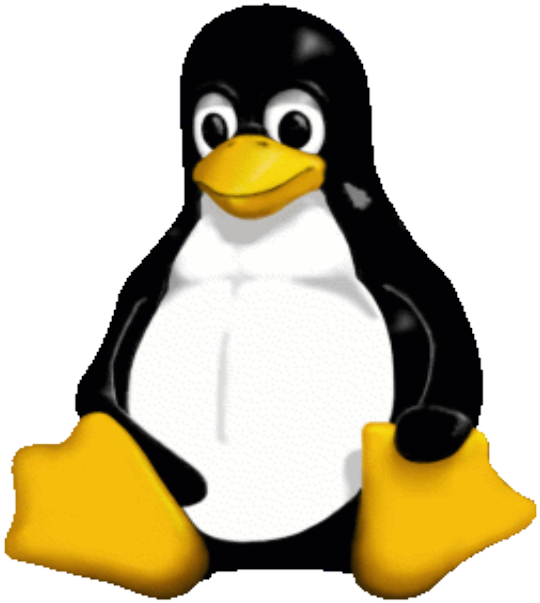
Bezpieczny serwer sieciowy Linux



Jacek Lach
jlach@star.iinf.polsl.gliwice.pl

Plan wykładu

- Skanowanie sieci
- Skanowanie portów
- Identyfikacja systemu operacyjnego

Skanowanie sieci (rekonesans)

- Jeden z pierwszych etapów testu penetracyjnego
- Badanie dostępności poszczególnych hostów w sieci oraz ustalenie struktury połączeń sieci
- Metody podstawowe:
  - ping
  - traceroute

Protokół ICMP

- Opisany w RFC 792
  - Bardziej precyzyjne określenie poszczególnych cech w dokumentach RFC: 1122, 1812
  - Dodatkowa funkcjonalność przedstawiona w dokumentach RFC: 896, 950, 1191, 1256, 1349
- Umożliwia:
  - Przesyłanie komunikatów dotyczących przejściowych problemów z siecią
  - Badanie ogólnej charakterystyki sieci

ICMP - specyfika

- Komunikaty ICMP wysyłane są w datagramach IP. ICMP stanowi część protokołu IP.
- ICMP jest sposobem na wysłanie komunikatów dotyczących problemów z siecią, nie zapewnia dostarczenia datagramu IP.
- W przypadku wystąpienia trwałej awarii sieci komunikaty ICMP nie powinny być wysyłane.

ICMP - specyfika cd.

- Komunikaty ICMP nie są wysyłane w odpowiedzi na komunikaty błędów.
- Komunikaty błędów nie są wysyłane w odpowiedzi na komunikaty wysłane na adresy rozgłoszeniowe.
- Komunikaty ICMP nieznanego typu powinny być odrzucane.
- Liczba komunikatów generowanych przez systemy docelowe zależy od implementacji.

ICMP - komunikaty

- Rodzaje:
  - Komunikaty błędów - ICMP Error Messages
  - Komunikaty zapytań - ICMP Query Messages
- Typ komunikatu określony jest przez pole Typ
- Pole Kod określa podtyp komunikatu
- Przykład:
  Typ = 8, Kod = 0 - Echo Request
- http://www.iana.org/assignments/icmp-parameters

Skanowanie sieci – ping

- ping adres_ip
- ping -b ip_sieci
  można zignorować zgodnie z RFC 1122 -
  domyślna konfiguracja systemów *BSD
  i Windows
- ping sweeps
- ping -R adres_ip

Skanowanie - ping sweep

```
[root]# nmap -n -sP -PI 10.0.0.1-14


Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host  (10.0.0.2) appears to be up.
Host  (10.0.0.3) appears to be up.
Host  (10.0.0.13) appears to be up.
Nmap run completed -- 14 IP addresses (3 hosts up)
scanned in 4 seconds
```

Skanowanie - ICMP

- Zgodnie z RFC implementacja części komunikatów jest opcjonalna.
- Nadużycia związane z ICMP:
  - Wykorzystanie generacji komunikatów przy skanowaniu.
  - Wykorzystanie dowolności implementacji przy identyfikacji systemu operacyjnego.

