Mandriva Conectiva

TCP/IP e Service Fingerprinting

Como descobrir informações a respeito de um host remoto explorando detalhes da implementação da pilha TCP/IP e seus serviços

Ademar de Souza Reis Jr.
<ademar@conectiva.com.br>
http://www.ademar.org

XII Congresso C. Computação Bolívia
Tarija – Bolívia – Outubro 2005

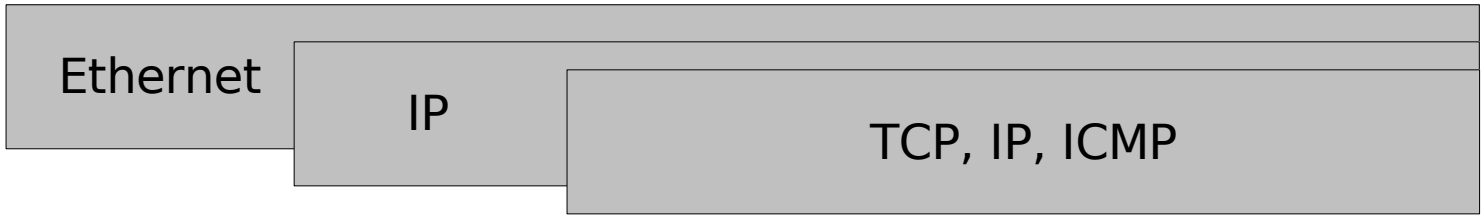
última versão atualizada disponível em
http://www.ademar.org/

Conteúdo

- Introdução: revisão conceitos TCP/IP
- Descobrindo o SO
- Descobrindo o uptime
- Implicações de segurança
- Técnicas anti-fingerprinting
- Conclusões e recomendações

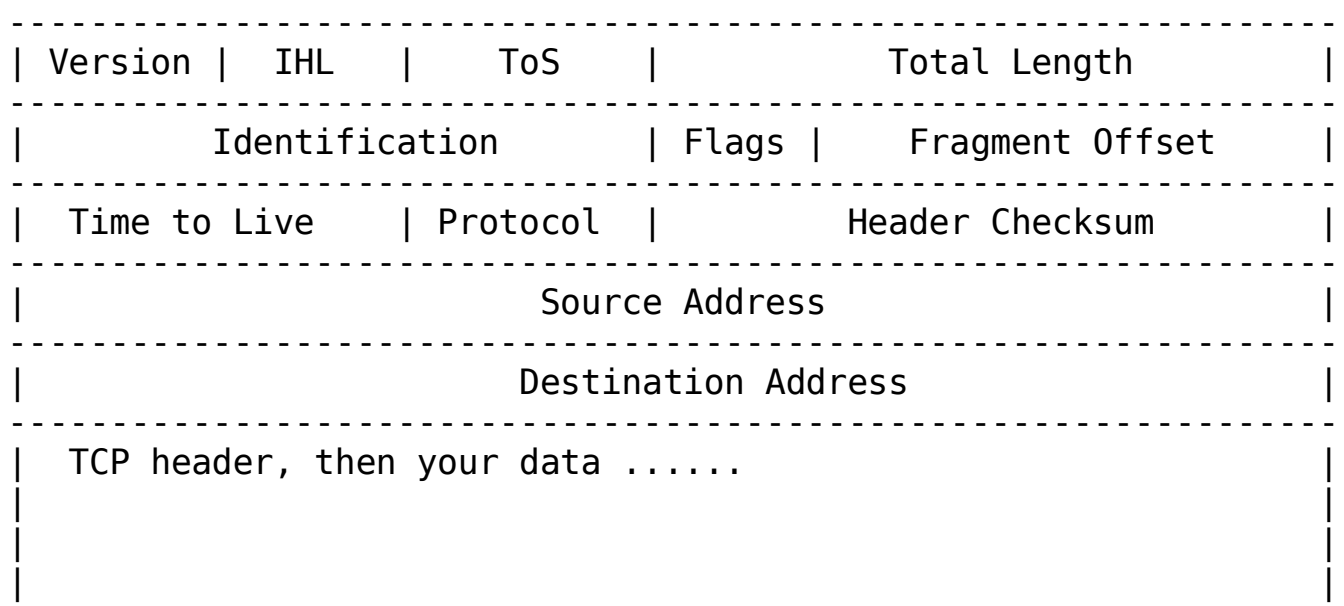
TCP/IP: Encapsulamento

- Ethernet, 811g, Bluetooth, etc
  - IPv4, IPv6
    - TCP, IP, UDP, ICMP, DCCP, etc

