

Cybersecurity Information Gathering using Kali Linux

Tim Scott

Cybersecurity Information Gathering using Kali Linux

by Tim Scott

About the Author

Tim Scott is a professional software developer and author. He has worked in one of the worlds leading pharmaceutical companies for over 25 years and has experience of the whole software development stack, including validation and training. His current focus is in the cybersecurity sector, promoting good security practices.

Preface

‘Cybersecurity Information Gathering using Kali Linux’ is a beginners book designed to explain what cybersecurity information gathering is, and how to use this knowledge to improve the security of data and programs. It’s not a manual on how to hack, but it does provide insight into information which may be required by hackers, as a precursor to hacking or penetrating a computer system. Information gathering (or target reconnaissance) can be thought of as organized curiosity, it’s about researching a subject rather than necessarily how to apply any discovered vulnerabilities. It is a major part of the hacking process time, and it is key to identifying exploitable security weaknesses.

Hacking of websites, networks, theft of corporate and private data, identity theft and scams have all become a part of everyday news. However, when news of hacking is reported, it does not normally convey the type of background work and organized effort it takes to implement a hack. The result is that many people perceive hacking to be typically based on a group or person, quickly and cleverly just pressing a few buttons and magically gaining access to a website or network. This can encourage data owners to become complacent and have the opinion ‘if they want to get in, there’s not much we can do about it’. It is hoped that this book will encourage a positive approach to dealing with information security, and help keep data safe.

If people can become more security conscious, then cyber-attacks may become less common and less effective.

The use of images in this book, has been kept to a minimum. Images have only been used where they really add value to either a description, or improve understanding. They have been largely excluded, because eBooks are not the best format for displaying images. Additionally, it’s hoped that fewer images provides a more concise feel to the book, and improve the effectiveness of word searching to find required information. However, when images have been used, they have a good resolution level for a quality viewing experience.

As a final note, although the information contained in this book has been prepared carefully, all software that you use remains your responsibility. Kali Linux has many software applications, some of which if used incorrectly or abused, could damage systems and in some cases not be legal. It is your responsibility to make sure that you use the software legally, and please take care to use the software responsibly.

Conventions Used in This Book

Many of the examples in this book require command line entries to be made into a Linux terminal. These entries will be clearly marked and formatted as follows:

command-line code to enter

Data in the boxed area should be entered as a single line followed by pressing Enter.

Table of Contents

[1 Introduction](#)

[Information Gathering](#)

[Why Kali Linux](#)

[Record Your Findings](#)

[A Real Example](#)

[2 Installing Kali Linux](#)

[Overview](#)

[Download and Verify the ISO file](#)

[Create a Live DVD](#)

[Create a Live USB Stick](#)

[Create a Live USB Stick with Persistence](#)

[Partition the USB Stick](#)

[Configure Persistence](#)

[3 Update Kali Linux](#)

[Update Procedure](#)

[Use a Shell Script](#)

[Error - Something has gone wrong](#)

[4 Using Kali Linux](#)

[General](#)

[Region and Keyboard](#)

[5 Stay Anonymous](#)

[Introduction](#)

[Tor - The Onion Router](#)

[Install Tor and Setup ProxyChains](#)

[How to Start a Web Browser](#)

[Verify Anonymous Browsing](#)

[Virtual Private Network \(VPN\)](#)

[Install Required Software](#)

[Connect to a VPN](#)

[6 Basics of Internet Communication](#)

[Introduction](#)

[Bits](#)

[Bytes](#)

[IP Address](#)

[DNS and WHOIS](#)

[TCP/IP](#)

[7 List of Resources](#)

[The Wayback Machine](#)

[8 Search Engines](#)

[Overview](#)

[Google.com](#)

[Google Search Operators](#)

[The Google Hacking Database \(GHDB\)](#)

[Robots.txt](#)

[Other Search Engines](#)

[9 People Sites and Social Engineering](#)

[People Sites](#)

[Social Engineering](#)

[10 WHOIS, DNS and Packet Routes](#)

[Introduction](#)

[Ping](#)

[Maximum Transmission Unit](#)

[Traceroute](#)

[WHOIS](#)

[Deepmagic Information Gathering Tool \(DMitry\)](#)

[Nslookup](#)

[Non-Interactive Mode](#)

[Interactive Mode](#)

[11 Recon-ng](#)

[Introduction](#)

[Workspaces and Add Domains](#)

[Show Available Modules](#)

[Use of Modules](#)

[IPInfoDB](#)

[Combined Example](#)

[Setup Workspace and Domain](#)

[Gather Data](#)

[Report the Data](#)

[12 Final Review and Countermeasures](#)

[Glossary of Terms](#)

1 Introduction

Information Gathering

Unlike the typical movie depiction of hacking, where a target site is hacked into after a quick rattle of the keyboard, hacking is not normally a very quick process. The reality is, it's normally a phased approach over perhaps a number of weeks. The starting point, is the need to know a bit more about a potential target without raising any alarms that a system is being reviewed. These initial steps in determining more about a target, are referred to as 'Information Gathering'.

Information gathering is commonly categorized into two forms:

- Passive information gathering
- Active information gathering

Passive information gathering, relates to profiling a target using third party data. Only resources such as public archives are used, meaning that no direct contact is made with the target site, and therefore is essentially undetectable by the target. Active information gathering refers to direct contact being made with the target site. It may be anything from browsing the company website to running a detailed port scan.

Although information gathering is a key phase in the hacking process, it's not actually what would be commonly referred to as 'hacking', because gaining access to a target comes later. Information gathering and the subsequent stages of hacking are commonly:

- Information Gathering
- Scanning and Enumeration – Mapping and investigation of the target network.
- Gaining Access – Attack of the target site based on identified security weaknesses (exploits).
- Maintaining Access – After successfully compromising a host, it may be possible to enable future reconnection.
- Covering Tracks – To avoid the intrusion being detected, it may be possible to erase log files etc.

In the case of ethical hacking and penetration testing, all phases will be thoroughly scoped and preauthorized prior to commencement. All findings will be reported back to the data owners, to enable security improvements and to provide a complete record of all work performed. Information gathering is a discrete process, but nonetheless a critical phase.

This objective of this book is to encourage awareness of how and why information gathering is performed, so as to encourage good cybersecurity and information security practices.

Why Kali Linux

Linux is a general name which refers to operating systems derived from a Unix-like operating system first released by Linus Torvalds in 1991 (<https://en.wikipedia.org/wiki/Linux>). It was originally developed to be a free operating system to use and to distribute. Since then it has grown in many directions over the decades, so that now there are many different distributions of Linux.

Cybersecurity is a specialized area of computing, and as such, there are specialized applications and operating systems. Probably the most popular Linux distribution for cybersecurity and penetration testing is currently Kali Linux. It is a mature operating system with excellent hardware support and is freely available from <https://www.kali.org> for download and installation.

All practical examples in this book are based on using Kali Linux. Many of the examples use command line tools (a bit like the old DOS screens that you may remember). Although it may seem strange to be using command line tools, many notable penetration testing tools use this environment because it is fast and efficient.

Record Your Findings

Because of the nature of information gathering, a large amount of data is likely to be collected. A key part of information gathering is to be well organized and structured in the way data is recorded. Open source software tools are available which are specifically designed to assist with the recording of cybersecurity information gathering. However, they are not necessary and conventional spreadsheets work very well.

A Real Example

Having covered a bit about the hacking process, you may now be wondering, what's the best way to start security testing and using Kali Linux? The good news is, that there are websites setup to enable you to. practice hacking techniques. One in particular (<https://www.hackthissite.org>) is very informative and features quite a bit in this book in the examples. If you visit the site, you may feel that at first glance that it looks a little bit nefarious. It is however a great place to get started studying hacking methodologies and to learn how to find your vulnerabilities before somebody else does.

Please Note: If you are at work on a company network or using a computer or Internet connection that is not yours, it is recommended to verify you have permission to access these websites before you try out the hacking examples.

2 Installing Kali Linux

Overview

Kali Linux is a popular and mature Linux distribution derived from Debian Linux. It is designed for digital forensics and penetration testing, and loads pre-installed with hundreds of applications. It is intuitively laid out to enable you to find penetration testing software based on activity.

Kali has excellent hardware support and may be installed in many different ways. For example, as a Live DVD (just runs from a DVD), a USB memory stick, or just a standard hard-drive installation. Additionally, VMWare, VirtualBox and ARM architecture, Kali images are available for download. Because this book is only providing a basic introduction to Kali, only installation of a Live DVD and USB memory stick will be detailed.

An ISO image of Kali Linux for the required hardware platform can be easily downloaded and used to create bootable media. Probably the simplest way to run Kali, is with a Live DVD, where Kali simply boots from the DVD and does not require use of the hard-drive. However, this has limitations because system changes cannot be saved. It is also possible to create a bootable USB memory stick which permits system settings to be saved, this is referred to as 'persistence'. Both of these installation methods are detailed in this book. However, if you have a spare computer, you may just find it simplest to use the Live DVD to install Kali onto your hard-drive. This will of course overwrite any existing data, but will be very quick and efficient to work with.

A bootable USB memory stick with persistence is a very popular method of regularly using Kali Linux. It does take a little more time to setup than a Live DVD, but can run very efficiently and is very portable. Once you have a USB memory stick setup as you require, you may find it convenient to use disk imaging software to take a copy of the final updated USB drive. This should enable you to quickly and easily restore a new copy of your USB stick whenever you require.

Typically, you will login to Kali as 'root' user, which means you have full administrative access while using Linux. This is to enable convenient use of the many tools contained in Kali which require this level of access. If you have already used Linux for general purpose computing, you may find this surprising, but for cybersecurity testing it is quite common.

If you need more details regarding the installation of Kali Linux, please refer to the official on-line documentation (<http://docs.kali.org/category/installation/>).

If you do decide to use a USB memory stick, make sure it is able to store at least 8GB data. Fast data read-write times will improve performance and reduce the setup time. However, although at least 8GB is required, bear in mind that larger sizes will take longer to create.

Download and Verify the ISO file

Whatever installation method you choose, you will need to have an ISO image of Kali Linux. You can download this from the official Kali Linux website at <https://www.kali.org/downloads/>. You will need to choose the correct ISO image for the

computer you are using. The examples in this book are demonstrated using Kali Linux 64 bit, Version 2.0.

Before you begin to download the ISO image file, please make a note of the SHA1 checksum specified in the SHA1Sum column for your particular download.

If you downloaded the ISO file using a Windows PC, you possibly won't have necessary software to verify the SHA1 checksum. The Microsoft 'File Checksum Integrity Verifier utility' works well. It's free to use and download from Microsoft at <https://support.microsoft.com/en-gb/kb/841290>.

When you open this web-page, scroll down a bit and you will see a link to download the file, with the text 'Download the File Checksum Integrity Verifier utility package now.'

The downloaded file (Windows-KB841290-x86-ENU.exe) is a self extracting executable file. Simply double-click the file in Windows Explorer and follow the on-screen instructions. Choose a convenient location to extract the files to. The extracted file is 'fciv.exe' and does not require any specific installation to use it, however, it is a command-line tool, so don't expect to double-click on it and see it open.

fciv.exe as stated previously is a command-line tool, and may be setup for use on a PC in a few different ways. To quickly and easily use fciv.exe to determine the SHA1 checksum for the downloaded file, proceed as follows:

1. Open Windows Explorer (shortcut: WindowsKey+E).
2. Copy the fciv.exe file to the same folder as the downloaded iso file.
3. Hold down the Shift key and right-click the folder containing both files. Select 'Open command window here'.
4. In the command window, enter the following command (where 'downloadedfilename' is the full name of the ISO file you downloaded):

```
fciv.exe -sha1 downloadedfilename
```

The result of this should match the stated SHA1 checksum value stated when you downloaded your file.

If for any reason the checksum does not match the specified value, simply retry downloading the ISO and recheck the SHA1 value.

Create a Live DVD

This section only relates to creating a Live DVD, if you require a USB installation, you do not need to follow through this section.

Once you have a verified ISO image file, you can proceed and create a bootable live DVD. Creating a bootable Kali Linux DVD in Windows should be straight forward.

1. Put a blank DVD into the DVD writer (close any boxes automatically appearing on-screen).
2. In Windows Explorer, right-click on the ISO file and select 'Burn disk image'.
3. Tick the 'Verify disc after burning' and press 'Burn'.

After a short while, you should have a DVD that you can use to get started working with Kali Linux. If you put it into your computer and reboot or switch on the computer, assuming your BIOS is configured to permit a DVD booting-up, you should soon see the Kali boot screen:



Select the 'Live' option and press Enter.

Kali will then simply boot-up into memory without using your hard-drive. However, although all the software is usable, any changes or settings you select will not be saved if you switch off your computer. If you would like your changes to be saved, you will need to either install it to your hard-drive or make a 'persistent' copy onto a USB stick.

If you want to install Kali to your computer's hard-drive, simply select the 'Install' option at the boot screen and press Enter. Then follow the on-screen instructions. Please be warned however, that you will delete and over-write the contents of your hard-drive.

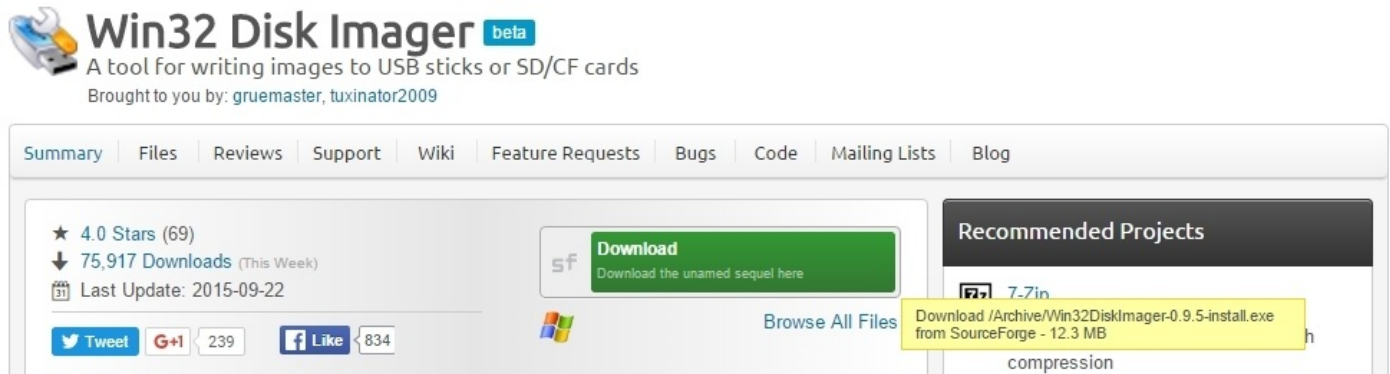
Create a Live USB Stick

This section explains how to create a Live USB stick. If you require a USB stick with persistence, you need to perform this section and then continue with the procedure in the next section to enable persistence.

The Kali.org website provides very complete information describing how to install Kali Linux onto a USB memory stick (pdf file): <http://docs.kali.org/pdf/articles/kali-linux-live-usb-install-en.pdf>. This section explains a similar routine, but provides a bit more clarity with downloading and using the software.

If you are preparing the USB drive on a Windows machine, you will need disk imaging

software. A convenient application for this is ‘Win32 Disk Imager’. This is free software, and a well known and used open source application. The main ‘Win32 Disk Imager’ Web-site is as follows: <http://sourceforge.net/projects/win32diskimager/>. There is a banner advert at the top of the web page, but more centrally there is a green Download button. If you hover over the button it will indicate the download source. Click the green Download button:

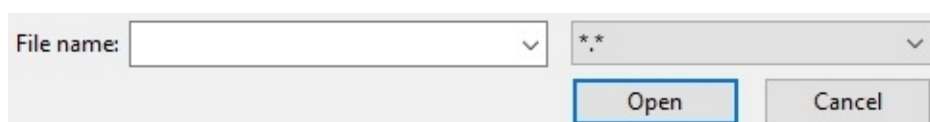


After the file has finished downloading, open Windows Explorer and double-click on the file to install it to your PC.

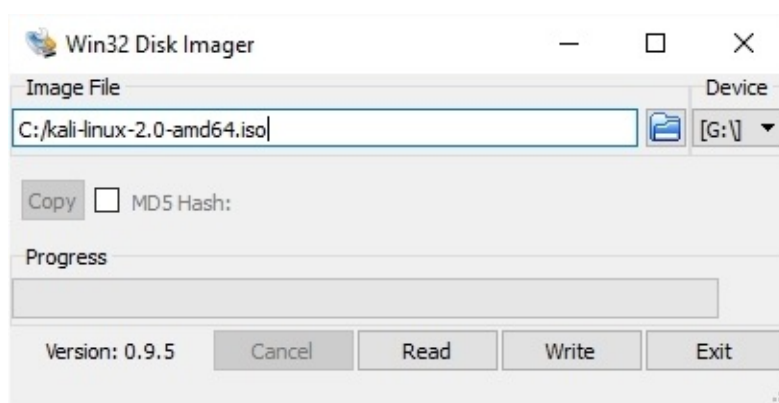
After you install the software to your PC, you will find a shortcut to it in the application menu under ‘Image Writer’.

