2021

ISN 1604-PROJECT REPORT

TARGET WEBSITE-http://testaspnet.vulnweb.com/

ANANTH RAJAN KILAMBI (813704), GAGANPREET SINGH (810468)

LAMBTON COLLEGE | MISSISSAUGA

Table of Contents

1.PASSIVE SCANNING TOOLS

Passive scanning is a method of reconnaissance in which there is no direct interaction between the network, server or system and the system which is trying to glen the information.

This is a relatively harmless method of information gathering which can be done by using resources available on the internet such as the target's website, social media and other such general information.

In this case we have used exclusively web-based tools available in the form of websites and extensions.

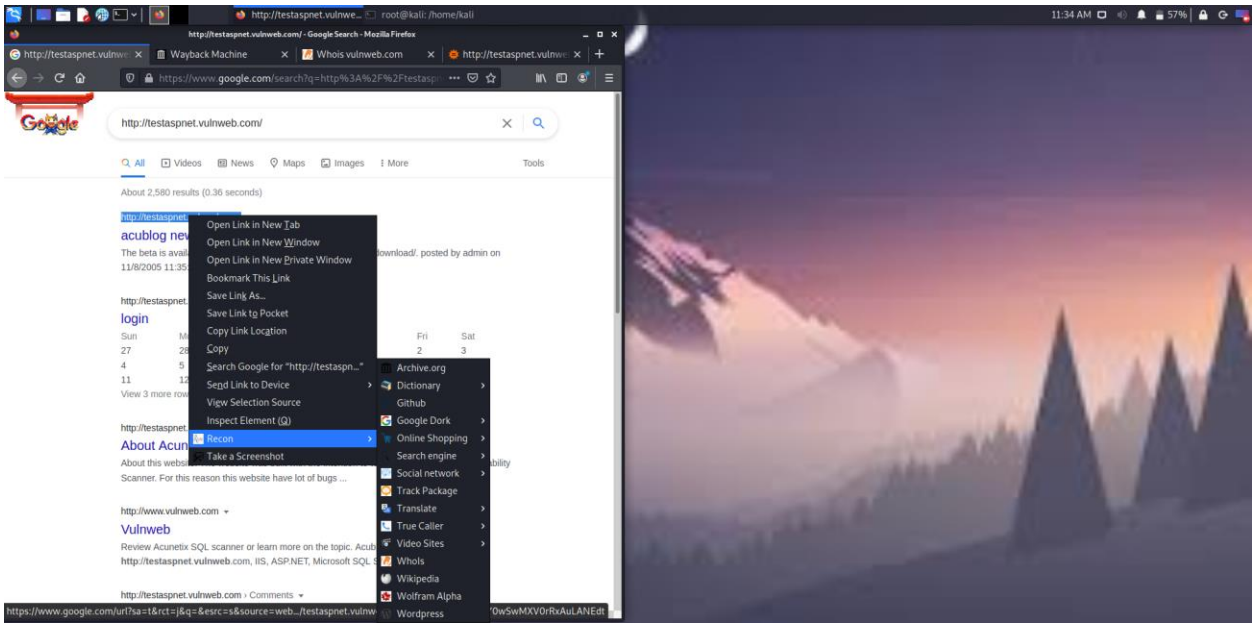
The extension was downloaded from Mozilla Store and is called Recon.

It is very intuitive to use. Just select the website you want to know more about, right-click on your mouse and it shows a litany of sources to look for more details.

The other tools such as **Builtwith**, **Wappanalyzer**, VirusTotal and Find SubDomains are all tools which can be accessed through the browser and are very simple to use.

