Zagrożenia usługi DNS

Marek BORZYM, Zbigniew SUSKI

Instytut Teleinformatyki i Automatyki WAT ul. Gen. S. Kaliskiego 2, 00-908 Warszawa,
Wyższa Szkoła Technik Informatycznych ul. Pawia 55, 01-030 Warszawa

STRESZCZENIE: W artykule opisano zagrożenia związane z funkcjonowaniem usługi DNS. Jest to pierwszy z cyklu artykułów dotyczących bezpieczeństwa usługi DNS. Ma on charakter przeglądowy. Przedstawiono w nim usystematyzowany wykaz zagrożeń dotyczących bezpieczeństwa usługi DNS oraz podano charakterystyki tych zagrożeń. Informacje na taki temat można znaleźć w wielu publikacjach ale mają one zwykle charakter szczątkowy i nieusystematyzowany. W przyszłych publikacjach planowane jest przedstawienie wyników badań eksperymentalnych różnych implementacji serwerów DNS oraz sposoby przeciwdziałania zagrożeniom.

SŁOWA KLUCZOWE: testy penetracyjne, zagrożenia bezpieczeństwa, DNS

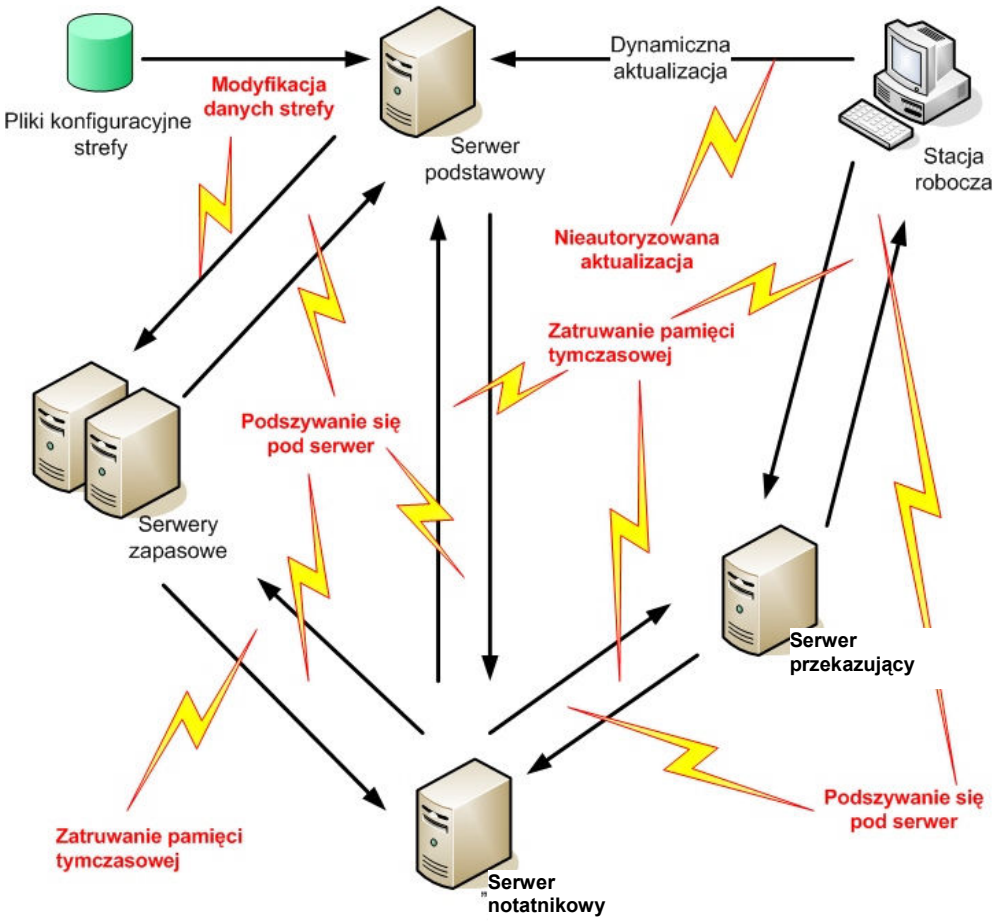
1. Wstęp

Podczas opracowywania specyfikacji systemu DNS bezpieczeństwo systemu nie było brane pod uwagę. Pierwszy problem z protokołem DNS wykryto w roku 1990. Z czasem odkrywano kolejne luki w systemie. Wreszcie informacje o zagrożeniach opublikowano w RFC 3833. W dokumencie tym zwrócono również uwagę na zastosowanie DNSSEC[1] i TSIG[2] w celu przeciwdziałania zagrożeniom oraz na niedoskonałości tych rozszerzeń. Miejsca występowania zagrożeń w DNS przedstawiono na rys. 1.

Podstawowym zagrożeniem jest możliwość przechwytywania komunikatów DNS pomiędzy serwerem a klientem. Wykorzystywane są

[1] DNSSEC - (ang. *DNS Security Extensions*) to rozszerzenie systemu DNS mające na celu zwiększenie bezpieczeństwa DNS. DNSSEC zapewnia autoryzację źródeł danych (serwerów DNS) za pomocą kryptografii asymetrycznej oraz podpisów cyfrowych.
[2] TSIG – mechanizm zabezpieczenia kryptograficznego transakcji transferu stref.

wówczas techniki ataku niezwiązane bezpośrednio z samym protokołem DNS. Może to być np. atak typu *man-in-the-middle* polegający na pośredniczeniu komputera atakującego w wymianie informacji pomiędzy serwerem i klientem. Do przechwycenia danych wykorzystane mogą być ataki poprzez podszywanie się, np. *IP Spoofing* lub *ARP Spoofing*. Gdy napastnik pozyska zapytanie kierowane do serwera, może na tej podstawie w łatwy sposób wygenerować i wysłać sfałszowaną odpowiedź.



Rys. 1. Zagrożone atakami przepływy danych w systemie DNS.

Jedną z luk w protokole DNS jest łatwość generowania przez atakującego spreparowanych komunikatów odpowiedzi serwera, w taki sposób, że klient interpretuje odpowiedź jako prawdziwą i zaczyna korzystać ze sfałszowanych danych, tzn. niezgodnych z rzeczywistością, „podstawionych" przez

atakującego. Jedynym zabezpieczeniem komunikatu jest 16-bitowe pole danych, zawierające numer, który musi być taki sam w komunikacie zapytania i odpowiedzi. Jednak to zabezpieczenie nie jest wystarczające. Można je łatwo obejść. Ta technika ataku jest trudniejsza niż przechwytywanie komunikatów, ale może być skuteczna w sieciach rozległych a nie tylko lokalnych.

Opisane wyżej zagrożenia dotyczyły możliwości wysyłania komunikatów odpowiedzi, które ofiara będzie traktowała jako autentyczne. Innym zagrożeniem jest możliwość zatruwania pamięci tymczasowej (podręcznej) w celu zdezorganizowania funkcjonowania usługi DNS. Zagrożenie tego typu niejako utrwala skutki przeprowadzonych ataków. Wykorzystywany jest mechanizm przechowywania przez klienta informacji w pamięci podręcznej.

