Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 7
Year 2, Semester 1

What is Penetration testing?

Penetration testing also called pen testing or ethical hacking is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. Pen testing can be performed manually or automatically using software applications. The main objective of penetration testing is to identify security weaknesses.

What is Ethical hacking?

Ethical hacking is an extensive term that covers all hacking techniques, discovering the security flaws and vulnerabilities, and ensuring the security of the target system, it is beyond hacking the system but with permission in order to safeguard the security for future purposes.

• What is the difference between Ethical Hacking and Penetration Testing?

Information Gathering

Penetration testing or ethical hacking is about breaking into the system and taking ownership of it. To break into a system, it is essential to identify possible entry points and any vulnerabilities in these entry points. To identify the above information, you need to gather information about your targets. The more you know about the targets, the better your chances of successfully penetrating the system.

1. Active Information Gathering
When you have enough information about your targets, you can gather more information about these targets by actively interacting with them. Doing this without authorization can be illegal.
The goal of active information gathering is to gather information as much as possible.
Eg: DNS Enumeration, Port Scanning, OS Fingerprinting

2. Passive Information Gathering
Collecting information about targets using publicly available information. The goal is to find as much information as possible.

Eg: Search engine results, Directory listing (directory indexes), Leaked credentials

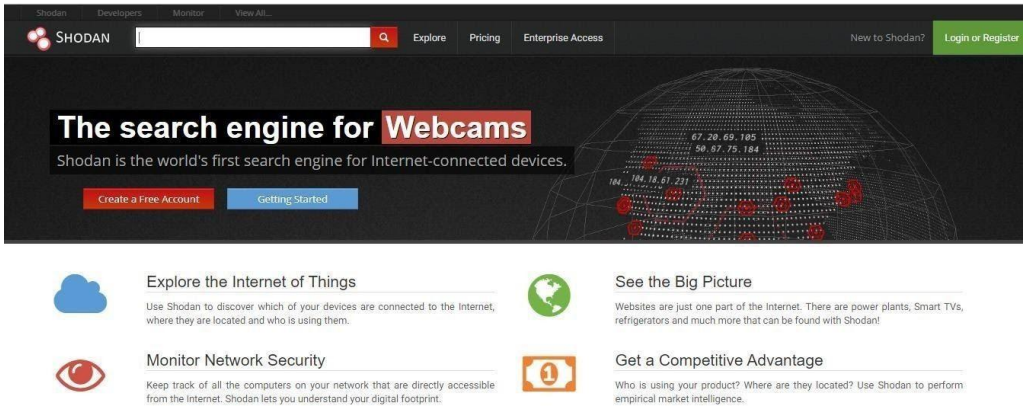
Passive information gathering

➢ Google Hacking
Google hacking is referred to as Google Dorking, is also an information-gathering technique used by attackers leveraging advanced Google searching techniques. Google hacking search queries can be used to identify security vulnerabilities in web applications, gather information for individual targets, sensitive information. The advanced search string crafted by an attacker could be searching for the vulnerable version of a web application, or a specific file-type (.pwd, .sql...) in order to further restrict the search.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 7
Year 2, Semester 1

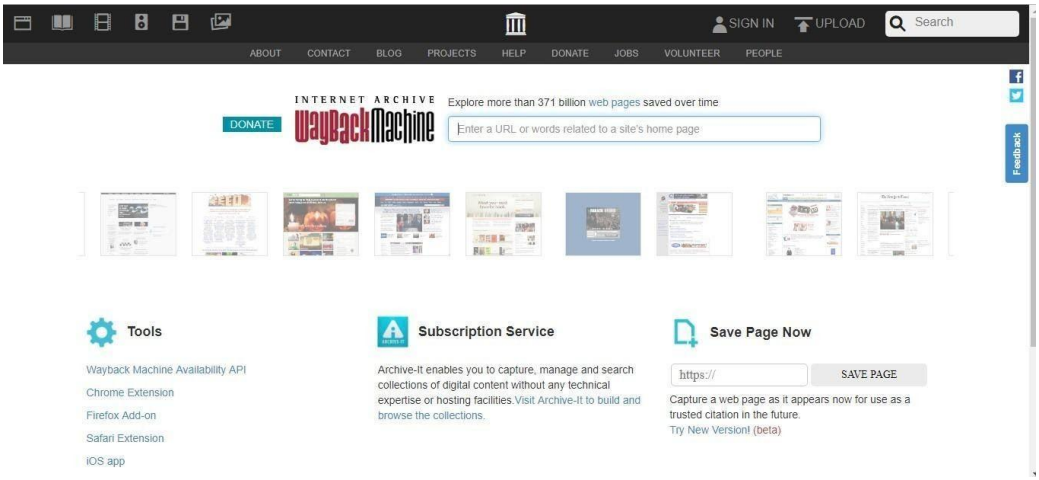
➢ What is Shodan.io?

