# Black Hat

Rules and Information v1.6

## 1 Welcome!

For years, you have been a king of the information superhighway. Using your skill, ingenuity, and a bit of luck, no computer on the cloud has ever been out of your reach. But now, a challenge has been issued. It's time to don your black hat and prepare to fight. The goal is simple – whoever hacks the Gibson supercomputer[1] will win eternal glory. To achieve this goal, you will be researching software exploits, blocking computers from use, installing firewalls, and taking over computers.

## 2 Basic Information

### 2.1 Number of players

This game supports 2 players (hereafter known as Hackers).

### 2.2 Estimated play time

Estimated play time is 30-40 minutes.

### 2.3 Materials

- 2 sets of Rules and Information with cheat sheets
- Playing Board with a computer network, 2 sets of 4 software research dials (red, green, blue, and yellow to indicate how close a player is to discovering an exploit for a particular color of software), 2 sets of Total CPU and Used CPU spaces, 1 DDOS space, and 1 Firewall space.
- The computer network should have 2 personal computers, approximately 19 cloud computers, and 1 Gibson Supercomputer. Each computer has a color or several colors determining which software have been installed on it (and therefore, which software exploits will be effective)
- 22 red and 22 green Rootkit markers to signify possession of computers by hackers

[1] Check out the movie *Hackers*

- 10 yellow DDOS Markers
- 10 blue Firewall Markers
- 60 CPU Beans
- 12 6-sided dice (Note: *True hackers use digital dice.* If you would like a faster and more convenient way to roll dice, grab a laptop and use the program at: `web.mit.edu/alect/www/blackhat/dice.html`)

### 2.4 How to Win

There are two ways to win. A hacker can either:

- Successfully take over the Gibson Supercomputer
- Take over all the other hacker's computers

# 3 Let's play!

## 3.1 Setup

Each hacker gets one of the starting computers which have a CPU of 4. Place a rootkit marker on it to indicate ownership. Each hacker then takes 4 CPU "beans" and places it into the respective "Total CPU" space to indicate their current CPU total. Each hacker sets all of their research dials to 0.

## 3.2 How to play

### 3.2.1 Determine who goes first

The player who can come up with the coolest hacker nickname goes first.

### 3.2.2 A turn

This is information about what a turn looks like:

- A hacker gets a number of CPU to spend based on the computers she controls. Unless a computer has a number written on it, assume its CPU is 1. Hackers should use CPU beans to keep track of how much CPU they have. Extra CPU does not carry over from turn to turn. At the start of her turn, a hacker piles all her CPU beans onto the Total CPU space.

- A hacker can spend as much CPU during her turn as she wants, limited only by the total CPU. As a hacker spends CPU, she should move spent CPU beans from the Total CPU space to the Used CPU space to keep track of how much CPU she has left to spend.
- A hacker can spend CPU to perform the following actions:
  - Research Exploit: A hacker can spend any number of CPU to research an exploit for a certain piece of software. She can increase the corresponding research dial a number of steps equal to the amount of CPU she spends to indicate her progress. When a hacker reaches level 6 of a single color, the hacker has discovered an exploit and computers with the corresponding color become easier to rootkit. If the hacker is the only one to have discovered this exploit, it's a "zero-day" exploit and it's even easier to rootkit computers of that color until another hacker discovers that exploit.
  - Research Patch: A hacker can spend any number of CPU to research a patch for a certain piece of software. When a patch is researched, any hacker with research for that piece of software has to decrease the research counter for that piece of software a number of steps equal to the amount of CPU spent on the patch. If a player no longer has enough research to exploit the software, that player no longer has an exploit for the software. A common strategy to prevent another player from removing your exploits is to research a piece of software beyond level 6 (the research dials go up to 10).
  - DDOS Attack: A hacker may DDOS a computer that neighbors one of their computers. A particular computer may only be DDOSed once per turn. DDOSing a computer takes twice the amount of CPU on the computer the hacker wishes to DDOS. That computer is shut down until the hacker decides not to DDOS anymore. To signify that it has been shut down, place a DDOS token on it. A computer that is shut down cannot be attacked and cannot contribute to the total CPU usable by the owner. The owner of the DDOSed computer should set aside a number of CPU beans equal to the CPU of the DDOSed computer to indicate that these cannot be used on the next turn. Essentially, a DDOSed computer acts as if it were removed from the board, so rules that require a hacker to have a neighboring computer act as though the DDOSed computer does not exist. A computer with a firewall on it *cannot* be DDOSed. DDOSes are removed at the beginning of the hacker's next turn.
  - Install Firewall: A hacker can place a firewall on an existing computer to prevent a future DDOS or defend a computer against potential future attacks. Installing a firewall costs twice the amount of CPU of that computer. Note that a player may *install multiple firewalls on a computer.*

