Politechnika Warszawska

WYDZIAŁ ELEKTRONIKI
I TECHNIK INFORMACYJNYCH

Instytut Telekomunikacji

Praca dyplomowa magisterska

na kierunku Telekomunikacja
w specjalności Telekomunikacja

Ataki odmowy usługi oraz sposoby im przeciwdziałania w sieciach operatorskich

Mikołaj Kowalski
Numer albumu 230346

promotor
dr hab. inż. Wojciech Mazurczyk

Warszawa, 2017 r.

0.1 git last changes

docs
doc
deps
wdowy i bekarty
glo

Streszczenie

Polskie streszczenie pracy...

Dalsza część streszczenia...

I coś jeszcze

Słowa kluczowe: polskie, słowa, kluczowe, pracy

Denial of Service in telecommunication networks – attacks and mitigation

English abstract...

Something more...

And something else...

Keywords: english, keywords

Oswiadczenie o autorstwie pracy z USOS

Spis treści

Rozdział 1

Wstęp: znaczenie niezawodnej infrastruktury sieciowej

Wstęp do pracy.

1.1 Zastosowanie testów sieci i urządzeń sieciowych

1.1.1 Dlaczego warto testować infrastrukturę

Sprawdzenie możliwości architektury
Symulacja ataków (pentesty)
Poznanie realnej wydajności infrastruktury

1.1.2 Dlaczego warto testować urządzenia sieciowe

Zgodność ze specyfikacją
Szukanie podatności w urządzeniach
Rola testów przy zakupach (nowych inwestycjach) - spełnienie wymagań projektowych

1.2 Wprowadzenie do wysokiej dostępności (ang. HA) i równoważenia obciążenia (ang. LB)

(ten rozdział jest
nieważ praca dot
również testowan
chitektury, w test
przewidziany jest
zob. schematy lal

Co to jest High-Availbility (HA) i dlaczego to robimy, Single Point of Failure

Cel uzyskania niezawodnej i optymalnie wykorzystanej architektury

Test Frame per Second (FPS)

1.2.1 Algorytmy Load-Balancing

1.2.2 Znaczenie session-persistence

1.2.3 Przykłady

Alteon VADC asd

HAProxy asd

Keepalived + pacemaker asd

Rozdział 2

Przegląd generatorów ruchu sieciowego

2.1 Generatory sprzętowe

charakterystyka, przykłady

- Spirent
- Ixia

2.2 Generatory programowe w Linuksie

2.2.1 Metody generowania wielkowolumenowego ruchu

Opis procesu generowania pojedynczego pakietu w Linuksie
Po co robić memory zero-copy
Szybkie vs wolne backendy: SOCKET_RAW, libpcap, netmap, PF_RING, AF_PACKET

2.2.2 Funkcjonalności różnych generatorów/frameworków

Badanie: netsniff-ng, scapy, PKTGEN)

2.2.3 Wyspecjalizowane generatory

JMeter

2.2.4 Fuzzery

Na tą chwilę brak wiedzy/doświadczenia z tego typu programami

2.3 Generatory – analiza komparatywna

(tabelka zalety-wady)

Funkcjonalność vs Wydajność vs Cena

Metoda	Funkcjonalność	Wydajność	Cena
A	15	15	1
B	10	15	2
C	12	13	3
D	110	230	4

2.4 Metody analizy ruchu sieciowego

klasyfikacja

2.4.1 Metody opierające się na (kopii) ruchu

Urządzenie in-line

Kopia ruchu (port-mirroring)

Backendy: netmap, PF_RING, pcap

Metody statystyczne

Flowy: sFlow, NetFlow

SNMP/Netconf

2.4.2 Analiza komparatywna (tabelka)

Algorytm	Czas symulacji [sek]	
	implementacji X	implementacji Y
A	15	15
B	10	15
C	12	13
D	110	230

Rozdział 3

Wprowadzenie do ataków odmowy usługi i istniejące sposoby przeciwdziałania

rodziale ma się
także przegląd
ury naukowej
nej z DDoS i
i na tym tle po-
e o czym będzie
raca

3.1 Motywy/powody ataków

3.1.1 Straty wizerunkowe, odpływ klientów, okupy, kasa dla botmasterów

3.2 Możliwe skutki ataków

3.2.1 Kilka przykładów historycznych medialnych ataków

3.3 Charakterystyka ataków za rok 2016 w sieci OPL

4.3.1. Średnie natężenie
4.3.2. Szczytowy ruch
4.3.3. Średnia długość trwania
4.3.4. Szczytowa długość trwania
4.3.5. Procentowo protokoły
4.3.6. Atakujący wg kraju
4.3.7. Inne - zobaczymy co się da wyciągnąć (więcej niż raport certu)
4.3.8. Być może porównanie do 2015 i wyznaczenie trendu \info{tak, porównanie to dobr

3.4 Klasyfikacja ataków

Nie mogę opisać wszystkich ataków które są na świecie, trzeba znaleźć kryterium stopu – Na razie lista jest wstępna, pisana z pamięci. Trzeba pamietac o multivector attacks

tu oczywiście trz
dobrać odpowied
kryterium, żeby
lepiej to odpowia
tym atakom, któ
będą przeprowad
części eksperyme
nej pracy dyplom

