Vulnerability Analysis and Password Cracking Using Wireshark

Ginilekshmi A.O
Department of Computer Applications
Amal Jyothi College of Engineering
Kottayam, India
ginilekshmiao@mca.ajce.in

Anjaly Devassia
Department of Computer Applications
Amal Jyothi College of Engineering
Kottayam, India
anjalydevassia@mca.ajce.in

Ananthu Krishna P.S
Department of Computer Applications
Amal Jyothi College of Engineering
Kottayam, India
ananthukrishnaps@mca.ajce.in

Ajith G.S
Assistant Professor, Department of Computer Applications
Amal Jyothi College of Engineering
Kottayam, India
gsajith@amaljyothi.ac.in

Abstract— A lot of data is being transferred across a network every time. These data can be used by the system administrators for analyzing real time network traffic. But, the data being transferred may be confidential or proprietary and there are chances for an attacker or cracker to discover vulnerabilities in the network and exploit the information contained in it. Wireshark, a network protocol analyzer uses network sniffing to capture usernames and passwords. This paper demonstrates a website which can be used with Wireshark to enable the captured passwords and usernames of several sites to be listed in an efficient way.
.

Keywords—Wireshark, password cracking, network sniffing, SSL, HTTP, HTTPS

I. INTRODUCTION

According to current trend almost all the public and private sectors are digitizing their business. About 24000 gigabytes of data are transmitted through the internet every single second. Most of the companies know how to sell data but not how to protect it. A majority of corporates are unprepared for cyber security challenges.

Though India is the second-fastest-growing digital economy, CIO survey by Force point and Frost & Sullivan portraits that about 69% of Indian companies are at a risk of data breach. Also, nearly 7.5 million Adobe Creative Cloud user records were left exposed to the public in 2019 due to poor security.

Low-level package data that is transmitted over a network can be captured using network sniffers. For discovering valuable information such as user ids, passwords etc., a hacker or an attacker can use this captured data. Wireshark is one among such network sniffers which is aimed to be used by the network architects to analyze real-time traffic over the network. On the other hand, it is misused for the purpose of hacking and theft of sensitive information.

HTTP is an application layer protocol that offers a set of rules and standards for transmitting information over the World Wide Web. Even if you type in HTTP:// it will redirect to an https for providing more security. The data sent through HTTP channel can be taken and read by anyone because it does not use any encryption methods to protect the data. This limitation of HTTP is favorable for Wireshark in network sniffing.

a) Penetration Testing
To exploit vulnerabilities in a computer system cyber-security expert uses a security exercise called penetration testing (or pen testing). Pen tests can be performed manually or it can be done automatically through software applications

b) HTTP
Hypertext Transfer Protocol is used for establishing communication between client computers and servers. There is a higher chance of information exploitation because it does not use encryption for data security. So, it is a good fit for websites designed for information consumption

c) HTTPS
Hypertext Transfer Protocol Secure is a safe way to send data between web browser and a website. It is a secure version of HTTP because it has SSL technology and encryption to protect data

d) Wireshark
It is a free and leading open source network traffic analyzer which can be used for network troubleshooting, and packet capturing. To identify particular types of network traffic, it uses built-in color coding features.

e) Password Cracking
Confidential information can be tracked from the place it is stored or transport from, a computer system. It is mainly done by using different cracking algorithms or trying different combinations in the wordlist of passwords

II. METHODOLOGY

The packets transmitted over the network are intercepted by wireshark and the content that is being used by other network users are exposed.

