Najważniejsze zagadnienia z BSI
na podstawie pytań zebranych przez Teemonka
opracowane przez Flowera

opracowane 216 pytań z wyjątkami

VPN - Virtual Private Network

IPsec - IP Security

- IKE - Internet Key Exchange
    - oferuje uwierzytelnianie stron
    - korzysta z UDP port 500
    - oferuje negocjację algorytmów szyfrujących
    - oferuje wymianę kluczy metodą Diffiego-Hellmana
- ESP - Encapsulating Security Payload
    - uwierzytelnianie źródła danych
    - integralność danych (przy pomocy obliczenia skrótu z zaszyfrowanych już danych)
    - niezaprzeczalność danych (przy pomocy obliczenia skrótu z zaszyfrowanych już danych)
    - obsługuje unikanie duplikacji pakietów jak również ataku przez powtórzenie (zastosowanie numerów sekwencji)
    - zapewnia poufność danych
    - umożliwia zapewnienie
        - autentyczności treści datagramu przy wykorzystaniu algorytmu MD5
        - poufności treści datagramu w trybie tunelowym
        - poufności treści datagramu w trybie transportowym
        - poufności i/lub autentyczności treści datagramu, w trybie tunelowym
- AH - Authentication Header
    - uwierzytelniania
    - integralności
- Tryby pracy
    - transportowy
    - tunelowy

SSL - Secure Socket Layer; TLS - Transport Layer Security

- ochrona poufności
- propagacja portów w tunelu kryptograficznym
- nawiązywanie sesji SSL
    - serwer przesyła komunikat ServerHello ze swoim certyfikatem
    - klient uwierzytelnia serwer na podstawie odebranego certyfikatu

        - serwer przesyła komunikat ServerHello z opcjonalnym losowym zawołaniem
        - klient odsyła podpisane zawołanie do serwera tylko jeśli serwer żądał uwierzytelnienia klienta
- OpenVPN
    - nie ma wyróżnionego programu serwerowego i klienckiego
    - certyfikaty SSL dla obu stron połączenia muszą by podpisane przez tą sam zaufaną stronę trzecią
    - utworzenie wielu połączeń z danego hosta za pomocą programu OpenVPN
        - ?należy uruchomić program OpenVPN z wieloma plikami konfiguracyjnymi, każdy plik definiuje jedno połączenie?
        - ?należy uruchomić kolejne instancje programu OpenVPN wraz z osobnymi plikami konfiguracyjnymi?
    - należy wpisać gdzie znajduje się drugi koniec tunelu VPN w pliku konfiguracyjnym
    - wykorzystuje tablice routingu w Linuxie
        - do przechowywania trasy do sieci dostępnej po drugiej stronie połączenia VPN

SSH - Secure SHell

- propagacja portów w tunelu kryptograficznym
- pozwala uniknąć przesyłania hasła podmiotu uwierzytelnianego
    - metodą Diffiego-Hellmana
    - ?metodą klucza asymetrycznego?
- SFTP
    - podsystem ssh służący do przesyłania plików
- umożliwia nawiązywanie połączeń ze zdalnymi terminalami
- Możliwości uwierzytelniania się przy użyciu SSH
    - trójka login, klucz publiczny i klucz prywatny
    - para login, hasło naszego konta na zdalnym hoście
- $ssh host
    - Enter passphrase for key '/home/junior/.ssh/id_dsa':
    - Wpis passphrase to:
        - hasło, którym jest zaszyfrowany klucz prywatny

Tunel host-to-host

- połączenie punkt - punkt między dwoma hostami ale tylko na czas transmisji zaszyfrowanej

Tunel net-to-net

- bezpośrednie połączenie dwóch lub więcej sieci przez Internet
- koncepcja połączenia dwóch lub więcej sieci w której istnieją zestawione tunele między bramami dla każdej z sieci

Ideą połączeń typu VPN jest

- utworzenie sieci łączącej odseparowane, odległe sieci lokalne

Zdalny dostęp

PAP - PPP Authentication Protocol

- login i hasło przesyłane jawnym tekstem
- przez to nie chroni przed podszywaniem się pod podmiot uwierzytelniający

