GNU/Linux Administration - Support #591

Hardening an SSH Server

04/05/2015 06:34 PM - Daniel Curtis

Status:	Closed	**Start date:**	04/05/2015
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Server	**Estimated time:**	1.00 hour
Target version:	*nix	**Spent time:**	1.50 hour

Description

This is guide for hardening an SSH server.

- **WARNING**: You will need a recent OpenSSH version. It should work with 6.5 but I have only tested 6.6; you can check the current version by running:

```
ssh -V
```

Key Exchange

- Add a strong Key Exchange:

```
echo 'KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256' >> /etc
/ssh/sshd_config
```

- Open /etc/ssh/moduli if exists, and delete lines where the 5th column is less than 2000.

```
awk '$5 > 2000' /etc/ssh/moduli > "${HOME}/moduli"
wc -l "${HOME}/moduli"
mv "${HOME}/moduli" /etc/ssh/moduli
```

  - If wc -l is empty, create it:

```
ssh-keygen -G "${HOME}/moduli" -b 4096
ssh-keygen -T /etc/ssh/moduli -f "${HOME}/moduli"
rm "${HOME}/moduli"
```

Authentication

- Edit the sshd config file:

```
vi /etc/ssh/sshd_config
```

  - And modify the following parameters to only use SSHv2 and ed25519 and rsa key algorithms:

```
Protocol 2
HostKey /etc/ssh/ssh_host_ed25519_key
HostKey /etc/ssh/ssh_host_rsa_key
```

Client Authentication

- edit the sshd config file:

```
vi /etc/ssh/sshd_config
```

- And modify the following parameters to disable password based logins:

```
PasswordAuthentication no
ChallengeResponseAuthentication no
PubkeyAuthentication yes
```

Symmetric Ciphers

NOTE: For some reason I could not get the aes256-gcm@openssh.com and aes128-gcm@openssh.com ciphers to work on OpenSSH 6.6.

- Add strong Symmetric Ciphers:

```
echo 'Ciphers chacha20-poly1305@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr' >> /etc/ssh/sshd_config
```

Message Authentication Codes

- Add strong Message Authentication Codes:

```
echo 'MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-ripemd160-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-ripemd160,umac-128@openssh.com' >> /etc/ssh/sshd_config
```

Generate Strong Client Keypairs

- Generate strong client ssh keypairs:

```
ssh-keygen -t ed25519 -o -a 512
ssh-keygen -t rsa -b 4096 -o -a 512
```

Resources

- https://stribika.github.io/2015/01/04/secure-secure-shell.html

History

#1 - 04/05/2015 06:55 PM - Daniel Curtis

- Description updated

- Status changed from New to In Progress

- % Done changed from 0 to 50

#2 - 04/05/2015 06:56 PM - Daniel Curtis

- Description updated

#3 - 04/08/2015 08:30 PM - Daniel Curtis

- Status changed from In Progress to Resolved

- % Done changed from 50 to 100

#4 - 04/11/2015 01:22 PM - Daniel Curtis

- Status changed from Resolved to Closed