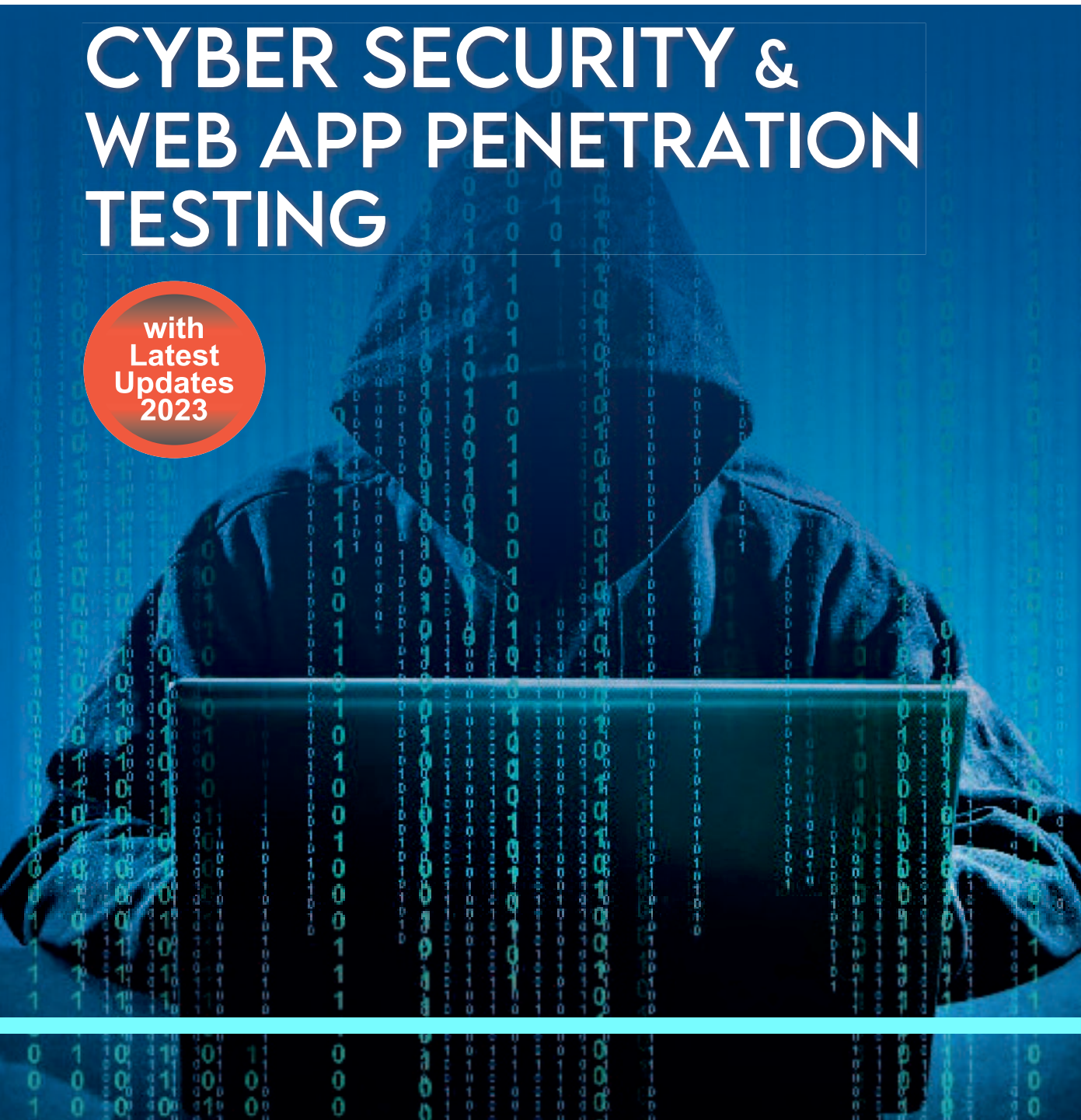
ETHICAL HACKING

CYBER SECURITY & WEB APP PENETRATION TESTING

with Latest Updates 2023



Ethical Hacking, Cyber Security & Web App Penetration Testing

T Balaji

TBALAJI PUBLICATION

INFRONT OF A.N JHA HOSTEL UNIVERSITY ROAD PRAYAGRAJ

Contact: 9415631990, 9450976411

E-Mail : tbpprayag@gmail.com

Web site www.tbalaji.in/

Dedicated to ...

LORD TIRUPATI BALAJI

Table of Content

1

Ethical Hacking & Cyber Security

1.1 Introduction to Ethical hacking
एथिकल हैकिंग एक परिचय

Ethical hacking, also known as ***penetration testing*** or ***white-hat hacking***, is the practice of testing computer systems, networks, and applications of vulnerabilities in order to identify and address security weaknesses. It is a proactive approach to cybersecurity that helps organizations assess their security posture and take appropriate countermeasures to protect against potential attacks.

