Backdoors and Breaches: Taggart Institute Rules/FAQ

So, you wanna play Backdoors and Breaches? Awesome! I'm so glad you decided to join us. I put this doc together as some prior reading so newcomers could have a reference to how we play the game.

FAQ

What *is* Backdoors and Breaches?

BnB is a tabletop incident response simulator created by Black Hills Information Security. Its intent is to simulate how the defenders ("blue team") of an organization would detect, investigate, and remediate attacks by malicious actors. Using a set of cards to represent defensive and offensive techniques, players are tasked with revealing the steps of a compromise, from initial access to persistence and data exfiltration—a set of steps known as the "kill chain."

When do we play?

When we can!

The game is hosted on the Taggart Institute Discord. If you'd like to play, watch for game announcements in the #announcements channel.

I'm a n00b. Can I just listen/watch?

First, we're all n00bs. If you want to participate but are worried about asking silly questions, please know that we welcome *all* participants. This is a learning space for people of all skill levels. Anti-gatekeeping and inclusion are core values of our community. If you don't feel comfortable speaking up, consider asking questions in the text chat. But of course, you're welcome to just listen and learn as well. This space is for you to learn, so use it how you feel comfortable.

Are Games Recorded?

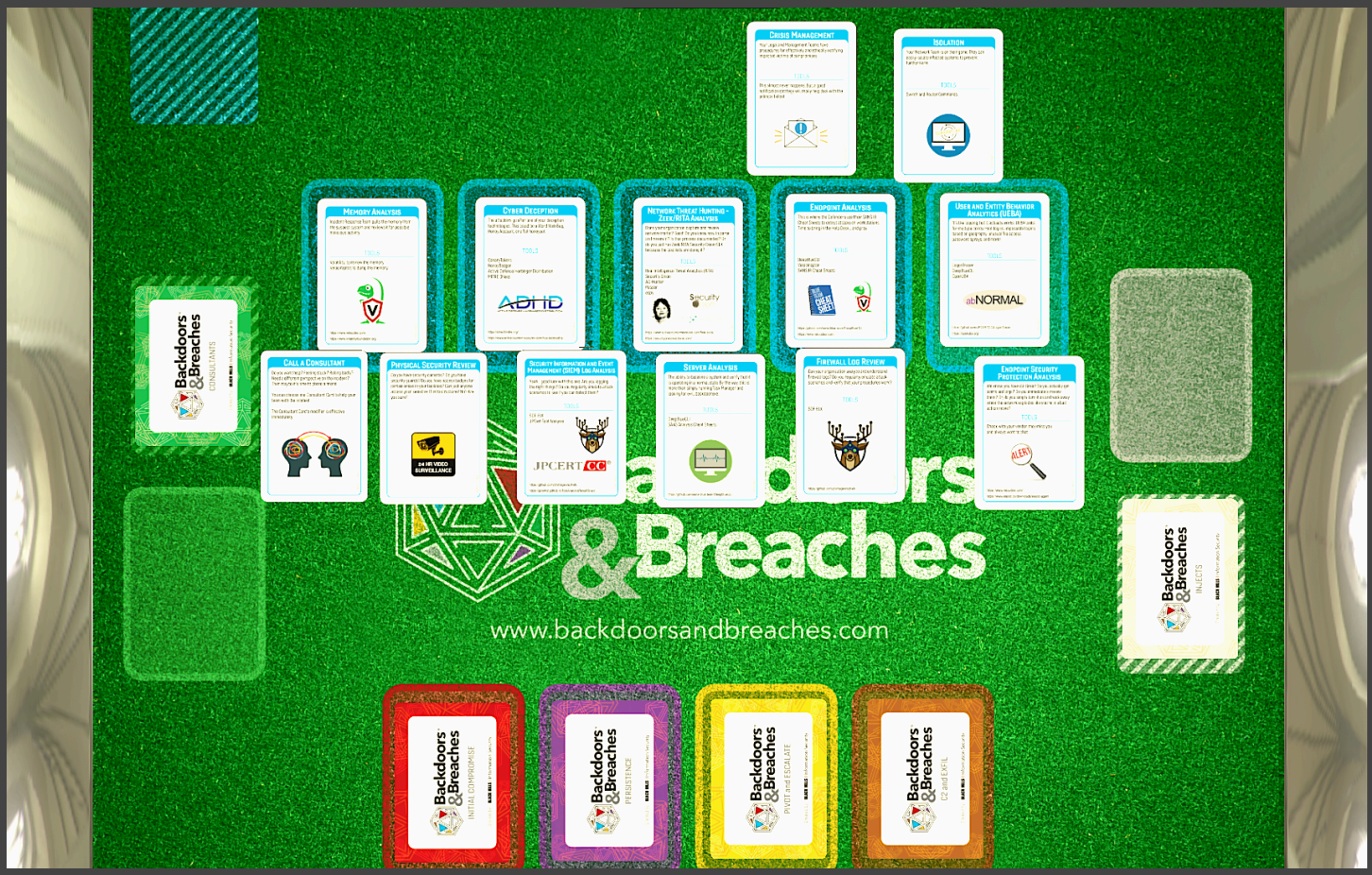
Although they'd be amazing content and useful for all, **we do not record** games. We want this to be a safe learning environment for all, and not everyone is comfortable being recorded. Also, given the

