

Segurança de Sistemas

Miguel Frade - Nuno Rasteiro

Departamento de Engenharia Informática
Instituto Politécnico de Leiria

Setembro de 2019

- Serviços de Transmissão de dados
 - Serviços
 - Transmissão de dados
 - WireShark

Serviços

- Todos os dispositivos de rede ativos fornecem serviços. Por exemplo:
 - acesso remoto para configuração
 - telnet
- No caso dos computadores e dos encaminhadores existem muitos serviços ativos por omissão, muitos deles nem sequer são usados
- Muitos desses serviços apresentam vulnerabilidades

Serviços

- Os serviços usam portos TCP ou UDP
- Como verificar localmente quais os serviços activos?
- comando **netstat**
- este comando permite-nos listar quais os portos que estão em escuta e quais os portos que contém ligações
- é o método mais eficaz e fiável, mas mais moroso
- Instalar o net-tools `sudo apt install net-tools`
- Netstat actualmente substituído pelo `ss`

```
nr@nr-VirtualBox: ~  
nr@nr-VirtualBox:~$ netstat -at  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN  
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN  
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN  
nr@nr-VirtualBox:~$
```

Serviços

- ◆ Os computadores com o Windows normalmente são mais vulneráveis porque após a instalação contêm mais serviços ativos.
 - Neste exemplo o Windows 10 tem serviços **TCP** ativos. Quantos serviços ativos (modo LISTENING) tem o vosso S.O?
 - Qual é o número máximo de portos que podem existir?

```
C:\Users\nr>netstat -a -p tcp
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49669	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49686	DESKTOP-NL9RR89:0	LISTENING
TCP	0.0.0.0:49687	DESKTOP-NL9RR89:0	LISTENING
TCP	10.200.30.186:139	DESKTOP-NL9RR89:0	LISTENING
TCP	10.200.30.186:64566	40.67.251.132:https	ESTABLISHED
TCP	10.200.30.186:64613	13.68.168.63:https	ESTABLISHED
TCP	10.200.30.186:65051	mad01s26-in-f14:https	ESTABLISHED
TCP	10.200.30.186:65065	13.107.6.171:https	ESTABLISHED
TCP	10.200.30.186:65079	52.109.76.92:https	ESTABLISHED
TCP	10.200.30.186:65316	ec2-52-10-254-61:https	ESTABLISHED
TCP	10.200.30.186:65375	muc03s14-in-f3:https	ESTABLISHED
TCP	10.200.30.186:65400	ws-in-f189:https	ESTABLISHED
TCP	10.200.30.186:65484	52.114.132.21:https	TIME_WAIT
TCP	10.200.30.186:65494	13.107.136.9:https	TIME_WAIT
TCP	10.200.30.186:65495	52.109.76.8:https	TIME_WAIT
TCP	10.200.30.186:65499	13.107.21.200:https	ESTABLISHED
TCP	10.200.30.186:65500	muc03s14-in-f5:https	ESTABLISHED
TCP	10.200.30.186:65501	muc03s14-in-f3:http	ESTABLISHED
TCP	10.200.30.186:65502	185.63.144.1:https	ESTABLISHED
TCP	10.200.30.186:65503	93.184.220.29:http	ESTABLISHED
TCP	10.200.30.186:65504	131.253.33.254:https	ESTABLISHED
TCP	10.200.30.186:65505	13.107.136.254:https	ESTABLISHED
TCP	10.200.30.186:65506	204.79.197.222:https	ESTABLISHED

Serviços

- ◆ Nos serviços conhecidos aparece o nome em vez do número do porto
- ◆ No ficheiro `/etc/services` estão listados os nomes dos serviços mais conhecidos e respetivos portos

