Backdoors & Breaches™

An Incident Response Card Game from Black Hills Information Security and Active Countermeasures that helps you conduct information security tabletop exercises and roleplay various attack tactics, tools, and methods.

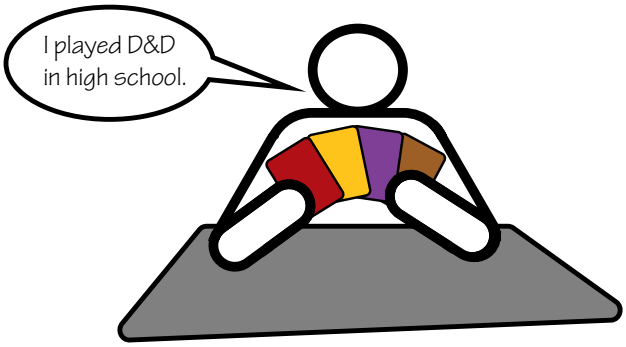
YOU NEED:

- At least 2 people
- 1 set of Backdoors & Breaches playing cards
- 1 d20 (i.e., a 20-sided die) 

If a physical d20 isn't available, we suggest using Google's digital dice rolling.

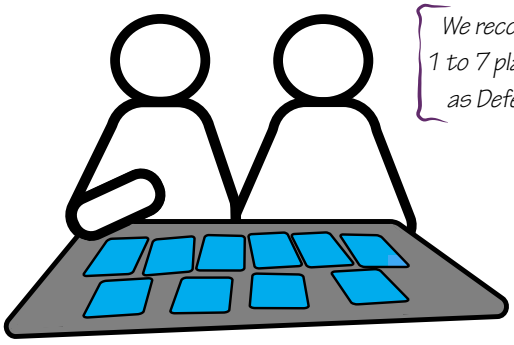
ROLES:

INCIDENT MASTER



This role should initially be assigned to the player with the most cybersecurity knowledge. Their job is to develop a narrative and keep gameplay moving.

DEFENDERS



We recommend 1 to 7 players act as Defenders.

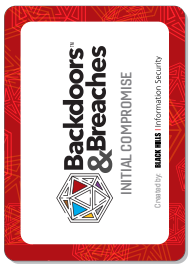
This role is assigned to the remaining players. Their job is to reveal the attack cards before 10 turns have elapsed.

GOAL:

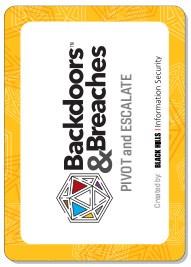
Basically, the Incident Master creates a situation based on their attack cards and guides the gameplay. The Defenders roll the d20 each turn to run various procedures in an attempt to reveal the situation. If the Defenders reveal the entirety of the situation within 10 turns, they win. If not, they lose.

SET UP:

Shuffle each deck (as designated by name and color) **INDIVIDUALLY**. Don't shuffle the WHOLE deck together!

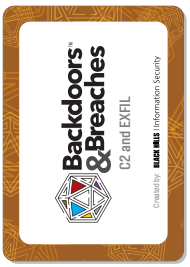


(RED)

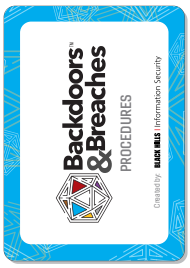


(YELLOW)

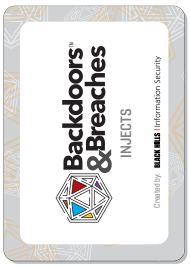
(PURPLE)



(BROWN)



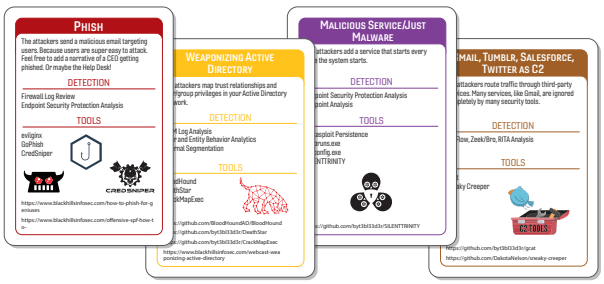
(BLUE)



(GREY)

Without revealing their cards, the Incident Master draws 1 card each from the **INITIAL COMPROMISE**, **PIVOT and ESCALATE**, **PERSISTENCE**, and **C2 and EXFIL** decks. These are the attack cards.

