

The background is a gradient of dark blue and purple. It features several faint, stylized circular patterns, some resembling orbits or data paths, with small arrows indicating direction. There are also small, white, star-like specks scattered across the background, giving it a cosmic or digital feel.

PENETRATION TESTING AND HACKING TOOLS FOR KALI LINUX INFORMATION AND NETWORK SECURITY

CONTENT

- Introduction
- ***Nmap***
- WPScan
- Metasploit
- Traceroute
- Wireshark
- Burp Suite
- Maltego
- Nessus
- BeEF
- Nikto
- Social Engineering Toolkit (SET)

INTRODUCTION:

Best Kali Linux Tools for Hacking and Penetration Testing

Here's our list of best Kali Linux tools that will allow you to assess the security of web-servers and help in performing hacking and pen-testing.

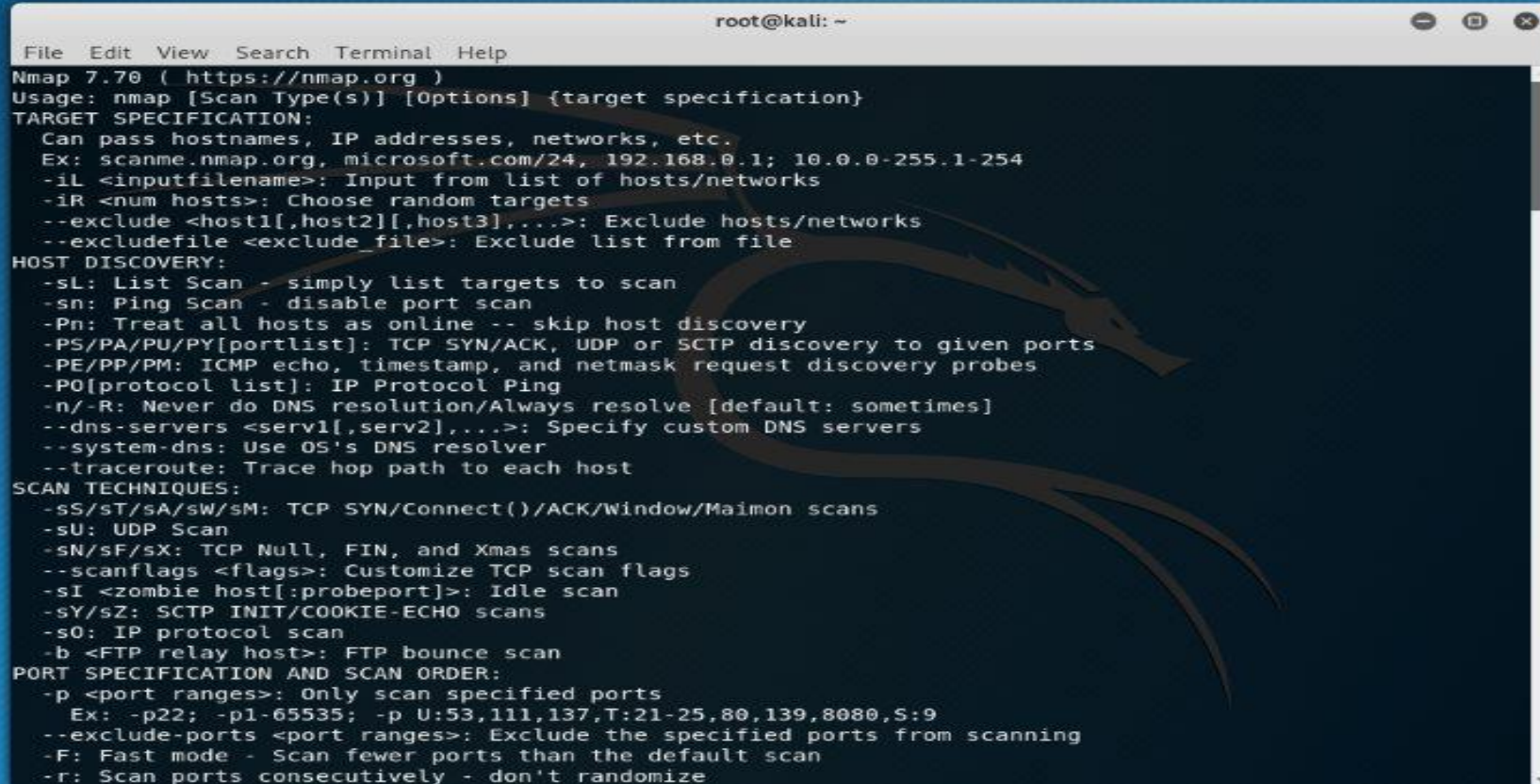
If you read the Kali Linux review, you know why it is considered one of the best Linux distributions for hacking and pen-testing and rightly so. It comes baked in with a lot of tools to make it easier for you to test, hack, and for anything else related to digital forensics.

