

In this issue:

- 4. Teaching Cybersecurity Incident Response Using the Backdoors & Breaches Tabletop Exercise Game**
Jacob Young, Bradley University
Sahar Farshadkhah, University of Illinois Springfield
- 18. Going Beyond Considering the Use of Competency-based Education for Designing a Cybersecurity Curriculum**
Fred L. Strickland, University of Maine at Presque Isle
- 29. Preparation for a Cybersecurity Apprenticeship Program (PCAP)**
Jonathan Lancelot, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington
Grace Smith, University of North Carolina Wilmington
Chris Nichols, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Ron Vetter, University of North Carolina Wilmington
William Wetherill, University of North Carolina Wilmington
- 40. Rubber Duckies in the Wild: Proof of Concept Lab for USB Pen Testing Tool (Teaching Case)**
Anthony Serapiglia, Saint Vincent College
- 44. An IoT Based New Platform for Teaching Web Application Security**
Zhouzhou Li, Southeast Missouri State University
Ethan Chou, Southeast Missouri State University
Charles McAllister, Southeast Missouri State University
- 54. Proposing the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C)**
Jeff Greer, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
- 66. Identity Attributes in Teaching Privacy (Teaching Case)**
Yaprak Dalat Ward, Fort Hays State University
Li-Jen Lester, Sam Houston State University

The **Cybersecurity Pedagogy and Practice Journal (CPPJ)** is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (<https://cppj.info>). Our sister publication, the proceedings of the ISCAP Conference (<https://proc.iscap.info>) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal. Currently the target acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2022 ISCAP Board of Directors

Eric Breimer Siena College President	Jeff Cummings Univ of NC Wilmington Vice President	Jeffry Babb West Texas A&M Past President/ Curriculum Chair
Jennifer Breese Penn State University Director	Amy Connolly James Madison University Director	Niki Kunene Eastern CT St Univ Director/Treasurer
RJ Podeschi Millikin University Director	Michael Smith Georgia Institute of Technology Director/Secretary	Tom Janicki Univ of NC Wilmington Director / Meeting Facilitator
Anthony Serapiglia St. Vincent College Director/2022 Conf Chair	Xihui "Paul" Zhang University of North Alabama Director/JISE Editor	

Copyright © 2022 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Anthony Serapiglia
Co-Editor
St. Vincent College

Jeffrey Cummings
Co-Editor
University of North Carolina
Wilmington

Paul Witman
Associate Editor
California Lutheran
University

Thomas Janicki
Publisher
University of North Carolina
Wilmington

Teaching Cybersecurity Incident Response Using the *Backdoors & Breaches* Tabletop Exercise Game

Jacob Young
jayoung@bradley.edu
Bradley University
Peoria, Illinois

Sahar Farshadkhah
sfars2@uis.edu
University of Illinois Springfield
Springfield, Illinois

Abstract

In this paper, we describe an in-class cybersecurity exercise based upon the tabletop incident response game, *Backdoors & Breaches* (B&B), developed by Black Hills Security and Active Countermeasures. Instructors present students with a cybersecurity incident scenario and then task them with selecting appropriate defensive measures and analysis techniques to mitigate the threat. First, we provide background discussion on business continuity, incident response, and tabletop exercises. Second, we explain B&B and provide an example incident scenario. Third, we describe how we utilized the game in an Executive Master of Business Administration program and a junior-level information security course. Fourth, we discuss feedback that we received from students. Fifth, we discuss additional game development that has occurred since we employed B&B in our courses. Sixth, we provide recommendations for others interested in replicating the exercise. Lastly, we outline future research directions.

Keywords: Incident response, Business continuity, Tabletop exercise, Cybersecurity, Pedagogy.

1. INTRODUCTION

In this paper, we describe our implementation of an in-class security exercise based upon the tabletop incident response game, *Backdoors & Breaches*. The game was developed in 2019 by the cybersecurity firm Black Hills Information Security and Active Countermeasures (Black Hills Information Security & Active Countermeasures, 2021). *Backdoors & Breaches* was originally intended to help organizations review and improve incident response procedures, but we felt that it would also translate well to the classroom. Although *Backdoors & Breaches* has been mentioned in two articles (Puchkov et al., 2021; Straub, 2020), none of the extant pedagogical research has focused specifically on employing the game as an in-class exercise. Therefore, we piloted the game to assess how well *Backdoors & Breaches* (B&B) would be received by students.

First, we discuss business continuity and the importance of tabletop exercises in incident response planning. Second, we explain B&B and provide an example incident scenario. Third, we discuss how we used the game in our course. Fourth, we discuss the feedback that we received from students. Fifth, we discuss additional game development that occurred after our study. Sixth, we provide suggestions for instructors to consider when utilizing the game in their courses. Lastly, we outline future research directions involving B&B.

2. BACKGROUND

In this section, we discuss the importance of business continuity planning, the implementation of incident response procedures, and how the use of tabletop exercises can improve organizational preparedness.

Business Continuity

Business leaders and information technology professionals must ensure that their organization can withstand and recover from a wide variety of operational disruptions, such as cyber-attacks, extreme weather events, and global pandemics. When a disaster happens, all organizations want to mitigate its disruptive impact and get back to normal operations as quickly as possible. Developing, testing, and refining organizational processes to prepare for abnormal scenarios improves their business continuity.

Business continuity is the ability of an organization to maintain operations under disaster conditions. Business Continuity Planning (BCP) involves recognizing potential threats and their likely impact to an organization's operations, then developing a collection of procedures for the various business units (Wilson, 2000) that will mitigate the disruption on key functions (Rezaei Soufi et al., 2019).

Incident Response

One aspect to ensuring continuity of operations at a time of crisis, especially when a cybersecurity attack occurs, is incident response. Core activities involved in incident response are detection, containment, eradication, and recovery. It is also important for organizations to be agile in addressing emerging threats (Naseer et al., 2021). Any response to potential or ongoing cybersecurity incidents needs to happen in a timely and cost-effective manner (Cichonski et al., 2012).

