Testy penetracyjne

Materiały pomocnicze do wykładu

Bezpieczeństwo systemów informatycznych

Testy penetracyjne
część 1

Testy penetracyjne

- Celem tego testów penetracyjnych jest empiryczne określenie odporności systemu na ataki.
- Testy penetracyjne mogą być prowadzone z wnętrza badanej sieci oraz z zewnątrz.
- Należy liczyć się z możliwością załamania systemu.
- Należy utworzyć nowe, pełne kopie zapasowe.

Przebieg testu penetracyjnego

- Zebranie informacji o systemie poza nim samym.
- Próby uzyskania dostępu do zasobów badanego systemu.
- Wstępna ocena możliwości systemu w zakresie wykrywania i blokowania włamań.
- Próby włamań.

Etapy testu zewnętrznego

- Rekonesans
- Skanowanie przestrzeni adresowej sieci
- Skanowanie sieci telefonicznej
- Skanowanie portów urządzeń sieciowych
- Identyfikacja systemu
- Symulacja włamania
- Badanie odporności na ataki typu *odmowa usługi*

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,
- systemy wykrywania intruzów i zapory sieciowe,
- używane protokoły,
- numery linii telefonicznych,
- mechanizmy autoryzacji dla zdalnego dostępu.

Rekonesans - metody

- Przeszukiwanie ogólnie dostępnych źródeł:
  - ✓ strony www,
  - ✓ artykuły i informacje prasowe,
  - ✓ listy dyskusyjne,
  - ✓ serwisy wyszukiwawcze.

Przeciwdziałanie polega przede wszystkim na usunięciu wszystkich informacji, które mogłyby pomóc w zdobyciu dostępu do naszej sieci

RFC 2196 - *Site Security Handbook*.

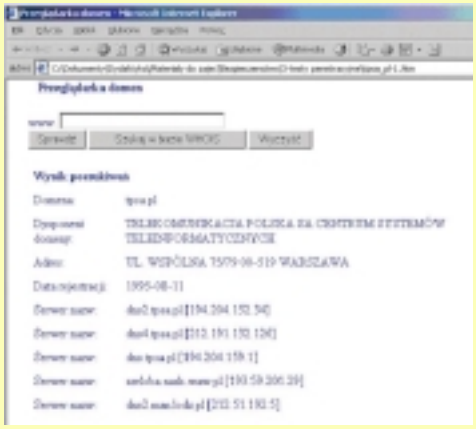
Rekonesans - metody

- Analiza sieci – bazy whois
  - ✓ www.allwhois.com
  - ✓ www.arin.net - *American Registry for Internet Numbers*
  - ✓ www.samspade.org - *SamSpade*
  - ✓ www.apnic.net - *Asia-Pacific Network Information Center*
  - ✓ www.ripe.net - *Reseaux IP Europeens*
  - ✓ www.dns.pl - *Naukowa i Akademicka Sieć Komputerowa*

Rekonesans - metody

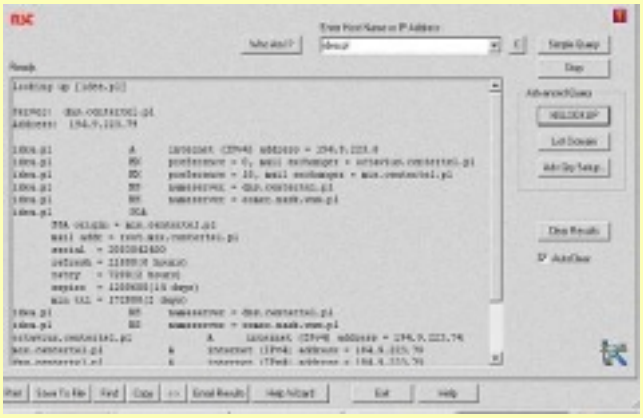
- Kontrola serwerów DNS
  - ➢ program *nslookup*
  - ➢ przesyłanie strefy
  - ➢ rekordy HINFO
- Badanie sieci
  - ➢ programy *traceroute*, *tracert*
  - ➢ programy *Visual Route, Neo Trace*
  - ➢ i inne

