

**NAME: P.NITYASREE**

**REGNO: 17MIS1007**

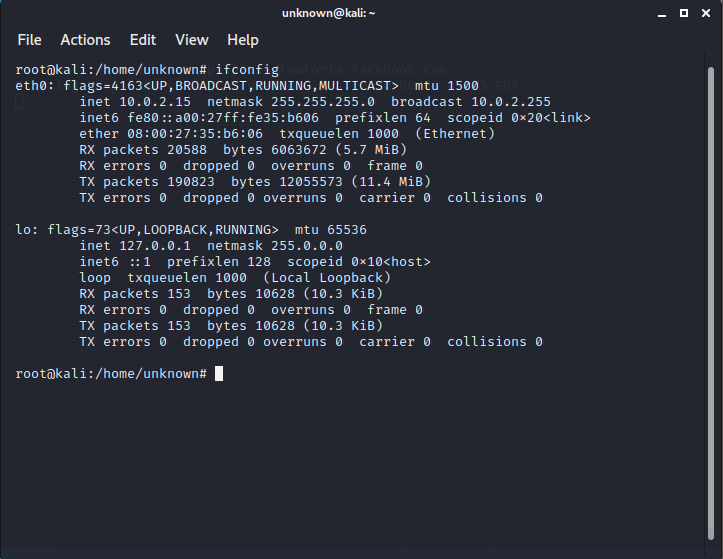
**COURSE: INFORMATION SECURITY MANAGEMENT**

**COURSE CODE: CSE 3502**

**FACULTY: ANUSHA**

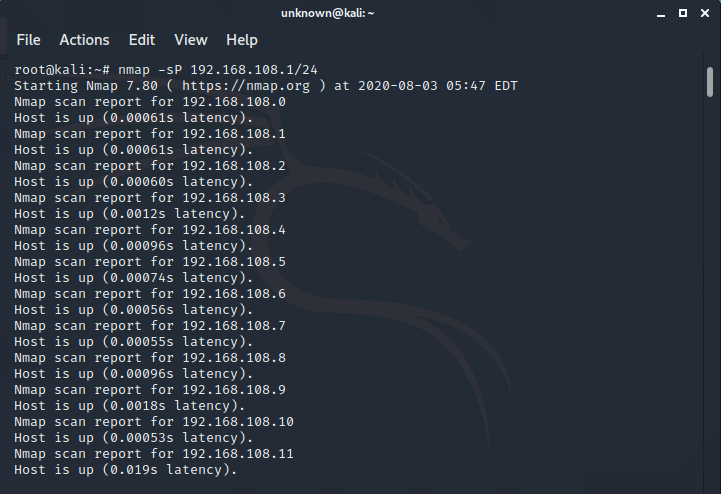
**INFORMATION GATHERING USING METASPOILT AND NMAP:**

