ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse234932020.pdf
https://doi.org/10.30534/ijatcse/2020/234932020

Security, Control and Management of Smart Remote Laboratory for Remote Experiments in Electricity and Electronics

Yassine Larbaoui[1], Ahmed Naddami[2], Ahmed Fahli[3]
[1]Electrical engineering department, University Hassan I, Morocco, Yassine.larbaoui.uh1@gmail.com
[2] Electrical engineering department, University Hassan I, Morocco, ahmed.naddami@gmail.com
[3] Electrical engineering department, University Hassan I, Morocco, fahli@uhp.ac.ma

ABSTRACT

This paper presents the work of securing and managing the hardware and software resources of a smart remote lab, which supports different remote experiments in electricity and electronics, where we elaborated different techniques for smart environment control and management. This remote lab consists of a hybrid e-learning platform, where we conducted web penetration tests and security assessment on the network topology, to evaluate its security level and define how much it may be considered as secured and reliable. In addition, this paper presents the major parts of developed, integrated and deployed resources for online experimenting and distance learning through this hybrid platform. Moreover, this paper presents an optimized secured topology, with reliable security measures and attack counter measures. This topology and measures are designated to our remote lab networks and educational establishment; to provide secured online services through internet and assure high levels of integrity and confidentiality of critical data, deployed networking systems and digital resources.

Key words: e-learning, network architecture, network security, remote experiments, remote management, smart laboratory.

1. INTRODUCTION

In the last decades, Information technologies (Its) have been evolving through continues processes of development, which support enormous enhancements and revolutionary renovations and innovations. These information technologies had been reaching various fields of human activities such as industries, business, finance, health, management, education and other learning services. Implicitly, education and learning frameworks and apparatuses have increase in size and revolve quickly by relying on the concepts and tools of e-learning and remote experimenting through remote laboratories. These concepts and tools are direct results of the corporation between telecommunication technologies and the educational pedagogies [1].

E-learning has become a primary service and mainstream in the divers fields of learning and education, in either public or private sectors.

E-learning has been enormously seized and incorporated in higher education areas of United Kingdom, United States of America, Germany, Australia and other worldwide countries. The delivered services of e-learning systems and their provided quality have attract an appreciable amount of research attention and analytic attempts of study and evaluation [2]-[4]. A significant number of researchers have tried to identify the responsible factors of e-learning success, to increase the effectiveness of distance education through the internet while exploiting those systems of e-learning [5]-[7]. Mainly, the major parts of these researches and studies have treated different entities and success factors of e-learning separately from each other; disregarding the crucial synergistic effects of interacting between them and their impacts on each other [8]. Likewise, other orientations of study and research have treated the correspondences between the quality factors of e-learning and the usage and/or contentment of the end users of e-learning systems [9], [10].

In e-learning and distance education, the significant amount of research papers has significantly contribute in defining and advancing the pivotal success factors of e-learning; such as the factors of availability, delivered information quality, provided service quality, in addition of human-system interactivity, satisfaction and content usefulness. On other hand, the high number of analytic evaluations among dependent and independent factors and variables is the leading challenge of actual researches toward developing an effective and successful model of e-learning.

It is essential to have a comprehensive model about the multiple levels of success factors of e-learning while relying on information technologies [8]. These systems of e-learning are, basically, information systems that involve human apparatuses such as students and professors, and nonhuman

entities such as learning management systems and educational contents of documents and multimedia resources. Therefore, it is paramount to investigate multiple areas and dimensions of successful and productive interaction between the potential clients of these information systems and the online provided resources of e-learning.

Hands-on experiments and physical practices of laboratories represent the essence of engineering education and learning. They allow transforming the bare knowledge into tangible tools and technologies, exploited to the welfare and benefit of students, researchers and engineers.

There are three general categories of labs [11], [12]: hands-on laboratories, simulators and virtual labs, then the remote laboratories. However, to be specific, there are four principal types of experiments: Hands-on experiments, emulation based experiments, simulation based experiments, virtual experiments and remote experiments.

Hands-on laboratories are the most popular and renowned in the fields of education, and they are based on hands-on experimenting. They obligate the physical presence of both instruments and students at the same local space. They grant students with the clearest tangible experiments at the levels of interaction and manipulation. However, their needs of high financial investment, significant maintenance requirements and considerable amount of infrastructures; impose to regard other supplementary resources or alternatives.

Virtual labs and simulators are simply imitators; they count on mathematical models and virtualized systems. The provided experiments of these laboratories may diminish the reference of students to physical interaction with real equipment and instrument, if they do not provide high-level approximations of manipulation and accuracy to hands-on experimenting.