CHAP - Challenge Handshake Authentication Protocol

- zawołanie-odzew (challenge-response)
- odzew = hasło kodowane MD5
- pozwala więc uniknąć przesyłania hasła podmiotu uwierzytelnianego

EAP - Extensible Authentication Protocol

RADIUS - Remote Access Dial-In User Service

- wspomaga uwierzytelnianie
- pracuje w architekturze klient-serwer
- udostępnia informacje niezbędne do kontroli uprawnień zdalnego dostępu (np. restrykcje czasowe)
- pozwala na scentralizowane przechowywanie danych uwierzytelniających dla wielu punktów dostępowych

TACACS - Terminal Access Control - Access Control System

Uwierzytelnianie

Kerberos

- protokół uwierzytelniania i autoryzacji w sieci komputerowej
- KDC - Key Distribution Center
    - może zapewnić bardzo dobre bezpieczeństwo w sieci
    - ufa uwiarygodnionym użytkownikom
    - Nie przechowuje kont (pliki, inne głupoty) tylko dane uwierzytelniające!
- AS = Authentication Server
- SS = Service Server
- TGS = Ticket-Granting Server
- TGT = Ticket Granting Ticket
- Określ prawidłową kolejność pełnej sekwencji odwołań klienta do serwerów w przypadku

dostępu do usługi SMTP w środowisku Kerberos
    - serwer AS - serwer TGS - serwer SMTP
- Kerberos jest bezpieczniejszy niż LM i NTLM
- Nazwa domenowa komputera a nazwa domeny kerberos
    - zaleca się, aby była identyczna
- Aby serwer usług w domenie kerberos mógł działać wykorzystując uwierzytelniania Single-Sign-On, musi
    - używać odpowiednio zmodyfikowanych demonów usług, które potrafią rozmawiać z serwerem Kerberos

SASL - Simple Authentication and Security Layer
- rozszerzenie mechanizmu uwierzytelniania protokołu SMTP o mechanizm haseł jednorazowych
- rozszerzenie mechanizmu uwierzytelniania protokołu IMAP o współpracę z systemem Kerberos

Uwierzytelnianie z udziałem trzeciej strony
- Kerberos
- system PKI - Public Key Infrastructure
    - urząd CA - Certification Authority
- serwer uwierzytelnia klienta na podstawie poświadczenia wystawionego przez trzecią stronę
- do zadań strony uwierzytelnianej należy
    - przekazanie poświadczenia uwierzytelnienia drugiej ze stron
    - przekazanie danych uwierzytelniających stronie trzeciej
- do zadań tej trzeciej strony należy
    - poświadczenie uwierzytelnienia
- opłaca się stosować szczególnie wobec większej ilości serwerów

PAM - Pluggable Authentication Modules
- umożliwia oddzielenie konfiguracji procesu uwierzytelniania od kodu aplikacji
- korzystając z PAM administrator może narzucić ograniczenia użytkownikom (limity)

SSO - Single Sign-On
- uwierzytelnianie użytkownika wobec wielu serwerów jednorazową procedurą weryfikacji hasła
- służy ochronie danych uwierzytelniających użytkownika
- pozwala na tworzenie relacji zaufania między hostami
- zalety:
    - jednokrotne uwierzytelnianie

Relacja zaufania w uwierzytelnianiu w środowisku sieciowym:
- jest wykorzystywana zarówno przez systemy Unix, jak i MS Windows
- może być jednostronna lub dwustronna

- nie jest przechodnia

Funkcje skrótu

Funkcja skrótu dająca wynik 512-bitowy:

- ma teoretyczną odporność na kolizje = 2^256
- ma teoretyczną odporność na atak urodzinowy = 2^256

MD4

MD5

SHA - Secure Hash Algorithm

- algorytmy SHA-256 i SHA-512 różnią się wzajemnie
    - wielkością wynikowego skrótu
    - podatnością na kolicja

