**Expanded Description of the Backdoors & Breaches Incident Response Simulation**

**What Is It?**

**Backdoors & Breaches (B&B)** is a structured and gamified tabletop exercise developed by **Black Hills Information Security** and **Active Countermeasures** to simulate cybersecurity incidents in a hands-on, engaging format. Instead of learning about incident response from theory alone, this exercise places participants inside a realistic breach scenario and challenges them to defend an organization in real time.

It is used widely in education, industry workshops, and blue-team training sessions to **build muscle memory** for responding to complex cyber threats.

In the **Security Operations Management (SOM) Lab 3**, this game serves as a practical learning tool to reinforce incident response phases discussed in lectures.

**Goals:**

* Familiarize participants with **cyber-attack kill chains** and **real-world attacker tactics**.
* Practice making **defensive decisions under pressure**.
* Learn the importance of **collaborative response**, **documentation**, and **post-mortem evaluation**.
* Improve understanding of standard procedures such as **MITRE ATT&CK**, **NIST Incident Response Lifecycle**, and use of tools like **SIEM**, **packet capture**, and **endpoint detection**.

**Game Structure and Mechanics (With Examples)**

**1. The Incident Master (Facilitator)**

The session is led by an **Incident Master**, who:

* Guides the narrative,
* Controls which attacker cards are revealed,
* Responds to team queries,
* Rolls dice to determine outcomes of defender actions.

*Example*: The Incident Master reveals that “a malicious insider has gained access to a database through stolen credentials.” The defenders must now detect, contain, and eradicate this threat.

**2. The Cards**

**a. Attack Cards**

There are four attack categories, each representing a step in the attacker’s operation:

* **Initial Compromise**: How the attacker enters the environment.

*Example Card*: *“Phishing Email with Malicious Attachment”*

* **Persistence**: How the attacker maintains access.

*Example Card*: *“Creates Hidden Scheduled Task”*

* **Command & Control (C2) / Exfiltration**: How they communicate and steal data.

*Example Card*: *“Encrypted HTTPS Tunnel to Remote Server”*

* **Lateral Movement**: How they move deeper into the network.

*Example Card*: *“Uses Pass-the-Hash Attack via SMB”*

These cards are played **sequentially**, and participants respond to each as they are revealed.

**b. Response Cards**

Participants have a deck of **defensive actions** to choose from, such as:

* “Search Firewall Logs”
* “Conduct Endpoint Triage”
* “Reset User Credentials”
* “Check DNS Queries”

*Example*: When attackers exfiltrate data via DNS tunneling, defenders might play “Analyze DNS Traffic.” A die is rolled to see if the action is successful, with modifiers based on procedure familiarity.

**3. Rolling the 1d20 Dice**

Every action is tested with a **20-sided die**:

* A roll of 17 might reveal key evidence.
* A roll of 4 might mean nothing is detected.
* **+3 bonus** is applied when **well-known or documented procedures** (e.g., MITRE ATT&CK techniques, playbooks) are used.

This adds randomness and forces defenders to **justify their toolset and technique choices**.

**Timeboxed Phases and Response Flow**

The simulation is carried out in **phases**, each mirroring the **NIST Incident Response Lifecycle**:

1. **Preparation** – Set context: What security tools and policies are in place?
2. **Identification** – Detect the incident.

*Example*: A strange spike in DNS traffic is detected.

1. **Containment** – Stop the attacker from spreading.

*Example*: Disable a compromised account or isolate an endpoint.

1. **Eradication** – Remove malicious components.

*Example*: Delete malware and scheduled tasks from infected machines.

1. **Recovery** – Restore affected services/data.

*Example*: Rebuild the compromised server using clean backups.

1. **Post-Incident (Lessons Learned)** – Reflect on what happened, what worked, and what didn’t.

**Example Walkthrough**

Let’s say your team is playing and this scenario unfolds:

* **Initial Compromise**: *“User opens malicious Excel file with macro”*
* **Your Action**: You choose “Check Email Gateway Logs”
  + Roll a 1d20 → You roll a 14 (+3 bonus) → **Success**
* **Next Card**: *“Creates scheduled task to run PowerShell script at login”*
* **Your Action**: Choose “Check Windows Event Logs”
  + Roll → You roll a 5 → **Fail** – You miss it
* **Lesson Learned**: You decide your logging is too limited and suggest enabling enhanced logging and PowerShell monitoring

**Learning Outcomes and Benefits**

Participants walk away with:

* Stronger understanding of **how real attacks unfold** across multiple stages.
* Practical experience in **detecting, investigating, and responding** to threats.
* Familiarity with **incident response tools and strategies**.
* Confidence in conducting **post-incident reviews**.

**Post-Exercise Deliverables**

After the simulation, each participant must complete:

1. **Post-Incident Evaluation Template** – Describe each phase, actions, and rationales.
2. **Lessons Learned Report** – Document what went well, what didn’t, and propose specific improvements.

These documents help translate the game experience into **real-world response maturity**.