एथिकल हैकिंग, जिसे पेनेट्रेशन परीक्षण(एन्ट्री लेवल की टेस्टिंग) या व्हाइट–हैट हैकिंग के रूप में भी जाना जाता है, सुरक्षा कमजोरियों की पहचान करने और उन्हें दूर करने के लिए कंप्यूटर सिस्टम, नेटवर्क और कमजोरियो के ऐप्लिकेशनो का परीक्षण करने का अभ्यास है। यह साइबर सुरक्षा के लिए एक सक्रिय दृष्टिकोण है जो संगठनों को उनकी सुरक्षा स्थिति का आकलन करने और संभावित हमलों से बचाने के लिए उचित जवाबी उपाय करने में मदद करता है।

Here are some key aspects of ethical hacking and countermeasures:
यहां एथिकल हैकिंग और उसके प्रति उपायों के कुछ प्रमुख पहलू दिए गए हैं:

- **Scope and Authorization**: Ethical hacking should always be conducted within a well-defined scope and with proper authorization from the system owner. This ensures that the testing is legal and avoids unintended consequences.

  स्कोप और ऑथोराइजेशन: एथिकल हैकिंग हमेशा एक अच्छी तरह से निर्धारित स्कोप में और सिस्टम मालिक द्वारा उचित ऑथोराइजेशन के साथ संचालित किया जाना चाहिए। जो यह सुनिश्चित करता है कि परीक्षण कानूनी है और अनपेक्षित परिणामों से बचा जाये।

- **Reconnaissance:** This phase involves gathering information about the target system or network. Ethical hackers use publicly available information, such as *domain registration records* and *search engine results*, to understand potential vulnerabilities and attack vectors.

  पूर्व परीक्षण: इस चरण में टार्गेट किये गये सिस्टम या नेटवर्क के बारे में जानकारी एकत्र करना शामिल है। संभावित कमजोरियों और आक्रमण वैक्टरों को समझने के लिए एथिकल हैकर्स सार्वजनिक रूप से उपलब्ध जानकारी, जैसे डोमेन रजिस्ट्रेशन रिकॉर्ड और सर्च इंजन परिणाम का उपयोग करते हैं।

- **Vulnerability Assessment**: In this phase, ethical hackers use various tools and techniques to scan the target system or network for known vulnerabilities. They may employ vulnerability *scanners*, *port scanners*, and *network mapping* tools to identify weaknesses that can be exploited.

कमजोरियो का आकलनः इस चरण में, एथिकल हैकर टार्गेट किये गये सिस्टम या नेटवर्क की कमजोरियो का पता लगााने के लिए विभिन्न उपकरणो और तकनीको का उपयोग स्कैन करने के लिए करते है। वे ज्ञात कमजोरियों की पहचान करने के लिए भेद्यता स्कैनर, पोर्ट स्कैनर और नेटवर्क मैपिंग टूल का उपयोग कर सकते हैं जिनका फायदा उठाया जा सकता है।

- **Exploitation:** Once vulnerabilities are identified, ethical hackers attempt to exploit them to gain unauthorized access or escalate privileges. The goal is to demonstrate the impact of the vulnerabilities and the potential damage an attacker could cause.

  शोषणः एक बार कमजोरियों की पहचान हो जाने के बाद, एथिकल हैकर्स अनधिकृत पहुंच हासिल करने या विशेषाधिकार बढ़ाने के लिए उनका शोषण करने का प्रयास करते हैं। इनका लक्ष्य कमजोरियों के प्रभाव और हमलावर द्वारा पहुंचाई जा सकने वाली संभावित क्षति को प्रदर्शित करना होता है।

- **Post-Exploitation and Reporting:** Ethical hackers document their findings and provide a detailed report to the organization, highlighting the vulnerabilities and recommended counter measures. This helps the organization understand the risks and take appropriate actions to mitigate them.

  बाद मे काम लेना और रिपोर्ट करनाः एथिकल हैकर्स अपने निष्कर्षों का डाक्यूमेन्ट बनाते हैं और संगठन को एक विस्तृत रिपोर्ट प्रदान करते हैं, जिसमें कमजोरियों और अनुशंसित प्रति उपायों पर प्रकाश डाला जाता है। इससे संगठन को जोखिमों को समझने और उन्हें कम करने के लिए उचित कार्रवाई करने में मदद मिलती है।

***Countermeasures** are the steps taken to protect systems and networks from potential attacks.*
काउंटरमेजर्स (प्रतिउपाय) सिस्टम और नेटवर्क को संभावित हमलों से बचाने के लिए उठाए गए कदम हैं।

Here are some common countermeasures: - यहां कुछ सामान्य प्रतिउपाय दिए गए हैं:

- **Access Controls:** Implement strong authentication mechanisms, such as *two-factor authentication*, and *enforce access controls based on the principle of least privilege*. Regularly review and revoke unnecessary privileges.

  एक्सेस कन्ट्रोलः मजबूत आथेन्टिकेशन(प्रमाणीकरण) मेकानिज्म जैसे टू–फैक्टर आथेन्टिकेशन, और कम से कम विशेषाधिकार के सिद्धांत के आधार पर एक्सेस कन्ट्रोल लागू करें। अनावश्यक विशेषाधिकारों की नियमित समीक्षा करें और उन्हें हटाये।

- **Patch Management:** Keep software and systems up to date with the latest security patches and updates to address known vulnerabilities. Establish a robust patch management process to ensure timely updates.

