|  |  |
| --- | --- |
| A picture of a winding road and trees  Final-security lab-1 | Abstract  Security Information: A science specialized in securing information circulated over the Internet from the risks that threaten it.  Hasan Alhwietat  Security |

# Part 1: -

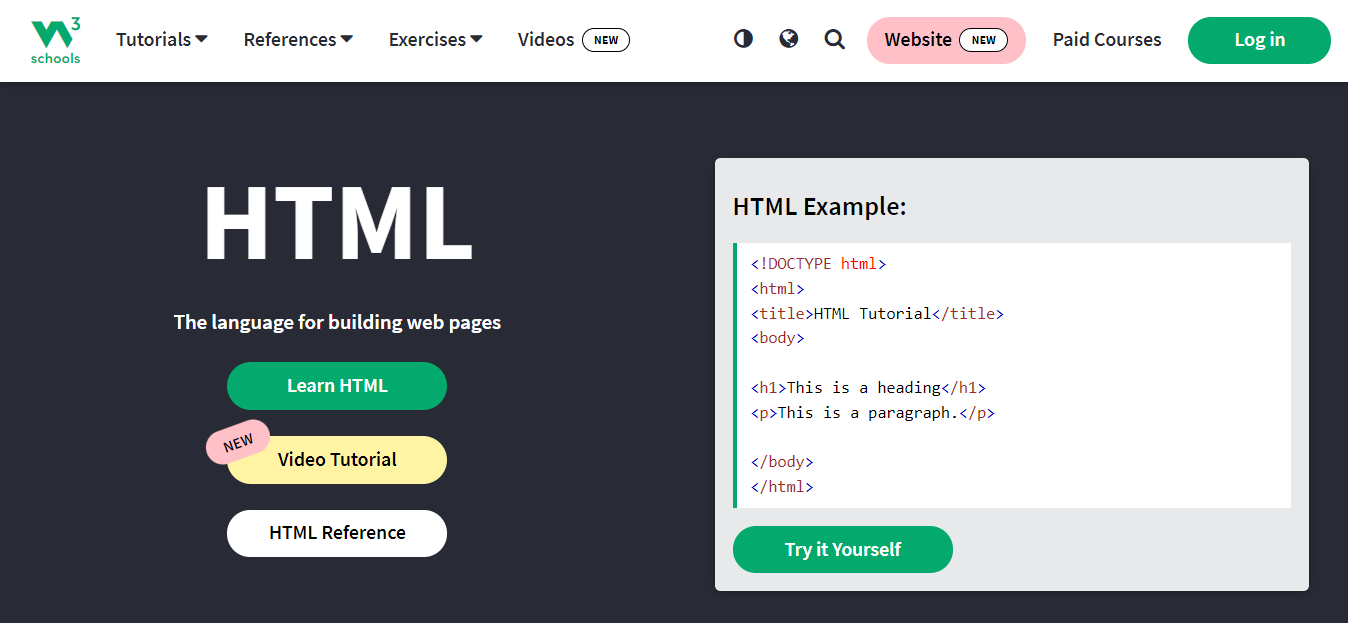
## 1-Determine domain name or public IP of your choice.

<https://www.w3schools.com> and IP address 13.248.240.135

## 2- Create formal report Contain the information about the domain.

Name domain: w3schools.com

Site information: It is an educational site to teach beginners or those who want to know some things related to programming languages.

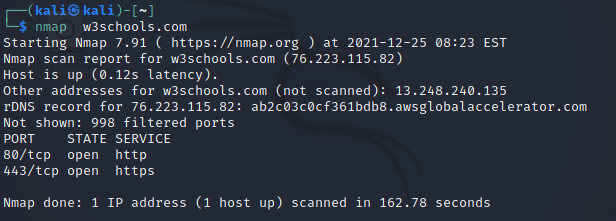


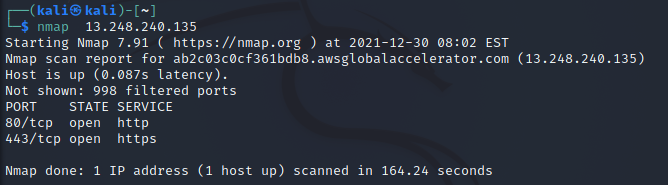
## 3- Scanning the domain or public IP and fill the result in the above report. And 4-You must use NMAP and Nessus tools.

