Nessus Report

Report

22/Mar/2012:10:14:10 GMT

Table Of Contents

Compliance 'FAILED'

4.5 Change admin account name

Info

Change db admin account from default ('root') to something else

Policy Value

NULL

Hosts

192.168.150.131

```
"root"
"root"
"root"
"root"
```

4.9 Wildcards in user hostname

Info

Verify if users have wildcard ('%') in hostname

Policy Value

NULL

Hosts

192.168.150.131

```
"root"
```

5.1 (1) Access to mysql database

Info

Only admin users should have access to the mysql database

Policy Value

regex:"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
"readonly", localhost
```

5.2 FILE privelege

Info

Do not grant to non Admin users

Policy Value

"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
```

5.3 PROCESS privelege

Info

Do not grant to non Admin users

Policy Value

"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
```

5.4 SUPER privelege

Info

Do not grant to non Admin users

Policy Value

"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
```

5.5 SHUTDOWN privelege

Info

Do not grant to non Admin users

Policy Value

"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
```

5.6 CREATE USER privelege

Info

Do not grant to non Admin users

Policy Value

"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
```

5.7 RELOAD privelege

Info

Do not grant to non Admin users

Policy Value

"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
```

5.8 GRANT privelege

Info

Do not grant to non Admin users

Policy Value

"root"

Hosts

192.168.150.131

```
"root", localhost
"root", secfail1
"root", 127.0.0.1
"debian-sys-maint", localhost
"root", %
```

6.2 Disable Load data local

Info

Check that --local-infile=0

Policy Value

regex:"local_infile", regex:"off"

Hosts

192.168.150.131

```
"local_infile", "ON"
```

6.5 Secure auth

Info

Must use: --secure-auth

Policy Value

regex:"secure_auth", regex:"on"

Hosts

192.168.150.131

```
"secure_auth", "OFF"
```

6.10 Skip Symbolic Links

Info

Use --skip-symbolic-links

Policy Value

regex:"skip_symbolic_links", regex:"disabled"

Hosts

192.168.150.131

```
"have_symlink", "YES"
```

7.2 (1) SSL Connection

Info

Must use SSL over untrusted networks (internet) or when restricted PII is transferred

Policy Value

regex:"have_openssl", regex:"yes"

Hosts

192.168.150.131

```
"have_openssl", "DISABLED"
```

Compliance 'SKIPPED'

Compliance 'PASSED'

3.1 Error Logging Enabled

Hosts

192.168.150.131

4.1 Supported version of MySQL

Info

Migrate to version 4.1 or 5.0.

Hosts

192.168.150.131

4.4 Remove test database

Hosts

192.168.150.131

4.7 Verify Secure Password Hashes

Info

All password hashes should be 41 bytes or longer

Hosts

192.168.150.131

4.10 No blank passwords

Hosts

192.168.150.131

4.11 Anonymous account

Info

Verify and remove anonymous accounts ; Anonymous accounts are users with no name (").
They allow for default logins and there permissions can sometimes be used by other users.

Hosts

192.168.150.131

5.1 (2) Access to mysql database

Info

Only admin users should have access to the mysql database

Hosts

192.168.150.131

6.3 Old password hashing

Info

Must not use: --old-passwords

Hosts

192.168.150.131

Compliance 'INFO', 'WARNING', 'ERROR'