**Perform Scanning module by using Nmap tool (Download from internet) and scan kalilinux and Windows 7 machine and find open/closed ports and services running on machine.**

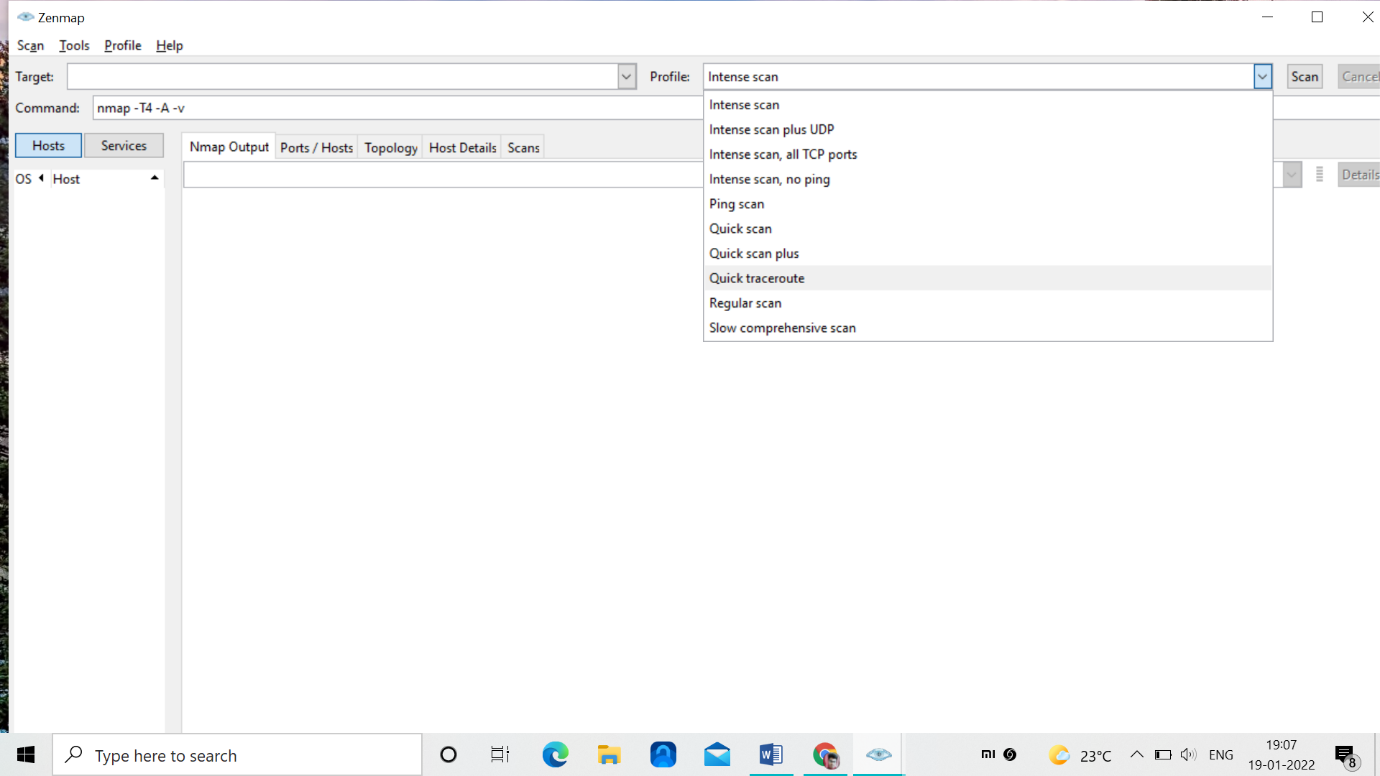
**Hacker Machine: Windows 10**

**Victim machine: kali Linux and Windows 7**

* Download nmap tool from internet from the given link below.

