Zarządzanie bezpieczeństwem systemów informatycznych

Zagadnienia

1. **Narzędzia**
   - systemy NAC (*Network Admission Control*)
   - systemy IDS (*Intrusion Detection Systems*) / IPS (*Intrusion Prevention Systems*)
   - przynęty (*honey-pot, honey-net*)
2. **Monitorowanie zabezpieczeń**
3. **Aktualizacja systemów operacyjnych**
4. **Inne dziedziny bezpieczeństwa**

Narzędzia zarządzania

Ochrona

Klasy narzędzi

- filtracja dostępu i ruchu sieciowego – zapory sieciowe
- kontrola dostępu na poziomie poszczególnych użytkowników i zasobów
- kontrola stopnia aktualizacji systemu operacyjnego / aplikacji (weryfikacja zainstalowania poprawek wydanych przez producenta)
- kontrola występowania innych znanych słabości w konfiguracji

Narzędzia zarządzania

Filtracja dostępu i ruchu

filtracja ruchu RFC 1918

- ruch przychodzący z sieci publicznej (i wychodzący do niej) z dowolnymi adresami należącymi do puli prywatnych

filtracja ruchu RFC 2827

- ruch przychodzący z sieci publicznej z adresów należących do sieci wewnętrznej
- localhost
- ruch multicast (o ile właściwe): 224.0.0.0/4
- adresy nieprzydzielone przez IANA ani przez ARIN
  (tzw. bogons, np. 1.0.0.0/8, 169.254.0.0/16 czy 192.0.2.0/24)
  http://www.completewhois.com/bogons/
- inne zastrzeżone adresy

Narzędzia zarządzania

Filtracja dostępu i ruchu

szczególnie niebezpieczne usługi

Internet:	systat	11 / tcp / udp
	chargen	19 / tcp / udp
	TFTP	69 / tcp / udp
	talk	517 / udp
	ntalk	518 / udp
	IRC	6667 / tcp
Windows:	UPnP	1900 / tcp / udp
	SSDP	5000 / tcp / udp
MS Network:	NetBus	12345 / tcp i 12346 / tcp
	BackOrifrice	31337 / tcp / udp

Narzędzia zarządzania

Filtracja dostępu i ruchu

szczególnie niebezpieczne usługi

DDoS:	trin00	27665 / tcp, 27444 / udp, 31335 / udp
	trinity v3	33270 / tcp i 39168 / tcp
	stacheldracht	16660 / tcp i 65000 / tcp
	subseven	2222, 6711, 6712, 6776, 6669, 7000 / tcp

wychodzące w sieć publiczną pakiety traceroute: 33400, 34400 / udp

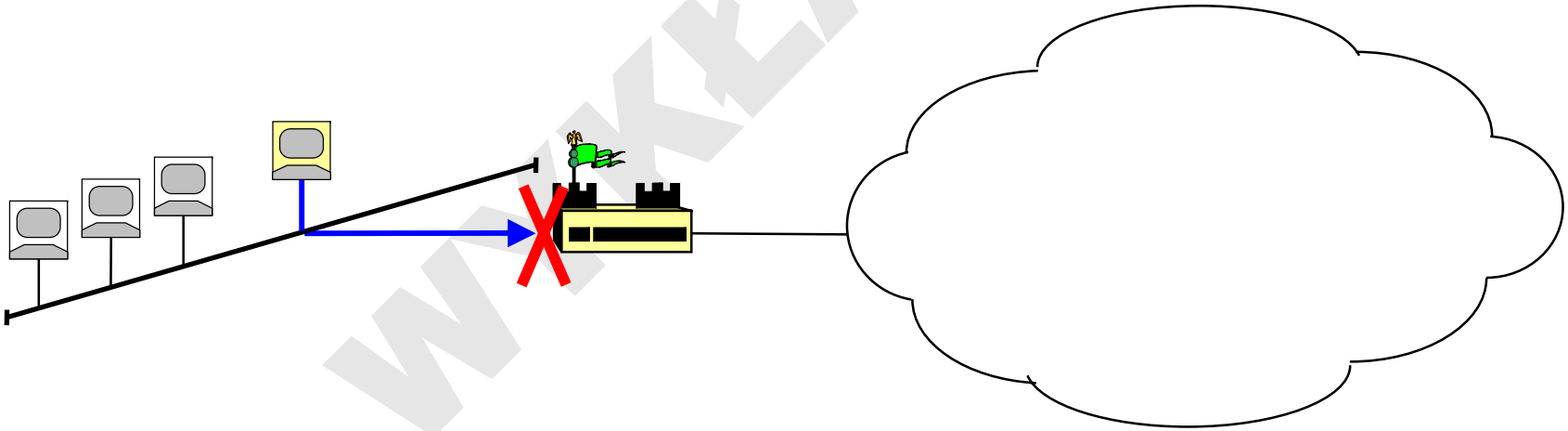
(analiza ich zawartości umożliwia napastnikowi odkrycie struktury sieci wewnętrznej)

Narzędzia zarządzania

Kontrola dostępu

metoda „zamka i klucza” (*lock-and-key*)

- wykorzystywana w sytuacji, gdy normalnie dostęp (zdalne wejście lub wyjście z sieci) jest blokowany:

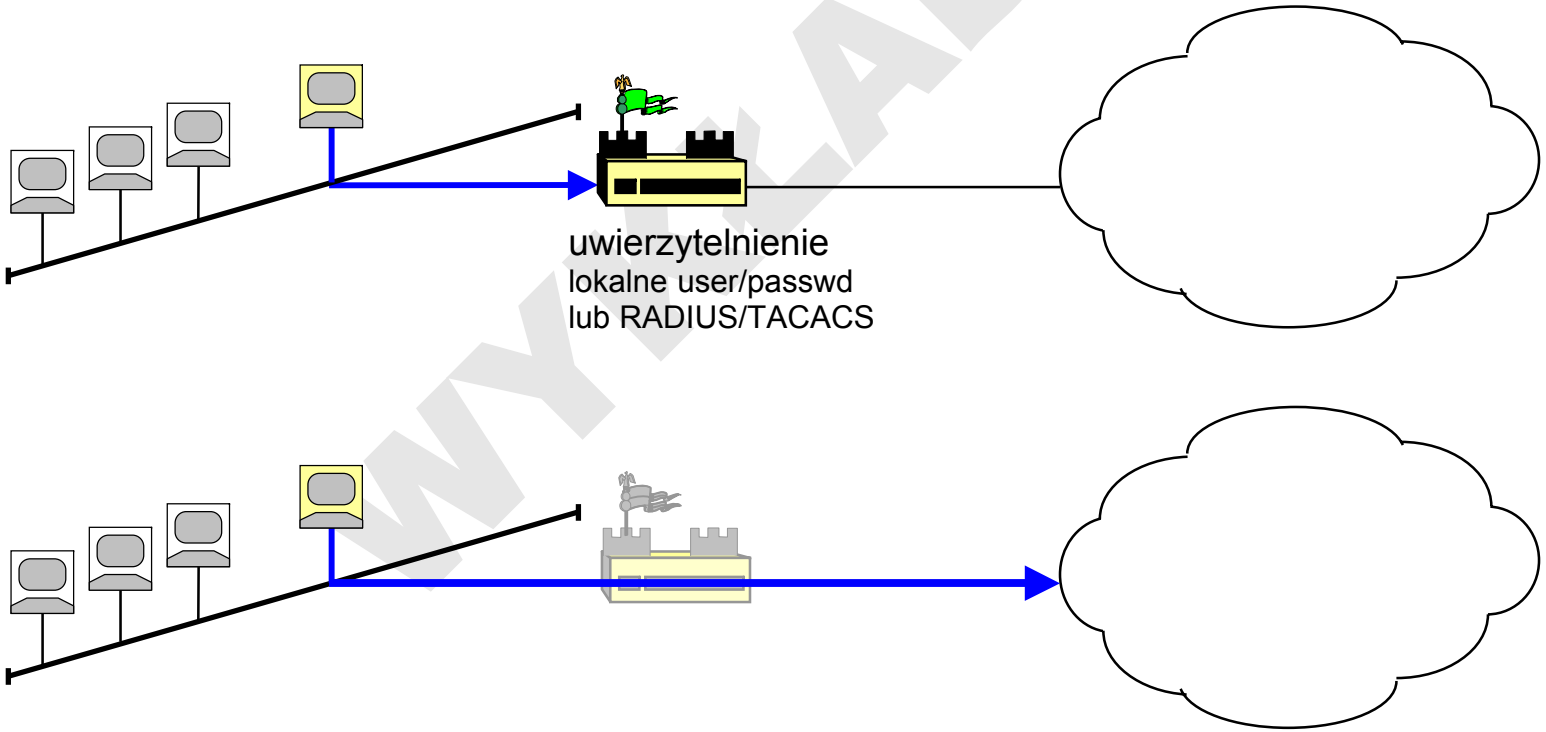


Narzędzia zarządzania

Kontrola dostępu

metoda „zamka i klucza” (*lock-and-key*)

- jednak uwierzytelnione sesje są uprawnione do obejścia blokady:



Narzędzia zarządzania

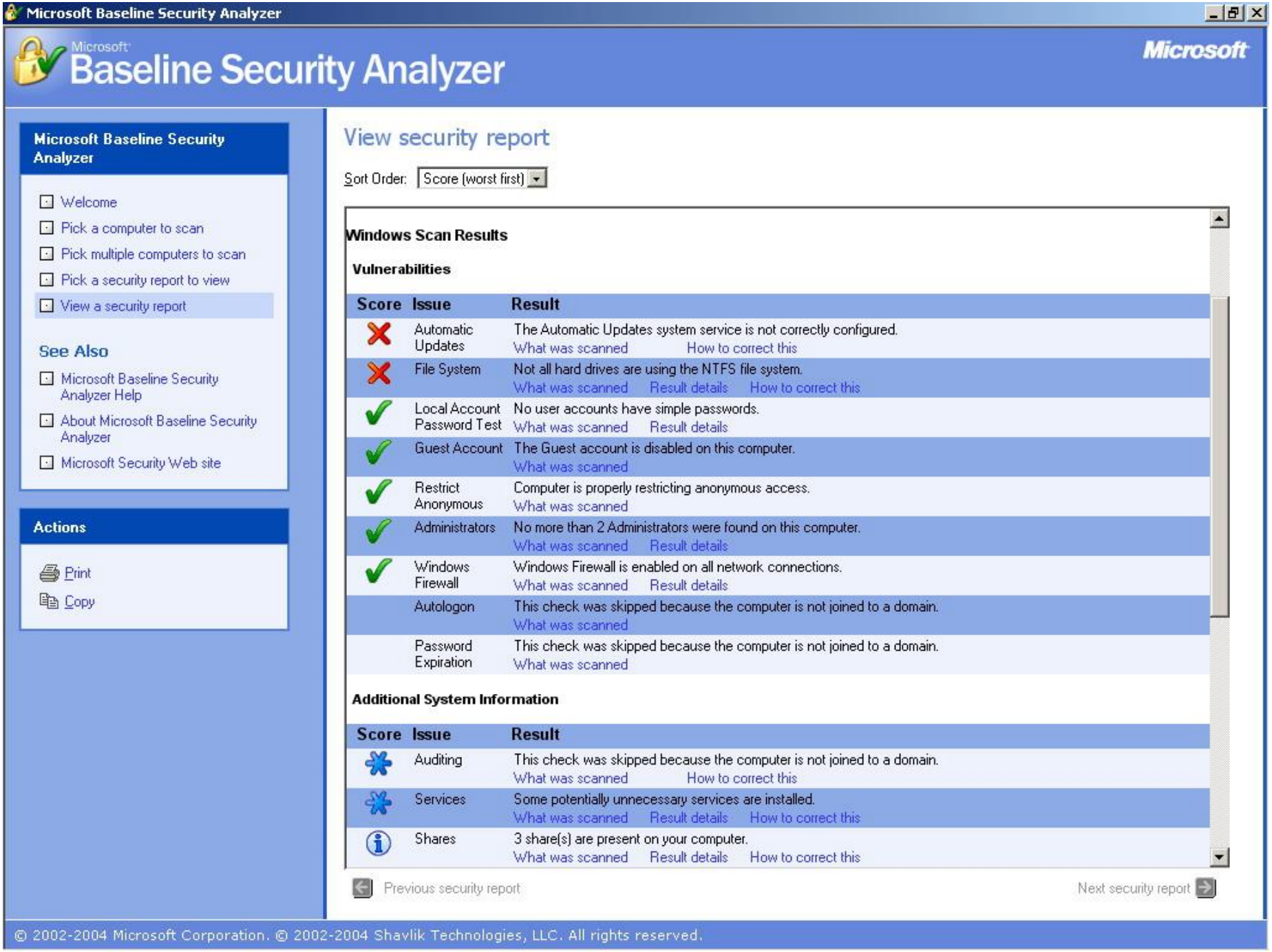
Monitorowanie konfiguracji systemu operacyjnego:

- Microsoft Baseline Security Analyzer

  http://www.microsoft.com/mbsa

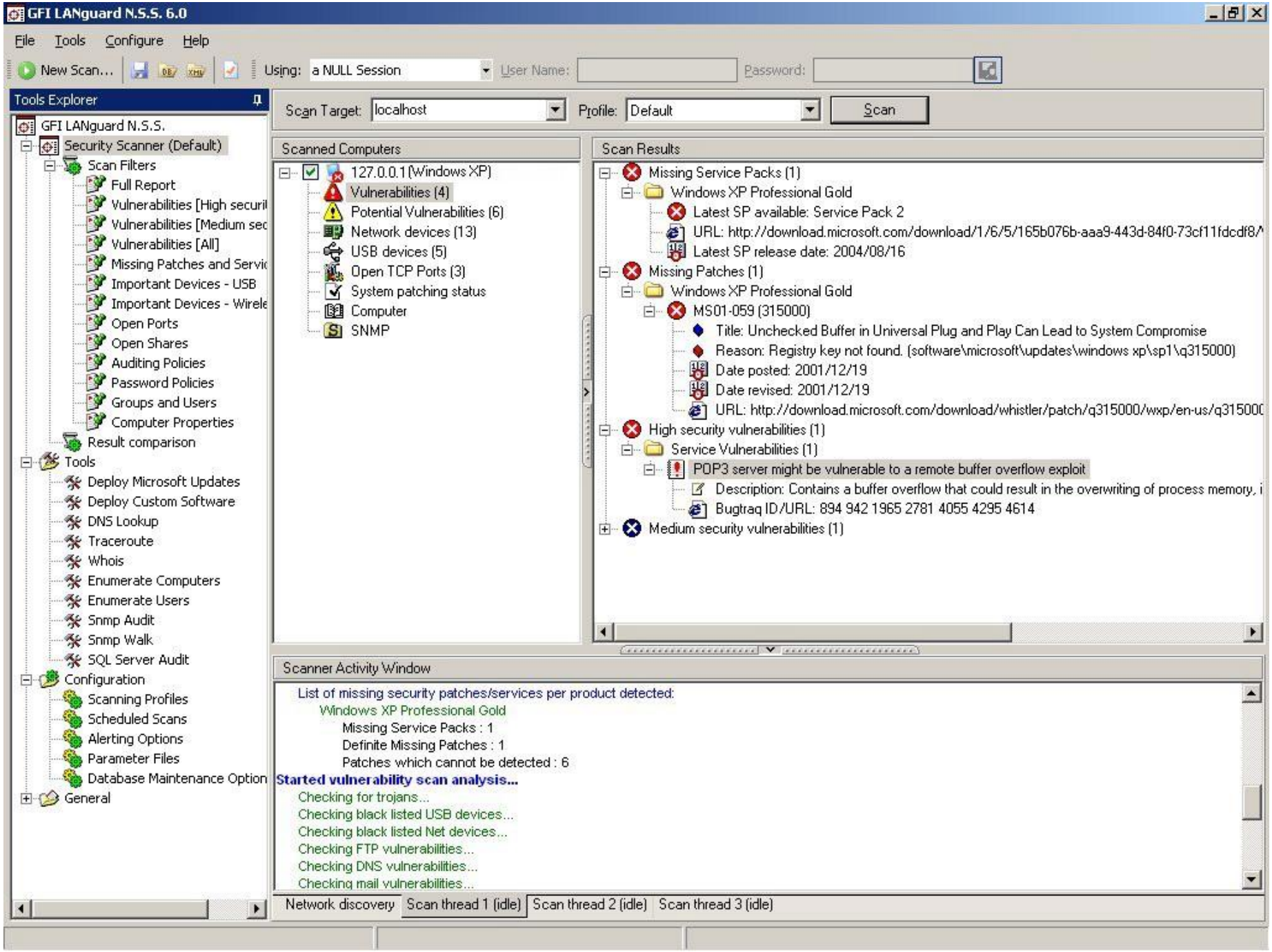
  http://www.microsoft.com/technet/security/tools/mbsahome.mspx

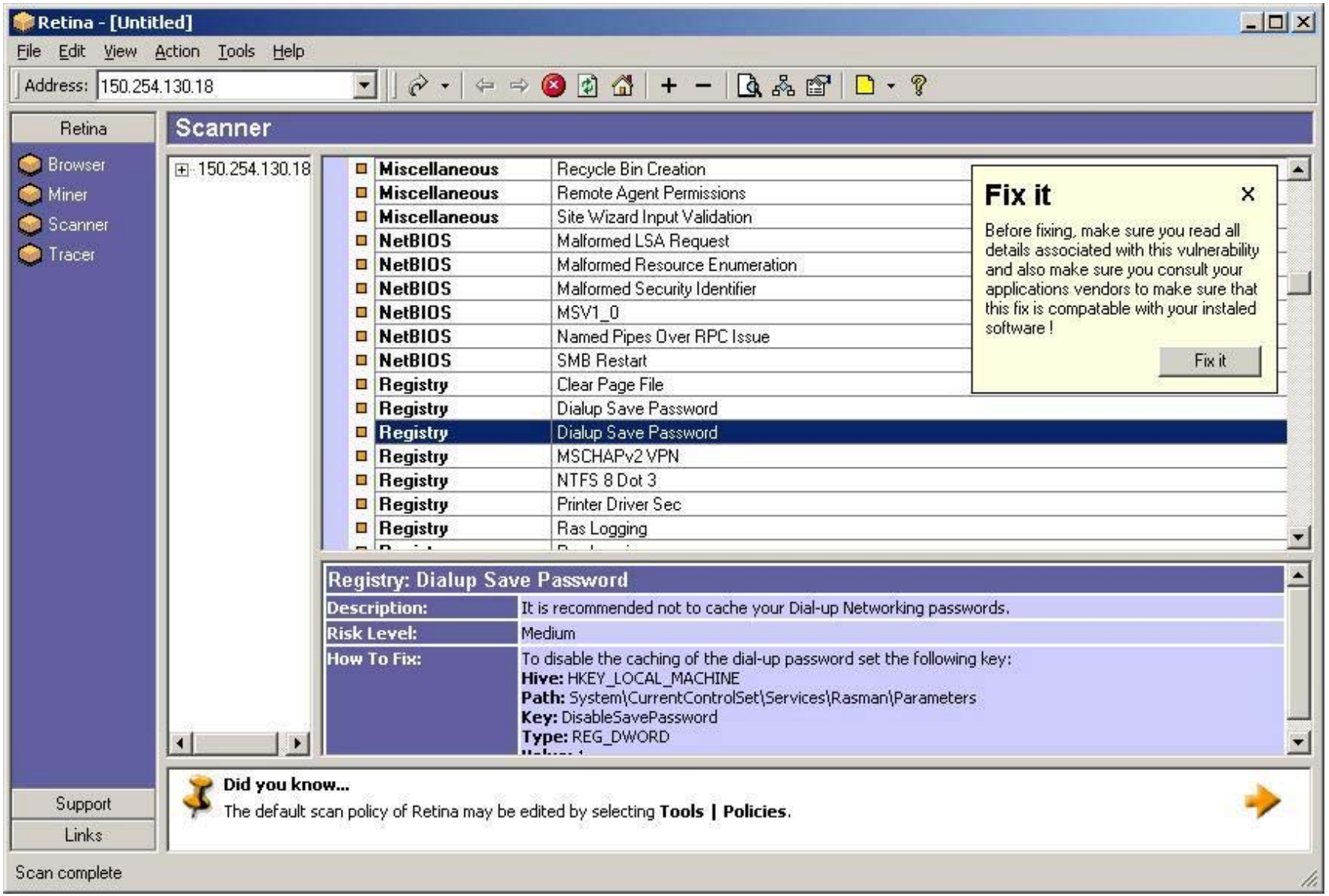
- MOM – Microsoft Operations Manager
  - m.in. zarządzanie zdalne i zdalny monitor (tester) konfiguracji


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
View security report
Sort Order: Score (worst first)
Windows Scan Results
Vulnerabilities
Score Issue Result
Automatic Updates
The Automatic Updates system service is not correctly configured.
What was scanned How to correct this
File System
Not all hard drives are using the NTFS file system.
What was scanned Result details How to correct this
Local Account Password Test
No user accounts have simple passwords.
What was scanned Result details
Guest Account
The Guest account is disabled on this computer.
What was scanned
Restrict Anonymous
Computer is properly restricting anonymous access.
What was scanned
Administrators
No more than 2 Administrators were found on this computer.
What was scanned Result details
Windows Firewall
Windows Firewall is enabled on all network connections.
What was scanned Result details
Autologon
This check was skipped because the computer is not joined to a domain.
What was scanned
Password Expiration
This check was skipped because the computer is not joined to a domain.
What was scanned
Additional System Information
Score Issue Result
Auditing
This check was skipped because the computer is not joined to a domain.
What was scanned How to correct this
Services
Some potentially unnecessary services are installed.
What was scanned Result details How to correct this
Shares
3 share(s) are present on your computer.
What was scanned Result details How to correct this
Previous security report
Next security report
© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

