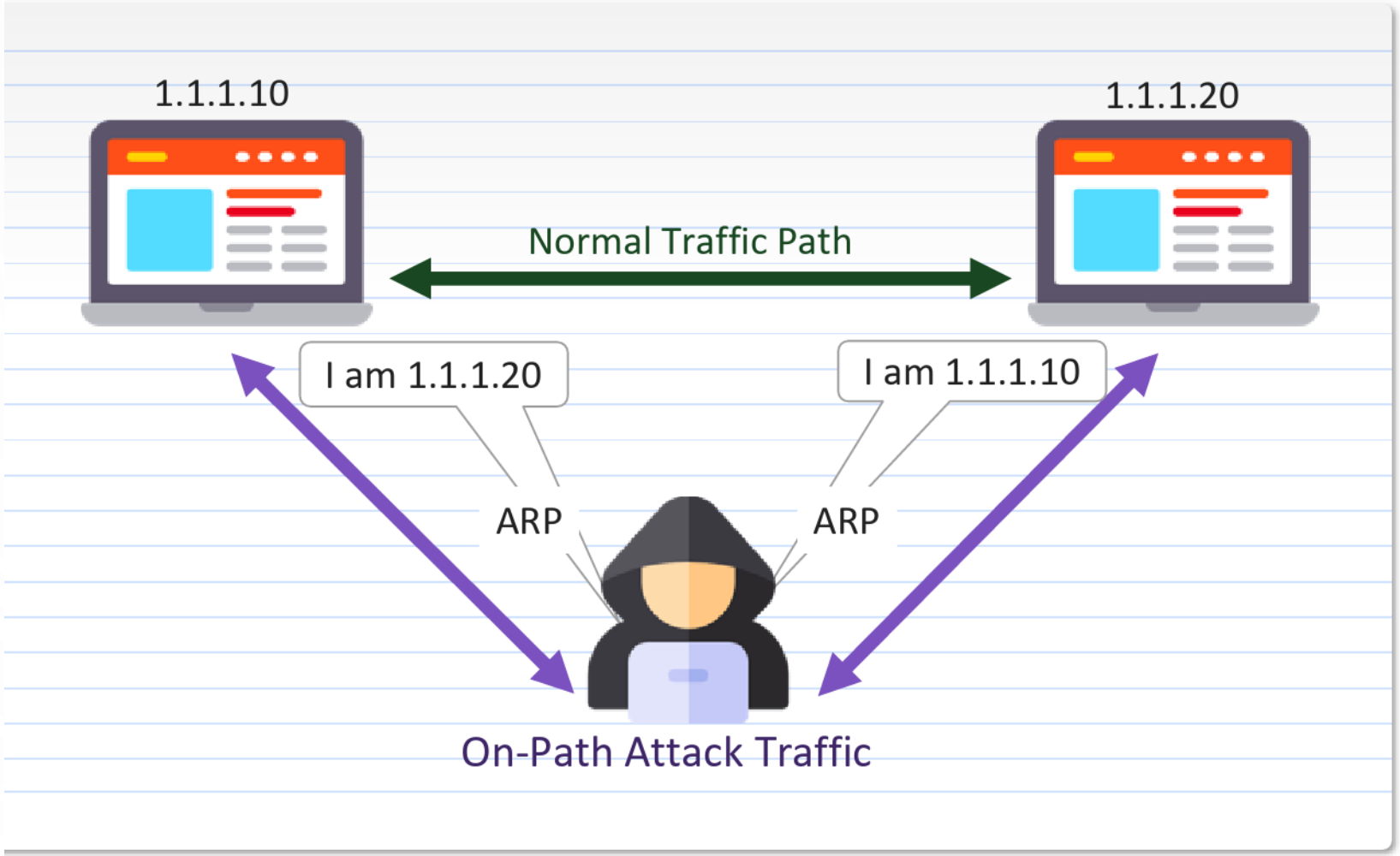
Spójrz na tabelę ARP na komputerze i zidentyfikuj router.

- Otwórz Wiersz poleceń (cmd) na swoim komputerze.
- Uruchom komendę **arp –a**
- Czego można się dowiedzieć z wyników?
- Jaki jest ostatni adres?

ON-PATH WITH ARP POISONING

Łączenie się z siecią i manipulowanie ruchem poprzez wysyłanie pakietów ARP i udawanie innego urządzenia.

Może służyć do podszywania się pod komputery lub routery.

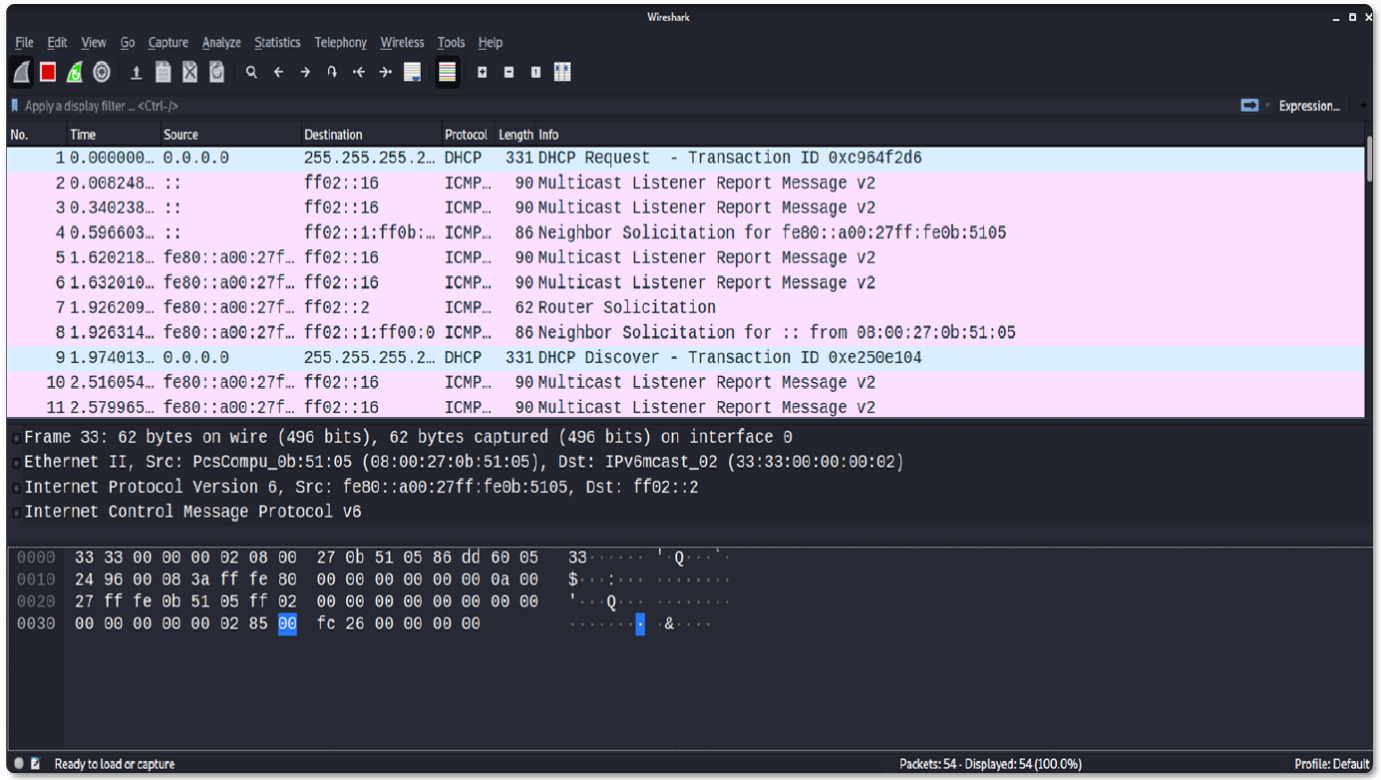


WIRESHARK

Bezpłatne narzędzie do analizy ruchu w sieciach komputerowych

Stworzony do legalnego monitorowania sieci

Używany do złośliwego podglądania danych przesyłanych w sieciach



DOS/DDOS

ATAKI TYPU ODMOWA USŁUGI (DENIAL OF SERVICE)

