Compu Castel: An Instructional Tool for Teaching Firewall Concepts

"Analysis of Knowledge Retention"

Mahmoud Mostafa[1,2]
[1]Department of Information Technology, College of Computers and Information Technology,
Taif University, Al-Hawiya 21974, KSA
[2]Information Systems Department, Faculty of Computers and Information,
Helwan University, Helwan, 11795, Egypt
Email: mahmoud.mostafa.m [AT] gmail.com

Abstract— **Firewall is an essential device in every computer network. It needs skillful professionals to accurately configure its rules for proper functioning. To help prepare these professionals, university level students need more engaging and attractive interactive tools to develop their skills. For this regard, this paper presents the design, implementation and evaluation of "Compu Castel" educational video game that teaches firewall concepts. In addition to evaluating the impact of educational game on short-term knowledge acquisition, both, mid-term (after 2 months) and long-term (after 5 months) knowledge retention is analyzed. The results confirm that educational games affect positively short-term knowledge acquisition compared with traditional text based methods. Moreover, educational games enhance knowledge retention for mid-term and long-term periods.**

Keywords- firewall; security; educational; game; retention.

I. Introduction

Firewalls have become the first line of defense for almost all networked information systems [1]. All organizations search for highly qualified professionals to administrate these firewall systems. Their purpose is to provide the maximum security protection for their networked information systems. For the firewall, to work properly, the administrator must write accurately filtering rules to determine which traffic is allowed, and which is denied. Unless these firewall rules are set appropriately, it will not provide the desired protection. Worst, firewalls misconfiguration may give false sense of security protection. As inaccurately defined rules may leave holes that attackers may exploit to penetrate the system [2]. Writing and modifying firewall filtering rules is a complicated error brown task that require qualified personnel especially in large information systems that requires hundreds of filtering rules [1]. To protect national critical infrastructure and to fulfill the society needs, universities provide educational programs to help prepare specialized computer security professionals. Due to its importance, Firewall topic becomes a mandatory part in every computer science curriculum [3]. However, the new generations of technology native students need more engaging and effective teaching methods rather than traditional textbooks and lectures. They need to practice and get feedback about their work. Currently, educational video games became proven instructional tool in many disciplines including medicine [4], engineering [5] computer science [6] and many other disciplines [7, 8]. Researchers found that videogames have many rich features that could engage learners for longer time and increase learning efficacy [9]. This paper presents "Compu Castel" educational video game to teach firewall concepts and help prepare information security professionals.

The rest of this paper is organized as follow: section 2 gives the basic background necessary to understand firewall system. Then, in section 3, educational serious games are presented. Section 4 reviews previous work and highlights differences. Section 5 presents design principles and give details of the developed game. Section 6 describes the evaluation methodology and discusses the obtained results. Finally, Section 7 gives the conclusion and perspectives for future work.

II. Firewall

Firewall is a software or hardware device installed at the entrance point of a private network. It splits network environment into external and internal networks [10]. Its main role is to protect the internal network form external networks. To perform its function, firewall system inspects incoming and outgoing network traffic to apply specific policy that prevents or permits certain connections.

Firewall policy is high-level statement defines how an organization's firewalls should handle inbound and outbound network traffic. It must align with the organization's overall information security policies [11].

For example, assume an organization management wants to prevent their employees from accessing external web servers from the internal network of the organization. The high-level policy statement might be "No outside Web access". This implies that the firewall must drop all outgoing packets to any IP address for port 80. To force a firewall to apply this policy administrator must write the following filtering rule.

tcp, *.*.*.*, any, *.*.*.*, 80, accept

Firewall administrator writes firewall policy in a form of chains of ordered rules. Input chain is used to inspect packets coming from outside the protected network to filter out undesired traffic and block it from entering the secure network. While output chain contains the rules that inspect outgoing packets and prevents certain packets from leaving the boundary of the protected network to avoid the establishment of undesired connections and to forbids information leakage. A typical firewall rule is written in the following format:

<Order> <Prtcl> <Src_ Add> <Src_Port> <Des_Add> <Des_Port> <Action>

Each rule consists of seven fields divided into three parts. The first part contains <Order> field. It is a number that determines the position of the rule inside the chain.

The second part is the criteria part [12]. It contains <Prtcl>, <Src_Add>, <Src_Port>, <Des_Add> , and <Des_Port>. The <Prtcl> filed identifies the protocol stored in the payload of IP packet. Its value may be IP, TCP, UDP, IGMP, ICMP or wildcard character (*) that means any of the previous values. The <Src_ Add> and <Des_Add> fields respectively represent source IP address and destination IP Address of the packet. Their values may contain the address of a single host, a network address, range of addresses or wildcard character (*) to specify any address. While, <Src_ Port> and <Des_Port> fields determine the source port number and the destination port number used by the sending and receiving applications respectively. Their values may contain single port number, range of values or wildcard character. The third part contains action filed. This field identifies the action to perform on the packet that matches the criteria part of this rule. If the action filed value is accept, the packet will allowed passing through the firewall. Nevertheless, if the action filed value is deny, the becket will be dropped.

The firewall is placed in between the internal and external network to inspect all incoming and outgoing packets. The information exists on packet header fields used to search the filtering rule staring form the first rule in a sequential order. The action associated with the first matching rule is performed [13]. Therefore, the order of the rules is very significant.

