48730/32548, Cyber Security Lab 1, Part 1

Information Gathering and Extracting Unencrypted Data

The Tasks included in Lab – 1, Part 1 do not require VMware Workstation or VMware Fusion, Task 1 and Task 2 will require Wireshark. Wireshark is an open-source Packet analysing software. Wireshark can be downloaded from https://www.wireshark.org/download.html . Lab 1, Part 1 should be submitted along with Lab 1, Part 2 in Week 3 (refer to assignment section of the course on Canvas for the Due date). The assignment document should contain only questions from the lab manual, your answers and screenshots to support your answers.

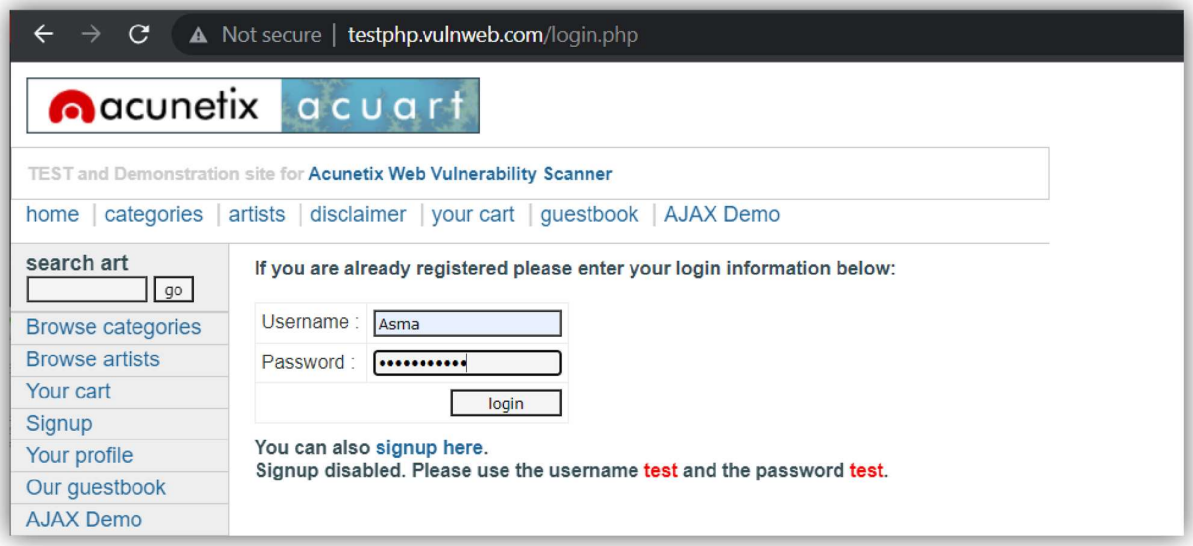
Task 1: Sniff Login details from unencrypted HTTP traffic:

Data transmitted through HTTP is vulnerable to interception by malicious actors, who can potentially eavesdrop on unencrypted packets and extract sensitive information such as images, login credentials, or personal data. Therefore, cybersecurity professionals employ specialised tools and methodologies, like packet sniffers, to analyse network traffic, identify potential security gaps, and implement robust encryption measures, safeguarding data integrity and preserving user privacy.

In this practical lab, you will acquire fundamental information gathering skills using Wireshark. Through the analysis of captured network packets, you'll explore the extraction of valuable data transmitted over unencrypted HTTP connections. This hands-on experience will equip you with essential tools to identify and understand potential security risks and vulnerabilities, enhancing your expertise in cybersecurity information analysis.

Step 1:

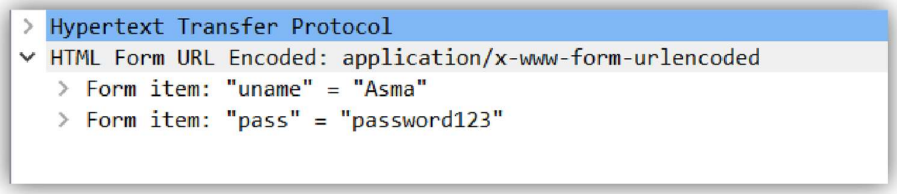
a. Open Wireshark and make sure that promiscuous mode is enabled on all interfaces.
b. Start the capturing of files.
c. Go to: http://testphp.vulnweb.com/login.php
d. Enter **your name** as the login username and enter a “password123” as the password. Make sure you hit the login button.



Step 2:

a. Utilise the search bar to locate the packet with the login information. [**Hint:** the packet will be using HTTP protocol and will start with POST].
b. In Wireshark, locate the login details which are the username and the password you have used for the unsecure website.

This will look like:



Hints:

Write frame contains "POST" in search bar of Wireshark to look for packet containing the login information.

Question:

a. Submit a screenshot of the username and password from Wireshark.

