BYU

Teaching with Cybersecurity Playable Case Studies

Derek Hansen[1], Elizabeth Bosignore[2], Justin Giboney[1], Kira Gedris[3], Aatish Neupane[1], Andy Fellows[2], Skylar Hoffman[2], Trevor McClellan[1], Angelina Lopez[1]

1. Brigham Young University, 2. University of Maryland, 3. University of Virginia

Research funded by National Science Foundation (NSF) Awards #1915563 and #1915620.

CAE IN CYBERSECURITY COMMUNITY

What are Playable Case Studies?

Playable Case Studies (PCSs) are interactive simulations that allow students to "play" through an authentic "case study" (i.e., scenario) as a member of a professional team. They include (a) an immersive, simulated online environment, and (b) accompanying in-class activities and discussions facilitated by a teacher to provide educational scaffolding and metacognition. PCSs are designed to be authentic and feel "real" by incorporating the "This is Not a Game" (TINAG) ethos from Alternate Reality Games.

What are Playable Case Studies?

CAE IN CYBERSECURITY COMMUNITY

Playable Case Study – Online Platform Components

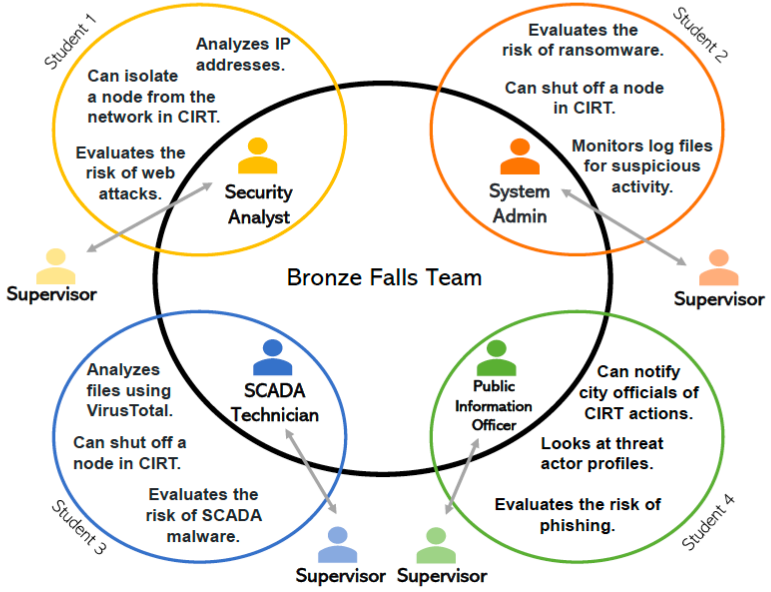
(1) Time-Released Narrative: *The city of Bronze Falls is under attack by r0binh00d, a hacker group who has been attacking cities across the nation. Junior Associates in the Bronze Falls Professional Development Program will take on 1 of 4 professional roles and collaboratively perform a risk assessment, respond to a live cyber attack and identify who was behind the attack.*

Day 1	Day 2	Day 3	Day 4	Day 5
☑☑☑☑	☑☑☑	☑☑☑☑	☑☑☑☑	☑☑☑

(2) Immersive, Transmedia Interface

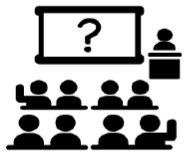
(3) Embedded Activities & Assessments

(4) Role-Based Interactions



In-Class Component

(5) Case Study Discussions



Class reflections, activities & discussions about the case

(6) Expansive Framing

Connect learning to people, places topics, & times outside the case

(7) Out-of-game Assessment

Complete self & peer assessments of student performance & outcomes

Cybermatics

Students join the fictional penetration testing company, Cybermatics, to perform a pentest of Riptech.xyz, helping to identify vulnerabilities and uncover a hacker who has burrowed into their site.

Learning outcomes:

- Penetration testing documentation and reporting
- Penetration testing process
- SQL injection
- Command-line Basics
- Password cracking
- Cybersecurity ethics

Day 1

Cybermatics

THE TEAM | DOCUMENTS | TERMINAL | CHAT | EMAIL | PENTEST REPORT | CYBERMATICS

Progress

Day 1 Tasks

- [x] Read your Welcome Email
  Read the email from Jennifer, Director of Human Resources
- [x] Complete Entrance Survey
  Complete the survey sent through email
- [x] Greet your Team
  Say hi to the team through the Chat tab
- [x] Read Scope Document
  Find the Scope Document in the Documents tab
- [ ] Submit a Daily Report
  Email Kimberly about the day's progress

Cybermatics

Channels

Team

Direct Messages

KS Kimberly Smitherton - CISO

IM Ian Montgomery - Lead Technical Specialist

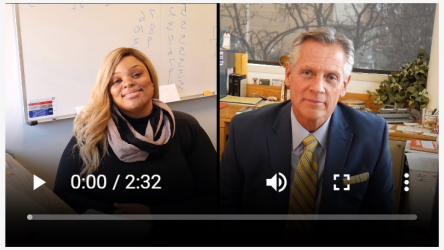
SM Samuel McCarthy - Lead Social Engineer

JF Jennifer Franco - Director of Human Resources

Team

3 members in this channel

Kimberly Smitherton 3:03 PM
We also recorded the conference call we had with our client this morning. Once you watch this you should be up to speed.



