ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 294, Elektrotechnika 35
RUTJEE, z. 35 (2/2016), kwiecień-czerwiec 2016, s. 35-46

Paweł SZELIGA[1]
Mariusz NYCZ[2]
Sara NIENAJADŁO[3]

ANALIZA PODATNOŚCI SERWERÓW WWW W ODNIESIENIU DO ATAKÓW ODMOWY USŁUGI

Artykuł jest adresowany w głównej mierze do osób zajmujących się bezpieczeństwem serwerów WWW. Praca rozpoczyna się od przedstawienia statystycznego ujęcia problemu, jakim są ataki DDoS. Autorzy kładą szczególny nacisk na problematykę ochrony serwerów przed szybko rozwijającymi się atakami odmowy usługi. W pracy przeanalizowano odporności podstawowych konfiguracji dla najpopularniejszych obecnie serwerów web. Na potrzeby badań zostało opracowane wirtualne środowisko testowe, na którym zrealizowano badania podatności wybranych systemów WWW. Celem wykonanej analizy jest rozpoznanie oraz omówienie podstawowych podatności serwera Apache oraz serwera IIS. Dla każdego z omawianych serwerów WWW autorzy zaimplementowali podstawowe mechanizmy ochrony. Artykuł jest adresowany do osób zajmujących się analizą oraz bezpieczeństwem serwerów web.

Słowa kluczowe: DDoS, ochrona, bezpieczeństwo, podatność serwerów WWW, Apache, IIS.

1. Wstęp

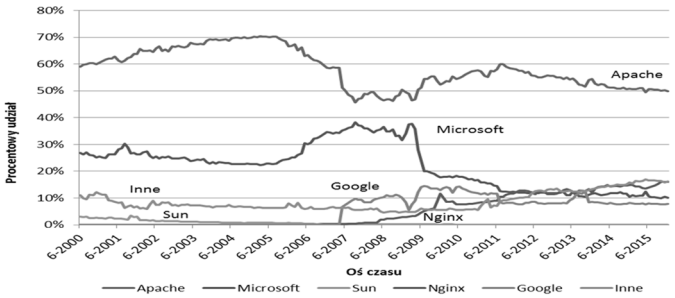
Wraz z postępem techniki powstaje coraz więcej nowych zagrożeń. Autorzy zwracają uwagę, iż ataki DDoS dotyczą każdego z użytkowników sieci WWW. Dlaczego? Odpowiedź na to pytanie jest bardzo prosta, mianowicie większość użytkowników korzysta z wielu usług internetowych często nie zdając sobie o tym sprawy. W ostatnich latach coraz popularniejsze stały się sklepy internetowe, internetowe konta bankowe czy inne rodzaje e-usług. Ataki DDoS mogą być wykorzystywane do powodowania strat finansowych dużych korporacji, wykradania rekordów zawierających hasła i loginy z baz danych banków a

[1] Paweł Szeliga, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Wydział Elektrotechniki i Informatyki, email: polozaq1@wp.pl
[2] Autor do korespondencji: Mariusz Nycz, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, mnycz@prz.edu.pl
[3] Sara Nienajadło, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Wydział Elektrotechniki i Informatyki, email: sara.n@op.pl

także znajdują swoje zastosowanie do walki z organizacjami rządowymi. Niestety to nie wszystkie cele, do których wykorzystuje się ataki DDoS. Większość administratorów i osób zajmujących się bezpieczeństwem w sieci, postrzega ataki DDoS, jako zagrożenie, z którym należy walczyć. Ataki odmowy usługi mogą być także wykorzystywane do badania podatności serwerów WWW. Niestety bardzo rzadko ataki DDoS są wykorzystywane w dobrych celach. Dużo częściej stają się narzędziem służącym do nielegalnego zarabiania pieniędzy czy pozyskiwania informacji. To jak zostaną wykorzystane zależy w głównej mierze od zamiarów atakującego. Z każdym rokiem powstają nowe, bardziej skomplikowane narzędzia umożliwiające przeprowadzenie niebezpiecznych ataków DDoS. Administratorzy serwerów WWW oraz osoby zajmujące się bezpieczeństwem w sieci stają przed bardzo trudnym zadaniem, jakim jest zapewnienie bezpieczeństwa sprzętowi i aplikacjom internetowym. Autorzy zwracają uwagę, iż szybko rozwijające mechanizmy ataków uniemożliwiają 100% zabezpieczenie serwerów. W ostatnich latach atakujący coraz częściej powracają do starych metod ataków skierowanych na warstwę aplikacji, dlatego istotnym elementem bezpieczeństwa stało się projektowanie oraz wdrażanie odpowiednio zabezpieczonych aplikacji internetowych.