1. Wg źródła
   (a) Strumieniowe - DoS
   (b) Rozproszone (Distributed) - DDoS
   (c) Rozproszone (Distributed) - DDoS
   (d) Odbite (Reflected) – DRDoS
   (e) Wzmocnione (Amplified) – DRADoS
2. Wg warstwy protokołu

```
4.4.2.1. L3:
4.4.2.1.1. GRE
4.4.2.2. L4:
4.4.2.2.1. TCP flood flagi: SYN, ACK, SYN-ACK, PSH, FIN, FRAG
4.4.2.2.2. UDP flood, UDP fragment
4.4.2.2.3. ICMP flood
4.4.2.2.4. TCP out of state
4.4.2.3. L6
4.4.2.3.1. THC-SSL-DoS (HTTPS renegotiation flood)
4.4.2.4. L7
4.4.2.4.1. HTTP
4.4.2.4.1.1. Flood (GET/POST)
4.4.2.4.1.2. Low and slow
4.4.2.4.2. SNMP, DNS+DNSSEC, NTP
```

3.5 Mitygacja ataków DDoS

tutaj też można
wprowadzić jakąś
syfikację

3.5.1 Metody

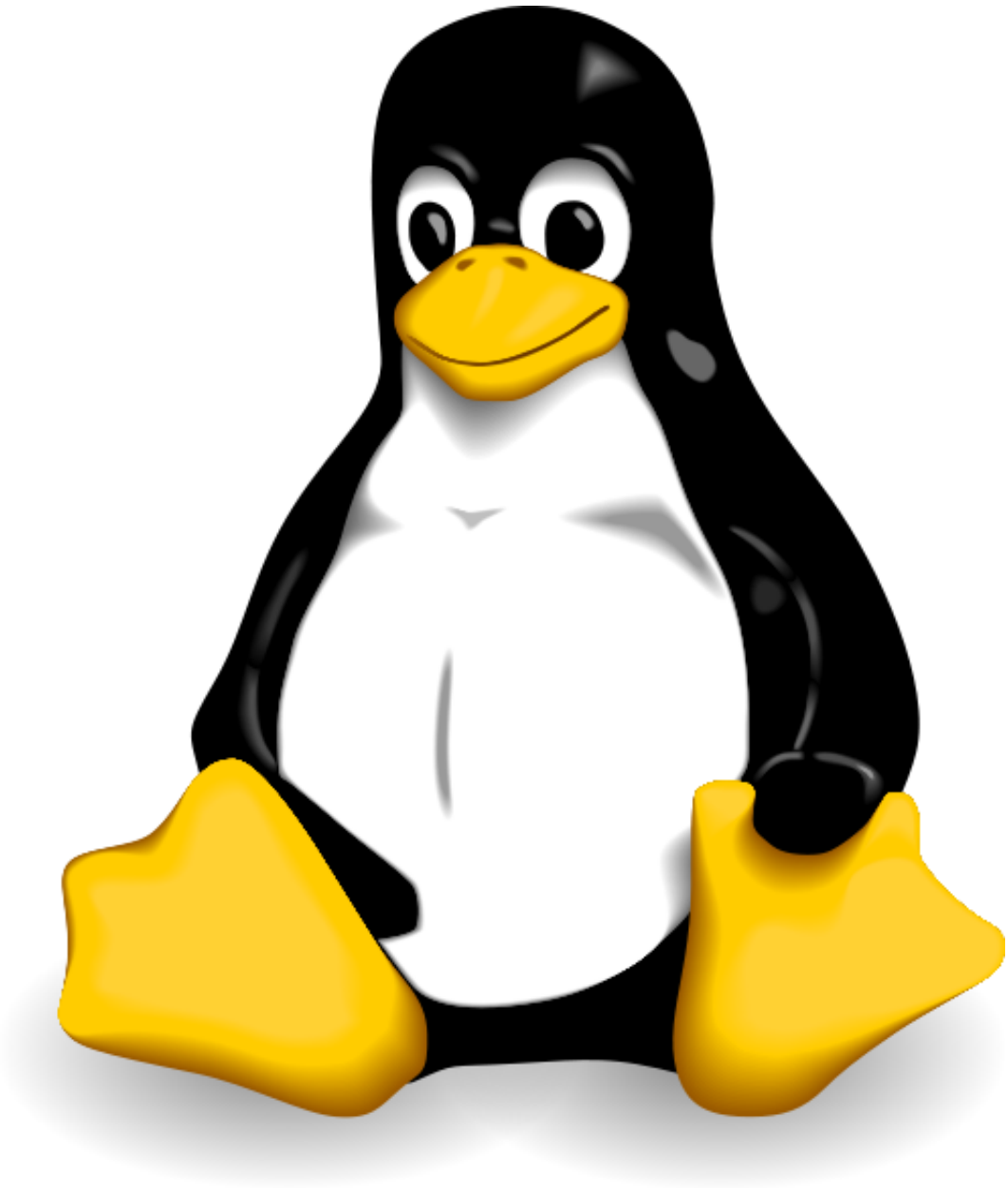
Tryb in-line
BGP Flowspec
Mitgacja w cloudzie / scrubbing center

3.5.2 Rozwiązania na rynku

Radware DefensePro + DefenseFlow
Arbor
FastNetMon
...

Rozdział 4

Podsumowanie



Podsumowanie.
Drugi paragraf.

Odniesienie do Aksın i in., 2006.

W rozdziale **??** przedstawiono cośtam, a w 4 coś innego.

Na rysunku **??** umieszczono pingwina :)

Bibliografia

Aksın, Özge i in. (2006). **?**Effect of immobilization on catalytic characteristics of saturated Pd-N-heterocyclic carbenes in Mizoroki-Heck reactions**?** W: *J. Organomet. Chem.* 691.13, s. 3027–3036.

Skrót

FPS Frame per Second. 2

HA High-Availbility. 1

LB Load-Balancing. 1

Słownik terminów

Single Point of Failure is a generic term referring to the family of Unix-like computer operating systems that use the Linux kernel. 1

Spis rysunków

Spis tablic

Spis załączników

Załączniki

ap1

asdasd