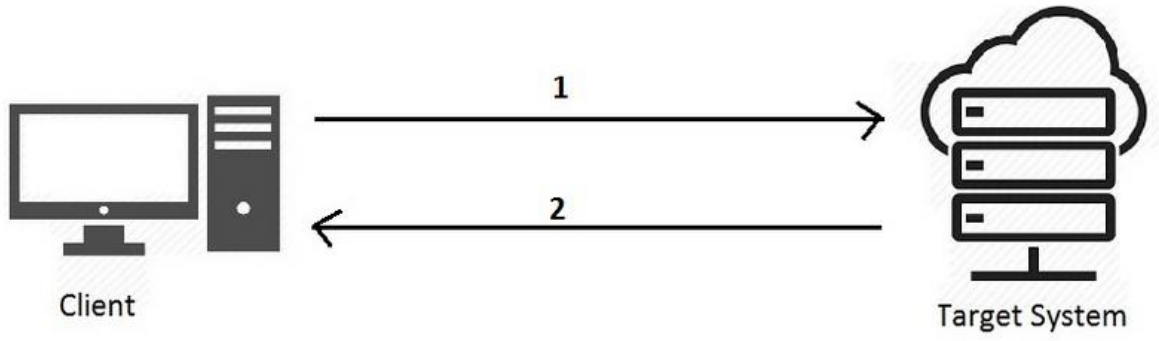
Lab - Enumerate DNS Records Using DNSRecon

Overview

In this lab, you will learn how to perform active information gathering of DNS records using DNSRecon. Active information gathering during a pentest involves scanning the target systems to find out about the up and running systems, what ports are open, and the software being used. This consists of communicating directly with the systems and potentially being detected.

Passive information gathering involves using public internet resources to discover information about a target without being detected.



Domain Name System (DNS) enumeration identifies any DNS servers and DNS records associated with a target.

DNS reconnaissance is part of the information gathering stage of a penetration test engagement. DNS reconnaissance is used to obtain as much information as possible about the target's network by scanning their DNS servers for DNS records. Most organizations do not monitor their DNS server traffic and those that do only monitor zone transfer attempts.

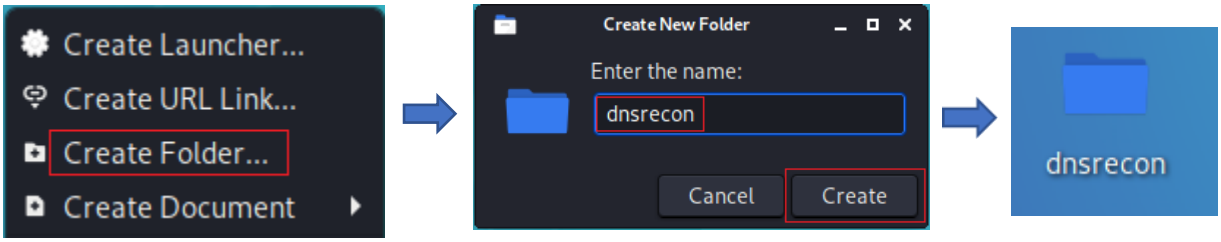
Lab Requirements

- Installation of VirtualBox, the latest version with the extension pack
- One virtual install of Kali Linux
- Kali network adapter set to NAT network

Begin the lab!

Passive Information Gathering

Begin by making a **`dnsrecon`** working directory on our desktop. Right-click anywhere on your Kali Desktop, and from the context menu, select **`Create Folder`**. In the name field, type **`dnsrecon`**. Click the **`Create`** button.