2. Statystyczne ujęcie problemu ataków DDoS

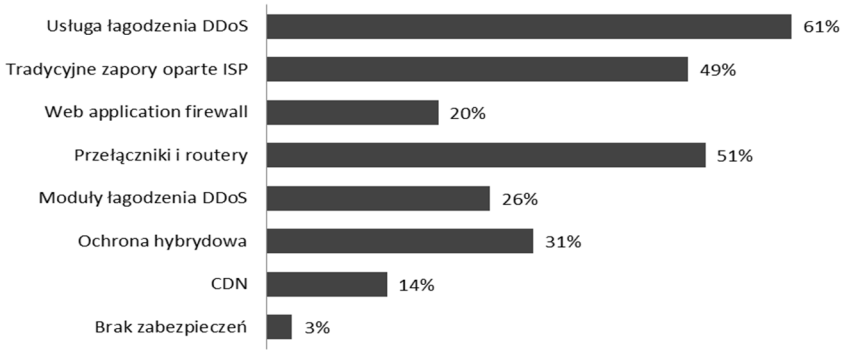
Celem dla ataku może stać się dowolna witryna lub usługa WWW. Według raportu Netcraft do najpopularniejszych a co za tym idzie najczęściej wykorzystywanych serwerów sieci Web zaliczano m.in. serwer Apache, Nginx czy serwer Microsoftu [10]. Jak podaje raport [10], z usług serwera Apache w roku 2015 korzystało 50,45% wszystkich stron i serwisów WWW. Natomiast drugie miejsce w rankingu zajął serwer Nginx, udostępniając swoje usługi dla 15,33% klientów.



Rys. 1. Procentowy rozkład aktywnych serwisów WWW w odniesieniu do serwerów WWW w latach 2000- 2015

Fig. 1. The percentage distribution of active Web sites in relation to the web servers in the years 2000- 2015

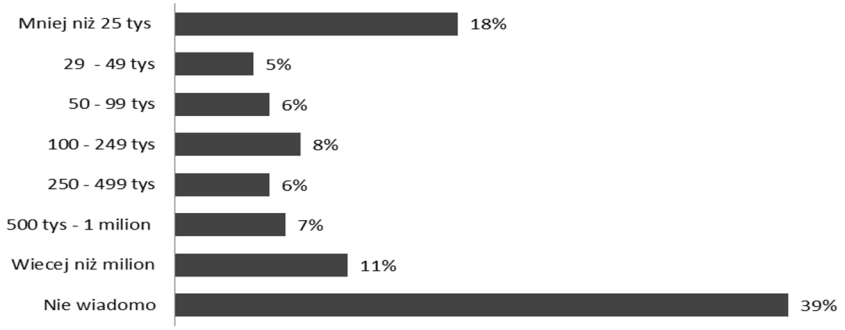
Według raportu Neustar DDoS Attacks & Protection Report [11] większość firm, atakowanych jest kilka razy rocznie, natomiast 30% badanych firm pada ofiarą ataku ponad 10 razy w ciągu roku. Jeżeli atak zakończy się powodzeniem, średnie straty finansowe w godzinach szczytu szacowane są na ponad 100 tys. dolarów. Większość spółek finansowych (94%), do obrony wykorzystuje tzw. hybrydowe mechanizmy ochrony. Wraz z postępem techniki, duże firmy zmieniają podejście do ochrony przed atakami DDoS. W dzisiejszych czasach większość firm nadal korzysta z różnego rodzaju firewall-i, ale ponadto wykorzystywane są mechanizmy łagodzące czy usługi w chmurze w celu zwalczenia ataków. W ostatnim roku dużą popularność zyskały rozwiązania hybrydowe. Rysunek 2 przedstawia dane statystyczne.



