Imran Melikov 14/07/2024

Task2 Report

Web Open Source Intelligence (WebOSINT) focuses on gathering and analyzing publicly accessible data specifically from the web. It includes sources like websites, blogs, forums, and social media platforms. WebOSINT is widely used in cybersecurity, digital forensics, and market research. Ensuring ethical use and respecting privacy are crucial when conducting WebOSINT investigations.

Table of Contents

1.0 Future Intern Task2 Report

1.1 Introduction

The Offensive Security Lab and Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security course. This report should contain all items that were used to pass the overall exam and it will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

2.0 Executive Summary

Conducted penetration test uncovered several security weaknesses present in web applications owned by testphp.vulnweb.com website

When performing the penetration test, there were several alarming vulnerabilities that were identified on testphp.vulnweb.com networks. When performing the attacks, I was able to find different information, primarily due to outdated patches and poor security configurations.

2.1 Executive Summary - Recommendations

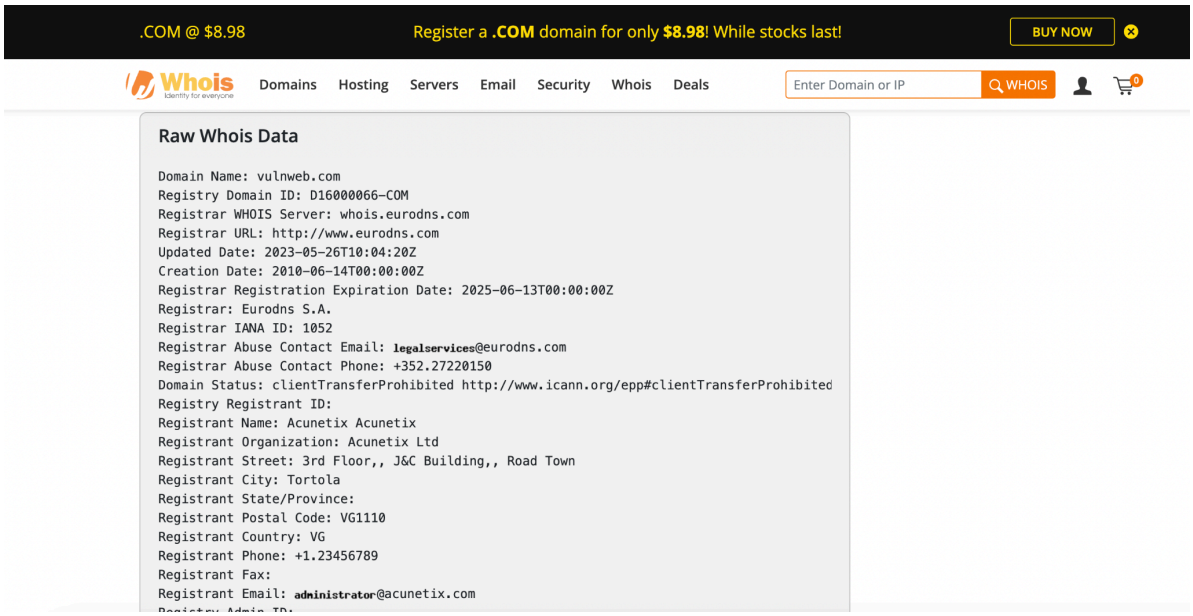
I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

