Introduction

Consider when you are downloading free software or anything from internet or put a pendrive on your laptop, however , suddenly your system shutting down or not responding. Now you can think what is the problem? My laptop has 16 GB RAM, i7 Processor and I have done all my defragmentation and cleaned cookies. This is called malfunction of the system.

You have to believe most of the laptop are giving way to hackers. Because of people think they have enough security. People are thinking that nothing information from laptop. But that nothing would be the important to hackers.

Do you believe? Some of the Trojans are may corrupt your disk and there is no way to repair. The source of that Trojans is surely a web. Something on the web force you to download a fake antivirus software. Finally, they can control your full system function. So that laptop may restarting, Not responding, Network failure, Continuous ads on web, porn websites continuously top of the page or hardware failure.

Do you believe? Worms can spread, even if you not click it. Email attachments are the prime place to spread. Before you download some attachments, must check that mail from trusted web source, Otherwise, don't download. If you want to download, after check that file on www.virustotal.com

Computer security is important for protecting the confidentiality and availability of computer systems and their resources. Computer administration and management have become more complex which produces more attack avenues. Network environments and network-based applications provide more attack paths.

Evolution of technology has focused on the ease of use while the skill level needed for exploits has decreased.

What you may loss because of the attacks?

- Financial Loss
- Data Loss
- Misuse of your system and Loss of Trust

Types of security

- Software and Hardware
- Communication
- Information

Top Ten Most-Destructive Computer Viruses

- Stuxnet (2009-2010)
- Conficker Virus (2009)
- agent.btz (2008)
- Zeus (2007
- PoisonIvy (2005)
- MyDoom (2004)
- Fizzer (2003)
- Slammer (2003)
- Code Red (2001)
- Love Letter/I LOVE YOU (2000)

Top Ten Most-Destructive Computer Viruses

- NetBus
- Back Orifice
- Sub7
- Beast (Pretty cool one. I will teach it at the end of the chapter. Prank your friend!)
- ProRat
- Zlob Trojan
- SpySheriff
- Vundo
- Turkojan
- Trojan-Downloader.Win32.Kido.a

Who is hacker?

Notable quote

"Before Google, companies in Silicon Valley already knew it was important to have the best hackers. So they claimed, at least. But Google pushed this idea further than anyone had before. Their hypothesis seems to have been that, in the initial stages at least, all you need is good hackers: if you hire all the smartest people and put them to work on a problem where their success can be measured, you win. All the other stuff-which includes all the stuff that business schools think business consists of-you can figure out along the way. The results won't be perfect, but they'll be optimal. If this was their hypothesis, it's now been verified experimentally."

- Paul Graham

- A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
- One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.
- A hacker is a person who breaks codes and passwords to gain unauthorised entry to computer systems.
- A person who is good at programming quickly.
- One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
- A malicious meddler who tries to discover sensitive information by poking around.
- A hacker is anonymous.

For some people, the challenge of breaking the codes is irresistible and so precautions have to be taken.

Stand-alone computers are usually safe as there is no connection for the hackers to break into. Computers which form part of networks or those with external links, such as attached modems, are in danger from hackers.

Many hackers often don't intend to cause damage or steal data, they just enjoy the challenge of breaking into a system. However, in some instances the hacker's purpose could be to commit fraud, to steal valuable data or to damage or delete the data in order to harm the company.

It might be hard to believe, but most hacking is carried out by employees with a grudge or those who want to 'make a quick buck'. They have insider knowledge of passwords and User IDs which makes it easy for them.

Hacking is not a recent invention. In fact, it has been around since the 1930s, although not always associated with computers. Here's a rundown of some of the most noteworthy hackers in history.

1: Kevin Mitnick

Kevin Mitnick, once considered the most-wanted cybercriminal in the United States, is often touted as the poster child of computer hacking. Kevin mastered an early form of social engineering (scamming operators) and computer hacking to gain access to and modify telephony switching systems. After a very public two-year chase, arrest ,and incarceration, the hacker community collectively rose in protest against what they viewed as a witch hunt.

