Network Security Threats and Vulnerabilities

Manal Alshahrani , Haydar Teymourlouei
Department of Computer Science
Bowie State University,
Bowie, MD, USA

Abstract - *The transfer of confidential data over the Internet has become normality in the digital age with organizations and individuals using different digital platforms to share confidential information. This private information has become a target for hackers. With hackers targeting these networks, there has been a growing need to protect data, hardware, and software from vulnerabilities. A broad definition of network security can be constructed by defining its two components, security and networks. Two of the main focuses of this paper are to define network threats, such as phishing email, and to discuss some anti-phishing techniques. This research investigates various tools to identify different types of vulnerabilities and threats to the critical infrastructure and also identifies the network vulnerability and prevention methods for the network threats.*

Keywords: *network security, hackers, attack, vulnerabilities, threats*

1 Introduction

Security threats affecting networks are complex and pervasive in nature. To successfully protect a system from threats and vulnerability, it is essential to understand how security professionals assess and determine risks, the definitions of threats, exploitation, and vulnerability, and how security mechanisms are used. A threat may be demonstrated as intent to harm an asset or cause it to become unavailable. Identifying threats is an important but extremely complicated aspect of security management. Vulnerability, on the other hand, can be defined as flaws or weaknesses in system security procedures, design, implementation, or internal controls. Vulnerabilities can be accidentally triggered or intentionally exploited, resulting in security breaches. Security is a term used to describe different situations such as a situation without risk or sense of threat, prevention of risk, or a sense of confidence. A threat is an event that can take advantage of a vulnerability and cause a negative impact on the network. With the increase of universal electronic connectivity, threats such as eavesdropping, hackers, fraud, and viruses have grown exponentially. The fast growth of computer networks and systems has increased the need for individuals and organizations to store their information electronically or to use these systems for communication purposes. With more and more individuals and companies engaging in digital platforms, there has been a need to raise awareness about the importance of protecting data and resources, offering authentic messages and data, and protecting systems from network-based attacks.

Network security is not meant only for computers with significant data such as those used in businesses and offices [8]. Home users can also benefit from securing their networks. It is also important to note that not only broadband users or individuals with high-speed connection need to secure their networks. Another significant piece of information to have in mind is that the majority of computer systems, including corporate ones, have no immediate threat targeting their data; rather, compromised systems are used for practical purposes, for example, a launch of a DDOS attack in opposition to competing networks.

Furthermore, securing computer networks can be complicated. Historically, only qualified and experienced experts have been taxed with securing networks. However, as more people become concerned about potential security threats, there is need for more individuals who can understand the basics of the principles of network security and the network security world in general [9]. Different organizations and individuals are in need of appropriate security; therefore, the level of security varies from one organization to another. To be able to ensure better security for oneself and one's organization, it is crucial for network users to use the systematic approach, which includes analyzing, designing, implementing, and maintaining a desired network security system. The analysis phase requires a complete investigation of an entire network system, which is inclusive of both the hardware and software. This is an important phase because it helps to establish the level of vulnerability within the system and the requirements needed to ensure that the system is secure. Nowadays, all of the major browsers on Windows and Mac OS X are vulnerable to attack, so there is a significant increase in the use of HTML attachments to deliver malicious content. Typically, phishers will set up a fake login screen on a web page and then send spam emails with links to the site to as many people as possible in an attempt to trap them. For the attacker phishing, it is desirable to have a general method of spoofing any URL without relying on temporary exploit or clever domain registration. In this paper, we identify phishing attacks as a security problem resulting from utilization of Unicode on the Internet; demonstrate this potential and dangerous attack; and propose corresponding countermeasures to solve these kinds of problems.

. 2 Research Methodology

To achieve our goals, we will investigate following parameters. The comparative research of Linux versus Windows versus UNIX network security focuses on which operating system has the better security tools and is more secure. It also focuses on the different threats and

vulnerabilities that can affect each type of operating system, different types of security attacks, and available security countermeasure tools, techniques, and essential open source security tools. The results of these findings will be based on the simulation experiment.