Skanowanie sieci - Time Stamp

- Timestamp Request (Typ = 13)
  Umożliwia odpytanie zdalnego hosta o aktualny czas. Uzyskana odpowiedź umożliwia określenie opóźnień w sieci. Przesyłany znacznik czasu to liczba milisekund, która upłynęła od północy.

```
$ hping2 -c 1 --icmptype 13 10.0.0.1

13:52:56.458056 10.0.0.2 > 10.0.0.1: icmp: time stamp query id 57392
    seq 0 (ttl 64, id 62993, len 40)

13:52:56.458472 10.0.0.1 > 10.0.0.2: icmp: time stamp reply id 57392
    seq 0 : org 0x28cb789 recv 0x28c5c46 xmit 0x28c5c46 (DF) (ttl
    255, id 0, len 40)
```

Skanowanie - Information Request

- Information Request (Typ = 15)
  Zaprojektowany w celu konfiguracji stacji bezdyskowych. Funkcjonalność lepiej implementowana przez protokoły BOOTP, DHCP.
- Zgodnie z RFC:
  - router nie powinien generować tego typu komunikatów, nie powinien na nie odpowiadać
  - host nie powinien mieć tego typu komunikatów zaimplementowanych

Skanowanie - Address Map

- Address Map Request (Typ = 17)
  Umożliwia uzyskanie maski sieci przez stacje bezdyskowe.
- Router musi mieć zaimplementowaną obsługę tego komunikatu (możliwa jego identyfikacja na drodze pakietu).

Skanowanie - techniki zaawansowane

- Nietypowe ustawienia typu protokołu - wymuszenie komunikatu ICMP Destination Unreachable (np. port unreachable)

```
$ nmap -sU -p 777 10.0.0.1
```

```
10.0.0.2.40309 > 10.0.0.1.777:  udp 0
10.0.0.1 > 10.0.0.2: icmp: 10.0.0.1 udp port
777 unreachable (DF) [tos 0xc0]
```

