Five Steps to Improve Internal Network Security

Chattanooga ISSA

ASG Consulting

Find Me

AverageSecurityGuy.info

@averagesecguy

stephen@averagesecurityguy.info

github.com/averagesecurityguy

ChattSec.org

Why?

The methodical workflow honed by many state-affiliated actors of setting up a backdoor to gain initial access, and **then using shell services to move laterally through the organization**, has proven to be successful against victims of all types and sizes.

2013 Data Breach Investigations Report p.36

ASG Consulting

What?

1. Eliminate LanMan Hashes
2. Remove Shared Local Admin Passwords
3. Lockdown Open File Shares
4. Replace Default/Blank Passwords
5. Lockdown Remote Desktop Protocol

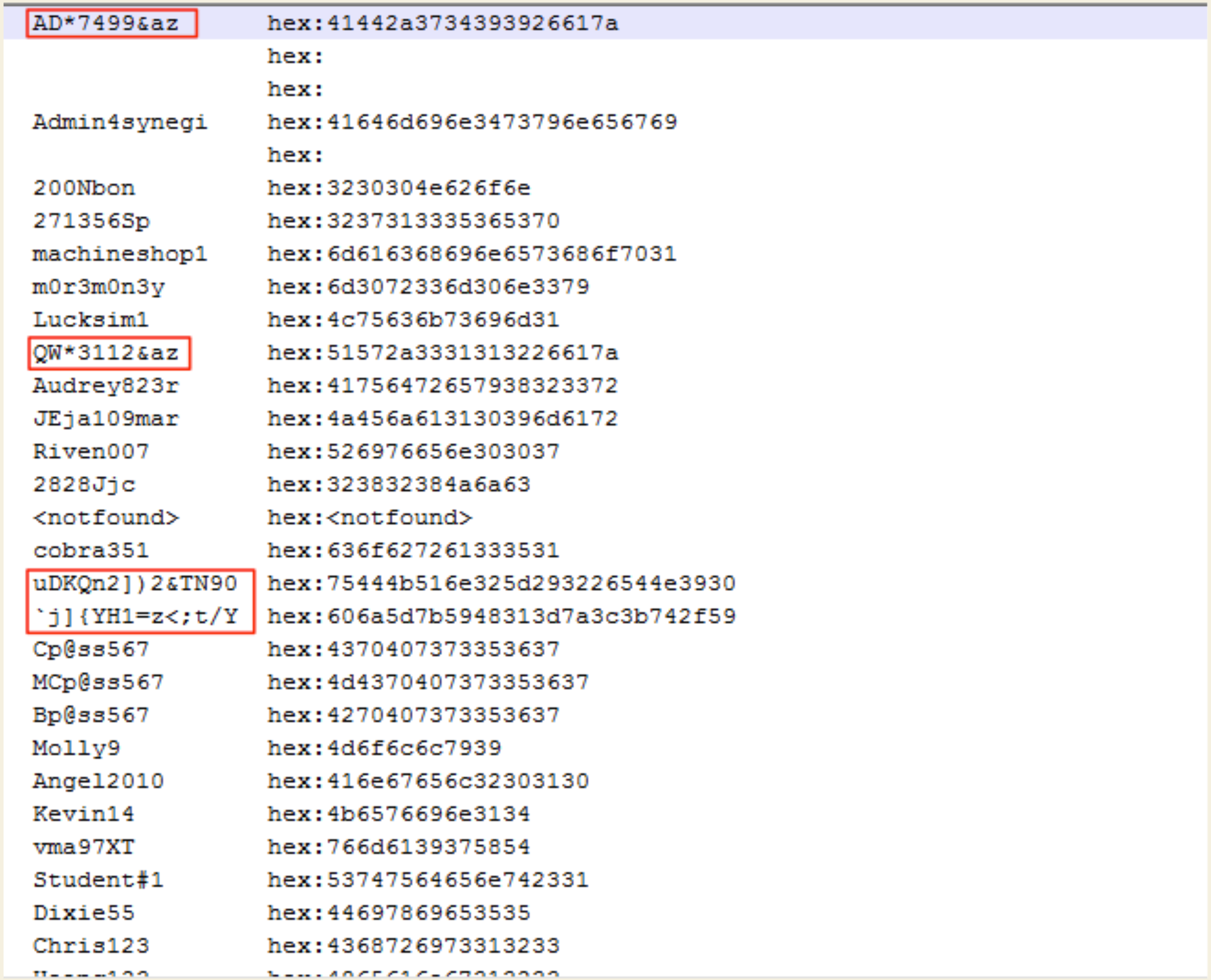
Eliminate LanMan Password Hashes

Eliminate LanMan Hashes

LanMan is a weak hashing algorithm, which only works on passwords of 14 characters or less. **The password is converted to upper case and split into two easily cracked 7 character chunks.**

Tools such as Ophcrack, Rcracki_mt, John the Ripper, and Hashcat can crack LM hashes very quickly.

ASG Consulting



```
AD*7499&az       hex:41442a3734393926617a
                 hex:
                 hex:
Admin4synegi     hex:41646d696e3473796e656769
                 hex:
200Nbon          hex:3230304e626f6e
271356Sp         hex:323731333536537 0
machineshop1     hex:6d616368696e6573686f7031
m0r3m0n3y        hex:6d3072336d306e3379
Lucksim1         hex:4c75636b73696d31
QW*3112&az       hex:51572a3331313226617a
Audrey823r       hex:41756472657938323372
JEja109mar       hex:4a456a613130396d6172
Riven007         hex:526976656e303037
2828Jjc          hex:323832384a6a63
<notfound>       hex:<notfound>
cobra351         hex:636f627261333531
uDKQn2])2&TN90   hex:75444b516e325d293226544e3930
`j]{YH1=z<;t/Y   hex:606a5d7b5948313d7a3c3b742f59
Cp@ss567         hex:43704073733536 37
MCp@ss567        hex:4d437040737335 3637
Bp@ss567         hex:42704073733536 37
Molly9           hex:4d6f6c6c7939
Angel2010        hex:416e67656c32303130
Kevin14          hex:4b6576696e3134
vma97XT          hex:766d6139375854
Student#1        hex:53747564656e742331
Dixie55          hex:44697869653535
Chris123         hex:4368726973313233
```

Eliminate LanMan Hashes

Group Policy

1. Open Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options
2. Network security: Do not store LAN Manager hash value on **next password change.**

Eliminate LanMan Hashes

Local Machine

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
2. Add DWORD NoLMHash
3. Set the value to 1

Eliminate LanMan Hashes

Unfortunately, these changes only mean LM hashes **are not saved to disk**. Windows still calculates the LM hashes and **stores them in memory**, which means they can still be extracted and cracked using tools like Windows Credential Editor (WCE). The only way to completely remove LM hashes is to **use passwords of 15 characters or more**.

Side Note: Mimikatz

Authentication algorithms such as HTTP Digest and Kerberos require knowledge of the plaintext password so **Windows stores it in memory** in encrypted form. The password can be **easily decrypted to recover the plaintext password**.

Mimikatz finds and decrypts these passwords.

ASG Consulting

Side Note: Mimikatz

The only way to protect against Mimikatz is to **not logon interactively with privileged accounts**. When interacting with a compromised machine, **use WMIC, PSExec, or Net** commands.