Narzędzia zarządzania

- protoplasci współczesnych skanerów luk bezpieczeństwa: Internet Security Scanner (**ISS** – http://www.iss.net), Security Administrator Tool for Analyzing Networks (**SATAN** – http://www.porcupine.org/satan/, http://www.fish.com/satan/), **Cybercop** Scanner (http://www.mcafeesecurity.com)
- **LanGuard NSS** (http://www.gfi.com/lannetscan/) *Network Security Scanner* firmy GFI Software – bardzo szczegółowa analiza systemu operacyjnego i aplikacji
- **RETINA** (http://www.eeye.com) firmy eEye Digital Security – wykorzystuje zaawansowane mechanizmy heurystyczne CHAM (*Common Hacker Attack Methods*)
- **NetRecon** (http://enterprisesecurity.symantec.com) – systematycznie aktualizowana baza luk; mechanizm samouczenia – wykorzystanie wiedzy nabytej przy skanowaniu jednego stanowiska do oceny zabezpieczeń następnych


GFI LANguard N.S.S. 6.0
File Tools Configure Help
New Scan... Using: a NULL Session User Name: Password:
Tools Explorer
GFI LANguard N.S.S.
Security Scanner (Default)
Scan Filters
Full Report
Vulnerabilities [High securil
Vulnerabilities [Medium sec
Vulnerabilities [All]
Missing Patches and Servic
Important Devices - USB
Important Devices - Wirele
Open Ports
Open Shares
Auditing Policies
Password Policies
Groups and Users
Computer Properties
Result comparison
Tools
Deploy Microsoft Updates
Deploy Custom Software
DNS Lookup
Traceroute
Whois
Enumerate Computers
Enumerate Users
Snmp Audit
Snmp Walk
SQL Server Audit
Configuration
Scanning Profiles
Scheduled Scans
Alerting Options
Parameter Files
Database Maintenance Option
General
Scan Target: localhost Profile: Default Scan
Scanned Computers
127.0.0.1 (Windows XP)
Vulnerabilities (4)
Potential Vulnerabilities (6)
Network devices (13)
USB devices (5)
Open TCP Ports (3)
System patching status
Computer
SNMP
Scan Results
Missing Service Packs (1)
Windows XP Professional Gold
Latest SP available: Service Pack 2
URL: http://download.microsoft.com/download/1/6/5/165b076b-aaa9-443d-84f0-73cf11fdcdf8/
Latest SP release date: 2004/08/16
Missing Patches (1)
Windows XP Professional Gold
MS01-059 (315000)
Title: Unchecked Buffer in Universal Plug and Play Can Lead to System Compromise
Reason: Registry key not found. (software\microsoft\updates\windows xp\sp1\q315000)
Date posted: 2001/12/19
Date revised: 2001/12/19
URL: http://download.microsoft.com/download/whistler/patch/q315000/wxp/en-us/q315000
High security vulnerabilities (1)
Service Vulnerabilities (1)
POP3 server might be vulnerable to a remote buffer overflow exploit
Description: Contains a buffer overflow that could result in the overwriting of process memory, i
Bugtraq ID/URL: 894 942 1965 2781 4055 4295 4614
Medium security vulnerabilities (1)
Scanner Activity Window
List of missing security patches/services per product detected:
Windows XP Professional Gold
Missing Service Packs : 1
Definite Missing Patches : 1
Patches which cannot be detected : 6
Started vulnerability scan analysis...
Checking for trojans...
Checking black listed USB devices...
Checking black listed Net devices...
Checking FTP vulnerabilities...
Checking DNS vulnerabilities...
Checking mail vulnerabilities...
Network discovery
Scan thread 1 (idle)
Scan thread 2 (idle)
Scan thread 3 (idle)


Retina - [Untitled]
File Edit View Action Tools Help
Address: 150.254.130.18
Retina
Browser
Miner
Scanner
Tracer
Support
Links
Scanner
150.254.130.18
Miscellaneous Recycle Bin Creation
Miscellaneous Remote Agent Permissions
Miscellaneous Site Wizard Input Validation
NetBIOS Malformed LSA Request
NetBIOS Malformed Resource Enumeration
NetBIOS Malformed Security Identifier
NetBIOS MSV1_0
NetBIOS Named Pipes Over RPC Issue
NetBIOS SMB Restart
Registry Clear Page File
Registry Dialup Save Password
Registry Dialup Save Password
Registry MSCHAPv2 VPN
Registry NTFS 8 Dot 3
Registry Printer Driver Sec
Registry Ras Logging
Fix it
Before fixing, make sure you read all details associated with this vulnerability and also make sure you consult your applications vendors to make sure that this fix is compatable with your instaled software !
Fix it
Registry: Dialup Save Password
Description: It is recommended not to cache your Dial-up Networking passwords.
Risk Level: Medium
How To Fix: To disable the caching of the dial-up password set the following key:
Hive: HKEY_LOCAL_MACHINE
Path: System\CurrentControlSet\Services\Rasman\Parameters
Key: DisableSavePassword
Type: REG_DWORD
Did you know...
The default scan policy of Retina may be edited by selecting Tools | Policies.
Scan complete

Narzędzia zarządzania

- **Nessus** (www.nessus.org) autorstwa Renauda Deraison – model wtyczek (*plug-in*) pozwala swobodnie dodawać moduły skanujące
- **Nikto** – skaner luk bezpieczeństwa wykorzystujący rozszerzoną bibliotekę Whisker (autorstwa Rain Forest Puppy)
- **Stealth** (http://www.nstalker.com) – skanowanie serwisów www
- **Curl** (http://curl.haxx.se) – testowanie luk wielu protokołów aplikacyjnych: telnet, FTP, HTTP, SSL, LDAP ...

Zautomatyzowane sondowanie

- **nmap** / **nmapwin** – zaawansowane skanowanie protokołów i portów (np. metodą fragmentacji, odbijania FTP itp.), detekcja systemu operacyjnego

Narzędzia zarządzania

Zdalne monitorowanie

Przykładowy serwis: http://security.symantec.com/

Systemy nadzoru stanowisk sieciowych

Network Admission Control

Cel:

- zdalna weryfikacja w sieci lokalnej / korporacyjnej, czy poszczególne stanowiska sieciowe spełniają wymagania polityki bezpieczeństwa, np. w zakresie kontroli antywirusowej czy uaktualnień systemu operacyjnego
- stanowiska nie spełniające wymagań są odcinane od sieci rozległej lub kręgosłupowej, ewentualnie otrzymują możliwość ograniczonej komunikacji z innymi segmentami / podsieciami

Systemy nadzoru stanowisk sieciowych

Komponenty systemu NAC:

Serwer Kontroli Dostępu (Policy Server / Secure Access Control Server)

- instalowany na stacji administracyjnej, analizuje informacje o stanie bezpieczeństwa pobrane ze stacji sieciowych i podejmuje decyzje o dopuszczeniu ich do sieci

Lokalny agent nadzoru (Trust Agent)

- instalowany na stacjach sieciowych, zbiera informacje o stanie bezpieczeństwa systemu od innych modułów programowych (np. aplikacji antywirusowych)

Network Access Devices

- węzły międzysieciowe (lub zapory sieciowe) pośredniczą z przekazywaniu tych informacji do Serwera Kontroli Dostępu
- na podstawie jego decyzji blokują/ograniczają ruch

Systemy IDS
(*Intrusion Detection Systems*)

- monitorowanie ruchu sieciowego w celu wykrycia zagrożeń:
  - podejrzanej aktywności (skanowania portów, adresów sieciowych)
  - podejrzanej zawartości pakietów (wirusów)
  - dostępu do usług informacyjnych i katalogowych
  - ataków DoS

  na podstawie bazy wzorców ataków
- raportowanie stanu bezpieczeństwa
- pułapki / przynęty – IPS (*Intrusion Prevention Systems*)
  - mają za zadanie skierować intruza w „ślepy zaułek” (fałszywe serwery) odwodząc go od serwerów właściwych
  - dając administratorowi czas na reakcję

Systemy IDS

Systemy IDS / IPS mogą pracować jako:

Host IDS (HIDS/HIPS)

- ochrona lokalnego systemu operacyjnego / aplikacji (np. przed buffer overflow)

Network IDS

- wydzielone stacje sieciowe w sieci lokalnej, np. eTrust Intrusion Detection (CA)
- moduły urządzeń sieciowych, np. Catalyst 6000 IDS Module (Cisco)
- zestaw wielokomponentowy, np. BlackICE (Network ICE), NetProwler (Symantec) obejmujący m.in.:
  - monitor sieci (BlackICE Sentry/Guard)
  - agentów nadzoru stanowisk sieciowych (BlackICE Agent, NetProwler Agent)
  - centralnego zarządcę (ICEcap Manager, NetProwler Manager/Console)

Systemy IDS

Metody detekcji:

- analiza pochodzenia i intensywności strumienia ruchu
- rozpoznawanie zagrożeń na podstawie tzw. sygnatur – wzorców niebezpiecznych pakietów (adresów źródłowych, portów, korelacji pomiędzy wartościami pól nagłówka)

ID	Signature Title	Type
1100	IP Fragment attack	Attack
1103	IP Fragments Overlap	Attack
1107	IP Source Address Private (RFC1918)	Attack
2151	Large ICMP Traffic	Attack
2154	Ping of Death attack	Attack
3040	TCP NULL flags	Attack
3041	TCP SYN+FIN flags	Attack
3042	TCP FIN only flags	Attack
4050	UDP Bomb attack	Attack
4051	UDP Snork attack	Attack
4052	UDP Chargen DoS attack	Informational
6052	DNS Zone Transfer from High Port	Informational
6190	statd Buffer Overflow	Attack

Systemy IDS

Problem wydajności systemów IDS / IPS

- jest ponad 1000 (!) wzorców ataków (sygnatur)
- w niektórych przypadkach wymagana jest analiza całego pakietu
- do tego może być niezbędna analiza stanu sesji itp.
- problem zwłaszcza specjalizowanych modułów routerów filtrujących
  - zwykle kilkadziesiąt Mb/s
  - chociaż np. sensor IDS Cisco serii 4200 ma nominalną wydajność rzędu Gb/s

Systemy IDS

Ataki na systemy IDS:

Techniki Anti-IDS (AIDS):

- ukrywanie cech charakterystycznych (modyfikacja sygnatur)
- fragmentacja
- ataki DoS na systemy IDS
- przykład: Whisker (ataki na WWW z predefiniowanymi sposobami obejścia IDS)

Detektory snifferów

Popularne metody detekcji snifferów

- metoda DNS
- metoda ARP
- metoda ARP cache
- metoda PING
- metoda ICMP delta (*latency test*)

Metoda DNS

Idea

- monitorowanie ruchu w sieci pod kątem zapytań o adresy IP kierowane do serwera DNS (*reverse DNS lookup*)
- często wykonywanych przez sniffery w celu zapisania informacji o nazwach stacji w przechwyconych pakietach

Ograniczenia

- konieczny dostęp do całości ruchu w naszej sieci lokalnej – bez mostowania / przełączania (w przypadku przełącznika – wpięcie do portu monitorującego)

Metoda ARP

Idea

- normalne zapytania ARP kieruje się pod rozgłoszeniowy adres MAC
- ale karta sieciowa pracująca w trybie promiscuous będzie odbierać również ramki skierowane pod inne adresy i przekazywać wyżej (np. do stacji protokołu ARP)
- i stacja ARP na nie odpowie

