WEB-PROWLER Vulnerability Scanner

JEJO.J & **PADMESH.PS**
First year of B.E CSE (Cybersecurity)
Sri Krishna College of Technology ,
Coimbatore, Tamil Nadu, india.

Abstract:

The WEB-PROWLER Vulnerability Scanner is an open-source project designed to elevate the standards of web security assessment. Leveraging the potent capabilities of Nmap and the Tor framework, this scanner provides a sophisticated analysis of a target's open ports, services, and potential vulnerabilities. Its influence extends beyond mere website assessment; it serves as a robust tool for business owners to proactively identify and address security issues within their web infrastructure.

The Nmap integration facilitates detailed port scans, revealing open ports, services, and version information, enabling a comprehensive understanding of the target's network. The script then cross-references this data with the Exploit Database using the `searchsploit` command, reporting potential exploits with precision.

Unique to WEB-PROWLER is the stealth scan option, employing the Tor framework for discreet identification of vulnerabilities, minimizing the risk of detection. The interactive menu offers flexibility, allowing users to choose scanning options tailored to their needs, from fast scans to comprehensive assessments.

Crucially, the scanner emphasizes education, with a cautionary message and a focus on responsible usage for enhancing website security. It is positioned not only as a valuable resource for business security assessments but also as a tool for security professionals to efficiently analyze target networks and servers.

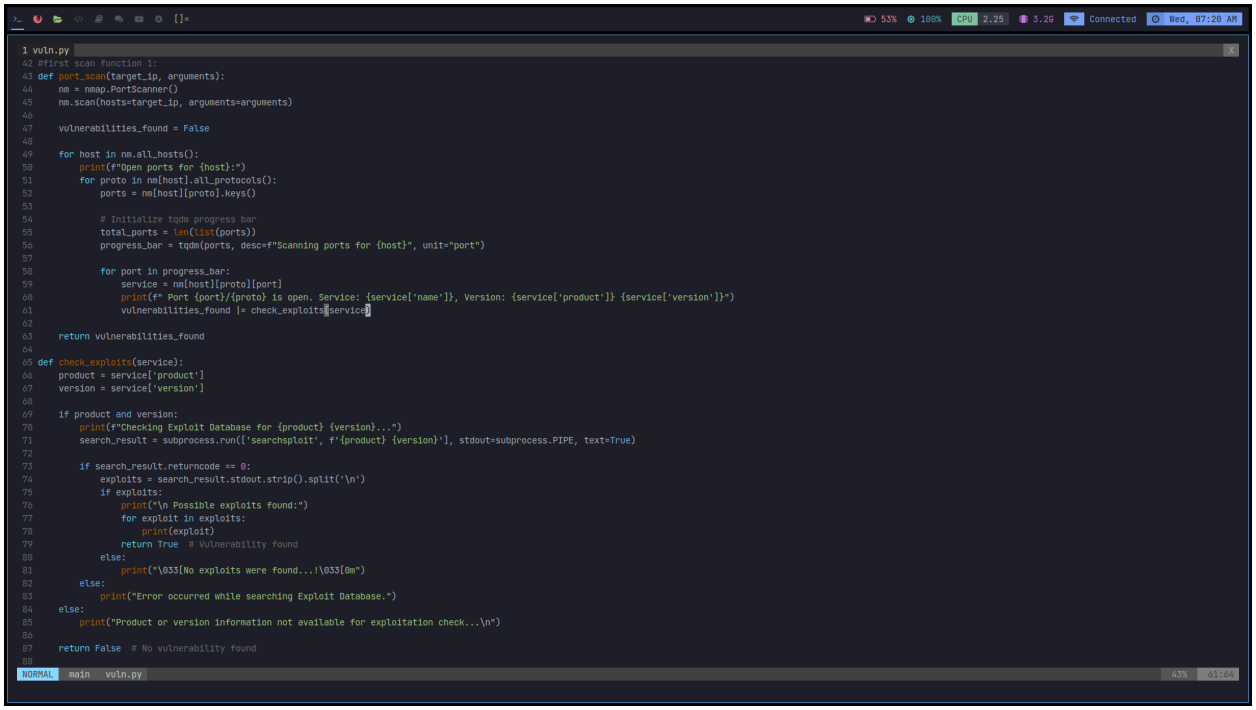
WEB-PROWLER stands as a testament to the power of collaboration in cybersecurity. Being an open-source project, it extends an invitation to students and developers to contribute and shape its evolution. Its impact on cybersecurity lies not only in its ability to identify vulnerabilities but in its potential to foster a community committed to enhancing web security.