  पैच प्रबंधनः ज्ञात कमजोरियों को दूर करने के लिए सॉफ्टवेयर और सिस्टम को नवीनतम सुरक्षा पैच और अपडेट के साथ अप टू डेट रखें। समय पर अपडेट सुनिश्चित करने के लिए एक मजबूत पैच प्रबंधन प्रक्रिया स्थापित करें।

- **Secure Configuration:** *Configure systems*, *networks*, and *applications* with secure settings, following industry best practices and security guidelines. Disable unnecessary services and apply appropriate security controls.

  सुरक्षित कॉन्फिगरेशनः उद्योग की सर्वोत्तम प्रथाओं और सुरक्षा दिशानिर्देशों का पालन करते हुए सुरक्षित सेटिंग्स के साथ सिस्टम, नेटवर्क और एप्लिकेशन को कॉन्फिगर करें। अनावश्यक सेवाएँ अक्षम करें और उचित सुरक्षा नियंत्रण लागू करें।

- **Network Security:** Implement firewalls, intrusion detection and prevention systems, and network segmentation to protect against unauthorized access and network-based attacks. Regularly monitor network traffic for suspicious activities.

नेटवर्क सुरक्षा: अनधिकृत पहुंच और नेटवर्क–आधारित हमलों से बचाने के लिए फायरवॉल, घुसपैठ का पता लगाने और रोकथाम प्रणाली और नेटवर्क विभाजन लागू करें। संदिग्ध गतिविधियों को जानने के लिए नियमित रूप से नेटवर्क ट्रैफिक की निगरानी करें।

- **Secure Coding Practices:** Develop web applications and software using secure coding practices to prevent common vulnerabilities like *injection attacks, cross-site scripting (XSS), or cross-site request forgery (CSRF)*. Conduct regular code reviews and use static code analysis tools.

  सुरक्षित कोडिंग प्रथाएं: सामान्य कमजोरियों जैसे इंजेक्शन हमलों, क्रॉस–साइट स्क्रिप्टिंग (एक्सएसएस), या क्रॉस–साइट रिक्वेस्ट फॉरग्रेरी(*CSRF*) को रोकने के लिए सुरक्षित कोडिंग प्रथाओं का उपयोग करके वेब एप्लिकेशन और सॉफ्टवेयर विकसित करें। नियमित कोड समीक्षा करें और स्टैटिक कोड विश्लेषण टूल का उपयोग करें।

- **Security Awareness Training:** Educate employees and users about cyber security threats, social engineering, and best practices for secure behavior. Promote a culture of security awareness and ensure users understand their role in protecting the organization's assets.

  सुरक्षा जागरूकता प्रशिक्षण: कर्मचारियों और उपयोगकर्ताओं को साइबर सुरक्षा खतरों, सोशल इंजीनियरिंग और सुरक्षित व्यवहार के लिए सर्वोत्तम प्रथाओं के बारे में शिक्षित करें। सुरक्षा जागरूकता की संस्कृति को बढ़ावा दें और सुनिश्चित करें कि उपयोगकर्ता संगठन की संपत्ति की सुरक्षा में अपनी भूमिका को समझें।

- **Incident Response:** Develop an incident response plan to effectively respond to security incidents. This includes detection, containment, eradication, and recovery strategies. Regularly test and update the plan based on lessons learned from exercises or real incidents.

  घटना प्रतिक्रिया: सुरक्षा घटनाओं पर प्रभावी ढंग से प्रतिक्रिया देने के लिए एक घटना पर प्रतिक्रिया करने का प्लान विकसित करें। इसमें पता लगाना, रोकथाम, उन्मूलन और पुनर्प्राप्ति रणनीतियाँ शामिल हैं। अभ्यास या वास्तविक घटनाओं से सीखे गए सबक के आधार पर योजना का नियमित परीक्षण और अपडेट करें।

- **Continuous Monitoring:** Implement security monitoring solutions to detect and respond to security events in real-time. Use intrusion detection systems (IDS), security information and event management (SIEM) tools, and log analysis to identify and investigate suspicious activities.

  सतत निगरानी: वास्तविक समय में सुरक्षा घटनाओं का पता लगाने और उन पर प्रतिक्रिया देने के लिए सुरक्षा निगरानी समाधान लागू करें। संदिग्ध गतिविधियों की पहचान करने और जांच करने के लिए घुसपैठ का पता लगाने वाली प्रणाली (आईडीएस), सुरक्षा इनफार्मेशन और इवेन्ट प्रबंधन (SIEM) उपकरण और लॉग विश्लेषण का उपयोग करें।

- **Encryption and Data Protection:** Use encryption to protect sensitive data in transit and at rest. Implement data loss prevention (DLP) measures to prevent unauthorized data leakage. Regularly backup data and test restoration procedures.

  एन्क्रिप्शन और डेटा सुरक्षा: पारगमन और आराम के दौरान संवेदनशील डेटा की सुरक्षा के लिए एन्क्रिप्शन का उपयोग करें। अनधिकृत डेटा के नुकसान को रोकने के लिए डेटा हानि रोकथाम (डीएलपी) उपायों को लागू करें। नियमित रूप से डेटा का बैकअप लें और रिस्टोरेशन प्रक्रियाओं का परीक्षण करें।

- **Regular Security Audits and Assessments:** Conduct periodic security audits and assessments, including penetration testing and vulnerability scanning, to proactively identify vulnerabilities and weaknesses. Address the identified issues promptly.

