Backdoors & Breaches Visual Guide

2+ players

30-60 minutes

Created by Black Hills Information Security and Antisyphon Training

Backdoors & Breaches is a cooperative, cybersecurity threat emulation game in which "Defenders" will work together to uncover the attack pathways used to hack into their environment. Taking the concept of traditional tabletop exercises, Backdoors & Breaches combines the structure of a card game with the flair of classic role-playing games to help organizations and individuals learn about the tactics, methods, and tools used in cyber attacks and defense.

Backdoors & Breaches provides a reason to consider attacks, discuss procedures, and strategize solutions BEFORE they happen in your environment... while having fun!

Contents:

Among the 52 unique playing cards* in your Backdoors & Breaches: Core Deck, you will find:

Attacks

INITIAL COMPROMISE (red), PIVOT and ESCALATE (yellow), C2 and EXFIL (brown), and PERSISTENCE (purple) cards

Procedures

PROCEDURE cards (blue)

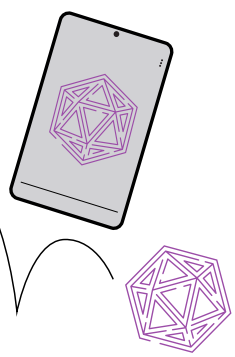
Injects

INJECT cards (grey)

Psssst, hey! Expansion Decks with additional attacks, procedures, and inject cards are available to enhance gameplay.

You will also need:

A crew of 2 or more (ideal number of players is 5-7)
A d20 (20-sided die) OR a virtual dice-rolling app
A healthy dose of imagination!



Getting Started

Overview

Using a secret array of 4 Attack cards, the "Incident Captain" will craft an imagined security breach and guide the "Defenders" through the scenario. Equipped with critical thinking, dice, and PROCEDURES, the Defenders will attempt to discover what the attackers are doing before it's too late!

The gameplay of Backdoors & Breaches is cooperative. You either win as a team, or you lose as a team.

Objective

To win, the Defenders must reveal all 4 Attack cards before 10 turns have passed. Otherwise, they have failed to uncover the various avenues of the attack, and they lose!

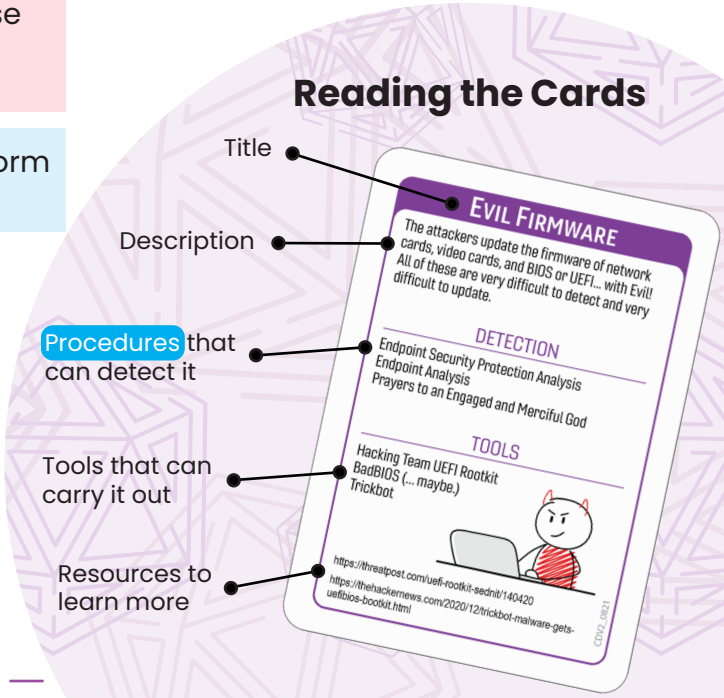
Determining Roles

Before you start, you must determine roles for each player: Incident Captain or Defender.

Choose 1 person to serve as the Incident Captain. This person will be responsible for crafting the starting scenario, answering questions, improvising situations, and is overall in charge of guiding the game process. Whoever you choose should have a wide breadth of cybersecurity knowledge and be a quick thinker.

All other players will serve as Defenders. They form the team responding to the incident at hand.

Reading the Cards



Setup

Sorting the Cards

Once roles are decided, it's time to set up the cards.

Separate the deck into 6 piles sorted by color, and shuffle each pile individually.