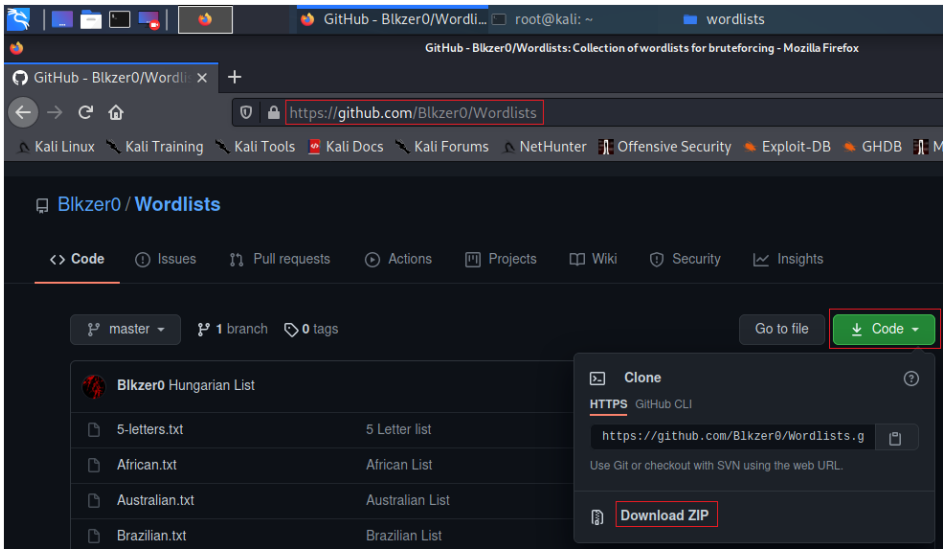


Download the dnsmap.txt wordlist.

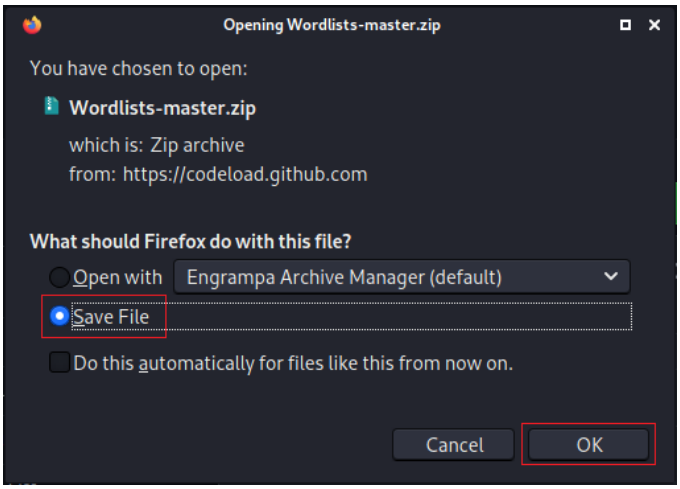
From this lab, we will need a specific wordlist labeled, dnsmap.txt. From your Kali machine, open a browser, and in the address bar, type the following address.

https://github.com/Blkzer0/Wordlists

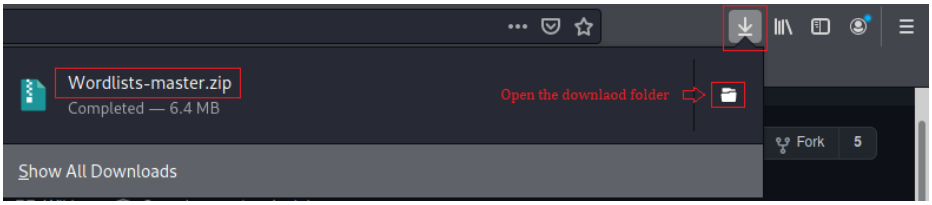
Click on the green code button and download the contents using the Download Zip option from the context menu.



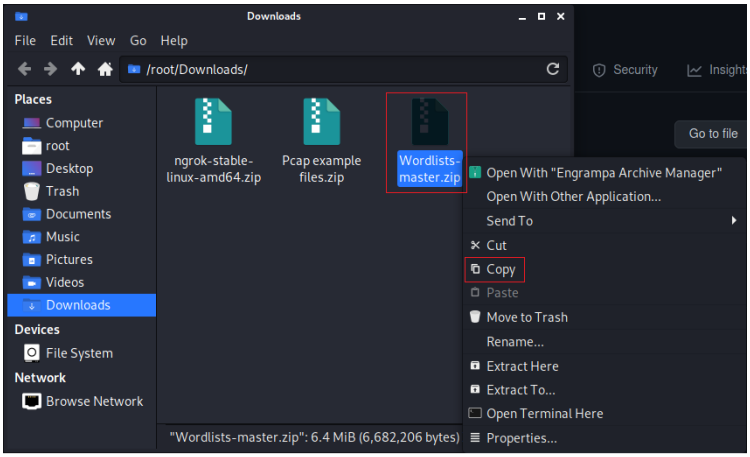
Save the file to your Kali downloads folder (default location).