```
ftp-data      20/tcp
ftp           21/tcp
fsp           21/udp      fspd
ssh           22/tcp      # SSH Remote Login Protocol
telnet        23/tcp
smtp          25/tcp      mail
time          37/tcp      timserver
time          37/udp      timserver
rlp           39/udp      resource    # resource location
nameserver    42/tcp      name        # IEN 116
whois         43/tcp      nickname
tacacs        49/tcp      # Login Host Protocol (TACACS)
```

Serviços

- ◆ Quais são os portos dos seguintes serviços?
 - epmap
 - microsoft-ds
 - ssh
 - domain
 - Netbios-ssn
 - X11

Serviços

- ◆ Só alguns dos serviços registados pela Internet Assigned Numbers Authority (IANA <http://www.iana.org/>) é que estão listados no ficheiro **/etc/services**
- ◆ Para obter uma listagem completa e actualizada consultar:
 - <http://www.iana.org/assignments/port-numbers>
- ◆ A gama de portos está dividida [RFC6335]
 - De 0 a 1023 são os portos do sistema (ou bem conhecidos)
 - De 1024 a 49151 são os portos registados
 - De 49152 a 65535 são os portos dinâmicos ou efémeros
- ◆ Qual o nome dos serviços associado aos portos
 - 2087
 - 24922

- ◆ Como verificar remotamente quais os serviços ativos?
 - Com um *scanner* de portos como o **nmap**
 - Envia pacotes para sondar os portos abertos noutro dispositivo de rede e tenta determinar o S.O.
 - Para algumas opções é necessário ter permissões de *root*
 - É possível determinar os portos abertos num único dispositivo ou numa rede inteira
 - Este método é menos fiável porque os pacotes podem ser filtrados

Serviços

- Cenário:
 - Instalar Oracle Virtualbox
 - Configurar rede Host-Only Ethernet adapter
 - Importar a VM fornecida
 - Ter outra VM com Ubuntu com 2 adaptadores de rede

Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		<input checked="" type="checkbox"/> Enable

Adapter	DHCP Server
<input type="radio"/> Configure Adapter Automatically <input checked="" type="radio"/> Configure Adapter Manually	<input checked="" type="checkbox"/> Enable Server Server Address: 192.168.56.100 Server Mask: 255.255.255.0 Lower Address Bound: 192.168.56.101 Upper Address Bound: 192.168.56.254

IPv4 Address:	192.168.56.1
IPv4 Network Mask:	255.255.255.0

Serviços

◆ Para obter permissões de *root* escrever o comando *sudo* antes do comando desejado
nmap -sP 192.168.56.0/24

- Quantos Hosts estão activos?
 - Quantos portos abertos tem a máquina 192.168.56.101 e que serviços tem instalado que têm instalado?
- sudo nmap -sS 192.168.56.101*

Nmap avançado depois do intervalo