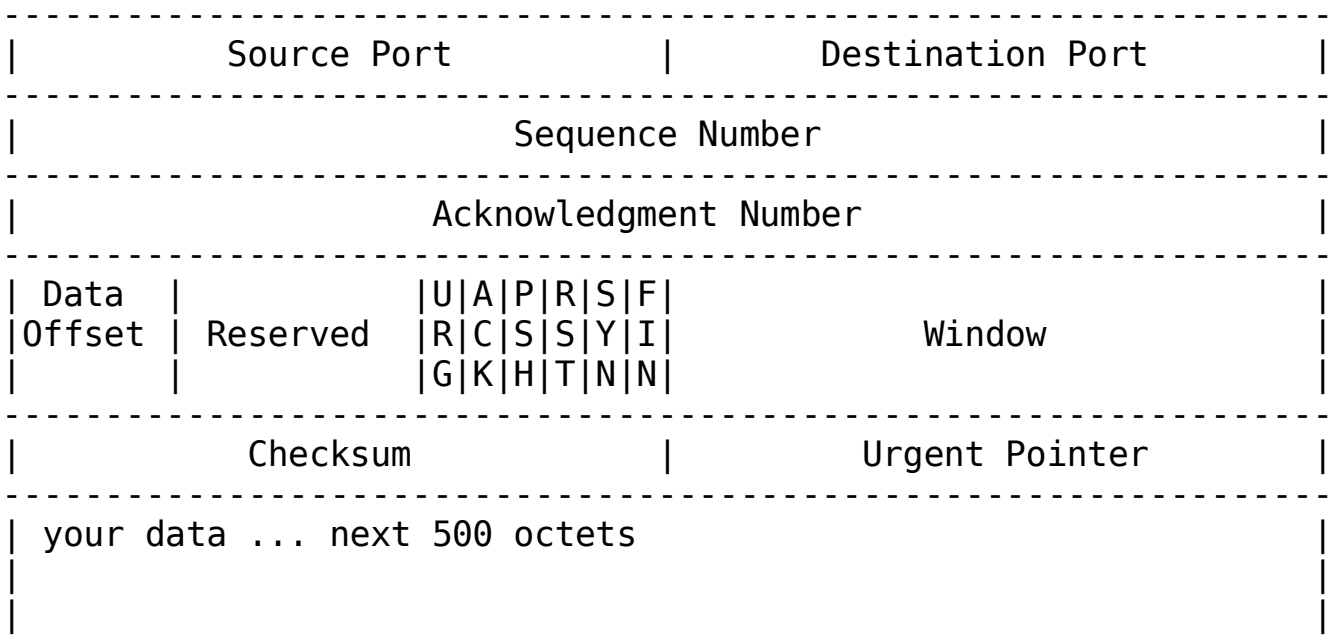


- Cada datagrama tem seus cabeçalhos

Um datagrama IP



Um datagrama TCP



Conexão TCP (three-way-handshaking)

Cliente --> Servidor

Iniciar:

```
--> SYN(ISNc)
<-- SYN(ISNs), ACK(ISNc)
--> ACK(ISNs)
(conexão estabelecida)
```

Fechar:

```
--> FIN(ISNc)
<-- ACK(ISNc) #informa aplicação
<-- FIN(ISNs), ACK(ISNc)
--> ACK(ISNs)
```

Mensagens ICMP

Internet Control Message Protocol

- Parte integrante da pilha IP
- Detecção/reporte de erros
- Obtenção de informações
- Uso comum: ping, traceroute

```
toy~> ping www.google.com
PING www.l.google.com (72.14.207.104) 56(84) bytes of data.
64 bytes from 72.14.207.104: icmp_seq=1 ttl=240 time=299 ms
64 bytes from 72.14.207.104: icmp_seq=2 ttl=240 time=253 ms
```

Detecção remota: técnicas clássicas

```
toy~> telnet server.mydomain
Trying 10.0.0.1 ...
Connected to server.mydomain
Escape character is '^]'.

HP-UX hpux B.10.01 A 9000/715 (ttyp2)

login:

toy~> telnet ftp.mydomain 21
Trying 10.0.0.2 ...
Connected to ftp.mydomain.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

```
toy~> telnet server.mydomain 22
Trying 10.0.0.1
Connected to server.mydomain.
Escape character is '^]'.
SSH-1.99-OpenSSH_3.8.1p1

