5. Scanarea şi enumerarea

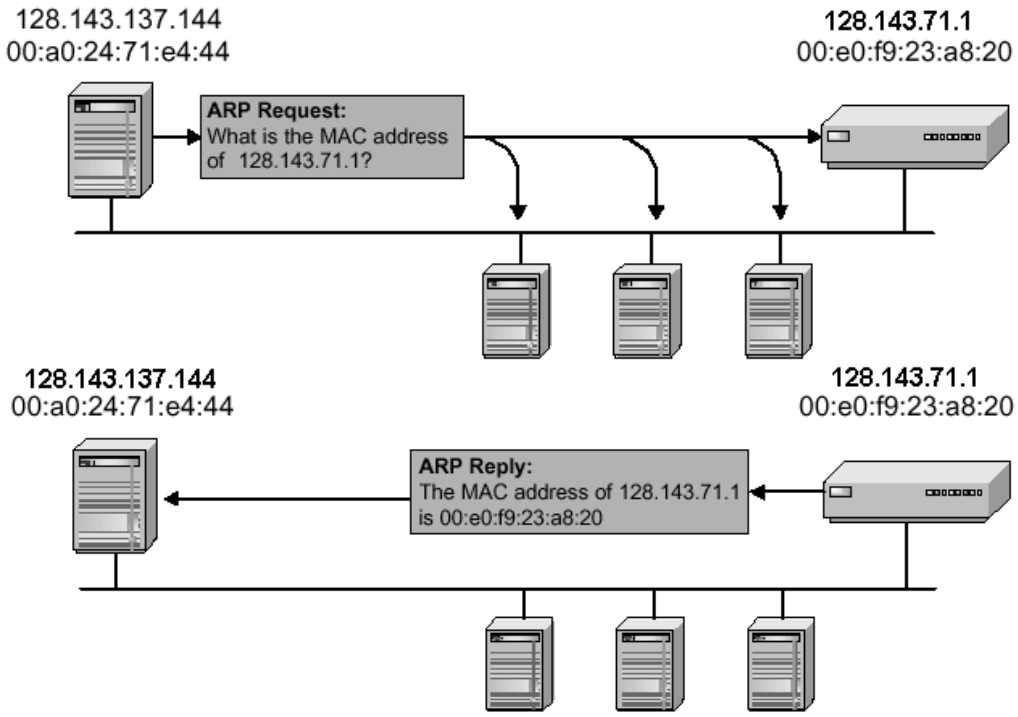
Rol

- **Scanarea**
  - identificare sisteme active, porturi deschise şi servicii asociate, reguli firewall, etc
  - analiză la nivel de reţea (network scanning) / sistem (port scanning)
- **Enumerarea**
  - determinare conturi utilizator, foldere partajate, mod de configurare, etc
  - interogări directe prin intermediul conexiunilor active
- **Implică, de regulă, interacţiuni directe cu ţinta**
  - pot fi detectate prin jurnalizare, IDS, etc

Etape

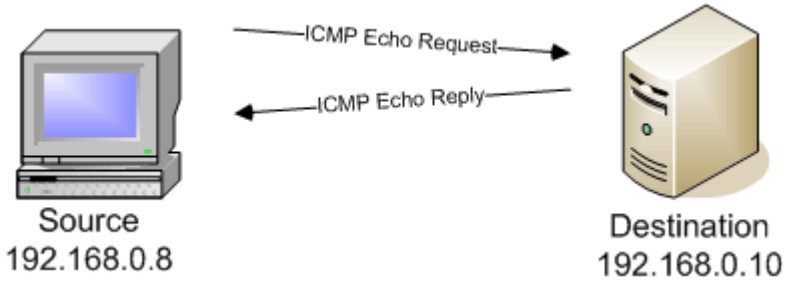
1. Descoperirea sistemelor active
2. Identificarea porturilor deschise
3. Determinarea serviciilor ce rulează pe fiecare port în parte
4. Stabilirea versiunii sistemului de operare şi a serviciilor
5. Identificarea vulnerabilităţilor

ARP Ping



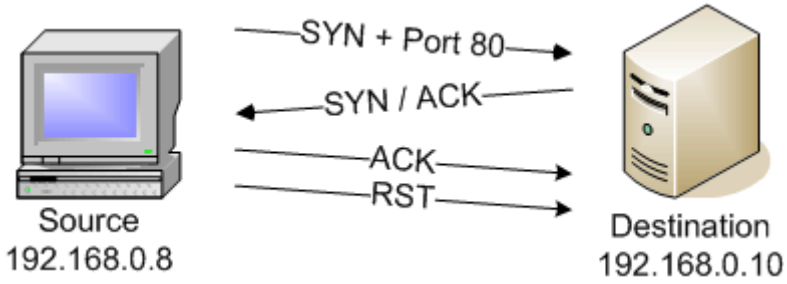
- Permite descoperirea numai a sistemelor din reţeaua locală
- Nu funcţionează dacă Proxy ARP este configurat pe routere
- Unelte:
  - arping
  - nmap –PR

ICMP Ping



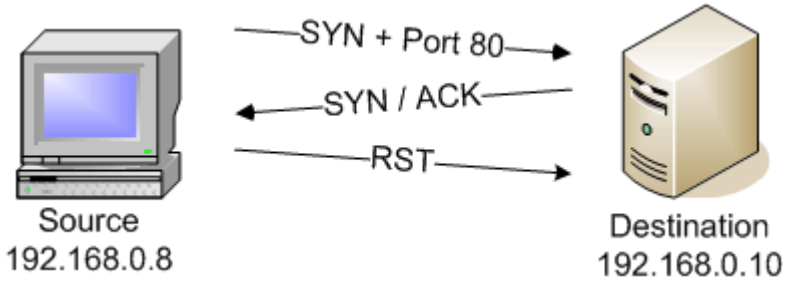
- Interogări ICMP
  - ICMP ECHO_REQUEST (Type 8)
  - ICMP ECHO_REPLY (Type 0)
- Poate fi blocat de network firewall / personal firewall
- Unelte:
  - ping / fping
  - nmap –sP –PE
  - hping3 --icmp

TCP Connect Scan



- Metodă de scanare simplă şi rapidă
- Creează conexiuni TCP complete
- Apelurile connect() sunt în general jurnalizate
- Unelte:
  - telnet
  - netcat
  - nmap –sT

TCP SYN Scan

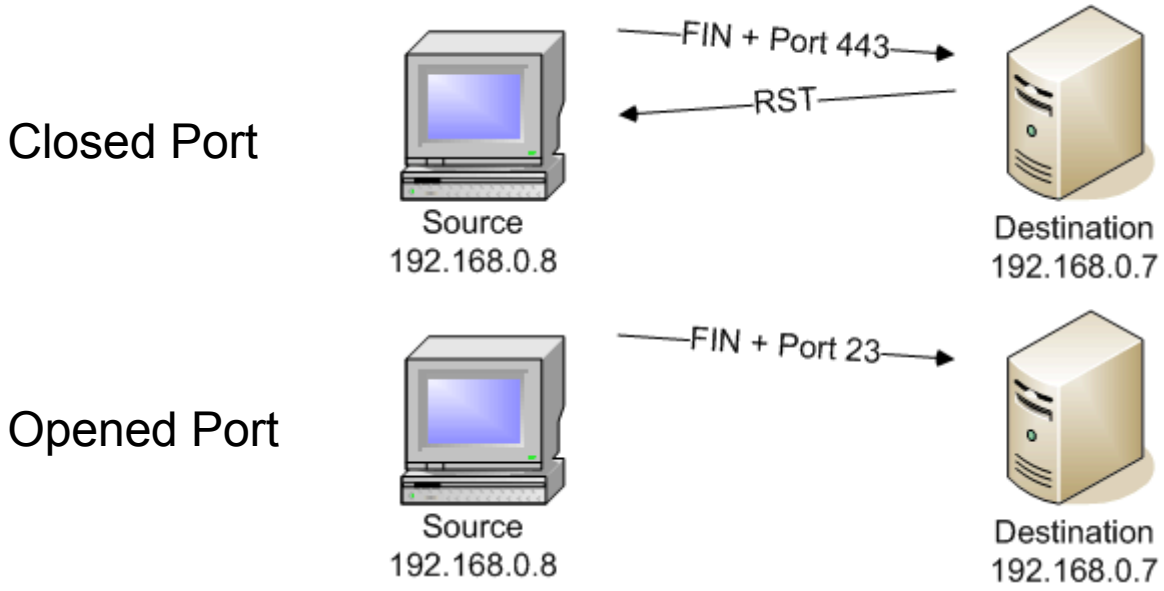


- Conexiuni pe jumătate deschise (half open connection)
  - se transmite un pachet SYN pentru a cere deschiderea conexiunii
  - după recepţionarea unui SYN/ACK se renunţă la conexiune trimiţându-se un pachet RST
- Greu de detectat
  - majoritatea IDS şi firewall-urilor nu interpretează pachetele SYN
- Unelte:
  - nmap –sS
  - hping3 --syn

TCP FIN, Xmas Tree, Null Scan

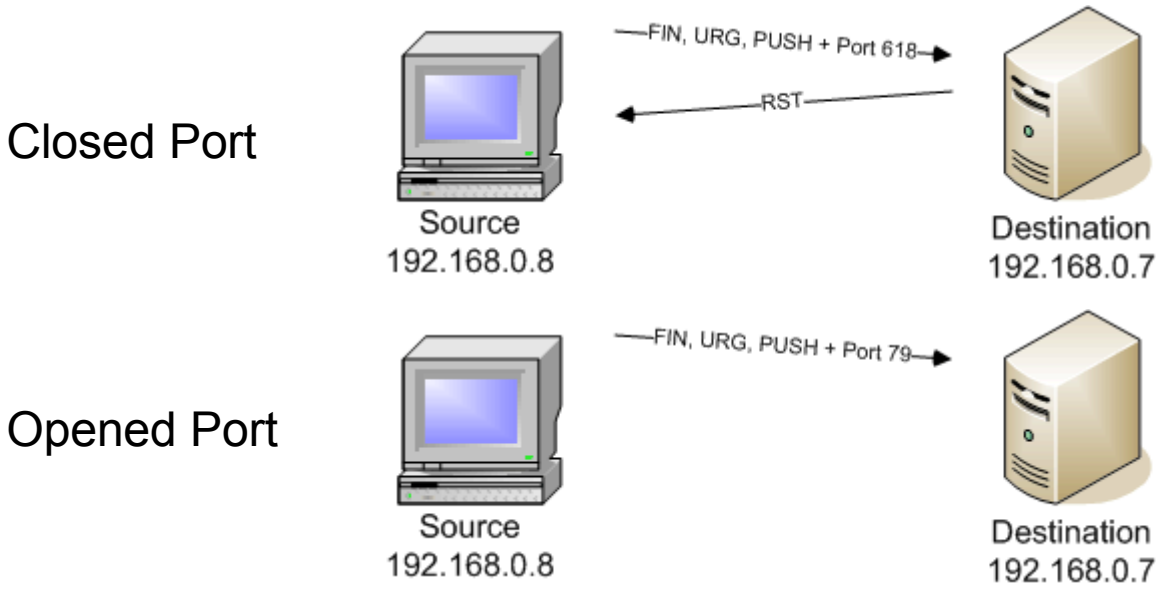
- Stealth scans
- Principiul de funcţionare este acelaşi
  - manipularea biţilor de control (flags) din antetul pachetelor TCP
  - pachete atipice (ce nu pot şi întâlnite în realitate)
- Conform RFC 793, atunci când un sistem primeşte un pachet pe un port închis, trebuie să răspundă cu un RST
  - dacă nu se recepţionează nici un RST înseamnă că portul este deschis sau comunicaţia este filtrată de firewall
- Nu funcţionează în cazul sistemelor Windows
  - returnează RST chiar dacă portul este deschis
- Pentru a putea efectua aceste tipuri de scanări utilizatorul trebuie să aibă drepturi administrative