Open your downloads folder.

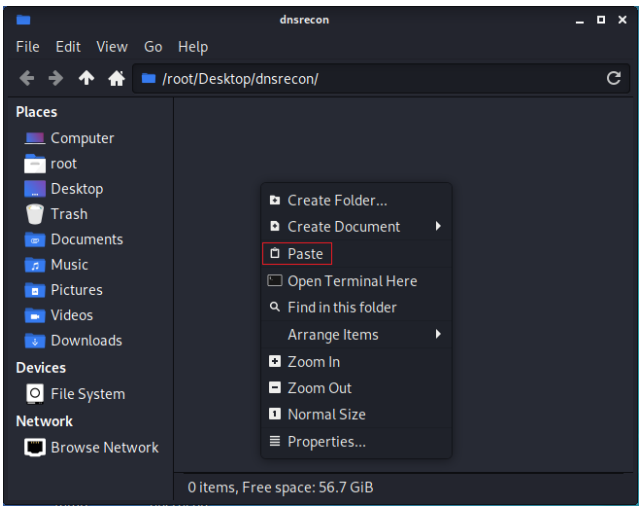


Find your downloaded file—Right-click on the download, and from the context menu, select **copy**.

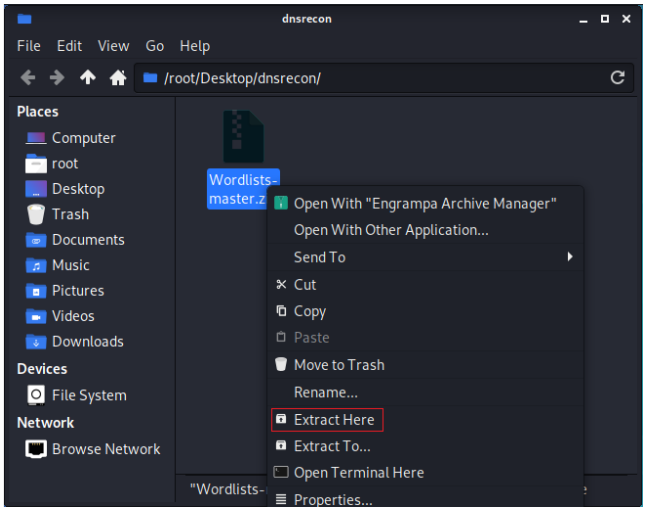


Close the download folder. Close the browser.

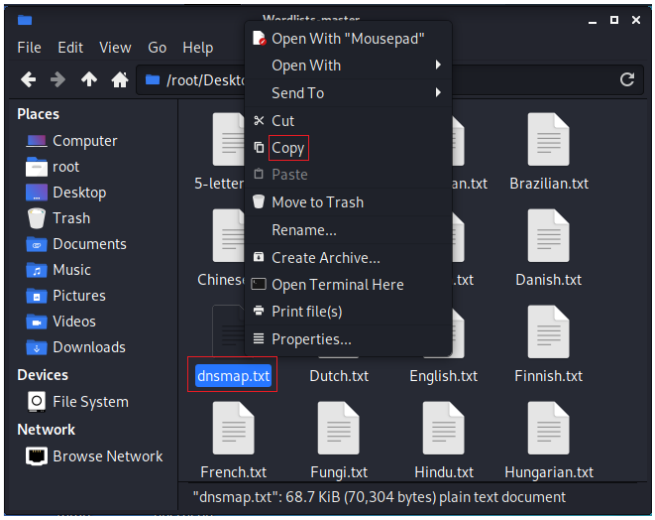
Open your dnsrecon work folder, and in the right windowpane, right-click, and from the context menu, select paste.



