ISSN: 2473-4901
v8 n5751

A Case Study in Identifying and Measuring Skills Honed from a Cybersecurity Competition

Ron Pike
rpike@cpp.edu

Jasmine Weddell
jweddle@cpp.edu

Sydney Duong
slduong@cpp.edu

Department of Computer Information Systems
Cal Poly Pomona
Pomona, CA United States

Brandon Brown
bbrown118@coastline.edu

Department of Computer Service Technology
Coastline College
Fountain Valley, CA

Abstract

Many tools have evolved in the extracurricular space for the cybersecurity field that could belong in cybersecurity education. Additionally, the measurable learning students complete outside of formal classroom education before entering college or university needs to be formally recognized and awarded academic credit. These strategies are novel in their approach for learners to gain or demonstrate their cybersecurity skills meaningfully. The following case explores a dynamic example about the benefits of these tools through a cybersecurity competition named Red vs. Blue. The case outlines methods of assessment relative to the competition and exemplifies the impact on students from a test case competition in their own words.

Keywords: Cybersecurity, Competency-Based Education, Assessment, Cyber Competitions.

1. INTRODUCTION

The focus of this paper is to highlight the efforts of students and faculty in measuring skills derived from a cybersecurity competition created and operated by students at a state university in the Southwestern United States. The university is part of the National Centers of Academic Excellence (CAE) program and focuses on students putting their learning into practice.

The students are engaged in cybersecurity academic programs and are contributors to co-curricular and extra-curricular cybersecurity programs and research. One of the students is studying Computer Science within the College of

Science and the other Computer Information Systems within the College of Business. There are two perspectives presented in the paper: the students examining the impact of a particular cybersecurity competition on the learning environment and the faculty exploring the process of assessing and mapping competencies in a fashion that supports robust learning pathways from middle school to career.

Cybersecurity, like many other professions, has a need for lifelong learning. However, we argue that cybersecurity faces a greater challenge than most disciplines related lifelong learning, due to four key challenges. First, cybersecurity is in an early phase of maturation as a discipline, which creates a need for constant change and development. Second, cybersecurity is influenced by ongoing change within the IT infrastructure domain. Third, cybersecurity faces an adversarial relationship with perpetrators who make a profession out of undermining and evading cybersecurity controls. Finally, the fourth challenge is the multi-disciplinary aspect of cybersecurity, which encompasses multiple technological fields not limited to computer engineering and computer science, but also encompassing business, political science, psychology, and more. All these fields are required to develop security and privacy controls necessary to empower and protect organizations and individuals. Each of these challenges contributes to a constantly changing landscape for the cybersecurity field and the academic programs that service the field. Such rapid changes create a need for flexibility in cybersecurity programs to adapt to new developments within the IT infrastructure domain while also creating and maintaining an academic core that ensures the consistent growth of the field. A grand theory of cybersecurity is needed, but none are visible on the horizon.

Academic programs in cybersecurity have drawn on numerous tools and pedagogies to address these challenges. We explore key tools and pedagogies that allow for academic programs to interconnect with one another and external learning opportunities, creating pathways for learners from their first exposure with cybersecurity to the end of a successful cybersecurity career. We also draw on the concept of holistic assessment to help learners demonstrate their cybersecurity learning achievements to academia and employers, as well as enable academic programs to honor learning already achieved (Pike, 2022). Academic tools such as articulation, transfer of credit, competency-based education, and credit for prior learning will enable academic providers to pattern their programs in a way that builds upon prior learning, as opposed to requiring students to retake classes on concepts they have already learned in order to fit into a particular academic program. The freedom to build upon learning already achieved empowers students as they navigate through learning pathways toward cybersecurity competencies.

2. METHOD OF ASSESSMENT

The methodology of a holistic assessment is to broaden the types of cybersecurity learning environments that can be formally assessed. This not only increases the activities that can be assessed, but also offers more authentic forms of assessment with a focus on measurable competencies. For example, asking a student to define how they would enhance firewall protections in the event of an emergency by writing an essay is not effective, especially for a learning with language or writing deficiencies. A much stronger form of assessment is to place a student in an environment, such as a competition, where they are confronted with an emergency, and the firewall must be configured to mitigate the current threat. This is more authentic both because the student is doing the work rather than writing about it, and because there is a live context that helps the student to make sense of the task at hand. While writing is an effective learning tool in many cases, it is not effective in evaluating students' ability to adapt to active-attack scenarios. Our example of the dynamic Red vs. Blue competition (RvB) sets forth a case study in the analysis of skills attainment through Competency Based Education, Life-Long Learning, and Skills-Based Education practices.