It is one of the most recommended Linux distro for ethical hackers. Even if you are not a hacker but a webmaster – you can still utilize some of the tools to easily run a scan of your web server or web page.

Note that not all tools mentioned here are open source.

NMAP

Nmap or “Network Mapper” is one of the most popular tools on Kali Linux for information gathering. In other words, to get insights about the host, its IP address, OS detection, and similar network security details

A screenshot of a terminal window titled 'root@kali: ~'. The window displays the Nmap 7.70 usage and options. The text is as follows:

```
File Edit View Search Terminal Help
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
```

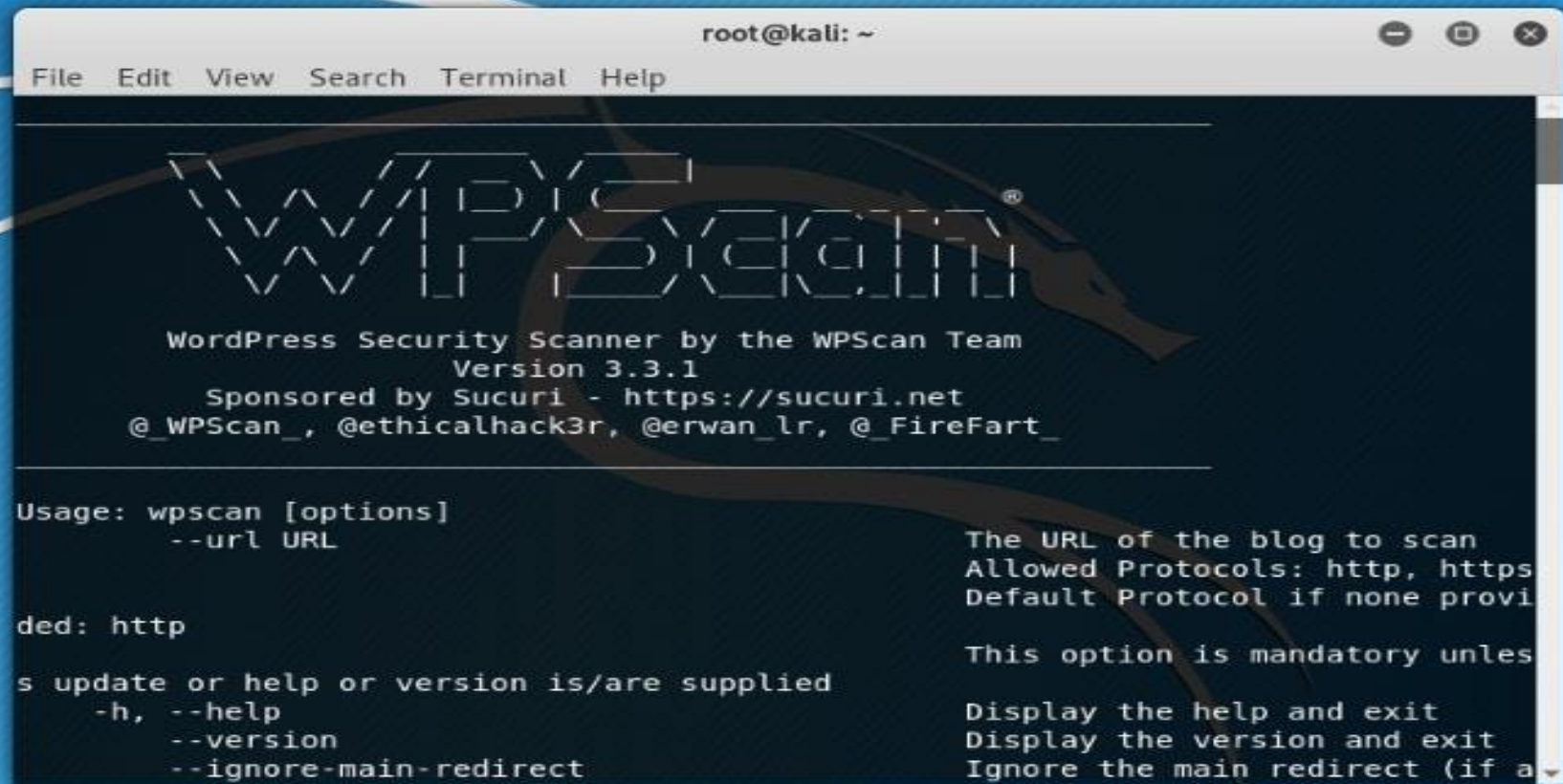
WPSCAN

WordPress is one of the best open source CMS and this would be the best free WordPress security auditing tool. It's free but not open source.

