Investigation of Threats for Common Network Attacks

Haytham F. Dhaw, Abdelsalam A. Almarimi [2], Alhadi A. Alajeili[3].
[1] Dept. of Computer Engineering & IT. College of Electronic Technology Bani walid, Libya, h.modo89@gmail.com
[2]Dept. of Computer Technologies. Higher Institute of Engineering. Technologies Bani walid, Libya, belgasem_2000@yahoo.com
[3] Dept. of Quality Assurance Misrata IT Services Company Tripoli, Libya, A.taher@masarat.ly

***Abstract* – Security in computer networks and Internet have serious implications in today's dynamic work environment. Therefore, security mechanisms and policies must be followed and studied continually by investigating the techniques and sophisticated tools for protecting assets of essential network security, which is always required and important for any organization to maintain the confidentiality, integrity and to ensure availability of data. In this context, computer networks needed to be tested and audited against any possible attacks and analyzing the existing vulnerabilities. In this paper, we propose a penetration testing model to evaluate and analyze the vulnerabilities and weaknesses of four VMware workstations.**

We have studied and implemented three attacks using nmap, nessus, and metasploit tools were. The studied attacks include denial of service, backdoor, and man in the middle. The obtained results showed that vulnerabilities were exist in Windows 8, Windows 10, and Windows XP, and hence the proper countermeasures were found and reported to keep such systems secure.

Keywords: Information Security; Network Security; Ethical Hacking.

I. INTRODUCTION

The world is becoming increasingly interconnected, there is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide, as well as, information are critical assets for any organization and that are required to be protected against unauthorized reproduction and attacks from internal and external intruders' sources [1]. Thus, information security management is considerably an important issue to variety of computer networks both public and private on daily basis that involved in different organizations.

Computer and information security are a comprehensive term regarding the protection of computing systems, confidentiality, integrity, and availability against threats and attacks. Numerous approaches and tools have been utilized for assessing the networks and computer systems security.

Recently, threats and attacks against computer and information infrastructures are becoming an increasingly serious problem due to exponentially penetration and hacking processes. Almost all networks may be exploited by a threat in all areas of network technologies. These systems consist of different network devices and computers that is highly important to protect these applications and devices from malicious hackers [2].

In this context, computer networks required to be tested and audited against any possible attacks and analyze the results and its consequences, and investigation of techniques and tools for protecting essential assets of network security is always required and important for any organization to maintain the confidentiality, integrity and to ensure availability of data. Therefore, due to importance of network and information security issues, we have selected such a topic to be investigated in this paper [3].

Penetration testing is the activity conducted as ethical hacking by a penetration tester (PenTester) or auditor. Technically, a penetration test is a security-oriented systematic probing of system from "inside" or "outside" to seek out vulnerabilities that an attacker could exploit. Penetration test can be defined as the simulation of a real-world attack against a target network or application, encompassing a wide range of activities and variations [4]. The variations include simulating an insider threat as opposed to an external attacker, varying the amount of target information provided in advance of the testing.

II. THE PROPOSED MODEL

In this paper, a penetration testing model was proposed as a model to test the integrity of the network security throughout a particular six phases procedure as shown in "Fig. 1". Several tools and techniques are used for information gathering, and to perform scanning and attacks on the intended network security. Therefore, the test network laboratory was setup in attempt to simulate attacks on the given network with a few information about the target system or network, for this reason, the used type of penetration testing known as a grey-box approach to reduce the amount of irrelevant tests and minimize the possibility of damage to the system or network.

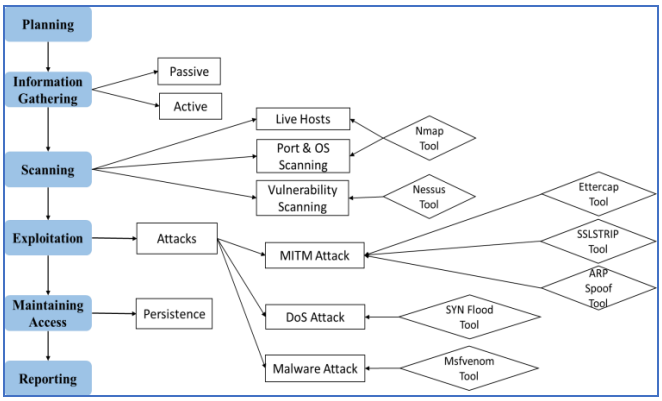

Fig. 1. The proposed Penetration Testing Model.

