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

grep *pattern files* – Search for ***pattern*** in ***files*** **grep -r *pattern dir*** – Search recursively for ***pattern*** in ***dir***

command* | grep *pattern – Search for ***pattern*** in the output of ***command*** **locate *file*** – Find all instances of ***file***

find / -name *filename* – Starting with the root directory, look for the file called ***filename***

find / -name "filename**"** – Starting with the root directory, look for the file containing the string ***filename*** **locate *filename*** – Find a file called ***filename*** using the locate command; this assumes you have already used the command **updatedb** (see next)

updatedb – Create or update the database of files on all file systems attached to the Linux root directory **which *filename*** – Show the subdirectory containing the executable file called ***filename*** **grep *TextStringToFind /dir*** – Starting with the directory called ***dir***, look for and list all files containing ***TextStringToFind*** **File Permissions**

chmod *octal file* – Change the permissions of ***file*** to ***octal***, which can be found separately for user, group, and world by adding: 4 – read (r),2 – write (w), 1 – execute (x) Examples:

chmod 777 – read, write, execute for all **chmod 755** – rwx for owner, rx for group and world For more options, see **man chmod**. **File Commands**

ls – Directory listing

ls -l – List files in current directory using long format

ls -laC – List all files in current directory in long format and display in columns **ls -F** – List files in current directory and indicate the file type **ls -al** – Formatted listing with hidden files

cd *dir* – Change directory to ***dir*** **cd** – Change to home **mkdir *dir*** – Create a directory ***dir*** **pwd** – Show current directory

rm *name* – Remove a file or directory called ***name***

rm *-r dir* – Delete directory ***dir*** **rm -f *file*** – Force remove ***file***

rm -rf ***dir*** – Force remove an entire directory ***dir*** and all it’s included files and subdirectories (use with extreme caution)

cp ***file1 file2*** – Copy ***file1*** to ***file2***

cp -r ***dir1 dir2*** – Copy ***dir1*** to ***dir2***; create ***dir2*** if it doesn't exist

cp ***file*** **/home/*dirname*** – Copy the filename called ***file*** to the **/home/dirname** directory

mv ***file*** **/home/*dirname*** – Move the ***file*** called filename to the ***/home/dirname*** directory

mv ***file1 file2*** – Rename or move ***file1*** to ***file2***; if ***file2*** is an existing directory, moves ***file1*** into directory ***file2***

ln -s ***file link*** – Create symbolic link ***link*** to ***file*** **touch** ***file*** – Create or update ***file*** **cat > *file*** – Places standard input into ***file*** **cat** ***file*** – Display the file called ***file***

more ***file*** – Display the file called ***file*** one page at a time, proceed to next page using the spacebar **head** ***file*** – Output the first 10 lines of ***file***

head -20 ***file*** – Display the first 20 lines of the file called ***file*** **tail** ***file*** – Output the last 10 lines of ***file***

tail -20 ***file*** – Display the last 20 lines of the file called ***file*** **tail -f** ***file*** – Output the contents of ***file*** as it grows, starting with the last 10 lines

Compression

tar cf ***file.tar files*** – Create a tar named ***file.tar*** containing ***files tar xf file.tar*** – Extract the files from ***file.tar***

tar czf ***file.tar.gz files*** – Create a tar with Gzip compression **tar xzf** ***file.tar.gz*** – Extract a tar using Gzip

tar cjf file.tar.bz2 – Create a tar with Bzip2 compression **tar xjf** ***file.tar.bz2*** – Extract a tar using Bzip2

gzip ***file*** – Compresses ***file*** and renames it to ***file.gz*** **gzip -d** ***file.gz*** – Decompresses ***file.gz*** back to ***file***

Printing

/etc/rc.d/init.d/lpd start – Start the print daemon **/etc/rc.d/init.d/lpd stop** – Stop the print daemon

/etc/rc.d/init.d/lpd status – Display status of the print daemon **lpq** – Display jobs in print queue **lprm** – Remove jobs from queue

lpr – Print a file **lpc** – Printer control tool

man *subject* | lpr – Print the manual page called ***subject*** as plain text **man -t *subject* | lpr** – Print the manual page called ***subject*** as Postscript output **printtool** – Start X printer setup interface **Network**

ifconfig – List IP addresses for all devices on the local machine

iwconfig – Used to set the parameters of the network interface which are specific to the wireless operation (for example: the frequency) **iwlist** – used to display some additional information from a wireless network interface that is not displayed by **iwconfig**

ping *host* – Ping ***host*** and output results **whois *domain*** – Get whois information for ***domain*** **dig *domain*** – Get DNS information for ***domain*** **dig -x *host*** – Reverse lookup ***host*** **wget *file*** – Download ***file*** **wget -c *file*** – Continue a stopped download **SSH**

ssh *user@host* – Connect to ***host*** as ***user***

ssh -p *port user@host* – Connect to ***host*** on port ***port*** as ***user*** **ssh-copy-id *user@host*** – Add your key to ***host*** for ***user*** to enable a keyed or passwordless login

