DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

CHANDIGARH UNIVERSITY
Discover. Learn. Empower.

UNIVERSITY INSTITUTE OF ENGINEERING

Department of Computer Science & Engineering

Subject Name: WEB AND MOBILE SECURITY LAB

Subject Code: 20ITP-378

Submitted to:

MARIAM KHAN

Submitted by:

Name: Tushar Singh

UID: 20BET1094

Section: 20BET601

Group: B

Experiment-2.2

Student Name: Tushar Singh **UID: 20BET1094**
Branch: BE-IT **Section/Group:20BET_WM_601-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.

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

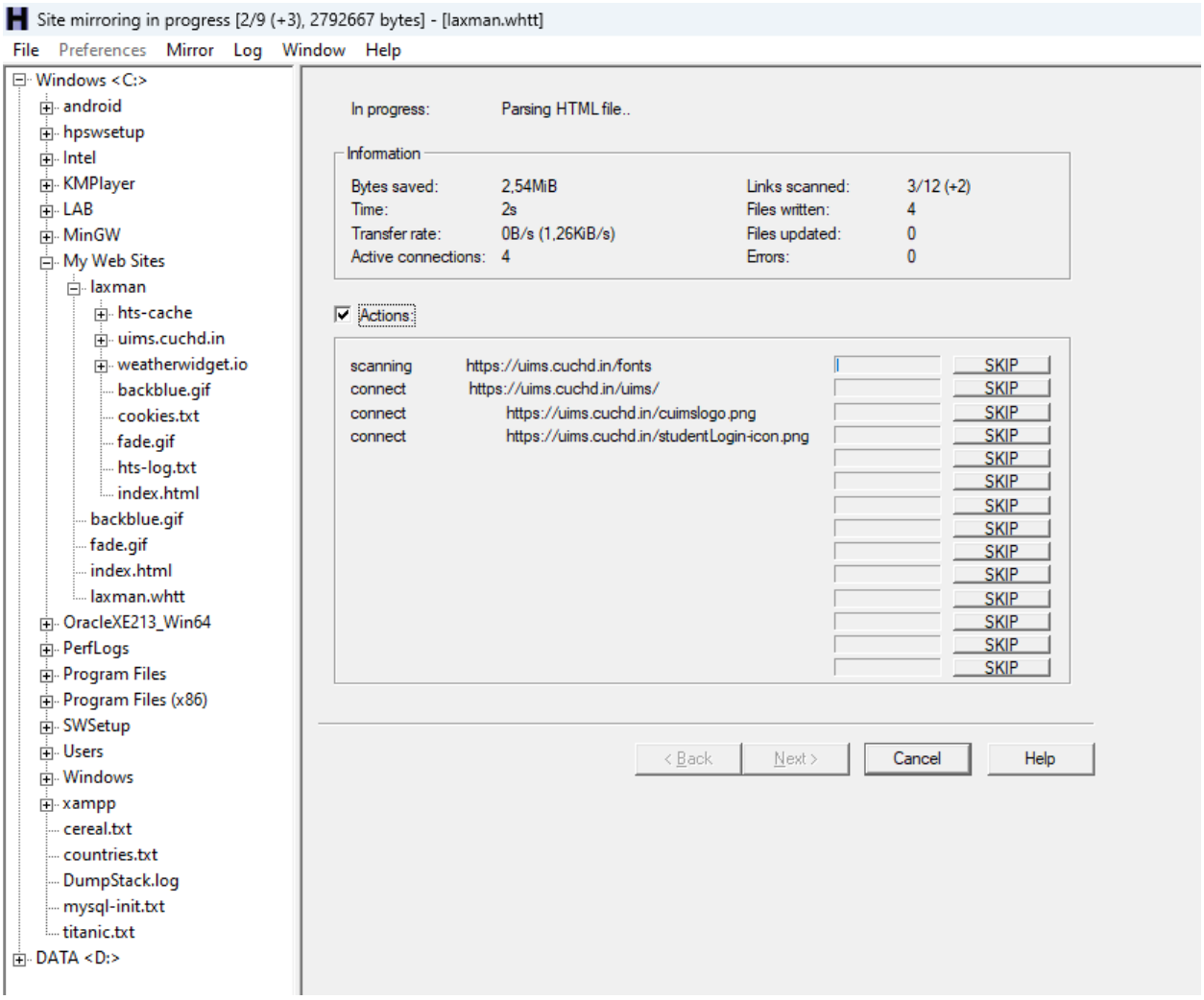
Email Foot printing:

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:


Site mirroring in progress [2/9 (+3), 2792667 bytes] - [laxman.whtt]
File Preferences Mirror Log Window Help
Windows <C:>
android
hpswsetup
Intel
KMPlayer
LAB
MinGW
My Web Sites
laxman
hts-cache
uims.cuchd.in
weatherwidget.io
backblue.gif
cookies.txt
fade.gif
hts-log.txt
index.html
backblue.gif
fade.gif
index.html
laxman.whtt
OracleXE213_Win64
PerfLogs
Program Files
Program Files (x86)
SWSetup
Users
Windows
xampp
cereal.txt
countries.txt
DumpStack.log
mysql-init.txt
titanic.txt
DATA <D:>
In progress: Parsing HTML file..
Information
Bytes saved: 2,54MiB
Time: 2s
Transfer rate: 0B/s (1,26KiB/s)
Active connections: 4
Links scanned: 3/12 (+2)
Files written: 4
Files updated: 0
Errors: 0
Actions:
scanning https://uims.cuchd.in/fonts
connect https://uims.cuchd.in/uims/
connect https://uims.cuchd.in/cuimslogo.png
connect https://uims.cuchd.in/studentLogin-icon.png
SKIP
< Back
Next >
Cancel
Help

Whois IP 103.70.135.7

Updated 1 second ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '103.70.132.0 - 103.70.135.255'

% Abuse contact for '103.70.132.0 - 103.70.135.255' is 'guru@move2inbox.in'

inetnum:        103.70.132.0 - 103.70.135.255
netname:        MSPL-IN
descr:          Mify Solutions Pvt. Ltd.
country:        IN
org:            ORG-MSPL3-AP
admin-c:        MSPL6-AP
tech-c:         MSPL6-AP
abuse-c:        AM2778-AP
status:         ALLOCATED PORTABLE
remarks:        -------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        -------------------------------------------------------
mnt-by:         APNIC-HM
mnt-lower:      MAINT-MSPL-IN
mnt-routes:     MAINT-MSPL-IN
mnt-irt:        IRT-MSPL-IN
last-modified:  2020-09-22T13:43:54Z
source:         APNIC

irt:            IRT-MSPL-IN
address:        FF-12/A, Omaxe Plaza, Shakti Khand-II, Indirapuram, Ghaziabad,
e-mail:         guru@move2inbox.in
abuse-mailbox:  guru@move2inbox.in
admin-c:        MSPL6-AP
tech-c:         MSPL6-AP
auth:           # Filtered
remarks:        guru@move2inbox.in is invalid
mnt-by:         MAINT-MSPL-IN
last-modified:  2022-06-16T07:12:30Z
source:         APNIC

organisation:   ORG-MSPL3-AP
org-name:       Mify Solutions Pvt. Ltd.
country:        IN
address:        H-163 SECTOR-63
address:        NOIDA
phone:          +91-9582450297
e-mail:         guru@move2inbox.in
mnt-ref:        APNIC-HM
```

```
address:        NOIDA
phone:          +91-9582450297
e-mail:         guru@move2inbox.in
mnt-ref:        APNIC-HM
mnt-by:         APNIC-HM
last-modified:  2022-07-13T12:55:48Z
source:         APNIC

role:           ABUSE MSPLIN
address:        FF-12/A, Omaxe Plaza, Shakti Khand-II, Indirapuram, Ghaziabad,
country:        ZZ
phone:          +000000000
e-mail:         guru@move2inbox.in
admin-c:        MSPL6-AP
tech-c:         MSPL6-AP
nic-hdl:        AM2778-AP
remarks:        Generated from irt object IRT-MSPL-IN
remarks:        guru@move2inbox.in is invalid
abuse-mailbox:  guru@move2inbox.in
mnt-by:         APNIC-ABUSE
last-modified:  2022-06-16T07:13:28Z
source:         APNIC

role:           Mify Solutions Pvt Ltd administrator
address:        FF-12/A, Omaxe Plaza, Shakti Khand-II, Indirapuram, Ghaziabad,
country:        IN
phone:          +91-9810448528
e-mail:         guru@move2inbox.in
admin-c:        MSPL6-AP
tech-c:         MSPL6-AP
nic-hdl:        MSPL6-AP
mnt-by:         MAINT-MSPL-IN
last-modified:  2019-09-03T07:02:36Z
source:         APNIC

