Forum:Hack Forums

Thread: Complete Beginners Hacking Guide

Batman96 - *November 1, 2018, 5:38 am*

Introduction:
Hello and welcome to the official "Beginners Hacking Guide" in this guide we will be going over many different things, which include DDoS, VPN, RATS and more.

What is hacking?: (Section 1)
In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking. The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks.

Choosing your hacking path: (Section 2)
Explaining this simply, there is "three" different types of hackers being:

Black hats: A black hat hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security. Black hat hackers are also known as crackers or dark-side hackers. The general view is that, while hackers build things, crackers break things. They are computer security hackers that break into computers and networks or also create computer viruses. The term â€œblack hatâ€? comes from old westerns where the bad guys usually wore black hats and the good guys wore white ones.

Grey hats: The term "grey hat" refers to a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.

And last but not least:

White hats: White hat hackers are usually seen as hackers who use their skills to benefit society. They may be reformed black hat hackers or they may simply be well-versed in the methods and techniques used by hackers. An organisation can hire these consultants to do tests and implement best practices that make them less vulnerable to malicious hacking attempts in the future.

Hacking/Networking terms: (Section 3)

Back door: A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections. Some have alleged that manufacturers have worked with government intelligence to build backdoors into their products. Malware is often designed to exploit back doors.

Botnet: A botnet is a group of computers controlled without their ownersâ€™ knowledge and used to send spam or make denial of service attacks. Malware is used to hijack the individual computers, also known as â€œzombies,â€? and send directions through them. They are best known in terms of large spam networks, frequently based in the former Soviet Union.

Brute force: Also known as an exhaustive key search, a brute force attack is an automated search

for every possible password to a system. It is an inefficient method of hacking compared to others like phishing. Itâ€™s used usually when there is no alternative. The process can be made shorter by focusing the attack on password elements likely to be used by a specific system.

Cookies: Cookies are text files sent from your Web browser to a server, usually to customise information from a website.

Cracking: To break into a secure computer system, frequently to do damage or gain financially, though sometimes in political protest.

Denial of service attack (DoS): DoS is used against a website or computer network to make it temporarily unresponsive. This is often achieved by sending so many content requests to the site that the server overloads. Content requests are the instructions sent, for instance, from your browser to a website that enables you to see the website in question. Some have described such attacks as the Internet equivalent of street protests and some groups, such as Anonymous frequently use it as a protest tool.

Distributed denial of service attack (DDoS): A DoS using a number of separate machines. This can be accomplished by seeding machines with a Trojan and creating a botnet or, as is the case with a number of Anonymous attacks, by using the machines of volunteers.

Doxing: Discovering and publishing the identity of an otherwise anonymous Internet user by tracing their online publically available accounts, metadata, and documents like email accounts, as well as by hacking, stalking, and harassing.

Firewall: A system using hardware, software, or both to prevent unauthorized access to a system or machine.

Hacktivist: A hacker whose goals are social or political. Examples range from reporting online anonymously from a country that attacks free speech to launching a DDoS campaign against a company whose CEO has issued objectionable statements. Not to be confused with slacktivism, which refers to push-button activism in which a supporter of a social or political campaignâ€™s goals does nothing but register their support online, for instance by â€œlikingâ€? a Facebook page.

IP: Internet protocol address. Itâ€™s the distinctive numeral fingerprint that each device carries thatâ€™s connected to a network using Internet Protocol. If you have a deviceâ€™s IP you can often identify the person using it, track its activity, and discover its location. These addresses are apportioned by the regional Internet registries of the IANA (the Internet Assigned Numbers Authority). Crackers can use knowledge of your IP address to your computer via one of its ports, the points that regulate information traffic flow.

Malware: A software program designed to hijack, damage, or steal information from a device or system. Examples include spyware, adware, rootkits, viruses, keyloggers, and many more. The software can be delivered in a number of ways, from decoy websites and spam to USB drives.

Phishing: Tricking someone into giving you their personal information, including login information and passwords, credit card numbers, and so on by imitating legitimate companies, organizations, or people online. Phishingâ€™s often done via fake emails or links to fraudulent websites.

Rootkit: A rootkit is a set of software programs used to gain administrator-level access to a system and set up malware, while simultaneously camouflaging the takeover.

Script kiddie: A pejorative term for a would-be cracker without technical skills. Script kiddies use

prefab cracking tools to attack systems and deface them, often in an attempt to score points with their peers.

Social engineering: A custodian is to a janitor as a social engineer is to a con man. Social engineering is conning people into giving you confidential information, such as passwords to their accounts. Given the difficulty of breaking, 128-bit encryption with brute force, for example, social engineering is an integral element of cracking. Examples include phishing and spear-phishing.

Spoofing: Email spoofing is altering the header of an email so that it appears to come from elsewhere. A black hat hacker, for instance, might alter his email header so it appears to come from your bank. IP spoofing is the computer version, in which a packet is sent to a computer with the IP altered to imitate a trusted host in the hope that the packet will be accepted and allow the sender access to the target machine.

Virus: Self-replicating malware that injects copies of itself in the infected machine. A virus can destroy a hard drive, steal information, log keystrokes, and many other malicious activities.

Vulnerability: A weak spot hackers can exploit to gain access to a machine.