Rys. 2. Procentowy rozkład stosowanych mechanizmów obrony przed atakami DDoS

Fig. 2. The percentage distribution of used defense mechanisms against DDoS attacks

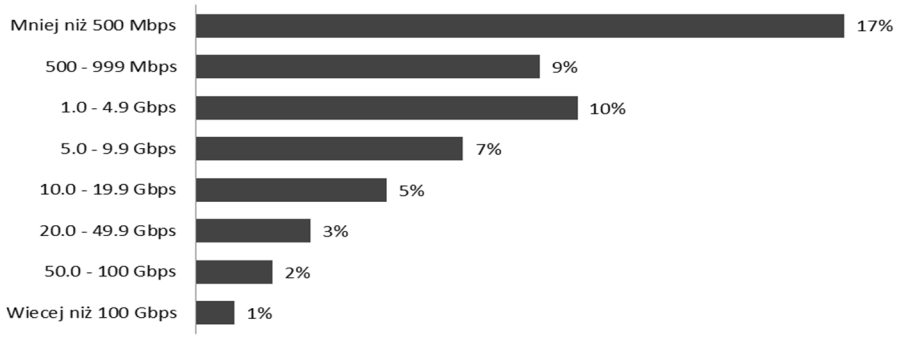
Jak podaje raport [11], coraz więcej ataków DDoS jest przeprowadzanych na firmy finansowe. W związku z dużym prawdopodobieństwem ataku, większość firm zmuszona jest do podjęcia kroków zapobiegawczych, jednocześnie inwestując w hybrydową ochronne przeciw atakom odmowy usługi. Według raportu Neustar czynności te podejmuje 43% zagrożonych firm finansowych. Branża usług finansowych opiera się na równoważeniu ryzyka oraz odpowiedniemu inwestowaniu. Niedostępność jakichkolwiek usług zawsze związana jest z dużymi stratami. Dlatego dobrze przygotowane mechanizmy ochrony a także detekcji ataków DDoS są kluczowe dla działania firm świadczących usługi finansowe. Jak podaje raport [11], firmy ponoszą największe straty finansowe w godzinach szczytu. Należy pamiętać, iż dane pochodzą z firm zlokalizowanych w Stanach Zjednoczonych.



Rys. 3. Straty finansowe wynikające z ataków DDoS przeprowadzonych w godzinach szczytu

Fig. 3. Financial losses resulting from DDoS attacks carried out during peak hours

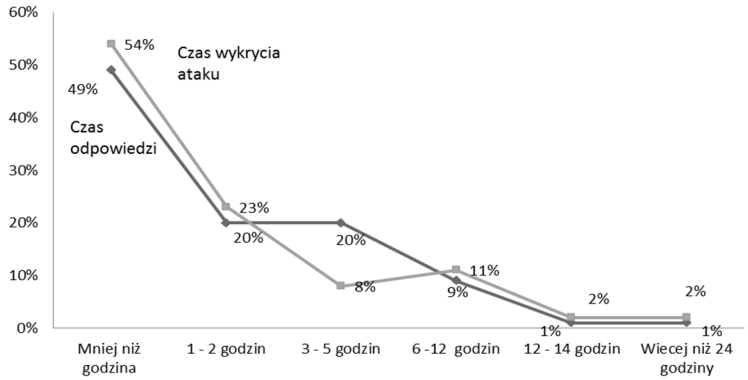
Bezpośrednio z ilością przeprowadzanych ataków wiąże się siła przeprowadzonego ataku. Interesującymi statystykami przedstawionymi w raporcie [11] są statystyki ukazujące częstotliwość ataków wraz z podziałem na moc. Najwięcej ataków wykonywanych jest z małą siłą. Nie oznacza to, iż są one nie skuteczne, ponieważ zadaniem ataku DDoS jest doprowadzenie serwera do sytuacji, w której zgłoszona zostanie odmowa usługi. Niektóre mechanizmy ataków wykorzystują do tego celu luki w aplikacjach. Ponadto istnieje grupa ataków Slow HTTP, których działanie opiera się o powolne uzupełnianie ciała bądź nagłówka HTTP. Ilość ataków wykorzystujących małą przepustowość łącza uzależniona jest także od dostępnych narzędzi umożliwiających wykonanie prostego ataku DDoS. W większości przypadków są to aplikacje okienkowe, w których działanie osoby wykonującej atak ogranicza się do podania adresu ofiary oraz wybrania rodzaju przeprowadzanego ataku.