2: Robert Tappan Morris

On November 2, 1988, Robert Morris released a worm that brought down one-tenth of the Internet. With the need for social acceptance that seems to infect many young hackers, Morris made the mistake of chatting about his worm for months before he actually released it on the Internet, so it didn't take long for the police to track him down. Morris said it was just a stunt and added that he truly regretted wreaking $15 million worth of damage, the estimated amount of carnage caused by his worm.

3: Vladimir Levin

Seeming like the opening of a James Bond movie, Vladimir Levin was working on his laptop in 1994 from his St. Petersburg, Russia, apartment. He transferred $10 million from Citibank clients to his own accounts around the world. As with most Bond movies, Levin's career as a hacker was short lived — with a capture, imprisonment, and recovery of all but $400,000 of the original $10 million.

4: Yan Romanowski

Yan Romanowski, also known as MafiaBoy, was arrested in February 2000 for launching a denial-of-service attack that brought down many of the Internet's largest sites, including Amazon, eBay, and Yahoo. Yan's lawyer claimed, "If [MafiaBoy] had used all his powers, he could have done unimaginable damage." It is widely believed that Romanowski is no more than a script kiddie. His attacks, however successful, were implemented using computer scripts that clogged networks full of garbage data.

5: Kevin Poulsen

Kevin Poulsen, known as Dark Dante in the hacker community, specialized in hacking phone systems, particularly radio stations. This talent allowed only calls originating from his house to make it through to the station, assuring him of wins in listener radio contests. His iconic 1991 hack was a takeover of all of the telephone lines for the Los Angeles KIIS-FM radio station, guaranteeing that he would be the 102nd caller and win the prize of a Porsche 944 S2. The bold Poulsen was wanted by the FBI for federal computer hacking at the same time he was winning the Porsche and $20,000 in prize money at a separate station. Poulsen spent 51 months in a federal prison, the longest sentence of a cybercriminal at that time.

6: Steve Jobs and Steve Wozniak

The now-famous founders of Apple Computer spent part of their youth as hackers. They spent their pre-Apple days (circa 1971) building Blue Box devices (an early phreaking tool allowing users to make long distance calls without the financial charges) and selling them to fellow students at the University of California, Berkeley.

7: David Smith

Smith's fame comes from being the author of the infamous email virus known as Melissa. According to Smith, the Melissa virus was never meant to cause harm, but its simple means of propagation (each infected computer sent out multiple infected emails) overloaded computer systems and servers around the world. Smith's virus was unusual in that it was originally hidden in a file containing passwords to 80 well-known pornography Web sites. Even though more than 60,000 email viruses have been discovered, Smith is the only person to go to federal prison in the United States for sending one.

8: Jonathan James

James gained notoriety when he became the first juvenile, at age 16, to be sent to prison for hacking. James specialized in hacking high-profile government systems, such as NASA and the Department of Defense. He was reported to have stolen software worth more than $1.7 million.

9: George Hotz

While George Hotz may be a renowned jailbreak artist, he's best known for being named as the primary reason for the April 2011 PlayStation breach. As one of the first hackers to jailbreak the Sony PlayStation 3, Hotz found himself in the middle

of a very mean, public, and messy court battle with Sony — perhaps because of his public release of his jailbreaking methods. In stated retaliation, the hacker group Anonymous attacked Sony in what has been the most costly security break of all time. Hotz denied any responsibility for the attack and said, "Running homebrew and exploring security on your devices is cool; hacking into someone else's server and stealing databases of user info is not cool."

10: Gary McKinnon

In 2002, a decidedly odd message appeared on a U.S. Army computer: "Your security system is crap," it read. "I am Solo. I will continue to disrupt at the highest levels." It was later found to be the work of Gary McKinnon, a Scottish system administrator. Gary has been accused of mounting the largest ever hack of U.S. government computer networks — including Army, Air Force, Navy, and NASA systems. The court has recommended that McKinnon be extradited to the United States to face charges of illegally accessing 97 computers, causing $700,000 in damage. Adding even more interest to McKinnon's actions is his insistence that much of his hacking was in search of information on UFOs, information he believed the U.S. government was hiding in its military computers.

Types of hackers

Do you think hackers are only evil?

Mainly three types (White,Black,Grey)

There are seven types of hacker,

White Hat Hackers: These are the good guys, computer security experts who specialize in penetration testing and other methodologies to ensure that a company's information systems are secure. These IT security professionals rely on a constantly evolving arsenal of technology to battle hackers.