Skanowanie - techniki zaawansowane

- Wymuszenie komunikatu ICMP Fragment Reassembly Time Exceeded

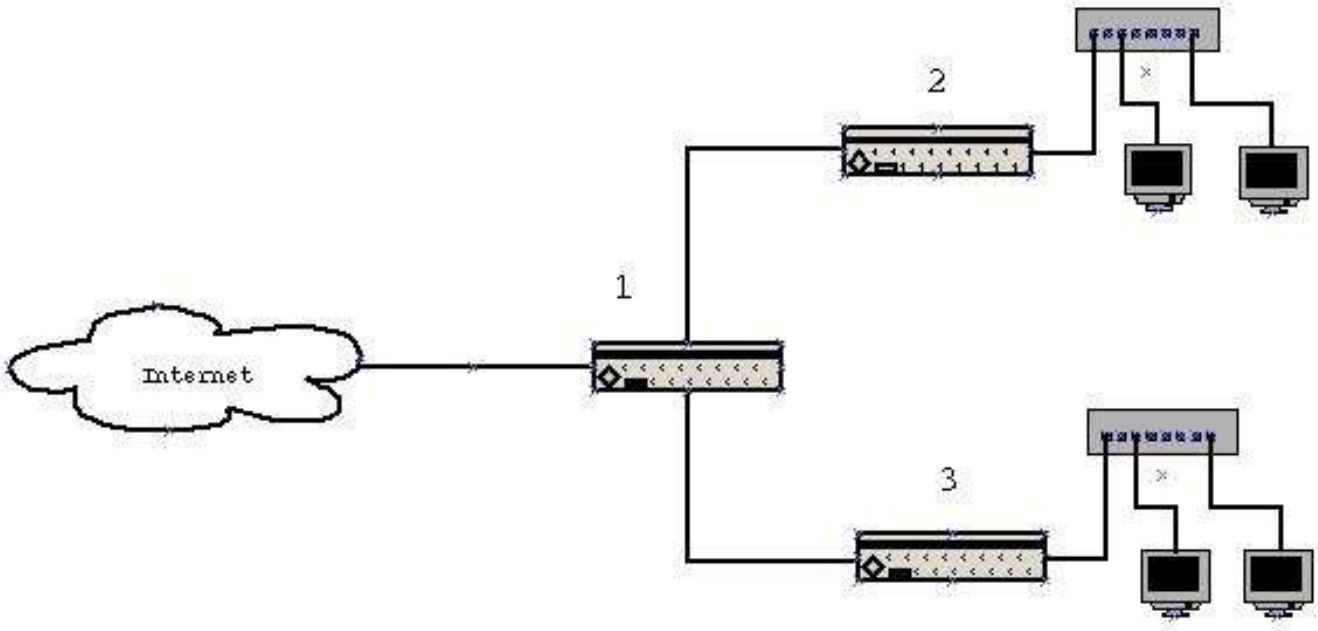
```
$ hping2 -c 1 -S -p 22 --morefrag 10.0.0.13
```

```
10.0.0.2.2115 > 10.0.0.13.22: S 1950284836:1950284836
(0) win 512 (frag 2524:20@0+)
```

```
10.0.0.13 > 10.0.0.2: icmp: ip reassembly time
exceeded [tos 0xc0]
```

Skanowanie - techniki zaawansowane

- Wykorzystanie cech konfiguracji sieci: wymuszenie komunikatu ICMP Fragmentation Needed and Don't Fragment Bit was Set



Mapowanie sieci

- Polecenie traceroute - wykorzystanie komunikatów ICMP Time Exceeded pochodzących od kolejnych hostów na drodze pakietu UDP
- Wykorzystanie komunikatów ICMP Echo Request: opcja -I
- W przypadku gdy badana sieć jest chroniona można próbować techniki firewalking'u
- Ochrona: filtracja pakietów ICMP

Skanowanie portów - 3 way handshaking

- Host 1: SYN - ISN1
- Host 2: SYN - ISN2, ACK - ISN1
- Host 1: ACK - ISN2

Skanowanie portów - techniki podstawowe

- Skanowanie vanilla (TCP connect())
- Cechy:
  - szybka
  - nie wymaga specjalnych uprawnień
  - łatwo wykrywalne, nawet w systemach bez jakichkolwiek zabezpieczeń

Skanowanie - TCP connect()

- **$ nmap -sT -P0 10.0.0.2**
- **Jun 3 01:15:58 machina sendmail[3012]: g581Fwv03012: SYSERR: putoutmsg (laptop): error on output channel sending "220 machina ESMTP": Connection reset by laptop**
- **Jun 3 01:15:58 machina sendmail[3012]: NOQUEUE: root@localhost did not issue MAIL/EXPN/VRFY/ETRN during connection to MTA**
- **Jun 3 01:30:07 machina xinetd[3814]: warning: can't get client address: Connection reset by peer**
- **Jun 3 01:30:07 machina ftpd[3814]: getpeername (in.ftpd): Transport endpoint is not connected**
- **06/03-01:37:30.168470 [**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 10.0.0.4 (THRESHOLD 4 connections exceeded in 0 seconds) [**]**

Skanowanie portów - techniki podstawowe

- Skanowanie półotwarte (TCP SYN scan) - zerwanie połączenia zaraz po drugim kroku nawiązania połączenia
- Cechy:
  - nienawiązane połączenia nie są umieszczane w logach
  - w celu ochrony konieczna instalacja systemu IDS