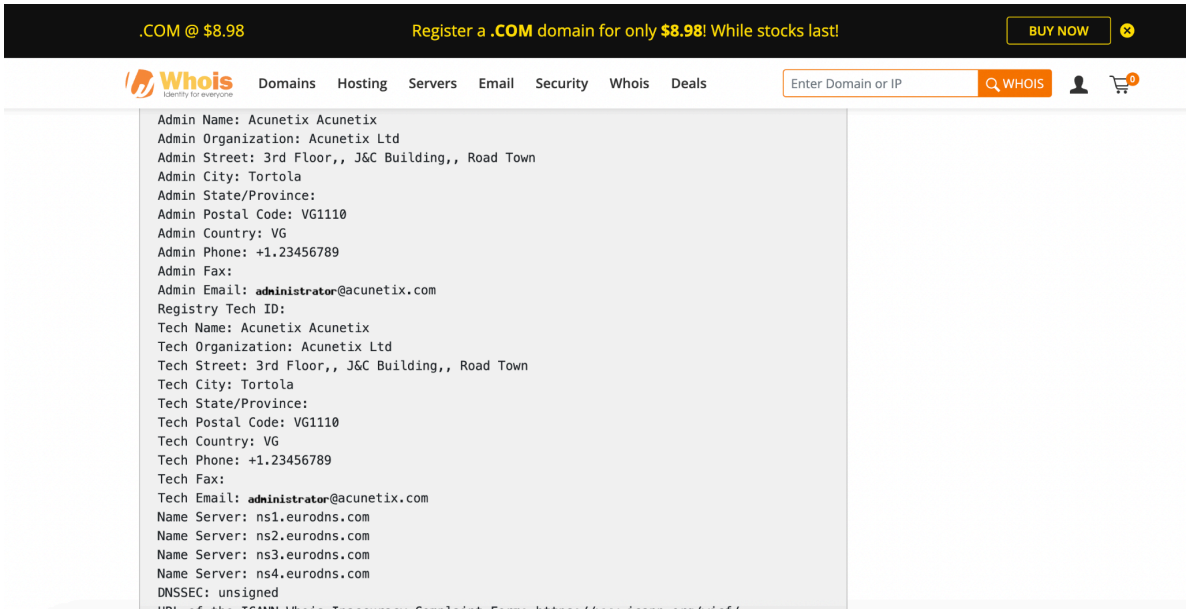
3.0 Information Gathering

We try to get information about testphp.vulnweb.com website.We use many tools and websites for this.

3.1.1 Whois Lookup

WHOIS lookup involves querying databases to obtain information about domain names and IP addresses. It provides details such as the registrant's name, contact information, registration dates, and domain status. This tool is essential for managing internet resources, ensuring security, and conducting digital investigations. Ethical use and privacy respect are vital when performing WHOIS lookups.We use Whois.com website to get information.

