Assessment of Website Security by Penetration Testing Using Wireshark

Sandhya S[1],
Assistant Professor[1]
MCA Department, RVCE, Bengaluru
sandhyas@rvce.edu.in

Sohini Purkayastha[2], Emil Joshua[3], Akash Deep[4]
Student[2,3,4]
MCA Department, RVCE, Bengaluru
sohinipurkayastha93@gmail.com,emil.j009@gmail.com, akashdeep9312@gmail.com

***Abstract*— Evolving technology has created an inevitable threat of expose of data that is shared online. Wireshark tool enables the ethical hacker to reveal the flaws in the system security at the user authentication level. This approach of identifying vulnerabilities is deemed fit as the strategy involved in this testing is rapid and provides good success in identifying vulnerabilities. The usage of Wireshark also ensures that the procedure followed is up to the required standards. This paper discussed about the need to utilize penetration testing, the benefits of using Wireshark for the same and goes on to illustrate one method of using the tool to perform penetration testing. Most areas of a network are highly susceptible to security attacks by adversaries. This paper focuses on solving the aforementioned issue by surveying various tools available for penetration testing. This also provides a sample of basic penetration testing using Wireshark.**

Keywords— Penetration testing, Wireshark

I.INTRODUCTION

Considering the exponential increase in the exploitation of networks, penetration testing has become an essential tool and technology for the maintenance of network security. Several websites of renowned banks and organizations may contain information that need to remain encrypted but more often than not, attackers succeed in decrypting the users' privacy by hacking such websites.

The past decade has witnessed some of the most serious security breaches. In the year 2015 the Kerala Government website was hacked, which placed the policies and schemes of the Government at stake [1]. Cybercriminals recently came up with the disguise of fake technical support to steal data. A report generated by security firm Symantec stated that the year 2015 saw close to 5 lakh attacks which made India the 11th nation to be most prone to tech support scams [2].

A major breach happened when the US government database that stored information about the personnel was hacked and data about approximately 22 million people was revealed as stated by the Washington Post in the year 2015 [3].

These security breaches have been a matter of serious concern as to how should the data be protected from such strong attacks by people with criminal intent. These attacks have led to the improvement of current cyber security systems by exposing those weaknesses which encourage hacking. This is when we need penetration testing. The process involved in it is maleficent but ethical and can be used to analyze a system or network to identify the security vulnerabilities that are present.

A penetration tester or a pen tester reuses methods commonly used by hackers, to find any glitch in the security of the system [4]. The most significant part of penetration testing is checking the results of an attack [5]. The moment a vulnerability is detected it starts exploiting sensitive data [6].Manual or automated technologies are used to perform penetration testing in a very systematic approach thereby unmasking the potential points of exposure in the security of servers, web applications, wireless networks, network devices and mobile devices [7], that might be used by a cybercriminal to gain entry into a system.

Wireshark is a tool that has proven itself very useful in network sniffing. The packets that it captures from a live network can be analyzed without difficulty within the tool itself. If there is a security lapse in any of the systems, that record data online for big organizations, then access to such systems can be gained by analyzing the packets being transmitted during user authentication. Wireshark aims at understanding, how prone a system is to security breaches.

II.REVIEW OF LITERATURE

Various methods perform penetration testing to check the vulnerability level of websites. The section below describes the related work through such techniques:

***A. Metasploit*:** The Metasploit Framework is an open source platform that provides a library of constantly updated exploits and an environment for developing tools and automating the process of penetration testing [8].It has a built-in sniffer, DNS server and access point [9] that can be used in the simulation of attacks. There is also a shell called 'Meterpreter' that can be used by pen testers to capture sensitive data like user credentials [8].

978-1-5090-4559-4/17/$31.00©2017IEEE

This is done in order to detect user credentials that maybe weak or reused. When using this framework the exploit is selected first, then configured with the remote IP address and port number. This is followed by choosing the payload which is also configured with the local IP address and port number. The final step is execution of the exploit [9].

