

ISN 1604-PROJECT REPORT

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

[ANANTH RAJAN KILAMBI \(813704\)](#), [GAGANPREET SINGH \(810468\)](#)

Table of Contents

1. PASSIVE SCANNING TOOLS	2
1.1 PASSIVE RECON USING RECON WEB EXTENSION.....	2
1.2 WHOIS	3
1.3 WAYBACK MACHINE	4
1.4 WOLFRAM ALPHA.....	4
1.5 BUILTWITH.COM	5
1.6 WAPPALYZER.....	5
1.7 VIRUSTOTAL.COM	6
1.8 PENTEST-TOOLS.COM	6
2. ACTIVE SCANNING TOOLS	7
2.1 MALTEGO.....	7
2.2 UNISCAN.....	8
2.3 UNICORNSCAN.....	8
3. NETWORK SCANNING TOOLS	9
3.1 NIKTO.....	9
3.2 NMAP.....	10
3.3 CENSYS	10
3.4 DIG	11

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 glean 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.

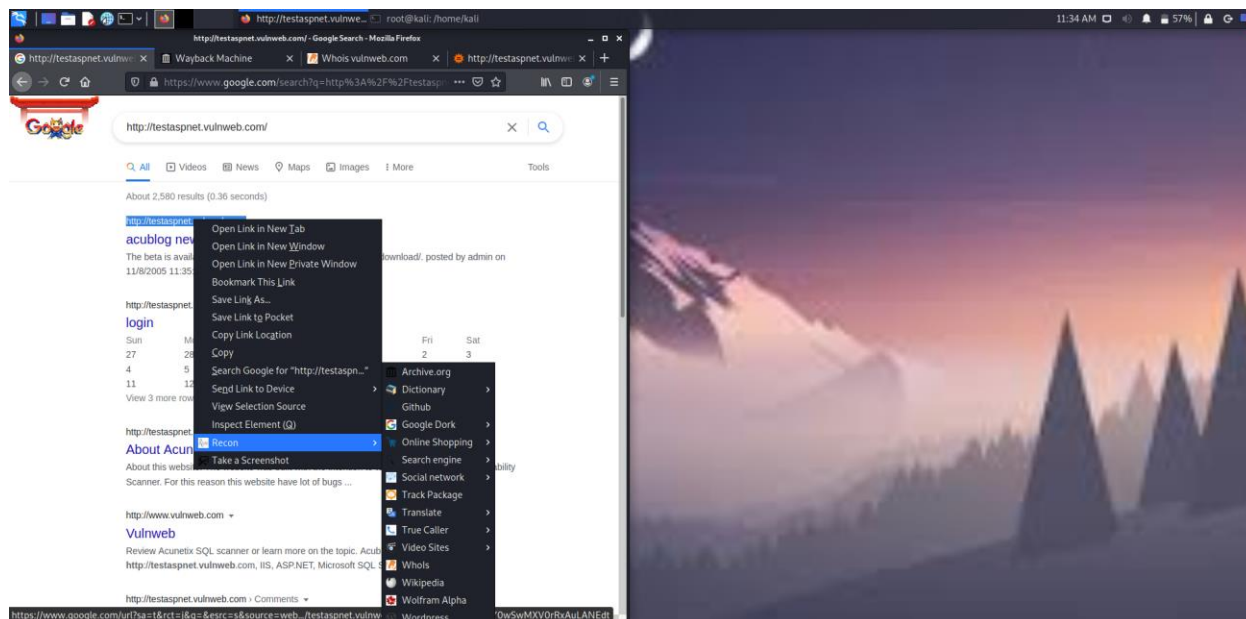
The extension was downloaded from Mozilla Store and is called Recon.

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.