Odmowa usługi (DoS)
Atak powodujący awarię usługi poprzez wykorzystanie podatnej na ataki funkcji

Rozproszona odmowa usługi (DDoS)
Atak DoS, który jest rozdzielany pomiędzy wiele źródeł w celu wygenerowania większego ruchu

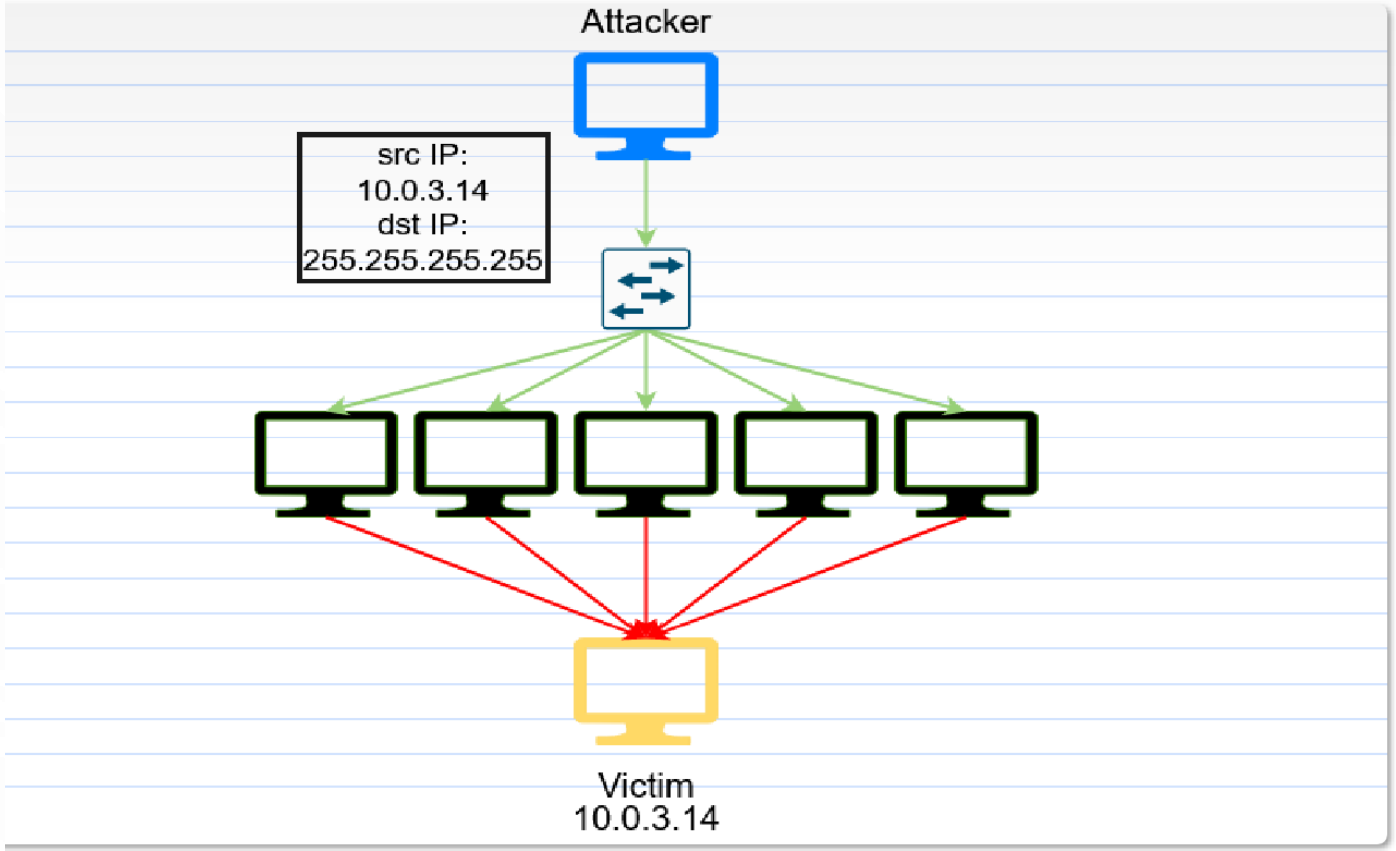
Atak DDoS to atak DoS na większą skalę

ATAK TYPU SMURF

Atak DDoS wykorzystujący protokół ICMP

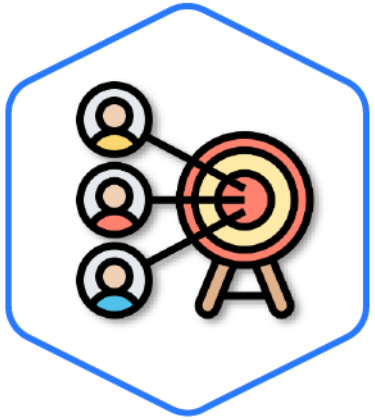
Sfałszowany adres IP jest używany
jako źródło rozgłaszania polecenia ping

Komputery odpowiadają na adres źródłowy



