Test penetracyjny wykonywany z zewnątrz może obejmować:

- **Rekonesans - zbieranie informacji o celu ataku.**
- **Skanowanie przestrzeni adresowej sieci prywatnej - wykrywanie dostępnych serwerów, stacji roboczych, drukarek, routerów i innych urządzeń.**
- **Skanowanie sieci telefonicznej - wykrywanie aktywnych modemów sieci prywatnej.**
- **Skanowanie portów serwerów i urządzeń sieciowych - wykrywanie dostępnych usług.**
- **Identyfikacja systemu - ustalanie rodzaju i wersji systemu, oprogramowania użytkowego, kont użytkowników.**
- **Symulacja włamania - przejmowanie kont, odczytywanie informacji z baz, odczytywanie katalogów współdzielonych, ataki na system kontroli dostępu.**
- **Badanie odporności na ataki typu *odmowa usługi* (*denial of service*) - uruchamianie exploitów.**

Rekonesans - co może zidentyfikować agresor:?

- **nazwę domeny,**
- **bloki sieci,**
- **adresy IP komputerów osiągalnych poprzez usługi działające na zidentyfikowanych komputerach,**
- **architekturę i zainstalowany system operacyjny,**
- **mechanizmy kontroli dostępu i listy kontroli dostępu,**
- **systemy wykrywania intruzów,**
- **używane protokoły,**
- **numery linii telefonicznych,**
- **mechanizmy autoryzacji dla zdalnego dostępu.**

Przeszukiwanie ogólnie dostępnych źródeł:

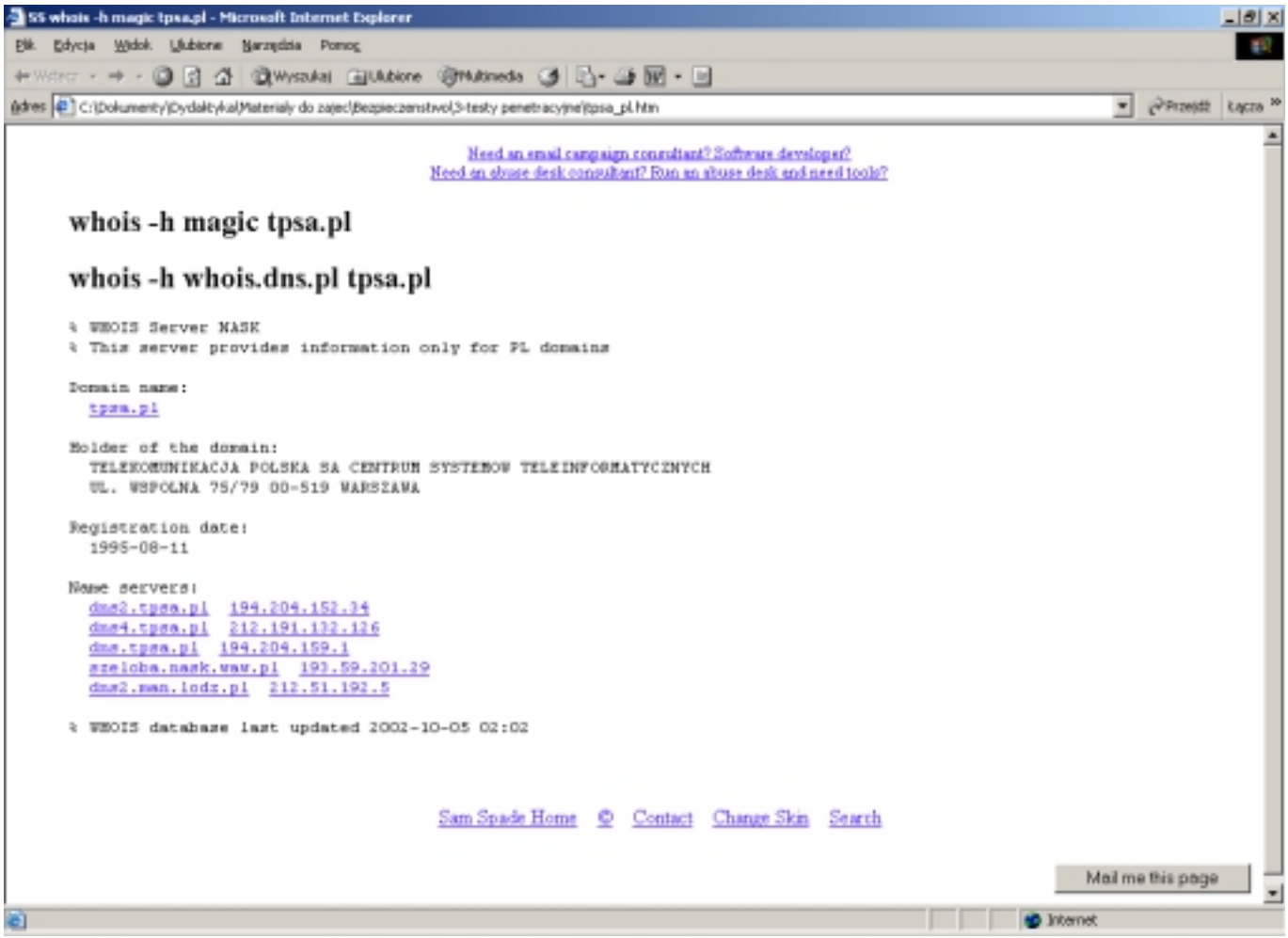
- **strony www,**
- **artykuły i informacje prasowe,**
- **listy dyskusyjne,**
- **serwisy wyszukiwawcze**

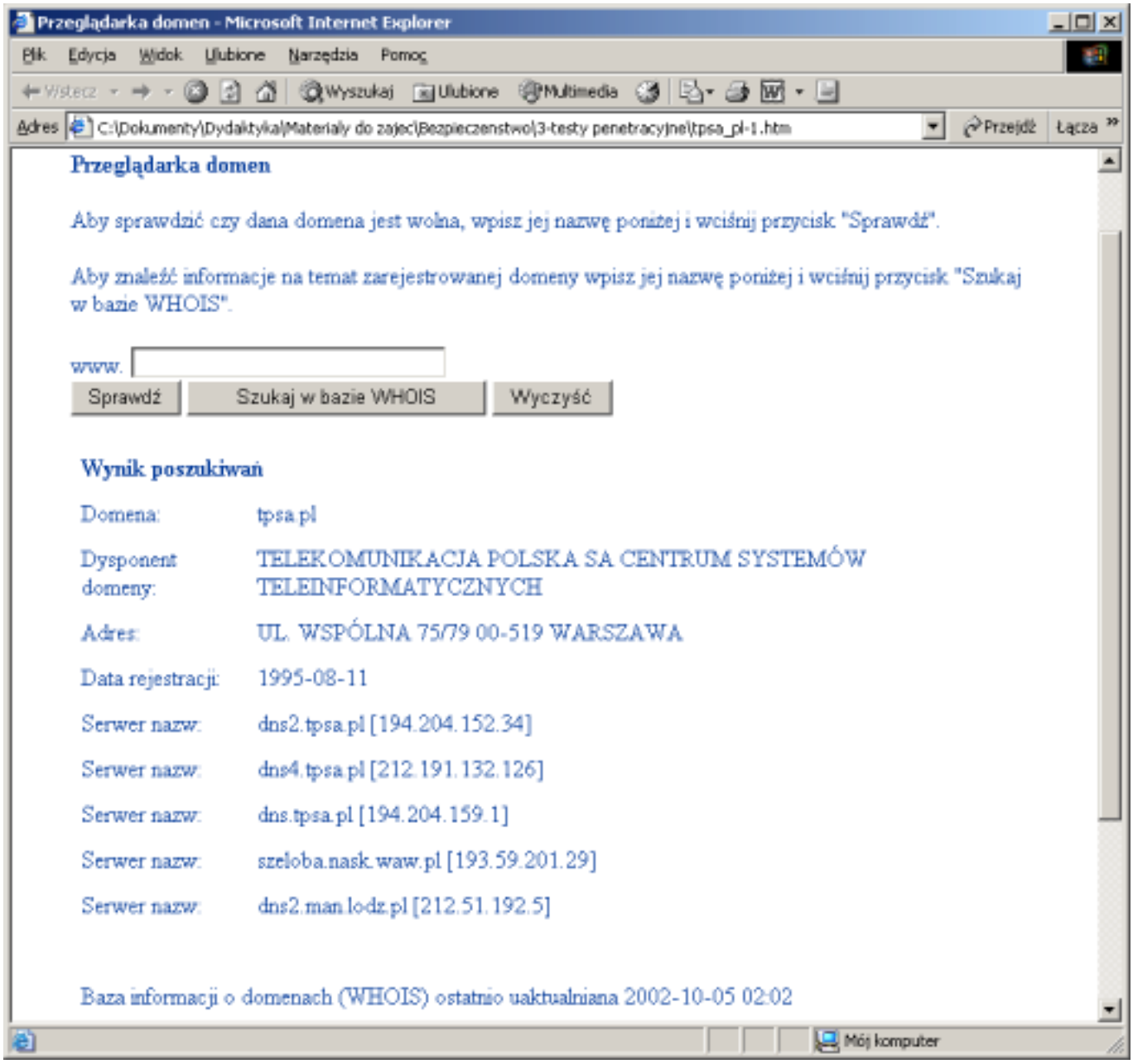
Analiza sieci

- **identyfikacja nazw domen i sieci**
- **bazy danych *whois***

Kontrola serwerów DNS

Badanie sieci


55 whois -h magic tpsa.pl - Microsoft Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Wstecz Wyszukaj Ulubione Multimedia
Adres C:\Dokumenty\Dydaktyka\Materiały do zajęć\Bezpieczeństwo\3-testy penetracyjne\tpsa_pl.htm
Przejdź Łącza
Need an email campaign consultant? Software developer?
Need an abuse desk consultant? Run an abuse desk and need tools?
whois -h magic tpsa.pl
whois -h whois.dns.pl tpsa.pl
% WHOIS Server NASK
% This server provides information only for PL domains
Domain name:
tpsa.pl
Holder of the domain:
TELEKOMUNIKACJA POLSKA SA CENTRUM SYSTEMOW TELEINFORMATYCZNYCH
UL. WSPOLNA 75/79 00-519 WARSZAWA
Registration date:
1995-08-11
Name servers:
dns2.tpsa.pl 194.204.152.34
dns4.tpsa.pl 212.191.132.126
dns.tpsa.pl 194.204.159.1
szeloba.nask.waw.pl 193.59.201.29
dns2.man.lodz.pl 212.51.192.5
% WHOIS database last updated 2002-10-05 02:02
Sam Spade Home © Contact Change Skin Search
Mail me this page
Internet