Skanowanie półotwarte

```
$ nmap -sS -P0 10.0.0.2


Jun  3 01:44:04 10.0.0.4:41337 -> 10.0.0.2:600 SYN
******S*

Jun  3 01:44:04 10.0.0.4:41337 -> 10.0.0.2:482 SYN
******S*

Jun  3 01:44:04 10.0.0.4:41337 -> 10.0.0.2:645 SYN
******S*

Jun  3 01:44:04 10.0.0.4:41337 -> 10.0.0.2:906 SYN
******S*
```

Skanowanie portów - techniki podstawowe

- Skanowanie ukryte (TCP FIN scanning) - wysłanie na port pakietu z ustawioną flagą FIN (odpowiedź: RST - port zamknięty)
- Cechy:
  - niewykrywane przez proste systemy IDS
  - pakiety z flagą FIN rzadziej są filtrowane
  - nie działa w odniesieniu do systemów Windows

Skanowanie ukryte

```
$ nmap -sF -P0 10.0.0.2

06/03-01:50:21.945584  [**] [111:8:1] spp_stream4: STEALTH ACTIVITY
(FIN scan) detection [**] {TCP} 10.0.0.4:36762 -> 10.0.0.2:1212

06/03-01:50:21.945653  [**] [111:8:1] spp_stream4: STEALTH ACTIVITY
(FIN scan) detection [**] {TCP} 10.0.0.4:36762 -> 10.0.0.2:838

06/03-01:50:22.253362  [**] [111:8:1] spp_stream4: STEALTH ACTIVITY
(FIN scan) detection [**] {TCP} 10.0.0.4:36762 -> 10.0.0.2:515

06/03-01:50:22.259857  [**] [100:2:1] spp_portscan: portscan status
from 10.0.0.4: 599 connections across 1 hosts: TCP(599), UDP(0)
STEALTH [**]

$ hping -c 1 -p 23 -F 10.0.0.1

10.0.0.2.2505 > 10.0.0.1.23: F 1222498996:1222498996(0) win 512
10.0.0.1.23 > 10.0.0.2.2505: R 0:0(0) ack 1222498997 win 0 (DF)
```

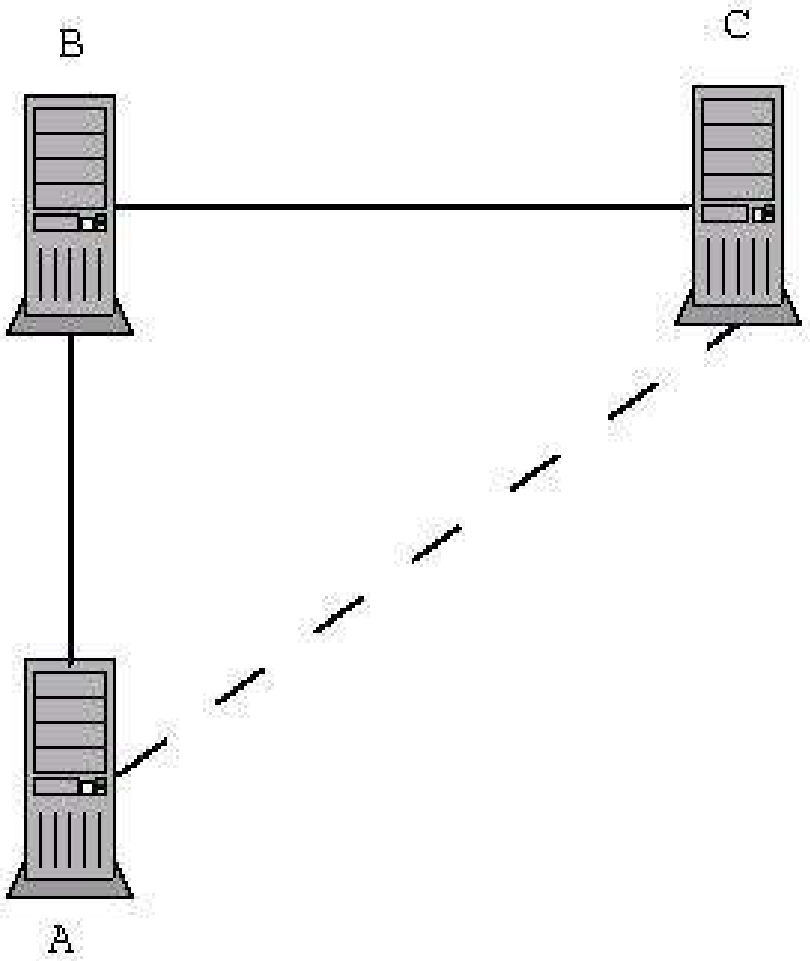
Skanowanie portów - techniki podstawowe

- Skanowanie fragmentami - polega na użyciu dowolnej techniki z podziałem pakietu na fragmenty
- Cechy:
  - niewykrywalne przez filtry pakietów, które nie scalają pakietów - konfiguracja spotykana w urządzeniach mocno obciążonych

Skanowanie portów - ukrywanie

- Techniki ukrywania źródła ataku:
  - Skanowanie dumb host
  - FTP bounce attack
  - Decoy scanning

Skanowanie portów - dumb host



Skanowanie dumb host

```
$ nmap -P0 -p 8080,3128,1433 -sI 10.0.0.2 10.0.0.3


Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )

Idlescan using zombie 10.0.0.2 (10.0.0.2:80); Class:
  Broken little-endian incremental

All 3 scanned ports on shost.localdomain (10.0.0.3) are:
  closed


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

Skanowanie portów - FTP Bounce Attack

- FTP bounce attack - wykorzystanie możliwości tworzenia połączeń proxy przez serwery FTP

```
$ nmap -b user:password@10.0.0.2 -P0 -p 3128,8080,1433
10.0.0.3


Starting nmap V. 2.54BETA7 ( www.insecure.org/nmap/ )

All 3 scanned ports on shost.localdomain (10.0.0.3) are:
closed

Nmap run completed -- 1 IP address (1 host up) scanned
in 9 seconds
```

FTP bounce scan

```
$ nmap -b user:password@10.0.0.2 -P0 -p 3128,8080,1433
10.0.0.3
```

```
Jun  8 02:29:33 lins snort: possible MSSQL probe:
10.0.0.2:20 -> 10.0.0.3:1433

Jun  8 02:29:33 lins snort: SCAN Proxy attempt:
10.0.0.2:20 -> 10.0.0.3:8080

Jun  8 02:29:33 lins snort: INFO - Possible Squid Scan:
10.0.0.2:20 -> 10.0.0.3:3128
```

Skanowanie portów - decoy scan

- Decoy scanning - fałszowanie dużej ilości pakietów w celu ukrycia faktycznego adresu, z którego odbywa się atak.

Decoy scanning

```
# nmap -sX -P0 -p 21,22,25,80,110,119 10.0.0.2
-D10.0.0.6,10.0.0.7,10.0.0.8,10.0.0.9

                                          10.0.0.6


06/03-02:00:08.485344  [**] [100:1:1] spp_portscan:
PORTSCAN DETECTED to port 119 from 10.0.0.7 (STEALTH)
[**]

06/03-02:00:08.485864  [**] [100:1:1] spp_portscan:
PORTSCAN DETECTED to port 119 from 10.0.0.4 (STEALTH)
[**]