When writing firewall policy there are two main strategies: allow-all strategy or deny-all strategy. Allow-all strategy permits all network packets except those which are expressly prohibited. While, deny-all strategy prohibits all network packets except those which are expressly permitted [14]. As a general rule, administrators prefer the use of the deny-all strategy as, it has two main advantages: 1) Administrators have to maintain only a small list of allowed network traffic rules. The smaller the list, the easier it is for administrators to verify that the configuration of the firewall is correct. 2) Administrators do not have to constantly add new rules to exclude newly discovered problems.

As shown in table 1, rule number 9 represents the deny-all strategy. This rule is placed at the end of each filtering rule chain to match all packets that does not match any of the preceding rules. Clearly, if one places deny-all rule at the beginning of the filtering rule chain this will result on denying all traffics from entering or leaving the protected network and will cause a denial of services. Hence, writing and placing firewall filtering rules in correct orders is very important for successful implementation of firewall system. However, anomalies appear when one packet matches with more than one filtering rule. According to Al-Shaer [15], placing firewall-filtering rules on incorrect order may produce four types of anomalies: shadowing anomalies, generalization anomalies, correlation anomalies and redundancy anomalies. Table 1 represents examples of these anomalies.

TABLE 1. SAMPLES OF FIREWALL-FILTERING RULES ANOMALIES.

Ord	Prtcl	Src_Add	Src_ Port	Des_Add	Des_ Port	Action
1	TCP	*.*.*.*	Any	156.223.234.17	80	Accept
2	TCP	154.143.29.*,	Any	156.223.234.17	80	Deny
3	TCP	154.143.29.89	Any	156.223.234.17	80	Deny
4	TCP	154.143.29.*,	Any	156.223.234.17	80	Accept
5	TCP	154.143.29.53	Any	*.*.*.*	Any	Deny
6	TCP	*.*.*.*	Any	156.223.234.*	Any	Accept
7	TCP	154.143.29.*	Any	156.223.234.17	23	Accept
8	TCP	*.*.*.*	Any	156.223.234.17	23	Accept
9	*	*	*	*	*	Deny

Shadowing anomaly occurs when more generic rule is placed before a specific one. In this case, the more general rule will firstly, match all the packets that matches the specific rule. In this case, the specific rule will never be reached and executed. Considering rule 1 and 2 from table 1, it is evident that rule 1 is more general as it indicates any IP address while rule 2 has specific network IP address "154.143.29.*". Here, any TCP packet sent to port 80 at 156.223.234.17 will match rule 1 first therefore, rule1 shadows rule 2 and rule 2 will never be reached and evaluated. Moreover, deleting rule 2 from the chain will have no effect on firewall functionality. Shadowing is a severe error as it may allow a traffic that must be denied and vice versa. The solution is to reorder the rules and place the more specific rule first. In this way, it will not be concealed (shadowed) by the general one.

Generalization anomaly occurs when the second rule in order matches all the packets that matches the first rule but both rules have different actions. Taking rule 3 and 4 from table 1, it is clear that rule 4 matches all packets that rule 3 matches and both rules have different actions. We can say that rule 4 is a generalization of rule 3 (which is more specific). However, if the order is reversed then rule 4 will shadow rule 3 and will make it useless. Actually, generalization anomaly needs careful treatment from administrators. As inserting more specific rule, which is an exception from the general rule, needs validation and confirmation from the administrator. By reviewing generalization anomaly, administrators can detect rules that incorrectly open exceptional holes or block permitted traffic.

Correlation anomaly occurs when some packets those match the first rule also match the second rule, and some packets thoset match the second rule also match the first rule but both rules have different actions. In this case, the two rules are correlated to each other. Considering rules 5 and 6 form table 1, it can be preserve that the same order, HTTP traffic coming from source address "154.143.29.53" to destination address "156.223.234.∗" is denied to pass. Contrarily, if the order is reversed then same traffic will be accepted. Correlation anomaly should be reported to the administrator in order to investigate it clearly. Hence, the right order should be chosen that serves the predetermined policy.

Redundancy anomaly occurs when a rule performs the same action on the same packets as another rule. For example, rules 7 and 8 from table 1 implies that rule 7 is a redundant of rule number 8. Therefore, rule 7 must be deleted to reduce filtering rule chain length. Removing redundant rules will definitely enhance firewall system performance at it will reduce memory-required space and processing time required to traverse the chain searching for the matched rule.

III. Educational Video Games

Educational games are video games designed for both entertain and educate as well. They are instructional serious games those benefit from the rich features of computer video games to engage learners for longer time. According to Heintz et al, [9] video games have a set of characteristics that encourage researches to use them to build instructional games which will then enrich the learning experience. Fantasy world provided in the video games allows users to live in an imaginary world that provides unique experience in contrast to the real-life [16]. The consequences of users' actions or wrong decisions do not have any effect on the users' real life world. Fantasy world provides a safe environment to practice dangerous or unacceptable actions and let the users to learn from their mistakes. Moreover, games have well defined goals and governed by clear rules. Additionally, games have graduated levels of challenges those encourage players to do their best to overcome their hesitations of learning. Furthermore, video games allow designers to provide players with immediate feedback regarding their actions or decisions. All these inherent characteristics are utilized in educational video games [17]. This forces researchers to use video games to build effective instructional tools.