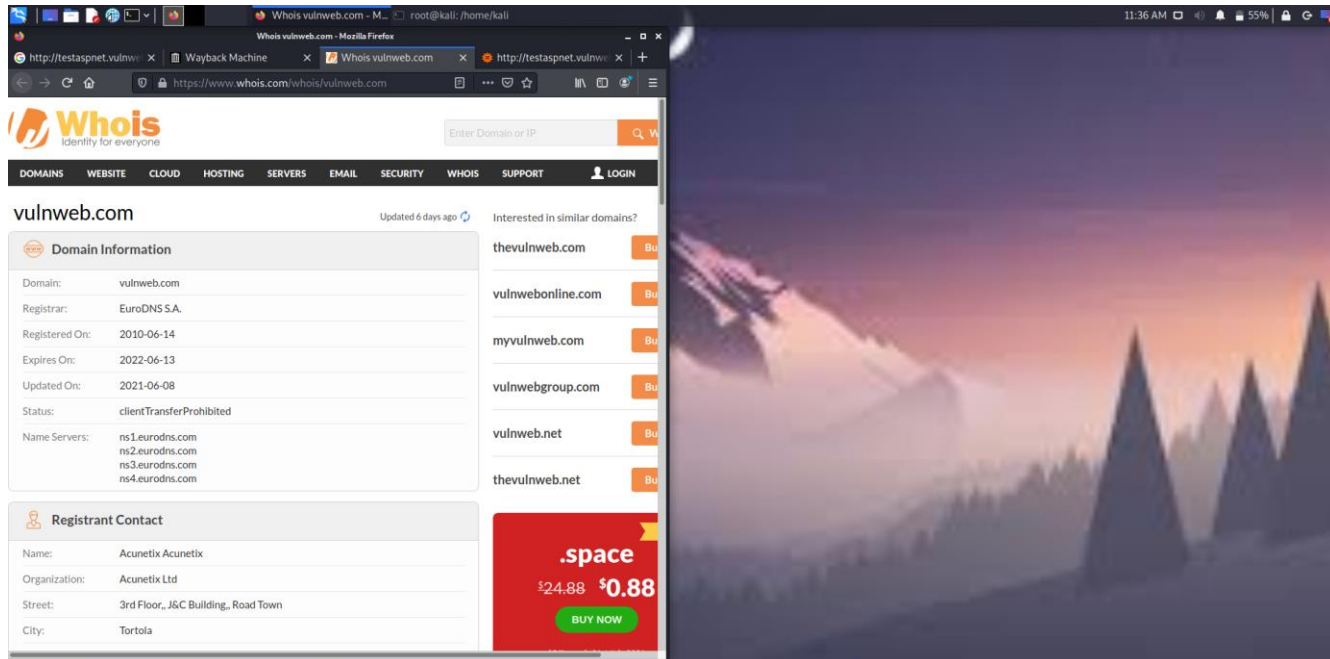
Note: A full working demonstration for all these tools will be available during our presentation.

1.1 PASSIVE RECON USING RECON WEB EXTENSION



1.2 WHOIS

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



The screenshot shows a web browser window with the URL <https://www.whois.com/whois/vulnweb.com>. The page displays the Whois information for the domain **vulnweb.com**, which was updated 6 days ago. The page is divided into two main sections: Domain Information and Registrant Contact.

Domain Information

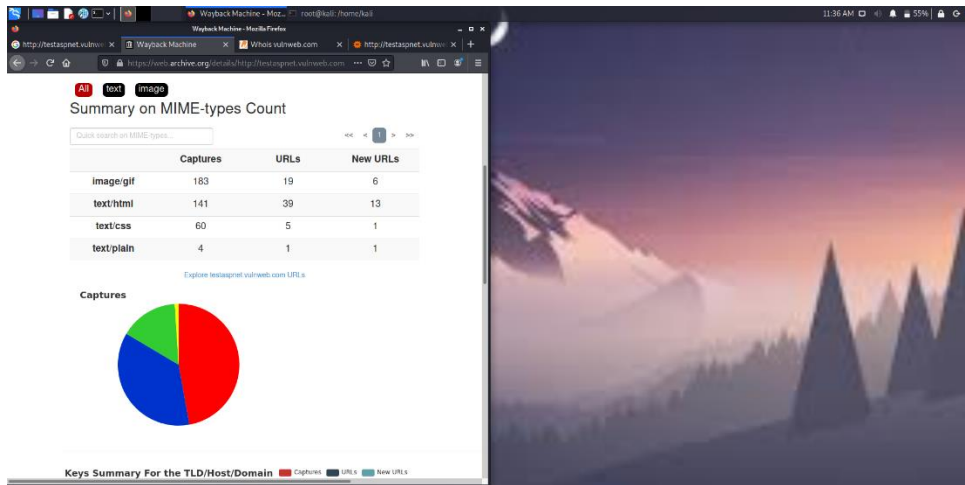
Domain:	vulnweb.com
Registrar:	EuroDNS S.A.
Registered On:	2010-06-14
Expires On:	2022-06-13
Updated On:	2021-06-08
Status:	clientTransferProhibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com

