Vulnerability Assessment and Evaluation of Associated Attacks on Physical and Virtual Networks

Moses Ashawa
Federal Ministry of Communication Technology,
Annex III Shehu Shagari Way, Abuja, Nigeria
Ashawa.moses@gmail.com

Abstract— There is no system in the 21st century that has no vulnerability. Most networks seem to be very secure because the vulnerabilities in them are yet to be discovered. However, these vulnerabilities decrease in networks that undergo regular checks and upgrade in their directories with embedded security parameters which have cryptographic primitives. Lack of network checks has fashioned various attack vectors in which hackers exploit to break into the security of private, public and even virtual networks. Network attacks such as brute forcing, man-in-the-middle (MITM) attack, social engineering and Advanced Persistent Threats (APT) occur as a result of the combinations of several vulnerabilities which are embedded in them. The aim of this paper is to discover vulnerabilities such as weak passwords on networks and to demonstrate some common attacks that are frequently carried out on vulnerable networks which lack strong security primitives. Basic attacks demonstrated in this research were Man-in-the-middle attack, ARP poisoning, DHCP starvation attack and brute forcing. This research was conducted using network attack tools such as Nmap and Ethercap which are attack tools in Kali Linux. The result obtained from the research showed those vulnerabilities on networks ranges from poor embedment of security parameters on networks, opened network ports, weak and unsalted passwords and host of others. The research highlighted that, networks and security protocols should be designed with standard encryption levels and passwords with high entropy of different security strengths be used in accordance to the importance of the information being secured on a network. The research concluded that when strong cryptographic algorithms for key generation such as Diffie-Hellman and Blowfish algorithm for data encryption are rooted in the network either during configuration, the security of data over SSL and HTTPs of such a network can be greatly enhanced and vulnerabilities greatly reduced.

Index Terms— Attacks, Countermeasures, Network vulnerabilities, Security parameters, APT.

1 INTRODUCTION

For any organization to have an enduring system that could stand the test of the current attacks and threats which are been perpetrated on internet nowadays, such a society must have a continual and up-to-date of all the security primitives and auditory parameters [29] set in place. Security auditing is the bedrock for every risk assessment on any network; be it public, private or virtual [2]. The security of network is a fast moving and fashionable area. The fashionable ideas behind it are that networks can be secured by firewalls for blocking unwanted or suspected network traffic. But all these ideas in place does not provide everlasting solution to cyber-attacks such as password fishing [38], [5], [23], [11], [37] man-in-the-middle (MITM) attack [12], [4] social engineering [20], [6], [35], unpatched software, Advanced Persistent Threats (APT) [25], hijacking and distribution of malwares. Most of these attacks occur as a result of the combinations of several vulnerabilities [34] which are involved in these networks. Most networks are outside the control of network administrators, managers and the security parameters [18]. Examples of these vulnerabilities include weak usernames and passwords, Vulnerable CGI programs on Web servers, a stack overflow attack on the remote procedure call (RPC) mechanism, a bug in Microsoft's Internet Information Server (IIS) Web server software, a stack overflow attack on Sun's Solaris operating system, Weak authentication in the SNMP protocol [41].

The study of [2] asserted that for CRNs create additional new security threats such as common control channel (CCC) misbehaviour and attacks generated by LU emulation in its network sensing spectrum. These threats fashioned by CRNs resulted to a transactional degradation of the inclusive network performance and overall operation. The further affirmed that most of these attacks on networks are possible due to lack of basic MAC protocols for secured information exchange in most network designs. Absence or deficiency of sensing channels which helps in matched filter detection, features detection and energy detection which enables secured and effectual network availability are other serious security flaws posed by improper network configuration. Also, [34] and [36] in their research surveyed some of the security attacks performed on network. The study enlisted security attacks on both private and public networks such as Denial of Services (DoS) [3] and VoIP media attacks. The research concluded that, many organizations and individuals are more concerned with the network cost and functionality without any credence to its security and proper encryption and authentication at end nodes of network architectures. Many transactions presently operating inside the world of cyberspace are susceptible to various kinds of cyber-attacks and threats [1] caused as a result of system or network vulnerabilities which could either be in the form of software or hardware or both. The research of [9] asserted that both the hardware and software of these networks need to be

under continues and regular check with the aim of producing a more secured system for early detection of system vulnerabilities. Some of the attack vectors are because of poor network configuration settings, unprotected exposed network ports or wrong redirection of iptables [14] which an attacker may exploit to sniff some traffic and probably lunch attack for information extraction. According to [24], many networks are designed without security considerations in mind which makes network survivability very difficult to endure attacks that are latter launched on them.

Most times, when a cyber-attack occurs, the three major goals of information security which are confidentiality, integrity and availability [26] are violated. This calls for a necessity to place prominence to the security characteristics of those networks. Some of these threats and attacks occur as a result of lack of safeguarding of network infrastructure and the complexity that exist in the security auditing methodologies that cause a restriction in the professional visage of the entire security system of such an organization.