Ograniczenia

- aby stacja ARP odpowiedziała, trzeba spreparować zapytanie o specyficzny adres, najczęściej broadcast lub multicast: FF:FF:FF:FF:FF:FF, FF:FF:FF:FF:FF:FE, FF:FF:00:00:00:00, FF:00:00:00:00:00, 01:00:5E:00:00:01
- nie wszystkie implementacje jednakowo reagują (nie na każdy adres odpowiadają)

Metoda ARP cache

Idea

- podobnie: karta sieciowa w trybie promiscuous przechwyci ramki skierowane pod adresy inne niż rozgłoszeniowe (np. FF:FF:FF:FF:FF:FE)
- np. ramkę ARP z ogłoszeniem nowego adresu IP, którego faktycznie nie przydzielono żadnemu stanowisku, np. "192.168.0.254, o adresie MAC AA:AA:AA:AA:AA:AA"
- stacja ARP na komputerze sniffera odbierze ramkę i zachowa te adresy w cache
- następne zapytanie ICMP *echo request* z adresem źródłowym (!) 192.168.0.254 spowoduje pojawienie się odpowiedzi *echo reply* bez uprzedniego zapytania ARP o ten adres

Ograniczenia

- musimy wiedzieć dokąd skierować zapytanie ICMP – kogoś podejrzewamy
- odpytujemy podejrzane lub wszystkie adresy IP w sieci

Metoda PING

Idea

- normalne zapytanie ICMP *echo request* do określonego adresu IP wysyłane jest w ramce MAC skierowanej pod adres MAC odpowiadający temu adresowi IP
- karta sieciowa w trybie promiscuous odbierze ramkę nawet jeśli adres MAC nie będzie odpowiadać odpytywanemu IP
- i ostatecznie pojawi się odpowiedź *echo reply*

Ograniczenia

- odpytujemy podejrzane lub wszystkie adresy IP w sieci

Metoda ICMP delta

Idea

- porównanie różnic w czasach odpowiedzi ICMP (lub dowolnych innych) w przypadku obciążenia karty odpytywanego stanowiska
- kartę sieciową pracującą w trybie promiscuous łatwo obciążyć generując w sieci dużo ramek skierowanych pod fałszywe adresy MAC
- i porównać czas odpowiedzi z przypadkiem znikomego ruchu w sieci

Ograniczenia

- zakładamy, że uda się szumem komunikacyjnym dostatecznie obciążyć CPU stanowiska podsłuchującego
- nieskuteczne, gdy sieć pasmo sieci normalnie jest już znacząco wykorzystane

Detektory snifferów

Przykłady detektorów snifferów

- Antisniff Unix: http://packetstorm.linuxsecurity.com/sniffers/antisniff/
- Anasil: http://www.anasil.net
- Cain: http://www.oxid.it/cain.html
- Sentinel: http://www.mirrors.wiretapped.net/security/network-monitoring/sentinel
- Neped: http://www.securiteam.com/tools/Neped
- Promiscan Windows: http://www.securityfriday.com
- Hunt: http://packetstormsecurity.nl/sniffers/hunt/
- Sniffdet: http://sniffdet.sourceforge.net/
- L0pth Antisniff (najbogatszy zestaw metod)

Detektory ataków DoS / DDoS

Przykłady detektorów ataków DoS / DDoS

- Peakflow (komercyjny Arbor Networks): http://www.arbornetworks.com
- Snort (open source): http://www.snort.org
- moduł IDS systemu Finesse (Cisco PIX)
- moduły HIPS zapór personal firewall (np. Kerio, Norton Internet Security, McAfee Desktop Firewall)
- proste reguły zapór sieciowych (np. iptables)

- SYN cookies: SYN Defender (Firewall-1), PIX, jądro Linuksa (od v.2.4)

Przynęty

System wabiący

- dedykowany niezabezpieczony system, którego celem jest zebranie informacji o ataku i atakującym oraz odciągnięcie jego uwagi od rzeczywistego chronionego systemu
- systemy jednostanowiskowe – honey-pot
- podsieci – honey-net
- gromadzą relatywnie małe ilości danych, które mają zwykle bardzo dużą wartość

Przykłady:

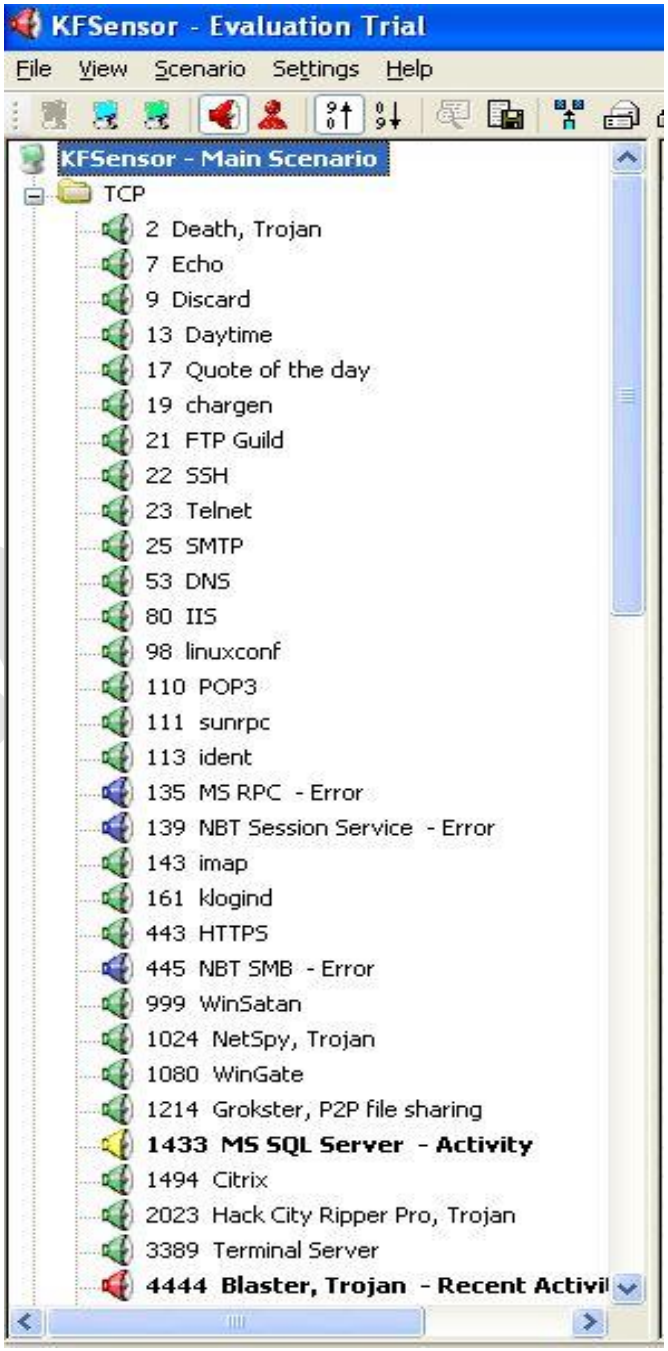
- Windows: KFSensor, Symantec ManTrap, BackOfficer friendly
- Linux/BDS: SmallPot, Tiny Honeypot

