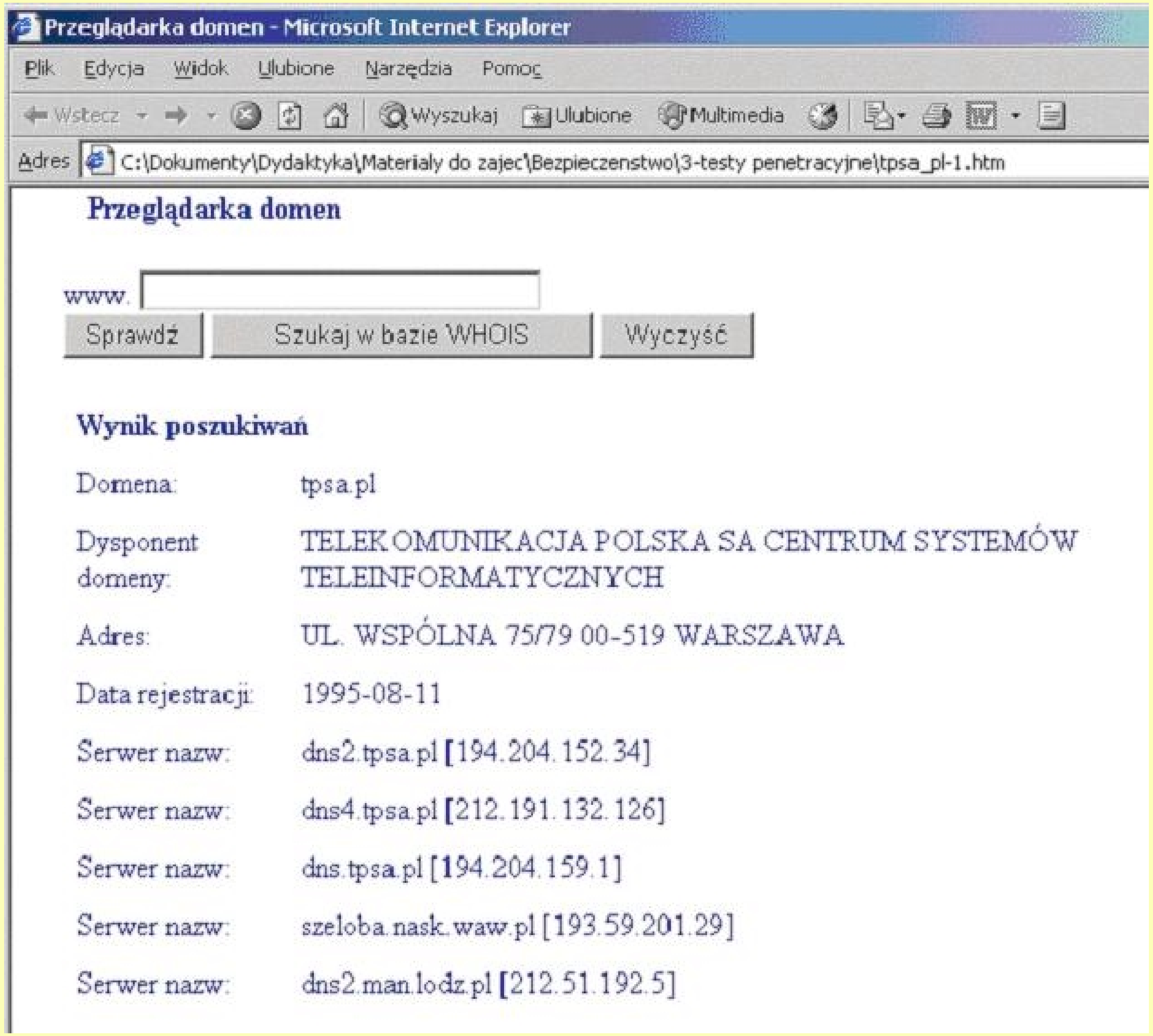
Bezpieczeństwo systemów informatycznych

Testy penetracyjne

Przykłady programów

Rekonesans - przykłady



Adres C:\Dokumenty\Dydaktyka\Materialy do zajec\Bezpieczenstwo\3-testy penetracyjne\tpsa_pl-1.htm

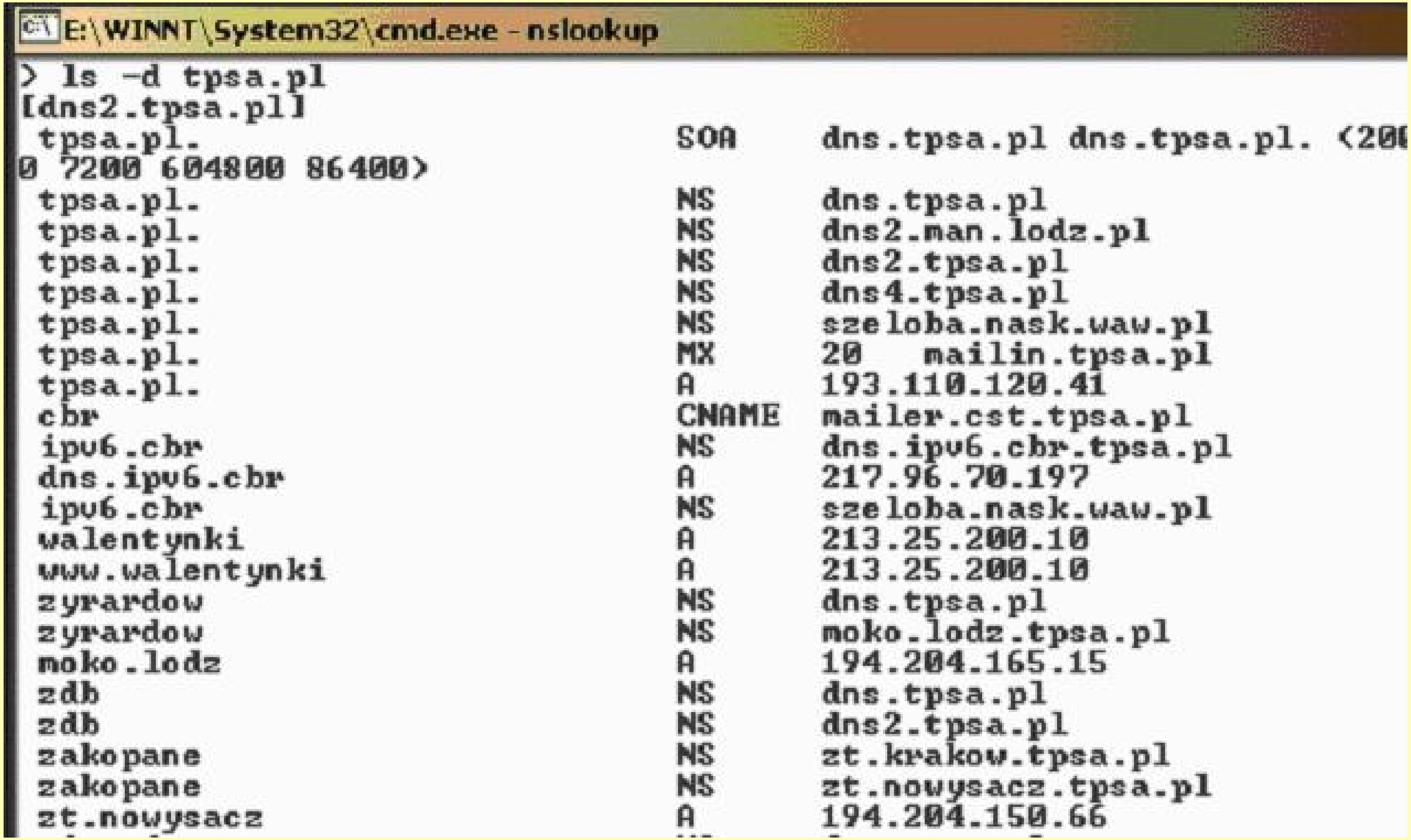
Przeglądarka domen

www.

Wynik poszukiwań

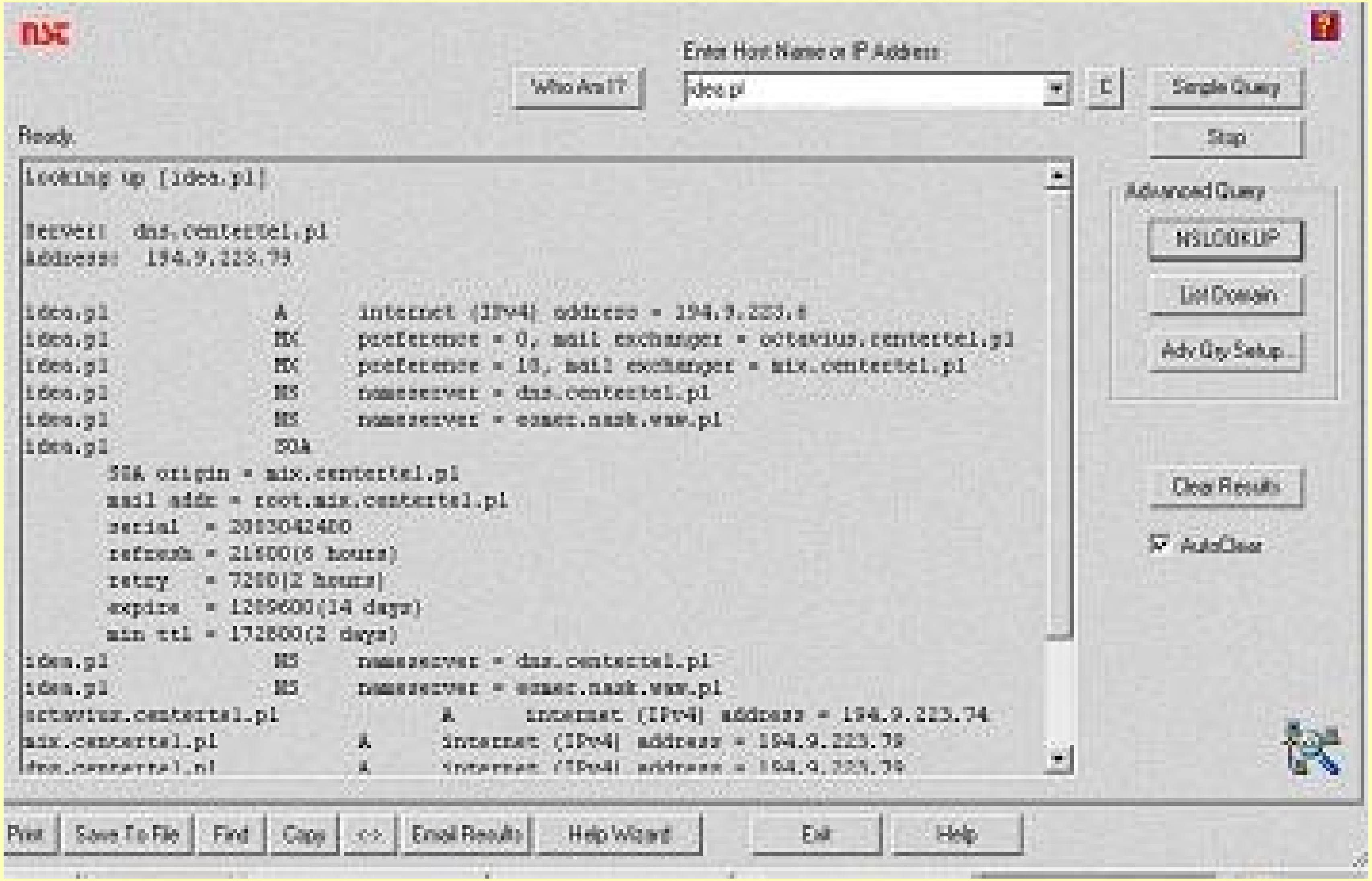
Domena:	tpsa.pl
Dysponent domeny:	TELEKOMUNIKACJA POLSKA SA CENTRUM SYSTEMÓW TELEINFORMATYCZNYCH
Adres:	UL. WSPÓLNA 75/79 00-519 WARSZAWA
Data rejestracji:	1995-08-11
Serwer nazw:	dns2.tpsa.pl [194.204.152.34]
Serwer nazw:	dns4.tpsa.pl [212.191.132.126]
Serwer nazw:	dns.tpsa.pl [194.204.159.1]
Serwer nazw:	szeloba.nask.waw.pl [193.59.201.29]
Serwer nazw:	dns2.man.lodz.pl [212.51.192.5]