Kolejną luką jest możliwość podszywania się pod serwer wybranej domeny. Klient systemu DNS otrzymuje adres serwera DNS np. od swojego dostawcy Internetu lub poprzez mechanizm DHCP w sieci lokalnej. Napastnik może umieścić w sieci własny serwer usługi DNS, bez wiedzy klienta. Atakujący może uzyskać kontrolę częściową, jeśli tylko podszywa się pod serwer wybranej strefy, lub całkowitą, jeśli podszył się pod serwer przekierowujący (*forwarding server*) lub serwer pamięci tymczasowej (*caching server*). Zagrożenie wynika z braku mechanizmów identyfikujących serwer jako zaufany.

Jak można zauważyć na rys. 1, każdy element systemu jest potencjalnie zagrożony. Nie wynika to jedynie ze słabości samego protokołu. Zagrożone elementy można podzielić na dwie grupy. W skład pierwszej wchodzą autorytatywne serwery stref (podstawowe i zapasowe), czyli system przechowywania i publikowania informacji. Ewentualny napastnik może bezpośrednio na danym serwerze zmodyfikować pliki konfiguracji. Jak już poprzednio napisano, może również podszyć się pod serwer podstawowy lub zapasowy, zmodyfikować dane przekazywane serwerom zapasowym. Drugą grupą są wszystkie inne serwery pośredniczące w pozyskiwaniu informacji z systemu. Na końcu tego łańcucha jest kliencka stacja robocza lub serwer dowolnej usługi, np. poczty elektronicznej. W tym przypadku na każdym etapie przekazywania informacji, może ona zostać zmieniona przez atakującego.

Aby uporządkować zagadnienia związane z zagrożeniami wynikającymi z funkcjonowania DNS, celowe jest dokonanie klasyfikacji tych zagrożeń. Jako kryterium klasyfikacji przyjęto źródło zagrożeń. Autorzy proponują następujący podział zagrożeń:

- Zagrożenia wynikające z luk w specyfikacji protokołu (np. zatruwanie pamięci podręcznej).
- Zagrożenia wynikające z niewłaściwej konfiguracji serwerów DNS (np. transfer strefy, sprawdzanie wersji, dynamiczna aktualizacja).

- Zagrożenia wynikające z niewłaściwej implementacji (np. przepełnienie bufora).
- Zagrożenia wynikające z luk w platformie systemowej, na której posadowiono serwer DNS (np. ataki typu odmowa usługi).

2. Transfer strefy

Transfer strefy związany jest z funkcją serwerów DNS polegającą na przesyłaniu rekordów bazy danych o strefie przez serwer główny do serwerów podrzędnych. Wszelkie modyfikacje polegające na dodaniu, usunięciu czy zmianie zawartości rekordu realizowane są na serwerze głównym. Aby serwery podrzędne dysponowały aktualnymi danymi o strefie, muszą one odświeżać swoją bazę zgodnie z harmonogramem zdefiniowanym przez administratora. W tym celu serwer podrzędny wysyła co pewien czas komunikat z żądaniem przesłania rekordów strefy. Jeżeli agresor przechwyci takie dane, to uzyska dostęp do takich informacji jak nazwy komputerów w sieci, ich adresy IP i inne opisy. Rys. 2 i 3 ilustrują możliwe sposoby uzyskania informacji podczas transferu strefy. Na rys. 2 przedstawiono formę ataku „człowiek pośrodku" (*ma-in-the-middle*). W czasie tego ataku intruz przechwytuje dane wymieniane pomiędzy stronami. Na rys. 3 przedstawiono zagrożenie polegające na możliwości podszycia się intruza pod jedną ze stron, w tym przypadku pomocniczy serwer DNS.

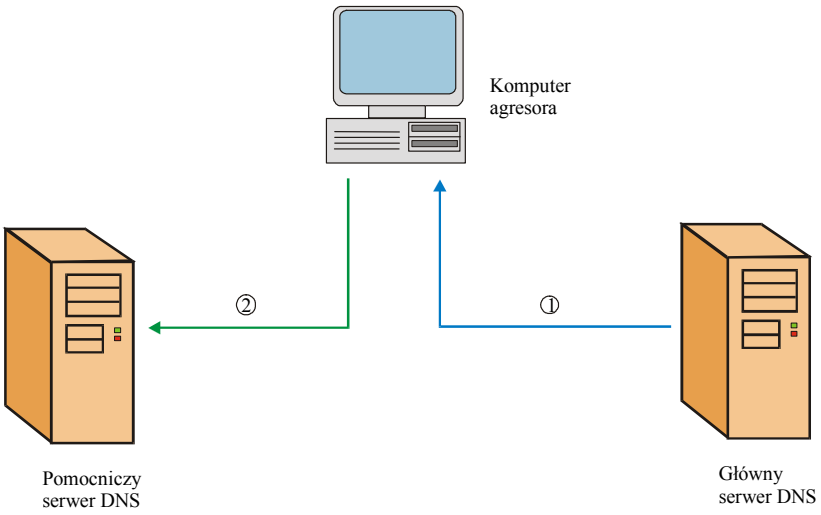
3. Sprawdzanie wersji

Sprawdzanie numeru wersji oprogramowania DNS przez agresora pomaga w ustaleniu profilu serwera. Posiadając tego typu informacje, tzn. znając konkretną wersję używanego serwera, atakujący może przygotować się do dalszego ataku, koncentrując się na słabościach tej wersji. Informacje o słabych stronach różnych wersji eksploatowanego oprogramowania można bez trudu znaleźć na wielu witrynach w Internecie.

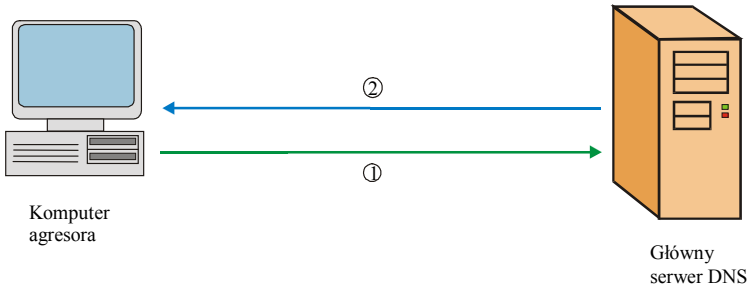
4. Ataki typu odmowa usługi

Celem ataków typu odmowa usługi (*DoS – Denial of Service*) jest całkowite lub częściowe zablokowanie możliwości korzystania z danej usługi. Podstawowe ataki DoS przeprowadzane są z jednego komputera. Uchronienie

się przed nimi jest możliwe poprzez zablokowanie adresu IP, z którego prowadzony jest atak.



Rys. 2. Przesyłanie strefy: 1) przechwycenie pliku strefy, 2) przesłanie pliku strefy do pomocniczego serwera DNS



Rys. 3. Przesyłanie strefy: 1) wysłanie żądania transferu strefy, 2) przesłanie pliku strefy do agresora

Udoskonaloną wersją ataku DoS jest atak typu rozproszonego (*DDoS - Distributed Denial of Service*). W przypadku ataku DDoS atak jest przeprowadzany z wielu komputerów jednocześnie. Komputery te znajdują się w różnych miejscach sieci, a ich użytkownicy najczęściej nie są świadomi tego, że biorą udział w przeprowadzanym ataku. Aby możliwe było wykorzystanie takiego komputera w czasie rozproszonego ataku DDoS, musi zostać na nim umieszczony odpowiedni złośliwy program. Może to być np. koń trojański, który aktywowany zostanie przez sygnał wysłany przez agresora. Ataki typu DDoS są trudniejsze do opanowania i często nawet firmy dysponujące niemal

nieograniczonymi środkami na ochronę informacji, nie są w stanie obronić się przed nimi.