The last two decades witnessed tremendous amount of research studies those have been undertaken to explore the effectiveness of educational video games as instructional tool in many educational domains [18]. Most of these studies reported positive impact in the use of educational video games for instructional or educational purposes.

IV. Related work

While many security educational games implicitly use firewall as a security tool inside the game [19-21]. But out of these, only two games explores firewall concepts explicitly in details. The first notable work dedicated to educate learners about how to write correctly firewall filtering rules to implement certain firewall policy is the work of Thompson [22] form university of Edinburgh. His game targets professionals who have good background with iptables firewall system. The player must use the command line prompt to correctly write iptables filtering rules to implement certain firewall policies. However, this work is a training simulation tool rather than being a real video game. Moreover, it targets professionals and has little fun.

Contrarily to Thompson [22], which targets professionals, Sehl et al, [23] developed “Permission Impossible” game to educate general public about some firewall terminology and constructing firewall rules. The game was usable but the level of entertainment is not sufficient to engage student for longer time.

Moreover, while both studies used survey tool to assess the usability level of their games, none of them conducted a study to evaluate the effectiveness of their games as instructional tool. Their focus was only on the usability aspects of their educational games. Additionally, the sample size used for both studies was small which affects the reliability of their surveys'.

This paper presents "Compu Castel" educational video game that delves deeply into firewall concepts. Unlike previous work, the goal of "Compu Castel" game is to teach computer science students the internal functioning of firewall system. How packet-filtering firewall inspects incoming and outgoing packets. Further to this, "Compu Castel" will also enable students to translate high-level security policy statements into firewall rules and check firewall-filtering rules for anomalies. After learning it properly, they will be able to resolve such conflict and write anomaly free filtering rules. All these topics are presented in a three dimensions role-play video game that has a rich story to engage learners for longer time.

Most studies in the area of educational video games focused on measuring the impact of educational video games on knowledge accusation [24-26]. On the other side, few works have been done to date to measure the impact of educational games on knowledge retention. For this reason, the current study analyzes the impact of educational video games on both knowledge acquisition and retention.

V. The game

In the next subsection game design learning principles are describe. Moreover, the most important game design choices namely game genre and game dimensions environment 2D/3D are identified.

A. Game Design Principles and Choices

To effectively design "Compu Castel" educational game, the following 5 learning science principles were considered:

- *Organized Knowledge Structure*

According to Cognitivist learning theory, learning content should be presented in a logically successive structured way starting from easy to hard and not too much information is presented at once [27]. To achieve this principle, the game is divided into four levels. Each level is dedicated to a single topic. Moreover, levels start from easy to hard in a progressive way.

- *Learner Set the Pace*

Students like to learn at their own pace. Educational video games allow students to use the games at their own pace when they are ready to learn. Moreover, as player/learner skills developed the game challenge increases at appropriate pace [28]. This is definitely support player/learner flow experience.

- *Goal-Directed Practice*

Each practice should have clearly defined and measurable goals. This helps player/learner to focus their efforts to achieve these goals [29]. In "Compu Castel" educational game, this is kept in mind during the design of the game and therefore, each level has a defined goal.

- *Story-Based Principle*

"Compu Castel" educational game uses the story telling technique to immerse players in a fantasy world that entertains them during learning. Stories help game designers organize events in a meaningful way. Stories also stimulate the cognitive process of the player/learner [30].

- *Feedback And Reflection Principle*

To allow learner to know if his committed action was wrong or wright, an immediate feedback is provided. "Compu Castel" educational game, ties the feedback principle with rewards and penalties concept [31]. Each acceptable action is rewarded by increasing the player's scores while for every wrong or unacceptable action; scores are deduced as a penalty. Through this feedback system, leaners remain continuously enthusiastic in the game and hence increase their learning experience as well. Moreover, the game also provides the opportunity for after mission reflection [32]. This is done by allowing the learner to browse all mission taken actions at the end of each level. This reflection process let learner thinks about what he has learned. Additionally, it permits him to know his wright decisions and hence reinforce them and know his wrong decisions to avoid them.

Besides the implemented learning principles, two important design choices must be determined. They are related to the game genre choice and dimensions 2D/3D to be used for implementing the game.

According to Prensky[33] role-play game genre is the most appropriate game genre for learning contents to teach learners skills and judgment decisions. Clearly this is the case with firewall concepts. Actually, role-play game allows learning activities such as, imitation that permits learners to emulate real life-situations. Moreover, role-play game genre provides coaching activities and allows learners to continuously practice the required skills. Furthermore, role-play game genre provides learners with feedback on their decisions during game play. For this reasons, "Compu Castel" is designed as a role-play game. Additionally, the game is designed in a three dimension (3D) environment. According to Bai et, al. [34], 3D games is more attractive. It engages learners more effectively in the game learning activities. Implementing educational games in 3D environment improves learning as it increase learners motivation.

B. Game Description

"Compu Castel" game story revolves around the computer firewall, which is represented by a castle surrounded by high walls from all its directions to protect it. The game consists of four levels. Each level is designed with the goal to teach a specific firewall topic.

The first level is dedicated to teach students how a firewall system handles incoming packets by consulting the input chain filtering rules. Table 2 shows samples of the input chain filtering rules used in the game.