Remote labs are physical labs, similarly approximated to hands-on laboratories, in addition of supporting online access and remote control on experiments. Their surplus convenience is their exploitability through the internet while providing multiuser-based web services, in order to support large numbers of students- or other users. The reduced costs and reduced requirements of local space and maintenance, in addition of time allocation flexibility and accuracy approximations to hands-on experiments, all that represent the most powerful advantages and criteria of strength of remote laboratories over the previous mentioned categories of laboratories.

In our remote lab, we aim to deploy various resources of remote experimenting in electronics and electricity, in addition of deploying different platforms and contents of virtualized experiments and simulation based experiments. Moreover, we aim to optimize the control and management of deployed resources in term of security, online access and monitoring. Furthermore, we are trying to elaborate a smart environment within our remote lab to simplify its resources management and supervision.

The security aspect of web services and network topologies of e-learning platforms and remote laboratories still poorly treated at the level of researches. Many Learning Management Systems (LMS), web services and online applications of remote laboratories are provided through internet with no reliable counter measures against web intrusions and network attacks, and with no assurance of having reliable security of their online services as it is the case of many online web services, which will be discussed in the rest of this paper.

Moreover, deploying remote lab networks and e-learning platforms usually focus on the provided contents of education and experiments, more than focusing on the security aspect of delivered services, communication scenarios, information transfer and data storage. This negligence may massively decrease the reliability and availability of delivered web services, and even being leveraged for network scaling to access more critical data, such as the drafts and papers of ongoing researches, invention results, credit cards data of the staff, etc.

On one hand, this paper presents the work of designing and elaborating a smart environment in term of control and monitoring within our remote lab network, in order to simplify resources management and supervision. On other hand, this paper presents the work of vulnerabilities assessment and web penetration testing on our remote lab network and deployed hybrid platform of e-learning after two conducted processes of results evaluation using different tools, to define their vulnerabilities and measure their risks to be attacked and intruded.

Moreover, this paper presents a general adapted model as an optimized topology of network, to be specifically deployed in our remote lab and educational establishment; to have more security of critical contents and web services, and have more reliable services through the internet.

Furthermore, this paper proposes multiplicity of security measures and attack counter measures, to brace the integrity and security of deployed resources and transferred information through local networks of our remote laboratory and educational establishment.

This paper is structured as follows: section 2 presents the aspect of smart environments of remote laboratories. Section 3 presents the security aspect of e-learning platforms and remote laboratories. Section 4 presents the deployed resources of online experiments and network topology in our remote lab. Whereas section 5 presents proposed topology of network, and security measures, in addition of presenting proposed counter measures against cyberattacks to be deployed for remote laboratories and educational establishments. Finally, section 6 for conclusion.

2. SMART ENVIRONMENTS OF REMOTE LABORATORIES

Smart environments [13] are impressively developing all around the world, and they have been projected on different fields. They had been relied-on to simplify the control, the monitoring and/or the management of various resources of hardware and software. The concept of smart environments is especially recognized under the terms of smart homes, smart cities, smart irrigation [14] and smart industrial zones. However, smart remote laboratories are not common as a term, even though there are many researches about smart laboratories [15].

A smart environment is any space that uses the collected information by sensors and other devices in order to monitor, control or manage the infrastructures and resources of environment efficiently.

Based on sensory data, the systems of monitoring and control are able to continuously learn and even adapt to the circumstances of environment. Moreover, smart environments may rely on different resources of software and applications to collect and manage digitized data, or communicate and interact with computer systems and networking devices at the network architecture of environment.

Furthermore, these environments may rely on learning methodologies basing on data processing, to augment or optimize the performance at specific levels of deployed services.

In our remote lab, we deploy different resources of hardware and software for e-learning and remote experimenting in electricity and electronics. We rely on various servers to provide our online web-based services and applications. In addition, we have many computer systems of staff and different types of connected networks. Thereby, controlling and managing these resources for 24 hours each day and seven days in week is ambiguous, especially that remote laboratories and e-learning platforms must provide continues access through the internet to enrolled students and other potential users.

The security aspect of our network architecture is a main problem, where we have to elevate the level of security and monitor the networking behaviours, in order to ensure the availability of the online access to our web services. In addition, we have to supervise the local field of laboratory and assemble the data of exploited services and resources. Furthermore, we need to monitor the power supply of certain deployed systems due to the rupture of electricity at specific times.