**IpConfig:**

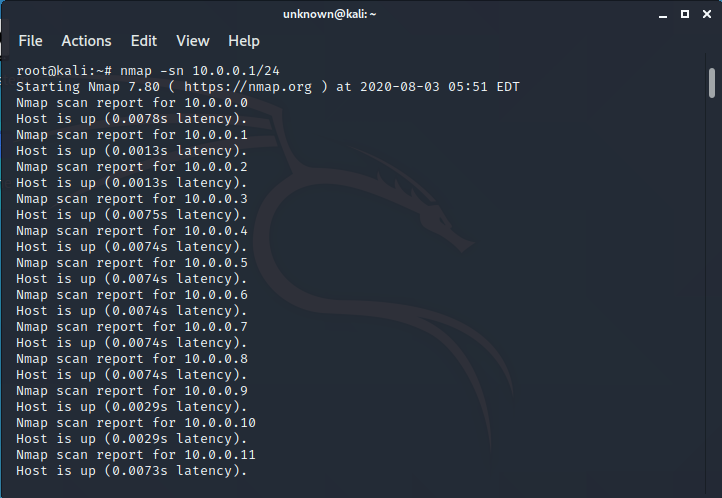


**Implement the following in NMAP:**

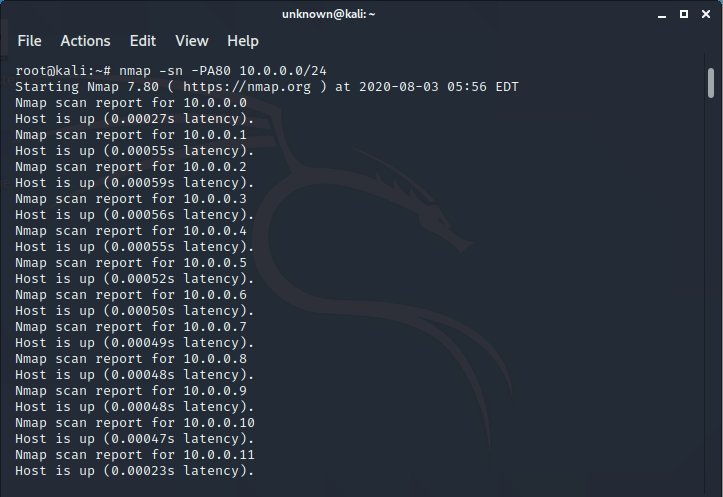
1. Perform host discovery (You can do sniffing using Wireshark and know about a connected host)



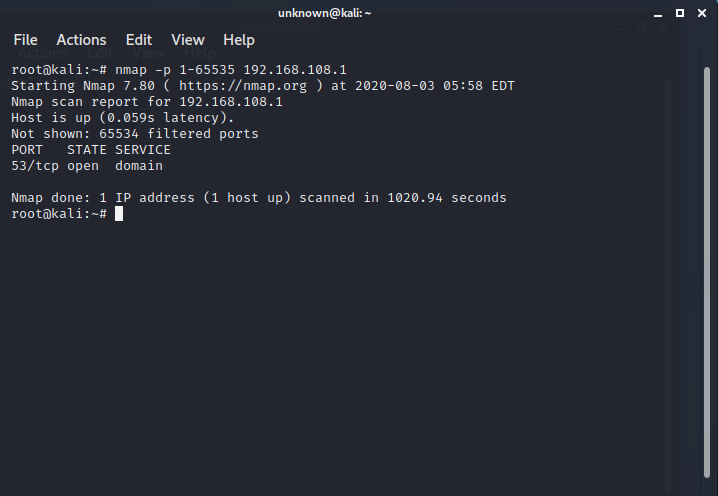
1. Identify Which hosts are up now? Apply ping sweeping (Port Sweeping)



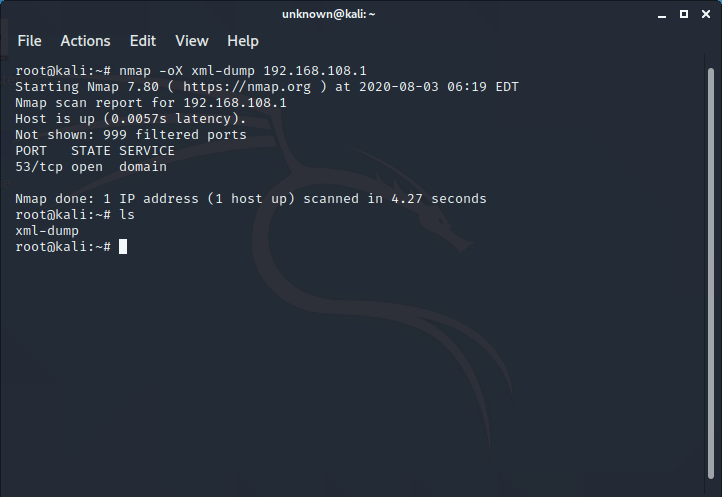
1. Use the TCP "ping" option with a ping scan with a flag to target port (Ping Sweeping)



