**Competitive Intelligence and DNS Enumerations-**

**Competitive Intelligence-**

Competitive intelligence gathering is the process of gathering information about the competitors from resources such as the Internet. This is a process of creating search queries to extract hidden information by using Google operators to search specific strings of text inside the search results.

Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet. Competitive intelligence means understanding and learning what about other businesses, in order to become as competitive as possible. It is non-interfering and subtle in nature compared to the direct intellectual property theft carried out through hacking or industrial espionage. It concentrates on the external business environment. In this method, professionals gather information ethically and legally instead of gathering it secretly.

Ethical Hacking uses the same methods as competitive intelligence to gather information. Facts about a target could be found using publicly available sources, those include: catalogs, financial reports, job postings, press releases, annual reports, news articles, trade journals, patents, and watermarks. In Infosavvy Training Institute you learn the multiple techniques to gather the information of organization and their employees details. Using the Whois we find out the full information of the company and there multiple ip address. There is another method call theharvester tool which is in kali linux. By using theharvester we can find out the employee’s details like name of employee, designation and some time we find there contact number also.

**Competitive intelligence helps in determining**:

– What the competitors are doing

– How competitors are positioning their products and services.

Companies carry out competitive intelligence either by employing people to search for the information, or by utilizing a commercial database service, which can be lower in cost.

**Sources of Competitive Intelligence**:

Competitive Intelligence gathering can be performed either using direct or indirect approach.

* Direct approach: serves as primary sources for competitive intelligence gathering. Direct approach techniques include gathering information from trade shows, social engineering employees and customers and so on.
* Indirect Approach: Through an indirect approach, information about competitors are gathered using online resources. Indirect approach techniques include:

1. Company websites anti employment ads

2. Search engines, Internet, and online database

3. Press releases and annual

**DNS Enumerations-**

Domain Name System(DNS) is nothing but a program that converts or translates a website name into an IP address and vice versa.

Example: A user enters www.geeksforgeeks.org in a browser, now the DNS will intercept this request and will fetch the corresponding IP address and connect the user to that fetched IP address.

**DNS Enumeration** is a technique used for Reconnaissance for better understanding of surface area of the Target systems(i.e. IP addresses).

The process of DNS Enumeration returns various important information about the target like DNS record types, host names, IP addresses and much more depending upon the configuration of that target system.

To perform DNS enumeration there are various open source tools, scripts available like Nmap, DNS recon etc.

**Importance and Impacts**:

**Importance**:

It helps in discovering the various services and hosts that are running on the domain.

It makes the target surface larger as we enumerate further.

Furthermore, it exposes the critical information about the target.

**Impact:**

The attacker can read about the system data and also can modify it.

It can also lead to various other potential DNS attacks.

It gives the Threat actor very critical details about the system that the attack can leverage to other attacks.

**Steps of DNS Enumeration**:

There are various tools to do DNS Enumeration, you are free to explore them by doing a simple web search about DNS Enumeration tools, but here we are going to use Nmap as an example:-

**Nmap**:

It is a tool used to discover host and services that are currently running of a computer network. Nmap provides an extensive Script by the name dns-nsec-enum.

Command Usage:

nmap -sSU -p 53 --script dns-nsec-enum -

-script-args dns-nsec-enum.domains=example.com

<target>