Therefore, we developed a software entity to supervise the local network by pinging on deployed servers periodically after each fifteen minutes, and send a report after each hour to an e-mail account of maintenance service to monitor the web services, in addition of sending exceptional reports at any time when detecting that a server is out of function. In addition, we rely on the use of local camera to send continues surveillance videos through developed software in LabVIEW platform. Moreover, we developed a detection system to detect the opening and closing of laboratory's door and detect the existence of any individuals within the laboratory while relying on Raspberry Pi. Furthermore, the developed software is relied on to monitor the power supply of electricity using sensing interrupters to detect the circulation of current and send the information to the Raspberry Pi, and then forwarding it to the computer system where the software is responsible of data collecting, data archiving and reporting. The developed web-user interface in Fig. 1 helps to observe the detection states of sensors, which are used for online monitoring.

The online web user interface in Fig. 1 is based on exploiting independent local variables in LabVIEW platform of a principal VI (Virtual interface). This principal VI is developed to run continuously within a loop and communicate with sensors after each fifteen minutes to collect their data and determine anomalies of functioning.

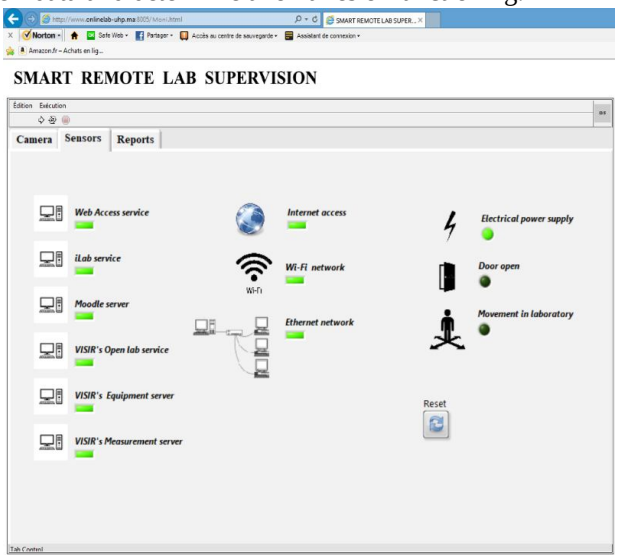

Figure 1: Online web user interface for supervision and monitoring of remote lab

We are working on embarking the developed software within the Raspberry Pi, separately from any computer, in order to make the developed software and used hardware as portable resources independently from the architecture of our remote lab's network.

3.SECURITY ASPECT OF REMOTE LABORATORIES AND E-LEARNING PLATFORMS

Nowadays, online web services are worldwide in use to support many services of learning, experimental contents and enterprise systems, while bridging between various apparatuses through the internet [16]. Web-based services are principal key element in the concept of Service Oriented Architectures (SOA), entailing based self-describing

components and entities that can be used by other software elements across the web in independent manners, which presents web-based services as the lingua franca to develop and incorporate different resources of software and hardware through the internet.

The security aspect of deployed web-based applications is, in many cases, quite poor and insufficient [17], [18] including remote experiments and e-learning platforms of remote laboratories where the lack of focus on the security of provided contents and delivered services through the internet and at local scales of networks.

Web services of e-learning platforms and remote laboratories are frequently deployed with integrated code vulnerabilities and network misconfigurations, as it is the common case of deployed web services at the global scale [19], [20]. This indisputable fact is confirmed by the field studies presented in [21], [22], which report the practices and results of experimental assessments and evaluations of security vulnerabilities on public available web services of different worldwide areas of businesses and activities. Numerous well-known tools of vulnerability scanning had been used to identify the flaws of security and implementation misconfigurations of these web services.

In these presented studies in [21], [22], large numbers of vulnerabilities were identified in different web penetration tests, where a considerable amount of tested services presented different types of security vulnerabilities and misconfigurations that could be harnessed and exploited. These results affirm that significant parts of web-based services are frequently deployed without proper security testing and evaluation. These conducted studies show that code injection vulnerabilities were- and still particularly frequent at the global scales of deployed services through internet [17].

These vulnerabilities are due to improperly coded web applications and web services that allow attackers to inject textual commands to vulnerable services, allowing for instance the access to critical resources of data, such as personal multimedia resources, credit cards data, etc.

Vulnerabilities allowing the widely known practices of XPath Injections and SQL Injections are globally common, even on the web services of remote laboratories and e-learning platforms where they integrate various techniques of software for data persisting, such as relying on relational databases [23] and XML solutions [24].

Web-based services are widely exposed through the internet, where any vulnerability of security may be divulged, uncovered and exploited by intruders and hackers. Therefore, to avoid having potential vulnerabilities within developed web services of remote laboratories and e-learning platforms, software developers should apply the best practices and techniques of software coding, perform precise security reviews and weaknesses fetching on developed codes, use different static code analyzers and conduct different processes of penetration testing from numerous aspects of view [25].