Rekonesans - przykłady



Rekonesans - przykłady

Rekonesans - przykłady



Rekonesans - przykłady

Skanowanie - cele

- detekcja urządzeń
- detekcja usług
- rozpoznanie systemu operacyjnego
- rozpoznanie topologii sieci
- rozpoznanie konfiguracji urządzeń dostępowych

Skanowanie - baza

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

Skanowanie - techniki

- Skanowanie z wykorzystaniem protokołu UDP
  - odpowiedź *ICMP Port Unreachable*
  - odpowiedź *ICMP Host Unreachable*
- Skanowanie z wykorzystaniem protokołu ICMP
  - ICMP *echo request*
  - *Timestamp Request*
  - *Address Mask Request*

Skanowanie – techniki TCP

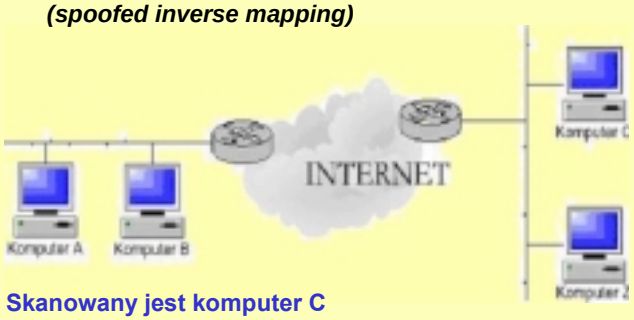
Skanowanie połączeniowe i półotwarte

Skanowanie – specjalne techniki TCP

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

Skanowanie – specjalne techniki TCP

- **Mapowanie odwrotne z podszywaniem się** *(spoofed inverse mapping)*



Skanowany jest komputer C
Skanuje komputer B
Dodatkowo wykorzystywany jest komputer A

Skanowanie – specjalne techniki TCP

A. Sprawdzanie pola TTL

host 10.1.1.2 port 20: F:RST -> ttl: 70 win: 0 => port zamknięty
host 10.1.1.2 port 21: F:RST -> ttl: 70 win: 0 => port zamknięty
host 10.1.1.2 port 22: F:RST -> ttl: 40 win: 0 => port otwarty
host 10.1.1.2 port 23: F:RST -> ttl: 70 win: 0 => port zamknięty

B. Sprawdzanie pola WINDOW

host 10.1.1.3 port 20: F:RST -> ttl: 64 win: 0 => port zamknięty
host 10.1.1.3 port 21: F:RST -> ttl: 64 win: 0 => port zamknięty
host 10.1.1.3 port 22: F:RST -> ttl: 64 win: 512 => port otwarty
host 10.1.1.3 port 23: F:RST -> ttl: 64 win: 0 => port zamknięty

Skanowanie – protokół IP (*IP ID idle scan*)

Odpowiedzi hosta niemego
60 bytes from 10.1.1.6: flags=RA seq=0 ttl=64 id=4166 win=0 time=32 ms
60 bytes from 10.1.1.6: flags=RA seq=1 ttl=64 id=+1 win=0 time=75 ms
60 bytes from 10.1.1.6: flags=RA seq=2 ttl=64 id=+1 win=0 time=91 ms
60 bytes from 10.1.1.6: flags=RA seq=3 ttl=64 id=+1 win=0 time=90 ms

Odpowiedzi hosta niemego w przypadku portu otwartego
60 bytes from 10.1.1.6: flags=RA seq=17 ttl=64 id=+1 win=0 time=96 ms
60 bytes from 10.1.1.6: flags=RA seq=18 ttl=64 id=+1 win=0 time=80 ms
60 bytes from 10.1.1.6: flags=RA seq=19 ttl=64 id=+2 win=0 time=83 ms
60 bytes from 10.1.1.6: flags=RA seq=20 ttl=64 id=+3 win=0 time=94 ms

