VonLehman Security Auditing

by

Ram Saminathan

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Ram Saminathan — 4/26/2021

Ram Saminathan — Date

Toni Iacobelli — 4/26/2021

Tony Iacobelli — Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2021

Table of Contents

Table of Illustrations

ABSTRACT

VonLehman Security Auditing is a service that aims to raise cyber security awareness and help local business better understand how to secure their systems. Approximately 60% of small business close within six months of being hacked. Technology is growing at speeds that many companies are not able to correctly implement and secure. VonLehman Security Auditing will review a company using a five-step approach. Educating users and testing various aspects of a company's security is vital to securing their systems from malicious actors. The results of these tests will be compiled into a final risk assessment report which will recommend next steps and give the client a better understanding of their vulnerabilities.

PROBLEM STATEMENT

1.1 Problem

Cybercrime is the largest growing threat to all businesses and organizations. A cyber attack's impact can be catastrophic and the responsibility of cyber security falls on every single employee within an organization. Cybersecurity Ventures predicts by 2021, cybercrime will cost $6 trillion annually to enterprises across the globe. This will affect businesses of all sizes and in every sector. Comparatively, this is a steep growth from the $3 trillion global cost of cybercrime in 2015 and is indicative of a dire need for cyber security.

With the added stress of a global pandemic, organizations are now forced to embrace a future integrated with technology. The unstable economic conditions and an uncertain future dramatically increases the impact of a cyber-attack, which could cripple and end many businesses. Phishing campaigns, social engineering attacks and ransomware are becoming increasingly successful as many workers are now required to work from home. Now with technology ingrained within the core of every business, the security of networks is more important than ever. Rapid growth in technology creates spaces for vulnerabilities and failed security best practices. Many small to medium sized businesses in the Greater Cincinnati area lack the knowledge to secure their network and surrounding technologies. VonLehman Security Auding is dedicated to consulting these businesses in order to educate and facilitate the securing of their networks through training and assessments.

1.2 Solution

VonLehman will offer comprehensive security trainings and assessments to local businesses through a tiered packaged approach. VonLehman will include security training services with educational presentations on security topics and targeted phishing campaigns that

allow users to utilize their knowledge. Security awareness is a great foundation to creating a culture that is secure. The results of the phishing campaigns will be organized into a report allowing the leaders of the business to establish the most vulnerable departments and determine next steps. VonLehman's security assessments will search for physical and cyber security vulnerabilities. VonLehman will determine the value of data collected and stored, establish and prioritize technological assets, identify threats and vulnerabilities, evaluate access controls and document the results in a risk assessment report.

1.3 Project Goals

VonLehman Security Auditing will offer various services to clients. It will include educating employees, targeted phishing campaigns and assessing the physical and cyber security of a client. Once a client has been audited the results and analysis will be delivered in a Risk Assessment report.

- Cyber Security Presentation
    - A presentation that will educate end users on identifying and mitigating basic security threats. End users need to be aware and understand what resources are available.
- Cyber Security Assessment
    - Using various security tools, phishing campaigns and other security assessments will be performed.
- Physical Security Audit
    - An audit of physical security resources deployed by a client.
- Cyber Security Audit

  - An audit of technical processes related to security and ensure NIST guidelines are being followed.
- Risk Assessment Report
  - All findings in a Cyber Security Risk Assessment report

1.4 Overview

Throughout this final report, there will be information on how the project was completed. The report includes in-depth processes and includes the following sections: design objectives, methodology, budget, timeline, problems encountered, and future planning.

DISCUSSION

2.1 Project Concept

VonLehman Security Auditing will become the newest offered service from VonLehman CPA & Advisory. This service offers training, testing and an audit of policies and procedures. This project was conceptualized with VonLehman CPA's IT Director. Looking to learn and apply knowledge while increasing profit was a combined goal and Security Auditing was agreed upon.

2.2 Design Objectives

VonLehman Security Auditing aims to educate, train, test and review policies in a standardized auditing and training process. This will be done in 5 modular phases of an assessment.

2.3 Methodology/Technical Approach

Educational Presentation

The first service VonLehman Security Auditing offers is an education presentation. This presentation is 45 minutes long and includes 15 minutes for questions and answers. This presentation was created in Microsoft PowerPoint.

