

CyberHack: A Card Game for Cybersecurity

Designed by Dr. Stylianos Karagiannis, PhD | Ionian University, Greece / PDM, Portugal



Description: CyberHack is a competitive card game where players simulate a cyber battlefield, managing networks, deploying services, and fending off attacks while strategically using resources like coins, logs, and port tokens. Players must balance building their defenses, launching attacks, and maintaining operational services on their hosts. Victory comes to the player who outlasts their opponents in this intense battle of strategy, resource management, and tactical planning.

Game Rules

Setup

Each player starts with: **10 Coins** (the game's primary resource ③).

- A hand of **7 cards**, drawn from their shuffled deck.
- A **Host Card**, which represents their network's central machine.

The maximum hand size is **9 cards**. If a player exceeds this limit, they must discard cards to stay within it.

Each deck contains a mix of **Host Cards**, **Service Cards**, **Attack Cards**, **Defense Cards**, and **Killchain Cards**.

Gameplay


1. **Rounds:** The game is played in rounds, with each player taking turns. During a turn, players can:
 - Deploy cards.
 - Use abilities.
 - Launch attacks or set up defenses.

At the end of each round, players replenish resources, update logs, and resolve card effects.

Coin Economy: Coins are used to Deploy cards.

- Change the deployment topology (4 coins per card, requiring 2 rounds to complete unless special abilities are used).
- Activate special abilities.
- Coins are earned by active **Service Cards**, which generate coins each round.

Host and Base Cards: Each **Host Card** can Deploy up to **2 Service Cards** or **2 Base Cards**.

- Deploy other **Base Cards**, which multiply the number of services the host can support ( indicates how many services a base card can host).
- If the **Host Card** has no services for 2 consecutive rounds, the player loses unless they perform a **System Reset**.

Defense Cards: Defense Cards are deployed **hidden** and are only revealed during an attack. After blocking or reducing

an attack, Defense Cards are hidden again, and their life is renewed at the start of the next round.

Each Defense Card has:

- **Effectiveness Threshold (ET) ②:** The maximum **Exploit Complexity (EC)** it can counter.
- **Defense Power (DP) ②:** Reduces incoming attack damage.

Attack Cards: Attack Cards deal damage to opponents' networks. Each Attack Card has:

- **Exploit Complexity (EC) ②:** Determines how difficult the attack is to counter.
- **Attack Power (AP) ⑥:** The amount of damage dealt.

If the EC of the attack exceeds the ET of the defender's Defense Card, the attack succeeds. The target service is damaged, and its operation is blocked for **X rounds**, where **X = AP - DP**.

Combo Cards (Killchain or Synergy Cards): Require specific card combinations to trigger powerful effects. **Port Tokens:** Used to activate certain **Attack Cards**. **Logs:** Generated by services or other cards, logs are used to trigger **special abilities**.

Card Lifecycle: Cards are discarded into a discard pile when used or destroyed.

- Once the deck is empty, the discard pile is reshuffled to form a new deck.
- Certain special cards are placed in the **Graveyard** and cannot be reused unless a specific ability is triggered.

Winning Conditions A player loses if their **Host** remains without active services or stops generating coins for **2 consecutive rounds**.

Mode 2: System Reset (Optional):

A player can perform a System Reset if their host is compromised: a) Restores their coins to **10** and redraws **7 cards**. b) Requires surrendering **all resources** or a **red/blue badge** (depending on the scenario). c) If after **5 rounds** post-reset, the player has fewer coins than any other player, they are **permanently defeated**.

Key Strategy Points: Players must focus on maintaining active services on their host, as they are the only way to generate coins and support other cards (attack/defense). Well-timed **attacks** can cripple an opponent's services, leaving them unable to recover or generate coins, leading to the losing condition. Ensuring that the host remains operational with services generating coins is vital. Without active services, the player's host will quickly fail.

CyberHack: A Card Game for Cybersecurity

Designed by Dr. Stylianos Karagiannis, PhD | Ionian University, Greece / PDM, Portugal



Case 1: Deployment/Setup Phase

Round 1: Setup Phase. Player A starts with a Host Machine card (capacity: 2 services, cost: 0 coins) and deploys the Apache Service card (cost: 4 coins, gain: 5 coins/round). With a starting balance of 10 coins, Player A spends 4 coins, leaving them with 6 coins. Player B, on the other hand, deploys a Virtual Machine card (capacity: 2 services, cost: 3 coins) and a DNS Service card (cost: 3 coins, gain: 4 coins/round). Player B begins with 10 coins, spends 6, and is left with 4 coins.