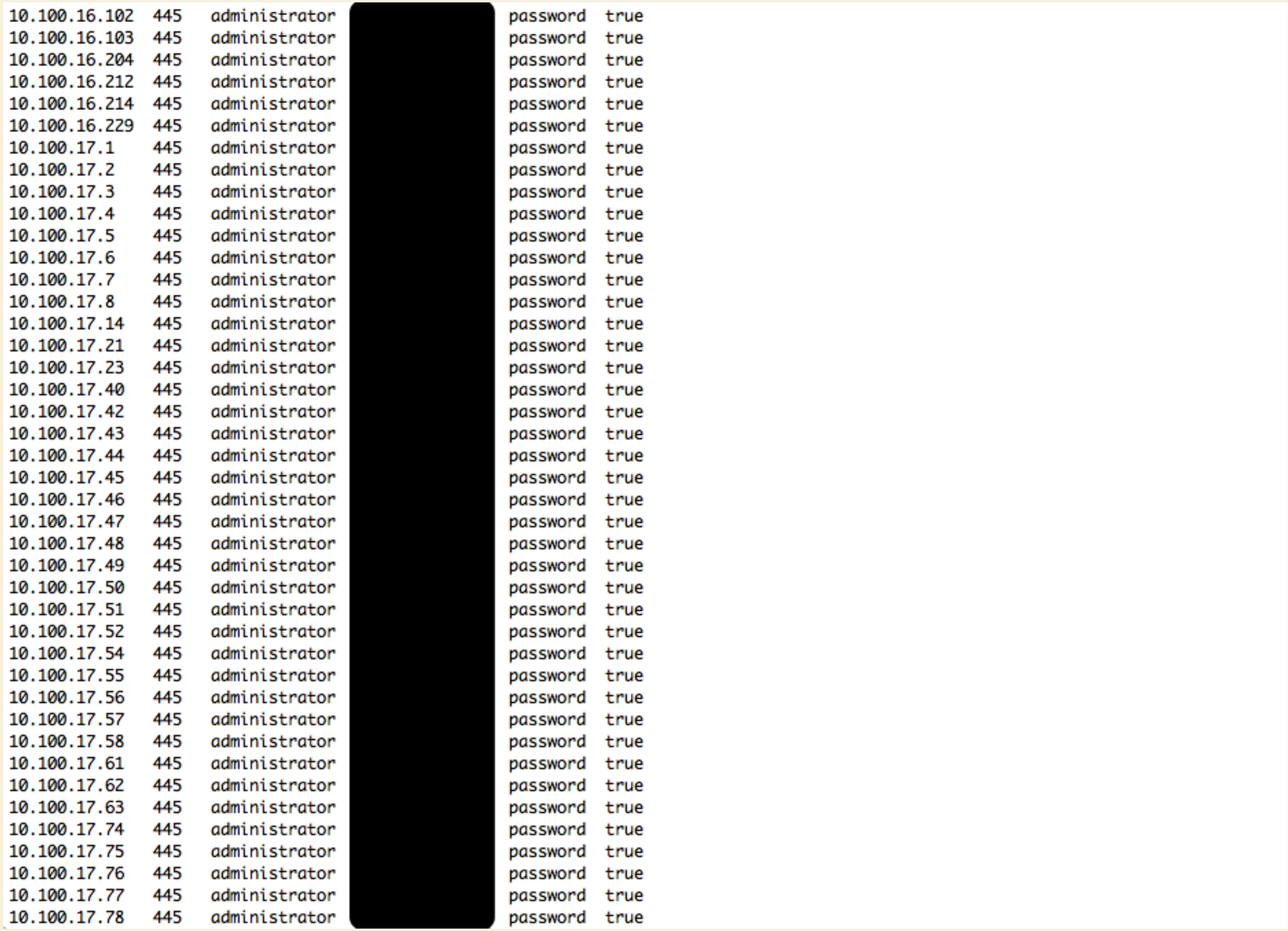
ASG Consulting

Remove Shared Local Admin Passwords

Remove Shared Local Admin Passwords

It is very common for the same local administrator password to be used throughout an organization. **Once an attacker has the shared password he has control of a large portion of the organization.**

ASG Consulting



```
10.100.16.102  445   administrator   [redacted]   password  true
10.100.16.103  445   administrator                password  true
10.100.16.204  445   administrator                password  true
10.100.16.212  445   administrator                password  true
10.100.16.214  445   administrator                password  true
10.100.16.229  445   administrator                password  true
10.100.17.1    445   administrator                password  true
10.100.17.2    445   administrator                password  true
10.100.17.3    445   administrator                password  true
10.100.17.4    445   administrator                password  true
10.100.17.5    445   administrator                password  true
10.100.17.6    445   administrator                password  true
10.100.17.7    445   administrator                password  true
10.100.17.8    445   administrator                password  true
10.100.17.14   445   administrator                password  true
10.100.17.21   445   administrator                password  true
10.100.17.23   445   administrator                password  true
10.100.17.40   445   administrator                password  true
10.100.17.42   445   administrator                password  true
10.100.17.43   445   administrator                password  true
10.100.17.44   445   administrator                password  true
10.100.17.45   445   administrator                password  true
10.100.17.46   445   administrator                password  true
10.100.17.47   445   administrator                password  true
10.100.17.48   445   administrator                password  true
10.100.17.49   445   administrator                password  true
10.100.17.50   445   administrator                password  true
10.100.17.51   445   administrator                password  true
10.100.17.52   445   administrator                password  true
10.100.17.54   445   administrator                password  true
10.100.17.55   445   administrator                password  true
10.100.17.56   445   administrator                password  true
10.100.17.57   445   administrator                password  true
10.100.17.58   445   administrator                password  true
10.100.17.61   445   administrator                password  true
10.100.17.62   445   administrator                password  true
10.100.17.63   445   administrator                password  true
10.100.17.74   445   administrator                password  true
10.100.17.75   445   administrator                password  true
10.100.17.76   445   administrator                password  true
10.100.17.77   445   administrator                password  true
10.100.17.78   445   administrator                password  true
```

Remove Shared Local Admin Passwords

Make sure the **local administrator** account and the **domain administrator** account use **unique passwords**.

Remove Shared Local Admin Passwords

Use a unique password for each local administrator account.

Deny network logons for the local administrator account.

ASG Consulting

Lockdown Open File Shares

Lock Down Open File Shares

Open file shares are an excellent source of sensitive data. Windows shared folders, NFS shared folders, and anonymous FTP servers are the most common source of open file shares.

Tools like Nmap, Nessus, or Metasploit can be used to find open shares.

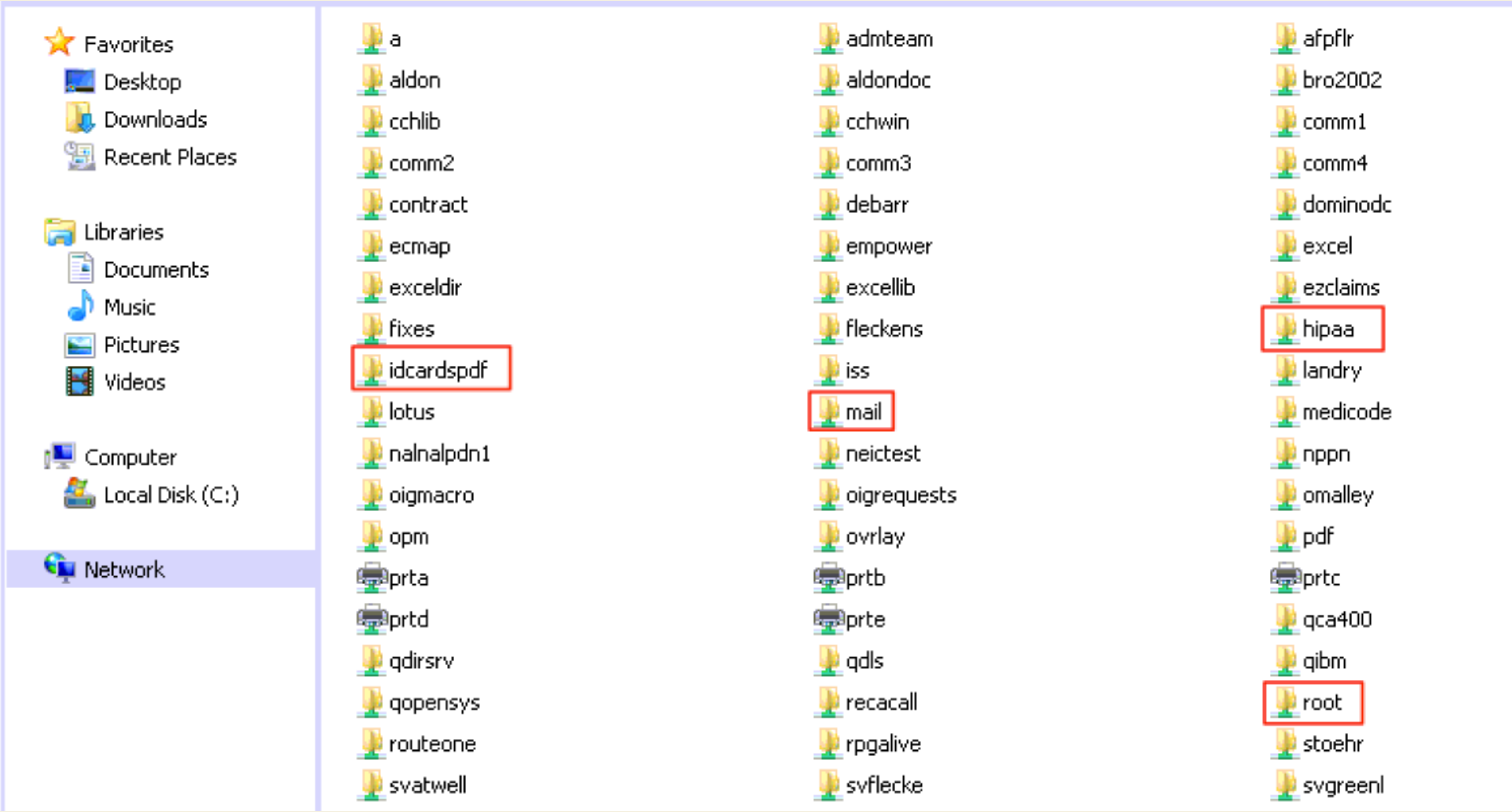
Lock Down Open File Shares

At one client the primary file server had many **open shares**, some of which contained **protected health information.** Other shares contained the source code to the client's web site, including **database credentials.**

Lock Down Open File Shares

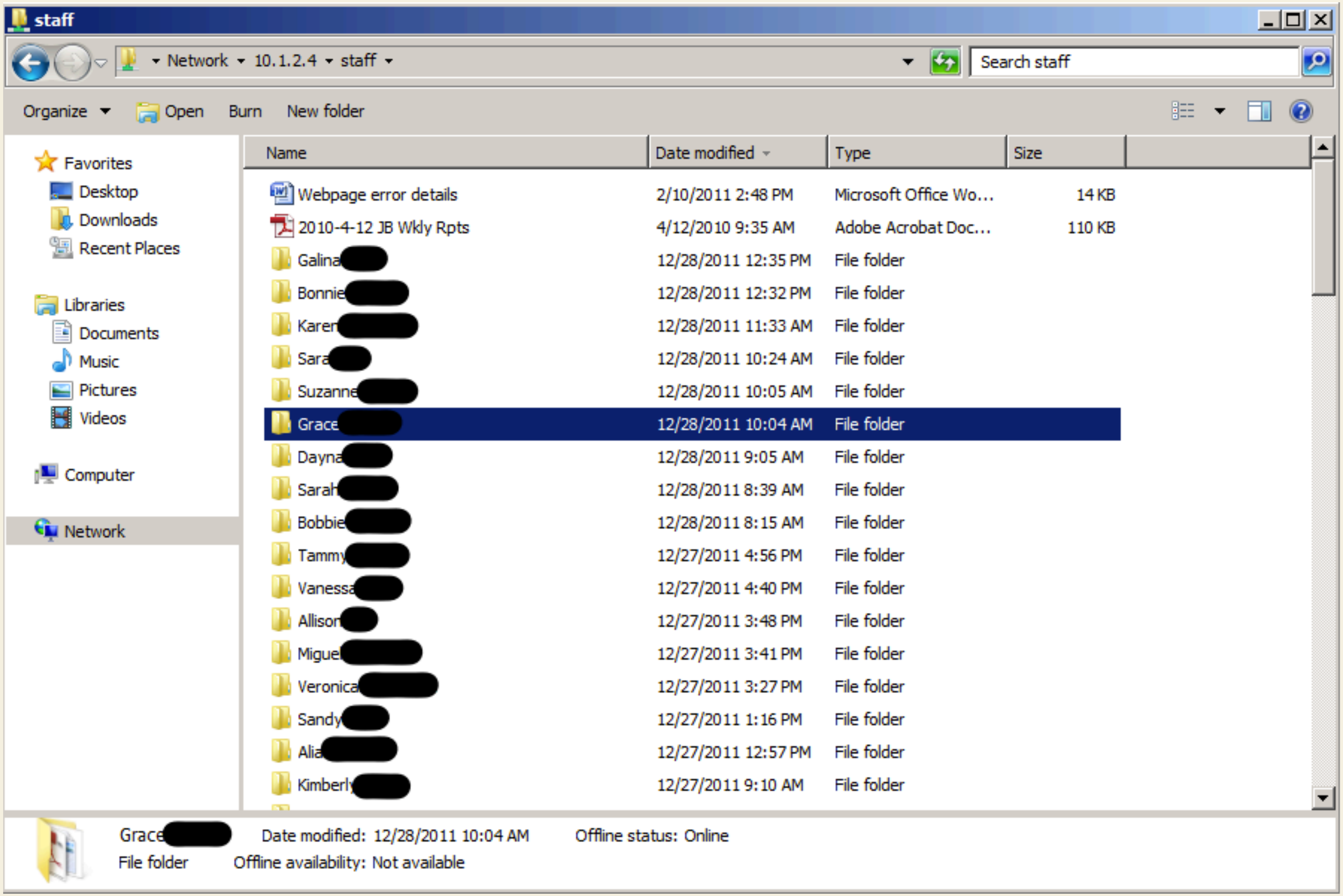
At another client, a user shared files with **Windows Simple File Sharing** in Windows XP. The shared folder contained a document that included **passwords** for the company **Facebook account** and **donor mailing list**.

ASG Consulting



a
aldon
cchlib
comm2
contract
ecmap
exceldir
fixes
idcardspdf
lotus
nalnalpdn1
oigmacro
opm
prta
prtd
qdirsrv
qopensys
routeone
svatwell
admteam
aldondoc
cchwin
comm3
debarr
empower
excellib
fleckens
iss
mail
neictest
oigrequests
ovrlay
prtb
prte
qdls
recacall
rpgalive
svflecke
afpflr
bro2002
comm1
comm4
dominodc
excel
ezclaims
hipaa
landry
medicode
nppn
omalley
pdf
prtc
qca400
qibm
root
stoehr
svgreenl