2.1 Network Security Comparison

2.1.1 Linux operating system

With the increase in internet traffic, more and more transactions are taking place. These transactions are at risk since people with ill motives can target these transactions with the aim of damaging, stealing, intercepting, or altering data. Linux based systems are popular because they have robust and sophisticated security measures. Linux security tools can be broken into if they are poorly implemented into a system. Usually, attackers exploit existing problems within the system although the Linux community is quick at spotting these exploits and releasing immediate fixes.

The Linux server offers different kinds of facilities such as mail, WWW, and ftp which it handles via the system of ports. For example, port 21 controls ftp [2]. To be able to save on system resources and make the system administration less complex, many services configure file/etc/inetd.conf. This is the file that informs the system how to run each available service. Many Linux vendors turn on the different inetd.conf services by default; however, to ensure maximum security, they need to be off to prevent accidental damage.

Linux enables a user to choose which hosts to allow or deny. For instance, a user can allow logins from machines available at their own site, but not from the Internet. The files /etc/hosts.allow and /etc/hosts.deny list allowed hosts and services. The method of limiting or denying connections by checking the host provides a fundamental method for discouraging attacks although it is possible to fake host names on incoming connections. Data that is transferred over the Internet is also in danger because anyone with knowledge can gain access to the information using a method referred to as spoofing. Spoofing enables unauthorized individuals to inject fake data into a legitimate stream. The way Internet protocols interact enables such problems to occur. To tackle these difficulties, ssh was created.

Ssh is a stable, well-developed open source system that provides authentication and encryption on connections through the use of codes to protect data while it is in transit. The authentication process allows for the verification of a packet of data to ensure that the connection is valid. By using Linux, an individual is able to provide ssh level security for an individual's network use.

Linux has a comprehensive group of subsystems that enable a systems administrator to know what is going on with her or his system. All manner of log files are kept in the /var/log directory. Most of the basic services log information to /var/log/syslog and /var/log/messages about network users attempting to connect or successfully connecting to them.

Linux offers tools such as Ethereal which help to capture various types of packets over a period of time, revealing different types of information about packets. It is a critical tool used for monitoring the movement of packets and also for detecting traffic on a network segment. Tripwire is another intrusion and logging tool that takes a snapshot of important system files and records their signature within the database. After the initialization of the database, users can use Tripwire to monitor the integrity of the system. Another program is referred to as Snort, which offers information on the number of access attempts to which a machine has been subjected.

2.1.2 Windows Operating System

Windows is considered a secure operating system. It offers an improved and more secure computing experience, which is founded on user feedback from the Vista experience during which users requested for more intuitive and user-friendly security features.Windows was developed according to the Security Development Lifecycle (SDL) and it is built to be a secure computing environment. It contains key security features, including Data Execution Prevention (DEP), Kernel Patch Protection, Mandatory Integrity levels, and Address Space Layout Randomization which provide a strong foundation that guard against malicious attacks [4]. Windows has an enhanced User Account Control, primarily built to force software developers to engage in better programming practices; it is also perceived as a security feature that aids in enforcing least-privileged access and improves the total cost of ownership. The features allow organizations to deploy the operating system without granting administrator access to users. To improve security in a machine, experts recommend a two-factor authentication. Namely, this involves adding a second layer of protection on top of a password for improved security. Many computers, especially laptops, have built in biometric security systems in the form of a fingerprint scanner. Windows provides easier and more reliable support for integration between the fingerprint-scanning hardware and the operating system. Configuring and using a fingerprint reader with Windows for gaining access into the operating system and also for user authentication is more efficient and allows for up to ten finger scans.

Laptops can get stolen easily. If a user does not have effective security controls, unauthorized individuals can have access to sensitive information. Windows uses data protection technologies, including Active Directory Rights Management Services, Encrypting File System, and BitLocker that enable data encryption. From this information, it is evident that although the Windows operating system has better network security, Linux and UNIX have their own strengths, which can appeal to a user’s preference.

3 Network Vulnerabilities

In a network, the first vulnerable assets are people because the majority of employees at a standard organization are not

particularly cautious about network security, and often, they will cause a security breach. Regardless of whether it was unintentional or intentional, this type of threat is called an insider attack. A threat that goes hand in hand with human error is social engineering, which involves taking advantage of gullible employees and gaining sensitive information or physical access. Typically, a social engineer will pretend to be a legitimate business representative, such as a member of a maintenance or repair crew, and ask to gain access to a server room or other restricted area. Other methods include false telephone calls, and email attachments and links to infected websites. It is the job of IT professionals and security management to prevent these kinds of attacks by providing security training to the staff and properly restricting access.