Kimberly Smitherton 3:03 PM
We're going to start with a pentest. Do you remember what that is?

Cybermatics 3:03 PM
Yes

Kimberly Smitherton just now
Just as a refresher, the purpose of a pentest is to help a company learn more about it's own vulnerabilities. When companies build websites, they often cannot predict how these sites will be attacked by hackers or other malicious entities. That's where we come in. We find the weaknesses and holes in their security. Riptech has asked us to find flaws in their system before the impending launch of their new app. That's it, just make sure you are familiar with the scope document before we begin. Let me know when you've read it!

Cybermatics just now
Done!

Kimberly Smitherton just now
Perfect. Sounds like you're up to speed. We'll see you tomorrow for the real work. Again, happy to have you aboard.

Send a message...

Day 2

CAE IN CYBERSECURITY COMMUNITY

- Intro to Documentation
- Scope Document
- SQL Injection
- Password Cracking
- Linux
- Technical Reports

Introduction

SQL (pronounced 'sequel') Injection is a way hackers can gain unauthorized access to information that is stored in a database. They can do this by entering a query written in SQL into an input field on a website, such as a username field. In other words, instead of typing in a username they will enter SQL code. When the code is then run by the system, hidden information can be shown or modified by an unauthorized user. For example, the image below shows how SQL code is entered into a website that is expecting to see a username.

SQL Basics

Before performing SQL injection, it is important to understand SQL queries. SQL queries have four basic parts—an action, a condition, a location, and a filter (optional). For example, the following statement includes an action (SELECT), a condition (*), a location (FROM Users), and a filter (WHERE firstname = Jon).
SELECT * FROM Users WHERE name = Jon;

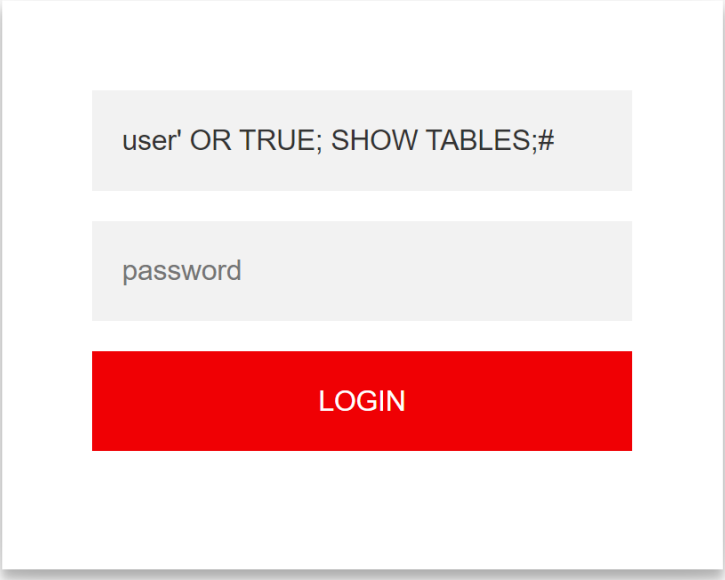
The various commands that can be used in each of these parts are described below:

Action
SELECT - Retrieves (i.e., views) information stored in a database table.
SHOW - Retrieves (i.e., views) information about the attributes of a database or table (e.g., name of the database; names of columns in a table).
UPDATE - Updates (i.e., modifies) data stored in a database table.
DELETE - Deletes information from a database table.

For SELECT, UPDATE, and DELETE statements you also need to specify what information you want to retrieve. This is done through the condition section.

Condition
SELECT, UPDATE, and DELETE statements need to know what information should be chosen. This is done through the condition section. SHOW statements do not need a condition section, since they work with the database attributes (e.g., column names), not the actual information in the database (e.g., a users' information stored in a column).

There are two ways to specify which data fields you want to grab information from:
* : Use the asterisk to show that you would like to grab information from all data fields in the table
column_name1, column_name2, column_name3 : Use comma separated column names to indicate which columns of



Day 3

Cybermatics

THE TEAM | DOCUMENTS | TERMINAL | CHAT | EMAIL | PENTEST REPORT

Progress

Day 3 Tasks

- [x] Get caught up
  Navigate to the Chat tab and get caught up with your team
- [x] Learn about Passwords
  Go to the Documents tab and learn about Passwords
- [x] Crack Passwords in Shell
  Use the Terminal tab to crack the passwords you retrieved
- [ ] Report Results
  Go to the Chat tab and let everyone know what you found
- [ ] Submit a Daily Report
  Email Kimberly about the day's progress. Include in today's email all cracked passwords and the corresponding usernames.