Przeglądarka domen - Microsoft Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Wstecz Wyszukaj Ulubione Multimedia
Adres C:\Dokumenty\Dydaktyka\Materiały do zajęć\Bezpieczeństwo\3-testy penetracyjne\tpsa_pl-1.htm
Przejdź Łącza
Przeglądarka domen
Aby sprawdzić czy dana domena jest wolna, wpisz jej nazwę poniżej i wciśnij przycisk "Sprawdź".
Aby znaleźć informacje na temat zarejestrowanej domeny wpisz jej nazwę poniżej i wciśnij przycisk "Szukaj w bazie WHOIS".
www.
Sprawdź
Szukaj w bazie WHOIS
Wyczyść
Wynik poszukiwań
Domena: tpsa.pl
Dysponent domeny: TELEKOMUNIKACJA POLSKA SA CENTRUM SYSTEMÓW TELEINFORMATYCZNYCH
Adres: UL. WSPÓLNA 75/79 00-519 WARSZAWA
Data rejestracji: 1995-08-11
Serwer nazw: dns2.tpsa.pl [194.204.152.34]
Serwer nazw: dns4.tpsa.pl [212.191.132.126]
Serwer nazw: dns.tpsa.pl [194.204.159.1]
Serwer nazw: szeloba.nask.waw.pl [193.59.201.29]
Serwer nazw: dns2.man.lodz.pl [212.51.192.5]
Baza informacji o domenach (WHOIS) ostatnio uaktualniana 2002-10-05 02:02
Mój komputer

Skanowanie

- **detekcja działających i nie działających urządzeń**
- **detekcja usług**
- **rozpoznanie systemu operacyjnego**
- **rozpoznanie topologii sieci**
- **rozpoznanie konfiguracji urządzeń dostępowych**

Istotne dla skanowania elementy nagłówka pakietu

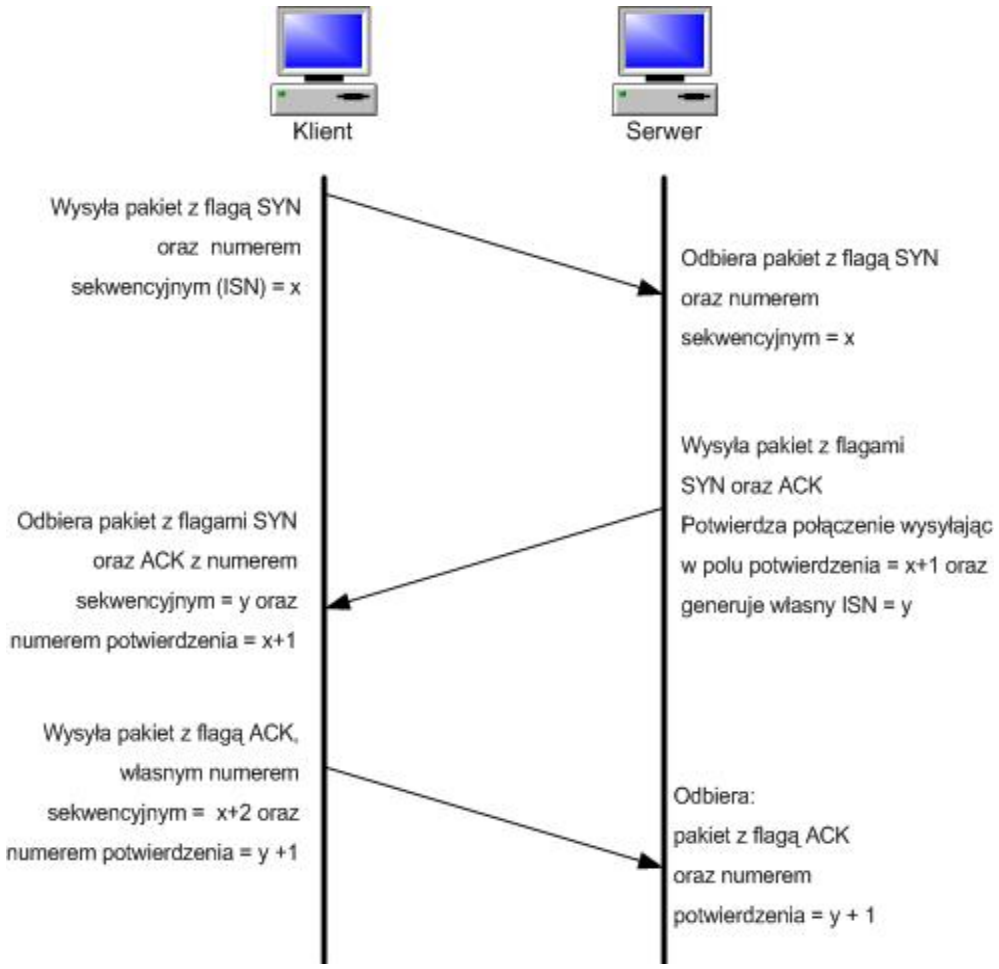
- **adresy i porty,**
- **okres życia (TTL)**
- **numer sekwencyjny**
- **wielkość okna**
- **znaczniki i przesunięcie fragmentacji**
- **flagi URG, ACK, PSH, RST, SYN, FIN**

Skanowanie z wykorzystaniem protokołu UDP

Skanowanie z wykorzystaniem protokołu ICMP

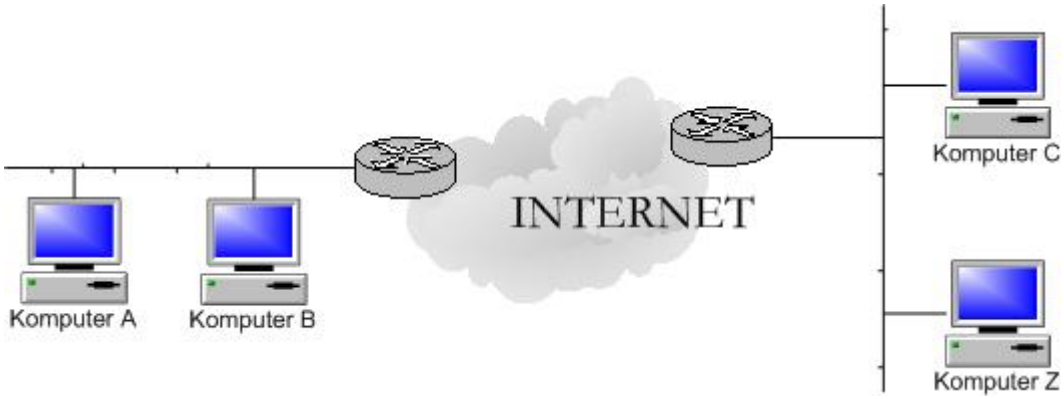
- *ICMP echo request*
- *Timestamp Request*
- *Address Mask Request*

Skanowanie z wykorzystaniem protokołu TCP



Skanowanie TCP

- **Skanowanie połączeniowe**
- **Skanowanie pół-otwarte**
- **Skanowanie specjalne**
  - **SYN/ACK – wysłanie SYN/ACK dla nieistniejącego połączenia; dla zamkniętego portu wróci RST.**
  - **FIN - wysłanie FIN dla nieistniejącego połączenia; dla zamkniętego portu wróci RST.**
  - **XMAS – wysłanie pakietu z wszystkimi flagami; dla zamkniętego portu wróci RST.**
  - **NULL – wysłanie pakietu bez flag; dla zamkniętego portu powinien wrócić RST.**
  - **RST – dla nieistniejącego hosta router odpowie pakietem ICMP *Host unreachable.***



Skanowanie *spoofed inverse mapping*
Skanuje komputer B
Wykorzystywany jest komputer A

A. Sprawdzanie pola TTL

pakiet 1: host XXX.XXX.XXX.XXX port 20: F:RST -> ttl: 70 win: 0 => port zamknięty
pakiet 2: host XXX.XXX.XXX.XXX port 21: F:RST -> ttl: 70 win: 0 => port zamknięty
pakiet 3: host XXX.XXX.XXX.XXX port 22: F:RST -> ttl: 40 win: 0 => port otwarty
pakiet 4: host XXX.XXX.XXX.XXX port 23: F:RST -> ttl: 70 win: 0 => port zamknięty

B. Sprawdzanie pola WINDOW

pakiet 6: host XXX.XXX.XXX.XXX port 20: F:RST -> ttl: 64 win: 0 => port zamknięty
pakiet 7: host XXX.XXX.XXX.XXX port 21: F:RST -> ttl: 64 win: 0 => port zamknięty
pakiet 8: host XXX.XXX.XXX.XXX port 22: F:RST -> ttl: 64 win: 512 => port otwarty
pakiet 9: host XXX.XXX.XXX.XXX port 23: F:RST -> ttl: 64 win: 0 => port zamknięty

Skanowanie z wykorzystaniem protokołu IP
IP ID idle scan

krok 1(A)

#hping B -r

HPING B (eth0 xxx.yyy.zzz.jjj): no flags are set, 40 data bytes

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=0 ttl=64 id=41660 win=0 time=1.2 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=1 ttl=64 id=+1 win=0 time=75 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=2 ttl=64 id=+1 win=0 time=91 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=3 ttl=64 id=+1 win=0 time=90 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=4 ttl=64 id=+1 win=0 time=91 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=5 ttl=64 id=+1 win=0 time=87 ms

Odpowiedź 1 (B)

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=17 ttl=64 id=+1 win=0 time=96 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=18 ttl=64 id=+1 win=0 time=80 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=19 ttl=64 id=+2 win=0 time=83 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=20 ttl=64 id=+3 win=0 time=94 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=21 ttl=64 id=+1 win=0 time=92 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=22 ttl=64 id=+2 win=0 time=82 ms

Odpowiedź 2 (C)

