MODULE no:- 5

**Vulnerabilty Analysis**

Vulnerbality anlysis is a research where you can find vulnerability and determine the risk of it.

An administrator need to research vulnerability to gather information security threat , security issue , weakness of os .

An Administrator should know , how to migrate of its.

**What is vulnerability research**

When an Administrator examine the server or os in depth to check security procedure, identifying the weakness that may be exploited by an intruder it is known as Vulnerability research

There are two-way search network vulnerability

Active and Passive

As we know these two factor of active and passive

**Active** where attacker interact directly with the victim.

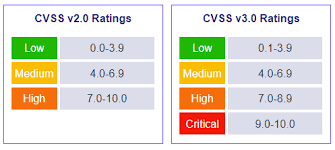
**Passive** where attacker gather info form web search and other platform as learn in footprinting and enumeration session

**Vulnerability scoring database**

**Basically threats have it own risk value , so according of it it get score**

**CVSS**  common vulnerability scoring system

Cvss provide a way to give numerical score according to its critical and risk .



* None - white (0.0)
* Low - green tones (0.1 - 3.9)
* Medium - yellow/light orange (4.0 - 4.9)
* High - orange (7.0 - 8.0)
* Critical - red (9.0 - 10.0)

***CVE: common vulnerabilities and Exposures***

Basically here every risk has Id which is know as CVE ID

Cve refers the security flaw which is assigned to that flaw or threats .

Source :- <https://cve.mitre.org/>

<https://cve.mitre.org/cve/search_cve_list.html>

Here we can check all cve list

**Vulnerability classification :-**

**Misconfiguration**:- It is mainly caused by human error, which allows an attacker to gain unauthorized access to the system.

**Default Installation :-** Many time device use default installation which is being used from previous time , user left it by thinking that it doesn’t contain any valuable information so why I should patch it , But attacker can gather all information of that device who is on the network of that device.

**Buffer Overflows** :- Buffer overflow occurs due to an error in code, which attacker takes advantage of it and tried to send data over limit so code cannot handle it. It causes a system crash, system become unstable, etc.

**Unpatched Servers:-** Many of the time organizations or user don’t update their os or use an update patches for carelessly , this is the main hub of hacker from which he can gain the access

**Design flaws :-** Design vulnerability is global flaws which occur due to incorrect encryption, poor validation of logic flaws , this vulnerability is exploited by hacker to gain access.

**Operating System flaws:-** Presence of worms , trojans or unwanted software in OS lead the attacker to do malicious script attack to steal the sensitive file.

**Application Flaws :-**  Application should me secured using the validation and authorization of user, if validation is a poor attacker can do data tampering or try to gain unauthorized access, it may cause us to loose sensitive data.

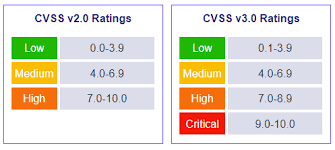
**Open Services:-** An administrator must check insecure ports or unwanted open ports , if it is open it increase the risk of network attack.

**Default Passwords:-** Many user left the default credential as it is given by many online organization. If user forgot to update the password and continue of using default credential. User device is vulnerable of brute force attack , dictionary attack.

**Vulnerablities Scoring**

**CVSS :-**  common vulnerability Scoribg system .

This is the method to give numerical score to threats.



