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 Scan (-sU)

-> OS Detection (-O)

-> Service Version Detection (-sV)

-> Aggressive Scan (-A)

* Practical

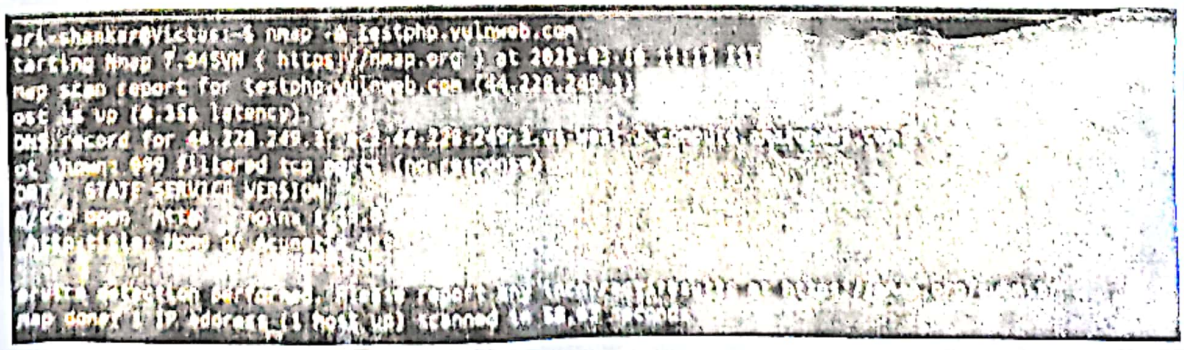
~~Pra~~ Perform a Basic

Scan nmap

<target>

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

nmap -A <target>



Sequential Port Scan

nmap -r <target>