Incident Captain Setup — Attacks

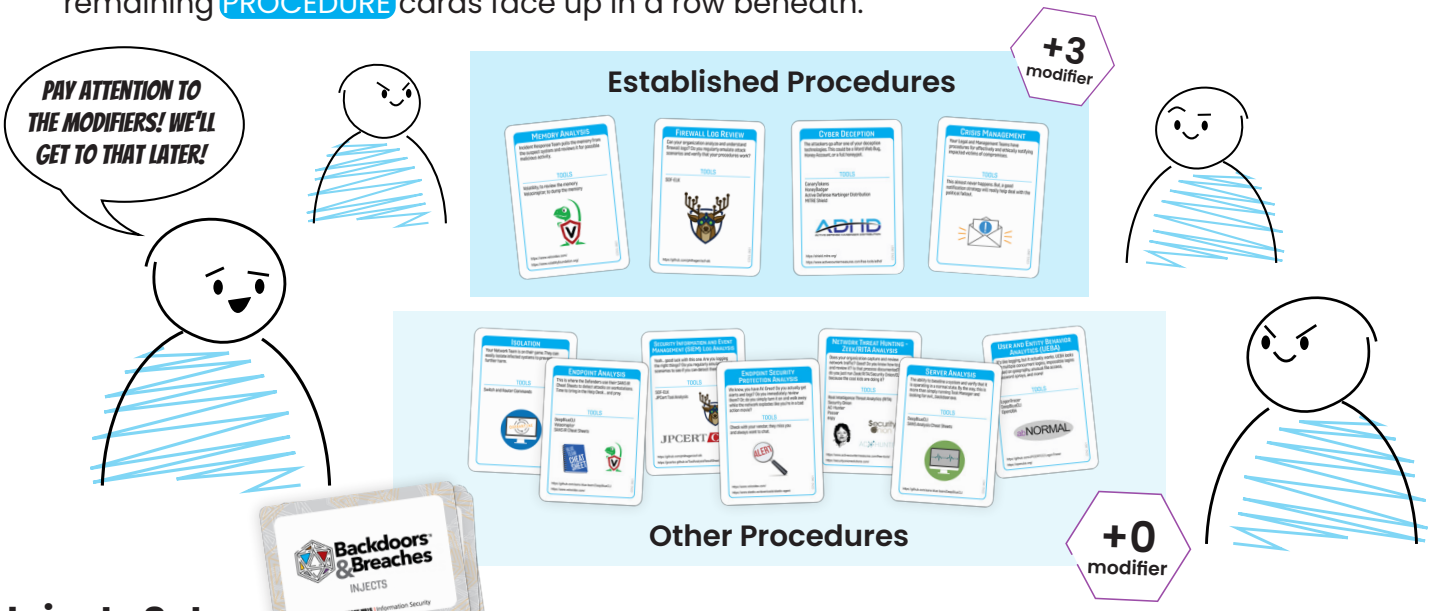
The Incident Captain chooses 1 card from each Attack card pile (INITIAL COMPROMISE, PIVOT and ESCALATE, C2 and EXFIL, PERSISTENCE) and keeps those cards hidden from the Defenders! More advanced players may want to draw the cards randomly for an added challenge.

[Once the Incident Captain has all 4 Attack cards, you will not need the rest of the Attack card piles for the remainder of the game.]

Defenders Setup - Procedures

You will now deal the PROCEDURE cards into 2 rows: Established Procedures and Other Procedures.

For Established Procedures, deal 4 random cards face up. For Other Procedures, place all remaining PROCEDURE cards face up in a row beneath.



Injects Setup

Place the INJECTS pile to the side of your play area, face down.

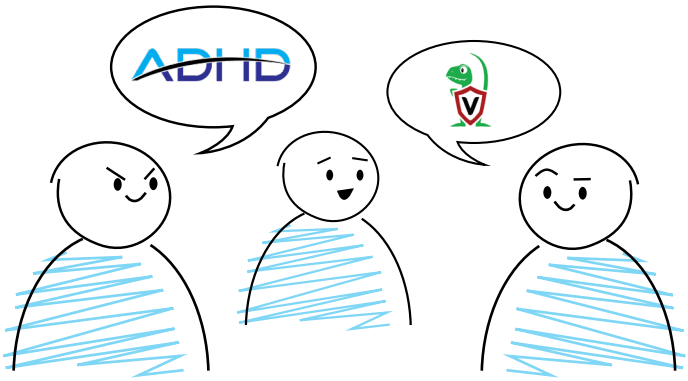
Playing the Game

Playing The Game

To begin, the Incident Captain must set the stage by crafting a breach scenario based on the 4 Attack cards. This should be detailed enough to give the Defenders a place to start, without giving away the specifics of any Attack cards.