Knowledge of the research is crucial for the working security engineer. The basic knowledge contribution to this research is that the continuous use of network monitoring and auditing methodologies can help to put in place necessary control and security measures over the cyberspace, systems and repositories in order to counter both the existed and emerging threats. The counter measures on privacy and security principles will help security engineers, network analysts and forensics experts in providing a guideline and framework on how to secure and audit internet-based systems without exposing their vulnerabilities to be exploited by black hackers and to address the risks associated with network auditing. The obtained result will help penetration testers and ethical hackers to analyse company's security policy and procedures and report any vulnerabilities to management. The objective of the research is to demonstrate some common attacks such as DHCP starvation attack, Brute force attack, ARP Spoofing and Man in the middle (MITM) attack using different attack tools such as Yersinia [36], [7], Ettercap [16], [31] and WPscan which are in Kali Linux environment. These attacks are very common and are been witnessed on daily basis on poorly configured, unmonitored and unaudited networks.

2 Related Work

Numerous research of attacks on physical and virtual networks have been carried out intensively in recent times [44], [42], [32]. Also, [30] carried out a research on passwords and methods used in Brute-Force SSH attacks. Their research investigated overview of attack activities which are perpetrated on SSH based networks. The research concluded that attackers are using and sharing attack dictionaries of username/password for easy brute forcing.

Relatedly, [15] carried out analysis of man-in-the-middle attacks which occur in different communication networks and the various techniques of protection against them. His research pointed out that MITM attacks on network make the effort of securing data and privacy very challenging especially when data is on transit. This is because most of MITM attacks are mounted majorly from remote systems using counterfeit addresses. The research concluded by highlighting ARP Cache Poisoning, DNS Spoofing, Session Hijacking, Address Resolution Protocol (ARP) and SSL Hijacking [19] as some of the causes of MITM attack. the research concluded that the ARP protocol cache has no fool proof mechanism. As a result, it can be easily spoofed.

The research of [43] investigated on how DHCP protocols (Dynamic host configuration protocol is a network protocol that works in the data link layer for host configuration) can be secured in order to mitigate attacks which occur at the Local Area Network (LAN). The research affirmed that DHCP is vulnerable to many forms of attack such as DHCP rouge server attack, DHCP client attack and DHCP starvation attack [33]. The research applying two techniques key management authentication using Diffie-Helllman key exchange algorithm and message authentication for DHCP message authentication between the server and the clients using digital signature introduced a new scheme called Secure DHCP (S-DHCP) to sheltered DHCP protocol partially from these attacks. The research of [33] was similar to that of [21] and [22] respectively.

The study of [28] investigated some of the possible ways in which MITM attacks are remotely deployed on VoIP using active and passive observation fuzz testing techniques. The study illustrated the challenges and serious security threats posed by MITM on different network infrastructures and platforms. It however, did not demonstrate clearly where the attack occurred at the network interface. The research performed a study on how ARP poisoning and Man-in-the-Middle attacks can be prevented using a voting-based resolution mechanism [8]. The research result proofed that MITM attacks can be prevented from network nodes that the IP/IMAC [13] mapping systems are already known. Though study proofed to have no point of failure and complexity while realising regressive compatibility, it however did not use cryptographic primitives at the system's central server.

3 Materials and Methods

3.1 Instruments

This section describes the installation and configuration of VMWare virtual machines and virtual networks used to examine a number of "ethical hacking" techniques exercised in this research work. This research was conducted with reference to network attack and vulnerability assessment trategies [15]. To demonstrate vulnerability assessment and these attacks, two physical PCs were configured and connected through a single network called Lab Network 10.9.?.0/24. The first PC was running kali Linux to perform

vulnerability assessment and the attacks while the other was acting as a server and client on Centos 9. Hacking tools such as nmap, Yersinia and Ethercap were then deployed as hybrid network for fingerprinting, information gathering and attacks on the network.

3.2 Experimental design

The experimental and network setup for the designed systems was basically built using three different network topologies. These topologies were configured on three different machines namely, multiple physical machines, two physical msachines and single physical machine respectively.

i. Multiple physical machines

The first topology used separate physical machines to run a single virtual machine. This made the virtual machine simple to configure however, this topology made it impractical to run certain types of attack using Kali Linux attack tools like Yersinia.

ii. Two physical machines

The second topology was designed to emulate a real-world situation where an attacker, running Kali, would often be on a different subnet to the network and device being attacked, which would be protected by a firewall.

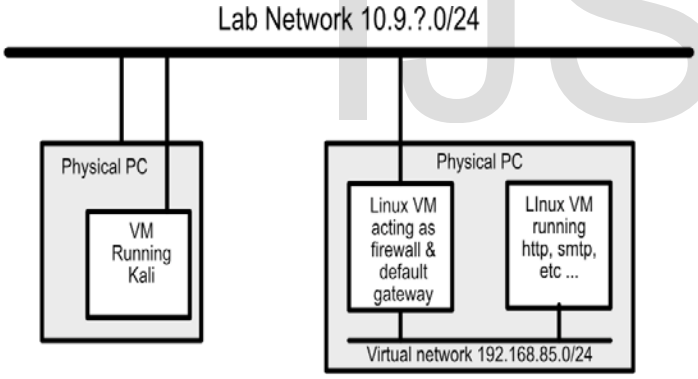

Figure 1: Topology with attacker on separate subnet

In this topology virtual machine (VM) running Kali was configured with a virtual network interface card (vNIC) that was bridged to the physical computer which was used as lab network. A second physical PC ran two Linux VMs connected via a VMWare virtual network with the machine acting as a firewall also having a bridged vNIC. This topology was created but it was quickly realised that many of the realisable attacks would require that the attacker was running on the same subnet as the devices being attacked (e.g. ARP poisoning).

iii. Single physical machine

The third topology placed all the virtual machines on the same VMware network.

