[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@62c336ee1d9142b4bd8ef1e81a4bb3c7?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Scan Target and Find Exploit Using Metasploit**

**Using Metasploit and Nmap to scan for vulnerabilities**

we discuss combining Nmap and Metasploit to perform port scanning and enumerate for vulnerabilities.

There are certain cases where we can’t just go and run noisy scans with Nmap on our target due to various reasons. One of these reasons is doing a black box test for your client with a firewall or IDS in place that would thwart or alert sysadmins about your Nmap scans.

So, combining two of the most effective tools used in the arena of penetration testing becomes more sensible and plausible for us. Let's assume that we have a client machine assigned to us to perform port scanning and report vulnerabilities.

**Scanning for open ports on the client machine with Metasploit**

1. We start by launching Metasploit and using the port scanner module.

msf 5> use auxiliary/scanner/portscan/tcp

1. Next, we set the options for this module with ‘show options’.
2. We set the RHOSTS with the IP/IP(s) of our client machine(s) and if we want to customize the scan for specific ports we can do that by changing PORTS.

msf 5 >set PORTS 22,25,80,110,21

4. After running the scan, we will have an output displaying the open ports on the target client machine we specified earlier.

**Combining Nmap with Metasploit for a more detailed and in-depth scan of the client machine**

Once we get a clear vision of the open ports, we can start enumerating them to see and find the running services alongside their version.

msf 5> db\_nmap -sV -p 80,22,110,25 192.168.94.134

And this is what we get