Zagrożenia bezpieczeństwa i systemy detekcji włamań

DNS, routing, programy i systemy operacyjne

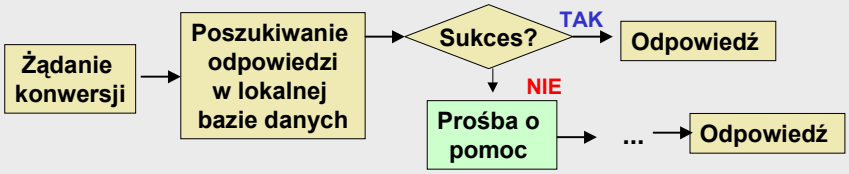
Zagadnienia

- Ataki wymierzone w infrastrukturę sieci
  - DNS spoofing - fałszywe IP
  - Kierowanie ruchu do podstawionych bram (routing redirection)
- Wykorzystywanie luk systemów operacyjnych i ich programów składowych

  Exploit-y: programy testujące oprogramowanie systemowe pod kątem wykorzystania jego potencjalnych słabości
  - Badanie programów pod kątem ich odporności na przepełnienie bufora (buffer overflow exploits)
  - Wykorzystanie luk związanych z uruchamianiem programów o uprawnieniach administratora
- Monitorowanie pracy i wykradanie danych z komputerów
- Systemy detekcji wtargnięć (IDS - intrusion detection systems)

Ataki przeciwko DNS

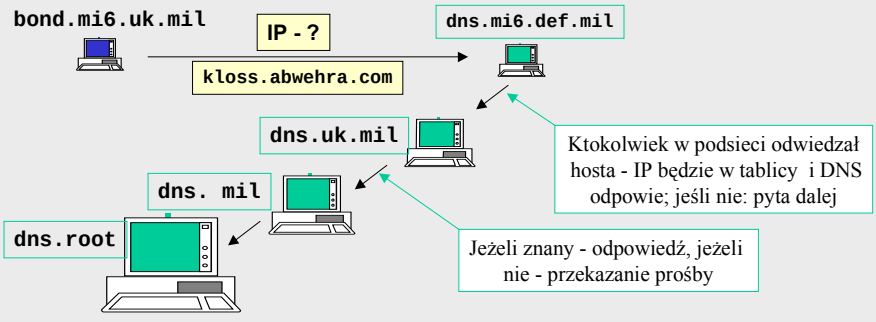
- DNS
  - Rozproszona baza danych z informacjami wiążącymi adresy IP z nazwami komputerów
  - Serwer DNS - komputer z odpowiednim oprogramowaniem: zwykle działający w systemie UNIX i posiadający usługę systemową BIND (Berkeley Internet Name Domain)
  - Usłudze przydzielony jest port 53 TCP
- Opanowanie serwera DNS = możliwość wprowadzanie w błąd użytkowników sieci co do tożsamości komunikujących się ze sobą komputerów
- Algorytm działania serwera DNS



Bezpieczeństwo systemów informatycznych

Ataki przeciwko DNS

- Tworzenie lokalnej bazy danych DNS
  - Uaktualnianie każdorazowo, gdy zajdzie potrzeba (prośba o dane dotyczące nieznanego wcześniej hosta), na podstawie informacji pobranej z innego DNS
- Mechanizm rozwikłania nieznanego adresu - serwery DNS 'wyższego' poziomu - drzewo DNS



Krzysztof Ślot © 2002

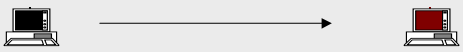
Ataki na DNS

- **DNS Spoofing - preparowanie odpowiedzi w wymianie danych między DNS**
  - Zapytanie o określenie adresu, jest opatrywane unikalnym ID - odpowiedź zawiera to samo ID i na tej podstawie jest ona zatwierdzana
  - Jeżeli generacja kolejnych ID w serwerze jest deterministyczna - możliwe jest jego przewidzenie i uprzedzenie prawdziwej odpowiedzi spreparowanym pakietem
- **Uwarunkowania ataku**

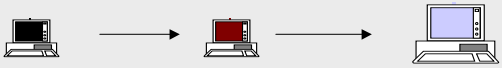
Cel: wprowadzenie fałszywego adresu D do serwera DNS G	Nie ma w nim dotychczas danych o komputerze D	DNS 2 zawiera informacje o komputerze D