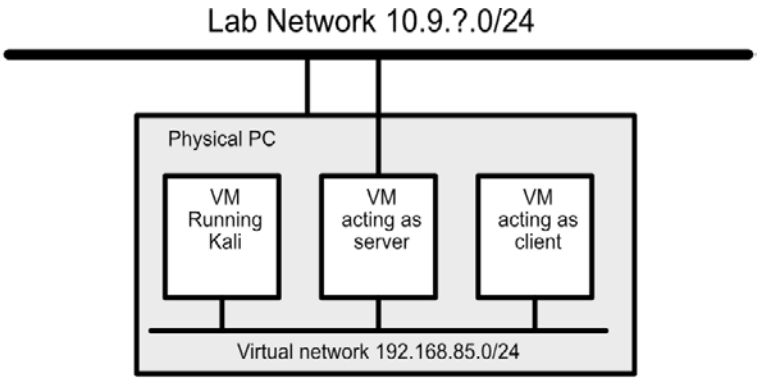

Figure 2: Topology 2 - All VMs on single physical host

Although this topology had the advantage of Kali being on the same (virtual) subnet as the other VMs however, the physical machine had only a single monitor which was impossible to view at the same time, Kali and the VM it was attacking or scanning. The rest of the system setup were on configurations and installations of different system services such as DHCP and DNS servers, dovecot and the web server as described briefly below.

3.3 Services installations and Configurations

Installations and configurations of different services were performed on the network as illustrated below:

A. Server Configuration

One of the virtual machines (the "server") was configured to provide the SMTP with IMAP4 server managing emails from client computer. For user and client application, SMTP is commonly used for sending messages to mail server, while client application use pop3 or imap3/imap4 for receiving mails. However, for the cause of this research IMAP4 was used to manage Mail in Client machine. During configuration, the command **Yum –y install postfix** was used to install postfix packages while **/etc/postfix/main.cf** was used to edit postfix configuration files. After all the vicissitudes were made, the command **systemctl start postfix** and **systemctl enable postfix** were used to start and enable postfix services respectively. The command **yum - y install dovecot** was used to install dovecot packages while **/etc/dovecot/dovecot.conf** was used to edit configuration files, protocols line in the configuration file is uncommented to IMAP4. A virtual network (VMnet10) was created to link the multiple virtual machines running on the physical PC to the second virtual NIC as shown below.

The VMware tools were installed in Centos to enable the physical machine share folders with the virtual machine. This necessitated the installation of a number of additional packages, including the "gcc" compiler and the kernel-devel package which includes the kernel header files. Once the VMWare tools were compiled and installed, shared folders

were automatically mounted in the /mnt/hgfs/ folder. This was used to export screen shots and configuration files from the Linux VMs to the physical PC. The interface connected to the VMNet10 virtual interface was configured with the manually allocated 192.168.85.1/24 IP address as this interface will be used to run the DHCP and DNS servers.

B DHCP, DNS and Web servers' configuration

With Centos the DHCP client is installed by default but the DHCP server has to be installed using # yum install dhcp. Before starting the newly installed DHCP server a suitable configuration was created in the /etc/dhcp/dhcpd.conf file (using /usr/share/doc/dhcp*/dhcpd.conf.example as an example). The DHCP server was configured to dynamically update the DNS service which is running on the same machine. The DHCP and DNS servers had a shared private key (HMAC-MD5) for message authentication. The private key was created using the dnssec-keygen utility: **dnssec-keygen -r /dev/random -a HMAC-MD5 -b 128 -n USER DHCP_UPDATER**. The DHCP client and the DNS server were configured using the file **/etc/resolv.conf** to ignore the details obtained from the DHCP server (on the physical LAN). Centos and other Linux distributions use the Bind DNS server which was installed using the yum package manager. The bind-utils package, which provides a number of utilities including dig, was also installed. Zone files such as forward, recursive and reverse zone files were created appropriately. The requirement was to add a web server to the host machine. Instead of simply installing the apache web server it was decided to install the WordPress content management system on top of Apache as this would give a better target for attack. other packages installed besides WordPress were apache, mariadb-server and php. The DHCP client-server set was moulded as shown below:

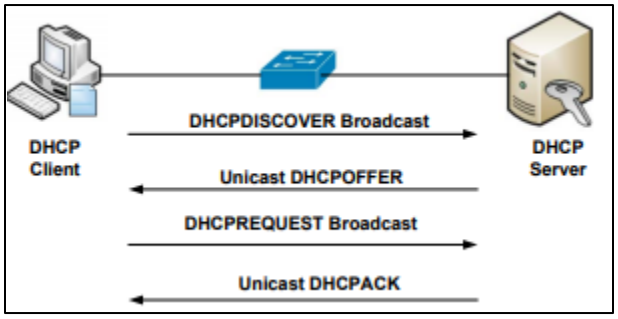

Figure 3: DHCP configuration [43]

After the configuration, Dovecot IMAp server was installed and configured to work with postfix. The clear text form uses TCP port 143, the secure form uses SSL/TLS over TCP port 465. The Centos firewall can be configured either by editing the iptables configuration files directly. One problem encountered was that both interfaces were being added back to the (default) internal zone on rebooting the system. This was resolved by adding zone=internal and zone=public lines to the ifcfg-* files in **/etc/sysconfig/network-scripts** using the following rules:

firewall-cmd --zone=public --remove-interface=eno3354984 --permanent
firewall-cmd --zone=internal --add-interface=eno3354984 --permanent

4. 0 Results presentation

The results described were based on the successful attacks that were performed on this network.

