Open Access License Notice

Factors of Success- The Potential Relationship Between CLI Commands and Cybersecurity Competitions

Abstract

Cybersecurity competitions are used in higher education to recruit, educate and assess students. Winners of competitions are recognized based on endgame conditions or rules. Uncovering factors that correlate with success in competitions is difficult and less studied. Some literature exists that investigates competition success relative to institutions, there is no existing investigation of success relative to individual participants. Therefore, this research examined one potential factor related to success of competition participants. Specifically, the study measured the degree of relationship between CLI commands and the percentage of challenges completed. Participants consisted of 100 competitors who engaged in a competition. CLI commands, data mined from Linux command history files, were analyzed. The results demonstrated two strong positive relationships and one negligible relationship. Educators may be interested in these results as a means for performance measurement. Likewise, researchers may leverage these findings to configure game conditions or conduct future causal studies.

Keywords: Cybersecurity competitions, command-line interface, correlation, cybersecurity education

I. Introduction

Cybersecurity competitions are increasingly accepted as methods of knowledge and skill measurement [1]. Indeed, much effort is underway to design, develop and implement cybersecurity competitions [2] [3] [4]. Perhaps intuitively, completion of a particular cybersecurity challenge equates to pre-defined levels of skill, knowledge or aptitude. For example: solving a software reverse-engineering challenge means that the player has, at a minimum, the knowledge to (a) code, (b) read code, (c) execute the reversing tool(s) properly and (d) understand the output to a degree sufficient to complete the challenge. Likewise, solving challenges first, solving the most challenges, or the most challenges the fastest are all subjective means of categorizing success [5] [6] [7]. Informally, such intuition serves as a basis for deciding which team or institution *wins* a cybersecurity competition. However, in formal settings such as educational assessment an empirical, quantified view of success is necessary. Some effort has been made to explain success at an institutional level [8] [9].Yet, there is still a need to understand what factors may be associated with success at the individual participant level. Such is particularly true in cybersecurity competitions where external behaviors may not reveal complete data. Thus, this study considered quantifiable, internal factors which may contribute to individual participant success in competitions. Ultimately, observation led this study to focus on the command-line interface (CLI) commands used during cybersecurity competitions as a possible internal factor related to success. A review of existing literature revealed no research examining the potential relationship between CLI commands and the percentage of challenges completed in a cybersecurity competition.

Accordingly, the purpose of this study was to measure the statistical relationship, if any, between the CLI commands used during a cybersecurity competition and the percentage of challenges completed during the same competition. The outcome of this study will have multifaceted significance. Firstly, educators may benefit from the results of this study as the potential relationship between CLI commands and completing cybersecurity challenges might reveal a means to measure academic performance assessment. Secondly, cybersecurity competition teams may leverage the results of this study to develop a mechanism to rank tryouts and team members. Lastly, this study extends the field of knowledge by providing a foundation for future causal investigation of the topic.

II. Method

A. Cybersecurity Competition

The cybersecurity competition consisted of 35 individual challenges implemented in an Ubuntu Linux virtual machine. The virtual machines were isolated and Internet access was disallowed. A simple desktop GUI was present but all utilities necessary for the challenges were only available at command-line. The challenges were designed to be of a basic difficulty. Challenges required fundamental knowledge of cryptography, Linux system administration, and general security principles to finish properly. Participants were able to engage individual challenges in any sequence and could request help at any time. When provided, assistance was given openly so that all participants were exposed equally. The objective of the competition was to complete the most challenges possible in six hours.

B. Participants

Participants were 100 students who engaged in a cybersecurity competition during the summer and fall of 2013. The competition was held five times in total. Students were a mixture of high school (~22%) and college undergraduate (~78%) students. Female and male genders were well represented (~17% and 83% respectively). Participants volunteered for participation and were selected for the study by engaging in the competition. Written informed consent was provided during the competition by all participants. Moreover, no personally identifiable information was collected as all participants' data were coded before data analysis.