COMPETENCY BASED EDUCATION (CBE) ASPECTS TO EVALUATION OF SKILLS

Competency Based Education (CBE) is defined as an approach which allows a student to advance based on their ability to master a skill or competency at their own pace, regardless of environment. The CBE method can be tailored to meet different learning abilities enabling more efficient student outcomes. (Educause, 2022). This modality of learning is focused on measuring the skill level already attained or through flexible learning methodologies. Students can progress through courses as soon as they can prove that they have mastered the material. CBE replaces the more traditional modality of higher education, where they would normally advance only when a term has ended and allows the student to progress at a faster rate since they can spend more time on skills and materials that are not already mastered.

Competitions offer the ability to measure the level of skill that a student possesses in a simulated/emulated real-world environment. The challenge here is the methodology of measuring the skill and setting a level to it. Beginner competitions, such as Capture the Flag events, are structured in a fashion where student learning outcomes can be measured efficiently since the challenges and problems are more static. However, many competitions that are open and flexible, such as Red vs. Blue style scenarios, are more dynamic and harder to measure. This is especially true for team-based competitions, as multiple students can work on the same problem or issue, and the ability to disambiguate which student demonstrated a particular competency is required.

3. CYBERSECURITY LIFE-LONG LEARNING

In a recent conversation among the authors of the paper, the maturity of the cybersecurity field was likened to a 40-year-old living in the basement of a parent's home. The field gets older but has not established many of the traits of a mature discipline, such as research streams building upon one another and the use of ongoing research from the field being a strategic asset in the teaching and learning process. While critical work has been accomplished in defining core components of cybersecurity through joint work between academia and government, this work is still in development and is not broadly used across academia (Petersen, et al, 2020). In fact, it seems there are many versions of core content for cyber academic programs, meaning that there is no true core, and a single academic core is likely not possible given the need for contributions related to computer hardware, software and protocols, implementation platforms and systems, organizational structures and ethical and psychological considerations which span numerous disciplines.

We do not seek to provide an answer to the question of a core for cybersecurity education, but rather suggest a systematic exploration and methodical documentation of competencies to enhance learners' preparedness. This process may illuminate paths to developing a stronger theoretical foundation for cybersecurity. In our exploration of CBE, we focus on the use of pedagogical tools that have been largely relegated to extra-curricular activities but should be required in formal cybersecurity education. Specifically, the assessment of competencies through competitions and Competency Based Education (CBE) is explored with an intent to create a wider variety of assessable activities that report on the attainment of Knowledge, Skills, and Abilities (KSAs) related to cybersecurity. This paper assumes the use of the NICE (National Initiative for Cybersecurity Education) framework as a source of KSAs, which have been developed through joint work between the federal government and academic partners.

4. INTRODUCTION TO RED VS BLUE (RVB)

Red vs. Blue (RvB) is a cybersecurity competition where teams of five students, the blue team, are provided with a fake business' vulnerable network, usually consisting of a router and five machines running different operating systems, that they must secure. The students are also actively defending their systems against outside threats that the red team (attackers) inflict upon them. Through RvB, students can troubleshoot and practice their incident response skills in an active breach scenario.

RvB uses three main metrics to give points to participants: Secure Configuration Score (SCS), Service Uptime, and Injects. SCS measures specific security configurations that are implemented on the computer. It awards points for things such as removing unauthorized users or turning on the firewall. Please see Appendix A for examples of security misconfigurations for a Windows machine and Appendix B for examples on a Linux machine. Since RvB simulates a real business environment, the competitors' main job is to keep the business' services, such as DNS and HTTP, up and running. Service uptime awards competitors' points for multi-minutes intervals in which services are still functional. Please see Appendix C for a table of all the scored services in the competition. Lastly, throughout the competition, as if defending a network from an active red team wasn't enough, students are given tasks, called injects, from the fake business manager. These injects are designed to allow students to apply their technical skills in a business setting, doing things such as submitting a report summarizing the findings on the threats they've encountered, or giving a presentation on cybersecurity safety guidelines that all employees should follow. Submitting injects within deadlines provides additional points.

5. RVB & TEACHING OF TECHNICAL SKILLS

Cybersecurity competitions are the ideal way of teaching and reinforcing students' technical skills, as students learn so much more through applying the knowledge they have accumulated in the classroom in a hands-on way and troubleshooting when coming across problems. RvB is also an optimal way to holistically assess a student's skills, since the true test of whether a student understands technical concepts is how well they apply their understanding and create solutions or mitigations in real-world situations.

Through competing in RvB, students can apply concepts such as setting up DNS, configuring a pfSense router, and editing the Windows Registry. The list of cyber tools students implement are endless as students use their initiative and creativity in developing solutions. A common situation competitors come across is finding that their computer is filled with hundreds of users, each with domain level privileges and default passwords. Having all these high-level privileges with default passwords poses a serious vulnerability to their network, since a threat actor can easily log in on any one of the hundreds of accounts and then gain domain-level access to the machine. Therefore, competitors must quickly research on the spot how to mass change user passwords to secure this vulnerability. Students then discover how to use commands such as *dsmod* and *dsquery* and how they are applied to real-world scenarios. This is one of the countless examples of how competitors learn through the unexpected situations they encounter.