4.1 DHCP Starvation Attack

The DHCP attack flooded the DHCP set up server with discover packets with spoofed MAC addresses. With this attack, diverse IP addresses were given by DHCP server every time a request was made therefore filling up the pool of the DHCP. This attack made it impossible for client to receive the IP address when requested for. To perform this attack, a kali Linux was used to attack the setup DHCP server and a centos machine having IP address of 192.168.85.1/24 on the physical machine network of 10.9.0.0/24. Finger printing service was the first step carried out while trying to gather information about the network setup of the server using a kali Linux tool called nmap as shown in the screenshot below.

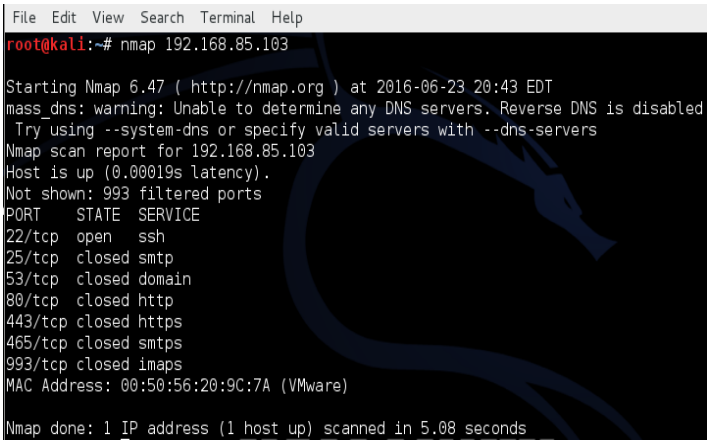

Figure 4: Scanning network with nmap

It was found that some ports like tcp performing ssh services was opened which gave a clue that it is likely to perform Apache related attacks. This revealed that the dhcp server is running an Apache httpd 2.4.6 on the centos using PHP version 5.4.16 on the WordPress version 4.5.2. This further gave a hint to look for lope holes (vulnerabilities) that can be exploited in WordPress. Yersinia command **Yersinia -G** which generated the Yersinia-gTK mode and the network interface to deploy and perform the dhcp attack. The sub-attack

correspondence was selected to send discover packets.

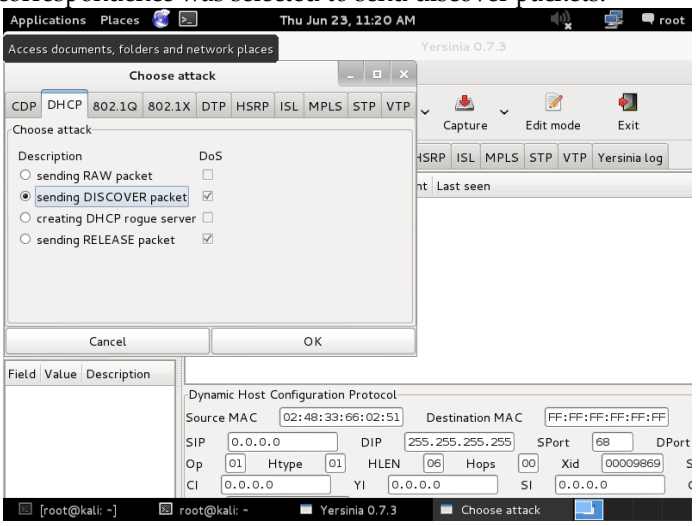

Figure 5: Sending DHCP DISCOVER packets

The attack was successful and millions of DHCP packets where sent to flood the DHCP pool.

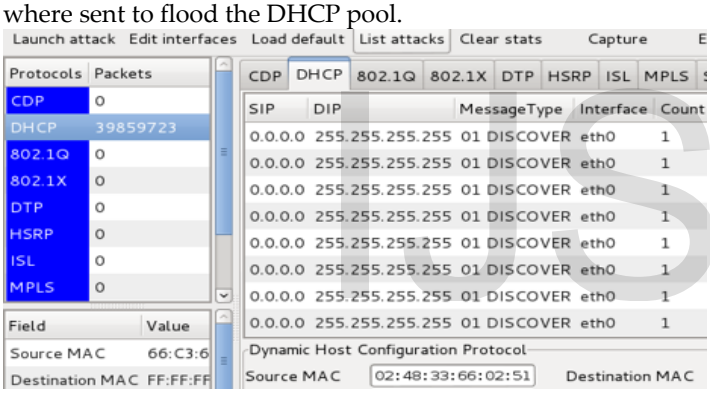

Figure 6: DHCP sending millions of DISCOVER packets

After waiting for 10 minutes, a window client was tried to connect on the centos machine which is on the same network with the attacker (eth0 interface). It then shows that the legitimised client was denied from getting IP address as shown below.

