Wybrane techniki ataków

Luki i słabości TCP / IP oraz implementacji protokołu

Wprowadzenie

- **Słabości protokołu TCP/IP**

  TCP/IP i infrastruktura implementująca protokół powstała by zapewnić komunikację w sieci - założenia projektowe nie miały charakteru militarnego

  ⇩

  Infrastruktura TCP/IP stała się łatwym łupem dla przestępców

- **Część nieuprawnionych działań dokonywanych przy użyciu narzędzi zaplanowanych jako pomoc w analizie ruchu sieci**

- **Wybrane zagadnienia ataków z wykorzystaniem TCP/IP**
  - Zbieranie informacji o ofiarach ataku - skanowanie sieci
  - Podsłuchiwanie ruchu w sieci - sniffing
  - Blokowanie komputerów - ataki DoS i DDoS
  - Podszywanie się pod zaufane komputery - IP spoofing
  - Przejmowanie sesji - session hijacking

Zbieranie informacji o obiekcie ataku

Cel - poznać ofiarę: komputery atakowanej sieci, OS, usługi

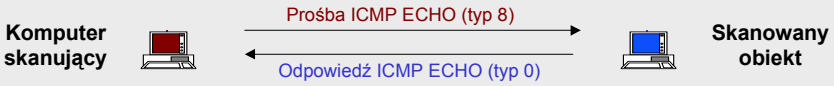
- **Tworzenie profilu ofiary (foot-printing) - wykorzystanie dostępnych informacji = przygotowania**
  - **Zakresy adresów IP, serwery poczty, serwery DNS**
  - **Dane o pracownikach, adresy poczty elektronicznej**
  - **Określanie: kont, tablic routingu, danych SNMP - (enumeration)**
- **Skanowanie sieci = wizja lokalna**
  - **Określanie komputerów dołączonych do sieci, usług, OS**

- **Techniki skanowania**
  - **Przemiatanie adresów IP (ping sweeps)**
  - **Nawiązywanie połączeń**
  - **Korzystanie z usług systemowych (luki)**

Skanowanie sieci

- **Wyszukiwanie aktywnych komputerów - ICMP**

1 **Żądania ICMP ECHO**



- **Odpowiedź - host jest aktywny, brak odpowiedzi - nieaktywny lub chroniony**
- **Prośba może być wysłana na adres rozgłoszeniowy (ICMP broadcast) - odpowiedź od wszystkich komputerów sieci (Windows - ignoruje, UNIX - różnie)**
- **Ochrona - zablokowanie ICMP ECHO**

2 **Inne żądania ICMP**

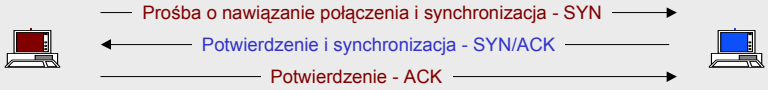
Prośba ICMP TIMESTAMP (typ 13), ICMP ADDRESS MASK (typ 17)

- **Uzgadnianie czasu i uzyskanie maski podsieci (terminale bez HD)**
- **Ochrona - zablokowanie żądań**

Skanowanie sieci

Wyszukiwanie aktywnych komputerów i portów - TCP

Nawiązanie połączenia w TCP (3-way handshake)



- Jeżeli port jest nieaktywny, host zrywa połączenie (pakiet z flagą RESET)

3 **Nawiązanie połączenia TCP**

Połączenie TCP (zwykle port 21,22,23,25,80) do badanej maszyny i analiza odpowiedzi

- Udane połączenie - maszyna i port aktywne, nieudane - maszyna lub port nieaktywne
- Połączenie jest zarejestrowane w dzienniku (logu) systemowym

Bezpieczeństwo systemów informatycznych

Skanowanie sieci

Wyszukiwanie aktywnych komputerów i portów - TCP

4 **Niepełne połączenie TCP**

Celowe odstępstwo od protokołu nawiązania połączenia TCP

- Rozpoczęcie SYN, zakończenie RST zamiast ACK
- Ponieważ połączenie nie zostało nawiązane (jest 'półotwarte'), może nie zostać odnotowane w logu
- Uzyskanie SYN/ACK daje poszukiwaną informację

5 **Nielegalne połączenie TCP**

Inicjacja połączenia nielegalnymi pakietami

- Rozpoczęcie połączenia - SYN/ACK, FIN - lub XMAS, NULL
- Port nasłuchujący - zignoruje, port nieaktywny - odeśle pakiet z RST
- Aktywność prawdopodobnie nie zostanie odnotowana w logu
- Ochrona - filtracja pakietów metodą inspekcji stanu