Received July 2019, Received in received from September 2019, Accepted December 2019, and Published July 2020

The overall process of penetration testing is divided into several phases collectively they form a comprehensive penetration testing methodology. Different methodologies may have different nomenclature for various phases, but these methodologies share the same objective. There are six phases as shown in "Fig. 1", to be used by the network penetration tester.

III. LABORATORY AND EXPERIMENTAL PROCEDURES

To conduct penetration test, first, we have installed VM Ware version 12, which is a virtualization software that allows us to use different operating systems on the virtual machine, to emulate a cross-platform environment. Second, four machines OSs (Kali Linux, Windows XP, Windows 8, and Windows 10) software were installed and the firewall is activated with each machine as depicted in "Fig. 2". Moreover, Windows 8 is provided with Intrusion Detection System (IDS). These OSs software served as target or victim machines throughout the test.

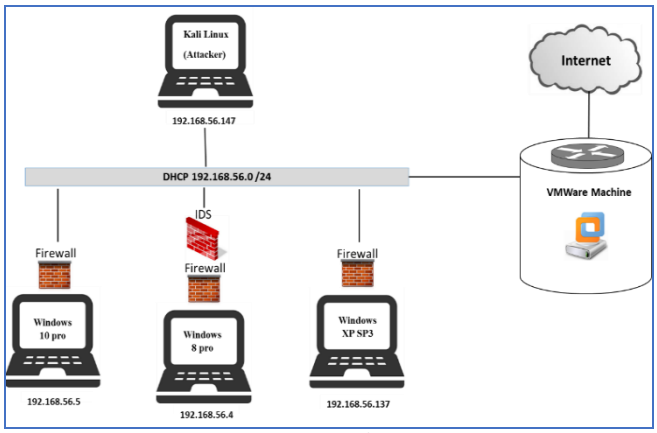

Fig. 2. Laboratory Infrastructure.

The *Nmap*, *Nessus* and *Metasploit* Framework are the main tools which were used to conduct the penetration test [5]. The Nessus tool (6.9.0 version) was installed on Kali machine, as one of the penetration testing tools during the scanning and vulnerability assessment of the penetration test methodology.

IV. PROCEDURE OF PENETRATION TEST

In this section, at first, the proposed penetration testing model is implemented using specific tools and techniques. Secondly, the implementation of each phase of the proposed model is presented with the obtained results for the studied attacks.

A. *Scanning*

Once the enumeration step is achieved via the above steps where the IP addresses (192.168.56.4, 192.168.56.5 and 192.168.56.137) had identified, port scanning along with OS and services fingerprinting were carried out against live hosts (Win 8, Win XP, and Win 10). The result of the achieved procedure contained the open ports and services for both TCP and UDP scans. "Table 1" shows the obtained results. Vulnerability assessment using Nessus tool was used for assessing the vulnerability against the target machines in our laboratory network by using default scan policy in Nessus client [6], as well as, all the scans were executed against the machines (192.168.56.4, 192.168.56.5 and 192.168.56.137). The scan was performed on local security checks for Windows based system.

In Nessus notation, each vulnerability was associated with a risk factor or severity. Identified vulnerabilities were labelled as Critical, High, Medium, Low and Information depending upon base score of Common Vulnerability Scoring System (CVSS) [7].

The results for the scanned target hosts showed a range of risk factors, for instance, target host on 192.168.56.4 demonstrated variable levels of severity as highly vulnerable as 2 Critical risk factors, 6 medium risk factors and 2 as low, while on host 192.168.56.5, were not risk factors for the critical and high levels, but shows 6 and 2 risk factors for the medium and low levels respectively.

Table 1. Open ports and services running on live hosts.