- Intro to Documentation
- Scope Document
- SQL Injection
- Password Cracking
- Linux
- Technical Reports

Password Security

Password security refers to how hard it is for the password to be guessed or otherwise obtained. Some ways you can make your passwords more secure include making your passwords longer, adding special characters (#%!@$), and using capitals or numbers. When possible, passphrases are the recommended option.

Passphrase

A passphrase is used like a password, but includes multiple words for added security.

An example of a passphrase:
correct horse battery staple

Hashes

Hashing is a way to store passwords securely by scrambling the password in a way so it cannot be read in its plain, original form. A hashing algorithm takes a string of characters and transforms it into a generally shorter value that represents the original string. It is a one-way function that is fast to calculate but almost makes it impossible to guess what the original data was.

SHA 1
SHA 1 (Secure Hash Alogorithm 1) is one type of hashing algorithm that you can apply to a password. It is an outdated hashing algorithm and is not recommended for password hashing when compared to newer methods. SHA 1 always scrambles the password into a 40 character string.

An example of what a SHA 1 hash would look like is displayed below:
38bca521a353930e209c8b49c7b4a1ed4dfa0f38

SHA 256
SHA 256 is newer type of hashing algorithm, but is still not recommended for use with passwords. SHA 256 always scrambles the password into a 64 character string.

An example of what a SHA 256 hash would look like is displayed below:
6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b

```
junior@cybermatics.io$ ls
wordlist.txt
junior@cybermatics.io$ hashcrack -t sha1 -w wordlist.txt -h 18576D4CF81BA7CA57797ADCA773FE2ECD752CC0
hashcrack starting on hash: 18576D4CF81BA7CA57797ADCA773FE2ECD752CC0
press ctrl-c to cancel operation
hashcat: password cracked: blackhawk
junior@cybermatics.io$ |
```

Day 4

Cybermatics

THE TEAM | DOCUMENTS | TERMINAL | CHAT | EMAIL | PENTEST REPORT

Progress

Day 4 Tasks

- [x] Get caught up
  Navigate to the Chat tab and get caught up with your team
- [x] Learn about Linux
  Go to the Documents tab and learn about Linux
- [ ] Explore the RipTech server
  Using SSH and the Terminal, look around the files in RipTech
- [ ] Report findings
  Go to the Chat tab and tell everyone what you found
- [ ] Submit a Daily Report
  Email Kimberly about the day's progress. Include in today's email your findings from the Riptech server.

Intro to Documentation

Scope Document

SQL Injection

Password Cracking

Linux

Technical Reports

Linux

Linux is a type of operating system (like Windows or Mac), but it is much simpler. Many versions of Linux can be run exclusively using a terminal.

User Access

When a file is created in Linux, users are granted permissions to read (r), write (w) and/or execute (x) the file. The all-powerful admin user in Linux is called root. It has the permissions to r, w, and x all files.

Linux files of importance

When navigating through a Linux file system as a pen tester, there are some files that you want

/etc/passwd is a file that will show you all of the users on the machine. This is useful to se
passwords you can reuse, or if there are any users that are not supposed to be there.

/etc/shadow is a similar file that lists all of the password hashes for the users on the mach
want to do some serious password cracking but will generally be too hard for you to crack

/var/log/auth.log on Ubuntu systems will allow you to see a log of all of the login and logou
users and */var/log/secure* on Centos systems. These files include timestamps useful to co
and other logged events.

/var/www/html is a folder where the files accessible to a web site are generally located. Th
hackers are likely to place backdoors in order to easily access the server from the Internet.
the server using commands like cd and ls to find these files.

In the simulation some of these files will be useful in the completion of some tasks.

