Studia i Materiały Informatyki Stosowanej, Tom 7, Nr 18, 2015
str. 7-10

ATAKI Z WYKRZYSTANIEM SERWERA DNS (DOMAIN NAME SYSTEM)

Antkowiak Magdalena, Engler Maria, Kośmider Magdalena

Uniwersytet Kazimierza Wielkiego w Bydgoszczy
Instytut Techniki

Streszczenie: *Serwery DNS (Domain Name System) to pewnego rodzaju książka telefoniczna Internetu. Bez nich nie byłoby możliwe wywołanie żadnej strony internetowej, nasz komputer nie widziałby, jak przyporządkować adres internetowy konkretnemu serwerowi. Obecnie hakerzy potrafią uzyskać dostęp do serwerów DNS, a następnie przekierować przepływ informacji na własne komputery. Ataki z wykorzystaniem serwera DNS są bardzo niebezpieczne, głównym celem jest wyszpiegowanie poufnych informacji, takich jak: hasła czy kody PIN umożliwiających dostęp do internetowych banków. W niniejszym artykule zostaną przedstawione zagrożenia usługi DNS..*

Słowa kluczowe: *zagrożenia bezpieczeństwa, ataki, DNS*

ATTACKS WITH THE USE OF DNS SERVERS (Domain Name System)

Abstarct: *DNS Servers are kind of the internet's phone book. Without DNS, there wouldn't be possible to open a website and our computer wouldn't know how to assign an internet address to a particular server. Currently, hackers are able to get an access to DNS servers and then transfer the information to their computers. The attacks with the use of DNS servers are very dangerous, as the main purpose of them is to spy sensitive information, such as passwords or PINs which allow the access to the online banks. In this article, there will be presented the danger of DNS service.*

Keywords: *security threats, attacks, DNS*

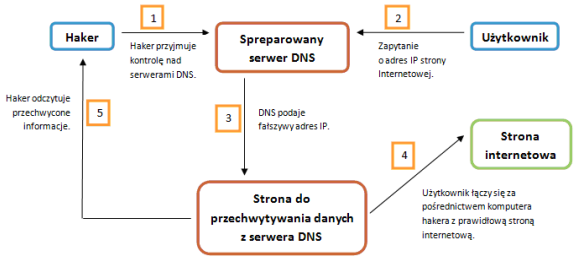
DNS jest złożonym systemem komputerowym oraz prawnym. Bezpieczeństwo systemu DNS podczas opracowania specyfikacji nie było brane pod uwagę. Od roku 1990 zaczęto odkrywać pierwsze problemy z protokołem DNS oraz luki w systemie. Informacje o zagrożeniach opublikowano w RFC 3833. W celu przeciwdziałaniu zagrożeniom czy niedoskonałościom rozszerzeń w wydanym dokumencie zwrócono uwagę na zastosowanie DNSSC i TSIG. DNSSC ma na celu zapewnienie autoryzacji źródeł danych za pomocą kryptografii asymetrycznej oraz podpisów cyfrowych. TSIG jest natomiast mechanizmem zabezpieczenia kryptograficznego transakcji transferu stref.

Podstawowe niebezpieczeństwo to możliwość przechwytywania komunikatów DNS między serwerem a klientem. Wówczas mogą wystąpić ataki typu np. man-in-the-middle polegające na pośredniczeniu komputera atakującego w wymianie treści pomiędzy serwerem a klientem. Podszycie się pod IP Spoofing umożliwi przechwycenie danych podczas ataku. Pozyskanie zapytania kierowanego do serwera przez napastnika umożliwi w łatwy sposób wygenerować i wysłać sfałszowaną odpowiedź.

Napastnik może w łatwy sposób generować spreparowane komunikaty, tak że klient interpretuje odpowiedź jako prawdziwą i zaczyna korzystać ze sfałszowanych danych, tzn. niezgodnych z rzeczywistością, „podstawionych” przez agresora.

Tak jak zostało wspomniane na początku artykułu protokół DNS zawiera w sobie luki, które może spowodować zagrożenie funkcjonowania systemu. Możliwość zatruwania pamięci podręcznej w celu zdezorganizowania funkcjonowania usługi DNS jest jednym z takich niebezpieczeństw. Innym rodzajem ataku może być podszycie się pod serwer wybranej domeny, który umożliwi częściową lub całkowitą kontrolę. Zagrożenia wynikające z niewłaściwej implementacji czy

wynikające z luk w platformie systemowej, na której posadowiono serwer DNS również przyczynią się do spowodowania strat [1].



Rysunek.1. Anatomia ataku z wykorzystaniem DNS – opracowanie własne.