INCIDENT MASTER EXAMPLE:

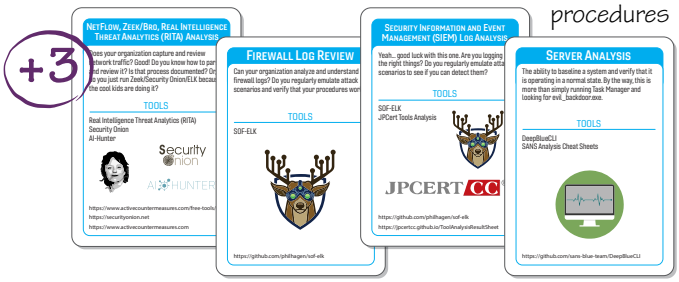


As a collective, the Defenders are randomly dealt 4 **PROCEDURES** cards, and these are laid out face up on the playing surface. These represent the written procedures in your organization. The Defenders are also given the remaining **PROCEDURES** cards, which are laid out face up in a row separated from the initial 4.

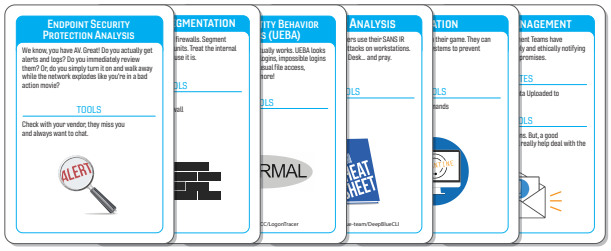
Players will notice example tools and instructional blog posts are listed on each card. These are to help players learn about/practice any procedures and attacks they are unfamiliar with.

DEFENDER EXAMPLE:

4 randomly drawn written procedures



Remaining cards (no bonus)



BLACK HILLS Information Security

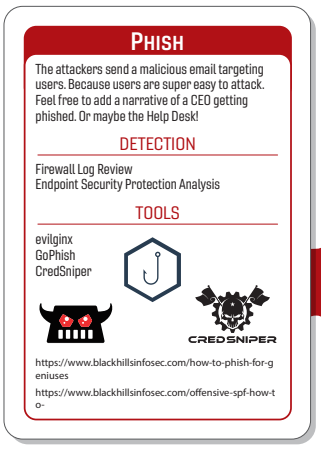
2 Backdoors & Breaches

GAMEPLAY:

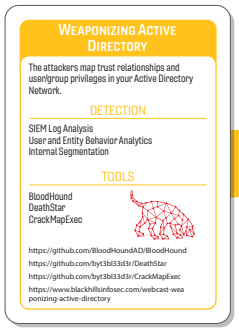
Now that everyone has their cards...

1st, the Incident Master must construct a narrative surrounding their attack cards. This narrative should give the Defenders enough context to start investigating without revealing any of the attack cards.

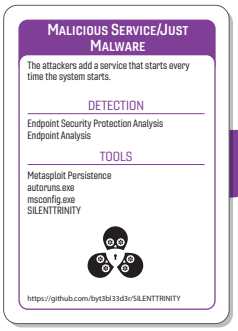
The initial narrative provided to the Defenders should be primarily based on the description of the INITIAL COMPROMISE card.



