Studia i Materiały Informatyki Stosowanej, Tom 7, Nr 18, 2015
str. 11-14

PRZYKŁADOWE NARZĘDZIE DO ATAKÓW DDOS

Katarzyna Rekosz, Izabela Świerczyńska, Agnieszka Zys
Uniwersytet Kazimierza Wielkiego
Wydział Matematyki, Fizyki i Techniki
Studentki III roku IB
ul. Chodkiewicza 30, 85-064 Bydgoszcz
e-mail: katkat7171@gmail.com
z_izuh90@wp.pl
a.zys@onet.pl

Streszczenie: *W artykule została przedstawiona problematyka dotycząca przykładowego narzędzia do ataku DDoS. Ataki DDoS stanowią rozproszoną wersję ataku Dos. Niniejsza publikacja opisuje specyfikę oraz etapy przeprowadzenia ataku DDoS. Szczegółowo zaprezentowane zostały dwie metody ataku DDoS tj. przy użyciu narzędzia Trinoo oraz Tribe Flood Network.*

Słowa klucze: *Narzędzie, atak DDoS*

EXAMPLES OF TOOLS FOR DDOS ATTACKS

Abstract: *This article presents issues concerning the exemplary tool for DDoS attack . DDoS attacks are a distributed version of the Dos attack . This publication describes the specifics and the stages of carrying out a DDoS attack. Two methods were presented in detail of DDoS attack using a tool Trinoo and Tribe Flood Network.*

Keywords*: Tool, DDoS attack*

1. WSTĘP

Wraz z rozwijającym się postępem technologicznym oraz narastającymi konfliktami na całym świecie coraz częściej można zaobserwować w cyberprzestrzeni próby ataków. Celem ich nie są wyłącznie duże korporacje, ale także pojedyncze osoby. Udana próba zaatakowania serwera przez cyberprzestępcę może nieść za sobą ogromne konsekwencje tzn., spowodować brak dostępu do stron, działanie systemu na skutek czego doprowadzić, to może także do ogromnych strat finansowych. Pomimo podejmowania działań w celu ograniczenia ataków, cyberprzestępcy wymyślają coraz, to nowsze ich wersje oraz stosowane metody.

2. DDOS

DDos, czyli Distributed Denial of Service jest rozproszoną wersją ataku DoS. W przypadku DoS atak dokonywany jest z ograniczonej liczby urządzeń, a najczęściej wykorzystuje się do tego jedno urządzenie, tak natomiast przy ataku DDoS ofiarę zalewają setki jak nie tysiące urządzeń jednocześnie. Ofiarami tego typu ataku są pojedyncze cele, których źródłem są kontrolowane przez crackerów urządzenia wykorzystujący złośliwe oprogramowanie. Na skutego tego, iż obecnie występują ataki o charakterze rozproszonym DoS zaczyna być traktowany jako synonim DDoSu [1].

Każdy przeprowadzany atak typu DDoS polega „na skutecznym uniemożliwieniu korzystania z usług świadczonych przez zaatakowany system przez zajęcie wszystkich zasobów bądź całej przepustowości sieci” [6].Do tego typu ataków wykorzystuje się mechanizmy, które uniemożliwiają wykrycie napastnika. Przykładem

takiego mechanizmu jest fałszowanie adresu źródłowego IP, dzięki czemu możliwe jest ukrycie miejsca, z którego atak został przeprowadzony [4].Ataki DDoS składają się z dwóch faz i przeprowadzane są zdalnie. Wyróżnia się 2 fazy:

1. Zgromadzenie komputerów.
2. Generowanie pakietów.

W pierwszej fazie, aby atak był skuteczny zadaniem atakującego jest zdobycie uprawnień administratora dużej ilości komputerów, przez co pozyskiwane w taki sposób komputery stanowią tak zwaną „sieć DDoS" [2]. Jest to bardzo istotna faza, ponieważ w przypadku kiedy atakujący nie zdobędzie odpowiedniej liczby komputerów będzie zmuszony do pozyskania dostępu do innych hostów, aby móc zainstalować na nich programy zwane demonami (narzędzia, gdzie jedne są serwerami, a inne pracują jako klienci). Zdobycie hostów oraz umieszczenie na nich narzędzi jest niezbędne do zbudowania następnych elementów sieciDDoS, czyli:

- Eksploitów, służących do pozyskania praw administratora, ułatwiając w ten sposób proces włamania.
- Skanerów, które skanują porty i pozwalają na szukanie kolejnych ofiar.
- Rootkitsów, pozwalają na ukrycie przed administratorem włamania do systemu.
- Snifferów, służą do szukania nowych ofiar wykorzystując do tego podsłuch oraz przechwytywanie określonych informacji.
- Autorooterów, program tworzący sieć DDoS, do którego zalicza się konia trojańskiego.

