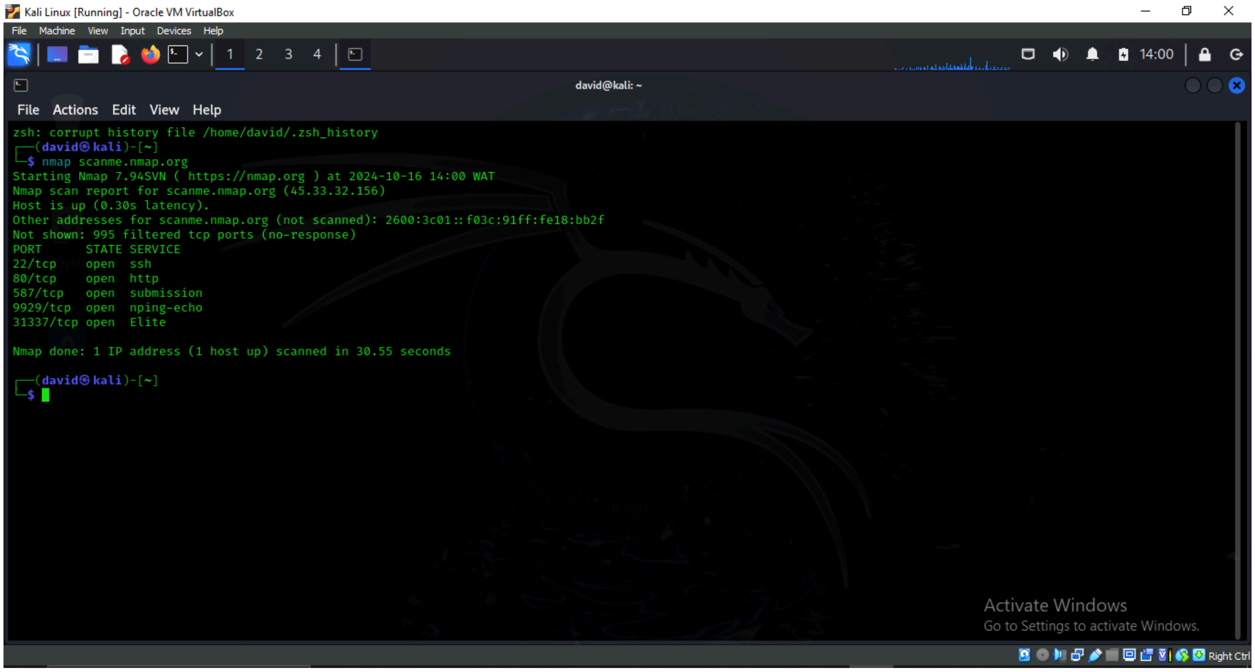
LAB 2:

SCANNING A HOST USING NMAP

TOOL: KALI LINUX

STEP 1: Scan the following site: scanme.nmap.org

Command: nmap scanme.nmap.org


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:00
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

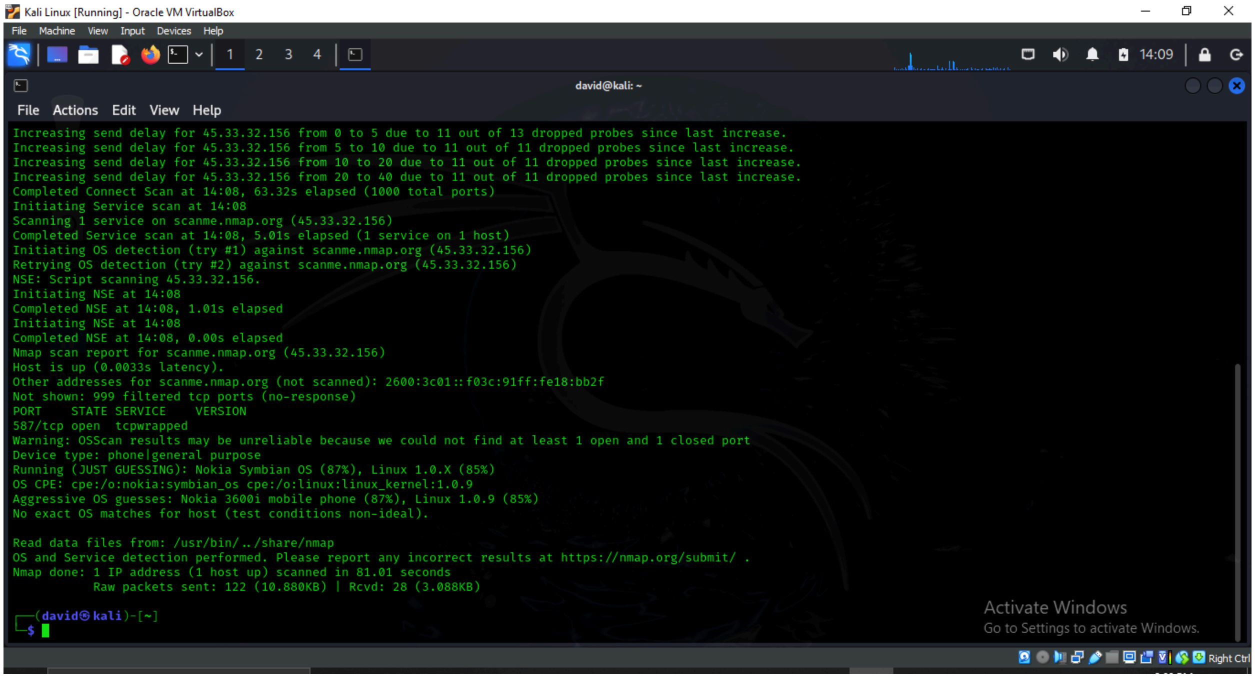
```
zsh: corrupt history file /home/david/.zsh_history
┌──(david㉿kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 14:00 WAT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
587/tcp   open  submission
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 30.55 seconds

┌──(david㉿kali)-[~]
└─$ 
```

STEP 2:In this step, we will be scanning the same target,but with a more advanced scan. We want to determine the versions for the services running on each port, so that we can determine if they are out of date and potentially vulnerable to exploitation and also determine the operating system of the webserver running the target site. We will run the following scan to determine this : sudo nmap -v -sT -sV -O scanme.nmap.org

:



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
14:09
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 20 to 40 due to 11 out of 11 dropped probes since last increase.
Completed Connect Scan at 14:08, 63.32s elapsed (1000 total ports)
Initiating Service scan at 14:08
Scanning 1 service on scanme.nmap.org (45.33.32.156)
Completed Service scan at 14:08, 5.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 14:08
Completed NSE at 14:08, 1.01s elapsed
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0033s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
587/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose
Running (JUST GUESSING): Nokia Symbian OS (87%), Linux 1.0.X (85%)
OS CPE: cpe:/o:nokia:symbian_os cpe:/o:linux:linux_kernel:1.0.9
Aggressive OS guesses: Nokia 3600i mobile phone (87%), Linux 1.0.9 (85%)
No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.01 seconds
           Raw packets sent: 122 (10.880KB) | Rcvd: 28 (3.088KB)

┌──(david㉿kali)-[~]
└─$ 
```