2.ATAKI

2.1. Ataki typu odmowa usługi

Ataki typu odmowa usługi (DoS) zmierzają do utraty korzystania z danej usługi. Zablokowanie IP komputera, z którego kierowany jest atak jest formą ochrony przed nim. Ataki te mogą być kierowane z jednego komputera, zaś kierowane z kilku komputerów naraz jest nowszą rozproszoną opcją ataku DoS czyli DDoS.
W wypadku ataku DDoS komputery użyte do natarcia są rozproszone w sieci i ich posiadacze nie wiedzą, że uczestniczą w ataku.
Przeprowadzenie ataku jest z danego komputera jest możliwe po zainstalowaniu na nim specjalnego programu np.: koń trojański. Obrona przed atakami typu DDoS jest praktycznie niemożliwa.
Przesyłanie dużej ilości danych bądź zapytań do serwera, mających na celu obciążenie go w pełni nazywamy atakami typu flood. Taki atak przyczynia się do zakłócania korzystania z usługi lub też całkowitego jej zablokowania.

2.2. Zatruwanie pamięci podręcznej

Proces ten polega na umieszczaniu do klienta DNS bądź do pamięci podręcznej sztucznego rekordu zasobu. Zadaniem tego rekordu jest wiązać nazwę z nieprawdziwym adresem IP. Jego treść zostaje zachowana w pamięci przez dany czas zdefiniowany przez parametr TTL. Zadanie atakującego jest bardzo trudne, gdyż musi on odgadnąć identyfikator transakcji, który później umieszcza w wysłanej, fałszywej odpowiedzi. Typy ataku zatruwania bufora dzielimy na:

* Atak dnia narodzin,

* Atak klasyczny,

* Zmodyfikowany atak klasyczny.

Atak dnia narodzin powiązany jest z odpowiedzią na pytanie: „ile osób należy wybrać, żeby prawdopodobieństwo tego, że co najmniej dwie osoby mają urodziny tego samego dnia, było większe od 12”. Jeśli chodzi o ataki trzeba odpowiedzieć na pytanie: „ile należy wysłać fałszywych odpowiedzi, aby przynajmniej jedno zapytanie i jedna odpowiedź miały ten sam numer identyfikacyjny” [2]. Skrupulatne badanie numerów transakcji wyświetlanych przez serwer mogą uprościć napastnikowi zadanie. Przypadkowe generowanie numerów jest największą przeszkodą dla agresora.

Atak klasyczny bazuje na przesłaniu przez agresora pytania o nazwę do serwera DNS i naciskaniu go do szukania rozwiązania u innych serwerów DNS. Kolejnym zadaniem atakującego jest dostarczenie odpowiedzi z prawidłowym numerem transakcji. Wiedząc, że numer ID stworzony jest z 16 bitów, agresor jest zmuszony do wysłania od 1 do 65535 błędnych odpowiedzi przez czas krótszy niż czas, w którym odpowiada odpowiedni serwer DNS.

Przesłanie na każdorazowe pytanie do serwera DNS pewnego szyku odpowiedzi nazywamy zmodyfikowanym atakiem klasycznym. Rozwiązania tworzone są przez pętle z przypadkowo tworzonymi numerami ID. Istotne jest, żeby przy każdym pokonaniu pętli, numery IP były takie same. W tej sytuacji użycie błędnych odpowiedzi jest mniejsze niż przy zwykłym ataku klasycznym.

2.3. Dynamiczna aktualizacja

Szansa szybkiego umieszczania danych w serwerze jest uproszczeniem jakie proponuje nam serwer DNS. Dana czynność ma zastosowanie między innymi w sieciach lokalnych, w których urządzenia nie mają nadanego niezmiennego numeru IP. W trakcie włączenia, system operacyjny aktualizuje poprawny rekord w serwerze DNS. Jeśli napotka się na błąd autoryzacji klienta może

skutkować wprowadzaniem jakichkolwiek sfałszowanych danych do bazy serwera.

2.4. Przepełnienie bufora

Przekształcenie bufora pamięci przypisanego do odpalonej aplikacji nazywamy przepełnieniem bufora (z ang. Buffet overflow). Daną operację można uzyskać spisując do bufora aktywnej aplikacji pewnej ilości danych, tak aby wystąpiło zapełnienie i nadpisanie miejsca w pamięci za buforem. Istnieje również opcja przebudowania bufora w taki sposób, by adres powrotu zalecał procedurę, która włączy dany program. Takie błędy przypisuje się do specjalnych cech konkretnych implementacji. [3]