Task 2: Extract an image form unencrypted HTTP packet

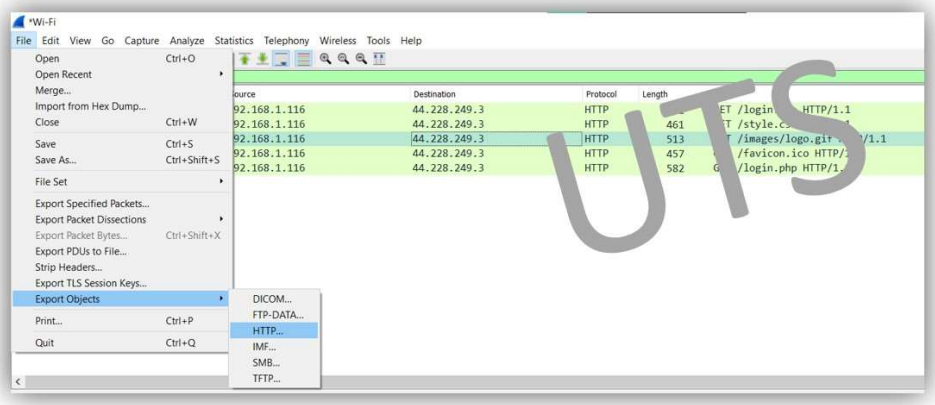
Wireshark and similar network sniffing tools, offers the ability to extract images from unencrypted packets transmitted via websites that use the HTTP protocol or other unencrypted protocols. This capability allows experts to identify potential vulnerabilities, assess data leakage risks, and bolster network security, strengthening overall digital

resilience and ensuring the protection of sensitive information effectively. In practice experts in industry use a number of tools to extract such information.

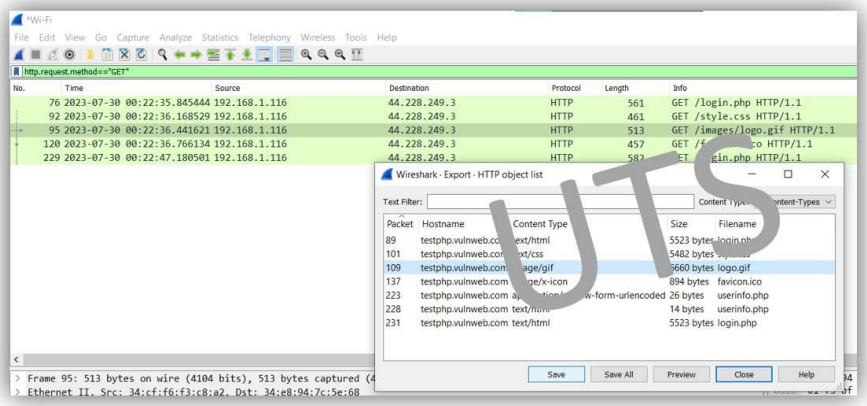
Steps:

You are tasked to extract the logo image of the same website (http://testphp.vulnweb.com/login.php) we have entered previously. Use the same packets captured from task 1.

a. Locate the GET packet that contains the logo.gif raw data. You may utilise the search bar similar to task 1.
b. Click on the packet with the image info, and go to file à Export Objects à HTTP…



c. Download the object that contains the logo.gif data.



Question:

a. Take a screenshot of the object of the image ‘logo.gif’ in the HTTP object list.

Task 3: Information Gathering

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities hat a malicious hacker could potentially exploit.

Passive information gathering

A lot of important information can be passively gathered and subsequently used in a direct attack or to reinforce other attacks targeted at an organization. Some Web Hosting service providers provide Website analysis that may pose a risk to security of an organization.

Active information gathering

Unlike passive information gathering, active information gathering collects the most updated and current data. The information collected in this manner can be influenced by various factors that include your current location, ISP, network constraints, etc. This information can be used to investigate the current state of the target.

Zenmap

Zenmap or Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. It is useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Read more at www.nmap.org

NetCraft

Netcraft is an internet services company providing internet security services, including antifraud and anti-phishing services, application testing, code reviews, and automated penetration testing. It also provides research data and analysis on many aspects of the internet. Netcraft has explored the internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the internet. Visit www.netcraft.com

Questions:

Using Zenmap and/or NetCraft to scan www.uts.edu.au. Gather and compare the information collected.

1. What is its Ip address?
2. Type the IP address in the browser to access the webpage, explain your observations.
3. Who is the IP owner?
4. What is the server's operating system?
5. What type of web server is being used?
6. What is its server-side scripting technology?
7. Can you find the email for the domain admin of this website for a possible phishing attack?
8. What is the 'Reverse DNS' for the website?
9. Who is the domain registrar?
10. What is nameserver organization?

11. What company is hosting the website?
12. Where is the hosting company geologically located?

Information gathering can be achieved using various open-source intelligence tools. A list of such possible tools can be found at: https://securitytrails.com/blog/osint-tools As always, use the tools within a controlled safe environment.