To prepare a Live memory stick, proceed as follows:

- 1) Plug your USB stick (8GB min) into your Windows USB port and launch the ‘Win32 Disk Imager’ software.
- 2) Choose the Kali Linux ISO file to be imaged. Note, in the ‘Select a disk image box’, the default file to locate is an *.IMG file, change this to be *.* so that you can see the required ISO file:



- 3) Verify that the USB drive to be overwritten is the correct one (in this example it is the G:\ drive):



- 4) Press the Write button. This will use the ISO image file to setup the USB stick as a Kali Linux bootable USB drive.
- 5) Once the imaging is complete, safely eject the USB drive from the Windows machine.

You can now use this USB device to boot into Kali Linux.

Please bear in mind, that the USB stick is still not capable of saving setup changes to Kali. To do this you will need to follow through the following sections, detailing 'Partition the USB Stick' and 'Adding Persistence'.

Create a Live USB Stick with Persistence

This section explains how to add 'persistence' to a Live USB memory stick. To proceed with this section, you will need to have already created a Live USB memory stick as detailed in the previous section.

Partition the USB Stick

Proceed with this section if you would like to use a Windows PC, to setup a new partition to your USB drive to hold persistent data. To do this, you will need to adjust the partition on the Kali USB drive.

Kali.org provide instruction with setting up persistence, but this is based on using the Linux operating system (<http://docs.kali.org/downloading/kali-linux-live-usb-persistence>).

If you would like to setup USB persistence using a Windows computer, you may not have appropriate software. The example in this book worked well using the 'Partition Wizard Free Edition'. It is convenient and free to use, and available at: <http://www.partitionwizard.com/free-partition-manager.html>.

Click on the 'Free Download' button:



You will be directed to the cnet.com website. Simply click on the 'Download Now' button to download the installation file:

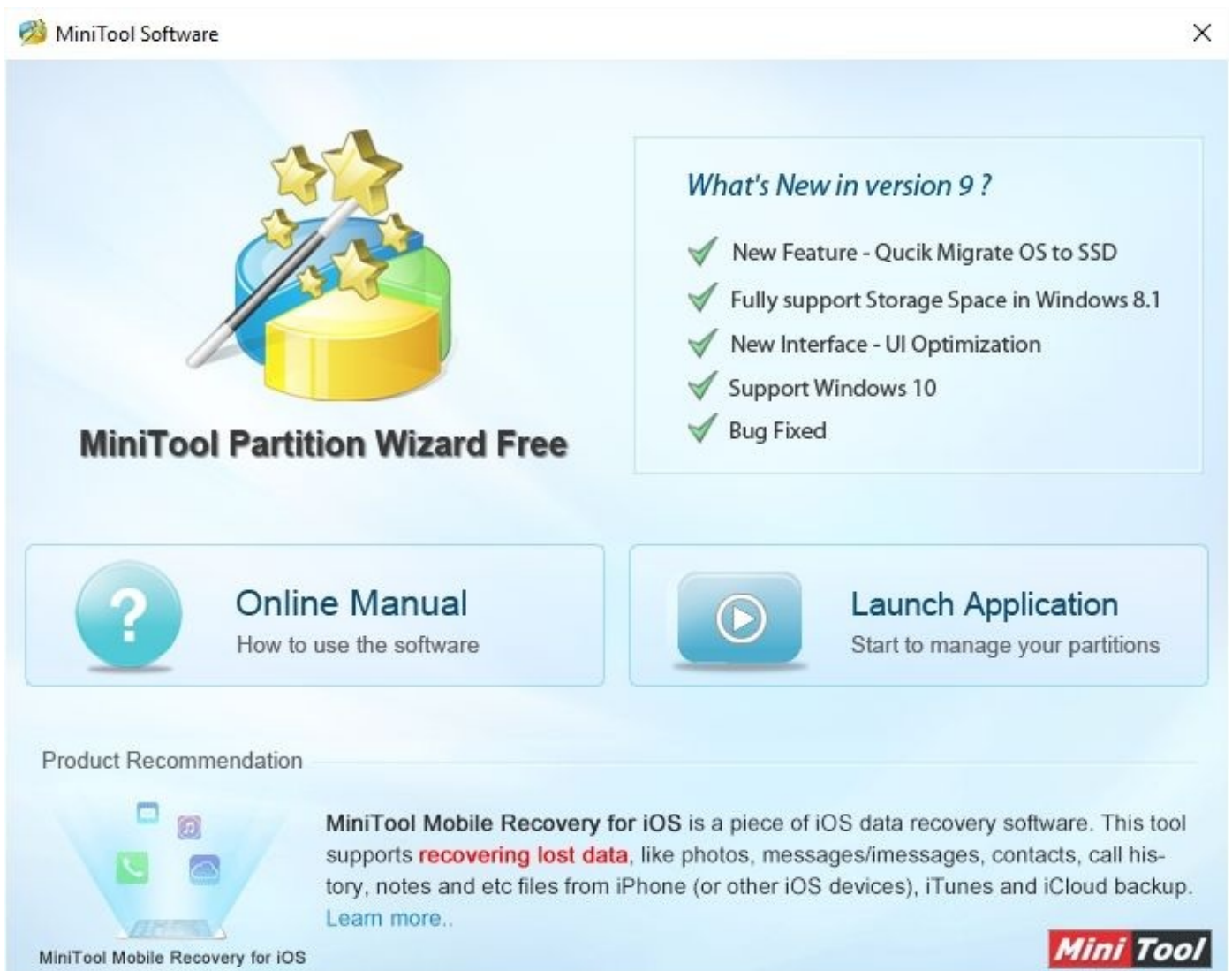


MiniTool Partition Wizard Free Edition

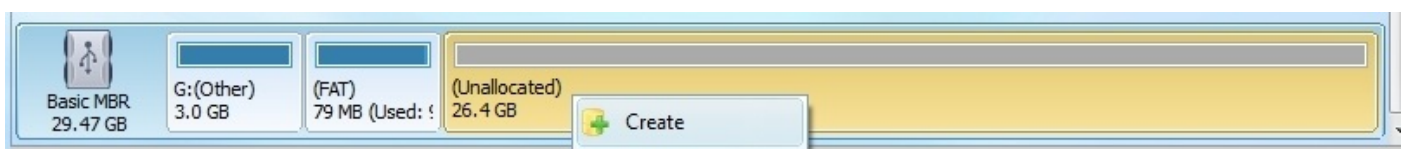


Open up windows explorer and double-click the downloaded file (in this example it is 'Pwfree91.exe') to install it to your PC.

When installed, plug the USB drive pen into your computer and click on 'Minitool Partition Wizard Free' in the Windows Application menu. Then click on the 'Launch Application' button:



This will launch the the partition wizard software and enable you to see the USB drive. In this example, it is represented by the drive letter G. Right-click on the Unallocated partition and select 'Create':



A warning will be displayed indicating that the new partition cannot be used in Windows, simply press 'Yes' to continue. Setup the 'Create New Partition' box as follows:

- Create As: Primary
- File System: Ext2
- Drive Letter: None
- Cluster Size: Default
- Partition Label: persistence

Create New Partition

Please specify the size and the location for the new partition.

Partition Label: persistence

Create As: Primary Drive Letter: None

File System: Ext2 Cluster Size: Default

Size And Location

4.01 GB

Unallocated Space Before: 0.00 MB

Partition Size: 4110.41 MB

Unallocated Space After: 22891.84 MB

Create Partition Tutorial

OK Cancel

This partition will be the persistent data partition, large partitions will take longer to create and will be slower to run. You may reduce the size of the partition if you require. In the example, the partition is approximately 4GB. Press OK to accept your settings, and then press the button marked 'Apply' in the top left corner of the application.

When this is complete, close the partition editor and eject your USB stick from the computer.

You now have a Live USB stick with a partition ready to be used to hold persistence data. To complete the procedure, you will need to follow through the next section, 'Adding Persistence'.

Configure Persistence

You should now have a Live USB stick with a partition ready to hold persistence data. This section details how to configure Kali to enable you to use this partition to actually hold the persistence data.

Kali.org provide detailed instruction with setting up persistence (<http://docs.kali.org/downloading/kali-linux-live-usb-persistence>), but this sections aims to provide a bit more clarity for new users. The instructions below relate to the section marked ‘Adding Persistence to a Kali Linux Live USB Drive’ section 4 (the previous sections relate to setting up the partition, using Linux rather than Windows).

Plug the USB stick into the computer you intend to run Kali Linux on, and switch on. If the computer’s BIOS is correctly setup to enable booting from a USB device, you should see the following screen appear:



Use the Up/Down arrow keys to select the ‘**Live USB Persistence**’ option and press Enter.

Be patient while the computer starts up, this may take a few minutes (and the screen may go blank for a few moments). Please note, by default, a screen saver is setup with the password ‘toor’ (the root user password).

Click the Terminal icon to start up a Terminal window, and enter the following command to review your drives and partitions:

(Note: If you need help using Kali, please refer to the later section ‘Using Kali Linux’).

```
fdisk -l
```

Fdisk will list all your drives, and also list the USB stick you are running Kali from. Have a look through the list to identify your USB stick.

In this example, the computer’s hard-drive is listed as sda and the USB pen is sdb. The partitions on the USB stick are as follows:

Device	Size	Type
/dev/sdb1	3G	Hidden HPFS/NTFS

/dev/sdb2	78.7M	FAT12
/dev/ sdb3	4G	Linux

In this case ‘/dev/**sdb3**’ refers to the persistence partition created earlier. Notice the Size and Type. A 4GB Ext2 partition was created (Ext2 is a Linux file system).

In this case, the persistence partition is ‘**sdb3**’, but may be different in your case. If yours is different, substitute your partition id wherever ‘**sdb3**’ is shown below:

Make a directory on the file-system to mount your USB stick:

```
mkdir -p /mnt/my_usb
```

Mount the persistence partition on the directory you made:

```
mount /dev/sdb3 /mnt/my_usb
```

Add a configuration file to enable persistence:

```
echo “/ union” > /mnt/my_usb/persistence.conf
```

Unmount the partition and reboot (note the spelling of umount has no letter n):

```
umount /dev/sdb3 && reboot
```

When you reboot, be sure to always select the ‘Live USB Persistence’ option if that is what you require.

You may be concerned that no login or password is required. The screensaver password will however work by default. The later section ‘Update Kali’ should alter Kali so that login is required.

Please note, all of the above settings only apply if you start Kali using the ‘Live USB Persistence’ option at the boot screen. If for example you start Kali using simply the ‘Live’ option, Kali will open but will not use any of your persistent data or settings.

3 Update Kali Linux

Update Procedure

If you have a persistent installation of Kali Linux, it's sensible to ensure all software is up-to-date. Simply proceed with the following four steps, entering each command into a Terminal window (note, you will need an Internet connection for this to work).

1) Download the package lists from repositories and update them to get information on the newest versions of packages and their dependencies:

```
apt-get update
```

2) Update installed software packages. Note the -y option so that you don't have to keep entering yes.

```
apt-get upgrade -y
```

3) Upgrade and remove obsolete packages if necessary:

```
apt-get dist-upgrade -y
```

4) Reboot the machine:

```
reboot
```

Use a Shell Script

As a side-note, if you are familiar with shell scripting, a good way to regularly update Kali is to run a shell scrip which automatically runs these four commands. For example, open a Terminal window and enter the following command to create a new text file and open it into a text editor called Leafpad:

```
leafpad kaliupdates.sh
```

Type the following single line of text into the file:

```
apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y && reboot
```

Save and close the file.

Change file access permissions to enable the file to be executed:

```
chmod +x kaliupdates.sh
```

Execute the script, this will cause the commands to be executed in sequence and finally reboot the machine.

```
./kaliupdates.sh
```

Next time, to execute the script, only the last command needs to be entered.

Error - Something has gone wrong

All going well, your USB memory stick with persistence, will bootup without errors and work well. If however, you boot up and the final graphical display fails, and provides you with a rather unhelpful message such as “Oh no! Something has gone wrong” (yes, really this is a genuine message), do not despair. It may be that the update/upgrade routine did not fully complete.

If you boot up and get the error message, although the screen just looks a light gray color and has no buttons, you may still be able to open a virtual terminal, enabling you to make command line entries. To try this, simply press the following combination of keys:

Ctrl+Alt+F4

If this opens a terminal window, you need to login as root user. Enter ‘root’ for the username, and ‘toor’ for the password.

Now, simply repeat the update routine mentioned in the previous section:

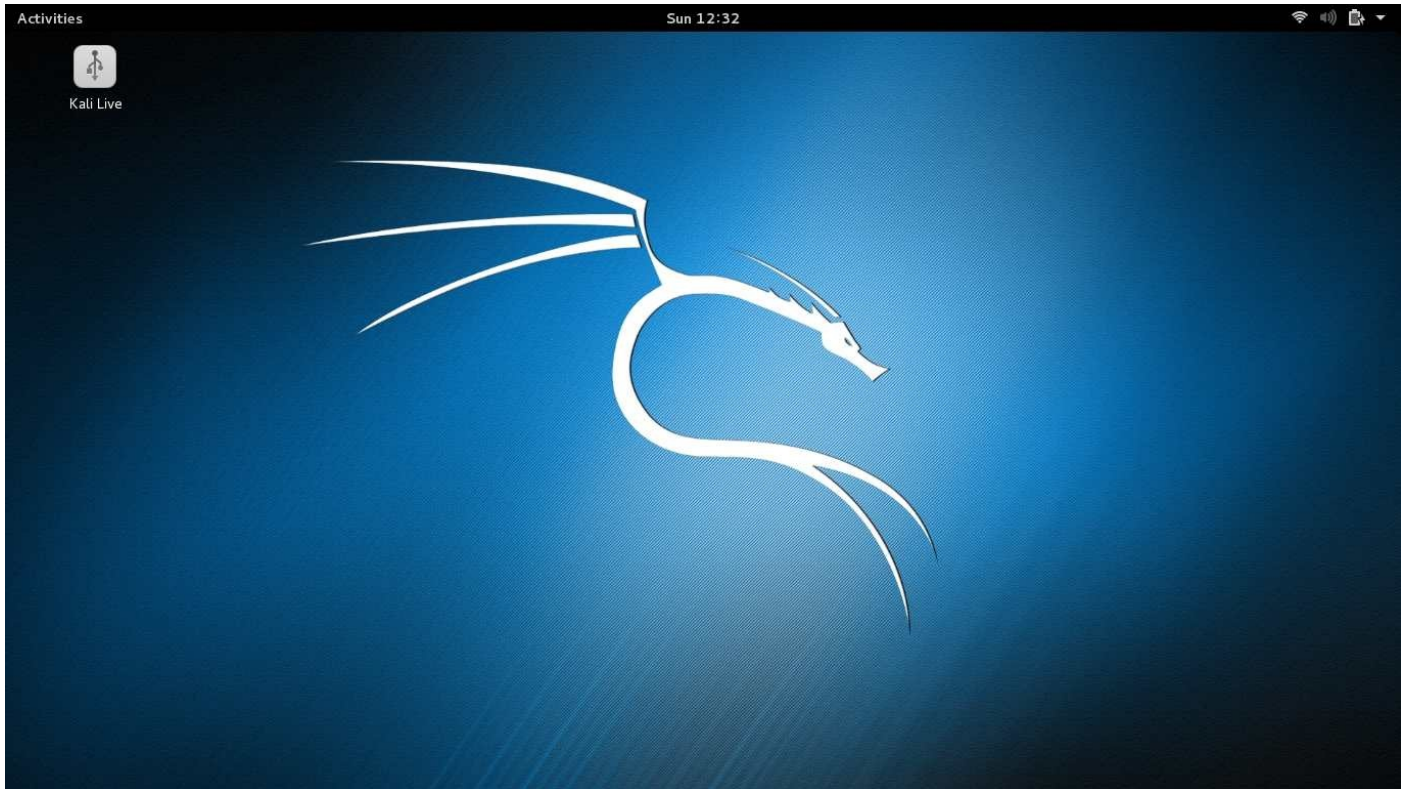
apt-get update
apt-get upgrade -y
apt-get dist-upgrade -y
reboot

All going well, your machine will now function correctly and have ‘persistence’.

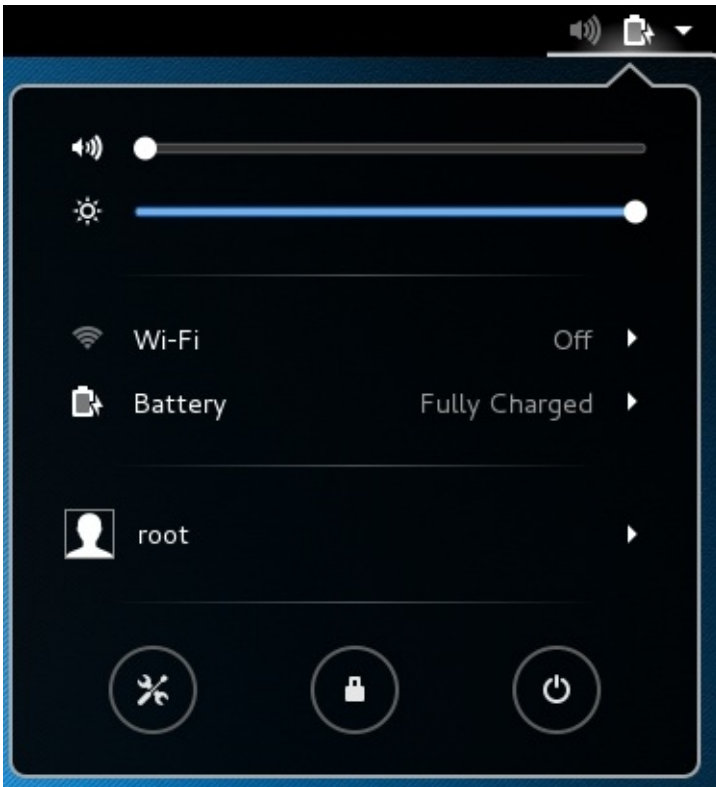
4 Using Kali Linux

General

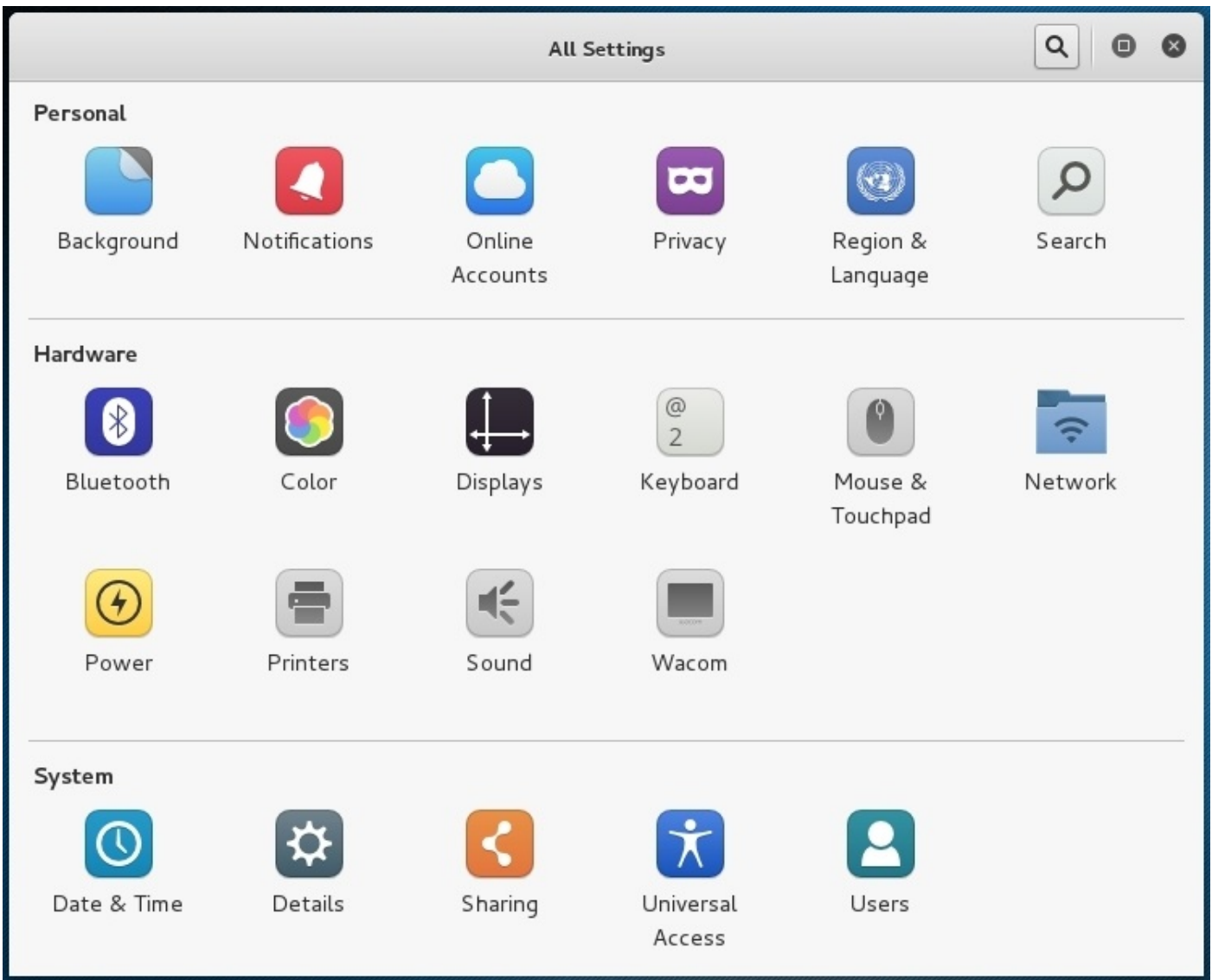
When Kali Linux initially loads up, press 'Esc' to remove the screensaver. Then enter 'root' for user, and 'toor' for password. You should now see the following screen:



The **system status area** to the right of the 'top bar' is useful for closing Kali, setting up Networking/Wifi and general computer status settings:



Notice the tools icon on the bottom-left. If you click on the tools icon, ‘All Settings’ will open, enabling all general configuration settings to be reviewed and edited:



If you click on 'Activities' to the left of the 'top bar' on the main screen, the Activities overview will open. This provides quick and intuitive access to all software applications installed in Kali:



In particular, you should be aware of the Terminal window icon located in the 'dash' (the vertical strip of icons on the left side of the Activities overview) which enables you to open a terminal window for command-line entries:



Notice also the 'Frequent' and 'All' buttons (bottom center of screen), enabling you to either see all of your applications, or just the ones you have already used.

This has been a very brief overview of how to find applications and setup Kali. It's aimed at providing you with helpful pointers to get you 'up and running' as quickly as possible with Kali. Further information is available online at <http://docs.kali.org>, and via the built in help system (simply press the F1 key to open). To search the help system for specific topics, just press the magnifying glass icon, and enter your text. For example, search on 'wifi' for assistance with connecting to your wireless network.

Region and Keyboard

Before you start using Kali Linux, it's a good idea to configure your region settings. If you don't, you might have difficulty finding the keyboard keys you require when using a Terminal window.

1) From the system status area to the right of the 'top bar', open 'All Settings'.

2) In the 'Personal' section, click on 'Region & Language'.

- Click on 'Language' and select your language, then press 'Done'.
- Click on 'Formats' and select your region. Note the preview of formats, then press 'Done'.
- If you require a different Input Source, click on the '+', select required source and press 'Add'.
- Click the 'x' to close the Region & Language box.

3) From the system status area to the right of the 'top bar' select your required input. Note, if only have one available input selection, it will be selected by default.

5 Stay Anonymous

Introduction

This chapter aims to provide insight into how a hacker may quite easily remain anonymous on the Internet, and perform reconnaissance on a target website without greatly compromising their own security.

Tor and VPNs are detailed later in this chapter and both enable anonymous use of the Internet. 'Tor' is possibly a rather slow way to regularly use the Internet, but a VPN service can provide you with a safe, secure and high-speed connection. VPN's commonly provide high security firewalls and encryption and can become an additional security layer to Internet shopping, banking and general communication.

Tor - The Onion Router

Anonymity like security, cannot be absolute, but this quick guide to using Tor should give you what is generally regarded as a good level of privacy from being tracked or monitored while you browse. Please note that these instructions relate to setting up the browser to use Tor, but software other than browsers will not be detailed.

Tor is a massive network consisting of computers known as Tor Relay Nodes. They provide an encrypted route into the Internet and route Internet traffic in a randomized way through different Tor Relay Nodes. If for example, you request a specific web-page by entering a URL into your browser, this request will be encrypted and sent through the Tor network via a randomized path to and from the destination server. In this way the Tor network provides anonymity. This means that the following links will be securely connected:

Source Computer -> ISP -> Tor

However, the final stage of the connection, between Tor and the web server is not encrypted by Tor. So consider the following two data request scenarios (the first one is to a secure HTTPS web server, and the second one is not):

1. Source Computer -> ISP -> Tor -> HTTPS Web server
2. Source Computer -> ISP -> Tor -> **HTTP Web server**

In the first scenario the whole path is encrypted, because the source computer has a secure encrypted connection with the HTTPS web server, so Tor at the final Node has a secure connection with a secure web server. In the second example however, Tor does not connect with a secure server, so data between Tor and the HTTP web server is not encrypted. This means that data at this stage is technically not secure, unencrypted and viewable by third parties. Although this data will relate to an apparently untraceable IP address, it is still possible for the content to be intercepted. Of course if this data contains names of individuals it may provide immediate indication of the sender. However, even styles of entering text can be used to identify the sender, this is referred to as 'Writeprints'. Bloggers and tweeters for example may have a particular writing style which may be used to provide an indication as to who the sender of the data actually is. The point of this is, is that if a connection is made to an HTTP server, one should be aware that data may be reviewed by third parties.

Additional information regarding Tor can be obtained from the Tor website (<https://www.torproject.org/>). The Tor website explains very nicely what Tor is for:

“Tor is free software and an open network that helps you defend against traffic analysis, a

form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security”.

Install Tor and Setup ProxyChains

Please note that if you follow these installation instructions while using the Live DVD version of Kali Linux, your settings will not be saved if you power off your machine. However, this procedure should still work, and enable you to browse using the Tor network.

Tor is well known for providing anonymity while browsing, but it may be interesting to note that it may in certain cases, be used with other programs. ProxyChains (<http://proxychains.sourceforge.net/>) enables you to run a program through a proxy server and can be used to enable software to run using Tor. In fact, the default is that ProxyChains works with Tor.

Open a Terminal window to enable command line entries to be made, and enter the following command:

```
apt-get install tor
```

When tor has been installed, type in the following:

```
apt-get install proxychains
```

```
leafpad /etc/proxychains.conf
```

A text editor will open and display the contents of the proxychains.conf file. On about the 10th line, ensure the hash prefixing dynamic_chain is removed:

```
dynamic_chain
```

On about the 18th line, ensure a hash prefixes the text ‘strict_chain’:

```
#strict_chain
```

Page down to the bottom of the file. After the ProxyList section on the last line of the file, enter the following text to ensure the socks5 is present:


```
socks5 127.0.0.1 9050
```

Save and close the proxychains.conf file.

Before proceeding, update Kali Linux as detailed in the Kali Linux section, titled ‘Update Kali’.

How to Start a Web Browser

Start the Tor service:

```
service tor start
```

Verify Tor is started:

```
service tor status
```

You should see in the generated text, that Tor is active and running. Open a browser using proxychains:

```
proxychains iceweasel check.torproject.org
```

This should open up the web browser called ‘IceWeasel’ and connect to the Internet using Tor. The website (<https://check.torproject.org>) should be visible and verify the browser is correctly configured to use Tor, but provide you with a warning that you are not using the specific Tor Browser.

If you would like to use the Tor Browser, download it from the Tor website (<https://www.torproject.org>) and follow the instructions given on the website.

Verify Anonymous Browsing

Every time you go on-line via Tor, it’s a good idea to verify your browser is securely connected to the Tor network by visiting the Tor Project website (<https://check.torproject.org>). The website will clearly state if there is a problem with your connection.

You can also check the Tor network is providing anonymous connectivity by visiting <https://www.whatismyip.com>. When the site opens, click the button named 'My IP Information' to verify your normal IP and region are not recognized.

It should be emphasized that you have only been provided with a basic Tor setup. You may like to review Tor further by studying the Tor Project website (<https://www.torproject.org>).

Virtual Private Network (VPN)

A Virtual Private Network (VPN), was originally simply used to enable remote offices and users to connect via secure access to their organizations network. However, there are now Internet services setup to provide users with high-security, high-speed, anonymous access to the Internet. This works by setting up a secure link between the user's computer and the VPN service provider (via a VPN 'tunnel').

Because a VPN tunnel provides encrypted data transfer between the user's computer and the VPN service, the data should remain private from your ISP and other third parties. This means that your ISP and third parties, should not be able to review what Internet sites you visit, and the target site connection should be anonymous.

The final link between the VPN provider and the target site is ideally to a secure server. If not, this final stage can potentially be intercepted in a similar way as explained with Tor.

VPN providers may offer improved firewall protection, ad-free browsing, and data compression to save mobile data when using your phone. Probably the main caveat with using VPN services is the slight reduction in network speed, and the nominal fee required by the provider. Free services do exist, but tend to offer lower speeds, and generally be less attractive as a solution. Of course, one has to trust the VPN service provider because there is the potential for data at the VPN server to be reviewed. They may advertise military grade encryption and no logs, but for the paranoid among us, this still may not be enough.

From the point-of-view of cybersecurity testing, you don't necessarily need a VPN service, and one may argue that legal activities do not need to be hidden. However, a review of 'Information Gathering' techniques would not be complete without providing knowledge about how to stay anonymous. Active information gathering, when the target site is reviewed for available information, is normally carried out anonymously. There are in fact many ways of remaining anonymous, but for the purposes of this book, it should be sufficient to be aware of Tor and VPNs.

Install Required Software

If you have an account with a VPN service provider, you will need to have some way of setting up a secure connection with them. They may provide you with proprietary software, or expect you to setup appropriate client software. In Linux, a common solution is to use 'OpenVPN' (see <https://openvpn.net/index.php/open-source.html>). This is open-source, full strength free software. In Kali, with a Terminal window open, it is simple to install. Simply enter the following commands:

<code>apt-get update</code>
<code>apt-get install openvpn</code>
<code>apt-get install network-manager-openvpn</code>
<code>apt-get install network-manager-openvpn-gnome</code>

Before you proceed and attempt to connect to a VPN service, you must update Kali Linux as detailed in the Kali Linux section, titled 'Update Kali'.

Connect to a VPN

After you have installed your VPN software, you can set up the VPN connection:

1. Open the Activities overview and start typing Network in the 'Type to search' box.
2. Click on Network to open the control center.
3. At the bottom of the list on the left, click the + button to add a new connection.
4. Choose VPN in the interface list.
5. Choose which kind of VPN connection you have (if you have an ovpn file, choose 'Import from file...', browse for the file and double-click to open it).
6. Fill in the VPN connection details (if you imported an ovpn file just enter your vpn username and password for the connection), then press Add once you are finished.
7. When you have finished setting-up the VPN, click the system status area on the top bar, click VPN and select the connection you just created. You may need to enter a password for the connection before it is established. Once the connection is made, you should see a lock shaped icon in the top bar.
8. Verify a connection has been made to your VPN service by checking your IP address details. A website such as <https://www.whatismyip.com> can provide you with this information.
9. Hopefully you will successfully connect to the VPN. If not, you may need to double-check the VPN settings you entered. You can do this from the Network panel that you used to create the connection, select the VPN connection from the list, then press the button in the bottom right corner of the panel.
10. To disconnect from the VPN, click the system status area on the top bar and click Turn Off under the name of your VPN connection.

6 Basics of Internet Communication

Introduction

This chapter provides some basic knowledge about the Internet Protocol suite. If you already understand the concepts of IP addresses, DNS, WHOIS and TCP/IP, please skip to the next chapter.

The Internet is all about being a massive network of computers, being able to send and receive data between each other. In data gathering, it helps to have an understanding about the make-up of this data.

This chapter very simply outlines some of the protocols (i.e. standardized methods of information transfer) by which network communications are performed. It looks at how computers are addressed (i.e. identified) using an IP Address and how this rather odd looking numbering system (IP Address) is actually just a convenient way to write a large number.

To understand the format of an IP Address, it helps to have an understanding of bits and bytes, and again, this will be explained in this chapter.

Bits

Digital technology is fundamentally based upon representing data with numbers using only one's and zero's. Because computers use ones and zeros, they are naturally setup to count in binary. Binary counting is simply representing numbers using ones and zeros.

The following table is a short example to show how counting in binary compares to counting in decimal:

<i>Decimal</i>	<i>Binary</i>
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010

Binary counting follows the same principle as decimal counting, in that after all digits reach their maximum (e.g. 111), they all reset to their minimum and increment the next digit to the left (e.g. 1000). Counting then resumes from the right-most digit (e.g. 1001).

In reviewing binary counting, we have also simultaneously been reviewing 'bits'. The term 'bit' is actually just an abbreviation for binary digit, and as the name implies, is a digit in a binary number.

A bit is the smallest unit of information handled by a computer and can be represented by either a pulse sent through a circuit or perhaps more physically by a small reflective spot on a CD. The point is that computers operate using binary, and that all computer storage is based on the ability to retain a binary representation of that data.