Krzysztof Ślot © 2002

Skanowanie sieci

- **Wyszukiwanie aktywnych komputerów i portów - TCP**

6 **Wykorzystanie serwera PROXY FTP**

Jeżeli serwer FTP ma publiczny, zapisywalny katalog i ma aktywną opcję PROXY można go wykorzystać do zdobycia informacji o sieci (nawet poprzez zaporę)

... **Inverse mapping, fragmentacja pakietów, ...** http://www.insecure.org/nmap/p51-11.txt

- **Identyfikacja systemów operacyjnych (wykorzystanie dziur)**
  - **Wykorzystanie usług ujawniających system (telnet, ftp)**
  - **Wykorzystanie różnic implementacji TCP/IP**

TTL0 : Windows - 128, Linux - 64
Odpowiedź na pakiet TCP FIN
Początkowy rozmiar okna
Wartość liczby pola ACK w odpowiedzi na pewne akcje
Treść komunikatów błędów ICMP
...

Podsłuchiwanie ruchu w sieci

- **Karty sieciowe mogą przyjmować wszystkie pakiety - mogą więc one być analizowane ...**

☺ **W celu analizy ruchu sieci dla potrzeb diagnostyki i statystyk**

☹ **W celu nieuprawnionego przechwycenia informacji - treści danych w celu identyfikacji stosowanych protokołów komunikacji, uzyskania haseł i innych informacji**

- **Sposoby wykrywania podsłuchu**
  - **Monitorowanie komputera - detekcja obniżenia wydajności (spowolnienia pracy) komputera, na którym zainstalowano podsłuch**
  - **Aktywne monitorowanie sieci - podstępy: wysyłanie zapytań generujących automatyczne odpowiedzi**
  - **Detekcja sprzętowa - zmiany impedancji obwodu**

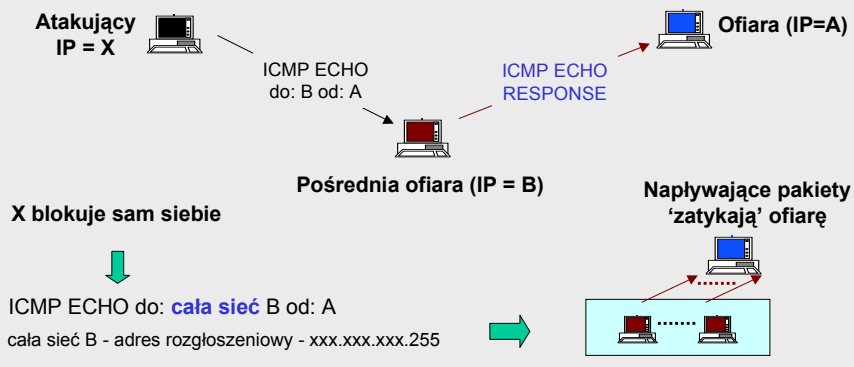
Blokowanie komputerów - ataki DoS

- Cel ataku - wyeliminować komputery (routery) z sieci poprzez zablokowanie ich portów (możliwości komunikacji), zawieszenie działania (systemu operacyjnego), zablokowanie aplikacji
- Powody ataku
  - Zadanie strat finansowych
    Amazon – zyski za pierwszy kwartał 2001 = 580 mln $
    Jedna godzina zablokowania serwera - ponad $200 000
  - Element innych, poważniejszych ataków (IP spoofing)
  - ...
- Metody ataku
  - Wysyłanie do komputera pakietów w liczbie przekraczającej możliwości obsługi
  - Wysyłanie pakietów spreparowanych w celu zablokowania działania systemu operacyjnego lub aplikacji

Ataki DoS

- Obciążanie serwera nadmierną ilością pakietów

'Twórcze' rozwinięcie techniki stosowanej do skanowania sieci



Stosowane nazwy ataków: „FRAGGLE" (UDP), „SMURF" (ICMP)