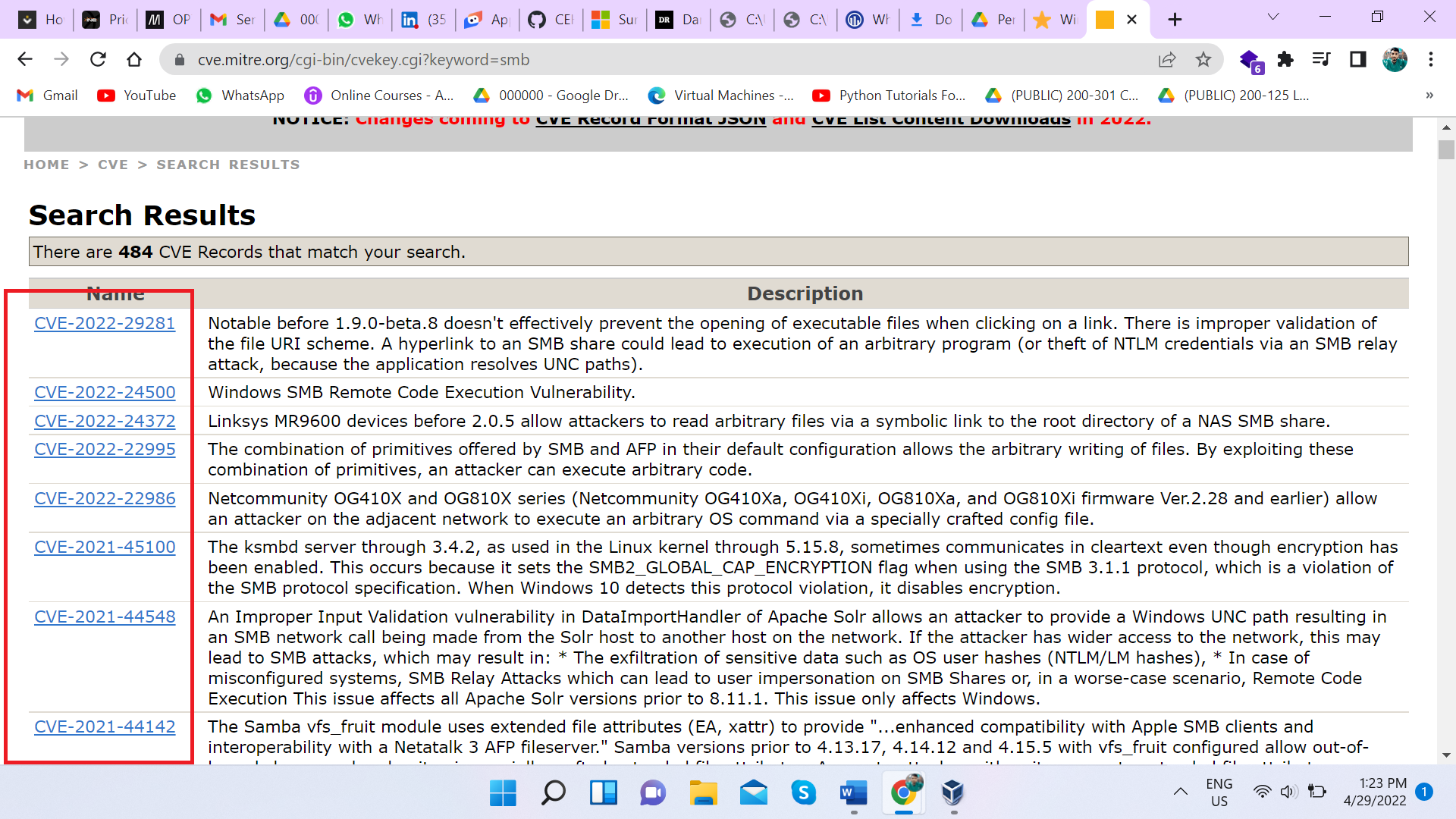
* None - white (0.0)
* Low - green tones (0.1 - 3.9)
* Medium - yellow/light orange (4.0 - 4.9)
* High - orange (7.0 - 8.0)
* Critical - red (9.0 - 10.0)

**Perform Vulnerability research in Common Vulnerability and Exposure**

* With same website we can research vulnerablity
* Search the keyword:- smb

**CVE :- Common vulnerability Exposure**

**Source:-** [**https://cve.mitre.org/**](https://cve.mitre.org/)



**NVD :- National vulnerability Database**

The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).