Rekonesans - przykłady



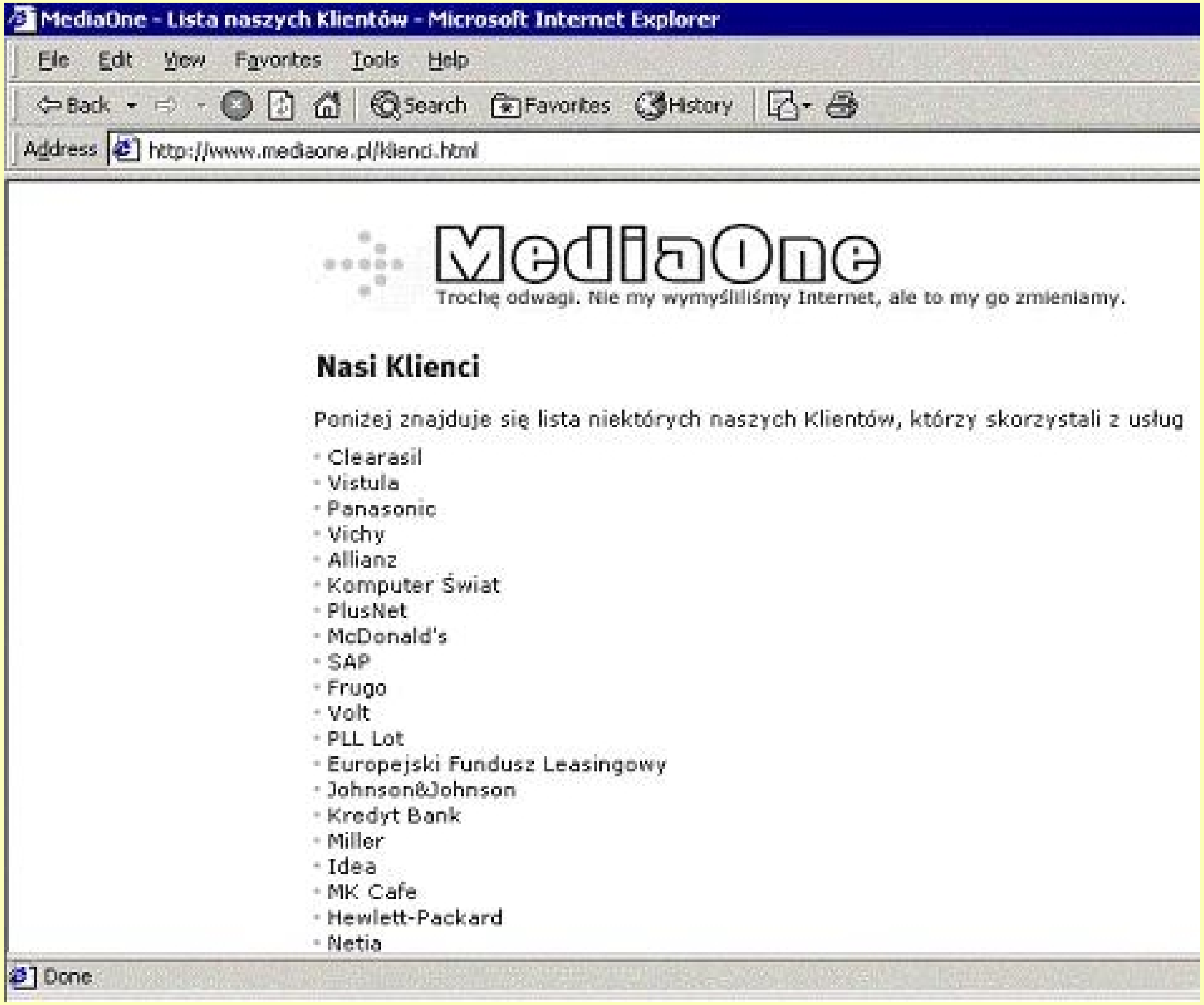
```
> ls -d tpsa.pl
[dns2.tpsa.pl]
 tpsa.pl.                       SOA    dns.tpsa.pl dns.tpsa.pl. (200
0 7200 604800 86400)
 tpsa.pl.                       NS     dns.tpsa.pl
 tpsa.pl.                       NS     dns2.man.lodz.pl
 tpsa.pl.                       NS     dns2.tpsa.pl
 tpsa.pl.                       NS     dns4.tpsa.pl
 tpsa.pl.                       NS     szeloba.nask.waw.pl
 tpsa.pl.                       MX     20   mailin.tpsa.pl
 tpsa.pl.                       A      193.110.120.41
 cbr                            CNAME  mailer.cst.tpsa.pl
 ipv6.cbr                       NS     dns.ipv6.cbr.tpsa.pl
 dns.ipv6.cbr                   A      217.96.70.197
 ipv6.cbr                       NS     szeloba.nask.waw.pl
 walentynki                     A      213.25.200.10
 www.walentynki                 A      213.25.200.10
 zyrardow                       NS     dns.tpsa.pl
 zyrardow                       NS     moko.lodz.tpsa.pl
 moko.lodz                      A      194.204.165.15
 zdb                            NS     dns.tpsa.pl
 zdb                            NS     dns2.tpsa.pl
 zakopane                       NS     zt.krakow.tpsa.pl
 zakopane                       NS     zt.nowysacz.tpsa.pl
 zt.nowysacz                    A      194.204.150.66
```

Rekonesans - przykłady



```
Looking up [idea.pl]

Server:   dns.centertel.pl
Address:   194.9.223.79

idea.pl              A     internet (IPv4) address = 194.9.223.6
idea.pl              MX    preference = 0, mail exchanger = octavius.centertel.pl
idea.pl              MX    preference = 10, mail exchanger = mix.centertel.pl
idea.pl              NS    nameserver = dns.centertel.pl
idea.pl              NS    nameserver = ecmec.nask.waw.pl
idea.pl              SOA
       SOA origin = mix.centertel.pl
       mail addr = root.mix.centertel.pl
       serial  = 2003042400
       refresh = 21600(6 hours)
       retry   = 7200(2 hours)
       expire  = 1209600(14 days)
       min ttl = 172800(2 days)
idea.pl              NS    nameserver = dns.centertel.pl
idea.pl              NS    nameserver = ecmec.nask.waw.pl
octavius.centertel.pl         A     internet (IPv4) address = 194.9.223.74
mix.centertel.pl         A     internet (IPv4) address = 194.9.223.78
dns.centertel.pl         A     internet (IPv4) address = 194.9.223.79
```

Rekonesans - przykłady



MediaOne - Lista naszych Klientów - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Done

http://www.mediaone.pl/klienci.html

MediaOne

Trochę odwagi. Nie my wymyśliliśmy Internet, ale to my go zmieniamy.

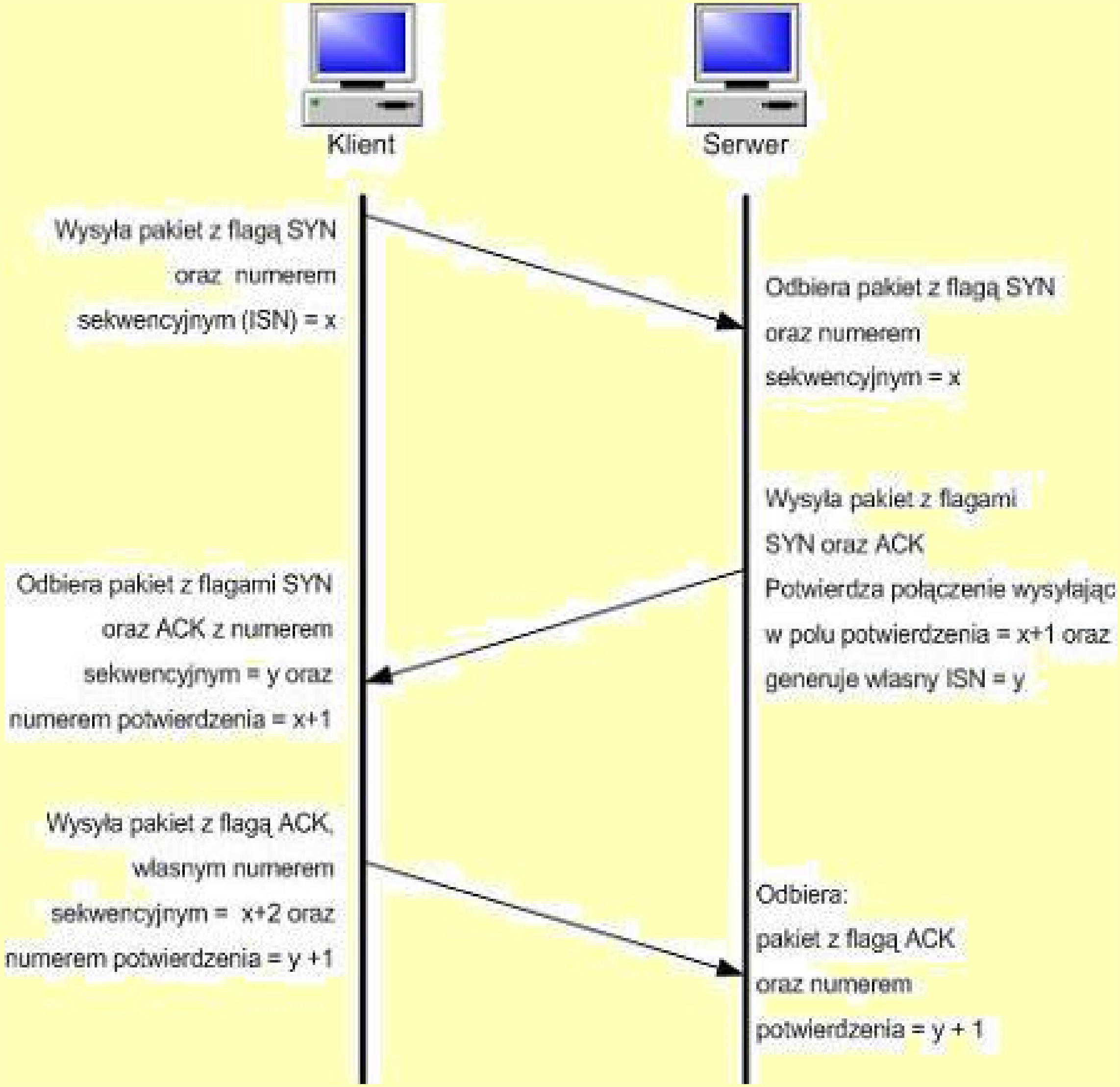
Nasi Klienci

Poniżej znajduje się lista niektórych naszych Klientów, którzy skorzystali z usług

- Clearasil
- Vistula
- Panasonic
- Vichy
- Allianz
- Komputer Świat
- PlusNet
- McDonald's
- SAP
- Frugo
- Volt
- PLL Lot
- Europejski Fundusz Leasingowy
- Johnson&Johnson
- Kredyt Bank
- Miller
- Idea
- MK Cafe
- Hewlett-Packard
- Netia

Skanowanie – techniki TCP

Skanowanie połączeniowe i półotwarte



Wysyła pakiet z flagą SYN oraz numerem sekwencyjnym (ISN) = x

Odbiera pakiet z flagą SYN oraz numerem sekwencyjnym = x

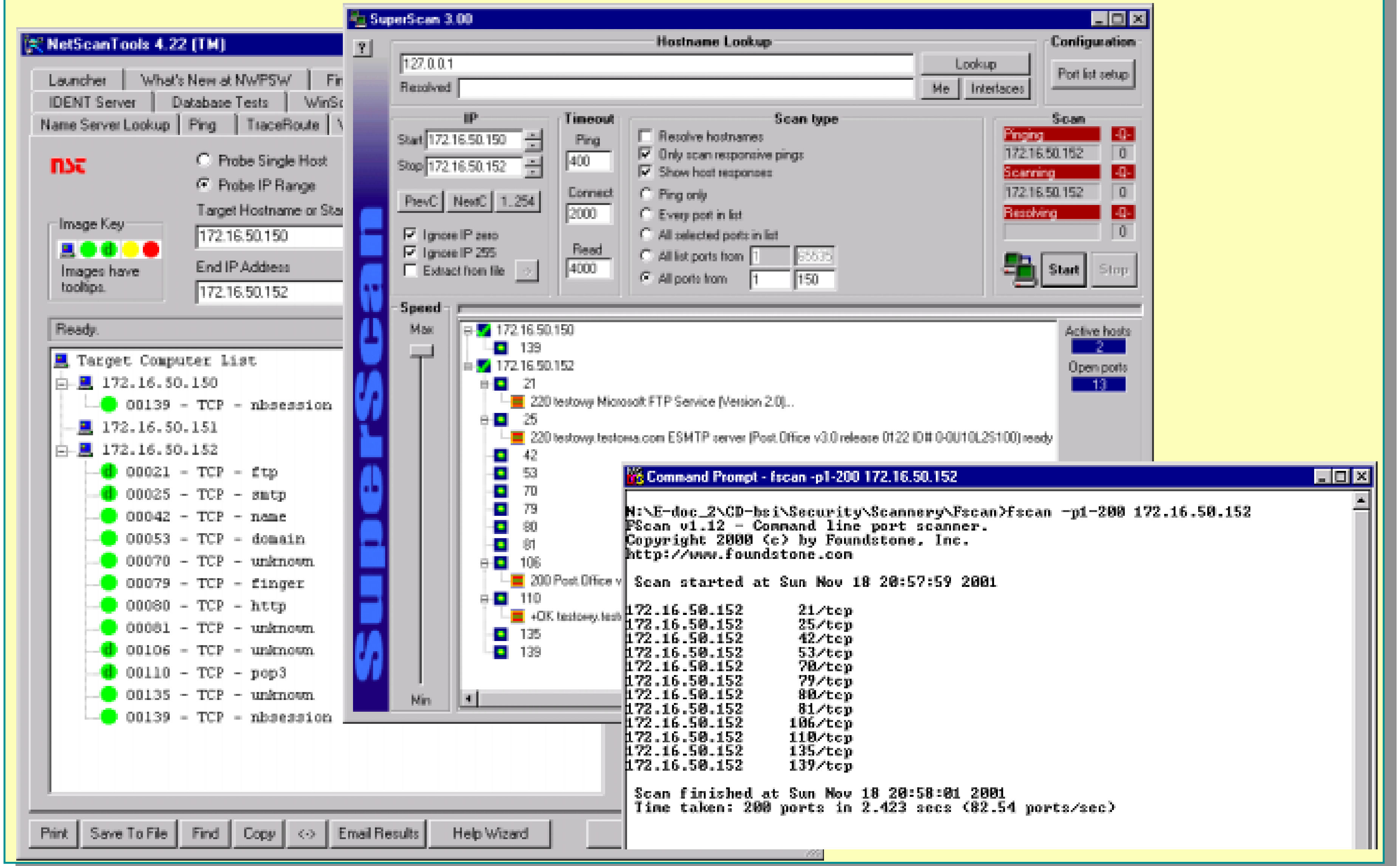
Wysyła pakiet z flagami SYN oraz ACK Potwierdza połączenie wysyłając w polu potwierdzenia = x+1 oraz generuje własny ISN = y