Odpowiedzi hosta niemego w przypadku portu zamkniętego
60 bytes from 10.1.1.6: flags=RA seq=52 ttl=64 id=+1 win=0 time=85 ms
60 bytes from 10.1.1.6: flags=RA seq=53 ttl=64 id=+1 win=0 time=83 ms
60 bytes from 10.1.1.6: flags=RA seq=54 ttl=64 id=+1 win=0 time=93 ms
60 bytes from 10.1.1.6: flags=RA seq=55 ttl=64 id=+1 win=0 time=74 ms

Skanowanie – protokół IP za bramką (*IP masqurading*)

[root] # nmap - sI 10.1.1.8 - P0 10.1.1.40
Starting nmap V 2.54BETA30 (www.insecure.org/nmap /)
Idlescan using .....
Interesting ports one .....:
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 – protokół FTP (*FTP Bounce Scanning*)

- Serwer FTP jako punkt pośredniczący
- Własność FXP protokołu FTP (RFC 959)
- Komenda PORT (adres i port docelowy)
- Odpowiedź serwera FTP przy porcie otwartym:

  150 i/lub 226
- Odpowiedź serwera FTP przy porcie zamkniętym:

  425 Can't build data connection: Connection refused

Skanowanie – identyfikowanie połączenia

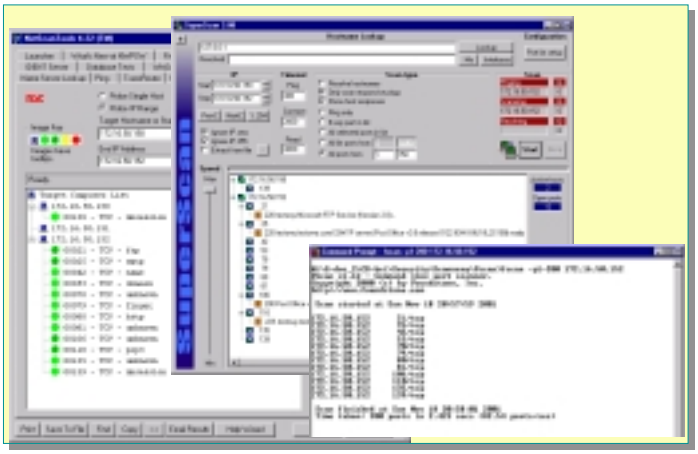
Identyfikowanie połączenia (*reverse ident scanning*)

- Wykorzystanie protokołu *ident* (RFC 1413)
- Protokół *ident* zwraca dane właściciela procesu, z którym nawiązane zostało połączenie TCP
- Wysłanie zapytania protokołu ident na port z którym nawiązano połączenie
- Otrzymujemy nazwę użytkownika, z którego uprawnieniami działa dana usługa

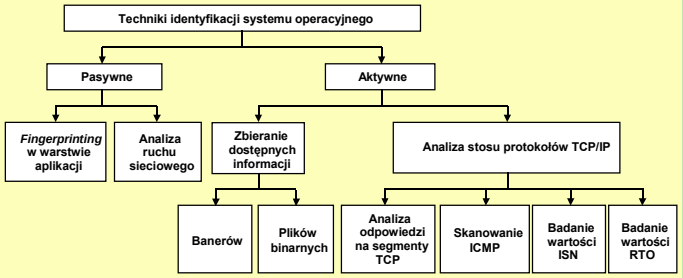
Skanowanie ukryte

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

Skanowanie - przykłady



Zdalna identyfikacja systemu operacyjnego



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

Analiza stosu TCP/IP (aktywna) i ruchu (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

Zdalna identyfikacja systemu operacyjnego

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 systemu operacyjnego

- Test z flagą FIN
- Test z nieistniejącą flagą (*Bogus Flag Probe Test*)
- Obsługa fragmentacji (*Fragmentation Handling*)

