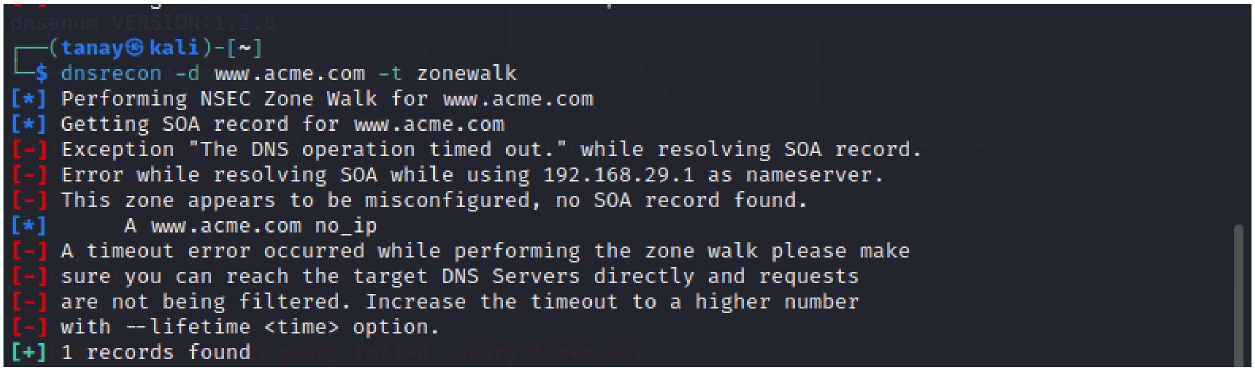
Exploring different Inbuilt tools in Kali Linux

1)Information Gathering
DSN recon:

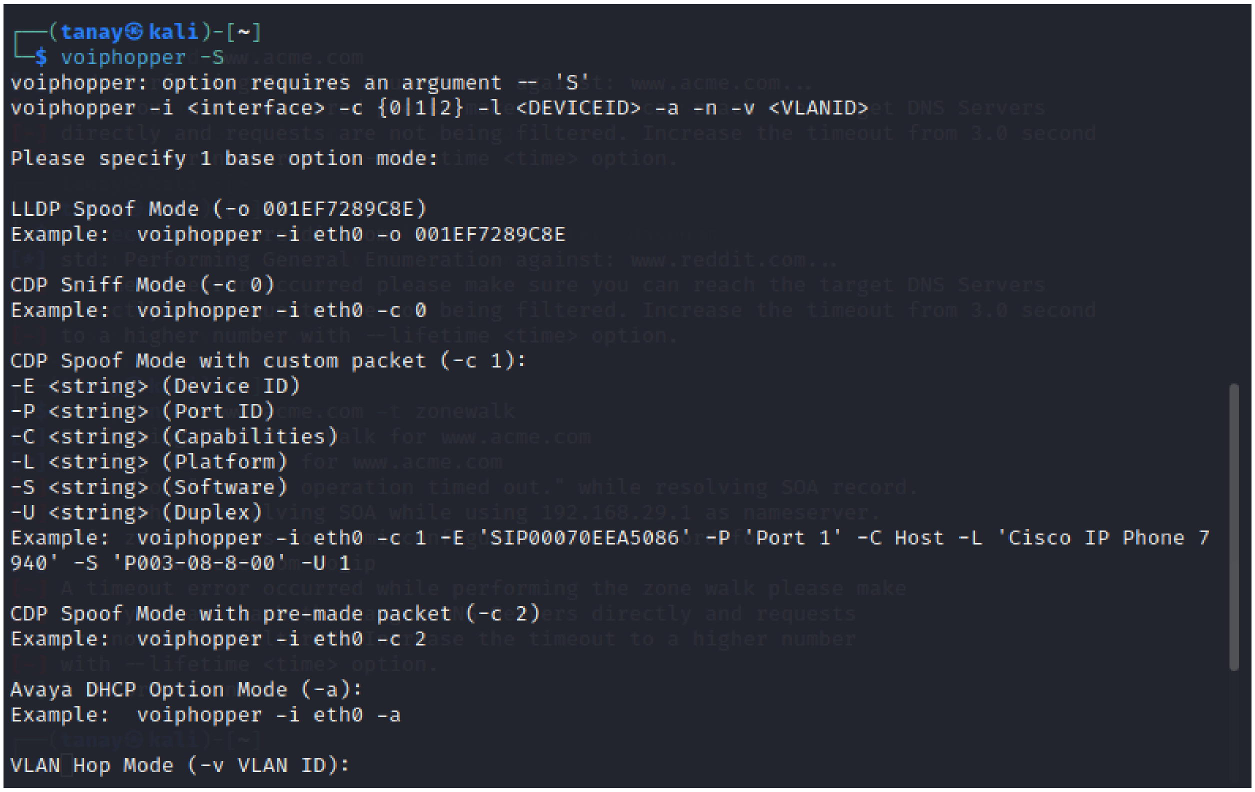
DNSRecon, as it is known today, is the Python equivalent of a Ruby script originally written by Carlos Perez toward the end of 2006. In his own words, this tool largely emerged from his personal need to reflect DNS-related data collection in an intuitive manner while the Python version allowed him to practice his newly acquired skills with the programming language.



