

## TASK - 5

# **NETWORK SCANNING**

By: Mearaj Sadhikunnisa

## **TABLE OF CONTENTS:**

01) EXECUTIVE SUMMARY

A) Findings

B) Risk Distribution

C) Methodology

02) Determination the scope

03) Information Gathering

04) Scanning

05) Risk

## Executive Summary


### Findings:

The risks found are just the info of the threats which can be fixed upon when better nodes are used to transmit signals and for storing data.

Vulnerability testing of a website involves identifying potential security weaknesses in the web application, network, and operating system. The findings of vulnerability testing can vary depending on the scope of the testing and the tools and techniques used.

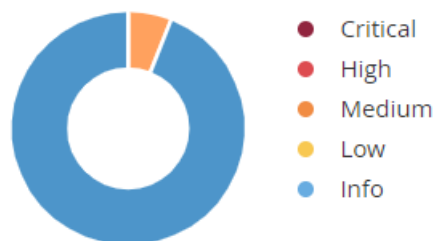
#### Scan Details

---

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0 
Scanner:	Local Scanner
Start:	Today at 5:48 PM
End:	Today at 6:00 PM
Elapsed:	12 minutes

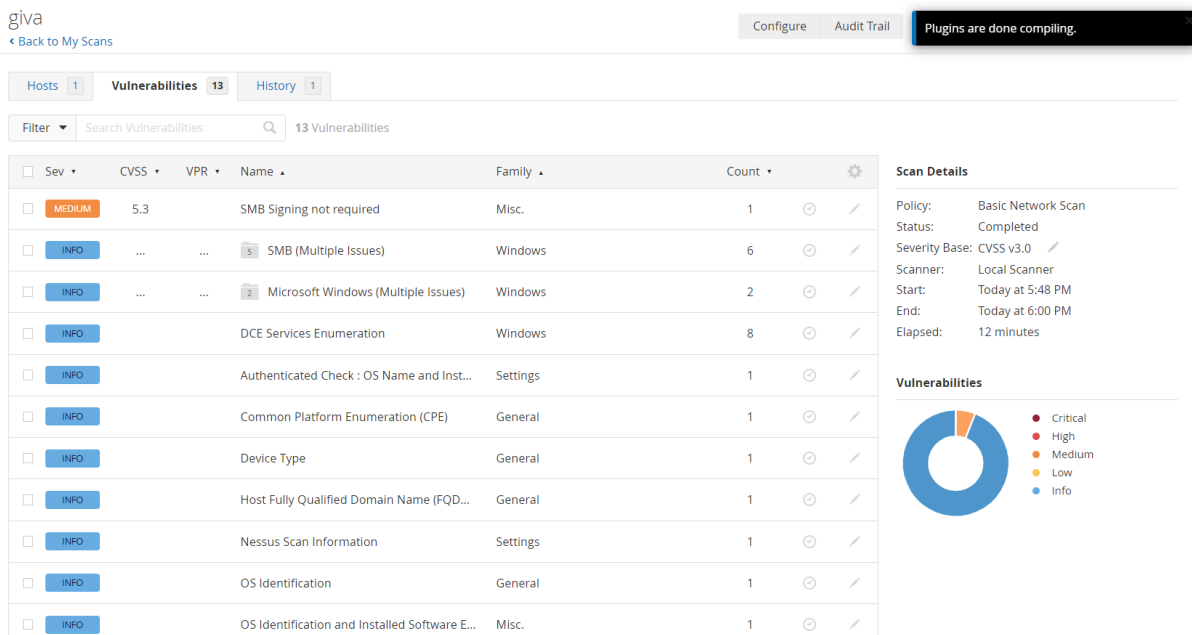
#### Vulnerabilities

---



However, some common findings in vulnerability testing of a website may include:

- Injection flaws: Vulnerabilities that allow attackers to inject malicious code or commands into a website's database or operating system.
- Cross-site scripting (XSS) vulnerabilities: These vulnerabilities allow attackers to inject malicious scripts into a web page viewed by other users.
- Cross-site request forgery (CSRF) vulnerabilities: These vulnerabilities allow attackers to trick users into unknowingly executing unwanted actions on a website, such as changing their password or making a purchase.
- Broken authentication and session management: These vulnerabilities may allow attackers to gain unauthorized access to user accounts or sensitive information by exploiting weak or insecure login mechanisms.
- Information leakage: This refers to the unintentional disclosure of sensitive information through error messages, server headers, or other means.
- Insufficient authorization checks: These vulnerabilities allow attackers to access or modify sensitive information or functionality without proper authorization.
- Insecure communication: This refers to the use of insecure protocols or encryption algorithms that can be exploited by attackers to intercept or modify sensitive data in transit.