TCP FIN Scan



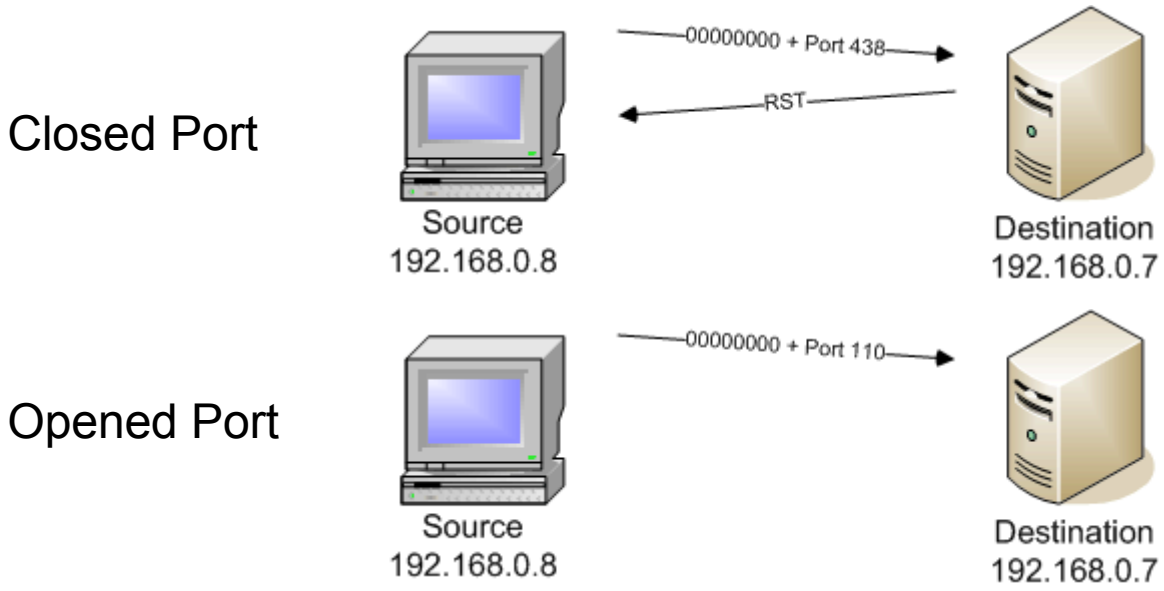
- **Se trimite din prima un pachet TCP având flag-ul FIN setat**
- **Unelte:**
  - **nmap –sF**
  - **hping3 --fin**

TCP Xmas Tree Scan



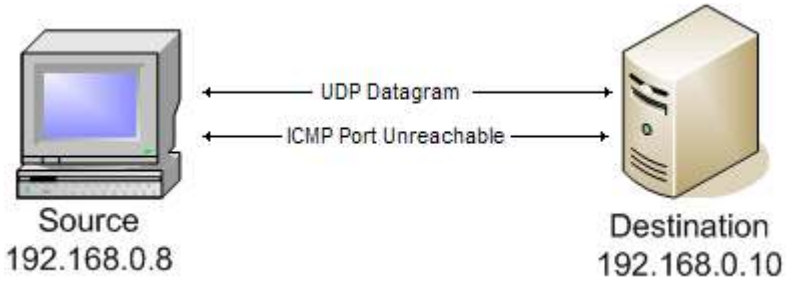
- **Se trimite din prima un pachet TCP având flag-urile FIN, URG şi PUSH setate**
- **Unelte:**
  - **nmap –sX**
  - **hping3 --fin --urg --push**

TCP Null Scan



- **Se trimite din prima un pachet TCP fără nici un flag setat**
- **Unelte:**
  - **nmap –sN**
  - **hping3**

UDP Scan



- Similar unui TCP scan dar cu pachete UDP
- Se transmit pachete UDP către porturile de pe calculatorul ţintă; dacă nu apare nici o eroare ICMP atunci portul UDP este deschis
- Proces lent
  - timp de răspuns mare 1-4 sec
- Unelte:
  - nmap –sU
  - hping3 --udp