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=52 ttl=64 id=+1 win=0 time=85 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=53 ttl=64 id=+1 win=0 time=83 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=54 ttl=64 id=+1 win=0 time=93 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=55 ttl=64 id=+1 win=0 time=74 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=56 ttl=64 id=+1 win=0 time=95 ms

60 bytes from xxx.yyy.zzz.jjj: flags=RA seq=57 ttl=64 id=+1 win=0 time=81 ms

Skanowanie za bramką *IP masqurading*

[root] # nmap - sI 192.168.2.1 - P0 192.168.2.40
Starting nmap V 2.54BETA30 (www.insecure.org/nmap /)
Idlescan using .....
Interesting ports one .....:
(The 1541 ports scanned goal not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open HTTP

2 warunki

- **Bramka nie może generować ruchu**
- **Bramka musi przyjmować pakiety na interfejsie zewnętrznym z adresem zwrotnym komputera sieci wewnętrznej**

Skanowanie z wykorzystaniem protokołu FTP (*FTP bounce*)

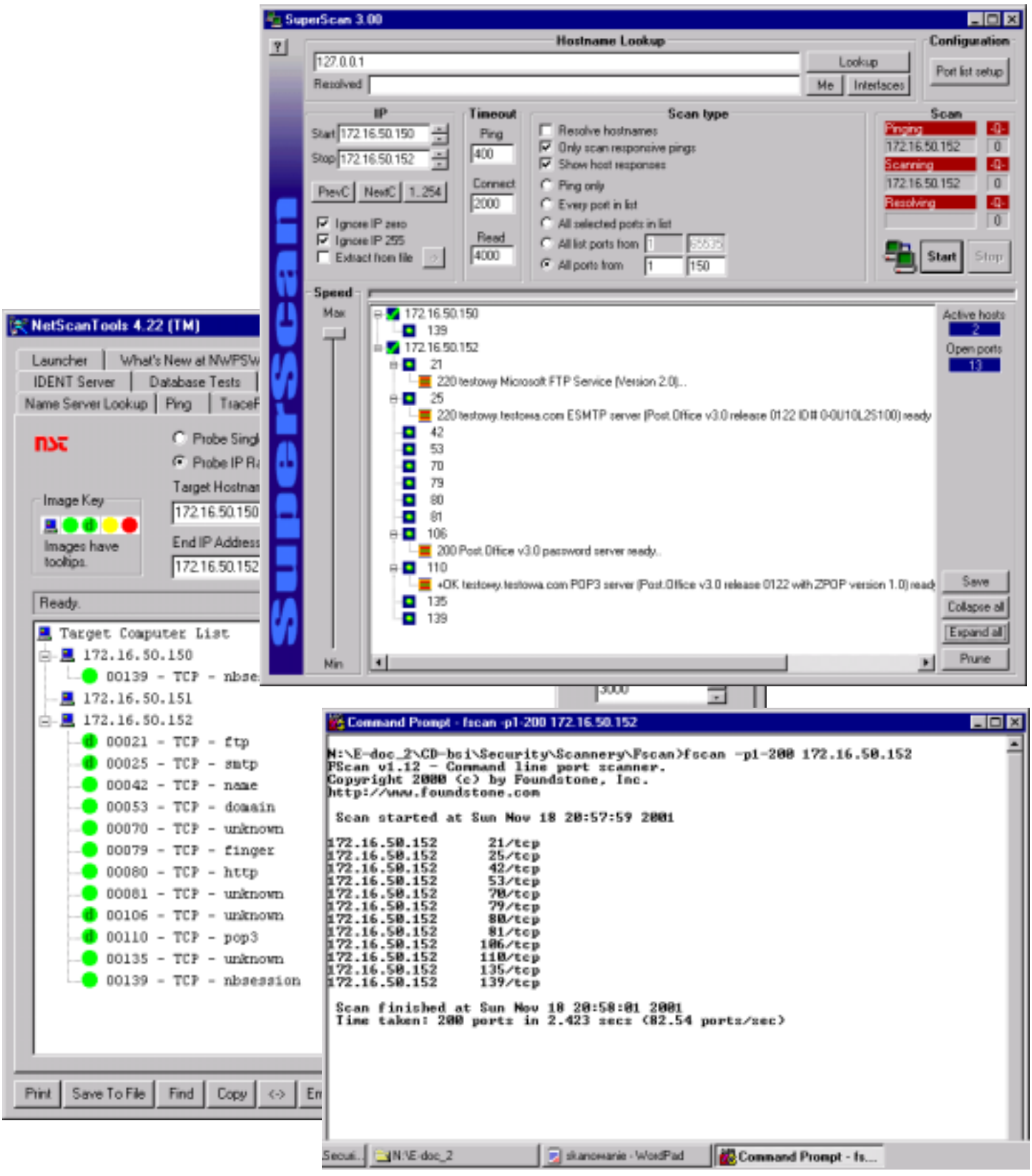
Właściwość FXP - serwer FTP może wysłać dane do innego hosta niż źródłowy

Identyfikowanie połączenia (*reverse ident scanning*)

Wykorzystanie protokołu ident (RFC 1413)

Skanowanie ukryte

- **Skanowanie portów w losowej kolejności**
- **Powolne skanowanie**
- **Fragmentacja pakietów**
- **Odwrócenie uwagi**
- **Fałszowanie adresu nadawcy**
- **Skanowanie rozproszone**


SuperScan 3.00
Hostname Lookup
127.0.0.1
Resolved
Lookup
Me
Interfaces
Configuration
Port list setup
IP
Start 172.16.50.150
Stop 172.16.50.152
PrevC
NextC
1..254
Ignore IP zero
Ignore IP 255
Extract from file
Timeout
Ping
400
Connect
2000
Read
4000
Scan type
Resolve hostnames
Only scan responsive pings
Show host responses
Ping only
Every port in list
All selected ports in list
All list ports from
All ports from
Scan
Pinging
172.16.50.152
Scanning
172.16.50.152
Resolving
Start
Stop
Speed
Max
Min
172.16.50.150
139
172.16.50.152
21
220 testowy Microsoft FTP Service (Version 2.0)..
25
220 testowy.testowa.com ESMTP server (Post.Office v3.0 release 0122 ID# 0-0U10L2S100) ready
42
53
70
79
80
81
106
200 Post.Office v3.0 password server ready..
110
+OK testowy.testowa.com POP3 server (Post.Office v3.0 release 0122 with ZPOP version 1.0) ready
135
139
Active hosts
2
Open ports
13
Save
Collapse all
Expand all
Prune
NetScanTools 4.22 (TM)
Launcher
What's New at NWPSW
IDENT Server
Database Tests
Name Server Lookup
Ping
Image Key
Images have tooltips.
Target Hostnam
172.16.50.150
End IP Address
172.16.50.152
Ready.
Target Computer List
172.16.50.150
00139 - TCP - nbse
172.16.50.151
172.16.50.152
00021 - TCP - ftp
00025 - TCP - smtp
00042 - TCP - name
00053 - TCP - domain
00070 - TCP - unknown
00079 - TCP - finger
00080 - TCP - http
00081 - TCP - unknown
00106 - TCP - unknown
00110 - TCP - pop3
00135 - TCP - unknown
00139 - TCP - nbsession
Print
Save To File
Find
Copy
Command Prompt - fscan -p1-200 172.16.50.152
N:\E-doc_2\CD-bsi\Security\Scannery\Fscan>fscan -p1-200 172.16.50.152
FScan v1.12 - Command line port scanner.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com
Scan started at Sun Nov 18 20:57:59 2001
172.16.50.152 21/tcp
172.16.50.152 25/tcp
172.16.50.152 42/tcp
172.16.50.152 53/tcp
172.16.50.152 70/tcp
172.16.50.152 79/tcp
172.16.50.152 80/tcp
172.16.50.152 81/tcp
172.16.50.152 106/tcp
172.16.50.152 110/tcp
172.16.50.152 135/tcp
172.16.50.152 139/tcp
Scan finished at Sun Nov 18 20:58:01 2001
Time taken: 200 ports in 2.423 secs (82.54 ports/sec)
N:\E-doc_2
skanowanie - WordPad
Command Prompt - fs...

Zdalna identyfikacja rodzaju i wersji systemu operacyjnego (*fingerprinting*)

Banner grabbing

Analiza stosu TCP/IP (aktywna i pasywna)

- **Początkowa wartość TTL (*Time To Live*)**
- **Wielkość okna**
- **Bit DF (*Don't fr*agment)**
- **Pole MSS (*Maximum Segment Size*)**
- **Opcja skalowania okna**
- **Opcja selektywnego potwierdzania (Selective Acknowledgment)**
- **Opcja NOP (*No Operation*)**
- **Pole IP ID**

System operacyjny	TTL	Window	Bit DF	TOS
FreeBSD 3.x	64	17520	1	16
OpenBSD 2.x	64	17520	0	16
Linux	64	32120	1	0
Solaris 2.x	255	8760	1	0
Solaris 8	64	24820	1	0
MS Windows 95	32	5000-9000	1	0
MS Windows NT	128	5000-9000	1	0
MS Windows 2000	128	17000-18000	1	0
SCO	64	24820	0	0
Netware 4.11	128	32000-32768	1	0

Zdalna identyfikacja rodzaju i wersji systemu operacyjnego (*fingerprinting*)

- **Test z nieistniejącą flagą *(Bogus Flag Probe Test)***
- **Próbkowanie początkowego numeru sekwencyjnego (*Initial Sequence Number*)**
  - **cykliczne**
  - **pseudolosowe**
  - **losowe bazujące na aktualnym czasie**
  - **stałe**
- **Obsługa fragmentacji**
- **Nowe opcje TCP**
- **Skanowanie ICMP**
  - **Rozmiar cytowanych błędów (*ICMP Error Message Quoting Size*)**
  - **Test integralności odpowiedzi ICMP (*ICMP Error Message Echoing Integrity*)**
  - **Bity precedencji (Precedence Bits in ICMP Error Messages)**

Zdalna identyfikacja rodzaju i wersji systemu operacyjnego (*fingerprinting*)