Black Hat Hackers: These are the bad guys, who are typically referred to as just plain hackers. The term is often used specifically for hackers who break into networks or computers, or create computer viruses. Black hat hackers continue to technologically outpace white hats. They often manage to find the path of least resistance, whether due to human error or laziness, or with a new type of attack. Hacking purists often use the term "crackers" to refer to black hat hackers. Black hats' motivation is generally to get paid.

Script Kiddies: This is a derogatory term for black hat hackers who use borrowed programs to attack networks and deface websites in an attempt to make names for themselves.

Hacktivists: Some hacker activists are motivated by politics or religion, while others may wish to expose wrongdoing, or exact revenge, or simply harass their target for their own entertainment.

State Sponsored Hackers: Governments around the globe realize that it serves their military objectives to be well positioned online. The saying used to be, "He who controls the seas controls the world," and then it was, "He who controls the air controls the world." Now it's all about controlling cyberspace. State sponsored hackers have limitless time and funding to target civilians, corporations, and governments.

Spy Hackers: Corporations hire hackers to infiltrate the competition and steal trade secrets. They may hack in from the outside or gain employment in order to act as a mole. Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client's goals and get paid.

Cyber Terrorists: These hackers, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures. Cyber terrorists are by far the most dangerous, with a wide range of skills and goals. Cyber Terrorists ultimate motivation is to spread fear, terror and commit murder.

How to be hacker?

1. Start by learning the fundamentals before attempting to do anything: Rather than unnecessarily trying to be one with no sound technical knowledge to back you up, you ought to start at the very beginning by having a sound knowledge in computers. A great way to dip your toes into the water, when you are confused about where to begin from is by understanding Unix. What many do not know is that Unix is the operating system of the internet. You can use the internet without learning about Unix, Yet you cannot become a hacker without learning Unix.

2. Begin by trying to learn the correct attitude of a hacker: If being a professional hacker is something which you are interested in, then make sure that you imbibe the correct attitude. It is of paramount importance that a hacker, besides knowing the intricate nuances of computer system as well as computer programming, knows that

he or she does not need to adhere to any stereotype when it comes to hacking. There are a lot of negative things which are said and written about hackers, yet you should work as per what you want to do with your skill.

3. Know that not all hacking has to be a negative thing: Before you think that you rather not become a hacker, because there is so much negativity associated with it, you ought to remember that hacking is not always a negative thing. People that use their ability for negative use are commonly referred to as hackers, but this term is actually wrong, as such people should be correctly referred to as crackers. Crackers in a community are people that are involved in illegal as well as unethical things which you ought to steer clear off.

4. Gradually build on your ability to write in Hyper Text Mark Language: To become a professional hacker, it is not merely enough to have the correct attitude, you must know how to write in Hyper Text Mark Language, or html as it is popularly referred to as. When you see a website which is composed of pictures, images as well as text, it is all done through the use of HTML.You can write your HTML in any basic word processing program, like for example Notepad. It is not at all difficult to master the art of writing in HTML and over time you have to keep improving.

5. Do be proficient in more than one language of programming: Needless to say, before you can run, you ought to learn to walk, before you can write an essay you need to learn the alphabet, similarly, to become a hacker and break the rules, you need to be well versed in all the rules first. So keeping this in mind, a hacker has to have a sound and in depth knowledge in the language of programming. It is advisable to make use of a starting platform such as r3 or Kali. In addition to this a good language to start off with is 'Python' and for more serious work, C or C++.

6. Become a Creative and unconventional thinker: Hackers are known for their unconventional as well as creative bend of mind. To become a hacker you too must try and think of out of the box techniques when it comes to getting things done. There is no particular set of rules a hacker can follow to get his work done therefore it is up to him to assimilate all the textbook knowledge in programming which he or she has gained and to put it to use in a practical manner. There is no diploma course in hacking therefore to a large extent hackers must rely on their own expertise.

