OBJECTIVE OF IoT Pentest Blitz: Be the player with the most points at the end of the game.

NUMBER OF PLAYERS: 2 - 5 players

MATERIALS: 15 IoT Device Cards, 77(89?) Attack Chain Cards, 12 Blue Team Cards Defense Cards, 10 Ransomware Cards

TYPE OF GAME: Set Collection

AUDIENCE: Kids, Adults

OVERVIEW OF IoT Pentest Blitz

In this game, players are trying to build high scoring IoT Device Penetration Tests. On each turn, players perform two actions: Add Attack Chain cards, raid the Toolbox, steal Attack Chain cards from an opponent's IoT Device Penetration Tests, or simply stockpile resources - there are plenty of decisions to be made each turn.

MATERIALS

- **IoT Device Cards**

  - Each target could be an IoT device, Embedded Device, Web Server, Medical Device, etc.
- **Ransomware Cards**

  - Each Ransomware represents a theft from a penetration test, removing resources for Incident Response
- **Attack Chain**
  - **Attack Cards**

    - Represent techniques like phishing, exploiting a known CVE, or password spraying. Some attacks may require specific conditions or prerequisites. IE specific Resource card classes (Protein, Vegetable or Nori)

- **Defense**
  - Finite State - Binary SCA
  - Finite State - Firmware Analysis
  - Finite State - Vulnerability Management
  - Finite State - Enriched SBOMs
  - Finite State - Regulatory Compliance
  - Finite State - Supply Chain Risk Management
  - Finite State - Risk Assessment and Penetration Testing
- **Resource Cards**
  - Tools, exploits, or tactics (e.g., Mimikatz, Metasploit, Powershell, Jack the Ripper, Hydra, etc.). These act as boosters to increase attack success. Reconnaissance techniques.
  - Subject Matter Expert

Each player will have three IoT Device cards that they will need to fill with Attack Chain cards.

There are a variety of different Attack Chain cards. In the picture above, the top row contains the Attack cards. These determine the Resource cards that will be included in the IoT Device Penetration Test and how points will be earned. The middle row contains the different Resource cards. Green cards are Recon, yellow cards are tools, and green/yellow represents both recon and tools. In the bottom row are the Defense In Depth cards and Subject Matter Expert (SME) cards. These are special cards that add or take away points from a bowl.

Use a Ransomware card to steal a Resource from the top of an opponent's IoT Device Penetration Test.

SETUP

Each player begins the game with three IoT Device cards and two Incident Response cards. Place the three IoT Device cards in a row with the "safe" side face up.

Shuffle and deal three Attack Chain cards to each player. Players should not display their hand. Place the remaining Attack Chain cards face down as a draw pile in the center of the table and flip up four cards. Place them in a row alongside the Attack Chain cards draw pile. This row is called the Toolbox.

THE PLAY

Whoever conducted the most recent IoT penetration test, penetration test or security audit goes first. During a player's turn, they choose two actions to complete. Actions may be completed in any order, and the same action can be completed twice.

ACTIONS

Attack: Place one Attack Chain card from your hand onto an IoT Device pile. The card must be placed on top of that IoT Device pile. IoT Devices can only have one Attack card, and cannot have more than five Attack Chain cards.

Draw: Choose one of the Attack Chain cards from the Toolbox and add it to your hand. When a card is taken from the Toolbox, the player immediately replaces it with a card from the draw pile. The moment a player has more than five cards in their hand, they must immediately discard back down to five.

Incident Response: Use a Ransomware card to take an Attack Chain card from the top of an IoT Device Penetration Test on the table and add it to your hand. The Ransomware card must be discarded in this usage.

Resource Refresh: Remove all the cards from the Toolbox and replace them with four new ones from the draw pile. The special abilities on any Blue Team or Subject Matter Expert (SME) cards are activated when a player restocks.

Complete a Penetration Test: To complete a Penetration Test on an IoT Device, flip the entire pile over. The back side of the IoT Device will be displayed showing a "hacked" IoT Device. An IoT Device must have one Attack Card and at least one other Resource cards before it can be classified as a Completed

Penetration Test. An IoT Device that has been classified as a Completed Penetration Test cannot have more Attack Chain cards added or taken away.

Re-Scope: Remove all the Attack Chain cards from one of your IoT Device Penetration Tests. The Attack Chain cards are discarded.

SPECIAL ACTIONS

- Any time a Defense In Depth or a Subject Matter Expert (SME) card is placed in the Toolbox during a player's turn, that player may immediately play one Defense In Depth or Subject Matter Expert (SME) cards on an IoT Penetration Test. The card can be added to an opponent's Penetration Test or their own. Once a Subject Matter Expert (SME) card or Defense In Depth card is played from the Toolbox, immediately replace it with another card from the draw pile. If it is again a Defense In Depth or Subject Matter Expert (SME) card, play the card. This continues until the new card cannot be played.
- Defense In Depth and Subject Matter Expert (SME) cards can also be played from a player's hand on their turn. Playing these cards is considered a free action.

CONTINUING PLAY

Play continues around the table with each player trying to build valuable IoT Penetration Tests.

ENDING THE GAME

A player completing Penetration Tests on their third IoT Device signals that the game is about to end. Each player gets one more turn. After the last player finishes their final turn, it is time to tally up the score.

SCORING

- Players earn points for the IoT Device they completed a Penetration Test upon. Any unfinished Penetration Tests do not earn points for the player.
- Each Blue Team card deducts one point from a completed Penetration Test on an IoT Device unless it has the Defense Attack Attack Chain card in it.
- Each Subject Matter Expert (SME) card adds one point to the IoT Device Penetration Test it is in.
- RCE powered Penetration Tests earn 4 points for every pair of vegetable and protein Resource cards.
- Debug Port powered Penetration Tests earn 2, 5, 9, or 14 points based on whether they have 1, 2, 3, or 4 unique Red Resource cards.
- MiTM powered Penetration Tests earn 2, 5, 9, or 14 points based on whether they have 1, 2, 3, or 4 different Green Resource cards.
- Defense In Depth earn 2 points for every Blue Team card they have in them.
- Brute Force powered Penetration Tests earn 6 points if they have a pair of matching Resource cards. They are worth 10 points if they have three matching Resource cards. Subject Matter Expert (SME) cards and Blue Team cards do not count as part of the matching requirement.
- Players add all their completed IoT Device Penetration Test' point values together to find their final score.

WINNING

The player with the highest score at the end of the game wins.