If you want to know whether a WordPress blog is vulnerable in some way, WPScan is your friend.

In addition, it also gives you details of the plugins active. Of course, a well-secured blog may not give you a lot of details, but it is still the best tool for WordPress security scans to find potential vulnerabilities.

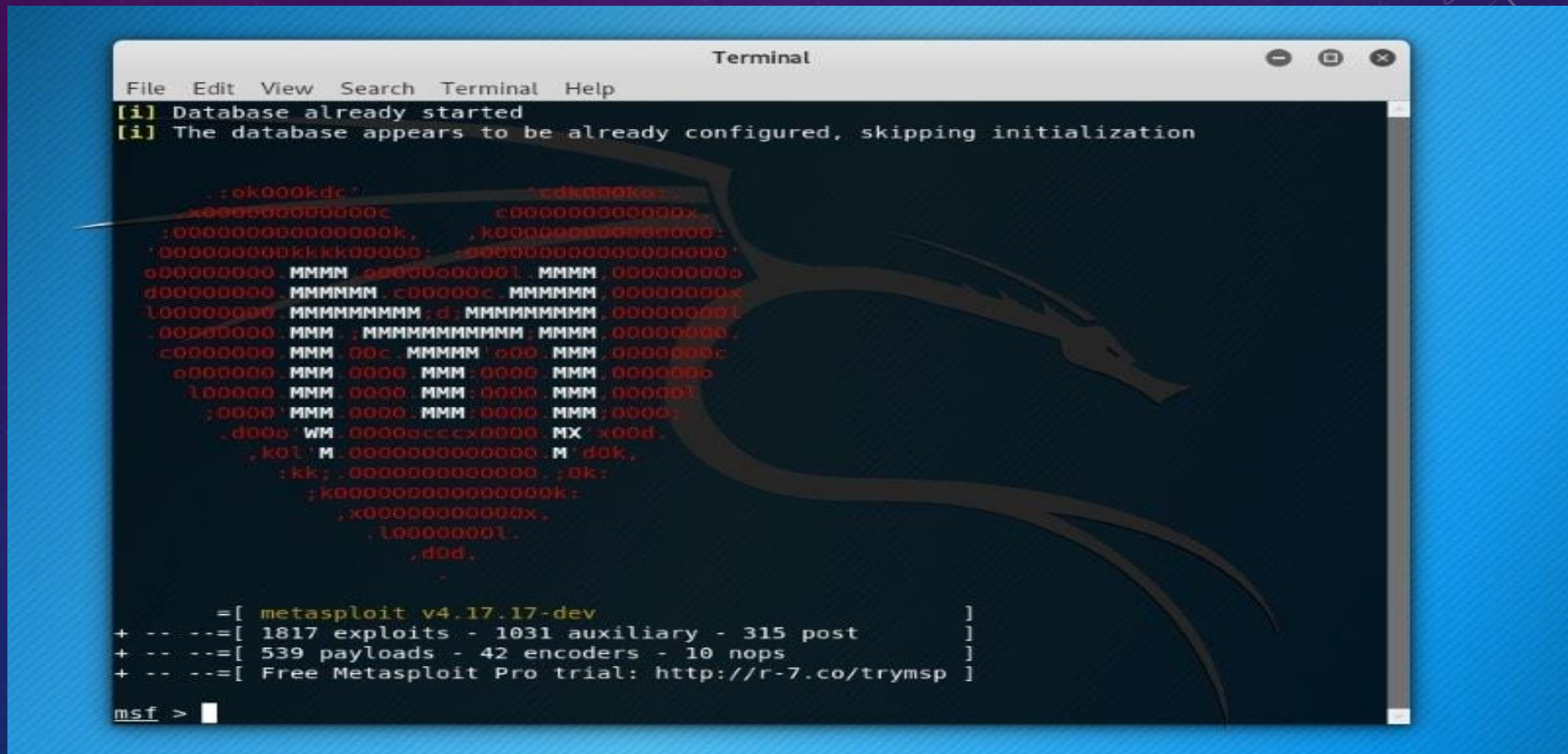
WPSCAN



```
root@kali: ~  
File Edit View Search Terminal Help  
  
  WPSCAN®  
WordPress Security Scanner by the WPScan Team  
Version 3.3.1  
Sponsored by Sucuri - https://sucuri.net  
@_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_  
  
Usage: wpscan [options]  
    --url URL  
    -u URL  
    -d: http  
    -s update or help or version is/are supplied  
    -h, --help  
    --version  
    --ignore-main-redirect  
  
The URL of the blog to scan  
Allowed Protocols: http, https  
Default Protocol if none provided  
This option is mandatory unless  
Display the help and exit  
Display the version and exit  
Ignore the main redirect (if a
```

METASPLOIT

Metsploit Framework is the most used penetration testing framework. It offers two editions – one (open source) and the second is the pro version to it. With this tool, you can verify vulnerabilities, test known exploits, and perform a complete security assessment.