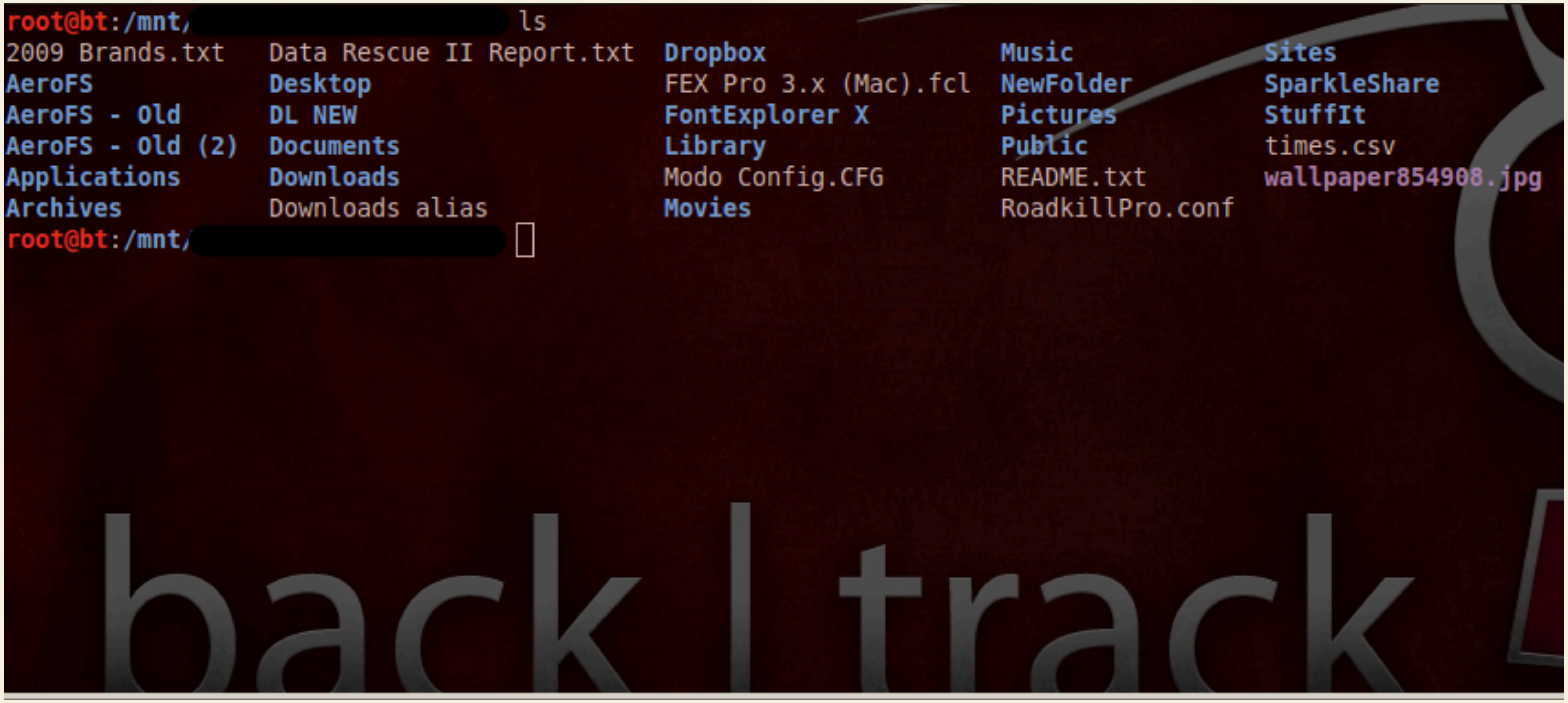
ASG Consulting



Name	Date modified	Type	Size
Webpage error details	2/10/2011 2:48 PM	Microsoft Office Wo...	14 KB
2010-4-12 JB Wkly Rpts	4/12/2010 9:35 AM	Adobe Acrobat Doc...	110 KB
Galina [redacted]	12/28/2011 12:35 PM	File folder	
Bonnie [redacted]	12/28/2011 12:32 PM	File folder	
Karen [redacted]	12/28/2011 11:33 AM	File folder	
Sara [redacted]	12/28/2011 10:24 AM	File folder	
Suzanne [redacted]	12/28/2011 10:05 AM	File folder	
Grace [redacted]	12/28/2011 10:04 AM	File folder	
Dayna [redacted]	12/28/2011 9:05 AM	File folder	
Sarah [redacted]	12/28/2011 8:39 AM	File folder	
Bobbie [redacted]	12/28/2011 8:15 AM	File folder	
Tammy [redacted]	12/27/2011 4:56 PM	File folder	
Vanessa [redacted]	12/27/2011 4:40 PM	File folder	
Allison [redacted]	12/27/2011 3:48 PM	File folder	
Miguel [redacted]	12/27/2011 3:41 PM	File folder	
Veronica [redacted]	12/27/2011 3:27 PM	File folder	
Sandy [redacted]	12/27/2011 1:16 PM	File folder	
Alia [redacted]	12/27/2011 12:57 PM	File folder	
Kimberly [redacted]	12/27/2011 9:10 AM	File folder	

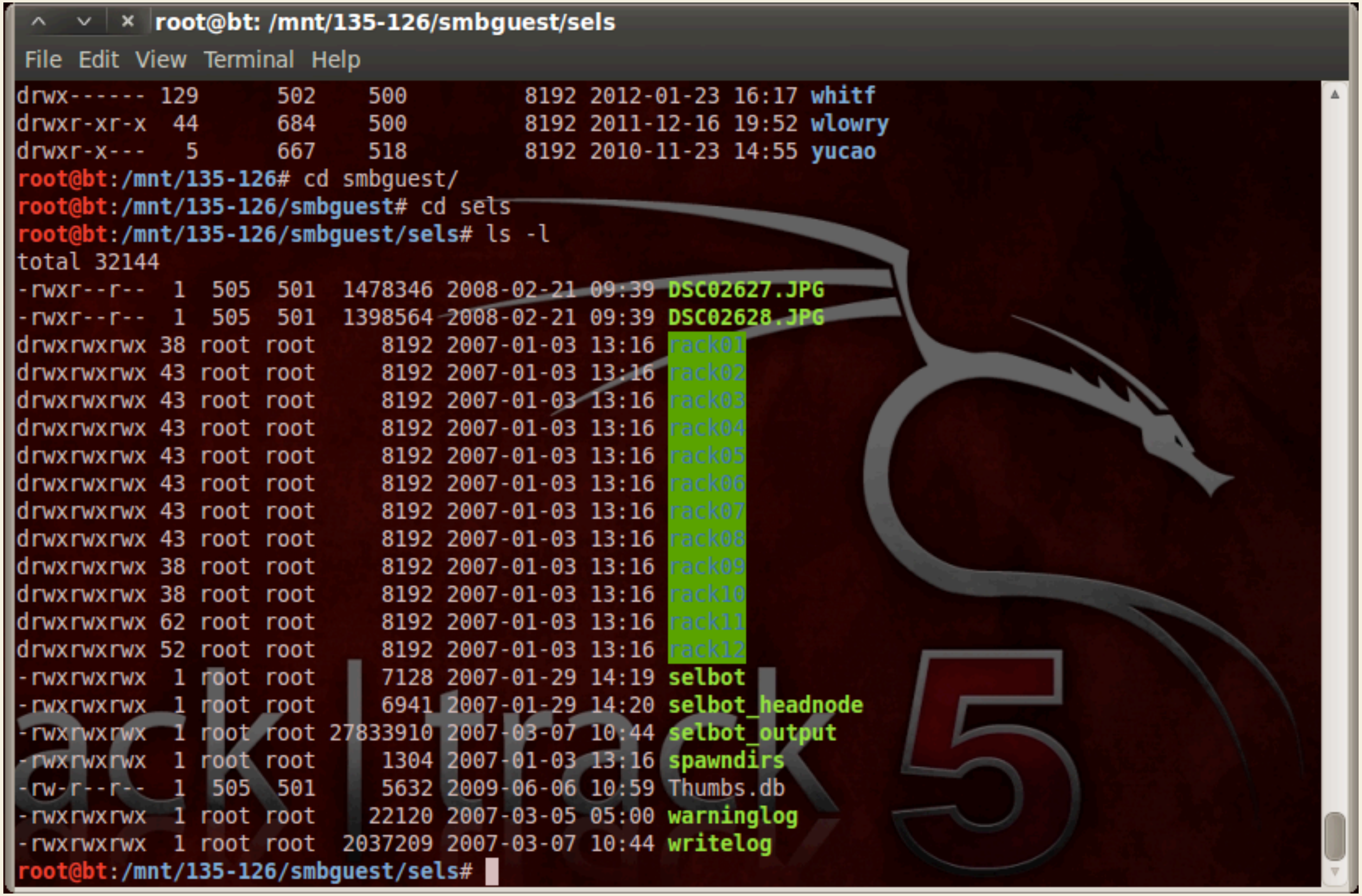
Grace [redacted] Date modified: 12/28/2011 10:04 AM Offline status: Online
File folder Offline availability: Not available

ASG Consulting



```
root@bt:/mnt/[redacted] ls
2009 Brands.txt    Data Rescue II Report.txt  Dropbox                   Music             Sites
AeroFS             Desktop                    FEX Pro 3.x (Mac).fcl     NewFolder         SparkleShare
AeroFS - Old       DL NEW                     FontExplorer X            Pictures          StuffIt
AeroFS - Old (2)   Documents                  Library                   Public            times.csv
Applications       Downloads                  Modo Config.CFG           README.txt        wallpaper854908.jpg
Archives           Downloads alias            Movies                    RoadkillPro.conf
root@bt:/mnt/[redacted] 
```

