

**UNIVERSITY INSTITUTE OF ENGINEERING**

**Department of Computer Science & Engineering**

**Subject Name:** WEB AND MOBILE SECURITY LAB

**Subject Code:** 20CSP-338

**Submitted to: Submitted by:**

Er. Mandeep Kaur Name: Ruchika Raj

UID: 20BCS9285

Section: 20BCS615

Group: B

# Experiment-2.2

**Student Name: Ruchika Raj UID: 20BCS9285**

**Branch: BE-CSE Section/Group:20BCS\_WM\_615-B**

**Semester: FIFTH Date of Performance: 17/10/22**

**Subject Name: WMS LAB**

**Aim:** Perform Penetration testing on a web application to gather Information about the system (Foot Printing).

**Objective:** To perform penetration testing and foot printing on any Web Application.

**Software/Hardware Requirements:** Kali Linux, D-tech tools or any pen Testing tools and any platform using Python 2.7 Tools to be used:

1. D-Tech
2. NMAP
3. Metasploit
4. Wire Shark

**Introduction:**

**Footprinting** means gathering information about a target system that can be used to execute a successful cyber-attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system.

**Different kinds of information that can be gathered from Footprinting are as follows:**

* The operating system of the target machine
* Firewall
* IP address
* Network map
* Security configurations of the target machine
* Email id, password
* Server configurations
* URLs
* VPN

**Sources**

**Using Neo Trace:** Neo Trace is a powerful tool for getting path information. The graphical display displays the route between you and the remote site, including all intermediate nodes and their information. Neo Trace is a well-known GUI route tracer program. **Along with a graphical route, it also displays information on each node such as IP address, contact information, and location.**

**Steps:**

**Website Footprinting: website mirroring**

1. Go to google and open HtTrack link and download first link.
2. Install this tool and put URL of any demo website to copy the website.

1. To check the detail coding and web pages of copied website just go to the location where this tool is installed.

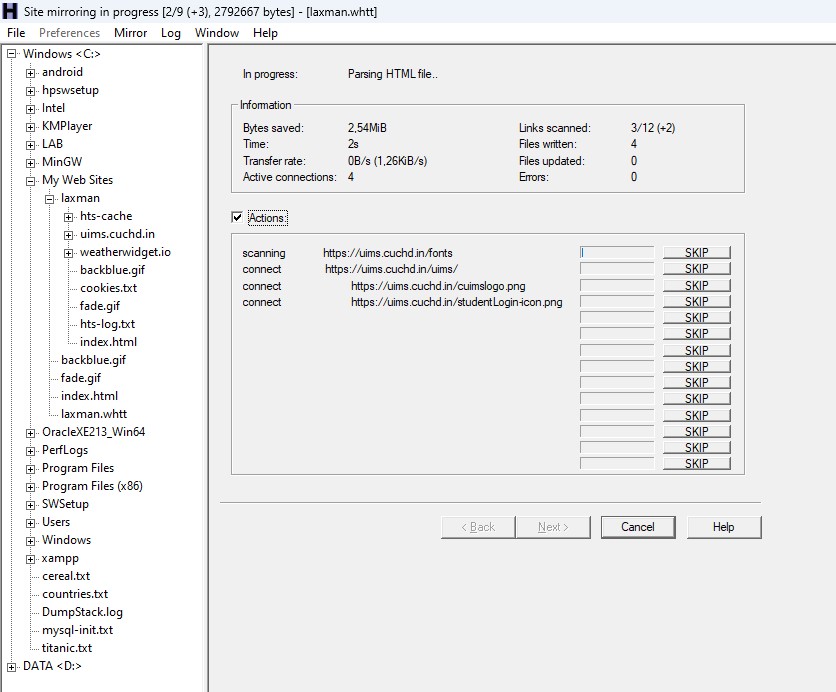
**Email Foot printing:**

* 1. Open any spam mail
  2. Click on three dots and click on show original. Search “received from” on page and copy ip address
  3. Open a website ultratools.com or Whois Ip Lookup and paste ip address there.
  4. You can track all information there.