However, in most times, web service developers, in addition of many developers of software and applications, concentrate their focus on implementing the needed functionalities to respond to their client requirements and constraints of time-to-market. Commonly, this focus may disregard the security aspects of deployed resources, deployed web services and integrated contents. In this context, vulnerability detection tools and network scanners provide easy and low cost methodologies to asses and test these web services of remote laboratories and worldwide servers.

Web service developers conduct various automated processes of security scanning and verifying while relying on different vulnerability detection tools and related code scripts. In addition, they compare between the results of these utilities and tools to validate them, and use the most reliable among these tools and utilities to have a secured development of software. Numerous techniques of vulnerability detection have been proposed in different research projects and papers [25], including the techniques of code static analyzing and penetration testing.

Due to resources limitation or confronted time constraints, developers frequently have to select and choose specific tools among large available sets at the market, or other open source utilities, usually without having a real approximation of how much each one of them may be considered as reliable.

Precedent works of testing, analyzing and comparing show that the reliability and effectiveness of a considerable number of vulnerability scanning tools is poor and insufficient [21], [26], [27]. In fact, there are many weaknesses and limitations in numerous tools of vulnerabilities scanning either due to their low coverage or due to collecting false results.

Moreover, it is clear that the performance of many specific tools of vulnerability detection is strongly dependent on the specificities of conducted testing scenarios, the used programming languages, the used technologies within the tested web services, the types of vulnerabilities, etc. Furthermore, the same used tool of vulnerability detection may have different ambiguous results in different conducted scenarios of network scanning and web testing. Therefore, there is an absolute necessity to use various tools from different approaches and technical views to assess, compare and validate their assembled results and cover much more types of vulnerabilities and service misconfigurations.

The networks of remote laboratories and e-learning platforms are also frequently deployed with misconfigurations that make them vulnerable to MITM attacks (Man In The Middle attacks) [28], where the possibility of sniffing and spoofing user's transmitted data at the local scales, such as the professional or personnel data of researchers and professors. These MITM attacks may threat the ongoing research works of their victims and even threat critical personal data of credit cards and bank accounts. Therefore, there is a principal need to deploy secured architectures of networks with reliable

security measures, and deploy the right configurations and the best counter measures against potential attacks at the local levels of networks and through the Internet.

In our remote lab, we deploy numerous web services and computer systems that need to be properly secured. Therefore, we conducted different processes of web penetration testing and cybersecurity testing, to assess and evaluate the security aspect of our deployed networks and installed web-based services, in order to determine the most appropriate measures of security to deploy. These conducted processes are presented in section 5.

4. DEPLOYED RESOURCES AND NETWORK TOPOLOGY IN OUR REMOTE LABORATORY

We deploy different resources and systems in our remote laboratory for remote experimenting, virtual experimenting and e-learning. In addition, we managed to develop and adjust the incorporated resources of hardware and software to satisfy two of our primer axes of development and research. The first axe of our research is about developing and deploying shared architectures and topologies of software and hardware for

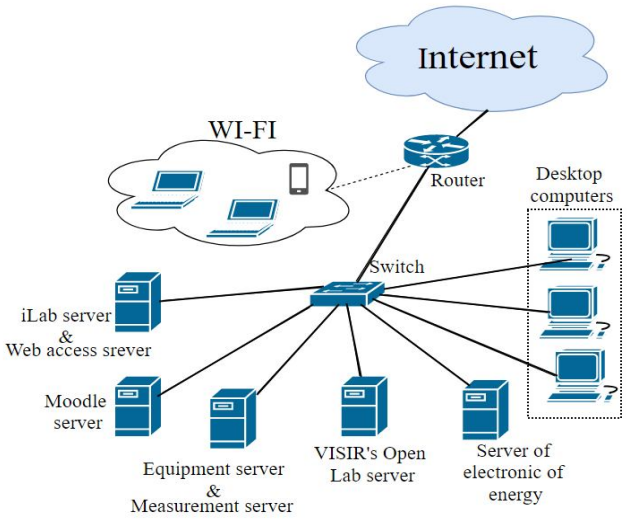

Figure 2: Deployed services and network topology of our remote laboratory

remote experimenting, to be exploited by different remote laboratories and educational establishments. The second axe of our research is about adapting usual hands-on laboratory resources of equipment and instruments to remote experimenting through the internet.

