Welcome to Backdoors & Breaches!

The goal of this game is to help organizations and people have a better understanding of attacks and defenses.

In this game, there are 6 different kinds of cards.

The first set of cards is called Initial Compromise. These cards are red and represent how an attacker would first gain access to your network.

The second set of cards is called C2 and EXFIL. These cards are brown and represent how an attacker would maintain access to the system they compromised on a network.

The third set of cards is called PERSISTENCE. These cards are purple, and represent how an attacker would maintain access to a compromised system.

The fourth set of cards is called PIVOT and ESCALATE. These cards are yellow and cover how an attacker would move around a network and escalate their privileges.

The fifth set of cards is called PROCEDURES. These cards are blue, and represent the various Incident Response (IR) procedures an organization can use to identify and neutralize an attack. Any time an action is taken using one of the PROCEDURE cards, there is a +3 modifier on that action. This increases the odds this action is successful.

The sixth set of cards is called INJECTS. These cards are white and are pulled at various times in a game to add twists and turns to the game. They are also used to make the game highly replayable.

To start the game pick one person who is the Incident Master. This person's one goal in life is to keep the game moving. They will pull one random card from the Initial Compromise, C2 and EXFIL, PERSISTENCE, and PIVOT and ESCALATE decks. This is "building the incident." These cards are not to be shown to the other players yet.

Next, the other players will make up the IR team and will draw 4 random PROCEDURES cards. These cards are the documented procedures for the defenders.

Now, the IR master starts the game. Ideally, this is with a slight narrative of how the IR team finds out about the incident.

For example:

"The helpdesk calls and notifies you that an end-user noticed an Anti-Virus (AV) alert."

"The lead systems administrator says his desktop is not performing as it normally does."

"The CISO says he "feels something is wrong."

"An end-user calls and says they think something is wrong with their computer. But, they totally do not surf porn and that cannot possibly be the issue."

Now, the IR team starts to take actions. All actions require a roll of a 20 sided dice. Also called a 20d by people who did not date in high school... People like me.

If the roll is 11-20 the action is successful. At this point, one of the incident cards can be revealed. I say “can be” because the decision to reveal a card is completely up to the Incident Master. For example, the IR team may decide to give up and go get coffee. They would roll. It could be a successful roll and still no cards would be revealed. Why? Because we just do not want to reward that kind of behavior in the middle of an incident.

If the IR team does an action for which they have a PROCEDURES card for, they will get a +3 modifier on their roll. What this means is that if they roll a 9, it would normally fail. However, if they take an action for which they have a PROCEDURES card for, the roll would be 9+3=12. Now it is successful. This is to highlight the importance of documented procedures for IR. Another way to use the PROCEDURES cards is to grant the PROCEDURES cards that your company has. So, if your company has 8 of the PROCEDURES cards your IR team can get all of those procedures, just so long as they are properly documented and approved by management.

It should be noted that the IR team does not have to only do the actions on the pulled PROCEDURES cards. They can do whatever they want. Any action that is not a pulled PROCEDURE card is a straight 50/50 chance of success. Or, if they roll a 1-10, the action fails. If they roll an 11-20, the action succeeds.

Now, if the IR team rolls a 20, a 1 or fails and rolls 3 times in a row, an inject card is pulled. This only applies to natural 20 rolls, not a +3 modifiers from PROCEDURE cards (17+3=20). The goal of the INJECT cards is to add an additional narrative dynamic to the game.

Once the IR team has successfully taken actions to reveal all incident cards, the game is over. Now, they can bask in the glow of a successful incident and they can start blaming others for what went wrong.

However, if the IR team takes 10 rolls without revealing all Incident cards, they fail the game. The incident is unresolved and it is time to figure out what went wrong. Missing procedures? Possibly. Incredibly bad luck at rolling? Most definitely.

You can play this game in two ways.

The first is to just go through the games as quickly as possible to note missing procedures in your organization.

The second way is to ponder and discuss. Both are fine. The overall goal of the game is to improve defenses and help convince management of the importance of having procedures and the merit of being lucky. It is also to develop and foster IR and defense discussions before an incident occurs.

Remember, this is a tabletop game. The goal is for the Incident Master to develop a narrative. The cards help with that.