```
nr@nr-VirtualBox:~$ nmap -sP 192.168.56.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 21:41 WEST
Nmap scan report for 192.168.56.101
Host is up (0.00066s latency).
Nmap scan report for nr-VirtualBox (192.168.56.102)
Host is up (0.00026s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 17.79 seconds
nr@nr-VirtualBox:~$ sudo nmap -sS 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 21:46 WEST
Nmap scan report for 192.168.56.101
Host is up (0.00073s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  snmp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:21:6B:AC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
nr@nr-VirtualBox:~$
```

Serviços

◆ Funcionamento do **nmap**

- Por omissão o nmap não verifica todos os 65535 portos
- verifica apenas uma lista de 1663 portos correspondentes a serviços conhecidos
- Por isso podem existir portos abertos que não são detetados com um *scan* normal do nmap
- mas podemos forçá-lo a percorrer todos os portos ou apenas uma parcela:
 - `nmap -sS -p 1-3000 192.168.56.101`

Transmissão de dados

- ◆ Muitos serviços de rede transmitem os dados em claro ou com mecanismos de protecção fracos
 - o que permite a qualquer pessoa lê-los desde que tenha as ferramentas certas
- ◆ 33 exemplos de protocolos ou aplicações que transmitem os dados em claro ou com mecanismos de protecção fracos:
 - FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP
 - IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP
 - MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS
 - IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker
 - Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB
 - Oracle SQL*Net, Sybase, Microsoft SQL auth info.

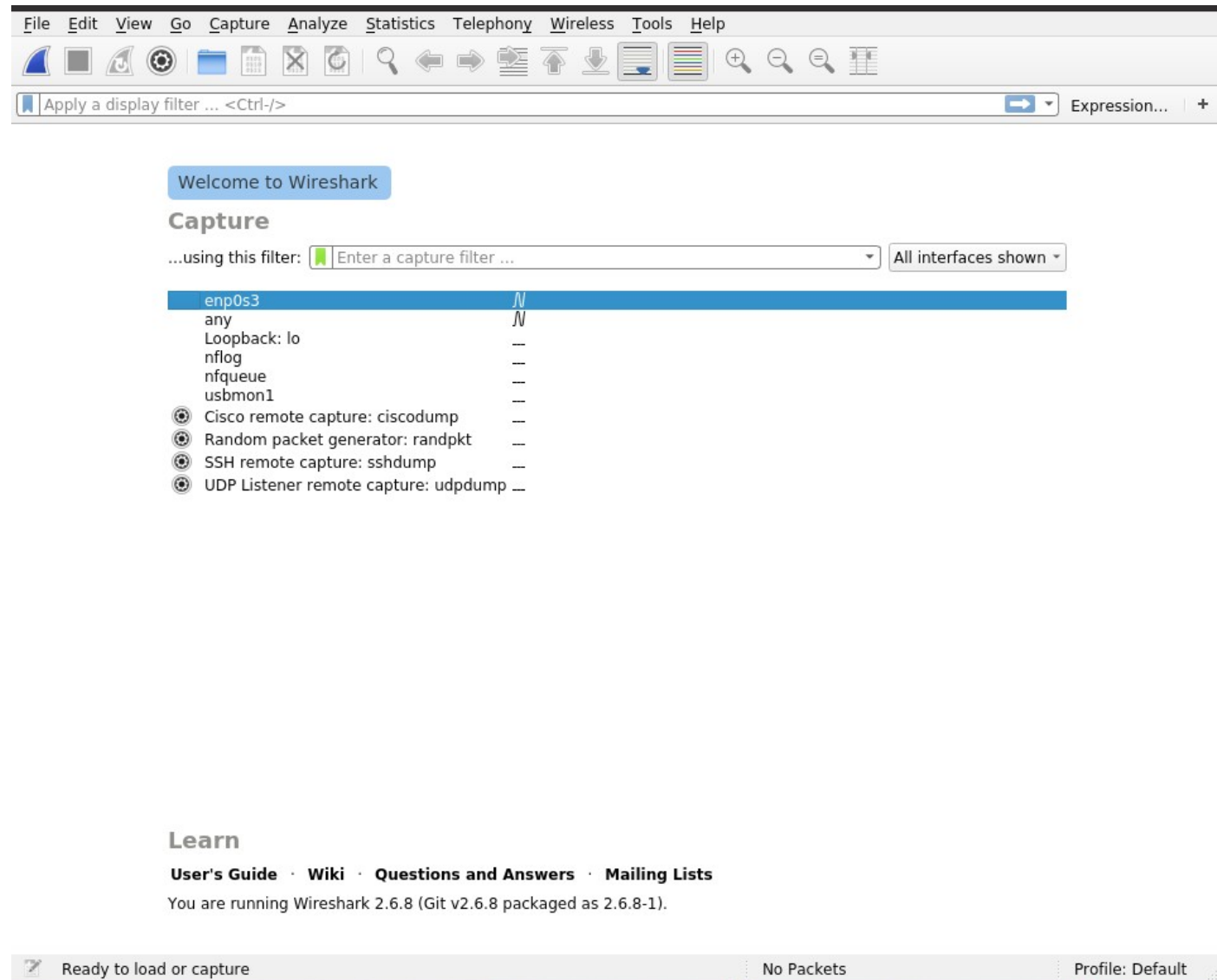
Transmissão de dados

◆ Analisador de protocolos

- Serve para fazer auditorias às redes informáticas
- Se usado por pessoas mal intencionadas, também pode ser usado para capturar dados que circulem na rede em claro
- O analisador é introduzido na rede normalmente com a placa de rede em modo promíscuo (só com permissões de *root*)
- Exemplo de um analisador *OpenSource*: **Wireshark**
- Comando para instalar o wireshark
- **`sudo apt install wireshark-qt`**



Wireshark



Wireshark

- ◆ Podemos filtrar o que queremos capturar
- ◆ Para capturar o tráfego do FTP: **FTP**

Wireshark interface showing a capture of FTP traffic. The packet list on the left shows 56 packets, with packet 9 selected. The packet details on the right show the structure of the selected packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and File Transfer Protocol (FTP). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
5	2.936322343	192.168.56.101	192.168.56.102	FTP	86	Response: 220 (vsFTPd 2.3.4)
9	10.957369340	192.168.56.102	192.168.56.101	FTP	81	Request: USER msfadmin
11	10.957813386	192.168.56.101	192.168.56.102	FTP	100	Response: 331 Please specify the password.
13	21.031616568	192.168.56.102	192.168.56.101	FTP	81	Request: PASS msfadmin
14	21.034353478	192.168.56.101	192.168.56.102	FTP	89	Response: 230 Login successful.
16	21.034468657	192.168.56.102	192.168.56.101	FTP	72	Request: SYST
17	21.034821881	192.168.56.101	192.168.56.102	FTP	85	Response: 215 UNIX Type: L8
19	26.673864583	192.168.56.102	192.168.56.101	FTP	74	Request: TYPE A
20	26.674211594	192.168.56.101	192.168.56.102	FTP	96	Response: 200 Switching to ASCII mode.
23	30.583072923	192.168.56.102	192.168.56.101	FTP	71	Request: PWD
