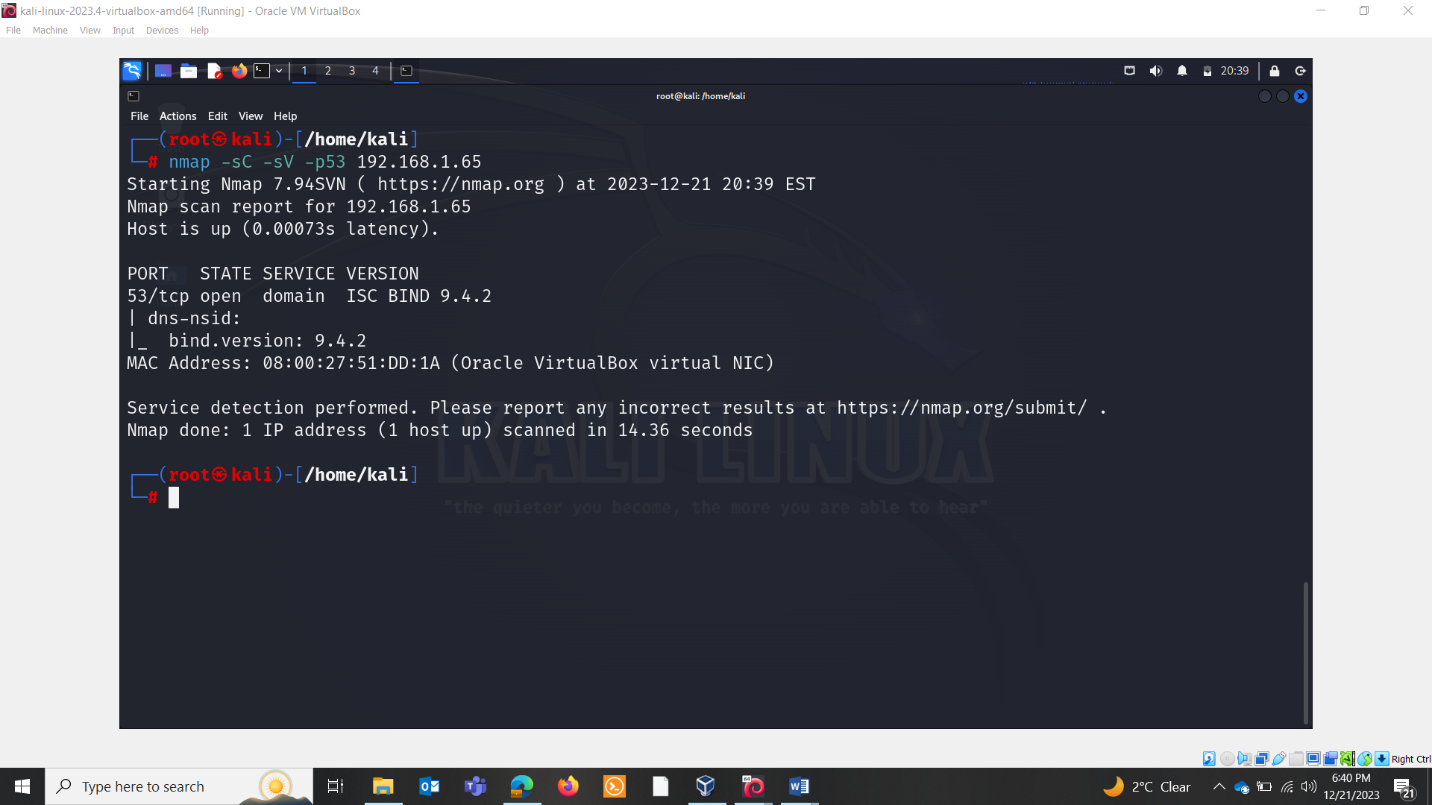
