Encryption Technologies used in Ezeelogin

What are the Encryption algorithms used in Ezeelogin?

Overview: This article outlines the encryption technologies used for SSH gateway users.

The user **passwords** and **security codes** stored in the gateway server database use multiple rounds **SHA512, SHA256, BLOWFISH,** or **DES** depending on what's supported in the SSH gateway OS.
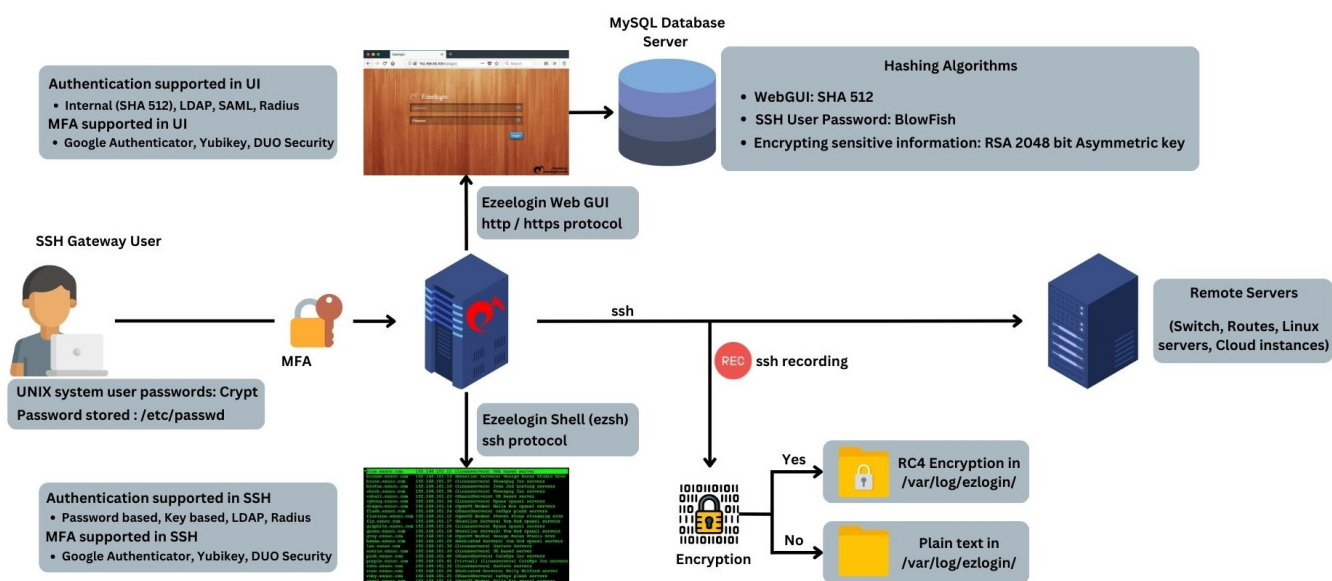
The UNIX System User passwords uses Crypt.

The parameter after the " : " in /etc/shadow refers to the hashing function in use.

User credentials on the database are encrypted.

2. The SSH private keys, server credentials are encrypted with 4096 bit RSA keys.

devops.myserver.com

3. Web portal login credentials are encrypted.

4. The Gateway User SSH logs are encrypted using RC4 which is recognized as the most commonly utilized stream cipher in the world of cryptography. You may read more about RC4 http://en.wikipedia.org/wiki/RC4

Step 4(A): Run the following command to find the default Ciphers, MAC , Kex Algorithms supported in the gateway OS.

```
root@gateway:~# sshd -T | grep "(ciphers|macs|kexalgorithms)"



gssapikexalgorithms gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-ciphers chacha20-poly1305@ope
nssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes12
8-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc



macs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hma
c-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@opens
sh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1



kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp3
84,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hell
man-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-
hellman-group14-sha1,diffie-hellman-group1-sha1
```

SSH logs are stored in an encrypted format within the database, as depicted below.

```
root@gateway:~# cat /var/log/ezlogin/full/ezadmin/devops.myserver.com~Wed_May_17_12:24:48_2023



�����lv�QRn!.�V���;��=�C��6����!��/�0��kT��NC ̋Xk�p�z�o�:��)s��ʃ
&���+�����e��ɟ�)�f��qY���o��S0��-��/�Wy�[
�:7A�'�/�nj�M�bT����}��n!��S��/
��t��P�i���^��s�fh���Y��'|�r���P�A��G�,�uQ�xJ��v���
/f����� s6>�K��������;uQ��R�w��Ws
(�Y����7��=0[��7���4zV��1�ǒJ�Ul<����o� �/4_� (�;M��*�
����CJB� ���q��'���9�2cuJ �H ,�L'�a��}���C3`!�E���'���@��d�
```

�p^���I��F�J��o��TJ%����P9��d��;=�0T���g��
�o�����Λ�ζ_�9�ش‌B�D ��}� e�%*�%������d-l��
�6�;cItP���$Z�V��&������$F�H(� ���A��q�� ��nC<{K-.D�a�f��Co
��AnCf2�����;T��S���L4��I�0~� c�d.����w���������A5"�a�Qa�₃�!pB
<QU��Jg�����>�;4$��Y��]Z��}F�����þOo�=��I�7�
������c9�5��d��t�'���=�8̲�h8�C�m�������N�1B�[�EX���
�J(�t~�z���aOV

Related Articles:

[Encryption type used for securing users' SSH logs in ezeelogin](#)

[Why is Ezeelogin the most secure SSH gateway?](#)

Online URL: https://www.ezeelogin.com/kb/article/encryption-technologies-used-in-ezeelogin-98.html