C. Research Design

This study employed a quantitative correlational research design in order to measure the degree of relationship, if any, between CLI commands and the percentage of discrete challenges completed during a cybersecurity competition. The conjectured correlation would be explanatory in nature as opposed to predictive. Accordingly [10], a quantitative methodology was appropriate because this study sought to test hypotheses through empirical measurement. Similarly, a correlational design was appropriate since the design establishes the statistical relationship between variables [11]. Together, the research method and design facilitate answering the research question.

D. Research Questions

The overarching research question asked in this study is *are the CLI commands used during a cybersecurity competition related to the percentage of discrete challenges completed during the same competition*. This question arose after the a priori suggestion that highly skilled participants might be able to complete more challenges using fewer CLI commands total while using more different CLI and making fewer typos in those commands. Participants of low skill might demonstrate the opposite. Such a priori reasoning however assumes that a relationship between CLI commands and percentage of challenges completed exists. Therefore, the research construct of CLI commands expanded into three more detailed questions.

The three questions were, *does using more CLI commands correlate with a higher percentage of challenges completed*, *does using more different CLI commands correlate with a higher percentage of challenges completed* and finally *do fewer CLI commands typos correlated with lower percentage of challenges completed*. In turn, these specific but still informal questions were transcribed into technical, testable research questions as follows.

1. Is there a statistically significant relationship between the total number of CLI commands used in a cybersecurity competition and the percentage of discrete challenges completed?

2. Is there a statistically significant relationship between the number of different CLI commands used in a cybersecurity competition and the percentage of discrete challenges completed?

3. Is there a statistically significant relationship between the number of CLI command typos committed in a cybersecurity competition used during a cybersecurity challenge and the percentage of discrete challenges completed?

E. Hypotheses

Based on the research questions, this study tested three pairs of hypotheses. The pairs of hypotheses provided criteria for testing statistical significance. Table 1 contains the hypotheses mapped with the corresponding research question. Negative, in the content of this study, meant that fewer CLI commands or typos would correlate with a higher percentage of challenges completed. In contrast, positive meant that more CLI commands or typos would correlate with a higher percentage of challenges completed. No relationship in the context of this study equated to no discernible correlation between commands or typos and higher percentage of challenges completed.

Table 1
Hypotheses Mapped to Research Questions

Research Question Index	Code	Hypotheses
1	H_{A1}	There is a positive statistically significant relationship between the total number of CLI commands used and the percentage of discrete challenges completed.
	H_{01}	There is a negative or no statistically significant relationship between the total number of CLI commands used and the percentage of discrete challenges completed.
2	H_{A2}	There is a positive statistically significant relationship between the number of different CLI commands used and the percentage of discrete challenges completed.
	H_{02}	There is a negative or no statistically significant relationship between the number of different CLI commands used and the percentage of discrete challenges completed.
3	H_{A3}	There is a negative statistically significant relationship between the number of CLI command typos committed and the percentage of discrete challenges completed.
	H_{03}	There is a positive or no statistically significant relationship between the number of CLI command typos committed and the percentage of discrete challenges completed.

F. Variables

Stemming from the research questions and hypotheses, this study identified three independent variables and a single dependent variable. This study investigated the potential relationship between the CLI commands used during a cybersecurity competition and the percentage of discrete challenges completed during the same competition. For this study, *challenge percent completed* served as the

dependent variable (*x*) and represented the percentage of total cybersecurity puzzles successfully completed by participants. The three independent variables were *number of commands total*, *number of typos total* and *number of different commands*.

Table 2
Research Variables Defined By Type

Variable Name	Variable Type	Figure Legend Names
Challenge Percent Completed	Dependent	ChalngPerComp
Number of Commands Total	Independent	NumOfCmds
Number of Typos Total	Independent	NumOfTypos
Number of Different Commands	Independent	NumOfDiff