Round 2: Resource Generation and Expansion. Player A earns 5 coins from the Apache Service, bringing their balance to 11 coins. Player B earns 4 coins from the DNS Service, raising their balance to 8 coins. Player A then invests in a Firewall card (cost: 6 coins), which reduces incoming attack power by 50% for 3 turns and generates 1 log token per identified attack, leaving 5 coins. Player B deploys a MySQL Service card (cost: 5 coins, gain: 6 coins/round), leaving them with 3 coins.

Round 3: Attack and Defense. Both players generate resources again, with Player A accumulating 10 coins and Player B 13 coins. Player A launches the Nikto attack card (cost: 5 coins, requiring 2 port tokens) targeting Player B's DNS Service. Nikto's special ability, "Silent Auditor," bypasses defenses if no firewall is active, so the attack succeeds, temporarily disabling the DNS Service for 1 round. Player B spends 3 coins to deploy Nmap (generates 2 port tokens), preparing for a larger attack. This leaves Player B with 10 coins.

Case 2: Attack and Defense

Defense cards are equipped with Defense Power (DP), which is used to reduce or completely block incoming attacks, and an Effectiveness Threshold (ET), which determines their ability to counter specific attacks. On the other hand, attack cards possess Attack Power (AP) and Exploit Complexity (EC). If the Exploit Complexity (EC) of an attack exceeds the Effectiveness Threshold (ET) of the defense, the attack bypasses the defense mechanism entirely and inflicts damage equal to the Attack Power (AP). In cases where the defense partially blocks an attack, the residual damage does not cause direct destruction but temporarily disables services, impacting system functionality until mitigated or restored.

Scenario Setup. Player A, the defender, has a **Host Machine**, an **Apache Service** (5 coins/round), and a **Firewall** (reduces attack power by 50% for 3 turns). Player B, the attacker, has a **Virtual Machine**, a **MySQL**

Service (6 coins/round), **Nmap** (generating 2 port tokens), and an **Attack Card: Nikto** (cost: 5 coins, attack power: 8, requires 2 port tokens). **Attack Phase.** Player B launches **Nikto** targeting Player A's Apache Service. Nikto's special effect bypasses one defense layer if no IDS is active. Player A's Firewall reduces the attack power by 50%, reducing Nikto's power to 4. The Apache Service, which has a default health of 6, is reduced to 2 health. The Firewall generates 1 log token for detecting the attack. **Defense Phase.** Player A counters by showing the **Firewall**. If the $EC < ET$ then the firewall counters the attack. The attack that passes is $X = AP - DP$. Additionally, Player A shows a **Honeypot**, for additional DP if needed. **Outcome.** Player A's defenses are reinforced, with the Apache Service fully restored and the Honeypot in play to absorb future attacks. Player B has expended port tokens and coins but still poses a significant threat with active resources.

Case 3: Game Dynamics

Host Management and Resource Generation. The host card serves as the central base, requiring active services to remain functional. If a host is without services for 2 consecutive rounds, the player loses unless a System Reset is performed. System Reset sacrifices all resources but gives the player 10 coins and 7 cards, requiring them to surpass the opponent's coin total within 5 rounds to avoid defeat.

Attack and Defense Mechanics. Defense cards block or reduce attacks based on their Defense Power (DP) and Effectiveness Threshold (ET). If an attack's Exploit Complexity (EC) exceeds the defense's ET, it bypasses the defense and inflicts full damage. Partial blocks disable services temporarily, while combo cards enable advanced attack or defense strategies.

Case 4: Winning Conditions and Endgame

Round-by-Round Breakdown. In the final stages, Player A's inability to generate coins due to a disabled Web Server leads to a critical situation. With no active services for 2 consecutive rounds, Player A triggers the losing condition. Player B's consistent resource generation allows them to deploy additional services and attacks, overwhelming Player A's defenses.

Endgame Mechanics. Victory is achieved by either reducing the opponent's host to 0 services or coins for 2 consecutive rounds or accumulating more resources after a System Reset. Strategic deployment of services, defense cards, and calculated attacks is crucial for maintaining control and achieving victory.