ASG Consulting


root@bt: /mnt/135-126/smbguest/sels
File Edit View Terminal Help

```
drwx------ 129      502    500          8192 2012-01-23 16:17 whitf
drwxr-xr-x  44      684    500          8192 2011-12-16 19:52 wlowry
drwxr-x---   5      667    518          8192 2010-11-23 14:55 yucao
root@bt:/mnt/135-126# cd smbguest/
root@bt:/mnt/135-126/smbguest# cd sels
root@bt:/mnt/135-126/smbguest/sels# ls -l
total 32144
-rwxr--r--  1  505  501  1478346 2008-02-21 09:39 DSC02627.JPG
-rwxr--r--  1  505  501  1398564 2008-02-21 09:39 DSC02628.JPG
drwxrwxrwx 38 root root     8192 2007-01-03 13:16 rack01
drwxrwxrwx 43 root root     8192 2007-01-03 13:16 rack02
drwxrwxrwx 43 root root     8192 2007-01-03 13:16 rack03
drwxrwxrwx 43 root root     8192 2007-01-03 13:16 rack04
drwxrwxrwx 43 root root     8192 2007-01-03 13:16 rack05
drwxrwxrwx 43 root root     8192 2007-01-03 13:16 rack06
drwxrwxrwx 43 root root     8192 2007-01-03 13:16 rack07
drwxrwxrwx 43 root root     8192 2007-01-03 13:16 rack08
drwxrwxrwx 38 root root     8192 2007-01-03 13:16 rack09
drwxrwxrwx 38 root root     8192 2007-01-03 13:16 rack10
drwxrwxrwx 62 root root     8192 2007-01-03 13:16 rack11
drwxrwxrwx 52 root root     8192 2007-01-03 13:16 rack12
-rwxrwxrwx  1 root root     7128 2007-01-29 14:19 selbot
-rwxrwxrwx  1 root root     6941 2007-01-29 14:20 selbot_headnode
-rwxrwxrwx  1 root root 27833910 2007-03-07 10:44 selbot_output
-rwxrwxrwx  1 root root     1304 2007-01-03 13:16 spawndirs
-rw-r--r--  1  505  501     5632 2009-06-06 10:59 Thumbs.db
-rwxrwxrwx  1 root root    22120 2007-03-05 05:00 warninglog
-rwxrwxrwx  1 root root  2037209 2007-03-07 10:44 writelog
root@bt:/mnt/135-126/smbguest/sels#
```

Lock Down Open File Shares

1. Open Folder Options
2. Go to the View tab
3. Uncheck “Use Simple File Sharing”
4. View the Properties for a Folder
5. Go to the Sharing tab and set the permissions to Everyone Full Control
6. Go to the Security tab and set appropriate NTFS permissions.

Lock Down Open File Shares

1. Edit /etc/exports to ensure only appropriate directories are listed.
2. For each directory, **grant access to only the appropriate IP addresses**.
3. For each IP address, **ensure read/write permissions are set correctly**.
4. Ensure **root is squashed**.

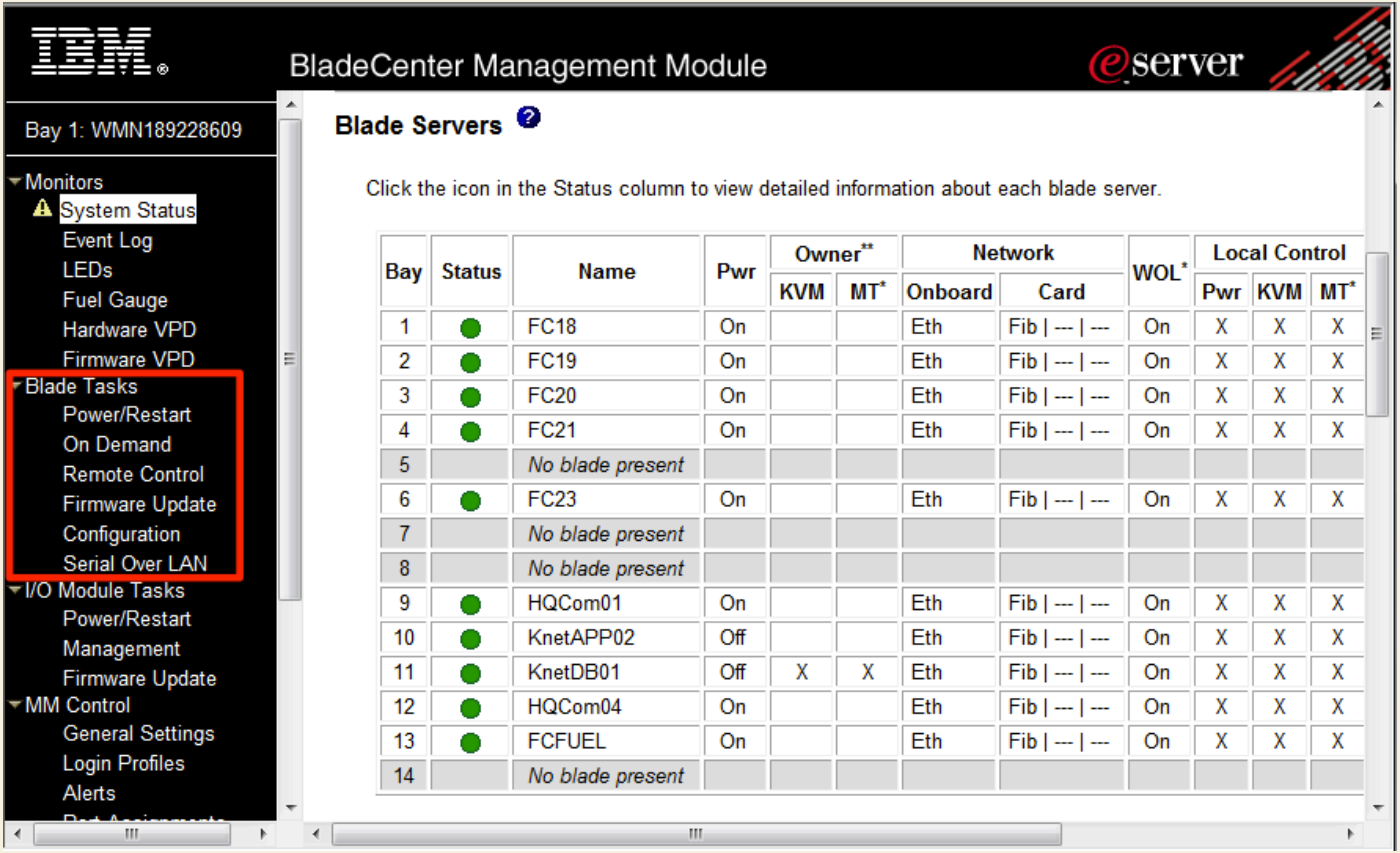
Replace Default/Blank Passwords

Replace Default/Blank Passwords

Blank sa passwords in MSSQL can lead to full machine compromise.

Blank local administrator passwords allow full machine compromise.

Default/blank passwords on web-based management interfaces lead to various levels of compromise.



Bay 1: WMN189228609

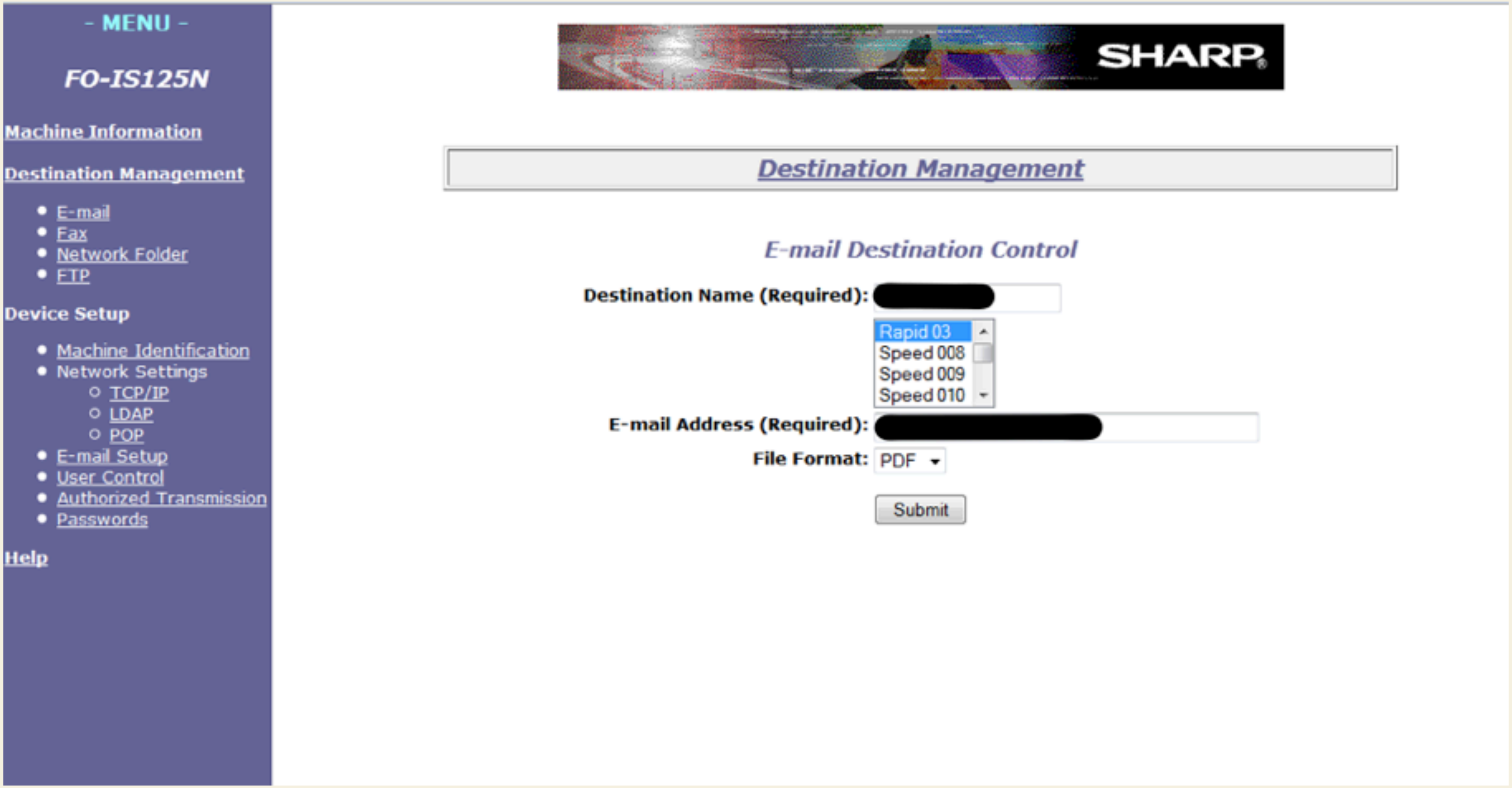
- Monitors
  - ⚠ System Status
  - Event Log
  - LEDs
  - Fuel Gauge
  - Hardware VPD
  - Firmware VPD
- Blade Tasks
  - Power/Restart
  - On Demand
  - Remote Control
  - Firmware Update
  - Configuration
  - Serial Over LAN
- I/O Module Tasks
  - Power/Restart
  - Management
  - Firmware Update
- MM Control
  - General Settings
  - Login Profiles
  - Alerts
  - Port Assignments

