Example Card

Attack Suit

You carry out a **[name]** attack on one target.

[attack description].

Target can choose to:

A.	[option]	S
B.	[option]	M
C.	[option]	F
D.	[option]	F

On Failure: [worse consequence]

On Mitigation: [consequence]

OFFENSE

Tampering

You carry out a **Web Parameter Tampering** attack on one target.

> You manipulate the parameters in hidden field in HTML to bypass the logic validation of the victim server.

Target can choose to:

A.	Encrypt the input and channel.	F
B.	Add a variable for integrity checking.	M
C.	Filter all input field.	S
D.	Authenticate users at every stage.	F

On Failure: target –1 credit , you +1 credit.

On Mitigation: target –1 credit.

OFFENSE

Tampering

You carry out a **Buffer Overflow** attack on one target.

> You write data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

Target can choose to:

A.	Use safe programming language.	M
B.	Escape from certain characters.	F
C.	Check that the stack is not altered when a function returns.	S
D.	Clean the buffer periodically.	F

On Failure: target –1 credit, you +1 credit.

On Mitigation: target –1 credit.

OFFENSE

Spoofing

You carry out a **DNS spoofing** attack on one target.

> You spoof the IP address DNS entries for a target website and replace them with a server which holds malicious content.

Target can choose to:

A. Change the web browser. F

B. Apply source port randomization for DNS requests. S

C. Perform end-to-end validation once a connection is established. M

D. Ignore irrelevant DNS requests. F

On Failure: target –1 credit, you +1 credit.

On Mitigation: you +1 credit.

OFFENSE

Spoofing

You carry out a **Session Hijacking** attack on one target.

> You manage to predict a valid session token to gain unauthorized access to the web server of the victim.

Target can choose to:

A. Double check the cookie. F

B. Encrypt all the traffic data. F

C. Regenerate the session id after a successful login. M

D. Use a long random session key. S

On Failure: target –1 credit, you +1 credit.

On Mitigation: you +1 credit.

OFFENSE

Spoofing

You carry out a **Cross-site Request Forgery (CSRF)** attack on one target.

> You force the victim to execute unwanted actions on a web application in which he/she currently authenticated.

Target can choose to:

A. Double check the cookie. F

B. Use a a secure random token. S

C. Disallow browsers to save passwords. F

D. Require more user interaction for a request. M

On Failure: target –1 credit, you +1 credit.

On Mitigation: you +1 credit.

OFFENSE

Denial of Service

You carry out a **SYN flooding** attack on one tar-

> You send TCP packets with set SYN flag and with constantly changing source ports on open ports of its victim.

Target can choose to:

A.	Contact the ISP provider.	F
B.	Automatically blacklist IP addresses.	F
C.	Limit the number of half-open connections.	S
D.	Buy a content delivery network.	M

On Failure: target –2 credit.

On Mitigation: target –1 credit.

OFFENSE

Denial of Service

You carry out a **DNS amplification DDOS** attack on one target.

> You send requests to open DNS servers who then respond by sending even greater volumes of traffic to the victim.

Target can choose to:

A. Stop trusting the DNS server. F

B. Drop artificial packets trying to flood systems. S

C. Automatically blacklist IP addresses. F

D. Host a back-up server. M

On Failure: target –2 credit.

On Mitigation: target –1 credit.

OFFENSE

Information Disclosure

You carry out a **Man-in-the-middle (MITM)** attack on 1-2 target.

> You make independent connections with the victims, secretly relay and alter the messages between them.

Target can choose to:

A. Check for discrepancies in response M

B. Authenticate endpoints of a network connection. S

C. Periodically change private key. F

D. Use a better encryption algorithm. F

On Failure: target –1 credit and reveal all deployed Defensive cards.

On Mitigation: target –1 credit.

OFFENSE

Information Disclosure

You carry out a **Social Engineering** attack on one target.

> You phish the administrator of your victim’s server to enter sensitive information at a fake website.

Target can choose to:

A. Check messages from outer sources. F

B. Make browser alert the user to fraudulent websites. M

C. Authenticate the users each time. F

D. Add more authentication methods S

On Failure: target –1 credit and reveal all deployed Defensive cards.

On Mitigation: target –1 credit.

OFFENSE

Repudiation

You carry out a **Log Injection** attack on one target.

> You inject unexpected characters into the victim’s log files, making them corrupt to cover your tracks.

Target can choose to:

A. Validate all the output. M

B. Log to a database instead of files. M

C. Encode all the output. S

D. Limit user access to the log files. F

On Failure: You immediately gain an extra turn.

On Mitigation: target –1 credit.

OFFENSE

Elevation of Privilege

You carry out a **Dictionary Attack** on one target.

> You pre-compute a rainbow table to determine the password and defeat the authentication system of the victim.

Target can choose to:

A. Add salt when hashing passwords. M

B. Make passwords hard to guess. F

C. Authenticate the user each time. F

D. Limit the number of login attempts. S

On Failure: target –1 credit, you draw 1 card.

On Mitigation: target –1 credit.

OFFENSE

Elevation of Privilege

You carry out a **Cross Site Scripting (XSS)** attack on one target.

> You insert malicious code into the victim’s website, causing all users to execute your script.

Target can choose to:

A. Redirect the web pages. F

B. Encode any untrusted input. M

C. Authenticate the user for each re- F

D. Check the input and escape from cer- S

On Failure: target –1 credit, you draw 1 card.

On Mitigation: target –1 credit.

OFFENSE

Elevation of Privilege

You carry out a **SQL injection** attack on one target.