Although many organizations use prevention-oriented strategies to deal with cybersecurity threats, they are more vulnerable to dynamic and unpredictable attacks. Therefore, organizations need to develop a dynamic response capability to detect cyberattack activity in real-time. This approach provides security managers with actionable insights to stop and prevent/mitigate the damage (Naseer et al., 2021).

We believe that employing tabletop exercises in the classroom helps demonstrate the importance of an agile response to disruptive incidents while also developing essential skills for future information technology professionals.

Tabletop Exercises

Cybersecurity educators are using different methods to fill the cybersecurity skills gap that employers are facing. Angafor, Yevseyeva, & He (2020) suggest using tabletop exercises to nurture and enhance practical hand-on skills. These exercises not only improve problem-solving, communication, and teamwork skills, but

also further enhance understanding of business processes. These skills prepare future professionals to perform more effectively as members of cybersecurity incident response teams.

It is important that tabletop exercises improve both technical and nontechnical skills of students. By playing games and scenario-based exercises, educators can simulate the unpredictable nature of cyber incidents (White et al., 2004). This not only demonstrates the importance of time and teamwork in the decision-making process but also gives students the opportunity to learn from unsuccessful outcomes.

3. BACKDOORS & BREACHES

In this section, we describe the requirements and basic gameplay for *Backdoors & Breaches*.

Requirements

Typically, the game would be played with one participant serving as the Incident Master (IM) and up to seven players acting as Defenders. Complete gameplay instructions are available on the *Backdoors & Breaches* website. Black Hills Information Security has also published a helpful tutorial video on YouTube (Black Hills Information Security, 2019).

Instructors will need at least one set of *Backdoors & Breaches* (Spearfish General Store, 2021). Recently, the core deck was refreshed to reflect current practices and an expansion pack was also just released. The original deck contains 52 cards, organized into six different categories: Initial Compromise (10), Pivot and Escalate (7), Persistence (9), C2 and Exfil (6), Procedure (10), and Inject (10). Version two has one additional Procedure card and one fewer Inject card. The first four categories are attack cards. Procedure cards are played by the Defenders and Inject cards are used by the IM to alter gameplay. We provide example cards in Appendix A.

Gameplay

To begin, the IM draws a single card from each of the attack categories (Initial Compromise, Pivot and Escalate, Persistence, and C2 and Exfil) without revealing them to the defending team. The IM would then craft an incident scenario that incorporates the issues described in the cards. A total of 3,780 incidents can be generated.

All Procedure cards are made available to the Defenders, but four cards are randomly selected to serve as written procedure cards. These cards are given a +3 point modifier. After the Defenders

select a Procedure card, they then roll a 20-sided die, also known as a d20. The randomness provided by rolling a die helps demonstrate the unpredictable nature of incident response. If a physical d20 is not available, there are several d20 simulators available online.

If the result of the die roll, plus any applicable modifiers, is greater than ten, then the IM will announce whether the selected Procedure card defeats one of the attack cards. If the Procedure card is successful, then it may be replayed by the Defenders in a subsequent turn. If the die roll is ten or lower, then the turn fails, and the Procedure card cannot be replayed for the next three turns. When a turn fails due to the die roll, the IM should not reveal to the Defenders whether the chosen Procedure card would have been effective against any of the attack cards. Defenders continue to select various Procedure cards to mitigate the incident. The Defenders win if they manage to reveal all four attack cards within 10 turns.

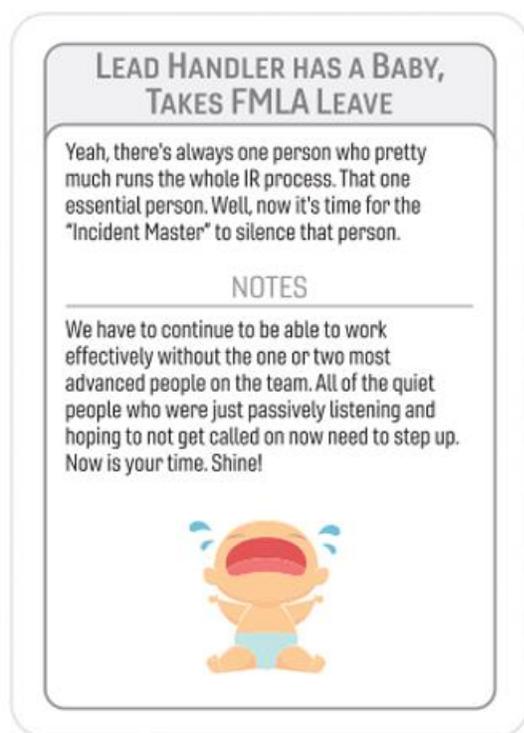


Figure 1: FMLA Inject Card

An optional aspect of the game involves the use of Inject cards. For example, the IM can elect to introduce additional chaos to the incident by selecting an Inject card whenever the Defenders roll a 1, roll a natural 20 (meaning without any modifiers), or roll unsuccessfully 3 times in a row.

Inject cards can impact the incident in a wide variety of ways. Some Injects allow for an attack card to be revealed to the Defenders, others might not impact the game, whereas some could end the game altogether. We provide an example Inject card in Figure 1. Injecting this card would result in silencing the best Defender, as if they were unavailable due to leave protected under the Family and Medical Leave Act.

4. EXAMPLE INCIDENT

In this section, we describe a round of *Backdoors & Breaches*, from dealing Procedure cards, to creating the incident scenario, and playing each turn. We also provide a completed turn tracker worksheet in Appendix B, which can be used to follow along with the gameplay.

Procedure Cards

To begin, the Defenders are dealt all ten Procedure cards, with four randomly selected to serve as written procedure cards. These cards carry a +3 modifier bonus and should be spread out across the top row so that the Defenders can differentiate them from the other six Procedure cards, as shown in Figure 2.