Bytes

In the previous section about bits, the table indicated that the maximum value 3 bits can represent is the decimal value 7 (111). If we have 8 bits, the maximum value it may represent is binary 11111111 which is decimal 255.

Byte is an abbreviation for ‘binary term’ and is a collection of 8 bits. 8 bits are able to represent decimal values in the range 0 to 255. A byte can be used for example, to represent a letter of the alphabet by relating it to a character set such as ASCII.

A kilobyte may loosely be referred to as “a thousand bytes”, but it is in fact 1024 bytes. The value 1024 is used because binary is the counting system. This may be simply represented as:

<i>Binary</i>	<i>Decimal Value</i>
1	1
10	2
100	4
1000	8
10000	16
100000	32
1000000	64
10000000	128
100000000	256
1000000000	512
10000000000	1024

As stated previously, a byte is capable of representing decimal values from 0 to 255. The value 255 may be determined by summing the first 8 decimal values listed in the table (1+2+4+8+16+32+64+128).

IP Address

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to an IP based network. In other words all devices connected to the Internet have an IP address assigned to them. It is in effect a name and address for an Internet device.

The basic IPv4 IP address number is a 32-bit number. This means it's a binary number with 32 possible combinations of ones and zeroes. This is a very big number and potentially rather awkward to represent in a memorable way. Fortunately the Internet is sensibly designed, and the 32-bit number is normally split into blocks of 4 x 8-bit numbers. The maximum possible IP value is:

255.255.255.255

DNS and WHOIS

The Domain Name Service (DNS) is an essential part of the way the Internet works. It enables text based Internet addresses such as URL's to be translated into an IP address of a machine. It also provides the hierarchical method by which Internet addresses are constructed. A helpful analogy of DNS is that it's a bit like a phone book for the Internet, it can be used to lookup human-friendly computer hostnames to find their IP addresses (and vice-versa).

A domain name registrar is an organization or commercial entity that manages the reservation of Internet domain names. When a domain name is registered, the registrar requires the assignment of a primary domain name server and at least one secondary name server. If you purchase a domain name via an ISP, this will normally be done for you. These name servers are known as authoritative name servers, because they have been configured by the original source of the domain.

The Domain Name System is maintained by a distributed database system where the nodes of this system are name servers. If an update is made to an authoritative name server, the update will be propagated to non-authoritative DNS servers all over the world, however this may take some time.

The most common types of records stored in the DNS database are:

- DNS zone authority (SOA)
- IP addresses (A and AAAA)
- SMTP mail exchangers (MX)
- Name Servers (NS)
- Pointers for reverse DNS lookups (PTR)
- Domain name aliases (CNAME)

The DNS system is specifically the Internet's IP address database and translator to human-friendly text names. The WHOIS system is the database system used to provide registrant information even if an IP address has not been assigned to a domain name.

TCP/IP

The Internet is basically a collection of networks and gateways that use the TCP/IP suite of protocols to communicate. TCP/IP is an acronym for Transport Control Protocol/Internet Protocol and is a method of communicating packets of data between computers. It was originally created by DARPA, an agency of the United States Department of Defense in 1958.

TCP/IP uses packet-switching technology, which means data can be routed to a destination through any number of transmission points, making the network decentralized and less vulnerable to equipment failure.

TCP provides data integrity and delivery guarantee, by transmitting, and retransmitting packets until the receiver acknowledges the reception of the packet. IP is used to send packets of information to a host based on an IP address.

A datagram is more basic than a packet, and is in fact the basic transfer unit associated with a packet-switched network. Delivery, arrival time, and order of arrival need not be guaranteed by the network, such guarantees are provided by additional layers, to for example provide datagram checksums.

The details of TCP/IP in the table below have been simplified into 4 layers. When a computer communicates with another computer, normally all the layers shown below are used, except that only certain protocols may be applied:

Application Layer This makes the communication between programs and the transport layer. <ul style="list-style-type: none">• HTTP (HyperText Transfer Protocol)• FTP (File Transfer Protocol)• DNS (Domain Name Service)• DHCP (Dynamic Host Configuration Protocol)
Transport Layer Used to establish basic host to host communications through routers. UDP provides data integrity via checksums. TCP provides both data integrity and delivery guarantee by retransmitting until the receiver acknowledges the reception of the packet. <ul style="list-style-type: none">• TCP (Transmission Control Protocol)• UDP (User Datagram Protocol)
Internet Layer Has the function of sending packets of data across networks. IP is used to send packets of information to a host based on an IP address. <ul style="list-style-type: none">• IP (Internet Protocol)• ICMP (Internet Control Message Protocol)• ARP (Address Resolution Protocol)

Network Access Layer

Network hardware protocols such as Ethernet

Note: The above table is not intended to be an exhaustive list of protocols, but rather to just provide an indication as to what each layer is and how it may function.

A good way to explain the layers and the suite of protocol listed, is to draw an analogy to the ‘snail mail’ postal system:

It starts at home in the Application Layer, where you decide that you want to send a letter to someone...

The Transport Layer is a bit like what type of letter you send:

- UDP is like regular mail, to send a letter out you just pop it in an envelope and send it off. If it’s something the recipient requested and they don’t receive it they will request it again. If it’s something you wanted and didn’t get a reply, you will just request it again.
- TCP is a bit like regular mail, but also requires a receipt signature, and the sender receives conformation of successful delivery of the package. Larger more important pieces of data tend to be sent via TCP, but this transfer protocol does have a slightly larger data overhead.

The Internet Layer is a bit like how you address a letter. The sole purpose of IP is to address the packet. It does this by adding additional data to the datagram. ARP is used to resolve a MAC address (the physical address of a computer) within a network and ICMP is a diagnostics protocol for IP.

The data packets are then communicated via the Network Access Layer, which is a bit like the postal delivery infrastructure; with trucks, planes, roads, sorting offices and the people who actually deliver the letters to your door.

The point of this section has not been to provide a detailed description of TCP/IP, but to ensure that you have a reasonable notion about what TCP/IP is, and at least roughly how it functions as a suite of communication protocols. This will help you better understand some of the tools and methods mentioned in this book.

7 List of Resources

The public resources listed below are a quick, easy and passive way to gather information about the target site. It is a great way to see what other people can easily see about your website and may give you a few pointers regarding possible vulnerabilities which need to be reviewed:

The Wayback Machine (<http://archive.org/web/>): This website is detailed more thoroughly in the next section. Basically, it's a freely available archive of timestamped copies of websites over the ages.

CentralOps.net (<http://centralops.net/>): A Domain Dossier is quickly and easily obtained simply by entering a domain or IP address. Get registrant information, DNS records, and more, all in one report. The free service is limited to 50 queries a day.

Netcraft (<http://www.netcraft.com/>): The front page of their site has a sub-title "What's that site running" with a prompt requesting a website URL to be entered. The following list is a brief summary of the sort of information you are likely to retrieve:

- Background (Description of site, Keywords)
- Network (IP address, Registrar, Nameserver, Hosting company)
- Hosting history (Netblock owner, IP (and IPv6) address, Operating System, Server/Load Balancer)
- Security (Netcraft Risk Rating)
- Site technology (an extensive review of server-side and client-side software)

pipl (<https://pipl.com/>): The sites tagline is 'The most comprehensive people search on the web'. Just enter a persons name and location and see the results.

Robotex (<https://www.robtex.com/>): Although the site is still just in beta release, they aim to make the fastest and most comprehensive free DNS lookup tool on the Internet. Enter an IP address or hostname into their webpage and then click on any of the buttons to look up information. It is very comprehensive.

The Wayback Machine

The Internet has evolved massively over the last few decades. In the early days of the Internet websites were quite plain with a few graphics and images. This was largely due to Internet download speeds and the use of slower hardware such as modems. These days with HTML5, widespread use of JavaScript, ASP.NET and many more technologies, the Internet has become a highly developed technical entity. Websites evolve for many reasons, it may be they require increased functionality, vulnerabilities may need fixing, inappropriate or compromising data may be found which requires removal. The list of possibilities goes on and on.

Now, imagine from the point of view of a hacker, if a website existed which contains timestamped archived copied of websites over the ages. This would of course be a source worthy of review because it may contain any amount of relevant information to the goals of information gathering.

Well, as you have probably already guessed, such a website does exist and is called the Wayback Machine (<http://archive.org/web/>).

The Wayback Machine is part of the Internet Archive (<https://archive.org/>). To quote their website “Internet Archive is a non-profit library of millions of free books, movies, software, music, and more.”. At the time of writing this book, the Wayback Machine has over 459 billion web pages saved since 1996.

When you visit the Wayback Machine you will see a Wayback Machine logo at the top of the page requesting a URL to be entered. In this example, perhaps enter ‘microsoft.com’.

1. Enter your URL and press enter.
2. From the horizontal bar of years, click on the year of your choice
3. In the calendar area below, click on a blue-circled date indicating the archive date
4. Links on the archived site will work if further pages have been archived

When you review the archive page of your choice, you will find it is stored containing the original HTML code. In the same way as any page you view in a browser, you can simply right-mouse click and select view page source to review the HTML.

If you have a website and do not want it to be archived, it will be useful to note that the Wayback Machine state the following archive exclusions:

- Pages that require a password to access
- Pages that are only accessible when a person types into and sends a form
- Pages on secure servers

- Pages may not be archived due to robots exclusions
- Sites that are excluded by direct site owner request

Specific advice from the Wayback Machine, in order to have pages excluded from the archive are as follows: “You can exclude your site from display in the Wayback Machine by placing a robots.txt file on your web server that is set to disallow User-Agent: ia_archiver. You can also send an email request for us to review to info@archive.org with the URL (web address) in the text of your message.”.

Once you are aware of the Wayback Machine and that there are recognized ways to exclude pages and sites from the archive, you may relax and perhaps enjoy a trip down memory lane!

8 Search Engines

Overview

Search engines are a great way to find out loads of information about a target website.

When using a search engine it helps to have a rough idea about how they initially gather all their search data and the types of data which they may store.

Crawling is the basic operation all search engines adopt. A search engine will scan through a website and record its content. Examples of some basic information it will record are page titles, keywords, links, sections and images. This crawling operation is performed automatically by what is referred to as a 'spider'. The spider (also known as a 'bot') will then move on to any new links it finds, re-check older links and also go to links people may have recorded in the search engine.

The major search engine crawlers will also save a cached copy of the whole page. This may surprise some people because it enables pages to be reviewed even if the live website is offline.

Google.com

This is certainly the most widely know and used search engine and can be quite amazing in it's usefulness in finding data. Simply typing search words into Google will find pages relating to some or all of the words you entered. This is just very basic use of a Google.

They do also provide an advanced search facility which is very helpful in guiding you through more complex searching:

https://www.google.com/advanced_search

For even greater searching power, you can use the Google Search Operators described in the next section

Google Search Operators

A search operator is a set of characters that joins search words to form a new, more complex search query. For example if you just type in 'bbc.com' to Google, you will get search results based on any website page containing the text 'bbc.com'. Google will put what it regards as more relevant search results first, so in this way the BBC website is likely be top of the results. However, even the second or third result may refer to a website just containing the text 'bbc.com'. If you wanted to only search the BBC site for certain information, you could enter:

<code>site:www.bbc.com</code>

In this case 'site:' is a special operator telling Google to use the search characters 'www.bbc.com' in a very specific way. This will only return search results relating to this particular website. Even if you go to page 10 of the returned results, you will only find results relating to this website. Note however, there must not be a gap between the operator and the search text. If there is a gap, Google will simply regard these as extra words to search for in the regular way.

Speech marks for quoted phrases can be used to search for a specific term rather than just individual words:

<code>site:www.bbc.com "ashley madison"</code>
--

In this example only results relating to the BBC website with pages containing the term "ashley madison" will be returned. If the speech marks are not used, pages containing only 'ashley' or just 'madison' may also be returned.

As a side-note, the ‘Ashley Madison’ search results will probably refer to a very notable security leak during 2015, where the security of a Canadian-based on-line dating service was severely compromised. The site itself is rather controversial, because it encourages married couples to have affairs. 33 million accounts (including login names and passwords) were leaked, 300 gigabytes of data reported stolen and over 197,000 emails were leaked. It is a large company with sales reported by its parent company Avid Life Media in 2014 of \$115m. The impact of this hack could hardly have been greater, with blackmail and suicides becoming a part of the unfolding story.

How exactly the site was compromised has not been publicized, but it has been suggested it was assisted by someone on the inside the company. The main point here is that security weaknesses are not always highly technical. If a website is securely locked down, employees may still be subject to such things as phishing emails. In reviewing security, all possible weak links to exploits must be considered.

Another particularly useful operator is the ‘info:’ operator which returns information about the corresponding web page:

<code>info:www.bbc.com</code>

Google will return an entry which at first glance looks just like a regular entry. However if you look below the result on the results page, there will be a list of items enabling you to, for example, see a cached version of the site and sites which link TO this site:

- Show Google’s cache of www.bbc.com
- Find web pages that are similar to www.bbc.com
- Find web pages that link to www.bbc.com
- Find web pages from the site www.bbc.com
- Find web pages that contain the term “www.bbc.com”

The following list of some of the possible search operators you will probably find useful, in each case showing operator, example of operator and a description:

(Note: The search won’t work if you add any spaces between the operator and your search terms).

allintitle:

allintitle:ceo bbc

Only documents containing the search words in the title.

allinurl:

allinurl:ford car

Only documents containing the search words in the URL. In the example, returned pages will have both ford and car in the URL.

cache:

cache:www.bbc.co.uk

Will display Google's cached version of the page.

info:

info:www.hackthissite.org

Will present some information about the corresponding web page. See above for explanation.

intitle:

intitle:bbc

Documents containing the search words in the title. In the example, returned pages will have bbc in the title.

inurl:

inurl:bbc.com

Documents containing that word in the URL. In the example, returned pages will have bbc in the URL.

link:

link:www.bbc.com

Pages that point to that URL.

related:

related:www.bbc.co.uk

Web pages that are similar to the web page you specify. In this case results will link to alternative well known news websites.

site:

site:www.bbc.co.uk

Results limited to the site or domain you specify.

Note: If you find some of the operators are not working (e.g. cache:) and your computer seems to keep defaulting to your region (e.g. www.google.co.uk), then you might find it helpful to try entering the search criteria as a URL in the address bar of your browser in the following format:

`http://www.google.com/search?q=cache:www.bbc.co.uk`

You can of course group any of the above search criteria together. For example, if you would like to search the BBC website for pages with 'golf' in the title and 'championship' in the body of the text, then your search string would look like:

`site:www.bbc.co.uk intitle:golf championship`

Once you become comfortable using Google search operators in this way, you will probably start using them with almost all of your searches. Of course the point of this description of operators is to ensure that you are aware that very focused searches are very simply conducted and that they may reveal a surprising amount of data, that in some cases you did not know was easily accessible.

The Google Hacking Database (GHDB)

This is not about how to hack into Google, it's about a website which is a repository of Google search strings which will return possible on-line exploits. What this means is that you simply search through the categories of possible vulnerabilities and you will be provided with lists of search strings to enter into Google.

GHDB is part of a larger website called the Exploit Database. If you ever can't remember its URL, simply type "google hacking database" into Google, and your first search result is likely to be:

<https://www.exploit-db.com/google-hacking-database/>.

Their purpose is very nicely summed up in their website:

"The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Our aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away."

For example, a recent entry in the database relating to the category 'Files containing passwords' is one which uses Google to return results relating to website web.config files containing passwords. In this case the Google search string is:

"Password=" inurl:web.config -intext:web.config ext:config

Simply enter this text into Google exactly as written in the box including the speech marks.

Robots.txt

Robots.txt is a plain-text file you put on your site to tell search robots which pages you

would like them not to visit. This is commonly used as a way to stop search engines indexing a website if you don't want the content to be listed.

If however, you visit the Google Hacking Database, and enter 'robot.txt' into the search you should find an entry showing how to list these excluded websites in a search.

Simply enter the following text into the Google search box:

<code>(inurl:"robot.txt" inurl:"robots.txt") intext:disallow filetype:txt</code>
--

This particular entry was submitted to GHDB on 9th Aug 2004. It is a very old entry and is accompanied with the following explanatory text:

"Webmasters wanting to exclude search engine robots from certain parts of their site often choose the use of a robot.txt file on the root of the server. This file basically tells the bot which directories are supposed to be off-limits. An attacker can easily obtain that information by very simply opening that plain text file in his browser. Webmasters should **never** rely on this for real security issues. Google helps the attacker by allowing a search for the "disallow" keyword."

Now this might appear at first glance that things are not working as they should, but rather oddly, all is 'fine'. When a search engine crawler arrives at a website, it will have a look at the publicly available robot.txt file. If the file indicates it is acceptable to crawl through the site and index pages, then it will, otherwise it will just move on to the next site. At this point however, it will have already read and indexed the robot.txt site.