24	30.583502747	192.168.56.101	192.168.56.102	FTP	88	Response: 257 "/home/msfadmin"
26	32.436100551	192.168.56.102	192.168.56.101	FTP	94	Request: PORT 192,168,56,102,184,21
27	32.436528070	192.168.56.101	192.168.56.102	FTP	117	Response: 200 PORT command successful. Consider using PASV.
29	32.436598171	192.168.56.102	192.168.56.101	FTP	72	Request: LIST
33	32.437267478	192.168.56.101	192.168.56.102	FTP	105	Response: 150 Here comes the directory listing.
39	32.438668072	192.168.56.101	192.168.56.102	FTP	90	Response: 226 Directory send OK.
41	49.469898231	192.168.56.102	192.168.56.101	FTP	95	Request: PORT 192,168,56,102,225,165
42	49.470400189	192.168.56.101	192.168.56.102	FTP	117	Response: 200 PORT command successful. Consider using PASV.
43	49.470488654	192.168.56.102	192.168.56.101	FTP	78	Request: RETR teste
47	49.471427603	192.168.56.101	192.168.56.102	FTP	129	Response: 150 Opening BINARY mode data connection for teste (19 bytes).
53	49.472394472	192.168.56.101	192.168.56.102	FTP	90	Response: 226 Transfer complete.
55	54.134175711	192.168.56.102	192.168.56.101	FTP	72	Request: QUIT
56	54.134631059	192.168.56.101	192.168.56.102	FTP	80	Response: 221 Goodbye.

Frame 9: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Ethernet II, Src: PcsCompu_eb:7d:d6 (08:00:27:eb:7d:d6), Dst: PcsCompu_21:6b:ac (08:00:27:21:6b:ac)
Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.101
Transmission Control Protocol, Src Port: 48940, Dst Port: 21, Seq: 1, Ack: 21, Len: 15
File Transfer Protocol (FTP)
[Current working directory:]

0000 08 00 27 21 6b ac 08 00 27 eb 7d d6 08 00 45 10 ..'lk...'}...E
0010 00 43 cb d7 40 00 40 06 7c b1 c0 a8 38 66 c0 a8 .C..@.@. |...8f..
0020 38 65 bf 2c 00 15 42 d0 cd c3 29 29 ee 01 80 18 8e, .B. .))....
0030 01 f6 f2 51 00 00 01 01 08 0a 02 25 d5 bf 00 05 ...Q.....%....
0040 37 11 55 53 45 52 20 6d 73 66 61 64 6d 69 6e 0d 7-USER m sfadmin..

Transmission Control Protocol (tcp), 32 bytes

Packets: 60 · Displayed: 23 (38.3%) · Dropped: 0

Wireshark

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes. The top pane shows a list of captured packets, with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 66), including the HTTP request and the form data. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
8	17.978070279	192.168.56.102	192.168.56.101	HTTP	388	GET / HTTP/1.1
10	17.990480834	192.168.56.101	192.168.56.102	HTTP	1190	HTTP/1.1 200 OK (text/html)
18	32.686609442	192.168.56.102	192.168.56.101	HTTP	432	GET /phpMyAdmin/ HTTP/1.1
24	32.790240397	192.168.56.101	192.168.56.102	HTTP	71	HTTP/1.1 200 OK (text/html)
26	32.827272435	192.168.56.102	192.168.56.101	HTTP	610	GET /phpMyAdmin/phpmyadmin.css.php?lang=en-utf-8&convcharset=utf-8&token=8bbddb4da4f830b9b7237829960dd4c
31	32.828322552	192.168.56.102	192.168.56.101	HTTP	496	GET /phpMyAdmin/print.css HTTP/1.1
33	32.829276342	192.168.56.101	192.168.56.102	HTTP	1426	HTTP/1.1 200 OK (text/css)
43	32.877342876	192.168.56.101	192.168.56.102	HTTP	71	HTTP/1.1 200 OK (text/css)
44	32.877494817	192.168.56.102	192.168.56.101	HTTP	517	GET /phpMyAdmin/themes/original/img/logo_right.png HTTP/1.1
47	32.878598471	192.168.56.101	192.168.56.102	HTTP	1678	HTTP/1.1 200 OK (PNG)
49	32.900229031	192.168.56.102	192.168.56.101	HTTP	470	GET /phpMyAdmin/favicon.ico HTTP/1.1
51	32.902293798	192.168.56.102	192.168.56.101	HTTP	656	GET /phpMyAdmin/themes/original/img/s_warn.png HTTP/1.1