Among many resources and entities, we deploy VISIR system (Virtual Instrument Systems In Reality) for remote experimenting in electronics and electricity, we deploy the iLab architecture for emulated and simulated experiments while using LabVIEW resources, and we deploy the Moodle platform for distance learning and online experimenting on virtualized and simulated practices. Furthermore, we deploy other market products such as NI Elvis and Quanser system, which are usually used for local in-post experiments on computers. We adapted these resources of NI Elvis and Quanser to be exploited through the internet for remote experimenting in the field of electronic of energy.

The deployed system of VISIR (Virtual Instrument Systems in Reality) [29] was, basically, initiated and created in the Blekinge Institute of Technology (BTH). Numerous worldwide remote laboratories and educational establishments have deployed it; either for their own exploit or for further purposes of collaborative use through their own web-based services. VISIR system provides a remote environment and platform for remote experimenting in electricity and electronics. It was developed to serve similar traditional functionalities of manipulation and experimentation that usually take place in hands-on laboratories of electronics and electricity.

The Massachusetts Institute of Technology (MIT) in United States of America initiated and developed the iLab Shared Architecture (ISA) [30]. This Shared Architecture of iLab project has demonstrated and proved that online laboratory's use can spread and scale to thousands of benefiters dispersed on worldwide countries, where students (or other users) can access these online laboratories through simple standard administrative platforms and single sign-on interfaces as long as having reliable internet connections. Although this iLab platform is outdated, we still rely on it in order to extract its functionalities and deploy them in a new platform of e-learning and remote experimenting that we are currently developing.

One of the most widely used open-source platforms of Learning Management System (LMS): the Moodle platform. This LMS platform enables the creation of online web-based courses of documents, PDFs and videos. In addition, the Moodle platform provides the required services of identification and authentication to ensure the access to supported resources only by enrolled students [31]. This Moodle platform allows the exchange of data and educational contents among geographically dispersed users such as students, professors, instructors, etc. These exchanges are supported either through synchronous mechanisms of web-based communications such as chat and video conferencing, or through asynchronous web-based communication services such as discussion forums and workshops. Moreover, this platform of Moodle provides a monitoring service on accounts access to supported courses and other deployed contents.

The deployed resources of hybrid platform of e-learning and deployed network topology in our remote lab are as shown in Fig. 2. At this network topology in Fig. 2, we deploy a principal web access service to inform service users about all activities and services of distance learning and online experimenting of our remote lab. We deploy VISIR's measurement server and its equipment server on the same host, in order to control the hardware filed of VISIR's resources, receive the incoming requests of online

experimenting and to conduct those experiments.

We deploy VISIR's Open Lab platform for the processes of identification, authentication and scheduling, in order to experiment on VISIR system. In addition, we deploy another server of experiments in electronic of energy, which serves developed and adjusted experiments through LabVIEW resources while exploiting NI Elvis and Quanser after adapting them to remote experimenting.

Due to online sharing of different hardware resources of our remote lab through the internet, to be exploited by other webservers of collaborative establishments and laboratories; the security aspect of our network topology and its resources turns to be more critical and composed. This criticality and composition is due to the necessity of taking into account the interconnections, the accessing scenarios and the online exploit and sharing of these resources through the internet.

5. PROPOSED TOPOLOGY OF NETWORK AND SECURITY MEASURES

After conducting numerous processes of web penetration testing, to evaluate and asses the security level of our remote lab's network and determine its weaknesses and

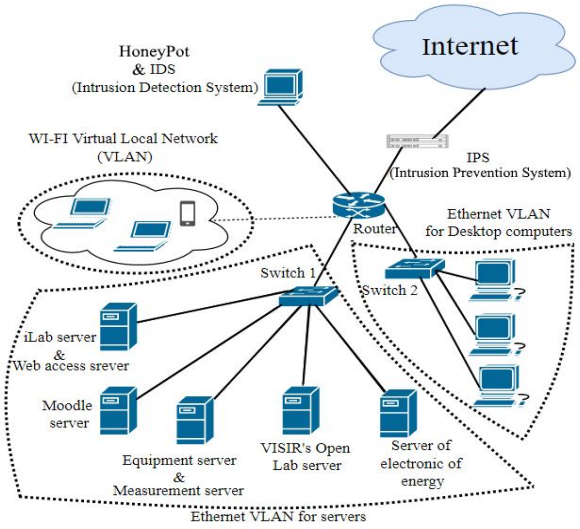

Figure 3: Proposed network topology for our remote laboratory and web services

vulnerabilities, we conducted additional processes of assessment to verify and measure the exploitability of those vulnerabilities. In addition, we repeated the conduction of these processes using different tools.

Moreover, we leveraged the captured credentials during our conducted Man In The Middle attacks (MITM), to scale through the deployed systems of our network. This scaling was conducted at the horizontal level by scaling to different systems, and at the vertical level by scaling to higher privileges of access. Furthermore, we relied on different tools, utilities and code scripts to execute those processes from different aspects of view, and validate the assembled results by comparing them.