OS Fingerprinting

- RFC-urile nu conţin specificaţii complete
- Diferenţe subtile în implementarea stivei TCP/IP
  - TTL (time-to-live)
  - Numerele de secvenţă iniţiale
  - Window size
  - DF (Don't fragment bit)
  - …
- Passive fingerprinting
  - analiza pachetelor care trec prin dreptul staţiei de observare
  - precizie scăzută
- Active fingerprinting
  - trimiterea de pachete către ţintă pentru a vedea cum se comportă
  - precizie ridicată

Passive OS fingerprinting

- p0f (http://lcamtuf.coredump.cx/p0f.shtml)
- p0f poate identifica sistemul de operare al:
  - maşinilor care se conectează la dumneavoastră (SYN mode)
  - maşinilor la care dumneavoastră vă conectaţi (SYN+ACK mode)
  - maşinilor la care nu vă puteţi conecta (RST mode)
  - maşinilor a căror comunicaţie o puteţi observa
- p0f output

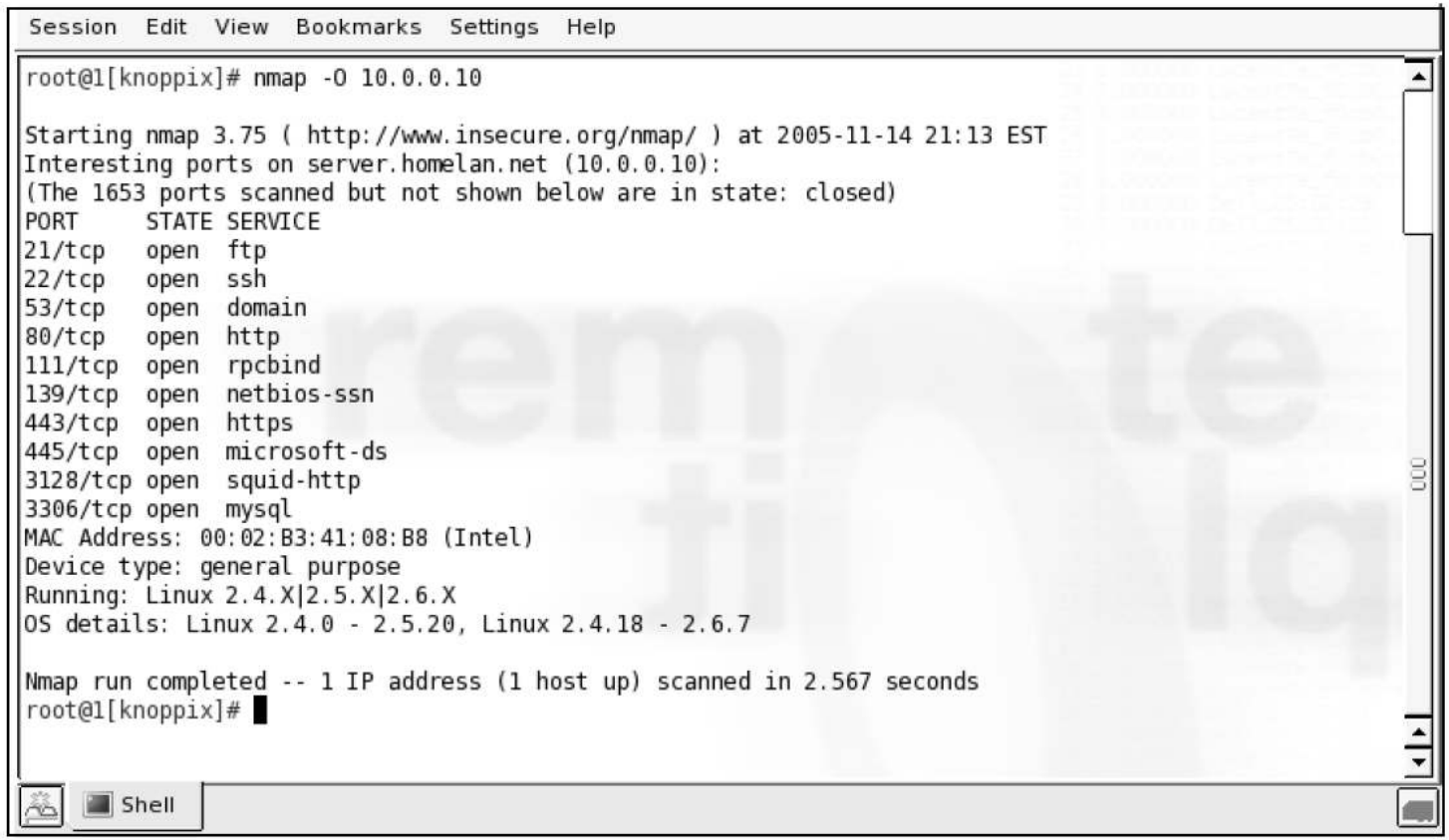
```
<Wed Feb 27 18:26:58 2008> 213.215.x.x:45291 - Linux 2.6
   (newer, 2) (up: 1421 hrs) -> 208.83.x.x:2703 (distance 0,
   link: ethernet/modem)

<Wed Feb 27 18:27:02 2008> 212.24.x.x:62994 - FreeBSD 5.3-
   5.4 (up: 4556 hrs) -> 213.215.x.x:80 (distance 9, link:
   ethernet/modem)

<Wed Feb 27 18:27:16 2008> 90.2.x.x:1322 - Windows 2000 SP4,
   XP SP1+ -> 213.215.x.x:80 (distance 9, link: pppoe (DSL))
```

