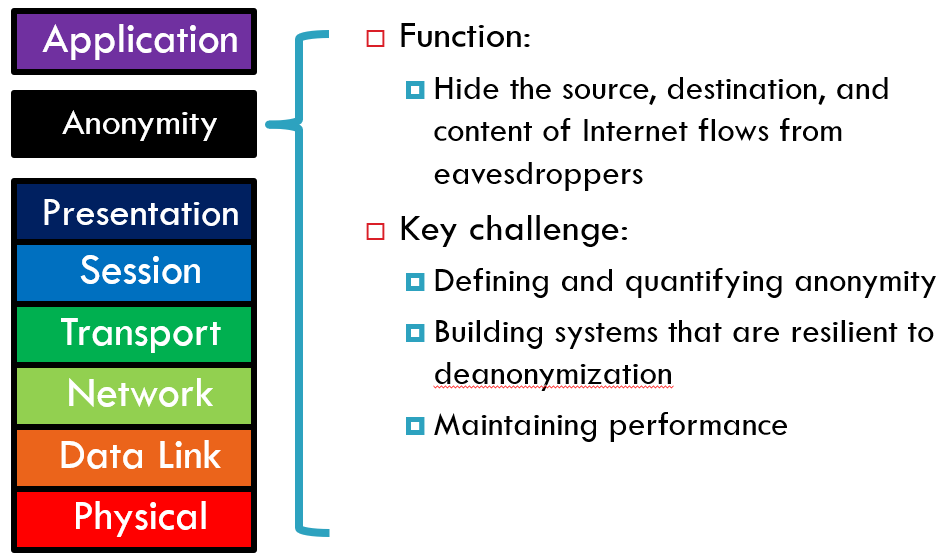


## 2.1

### Anonymity

Anonymity describes situations where the acting person's identity is unknown i.e. a person being non-identifiable, unreachable, or untrackable.



#### Threats to Anonymity

* Your IP address can be linked directly to you

ISPs store communications records

Usually for several years (Data Retention Laws)

Law enforcement can subpoena these records

* Your browser is being tracked

Cookies, Flash cookies, E-Tags, HTML5 Storage

* Browser fingerprinting

Your activities can be used to identify you

Unique websites and apps that you use

Types of links that you click

* Wireless traffic can be trivially intercepted

Airsnort, Firesheep, etc.

Encryption helps if it’s strong

#### Reasons for Anonymity

* To protect privacy

Avoid tracking by advertising companies

Viewing sensitive content

* Protection from prosecution

Not every country guarantees free speech

Downloading copyrighted material

* To prevent chilling-effects

It’s easier to voice unpopular or controversial opinions if you are anonymous

#### Data to be masked

* Personally Identifiable Information (PII)

Name, address, phone number, etc.

* OS and browser information

Cookies, etc.

* Language information
* IP address
* Amount of data sent and received
* Traffic timing

#### Achieving anonymity

1. Use of ProxyChains

Proxy chains is a program that allows you to use SSH, TELNET, VNC, FTP, and any other Internet application from behind HTTP(HTTPS) and SOCKS(4/5) proxy servers. This "proxifier" provides proxy server support to any app.

2. Use of VPN

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

3. Use of TOR Networking

Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

##### Proxy Chains

Proxying refers to the technique of bouncing your Internet traffic through multiple machines to hide the identity of the original machine, or to overcome network restrictions. ProxyChains is a tool that hackers often use to accomplish this goal. Supports SOCKS5, SOCKS4, and HTTP CONNECT proxy servers. Proxychains can be mixed up with a different proxy type in a list. Proxychains also supports any kind of chaining option methods, like random, which takes a random proxy in the list stored in a configuration file, or chaining proxies in the exact order list, different proxies are separated by a new line in a file. There is also a dynamic option, that lets Proxychains go through the live-only proxies, it will exclude the dead or unreachable proxies, the dynamic option is often called the smart option. Proxychains can be used with servers, like squid, sendmail, etc. Proxychains are capable of doing DNS resolving through proxy. Proxychains can handle any TCP client application, ie., nmap, telnet.

##### VPN

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

In simple terms, a virtual channel is created for the client's request trading. The server will think that the VPN node sent the request. This will allow a basic level of security for your requests. This will be a single anonymity layer that will keep your real identity hidden.

