**PROJECT 1: ANALYZING VULNERABILITY**

**AND IDENTIFYING ATTACKS**

**TARGET: MITHIBAI.AC.IN**

**Information Gathering:**

-Google Based Information Gathering

-Other Search based Information Gathering

-System Based Information gathering

-Browser Adon/ Extension Based Information Gathering

-Social Media Based Information gathering

-Software Based Information Gathering

-OS based Informatiopn Gathering

**Google:-**

-Understaning the Database Architecture

- Understaning the Google Data Base

-Importance of Keywords

-Google results

-Google Dorks

-Bug Submission

-Other Google related products

**To Identify that Directories are Exposed:**

**Use the Command :**

**Type the Command in Google.com**

Indexof site:<site name>

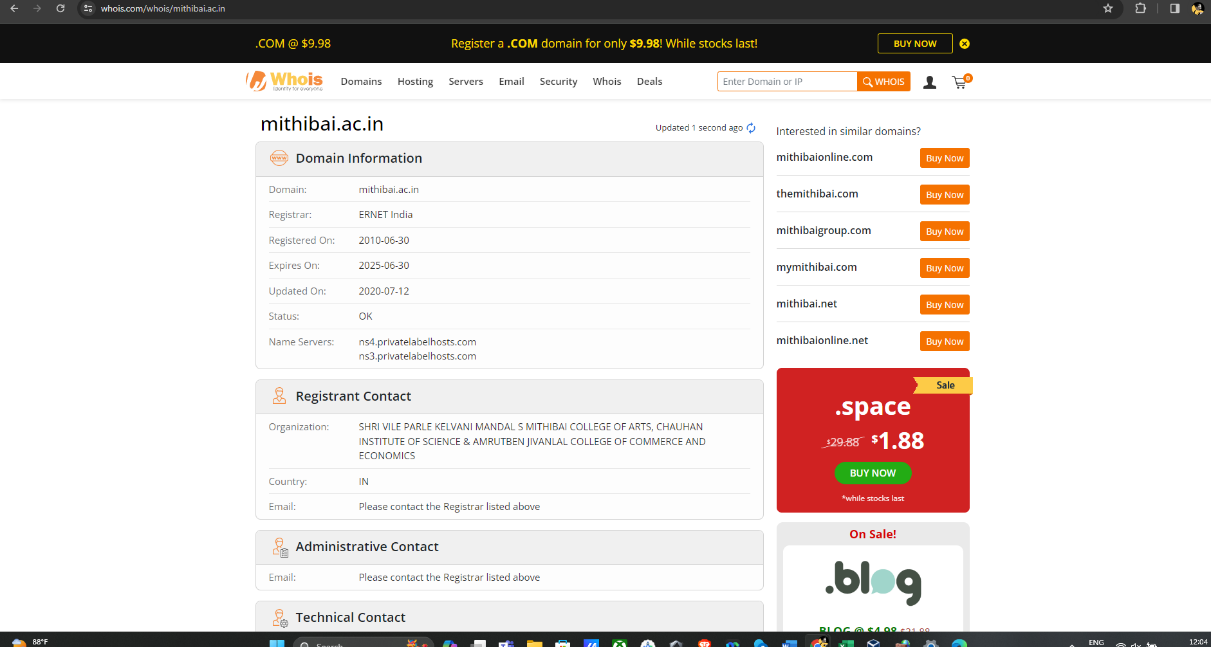
**Target Website:** mithibai.ac.in

**INFORMATION GATHERING:**

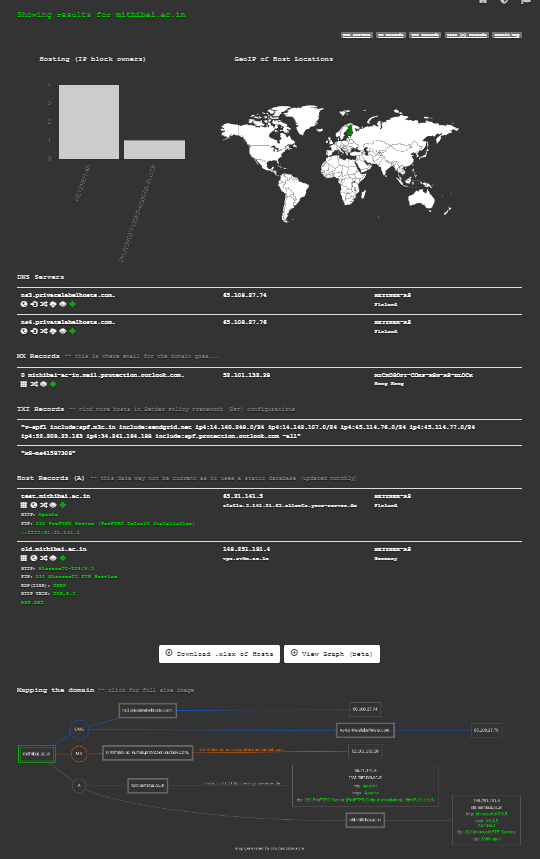
It is first phase in ethical Hacking in which the valuable Informations are need to be gain from the website or Tools we used in Kali

Sites Used for Information Gathering:

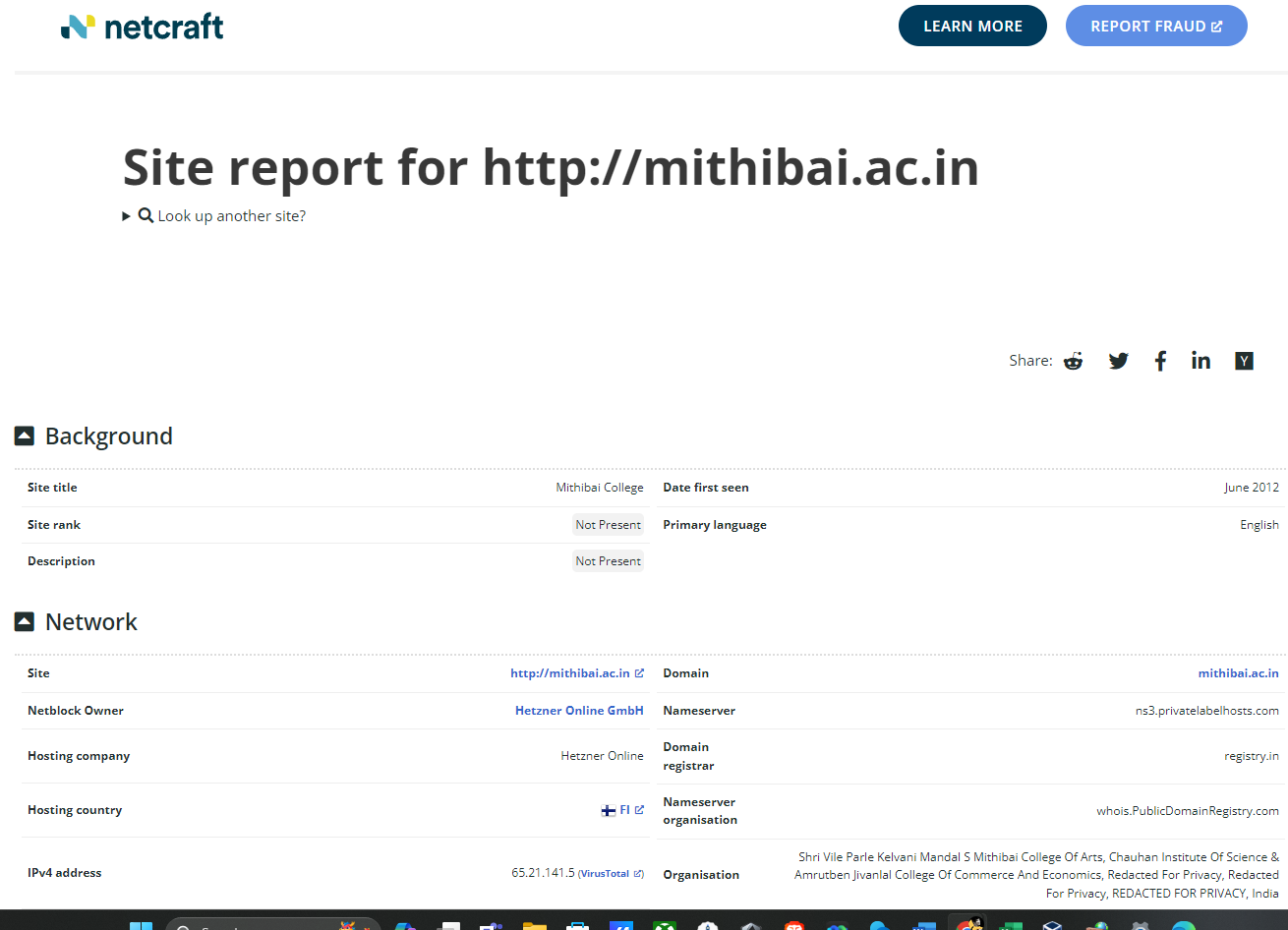
-Whoislookup.com



-dnsdumpster.org

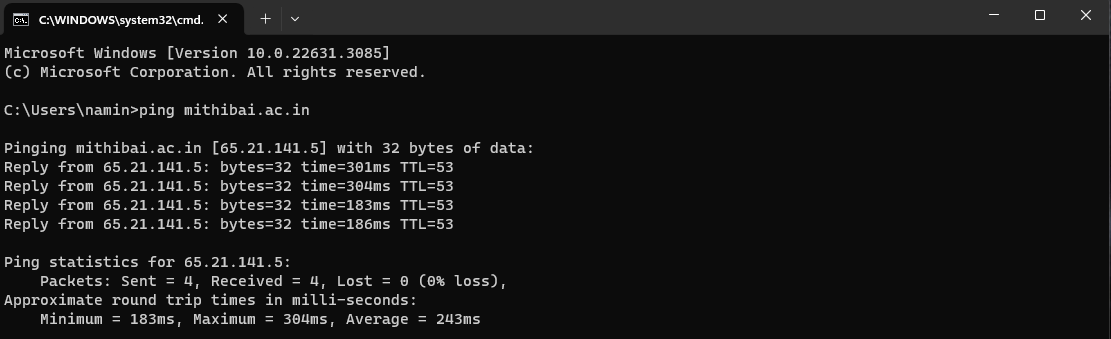