Scenario Creation

The IM then draws a card from each of the attack categories to develop the incident scenario. In this example, we will describe an incident based upon the following attack cards: Bring Your Own (Exploited) Device, Internal Password Spray, New User Added, and Gmail, Tumblr, Salesforce, Twitter as C2. We will reveal each attack card as they are detected by the Defenders throughout our example.

Turn One

To begin play, the IM will vaguely describe the cards to give the Defenders a rough idea of what kind of incident they might be facing. In this example, the IM might say, "Our intrusion detection system just alerted us to rapid login attempts. It appears to have been focused on one of our devices, but now the attempts seem to be targeting several devices across our network." The Defenders would then select a Procedure card that they believe would best address the incident.

Since the Defenders want to keep the intrusion from spreading further, they elect to play the Isolation card, which has the +3 point modifier. The Defenders then roll an eight, which results in a total of 11 points after the modifier has been added. Since the roll is greater than ten, the IM now checks the Detection section of each attack

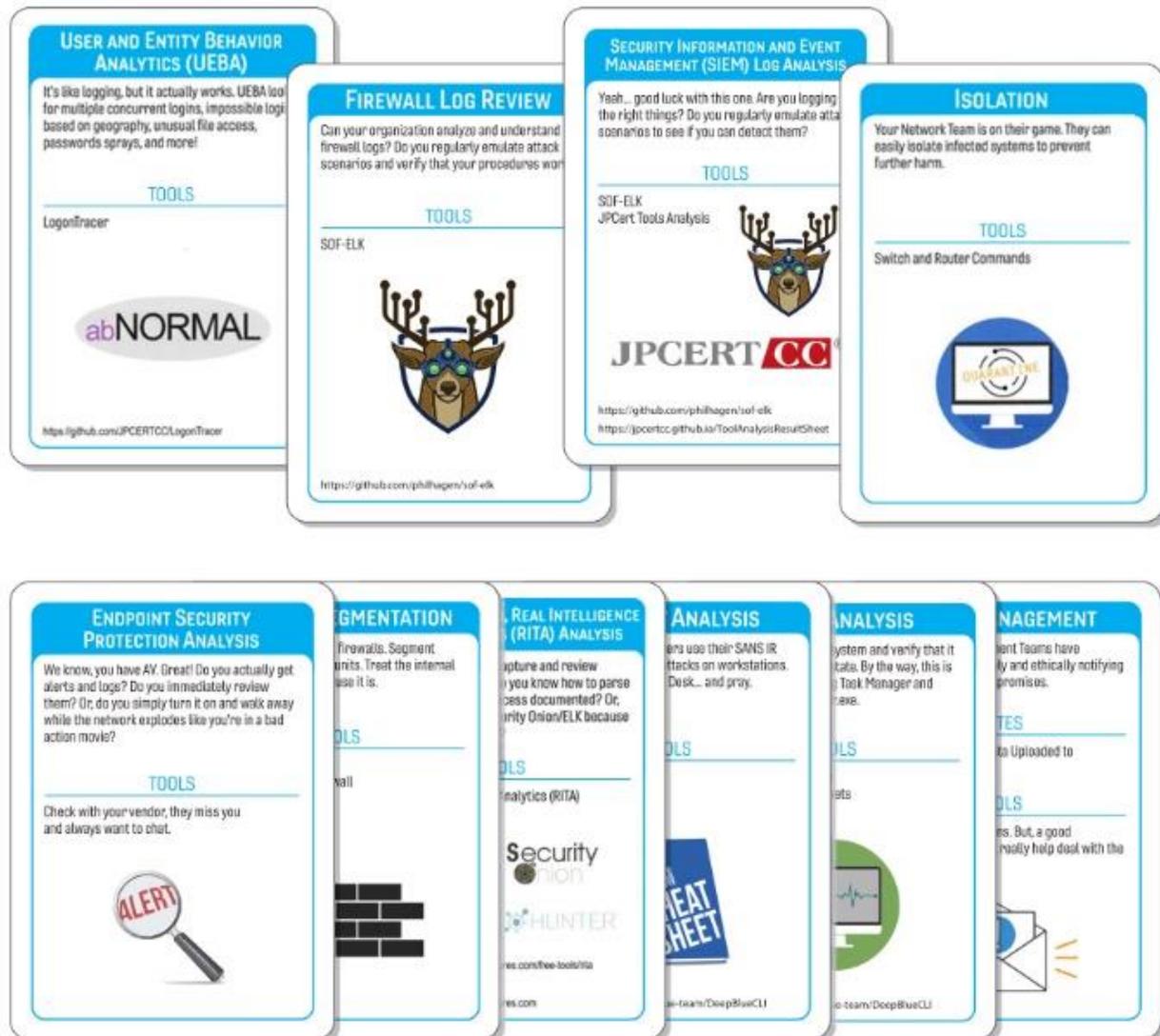


Figure 2: Procedure Cards

card to see if the Isolation procedure defeats any of the attacks. In this case, it does not, so the turn is unsuccessful. The IM can always add some humor by coming up with a reason for why the procedure did not work, such as, "Despite our objections, the CEO doesn't want you to 'waste your time' with isolation since he believes the devices already shouldn't have been able to communicate with one another."

Turn Two

The Defenders respond by selecting the Endpoint Analysis card and roll a 14. Since the roll was greater than ten and the Endpoint Analysis card detects the New User Added attack card, it would be revealed to the Defenders (see Figure 3). The Endpoint Analysis card can also be replayed during another roll. For this turn, the IM could

explain how the Persistence aspect of the incident was defeated by saying, "Your quick decision to analyze each endpoint resulted in the discovery of an unauthorized account on a file server."

Turn Three

For their third turn, the Defenders select the Server Analysis card and roll a 6, which is not large enough to reveal whether the card would have been effective. The IM might describe this outcome by saying, "No one ever established a baseline for this server, so we cannot tell if anything else has been changed." Therefore, the Defenders do not learn anything meaningful from this turn. Note, the Defenders cannot replay the Server Analysis card until at least turn seven.