Cyber Security Assessment

The next service VonLehman Security Auditing offers is the cyber security assessment. The parameters for these campaigns will be set up beforehand. The parameters will include the number of attempts, strength of the emails/landing pages, and the targets within the company. These campaigns will be carried out using KnowBe4 phishing tools. Elements of vishing and a USB drive drop test are also incorporated into this phase of the assessment.

Physical Security Audit

VonLehman's physical security audit will be comprised of the top physical security recommendations in the industry including NIST guidelines. This will be a process that is conducted on-site, at the client's place of business.

Cyber Security Audit

VonLehman's cyber security audit will be comprised of the top physical security recommendations in the industry including NIST guidelines. This will be a process that is conducted on-site and from a remote location using Nessus Professional.

Risk Assessment Report

The Risk Assessment report will compile all the information gathered on a client and present it in one document. This will be done using a mix of Microsoft Office products and is presented as a pdf to the client.

2.4 User Profiles

Figure 1 represents the VonLehman Auditor. This will be the technician who is preforming tests on behalf of VonLehman.

User Profile Form 1
Application: KnowBe4, Kali Linux, Microsoft Office Suite
Potential Users: The IT Auditing team at VonLehman

Software and Interface Experience: Will need to be well versed with KnowBe4 and Kali Linux. This will be someone with IT who is knowledgeable on the Audit process.
Experience with Similar Applications: Penetration testing tools
Task Experience: In charge of updating methodology and conducting security audits.
Frequency of Use: Will be used as often as audits are scheduled. Will regularly be updating and testing methodology.
Key Interface Design Requirements that the Profile Suggests: The User will need to know how to use KnowBe4 tools and Kali Linux to conduct an audit. They will need to be able to present and educate end users for the client.

Figure 1: User Profile 1

Figure 2 represents Client Level 1. This will include IT administrators and the person in charge of communication with VonLehman.

User Profile Form 2
Application: Email and Phone Communication
Potential Users: Executives, business owners and higher-level IT administrators.
Software and Interface Experience: Users will need to have strong communications skills and facilitate meetings between auditors and IT.
Experience with Similar Applications: Outlook

Task Experience: Will help schedule and set up presentation. Will receive final Risk Assessment report.
Frequency of Use: Will only be part of initial presentation and final risk assessment.
Key Interface Design Requirements that the Profile Suggests: All communication and reports should be easily readable for technical and non-technical people.

Figure 2: User Profile 2

Figure 3 Represents Client Level 2. This will include the IT or Security technicians within the client.

User Profile Form 3
Application: Client network administration tools. Firewall and spam filter applications
Potential Users: IT or Security team for Client
Software and Interface Experience: Users should have in-depth knowledge of
Experience with Similar Applications: Must have experience with managing client network to allow audit process to complete smoothly.
Task Experience: Will be involved in phishing campaigns, physical security audit, cyber security audit and final risk assessment report.
Frequency of Use: Will only be required to participate during security audit.
Key Interface Design Requirements that the Profile Suggests: All communication and reports should be easily readable for technical and non-technical people.

Figure 3: User Profile 3

Figure 4 represents Client Level 4. This represent all of the target users who will be educated and tested within an audit.

User Profile Form 4
Application: Email
Potential Users: All users who will learn and be tested from the audit
Software and Interface Experience: Users should have experience interacting with and sending emails.
Experience with Similar Applications: Outlook, Gmail, Yahoo mail
Task Experience: Will be involved in the educational presentation and be tested during the phishing campaigns.
Frequency of Use: Will only be required to participate during security audit.
Key Interface Design Requirements that the Profile Suggests: All communication and reports should be easily readable for technical and non-technical people.

Figure 4: User Profile 4

2.5 Use Case Diagram

Figure 5 represents the use case for VonLehman Security Auditing. This diagram shows all possible users and their corresponding tasks.