-sitereport.netcraft.com

`

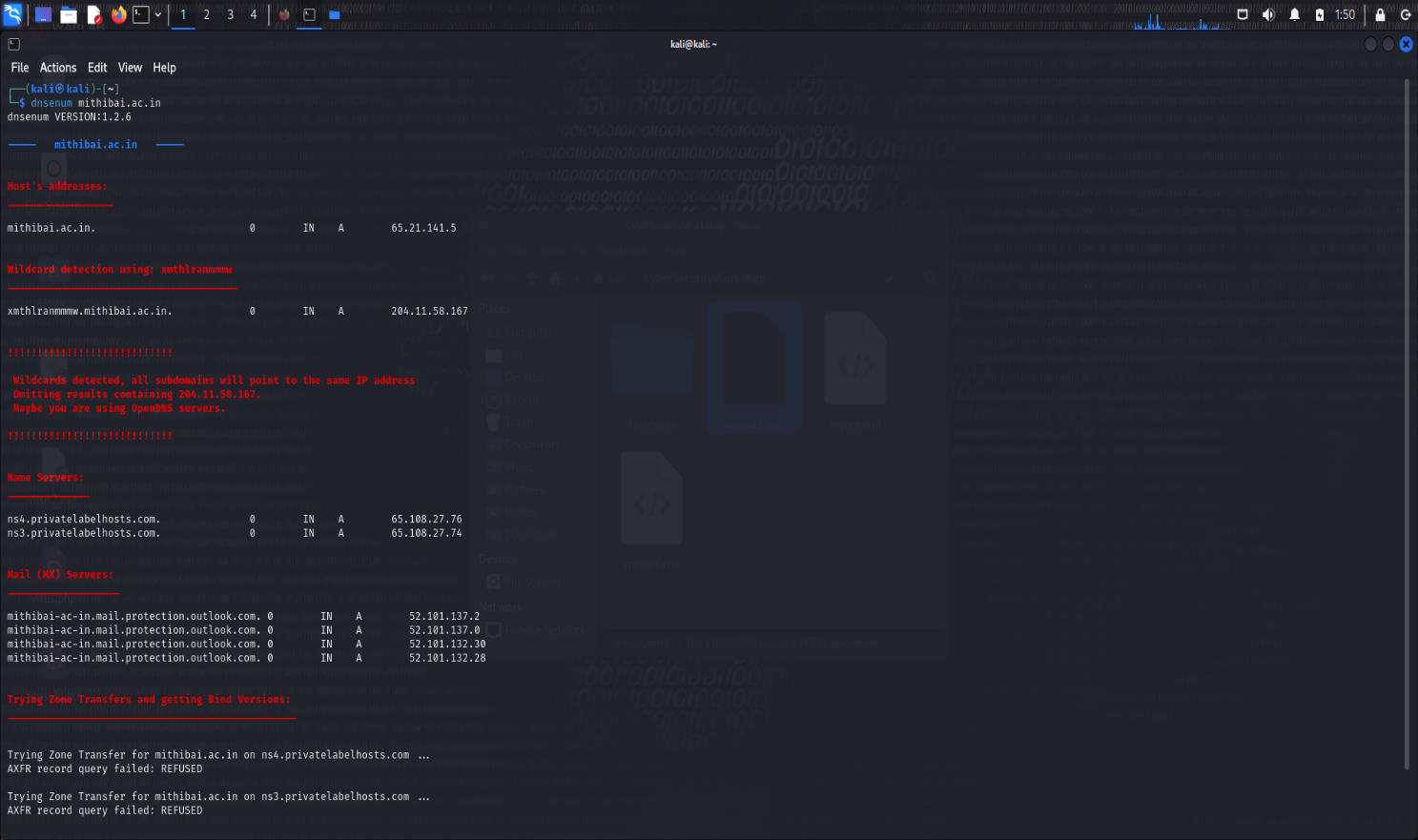
IP Gathering:

- Use of ping Command



-Use Of Nslookup



**OS Based Information Gathering: DNS ENUM**

**SCANNING:**

NMAP [Network MAPper] is a tool used for scanning the site

**NAMP COMMANDS:**

-sT

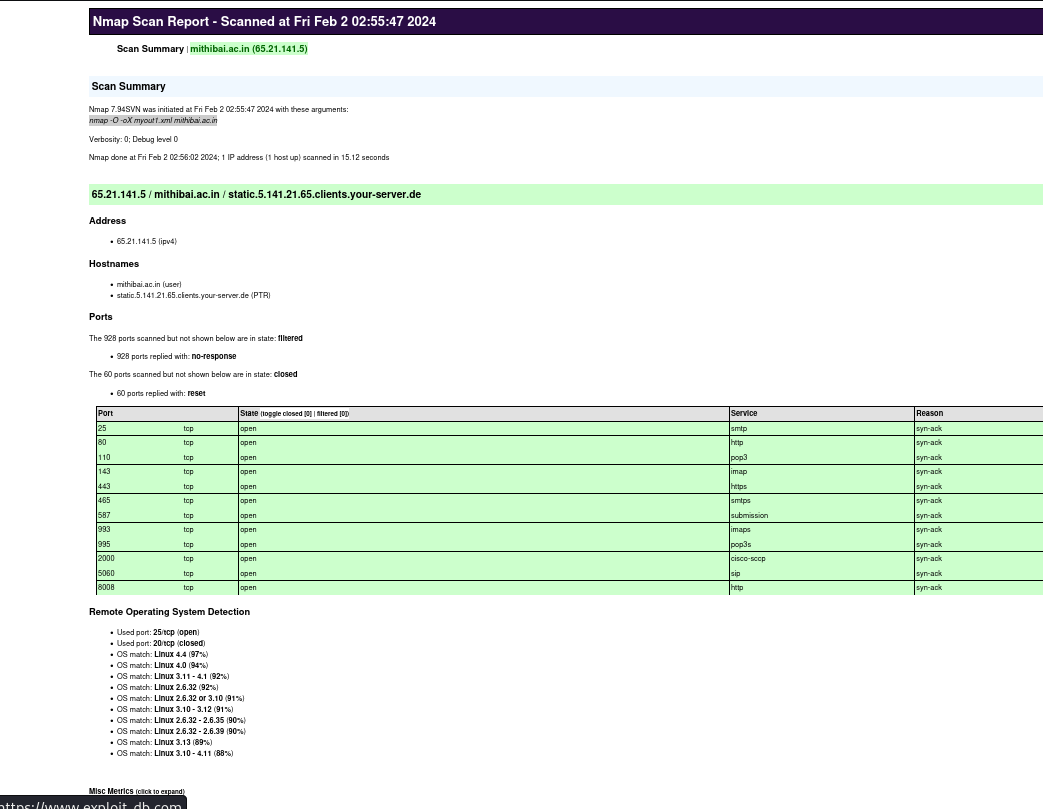
-sS

-A

-V

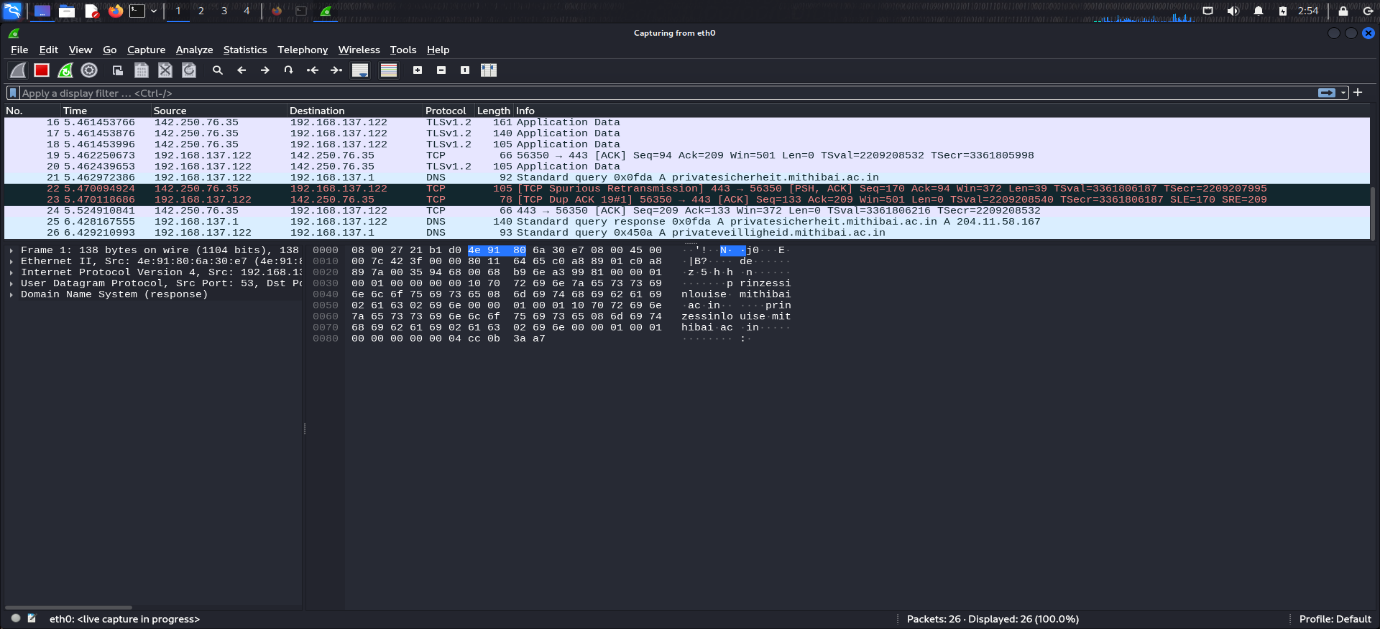
-O

**NMAP Final Report:**

****

**WIRESHARK:**

Here we use the WireShark Tool for vulnerability Analysis in which it analyse the Network Traffic and Vulnerable port



**VULNERABILITY ANALYSIS:**

A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage.

**Tools Used:**

**Website Based Tools**: [www.sitecheck.scuri.net](http://www.sitecheck.scuri.net), immuniweb.com

**OS based Tools:** Nikto, rapidscan

**EXPLOITATION:**

This is the actual attacking phase in which attacking takes place in this phase we are attack our Target/Victim through this phase

**Tools Used:**

-MSF(MetaSploit Frmaework)

