Cyber security long-term internship

Technology stack:-cyber security with IBM Qrader

Project tittle:-Mastering Website Security: Techniques for Effective defence

TEAM ID:LTVIP2024TMID14858

TEAM SIZE:5

TEAM LEADER: REDDY HEMA LATHA

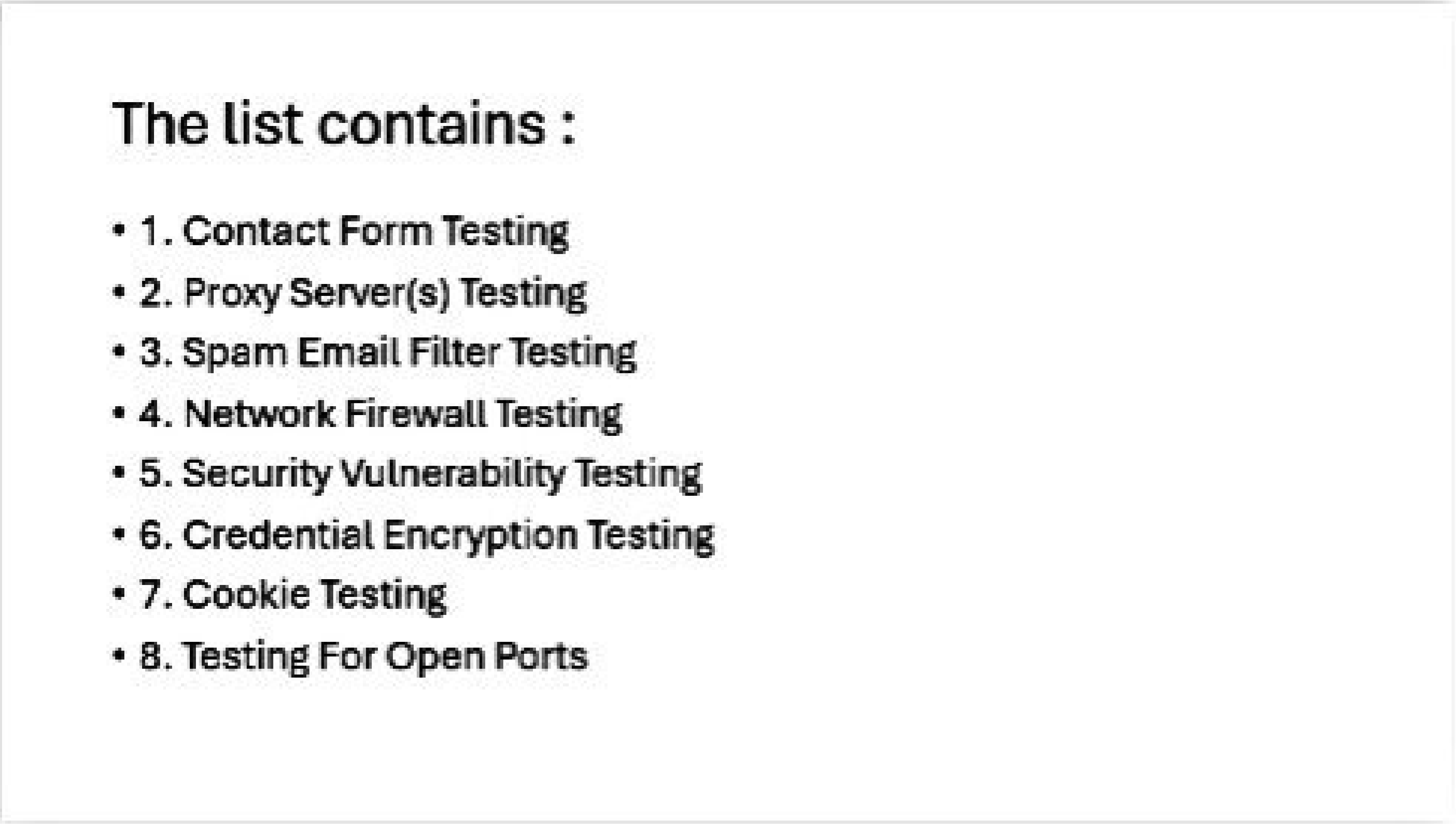
TEAM MEMBER: REVU ANUSHA

REGISTER NUMBER:SBAP0014860

My task

Introduction to-web application penetration testing :-

Web application penetration testing is the practice of simulating attacks on a system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure.



