System Breach: The Awareness and Vulnerability That People Face

Edwin Romero Pérez
Master of Engineering in Computer Engineering
Advisor: Nelliud Torres, DBA
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— The Cyber Force Support webpage will educate the user to protect the system through the correct use of tools associated to the cyber security. This will help maintain, protect and support properly the system and network security. It will also explain how to use a tool to audit informatic security. Take for example, security tests and system penetrations, which will allow the handling of cyber-attacks, whose objective is the cyber defense, as well as to capture data, shared sections and communications. It performs analysis on communications networks whose objective is to capture, troubleshoot and avoid threats like computer viruses, data breaches, and Denial of Service attacks on the network by analyzing data packages. The goal is to help users understand the risk of not knowing the threats and consequences of security breaches; therefore, the importance of Cyber Force Support.*

Key Terms *— Audit Information Security, Cyber Attacks, Cyber Defense, Troubleshoot.*

INTRODUCTION

According to Ponemon Institute, a Cyber Crime Study indicates that cyber-attacks generally refer to criminal activity conducted via internet [1]. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, among others. Based on these findings, organizations need to be more aware in protecting their most sensitive and confidential information [1].

Therefore, it's important to not ignore successful attacks and threats since that means, the attacker has penetrated the system, which implies that it's one step away from stealing all information and confidential data, both personal and/or of the company, as well as considering that these attackers are hackers who have the knowledge and experience to manipulate everything in your system. As a result, the content and purpose of Cyber Force Support is fundamental and necessary, both to raise awareness and understand the vulnerability that people face when the system is breached as well as to prevent and protect.

The aim of this project is to present strategies and ideas intended to accomplish the full development of the Cyber Force Support. It's divided into six sections for better understanding. The sections are the literature review, problem statement, methodology, results, conclusions and references.

LITERATURE REVIEW

A series of studies associated with the risks of security management reveal that many organizations have overlooked security systems and don't take measures to correct the vulnerabilities in the system [2]. The researcher can list non-efficient ways, which can lead to a possible cyber security problem, as shown in Figure 1.

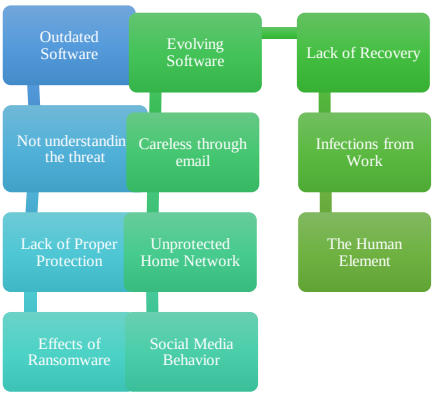

Figure 1
Possible Cyber Security Problems

Security Scheme

The importance of informatics is to:

- Identify and select what should be protected, such as sensitive information.
- Establish levels of priority and importance on this information.
- Know the consequences that the loss of sensitive data would bring to the company, in terms of costs and productivity.
- Identify the threats, as well as the vulnerability levels of the network.
- Perform a cost analysis in prevention and recovery to reduce the impact.

It's important to take into consideration that the threats and vulnerabilities will not disappear in their entirety. The implementation of security measures such as those mentioned above, will help to reduce the impact on the systems. Before starting to implement Cyber Force Support, a series of webpages will be carried out with information on cyber security, articles and latest free tools for computer security. The purpose of consulting and studying this information and security tools, is to get acquainted with the latest attacks and tools available on the Internet. Once the different security tools are chosen, each one will be approved, presenting a tutorial on how to use and manage it. Brief summary is illustrated in Figure 2.

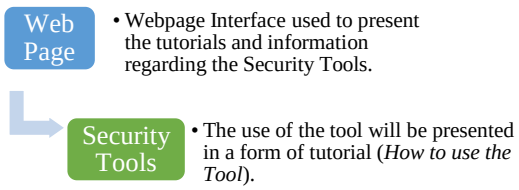

Figure 2
How the Cyber Force Support will be Carried Out

The Cyber Force Support webpage will show "How to" tutorials of the tools. For every tool, there will be background information about where and how to download and install the tool. Table 1 describes the Cyber Force Support Tools.