MAC - Message Authentication Code

HMAC - keyed-Hash Message Authentication Code

- kod MAC z wmieszanym kluczem tajnym zapewniający zarówno ochronę integralności jak i autentyczności danych
- wykorzystuje
    - SHA-1
    - MD5

Algorytmy kryptograficzne

Symetryczne:

- **DES - Data Encryption Standard**
    - klucz 56b
- **3DES-EDE**
    - klucz 168b
    - trzykrotne użycie algorytmu DES w trybie szyfrowania, deszyfrowania i ponownie szyfrowania
- **AES - Advanced Encryption Standard**
    - klucze: 128b, 192b, 256b
- **Rijndael**
- **Blowfish**
- **RC2**
- **RC4**
    - szyfr strumieniowy

- **IDEA**
- **Klucze w szyfrowaniu symetrycznym**
    - zawsze powinny być znane tylko komunikującym się stronom

Asymetryczne:
- **RSA**
- **ElGamal**
- **Szyfrowanie asymetryczne zapewnia**
    - poufność pod warunkiem zachowania tajności klucza prywatnego odbiorcy
    - autentyczność pod warunkiem zachowania tajności klucza prywatnego nadawcy

Tryb strumieniowy szyfrowania
- umożliwia szyfrowanie komunikacji asynchronicznej
- polega na szyfrowaniu każdorazowo po jednym znaku
- szyfr, w którym poddawana szyfrowaniu zostaje tej samej wielkości jednobajtowa porcja nieregularnie pojawiających się danych

Klucz FEK to
- klucz symetryczny

Protokół uzgadniania kluczy Diffiego-Hellmana
- jest odporny na ataki pasywne (podsłuchanie klucza)
- możliwe podstawienie fałszywego klucza w miejsce każdego z wymienianych (atak aktywny)

OTP - One-Time Password; Hasła jednorazowe
- Techniki
    - metoda zawołanie-odzew (challenge-response)
    - synchronizacja czasu
    - listy haseł jednorazowych
- uniemożliwia atak poprzez odtwarzanie (replaying)

Wektor inicjujący; IV
- powinien mieć losową wartość, za każdym razem inną

Pre-shared key
- prosty mechanizm pozwalający szyfrować i uwierzytelniać strony za pomocą jednego klucza
- jest to przykład kryptografii symetrycznej

Ataki i zagrożenia

TCP Spoofing

- odgadnięcie numeru ISN strony odbierającej dane nawiązania połączenia
- usługi r* są szczególnie narażone na ataki
    - rcp, ponieważ używa adresu klienta do uwierzytelnienia

rlogin
- pozwala na zdalny dostęp do hosta
- wszystko przesyłane jawnym tekstem

rsh
- pozwala wykonać polecenie na zdalnym hoście
- nie podanie loginu powoduje użycie nazwy lokalnego bieżącego użytkownika
- komunikacja nie jest chroniona

Przepełnienie bufora
- Bezpośrednim celem ataku metodą przepełnienia bufora jest
    - nadpisanie adresu powrotu na stosie
- środki ochronne
    - niewykonywany segment stosu
    - kontrola zakresu danych globalnych programu na etapie wykonania -> ??
    - kontrola zakresu danych lokalnych funkcji na etapie kompilacji
- funkcje biblioteczne odpowiedzialne za podatność na atak przepełnienia bufora
    - gets()
    - strcpy()
- Problem przepełnienia bufora dotyczy potencjalnie aplikacji
    - napisanych w języku C
    - uruchamianych w systemie z rodziny Windows
    - uruchamianych w systemie z rodziny Unix/Linux

Zagrożenia bezpieczeństwa związane z fragmentacją datagramów w protokole IP
- fragmentacja utrudnia filtrację pakietów

SYN flood
- intensywny strumień segmentów SYN skierowany na adres ofiary
- brak segmentów ACK

Malware - złośliwe oprogramowanie
- kamuflaż
    - opancerzenie (armor)
    - polimorfizm

DoS - Denial of Service
- intensywny strumień rozgłoszeniowych segmentów SYN z adresem źródłowym ofiary
- fragmentacja datagramu o sumarycznej wielkości ponad 64kB
- intensywny strumień pakietów UDP echo z adresem docelowym ofiary