User Administration

adduser *accountname* – Create a new user call ***accountname***

passwd *accountname* – Give ***accountname*** a new password

su – Log in as superuser from current login **exit** – Stop being superuser and revert to normal user **Process Management**

ps – Display your currently active processes **top** – Display all running processes **kill *pid*** – Kill process id ***pid*** **killall *proc*** – Kill all processes named ***proc*** (use with extreme caution) **bg** – Lists stopped or background jobs; resume a stopped job in the background **fg** – Brings the most recent job to foreground **fg *n*** – Brings job ***n*** to the foreground

Installation from source

./configure make make install

dpkg -i *pkg.deb* – install a DEB package (Debian / Ubuntu / Linux Mint) **rpm -Uvh *pkg.rpm*** – install a RPM package (Red Hat / Fedora) **Stopping & Starting**

shutdown -h now – Shutdown the system now and do not reboot **halt** – Stop all processes - same as above **shutdown -r 5** – Shutdown the system in 5 minutes and reboot **shutdown -r now** – Shutdown the system now and reboot **reboot** – Stop all processes and then reboot - same as above **startx** – Start the X system

All hacker's tools list

Password Cracker Software

A password cracker software, which is often referred to as a password recovery tool, can be used to crack or recover the password either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. In the process of password cracking, a very common methodology used to crack the user password is to repeatedly make guesses for the probable password and perhaps finally hitting on the correct one. It cannot be denied that whenever we are referring to cyber security, passwords are the most vulnerable security links. On the other hand if the password is too completed, the user might forget it. Password Cracker software are often used by the hackers to crack the password and access a system to manipulate it. Do not unethically use these software for hacking passwords.

In the next section you would be getting familiar with some of the popular Password Cracker tools which are used by hackers for password cracking.

Ophcrack

It is a free password cracker software which is based on the effective implementation of the rainbow tables. It runs on a number of Operating Systems like Mac OS X, Unix/Linux and Windows Operating System. It is equipped with real-time graphs for analyzing the passwords and is an open source software. Ophcrack has the capability to crack both NTLM hashes as well as LM hashes.

Medusa

Medusa is one of the best online brute-force, speedy, parallel password crackers which is available on the Internet. It has been designed by the members of the website foofus.net. It is also widely used in Penetration testing to ensure that the vulnerability of the system can be exposed and appropriate security measures can be taken against hacking.

RainbowCrack

Rainbow Crack as the name suggests, is a cracker for hashes with the Rainbow Tables. It runs on multiple operating systems such as Linux, Windows Vista, Windows XP (Windows Operating Systems). It supports both Graphical User Interface as well as Command line Interface. It's software which is used for password cracking by generating rainbow tables, fuzzing all the parameters.

Wfuzz

Wfuzz is a flexible tool for brute forcing Internet based applications. It supports many features like Multithreading, Header brute forcing, Recursion when discovering directories, Cookies, Proxy Support, hiding results and encoding the

URLs to name a few. Wfuzz is a useful tool for finding unlinked resources like scripts, directories and servlets as well.

Brutus

Brutus is one of the most flexible and free password crackers which operates remotely. It is popular also because of its high speed and operates under operating systems such as Windows 2000, Windows NT and Windows 9x. Currently it does not operate under the UNIX operating system. Brutus was initially designed to check network devices like routers for common as well as default passwords.

L0phtCrack

L0phtCrack which is now known as L0phtCrack6, is a tool which tests the strength of a password given, as well as to recover lost passwords on Microsoft Windows platform. Thus it is a tool for both password recovery as well as auditing the password. It uses techniques such as Rainbow tables, brute-force and dictionary to recover passwords.

Fgdump

Fgdump is a powerful cracking tool. In fact, it's much more powerful than pwdump6 as the latter has the tendency to hang whenever there is a presence of an antivirus. Fgdump has the capability to handle this problem of hanging by shutting down first. It later restarts the Antivirus software. It supports multi threading which is very relevant in the multitasking and multi-user environment.

THC Hydra

Every password security study has revealed that the biggest security weaknesses are the passwords. THC Hydra is a tool for cracking logins and it is flexible as it supports various protocols. It is very fast and at the same time, new modules can be easily added. Hydra can run on operating systems like Solaris 11, OSX, Windows and Linux.

John The Ripper

John the Ripper is a free software for password cracking which was originally designed for the Unix Operating System. At present, it can run on 15 Operating systems which includes 11 different versions of UNIX, Win32, DOS and BeOS. It has the capability to combine several password crackers into a single package which has made it one of the most popular cracking tools for hackers.

Aircrack

It is a network software suite used in 802.11 Wireless Local Area Networks. It consists of tools such as a packet sniffer, detector and a WEP. This tool runs on both Windows and Linux Operating systems. It can work with any type of wireless network interface controller, provided the driver is supporting the raw monitoring mode.

Cain And Abel

Cain and Abel, often referred to as Cain, is a tool for recovering the password in the Windows platform. It has the capability to recover various kinds of passwords using techniques such as cracking the password hashes by using brute-forcing, dictionary attacks, cryptanalysis attacks and packet sniffing in the network.

IKECrack

The objective of this security tool is to locate the valid user identities in a Virtual Public Network along with the secret key combinations. Once this is accomplished, this information can be used easily by a hacker to have access to a VPN in an unauthorized manner

Wireless Hacking Tools

Wireless Hacking Tools are those hacking tools which are used to hack into a wireless network which is usually more susceptible to security threats. One must also ensure that the network is completely secured against hacking or other malwares. The list of wireless hacking tools which would be discussed now can be used to do a Penetration Testing for a Wireless Network. This is an intentional attack on a network to detect security vulnerabilities by accessing its data and functionality.

Aircrack-ng

It is a software suit specially designed for a wireless network and which operates under both the Windows and the Linux Operating System. Aircrack-ng consists of a packet sniffer, WPA cracker and analysis tool and a detector for the wireless Local Area Networks (802.11). The best part of this software suit is one need not install it to use it. It is a collection of files which can be easily used with a command prompt.

There have been many wireless hacking tools exposed in recent past. When a hacker hacks a wireless network, it is supposed to defeat the Wireless network's security devices. The Wi-Fi networks i.e. the Wireless LANs are more exposed to the security threats from a hacker while compared to that of a wired network. While hackers are always more than ready to hack specially if there are weaknesses in a computer network, hacking is often a tedious and complicated procedure.

Kismet

Kismet is a wireless detector system which detects possible intrusion to an 802.11 layer2 wireless network, it is also a sniffer. There are certain plug-in supported by

Kismet which enable sniffing media like DECT. . It also has the capacity to infer whether a non beaconing network is present or not via the data traffic in the network and a network is identified by this tool by collecting data packets passively, detecting hidden and standard named networks.

InSSIDer

InSSIDer is a network scanner which is used in a Wi-Fi network for the Windows Operating System as well as the Apple OS X. It has been developed by MetaGeek, LLC. It is used to collect information from both software and a wireless card and is useful in selecting the availability of the best wireless channel. It also shows those Wi-Fi network channels which overlap with each other.

KisMAC

It is a discovery tool for a wireless network for the Mac OS X operating system. It has many features which are similar to another wireless detector tool called Kismet. This tool is meant for expert network security personnel and is not very user friendly for the beginners

Firesheep

In order to log into a website, a user has submit details like his or her username and password. The server validates these data and sends back a “cookie”. The websites usually encrypts the password however does not encrypt other details which leaves the cookie exposed to hacking threats which are also known as HTTP session hijacking. Firesheep has a packet sniffer which can intercept the cookies which are encrypted from Social Media sites like Twitter and Facebook and comes with the Firefox web browser. Firesheep is available for both the Windows and Mac OS X operating system. It would also run on the Linux platform in the new future.

Airjack

It is a powerful tool for packet injection in an 802.11 wireless network and is very useful as it has the capability to send in forged de-authentication packets. This feature is usually used by a hacker to bring down a network.

KARMA

KARMA is an attack tool which takes the advantage of the probing techniques that is used by used by a client of a WLAN. The station searches for a Wireless LAN in the list of preferred network and it is then that it makes the SSID open for an attacker who is listening. The disclosed SSID is used by KARMA for impersonation of a valid WLAN and attracts the station to the listening attacker.

NetStumbler

NetStumbler is a hacking tool which is used in the Windows Operating system and comes with add ons which are used to hack a wireless network. It has the capability to convert a WIFI enabled laptop on Windows OS into a network detector in an 802.11 WLAN.

WepLab

The WebLab is a tool which teaches about the weaknesses of a WEP, how a WEP works and how it is used to break a wireless network which is WEP protected. It has the features of a WEP Security Analyzer.

Best Network Scanning & Hacking Tools

Nmap

Nmap or Network Mapper is a free open source utility tool for network discovery and security auditing solution for you. It is a flexible, powerful, portable and easy-to-use tool that is supported by most of the operating systems like Linux, Windows, Solaris, Mac OS and others.

SuperScan

It is an multi-functional application that is designed for scanning TPC port. This is also a pinger and address resolver. It also has useful features like ping, traceroute, WhoIs and HTTP request. There is no need of installation as it is a portable application.

Angry IP Scanner

It is a fast port and IP address scanner. It is a lightweight and cross-platform application that has the capacity to scan the IP addresses in any range and also in their ports. It simply pings each IP address.

Packet Crafting To Exploit Firewall Weaknesses

Through Packet crafting technique, an attacker capitalizes your firewall's vulnerabilities. Here are some packet crafting tools

Hping

Earlier Hping was used as a security tool. Now it is used as a command-line oriented TCP/IP packet analyzer or assembler. You can use this for Firewall testing, advance port scanning, network testing by using fragmentation, TOS and different other protocols.

Scapy

It is a powerful and interactive packet manipulation program. Scapy has the capability to decode or forge the packets of a large number of protocols at a time. One of the best feature is that it can confuse the process of decoding and interpreting.

Netcat

Netcat is a simple Unix utility program. This program has the capability to read and write data across network connections and it does so by using UDP or TPC protocol. It was created as a reliable back-end tool.

Yersinia

Not all the network protocols are powerful. In order to take advantage of the weakness of certain network protocols Yersinia is created. It is a full-proof framework that analyzes and tests the deployed networks and systems.

Nemesis

It is a command-line crafting and injecting utility tool used for network packets. This program works for both Unix and Windows operating systems. This is a well-suited tool for testing Network, Intrusion Detection System, IP Stacks, Firewalls and many others

Socat

This is again a command-line based utility tool. It has the capability to establish a two bidirectional byte streams through which it transfers data. In this tool streams can be constructed from a large set of different data sinks.

Traffic Monitoring for Network Related Hacking

These tools allow users to monitor the websites one's children or employees are viewing. Here's a list of some of these tools

Splunk

If you want to convert your data into powerful insights Splunk tools are the best options for you. The Splunk tools are the leading platforms for operational intelligence. It can collect any type of data from any machine in real time.

Nagios

Nagios is the name for the industry standard in monitoring IT infrastructure. The Nagios tools helps you monitor your entire IT infrastructure and have the capability to detect problems well ahead they occur. It can also detect security breaches and share data availability with stakeholders.

P0f

It is versatile passive tool that is used for OS fingerprinting. This passive tool works well in both Linux and Windows operating systems. It has the capability to detect the hooking up of the remote system whether it is Ethernet, DSL or OC3.

Ngrep

Ngrep or network grep is a pcap-aware tool that allows you to extend hexadecimal or regular expressions in order to match it against the data loads of the packet. It can recognize IPv4/6, UDP, TCP, Ethernet, SLIP, PPP, FDDI and many others.

Packet Sniffers To Analyze Traffic

These tools help capture and analyze incoming traffic on your website. Some of the popular ones are listed below

Wireshark

If you want to put a security system, Wireshark is the must have security tool. It monitors every single byte of the data that is transferred via the network system. If you are a network administrator or penetration tester this tool is a must have.

Tcpdump

Tcpdump is a command-line packet analyzer. After completing the designated task of packet capturing Tcpdump will throw the report that will contain numbers of captured packet and packets received by the filter. The user can use flags like –v, -r and –w to run this packet analyzer tool.

Ettercap

It is comprehensive suite in the middle of the attack. It has the feature of sniffing the live connections and content filtering along with many other interesting tricks. It offers three interfaces, traditional command line, GUI and Ncurses.

Dsniff

Dsniff is the collection of various tools that are used for penetration testing and network auditing. The tools like dsniff, msgsnarf, mailsnarf, webspy and urlsnarf passively monitor a network of interesting data like files, emails, passwords and many others.

EtherApe

EtherApe is graphical network monitor for UNIX model PCs after etherman. This interactive tool graphically displays network activity. It features link layer and TCP/IP modes. It supports Token Ring, FDDI, Ethernet, PPP, SLIP, ISDN and other WLAN devices.

