

Forum:[Hack Forums](#)

Thread: [The Beginner Hacking Help Thread](#)

Nas - September 7, 2013, 7:41 am

[img]http://i.minus.com/j725pgTr4MikE.png[/img]

In this thread i will be showing you different units of beginner hacking and answer most frequently asked questions. Please keep in mind this is not a help desk and nor is it a expert guide for hacking.

[img]http://i.minus.com/j2wLbqWwR1cwB.png[/img]

Remote Administration Tools

Keylogging

Shelling

java Drive By

DDoS/DoS/Booters

Crypter

VPN / Proxy

[img]http://i.minus.com/jcf4Y2WnU4hZO.png[/img]

A remote Administration tool (AKA. RAT) is a software that allows a person to control a system as if he/she has physical access to the system. Remote Administration tools are often Malicious and is used to get information from a person, information as in passwords,doxing, exposing or many other things. Malicious RAT software is typically installed without the victim's knowledge. If you want to know how to use a RAT or learn more about it, please visit HackForums official section for [Remote Administration tool's](#).

Some Features :

Screen/camera capture or image control

File management

Shell control

Computer Power Control

Registry management

Block mouse and keyboard

Change your desktop wallpaper

Drop other viruses and worms

View, kill, and start tasks in task manager

View screen

Save all saved passwords on your PC

Log keystrokes, keystroke capture

and many other things..

Quote:If you have been infected by a RAT and do not know how to remove it please look in the [Malware, Virus, and Rat Removal Help by MRT](#) section of HackForums.

[img]http://i2.minus.com/ihNlMn3dYYNxz.png[/img]

Keylogging is the when recording the keys you or another person type on a keyboard, similar to the ratting manner people who are using the keyboard is unaware that their keystroke is being recorded. People use keylogging to record victims passwords. A keylogger recorder can record instant messages, e-mail's, and password input at any moment. If you want to know how to use a keylogging or learn more about it, please visit HackForums official section for [Keylogging](#).

Quote:If you have been infected by a Keylogger and do not know how to remove it please look in the [Malware, Virus, and Rat Removal Help by MRT](#) section of HackForums.

[img]http://i2.minus.com/i9N2YpezxvUsZ.png[/img]

Shelling is one of the basic or expert tools when hacking a website. If you're going to " shell " a website , it means that you are uploading a .php (shell) file in one of the websites directory to have full control of the website. There is many shelling tutorials and can be easily found in a [search](#) on hackforums. If you are wondering how do you get to upload a file in a website's directory, well that's the interesting part. You will have to find a exploit on the website. There is many different types of exploits and exploit finders.

The most known and useful exploits would be:MySQL exploit

[Other Exploits can be found here](#)

A Good website Vulnerability/directory scanner for beginners would be Acunetix. You can find the download link [here](#).

[img]http://i.minus.com/jXsnPdYO8bRwA.png[/img]

A Java Drive By is a java exploit that is put on websites. Once you visit the website you will see a pop-up that says " Run " , It will automatically download a program (Most likely a Rat/Keylogger). The program will not only download it will also run. If you want to use or know how to use it, visit this [thread](#).

There is also something called a Silent Java Drive By, Which you can determine with the name is the same thing as a regular ordinary Java Drive By, but Silent. Which means when you go visit the malicious website, you will not receive a pop up and it will just download also run automatically. This only works with certain types of java's so far.

Current Versions and exploits:

2013 - 7u10 - 7u6

2012 - 7u6 - 7u0

2011 - 7u0 and below

align=center][img]http://i.minus.com/j3k72ZgguR7wi.png[/img][align]

DDoS or Distributed Denial-of-service attack is using more then 1 Network to take a website/server offline. DDoS is caused by sending multiple packets using many different Networks to take down a target so much so that it cannot respond to the traffic.

Picture explanation for DDoS :

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/3/3f/Stachledraht_DDos_Attack.svg/424px-Stachledraht_DDos_Attack.svg.png[/img]

[img]http://i.minus.com/j3ynZxdAILmkk.png[/img]

Short for denial-of-service attack, a type of attack on a network that is designed to bring the network offline by flooding it with traffic. Unlike DDoS, DoS attacks use one connection to take down a network. For all known DoS attacks, there are softwares that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being made.