Active OS fingerprinting

- nmap –O <target>
- 7 probe TCP, 1 ICMP, 1 UDP, la interval de 110 milisecunde



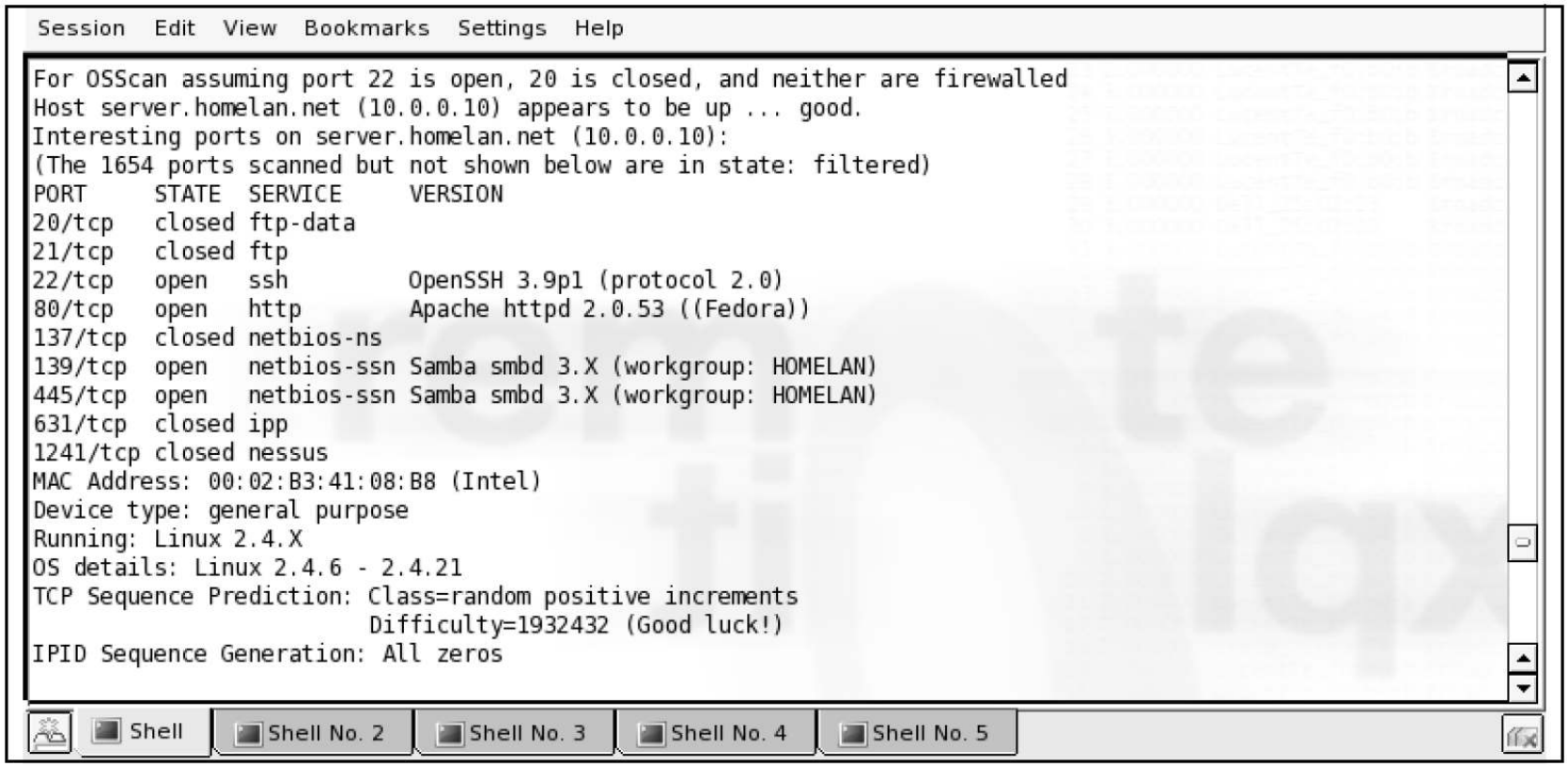
Banner Grabbing

- Foarte multe servicii “se prezintă” în momentul conectării
- Unelte:
  - telnet 192.168.2.10 80
  - nc 192.168.2.10 80
  - amap
  - httprint

```
HTTP/1.1 200 OK
Date: Fri, 25 Jan 2008 23:46:30 GMT
Server: Apache/1.3.26 (Unix) mod_ssl/2.8.10 OpenSSL/0.9.7d
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Banner Grabbing (cont.)

- nmap –sV <target>
- Detectarea versiunii serviciilor



Enumerarea

- Interogări directe asupra ţintei
- Are ca obiectiv obţinerea de informaţii particulare despre fiecare sistem în parte:
  - conturi utilizator
  - foldere partajate
  - mod de configurare
- Activitate intruzivă
  - se jurnalizează

Enumerarea pe platforme Windows

- NetBIOS Name Resolution
  - Listare domenii sau calculatoare dintr-un domeniu
  - Unelte:
    - net view / domanin
    - nbtscan –A <IP address> (Windows 2000)
- SMB Null Sessions
  - Listare conturi utilizator, foldere partajate, etc
  - Dezactivate implicit începând cu Windows XP
