**Lab Experiment 05**

**B. Tech CSF-CSE Semester III Course: Physical and IT Security**

**By: Dr. Gopal Singh Rawat**

**Lab Objective: Perform Internet Footprinting**

**What is Footprinting:**

* 1st step to Hacking
* Collect all possible information regarding the target
* Identify possible ways to attack and exploit the target
* Use publically available information, social engineering, system/network attacks, scanning…

**Objective of this Lab:**

* Know the security posture of the Target (Person, Web Site, IP Address, Server, Machine…)
* Why 🡪 Reduce the focus area to Identify Vulnerabilities
* Draw network map of target

**Ways (Methodology) to perform Footprinting (find information):**

1. Using Search Engines
2. Social Networking sites
3. Tools
4. Competitive Intelligence
5. WHOIS
6. DNS
7. Social Engineering
8. **Use Search Engines**
9. **Collect official website information**

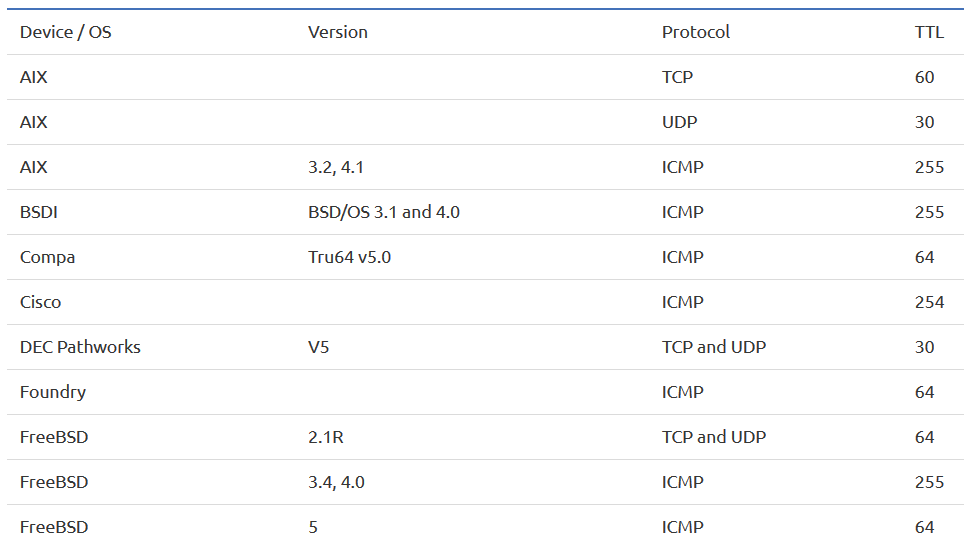
* Find URLs 🡪 Public Search Engines (Google/Bing/Yahoo)

1. **Physical location Finder**
   * Google Earth <https://www.google.com/intl/en_in/earth/>
   * <https://ipstack.com/>
   * <https://www.ip2location.com/demo/14.139.239.66>
2. **Find info about People**

* Names, Address, Phone, Background Check, Criminal Records Public Records
  + [www.PrivateEye.com](http://www.PrivateEye.com)
  + [www.PeopleSearchNow.com](http://www.PeopleSearchNow.com)
  + [www.PublicBackgroundChecks.com](http://www.PublicBackgroundChecks.com)
  + [www.anywho.com](http://www.anywho.com)
  + [www.Intelius.com](http://www.Intelius.com)
  + [www.411.com](http://www.411.com)
  + [www.PeopleFinders.com](http://www.PeopleFinders.com)
* Search Financial Info 🡪 [www.google.com/finance or finance.yahoo.com](http://www.google.com/finance%20or%20finance.yahoo.com)
* Search Job Sites 🡪 [www.Linkedin.com](http://www.Linkedin.com), [www.Monster.com](http://www.Monster.com), [www.Indeed.com](http://www.Indeed.com)
* Search Groups, Forums, Blogs, Communities, Web sites