nature of how we play, it's possible folks may disclose sensitive info about their experiences. Best to keep that in the session.

How We Play

We take the core ruleset of BnB and add a little flavor of our own. Let's go over the basics.

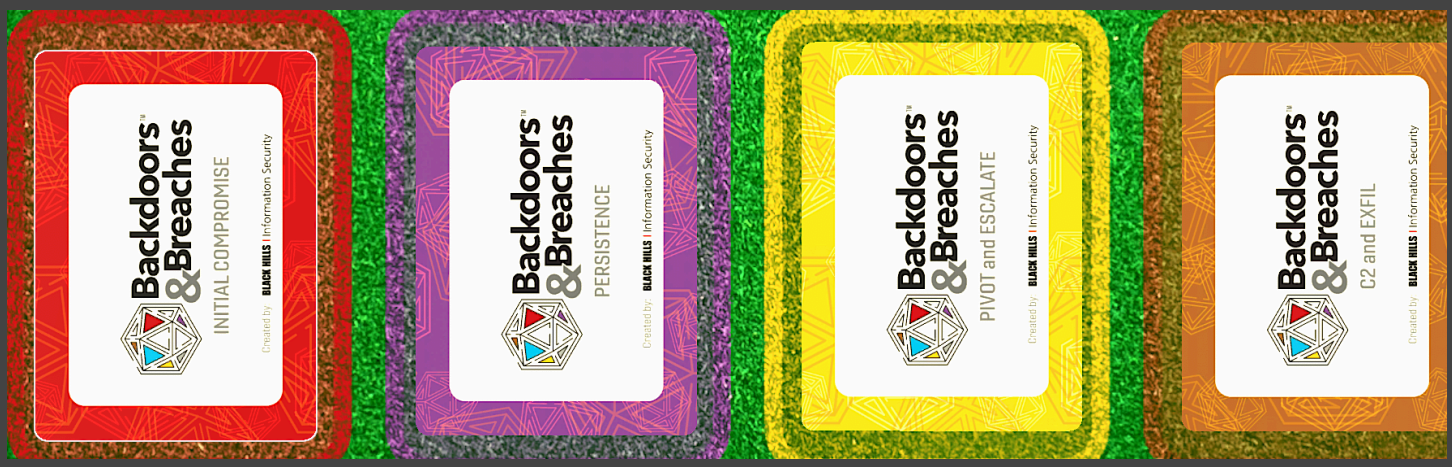
We play using Tabletop Simulator. The Simulator is ~$15 on Steam, but the game board is free. Search for "BHIS" in the workshop if you want to download and play yourself!



The Game Board

You're looking at the main game board. The blue cards you see there are the **Procedures** that you, the defenders, can use to reveal the red, purple, yellow, and brown cards (the **Kill Chain**). Each **Procedure** will detect different tactics, techniques, and procedures used by the attackers.

Your Objective: reveal the Kill Chain within 10 turns.