Additionally, students do not only learn from the technical problems that they are able to overcome during the competition. Their failures and shortcomings serve as a starting point for further research after the competition ends. After every competition, the development team and the red team perform a debrief, where they take turns explaining all the vulnerabilities on the machines, how they can be breached, and ways to patch them. Through these debrief sessions, competitors learn what they missed and how to fix them for next time. One student example of this is based on a situation with PAM, or Pluggable Authentication Module, which is used by Linux systems to authenticate a user to applications or services. PAM was misconfigured on this student's computer to allow any input for a password, meaning that a red teamer could login to a user with a random password. This student was aware that someone was logging onto their computer but was unsure how they were able to do so. Through the debrief, the student was told about PAM, and learned about a new Linux file and can now do their own research about how to secure it for future competitions.

Competing more than one time in RvB also poses a valuable way for students to learn. One past competitor state, "most, if not all, of my technical skills I practiced during the competition were learned through RvB events. I would research how to avoid these vulnerabilities by looking up fixes to them after the event, making me more effective for the next RvB event" (Student A, May 30, 2022). Cybersecurity competitions, such as this one, greatly motivate students to take the initiative to study for their own improvement. When a student is able to directly experience what it feels like to be breached, they are inspired and more compelled to do research on the different ways to prevent the breach in the future. One student explains how, "because RvB has a more hands-on approach than a traditional class, I was able to become more interested in cybersecurity. Additionally, because RvB has a competitive aspect, it was fun trying to secure as many services as I could and see how other teams were doing as well" (Student B, May 30, 2022). Student competitors greatly enjoy and take great interest in Red vs Blue. This interest sparks a desire for wider and deeper learning based on the material they encounter during the competition.

The lessons and skills learned from competing in competitions, such as RvB, are more valuable than what can be learned in a regular cyber class. A repeating competitor in RvB explains, "traditional classroom settings don't teach you anything you could have possibly learned in RvB. I can confidently say that everything that I learned about cybersecurity in the past year was due to activities I did outside the classroom. Going to class teaches you the theory of things, but no real hands-on experience. Not even emphasis courses go in as much detail as RvB does" (Student C, May 29, 2022).

Students become more confident in their own skills after seeing themselves put their knowledge to use. This leads to how students with hands-on experience are more equipped to deal with the technical demands of their future jobs. Hiring managers look for people with technical experience, and cybersecurity competitions are a way for students to demonstrate what they know and what they can do. This student disclosed, "RvB has been one of the many things I have talked about in interviews, and it always brings up more and more questions from interviewers. I've noticed that they would rather keep asking me questions about the business injects, what vulnerabilities I patched, and how I dealt with the red team instead of asking me to 'describe some of the courses you have taken'" (Student C, May 29, 2022). Many competitors who participate in RvB feel that they can learn much more by competing than taking a class.

6. RVB & TEACHING OF PROFESSIONAL SKILLS

RvB not only puts the technical skills of competitors to the test, but it also helps build critical professional skills including teamwork, communication, and collaboration. These are all qualities that are much more difficult to learn in a traditional classroom setting. RvB puts students in an environment that forces them to work together to become successful in the competition. Practicing teamwork begins even before the competition day arrives. Strong teams learn to strategize beforehand, setting up meetings to determine what their game plan is, deciding who owns which tasks on which computers, and sharing resources to study. Being in a team environment can therefore result in more successful students, as they are surrounded with others who are working towards the same goals.

During the competition, students are quick to learn that because there are so many tasks to juggle and factors to keep track of during the competition, cooperation is necessary to stay on top of the day’s demands. For example, competitors are given multiple machines to secure, but it is up to their team to decide if one set person is going to be working on one machine or if they are going to rotate the machines around. A past competitor suggests the importance of this decision, when they explained, “An important lesson that I learned was how to delegate what each member of a team works on. I feel that this is a very good way to increase the overall efficiency of the team, as well as become more educated on the specific boxes each member is assigned. During the first couple of RvB events, many members weren’t assigned a role and were just let loose on the environment. Because of this, it was harder to find who was working on what and which boxes were available to be worked on” (Student A, May 30, 2022). Additionally, teams must decide on other factors, such as who will take on which injects and who will check the scoreboard to see which of their services were hit. Generally, teams decide on a leader, or team captain, whose job is to keep all their teammates on track and delegate tasks when necessary. However, every competitor takes on a leadership role in one way or another since teammates will help each other out when another teammate is unsure about how to approach a situation. The competitors know their own strengths and learn the strengths of their teammates, so when a problem does arise, they know who they can talk to and can communicate effectively.