Rys. 4. Siła ataku DDoS wśród badanych firm

Fig. 4. The strength of DDoS attack among the surveyed companies

Aby atak przyniósł oczekiwane efekty w postaci strat finansowych należy go przeprowadzić w odpowiednim momencie. Według danych statystycznych przedstawionych w raporcie [11] najwięcej firm, bo aż 27% wśród badanych, pada ofiarą ataków DDoS od dwóch do pięciu razy w ciągu roku, natomiast 14% firm staje się ofiarą ataku w każdym miesiącu. Innym ważnym parametrem przedstawionym w raporcie Neustar, jest czas wykrywania ataków oraz czas odpowiedzi. Jak najszybsze wykrywanie ataków jest jednym z kluczowych elementów stosowanych do walki z tego typu zagrożeniami. Efektywne wykrywanie zagrożenia jest procesem niezwykle trudnym do zrealizowania. Bez odpowiednich mechanizmów umożliwiających wykrywanie ataków, w żaden sposób nie jest możliwa obrona przed atakami DDoS. Według raportu u większości badanych firm proces ten trwa mniej niż godzinę. Istnieją jednak przypadki, iż atak nie zostanie wykryty nawet przez więcej niż 24 godziny.



Rys. 5. Czas wykrycia ataku DDoS w stosunku do czasu odpowiedzi

Fig. 5. DDoS attack detection time relative to the response time

3. Rodzaje ataków odmowy usługi

Przeprowadzona analiza skuteczności ataków wykazała skuteczność poszczególnych typów ataków. Do przeprowadzenia analizy wykorzystano skrypt Slowloris, R.U.Dead.Yet oraz atak Syn Flood. Poniżej zostały przedstawione pokrótce charakterystyki zastosowanych typów ataków:

- Slowloris – atak wykorzystujący podczas swojego działania zapytania HTTP Get. Jednym z głównych zadań skryptu jest podtrzymywanie aktywnego połączenia. Połączenie może zostać zamknięte poprzez wysłanie znaku pustej linii za pomocą dwóch znaczników [CRLF][CRLF]. Dane podtrzymujące połączenie z serwerem zakończone są pojedynczym znacznikiem [CRLF]. Skuteczność ataku Slowloris zapewniona jest poprzez utrzymywanie wielu pół-otwartych połączeń. Maksymalny czas przezna-

czony na uzupełnienie nagłówka wynosi 300s. Czas ten może być dowolnie zmodyfikowany przez administratora serwera WWW. Każde przesłanie pakietu do serwera powoduje ustawienie czasu odnowa na wartość 300s. Istotną informacją dotyczącą ataku Slowloris jest fakt, iż atak ten nie niszczy w żaden sposób danych a jedynie może doprowadzić do niedostępności serwera WWW. Podczas trwania samego ataku, nie istnieje możliwość namierzenia sprawcy wykorzystując jedynie logi serwera Apache. Żądania przesyłane do serwera wydają się być uzasadnione, przez co systemy IPS nie są wstanie wykryć ataku za pomocą skryptu Slowloris. Atak Slowloris nie jest atakiem wymagającym dużej przepustowości. Po kilku sekundach od zakończenia ataku serwer wraca do normalnego trybu pracy [7, 8, 9, 13].

- R.U.Dead.Yet – darmowy skrypt bazujący na zapytaniach HTTP Post. Ideą działania ataku jest przesyłanie niekompletnych, ale uzasadnionych fragmentów ciała nagłówka. Podczas podtrzymywania pół-otwartego połączenia wykorzystywane jest długie pole Content – Lenght. Atak R.U.Dead.Yet wysyła fragmenty nagłówka o rozmiarach 1 bajta wykorzystując do tego niewielką prędkość. Odpowiednia konfiguracja ataku może spowodować, iż pakiety będą wysyłane w losowej kolejności, przez co proces wykrywania i ochrony przed atakiem będzie znacznie trudniejszy. Istnieje możliwość zamaskowania prawdziwego, źródłowego adresu IP poprzez wykorzystanie proxy [5 ,13].
- Syn Flood – atak wykorzystujący niedoskonałości połączenia TCP/IP. Three Way Handshake jest to proces tworzenia połączenia klient – serwer. W pierwszym etapie ustanawiania połączenia, zadaniem klienta jest zarezerwowanie portu oraz przesłanie pakietu SYN do serwera WWW. Następnie zadaniem serwera jest rezerwacja zasobów oraz odpowiedź pakietem SYN-ACK. Kolejnym etapem ustanowienia połączenia jest odpowiedz klienta pakietem ACK, czego efektem jest zakończenie procesu tworzenia połączenia klient – serwer. Podczas ataku Syn odpowiedź serwera zostaje przesłana na sfałszowany adres IP. Co określony interwał czasowy serwer wysyła kolejny pakiet SYN-ACK. Pół-otwarte połączenie może być podtrzymane nawet od 3 do 4 minut, przez co zasoby serwera nie zostaną zwolnione. Oznacza to, iż utworzenie dużej liczby połączeń może wyczerpać ograniczone zasoby serwera, dzięki czemu zgłoszona zostanie odmowa usług [1, 3, 13].