Program Xprobe

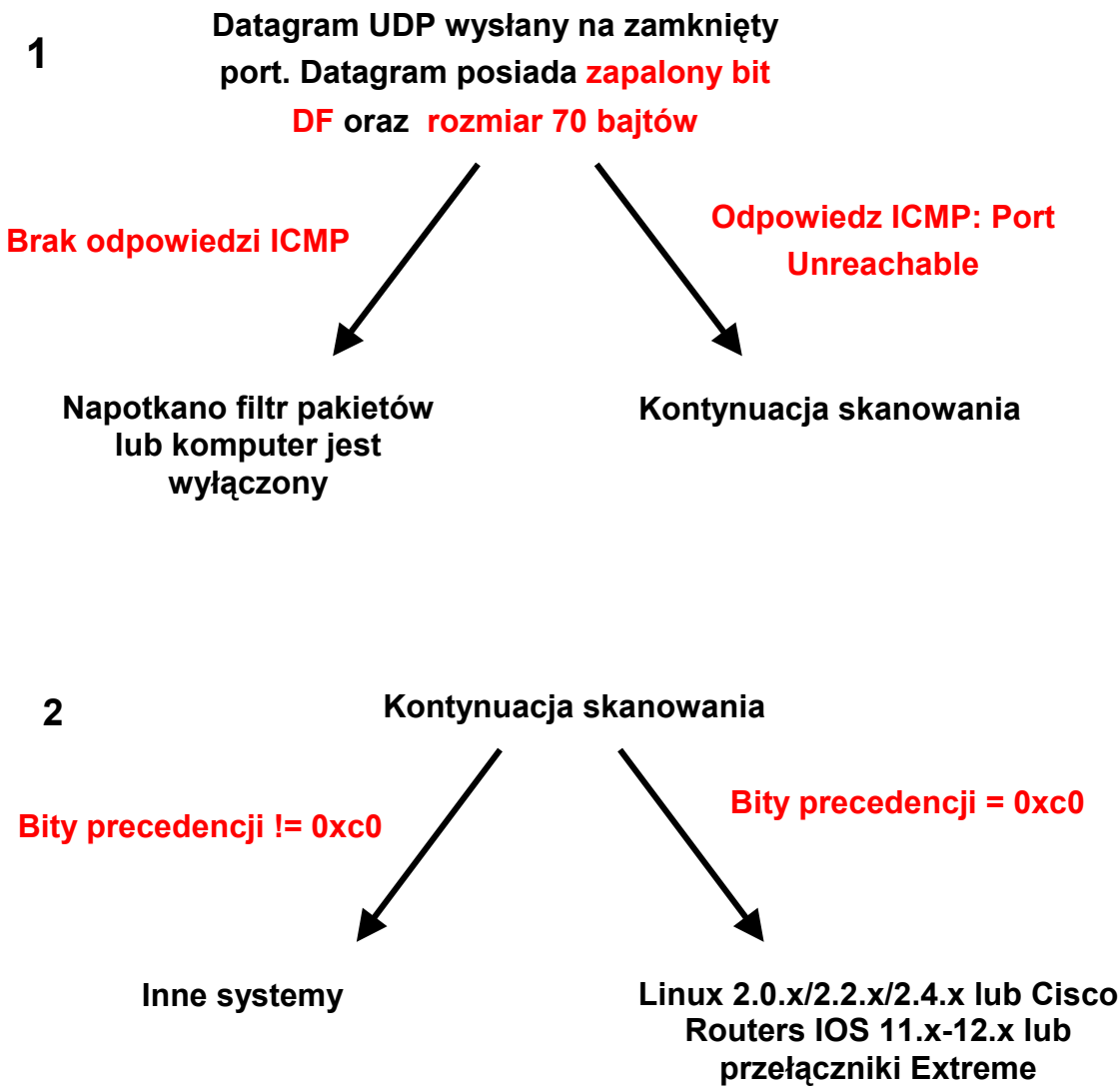
- ***Echo Request***
- ***Timestamp Request***
- ***Information Request***
- ***Address Mask Request***

[root@imp xprobe-0.0.2]# ./xprobe 192.168.6.43
X probe ver. 0.0.2

Interface: eth0/192.168.6.38
LOG: Target: 192.168.6.43
LOG: Netmask: 255.255.255.255
LOG: probing: 192.168.6.43
LOG: [send]-> UDP to 192.168.6.43:32132
LOG: [98 bytes] sent, waiting for response.
LOG: [send]-> ICMP echo request to 192.168.6.43
LOG: [68 bytes] sent, waiting for response.
LOG: [send]-> ICMP time stamp request to 192.168.6.43
LOG: [68 bytes] sent, waiting for response.
LOG: [send]-> ICMP address mask request to 192.168.6.43
LOG: [48 bytes] sent, waiting for response.
INAL:[Windows 98/98SE]

Zdalna identyfikacja rodzaju i wersji systemu operacyjnego (*fingerprinting*)

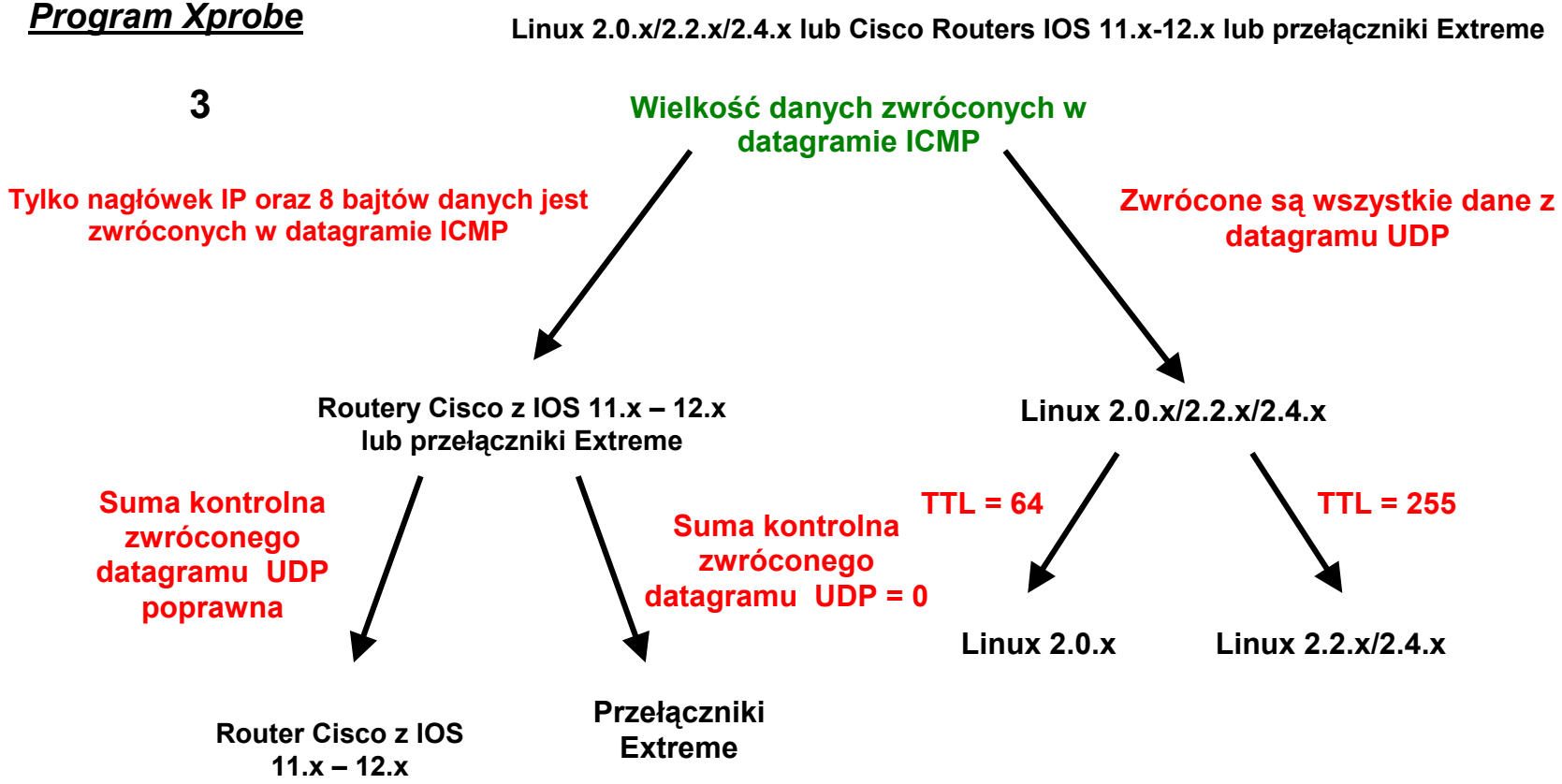
Program Xprobe



Zdalna identyfikacja rodzaju i wersji systemu operacyjnego (*fingerprinting*)

Program Xprobe

3



Enumeracja

Enumeracją nazywamy proces wyszukiwania poprawnych kont użytkowników lub źle zabezpieczonych zasobów współdzielonych.

