APPLYING VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) AND NETWORK ENHANCEMENT ON THE NETWORK INFRASTRUCTURE OF JOURNEY TECH INC.

Kit Arvin R. Cadiente
University of Santo Tomas
Taytay, Rizal, 1920, Philippines
2015081035@ust-ics.mygbiz.com

Rafael A. Castro
University of Santo Tomas
Quezon City 1107, Philippines
2015081607@ust-ics.mygbiz.com

Elia Van A. Gica
University of Santo Tomas
Las Pinas City, 1745, Philippines
eagica@ust-ics.mygbiz.com

Kathrice Marie C. Mora
University of Santo Tomas
Sampaloc, Manila, 1015, Philippines
2015086062@ust-ics.mygbiz.com

Joan V. Ternio
University of Santo Tomas
Las Pinas City, 1742, Philippines
2015081556@ust-ics.mygbiz.com

ABSTRACT

The purpose of this project is to establish a Vulnerability Management process for Journey Tech Inc., to be periodically conducted by their organization as it is important for an organization to perform continuous vulnerability management and remediation so weaknesses and vulnerabilities may be discovered before they can be exploited.

The Vulnerability Assessment and Penetration Testing Work Flow was used as the methodology as it comprises all of the necessary steps to the VAPT process such as Vulnerability Detection, Attack and Penetration, and Remediation. The implementation of the project objectives were done in a simulated virtual environment where the twelve (12) servers and the firewall appliance of the company were replicated.

The researchers used the OpenVAS tool to execute Vulnerability Detection while Metasploit was used for Penetration testing. The suggested Remediation solutions and fixes stated in the Vulnerability scan reports produced were applied to the machines to significantly decrease the number of vulnerabilities found per machine.

The results were monitored and each objective was tested to verify that the client's requirements were properly met. The researchers also provided a network enhancement proposal and a proposed remediated network topology.

KEYWORDS
Network Security, Vulnerability Assessment, Penetration Testing, Remediation, threats

1. INTRODUCTION

As organizations expand on a larger scale to provide the best possible service/s, they have also become more and more reliant on technology and the functionality of computer networks for their operations. As these networks become more complex and with the fast-paced development of new vulnerabilities and exploits on a daily basis, security flaws become an issue as these networks are increasingly faced with security threats from a wide range of sources. Last 2017, Journey Tech Inc. faced a great struggle when their network was maliciously attacked by an unknown hacker. Due to the lack of knowledge on network security and knowledge on threat control, the company was not able to prevent the event from happening and was also not able to perform countermeasures and responses to the said attack. Their systems and databases, as well as critical data they needed for their business operations (e.g. GPS data) were compromised. Because of this, all configurations were reset to default and the company took some time to recover.

With the rise in hacking attempts and increase of cyber-attacks, irrespective of organization/industry type, there is a need for a process to continuously find and remediate network vulnerabilities. Thus, the researchers decided to introduce a Vulnerability Management process to the organization. To determine what security flaws and vulnerabilities are present in the company's current network, the proponents will perform Vulnerability Assessment and Penetration Testing (VAPT). With this approach, the company will be given a more detailed view of the threats facing its network. The VAPT process will be divided into two main tasks: the Network Vulnerability Assessment and Network Penetration Testing.

2. OBJECTIVES

2.1. General Objectives

The project aims to develop and implement a Vulnerability Management process, implement remediation to the vulnerabilities found and propose an enhanced version of the network.

2.2. Specific Objectives

1. To replicate the 12 servers and one firewall appliance of the company.
2. To install a vulnerability assessment software on the proponent's device, which will be used in scanning the 12 replicated servers and one firewall appliance in the simulated environment.
3. To perform a vulnerability assessment scan, on the 12 servers and one firewall appliance on the simulated network, in order to identify the security issues of Journey Tech Inc.
4. To generate a report on the results obtained from the vulnerability assessment scan.

5. To perform a penetration test on the replicated servers and firewall appliance, to verify exploitable vulnerabilities that can be used to an attacker's advantage.
6. To implement remediation based on the reports generated during the Vulnerabilities Assessment.
7. To propose an enhanced version of the network on a device level

2.3. Scope and Limitations

This project includes applying Vulnerability Assessment and Penetration Testing (VAPT) with analysis and report.