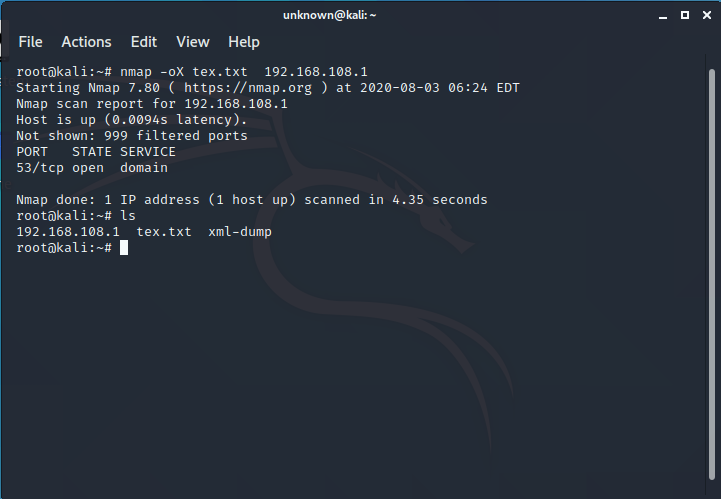
1. scan all the TCP ports



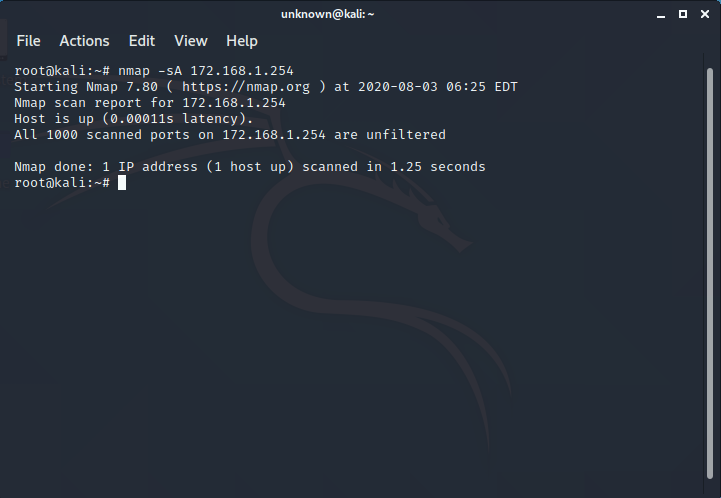
1. Save the results in xml file



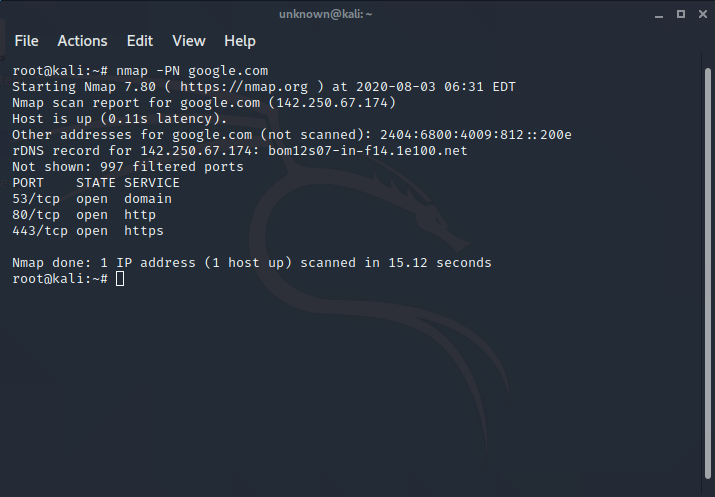
1. Save the results in a text



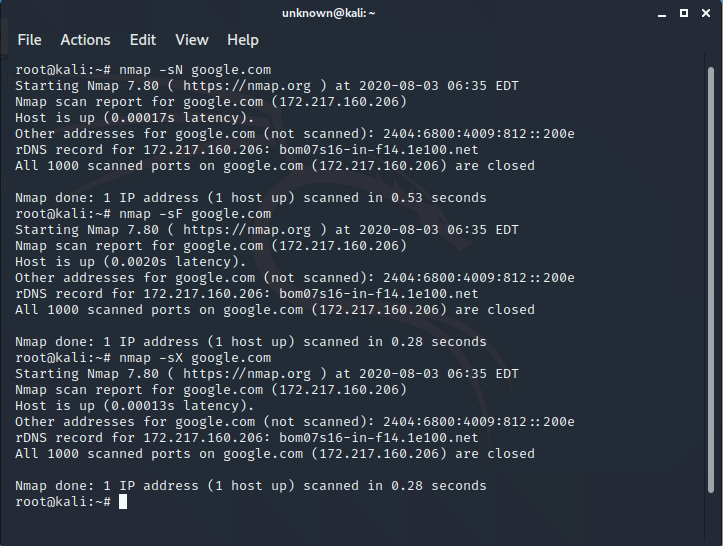
1. Find out if a host/network is protected by a firewall



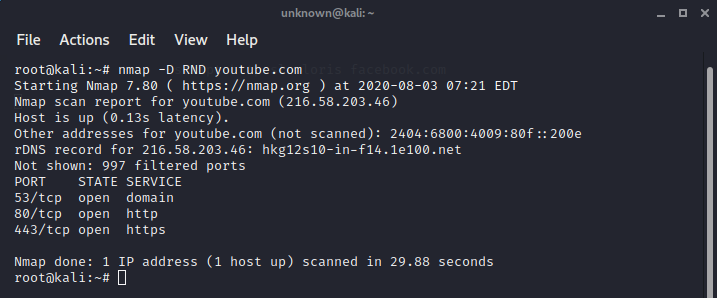
1. Scan a host when protected by the firewall