Ze względu na charakter ataku DoS/DDoS, możemy rozróżnić następujące efekty działania:

- wstrzymanie usługi (*Designed Outage),*
- zniszczenie zasobów (*Resource Destruction*),
- wyczerpanie zasobów (*Resource Exhaustion*).

Rys. 4 ilustruje atak typu *flooding*. Polega on na wysyłaniu dużej ilości zapytań lub innych danych do serwera tak, aby w maksymalnym stopniu obciążyć go odbieraniem takich żądań i przygotowywaniem odpowiedzi. Atak ten może spowodować całkowite zablokowanie usługi lub przynajmniej znaczne utrudnienie korzystania z niej.

Serwery DNS mogą być podatne na ataki typu odmowa dostępu (*DoS*). Napastnik może wykorzystać w tym celu mechanizm odpytywania rekursywnego. Wysyła pojedyncze zapytania do serwera. Jeżeli odpytywany serwer nie jest w stanie udzielić odpowiedzi na podstawie posiadanych przez siebie danych, to jego reakcja polegać będzie na wysyłaniu zapytań do kolejnych serwerów autorytatywnych stref szukanej nazwy domeny. Jeśli atakujący prześle dużą ilość zapytań dotyczących domeny, o których atakowany serwer nazw nie posiada informacji w swojej pamięci podręcznej, to wykona on dużą ilość zapytań iteracyjnych.

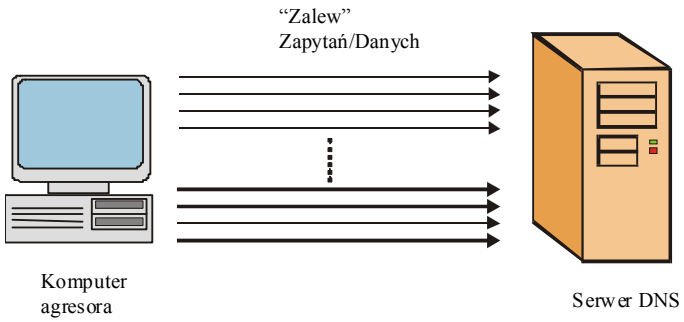
Rys. 5 ilustruje atak typu *SYN flooding*, który polega na wysyłaniu pakietów SYN na określony port. W przypadku serwera DNS będzie to port 53. W czasie tego ataku inicjowane są połączenia TCP, ale pozostają one w stanie „półotwarcia". Powoduje to przede wszystkim zużycie zasobów pamięciowych, czasu procesora i pasma medium transmisyjnego.

Serwer DNS może zostać również wykorzystany jako źródło ataku *DoS*. Ponieważ komunikat odpowiedzi może być wielokrotnie dłuższy od zapytania, więc wysłanie przez napastnika pojedynczego, krótkiego żądania może spowodować wysyłanie przez serwer długich odpowiedzi, które będą obciążały ofiarę. Udane ataki są możliwe, gdyż często serwery nazw podłączone są do szybkich łączy sieciowych, szybszych niż łącza ofiary.

5. Zatruwanie pamięci podręcznej

Zatruwanie pamięci podręcznej (*cache poisoning*) polega na wprowadzeniu do pamięci podręcznej serwera lub klienta DNS fałszywego

rekordu zasobu, który będzie wiązał nazwę z fałszywym adresem IP. Zawartość takiego rekordu będzie pamiętana przez czas określony przez parametr TTL (*Time To Live*). Gdy jakiś klient zapyta o nazwę występującą w takim rekordzie, zostanie mu zwrócony fałszywy adres IP.



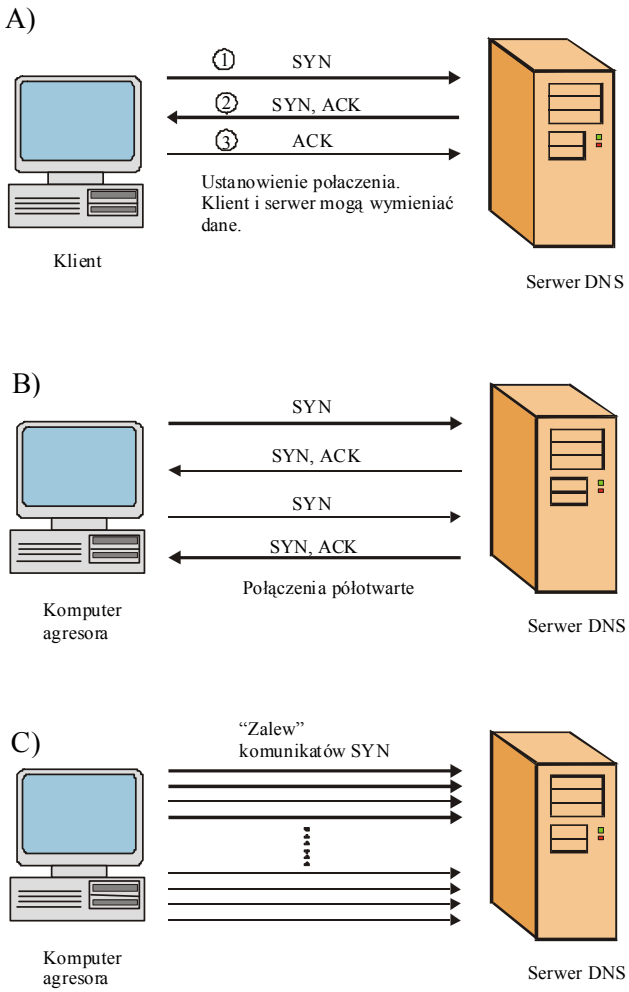
Rys. 4. Atak typu *DoS - flooding* na serwer DNS

Największa trudność po stronie agresora polega na konieczności odgadnięcia identyfikatorów transakcji, które powinien on umieścić w wysyłanej, spreparowanej odpowiedzi. Obecnie można rozróżnić następujące typy ataku zatruwania bufora:

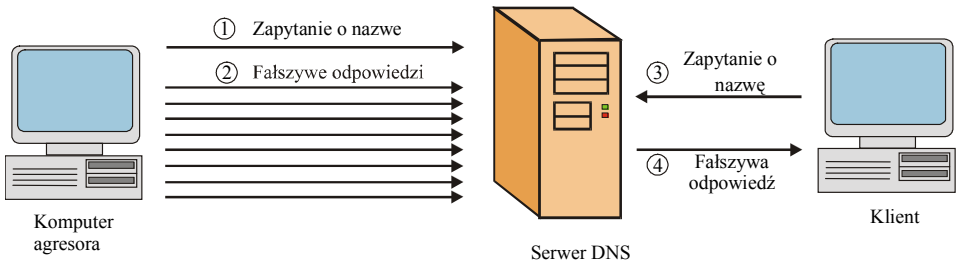
- atak klasyczny,
- zmodyfikowany atak klasyczny,
- atak dnia narodzin.