www.honeynet.org

Przynęty

KFSensor

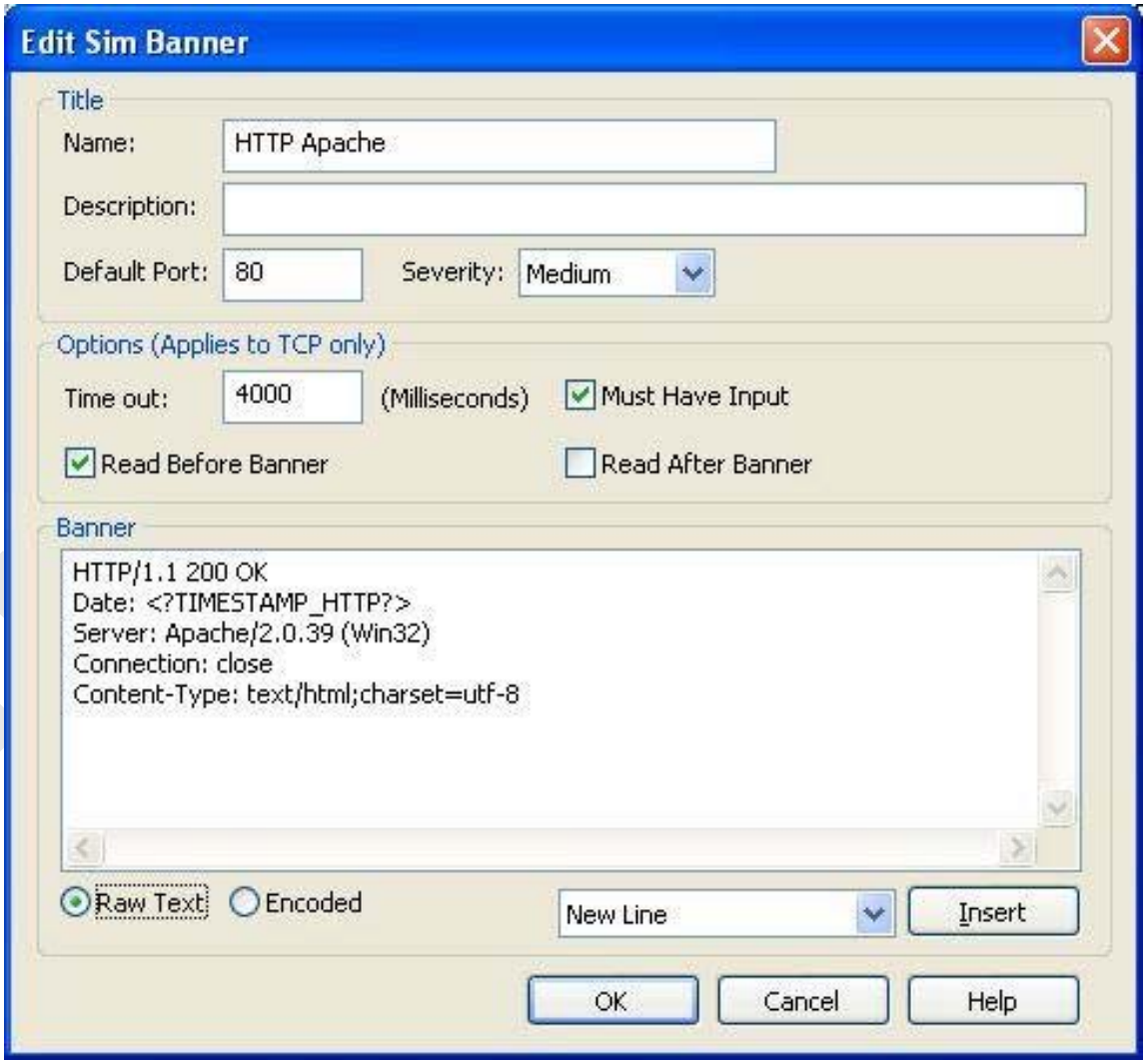
- wiele symulowanych usług



Przynęty

KFSensor

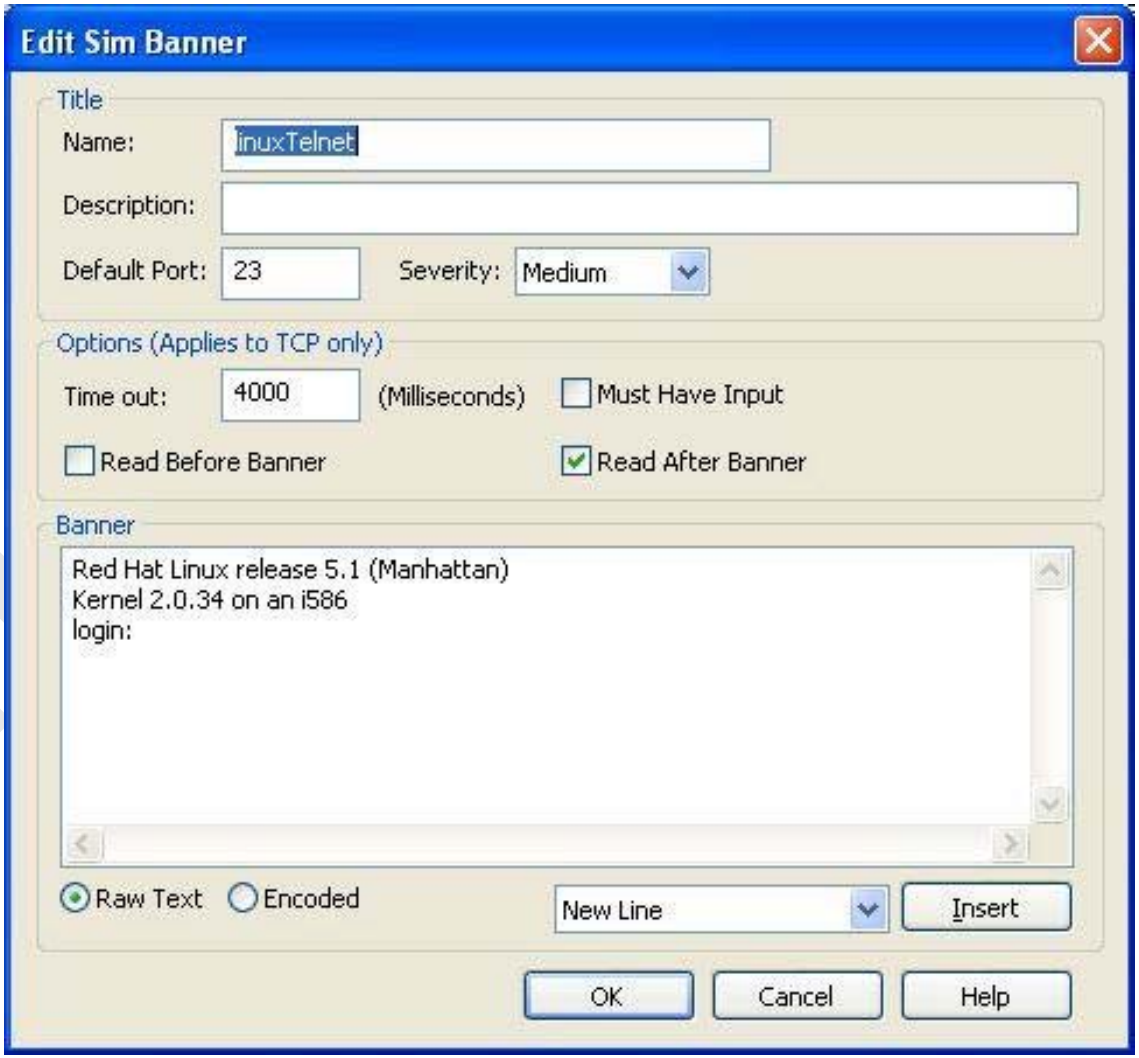
- własne definicje zachowania usług



Przynęty

KFSensor

- możliwość dodawania własnych usług



http://project.honeynet.org

http://www.lucidic.net

http://www.thdp.org

http://www.cisecurity.org

Kompleksowe systemy nadzoru sieci

CryptoSystem (RADguard)

1) **CryptoWall – urządzenie dedykowane**
   - zapora sieciowa (filtracja pakietów IP)
   - szyfracja (VPN)
   - rejestr zdarzeń
   - interfejsy Ethernet + wyjście *alarm signal*
2) **CryptoWall – konsola zarządzająca**
   - monitorowanie
   - konfigurowanie
   - dostępne dla HP OpenView for MSWindows
3) **CryptoCA (Certification Authority)**
   - dostępne razem z CryptoWall

Kompleksowe systemy nadzoru sieci

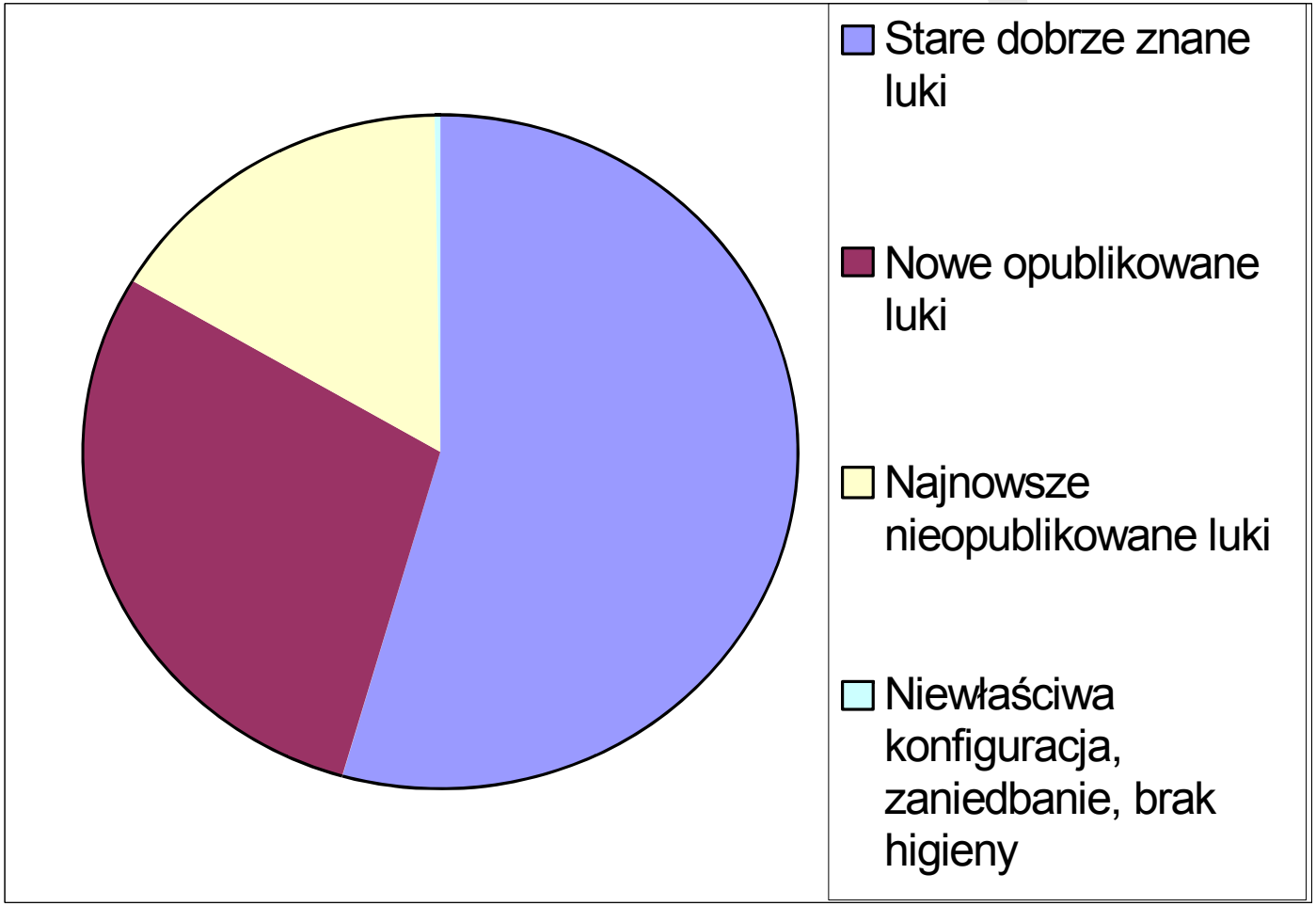
Border Manager (Novell)

- Firewall Services – zapora sieciowa
- hierarchiczne proxy-cache – m.in. filtracja wybranych połączeń (Cyber Patrol)
- VPN Services – szyfrowany kanał TCP/IP pomiędzy sieciami (3DES, RC2, RC5, IPsec, SKIP)
- IPX/IP gateway (ten sam co w IntranetWare) m.in. serwer DNS
- single sign-on (obsługa protokołu LDAP umożliwia dostęp do NDS)
- uwierzytelnianie za pomocą tokenów, kart chipowych, czytników biometrycznych
- dostęp do NDS umożliwia alternatywne posługiwanie się adresem zarówno IP, FQDN jak i nazwą obiektu NDS

- **Border Manager Authentication Service** – uwierzytelnianie zdalnych użytkowników (RADIUS zintegrowany z NDS), monitoring sesji i rozliczanie kosztów zdalnej łączności