Web Proxies: Proxies fundamentally assist in adding encapsulation to distributed systems. The client can request an item on your server by contacting a proxy server.

Paros

It is a Java-based HTTP/HTTPS proxy that helps in assessing the vulnerability of web applications. It supports both viewing and editing HTTP messages on-the-fly. It is supported by Unix and Windows systems. There are some other features as well like client certificate, spiders, proxy chaining and many others.

Fiddler

It is free web debugging proxy tool that can be used for any browser, platforms or systems. The key features of this tool include performance testing, HTTP/HTTPS traffic recording, web session manipulation and security testing.

Ratproxy

A passive and semi-automated application which is essentially a security audit tool. It can accurately detect and annotate problems in web 2.0 platforms.

Sslstrip

This tool is the one that demonstrate HTTPS stripping attack. It has the capability to hijack HTTP traffic on the network in a transparent manner. It watches the HTTPS link and then redirect and maps those links into homograph-similar or look-alike HTTP links.

SSL/TLS Security Test By High-Tech Bridge

This free online service performs a detailed security analysis and configuration test of SSL/TLS implementation on any web server for compliance with NIST guidelines and PCI DSS requirements, as well as for various industry best-practices.

Rootkit Detectors To Hack File System

This is a directory and file integrity checker. It checks the veracity of files and notifies the user if there’s an issue.

AIDE (Advanced Intrusion Detection Environment)

It is a directory and file integrity checker that helps in creating a database using the regular expression rules that it finds from the config files. This tool also supports message digest algorithms and file attributes like File type, Permissions, Inode, Uid, Gid and others.

Firewalls: Firewalls monitor and control network traffic. A firewall is the quintessential security tool used by novices and tech experts alike. Here are a few of the best ones for hackers:

Netfilter

Netfilter offers softwares for the packet filtering framework that works within the Linux 2.4.x and later series of kernel. The softwares of Netfilter help in packet mangling including packet filtering along with network address and port translation.

PF: OpenBSD Packet Filter

It is an OpenBSD system that enables filtering of TCP/IP traffic and also performs Network Address Translation. It also helps in conditioning and normalizing of TCP/IP traffic along with packet prioritization and bandwidth control.

Fuzzers To Search Vulnerabilities

Fuzzing is a term used by hackers for searching a computer system's security vulnerabilities. Here is a list of a few:

Skipfish

It's a reconnaissance web application security tool. Some of it's features are dictionary-based probes and recursive crawls. A website's sitemap is eventually annotated for security assessments.

Wfuzz

This tool is designed in such a way that it helps in brute-forcing web applications. Wfuzz can be used for finding resources but it does not play any role in finding the links like directories, servlets, scripts and others. It has multiple injection points and allows multi-threading.

Wapiti

Wapiti is a web application vulnerability scanner that allows you to audit the security of the web applications that you are using. The scanning process is “black-box” type and detects the vulnerabilities like file disclosure, data injection, XSS injection and many others.

W3af

It is a web application attack and audit framework that helps in auditing any threat that the web application experiences. This framework is built on Python and is easy-to-use and can be extended. It is licensed under GPLv2.0.

Forensics

These tools are used for computer forensics, especially to sniff out any trace of evidence existing in a particular computer system. Here are some of the most popular.

Sleuth Kit

It is an open source digital intervention or forensic tool kit. It runs on varied operating systems including Windows, Linux, OS X and many other Unix systems. It can be used for analyzing disk images along with in-depth analysis of file system like FAT, Ext3, HFS+, UFS and NTFS.

Helix

This is a Linux based incident response system. It is also used in system investigation and analysis along with data recovery and security auditing. The most recent version of this tool is based on Ubuntu that promises ease of use and stability.

Maltego

It is an open source forensic and intelligence application. It can be used for gathering information in all phases of security related work. It saves you time and money by performing the task on time in smarter way.

Encase

Encase is the fastest and most comprehensive network forensic solution available in the market. It is created following the global standard of forensic investigation software. It has the capability of quickly gathering data from wide variety of devices.

Debuggers To Hack Running Programs

These tools are utilized for reverse engineering binary files for writing exploits and analyzing malware.

GDB

GDB is a GNU Project debugger. The unique feature of this debugger enables the user to see what is happening inside one program while it is being executed or check a program at the moment of crash.

Immunity Debugger

It's a powerful debugger for analyzing malware. It's unique features include an advanced user interface with heap analysis tool and function graphing.