The testimonials of past students stress how important having soft skills are when competing. One past competitor stated, “leadership and teamwork skills are essential to the competition. There are more boxes to fix than people. Also, many of the challenges can take time, while tasks pile on with the red team and injects. Competing in RvB is like trying to fix a sinking ship. If you panic and try to do things yourself, your team will fall very quickly. Having a calm, planned approach while aiding each other with our personal strengths leads to a smooth approach to problems” (Student B, May 29, 2022). Another student comments on the large technical strain of RvB, stating that “multiple people will be working on the same machine throughout the competition, so it's important to document and communicate what is being done to each box and make it clear enough for everything to be understood. If this wasn't established properly, someone could accidentally undo all the work that had been done” (Student C, May 29, 2022).

7. THE DEVELOPERS PERSPECTIVE

Red vs. Blue is an entirely student run student developed event, from its very inception to the execution of the event itself. On the development side, it all begins with a theme, then an entire environment is developed around it. Developers then configure various operating systems in virtual machines to be vulnerable. The boxes are designed to interact with each other to appropriately simulate a business environment, and the vulnerabilities and possible mitigations are well documented, so that competitors can learn from after action reports. In summation, throughout the development process, students develop these boxes, integrate them with the theme, and configure them appropriately for business devices, although they are improperly configured to force competitors to apply fixes.

The key skills that development bolsters are technical. When students develop the competition environment, they first must fully understand how to configure a business environment that depends on the systems that are being scored eg: SSH, HTTP, MySQL, and FTP. This is because to design vulnerable systems in a way that is consistent~~,~~ and stable enough that they will be repairable, they must first be familiar with a fully functional and properly configured version of the system. One developer described the value they achieved from the program thusly, “I believe that the understanding that resulted from identifying misconfigurations and proper security practices for multiple services in RvB environments provided me with the perspectives necessary to truly understand the nuances of securing these services.” (Student 2, June 1, 2022). Much of this technical experience, while condensed into a much shorter time frame than if they were to self-study, is entirely achievable on their own. However, learning to work under extreme pressure, as a team, and manage a massive project on a tight and immovable deadline are skills that don’t come out of personal projects.

High quality, functional, time management skills are something rarely found amongst college students. Usually, it's a skill not learned until they are exposed to industry pressure and consequences. However, RvB completely simulates this experience in a comparably low stakes environment. Developers hone their time management skills when it comes to managing tasks assigned to them, such that development is completed on time and with enough lead time that iteration and growth can occur. One developer described their newly developed time management strategy as, “Just do the work. If you don’t, you're done for.” (Student 2, June 1, 2022). This developer felt this way because they were faced with the dependency that all the developers have on each other as all of the boxes are inter-reliant. A failure on one machine means potential failure on the other systems. A student described the process as “~~…~~incremental work as a driver for good ideas” (Student 2, June 1, 2022). Since RvB is an ever-evolving project, the more time developers invest iterateing on an idea and improving the system, the higher the product quality. Waiting until the last minute would still result in a finished product but it would be dramatically less creative and inventive which would sacrifice the novelty and whimsey of the competition.

8. MEASURING AND ASSESSING SKILLS IN CYBER COMPETITIONS

As aforementioned, cybersecurity is a continually growing and changing industry. Red vs. Blue provides the ability for education to adapt to change better in ways that other curricular or extracurricular program tools cannot. This is because of the hands-on nature of the competition and fact that the development team works tirelessly to keep the environment on par with industry standards and expectations completing multiple competition environments each year. Consequently, the development team stays up to date on the knowledge base and relevant current events. Moreover, as the development process is incredibly fluid and nuanced, the developers must be able to move between machines as necessary to complete the deliverable on time. One developer commented that, “I was initially terrified of being stuck in such a situation [where the answer is unknown] … I quickly learned that researching, troubleshooting, and filling in the gaps of my knowledge with Google searches was inherent to anything cyber related.” (Student 2, June 1, 2022). This is the single most important skill that RvB teaches because it guarantees that the developers cannot be made obsolete in industry. The self-directed learning will continue to serve them for decades to come.

The challenge to measuring competencies in competitions for student players comes down to planning, design, and construction of the competition and its underlying challenges. Beginning with the end in mind is a key conceptual mantra for organizers. This concept is critical to constructing learning outcomes and crafting the challenges in a building block style regardless of the modality of the competition~~.~~ (I.E. CTF, RED V. BLUE, or Forensic Scenario). Careful consideration needs to go into the design in the form of challenge difficulty, skill area, and overall cybersecurity discipline. Couple this with the overall “story” of the competition, and these compounding factors contribute to the time it takes to develop and produce a well-rounded, meaningful, and enjoyable experience for the student which includes the ability to measure their skill level. The final key component for an exercise such as this would be a measurement scale based on challenges with an overall matrix which would gauge a student’s competency in one or more areas. This is supported by Pusey, Gondree, and Peterson (2016), in which they found that learning outcomes are taking a back seat to making competitions fun and meaningful for diverse groups of students across many modalities nationwide.

Other preliminary work on this topic has been characterized by Straub (2020), where quantitative measurements were taken from a broad population of students in the National Cyber League (NCL) to measure skills and how they gain those skills compared to the classroom. However, the NCL competition is static and easy to measure, but does not provide intangible skill measurements such as troubleshooting or dynamic incident response).

To date the expectation is that students learn cybersecurity fundamentals using traditional pedagogies in the classroom. Classroom learning then serves as series of diagnostic assessments in which students gain insight into their strengths and weaknesses and plan their gameplay

accordingly.
Cybersecurity competitions are often used as a forum to exercise the knowledge and skills attained in the classroom. This allow students to test and revise their skills as they adapt and learn through a series of competition experiences allowing competitions to serve as a formative assessment to refine knowledge, skills and abilities.
However, the next evolution of RvB is to craft the measurement of skills into a summative assessment focused on competition outcomes. The competition will not only serve as a summative assessment for fundamental skills but also a diagnostic assessment showing that students attained a degree of mastery with respect to knowledge, skills and abilities related to applied cybersecurity outcomes and are ready to engage in higher-level learning with respect to the application of cybersecurity practices in organizations. The need to assess learning in competitions stresses the importance of outcomes-based competitions mentioned in Pusey, Gondree, and Peterson (2016) and the need to design competition content to support the assessment of outcomes.

9. CONCLUSIONS & OPPORTUNITIES FOR FURTHER RESEARCH

This case clearly outlines the advantages of using competitions to gauge student's strengths learned in the classroom. Furthermore, it surmises the link between curricula and practice, and gives educators different views to hone and improve upon the pedagogy of their program. This comes in the form of different modality and provides the opportunity to measure skills in different ways and track them over years or even careers.

Maintaining an inventory of competencies and relating these to courses may also offer enhanced ways to effectively measure students' knowledge, skills and abilities and lead to more effective capabilities in offering credit for courses in a curriculum set. Effective cybersecurity pathways from middle school to the end of a career necessitate the ability to understand skills and develop/award credit in a more effective manner.

Given these opportunities, it is proposed that further research be done with dynamic competitions, such as National and Regional Collegiate Cyber Defense Competitions, Dynamic CTFs, Red vs Blue competitions and any others willing to join to gain a better understanding of how to define and measure these dynamic skills that are so critical to aspects of cybersecurity such as incident response, penetration testing, and real-time forensics.

10. REFERENCES

Educause (2022, June9). Competency-Based Education (CBE) Retrieved from: https://library.educause.edu/topics/teaching-and-learning/competency-based-education-cbe#:~:text=The%20competency%2Dbased%20education%20(CBE,to%20more%20efficient%20student%20outcomes.

Petersen, Santos, Smith, Wetzel & Witte (2020). Workforce Framework for Cybersecurity NICE Framework), Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

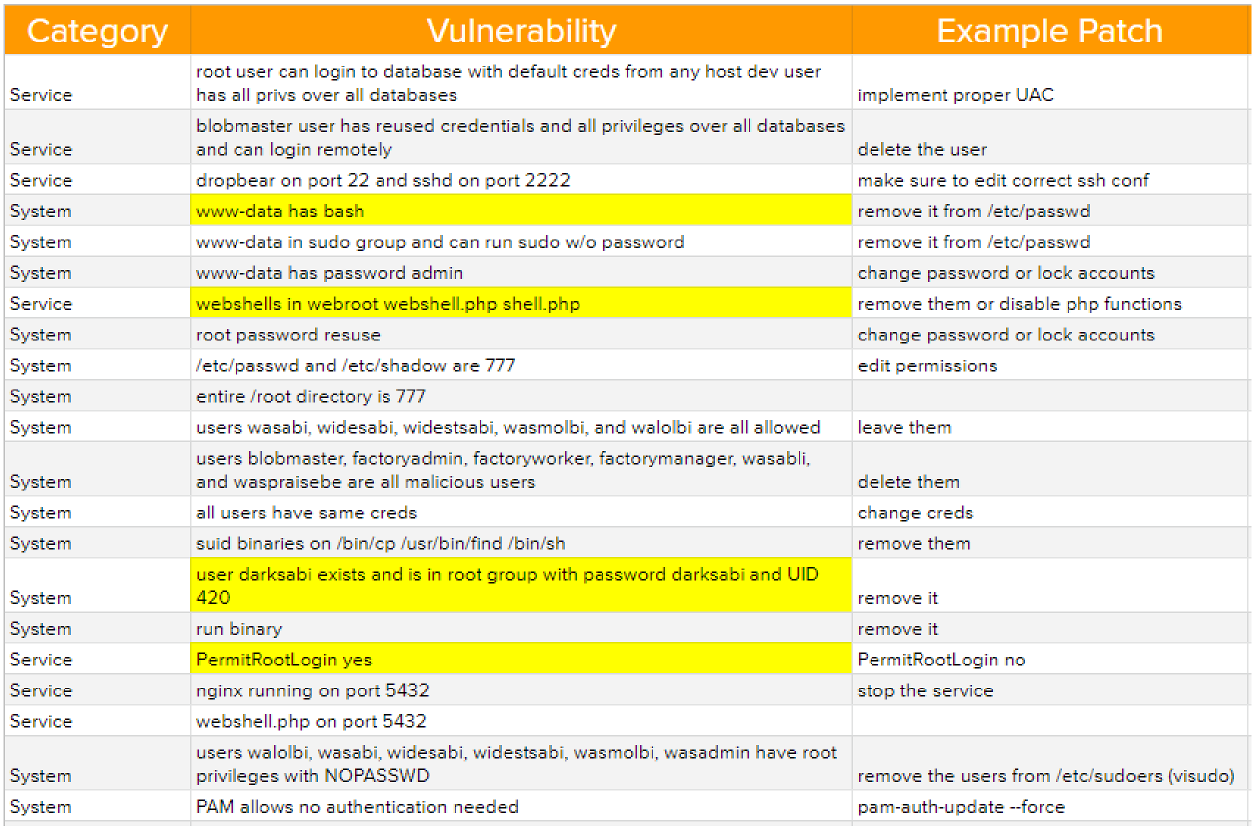
Pike, R. (2022, April). Innovation in Education through Holistic Assessment. Paper presented at 50th Annual Meeting of Western Decision Sciences Institute: WDSI 2022, http://wdsinet.org/Annual_Meetings/2022_Proceedings/papers.php.

Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented populations. IEEE Security & Privacy, 14(6), 90-95.

Straub, J. (2020, June), Assessment of Cybersecurity Competition Teams as Experiential Education Exercises. Paper presented at 2020 ASEE Virtual Annual Conference Content Access, Virtual On line . 10.18260/1-2—34187

Appendix A
Environment Details for Ubuntu 14.04 Machine

This appendix shows a table from a Red vs. Blue competition on the development side. The developer will document the security misconfigurations they add to a computer, similar to the table that is shown below for a Linux machine. The "Category" column categorizes the vulnerability as a service, which means the setting relates to a scored service like DNS or FTP, or as a system, which regards the computer itself. The "Vulnerability" column is to explain what misconfiguration was added, and the "Example Patch" column gives a possible solution to the insecure setting. Teams are awarded 100 points for each of the misconfigurations they fix. Additionally, the more of these vulnerabilities competitors fix, the harder it is for the red team to infiltrate their systems and take down their scored services, resulting in a higher number of points for service uptime. Competitors do not have access to this table during the competition.

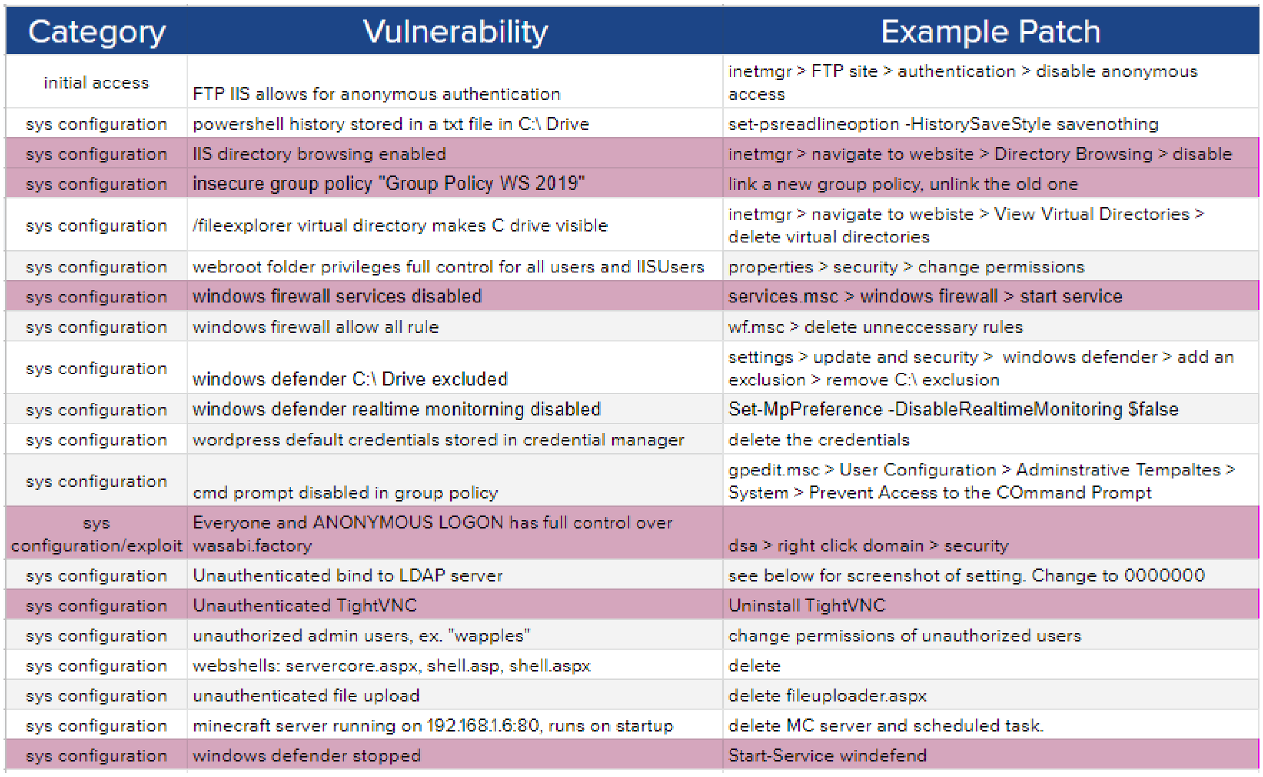


Category	Vulnerability	Example Patch
Service	root user can login to database with default creds from any host dev user has all privs over all databases	implement proper UAC
Service	blobmaster user has reused credentials and all privileges over all databases and can login remotely	delete the user
Service	dropbear on port 22 and sshd on port 2222	make sure to edit correct ssh conf
System	www-data has bash	remove it from /etc/passwd
System	www-data in sudo group and can run sudo w/o password	remove it from /etc/passwd
System	www-data has password admin	change password or lock accounts
Service	webshells in webroot webshell.php shell.php	remove them or disable php functions
System	root password resuse	change password or lock accounts
System	/etc/passwd and /etc/shadow are 777	edit permissions
System	entire /root directory is 777	
System	users wasabi, widesabi, widestsabi, wasmolbi, and walolbi are all allowed	leave them
System	users blobmaster, factoryadmin, factoryworker, factorymanager, wasabli, and waspraisebe are all malicious users	delete them
System	all users have same creds	change creds
System	suid binaries on /bin/cp /usr/bin/find /bin/sh	remove them
System	user darksabi exists and is in root group with password darksabi and UID 420	remove it
System	run binary	remove it
Service	PermitRootLogin yes	PermitRootLogin no
Service	nginx running on port 5432	stop the service
Service	webshell.php on port 5432	
System	users walolbi, wasabi, widesabi, widestsabi, wasmolbi, wasadmin have root privileges with NOPASSWD	remove the users from /etc/sudoers (visudo)
System	PAM allows no authentication needed	pam-auth-update --force

Appendix B

Environment Details for Windows Server 2016

This appendix shows the misconfigurations applied on a Windows machine for a Red vs. Blue competition.