Atak klasyczny polega na wysłaniu przez atakującego zapytania o nazwę do serwera DNS i zmuszeniu go w ten sposób do poszukiwania odpowiedzi u innych serwerów DNS. Następnie agresor powinien wysłać odpowiedź z poprawnym numerem transakcji (ID). Ponieważ pole ID składa się z 16 bitów, więc wartość numeru transakcji może przyjmować wartości z przedziału od 1 do 65535. Aby atak się powiódł atakujący musi przesłać od 1 do 65535 fałszywych odpowiedzi w czasie krótszym niż czas odpowiedzi właściwego serwera DNS. Rys. 6 przedstawia ilustrację ataku klasycznego.

Zmodyfikowany atak klasyczny polega na wysyłaniu na każde zadane zapytanie do serwera DNS pewnej sekwencji odpowiedzi. Odpowiedzi są generowane w pętli z losowo generowanymi numerami ID. Ważne przy tym jest, aby przy każdym przejściu pętli były to zawsze te same numery ID. Liczba fałszywych odpowiedzi w tym przypadku jest dużo mniejsza niż 65535.



Rys. 5. Atak typu *SYN flooding* A) Prezentacja nawiązania połączenia TCP; B) Idea ataku *SYN flooding*; C) Atak *SYN flooding* na serwer DNS



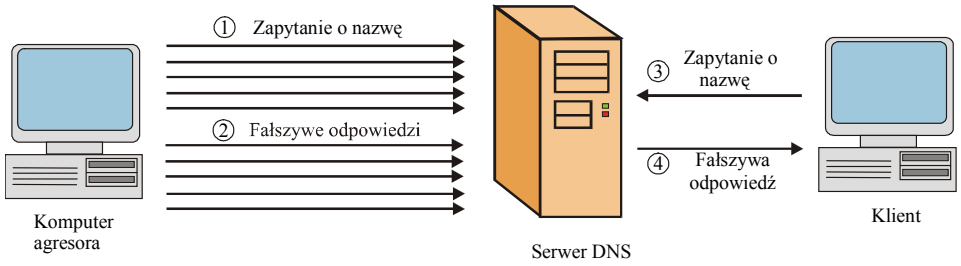
Rys. 6. Zatruwanie bufora. Atak klasyczny (opis przesyłanych elementów: 1) Agresor wysyła zapytanie o nazwę. 2) Agresor wysyła fałszywe odpowiedzi do serwera. 3) Klient zadaje pytanie o adres. 4) Serwer odpowiada fałszywym adresem IP)

Atak dnia narodzin (*birthday attack*) oparty jest na paradoksie dnia narodzin. Jest on związany z odpowiedzią na pytanie: ile osób należy wybrać, żeby prawdopodobieństwo tego, że co najmniej dwie osoby mają urodziny tego samego dnia, było większe od ½. W naszym przypadku chodzi o odpowiedź na pytanie: ile należy wysłać fałszywych odpowiedzi, aby przynajmniej jedno zapytanie i jedna odpowiedź miały ten sam numer identyfikacyjny. Prawdopodobieństwo powodzenia takiego ataku można wyrazić wzorem:

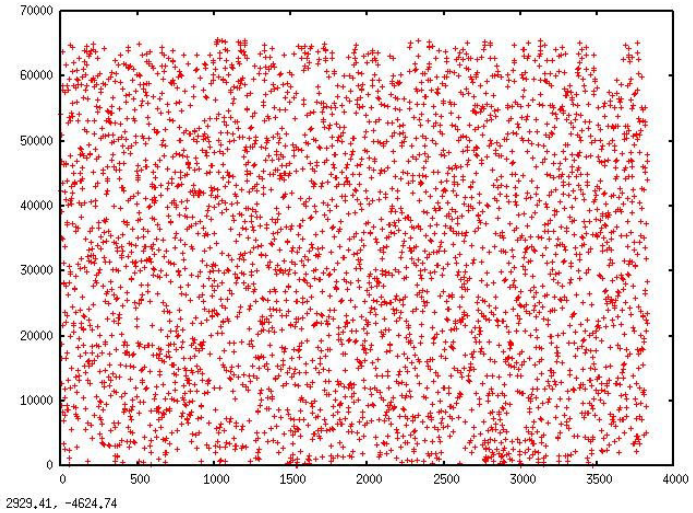
$$P = 1 - \left(1 - \frac{1}{t}\right)^{\frac{n*(n-1)}{2}}$$

gdzie t oznacza ilość wszystkich pakietów mogących być odpowiedzią, a n ilość wysłanych pakietów DNS. Z powyższego wzoru wynika, że przy 700 wysłanych pakietach zawierających fałszywą odpowiedź prawdopodobieństwo powodzenia ataku wynosi 0,97608. Jak widać znacznie ułatwia to intruzowi przeprowadzenie ataku. Na rys. 7 przedstawiono ilustrację omówionego wariantu ataku.

Agresorowi może ułatwić zadanie dokładniejsza analiza numerów transakcji generowanych przez serwer. Najtrudniejszym przypadkiem dla agresora jest losowe generowanie numerów. Na rys. 8 i 9 przedstawiono wartości tych numerów generowane przez różne serwery. Jak można zauważyć, implementacja serwera DNS w systemie Windows znacznie ułatwia zadanie agresorom.



Rys. 7. Zatruwanie bufora. Atak dnia narodzin. 1) Agresor wysyła zapytanie o nazwę. 2) Agresor wysyła fałszywe odpowiedzi do serwera. 3) Klient zadaje pytanie o adres. 4) Serwer odpowiada fałszywym adresem IP.



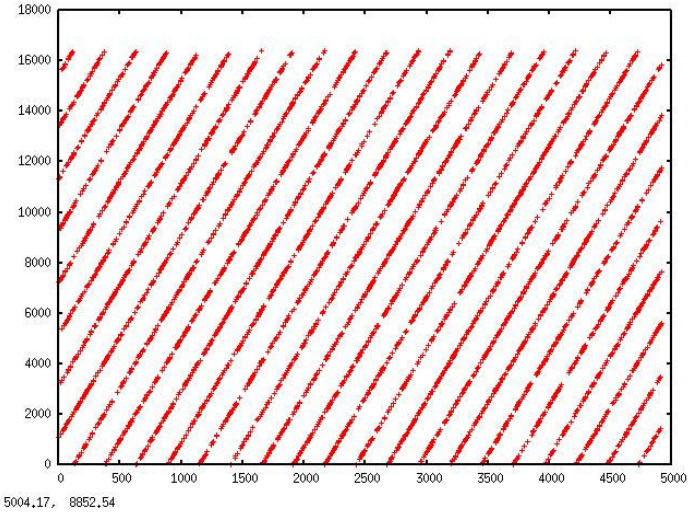
Rys. 8. Rozkład numerów transakcji generowanych przez serwer BIND

