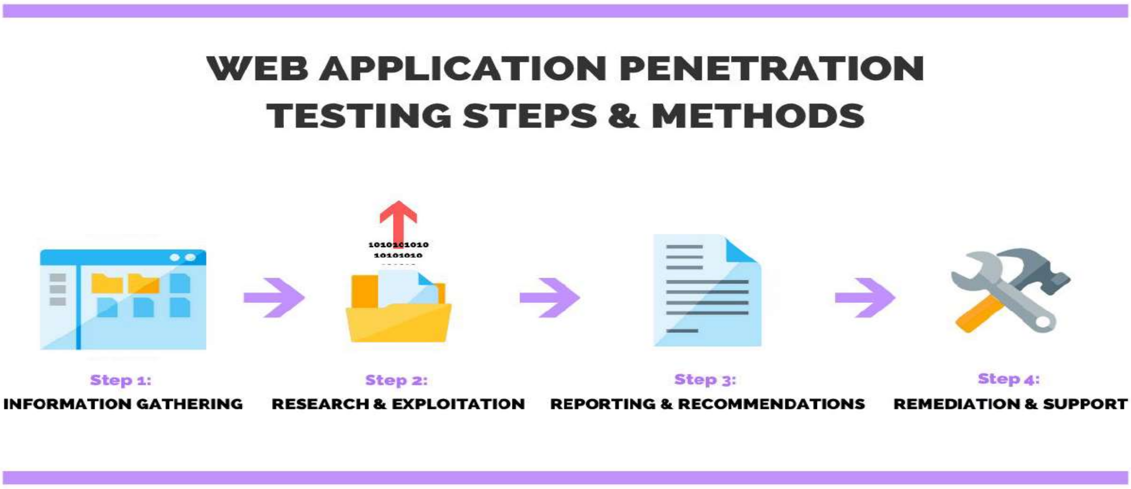
NISM Team Assignment Part 1



WEB APPLICATION PENETRATION TESTING STEPS & METHODS

Step 1: INFORMATION GATHERING

Step 2: RESEARCH & EXPLOITATION

Step 3: REPORTING & RECOMMENDATIONS

Step 4: REMEDIATION & SUPPORT

Q: How will you identify, investigate and classify their security challenges.

Step 1 Information Gathering (Reconnaissance)

We are going to perform an active reconnaissance on the web application. The information we intend to collect during the reconnaissance is the following:

1. Fingerprinting –fingerprinting enables gathering information about the web app, such as the scripting language used, the server's operating system, server software and the version, open network ports, and services running on the server. Nmap network scanner is one of the tools to be used.
2. DNS forward and reverse lookup – to associate IP addresses with the fully qualified domain names (FQDN) or subdomain of the web app, we will utilise nslookup.
3. DNS Zone transfer – to attempt the DNS transfer zone, the 'dig' command line will be used. The goal is to identify related external sites related to the target server and monitor traffic exchanged.
4. Analyse HEAD and OPTIONS request – to obtain information about the webserver software and its version, analysis of the response generated from the HEAD and OPTIONS HTTP REQUEST will be performed.
5. Inspecting the source code – to discover other vulnerabilities, we will inspect the source code to determine the application environment and discover the application's overall functioning.
6. Automated vulnerability tools- to supplement reconnaissance, we will use automated vulnerability scanning tools such as pentest-tools.com and ImmuniWeb network security test tool.

Documentation and Investigation of gathered data

- Information and vulnerabilities discovered during the reconnaissance will be documented for classification and investigation of the discovered vulnerabilities.
- Open Web Application Security Project (OWASP), Center for Internet Security, cve.mitre.org, and other scholarly research papers will be used to research and investigate identified vulnerabilities.
- Detected vulnerabilities will be classified by the categories Network, Application, and Software
- The probability and severity of each identified vulnerability will be factored into determining the risk rating it poses to the web application. Classification of the identified vulnerabilities will be a derivative of the risk rating. The rating will rank from low, medium to high.