*How the attackers **enter** the organization.*



*How the attackers **gain privileges** once inside the organization.*



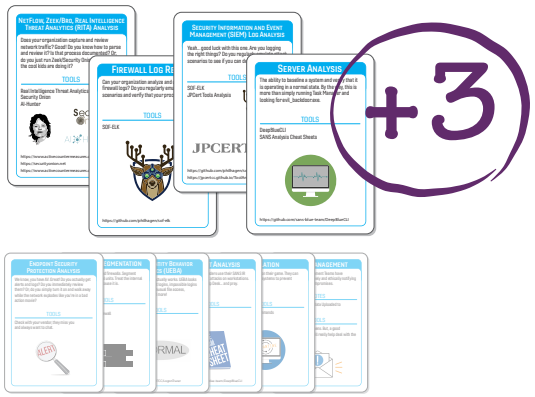
*How the attackers are able to **re-enter** the organization.*

*How the attackers **communicate** with the organization from the outside.*

EXAMPLE:

Perhaps Dahlia starts noticing strange pop-ups on her computer after downloading new software, or maybe Xavier receives a notification from his Anti-Virus program.

2nd, the Defenders will select a PROCEDURES card they decide is logical based on the narrative given by the Incident Master. To determine success, they will roll their d20. A successful roll is between **11 and 20**. An unsuccessful roll is between **1 and 10**.



However, if the PROCEDURES card chosen is from the initial 4 cards, it receives a **+3 modifier**, meaning 3 will be added to the value of the roll.

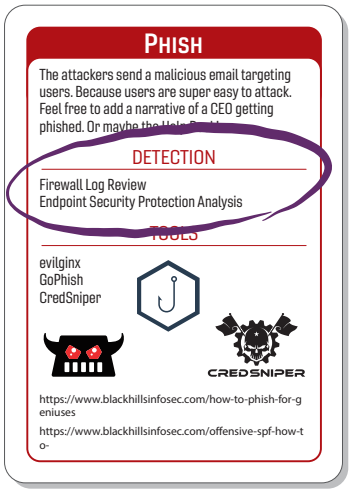
EXAMPLE:

Even if you roll an 8 while attempting 1 of the initial 4 PROCEDURES, the roll is still successful.

+ 3 = 11

BLACK HILLS Information Security

3 Backdoors & Breaches

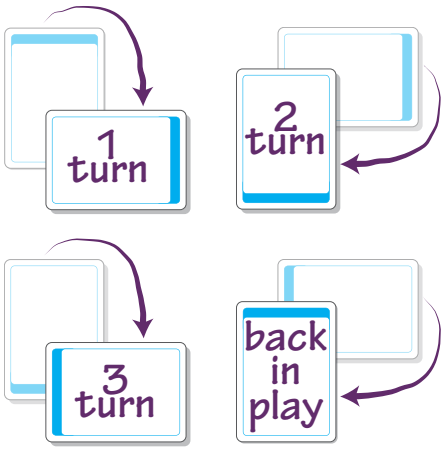


If the roll is successful, the Incident Master will use the listed detections on the front of each attack card to determine if the Defenders detected any of the attacks. If so, the Incident Master will reveal that card.

If more than one card COULD be detected by the procedure, the Incident Master will choose **only 1** attack card to reveal.

If the roll is successful, but the procedure does not reveal any attack cards, the Incident Master will explain why it failed to detect any attacks.

EXAMPLE:
Maybe the computer was off, or the procedure was not calibrated correctly...



If the roll is unsuccessful, the attempted PROCEDURES card can be played again in **3 turns**. (Rotate the card to keep track) The Incident Master will still provide an explanation for failure.

Successful PROCEDURES can be played again without waiting.

This process repeats until either the Defenders have revealed all the attack cards (in which case they win), or the Defenders use all 10 turns without revealing all 4 attack cards (in which case they lose).

x10

OTHER RULES:

When the Defenders roll a 1, a natural 20 (meaning without any modifiers), or roll unsuccessfully 3 times in a row, an INJECT card is drawn by the Incident Master and shared with the Defenders.

INJECT cards add chaos to the game and facilitate conversation. Sometimes they reveal a card, sometimes they do not affect the game, sometimes they end the game.

Remember, this game is a teaching tool and the rules are flexible. You can add modifiers to any PROCEDURES card you want or add attacks and actions not included on the cards. (Perhaps your organization has a great Network Team and you feel the Isolation card deserves a +5 or you have a really inportant procedure not included in the deck.) Adapt the game to best suit you.

HAVE FUN!