Registrant Contact

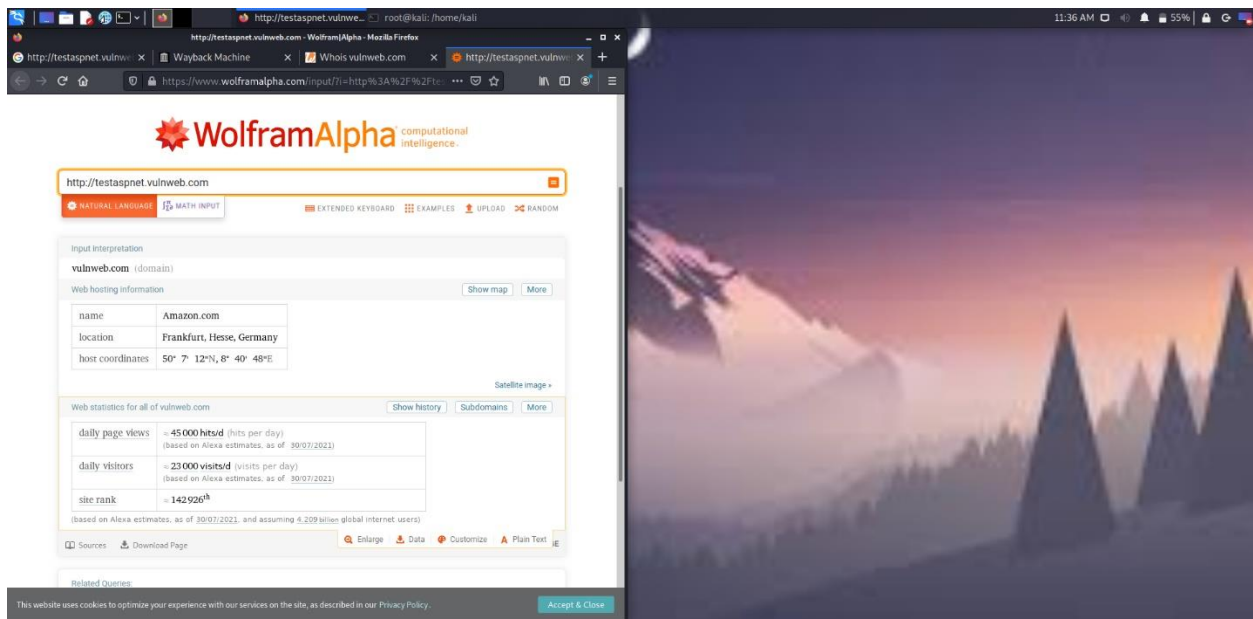
Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor, J&C Building, Road Town
City:	Tortola

On the right side of the page, there is a list of similar domains for sale, including [thevulnweb.com](#), [vulnwebonline.com](#), [myvulnweb.com](#), [vulnwebgroup.com](#), [vulnweb.net](#), and [thevulnweb.net](#). A red banner at the bottom right promotes the purchase of a **.space** domain for \$0.88 (down from \$24.88) with a "BUY NOW" button.

