

Demonstration of Windows XP Privilege Escalation Exploit

This article is a tutorial on how to trick Windows XP into giving you system privileges. Using simple command line tools on a machine running Windows XP, we will obtain system level privileges. The system run level is higher than administrator, and has full control of the operating system and it's kernel. On many machines this can be exploited even with the guest account. This system account allows for several other things that aren't normally possible (like resetting the administrator password).

The Local System account is used by the Windows OS to control various aspects of the system (kernel, services, etc); the account shows up as SYSTEM in the Task Manager process list, as seen in the following screen shot:

Local System differs from an Administrator account in that it has full control of the operating system, similar to root on a *nix machine. Most System processes are required by the operating system, and cannot be closed, even by an Administrator account; attempting to close them will result in a error message.

The following quote from Wikipedia explains this in a easy to understand way:

Quote: In Windows NT and later systems derived from it (Windows 2000, Windows XP, Windows Server 2003 and Windows Vista), there may or may not be a superuser. By default, there is a superuser named Administrator, although it is not an exact analogue of the Unix root superuser account. Administrator does not have all the privileges of root because some superuser privileges are assigned to the Local System account in Windows NT.

Under normal circumstances, a user cannot run code as System, only the operating system itself has this ability, but by using the command line, we will trick Windows into running our desktop as System, along with all applications that are started from within.

Procedure to get system level access and privilege escalation in windows I will now walk you through the process of obtaining **SYSTEM** privileges and a demonstration of this Windows XP admin exploit / super user hack

To start, lets open up a command prompt (Start > Run > cmd > [ENTER]) .

At the prompt, enter the following command, then press [ENTER]:

Code:

at

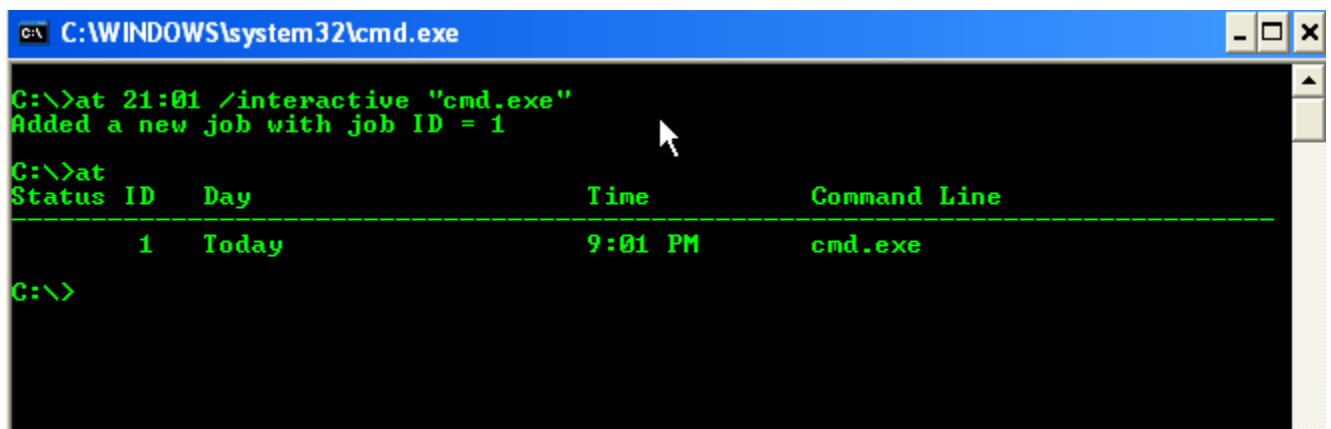
If it responds with an "access denied" error, then we are out of luck, and you'll have to try another method of privilege escalation; if it responds with "There are no entries in the list" (or sometimes with multiple entries already in the list) then we are good. Access to

the at command varies, on some installations of Windows, even the Guest account can access it, on others it's limited to Administrator accounts. If you can use the at command, enter the following commands, then press [ENTER]:

Code:

```
at 21:01 /interactive "cmd.exe"
```

Lets break down the preceding code. The "at" told the machine to run the at command, everything after that are the operators for the command, the important thing here, is to change the time (24 hour format) to one minute after the time currently set on your computers clock, for example: If your computer's clock says it's 4:30pm, convert this to 24 hour format (16:30) then use 16:31 as the time in the command. If you issue the **at** command again with no operators, then you should see something similar to this:



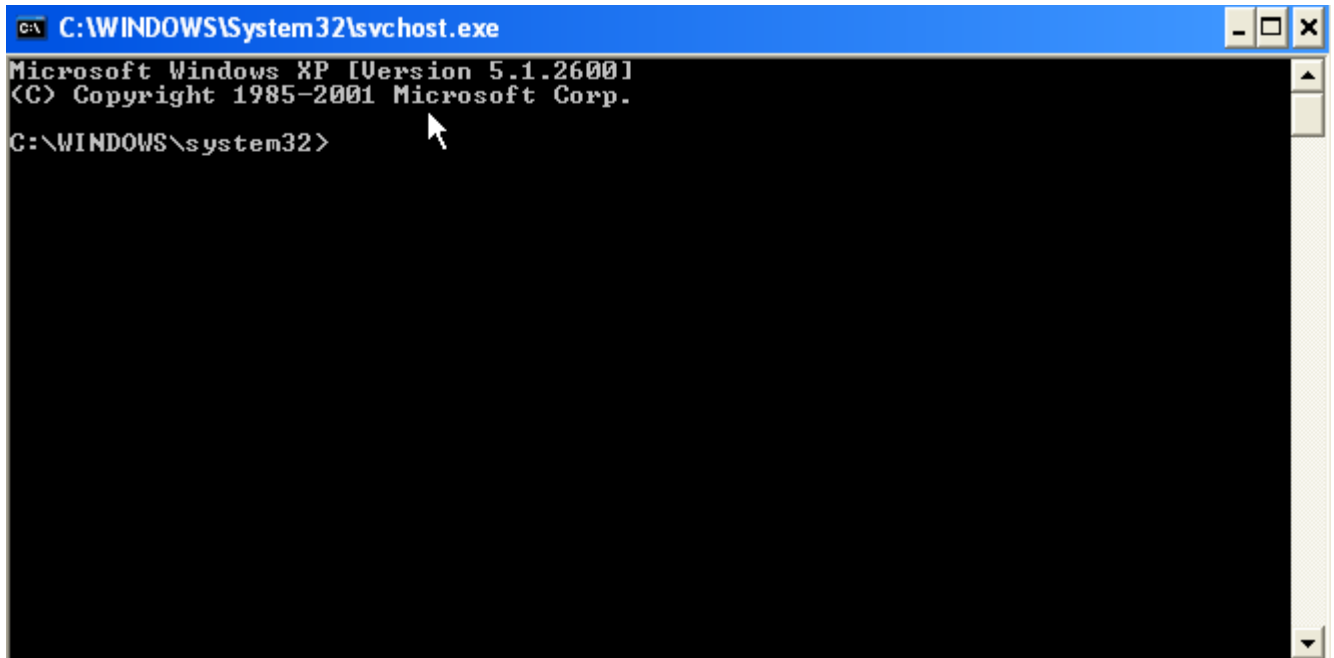
The screenshot shows a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The prompt is "C:\>". The user has entered the command "at 21:01 /interactive \"cmd.exe\"". The output is "Added a new job with job ID = 1". Below this, the user has entered "at", and the output shows a table of scheduled tasks.

Status	ID	Day	Time	Command Line
	1	Today	9:01 PM	cmd.exe

The prompt is now "C:\>".

When the system clock reaches the time you set, then a new command prompt will magically run. The difference is that this one is running with system privileges (because it was started by the task scheduler service, which runs under the Local System account). It should look like

this:

A screenshot of a Windows XP command prompt window. The title bar is blue and reads "C:\WINDOWS\System32\svchost.exe". The window content is black with white text. It shows "Microsoft Windows XP [Version 5.1.2600]" and "<C> Copyright 1985-2001 Microsoft Corp." followed by the prompt "C:\WINDOWS\system32>". A mouse cursor is pointing at the prompt.

```
C:\WINDOWS\System32\svchost.exe
Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

You'll notice that the title bar has changed from cmd.exe to svchost.exe (which is short for Service Host). Now that we have our system command prompt, you may close the old one. Run Task Manager by either pressing CTRL+ALT+DELETE or typing taskmgr at the command prompt. In task manager, go to the processes tab, and kill explorer.exe; your desktop and all open folders should disappear, but the system command prompt should still be there.

At the system command prompt, enter in the following:

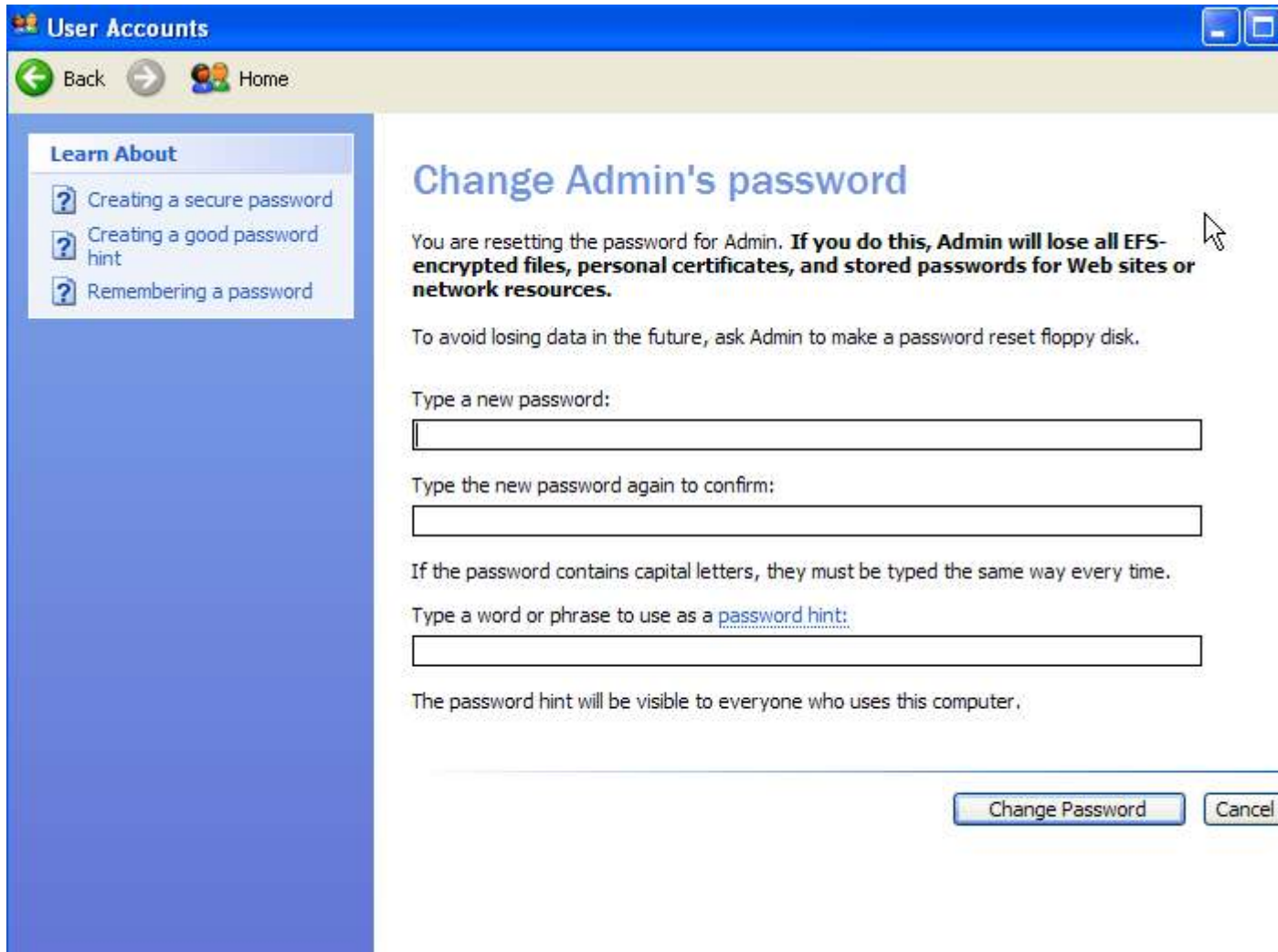
Code:

```
explorer.exe
```

A desktop will come back up, but what this? It isn't your desktop. Go to the start menu and look at the user name, it should say "SYSTEM". Also open up task manager again, and you'll notice that explorer.exe is now running as SYSTEM. The easiest way to get back into your own desktop, is to log out and then log back in.



Now that we have **SYSTEM** access, everything that we run from our explorer process will have it too, browsers, games, etc. You also have the ability to reset the administrator's password, and kill other processes owned by **SYSTEM**. You can do anything on the machine, the equivalent of root; you are now God of the Windows machine. I'll leave the rest up to your imagination.



Resetting Administrator's password