Blade Servers

Click the icon in the Status column to view detailed information about each blade server.

Bay	Status	Name	Pwr	Owner**		Network		WOL*	Local Control		
				KVM	MT*	Onboard	Card		Pwr	KVM	MT*
1	●	FC18	On			Eth	Fib | --- | ---	On	X	X	X
2	●	FC19	On			Eth	Fib | --- | ---	On	X	X	X
3	●	FC20	On			Eth	Fib | --- | ---	On	X	X	X
4	●	FC21	On			Eth	Fib | --- | ---	On	X	X	X
5		*No blade present*									
6	●	FC23	On			Eth	Fib | --- | ---	On	X	X	X
7		*No blade present*									
8		*No blade present*									
9	●	HQCom01	On			Eth	Fib | --- | ---	On	X	X	X
10	●	KnetAPP02	Off			Eth	Fib | --- | ---	On	X	X	X
11	●	KnetDB01	Off	X	X	Eth	Fib | --- | ---	On	X	X	X
12	●	HQCom04	On			Eth	Fib | --- | ---	On	X	X	X
13	●	FCFUEL	On			Eth	Fib | --- | ---	On	X	X	X
14		*No blade present*									

ASG Consulting



Destination Management

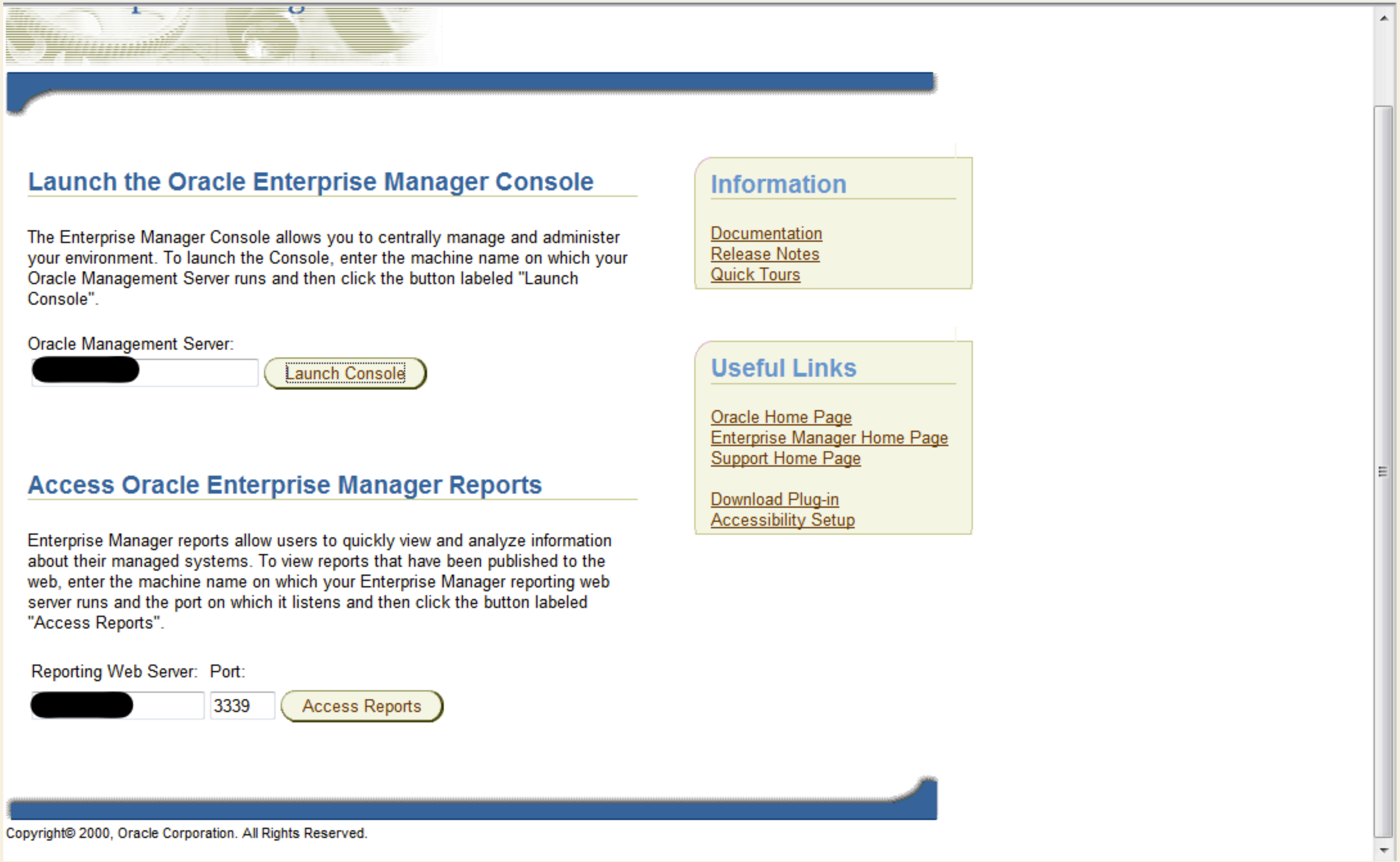
E-mail Destination Control

Destination Name (Required): [redacted]

Rapid 03
Speed 008
Speed 009
Speed 010

E-mail Address (Required): [redacted]

File Format: PDF



Launch the Oracle Enterprise Manager Console

The Enterprise Manager Console allows you to centrally manage and administer your environment. To launch the Console, enter the machine name on which your Oracle Management Server runs and then click the button labeled "Launch Console".