The list contains :

- 1. Contact Form Testing
- 2. Proxy Server(s) Testing
- 3. Spam Email Filter Testing
- 4. Network Firewall Testing
- 5. Security Vulnerability Testing
- 6. Credential Encryption Testing
- 7. Cookie Testing
- 8. Testing For Open Ports

Principal of web application :-

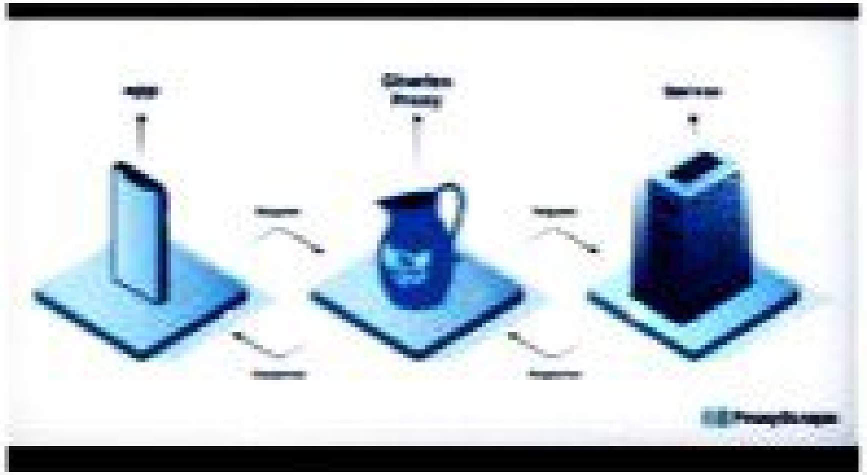
- Exploitation: In this stage of web app penetration testing, all potential vulnerabilities found in the earlier phases will be taken and used to exploits.
- Intelligence Gathering: Once the test has officially begun, a start notification will be sent to the client informing them of the activity's commencement
- Intelligence Gathering; Threat Modeling; Vulnerability Analysis; Exploitation; Post Exploitation; Reporting. Instead of simply methodology or process, PTES also ...

Contact form tasting:-

A contact form is a web form that allows website visitors to send you messages or inquiries. It typically includes fields for the visitor's name, email address, message or any other field that's relevant to your business.

Proxy server testing:-

Testing proxies is one of the most important things for anyone considering using proxy servers. A proxy server forwards requests and responses and works hard to protect you online. Its main function is to improve online privacy and security by hiding your IP address, which conceals your identity and location.