Odbiera pakiet z flagami SYN oraz ACK z numerem sekwencyjnym = y oraz numerem potwierdzenia = x+1

Wysyła pakiet z flagą ACK, własnym numerem sekwencyjnym = x+2 oraz numerem potwierdzenia = y +1

Odbiera: pakiet z flagą ACK oraz numerem potwierdzenia = y + 1

Skanowanie - przykłady



○ Probe Single Host
● Probe IP Range

Target Hostname or Sta
172.16.50.150

End IP Address
172.16.50.152

Ready.

```
Target Computer List
172.16.50.150
    00139 - TCP - nbsession
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
```

Hostname Lookup: 127.0.0.1
Resolved:

IP — Start: 172.16.50.150; Stop: 172.16.50.152
☑ 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 1 65535
● All ports from 1 150

Scan
Pinging -0-
172.16.50.152 0
Scanning -0-
172.16.50.152 0
Resolving -0-
0

Active hosts: 2
Open ports: 13

```
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# 0-0U10L25100) ready
    42
    53
    70
    79
    80
    81
    106
        200 Post Office v
    110
        +OK testowy.test
    135
    139
```

Command Prompt - fscan -p1-200 172.16.50.152

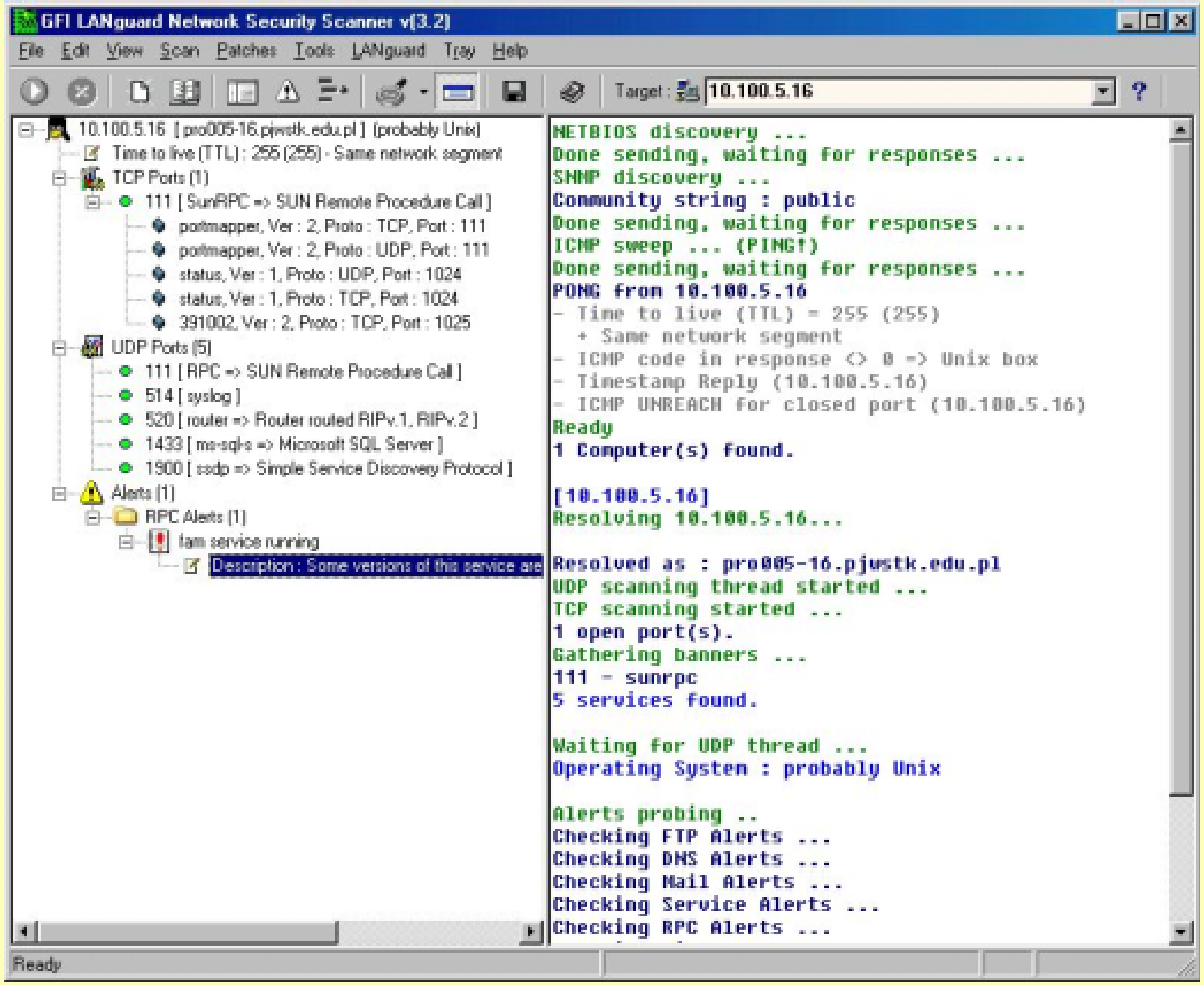
```
N:\E-doc_2\CD-bsi\Security\Scannery\Fscan>fscan -p1-200 172.16.50.152
FScan v1.12 - Command line port scanner.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

 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)
```

Zdalna identyfikacja systemu operacyjnego

```
ftp> open ftp.netscape.com
Connected to 207.200.85.53 (207.200.85.53)
220 ftp.netscape.com FTP server (SunOS 5.8) ready
Name (ftp.netscape.com:anonymous): anonymous
331 Guest login ok, send your complete e-mail address
as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> SYST
215 UNIX Type: L8 Version SUNOS
```

```
[~]# telnet 192.168.9.130
Trying 192.168.9.130 ...
Connected to potato.
Escape character is ‘^]’.
Debian GNU/Linux 2.2 potato
login:
```

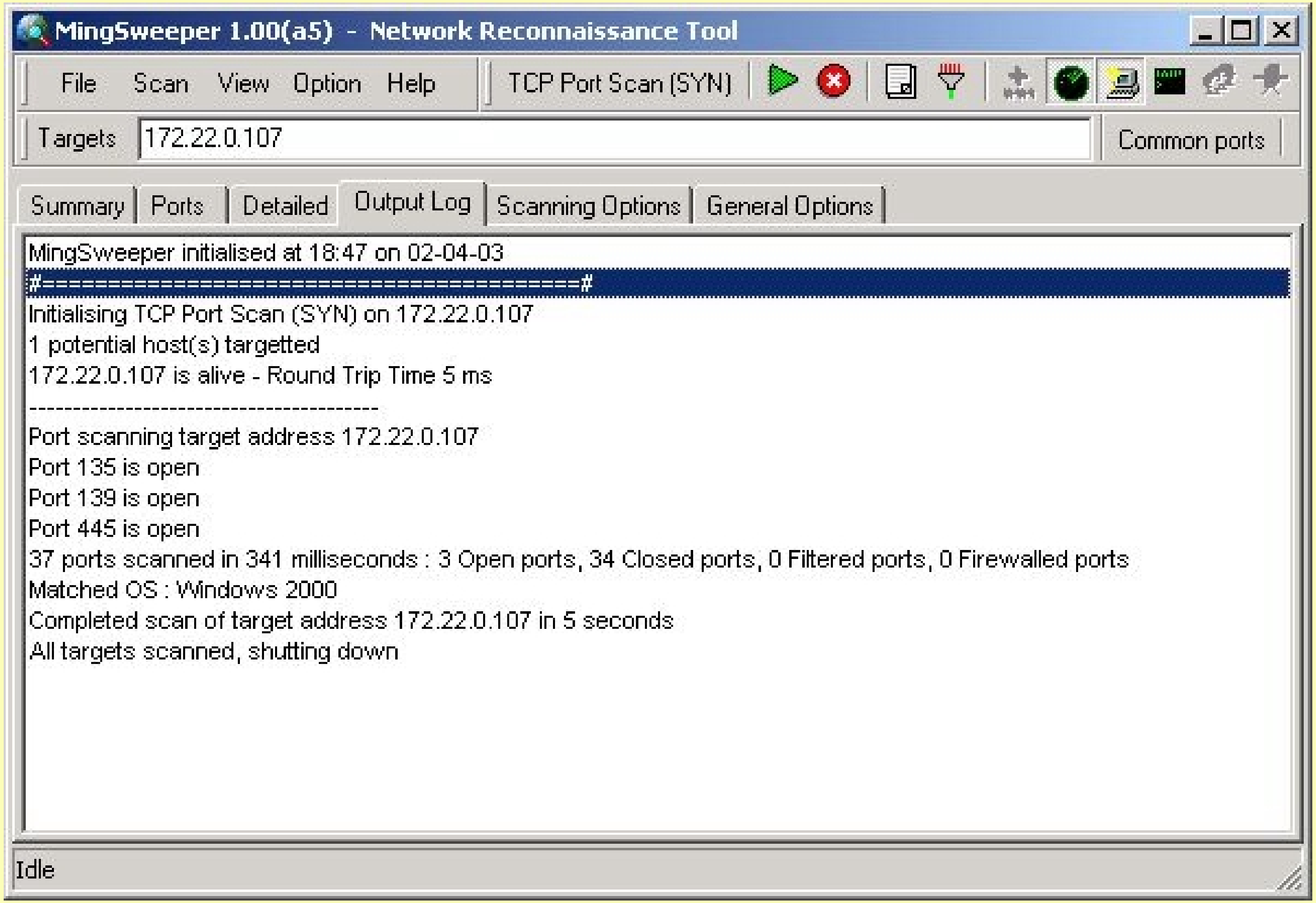
Zdalna identyfikacja systemu operacyjnego


GFI LANguard Network Security Scanner v(3.2)
File Edit View Scan Patches Tools LANguard Tray Help
Target : 10.100.5.16
Ready

```
10.100.5.16 [ pro005-16.pjwstk.edu.pl ] (probably Unix)
  Time to live (TTL) : 255 (255) - Same network segment
  TCP Ports (1)
    111 [ SunRPC => SUN Remote Procedure Call ]
      portmapper, Ver : 2, Proto : TCP, Port : 111
      portmapper, Ver : 2, Proto : UDP, Port : 111
      status, Ver : 1, Proto : UDP, Port : 1024
      status, Ver : 1, Proto : TCP, Port : 1024
      391002, Ver : 2, Proto : TCP, Port : 1025
  UDP Ports (5)
    111 [ RPC => SUN Remote Procedure Call ]
    514 [ syslog ]
    520 [ router => Router routed RIPv.1, RIPv.2 ]
    1433 [ ms-sql-s => Microsoft SQL Server ]
    1900 [ ssdp => Simple Service Discovery Protocol ]
  Alerts (1)
    RPC Alerts (1)
      fam service running
        Description : Some versions of this service are
```

```
NETBIOS discovery ...
Done sending, waiting for responses ...
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING!)
Done sending, waiting for responses ...
PONG from 10.100.5.16
- Time to live (TTL) = 255 (255)
  + Same network segment
- ICMP code in response <> 0 -> Unix box
- Timestamp Reply (10.100.5.16)
- ICMP UNREACH for closed port (10.100.5.16)
Ready
1 Computer(s) found.

[10.100.5.16]
Resolving 10.100.5.16...

Resolved as : pro005-16.pjwstk.edu.pl
UDP scanning thread started ...
TCP scanning started ...
1 open port(s).
Gathering banners ...
111 - sunrpc
5 services found.

Waiting for UDP thread ...
Operating System : probably Unix

Alerts probing ..
Checking FTP Alerts ...
Checking DNS Alerts ...
Checking Mail Alerts ...
Checking Service Alerts ...
Checking RPC Alerts ...
```

Zdalna identyfikacja systemu operacyjnego



```
MingSweeper initialised at 18:47 on 02-04-03
#========================================#
Initialising TCP Port Scan (SYN) on 172.22.0.107
1 potential host(s) targetted
172.22.0.107 is alive - Round Trip Time 5 ms
----------------------------------------
Port scanning target address 172.22.0.107
Port 135 is open
Port 139 is open
Port 445 is open
37 ports scanned in 341 milliseconds : 3 Open ports, 34 Closed ports, 0 Filtered ports, 0 Firewalled ports
Matched OS : Windows 2000
Completed scan of target address 172.22.0.107 in 5 seconds
All targets scanned, shutting down
```

Zdalna identyfikacja systemu operacyjnego

```
[~]# nmap -O 10.100.5.16
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on pro.pjwstk.edu.pl (10.100.5.16):

Port       State       Service
23/tcp     open        telnet
111/tcp    open        sunrpc
1024/tcp   open        kdm

Remote operating system guess: Linux Kernel 2.4.0-2.5.20
Uptime 0.024 days (since Wed Apr  2 08:46:48 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds
```

