Segurança de Sistemas

Miguel Frade - Nuno Rasteiro

Departamento de Engenharia Informática
Instituto Politécnico de Leiria

Setembro de 2019

Segurança de Sistemas

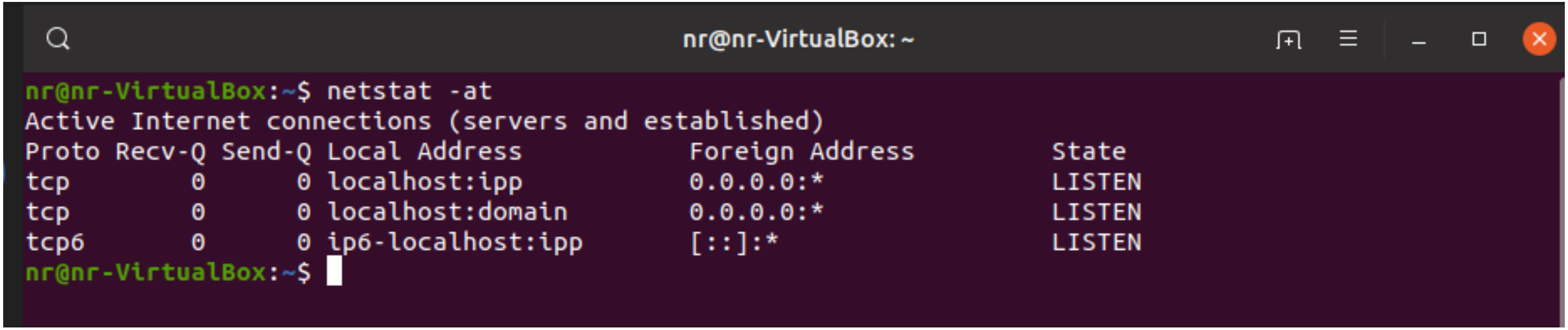
- Serviços de Transmissão de dados
  - Serviços
  - Transmissão de dados
  - WireShark

