Penetration Testing methodology

NOTICE

Version Control

Version No.	Version Date	Changes	Owner/ Author	Date of Review/Expiry
V1.0	30-Jan-2019	First Release	Adrian Tudor	

Table of Contents

Purpose

The purpose of this document is to describe the Genpact's Penetration Testing Program that defines the overall methodology of the Penetration Testing processes that will govern the Penetration testing team activity.

Objective

The objective of the Penetration Testing methodology is to assess the security within Genpact through a simulated cyber-attack, improve team's organizational readiness, evaluate the effectiveness of your IT security defenses and controls and gain objective insight into vulnerabilities that may exist within Genpact's environment.

Penetration testing Phases

1. Preparation
    a. Pre-engagement Interactions
2. Testing
    a. Intelligence Gathering
    b. Vulnerability Analysis
    c. Exploitation
    d. Post Exploitation
    e. Reporting
3. Follow up
    a. Remediate weaknesses
    b. Address root causes of weaknesses
    c. Build on lessons learned

1. Preparation

a. Pre-engagement Interactions

In this phase we'll identify target environments, produce the requirements specifications, agree on the testing style and type and Identify the testing constraints. An assessment plan will be created that outlines assessment-related legal considerations that organizations may need to address.

Scoping Meeting:

During initial communications there are several questions which the Pentest requester will have to answer in order for the engagement scope can be properly estimated. Stress testing or Denial of Service testing should be discussed before the engagement begins.
In this phase of engagement, we'll define the approach for the Pentest:

1. White Box Penetration Testing: Here, the tester has complete access and in-depth knowledge of the system to be tested.
2. Black Box Penetration Testing: In black box penetration testing approach, high-level of information is made available to the tester. The tester is totally unaware of the system/network.
3. Gray Box Penetration testing: Gray box penetration testing makes only limited information available to the tester to attack the system externally.

General questions:

1. Why is the requester having the penetration test performed against their environment?
2. Is the penetration test required for a specific compliance requirement?
3. When does the requester want the active portions (scanning, enumeration, exploitation, etc...) of the penetration test conducted?
(a) During business hours?
(b) After business hours?
(c) On the weekends?
4. How many total IP addresses are being tested?
(a) How many internal IP addresses, if applicable?
(b) How many external IP addresses, if applicable?
5. Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion
detection/prevention system, web application firewall, or load balancer?
6. In order to move laterally in the network, privilege escalation will be performed on the systems. For this task services may be modified. Are there any services "critical" to the infrastructure that we are not allowed to modify?

Specific questions:

Web Application Penetration Test

1. How many web applications are being assessed?
2. Will the source code be made readily available?
3. Will there be any kind of documentation?
(a) If yes, what kind of documentation?

Wireless Network Penetration Test

1. How many wireless networks are in place?
2. Is a guest wireless network used? If so:
(a) Does the guest network require authentication?
(b) What type of encryption is used on the wireless networks?
(e) Will the team be assessing wireless attacks?
(f) Approximately how many clients will be using the wireless network?

Social Engineering

1. Does the requester have a list of email addresses they would like a Social Engineering attack to be performed against?
2. Does the requester have a list of phone numbers they would like a Social Engineering attack to be performed against?

Emergency Contact Information

Emergencies may arise, and a point of contact must have been established in order to handle them. Create an emergency contact list. This list should include contact information for all parties in the scope of testing. Once created, the emergency contact list should be shared with all those on the list. Also the requester team may also need to contact the testers in an emergency.

The list should include the following people:
1. All key contacts from the requester side (24/7 immediate contact if possible)
2. All penetration testers in the test group for the engagement
3. The manager of the test group

Incident Reporting Process

Part of a penetration test is not only testing the security an organization has in place, but also their incident response capabilities.
If an entire engagement can be completed without the target's internal security teams ever noticing, a major gap in security posture has been identified. It is also important to ensure that before testing machines, network segments, etc., that are being monitor by CDC, someone from organization is aware of when the tests are being conducted so the incident response team does not start the escalation procedure and alert upper management in the middle of the night because they thought they were under attack or compromised.

2. Testing Methodology

a. Intelligence Gathering

This section defines the Intelligence Gathering activities of a penetration test. Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the systems in scope during the vulnerability assessment and exploitation phases.

Footprinting

External information gathering, also known as footprinting, is a phase of information gathering that consists of interaction with the target in order to gain information from a perspective external to the organization

1. Passive Reconnaissance
   -WHOIS Lookups

2. Active Footprinting
   - Port Scanning
   - Banner Grabbing
   - SNMP Sweeps
   - Zone Transfers
   - SMTP Bounce Back
   - DNS Discovery, Forward/Reverse DNS, DNS zone transfer
   - Identify lockout threshold
   - Directory services (Active Directory)

Example activity:
SNMP Sweeps

SNMP sweeps are performed too as they offer a multitude of information about a specific system. The SNMP protocol is a stateless, datagram oriented protocol. Unfortunately, SNMP servers don't respond to requests with invalid community strings and the underlying UDP protocol does not reliably report closed UDP ports. This means that "no response" from a probed IP address can mean either of the following:
- machine unreachable
- SNMP server not running
- invalid community string
- the response datagram has not yet arrived

Identify lockout threshold

Identifying the lockout threshold of an authentication service will allow you to ensure that your bruteforce attacks do not intentionally lock out valid users during your testing.

b. Vulnerability Analysis

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design.

Automated testing utilizes software to interact with a target, examine responses, and determine whether a vulnerability exists based on those responses. An automated process can help reduce time and labor requirements.

Validation

Penetration team may leverage the tools from the Vulnerability Management program for correlation of findings between multiple tools in order to validate them. Once a vulnerability has been reported in a target system, it is necessary to determine the accuracy of the identification of the issue, and to research the potential exploitability of the vulnerability within the scope of the penetration test. Vulnerability Databases and Vendor Advisories may be consulted in this scope.

c. Exploitation

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions.

d. Post Exploitation

The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network

The following rules are to be used as a guideline of rules to establish with a requester team to ensure that the day to day operations and data are not exposed to risk:

Unless previously agreed upon, there will be no modification of services which the client deems "critical" to their infrastructure. The purpose of modifying such services would be to demonstrate to the client how an attacker may:

– Escalate privileges
– Gain access to specific data
– Cause denial of service

All modifications, including configuration changes, executed against a system must be documented. After
finishing the intended purpose of the modification, all settings should be returned to their original positions if possible. Changes that could not be returned to their original positions should be clearly differentiated from changes that were successfully reversed.

Passwords (including those in encrypted form) will not be included in the final report, or must be masked enough to ensure recipients of the report cannot recreate or guess the password. This is done to safeguard the confidentiality of the users the passwords belong to, as well as to maintain the integrity of the systems they protect.

Any information included in the report that could contain sensitive data (screenshots, tables, figures) must be sanitized or masked using techniques that render the data permanently unrecoverable by recipients of the report.

If data gathered is regulated by any law, the systems used and their locations will be provided by the requester to ensure that the data collected and processed does not violate any applicable laws. If the systems will be those of the penetration testing team the data may not be downloaded and stored on to their systems and only proof of access will be shown (File Permissions, Record Count, file names..etc).

No logs should be removed, cleared or modified unless it was specifically authorized in the engagement statement of work. If authorized, the logs must be backed up prior to any changes.

Persistence

Installation of backdoor that requires authentication.

Installation and/or modification of services to connect back to system. User and complex password should be used as a minimum; use of certificates or cryptographic keys is preferred where possible. (SSH, Ncat, RDP). Reverse connections limited to a single IP may be used.
Creation of alternate accounts with complex passwords.
When possible backdoor must survive reboots.

Actions that can be taken from a compromised system:

- Upload tools
- Use local system tools
- ARP Scan
- Ping Sweep
- DNS Enumeration of internal network
- Directory Services Enumeration
- Brute force attacks

- Enumeration and Management thru Management Protocols and compromised credentials (WinRM, WMI, SMB, SNMP..etc)
- Abuse of compromised credentials and keys (Webpages, Databases..etc)
- Execute Remote Exploits

Cleanup

The cleanup process covers the requirements for cleaning up systems once the penetration test has been completed.

This will include all user accounts and binaries used during the test.

- Remove all executable, scripts and temporary file from a compromised system. If possible, use secure delete method for removing the files and folders.
- Return to original values system settings and application configuration parameters if they were modified during the assessment.
- Remove all backdoors and/or rootkits installed.
- Remove any user accounts created for connecting back to compromise systems.

e. Reporting

E template will be created with customized structure and Genpact branded format.

Report Structure

i. The Executive Summary: This section will communicate to the reader the specific goals of the Penetration Test and the high level findings of the testing exercise.
   a. Overall Posture: This area will be a narrative of the overall effectiveness of the test and the pentesters ability to achieve the goals set forth within the pre engagement sessions.
   b. General Findings: The general findings will provide details of the issues found during the penetration test in a basic and statistical format.
   c. Recommendation Summary: The recommendation section of the report should provide the reader with a high level understanding of the tasks needed to resolve the risks identified
   d. Strategic Roadmap: Roadmaps should include a prioritized plan for remediation of the insecure items found and should be align with the business objectives/ level of potential impact.

ii. Technical Report This section will communicate to the reader the technical details of the test

3. Follow up

In this phase Penetration testing team and the beneficiary of the test will follow up on the remediate weaknesses and address root causes of weaknesses.

Also Penetration testing can build on lessons learned from the engagement and identify opportunities of improvement for the penetration testing program.