G. Data Collection and Analysis

Data were collected through mining of the Bash shell history files harvested from participants' Linux virtual machines. Capture of all commands was ensured by modifying the Linux virtual machine to retain up to 5,000 commands in the history file [12]. Data mining indexed the total number of CLI commands and the total different CLI commands. The index value per participant was then entered into a spreadsheet. Total number of CLI command typos was manually indexed and entered into a spreadsheet. Manual indexing was necessary to avoid potential skewing by missing typos in an automated data miner. Finally, data belonging to one variable category was not indexed in any other category. For example, typos were excluded when indexing the total number of CLI commands. Subsequently, data analysis was conducted using the R statistical computing language. The data studied in this research were ratio scale values and thus continuous. As such, two statistical measures were conducted in order to (ultimately) test the hypotheses. Initially, scatterplot graphs were generated in order to determine whether a linear, curvilinear, or nonexistent relationship existed between variables. Secondly, a correlational coefficient, via a Pearson product-moment correlation statistic, measured the strength of the correlation. Statistical significance was an additional output of the coefficient calculation. This procedure was consistent with correlational research design standards [11] [13] [14].

H. Reliability and Validity

A pilot test of data collection and data analysis tools measured the reliability and validity of the instrumentation and allowed for assessment of the overall study validity [10] [11]. The pilot test for data collection consisted of executing the data mining procedure against a 10 test Bash shell history files. A research assistant generated the test files on an isolated Linux system by entering CLI commands for 30 minutes. Data mining of the test history file returned results consistent with (a) functional CLI Linux commands and (b) correct totals of CLI commands. Therefore, the instrumentation appeared reliable and valid.

This study also considered threats to the internal and external validity of the research. Due to the nature of correlational research design, the study possessed limited internal validity [10]. Future causal studies may establish appropriate levels of internal validity. In contrast, this study established high external validity as the results are generalizable across different settings [11].

III. Results

The purpose of this study was to measure the statistical relationship, if any, between the CLI commands used during a cybersecurity competition and the percentage of discrete challenges completed during the same competition. This study tested three hypotheses to achieve such a purpose and address the stated research questions. Testing, in turn, consisted of two statistical measures: scatterplot graphing and Pearson product-moment correlation coefficient. The results generated specific recommendations for future work according to each independent variable.

A. Number of Commands Total

The first results analyzed were the number of commands total. The minimum number of commands total contained in the data was 45. Meanwhile, the maximum number of commands total was 1366. Analysis computed the mean at 744.5 commands total. Along the opposite axis, the minimum percentage of challenge completed was nine percent. The maximum percentage completed was 98%. Finally, the calculated mean was 54.7%.

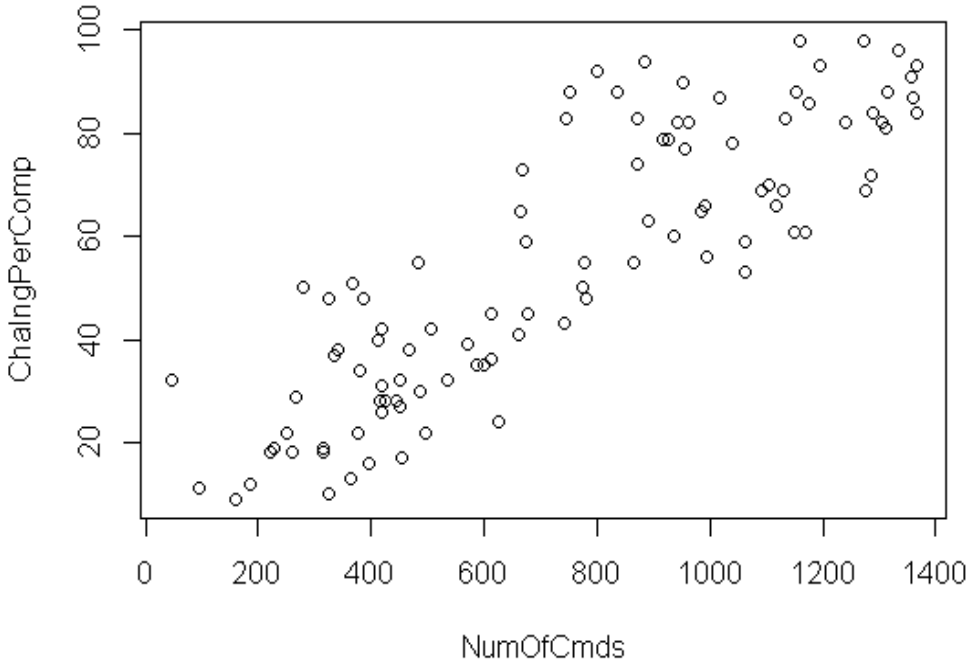

Figure 1. The relationship between number of commands total and challenge percentage completed.