नियमित सुरक्षा ऑडिट और मूल्यांकनः भेद्यता और कमजोरियों की सक्रिय रूप से पहचान करने के लिए पेनेट्रेशन परीक्षण और भेद्यता स्कैनिंग सहित समय–समय पर सुरक्षा ऑडिट और मूल्यांकन करें। पहचाने गए मुद्दों का तुरंत समाधान करें।

It's important to note that ethical hacking should always be conducted by trained professionals who adhere to legal and ethical guidelines. Organizations should engage with reputable cybersecurity firms or employ in-house experts with the necessary skills to perform ethical hacking and implement appropriate countermeasures.

यह ध्यान रखना महत्वपूर्ण है कि एथिकल हैकिंग हमेशा प्रशिक्षित पेशेवरों द्वारा की जानी चाहिए जो कानूनी और नैतिक दिशानिर्देशों का पालन करते हैं। संगठनों को प्रतिष्ठित साइबर सुरक्षा फर्मों के साथ जुड़ना चाहिए या एथिकल हैकिंग करने और उचित जवाबी उपायों को लागू करने के लिए आवश्यक कौशल वाले इन–हाउस विशेषज्ञों को नियुक्त करना चाहिए।

1.2 Basics of Cyber Security
साइबर सुरक्षा की मूल बातें

Cybersecurity refers to the practice of *protecting computer systems, networks*, and *data* from unauthorized access, use, dislosure, disruption, modification, or destruction. With the increasing reliance on technology and the interconnectedness of devices and networks, cybersecurity has become a critical concern for individuals, businesses, and governments.

साइबर सुरक्षा कंप्यूटर सिस्टम, नेटवर्क और डेटा को अनधिकृत पहुंच, उपयोग, प्रकटीकरण, व्यवधान, संशोधन या विनाश से बचाने की प्रथा को संदर्भित करती है। प्रौद्योगिकी पर बढ़ती निर्भरता और उपकरणों और नेटवर्कों के अंतर्संबंध के साथ, साइबर सुरक्षा व्यक्तियों, व्यवसायों और सरकारों के लिए एक महत्वपूर्ण चिंता का विषय बन गई है।

Here are some key basics of cybersecurity: - यहां साइबर सुरक्षा की कुछ प्रमुख बुनियादी बातें दी गई हैं:

1. **Confidentiality:** It ensures that sensitive information is only accessible to authorized individuals or systems. This is achieved through measures such as encryption, access controls, and secure communication channels.

गोपनीयताः यह सुनिश्चित करती है कि संवेदनशील जानकारी केवल अधिकृत व्यक्तियों या सिस्टमो तक ही पहुंच योग्य है। इसे एन्क्रिप्शन, एक्सेस कन्ट्रोल और सुरक्षित संचार चैनल जैसे उपायों के माध्यम से हासिल किया जाता है।

2. **Integrity:** It ensures that data remains intact, accurate, and unaltered during storage, transmission, and processing. That means this property refers to that information has not be altered in an unauthorized way, and that source of the information is genuine.Data integrity can be maintained through mechanisms like checksums, digital signatures, and access controls.

इन्टीग्रिटीः यह सुनिश्चित करती है कि स्टोरेज, ट्रॉन्समिशन और प्रोसेसिंग के दौरान डेटा बरकरार, सटीक और अपरिवर्तित रहे। इसका मतलब है कि यह प्रॉपर्टी बताती है कि इन्फार्मेशन को अनधिकृत तरीके से नहीं बदला गया है, और इन्फार्मेशन का स्रोत वास्तविक है। डेटा इन्टीग्रिटी को चेकसम, डिजिटल हस्ताक्षर और एक्सेस कन्ट्रोल जैसे मैकेनिज्मो के माध्यम से बनाए रखा जा सकता है।

3. **Availability:** It ensures that information and systems are accessible and usable when needed. Measures such as redundancy, backup systems, and disaster recovery plans help ensure continuity of operations in the event of an incident.

   उपलब्धता: यह सुनिश्चित करती है कि इन्फार्मेशन और सिस्टम जरूरत पड़ने पर एक्सेस करने योग्य और उपयोग करने योग्य हों। अतिरेक, बैकअप सिस्टम और आपदा पुनर्प्राप्ति योजना जैसे उपाय किसी घटना की स्थिति में संचालन की निरंतरता सुनिश्चित करने में मदद करती हैं।

4. **Authentication:** Authentication verifies the identity of users, systems, or devices before granting access to resources. Common authentication methods include passwords, biometrics, two-factor authentication (2FA), and multi-factor authentication (MFA).