https://nmap.org/download.html

* Install nmap in your system
* After installing nmap will look like

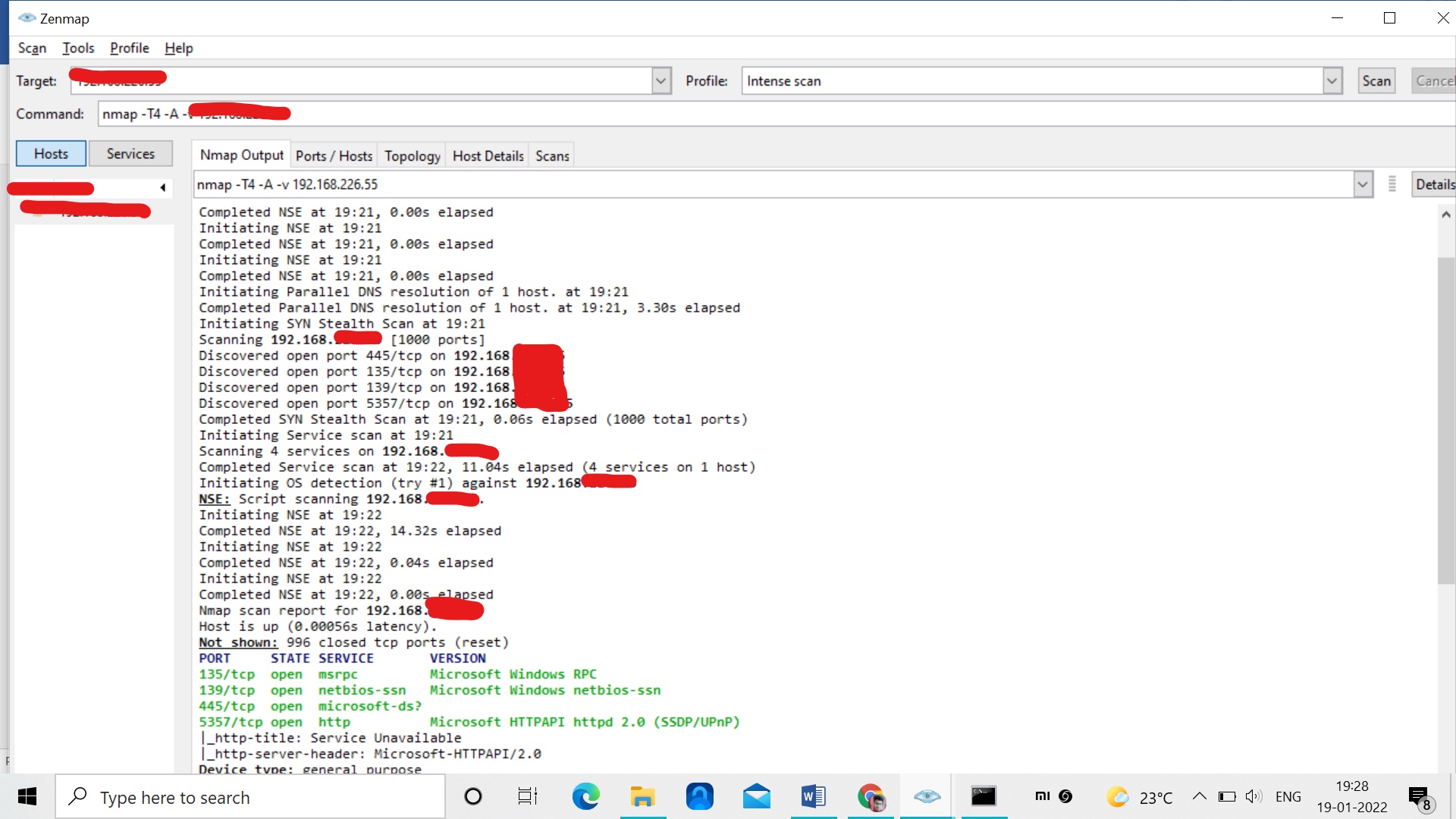


* Here we have type of scans that could be performed on a target
* nmap can be used in two ways

