NETCAT

Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking

Definição

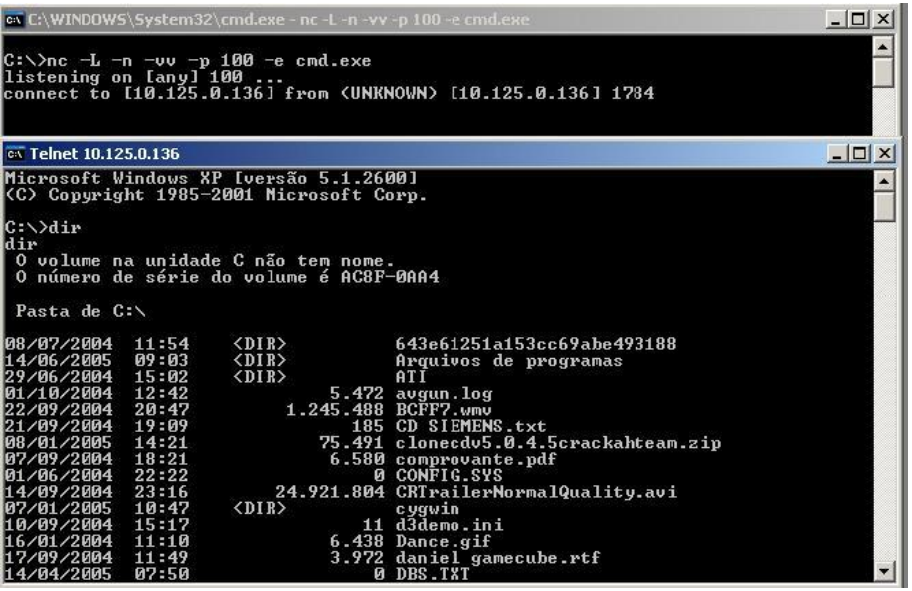
- O Netcat é ainda hoje um dos programas mais úteis para ser utilizado como auxílio em um Penetration test. Chamado de “canivete suíço”do TCP/IP, ele permite agir tanto como cliente quanto como servidor.
- Utilizando o netcat como um backdoor, podemos conseguir um bind shell, no qual abrimos uma porta no sistema alvo para explorarmos, ou reverse shell, na qual o usuário se conecta de volta ao atacante.