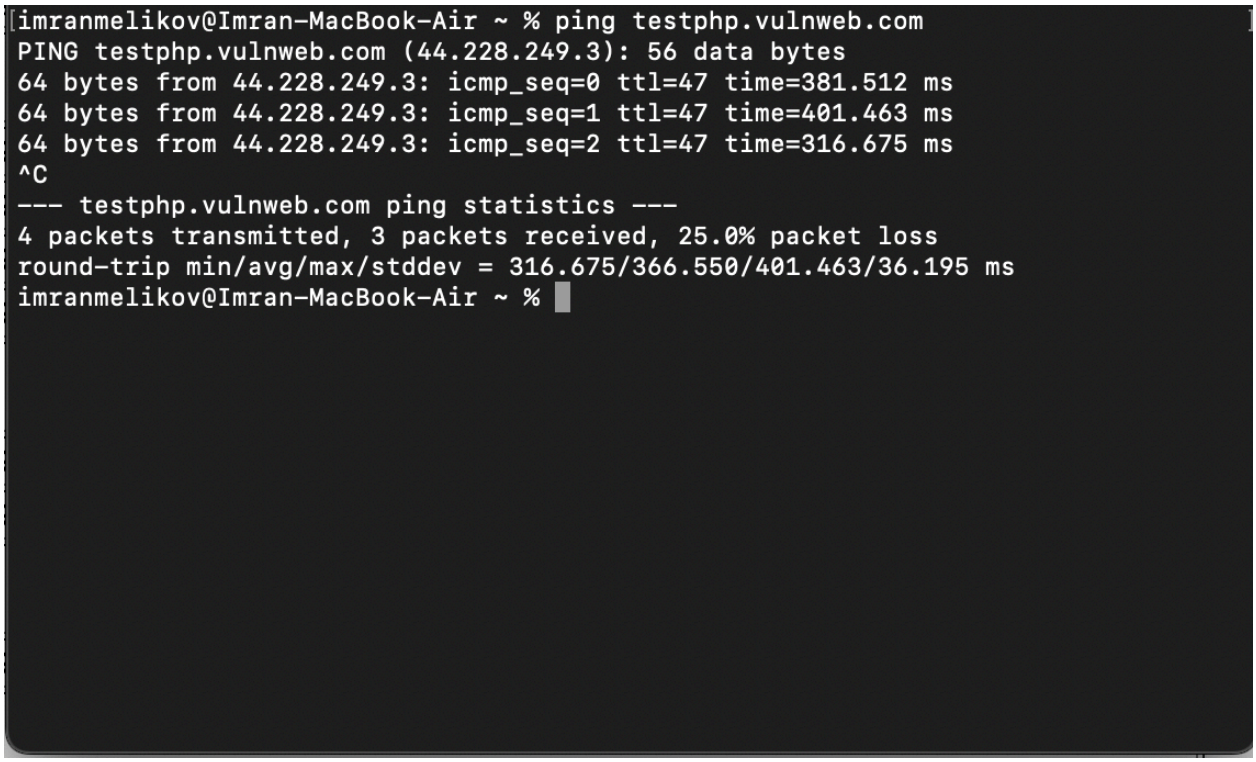




We can see company name,phone number,email,registrant name,country, name serves etc.

3.2.2 Ip address

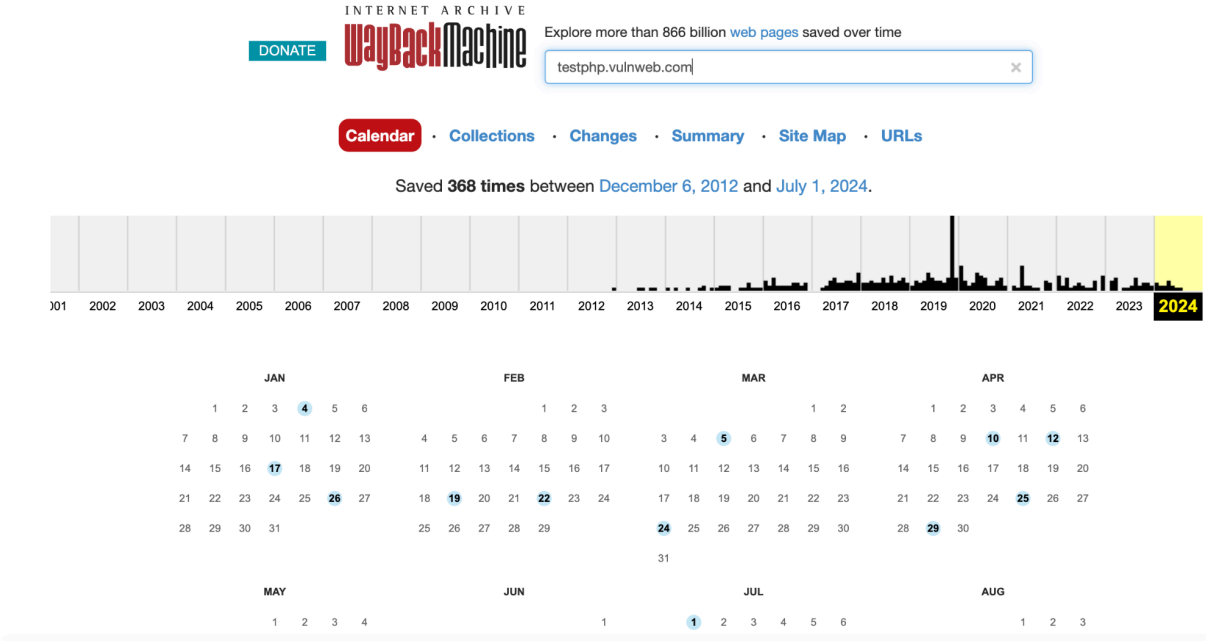
Ip address is the critical factor for websites because when we get an ip address we can scan the ip address with nmap or we can do other things.



We use the ping command to learn the ip address.After this if we want we can scan the ip address with nmap.Our target ip is 44.228.249.3.

3.3.3 Archive.org

Archive.org, also known as the Internet Archive, is a digital library that provides free access to a vast collection of digital content. It includes websites, books, audio recordings, videos, and software. The Wayback Machine, a prominent feature, allows users to view archived versions of web pages across different times. Archive.org supports research, historical preservation, and access to cultural artifacts.We can see last snapshots about the target.


INTERNET ARCHIVE
DONATE
WayBackMachine
Explore more than 866 billion web pages saved over time
testphp.vulnweb.com
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 368 times between December 6, 2012 and July 1, 2024.
2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG