CYBER SECURITY INDEX

POWERED BY

CMKL UNIVERSITY

TABLE OF CONTENTS

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 unique vulnerabilities were found. The scan inspected the opened 0 port(s).

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

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

Scan Information

Start Time:

Finish Time:

Scan Duration:

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

02 SCOPE

Scope

END POINTS

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 with industry-standard tools and frameworks, including DNSmap, Nmap, Drib, and Argo.

03 METHLOGY

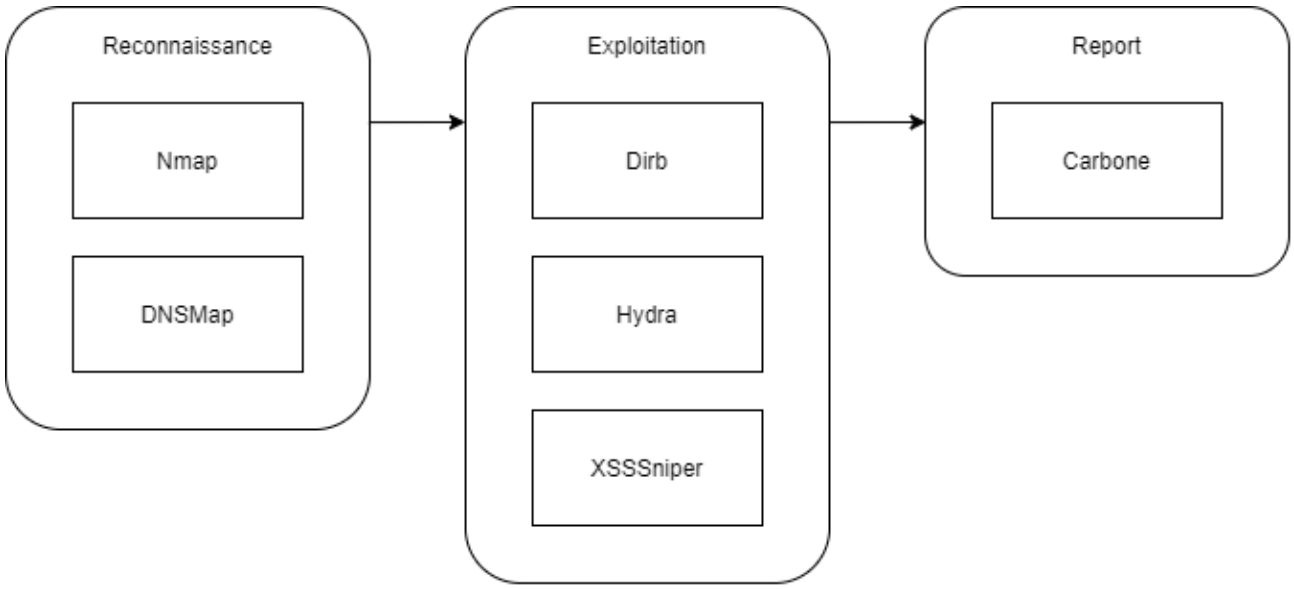
METHODOLOGY

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
3) Report

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

Port and Protocol Found

IP Address	Hostname	Protocol / Port
159.203.96.214		ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211
165.227.186.93		ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211
159.203.96.214		ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211
165.227.186.93		ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211

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
4	4	-	-	-	-
4					

05 /FINDINGS

FINDINGS

Path Found

URL BASE: 5
TOTAL NUMBER OF PATHS: 5

PATH	HTTP RESPONSE	RESPONSE DEFINITION
5	5	5
5		

URL BASE: 5