A screenshot of a terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the Metasploit framework startup process. It starts with two informational messages: "[i] Database already started" and "[i] The database appears to be already configured, skipping initialization". This is followed by a large ASCII art logo of a dragon in red and white. Below the logo, the terminal displays the version and statistics for Metasploit v4.17.17-dev, including the number of exploits, auxiliary modules, payloads, encoders, and nops. It also provides a link for the free trial of Metasploit Pro. The prompt "msf >" is visible at the bottom left.

```
File Edit View Search Terminal Help
[i] Database already started
[i] The database appears to be already configured, skipping initialization

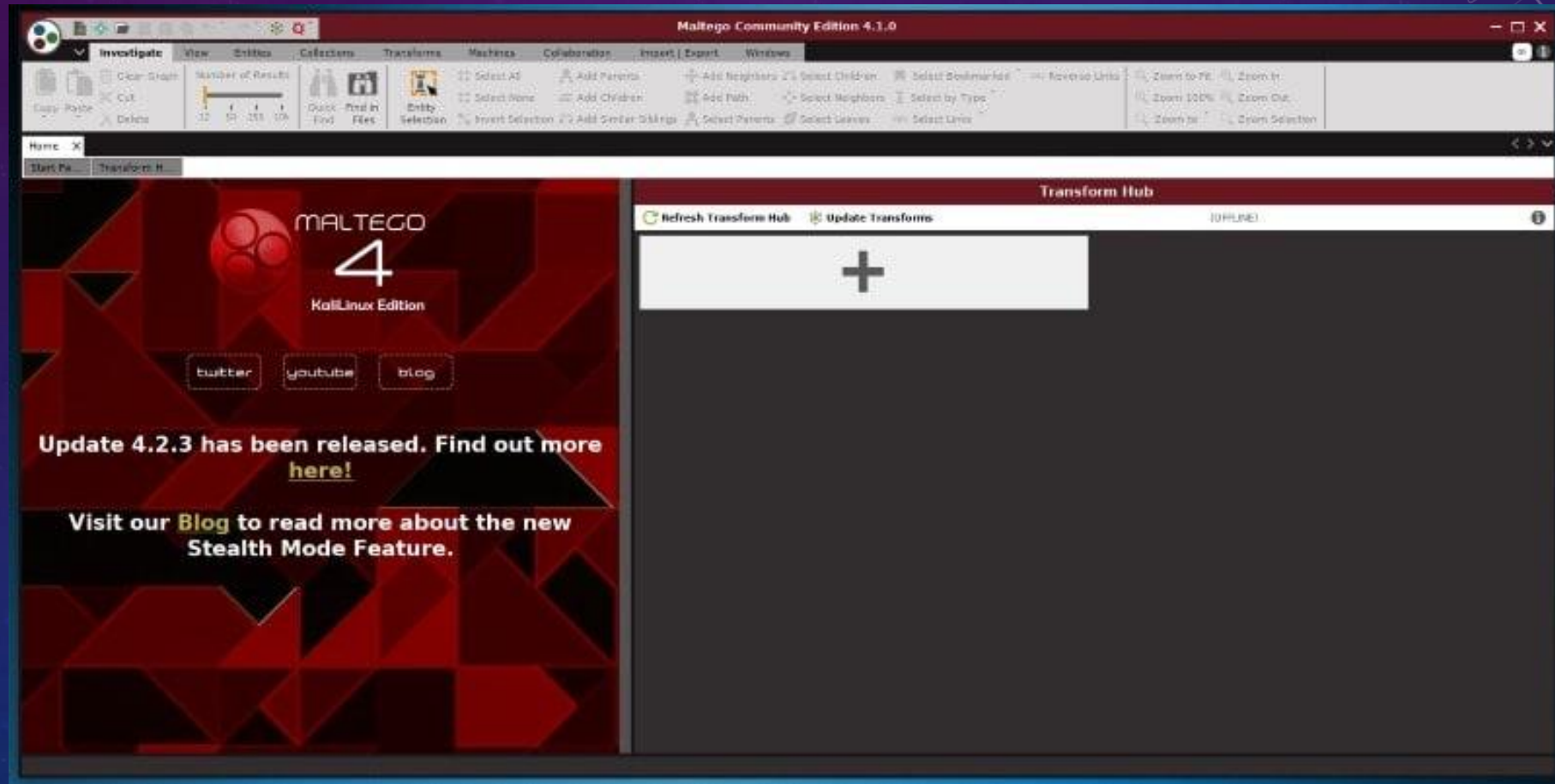
      .:ok000kdc'      'cdk000ko:
      x0000000000000c  c000000000000x
      :000000000000000k,  k00000000000000-
      '000000000k000000:  0000000000000000
      000000000 MMMM .0000000000001 MMMM 000000000
      000000000 MMMMMM .c00000c MMMMMM 00000000x