Table 2. Samples of input chain filtering rules

Order	**Prtcl**	**Src_Add**	**Src_ Port**	**Des_Add**	**Des_ Port**	**Action**
1						
2	UDP	154.95.76.11	53	156.223.2.0	*	Allow
3	TCP	176.1.1.1	80	156.223.2.2	*	Deny
4	UDP	154.55.66.11	*	156.223.2.0	53	Allow
5	TCP	154.95.1.*	80	156.223.2.2	*	Deny
6	*	*	*	*	*	Deny

As presented in figure 1, the castle has only one gate designated to control the entry of carts (data packets). The castle is surround by a groove filed with fire. The carts (data packets) must pass above the groove to reach the castle gate. When the cart passes over the groove, its contents (IP packet header fields) appears, which must be checked by the soldier (player) guarding the gate. The soldier consults set of declared rules (firewall input chain filtering rules) hanged on the wall of the castle to decide whether to allow the vehicle to enter or not.

There is also a clock that specifies the time remaining to complete the task. If the player fails to determine whether allowing the cart to pass or not during the specified time. A time-over message appears, the score is decreased and a different cart appears with different contents. Thus, the game continues and if the player fails to respond within specified time for three allowed trials then the game will stop and a message for Game Over will be displayed. If the player decides to allow the cart to enter the castle, as it is desirable according to the rules, the gate opens and let the cart go inside the castle. As an immediate feedback and to reward the player, soldiers launch fireworks from inside the castle to welcome the entry. The correct decision taken by the player results in increase the player score. If the player makes mistake and allows the cart to enter while it is not desirable according to the declared rules, then the bombed cart explodes inside the castle, causing destruction and therefore reducing the player score accordingly. If the player decides that the cart is not desirable and the player destroys it by opening the bridge in which the cart stands in front of the gate, then this action of the player will lead fire flames appearing. The scores then increase accordingly. If the player mistakes and dropped a desirable (according to the rules) vehicle, the game scores are then decreased as a penalty and an eye sign full of tears appears which shows the regret for destroying a benign vehicle through wrong action of the player. To allow learner to review his work and learn from his wrong trails; scene in the

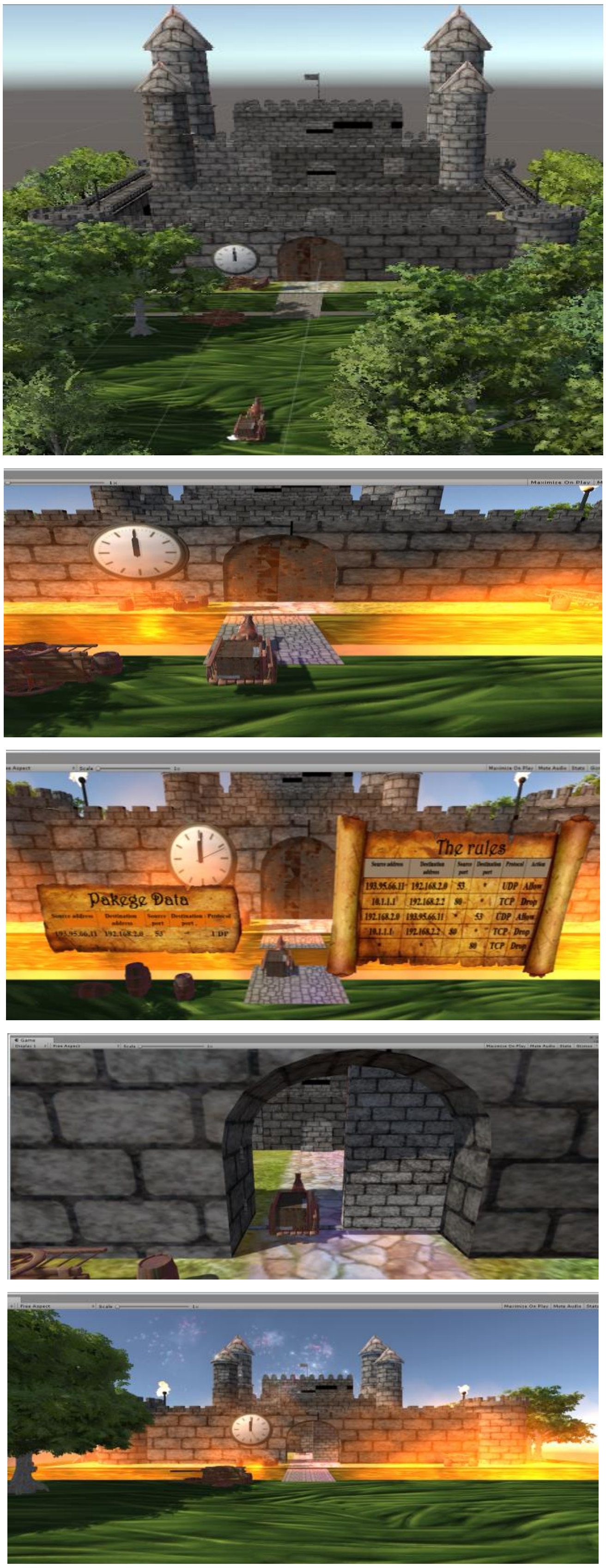

Figure 1. Snapshots of level 1.

respective level shows a list of all player's activities including success and fail trials.