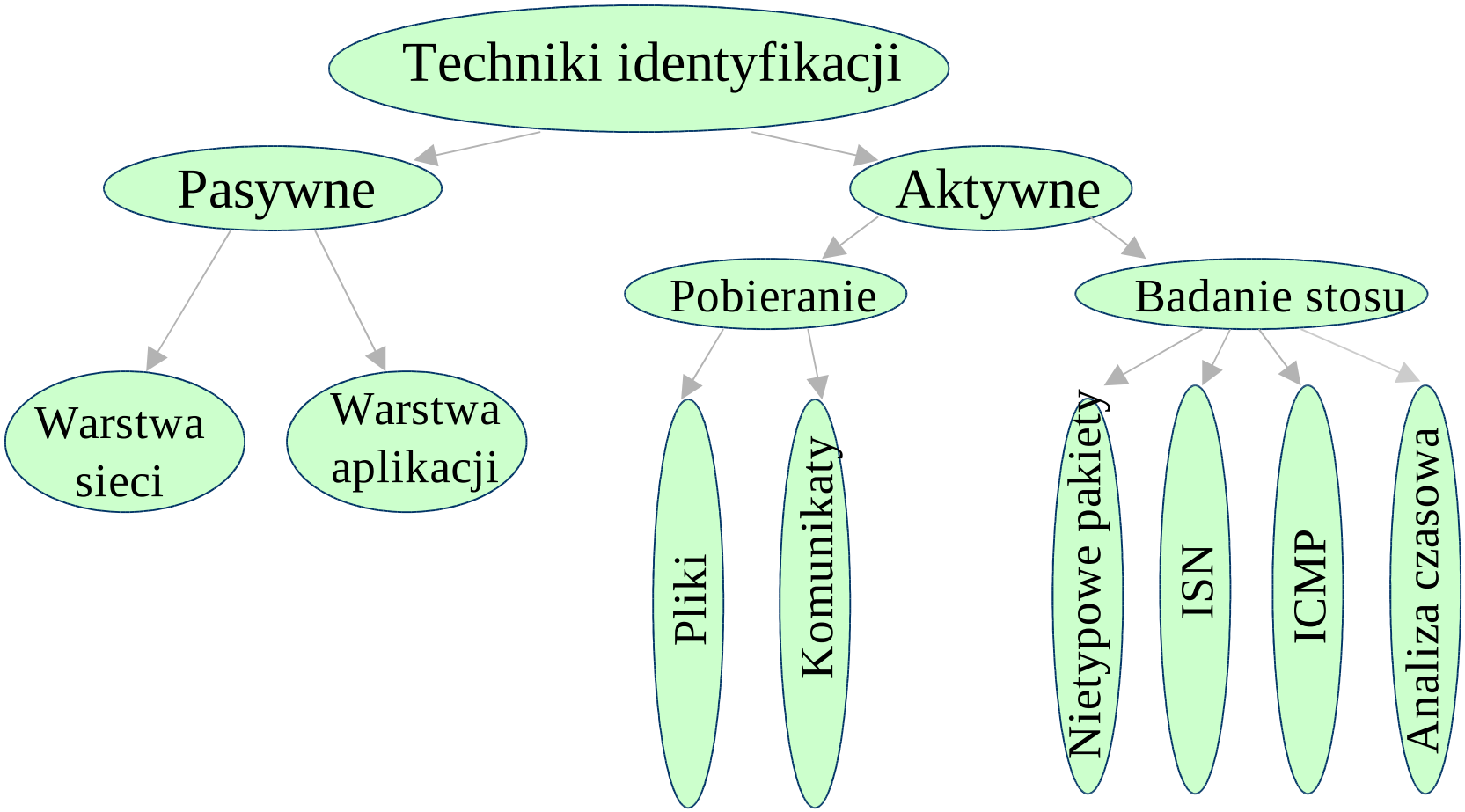
06/03-02:00:08.486514  [**] [100:1:1] spp_portscan:
PORTSCAN DETECTED to port 119 from 10.0.0.8 (STEALTH)
[**]