Other Hacking Tools: Besides the aforementioned tools, there are myriad of hacking tools used by hackers. They don’t belong to a particular category, but are very popular among hackers nonetheless:

Netcat

It is a featured network utility tool. It has the capability to read and write data across all network connections that uses TCP/IP protocol. It is a reliable back-end tool that can be easily and directly driven by other scripts and programs.

Traceroute

It is a tracert or IP tracking tool that displays the path of internet packets through which it traversed to reach the specific destination. It identifies the IP address of each hop along the way it reaches the destination.

Ping.eu

It is the tracing tool that helps the user to know the time that the data packets took to reach the host. This is an online application where you just need to place the host name or IP address and fetch the result.

Dig

It is a complete searching and indexing system that is used for a domain or internet. It works in both Linux and Windows system. It however does not replace the internet-wide search systems like Google, Infoseek, AltaVista and Lycos.

CURL

It is a free and open source software command-line tool that transfers data with URL syntax. It supports HTTP/HTTPS, Gopher, FTPS, LDAP, POP3 and many others. It can run under a wide variety of operating systems. The recent stable version is v7.37.1.

Hacking Operating Systems

There are numerous professionals who aspire to have a career as ethical hackers. Hacking is not an easy task as it requires great insight about technology and programing. There are specific operating systems as well that are specially designed for the hackers to use. These operating systems have preloaded tools and technologies that hackers can utilize to hack. This article offers a detailed overview of various operating systems that are built keeping hacking in mind. All these operating systems are unique from each other and have proved to be a great resource for the hackers around the world.

Backtrack 5r3

This operating system is built keeping the most savvy security personnel in mind as audience. This is also a useful tool even for the early newcomers in the information security field. It offers quick and easy way to find and also update the largest database available for the security tools collection till date.

Kali Linux

This is a creation of the makers of BackTrack. This is regarded as the most versatile and advanced penetration testing distribution ever created. The documentation of the software is built in an easy format to make it the most user friendly. It is one of the must-have tools for ethical hackers that is making a buzz in the market.

SELinux

Security Enhanced Linux or SELinux is an upstream repository that is used for various userland tools and libraries. There are various capabilities like policy compilation, policy management and policy development which are incorporated in this utility tool along with SELinux services and utilities. The user can get the software as a tested release or from the development repository.

Knoppix

The website of Knoppix offers a free open source live Linux CD. The CD and DVD that is available contain the latest and recent updated Linux software along with desktop environments. This is one of the best tools for the beginners and includes programs like OpenOffice.org, Mozilla, Konqueror, Apache, MySQL and PHP.

BackBox Linux

It is a Linux distribution that is based on Ubuntu. If you want to perform security assessment and penetration tests, this software is the one that you should have in your repository. It proactively protects the IT infrastructure. It has the capability to simplify the complexity of your IT infrastructure with ease as well.

Pentoo

It is security focused live CD that is created based on Gentoo. It has a large number of customized tools and kernels including a hardened kernel consisting of aufs patches. It can backport Wi-Fi stack from the latest kernel release that is stable as well. There are development tools in Pentoo that have Cuda/OPENCL cracking.

Matriux Krypton

If you are looking for a distro to be used in penetration testing and cyber forensic investigation, then Matriux Krypton is the name that you can trust. This is a Debian based GNU/Linux security distribution. It has more than 340 powerful tools for penetration testing and forensics; additionally, it contains custom kernel 3.9.4.

NodeZero

This is regarded as the specialist tool that is specifically designed for security auditing and penetration testing. It is a reliable, stable and powerful tool to be used for this purpose and is based on the current Ubuntu Linux distribution. It is a free and open source system that you can download from the website.

Blackbuntu

It is free and open source penetration testing distribution available over the internet. It is based on Ubuntu 10.10, which is designed specifically for the information security training students and professional. It is fast and stable yet a powerful tool that works perfectly for you. This software is a recommendation from most of the users.

Blackbuntu

It is free and open source penetration testing distribution available over the internet. It is based on Ubuntu 10.10, which is designed specifically for information security, training students and professionals. It is fast and stable, yet a powerful tool that works perfectly for you. This software is a recommendation from most of the users.

Samurai Web Testing Framework

It is a live Linux environment that is designed in such a way that it functions as a web-pen testing environment. The software CD contains tools and programs that are open source and free. The tool selection is based on the ones that the company themselves use for security of their IT infrastructure.

WEAKERTH4N

It's a great pentesting distro comprising of some innovative pentesting tools. The software uses Fluxbox and is built using Debian Squeeze. One of it's popular features is its ability to hack old Android based systems.