Shodan.io is a search engine for everything on the internet. This is the final product of research of university students. While Google and other search engines index only the web, Shodan indexes pretty much everything else — webcams, water treatment facilities, yachts, medical devices, traffic lights, wind turbines, license plate readers, smart TVs, refrigerators, anything and everything you could possibly imagine that's plugged into the internet.



➢ What is the Wayback machine?

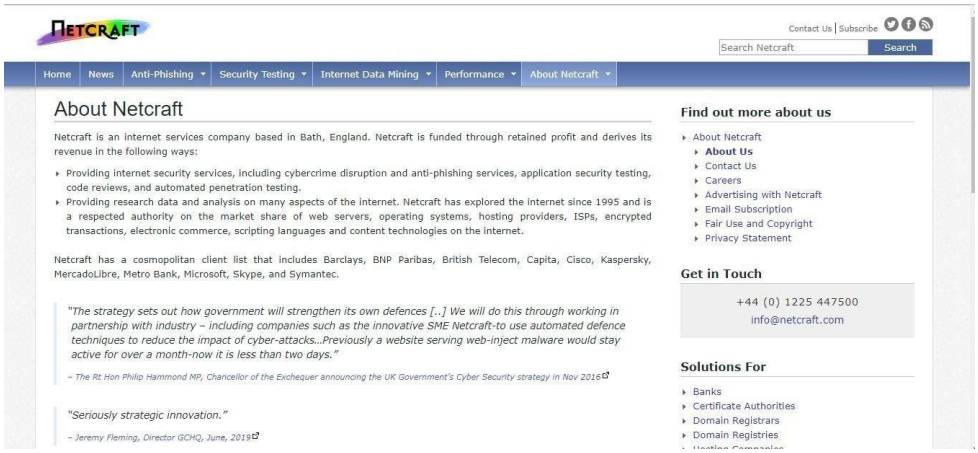
The Wayback Machine is a Web site that enables anyone to see what a website looked like at some time in the past - from 1996 to the present. At the Wayback Machine site, you can search for and link to any of your favorite Web sites of the past and find them preserved very much as they were at various "snapshots" in time.



Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 7
Year 2, Semester 1

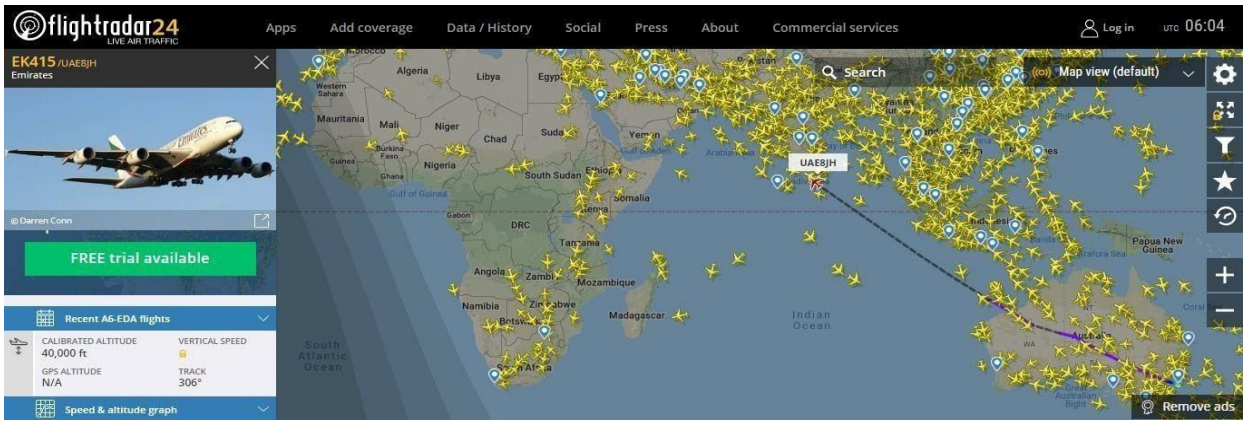
➢ What is Net craft?

Netcraft provides internet security services, including cybercrime disruption and anti-phishing services, application security testing, code reviews, automated penetration testing, research data, and analysis on many aspects of the internet. Netcraft has explored the internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages, and content technologies on the internet.



➢ Flight radar

Flightradar24 is a flight tracker that shows live air traffic from around the world. Flightradar24 combines data from several data sources including ADS-B, MLAT, and radar data. The ADS-B, MLAT, and radar data are aggregated together with schedule and flight status data from airlines and airports to create a unique flight tracking experience on www.flightradar24.com and in Flightradar24 apps.



Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 7
Year 2, Semester 1

➢ Marine Traffic

MarineTraffic is the world's leading provider of ship tracking and maritime intelligence. They are dedicated to making actionable information easily accessible. Monitoring vessel movements are at the core of what they do. Building on a base of data gathered from their network of coastal AIS-receiving stations, supplemented by satellite receivers, they apply algorithms and integrate complementary data sources to provide the shipping, trade, and logistics industries with actionable insights into shipping activity.