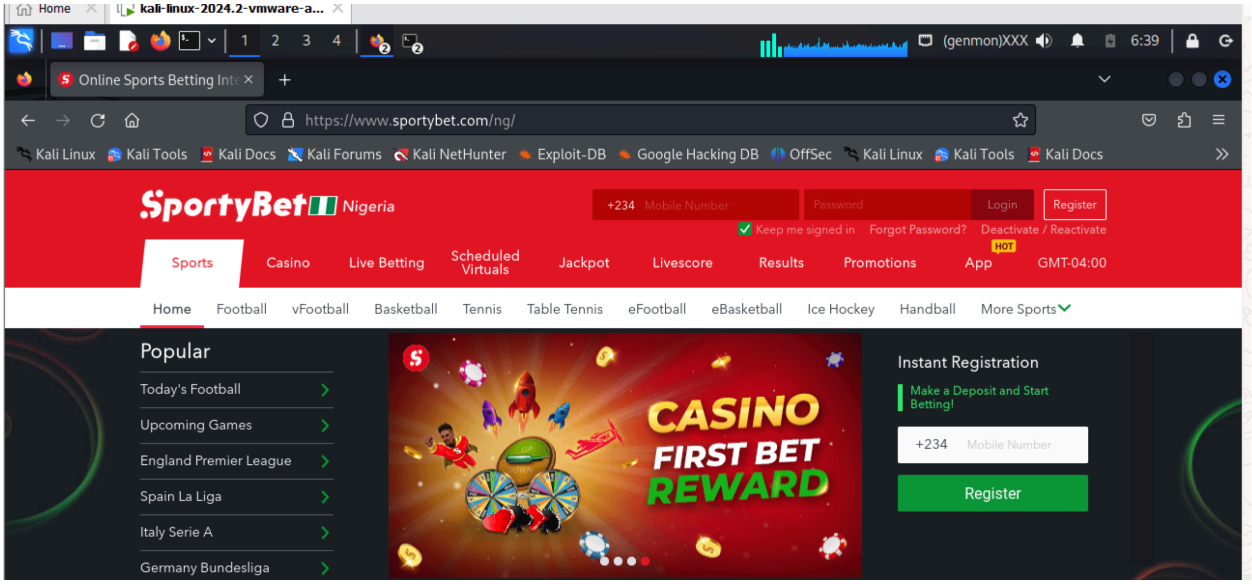

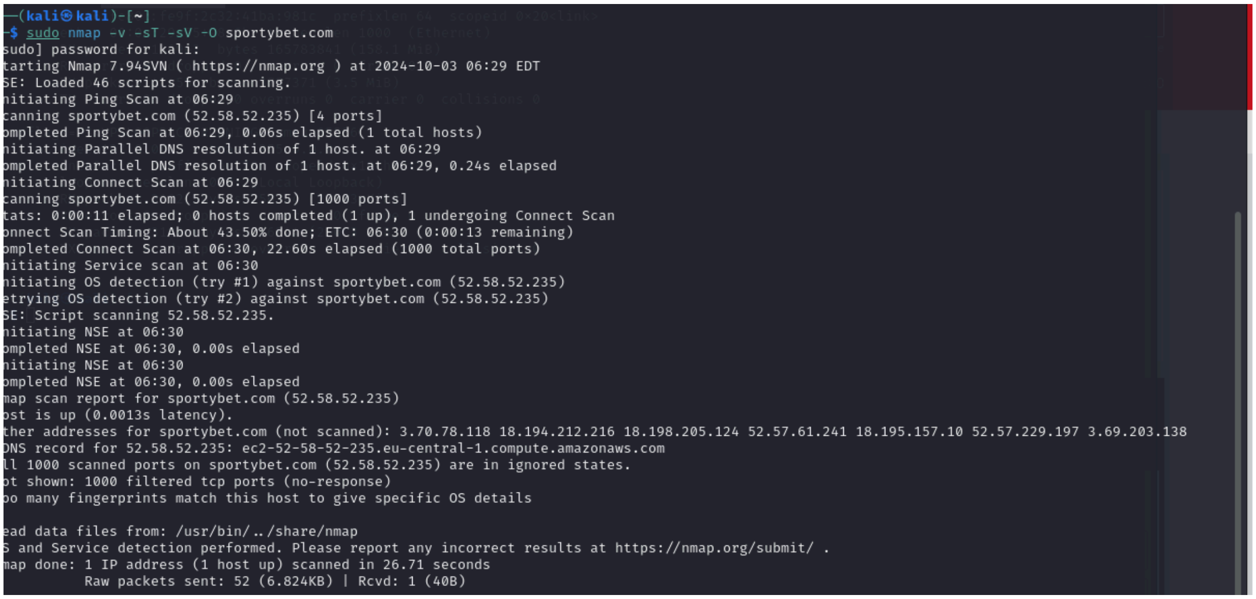

```
—(kali㉿kali)-[~]
-$ sudo nmap -v -sT -sV -O sportybet.com
sudo] password for kali:
tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 06:29 EDT
SE: Loaded 46 scripts for scanning.
nitiating Ping Scan at 06:29
canning sportybet.com (52.58.52.235) [4 ports]
ompleted Ping Scan at 06:29, 0.06s elapsed (1 total hosts)
nitiating Parallel DNS resolution of 1 host. at 06:29
ompleted Parallel DNS resolution of 1 host. at 06:29, 0.24s elapsed
nitiating Connect Scan at 06:29
canning sportybet.com (52.58.52.235) [1000 ports]
tats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
onnect Scan Timing: About 43.50% done; ETC: 06:30 (0:00:13 remaining)
ompleted Connect Scan at 06:30, 22.60s elapsed (1000 total ports)
nitiating Service scan at 06:30
nitiating OS detection (try #1) against sportybet.com (52.58.52.235)
etrying OS detection (try #2) against sportybet.com (52.58.52.235)
SE: Script scanning 52.58.52.235.
nitiating NSE at 06:30
ompleted NSE at 06:30, 0.00s elapsed
nitiating NSE at 06:30
ompleted NSE at 06:30, 0.00s elapsed
map scan report for sportybet.com (52.58.52.235)
ost is up (0.0013s latency).
ther addresses for sportybet.com (not scanned): 3.70.78.118 18.194.212.216 18.198.205.124 52.57.61.241 18.195.157.10 52.57.229.197 3.69.203.138
DNS record for 52.58.52.235: ec2-52-58-52-235.eu-central-1.compute.amazonaws.com
ll 1000 scanned ports on sportybet.com (52.58.52.235) are in ignored states.
ot shown: 1000 filtered tcp ports (no-response)
oo many fingerprints match this host to give specific OS details

ead data files from: /usr/bin/../share/nmap
S and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 26.71 seconds
          Raw packets sent: 52 (6.824KB) | Rcvd: 1 (40B)
```

When all 1000 ports are in an ignored state, it typically indicates a network configuration or security issue. Here are possible reasons and solutions:

Reasons:

1. Firewall configuration: Firewall rules might be blocking or ignoring traffic on these ports.
2. Network segmentation: Ports might be isolated or segmented from the rest of the network.
3. Port scanning defense: Network security measures might be ignoring traffic to prevent port scanning attacks.
4. Misconfigured network devices: Routers, switches, or other devices might be misconfigured.

Solutions:

1. Review firewall rules and configurations.
2. Check network segmentation and VLAN settings.
3. Verify port scanning defense mechanisms.
4. Inspect network device configurations.
5. Run network scans or diagnostics to identify issues.
6. Consult network documentation and logs.