55	32.903156659	192.168.56.102	192.168.56.101	HTTP	658	GET /phpMyAdmin/themes/original/img/s_notice.png HTTP/1.1
56	32.903187142	192.168.56.101	192.168.56.102	HTTP	623	HTTP/1.1 200 OK (PNG)
58	32.904197721	192.168.56.101	192.168.56.102	HTTP	609	HTTP/1.1 200 OK (PNG)
62	32.925337220	192.168.56.101	192.168.56.102	HTTP	9134	HTTP/1.1 200 OK (image/x-icon)
66	41.039069427	192.168.56.102	192.168.56.101	HTTP	935	POST /phpMyAdmin/index.php HTTP/1.1 (application/x-www-form-urlencoded)
68	41.112596151	192.168.56.101	192.168.56.102	HTTP	1045	HTTP/1.1 302 Found
69	41.115745475	192.168.56.102	192.168.56.101	HTTP	646	GET /phpMyAdmin/index.php?token=8bbddb4da4f830b9b7237829960dd4d9 HTTP/1.1
106	41.265093789	192.168.56.101	192.168.56.102	HTTP	71	HTTP/1.1 200 OK (text/html)
108	41.302721114	192.168.56.102	192.168.56.101	HTTP	674	GET /phpMyAdmin/phpmyadmin.css.php?token=8bbddb4da4f830b9b7237829960dd4d9&js_frame=right&nocache=2457687
112	41.349896138	192.168.56.101	192.168.56.102	HTTP	8905	HTTP/1.1 200 OK (text/css)
114	41.364565235	192.168.56.102	192.168.56.101	HTTP	633	GET /phpMyAdmin/themes/original/img/s_error.png HTTP/1.1
116	41.365517245	192.168.56.101	192.168.56.102	HTTP	624	HTTP/1.1 200 OK (PNG)

[HTTP request 5/8]
[\[Prev request in frame: 49\]](#)
[\[Response in frame: 68\]](#)
[\[Next request in frame: 69\]](#)
File Data: 273 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "phpMyAdmin" = "d1c9b782ddcadafb05579c315435add8a0fb0c0f"
- Form item: "phpMyAdmin" = "d1c9b782ddcadafb05579c315435add8a0fb0c0f"
- Form item: "pma_username" = "admin"
- Form item: "pma_password" = "admin"
- Form item: "server" = "1"
- Form item: "phpMyAdmin" = "d1c9b782ddcadafb05579c315435add8a0fb0c0f"
- Form item: "lang" = "en-utf-8"

0310 26 70 6d 61 5f 70 61 73 73 77 6f 72 64 3d 61 64 &pma_password=ad
0320 6d 69 6e 26 73 65 72 76 65 72 3d 31 26 70 68 70 min&server=1&php
0330 4d 79 41 64 6d 69 6e 3d 64 31 63 39 62 37 38 32 MyAdmin= d1c9b782
0340 64 64 63 61 64 61 66 62 30 35 35 37 39 63 33 31 ddcadafb 05579c31
0350 35 34 33 35 61 64 64 38 61 30 66 62 30 63 30 66 5435add8 a0fb0c0f

Text item (text), 19 bytes

Packets: 182 · Displayed: 28 (15.4%)

Wireshark

◆ Exercício 1

- No Wireshark coloquem um filtro para
 - tcp port 23
 - Iniciem a captura de pacotes
- Na linha de comando fazer
 - telnet 192.168.56.101
 - No *login* colocar **msfadmin** e na *password* escrevam **msfadmin**
 - Executem o comando **ls /etc**
- Parar a captura de pacotes
- Procurar no Wireshark a informação que escreveram
- **O telnet é seguro?**

Wireshark

◆ Exercício 2

- No Wireshark coloquem um filtro para
 - Tcp port 22
- Iniciem a captura
- Na linha de comando fazer
 - `ssh msfadmin@192.168.56.101` e na *password* escrever `msfadmin`
 - Depois executem o comando `ls /etc`
- Parar a captura de pacotes
- Procurar no wireshark a informação que escreveram
- **O que é que se consegue ler?**

Conclusões

- ◆ Quando os protocolos da Internet foram desenvolvidos não existiam preocupações com a segurança, por isso existem muitos protocolos que não são seguros
- ◆ Os utilizadores devem ter muito cuidado quando usam as redes informáticas principalmente a Internet e procurar usar aplicações que usam protocolos seguros sempre que quiser transmitir dados sensíveis
- ◆ Mesmo nos sítios da Internet que usam protocolos seguros, como o HTTPS, é preciso ter cuidado e procurar saber a idoneidade do dono do site, porque este consegue decifrar a informação