      100000000 MMMMMMMMMM .d: MMMMMMMMMM 000000001
      .000000000 MMM .MMMMMMMMMMMMM MMMM 000000000
      c00000000 MMM .00c MMMMM '000 MMM 00000000c
      000000000 MMM .0000 MMM .0000 MMM 00000000
      100000000 MMM .0000 MMM .0000 MMM 00000000!
      :000000000 MMM .0000 MMM .0000 MMM 00000000:
      .0000 WM .000000000000 MX x000.
      .kol M .0000000000000 M dok,
      :kk: .00000000000000 :0k:
      :k0000000000000000k:
      .x00000000x.
      .100000001.
      .000.

      =[ metasploit v4.17.17-dev                               ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post             ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops                ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

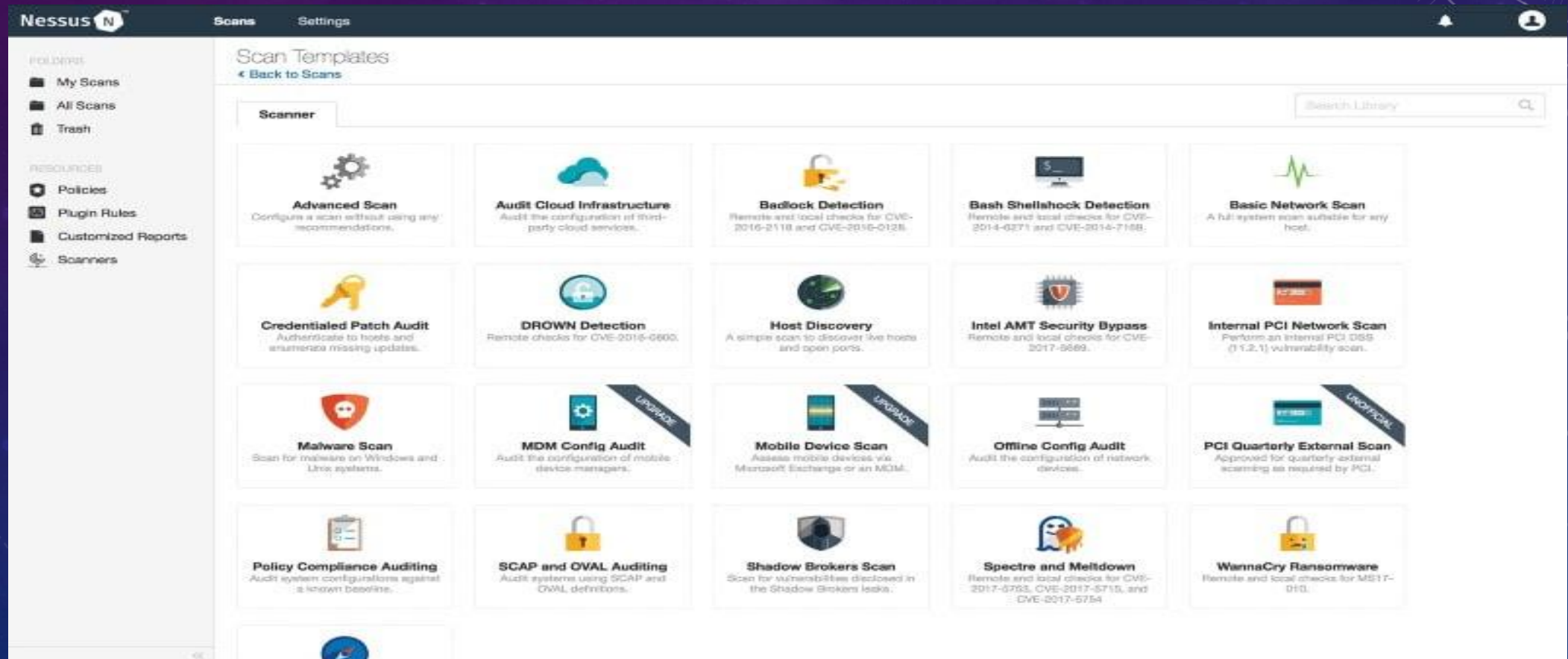

MALTEGO

Maltego is an impressive data mining tool to analyze information online and connect the dots (if any). As per the information, it creates a directed graph to help analyze the link between those pieces of data.



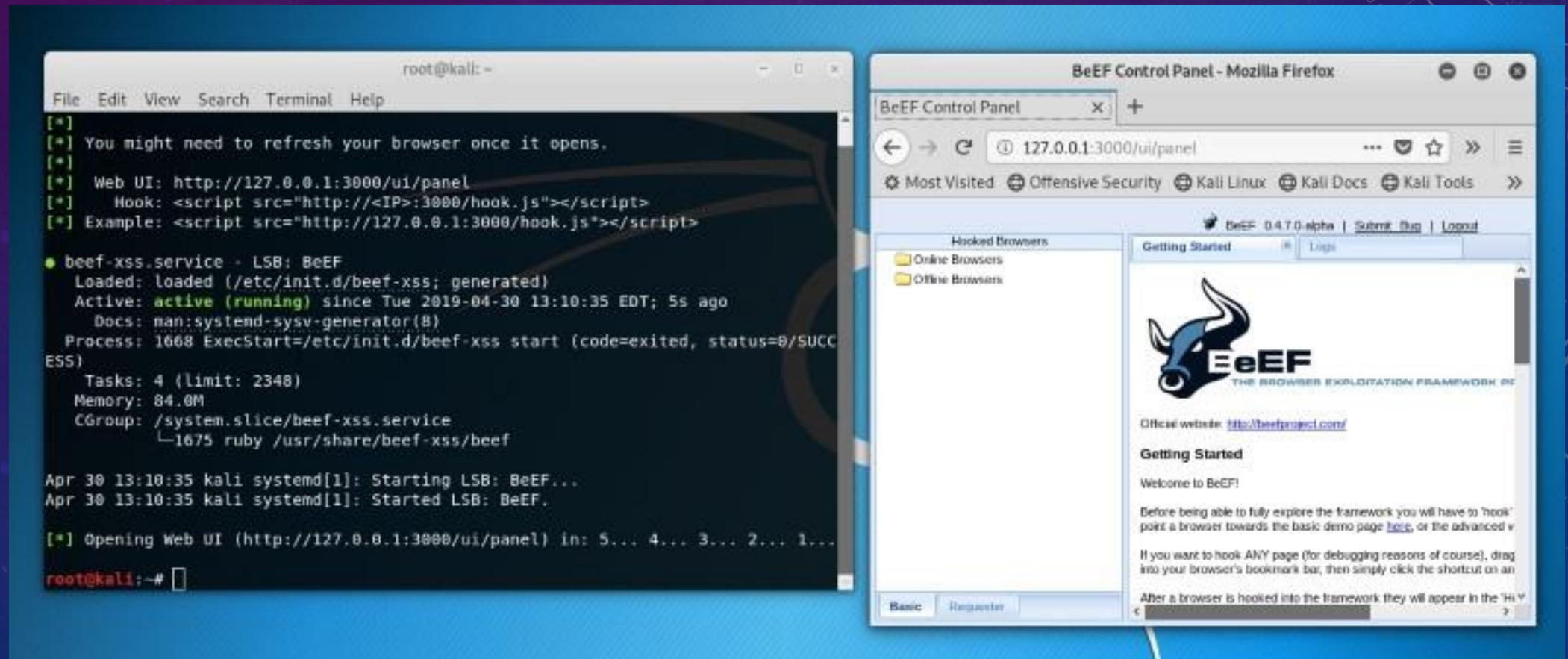
