AccessReal

Penetration Test Process Specification

Version 1.0

i-Sprint
Trust without Boundaries

Table of Contents

1 Overview

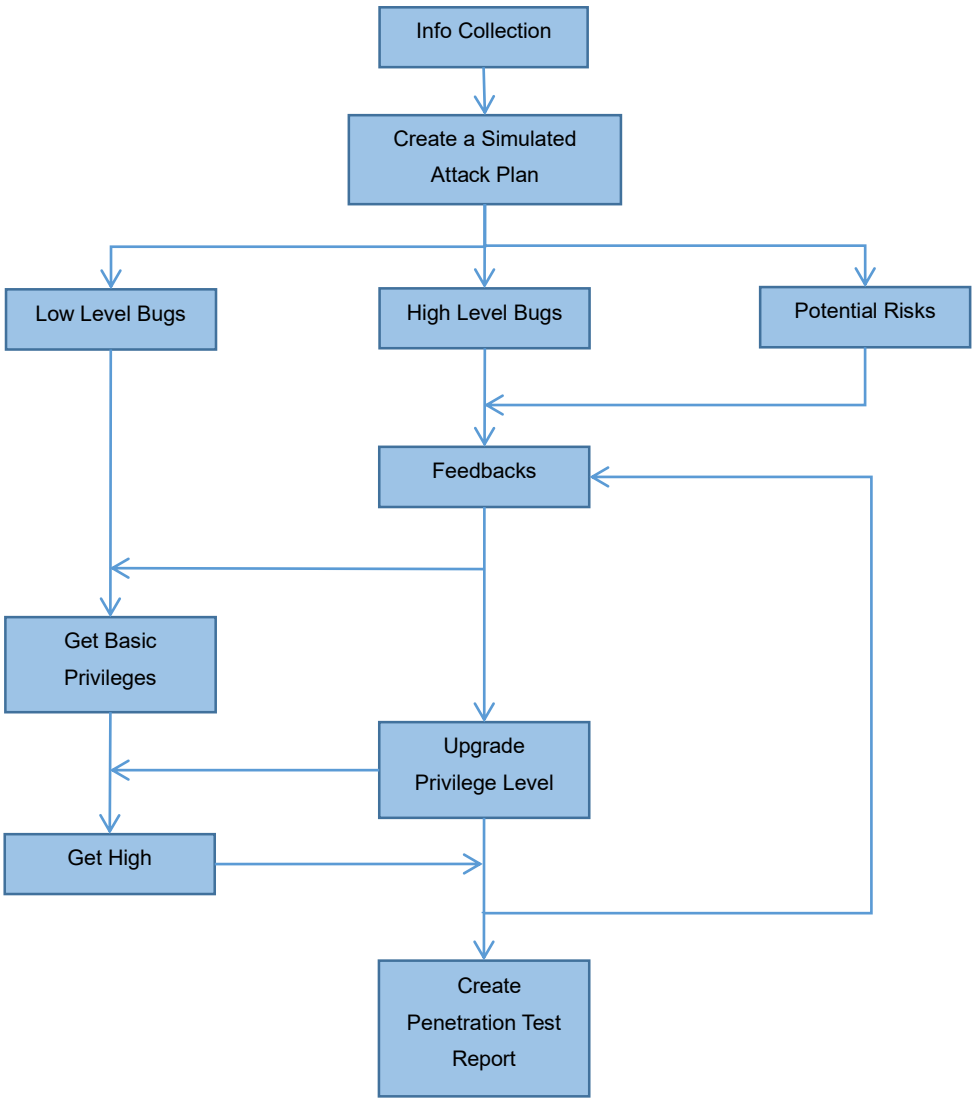
Penetration testing is based on security vulnerabilities that have been discovered by CVE (Common Vulnerabilities & Exposures) and the potentially hidden bugs. The penetration test simulates the intruder's attack method, will have non-destructive attacks on the AccessReal™ systems, server systems, and network devices.

Purpose

To determine the security threats in the AccessReal system and improve the security policies in a timely manner to reduce security risks.

2 Penetration Testing Process and Authorization

2.1 Penetration Testing Process Chart



2.2 Penetration Test Authorization

Test authorization is a necessary condition for penetration testing. Testers, system administrators, IT department heads, project leaders, and other relevant personnel should be aware of all the details and risks of penetration testing, work with testers and to give test authorization. The entire testing process must be carried out under risk control.

3 Penetration Test Methods

3.1 Test Objectives

- **Host Operating System**
  Penetration test for Linux operating system Centos.

- **Database System**
  Penetration test for MySQL and MongoDB.

- **Application System**
  Penetration test for various apps, e.g. the web applications consisting of CGI, JSP, XML and Java.

- **Network Device**
  Penetration testing of various firewalls, intrusion detection systems and network devices.

