

Forum:[Hack Forums](#)

Thread: [\(Kali Linux Tutorial\) How to scan for open ports with built-in Metasploit Scanner](#)

Sigma - July 6, 2019, 2:33 pm

There are multiple scanners you can use for open ports using Metasploit. But for this tutorial, we will just be using the TCP scanner.

You will need to be running Kali Linux in order to complete this tutorial. Or have an installation of the framework.

Step 1: Open up a terminal and type in "msfconsole" to get the Metasploit framework started.

Step 2: If you type in "Search Scanner" you will be able to see all the scanners you are able to use within Metasploit. We are going to be using something called "auxiliary/scanner/portscan/tcp". If you keep scrolling you will eventually find it, or you can add some keywords to make it easier to find.

Step 3: To use this scanner, type "use" followed by the exact scanner "auxiliary/scanner/portscan/tcp"

Step 4: We will then type "show options" so we know what tweaks we need to make to scan our selected target.

Step 5: As you can see, there are multiple different options to choose from, for now, we are going to change the target option (RHOST) to our specific target IP address. To do this we type "set RHOST" followed by the targets IP address.

Step 6: Next we will set the Ports you would like to scan, so just like before we will type "set" followed by the port numbers.

Final step: Type "run" to start the scan!

VoIPv2 - July 6, 2019, 9:03 pm

Any special reason why you choose metasploit for scanning? Nmap pretty much is the goto in my book.

moveddisk - July 6, 2019, 11:10 pm

Its very helpful for me thank u

Sigma - July 7, 2019, 6:06 am

(Jul 6, 2019 09:03 PM)VoIPv2 Wrote: [\[CITE\]](#) Any special reason why you choose metasploit for scanning? Nmap pretty much is the goto in my book.

No particular reason.

Dimeblade - *August 10, 2020, 9:14 am*

Nice tut. I beleive you can also set a list of ips to rhost and can use exploits / brutepass smtp mysql etc. Last time got very few resiults because of vps lag. Havent tried long time though
Your threads are really interesting and can use for good use