System operacyjny	Reakcja na nakładające się fragmenty
MS Windows NT 4.0	Dane z poprzedniego fragmentu nie zostaną nadpisane
Solaris 2.6	
4.4 BSD	Dane z poprzedniego fragmentu zostaną nadpisane przez przychodzący fragment
Linux	
HP/UX 9.02	
Irix 5.3	

Zdalna identyfikacja systemu operacyjnego

- Próbkowanie początkowego numeru sekwencyjnego (*Initial Sequence Number*)
  - cykliczne
  - pseudolosowe
  - losowe bazujące na aktualnym czasie
  - stałe
- Nowe opcje TCP

Zdalna identyfikacja systemu operacyjnego

- Czas retransmisji pakietów

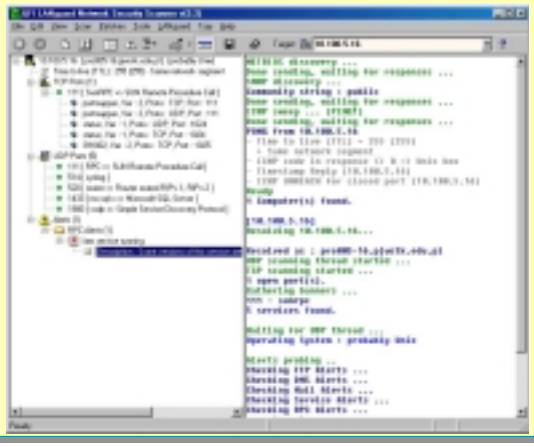
Powtórzenia	Windows 98	Windows 2K	Linux 2.2.14	Linux 2.4	FreeBSD 4.4
1	3	3	3,5	4,26	3
2	6	6	6,5	6	6
3	12	Koniec	12,5	12	12
4	Koniec		24,5	24	24
5			48,5	48,5	Koniec
6			96,5	Koniec	
7			120,5		
8			Koniec		
Reset	Nie	Nie	Nie	Nie	Tak po 30 s

Zdalna identyfikacja systemu operacyjnego

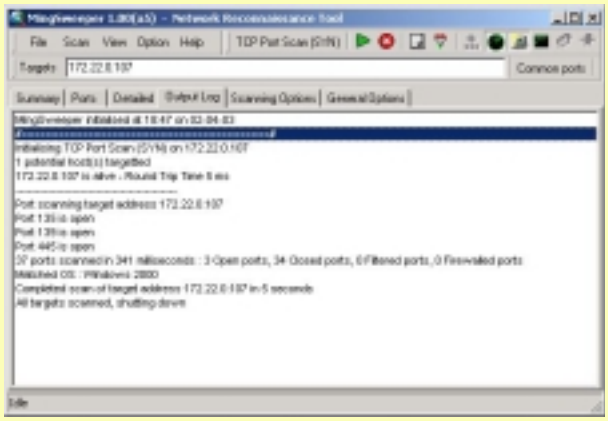
Implementacja protokołu ICMP

- 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 systemu operacyjnego



Zdalna identyfikacja systemu operacyjnego



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
```

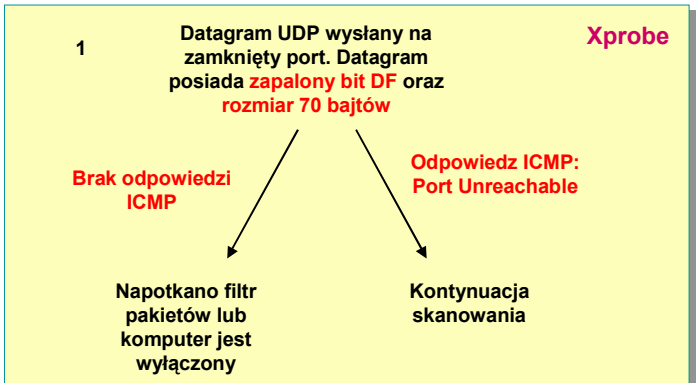

Zdalna identyfikacja systemu operacyjnego

```
[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 ]
```

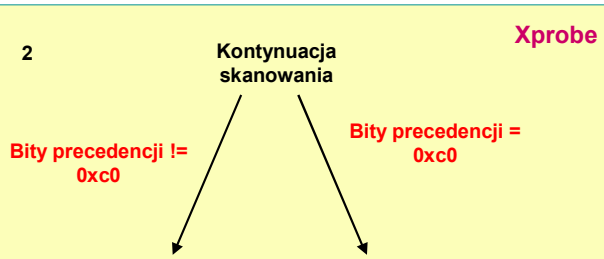
Program Xprobe

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

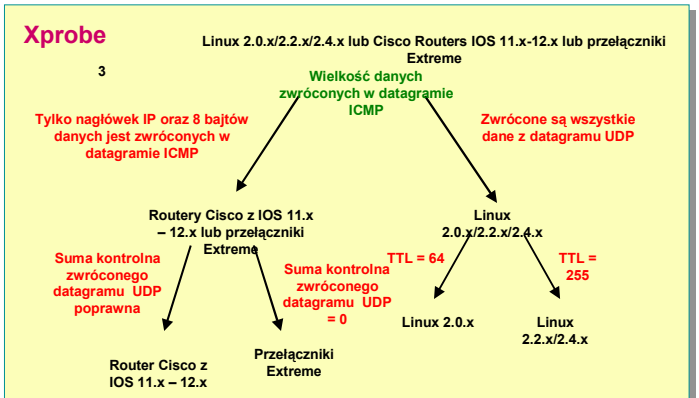
Zdalna identyfikacja systemu operacyjnego



Zdalna identyfikacja systemu operacyjnego



Zdalna identyfikacja systemu operacyjnego



Bezpieczeństwo systemów informatycznych

Testy penetracyjne
część 2

Zbigniew Suski BSI – testy penetracyjne cz.2 1

Enumeracja

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

Do głównych rodzajów zbieranych informacji należą:

- **zasoby sieciowe i sposób ich udostępniania,**
- **użytkownicy i grupy,**
- **aplikacje.**

Zbigniew Suski BSI – testy penetracyjne cz.2 2

Enumeracja systemu Windows

- **CIFS/SMB (*Common Internet File System/ Server Message Block*)**
- **NetBIOS**
- ***Windows NT/2000 Resource Kit***

Enumeracja NetBIOS

- **Porty: 135 ÷ 139, 445**
- **P*uste sesje:***

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

Zbigniew Suski BSI – testy penetracyjne cz.2 3

Enumeracja systemu Windows (Nazwy NetBIOS)

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

Zbigniew Suski BSI – testy penetracyjne cz.2 4

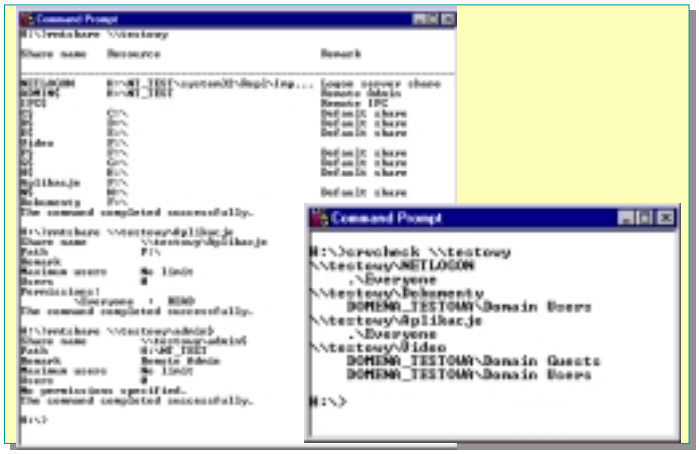
Enumeracja systemu Windows (Nazwy NetBIOS)

Zbigniew Suski BSI – testy penetracyjne cz.2 5

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)



Enumeracja systemu Windows

Przeciwdziałanie enumeracji NetBIOS

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

  Nazwa wartości: *RestrictAnonymous*

  Typ danych: REG_DWORD

  Wartość: 1 (2 - dla W2K)

Enumeracja systemu Windows (SNMP)

Udostępnianie danych przez agenta SNMP

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

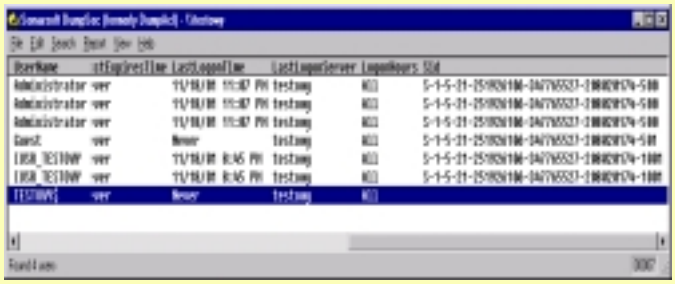
Enumeracja systemu Windows (SNMP) - obrona

- 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 (DNS)

- Rekordy SRV
  - *_gc._tcp* Katalog Globalny (port 3268),
  - *_kerberos._tcp* Kontroler domeny wykorzystujący Kerberosa (port 88),
  - *_ldap._tcp* serwer LDAP (port 389).
- Transfer strefy - program *nslookup*

Enumeracja systemu Windows (SID)



Enumeracja systemu Windows

- Enumeracja *Active Directory*

  dwa tryby pracy *Active Directory*

- Przechwytywanie etykiet z wykorzystaniem *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

Narzędzia z zestawu *Resource Kit*:

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

Enumeracja systemu Windows

Narzędzia dostępne w Internecie:

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

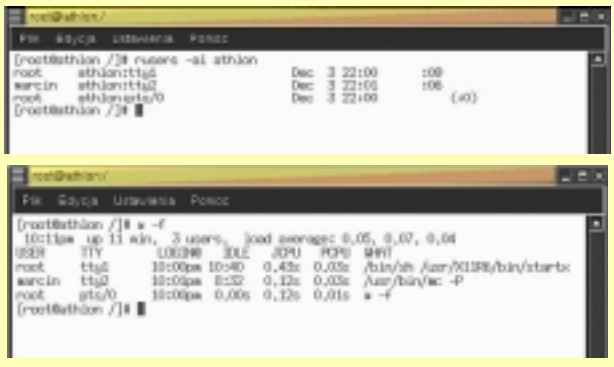
Enumeracja systemu UNIX/Linux

- Polec