Furthermore, the project includes the following:

- Replication of the 12 servers and one firewall appliance of the company on virtual machines.
- Installation of an open-source vulnerability assessment tool (OpenVAS) that will scan the network devices using their IP addresses.
- Conducting a vulnerability scan on the 12 replicated servers and one replicated firewall appliance, which will include the scanning of well-known ports.
- Generate a report which will include the following details about the vulnerability assessment:
    1. Name of Scan
    2. Severity Level
    3. Vulnerability Detection Result
    4. Impact
    5. Solution
    6. Affected Software/OS
- Installation of an open-source penetration testing tool (Metasploit) on an external device that will be used to exploit the network vulnerabilities that was found on the generated network vulnerability assessment result.
- Conducting a penetration test on the 12 replicated servers and one replicated firewall appliance on the simulated network.
- Implement the appropriate remediation solution to high severity and common vulnerabilities based on the report generated by OpenVAS. These remediation solutions include:
    1. Security Patching
    2. Mitigation
    3. Workaround Fixes
- Proposal of network enhancement on a device level.
    - This project is limited to:
- Due to the simulated environment limitations, a similar topology from the company's current network topology will be built with one switch and a minimum of four end devices to hold the 12 replicated servers on virtual machines.
- Replicate servers will include the server configuration. Due to client restrictions, actual data will not be provided.
- Company end devices are not included in the Vulnerability Management Process.
- Penetration testing will only be done on the simulated network.

- Execution of the vulnerability assessment scanning will be done on the simulated network.

4. REVIEW OF RELATED LITERATURE

The researchers aim to implement a Vulnerability Management process using the Vulnerability Assessment and Penetration Testing (VAPT) approach that will be performed on the servers, switches and firewall appliance of Journey Tech Inc. A regular vulnerability assessment is necessary because threats on network security continually change and evolve, and it is important to ensure that the organization's security is able to match this [1] through periodic vulnerability assessment and remediation. VAPT will be done as a step-by-step process that will be divided into two main agendas: Vulnerability Assessment, where the weaknesses and loopholes of the network will be identified, and Penetration Testing, in which the network will be exploited in an authorized manner [2]. The purpose of executing the VAPT process as a whole is to discover the flaws in the current security setup of the company, to present an overview of the potential threats or possible malicious attacks that the network may be challenged with, and to provide intelligence needed to efficiently plan threat mitigation strategies [3].

To start the VAPT process, a Vulnerability Assessment on the network of Journey Tech Inc. will be conducted. The weaknesses of the organization's network will be listed in a non-intrusive approach. This will enable the organization to identify critical vulnerabilities that they may prioritize to resolve based on the current available resources. It also aims to highlight the overall security posture of the organization, which can assist the organization in trending the level of risk exposure that currently exists on the network, information that will help in deciding the security measures and solutions needed to be put in place [4].

After the Vulnerability Assessment, the next step is to conduct Penetration Testing against the organization's network. Penetration Testing usually involves the use of attacking methods conducted by trusted individuals that are similarly used by hostile intruders or hackers [5]. Penetration testing simulates a real-world attack against a target network or application ([6] which will enumerate what vulnerabilities may be exploited by potential attackers in the future. Penetration testing may assist the company to fine-tune and check improvements in software or patches to proactively remove defined risks [7]. Proper penetration testing always ends with specific recommendations for addressing and fixing the issues that were discovered during the test. On the whole, this process is used to help secure computers and networks against future attacks [8]. For this project, the researchers/testers will be provided with partial disclosure of information about the test targets and will use these pieces of information to gather more by conducting the tests. This approach is also known as Grey Box Testing. It saves time for the penetration testers to uncover information that is publicly available. [9].

A second Vulnerability Scan Test will be conducted during the Remediation stage of the project. This will ensure that the security patches that were put in place during the remediation phase were effective and reviewing and analyzing the system for new possible threats and attacks.