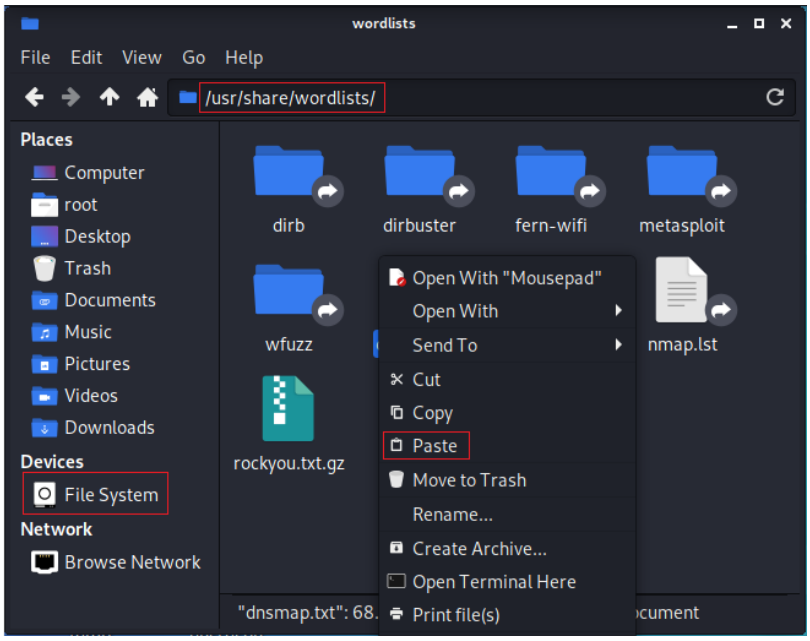
Right-click on the Wordlist-master.zip file, and from the context menu, select **Extract here**.



Open the extracted Wordlists-master extracted folder. Inside the extracted folder, find the **`dnsmap.txt`** file.



Close all open folders. From your desktop, open your **`file system`**. In the right windowpane, scroll down, find, and open your **`usr`** directory. Inside the **`usr`** directory, find and open the **`share`** directory. Inside the **`share`** directory, find and open the **`wordlist`** directory. Inside the right windowpane of the **`wordlist`** directory, right-click, and from the context menu, select **`paste`**.



DNS record types

SRV – *Service***.** Used to identify computers hosting specific services. SRV resource records are used to locate domain controllers for Active Directory.

SOA – *State of Authority*. Indicates which DNS server is the best source of information for the specified domain.

NS – *Nameserver*. Indicates which DNS server is authoritative for that domain (i.e., which server contains the actual DNS records).

TXT – *Text*. Provide the ability to associate arbitrary text with a host of another name, such as human-readable information about a server, network, data center, or other accounting information.

MX - *Mail exchanger*. Specifies the mail server responsible for accepting email messages on behalf of a domain name.

A - *Address*. Maps a domain name to the IP address (Version 4) of the computer hosting the domain. An A record uses a domain name to find the IP address of a machine connected to the internet.

CNAME - *Canonical Name*. Forwards one domain or subdomain to another domain; does NOT provide an IP address.

PTR – *Pointer*. Provides a domain name in reverse-lookups.

Using DNSRecon

From your kali machine, open a new terminal window.

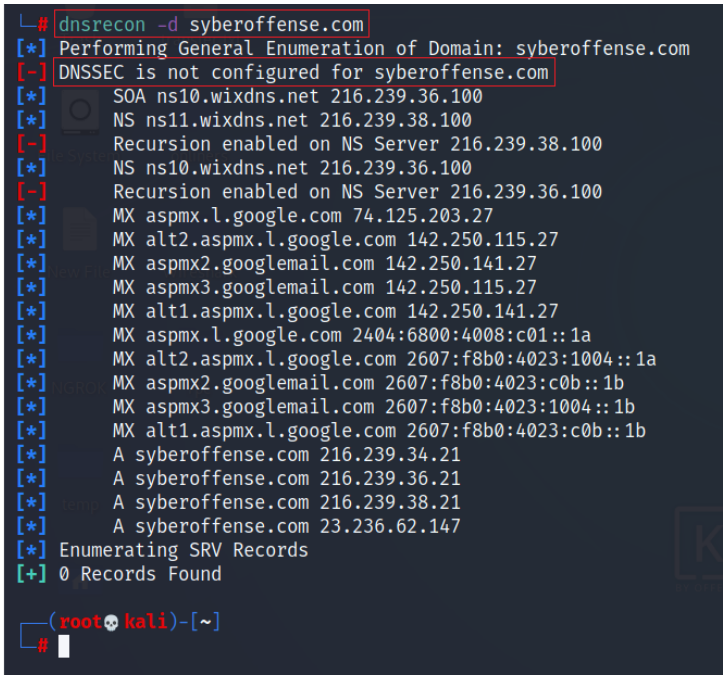
To see what options are available with dnsrecon, at the prompt, type the following command.

```
dnsrecon --h
```