3.PROTOKÓŁ DNSSEC

DNSSEC jest odpowiednikiem DNS, najważniejsze podczas jego projektowania było bezpieczeństwo użytkowników. Podczas mapowania adresów wykorzystywana jest baza klucza publicznego serwerów i właściwe certyfikaty potwierdzające oryginalność informacji zwrotnych.
Od grudnia 2011 roku do czerwca 2012 roku trwało produkcyjne wdrażanie DNSSEC, co umożliwiło użytkownikom przekazywanie rekordów DS zabezpieczonych domen.
DNSSEC pozwala na ochronę realności odpowiedzi DNS. Odpowiedź na zapytanie wraca do użytkownika z kluczem, który utrzymuje, że odesłany adres IP jest właściwy bądź nie. Abonent jest pewien, że korzysta z bezpiecznej strony, kiedy dostaje IP akceptowane przez DNSSEC.
Protokół DNSSEC dba o bezpieczeństwo internautów oraz instytucji, które funkcjonują w Internecie, m.in. banków, urzędów i firm. Użytkownicy Internetu mogą dowiedzieć się dzięki niemu czy korzystają z bezpiecznej strony, a różne instytucje dzięki temu dbają o swoją renomę oraz bezpieczeństwo klientów i świadczonych dla nich usług.
Uwierzytelnianie informacji otrzymanych protokołem DNS polega na tzw. ,,łańcuchu zaufania", wymaga to właściwego podpisania danych poziomów stref domen zgodnie ze strukturą DNS.

Aby zabezpieczyć nazwę domeny trzeba podpisać strefę oraz wpisać unikatowy kryptograficzny skrót z publicznej części klucza podpisującego do strefy domeny nadrzędnej w DNS, gdzie nazwa domeny podlegającej zabezpieczeniu została zarejestrowana. W tym miejscu skrót należy podpisać kluczem prywatnym, a jego skrót przekazać do strefy nadrzędnej. Łańcuch zaufania budowany jest do najwyższego poziomu w DNS, gdzie jest klucz tzw. ,,Trust Anchor", który uznaje się za zaufany.

4. PODPISY TSIG

DNSSEC pozwala na wprowadzanie usług uwierzytelniania i nienaruszalności, jest on oparty o podpisy cyfrowe oraz korzysta z mechanizmów kryptograficznych opartych na kluczach publicznych. W miejscach gdzie używanie DNSSEC może być kłopotem lub być nawet niemożliwe, stosuje się rekordy TSIG.

TSIG pozwala m.in. na:

- bezpieczną komunikację pomiędzy stub-resolwerem, a serwerem cache'ującym,
- autoryzowanie szybkich update'ów,
- zabezpieczanie poruszania całych stref,
- zabezpieczanie porozumiewania się między klientem a lokalnym serwerem.

Rekord TSIG powiązany jest z tzw. łańcuchem żądania-odpowiedzi DNS. Wartości rekordu TSIG wyznacza się zaraz po sporządzeniu właściwej wiadomości DNS. Obliczany skrót zawiera całą wiadomość oraz część rekordu TSIG, która obejmuje między innymi dane o czasie utworzenia skrótu. Obliczony skrót to jedno z pól rekordu TSIG. Pełen rekord jest lokalizowany w sekcji dodatkowych danych wiadomości DNS, a nagłówek informacji jest modyfikowany. Gdyby wiadomość przekraczała dozwoloną wielkość to serwer skonstruuje ją tak, aby obejmowała tylko zapytanie klienta i rekord TSIG i miała należytą flagę.

Użytkownik, który dostał taką odpowiedź powinien znowu zadać zapytanie używając TCP.

Natychmiast po otrzymaniu wiadomości TSIG jest dublowany w odpowiednio zabezpieczone miejsce i usuwany z DNS. Z takiej wiadomości obliczany jest skrót i porównywany jest z tym, który został odebrany w rekordzie TSIG.

Jeżeli skróty nie są jednakowe, wiadomość zostaje porzucona, a nadawca otrzymuje informację o problemie. Możliwe jest pojawienie się błędów, które jest związane z nie rozpoznaniem klucza, wtedy serwer wysyła informację o błędzie i go zapisuje.

Poziom bezpieczeństwa zależny jest między innymi od zabezpieczenia kluczy do podpisywania wiadomości DNS. Są one bardzo ważnym elementem systemu i muszą być zabezpieczone przy wykorzystaniu wszelkich udostępnionych do tego środków. [4]

5.PODSUMOWANIE I WNIOSKI

Artykuł ten opisuje rodzaje ataków wykorzystujące usługi DNS. Można zauważyć, że niektóre ataki są bardzo proste do zrealizowania. Łatwość w wykonaniu takiej odmiany ataku spowodowana jest niedopatrzeniami w budowie programowej serwerów DNS. Występujące luki w systemie DNS trzeba wypełnić przemyślanymi rozwiązaniami. Istnieje wiele form obrony przed nimi ale nie zawsze są skuteczne, a nawet jeśli są skuteczne to nie zawsze są wykorzystywane.

Literatura

1. Borzym, M., & Suski, Z. (2008). Zagrożenia usługi DNS. Biuletyn Instytutu Automatyki i Robotyki, 14, 3-6.

2. Suski, Z. (2011). Wybrane aspekty bezpieczeństwa DNS. Biuletyn Wojskowej Akademii Technicznej, 60(4), 281-302.

3. Borzym, M., & Suski, Z. (2008). Zagrożenia usługi DNS. Biuletyn Instytutu Automatyki i Robotyki, 14, 3-23

4. https://www.dns.pl