For the Vulnerability Assessment, Open Vulnerability Assessment System (OpenVAS), a vulnerability scanner will be installed in one of the proponent's device which will present a summary of computer networks security level. [10]. OpenVAS is an open source software that is capable of scanning systems and provides a list of security issues found by the software. The software is also capable of giving possible solutions to the issues mentioned [11]. This security scanner will work hand in hand with a day by day overhauled feed of Network Vulnerability Tests (Nvts), in excess of 30,000 in aggregate (as of April 2013) [12]. For the Penetration Testing phase, Kali Linux, an open source project that is maintained and funded by Offensive Security, a provider of world-class information security [13].
After the Penetration Testing Phase, Remediation would be initiated. Some vulnerabilities can be resolved through the application's latest version or the latest OS patch. [14].

Succeeding the Remediation phase, proponents would propose an enhanced version of the network which may include different network infrastructure changes depending on the current posture of the organization network security.

4. METHODOLOGY

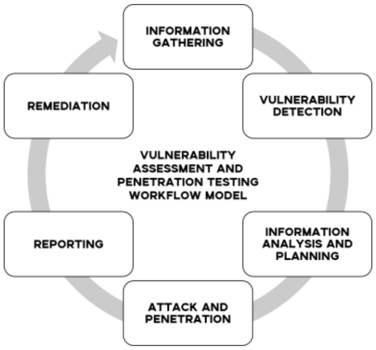

INFORMATION GATHERING
VULNERABILITY DETECTION
INFORMATION ANALYSIS AND PLANNING
ATTACK AND PENETRATION
REPORTING
REMEDIATION
VULNERABILITY ASSESSMENT AND PENETRATION TESTING WORKFLOW MODEL

Figure 1. VAPT Workflow

The Vulnerability Assessment and Penetration Testing Work Flow Model which the researchers chose to use as it sufficiently covers all the tasks needed to perform VAPT on the client network. The model consists of 6 phases, namely the Information Gathering phase, Vulnerability Detection phase, Information Analysis and Planning phase, Attack and Penetration phase, and Reporting phase.

In order to gather the information needed for this project, the researchers consulted representatives of the company on how the servers and the firewall should be replicated in the simulated environment. A list of necessary installations was given to aid the group in building the replicates. For the Vulnerability Detection step of the project, OpenVAS was utilized as the scanner as it offers services and tools that are relevant to Vulnerability Management. A total of 13 scans were made and executed. After the replicated devices were scanned, reports were generated by OpenVAS to show the detected vulnerabilities and their criticality to the network. For the Penetration testing and execution of real-world attacks on the simulated network, Metasploit, which may be found in Kali Linux, was used to perform actions that may be used by attackers. Kali Linux was also connected to the virtual network which allowed Metasploit to create sessions inside the target servers and the target firewall. The results of the previous phases was shown and presented to the client to inform them on what potential danger lies for the current company network. This was also done to consult the client in verification of the successful execution of the VAPT process in the simulated network The suggested remediation steps from the generated vulnerability scan reports was applied to the simulated network. A second Vulnerability scan was also done to the now remediated network to verify successful patching or mitigation of the discovered security issues.

5. IMPLEMENTATION AND RESULTS

5.1. Replication

The proponents built and made use of a simulated environment where all tasks, including Vulnerability Detection and Penetration Testing, was executed. This was decided because running these steps on the actual network of the company may harm or interrupt the business operations. A total of 12 servers and 1 firewall were built by installing their respective OS images in the hypervisors mentioned above.

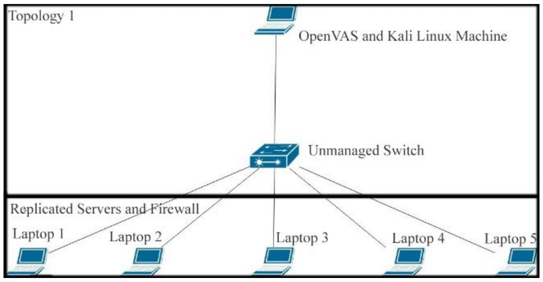


Figure 2. Replicated Network Topology 1 with Implementation of Testing Tools

Figure 2. shows the topology that will be applied in building the simulated network. The company's servers and firewall will be replicated into multiple devices. Each device may hold three to four replicated servers depending on the device's capability. Each device is also connected to an unmanaged switch and another device will have the vulnerability scanning and penetration testing tools installed.