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

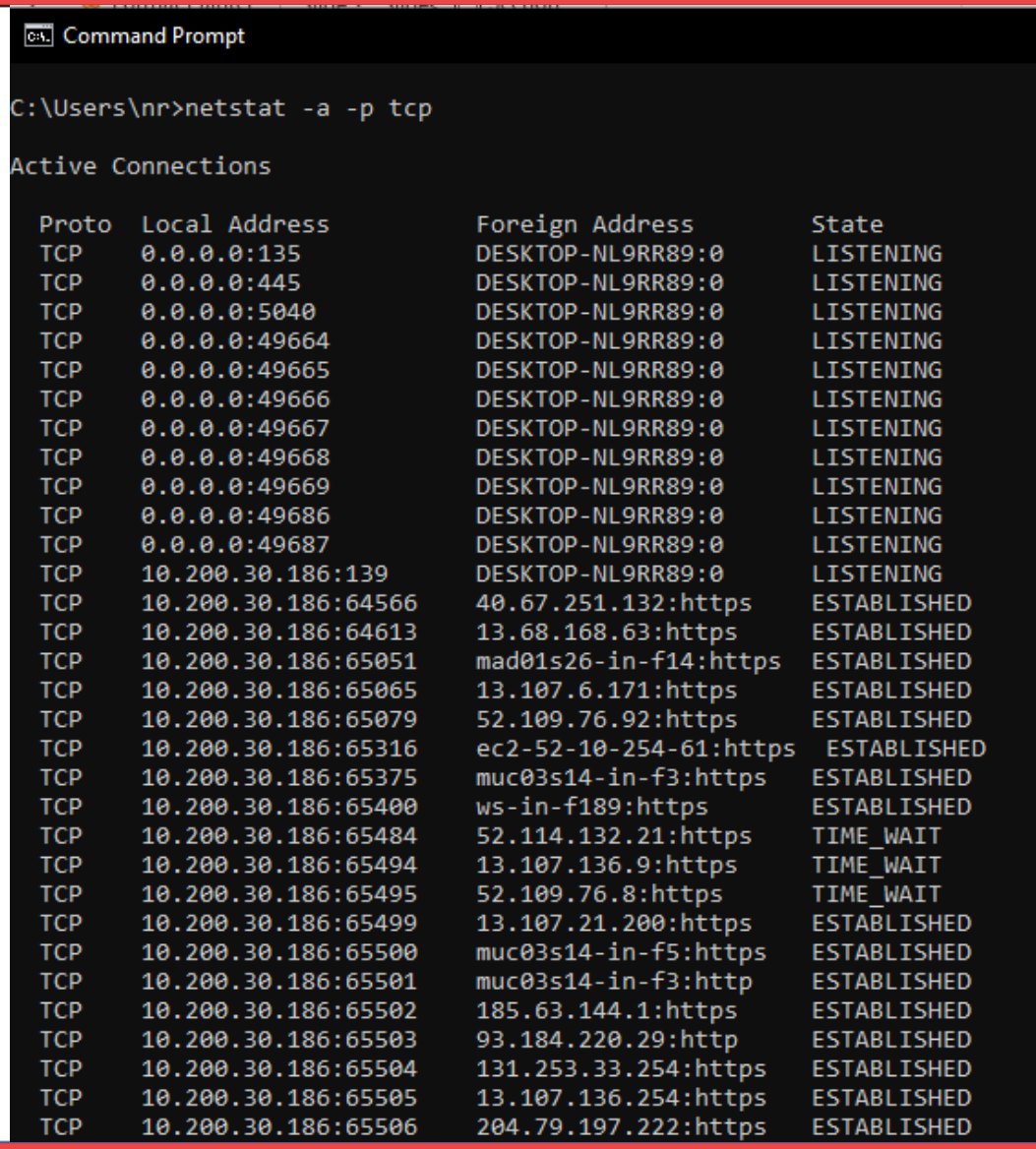
Serviços

- 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 substituido pelo ss



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?