The scatterplot for the number of commands total, as displayed in Figure 1, demonstrated a linear relationship between the number of commands total and challenge percentage completed. Next, the Pearson product-moment correlation coefficient was calculated in order to determine the strength and significance of the relationship between the total number of commands and the percentage of challenges completed. Overall, the results indicated a *very strong* and *positive* relationship (Table 3). Lastly, the correlation demonstrated statistical significance. Since p computed to less than five percent, the null hypothesis (H_{01}) was rejected and the alternate hypothesis (H_{A1}) accepted. Collectively, these results comport with the graphical relationship between variables shown in Figure 1.

Table 3
Strength of total number of commands and percentage of challenges completed

Pearson's Coefficient (r)	*df*	*t*	*p*
0.86	98	16.6	2.2e-16

Note: Correlation is very strong at $r < .70$ and significant at $p < .05$

B. Number of Different Commands Total

The second results analyzed were the number of different commands total. The minimum number of different commands total contained in the data was 73. Meanwhile, the maximum number of different commands total was 227. Analysis computed the mean at 156.7 commands total. Again, the minimum percentage of challenge completed was nine percent. The maximum percentage completed was 98%. Finally, the calculated mean was 54.7%.

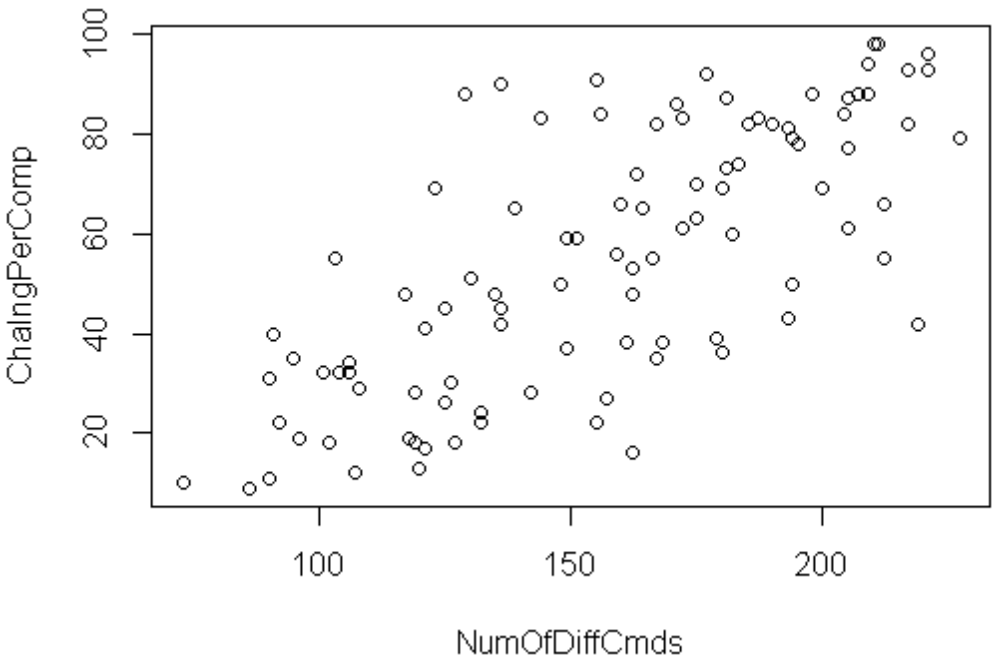

Figure 2. The relationship between the total number of different commands and the percentage of challenges completed.

There was a demonstrable linear relationship between the total number of different commands and the percentage of challenges completed (Figure 2). Further, the Pearson product-moment correlation coefficient indicated a *very strong* and *positive* relationship (Table 4). Finally, the correlation demonstrated statistical significance as p computed to less than five percent. Accordingly, the null hypothesis was rejected and the alternate hypothesis (H_{A2}) accepted. Such results correspond to the graphical relationship between variables shown in Figure 2.

