From
The Eye,
Computer Science and Engineering Association,
PSG College of Technology,
Coimbatore.

22nd November 2022

To
The Principal,
PSG College of Technology,
Coimbatore.

Through
The HOD,
Department of Computer Science and Engineering,
PSG College of Technology,
Coimbatore.

Subject: Black Box Penetration Testing

Respected Sir,

I wish to humbly request your permission to conduct a black box penetration testing on PSG College of Technology under the CSEA (The Eye) club.

We would like to conduct a penetration testing operation on PSG College Of Technology servers and websites and make a report on all the security vulnerabilities and proposed mitigation solutions and techniques.

The abovementioned operation will be purely ethical and no critical data will be leaked.

This operation will be carried out only by Aaditya Rengarajan (21Z202) and R. Ajay(21Z239) of BE CSE G1 Second Years. We wish to request for any possible mode of recognition on our findings – it may be monetary or through other means of physical reward.

With this request, I have attached a study on Black Box Penetration Testing.

I look forward to updates on approval for the same.

Yours Respectfully,
Aaditya Rengarajan (21Z202),
R. Ajay (21Z239)
Point of Contact, The Eye.
BE CSE - G1 (Second Year)

The Eye,
CSEA

A Study on Black Box Penetration Testing

Prepared By
Documentation
Wing of The Eye

Penetration Testing

A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the weaknesses in a system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of.

Black Box Testing

Black box testing is a type of software testing in which the functionality of the software is not known. The testing is done with or without the internal knowledge of the organization. Black Box Testing mainly focuses on input and output of software applications and it is entirely based on software requirements and specifications. It is also known as Behavioral Testing.

Starting Vectors for Black Box Testing

1. Software designed to produce brute-force attacks or SQL injections.
2. Hardware specifically designed for pen testing can also be used. They are inconspicuous boxes which are attached to a computer on the target network, to get remote access to the network.
3. Social engineering techniques can also be used. Examples are sending phishing emails to company employees.
4. It can also include Dumpster Diving to get access to important hardrives etc.

Black Box Penetration Testing Procedure

1. ***Preparation and intelligence gathering*** – This phase officially marks the beginning of a pen-test. Testers begin by collecting as much information as possible on the organization, which is done through online searches, public information queries, and, in some cases, social engineering.

2. ***Vulnerability Identification and Threat Modeling*** – In this phase the tester decides which strategies they'll take when running mock attacks on the system. This phase lets the tester see how effective—or ineffective—the current network security truly is.

3. ***Penetration*** – This is when the actual penetration and subsequent testing occur. Professional testers utilize every tool at their disposal when trying to penetrate the system or exploit any identified vulnerabilities, including network-based attacks, wireless network exploitation, and memory-based attacks.

4. ***Risk Analysis*** – This phase only occurs after the tester has gained access to the system. From here, it determines how deep one can penetrate the network, including any vulnerable assets, databases, or other resources. This step generally represents the brunt of the tester's work and expertise.

5. ***Reporting and review*** – Scheduled as the final step, the tester will present their findings during the reporting phase. Recommendations will be provided on how one can improve their security framework in the future.

Organization Level Procedure for Penetration Testing

The penetration testing process can be broken down into five stages

1. Planning and Reconnaissance

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used. Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using,

Static analysis – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.

Dynamic analysis – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.

3. Gaining Access

This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try to exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis

The results of the penetration test are then compiled into a report detailing:

· *Specific vulnerabilities that were exploited*

· *Sensitive data that was accessed*

· *The amount of time the pen tester was able to remain in the system undetected.*

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Positive Outcomes of Pen-testing

Exposing Vulnerabilities

A penetration test is one of the best ways to expose potential vulnerabilities in system. This can be in relation to a cloud database, an in-house service or any form of tech system that is being operated. This ability to expose vulnerabilities is vital to ensure that the system is as secure as it possibly can be.

· **Acknowledges the System Strengths**

The ability for a penetration test to also show where the system is strong and is also beneficial. This can enable one to focus more time and effort on areas of the system that aren't working. It also shows the techniques that have been implemented which have been paid off. These can then be utilized on additional systems in the future, now that one knows they work. This ability to take both the positive and the negative is what helps these kinds of tests provide a comprehensive report.