It's important to note that the severity and impact of these vulnerabilities can vary widely depending on the specific website, its functionality, and the data it handles. It's recommended to work with a professional security team to conduct vulnerability testing and address any identified issues.

## DETERMINING THE SCOPE:

Determination of scope is a critical aspect of any project planning, and it is no different for a vulnerability testing project. The scope of a vulnerability testing project should be defined based on the goals and objectives of the testing, the budget, the time frame, and the resources available.

Domain Name: GIVA.COM

Registry Domain ID: 5053200\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: https://www.godaddy.com

Updated Date: 2021-08-03T07:59:04Z

Creation Date: 1999-04-06T23:00:00Z

Registrar Registration Expiration Date: 2025-04-06T23:00:00Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146  
Registrar Abuse Contact Email: abuse@godaddy.com  
Registrar Abuse Contact Phone: +1.4806242505  
Domain Status: clientTransferProhibited  
<https://icann.org/epp#clientTransferProhibited>  
Domain Status: clientUpdateProhibited  
<https://icann.org/epp#clientUpdateProhibited>  
Domain Status: clientRenewProhibited  
<https://icann.org/epp#clientRenewProhibited>  
Domain Status: clientDeleteProhibited  
<https://icann.org/epp#clientDeleteProhibited>  
Registry Registrant ID: Not Available From Registry  
Registrant Name: Registration Private  
Registrant Organization: Domains By Proxy, LLC  
Registrant Street: DomainsByProxy.com  
Registrant Street: 2155 E Warner Rd  
Registrant City: Tempe  
Registrant State/Province: Arizona  
Registrant Postal Code: 85284  
Registrant Country: US  
Registrant Phone: +1.4806242599  
Registrant Phone Ext:  
Registrant Fax: +1.4806242598  
Registrant Fax Ext:  
Registrant Email: Select Contact Domain Holder link at  
<https://www.godaddy.com/whois/results.aspx?domain=GIVA.COM>  
Registry Admin ID: Not Available From Registry  
Admin Name: Registration Private  
Admin Organization: Domains By Proxy, LLC  
Admin Street: DomainsByProxy.com  
Admin Street: 2155 E Warner Rd  
Admin City: Tempe  
Admin State/Province: Arizona  
Admin Postal Code: 85284  
Admin Country: US  
Admin Phone: +1.4806242599

Admin Phone Ext:

Admin Fax: +1.4806242598

Admin Fax Ext:

Admin Email: Select Contact Domain Holder link at

<https://www.godaddy.com/whois/results.aspx?domain=GIVA.COM>

Registry Tech ID: Not Available From Registry

Tech Name: Registration Private

Tech Organization: Domains By Proxy, LLC

Tech Street: DomainsByProxy.com

Tech Street: 2155 E Warner Rd

Tech City: Tempe

Tech State/Province: Arizona

Tech Postal Code: 85284

Tech Country: US

Tech Phone: +1.4806242599

Tech Phone Ext:

Tech Fax: +1.4806242598

Tech Fax Ext:

Tech Email: Select Contact Domain Holder link at

<https://www.godaddy.com/whois/results.aspx?domain=GIVA.COM>

Name Server: NS1.DAN.COM

Name Server: NS2.DAN.COM

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System:

<http://wdprs.internic.net/>

>>> Last update of WHOIS database: 2023-05-02T13:34:02Z

<<<

For more information on Whois status codes, please visit

<https://icann.org/epp>

**TERMS OF USE:** The data contained in this registrar's Whois database, while believed by the registrar to be reliable, is provided "as is" with no guarantee or warranties regarding its accuracy. This information is provided for the sole purpose of assisting you in obtaining information about domain name registration records. Any use of this data for any other purpose

is expressly forbidden without the prior written permission of this registrar. By submitting an inquiry, you agree to these terms and limitations of warranty. In particular, you agree not to use this data to allow, enable, or otherwise support the dissemination or collection of this data, in part or in its entirety, for any purpose, such as transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations of any kind, including spam. You further agree not to use this data to enable high volume, automated or robotic electronic processes designed to collect or compile this data for any purpose, including mining this data for your own personal or commercial purposes. Failure to comply with these terms may result in termination of access to the Whois database. These terms may be subject to modification at any time without notice.

### Whois lookup from mxlookup

if you want to perform a Whois lookup, you need to use a tool specifically designed for that purpose, such as "whois.net" or "whois.icann.org". These tools will allow you to enter a domain name and retrieve the associated domain information from the Whois database.