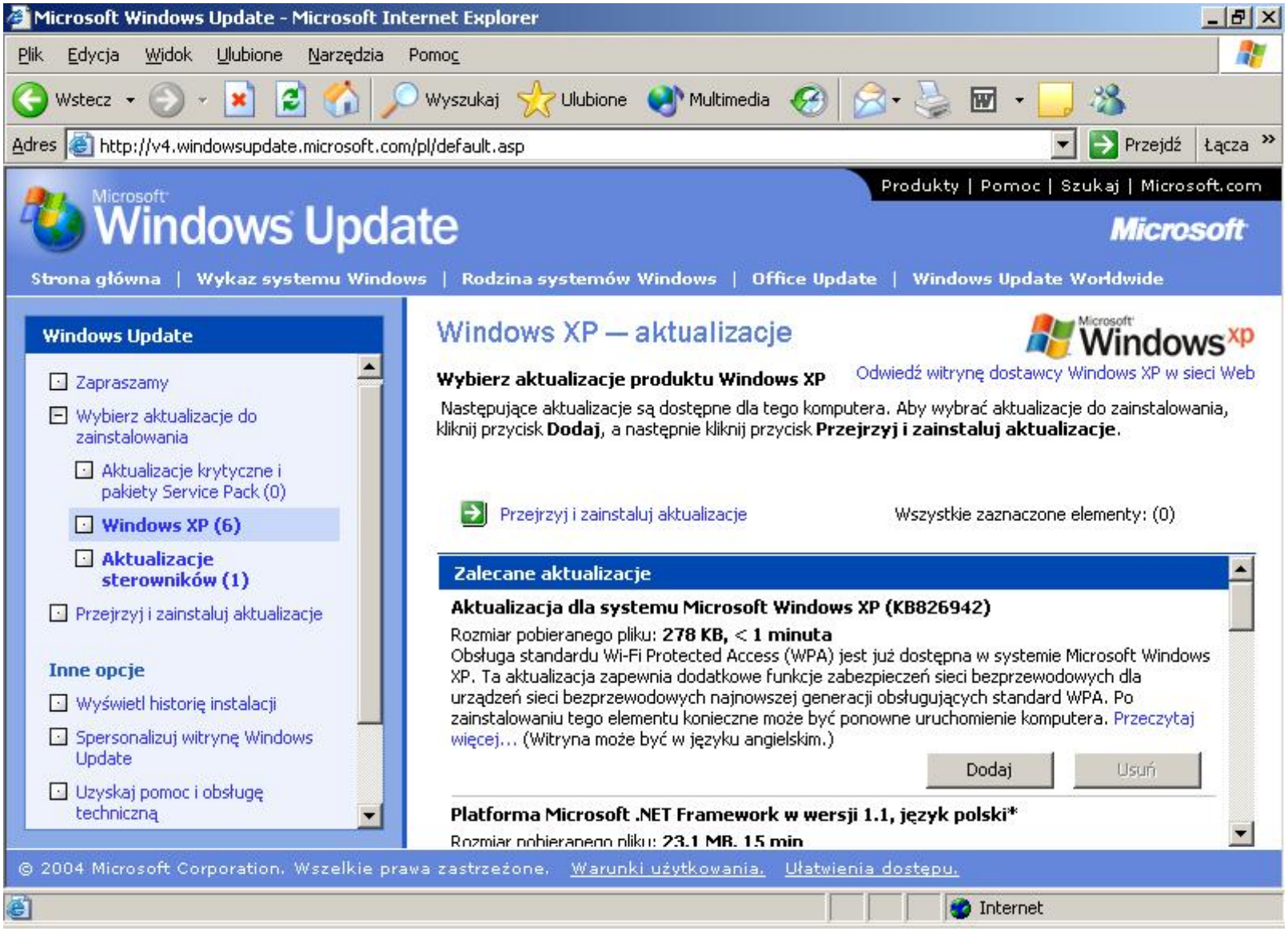
Aktualizacja systemów

Przyczyny udanych włamań:



Aktualizacja systemów

Windows



Aktualizacja systemów

Windows

- podstawowe grupy poprawek Microsoft Windows:
  - krytyczne (również Service Pack)
  - zalecane
  - sterowników (nowsze wersje)
- inne aktualizacje:
  - Development Kit – dla projektantów
  - Feature Pack – nowa funkcja produktu, która jest najpierw rozpowszechniana poza kontekstem wersji produktu, a następnie zwykle dołączana do następnej pełnej wersji produktu

Aktualizacja systemów

Windows

Schemat nazewnictwa pakietów aktualizacji oprogramowania

***NazwaProduktu*-KB*NumerArtykułu*-*Opcja*-*Język*.exe**

- przykłady:

  Windows2000-KB123456-PL.exe

  WindowsXP-KB123456-IA64-PL.exe

  WindowsServer2003-KB123456-x86-PL.exe

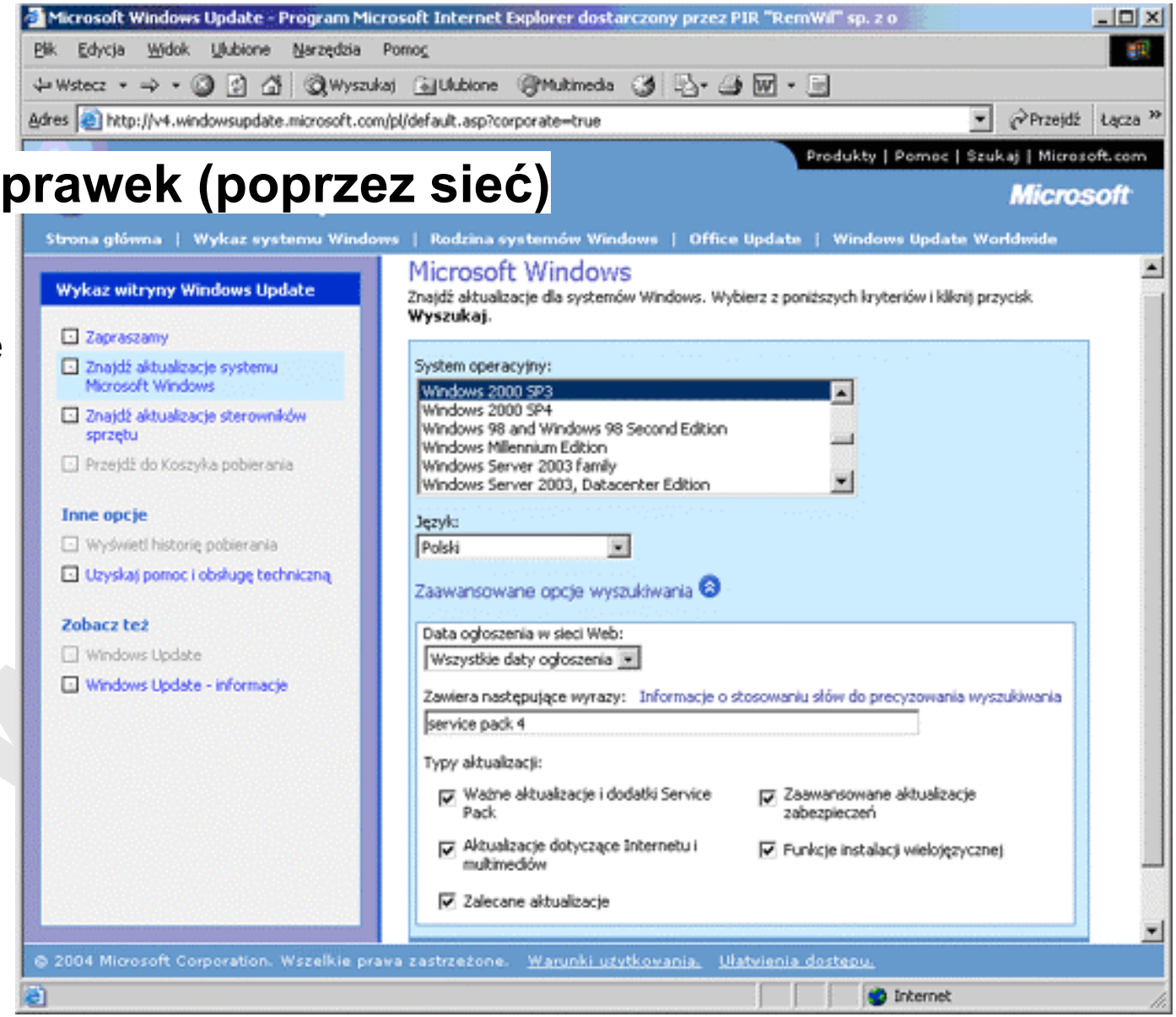
Aktualizacja systemów

Windows

Ręczna instalacja poprawek (poprzez sieć)

1. pobranie poprawek

   z witryny Windows Update



Aktualizacja systemów

Windows

Ręczna instalacja poprawek (poprzez sieć)

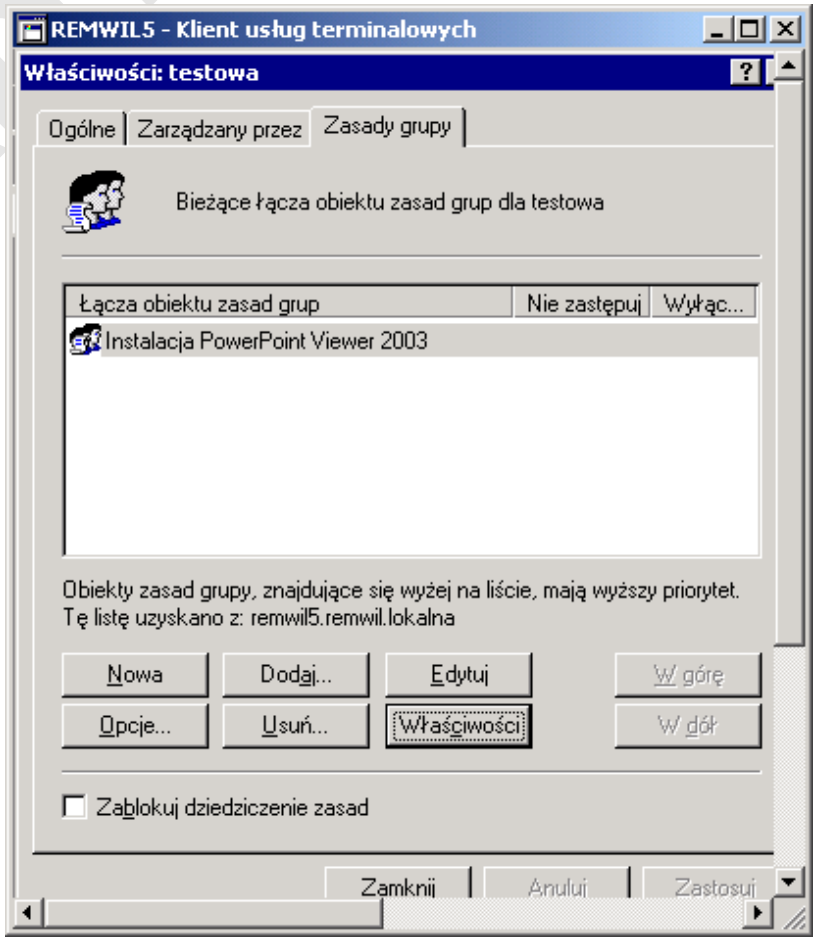
2. przygotowanie do zdalnej instalacji
   - wyodrębnienie plików instalacyjnych (.msi) w udostępniony folder sieciowy
   - przydział uprawnienia dla tego udziału, tak aby zezwolić na zdalny dostęp do pakietu dystrybucyjnego

Aktualizacja systemów

Windows

Ręczna instalacja poprawek (poprzez sieć)

3. wykorzystanie Zasad Grupy w Active Directory do zlecenia instalacji
   - utworzenie obiektu zasad grupy (GPO)