Table 4
Strength of total number of different commands and percentage of challenges completed

Pearson's Coefficient (r)	*df*	*t*	*p*
0.72	98	10.5	2.2e-16

Note: Correlation is very strong at $r > .70$ and significant at $p < .05$

C. Number of Command Typos Total

The last results analyzed were the number of command typos that minimally equaled one. In contrast, the maximum number of command typos totaled 60. Mean number of typos computed at 27.1. As previously discussed, the minimum percentage of challenge completed was nine percent. The maximum percentage of challenges completed was 98%. Lastly, the calculated mean of challenges completed was 54.7%.

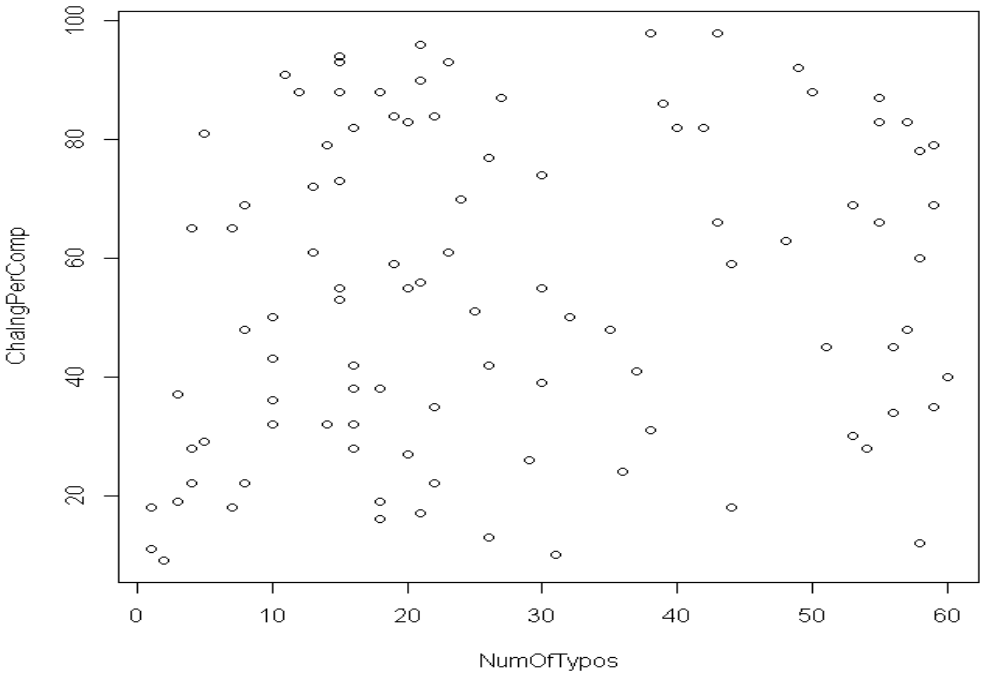

Figure 3. The relationship between the total number of command typos and the percentage of challenges completed.

Based on the scatterplot (Figure 3), there appeared to be no correlation between the number of command typos and the percentage of challenges completed. Calculation of the Pearson product-moment correlation coefficient confirmed a negligible relationship (Table 5). Further, calculation of statistical significance demonstrated a non-statistically significant correlation between variables. Therefore, the null hypothesis (H_{03}) was accepted. Such results correspond to the Figure 3 scatterplot.

Table 5
Strength of total command typos and percentage of challenges completed

Pearson's Coefficient (r)	*df*	*t*	*p*
0.17	98	1.7	.09

Note: Correlation is negligible at $r > .01$ - $.19$ and non-significant at $p < .05$

IV. Conclusion

Cybersecurity competitions function as pedagogical tools, recruitment vehicles and student performance measurements [1]. The design and implementation of these competitions is of timely interest to both educators and researchers [2] [3] [4]. Yet, although research [8] [9] provides insight into

success at a broad, organizational level, there is little investigation of potential factors contributing to individual competitor success. Intuitive constructs such as scoring the most points or completing the most challenges [5] [6] serve as clear delineations between winning and losing a cybersecurity competition. However, such do not provide attributable performance metrics that work towards explaining individual participant success.