Zdalna identyfikacja systemu operacyjnego

```
[/usr/src/bsf]# ./bsf -t 10.1.1.15 –v
BSF v1.1.2ALPHA2
Better Stack Fingerprinting.
Host 10.1.1.15 appears up.
Preforming BSF traceroute to 10.1.1.15:
hop 1: 10.1.1.15
We are 1 hop(s) away.
BSF traceroute completed in 0 second(s).

Begining to probe 10.1.1.15 (-)
P1: TTL: 129, IPID:64885, ICMPID:40042, ICMP_SEQ:49339
P2: TTL: 129 , IPID: 64891 , ICMPID: 41482 , ICMP_SEQ: 32393
P3: TTL: 129 , IPID: 64898 , ICMPID: 39881 , ICMP_SEQ:  2071
P4: TTL: 129 , IPID: 64905 , ICMPID: 45549 , ICMP_SEQ: 53495
P5: TTL: 129 , IPID: 64910 , ICMPID: 26507 , ICMP_SEQ: 47664
P6: TTL: 129 , IPID: 64917 , ICMPID: 55108 , ICMP_SEQ:  4540
Generated Fingerprint: NC129D677LLLHLH
Predicted Operating System: Microsoft Windows XP Pro RC1 through final
release
```

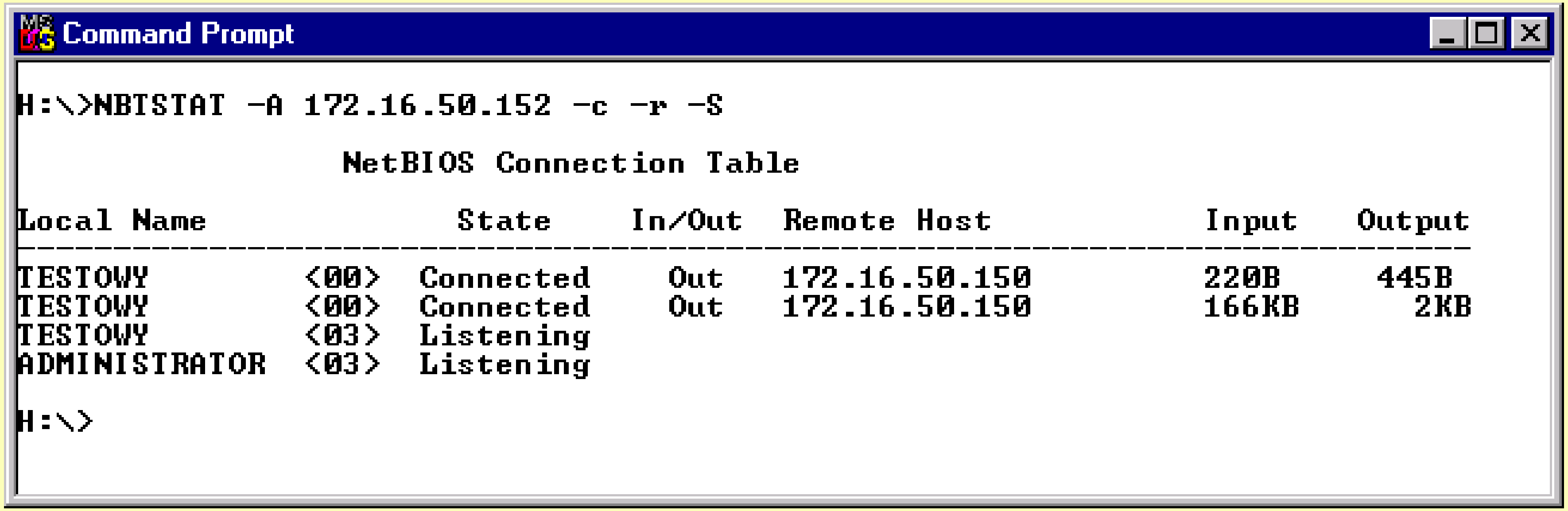
Zdalna identyfikacja systemu operacyjnego

```
[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 ]
```

Program Xprobe

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

Enumeracja systemu Windows (Nazwy NetBIOS)

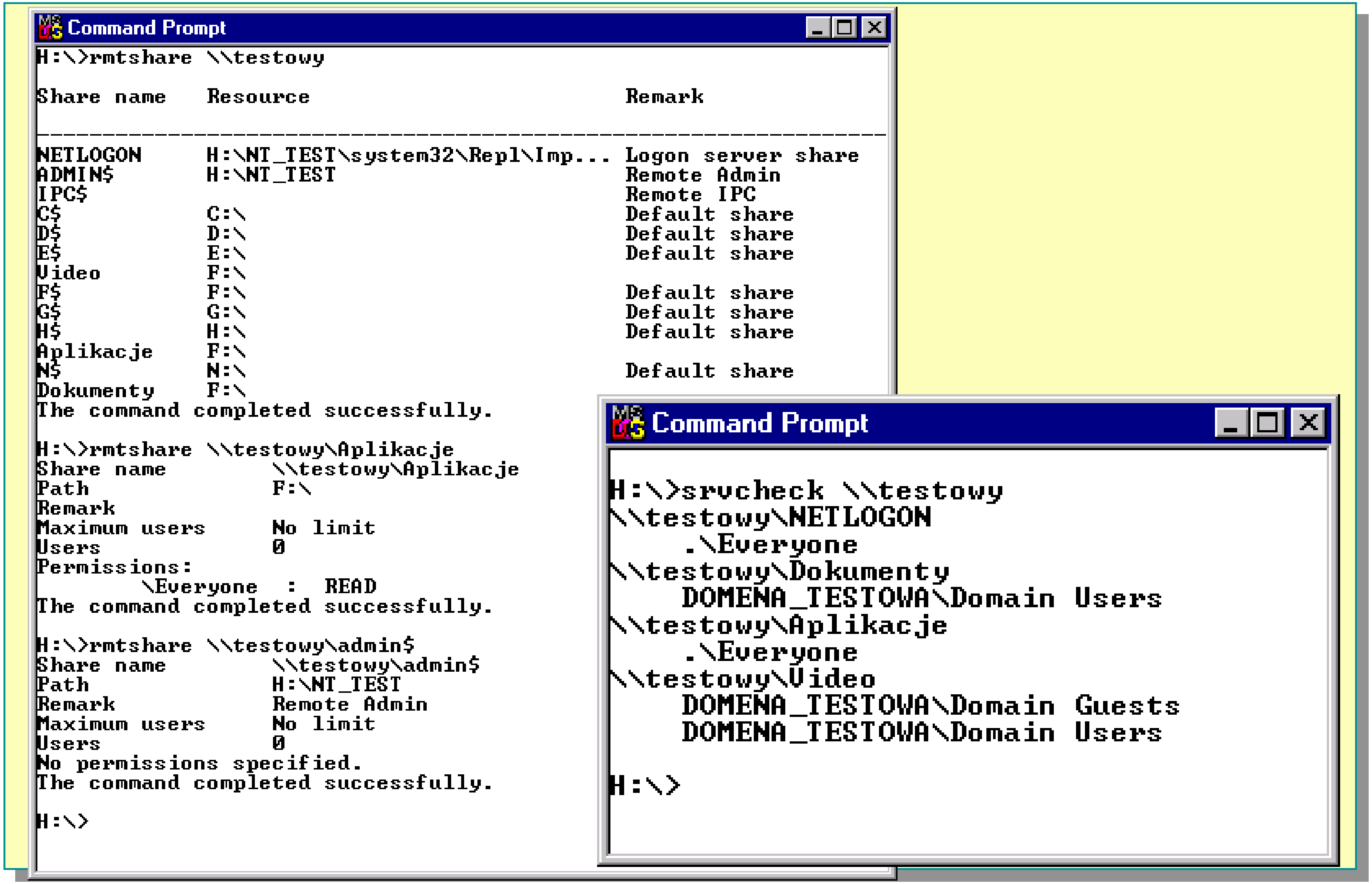


```
H:\>NBTSTAT -A 172.16.50.152 -c -r -S

                 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:\>
```

Enumeracja systemu Windows (Nazwy NetBIOS)

```
C:\net view \\192.168.3.58
Shared resources at \\192.168.3.58
Share name Type Used as Comment
----------------------------------------------------------------------------
BE                    Dysk
CertEnroll            Dysk            Certificate Services share
Home                  Dysk
HPColorL_new          Wydruk          HP Color LaserJet 4550
LJ2200                Wydruk          HP LaserJet 2200 Series PCL 5e
NETLOGON              Dysk            Logon server share
profile               Dysk
SYSVOL                Dysk            Logon server share

The command completed successfully.
```

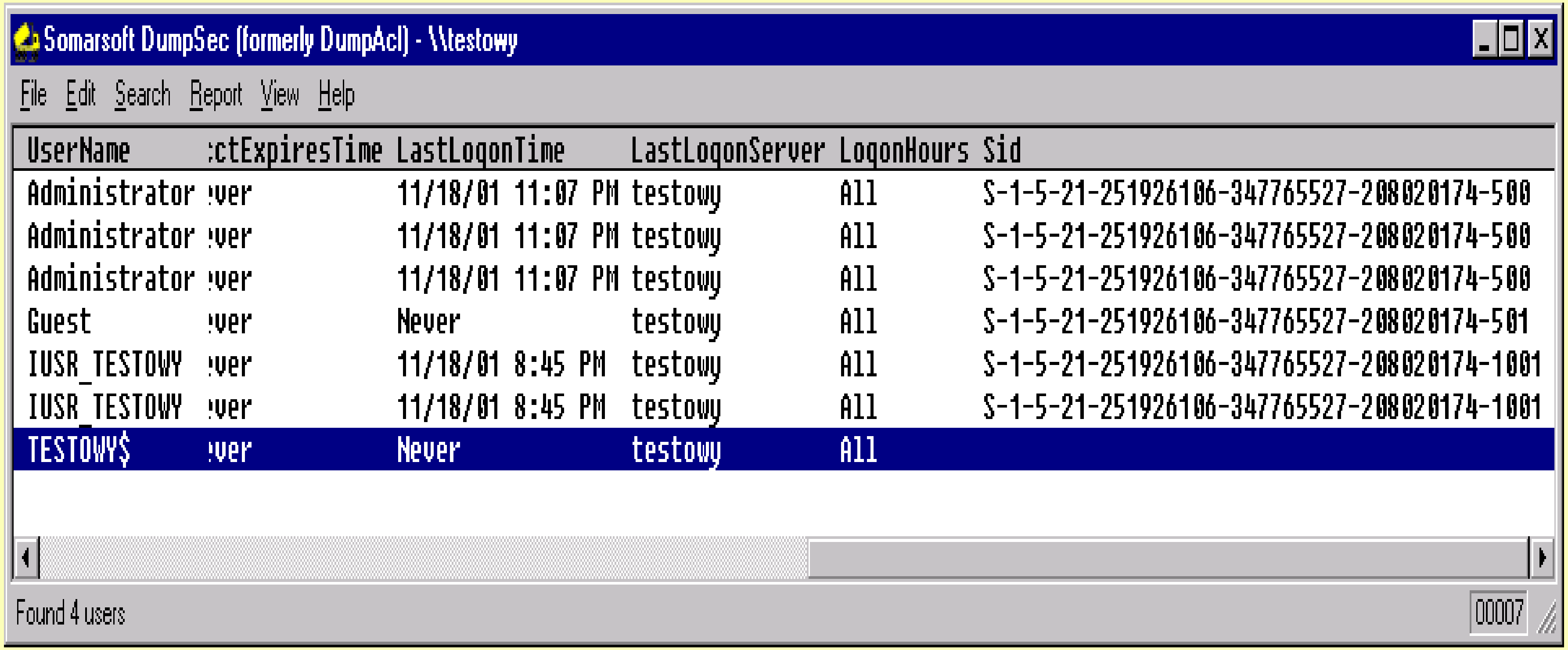
Enumeracja systemu Windows (Nazwy NetBIOS)



```
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:\>
```

```
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:\>
```

Enumeracja systemu Windows (SID)


Somarsoft DumpSec (formerly DumpAcl) - \\testowy
File Edit Search Report View Help
Found 4 users
00007

UserName	:ctExpiresTime	LastLogonTime	LastLogonServer	LogonHours	Sid
Administrator	:ver	11/18/01 11:07 PM	testowy	All	S-1-5-21-251926106-347765527-208020174-500
Administrator	:ver	11/18/01 11:07 PM	testowy	All	S-1-5-21-251926106-347765527-208020174-500
Administrator	:ver	11/18/01 11:07 PM	testowy	All	S-1-5-21-251926106-347765527-208020174-500
Guest	:ver	Never	testowy	All	S-1-5-21-251926106-347765527-208020174-501
IUSR_TESTOWY	:ver	11/18/01 8:45 PM	testowy	All	S-1-5-21-251926106-347765527-208020174-1001
IUSR_TESTOWY	:ver	11/18/01 8:45 PM	testowy	All	S-1-5-21-251926106-347765527-208020174-1001
TESTOWY$	:ver	Never	testowy	All	

Enumeracja systemu UNIX/Linux

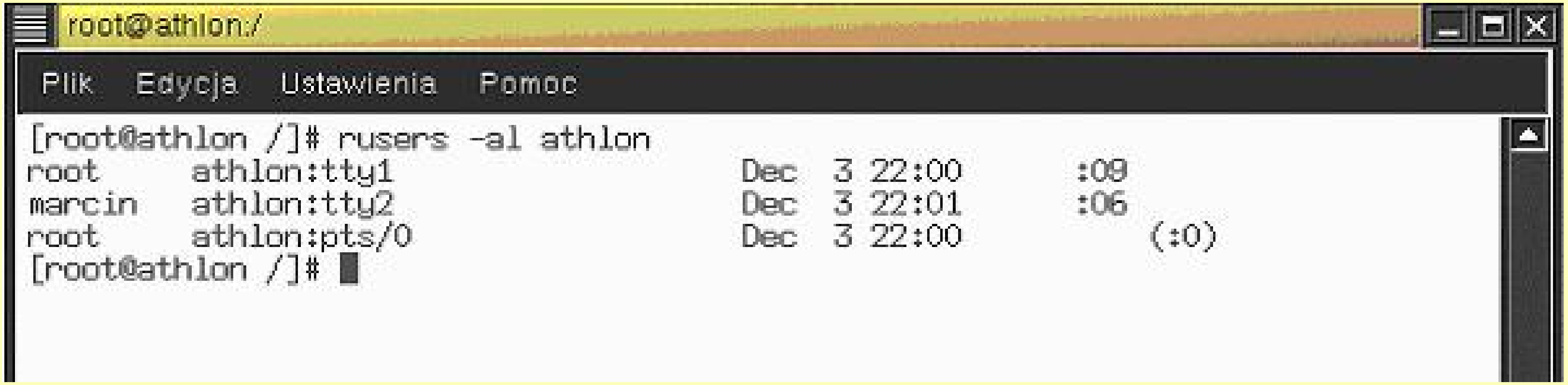
- Polec

```
[root@athlon
Login: root
Directory: /
On since Tue
On since Tue
New mail rec
     Unread
No Plan.

Login: marci
Directory: /
On since Tue
No mail.
Plan:

[root@athlon
```

