### Intrainz Project Submission

**Footprinting with Nmap (Minor Project )**

**Introduction :**

* Footprinting is the process of gathering information about a target or network.
* Nmap is a network exploration tool that can be used for footprinting.
* With Nmap, you can scan a target for open ports, services, operating systems, and other information.
* Nmap also has many potential uses beyond footprinting, such as creating password crackers and network scanners.

**Scanning the Target :**

**Step-1** : Identifying the target and start scanning with Nmap .

* Select the target **nmap scanme.nmap.org**
* Enter the target in the linux terminal and start scanning .

## step-1.JPG

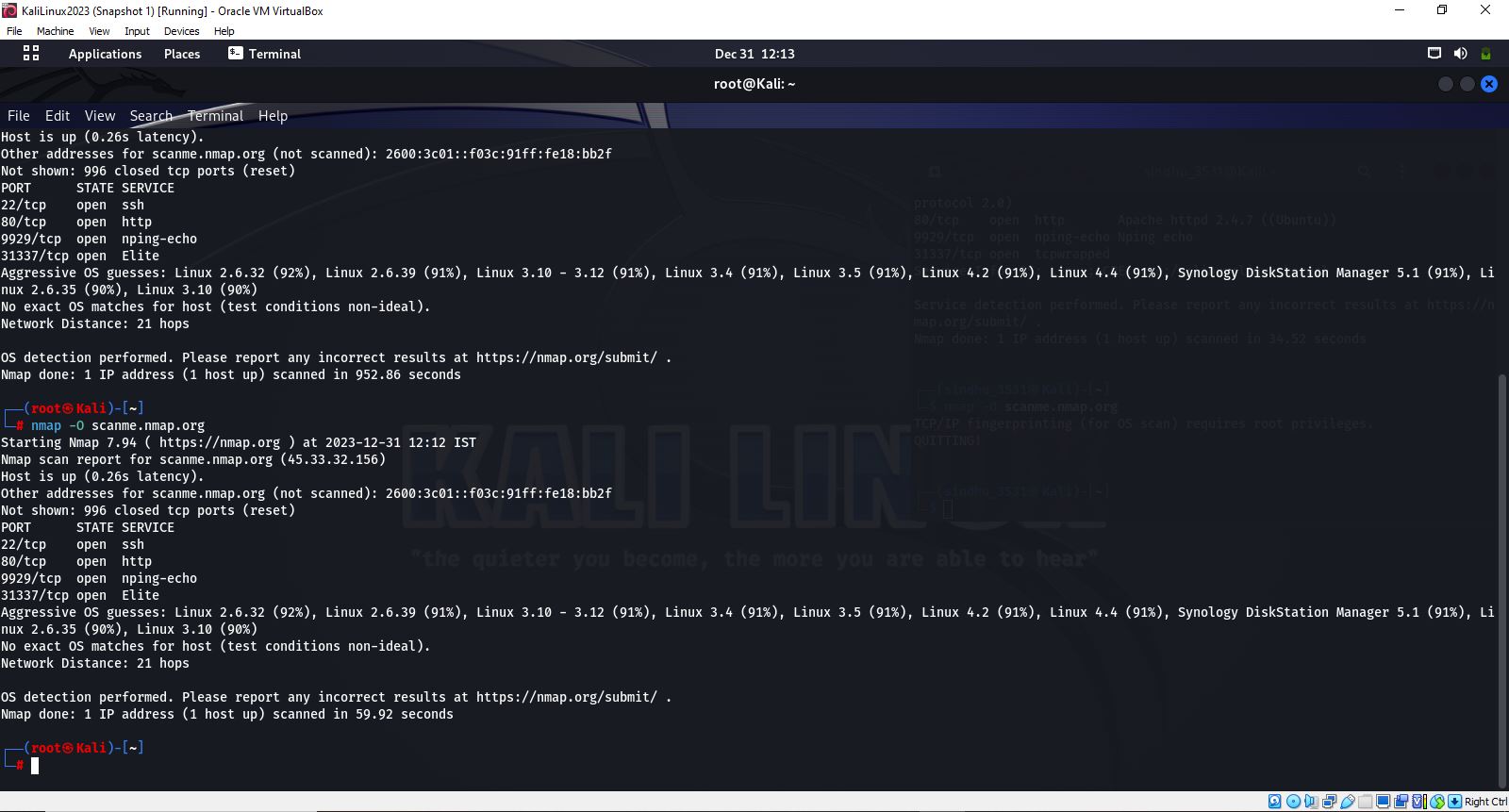
**Step-2 :** Performing Service Version Detection on the Target.

* Version Detection is used with the -sV command, and it allows the user to collect information about the port.
* This can include the version number, the service type, the operating system, the hostname, etc.
* The following command is used for performing the service version detection network scanning (nmap –sV <target>)(nmap –sV scanme.nmap.org)