### A-Nmap:

It is an open source Linux command line tool for network exploration and security auditing. With Nmap, server administrators can quickly discover hosts and services, look for security issues, and look for open ports. Nmap can review and discover open local and remote ports, as well as network and host information.

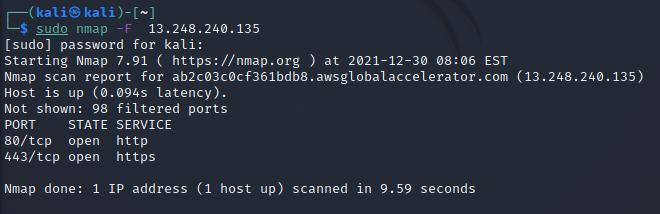
a. This code shows all ports and their status and services for this site.



b. This code shows all ports, their status, and services and for your device's IP address. 

c. If you need to do a quick check, you can use the "-F" flag. The "-F" flag will list the ports in the Nmap services files. Since the -F "Fast Scan" flag does not scan many ports, it is not exhaustive.

**This code shows ports and the name of the device and the IP address of the device and the Mac Address.**

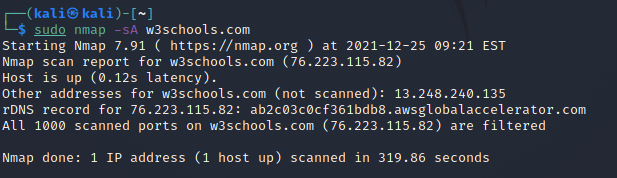


d. Scan to Find out Operating System Information.

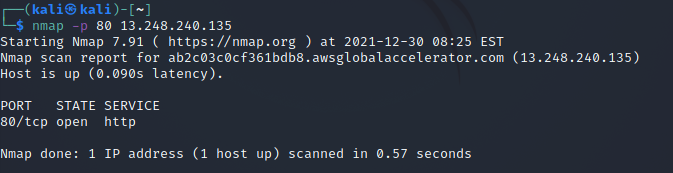
This code can also provide OS detection, script scanning, path tracing, and version detection. But it may not always be completely accurate.



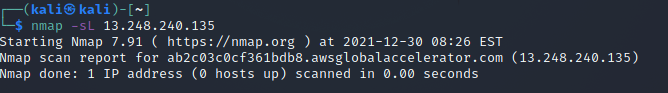
e. Scan to Detect Firewall Settings. Using the sA flag lets you know if the firewall is active on the host. This uses an ACK scan to receive the information.



f. scan for ports. By using the flag "-p" followed by the port, you can search for information regarding a specific port on a host.

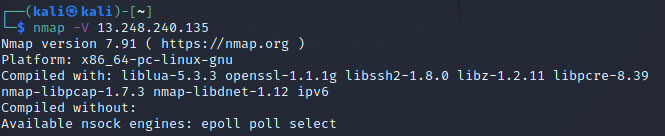


g. Identify Hostnames. The "-sL" flag will find the hostnames of the given host, completing a DNS query for each.



h. Get More Information with Verbose

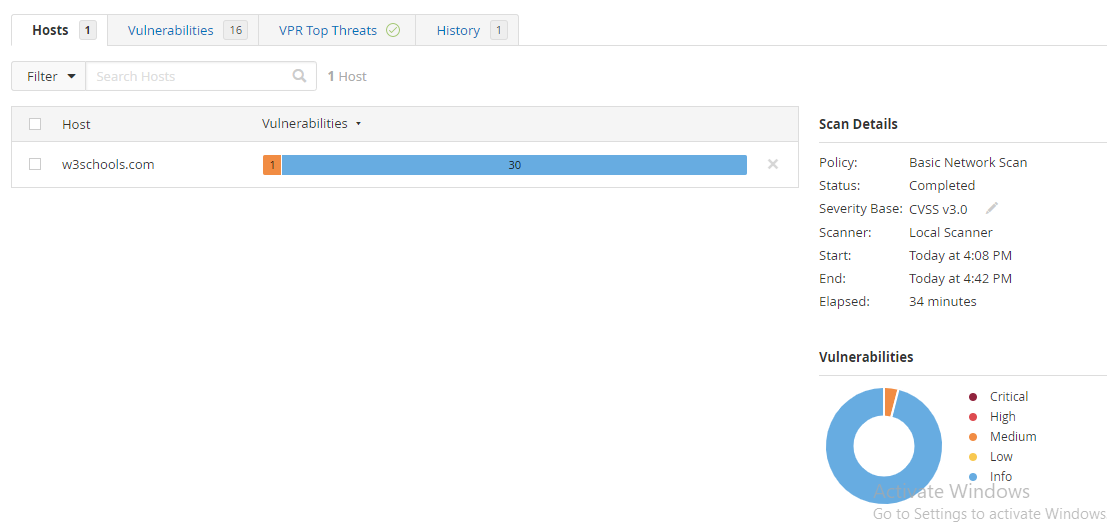
"-v" flag will provide additional information about the completed scan. It can be added to most commands to give more information. Without the "-v" flag, Nmap will generally return only important available information.