  - Unelte:
    - net use \\192.168.5.10 \IPC$ " " /u: " "
      net view \\192.168.5.10
    - DumpSec
    - Hyena
- Registry Enumeration
- SAM (Security Accounts Manager)
  - user2sid / sid2user

Enumerarea SNMP

- Simple Network Management Protocol (SNMP)
  - SNMP Agent (echipament de reţea, claculatoare, etc)
  - SNMP Management Station
- Interogări (UDP / 161)
- Trape (UDP / 162)
- Management Information Base (MIB)
  - baza de date cu variabilele de configurare
  - Microsoft stochează în MIB numele conturilor utilizator
- Parole de acces
  - read community string (valoarea default este *public*)
  - read/write community string (valoarea default este *private*)
- Unelte:
  - SNMPUtil (Windows 2000 Resource Kit)
  - snmpget / snmpwalk (Unix)
  - IP Network Browser (http://www.solarwinds.com/downloads/)

Alte unelte de scanare / enumerare

- nmap (http://www.insecure.org/nmap/)
- hping3 (http://www.hping.org)
- IPEye (http://ntsecurity.nu/toolbox/)
- NetScan Tools Pro (http://www.netscantools.com/)
- SuperScan (http://www.foundstone.com)
- Cheops-ng (http://cheops-ng.sourceforge.net/)