Ataki na DNS

- **Scenariusz ataku**



1. Wysyła do DNS G prośbę o swój własny adres - zyskuje aktualne ID pakietu



2. Wysyła do DNS G prośbę o adres D. Adresu nie ma w DNS G, więc będzie on pytał kolejne serwery DNS, wysyłając do nich pakiety z ID+1

3. Szybko podsyła do DNS odpowiedź w imieniu DNS 2 z fałszywymi danymi komputera D

- **Ochrona**
  - Stosowanie losowych zmian ID pakietów z zapytaniami o dane (standardowy element aktualnych wersji programu BIND)

Ataki na DNS

- DNS Spoofing - ochrona c.d.
  - DNSSEC - uwierzytelnianie wymiany danych między serwerami DNS - uaktualnianie informacjami pochodzącymi wyłącznie z zaufanych źródeł
- Fałszywe serwisy www - mechanizm oszustwa
  - Tworzenie stron z pozornymi linkami (na stronie link prowadzi rzekomo do pko.bp.pl, podczas gdy naprawdę wskazuje na url=hack.com/pko.bp.pl)
  - Wybranie linku to odwołanie do serwera hack.com - atakujący wie, jaka strona miała być wczytana - preparuje atrapę o wyglądzie odpowiadającym oczekiwaniom użytkownika i zbiera za jej pomocą wymagane informacje

Bezpieczeństwo systemów informatycznych

Ataki na DNS

- DNS Spoofing poprzez DHCP
  - DHCP - użytkownik jest obsługiwany przez dynamicznie przypisywany serwer DNS
- Mechanizm ataku

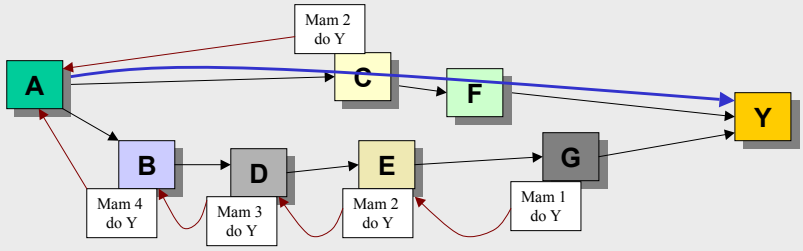
1. Hacker wysyła w imieniu serwera DHCP do komputera z dynamicznie przydzielanym IP informację o rzekomej zmianie adresu serwera DNS.
2. Serwer DNS należy do hackera i zawiera nieprawdziwe dane
3. Żądania użytkownika są obsługiwane przez podstawiony DNS - zamiast połączeń z amazon.com itp., użytkownik wczyta spreparowane odpowiednio strony atakującego

- Ochrona - zablokowanie zewnętrznych żądań DHCP

Krzysztof Ślot © 2002

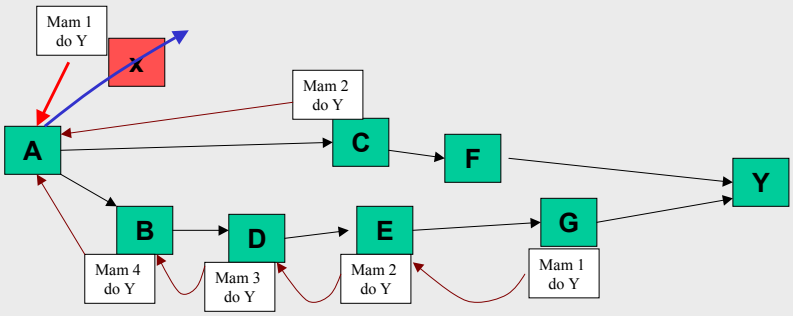
Ataki związane z routingiem

- **Prosty protokół przesyłania pakietów (RIP - Routing Information)**
  - Zakłada, że wszystkie routery są godne zaufania, bo trasa jest budowana na podstawie ‘oświadczeń’ routera o odległości do wybranego hosta
  - Routery używają tablic (forwarding table) z informacjami o najkrótszych połączeniach do różnych hostów, pobieraną od sąsiadów i okresowo uaktualnianą (co ok. 30 s, między innymi po to by znać stan połączenia)
  - Pakiety są przesyłane najkrótszą drogą



Ataki związane z routingiem

- **Atak przeciwko RIP - podsunięcie fikcyjnych informacji o odległości do celu**