Turn Four

The Defenders then select the User and Entity Behavior Analytics (UEBA) procedure card for their fourth turn and roll a 16, which results in a total roll value of 19 due to the modifier. The UEBA card successfully detects the Internal Password Spray attack card (see Figure 4). Since this turn was effective, the Defenders can replay the UEBA card during another turn.

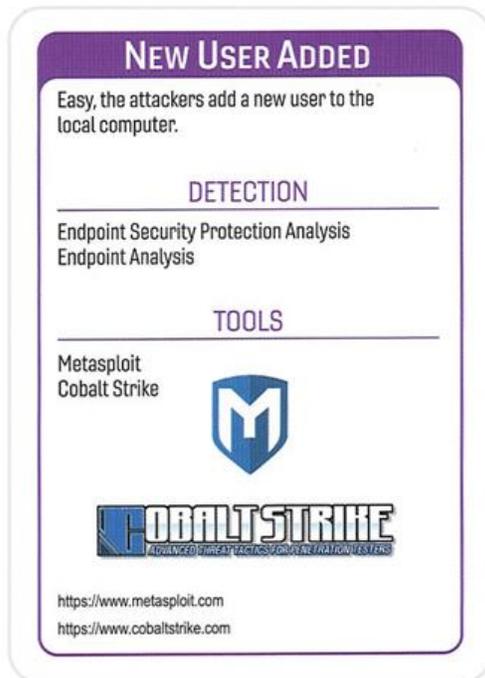


Figure 3: New User Added Attack Card

The IM could describe the outcome of this turn as, "We now know how the attackers gained access to the server. They launched the password spray from one of our workstations in the marketing department. Apparently, an employee was still using a password that was compromised in 2019. Although we are making good progress, we are unsure how the attackers gained access to our internal network."

Turn Five

For their fifth turn, the Defenders elect to play the modified Firewall Log Review card and roll a 4, for a total of 7. Since the procedure is ineffective, the Firewall Log Review card cannot be replayed until turn nine. The IM could describe this result as, "Unfortunately, it looks like our firewall logs were only retaining the last 48 hours of activity. It looks like the unauthorized user was added to the server a week ago, so we're still in the dark."

The IM might consider sharing more information about the Initial Compromise card to help them

select their next card. For example, the IM could say, "After quickly surveying our IT help desk staff, we found out that an employee asked for help connecting their personal device to the corporate network a couple weeks ago."

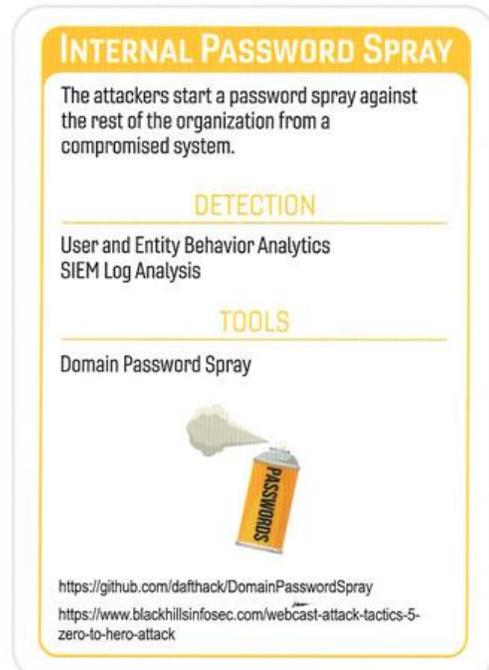


Figure 4: Internal Password Spray Attack Card

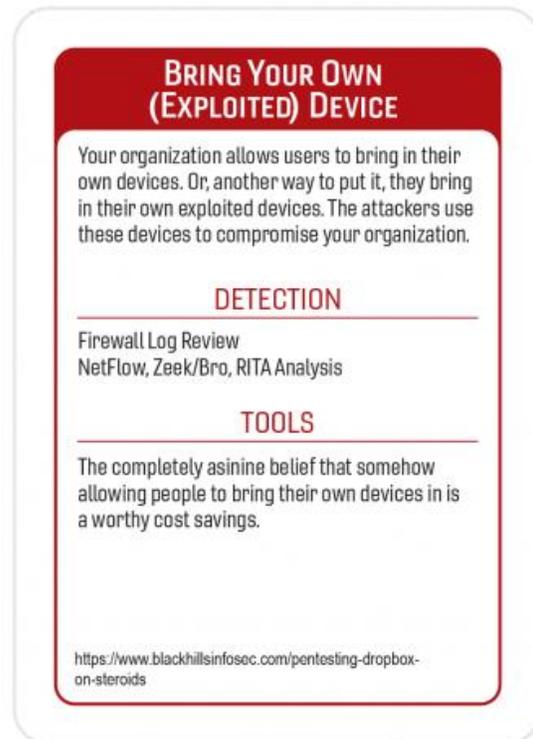


Figure 5: BYOD Attack Card

Turn Six

The Defenders select the NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis card for their sixth turn and roll a 12. Even though this card is effective against both of the remaining attack cards, the IM elects to reveal the BYOD card (Figure 5) to increase the difficulty. The Gmail, Tumblr, Salesforce, Twitter as C2 card (Figure 6) can only be detected by RITA, whereas BYOD can also be detected by the Firewall Log Review card.



Figure 6: Gmail, Tumbler, Salesforce, Twitter as C2 Attack Card

Turn Seven

For their seventh turn, the Defenders decide to replay the RITA card. However, they only roll a 7 this time, which means it failed to detect the final attack card.

Turns 8, 9, and 10

Although the Defenders would still be able to play the remaining procedure cards, the RITA card is the only one that could detect the C2 & Exfil attack card. Therefore, the Defenders will ultimately lose the game since they were only able to successfully detect three of the four attack cards within ten turns.

5. IMPLEMENTATION

In this section, we describe how we employed *Backdoors & Breaches* into our courses and discuss the feedback we received from our students.

