

Forum:[Hack Forums](#)

Thread: [\[TUT\] A Guide For Every Beginner](#)

?? - February 6, 2010, 6:39 am

Hey Guys ?, This Tutorial is made by me and it's for every beginner here , this will help them to start hacking. the best operating system used for hacking is Linux , you can download a very useful linux distribution from here <http://www.backtrack-linux.org/> it contains everything a hacker needs.

Here's what you should do :

- 1-read lots of tutorials (especially on hackforums)
- 2-practice the tutorials you learned
- 3-learn HTML (it helps a hacker a lot) <http://www.w3schools.com/>
- 4-learn a programming language (start with python or visual basic)

Check this thread by hacker22 :

<https://hackforums.net/showthread.php?tid=207223>

Later learn more advanced programming languages like C++

In this Guide :

- 1-Types of Hackers
- 2-Netbios Hacking
- 3-Definition of some terms
- 4-Basic Command Prompt (cmd) commands
- 5-Tools that you should have
- 6-Useful threads

Types Of Hackers :

1-The Black Hat (also known as crackers) they attack computer systems for profit or fun or for other causes , they distribute viruses worms...

2-The White Hat (Ethical Hacker) they are computer security experts specialized in penetration testing , usually they are hired by companies to protect their systems.

3-The Gray Hat (combination between the black and the white hat , you can't know on what side they are)

NetBios Hacking (Network Basic Input/Output System) it's the most simple and easy way for hacking remote computers, it can be used for reading or writing to a remote computer or can be used for denial of service attack. First you need a port scanner like angryip <http://www.angryip.org/> scan a range of IPs (netbios session runs on port 139) lets assume that you found an IP 192.168.0.140 first you need to get some information (go to Run and type cmd) now in the command prompt type nbtstat -a (IP) in this case nbtstat -a 192.168.0.140 you'll get something like this

[img]<http://www.bujarra.com/imagenes/netbios.jpg>[img]

If we find the hex code <20> that means file sharing is enabled. Next type in the cmd net view \\192.168.0.140 You'll get a list of shared resources or an error (access is denied) If you get a list of

the shared drives or folders (assuming that you have found the C: drive is shared) Type in the cmd
net use K: \\192.168.0.140\C:

K: represents the drive that will be created on your computer , that when you access it you can view the C: drive of the victim Now let's go back , if you get access is denied (we have to be logged in) , on windows 95/98 and Windows ME we can crack the password using PQWAK (of course this is old , but some people still use these versions on Windows)

download PQWAK2 Here :

<http://www.mediafire.com/file/w0tqgzcdtdo/pqwak2.zip>

after cracking the password you can login and continue : net use K: \\(IP)\(Share name)

password:***** \user:*****

in other cases when you can't use PQWAK , we can just use a null session access to gather information about a machine. Using : net use \\(IP)\ipc\$ "" /user:""

Here's a Tutorial by h4ckingURLife :

<https://hackforums.net/showthread.php?tid=173385>

Definition of some terms : (some definitions are taken from wikipedia.org and whatis.com)

DNS : (Domain Name System) a database system that translates domain names to ip addresses , so instead of typing the ip address of hackforums in our browser we type hackforums.net and the DNS redirects us to the ip of the server. Hackers can spoof the DNS a common software used is Cain & Abel, for example when a user types www.google.com he gets the page www.yahoo.com , and also it can be used for phishing.

Trojan Horse : a Trojan is designed to allow a remote access by a hacker to a target computer (it's composed from two parts the server and the client) the server is installed on the victims machine , and the client is used by the hacker to connect to the server.

Things that can be performed by a hacker on a target computer :

- 1-data theft
- 2-installation of a software
- 3-downloading or uploading files
- 4-keylogging
- 5-viewing screenshots And more

Keylogger : (keystroke logging) a keylogger is a software used for logging keystrokes and saving them to a text file or sending them to an email address , it runs in the background in a stealth manner so the victim won't notice what's happening.