CAINE (Computer Aided Investigative Environment)

It is an Italian GNU/Linux live distribution list that was created as project of Digital Forensic. It offers a complete forensic environment. This environment is organized in such a way that it integrates the existing software tools and software module, and finally throws the result in the form of friendly graphical interface.

Bugtraq

It is one of the most stable and comprehensive distributions. It offers stable and optimal functionalities with stable manger in real-time. It is based upon 3.2 and 3.4 kernel Generic that is available in both 32 and 64 Bits. Bugtraq has a wide range of tools in various branches of the kernel. The features of the distribution vary as per your desktop environment

DEFT

DEFT is a distribution that is created for computer forensics. It can run in live stream on the system without corrupting the device. The system is based on GNU/Linux and the user can run this live using CD/DVD or USB pendrive. DEFT is now paired with DART, which is a forensic system.

Helix

There are various versions of Helix released by e-fense that are useful for both home and business use. The Helix3 Enterprise is a cyber-security solution offered by this organization that provides incident response. It throws live response and acquires volatile data. Helix3 Pro is the newest version in the block of Helix family products.

Encryption Tools

Times are changing and spying has become a common phenomenon everywhere. There have been increasing instances where even the governments have been found to be spying on their citizens from time to time. This is one of the prime reasons why the importance of Encryption has increased manifold. Encryption tools are very important because they keep the data safe by encrypting it so that even if someone accesses the data, they can't get through the data unless they know how to decrypt the data. These tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data.

TrueCrypt

TrueCrypt is open source encryption tool which can encrypt a partition in the Windows environment (except Windows 8); it's equipped for creating a virtual encrypted disk in a file. Moreover, it has the capability to encrypt the complete storage device. TrueCrypt can run on different operating systems like Linux, Microsoft Windows and OSX. TrueCrypt stores the encryption keys in the RAM of the computer.

OpenSSH

OpenSSH is the short name for Open Secure Shell and is a free software suite which is used to make your network connections secured. It uses the SSH protocol to provide encrypted communication sessions in a computer network. It was designed originally as an alternative to the Secure Shell Software developed by SSH Communications Security. The tool was designed as a part of the OpenBSD project.

PuTTY

It an open source encryption tool available on both UNIX and Windows operating system. It is a free implementation of SSH (Secure Shell) and Telnet for both Windows as well as UNIX. The beauty of this tool is that it supports many network protocols like Telnet, SCP, rlogin, SSH and raw socket connection. The word PuTTY has no specific meaning, however as in UNIX tradition, tty is a terminal name.

OpenSSL

OpenSSL is an open source encryption tool which implements the TLS and SSL protocols. OpenSSL's core library is written in the C programming language. The fundamental cryptographic functions are implemented by it. OpenSSL versions are available for operating systems like UNIX, Solaris, Linux and Mac OS X. The project was undertaken in 1988 with the objective of inventing free encryption tools for the programs being used on the internet.

Tor

Tor is a free encryption tool and has the capability to provide online anonymity as well as censorship resistance. Internal traffic is directed through a free network which consists of more than five thousand relays so that the user's actual location can be hidden. It is difficult to track the Internet activities like visiting web sites and instant messages; the most important goal of this tool is to ensure the personal privacy of the users.

OpenVPN

It is an open source tool for the implementation of virtual private network techniques so that secured site-to-site or point-to-point connections using routers or bridges are possible, also remote access is possible. OpenVPN offers the users a secured authentication process by using secret keys which are pre-shared.

Stunnel

Stunnel is a multi-platform open source tool which is used to ensure that both the clients and the servers get secured encrypted connections. This encryption software can operate on a number of operating system platforms like Windows as well as all operating systems which are UNIX like. Stunnel depends upon a distinct library like SSLeay or OpenSSL to implement the protocols (SSL or TLS)

KeePass

KeePass is an open source as well as free password management tool for the Microsoft Windows as well as unofficial ports for operating systems such as iOS, Linux, Android, Mac OS X and Windows Phone. All the usernames, passwords and all other fields are stored by KeePass in a secured encrypted database. This database in turn is protected by a single password.

Intrusion Detection System And The IDS Tools

An Intrusion Detection System is a software application or a device which is equipped to do network or system monitoring activities for any malicious threats and sends reports to the management station. Intrusion detection tools can help in identifying potential threats which can be dangerous for the system or the network.

Snort

It is an open source Network Intrusion System as well as a Network Intrusion Prevention System which is free for all to use. It was created in 1988 by Martin Roesch. It has the capability to perform packet logging and analysis of real time traffic on networks which are using the internet protocol.