7. Read up some old pieces to get the true spirit of a hacker: To be a good professional hacker one think which you ought to imbibe is the spirit of a true hacker. It is practically impossible that you will imbibe this spirit on your own without any source of inspiration, therefore , for you it is advisable to read up some old pieces

that might help you know what hacking is all about. Two examples of such old pieces include, 'Jargon File' as well as 'Hackers Manifesto' written by The Mentor, the technical issues addressed may be old but the essence surpasses the boundaries of time.

8. Use your expertise to stand up against injustice and inequality: If you think you have what it takes to become a professional hacker, then you can put your knowledge to positive use by helping people in need. In such a case you can make your chief enemy those sources of authority that use their power in a bad way to withhold information from the common man or from weaker individuals. By doing this positive work you will become a crusader raising your voice for those individuals who are too afraid or even too backward to raise their voices on their own.

9. You can land a corporate job if that interests you: There are many people who have a joint interest for becoming professional hackers as well as landing a corporate job. If you are one of these people as well, then you need not worry at all, you can fulfill your dream. It is not a very well known fact that hackers are hired by big companies as well so as to ensure that all their data is very well protected. Since hackers know how other hackers work, therefore they will be able to take the necessary precautions as well as ensure any damage is minimal.

10. Learn about a number of operating systems, rather than just one: There are a number of operating systems that are being used across the globe and as a hacker it would greatly benefit you to learn about a number of different operating systems rather than being acquainted with only one. Apart from the popular operating system UNIX, there are numerous other ones as well. Windows is in fact one of the systems which is compromised most often and therefore you should have a working knowledge of a Microsoft System.

11. Your networking concepts need to be very sharp to become a hacker: Learning network concepts will really help you go a long way when it comes to becoming a hacker. A great reference book that you can make use of is 'A Top down Approach', which is by James F. Kurose and Keith W. Ross. In addition to reading this what you must do is to familiarize yourself with what exactly is VPN, LAN, WAN as well as subnet. If your primary aim as a hacker is to use to your advantage the vulnerabilities of the net, then you ought to know about, UDP protocol and TCP/IP.

12. Embark on a project to help you get in depth knowledge on computers: Being a hacker you must have all computer related knowledge at your finger tips. What can really help you is embarking on a self assigned project. A popular project which many hackers do is building a computer on their own right from scratch. This sounds like a lot of work and indeed it is, yet this has been a tried and tested method to help hackers improve on their work and get better acquainted with a computer as well as a computer system.

13. Carefully read up on tutorials for hacking which you can find online: There is a lot of information online as well, when hackers are looking for help or even information. In addition to the information, there are also several step by step tutorials online which are very helpful indeed. Figuring things out in your own way and in your own time is a good thing yet if you reach a dead end then you can always find answers for your queries online. They may not be the best, but they will certainly guide you in the right direction.

14. Keep a log book to document your progress: A method which scientists make use of to keep a track of the work they are doing is by maintaining a log book. If you wish to be a hacker, then this is something that you can do as well so that you know what all you have experimented with, what has worked successfully as well as what has not. In addition to this when maintaining a log book, it becomes easy for you to keep a track of what as well as how much you have been able to accomplish in a given span of time.

15. It is advisable to work alone rather than in a team: Becoming a hacker is not a very popular job that people opt for and given the general job description it is always advisable to work on your own. This does not imply that you cannot seek good council from friends or colleagues, but it has been noticed that working in solitude yields more positive results in general.

16. Continuous practice is a must: Once you become a hacker you cannot possibly assume that your studying or practicing days are over. If you want to succeed it is up to you to keep up with the changing times in terms of advancements in programming and make sure that you do your studying well, such that you are not left behind in the rat race. There are a number of individuals who choose to become hackers, for the sheer thrill of the fact that they can constantly as well as continuously gain more information with each passing day.

17. Do participate in several hacking challenges online: Healthy competition has proved as a highly effective way of making us give our hundred percent at all times.

To improve on your skill and ability you can participate in a number of hacking challenges online where you can test yourself as well as find out, as opposed to others in your field, where you stand and how you perform. As a professional hacker you will have to brace yourself to work under pressure, so this can be an excellent way for you to gauge, how quickly you are able to act when the going gets tough.