Figure 7: No free leases in the server

The DHCP starvation attack successfully exhausted all the IP addresses of the server. The logs above demonstrated that the dhcp server has leases all the addresses. Comparing snapshots taken before and after the attack was lunched shows that dhcp protocol had zero (0) packet lease with no SIP and DIP in its interface counter mode before attack. However, DHCP rogue packets of 35359723 flooded the pool with a DIP of 255.255.255.255 after the attack as shown below.

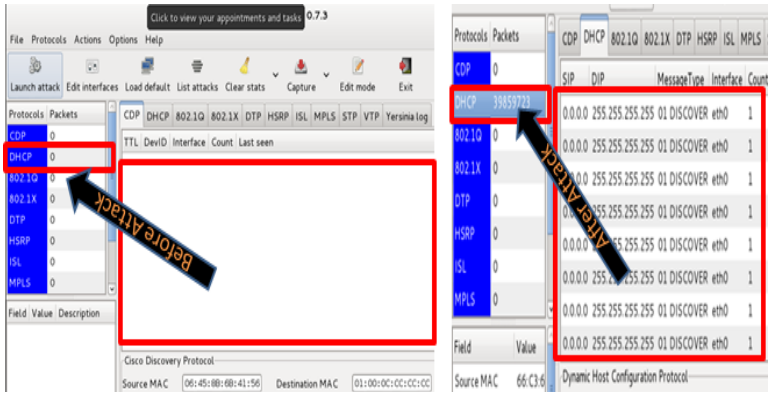

Figure 8: Comparison of before and after DHCP starvation attack.

The DHCP starvation attack successfully exhausted all the IP addresses of the server. This demonstrated that the network has a good number of vulnerabilities that requires patching through auditing. The attack succeeded because various details of the system details such as the program version, Daemon mode, debug and other network ports such as TCP were exposed which were used as attack vectors. This attack can be mitigated by enabling sport securities of the server. This can be done by designating ports that forward traffic towards the DHCP server as trusted and designating all other ports including those with statically addressed hosts as untrusted. In addition, DHCP security such as DHCP snooping can also be enabled as a countermeasure to drop unwanted generated DHCP traffics (Younes, 2016). With the DHCP snooping, rogue DHCP servers will be prevented from offering or giving IP addresses to the clients of the DHCP. DHCP snooping will enable the switch to build a table that maps a client MAC address, IP address and port identity. This security layer can be implemented at security layer 2. Based on the attack vectors identified, the following countermeasures could be applied to mitigate DHCP starvation attack which are Specifying trusted client with their MAC address, authentication of client, limiting number of MAC address per port, detecting DHCP request message rate and detecting validity of client using ICMP echo service.

4.2 Brute Force Attack

WPscan is one of the tools for cracking password of computer system and having access to vital information like user name, password and other vulnerabilities. With few commands, the website vulnerabilities services such as plugins and usernames created and added in the server were exposed. Arguments and enumerator command were added to get more details of the network system.

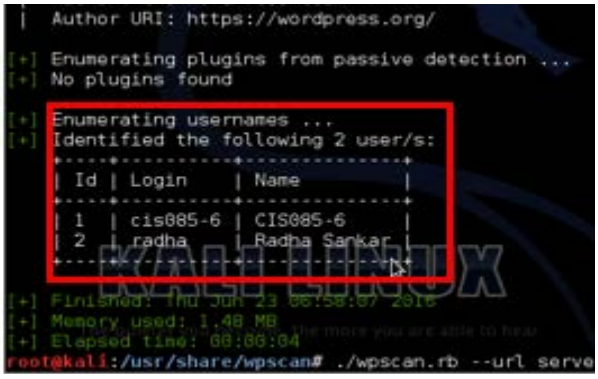

Figure 9: Brute forced login and usernames

The command line rubywpscan.rb –url http://yourewebsite.com –wordlist passwords.txt threads 50. enumerated vital information from the target system such as user password and username and were brute forced.

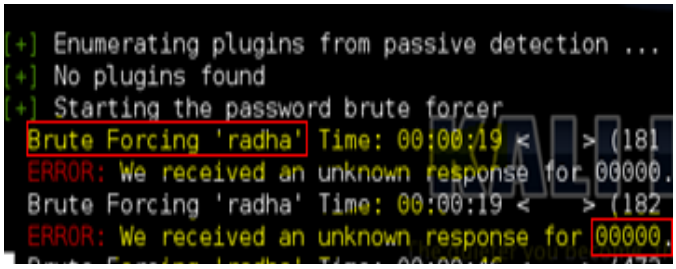

Figure 10: Brute forced password

From the screenshot above, it is seen that username **radha** was brute forced and the password **0000** was recovered as created by the network administrator. It only took the attacker 19 seconds to brute force '0000' password created.