% Information related to '103.70.134.0/23AS132090'

route:          103.70.134.0/23
origin:         AS132090
descr:          Mify Solutions Pvt. Ltd.
                SEC 63
                NOIDA
                U. P. - 201301, , India, , T :  +91 - 120 - 4835000
mnt-by:         MAINT-MSPL-IN
last-modified:  2019-03-08T06:13:21Z
source:         APNIC

% This query was served by the APNIC Whois Service version 1.88.16 (WHOIS-US4)
```

DNS records

name	class	type	data	time to live
lms.cuchd.in	IN	A	3.6.55.179	600s (00:10:00)
cuchd.in	IN	A	23.186.192.187	600s (00:10:00)
cuchd.in	IN	A	104.255.32.116	600s (00:10:00)
cuchd.in	IN	NS	pdns07.domaincontrol.com	3600s (01:00:00)
cuchd.in	IN	NS	pdns08.domaincontrol.com	3600s (01:00:00)
cuchd.in	IN	SOA	server: pdns07.domaincontrol.com email: dns@jomax.net serial: 2022090202 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600	3600s (01:00:00)
cuchd.in	IN	MX	preference: 1 exchange: cuchd-in.mail.protection.outlook.com	3600s (01:00:00)
cuchd.in	IN	TXT	v=spf1 include:spf.protection.outlook.com -all	3600s (01:00:00)
cuchd.in	IN	TXT	google-site-verification=AdvZQ-lYyjuFDnld1Q-X01BfDzqXB5bSsdbGkW8DPew	3600s (01:00:00)
179.55.6.3.in-addr.arpa	IN	PTR	ec2-3-6-55-179.ap-south-1.compute.amazonaws.com	300s (00:05:00)
55.6.3.in-addr.arpa	IN	NS	ns1-24-ap-south-1.ec2-rdns.amazonaws.com	300s (00:05:00)
55.6.3.in-addr.arpa	IN	NS	ns2-24-ap-south-1.ec2-rdns.amazonaws.com	300s (00:05:00)
55.6.3.in-addr.arpa	IN	NS	ns3-24-ap-south-1.ec2-rdns.amazonaws.com	300s (00:05:00)
55.6.3.in-addr.arpa	IN	NS	ns4-24-ap-south-1.ec2-rdns.amazonaws.com	300s (00:05:00)
55.6.3.in-addr.arpa	IN	SOA	server: ns-510.awsdns-63.com email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	300s (00:05:00)

Network Whois record

Queried **whois.arin.net** with "**n ! NET-3-6-0-0-1**"...

```
NetRange:       3.6.0.0 - 3.7.255.255
CIDR:           3.6.0.0/15
NetName:        AMAZON-BOM
NetHandle:      NET-3-6-0-0-1
Parent:         AT-88-Z (NET-3-0-0-0-1)
NetType:        Reallocated
OriginAS:
Organization:   Amazon Data Services India (ADSI-6)
RegDate:        2019-10-29
Updated:        2019-10-29
Ref:            https://rdap.arin.net/registry/ip/3.6.0.0



OrgName:        Amazon Data Services India
OrgId:          ADSI-6
Address:        L&T Business Park, Gate No.5, Tower A
Address:        Ground Floor, Sakivihar Road, Pawai
City:           Mumbai
StateProv:      MAHARASHTRA
PostalCode:     400072
Country:        IN
RegDate:        2016-08-05
Updated:        2019-08-02
Ref:            https://rdap.arin.net/registry/entity/ADSI-6


OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-555-0000
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-555-0000
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-555-0000
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEA8-ARIN
```

Domain Whois record

Queried **whois.registry.in** with "**cuchd.in**"...

```
Domain Name: cuchd.in
Registry Domain ID: D8634765-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2020-05-04T14:42:51Z
Creation Date: 2014-08-05T06:32:26Z
Registry Expiry Date: 2023-08-05T06:32:26Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Punjab
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
```

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.