Target Host	Protocol			
	TCP		UDP	
	Port	Service	Port	Service
Windows XP SP3 IP 192.168.56.137	135	Msrpc	123	Ntp
	139	Netbios-ssn	137	Netbios-ns
	445	Microsoft-ds	138	Netbios-dgm
			445	Microsoft-ds
			500	Isakmp
			1900	Upnp
			4500	Nat-t-ike
Windows 8 IP 192.168.56.4	135	Msrpc	137	Netbios-ns
	139	Netbios-ssn	138	Netbios-dgm
	445	Microsoft-ds	500	Iskamp
	554	Rtsp	1900	Upnp
	2869	Icslap	3702	Ws-discovery
	5357	Wsdapi	4500	Nat-t-ike
	10243	unknown	5355	Llmnr
	49152-58			
Windows 10 IP 192.168.56.5	135	Msrpc	137	Netbios-ns
	139	Netbios-ssn	138	Netbios-dgm
	445	Microsoft-ds	500	Iskamp
			1900	Upnp
			4500	Nat-t-ike
			5353	Zerconf

As far as, the target host on 192.168.56.137 is concerned, we found two factors are in high risk lever, two are in medium, and one factor in low risk level, but there was no factor in the critical risk level as shown in "Fig. 3".

Received July 2019, Received in received from September 2019, Accepted December 2019, and Published July 2020

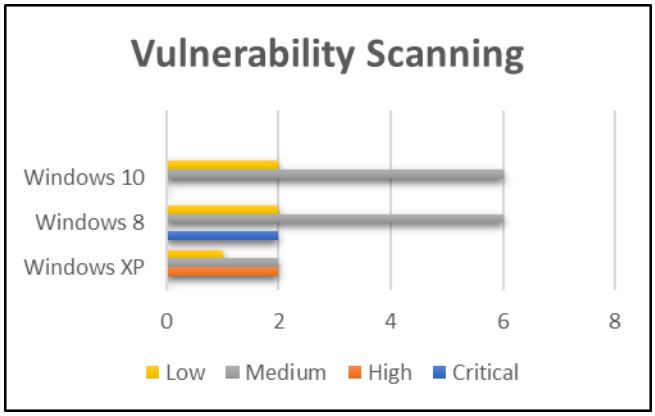

Fig. 3. Vulnerability Scanning from Nessus Tool.

To make a victim machine protected from scanning, some techniques can be considered as countermeasures such as [8]:

1. Firewall should be run to detect scan ports.
2. Use an intrusion detection system, such as, snort tool.
3. Only important ports should remain open.
4. Disable the ICMP protocol for preventing ping scanning.
5. Scanning system ports periodically for both TCP and UDP.
6. Keep the system updated.

B. *Exploitation*

Exploitation is one of most important phases of penetration testing, where the attacks are executed on the victim machines after acknowledge with previous penetration testing phases. These attacks were carried out as following:

- Creating Backdoor executable script was created by *msfvenom* tool to make a reverse connection by a victim machine over port 4444 by Metasploit tool for Kali Linux machine with IP address 192.168.56.147 and the payload was crafted and encoded to ensure that the payload is not detected by antivirus scanners. "Fig. 4", shows the implantation of this task.

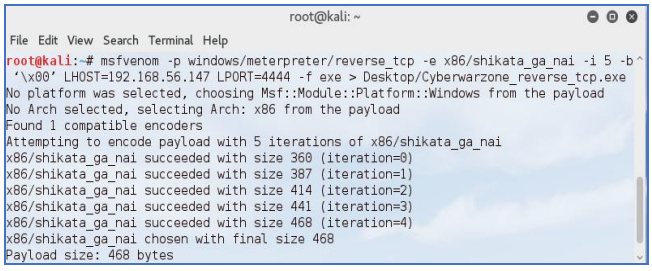

Fig. 4. Create the Backdoor by *Msfvenom*.

Secondly, EXE file is verified on the victim host. Normally, attackers would do this through a phishing, drive-by-download, or other types of attack. Then, the listener is created by *msfconsole* Kali tool to exploit the target machine and uses the command *reverse-tcp* payload [9]. After that it is run on the victim machine and wait for the infected machine to connect to new crafted *msfvenom* reverse tcp *handler*, which is listening on the port 4444 and 192.168.56.147 machine, as shown on "Fig. 5".