6. Przepełnienie bufora

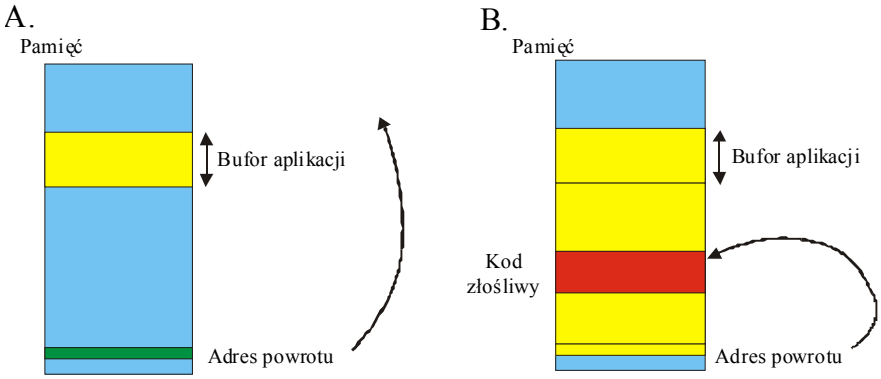
Przepełnienie bufora (*buffer overflow*) jest techniką ataku polegającą na modyfikacji bufora pamięci, jaki został przydzielony uruchomionej aplikacji. Można to osiągnąć poprzez zapisanie do bufora uruchomionej aplikacji dużej porcji danych w taki sposób, aby nastąpiło jego przepełnienie oraz nadpisanie obszaru pamięci za buforem. Posiadając odpowiednią wiedzę można zmodyfikować bufor w ten sposób, że adres powrotu wskaże na procedurę uruchamiającą wskazany program. Można w ten sposób wywołać np. program interpretera poleceń (*shell)*. Rys. 10 pokazuje ideę takiego ataku. Luki tego typu zaliczamy zwykle do szczególnych właściwości konkretnych implementacji.

7. Dynamiczna aktualizacja

Jednym z ułatwień, jakie może oferować serwer DNS jest możliwość dynamicznego wprowadzania danych do bazy serwera przez jego klientów. Funkcja ta jest np. wykorzystywana przez komputery w sieci lokalnej, które nie mają przypisanego stałego adresu IP. Podczas uruchamiania, system operacyjny stara się uaktualnić właściwy rekord w lokalnym serwerze DNS. Brak autoryzacji klienta może spowodować wprowadzenie do bazy serwera, dowolnych sfałszowanych danych.



Rys. 9. Rozkład numerów transakcji generowanych przez serwer MS DNS



Rys. 10. Przepełnienie bufora. A) Dane mieszczą się w buforze. Adres powrotu wskazuje gdzie ma powrócić aplikacja po zakończeniu działania funkcji. B) Przepełnienie bufora. Adres powrotu wskazuje na adres gdzie znajduje się złośliwy kod

8. Wybrane luki w popularnych wersjach serwerów DNS

Zamieszczenie w niniejszym opracowaniu częściowego wykazu odkrytych luk ma przede wszystkim na celu zilustrowanie różnorodności i ilości usterek występujących w popularnych implementacjach serwerów DNS. Powinno to uświadomić czytelnikowi słabości wykorzystywanego powszechnie

oprogramowania. Należy zdawać sobie sprawę, że lista takich luk jest ciągle rozszerzana. Wynika to z faktu ich stopniowego wykrywania. Na podstawie opisu każdej z luk można zbudować stosowny program (exploit) pozwalający na jej wykorzystanie. W zasobach Internetu bez większego trudu można znaleźć takie exploity. Po uzyskaniu przez napastnika wiedzy o wersji zainstalowanego oprogramowania, może on ograniczyć swoje działania do prób wykorzystania luk charakterystycznych dla danej wersji.

8.1. Wybrane luki serwerów BIND v.8.x i v.9.x

W dniu 20.07.2007 lista stwierdzonych i opisanych luk w serwerach BIND liczyła 24 pozycje [9]. Poniżej, dla zilustrowania rodzajów występujących usterek, przedstawiono niektóre z nich.

- **BIND: q_usedns** - luka pozwala na przekroczenie tablicy q_usedns, która służy do śledzenia nazw/adresów serwerów, które były odpytywane. Wynikiem przekroczenia tej tablicy może być odmowa usługi. Luka ta występuje tylko w wersji 8.4.4 i 8.4.5.
- **BIND: Multiple Denial of Service A/K/A DoS_multi** – wykorzystanie tej luki może doprowadzić do zatrzymania usługi DNS. Może to nastąpić w dwóch przypadkach:
    1. Kiedy utworzona odpowiedź zawiera odpowiedź NXDOMAIN dla odpowiedzi ENDS z dużym rozmiarem pakietu UDP.
    2. Ustawienie wartości NULL dla znacznika ważności.

  Luka występuje w wersji 8.3.0 - 8.3.3, 8.2 - 8.2.6, 8.3.0 - 8.3.3.
- **BIND: Negative Cache DOS A/K/A negcache** - wykorzystanie tej luki może doprowadzić do niedostępności określonej domeny dla zaatakowanego serwera. Po udanym ataku, odpowiedź dotycząca domeny będzie negatywna i zostanie wysyłany komunikat o niedostępności domeny dopóki nie upłynie czas TTL określający czas życia tego rekordu. Luka występuje we wszystkich wcześniejszych wersjach niż 8.4.3, 8.3.7, oprócz wersji 8.1.3, 8.2.2-P8, 8.2.4-P1, 8.2.5-P1.
- **BIND: Remote Execution of Code A/K/A sigrec** - w przypadku utworzenia odpowiedzi zawierającej źle sformatowany rekord SIG może nastąpić przepełnienie bufora. Istnieje wówczas możliwość wykonania kodu ze wskazanymi uprawnieniami oraz możliwość uzyskania dostępu do konsoli z uprawnieniami *root*, a tym samym przejęcia kontroli nad serwerem. Luka występuje w wersjach 8.1, 8.2 - 8.2.6, 8.3.0 - 8.3.3.

- **fdmax bug -** błąd ten umożliwia manipulowanie deskryptorami plików. W przypadku, kiedy zostanie zajęte więcej deskryptorów niż jest to określone przez wartość FD_SETSIZE może dojść do awarii serwera. Luka występuje w wersjach 8.1, 8.1.1, 8.1.2, 8.2, 8.2-P1.
- **infoleak** – luka umożliwia skonstruowanie odwrotnego zapytania, które pozwoli na zdalne odczytanie stosu i ujawnienie zmiennych środowiskowych. Luka występuje w wersjach 8.1, 8.1.1, 8.1.2, 8.2, 8.2-P1, 8.2.1, 8.2.2-P1, 8.2.2-P2, 8.2.2-P3, 8.2.2-P4, 8.2.2-P5, 8.2.2-P6, 8.2.2-P7.
- **libbind buffer overflow** – błąd ten umożliwia skonstruowanie odpowiedzi do zapytania DNS przekazanego przez aplikację powiązaną z podatną wersją biblioteki rdzenia *resolvera*. Taka odpowiedź może spowodować przepełnienie bufora o kilka bajtów. Ten błąd nie dotyczy samego serwera nazw, ale raczej aplikacji powiązanej z biblioteką *resolvera*. Luka występuje w wersjach 8.x wcześniejszych niż 8.2.6, 8.3.0, 8.3.1, 8.3.2.
- **maxdname bug** – w wyniku użycia funkcji *sprintf*() z danymi pobranymi z sieci komputerowej może dojść do przepełnienia bufora. Może to spowodować niespodziewane zachowanie serwera. Ze względu na umiejscowienie tego bufora, istnieje małe prawdopodobieństwo, że ten błąd może spowodować poważne konsekwencje. Nie można jednak wykluczyć możliwości spowodowania zdalnego załamania serwera. Luka występuje w wersjach 8.1, 8.1.1, 8.1.2, 8.2, 8.2-P1, 8.2.1, 8.2.2, 8.2.2-P1.
- **naptr bug** - niewłaściwa walidacja danych strefy dla rekordu NAPTR pobranych z dysku może spowodować załamanie serwera DNS. Dane strefy pobierane z sieci nie powodują uaktywnienia tej luki. Nadany poziom uprawnień do modyfikacji danych strefy jest standardowo taki sam jak dla uruchomionego serwera DNS. Wykorzystanie tego błędu przez exploit jest mało prawdopodobne dopóki pliki strefy nie mają nadanych standardowych uprawnień. Luka występuje w wersjach 8.1, 8.1.1, 8.1.2, 8.2, 8.2-P1, 8.2.1, 8.2.2, 8.2.2-P1.
- **nxt bug** – błąd ten, przy przetwarzaniu rekordów NXT, może umożliwić atakującemu uzyskanie dostępu do systemu, na którym uruchomiony jest serwer DNS. Uprawnienia, jakie wtedy uzyskuje atakujący są takie same, z jakimi został uruchomiony serwer. Luka występuje w wersjach 8.2, 8.2-P1, 8.2.1.
- **sig bug** – przy niewłaściwej walidacji zawartości rekordu SIG, błąd ten może spowodować załamanie serwera DNS ze skutkami ataku *denial of service* (*DoS*). Luka występuje w wersjach 8.1, 8.1.1, 8.2, 8.2-P1, 8.2.1.

