**NMAP**

nmap -sV <machines ip>

nmap is an free, open-source and powerful tool used to discover hosts and services on a computer network. In our example, we are using nmap to scan this machine to identify all services that are running on a particular port. nmap has many capabilities, below is a table summarising some of the functionality it provides.

 Scan Techniques

|  |  |  |
| --- | --- | --- |
| **Switch** | **Example** | **Description** |
| -sS | nmap 192.168.1.1 -sS | TCP SYN port scan (Default) |
| -sT | nmap 192.168.1.1 -sT | TCP connect port scan (Default without root privilege) |
| -sU | nmap 192.168.1.1 -sU | UDP port scan |
| -sA | nmap 192.168.1.1 -sA | TCP ACK port scan |
| -sW | nmap 192.168.1.1 -sW | TCP Window port scan |
| -sM | nmap 192.168.1.1 -sM | TCP Maimon port scan |

 Service and Version Detection

|  |  |  |
| --- | --- | --- |
| **Switch** | **Example** | **Description** |
| -sV | nmap 192.168.1.1 -sV | Attempts to determine the version of the service running on port |
| -sV –version-intensity | nmap 192.168.1.1 -sV –version-intensity 8 | Intensity level 0 to 9. Higher number increases possibility of correctness |
| -sV –version-light | nmap 192.168.1.1 -sV –version-light | Enable light mode. Lower possibility of correctness. Faster |
| -sV –version-all | nmap 192.168.1.1 -sV –version-all | Enable intensity level 9. Higher possibility of correctness. Slower |
| -A | nmap 192.168.1.1 -A | Enables OS detection, version detection, script scanning, and traceroute |