Audience

We piloted this exercise at both the graduate and undergraduate levels in the spring semester of 2021. We employed the game at the conclusion of a two-day module of an Executive Master of Business Administration program and at the end of the semester in two sections of a junior-level information security course. Students in the EMBA module had little to no prior experience with incident response, so the game simply provided a fun introduction to tabletop exercises. The undergraduate students had completed approximately 90% of a course tailored towards earning CompTIA's Security+ certification. Therefore, they managed to apply course content at a higher level as they worked through each incident response scenario.

Preparation

The instructor preselected attack cards to build multiple incident scenarios prior to each class meeting. The instructor also randomly selected four Procedure cards that would have a +3 bonus modifier for each scenario. Since the course was delivered using a hybrid manner (both in-class and remote) due to the COVID-19 pandemic, the Procedure cards were scanned and uploaded to the course learning management system so that students would be able to clearly view the options available during each scenario.

Implementation

In our pilot, the instructor served as the IM and all students played the defender role together. There were eight students in the EMBA module and 16 students in each section of the information security course, resulting in a total of 40 students. After the instructor provided an initial description of the scenario, students were encouraged to discuss the incident amongst themselves prior to agreeing on a Procedure card to play. The first ten-turn round of the game for each section took approximately 25 minutes to play, but subsequent rounds were typically completed in 15-20 minutes. We provide the estimated time to complete each stage of the exercise in Table 1 below.

Stage	Time	Total
Instructions	3 minutes	3:00
Scenario	2 minutes	5:00
Each turn	2 minutes	25:00

Table 1: Time Estimate for a Single Round

6. RESULTS

The exercise proved to be highly effective in introducing and reinforcing cybersecurity topics

to students with limited cybersecurity experience, as well as developing deeper critical thinking skills. Therefore, we believe that this exercise is appropriate for a diverse range of student backgrounds. For example, *Backdoors & Breaches* could also be played in introductory information systems courses to expose students in other majors to cybersecurity issues.

Reception

After completing three rounds of *Backdoors & Breaches*, we asked the 32 students in the undergraduate course to provide their thoughts on the exercise by answering a short survey. We received 21 responses (65.6% response rate). We summarize their feedback in this section, but also provide their responses in Appendix C.

First, we asked students what they enjoyed about the exercise. The most common theme was that they enjoyed how challenging the game was, while also allowing for multiple solutions. Others commented on how comprehensive the incidents were and how well they mimicked real-world scenarios. Several students also recognized how important effective teamwork is to successful incident response.

Second, we asked them to explain how playing *Backdoors & Breaches* helped them relate to the course material. Many students felt that the exercise forced them to think critically and better understand how to apply various security tools

and concepts to respond effectively, which is consistent with the “learn while playing” benefits of gamification. Even though the exercise was a low-stakes card game, several noted that they felt playing *Backdoors & Breaches* replicated the high-stress, time-sensitive, and unpredictable nature of incident response. Others stated that they felt playing the game better prepared them to respond to future incidents.

In our final question, we asked students to share how the exercise helped them realize the value of conducting tabletop exercises. While many further reiterated points made in their responses to the first two questions, several new themes emerged. Many enjoyed how playing *Backdoors & Breaches* provided a nice change of pace when compared to traditional lectures and lab activities. Some felt that participating in a tabletop exercise helped them better connect to the course content, whereas one mentioned that they are considering conducting an exercise at their current workplace.

7. FURTHER GAME DEVELOPMENT

In addition to the release of the expansion pack, further development of *Backdoors & Breaches* has occurred since we conducted our exercise. In this section, we describe an online and competitive version of the game.

Online Version

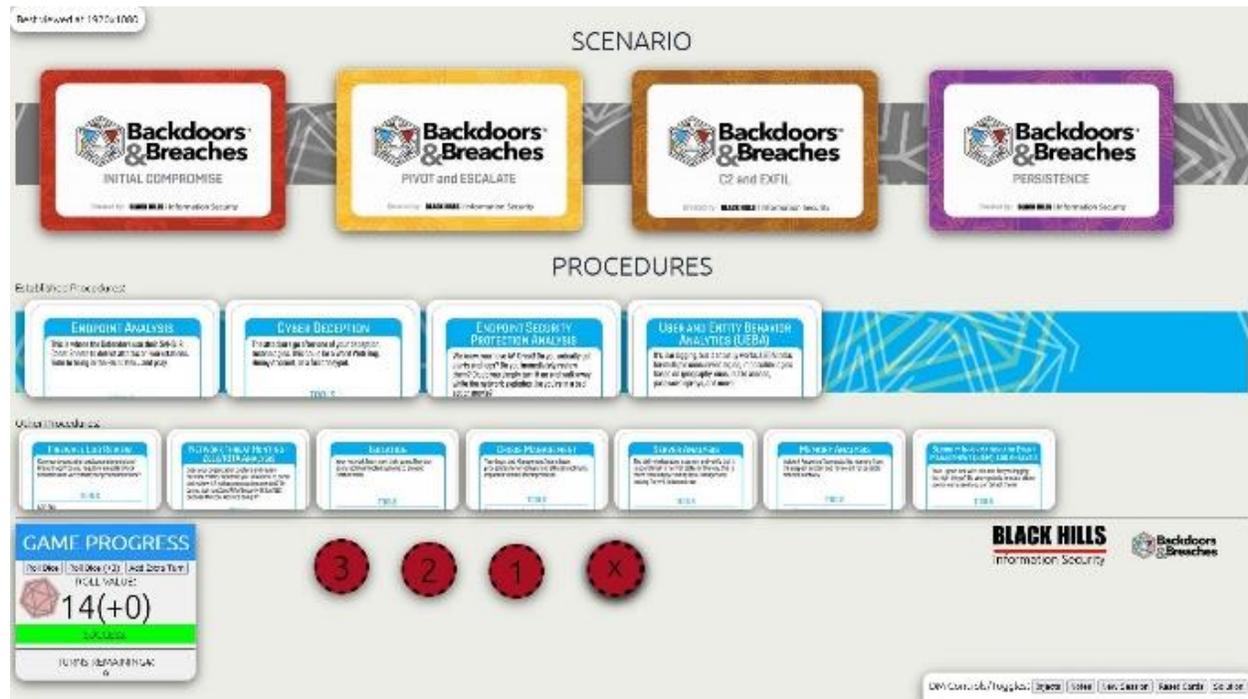


Figure 7: B&B Shuffle (Phung, 2021)