Table 1
Cyber Force Support Tools

TOOLS	DESCRIPTION
Wireshark	Used to capture and view the data traveling back and forth on your network. Provides the ability to drill down and read the contents of each packet and is commonly used to troubleshoot network problems and to develop and test software.
NMAP	Scanning and host detection tool used for several steps of penetration testing. Also, can be used as a vulnerability detector or a security scanner. Runs on operating systems like Windows, Linux, BSD and Mac.
PFSENSE	Firewall / router software installed on a physical or virtual machine to generate a dedicated firewall/router for a network. It can be configured and upgraded through a web-based interface and is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNS server and as a VPN endpoint.
THC Hydra	Hydra is a parallelized login cracker which supports numerous protocols to attack. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.
Kali Linux	Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
Squid	Unix-based proxy server that caches Internet content closer to a requestor than its original point of origin. Squid supports caching of many different kinds of Web objects, media files, including those accessed through HTTP and FTP. This, accelerates response time and reduces bandwidth congestion.
Squidguard	Web filter plugin for Squid which is used to restrict access to domains/URLs based upon access control lists. When Squid Guard receives a request, it's examined and will either allow the page to load or

	will redirect to a predetermined "block" page or script.
SNORT	Network intrusion detection system (NIDS) or packet sniffer that monitors network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. Used in TCP/IP-traffic sniffers and analyzers for detection of attack methods, including denial of service, buffer overflow, CGI attacks, stealth port scans, and SMB probes.

Content Outline and Tutorials

In this section, the researcher discusses how the Cyber Force Support will be presented. When users access the webpage, they will see different tabs with tools names and an introduction background with information about the purpose of the webpage. Also, there will be a menu with information about the tools, links to download the tool, references of security strategies and articles, contact information and others.

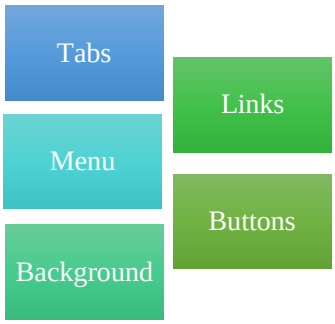

Figure 3
Page Preview

PROBLEM STATEMENT

One of the mayor concerns that are disregarded by companies and regular users is the fact that they are not properly educated regarding cyber-attacks, system breaches nor hackers. Therefore, a successful attack will lead to compromise and expose any confidential information of the company or single user, which can be subtracted and modified to the attacker's benefit.

Based on studies performed by Easttom, it's established that despite daily horror stories, however, many people (including law enforcement professionals and trained computer professionals) lack an adequate understanding about the reality of these threats. Clearly the media will focus attention on the most dramatic computer security breaches, not necessarily giving an accurate picture of the most plausible threat scenarios [3].

One of the data analytics and technology companies that assists organizations and individuals in making informed business and personal decisions is Equifax. Based on Lim, Equifax had a massive data breach that costed the company over $4 Billion dollars [4].

Analysts at William Blair estimate that after insurance kicks in, Equifax's costs tied to dealing with this crisis could run between $200 million and $300 million [4]. They note that in 2015, rival credit bureau Experian experienced a smaller-scale breach that affected 15 million people and cost that company about $20 million in immediate costs. Equifax's breach affected roughly ten times as many people. Hence, they expect Equifax to incur at least 10 times the expenses [4].

It's not uncommon to encounter the occasional system administrator whose knowledge of computer security is inadequate. Currently, all systems are exposed and vulnerable to an attack. According to Wong, studies have demonstrated that one of the great reasons behind this is the Internet [5]. For example, before the internet, the systems had approximately dozens of users, which worked for a single organization, using its own software or a commercial software. Also, the data was moved over discs or tapes [5].

The reality is that everything changes drastically with the arrival of the internet. It's not just dozens of users, but billions all around the world, which leads to new problems much more complex to resolve. According to the different sectors (Finance Information, Professional Information Manufacturing, Mining Healthcare ADM, Retail and Edu finance), it shows that the 63% of the breaches have been due to weak passwords, default passwords or stolen passwords [5].

One can assume that of many types of cyber-attacks, in most of cases, several bad results are obtained. Take for example the hacking, which is prompt by people that write programs or viruses that can affect profusely any machine, whose function it's based on exploiting buffer that allows the codes to run. On top of that, it also tricks the user into running the code from a web page or even from emails without even realizing it.