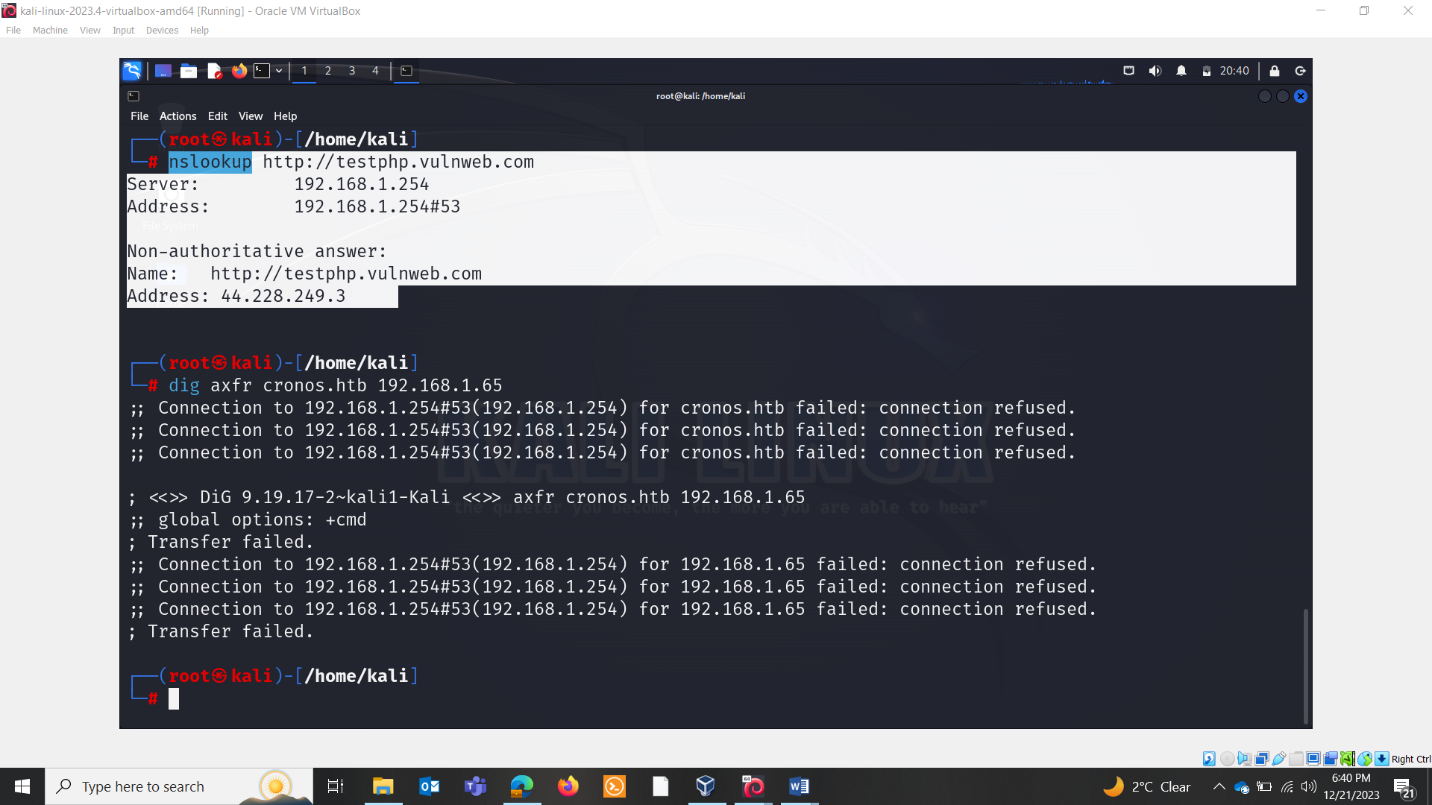
**DNS**

**Nmap -sV -sC -p53 192.168.1.65**

****

**Nslookup $ip**

****

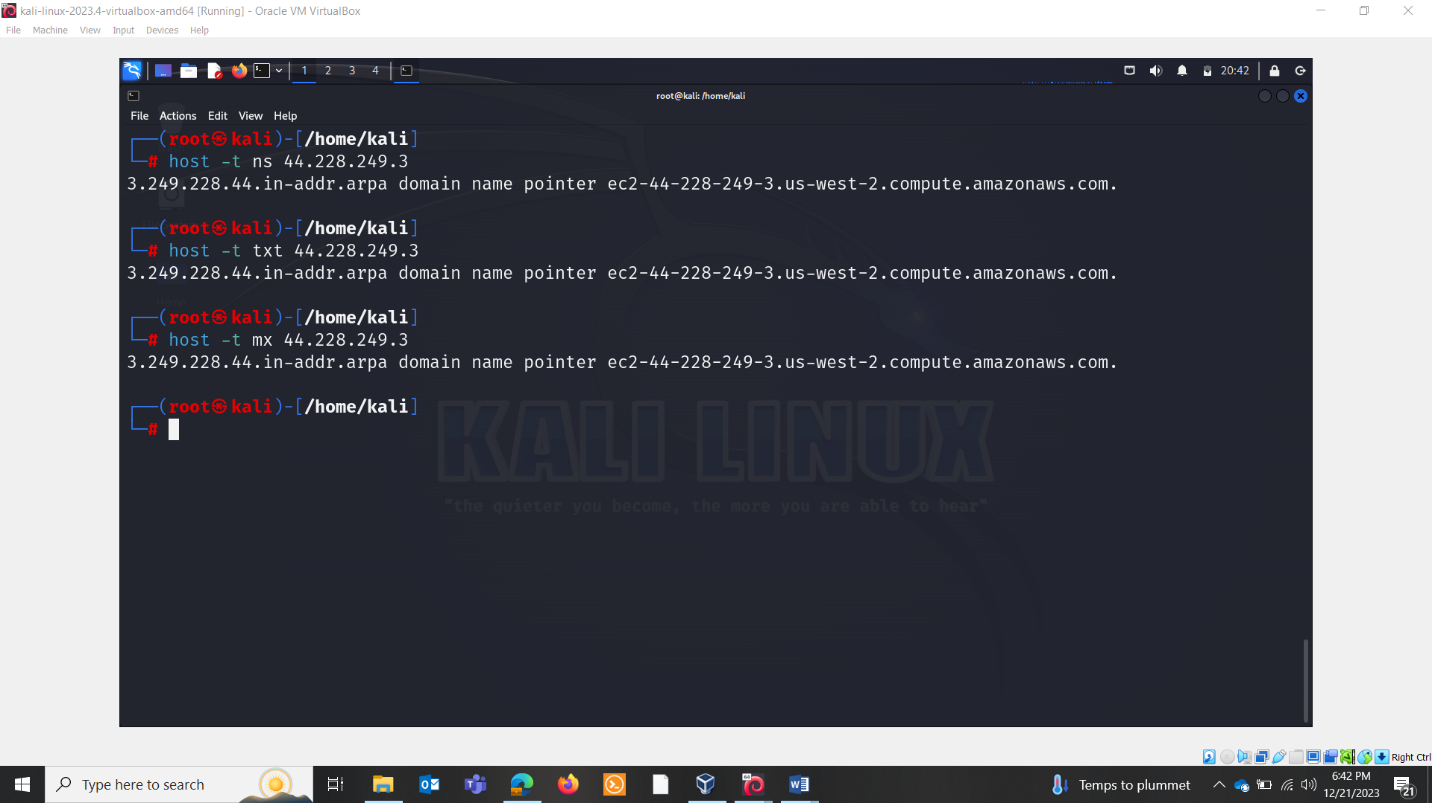
**Dig deeper**

**Dig axfr cronos.htb 192.168.1.65**

**Finding name servers: ns**

**Txt records: txt**

**Email servers: mx**

****

**FIERCE**

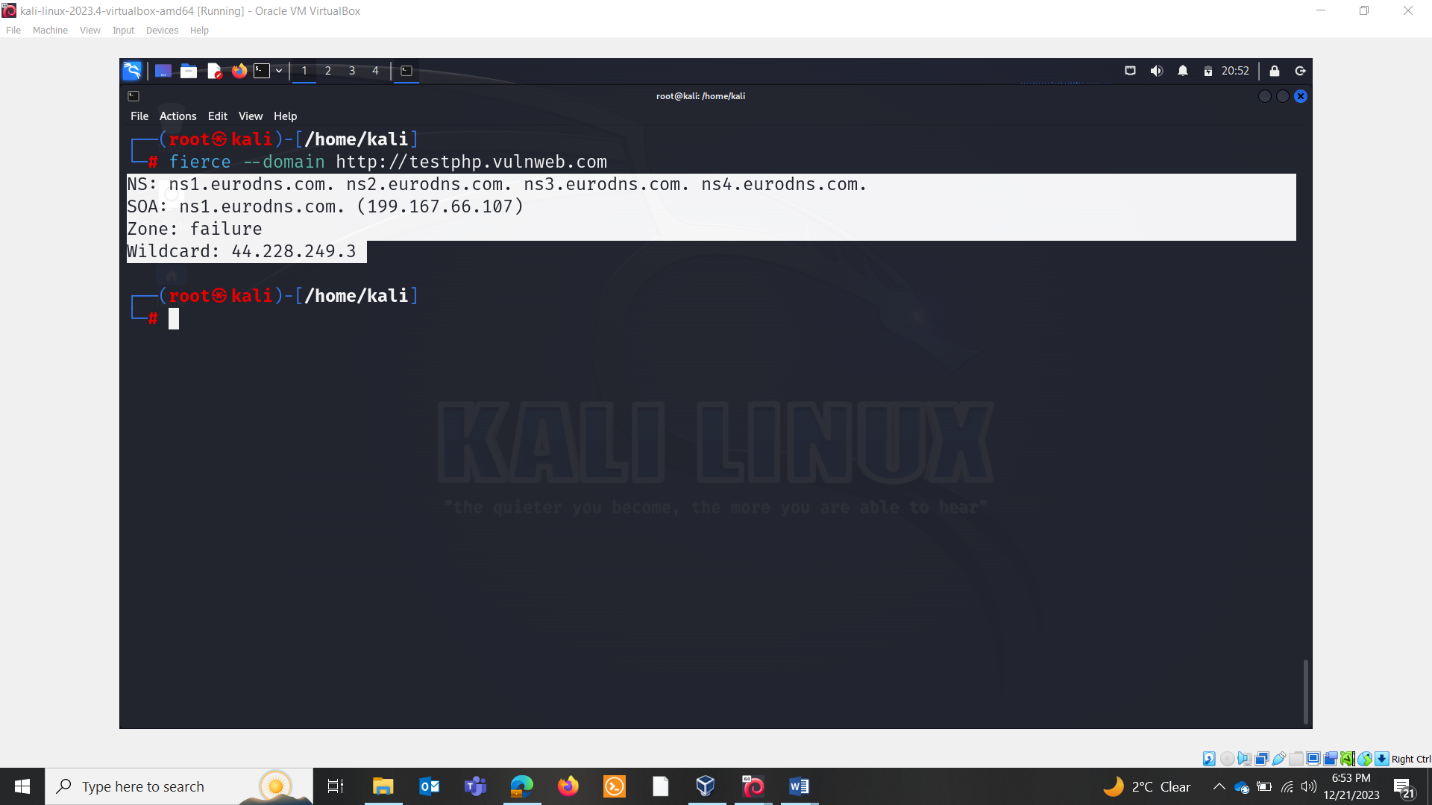
"Fierce" is a DNS reconnaissance tool used for DNS enumeration. It helps gather information about a domain by attempting to discover the domain's infrastructure, including subdomains and associated IP addresses. The tool is particularly useful for penetration testers, network administrators, and security professionals to assess the security of a domain.

The command you provided is using fierce with the -dns option and specifying a domain using $domain. Here's a breakdown of the command:

* fierce: This is the command-line tool for DNS reconnaissance.
* -dns: This option specifies the target domain for DNS enumeration.
* $domain: Replace this with the actual domain you want to enumerate.

When you run this command, fierce will perform various DNS-related tasks to gather information about the specified domain. This may include:

* Subdomain Enumeration: Fierce will attempt to discover subdomains associated with the target domain.
* DNS Zone Transfers: Fierce may attempt DNS zone transfers to gather information about authoritative name servers and their configurations.
* Brute Force Subdomains: Fierce may perform brute-force attacks to identify subdomains by trying common subdomain names.
* Reverse DNS Lookups: The tool may conduct reverse DNS lookups to map IP addresses to hostnames.



NS Records:

* ns1.eurodns.com.
* ns2.eurodns.com.
* ns3.eurodns.com.
* ns4.eurodns.com.

These are the authoritative name servers for the domain. NS records specify the DNS servers that are authoritative for a particular domain. In this case, the authoritative name servers are hosted at eurodns.com, and there are four of them (ns1 through ns4).

SOA Record: ns1.eurodns.com. (199.167.66.107)

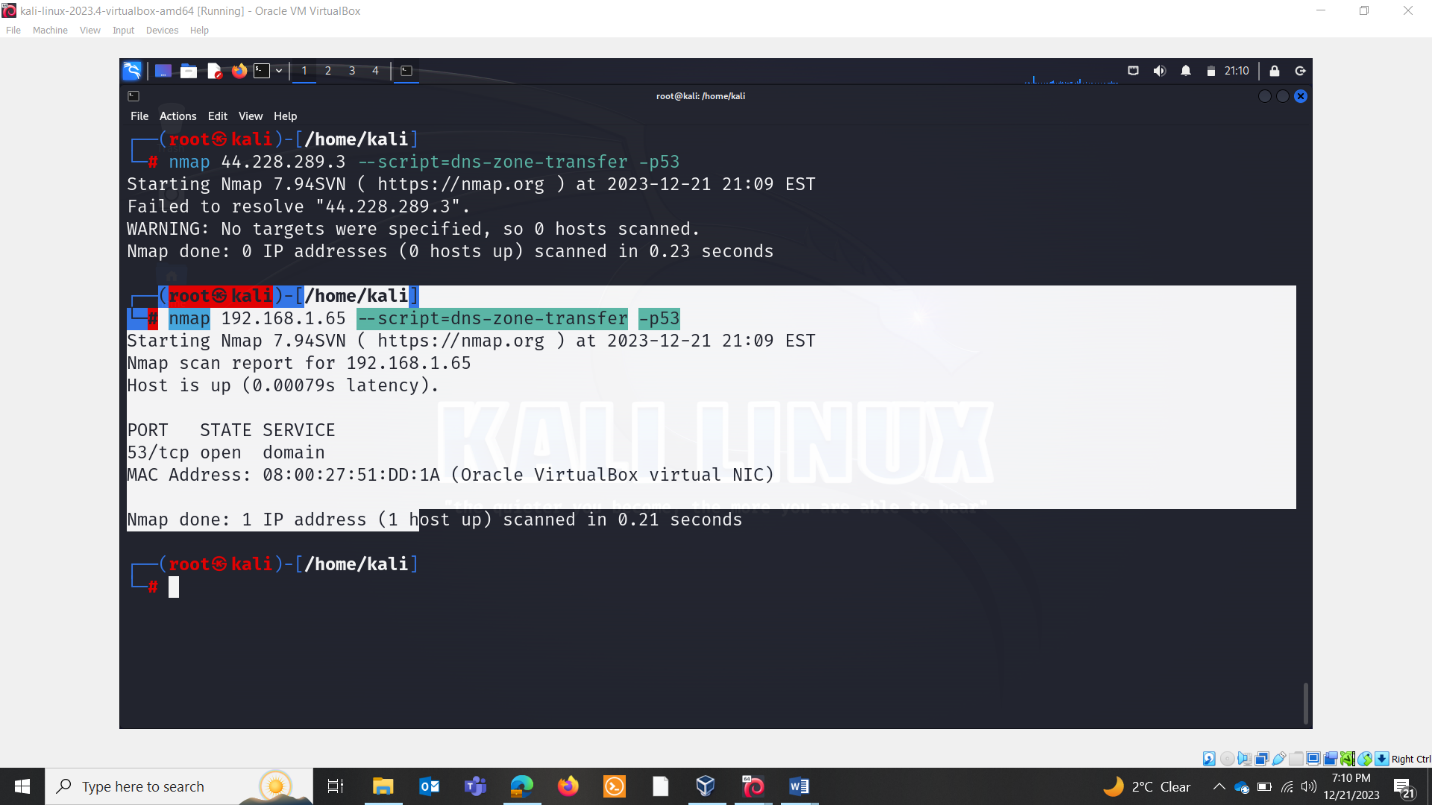
The SOA (Start of Authority) record specifies information about the domain and the zone. The format is typically as follows: primary authoritative DNS server, contact email for the domain, serial number, refresh time, retry time, expire time, and minimum TTL (Time to Live). In this case, it seems that the SOA record only includes the primary authoritative DNS server (ns1.eurodns.com) and its IP address (199.167.66.107).

Zone:failure

The term "Zone: failure" suggests that there might be an issue with the DNS zone. It could indicate that there's a problem with the DNS configuration for the specified domain, leading to a failure in the zone.

Wildcard: 44.228.249.3

The "Wildcard" entry typically refers to the IP address associated with a wildcard DNS record. Wildcard DNS records are used to match requests for non-existent subdomains. In this case, requests for subdomains that do not have explicit DNS records may be directed to the IP address 44.228.249.3.



Whois ip