ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 294, Elektrotechnika 35
RUTJEE, z. 35 (2/2016), kwiecień-czerwiec 2016, s. 19-34

Mariusz SZAREK[1]
Mariusz NYCZ[2]
Piotr HAJDER[3]

BADANIE SPRAWNOŚCI SYSTEMÓW IDS/IPS PRZED ATAKAMI DOS I DDOS

Tematem artykułu jest analiza sprawności systemów wykrywania i zapobiegania włamaniom przed atakami odmowy usługi. W początkowej cześć artykuł w oparciu o wynik analiz, zaprezentowano skalę problemu omawianych zagrożeń. W kolejnych paragrafach przedstawiono metodykę badań określenia podatności na ataki odmowy usługi. Następnie przeprowadzono symulacje wydajności i skuteczności obrony przed atakami dwóch sieciowych systemów wykrywania włamań w segmencie open-source Snort i Suricata. Analizowano rozwiązania pracując w trybach nfqueue i af-packet, przy zestawie tych samych reguł. Przeprowadzone testy porównawcze z wykorzystaniem dwóch najpopularniejszy zagrożeń tj. Land i SYN Flood, wykazały przewagę rozwiązania Suricata w skuteczności wykrywania analizowanych ataków. Artykuł jest adresowany do osób zajmujących się wdrażaniem i administracją systemów zabezpieczeń.

Słowa kluczowe: sieci, bezpieczeństwo, ochrona, testy, odmowa, usługi, wykrywanie, wtargnięcie, przeciwdziałanie

1. Wprowadzenie

XXI wiek to okres olbrzymiego rozwoju Informatyki w kontekście urządzeń elektronicznych mających dostęp do globalnej sieci Internet. Można zaobserwować, że to zjawisko nieustannie pogłębia i rozwija się. Standardem stało się, że urządzenia elektroniczne takie jak smartfony, tablety, komputery czy telewizory są wyposażone w możliwość dostępu do sieci, co więcej w najbliższym czasie przewiduje się, że dostęp do sieci uzyskają także urządzenia AGD. W konsekwencji, wraz z rozwojem urządzeń i technik sieciowych rośnie zagrożenie dla osób z nich korzystających. Na przestrzeni ostatnich lat, odnotowuję się permanentny wzrost pojawiania się nowych zagrożeń takich jak: cyberataki,

[1] Mariusz Szarek, Politechnika Rzeszowska, 783535006, 132887@stud.prz.edu.pl
[2] Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, mnycz@prz.edu.pl
[3] Piotr Hajder, Akademia Górniczo-Hutnicza, piootr.hajder@gmail.com

wirusy, robaki, konie trojańskie które głównie ukierunkowane są na wykorzystanie luk w zabezpieczeniach sprzętowych i oprogramowaniu. Motywacją atakujących jest przede wszystkich chęć kradzieży danych użytkownika/firmy/instytucji, usunięcia danych, przejęcia kontroli nad urządzeniem/kontem/systemem czy spowodowaniem sytuacji braku dostępu do danego serwisu. Skuteczna obrona przed tego typu zagrożeniami wymaga od administratora zastosowania szerokiego spektrum zabezpieczeń. Rodzaj, skala i zaawansowanie stosowanych zabezpieczeń powinno być dostosowane do cenności danych, które będą podlegać ochronie.

Wytwarzane aplikacje, programy i systemy bardzo często posiadają różne luki programowe, które uzależnione są od rodzaju i wielkości programu oraz zastosowanego kodu źródłowego. Luki te są wykorzystywane przez hackerów do przeprowadzania różnego typu ataków. Wsparcie oraz aktualizacje oprogramowania zazwyczaj są niewystarczające gdyż czas pomiędzy wykryciem luki przez hackera a opracowaniem i wprowadzeniem aktualizacji jest wykorzystywany do przeprowadzenia ataków. Istnieje wiele rozwiązań umożliwiających znaczące obniżenie a czasami nawet wyeliminowanie występującego ryzyka.

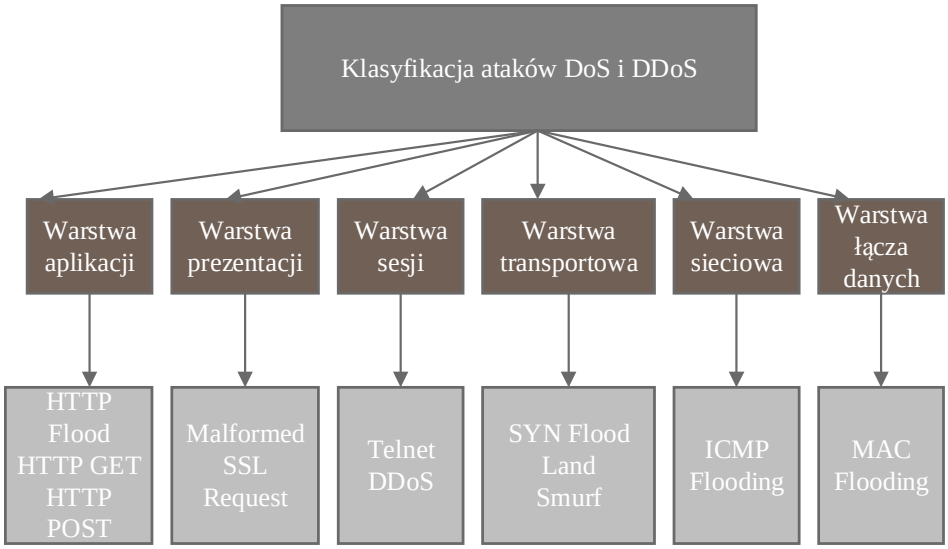
Aktualnie jednym z najbardziej powszechnych i stosowanych ataków są ataki odmowy usługi (ang. Denial of Service) oraz rozproszone ataki odmowy usługi (ang. Distributed Denial of Service). Celem tych ataków jest wywołanie paraliżu serwerów różnego rodzaju firm i instytucji takich jak portale internetowe, banki, sklepy internetowe, strony organizacji rządowych czy naukowych. Ataki te powodują znaczące wydłużenie czasu oczekiwania na odpowiedź danego serwisu lub w najgorszym czasie jego całkowite zablokowanie. Atakowany podmiot może ponieść wysokie straty finansowe i marketingowe, gdyż klienci mogą stracić zaufanie do bezpieczeństwa i kompetencji danej firmy. Atak typu DoS wykorzystywany może być również w celach politycznych aby spowodować unieruchomienie newralgicznych dla państwa serwisów i systemów.