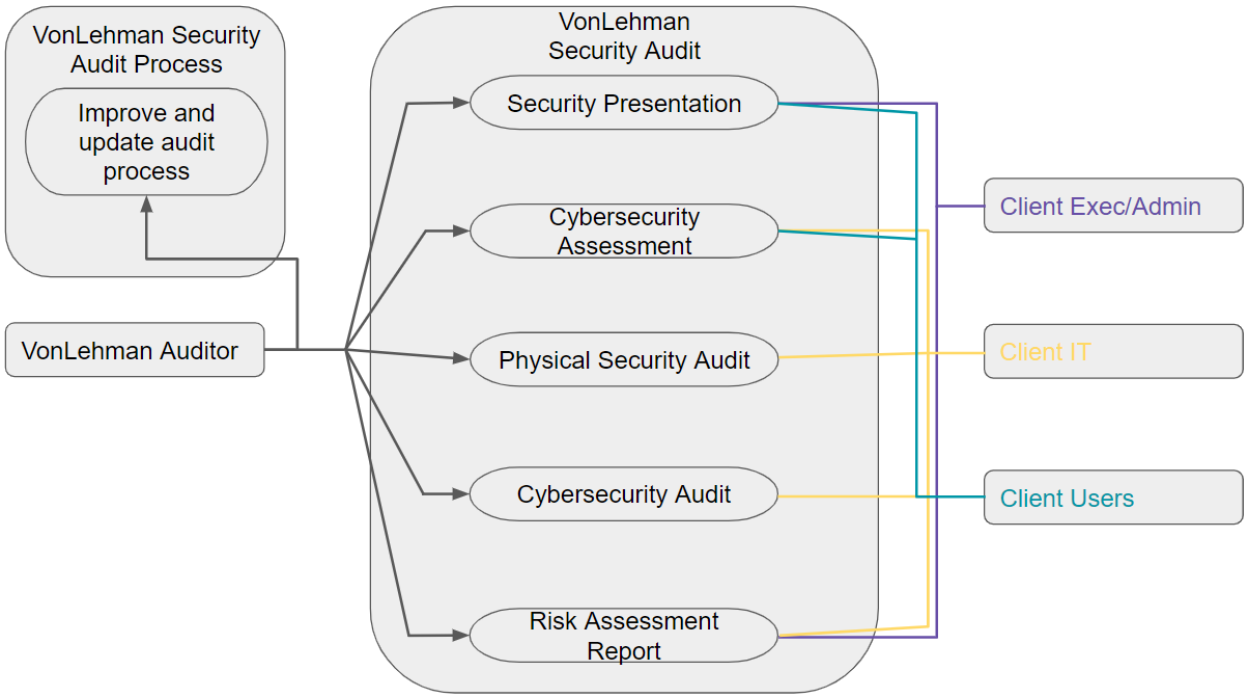

Figure 5: Use Case Diagram

2.6 Testing

All testing for VonLehman Security Auditing was done on VonLehman employees. An example of results are shown to adhere to VonLehman's confidentiality requirements. Names, email addresses, phone numbers and IP addresses were changed.

Name & Email	Scheduled	Delivered	Opened	Clicked	Replied	Attachment Opened	Data Entered
Michael Scott mscott@dm.com	1/1/2021 8:00 am	X	X	X			X
Jim Halpert jhalpert@dm.com	1/1/2021 8:00 am	X	X				
Dwight Schrute dschrute@dm.com	1/1/2021 8:00 am	X	X	X			
Pam Beesly pbeesly@dm.com	1/1/2021 8:00 am	X	X				
Andy Bernard abernard@dm.com	1/1/2021 8:00 am	X					
Stanley Hudson shudson@dm.com	1/1/2021 8:00 am	X	X				
Phyllis Vance pvance@dm.com	1/1/2021 8:00 am	X	X	X			X
Ryan Howard rhoward@dm.com	1/1/2021 8:00 am	X					
Angela Martin amartin@dm.com	1/1/2021 8:00 am	X	X	X			
Kevin Malone kmalone@dm.com	1/1/2021 8:00 am	X	X	X			X
Oscar Martinez omartinez@dm.com	1/1/2021 8:00 am	X	X				
Meredith Palmer mpalmer@dm.com	1/1/2021 8:00 am	X					
Creed Bratton cbratton@dm.com	1/1/2021 8:01 am	X					
Darryl Philbin dphilbin@dm.com	1/1/2021 8:01 am	X	X				
Toby Flenderson tflenderson@dm.com	1/1/2021 8:01 am	X	X				
Kelly Kapoor kkapoor@dm.com	1/1/2021 8:01 am	X	X	X			X

Figure 6: Phishing Campaign Results

A Phishing campaign was conducted, and the results are show. The campaign's focus was to trick employees to click on a reset password email link. The webpage that followed would then track if information were entered.