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          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
```

Serviços

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

Serviços

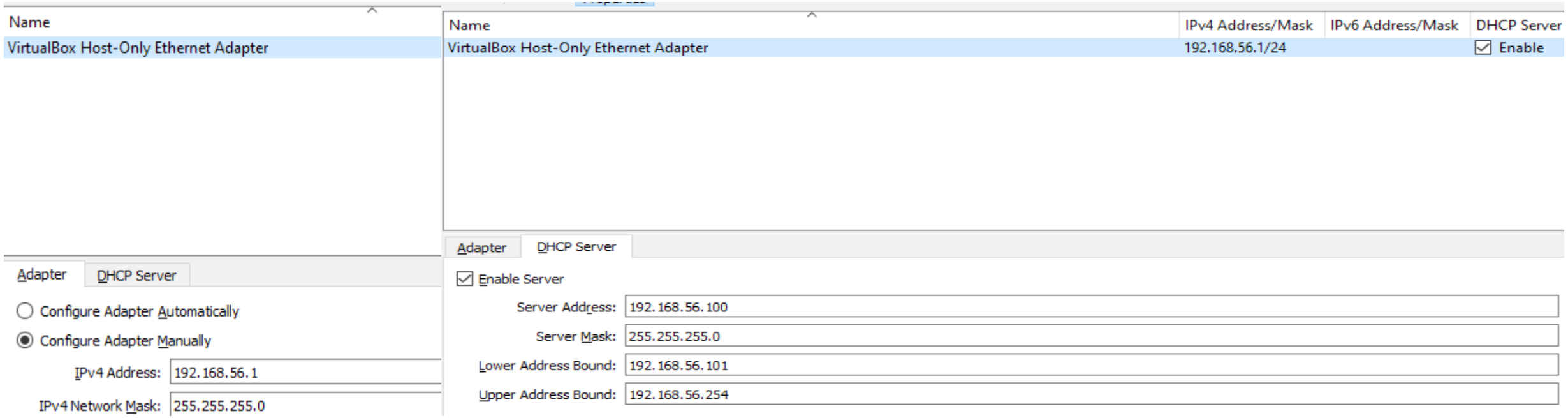
- Só alguns dos serviços registados pela Internet Assigned Numbers Authority (IANA http://www.iana.org/) é que estão listados no ficheiro **/etc/services**
- Para obter uma listagem completa e actualizada consultar:
  - http://www.iana.org/assignments/port-numbers
- A gama de portos está dividida [RFC6335]
  - 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

Serviços

- 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