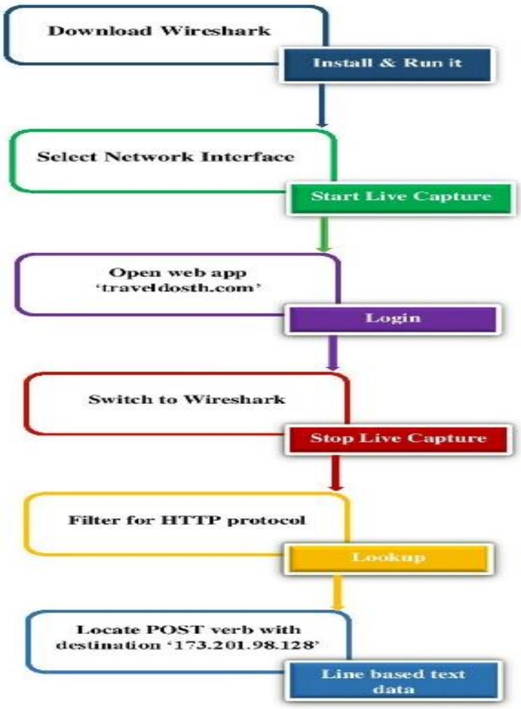
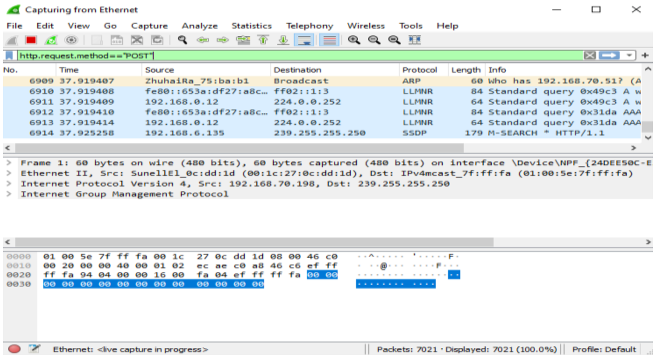


Fig 1: Working of wireshark

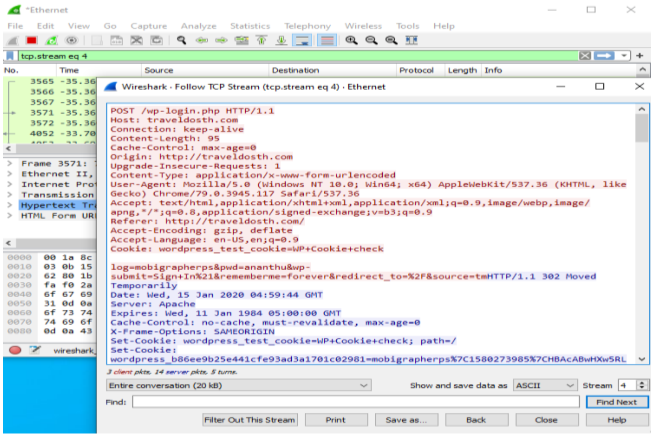
- Open wireshark. It will ask you to "Choose one interface to capture from".
- Select the network interface you want to sniff. If you are on a local area network, then you should select the local area network interface.
- Login to a page which uses http protocol.
- To filter the packets type http.request.method==”POST”


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method=="POST"
No.   Time       Source                    Destination      Protocol Length Info
 6909 37.919407  ZhuhaiRa_75:ba:b1         Broadcast        ARP        60 Who has 192.168.70.51? (A
 6910 37.919408  fe80::653a:df27:a8c…      ff02::1:3        LLMNR      84 Standard query 0x49c3 A w
 6911 37.919409  192.168.0.12              224.0.0.252      LLMNR      64 Standard query 0x49c3 A w
 6912 37.919410  fe80::653a:df27:a8c…      ff02::1:3        LLMNR      84 Standard query 0x31da AAA
 6913 37.919414  192.168.0.12              224.0.0.252      LLMNR      64 Standard query 0x31da AAA
 6914 37.925258  192.168.6.135             239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{24DEE50C-E
> Ethernet II, Src: SunellEl_0c:dd:1d (00:1c:27:0c:dd:1d), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.70.198, Dst: 239.255.255.250
> Internet Group Management Protocol

0000  01 00 5e 7f ff fa 00 1c  27 0c dd 1d 08 00 46 c0   ··^·····'·····F·
0010  00 20 00 00 40 00 01 02  ec ae c0 a8 46 c6 ef ff   · ··@·······F···
0020  ff fa 94 04 00 00 16 00  fa 04 ef ff ff fa 00 00   ················
0030  00 00 00 00 00 00 00 00  00 00 00 00               ············