Do głównych rodzajów zbieranych informacji należą:

- **zasoby sieciowe i ich udostępnianie,**
- **użytkownicy i grupy,**
- **aplikacje i etykiety.**

Enumeracja systemu Windows NT i W2K

Tworzenie *pustej sesji:*

net use \\192.168.1.2\IPC$ "" /user:""

Nazwa NetBIOS	Przyrostek	Usługa
<nazwa komputera>	00	Workstation
<nazwa komputera>	01	Messenger
<nazwa komputera>	03	Messenger
<nazwa komputera>	06	RAS Server
<nazwa komputera>	21	RAS Client
<nazwa komputera>	30	Modem Sharing Server
<nazwa komputera>	20	Server
<nazwa użytkownika>	03	Messenger
<nazwa domeny>	00	Domain Name
<nazwa domeny>	1B	Domain Master Browser
<nazwa domeny>	1C	Domain Controller
<nazwa domeny>	1E	Browser Service Election
<_MS_BROWSE_>	01	Master Browser
<INet~Services>	1C	Iis
<IS~nazwa komputera>	00	IIS

Enumeracja systemu Windows NT i W2K

Poprawka *RestrictAnonymous* w kluczu:
HKLM\SYSTEM\CurrentControlSet\Control\LSA

Nazwa wartości: ***RestrictAnonymous***
Typ danych: **REG_DWORD**
Wartość: **1 (2 - dla W2K)**

Udostępnianie danych przez agenta SNMP

- **uruchomione usługi,**
- **nazwy zasobów sieciowych,**
- **nazwy użytkowników,**
- **nazwy domen,**
- **nazwy komputerów,**
- **szczegółowe informacje dotyczące konfiguracji urządzeń.**

Metody obrony:

- **Usunięcie agenta SNMP lub wyłączenie (niewłączanie) usługi SNMP.**
- **Skonfigurowanie prywatnej nazwy wspólnoty.**
- **Określenie adresów zaufanych serwerów.**
- **Modyfikacja rejestru aby dopuszczać jedynie autoryzowany dostęp do nazwy wspólnoty SNMP:**

HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities
HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents

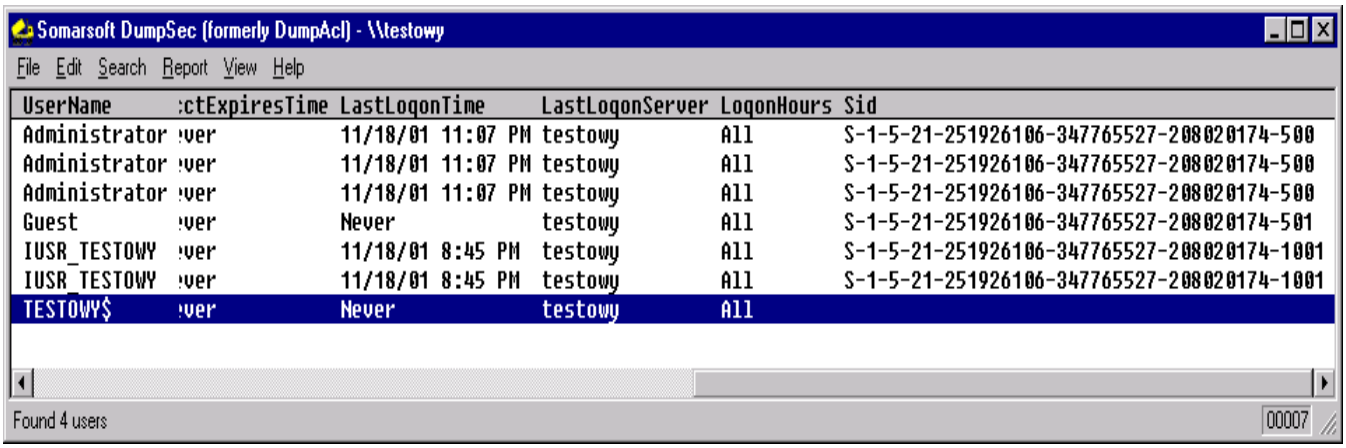
- **Blokada portu 161 TCP i UDP (SNMP GET/SET) w granicznych urządzeniach kontroli dostępu (odcięcie od sieci publicznej).**

Enumeracja systemu Windows NT i W2K

Enumeracja z wykorzystaniem DNS

- rekordy SRV
- transfer strefy

Enumeracja kont z wykorzystaniem SID



Enumeracja *Active Directory*

dwa tryby pracy *Active Directory*

Przechwytywanie etykiet z wykorzystaniem usługi *telnet*

```
c:\telnet   www.testowa.com  80
HTTP/1.0  400 Bad Request
Server:  Netscape-Commerce/1.12
Your browser sent a non-HTTP compliant message
```

Pobieranie zawartości rejestru

HKLM\System\CurrentControlSet\Control\SecurePipeServer\WinReg\AllowedPaths
HKLM\Software\Microsoft\WindowsNT\CurrentVersion.

Enumeracja systemu Windows NT/2000 przy użyciu narzędzi wbudowanych w system operacyjny:

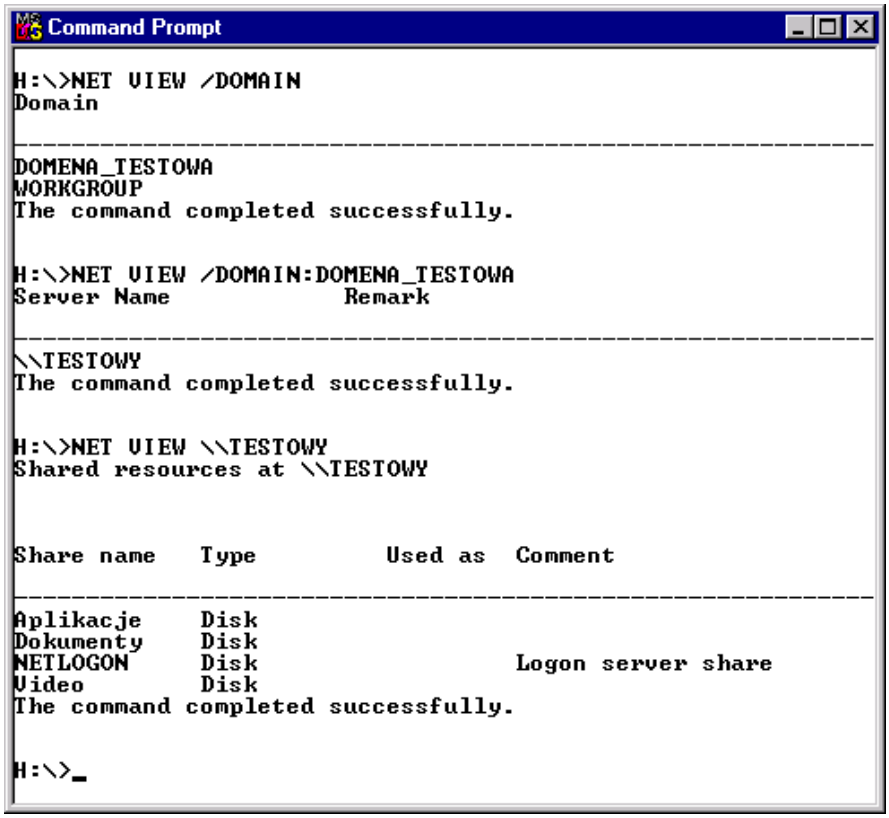
- **Polecenie *net view*.**
- **Program *nbtstat*.**

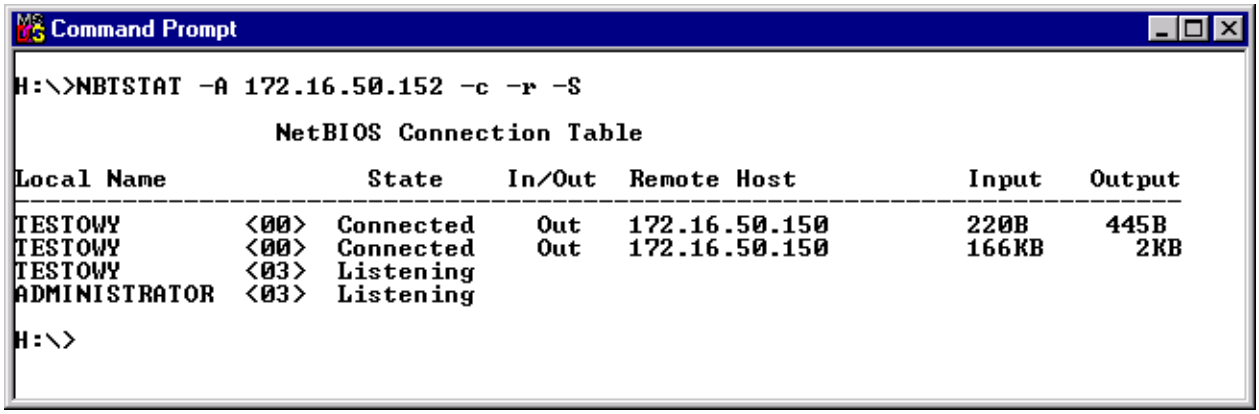
Enumeracja systemu Windows NT przy użyciu narzędzi z zestawu *Windows NT Resource Kit*:

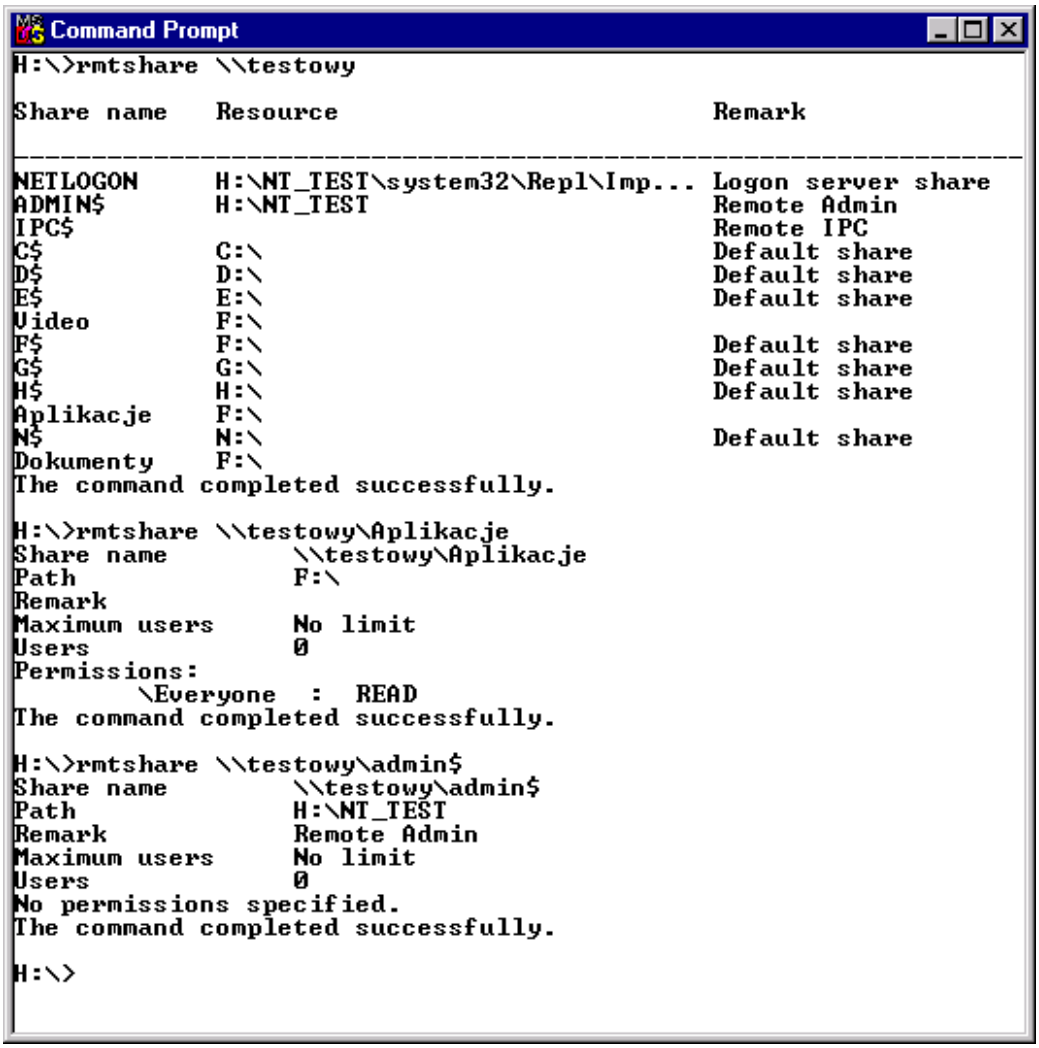
- ***nltest***
- ***srvcheck***
- ***getmac***
- ***snmputil***
- ***showgrps***
- ***global***
- ***rmtshare.***
- ***srvinfo***
- ***netdom*.**
- ***usrstat***
- ***local***
- ***regdmp***

