Process Verbal of Validation Penetration Test

Date: [Enter Date]  
Auditor: [Auditor's Name]  
Subject:Validation of penetration test performed at [Organization]  
Reference: [Report Number]

I do process report of investigation report with reference [attribute] dated [date] issued by [organization name of pentesting party].

# What this official report looks at

This official report was prepared in response to an information security audit-validated, structured pen test, a report of which with underlying evidence was made available.

This record relates to the following documents, which were available to me at the time of the determination:

|  |  |  |
| --- | --- | --- |
| File name | Date | SHA256 |
|  |  |  |

The investigation report of the penetration test performed describes an investigation conducted under the auspices of [Name of Pentester]. The purpose of this document is to validate the report and underlying facts according to the established requirements as described in the Meow diagram version [VERSION HERE].

# Validation of the study

The report shows that the findings were established as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Informational**  **0.0** | **Low**  **0.1-.39** | **Medium**  **4.0-6.9** | **High**  **7.0-8.9** | **Critique**  **9.0-10.0** |
| **Number of findings** |  |  |  |  |  |
| **Number open after retest** |  |  |  |  |  |

Points from the chart

| **Claim** | **Validation** | **Found** | **Not found** |
| --- | --- | --- | --- |
| The research report is provided in digital form. | There is a file that the survey report. This is provided digitally. |  |  |
| The report includes the name of the rapporteur. | The report mentioned the name of an individual. This person was identified in the report as the rapporteur. |  |  |
| The report identifies the valid certification(s) held by the rapporteur. Valid certifications are: \* OffSec Certified Professional (OSCP) \* OffSec Experienced Pentester (OSEP) \* OffSec Offensive Security Certified Expert (OSCE or OSCE³) \* OffSec Web Expert (OSWE) \* Web application Penetration Tester eXtreme (eWPTX | The report named what certification this person has. This is one of the accepted certifications. |  |  |
| The report provides proof of certification in the form of a link to an online validation platform to validate the authenticity of the claimed certification or a copy of the diploma, allowing other validation. For digital documents, this link is not clickable; for hard copies, the link need not be clickable. | Every certification has a platform to validate the validity of the rapporteur's certification. By clicking and looking for the correct platform to validate that certification actually exists and taking a screenshot of this, validation can take place. |  |  |
| There is mention of the version number of the document in the "About this document" section. | The "About this document" section establishes the version number of the document. |  |  |
| The report shall be provided with a text, attesting that the report: 1. has been prepared accurately and truthfully; 2. a quality review of this version of the document has been conducted by other a person not involved in the study.  This text bears the signature of the rapporteur. This signature may be a physically placed signature or a digital signature. | Check for a statement in which the rapporteur states: 1. that the report was prepared accurately; 2. that the report was prepared truthfully; 3. that there was a review by another person not involved in the study.   Below this passage should be a signature of the rapporteur. A signature can be either a physical or digital signature. |  |  |
| The investigation is conducted according to the seven phases of the Pentest Execution Standard (PTES) (https://www.pentest-standard.org/index.php/Main\_Page). The seven phases are:  1.Pre-engagement Interactions (Pre-engagement Interactions) 2.Intelligence Gathering (Intelligence Gathering) 3.Threat Modeling(Threat Modeling) 4.Vulnerability Analysis (Vulnerability Analysis) 5.Exploitation 6.Post Exploitation 7.Reporting  This format is reflected in the reporting. | Is the reporting structured according to the seven phases of the Pentest Execution Standard (PTES). Are all seven components covered in the reporting. |  |  |
| There is a description regarding confidentiality for the contractor (rapporteur, researchers). It is described what this includes. If confidentiality is not agreed upon, this is also described. | The report describes the confidentiality applicable to the contractor (including rapporteur and researchers). If there is no confidentiality, this is also described. |  |  |
| No restrictions are imposed on the client with regard to distribution, publication or storage of the report and the underlying documents. Excluded from this are financial data relating to the execution of the study, such as hourly rates, prices and invoices. | There are no passages in the report that place restrictions on the client for sharing the report (e.g., publication, dissemination, distribution, storage, etc.) |  |  |
| The plan of action has a description of the intake interview. | There is a passage under the Interactions for Engagement (pre engagement) section titled "Intake Interview |  |  |
| It is named when the conversation took place. | The passage mentions when the interview was held |  |  |