Malicious files

As a pen tester you are always on the lookout for things that seem out of place. Thinking like a
figure out where some of these files may be. If you do find a file that looks malicious be very ca
handle it. It could be a virus that will spread if you download it to another computer for analysis

```
adm:*:16231:0:99999:7:::
lp:*:16231:0:99999:7:::
sync:*:16231:0:99999:7:::
shutdown:*:16231:0:99999:7:::
halt:*:16231:0:99999:7:::
mail:*:16231:0:99999:7:::
operator:*:16231:0:99999:7:::
games:*:16231:0:99999:7:::
ftp:*:16231:0:99999:7:::
nobody:*:16231:0:99999:7:::
dbus:!!:16443::::::
polkitd:!!:16443::::::
libstoragemgmt:!!:16443::::::
avahi:!!:16443::::::
avahi-autoipd:!!:16443::::::
abrt:!!:16443::::::
postfix:!!:16443::::::
sshd:!!:16443::::::
ntp:!!:16443::::::
chrony:!!:16443::::::
tcpdump:!!:16443::::::
centos:!!:16452:0:99999:7:::
apache:!!:16452::::::
tshawcroft:$6$8Fba77H1$GemEkkNtQLQKjwPHq3Se6gKa5fhdSsGJzzKY4AdfcidfeUXyOryBLbTAmSas5of/D0ZJ16IXiBFalR0eAO
tss:!!:16526::::::
systemd-bus-proxy:!!:16784::::::
systemd-network:!!:16784::::::
rpc:!!:16933:0:99999:7:::
kosmo:$2$eTC4w5ao$kjR4Yl15M3Z4Pbd22zaGG05XUL2xZLWftg2szZB3GZtmiH5Bk9nvCcfwXp5jkw2/A69RRbV1BON9IlNTOkqi31:1

tshawcroft@riptech.xyz$ |
```

Day 5

Cybermatics

THE TEAM | DOCUMENTS | TERMINAL | CHAT | EMAIL | PENTEST REPORT | CYBERMATICS

Progress

Day 5 Tasks

- [x] Get caught up
  Navigate to the Chat tab and get caught up with your team
- [ ] Read about Technical Reports
  Go to the Documents tab and learn about Technical Reports
- [ ] Create Final Report
  Use the template found in the Documents tab to complete and submit your report, then send Kimberly an email indicating you are done
- [ ] Complete Exit Survey
  Complete the survey sent through email

Submit Riptech Penetration Test Final Report

Riptech Penetration Test Final Report

RIPTECH PENETRATION TEST FINAL REPORT

EXECUTIVE SUMMARY

Scope of Work

Cybermatics completed a penetration test on the systems from Riptech LLC, in accordance with the agreed scope document conditions. The test included all forms of cyber attack targeting the RipTech website, as well as a physical attack that included only social engineering techniques; breaking and entering the premises was disallowed.

Project Objectives

- Gain remote access to Riptech servers.
- Escalate privileges to attempt to gain admin access to Riptech's databases.
- Explore the available databases using admin rights to find any insecure information.
- Use social engineering to test Riptech's employees' compliance with safety protocol.

Summary of Findings

Characters: 2793

Bronze Falls

Students work in teams to protect the city of Bronze Falls by performing a cybersecurity risk analysis, responding to a live cyberattack, and completing an after-action attribution report.

Learning outcomes:

- Understand NIST Framework
- Risk Assessment using the Risk Calculator
- Incident Response simulation (CIRT)
- Cybersecurity Attribution Report
- Debrief

Day 1

ProDev Dashboard

Tasks

Day 1

Student 1: Security Analyst
Group: Group 1

100%

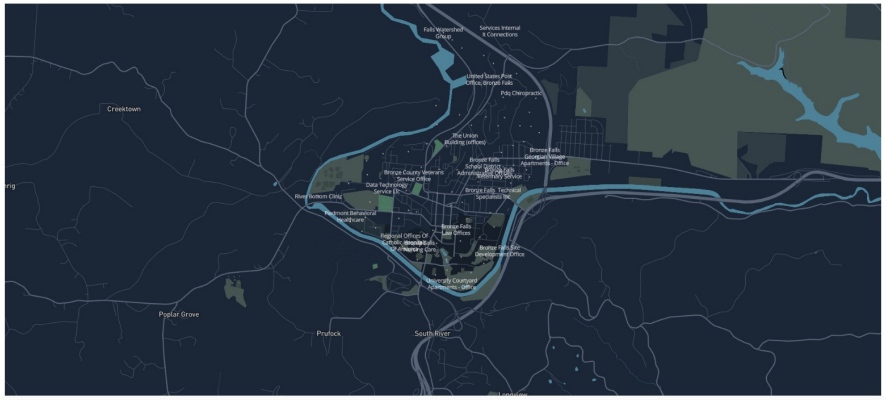
Completed 5 out of 5

- **Complete Dashboard Tour**
  Take the tour of your ProDev Dashboard.
  Completed on: 2023-03-03 12:51:25
- **Read 'Welcome to Bronze Falls' Email**
  Read the email from Penny Davis.
  Completed on: 2023-05-05 14:06:41
- **Complete ProDev Entrance Survey**
  Complete ProDev Entrance Survey
  Completed on: 2023-05-05 14:06:57
- **Read 'Welcome and Role Selection' Email**
  Read the new email from Penny Davis and watch the embedded welcome video from the mayor.
  Completed on: 2023-05-05 14:07:00
- **Complete Role Ranking Survey**
  Complete the role ranking survey linked in the 'Welcome Video and Roles' email.
  Completed on: 2023-05-05 14:07:57