· **An Authentic Simulation**

A penetration test is designed to simulate what an actual hacker might go through to get into the system. This makes it a test that's very true-to-life in the way it's designed. This is a notable benefit for penetration tests, as it's an authentic way of testing how secure the system really is. The parameters are the same as they would be if an actual hacker tried to enter the system.

· **Helps to Improve the Compliance**

Another way in which penetration tests can benefit the business lies in regulation and compliance. A pen-test can be used to ensure that the system's design is in keeping with any current regulations. If it isn't, these problems will be flagged by penetration testers.

· **Keeps the Data Protected**

Data protection is one of the most important aspects of security for all businesses today. If one's not keeping their company and customer data secure, they're risking serious breaches down the line. A penetration test can check to ensure that none of the data is reachable by an experienced hacker. If it isn't protected, then a pen-test will let them know about it. They can then quickly make any changes to the system based on the feedback obtained from the test.

· **Provides a Cyber Chain Map**

Because a penetration test simulates a real hack, they're able to see the kind of direction a hacker might go through their system. This is usually what's known as lateral movement. This is because a hacker usually penetrates a system, they must go deeper to find the most secure data. If

they're conducting a penetration test, one will be able to map a full route through their system's security. This can be a good way of showing which barriers are working, and which aren't.

·**Provides Thorough Feedback for the Employees**

If the system one's operating on is their own, chances are their own employees will need to make the changes required. Therefore, penetration testing can help, thanks to the thorough feedback this kind of test into cybercrime provides. It can ensure that their employees have a detailed map of what's working, as well as what isn't. This can give them key targets to focus on when they come to modify the security features of their system.

Penetration Testing Report / VAPT Report -

A Penetration Testing report is a document that contains a detailed analysis of the vulnerabilities uncovered during the security test. It records the weaknesses, the threat they pose, and possible remedial steps. The Pentest Report gives one a complete overview of vulnerabilities with a POC (Proof of Concept) and remediation to fix those vulnerabilities on priority. A good penetration test report also gives a score against each found issue and how much it can impact one's application/website.

Expectations from Penetration Testing Report -

Risk Level Descriptions

As there are no standardized risk level descriptions, it's important that the report has risk level measurements so that one understands the level of risk for each finding. A clearly defined description supports the rest of the penetration test report. Each risk that the tester identified should be divided into different levels:

- *Critical-risk*
- *High-risk*
- *Medium-risk*
- *Low-risk*
- *Informational findings*
- *Remediated findings*

Executive Summary

A good penetration test report starts with a clear and concise summary of its contents, laid out in simple, non-technical language that can be understood even by those who don't have a background in software or technology. The main purpose of an executive summary is to effectively communicate the risks and consequences of a security breach to the organization. In order to do that well, the summary should mention the scope, objectives, methods, data accessed, possible losses, and recommendations.

Approach

The approach section should highlight the scope of the test and objectives. To ensure compliance with most regulatory requirements, it's important to ask your penetration tester what methodology one uses to ensure regulatory requirements are met.

Methodology

The methodology shows high-level phases and what areas were tested. The Methodology section should indicate what testing was conducted and whether the testing was automated or manually conducted.

Technical Findings

The penetration testing report should clarify how valuable the assets that were accessed were, and the possible consequences of a breach.

Data that was accessed during testing should also be included. There are different types of data that leave an organization or business vulnerable if it was hacked. Assets include information about a business that could be advantageous to their competition, or data about their consumers that could violate privacy laws if revealed.

Recommendations

Recommendations should be detailed and unique to each system and organization. Documented steps to reproduce findings to ensure application developers can validate remediation efforts prior to re-testing should also be included. Unique and customized recommendations pertaining to the client's specific security status should be included.

Conclusion

It is important to understand the findings and recommendations in the penetration testing report to make informed security decisions for one's company. It is also vital to fill the gaps and prevent vulnerabilities that remain in the application or system. A trusted pen testing partner is key when conducting a successful pen test and achieving your internet security business objectives.

Case Study Example

This real-life incident includes all the processes followed by an organization called **UNDER DEFENSE** in penetration testing to a client.

Background

One of the world's leading international oil and gas companies, providing fuel, energy, retail services and petrochemicals, best known to the public for its service stations and for

exploring and producing oil and gas on land and at sea. Prominent in over 140 countries and territories and employing more than 112,000 people around the globe

The Challenge

Holding a major global presence and continuously being targeted, our client understood the risks they faced on a daily basis. In order to meet compliance and regulation standards they engaged the Security Team at UnderDefense to conduct and full black-box Organizational pen test, to learn more about the vulnerabilities they have and how they can be remediated

Additionally, the customer had specific business continuity and compliance requirements, relating to its duty of care to maintain employee and clients personal and financial data. With a multinational presence the pen test itself was conducted on multiple territories to ensure the highest level of results.

Process and Technology

TEST PLANNING *- Meeting with consumer goals, align test goals and scope, intelligence gathering.*

VULNERABILITIES IDENTIFICATION*- Potential vulnerabilities deduction, threat modeling, business process analysis.*

VULNERABILITIES EXPLOITING*- Vulnerabilities testing, vulnerabilities validation, vulnerabilities research.*

POST EXPLOITATION*- Escalating privileges, infrastructure analysis, vulnerabilities research.*

With a team of 4 engineers and a duration of 4 weeks it was were possible to fully compromise not only the organizations infrastructure but also, web applications as well as expose critical data related to key organizational stakeholders.

Result

Penetration testing is often done for varying reasons. Two of the key goals that were aimed for, were to increase upper management awareness of security issues and to test intrusion detection and response capabilities. After conducting the pentest and compromising the organization, UnderDefense engaged the client in a controlled offensive/defensive threat detection challenge , allowing the client several days to identify and remediate active threats within their systems. After this challenge was completed UnderDefense was commissioned to conduct training for the key internal security team as well as further advisory on remediation tactics. In the end the client was able to meet the highest level of compliance and regulation standards, develop better security practices and reassure their customers, employees, and board of their continued dedication to best business practices and continued growth.

Example Of Critical Issues That Have Been Exploited Due To Insufficient Testing

Remote Management Services

Remote management services help perform critical tasks such as managing a network device etc. Sometimes, these services are offered over an insecure protocol/interface despite there being safer alternatives available. Examples of insecure protocols include TFTP, FTP, Telnet, and HTTP. These do not offer encryption and so any communications that travel over these can be easily sniffed by a malicious actor and stolen with remarkable ease. Add to this the fact that these are, sometimes, also poorly configured – such as an FTP with anonymous access.

Unencrypted protocols should be completely avoided when offering these remote management services. Remember that the default settings often use insecure protocols. Change

them and use secure alternatives that offer strong encryption. Furthermore, place restrictions on who can access your critical remote management services instead of leaving them open for anyone to connect.

Default Passwords and Settings

This is the lowest of all the low hanging fruits out there. Software and hardware often ship with factory default settings and passwords. While thankfully, the incidence of this issue has declined over the years, there are still enough times when penetration testers and ethical hackers encounter it. What is worse: the issue occurs across the board - from printers to routers and from databases to load balancers.

The process to deal with this issue ties in closely with patch management practices. Create a reliable inventory of software and hardware that you track closely and update on an ongoing basis. This will make it easier to ensure no defaults are being used. And again, restricting access to critical infrastructure devices and systems is important. Hackers love probing for defaults. If we don't fix them, they will find them. It's only a matter of time

Weak Encryption

Encryption is one of those things where everyone will always find themselves playing the game of catch up. For instance, there was once a time when 56 bits of encryption was reasonable, but now even 128 bits isn't comfortable enough. Penetration testers and ethical hackers come across weak encryption issues in almost every penetration test. Obsolete encryption protocols and weak encryption ciphers are very common to see. These issues make attacks like man-in-the-middle (MITM) attacks easy to execute for hackers.

Error Messages

When a web page doesn't load, it's not unusual to see an error page. These pages, though, sometimes have verbose error messages that inadvertently reveal information about the underlying infrastructure.

For hackers, these are treasure troves. These could include internal paths, stack traces, code snippets, database queries, and just about anything that the underlying platform decides to spew out the moment it is unable to handle a particular request. The information in these error messages can be leveraged to mount serious and targeted attacks. Hackers are aware of this possibility and it is handled by sending specially crafted requests that the infrastructure doesn't know how to handle which then leads to information leakage.

For applications, this is an issue that developers need to resolve. Better error-handling measures need to be incorporated during application development. Developers need to ensure that applications only issue generic error pages that do not reveal sensitive internal information. User input needs to be adequately validated before being processed to avoid generating error messages in the first place.

The #1 priority is to focus on the critical and high-severity findings in the pen-test report *as they represent the biggest risk and may be more likely to be exploited. Determine the order of priority before moving forward because some issues may be more important to one's organization than others.*

As a general rule, the penetration testing provider should list the discovered vulnerabilities in order of criticality and priority to one's organization.

Patch Management

The most rudimentary way to remediate vulnerabilities uncovered in a pen test would be to check each system and update each affected component individually. If one's scope is small and one doesn't have the tools to automate this process, then that's fine, and in some cases it may even only be possible to do this manually. Obviously, this is not an efficient process, and software can help automate some of this process for larger organizations.

There are a multitude of patch management applications out there which aid in patch and security deployment automation that can be heavily relied upon in environments of all sizes. There is a popular product called Microsoft System Center Configuration Manager (SCCM) which enables management of Microsoft endpoint systems from a central server. Admins can easily use such tools to control the deployment of patches and updates on all types of systems.

Pentest reports often reveal very specific vulnerabilities that require manual validation and fixing. In these cases, a system may have to manually be accessed to test for a vulnerability and patch it. Depending on the size of one's pen test and the number of findings, this could be a laborious effort but is a required step nonetheless. Even though it takes some time, it's important to have a process for testing and verifying a vulnerability and manually patching.

From
The Eye,
Computer Science and Engineering Association,
PSG College of Technology,
Coimbatore.

22nd November 2022

To
The Principal,
PSG College of Technology,
Coimbatore.

Through
The HOD,
Department of Computer Science and Engineering,
PSG College of Technology,
Coimbatore.

Subject: Grey Box Penetration Testing

Respected Sir,

I wish to humbly request your permission to conduct a grey box penetration testing on PSG College of Technology under the CSEA (The Eye) club.

We would like to conduct a penetration testing operation on PSG College Of Technology servers and websites and make a report on all the security vulnerabilities and proposed mitigation solutions and techniques.

The abovementioned operation will be purely ethical and no critical data will be leaked.

This operation will be carried out only by Aaditya Rengarajan(21Z202) and R. Ajay(21Z239) of BE CSE G1 Second Years. We wish to request for any possible mode of recognition on our findings – it may be monetary or through other means of physical reward.

With this request, I have attached a study on Grey Box Penetration Testing.

I look forward to updates on approval for the same.

Yours Respectfully,
Aaditya Rengarajan (21Z202),
R. Ajay (21Z239)
Point of Contact, The Eye.
BE CSE - G1 (Second Year)

The Eye,
CSEA

A Study on Grey Box Penetration Testing

Prepared By
Documentation
Wing of The Eye

Penetration Testing

A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the weaknesses in a system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of.

Grey Box Testing

Penetration testing is a simulated cyber-attack on a system checking for exploitable vulnerabilities. In other words, penetration testing is a type of security testing which helps one to secure the system from external security attacks. The targets of this test may be white boxes (all information known) or black boxes (basic information known) or grey boxes (partial knowledge about the system).

Grey box testing is a software testing type which looks into the system's architecture and internal structure to find potential errors. White box or transparent testing is where the tester has complete access to the infrastructure, source code, etc. Black box or opaque testing is where no details about the system and its source code are shared with the tester. Grey boxes or translucent testing are a combination of both white and black boxes with their best features combined.

Step-by-step procedure:

This grey box testing follows a series of steps:

1. Requirement analysis
2. Reconnaissance phase- surveying and researching
3. Initial exploitation
4. Advanced security testing
5. Clearing tracks
6. Report preparation.