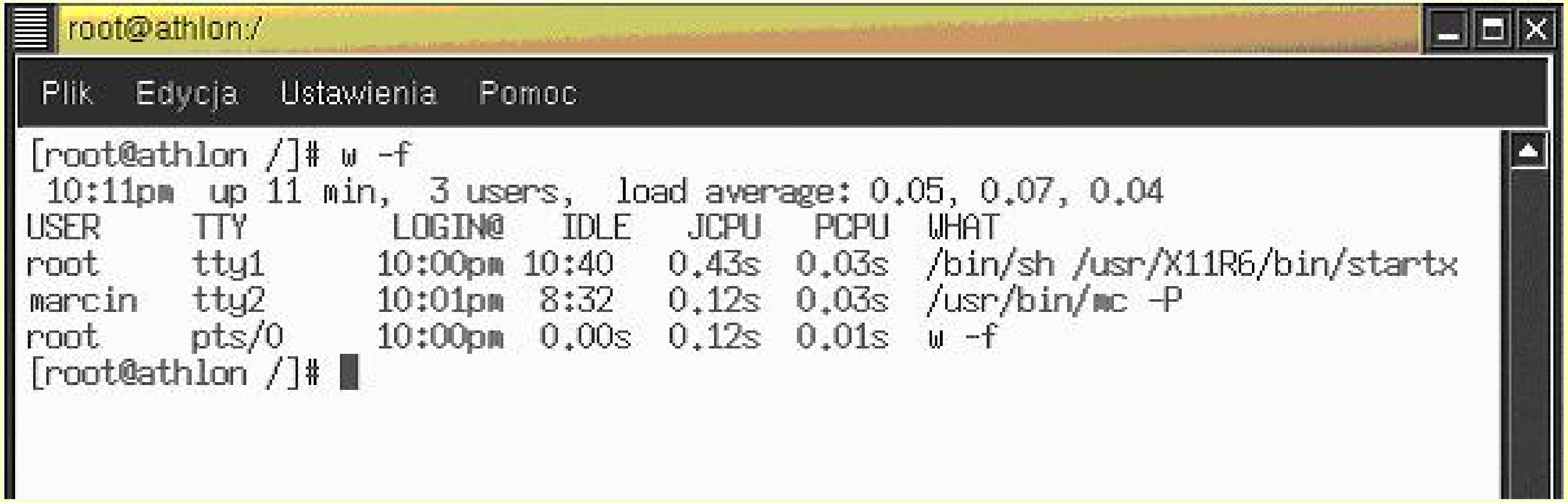
```
C:\nc –nvv 192.168.1.2 79
<UNKNOWN> [192.168.1.2] 79 <?> open
user

Login: user           Name: (null)
Directory: /home/user        Shell: /bin/bash
Last login Thu Mar  6 05:10 (CET) on 2 from cocktail
No mail.
No Plan.

Login: ftp                          Name: FTP User
Directory: /home/ftp                Shell: /bin/sh
Never logged in.
No mail.
No Plan.

Login: test                         Name: test
Directory: /home/test               Shell: /bin/bash
Never logged in.
No mail.
No Plan.
```

Enumeracja systemu UNIX/Linux

- Polecenie *rwho* lub *rusers* lub *w*



```
[root@athlon /]# rusers -al athlon
root      athlon:tty1                    Dec  3 22:00      :09
marcin    athlon:tty2                    Dec  3 22:01      :06
root      athlon:pts/0                   Dec  3 22:00          (:0)
[root@athlon /]#
```



```
[root@athlon /]# w -f
 10:11pm  up 11 min,  3 users,  load average: 0.05, 0.07, 0.04
USER     TTY        LOGIN@   IDLE   JCPU   PCPU  WHAT
root     tty1      10:00pm 10:40   0.43s  0.03s  /bin/sh /usr/X11R6/bin/startx
marcin   tty2      10:01pm  8:32   0.12s  0.03s  /usr/bin/mc -P
root     pts/0     10:00pm  0.00s  0.12s  0.01s  w -f
[root@athlon /]#
```

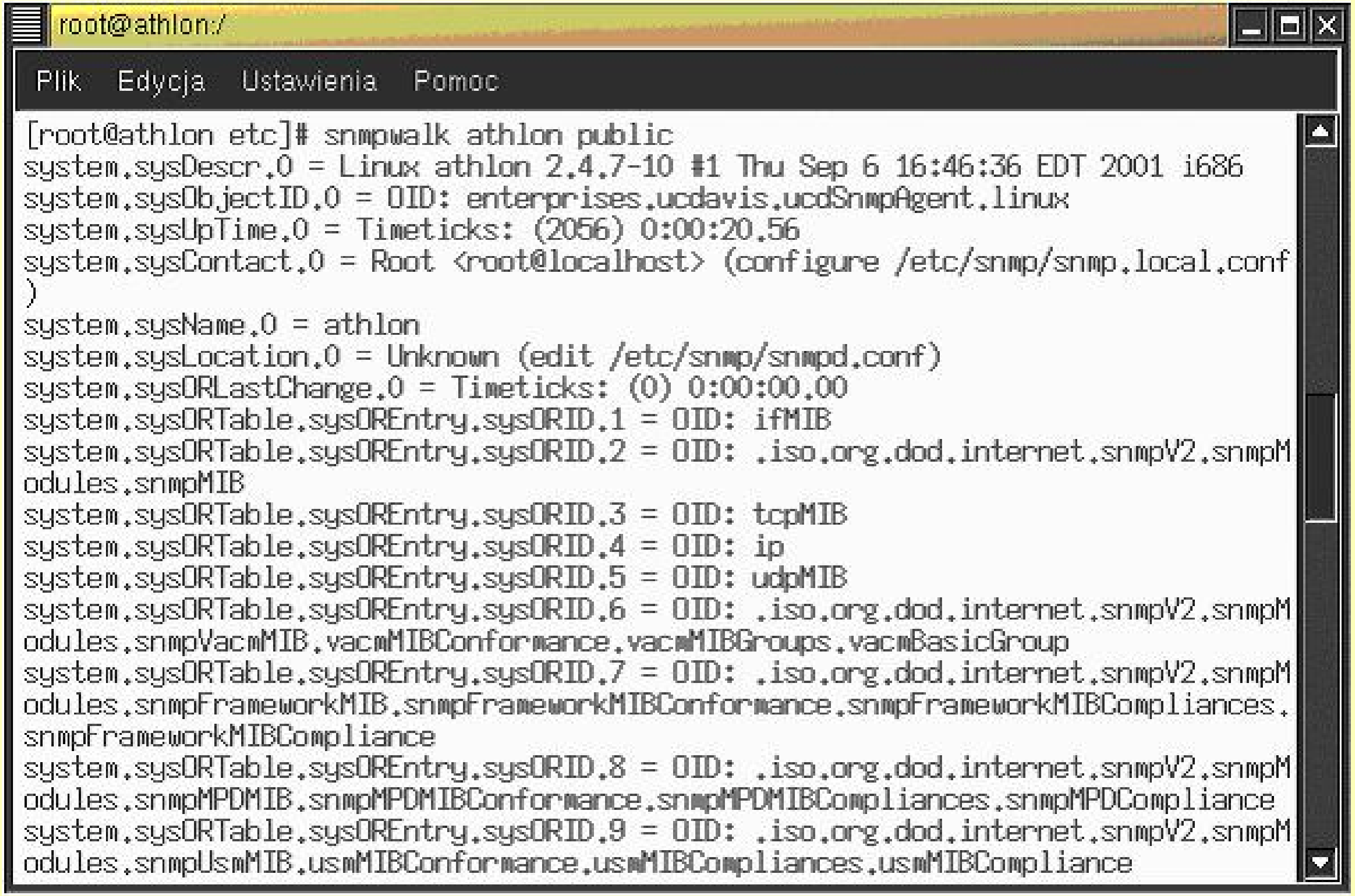
Enumeracja systemu UNIX/Linux

- Wykrywanie kont za pomocą SMTP

```
C:\nc –nvv 192.168.1.2 25
<UNKNOWN> [192.168.1.2] 25 <?> open
220 kazio ESMTP Sendmail 8.9.3/8.8.7; Tue, 11 Mar 2003 15:08:34 +0100
EXPN root
250 root root@kazio
EXPN user
250 user@kazio
EXPN ftp
250 FTP User ftp@kazio
EXPN gosc
550 gosc... User unknown
EXPN test
250 test test@kazio
EXPN admin
550 admin... User unknown
quit
221 kazio closing connection
```

Enumeracja systemu UNIX/Linux

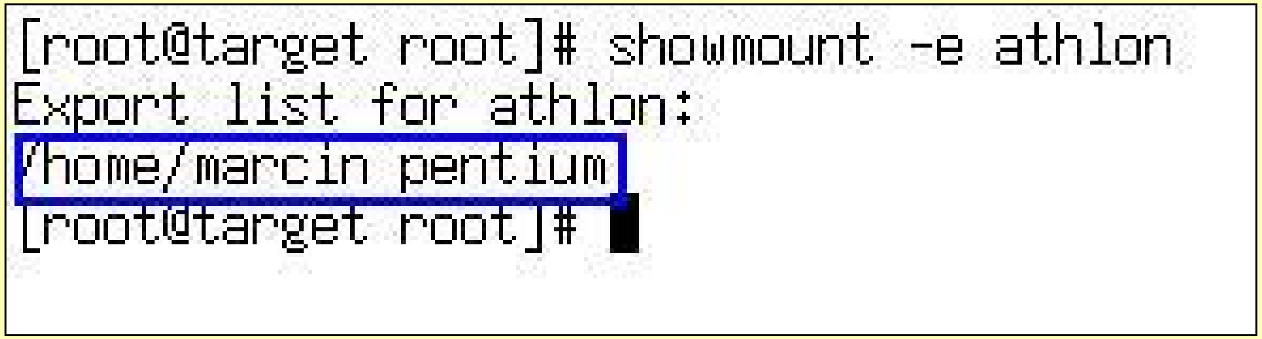
- Wykrywanie kont za pomocą SNMP



```
[root@athlon etc]# snmpwalk athlon public
system.sysDescr.0 = Linux athlon 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686
system.sysObjectID.0 = OID: enterprises.ucdavis.ucdSnmpAgent.linux
system.sysUpTime.0 = Timeticks: (2056) 0:00:20.56
system.sysContact.0 = Root <root@localhost> (configure /etc/snmp/snmp.local.conf
)
system.sysName.0 = athlon
system.sysLocation.0 = Unknown (edit /etc/snmp/snmpd.conf)
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
system.sysORTable.sysOREntry.sysORID.1 = OID: ifMIB
system.sysORTable.sysOREntry.sysORID.2 = OID: .iso.org.dod.internet.snmpV2.snmpM
odules.snmpMIB
system.sysORTable.sysOREntry.sysORID.3 = OID: tcpMIB
system.sysORTable.sysOREntry.sysORID.4 = OID: ip
system.sysORTable.sysOREntry.sysORID.5 = OID: udpMIB
system.sysORTable.sysOREntry.sysORID.6 = OID: .iso.org.dod.internet.snmpV2.snmpM
odules.snmpVacmMIB.vacmMIBConformance.vacmMIBGroups.vacmBasicGroup
system.sysORTable.sysOREntry.sysORID.7 = OID: .iso.org.dod.internet.snmpV2.snmpM
odules.snmpFrameworkMIB.snmpFrameworkMIBConformance.snmpFrameworkMIBCompliances.
snmpFrameworkMIBCompliance
system.sysORTable.sysOREntry.sysORID.8 = OID: .iso.org.dod.internet.snmpV2.snmpM
odules.snmpMPDMIB.snmpMPDMIBConformance.snmpMPDMIBCompliances.snmpMPDCompliance
system.sysORTable.sysOREntry.sysORID.9 = OID: .iso.org.dod.internet.snmpV2.snmpM
odules.snmpUsmMIB.usmMIBConformance.usmMIBCompliances.usmMIBCompliance
```