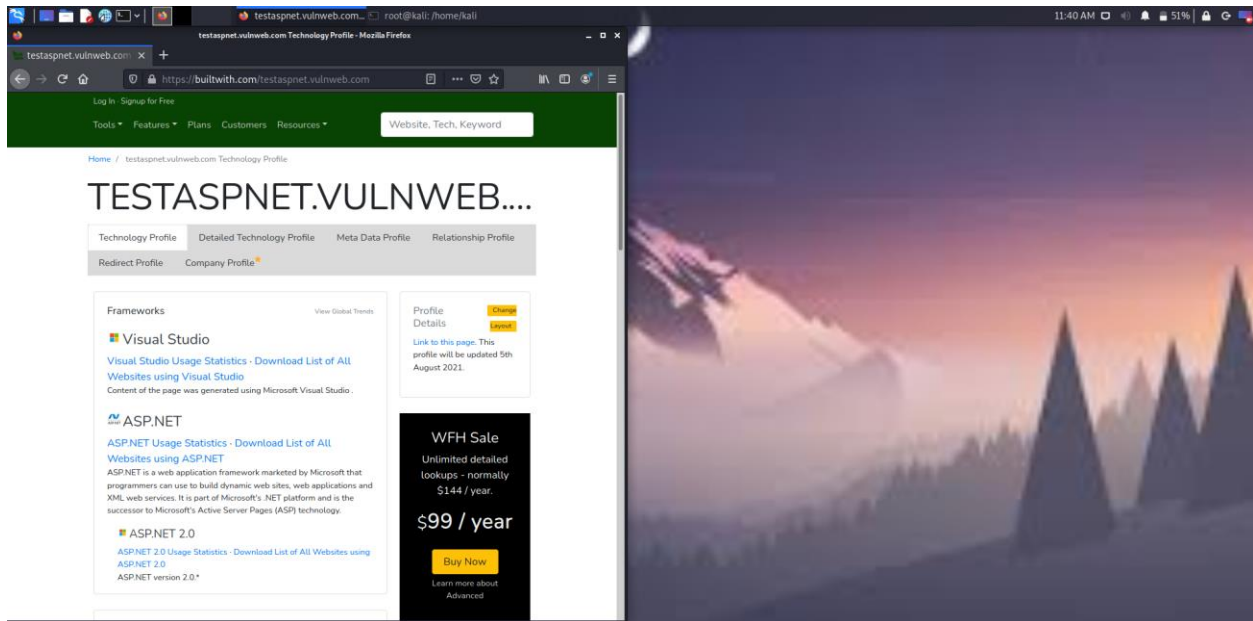
1.3 WAYBACK MACHINE



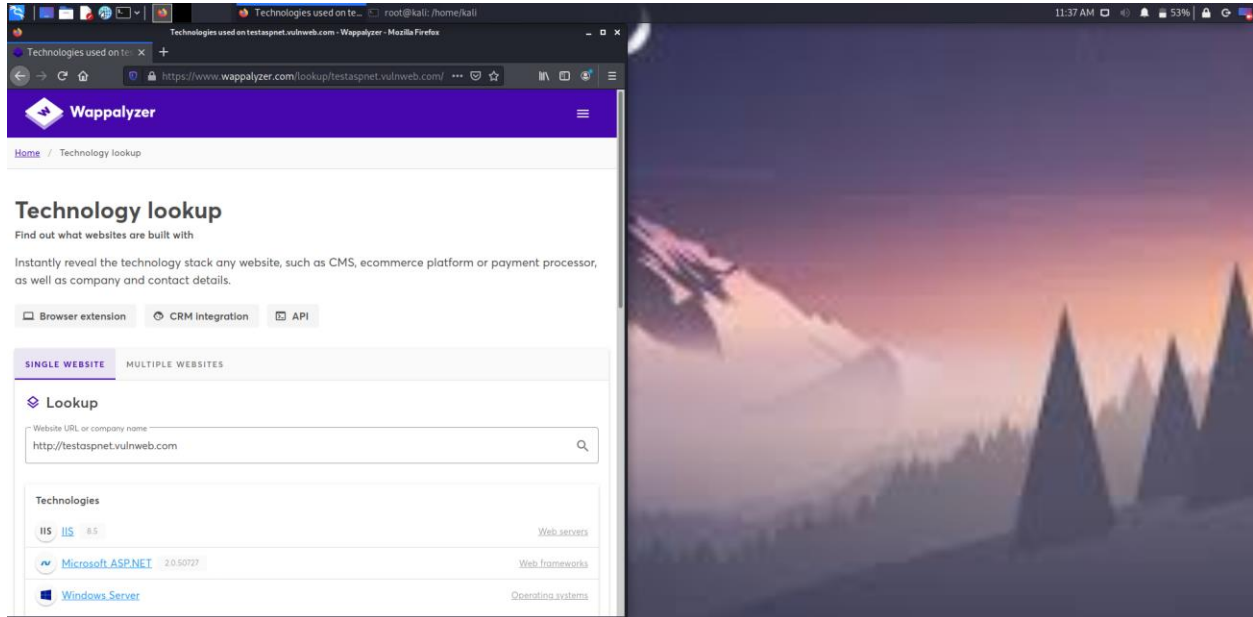
1.4 WOLFRAM ALPHA



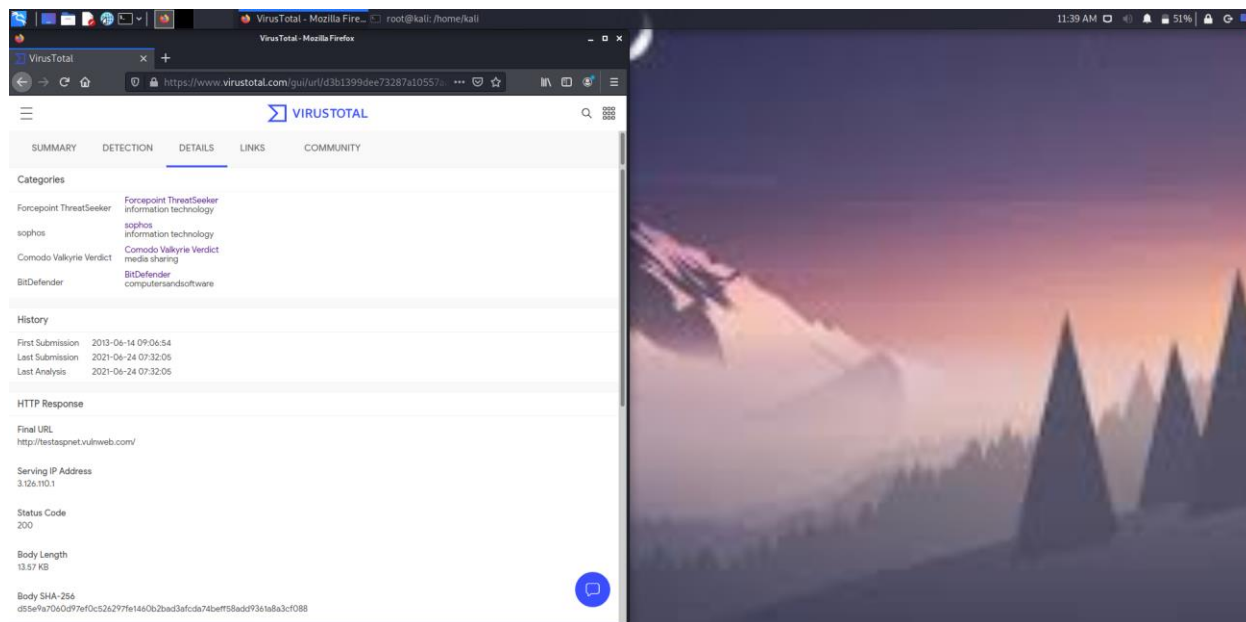