Firewalling must be performed at the end of the hacker’s turn. Firewalls are removed at the beginning of the hacker’s next turn.

- Install Rootkit: A hacker can attempt to invade and install a rootkit on any computer neighboring a computer they own that was not invaded on the same turn. A hacker may only attempt to invade a particular computer once per turn. To rootkit a computer, the invading hacker must pay the amount of CPU on the target computer to get a single die roll. The invading hacker may then pay for extra die rolls at a cost of 2 CPU per die roll. The hacker must *announce the number of extra dice to be used before rolling the dice.* The player then rolls a number of 6-sided dice based on how much CPU she spent. The maximum value of the hacker’s rolls determines a successful rootkit install depending on conditions outlined below:

  - For a completely protected computer (no exploits), the player must roll a max of 6 to succeed.
  - For a computer with a color of software for which the hacker has an exploit, the hacker must roll a 5 or a 6 to succeed. Note that a computer with multiple colors can be exploited through any of those pieces of software.
  - For a computer with a color of software for which the hacker has a ”zero-day” exploit, the hacker must roll a 4, 5, or 6 to succeed.

  If the computer is owned by another hacker, the attacker must first roll using the above rules. If successful, the attacker and defender then have a roll-off to determine who gets the computer. The roll-off rules are as follows:

  - The defending hacker can spend up to the amount of CPU on the defending computer to get one die roll per CPU. This CPU cannot be used on the defending hacker’s next turn. If the defending computer has a *firewall(s)* installed on it, the defending player can choose to discard a number of these firewalls to gain a corresponding number of extra dice rolls.
  - The attacking hacker can spend up to the amount of CPU on any computers she owns that neighbor the defending computer to get a single die roll per CPU. Note that the amount of CPU the attacking hacker can spend cannot exceed the amount of CPU they have left for their turn. Whoever gets the higher total for all dice rolls wins the roll-off and gets the computer. If the defending hacker no longer has any computers, she is out of the game.

  If a hacker has gained a new computer on this turn, she can take a number of CPU beans equal to the amount of CPU on the computer she just acquired. These CPU beans may not be used until the next turn.

## 4 Turn cheat sheet

At the beginning of each round, remove any DDOS or Firewall tokens placed last turn.

Here's what you can do during a turn and how much CPU it costs:

- Research Exploit – Cost: Same as the amount you wish to research.
- Research Patch – Cost: Same as the amount you wish to research.
- DDOS Attack – Cost: Twice as much CPU as the target computer
- Install Rootkit – Cost: The amount of CPU on target computer + 2 CPU for every additional die roll.

  Rolls for successful install:

  - Completely protected computer: 6
  - Exploited computer: 6, 5
  - Zero-day exploited computer: 6, 5, 4

  Combat rules:

  1. Attacker chooses number of CPU used for die rolls (1 die roll/CPU, up to the number of computers flanking the defending computer).
  2. Defender chooses the number of CPU used for die rolls (1 die roll/CPU, up to the amount of CPU on the defending computer + extra die rolls if firewalls are discarded from defending computer.).
  3. Both hackers roll (if neither wants to roll first, defender rolls first)
  4. Hacker with higher total wins the computer