Jednym z najnowszych i najbardziej skutecznych sposobów na ochronę urządzeń, systemów i sieci przed atakami DoS i DDoS są systemy wykrywania wtargnięć (ang. Intrusion Detection System) i systemy przeciwdziałania wtargnięciom (ang. Intrusion Prevention System). Systemy IDS i IPS są fizycznymi i programowymi rozwiązaniami wykorzystywanymi w celu wykrycia, a w przypadku systemów IPS również reagowania na próby ataku na systemy, urządzenia i sieci komputerowe.

2. Charakterystyka ataków odmowy usługi

Ataki odmowy usługi są atakami cybernetycznymi, których celem jest uniemożliwienie funkcjonowania danego systemu komputerowego lub usługi sieciowej. Są to jedne z najstarszych zagrożeń informatycznych, pomimo tego wciąż należą do czołówki najbardziej skutecznych i wydajnych ataków cyberne-

tycznych. Ataki te posiadają szerokie spektrum wersji i rodzajów, które występują w zależności od sposobu wykonania ataku i jego złożoności. Jednym ze sposobów jest emisja nadmiernego ruchu, aby wykorzystać wszystkie zasoby sprzętowe i obliczeniowe ofiary przez co nastąpić może uszkodzenie sprzętu ofiary. Inny sposób polega na użyciu znalezionych luk w zabezpieczeniach różnych protokołów warstw modelu ISO/OSI. Niskie koszty przeprowadzenia ataków odmowy usługi oraz ich małe skomplikowanie powoduje, że częstotliwość i złożoność ataków systematycznie zwiększa się. Powstają coraz to nowsze i bardziej skomplikowane i rozbudowane metody, techniki, sposoby i rodzaje tych ataków. Można dokonać klasyfikacji ataków odmowy usługi pod kątem warstw modelu ISO/OSI na które te ataki ingerują [1][2][17][18].



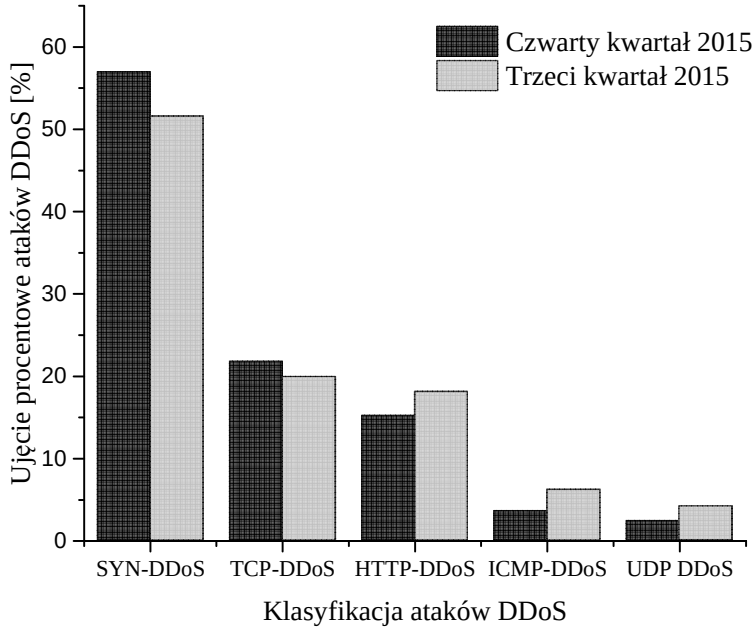
Rys. 1. Klasyfikacja ataków DoS na podstawie warstw modelu ISO/OSI [1][2].

Fig. 1. The classification of DoS attacks on the basis of the ISO/OSI model layers [1][2].

2.1. Statystyczne zestawienie występujących na świecie ataków odmowy usługi

Ochrona sprzętu, serwerów, serwisów sieciowych, zasobów i danych przed atakami odmowy dostępu jest jednym z dominujących zagadnień z jakimi spotykają się firmy zajmujące się bezpieczeństwem elektronicznym i produkcją rozwiązań sprzętowych i programowych zapewniających ochronę przed zagrożeniami cybernetycznymi. Firmy te dokonują badań występujących ataków cybernetycznych i ich trendów a następnie przedstawiają wyniki tych badań za pomocą licznych statystyk. Firma Kaspersky co kwartał opracowuje i publikuje

dane statyczne dotyczące ataków DoS i DDoS występujących na świecie. Według raportu *Kaspersky DDoS Intelligence Report for Q4 2015* wynika, że w czwartym kwartale 2015 najczęściej występującym na świecie rozproszonym atakiem odmowy usługi był atak SYN-Flood, który stanowił 57% wszystkich przeprowadzonych w czwartym kwartale 2015 roku rozproszonych ataków odmowy usługi. Tendencja w porównaniu do poprzedzającego kwartału wskazuje, że atak ten jest coraz bardziej powszechny, gdyż jego częstotliwość wzrosła o 6 punktów procentowych. Innymi często występującymi atakami DDoS były TCP-DDoS, HTTP-DDoS, ICMP-DDoS i UDP-DDoS. Na poniższym wykresie zaprezentowano zestawienie częstotliwości występowania określonych ataków DDoS w trzecim i czwartym kwartale 2015 roku[3]:

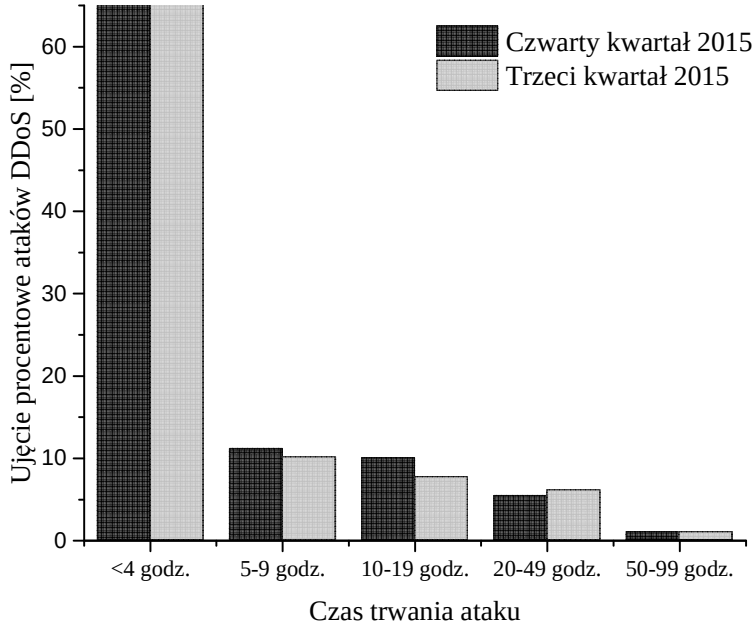


Rys. 2. Procentowe zestawienie występujących w trzecim i czwartym kwartale 2015 roku rodzajów ataków DDoS na świecie [3].

Fig. 2. The percentage summary of DDoS attacks which took place around the world in Q3 and Q4 2015 [3].

Z raportu firmy Kaspersky wynika ponadto, że najczęściej spotykanymi w czwartym kwartale 2015 roku atakami DDoS na świecie były ataki o bardzo krótkim czasie trwania to znaczy ataki poniżej 4 godzin, które zajmowały 70% wszystkich ataków. W porównaniu z trzecim kwartałem nieznacznie wzrosła częstotliwość ataków średniej długości (5-49 godzin), która wynosiła 26,5% w porównaniu do 23,9% z trzeciego kwartału. Podobnie ma się rzecz z atakami

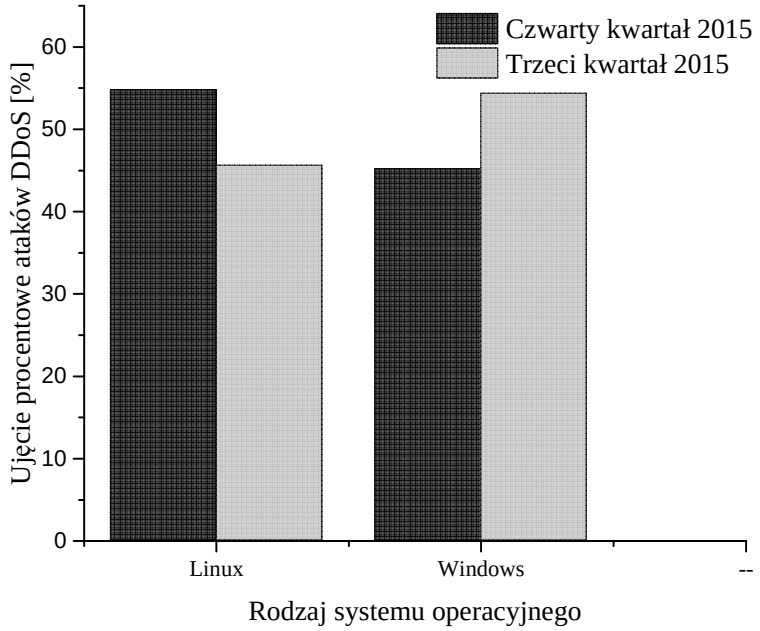
długimi (powyżej 50 godzin), choć mimo to te ataki nadal występowały marginalnie to znaczy przeciętnie 2 na 100 występujących w czwartym kwartale ataków DDoS było atakami długimi. Na poniższym wykresie zaprezentowano zestawienie częstotliwości występowania ataków DDoS o określonej długości w trzecim i czwartym kwartale 2015 roku [3]:



Rys. 3. Procentowe zestawienie występujących w trzecim i czwartym kwartale 2015 roku ataków DDoS o określonych długościach na świecie [3].

Fig. 3. The percentage summary of DDoS attacks of particular duration which took place around the world in Q3 and Q4 2015 [3].