Website Directory

- Bronze Falls City Website
- State Highway Administration Website
- Bronze Falls Memorial Hospital Website
- Electric Company - Burns Energy
- Gas Company - Imperial Gas
- Telecommunications Company - C4Myles

Map of Bronze Falls



Day 2

CAE IN CYBERSECURITY COMMUNITY

Risk Calculator

Submit

Submitted: 5/5/2023, 2:30:18 PM

Total ALE	Total Savings
Annualized Loss Expectancy ($ lost this year)	($ saved this year due to investments)
$125K	$10K

Budget

$125K	-	$118K	=	$7K
Budget		Spent		Remaining

SCADA Malware: SCADA Technician ● Savings: $0

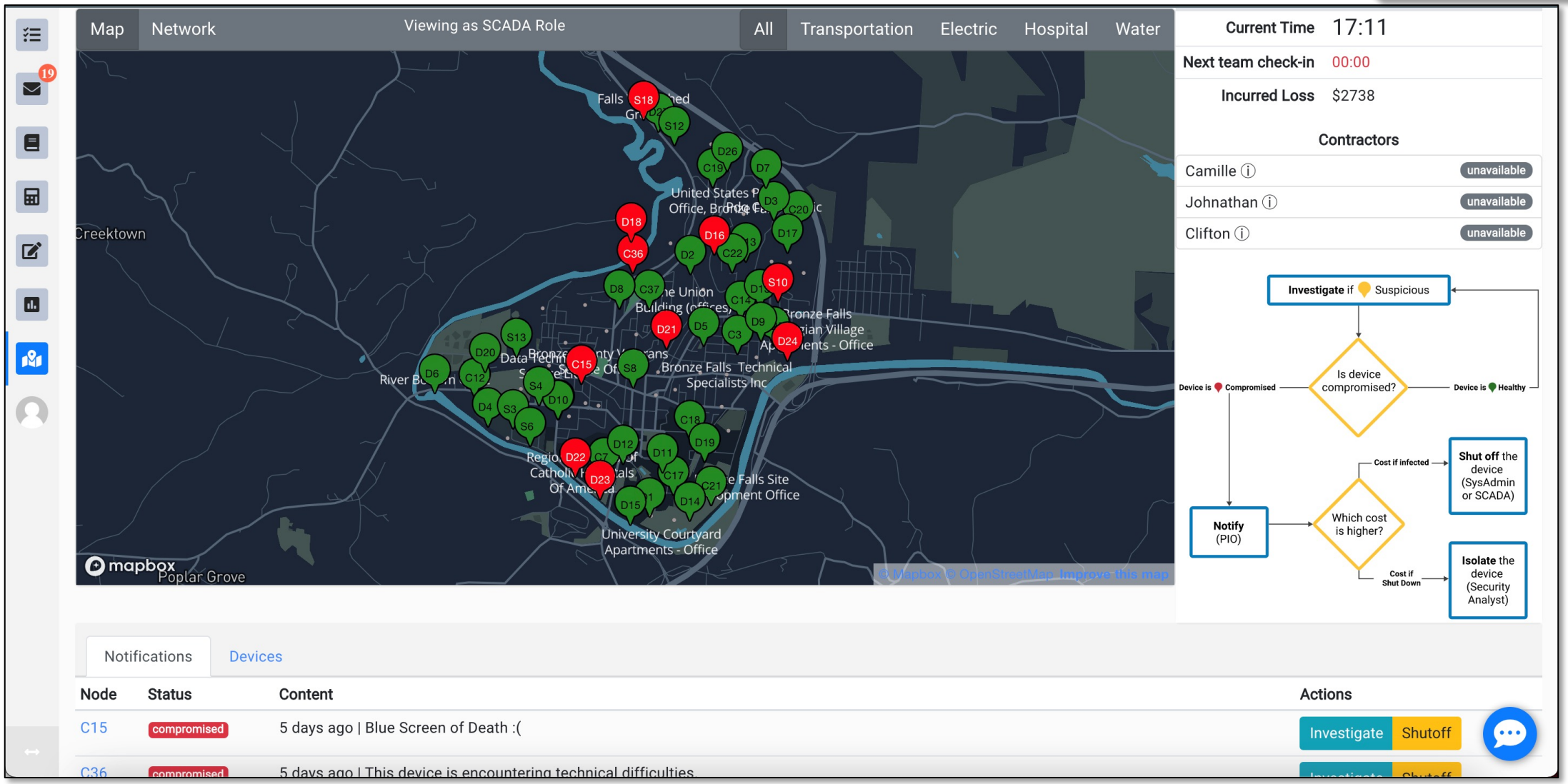
Phishing: Public Information Officer ● Savings: $0