4. Mechanizmy ochrony przed atakami odmowy usługi

Jednym z elementów przeprowadzanej przez autorów analizy serwerów WWW była implementacja wybranych mechanizmów ochrony przed atakami DDoS. Implementacja mechanizmów miała na celu zbadanie zachowania wybranych web serwerów w stosunku do ataków odmowy usługi w przypadku

braku zastosowania mechanizmów bezpieczeństwa jak i w przypadku uruchomienia każdej z zaimplementowanych metod ochrony. Ponieważ architektura większości serwerów jest różna, nie można zaimplementować tej samej wersji mechanizmu dla różnych serwerów. Niemniej jednak istnieją różne wersje tych samych aplikacji, z których każda jest dedykowana dla różnych serwerów. Wykorzystane mechanizmy ochrony przed atakami DDoS zostały przedstawione poniżej:

- Moduł mod_security – pełni role zawansowanego firewall-u dla serwera Apache. Głównymi zadaniami modułu jest monitorowanie i analiza napływającego ruchu do serwera WWW. Natomiast wprowadzenie właściwych reguł umożliwia ograniczenie ilości logowań do jednego na minutę czy też umożliwia stworzenie czarnej listy, do której dodawane będą adresy IP, dla których zostały przekroczone ustalone parametry. Ponadto moduł może sprawdzać ilość wysłanych żądań z danego adresu IP oraz ilość żądań wymagających zasobów dynamicznych. Domyślnie adres IP może zostać usunięty z listy zakazanych adresów po upływie 5 min [15].
- Moduł mod_qos – moduł przeważnie wykorzystywany do zabezpieczenia odrębnych usług serwera Apache. Jego główną zaletą jest możliwość ograniczenia zarówno dolnej jak i górnej przepustowości łącza, którym będą przesyłane informacje. Takie podejście twórców przy projektowaniu modułu zapewnia skuteczna ochronę przed atakami Slow HTTP. Istnieje także możliwość ograniczenia maksymalnej liczby obsługiwanych klientów, maksymalnej liczby połączeń HTTP Keep – alive, maksymalnej liczby aktywnych połączeń TCP oraz maksymalnego rozmiaru ciała i nagłówka żądania. Dodatkową zaletą modułu jest możliwość dołączenia innego modułu umożliwiającego generowanie statystyk i raportów przedstawiających sytuacje, jaka panuje w danej chwili na serwerze Apache [15].
- Moduł mod_evasive – moduł stworzony zarówno dla serwera Apache jak i dla serwera IIS. Jego głównym zadaniem jest ochrona przed atakami odmowy usługi wykorzystując ograniczenia ilości jednoczesnych żądań dla wątku lub procesu. Jego konstrukcja umożliwia na komunikacje z routerami, ipchains oraz z firewallami [6].
- Moduł dynamicznego ograniczenia IP – zapewnia ochronę przed atakami typu Slow HTTP oraz Syn Flood dla serwera IIS. Dla każdego adresu IP zliczana jest liczba nawiązanych połączeń. Dodatkowym parametrem ograniczającym możliwość wykonania ataku DDoS jest ograniczenie maksymalnej liczby żądań dla danego adresu IP, jakie może obsłużyć serwer w danej chwili. Jeżeli zostanie przekroczony jeden z wymienionych parametrów, połączenie może zostać zamknięte przez serwer lub może zostać zablokowane do momentu, kiedy liczba połączeń lub żądań nie spadnie poniżej określonego limitu. W obydwóch przypadkach atakujący zostanie poin-

formowany jednym z 4 komunikatów: błąd 401 –połączenie nieautoryzowane, błąd 403 – zabronione po-łączenie, błąd 404 – plik nie został znaleziony lub żądanie zamknięte [1, 2].

5. Analiza podatności serwerów WWW

Jednym z podstawowych zadań każdego serwera jest obsługa żądań protokołu HTTP. Serwery WWW są wykorzystywane m.in. do utrzymywania stron WWW oraz wielu innych usług internetowych. Do najpopularniejszych należy poczta WWW. Istnieje wiele serwerów różniących się architekturą, mechanizmami ochrony czy obsługą żądań klientów. Autorzy badali podatności serwera Apache oraz serwera firmy Microsoft.