So what the above search string is doing is to simply return all of the indexed robot.txt files for sites not wanting to be public. The search results simply point to the indexed robot.txt file itself.

The point is that the robot.txt file is commonly regarded as a security feature. Although it does normally prevent a site from being crawled and cached, it should not be regarded as a secure way of totally hiding your website from search engines.

Other Search Engines

After you have finished gathering information from Google, don't forget that other search engines store independent data and can potentially supply you with further useful information:

- <https://www.google.com>
- <http://www.bing.com>
- <http://www.yahoo.com>
- <https://duckduckgo.com>
- <http://www.ask.com>
- <http://www.aol.com>
- <http://www.wow.com>
- <http://www.webcrawler.com>
- <http://www.infospace.com>
- <http://www.info.com>

Also don't forget that you shouldn't just look at the first page of results. To find more search engines, perhaps specific to your requirements, don't forget that you can use search engines to find them.

If you want to find more help and advice about how to use the search engines, again, don't forget that you can use a search engine. A quick search in Google for say 'google search operators' will simply provide lots of help with Google search operators.

9 People Sites and Social Engineering

People Sites

The term ‘people sites’ has been used here to cover the vast range of websites designed to hold information about people and to enable them to link and communicate with other people. This includes social sites such as Facebook and professional sites such as LinkedIn. Additionally, it also covers job sites where people upload their CV and interact with prospective employers and agencies.

From an organization’s perspective, if employees use websites such as Facebook and LinkedIn, there is probably very little they can do about it, unless an employee makes specific references about their employer. In fact in some cases it may be encouraged for employees to use certain sites. The point here is not whether sites are used, but to be aware of the kind of information which might be obtained.

- Name
- Date of birth
- Address
- Technical skill and qualifications
- Email addresses
- Employers name
- Employers location
- How long employed
- Interests
- If you have just moved
- What your cats name is
- Friends names
- Family names
- Parents names
- Maiden names
- ...

Clearly, not all of the above information is always available, but to a hacker, this is exactly the kind of information they want. In fact, other than hackers, thieves and fraudsters use this kind of data in phishing emails and phone calls. To a hacker, this can assist finding passwords and may also be used to email you malware that may make exploits possible. Exploits may then be used to gather even more information.

It should also be pointed out that job adverts are commonly used to gain additional information about an organization. For example, job adverts for developers and system administrators may indicate details about the network infrastructure. The kinds of hardware used, operating systems, and perhaps the technologies used in setting up their websites and other Internet connected services. Job adverts are of course a necessary part of recruitment, but an awareness of how adverts are worded, may limit the amount of information being publicly released.

Social Engineering

Social engineering is the art of manipulating people so they give up confidential information. At a basic level, an email address is a useful piece of information, but by gradually applying social engineering tactics, employees may be tricked into passing on more critical information.

Normally, social engineering is based on a communication, maybe via email or telephone, which is designed to provoke an emotion. It may be stress, fear or a more positive emotion, but these are powerful techniques which have been the root of numerous high profile hacks.

Phishing, vishing and impersonation are the three main pillars of social engineering, and it is good practice to make sure employees have a basic knowledge of these tactics. Employees will be less vulnerable and organizations will be more secure.

10 WHOIS, DNS and Packet Routes

Introduction

This chapter provides a review of some basics tools you may use to gather the following information:

- **DNS Information:** The Domain Name System (DNS) is an Internet based service that translates domain names into IP addresses.
- **WHOIS Information:** The WHOIS system is the database system used to provide registrant information even if an IP address has not been assigned to a domain name.
- **Packet Route Information:** A Packet route is the route a packet takes to get to a given address and may include the time it takes for the packet to traverse the path.

Ping

Ping is a very well known networking tool, and is used to check whether the specified host is available. It works by sending an Internet Control Message Protocol (ICMP) echo request packet to the specified host. If all goes well, the host will reply with an echo reply packet. Ping also performs a quick DNS resolution and shows the IP address of the specified host. A set of statistics are shown at the end of the results, such as: number of packets sent/received, percent of packet loss, round trip time information.

To view of all the additional ping command options you can use the ‘—help’ option:

```
ping --help
```

Before using ping to test anything, you should verify that the local network is up and running:

```
ping localhost -c 1
```

The -c option is used to limit the number of packets sent, in this case to 1.

Use Ctrl+C to stop results being listed if you have not limited the packet count.

After entering this into a Terminal window you should see a row of results for the packet. The row will state the round-trip time in milli-seconds like so: ‘time=0.041 ms’, although in your case the time is likely to be a different value.

To verify whether a network host is available, simply enter the domain or IP address as follows:

```
ping www.hackthissite.org -c 1
```

The following data should be included in the results, but again the time is likely to be different in your case:

```
64 bytes from hackthissite.org (198.148.81.136) time=141ms
```

Assuming you got the expected result, you have now determined that you can connect with the target site and what it’s the IP address is.

If we had just known the IP address, the following line could equally have been entered:

```
ping 198.148.81.136 -c 1
```

Maximum Transmission Unit

In addition to determining an IP address and checking whether a network host is reachable, it may also be used to determine the Maximum Transmission Unit (MTU) of the remote host. This relates to the maximum IP packet size that can be transmitted, and in turn can be used to imply types of network setup.

To be specific, MTU is not exactly the same as packet size, because an MTU also includes IP headers. So the result of the ping will need 28 adding to it (20 bytes for the IP header and 8 bytes for the ICMP header).

So continuing with the example, enter the following (note in this case we are just sending

one packet):

```
ping www.hackthissite.org -c 1 -s 1472
```

The new ping command option used this time is ‘-s’, which specifies the size of every packet (specified in bytes, the default is 56). By default, ping does not fragment packets, which means if a packet is too large for the target, an error will be returned. In this example, a packet size of 1472 should be OK, so the results for each packet will be displayed as before.

If however the following is entered:

```
ping www.hackthissite.org -c 1 -s 1473
```

This result should indicate 100% packet loss. This packet loss is an indication that the remote host is not able to accept packets of this size and therefore is larger than the MTU. This value was of course just determined by trial and error.

As indicated previously, to translate the maximum packet size into an MTU, we need to add 28. $1472 + 28 = 1500$ bytes.

Wikipedia has a detailed section on MTU’s and incorporates a table of common media results:

https://en.wikipedia.org/wiki/Maximum_transmission_unit.

From this table of MTU’s, we can determine that one of the possible media types is Ethernet v2.

Ok, this isn’t in itself an unusual result, but it has excluded many other more unusual possibilities and has demonstrated how to determine an MTU using ping.

Traceroute

This command line program is used to see the route a packet takes to get to a given address and the time it takes for packets to traverse the path. For example:

```
traceroute www.hackthissite.org
```

Each host in the route is probed 3 times and the return times reported. If a host does not respond within 5 seconds, asterisks are displayed. A lack of response could be for firewall reasons, the host may just not be setup to respond to a 'ping'.

Alternatively if you know the IP address of the remote host, you can just enter the command as follows:

```
traceroute 198.148.81.136
```

For completeness, each host in the path may then in turn be investigated using ping, to find their MTU.

WHOIS

‘whois’ is a command line application which enables a WHOIS lookup to be performed. WHOIS, is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block.

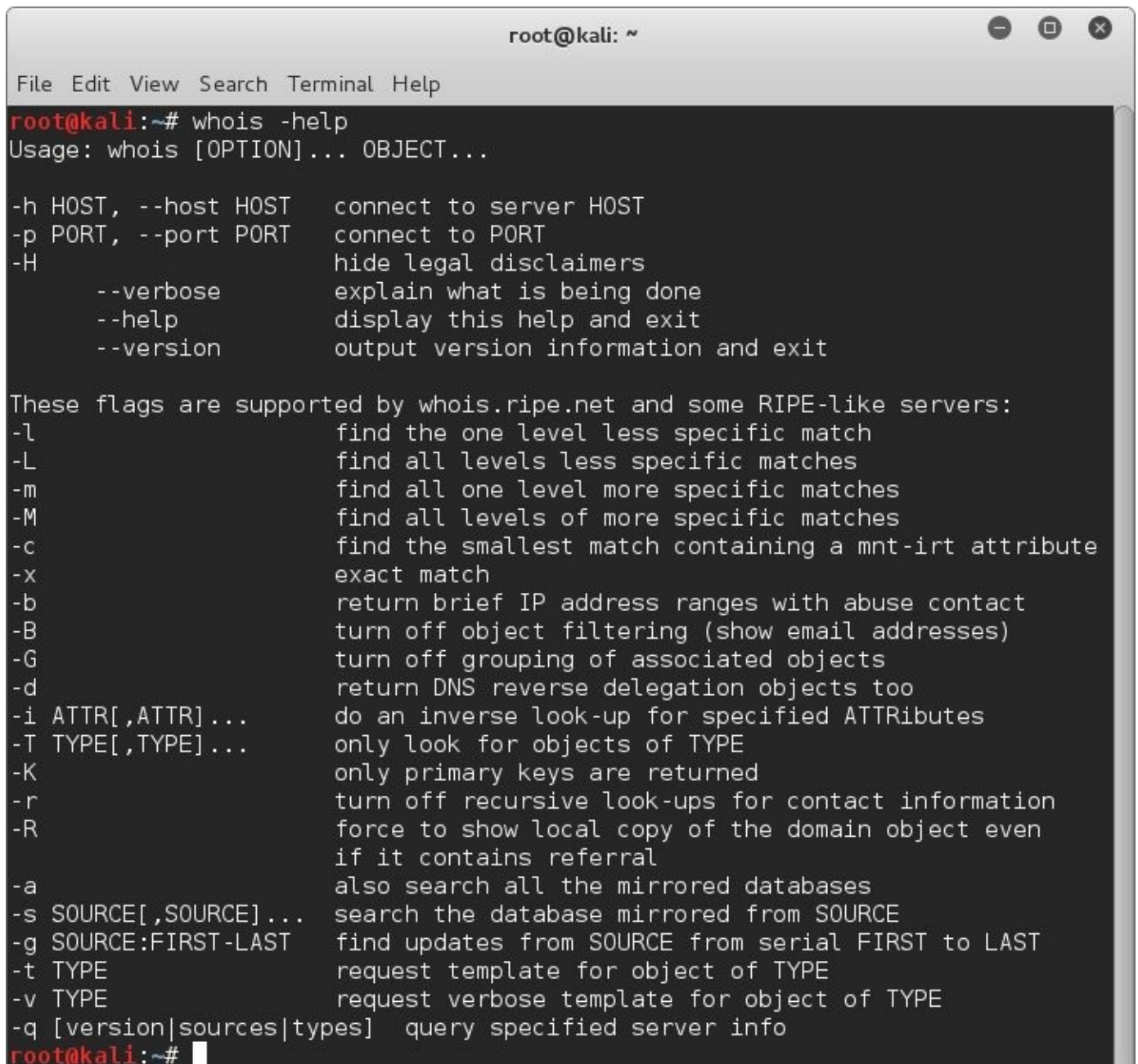
It should already be installed in Kali, but if not, you can install it with the following command:

```
apt-get install whois
```

If you would like a list of available options, just enter the following command:

```
whois -help
```

A list of possible options complete with a description of them all should be displayed:

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'whois -help' being executed. The output displays the usage of the whois command, listing various options like -h, -p, -H, --verbose, --help, and --version, along with their descriptions. It also lists flags supported by whois.ripe.net and some RIPE-like servers, such as -l, -L, -m, -M, -c, -x, -b, -B, -G, -d, -i, -T, -K, -r, -R, -a, -s, -g, -t, -v, and -q, each with a brief explanation of their function. The terminal prompt 'root@kali:~#' is visible at the bottom.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# whois -help
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-H                      hide legal disclaimers
    --verbose           explain what is being done
    --help              display this help and exit
    --version           output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRIBUTES
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types] query specified server info
root@kali:~#
```

Basic use of this command is very simple. Just enter the command followed by the

domain as follows:

whois hackthissite.org

In this particular case, the results will generate a large amount of data relating to the hackthissite.org domain. It will include registrant, admin, technical contact details and Name Server details. The listing is quite long and easily obtained, so it has not been included in this book.

You can also search WHOIS based on a DNS number in the same way if you have one.

You should at least be aware that domain privacy is normally an option when purchasing a domain name. It offers privacy of personal information such as name, address, telephone number and email.

Deepmagic Information Gathering Tool (DMitry)

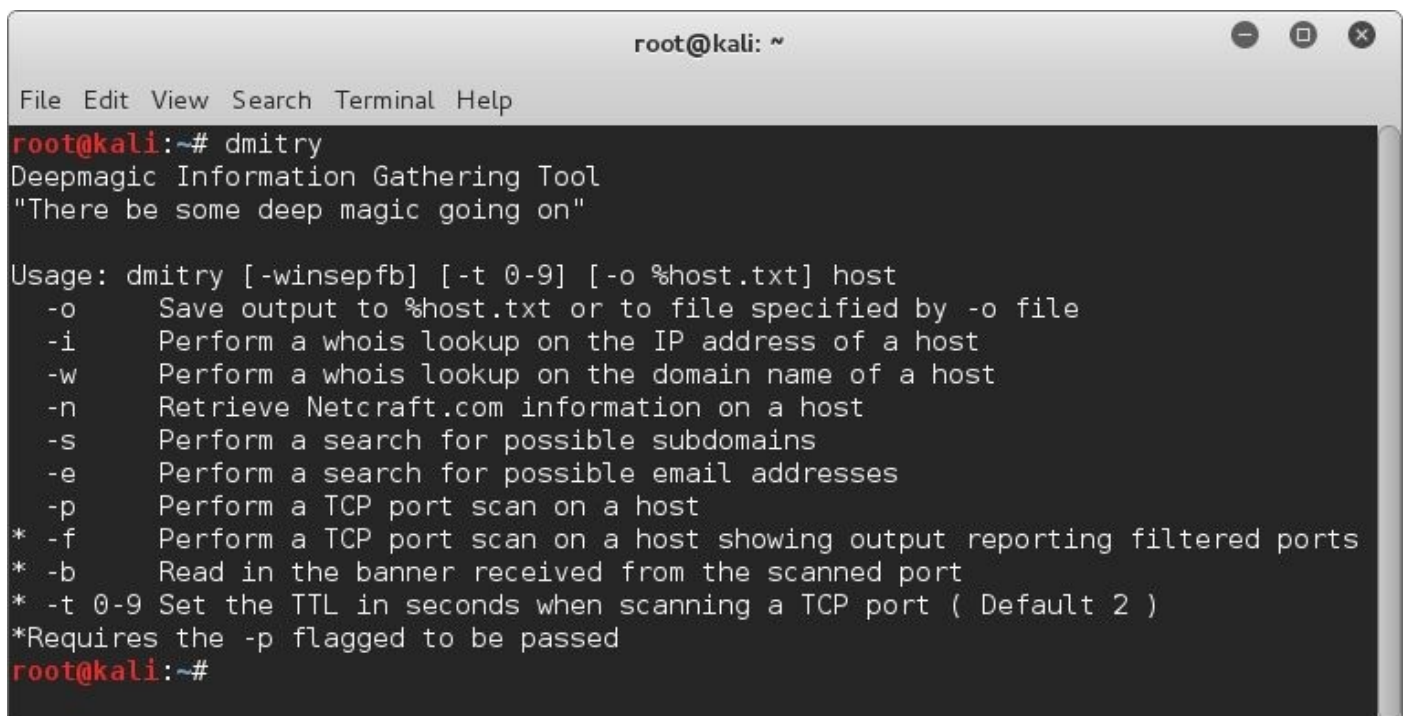
This is a command line application capable of gathering a large amount of information about a host. It is a simple application to use and further information is available on the Kali website (<http://tools.kali.org/information-gathering/dmitry>). It's base functionality is as follows:

- Search for sub-domains
- Search for email addresses
- Retrieve uptime, system and server data
- Perform a TCP Portscan
- Perform a WHOIS lookup

To list all possible options when using DMitry, simply type in the command without any options:

```
dmitry
```

This should provide you with the following output:

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'dmitry' being executed. The output includes the tool's name 'Deepmagic Information Gathering Tool', a quote 'There be some deep magic going on', and a usage section. The usage section lists various options: -o (Save output to %host.txt or to file specified by -o file), -i (Perform a whois lookup on the IP address of a host), -w (Perform a whois lookup on the domain name of a host), -n (Retrieve Netcraft.com information on a host), -s (Perform a search for possible subdomains), -e (Perform a search for possible email addresses), -p (Perform a TCP port scan on a host), * -f (Perform a TCP port scan on a host showing output reporting filtered ports), * -b (Read in the banner received from the scanned port), * -t 0-9 (Set the TTL in seconds when scanning a TCP port (Default 2)), and a note '*Requires the -p flagged to be passed'. The prompt 'root@kali:~#' is visible at the bottom.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepf] [-t 0-9] [-o %host.txt] host
-o      Save output to %host.txt or to file specified by -o file
-i      Perform a whois lookup on the IP address of a host
-w      Perform a whois lookup on the domain name of a host
-n      Retrieve Netcraft.com information on a host
-s      Perform a search for possible subdomains
-e      Perform a search for possible email addresses
-p      Perform a TCP port scan on a host
* -f    Perform a TCP port scan on a host showing output reporting filtered ports
* -b    Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~#
```

An example of using this command is as follows;

```
dmitry -winsepo hackthissite.txt hackthissite.org
```

In this example, DMitry will run a domain whois lookup (w), an IP whois lookup (i), retrieve Netcraft info (n), search for subdomains (s), search for email addresses (e), do a TCP port scan (p), and save the output to hackthissite.txt (o) for the domain hackthissite.org.