1. **Find OS by using PING and TRACERT**

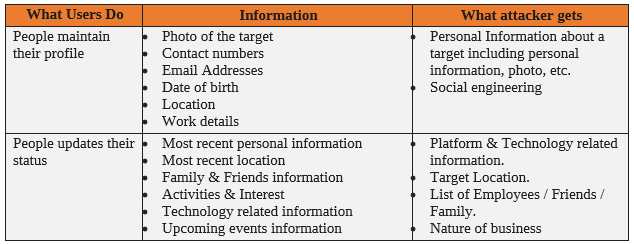
* C:\> Tracert <target> 🡪 note the number of hops (on Internet)
* C:\> Ping <Target> 🡪 note the TTL
* Add the two numbers OR check the TTL values
* Google “Default TTL Values” for Operating System of target
  + <https://subinsb.com/default-device-ttl-values/>
  + <http://www.kellyodonnell.com/content/determining-os-type-ping>



1. **Social Networking sites**
2. **Create accounts on social networking sites and search/gather information about the target.**



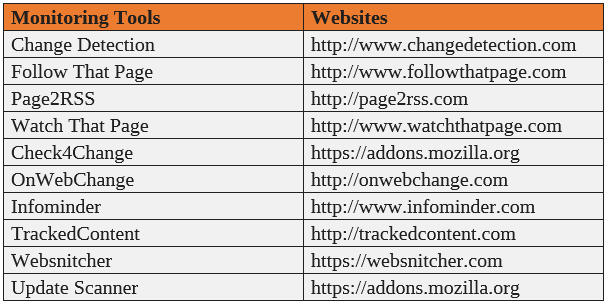
1. **Gather information**



1. **Tools to get information about target regarding**
2. Web Crawlers, Web Spiders or Web Copiers 🡪 Web Data Extractor 🡪 dump website contents on your disk



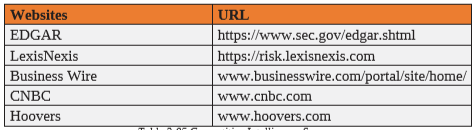
1. Extract Website Information 🡪 <https://web.archive.org>
2. Website Monitoring tools



1. **Competitive Intelligence**

Collect information, analyze and gather statistics regarding competitors using

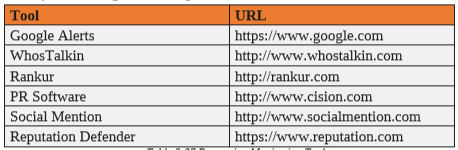
* Official websites
* Job Advertisements
* Press Release
* Annual Reports
* Product Catalogs
* Regulatory, Analysis Reports
* Agent, Distributors, Contractors, Suppliers



**Web Traffic Analysis of Target:**

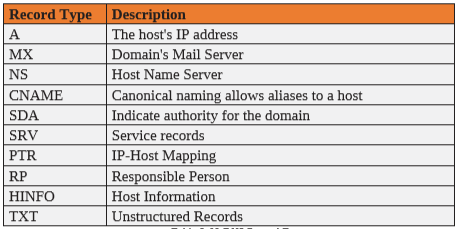


**Tracking Online Reputation of Target**



1. **WHOIS**
2. Gain information regarding Domain, Ownership, Location, IP Address, Netblock, ASN, DNS from Regional Internet Registries (RIR) from WHOIS Database

* [**www.whois.com**](http://www.whois.com)
* [**https://whois.domaintools.com**](https://whois.domaintools.com)
* [**http://lantricks.com**](http://lantricks.com)
* [**http://www.networkmost.com**](http://www.networkmost.com)



1. **WHOIS Lookup App for Mobiles:**

* **DNS Tools app from** [**www.dnssniffers.com**](http://www.dnssniffers.com)
* [**www.Ultratools.com**](http://www.Ultratools.com)

1. **Network Tracing**
2. **PING, TRACERT, NSLOOKUP 🡪 GUI**



**Lab #05 File Work:**

1. Perform this Experiment by identifying maximum details about at least Five (05) different types of targets (Person, Web Site, IP Address, Servers) from the Internet
2. Report details about those targets as per the below table.

|  |  |
| --- | --- |
| **Type of Target** | **Information Obtained** |
| E.g. Website / Domain | * IP Address * Geolocation * Hosted by * Physical address * Services provided * Server names * Server OS * Top Management |
| E.g. Person | * Name * Location * Phone * Office Address * Home Address * Role * Credit Card * Hobbies * Buying Habits * Friends * Social Media Posts 🡪 * Twitter / Facebook |
|  |  |