Table 1: Machine Information for Replication

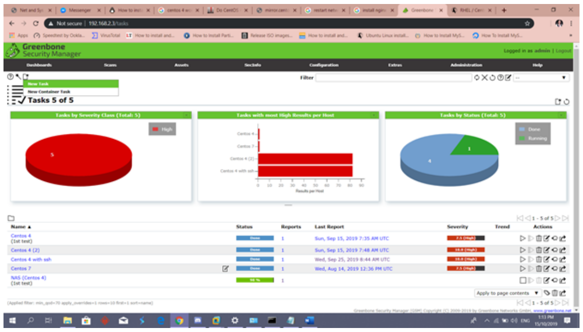
SERVER NAME	OPERATING SYSTEM	IP ADDRESS
Active Server	Windows Server 2008 R2	192.168.2.72
Bus Server	Windows Server 2008 R2	192.168.2.73
Fast and Trans Server	Windows Server 2008 R2	192.168.2.74
HM Server	Windows Server 2008 R2	192.168.2.75
MySQL Server	Windows Server 2008 R2	192.168.2.76
Passive Server	Windows Server 2008 R2	192.168.2.77
Web Server	Windows Server 2008 R2	192.168.2.78
ATTS 34 Server	Ubuntu 16.04	192.168.2.101

ATTS Dev Server	Ubuntu 16.04	192.168.2.102
Mark Linux Server	Ubuntu 16.04	192.168.2.103
Mark Mongo Server	Ubuntu 16.04	192.168.2.104
NAS Server	Centos 4.9	192.168.2.71
FortiGate Firewall	FortiGate	192.168.2.79

Table 1 lists the names of each server and the firewall, their respective operating systems, and the IP addresses that will be used for the simulated environment. These information were provided by the company to aid the researchers in replicating the machines.

5.2 Vulnerability Detection

The researchers' chosen vulnerability assessment tool is an application called OpenVAS. It is a scanner designed to run in a linux environment and is loaded with built-in tests and the Greenbone Feed



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Centos 4 (1st test)	Done	1	Sun, Sep 15, 2019 7:35 AM UTC	7.5 (High)		
Centos 4 (2)	Done	1	Sun, Sep 15, 2019 7:48 AM UTC	10.0 (High)		
Centos 4 with ssh	Done	1	Wed, Sep 25, 2019 8:44 AM UTC	10.0 (High)		
Centos 7	Done	1	Wed, Aug 14, 2019 12:36 PM UTC	7.5 (High)		
NAS (Centos 4) (1st test)	98 %	1				

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

Figure 3. OpenVAS Vulnerability Assessment Tool

Figure 3 shows the OpenVAS tool installed on one of the researchers' device. The proponents' made use of a readily available version of OpenVAS that uses the Greenbone Community Feed. It also includes a web interface that promotes easy and fast vulnerability scans. The table below summarizes the results of the Vulnerability Detection phase.

Table 2: Overview of OpenVAS Vulnerability Scan Results Count

SERVER NAME	HIGH	MEDIUM	LOW	LOGS
Active Server	82	115	7	40
Bus Server	37	36	3	20
Fast and Trans Server	82	113	7	38
HM Server	36	36	3	20
MySQL Server	80	115	7	40
Passive Server	37	36	3	20
Web Server	80	115	7	20
ATTS 34 Server	0	14	2	38
ATTS Dev Server	0	14	2	38
Mark Linux Server	2	16	2	41
Mark Mongo Server	0	14	2	38
NAS Server	68	45	2	24
FortiGate Firewall	0	8	2	22

As seen in Table 2, the Active Server, which is a Windows 2008 R2 server, garnered the most number of 'High' vulnerabilities. In contrast to this, no 'High' vulnerabilities were found for the firewall and it produced the lowest output overall.

5.3 Penetration Testing

Kali Linux was installed to be able to use Metasploit for attack penetration. The proponents were able to simulate some of the exploits that can make the servers of the company prone to hacking. Prior to all penetration scenarios done, the attackers have performed initial network reconnaissance thus having information on the targets' ip addresses and open ports.