- intensywny strumień segmentów FIN z adresem docelowym ofiary

Atak aktywny

- Atak ten przeprowadza osoba, która wobec każdej z dwóch uprawnionych stron komunikacji podszywa się za przeciwną stronę, pośrednicząc w przesyłaniu danych

Zabezpieczenia przed atakami

LINUX

- **chroot()**
  - ograniczenie odczytu do określonego poddrzewa systemu plików
  - ograniczenie zapisu do określonego poddrzewa systemu plików
- **inetd**
  - jest ważnym elementem systemu operacyjnego Linux, odpowiedzialny za uruchamianie innych programów
- **TCP Wrapper**
  - filtracja dostępu do usług sieciowych
  - przekierowanie dostępu na proxy-services
  - umożliwia realizację dual home gateway
  - pozwala ograniczać dostęp do usług uruchamianych przez xinetd
  - zarządzanie poprzez pliki
    - /etc/hosts.deny
      - PARANOID
        - blokuje pakiety pochodzące od hosta, którego ip nie posiada nazwy domenowej
      - spawn
        - pozwala odesłać do nadawcy specjalnie spreparowaną wiadomość w odpowiedzi na żądanie
    - /etc/hosts.allow
- **RSBAC - Rule Set Based Access Control**
  - zestaw rozszerzający kontrolę uprawnień
  - zestaw łat na jądro systemu Linux
  - zapewnia
    - stosowanie polityki MAC
    - system trudny do przechwycenia przez osobę niepowołaną
  - czy każdy program może zmienić uprawnienia na inne niż te, na których został uruchomiony?
    - zgodę wydaje oficer bezpieczeństwa modyfikując odpowiednio politykę bezpieczeństwa
- **SUDO**
  - uruchamianie innych aplikacji na prawach innych użytkowników
  - pozwala wykonywać dowolne polecenia bez pytania o hasło //zależy od confa

    - może prosić o hasło użytkownika

PHP

- ochrona przed command injection
    - magic_quotes_gpc
    - addslashes()
    - mysql_escape_string()
    - strip_tags()
- tryb Safe w konfiguracji modułu PHP serwera WWW
    - blokowanie wybranych funkcji
    - ograniczenie dostępu do fragmentu systemu plików
    - dostęp tylko do plików o tym samym właścicielu co skrypt
    - ograniczenie zakresu zmiennych modyfikowalnych

ACL - Access Control List; Lista kontroli dostępu

- jest narzędziem kontroli dostępu do zasobów
- umożliwia nadawanie praw (rwx) wielu użytkownikom i grupom
- maska mechanizmu ACL NIE jest definiowana dla każdego użytkownika osobno
- maska określa maksymalne prawa efektywne
- Dyrektywa "mask" w ACL
    - jest utożsamiana z uprawnieniami grupy
    - określa ukrywanie nadanych uprawnień dodatkowych użytkowników
- Jeśli ls -l plik.txt wygląda następująco *1+:
    - -rwxr-xr-x+ 1 user group 1000 2005-01-10 09:00 plik.txt
    - to "chmod 715 plik.txt" spowoduje:
        - zmniejszenie uprawnień wpisom ACL'owym
- getfacl --omit-header acl-test5
    - user::r-x
    - user:inf44444:r--
    - group::rw-
    - group:student:r-x
    - mask::rwx
    - other::--x
        - oznacza
            - użytkownik "inf44444" może czytać plik acl-test5
            - grupa właściciela może zmodyfikować plik acl-test5
- getfacl --omit-header acl-test1
    - user::rw-
    - user:junior:rwx
    - group::r--
    - group:student:r-x
    - mask::r--
    - other::---
        - oznacza

