Laud Mills

1. Write down the purpose and function of following penetration testing Tools. Also define whether it is an open source or paid version is available?

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Purpose** | **Functionality** | **Open Source/Professional paid version?** |
| Wireshark | Traffic monitoring and analysis | Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. | Open Source |
| tcpdump | It is a network packet analyzer that is used to capture and display the data traveling over a network. | Tcpdump displays captured packets in human-readable format, showing information such as the source and destination IP addresses, protocol types (TCP, UDP, ICMP), and the contents of each packet | Open source |
| Skip fish | It is an active web application security scanner designed to identify security vulnerabilities in web applications. | Skipfish automates the process of scanning a web application for various vulnerabilities, such as SQL injection, XSS, and other web-specific security issues. | Open source |
| Nikto | It scans web servers for potential threats such as outdated software, misconfigurations, insecure files, and common vulnerabilities like cross-site scripting (XSS), SQL injection, and more. | Nikto scans web servers and identifies potential security flaws or misconfigurations that could be exploited by attackers. It checks for common vulnerabilities, including outdated software versions, security holes, insecure HTTP methods, and other potential weaknesses. | Open Source |
| OpenVAS | OpenVAS is an open-source vulnerability scanning and management tool designed to assess the security of networked systems, such as servers, routers, and firewalls, by identifying vulnerabilities and weaknesses in the system. | OpenVAS performs in-depth security scans of systems to identify vulnerabilities like misconfigurations, unpatched software, insecure protocols, and other weaknesses. It scans a range of systems, including operating systems, network services, and applications, to identify potential security risks. | Open Source and Paid version (Greenbone Vulnerability Management) |
| Nessus | Nessus is a widely used vulnerability scanner designed to identify security weaknesses and vulnerabilities in IT systems, such as servers, network devices, and web applications. | Nessus performs in-depth scans of networked systems to detect vulnerabilities in operating systems, services, databases, and applications. It includes templates and plugins that help organizations ensure they meet various compliance standards, including PCI-DSS, HIPAA, and GDPR | Paid but has free version (Nessus Essentials) |
| Burp | Burp Suite is a comprehensive web application security testing tool primarily used for identifying and exploiting vulnerabilities in web applications. | Burp Suite’s core feature is its intercepting proxy, which allows testers to intercept, modify, and analyze HTTP/HTTPS traffic between the browser and the target web server. This helps in analyzing requests and responses to uncover vulnerabilities. | Paid and Unpaid versions available |

1. Write down the Top OWASP vulnerabilities. Map the vulnerability according to the given action. You can refer to the OWASP Vulnerability document to understand list of vulnerability for following items: <https://owasp.org/www-community/vulnerabilities/>.

Below is the list of vulnerabilities that you need to map with each input item:

* Broken access control
* Buffer Overflow
* Broken authentication
* Carriage Return and Line Feed (CRLF) Injection
* Cross-site scripting (XSS)
* Cross-site request forgery (CSRF)
* Improper certificate validation
* Poor Credentials management

|  |  |
| --- | --- |
| **Action** | **Vulnerability** |
| They can escalate the privileges and give the additional user ID an access within the system, that impact data confidentiality, integrity, or availability. | Broken Authentication |
| leverages social engineering methods to get a user to change information, like username or password, in an application. |  |
| This exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. | Buffer Overflow |
| The malicious user gains unauthorized access to the systems, networks, and software because the company failed to adequately set appropriate identity and access management controls. | Broken Access Control |
| Attackers create a false trusted entity that tricks the server or application into thinking the certificate is valid, so it accepts the data transfer as legitimate. | Improper Certificate Validation |
| The inserted code changes the way that the web application responds to commands. This can be used to either disclosure sensitive information or execute code. | Carriage Return and Line Feed (CRLF) Injection |
| When the user opens the web page on their browser, the malicious code downloads and executes in the browser. For example, the code may redirect users from a legitimate site to a malicious one. | Cross-site scripting (XSS) |
| Makes it easy for attackers to steal credentials and use them to gain access to web applications. | Poor Credentials Management |

1. List out 10 SQL Injection tools that attackers can used to exploit the a web application.

They are : SQLmap, Havij, Burp Suite, Acunetix, OWASP ZAP, Nikto, jSQL Injection, SQLNinja, PentesterLab, XSSer

1. Why is it critical to perform periodic web-application vulnerability assessments and penetration tests?

Periodic web application vulnerability assessments and penetration tests are essential for identifying new vulnerabilities and staying ahead of evolving cyber threats. Investments Made into applications need to serve specific business processes as well as purpose and hence there is the need for the cardinal principles of Confidentiality, Integrity and Availability of web resources as needed.

Periodic assessment helps to ensure compliance with industry regulations such as GDPR, HIPAA, and PCI-DSS, reducing the risk of legal penalties. These tests proactively manage risks by discovering weaknesses before attackers can exploit them, protecting sensitive user data and maintaining trust.

Regular assessments also prevent business disruptions, reduce financial losses from breaches, and improve incident response plans. Additionally, they ensure adherence to security best practices, strengthening the overall security posture. By demonstrating a commitment to security, these assessments enhance an organization's reputation and safeguard its operations.

1. Explore the Firefox Live HTTP Headers plug-in application. What does it do, and why is this a good tool for web server and web application security testing?

It is a tool used for checking and monitoring HTTP requests and response headers in real time. It gives detailed http traffic travers between the web browser and the server. It helps to detect vulnerabilities on the server side. Example due to its liveliness, it helps to identify if sensitive data is being transmitted insecurely.