To summarize the Attack and Penetration Testing Phase, all attacks were successful except for those done on the replicated firewall. For the Windows servers, the eternalblue vulnerability was exploited to gain access and execute malicious commands on the server. While for the Linux based servers, SSH Brute force attacks were executed and the established sessions were upgraded to meterpreter sessions to further exploit the systems.

5.4 Remediation

For the Remediation phase, the researchers applied the solutions and fixes suggested in the reports generated by OpenVAS, which were mostly updates for the obsolete and outdated software and packages installed on the machines. Some of the remediation also include steps to prevent the execution of the successful attacks done during the Penetration test such as installing Fail2Ban to prevent Brute force attacks through SSH. Additional policies for the firewall were also set in place to upgrade the firewall's security.

A Second Vulnerability Assessment was done on the now remediated machines to show if the applied remediation was effective. The table below shows the number of vulnerabilities found after remediation was applied.

Table 3: Overview of OpenVAS Post Remediation Vulnerability Scan Results Count

SERVER NAME	HIGH	MEDIUM	LOW	LOGS
Active Server	0	1	1	38
Bus Server	0	1	1	17
Fast and Trans Server	0	1	1	38
HM Server	0	1	1	17
MySQL Server	0	0	1	8
Passive Server	0	1	1	10
Web Server	0	1	1	10
ATTS 34 Server	0	0	0	45
ATTS Dev Server	0	0	0	43
Mark Linux Server	0	0	0	31
Mark Mongo Server	0	0	0	45
NAS Server	0	0	0	7
FortiGate Firewall	0	8	2	22

As shown in Table 3, the number of vulnerabilities detected after applying remediation were significantly decreased as compared to the results produced from the first vulnerability assessment performed.

5.5 Proposed Network Enhancement

Currently, the company uses unmanaged switches in their network. While unmanaged switches do play its function by allowing a user to immediately plug and play into the network, it offers very minimal control over your device. It has a fixed configuration that users cannot make changes to. This prompted the researchers to propose a change from unmanaged switches to managed ones. In terms of Security, managed switches increases protection and have other security benefits including the ability to monitor and control the LAN network in order to shut down active threats. For this project, the researchers used a Cisco Catalyst 2960-24TT-L Switch. The researchers configured basic settings to the switch, IP addressing and port security for added security.

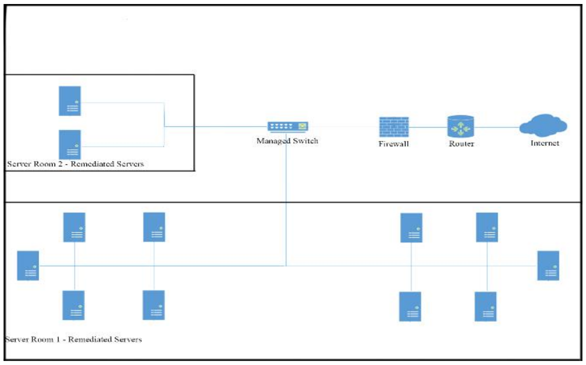

Server Room 2 - Remediated Servers
Managed Switch
Firewall
Router
Internet
Server Room 1 - Remediated Servers

Figure 4. Proposed Remediated Network Topology

Figure 4 shows the researchers proposal for the company to implement the suggested remediation fixes and solutions on the servers and firewall and to replace the unmanaged switch with a managed one, as previously stated. The researchers also propose to implement additional network policies configuration on the Fortigate Firewall to further improve the control of data over the network.

6. CONCLUSION AND RECOMMENDATIONS

6.1. Conclusion

The researchers were able to apply Vulnerability Assessment and Penetration Testing through this project. Due to some limitations as per discussed with the company administration, all servers and the firewall were replicated and all task was done in a simulated environment only. The researchers were able to perform the objectives of VAPT on the simulated network that was built. By performing the said tasks, the researchers were able to conclude that the Active Server is the most vulnerable server, garnering the highest number of vulnerabilities, In general, the Windows servers were found to be more vulnerable than the other servers with different Operating Systems. Both Vulnerability Detection and Penetrating Testing produced results for all servers, but were not able to produce results for the firewall only.