                - grupa domyślna/właściciela może odczytać plik
                - właściciel może modyfikować plik
- user::rw-
    - user:inf44444:r-x
    - group::rwx
    - group:student:rwx
    - mask::rwx
    - other::---
        - oznacza
            - użytkownik "inf44444" może wykonać plik
            - grupa "student" może skasować katalog
- user::r-x
    - user:inf44444:r--
    - group::rw-
    - group:student:r-x
    - mask::rwx
    - other::--x
        - oznacza
            - użytkownik "inf44444" może czytać plik
            - grupa właściciela może zmodyfikować plik
- Jak zachowa się system kontroli ACL standardu POSIX w przypadku użytkownika U należącego do grupy G jeśli ani U ani G nie mają jawnie przydzielonego prawa r wobec obiektu p, ale kategoria "wszyscy użytkownicy" (others) takie uprawnienie posiada
    - prawo r zostanie efektywnie przyznane bezwarunkowo
- Jak zachowa się system kontroli ACL standardu POSIX w przypadku użytkownika U należącego do grupy G i wpisanego na liście ACL obiektu p, jeśli ani U ani G nie mają jawnie przydzielonego prawa r, ale kategoria „wszyscy użytkownicy” (others) takie uprawnienie do obiektu posiada
    - prawo r do obiektu p nie zostanie efektywnie przyznane
- W przypadku systemu kontroli ACL standardu POSIX użytkownik U należący do grupy G posiada efektywne uprawnienie r do zasobu p jeśli
    - U jest właścicielem p - bez względu na zawartość ACL
    - prawo r zostanie jawnie nadane U lub G

RAID - Redundant Array of Independent Disks

- RAID 0
    - Nie oferuje żadnej redundancji
- RAID 1 - lustrzany
    - replikacja pracy dwóch lub więcej dysków fizycznych
    - odporny na awarię 2 dysków w 5-dyskowej macierzy
- RAID 6
    - odporny na awarię 2 dysków w 5-dyskowej macierzy

Sandbox

- ograniczone środowisko wykonawcze aplikacji lub jej komponentu

WIFI

- **IEEE 802.11i - WPA2 -** najbezpieczniejszy standard zabezpieczeń komunikacji w sieciach bezprzewodowych

Hot Standby Routing Protocol

- pozwala uzyskać redundancję routerów
- umożliwia transparentną dla stacji sieciowej obsługę uszkodzenia jej routera domyślnego
- oferuje trasparentną redundancję urządzeń sieciowych

SYN cookies

- identyfikuje połączenie wartością wpisywaną do pola ACK
- minimalizuje wielkość zasobów przydzielanych przy odbiorze żądania nawiązania połączenia

ARP cache detekcja snifferów

- wysłanie zapytania ICMP echo request z fałszywym adresem źródłowym IP na adres podejrzewanej stacji
- wysłanie ogłoszenia ARP o fałszywym adresie IP

VLAN

- Koncepcja "zamkniętych grup użytkowników" dotyczy odseparowania danych przetwarzanych przez odrębne grupy użytkowników tego samego środowiska sieciowego.

IDS - Intrusion Detection System

- Metoda PING stosowana przez systemy IDS polega na wysłaniu
    - zapytania ICMP echo request pod adres MAC niezgodny z odpytywanym IP i oczekiwaniu na odpowiedź
    - zapytania ICMP echo request pod adres MAC podejrzewanej stacji i oczekiwaniu na odpowiedź

NAC -Network Admission Control

- restricts access to the network based on identity or security posture
- it can force user or machine authentication prior to granting access to the network
- umożliwiają blokowanie ruchu sieciowego ze stacji nie spełniających wymagań polityki bezpieczeństwa

Zapory sieciowe

SPF - Stateful Packet Filter; filtracja kontekstowa

- pozwala uniknąć niepotrzebnego sprawdzania reguł dla pakietów powracających w ruchu zweryfikowanym w stronę przeciwną
- pozwala odrzucić pakiety próbujące podszyć się pod rzekomo istniejące połączenia
- pozwala określić czy połączenie jest już ustanowione
- dopasowuje pakiety do zapamiętanej historii komunikacji