Having collected and examined a huge amount of information on brute force attack on the SSH of the network, an evaluation of a variety of mitigation techniques that can be applied for protecting ssh servers is proffered in light of the insights gained from this research. The study also suggested other defensive strategies. The result showed that both the username **radha** and the password **0000** were weakly created without salting, thus making password brute forcing. To mitigate this attack, the password used should be created using random selection of number and the selected password should have a high entropy of key size. Instead of using just password for security, the created password should be hashed using cryptographic algorithms and primitives such as RIPEMD-60 for better security [25]. From the result obtained, it is observed that majority of the people used weak passwords which makes it easy for brute forcing. This research recommends that users should make it passwords lengthy, combine letters, numbers, and symbols, use words and phrases that are easy for you to remember, but difficult for others to guess to form a strong password. Apart from choosing a strong password, the study provided a broad consensus for securing networks running ssh servers as follows:

A. Disabling logins via SSH for the root account. This is a good security practise because it causes attackers to face the challenge of obtaining valid user details and network ip address [30]. The root account is an obvious target, since it is known to exist on all Unix/Linux systems. When root logins through SSH are deactivated, login efforts nose-dive silently. Therefore, the hacker does not know whether these attempts have any tendency of succeeding and renders useless a large percentage of malicious traffic on the network; but when this is not done, the attacker easily can compromise the non-privileged account and gains a foothold on the system and exploits.

A. Running the SSH server on a non-standard high port.

SSH servers listen on port 22 of the TCP traditionally. When ssh is configured to listen on alternative ports among the unused 65,535 ports provided by the TCP protocol, it hides ssh services from the attacker. The research noted that running a well-secured ssh server on a nonstandard and unusual port helps in reducing its vulnerability to brute-force attacks without exposing the server to additional risk.

B. Using TCP Wrappers to block IP addresses with repeated failed login attempts.

Networks and systems can be secured from brute force attack by locking out attacking IP addresses using iptables, TCP Wrappers, or null routing rules.

C. Replacing passwords with public-key authentication

To offer defence against brute force password attacks, the server's administrators must disable password-based SSH authentication and then generates a public/private key pair and place the public key in the appropriate file on the destination server for users [27]. The private key, in turn, must be stored on each client system from which the user wishes to log in to the server. In summary, the research found that a

number of the suggested procedures (techniques) for protecting against brute-force attacks can be relatively effectual, especially when used in combination.

4.4 Man in the Middle attack

The man-in-the-middle (MITM) attack is a type of eavesdropping. Communication between two users is monitored and modified by an unauthorized party on the same network. The attacker actively eavesdropped by intercepting a public key message exchange and retransmitting the message while replacing the requested key with his own while the original parties appeared to be communicating normally. The target host was sniffed from remote connection via the network. Using Wireshark, the network traffic carrying the login details of the message of the legitimate user of the system (stevej) was captured by the hacker as shown in the red highlight.

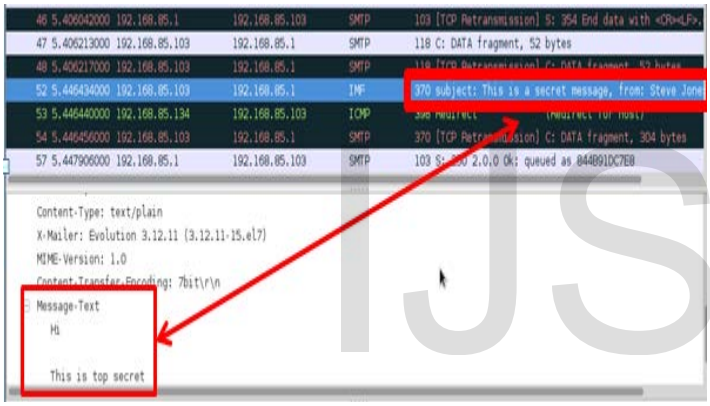

Figure 11: Message captured and decrypted by the hacker in plain text

The MITM attacker controls the entire communication by intercepting communications between two systems by the attacker by taking control of a router along normal point of traffic. An MITM attack takes advantage of the weakness in network communication protocol. The session cookie reading the HTTP header was easily captured and decrypted by the intruder (black hacker). The message sent on transit was captured and viewed by the third party (the middle man) in plaintext "**Hi this is top secret**".

The man-in-the-middle (MITM) attack is a type of eavesdropping. Communication between two users is monitored and modified by an unauthorized party. The attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with their own. In the process, the two original parties appear to communicate normally. The message sender does not realise or recognize that the receiver is actually an unknown attacker trying to access or modify the message before retransmitting it to the receiver. Thus, the MITM attacker controls the entire communication by intercepting communications between two systems by the attacker by taking control of a router along normal point of traffic. In almost all cases, the attacker is located on the same broadcast domain as the victim. In an HTTP transaction, a TCP connection exists between client and server. The attacker splits the TCP connection into two connections – one between the victim and the attacker and the other between attacker and the server. When the TCP connection is intercepted, the attacker acts as a proxy by reading, altering and inserting data in the intercepted communication. The session cookie reading the HTTP header can easily be captured by the intruder. In an HTTPS connection, two independent SSL connections are established over each TCP connection. An MITM attack takes advantage of the weakness in network communication protocol [4].