Although firewalls and antivirus technologies remain significant in blocking many external attacks and removing malware, there are some key internal threats that increase network vulnerability. This category includes a range of portable devices that can bypass firewalls and other network perimeter measures. These devices include, but are not limited to, the following: USB thumb drives and miscellaneous USB devices; optical media; laptops and netbooks; and smart phones and other digital devices (Manky, 2010).

USB or other mass storage devices have the capability to transfer and store large amounts of data; this means that they can be used to hold stolen data and at the same time, they can be easily disguised and transported out of the company. In addition to being portable for data theft, these devices can carry computer viruses and other forms of malware that can infect an endpoint computer. They can hide in many types of devices. For example, in 2008, Best Buy found a virus in an electronic picture frame that was used to hold photos (Manky, 2010). The malware can then wreak havoc on the system or install a backdoor which creates a network vulnerability that allows unauthorized users to access the network. A technique to mitigate a USB device problem is to disallow auto-run of these devices when connecting to a USB port. Other solutions come in the form of security policies implemented by management such as banning removable media from the workplace.

Another network vulnerability related to removable devices is portable end points and wireless access points. The portable end points are laptops and similar devices that can connect wirelessly or wire to a network. Once inside, these devices can scan the network for more vulnerable devices that they can infect. It is important to safeguard open RJ-45 ports that malicious users can connect to by turning off unused ports and restricting physical access. Laptops can also carry home sensitive company information, so it is prudent to use an encrypted file system to protect the data. Wireless access points are known to be vulnerable because of weak protocols, namely wireless encryption protocol (WEP). It is recommended to use stronger encryption protocols such as WPA2 with strong passwords and scheduled password changes to prevent brute force attacks.

3.1 Tripwire's SecureCheq

Tripwire's SecureCheq is a free network vulnerability scanner that has a simple user interface and scans for advanced Windows settings to check for vulnerabilities. Although limited to Windows systems, it can perform local scans of both desktops and servers. The categories of settings that it checks for are OS hardening, data protection, communication security, user account security, and logs and auditing. After a scan is complete, the results of each test for the settings are displayed in a summary report. In addition to the summary report, it provides a test report that holds individual test results, suggest methods of mediation, and references additional vulnerability information. The downside is that the results cannot be saved, which means it cannot be processed by an external script. However, the results can be printed and the OVAL XML file can be exported and saved.

The test under OS hardening includes the following: Windows Remote Desktop configured to allow only system administrator access; Windows Remote Desktop configured to always prompt for password; and an enabled safe DDL search mode. For the Windows Remote Desktop settings, allowed users and password prompts can be configured in local or group policy. These settings are necessary so that regular users cannot gain remote access into a server; another layer of security is provided when the password is entered manually. Safe DDL search mode can be enabled in group policy as well. This setting is important because it points DDL queries to the more restricted Windows system DDL files first instead of local DDL files which can be corrupted.

Under the data protection category, the settings focus on preventing anonymous access to Windows shares and disabling default guest accounts. These settings can be configured in a group policy object under security settings. Restricting anonymous access on shares is important, but a related topic is setting proper access controls on shares for users that do have access. This prevents users from deleting other's work by restricting them to their own files or folders. Windows guest accounts and other default accounts should be disabled because of they are often the target of hackers who seek to use them as backdoors into systems.

In the communication security section, the settings focus on enabling stronger encryption and disabling weaker encryption standards. The settings are also configured in group policy. The first step is making sure encryption is required for Windows network passwords, which prevents sending passwords in plain text over the network. It is also recommended to disable LM authentication in favor of stronger NTLMv2 authentication. The other settings cover encryption over remote sessions which protect data from eavesdroppers.

The user account security category focuses on Windows password and account lockout policy. These settings are located within group policy. It is recommended that Windows password complexity is enabled along with a minimum password length of at least eight (8) characters. This helps prevent brute force or dictionary attacks that attempt to guess a password. The account lockout policy should be configured

to a duration of at 15 least minutes, and the counter reset should be at least 15 minutes as well. This helps deter or slow down an attacker trying to guess a password or login.