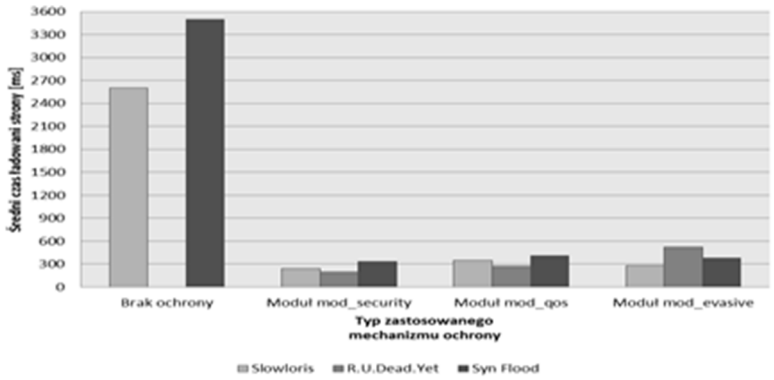
Serwer Apache – najbardziej popularny i jednocześnie darmowy serwer WWW. Może działać w jednym z dwóch trybów: MPM Prefork oraz MPM Worker [4]. Istotną różnicą pomiędzy trybami pracy jest sposób obsługi żądań. Pracując w trybie MPM Prefork, serwer dla każdego przychodzącego żądania tworzy nowy proces potomny natomiast, jeżeli serwer pracuje w trybie MPM Worker dla każdego żądania tworzony jest nowy wątek potomny. Obydwie architektury posiadają wady jak i zalety. Serwer pracujący w trybie Prefork zapewnia bezpieczeństwo każdego z nawiązanych połączeń gdyż w sytuacji, gdy połączenie musi być zerwane, zostanie zakończony tylko jeden proces. Zaletą pracy w trybie MPM Worker jest możliwość zestawienia przez serwer większej ilości połączeń, ponieważ pojedyncze żądanie zużywa mniejszą liczbę zasobów [4, 14].

Serwer IIS – serwer stworzony i rozwijany przez firmę Microsoft. Zapewnia szerokie wsparcie dla produktów .NET Framework oraz ASPX. Oferuje narzędzia umożliwiające śledzenie nieprawidłowych żądań czy wsparcie wirtualnego hostingu. Do obsługi żądań aplikacji routingu, usług multimedialnych, obsługi FTP wykorzystuje zewnętrzne rozszerzenia internetowe.

Niezależnie od zastosowanego serwera WWW ważnym elementem jego pracy jest zapewnienie bezpieczeństwa przechowywanym danym jak i działającym usługom. Aplikacje te powinny być zabezpieczone przed wszystkimi potencjalnymi atakami. Autorzy zwracają uwagę na problem 100% zabezpieczenia serwera WWW przed naruszeniem procedur bezpieczeństwa. Niestety nie można powiedzieć, iż istnieje serwer zabezpieczony w takim stopniu, ponieważ zawsze jest szansa, iż jakiś atak zostanie zakończony sukcesem. Ówcześnie stosowane mechanizmy ochrony przed atakami DDoS są wystarczające, ale ciągle muszą być rozwijane. Przeprowadzona analiza podatności dwóch najpopularniejszych serwerów miała na celu pokazanie poszczególnych słabych punktów. Analiza podatności została powtórzona po zaimplementowaniu mechanizmów obrony przed atakami. Przeprowadzane testy wykonane zostały w zamkniętym środowisku testowym. Zastosowanie wirtualnego środowiska umożliwiło auto-

rom na przeprowadzenie bezpiecznej analizy podatności serwerów WWW [12, 13, 17, 18]. Do przeprowadzenia wcześniej wspomnianej analizy zostały wykorzystane 3 maszyny wirtualne, z których każda posiadała zainstalowany system Kali Linux. Dla maszyny wirtualnej pełniącej role serwera www został ustawiony rozmiar pamięci RAM na wartość 4GB, stworzony wirtualny dysk SCSI o rozmiarze 60GB. Serwer przez cały czas miał do dyspozycji dwu rdzeniowy procesor. Serwer Apache przez cały okres trwania testów pracował w trybie MPM Prefork, co pozwoliło na bezpieczne zamykanie żądań sklasyfikowanych, jako prawdopodobny atak. Każdy z testów został wykonany 4 razy. Niestety do testów nie zostały wykorzystane zasoby fizycznego serwera.