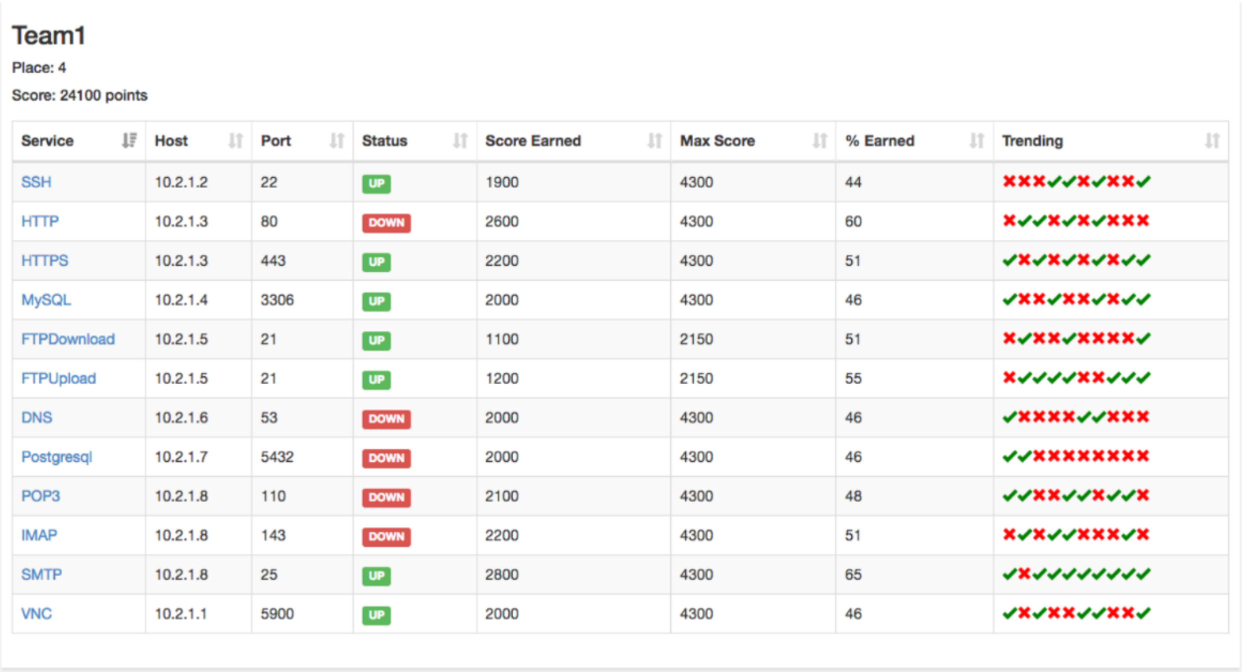


Category	Vulnerability	Example Patch
initial access	FTP IIS allows for anonymous authentication	inetmgr > FTP site > authentication > disable anonymous access
sys configuration	powershell history stored in a txt file in C:\ Drive	set-psreadlineoption -HistorySaveStyle savenothing
sys configuration	IIS directory browsing enabled	inetmgr > navigate to website > Directory Browsing > disable
sys configuration	insecure group policy "Group Policy WS 2019"	link a new group policy, unlink the old one
sys configuration	/fileexplorer virtual directory makes C drive visible	inetmgr > navigate to webiste > View Virtual Directories > delete virtual directories
sys configuration	webroot folder privileges full control for all users and IISUsers	properties > security > change permissions
sys configuration	windows firewall services disabled	services.msc > windows firewall > start service
sys configuration	windows firewall allow all rule	wf.msc > delete unneccessary rules
sys configuration	windows defender C:\ Drive excluded	settings > update and security > windows defender > add an exclusion > remove C:\ exclusion
sys configuration	windows defender realtime monitorning disabled	Set-MpPreference -DisableRealtimeMonitoring $false
sys configuration	wordpress default credentials stored in credential manager	delete the credentials
sys configuration	cmd prompt disabled in group policy	gpedit.msc > User Configuration > Adminstrative Tempaltes > System > Prevent Access to the COmmand Prompt
sys configuration/exploit	Everyone and ANONYMOUS LOGON has full control over wasabi.factory	dsa > right click domain > security
sys configuration	Unauthenticated bind to LDAP server	see below for screenshot of setting. Change to 0000000
sys configuration	Unauthenticated TightVNC	Uninstall TightVNC
sys configuration	unauthorized admin users, ex. "wapples"	change permissions of unauthorized users
sys configuration	webshells: servercore.aspx, shell.asp, shell.aspx	delete