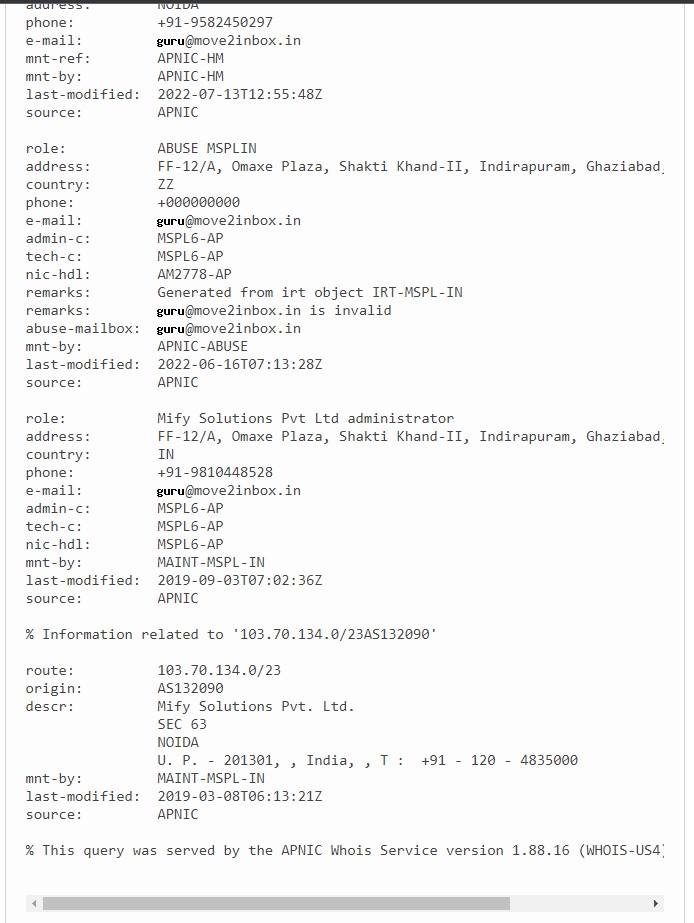
**Network Foot printing:**

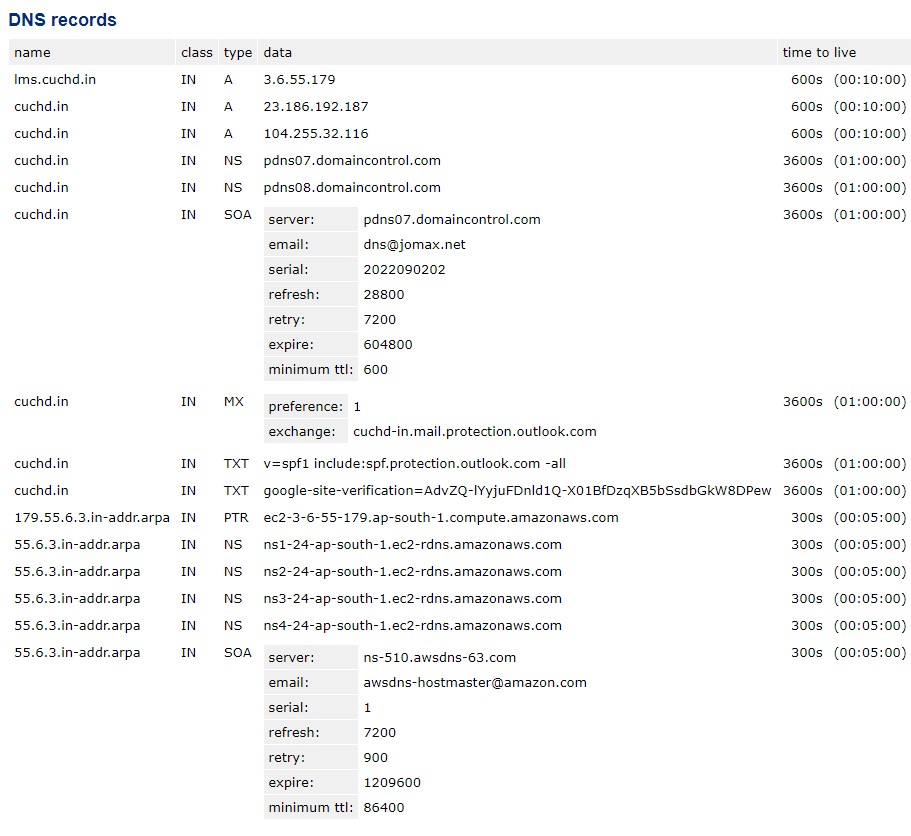
* 1. Centralops.net and enter any domain there like Netflix.com
  2. All information you can view there (for educational purpose only)

**Output Screenshots:**













**Learning Outcomes:**

Finally, as a penetration tester, you should collect and log all vulnerabilities in the system. Don’t ignore any scenario considering that it won’t be executed by the end-users. If you are a penetration tester, please help our readers with your experience, tips, and sample test cases on how to perform Penetration Testing effectively.