toy~> echo 'bla' | nc www.ademar.org 80 | grep '<address>'
<address>Apache/2.0.49 (Unix) mod_ssl/2.0.49 OpenSSL/0.9.7c DAV/2 Server
at www.ademar.org Port 80</address>
```

Nmap: Service Fingerprinting

- Port-scan
- Rápido
- Aguarda por banner em silêncio (5 segs)
- Envia probe conforme a porta (helo, help, GET /, etc)
- Suporte a SSL
- Suporte a regexps e sequências em formato binário
- Amplo banco de dados (> de 2800 atualmente)

Nmap: Service Fingerprinting

Exemplo real

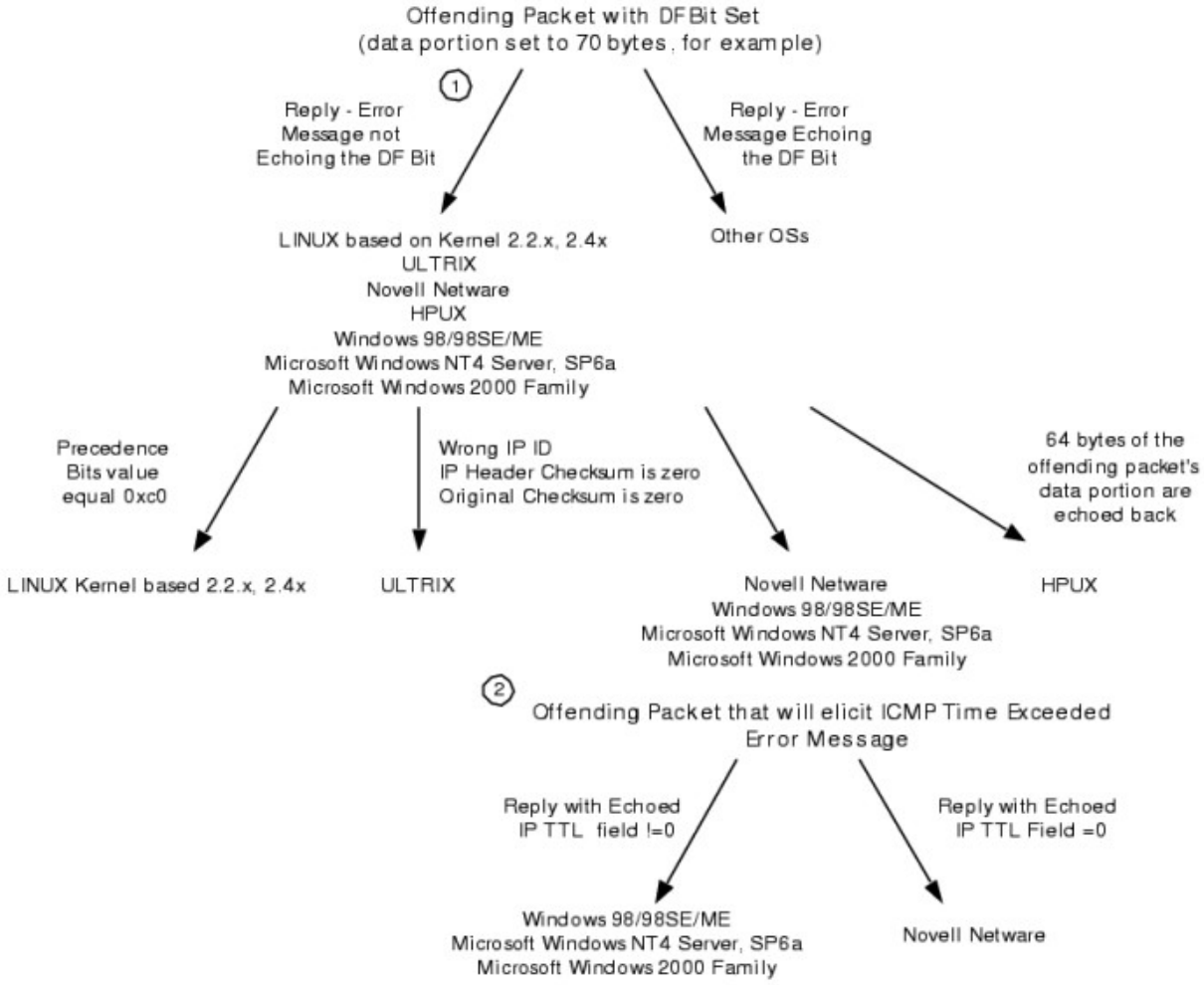
```
[root@optimus64 /]# nmap -sV localhost

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-10-18 22:38 UTC
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1655 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE                VERSION
21/tcp   open  ftp                    ProFTPD 1.2.9
22/tcp   open  ssh                    OpenSSH 3.8.1p1 (protocol 1.99)
80/tcp   open  http                   Apache httpd 2.0.49 ((Unix) mod_ssl/2.0.49 OpenSSL/0.9.7c DAV/2)
111/tcp  open  rpcbind                2 (rpc #100000)
443/tcp  open  ssl/http               Apache httpd 2.0.49 ((Unix) mod_ssl/2.0.49 OpenSSL/0.9.7c DAV/2)
875/tcp  open  rquotad (rquotad V1-2) 1-2 (rpc #100011)
912/tcp  open  mountd (mountd V1-3)   1-3 (rpc #100005)
2049/tcp open  nfs (nfs V2-4)         2-4 (rpc #100003)

