**Hacker-TCG Card List**

**Legend**:

(E): Execute (runs once).

(D): Daemon (continuous).

"text": flavor text

Note: None of these cards have been assigned Cycle Counts, Vulnerabilities, or Dependencies yet.

* **Cards**
  + **Hackers**
    - **Script Kitty**
      * Color: Black
      * Prof: Ubuntu, Windows
      * Special: All cards that require Perl, Python, or Ruby get their Cycle reduced by 1.
      * Objective: Infect the opponents computer or bring down 3 servers.
      * “Aww...say goodbye to your web server...hope it wasn’t important.”
    - **BOFH**
      * Color: Gray
      * Prof: BSD, Solaris, Unix
      * Special: All instant cards are shuffled back into your deck instead of being trashed.
      * Objective: Infect the opponent’s computer and deliver 75% of them via instants.
      * “There, you have more space now...I deleted your user directory. Hope that helps!”
    - **Anonymous**
      * Color: Gray
      * Prof: Ubuntu, Windows
      * Special: All cards with DDOS in their name last 4 times as long.
      * Objective: Deface the opponent’s computer or bring down their network 8 times.
      * “We are Anonymous, we are legion. We do not forgive, we do not forget. Expect us.”
  + **CPU Goddesses**
    - **Virtuous PC- Melon**
      * Architecture: x86\_64
      * CPU: 8GHz
      * RAM: 8GB
      * HDD: 7TB
      * SLT: 5
      * CONT: processes with largest CPU Cycle requirements are filled first.
    - **Discarded PC- Orphan**
      * Architecture: x86\_64
      * CPU: 4GHz
      * RAM: 6GB
      * HDD: 10TB
      * SLT: 2
      * CONT: each turn a card isn’t discarded; decrease CPU by 1GHz to a minimum of 4GHz.
      * COND: when a card is discarded, increase CPU by 1GHz up to a maximum of 10GHz.
    - Helper CPU- Cache
      * Architecture: x86\_64
      * CPU: 6GHz
      * RAM: 6GB
      * HDD: 5TB
      * SLT: 5
      * CONT: RAM slot 1 and 2 have reduced Cycle Count requirements.
  + **Packages**
    - libopenSSL-dev: anything that uses encryption or a secure socket uses this.
    - libpcap-dev: anything that is a network sniffer uses this.
    - libmysql-dev: for any software requiring persistence.
    - python-latest: for any software written in python.
    - ruby-latest: for any software written in ruby.
    - perl-latest: for any software written in perl.
  + **Software**
    - **White**
      * **Scanner**
        + tripwire(D)

INIT: play this card face down in an open RAM slot.

COND: when a card would attempt to affect your HDD, flip this card.

FLIP: capture card that triggered this flip.

* + - * + snort(D)

INIT: play this card face down in an open RAM slot.

COND: when a card would attempt to affect your network, flip this card.

FLIP: capture card that triggered this flip.

* + - * + honeypot(D)

INIT: play this card under a running program face down.

COND: when a card would attempt to install a rootkit over this program, flip this card.

FLIP: capture card that triggered this flip.

* + - * + chroot(D)

INIT: play this card under a running program.

COND: when a card would attempt to access your RAM field, flip this card.

CONT: prevent all future exploits from affecting this software.

* + - * + clam-av(D)

INIT: play this card face down in an open RAM slot.

COND: when a card would attempt to install malware, flip this card.

FLIP: capture card that triggered this flip.

CONT: remove one clock counter from each black card in your RAM field each time this program executes.

* + - * + san-guard(D)

INIT: play this card face down in an open RAM slot.

COND: when a card would attempt to affect your SAN, flip this card.

FLIP: capture card that triggered this flip.

* + - * + email-scanner(D)

INIT: play this card face down in an open RAM slot.

COND: when a card would attempt to install a Trojan via the SMTP protocol, flip this card.

FLIP: capture card that triggered this flip.

CONT: prevent future attacks by Trojan that was captured.

* + - * + metasploit(D)

EXE: patch 1 vulnerability. Cycle cost of this card is the number of running processes.

* + - * **Firewall**
        + iptables(D)

CONT: name a port number. All connections to/from that port are now disabled.

* + - * **Server**:
        + httpd(D)

CONT: patch one vulnerability every 10 turns. The vulnerability cannot be on this process.

"The community never lets me down!"

* + - * + ftpd(D)

CONT: +1 card during your draw phase.

* + - * + ldap(D)

CONT: any attempt to gain a core file will fail.

* + - * + vpn(D)

CONT: negate any ability preventing you from drawing except for total network outage.

* + - * + Local Repo(D)

CONT: put any number of cards from your deck on top of this card. The number of cards placed on this card is the Cycle Count requirement. Each turn you may draw an additional card from this pile. Also loss of network connectivity doesn’t affect this card.

* + - * **Tools**
        + ctrl-c(E)

EXE: kills process in RAM slot 1.