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 istalado 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  smtp
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 forcá-lo a percorrer todos os portos ou apenas uma parcela:
    - nmap –sS –p 1-3000 192.168.56.101

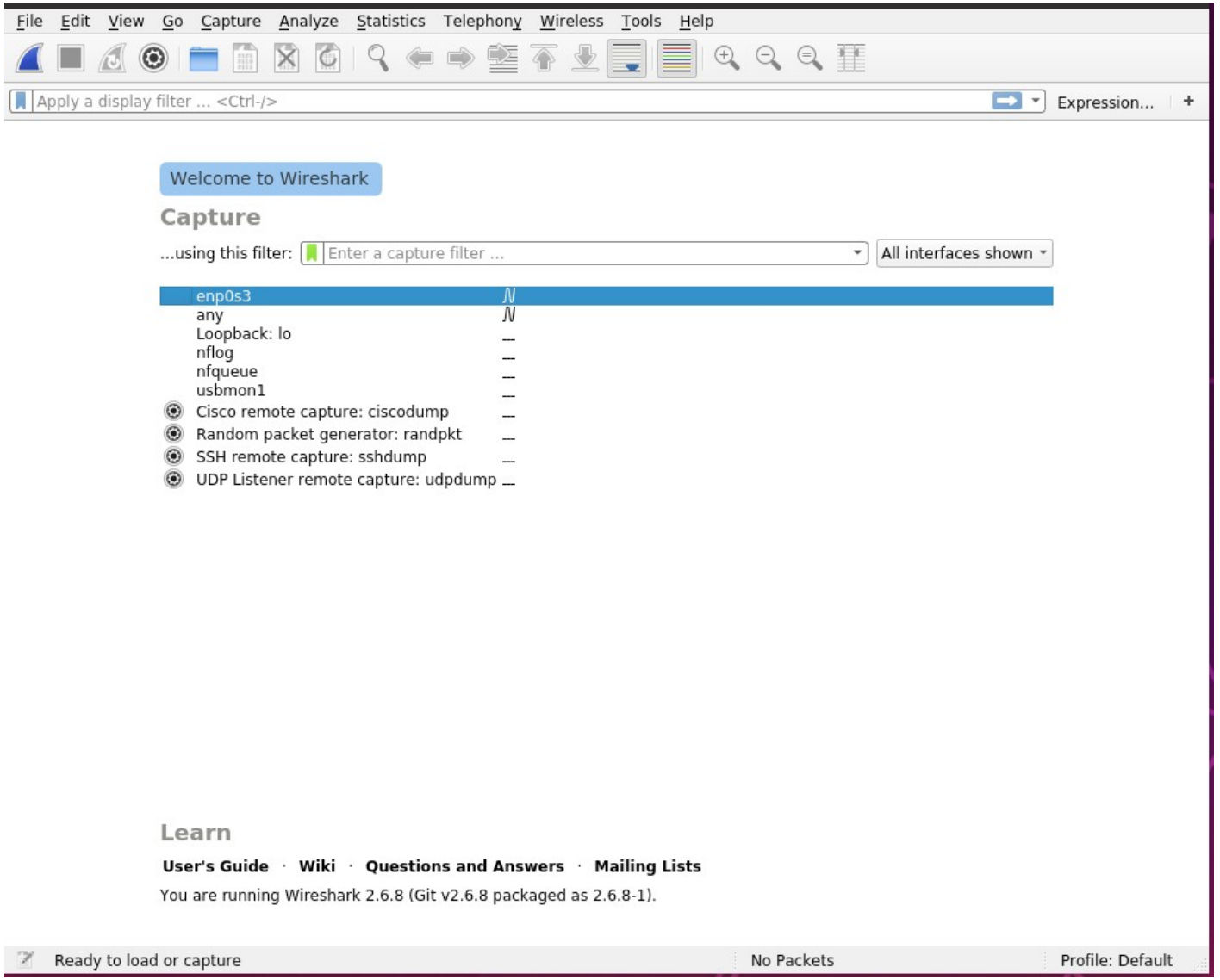
Transmissão de dados

- 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

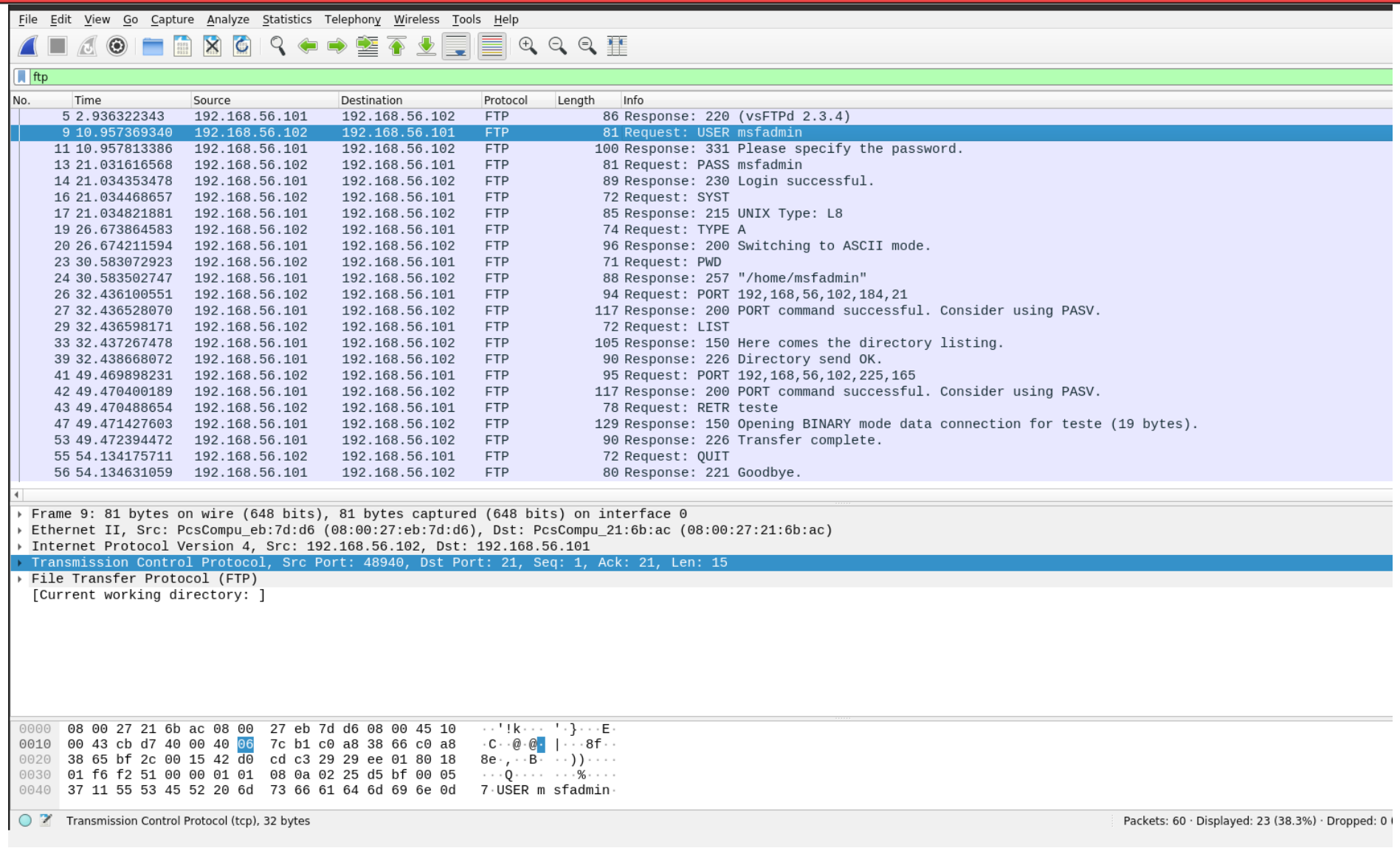
- Analisador de protocolos
  - Serve para fazer auditorias às redes informáticas
  - Se usado por pessoas mal intencionadas, também pode ser usado para capturar dados que circulem na rede em claro
  - O analisador é introduzido na rede normalmente com a placa de rede em modo promíscuo (só com permissões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