1.5 BUILTWITH.COM



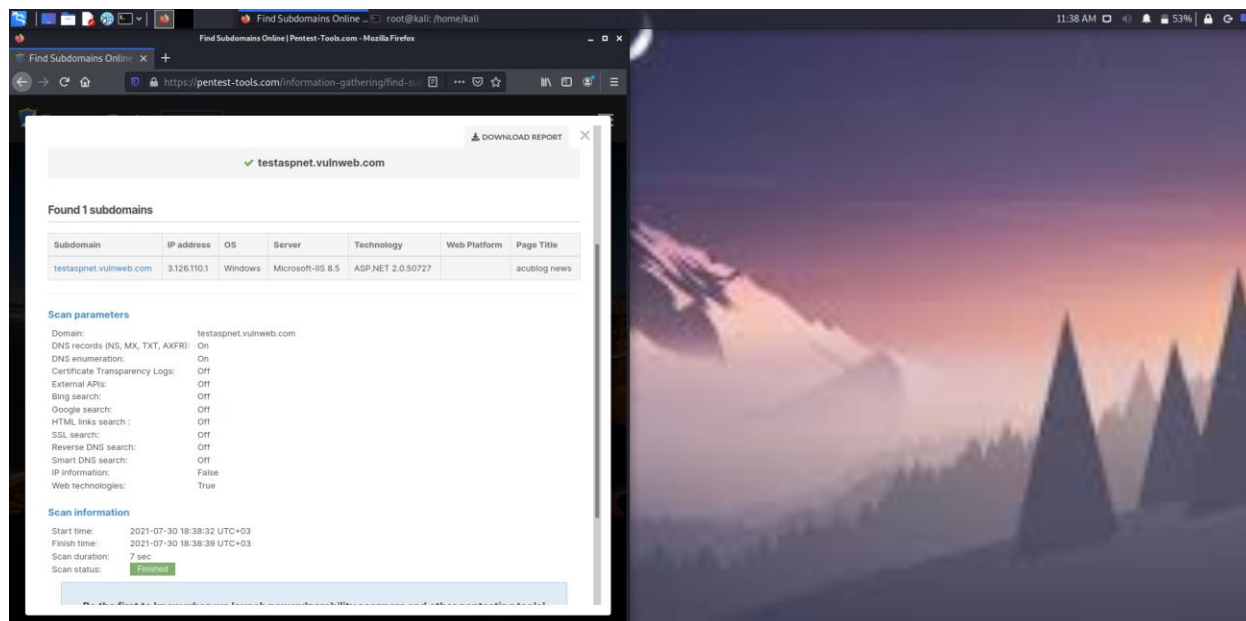
1.6 WAPPALYZER



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.