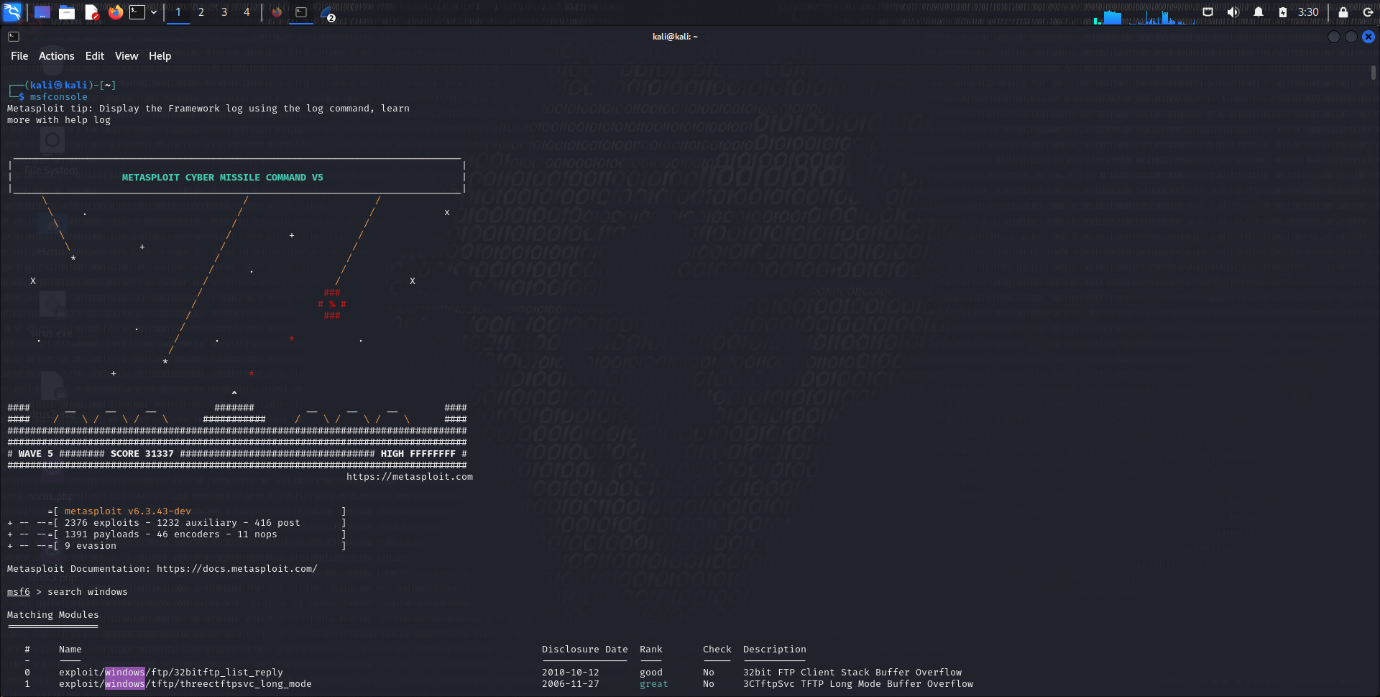
-Armitage GUI

-MSFVENOM

-Ettercap

-FOCA

**MSF(MetaSploit Framework):**

****

**MAINTAINING ACCESS:**

Maintaining Access is a process of Saving the Entire Targets Attack within ourself that we can be access anytime as we want. Maintaining Access is to keep our virus/malware in our targeted system in which give us the access to use the victims

**CLEARING TRACKS:**

Clearing Tracks is a way to Remove all the Records that attack our victim which is for avoiding tracking/tracing processes from the victim side

**FINAL TARGET REPORT:**

|  |  |
| --- | --- |
| **Column1** | **Column2** |
| Target | <https://mithibai.ac.in/> |
| TARGET STATUS | ACTIVE |
| Directories are Exposed | YES |
| robots.txt | YES |
| PING COMMAND | REPLYING |
| SECURITY TECHNOLOGIES OR FIREWALL | YES |
| DNS Server | BBK.mshome.net |
| DNS IP | 192.168.137.1 |
| DOMAIN CREATED DATE | 2010-06-30T03:56:34Z |
| DOMAIN EXPIRY | 2025-06-30T03:56:34Z |
| REGISTRAR DETAILS | ERNET India |
| SERVER LOCATION | FI |
| WEBADMIN EMAIL | [web-xls@awareindia.com](mailto:web-xls@awareindia.com) |
| DNS SERVER DETAIL | Microsoft-IIS/8.5 |
| CONTENT MANAGEMENT SYSTEM | PLESK, WORDPRESS |
| TYPE OF OS USED | Windows Server 2012 |
| EMAIL PROVIDER | registry.in |