Nslookup

This tool is used to query DNS for information. Ordinarily it's a helpful tool to verify that DNS is working within an organization. It's a simple tool to use, and by default it's used in 'non-interactive' mode. This simply means that a single command is entered and a result returned, and the result is based on your default DNS server. Nslookup will indicate this server is the 'Non-authoritative' server if it isn't assigned as a primary or secondary name server to the domain.

Interactive mode enables you to enter a sequence of commands which specify what you are searching for. In this way, interactive mode enables you to perform a variety of searches, including selecting the type of DNS record to be returned.

The most common types of DNS record are:

- A (Address record)
- AAAA (IPv6 address record)
- CNAME (Canonical Name record.)
- MX (Mail exchange record.)
- NS (Name Server record.)
- PTR (Pointers record for reverse lookups.)
- SOA (Zone authority, to determine the authoritative server.)

For a full list of DNS record types you can visit the wikipedia website:
(https://en.wikipedia.org/wiki/List_of_DNS_record_types)

Non-Interactive Mode

For example, to perform a non-interactive lookup on hackthissite.org, simply enter the command as follow:

```
nslookup hackthissite.org
```

The returned results should be similar to this:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nslookup hackthissite.org  
Server:          95.169.183.219  
Address:         95.169.183.219#53  
  
Non-authoritative answer:  
Name:   hackthissite.org  
Address: 198.148.81.137  
Name:   hackthissite.org  
Address: 198.148.81.138  
Name:   hackthissite.org  
Address: 198.148.81.139  
Name:   hackthissite.org  
Address: 198.148.81.135  
Name:   hackthissite.org  
Address: 198.148.81.136  
  
root@kali:~#
```

The results indicate the lookup was performed on a non-authoritative DNS server, and state what that server is. It then goes on to list 5 different IP addresses assigned to the hackthissite.org domain. If you see multiple IP addresses, it means that the site is configured to host content across multiple web servers.

If you have an IP address, it's easy to perform a reverse lookup. For example, enter, the following command:

```
nslookup 190.148.81.137
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nslookup 198.148.81.137  
Server:          95.169.183.219  
Address:         95.169.183.219#53  
  
Non-authoritative answer:  
137.81.148.198.in-addr.arpa      name = hackthissite.org.  
  
Authoritative answers can be found from:  
137.81.148.198.in-addr.arpa      nameserver = ns1.hackthissite.org.  
ns1.hackthissite.org             internet address = 198.148.81.188  
  
root@kali:~#
```

As expected, the domain name is hackthissite.org, but additionally, authoritative nameserver details have been provided.

Interactive Mode

To put nslookup into interactive mode, simply enter nslookup and press enter:

```
nslookup
```


No results have been returned, but it's now in interactive mode and waiting for further commands. If for example you would like to identify Mail servers, the MX record type can be specified as follows:

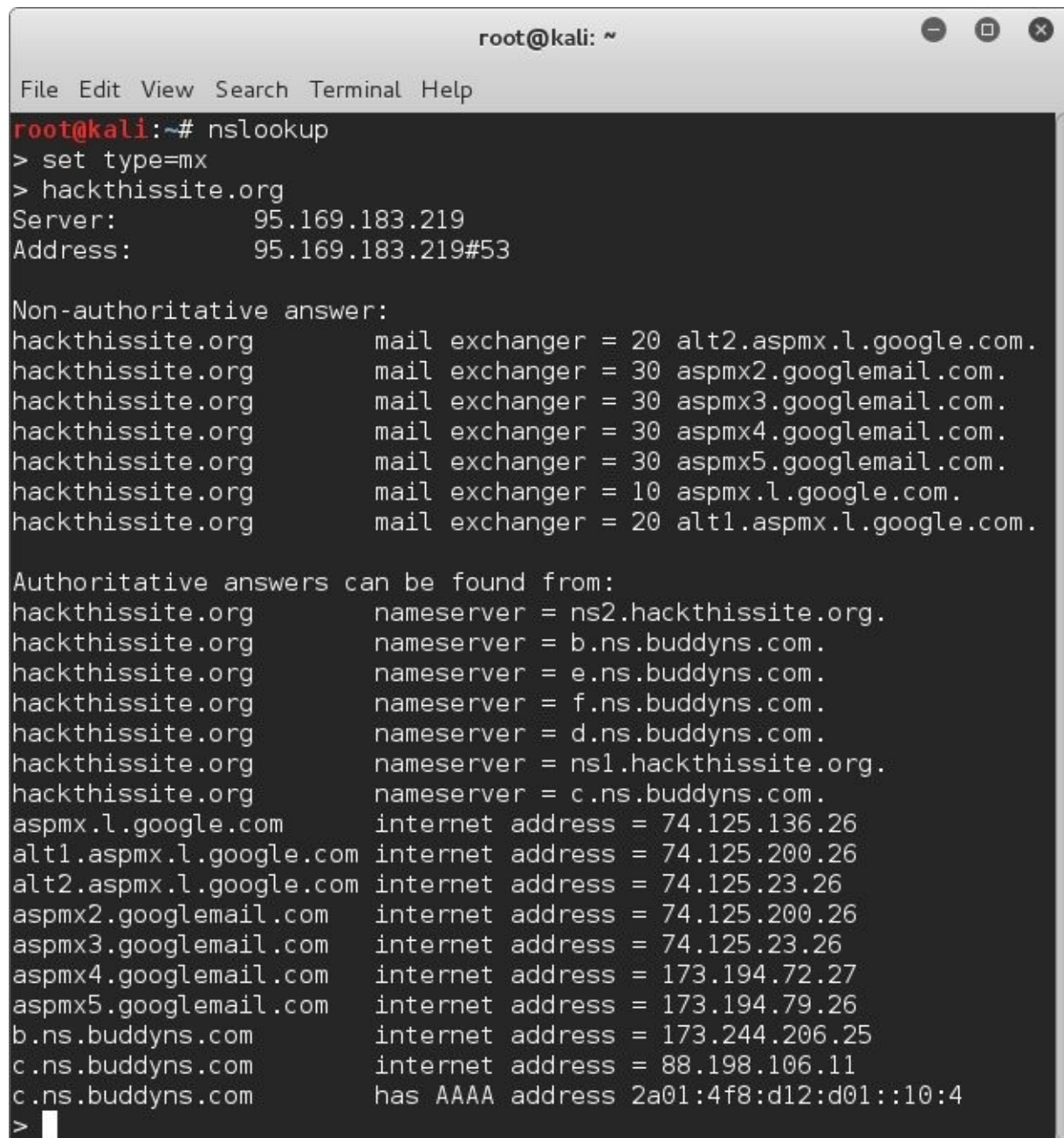
```
set type=mx
```

(If you need to reset this back to perform a standard 'A' record lookup, simply enter set type=a).

Then enter the following to request a hackthissite.org lookup:

```
hackthissite.org
```

Results are returned relating to the hackthissite.org Mail servers:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nslookup  
> set type=mx  
> hackthissite.org  
Server:          95.169.183.219  
Address:         95.169.183.219#53  
  
Non-authoritative answer:  
hackthissite.org      mail exchanger = 20 alt2.aspmx.l.google.com.  
hackthissite.org      mail exchanger = 30 aspmx2.googlemail.com.  
hackthissite.org      mail exchanger = 30 aspmx3.googlemail.com.  
hackthissite.org      mail exchanger = 30 aspmx4.googlemail.com.  
hackthissite.org      mail exchanger = 30 aspmx5.googlemail.com.  
hackthissite.org      mail exchanger = 10 aspmx.l.google.com.  
hackthissite.org      mail exchanger = 20 alt1.aspmx.l.google.com.  
  
Authoritative answers can be found from:  
hackthissite.org      nameserver = ns2.hackthissite.org.  
hackthissite.org      nameserver = b.ns.buddyns.com.  
hackthissite.org      nameserver = e.ns.buddyns.com.  
hackthissite.org      nameserver = f.ns.buddyns.com.  
hackthissite.org      nameserver = d.ns.buddyns.com.  
hackthissite.org      nameserver = ns1.hackthissite.org.  
hackthissite.org      nameserver = c.ns.buddyns.com.  
aspmx.l.google.com    internet address = 74.125.136.26  
alt1.aspmx.l.google.com internet address = 74.125.200.26  
alt2.aspmx.l.google.com internet address = 74.125.23.26  
aspmx2.googlemail.com internet address = 74.125.200.26  
aspmx3.googlemail.com internet address = 74.125.23.26  
aspmx4.googlemail.com internet address = 173.194.72.27  
aspmx5.googlemail.com internet address = 173.194.79.26  
b.ns.buddyns.com      internet address = 173.244.206.25  
c.ns.buddyns.com      internet address = 88.198.106.11  
c.ns.buddyns.com      has AAAA address 2a01:4f8:d12:d01::10:4  
>
```

In addition to listing the Mail servers, it has also listed the authoritative DNS servers and performed a reverse lookup so as to display IP addresses.

So with a few quick commands, IP addresses, Mail server and authoritative DNS servers have been easily identified.

The point of demonstration is to show how easy it is to obtain this kind of information. Unfortunately it's not data that can be hidden, because it is necessary for the basic communication of servers. However, it does demonstrate quite well, how organized information gathering begins.

11 Recon-ng

Introduction

This chapter takes a detailed look at Recon-ng because it is a substantial piece of software and can provide an excellent amount of information.

“Recon-ng is a full-featured Web Reconnaissance framework authored by Tim Tomes and written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly”.

The above quote is from the Black Hills Information Security website (<http://www.blackhillsinfosec.com/>), the company who lead the development of recon-ng. If you need to download the application, it is available from the author’s website: <https://bitbucket.org/LaNMaSteR53/recon-ng/overview>.

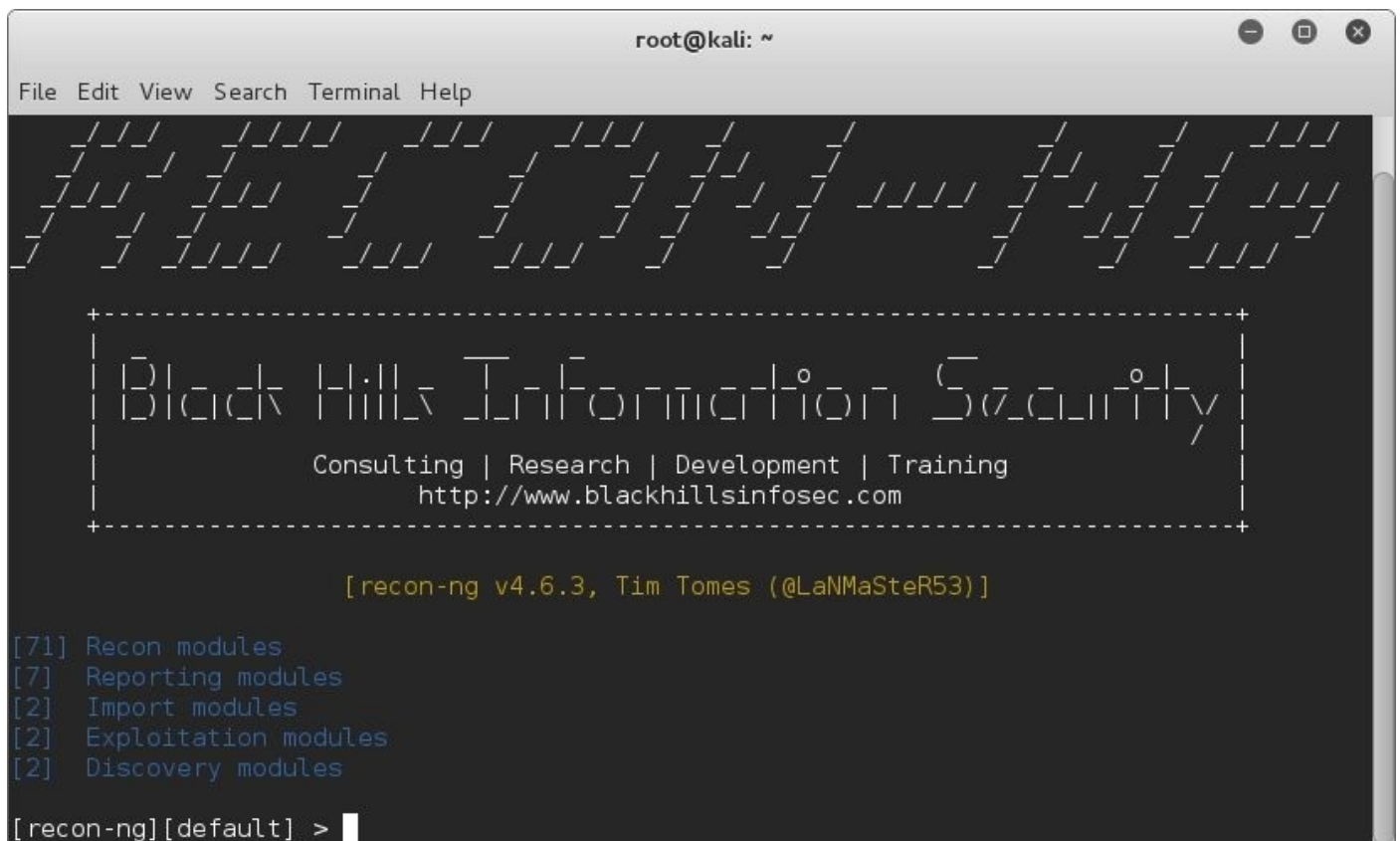
The modular framework of recon-ng is a key part of its usage. Modules are used to enable specific functionality, so that target data may be progressively acquired. The modules are written in Python, and may be customized or new ones added. Many of the modules are designed to use third party API’s, meaning that specific online services may be utilized by the program.

Once data has been collected by recon-ng, it stores it in its database. This is a really great feature because you can progressively gather data on a target using different methodologies, and then run a final report to very nicely present all of your findings. Additionally, the use of Workspaces enables segregation of work.

To open Recon-ng, just open a Terminal window and enter the following command:

```
recon-ng
```

You should see the application startup, and display title information and the number of different modules available in each different categorized activity.



```
root@kali: ~
File Edit View Search Terminal Help

+-----+
| Black Hills Information Security |
+-----+
| Consulting | Research | Development | Training |
| http://www.blackhillsinfosec.com |
+-----+

[recon-ng v4.6.3, Tim Tomes (@LaNMaSteR53)]

[71] Recon modules
[7] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] >
```

From an information gathering perspective, it's useful to note the terminology used to categorize passive and active information gathering:

- Recon modules (Passive Information Gathering)
- Discovery modules (Active Information Gathering)

The final command prompt indicates the current Recon-ng workspace is 'default', and that Recon-ng is ready to accept further commands. Recon-ng runs interactively, and has specific commands to enable you to work with different workspaces and modules. You can generate a list of these commands by typing 'help' and pressing enter:

```
root@kali: ~  
File Edit View Search Terminal Help  
Commands (type [help|?] <topic>):  
-----  
add           Adds records to the database  
back          Exits the current context  
delete        Deletes records from the database  
exit          Exits the framework  
help          Displays this menu  
keys          Manages framework API keys  
load          Loads specified module  
pdb           Starts a Python Debugger session  
query         Queries the database  
record        Records commands to a resource file  
reload        Reloads all modules  
resource      Executes commands from a resource file  
search        Searches available modules  
set           Sets module options  
shell         Executes shell commands  
show          Shows various framework items  
snapshots     Manages workspace snapshots  
spool         Spools output to a file  
unset         Unsets module options  
use           Loads specified module  
workspaces    Manages workspaces  
  
[recon-ng][test01] > 
```

Workspaces and Add Domains

Before starting to look at the functionality of Recon-ng, it's a good idea to start with creating a new workspace to keep any data gathering tests separate from other work.

If for example you would like to create and use a workspace called 'test01', the useful commands to know are:

Command	Description
workspaces add test01	The workspace will be created and become the current workspace.
workspaces select test01	Used if you are returning to work with Recon-ng, and want to select a workspace which has already been created. Also, if you are currently using a certain workspace, this enables you to select a different workspace.
workspaces delete test01	The workspace will be deleted. Note, you cannot delete a workspace if you have it currently selected.
workspaces list	List all available workspaces.
back	If you are currently using a module, use the 'back' command to return to the recon-ng prompt.

If you go ahead and enter the following command, you will create the 'test01' workspace:

```
workspaces add test01
```

You should see the command prompt change from:

```
[recon-ng][default] >
```

to

```
[recon-ng][test01] >
```

This indicates that you are now using the 'test01' workspace.

To finally setup a workspace ready for use, you will need to assign at least one domain to

it. Any modules that you subsequently use, will perform searches based on this domain. In this case, just go ahead and enter the following command to associate 'hackthissite.org' with the workspace test01:

```
add domains hackthissite.org
```

Show Available Modules

The startup screen listed all the different categories of modules available, along with a count of how many modules there are in each category. If you would like to see the full listing of all modules, simply type in the following command:

```
show modules
```

For completeness, here is the full listing of the results:

```
[recon-ng][test01] > show modules
```

Discovery

```
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files
```

Exploitation

```
exploitation/injection/command_injector
exploitation/injection/xpath_bruter
```

Import

--

```
import/csv_file
import/list
```

Recon

--

```
recon/companies-contacts/facebook
recon/companies-contacts/jigsaw/point_usage
recon/companies-contacts/jigsaw/purchase_contact
recon/companies-contacts/jigsaw/search_contacts
recon/companies-contacts/jigsaw_auth
recon/companies-contacts/linkedin_auth
recon/companies-multi/whois_miner
```


recon/companies-profiles/bing_linkedin
recon/contacts-contacts/mailtester
recon/contacts-contacts/mangle
recon/contacts-contacts/unmangle
recon/contacts-credentials/hibp_breach
recon/contacts-credentials/hibp_paste
recon/contacts-credentials/pwnedlist
recon/contacts-domains/migrate_contacts
recon/contacts-profiles/fullcontact
recon/credentials-credentials/adobe
recon/credentials-credentials/bozocrack
recon/credentials-credentials/hasheorg
recon/credentials-credentials/leakdb
recon/domains-contacts/pgp_search
recon/domains-contacts/salesmaple
recon/domains-contacts/whois_pocs
recon/domains-credentials/pwnedlist/account_creds
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_creds
recon/domains-credentials/pwnedlist/domain_ispwned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump
recon/domains-domains/brute_suffix
recon/domains-hosts/baidu_site
recon/domains-hosts/bing_domain_api
recon/domains-hosts/bing_domain_web
recon/domains-hosts/brute_hosts
recon/domains-hosts/builtwith
recon/domains-hosts/google_site_api
recon/domains-hosts/google_site_web
recon/domains-hosts/netcraft
recon/domains-hosts/shodan_hostname
recon/domains-hosts/ssl_san
recon/domains-hosts/vpnhunter
recon/domains-hosts/yahoo_domain
recon/domains-vulnerabilities/punkspider
recon/domains-vulnerabilities/xssed

recon/domains-vulnerabilities/xssposed
recon/hosts-domains/migrate_hosts
recon/hosts-hosts/bing_ip
recon/hosts-hosts/freegeoip
recon/hosts-hosts/ip_neighbor
recon/hosts-hosts/ipinfodb
recon/hosts-hosts/resolve
recon/hosts-hosts/reverse_resolve
recon/locations-locations/geocode
recon/locations-locations/reverse_geocode
recon/locations-pushpins/flickr
recon/locations-pushpins/instagram
recon/locations-pushpins/picasa
recon/locations-pushpins/shodan
recon/locations-pushpins/twitter
recon/locations-pushpins/youtube
recon/netblocks-companies/whois_orgs
recon/netblocks-hosts/reverse_resolve
recon/netblocks-hosts/shodan_net
recon/netblocks-ports/census_2012
recon/ports-hosts/migrate_ports
recon/profiles-contacts/dev_diver
recon/profiles-contacts/linkedin
recon/profiles-profiles/linkedin_crawl
recon/profiles-profiles/namechk
recon/profiles-profiles/profiler
recon/profiles-profiles/twitter

Reporting

reporting/csv
reporting/html
reporting/json
reporting/list
reporting/pushpin
reporting/xlsx
reporting/xml

```
[recon-ng][test01] >
```

Use of Modules

In the previous section, all the available modules were displayed, but you might now be wondering how to put them to use. The good news is that it's quite straight forward, and you only need to know a few commands to become comfortable using modules:

<i>Command</i>	<i>Description</i>
back	Exit the module currently being used.
use <module>	Opens a module ready to be used.
show modules	Display all available modules.
show info	Display information about the current module.
show source	Display the Python source code of the current module.
show hosts	Display all host data from the database.

If for example you would like to find host names for a given domain, the 'bing_domain_web' module is a quick and easy one to start with. It doesn't require any additional API information, and does normally return a good list of host names.

If you look in the list of available modules you will find 'bing_domain_web' listed in the 'recon' category as follows:

```
recon/domains-hosts/bing_domain_web
```

To use this module you can use the following command:

```
use recon/domains-hosts/bing_domain_web
```

Because 'bing_domain_web' is a unique name within the full list of possible modules, you may alternatively use the following abbreviated command:

```
use bing_domain_web
```

You should now see the command prompt change to the following

```
[recon-ng][test01][bing_domain_web] >
```

This indicates that you are using the test01 workspace and have the `bing_domain_web` module ready for use.

If you type in the ‘show info’ command:

```
show info
```

You will see help information displayed which includes it’s name (‘Bing Hostname Enumerator’) and a description of the module:

“Harvests hosts from Bing.com by using the ‘site’ search operator. Updates the ‘hosts’ table with the results.”

This explains how the information is gathered, and that the results will be conveniently added to the hosts table in the Recon-ng database for the current workspace.

In the earlier section ‘Workspaces and Add Domain’ a domain was associated with the current workspace. The module is now ready to begin gathering data. Simply enter the ‘run’ command as follows to execute the module:

```
run
```

It may take a minute or two to execute, but you should soon see a list of domain names. These details will be recorded in the Recon-ng database.

To display information currently gathered, enter the following:

```
show hosts
```

```
root@kali: ~
File Edit View Search Terminal Help
[recon-ng][test01][bing_domain_web] > show hosts

+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | host | ip_address | region | country | latitude | longitude | module |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | www.hackthissite.org | | | | | | bing_domain_web |
| 2 | tor.hackthissite.org | | | | | | bing_domain_web |
| 3 | www.irc.hackthissite.org | | | | | | bing_domain_web |
| 4 | irc-www.hackthissite.org | | | | | | bing_domain_web |
| 5 | v3dev.hackthissite.org | | | | | | bing_domain_web |
| 6 | radio.hackthissite.org | | | | | | bing_domain_web |
| 7 | mirror.hackthissite.org | | | | | | bing_domain_web |
| 8 | forums.hackthissite.org | | | | | | bing_domain_web |
| 9 | admin.hackthissite.org | | | | | | bing_domain_web |
+-----+-----+-----+-----+-----+-----+-----+

[*] 9 rows returned
[recon-ng][test01][bing_domain_web] > 
```

So in this case, 9 different hosts have been identified for the specified domain. The results also conveniently show the module which generated each row of the data.

It may be that you collect large amounts of data, and the basic ‘show hosts’ command displays too much data to be conveniently reviewed. The ‘query’ command enables your viewed data to be filtered, the database is queried in a similar way to using standard database SQL.

Here are a couple of examples:

<i>Query Command</i>	<i>Description</i>
query select host,module from hosts	Only list specified columns. Multiple column requests need to be separated by a comma.
query select * from hosts where ip_address is not null	Will return all columns, but only if an IP address has been determined. With the current table of data, no records will be returned because there are not any IP addresses.

In a similar format as the first example in the above table, we can request only one column to be returned:

```
query select host from hosts
```

```
[recon-ng][test01][bing_domain_web] > query select host from hosts
```

```
+-----+  
|          host          |  
+-----+  
| www.hackthissite.org  |  
| tor.hackthissite.org  |  
| www.irc.hackthissite.org |  
| irc-www.hackthissite.org |  
| v3dev.hackthissite.org |  
| radio.hackthissite.org |  
| mirror.hackthissite.org |  
| forums.hackthissite.org |  
| admin.hackthissite.org |  
+-----+
```

```
[*] 9 rows returned
```

```
[recon-ng][test01][bing_domain_web] > █
```

IPInfoDB

Before attempting to follow along with the example, you will need to make sure you have an API Key to enable you to use services from ipinfodb.com. This is a website specializing in web based geolocation lookup. It's very convenient to use this with Recon-ng because they have an API available free of charge. You do however have to register with IPInfoDB to obtain an API Key.

To register with the website, go to the Account section, and click to create a new account: <http://ipinfodb.com/register.php>.

After your account is activated, you should be provided with an API Key in your account details. Copy the API Key to Recon-ng as follows:

```
keys add ipinfodb_api yourapikey
```

To see a list of all your API keys, enter the following command:

```
keys list
```


Combined Example

This demonstration of Recon-ng gathers data on the target domain (hackthissite.org) using five different modules. The following list details their names, modules and official descriptions:

Bing Hostname Enumerator

Module: recon/domains-hosts/bing_domain_web

Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results.

DNS Hostname Brute Forcer

Module: recon/domains-hosts/brute_hosts

Brute forces host names using DNS. Updates the 'hosts' table with the results.

Hostname Resolver

Module: recon/hosts-hosts/resolve

Resolves the IP address for a host. Updates the 'hosts' table with the results.

Reverse Resolver

Module: recon/hosts-hosts/reverse_resolve

Conducts a reverse lookup for each IP address to resolve the hostname. Updates the 'hosts' table with the results.

IPInfoDB GeoIP

Module: recon/hosts-hosts/ipinfodb

Leverages the ipinfodb.com API to geolocate a host by IP address. Updates the 'hosts' table with the results.

Note, you will need an ipinfodb_api API key to use this module.

A sixth module is then used to present the final collection of data in a nicely laid out html report:

HTML Report Generator

Module: reporting/html

It's worth noting that when a series of modules is used, data recovered by earlier modules is also used to seed more data from subsequent modules. Basically, any data gathered into the database may then be used to gather more data.

So to summarize the overall process: Initially the **Bing Hostname Enumerator** gathers a list of hosts based on the target domain. The **DNS Hostname Brute Forcer** extends this list with more host names. The **Hostname Resolver** then determines IP addresses, and in some cases, multiple IP addresses assigned to each host. The **Reverse Resolver** performs a reverse lookup on the list of IP addresses to determine more host names. The **IPInfoDB GeoIP** then works its magic and provides region, country, latitude and longitude values for each host.

Setup Workspace and Domain

Create a workspace

```
workspaces add combined01
```

Associate a domain with the workspace:

```
add domains hackthissite.org
```

Gather Data

This section performs data gathering using the five modules detailed earlier.

1) Bing Hostname Enumerator

Enter the following three commands to execute the module and display the results:

```
use bing_domain_web
```

```
run
```

```
show hosts
```

```
root@kali: ~
File Edit View Search Terminal Help
[recon-ng][combined01][bing_domain_web] > show hosts

+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | host | ip_address | region | country | latitude | longitude | module |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | www.hackthissite.org | | | | | | bing_domain_web |
| 2 | tor.hackthissite.org | | | | | | bing_domain_web |
| 3 | www.irc.hackthissite.org | | | | | | bing_domain_web |
| 4 | irc-www.hackthissite.org | | | | | | bing_domain_web |
| 5 | v3dev.hackthissite.org | | | | | | bing_domain_web |
| 6 | radio.hackthissite.org | | | | | | bing_domain_web |
| 7 | mirror.hackthissite.org | | | | | | bing_domain_web |
| 8 | forums.hackthissite.org | | | | | | bing_domain_web |
| 9 | admin.hackthissite.org | | | | | | bing_domain_web |
+-----+-----+-----+-----+-----+-----+-----+-----+

[*] 9 rows returned
[recon-ng][combined01][bing_domain_web] >
```

2) DNS Hostname Brute Forcer

Enter the following three commands to execute the module and display the results:

```
use brute_hosts
```

```
run
```

```
show hosts
```

```
root@kali: ~
File Edit View Search Terminal Help
[recon-ng][combined01][brute_hosts] > show hosts

+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | host | ip_address | region | country | latitude | longitude | module |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | www.hackthissite.org | | | | | | bing_domain_web |
| 2 | tor.hackthissite.org | | | | | | bing_domain_web |
| 3 | www.irc.hackthissite.org | | | | | | bing_domain_web |
| 4 | irc-www.hackthissite.org | | | | | | bing_domain_web |
| 5 | v3dev.hackthissite.org | | | | | | bing_domain_web |
| 6 | radio.hackthissite.org | | | | | | bing_domain_web |
| 7 | mirror.hackthissite.org | | | | | | bing_domain_web |
| 8 | forums.hackthissite.org | | | | | | bing_domain_web |
| 9 | admin.hackthissite.org | | | | | | bing_domain_web |
| 10 | hackthissite.org | | | | | | brute_hosts |
| 11 | forum.hackthissite.org | | | | | | brute_hosts |
| 12 | hp.hackthissite.org | | | | | | brute_hosts |
| 13 | irc.hackthissite.org | | | | | | brute_hosts |
| 14 | mail.hackthissite.org | | | | | | brute_hosts |
| 15 | ns2.hackthissite.org | | | | | | brute_hosts |
| 16 | ns1.hackthissite.org | | | | | | brute_hosts |
| 17 | store.printfection.com | | | | | | brute_hosts |
| 18 | store.hackthissite.org | | | | | | brute_hosts |
| 19 | printfection.com | | | | | | brute_hosts |
+-----+-----+-----+-----+-----+-----+-----+-----+

[*] 19 rows returned
[recon-ng][combined01][brute_hosts] >
```

3) Hostname Resolver

Enter the following three commands to execute the module and display the results:

```
use hosts-hosts/resolve
```

```
run
```

```
show hosts
```

```
root@kali: ~  
File Edit View Search Terminal Help  
[recon-ng][combined01][resolve] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	module
1	www.hackthissite.org	198.148.81.135					bing_domain_web
2	tor.hackthissite.org	198.148.81.167					bing_domain_web
3	www.irc.hackthissite.org	198.148.81.169					bing_domain_web
4	irc-www.hackthissite.org	198.148.81.169					bing_domain_web
5	v3dev.hackthissite.org	198.148.81.145					bing_domain_web
6	radio.hackthissite.org	198.148.81.170					bing_domain_web
7	mirror.hackthissite.org	198.148.81.143					bing_domain_web
8	forums.hackthissite.org	198.148.81.138					bing_domain_web
9	admin.hackthissite.org	198.148.81.160					bing_domain_web
10	hackthissite.org	198.148.81.138					brute_hosts
11	forum.hackthissite.org	198.148.81.135					brute_hosts
12	hp.hackthissite.org	198.148.81.139					brute_hosts
13	irc.hackthissite.org	198.148.81.169					brute_hosts
14	mail.hackthissite.org	198.148.81.135					brute_hosts
15	ns2.hackthissite.org	198.148.81.189					brute_hosts
16	ns1.hackthissite.org	198.148.81.188					brute_hosts
17	store.printfection.com	66.35.35.101					brute_hosts
18	store.hackthissite.org	66.35.35.101					brute_hosts
19	printfection.com	66.35.35.101					brute_hosts
20	www.hackthissite.org	198.148.81.136					resolve
21	www.hackthissite.org	198.148.81.137					resolve
22	www.hackthissite.org	198.148.81.138					resolve
23	www.hackthissite.org	198.148.81.139					resolve
24	mirror.hackthissite.org	198.148.81.144					resolve
25	mirror.hackthissite.org	198.148.81.141					resolve
26	mirror.hackthissite.org	198.148.81.142					resolve
27	mirror.hackthissite.org	198.148.81.140					resolve
28	forums.hackthissite.org	198.148.81.139					resolve
29	forums.hackthissite.org	198.148.81.135					resolve
30	forums.hackthissite.org	198.148.81.136					resolve
31	forums.hackthissite.org	198.148.81.137					resolve
32	hackthissite.org	198.148.81.139					resolve
33	hackthissite.org	198.148.81.135					resolve
34	hackthissite.org	198.148.81.136					resolve
35	hackthissite.org	198.148.81.137					resolve
36	forum.hackthissite.org	198.148.81.136					resolve
37	forum.hackthissite.org	198.148.81.137					resolve
38	forum.hackthissite.org	198.148.81.138					resolve
39	forum.hackthissite.org	198.148.81.139					resolve
40	hp.hackthissite.org	198.148.81.136					resolve
41	hp.hackthissite.org	198.148.81.135					resolve
42	hp.hackthissite.org	198.148.81.137					resolve
43	hp.hackthissite.org	198.148.81.138					resolve
44	irc.hackthissite.org	185.24.222.13					resolve

```
[*] 44 rows returned  
[recon-ng][combined01][resolve] >
```

4)Reverse Resolver

Enter the following three commands to execute the module and display the results:

```
use hosts-hosts/reverse_resolve
```

```
run
```

```
show hosts
```

```
root@kali: ~  
File Edit View Search Terminal Help  
[recon-ng][combined01][reverse_resolve] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	module
1	www.hackthissite.org	198.148.81.135					bing_domain_web
2	tor.hackthissite.org	198.148.81.167					bing_domain_web
3	www.irc.hackthissite.org	198.148.81.169					bing_domain_web
4	irc-www.hackthissite.org	198.148.81.169					bing_domain_web
5	v3dev.hackthissite.org	198.148.81.145					bing_domain_web
6	radio.hackthissite.org	198.148.81.170					bing_domain_web
7	mirror.hackthissite.org	198.148.81.143					bing_domain_web
8	forums.hackthissite.org	198.148.81.138					bing_domain_web
9	admin.hackthissite.org	198.148.81.160					bing_domain_web
10	hackthissite.org	198.148.81.138					brute_hosts
11	forum.hackthissite.org	198.148.81.135					brute_hosts
12	hp.hackthissite.org	198.148.81.139					brute_hosts
13	irc.hackthissite.org	198.148.81.169					brute_hosts
14	mail.hackthissite.org	198.148.81.135					brute_hosts
15	ns2.hackthissite.org	198.148.81.189					brute_hosts
16	ns1.hackthissite.org	198.148.81.188					brute_hosts
17	store.printfection.com	66.35.35.101					brute_hosts
18	store.hackthissite.org	66.35.35.101					brute_hosts
19	printfection.com	66.35.35.101					brute_hosts
20	www.hackthissite.org	198.148.81.136					resolve
21	www.hackthissite.org	198.148.81.137					resolve
22	www.hackthissite.org	198.148.81.138					resolve
23	www.hackthissite.org	198.148.81.139					resolve
24	mirror.hackthissite.org	198.148.81.144					resolve
25	mirror.hackthissite.org	198.148.81.141					resolve
26	mirror.hackthissite.org	198.148.81.142					resolve
27	mirror.hackthissite.org	198.148.81.140					resolve
28	forums.hackthissite.org	198.148.81.139					resolve
29	forums.hackthissite.org	198.148.81.135					resolve
30	forums.hackthissite.org	198.148.81.136					resolve
31	forums.hackthissite.org	198.148.81.137					resolve
32	hackthissite.org	198.148.81.139					resolve
33	hackthissite.org	198.148.81.135					resolve
34	hackthissite.org	198.148.81.136					resolve
35	hackthissite.org	198.148.81.137					resolve
36	forum.hackthissite.org	198.148.81.136					resolve
37	forum.hackthissite.org	198.148.81.137					resolve
38	forum.hackthissite.org	198.148.81.138					resolve
39	forum.hackthissite.org	198.148.81.139					resolve
40	hp.hackthissite.org	198.148.81.136					resolve
41	hp.hackthissite.org	198.148.81.135					resolve
42	hp.hackthissite.org	198.148.81.137					resolve
43	hp.hackthissite.org	198.148.81.138					resolve
44	irc.hackthissite.org	185.24.222.13					resolve
45	3.static.htscdn.org	198.148.81.143					reverse_resolve
46	dns.hackthissite.org	198.148.81.189					reverse_resolve
47	dns.hackthissite.org	198.148.81.188					reverse_resolve
48	4.static.htscdn.org	198.148.81.144					reverse_resolve
49	1.static.htscdn.org	198.148.81.141					reverse_resolve
50	2.static.htscdn.org	198.148.81.142					reverse_resolve
51	0.static.htscdn.org	198.148.81.140					reverse_resolve
52	wolf.irc.hackthissite.org	185.24.222.13					reverse_resolve

```
[*] 52 rows returned  
[recon-ng][combined01][reverse_resolve] >
```

5) IPInfoDB GeoIP

(Note: You must have followed the previous instructions and setup the API Key for this step to work)

Enter the following three commands to execute the module and display the results:

```
use ipinfodb
```

```
run
```

```
show hosts
```


[recon-ng][combined01][ipinfodb] > show hosts

rowid	host	ip_address	region	country	latitude	longitude	module
1	www.hackthissite.org	198.148.81.135	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
2	tor.hackthissite.org	198.148.81.167	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
3	www.irc.hackthissite.org	198.148.81.169	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
4	irc-www.hackthissite.org	198.148.81.169	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
5	v3dev.hackthissite.org	198.148.81.145	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
6	radio.hackthissite.org	198.148.81.170	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
7	mirror.hackthissite.org	198.148.81.143	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
8	forums.hackthissite.org	198.148.81.138	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
9	admin.hackthissite.org	198.148.81.160	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
10	hackthissite.org	198.148.81.138	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
11	forum.hackthissite.org	198.148.81.135	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
12	hp.hackthissite.org	198.148.81.139	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
13	irc.hackthissite.org	198.148.81.169	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
14	mail.hackthissite.org	198.148.81.135	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
15	ns2.hackthissite.org	198.148.81.189	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
16	ns1.hackthissite.org	198.148.81.188	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
17	store.printfection.com	66.35.35.101	Louisville, Colorado	United States	39.9778	-105.132	brute_hosts
18	store.hackthissite.org	66.35.35.101	Louisville, Colorado	United States	39.9778	-105.132	brute_hosts
19	printfection.com	66.35.35.101	Louisville, Colorado	United States	39.9778	-105.132	brute_hosts
20	www.hackthissite.org	198.148.81.136	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
21	www.hackthissite.org	198.148.81.137	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
22	www.hackthissite.org	198.148.81.138	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
23	www.hackthissite.org	198.148.81.139	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
24	mirror.hackthissite.org	198.148.81.144	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
25	mirror.hackthissite.org	198.148.81.141	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
26	mirror.hackthissite.org	198.148.81.142	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
27	mirror.hackthissite.org	198.148.81.140	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
28	forums.hackthissite.org	198.148.81.139	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
29	forums.hackthissite.org	198.148.81.135	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
30	forums.hackthissite.org	198.148.81.136	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
31	forums.hackthissite.org	198.148.81.137	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
32	hackthissite.org	198.148.81.139	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
33	hackthissite.org	198.148.81.135	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
34	hackthissite.org	198.148.81.136	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
35	hackthissite.org	198.148.81.137	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
36	forum.hackthissite.org	198.148.81.136	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
37	forum.hackthissite.org	198.148.81.137	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
38	forum.hackthissite.org	198.148.81.138	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
39	forum.hackthissite.org	198.148.81.139	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
40	hp.hackthissite.org	198.148.81.136	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
41	hp.hackthissite.org	198.148.81.135	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
42	hp.hackthissite.org	198.148.81.137	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
43	hp.hackthissite.org	198.148.81.138	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
44	irc.hackthissite.org	185.24.222.13	Amsterdam, Noord-Holland	Netherlands	52.374	4.88969	resolve
45	3.static.htscdn.org	198.148.81.143	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
46	dns.hackthissite.org	198.148.81.189	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
47	dns.hackthissite.org	198.148.81.188	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
48	4.static.htscdn.org	198.148.81.144	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
49	1.static.htscdn.org	198.148.81.141	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
50	2.static.htscdn.org	198.148.81.142	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
51	0.static.htscdn.org	198.148.81.140	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
52	wolf.irc.hackthissite.org	185.24.222.13	Amsterdam, Noord-Holland	Netherlands	52.374	4.88969	reverse_resolve

[*] 52 rows returned

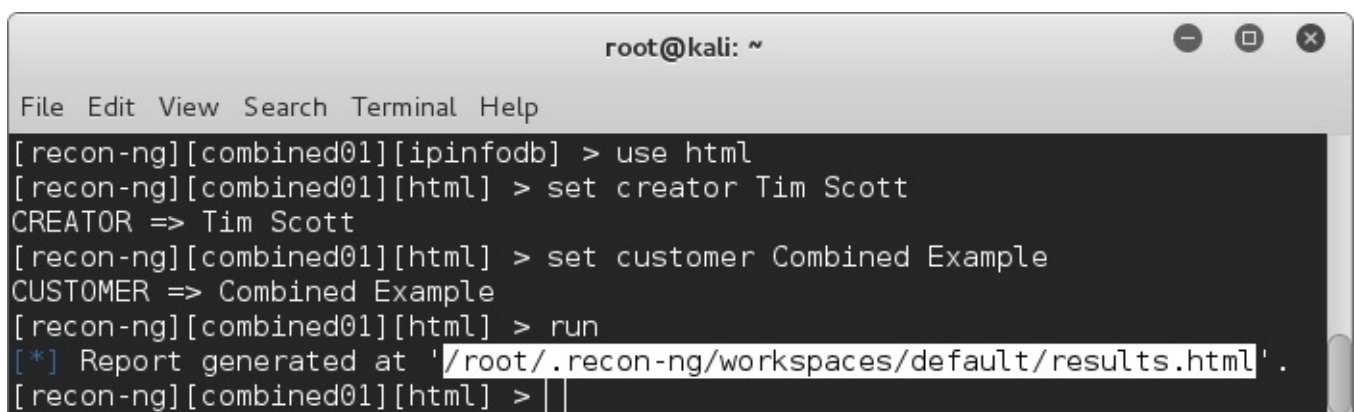
[recon-ng][combined01][ipinfodb] >

Report the Data

The HTML Report Generator module will now be used to create a report based on the data in the database. Type in the following commands (substituting the creator and customer as required):

use html
set creator Tim Scott
set customer Combined Example
run

This will create an html report file to neatly display the data. The path to the file is highlighted in the image:



```
root@kali: ~  
File Edit View Search Terminal Help  
[recon-ng][combined01][ipinfodb] > use html  
[recon-ng][combined01][html] > set creator Tim Scott  
CREATOR => Tim Scott  
[recon-ng][combined01][html] > set customer Combined Example  
CUSTOMER => Combined Example  
[recon-ng][combined01][html] > run  
[*] Report generated at '/root/.recon-ng/workspaces/default/results.html'.  
[recon-ng][combined01][html] > 
```

Copy the highlighted path, and open Iceweasel (the default web browser in Kali) and paste it into the browser address bar. You should now be able to review the well presented report:

Recon-ng Reconnaissance Report - Iceweasel

Recon-ng Reconnaissanc... x

file:///root/.recon-ng/workspaces/default/results.html

Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Combined Example

www.recon-ng.com

Recon-ng Reconnaissance Report

[+] Summary

[+] Domains

[+] Hosts

host	ip_address	region	country	latitude	longitude	module
0.static.htscdn.org	198.148.81.140	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
1.static.htscdn.org	198.148.81.141	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
2.static.htscdn.org	198.148.81.142	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
3.static.htscdn.org	198.148.81.143	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
4.static.htscdn.org	198.148.81.144	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
admin.hackthissite.org	198.148.81.160	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web
dns.hackthissite.org	198.148.81.189	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
dns.hackthissite.org	198.148.81.188	Las Vegas, Nevada	United States	36.0824	-115.101	reverse_resolve
forum.hackthissite.org	198.148.81.135	Las Vegas, Nevada	United States	36.0824	-115.101	brute_hosts
forum.hackthissite.org	198.148.81.136	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
forum.hackthissite.org	198.148.81.137	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
forum.hackthissite.org	198.148.81.138	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
forum.hackthissite.org	198.148.81.139	Las Vegas, Nevada	United States	36.0824	-115.101	resolve
forums.hackthissite.org	198.148.81.138	Las Vegas, Nevada	United States	36.0824	-115.101	bing_domain_web

Notice the interactive ‘+’ icon to enable showing and hiding of data.

12 Final Review and Countermeasures

You may at this point be feeling somewhat concerned about the plethora of information gathering methodologies, that are readily available to anyone with a computer and an Internet connection. However, concern is often a natural side-effect of being more aware of security issues, and if this awareness can be used to improve security, then this can be only perceived as a positive outcome.

Of course, any potential exploits discovered which are known to be correctable, should be corrected as soon as possible. If suitable expertise is not available, it may imply training or staff recruitment is required, or perhaps to request the services of suitably qualified professionals.

Social engineering attacks are almost impossible to prevent, but staff training can certainly help to minimize the risks. For example, if staff are trained to be aware of phishing emails and phone calls, and have procedures in place explaining what they should do if they receive any, then this represents an additional layer of security to the company.

Physical security should not be overlooked. A multi-layered entrance strategy, incorporating personnel identification, intrusion alarm, CCTV and of course good physical security will certainly help protect against unauthorized access. Physical security does not necessarily just protect against intruders, equally fire, flooding and earthquakes are all potential risks which may need to be mitigated against.

Network security is an obvious part of cybersecurity. If network security remains a concern, it may be necessary to deploy verified and trusted third-party solutions:

- IDS
- IPS
- Firewalls
- Anti-virus
- IAM technology

Taking data home or off-site, and generally how it is stored, should not be overlooked. Many data leaks have occurred by staff taking unencrypted sensitive data home to work on, while not being aware of the security risks this may introduce. Clear policies regarding communication of data, copying of data and removal of data are good countermeasures to mitigate against these risks.

If website development or application development is seen as a potential weakness in security, it could be helpful to either recruit specific expertise or to train existing developers. Code audits can help to both find vulnerabilities and also to encourage good practices. There are of course many companies who will provide professional advice in all aspects of your cybersecurity measures.

So to sum-up the things you should keep remembering to do or at least consider doing are:

- Keep employees up-to-date in security principles.
- Keep software up-to-date.

- Keep firewalls up-to-date.
- Keep data physically secure from unauthorized access.
- Keep Wi-Fi networks secure.
- Keep passwords secure (use strong passwords and force regular changes).
- Keep off-site data secure (password protected and encrypted).
- Keep regular backups of data.
- Keep performing regular security audits and consider contracting in third-party expertise.

Glossary of Terms

ARP (Address Resolution Protocol)

A network layer protocol used to convert an IP address into a physical address such as an Ethernet address.

Banner Grabbing

A technique used to gain information about a computer system on a network and the services running on its open ports. This may be used by a system administrator to review systems and services on their network. However a malicious hacker may use this to find network hosts running operating systems with known exploits.

CVE

Common Vulnerabilities and Exposures (see <http://cve.mitre.org>) is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cybersecurity issues.

Cybersecurity

Is the group of technologies, processes and practices designed to protect programs and data from attack, damage or unauthorized access. The data or programs may be on the Internet, in a network, in a stand-alone computer or on any data-storage medium.

DNS (Domain Name System)

An Internet based service that translates domain names into IP addresses.

Firewall

A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

ICMP (Internet Control Message Protocol)

Is part of any IP implementation and provides error reporting and diagnostics. It is used by routers, intermediary devices, or hosts to communicate updates or error information. It is not a transport protocol that sends data between systems, but rather an indicator that a gateway to the Internet can or cannot be reached for packet delivery.

IDS (Intrusion Detection System)

A software application or device that monitors and reports network or system malicious activities.

IAM (Identity Access Management)

Policies and technologies to ensure that people in an enterprise have appropriate access to technology resources.

IP (Internet Protocol)

The method by which data is sent from one computer gateway to another on the Internet. Data is divided into smaller pieces called packets and each packet contains both the sender's and receiver's IP Address. Each packet is passed from gateway to gateway until a gateway recognizes it as belonging to a computer within it's domain, at which point it's forwarded directly to that computer or device.

IP Address

A numerical label assigned to each device in a network using the Internet Protocol for communication. The communications protocol provides an identification and location system for computers on networks and routes traffic across the Internet.

IPS (Intrusion Prevention System)

Network security appliances that monitor network and/or system activities for malicious activity.

IPv4

The most widely used version of Internet Protocol (IP).

IPv6

The most recent version of the Internet Protocol (IP).

ISP (Internet Service Provider)

An organization that provides services for accessing, using, or participating in the Internet.

MTU (Maximum Transmission Unit)

Relates to the maximum IP packet size that can be transmitted.

Netblock

A group of IP Addresses with a start IP and end IP address.

Penetration Test

Security-oriented probing of a computer system or network to seek out vulnerabilities.

Phishing Email

A deceptive email designed to extract private information from the recipient. Typically carried out by email spoofing (email messages with a forged sender address) or instant messaging, and often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

PTES (Penetration Testing Execution Standard)

Is a standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing. It is detailed in a publicly available website on the Internet: <http://www.pentest-standard.org/>.

RTT (Round-Trip Time)

The length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received.

Social Engineering

Psychological manipulation or 'confidence trick' causing people to divulge confidential information or perform actions they would not otherwise do.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Is the basic communication language or protocol of the Internet.

Tor (The Onion Router)

Originally a network of servers developed for the US Navy, but is now an open network enabling anonymous communication (<https://www.torproject.org/>).

Vishing

Voice phishing is telephone based social engineering, to gain access to private personal and financial information.

VPN

Virtual Private Network.

WHOIS

An Internet based service to provide domain name registrant information, even if a domain name has not been assigned an IP address in the Domain Name System (DNS).