Second level teaches student how to inspect the output chain filtering rules. After successfully passing the first level, the player is promoted to become a top-ranking guard soldier who is responsible for protecting the castle from the inside.

For this regard, the player must check all carts leaving the castle to prevent any leakage of information by spies or any unwanted connection as depicted in Figure 2. The player should inspect each cart (IP packet header fields) and consult the declared (output chain) filtering rules. Then, he must decide either to allow the cart to safely go out the castle or to destroy it. Correct decision action results in scores increment and wrong decision is punished in terms of scores decrement..

Figure 2. Snapshot of level 2.

Third level teaches student how to create firewall security policy. After successful passing the second level, the player is promoted to become an army commander. In this new mission, the player is responsible for formulating security polices in the form of declared rules for soldiers to follow up. As shown in figure 3, the player is given a security policy and he should write the filtering rule or rules to implement this policy. Table 3 represents samples of used firewall policies.

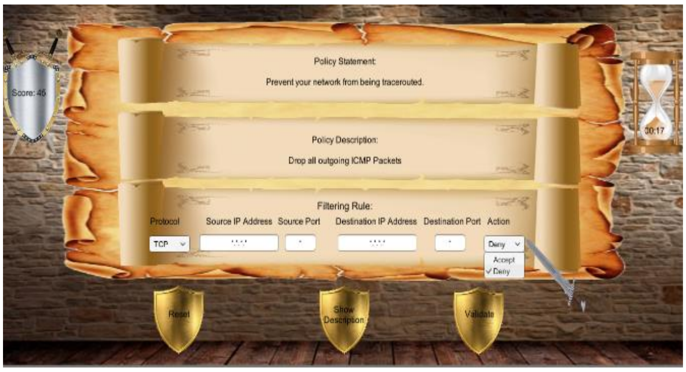

Figure 3. Snapshot of level 3.

The user can press the "show description" button to read the policy description. This description is helpful for the player to formulate the rule more appropriately. This also provides more learning materials in a more interactive way. To validate the rule/s written by the player, the player must press "validate" button. Moreover, the reset button is also available in the screen which can be pressed to reset the content of the game scene. .The filtering rule must be written very accurately and precisely to implement the desired policy before the timer runs out.

TABLE 3. SAMPLES OF USED FIREWALL POLICIES, THEIR DESCRIPTION AND CORRESPONDING FILTERING RULES

No	Policy	
1	**Statement**	No outside Web access.
	Description	Drop all outgoing packets to any IP address, port 80
	Rule	tcp, *.*.*.*, any, *.*.*.*, 80, accept
2	**Statement**	External connections to public Web server (address 156.223.234.207) only.
	Description	Drop all incoming TCP SYN packets to any IP except 156.223.234.207, port 80
	Rule	tcp, *.*.*.*, any, 156.223.234.207, 80, accept
3	**Statement**	Prevent IPTV from eating up the available bandwidth
	Description	Drop all incoming UDP packets - except DNS and router broadcasts.
	Rule	udp, *.*.*.*, any, *.*.*.*, any, Deny
4	**Statement**	Prevent your network from being used for a Smurf DoS attack.
	Description	Drop all ICMP packets going to a “broadcast” address (156.223.255.255).
	Rule	icmp, *.*.*.*, any, 156.223.255.255, any, Deny
5	**Statement**	Prevent your network from being tracerouted.
	Description	Drop all outgoing ICMP Packets.
	Rule	icmp, *.*.*.*, any, *.*.*.*, any, Deny
6	**Statement**	prohibit all network packets except those that are expressly permitted (deny-all strategy)
	Description	Drop any packet that does not have a rule in the chain list (this must be the last rule)
	Rule	any, *.*.*.*, any, *.*.*.*, any, Deny

Fourth level focuses on the detection and resolution of filtering rules conflicts.

Figure 4. Snapshot of level 4.

After successfully passing the third level, the player is promoted to be the "King's Advisor for Security Affairs". During this final level, the player is required to review existing filtering rules and to identify the conflicting rules and then resolve such conflicts. Figure 4 represents a snapshot of level 4. Table 1 (above) presents samples of conflicting rules used in the game. If the player completes this level successfully then the Royal medal is awarded to acknowledge the achievements of the player.

"Compu Castel" game is developed using Unity game engine [35]. Unity is a very rich game engine that has a very large community. It uses C# programming language to allow programmers write programming scripts for controlling game objects and gaming environment.

VI. METHOD

There is a common consensus on the effectiveness of educational games as instructional tools in enhancing knowledge acquisition comparing to traditional teaching methods. Besides, there is a debate on its effect on knowledge retention. Some studies [36-38] confirm that the use of educational games increases knowledge retention while other studies [39] claim that traditional teaching techniques still more effective than educational games.

For further investigation of these topics, the current study hypothesizes that::

H1: Educational games enhance short-term knowledge acquisition.

H2: Educational games enhance mid-term knowledge retention.

H3: Educational games enhance long-term knowledge retention.

To validate the above hypotheses, a quasi-experimental design of two nonequivalent groups was followed [40]. The study was conducted with fourth- and fifth-year Information Technology students of the College of Computers and Information Technology (CCIT) at Taif University who were enrolled in the information security track. 76 students (29 meals and 47 females) participated in a period of five months. Students were randomly distributed into two groups. 37 students for the game group (15 meals and 22 females) and 39 for the control group (14 meals and 25 females).

