Kabeer Ahmed SE-19028

LAB 11

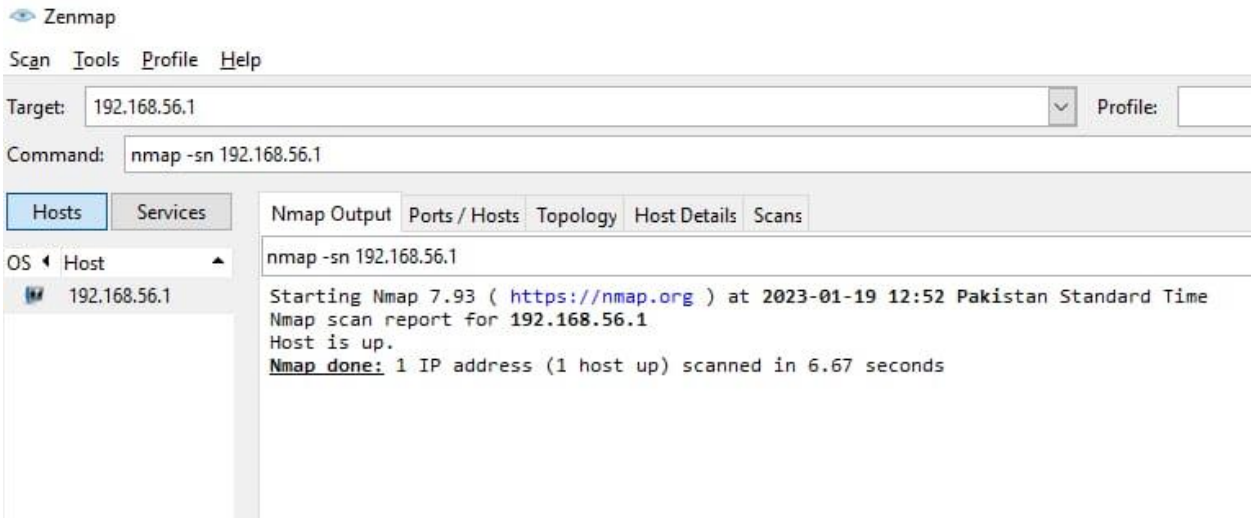
Exercise:

1. What is the difference between a TCP-connect scan and a SYN scan?

A TCP connect scan is a type of port scan that establishes a full TCP connection with the target host in order to determine which ports are open. A SYN scan, also known as a "half-open" scan, is a type of port scan that sends a SYN packet to a target host in order to initiate a connection, but does not complete the handshake process. The target host will respond with a SYN-ACK if the port is open, and a RST if the port is closed. The scanner can determine the state of the port by observing the response. SYN scan is considered to be stealthier than TCP connect scan because it does not establish a full connection with the target host.

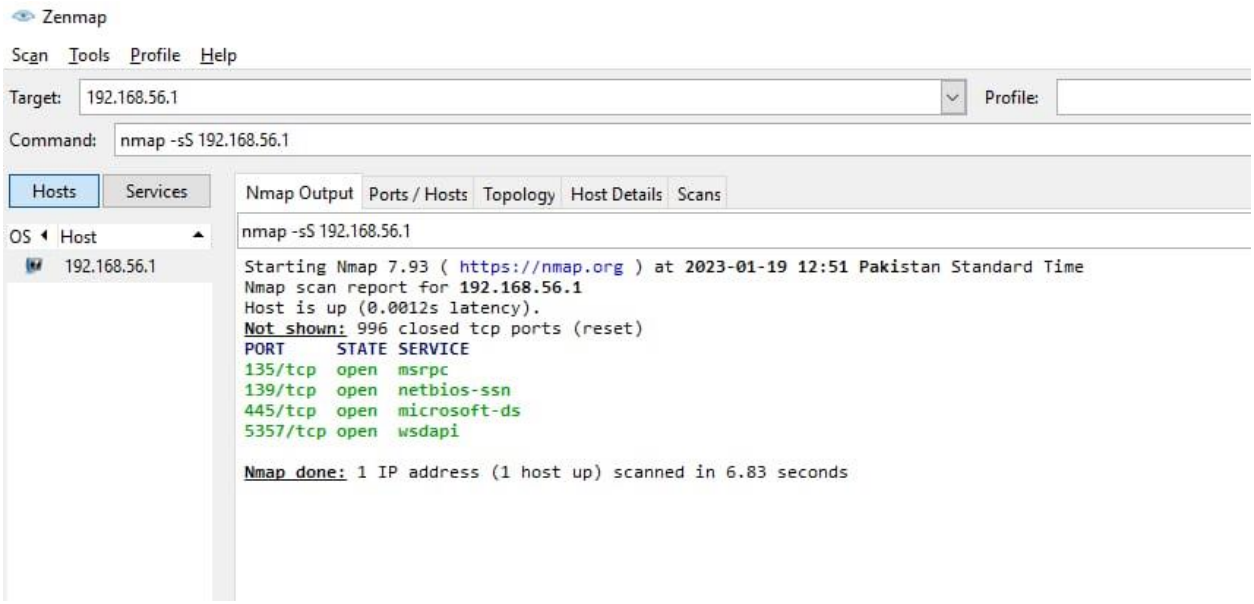
2. What is the purpose of the –sP command line switch? Show practical demonstration.

The -sP command line switch is used in Nmap (Network Mapper) to perform a ping scan. This means that Nmap will send a simple ICMP echo request packet, also known as a "ping", to the target host to determine if it is online and responding. The purpose of this switch is to determine which hosts on a network are live, without attempting to determine open ports or gather detailed information about the target host.



3. What is the purpose of the –sS command line switch? Show practical demonstration.

The -sS command line switch is used in Nmap (Network Mapper) to perform a SYN scan. This is a type of stealthy scan that sends a SYN packet to the target host in order to initiate a connection, but does not complete the handshake process. The target host will respond with a SYN-ACK if the port is open, and a RST if the port is closed. The scanner can determine the state of the port by observing the response. This type of scan is also known as a "half-open" scan because it does not establish a full connection with the target host. The purpose of this switch is to quickly determine which ports on a target host are open without the target host logging the entire connection.



4. What command would you issue to scan for computers running web servers?

To scan for computers running web servers, you could use the following command in Nmap:

nmap -p 80,443 -sV <target>

This command will perform a version scan (-sV) on the target host, checking ports 80 and 443 (HTTP and HTTPS respectively) to determine if a web server is running.

You can also use the -T4 option for a faster scan.

nmap -p 80,443 -sV -T4 <target>

You can also use -A option for more aggressive scan which includes OS detection, version detection, script scanning and traceroute.

nmap -p 80,443 -sV -A <target>

You can also use -Pn option if the target host is blocking ping request

nmap -p 80,443 -sV -Pn <target>

You can also use -oN option to save the scan results to a file

nmap -p 80,443 -sV <target> -oN web_server_scan.txt

Replace <target> with the IP address or hostname of the computer you want to scan.

Please note that, some web servers may not listen to default ports 80 and 443 or may be behind a firewall, in this case you have to scan for different ports or use other techniques to find the web servers.