Thus, the purpose of this study was to measure the statistical relationship, if any, between the CLI commands used during a cybersecurity competition and the percentage of challenges completed during the same competition. Realization of such a purpose may uncover some factors of success in cybersecurity competitions. An explanatory correlational research design facilitated actualization of this purpose through the collection of data and subsequent statistical analysis. The study included 100 participants who engaged in a cybersecurity competition held over the summer of 2013. Participants ranged from high school freshmen to undergraduate seniors and included men and women. The nature of the cybersecurity competition necessitated the exclusive use of the CLI in order to complete challenges. Accordingly, independent variables included number of CLI commands, the number of different CLI commands, and the number of CLI command typos. The percentage of total challenges completed served as the dependent variable.

Three null hypotheses underwent statistical testing in order to determine if a relationship existed between study variables as well as the strength and significance of such relationships. Data were collected from individual participant's Linux CLI history files after the conclusion of the cybersecurity competition The testing consisted of scatterplot graphing and a Pearson product-moment coefficient correlation. Data analysis yielded results reliable and valid given the design and nature of the research.

A. Interpretations and Recommendations

Analysis of the data (summarized in Table 6) revealed relationships in two of the independent variables and no statistical relationship in the remaining independent variable. Overall, future research investigating the transferability of the results of this study to other types of cybersecurity competitions (e.g. capture the flag) would be of demonstrable benefit to the field. Also in a general sense, future work should focus on extending the results of this study by examining potential casual relationships between the variables outlined in Table 2. Interpretations for each category of results follow and are separated according to independent variable for readability.

Table 6
Summary of findings according to independent variables

Independent Variable	Relationship Found	Null Hypotheses	Alternate Hypotheses
Number of commands total	Yes (very strong)	Rejected	Accepted
Number of different commands	Yes (very strong)	Rejected	Accepted
Number of command typos	No	Accepted	Rejected

I. Number of commands total

Cybersecurity competition participants who used more CLI commands exhibited higher percentages of completed challenges in a very strong and significant manner (Figure 1). This result answers affirmatively whether there is a statistically significant relationship between the total number of CLI commands used in a cybersecurity competition and the percentage of discrete challenges completed. Although such an answers is perhaps self-obvious upon first glance, such a result may actually be less

straightforward than a priori reasoning leads educators and researchers to believe. Indeed, there are two potential interpretations of this relationship. Firstly, the data may indicate that the more commands a participant uses, the more challenges that participant is able to complete. In this interpretation, *more* could indicate a blind shotgun approach- just throwing seemingly random commands at a challenge- or *more* could equate with a logical trial-and-error approach. Alternatively, the data may imply that increased completion of cybersecurity competition challenges necessitates more commands per challenge than more limited completion of challenges due to challenge difficulty. Unknown is whether the higher numbers of CLI commands included *meaningful* commands relative to the particular challenge being solved.

Educators may be interested in the relationship between the number of CLI commands and percentage of challenges completed due to the need for academic performance measurement. Although far from an absolute measure, educators could leverage the total number of CLI commands, as an explanation for as well as a predictor of success, for the purposes of measuring knowledge mastery. Concurrently, researchers may find this result significant as such indicates a potential avenue for future investigation of the causal relationship between the stated variables (Table 2). Accordingly, future work in this area might focus on the cause and effect associated with total number of CLI commands and percentage of challenges completed.

II. Number of different commands total

Per the results, as the total number of different CLI commands increased so did the percentage of challenges completed. The research question as to whether a statistically significant relationship exists between the number of different CLI commands used in a cybersecurity competition and the percentage of discrete challenges completed is thus affirmatively addressed. One interpretation of the data may indicate that larger varieties of commands contributes to increased completion of challenges. Variety in this context, similar to the interpretations associated with the total number of CLI commands, might be related to trial-and-error or related to arbitrary command usage. Alternatively, the data may imply that increased completion of cybersecurity competition challenges necessitates many different commands as opposed to more focused or limited approaches.