KATEGORIE ATAKÓW DDOS

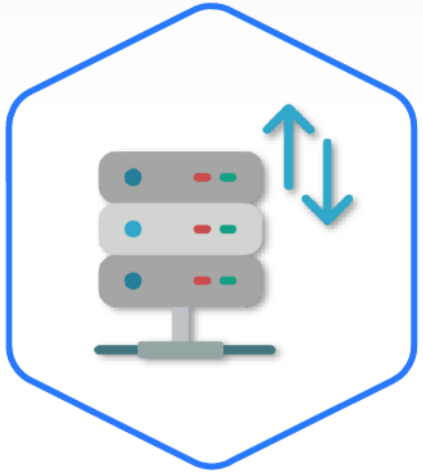
Aplikacyjny DoS
Atak powodujący awarię usługi poprzez wykorzystanie podatnej na ataki funkcji



Wolumetryczny DDoS
Atak wykorzystujący ogromne ilości ruchu w celu wyłączenia usług

Wolumetryczny wskazuje, że atak obejmuje duży ruch

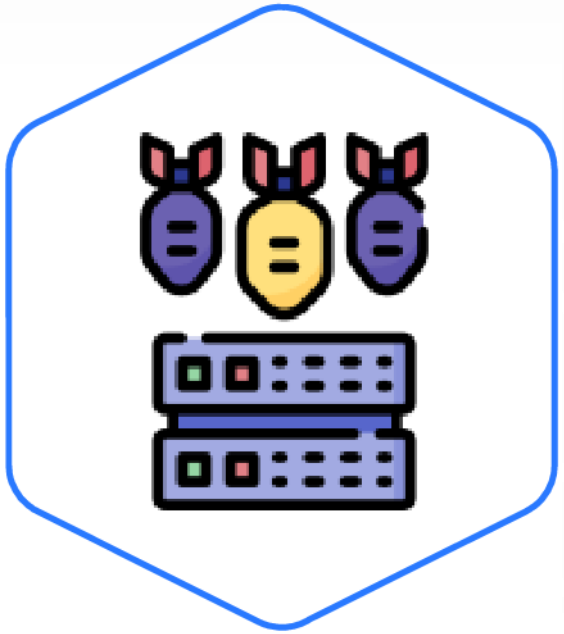
ATAKI DOS NA POZIOMIE APLIKACYJNYM



Zasoby serwera
Każdy serwer zużywa część swoich zasobów
na wykonanie instrukcji. Zasoby nie są nieograniczone

