Bezpieczeństwo systemów i sieci

- Marcin Szewczyk, 198370

Treść prezentacji

- Przegląd zagrożeń dla użytkownika
- Samoobrona
- Jak administrator może pomóc
- Reakcja na włamanie
- Poskramianie użytkowników

Problemy ochrony

- Koszty
- Wydajność maszyn
- Wygoda a bezpieczeństwo
- Heterogeniczna struktura
- Odkrywanie koła
- Tajność rozwiązań

Porządek prezentacji

- 7 warstw ISO/OSI
  - Aplikacji (Application)
  - Prezentacji (Presentation)
  - Sesji (Session)
  - Transportowa (Transport)
  - Sieci (Network)
  - Łącza (Data Link)
  - Fizyczna (Physical)

Porządek prezentacji (2)

- Internet Protocol Suite (TCP/IP)
  - Uproszczony stos
  - Mniej warstw
    - Aplikacji (Application)
    - Transportowa (Transport)
    - Internet (Internet)
    - Łącza (Link)

Systemy a sieć

- Nieodłączne towarzystwo sieci, w szczególności Internetu
- Cloud computing – usługi na serwerach sieciowych
  - Google Docs
  - Google Calendar
  - Gmail
- Amoeba, Microsoft Midori

Zagrożenia

- Straty materialne
- Brak dostępu
- Naruszenie tajności danych
- Kradzież personaliów
- Konsekwencje prawne cudzych działań

Warstwa aplikacji – błędy programistów

- DoS
  - Upadek aplikacji
  - Zużycie zasobów (CPU, pamięć RAM i trwała)
- Exploit
  - buffer overflow, wykonanie danych
  - bit NX (x86_64)
  - Łatwość realizacji – Metasploit
    - Ernst & Young

Warstwa aplikacji – błędy programistów (2)

- Fontanna i chromowane linijki kodu
  - FTP – SITE EXEC
- GNU Linux
  - magia przetwarzania w pipe'ach
  - jedno narzędzie do jednego zadania

Warstwa aplikacji – błędy programistów (3)

- SQL Injection
  - tekstowe budowanie zapytań zamiast np. pg_execute w PHP
  - czyszczenie zapytań
- include, printf, escape characters
- Sprawdzanie poprawności danych tylko u klienta
- Poufne dane w logach (publicznie dostępnych)
- XSS

Izolowanie problemów

- Wirtualizacja
  - VirtualBox
  - XEN
- Kod zarządzany
  - .NET
  - Java
  - (JavaScript, Mozilla)
- OS
  - chroot, zmiana użytkownika, SELinux, AppArmor

Warstwa aplikacji – błędy użytkownika

- Łatwowierność
  - „łatki” od Microsoftu
- Panika i brak współpracy
- Złe praktyki
  - Konto administratora/roota
  - Autouruchamianie
  - Nadmiar usług
  - Dostęp do usług dla połączeń przychodzących
  - Bezrefleksyjna akceptacja błędnych certyfikatów

Błędy użytkownika-administratora

- Błędna konfiguracja
  - SMTP open relay
- Brak sprawdzenia
- Przekonanie o własnym geniuszu
- Brak rozwoju
- Niezapamiętanie ustawień w pamięci trwałej
  - iptables
  - switche i routery

Połączenie obu

- JavaScript
- Flash
  - NoScript
  - AdBlock Plus
- PDF (ActiveX, inne wtyczki)
- Bycie szkodnikiem
  - botnet DDoS
  - SPAM, port 53

Asysta administratorów

- Filtrowanie w warstwie 7.
  - nieskuteczne dla połączeń szyfrowanych
  - proxy: Squid, WebWasher, ipp2p, l7filter, smtp-gated
- Blokowanie portów
- Stosowanie RFC
  - poczta a porty 25, 465, 587

Asysta administratorów

- Poczta
  - filtry antyspamowe
  - reverse DNS
  - SPF, SRS

Warstwa aplikacji

- Popularne wykorzystywanie usług z prawami SYSTEM na systemie Windows
  - pierwszy popularny Blaster
  - połączenia przychodzące
  - brak ochrony pracą jako użytkownik
- Rootkity na Windows i Linux

Bezpieczne połączenia

- SSH, SFTP, SCP
- Hasła czy klucze?
- Tunele (VNC, rdesktop)
- Man-in-the-middle
- Uwierzytelnianie
  - serwera
  - klienta
  - dwóch klientów