   ऑथेन्टिकेशन: संसाधनों तक पहुंच प्रदान करने से पहले ऑथेन्टिकेशन यूजरो, सिस्टम या डिवाइसो की पहचान की पुष्टि करता है। सामान्य ऑथेन्टिकेशन मेथडो में पासवर्ड, बायोमेट्रिक्स, टू–फैक्टर ऑथेन्टिकेशन (2FA), और मल्टी–फैक्टर ऑथेन्टिकेशन (एमएफए) शामिल हैं।

5. **Authorization:** It controls the level of access granted to authenticated users or systems based on their roles and privileges. It ensures that users can only access the resources they are authorized to use.

   ऑथोराईजेशन: यह अधिकृत यूजरो या सिस्टमो को उनकी भूमिकाओं और विशेषाधिकारों के आधार पर दी गई पहुंच के स्तर को नियंत्रित करता है। यह सुनिश्चित करता है कि यूजर केवल उन संसाधनों तक पहुंच सकते हैं जिनके उपयोग के लिए वे अधिकृत होते हैं।

6. **Risk Assessment:** Risk assessment involves identifying and evaluating potential threats and vulnerabilities to determine their impact on the organization's assets. This helps prioritize security measures and allocate resources effectively.

   जोखिम मूल्यांकन: जोखिम मूल्यांकन में संगठन की संपत्ति पर उनके प्रभाव को निर्धारित करने के लिए संभावित खतरों और कमजोरियों की पहचान और मूल्यांकन करना शामिल है। इससे सुरक्षा उपायों को प्राथमिकता देने और संसाधनों को प्रभावी ढंग से आवंटित करने में मदद मिलती है।

7. **Security Awareness and Training:** Educating employees and users about cyber security threats, best practices, and their roles and responsibilities is crucial. Regular training programs raise awareness and promote a security-conscious culture.

   सुरक्षा जागरूकता और प्रशिक्षण: कर्मचारियों और यूजरो को साइबर सुरक्षा खतरों, सर्वोत्तम प्रथाओं और उनकी भूमिकाओं और जिम्मेदारियों के बारे में शिक्षित करना महत्वपूर्ण है। नियमित प्रशिक्षण प्रोग्राम जागरूकता बढ़ाते हैं और सुरक्षा के प्रति जागरूक संस्कृति को बढ़ावा देते हैं।

8. **Vulnerability Management:** Regularly scanning systems and networks for vulnerabilities, and promptly patching or mitigating them, is essential. This includes keeping software and systems up to date with security patches and updates.

   भेद्यता प्रबंधन: कमजोरियों के लिए सिस्टम और नेटवर्क को नियमित रूप से स्कैन करना और उन्हें तुरंत ठीक करना या कम करना आवश्यक है। इसमें सॉफ़्टवेयर और सिस्टम को सुरक्षा पैच और अपडेट के साथ अप टू डेट रखना शामिल है।

9. **Incident Response:** Developing an incident response plan helps organizations respond effectively to security incidents. It outlines procedures for detecting, containing, investigating, and recovering from cyber security events.

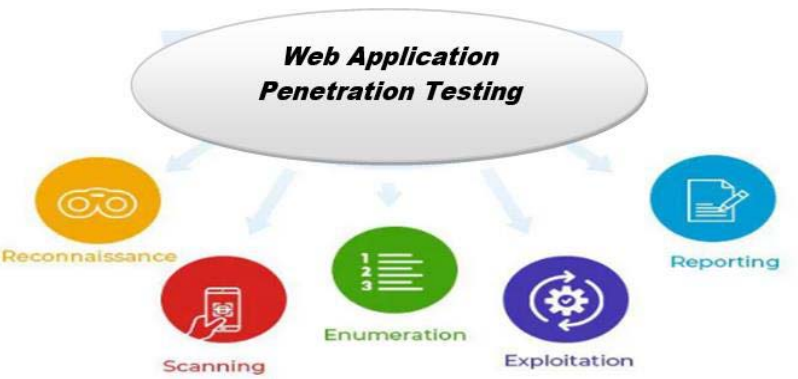
2

Web App Penetration Testing

2.1 What is Web Application Penetration?
वेब एप्लिकेशन पेनेट्रेशन परीक्षण क्या है?

Web application penetration testing, also known as *web app pen-testing*, is a security assessment technique used to identify vulnerabilities and weaknesses in web applications. The goal is to simulate real-world attacks and provide recommendations for improving the security posture of the application.

वेब एप्लिकेशन पेनेट्रेशन परीक्षण (प्रवेश परीक्षण), जिसे ***वेब ऐप पेन–टेस्टिंग*** के रूप में भी जाना जाता है, एक सुरक्षा मूल्यांकन की तकनीक है जिसका उपयोग वेब ऐप्लिकेशनो में कमजोरियों और भेद्यताओ की पहचान करने के लिए किया जाता है। लक्ष्य वास्तविक दुनिया के हमलों का अनुकरण करना और एप्लिकेशन की सुरक्षा स्थिति में सुधार के लिए सिफारिशें प्रदान करना होता है।



Here are the key steps involved in web app penetration testing:

वेब ऐप प्रवेश परीक्षण में शामिल प्रमुख चरण यहां दिए गए हैं:

2.1.1 Planning and Reconnaissance - योजना और पूर्व–परीक्षण

Web application penetration testing involves assessing the security of a web application by simulating real-world attacks. The initial phase of penetration testing involves planning and reconnaissance to gather information and prepare for the assessment.