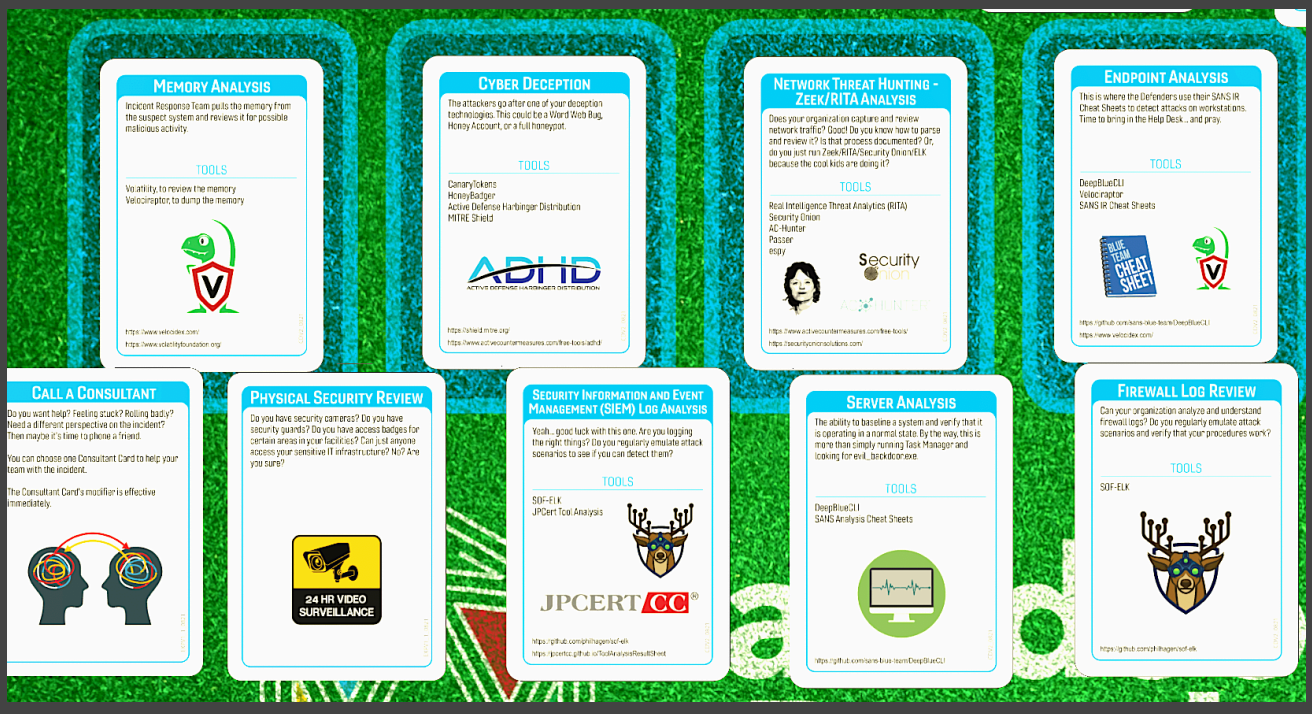


The Kill Chain

The game begins with a **scenario**, as narrated by the Game Master. This scenario is how the defenders are first alerted to an incident. Depending on the attack, the alert might be user contact, a SOC alert, or even a threat hunt finding. This is the storytelling component of the game. Players can ask the Game Master for more information about the scenario, as details not represented on the cards may be extremely helpful in determining the best course of action.

ASK QUESTIONS!

Procedures



Procedures

The blue **Procedure** cards are the tools and techniques the defenders can use to reveal the **Kill Chain**. Each tool will detect different techniques, so the defenders must match their choice to what they know about the attack so far.

The game board separates Procedures into 2 types: normal and “preferred” Procedures. Preferred Procedures, outlined in blue, are the defenders’ most well-known tools. These are the things they do every day. Consequently, defenders receive a **+3** bonus when using them.

The Kill Chain

The game’s “Kill Chain” is a simplified version of Lockheed Martin’s framework for describing attack methodology. In BnB, the Kill Chain has 4 segments:

1. **Initial Compromise**: How the attackers got in
2. **Persistence**: How the attackers maintained access
3. **Pivot and Escalate**: How the attackers moved around the network and elevated their privileges
4. **C2 and Exfil**: How the attackers controlled their access (C2: Command and Control) and retrieved sensitive data

Basic Gameplay

Every turn consists of 3 phases:

1. Decision Phase
2. Roll Phase
3. Results Phase

During the **Decision Phase**, defenders arrive at consensus about what **Procedure** to employ. This can (and should!) involve a fair amount of discussion.

Once a **Procedure** has been chosen, it’s time for the **Roll Phase**. Players roll a d20 (20-sided die) to determine the outcome. A 1-10 is a failure; and 11-20 is a success. Don’t forget that preferred Procedures get a +3!

If the Procedure succeeds *and* matches one of the detection rules for a **Kill Chain** card, that card is revealed. Otherwise, the game advances with no other action.

If the Procedure fails, the card is disabled for **3 turns**. Defenders discuss how a detection might have gone wrong.

Rolling a **1** or a **20** will result in an **Inject**—a random event with unique impacts on the game.