NESSUS

If you have a computer connected to a network, Nessus can help find vulnerabilities that a potential attacker may take advantage of. Of course, if you are an administrator for multiple computers connected to a network, you can make use of it and secure those computers.



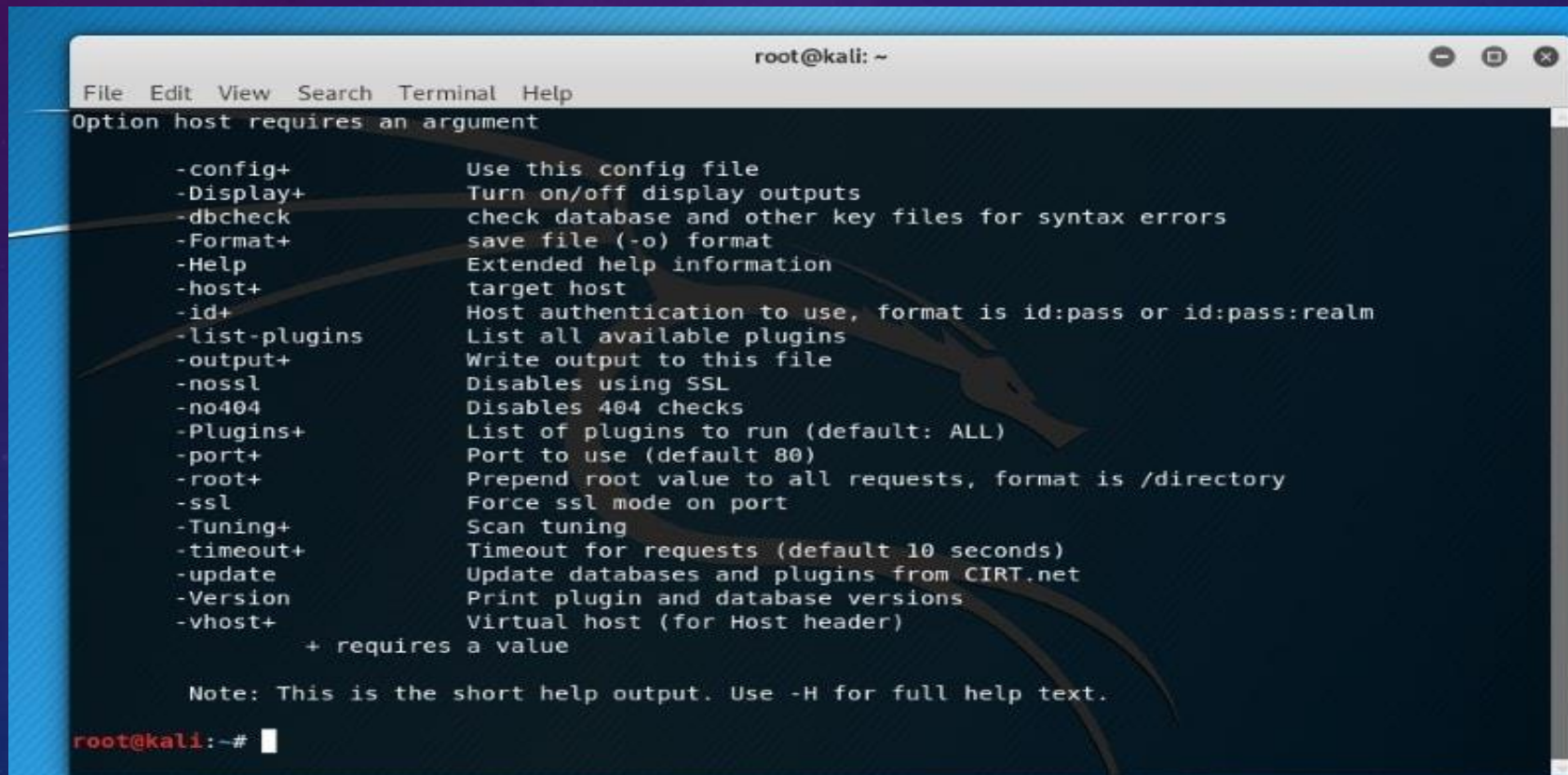
BEEF

BeEF (Browser Exploitation Framework) is yet another impressive tool. It has been tailored for penetration testers to assess the security of a web browser.



NIKTO

Nikto is a powerful web server scanner – that makes it one of the best Kali Linux tools available. It checks in against potentially dangerous files/programs, outdated versions of server, and many more things.

A screenshot of a terminal window titled 'root@kali: ~'. The window shows the output of the 'nikto' command, which is a list of options and their descriptions. The options are listed on the left, and their descriptions are on the right. The options include: -config+, -Display+, -dbcheck, -Format+, -Help, -host+, -id+, -list-plugins, -output+, -noss, -no404, -Plugins+, -port+, -root+, -ssl, -Tuning+, -timeout+, -update, -Version, and -vhost+. The descriptions are: 'Use this config file', 'Turn on/off display outputs', 'check database and other key files for syntax errors', 'save file (-o) format', 'Extended help information', 'target host', 'Host authentication to use, format is id:pass or id:pass:realm', 'List all available plugins', 'Write output to this file', 'Disables using SSL', 'Disables 404 checks', 'List of plugins to run (default: ALL)', 'Port to use (default 80)', 'Prepend root value to all requests, format is /directory', 'Force ssl mode on port', 'Scan tuning', 'Timeout for requests (default 10 seconds)', 'Update databases and plugins from CIRT.net', 'Print plugin and database versions', and 'Virtual host (for Host header)'. A note at the bottom says: 'Note: This is the short help output. Use -H for full help text.' The terminal prompt is 'root@kali:~#'.

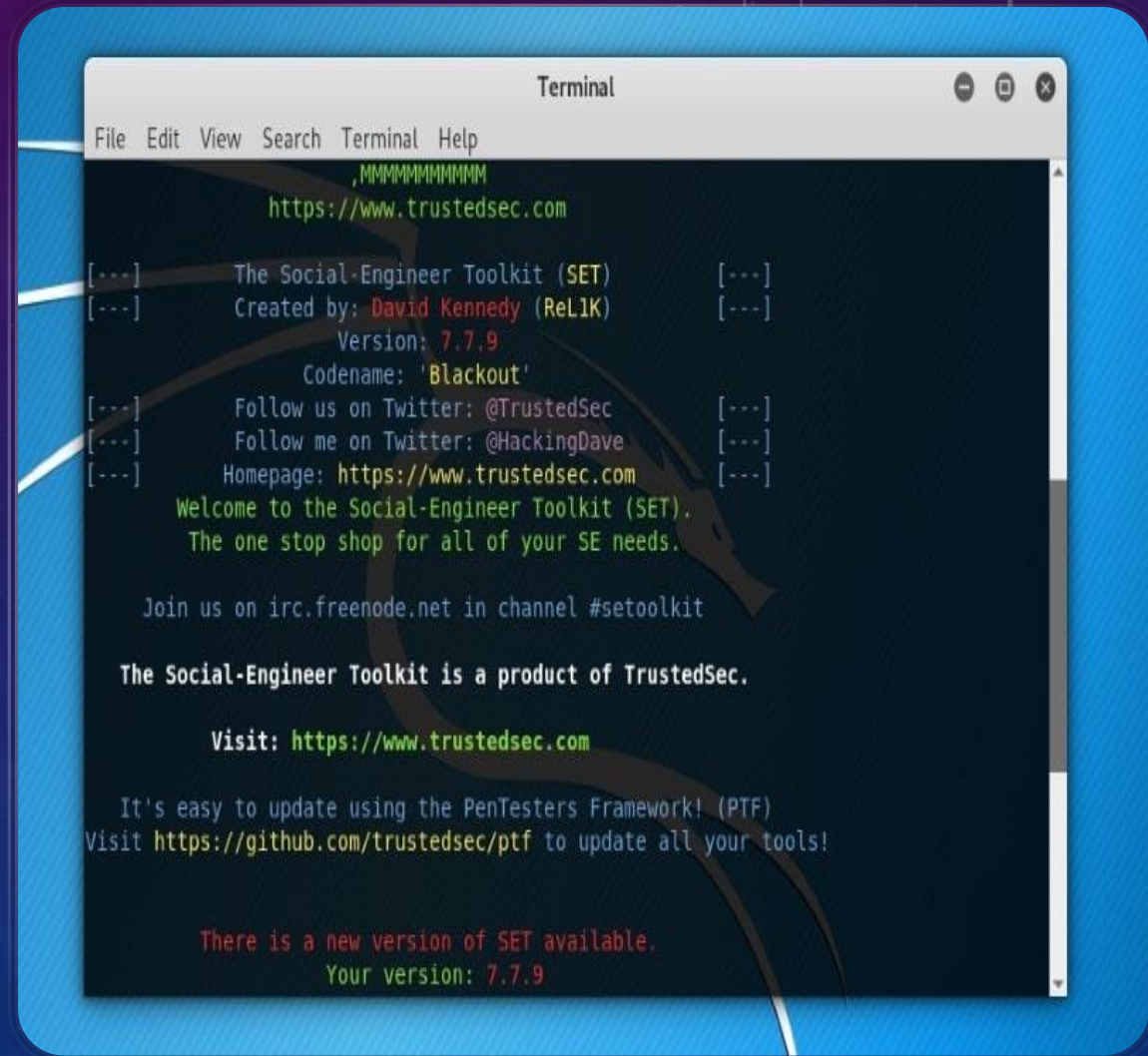
```
root@kali: ~
File Edit View Search Terminal Help
Option host requires an argument