This is a list generated by automation in this checklist contains security-related flaws, product name, and impact.

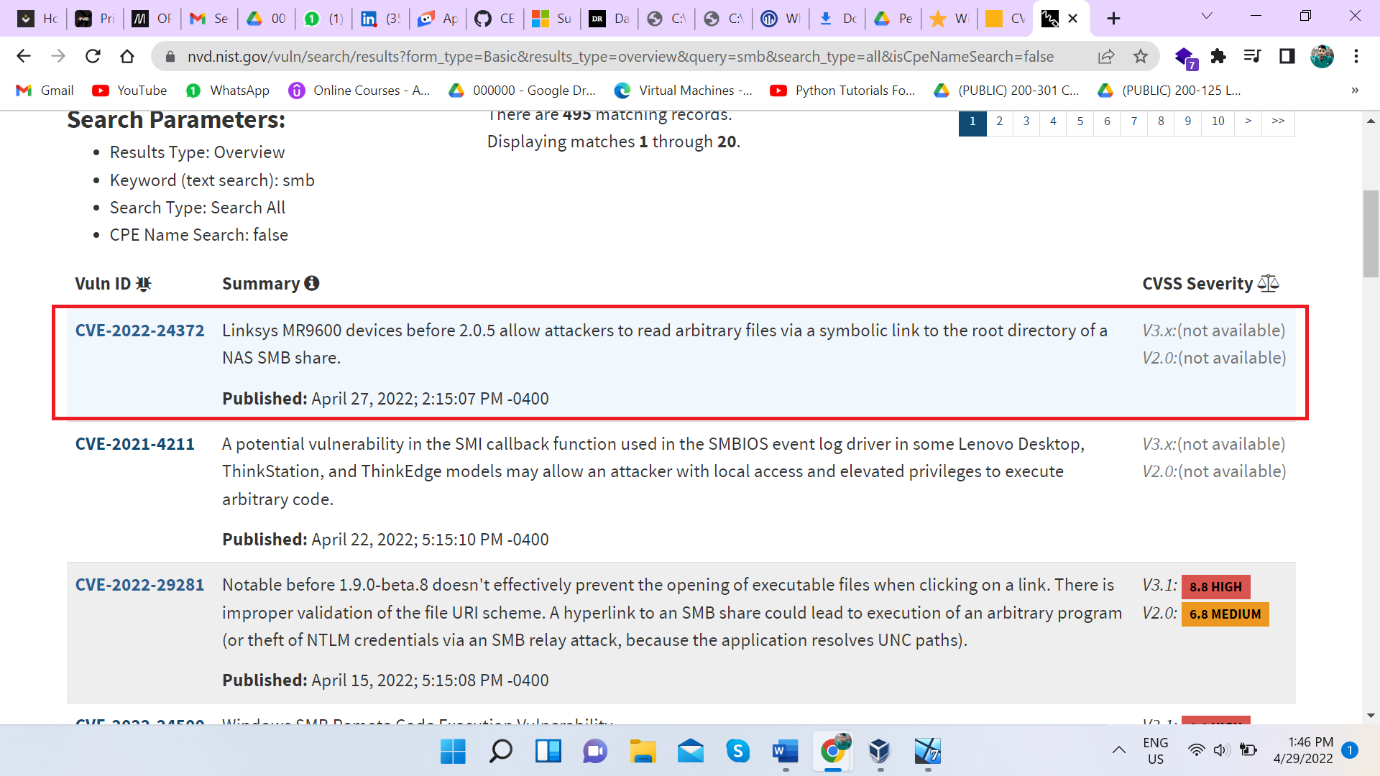
**Perform vulnerability research with NVD**