We counted on using the black box approach where we approximated real life hacking scenarios, by supposing having no knowledge or preinformation about the deployed network architecture and deployed web services. During this utilized approach, our conducted procedures were based on the concept of the kill chain attack.

We relied on an ordered conduction during those processes of security testing and evaluating while basing on the concept of the kill chain attack.

At these processes of kill chain attack, we launched by the phase of passive reconnaissance, to explore how much existing leaked data on web services and social medias that may help malicious hackers to intrude and attack our remote lab's web services and access critical data of existing staff. Then, we conducted the phase of active reconnaissance, where we scanned all web services to retrieve their relative data and determine their used ports for internet, by utilizing different tools such as DNSMap, Traceroute, NMAP, Fierce, etc. Then we launched the processes of the exploit of determined vulnerabilities while using SQL inject, Low Ion Orbit Cannon, Metasploit, Social Engineer Toolkit, WebScarab, etc. Finally, we concluded the kill chain scenario by the process of in-poste exploit where we confirmed the exploitability of different vulnerabilities and network misconfigurations.

The resulted findings of exploitable security vulnerabilities are as follow:

- We found four SQL injection vulnerabilities in different deployed web services of our remote lab and e-learning platforms.
- We found three vulnerabilities of XML (Extension Markup Language) parser injection in our web services.
- We found three different vulnerabilities of Xpath (XML path) injections.
- We found two vulnerabilities of LDAP (Light Weight Data Access Protocol).
- We found two vulnerable servers to SMTP (Simple Mail Transfer Protocol) header injection.
- We found four deployed systems vulnerable to DOS attacks (Denial Of Service attacks).
- We found three vulnerabilities of XSS (cross-site scripting) through our web-based services.
- We have Multiplicity of vulnerable open ports of web services used by various servers.
- Our remote lab's network is vulnerable to Man In The Middle attacks (MITM attacks) at the locale scale.
- Certain number of our remote lab's web services are vulnerable to Man In The Middle attacks (MITM attacks) between users and web services.
- We found six computer systems with vulnerabilities of SSH (Secure Shell) and RDS (Remote Desktop Services).

The resulted findings of network misconfigurations are as follow:

- Having no reliable firewalls at the external level of network.
- Relying on medium composed passwords for computers in terms of sequence length, used strings and used digits.
- Using medium composed passwords for servers in terms of sequence length, involved characters and used digits.
- Using weak passwords for web login accounts of online services.
- Relying on weak internal policies and roles of internet access and networking.
- Using weak password and encryption on deployed Wi-Fi.
- Vulnerable network architecture to Man In The Middle attacks (MITM attacks) at the local scale of topology.
- Scalable network topology and scalable systems by using repeated passwords and iterative credentials.

Responding to the critical necessity of elaborating and deploying secured network topology for our remote laboratory and e-learning web services, we proposed a much more reliable architecture of network, as shown in Fig. 3, to deploy the software and hardware resources, and more properly configure the systems of networks and their interconnections. The proposed architecture of network is based on the standards of ISO/IEC 27033 [32].

The proposed security measures and suggested counter measures against potential attacks and potential intruders to our e-learning web services are based on the standards of ISO/IEC 27033 and described standards of RIT (Rochester Institute of Technologies) [33]. These propositions and suggestions are detailed to be more specific and suitable to our remote lab's networks and our deployed web services, and they are as follow:

- Relying on technical architectures of VLANs (Virtual Local Architecture of Networks) to separate and insulate the computing systems of the staff from the deployed servers and other critical systems.
- Separating the local networks of Wi-Fi from deployed Ethernet networks using the VLAN concept of network architectures.
- Relying on static IP addressing for Ethernet networks and Wi-Fi networks, instead of using the dynamic version of IP addressing of DHCP (Dynamic Host Control Protocol).
- If there is a necessity of deploying Wi-Fi networks with dynamic IP addressing of DHCP, at least deploy these Wi-Fi networks with composed passwords, change or modify passwords periodically and use the protocols of WPA3 (WI-FI Protected Access 3) or WPA2 for more access security on those Wi-Fi networks.
- Configuring reliable encryption methods for networking and communication such as AES (Advanced Encryption Standard) and Twofish.
- Deploying and configuring a monitoring service at the local scale of network, to supervise the networking behaviours and control the internet access, in addition of detecting the malicious activities or attempts.
- Deploying a Honeypot station, which is a decoy web-based system, to attract the attention of potential attackers, divulge and reveal their activities, identify their intruding behaviours and stop them before conducting any damages. Furthermore, stop them before accessing vital resources of web services and capturing important data of the staff.
- Deploying Intrusion Detection System(s) (IDS) and Intrusion Prevention system(s) (IPS) at the locale scale of network architecture.
- Deploying Web Application Firewall(s) (WAFs) for much more security through integrated web-based applications.
- Open all used networking ports on only the principal deployed server, and configure it as a forwarding proxy to the online services of other deployed servers, to make them less detectable and accessible by potential malicious intruders and hackers.
- Deploying multilevel firewalls and policies for network security, to condition the communication scenarios, in addition of coordinating the allowed protocols of interconnecting and expected behaviours of networking.
- Installing antiviruses and malware detectors on each deployed computer system and webserver.
- Disabling the configurable option of Near Field Transmission (NFT) on routers.
- Using long sequences of composed and complexed passwords for each computer system and webserver.
- Changing the used passwords periodically; at least once after each successive three months.
- Relying on access lists to control the access to the equipment of networks.
- Creating backups for the configurations of all deployed servers and networking systems.

6. CONCLUSION

There are multiple factors that influence the success of e-learning and online experimenting services through remote laboratories. The security aspect of provided web services and deployed web-based applications of e-learning and remote experimenting is massively influencing the availability and reliability of deployed resources. This influence is significantly reflecting on the quality and success of distance learning and remote experimenting through the internet.

Relying on smart environment control and management in our remote laboratory helps to have a continuous tracking of

service availability and have a continuous surveillance on locale space. In addition, it helps to determine the causes of potential situations of web service ruptures.

The proposed network topology and proposed security measures and attack counter measures for our e-learning platforms and our remote services of experimenting, aim to provide a more reliable approach of cybersecurity through web-based applications and webservers, to augment the availability and reliability of our online web services.

REFERENCES

1. G. Attwell. ***Evaluating E-learning: A Guide to the Evaluation of E-learning***, vol. 2, Evaluate Europe Handbook Series, 2006.
2. Y. S. Wang. **Assessment of learner satisfaction with asynchronous electronic learning systems**, J. *Information and Management*, vol. 41, no. 1, pp. 75–86, 2003. https://doi.org/10.1016/S0378-7206(03)00028-4
3. A. G. abdel WAHAB. **Modeling students' intention to adopt e-learning: A case from Egypt**, *The Electronic Journal of Information Systems in Developing Countries*, vol. 34, no. 1, pp. 01–13, 2008.
4. J. K. Lee, W. K. Lee. **The relationship of e-learner's self-regulatory e□cacy and perception of e-learning environmental quality**, *Computers in Human Behavior*, vol. 24, no. 1, pp. 32–47, 2008.
5. B. C. Lee, J. O. Yoon, I. Lee. **Learners acceptance of e-learning in south korea: Theories and results**, *Computers & Education*, vol. 53, no. 4, pp. 1320–1329, 2009.
6. H. Mohammadi. **Investigating users' perspectives on e-learning: An integration of TAM and IS success model**, *Computers in Human Behavior*, vol. 45, pp. 359–374, 2015. https://doi.org/10.1016/j.chb.2014.07.044
7. J. Mtebe, C. Raphael. **Key factors in learners' satisfaction with the e-learning system at the university of dar es salaam, Tanzania**, *Australasian Journal of Educational Technology*, vol. 34, no. 4, 2018.
8. S. Eom, N. J. Ashill, **A system's view of e-learning success model**, *Decision Sciences Journal of Innovative Education*, vol. 16, no. 1, pp. 42–76, 2018.
9. H. M. Selim. **Critical success factors for e-learning acceptance: Confirmatory factor models**, *Computers & Education*, vol. 49, no. 2, pp. 396–413, 2007.
10. S. Ozkan, R. Koseler. **Multi-dimensional students' evaluation of e-learning systems in the higher education context: An empirical investigation**, Computers & Education, vol. 53, no. 4, pp. 1285–1296, 2009.
11. R. Heradio, L. de la Torre Cubillo, D. Galan, F. J. Cabrerizo, E. H. Viedma, S. Dormido. **Virtual and remote labs in education: A bibliometric analysis**, *Computers & Education*, vol. 98, pp. 14–38, 2016. https://doi.org/10.1016/j.compedu.2016.03.010
12. R. Heradio, L. de la Torre Cubillo, S. Dormido. **Virtual and remote labs in control education: A survey**. *Annual Reviews in Control*, vol. 42, pp. 1–10, 2016.
13. E. Ahmed, I. Yaqoob, A. Gani, M. Imran, M. Guizani. **Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges**, *IEEE Wireless Communications*, vol. 23, no. 5, pp. 10–16, 2016.
14. K. A. Olatunji, A. Oguntimilehin, O. A. Adeyemo, **A Mobile Phone Controllable Smart Irrigation System**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 1, pp. 279–284, 2020. https://doi.org/10.30534/ijatcse/2020/42912020
15. M. Poongothai, P. M. Subramanian, A. Rajeswari, "**Design and implementation of iot based smart laboratory**, *in Proc. 5th International Conference on Industrial Engineering and Applications*, Singaphore, Singaphore, IEEE, 2018.
16. G. Alonso, F. Casati, H. Kuno, V. Machiraju. ***Web Services: Concepts, Architectures and Applications***, vol. 2, Springer, 2004. https://doi.org/10.1007/978-3-662-10876-5
17. S. Christey, R. A. Martin, Vulnerability type distributions in cve (May 2007). [Online]. Available: https://cwe.mitre.org/documents/vuln-trends/index.html
18. R. K. Alqurashi, M. A. AlZain, B. Soh, M. Masud, J. Al-Amri, **Cyber Attacks and Impacts: A Case Study in Saudi Arabia**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 1, pp. 217–224, 2020.
19. L. Lowis, R. Accorsi. **On a classification approach for soa vulnerabilities**, *in Proc. 33rd Annual IEEE International Computer Software and Applications Conference, Seattle, WA, USA, IEEE*, 2009.
20. M. Jensen, N. Gruschka, R. Herkenhoner, N. Luttenberger. **Soa and web services: New technologies, new standards- new attacks**, *in Proc, Fifth European Conference on Web Services, Halle, Germany, IEEE*, 2007.
21. M. Vieira, N. Antunes, H. Madeira. **Using web security scanners to detect vulnerabilities in web services**, *in Proc.* IEEE/IFIP International Conference on Dependable Systems and Networks, *Lisbon, Portugal, IEEE*, 2009.
22. A. Neumann, N. Laranjeiro, J. Bernardino. **An analysis of public rest web service apis**, *IEEE Transactions on Services Computing*, 2018. https://doi.org/10.1109/TSC.2018.2847344
23. Tpc benchmarktm app (application server), specification, version 1.3 (February 2008). [Online]. Available: http://www.tpc.org/tpc_documents_current_versions/pdf/tpc-app_v1.3.0.pdf
24. W. Meier. **exist: An open source native xml database**, International Conference on Object Oriented and Internet-Based Technologies, Concepts, and