Enumeracja systemu UNIX/Linux

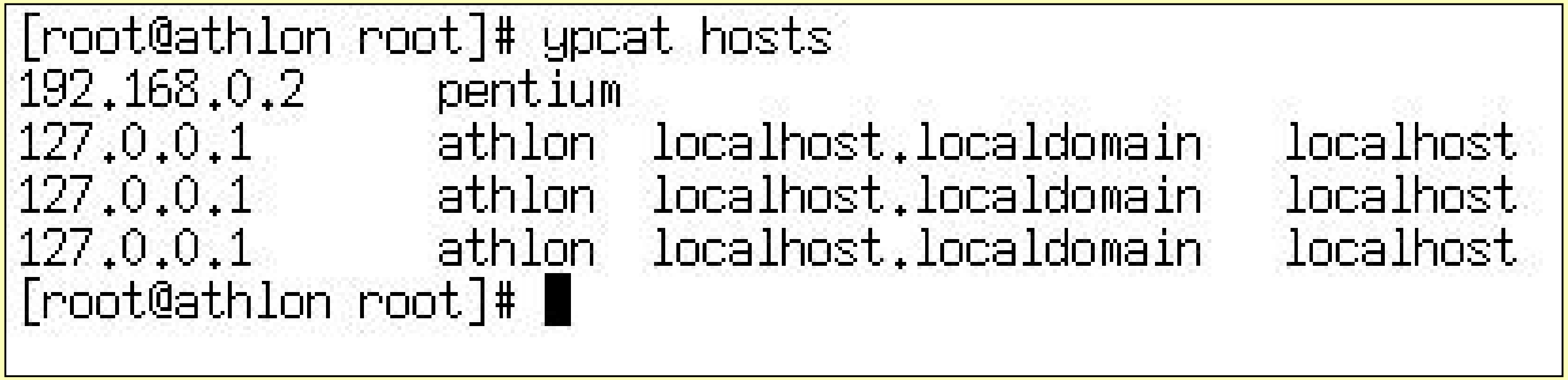
- **Wykrywanie zasobów NFS**



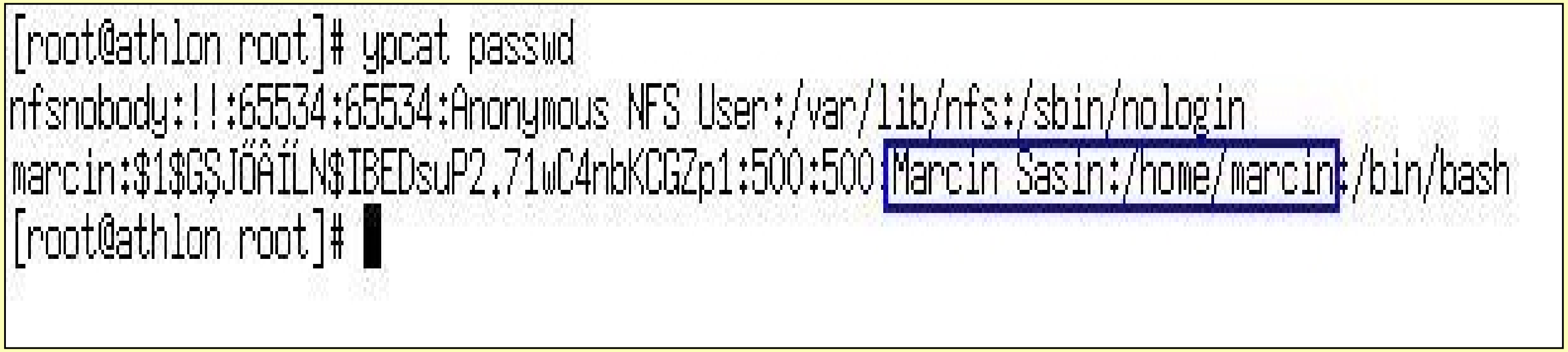
```
[root@target root]# showmount -e athlon
Export list for athlon:
/home/marcin pentium
[root@target root]#
```

Enumeracja systemu UNIX/Linux

- ❑ **Wykrywanie zasobów NIS**



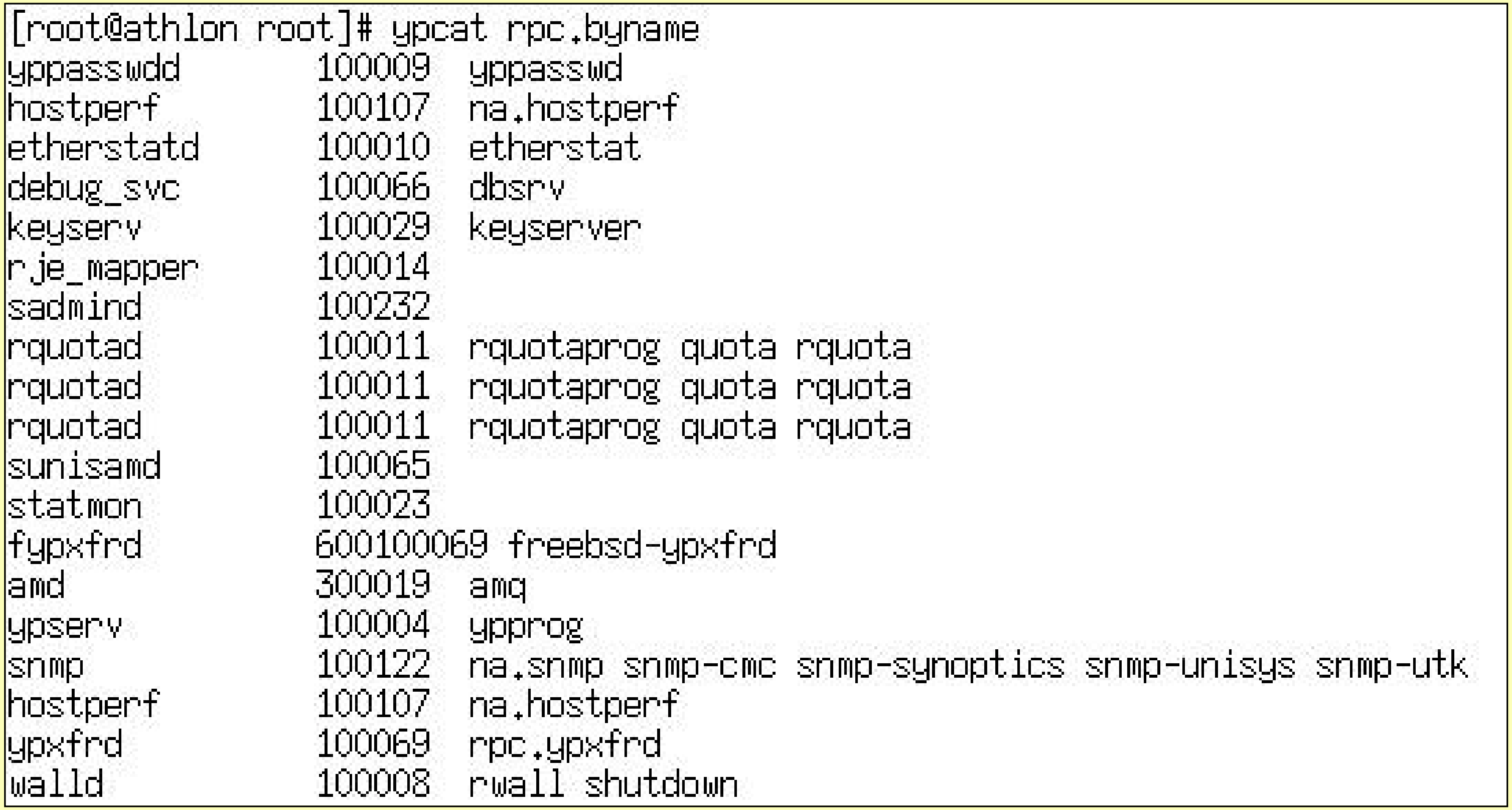
```
[root@athlon root]# ypcat hosts
192.168.0.2     pentium
127.0.0.1       athlon  localhost.localdomain   localhost
127.0.0.1       athlon  localhost.localdomain   localhost
127.0.0.1       athlon  localhost.localdomain   localhost
[root@athlon root]# █
```



```
[root@athlon root]# ypcat passwd
nfsnobody:!!:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
marcin:$1$GŞJŐÂÍLN$IBEDsuP2,71wC4nbKCGZp1:500:500:Marcin Sasin:/home/marcin:/bin/bash
[root@athlon root]# █
```

Enumeracja systemu UNIX/Linux

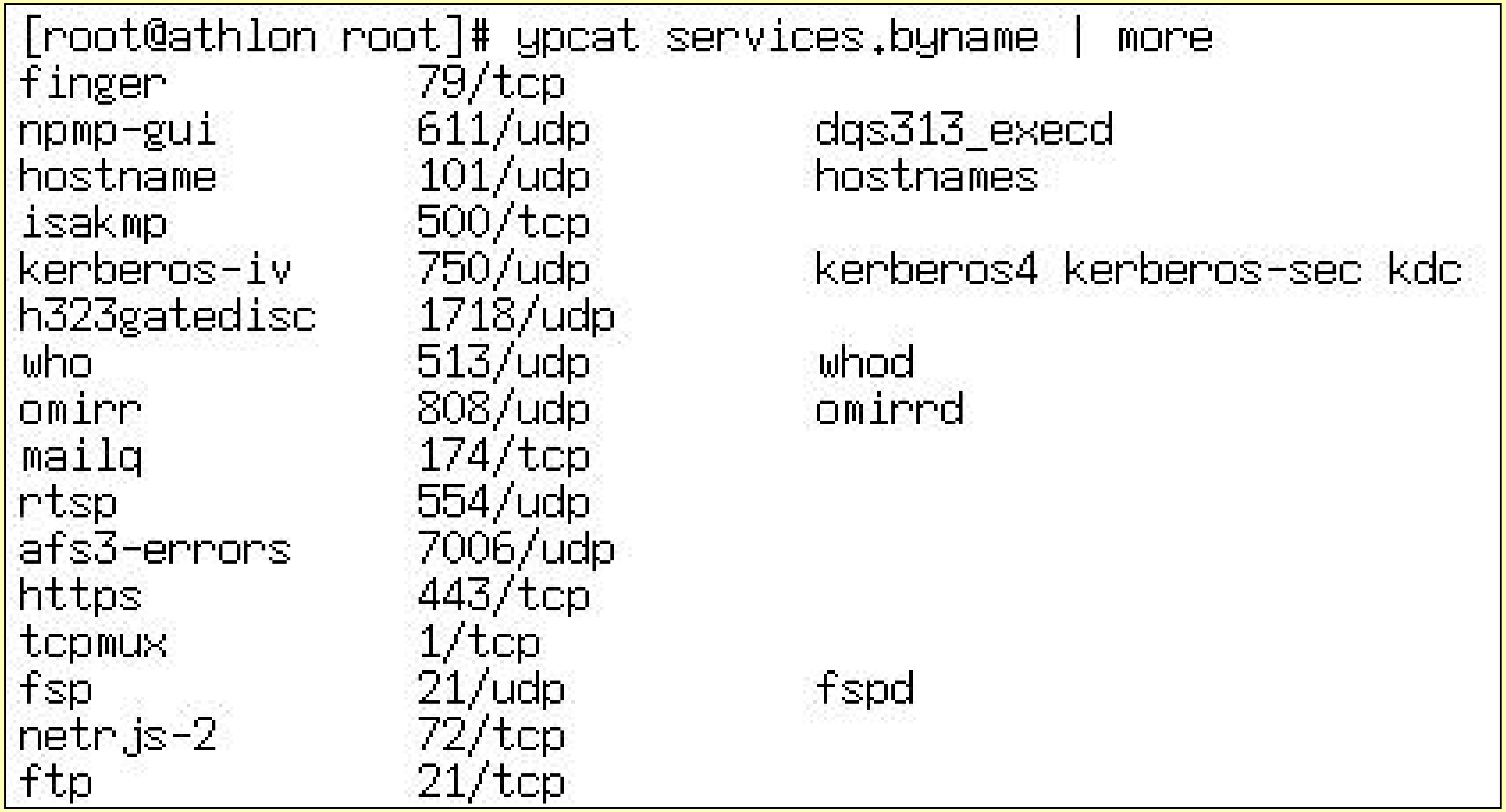
❑ Wykrywanie zasobów NIS



```
[root@athlon root]# ypcat rpc.byname
yppasswdd       100009  yppasswd
hostperf        100107  na.hostperf
etherstatd      100010  etherstat
debug_svc       100066  dbsrv
keyserv         100029  keyserver
rje_mapper      100014
sadmind         100232
rquotad         100011  rquotaprog quota rquota
rquotad         100011  rquotaprog quota rquota
rquotad         100011  rquotaprog quota rquota
sunisamd        100065
statmon         100023
fypxfrd         600100069 freebsd-ypxfrd
amd             300019  amq
ypserv          100004  ypprog
snmp            100122  na.snmp snmp-cmc snmp-synoptics snmp-unisys snmp-utk
hostperf        100107  na.hostperf
ypxfrd          100069  rpc.ypxfrd
walld           100008  rwall shutdown
```

