

# CYBERSECURITY

## SCANNING: SCANME.NMAP.COM

### SCANME

The Nmap company has provided an online machine to scan: [scanme.nmap.com](https://scanme.nmap.com) (Detected in a previous lab.)

Perform the following tasks:

1. Run a command line (shell).
2. Proceed to run the *nmap* command with the following option:  
`nmap -h`
3. Take time to review all the options available. Then execute a stealth scan (half open) over the target [scanme.nmap.org](https://scanme.nmap.org) with the command:  
`nmap -sS scanme.nmap.org`  
Interpret the result. What does the status “filtered” indicate?
4. Proceed now to run a deep scan in “connect” mode, remember that although this type of scan is more accurate than the half-scan, by completing the 3-way handshake from TCP we expose ourselves to be detected. What is the command to be executed?
5. Now try to detect the operating system version. What command should you run?