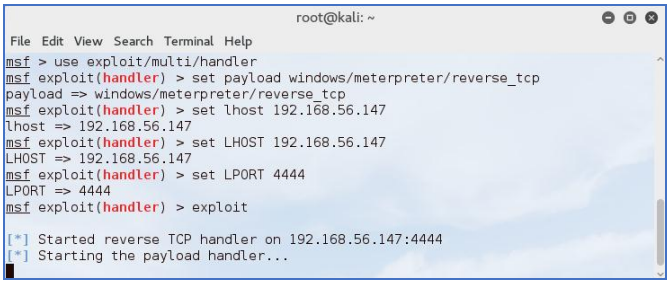

Fig. 5. Launching the Multihandler.

Having run the executable file on the victim machine, *meterpreter* session is viewed by the attacker and full control of the victim machine is obtained as shown in "Fig. 6".

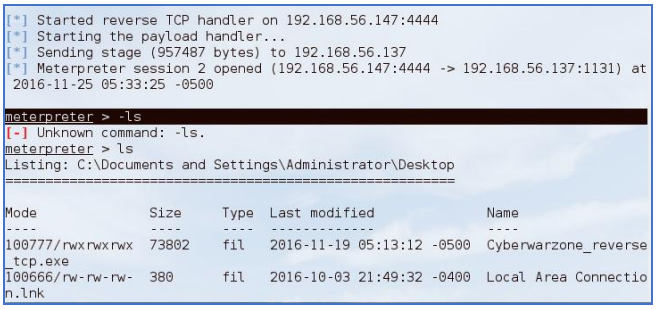

Fig. 6. Meterpreter Session.

After, the back door is being created, we can maintain the access on the victim machine using the *Metasploit* tool for a Meterpreter session to run the persistence script. This is in turn, make a Meterpreter service available even if the remote system is rebooted. To apply this the option -X was used to reconnect back by the victim machine that has IP (192.168.56.137) to attacker machine that has IP (192.168.56.147) on port 4455 when the user login the remote system, and Meterpreter session will be open up as shown in "Fig. 7 and Fig. 8".

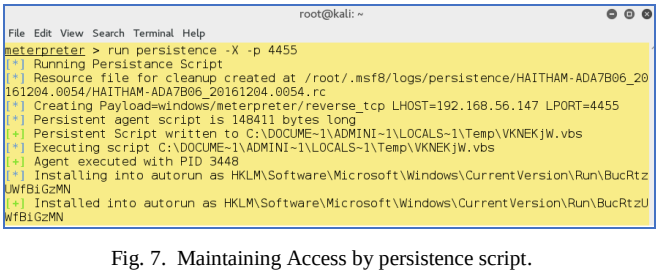

Fig. 7. Maintaining Access by persistence script.

Received July 2019, Received in received from September 2019, Accepted December 2019, and Published July 2020

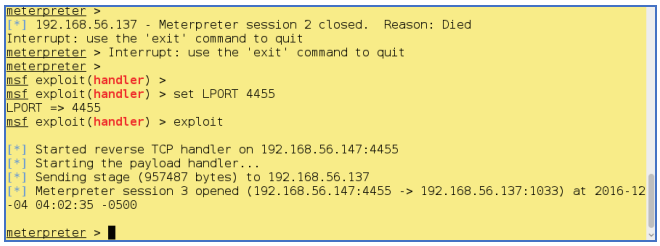

Fig.8. Opening up of Meterpreter session after reboot.

Finally, the victim machine became compromised. So, the below proposed techniques that should be considered and highly recommended as countermeasures to make a victim machine protected from this type of attack are listed as following:

1. Installing Anti-Malware Applications.
2. Using trusted software vendors.
3. Avoiding unknown attachments.
4. Avoiding the use of infected computers.
5. Deleting the old files.
6. Monitoring the network traffic.
7. Updating the operating system.

- Denial of Service Attack was used Metasploit framework has many built-in *auxiliary* modules that perform different types of attack [6]. One of them is the *auxiliary* module (*SYNFLOOD* module) which used for DoS attack by flooding the server with SYN packets that cause denial of service as shown in "Fig. 9".

