Keeping up to speed with Hacker Lingo

Posted At : December 29, 2018 6:15 PM | Posted By : Admin
Related Categories: General Info

Like nearly every passion, sport, profession, or hobby, hacking has its own lingo. Here's a quick review of some hacking lingo!

Test your knowledge here

You already know what phishing and spyware are, but how about spearfishing? Shodan? Zombies? Here's a glossary of some hacker lingo that you and your IT team should be aware of.

Brute Force Attack

When a hacker tries to guess your system's password by guessing all the passwords with an intensive automated search. One of the biggest reasons the US and China are investing in quantum computing research is because quantum machines can, in theory, defend against this kind of barrage.

Doxxing

Exposing a person's sensitive personal information on the internet. It can be anything from addresses and phone numbers to credit card and social security numbers. An example of doxxing specific to the business world is Whaling.

Evil Maid Attack

When a hacker goes in and hacks your device in person. This person has access to your space—the kind of access that a maid tidying your office might have.

Grey Hat

Black hats are hackers who are up to no good; White hats are cybersecurity experts who spend their time helping organizations defend themselves. (To make things more confusing, some white hats are good at their jobs because they used to be black hats.) Meanwhile, grey hats employ black hat techniques, but they don't do it for profit or nefarious reasons; they're hacking because they're on a mission (that can be good or bad). If you are a grey hat, sometimes you are also a...

Hacktivist

People who hack to make a political or social statement. Prominent groups like Anonymous and WikiLeaks think of themselves as hacktivists.

R.U.D.Y attack

Short for "R U Dead Yet," this is a slow-rate (also known as a "low and slow") attack designed to exhaust a web server by submitting long-form fields until it crashes.

Sniffing

Capturing unencrypted data as it transmits over a network. Sniffers can be used to diagnose network issues—or steal sensitive information.

Spearphishing

A phishing scheme that targets a certain group within an organization. (Also see Whaling.)

Shodan

Shodan refers to Shodan.io, a site that scans entry-level devices connected to the internet (such as many IoT devices) and looks for vulnerabilities. Ostensibly it's used to help you secure devices, but hackers will look for vulnerabilities to exploit them. (In Japanese, "shodan" refers to an entry-level martial arts belt.)

Whaling

A phishing scheme that takes aim at the very top of the c-suite food chain. Hackers collect executives' personal information (and threaten to doxx them) or compromising information (such as their salaries) to blackmail them into paying a ransom or some other demand.

Worm

A type of malware that replicates itself automatically, spreading across the network.

Zero-day exploit

Also known as a zero-day attack. This is when a hacker finds a weak point in a system and releases malware before developers can release a patch. "Day zero" is jargon for the day the target learns of the vulnerability; in a zero-day exploit, the target has "zero days" to do anything about it.