वेब एप्लिकेशन प्रवेश परीक्षण में वास्तविक दुनिया के हमलों का अनुकरण करके वेब एप्लिकेशन की सुरक्षा का आकलन करना शामिल है। प्रवेश परीक्षण के प्रारंभिक चरण में जानकारी इकट्ठा करने और मूल्यांकन के लिए तैयारी करने के लिए योजना और पूर्व–परीक्षण शामिल है।

Here are the key steps involved in planning and reconnaissance for web application penetration testing:
वेब एप्लिकेशन प्रवेश परीक्षण के लिए योजना और पूर्व–परीक्षण में शामिल प्रमुख चरण यहां दिए गए हैं:

1. **Define the Scope:** Clearly define the scope of the penetration testing engagement. Identify the target web application(s) and determine the specific areas and functionalities to be tested. Consider any constraints or limitations imposed by the organization.

   स्कोप डिफाइन करें: प्रवेश परीक्षण संलग्नता के स्कोप को स्पष्ट रूप से डिफाइन करें। लक्ष्य वेब एप्लिकेशन की पहचान करें और परीक्षण किए जाने वाले विशिष्ट क्षेत्रों और कार्यक्षमताओं का निर्धारण करें। संगठन द्वारा लगाई गई किसी भी बाधा या सीमा पर विचार करें।

2. **Obtain Authorization:** Obtain proper authorization from the organization or application owner before conducting any penetration testing activities. Ensure that legal agreements, such as *Non-Disclosure Agreements (NDAs)* and *Rules of Engagement (ROE)*, are in place.

   ऑथोराईजेशन प्राप्त करें: किसी भी प्रवेश परीक्षण की ऐक्टिवीटी को संचालित करने से पहले संगठन या एप्लिकेशन स्वामी से उचित ऑथोराईजेशन प्राप्त करें। सुनिश्चित करें कि कानूनी समझौते, जैसे गैर–प्रकटीकरण समझौते (एनडीए) और इन्गेजमेन्ट के नियम (आरओई), लागू हैं।

3. **Information Gathering:** Gather information about the target web application to understand its architecture, technologies used, and potential vulnerabilities. Techniques for information gathering include:

   जानकारी एकत्र करना: टार्गेट वेब एप्लिकेशन के आर्किटेक्चर, उपयोग की गई तकनीकों और संभावित कमजोरियों को समझने के लिए उसके बारे में जानकारी इकट्ठा करें। इन्फार्मेशन एकत्र करने की तकनीकों में शामिल हैं:

   - **Passive Reconnaissance:** Conduct open-source intelligence (OSINT) gathering using public sources such as search engines, social media, forums, and job postings.
     निष्क्रिय पूर्व–परीक्षण: पब्लिक स्रोतों जैसे सर्च इंजन, सोशल मीडिया, फ़ोरम और नौकरी पोस्टिंग का उपयोग करके ओपन–सोर्स इंटेलिजेंस (OSINT) एकत्र करना।

   - **WHOIS Lookup:** Retrieve domain registration information to identify the organization behind the web application.
     WHOIS लुकअप: वेब एप्लिकेशन के पीछे संगठन की पहचान करने के लिए डोमेन पंजीकरण जानकारी प्राप्त करें।

- **DNS Enumeration:** Enumerate the DNS records to identify subdomains, mail servers, or other related services.
  डीएनएस गणना: सबडोमेन, मेल सर्वर, या अन्य संबंधित सेवाओं की पहचान करने के लिए डीएनएस रिकॉर्ड की गणना करें।

- **Web Spidering:** Use web spidering tools to crawl the target application and identify its structure, endpoints, and associated resources.
  वेब स्पाइडरिंग: टार्गेट एप्लिकेशन को क्रॉल करना और उसका स्ट्रक्चर, समापन बिंदु और संबंधित संसाधनों की पहचान करने के लिए वेब स्पाइडरिंग टूल का उपयोग करें।

- **Port Scanning:** Perform port scanning to identify open ports and services running on the target application's infrastructure.
  पोर्ट स्कैनिंग: खुले पोर्ट और टार्गेट एप्लिकेशन के बुनियादी ढांचे पर चल रही सेवाओं की पहचान करने के लिए पोर्ट स्कैनिंग करें।

4. **Mapping the Application:** Create a detailed map or inventory of the web application, including its URLs, endpoints, and functionalities. Document the different components, user roles, and potential attack surfaces within the application.

   एप्लिकेशन को मैप करना: वेब एप्लिकेशन का एक विस्तृत मैप या सूची बनाएं, जिसमें उसके यूआरएल, एंडपॉइंट और कार्यात्मकताएं शामिल हों। एप्लिकेशन के भीतर विभिन्न कम्पोनेन्टो, यूजर की भूमिकाओं और संभावित हमले की सतहों का डॉक्यूमेन्टो को बनाये।

5. **Identify Technologies and Frameworks:** Identify the technologies, frameworks, and libraries used by the web application. This information helps in understanding potential vulnerabilities associated with specific technologies and enables targeted testing.