Ethernet: <live capture in progress>  || Packets: 7021 · Displayed: 7021 (100.0%) || Profile: Default
```

Fig 2: Filter HTTP packets

- Then choose the corresponding packet. Right click and select Follow TCP Stream.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 4
No. Time Source Destination Protocol Length Info
Wireshark · Follow TCP Stream (tcp.stream eq 4) · Ethernet

```
POST /wp-login.php HTTP/1.1
Host: traveldosth.com
Connection: keep-alive
Content-Length: 95
Cache-Control: max-age=0
Origin: http://traveldosth.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/79.0.3945.117 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://traveldosth.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_test_cookie=WP+Cookie+check

log=mobigrapherps&pwd=ananthu&wp-
submit=Sign+In%21&rememberme=forever&redirect_to=%2F&source=tmHTTP/1.1 302 Moved
Temporarily
Date: Wed, 15 Jan 2020 04:59:44 GMT
Server: Apache
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
Set-Cookie:
wordpress_b86ee9b25e441cfe93ad3a1701c02981=mobigrapherps%7C1580273985%7CHBAcABwHXw5RL

3 client pkts, 14 server pkts, 5 turns.
Entire conversation (20 kB)    Show and save data as ASCII    Stream 4
Find:
```

Fig 3: Save file contents

- Click on save as button to save the files
- Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.

III. RESULT

The information of several websites collected using wireshark is available as individual files. These files can be saved separately. So, next time when we login to those websites, there is a need to check each of the saved files to find the password and username. It is difficult to obtain the required data each time by accessing different files. To ease the process, we suggest to use a method to sort the collected data. After saving data of several sites, all these files are uploaded to a website which arranges the captured usernames and passwords in an efficient way.

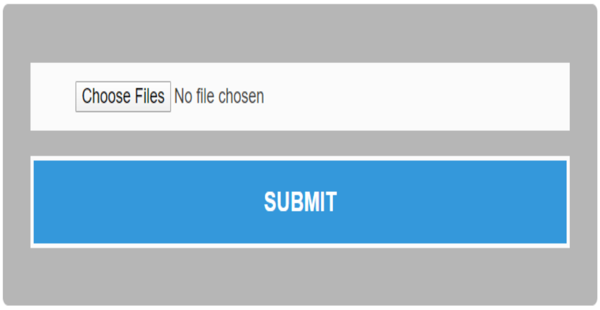
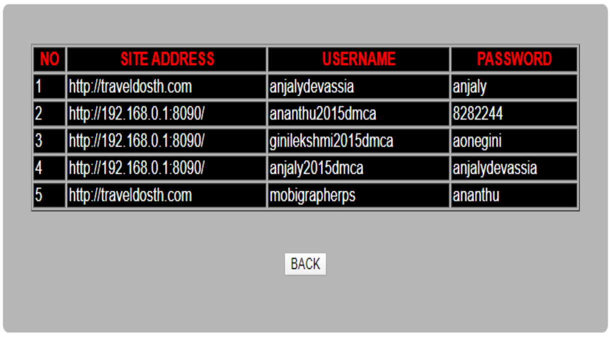


Fig 4: Upload saved files



NO	SITE ADDRESS	USERNAME	PASSWORD
1	http://traveldosth.com	anjalydevassia	anjaly
2	http://192.168.0.1:8090/	ananthu2015dmca	8282244
3	http://192.168.0.1:8090/	ginilekshmi2015dmca	aonegini
4	http://192.168.0.1:8090/	anjaly2015dmca	anjalydevassia
5	http://traveldosth.com	mobigrapherps	ananthu

Fig 5: Filter usernames and passwords

IV. LITERATURE REVIEW

A. Piyush Goyal [1]

- Many tools like wireshark and tcpdump are useful in cyber mitigation and assist the network administrators in better assessing the servers, traffic and diagnosing the issues.
- But they have become the favourite tool of cyber criminals to scan a particular network and sniff on unprotected data.
- Tcpdump is useful in task of analyzing the raw data by providing various options.
- Wireshark is accredited to its simple and graphical interface and it has powerful capturing and filtering options.

B. Sandhya S [2]

- The most significant part of penetration testing is checking the results of an attack.
- The moment a vulnerability is detected it starts exploiting sensitive data.
- Wireshark aims at understanding, how prone a system is to security breaches.

C. Alberto Dainotti [3]

- Traffic characterization at packet level on both HTTP and SMTP traffic.
- Packet level characterizations express traffic flows in terms of inter-packet time and packet size.
- According to some generalization properties the Egress and Ingress traffic varies.
- Here the analysis performed on TCP packets. Traffic was captured and analysed using Plab software.