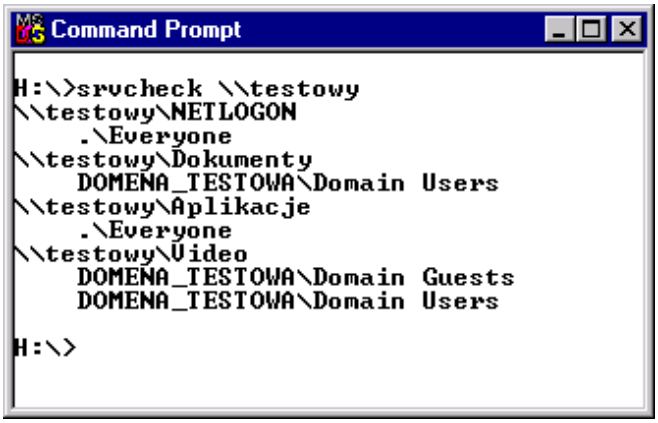
Enumeracja systemu Windows NT przy użyciu narzędzi dostępnych w Internecie:

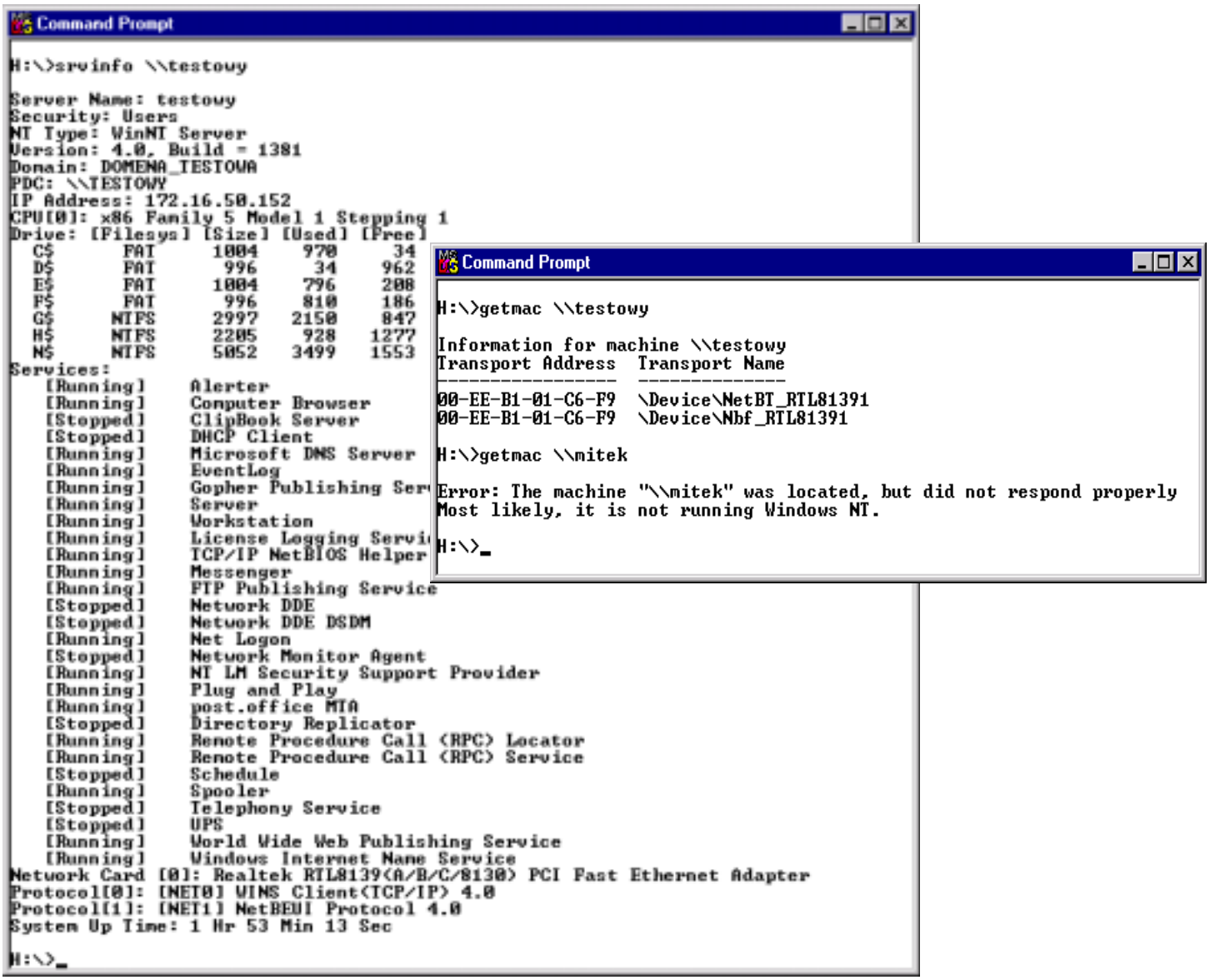
- ***nbtscan***
- ***Legion***
- ***epdump***
- ***winfo***
- ***enum***
- ***user2sid***
- ***netcat*** -
- ***DumpSec*** -
- ***NetBIOS Auditing Tool (NAT)***
- ***netviewx***
- ***nbtdump***
- ***IP Network Browser***
- ***sid2user***

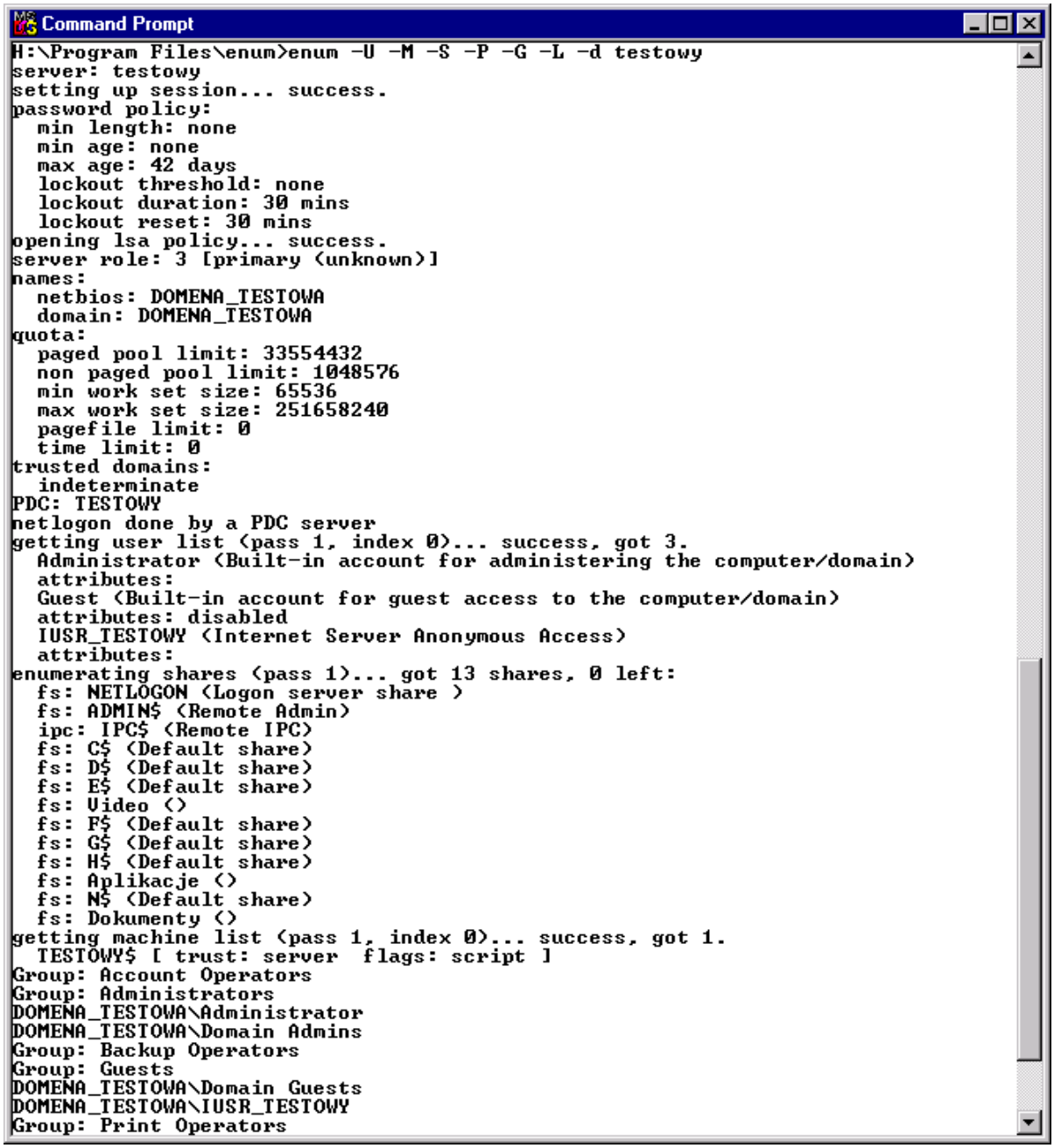

Command Prompt
H:\>NET VIEW /DOMAIN
Domain
DOMENA_TESTOWA
WORKGROUP
The command completed successfully.
H:\>NET VIEW /DOMAIN:DOMENA_TESTOWA
Server Name Remark
\\TESTOWY
The command completed successfully.
H:\>NET VIEW \\TESTOWY
Shared resources at \\TESTOWY
Share name Type Used as Comment
Aplikacje Disk
Dokumenty Disk
NETLOGON Disk Logon server share
Video Disk
The command completed successfully.
H:\>