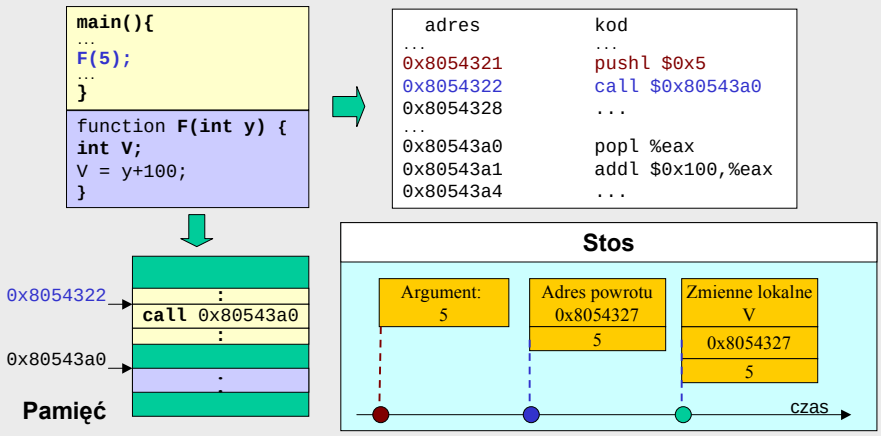
  - Przekazanie fałszywych informacji o odległości do celu wymusi przesyłanie pakietów do określonych sieci przez router atakującego
- **Metody ochrony**
  - Stosowanie innych protokołów - OSPF (Open Shortest Path Protocol)
  - Uwierzytelnianie

Ataki w OS i jego usługi - exploity

- **Język C**

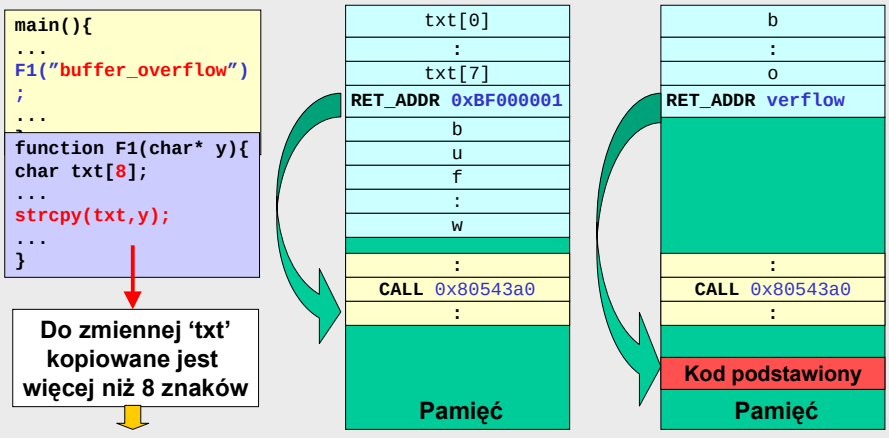
  Powstał (lata 70-te) dla uniezależnienia UNIX-a od konkretnego procesora (UNIX był napisany w języku assemblera)

- **Mechanizm wywoływania funkcji w C**



Przepełnienie bufora

- **Zmiana adresu powrotu z procedury przez nadpisanie danymi**



Nadpisanie adresu powrotu

- **Błąd programisty - skok niedozwolony przez OS i przerwanie programu**

Przepełnienie bufora

- **Buffer overflow exploit - zamierzona wartość adresu powrotu**

  Idea postępowania - tak nadpisać adres powrotny, by wskazywał początek procedury, którą chce się wykorzystać do przeprowadzenia ataku (może to być dowolny z systemowych plików 'dll', dających dostęp do plików, uprawnień, może to być uruchomienie serwera itp.)

- **Ochrona**
  - Opracowywanie programów odpornych na atak (sprawdzanie danych wprowadzanych przez użytkownika) - twórcy oprogramowania
  - Monitorowanie stanu komputera (np. obecność zrzutów 'core' w katalogach użytkowników może świadczyć o działaniu exploit-a)
  - Stosowanie ogólnych zasad bezpieczeństwa - sprawdzone serwisy, instalowanie 'ugrade-ów' i łat w systemach itp.

- **Inne ataki metodą przepełnienia bufora**
  - Skrypty CGI (Perl, PHP)
  - Dowolne usługi OS, ...