**Source :-** <https://nvd.nist.gov/>

Perform Vulnerability research Through Common Vulnerability Exposure

Search the keyword:- smb

We can see below Image

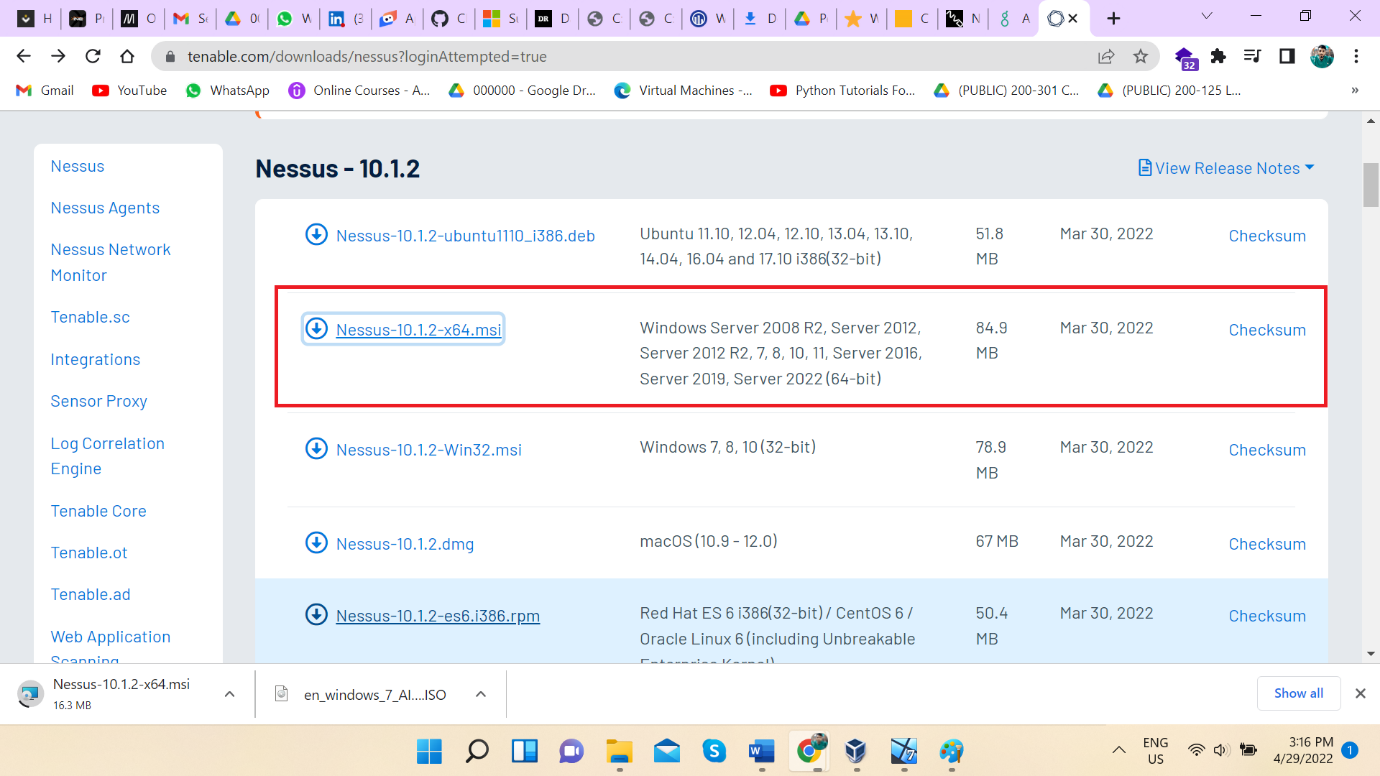


If we go through this we can find more detail , through this.

**Perform Vulnerability Scanning with Nessus**

Basically this tool is used to scan vulnerability and create report

Sources :- <https://www.tenable.com/downloads/nessus?loginAttempted=true>



Nessus ip :- <https://localhost:8834/#/>

**Perform Vulnerablity with NIKTO tool**

Command :- nikto -h craw.in