

# Vulnerability scanner

NETWORKS PROJECT

## What is Vulnerability Scanner

- A vulnerability scanner is a tool that scans computer systems or networks to identify potential security weaknesses or vulnerabilities that could be exploited by attackers. It compares information about the target system or network against a database of known vulnerabilities, coding bugs, and other security issues to identify any vulnerabilities. The scanner generates a report that lists the vulnerabilities found, their severity, and recommended actions to remediate them. This allows organizations to proactively identify and address potential security risks before they are exploited by attackers. Vulnerability scanners are commonly used by security professionals, IT administrators, and organizations to ensure that their systems and networks are secure and protected against potential attacks.

### 1. Description of the Application:

This is a Python script for a graphical user interface (GUI) for a vulnerability scanner. The script uses several libraries such as text wrap, tkinter, socket, and IPy to build the user interface and perform the vulnerability scanning.

The GUI includes input fields for entering an IP address and number of ports, a button for initiating the scan, and a table for displaying the results of the scan.

## 2. Description of the Functions and Classes:

- `wrap (string, length=100)`: This function takes a string and wraps it to a specified length.
- `port scan ()`: This is a class that includes methods for scanning ports. The constructor takes a target IP address and port number as input. The `scan ()` method scans for open ports on the target IP address and stores the results in the `open ports` and `banners` lists. The `check_ip()` method converts a URL into an IP address and converts the target IP address into an IP datatype. The `scan_port()` method scans a specific port for vulnerabilities and adds them to the `banners` list if found.
- `perform_scan(ip_address: str, num_ports: int) -> list[tuple[str, str, str]]` : This function takes an IP address and number of ports as input and returns a list of vulnerabilities found during the scan. It uses the `portscan()` class to perform the scan and reads vulnerability data from a file. It then checks the banners of each open port for vulnerabilities and adds them to the `data` list if found.
- GUI functions:
  - `button_pressed()` : This function is called when the "Scan" button is pressed. It retrieves the IP address and number of ports from the input fields, performs the scan using `perform_scan()` , and populates the vulnerability table with the results.
  - `root` : This is the main tkinter window that displays the GUI.
  - `label_ip` , `ip_address_input` , `label_num_ports` , `num_ports_input` , `label_output` , `scan_button` : These are various tkinter widgets that make up the input fields, output label, and scan button in the GUI.

- table : This is the Treeview widget that displays the results of the vulnerability scan.

### 3.The models, frameworks, and protocols used in the implementation:

- Models:

This uses a port scanning algorithm to identify open ports on a target IP address and checks the banner messages received from open ports for known vulnerabilities. The script also reads vulnerability data from a file to compare with the banner messages.