User	Scheduled Date	Phone Number	Call Duration	Call From	Call Status	Failed
Michael Scott mscott@dm.com	1/1/2021 8:00	513-123-0001	21 Seconds	513-789-9998	Completed	
Jim Halpert jhalpert@dm.com	1/1/2021 8:05	513-123-0002	21 Seconds	513-789-9998	Completed	
Dwight Schrute dschrute@dm.com	1/1/2021 8:10	513-123-0003	21 Seconds	513-789-9998	Completed	
Pam Beesly pbeesly@dm.com	1/1/2021 8:15	513-123-0004	21 Seconds	513-789-9998	Completed	
Andy Bernard abernard@dm.com	1/1/2021 8:20	513-123-0005	1:41 Minutes	513-789-9998	Completed	X
Stanley Hudson shudson@dm.com	1/1/2021 8:25	513-123-0006	21 Seconds	513-789-9998	Completed	
Phyllis Vance pvance@dm.com	1/1/2021 8:25	513-123-0007	21 Seconds	513-789-9998	Completed	
Ryan Howard rhoward@dm.com	1/1/2021 8:30	513-123-0008	21 Seconds	513-789-9998	Completed	
Angela Martin amartin@dm.com	1/1/2021 8:35	513-123-0009	21 Seconds	513-789-9998	Completed	
Kevin Malone kmalone@dm.com	1/1/2021 8:40	513-123-0010	21 Seconds	513-789-9998	Completed	
Oscar Martinez omartinez@dm.com	1/1/2021 8:45	513-123-0011	21 Seconds	513-789-9998	Completed	
Meredith Palmer mpalmer@dm.com	1/1/2021 8:50	513-123-0012	21 Seconds	513-789-9998	Completed	
Creed Bratton cbratton@dm.com	1/1/2021 8:55	513-123-0013	2:21 Minutes	513-789-9998	Completed	X
Darryl Philbin dphilbin@dm.com	1/1/2021 9:00	513-123-0014	21 Seconds	513-789-9998	Completed	
Toby Flenderson tflenderson@dm.com	1/1/2021 9:05	513-123-0015	21 Seconds	513-789-9998	Completed	
Kelly Kapoor kkapoor@dm.com	1/1/2021 9:10	513-123-0016	55 Seconds	513-789-9998	Completed	X

Figure 7: Vishing Campaign Results

A Vishing Campaign was conducted, and the results are shown. The focus of the campaign was to capture employee voicemail pin numbers.

Flash Drive 1: North Parking Lot							
File Type	Opened Date/Time	Macro Enabled Date/Time	IP Address	IP Location	Username	Display Name	Computer Name
.docx	1/1/2021 8:05am		192.168.1.1	Covington, KY	MGS	Michael Scott	PC-01
.pdf	1/1/2021 8:07am		192.168.1.1	Covington, KY	MGS	Michael Scott	PC-01
.xlsx	1/1/2021 8:10am		192.168.1.1	Covington, KY	MGS	Michael Scott	PC-01

Figure 8: USB Drive Drop Test

A USB Drive Drop test was conducted, and the results are shown. USB Flash Drives were strategically placed in and around the VonLehman office building. The flash drives contained malicious files that track and report if they are accessed.

Host 1: Web Server

IP Address: 192.168.56.101

7	5	21	5	74
Critical	High	Medium	Low	Info

Severity	CVSS	Plugin	Name
CRITICAL	10	51988	Bind Shell Backdoor Detection
CRITICAL	10	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10	11356	NFS Exported Share Information Disclosure
CRITICAL	10	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10	61708	VNC Server 'password' Password
CRITICAL	10	10203	rexecd Service Detection
HIGH	7.8	136808	ISC BIND Denial of Service
HIGH	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	7.5	34460	Unsupported Web Server Detection
HIGH	7.5	10205	rlogin Service Detection
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5	12085	Apache Tomcat Default Files
MEDIUM	5	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	5	42256	NFS Shares World Readable
MEDIUM	5	57608	SMB Signing not required
MEDIUM	5	15901	SSL Certificate Expiry
MEDIUM	5	45411	SSL Certificate with Wrong Hostname
MEDIUM	5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and

Figure 9: Nessus Scan Results

A Vulnerable Virtual Machine was set up and scanned. The results are shown. Each plugin code leads to a corresponding solution to the vulnerability.

2.7 Budget

Table 1 represents the budget of what has been spent to create VonLehman Security Auditing.

VonLehman Security Auditing Budget				
NO.	ITEM	UNIT, HOURS	UNIT PRICE	TOTAL
SOFTWARE				
1	KnowBe4	1	$3,707.88 (annually)	$3,707.88
2	Nessus Professional	1	$3,390.00 (annually)	$3,390.00
3	Subtotal			$7,097.88
4	**Total**			**$7,097.88**

Table 1: Budget

2.8 Project Timeline

Table 2 shows the project timeline for VonLehman Security Auditing. This timeline displays the fall and spring semester.