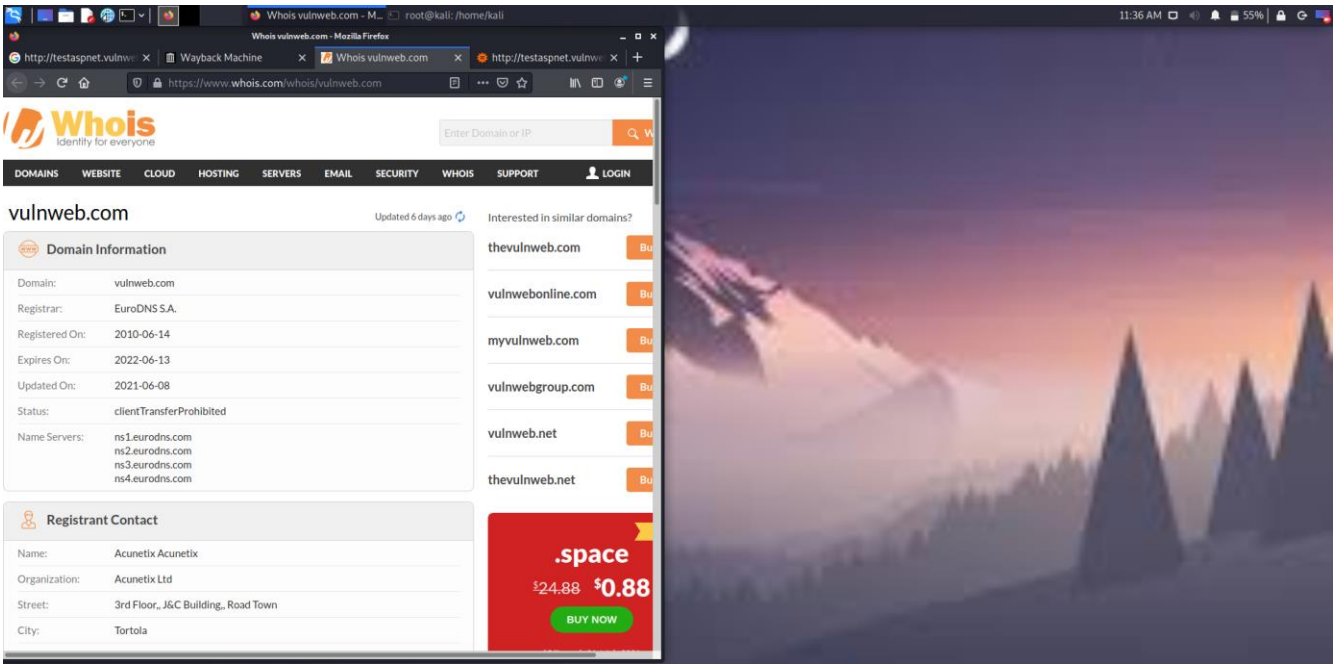
Note: A full working demonstration for all these tools will be available during our presentation.

1.1 PASSIVE RECON USING RECON WEB EXTENSION

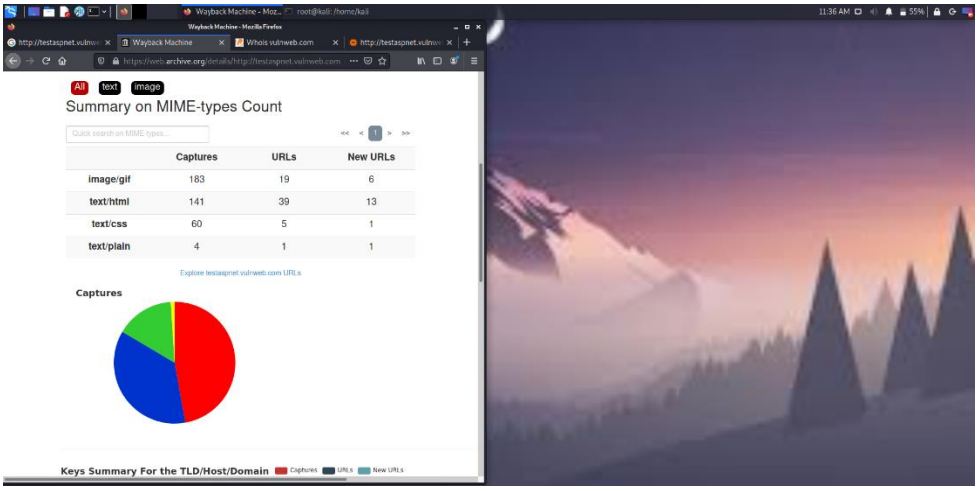


1.2 WHOIS

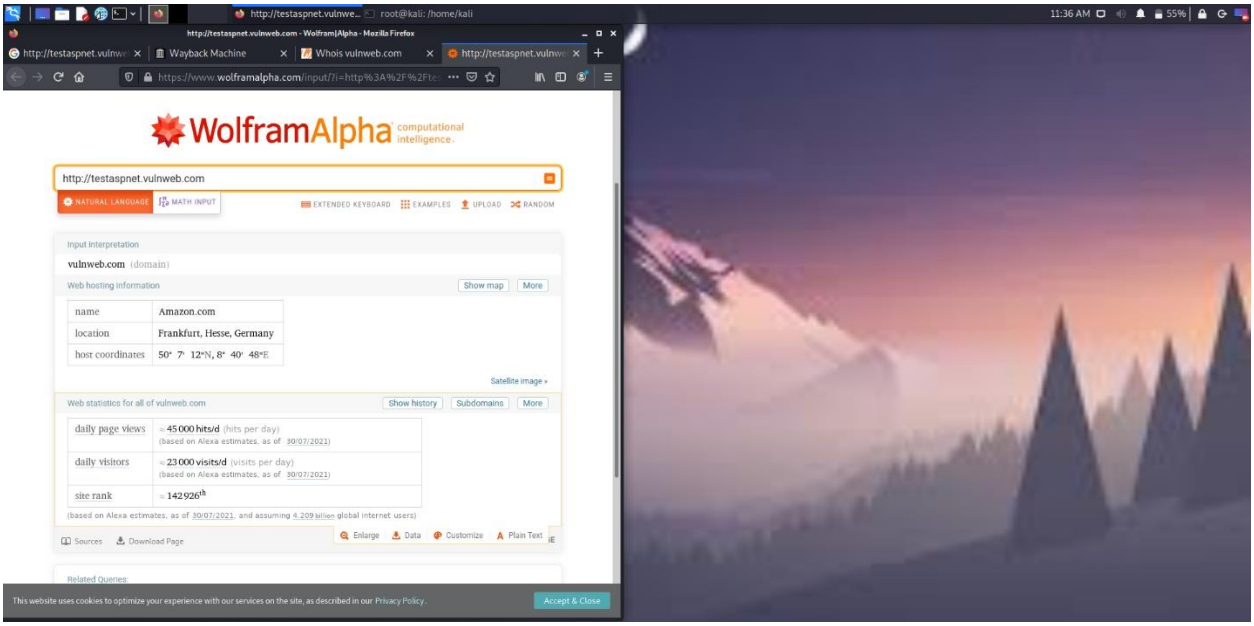
- Used to discover the owner of the website or any domain.