Filtracja bezstanowa

- Statyczne reguły filtracji (filtracja bezstanowa) nie radzą sobie z precyzyjną filtracją ruchu
    - FTP, gdy serwer pracuje w trybie aktywnym (serwer FTP nawiązuje połączenie z portem klienta)
- wymaga sprawdzania reguł dla każdego pakietu
- historia komunikacji nie ma wpływu na decyzje zapory

Czy istnieje możliwość zmiany portu docelowego i adresu docelowego na adres localhost i dowolny inny port

- tak
- tylko, jeśli określimy protokół oraz oryginalny port docelowy

iptables

- umożliwia ograniczenie dostępu do usługi w jednym poleceniu
    - jeśli określamy protokół
- umożliwia określenie domyślnej polityki w łańcuchu
    - tylko w standardowych łańcuchach
- Poniższa reguła została wpisana na komputerze pełniącym rolę routera:
    - iptables -t filter -A INPUT -m state --state NEW -j DROP
        - odrzuca nowe połączenia do tego komputera
- Czy polecenie jest poprawne
    - iptables -t mangle -A PREROUTING -s localnet -d ! localnet -m ipp2p --dc -m comment --comment "zla regulka" -j TTL --ttl-set 1
        - tak, ale system będzie usuwał te pakiety
- **NAT - Network Address Translation**
    - **SNAT - Source NAT**
        - zmiana adresów źródłowych IP na inne
        - iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 150.254.17.2
        - iptables -t nat -A POSTROUTING -o eth0 -j SAME --to 150.254.17.2
    - **DNAT - Destination NAT**
        - zamiana adresów docelowych IP na inne

Klasy bezpieczeństwa

B1

- ochrony systemowych obszarów pamięci
- uwierzytelniania użytkowników
- ścisłej kontroli dostępu do danych (MAC)

Inne

Certyfikaty kwalifikowane

- ważne są nie dłużej niż 2 lata
- wywołują skutki prawne równoważne podpisowi własnoręcznemu

Podpis elektroniczny

- przewaga podpisu elektronicznego nad odręcznym
    - jest ściśle powiązany z treścią podpisywanego dokumentu
    - autentyczność podpisu można zweryfikować poprzez prostą weryfikację certyfikatu klucza publicznego podpisującego
    - samo złożenie podpisu uniemożliwia wyparcie się tego przez podpisującego

Zamaskowane kanały komunikacyjne:

- kolejka drukowania
- system plików
- obciążenie systemu

HIPS - Host Intruder Prevention System

- monitor antywirusowy
- ochrona przed atakami DoS

Szyfrowana transmisja wiadomości pocztowych

- X.400
- S/MIME
- PGP

SMTP - Simple Mail Transfer Protocol

- pozwala na wysyłanie wiadomości do innych użytkowników
- ochrona antyspamowa
    - szare listy - odesłanie komunikatu SMTP o czasowej niedostępności usługi
    - filtry Bayesa
- w standardzie SMTP serwery uwierzytelniane są na podstawie adresów

- **ESMTP**
    - standard ESMTP umożliwia uwierzytelnianie metodą zawołanie-odzew
    - standard ESMTP oferuje mechanizmy uwierzytelniania SASL i TLS

MAC - Mandatory Access Control

- "Podmiot nie może ...
    - ...zapisać danych o etykiecie niższej niż jego aktualna"
    - ...uruchomić procesu o etykiecie wyższej niż jego aktualna”
- MAC nie zezwoli podmiotowi P na dopisanie danych do zasobu Z
    - gdy zbiory kategorii przynależności danych P i Z są rozłączne
    - gdy poziom zaufania Z jest niższy niż P
- właściciel zasobu nie może dysponować prawami dostępu do tego zasobu
- właściciel zasobu nie może przekazać możliwość decydowania o uprawnieniach dostępu do tego zasobu
- etykiety ochrony danych przypisane do zasobów automatycznie wymuszają uprawnienia

Zasada spójności poziomej

- wymaga konsekwentnego zastosowania odpowiedniego mechanizmu ochrony wobec wszystkich wykorzystywanych protokołów aplikacyjnych
- Wyobraźmy sobie serwer udostępniający wybranym podsieciom dwie usługi: www i ftp. Zapewnienie kontroli dostępu, np. za pomocą narzędzia personal firewall (lub wrappera połączeń) tylko do jednej z tych usług stanowi
    - naruszenie warunków spójności poziomej zabezpieczeń