### B- Nessus:

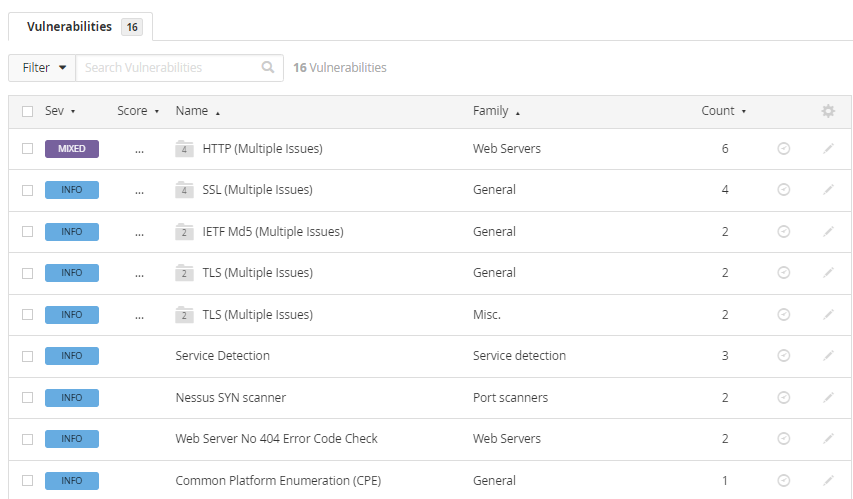
It’s a remote security scanning tool, which scans a computer and issues an alert if it detects any vulnerabilities that malicious hackers can use to gain access to any computer you have connected to a network.

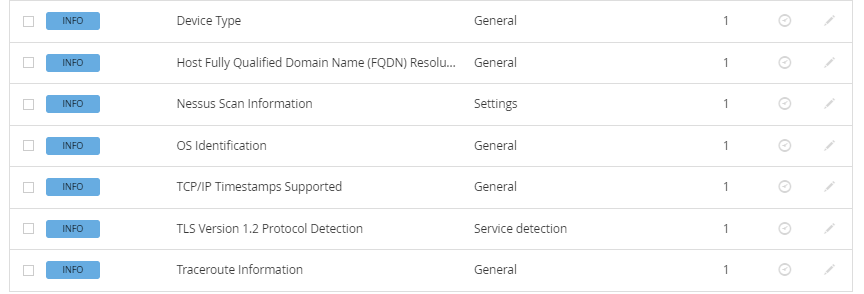
-Here I did a survey on this domain "w3schools.com" and resulted.



# Part 2: -

## 1- Scanning the vulnerabilities and mention in the report.





## 2-Describe the vulnerabilities and find the Severity it.

Critical: 0% High: 0% Medium: 4% Low: 0% Info: 96%



-- Describe:

The remote web server does not enforce Hypertext Transfer Protocol Strict Transfer Security, as defined by RFC 6797. Hypertext Transfer Protocol Strict Transfer Security is an optional response header that can be configured on the server to instruct the browser to communicate only via Hypertext Transfer Protocol Secure. The lack of Hypertext Transfer Protocol strict transfer security allows for downgrade attacks, Secure Sockets Layer attacks, man-in-the-middle attacks, and weakens protection from cookie hijacking.

-- Risk information:

-Risk Factor: Medium

-CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

-CVSS v2.0 Base Score: 5.8

CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

-- Hosts: w3schools.com (tcp/443).

## 3-Search the CVE in the internet and mention the reference.

I do not have CVE.