

ÚLOHA 6. SSH A CERTIFIKÁTY

Datum zpracování:

16.04.2024

Zpracovali: Jakub Novotný, Jan Ezr a Jakub Frýdek



Zadání

1. Zapojte lokální síť s DHCP.
2. Ve virtuálních strojích (nebo na vlastních počítačích) vytvořte každému členovi týmu uživatelský účet se stejným uživatelským jménem jako v LIANE.
3. Pomocí **ssh-keygen** vytvořte na fyzickém počítači certifikáty a umístěte je na virtuální stroje.
4. Po úspěšné instalaci certifikátů zakažte na virtuálech přihlašování heslem.
5. Proces dokumentujte screenshoty a kopiemi relevantních příkazů.





Postup

1. vytvořil jsem si virtuální počítač a vněm jsem vytvořil uživatele svých kolegů ze skupiny za pomoci příkazu **`sudo adduser --force-badname jan.ezr`**

```
student@virtcli: ~  
File Edit View Search Terminal Help  
student@virtcli:~$ sudo adduser --force-badname jan.ezr  
[sudo] password for student:  
Allowing use of questionable username.  
Adding user `jan.ezr' ...  
Adding new group `jan.ezr' (1001) ...  
Adding new user `jan.ezr' (1001) with group `jan.ezr' ...  
Creating home directory `/home/jan.ezr' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for jan.ezr  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] y  
student@virtcli:~$ sudo adduser --force-badname jakub.frydek  
Allowing use of questionable username.  
Adding user `jakub.frydek' ...  
Adding new group `jakub.frydek' (1002) ...  
Adding new user `jakub.frydek' (1002) with group `jakub.frydek' ...  
Creating home directory `/home/jakub.frydek' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for jakub.frydek  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] y  
student@virtcli:~$ sudo adduser --force-badname jakub.novotny  
Allowing use of questionable username.  
Adding user `jakub.novotny' ...  
Adding new group `jakub.novotny' (1003) ...  
Adding new user `jakub.novotny' (1003) with group `jakub.novotny' ...  
Creating home directory `/home/jakub.novotny' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for jakub.novotny  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:
```





2. za pomoci příkazu `ssh-keygen` jsme vytvořili certifikáty a umístili na virtuální stroje

```
jan.ezr@a0311: ~  
File Edit View Search Terminal Help  
jan.ezr@a0311:~$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/j/jan.ezr/.ssh/id_rsa):  
/home/j/jan.ezr/.ssh/id_rsa already exists.  
Overwrite (y/n)? y  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/j/jan.ezr/.ssh/id_rsa  
Your public key has been saved in /home/j/jan.ezr/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:GA3P9tpI97dJrTewt3DD3cCL2nYFKWA1/ildsRjdTpI jan.ezr@a0311.nti.tul.cz  
The key's randomart image is:  
+----[RSA 3072]-----+  
| . .o..o.|  
| = o. .E.=|  
| . =. ...*|  
| + . .+oo.|  
| . S o ..*|  
| . = . +.++|  
| o . o.*=+|  
| o.++*o|  
| ....=oo|  
+----[SHA256]-----+  
jan.ezr@a0311:~$
```

3. Po úspěšné instalaci certifikátu jsme zkopírali certifikáty za pomoci `ssh-copy-id`.

```
jan.ezr@a0311: ~  
File Edit View Search Terminal Help  
jan.ezr@a0311:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub jakub.frydek@192.168.56.101/  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/j/jan.ezr/.ssh/id_rsa.pub"  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already  
installed  
/usr/bin/ssh-copy-id: ERROR: ssh: Could not resolve hostname 192.168.56.101/: Name or service not known  
jan.ezr@a0311:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub jan.ezr@192.168.56.101  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/j/jan.ezr/.ssh/id_rsa.pub"  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already  
installed  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install t  
he new keys  
jan.ezr@192.168.56.101's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'jan.ezr@192.168.56.101'"  
and check to make sure that only the key(s) you wanted were added.  
jan.ezr@a0311:~$
```





4. Jsme zakázali při hlasování heslem na virtuálech

```
jakub.frydek@virtcli: ~  
File Edit View Search Terminal Help  
jan.ezr@a0311:~$ ssh jakub.frydek@192.168.56.101  
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-97-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
System information as of Tue Apr 30 01:00:59 PM UTC 2024  
  
System load:          0.0732421875  
Usage of /:           31.9% of 19.51GB  
Memory usage:         17%  
Swap usage:           0%  
Processes:            109  
Users logged in:      1  
IPv4 address for enp0s3: 10.0.2.15  
IPv4 address for enp0s8: 192.168.1.113  
IPv6 address for enp0s8: fdb7:3f96:41e6::e6d  
IPv6 address for enp0s8: fdb7:3f96:41e6:0:a00:27ff:fea8:4293  
IPv4 address for enp0s9: 192.168.56.101  
  
Expanded Security Maintenance for Applications is not enabled.  
  
21 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
3 additional security updates can be applied with ESM Apps.  
Learn more about enabling ESM Apps service at https://ubuntu.com/esm  
  
*** System restart required ***  
Last login: Tue Apr 30 13:00:59 2024 from 192.168.56.1  
jakub.frydek@virtcli:~$
```



Závěr

Jako první jsme zkontrovali jestli byl stroj připojen k DHCP což byl. Poté jsme si vytvořili virtuální počítače podle návodu z druhé úlohy a pojmenoval jsem je jako v liane (jmeno.prijmeni) za pomoci příkazu `ssh adduser -force-badname jmeno.prijmeni`. Po tom jsme si za pomoci příkazu `ssh keygen` vytvořili certifikát a za pomoci `ssh-copy-id` jsme certifikát zkopírovali a odstranili možnost přihlášení heslem.