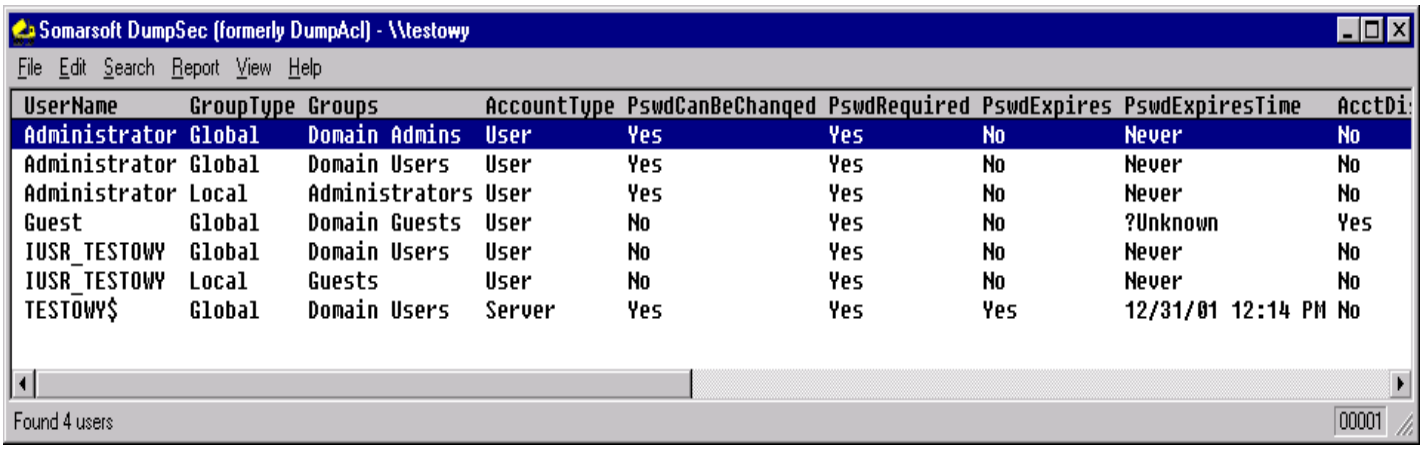

Command Prompt
H:\>NBTSTAT -A 172.16.50.152 -c -r -S
NetBIOS Connection Table
Local Name State In/Out Remote Host Input Output
TESTOWY <00> Connected Out 172.16.50.150 220B 445B
TESTOWY <00> Connected Out 172.16.50.150 166KB 2KB
TESTOWY <03> Listening
ADMINISTRATOR <03> Listening
H:\>


Command Prompt
H:\>rmtshare \\testowy
Share name Resource Remark
NETLOGON H:\NT_TEST\system32\Repl\Imp... Logon server share
ADMIN$ H:\NT_TEST Remote Admin
IPC$ Remote IPC
C$ C:\ Default share
D$ D:\ Default share
E$ E:\ Default share
Video F:\
F$ F:\ Default share
G$ G:\ Default share
H$ H:\ Default share
Aplikacje F:\
N$ N:\ Default share
Dokumenty F:\
The command completed successfully.
H:\>rmtshare \\testowy\Aplikacje
Share name \\testowy\Aplikacje
Path F:\
Remark
Maximum users No limit
Users 0
Permissions:
\Everyone : READ
The command completed successfully.
H:\>rmtshare \\testowy\admin$
Share name \\testowy\admin$
Path H:\NT_TEST
Remark Remote Admin
Maximum users No limit
Users 0
No permissions specified.
The command completed successfully.
H:\>


Command Prompt
H:\>srvcheck \\testowy
\\testowy\NETLOGON
.\Everyone
\\testowy\Dokumenty
DOMENA_TESTOWA\Domain Users
\\testowy\Aplikacje
.\Everyone
\\testowy\Video
DOMENA_TESTOWA\Domain Guests
DOMENA_TESTOWA\Domain Users
H:\>

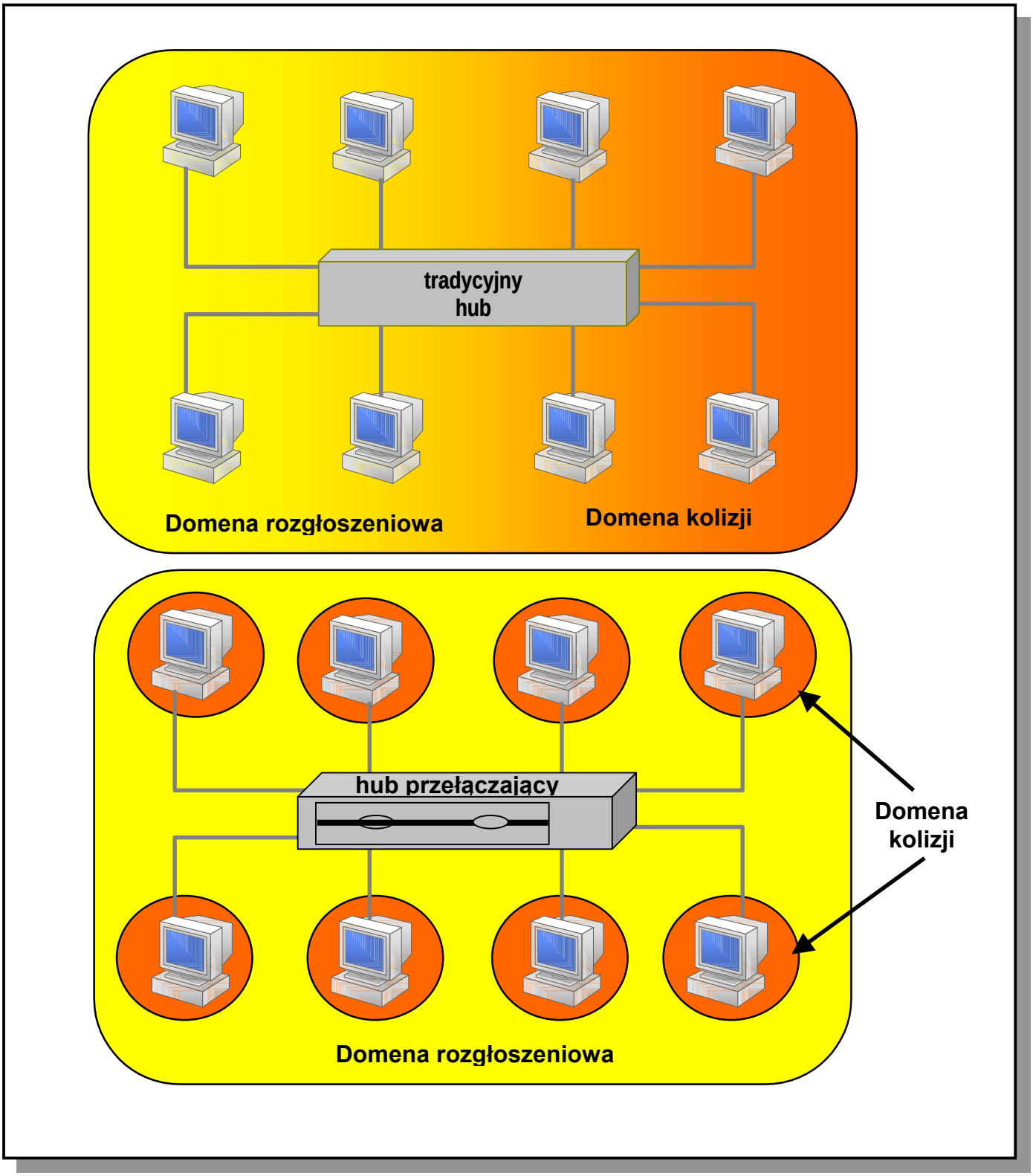

Command Prompt
H:\>srvinfo \\testowy
Server Name: testowy
Security: Users
NT Type: WinNT Server
Version: 4.0, Build = 1381
Domain: DOMENA_TESTOWA
PDC: \\TESTOWY
IP Address: 172.16.50.152
CPU[0]: x86 Family 5 Model 1 Stepping 1
Drive: [Filesys] [Size] [Used] [Free]
C$ FAT 1004 970 34
D$ FAT 996 34 962
E$ FAT 1004 796 208
F$ FAT 996 810 186
G$ NTFS 2997 2150 847
H$ NTFS 2205 928 1277
N$ NTFS 5052 3499 1553
Services:
[Running] Alerter
[Running] Computer Browser
[Stopped] ClipBook Server
[Stopped] DHCP Client
[Running] Microsoft DNS Server
[Running] EventLog
[Running] Gopher Publishing Ser
[Running] Server
[Running] Workstation
[Running] License Logging Servi
[Running] TCP/IP NetBIOS Helper
[Running] Messenger
[Running] FTP Publishing Service
[Stopped] Network DDE
[Stopped] Network DDE DSDM
[Running] Net Logon
[Stopped] Network Monitor Agent
[Running] NT LM Security Support Provider
[Running] Plug and Play
[Running] post.office MTA
[Stopped] Directory Replicator
[Running] Remote Procedure Call (RPC) Locator
[Running] Remote Procedure Call (RPC) Service
[Stopped] Schedule
[Running] Spooler
[Stopped] Telephony Service
[Stopped] UPS
[Running] World Wide Web Publishing Service
[Running] Windows Internet Name Service
Network Card [0]: Realtek RTL8139(A/B/C/8130) PCI Fast Ethernet Adapter
Protocol[0]: [NET0] WINS Client(TCP/IP) 4.0
Protocol[1]: [NET1] NetBEUI Protocol 4.0
System Up Time: 1 Hr 53 Min 13 Sec
H:\>
Command Prompt
H:\>getmac \\testowy
Information for machine \\testowy
Transport Address Transport Name
00-EE-B1-01-C6-F9 \Device\NetBT_RTL81391
00-EE-B1-01-C6-F9 \Device\Nbf_RTL81391
H:\>getmac \\mitek
Error: The machine "\\mitek" was located, but did not respond properly
Most likely, it is not running Windows NT.
H:\>