Nmap finished: 1 IP address (1 host up) scanned in 14.570 seconds

[root@optimus64 root]# rpm -q proftpd openssh-server apache openssl-progs
proftpd-1.2.9-58668U10_1cl
openssh-server-3.8.1p1-60281cl
apache-2.0.49-61251U10_5cl
openssl-progs-0.9.7c-52922cl
```

TCP/IP Stack Fingerprinting

- **Diferentes implementações da pilha TCP/IP**
- **Testes**
  - Opções TCP
  - FIN
  - Flag inválida
  - Bit de não fragmentação
  - Exemplo ISN
  - Mensagem de erro ICMP
  - Type of Service
  - etc...

TCP/IP Stack Fingerprinting

Exemplo usando pacotes ICMP



TCP/IP Stack Fingerprinting

Nmap

- Amplo banco de dados (> 1700 entradas atualmente)
- Múltiplas técnicas

Exemplos de fingerprint

```
FingerPrint  IRIX 6.2 - 6.4
TSeq(Class=i800)
T1(DF=N%W=C000|EF2A%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=N%W=C000|EF2A%ACK=O%Flags=A%Ops=NNT)
T4(DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)
```

```
Fingerprint Apple Mac OS X 10.1.5
Class Apple | Mac OS X | 10.1.X | general purpose
TSeq(Class=TR%gcd=<6%IPID=RD%TS=2HZ)
T1(DF=N|Y%W=0|FFFF%ACK=S++%Flags=AR|AS%Ops=|MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=N|Y%W=0|FFFF%ACK=S++%Flags=AR|AS%Ops=|MNWNNT)
T4(DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=0%ULEN=134%DAT=E)
```

TCP/IP Stack Fingerprinting

Nmap: exemplos de uso

```
[root@optimus64 ~]# nmap -O localhost
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-10-18 22:38 UTC
[...]
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7), Linux 2.6.3 – 2.6.8
[...]
```

```
[root@optimus64 ~]# nmap -O anotherbox
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-10-18 22:38 UTC
[...]
Device type: general purpose
Running: Microsoft Windows|2003/.NET|NT/2K/XP
OS details: Microsoft Windows 2003 Server or XP SP2
[...]
```

Remote uptime

Técnicas

- **Netcraft** (http://www.netcraft.com)
  - Técnica não revelada (TCP Timestamp + pings frequentes?)
- **TCP Timestamp** (Opção TCP - RFC 1323, 1992)
  - Incrementado a partir de 0
  - Incrementado a partir de um número aleatório
  - Criado randomicamente a cada conexão

TCP Timestamp (RFC 1323)

- **Windows**
  - Win95/98/Me/NT3.5/4.0: não suportado
  - Windows 2000/XP: a cada 100ms. valor inicial randômico
- **Linux**
  - 2.0.X: não suportado
  - 2.1.9-2.6.12: a cada 100ms, inicia em 0
- **4.4BSD // OpenBSD, BSDi, BSD/OS, FreeBSD (2.1.5)**
  - a cada 500ms, inicia em 0

Implicações de Segurança

- Vulnerabilidades conhecidas
- “Script kiddies”
- Uptime alto: máquina desatualizada?
- Engenharia social

Futuro

- Novo design nmap stack fingerprinting
- nmap com service + stack fingerprinting integrados para resultados mais consistentes (nmap 3.90)

Técnicas Anti-fingerprinting

- Desabilitar os banners :-)
- Fingerprint scrubber e outros projetos
- Falsos fingerprints

Para saber mais...

- Commer, Douglas E., Internetworking with TCP/IP, 4th edition
- Fyodor, Remote OS detection via TCP/IP Stack Fingerprinting (incluindo tradução em espanhol e português): http://www.insecure.org/nmap/nmap-fingerprinting-article.html
- Fyodor, Nmap Version Scanning: http://www.insecure.org/nmap/versionscan.html
- Fyodor, message to nmap-dev mailing list: http://seclists.org/lists/nmap-dev/2005/Jul-Sep/0039.html
- Fyodor, message to nmap-hackers mailing list: http://seclists.org/lists/nmap-hackers/2005/Jul-Sep/0002.html
- Smart, Matthew et all, Defeating TCP/IP Stack Fingerprinting, Proceedings of the 9th USENIX Security Simposium, 2000
- David Barroso Berrueta, A practical approach for defeating Nmap OS-fingerprinting, http://voodoo.somoslopeor.com/papers/nmap.html
- McDanel, Bret, TCP Timestamping and Remotely gathering uptime information, 2001, Bugtraq Archives, http://www.securityfocus.com/archive/1/168637