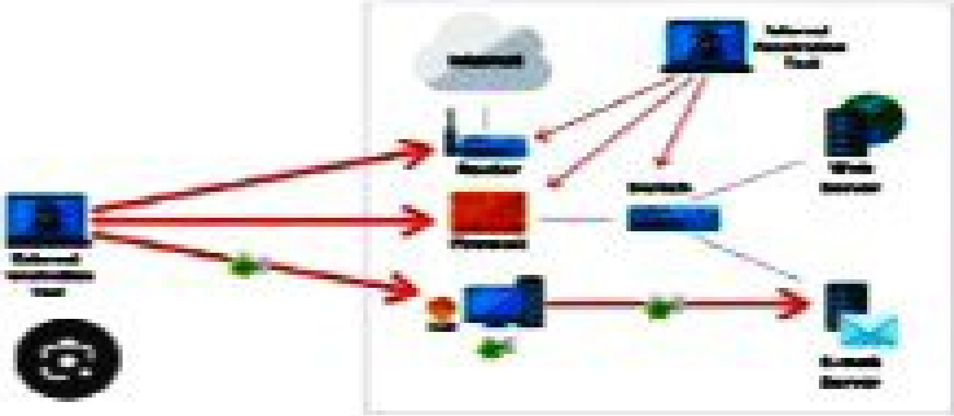


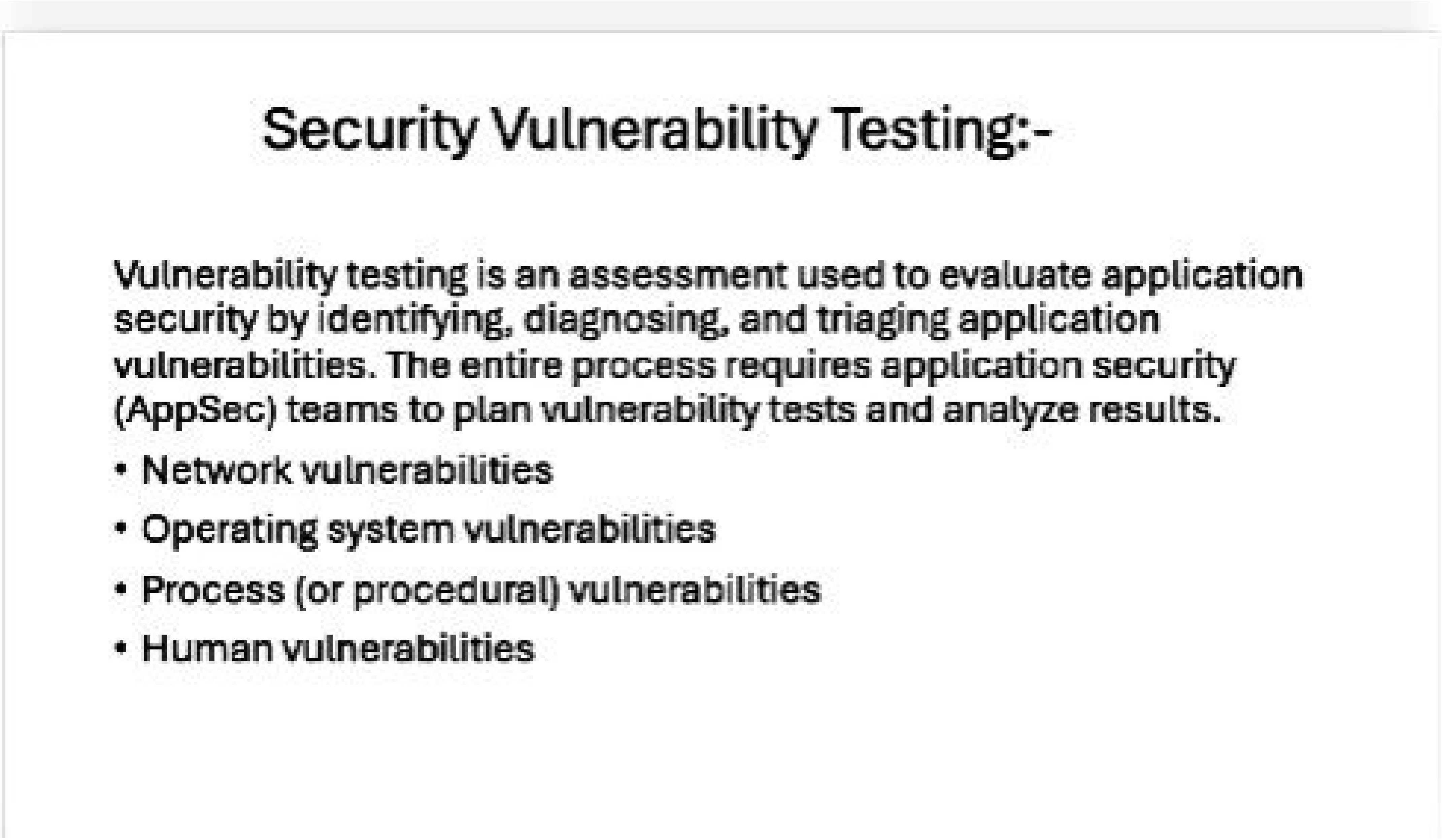
Spam Email Filter Testing:-

Gmail spam filters are primarily based on machine learning algorithms. They use user feedback and spam complaints to improve spam detection constantly. Spam filters examine factors such as IP addresses, authentication protocols behind bulk email sender domains, and domains and subdomains themselves.

Network Firewall Testing:-

There is a plethora of tools to test firewalls. Prominent among them are Nmap, Net cat, and Shields Up. These not only assist in port scanning but also in conducting traceroute checks, creating reverse shell scenarios, and ICMP requests, crucial for advanced security testing.

