



Serviços e Transmissão de Dados

Curso de Engenharia Informática 3º ano – Segurança de Sistema

Software necessário

- Firefox (alguns exercícios com certificados digitais não funcionam no Chrome / some exercises won't work in Chrome)
- [nmap](#)
- wireshark
- openssh-server
- keepassx
- steghide
- thunderbird
- gns3

UBUNTU /DEBIAN

- Como instalar / how to install:

1. # atualizar a base de dados do software linux / update linux software database
`sudo apt-get update`
2. # instalar todas as atualizações do Linux / install all Linux updates
`sudo apt-get dist-upgraded`
3. # instalar o software necessário para a UC / install all required software for this class
`sudo apt-get install firefox nmap wireshark openssh-server keepassx steghide thunderbird gns3`

Serviços (1)

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

Serviços (2)

- Os serviços usam portos TCP ou UDP
- Como verificar localmente quais os serviços ativos?
 - 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

```
ssuser@SSServer:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 SSServer:59650         archive.ubuntumirr:http TIME_WAIT
tcp6       0      0 [::]:1716              [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp      [::]:*                  LISTEN
```

Serviços (3)

- Os computadores com o Windows normalmente são mais vulneráveis porque após a instalação contêm mais serviços ativos.
 - Neste exemplo o Windows 10 tem 8 serviços TCP ativos. Quantos serviços ativos (modo LISTENING) tem o vosso S.O?
 - Qual é o número máximo de portos que podem existir?

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

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:445              DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:5040             DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:5357             DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:7680             DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:49664            DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:49665            DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:49666            DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:49667            DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:49668            DESKTOP-TVKC59C:0      LISTENING
TCP   0.0.0.0:49669            DESKTOP-TVKC59C:0      LISTENING
TCP   192.168.200.31:139       DESKTOP-TVKC59C:0      LISTENING
TCP   192.168.200.31:49177    192.168.200.1:domain    TIME_WAIT
TCP   192.168.200.31:49178    8.238.65.126:http       TIME_WAIT
TCP   192.168.200.31:49829    192.168.200.1:domain    TIME_WAIT
TCP   192.168.200.31:49830    52.114.77.34:https      TIME_WAIT
TCP   192.168.200.31:49891    192.168.200.1:domain    TIME_WAIT
TCP   192.168.200.31:49893    8.247.215.126:http      ESTABLISHED
TCP   192.168.200.31:50742    192.168.200.1:domain    TIME_WAIT
TCP   192.168.200.31:51275    192.168.200.1:domain    TIME_WAIT
TCP   192.168.200.31:51276    52.114.75.78:https      TIME_WAIT
TCP   192.168.200.31:51281    20.49.150.241:https     TIME_WAIT
TCP   192.168.200.31:51282    13.107.5.88:https       ESTABLISHED
```

Serviços (4)

- 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

```
- : sudo edit — Konsole
File Edit View Bookmarks Settings Help
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux      1/tcp          # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp          sink null
discard     9/udp          sink null
systat      11/tcp         users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd        17/tcp          quote
chargen     19/tcp         ttytst source
chargen     19/udp         ttytst source
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp          fsp
ssh         22/tcp         # SSH Remote Login Protocol
telnet      23/tcp
smtp        25/tcp          mail
```

Serviços (5)

- Quais são os portos dos seguintes serviços?
 - epmap
 - microsoft-ds
 - ssh
 - domain
 - netbios-ssn
 - x11

Serviços (6)

- 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 (7)

- Como verificar remotamente quais os serviços activos?
 - Com um scanner de portos como o nmap
 - Envia pacotes para sondar os portos abertos noutra 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 (8)

- Para obter permissões de root escrever o comando sudo antes do comando desejado: sudo nmap -sS 192.168.226.1
 - Quantos portos abertos tem as máquinas e qual é o sistema operativo que têm instalado?
 - 192.168.226.1 192.168.226.<colega do lado>

Serviços (9)

- 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 detectados com um scan normal do nmap mas podemos forçá-lo a percorrer todos os portos ou apenas uma parcela:
 - `nmap -sS -p 1-3000 192.168.226.9`

Transmissão de dados (2)

- 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 freeware: Ethereal/Wireshark

Transmissão de dados (2)

- 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 freeware: Ethereal/Wireshark