| It names who participated in the interview including their respective positions. | Interview participants were named, with their functions described in the study. |  |  |
| It indicates what information must be provided before the study begins. | The passage contains the information still to be supplied to the rapporteur for the study. |  |  |
| There is a description of the scope of the study. This includes the relevant selection of parts and objects according to sub 2.2.1 to 2.2.8. The scope matches the needs from the intake interview and fits within the agreed time frame. | A check is made by the participants of the call, who verify that the scope matches the call. |  |  |
| The scope description includes the attack perspectives based on the intake interview, divided among: Greybox and Whitebox. Performing a blackbox test is expressly not included in this methodology | The scope description includes the agreed-upon attack perspective, which is validated by the client and contractor. A test based on greybox or a whitebox (also called crystelbox) is offered. A blackbox test is expressly not allowed. |  |  |
| The objects that have emerged as a result of the intake form the basis for the scope components and associated standards applicable in 2.2.3 through 2.2.8. All standards that may be applicable to the object in question are included in the scope. If there is a scope object with a specific version number, it must be recorded as part of the object. | The proposed standards fit the requested objects. Multiple standards may apply here (a web application is also on a network component, so PTES and WSTG may both apply). Possibly using a seperate matrix? |  |  |
| If intake interview reveals that a network survey is part of the pen test, the objects (IP addresses or IP ranges) should be tested according to the standard PTES. | In the presence of IP addresses or IP ranges (internal or external), the provider has offered the PTES over those components. |  |  |
| If the intake interview reveals that one or more Web applications should be tested, the objects (domain names, urls) should be tested according to the standard OWASP Web Security Testing Guide (WSTG). | In the presence of a web application object, the provider has offered the WSTG over relevant component. |  |  |
| If the intake interview reveals that part of the pen test is Internet of Things device(s), the objects should be tested according to the standard OWASP IoT Security Testing Guide (ISTG). | In the presence of an IoT object, the provider offered the ISTG over relevant component. |  |  |
| If the intake interview indicates that firmware of objects should be tested, this should be done according to the standard OWASP Firmware Security Testing Methodology (FSTM). | In the case of firmware in an object (embedded), the provider offered the OWASP Firmware Security Test. |  |  |
| If the intake interview reveals that an API should be part of the pen test, it should be performed according to the standard WSTG Chapter 12 API Testing | In the presence of an API, the provider offered the OWASP WSTG on relevant component. |  |  |
| If the intake interview reveals that a mobile application needs to be tested as part of the pen test, the output takes place according to the standard OWASP Mobile Application Security Testing Guide (MASTG). | In the presence of a mobile application, the provider offered the MASTG on relevant part. |  |  |
| Prior to start of the research, the complete list of exact research objects, attack perspective and components is known and recorded. | A list of exact research objects, attack perspective and scope components is included with the scope description. |  |  |
| Before starting the investigation, it was verified that the list of objects belonged to the client or permission was given by the entitled third party to perform the pen test. | 1. The objects are based on open sources (whois, domain registration, publisher) property of client. 2. Entitled third party has submitted written permission to perform the pen test. |  |  |
| Prior to starting the study, the legal framework was validated of the locations where the systems are physically located. The pen test is performed according to the legal frameworks there applicable. | There is an overview of the locations of the objects to be tested. If an object is located abroad, the conditions under which a pen test may or may not be performed in that country have been determined. |  |  |
| Prior to the start of the study, the scope was submitted to the client and confirmed. | A document (physical, pdf, e-mail) showing that the scope from head 2.2 has been submitted in its entirety to the client. The latter has confirmed it in writing or with a signature. |  |  |
| Prior to the pen test, the language in which the report is to be written is agreed and defined. | Agreements on the language of reporting are included. |  |  |
| A plan of action includes the purpose of the penetration test and any secondary objective(s) if they emerged in the intake interview. | An objective is included, which were validated by the participants of the intake interview. |  |  |
| An indemnification agreement must be signed between client and contractor before performing the penetration test, this indemnification agreement specifically refers to the scope | A signed disclaimer is present |  |  |
| The "assume breach" principle in pen testing (penetration testing) is an approach that assumes an attacker has already gained access to the network. Instead of trying to get in (as non MIAUW penetration testing does), one focuses on mitigating damage, discovering the attacker's presence, and recovering systems. This principle is intended to better prepare organizations in case a security incident occurs. | The report describes that work was done in accordance with "assume breach," with a listing of measures taken to make that possible also present. |  |  |
| A finding is assigned a value based on the Common Vulnerability Scoring System 4.0 or higher. | A CVSS score version 4.0 is provided with each finding. |  |  |
| CVSS scores should be calculated from the Base Metrics, supplemented by the Supplemental Metrics, Environmental (Modified Base Metrics - Vulnerable System Impact Metrics, Subsequent System Impact Metrics) and Threat Metrics. | By accessing the CVSS strings from the report at https://www.first.org/cvss/calculator/4.0. The CVSS strings included in the reporting also have values defined under supplemental, environmental and threat metrics. |  |  |
| The rapporteur shall store and have available to the client all scan results, productions and other results encrypted. All results shall be hashed so that the contents of the files can be verified. The parties shall agree on retention periods. | Evidence is available and can be requested. The hash value of the retrieved files match the report. |  |  |
| All scans are performed against scope objects that are determined in advance not to be additionally protected by a rate-limiting firewall, a Web application Firewall (WAF), or other measures in the communication line that may interfere with the scan results. | Evidence is available that the configuration of any intervening objects were adjusted or other protective measures were rendered inoperative. In addition, the investigator provides evidence that it was verified that other parameters (e.g., IP address or intensity of scanning) validated that additional protective measures for the study did not function during the study. |  |  |
| All detected and identified access paths that can connect to an investigated scope object are documented, even if they did not directly lead to misuse | There is a record of detected and identified access routes. |  |  |
| The report contains a numbered table of contents of chapters and sub-chapters |  |  |  |
| The report includes a methodology section that describes the lines of investigation - naming that the investigation is conducted according to the seven phases of the Pentest Execution Standard (PTES) (https://www.pentest-standard.org/index.php/Main\_Page). The seven phases are:  1.Pre-engagement Interactions (Pre-engagement Interactions) 2.Information Gathering (Intelligence Gathering) 3.Threat Modeling (Threat Modeling) 4.Vulnerability Analysis 5.Exploitation (Exploitation) 6.Post Exploitation 7. Reporting(Reporting) | The format of the chapters in the report conforms to the standard. |  |  |
| The report contains a sub-chapter within the methodology chapter - describing that the findings made by researchers are classified using the Common Vulnerability Scoring System (latest version available) and provided with a so-called CVSS vector string in order to be able to trace back how the calculation of the score was arrived at. | The report includes an explanation of CVSS and how they can be traced back to a CVSS calculation. |  |  |
| The report contains a section on the document (document management) - this section defines at least: Client, project number/name, project start and end date, rapporteurs, reviewers, document classification, version number of the document and the signature of the responsible rapporteur | The report contains the components on document management. |  |  |
| The report includes a section on version management - this section defines at least (by version): Version, Date, Author and Version Description | The report contains the components on version control. |  |  |
| The report includes a distribution list section - this section defines at least: Version, date, name, organization and distribution method | The report includes an overview about the distribution in the different versions. |  |  |
| The report contains a chapter in which the reason for the study is described, describing at least: whether there is a timeboxed test and if so, what the maximum hours are, which parts could not be (fully) tested and why not, a general description of the client's environments to be tested | The introduction contains information about the minimum preconditions under which the penetration test is performed. In addition, the report also includes whether certain components could not be tested and what caused that. |  |  |
| An objective is included that corresponds to what emerged during the intake. | The objective corresponds to that agreed upon with client. |  |  |
| The report contains a numbered list of findings and refers to the invidiual findings | There is a list, in which all findings are labeled with a number referring to the individual findings. |  |  |
| The report includes a management summary | The report includes a management summary |  |  |
| The management summary includes a start and end date of the study | It is clear when the investigation began and when it was completed. |  |  |
| The management summary includes an overview of the standards used during the study | The management summary contains an overview of the standards used during the study. |  |  |
| The management summary includes an overview of the client-supplied CIA scores for each scope object if delivered by client | The management summary includes a summary of client-supplied CIA scores for each scope object if delivered by client. |  |  |
| The management summary contains a root-cause analysis based on the information obtained from the survey and the findings | The management summary includes a root-cause analysis based on the information obtained from the survey and findings. |  |  |
| The management summary contains an overview of the vulnerabilities found by the rapporteur (number of findings per risk category) - based on the Common Vulnerability Scoring System - CVSS (latest version available) - using the following categories: Critical, High, Medium, Low and Informational (as defined by FIRST) | The management summary contains an overview of the vulnerabilities found by the rapporteur (number of findings per risk category) - based on the Common Vulnerability Scoring System - CVSS (latest version available) - using the following categories: Critical, High, Medium, Low and Informational (as defined by FIRST) |  |  |
| The report contains an overview of the scope objects, indicating for each scope object whether it has been tested and, if there are any deviations, what these deviations involve is described for each scope object. | The report contains an overview of the scope objects, indicating for each scope object whether it has been tested and, if there are any deviations, what these deviations involve is described for each scope object. |  |  |
| The scope described should be consistent with the Plan of Action | The scope described should be consistent with the Plan of Action. |  |  |
| The report contains a (sub)chapter describing testing by means of the assume breach principle and how validation of the application of the principle has been established by the contractor. | The report contains a (sub)chapter describing testing by means of the assume breach principle and how validation of the application of the principle has been established by the contractor. |  |  |
| The report includes a timeline indicating what actions were performed at what point in time (during the test period). | The report includes a timeline of the work. |  |  |
| The report contains a chapter findings | The report contains a chapter findings |  |  |
| The report should define a scope object for each recorded finding - this scope object should be directly traceable to the system, environment or application (or direct URL) within which the vulnerability resides. | The findings are directly traceable to the system, environment, application or URL in which the vulnerability was found. |  |  |
| In the report, a CVSS score for each recorded finding should be deﬁned along with a CVSS rating according to the standard (https://www.first.org/cvss/v4.0/specification-document - 6. Qualitative Severity Rating Scale) and if applicable, the calculation shall include weighting from the CIA scores provided by the client. | The findings are provided with a valid CVSS calculation, which can be recalculated via the standard (vector string). |  |  |
| The report shall provide a CVSS vector string for each recorded finding, according to the standard (https://www.first.org/cvss/v4.0/specification-document - 7 Vector String). If applicable, the calculation includes weighting from the CIA scores provided by the client. | The findings are provided with a valid CVSS vector string, which can be recalculated via the standard. |  |  |
| The report should include a description of the vulnerability for each included finding, referring to external sources (e.g., CVE numbers, public advisories) if available | The vulnerabilities are described with references to external sources describing the exact vulnerability. |  |  |
| The report should include a confirmation of the vulnerability for each recorded finding, explicitly including how the vulnerability can be reproduced, whether a public exploit was used, whether access to the system and/or available information was gained through misuse of the vulnerability. | For each finding, the rapporteur demonstrates how the vulnerability can be exploited in a way that the steps are also reproducible and what tools were used in the process. |  |  |
| The report should describe a possible impact for each included finding. The impact on surrounding environments/systems that are related to the scope object must also be taken into account. | For each finding, the rapporteur indicates the potential impact of the vulnerability on the system and/or within the network. |  |  |
| In the report a recommendation should be written for each recorded finding on how a vulnerability can be resolved. This should include (if applicable) a clickable (link) to an individual addition to the Common Weakness Enumeration (CWE) database associated with the vulnerability. | There is a recommendation in the report for each included finding. This should include how a vulnerability can be resolved. It should include (if applicable) a clickable (link) to an individual addition to the Common Weakness Enumeration (CWE) database associated with the vulnerability. |  |  |
| The report contains a chapter that includes attachments | The report contains a chapter that includes attachments |  |  |
| The report includes a chapter that includes a glossary. | The report includes a chapter that includes a glossary. |  |  |
| The report includes a section that includes tools used during the study. | The report includes a section that includes tools used during the study. |  |  |
| A description of the device should be included for each device used | A description of the device should be included for each device used |  |  |
| A specific version number corresponding to the version of the device deployed should be included for each device used | A specific version number corresponding to the version of the device deployed should be included for each device used |  |  |
| A public reference (URL) for each tool used should be included where the specific tool can be obtained (download/information website) | A public reference (URL) for each tool used should be included where the specific tool can be obtained (download/information website) |  |  |
| The report shall include a section listing ALL documents received by the contractor (including file name). | The report shall include a section listing ALL documents received by the contractor (including file name). |  |  |
| All documents received should include a description of the specific document | All documents received should include a description of the specific document |  |  |
| For all documents received, an SHA1 hash should be calculated and included | For all documents received, an SHA1 hash should be calculated and included |  |  |
| The report shall include a section listing ALL files received by the contractor (including file name). | The report shall include a section listing ALL files received by the contractor (including file name). |  |  |
| All files received should include a description of the specific file | All files received should include a description of the specific file |  |  |
| For all files received, an SHA1 hash should be calculated and included | For all files received, an SHA1 hash should be calculated and included |  |  |
| The report includes a section that lists the accounts provided by the client | The report includes a section that lists the accounts provided by the client |  |  |
| For each account included, the associated scope object should be described | For each account included, the associated scope object should be described |  |  |
| Each recorded account should include a description and role/a brief description of permissions | Each recorded account should include a description and role/a brief description of permissions |  |  |
| The report contains a section that includes the scan outputs from the scans performed. | The report contains a section that includes the scan outputs from the scans performed. |  |  |
| For each recorded scan result, the scope object should be defined | For each recorded scan result, the scope object should be defined |  |  |
| Each recorded scan result should include the raw scan output | Each recorded scan result should include the raw scan output |  |  |
| The report includes a section listing all information created/generated by the contractor - examples include state files (Burp), Nessus scans, nmap scans, testssl.sh scans and any other output belonging to the investigation | The report includes a section listing all information created/generated by the contractor - examples include state files (Burp), Nessus scans, nmap scans, testssl.sh scans and any other output belonging to the investigation |  |  |
| For all files belonging to the evidence, an SHA1 hash should be calculated and included | For all files belonging to the evidence, an SHA1 hash should be calculated and included |  |  |
| The report contains a section that includes checklists for the standards applicable to the study | The report contains a section that includes checklists for the standards applicable to the study |  |  |
| Depending on the checklists defined in the study, a checklist should be included for each standard - within this checklist, each test should be checked off, with three different statuses possible:  1. Tested.  2. Not tested.  3. Cannot be tested (functionality absent).   If there is a finding, it should be included with the invidiual check as an anomaly. If a check is not tested, it should be marked as red and an explanation should be given as to why a test was not performed. | Depending on the checklists defined in the study, a checklist should be included for each standard - within this checklist, each test should be checked off, with three different statuses possible:  1. Tested.  2. Not tested.  3. Cannot be tested (functionality absent).   If there is a finding, it should be included with the invidiual check as an anomaly. If a check is not tested, it should be marked as red and an explanation should be given as to why a test was not performed. |  |  |
| The report includes a section describing whether scope objects were technically inaccessible at the time of the investigation, which scope objects this concerned and how it was determined that these objects were technically inaccessible. | The report will include a section describing whether scope objects were technically inaccessible at the time of the investigation, which scope objects this concerned and how it was determined that these objects were technically inaccessible. |  |  |

Thus drawn up truthfully in [Place name] on [Date].

[Signature]

[Auditor's name]