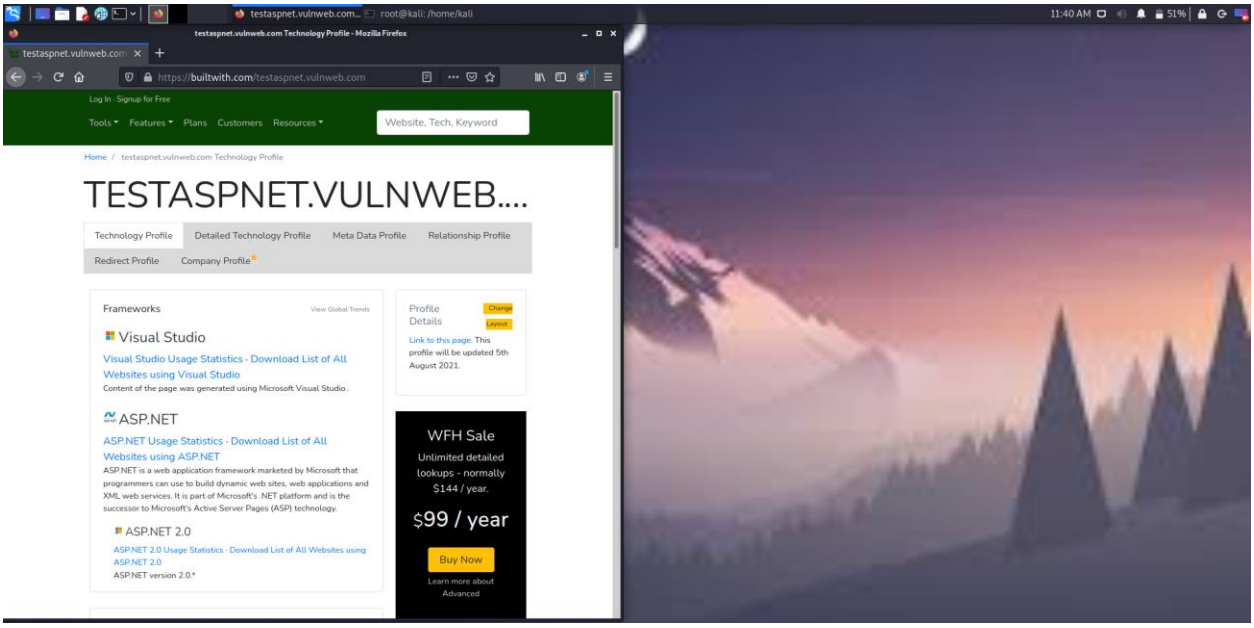
1.3 WAYBACK MACHINE



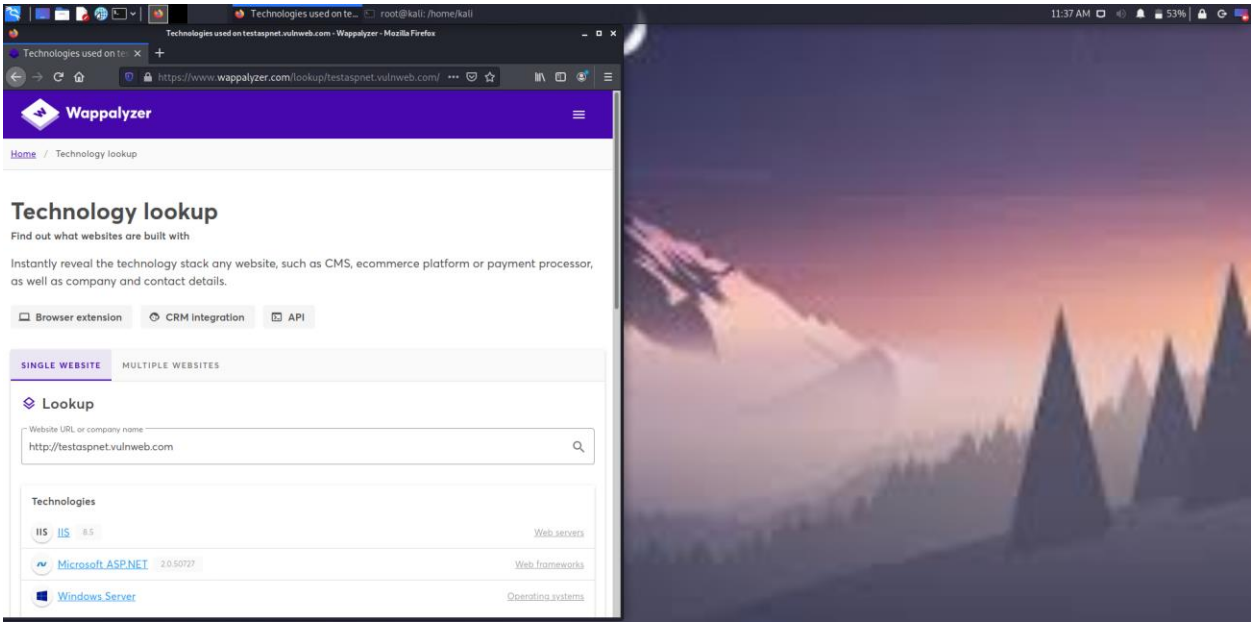
1.4 WOLFRAM ALPHA



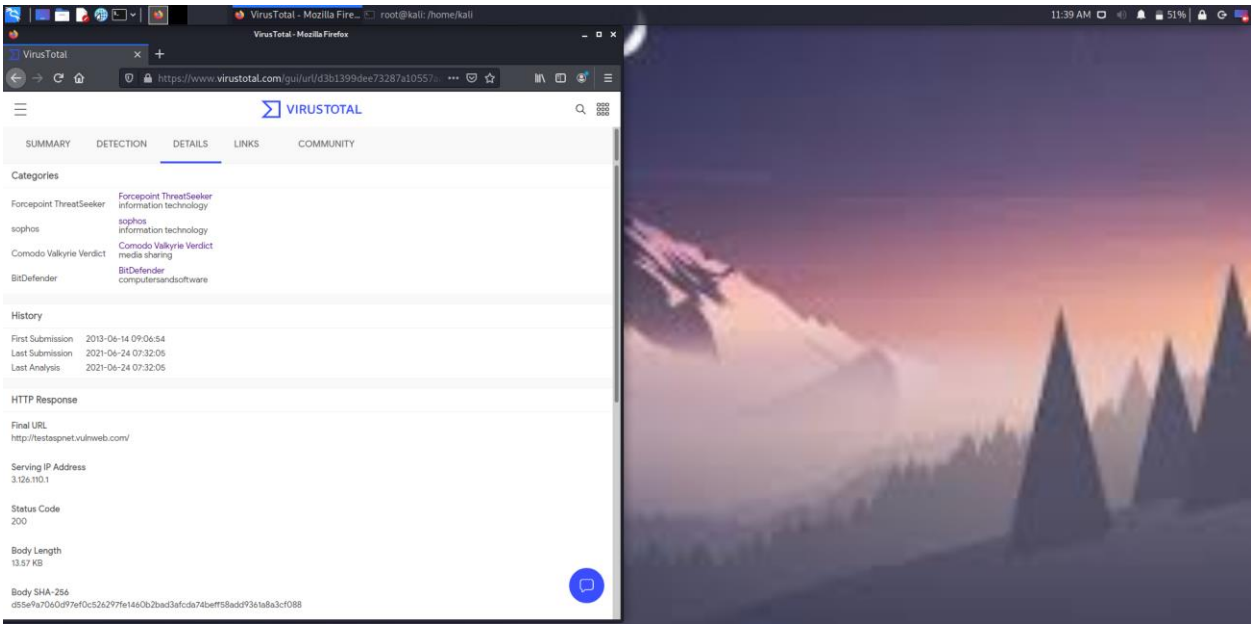
1.5 BUILTWITH.COM



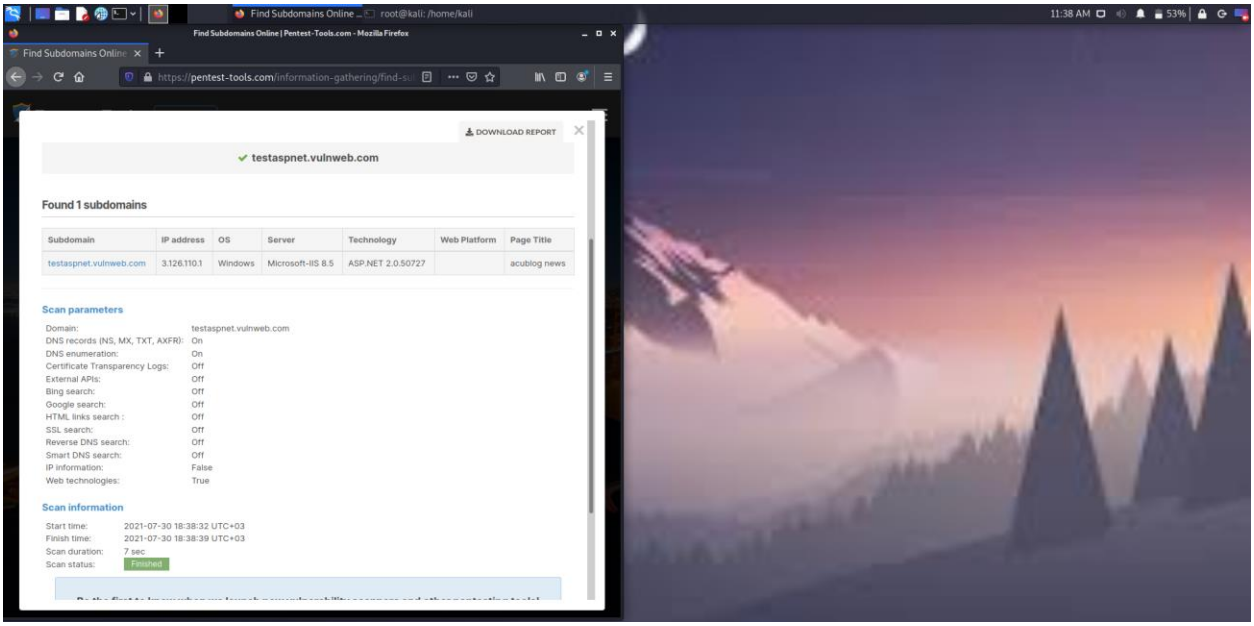
1.6 WAPPALYZER



1.7 VIRUSTOTAL.COM



1.8 PENTEST-TOOLS.COM



2.ACTIVE SCANNING TOOLS