5. Discussion

The research demonstrated that using a wireless medium instead of a wire to transmit information, it faces diverse susceptibilities to attack. this most times result in the disposal of the communication progression between end users [39]. These vulnerabilities lead to varied specific and common security threats in both conventional wireless and CR networks users. The transmitted information can be sensitive, such as the user's identity, the user's privacy, allocation and signalling information, as well as key information like passwords and usernames. However, attackers deploy different techniques such as eavesdropping, ARP poisoning, brute force, masquerading and others to intercept communication during the transmission process when a network is weakly configured and there are no network auditory security parameters and processes in checking constantly the network vulnerabilities.

Conclusion

Data protection is one of the most pertinent concerned issues in information security which most times is enabled via network auditing and vulnerability assessment. To enhance different security measurements for protection, detection, and countermeasures networks security protocols such as DHCP, WEP, WPA, and WPA2 can be deployed during network setup and auditing. These networks and security protocols should be designed with standard encryption levels and passwords with high entropy of different security strengths being used according to the importance of the information being secured. The research identified and highlighted some of the ways in which attacks such as man-in-the-middle attack can be conducted on a network some of which are: listening to

transmitted communications by an attacker over the network, processing, requesting and responding to the to the malicious website server, intercepting and injecting payloads by hackers, login into the website and interacting as a valid website user can by an attacker. In summary, this research recognised that online data protection will continue to be a battle and not an easy job most especially now that hackers are constantly formulating new strategies and techniques to exploit, break into networks and steal data on less secure networks. However, the research discovered that when strong cryptographic algorithms for key generation such as Diffie-Hellman and Blowfish algorithm for data encryption are rooted in the network either during configuration or auditing, the security of data over SSL and HTTPs of such a network can be greatly enhance thus, mitigating attacks like MITM, DHCP starvation, DoS and other related attacks.

REFERENCES

[1] S. Alhabash, M. Jiang, Brooks, and S.R. Cotten, "Online Banking for the Ages". Generational Differences in Institutional and System Trust. In *Communication and Information Technologies Annual conference*, pp. 145-171, 2015.

[2] W. Alhakami, "Secure MAC Protocols for Cognitive Radio Networks". IEEE Communications Magazine, vol. 76, no.4, pp. 36-47, April, 2016.

[3] M. Ambrosin, and M. Conti, "Efficiently managing switch flow in software-defined networking while effectively tackling dos attacks. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pp. 639-644, 2015. (ACM proceeding).

[4] N. Athavale, S. Deshpande, and V. Chaudhary, "Framework for Threat Analysis and Attack Modelling of Network Security Protocols", *International Journal of Synthetic Emotions (IJSE)*, vol. *8, no.* 2, pp.62-75, 2017.

[5] R. Belani, and A. Higbee, "Performance *benchmarking for simulated phishing attacks"*, U.S. Patent 9,246,936.

[6] A. Beutel, W. Xu, and C. Faloutsos, "Stopping group attacks by spotting lockstep behavior in social networks", In 2013 ACM *Proceedings of the 22nd international conference on World Wide Web* (pp. 119-130).

[7] Y. Bhaiji, "Understanding, preventing, and defending against layer 2 attacks", In *Cisco, http://www. nanog. org/meetings/nanog42/presentations/Bhaiji_Layer_2_Attacks*,2007.

[8] R.K. Bijral, A. Gupta, and L.S. Sharma, "Study of Vulnerabilities of ARP Spoofing and its detection using SNORT", *International Journal of Computer Security*, vol. *8, no.*5, 2017.

[9] D. D. Coleman, D. A. Westcott, and B. E. Harkins, "Wireless LAN Security Auditing. Certified Wireless Security Professional Study Guide CWSP-205", Certified Wireless Security Professional Study Guide CWSP-205, 439-468, 2017.

[10] E. Crowley, "Information system security curricula development", In ACM 2003 Proceedings of the 4th conference on Information technology curriculum (pp. 249-255).

[11] J.A. Chaudhry, S.A. Chaudhry, and R.G. Rittenhouse, "Phishing attacks and defences", *International Journal of Security and Its Applications*, vol. *10, no.*1, pp.247-256, 2016.

[12] M., Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks", *IEEE Communications Surveys & Tutorials*, vol. *18, no.* 3, pp.2027-2051, 2016.

[13] T.G. Curran, "*Tools for investigating cellular signaling networks by mass spectrometry,* (Doctoral dissertation, Massachusetts Institute of Technology), 2014.

[14] C. Diekmann, J. Michaelis, M. Haslbeck, and G. Carle, "Verified iptables firewall analysis", In 2016 IEEE Networking Conference (IFIP Networking) and Workshops, (pp. 252-260).

[15] S. Gangan, "A review of man-in-the-middle attacks", arXiv preprint arXiv:1504.02115. 2015

[16] W.A.H. Ghanem, and B. Belaton, "Improving accuracy of applications fingerprinting on local networks using NMAP-AMAP-ETTERCAP as a hybrid framework", In *Control System, Computing and Engineering (ICCSCE), 2013 IEEE International Conference on* (pp. 403-407).

[17] S. Jyoti, S. Bhavana, "A Survey on VoIP Security Attacks and their Proposed Solutions", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 2, no. 3, 2013.

[18] P. Klein and A. Kliger, "U.S. Patent No. 9,369,448. Washington, DC: U.S. Patent and Trademark Office, 2016.