   प्रौद्योगिकियों और फ्रेमवर्को की पहचान करें: वेब एप्लिकेशन द्वारा उपयोग की जाने वाली प्रौद्योगिकियों, फ्रेमवर्को और लाईब्रेरीज की पहचान करें। यह जानकारी विशिष्ट प्रौद्योगिकियों से जुड़ी संभावित कमजोरियों को समझने में मदद करती है और टार्गेट किये गये परीक्षण को सक्षम बनाती है।

6. **Vulnerability Research:** Conduct research on known vulnerabilities and security issues associated with the technologies used in the web application. Stay updated with the latest security advisories, vulnerabilities, and patches.

   भेद्यता अनुसंधान: वेब एप्लिकेशन में उपयोग की जाने वाली प्रौद्योगिकियों से जुड़ी ज्ञात कमजोरियों और सुरक्षा मुद्दों पर शोध करिये। नवीनतम सुरक्षा सलाह, कमजोरियों और पैच के साथ अपडेट रहें।

7. **Identify Attack Vectors:** Analyze the information gathered to identify potential attack vectors and entry points for exploitation. Common attack vectors include injection attacks (SQL, XSS), authentication bypass, insecure direct object references (IDOR), and server misconfigurations.

   आक्रमण वाहकों की पहचान करें: संभावित आक्रमण वाहकों और शोषण के प्रवेश बिंदुओं की पहचान करने के लिए एकत्रित जानकारी का विश्लेषण करें। सामान्य आक्रमण वैक्टर में इंजेक्शन हमले (एसक्यूएल, एक्सएसएस), ऑथेन्टिकेशन बाईपास, असुरक्षित प्रत्यक्ष ऑब्जेक्ट रेफरेन्स (आईडीओआर), और सर्वर गलत कॉन्फ़िगरेशन शामिल हैं।

8. **Prioritize Targets:** Prioritize the identified targets based on criticality, potential impact, and feasibility of exploitation. Focus on high-risk areas that could lead to unauthorized access, data exposure, or compromise of sensitive functionality.

लक्ष्यों को प्राथमिकता दें: गंभीरता, संभावित प्रभाव और शोषण की व्यवहार्यता के आधार पर पहचाने गए लक्ष्यों को प्राथमिकता दें। उच्च जोखिम वाले क्षेत्रों पर ध्यान केंद्रित करें जो अनधिकृत एक्सेस, डेटा एक्सपोज़र या संवेदनशील कार्यक्षमता से समझौता कर सकते हैं।

9. **Documentation:** Document all the information gathered during the planning and reconnaissance phase. This includes the target web application details, findings, identified attack vectors, and any other relevant information. Maintain a detailed record to guide subsequent testing activities and aid in reporting.

   दस्तावेज़ीकरण: योजना और पूर्व–परीक्षण चरण के दौरान एकत्र की गई सभी जानकारी का डाक्यूमेन्टेशन करें। इसमें टार्गेट वेब एप्लिकेशन विवरण, निष्कर्ष, पहचाने गए हमले वैक्टर और कोई अन्य प्रासंगिक जानकारी शामिल है। बाद की परीक्षण गतिविधियों का मार्गदर्शन करने और रिपोर्टिंग में सहायता के लिए एक विस्तृत रिकॉर्ड बनाए रखें।

10. **Communication:** Maintain effective communication with stakeholders throughout the planning and reconnaissance phase. Regularly update the relevant parties about the progress, findings, and any potential risks or concerns.

    संचार: योजना और पूर्व–परीक्षण चरण के दौरान हितधारकों के साथ प्रभावी संचार बनाए रखें। प्रगति, निष्कर्ष और किसी भी संभावित जोखिम या चिंता के बारे में संबंधित पक्षों को नियमित रूप से अपडेट करें।

By carefully planning and conducting thorough reconnaissance, you can gather critical information about the target web application, identify potential vulnerabilities, and lay the foundation for an effective and focused web application penetration test.

सावधानीपूर्वक योजना बनाकर और पूरी तरह से जांच करके, आप टार्गेट वेब एप्लिकेशन के बारे में महत्वपूर्ण जानकारी एकत्र कर सकते हैं, संभावित कमजोरियों की पहचान कर सकते हैं और एक प्रभावी और केंद्रित वेब एप्लिकेशन प्रवेश परीक्षण की नींव रख सकते हैं।

2.1.2 Threat Modeling - थ्रेट मॉडलिंग

Web application penetration testing involves identifying and assessing potential threats and vulnerabilities to understand the security risks associated with the application. Threat modeling is an essential step in the penetration testing process that helps in systematically identifying and prioritizing potential threats.

वेब एप्लिकेशन प्रवेश परीक्षण में एप्लिकेशन से जुड़े सुरक्षा जोखिमों को समझने के लिए संभावित खतरों और कमजोरियों की पहचान करना और उनका आकलन करना शामिल है। थ्रेट मॉडलिंग प्रवेश परीक्षण प्रक्रिया में एक आवश्यक कदम है जो संभावित खतरों को व्यवस्थित रूप से पहचानने और प्राथमिकता देने में मदद करता है।

Here's an overview of the steps involved in threat modeling for web application penetration testing:
यहां वेब एप्लिकेशन प्रवेश परीक्षण के लिए थ्रेट मॉडलिंग में शामिल चरणों का अवलोकन दिया गया है:

- **Identify the Assets:** Start by identifying the assets that need protection within the web application. This includes sensitive data, user credentials, intellectual property, financial information, and any other critical resources.