Active scanning is a bit more intrusive than passive scanning.

In this the attacker will target specific ports, services and sectors of the target server, website or computer.

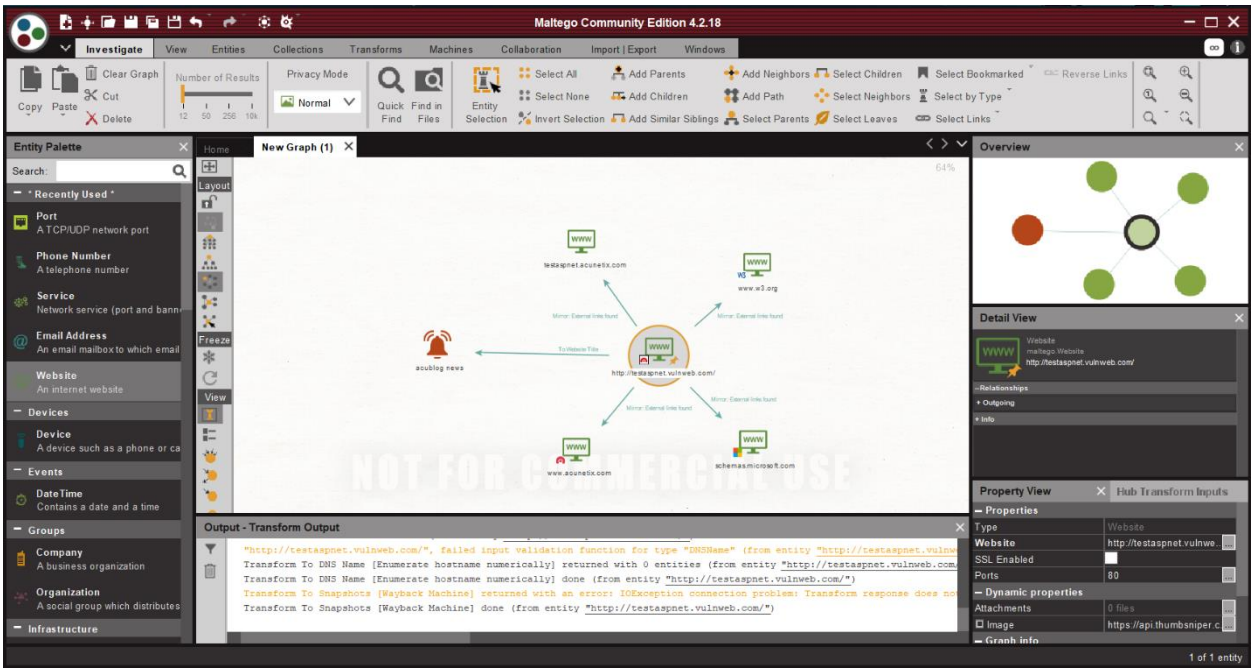
There are various methods used for this but we have gone with **Maltego, Recon-ng, UniScan** and **UnicornScan.**

The results are not always obvious, as in the case of Recon-ng, our target website did not yield any positive results for a variety of modules but it can work if the right module is used for it. The process for conducting a recon-ng scan will be shown in the video presentation.