This leads the critic production servers to interrupt their function over the infection of a virus, which at the same time, goes into the machines of the end-users causing the network flow to overheat as well as the webserver. Therefore, another bad result will be a specific attack, whose purpose is to steal or damage the corporation's data.

METHODOLOGY

As a solution to the previously established problem, the researcher developed a webpage whose objective will be focused in creating conscience and create awareness regarding the cyber-attacks and the system security. It's intended to educate the user with a series of tutorials and tools for their cyber-security. The different tutorials will show how to acquire the tool, its utility, the operative system in which it functions, how to install it, how to use the tools through personally advised tests, among others.

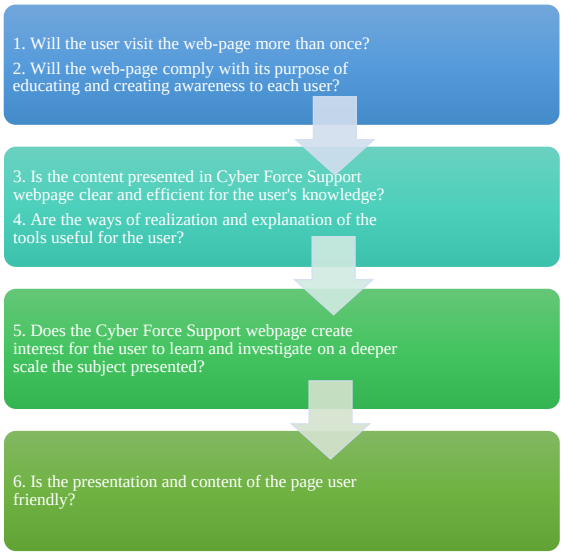

Figure 4
Research Questions for Web Page Development

Cyber Force Support promotes the importance of knowing and managing vulnerabilities in a system, possible attacks, theft and corruption of data. Some research questions purpose is to contribute to the development of the web page. It's important to emphasize that the questions illustrated in Figure 4 can vary during the development process.

Systems are being vulnerable to attacks by hackers. There's a serious situation with the systems that are being attacked and there's a lack of action in the face of these events, mainly due to the deficit of knowledge in the field of computer security. Poor security practices could put everyone's information in the hands of vague people.

Oberman stated that more than half of security professionals believe that their organizations' security controls don't provide adequate protection against advanced cyber-attacks, according to more than 5,000 IT professionals from 15 countries including the U.S. [6]. Stating how far-ranging is the problem and how great is the impact, the same portion of IT professionals said that executives fail to appreciate the value of putting effective security controls in place, and do not equate a data breach with financial loss [6].

The consequences of not solving the problem lead to a similar study conducted also by The Ponemon Institute, which concluded that a majority of IT professionals fail to communicate security risks effectively to upper management [1].

Since cyberattacks are increasing in size and cost, they are the fastest growing crime in the U. S. A list of the Top 10 of the world's largest cyberattacks was revealed by Outpost24, in which mentions the number one spot was Yahoo!. Yahoo! announced it had suffered a cyberattack in 2014 that affected 500 million user accounts, constituting the largest massive hacking of individual data directed against a single company [7]. Names, dates of birth, telephone numbers and passwords were stolen. While the company assured users that banking data had not been affected, it nonetheless recommended caution. Prior to this event, in 2012 the hacker "Peace" had sold 200 million usernames and passwords for $1900 [7].

As mentioned by Outpost24, in March 2018, Yahoo! confessed to being hacked once again. This time, "only" 32 million accounts were affected [7]. But the cyberattack relaunched the investigation of the 2014 hack, as the attackers used a tool stolen that year, allowing them to create malicious cookies and log in without passwords. A direct result of this is that the firm was bought by Verizon in 2017 for $4.5 million instead of the $4.8 million announced in 2016. In December 2018, Yahoo! has admitted that all the 3 billion user accounts had been hacked in 2013. This cyberattack is the most significant in Internet history [7].

Last year, Cybersecurity Ventures, predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015 [8]. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined [8].