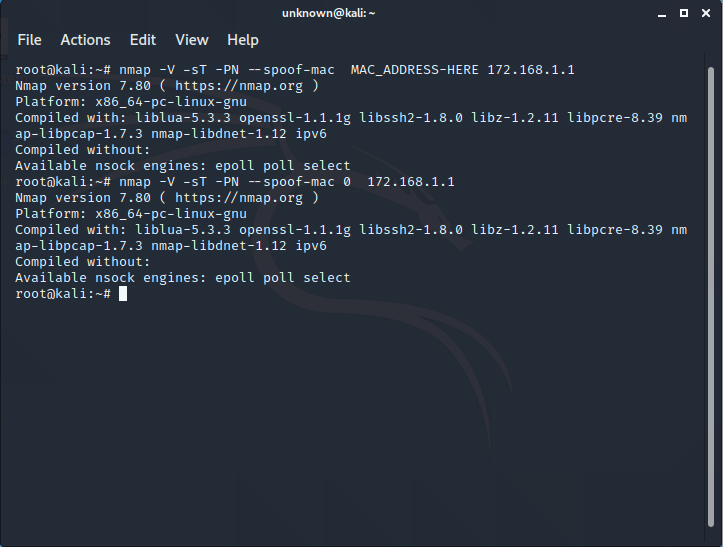
1. Scan a firewall for security weakness



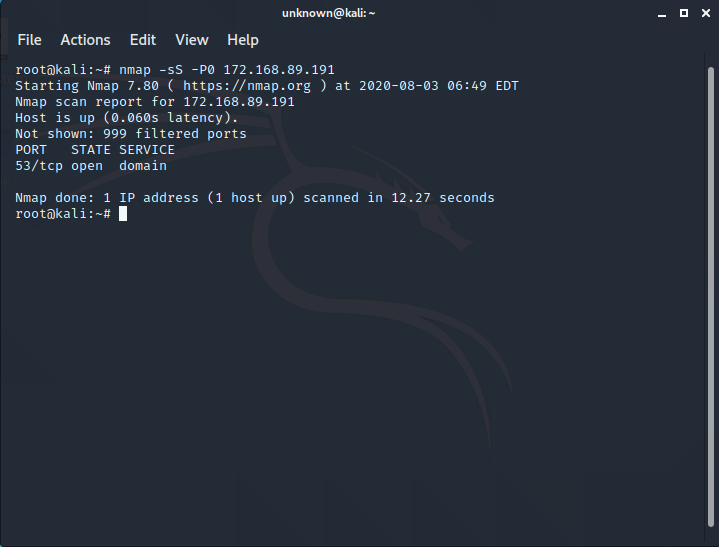
1. Cloak a scan with decoys



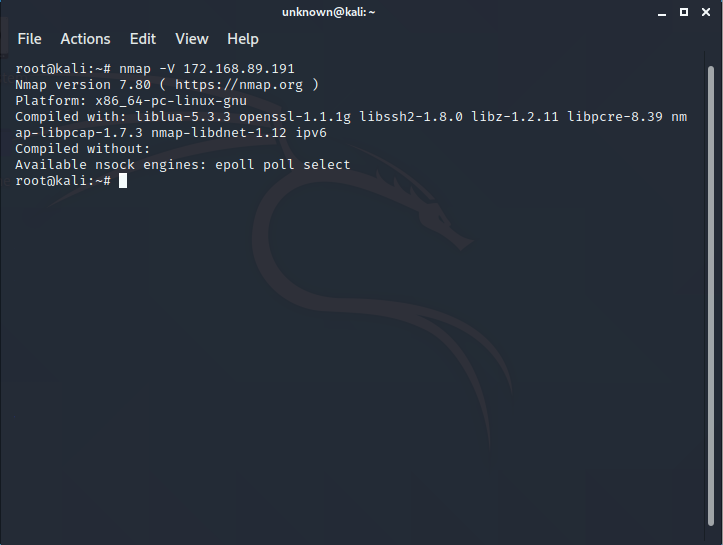
1. Bypass Firewall (locally) (MAC Address spoofing)