You can use a great keylogger found here on HF which is Albertino Keylogger.

<https://hackforums.net/showthread.php?tid=219628>

Keylogging Tutorial:

<https://hackforums.net/showthread.php?tid=29821>

Bruteforce attack : is a method used to crack encrypted data such as passwords by trying all possible combinations of characters , bruteforcing takes a long time and sometimes can't crack the password.

Dictionary attack : is a method used to crack a password or a key that tries all the words in a dictionary , the difference between a dictionary attack and a bruteforce attack is that it uses a

predefined list of words.

RAT : (Remote Administration Tool, Remote Access Trojan) a RAT is a malware that includes a Backdoor for administrative control over the target computer, gives the attacker almost full control over the infected computer, infected computers are called zombies.

Botnet : (Robot Network, Zombie Army) botnets are networks of infected computers controlled by the attacker used send spam and viruses.

Crypter : A Crypter is a programs that makes other programs UD or FUD by encrypting them.(UD means undetectable by antivirus programs, and FUD means fully undetectable)

Binder :A Binder is a program that makes other programs UD or FUD by binding them with another file.

Backdoor : is a means of access to a computer that bypasses security mechanism, I other words a backdoor is a method of bypassing normal authentication or securing remote access, a backdoor can be a form of an installed program or a modification to an existing program.

Worm : a worm is a self-replicating virus that does not alter files, but resides in active memory and duplicate itself, sometimes a worm's job is to take advantage of a backdoor created by an earlier attack.

Vulnerability : (security Hole) a vulnerability is a weakness in the system, it's also classified as a security risk.

Exploit : an exploit is an attack on a computer system that takes advantage of a vulnerability, the term exploit refers to the act of successfully making an attack.

A great tool used for exploiting vulnerabilities is metasploit <http://www.metasploit.com/>

Proxy : a proxy server is a server that acts as an intermediary for requests from clients seeking resources from other server, here the client's IP is not shown, instead the IP address of the proxy server is shown, hackers use proxies to protect themselves and hide their IP address.

Find your IP and Trace other IPs Here: <http://www.ip-adress.com/>

DoS Attack : (Denial Of Service Attack) a DoS attack is an attempt to make a computer resource unavailable to its intended users, one common method of attack involves saturating the target machine with external communication requests.

Find the difference between Dos and DDos Here:

<https://hackforums.net/showthread.php?tid=64591>

Phishing : phishing is a fraud process of attempting to acquire sensitive information like user names and passwords or credit card details, it consists of making a website that looks like the real website that victims use, and sending fake emails to them to trick them, so they enter their sensitive information on your fake website which are logged in a log file on the server.

SQL injection : is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

SQL injection tutorials :

<https://hackforums.net/showthread.php?tid=50356>

<https://hackforums.net/showthread.php?tid=45621>

Social engineering : is the act of manipulating people into revealing information or tricking the victim

to performing actions that are beneficial to the user.

A great guide by Solid:

<https://hackforums.net/showthread.php?tid=67193>

Some Command prompt commands that you should know :

cd : change the directory Later you'll download tools that doesn't have a graphical use interface GUI, and when you click on them the cmd opens and then closes, for example hydra. Example to go and run hydra bruteforcer which is on the desktop in the folder hydra: Cd desktop\hydra Hydra.exe

ping (IP/Host) : checks to see if a host is alive

Example : Ping 192.168.0.1

Or

Ping www.google.com

Tracert (host) : traces a host and finds the IP of the host

Example : Tracert www.google.com

ipconfig : displays the current ip address of your computer and the DNS server

Attrib : hides files type attrib/? for help Example (hide a folder ABC in the drive C:)

Attrib +s +h C:\ABC

To show it again Attrib -s -h C:\ABC

Shutdown -s : shuts down your pc

Shutdown -r : restarts your pc

Shutdown -l : log off

Shutdown -a : abort shutdown , sometimes an error happens and you get a windows telling you that your pc will shutdown or restart in few seconds , you can type this to abort the shutdown, you can type it in Run.

Netstat : you can see your connections to remote computers, type netstat -n to view the ips instead of hosts.

You can find all command by typing help in the cmd. And to get help for a each command type after it /? Example attrib/?

Helpful Tools For Every Hacker :

Cain & Abel : <http://www.oxid.it/cain.html>

IP scanner: <http://www.angryip.org/>

Port scanner: <http://www.nmap.org/>

Vulnerability scanner:

<http://www.nessus.org/>

Resource Hacker : used to view and modify windows executable sources

http://www.soft32.com/download_3568.html

<http://www.softpedia.com/get/Programming/File-Editors/Resource-Hacker.shtml>

MacMakeup : change the mac of your interfaces

<http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp>

<http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/Mac-Makeup.shtml>

Wireshark : known before as ethereal a very good sniffer:

<http://www.wireshark.org/>

Password Recovery Tools:

<http://www.nirsoft.net/>

Download all windows password recovery tools

<http://www.nirsoft.net/packages/passrec.zip>

SIW Get detailed system information hardware and software :

<http://www.gtopala.com/siw-download.html>

Download Sysinternals Tools like process explorer and file monitor and registry monitor:

<http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

Metasploit Framework:

<http://www.metasploit.com/framework/download/>

Offline NT Password and Registry editor:

<http://pogostick.net/~pnh/ntpasswd/>

Brutus (bruteforcer):

<http://www.hoobie.net/brutus/brutus-download.html>

Hydra (bruteforcer):

<http://hydra.hellug.gr/download.html>

Cracked registry editor (you can edit the registry even if it's disabled) :

<http://www.mediafire.com/file/u30jy1ym4od/Registryeditor.rar>

Useful Threads :

Help:

<https://hackforums.net/misc.php?action=help>

Ultimate Tools Pack:

<https://hackforums.net/showthread.php?tid=238890>

the same tools but in one rar file :

<https://hackforums.net/showthread.php?tid=250970>

HackForums FAQ:

<https://hackforums.net/showthread.php?tid=19608>

I hope this guide helps someone, and sorry if I missed something.?

Kr4z1 - February 6, 2010, 6:41 am

Google/Wikipedia much? Nice tho for all new people :D

?? - February 6, 2010, 7:49 am

PLZ give your Feedback ?

imAcarrot - February 6, 2010, 7:55 am

very good work! helpful for the begginers...

5rvbu7 - February 6, 2010, 8:47 am

Hey, nice thread. :) I'll direct new users to it.

?? - February 6, 2010, 8:52 am

(Feb 6, 2010 09:47 AM)5rvbu7 Wrote: [\[CITE\]](#) Hey, nice thread. :) I'll direct new users to it.

Thanks for your help ?

MarkW7 - February 6, 2010, 9:28 am

Suppose it's info from different places put in one place, good for noobs / beginners. It seems to be Windows based though - i'd always recommend using *nix.

eXeSoul™ - February 17, 2010, 1:29 pm

Nice info >> :)

azhure - February 17, 2010, 7:26 pm

Wow this is what I need!!!

sevvian - February 17, 2010, 7:39 pm

thanks mate .. Nice share

Paradoxum - February 19, 2010, 7:04 am

Really basic and great. Take this as a free bump and approval. ?

Uncle Pillow - February 19, 2010, 10:06 am

would +rep if i could but im not leet. all i can do is bump it for u :)
good tut

?? - February 19, 2010, 11:05 am

(Feb 19, 2010 08:04 AM)Paradoxum Wrote: [\[CITE\]](#) Really basic and great. Take this as a free bump and approval. ?

(Feb 19, 2010 11:06 AM)hackbot Wrote: [\[CITE\]](#) would +rep if i could but im not leet. all i can do is bump it for u :)

good tut

Thanks Guys :)

Knight_999 - February 22, 2010, 11:31 am

amazing guide, would rep u the max if I could.
Highly appreciate this work of urs :P

Good luck.

msuper28 - February 22, 2010, 12:14 pm

awesome guide and easy to understand! good work bro! thanks!

stolen13 - February 22, 2010, 1:02 pm

Thanks man for this post

Notorious Mental - February 22, 2010, 1:04 pm

Very good and explanatory. Also basic and will help a lot the new members. Nice.

F-417Erkan - February 22, 2010, 3:34 pm

Thx m8, very helpfull and thx 4 sharin´

?? - February 23, 2010, 5:28 am

(Feb 22, 2010 12:31 PM)Knight_999 Wrote: [\[CITE\]](#) amazing guide, would rep u the max if I could.
Highly appreciate this work of urs :P

Good luck.

Thanks m8 ? I've just replied your pm.
and thanks guys for your feedback.

Cloud_DMS - February 24, 2010, 3:14 pm

Thanks again, your work in much appreciated...

?? - February 26, 2010, 3:17 am

the cracked registry editor was deleted from mediafire so here is another link :
<http://bit.ly> [WARNING: potentially infected]/ct5L7V

smithiiiboi1223 - February 26, 2010, 5:10 am

thank you very much keep it up!
helped me a bit :)

Nelson - March 31, 2010, 5:58 am

Nice info,but what about keylogger,i use ProteMac KeyBag.It's really cool prog.

Cycl0ne - March 31, 2010, 6:12 am

Nice share !!
All links working :)

LUR3TryN3 - August 5, 2010, 4:26 pm

Thank you! Very nice tutorial for beginners. Really good.

Awcdfri - August 5, 2010, 4:29 pm

Very good post here should be very useful for all beginners.

Godli - August 5, 2010, 6:23 pm

Thanks didnt know all of this stuff
Nice share!

harkalabe - September 30, 2010, 4:08 am

thank you very nice tut
very useful.

shamisyl - September 30, 2010, 8:20 am

nice tutorial dude..keep up the good work

`P R O D I G Y™ - September 30, 2010, 8:31 am

Not bad at all, actually good. Good work. :)

?? - May 13, 2011, 3:22 am

(Sep 30, 2010 08:31 AM)`P R O D I G Y™ Wrote: [\[CITE\]](#) Not bad at all, actually good. Good work. :)
thank you P R O D I G Y™ ?
and thanks guys, hope this helped you.

cyberflexxx - June 5, 2011, 8:37 pm

very nice tutorial thanks a lot

sumoninja92 - June 6, 2011, 10:22 am

When downloading BackTrack. Do I want KDE or Knome? I have no idea.

DarkXehanort - June 6, 2011, 11:21 am

Nice bro. good job :)

will read it later and hope to understand the things I didn't know

asifali2000 - June 6, 2011, 11:38 am

thats great tutorial nice thanks to share

Boo. - June 6, 2011, 11:42 am

:D Nice share, great for the new comers. Especially all the "terms"

Anonymous.7654 - June 6, 2011, 12:28 pm

Thanks for Tutorial,very detail.

?? - June 6, 2011, 1:02 pm

(Jun 6, 2011 10:22 AM)sumoninja92 Wrote: [\[CITE\]](#) When downloading BackTrack. Do I want KDE or Knome? I have no idea.
you're all welcome guys ?
and about KDE and Gnome, it's the same backtrack with 2 different desktop environments so you should decide what's best for you, if you like the older backtrack it was KDE.

will.sin - June 6, 2011, 1:19 pm

Nice guide, hopefully will help out others :)

rcoleman - June 6, 2011, 2:53 pm

Thanks, Needed some of the info.?

ProjectTrojan - June 21, 2011, 2:16 pm

Nice one man ;)

Thanks and regards.

LaughingMan - June 25, 2011, 1:07 am

nice info, but your missing Blue Hats, like me.

kreat1v - June 25, 2011, 6:39 am

thank u this really helped me :)

RedStar - *August 1, 2011, 8:18 am*

Nice info helps out alot of people