##### TOR

TOR uses Onion Routing to anonymize one's network traffic. Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address.

If the website tries to find the user, the backtracking process is like peeling process of an onion. One layer after another. The website sees that the request has been made from the TOR exit node of the TOR relay. This gives the user multiple layers of anonymity to keep one's identity hidden. Having more nodes will enable higher degree of anonymity, but it make all the request transactions really slow because each request has to make even higher number of hops from one layer to another.

**Censorship** - Areas of censorship include copyrights, defamation, harassment and obscene material. It is done through various technical and non-technical methods including content filtering and site blocking.

Areas of censorship include:

• Copyrights: it is a legal concept, which gives the creator of original work exclusive rights to it, i.e; nobody else has a claim on it.

•Defamation: it is the communication of a statement, which could be true or false, intended to give an individual, business or a product a negative image or a bad name.

• Harassment: it refers to behavior of an offensive nature that intends to disturb or upset an individual or a group of people. It can also be threatening at times.

• Obscene material: it refers to statements or acts that hurt moral, religious, cultural or traditional sentiments of society

Technical Internet Censorship Methods

• Internet Protocol (IP) address blocking

• Domain name system (DNS) filtering and redirection

• Uniform Resource Locator filtering

• Packet filtering

• Network disconnection

• Portal censorship and search result removal

Non Technical Internet Censorship Method

• Different publishers, authors, and ISPs may receive formal and informal requests to remove, alter, slant, or block access to specific sites or content.

• Publishers, authors, and ISPs may be subject to civil lawsuits.

• Access to the Internet may be limited due to restrictive licensing policies or high costs, lack of the necessary infrastructure, deliberate or not.

• Equipment may be confiscated and/or destroyed.

The main goal of OpenNet Initiative (ONI) is to monitor and report on internet filtering and surveillance practices by nations. The project employs a number of technical means and also international network of investigators, to determine the extent and nature of government-run internet filtering programs. ONI classifies the magnitude of censorship or filtering occurring in a country in four areas of activity.

The magnitude or level of censorship is classified as follows:

• Pervasive: A large portion of content in several categories is blocked.

• Substantial: A number of categories are subject to a medium level of filtering or many categories are subject to a low level of filtering.

• Selective: A small number of specific sites are blocked or filtering targets a small number of categories or issues.

• Suspected: It is suspected, but not confirmed, that Web sites are being blocked.

• No evidence: No evidence of blocked Web-sites, although other forms of controls may exist.

2.2 Introduction to Footprinting

Footprinting is a part of the reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both passive and active. Reviewing a company’s website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

Footprinting is basically the first step where a hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information −

* Domain name
* IP Addresses
* Namespaces
* Employee information
* Phone numbers
* E-mails
* Job Information

Methods of Information Gathering

There are the following three methods of information gathering:

* Footprinting
* Scanning
* Enumeration

Vulnerability Scanning -

Vulnerability scanning is the process of identifying vulnerabilities or weaknesses on a target system. Vulnerability scans can locate vulnerabilities without exploiting them.

Vulnerability scans are usually performed by an organization’s own employees and contractors, who have been expressly authorized by the company. Vulnerability scans are usually performed over a longer period of time, with periodic reviews.

WHOIS Lookup - You can use <http://www.whois.com/whois> website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

Dimitry - Dmitry is a free and open-source tool available on GitHub. The tool is used for information gathering. You can download the tool and install it in your Kali Linux. Dmitry stands for DeepMagic Information Gathering Tool. It’s a command-line tool Using Dmitry tool You can collect information about the target, this information can be used for social engineering attacks. It can be used to gather a number of valuable pieces of information.

Usages of Dmitry Tool :

Dmitry Tool can be used to search subdomains of the target.

Dmitry Tool can be used to find open ports of the target system.

Dmitry Tool can be used to perform TCP scan.

Dmitry Tool can be used with netcraft service to get the target information such as operating system, web server details, web host details, hosting service details, etc.

Dmitry Tool can be used with whois service to get the target information such as registered domain, name, address, the contact information of the person who registered it.

Dmitry Tool can be used to get email addresses that are associated with the domain of the target.