Task #	Task Name	Duration	Start Date	End Date
1.0	**Research**	61	9/1	11/30
1.1	End user training methods	10	9/1	9/10
1.2	Presentation methods	10	9/10	9/20
1.3	Phishing Campaign tools	20	9/5	9/25
1.4	Physical Assessment tools	20	9/10	9/30
1.5	USB drop tools	5	9/20	9/25
1.6	Kali Linux Research	31	10/1	10/31
1.7	Network Analysis Tools	31	10/1	10/31
1.8	Physical Security Standards	15	11/1	11/15
1.9	Risk Assessment Report Research	15	11/15	11/30
2.0	**Testing**	153	9/14	4/1
2.1	Phishing Campaign testing	36	9/14	10/31
2.2	Physical Assessment Testing	20	10/12	11/1
2.3	Network Analysis Testing	91	11/1	1/31
2.4	Physical Security Testing	15	2/1	2/15
2.5	Testing at VonLehman	91	1/1	4/1
3.0	**Deliverables/Senior Design Expo**			
3.1	Assignment 1	8	8/24	9/1
3.2	Assignment 2	42	9/1	10/12
3.3	Assignment 3	42	9/1	10/12
3.4	3-Minute Elevator Speech	7	10/12	10/19
3.5	Assignment 4	7	10/12	10/19
3.6	Assignment 5	7	10/12	10/19
3.7	Assignment 6	7	10/19	11/9
3.8	Assignment 7	21	11/9	11/30

3.9	Assignment 1	29	1/11	2/8
3.11	Assignment 2	6	2/9	2/15
3.12	Assignment 3	13	2/16	3/1
3.13	Assignment 4	13	3/2	3/15
3.14	Assignment 5	20	3/16	4/5
3.15	Assignment 6	20	3/16	4/5
3.16	Assignment 7	27	3/16	4/12
3.17	Assignment 8	27	3/16	4/12
3.18	Assignment 9	41	3/16	4/26

Table 2: Project Timeline

2.9 Problems Encountered

1. HTML5/CSS

   VonLehman Security Auditing's phishing campaigns include custom emails and landing pages. Landing pages and phishing emails can include HTML5 and CSS. This required training through practice of custom phishing campaigns preformed at VonLehman. This tested the boundaries of auditor's strengths with creating web pages and phishing emails.

2. Licensing

   Working with VonLehman required working with the companies internal accounting and shareholders for purchasing commercial licensing. This licensing allows for tools to be used externally but required meetings, budgeting and presenting in a professional environment. All licensing was abled to be solved after meeting with the internal accounting department and IT Director.

3. Configuring Nessus Scans

   Understanding the many Uses of Nessus required training and practice. Using a variety of vulnerable virtual machines, auditors were able to understand how to use the tool and

provide analysis on the results. This problem was partially solved. Auditors took time to become competent in using Nessus and continually worked to improve.

CONCLUSION

3.1 Lessons Learned

This project has led to becoming much more educated in the business side of IT. Budgeting, scheduling, meeting deadlines and working multiple roles within a real business is different than working on a normal class project. Time management also helped and getting work done with deadlines helped build a great relationship with VonLehman. The business world of IT is extremely important to anyone with a career in IT and will be extremely useful in the future.

3.2 Abilities Developed

Creating a Cyber Security Auditing service allowed for many soft and hard technical skills to develop. Methodologies using phishing, vishing and usb drop test tools were formed. Growth in understanding how to work and communicate with technical and non-technical people was necessary. Understanding and utilizing Nessus Professional required lots of trial and error. Developing professional relationships with future clients was very new. The cultivation of VonLehman Security Auditing led to the development of many technical and business skills.

3.3 Future Plans

Moving forward VonLehman looks forward to integrating security auditing to their comprehensive list of client services.

Back Matter

References

"60 Percent Of Small Companies Close Within 6 Months Of Being Hacked," *Cybercrime Magazine,* 16 Dec. 2019, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20predicts%20there%20will,Palo%20Alto%20Networks%20Research%20Center.

"Cybercrime Damages $6 Trillion by 2021," *Cybercrime Magazine,* 10 Dec. 2018, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20predicts%20there%20will,Palo%20Alto%20Networks%20Research%20Center.