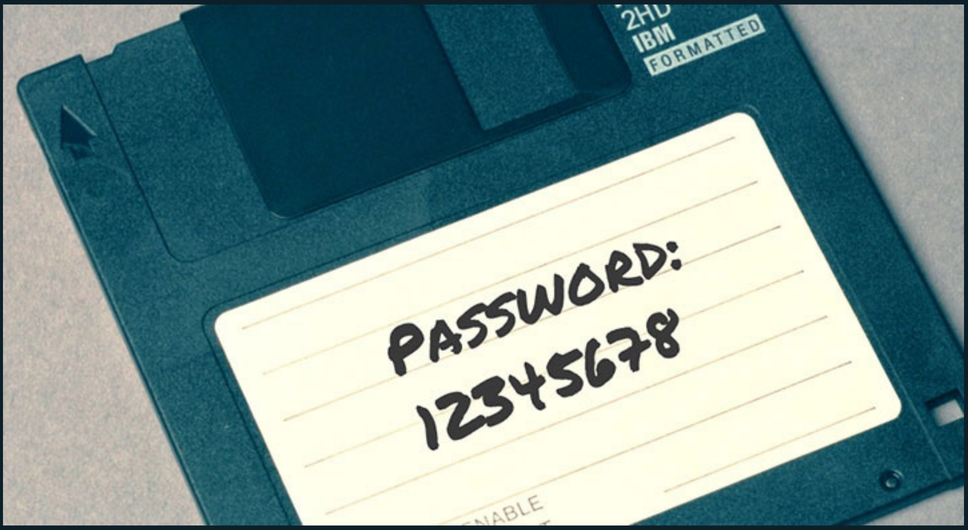
What is a Hacker (part 1): Types, tools and techniques

The popular definition of a hacker is someone who uses their technical abilities to gain unauthorized access to computers. In reality hackers are as diverse as people in general, having expert technical abilities does not have to make you a criminal; it can make you a hero.

Types of hackers

As with people, there are many different types of hackers with wildly different world views and motivations. The term "Hats" comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively.



- **White Hat Hacker**
  First of all, we have the good guys; these are the ethical hackers that use their power for good. Usually they are employed or contracted by companies and governmental entities to find vulnerabilities before other hackers will. White hat hackers always operate within the confines of the law.

  Famous: Charlie Miller, Tsutomu Shimomura, Greg Hoglund

- **Black Hat Hacker**
  On the opposite side of the spectrum, the Black Hats operate outside any moral and legal framework, motivated by personal or financial gain. They break into systems, steal login credentials and private data which they use for extortion or put up for sale online.

  Infamous: Kevin Mitnick, Jonathan James, Albert Gonzalez

- **Grey Hat Hacker**
  As the name suggests the Grey Hat hacker is a mix of both White and Black hats. They look for vulnerabilities without permission but often report them to the owner, sometimes for free and sometimes with demand for compensation. If that demand is not meet they might leak the information online or exploit it, becoming a Black Hat.

  Famous: Adrian Lamo, Gary McKinnon, Kevin Poulsen

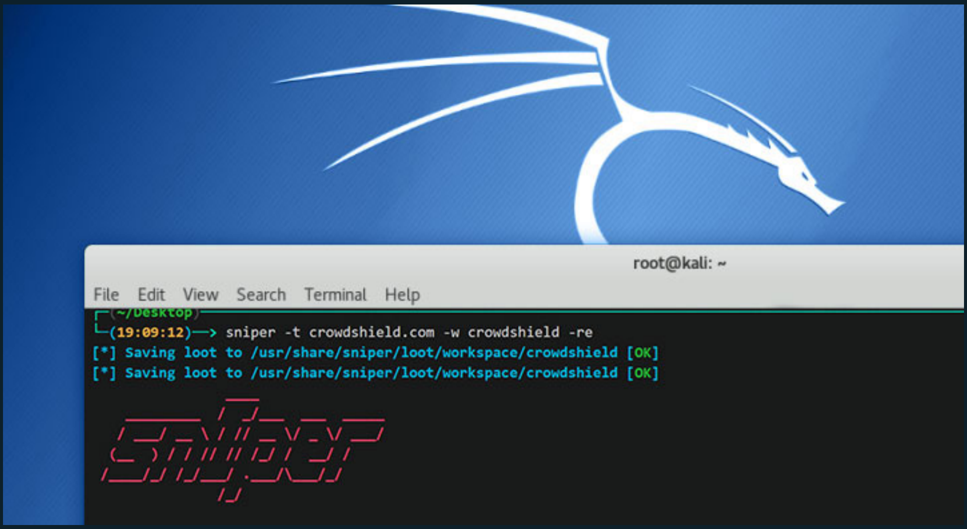
- **Red Hat Hacker**
  These are the hunters of the hacker world, and their prey are Black Hats. Their sole objective is to destroy the efforts of illegal hackers and take their infrastructure down.

- **Blue Hat Hacker**
  These are novice hackers who's main agenda is revenge on anyone who makes them angry. They have little interest in learning and use ready-made scripts to do their dirty work.

- **Green Hat Hacker**
  You will find the Green Hats on online hacking forums asking questions to the more seasoned professionals. These are the amateurs eager to learn the tools of the trade and become a full-blown hacker.