Enumeracja systemu UNIX/Linux

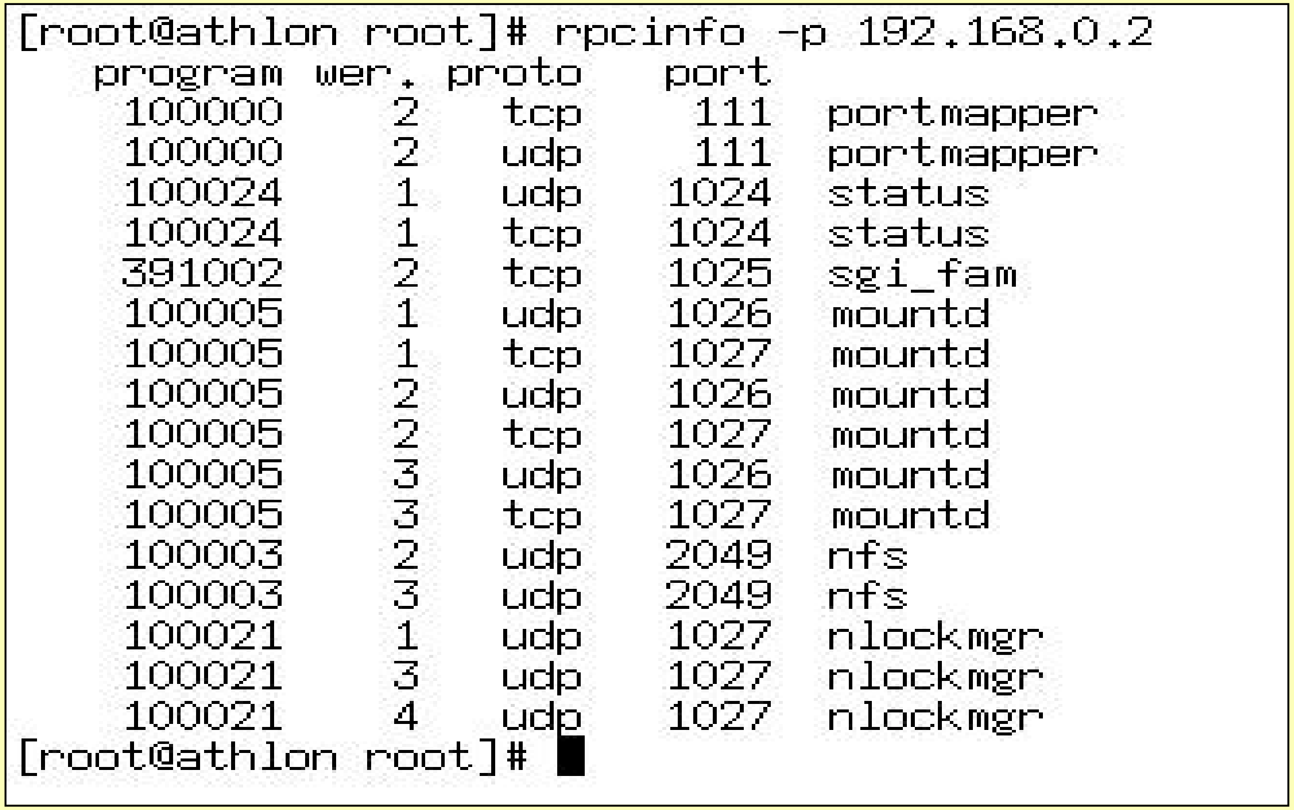
❑ Wykrywanie zasobów NIS



```
[root@athlon root]# ypcat services.byname | more
finger          79/tcp
npmp-gui        611/udp         dqs313_execd
hostname        101/udp         hostnames
isakmp          500/tcp
kerberos-iv     750/udp         kerberos4 kerberos-sec kdc
h323gatedisc    1718/udp
who             513/udp         whod
omirr           808/udp         omirrd
mailq           174/tcp
rtsp            554/udp
afs3-errors     7006/udp
https           443/tcp
tcpmux          1/tcp
fsp             21/udp          fspd
netrjs-2        72/tcp
ftp             21/tcp
```

Enumeracja systemu UNIX/Linux

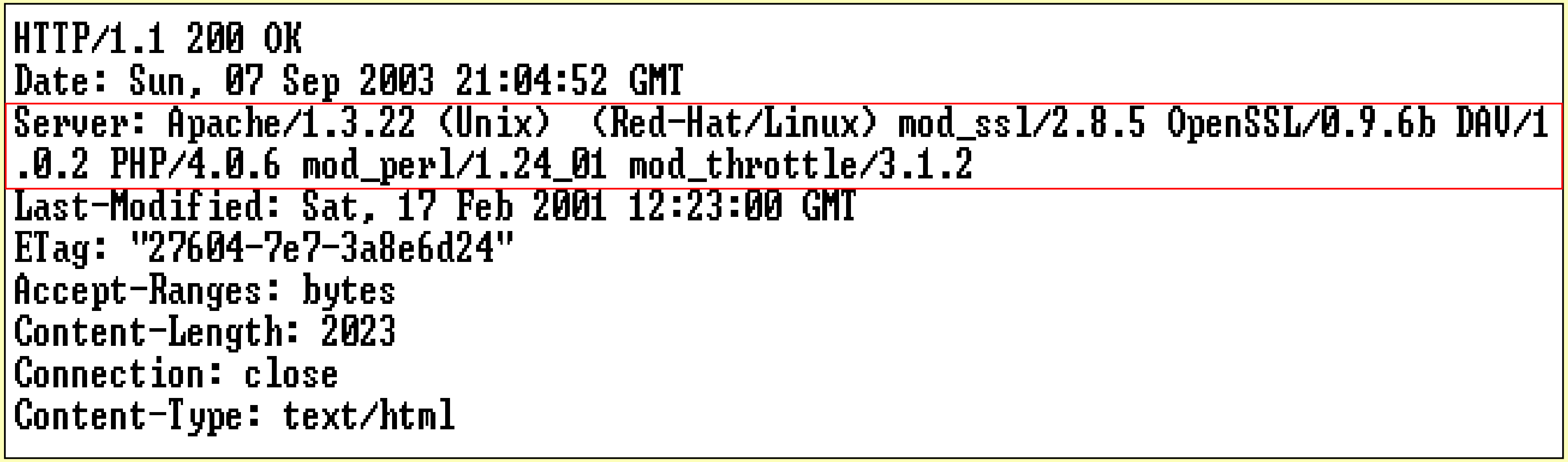
❑ Wykrywanie zasobów RPC



```
[root@athlon root]# rpcinfo -p 192.168.0.2
   program wer. proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp   1024  status
    100024    1   tcp   1024  status
    391002    2   tcp   1025  sgi_fam
    100005    1   udp   1026  mountd
    100005    1   tcp   1027  mountd
    100005    2   udp   1026  mountd
    100005    2   tcp   1027  mountd
    100005    3   udp   1026  mountd
    100005    3   tcp   1027  mountd
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100021    1   udp   1027  nlockmgr
    100021    3   udp   1027  nlockmgr
    100021    4   udp   1027  nlockmgr
[root@athlon root]# █
```

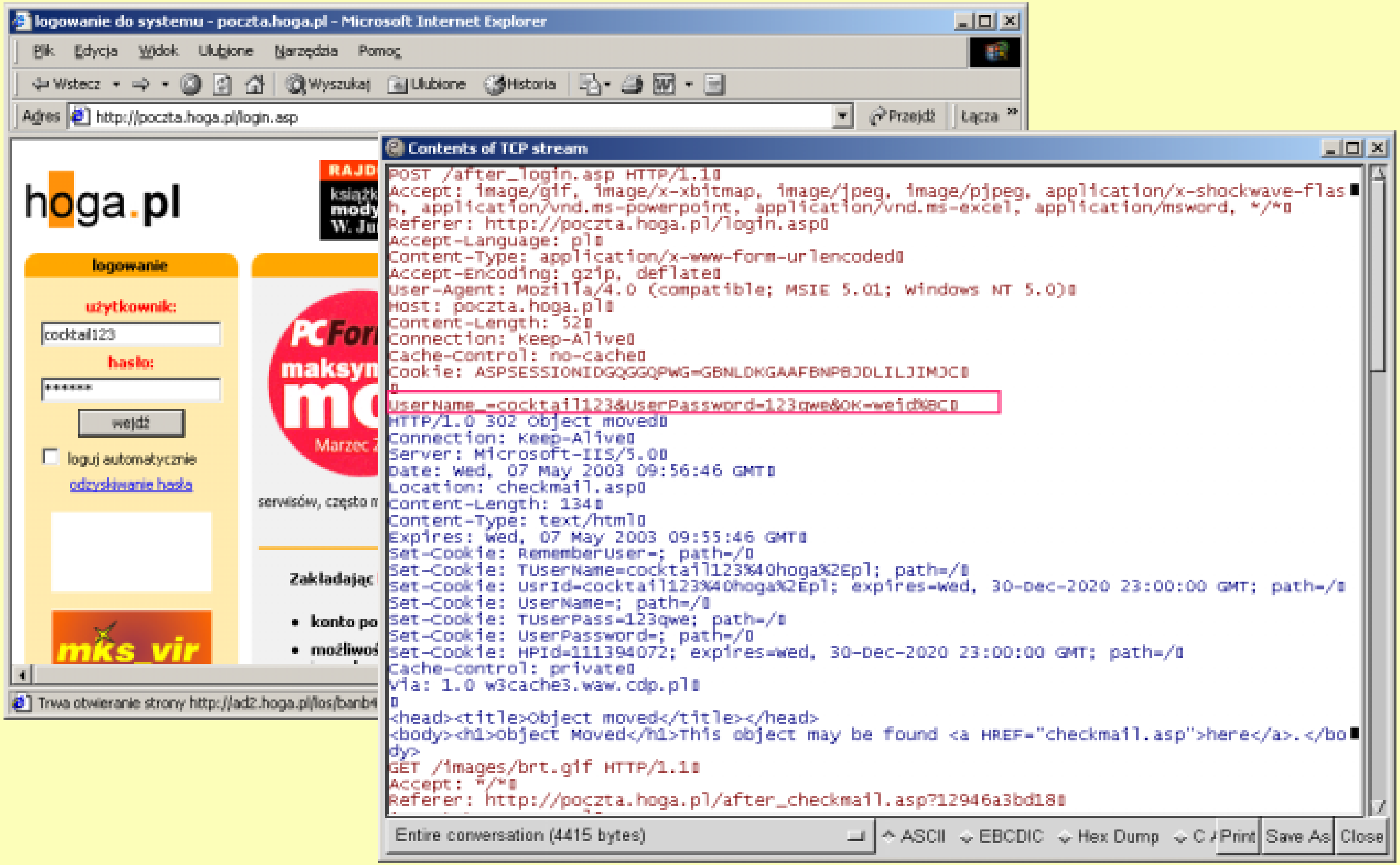
Enumeracja systemu UNIX/Linux

- Pozyskiwanie banerów aplikacji (*telnet*)



```
HTTP/1.1 200 OK
Date: Sun, 07 Sep 2003 21:04:52 GMT
Server: Apache/1.3.22 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.5 OpenSSL/0.9.6b DAV/1
.0.2 PHP/4.0.6 mod_perl/1.24_01 mod_throttle/3.1.2
Last-Modified: Sat, 17 Feb 2001 12:23:00 GMT
ETag: "27604-7e7-3a8e6d24"
Accept-Ranges: bytes
Content-Length: 2023
Connection: close
Content-Type: text/html
```

Podsłuchiwanie logowania do poczty WWW


logowanie do systemu - poczta.hoga.pl - Microsoft Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Wstecz Wyszukaj Ulubione Historia
Adres http://poczta.hoga.pl/login.asp
Przejdź Łącza
hoga.pl
RAJD
logowanie
wejdź
odzyskiwanie hasła
PC Forum
Marzec
mks_vir
Trwa otwieranie strony http://ad2.hoga.pl/los/banb4
Contents of TCP stream
Entire conversation (4415 bytes)
ASCII EBCDIC Hex Dump C Print Save As Close