```
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*



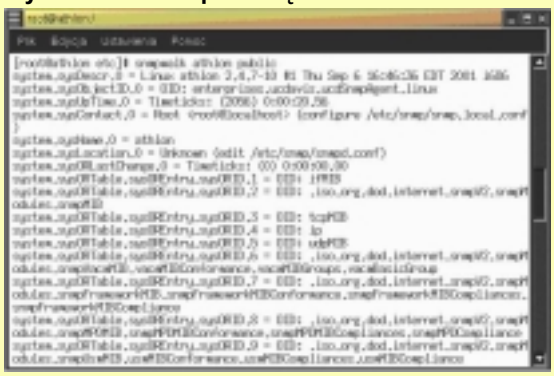
Enumeracja systemu UNIX/Linux

- **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**



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:$1$GSJÔÂÍLN$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.bynawe
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
yppserv         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
cmirr           808/udp         cmirrd
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 vers 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*)**

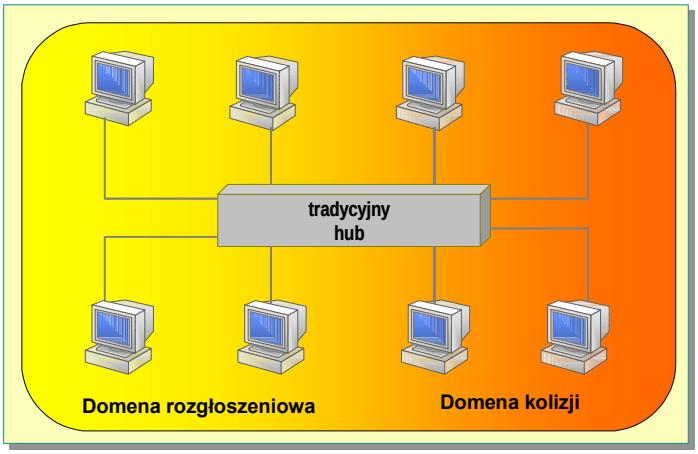
```
HTTP/1.1 200 OK
Date: Sun, 07 Sep 2003 21:04:52 GMT
Server: Apache/1.3.22 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.5 OpenSSL/0.9.6b DAV/1
.0.2 PHP/4.0.6 mod_perl/1.24_01 mod_throttle/3.1.2
Last-Modified: Sat, 17 Feb 2001 12:23:00 GMT
ETag: "27604-7e7-3a8e6d24"
Accept-Ranges: bytes
Content-Length: 2023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