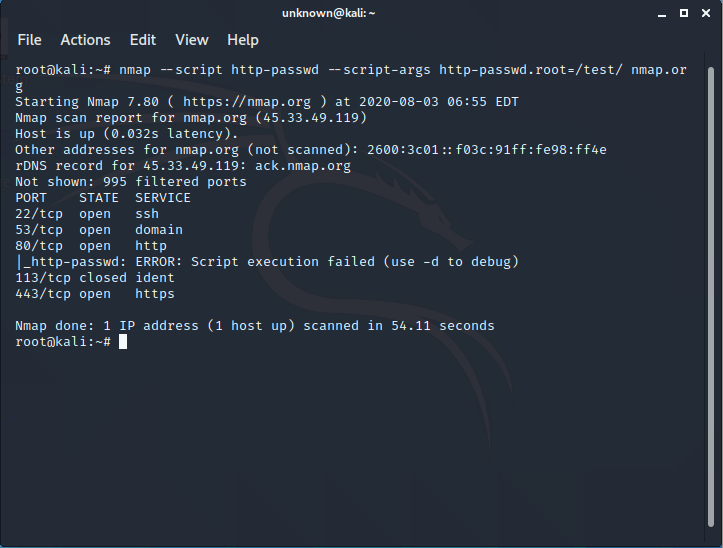
1. Bypass Firewall



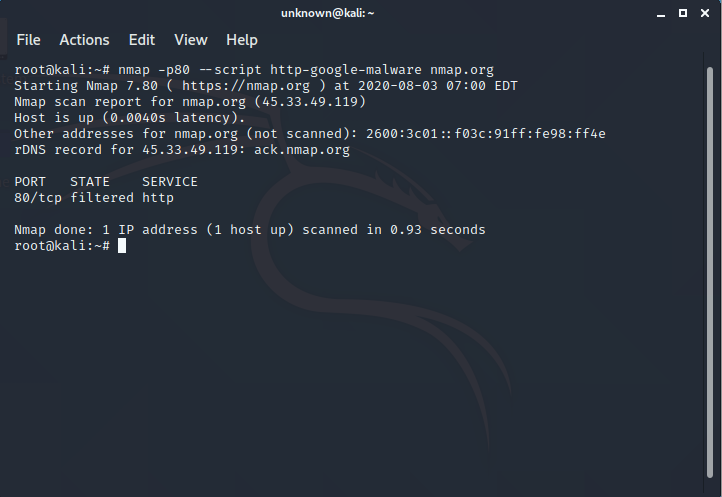
1. Find out Version Info



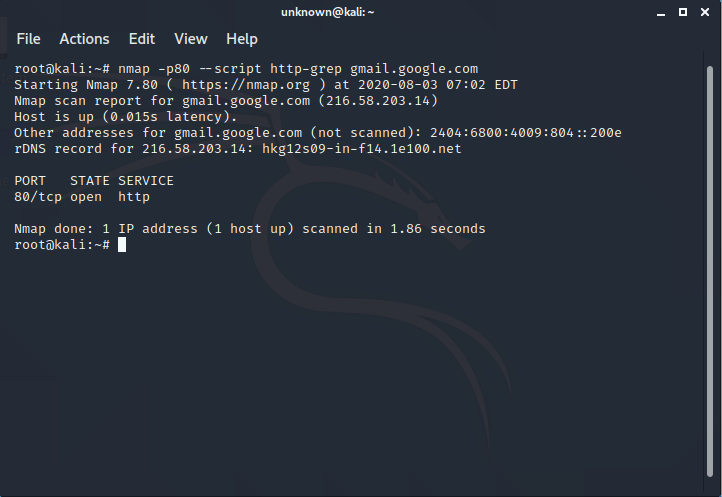
1. Check if a web server is vulnerable to directory traversal by attempting toretrieve /etc/passwd or \boot.ini



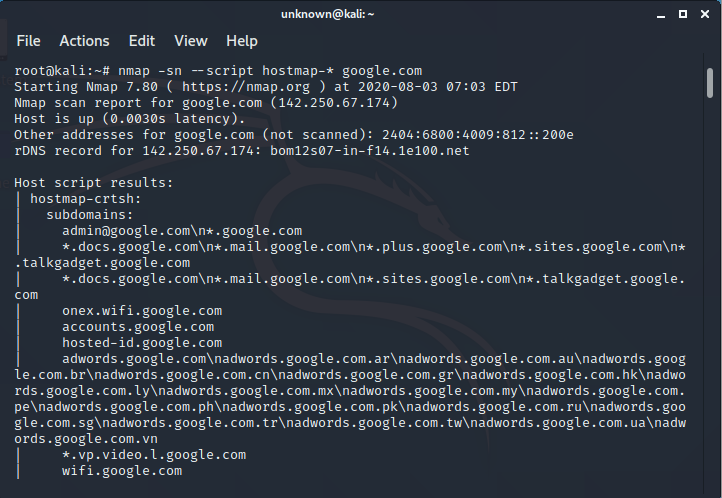
1. Test a web server for vulnerability to the Slowloris DoS attack by launching a Slowloris attack
2. Do Google safe browsing api



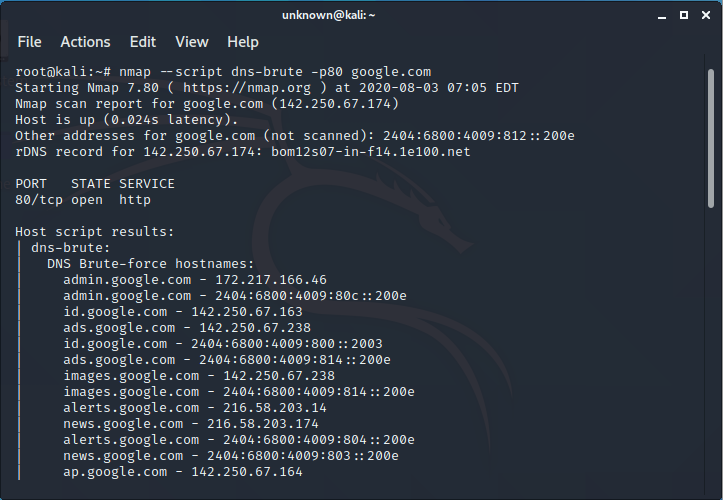
1. Grep public emails using nmap



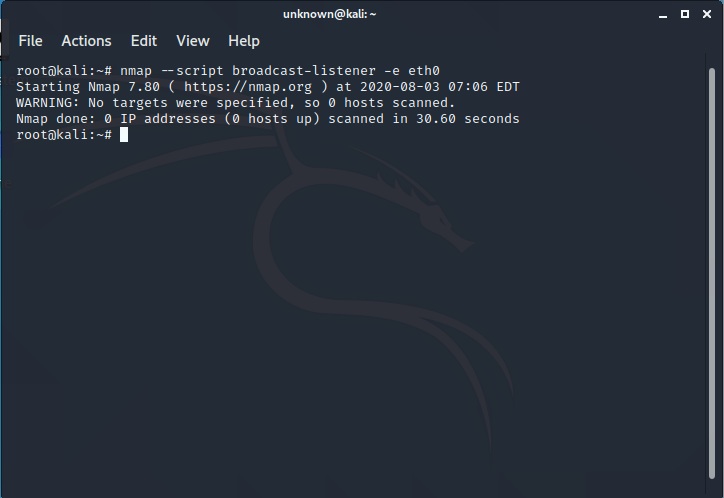
1. Discover hostnames pointing to the same IP address



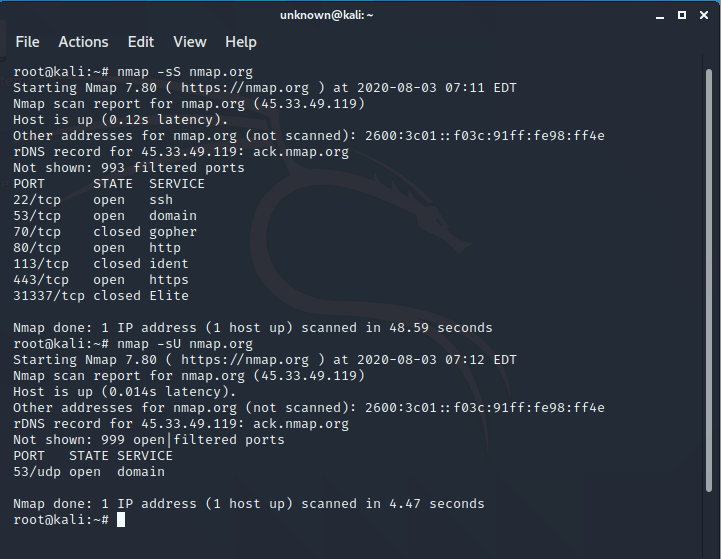
1. Discover hostnames by brute forcing DNS records



1. Validate your network broadcast



1. If a computer is up, which services (TCP and UDP) are open on it?



1. Determine the Operating system and its possible version that is running on each alive computer

