Metasploitable2

What is Metasploitable?

Metasploitable is a machine that was created to practice pentesting, it has a lot of vulnerabilities that we can use to practice.

My goal is to discover as many vulnerabilities as possible, to the best of my limited knowledge.

I will upload my reports to GitHub: https://github.com/Noli18P

How will my reports be structured?

I will start with an enumeration to discover ONLY the open ports and once I have the list, I will use each one of them to try to discover vulnerabilities and write a small report about it, without rushing and trying to learn as much as I can.

Enumeration

To know the open ports I need to run nmap together with a series of parameters, I will divide this scan in two parts

→ A scan to get only open ports.
→ Another much deeper scan to get versions and run some scripts.

nmap -p- -sS --min-rate 5000 --open -vvv 192.168.56.101 -o allPorts.txt

How does the command work?

→ **-p-** To scan all 65535 ports.
→ **-sS** For scanning over TCP.
→ **--min-rate 5000** It allows me to choose the number of packets per second to be sent.
→ **--open** To show only open ports.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

Now thanks to this super fast scan it allows me to save a lot of time and focus only on the open ports:

⇒ 21,22,23,25,53,80,11,139,445,512,513,514,1099,1524,2049,2121,3306,
⇒ 3632,5432,5900,6000,6667,6697,8009,8180,8787,35331,38712,
⇒ 46167,53241

Some of these ports are common such as FTP, SSH, HTTP, telnet, smpt, etc.

Once the ports are open I can run the second scan which will allow me to get much more information about the ports:

nmap -p (allports) -sV -sC -T5 -vvv -o deepScan.txt

How does the command work?

→ **-p** To specify the ports.
→ **-sV** To obtain the versions of the services that are being executed.
→ **-sC** To run some common scripts and try to obtain more information.
→ **-T5** To increase the speed to the maximum level.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

RPCBIND - 111

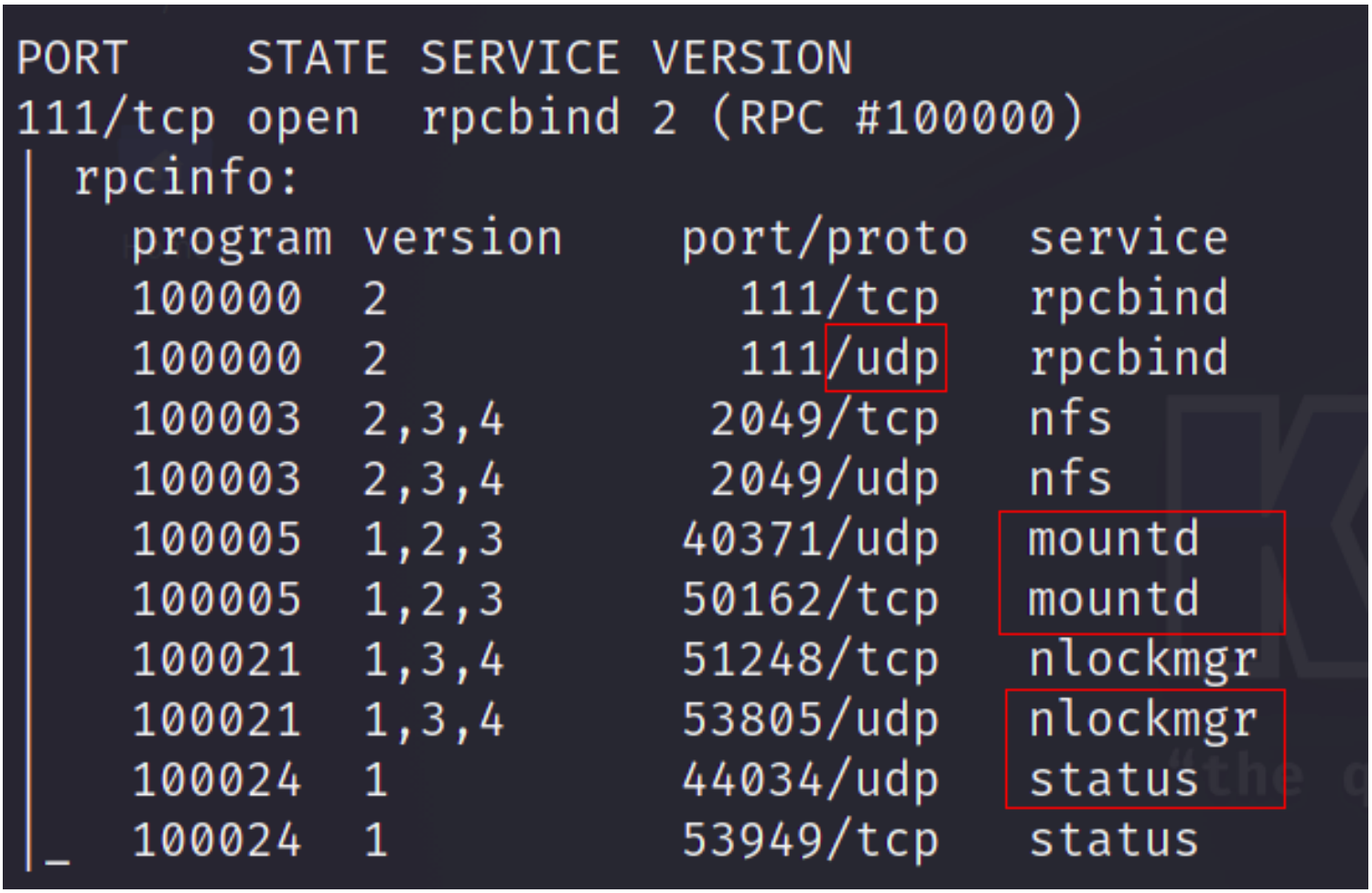
RCPBind is part of the **Open Network Computing** protocol and is listening for requests.