Ataki wykorzystujące SUID

- **Bit SUID (GUID) - określanie uprawnień programu**
  - SUID/SGID wyzerowany - uprawnienia użytkownika (grupy), który go uruchamia
  - SUID/SGID (user id / group id) ustawiony - program ma uprawnienia właściciela (tego, kto go zainstalował)

```
-r-sr-xr-x root bin 1000 some_prog DEC 13 02
```

Uruchomienie program z ustawionym SUID - uzyskanie uprawnień instalującego (np. root-a)

⇩

Potencjalne zagrożenie bezpieczeństwa

- **Zmniejszanie zagrożenia atakiem**
  - Zerowanie flagi SUID jeżeli nie jest to konieczne
  - Instalowanie programów z kont o mniejszych uprawnieniach (jeżeli to możliwe, np. użycie konta root jedynie do kopiowania binariów, zaś instalacja z poziomu zwykłego użytkownika)

Ataki wykorzystujące SUID

- Wykorzystanie programu SUID do uruchomienia programu podstawionego przez atakującego (root shell vulnerability)
- Uwarunkowania ataku
  - Program SUID wywołuje inne programy
  - Wywołanie nie jest poprzedzone dokonaniem żadnych sprawdzeń (np. dotyczących lokalizacji uruchamianych plików)
- Metoda ataku
  Podstawienie pod procedurę (program, plik wsadowy) uruchamianą przez program SUID swojego pliku
- Scenariusz ataku
  - Utworzenie pliku o nazwie identycznej z programem uruchamianym przez program SUID i odpowiednio spreparowanym kodem
  - Umieszczenie podstawianego pliku w dowolnym katalogu użytkownika
  - Dodanie na początku pliku 'path' ścieżki do wybranego katalogu
  - Wykonanie programu SUID (czyli, wykonanie ataku)

Bezpieczeństwo systemów informatycznych

Ataki wykorzystujące SUID

- Uruchamianie podstawionych programów - przykład

  Obiekt ataku - program `SubnetConfig` systemu UNIX - korzystający z programu '`cat`'.
  - Utworzenie pliku o nazwie 'cat' z kodem ingerującym w system zgodnie z zamiarem atakującego (wstawienie polecenia kopiowania tekstu '++' do pliku .rhosts)
  - Umieszczenie pliku w wybranym folderze (np. o nazwie 'temp')
  - Dodanie na początek ścieżki systemowej ścieżki do wybranego foldera

    ```
    path = /temp:$path;
    ```
  - Uruchomienie programu `SubnetConfig` , i pośrednio - procedury `cat`
- Efekt

  Wywołanie podstawionej procedury cat, modyfikującej plik .rhosts w sposób pozwalający na uzyskanie uprawnień administratora dowolnemu logującemu się użytkownikowi (program działa w imieniu administratora, ma więc prawo modyfikacji pliku .rhosts)

Krzysztof Ślot © 2002

Ataki wykorzystujące SUID

- Wykorzystanie programu SUID do nadpisania plików (SUID file overwriting vulnerability)
- Uwarunkowania ataku
  - program o uprawnieniach SUID tworzy plik, do którego wpisuje dane (np. log).
  - program SUID nie upewnia się czy istnieją jakiekolwiek dodatkowe uwarunkowania dla procedury zapisywania pliku (jak np. powiązanie zapisywanego dziennika z innym plikiem)
- Scenariusz
  - Utworzenie linku, łączącego plik logu programu SUID z plikiem, który chcemy nadpisać (obiektem ataku).
  - Uruchomienie programu SUID i zapewnienie, by tekst rejestrowany w logu zawierał informacje, które mają znaleźć się w atakowanym pliku (wprowadzany tekst jest jednocześnie wpisywany do logu i do wybranego przez nas pliku)

Bezpieczeństwo systemów informatycznych

Ataki wykorzystujące SUID

- Nadpisywanie plików - przykład

  Atakowany plik - '.rhosts' systemu UNIX, wykorzystywany program - PPS (point to point serial protocol)
  - Utworzenie linku

    `ln -s /.rhosts log` log- alias do pliku dziennika programu PPS
  - Atak (uruchomienie programu)

    `pps -o '++'` - wpisanie '++' do .rhosts
  - Zatarcie śladów `mv log old_log`
- Efekt