[img]http://i.minus.com/jk7FxetgqAJFO.png[/img]

Booter can run on bots which is infected computers, or it can run on API's which are servers, You use the booter to send a certain amount of traffic towards someones IP which will over-flood their router and hit them offline or it can be used to hit a servers IP which will do the same and hit it offline

The more bots or shells you have the powerful the booter is going to be. you can hold people offline with it and if the booter is strong enough also websites. Booters are most of the time is a product that is being sold. If you would like to buy them please visit HackForums official Section for [Server Stress Testing](#) Products.

[img]http://i.minus.com/jbg814HTXRJzkC.png[/img]

Crypter is a software used to hide viruses, keyloggers or any RAT tool from antiviruses so that they

are not detected and deleted by antiviruses. A crypter is a program that allows users to crypt the coding of their program. Generally, antivirus work by splitting source code of application and then search for certain string within source code. If antivirus detects any certain malicious strings, it either stops scan or deletes the file as virus from system.

[img]http://i.minus.com/jMfw5yJCnM7W7.png[/img]

FUD is acronym for Fully UnDetectable.

[img]http://i.minus.com/jhPPAUcydR48c.png[/img]

A VPN (virtual private network) is a private network connecting to a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private connection, This is done by making a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. VPN's is used to keep " anonymous " from blackhat activities. Beware most VPN's do leave logs.

Example of VPN :

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/0/00/Virtual_Private_Network_overview.svg/800px-Virtual_Private_Network_overview.svg.png[/img]

[img]http://i.minus.com/jiwTPS11SfZSx.png[/img]

A proxy server is a server (a computer system or an application) that acts as a middle-man for requests from clients wanting resources from other servers. You can connect to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different person/server and the proxy server evaluates the request as a way to simplify and control its complexity.

Example Of Proxy:

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/b/bb/Proxy_concept_en.svg/400px-Prox_y_concept_en.svg.png[/img]

[img]http://i.minus.com/jxzFhXE2SVeet.png[/img]

Please keep in mind that this thread was made to help lower down the LQ posts that is in this section. I gathered information from frequently asked questions and put it in one thread. This thread will keep being updated as more questions are being being asked

[Credits.](#)

F-Nuke - September 7, 2013, 7:43 am

Nice thread. It'll be of use to beginners/noobs.

Good luck.

Nas - September 7, 2013, 7:45 am

(Sep 7, 2013 07:43 AM)a3ro Wrote: [CITE](#) Nice thread. It'll be of use to beginners/noobs.

Good luck.

That's what its made for ?

Anyways i hope its simple enough and good explanation took me about 1 hour and 30min - 2 hours.

muzzy. - September 7, 2013, 8:06 am

Wonderful thread, but bigger & better ones have been made and they end up buried in days.

Nice share though man, it's appreciated.

Nas - September 7, 2013, 8:43 am

(Sep 7, 2013 08:06 AM)Rogue? Wrote: [\[CITE\]](#) Wonderful thread, but bigger & better ones have been made and they end up buried in days.

Nice share though man, it's appreciated.

Yup, and I guess this thread will most likely die out also . I don't know people are being lazy and not using the search button other then posing a million threads on " how to hack my wife's fb " ffs.

CreepyPasta - September 7, 2013, 8:46 am

Amazing man. You put a lot of hard work in this.

I hope you get 5/5 on this thread.

Nas - September 12, 2013, 1:47 pm

(Sep 7, 2013 08:46 AM)Homework™ Wrote: [\[CITE\]](#) Amazing man. You put a lot of hard work in this.

I hope you get 5/5 on this thread.

Thank's a lot but i think the thread died out. Oh well, it was a good guide and i thought it would help.
:/

'Snorlax - September 12, 2013, 1:58 pm

You missed a bracket in the DDoS part ;)
align=center] IMAGE [/align]

Nas - September 12, 2013, 2:02 pm

(Sep 12, 2013 01:58 PM)Snorlax Wrote: [\[CITE\]](#) You missed a bracket in the DDoS part ;)
align=center] IMAGE [/align]
Been knowing this, but i cant.
It says that i have 7 images and i can't add more. ?