Druga faza składa się już z właściwego ataku DDoS. Polega ona na tym, iż osoba przeprowadza atak za pomocą sieci komputerów, w efekcie czego doprowadza do wygenerowania dużego strumienia pakietów, które skierowane są na wybraną ofiarę z wielu różnych miejsc naraz. Opisując topologię sieci DDoS może ona posiadać:

- Architekturę dwustopniową, czyli atakujący oraz domena;
- Architekturę trójstopniową, czyli atakujący, węzły oraz domena.

W przypadku topologii składa się ona z takich elementów jak:

- Komputera atakującego, czyli z tego komputera, z którego zostaje wydawany rozkaz rozpoczynający atak.
- Komputerów master (węzłów), czyli komputery kontrolujące komputery demony oraz wydające polecenie ataku z komputera atakującego, a także przekazują informacje dotyczącą zastosowania odpowiedniego typu ataku.
- Komputerów demonów, których zadaniem jest odbieranie jak i wysyłanie poleceń od komputerów master. Do ich funkcji należy generowanie strumieni pakietów.
- Ofiary, którą może być cała sieć bądź jeden pojedynczy komputer.

Atak DDoS jest przeważnie zwiększeniem siły ataku DoS [2, 5, 6].

3. NARZĘDZIE DO ATAKÓW DDOS

Ataki DDoS charakteryzują się tym, że wtargnięcie do komputera ofiary odbywa się z różnych źródeł. Haker wykorzystując specjalne oprogramowanie zarządza zainfekowanymi komputerami i za ich pośrednictwem dokonuje ataków. Właściciele komputerów ,,zombie" (bo tak właśnie można je nazwać) nie wiedzą, że biorą udział w ataku, co sprawia, że obrona przed atakami jest niezwykle trudna[2].
Do realizacji ataków DDoS wykorzystuje się dwa podstawowe typy metod. Jedna z nich polega na zalewaniu (flood) pakietami danych urządzenie ofiary, natomiast druga na preparowaniu pakietów.

Do najpopularniejszych ataków DDoS należą m.in. [8].:

- Trinoo,
- TribeFlood Network.
- Stacheldtaht,
- TFN 2000,
- Shaft,
- Mstream.

Pionierskim atakiem DDoS jest Trinoo. Bazując na jego założeniach, powstały ww. metody. Trinoo charakteryzuje się trójstopniową architekturą ataku. Elementy jego oprogramowania są instalowane na urządzeniach posiadających następujące systemy: Linux, Solaris, Windows. Osoba przeprowadzająca atak, wykorzystuje wysokie porty TCP oraz UDP, aby wysyłać komendy do komputerów biorących udział w ataku. Łączność między hakerem a węzłami zachodzi na porcie 27665 TCP, natomiast węzły przesyłają rozkazy domenom poprzez port 27444 UDP. Domeny odpowiadają węzłom na innym porcie (31335 UDP).

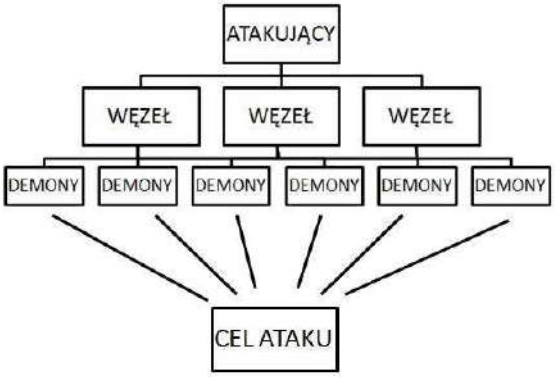
Schemat ataku:

1. Aby dokonać ataku, haker kontaktuje się z węzłem (master) i wysyła polecenie ataku na jeden lub kilka

adresów IP. Agresor może zabezpieczyć połączenia (attacker-to-master(s) oraz master-to-daemon(s))hasłem, które uniemożliwi dostęp do sieci Trinoo innym hakerom.