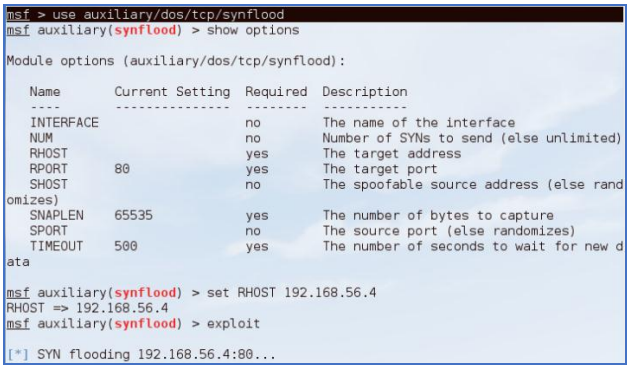

Fig. 9. SYN flooding attack using *metasploit* tool.

The impact of DoS attack on the CPU performance of victim machine that has the IP Address (192.168.56.4) in our network is monitored. Figure (10) shows the difference of the processor performance before and after implementing the attack. From "Fig. 10", it is clear that the performance of the processer is affected and became very slow.

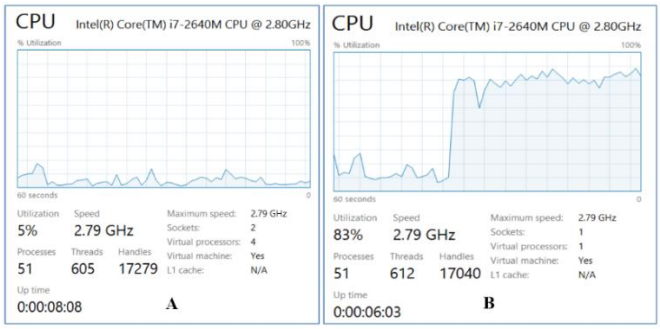

Fig. 10. A. The performance of the processor before the attack. B. The performance of the processor after the attack.

So, many techniques should be applied and considered as countermeasures to avoid the DoS attack as follows:

1. Firewall serves according to the set of rules and some other criteria.
2. Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS): for the certain protocols like (TCP, UDP, ARP), the IPS can identify the abnormalities in the behavior of the network such as significant difference in a number of connections per second, packets per connection, packets to specific ports.
3. Infrastructure and network configuration: the configurations have should be managed to make network secure. The basic rate limiting and access control list (ACL) capabilities should be identified by the routers. Some routers have mechanisms and proprities that can be used to block flooding attacks.
4. Audits: is an evaluation of the system done by the experts. Their knowledge and tools for the fake attacks may reveal a wrong configuration, the weaknesses in the network and the level of security that is implemented [4].

- Man-In-The-Middle attack

The Man-In-The-Middle (MITM) attack takes advantage of the weaknesses in the authentication protocols which used by communicating parties. Since, the third-party issue certificates generally provide authentication, the system of certificate generation becomes vulnerable once the attack is implemented.

The ARP Spoofing and SSL Stripping techniques were used to implement an MITM attack. In this attack, firstly, we let the IP forward option in enable mode. Also, the enable mode should be checked to verify whether the forwarded IP is pre-configured or not. "Fig. 11", shows the implementation of this task.

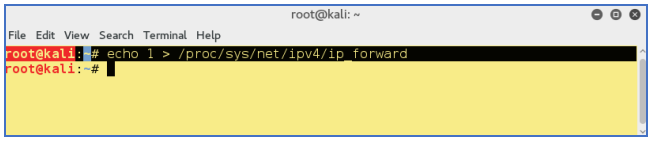

Fig .11. Enabled IP Forwarding.

Received July 2019, Received in received from September 2019, Accepted December 2019, and Published July 2020

Secondly, redirecting the traffic from source port 80 to the destination port 10000, which should mainly transmit via TCP protocol. All of this traffic will take place by updating the NAT table. Whenever the conditions with match the packets will be redirected to port 10000 as specified. “Fig. 12”, shows the implementation of this step.

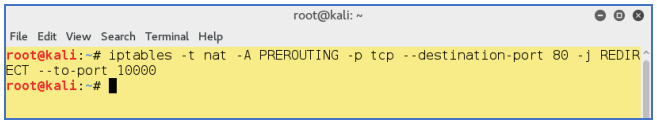

Fig. 12. Redirection of the Packet.