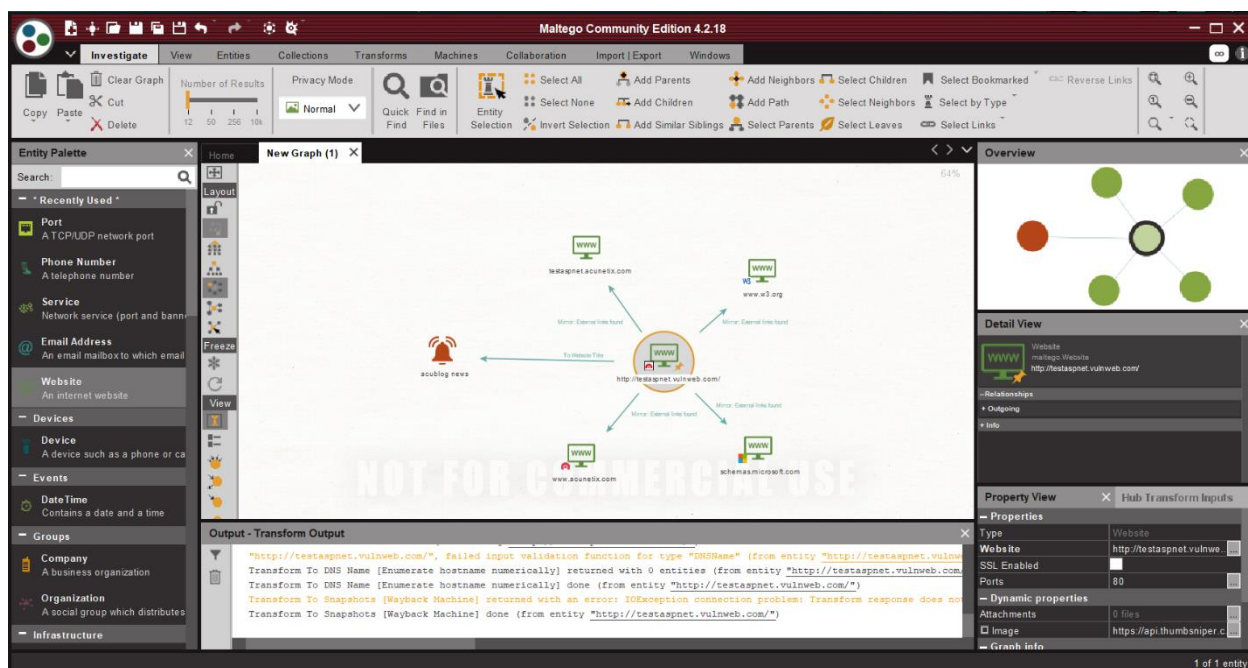
There are various methods used for this but we have gone with **Maltego**, **Recon-ng**, **UniScan** and **UnicornScan**.

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.