The last category that the free version of SecureCheq tests for is logs and auditing. The majority of these settings are configured in group policy, and specific details are configured in the auditpol command line tool. It is recommended that the system and security log files' maximum size be large enough to hold the events but small enough increase system performance. Some of the recommended auditing settings to enable include the following: logging of executed applications; logging of credential validation; logging of successful and failed login attempts for domain and local accounts; and logging of successful system changes.

3.2 Angry IP Scanner

Angry IP Scanner is a network scanner that is open-source and can work on any platform. It is able to function on a Linux system as well as a Windows system and Mac OS X. There are many different features in Angry IP scanner. These features are good to have when scanning a network. One feature is the ability to set an IP range, which is very convenient if certain IP addresses should be scanned. As a result, time will not be wasted scanning unnecessary hosts. With this method, the administrator can enter the IP address to start from and the IP address to end the scan. The IP addresses can also be randomized. If the administrator is unaware of what IP addressed to scan, Angry IP scanner will be able to choose for them. The actual process of scanning is very quick. After the scan, the amount of time the scan took to run is displayed as well as the IP range scanned, the amount of hosts scanned, and the amount of hosts that are alive. Another feature that is useful is the identification of the hosts that are alive or dead. If the IP address has a blue circle beside it, the host is considered alive. If there is a red circle beside it, the hosts are not alive, and there is a dead ping. You can also right-click on a specific host, and some options such as Show Details, Rescan IP, Delete IP, Copy IP, Copy Details, and Open are shown. You are also able to copy the details and paste them into a report or save the results in a Word document.

All of the options are self-explanatory in what they do, but the "Open" option has different choices when you click it. These options include Edit Openers, Windows Shares, Web Browser, FTP, Telnet, Ping, Trace Route, Geo Locate, and E-mail Sample. Angry IP gives these options under "Open" because the IP address can be opened in those particular ways. If the IP address is opened in "Windows Shares," it will show all the shares associated with that IP address. If opened in "Web Browser," it will open the web UI where settings can be changed, etc. If opened in "FTP," it will show the FTP. The user also has the option to "Edit Openers," which allows the addition or deletion of options to one's preference. Also, penetration tests can be conducted.

3.3 Browsers Vulnerabilities

3.3.1 Simulated browsers attack

This simulation presents an example of phishing attack 'phishing email' to offer comprehensive information on phishing. We used simple method "Email / Spam" based on our project requirement in an Information Security and Privacy course. The assignment required students to investigate network attacks and list the tools that exciting with this attack to familiarize students with different types of attacks. The purpose of this study was to help students gain a better understand of how this attack works and how they can avoid falling victim to phishing attacks. Additionally, the project was designed to give students insight into how extensive a problem phishing is in information technology. Ultimately, the study enables us to present some phishing protection tips to safeguard the network and identity.

3.3.2 How does phishing work?

Phishing is the attempt to gain sensitive information such as usernames, passwords, and credit card details, in order to carry out identity theft using fraudulent e-mail messages that appear to come from legitimate businesses. Phishing is typically carried out by email spoofing [5] or instant messaging [6], and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Once the user visits the website, any information entered on the webpage will be collected by the phisher and may be used fraudulently.

Type of phishing attacks:

In this section, we give a brief overview of the different types of phishing attacks to familiarize readers with the various threats.

1. Phishing-Link Manipulation:

   Most methods of phishing use some form of automated trickery considered to make a link in an e-mail emerge to belong to the spoofed organization. It could use misspelled URLs or subdomains, tricks commonly used by phishers. Another common trick is to make the anchor text for a link appear to be a valid URL when the link actually goes to the phishers' site.

2. Filter avoidance:

   Phishers have used images in place of text to make it harder for anti-phishing filters to sense text commonly used in phishing e-mails

3. Phone phishing:

   An example of phone phising is a message that appears to come from a bank that instructs users to dial a phone number to resolve time-sensitive problems with their bank accounts. Once the owner (victim) provides his or her personal information, including account number and PIN over IP service, the phisher (hunter) will capture it and use it to the detriment of the owner.