06/03-02:00:08.486805  [**] [100:1:1] spp_portscan:
PORTSCAN DETECTED to port 119 from 10.0.0.9 (STEALTH)
[**]
```

Identyfikacja systemu operacyjnego - OS fingerprinting

- Określeniu systemu operacyjnego oraz jego wersji
- Cele identyfikacji:
  - badanie sieci
  - testy bezpieczeństwa
  - włamanie
  - ciekawość

Identyfikacja - przegląd technik



Identyfikacja - techniki pasywne

- Podstawa działania: podsłuch ruchu sieciowego
- Analiza ruchu na poziomie:
  - sieci
  - aplikacji
- Cechy:
  - bardzo trudno wykrywalne (o ile możliwe)
  - jakość identyfikacji zależy od lokalizacji sensora
  - mogą być bardzo czasochłonne (bierne oczekiwanie na działanie obserwowanego systemu)

Techniki pasywne - przykład

Message-ID:<Pine.HPX.4.44.0203291854390.4201-100000@host.domain>

X-mailer: Pegasus Mail v3.50 (NDS)

X-Mailer: KMail [version 1.3.1]

X-Mailer: The Bat! (v1.53d)

X-Newsreader: Yanoff 1.5.4 PalmPilot

X-Newsreader: Microsoft Outlook Express 5.00.2919.6600

X-Mailer: Mozilla 4.76 [en] (Win98; U)

Techniki aktywne - pobieranie plików

- Analiza plików binarnych pobranych z serwera
- Wykorzystanie kont anonimowych i błędów w skryptach obsługujących serwisy WWW

Pobieranie plików anonymous FTP

```
$ ftp anonymous.ftp.com
[...]
230 Guest login ok, access restrictions apply.
ftp> cd /usr/lib
250 CWD command successful.
ftp> ls
[...]
-rwxr-xr-x   1 0    1       53656 Feb  3  1999 libsocket.so
226 ASCII Transfer complete.
ftp> get libsocket.so
226 Binary Transfer complete.

$ file libsocket.so
libsocket.so: ELF 32-bit MSB shared object, SPARC, version 1,
   not stripped
SunOS 5.6 Generic
```

Pobieranie plików
błędy w oprogramowaniu

```
                                                ?USERNAME=&PASSWORD=
&ALTERNATE_TEMPLATES=../../../../var/log/dmesg%00


Linux version 2.4.2-2 (root@porky.devel.redhat.com) (gcc
version 2.96 20000731 (Red Hat Linux 7.1 2.96-79))

Initializing CPU#0

Detected 300.684 MHz processor.

Memory: 126492k/131072k available

CPU: AMD-K6(tm) 3D processor stepping 00

hda: QUANTUM FIREBALL ST3.2A, ATA DISK drive ide0 at
0x1f0-0x1f7,0x3f6 on irq 14
```

Identyfikacja - pobieranie komunikatów (banner grabbing)

- Nawiązanie poprawnego połączenia z działającą usługą
- Analiza treści komunikatu

Analiza komunikatów - telnet

```
$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to hostname.domain.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (hostname)

login:
```

Analiza komunikatów - telnet 2

```
$ telnet 192.168.1.2 25

Trying 192.168.1.2...

Connected to hostname.domain.

Escape character is '^]'.

220 (none) ESMTP Sendmail 8.9.3+3.2W/8.9.3/Debian 8.9.3-
  21; Tue, 27 Nov 2001 10:34:23 +0100
```

Techniki aktywne
analiza stosu TCP/IP

- Nawiązanie połączenia
- Analiza zachowania stosu TCP/IP:
  - test rozmiaru okna początkowego
  - próbkowanie ISN
  - test bitu fragmentacji

Techniki aktywne
sytuacje nietypowe

- Badanie reakcji systemu na specjalnie skonstruowane pakiety:
  - test FIN
  - test nieprawidłowej flagi
  - test obsługi fragmentów
  - test obsługi opcji TCP
  - test reakcji na fałszowane pakiety SYN

Techniki aktywne
ICMP

- Wykorzystywane komunikaty:
  - ICMP Message Quoting
  - ICMP error Message Quenching
  - ICMP Error Message Echoing Integrity
  - Type of Service
  - ICMP Time Stamp Request
  - ICMP Information Request
  - ICMP Address Mask Request

nmap - identyfikacja systemu

- Tseq test sekwencji TCP
- T1 test SYN + opcje TCP (otwarty port)
- T2 test NULL + opcje TCP (otwarty port)
- T3 pakiet SYN | FIN | URG | PSH + opcje TCP (otwarty port)
- T4 test ACK + opcje (otwarty port)
- T5 test SYN + opcje (zamknięty port)
- T6 test ACK + opcje (zamknięty port)
- T7 pakiet FIN | URG | PSH + opcje TCP (zamknięty port)
- PU pakiet UDP (zamknięty port)

nmap - przykład