Checking Enumeration

At the terminal, type the following command. This first command checks to see if the site is vulnerable to enumeration. Please note that we are saving the scan results as a CSV file type to our working directory. The saved file can be opened as either an Excel or text file.

```
dnsrecon -d syberoffense.com --csv ~/Desktop/dnsrecon/syber.csv
```



Pull SRV records for a domain

```
dnsrecon -d cisco.com -t srv --csv ~/Desktop/dnsrecon/cisco.csv
```

Note!

All generated files are being saved to my working directory!

```
┌──(root💀kali)-[~]
└─# dnsrecon -d cisco.com -t srv
[*] Enumerating Common SRV Records against cisco.com
[+]     SRV _h323cs._tcp.cisco.com vcsgw.cisco.com 173.39.112.104 1720
[+]     SRV _sip._udp.cisco.com vcsgw.cisco.com 173.39.112.104 5060
[+]     SRV _h323ls._udp.cisco.com vcsgw.cisco.com 173.39.112.104 1719
[+]     SRV _sip._tcp.cisco.com vcsgw104.cisco.com 173.39.112.104 5060
[+]     SRV _sip._tcp.cisco.com vcsgw102.cisco.com 64.104.254.229 5060
[+]     SRV _sip._tcp.cisco.com vcsgw101.cisco.com 64.104.254.228 5060
[+]     SRV _sip._tcp.cisco.com vcsgw103.cisco.com 173.39.112.103 5060
[+]     SRV _sips._tcp.cisco.com vcsgw104.cisco.com 173.39.112.104 5061
[+]     SRV _sips._tcp.cisco.com vcsgw101.cisco.com 64.104.254.228 5061
[+]     SRV _sips._tcp.cisco.com vcsgw102.cisco.com 64.104.254.229 5061
[+]     SRV _sips._tcp.cisco.com vcsgw103.cisco.com 173.39.112.103 5061
[+]     SRV _xmpp-client._tcp.cisco.com isj3cmx.webexconnect.com 66.163.36.181 5222
[+]     SRV _xmpp-server._tcp.cisco.com isj3jxf.webexconnect.com 66.163.36.186 5269
[+] 13 Records Found

┌──(root💀kali)-[~]
└─#
```

Domain Bruteforcing

To bruteforce the DNS records for a domain, we must use a name list to try and resolve the A, AAA, and CNAME records against the domain by trying each entry one by one.

`dnsrecon -D /usr/share/wordlists/dnsmap.txt -t brt -d line.me  --csv ~/Desktop/dnsrecon/line.me.csv`

This s a slow process, and it can take 10 minutes or more to complete, so be patient!