Common hacking tools

Most Hacking tools are used by both security researchers and criminals. If the tool finds a vulnerability it can be patched, or exploited, depending on your ethical alignment.



```
┌─(~/Desktop)
└─(19:09:12)──> sniper -t crowdshield.com -w crowdshield -re
[*] Saving loot to /usr/share/sniper/loot/workspace/crowdshield [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/crowdshield [OK]
```

- **Rootkits**
  Special software that allows a hacker to gain remote access to a victim's computer. Originally, rootkits were developed to fix software problems remotely but have since then been weaponized by hackers.

  In the news: Sony BMG copy protection rootkit scandal, Greek wiretapping case

- **Keyloggers**
  Software designed to eavesdrop on the victim's computer, recording every keystroke the user does. Everything is intercepted and stored on a log file, credit card numbers, personal communication, phone numbers, passwords.

  In the news: Selectric Bug (Oldschool), PunkeyPOS

- **Vulnerability scanners**
  A software that scans large networks of computers to find weaknesses that can be exploited or patched. For example, a White Hat scans to find holes to patch while a Black Hat scans to find holes to exploit.

  Most used: Sn1per, Nessus, MBSA, GFI Languard

- **Worm, Virus & Trojan**
  Worms and Viruses are malicious programs designed to steal your data and spread to other computers within the network. Trojans are impostors, files that look like desirable programs but contain malicious code. The main difference is that Trojans do not infect other computers; they do not self-replicate.

  Most destructive: ILOVEYOU, MyDOOM, Storm Worm, SLAMMER

- **Botnet**
  A Botnet is a series of hijacked computers all around the world that the Hacker controls. They can be used to perform DDoS-attacks, bringing down specific servers with massive amount of traffic. Botnets are created and managed by Hackers that either use them for their own purposes or sell them as a service.

Common hacking techniques

Usually a Hacker deploys multiple techniques to reach their goal, sometimes the simplest ways are the most efficient. Using social engineering techniques exploiting human kindness, greed and curiosity to gain access is not uncommon.

- **Phishing**
  The Hacker makes a perfect copy of a popular website and uses a URL that is close enough to the original to go unnoticed. He then sends a legitimate-looking email to the target containing a link to the phishing site. The target will unknowingly sign in to the fake website giving the hacker his login credentials.

  More info: Phishing.org, Tripwire
  Attacks: Phish Phry, Walter Stephan, FMS Scam

- **SQL Injections**
  Most websites use an SQL database to store information about their customers. An application communicating with that database can be exploited with SQL-injections if it's poorly coded. The attack is executed on the website's user-input fields (search box, login box, etc) that accept illegal input, giving the hacker access to the database.

  More info: Wiki, Portswigger
  Attacks: TalkTalk, WTO, Wall Street Journal

- **DoS/DDoS**
  In a Denial of Service attack, the hacker uses a Botnet (network of hijacked computers) to flood a specific server with massive amounts of traffic. The server is quickly overloaded, and all websites hosted on it will be offline.

  More info: Wiki, Cloudflare
  Attacks: Github, Occupy Central Hong Kong, CloudFlare

- **Brute Force**
  Essentially it's guessing passwords until the hacker get's it right. If a user has a weak password, i.e. "1234" or "password", the hacker can try to guess it either by hand or using specialized tools.

  More info: Wiki, Infosec
  Attacks: GitHub, Alibaba's Taobao, U.S Utility Control System

- **Fake WAP**
  Free WiFi is common in public spaces like airports & coffee shops making it an ideal target for a hacker to exploit. The hacker creates a fake Wireless Access Point (WAP) mimicking the name of the real WiFi, so users connect to it. While the users is connected to the fake WiFi the hacker can read all information going through it, login credentials, credit card, and personal messages.

  More info: Wiki, Lifewire
  Examples: 7-year old break public network in 11 minutes, WiFi Pineapple

- **Sniffing/Snooping**
  The hacker monitors traffic on unsecured networks to find relevant information that can be used in a future attack.

  More info: Wiki, GreyCampus
  Examples: Sniffing attack against European hotels

- **Bait & Switch**
  In this attack, the Hacker buys advertising space on popular websites, and the ads will redirect the target to a page full of malware. The hacker's ads will look legitimate and very appealing to the target, but as soon as the target clicks them they will be infected. It's called Bait & Switch since the hacker's baiting with good ads and then switching the link to a bad page.

  More info: Wiki
  Examples: Hackers sell access to Bait-and-Switch empire

- **Cookie Theft**
  Most websites use cookies to store user data and make them load faster; this can be passwords, browsing history, etc. If the connections are not secured trough SSL the hacker can steal this data and use the cookie to authenticate themselves as the target.

  More info: Wiki
  Examples: Yahoo Cookie Forging Attack, iOS Cookie theft

- **Waterhole Attacks**
  The Hacker studies the target's daily routines to find out his favorite physical locations (café f.ex); these are the waterholes. Once the Hacker knows the waterholes and the timing of the target he sets his trap using a combination of techniques. He might create a Fake WAP free WiFi access point at that location, and knowing the target's favorite websites, he uses Phishing to steal the login credentials.

  More info: Wiki
  Examples: US Department of Labor, Forbes, ICAO

- **UI Redress/ClickJacking**
  In essence, the Hacker tricks the target to click on a specific link by making it look like something else. It's very common on movie streaming or torrent download pages; when the user clicks on "Download" or "Play", it's an advertising link they are clicking. In other cases it can be used to trick the target to transfer money to the Hacker from their online bank.

  More info: Wiki, Nodeswat
  Examples: Facebook

Original post can be found at our homepage:
https://www.bitidentify.com/blog/hacker-types-tools-and-techniques/