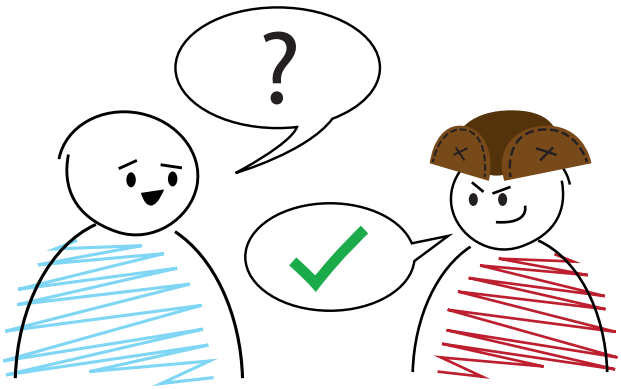
[Incident Captain Tip: It is usually easiest to build the scenario from the INITIAL COMPROMISE card. Check out the example gameplay at the end of this guide!]

Sequence of Play



1. Discussion

The Defenders should discuss the current situation amongst themselves and decide which of the PROCEDURES they should attempt to use.



*[**Defenders Tip:** The Defenders can seek clarity from the Incident Captain during this phase. They may ask the Incident Captain to expand on details that would make sense for them to know. This does not require any dice rolls. It is up to the Incident Captain to decide whether or not the Defenders would have access to the information they are seeking clarity on.]*

2. Decision

Once the Defenders have reached a consensus, they declare which PROCEDURE they will be attempting, and roll the d20. You may only play 1 PROCEDURE per turn.

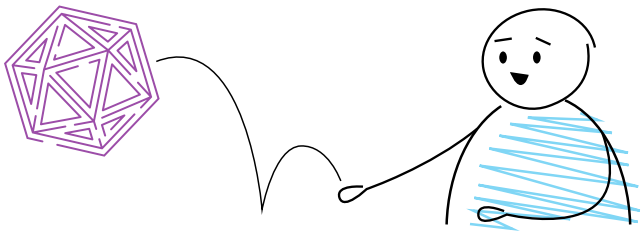
Established Procedures (top row) add a **+3 modifier** to the dice roll when they are played. These have an advantage as they indicate procedures that your team is very experienced with.

Other Procedures (bottom row) **do not receive any modifiers.**

3. Rolling

When the Defenders wish to play a PROCEDURE card, they must roll the die to determine if the PROCEDURE is successful or if it fails to detect an attack.

Failure	**1–10**
Success	**11–20**



Remember to add any relevant modifiers to the roll!

A roll of either a natural 1 or natural 20 (indicating the number on the die face before any modifiers are added) or 3 failures in a row will trigger an INJECT!

If an INJECT is triggered: Draw 1 card from the top of the INJECT pile and reveal it to all players. Follow any instructions that may be on the card, and have the Defenders discuss how (or if) this INJECT will affect their investigation.

INJECTS simulate the random events that can happen during a security incident. They add a bit of chaos to the scenario and spur important conversations. Some might not affect the game at all... or might end it. Either way, they're always unexpected.

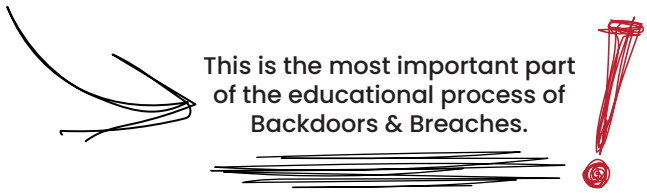
4. Outcome

On a failure, nothing new is learned and the turn ends.

On a success, the Incident Captain checks if the PROCEDURE played is listed under "Detection" on any of the Attack cards. If it is, they reveal that card to the Defenders. If the PROCEDURE could detect multiple Attack cards, it is up to the Incident Captain to choose only one card to reveal. (As in real life, when doing incident response, you find one thing at a time, not everything all at once.)

After a PROCEDURE has been played, regardless of outcome, that card will have a 3-turn cooldown period during which it cannot be used again.

*[**Incident Captain Tip:** If a PROCEDURE is unsuccessful, ask the Defenders for a reason — whether financial, political, personnel-wise, or technological — why the PROCEDURE would not be successful at that time.]*



Ending the Game

The turn cycle repeats until whichever comes first:

The Defenders have revealed all 4 Attack cards

OR

10 turns have passed

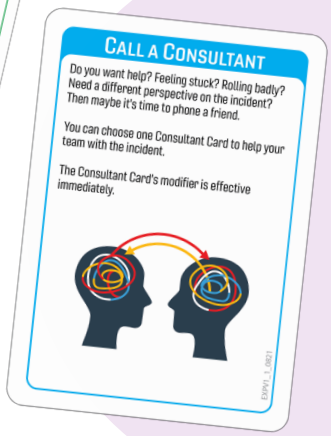
Additional Considerations

Breaking the Rules

As is the spirit of any classic tabletop RPG — the "rules" are merely suggestions! Feel free to modify and adapt gameplay in whatever way fits your team's needs.

