

Nmap

Scans a host and its open ports

```
$ nmap [OPTIONS] TARGET
```

Arguments

- sS SYN scan
- sU UDP scan
- O OS detect
- sV Enumerate versions
- v verbose output
- OA Output all formats
- ON Output nmap
- A Aggressive mode
- badsum sends invalid checksum, firewall will likely respond
- T ^(0,5) Timing template
Increase speed, more visible
- p what ports to scan
- P- scan all ports
- mtu max frag size
- script run script
- f Fragment packets
firewall won't be as likely
- scan-delay
Delay between packet sends