[19] S. Khurana, "A Security Approach to Prevent ARP Poisoning and Defensive tools", International Journal of Computer and Communication System Engineering, vol. 2, no.3, pp. 431-437. , 2015.

[20] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks", *Journal of Information Security and applications*, vol. *22*, no. 2, pp.113-122, 2015.

[21] S. Kumar, and S. Tapaswi, "A centralized detection and prevention technique against ARP poisoning", In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference on (pp. 259-264), IEEE.

[22] T. Lemon, and S. Cheshire, Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4). RFC 3396.

[23] E.R. Leukfeldt, R. Kleemans, and W.P. Stol, "Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks". *British Journal of Criminology*, vol. *57*, no. 3, pp.704-722, 2016.

[24] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modeling for information security and survivability", (No. CMU-SEI-2001-TN-001)., CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2001.

[25] D. Moon, H., Im, I. Kim, and P. J.H. Ark, "DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks", *The Journal of Supercomputing*, vol. *73*, no. 7, pp.2881-2895, 2017.

[26] H. Moghaddasi, S. Sajjadi, and M. Kamkarhaghighi, "Reasons in Support of Data Security and Data Security Management as Two Independent Concepts", A New Model, the open medical informatics journal, vol. 10, no. 4, 2016.

[27] H. Nakai, "U.S. Patent Application No. 14/246,998, 2014.

[28] S.Y. Nam, D. Kim, and J. Kim, "Enhanced ARP: prevent ARP poisoning-basedman-in-the-middle attacks", *IEEE communications letters*, vol. *14, no*. 2, pp.187-189, 2010.

[29] K. M. Osei-Bryson, and L. Carter, "Toward an Assessment of Cultural Relativity and Impacts of ICT Interventions: Assessing

ICT4D at the National Level", In Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

[30] J. Owens, and J. Matthews, "A study of passwords and methods used in brute-force SSH attacks", In USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008.

[31] A. Ornaghi, and M. Valleri,, Man-in-the-middle attacks. In 2003 *Blackhat Conference Europe*.

[32] D. Ramsbrock, R. Berthier, and M. Cukier , "Profiling Attacker Behavior Following SSH Compromises," in Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp.119- 124. , 2007.

[33] S. S. Ray, K. Das, and S. Ghosh, "A RAM-Based MAC Table with Two-Tier Security at Layer 2. IETE Journal of Research", vol. 62, no. 4, pp. 435-445, 2016.

[34] A. Sinnaya, S. Dubus, L. Clevy, and A. Martin, and L. Alcatel, "*Intrusion detection method and system*", U.S. Patent 8,418,247., 2013.

[35] N. Stembert, A. Padmos, M.S. Bargh , and F. Jansen, "A study of preventing email (spear) phishing by enabling human intelligence", In 2015 *Intelligence and Security Informatics Conference (EISIC), 2015 European* (pp. 113-120).

[36] A.K Talukder, V.K., Maurya, B.G., Santhosh, and A.R. Pais, "Security-aware software development life cycle (SaSDLC)-processes and tools", In *Wireless and Optical Communications Networks, 2009. WOCN'09. IFIP International Conference on* (pp. 1-5). IEEE, 2000.

[37] A. Tewari, A.K Jain, and B.B. Gupta, "Recent survey of various defense mechanisms against phishing attacks", *Journal of Information Privacy and Security*, vol. *12, no.*1, pp.3-13, 2016.

[38] Y. Tian, J. Yuan, and S. Yu, "SBPA: Social behaviour based cross Social Network phishing attacks", In *Communications and Network Security (CNS), 2016 IEEE Conference on* (pp. 366-367). IEEE.

[39] A. Wajdi and M. Ali, "Spectrum Sharing Security and Attacks in CRNs: a Review.",(IJACSA) International Journal of Advanced Computer Science and Applications, vol. 5, no.6, pp. 78-87, 2014.

[40] A. J. Zaliwski, "Computer network simulation and network security auditing in a spatial context of an organization. Informing Science", International Journal of an Emerging Transdiscipline, vol. 2, no.10, pp. 159-168, 2011.

[41] Z. Yan, Y. Wang, S. Shao, and B. Li, "The design and implementation of network attack and defense platform based on cloud desktop", In Journal of Physics: Conference Series ,vol. 887, no. 1, pp. 012038, 2017. IOP Publishing.

[42] Q. Yan, and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing", IEEE Communications Magazine, vol. 53, no. 4, pp.52-59, 2017.

[43] O. S. Younes, "A Secure DHCP Protocol to Mitigate LAN Attacks", Journal of Computer and Communications, vol. 4, no. 01, pp. 39, 2016.

[44] S, Sridhar, A. Hahn, and M. Govindarasu," Cyber–physical system security for the electric power grid", *Proceedings of the IEEE*, vol. *100, no.* 1, pp.210-224, 2012.

[45] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds", Architecture, application, and evaluation for smart grid, *IEEE Transactions on Smart Grid*, vol. *4, no.* 2, pp.847-855, 2013.

[46] R. Zhang, X. Wang, R. Farley, and X. Jiang, "On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers", In *Proceedings of the 4th International* ACM. *Symposium on Information, Computer, and Communications Security* pp. 61-69, 2013.