Oracle Management Server: [redacted]

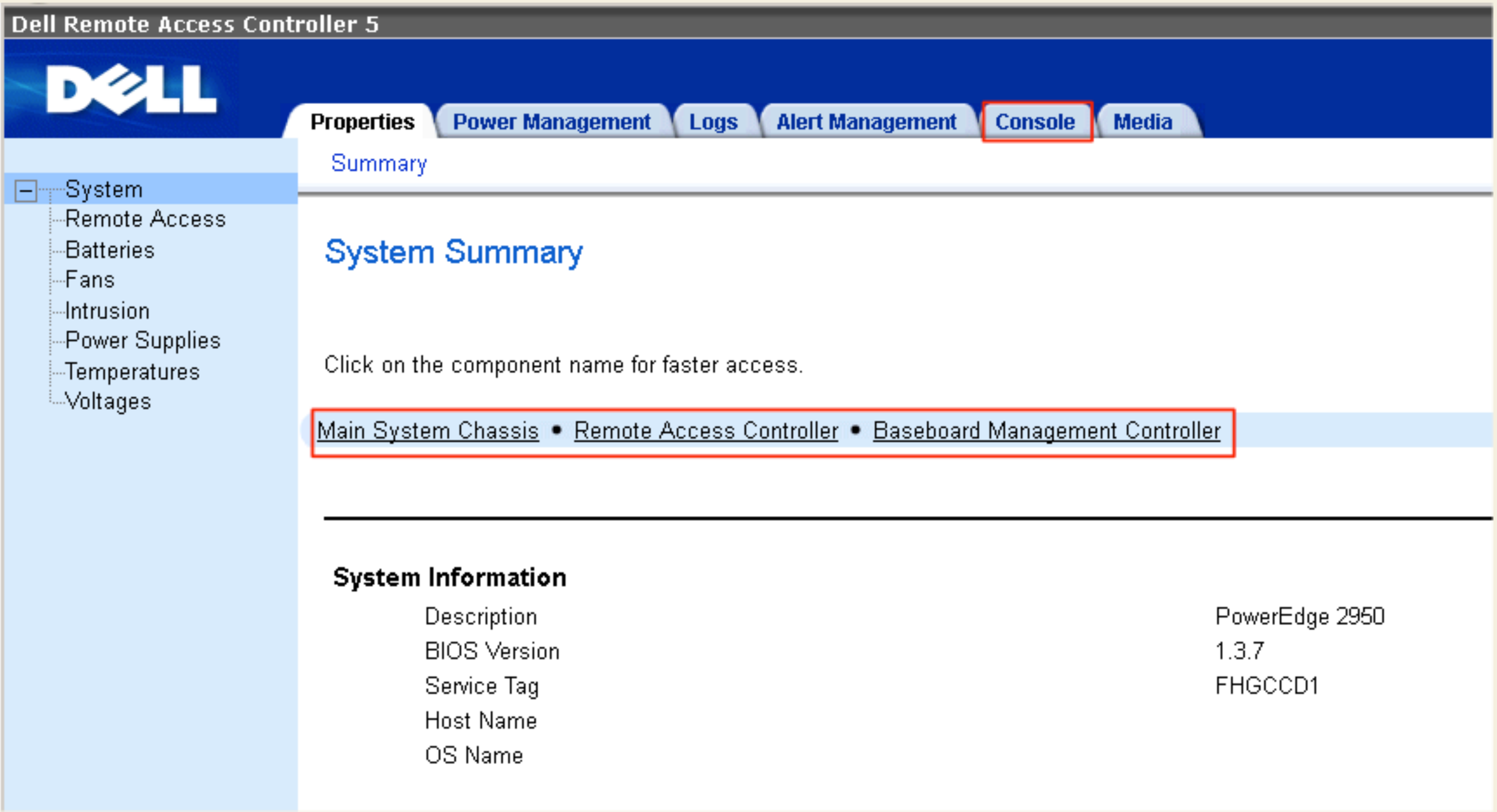
Access Oracle Enterprise Manager Reports

Enterprise Manager reports allow users to quickly view and analyze information about their managed systems. To view reports that have been published to the web, enter the machine name on which your Enterprise Manager reporting web server runs and the port on which it listens and then click the button labeled "Access Reports".

Reporting Web Server: [redacted] Port: 3339

Information

Useful Links



System Summary

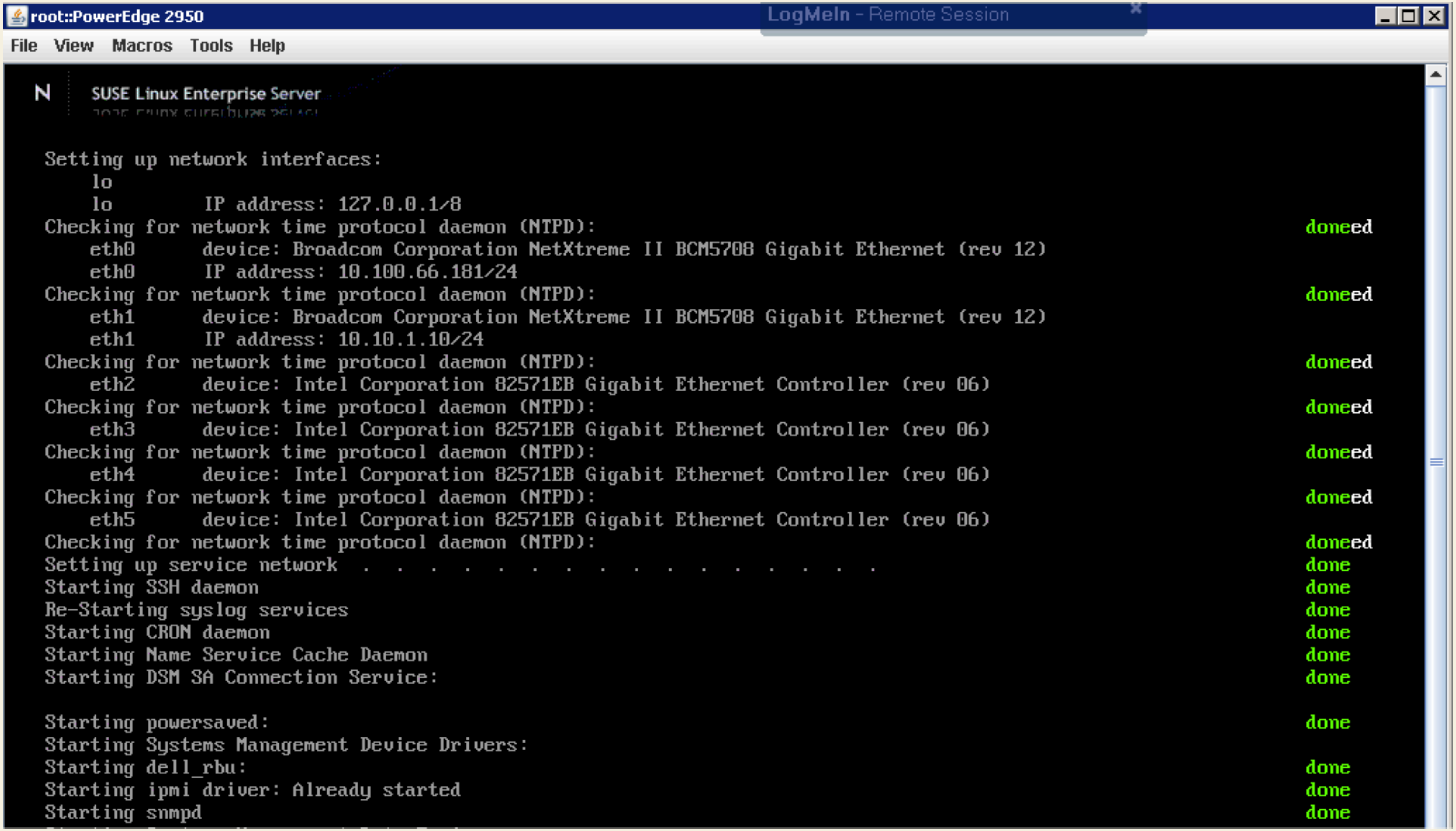
Click on the component name for faster access.