***B. w3af(Web Application Audit and Attack Framework)*:** w3af is a framework that has been refined by the developers of Metasploit to audit and exploit web applications [10].It has a core and plugins. The core acts as a coordinator of processes and the plugins look for vulnerabilities to be exploited [10].It's very flexible and user-friendly. Its features include proxy support, cookie handling and user-agent faking that can prove highly useful in testing the weaknesses of websites and applications [10].

***C. Nipper Studio*:** An organization called Titania has created a tool called Nipper Studio that is used to analyze security issues of an application [10, 11].It can be easily configured as compared to w3af and is very user-friendly. It generates reports that can be used as a basis for improving the network infrastructure of organizations. It works with Cisco, First Base Technologies and many such companies [11].

***D. OWASP Zed Attack Proxy*:** The OWASP Zed Attack Proxy is a web application vulnerability scanner [12] that studies a web application to reveal the loopholes it has with regard to security. It has been developed as a part of the Open Web Application Security Project. The penetration testing done using this tool is mostly manual. ZAP is capable of providing proxy support.

One of the most important features of ZAP is that if there is a testing in progress, there is a facility to pause it and come back later to exactly where it had been stopped and resume from there [12]. OWASP ZAP can check if specific vulnerabilities of a website have been fixed or not.

***E. Back Track*:** Back Track is a penetration testing tool exclusively for LINUX users. It is used to study packets being transferred online to retrieve information from them and in turn find out how secure the network being used is. User credentials can easily be cracked using this [13]. Also, it can be used to add new encrypted tools to the database that holds the most varied collection of security tools [14].

***F. Skipfish*:** Skipfish is another highly recommended web application security scanner. With Skipfish the assessment of the target applications are very specific and focused so naturally the time taken is a lot lesser than many of the other tools that are available [15].If necessary the brute force feature of this tool can be turned on. It uses well-designed probes to perform quality checks.

Skipfish covers most of the security problems, even those that are generally ignored by other tools used for assessing vulnerabilities [15].At the end of a scanning procedure a scan report can be generated that consists of information about issues that are very specific to the problem[15].

Need and Relevance of Wireshark:

Wireshark is a network protocol analyzer that satisfies standards of industries and educational institutions all around the world and therefore is a more preferable choice for most penetration testers for testing the strength of sites against security attacks. Data can be easily captured from a live network and analyzed offline.

It supports hundreds of protocols and is not exclusive to any particular operating system. Also it is said to have the most powerful display filters in the industry. Proper documentation about Wireshark is available which helps in learning it quickly

III. MOTIVATION AND CONTRIBUTION – PROPOSED MECHANISM

The work proposed involves the usage of Wireshark in a very basic penetration testing technique of information gathering. A matrimonial website called www.abpweddings.com has been used for the purpose of demonstration.

The steps have been listed as follows:

***Start Wireshark from command line*:**

Start the Linux terminal as root user and from root Wireshark is started. This will make all the local interfaces of the system available under the list of interfaces in Wireshark

Select interface and start live capture:

From the list of local interfaces of the system that are available under the label 'Capture', wlan0 (wireless

connection) is selected and capture is started as shown in Figure-1.

This list shows only the local interfaces that are accessible to Wireshark. It is possible to select more than one interface and capture from them simultaneously [16].

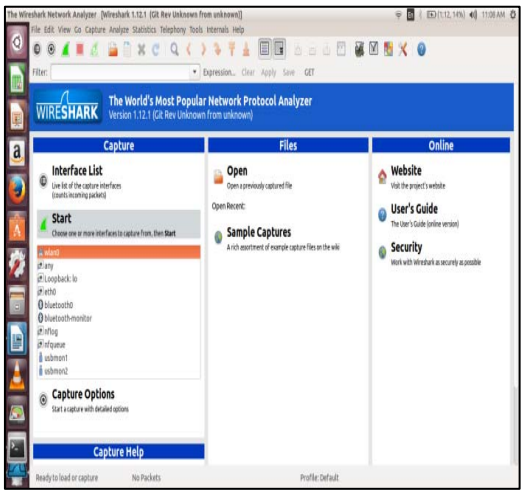

Figure 1: Selecting wlan0 as preferred capture interface

The Wireshark window is then minimized to let it continue to capture live packets while websites are surfed in the browser.