The other 3 scans reveal certain information about the website we are targeting.

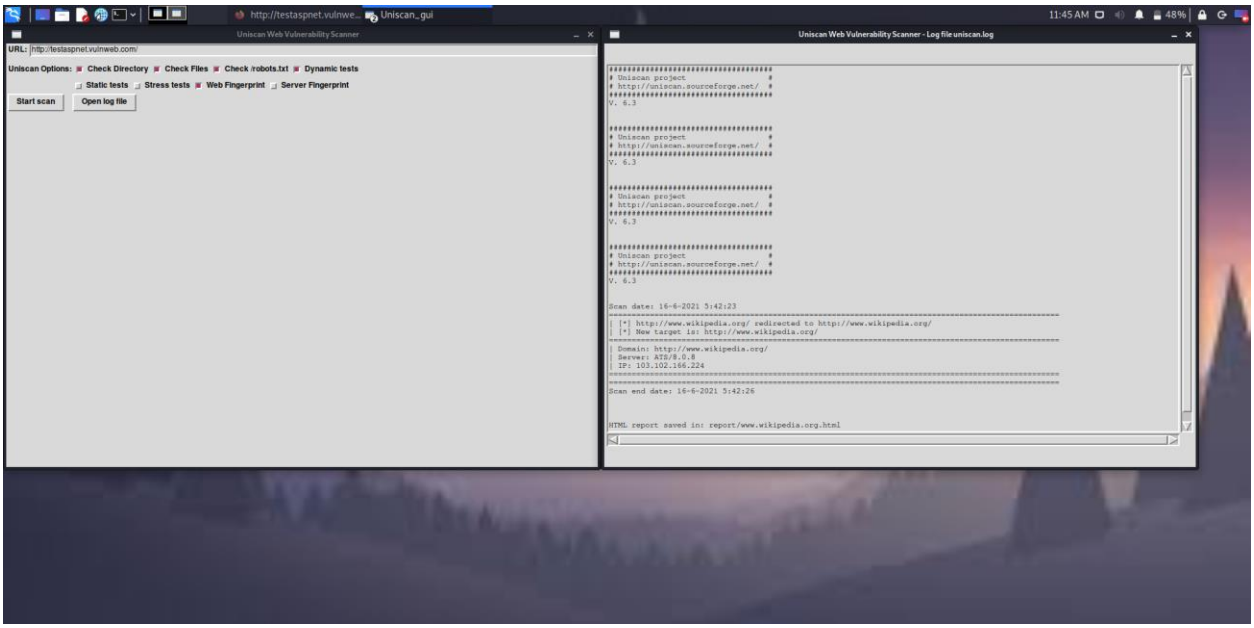
2.1 MALTEGO

Maltego leads to external links the website has to other sites and a link to its title