Main System Chassis • Remote Access Controller • Baseboard Management Controller

System Information

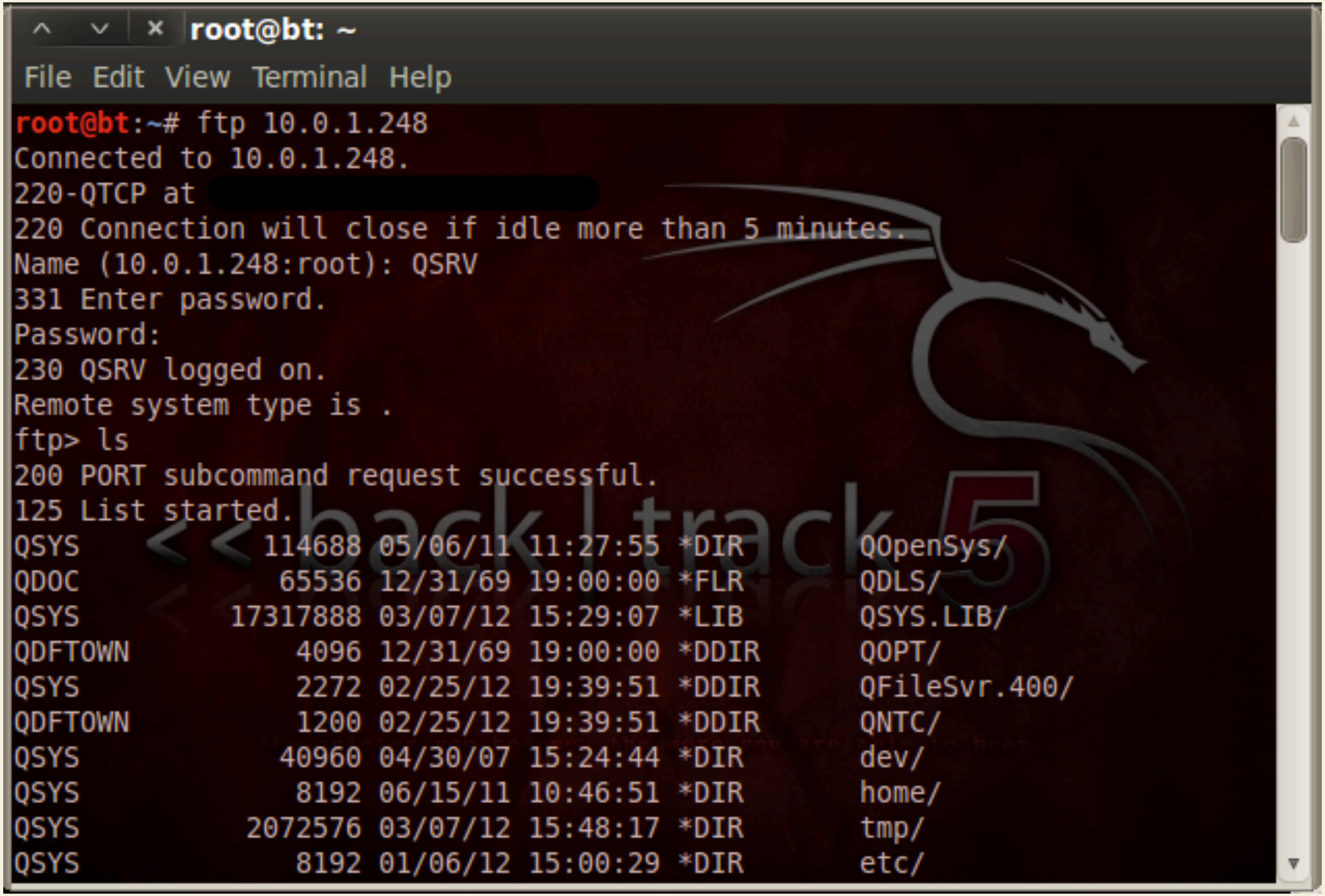
Description	PowerEdge 2950
BIOS Version	1.3.7
Service Tag	FHGCCD1
Host Name	
OS Name	

ASG Consulting



```
Setting up network interfaces:
    lo
    lo         IP address: 127.0.0.1/8
Checking for network time protocol daemon (NTPD):                                     doneed
    eth0       device: Broadcom Corporation NetXtreme II BCM5708 Gigabit Ethernet (rev 12)
    eth0       IP address: 10.100.66.181/24
Checking for network time protocol daemon (NTPD):                                     doneed
    eth1       device: Broadcom Corporation NetXtreme II BCM5708 Gigabit Ethernet (rev 12)
    eth1       IP address: 10.10.1.10/24
Checking for network time protocol daemon (NTPD):                                     doneed
    eth2       device: Intel Corporation 82571EB Gigabit Ethernet Controller (rev 06)
Checking for network time protocol daemon (NTPD):                                     doneed
    eth3       device: Intel Corporation 82571EB Gigabit Ethernet Controller (rev 06)
Checking for network time protocol daemon (NTPD):                                     doneed
    eth4       device: Intel Corporation 82571EB Gigabit Ethernet Controller (rev 06)
Checking for network time protocol daemon (NTPD):                                     doneed
    eth5       device: Intel Corporation 82571EB Gigabit Ethernet Controller (rev 06)
Checking for network time protocol daemon (NTPD):                                     doneed
Setting up service network  . . . . . . . . . . . . . . . .                           done
Starting SSH daemon                                                                   done
Re-Starting syslog services                                                           done
Starting CRON daemon                                                                  done
Starting Name Service Cache Daemon                                                    done
Starting DSM SA Connection Service:                                                   done

Starting powersaved:                                                                  done
Starting Systems Management Device Drivers:
Starting dell_rbu:                                                                    done
Starting ipmi driver: Already started                                                 done
Starting snmpd                                                                        done
```



```
root@bt:~# ftp 10.0.1.248
Connected to 10.0.1.248.
220-QTCP at [redacted]
220 Connection will close if idle more than 5 minutes.
Name (10.0.1.248:root): QSRV
331 Enter password.
Password:
230 QSRV logged on.
Remote system type is .
ftp> ls
200 PORT subcommand request successful.
125 List started.
QSYS         114688 05/06/11 11:27:55 *DIR       QOpenSys/
QDOC          65536 12/31/69 19:00:00 *FLR       QDLS/
QSYS       17317888 03/07/12 15:29:07 *LIB       QSYS.LIB/
QDFTOWN        4096 12/31/69 19:00:00 *DDIR      QOPT/
QSYS           2272 02/25/12 19:39:51 *DDIR      QFileSvr.400/
QDFTOWN        1200 02/25/12 19:39:51 *DDIR      QNTC/
QSYS          40960 04/30/07 15:24:44 *DIR       dev/
QSYS           8192 06/15/11 10:46:51 *DIR       home/
QSYS        2072576 03/07/12 15:48:17 *DIR       tmp/
QSYS           8192 01/06/12 15:00:29 *DIR       etc/
```

Replace Default/Blank Passwords

There is **no automated method for fixing this issue**.

Vulnerability scanners cannot identify all instances of default/blank passwords but can identify a number of them.

Replace Default/Blank Passwords

1. Scan the network for HTTP, FTP, Telnet, and SSH services.
2. Disable any services that are not needed.
3. Ensure a strong password is used on any services that are not disabled.

ASG Consulting

Replace Default/Blank Passwords

http://www.phenoelit.org/dpl/dpl.html

http://cirt.net/passwords

http://www.virus.org/default-password

Lockdown Remote Desktop Protocol

Lockdown Remote Desktop Protocol

RDP is used throughout many organizations to remotely administer internal machines and is typically configured with **no restrictions other than username and password**.

Lockdown Remote Desktop Protocol

The **Morto worm** scans a network for machines running RDP and attempts to login using the administrator account and a list of weak passwords. After it logs in, it copies itself to the new machine, searches for other vulnerable machines, and calls back to a C&C server to await commands.

Lockdown Remote Desktop Protocol

The update in **MS12-020** fixes a vulnerability in RDP, which is present in all versions of Windows. Newer versions of RDP use network level authentication (NLA), which requires an attacker to authenticate to the server before connecting to the RDP service, but this does not fix the underlying vulnerability. The only fix is to apply the update.

Lockdown Remote Desktop Protocol

Disable RDP with Group Policy (Server 2003)

1. Open Computer Configuration -> Administrative Templates -> Windows Components -> Terminal Services
2. Set “Allow users to connect remotely using Terminal Services” to disabled.

Lockdown Remote Desktop Protocol

Disable RDP with Group Policy (Server 2008)

1. Open Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Connections
2. Set "Allow users to connect remotely using Remote Desktop Services" to disabled.

Lockdown Remote Desktop Protocol

Additional Controls

1. Use Windows Firewall to restrict access by IP address.
2. Use Group Policy to restrict access to specific users.

Recap

1. Eliminate LanMan Hashes
2. Remove Shared Local Admin Passwords
3. Lockdown Open File Shares
4. Replace Default/Blank Passwords
5. Lockdown Remote Desktop Protocol

Additional Resources

- http://computer-forensics.sans.org/blog/2012/03/09/protecting-privileged-domain-accounts-disabling-encrypted-passwords
- http://computer-forensics.sans.org/blog/2012/02/21/protecting-privileged-domain-account-safeguarding-password-hashes
- http://support.microsoft.com/kb/306300 (Disable RDP Server 2003)
- http://www.reborndigital.com/?p=88 (Disable RDP Server 2008)

Five Steps to Improve Internal Network Security

Chattanooga ISSA