You exploit a security vulnerability in target’s system and insert a SQL statement into an entry field for execution.

Target can choose to:

A. Use Parameterized statements only. S

B. Check user’s authority for each input. F

C. Limit the executable space for all soft- F

D. Limit the database login permissions. M

On Failure: target –1 credit, you draw 1 card.

On Mitigation: target –1 credit.

SERVICE

You write a simple BBS website by yourself and profit from it.

Instant effect:

Your credit +1.

After deployed:

Each round, your credit +1.

Whenever you are attacked, your credit –1.

SERVICE

You rent a web server that provides online service on 24/7, using port 80.

Instant effect:

Your credit –2.

After deployed:

Each round, your credit +1.

If you FAIL on any attack, this card is destroyed.

SERVICE

You dig big data from the internet and analyze it.

Instant effect:

None.

After deployed:

At the beginning of each round, you can choose to reveal 1 hidden card on the desk.

If you did not reveal any card, you gain 1 credit.

SERVICE

You own a BotNet which can be used to perform Denial of Service attacks.

Instant effect:

Your credit –1.

After deployed:

When your turn begins, you can pick one player to lose 1 credit.

SERVICE

You develop an online webpage game to earn some quick money.

Instant effect:

None.

After deployed:

Each round, your credit +1.

This card is wasted after 3 turns.

SERVICE

You gain access to the deep web and sell cyber vulnerabilities.

Instant effect:

None.

After deployed:

Each time you attack, your credit +1.

SERVICE

You rent a second server, which allows you to run multiple tasks.

Instant effect:

Your credit –2.

After deployed:

You can play 2 Offensive cards at your turn.

You have 1 extra slot to deploy Service or Defensive card.

DEFENSE

You upgrade all your software, including the firewall.

Instant effect:

Your credit –1.

After deployed:

Each time you are targeted, one Fail option is automatically removed (at attacker’s choice).

This card is revealed after use.

DEFENSE

You buy a content delivery network (CDN) to prevent Denial of Service attacks.

Instant effect:

Your credit –1.

After deployed:

You are immune to Denial of service attacks.

This card is revealed after use.

DEFENSE

You have invented a new algorithm to encrypt data.

Instant effect:

Your credit –1.

After deployed:

You are immune to Information Disclosure attacks.

This card is revealed after use.

DEFENSE

You own a DNS server and become less trusting of other DNS servers.

Instant effect:

Your credit –1.

After deployed:

You are immune to Spoofing attack.

This card is revealed after use.

DEFENSE

You deployed the Supervisor Mode Execution Prevention (SMEP), a strategic mitigation to common EoP exploits.

Instant effect:

None.

After deployed:

You automatically mitigate Elevation of Privilege attacks.

This card is revealed after use.

DEFENSE

You buy a back-up server.

Instant effect:

Your credit –2.

After deployed:

Each time you are attacked, you can use this card to avoid the consequence.

This card is destroyed after use.

DEFENSE

You have several back-ups and can rollback the system status at any time.

Instant effect:

Your credit –1.

After deployed:

Each time you are attacked, you can use this card to mitigate the consequence.

This card is destroyed after use.

RANDOM EVENTS

The government decided to tax more on online services.

Each player must:

-1 credit for each Service card deployed on the server.

Events cannot make player’s credit lower than 2.

RANDOM EVENTS

Due to the support from new government policies, new internet technologies emerge in an endless stream.

Each player must:

Draw 1 card, if it is not an offensive card, draw another one.

RANDOM EVENTS

A large company starts an extensive acquisition for internet technologies.

Each player can:

Discard up to 3 cards in hand. +2 credit for the first card, and +1 for next ones.

Player cannot discard his/her last in-hand card.

RANDOM EVENTS

A large cyber security activity is held on this day.

You are encouraged to hack each other.

Each player can:

Play 1 Offensive card instantly.

RANDOM EVENTS

A new server operating system is released to the market.

Each player can:

Pay 1 credit to gain 1 extra slot for Service card only.

Events cannot make player’s credit lower than 2.

RANDOM EVENTS

As IPv6 replaced IPv4, some of the old technologies retired.

Each player can:

Discard 1 card in hand of his/her choice and then draw 1 card.

RANDOM EVENTS

Secure DNS (DNSSEC) is implemented at all stages of the DNS protocol , preventing all DNS attack.

Each player must:

Discard all the Offensive cards on hand that includes “DNS”.

Player cannot discard his/her last in-hand card.

RANDOM EVENTS

Lightening strikes the main power supply station and causes a power failure.

Each player must:

Discard 1 deployed Defense or Service card at his/her choice.

If no such card, discard 1 Defense or Service card in hand, at his/her choice.

Player cannot discard his/her last in-hand card.

RANDOM EVENTS

Stock market are volatile due to an unknown reason.

Instant effect:

Until the beginning of your next turn, all the credit changes are doubled.

RANDOM EVENTS

The stock market rise sharply.

You can:

Pick a number from 1 to 3. All players lose credits according to this number.

Events cannot make player's credit lower than 2.

RANDOM EVENTS

Information leakage happens everyday, everywhere.

Each player must:

Give X cards in your hand to the player left to you. X equals to the minimum number of in-hand cards among all players.

RANDOM EVENTS

Several computer viruses are leaked from security database. An agency is looking into this event.

instant effect:

Until the beginning of your next turn, all the Offensive cards will cost 1 credit to play but the victim also lose 1 more credit.

RANDOM EVENTS

A new type of computer is invented. Cyber security technologies need to start over.

Instant effect:

All used cards on desk are brought back to the deck and shuffled.