# Ataki typu DoS

- Wstęp,
- Metody ataków,
- Zapobieganie i zwalczanie,
- Ataki DoS, a prawo polskie,

Andrzej Talarek
a@puchaczy.waw.pl

# Wstęp

Atak **DoS**, czyli **D**enial **o**f **S**ervice:

- „*atak na system komputerowy, bądź usługę w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów*”

- Zasoby fizyczne (CPU, RAM, DYSK),
- Zasoby sieciowe (pasmo),
- Zakłócenie konfiguracji (routing, DNS),

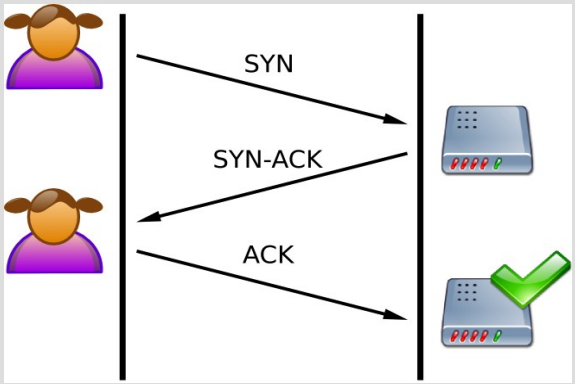
# Wstęp

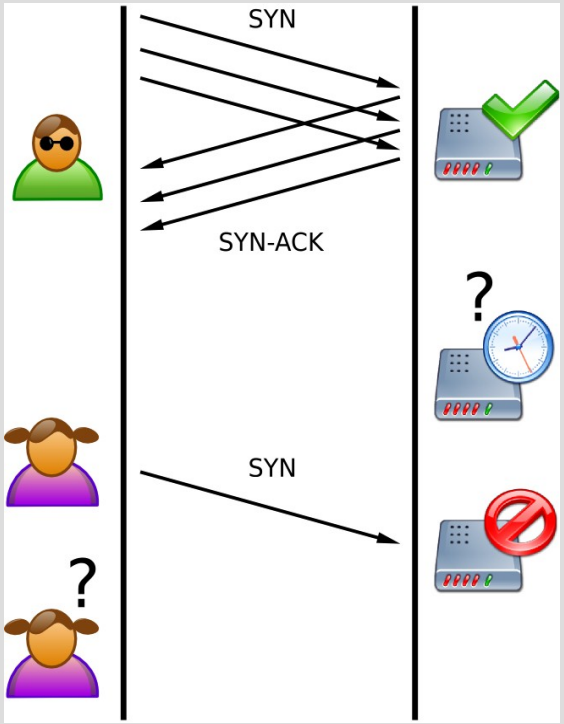
Objawy:

- Mała wydolność pracy,
- Niedostępność wybranych zasobów,
- Niedostępność żadnych zasobów,
- Wzrost (ogromny) ilości fałszywych wiadomości pocztowych,

# Metody ataków

- SYN-FLOOD
  connlimit, syn cookies
- LAND ATTACK
  ip:port=ip:port
- ICMP FLOOD
  smurf, ping
- UDP FLOOD
  dns, sql slummer, chargen
- TEARDROP
  fragmentowanie pakietów



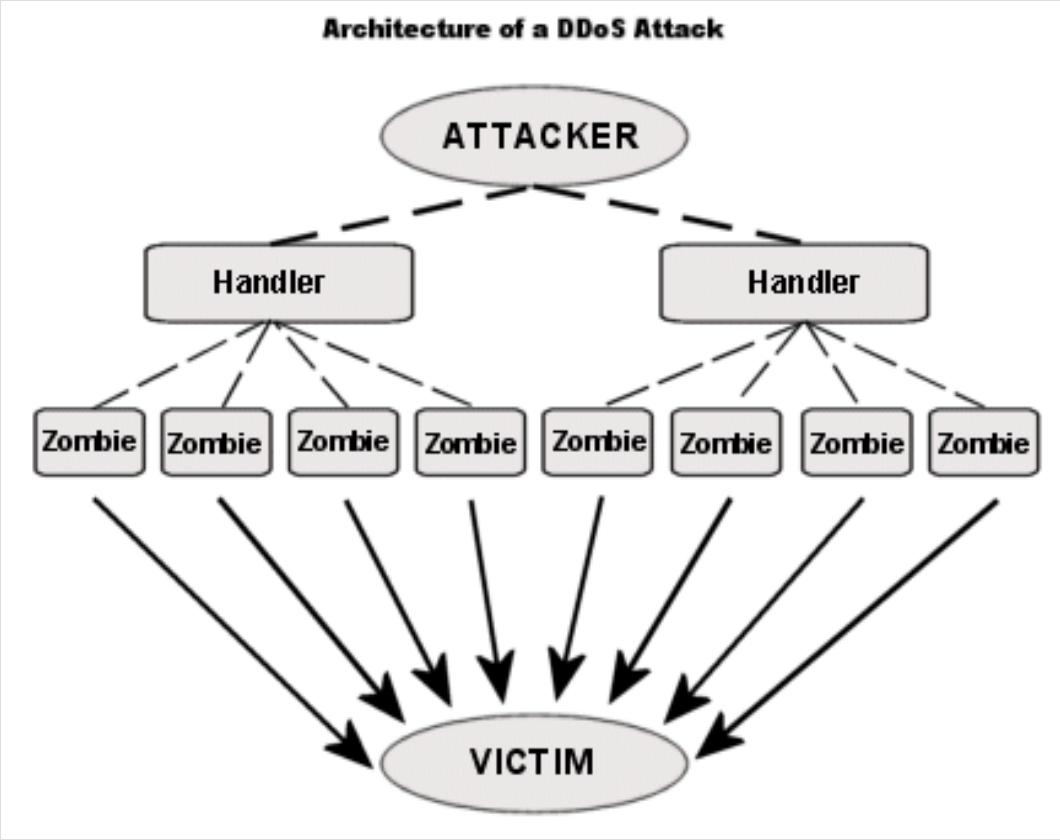



# Metody ataków

- APPLICATION LEVEL FLOOD
  buffer overflow, log/memory overflow, irc
- NUKES
  winnuke-netbios,
- SQL INJECTION
  wielokrotne złączenia, agregacje, xp_cmdshell

# Metody ataków

- Distributed DoS
  ataki zwrotne, ataki niezawinione



# Zapobieganie i zwalczanie

- Przeżycie ataku
  wyśledzenie źródła,
  poinformowanie ISP,
  zmiana IP,
  blokada określonego ruchu,
  zwiększenie krytycznych zasobów,
  odłączenie usług,
- Firewalle
  zwłaszcza stanowe
- Switche, routery
  spoofing, delayed binding, bandwidth managers

# Ataki DoS, a prawo polskie

- art. 49 Konstytucji RP "*Zapewnia się wolność i tajemnice komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.*"
- *„Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*
  *§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.*
  *§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
  *§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.*”

# Ataki DoS, a prawo polskie

- Chroniona jest tylko „*istotna*" informacja.
- Zgodnie z art. 115 § 7 k. k. w zw. z § 5 znaczną szkodę majątkową stanowi szkoda przekraczająca dwustukrotną wartość najniższego miesięcznego wynagrodzenia.
- Przestępstwo z art. 268 § 2 k. k. jest przestępstwem umyślnym. Nie będzie zatem podlegał karze użytkownik który np. w wyniku awarii programu lub sprzętu przypadkowo dokonał ataku DOS na inny host.
- Ponadto atak typu DOS łączy się z odpowiedzialnością cywilną sprawcy.