A. Validation Protocol

First, the two groups attended a lecture about firewall topics. Immediately after the lecture, the two groups participated in knowledge acquisition pre-test (KAPRT) exam. The exam consists of 20 multiple-choice questions that cover all given firewall topics discussed above. Questions were automatically graded out of 20. Then, after that, the game group was allowed to play "Compu Castel" game while, control group was allowed to read the pre-prepared lecture notes. Clearly, game contents are identical to the lecture notes contents. Immediately after playing/reading educational content, the two groups participated in knowledge acquisition post-test (KAPOT) exam to assess knowledge acquisition level of each group.

In order to assess knowledge retention later after two months, mid-term knowledge retention test (MTKRT) was performed. Finally after more additional three months, long-term knowledge retention test (LTKRT) was held. Table 4 represents the number of participants in each test. While the number of participants for pre-test and post-test was the same as the two tests were performed on the same day, the number of participants for retention tests decreased because these tests were performed two and five months later and some students stop participating. Actually, it was impossible to retain the same number of participants in all tests as students were voluntarily applied for the experiment.

TABLE 4 NUMBER OF PARTICIPANTS IN EACH TEST .

Test	Group	Male	Female	Total
KAPRT	**Game**	15	22	37
	Ctrl	14	25	39
KAPOT	**Game**	15	22	37
	Ctrl	14	25	39
MTKRT	**Game**	15	20	35
	Ctrl	13	23	36
LTKRT	**Game**	14	17	31
	Ctrl	11	19	30

B. Results analysis

First, the collected data were inspected to detect any outliers. No outliers were detected.

An independent samples t-test analysis was performed to compare the means of the two groups in each exam. Independent samples t-test analysis is used to determine if there is a significant difference between the means of the two different groups. Moreover to identify the magnitude of the experimenter, the effect-size was calculated for significant values. Hedges' g measure was used to calculate the *effect-size* as each group has a different sample size [41]. Table 5 presents knowledge assessment t-test analysis results.

TABLE 5 KNOWLEDGE ASSESSMENT T-TEST ANALYSIS RESULTS

Test	Game Mean (SD)	Ctrl Mean (SD)	t – value	p-value	Effect-size g
KAPRT	14.19 (0.82)	14.21 (0.96)	p=0.05 0.073	0.47	Not significnt
KAPOT	18.70 (1.1)	17.03 (1.45)	p=0.01 6.459	<0.00001	1.292
MTKRT	17.66 (1.76)	16.36 (2.29)	p=0.01 3.830	0.000139	0.635
LTKRT	16.71 (1.95)	15.4 (1.49)	p=0.01 3.897	0.000126	0.753

As presented in table 5, the performance of the game group outweighs the performance of the control group except for knowledge acquisition pre-test (KAPRT). No significant difference was observed when comparing the results of KAPRT for the two groups. The results indicate that the two groups were equivalent before using different teaching methods.

According to the results of knowledge acquisition post-test (KAPOT), there is a significant difference between the two groups. The 37 participants who played the game (M = 18.7, SD = 1.1) comparing to the 39 participants in the control group (M = 17.03, SD = 1.45) demonstrated significant better knowledge acquisition $t(74) = 6.459$, $p < 0.00001$. Moreover, this test has a high effect size (1.292). This proves hypothesis H1. Educational games enhance short-term knowledge acquisition. As the performance of the game group exceeds the performance of the control group used traditional learning method.

Similarly, there is a significant difference when comparing the results of the two groups for mid-term knowledge retention test (MTKRT) performed after two months. The 35 participants who played the game (M = 17.66, SD = 1.76) comparing to the 36 participants in the control group (M = 16.36, SD = 2.29) demonstrated significant better mid-term knowledge retention $t(69) = 3.83$, $p = 0.000139$. This test has a moderate effect size (0.635). Therefore, hypothesis H2 is accepted. There is statistical evidence that educational games enhance mid-term knowledge retention.

The results of the long-term knowledge retention test (LTKRT) performed after five months showed a significant difference between the two groups. The 31 participants who played the game (M = 16.71, SD = 1.95) comparing to the 30 participants in the control group (M = 15.49, SD = 1.49) showed significant better long-term knowledge retention $t(59) = 3.897$, $p = 0.000126$. This test has a moderate effect size (0.753). Thus, hypothesis H3 is accepted. There is statistical evidence that educational games enhance long-term knowledge retention.