- **sigdiv0 bug** - w trakcie weryfikacji sygnatur, niewłaściwie zaznaczony argument może spowodować błąd dzielenia przez zero. Efektem może być załamanie serwera nazw. Błąd ten występuje tylko przy oznakowanej strefie. Luka występuje w wersjach 8.2, 8.2-P1, 8.2.2-P1 – 8.2.2-P5.
- **srv bug** – przy manipulowaniu skompresowanym wskaźnikiem tabel serwer nazw może wchodzić w nieskończoną pętlę. Luka występuje w wersjach 8.2, 8.2-P1, 8.2.1, 8.2.2, 8.2.2-P1 – 8.2.2-P6.
- **solinger bug** – luka ta umożliwia zdalne spowodowanie "wstrzymania" pracy serwera przez okres do 120 sekund. Może to nastąpić w wyniku nawiązania nietypowej sesji TCP. Luka występuje w wersjach 8.1, 8.1.1, 8.1.2, 8.2, 8.2-P1, 8.2.1.
- **tsig bug** – poprzez manipulację zapytaniem oznaczonym jako TSIG (*Transaction SIGnature*) luka umożliwia przepełnienie bufora. W rezultacie można uzyskać dostęp do systemu. Luka występuje w wersjach 8.2, 8.2-P1, 8.2.1, 8.2.2-P1, 8.2.2-P2, 8.2.2-P3, 8.2.2-P4, 8.2.2-P5, 8.2.2-P6, 8.2.2-P7 oraz we wszystkich wersjach beta 8.2.3.
- **zxfr bug** – błąd w kodzie programu, który podtrzymuje transfer skompresowanego pliku strefy. Może spowodować załamanie serwera nazw. Luka występuje w wersjach 8.2.2, 8.2.2-P1 – 8.2.2-P6.
- **OpenSSL buffer overflow** – luka umożliwia wykonanie dowolnego kodu. Występuje w wersjach 9.1, 9.2 jeżeli budowany był z wykorzystaniem OpenSSL (*configure --with-openssl*).
- **BIND: Self Check Failing –** nieprawidłowe założenia w walidatorze (*authvalidated*) mogą spowodować niedostateczny test REQUIRE (wewnętrznej zawartości), co może doprowadzić do zakończenia procesu serwera. Luka występuje w wersji 9.3.0.

8.2. Wybrane luki serwerów MS DNS 2000

Prezentowaną listę opracowano w oparciu o wykaz usterek usuniętych w dodatku *Service Pack* 4 dla systemu Windows 2000 [10].

- **Program zwraca błędne dane lub błędy, jeżeli używa funkcji DnsQuery do zapytania DNS o rekordy TXT w Windows 2000 z Service Pack 4** – spowodowane to jest niewłaściwą interpretacją ciągu znaków z polem o zerowej długości przez funkcję *DnsQuery*. Funkcja ta może również spowodować uszkodzenie danych na stosie. Jeżeli wystąpi uszkodzenie danych, program ulega zawieszeniu z naruszeniem praw dostępu.

- **Naruszenie praw dostępu w Dns.exe, kiedy próbujemy używać znaków Unicode** – błąd ten wynika z faktu, że Microsoft DNS Server nie obsługuje plików stref przechowywanych w formacie *Unicode*. Kiedy próbujemy używać plików z ciągiem znaków *Unicode*, może nastąpić zatrzymanie serwera DNS.
- **Wywołanie ADsOpenObject("LDAP://RootDSE",....) generuje nieprawidłowe zapytania DNS w sieci** – błąd ten nie stanowi zagrożenia dla serwera DNS, natomiast generuje dodatkowy ruch w sieci. Kiedy wywołujemy *ADsOpenObject(„LDAP://RootDSE",...)* do serwera DNS wysyłane jest zapytanie SRV zawierające nazwy *hosta*. Zapytanie takie nie powinno być wysyłane do sieci.
- **Nie można czyścić pamięci *cache* na serwerze DNS** – przy próbie oczyszczenia pamięci podręcznej serwera DNS możemy otrzymać komunikat błędu:

  The server cache cannot be cleared. DNS zone already exists in the directory service.

  Jeżeli używamy komendy *dnscmd/clearcache* możemy otrzymać komunikat:

  failed: status = 9718 (0x000025f6).
- **Nie można uruchomić Windows 2000 z wieloma strefami DNS** – problem ten występuje, kiedy system dynamiczny jest większy niż 10.3 MB. Kiedy system Windows jest uruchamiany, rozmiar jądra systemu Windows oraz systemu dynamicznego razem musi być mniejszy niż 16 MB. Jeżeli rozmiar ten będzie większy możemy otrzymać komunikat:

  \\winnt\system32\config\system file is missing or corrupt.
- **DNS Caches Last Negative Response Returned on Multihomed Server** – problem ten może wystąpić jeżeli komputer *Multihomed* pracuje jako Microsoft Proxy Server. Błędne odpowiedzi nazw mogą być przechowywane w poniższych sytuacjach:
  1. Pierwszy interfejs na komputerze *Multihomed* zwraca odpowiedź NAME_ERROR (nazwa nie istnieje) dla odpytywanej nazwy, a czas DNS upłynął zanim nadeszła odpowiedź z drugiego interfejsu. W takim przypadku komputer błędnie przechowuje odpowiedź NAME_ERROR.
  2. Pierwszy interfejs zwrócił odpowiedź NO_RECORDS (nazwa istnieje, ale nie dla tego typu rekordu), a drugi interfejs zwrócił odpowiedź NAME_ERROR (nazwa nie istnieje). W tej sytuacji, ostatnia odpowiedź jest przechowywana, a zapytania dla innych typów rekordów dla tej nazwy nie działają.