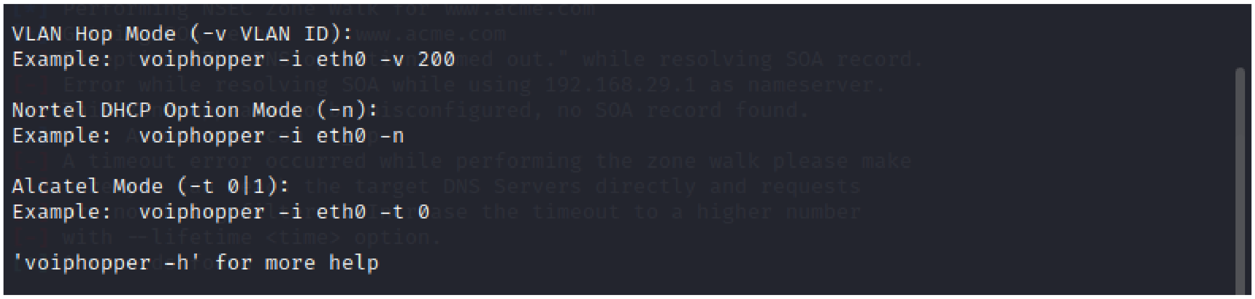
```
┌──(tanay㉿kali)-[~]
└─$ dnsrecon -d www.acme.com -t zonewalk
[*] Performing NSEC Zone Walk for www.acme.com
[*] Getting SOA record for www.acme.com
[-] Exception "The DNS operation timed out." while resolving SOA record.
[-] Error while resolving SOA while using 192.168.29.1 as nameserver.
[-] This zone appears to be misconfigured, no SOA record found.
[*]      A www.acme.com no_ip
[-] A timeout error occurred while performing the zone walk please make
[-] sure you can reach the target DNS Servers directly and requests
[-] are not being filtered. Increase the timeout to a higher number
[-] with --lifetime <time> option.
[+] 1 records found
```

2)Vulnerability Analysis
VoipHopper

VoIP Hopper is a GPLv3 licensed security tool, written in C that rapidly runs a VLAN Hop security test. VoIP Hopper is a VoIP infrastructure security testing tool but also a tool that can be used to test the (in)security of VLANs.



```
┌──(tanay㉿kali)-[~]
└─$ voiphopper -S
voiphopper: option requires an argument -- 'S'
voiphopper -i <interface> -c {0|1|2} -l <DEVICEID> -a -n -v <VLANID>

Please specify 1 base option mode:

LLDP Spoof Mode (-o 001EF7289C8E)
Example:  voiphopper -i eth0 -o 001EF7289C8E

CDP Sniff Mode (-c 0)
Example:  voiphopper -i eth0 -c 0

CDP Spoof Mode with custom packet (-c 1):
-E <string> (Device ID)
-P <string> (Port ID)
-C <string> (Capabilities)
-L <string> (Platform)
-S <string> (Software)
-U <string> (Duplex)
Example:  voiphopper -i eth0 -c 1 -E 'SIP00070EEA5086' -P 'Port 1' -C Host -L 'Cisco IP Phone 7
940' -S 'P003-08-8-00' -U 1

CDP Spoof Mode with pre-made packet (-c 2)
Example:  voiphopper -i eth0 -c 2

Avaya DHCP Option Mode (-a):
Example:  voiphopper -i eth0 -a

VLAN Hop Mode (-v VLAN ID):
```