Thirdly, the HTTP traffic is redirected to attacker machine that is done by ARP Spoofing tool as shown on “Fig. 13”, Then SSL stripping is carried out in order to obtain the credentials for a particular website as shown on “Fig. 14”.

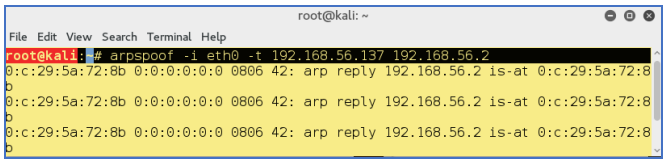

Fig. 13. ARP Spoofing Tool.

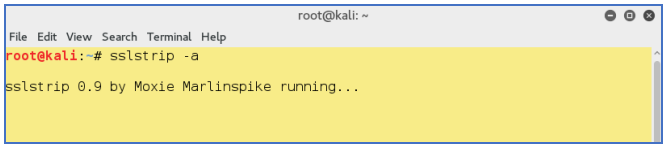

Fig. 14. SSL Stripping.

Finally, the given attack and stealing credentials was successfully performed by using ettercap tool as shown on “Fig. 15”. Having implemented the above mentioned steps on certain HTTPS website, so the user name, password and PIN number of such a website were obtained. The final result of this attack is shown in “Fig. 16”.

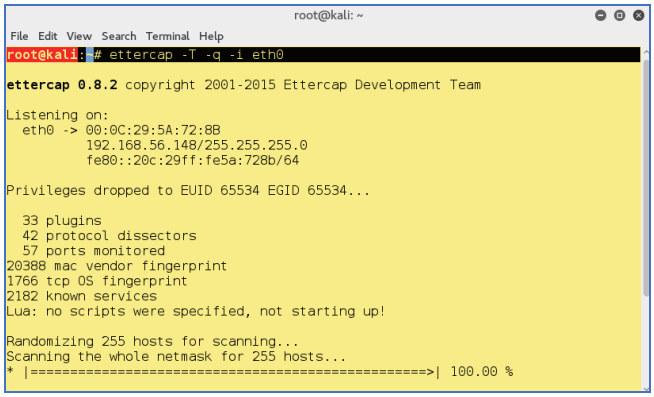

Fig. 15. Listening by Ettercap Tool.

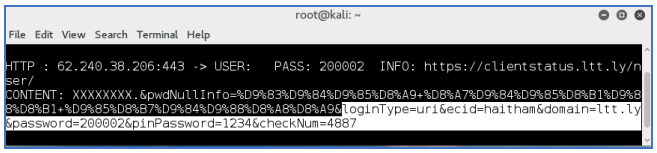

Fig. 16. Successful Attacked Performed to Obtain the User Credentials.

As the obtained information in this attack is critical and important, the developers should consider some techniques to be applied as countermeasures to avoid such an attack. The recommended countermeasures are:

1- Static ARP Table: is the easiest and efficient solution, where each host on the network, or at least the most sensitive ones (default gateway, DHCP server, DNS, Web server, etc), that have MAC address should be set manually in the ARP table so that cannot be modified with ARP reply. For instance, the syntax that can be used to add a static entry in the ARP table is: ***arp -s IP_ADDRESS MAC_ADDRESS*** [9].
2- Intrusion Detection System (IDS): this technique analyzes the behavior of the host and trigger an alarm when something is suspicious. Also, the IDS analyzes behaviors regarding some rules, such as:
   - Checking if the sender MAC address of an ARP reply coming from a sensitive host (e.g. default gateway) match the proper MAC address (wrote previously by the security admin).
   - Checking if a host sends unsolicited ARP reply.
   - Checking if each IP address has a unique MAC address in the LAN.
3- Encryption and authenticated channel: using robust cryptosystems to secure channel, then the captured encrypted data by an attacker will be irrelevant without the proper encryption key. In order to avoid this security issue, secure hosts (like Web server) use an authentication system to ensure that the communication is established with the proper host.
4- Older version of SSL protocol: is usually prone to a penetration by attackers using *SSLstrip* tool. Therefore, SSL protocol is highly recommended to be updated.