- **DNS nie wysyła zapytań o nazwę do WINS z rekordami CNAME** – problem ten pojawia się, kiedy pozycja CNAME dla nazwy *hosta* nie posiada rekordu adresu. W takim przypadku DNS kończy odpytywanie.
- **Szukanie domeny DNS kończy się nagle na komputerze z systemem Windows 2000** – kiedy uruchamiamy przeszukiwanie na komputerze z systemem Microsoft Windows 2000, a klient DNS Windows 2000 dodaje macierzysty przyrostek głównego przyrostka DNS do poszukiwania rozwiązującego poszukiwany przyrostek domeny, przeszukiwanie może się nagle zakończyć. Problem ten występuje, kiedy jedna ze stref w liście poszukiwania przyrostka ma ustawione odrzuć zapytania.
- **Dynamiczne uaktualnianie DNS może nie działać** – problem występuje, kiedy chroniona strefa DNS zostanie przełączona na strefę niechronioną, a następnie z powrotem zostanie przełączona na strefę chronioną. Działanie takie może przypisać nieprawidłowy kontekst do ustalonych rekordów. Nieprawidłowe ustawienia ochrony rekordu nie pozwalają na dynamiczne uaktualnienia.

8.3. Wybrane luki serwerów MS DNS 2003

Prezentowaną listę opracowano w oparciu o wykaz usterek usuniętych w dodatku *Service Pack* 1 dla systemu Windows 2003 [11].

- **Zanikanie *forwardera* DNS po restarcie usługi DNS w Windows Server 2003** - kiedy należymy do grupy *DnsAdmins* i utworzymy *forwarder* DNS, po restarcie usługi serwera DNS utworzony *forwarder* zanika. Zdarzenia 2200 i 2202 są zapisywane w logu zdarzeń aplikacji. W rezultacie, rozwiązanie DNS może być błędne. Problem ten występuje, ponieważ uprawnienia zapisu w rejestrach nie są przydzielone do grupy *DnsAdmins*. Sytuacja ta nie występuje, jeżeli należymy do grupy *Administrators*.
- **Kontener MicrosoftDNS jest tworzony przed pełną replikacją i wywołuje konflikt DNS w Windows Server 2003 –** kiedy komputer oparty na systemie Windows Server 2003 zostaje kontrolerem domeny, może wystąpić konflikt w *Active Directory* na odległej replice kontenera *MicrosoftDNS*. Odległa replika kontenera *MicrosoftDNS* jest zastępowana, a nowy kontener *MicrosoftDNS* zawiera tylko strefę *RootDNSServers*. Problem ten występuje, kiedy kontener *MicrosoftDNS* jest utworzony przed pełną replikacją partycji aplikacji. Kontener *MicrosoftDNS* dla lokalnej domeny jest młodszym kontenerem. Kiedy następuje replikacja, lokalny kontener *MicrosoftDNS* zastępuje odległy

kontener *MicrosoftDNS* a wówczas zamieniana jest nazwa istniejącego odległego kontenera *MicrosoftDNS* jako obiekt konfliktu.

- **Zanikanie podrzędnej strefy po restarcie usługi DNS -** kiedy członek grupy *DnsAdmins* utworzy podrzędną strefę, strefa ta zanika po restarcie usługi. Problem ten występuje, ponieważ domyślnie uprawnienia nie są przypisane do grupy *DnsAdmins*. Problem nie występuje dla członków grupy *Administrators*.
- **Nie można prawidłowo uaktualnić rekordu TTL hosta (A) przy użyciu *MicrosoftDNS AType: Modify method in Windows Server 2003* –** kiedy próbujemy ustawić prawidłowy czas życia (TTL) adresu (A) rekordu zasobu *hosta* na zero w Microsoft Windows Server 2003 używając metody *MicrosoftDNS AType:Modify*, metoda uruchamia się bez błędu. Jednak, kiedy prawidłowo zweryfikujemy wartość TTL używając narzędzi DNS w Windows lub używając *Windows Management Instumentation* (*WMI*), wartość jest ustawiona na 3600 sekund (1 godzina).
- **Klienci nie mogą się logować do kontrolerów domeny, które są serwerami DNS opartymi o Windows Server 2003, a interfejsy sieciowe, które nie są zarejestrowane w DNS mogą wciąż wykonywać dynamiczne uaktualnienia -**po zainstalowaniu Microsoft Windows Server 2003 na kontrolerze domeny "*multihomed*" będącym serwerem DNS, klienci mogą nie być zdolni do logowania, a interfejsy sieciowe, które nie są zarejestrowane w DNS mogą wciąż wykonywać dynamiczne uaktualnienia. Problem ten występuje na kontrolerze domeny z nową (nie uaktualnioną) instalacją Windows Server 2003 i na komputerach, które były uaktualnione do Windows Server 2003 z wersji Windows 2000.
- **Klient DNS może nie mieć dostępu do stron, dla których rekord zasobu CNAME dla strony był przechowywany na serwerze DNS Windows Server 2003 –** problem ten występuje, ponieważ Windows Server 2003 DNS nie może dodać rekordów zasobów CNAME, jeżeli były one wcześniej przechowywane i wygasły. Kiedy DNS nie doda rekordu zasobu CNAME dla strony, klient DNS nie może rozwiązać adresu nazwy domeny dla strony.
- **DNS generuje błąd naruszenia dostępu w Windows Server 2003 –** DNS może generować błąd naruszenia dostępu na komputer, na którym jest uruchomiony Microsoft Windows Server 2003. Problem ten może wystąpić, kiedy DNS próbuje usunąć rekord AAAA.
- **DNS.exe powoduje wyciek pamięci, kiedy strefy są dodawane przy użyciu skryptu w Windows Server 2003 –** jeżeli strefa DNS jest

dodawana do Microsoft Windows DNS serwer przy użyciu skryptu mogą wystąpić następujące problemy:

1. Dns.exe może spowodować wyciek pamięci.
2. Dns.exe może przestać odpowiadać.
3. Tworzenie nowej strefy może zatrzymać się wcześniej niż się spodziewamy.

Problem ten może wystąpić po utworzeniu dużej ilości stref (np. kilka tysięcy).

- **W Windows Server 2003 zdarzenie ID 5501 i zdarzenie ID 6524 są zapisywane do logu, kiedy DNS żąda przyrostowego transferu strefy –** problem ten występuje, ponieważ serwer BIND wysyła transfer całej strefy zamiast przyrostowego transferu. Pełny transfer zawiera rekord SOA jako początek transferu, następnie rekordy i drugi rekord SOA na końcu strefy. Po tym jak DNS otrzyma drugi rekord SOA, DNS automatycznie przełącza się do pełnego transferu strefy. Wówczas serwer DNS wykrywa pierwszy rekord strefy jako rekord SOA. Dlatego też, DNS nieprawidłowo wykrywa złe pakiety i zgłasza błąd zły pakiet jako zdarzenie ID 5501 i zdarzenie ID 6524. DNS kończy wówczas transfer strefy.
- **Wchodząca replikacja zawodzi na kontrolerze domeny ze zdarzeniem ID: *1699, Error 8451* lub błąd odrzutu – 1601 –** problem ten występuje, jeżeli partycja *Active Directory* zawiera jeden lub więcej obiektów z nieważnym deskryptorem bezpieczeństwa. Nieważny deskryptor bezpieczeństwa jest deskryptorem bezpieczeństwa, który jest mniejszy niż 8 bajtów. Problem ten występuje, jeżeli obiekt lub atrybut zawiera *msExchSecurityDescriptor*, którego długość jest właśnie mniejsza od 8 bajtów. Kontrolery domeny oparte o Microsoft Windows 2000 wcześniejsze niż *Service Pack 4* dopuszczały występowanie takiego nieważnego deskryptora bezpieczeństwa. Windows 2000 SP4 lub późniejsza wersja nie zezwala na zapisanie *msExchSecurityDescriptors* do globalnego katalogu. Jeżeli już istnieje w globalnym katalogu, to nie jest usuwany przy instalacji Windows 2000 SP4 lub późniejszej wersji. Aktualizacja kontrolera domeny Windows 2000 do Windows Server 2003 nie poprawia nieważnego deskryptora.
- **Klienci *MIT Kerberos* nie mogą ustalić autentykacji do kontrolera domeny w domenie Windows 2000 opartego o Windows Server 2003 –** po dodaniu kontrolera domeny opartego o Microsoft Windows Server 2003 do domeny Windows 2000, możemy zauważyć, że klient *MIT* (*Massachusetts Institute of Technology*) *Kerberos* nie może zrealizować uwierzytelnienia wobec kontrolera domeny opartego o Windows Server