| SUBDOMAINS | test.mithibai.ac.in |
| HOSTING COMPANY | Hetzner Online |
| HOSTING COUNTRY | IN, FI |
| SITE TECHNOLOGY | PHP |
| VULNERABLE FOR ZONE TRANSFER ATTACK | NO |
| LOAD BALANCE DETECTOR | DNS-NO, HTTP-YES |
| MALTIGO INFORMATION | Maltigo.domain: spf.protection.outlook.com , USAGE OF NETBLOCK maltego.NSRecord: ns4.privatelabelhosts.com, NEW IP: 52.209.23.163 |
| OPEN PORTS | 25/tcp open smtp 80/tcp open http 110/tcp open pop3 143/tcp open imap 443/tcp open https 465/tcp open smtps 587/tcp open submission 993/tcp open imaps 995/tcp open pop3s 2000/tcp open cisco-sccp 5060/tcp open sip 8008/tcp open http |
| VERSION DETAILS | 80/tcp open http Apache httpd 110/tcp open pop3 Dovecot pop3d 143/tcp open imap Dovecot imapd 443/tcp open ssl/http Apache httpd 465/tcp open ssl/smtp Exim smtpd 4.96.2 587/tcp open smtp Exim smtpd 4.96.2 |
| OS DETAILS | Linux 4.4 (97%) |
| PROTECTION | NO FIREWALL DETECTED, NO WEBSITE MONITORING DETECTED |
| SECURITY LEVEL | Medium Security Risk |
| MALICIOUS FILE | NO |
| SUSPICIOUS FILES | YES |
| VULNERABLE URL | NO |
| SPF |  |
|  |  |
|  |  |

**CONCLUSION:**

The Final Conclusion Of the Project is The Bugs were reported to the targeted site for their concerns legally.

\*\*\*\*\*\*\* THANK YOU \*\*\*\*\*\*