The researchers were also able to test the suggested remediation solutions and fixes gathered from the generated vulnerability scan reports. Through this, the number of vulnerabilities were significantly decreased as shown in the reports generated from the Post Remediation Vulnerability Assessment.

The objectives of the project were met, and a proposed enhancement was produced from the result of the VAPT processes. The researchers were able to introduce a Vulnerability Management process that the company may adapt and continue to perform to maintain a secured network for their organization.

6.2. Recommendations

These recommendations are based on the findings of the researchers during the making of the project.
Recommendations are as follow(s):

A. To the client
- It is highly recommended that the Vulnerability management process it to be adapted and performed on the network on a quarterly schedule.
- The process should be maintained and/or enhanced (if needed) to ensure a good security posture.
- The Remediation and Solutions presented in the document should be applied to the company's network to significantly decrease, if not totally eliminate the number of vulnerabilities that may compromise the security of the network.
- Along with the Vulnerability management process, software updates should also be done regularly to ensure that available vendor patches will be applied.
- Updating of the server Operating Systems should be performed.
- Unmanaged switches should be replaced with managed switches in order to increase control and protection over the network.
- Along with the replacement of unmanaged switches to managed ones, security configurations such as port security should be applied.

B. To the future researchers
- Other Vulnerability Assessment and Penetration Tools may be used in conjunction to those used in this project to produce a wider variety of results.
- If the company or client agrees to do so, it would be more advisable to request for an exact clone of the servers to further reduce discrepancies in the results of the vulnerability scanning.
- Other security configurations, if any, may be added to the proposed managed switch for a more secure and protected network.

REFERENCES

[1] Emmanuel Carabott (2012, November 29). *Three Tips for Effective Vulnerability Assessments*

[2] Jai Narayan Goel, BM Mehtre (2015). *Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology*

[3] Sherin S Panikar (2015, June 6). *Strengthening Information Security with VAPT*

[4] Robert Boyce. (2001, July 12). *Vulnerability Assessments: The Pro-active Steps to Secure Your Organization*

[5] Chan Wai. (2001, October 2001). *Conducting a Penetration Test on an Organization*

[6] Nishant Shrestha (2012) *Security Assessment via Penetration Testing: A Network and System Administrator's Approach*

[7] Aileen Bacudio, Xiaohong Yuan, Bei Tseng Bill Chu, Monique Jones (2011, November). *An Overview of Penetration Testing*

[8] Patrick Engebretson. (2013, August 1) *The Basics of hacking and penetration testing*

[9] Joel Kwesi Appiah (2014, July 21) *Network and Systems Security Assessment using penetration testing in a university environment: The case of Central University College*

[10] Johan Nilsson (2006) *Vulnerability Scanners*

[11] Ronald W. McCarty Jr. (2015, June 17) *Looking for Vulnerabilities with OpenVAS and Greenbone*

[12] Nikita Jhala (2014, May 13). *Network Scanning & Vulnerability Assessment with Report Generation*

[13] Raphaël Hertzog, Jim O'Gorman, Mati Aharoni (2017, June 5) *Kali Linux Revealed: Mastering the Penetration Testing Distribution*

[14] Pawan Kesharwani, Sudhanshu Shekhar Pandey, Vishal Dixit, Lokendra Kumar Tiwari (2018, December). *A Study on Penetration Testing Using Metasploit Framework*

Kit Arvin R. Cadiente is a 4th year Bachelor of Science in Information Technology student at the University of Santo Tomas.

Rafael A. Castro is a 4th year Bachelor of Science in Information Technology student at the University of Santo Tomas.

Kathrice Marie C. Mora is a 4th year Bachelor of Science in Information Technology student at the University of Santo Tomas.

Joan V. Ternio is a 4th year Bachelor of Science in Information Technology student at the University of Santo Tomas.

Elia Van A. Gica is an instructor at the University of Santo Tomas. He is also currently working at Netrust Philippines Corporation as a Technical Consultant.