Web Attacks: Security Analyst ●

Base ARO	Base EF	Unadjusted Risk							
Annual Rate of Occurrence 10	Exposure Factor 25 %	$50K Current Asset Value	X	25% Base EF	X	10 Base ARO	=	$125K Annualized Loss Expectancy	Savings $10K
Invest in: Gold	More info	Risk After Investment							
		$50K Current Asset Value	X	25 Base EF	X	9.20% Adjusted ARO	=	$115K Adjusted ALE	

Ransomware: System Administrator ● Savings: $0

Day 3


Map
Network
Viewing as SCADA Role
All
Transportation
Electric
Hospital
Water
Current Time 17:11
Next team check-in 00:00
Incurred Loss $2738
Contractors
Camille unavailable
Johnathan unavailable
Clifton unavailable
Investigate if Suspicious
Is device compromised?
Device is Compromised
Device is Healthy
Notify (PIO)
Which cost is higher?
Cost if infected
Shut off the device (SysAdmin or SCADA)
Cost if Shut Down
Isolate the device (Security Analyst)
Notifications
Devices
Node
Status
Content
Actions
C15
compromised
5 days ago | Blue Screen of Death :(
Investigate
Shutoff
C36
compromised
5 days ago | This device is encountering technical difficulties
mapbox
Poplar Grove
Creektown
University Courtyard Apartments - Office
Bronze Falls Technical Specialists Inc

Day 4

System Admin

"…
We've been combing through some of the computer and server log files on our system and we believe we've found the server from which the attacks spread. Sometimes an attacker will get in before the attack to scout out the network. Take a look at this log file from a week prior to the attack and see if the attackers were already accessing our systems.
…"

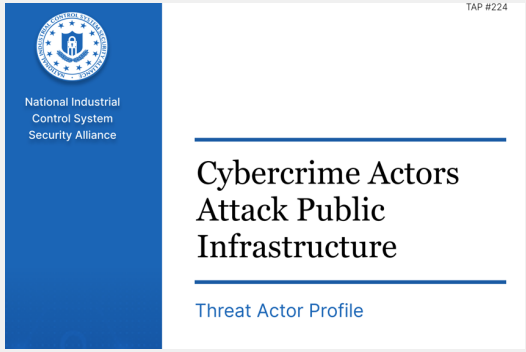
Log File

```
var/log/auth.log

12:17:01 S2 CRON[1762]: pam_unix(cron:session): session opened for user root by (uid=0)

12:17:01 S2 CRON[1762]: pam_unix(cron:session): session closed for user root

14:35:45 S2 sshd[836]: Accepted password for greg_w from 10.2.10.12 port 60280 ssh2

14:35:45 S2 sshd[836]: pam_unix(sshd:session): session opened for user greg_w by (uid=0)

14:35:45 S2 systemd-logind[357]: New session c2 of user greg_w.

16:42:15 S2 sshd[836]: pam_unix(sshd:session): session closed for user greg_w

16:42:15 S2 systemd-logind[357]: Session c2 logged out. Waiting for processes to exit.

16:42:15 S2 systemd-logind[357]: Removed session c2.

21:47:32 S2 sshd[862]: Accepted password for rose_h from 10.2.45.12 port 60291 ssh2

21:47:32 S2 sshd[862]: pam_unix(sshd:session): session opened for user rose_h by (uid=0)

21:47:32 S2 systemd-logind[357]: New session c3 of user rose_h.

21:48:02 S2 sudo:         serv_internal2 : TTY=pts/1 ; PWD=/home/serv_internal2 ; USER=root ; COMMAND=/lib/ufw allow 55545
```

Public Information Officer

"…
I found what appear to be good leads! I'm attaching two TAPs for you to read through that seemed to have some tactical similarities to what we experienced when R0b1nh00d attacked. I've uploaded them to the document repository as well, in case you want to share them with your team.
TAP #224
TAP #312
…"

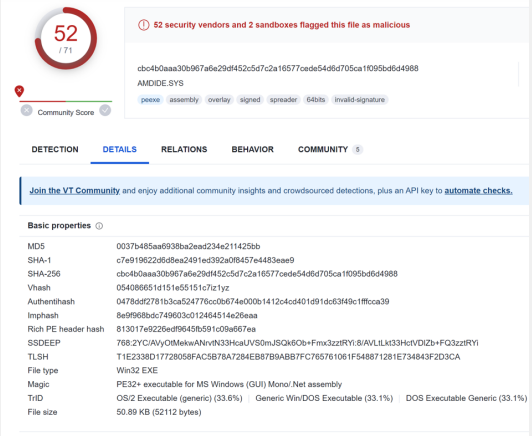
TAP Report



SCADA Technician

"…
Once you find a match for the file hash, VirusTotal will show information that different anti-virus and malware detection applications have reported about the file. I highly recommend checking out the Community tab where users that submitted the file hashes talk about what the file is, where it may have come from, or what systems it can infect. If you're lucky, sometimes they include links to websites with more details.
…"

