Hacker's Dictionary

 //////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*//////

Are you new to the realm of hacking?

Do you feel dumb when you don't know the meaning of a certain term?Well, then this will certainly help you out! This Dictionary Is Provided By Cyber elite. If you are ever unsure about anything, simply scroll down and find that specific word, then read the definition.

Anything includes: Abbreviations, Phrases, Words, and Techniques.*The list is in alphabetical order for convenience!*

Abbreviations

? DDoS = Distributed Denial of Service

? DrDoS = Distributed Reflected Denial of Service Attack, uses a list of reflection servers or other methods such as DNS to spoof an attack to look like it's coming from multiple ips. Amplification of power in the attack COULD occur.

? FTP =File Transfer Protocol. Used for transferring files over an FTP server.

? FUD = Fully Undetectable

? Hex =In computer science, hexadecimal refers to base-16 numbers. These are numbers that use digits in the range: 0123456789ABCDEF. In the C programming language (as well as Java, JavaScript, C++, and other places), hexadecimal numbers are prefixed by a 0x. In this manner, one can tell that the number 0x80 is equivalent to 128 decimal, not 80 decimal.

? HTTP =Hyper Text Transfer Protocol. The foundation of data communication for the World Wide Web.

? IRC = Internet Relay Chat. Transmiting text messages in real time between online users.

? JDB =Java drive-by, a very commonly used web-based exploit which allows an attacker to download and execute malicious code locally on a slave's machine through a widely known java vulnerability.

? Malware =Malicious Software

? Nix = Unix based operating system, usually refered to here when refering to DoS'ing.

? POP3 =This is the most popular protocol for picking up e-mail from a server.

? R.A.T = Remote Administration Tool

? SDB = Silent drive-by, using a zero day web-based exploit to hiddenly and un-detectably download and execute malicious code on a slave's system. (similar to a JDB however no notification or warning is given to the user)

? SE = Social Engineering

? Skid =Script Kid/Script Kiddie

? SMTP =A TCP/IP protocol used in sending and receiving e-mail.

? SQL =Structured Query Language. It's a programming language, that used to communicate with databases and DBMS. Can go along with a word after it, such as "SQL Injection."

? SSH =Secure Shell, used to connect to Virtual Private Servers.

? TCP = Transmission Control Protocol, creates connections and exchanges packets of data.

? UDP =User Datagram Protocol, An alternative data transport to TCP used for DNS, Voice over IP, and file sharing.

? VPN =Virtual Private Network

? VPS =Virtual Private Server

? XSS (CSS) = Cross Site Scripting

Words

?Algorithm = A series of steps specifying which actions to take in which order.

?ANSI Bomb = ANSI.SYS key-remapping commands consist of cryptic-looking text that specifies, using ansi numeric codes to redefine keys.

?Back Door = Something a hacker leaves behind on a system in order to be able to get back in at a later time.

?Binary = A numbering system in which there are only two possible values for each digit: 0 and 1.

?Black Hat = A hacker who performs illegal actions to do with hacking online. (Bad guy, per se)

?Blue Hat =A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term BlueHat to represent a series of security briefing events.

?Bot = A piece of malware that connects computer to an attacker commonly using the HTTP or IRC protocal to await malicous instructions.

?Botnet = Computers infected by worms or Trojans and taken over by hackers and brought into networks to send spam, more viruses, or launch denial of service attacks.

?Buffer Overflow = A classic exploit that sends more data than a programmer expects to receive. Buffer overflows are one of the most common programming errors, and the ones most likely to slip through quality assurance testing.

?Cracker = A specific type of hacker who decrypts passwords or breaks software copy protection schemes.

?DDoS = Distributed denial of service. Flooding someones connection with packets. Servers or web-hosted shells can send packets to a connection on a website usually from a booter.

?Deface =A website deface is an attack on a site that changes the appearance of the site or a certain webpage on the site.

?Dictionary Attack = A dictionary attack is an attack in which a cyber criminal can attempt to gain your account password. The attack uses a dictionary file, a simple list of possible passwords, and a program which fills them in. The program just fills in every single possible password on the list, untill it has found the correct one. Dictionary files usually contain the most common used passwords.

?DOX = Personal information about someone on the Internet usualy contains real name, address, phone number, SSN, credit card number, etc.

?E-Whore = A person who manipulates other people to believe that he/she is a beautiful girl doing cam shows or selling sexual pictures to make money.