Basic Requirements from organization:

The organization provides internal infrastructure details to the tester not the entire source code for grey box testing. Even without the entire source code, the tester will be able to identify most of the vulnerabilities in the systems. Organizations in various industries namely payment card service industry, financial institutions, tech industries and the medical sector are obliged to carry out this test in regular intervals.

Basic requirements from the testers:

The testers for performing grey box testing require,

- Ability to read architecture diagrams and design documentation and determine vulnerabilities at a system as well as local level.
- Partial knowledge of high-level programming languages.
- Ability to tackle difficult situations in case they arise
- A certification and past experience maybe.

Their aims are to:

- Try and attempt to breach into the security of the organization.
- Discovers the possible ways in which hackers may try to attack the system with the use of functional specifications and other design documents and enhance the security.

Organizational level procedure:

Companies normally take measures regarding vulnerability, confidentiality and integrity of data before allowing one into the organization. There are legal regulations that must be followed when a test is performed. There should be a written agreement duly signed by both parties regarding the data security, sharing, etc.. prior to any testing work.

Benefits of this test:

- Unbiased and non-intrusive
- Done from the user's perspective
- Less time consuming
- Reduces dependence of tester on developer
- Cost effective
- Primarily used in integration and penetration testing.

Techniques in grey box testing:

There are many effective techniques using which this testing can be performed. Some of them are:

Matrix Testing:

In matrix testing technique, business and technical risks which are defined by the developers in software programs are examined. Developers define all the variables that exist in the program. Each of the variables has an inherent technical and business risk and can be used with varied frequencies during its life cycle.

Pattern Testing:

To perform the testing, previous defects are analyzed. It determines the cause of the failure by looking into the code. Analysis template includes reasons for the defect. This helps test cases designed as they are proactive in finding other failures before hitting production.

Orthogonal Array Testing:

It is mainly a black box testing technique. In orthogonal array testing, test data have n numbers of permutations and combinations. Orthogonal array testing is preferred when maximum coverage is required when there are very few test cases and test data is large. This is very helpful in testing complex applications.

Regression Testing:

Regression testing is testing the software after every change in the software to make sure that the changes or the new functionalities are not affecting the existing functioning of the system. Regression testing is also carried out to ensure that fixing any defect has not affected other functionality of the software.

Report of grey box testing:

Every report of grey box testing prepared after the test is over must contain:

- Report properties including details about the organization as well as the testers.
- Executive summary of the test which is understandable even to non-technical readers.
- Tools used by the tester team
- List of findings in detail-security risks and vulnerabilities identified by the security breaches
- Suggestions to improve the defense mechanism.

Real life case study:

One of example of a real-life case study is the penetration test by Under Defense for an oil and energy platform. The organization wanted to know all the vulnerabilities and secure the payment portals as they'll be using digitalized transactions.

The key goals of this test were to test intrusion detection and response capabilities. This helped the organization save a lot of money and provide better security protection. They were also cautious on securing the client's data which was also tested and remediation methods were provided.

Critical issues due to insufficient testing:

A company had been getting penetration tests done every quarter of the year. Many teams have tried and tested the security with passing years. But after 16 such tests, in the successive one, a vulnerability was detected that was missed by all 16 tests. This could have cost 100 million dollars loss to the organization. The automated tools used in those 16 tests are not so efficient as it scans the system for known vulnerabilities only. The final test performed through advanced tools found the vulnerability.

Critical issues (LOG4J issue):

On December 2021, LOG4J, one of the most serious zero-day issue was discovered. This is an open-source Java based software, maintained by Apache used for logging by major companies in the world. Within days of its identification, all organizations were on the verge of their seat waiting for the security researchers to patch up the software. The LOG4J vulnerability, first identified in the game of Mine craft, provides access to external servers and leaks client data to the hacker which could result in huge losses for the company. Another major issue of the LOG4J is as it is used in different software in different manners, there is no single fix for all the software. Different patches were found and Apache offered an updated software which has temporarily resolved the issue. Yet there may be a day when a major company may be exploited.