  Po wykonaniu procedury, podmieniony plik .rhosts pozwala napastnikowi na przejęcie kontroli nad komputerem
- Jeżeli katalog domowy użytkownika jest otwarty do zapisu dla wszystkich, napastnik może w nim umieścić swój .rhosts i w ten sposób uzyskać możliwość logowania do konta

Krzysztof Ślot © 2002

Wykradanie danych z komputerów

- Wymaganie fizycznego dostępu do komputera lub instalacji odpowiedniego oprogramowania
- Wydobywanie ‘wymazanych’ danych (usuwanie plików)
  - Windows - usunięcie pliku to jedynie usunięcie wpisu z tablicy alokacji plików. Same dane pozostają na dysku do momentu ich późniejszego nadpisania. W warunkach silnej defragmentacji dysku dane te mogą być dostępne przez długi czas.
  - Ochrona - używanie programów do wymazywania danych (zastępują wymazywane dane losowymi wartościami)
- Swap file
  - Dane z RAM są czasowo składowane na dysku w tymczasowym pliku (swap file), zawierającym mnóstwo cennych informacji (hasła, klucze, treść dokumentów itp.)
  - Instalacja programu odczytującego dane z pliku tymczasowego (i analizującego dane, np. w poszukiwaniu słów password itp.) daje dostęp do tajnych informacji

Bezpieczeństwo systemów informatycznych

Wykradanie danych z komputerów

- Pliki historii
  - Przeglądanie automatycznie tworzonych plików historii daje informacje o aktywności użytkownika
- Podsłuch klawiatury i portów lokalnych (keyboard snooping / sniffing) - programowy lub sprzętowy
  - Uwaga na kawiarenki internetowe !
  - Idea programów detekcji - prośba o wpisanie zadanego tekstu i sprawdzenie, czy został zarejestrowany w pliku
- Inne metody podsłuchu
  - Zrzuty pamięci obrazu (‘zdjęcia’ ekranu)
  - Zdalne odczytywanie zawartości monitora
    Monitor emituje fale elektromagnetyczne, które mogą być podsłuchane i odczytane, zdradzając wyświetlane treści
    Metoda ochrony - zapewnienie spełnienia odpowiednich norm (TEMPEST - Transient ElectroMagnetic PulsE Standard)

Krzysztof Ślot © 2002

Systemy detekcji włamań

Systemy detekcji włamań (intrusion detection)

Założenie - istnieją ślady możliwe do znalezienia przez analizę ruchu, zużycie CPU, częstość operacji I/O, analizę pakietów, rodzaje aktywności w odniesieniu do systemu (usuwanie plików) itp.

Detekcja bazująca na regułach

Detekcja bazująca na statystyce

Zapory nie chronią przed potencjalnymi włamaniami dokonywanymi nie strzeżonymi przez nie kanałami (modem, dostęp bezprzewodowy, ataki dokonywane od wewnątrz sieci)

Detekcja anomalii — **Statystyczne niezgodności w aktywności użytkownika w stosunku do utworzonego wcześniej profilu**

Detekcja nadużyć

Bezpieczeństwo systemów informatycznych

Systemy detekcji włamań

Profil komputera - średnie obciążenie CPU, średnia liczba korzystających z niego użytkowników, najczęściej wykorzystywane usługi itp.

Profil użytkownika -

Działanie - monitorowanie sesji i alarmowanie w sytuacjach wyraźnych, dużych odstępstw od istniejącego profilu odniesienia

Detekcja nadużyć - porównywanie aktywności z charakterystykami znanych ataków, zgromadzonymi w bazie danych systemu. Baza musi być na bieżąco aktualizowana.

Ponieważ zasady mogą nie być jednoznaczne, detekcja aktywności uznawanej za atak może wymagać zaawansowanych metod analizy.

Pakiety IDS

Internet Security Systems (dodatek do zapór programowych CheckPoint) - monitorowanie TCP, UDP, ICMP

Krzysztof Ślot © 2002

Systemy detekcji włamań

Network Associates - CyberCop - rozproszony system z centralnym serwerem analizy danych

Pożądane cechy systemu

Monitorowanie w czasie rzeczywistym

Preludium wielu ataków

Nietypowe godziny aktywności

Celowe zasypywanie dziennika lawiną informacji

Aby wyczyścić dziennik

Rozmiary dziennika mogą sięgać setek MB