?Encryption = In cryptography, encryption applies mathematical operations to data in order to render it incomprehensible. The only way to read the data is apply the reverse mathematical operations. In technical speak, encryption is applies mathematical algorithms with a key that converts plaintext to ciphertext. Only someone in possession of the key can decrypt the message.

?Exploit = A way of breaking into a system. An exploit takes advantage of a weakness in a system in order to hack it.

?FUD = Fully undetectable, can be used in many terms. Generally in combination with crypters, or when trying to infect someone.

?Grey Hat = A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.Hacker (definition is widely disputed among people...) = A hacker is someone who is able to manipulate the inner workings of computers, information, and technology to work in his/her favor.

?Hacktivist = A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

?IP Address = On the Internet, your IP address is the unique number that others use to send you traffic.

?IP Grabber = A link that grabs someone's IP when they visit it.

?Keylogger = A software program that records all keystrokes on a computer's keyboard, used as a surveillance tool or covertly as spyware.Leach = A cultural term in the warez community referring to people who download lots of stuff but never give back to the community.

?LOIC/HOIC = Tool(s) used by many anonymous members to conduct DDoS attacks. It is not recommended to use these under any circumstances.

?Malware =Software designed to do all kinds of evil stuff like stealing identity information, running DDoS attacks, or soliciting money from the slave.

Neophyte = A neophyte, "n00b", or "newbie" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.

?smith = Somebody new to a forum/game.

?OldFag = Somebody who's been around a forum/game for a long time.

?Packet = Data that is sent across the Internet is broken up into packets, sent individually across the network, and reassembled back into the original data at the other end.

?Phreak =Phone Freaks. Hackers who hack cell phones for free calling. Free Long distance calling. Etc.

?Phreaking = The art and science of cracking the phone network.

?Proxy = A proxy is something that acts as a server, but when given requests from clients, acts itself as a client to the real servers.

?Rainbow Table = A rainbow table is a table of possible passwords and their hashes. It is way faster to crack a password using rainbow tables then using a dictionary attack (Bruteforce).

?Remote Administration Tool =A tool which is used to remotely control (an)other machine(s). These can be used for monitoring user actions, but often misused by cyber criminals as malware, to get their hands on valuable information, such as log in credentials.

?Resolver =Software created to get an IP address through IM (instant messenger, like Skype/MSN) programs.

?Reverse Engineering = A technique whereby the hacker attempts to discover secrets about a program. Often used by crackers, and in direct modifications to a process/application.

?Root = Highest permission level on a computer, able to modify anything on the system without restriction.

?Rootkit (ring3 ring0) =A powerful exploit used by malware to conceal all traces that it exists. Ring3 - Can be removed easily without booting in safemode. Ring0 - Very hard to remove and very rare in the wild, these can require you to format, it's very hard to remove certain ring0 rootkits without safemode.

?Script Kiddie = A script kid, or skid is a term used to describe those who use scripts created by others to hack computer systems and websites. Used as an insult, meaning that they know nothing about hacking.

?Shell = The common meaning here is a hacked web server with a DoS script uploaded to conduct DDoS attacks via a booter. OR A shell is an script-executing unit - Something you'd stick somewhere in order to execute commands of your choice.

?Social Engineer = Social engineering is a form of hacking that targets people's minds rather than their computers. A typical example is sending out snail mail marketing materials with the words "You may already have won" emblazoned across the outside of the letter. As you can see, social engineering is not unique to hackers; it's main practitioners are the marketing departments of corporations.

?Spoof = The word spoof generally means the act of forging your identity. More specifically, it refers to forging the sender's IP address (IP spoofing). (Spoofing an extension for a RAT to change it from .exe to .jpg, etc.)

?SQL Injection =An SQL injection is a method often used to hack SQL databases via a website, and gain admin control (sometimes) of the site. You can attack programs with SQLi too.

?Trojan = A Trojan is a type of malware that masquerades as a legitimate file or helpful program with the ultimate purpose of granting a hacker unauthorized access to a computer.

?VPS = The term is used for emphasizing that the virtual machine, although running in software on the same physical computer as other customers' virtual machines, is in many respects functionallyequivalent to a separate physical computer, is dedicated to the individual customer's needs, has the privacy of a separate physical computer, and can be configured to run server software.

?Warez = Software piracy

?White Hat = A "white hat" refers to an ethical hacker, or a computer security expert, who specializes in penetration testing and in other testing methods to ensure the security of a businesses information systems. (Good guy, per se)

?Worm = Software designed to spread malware with little to no human interaction.

Zero Day Exploit = An attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability. This means that the developers have had zero days to address and patch the vulnerability.

Hope we helped the new learners.............