VPNs: (Section 4)
So, you might be asking "Why should I hide my IP" what's the purpose here's some reasons:

Browse websites without leaving a trace of your identity.
Access to streaming, wherever you are.
Stay safe from snoopers looking to access your information.
Access websites that are not available to IP address's geographic location.

These are just a few benefits of using a VPN, there is many more.

Here is a list of some good VPN's (Paid):
https://www.purevpn.com
https://crypticvpn.com/
https://hidemyass.com
https://openvpn.com

If you're looking for a free VPN:
https://www.hotspotshield.com/
https://www.cyberghostvpn.com/

Another thing with VPNs people tend to get confused with is the fact that it doesn't actually "change" your IP address, it simply masks it.

Doxing: (Section 5)

What is doxing?

Doxing is the process of retrieving, hacking and publishing other peopleâ€™s information such as names, addresses, phone numbers and credit card details. Doxing may be targeted toward a specific person or an organization. There are many reasons for doxing, but one of the most popular is coercion.

How do I prevent being doxed?

There are a few different ways to make it harder to be doxed which include:
1) Using different usernames.
2) NEVER enter any of your real information on ANY website.
3) Use a VPN.

How do I DoX someone?

There is a lot of helpful websites that can assist you in the process:
http://pipl.com
https://namechk.com/
http://spokeo.com

RATs: (Section 6)

What is a RAT?

A remote administration tool (RAT) is a piece of software that allows a remote "operator" to control a system as if they have physical access to that system. While desktop sharing and remote administration have many legal uses, "RAT" software is usually associated with criminal or malicious activity. Malicious RAT software is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software.

The operator controls the RAT through a network connection. Such tools provide an operator the following capabilities:

Screen/camera capture or image control
File management (download/upload/execute/etc.)
Shell control (from command prompt)
Computer control (power off/on/log off if remote feature is supported)
Registry management (query/add/delete/modify)
Hardware Destroyer (overclocker)
Other software product-specific functions

Wouldn't an anti-virus detect it?

It depends, there are ways of "Crypting" your RAT's stub (the file you distribute) so it doesn't get detected by an anti-virus.

What are some good RAT's I can use?

Personally, I would recommend:
Luminosity (https://luminosity.link/)
Nano Core (https://nanocore.io/)

Key Loggers: (Section 7)

What is a Key Logger?:

A keylogger, also known as keystroke logging or keylogging, is a method of tracking the strokes on a keyboard without the knowledge of the user. (A Key logger is similar to a RAT, but with less features).

Anti-Virus (Section 8)

Despite people being able to crypt files etc, it's still very important to have a solid anti-virus, don't be to trusting and download files that seem sketchy.

You can also scan files/links using websites such as:
http://www.virustotal.com

Some good anti-viruses:
Norton 360
Malwarebytes
AVG
Bullguard

Bruteforcing: (Section 9)

(Refer to Section 3 for Definition)

How do I hack accounts?

There are many different ways of "hacking" accounts, which include:

Databases: This is the most effective way in my opinion, you can search through dropped databases and look for the victims login details, the down side with databases is they are often huge files, although there is a website called http://leakedsource.com (Paid) were you can simply search for the username/email/ip etc.

And obviously bruteforcing which was explained above.

Thanks for reading, a comment would be appreciated. If there's any errors or anything, don't hesitate to let me know!

sh4moon - *November 1, 2018, 6:59 am*
this would make a good computer security dictionary/encyclopedia. nicely done op. did you copy and paste the definitions?

Infamia - *November 1, 2018, 7:15 am*
Quote:Denial of service attack (DoS): DoS is used against a website or computer network to make it temporarily unresponsive. This is often achieved by sending so many content requests to the site that the server overloads. Content requests are the instructions sent, for instance, from your browser to a website that enables you to see the website in question. Some have described such attacks as the Internet equivalent of street protests and some groups, such as Anonymous frequently use it as a protest tool.

anonymous don't use dos to protest

Quote:Distributed denial of service attack (DDoS): A DoS using a number of separate machines. This can be accomplished by seeding machines with a Trojan and creating a botnet or, as is the case with a number of Anonymous attacks, by using the machines of volunteers.

separate networks, not separate machines.
you can't execute a ddos attack by adding more pcs, you do it by adding more networks and expanding your bandwidth.

unless your ddos tool doesn't occupy the whole bandwidth of the network, in which case, adding more would be better.

EDIT:

Quote:Phishingâ€™s often done via fake emails or links to fraudulent websites.

this aint it chief

SysAdmin - *November 1, 2018, 7:35 am*
I swear I've seen this exact thread somewhere.

Godarranco - *November 1, 2018, 7:51 am*
thanks aminaqi for infomation.

sh4moon - *November 1, 2018, 8:40 am*
(Nov 1, 2018 07:35 AM)SysAdmin Wrote: [CITE] I swear I've seen this exact thread somewhere.
I'm sure there's been a few threads like it in the past. everybody wants a beginners guide to hacking.

domation666 - *November 1, 2018, 3:26 pm*
does this needs to open a thread for some Wikipedia articles ?

Tchiko - *December 29, 2018, 3:10 pm*
I savored this article with much greed. what is he delisious

OBAMASELF - *December 30, 2018, 7:37 am*
This is really promising.