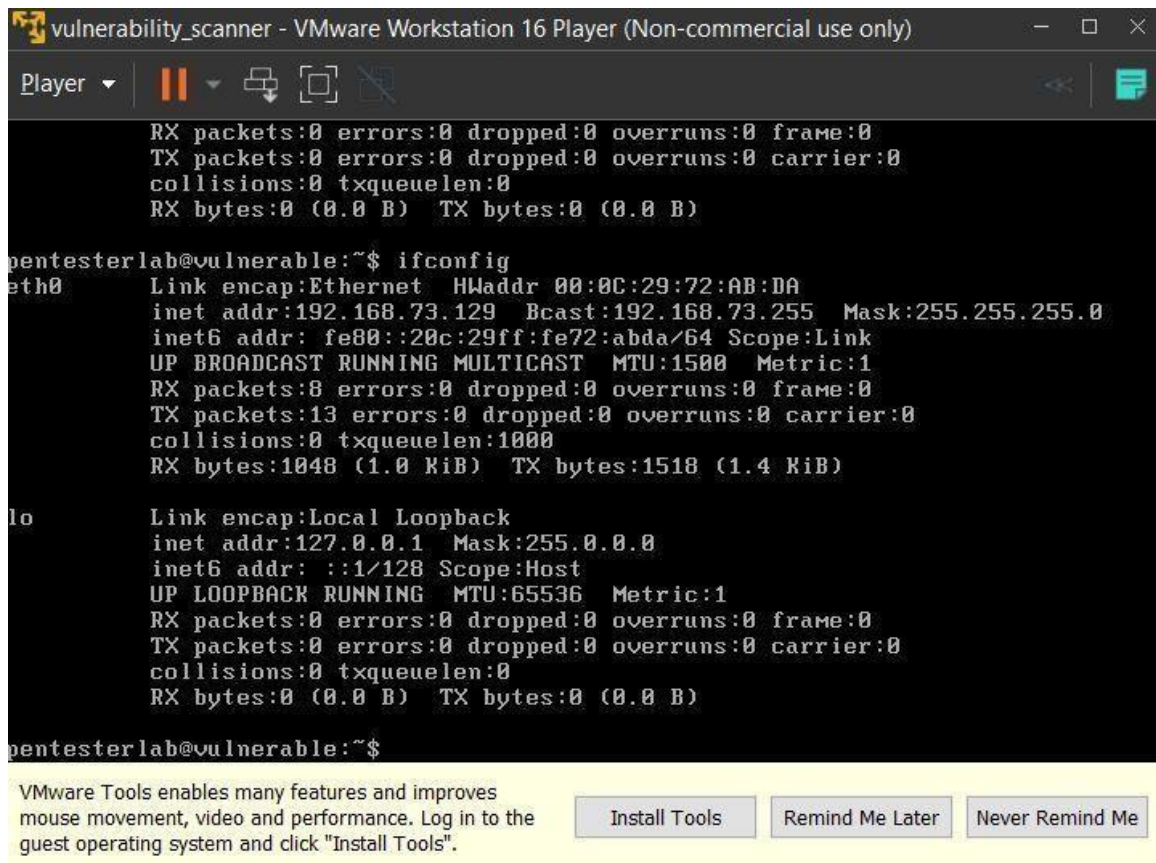
- 2. Frameworks:

The script uses the tkinter framework to create a (GUI) for the vulnerability scanner. tkinter is a standard Python library for creating GUI applications and is included in most Python installations. The script also uses the IPy library, which provides tools for working with IP addresses and networks.

- 3. Protocols:

The script uses (TCP) to scan for open ports and check the banner messages of network services. The script also uses the Internet Protocol (IP) to specify the target IP address to scan. IP is the primary protocol used for communication between devices on the Internet.

- Virtual machine that runs an IP address gowah vulnerability in this case el address 192.168.73.129



```
vulnerability_scanner - VMware Workstation 16 Player (Non-commercial use only)
Player
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

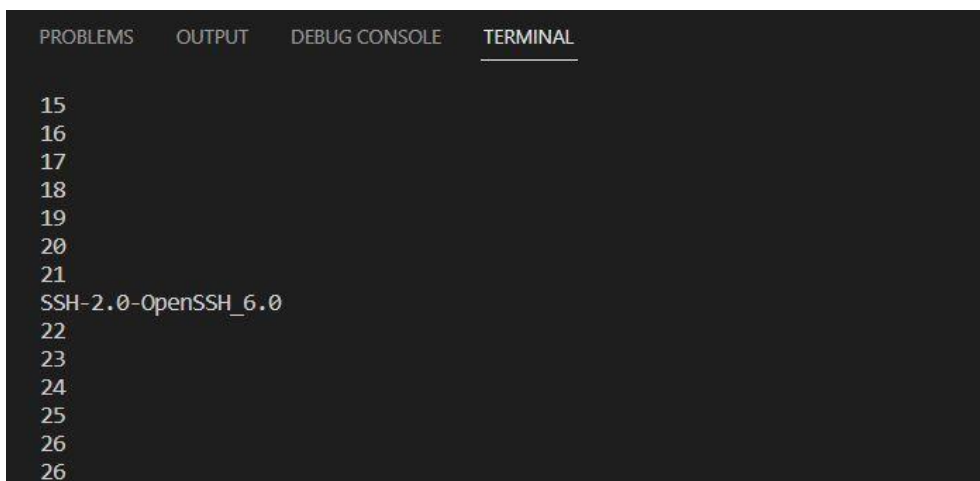
pentesterlab@vulnerable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:72:AB:DA
          inet addr:192.168.73.129  Bcast:192.168.73.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe72:abda/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1048 (1.0 KiB)  TX bytes:1518 (1.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

pentesterlab@vulnerable:~$

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
[Install Tools] [Remind Me Later] [Never Remind Me]
```