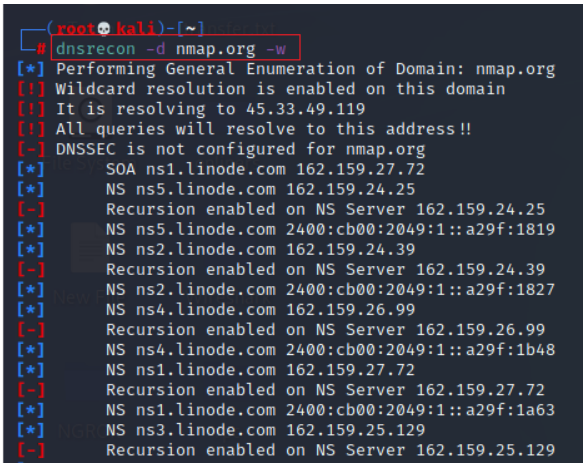
```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# dnsrecon -D /usr/share/wordlists/dnsmap.txt -t brt -d line.me
[*] Performing host and subdomain brute force against line.me
[+] ace.line.me: A : 203.104.166.20
[+] ads.line.me: A : 147.92.146.253
[+] air.line.me: A : 203.104.165.75
[+] api.line.me: A : 104.105.116.174
[+] biz.line.me: A : 125.6.149.168
[+] buy.line.me: A : 184.28.188.177
[+] egp.line.me: A : 147.92.144.235
[+] hub.line.me: A : 147.92.144.221
[+] lan.line.me: CNAME : lan.line.me.akadns.net
[+] lan.line.me.akadns.net: CNAME : lan-o.line.me
[+] lan-o.line.me: A : 203.104.142.52
[+] lbc.line.me: A : 147.92.146.211
[+] lbw.line.me: A : 147.92.139.71
[+] lcs.line.me: CNAME : lcs.line.me.akadns.net
[+] lcs.line.me.akadns.net: CNAME : lcs-sg.line.me.akadns.net
[+] lcs-sg.line.me.akadns.net: A : 203.104.175.36
[+] man.line.me: A : 147.92.165.129
[+] now.line.me: A : 147.92.184.29
[+] obs.line.me: CNAME : obs-org.line-apps.com
[+] obs-org.line-apps.com: A : 125.209.210.200
[+] obs-org.line-apps.com: A : 125.209.210.237
[+] pay.line.me: A : 203.104.135.24
[+] poi.line.me: CNAME : page.line.me
[+] page.line.me: A : 147.92.146.63
[+] red.line.me: A : 147.92.144.242
[+] scc.line.me: A : 125.209.222.43
[+] sch.line.me: A : 147.92.191.160
[+] wow.line.me: A : 147.92.146.211
[+] www.line.me: A : 203.104.129.195
[+] 29 Records Found

┌──(root💀kali)-[~]
└─#
```

Reverse Lookup

The following command performs a deep whois record analysis and reverse lookup of IP ranges found through Whois when doing a standard enumeration.

```
dnsrecon -d nmap.org -w --csv ~/Desktop/dnsrecon/reverse_lookup_nmap.csv
```

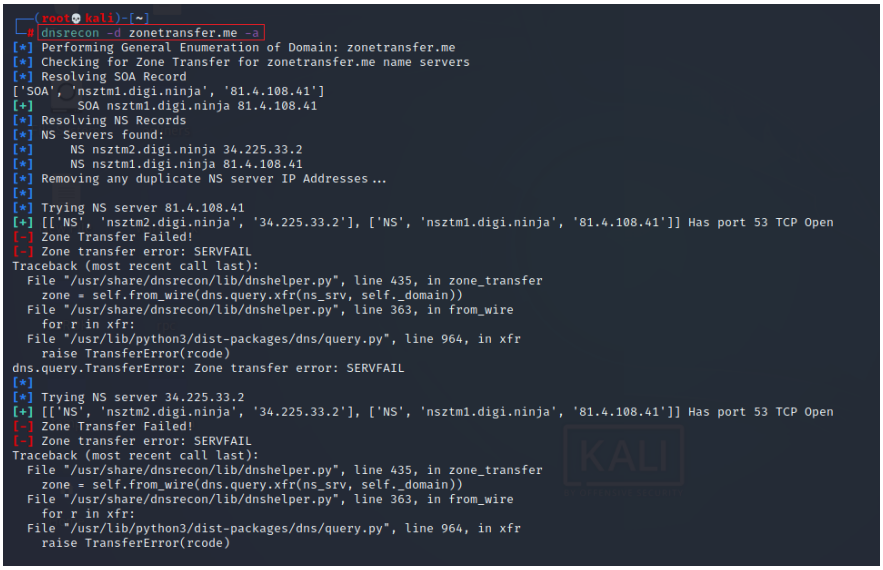


Working Zone Transfer

The security problem with DNS zone transfer is that it can be used to decipher the topology of a company's network. Specifically, when a user tries to perform a zone transfer, it sends a DNS query to list all DNS information like name servers, hostnames, MX and CNAME records, zone serial number, Time to Live records, etc.