Standard IEEE 802.1x:

- realizuje autoryzację i kontrolę dostępu do lokalnej infrastruktury sieciowej
- współpracuje z protokołami takimi jak RADIUS lub TACACS+
- dotyczy zabezpieczenia poufności [chyba TAK]
- umożliwia scentralizowane uwierzytelnianie wielu punktów zdalnego dostępu
- pozwala uwierzytelniać stanowiska sieciowe przy dostępie do sieci lokalnej

Lock-and-Key; Zamek-i-klucz

- wymaga uwierzytelnienia użytkownika, np. za pomocą RADIUS-a

MS Windows

- ochrona SYSKEY
    - wzmocnienie szyfrowania postaci hash haseł użytkowników
- LM - Lan Manager - hashuje hasła (słaby)
    - LMhash
        - hasła użytkowników w postaci skrótów (hashy) wykorzystywane przez Lan Managera

    - NTLM
        - bezpieczniejszy od LM
- Kerberos jest bezpieczniejszy niż LM i NTLM
- system MS Windows korzysta z serwera Kerberos
    - jeśli zostanie odpowiednio skonfigurowany
- NTFS
    - EFS - Encrypting File System
        - rozszyfrować plik zaszyfrowany mechanizmem EFS może
            - każdy agent DRA istniejący w momencie deszyfrowania pliku
            - właściciel pliku
    - dziedziczenie uprawnień
        - uprawnienia są pobierane bezpośrednio z uprawnień obiektu wyższego
- Zapora sieciowa wbudowana w Ms Win XP sp2
    - jest zaporą typu statefull
- Ukrycie widoczności systemu Ms Win spowoduje: (Chodzi o ukrycie w otoczeniu sieciowym)
    - ukrycie systemu przed innymi systemami
- Nazwa konta "administrator" w systemie Ms Windows XP
    - można zmienić w każdej chwili

PGP - Pretty Good Privacy

- w systemie Ms Windows można korzystać z szyfrowania PGP
    - jeżeli wykorzysta się odpowiednie oprogramowanie
- publikowanie klucza publicznego PGP
    - umożliwia zaszyfrowanie wiadomości adresowanej do właściciela klucza
    - umożliwienie sprawdzenia autentyczności listu wysłanego przez właściciela klucza
- Zastosowanie rozszerzenia Enigmail w kliencie poczty Thundebird pozwala na
    - wykorzystywanie PGP do szyfrowania i podpisywania wiadomości
    - ochronę przed atakami man-in-the-middle

IPv6

- oferuje mechanizm AH w celu zapewnienia autentyczności
- oferuje mechanizm ESP w celu zapewnienia poufności

SUID

- Flaga suid (bit uprawnień) wg standardu POSIX 1003.1
    - oznacza przejęcie przez proces uprawnień właściciela pliku, z którego proces został uruchomiony
- powoduje wykonanie aplikacji z uprawnieniami właściciela aplikacji

FTP

- połączenie aktywne
    - sytuacja w której serwer ftp tworzy połączenie do klienta na losowy wybrany port

przez klienta aby przesłać żądany plik
- połączenie pasywne
    - połączenie w którym klient informuje serwer aby to on określił port a klient połączy się z tym portem i pobierze dane

exploiting
- wykorzystanie do ataku znanych luk w systemie atakowanym

Capabilities
- Mechanizm umożliwiający przydzielenie poszczególnych uprawnień administracyjnych (uprzywilejowanych operacji jądra systemu operacyjnego) użytkownikom

Niezaprzeczalność
- potwierdza, że
    - nadawca wiadomości faktycznie ją wysłał
    - odbiorca wiadomości faktycznie ją otrzymał

TUN/TAP
- komponent pozwalający tworzyć wirtualne interfejsy sieciowe

pytania nieopracowane:
63
68
83
91
93
98
121
129
141
142
148
200
201
213