NetCat

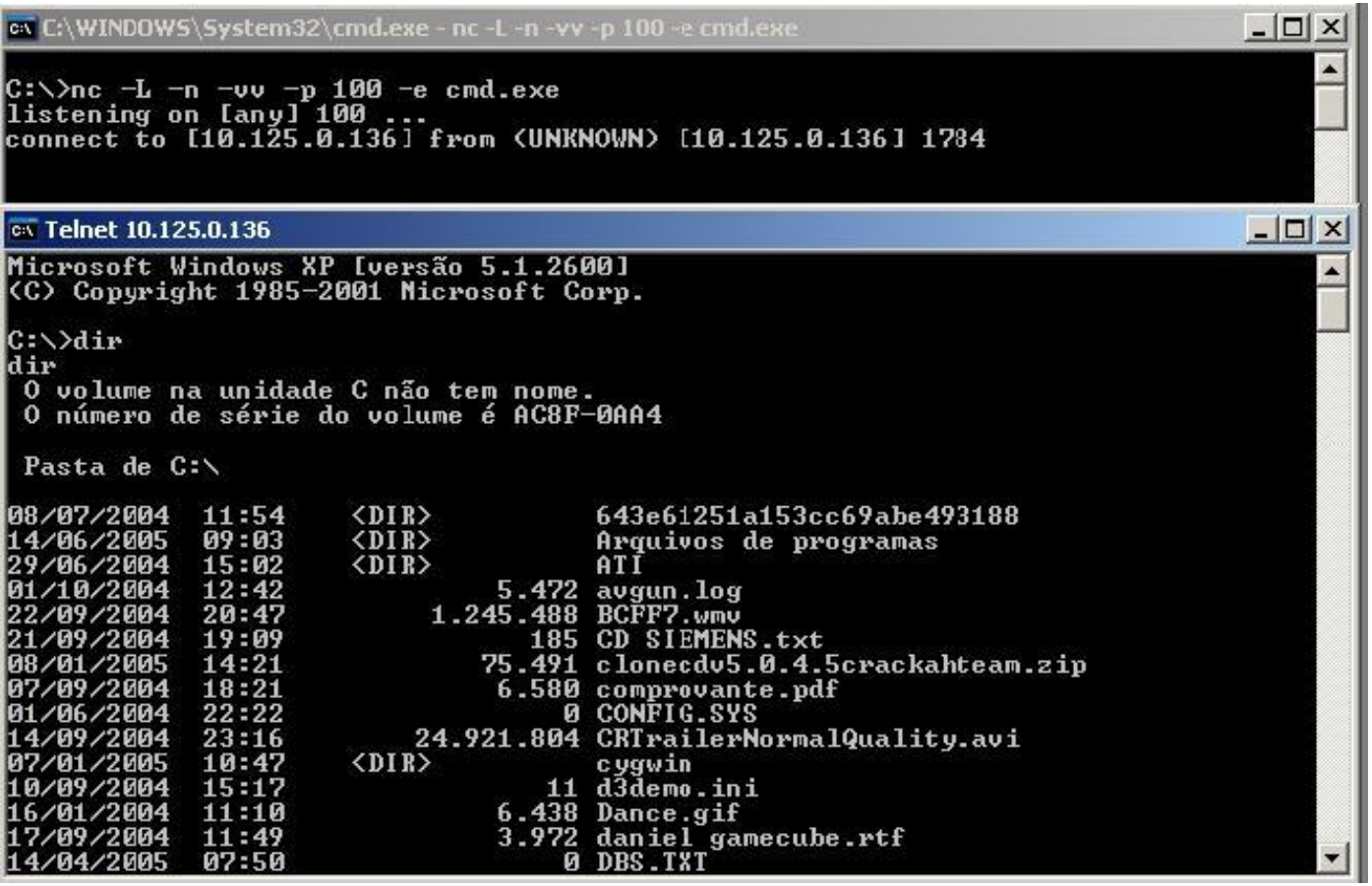
```
C:\WINDOWS\System32\cmd.exe
C:\>nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

- “Canivete suíço do TCP/IP”
- Cliente ou Servidor
- Conexão direta (bind)
- Conexão reversa
- Possui versão para vários sistemas: Linux, Windows, FreeBSD, etc.

Definição



- Utilizamos a opção –l quando queremos que o Netcat atue como servidor. Se essa opção não for usada, o modo utilizado será cliente.
- A opção –p define a porta que será utilizada
- A opção –e define a aplicação anexa à porta



Netcat

Conexão direta

C:\WINDOWS\System32\cmd.exe - nc -L -n -p 53 -vv

```
C:\>nc -L -n -p 53 -vv
listening on [any] 53 ...
connect to [10.125.0.136] from (UNKNOWN) [10.125.0.136] 1954
dir
ver
```

C:\WINDOWS\System32\cmd.exe - nc -L -n -p 79 -vv

```
26/12/2004  14:12    <DIR>          tempo
02/12/2004  12:41    <DIR>          Teste
14/04/2005  16:50           481.959 teste.3gp
11/02/2005  15:19               143 teste.htm
05/09/2004  17:31         2.528.103 uncut-stage.mov
05/09/2004  19:22         3.709.104 Usage.mpeg
01/10/2004  12:42                 0 VDM32A.tmp
27/04/2005  08:34           837.881 VideoEditor.log
13/06/2005  19:37    <DIR>          WINDOWS
01/07/2004  15:19    <DIR>          WUTemp
              63 arquivo(s)     82.236.756 bytes
              31 pasta(s)  7.309.213.696 bytes disponíveis

C:\>ver

Microsoft Windows XP [versão 5.1.2600]

C:\>_
```

Netcat

Conexão reversa