A significant amount of information can be obtained by using this technique. However, this technique is unlikely to work today due to organizations' security controls, but it's worth a shot.

```
dnsrecon -d zonetransfer.me -a --csv ~/Desktop/dnsrecon/zonetransfer.me.csv
```



Zone Walking

Zone Walking uncovers internal records if the DNSSEC zone is not configured correctly. The info obtained can help the pentester or hacker map network hosts by enumerating the contents of the DNSSEC zone.

If a DNSSEC zone uses NSEC, it can be DNSSEC zone walked.

DNSSEC zone walking does not work If NSEC3 is used. Only hashes of domains are returned.

DNSSEC Zone Walked

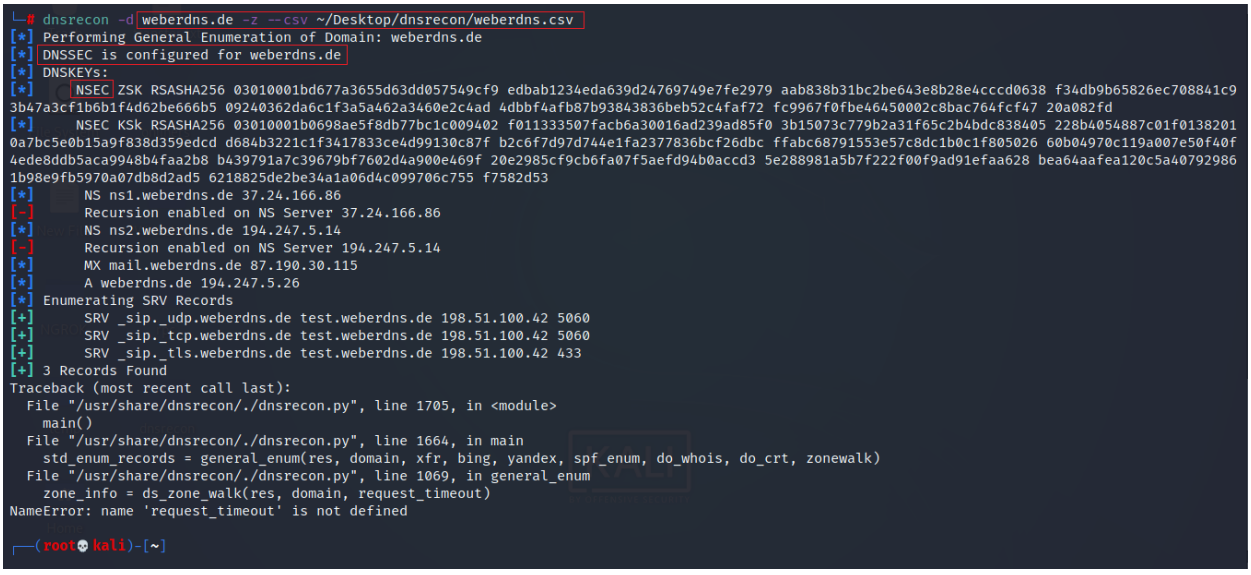
Domain Name System Security Extensions (DNSSEC) is a suite of extensions that add security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks.

The following command performs a DNSSEC zone walk using standard enumeration. To walk a DNSSEC zone, use the -z option.

In the following example, we attempt to walk through the weberdns.de DNSSEC zone, which uses only NSEC (instead of NSEC3) and is prone to zone walks.

If zone walking is not a security concern, NSEC is much simpler to configure. If zone walking is a concern, then NSEC3 is the solution.

`dnsrecon -d weberdns.de -z --csv ~/Desktop/dnsrecon/weberdns.csv`



Summary

In this short lab, you learned that the amount of information that can be discovered during DNS reconnaissance is huge. Misconfigurations of a target's DNS server helps to map the entire network. Domain name system (DNS) profiling involves sending queries to DNS servers to retrieve information on the systems that might exist within the company, such as a mail server or a web server. Keep in mind that you could obtain the DNS servers information for a company by passively gathering information by doing a Whois lookup. The next step is to actively scan those servers to find out what DNS records exist.