The same significance exhibited with total number of commands might apply to number of different commands as well. Further, educators potentially could harness fewer different commands to guide instructional content around cybersecurity related CLI commands. Future work involving the number of different commands might consider two lines of inquiry. The first line of inquiry would involve measuring the potential cause more various commands has on solving cybersecurity challenges. Secondly, future research may consider if a particular order of more various commands leads to higher rates of challenge completions compared to non-ordered commands.

III. Number of command typos total

Results of this study supported the conjecture that no statistical relationship existed between the number of CLI command typos in a cybersecurity competition and percentage of challenges completed. Interestingly, participants who completed a high percentage of challenges committed similar numbers of CLI command typos as participants completing lower percentages of challenges. Thus, CLI command typos appeared to have no bearing on success whatsoever. Therefore, given the seemingly arbitrary nature of typos relative to successfully completing challenges, interpretations of the data are extremely limited. Overall, typos appeared to have little or no interaction with (a) the other independent variables or (b) the dependent variable.

However, the demonstrated lack of relationship between CLI command typos and completing challenges may still hold significance to educators and researchers alike. In particular, educators might consider eliminating or not using CLI command typos as an academic performance indicator. Similarly, researchers may consider eliminating or not using CLI command typos as a variable in future causal studies.

References

[1] Fulton, S., Schweitzer, D., & Dressler, J. (2010). What are we teaching in cyber competitions? *2013 IEEE Frontiers in Education Conference Proceedings* (pp. 1-5). Seattle, WA: IEEE.

[2] Manson, D. (2013). National cybersecurity sports federation. Presented at *NIST NICE Workshop 2013*. Gaithersburg, MD.

[3] Novak, H, Likarish, D. M., & Moore, E. (2013). Developing cyber competition infrastructure using the SCRUM framework. In Dodge, R. and Futcher, L. (Eds), *Information assurance and security education and training 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Zealand, July 8-10, 2013, proceedings, WISE 7, Lucerne, Switzerland, June 9-10, 2011 and WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009, revised selected papers*. Berlin New York: Springer.

[4] Pittman, J. (2013). Understanding system utilization as a limitation associated with cybersecurity laboratories – A literature analysis. Journal of Information Technology Education: Research, 12,363-378. Retrieved from http://www.jite.org/documents/Vol12/JITEv12ResearchP363-378Pittman0440.pdf

[5] Conti, G., Babbitt, T., & Nelson, J. (2011). Hacking competitions and their untapped potential for security education. *IEEE Security & Privacy*, 56–59. doi:10.1109/MSP.2011.51

[6] Patriciu, V.V., & Furtuna, A.C. (2009). Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy*, pp. 172–177. Stevens Point, Wisconsin: WSEAS Press

[7] Wagner, P. J., & Wudi, J. M. (2004). Designing and implementing a cyberwar laboratory exercise for a computer security course. *Proceedings of the 35th SIGCSE technical symposium on Computer science education* (pp. 402-406). New York: ACM New York. doi:10.1145/1028174.971438

[8] Wankat, P. (2005). Undergraduate student competitions, *Journal of Engineering Education, 94*(3). 343-347. doi:10.1002/j.2168-9830.2005.tb00860.x

[9] Dolan, D. F., Batchelder, M., Krause, W. B., Allen, C., & Jensen, C. (2001). Manufacturing and design education through national competitions. *2001 ASEE Annual Conference*, Albuquerque, New Mexico.

[10] Salkind, N. (2011). *Exploring research.* Boston, Pearson.

[11] Creswell, J. (2008). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. New Jersey: Pearson: Merrill Prentice Hall.

[12] Bash Command Reference, (n.d.). Retrieved from

http://www.gnu.org/software/bash/manual/bashref.html#Commands-For-History

[13] Lodico, M. G., Spaulding, D. T., & Voegtle, K. H. (2006). *Methods in educational research: From theory to practice*. New York: Wiley & Sons.

[14] Siegle, D. (n.d.). Principles and methods in educational research. Retrieved from http://www.gifted.uconn.edu/siegle/research/correlation/correlation%20notes.htm