Ataki DoS

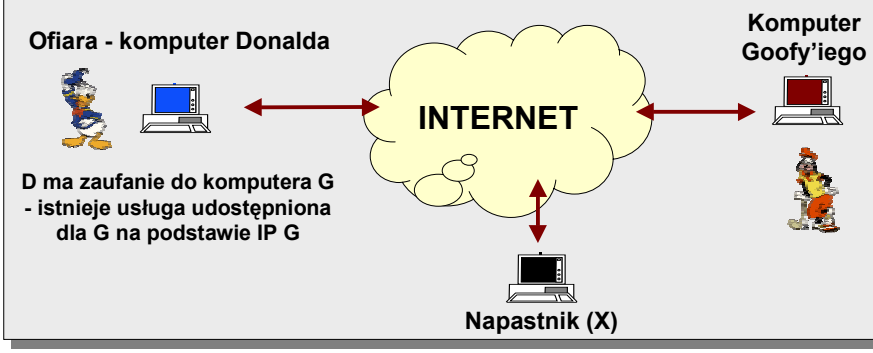
- **Blokowanie portów**
  - Dla danego gniazda TCP istnieje limit liczby zgłoszeń SYN, które mogą być jednocześnie obsłużone (tzw. Backlog - 6-7) - otwieranie 'niepełnych' połączeń (patrz spoofing)
- **Wykorzystywanie luk w SO i usługach**
  - Ping of death - wysyłanie pakietu ping z danymi o rozmiarze przekraczającym dopuszczalne maksimum (64k) - zawieszenie OS
  - Ataki na NetBIOS WIN,...
- **DDoS - distributed DoS**

  Ataki wykorzystujące wiele 'ofiar pośrednich'
- **Sposoby ochrony**
  - Blokowanie pakietów kierowanych na adres rozgłoszeniowy
  - Blokowanie pakietów ICMP, UDP, PING, ...

Podszywanie się pod IP - spoofing

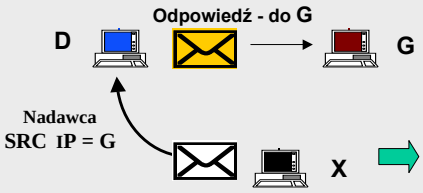
Cel - zaatakować komputer ofiary (D) wykorzystując zaufanie do G (przejawiające się udostępnieniem dla G określonych praw) przez podszycie się pod adres IP komputera G - IP spoofing

- **Przedstawienie postaci (czasem dramatu...)**



Spoofing

- Istota ataku - użycie przez X adresu IP G



Atak jest przeprowadzany 'na oślep' - atakujący nie otrzymuje pakietów od ofiary, musi przewidywać odpowiedzi ofiary

- Etapy ataku
  - Identyfikacja maszyn, do których upatrzona ofiara ma zaufanie (poszukiwanie komputera G)
  - Zablokowanie dostępu do komputera G
  - Zebranie dodatkowych danych koniecznych do przeprowadzenia ataku
  - Atak - uzyskanie dostępu do D i odpowiednia akcja (instalacja oprogramowania, założenie konta, zniszczenie danych itp.)

Spoofing - wprowadzenie

Wykorzystywane w ataku elementy TCP

Nagłówek TCP

0	15 16	31
Port nadawcy		Port odbiorcy
Numer identyfikujący pakiet - SN		
Numer potwierdzenia (ASN)		
Dł. nagł. / Rezerwa / FLAGI		Okno
CRC		Urgent pointer
Opcje		
Dane		

FLAGI

ACK	potwierdzenie połączenia
SYN	synchronizacja numerów porządkowych
RST	zerwanie połączenia
FIN	koniec strumienia u nadawcy

Spoofing

- **Faza 1 - Identyfikacja zaufanego G**

  Atak jest możliwy tylko wtedy, gdy taki komputer istnieje. Znalezienie może wymagać wcześniejszego zebrania informacji (podsłuch). Można też, na ślepo próbować sąsiednie IP

- **Faza 2 - zablokowanie komputera G**

  Wysłanie przez X sekwencji pakietów SYN do G w imieniu Y - hosta nieaktywnego w czasie przeprowadzania ataku, w celu przepełnienia limitu liczby zgłoszeń (backlog-u)

Pakiety SYN/ACK to nielegalne otwarcie połączenia - aktywny Y je zerwie (RST do G)

- **Faza 3 - zebranie dodatkowych informacji**

Określenie poprawnego numeru identyfikującego pakiet, w celu przekonania D, że ma do czynienia z G (nastąpi próba synchronizacji numerów)

Numery identyfikujące pakiety

- Zakres numerów SN: 0 do 2^{32}-1 (4 294 967 295)
- Uruchomienie systemu: SN=0
- W warunkach braku połączenia SN zwiększany co sekundę SN = SN + 128 000 (przepełnienie licznika co ok. 9h)
- Połączenie - zwiększenie SN o 64 000
- W trakcie wymiany danych SN zwiększany o numer kolejny pierwszego bajtu wysyłanego w danym pakiecie, ASN = SN + LB (liczba bajtów otrzymanych w pakiecie) - stanowi potwierdzenie otrzymania LB bajtów przez odbiorcę
- Cel przyjętej zasady zwiększania SN - umożliwienie porządkowania pakietów
- Okno - informacja o rozmiarze bufora (i przy okazji, o największym możliwym numerze SN kolejnej transmisji)