Q: A list of the tools you will use, justifications for why you selected the tools.

1. Nmap (Network Mapper)- to discover basic information on the target website. Leverage the tool's scripting module that can be used to detect vulnerability and backdoor and execution of exploitations. To discover network information of the target web application such as open ports, ICMP request to check if the system is available and the services offered and detecting security risks.
2. OWASP ZAP Proxy- to discover security vulnerabilities in web applications such as the following:
    - SQL injection
    - Broken Authentication
    - Sensitive data exposure
    - Sensitive data exposure
    - Broken Access control
    - Security misconfiguration
    - Cross-Site Scripting(XSS)
    - Insecure Deserialisation
    - Components with known vulnerabilities
    - Missing security headers
3. Traceroute, Pathping, nslookup, ping, and whois- to analyze the accessability and the network location of the web application.
4. Nikto-to supplement the capabilities of the ZAP proxy tool. Nikto performs comprehensive tests for multiple items, including outdated 1250 servers, and version specific problems on over 270 servers

Q: The methodology you will use.

Open Web Application Security Project. This framework assists with identifying vulnerabilities in web and mobile applications. The updated guide of OWASP provides 66 controls to identify and assess vulnerabilities with numerous functionalities found in the latest applications currently.

Q: A list of any (potential) impacts on normal operations caused by using the tools.

- Complications with Availability (DoS)- Certain penetration activities, such as automated scanning, have the potential to cause disruptions, more so on legacy systems.
- Accidental Confidentiality violation – Unintended disclosure of sensitive information while conducting penetration testing activities.
- Email flooding results from web forms with no CAPTCHA protection (Beaver, Kevin(Principle Logic, 2018).
- The risk of filling databases with illicit data junk data can be difficult to clean after penetration testing (Beaver, Kevin(Principle Logic, 2018).
- The need to use IT, security and development resources in ensuring the production environment remains stable during application testing.
- Impacting system performance negatively.

Q: A list of assumptions and limitations of the tools and outputs produced.

Assumption of availability of the web application to be tested: The stated timeline can only be met if the testers if the web application is available for testing.

Limitation of time: Penetration testing is an activity that is, in most cases, carried out with a defined period. The testing team has a specified period to identify threats and vulnerabilities and produce results in the form of a report. In contrast, attackers are not bound by time constraints and have ample time to identify and explore more vulnerabilities. Thus, timed penetration test provides the attacker with an edge over the tester, allowing them more time to exploit the vulnerabilities.

Limitation of Access: Pentester often has restricted access to the target environment. Such penetration tests would not reveal misconfiguration issues and potential vulnerabilities on the entire network that a white box vulnerability assessment would reveal.

Limitation of Methods: Depending on whether the production or staging environment is the testing target, conducting a penetration test is intended to exploit the system by performing transactions that the system was not intended to handle. Thus, during penetration testing, the testing team may be limited to specific methods to use in order to avoid downtime. For instance, creating a denial of service flood attack may impact the production system (Cure, 2020).

Q: A timeline for the completion of your task.

OWC Mark C (2021) states that two to six weeks is the period most penetration tests take to complete, from the initial discovery to the final report. We will finalize our testing activities until the 19th of July 2021.

References :

Beaver, Kevin (2018) *Testing applications in production vs. non-production benefits*. Available at: https://searchsecurity.techtarget.com/tip/Testing-applications-in-production-vs-non-production-benefits (Accessed: 12 June 2021).

Cure, A. (2020) *Major Limitations of Penetration Testing You Need to Know | Cypress Data Defense*. Available at: https://www.cypressdatadefense.com/blog/limitations-of-penetration-testing/ (Accessed: 12 June 2021).

OWC Mark C (2021) 'A Beginners Guide to Understanding Penetration Testing'. Available at: https://eshop.macsales.com/blog/56056-a-beginners-guide-to-understanding-raid/.