***Log into vulnerable website*:**

The website(www.abpweddings.com) is opened on Firefox and login is performed with valid username and password(a profile was created previously on this website for the purpose of demonstration) as shown in Figure-2

As soon as login is successful the live capture on Wireshark is stopped (Figure 3). Successful login means that the user credentials that were used to login are now on the network and are ready to be captured.

Figure 2:Logging into vulnerable website

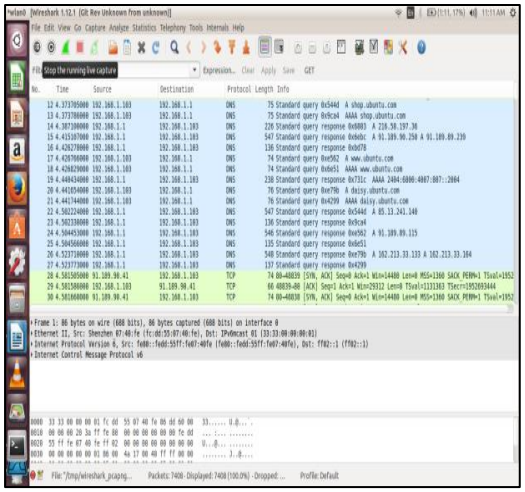

Figure 3:Stopping the running live capture

***Filter HTTP requests*:**

Specify the display filter as HTTP. This results in displaying a list of all HTTP packets because only HTTP traffic needs to be analyzed for the current experiment. Wireshark has the largest number of display filters that are used for packet filtering to view only specific traffic [16].

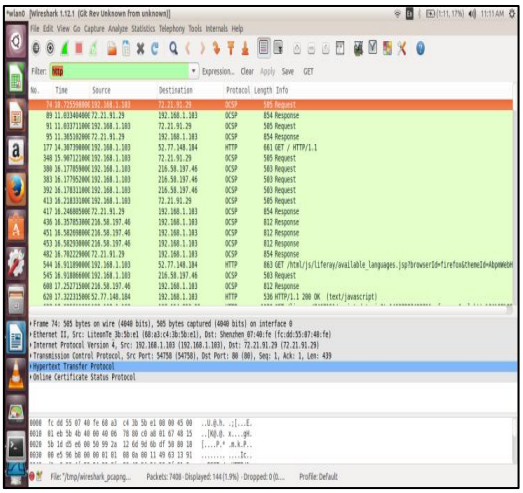

Figure 4: Filtering HTTP traffic

***Look for POST request*:**

Amongst the list of all HTTP packets the first HTTP POST request is selected. HTTP packets need to be sniffed for the first POST request because this is the request to login which contains user credentials.

This packet is then right clicked and the Follow TCP Stream option is selected. A Follow TCP Stream dialog appears which shows the entire ordered stream content of the packet selected [16]. The traffic from sender to receiver appears in red whereas the traffic from receiver to sender appears in blue.

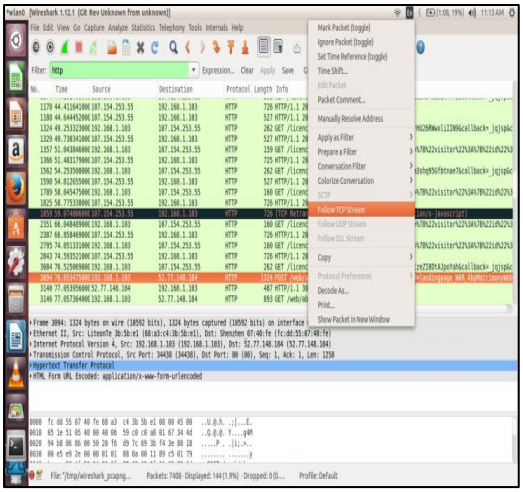

Figure 5: Following TCP Stream

***Analyzing the traffic from sender to receiver*:**

To look for user credentials the red content must be analyzed. The stream content shows the entire conversation between the client website and the server hence there is a set of red data followed by blue data which is again followed by red data and so on.