NetCop

NetCop is an advanced intrusion detection system which is available practically everywhere. NetCop makes use of a specific method to classify the spyware. This is because there are several software programs which intrude your privacy and which have different kind of capabilities. NetCop gives a distinct threat level to each program, thus classifying the threats.

Hacking Vulnerability Exploitation Tools

A tool which identifies whether a remote host is vulnerable to a security attack and tries to protect the host by providing a shell or other function remotely, is called a Vulnerability Exploitation tool. Here is a list of some o the popular ones:

Metasploit

Metasploit was released in the year 2004 and it was an instant hit in the world of computer security. Metasploit provides data on the vulnerabilities in the security system and it helps in conducting penetration testing too.

Sqlmap

It is a penetration testing tool which is available as an open source. Its goal is to automate the detection and exploitation process of the injection flaws in SQL and to take over the database servers.

Sqlninja

The main objective of this tool is to access a vulnerable DB server; it's used for pen testing so that the procedure of controlling a DB server can be automated when the vulnerability of an SQL injection has been tracked.

Social Engineer Toolkit

This tool kit also known as SET, was designed by TrustedSec. The tool comes as an open source code and is Python driven. It is used for conducting Penetration Testing around Social Engineer.

NetSparker

It is a web based security scanner which has an exploitation engine to confirm the security vulnerabilities and makes the user concentrate on elimination of security threats with its False-Positive free feature.

BeEF

BeEF is the short term for The Browser Exploitation Framework. It is a tool for penetration testing which concentrates on a web browser and thus accesses the actual security position of the environment it’s targeting.

Dradis

Dradis stands for Direction, Range and Distance. It is an open source vulnerability scanner or application which provides the facility of information sharing effectively, especially during assessing the security of the system in a central repository.

Vulnerability Scanners

The scanners which assess the vulnerability of a network or a computer to security attacks are known as Vulnerability Scanners. The tools might function differently, however all of them aim to provide an analysis on how vulnerable the system or a network is. Here is a list of the best ones:

Nessus

Nessus is the world's most popular vulnerable scanner topping the list in the years 2000, 2003 and in the year 2006 survey on security tools. It's a free to use vulnerability scanner for personal use in the non enterprise environment.

OpenVAS

This scanner is tipped by many to be the most advanced vulnerability scanner in the world and is a powerful and comprehensive tool for scanning as well as providing solutions for vulnerability management. It is free software and is maintained daily.

Nipper

It is a parser for network infrastructure and its full form is Network Infrastructure Parser. This open source scanner helps with features like auditing, configuring and managing devices for network infrastructure as well as managing the computer networks.

Secunia PSI

It is free computer security software which scans software on a computer system. It tracks those third party/non Microsoft programs which requires security updates to protect your computer against hackers and cyber-criminals.

Retina

Retina, with more than 10,000 deployments, is one of the most sophisticated vulnerability scanners in the market. It aids in efficient identifications of IT vulnerability and is also available as a standalone application as well. It essentially identifies weaknesses in the configuration and missing patches.

QualysGuard

It is a vulnerability management scanner which provides solutions for vulnerability management by applications through the web. Designed by Qualys Inc., it's available on demand. It helps the users by analyzing their vulnerability status.

Nexpose

Vulnerability management is one of the best security practices to protect the system or a network from security threats. Nexpose is a vulnerability management scanner which does different kind of vulnerability checks where there's a risk in IT security.

Web Vulnerability Scanners

While vulnerability scanners are meant for your system, the web vulnerability scanners assess the vulnerability of web applications. It identifies the security vulnerabilities that your app might have by conducting various tests.

Burp Suite

Burp Suite is a tool for conducting the security test of web based applications. It has a collection of tools which work together and conduct the entire process of testing with an objective to find as well as exploit the vulnerabilities in the security.

Webscarab

It is a testing tool for web security applications and has been written in Java and thus is operating system independent. It acts as a proxy and lets users change web requests by web browsers and web server replies. Webscarab often records the traffic to conduct a further review.

Websecurify

Website security is a crucial factor for both personal as well as organization websites. The prime goal should be to detect the vulnerability of your website before an intruder detects it. Websecurify is a testing tool for website security and can be used to detect the vulnerability of your webs

Nikto

It is a scanner for web servers and is available as an open source. It conducts detailed testing for several items against the web servers which include testing of more than 6700 files or programs which can be dangerous. It also tests for version specific problems of the web servers.

W3af

This tool exposes more than 200 potential vulnerabilities and thus minimizes security threats to your websites. Its written in the programming language Python. W3af has both console user interface as well as graphical user interface.