  The test technologies involved need to be different according to the test objectives. The followings are the descriptions of the technologies to be used in different locations.

- **Intranet**
  Intranet testing refers to the testers launching tests from an internal network that simulates the behavior of the internal violators. This test will bypass the protection of the firewall. Intrinsic possible internal penetration includes remote buffer overflow, password guessing, and B/S or C/S application testing.

- **External Network**
  External network testing means that the tester outside the network simulates the behavior of an external attacker who knows nothing about the internal state. These include the remote attacks on the network devices, password management security tests, firewall rule heuristics, evasion, and the security testing of Web and other open application services.

3.2 Information Collection

Info collection analysis is the premise of all intrusion attacks. Through the collection and analysis of network information, plans for simulating hacking attacks can be formulated accordingly to improve the success rate of intrusion, reduce the probability of exposure or discovery.

The methods of information collection include host network scanning, account scanning, operation type identification, application identification, configuration identification and others. The tools for simulating intrusion attacks include Nmap, Nessus, X-Scan, etc. Many tools that build into the operating system (such as telnet) can be very effective simulation attacks.

3.3 Port Scanning

This is the basis for all penetration testing by scanning the TCP/UDP port of the destination address to determine the number and type of services it is open to.
Through the port scanning, you can determine the basic information of a system, combined with the tester's experience to determine its possible existence, as well as the security weaknesses that are exploited, to provide a basis for deep penetration tests.

3.4 Privilege Level Upgrade

Through the collection of information and analysis, there are two potential results.

- The target system has major vulnerabilities: the tester can directly control the target system, and then investigate the distribution of vulnerabilities and causes in the target system to form the final test report.
- The target system has no major remote vulnerabilities, but can obtain remote normal privileges, and the tester can further collect the target system information through the normal privileges, and then upgrade the privilege levels. The results of these non-stop information collection analysis and privilege escalation will constitute the output of the entire penetration testing process.

3.5 Penetration test for Segment/ Vlan

The penetration test targeted at the Segment/ Vlan from an internal network or external network segment. The remote attack targets can be the network devices, wireless devices and firewalls (to spy its rules or how to bypass it). Tester needs to collect and analyze information for every test steps. Each of these test steps has three components that includes the operation, response, and the results analysis. The tester shall enforce the penetration test steps, get the result/response, and analyze them.

3.6 Overflow Test

When the tester cannot directly log in to the system with the account password, the system overflow will be directly obtained by the system overflow test. This method will cause the system to shut down or restart, but it will not cause system data loss. It just need to reboot the system and start the original system services. Tester will test overflow if only he or she is authorized to do so.

3.7 SQL Injection Attack

SQL injection is common in web servers that use the SQL database backend. By submitting some special SQL statements, it is possible to obtain, tamper with, and control the contents of the website server database.

3.8 Hidden Fields Detection

The web application system often uses hidden fields to store information, and attempts to conduct malicious transactions and steal information by operating hidden field contents in completing the penetration test task.

3.9 Attack via Website

You can use the website to attack end users who visit this target website, and then get the user password or use the site to control the client.

3.10 WEB Application Test

Web script and app tests are for AccessReal™ Web and database server. The target is to get the system access privilege or even the system control privilege. This test check points are:
Web scripts and application tests are specifically used at AccessReal™ web and database servers of the security system. The main objective is to obtain the system access and control privileges. The parts that need to be checked include:

- Check the application architecture to prevent users from bypassing the system and directly modifying the database.
- Check the user's identity authentication module to prevent illegal users from bypassing identity authentication.
- Check the database interface module to prevent users from obtaining system privileges.
- Check the file interface module to prevent users from obtaining system files.
- Check if there are any other security threats.

3.11 Codes Review

Conduct a security code review of the AccessReal™ system website to check if there are any codes/bugs that may cause problems. The codes review test work includes the followings:

- Examine the XSS script vulnerability in the code.
- Review the SQL injection vulnerability in the code.
- Review the potential buffer overflows in the code.
- Review malware codes that can be used to attack in the code.
- Review of other code errors or vulnerabilities.

4 Reduce Test Risks

The penetration test may impact the business. The following measures can be taken to reduce the risks.

- The test policy shall exclude DOS (Denial of Service) attack.
- Try to arrange the test during the low business period or at night.
- The test shall be stopped immediately if the testing system stop responding during the penetration tests. Analyze the situation with the relevant personnel of the user. After determining the cause and waiting for the system to be properly restored, take necessary precautions (such as adjusting the test strategy) before proceeding.
- Testers will maintain good communication with the system administrators to resolve any problems that arise at any time.
- The tester will complete the data in the process of the R&D test: operation, response, analysis, and finally forms a complete and effective penetration test report. The solutions, data and reports involved in the penetration test must be encrypted and properly kept.