* + - * + kill -9(E)

EXE: kills a white process of your choice that you own.

* + - * + rm -rf(E)

EXE: discard a card from your hand or move one card from the top of your deck to the trashcan.

* + - * + grep(E)

EXE: search deck for one card of your choice.

* + - * + sed(E)

EXE: replace all cards in RAM Field with a given name with cards from your hand.

"The stream editor is a great tool...a shame so few knows how to use it."

* + - * + vim(E)

EXE: place this card under a running program to reduce its clock cycle time by one (E).

"Look at this mess, I can make it better!"

* + - * + fdisk(E)

EXE: discard your entire hand and draw a new one.

* + - * + Nuke and Pave(E)

EXE: discard all packages, all cards in hand, all processes on RAM field, and all captured cards.

"Use it only as a last resort."

* + - * + ifconfig eth0 down(E)

INST: skip your Draw Phase the next 3 turns, but cut all connections opponent currently has with your RAM field.

"Let’s see you get in now asshole."

* + - * + ssh(E)

EXE: discard one password token and do one for the following:

Take one of his running processes.

Take one random card from his hand.

Take one running process from his RAM Field.

* + - * + git(E)

EXE: draw a card. If the card drawn is git, then draw again. Continue until drawn card isn't git.

* + - * + thread-priority(E)

INIT: play under a running process.

CONT: on each tick, this process consumes one extra CPU Cycle and gets one additional Clock counter.

* + - **Black**
      * **Delivery**
        + stack-overflow(E)

Protocol: TCP

Port: \*

Exploits: SO

EXE: deliver a program card from your hand into your opponents RAM field over exploited process.

* + - * + Email- You've Won a Free iPad!(D)

Protocol: SMTP

Port: 25

INIT: play this card directly into opponents RAM field with a program card from your hand underneath it.

EXE: reveal and start running the process underneath this card and discard this card.

"Congratulations! You've won!"

* + - * + fomat-string-vulnerability(E)

Protocol: TCP

Port: \*

Exploits: FS

EXE: deliver a program card from your hand into your opponents RAM field over exploited process.

* + - * + Inconspicuous Flash Drive(E)

INST: target draws 2 cards. Deliver a program card from your hand into your opponents RAM field.

"Cool! It is labeled free software! I'll just plug it in and...wait...what?"

* + - * **Technique**
        + SQL Injection(E)

Protocol: HTTP

Port: 80

EXE: deliver a program card from your hand into your opponents RAM field.

* + - * + Social Engineering(E)

INST: gain one password token.

* + - * + Email- Nigerian Prince(E)

INST: search opponents deck for two upgrade card and discard them.

"You are the descendent of a Nigerian Prince...simply give us your bank account info and..."

* + - * + I'm Behind 7 Proxies(D)

EXE: the next black card you play cannot be captured.

COND: once this card’s effect has been used, trash it.

* + - * + Core Dump(E)

Exploits: SO

EXE: take exploited running process and capture it.

* + - * **Malware**
        + Blaster.Worm(D)

EXE: process replicates into one free RAM slot. Once all free slots are taken, it begins to overwrite used RAM slots.

* + - * + SARAH.EXE(D)

EXE: decrease HDD size by one.

COND: when HDD size is 2 or less, halt this program.

* + - * + Conflicker.Worm(D)

CONT: player of this process can reorganize your RAM field during your Main Phase.

* + - * + EyeSpy.Mal(D)

CONT: while this process is running, affected player must play with hand revealed.

* + - * + Erosion.Mal(D)

CONT: while this process is running, you must trash one card from top of your deck during Resolution Phase.

* + - * + Thrasher.Mal(D)

CONT: while this process is running, your CPU speed is reduced by half.

* + - * + Lil'\_Bastard.Mal(D)

EXE: your opponent gains one password token.

* + - * **Rootkit**
        + Basic Rootkit(D)

Protocol: TCP

Port: 1337

EXE: your opponent can play 1 card into your RAM field.

* + - * + Advanced Rootkit(D)

Protocol: TCP

Port: 1234

INIT: this card must be played on top of Basic Rootkit

EXE: your opponent can play up to 2 cards into your RAM field.

* + - * + Military-grade Rootkit(D)

Protocol: TCP

Port: 3457

INIT: this card must be played on top of Advanced Rootkit

EXE: your opponent can play up to 3 cards into your RAM field and shut down one running process.

* + - * + Cluster Kit(D)

Protocol: TCP

Port: 1001

CONT: while in play, the player of this card gains +1 RAM slot, and CPU cycles equal to the number of counters on it.

* + - * **Tool**:
        + DDOS- Low Orbit Ion Cannon(E)

Protocol: TCP

Port: \*

EXE: skip your opponents next turn. No processes owned by opponent will accumulate clock cycles this turn.

* + - * + John the Ripper(E)

EXE: take one captured card and discard it to gain two password tokens.