Każdy z działających serwerów może stać się ofiarą ataku odmowy usługi. W porównaniu z ubiegłymi latami, częstotliwość przeprowadzanych ataków wzrosła. Oznacza to, iż z każdym kolejnym rokiem coraz istotniejszą kwestią są mechanizmy ochrony serwerów WWW. Szczególnie podatnymi serwerami są maszyny, które zostały pozbawione podstawowych metod ochrony, detekcji czy mechanizmów odpowiadających za zwalczanie zagrożeń. Poniżej przedstawione zostały wyniki przeprowadzonych badań zarówno dla serwera Apache jak i serwera IIS.

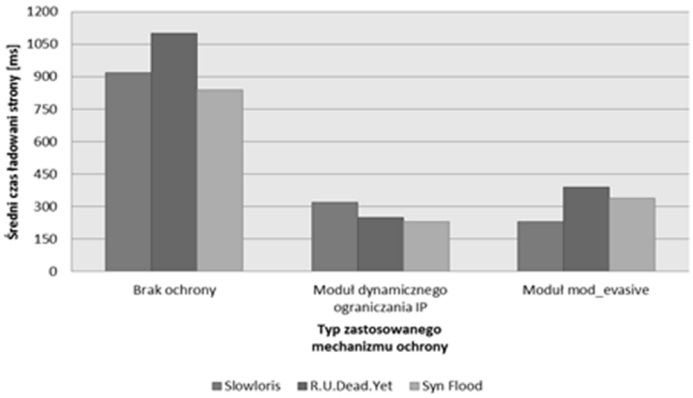


Rys. 6. Analiza czasu ładowania stron WWW serwera Apache w czasie trwania wybranych ataków DDoS

Fig. 6. Analysis of charging time web server Apache during the selected DDoS attacks

Przeprowadzone badania podatności serwera Apache wykazały istotne braki mechanizmów wykrywania oraz zapobiegania atakom DDoS. Niestety serwer Apache w domyślnej konfiguracji nie jest w stanie odeprzeć trwającego ataku. Podczas trwania ataku R.U.Dead.Yet serwer zgłosił odmowę usługi a strona testowa została załadowana kilka sekund po zakończeniu ataku. W przypadku wykonywania testów skryptem Slowloris oraz generatorem pakietów symulującym atak typu Syn Flood okazało się, iż serwis odpowiedział na żądanie klienta,

ale dopiero po 2600 ms oraz 3500 ms. Zastosowanie wybranych mechanizmów ochrony spowodowało, iż odpowiedzi serwera kształtowały się w przedziale do 200 ms do 600 ms w zależności od zastosowanej ochrony.



Rys. 7. Analiza czasu ładowania stron WWW serwera IIS w czasie trwania wybranych ataków DDoS

Fig. 7. Analysis of charging time Web IIS server for the duration of selected DDoS attacks

Analiza zachowania serwera IIS w odniesieniu do wybranych ataków wyglądała nieco inaczej. W przypadku braku zastosowanych mechanizmów ochrony serwer odpowiadał szybciej niż serwer Apache. Zastosowanie mechanizmów ochrony spowodowało poprawę w przypadku, gdy działały zaimplementowane moduły. W żadnym z testów niezgłoszona zastała odmowa usługi. W najbardziej pesymistycznym przypadku strony ładowane były w czasie krótszym niż 1200 ms. Najlepszą ochronę dla serwera IIS podczas ataku R.U.Dead.Yet oraz Syn Flood zapewnił moduł dynamicznego ograniczania IP. Natomiast w przypadku ataku Slowloris.

6. Podsumowanie

Przeprowadzone badania pokazały zachowania serwerów WWW w odniesieniu do różnych typów ataku. Typy ataków zostały dobrane w taki sposób, aby zbadać wiele słabych stron serwerów.

Odpowiednia implementacja mechanizmów ochrony może zapewnić skuteczniejszą ochronę przeciwko atakom DDoS. Należy zdawać sobie sprawę, iż ważnym elementem zabezpieczenia serwerów WWW jest stosowanie mechanizmów umożliwiających wykrywanie zagrożeń. Im wcześniej administrator serwera WWW będzie wiedział o zagrożeniu tym szybciej zostaną podjęte odpowiednie kroki walki z atakiem. Najbardziej podatnym serwerem w domyślnej

konfiguracji okazał się serwer Apache. Implementacja któregokolwiek z wybranych mechanizmów ochrony spowodowała, iż serwer nie zgłaszał odmowy usługi. Sytuacja serwera IIS była bardzo podobna. Pomimo iż w domyślnej konfiguracji serwer nie zgłaszał odmowy usług, po zaimplementowaniu mechanizmów ochrony strony WWW były ładowane dużo efektywniej niż podczas ataku DDoS bez uruchomionych metod zabezpieczeń.