Wireshark

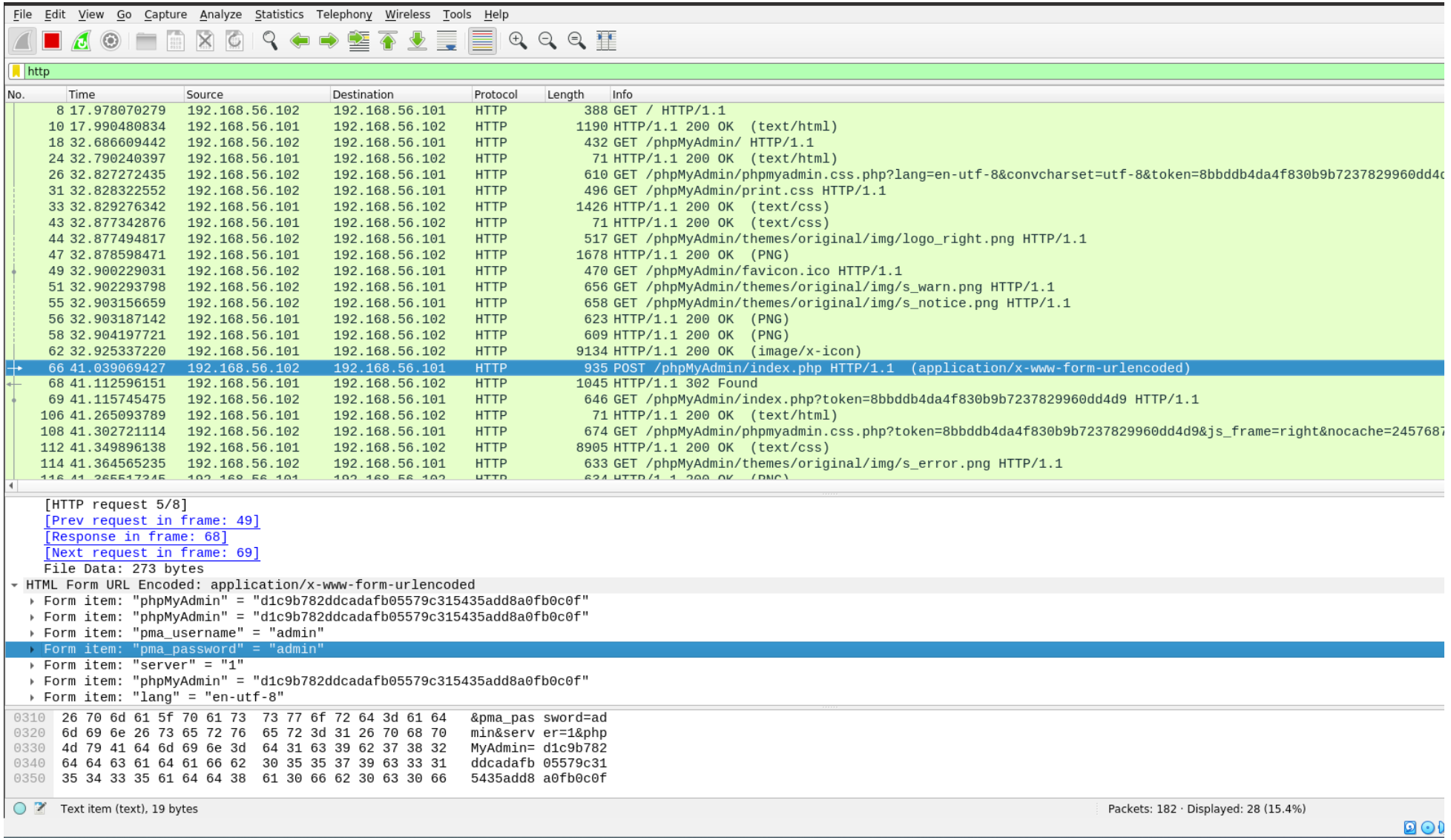

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.8 (Git v2.6.8 packaged as 2.6.8-1).
Ready to load or capture
No Packets
Profile: Default

Wireshark

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



Wireshark


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
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=8bbddb4da4f830b9b7237829960dd4
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
[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_pas sword=ad
0320 6d 69 6e 26 73 65 72 76 65 72 3d 31 26 70 68 70 min&serv er=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