- When we run code and input two things. The IP address and number ports we want to scan.
- For example IP is 192.168.73.129 and scan 30 ports it outputs a vulnerability named SSH-2.0-OpenSSH\_6.0 at port number 22



The image shows a terminal window with a dark background. At the top, there are four tabs: 'PROBLEMS', 'OUTPUT', 'DEBUG CONSOLE', and 'TERMINAL'. The 'TERMINAL' tab is selected and underlined. Below the tabs, a list of numbers representing ports is displayed: 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 26. The number 22 is highlighted in green, and next to it, the text 'SSH-2.0-OpenSSH\_6.0' is displayed in green, indicating a vulnerability found at that port.

- GUI example for the above figure it find 9 exploits (including its severity and description)

Vulnerability Scanner

Enter IP address

Enter number of ports

9 vulnerabilities found for 192.168.73.129 on 30 ports

Exploit	Severity	Description
CVE-2002-1715	7.2	SSH 1 through 3 and possibly other versions allows local users to bypass restricted shells such as rbash or r
CVE-2002-1645	10.0	Buffer overflow in the URL catcher feature for SSH Secure Shell for Workstations client 3.1 to 3.2.0 allows r
CVE-2002-1644	7.2	SSH Secure Shell for Servers and SSH Secure Shell for Workstations 2.0.13 through 3.2.1 when running without a

Scan

- Data base which check the vulnerability have what exploits

```
Computer Networks > vulnerability scanner > download.txt
1  vulnerability,exploit,severity,description
2  SSH-2.0-OpenSSH_6.0,CVE-2002-1715,7.2,SSH 1 through 3 and possibly other versions allows local users to bypass restricted shells such as rbash or r
3  SSH-2.0-OpenSSH_6.0,CVE-2002-1645,10.0,Buffer overflow in the URL catcher feature for SSH Secure Shell for Workstations client 3.1 to 3.2.0 allows r
4  SSH-2.0-OpenSSH_6.0,CVE-2002-1644,7.2,SSH Secure Shell for Servers and SSH Secure Shell for Workstations 2.0.13 through 3.2.1 when running without a
5  SSH-2.0-OpenSSH_6.0,CVE-2001-0364,5.0,Partial SSH Communications Security sshd 2.4 for Windows allows remote attackers to create a denial of servi
6  SSH-2.0-OpenSSH_6.0,CVE-2000-0217,5.1,The default configuration of SSH allows X forwarding which could allow a remote attacker to control a client's
7  SSH-2.0-OpenSSH_6.0,CVE-1999-1231,5.0,ssh 2.0.12 and possibly other versions allows valid user names to attempt to enter the correct password multip
8  SSH-2.0-OpenSSH_6.0,CVE-1999-1159,4.6,SSH 2.0.11 and earlier allows local users to request remote forwarding from privileged ports without being ro
9  SSH-2.0-OpenSSH_6.0,CVE-1999-1029,7.5,SSH server (sshd2) before 2.0.12 does not properly record login attempts if the connection is closed before th
10 SSH-2.0-OpenSSH_6.0,CVE-1999-0398,4.6,In some instances of SSH 1.2.27 and 2.0.11 on Linux systems SSH will allow users with expired accounts to logi
11 dummy,dummy,dummy,dummy
```