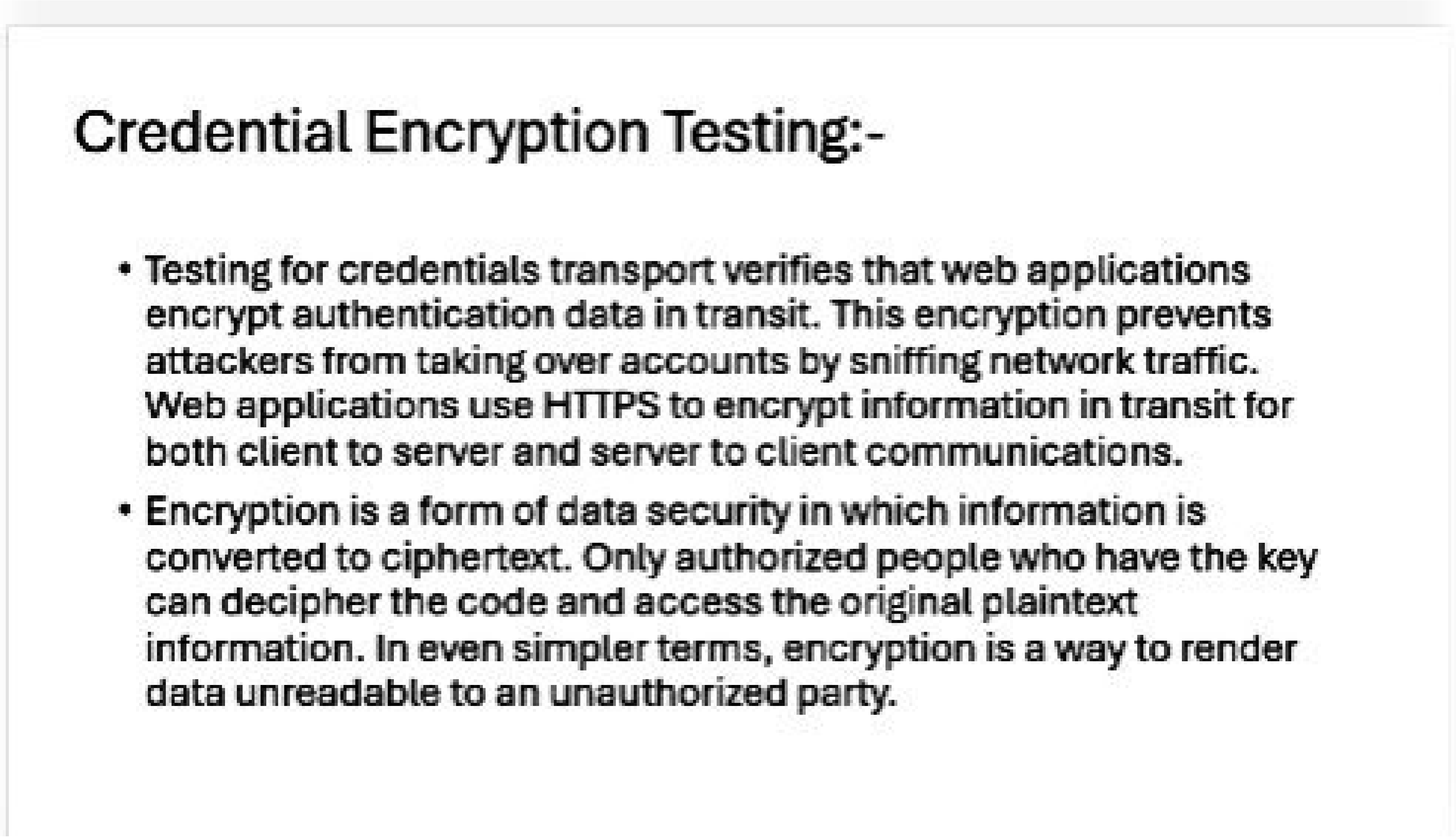




Security Vulnerability Testing:-

Vulnerability testing is an assessment used to evaluate application security by identifying, diagnosing, and triaging application vulnerabilities. The entire process requires application security (AppSec) teams to plan vulnerability tests and analyze results.

- Network vulnerabilities
- Operating system vulnerabilities
- Process (or procedural) vulnerabilities
- Human vulnerabilities