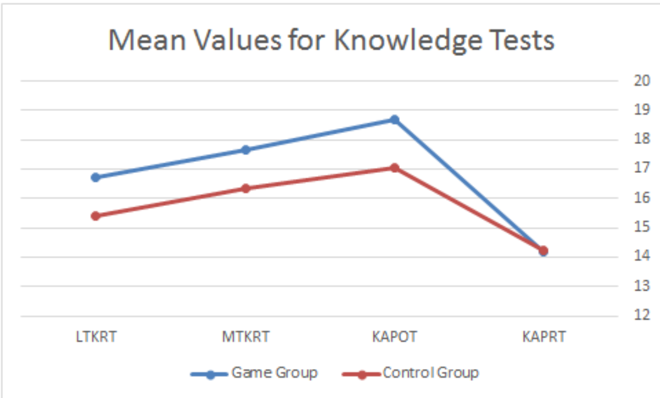

Figure 5 Mean values for all knowledge tests

As shown in figure 5, the mean values of the results for KAPRT performed immediately after the lecture were relatively low (game M= 14.19 and control M= 14.21) comparing to other tests. On the other hand, these values witnessed significant increases in KAPOT held after reading lecture notes (M = 17.03) or playing game (M = 18.7). However, the performance of the game group is better than the performance of the control group. Regarding mid-term knowledge retention test (MTKRT) the performance starts decreasing. However, students in the game group (M = 17.66) still perform better than their colleagues in the control group (M = 16.36). For the long-term knowledge retention test (LTKRT), the performance is still decreasing. This because the test is held after five months which is a long period. However, the game group (M = 16.71) demonstrates their ability in retaining the acquired knowledge better than their counterparts in the control group (M = 15.4).

VII. Conclusion

This paper described basic firewall concepts in brief and gave a detailed description of security policy creation and anomaly detection on firewall written rules. Based on this, the paper presented the need for more effective tools to help preparing professionals capable of administering firewall systems accurately. To provide such tool, "Compu Castel" educational game was proposed to teach the firewall concepts at university undergraduate level. Learning science principles were considered while designing the game. A study was performed to evaluate the effectiveness of "Compu Castel" game. The results proved the ability of the tool to enhance knowledge acquisition and retention for mid-term and long-tem periods comparing to traditional text-based learning method.

These findings encourage researches to explore this area and develop more educational games; especially in domains that need more practices such as information security domain. There are other aspects of educational games, which need further investigation such as the effect of game genre selection into game effectiveness as an instructional tool and the cognitive effects of educational games.

References

[1] Artem Voronkov , Leonardo Horn Iwaya , Leonardo A. Martucci , Stefan Lindskog, Systematic Literature Review on Usability of Firewall Configuration, ACM Computing Surveys (CSUR), v.50 n.6, p.1-35, January 2018

[2] Shackelford, R., McGettrick, A., Sloan, R., Topi, H., Davies, G., Kamali, R., and Lunt, B. Computing Curricula 2005: The overview report. Proceedings of the 37th SIGCSE technical symposium on Computer science education, Houston, Texas, USA, 2006, pp. 456-457.

[3] Haining Chen, Omar Chowdhury, Ninghui Li, Warut Khern-am-nuai, Suresh Chari, Ian Molloy, Youngja Park: Tri-Modularization of Firewall Policies. SACMAT 2016: 37-48

[4] Buijs-Spanjers, Kiki R. ; Hegge, Harianne HM; Jansen, Carolien J. "A Web-Based Serious Game on Delirium as an Educational Intervention for Medical Students: Randomized Controlled Trial.", Journal of Medical Internet Research. Oct 2018, Vol. 20 Issue 10, p149-149.

[5] Ebner, M., & Holzinger, A. (2007). Successful implementation of user-centered game-based learning in higher education: An example from civil engineering. Computers and Education, 49(3), 873-890. http://dx.doi.org/10.1016/j.compedu.2005.11.026

[6] D. Topalli, N. E. Cagiltay, "Improving programming skills in engineering education through problem-based game projects with Scratch", *Computers & Education*, vol. 120, pp. 64-74, 2018.

[7] Backlund, P., & Hendrix, M. (2013). Educational games-are they worth the effort? A literature survey of the effectiveness of serious games. In Games and virtual worlds for serious applications (VS-GAMES), 2013 5th international conference on (pp. 1-8). IEEE.

[8] P Battistella and CG von Wangenheim. Games for teaching computing in higher education–a systematic review. IEEE Technology and Engineering Education, 9(1):8–30, 2016.

[9] Heintz, S. and Law, E. L.-C. "Game Elements-Attributes Model: a first step towards a structured comparison of educational games". In DiGRA'15 - Proceedings of the 2015 DiGRA International Conference. Digital Games Research Association.

[10] Hajar Esmaeil As-Suhbani, S.D. Khamitkar, Using Data Mining for Discovering Anomalies from Firewall Logs: a Comprehensive Review, International Research Journal of Engineering and Technology (IRJET) 4 (11), Nov -2017 PP. 419- 423.

[11] Jabal, A.A., M. Davari, E. Bertino, C. Makaya, S. Calo, D. Verma, A. Russo, C. Williams, Methods and tools for policy analysis. ACM Computing Surveys (CSUR) 51(6), February 2019. PP. 1-35

[12] Rupali Chaure, Shishir K. Shandilya, " Firewall anamolies detection and removal techniques – a survey", International Journal on Emerging Technologies, 2010.

[13] Mostafa M, Abou El Kalam A, Minuta Dragos and FRABOUL C. QoS-aware Firewall Session Table. The IEEE International Conference on Risks and Security of Internet and Systems, Timişoara, Romania, 26-28 September 2011.

[14] Brian Komar, Ronald Beekelaar, Joern Wettern, Firewalls For Dummies®, 2nd Edition Published by Wiley Publishing, Inc. 2003.

[15] Ehab Al-Shaer and Hazem Hamed, "Discovery of Policy Anomalies in Distributed Firewalls" in Proc. of IEEE INFOCOM'04, vol. 23, no. 1,March 2004 pp. 2605-2616.