  संपत्तियों की पहचान करें: उन संपत्तियों की पहचान करके शुरुआत करें जिन्हें वेब एप्लिकेशन के भीतर सुरक्षा की आवश्यकता है। इसमें संवेदनशील डेटा, यूजर क्रेडेंशियल, बौद्धिक संपदा, वित्तीय जानकारी और अन्य महत्वपूर्ण संसाधन शामिल हैं।

- **Define the Application Scope:** Clearly define the boundaries and scope of the web application to be threat modeled. Identify the various components, modules, APIs, and interfaces involved.

एप्लिकेशन के स्कोप को डिफाइन करें: थ्रेट मॉडल वाले वेब एप्लिकेशन की सीमाओं और स्कोप को स्पष्ट रूप से डिफाइन करें। इसमें शामिल विभिन्न कम्पोनेन्टो, मॉड्यूल, एपीआई और इंटरफेस की पहचान करें।

- **Understand the Architecture:** Gain a comprehensive understanding of the web application's architecture, including the different layers, components, and their interactions. This includes the front-end interface, server-side components, databases, APIs, and external integrations.

  आर्किटेक्चर को समझें: विभिन्न लेयरो, कम्पोनेन्टो और उनके इंटरैक्शन सहित वेब एप्लिकेशन के आर्किटेक्चर की व्यापक समझ हासिल करें। इसमें फ्रंट–एंड इंटरफ़ेस, सर्वर–साइड कम्पोनेन्टो, डेटाबेस, एपीआई और बाहरी इन्टीग्रेशन शामिल हैं।

- **Identify Threat Actors:** Identify potential threat actors who may target the web application. This includes internal actors (employees, administrators) and external actors (hackers, competitors, malicious users).

  थ्रेट वाले ऐक्टरो की पहचान करें: संभावित थ्रेट वाले उन ऐक्टरो की पहचान करें जो वेब एप्लिकेशन को लक्षित कर सकते हैं। इसमें इन्टर्नल ऐक्टर (कर्मचारी, प्रशासक) और बाहरी ऐक्टर (हैकर, प्रतिस्पर्धी, दुर्भावनापूर्ण यूजर्स) शामिल हैं।

- **Enumerate Threats:** Identify and enumerate potential threats or attack vectors that could be leveraged by the threat actors to compromise the security of the web application. Common threats include injection attacks (SQL, XSS), authentication bypass, session hijacking, information disclosure, and privilege escalation.

  थ्रेटो की गणना करें: संभावित थ्रेटो या हमला करने वालो की पहचान करें और उनकी गणना करें जिनका लाभ वेब एप्लिकेशन की सुरक्षा से समझौता करने के लिए थ्रेटो वाले ऐक्टरो द्वारा उठाया जा सकता है। सामान्य थ्रेटो में इंजेक्शन हमले (एसक्यूएल, एक्सएसएस), ऑथेन्टिकेशन बाईपास, सेशन हाईजैकिंग, इन्फार्मेशन प्रकटीकरण और विशेषाधिकार वृद्धि शामिल हैं।

- **Assess Vulnerabilities:** Identify potential vulnerabilities within the web application that could be exploited by the identified threats. This includes security misconfigurations, insecure coding practices, weak authentication mechanisms, and inadequate access controls.

  कमजोरियों का आकलन करें: वेब एप्लिकेशन के भीतर संभावित कमजोरियों की पहचान करें जिनका पहचाने गए थ्रेटो द्वारा फायदा उठाया जा सकता है। इसमें सुरक्षा गलत कॉन्फ़िगरेशन, असुरक्षित कोडिंग प्रथाएं, कमजोर ऑथेन्टिकेशन मैकेनिज्म और अपर्याप्त एक्सेस कन्ट्रोल शामिल हैं।

- **Prioritize Threats:** Prioritize the identified threats based on their potential impact and likelihood of exploitation. Consider the criticality of the asset, the feasibility of the attack, and the potential consequences of a successful exploit.

  थ्रेटो को प्राथमिकता दें: पहचाने गए थ्रेटो को उनके संभावित प्रभाव और शोषण की संभावना के आधार पर प्राथमिकता दें। संपत्ति की गंभीरता, हमले की व्यवहार्यता और एक सफल शोषण के संभावित परिणामों पर विचार करें।

- **Mitigation Strategies:** Develop mitigation strategies to address the identified threats. This may involve implementing secure coding practices, applying security patches and updates, strengthening access controls, implementing encryption, and enhancing monitoring and logging mechanisms.

  शमन रणनीतियाँ: पहचाने गए खतरों से निपटने के लिए शमन(mitigation) रणनीतियाँ विकसित करें। इसमें सुरक्षित कोडिंग प्रथाओं को लागू करना, सुरक्षा पैच और अपडेट लागू करना, एक्सेस कन्ट्रोल को मजबूत करना, एन्क्रिप्शन लागू करना और निगरानी और लॉगिंग मैकेनिज्म को बढ़ाना शामिल हो सकता है।