Credential Encryption Testing:-

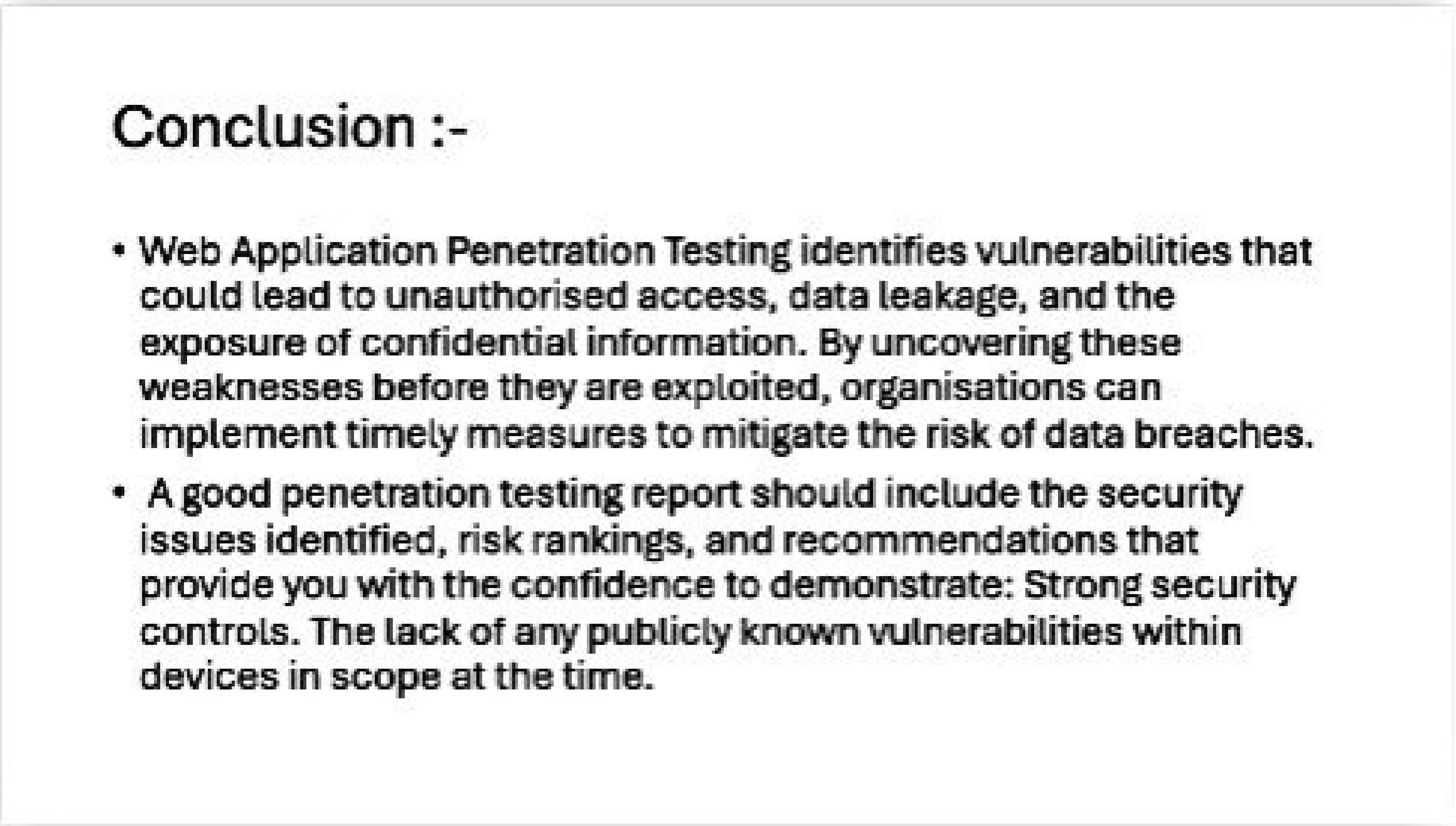
- Testing for credentials transport verifies that web applications encrypt authentication data in transit. This encryption prevents attackers from taking over accounts by sniffing network traffic. Web applications use HTTPS to encrypt information in transit for both client to server and server to client communications.
- Encryption is a form of data security in which information is converted to ciphertext. Only authorized people who have the key can decipher the code and access the original plaintext information. In even simpler terms, encryption is a way to render data unreadable to an unauthorized party.

Cookie tasting:-

- Cookie Testing is defined as a Software Testing type that checks Cookie created in your web browser. A cookie is a small piece of information that is stored in a text file on user's (client) hard drive by the web server.

Testing For Open Parts:-

- If you would like to test ports on your computer, use the Windows command prompt and the CMD command netstat –ano. Windows will show you all currently existing network connections via open ports or open, listening ports that are currently not establishing a connection.



Conclusion :-

- Web Application Penetration Testing identifies vulnerabilities that could lead to unauthorised access, data leakage, and the exposure of confidential information. By uncovering these weaknesses before they are exploited, organisations can implement timely measures to mitigate the risk of data breaches.
- A good penetration testing report should include the security issues identified, risk rankings, and recommendations that provide you with the confidence to demonstrate: Strong security controls. The lack of any publicly known vulnerabilities within devices in scope at the time.

Reference :-

- Web a penetration testing is comprised of four main steps including information gathering, research and exploitation, reporting and recommendations, and remediation with ongoing support. These tests are performed primarily to maintain secure software code development throughout its lifecycle.

- https://www. Digital defense. Com
- https://visme. Com
- https://www. Techtarget. Com
- https://www. You tube. Com
- https://www.Google . com