To make *Backdoors & Breaches* more accessible during the COVID-19 pandemic, Richard Phung (2021) published *B&B Shuffle*, an open-source version of *Backdoors & Breaches*. *B&B Shuffle* consists of an optimized interactive dashboard that simulates all the necessary functionality of the traditional game, including the ability to select either the core or expansion decks. Eventually, *B&B Shuffle* was officially released online by Black Hills (<https://play.backdoorsandbreaches.com/>), as shown in Figure 7.

Using *B&B Shuffle* would have greatly simplified our exercise delivery, especially when teaching in a hybrid environment. First, although the cost is minimal, using the online version would not have required purchasing any playing decks. Second, *B&B Shuffle* provides a far more polished way to display the game to students. That said, we recommend that incident masters practice developing scenarios prior to adopting the *B&B Shuffle* approach since the current version does not allow you to manually select attack cards.

Competitive Version

Black Hills Information Security & Active Countermeasures (2021) also developed a two-player, competitive version of the game with modified rules, as shown in Figure 8. Provided that enough playing decks have been purchased, instructors could consider extending our exercise by having students compete against one another.

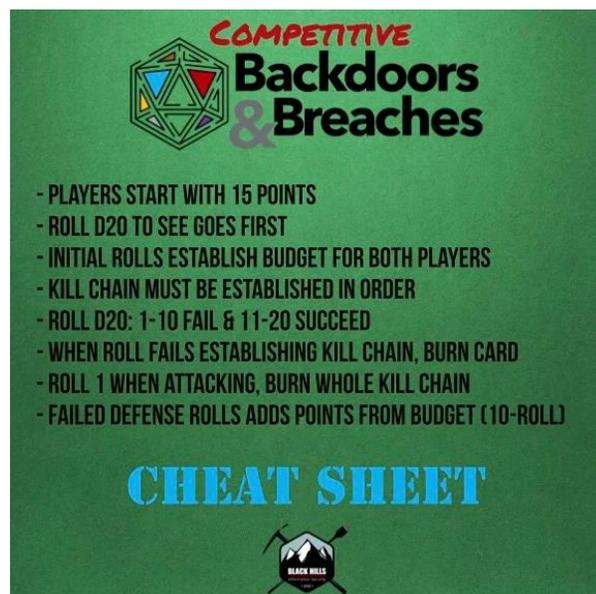


Figure 8: Rules for Competitive Version

Black Hills Information Security & Active Countermeasures (2021) also published a couple high-resolution playmat designs to enhance the

competitive version. We provide an example in Figure 9. Although the playmats can be printed at a vendor of the instructor's choosing, Black Hills recommends ordering them from Inked Gaming (<https://inkedgaming.com>).

8. RECOMMENDATIONS

After piloting *Backdoors & Breaches* in various class settings, we would like to provide several recommendations to help instructors adopt it in their courses. First, we recommend playing at least one complete round with the entire class serving as Defenders to introduce them to the mechanics of the game.

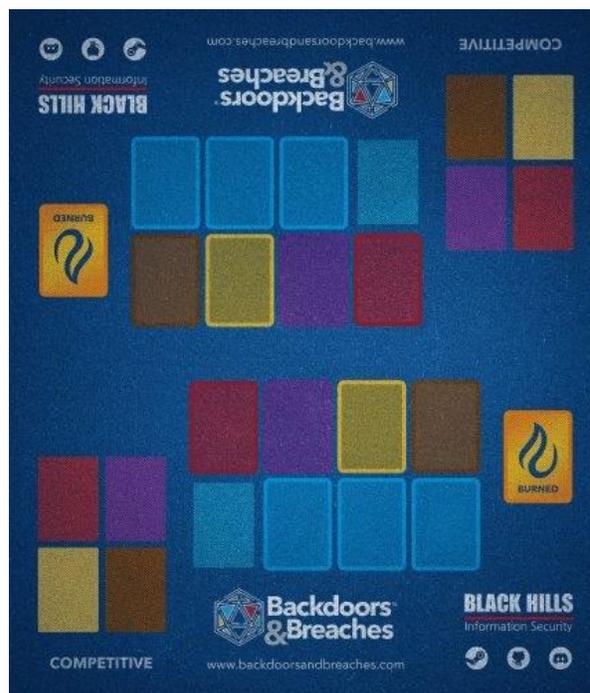


Figure 9: Competitive Playmat

Second, we encourage instructors to be generous in guiding the Defenders through the first couple of rounds. Once the class has demonstrated that they understand how to play, the IM can withhold more information and begin using Inject cards to increase unpredictability.

Third, we also encourage instructors to allow students to facilitate their own games in smaller groups. A single deck allows for up to six games to be played simultaneously, each with a completely different scenario, since there are at least six cards in each attack category. However, a more economical approach would be for students to create scenarios using *B&B Shuffle*, the online version.

9. FUTURE RESEARCH

Our motivation for this research project was to simply assess the mechanics of B&B to ensure that it was suitable for an academic environment. Now that we have determined that B&B can be a valuable addition to existing courses, we intend to further study the game's efficacy through more rigorous methodology. For example, we plan to conduct an experiment that compares student learning under the traditional lecture approach to a method that also integrates B&B. This study would allow for a more quantitative analysis.