Spoofing

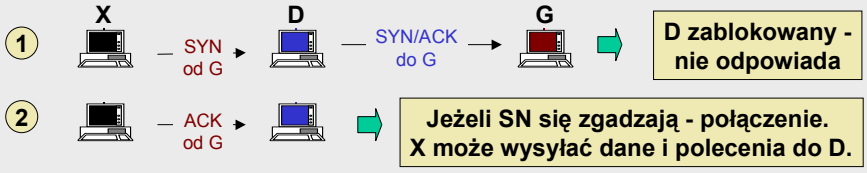
Faza 3 - odgadnięcie numeru SN Donalda

X łącząc się z D podaje jako adres zwrotny G, więc nie otrzyma numeru SN, bo D wyśle go do G

Odgadnięcie - wykorzystanie znanej zasady zmiany numeru SN:

- X wykonuje 'legalne' połączenie z D (np. wysyła pocztę) uzyskując bieżący SN (może kilkakrotnie powtórzyć połączenie)
- Szacuje SN jakiego musi użyć (czas potrzebny pakietom na dotarcie do komputera ofiary)

Faza 4 - atak



Bezpieczeństwo systemów informatycznych

Spoofing

Dobre oszacowanie SN

- SN jest zgodny z oczekiwanym przez D (SND): SN = SND
  Otwarcie połączenia

Złe oszacowanie SN: SN != SND

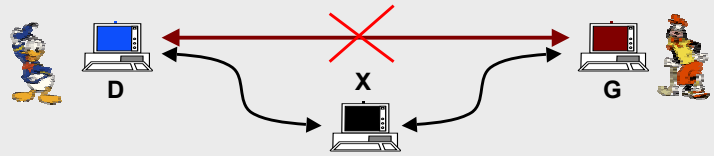
- SN < SND - pakiet potraktowany jako retransmisja i odrzucony
  Brak połączenia, brak potwierdzenia
- SN > SND + okno - pakiet odrzucany
  Brak połączenia, do D wysyłany pakiet z oczekiwanym SN
- SN > SND, SN < SND + okno - D wydaje się, że pakiet otrzymany przyszedł wcześniej niż oczekiwany - umieszcza go w odpowiednim miejscu w buforze
  Brak połączenia, brak potwierdzenia

Przeciwdziałanie atakowi - bezpieczne połączenie

Krzysztof Ślot © 2002

Uprowadzenie sesji (hijacking)

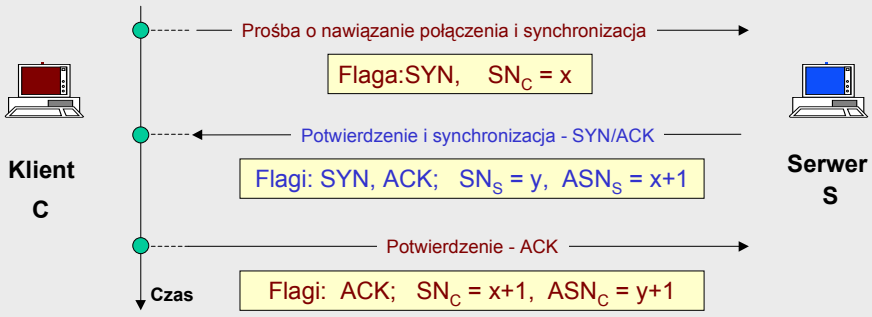
- **Cel: wkraść się 'pomiędzy' komunikujące się komputery i przejąć kontrolę nad sesją (a więc, dostęp do zasobów komputerów)**



X może dowolnie modyfikować treść komunikacji między D i G

- **Warunek konieczny wykonania ataku**
  - **X musi być w stanie podsłuchiwać wszystkie pakiety sesji (sniffer w sieci lokalnej którejś z maszyn)**
- **Metoda ataku**
  - **Wytworzenie i wykorzystanie stanu 'desynchronizacji' połączenia**

Otwieranie połączenia TCP



IP A	IP B	SN	ASN
35.42.1.56.1374 >	198.108.3.13.23: SYN	1496960000	xxxxxxxxx OKNO 4096
198.108.3.13.23 >	35.42.1.56.1374: SYN	1402880000 ACK	1496960001 OKNO 4096
35.42.1.56.1374 >	198.108.3.13.23:	1496960001 ACK	1402880001 OKNO 4096