Jedną z najciekawszych informacji w raporcie firmy Kaspersky jest ta mówiąca o systemach operacyjnych zainstalowanych na komputerach botnet, czyli komputerach, które zostały zainfekowane i są wykorzystywane przez hackerów między innymi do przeprowadzenia ataków odmowy usługi. Statystyka ta mówi że 54,8% ataków odmowy usługi było przeprowadzonych przez komputery zoombie z zainstalowaną dystrybucją systemu Linux, zaś 45,2% ataków odmowy usługi pochodziło z komputerów na których zainstalowany był system Windows. Wyniki te są niemal całkowitą korelacją wyników występujących w trzecim kwartale tego roku. Poniższy wykres przedstawia porównanie procentowe liczby komputerów zoombie z zainstalowaną dystrybucją Linuxa oraz z zainstalowanym systemem Windows, które posłużyły do przeprowadzenia ataków DDoS w trzecim i czwartym kwartale 2015 roku[3]:



Rys. 4. Procentowe porównanie komputerów „Zoombie" z zainstalowanymi systemami Linux i Windows, które zostały wykorzystane w trzecim i czwartym kwartale 2015r. do przeprowadzenia ataków DDoS [3].

Fig. 4. The percentage comparison between 'Zoombie' computers with Linux and Windows operating systems, which were used to carry out DDoS attacks in Q3 and Q4 2015 [3].

Na podstawie raportu firmy Kaspersky, która dokonała porównania trzeciego i czwartego kwartału 2015r. dotyczącego rozproszonych ataków usługi na świecie można wysunąć występujące tendencję dotyczące ataków odmowy usługi. Coraz większą częstotliwość zyskują najbardziej rozpowszechnione ataki SYN-Flood. Występuje stały rozwój i coraz większe zaawansowanie ataków i hackerów o czym świadczy zwiększająca się liczba ataków o średnim i długim czasie trwania. Nastąpiło odwrócenie częstotliwości środowisk systemowych z jakich przeprowadzane są rozproszone ataki odmowy usługi. Dominującym stało się przeprowadzanie ataków z jednostek komputerowych zaopatrzonych w system operacyjny Linux [3].

3. Analiza skuteczności systemów IDS/IPS Suricata i Snort na ataki DoS i DDoS

Systemy wykrywania wtargnięć (ang. Intrusion Detection System – IDS) oraz przeciwdziałania wtargnięciom (ang. Intrusion Prevention System) są rozwiązaniami sprzętowymi, programowymi i sieciowymi, które na celu mają

zmaksymalizowanie bezpieczeństwa użytkowania sieci komputerowych w czasie realnym poprzez wykorzystanie specjalnie do tego celu skonstruowanych aplikacji, usług i urządzeń [4].

Systemy IDS są wykorzystywane do wynajdywania wtargnięć, a ściślej rzecz ujmując są to specjalistycznie opracowane rozwiązania takie jak aplikacje, usługi i urządzenia, które są uruchamiane na urządzeniach mających dostęp do sieci. Celem funkcjonowania systemów tego typu jest obserwacja sieci pod kątem występowania potencjalnie niebezpiecznych działań, elementów, składników oraz przypadków złamania zasad bezpieczeństwa elektronicznego. Znalezienie niepożądanego zjawiska sprawia, że system generuje komunikat, który może być przechowywany w pliku tekstowym lub bazie danych. Jednym z najważniejszych elementów procesu opracowywania i tworzenia tego typu systemów jest implementacja rozwiązań dzięki którym możliwe jest pełne zautomatyzowanie procesu ochrony sieci na przykład poprzez implementację rozwiązania umożliwiającego dynamiczną transformację opcji i właściwości zapory ogniowej. Dzięki temu możliwe jest uniknięcie wystąpienia nadużyć na przykład użycia luk w oprogramowaniu[4][5][6].

Systemy IPS są ewolucją systemów IDS, które poza funkcją wykrywania pozwalają zapobiegać sytuacji włamania. Opiera się to na odrzucaniu zainfekowanych pakietów w transmisji do miejsca docelowego. Ta funkcjonalność systemów IPS wymaga ich montażu w miejscu na linii transmisji pakietów[4].

Badania skuteczności systemów IDS/IPS dokonano na przykładzie dwóch systemów Suricata i Snort.

3.1. Analiza skuteczności systemów Suricata i Snort pracujących w trybie nfqueue na rozproszone ataki odmowy usługi – Land oraz SYN-Flood.

Rozpatrywane systemy Suricata i Snort pracujące w trybie nfqueue poddano badaniu skuteczności ich działania w odpowiedzi na występujące rozproszone ataki odmowy usługi: Land oraz SYN-Flood. Poniżej omówiono charakter i właściwości tych ataków:

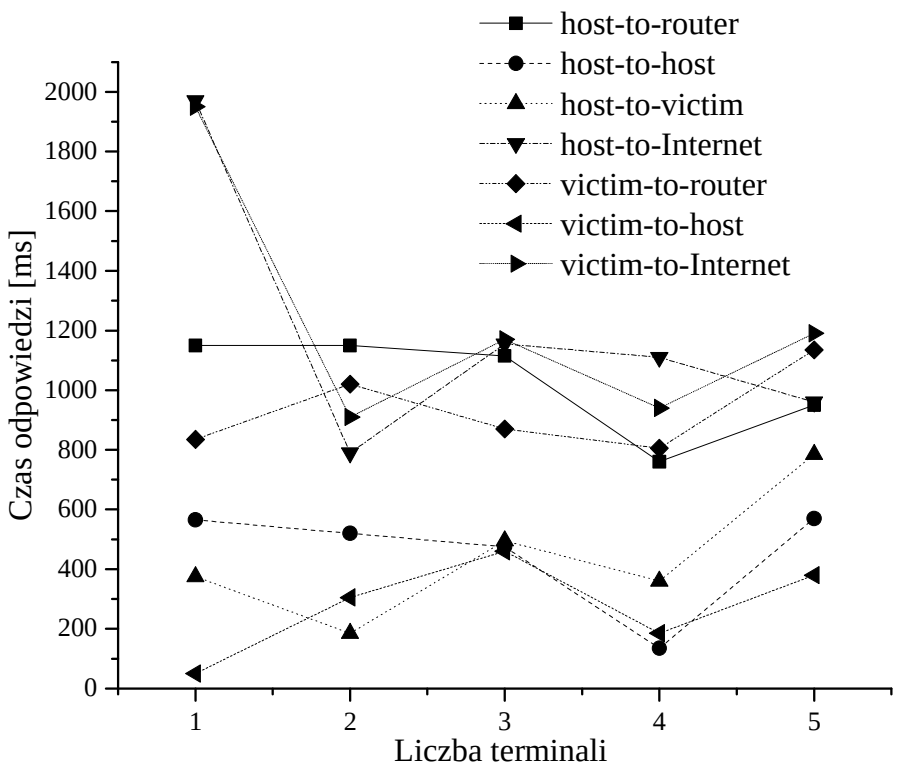
- Land – atak różniący się od standardowych ataków odmowy usługi, ponieważ nie polega on na obciążeniu środowiska atakowanego powodzią pakietów wysłanych z różnych urządzeń, lecz na wysłaniu pojedynczego, odpowiednio zmodyfikowanego pakietu. Spreparowany pakiet to pakiet TCP SYN, który ma ustawione odpowiednio zmodyfikowane pola SOURCE i DESTINATION (adres źródłowy i docelowy). Skutkuje to u ofiary konieczność nieustannego odpowiadania samemu sobie co sprawia, że praca zostaje znacznie spowolniona, a w najgorszym przypadku niemożliwa po-

przez wyczerpanie zasobów. Podobnie jak SYN-Flood Land jest atakiem operującym na czwartej warstwie modelu ISO/OSI[7][8].

- SYN Flood – jest atakiem skierowanym na doprowadzenie zasobów sprzętowych i obliczeniowych ofiary w stan wysycenia. Standardowy ruch sieciowy składa się z próby nawiązywania połączenia TCP z serwerem poprzez doręczenie komunikatu SYN do serwera. Transmisja komunikatu SYN-ACK do klienta oznacza że serwer wyraża zgodę na żądanie. Dzięki temu zachodzi proces nawiązania łączności. Atak SYN-Flood dąży aby proces nawiązania łączności nie skończył się powodzeniem, poprzez wysyłanie do serwera ogromnej liczby komunikatów SYN. Proces ten zazwyczaj używa nieprawdziwych, sfałszowanych adresów IP użytkownika. Każde zapytanie wymaga od serwera aby ten dokonał alokacji odpowiedniej liczby zasobów sprzętowych i obliczeniowych oraz aby nastąpiło dostarczenie komunikatu SYN-ACK w odpowiedzi na każde z nich. Sytuacja ta, w której serwer nie otrzymuje żadnych komunikatów ACK sprawia, że serwer nie może dokonać zwolnienia zasobów sprzętowych i obliczeniowych. Wszystkie zajęte zasoby powodują brak możliwości nawiązania połączenia u innych użytkowników[9][10].

Środowisko użyte do przeprowadzenia badań i symulacji składało się z maszyny wirtualnej z zainstalowanym systemem Kali Linux. Maszyna ta pełniła funkcję środowiska atakującego. Do przeprowadzenia ataku użyto darmowego generatora pakietów hping3. Poza środowiskiem atakującym utworzono maszynę wirtualną z zainstalowanym systemem Debian oraz systemami IDS/IPS, która pełniła funkcję środowiska atakowanego. Konfiguracja składała się też z routera, który zapełniał komunikację pomiędzy maszynami wirtualnymi i Internetem[11][12][13][14][15][16].

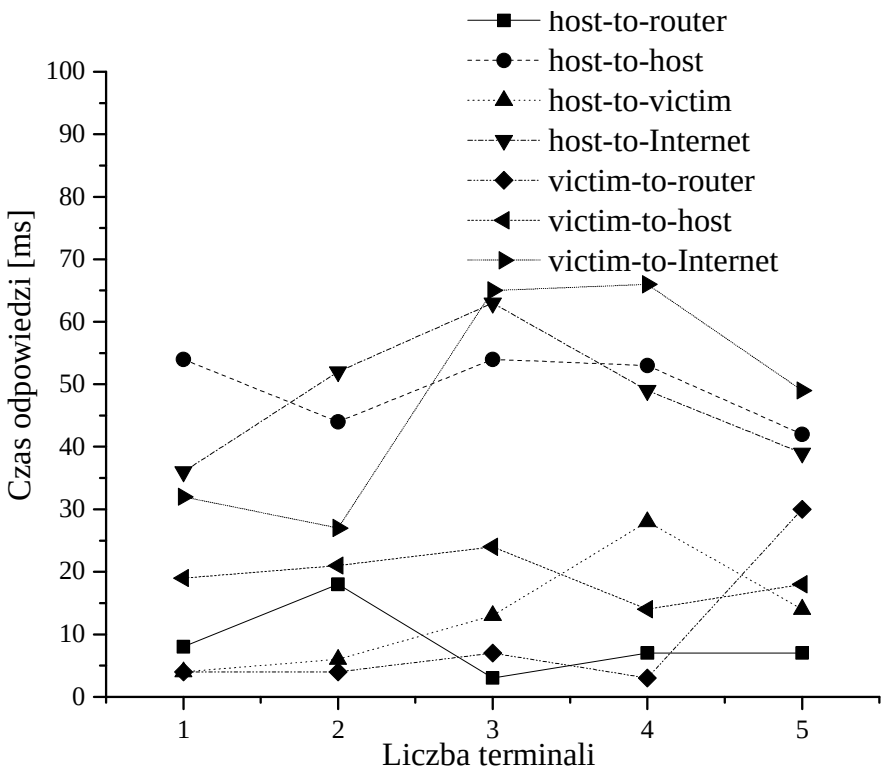
Na początku poddano analizie sprawność systemów IDS/IPS Snort i Suricata pracujących w trybie nfqueue w ochronie przed atakiem Land w przypadku różnej liczby terminali uruchomionych w środowisku atakującym. Poniższy wykres przedstawia czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku Land na system bez żadnego uruchomionego systemu IDS/IPS:



Rys. 5. Czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku Land na system bez żadnego uruchomionego systemu IDS/IPS.

Fig. 5. Response time during communication between respective network entities in case of Land attack on the system without any of the IDS/IPS systems operating.

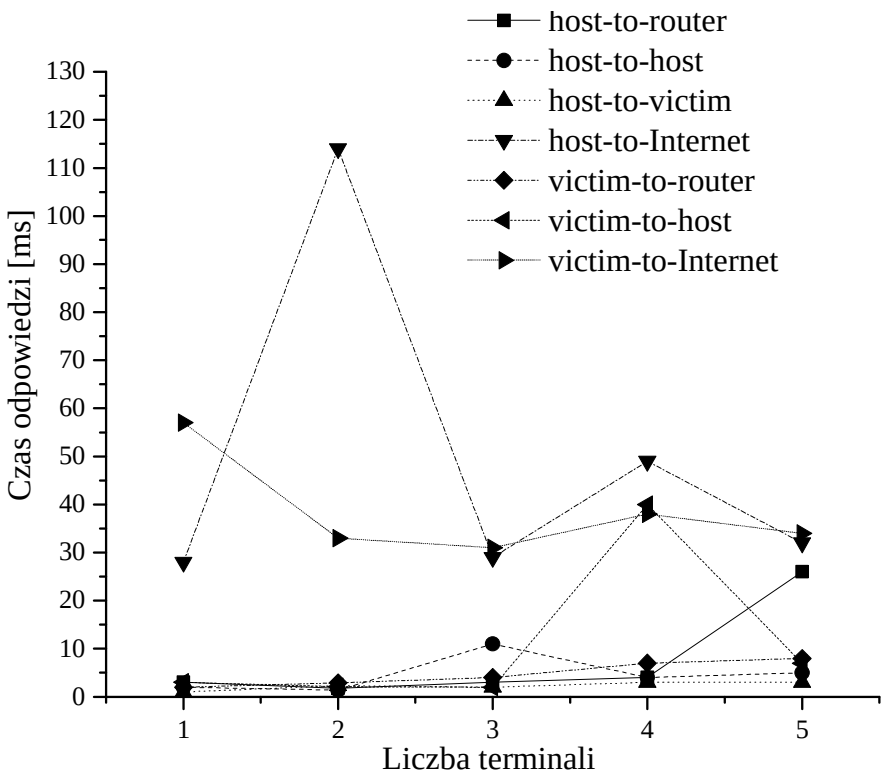
Poniższy wykres przedstawia czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku Land na system z uruchomionym systemem IDS/IPS Suricata pracującym w trybie nfqueue:



Rys. 6. Czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku Land na system z uruchomionym w trybie nfqueue systemem IDS/IPS Suricata.

Fig. 6. Response time during communication between respective network entities in case of Land attack on the system with IDS/ IPS Suricata system running in the nfqueue mode.

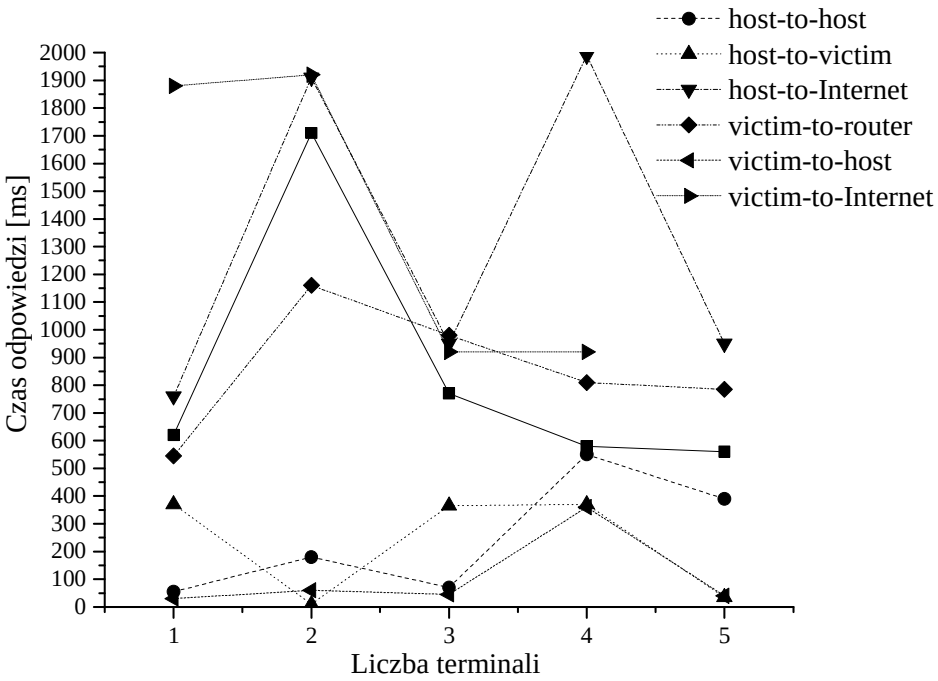
Poniższy wykres przedstawia czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku Land na system z uruchomionym systemem IDS/IPS Snort pracującym w trybie nfqueue:



Rys. 7. Czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku Land na system z uruchomionym w trybie nfqueue systemem IDS/IPS Snort.