[16] Garris, R., Ahlers, R., & Driskell, J. E. (2002). Games, motivation, and learning A research and practice model. Simulation & Gaming, 33(4), PP. 441-467.

[17] Wilson, K. A., Bedwell, W. L., Lazzara, E. H., Salas, E., Burke, C. S., Estock, J. L., Orvis, K. L., and Conkey, C. (2009). Relationships between game attributes and learning outcomes: Review and research proposals. Simulation & Gaming, 40(2):217{266.

[18] Boyle, E. A., Hainey, T., Connolly, T. M., Gray, G., Earp, J., Ott, M., et al. (2016). An update to the systematic literature review of empirical evidence of the impacts and outcomes of computer games and serious games. Computers & Education, 94, 178–192.

[19] Marc Olano, Alan T Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac S Kohane, and Donna Thomas. SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. In USENIX Summit on Gaming, Games, and Gamification in Security Education, 3GSE '14, San Diego, CA, USA, August 18, 2014. USENIX Association 2014.

[20] Twitchell, D., SecurityCom: a multi-player game for researching and teaching information security teams. Journal of Digital Forensics, Security & Law, 2007, 2, pp. 9-18.

[21] Irvine, C. E., Thompson, M. F., and Allen K., CyberCIEGE: gaming for information assurance, Security & Privacy Magazine, IEEE, 2005, 3, 3, pp. 61- 64.

[22] Thompson, S. (2017), `Firewall administration the game'. Thesis, Available at https://github.com/scottwthompson/Firewall-Administration-The-Game (Accessed 11/11/2019).

[23] Sibylle Sehl and Kami Vaniea, "Permission Impossible: Teaching Firewall Configuration in a Game Environment", European Workshop on Usable Security (EuroUSEC) 2018. 23 April 2018, London, England

[24] Sarah Pila, Fashina Aladé, Kelly J. Sheehan, Alexis R. Lauricell, Ellen A. Wartella, "Learning to code via tablet applications An evaluation of Daisy the Dinosaur and Kodable as learning tools for young children", computers and educations 2019

[25] Kristian Kiili, Korbinian Moeller, Manuel Ninaus, Evaluating the effectiveness of a game-based rational number training - In-game metrics as learning indicators, Computers & Education, Volume 120, May 2018, Pages 13-28

[26] Hendrix M., Al-Sherbaz A., Bloom V., Game Based Cyber Security Training: are Serious Games suitable for cyber security training? International Journal of Serious Games, Volume 3, Issue 1, January 2016

[27] Siang, A. C. and Rao, R. K. (2003). Theories of learning: A computer game perspective. In Proceedings of the IEEE Fifth

International Symposium on Multimedia Software Engineering, ISMSE'03, pages 239{245. IEEE.

[28] Sweetser, P. and Wyeth, P. (2005). GameFlow: A model for evaluating player enjoyment in games. Computers in Entertainment, 3(3):1{24.

[29] Quinn, C. N. 2005. Engaging Learning: Designing e-Learning Simulation Games. Pfeiffer.

[30] Mayer, R. E. Multimedia Learning. New York Cambridge University Press, 2001.

[31] Perry, D. and DeMaria, R. (2009). David Perry on Game Design: A Brainstorming Toolbox. Charles River Media.

[32] Donovan, M. S., Bransford, J. D., & Pellegrino, J.W. 1999. How people learn: Bridging research and practice. Washington, D.C.: National Academy Press.

[33] Prensky, M.: Computer Games and Learning: Digital Game-Based Learning. In: Raessens, J., Goldstein, J. (eds.) Handbook of Computer Game Studies, pp. 97–122. The MIT Press, Cambridge (2005)

[34] Bai, H., Pan,W., Hirumi, A. & Kebritchi, M. (2012). Assessing the effectiveness of a 3-D instructional game on improving mathematics achievement and motivation of middle school students. British Journal of Educational Technology, 43, 6, 993–1003. doi: 10.1111/j.1467-8535.2011.01269.x.

[35] Bond, J. G. (2014). Introduction to Game Design, Prototyping, and Development: From Concept to Playable Game with Unity and C#. 1st Edition. Addison-Wesley Professional.

[36] Brom C, Preuss M, Klement D: Are educational computer micro-games engaging and effective for knowledge acquisition at high-schools? A quasi-experimental study. Comput Educ 2011, 57:1971–1988.

[37] Kanthan R, Senger JL: The impact of specially designed digital gamebased learning in undergraduate pathology and medical education. Arch Pathol Lab Med 2011, 135:135–142.

[38] Egenfeldt-Nielsen S: Beyond edutainment: Exploring the educational potential of computer games. PhDthesis. Copenhagen: University of Copenhagen; 2005.

[39] Rondon S., Sassi F. C. & de Andrade C. R. F. Computer game-based and traditional learning method: A comparison regarding students' knowledge retention. BMC Medical Education, (2013) 13, 30-37. doi: 10.1186/1472-6920-13-30

[40] Albaum, G. (1997). The Likert scale revisited. Journal of the Market Research Society, 39, 331-348.

[41] Lakens, D. (2013). Calculating and reporting effect sizes to facilitate cumulative science: A practical primer for t-tests and ANOVAs. Frontiers in Psychology, 4:863. doi:10.3389/fpsyg.2013.00863