sys configuration	unauthenticated file upload	delete fileuploader.aspx
sys configuration	minecraft server running on 192.168.1.6:80, runs on startup	delete MC server and scheduled task.
sys configuration	windows defender stopped	Start-Service windefend

Appendix C
Table of Scored Services and their Status

This appendix shows the list of scored services that each team has to secure during the competition. The scoring engine checks every three minutes whether the service is up or down. If the service is up, the team is awarded 100 points. If it is not, then they get 0 points. For example, the scoring engine sees that HTTP is up, so the team gets 100 points. The next three minutes, the scoring engine sees that HTTP is down, so the team gets zero points. Then the next three minutes, the scoring engine sees that HTTP is back up, so the team gets 100 points and now has 200 points in total.

The "Status" column shows if the service is currently up or down, and the "Trending" column tracks every three minutes whether the service was up or down. For example, in the table below, SSH is currently up, so the last character in the "Trending" category for SSH is a check mark. The red cross to the left of the check mark tells us that SSH was down 3 minutes ago.



Team1

Place: 4

Score: 24100 points

Service	Host	Port	Status	Score Earned	Max Score	% Earned	Trending
SSH	10.2.1.2	22	UP	1900	4300	44	✗✗✗✓✓✗✓✗✗✓
HTTP	10.2.1.3	80	DOWN	2600	4300	60	✗✓✓✗✓✗✓✗✗✗
HTTPS	10.2.1.3	443	UP	2200	4300	51	✓✗✓✗✓✗✓✗✓✓
MySQL	10.2.1.4	3306	UP	2000	4300	46	✓✗✗✓✗✗✓✗✓✓
FTPDownload	10.2.1.5	21	UP	1100	2150	51	✗✓✗✗✓✗✗✗✗✓
FTPUpload	10.2.1.5	21	UP	1200	2150	55	✗✓✓✓✓✗✗✓✓✓
DNS	10.2.1.6	53	DOWN	2000	4300	46	✓✗✗✗✗✓✓✗✗✗
Postgresql	10.2.1.7	5432	DOWN	2000	4300	46	✓✓✗✗✗✗✗✗✗✗
POP3	10.2.1.8	110	DOWN	2100	4300	48	✓✓✗✗✓✓✗✓✓✗
IMAP	10.2.1.8	143	DOWN	2200	4300	51	✗✓✗✓✓✗✗✗✓✗
SMTP	10.2.1.8	25	UP	2800	4300	65	✓✗✓✓✓✓✓✓✓✓
VNC	10.2.1.1	5900	UP	2000	4300	46	✓✗✓✗✗✓✓✗✗✓