For example, with the Established Procedures: pre-select cards to mirror your own runbook, have more than 4, and/or give yourself additional modifiers to reflect your team's strengths!

CONSULTANTS



CONSULTANTS are a type of card first introduced in the Backdoors & Breaches Expansion Deck. CONSULTANTS each provide a unique modifier or ability. These modifiers or abilities will either have a limited time use or remain in play for the rest of the session, depending on the text of each card.

To use a CONSULTANT, Defenders must play the "Call a Consultant" PROCEDURE card (found in the Expansion Deck). This card follows the same rules as any other PROCEDURE.

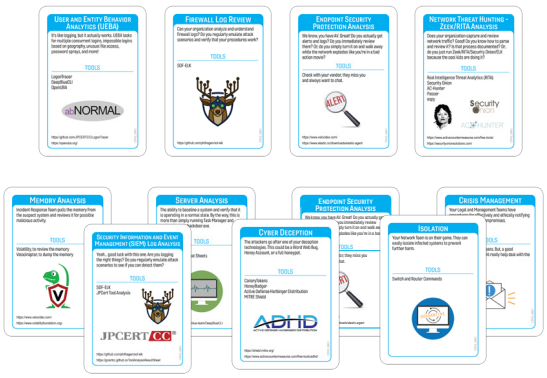
When "Call a Consultant" is successful, the Defenders team may choose any CONSULTANT card from their collection and immediately bring it into play. On repeat successes of the "Call a Consultant" PROCEDURE, Defenders may choose to bring in either a new CONSULTANT or one that they have previously played.

Example Gameplay

Welcome, Defenders. We believe our company was compromised. We need your help to discover how.

After the starting setup is done, the Incident Captain draws 4 Attack cards and looks at them privately.

Defenders also draw their 4 Established PROCEDURES, with the rest arranged below.



This morning, the SOC got a call from IT about some strange emails. Sarah, from sales, also mentioned during their daily team meeting that when she logged in, a black box flashed on her screen really fast before disappearing.

The Defenders consider their PROCEDURES and discuss the situation with the currently available information.

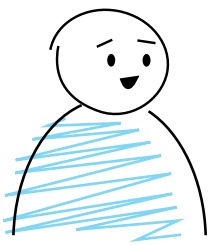
"Strange emails could be a phishing campaign. I think we should check the firewall logs and see if we can learn more about the attack."

The other Defenders agree, so they decide to use the FIREWALL LOG REVIEW PROCEDURE and they roll a d20. The result of the roll is an 8, but because the Defenders used an Established Procedure, they add +3 to the roll, for a total of 11.

11 is a successful roll... barely. Upon your in-depth FIREWALL LOG REVIEW, you are able to confirm the INITIAL COMPROMISE at work here is PHISHING. Well done, Defenders!

The Incident Captain then flips over the INITIAL COMPROMISE card.

Until we know more, it might make sense to do some CRISIS MANAGEMENT and notify stakeholders immediately.



The Defenders consider this and decide to declare one of their Other PROCEDURES. They roll their d20, and this time, the result is a 10.

Unfortunately, 10 isn't enough for a success here, team. We floated the idea of CRISIS MANAGEMENT with leadership and it's a no-go until we actually know what's going on. Any other ideas?

The black box Sarah mentioned is an interesting detail. Could be some kind of script or batch file running. Let's check our ENDPOINT SECURITY PROTECTION ANALYSIS.

The Defenders roll their d20 to attempt ENDPOINT SECURITY PROTECTION ANALYSIS. This time, they roll a natural 20 and easily succeed!

Boom! Good call, Defenders! You discovered how the attackers maintained PERSISTENCE in our systems: LOGON SCRIPTS.

The Incident Captain flips over the PERSISTENCE card. They then also draw and reveal an INJECT card, which the Defenders triggered by rolling a natural 20.

Alright, folks. I have some good news and bad news. The bad news is your investigation is over. The good news is the INJECT shows that you learned IT WAS A PENTEST, which effectively ends this incident response!

The Incident Captain flips over the rest of the Attack cards, showing the full chain.

Looks like we got ourselves a PENTEST. The testers sent out PHISHING emails that were clicked on by 3 users, which gave them access to those computers. Using stolen login credentials obtained from a hacked website, they conducted an INTERNAL PASSWORD SPRAY which allowed them to move deeper into the network. They also set up LOGON SCRIPTS to make sure they could get back in if they were discovered. Good thing our SOC team was already looking for unusual connections to the internet, because that led us to discover the penetration testers were using HTTPS AS EXFIL as part of their test.

The Defenders did a great job in this sample scenario.

Now, let's see what YOUR team can do!

Check out
https://backdoorsandbreaches.com
for more information, including videos of real gameplay!