```
# nmap -sS -P0 -O -p 80,135 10.0.0.3

Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Interesting ports on host.domain (10.0.0.3):
(The 1 port scanned but not shown below is in state:
  closed)
Port       State       Service
135/tcp    open        loc-srv
Remote operating system guess: Windows Millennium Edition
  (Me), Win 2000, or WinXP

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

- Packet count: 41 (3158)
- Bytes of traffic: 2980 (~300kB)

nmap - podsumowanie

- Cechy:
  - łatwa detekcja
  - stosunkowo wolna metoda przy skanowaniu dużej podsieci
  - duży generowany ruch w sieci

X i Xprobe

- Ofir Arkin 2001 (www.sys-security.com)
- Technika wykorzystania protokołu ICMP przy identyfikacji systemu: X
- Narzędzie wykorzystujące protokół ICMP: Xprobe
- Cechy:
  - duża szybkość
  - bardzo duża skuteczność
  - niewielki generowany ruch w sieci
  - możliwa detekcja i blokowanie

xprobe - przykład

```
$ ./xprobe 10.0.0.3
X probe ver. 0.0.2
------------------
Interface: eth0/10.0.0.2

LOG: Target: 10.0.0.3
LOG: Netmask: 255.255.255.255
LOG: probing: 10.0.0.3
LOG: [send]-> UDP to 10.0.0.3:32132
LOG: [98 bytes] sent, waiting for response.
LOG: [send]-> ICMP echo request to 10.0.0.3
LOG: [68 bytes] sent, waiting for response.
FINAL:[ Windows 2k. SP1, SP2/Windows XP ]

Packet count: 4

Bytes of traffic: 346
```

Analiza czasowa i RING

- RFC 793 nie precyzuje algorytmu retransmisji pakietu w sytuacji przeciążenia sieci
- Producenci przyjmują różne metody retransmisji pakietu
- Schemat działania:
  - wybór hosta z otwartym portem
  - zablokowanie pakietów pochodzących z badanego hosta
  - nasłuch wszystkich przychodzących pakietów
  - próba nawiązania połączenia (pakiet SYN)
  - analiza odstępów pomiędzy kolejnymi pakietami

RING - przykład

```
# ./ring -d 10.0.0.3 -s 10.0.0.2 -p 445 -f fingerprint
  -i eth0

2938429 6007911

OS:Windows_2000

distance:27549



Packet count: 4

Bytes of traffic: 318
```

Identyfikacja - ochrona

- Techniki aktywne:
  - instalacja systemu IDS
  - ograniczenie ruchu komunikatów ICMP
  - kontrola komunikatów systemowych
  - SYN Relay
- Techniki pasywne:
  - ograniczenie zbędnych informacji
  - szyfrowanie transmisji
- Próba "zmylenia przeciwnika"

Identyfikacja - ochrona

- Modyfikacja domyślnego działania systemu:
  - modyfikacja bannerów systemowych
  - modyfikacja działania stosu TCP/IP
- Technika stosowana jako dodatkowa, jedynie po wprowadzeniu innych zabezpieczeń
- Zagrożenia:
  - możliwość stworzenia nowych luk
  - destabilizacja lub pogorszenie działania stosu TCP/IP

Za tydzień ...

- Zabezpieczenie systemu po instalacji
- Start systemu