Zalanie zasobów aplikacji
Korzysta z funkcji takich jak zapomniane hasła, loginy
i tworzenie kont użytkowników

WOLUMETRYCZNY ATAK DOS



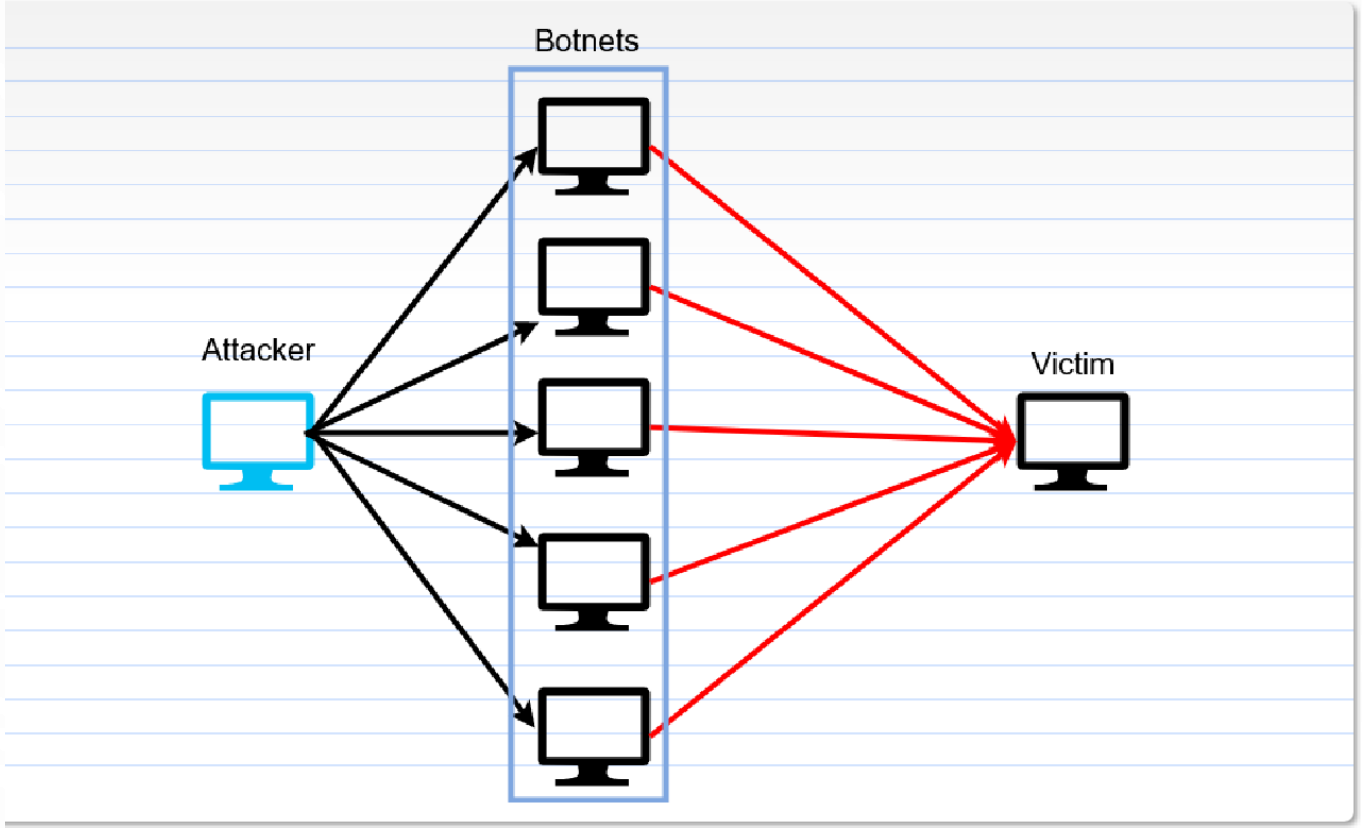
- Skierowany na protokoły komunikacyjne
- Zalewanie serwerów żądaniami
- Zużywanie zasobów sieciowych