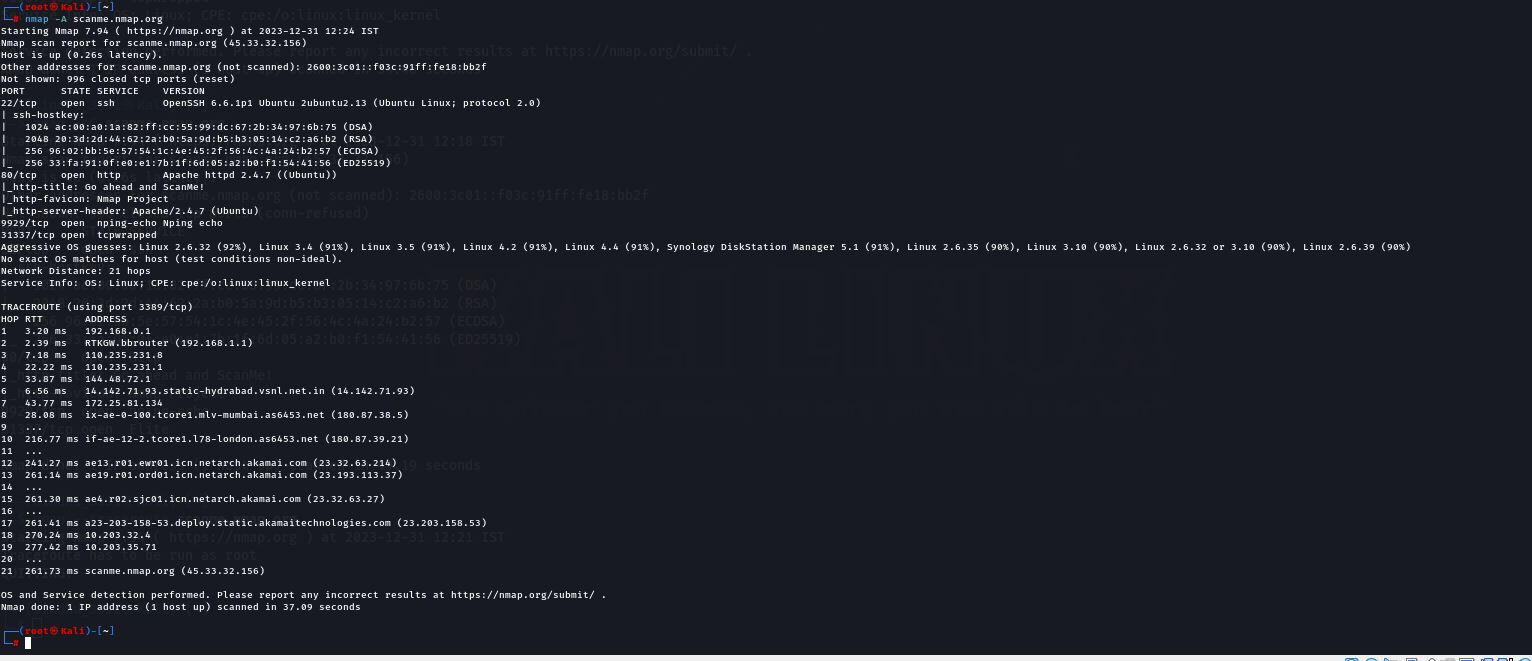
**Step-3 :** Performing OS detection Network scanning on the target

* Nmap OS detection is a quick and powerful way to determine what operating system a remote device is running**.**
* The following command is used for scanning the OS detection network scanning .
* That is “Nmap –O <target> (example: nmap –O scanme.namp.org).



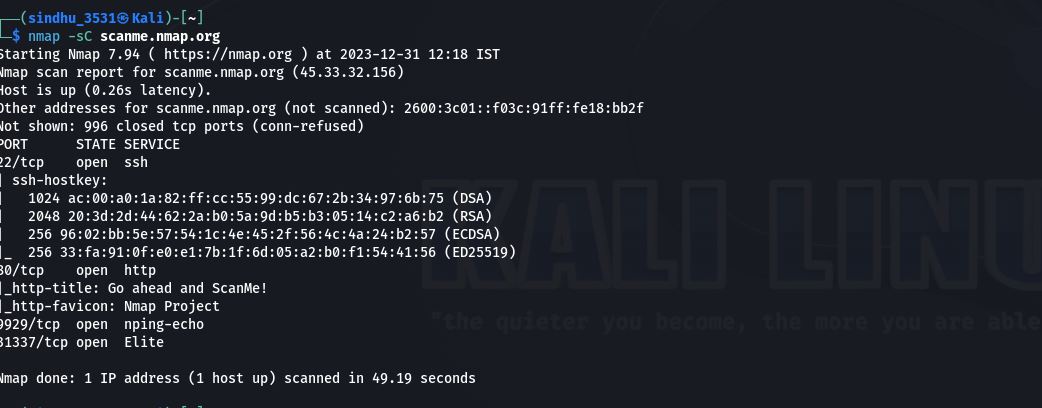
**Step-4 :** Performing Aggressive scan on the target

* Aggressive mode enables OS detection ( -O ), version detection ( -sV ), script scanning ( -sC ), and traceroute ( --traceroute ).
* This mode sends a lot more probes, and it is more likely to be detected, but provides a lot of valuable host information.
* This scan mode can provide more detailed information about the systems and services installed on the target system, but it also requires more time and resources to run.
* To perform aggressive scanning we use the following command
* Nmap –A <target> (nmap –A scanme.nmap.org)



**Step-5** : Performing Scripting Scanning on the target (-sC)

* Script scanning is a technique used in Nmap to execute predefined scripts against target systems to gather various types of information.
* These scripts are written in the Lua programming language and are designed to probe specific services, operating systems, and applications.
* Nmap script scanning can help identify vulnerabilities, misconfigurations , and potential security risks in target systems.
* To perform scripting scanning we use the following command.
* Nmap –sC <target> (nmap –sC scanme.nmap.org)



**Step-6 :** Performing traceroute scanning on the target.(--script)

* Script scanning is a technique used in Nmap to execute predefined scripts against target systems to gather various types of information.
* These scripts are written in the Lua programming language and are designed to probe specific services, operating systems, and applications.
* Nmap script scanning can help identify vulnerabilities, misconfigurations, and potential security risks in target systems.
* To perform script scanning we use the following command .
* Nmap –script<target> (nmap –script scanme.nmap.org)