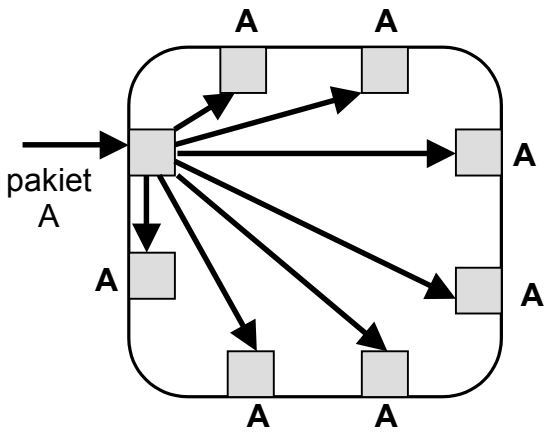

Command Prompt
H:\Program Files\enum>enum -U -M -S -P -G -L -d testowy
server: testowy
setting up session... success.
password policy:
min length: none
min age: none
max age: 42 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
netbios: DOMENA_TESTOWA
domain: DOMENA_TESTOWA
quota:
paged pool limit: 33554432
non paged pool limit: 1048576
min work set size: 65536
max work set size: 251658240
pagefile limit: 0
time limit: 0
trusted domains:
indeterminate
PDC: TESTOWY
netlogon done by a PDC server
getting user list (pass 1, index 0)... success, got 3.
Administrator (Built-in account for administering the computer/domain)
attributes:
Guest (Built-in account for guest access to the computer/domain)
attributes: disabled
IUSR_TESTOWY (Internet Server Anonymous Access)
attributes:
enumerating shares (pass 1)... got 13 shares, 0 left:
fs: NETLOGON (Logon server share)
fs: ADMIN$ (Remote Admin)
ipc: IPC$ (Remote IPC)
fs: C$ (Default share)
fs: D$ (Default share)
fs: E$ (Default share)
fs: Video ()
fs: F$ (Default share)
fs: G$ (Default share)
fs: H$ (Default share)
fs: Aplikacje ()
fs: N$ (Default share)
fs: Dokumenty ()
getting machine list (pass 1, index 0)... success, got 1.
TESTOWY$ [trust: server flags: script]
Group: Account Operators
Group: Administrators
DOMENA_TESTOWA\Administrator
DOMENA_TESTOWA\Domain Admins
Group: Backup Operators
Group: Guests
DOMENA_TESTOWA\Domain Guests
DOMENA_TESTOWA\IUSR_TESTOWY
Group: Print Operators

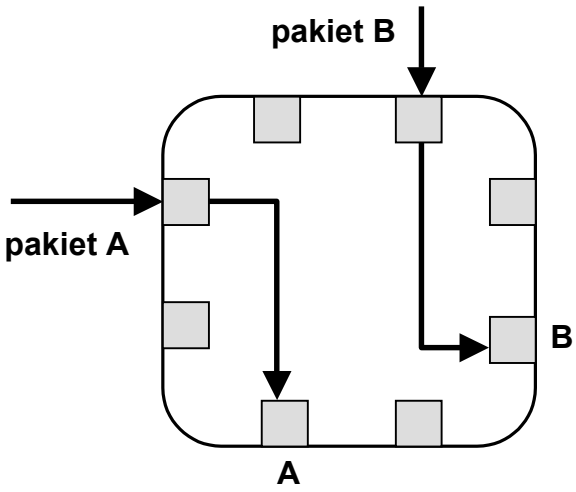

Somarsoft DumpSec (formerly DumpAcl) - \\testowy
File Edit Search Report View Help
UserName GroupType Groups AccountType PswdCanBeChanged PswdRequired PswdExpires PswdExpiresTime AcctDi
Administrator Global Domain Admins User Yes Yes No Never No
Administrator Global Domain Users User Yes Yes No Never No
Administrator Local Administrators User Yes Yes No Never No
Guest Global Domain Guests User No Yes No ?Unknown Yes
IUSR_TESTOWY Global Domain Users User No Yes No Never No
IUSR_TESTOWY Local Guests User No Yes No Never No
TESTOWY$ Global Domain Users Server Yes Yes Yes 12/31/01 12:14 PM No
Found 4 users
00001

Enumeracja systemu UNIX

- **Skanowanie**
- **NFS i program *showmount***
- **NIS i program *pscan***
- **SNMP i program *snmpwalk***
- **Program *finger***
- **Programy *rusers* lub *rwho***
- **Protokół SMTP i polecenia VRFY i EXPN**
- **Plik */etc/passwd* i protokół TFTP**
- **RPC i programy *portmapper* (*rpcbind*), *rpcinfo, rpcdump, netcat*.**


tradycyjny
hub
Domena rozgłoszeniowa
Domena kolizji
hub przełączający
Domena
kolizji
Domena rozgłoszeniowa

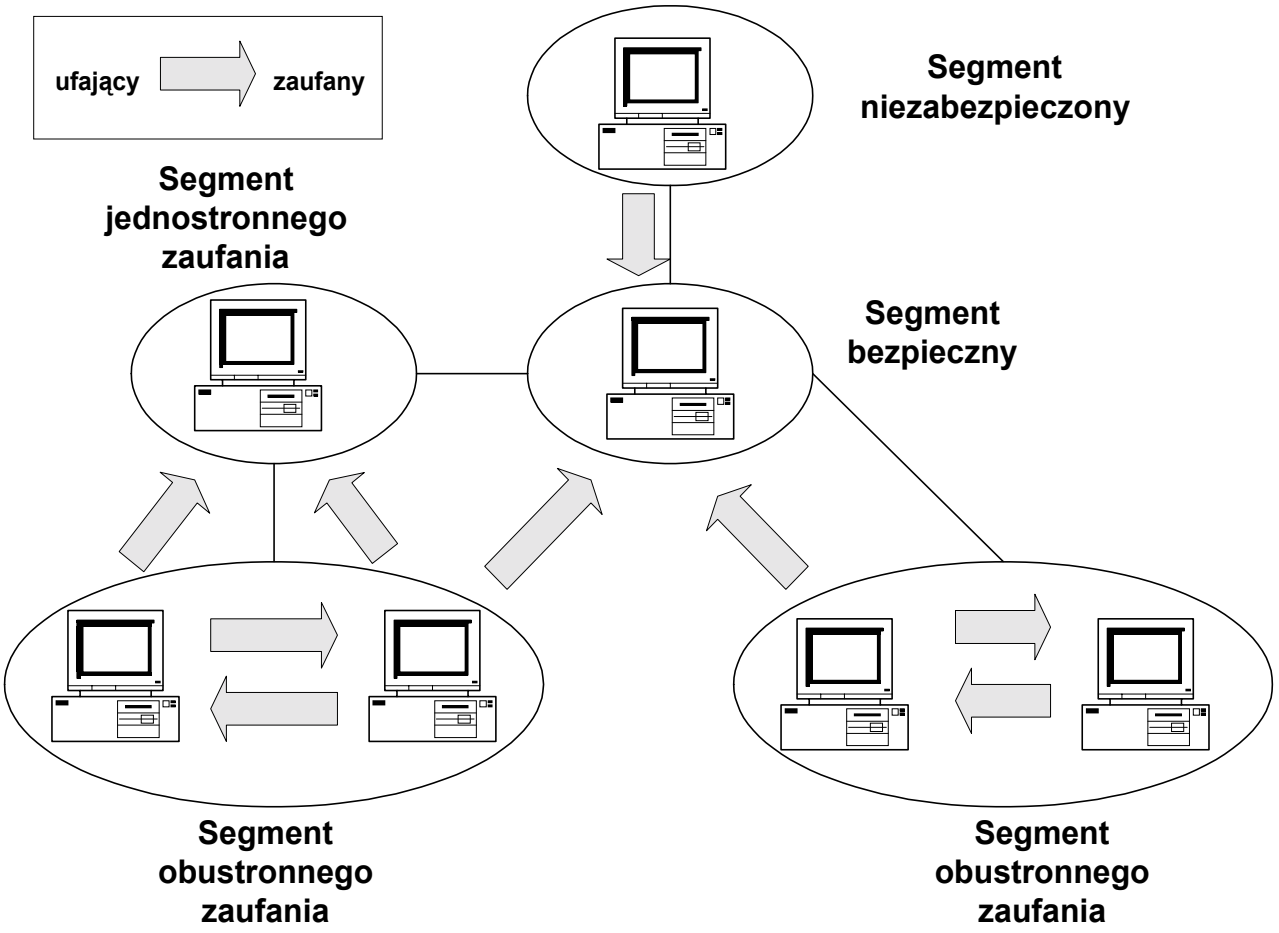




Hub tradycyjny
Pakiet odbierany przez port jest kierowany do wszystkich pozostałych portów

Hub przełączający
Pakiet odbierany przez port jest kierowany tylko do jednego portu - do tego, do którego jest dołączona stacja końcowa

Relacje zaufania i podział na segmenty



Literatura:

1) V. Ahuja. *Network & Internet Security*. Academic Press, Inc, 1996. (*tłum. MIKOM 1997*).
2) D. Atkins i inni. *Internet Security. Professional Reference.* New Riders Publishing, 1997 (*tłum. LT&P 1997*).
3) S. Garfinkel, G. Spafford. *Practical Unix and Internet Security,* O'Reilly&Associates Inc. 1996. (*tłum. RM 1997*).
4) J. Hruska, Computer viruses and antivirus warfare, Prentice Hall Int. 1992 (*tłum*. WKŁ 1995).
5) L. Klander. *Hacker Proof.* Jamsa Press, 1997. (*tłum. MIKOM 1998*).
6) J. Scambray, S. McClure, G. Kurtz, *Hacking Exposed: Network Security Secrets & Solutions,* Osborne/Mc Graw Hill 2000*. (tłum Translator 2001).*
7) S. Waldbusser. *Remote Network Monitoring Management Information Base.* RFC 1271, Nov 1991.