Bezpieczeństwo systemów informatycznych

Testy penetracyjne
część 3

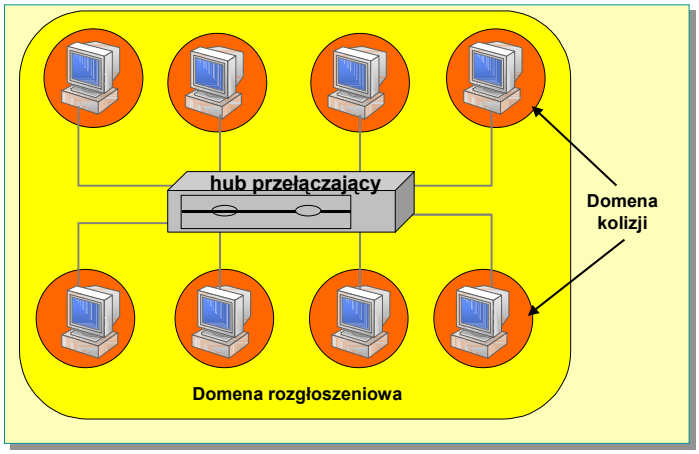
Zbigniew Suski BSI – testy penetracyjne cz.3 1

Domena kolizji i rozgłoszeniowa



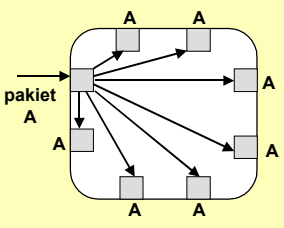
Zbigniew Suski BSI – testy penetracyjne cz.3 2

Domena kolizji i rozgłoszeniowa

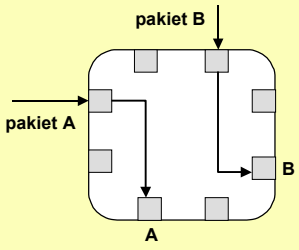


Zbigniew Suski BSI – testy penetracyjne cz.3 3

Hub tradycyjny i przełączający



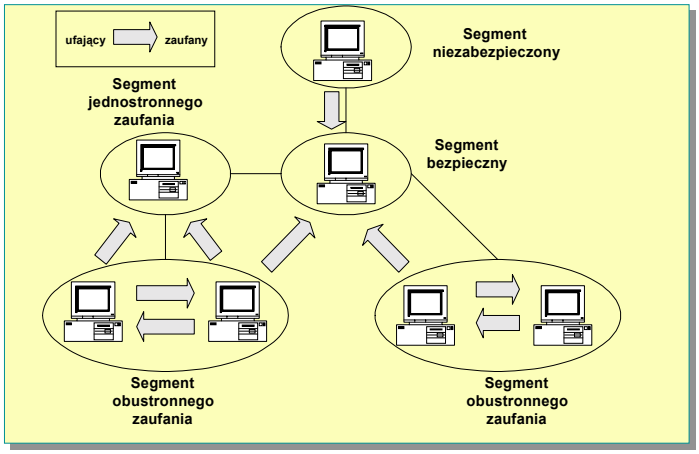
Hub tradycyjny
Pakiet odbierany przez port jest kierowany do wszystkich pozostałych portów



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

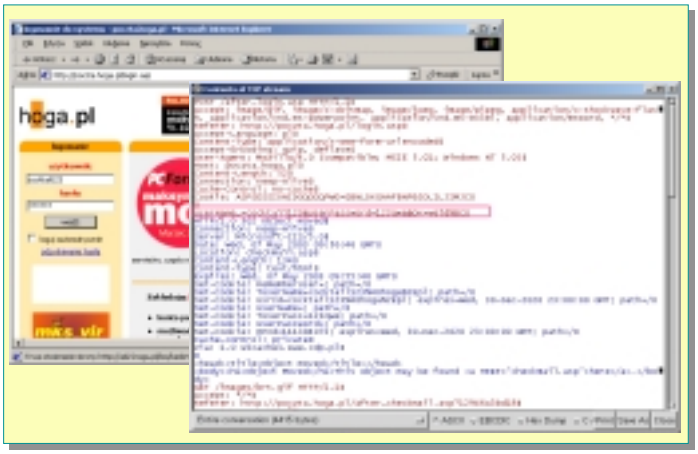
Zbigniew Suski BSI – testy penetracyjne cz.3 4

Relacje zaufania i podział na segmenty

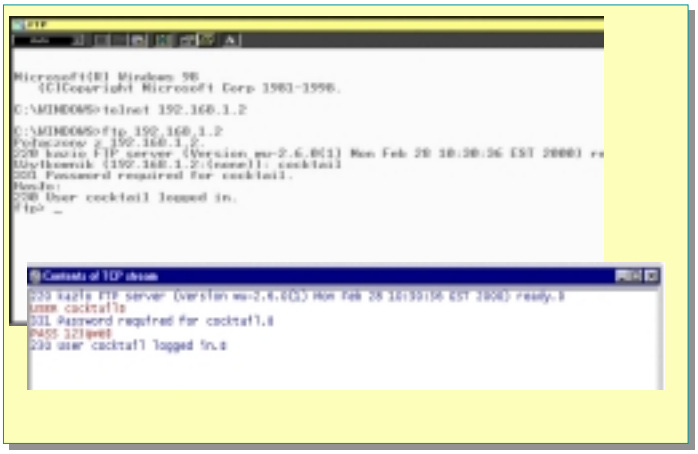


Zbigniew Suski BSI – testy penetracyjne cz.3 5

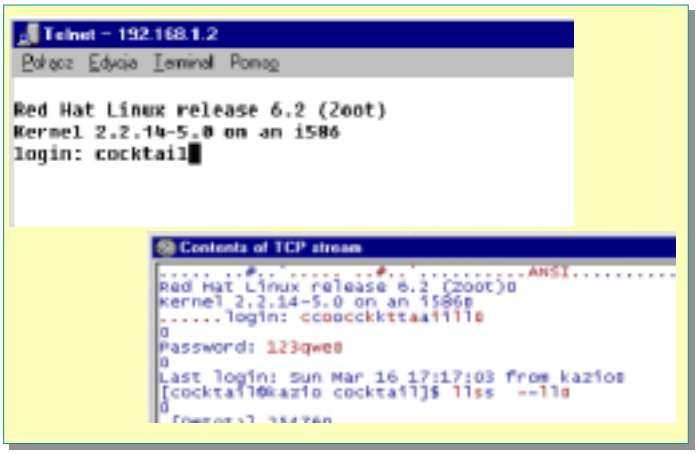
Podsłuchiwanie logowania do poczty WWW



Podsłuchiwanie protokołu FTP



Podsłuchiwanie protokołu Telnet



Podsłuchiwanie protokołu POP