If you want to perform an MX lookup, you can use a DNS lookup tool such as "mxtoolbox.com" or "dnschecker.org". These tools allow



SuperTool

Beta7

MX Lookup

mx:giva.co

Find Problems

Solve Email Delivery Problems

mx

**ARE YOU CONFIDENT** that your email is getting through? **FIND OUT WITH DELIVERY CENTER**

Pref	Hostname	IP Address	TTL		
1	aspmx.l.google.com	142.251.163.27 <small>Google LLC (AS15169)</small>	60 min	Blacklist Check	SMTP Test
1	aspmx.l.google.com	2607:f8b0:4004:c17::1b	60 min	Blacklist Check	
5	alt1.aspmx.l.google.com	209.85.202.26 <small>Google LLC (AS15169)</small>	60 min	Blacklist Check	SMTP Test
5	alt1.aspmx.l.google.com	2a00:1450:400b:c00::1a	60 min	Blacklist Check	
5	alt2.aspmx.l.google.com	64.233.184.27 <small>Google LLC (AS15169)</small>	60 min	Blacklist Check	SMTP Test
5	alt2.aspmx.l.google.com	2a00:1450:400c:c0b::1a	60 min	Blacklist Check	
10	alt3.aspmx.l.googlemail.com	{No A Record}	60 min	Blacklist Check	SMTP Test
10	alt4.aspmx.l.googlemail.com	{No A Record}	60 min	Blacklist Check	SMTP Test
12	smtp.secureserver.net	216.69.141.81 <small>GoDaddy.com, LLC (AS398101)</small>	60 min	Blacklist Check	SMTP Test
20	mailstore1.secureserver.net	216.69.141.82 <small>GoDaddy.com, LLC (AS398101)</small>	60 min	Blacklist Check	SMTP Test

## Ip address and domains:

A domain name is a human-readable name used to identify a website or other internet resource. It is typically composed of two or more parts separated by dots, such as "example.com". The rightmost part of the domain name is called the top-level domain (TLD), such as ".com" or ".org". Domain names are registered with domain registrars and assigned to specific IP addresses.

S. No.	Domain Name	IP Address
1	www.giva.co	shops.myshopify.com./23.227.38.74

## NMAP SCAN

Starting Nmap 7.40 (<https://nmap.org> ) at 2023-04-26 17:52 UTC

Nmap scan report for 163.53.76.86

Host is up (0.20s latency).

### PORT STATE SERVICE

21/tcp filtered ftp

22/tcp filtered ssh

23/tcp filtered telnet

80/tcp open http

110/tcp filtered pop3

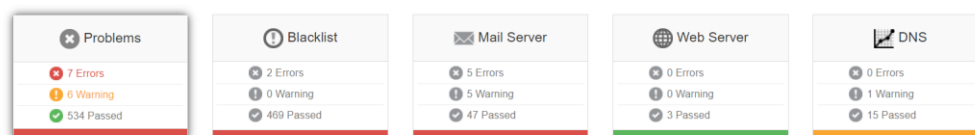
143/tcp filtered imap

443/tcp open https

3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds.

## RISK:



13 Problems			
Category	Host	Result	
✖ smtp	alt4.aspmx.l.googlemail.com	Failed To Connect	<a href="#">More Info</a>
✖ smtp	alt4.aspmx.l.googlemail.com	Problem getting IP Address for alt4.aspmx.l.googlemail.com	<a href="#">More Info</a>
✖ smtp	alt3.aspmx.l.googlemail.com	Failed To Connect	<a href="#">More Info</a>
✖ smtp	alt3.aspmx.l.googlemail.com	Problem getting IP Address for alt3.aspmx.l.googlemail.com	<a href="#">More Info</a>
✖ spf	giva.co	A null DNS lookup was found for include (_spf.unifiedrml.com)	<a href="#">More Info</a>
✖ blacklist	mailstore1.secureserver.net	Blacklisted by UCEPROTECTL3	<a href="#">More Info</a>
✖ blacklist	smtp.secureserver.net	Blacklisted by UCEPROTECTL3	<a href="#">More Info</a>
⚠️ dmarc	giva.co	DMARC Quarantine/Reject policy not enabled	<a href="#">More Info</a>
⚠️ smtp	aspmx.l.google.com	Reverse DNS does not match SMTP Banner	<a href="#">More Info</a>
⚠️ smtp	alt2.aspmx.l.google.com	Reverse DNS does not match SMTP Banner	<a href="#">More Info</a>
⚠️ mx	giva.co	DMARC Quarantine/Reject policy not enabled	<a href="#">More Info</a>
⚠️ dns	giva.co	SOA Expire Value out of recommended range	<a href="#">More Info</a>

This is the overall health check of the domain flipkart.com. As we can see there is an errors and warnings in DNS and Mail server has 5 warnings.