4. Website fake:

   Some phishing scams use JavaScript instructions in order to alter the address bar. Mainly, they direct

the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appear exactly like the trusted organization's. Phishers started to make a new technique to a void anti-phishing website that examine website for phishing they begun to use Flash-based websites to keep look much like the real website, but conceal the text in a multimedia object.

According to a study by Gartner, 57 million US Internet users have identified the receipt of e-mail linked to phishing scams, and about 2 million of them are estimated to have been tricked into giving away sensitive information [7].

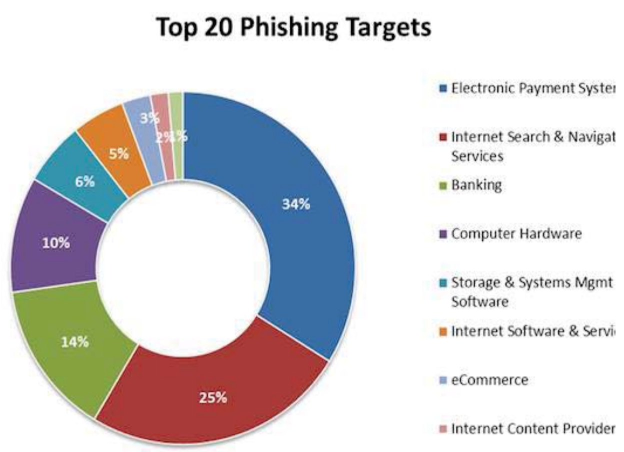

Figure1: Phishing Report In Various Activity.

3.3.3 Phishing Scenario

The approach used to simulate the problem was to create a phishing website and attempt to retrieve user's credentials. The testing environment comprised of creating an html file that contained a modified webpage with changed parameters, a php script that would record the victims' input and redirect them to the real login website once the login button is clicked, a log file that stored credentials in clear text, an email to send to the victim, and a php hosting website to host the malicious website. Once the victim receives the phishing email and clicks the malicious link, he or she will be directed to the phishing website. The layout of the phishing website will be an exact copy of the legitimate website, and, therefore, the victim would input their credentials. Upon clicking the login button, the php script would run, save the inputted credentials to the designated log file, and redirect the victim to the legitimate website. The log file is then examined and the victim's credentials are successfully retrieved.

3.3.4 Phishing web hosting

On a website where the users are supposed to enter/submit data (e.g., email, password), there is a piece of code in html called as action form.

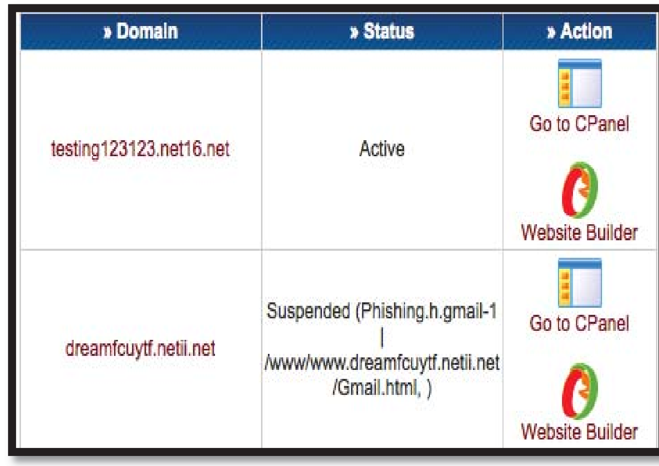

Figure 1: The Domain Website Builder

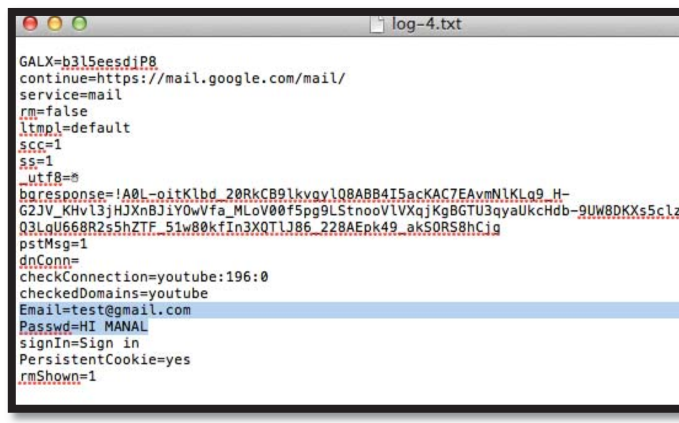

Figure 2: Log File Has the User Information

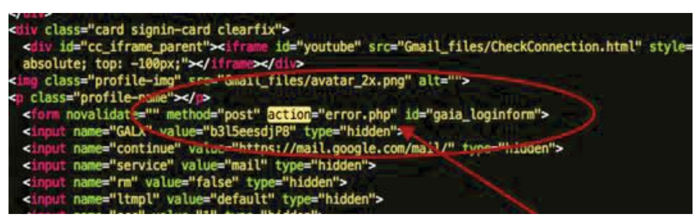

Figure 3: Place the Meta Tag to the Compromised Website

Figure 4: The Link To Fake Website

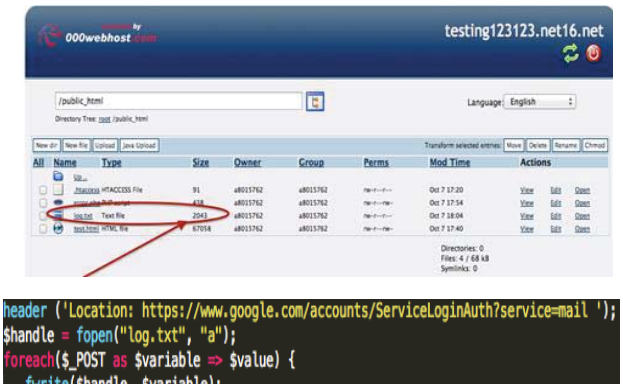

Figure 5: Code Capture Password

We captured how many times users success and log in spam phishing link where they are redirecting them, so we can have their information.

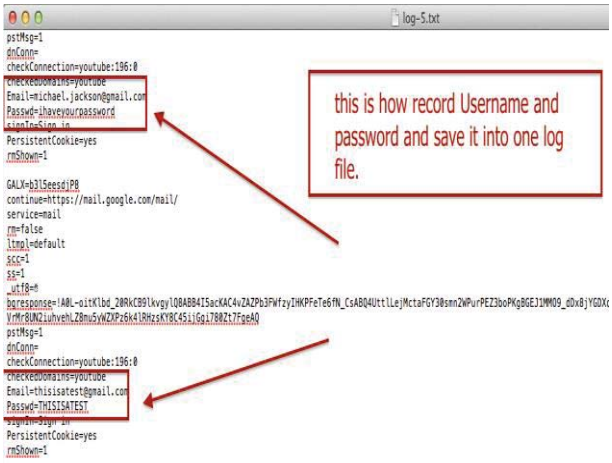

Figure 6: The Domain Website Shows the Number of Users Log In

Once the e-mail is opened by the user, the e-mail contents have to be sufficiently realistic to cause the recipient to follow the directions in the e-mail.

3.3.5 Phishing Prevention

Tips for phishing prevention incude the following: (1) Use dedicated systems for payment requests and approval processes. (2) Apply disabling email access on any system involved with payment processing. (3) Never trust alarm emails. (4) Be aware of attachments, and make sure not to open suspicious or strange emails, especially Word, Excel, PowerPoint, or PDF attachments, (5) Check the website you are visiting to ensure that it is secure; when you visit the page, examine the address bar; if the website you are visiting is on a secure server, it should start with "https://" ("s" for security) rather than the usual "http://"; most of phishing emails will direct the victim to pages where entries for financial or personal information are required. (6) Be wary of emails that request personal data, and never enter financial or personal information into kind of these pages. (7) Ensure that your software and firewalls that will enhance your defense against attackers are up-to-date; firewall protection prevents access to malicious files by blocking the attacks; antivirus software scans every file which comes through the Internet to your computer, which helps to prevent damage to your system.

4 Security Countermeasures Techniques and Tools

A security countermeasure is a device, procedure, technique or action that reduces a threat, attack, or vulnerability. Countermeasures against viruses includes having the latest software patches, service packs, and operating system; blocking irrelevant ports at the host or firewall; disabling unused services and protocols, and strengthening default configuration settings. To ensure your password is safe, users need to use strong passwords and audit login attempts to observe whether or not there have been hacking attempts.

4.1 Security Free Tools.

To be able to protect oneself from attackers and network vulnerability, there are free tools that can be used. These tools include, but are not limited to:

1. Wireshark: a multi-platform open-source network protocol analyzer that allows users to examine data from a live network or by capturing a file on a disk [10].
2. Metasploit: an elite open-source platform that enables users to build, test, and exploit code. This tool is perfect for exploitation research.
3. OpenVas: a tool that scans for vulnerability.

5 Recommendations

✓ For users to be able to protect themselves from phishing, it is important to have better email spam filters, two factor authentication, a site key, and an understanding of the factors that can enable and prevent phishing.

✓ The researchers would like to investigate potential methods of countering or stopping phishing attacks. Since the time window between the start and end of a phishing attack is likely to be limited to a matter of only hours or days and the source hosts are widely distributed, this is a difficult task.

✓ The researchers investigated how they can concentrate on collecting phishing emails received by end users. While this is a viable approach, capture occurs at the final stage in the incident lifecycle. An automated approach to capturing and responding to phishing attacks would be more desirable.

✓ If we hope to design web browsers, websites, and other tools to shield users from such attacks, we need to find a novel browser extension such as AntiPhish, that aims to protect users against spoofed website based phishing attacks.

6 Conclusion

From exploring network vulnerabilities and threats and by examining the different strengths of operating systems such as UNIX, Linux, and Windows with regards to security, it is evident that security is not a specific brand, product, firewall or operating system. Properly configured firewalls, antivirus updates, and passwords management strategies are good security practices; however, deficiencies in bad products can inhibit the results from these good practices. Therefore, it is essential for users to invest in software and hardware that are capable of withstanding common threats that might interfere, enable modification, fabrication, or facilitate interception of data. Our study suggests that a different approach is needed in the design of the security system rather than approaching the problem solely from a traditional cryptography-based security framework. In addition, most experts agree that anti-phishing education for end users needs to be implemented better. To resolve this matter, we recommend further study of development and innovative ways for combating anti-phishing attacks by finding better email spam filters, Two-Factor Authentication, or SiteKey.

8 References

[1] Ahmad, N., & Habib, M. K. (2010). Analysis of

Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution.

[2] Chen, X., Mu, B., & Chen, Z. (2011). NetSecu: A collaborative network security platform

for in-network security. In Communications and Mobile Computing (CMC), 2011 Third International Conference on (pp. 59-64). IEEE.

[3] Chung, C. J., Khatkar, P., Xing, T., Lee, J., & Huang, D. (2013). NICE: Network intrusion detection and countermeasure selection in virtual network systems. Dependable and Secure Computing, IEEE Transactions on, 10(4), 198-211.

[4] Cole, E. (2011). Network security bible (Vol. 768). John Wiley & Sons.

[5] "Landing another blow against email phishing (Google Online Security Blog)". Retrieved June 21, 2012.

[6] Tan, Koontorm Center. "Phishing and Spamming via IM (SPIM)". Retrieved December 5, 2006.

[7] McDaniel, Robert. "Cyveillance Weekly Phishing Report - September 21, 2015." Cyveillance Blog The Cyber Intelligence Blog RSS. Cyveillance Blog - The Cyber Intelligence Blog, 21 Sept. 2015. Web. 18 Mar. 2016.

[8] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[9]Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257

[10] Sanders, Chris (May 23, 2007). "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems". No Starch Press: 192. ISBN 1-59327-149-2.

[11]Ciampa, M. (2010, Jan. 29). Network Vulnerabilities and Attacks. Retrieved Sept. 20, 2015, from slideshare.net

[12] Manky, D. (2010, Nov. 8). Top 10 vulnerabilities inside the network. Retrieved Sept. 21, 2015, from networkworld.com

[13] *The Need for Vulnerability Assessment. (2013). Retrieved Sept. 20, 2015, from beyondtrust.com*