The goal of this research addresses the problem by presenting ways of how to protect the systems with the application of security techniques. Also, the proposed study offers to solve the main problem of attacks by hackers and the lack of importance in handling such events. It's intended to promote the user to know more about computer security, using tools of the computer security. This research will help the user's knowledge through tutorials explaining the use of the tool. The potential for the generation of results is to ensure that possible cyber-attacks can be managed properly and at the same time how to avoid them by applying the knowledge acquired in Cyber Force Support.

RESULTS

After understanding the goal and importance in interpreting the problem and presenting a solution to it, is possibly an option to work for the master's project. The researcher was struck by this issue of computer security, to be developed as a project, since both personally and professionally, have witnessed the mismanagement of successful attacks in big companies, as well as how vulnerable is a system or ignored when not knowing the consequences of them. Nowadays, this problem that the researcher presents as a project is one which has no solution, due to lack of knowledge, as well as, the discipline of a user when using the system.

When researching about *cyber-security*, everything comes across thousands of solutions and measures to prevent attacks and even tools or programs whose function is the systems protection, but these programs and their proper training come at a great cost, which many companies are not willing to pay for. The web page that the researcher intends to develop will be a source of support with tutorials of use and management of computer security tools free of cost. The page's interface will allow the user to access a series of tutorials, find information on the security tools and educate themselves about security.

Finally, the project is based on the initially established problem, which aims to build and develop Cyber Force Support as a reliable reference source for its users. In the future, the content of the website will be more robust, thus implementing a more comprehensive concept, through tutorials on security tools. As new tools come out, new tutorials will be added as sources of security knowledge on the website.

Table 2
Milestones

MILESTONES	DESCRIPTION
Proposal	The function of this document is to present the proposal of this project. You will also find information of the design of Cyber Force Support security tools used for the *"How to"* tutorials.
Design	During the Design stage, the researcher will be preparing the webpages interface, how information will be presented and planning tutorials.
Development	Once the interface on the webpage is ready to be populated, the researcher develops the tutorials along with the relative information for the Cyber Force Support webpage.

Testing and Release	During the testing and release stage, the researcher will conduct functionality and comprehensive tests to the Cyber Force Support before release.
Final Report	When Cyber Force Support is successfully tested, the webpage will be released to the Web, seeing the results, visits and feedback of the users.
Poster	In order to show the result of solution of the project, a poster will be developed and designed according to the guidelines provided by my advisor.

CONCLUSIONS

In order to develop the Cyber Force Support webpage, the use of security tools and webpage interface will be used as resources to accomplish this project.

For the development of the Cyber Force Support webpage, the researcher uses the user base open "*SDK*" to design the webpage through WIX, followed by Security Tools in which users can choose with different purposes, such as web scanners, sniffers, password audit, pocket crafters, etc. The "*How to*" tutorials will be used for the display on The Cyber Force Support webpage.

REFERENCES

[1] Ponemon Institute. (2013, October). *Cost of Cyber Crime Study: United States* [Online]. Available: https://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf. [Accessed: February 18, 2019].

[2] Previews Contributors. (2013, June 25). *Study: Majority of Organizations Committed to Risk-Based Security Management*," *Previews Contributors* [Online]. Available: https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/study-majority-of-organizations-committed-to-risk-based-security-management/. [Accessed: February 21, 2019].

[3] C. Easttom, *Computer Security Fundamentals*. Third Edition. Indiana, USA: Pearson Education Inc, 2016, ch. 1, sec. 4, pp. 3.

[4] P. Lim. (2017, Sept. 12). *Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far* [Online]. Available: http://money.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/. [Accessed: April 29, 2019].

[5] A. Wong. (2016, Nov.). *Cybersecurity: Threats, Challenges, Opportunities* [Online]. Available: https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf. [Accessed: March 9, 2019].

[6] E. Oberman. (2014, July 2). *A lack of Communication on Cyber Security Will Cost Your Business Big* [Online]. Available: https://www.entrepreneur.com/article/235318. [Accessed: March 11, 2019].

[7] Outpost24. (2018, Dec. 3). *TOP 10 of the world's largest cyberattacks* [Online]. Available: https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks. [Accessed: May 7, 2019].

[8] Cybersecurity Ventures. (2019). *Cybercrime Damages $6 Trillion by 2021* [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. [Accessed: May 7, 2019].