- In this paper they use payload for operations. Upstream and downstream traffic are separately studied here.

D. Antonio Pescapé [4]

- Common flow objects are TCP connections, flows, bidirectional flows, services, hosts, traffic profiles, application categories, applications, content type etc.
- Scalability is a challenging trend in internet evolution.
- Consistent evaluation and comparison methods needs standard testing, validation procedures, and benchmarking metrics.

E. Mohammed Abdul Qadeer [5]

- A packet sniffer captures the packets in promiscuous mode and then decodes them.
- The packet sniffing can be used by the system administrator to monitor and troubleshoot the network traffic
- Here they uses wireshark for output capturing.
- Basic steps for development of packet sniffer are socket creation, set NIC in promiscuous mode, Protocol interpretation etc.
- Some methods used to sniff packets are ARP spoofing, MAC flooding etc.
- ARP detection technique, RTT detection or SNMP monitoring can be used for detection of packet sniffers.

F. Pimjai Navabud[6]

- HTTPs encrypts the traffic between browser and the website. It has the same method syntax to the HTTP.
- However, it enables the browser to apply an extra encryption of SSL TLS to encrypt the traffic.
- It shown that HTTPS provides a much more secure channel over network than HTTP.

G. Arthur Callado[7]

- Traffic measurements can be divided into active and passive measurements.
- Through the injected traffic active measurement can be obtained. It is mainly used for vulnerability detection.
- Passive measurement is obtained without injecting traffic. It is done by observing the network and flows.

H. Fei YU[8]

- Password cracking classification from different dimensions.
- It uses rainbow table cracking, dictionary cracking, and brute-force cracking.
- Success and speed of password cracking can be increased by the integration of various methods.

V. CONCLUSION

Wireshark is a network protocol analyzer used mainly by network architects to analyze traffic in their network. It is also used as a hacking technique for sniffing confidential data of several users. It can be used by the security department of an organization to detect problems in their network and use efficient methods to solve it. This plays a big role in the investigations to prove crimes by sniffing sensitive information of criminals or victims. As a part of security, data integrity is a big issue in HTTP protocol as the data is not encrypted for protection. Since HTTPS has SSL technology, the data is protected to an extent.

VI. References

[1] Piyush Goyal, “Comparitive Study of two Most Popular Packet Sniffing Tools-Tcpdump and Wireshark” https://ieeexplore.ieee.org/document/8319360

[2] Sandhya S,”Assessment of Website Security by Penetration Testing Using Wireshark” https://ieeexplore.ieee.org/document/8014711

[3] Alberto Dainotti,”A Packet-level Characterization of Network Traffic” https://ieeexplore.ieee.org/document/1649716

[4] Antonio Pescapé,”Issuse and Future Directions in Traffic Classification” https://ieeexplore.ieee.org/document/6135854

[5] Mohammed Abdul Qadeer,"Network Traffic Analysis and Intrusion Detection using Packet Sniffer" https://ieeexplore.ieee.org/document/5437681?arnumber=5437681

[6] Pimjai Navabud, Chin-Ling Chen," Analyzing the web mail using Wireshark" https://ieeexplore.ieee.org/document/8686871

[7] Arthur Callado, Djamel Sadok," A Survey on Internet Traffic Identification" https://ieeexplore.ieee.org/document/52087

[8] Fei YU, Yulei HUANG," An Overview of Study of Passowrd Cracking" https://ieeexplore.ieee.org/document/7371616