

Practical 5 NMAP

* Theory

• Purpose :-

-> Nmap (Network Mapper) is an open-source tool for network discovery and security auditing. It is widely used by network administrators and security professionals to identify live hosts, open ports, running services, and operating system details of a target system.

• How it works :-

-> Nmap sends specially crafted packets to the target system and analyzes response to determine active hosts and services. It supports multiple scanning techniques, including:

-> TCP SYN Scan (-sS)

-> ~~UDP~~ UDP Scan (-sU)

-> OS Detection (-O)

-> Service Version Detection (-sV)

-> Aggressive Scan (-A)

* Practical

Pre Perform a Basic

Scen nmap

001-shankare@csu-5.nmap ref:001.vulnweb.com
 Starting Nmap 7.80 (https://nmap.org) at 2025-07-11 11:11:45
 Nmap scan report for vulnweb.com (44.221.249.1)
 Host is up (0.11s latency).
 DNS records for 44.221.249.1: 44.221.249.1.vulnweb.com, vulnweb.com
 of shown: DNS filtered (p. ports: no response)
 001 STATE SERVICE
 001cs open: 80/tcp

<target>

Performs an aggressive scan that includes OS detection, version detection, script scanning, and traceroute.

nmmap - A <target>

```

ari-shankar@victor-6 nmap -H testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2021-03-18 21:11:11 UTC
Nmap scan report for testphp.vulnweb.com (44.228.249.1)
Host is up (0.35s latency).
DNS record for 44.228.249.1: id: 44-228-249-1, type: A, class: IN, ttl: 300
of 4096 open TCP ports (NMAP IPID: 55555)
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  HTTPS
Info: ssl: http://www.letsencrypt.org
Nmap scan completed on 2021-03-18 21:11:11 UTC.
NAP done! (1 IP address [1 host up]) scanned in 59.97 seconds.
```


rmmap -91 <target>

```
nmap -sT target IP : Performs a basic scan of the specified IP address to discover open ports and services.  
nmap -sU target IP : Scans only the specified ports on the target IP address.  
nmap -sS target IP : Detects and reports the banners of services running on open ports.  
nmap -O target IP : Attempts to identify the operating system of the target.  
nmap -A target IP : Performs an aggressive scan that includes OS detection, version detection, script scanning, and traceroute.  
nmap -sn target IP : Performs a ping scan to determine which hosts are up without scanning ports.  
nmap -sR target IP : Performs a fire connect scan, establishing a full TCP connection to determine open ports.  
nmap -sV target IP : Performs a SYN scan, which is faster and stealthier than a TCP connect scan. It sends SYN packets and analyzes responses.  
nmap --script scripts target IP : Runs a specific NSE script, e.g., vulnerability script against the target IP address.  
nmap --script all target IP : The switch --script all is used to list the module interfaces and their configurations on the system where Nmap is running. This command provides detailed information about each module's interface, including its categories, file addresses, and other relevant feature parameters.  
nmap -F target IP : Speedtest Port Scan  
nmap -Pn target IP/port : Uses a range of IP addresses in a specific network to discover live hosts and identify open ports and services.  
nmap -PE target IP : It sends all the TCP SYN packets  
nmap -PS target IP : It sends TCP ACK packets
```