10. CONCLUSION

In this paper, we have demonstrated how *Backdoors & Breaches* can be employed to teach students the value of conducting tabletop exercises and to prepare them for incident response scenarios. Given the critical importance of business continuity and the multi-functional representation on incident response teams, we encourage instructors to consider implementing the game in information systems courses at all levels and disciplines, not just those that focus on cybersecurity. Doing so would not only enhance the education experience for students, but also prepare them to participate in incident response activities throughout their careers.

11. ACKNOWLEDGEMENTS

We appreciate Black Hills Information Security and Active Countermeasures for granting us permission to reproduce the playing cards and associated resources for this article. We must also thank them for developing such an enjoyable and effective game.

12. REFERENCES

- Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy*, 3(6), 1–19. 10.1002/spy2.126
- Black Hills Information Security. (2019). *How to Play Backdoors & Breaches, Incident Response Card Game by Black Hills Infosec*. youtube.com/watch?v=TAiJVrOzWMw
- Black Hills Information Security, & Active Countermeasures. (2021). *Backdoors &*

- Breaches*. blackhillsinfosec.com/projects/backdoorsandbreaches/
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, 800(61), 1–147.
- Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, 59, 102334. 10.1016/j.ijinfomgt.2021.102334
- Phung, R. (2021). *B-B-Shuffle*. <https://github.com/p3hndrx/B-B-Shuffle>
- Puchkov, O., Subach, I., Zhylin, A., & Tsyganok, V. (2021). Criteria for classification of cyber-training and analysis of organizational and technical platforms for their conduct. *CEUR Workshop Proceedings*, 2833, 37–47.
- Rezaei Soufi, H., Torabi, S. A., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for business continuity planning. *International Journal of Production Research*, 57(3), 779–800. 10.1080/00207543.2018.1483586
- Spearfish General Store. (2021). *Backdoors & Breaches, Incident Response Card Game*. spearfish-general-store.myshopify.com/collections/backdoors-breaches-incident-response-card-game
- Straub, J. (2020). Assessment of cybersecurity competition teams as experiential education exercises. *ASEE Annual Conference and Exposition, Conference Proceedings, 2020-June*. 10.18260/1-2--34187
- White, G. B., Dietrich, G., & Goles, T. (2004). Cyber security exercises: Testing an organization's ability to prevent, detect, and respond to cyber security events. *Proceedings of the Hawaii International Conference on System Sciences*, 37(C), 2635–2644. 10.1109/hicss.2004.1265411
- Wilson, B. (2000). Business continuity planning: a necessity in the new e-commerce era. *Disaster Recovery Journal*, 13(4), 24–26.

Appendix A – Example Cards

Initial Compromise	Pivot & Escalate	Persistence
<p>BRING YOUR OWN (EXPLOITED) DEVICE</p> <p>Your organization allows users to bring in their own devices. Or, another way to put it, they bring in their own exploited devices. The attackers use these devices to compromise your organization.</p> <p>DETECTION</p> <p>Firewall Log Review NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>The completely asinine belief that somehow allowing people to bring their own devices in is a worthy cost savings.</p> <p>https://www.blackhillsinfosec.com/penesting-dropbox-on-steroids</p>	<p>INTERNAL PASSWORD SPRAY</p> <p>The attackers start a password spray against the rest of the organization from a compromised system.</p> <p>DETECTION</p> <p>User and Entity Behavior Analytics SIEM Log Analysis</p> <p>TOOLS</p> <p>Domain Password Spray</p>  <p>https://github.com/dathack/DomainPasswordSpray https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack</p>	<p>NEW USER ADDED</p> <p>Easy, the attackers add a new user to the local computer.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>Metasploit Cobalt Strike</p>  <p>https://www.metasploit.com https://www.cobaltstrike.com</p>
C2 & Exfil	Procedure	Inject
<p>GMAIL, TUMBLR, SALESFORCE, TWITTER AS C2</p> <p>The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.</p> <p>DETECTION</p> <p>NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>Gcat Sneaky Creeper</p>  <p>https://github.com/byt3bl33d3r/gcat https://github.com/DakotaNelson/sneaky-creeper</p>	<p>ENDPOINT SECURITY PROTECTION ANALYSIS</p> <p>We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?</p> <p>TOOLS</p> <p>Check with your vendor, they miss you and always want to chat.</p> 	<p>LEGAL TAKES YOUR ONLY SKILLED HANDLER INTO A MEETING TO EXPLAIN THE INCIDENT</p> <p>Who brought a lawyer to the party? There's always one person who pretty much runs the whole IR process. That one essential person. Well, the legal team took that person away for "Very Important Reasons."</p> <p>NOTES</p> <p>They may never come back... all of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!</p> 

Appendix B – Example Exercise Turns



Use this chart to keep track of turns, rolls, and notes.

BHIS encourages your team to revisit what they learn during the game to evaluate what they may need to adjust in their organization.

Perhaps your team will realize they should write down more of their procedures or add completely new procedures.

Turn	Roll	Notes
1	11	Played the Isolation card, but it was ineffective.
2	14	Successfully played the Endpoint Analysis card, revealing the New User Added card.
3	6	Played the Server Analysis card, but the roll was too low.
4	19	Successfully played the UEBA card, which detected the Internal Password Spray card.
5	7	Played the Firewall Log Review card, but the roll was too low.
6	12	Successfully played the RITA card, so the incident master revealed the BOYD card.
7	7	Replayed the RITA card, but failed to defeat the C2 and Exfil card due to a low roll.
8		
9		
10		