Applications for a Networked World, Erfurt, Germany, 2002.

25. D. Stuttard, M. Pinto. ***The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws***, John Wiley & Sons, 2011.
26. N. Antunes, M. Vieira. **Comparing the e□ectiveness of penetration testing and static code analysis on the detection of sql injection vulnerabilities in web services**, *in Proc. 15th IEEE Pacific Rim International Symposium on Dependable Computing, Shanghai, China, IEEE*, 2009.
27. J. Fonseca, M. Vieira, H. Madeira, **Testing and comparing web vulnerability scanning tools for sql injection and xss attacks**, *in Proc. 13th Pacific Rim International Symposium on Dependable Computing, Melbourne, Qld., Australia, IEEE*, 2007.
28. Y. Eytani, S. Ur. **Compiling a benchmark of documented multi-threaded bugs**, *in Proc. 18th International Parallel and Distributed Processing Symposium, Santa Fe, New Mexico, USA, IEEE*, 2004.
29. J. G. Zubia, J. Cuadros, S. R. Yesa, U. Hernandez, P. Orduña, M. Guenaga, I. Gustavsson**. Empirical analysis of the use of the visir remote lab in teaching analog electronics**, *IEEE Transactions on Education*, vol. 60, no. 2, pp. 149–156, 2017 https://doi.org/10.1109/TE.2016.2608790.
30. J. L. Hardison, K. DeLong, P. H. Bailey, V. J. Harward. **Deploying interactive remote labs using the ilab shared architecture**, *in Proc. presented at 38th Annual Frontiers in Education Conference, Saratoga Springs, NY, USA, IEEE*, 2008.
31. G. C. Oproiu. **A study about using e-learning platform (moodle) in university teaching process**, *Procedia - Social and Behavioral Sciences*, vol. 180, pp. 426–432, 2015. https://doi.org/10.1016/j.sbspro.2015.02.140
32. Iso/iec 27033 (2015). [Online]. Available: https://www.iso27001security.com/html/27033.html
33. Rit standards (2015). [Online]. Available: https://www.rit.edu/security/content/intro-policies-standards