

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to bypass authentication on Windows Server 2008 R2](#)

SIM-4086413 - August 3, 2019, 1:17 pm

We will be looking at how easy it is to bypass authentication and reset the administrator password on a Windows Server 2008 R2 installation. This technique requires us to have physical access to the machine that is running the Windows server or have access to the management interface of the hypervisor when Windows Server 2008 R2 is running virtualized. This is not a great 'hacking' technique that can be used to pwn all Windows installations but it is more a sysadmins last resort trick when nothing else works on a forgotten password. And in some other situations it is definitely useful and comes in handy when you need it. Especially at the point when you've compromised the administration panel of the hypervisor software. This kind of access allows you to control the virtual machines as if you had physical access to it, including the ability to use boot disk and modify system files. Alternatively you can apply this technique when have some kind of physical access to a host.

A couple months ago I was conducting a penetration test on a staged Windows environment that was running on a VMware hypervisor. The environment contained a domain controller and 3 application servers that were running Windows Server 2008 R2. Other then the Windows machines I also encountered a few Linux based network and back-up devices. As it was not very hard to compromise the machines on this network I was able to access the VMware vSphere administration panel as administrator in a very early stage of the penetration test. This access level allowed me to reset the administrator password using a boot CD and finally login to the Windows Server with administrator privileges. In the follow sections I will explain how I did this and how you can secure your Windows installations from applying this technique.

Resetting the administrator password on Windows Server 2008 R2

The starting point of this tutorial is a machine with Windows Server 2008 R2 Enterprise that has been booted with a boot CD. In this example we've used the Hiren boot CD (HBCD) but you can use any alternative boot CD as well, including a Windows installation disk. After booting the system from the boot CD navigate to the following directory of the drive that contains the Windows Server 2008 R2 installation:

Code /Windows/System32

In this directory you will find an executable file named 'Utilman.exe'. Utilman is a small utility that is used to configure accessibility options such as the magnifier and the on-screen keyboard. What's so special about Utilman.exe is that we are able to execute this program before logging in the system. We can do this by clicking the small 'accessibility' button in the bottom left corner of the Windows logon menu:

The 'accessibility' button to launch Utilman.exe displayed at the left.

Now that we have access to the /Windows/System32 directory we can swap out the Utilman.exe program with the cmd.exe program. When we swap out these applications we can start cmd.exe with system privileges instead of Utilman.exe when pressing the accessibility button in the logon screen. From this point we are able to reset the administrator password and use it to login.

First we will rename the Utilman.exe program to Utilman.exe.old as following:

Rename Utilman.exe to Utilman.exe.old

The next step is to rename cmd.exe to Utilman.exe as following:

Rename cmd.exe to Utilman.exe. You can also copy cmd.exe and rename it so you can still use cmd.exe after logging in to Windows.

Now that we've swapped Utilman.exe with cmd.exe we only have to reboot the machine into Windows and click the accessibility button on the login screen. As expected this will launch a command line instead of the accessibility options:

Utilman.exe as cmd.exe

The next step is to change the administrator password as following:

Change the administrator password.

Finally we can logon Windows with the new administrator credentials:

Windows Server 2008 R2 Enterprise signing in with the new administrator credentials.

Lessons learned

In this article we've seen how easy it is to get administrator access to a Windows Server 2008 R2 Enterprise host after we've compromised the hypervisor. Just the fact that we were able to boot the machine with a boot CD allowing us to tamper with data on the hard drive is a serious security issue with serious consequences. There are several ways to prevent and mitigate these kind of attacks. One of them is to secure the BIOS with a password so that an attacker cannot change the boot options for the machine, thus unable to boot from the boot CD. A more effective way would be to apply full disk encryption which encrypts all the data on the disk preventing the attacker from tampering with it.

I hope you've found this small tutorial useful in some way. If you're looking to try this technique or to practice penetration testing techniques on Windows Server 2008 machines, I can recommend you to install Metasploitable 3 which is based on Windows Server 2008.

Credits: www.hackingtutorials.org