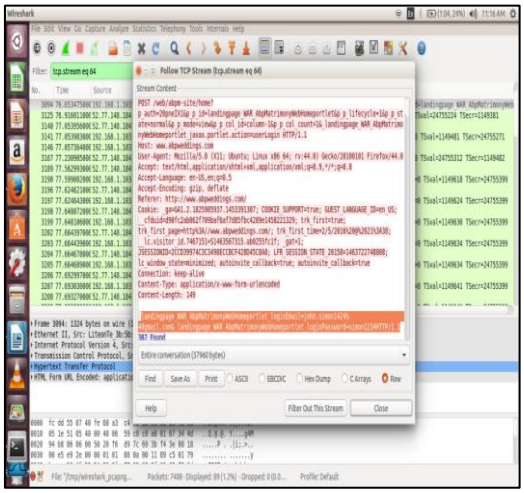

Figure 6: Analyzing the TCP Stream

The first set of red data according to the order of the conversation is analyzed in this particular case. The last line shows the loginEmail and loginPassword in plain text. Therefore, the conclusion is that the penetration test case resulted in a failure which indicates that the particular website is not secure.

IV. CONCLUSION

The Figure-4 depicts filtering of HTTP traffic using the HTTP display filter. Figure-5 depicts selecting the first HTTP POST request packet to follow its TCP stream. Figure-6 shows the stream content consisting of the user credentials highlighted in red. This work shows the usage of Wireshark as a packet sniffer to perform the penetration testing technique of information gathering to indicate whether a website is secure or vulnerable. The result shows that the website that has been assessed has a lapse in its security mechanism.

REFERENCES

[1]. http://timesofindia.indiatimes.com/city/thiruvananthapuram/Kerala-government-website-hacked/articleshow/49124011.cms

[2]. http://timesofindia.indiatimes.com/city/delhi/Cybercrooks-posing-as-tech-support-steal-data-Report/articleshow/51964242.cms

[3]. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[4]. Swarnjeet Kaur,Harmandeep Singh,A Descriptive Review Of Different Penetration Testing Toold And Methods, *International Journal Of Engineering Sciences &Research Technology*

[5]. William G. J. Halfond,Shauvik Roy Choudhary and Alessandro Orso: Penetration Testing with Improved Input Vector Identification, *International Conference on Software Testing Verification and Validation*, 2009, pp. 346-355.

[6]. http://www.softwaretestinghelp.com/penetration-testing-guide/

[7]. http://www.coresecurity.com/penetration-testing-overview

[8]. David Kennedy,Jim O'Gorman,Devon Kearns and Mati Aharoni,"Metasploit:The Penetration Tester's Guide",2011 Edition

[9]. http://www.computerweekly.com/tip/5-penetration-test-tools-to-secure-your-network

[10]. Manju Khari and Neha Singh:An Overview of Black Box Web Vulnerability Scanners, *International Journal of Advanced Research in Computer Science and Software Engineering*,Volume 4,Issue 5,May 2014

[11]. http://www.titania.co.uk

[12]. http://cybersecology.com/the-owasp-zed-attack-proxy-zap-scanner/

[13]. http://www.linuxuser.co.uk/reviews/backtrack-5-review-if-youre-serious-about-pentesting-dont-leave-home-without-it

[14]. http://www.backtrack-linux.org/

[15]. http://lcamtuf.blogspot.in/2010/11/understanding-and-using-skipfish.html

[16]. https://www.wireshark.org/docs/wsug_html_chunked/ChCapInterfaceSection.html

[17]. Kumar, CV Arul, D. Manoj Kumar, and P. Prithiviraj. "Privacy Policy Multiparty Access Control On Content Sharing Sites." Imperial Journal of Interdisciplinary Research 2.6 (2016).