-> diretly through nmap

-> using it in command line (where particular

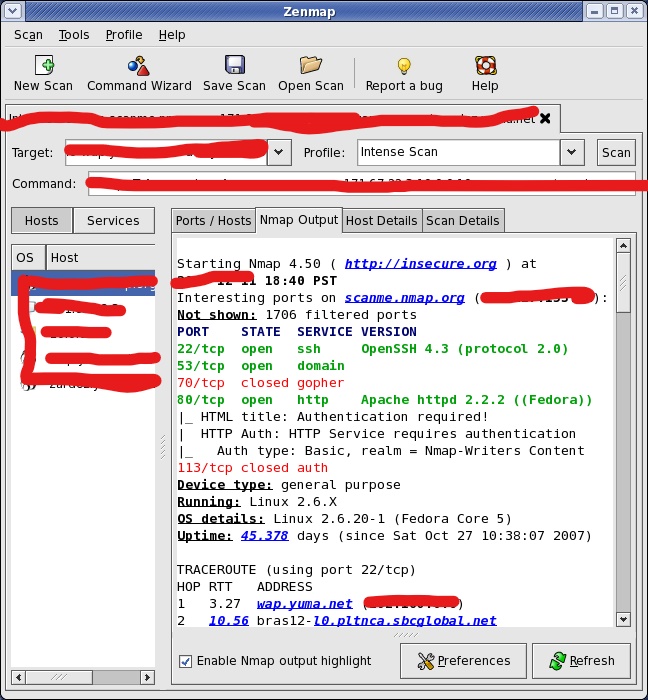
commands will be used)



* Here we will get the information of all the open ports in the windows victim machine by their ip address
* It will show the open TCP ports

135,139,445,5357

* It will also shows the services in the victim machine like msrpc, netbios-ssn Microsoft-ds?,http



* Here the open ports are 22,53,80
* The closed port is 70
* Services are ssh, domain, http

We can scan nmap using command line and some of the commands are note below

**Basic Scanning Commands**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Scan a Single Target | nmap [target] | nmap 192.168.0.1 |
| Scan Multiple Targets | nmap [target1, target2, etc | nmap 192.168.0.1 192.168.0.2 |
| Scan a Range of Hosts | nmap [range of ip addresses] | nmap 192.168.0.1-10 |
| Scan an Entire Subnet | nmap [ip address/cdir] | nmap 192.168.0.1/24 |
| Scan Random Hosts | nmap -iR [number] | nmap -iR 0 |
| Excluding Targets from a Scan | nmap [targets] – exclude [targets] | nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200 |
| Excluding Targets Using a List | nmap [targets] – excludefile [list.txt] | nmap 192.168.0.1/24 –excludefile notargets.txt |
| Perform an Aggressive Scan | nmap -A [target] | nmap -A 192.168.0.1 |

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Perform a Ping Only Scan | nmap -sP [target] | nmap -sP 192.168.0.1 |
| Don’t Ping | nmap -PN [target] | nmap -PN 192.168.0.1 |
| TCP SYN Ping | nmap -PS [target] | nmap -PS 192.168.0.1 |
| TCP ACK Ping | nmap -PA [target] | nmap -PA 192.168.0.1 |
| UDP Ping | nmap -PU [target] | nmap -PU 192.168.0.1 |
| SCTP INIT Ping | nmap -PY [target] | nmap -PY 192.168.0.1 |
| ICMP Echo Ping | nmap -PE [target] | nmap -PE 192.168.0.1 |
| ICMP Timestamp Ping | nmap -PP [target] | nmap -PP 192.168.0.1 |
| CMP Address Mask Ping | nmap -PM [target] | nmap -PM 192.168.0.1 |
| IP Protocol Ping | nmap -PO [target] | nmap -PO 192.168.0.1 |

**How to protect against nmap scans?**

We need to enable filters 7000 to7004 and 7016

These filters will ignore the following types of traffic:

* Blocked or trusted by a traffic management.
* Trusted flow due to trust as in action.
* Blocked or trusted by IP reputation.
* Matches an inspection-bypass rule.