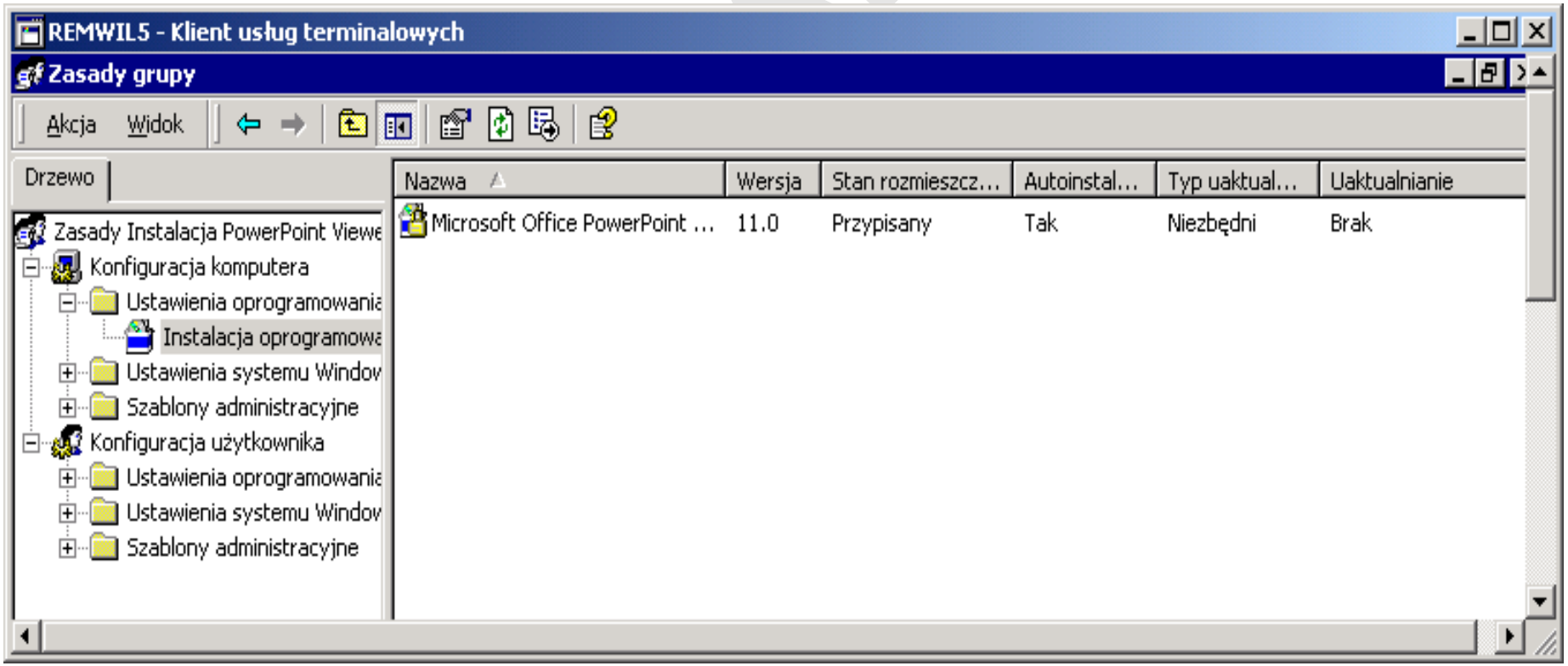


Aktualizacja systemów

Windows

Ręczna instalacja poprawek (poprzez sieć)

4. Przypisanie oprogramowania użytkownikom lub komputerom



Aktualizacja systemów

Windows

Zautomatyzowana instalacja poprawek

Software Update Services: http://www.microsoft.com/sus/

- SUS umożliwia automatyczne instalowanie kluczowych aktualizacji na komputerach w obrębie domeny
- jeden z pierwszych efektów inicjatywy *Strategic Technology Protection Program* (STPP)
- administrator zachowuje kontrolę nad tym, jakie aktualizacje mają być zainstalowane, kiedy i na których komputerach

Aktualizacja systemów

Windows

Zautomatyzowana instalacja poprawek

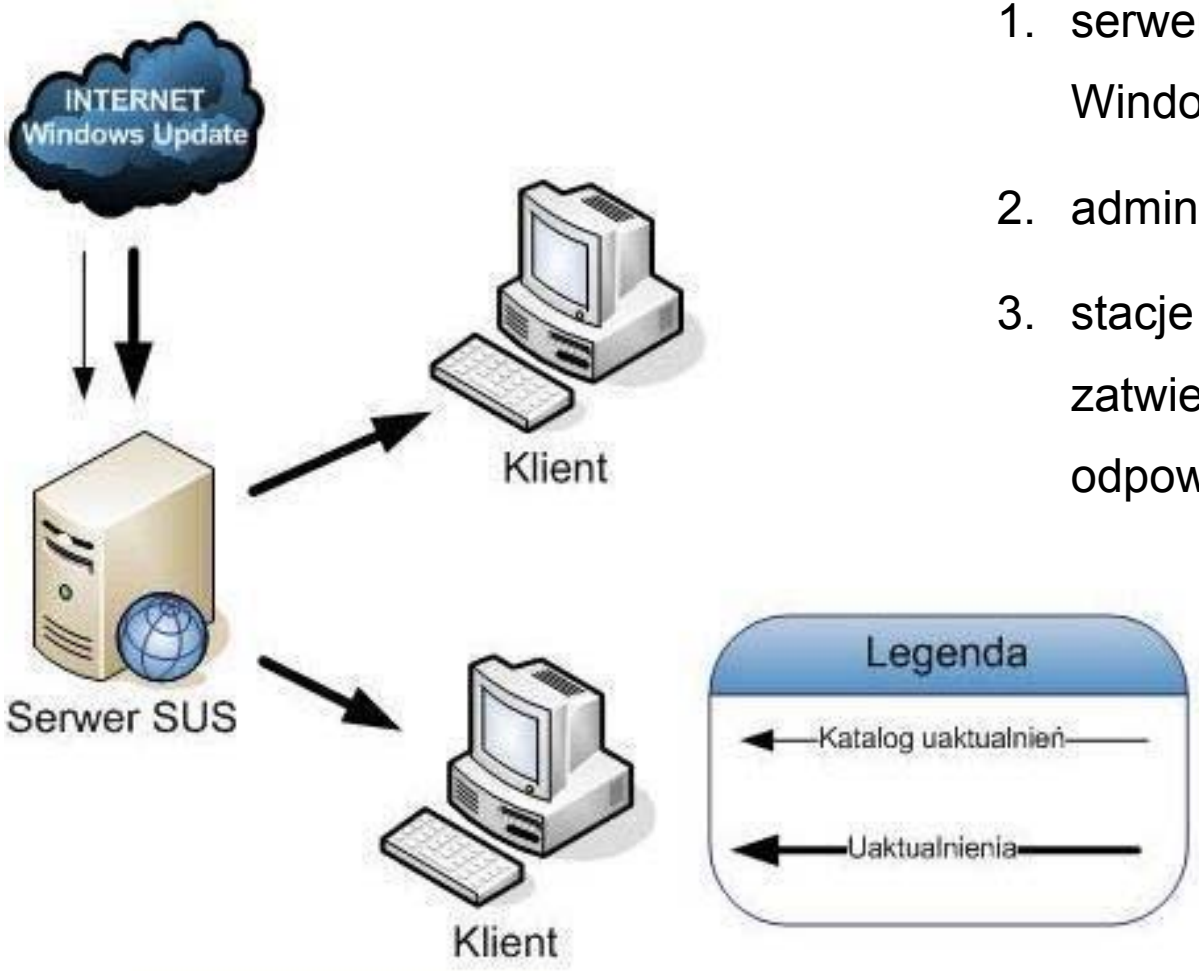
Komponenty SUS:

- SUS działający jako witryna serwera IIS
- usługa Automatic Updates (AU) na stacjach sieciowych
- ustawienia reguł grupowych w domenie Active Directory

Aktualizacja systemów

Windows

Zautomatyzowana instalacja poprawek

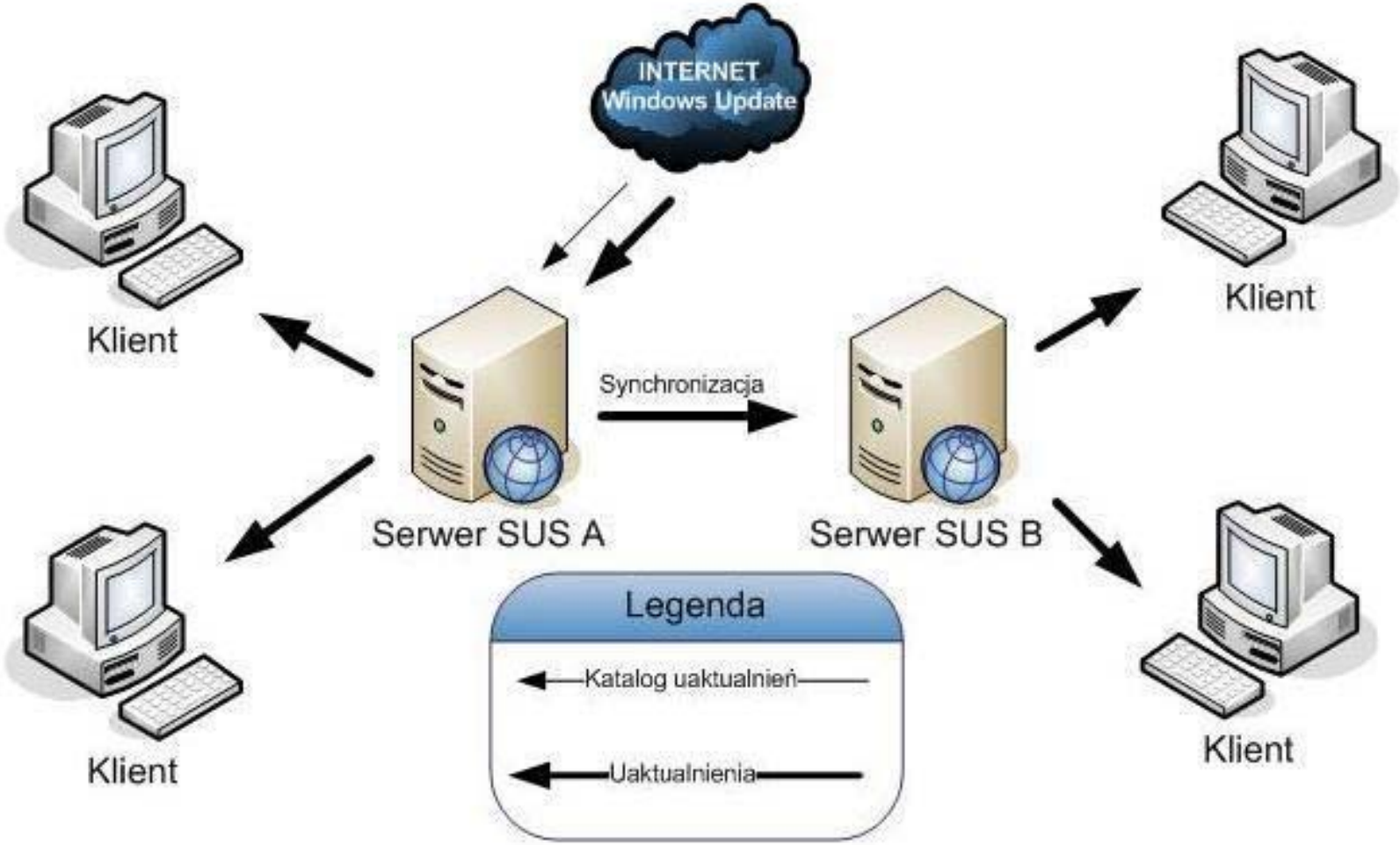


1. serwer SUS pobiera aktualizacje z witryny Windows Update
2. administrator zatwierdza aktualizacje
3. stacje łączą się z serwerem SUS i pobierają zatwierdzone przez administratora aktualizacje odpowiednie dla siebie