BOTNETY

Sieć zdalnie sterowanych komputerów

Komputery są infekowane złośliwym kodem
i reagują na polecenia atakującego

Botnety można wykorzystywać
do ataków DDoS
przeprowadzanych z komputera centralnego



DDOS JAKO USŁUGA

- Prosta metoda ataku DDoS
- Wykonywana za pośrednictwem usług online (za opłatą)
- Używana zarówno do celów testowych, jak i złośliwych
- Obejmuje usługi legalne i nielegalne

LOW ORBIT ION CANNON (LOIC)

Łatwe w użyciu
narzędzie DoS (do pobrania)

Do działania wymaga jedynie
adresu IP lub adresu URL

Istnieje również wersja online

OPERACJA „PAYBACK”

Członkowie grupy haktywistów „Anonymous” w roku 2010 użyli LOIC do przeprowadzenia masowego ataku DDoS podczas operacji Payback

HPING3

Narzędzie linuksowe przeznaczone do testowania bezpieczeństwa sieci

Zapewnia możliwość zalewania celu pakietami ICMP

Posiada możliwości generowania pakietów sieciowych

```
root@kali:~# hping3 -h
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
```

ŁAGODZENIE SKUTKÓW ATAKÓW DOS/DDOS

Identyfikacja
Masowe ruch sieciowy należy najpierw zidentyfikować jako atak DDoS, a nie naturalne zjawisko w sieci

Odpowiedź
Po zidentyfikowaniu, adresy IP i porty mogą zostać zablokowane, a pakiety zostaną odrzucone

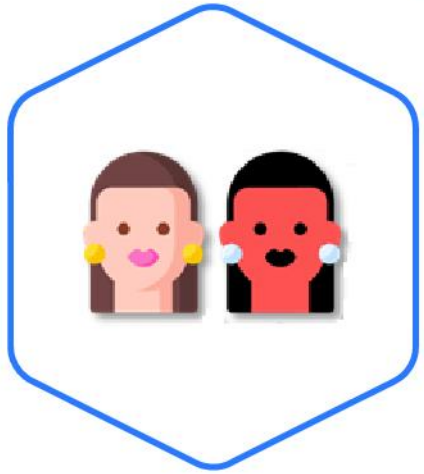
ATAKI NA SIECI BEZPRZEWODOWE

PRZEGLĄD MOŻLIWOŚCI

- Popularne rozwiązanie sieciowe (Wi-Fi)
- Do użytku publicznego, organizacyjnego i domowego
- Umożliwia badanie całego ruchu sieciowego
- Wykorzystuje „możliwe do wykorzystania” protokoły i funkcje

TYPY ATAKÓW NA SIECI BEZPRZEWODOWE

„Nieuczciwy” punkt dostępowy
Nieautoryzowane punkty dostępu są konfigurowane tak, aby użytkownicy nie zauważyli, że mogą mieć problemy z bezpieczeństwem i luki w zabezpieczeniach



Atak „bliźniaczy”
Podszywanie się pod punkt dostępowy, namawianie użytkowników do łączenia się z nim i potencjalna kradzież danych

ZABEZPIECZENIA SIECI BEZPRZEWODOWYCH

WEP
Protokół bezpieczeństwa stworzony
w celu zapewnienia sieciom bezprzewodowym warstwy bezpieczeństwa

WPA
Ulepszony protokół bezpieczeństwa
zaprojektowany jako kolejny poziom WEP

WPA2
Zmodyfikowana wersja WPA z wbudowanym CCMP i AES

WI-FI PROTECTED SETUP (WPS)

- Standard bezpieczeństwa wprowadzony w 2006 roku
- Umożliwia łatwą konfigurację domowej sieci bezprzewodowej
- Można używać kodu PIN z ośmioma cyframi
- Można go złamać przy użyciu metody brute-force

DZIĘKUJĘ ZA UWAGĘ!

MACIEJ.RYBCZYNSKI@UJK.EDU.PL