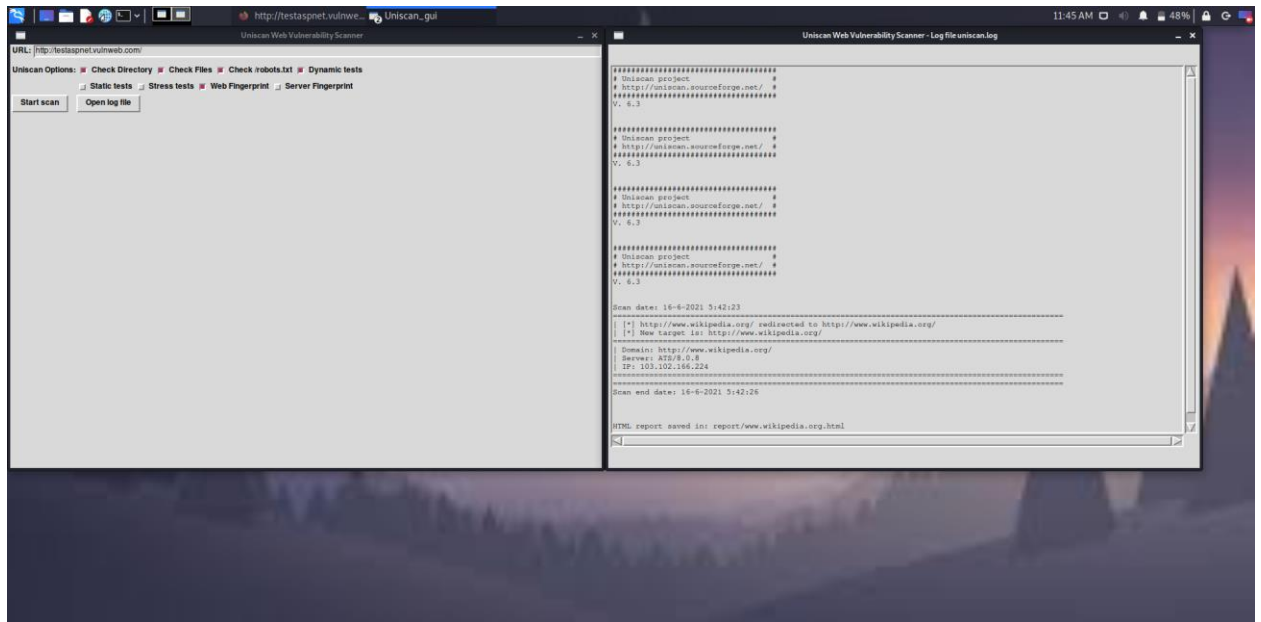
2.1 MALTEGO

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



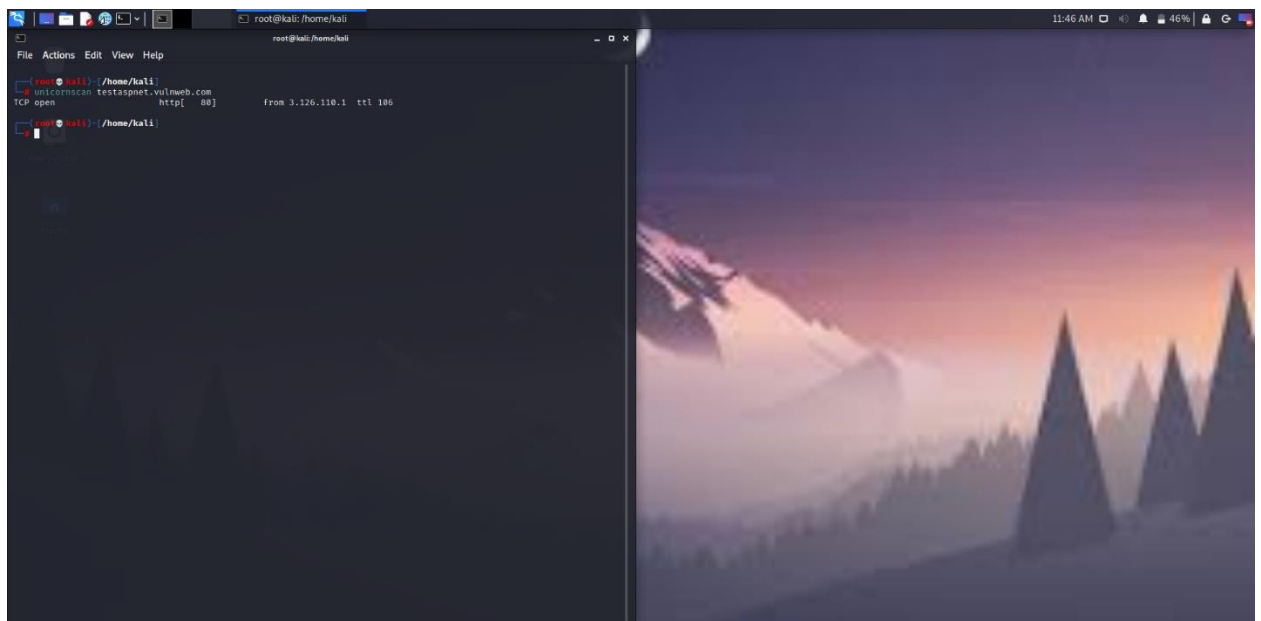
2.2 UNISCAN

- 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.

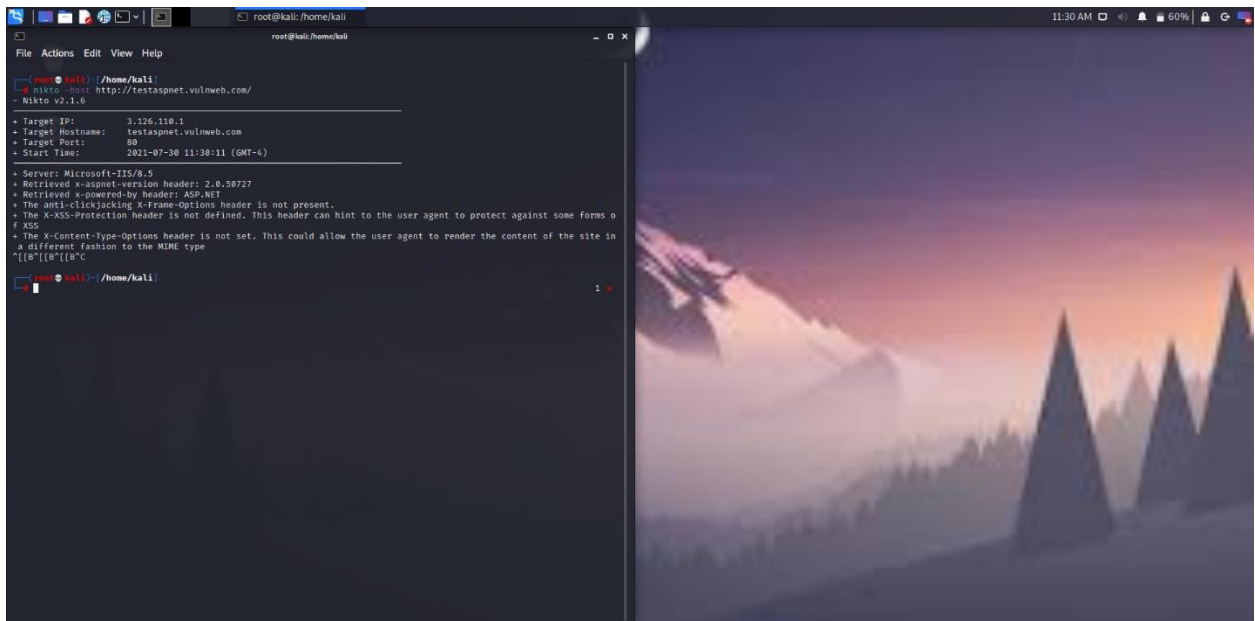
It is very useful for conducting vulnerability analysis and security assessments of the network.

