SSH Certificate

Wednesday, September 4, 2024 6:19 PM

CM --> CA --> RS
CA(Lock, Key) --> lock --> RS = CA --> RS
CM(lock, key) --> lock --> CA(RSL, RSK, CML) = CM --> CA
CM --> CA --> RS

1. Order 2 EC2 Instances
    a. Certificate Authority(CA) - Laptop
    b. Remote Server(RS) - EC2 Instance
    c. Client Machine (CM)- EC2 Instance
2. Generate Key and Lock **DONE**
    a. CA$ ssh-keygen -t rsa -f ca
3. CA(ca.pub) --> RS(/etc/ssh/ca.pub) **DONE**
    a. CA$ scp -i mujahed.pem ca.pub ubuntu@RS-IP:/home/ubuntu/
    b. CA$ ssh -i mujahed.pem ubuntu@RS-IP
    c. RS$ sudo su
    d. RS# cp /home/ubuntu/ca.pub /etc/ssh/ca.pub
4. In RS Configure Trusted Key **DONE**
    a. RS# vi /etc/ssh/sshd_config
    b. At the End: TrustedUserCAkeys /etc/ssh/ca.pub
    c. RS# service ssh restart
5. CM$ ssh-keygen -t rsa -f cm **DONE**
6. CM(cm.pub) --> CA(~/.ssh/cm.pub) **DONE**
7. Generate Certificate on CA **DONE**
    a. CA$ ssh-keygen -s ca -I cm -n developers,ops,ubuntu -V +1w -z 1 cm.pub
8. Verify Certificate
    a. CA$ ssh-keygen -Lf cm-cert.pub
9. Connect from CA --> CM
10. Connect From CM to RS