In conclusion, WEB-PROWLER is a powerful and versatile vulnerability scanner, embodying the principles of open-source collaboration and responsible usage. As businesses navigate the evolving landscape of cybersecurity threats, this tool stands as a valuable asset in fortifying web infrastructure and cultivating a community dedicated to digital defense.

1. Introduction:

WEB-PROWLER stands as a testament to the power of open-source collaboration in the realm of cybersecurity. Developed as a sophisticated open-source vulnerability scanner, it is meticulously designed to assess the security of websites by identifying open ports and potential vulnerabilities. Leveraging the capabilities of Nmap and the Tor framework, this tool provides a comprehensive analysis of a target's open ports, services, and potential exploits.

In an era where cybersecurity threats are evolving at an unprecedented pace, WEB-PROWLER emerges as a robust solution, empowering business owners and security professionals alike. The seamless integration of cutting-edge technologies such as Nmap and Tor makes it a potent tool in the arsenal against cyber threats. This open-source project not only provides a powerful and versatile solution for vulnerability assessment but also invites collaboration, fostering a community-driven approach to enhancing web security.



```
1 vuln.py
#first scan function 1:
def port_scan(target_ip, arguments):
    nm = nmap.PortScanner()
    nm.scan(hosts=target_ip, arguments=arguments)

    vulnerabilities_found = False

    for host in nm.all_hosts():
        print(f"Open ports for {host}:")
        for proto in nm[host].all_protocols():
            ports = nm[host][proto].keys()

            # Initialize tqdm progress bar
            total_ports = len(list(ports))
            progress_bar = tqdm(ports, desc=f"Scanning ports for {host}", unit="port")

            for port in progress_bar:
                service = nm[host][proto][port]
                print(f" Port {port}/{proto} is open. Service: {service['name']}, Version: {service['product']} {service['version']}")
                vulnerabilities_found |= check_exploits(service)

    return vulnerabilities_found

def check_exploits(service):
    product = service['product']
    version = service['version']

    if product and version:
        print(f"Checking Exploit Database for {product} {version}...")
        search_result = subprocess.run(['searchsploit', f'{product} {version}'], stdout=subprocess.PIPE, text=True)

        if search_result.returncode == 0:
            exploits = search_result.stdout.strip().split('\n')
            if exploits:
                print("\n Possible exploits found:")
                for exploit in exploits:
                    print(exploit)
                return True  # Vulnerability found
            else:
                print("\033[No exploits were found...!\033[0m")
        else:
            print("Error occurred while searching Exploit Database.")
    else:
        print("Product or version information not available for exploitation check...\n")

    return False  # No vulnerability found

NORMAL  main  vuln.py
```

2. Features:

Nmap Integration:

WEB-PROWLER utilizes the Nmap tool to perform detailed port scans on the specified target. Open ports, services running on those ports, and version information are gathered to provide a thorough understanding of the target's network.

Exploit Database Integration:

The script cross-references the obtained service information with the Exploit Database using the `searchsploit` command. If potential exploits are found, they are reported to the user, including the port number and the name of the exploit.

Stealth Scan with Tor:

WEB-PROWLER features a stealth scan option that utilizes the Tor framework for enhanced stealthiness. This option is particularly useful for discreetly identifying vulnerabilities while minimizing the risk of detection.

Interactive Menu:

Users are presented with an interactive menu, allowing them to choose from various scanning options. The menu provides flexibility, with options for fast scans, comprehensive scans, stealth scans, and nslookup.

File Output:

When potential exploits are identified, they are saved to a file named `possible_exploits.txt`. This file serves as a detailed record of the vulnerabilities found during the scanning process.