Uwierzytelnianie i szyfrowanie

- Szyfry symetryczne i asymetryczne
- SSL/TLS, PKI, CA
  - HTTP
  - SMTP
  - POP3
- Server Name Indication
- Słabość MD5, kolizje
  - fałszywe certyfikaty [ROGUE-CERT]

Szyfrowanie treści

- Szyfrowanie korespondencji
  - GnuPG, PGP (OpenPGP), web-of-trust
- Szyfrowanie dysków
  - tryb szyfrowania (ECB jest złe)
  - plik wymiany
  - pliki tymczasowe
  - wyciąganie z RAMu (DRM, podtrzymanie)

Warstwa aplikacji – problemy czysto sieciowe

- DHCP
  - każdy może być serwerem DHCP
  - popularne routery bezprzewodowe
- DNS
  - brak uwierzytelniania
  - DNSSEC
- FTP w zestawie z IP
  - komendy PORT, PASV, podszywanie

Asysta administratorów

- Cisco DHCP Snooping
  - nie pozwalaj być serwerem DHCP
  - pilnuj korelacji dzierżawa DHCP – adres źródłowy pakietu → ARP Inspection

Warstwa transportowa

- TCP
  - Zgadywanie numeru sekwencyjnego
  - Wstrzykiwanie pakietów z danymi
  - Wstrzykiwanie pakietów RST
- UDP
  - Cokolwiek

Warstwa Internet

- IP
  - Brak weryfikacji autentyczności
  - IPSec
  - IPv6 – wbudowane mechanizmy
  - VPN, Hamachi, Skype
- ICMP
  - błędna diagnoza
  - nieprzepuszczanie pakietów
  - dane w pingu

Asysta administratorów

- Cisco Unicast Reverse Path Forwarding
- iptables

Warstwa łącza

- ARP
  - brak ochrony
  - „jestem routerem” - wykradanie danych
  - generacja, modyfikacja MACów
  - DoS
  - switch → hub
- Zniszczenie łącza
  - brak redundancji
  - bezwładność

Asysta administratorów

- Static MAC address table (switch i komputer)
  - dobre, gdy przywłaszczamy MAC, nie IP
- Cisco ARP Inspection → DHCP Snooping
  - pilnuj prawidłowego adresu źródłowego, korelacji MAC-IP
  - modyfikacja adresu MAC dla danego IP nie stanowi zagrożenia
- Cisco Port Security
- RADIUS

Łącza beprzewodowe

- Otwarte sieci
- WEP
- WPA/WPA2
  - wersje Enterprise
- Ataki
  - bierne: nasłuchiwanie
  - aktywne: replay

Firewall

- Chroni przed atakami analizując ruch sieciowy
- Nie chroni bezpośrednio przed wirusami
- Firewall a NAT
  - router o jeden hop
  - IPv6 i brak NAT

Firewall dla użytkownia

- Linux – iptables
  - łańcuchy
  - reguły
- Windows
  - zintegrowana zapora
  - osobiste zapory
    - Sunbelt Kerio Personal Firewall

IDS

- Detekcja włamań
- Snort
- ipp2p, l7filter
- iptables
  - anomalie na porcie 25
  - anomalie na porcie 53
- Port mirroring
- Logi

Malware

- Wirusy
  - przeszłość – niszczenie danych
- Trojany, downloadery
  - współcześnie
    - wyślij dane
    - modyfikuj dane
    - ściągnij więcej malware'u
    - botnet, pieniądze, wojny elektroniczne

Oprogramowanie antywirusowe

- Sygnatury
- Heurystyka
- Aktualizacja baz
- Legalność oprogramowania, cracki
- Rezydentna ochrona
- *False positives*
- Pochłanianie zasobów

Reakcja na zagrożenie „przed”

- Aktualizacja pakietów
  - Windows
  - Linux
    - apticron
- Śledzenie biuletynów
- Kontakt ze „służbami” (abuse)
- Odcinanie atakujących

Reakcja na zagrożenie „po”

- Położenie maszyny wirtualnej
- Logi
- Kontakt ze „służbami” (abuse)
- Czyszczenie dysku
- Wycinanie „użyszkodników”
  - port shutdown
  - VMPS, RADIUS
  - filtrowanie

Zródła i przypisy

- Źródła
  - dokumentacja Cisco
  - Wikipedia
  - Linux manpages, netfilter project
  - różne dokumenty
- [ROGUE-CERT]
  - http://www.win.tue.nl/hashclash/rogue-ca/