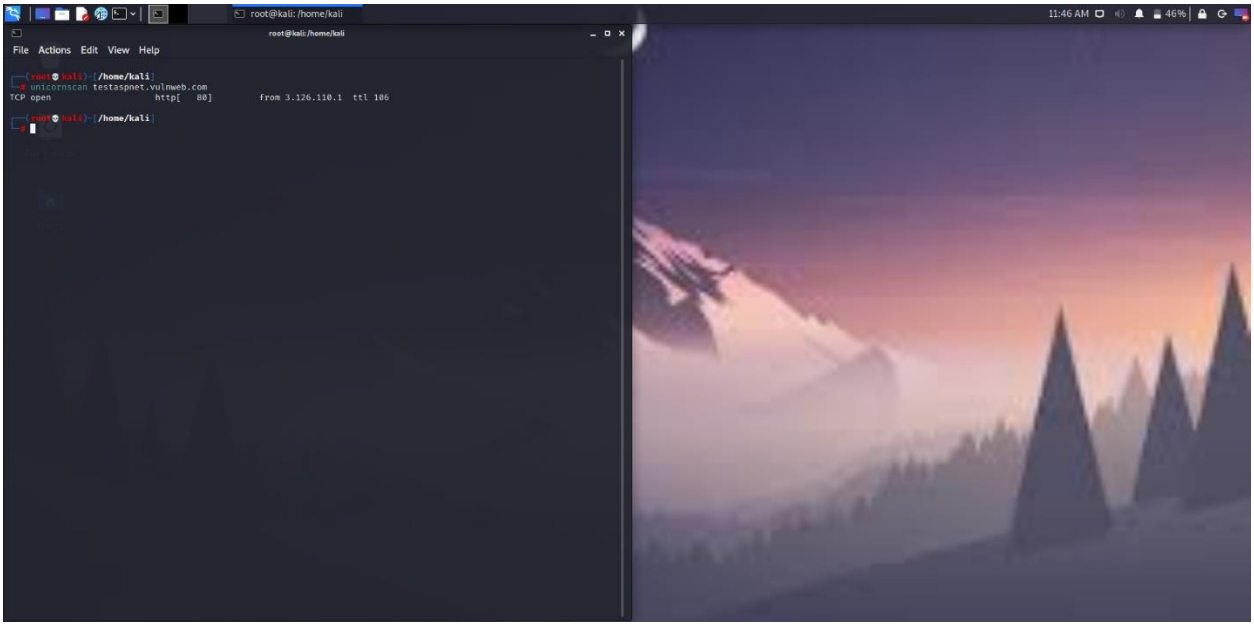
2.2 UNISCAN

- UNISCAN leads to a log file which will show details according to the selections the users input into the GUI



2.3 UNICORNSCAN

- UnicornScan will give the open services available on the website and display the protocol it uses



The end goal of all these tools is to ensure that information about any vulnerabilities, open ports, services or anything of value that can be exploited can be obtained from the website and be used to exploit the target website.

3.NETWORK SCANNING TOOLS

This type of scanning involves using a computer to gather more information about the devices on network.

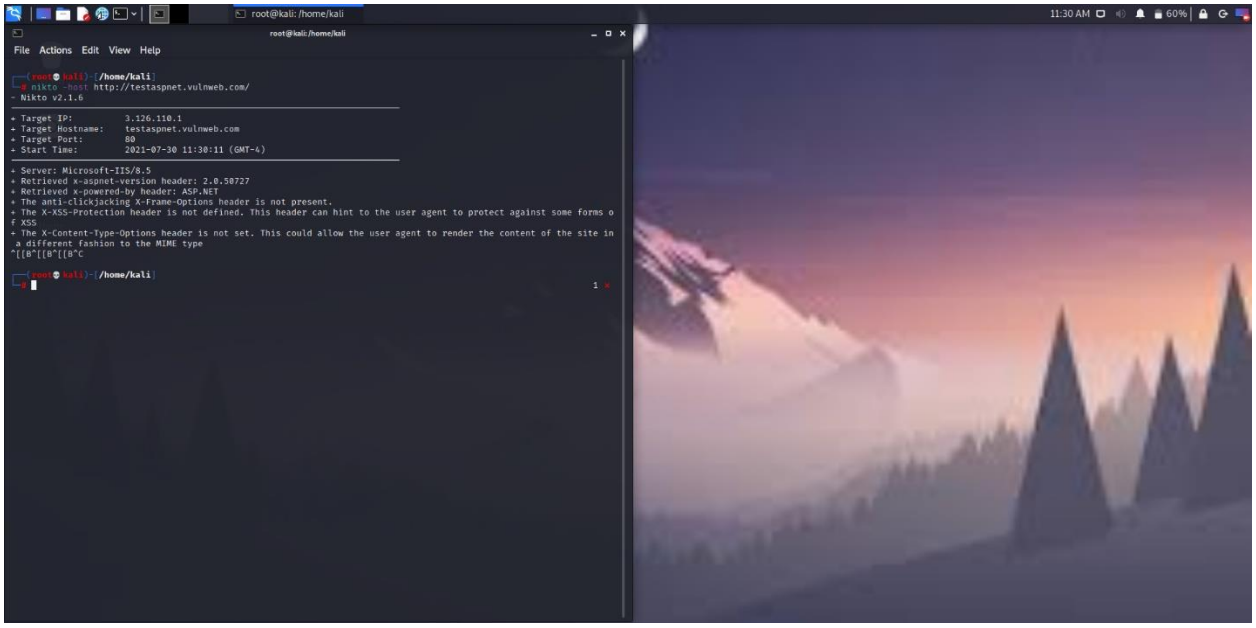
It is very useful for conducting vulnerability analysis and security assessments of the network.

The goal is similar, but we can use the information gathered from the previous 2 scanning methods and use it to conduct the reconnaissance.

We are using **nikto, nmap**, **censys**, and **dig** to conduct these scans.