'Snorlax - September 12, 2013, 2:09 pm

(Sep 12, 2013 02:02 PM)-Nas Wrote: [\[CITE\]](#) Been knowing this, but i cant.
It says that i have 7 images and i can't add more. ?
Alignment != Embedding an image.
You should be able to o.o

Rackzen - September 12, 2013, 2:19 pm

i know how to work with all things , anyways , very nice tutorial ! I recommend that ! :)

Nas - September 12, 2013, 2:23 pm

(Sep 12, 2013 02:09 PM)Snorlax Wrote: [\[CITE\]](#) Alignment != Embedding an image.
You should be able to o.o
It wont let me i dont know, i think its glitched or something.

(Sep 12, 2013 02:19 PM)Rackzen Wrote: [\[CITE\]](#) i know how to work with all things , anyways , very nice tutorial ! I recommend that ! :)

Thanks for the recommendation buddy i hope you like it.

Rackzen - September 12, 2013, 2:29 pm

believe bro , two days ago , i explained that to my cousin , but if i didnt do that , i would give your tutorial to him.. :)

Nas - September 12, 2013, 3:03 pm

(Sep 12, 2013 02:29 PM)Rackzen Wrote: [\[CITE\]](#) believe bro , two days ago , i explained that to my cousin , but if i didnt do that , i would give your tutorial to him.. :)

Hahaha, Thanks man. I appreciate it. ?

SHADOW REALM - September 17, 2013, 6:27 pm

Cause this somehow made the news I'm going to be critical on some of your things

1. Horrible Grammar (For starters)

SHELLING

1. There is more than just a .php shell, there are CGI,ASP and so on
2. Most known and useful? SQLi lol? I would way prefer RCE over SQLi

DDoS

1. Your image is wrong, And what the fuck are handlers
2. If your going to include the internet in there you have to add it to every single one unless they are all connected via a LAN cable which then they would all be on the same network and your definition of a DDoS attack that would only be a DoS

DoS

1. New methods aren't found daily. Nobody even cares about DoS attacks

Manboy719 - September 17, 2013, 7:19 pm

Hey guys I'm new to this but I'mgonna learn all the lingo and eeverything... If anyone has any beginner tips I would really appreciate it

Nas - September 18, 2013, 5:26 am

(Sep 17, 2013 06:27 PM)LevelUp Wrote: [\[CITE\]](#) Cause this somehow made the news I'm going to be critical on some of your things

1. Horrible Grammar (For starters)

SHELLING

1. There is more than just a .php shell, there are CGI,ASP and so on
2. Most known and useful? SQLi lol? I would way prefer RCE over SQLi

DDoS

1. Your image is wrong, And what the fuck are handlers
2. If your going to include the internet in there you have to add it to every single one unless they are all connected via a LAN cable which then they would all be on the same network and your definition of a DDoS attack that would only be a DoS

DoS

1. New methods aren't found daily. Nobody even cares about DoS attacks
All you have written is opinions, but thanks for the feedback. ?

prakash - September 18, 2013, 6:29 am

good thread.. useful for me java drive.,

Harshjani - September 18, 2013, 6:50 am

Nice one man..I like it very much as i am a beginner..Thanks!

Nas - September 18, 2013, 12:26 pm

No problem guys, enjoy. ? ?

Acrobix - September 18, 2013, 12:45 pm

Wonderful thread, but bigger & better ones have been made and they end up buried in days.

Nice share though man, it's appreciated. :D

Nas - September 18, 2013, 6:06 pm

(Sep 18, 2013 12:45 PM)Acrobix Wrote: [\[CITE\]](#) Wonderful thread, but bigger & better ones have been made and they end up buried in days.

Nice share though man, it's appreciated. :D

Im going to add more stuff this weekend. Every weekend i will. ? Hopefully it will help a lot of people. ?

Deep Web - September 19, 2013, 10:08 am

Nice thread here good work. Will help the people that don't know much.

Nas - September 19, 2013, 11:19 am

That's for the support , and yep it will .

waka23 - September 19, 2013, 5:01 pm

helped me out a lot and answered a bunch of questions, thanks!