Literatura

[1] Burdach M.: Hardening the TCP/IP stack to SYN attacks, http://www.symantec.com/connect/articles/hardening-tcpip-stack-syn-attacks [dostep: 5 Sierpień 2015 r.].

[2] Darmanin G.: 8 tips to secure your IIS installation, http://www.acunetix.com/blog/articles/8-tips-secure-iis-installation [dostep: 5 Listopad 2014 r.].

[3] Gangte T.: SYN Flood Attacks- "How to protect?", https://hakin9.org/syn-flood-attacks-how-to-protect-article/ [dostep: 21 Marzec 2014 r.].

[4] Guillermo G.: Understanding Apache 2 MPM (worker vs prefork), https://www.garron.me/en/blog/apache2-mpm-worker-prefork-php.html [dostep: 26 Grudzień 2012 r.].

[5] Incapsula: R.U.D.Y. (R-U-Dead-Yet?) - DDoS Attack Glossary, https://www.incapsula.com/ddos/attack-glossary/rudy-r-u-dead-yet.html.

[6] Linode: Mod_evasive on Apache, https://www.linode.com/docs/websites/apache-tips-and-tricks/modevasive-on-apache [dostep: 5 Luty 2013 r.].

[7] Michalczyk A.: Ataki Slow HTTP DoS (cz. 1.) – Slowloris, http://sekurak.pl/ataki-slow-http-dos-cz-1-slowloris [dostep: 9 czerwca 2014 r.].

[8] Michalczyk A.: Czym jest atak DDoS (cz. 2) — techniki i narzędzia http://sekurak.pl/czym-jest-atak-ddos-cz-2-techniki-i-narzedzia/ [dostep: 13 Luty 2015 r.].

[9] Muscat I.: How To Mitigate Slow HTTP DoS Attacks in Apache HTTP Server, https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/ [dostep: Październik 2013 r.].

[10] Netcraft : October 2015 Web Server Survey - Web server developers: Market share of active sites, http://news.netcraft.com/archives/2015/10/16/october-2015-web-server-survey.html [dostep: 16 Listopad 2015 r.].

[11] Neustar : April 2015 Neustar DDoS attacks & protection report : North America –, https://nscdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2015-us-ddos-report.pdf [dostep: Kwiecień 2015 r.].

[12] Poongothai M., Sathyakala M.: Simulation and Analysis of DDoS Attacks, International Conference on Emerging Trends in Science, Engineering and Technology.

[13] Radware: DDoS Survival Handbook - The Ultimate Guide to Everything You Need To Know About DDoS Attacks, https://security.radware.com/uploadedFiles/Resources_and_Content/DDoS_Handbook/DDoS_Handbook.pdf

[14] Seymour G.: Which Web Server: IIS vs. Apache, http://www.hostway.com/blog/which-web-server-iis-vs-apache/ [dostep: 24 Wrzesień 2013 r.].

[15] Shekyan S.: Security Labs - How to Protect Against Slow HTTP Attacks, https://blog.qualys.com/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks [dostep: Listopad 2011 r.].
[16] Stallings W.: Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Wydawnictwo Helion, Gliwice 2012.
[17] Zargar S.T., Joshi J.,Tipper D. : A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE communications surveys & tutorials.

VULNERABILITY ANALYSIS OF WEB SERVERS IN REFERENCE TO DENIAL-OF-SERVICE ATTACKS

S u m m a r y

The article is addressed primarily to those involved in the security of web servers. The work begins with the presentation of statistical treatment of the problem, which are DDoS attacks. The authors emphasize the problems of server protection against rapidly-evolving attacks denial of service. The study analyzed the resistance of the basic configuration for today's most popular web server. For the study, we have developed a virtual test environment, where the research was carried out vulnerability of selected sites. The aim of this analysis is to identify and discuss the fundamental vulnerability of Apache and IIS. For each of the Web servers authors have implemented the basic mechanisms of protection. The article is addressed to people involved in the analysis and the security of web servers.

Keywords: DDoS, security, protect, the vulnerability of web servers, Apache, IIS.

DOI: 10.7862/re.2016.8

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