In general, the intrusion detection system (IDS) was used as a countermeasure for both DoS and MITM attacks by utilizing *SAX2* tool for widely analyzing the suspicious behavior and alarming for implemented attacks on the target host (192.186.56.4).

The event curve on “Fig. 17”, shows information regarding ICMP ping, warning signal regarding TCP port which scanned, and the critical level occurred when ARP MAC address was altered. The traffic curve on "Fig. 17" shows the DoS attack where the influx of packets was relatively increased.

Received July 2019, Received in received from September 2019, Accepted December 2019, and Published July 2020

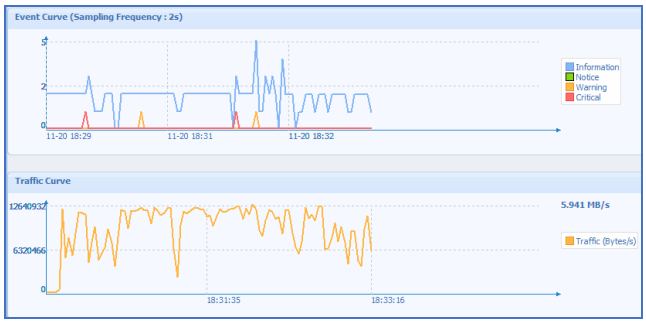

Fig. 17. Results Obtained from IDS (SAX2 Tool).

V. CONCLUSION AND FUTURE WORK

In conclusion, properly utilized of security methodologies and tools can verify their usefulness for understanding the weaknesses of the network or system and how they might be exploited. Penetration testing is not an alternative to other security measures however، it can be used to complement the defense in depth principle. Moreover, the use of old systems should be avoided as it may have serious vulnerabilities.

Full security cannot be reached, this is one of the fundamental principles of security, but a high rate of safety could be achieved through the implementation of network penetration testing periodically. Therefore, penetration testing techniques is very useful for building strategies for measuring the extent of securing data in order to improve the management performance, through the filtration of data.

Finally, in order to perform a successful penetration tests, the underlying methodology should also make use of different security tools.

The proposed model in this study dealt with the most basic penetration testing activities and artifacts at each test phase. As a future work, the suggested model which can be enhanced by utilizing more sophisticated tools to increase vulnerability coverage and try/launch more attacks, for instance, DNS spoofing, Brute Force, and Endpoint devices attacking (printer and routers) to highly evaluate a network security and providing beneficial countermeasures.

REFERENCES

[1] Purna Chandra Sethi and Prafulla Kumar Behera, “Methods of Network Security and Improving the Quality of Service – A Survey”, IJARCSSE, Volume 5, Issue 7, July 2015.

[2] Richard R. Linde, "Operating system penetration". In Proceedings of the May 19-22, 1975, national computer conference and exposition, AFIPS ’75, pages 361–368, New York, NY, USA, 1975. ACM.

[3] K. Xynos, I. Sutherlan, H. Read, E. Everitt, and J C A. Blyth. "Penetration testing and vulnerability assessments: A professional approach". In Proceedings of the 1st International Cyber Resilience Conference. Edith Cown University, Perth, Western Australia, SECAU - Security Research Centre, 2010.

[4] Nishant Shrestha, "Security Assessment via Penetration Testing; A Network and System Administrator's Approach", Master, DoI, OSLO, 2012.

[5] Robert W. Beggs, "Mastering Kali Linux for Advanced Penetration Testing", UK: Packt Publishing Ltd, 2014.

[6] James Broad and Andrew Bindner, "Hacking with Kali". First edition. USA: Steve Elliot, 2014.

[7] "Tenable Network Security”. http://www.nessus.org/expertresources/ Videos. [Accessed on Nov 25, 2018].

[8] Purna Chandra Sethi and Prafulla Kumar Behera, "Methods of Network Security and Improving the Quality of Service – A Survey", IJARCSSE, Volume 5, Issue 7, July 2015.

[9] Georgi Weidman, "Penetration Testing A Hand-on Introduction to Hacking". San Francisco: William Pollock, 2014.

Received July 2019, Received in received from September 2019, Accepted December 2019, and Published July 2020