Aktualizacja systemów

Windows

Zautomatyzowana instalacja poprawek



Aktualizacja systemów

Windows

Zautomatyzowana instalacja poprawek

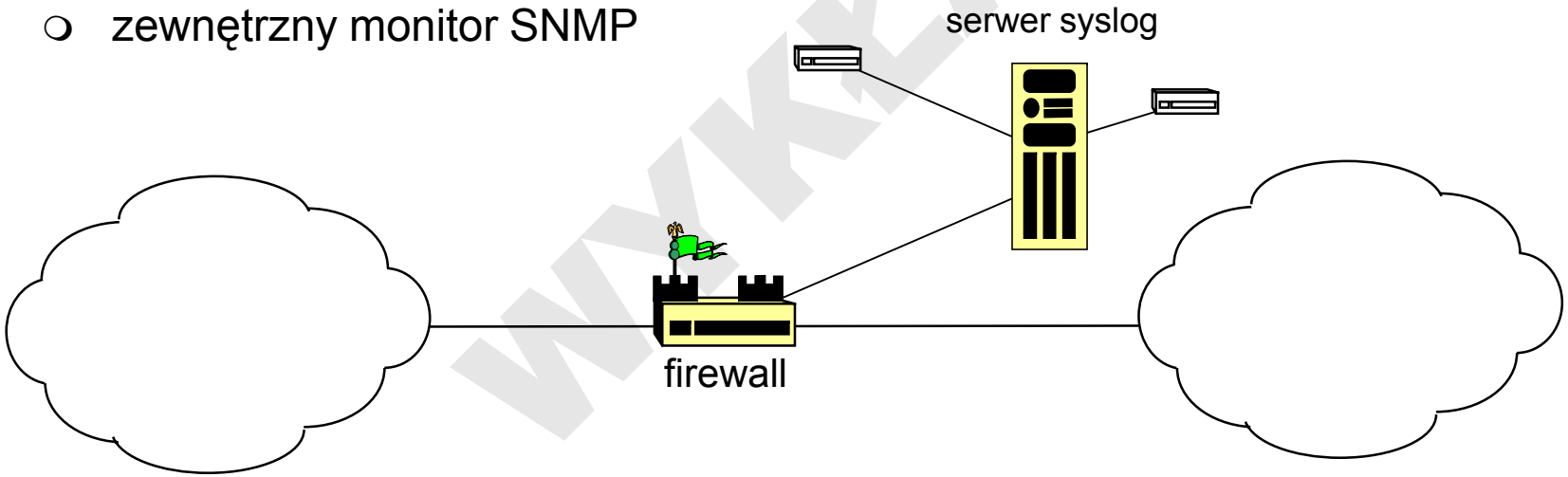
Ograniczenia SUS:

- nie obsługuje Windows NT i Windows 9x
- nie obsługuje produktów Microsoft Office i Microsoft BackOffice – aktualizacje dotyczą tylko systemu operacyjnego oraz Microsoft IIS i Internet Explorer
- nie ma możliwości odinstalowania aktualizacji – istotne jest przetestowanie aktualizacji przed ich zainstalowaniem przez SUS (możliwe jest jednak ręczne odinstalowanie aktualizacji)

Monitorowanie zabezpieczeń

Alerty i rejestry zdarzeń

- wewnętrzne repozytorium (*audit-trail*) lub konsola urządzenia (np. routera, zapory)
- zewnętrzny serwer usługi syslog
- zewnętrzny monitor SNMP



Monitorowanie zabezpieczeń

Okresowy audyt

- samodzielny – wsparcie narzędziami programowymi
- zlecany wyspecjalizowanym firmom zewnętrznym (brygady tygrysa)

Pomoc

Windows:

Microsoft

- http://www.microsoft.com/windowsxp
- http://www.microsoft.com/athome/security/default.mspx
- http://www.microsoft.com/technet/security/prodtech/winclnt/secwinxp/default.mspx

i inni

- http://www.w2k.pl
- http://www.windows2003.pl/

Pomoc

Organizacje:

CERT (*Computer Emergency Response Team*)

- rządowe (USA) Informatyczne Centrum Kryzysowe http://www.cert.org
- jego polski odpowiednik w NASK http://www.cert.pl
- CERT Advisory – baza informacji

FIRST (*Forum of Incident Response and Security Teams*)

- http://www.first.org/team-info – zespół sił szybkiego reagowania, informacje z pierwszej linii frontu

CIAC (*Computer Incident Advisory Capability*)

- http://www.ciac.org/ciac – biuletyny informacyjne na temat bezpieczeństwa, informacje o wirusach, narzędzia poprawiające bezpieczeństwo

Pomoc

Organizacje:

NIST CSRC (*National Institute of Standard and Technology, Computer Security Resource Clearinghouse*)

- http://csrc.nist.gov – biuletyny na temat bezpieczeństwa, projekty, baza zasobów publikowanych przez agencje bezpieczeństwa

Instytut SANS

- http://www.sans.org/sansnews/ – subskrypcje biuletynów na temat bezpieczeństwa, oraz własne publikacje elektroniczne Security Slerts Consensus i SANS NewBites (tygodniki) oraz Sans Windows Security Nesletter (miesięcznik)

Eugene Spafford (Purdue Univ.)

- http://www.cerias.purdue.edu/infosec/hotlist/ – zawsze najbardziej aktualne odnośniki na temat słabych punktów systemów i luk w programach

Pomoc

Organizacje:

SPOCK (*Security Proof for Concept Keystone*)

- organizacja testująca produkty

Zgłoszenia ataków:

Zespoły zgłoszeń Abuse:

- http://www.cert.pl/index3.html?id=11 (cert@cert.pl)
- http://www.dialog.pl/dialog/internet/internet.php?id=41
- http://www.tp.pl/dom/bws/zglaszanie/ (abuse@tpnet.pl)
- każda domena pocztowa: abuse@... (RFC 2142), postmaster@…
  (nieprawidłowości można zgłaszać pod www.rfc-ignorant.org)

Pomoc

Przykładowe listy dyskusyjne:

- X-Force (Internet Security System) – baza danych na temat bezpieczeństwa
  http://xforce.iss.net/xforce/search.php
  oraz konsultacje w zakresie bezpieczeństwa, raporty o linkach i zagrożeniach
  https://atla-mm1.iss.net/mailman/listinfo/alert
- lista alarmowa http://www.iss.net/security_center/maillists/ – informacje o zagrożeniach oraz zapowiedzi nowych produktów
- bugtraq http://securityfocus.com/subscribe – usterki w kodach programów
- http://honor.icsalabs.com/mailman/listinfo/firewall-wizards moderowane forum na temat zapór sieciowych firewall
- http://isc.org/services/public/lists/firewalls.html – lista na temat zapór sieciowych firewall
- Network World Fusion http://www.nwfusion.com/newsletters/sec/ – przeglądy, statystyki
- OpenSSH http://mindrot.org/mailman/listinfo/openssh-unix-announce – znane problemy, opis konserwacji, kontrybucje w rozwijaniu programu

Pomoc

Przykładowe grupy dyskusyjne:

- news:comp.security
- news:comp.security.firewalls
- news:comp.lang.java.security
- news:comp.security.unix
- news:comp.os.linux.security
- news:alt.computer.security

Inne dziedziny bezpieczeństwa

DRM

(*Digital Rights Management*)

http://www.epic.org/privacy/drm/

System kontroli praw autorskich (itp.)

- DVD – kodowanie materiału video: *CSS, Macrovision protecion,* kontrolowanie dystrybucji poprzez „strefy” (*Regions*)
- transmisja TV (*FCC Broadcast Flag*)
- Content/Copy Protection for Removable Media (CPRM)
- licencjonowanie oprogramowania (FlexLM, HASP)
- uniemożliwianie anonimowego wykorzystania mediów – np. Windows Media Player używa *globally-unique identifier* (GUID) do śledzenia aktywności użytkowników, eBook Reader po aktywacji usługi nadaje tzw. paszport powiązany z informacją o systemie (hardware) użytkownika

DRM

Ograniczanie czy ubezwłasnowolnienie?

- ryzyko „zamknięcia” użytkowników w określonych platformach (np. sys.op.)
- RMS (*Rights Management Service*) – usługa Microsoft Server 2003 – pozwala definiować ograniczenia dostępu na poziomie systemu plików:
  - można określić czas ważności korespondencji e-mail (po upływie okresu ważności nie da się listu odczytać
  - można zablokować drukowanie lub przesłanie innym użytkownikom
  - można ograniczyć dozwoloną liczbę kopii
- zabezpieczonych dokumentów MS Office nie da się otworzyć w OpenOffice
- Bolek otrzymał pisemne polecenie służbowe – jak po „wygaśnięciu” dokumentu udowodni jego otrzymanie?
- e-mail z żądaniem okupu z wyłączonym drukowaniem i kopiowaniem – jak udowodnić winę przestępcy?

Przyszłość

„Trudno cokolwiek przewidzieć, a już szczególnie przyszłość”

Yogi Berra

Przyszłość

Co się zmienia?

- zwiększa się poziom bezpieczeństwa rozwiązań informatycznych:
  - systemy operacyjne oraz krytyczne aplikacje (zwłaszcza serwery) są analizowane pod kontem błędów istotnych z punktu widzenia bezpieczeństwa,
  - nowe narzędzia informatyczne uwzględniają wymogi bezpieczeństwa (np. środowisko .NET, JVM),
  - proces zarządzania bezpieczeństwem organizacji staje się coraz bardziej spójny.
- zwiększa się świadomość bezpieczeństwa:
  - w kontekście technicznym coraz częściej wykorzystywane są odpowiednie procedury tworzenia bezpiecznego produktu, wprowadzane już na etapie projektu i obejmujące także coraz bardziej złożone procedury testowania,
  - w kontekście biznesowym bezpieczeństwo zaznacza się coraz wyraźniej – dorasta do rangi krytycznego wymagania odnośnie produktu (istotniejszego niż funkcjonalność),
  - z punktu użytkownika, coraz powszechniejsza staje się wiedza o ograniczeniach technologii informatycznych oraz zagrożeniach związanych z jej wykorzystaniem.

Przyszłość

Co się zmienia?

- pojawiają się coraz to nowsze mechanizmy i metodologie, które ułatwiają zarządzanie bezpieczeństwem informatycznym organizacji:
  - coraz bardziej zaawansowane systemy firewall, umożliwiające integrację z rozwiązaniami dodatkowymi, takimi jak systemy antywirusowe czy monitorowania
  - systemy IDS / IPS, zwłaszcza o modularnej strukturze, o coraz większej skuteczności oraz wydajności
  - systemy kompleksowego zarządzania bezpieczeństwem, zarówno w kontekście pojedynczego systemu jak i organizacji
  - mechanizmy silnego uwierzytelniania za pomocą kryptografii oraz dedykowanych urządzeń (karty, tokeny) umożliwiających identyfikację oraz precyzyjną autoryzację
  - inżynieria oprogramowania ukierunkowana na tworzenie bezpiecznego oprogramowania: projektowanie z uwzględnieniem przepływu informacji i kontroli dostępu do niej oraz poprawności samej implementacji jak i procedur wdrażania i administracji aplikacji

Przyszłość

Co się raczej nie zmieni?

- bezpieczeństwo informacji przetwarzanej w organizacji tylko częściowo uzależnione jest od komponentów technologicznych, istotna jest również np. polityka, odpowiednie przeszkolenie pracowników (podatność na socjotechniki) itp.
- technologie informatyczne wykorzystywane w coraz to szerszym obszarze zastosowań – problem świadomości zagrożeń przez długi czas będzie bardzo istotny
- pojawiają się coraz to nowsze technologie, oferujące nowe możliwości, a jednocześnie utrudniające efektywne wykorzystanie dotychczasowych zabezpieczeń (np. WLAN)
- błędy i niedoskonałości wykorzystywanych technologii były, są i będą, zmienią się jedynie sposoby ich wykorzystania oraz poziom trudności i nakład środków związany z ich usuwaniem