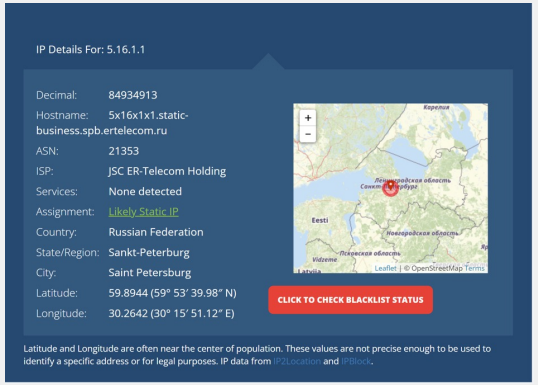
VirusTotal Analysis



Security Analyst

"…
First -- It looks like several of the compromised devices have been trying to access source devices within different IP address ranges. Use https://whatismyipaddress.com/ip-lookup and see if you can uncover the locations these IP ranges are associated with. Your findings may give us a better idea what countries R0b1nh00d already has a foothold in.
…"

IP Address Info



Day 5

Attribution Analysis | After Action Report | Notes

Insert Type...

After Action Report

Incident Report: The Sherwood Shakedown

Bronze Falls Department of Security and Incident Management

By: Insert Junior Associate names here

Month Day, Year (Date Updated)

Incident Overview / Abstract

Dates, scope, threat and threat actor; Short summary of what Student 3 and how the team can improve. What actually occurred? What actions did you take? What were the results of your actions?

Strengths

Team strengths specific to the current collaboration

Student 2

How was the team effective in this situation? What went well? Which parts of the process did the team excel in?

Team strengths that you will continue in future collaborative efforts

Student 4

How would you ensure that you used these strengths productively in the future?

Areas of Improvement

Areas of improvement specific to the current collaboration

How could the team have performed or coordinated better? Could you have done anything to prevent the incident? Could the Risk Assessment have been modified in some way to more effectively mitigate or prevent the attack?

PCS Authoring Tool

International Society of the Learning Sciences

The Playable Case Study Authoring and Simulation Platform

Elizabeth Bonsignore, University of Maryland College Park, ebonsign@umd.edu
Derek Hansen, Brigham Young University, dlhansen@umd.edu
Daniel Hickey, Indiana University, dthickey@indiana.edu
Philip Piety, University of Maryland College Park, ppiety@umd.edu
Grant Chartrand, Indiana University, gchartra@indiana.edu

Kira Gedris, Mitch Cross, Justin Giboney, Jon Balzotti, Jason McDonald, Kevin Kartchner
kira.gedris@gmail.com, mitch.s.cross@gmail.com, justin_giboney@byu.edu, jonathan_balzotti@byu.edu, jason@byu.edu, kevinkartchner.ca@gmail.com
Brigham Young University

Abstract: Playable Case Studies (PCSs) are online simulations that allow learners to adopt (*play*) a professional role within an authentic scenario (*case*) as they solve realistic problems alongside fictionalized experts in an unfolding narrative. The PCS architecture offers scalable options for creating learning activities for individual learners and student teams, and the means for observing and analyzing these activities. This interactive demo will showcase PCSs the team has developed for topics ranging from cybersecurity to technical writing to disaster response, illustrating how we embed learning assessments and research surveys and run them in classroom environments. Participants and potential collaborators will interact with and provide feedback on the prototype PCS Authoring Tool, designed to streamline the creation of new PCSs.

Keywords: *educational simulation, role-play, career awareness, productive disciplinary engagement, expansive framing.*

PCS Research

Simulating Municipal Cybersecurity Incidents: Recommendations from Expert Interviews

Kira Gedris, Brigham Young University, kira.gedris@gmail.com
Kayla Bowman, Brigham Young University, kaylabowman2@gmail.com
Aatish Neupane, Brigham Young University, aatishnn@gmail.com
Amanda Lee Hughes, Brigham Young University, amanda_hughes@byu.edu
Elizabeth Bonsignore, University of Maryland, ebonsign@umd.edu
Ryan W. West, Brigham Young University, ryanwest6@gmail.com
Jon Balzotti, Brigham Young University, jonathan_balzotti@byu.edu
Derek L. Hansen, Brigham Young University, dlhansen@byu.edu

Abstract

As cyberattacks on city and public infrastructures become increasingly common and harmful, it is critical that we train the professional workforce to prepare and respond appropriately. This paper supports the development of educational simulations and related experiential learning exercises that help prepare city and public infrastructure personnel to effectively respond to cybersecurity attacks. Specifically, it synthesizes the findings
including 12 cybersecurity
city organizations, as well
expertise. We organize the
outcomes, scenarios, roles,
designers should consider.
picture of the complex socio-
public infrastructure attacks
salient skills needed to respo

public infrastructures. Indeed, most local governments report being less than confident in their ability to prevent similar breaches [4, 5].