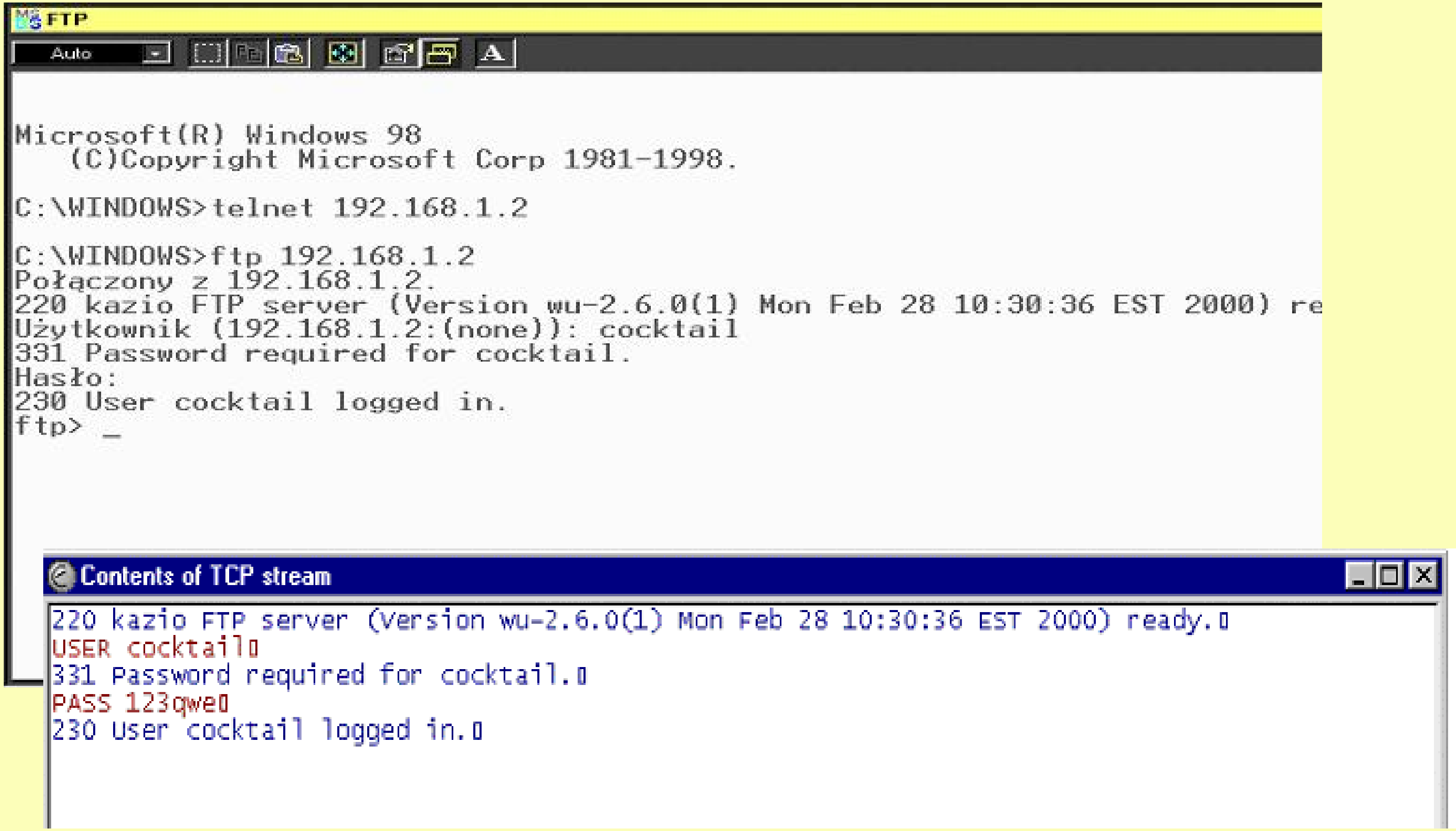
użytkownik: cocktail123

hasło: ******

□ loguj automatycznie

```
POST /after_login.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flas
h, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
Referer: http://poczta.hoga.pl/login.asp
Accept-Language: pl
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: poczta.hoga.pl
Content-Length: 52
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDGQGGQPWG=GBNLDKGAAFBNPBJDLILJIMJC

UserName_=cocktail123&UserPassword=123qwe&OK=wejd%BC
HTTP/1.0 302 Object moved
Connection: Keep-Alive
Server: Microsoft-IIS/5.0
Date: Wed, 07 May 2003 09:56:46 GMT
Location: checkmail.asp
Content-Length: 134
Content-Type: text/html
Expires: Wed, 07 May 2003 09:55:46 GMT
Set-Cookie: RememberUser=; path=/
Set-Cookie: TUserName=cocktail123%40hoga%2Epl; path=/
Set-Cookie: UsrId=cocktail123%40hoga%2Epl; expires=Wed, 30-Dec-2020 23:00:00 GMT; path=/
Set-Cookie: UserName=; path=/
Set-Cookie: TUserPass=123qwe; path=/
Set-Cookie: UserPassword=; path=/
Set-Cookie: HPId=111394072; expires=Wed, 30-Dec-2020 23:00:00 GMT; path=/
Cache-control: private
Via: 1.0 w3cache3.waw.cdp.pl

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="checkmail.asp">here</a>.</bo
dy>
GET /images/brt.gif HTTP/1.1
Accept: */*
Referer: http://poczta.hoga.pl/after_checkmail.asp?12946a3bd18
```

Podsłuchiwanie protokołu FTP

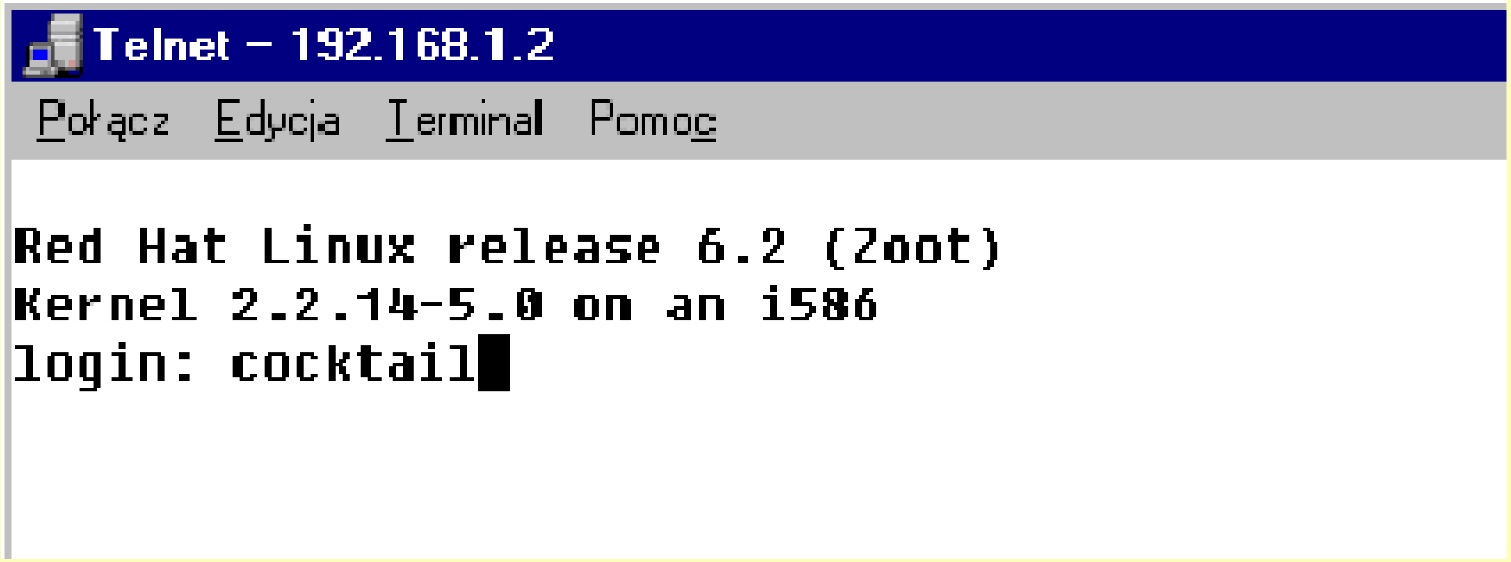


```
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1998.

C:\WINDOWS>telnet 192.168.1.2

C:\WINDOWS>ftp 192.168.1.2
Połączony z 192.168.1.2.
220 kazio FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) re
Użytkownik (192.168.1.2:(none)): cocktail
331 Password required for cocktail.
Hasło:
230 User cocktail logged in.
ftp> _
```

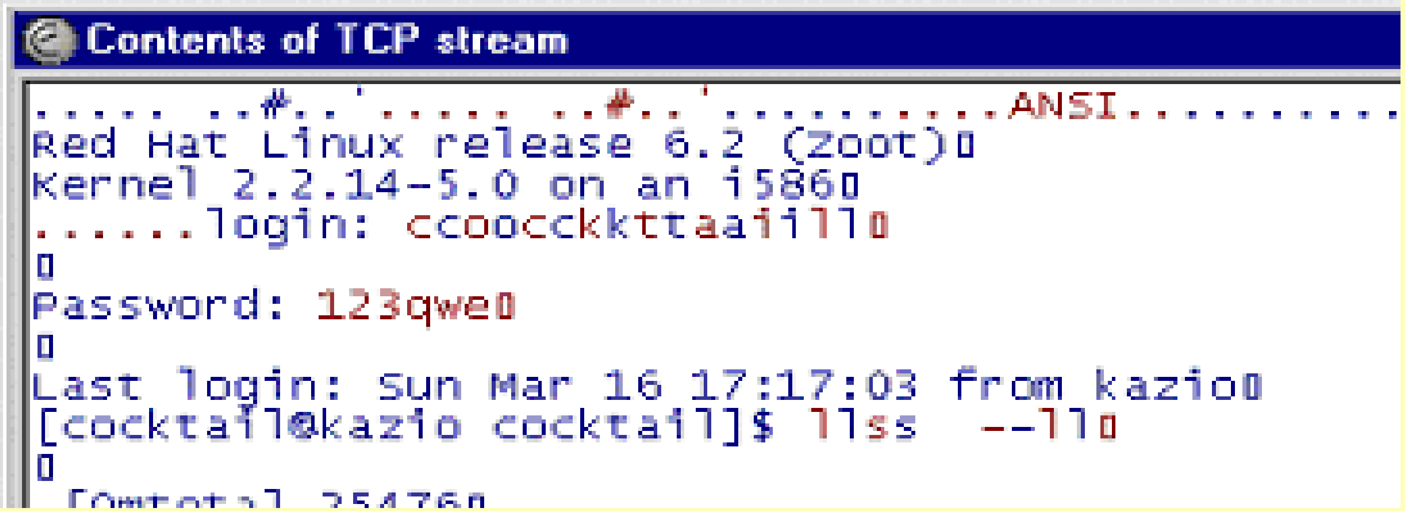
Contents of TCP stream

```
220 kazio FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.▯
USER cocktail▯
331 Password required for cocktail.▯
PASS 123qwe▯
230 User cocktail logged in.▯
```

Podsłuchiwanie protokołu Telnet

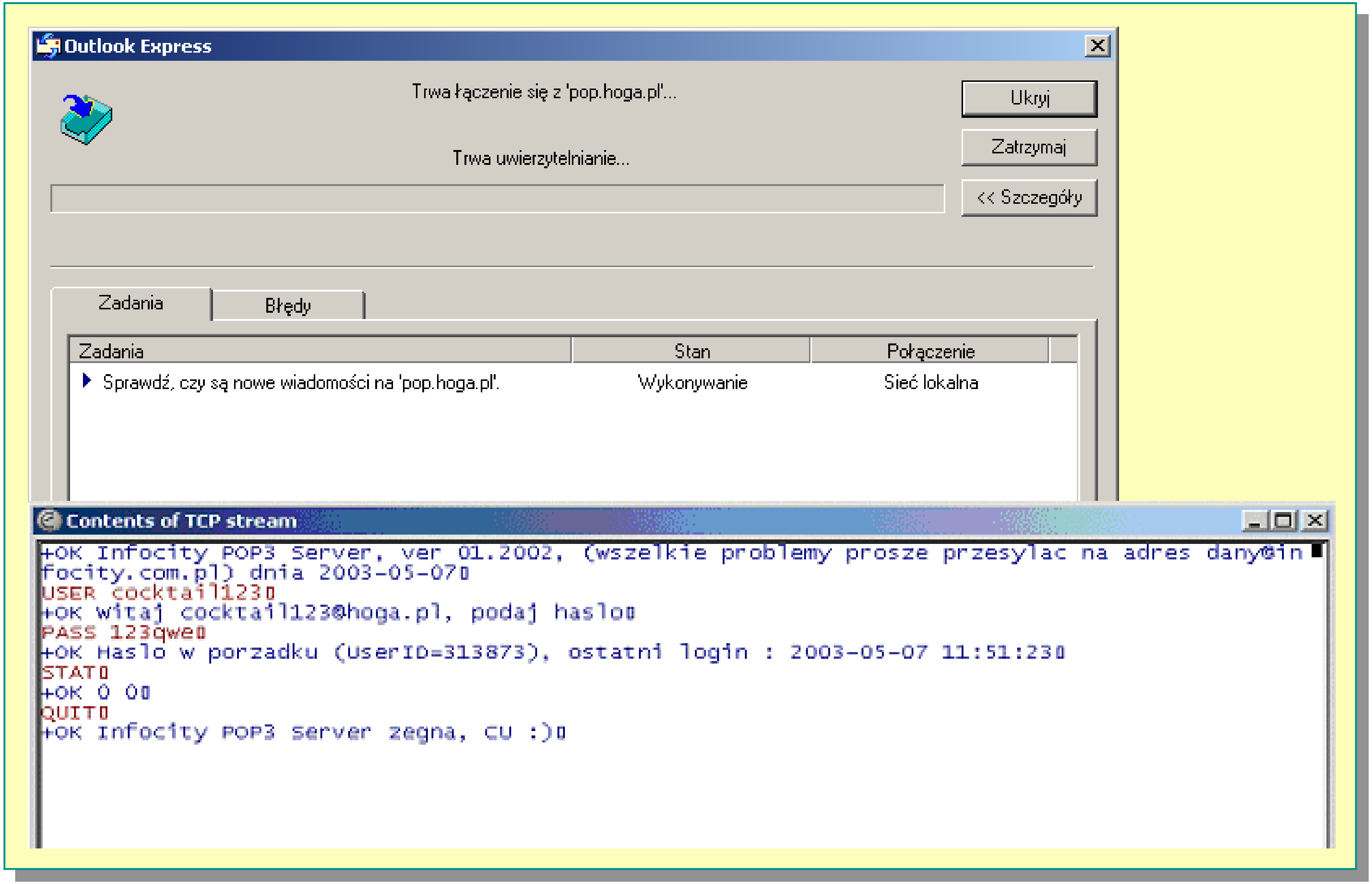


```
Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.14-5.0 on an i586
login: cocktail█
```



```
..... ..#..'..... ..#..'...........ANSI...........
Red Hat Linux release 6.2 (Zoot)▯
Kernel 2.2.14-5.0 on an i586▯
......login: ccoocckkttaaiill▯
▯
Password: 123qwe▯
▯
Last login: Sun Mar 16 17:17:03 from kazio▯
[cocktail@kazio cocktail]$ llss  --ll▯
▯
 [Omtotal 25476▯
```

Podsłuchiwanie protokołu POP



Trwa łączenie się z 'pop.hoga.pl'...

Trwa uwierzytelnianie...

Zadania	Stan	Połączenie
▸ Sprawdź, czy są nowe wiadomości na 'pop.hoga.pl'.	Wykonywanie	Sieć lokalna

```
+OK Infocity POP3 Server, ver 01.2002, (wszelkie problemy prosze przesylac na adres dany@in
focity.com.pl) dnia 2003-05-07▯
USER cocktail123▯
+OK witaj cocktail123@hoga.pl, podaj haslo▯
PASS 123qwe▯
+OK Haslo w porzadku (UserID=313873), ostatni login : 2003-05-07 11:51:23▯
STAT▯
+OK 0 0▯
QUIT▯
+OK Infocity POP3 server zegna, cu :)▯
```