However, it does **NOT actually handle the requests itself** but "forgets" them and **checks which port and service can resolve the request**.

Because this protocol actually maps the program numbers and ports we can get much more information and "hidden" ports that we normally could not see and for this I performed the following scan:

nmap -sC -sV metasploitable -p 111 -o rcpbind.txt

And I got much more information, for example ports running on TCP and UDP, as well as the corresponding services.



In the screenshot we can see a series of columns:

→ **program**: shows the number of the program or service running on the port.

→ **port/proto**: Shows the port number and on which protocol it is running, it can be TCP and UDP.

→ **service**: Shows the name of the program that is identified thanks to the number indicated in the column "program".

The programs shown in the screenshot have the following functions:

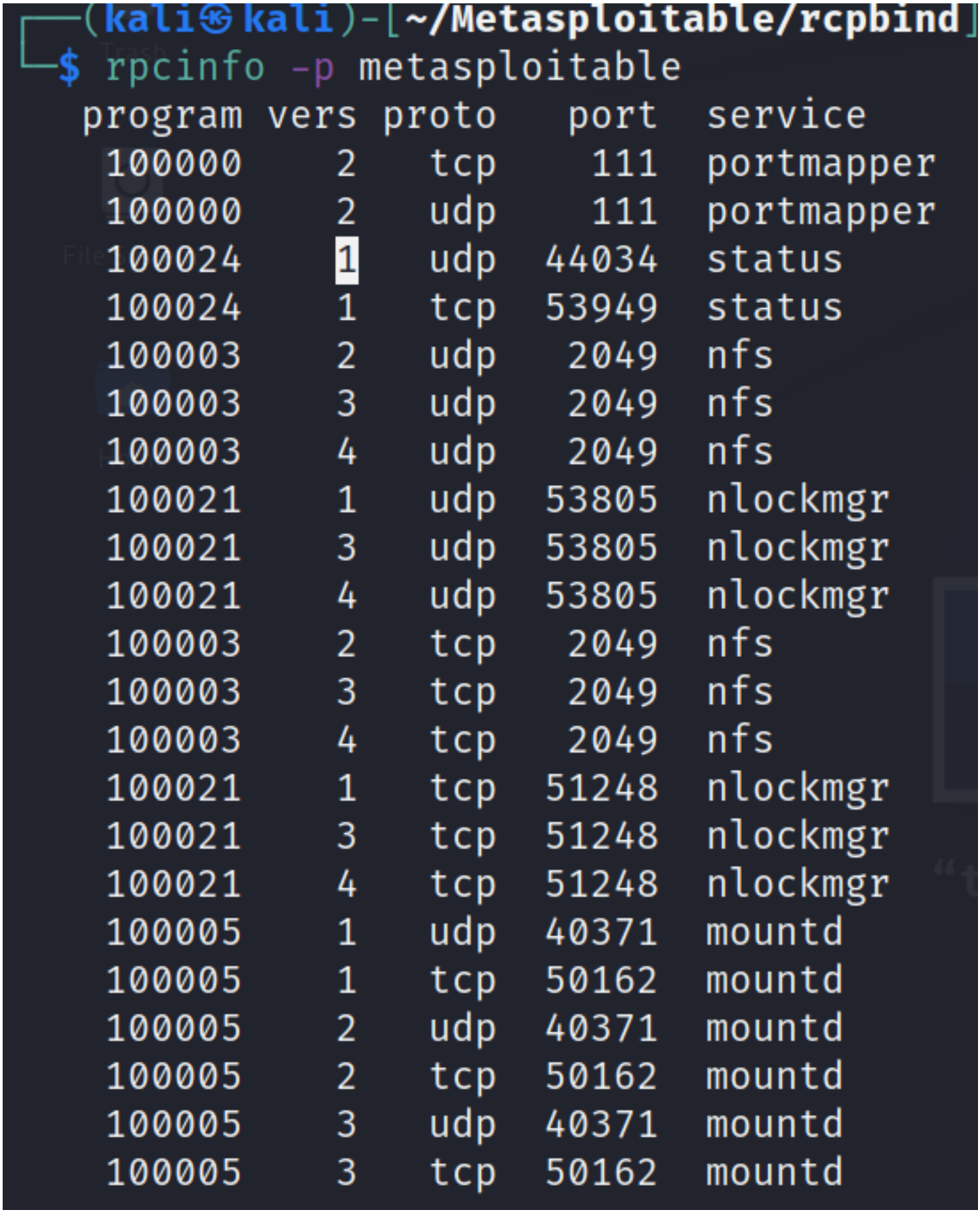
→ **rpcbind**: It is responsible for adding the numbers to each program.

→ **nfs** (Network File System): it is a service used to manage the mounting of NFS network folders called mountd.

→ **nlockmgr**: Network Lock Manager is a service that handles client requests to lock a file.

I am still learning about RPCBind but I found a very good tool that will give you even more information about port 111, it is called rpcinfo and to use it you need to run the following command:

rpcinfo -p <IP>


(kali㉿kali)-[~/Metasploitable/rcpbind]
$ rpcinfo -p metasploitable
program vers proto port service
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 44034 status
100024 1 tcp 53949 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 4 udp 2049 nfs
100021 1 udp 53805 nlockmgr
100021 3 udp 53805 nlockmgr
100021 4 udp 53805 nlockmgr
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100003 4 tcp 2049 nfs
100021 1 tcp 51248 nlockmgr
100021 3 tcp 51248 nlockmgr
100021 4 tcp 51248 nlockmgr
100005 1 udp 40371 mountd
100005 1 tcp 50162 mountd
100005 2 udp 40371 mountd
100005 2 tcp 50162 mountd
100005 3 udp 40371 mountd
100005 3 tcp 50162 mountd

The importance of this service

Although it is quite complicated but not impossible with the necessary recognition and good techniques this service would allow to execute code on other computers in the network!

Imagine what a malicious attacker could do?

Thanks to @hackerfantastic for teaching me a little more about this port in his book "Hand On Hacking".