Created by: **BLACK HILLS** | Information Security
www.backdoorsandbreaches.com

Appendix C – Student Comments

What did you enjoy about the exercise?
I liked how it made me take everything we know about the situation and cards into account instead of just shooting at whatever I was looking at.
I liked the skill needed and the real-world equivalencies that it introduced. The teamwork and debate were super interesting too.
It was a new and interesting way to see how an attack occurs and how hard it is to prevent the attack once it has occurred.
Fun approach to learning about security concepts.
I liked how it used everything that we have learned thus far in the class. I also liked how it stressed me out a little, it forced me to try and think of what to do on the spot.
The difficulty of the process. Trying to understand the scenario, then think about what it would take to solve it was challenging and forced us to really think about what it would take to get a resolution.
It was a creative way to practice stuff.
That there could be multiple answers to different scenarios.
I liked how it let us try multiple strategies for a given scenario.
It makes you think through every scenario
It was interesting and took the pressure off learning each individual way to know how to solve a problem and instead just throwing stuff to see what works.
It was a nice change of pace from our typical class exercises.
I thought it was enjoyable thinking through what solutions would be most effective and what would be most important.
I enjoyed the "real life" aspect of the dice roll and taking away certain cards because they may not have worked in real life. Also, just figuring out the other options that would work.
I enjoyed being able to practice situations that could happen and figuring out how to solve them.
I liked how it made me think about which incidents would work against what scenarios and it gave me an extensive thought procedure when thinking about these real-world events.
It was definitely a unique exercise; I've never done something like this before in any of my classes. I enjoy the hands-on nature of the stuff we do in this class.
I enjoyed that the exercise encouraged some collaboration and allowed multiple people to share their ideas.
I enjoyed simulating somewhat of an incident response scenario and deciding what the best mode of attack was in real-time.
I really enjoy the interactiveness of this exercise.
Even though I did not know much to begin with, it was interesting to see how many classmates were so knowledgeable on the subject. I enjoyed watching them collaborate.

How did the exercise enhance your understanding of security concepts?
It made me think about what each card said specifically.
I liked how it highlighted the stressfulness and timeliness of such a compromise and how it showed how random different instructions could be.
This helped me understand how there is no clear-cut response to an attack every time and that the responders will need to try a variety of methods to stop an attack.
I read over the cards to try and apply one of them to the given situation. My understanding of the concepts is still not all there but the exercise did help.
It forced me to think about how to use the security tools I have learned about in a real-world setting, and more specifically made me think about what concepts would (and would not) apply to a real-world situation.
At first blush, it kind of scrambled my thinking. By the third exercise, it started to make more sense to me what steps might need to be taken to get to the end of the process. Trying to keep straight how things might fit together for a solution and the importance of the tools you have available is what stood out to me. This also made me realize there is so much more to the security side than you realize.
It gave me an idea of how to deal with specific situations, and how to figure out what to do during a breach.
That a lot of the scenarios can do the same thing, but some are just better to use in certain situations.
It showed me multiple routes to solve a scenario and demonstrated how uncontrollable events could hamper progress.
It helps you think about what tools or practices to use in specific scenarios
It put concepts into practice in a simulated random environment in a fun way.
The game had us think about what each scenario was doing and which tools had a chance to work.
It helped me remember some of the different crisis response methods and network monitoring methods.
Especially when pairing it with the die rolls, it enhanced my security concepts because typically if one method does not work, another one will. Obviously, there are some scenarios where only one method worked.
I learned how to think about and solve security breaches.
It made me think in a procedural way about how we can use our defense mechanisms in order to stop or prevent attackers from escalating their attacks.
Going through realistic scenarios helps me understand the issues better. I'm someone who learns by doing things, rather than just reading out of a book.
I found that the exercise helped me understand some of the use cases and the security techniques we have discussed.
It introduced me to some concepts such as written procedures and pivot and escalate methods.
I enjoyed the exercise making us think about the various skills and how they interact with other skills.
It really showed me just how difficult cybersecurity can be in the real world. It was difficult for us, and everyone was going back and forth. I can only imagine how difficult it is in the real world.

How did completing the exercise help you realize the value in conducting tabletop exercises?

It showed me it is possible to practice without setting up a test environment.

I already knew the value of tabletop exercises, but it is really well put together and I think it's pretty interesting.

Completing this exercise helped show a simplified version of what we have been learning about all year. This helped me grasp the terms and dangers of attacks while giving me a fun game to play with my peers.

It was a nice change from what we have been typically doing all semester, so I guess the variety was some of the value in this exercise.

As we proceeded through the three scenarios, I felt as though I was to better identify which card to use, or at least understand why a card would/wouldn't be used.

It's kind of like the fire drill in school. Hopefully, you never have to do it for real but practicing it might make the actual event work as expected. We did these types of scenarios at my old company before I came here, but that was in the late 90's so some of the threats we have today were not even thought of yet or in their infancy. Doing this today makes me want to do some of this type of stuff just for my own unit on a smaller scale maybe. What to do if you get that phishing email, or you see something that doesn't look right. Being ready for a disaster before it happens can only be a good thing.

This exercise just makes you think more about how it all goes together.

It boosts teamwork and teaches multiple topics at the same time, bettering my understanding of the material.

It can be more engaging than a lecture.

It's basically like practicing for the real thing in terms of concepts rather than execution but still helps.

The real world is unpredictable, sometimes the right tool just doesn't work.

It was interactive, which is often more memorable than lectures.

I feel like completing this exercise gave me a better understanding of incident response and how to act when an incident does arise and what other options there are for it.

Tabletop exercises are effective in building problem-solving skills and getting used to the unpredictability of cybersecurity.

I think it is a great way to become acclimated to the procedures that must be taken when an alert or hint comes in. I think it sets up the general mindset in order to prepare for the unexpected by running through scenarios before the real thing happens, which is very valuable.

Similar to above, actually *doing* things in classes instead of just hypothetical situations and examples reinforces material and helps it stick. Not just for this exercise, but there have been a few times where I've applied the CompTIA labs to my internship, so I thoroughly enjoy the way this class is set up.

Matching up security methods with attacks helped show how some of those methods can be used in a more obvious way than in lectures or labs.

It helped me realize the value as it emphasizes the importance of preparation in any cybersecurity breach. Covering single points of failure, responsibilities, chain of command, and executive leadership are crucial in determining the best course of action in the event of an actual attack.

Tabletop exercises allow for a hands-on application besides the traditional methods of education. I really like these alternative exercises.

Again, it showed me how hard it can be to prevent cyber security crimes.