Educational Emphasis:

The script includes a cautionary message, emphasizing that it is intended for educational purposes only. Business owners are encouraged to use the tool responsibly to enhance the security posture of their websites.

3. Use Cases:

Business Security Assessment:

WEB-PROWLER is a valuable tool for business owners to assess the security of their websites. Regular scans can identify and address vulnerabilities in open ports, minimizing the risk of cyberattacks.

Proactive Vulnerability Management:

By leveraging the script's ability to check for exploits, businesses can proactively manage and mitigate potential security risks. Timely identification of vulnerabilities allows for prompt remediation.

Stealthy Security Audits:

The stealth scan option, utilizing the Tor framework, enables discreet security audits. This is crucial for businesses that prioritize a low-profile approach to vulnerability assessments.

4. Recommendations:

Dependency Check:

Ensure that the necessary dependencies, including Nmap, Tor, and searchsploit, are installed and configured properly.

Permissions:

Depending on the selected scanning option, users may need elevated privileges, especially for stealth scans.

Exploit Database Updates:

Regularly update the Exploit Database to ensure access to the latest information on potential exploits.

Tools Used in Vulnerability Scanner (WEB-PROWLER):

1. Nmap:

Nmap (Network Mapper) is a robust open-source tool used for network exploration and security auditing. In the WEB-PROWLER script, Nmap is employed for port scanning, enabling the identification of open ports on a target system. It provides detailed information about the services running on those ports, including version details. Nmap's versatility and efficiency make it a cornerstone tool for comprehensive network reconnaissance.

2. Tor:

Tor, short for "The Onion Router," is integrated into WEB-PROWLER to facilitate stealthy and anonymous scanning. Tor routes network traffic through a series of volunteer-operated servers, enhancing privacy and making it difficult to trace the origin of the scan. The use of Tor in the script's stealth scan option enables a low-profile approach to vulnerability assessment, crucial for discreet security audits.

3. nslookup:

The `nslookup` command is utilized in WEB-PROWLER for DNS (Domain Name System) lookups. It translates user-provided website names into corresponding IP addresses. This functionality enhances the script's usability by allowing users to target websites by name rather than requiring IP addresses. nslookup is crucial for obtaining the necessary IP address information for subsequent vulnerability assessments.

4. tqdm:

The `tqdm` library is incorporated into the WEB-PROWLER script to enhance the user experience during the scanning process. tqdm provides dynamic and interactive progress bars, allowing users to visualize the progress of the port scan and estimate the remaining time. This adds a level of interactivity to the script, making it more user-friendly and informative.

5. searchsploit:

`searchsploit` is a command-line tool used to interact with the Exploit Database. In WEB-PROWLER, searchsploit is employed to cross-reference the services identified during port scanning with known exploits. It searches the Exploit Database for potential vulnerabilities based on specific software and version information. If potential exploits are found, they are reported to the user, contributing to a more comprehensive vulnerability assessment.

Conclusion:

The integration of Nmap, Tor, nslookup, tqdm, and searchsploit in the WEB-PROWLER Vulnerability Scanner results in a powerful and versatile tool for conducting security assessments. Each tool plays a unique role, collectively enabling the identification of open ports, assessment of potential vulnerabilities, and maintenance of a discreet and privacy-focused approach when needed. Users are encouraged to understand the functionalities of these tools and use them responsibly and ethically in compliance with legal standards.

WEB-PROWLER is a powerful and versatile vulnerability scanner that combines the capabilities of Nmap and the Tor framework to provide a comprehensive security assessment for websites. Business owners can leverage this tool to identify and address potential vulnerabilities in their open ports, ultimately enhancing the overall security posture of their online assets. However, users are reminded to use this tool responsibly, adhering to ethical and legal standards. Regular updates and proactive vulnerability management are key to maintaining a secure web infrastructure.

CONTACTS:

GITHUB : https://github.com/jejo205713/vulnerablity-scanner/

LINKEDIN:

IG:
@_jejo_j
@i.m_padmesh

EMAIL:
jejo205713@gmail.com
padmesh77123@gmail.com