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.

```

root@kali: /home/kali
nikto -hurl http://testaspnet.vulnweb.com/
- Nikto v2.1.6

+ Target IP: 3.126.110.1
+ Target Hostname: testaspnet.vulnweb.com
+ Target Port: 80
+ Start Time: 2021-07-30 11:30:11 (GMT-4)

+ Server: Microsoft-IIS/8.5
+ Retrieved x-aspnet-version header: 2.0.50727
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ [IP] [0] [0]

root@kali: /home/kali
nmap -sV 3.126.110.1 -o-

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-30 11:31 EDT
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.27% done; ETC: 11:38 (0:06:26 remaining)
Nmap scan report for ec2-3-126-110-1.eu-central-1.compute.amazonaws.com (3.126.110.1)
Host is up (0.14s latency).
Not shown: 65536 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 8.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

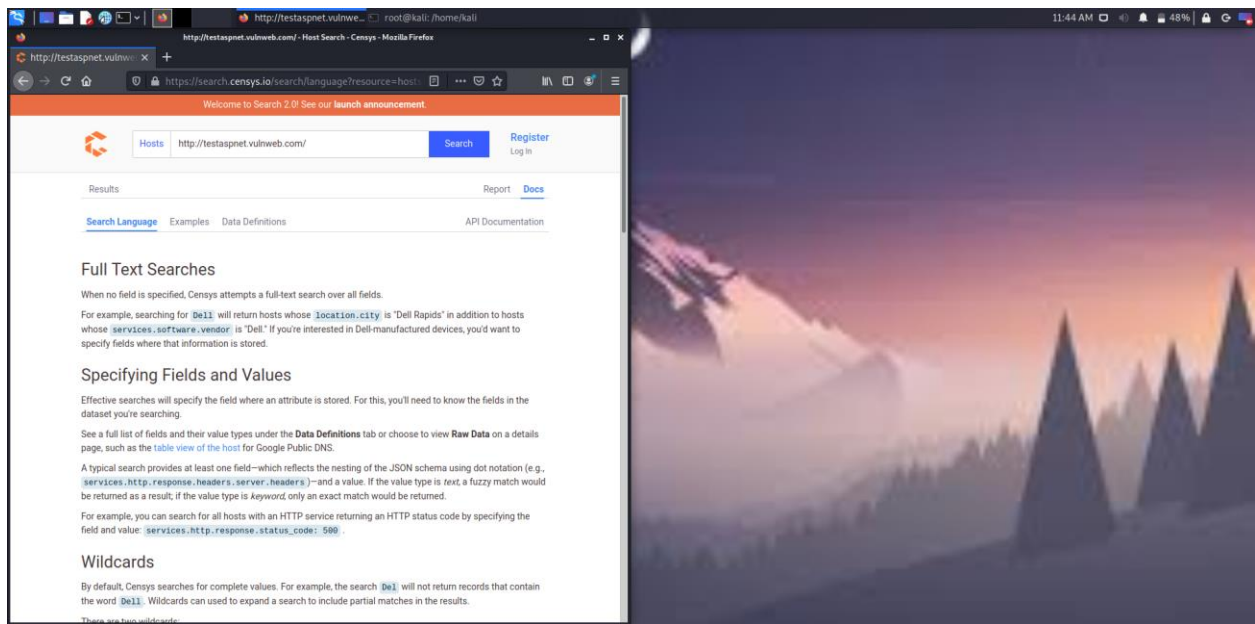
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 449.02 seconds

root@kali: /home/kali

```

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