Fig. 7. Response time during communication between respective network entities in case of Land attack on the system with IDS/ IPS Snort system running in the nfqueue mode.

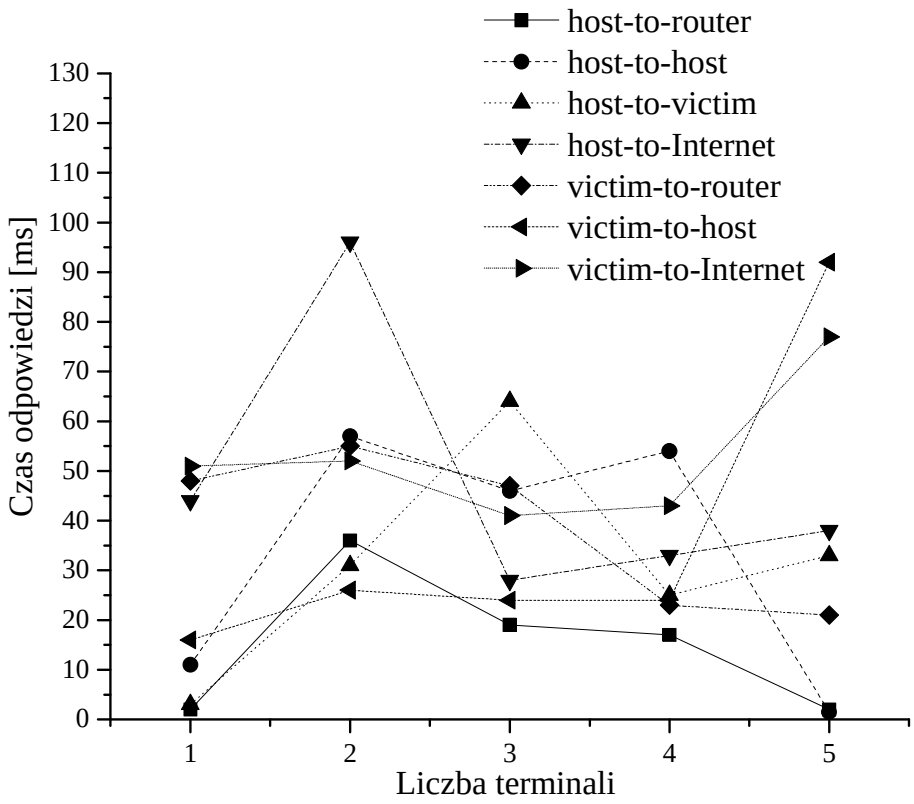
Drugim poddanym testom atakiem był SYN-Flood. Analogicznie jak w przypadku ataku Land zbadano sprawność systemów IDS/IPS Snort i Suricata pracujących w trybie nfqueue w przypadku różnej liczby terminali uruchomionych w środowisku atakującym. Poniższy wykres przedstawia czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku SYN-Flood na system bez żadnego uruchomionego systemu IDS/IPS:



Rys. 8. Czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku SYN-Flood na system bez żadnego uruchomionego systemu IDS/IPS.

Fig. 8. Response time during communication between respective network entities in case of SYN-Flood attack on the system without any of the IDS/IPS systems operating

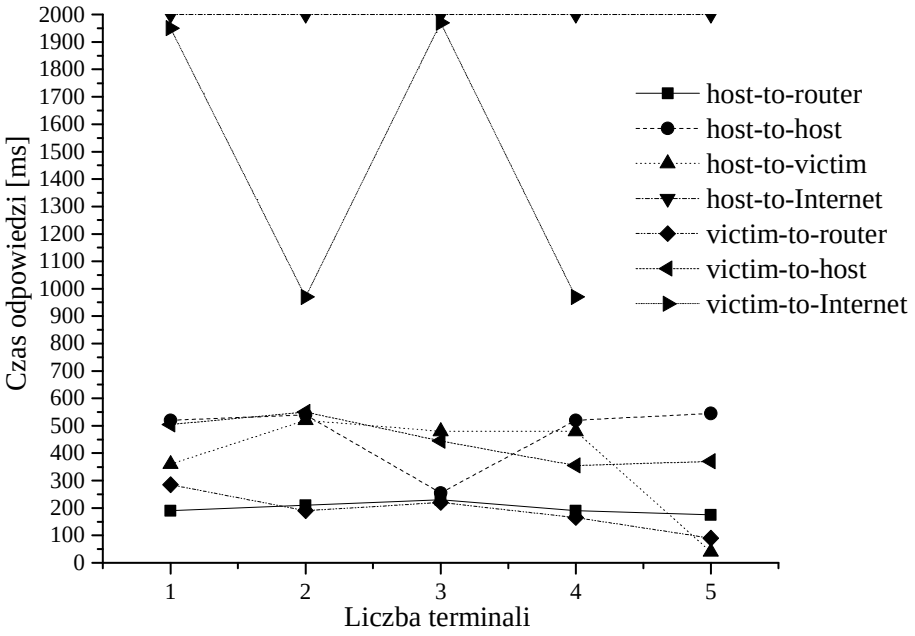
Poniższy wykres przedstawia czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku SYN-Flood na system z uruchomionym systemem IDS/IPS Suricata pracującym w trybie nfqueue:



Rys. 9. Czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku SYN-Flood na system z uruchomionym w trybie nfqueue systemem IDS/IPS Suricata.

Fig. 9. Response time during communication between respective network entities in case of SYN-Flood attack on the system with IDS/ IPS Suricata system running in the nfqueue mode.

Poniższy wykres przedstawia czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku SYN-Flood na system z uruchomionym systemem IDS/IPS Snort pracującym w trybie nfqueue:



Rys. 10. Czasy odpowiedzi podczas komunikacji pomiędzy poszczególnymi podmiotami sieci w sytuacji przeprowadzenia ataku SYN-Flood na system z uruchomionym w trybie nfqueue systemem IDS/IPS Snort.

Fig. 10. Response time during communication between respective network entities in case of SYN-Flood attack on the system with IDS/ IPS Snort system running in the nfqueue mode.

4. Podsumowanie

Porównanie systemów IDS/IPS Suricata i Snort pracujących w trybie nfqueue pokazuje, że oba te systemy są skuteczne w ochronie podmiotów, urządzeń i zasobów sieciowych przed należącym do rodziny ataków odmowy usługi atakiem Land. Działanie systemów pozwoliło bardzo widocznie zminimalizować czasy opóźnień komunikacji pomiędzy różnymi podmiotami w sieci przez co możliwe jest płynne, normalne korzystanie z sieci. Nieznacznie bardziej skutecznym systemem w ochronie przed atakiem Land jest system Suricata, ponieważ pod jego działaniem opóźnienia w sieci nie przekraczają 70[ms].

W przypadku ataku SYN-Flood system IDS/IPS Suricata pracujący w trybie nfqueue okazał się skutecznym narzędziem w ochronie sieci przed tym zagrożeniem. Maksymalne czasy opóźnień nie przekraczały 100[ms]. System Snort pracujący w trybie nfqueue nie zapobiega ogromnym czasom opóźnień wynikającym z działalności ataku SYN-Flood. Pakiety w tym przypadku są tracone, co powoduje że uniemożliwiona jest praca i korzystanie z sieci. Oznacza to że system ten jest nieefektywny w ochronie sieci przed atakiem SYN-Flood.

Na podstawie uzyskanych wyników można stwierdzić, że w przypadku trybu pracy nfqueue system Suricata cechuje się wysoką sprawnością w ochronie sieci przed skutkami ataków odmowy usługi, zaś system Snort tej ochrony nie zapewnia, gdyż jest nieskuteczny w ochronie sieci przed atakiem SYN-Flood.

Literatura

[1] https://dataspace.pl/dos-rodzaje-atakow-cz-1/[Dostęp: 24.08.2015]

[2] https://dataspace.pl/dos-rodzaje-atakow-cz-2/[Dostęp: 3.09.2015]

[3] https://securelist.com/analysis/quarterly-malware-reports/73414/kaspersky-ddos-intelligence-report-for-q4-2015/[Dostęp: 28.09.2015]

[4] K. Scarfone, P. Mell Guide to Intrusion Detection and Prevention Systems (IDPS)

[5] http://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html [Dostęp: 23.12.2015]

[6] http://sekurak.pl/wprowadzenie-do-systemow-ids/[Dostęp: 23.03.2015]

[7] http://insecure.org/sploits/land.ip.DOS.html[Dostęp: 20.11.1997]

[8] http://www.computerworld.pl/news/291980/Atak.na.sieci.IP.html [Dostęp: 29.12.1997]

[9] https://www.incapsula.com/ddos/attack-glossary/http-flood.html [Dostęp: 18.10.2015]

[10] https://www.incapsula.com/ddos/attack-glossary/syn-flood.html [Dostęp: 18.10.2015]

[11] https://www.debian.org/doc/[Dostęp: 7.04.2015]

[12] https://www.snort.org/documents/snort-ips-tutorial[Dostęp: 25.08.2015]

[13] https://www.kali.org/kali-linux-documentation/[Dostęp: 2.01.2016]

[14] https//www.snort.org/documents[Dostęp: 25.08.2015]

[15] http://wiki.hping.org[Dostęp: 30.09.2009]

[16] http://suricata-ids.org/docs/[Dostęp: 6.08.2014]

[17] Wang A.,Mohaisen A., Chang W., Chen S.:Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis, 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2015, pp. 379 - 390

[18] Zeb K., Baig O., Asif K. M.:DDoS attacks and countermeasures in cyberspace, 2015 2nd World Symposium on Web Applications and Networking, Sousse, 2015.

EFFICIENCY TEST OF IDS/IPS SYSTEMS AGAINST DOS AND DDOS ATTACKS

S u m m a r y

The theme of the article is to analyze the efficiency of detection systems and intrusion prevention against denial of service attacks. In the initial part of the article based on the analysis results, presented the scale of the problem of these threats. In the following paragraphs, the methodology of testing to determine susceptibility to denial of service attack. Then conducted simulations effectiveness and efficiency of defense against attacks by the two network intrusion detection systems in the segment of open-source Snort and Suricata. Analyzed solutions working modes nfqueue and af-packet, using the same set of rules. Comparative tests carried out using the two most common threats such Land and SYN Flood, showed superiority solutions Suricata the effectiveness of detection of the analyzed attacks. The article is addressed to people involved in the implementation and administration of security systems.

Keywords: networks, security, protection, tests, denial, service, detection, intrusion, counteraction

DOI: 10.7862/re.2016.7

Tekst złożono w redakcji: maj 2016
Przyjęto do druku: czerwiec 2016