-config+      Use this config file
-Display+     Turn on/off display outputs
-dbcheck      check database and other key files for syntax errors
-Format+      save file (-o) format
-Help         Extended help information
-host+        target host
-id+          Host authentication to use, format is id:pass or id:pass:realm
-list-plugins List all available plugins
-output+      Write output to this file
-noss         Disables using SSL
-no404        Disables 404 checks
-Plugins+     List of plugins to run (default: ALL)
-port+        Port to use (default 80)
-root+        Prepend root value to all requests, format is /directory
-ssl          Force ssl mode on port
-Tuning+      Scan tuning
-timeout+     Timeout for requests (default 10 seconds)
-update       Update databases and plugins from CIRT.net
-Version      Print plugin and database versions
-vhost+       Virtual host (for Host header)
              + requires a value

Note: This is the short help output. Use -H for full help text.
root@kali:~#
```


SOCIAL ENGINEERING TOOLKIT (SET)

If you are into pretty serious penetration testing stuff, this should be one of the best tools you should check out. Social engineering is a big deal and with SET tool, you can help protect against such attacks.

A screenshot of a terminal window titled "Terminal" showing the output of the Social-Engineer Toolkit (SET). The terminal has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The output is as follows:

```
,MMMMMMMMMMMM
https://www.trustedsec.com

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
      Version: 7.7.9
      Codename: 'Blackout'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.9
```

THE END 😊