18. Use your knowledge responsibly or the consequences could be dire: When choosing to take up a career as a professional hacker you must remember that in the course of your career there will be many temptations where you might want to use the wealth of knowledge which you have for negative purposes. Yet, you ought to remember that 'hacking 'in the negative sense if used, has serious as well as dire consequences as it has been deemed illegal by the law. So keeping this in mind this should be reason enough for you to not indulge in any illegal and unethical actions.

Programming: This is the most important. Learn how to solve problems and automate tasks.
- **Operating Systems**: Learn not (only) how to use them, but how they work, how and where it stores (important) information, how to access it's APIs.
- **Networking**: Know how networks works, not only the concepts, but the inner workings too, how each type of packet is formed and the tricks you can do manipulating its bits. And learn how to use this knowledge with some programming language.
- **Website Hacking**: There are lots of techniques to do this, just google OWASP.

This 4 are the main in my opinion, you can be an average to good hacker with this.

To be a ninja you'll need more:

- **Cryptography**: Deep knowledge, how to use, how to implement common cyphers and how to break them. (By common cyphers I mean cyphers used today, like RSA, not caesar's cypthers and others like this).
- **Reverse Engineering (and debugging)**: How to debug or disassemble and analyse software to see what and how a software process its information and how to extract this information from memory at run time.
- **(Anti-) Forensics**: Where incriminating information is stored and how to safely erase them.
- **Exploit writing**: You need to know debugging and computer memory to do this

Kali linux

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous forensics Linux distribution.

Kali Linux is preinstalled with numerous penetration-testing programs, including nmap (a port scanner), Wireshark (a packet analyzer), John the Ripper (a password cracker), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP (both web application security scanners). Kali Linux can run natively when installed on a computer's hard disk, can be booted from a live CD or live USB, or it can run within a virtual machine. It is a supported platform of the Metasploit Project's Metasploit Framework, a tool for developing and executing security exploits. Introduction to Kali Linux

Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution. Kali Linux Features

Kali is a complete re-build of BackTrack Linux, adhering completely to Debian development standards. All-new infrastructure has been put in place, all tools were reviewed and packaged, and we use Git for our VCS.

More than 300 penetration testing tools: After reviewing every tool that was included in BackTrack, we eliminated a great number of tools that either did not work or had other tools available that provided similar functionality.

Free and always will be: Kali Linux, like its predecessor, is completely free and always will be. You will never, ever have to pay for Kali Linux.

Open source Git tree: We are huge proponents of open source software and our development tree is available for all to see and all sources are available for those who wish to tweak and rebuild packages.

FHS compliant: Kali has been developed to adhere to the Filesystem Hierarchy Standard, allowing all Linux users to easily locate binaries, support files, libraries, etc.

Vast wireless device support: We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.

Custom kernel patched for injection: As penetration testers, the development team often needs to do wireless assessments so our kernel has the latest injection patches included.

Secure development environment: The Kali Linux team is made up of a small group of trusted individuals who can only commit packages and interact with the repositories while using multiple secure protocols.

GPG signed packages and repos: All Kali packages are signed by each individual developer when they are built and committed and the repositories subsequently sign the packages as well.

Multi-language: Although pentesting tools tend to be written in English, we have ensured that Kali has true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.

Completely customizable:

ARMEL and ARMHF support: Since ARM-based systems are becoming more and more prevalent and inexpensive, we knew that Kali's ARM support would need to be as robust as we could manage, resulting in working installations for both ARMEL and ARMHF systems. Kali Linux has ARM repositories integrated with the mainline distribution so tools for ARM will be updated in conjunction with the rest of the distribution. Kali is currently available for the following ARM devices:

- rk3306 mk/ss808

- Raspberry Pi
- ODROID U2/X2
- Samsung Chromebook
- EfikaMX
- Beaglebone Black
- CuBox
- Galaxy Note 10.1

its important to realize that most of the commands in kali are GUI or graphic user interface unlike previous installations of backtrack which require terminal input.

Terminal is like windows command prompt, with a derivative you will be quick to notice, in file paths in windows the slash is forwards

\

In the linux enviroment, the slash is backwards

/

Filepaths are case sensitive and when launching a program you also have to type the extension.

Ex. Root/user/admin/torhammer.py

If you had the above program installed, the extension being ".py" would launch the program.

Another cool thing about kali, and linux period, is if and when you learn a programming language, you can code your own programs in their "notepad" style program and save it as something like "hacklikeaboss.py" and it will save as a python file, then right click and change advanced settings to executable file andddddd voila! Your very own custom program has been created.

Enough about kali, im sure youre ready to get started on lesson 2

Real World Applications for Kali Linux

Real world applications for Kali Linux are very diverse. Incorperating them into your repertoire as a sales pitch is crucial to forming a thriving business model that will generate revenue for you and your company.

Small business examples:

Every 9 seconds a personal computer is hacked. Thousands of people either own their own business or work from home. These are businesses that you will start with at first to build a reputation.

Stressing the importance of Data Security to the customer is an integral part of the sales pitch. Looking up articles about local businesses around your area, and even college databases being breached can not only raise awareness, but also raise the fear factor. Ever heard the term a little fear is healthy? Well fear sells, and in todays day and age everyone is digital.

Some people run their business sites via wordpress, even blog on them daily about events. This consumes a good portion of time for the client, and if someone were to access that because they had a faulty line of code in their site, they could not only lose their investment, but lose customers and customer data as well.

A Kali Linux application for this would be a tool called wpscan, which we will review later on, but it scans the site for vulnerabilities allowing you to report them to the sitemaster or admin.

Its illegal to scan without permission, always get permission.

Another tool to use would be nmap

This tool scans open ports on wifi connections

Open ports are like open doors that anyone with the right knowledge can access, and access things like customer data, and even credit card transaction information.

You will find when launching these programs via the drop down menu that they launch a sort of command prompt via a program called terminal. Kali is already preconfigured to run root access, so a tutorial in sudo isnt necessary.

Terminal accepts your commands and runs basically every function on kali and this is where you will spend most of your time.

Everytime you start kali, if its a live disk and not a full install, i recommend opening up a terminal first thing Then type apt-get update

This updates the files

You can also search for upgraded software apt-get upgrade

Other commands are listed below S**ystem Info**

date – Show the current date and time **cal** – Show this month's calendar **uptime** – Show current uptime **w** – Display who is online **whoami** – Who you are logged in as **finger *user*** – Display information about ***user*** **uname -a** – Show kernel information **cat /proc/cpuinfo** – CPU information **cat /proc/meminfo** – Memory information **df -h** – Show disk usage **du** – Show directory space usage **free** – Show memory and swap usage

Keyboard Shortcuts

Enter – Run the command

Up Arrow – Show the previous command

Ctrl + R – Allows you to type a part of the command you're looking for and finds it

Ctrl + Z – Stops the current command, resume with **fg** in the foreground or **bg** in the background

Ctrl + C – Halts the current command, cancel the current operation and/or start with a fresh new line **Ctrl + L** – Clear the screen

command **| less** – Allows the scrolling of the bash command window using **Shift + Up Arrow**and **Shift + Down Arrow**

!! – Repeats the last command

command **!$** – Repeats the last argument of the previous command

Esc + . (a period) – Insert the last argument of the previous command on the fly, which enables you to edit it before executing the command

Ctrl + A – Return to the start of the command you're typing

Ctrl + E – Go to the end of the command you're typing

Ctrl + U – Cut everything before the cursor to a special clipboard, erases the whole line

Ctrl + K – Cut everything after the cursor to a special clipboard

Ctrl + Y – Paste from the special clipboard that **Ctrl + U** and **Ctrl + K** save their data to

Ctrl + T – Swap the two characters before the cursor (you can actually use this to transport a character from the left to the right, try it!)

Ctrl + W – Delete the word / argument left of the cursor in the current line

Ctrl + D – Log out of current session, similar to **exit Learn the Commands**

apropos ***subject*** – List manual pages for ***subject*** **man -k** ***keyword*** – Display man pages containing ***keyword*** **man** ***command*** – Show the manual for ***command*** **man -t** ***man*** **| ps2pdf - >** ***man.pdf*** – Make a pdf of a manual page **which** ***command*** – Show full path name of ***command*** **time** ***command*** – See how long a ***command*** takes

whereis ***app*** – Show possible locations of ***app***

which ***app*** – Show which ***app*** will be run by default; it shows the full path

Searching