2003. Ten sam klient może zrealizować uwierzytelnienie zakończone sukcesem do kontrolera domeny opartego o Windows 2000. Problem ten występuje, ponieważ Windows 2000 nie implementuje w pełni numeru wersji klucza dla głównego bezpieczeństwa. Bilet, który jest tworzony przez Windows 2000 *Kerberos Key Distribution Center* (*KDC*) zawsze ma numer wersji klucza ustawiony na 1. Wartość ta nie jest zwiększana, kiedy zasada hasła jest uaktualniana. W Windows Server 2003, nowy atrybut *msDS-KeyVersionNumber* został dodany do schematu. Dlatego też to zachowanie się zmieniło. Kontroler domeny oparty o Windows Server 2003 zwiększa atrybut *msDS-KeyVersionNumber* zawsze, kiedy główne hasło ulega zmianie. Bilety, które kontroler domeny oparty o Windows Server 2003 dystrybuuje zawierają zaktualizowany ten atrybut. Problem ten występuje, kiedy wartość głównego atrybutu *msDS-KeyVersionNumber* jest większa niż jeden i główny atrybut prosi o usługę biletu kontroler domeny oparty o Windows Server 2003. Jeżeli główny plik *keytab* był utworzony na kontrolerze domeny opartym o Windows 2000, numer wersji klucza w pliku *keytab* jest 1. W tej sytuacji, numer wersji klucza w prośbie inicjacji logowania klienta nie ma zaznaczenia numeru wersji klucza w katalogu usługi *Active Directory*. Dlatego też, proces uwierzytelnienia kończy się niepowodzeniem.

- **Uprawnienia są resetowane, kiedy tworzymy nową strefę w *DNS Management Console* –** kiedy przypiszemy uprawnienia do indywidualnej strefy w *DNS Management Console* w Microsoft Windows Server, uprawnienia mogą być zresetowane, kiedy tworzymy nową strefę.
- **Problemy z rozwiązaniem nazwy i replikacją po uaktualnieniu do Windows Server 2003 -** po uaktualnieniu kontrolera domeny Microsoft Windows 2000 do Microsoft Windows Server 2003, uaktualniony kontroler domeny nie może używać korzenia lasu domen, który jest przechowywany w *Active Directory*. Jest to powodem problemów z rozwiązaniem nazw i replikacji. Ten problem może wystąpić przed zakończeniem replikacji dla uaktualnionego serwera i restartowanej usługi DNS.
- **Otrzymujemy komunikat naruszenia dostępu i usługa DNS zatrzymuje się na uruchomionym serwerze na Windows 2000 lub Windows Server 2003 –** na serwerze DNS, który jest uruchomiony na Microsoft Windows 2000 Server lub Microsoft Windows Server 2003 i który jest skonfigurowany do pobierania informacji o strefie z pliku, możemy często otrzymać komunikat o naruszeniu dostępu. Usługa DNS może zostać zatrzymana. Kiedy ten problem wystąpi, musimy zrestartować usługę DNS. Problem ten może wystąpić, jeżeli rekord

DNS TXT zawiera znaki spoza ASCII. Znaki te są zachowywane w formie oktalnej w pliku strefy.

9. Podsumowanie

W artykule zostały przedstawione podstawowe zagrożenia związane z funkcjonowaniem usługi DNS. Dla części opisanych luk występujących w najbardziej popularnych implementacjach serwerów DNS opracowano już łaty programowe. Należy jednak zdawać sobie sprawę, że opracowanie łatwy nie rozwiązuje problemu. Jest dopiero pierwszym krokiem na drodze do zbudowania bezpiecznego serwera. Taką łatę należy jeszcze zainstalować. Wydaje się to truizmem. Niestety należy o tym przypominać, gdyż większość użytkowników nie realizuje żadnych zabiegów pielęgnacyjnych w stosunku do używanego przez siebie oprogramowania. Oznacza to między innymi rezygnację z instalowania jakichkolwiek łat.

Przedstawiony artykuł jest pierwszym z cyklu planowanych, dotyczących bezpieczeństwa usługi DNS. W kolejnych artykułach zostaną przedstawione wyniki badań eksperymentalnych różnych implementacji serwerów DNS oraz sposoby przeciwdziałania zagrożeniom.

Literatura:

[1] ALBITZ P., LIU C., *DNS and BIND. Edition 4*, O'Reilly & Associates, Inc 2001.

[2] LIU C., LARSON M., ALLEN R., *DNS on Windows Server 2003. Edition 3*, O'Reilly & Associates, Inc 2003.

[3] DANIELS A., KNIEF H., GRAHAM J., ABELL R., *Windows 2000 DNS.* Helion 2001.

[4] HATCH B., LEE J., KURTZ G., *Hakerzy w Linuksie. Sekrety zabezpieczeń sieci komputerowych*, Translator 2003.

[5] BIRKHOLZ E. P., *Operacje specjalne – Bezpieczeństwo komputerów i sieci Microsoft UNIX, ORACLE*, Translator 2003.

[6] TOMASZEWSKI M., *Pharming-Ataki DNS cache poisoning*, Hakin9 nr 4/2005.

[7] BORZYM M., *Weryfikacja bezpieczeństwa serwerów DN*, – praca magisterska. Biblioteka Wojskowej Akademii Technicznej, 2006.

[8] HAŁAJKO G., *Bezpieczeństwo serwerów DNS*, – praca magisterska. Biblioteka Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych, 2007.

[9] *BIND Vulnerabilities*, Internet Systems Consortium (www.isc.org) 2007.

[10] *Lista błędów usuniętych w dodatku Service Pack 4 dla systemu Windows 2000,* (support.microsoft.com) 2006.

[11] *Lista błędów usuniętych w dodatku Service Pack 1 dla systemu Windows 2003,* (support.microsoft.com) 2007.

DNS threats

ABSTRACT: The paper presents the threats connected with DNS. Systematized list of threats and description of that threats are presented. This is the first paper from a planned series of papers concerned with DNS security.

KEYWORDS: penetrative tests, security threats, DNS.

Praca została zrealizowana w ramach projektu badawczego GD 961.

Praca wpłynęła do redakcji 20.05.2008 r.