After the **Results Phase**, the turn counter is incremented, and the process begins again.

Procedures Reference

Here you'll find our definitions of each Procedure.

Call a Consultant: Need a little help? This card will reveal a **Consultant** card that provides some random assistance. Try to avoid it; we ain't made of money.

Crisis Management: Use the org's C-Suite to unlock resources. We have a house rule for this one; see below in the **House Rules** section.

Cyber Deception: Defenders can be sneaky too! Use honeypots, honeynets, and canaries to catch the bad guys in the act and discover their techniques.

Endpoint Analysis: Deep investigation on *targeted* endpoints. This can use either EDR tools or more intensive forensic tools. Either way, this is about specific endpoints, rather than the entire environment. Useful for discovering activity on endpoints once you know which ones to look at.

Endpoint Security Protection Analysis: This is your Endpoint Detection and Response (EDR) dashboard. Think of it as the overview of endpoint activity in your environment. Automated detections will appear here. Good for discovering what specific endpoints to investigate, and for identifying some common pivot/escalation paths.

Firewall Logs Review: Although the SIEM may have these logs too, everything that crosses your network's edge will be recorded here (theoretically). Useful for discovering external access attempts.

Isolation: Use network segmentation to slow the attackers. We have a house rule for this one; see below in the **House Rules** section.

Memory Analysis: Capture a memory dump of an endpoint/process. Useful for determining what is currently running on a system, and what it's doing under the hood.

Network Threat Hunting: Packet capture/netflow analysis. Using tools like Zeek, discover exactly what data is crossing your wires. Useful for discovering C2 via network artifacts

Physical Security Review: Look at cameras, door access logs, etc. for evidence of physical compromise. Useful if someone's trying to gain meatspace access.

Security Information and Event Management (SIEM) Log Analysis: Your SIEM should be where most sensitive systems log their data. This could be HTTP proxy logs, authentication logs, email, or even Windows Event logs. Useful for many different detections, and a threat hunter's best friend.

Server Analysis: Baselining of servers specifically to detect anomalies in behavior, such has high CPU/network usage. Useful for discovering compromise of servers based on patterns.

User and Entity Behavior Analytics (UEBA): Machine learning that baselines user activity and detects outliers. Useful for detecting whether user accounts have been compromised based on unusual access patterns.

House Rules

As we've played, we've discovered some modifications to the game to add realism or improve game balance.

Incident Commander

To promote game flow, each turn we nominate an "incident commander," who has ultimate responsibility to decide what procedure the team selects. This focuses conversation and provides a single decision point. At the end of the turn, the incident commander nominates their replacement.

Crisis Management

When a War Room is set up for a crisis, the budget faucet flows and you have easy access to people you need to talk to. But the chaos of the environment can diminish focus. Therefore, when you activate Crisis Management, you receive a **+2** to all Procedures, but lose the **+3** to preferred Procedures. This effect lasts **3 turns**.

Isolation

Network segmentation is a best practice. It limits what attackers can get to after a compromise. However, it can also slow down your efforts to review activity. Activating this card adds **3 turns**, but you receive a **-3** penalty on the next roll. Can only be used once per game.

Active Threat

This is a unique game mode in which we simulate an active attacker within the environment. Instead of beginning with a complete Kill Chain, the game begins with only **Initial Compromise** on the board. A separate player (or the Game Master) plays the role of the attacker.

We add an **Attacker Phase** to each turn, such that after the **Results Phase**, the attacker will attempt to add a Kill Chain card to the board. A d20 roll determines success/failure just like for the defenders. If the attacker completes the kill chain, the attacker wins. The defenders must either fully eliminate the Kill Chain or survive 10 rounds. As defenders reveal Kill Chain cards, the attacker loses the ability to add cards beyond that portion of the Kill Chain. However, if defenders reveal a lower Kill Chain segment but a higher segment remains, the attacker may progress up the Kill Chain. This simulates how persistence and pivot/escalation favors the attacker.

For example, if an attacker has Initial Compromise and Persistence and the defenders reveal Initial Compromise, the attacker may continue to attempt to add Pivot/Escalate cards without first reestablishing Initial Compromise (although the attacker will need to in order to finish the game).

On the other hand, if an attacker has Persistence, they may not attempt C2/Exfil before first establishing Pivot/Escalation.

When defenders reveal a Kill Chain card, it is “burned” to the attacker. In practice, this means the card is removed from the Kill Chain slots, but left face-up on the table and removed from the potential TTPs the attacker can use.