2. Uaktywnione demony sygnalizują swoją gotowość do przeprowadzenia ataku, poprzez wysłanie komunikatu ,,hello" zawartego w pakiecie UDP do węzłów.
Program demona archiwizuje listę adresów IP, natomiast węzły przechowują spis dostępnych demonów. Plik z katalogiem adresów IP demonów jest zaszyfrowany oraz posiada charakterystyczną nazwę (...).

3. Węzły uzyskując rozkaz od hakera, wysyłają komunikat do demonów, w którym znajdują się szczegóły dotyczące przeprowadzenia ataku. Na tym etapie osoba atakująca nie bierze już czynnego udziału w ataku, ponieważ połączenie między nią, a węzłami nie jest konieczne. Dalsza komunikacja przebiega między masterami i demonami.



Rysunek 1 Schemat trójstopniowej sieci DDoS
Źródło: opracowanie własne

Atak TribeFlood Network charakteryzuje się architekturą dwustopniową, która dostępna jest jedynie w systemie Unix. W tej metodzie haker może ulokować klientów na kilku komputerach, przez co schemat przypomina architekturę trójstopniową. W dalszych etapach atak ten działa na tych samych postulatach jak w przypadku ataku Trinoo. Różnicą między atakami jest metoda komunikacji między klientem, a demonami. Polega ona na tym, że w przypadku TribeFlood Network używane są pakiety ICMP echoreply. Połączenie między osobą atakującą, a klientem nie jest chronione jak w przypadku ataku Trinoo. Lista demonów jest archiwizowana przez każdego klienta. W kluczowej fazie ataku klient wysyła informację w postaci pakietu ICMP echoreply do demona. Komunikat ten składa się z 16-sto bitowej wartości znajdującej się w polu ID oraz argumentów umieszczonych w fragmencie pakietu przeznaczonego na dane. Wytyczne nadawane między klientami, a demonami reprezentowane są przez wartości w polu ID.

4. PODSUMOWANIE I WNIOSKI

W niniejszym artykule zostało wyjaśnione czym jest atak DDoS, a także przedstawione zostały stosowane metody tych ataków.Chcąc przeprowadzić skuteczny atak tego typu atakujący zmuszony jest do przejmowania kontroli nad ogromną liczbą komputerów w Internecie. Dzięki temu jak można zauważyć uzyskuje się w ten sposób rozproszenie między różnymi sieciami, co pozwala na trudniejsze wykrycie miejsca oraz osoby atakującej. Ze względu na różnorodne powody przeprowadzenia ataków oraz pomimo ich rzadkości występowania, należy pamiętać o tym, iż są to mimo wszystko zmasowane ataki trwające kilka godzin bądź dni. Zatem powinno się pamiętać o wykorzystywaniu oraz stosowaniu odpowiedniej ochrony serwerów, ponieważ atak typu DDoS może stanowić poważne zagrożenie dla bezpieczeństwa przedsiębiorstw. „Kamieniami milowymi w obszarze bezpieczeństwa transmisji danych są: zbudowanie sieci komputerowych, wprowadzenie do sieci struktury internetowej, rozpowszechnienie systemów antywirusowych i antyspamowych, wdrożenie technologii firewall, a wreszcie wyrafinowane metody zabezpieczania transmisji danych pomiędzy sieciami, takie jak IDS oraz IPS” [7].
Należy pamiętać jednak, że ataki DDoS są wciąż doskonalone i w przyszłości mogą się okazać bardziej wyrafinowane i groźne [8].

Literatura

1. Freedman A., Encyklopedia komputerów, Helion, 2004
2. Harley D., Slade R., GattikerUrs E., Wirusy cała prawda: rozum i powstrzymaj szkodliwe oprogramowanie, Translator, Warszawa 2003
3. Kołodziejczyk M., Nieinwazyjne metody oceny i poprawy bezpieczeństwa systemów komputerowych bazujących na standardzie disa, Tom 2 Nr2 2010
4. Polesek R., Hakin9: Ataki DDoS jak wykrywać, jak się bronić, nr 5/2004
5. Rzecki K., L. Siwik, Bezpieczeństwo w systemach komputerowych, Kraków 2001
6. Szmit M., Gusta M., Tomaszewski M., 101 zabezpieczeń przed atakami w sieci komputerowej: Metody obrony przed atakami Dos i DDoS, Helion, Gliwice 2005

7. Wrzesień M., Ł. Olejnik, P. Ryszawa, IDS/IPS: System wykrywania i zapobiegania włamaniom do sieci komputerowych, Tom 4 Nr7 2012
8. www.obfusc.at/ed/ddos_pl.html, data odczytu 29.04.2016r.