Protecting a city against cybersecurity attacks is becoming more difficult. Unlike companies, city-wide infrastructure systems feature a fragile combination of heterogeneous systems with multiple stakeholders like government (local, state, federal) and private entities, and intertwined dependencies between them [6]. Due to these complex interdependencies, even a small localized

Theory of Experiential Career Exploration Technology (TECET): Increasing cybersecurity career interest through playable case studies

Justin Scott Giboney, Brigham Young University, justin_giboney@byu.edu
Derek L Hansen, Brigham Young University, dlhansen@byu.edu
Tanner Johnson Brigham Young University, tannerwj@gmail.com
Desiree Winters Brigham Young University
Jason K McDonald Brigham Young University, jason@byu.edu
Jonathan Balzotti Brigham Young University, jonathan_balzotti@byu.edu
Elizabe

Abstract

There is a large demand to fill cybersecurity jobs. To alleviate this need, it is important to generate interest in cybersecurity as a career. One way to do this is through job shadowing and internships. Using design science principles, we have built and tested a playable case study (PCS) where participants can act out a virtual internship and lea
ran a study with
courses where th
internship at a p
CyberMatics. In the
helps students 1) be
are needed for, 2) m
and 3) increase t
succeed in a career
we propose the
Exploration Techno

has improved in recent
understanding of the n
cybersecurity professiona
occupational plans in hi
predictor of student's d
Retaining students once t
also a challenge for Scien
and Mathematics (STEM)

Evaluating an Educational Cybersecurity Playable Case Study

Tanner West Johnson, *Brigham Young University*

Follow

Abstract

The realities of cyberattacks have become more and more prevalent in the world today. Due to the growing number of these attacks, the need for highly trained individuals has also increased. Because of a shortage of qualified candidates for these positions, there is an increasing need for cybersecurity education within high schools and universities. In this thesis, I discuss the development and evaluation of Cybermatics, an educational simulation, or playable case study, designed to help students learn and develop skills within the

nding of the field
rity professional
mmersed within
another
el, introductory
reased the
ersecurity field. It
a cybersecurity
onfident about

Playable Case Studies: A New Educational Genre for Technical Writing Instruction

Jon Balzotti and Derek Hansen

Brigham Young University

ABSTRACT

A Playable Case Study (PCS) is a hybrid learning experience where students (1) participate in a fictional narrative that unfolds through an immersive, simulated environment and (2) engage in classroom activities and lessons that provide educational scaffolding and promote metacognition through in-game and out-of-game experiences. We present the Microcore PCS to illustrate the potential of this new type of experiential simulation that incorporates aspects of Alternate Reality Games (ARGs) to increase immersion and teach workplace literacies in the technical communication classroom. We explore results from a pilot test of Microcore with an undergraduate technical communication course, identifying design strategies that worked well and others that led to improvements that are currently being incorporated. We also provide questions to prompt future research of playable case studies and discuss our findings in a broader context of technical communication pedagogy.

KEYWORDS

Computer-based learning; curriculum design; digital technologies; instructional technology

Increasing Cybersecurity Career Interest through Playable Case Studies

Justin Scott Giboney[1] · Jason K. McDonald[1] · Jonathan Balzotti[1] · Derek L. Hansen[1] · Desiree M. Winters[1] · Elizabeth Bonsignore[2]

Accepted: 19 January 2021 / Published online: 8 February 2021

Abstract

In this paper we introduce an approach to cybersecurity education and helping students develop professional understanding in the form of a Playable Case Study (PCS), a form of educational simulation that draws on affordances of the broader educational simulation genre, case study instruction, and educational Alternate Reality Games (or ARGs). A PCS is an interactive simulation that allows students to "play" through an authentic scenario (case study) as a member of a professional team. We report our findings over a multi-year study of a PCS called Cybermatics, with data from 111 students from two different U.S. universities who interacted with the PCS. Cybermatics increased student understanding about certain key aspects of professional cybersecurity work, improved their confidence in being able to successfully apply certain skills associated with cybersecurity, and increased about half of the students' interest in pursuing a cybersecurity career. Students also reported a number of reasons why their perceptions changed in these areas (both positive and negative). We also discuss design tensions we experienced in our process that might be encountered by others when creating simulations like a PCS, as they attempt to balance the authenticity of designed learning experiences while also sufficiently scaffolding them for newcomers who have little background in a discipline.

Interested in using PCS?
Contact Dr. Derek Hansen at dlhansen@byu.edu

Visit us at pcs.byu.edu

CAE IN CYBERSECURITY COMMUNITY