Uprowadzanie sesji

Desynchronizacja połączenia między serwerem a klientem

- Sytuacja (normalna) po ustanowieniu połączenia
  Numer identyfikujący kolejny pakiet klienta zgadza się z numerem potwierdzenia serwera (i wzajemnie)

  $SN_C = ASN_S$ $SN_S = ASN_C$

- **Stan desynchronizacji**
  Numer identyfikujący kolejny pakiet klienta nie zgadza się z numerem potwierdzenia serwera

  $SN_C != ASN_S$ $SN_S != ASN_C$

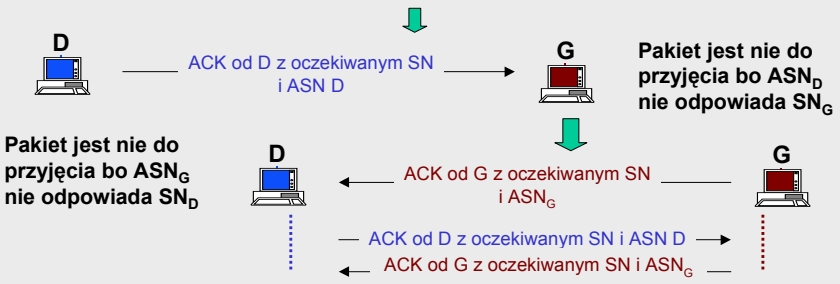
Reakcja na pakiety ze złym SN

- Odrzucenie (1)
- Odrzucenie i wysłanie ACK z oczekiwanym SN (2)
- Przyjęcie i potraktowanie pakietu jako przedwczesnego (3)

Uprowadzanie sesji

Zapętlenie wymiany komunikatów klient-serwer (TCP storm)
Stan komunikacji: desynchronizacja

- G wysyła do D pakiet danych, gdzie $SN_G > ASN_D + W$ ← okno

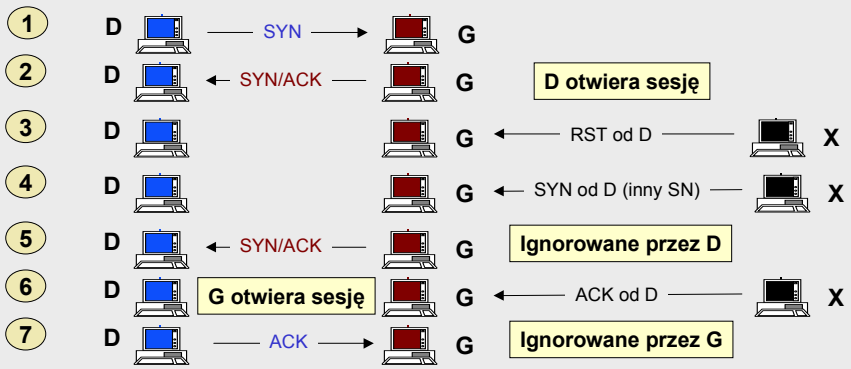


- Pętla nie jest nieskończona, bo IP gubi pakiety, po pewnym czasie połączenie zrywane (pakiet nie ma danych, więc nie jest retransmitowany)

Efekt - istnieje połączenie przy jednoczesnym braku komunikacji

Uprowadzenie sesji

- **Etapy ataku**
  - Wywołanie desynchronizacji
  - Przejęcie sesji - wysyłanie pakietów z właściwymi SN, podstawionymi IP nadawcy i odbiorcy oraz odpowiednio modyfikowaną treścią
- **Wywołanie desynchronizacji**



Uprowadzanie sesji

- **Wynik procedury - stan desynchronizacji**
  - Atakujący zna prawidłowe SN i ASN zarówno serwera jak i klienta, serwer i klient mają numery rozsynchronizowane (przez atakującego w 5 kroku procedury).
  - W trakcie procesu wywoływania desynchronizacji atakujący preparuje pakiety z adresem IP D jako nadawcy.
- **Przejęcie kontroli nad sesją**
  - D i G wysyłają do siebie pakiety, ale nie są one przez nie akceptowane, wywołując spiralę komunikatów ACK (TCP-storm)
  - Każdy z pakietów jest przechwytywany przez X. Umieszcza on w nim swoją treść oraz poprawne numery SN i ASN. W efekcie, zarówno G jak i D akceptują te pakiety, sądząc że odbywa się normalne komunikacja
- **Detekcja ataku - wykrycie zalewu komunikatów ACK**
- **Przeciwdziałanie atakowi - bezpieczne połączenie**