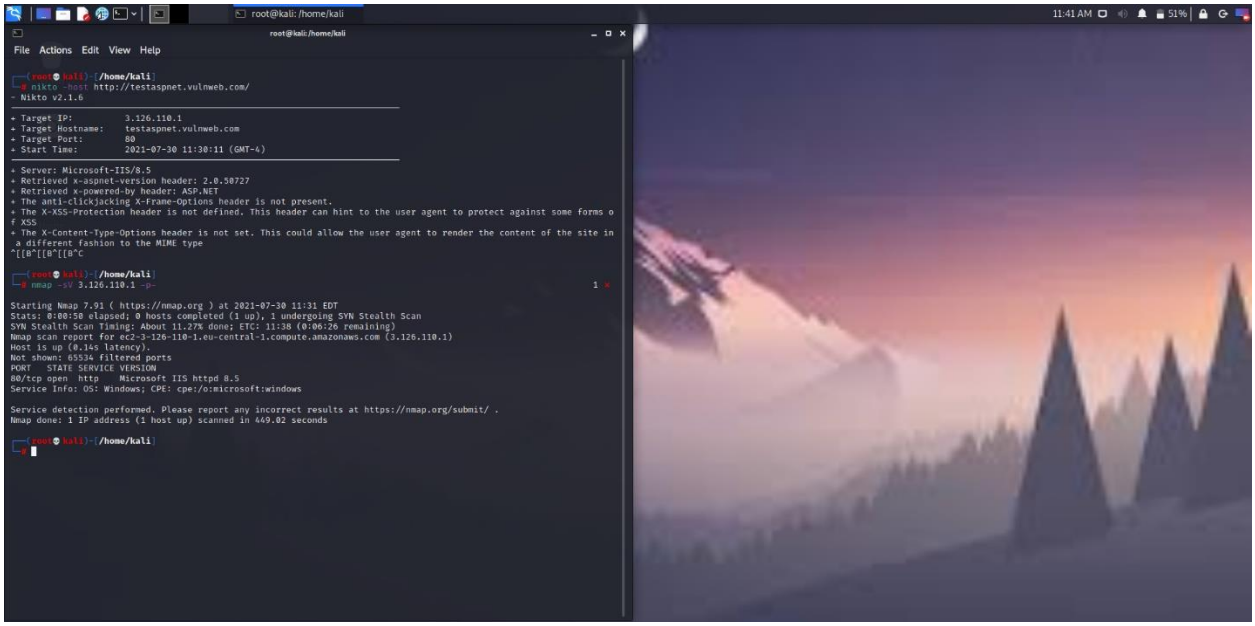
3.1 NIKTO

Nikto will give some information such as the IP address, target port and the server it is using to run its services.



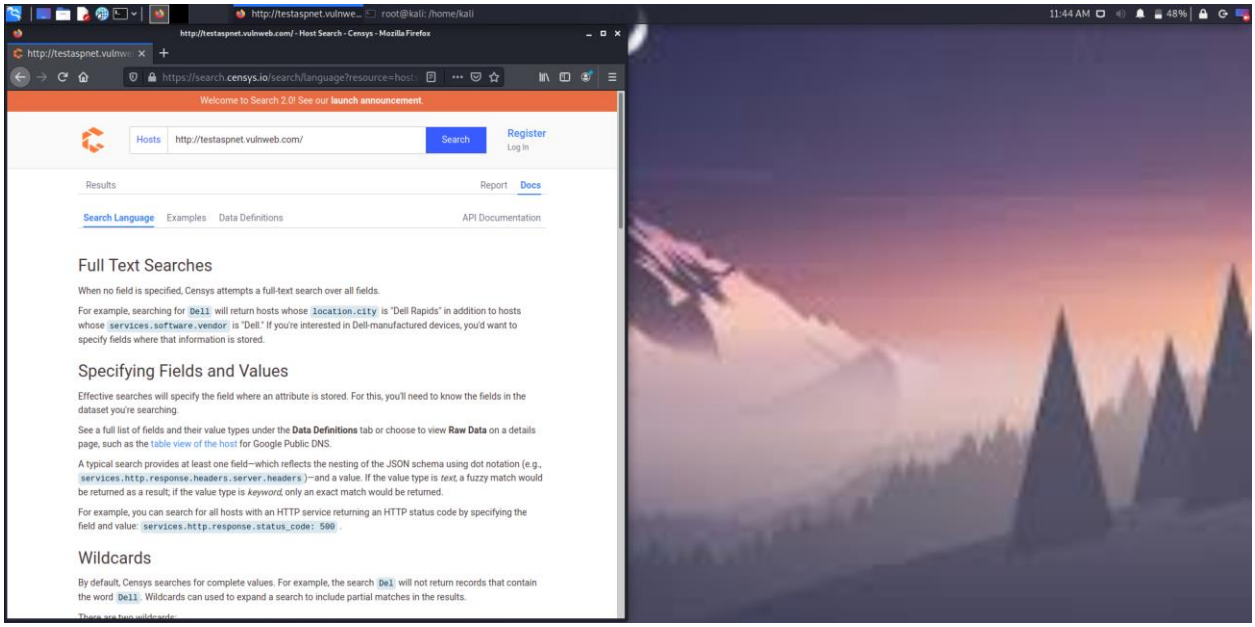
3.2 NMAP

Nmap is a good tool for conducting further in-depth research into a network and finding more details such as the services being run on all open ports in the network. Other core commands can be used to give more information, but knowing the service being run on what port is great for conducting a pen test of the network.



3.3 CENSYS

- Censys is another browser-based tool which we used. Our target website did not yield any results in this but if probed further it could give us some solid details about the network and other details.



3.4 DIG

- Dig stands for Domain Information Groper. This is a database-based tool which replaces nslookup and host tools.
- It is especially useful to diagnose DNS problems