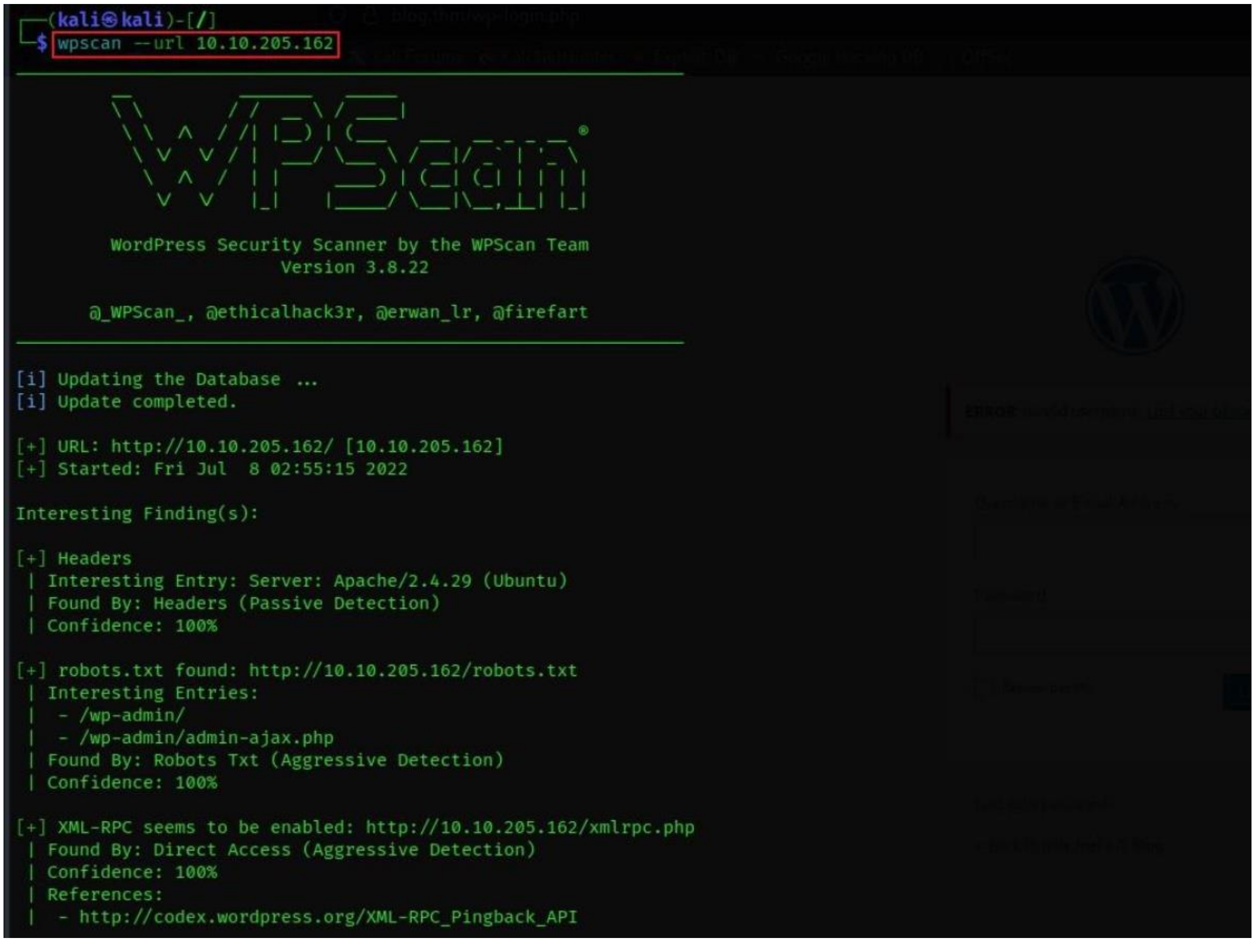


```
VLAN Hop Mode (-v VLAN ID):
Example:  voiphopper -i eth0 -v 200

Nortel DHCP Option Mode (-n):
Example:  voiphopper -i eth0 -n

Alcatel Mode (-t 0|1):
Example:  voiphopper -i eth0 -t 0

'voiphopper -h' for more help
```

3)Web Application Analysis

WPScan

Wpscan is a WordPress security scanner used to test WordPress installations and WordPress-powered websites



```
┌──(kali㉿kali)-[/]
└─$ wpscan --url 10.10.205.162
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://10.10.205.162/ [10.10.205.162]
[+] Started: Fri Jul  8 02:55:15 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.205.162/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.205.162/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
```