Nas - September 19, 2013, 5:55 pm

(Sep 19, 2013 05:01 PM)waka23 Wrote: [\[CITE\]](#) helped me out a lot and answered a bunch of questions, thanks!

No problem. Enjoy. ? ?

Nas - October 3, 2013, 7:30 am

Bump, Maybe people still might find this useful. ?

Th3PonyWizard - October 3, 2013, 11:06 am

It is actually saddening me to see those subjects once filtered as the highest level of Application-Hacking, Networking, and all around specialty to get down ever so quickly. A happier version of this planet would have this thread as well, just 90% coding at different languages instead of shit tools. That's beginning level, not your cancerous RATs. Should I laugh or cry, when you refer any-other-website-attack (Aside MySQL Exploit and that's a thing apparently) to acunetix, a completely automatic website scanning and exploitation tool? That's how you begin learning apparently, from the top to the bottom.

HellaCrow - October 3, 2013, 2:35 pm

Thanks bro great info. 5/5 amazing work :)

Nas - November 2, 2013, 7:08 pm

Bump, this still might help people.

Zapu - November 2, 2013, 7:10 pm

You should have added in TOR after you put VPN and Proxy.

Nas - November 2, 2013, 7:12 pm

(Nov 2, 2013 07:10 PM)Sakagami Wrote: [CITE](#) You should have added in TOR after you put VPN and Proxy.

I shall add that tomorrow or today.

UhOhDude - December 12, 2013, 7:05 pm

Very nice guide man. This has probably helped many beginner hackers.

iamlegend101542 - December 13, 2013, 8:13 am

Nice Thread, Learned something new here.

Nas - December 13, 2013, 10:39 am

No problem guys, will be updating this thread this weekend and add more things.

XxXDarkHunterXxX232 - December 13, 2013, 10:48 am

Although a large portion of this doesn't pertain to hacking, it'll still help the new users.

Nas - December 30, 2013, 8:00 am

Bump, this is still here.

Might help a lot of members. ?

balvant baldaniya - December 30, 2013, 10:13 am

wow..Amazing Amazing Amazing .,., nice job bro.,., its very usefull for noobs.,.,,

AlboX - December 30, 2013, 10:16 am

Nice thread here good work. Will help the people that don't know much.

Armadillobacon - January 1, 2014, 6:57 am

Thanks a heap for this! It's really quite helpful for beginners and people who are just unsure on a few of those topics.

Nas - February 4, 2014, 10:19 am

Bumping this. It might help people in the future.

mindfork - February 4, 2014, 11:50 am

While I appreciate you want to help newcomers, there are a few things you should improve imho:

Quote:Shelling is one of the basic or expert tools when hacking a website. If you're going to " shell " a website , it means that you are uploading a .php (shell) file in one of the websites directory to have full control of the website.

A shell is an interface that allows users to communicate with the OS. In this case you refer to a webshell which enables you to interact with the servers' OS through a web application. Therefor it doesn't needs to be written in .php, it's depending on the server.

Quote:You will have to find a exploit on the website.

You don't find exploits. You'll have to find vulnerabilities, then create an exploit (or use one that someone else already made).

Quote:The most known and useful exploits would be:

MySQL exploit

The term MySQL exploit is misleading. What you wanted to say was 'SQL injection' (there are more database management systems than MySQL: Oracle, MS-SQL, etc...), which is a technique to exploit regarding vulnerabilities.

Quote:DDoS is caused by sending multiple packets using many different Networks to take down a target so much so that it cannot respond to the traffic.

Kinda yes but then this picture. So you connect to your bots before actually reaching the internet, which implies that they're all in one network?

Quote:But, like viruses, new DoS attacks are constantly being made.

Yes? Which one?

Quote:A crypter is a program that allows users to crypt the coding of their program. Generally, antivirus work by splitting source code of application and then search for certain string within source code.

Crypters encrypt executable files, not their source code, which you can't examine after a program was compiled and linked. Likewise AVs can't see through source codes.

Furthermore I wouldn't refer beginners to tools like acunetix.

Hope I could help.

Brule - February 5, 2014, 10:46 am

Nice one mate! Just wanted to leave a comment to tell you that it hasn't died completely, and that it's amazing!

Thanks a lot for sharing this! ? ?