CYBER SECURITY INDEX

COMPANY SEC

Date: Wed Dec 09

POWERED BY

CMKL UNIVERSITY

i

TABLE OF CONTENTS

- Executive Summary 01
- Scope 01
- Results 02
- Methodology 03
- Findings 04
  - Severity assessments summary 04
  - Reconnaissance 05
  - Exploitation 06

01 /EXECUTTIVE SUMMARY

EXECUTIVE SUMMARY

Cyber Security Index powered by CMKL is a conducted service where a black-box perspective security assessment, to detect the current vulnerabilities found in the given endpoints and show the level of the current vulnerability severity levels. Our project's purposes are for the company to be able to continuously access our service for continuous improvement for the company's security system and gain reputation.

To achieve our goal, we must investigate the vulnerability of our client system's company. Of the 0 sub-domains identified. A total of 0 unique vulnerabilities were found. The scan inspected the opened 2 TCP ports and 0 UDP ports.

The following table is the summary of the overall severity test performed on the given endpoints.

Vulnerabilities severity	Unique Count
Critical severity	0
High severity	0
Medium severity	0
Low severity	0

Scan Information

Start Time: Wed Dec 09 14:47:52 +0700

Finish Time: Wed Dec 09 15:01:08 +0700

Scan Duration: 13 minutes 16 seconds

The furthermore details are included on the "finding pages" and in-depth details on the "details pages"

02 SCOPE

Scope

This test scope is engaged on only a black-box perspective(zero-knowledge) with a blind security assessment test on the network area. Testing was performed on Wed Dec 09 with industry-standard tools and frameworks, including DNSmap, Nmap, Drib, and Argo.

END POINTS
cswww-qa.zcomsec.com
csapi-qa.zcomsec.com

03 METHLOGY

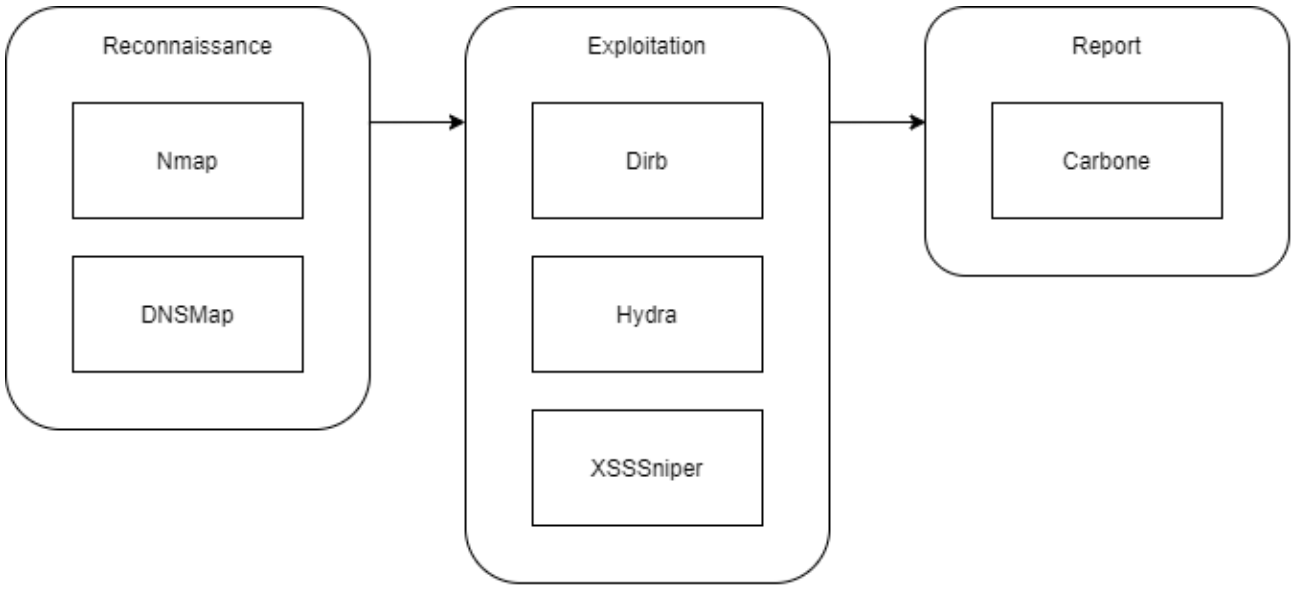
METHODOLOGY

As the starting point, the black-box or blinded scan was performed on the provided target server with following these steps:

1) Reconnaissance
2) Exploitation

Retrieve information from it by using Nmap, for protocols, and DNSMap, for the subdomain. Exploitation or search vulnerabilities in the system including find directory, brute force list of usernames and passwords.

.



04 FINDINGS

FINDINGS

IP Address	Hostname	Protocol / Port
150.95.79.133	cswww-qa.zcomsec.com	TCP//SSL/HTTP/22
150.95.79.134	csapi-qa.zcomsec.com	TCP//SSL/HTTP/22

Severity assessments summary

This table below expresses every sub-domains and IPs that were scanned and defined along with founding severity in each of them, classified as critical, high, medium, and low severity.

IP Address	Hostname	Critical Severity	High Severity	Medium Severity	Low Severity
150.95.79.133	cswww-qa.zcomsec.com	-	-	-	-
150.95.79.134	csapi-qa.zcomsec.com	-	-	-	-