Proces Verbaal van Validatie Penetratietest

Datum: [Invoeren Datum]  
Auditor: [Naam Auditor]  
Betreft: Validatie van de penetratietest uitgevoerd bij [Organisatie]  
Referentie: [Rapportnummer]

Ik doe proces verbaal van het onderzoeksrapport met kenmerk [kenmerk] van [datum] uitgegeven door [organisatienaam van de pentestende partij].

# Waar dit proces verbaal op ziet

Dit proces verbaal is opgesteld naar aanleiding een uitgevoerd informatiebeveiligingsonderzoek met auditwaarde, een gestructureerde pentest, waarvan een rapportage met onderliggend bewijsmateriaal beschikbaar is gesteld.

Dit proces-verbaal ziet op de volgende documenten, die bij de vaststelling voor mij beschikbaar waren:

|  |  |  |
| --- | --- | --- |
| **Bestandsnaam** | **Datum** | **SHA256** |
|  |  |  |

Het onderzoeksrapport van de penetratietest uitgevoerd beschrijft een onderzoek dat is uitgevoerd onder auspiciën van [Naam Pentester]. Het doel van dit document is om de rapportage en de onderliggende feiten te valideren volgens de opgestelde eisen zoals beschreven in het Miauw-schema versie [VERSIE HIER].

# Validatie van het onderzoek

Uit de rapportage blijkt dat de bevindingen als volgt zijn vastgesteld:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Informatief**  **0.0** | **Laag**  **0.1-.39** | **Middel**  **4.0-6.9** | **Hoog**  **7.0-8.9** | **Kritiek**  **9.0-10.0** |
| **Aantal bevindingen** |  |  |  |  |  |
| **Aantal open na hertest** |  |  |  |  |  |

Punten uit het schema

| **Eis** | **Validatie** | **Aangetroffen** | **Niet aangetroffen** |
| --- | --- | --- | --- |
| De onderzoeksrapportage wordt in digitale vorm verstrekt. | Er is een bestand dat de onderzoeksrapportage. Dit wordt digitaal aangeboden. |  |  |
| De rapportage vermeldt de naam van de rapporteur. | In de rapportage is de naam van een persoon genoemd. Deze persoon is in de rapportage als rapporteur aangemerkt. |  |  |
| De rapportage benoemt de geldige certificering(en), waarover de rapporteur beschikt. Geldige certificeringen zijn:  \* OffSec Certified Professional (OSCP) \* OffSec Experienced Pentester (OSEP)  \* OffSec Offensive Security Certified Expert (OSCE of OSCE³)  \* OffSec Web Expert (OSWE) \* Web application Penetration Tester eXtreme (eWPTX) | In de rapportage is benoemd over welke certificering deze persoon beschikt. Dit is een van de geaccepteerde certificeringen. |  |  |
| De rapportage levert bewijs van de certificering in de vorm van een link naar een online validatieplatform om de authenticiteit van de geclaimde certificering te valideren of een kopie van het diploma, waardoor andere validatie mogelijk is. Bij digitale documenten is deze link niet aanklikbaar, bij papieren versie hoeft de link aanklikbaar te zijn. | Iedere certificering heeft een platform om de geldigheid van de certificering van de rapporteur te valideren. Door te klikken en te kijken of er daadwerkelijk sprake is van het juiste platform wordt gevalideerd dat certificering daadwerkelijk bestaat en hiervan een screenshot te maken, kan validatie plaatsvinden. |  |  |
| Er wordt in de sectie 'Over dit document' melding gemaakt van het versienummer van het document. | In de passage 'Over dit document' wordt het versienummer van het document vastgesteld. |  |  |
| De rapportage wordt voorzien van een tekst, waaruit blijkt dat de rapportage: 1. accuraat en naar waarheid is opgesteld; 2. er een kwaliteitsreview op deze versie van het document heeft plaatsgevonden door andere een niet bij het onderzoek betrokken persoon.  Deze tekst voorzien van een handtekening van de rapporteur. Deze handtekening kan een fysiek gezette handtekening zijn of een digitale handtekening. | Controleer of er een verklaring is, waarbij de rapporteur verklaart: 1. dat de rapportage accuraat is opgesteld; 2. dat de rapportage naar waarheid is opgesteld; 3. dat er een review heeft plaatsgevonden door een andere, niet bij het onderzoek betrokken persoon.  Onder deze passage hoort een handtekening van de rapporteur te staan. Een handtekening kan een fysieke danwel een digitale handtekening zijn. |  |  |
| Het onderzoek wordt uitgevoerd volgens de zeven fasen van de Pentest Execution Standard (PTES) (https://www.pentest-standard.org/index.php/Main\_Page). De zeven fasen zijn: 1. Interacties vóór de betrokkenheid (Pre-engagement Interactions)  2. Informatie verzamelen (Intelligence Gathering) 3. Modellering van bedreigingen(Threat Modeling) 4. Kwetsbaarheidsanalyse (Vulnerability Analysis) 5. Exploitatie (Exploitation) 6. Post-exploitatie (Post Exploitation) 7. Rapportage (Reporting)  Deze indeling is in de rapportage terug te vinden. | Is de rapportage ingericht volgens de zeven fasen van de Pentest Execution Standard (PTES). Komen alle zeven onderdelen in de rapportage aan bod. |  |  |
| Er is een beschrijving met betrekking tot vertrouwelijkheid voor de opdrachtnemer (rapporteur, onderzoekers). Er wordt beschreven wat deze behelst. Indien er geen vertrouwelijkheid is afgesproken wordt dit ook beschreven. | In de rapportage wordt beschreven welke vertrouwelijkheid geldt voor de opdrachtnemer (met inbegrip van rapporteur en onderzoekers). Indien er geen vertrouwelijkheid is, is dit ook beschreven. |  |  |
| Er worden aan de opdrachtgever geen beperkingen opgelegd met betrekking tot verspreiding/distributie, publicatie of opslaan van de rapportage en de onderliggende stukken. Uitgezonderd hiervan zijn financiele gegevens met betrekking tot de uitvoering van het onderzoek, zoals uurtarieven, prijzen en facturen. | In de rapportage zijn geen passages te vinden die beperkingen opleggen aan de opdrachtgever voor het delen van de rapportage (bijvoorbeeld publicatie, verspreiding, distributie, opslag, etc.) |  |  |
| Het plan van aanpak heeft een beschrijving van het intake gesprek. | Er is een passage onder het hoofdstuk Interacties voor betrokkenheid (pre engagement) met de titel 'Intakegesprek' |  |  |
| Er wordt benoemd wanneer het gesprek heeft plaats gevonden. | In de passage wordt genoemd wanneer het gesprek is gehouden |  |  |
| Er wordt benoemd wie er aan het gesprek hebben deelgenomen met inbegrip van de respectievelijke functies. | De deelnemers aan het gesprek zijn benoemd, waarbij hun functies in het onderzoek zijn beschreven. |  |  |
| Er wordt aangegeven welke informatie voor aanvang van het onderzoek moet worden aangeleverd. | De passage bevat de nog aan de rapporteur aan te leveren informatie voor het onderzoek. |  |  |
| Er is een beschrijving van de scope van het onderzoek. Deze bevat de relevante selectie van onderdelen en objecten volgens sub 2.2.1 t/m 2.2.8. De scope komt overeen met de behoeftes uit het intakegesprek en past binnen de afgesproken tijdspanne. | Een controle vind plaats door de deelnemers van het gesprek, die verifieren of de scope overeenkomt met het gesprek. |  |  |
| In de scopebeschrijving staan de aanvalsperspectieven opgenomen op basis van het intakegesprek, verdeeld onder: Greybox en Whitebox. Het uitvoeren van een blackbox-test valt nadrukkelijk niet onder deze methodiek | In de scopebeschrijving is opgenomen welk aanvalsperspectief is afgesproken, wat gevalideerd wordt door de opdrachtgever en opdrachtnemer. Er wordt een test op basis van greybox of een whitebox (ook wel crystelbox genoemd) aangeboden. Een blackbox-onderzoek is nadrukkelijk niet toegestaan. |  |  |
| De objecten die naar voren zijn gekomen naar aanleiding van de intake, vormen de basis voor de scopeonderdelen en bijbehorende standaarden die van toepassing zijn in 2.2.3 tot en met 2.2.8. Alle standaarden die van toepassing kunnen zijn op het betrokken object, zijn in de scope opgenomen. Indien een sprake is van een scope-object met een specifiek versienummer dient deze vast te worden gelegd als onderdeel van het object. | De voorgestelde standaarden passen bij de gevraagde objecten. Hier kunnen meerdere standaarden van toepassing zijn (een webapplicatie staat ook op een netwerkcomponent, dus PTES en WSTG kan beide van toepassing zijn). Eventueel aan de hand van een seperate matrix? |  |  |
| Indien uit intakegesprek naar voren komt dat een netwerkonderzoek onderdeel is van de pentest, dienen de objecten (IP-adressen of IP-ranges) volgens de standaard PTES te worden getest. | Bij de aanwezigheid van IP-adressen of IP-ranges (intern of extern), heeft de aanbieder de PTES aangeboden over die onderdelen. |  |  |
| Indien uit het intakegesprek naar voren komt dat een of meerdere webapplicaties getest dient te worden, dienen de objecten (domeinnamen, urls) volgens de standaard OWASP Web Security Testing Guide (WSTG) te worden getest. | Bij de aanwezigheid van een webapplicatie object, heeft de aanbieder de WSTG aangeboden over desbetreffende onderdeel. |  |  |
| Indien uit het intakegesprek naar voren komt dat onderdeel van de pentest Internet of Things appara(a)t(en) is of zijn, dienen de objecten volgens de standaard OWASP IoT Security Testing Guide (ISTG) te worden getest. | Bij de aanwezigheid van een IoT object, heeft de aanbieder de ISTG aangeboden over desbetreffende onderdeel. |  |  |
| Indien uit het intakegesprek blijkt dat firmware van objecten dient te worden getest, dient dit te worden uitgevoerd volgens de standaard OWASP Firmware Security Testing Methodology (FSTM). | In het geval dat de firmware in een object (embedded), heeft de aanbieder de OWASP Firmware Security Test aangeboden. |  |  |
| Als uit het intakegesprek blijkt dat een API onderdeel behoort te zijn van de pentest, dient deze te worden uitgevoerd volgens de standaard WSTG hoofdstuk 12 API Testing | Bij de aanwezigheid van een API, heeft de aanbieder de OWASP WSTG aangeboden over desbetreffende onderdeel. |  |  |
| Als uit het intakegesprek blijkt dat als onderdeel van de pentest een mobiele applicatie dient te worden getest, vind de uitvoer plaats volgens de standaard OWASP Mobile Application Security Testing Guide (MASTG). | Bij de aanwezigheid van een mobiele applicatie, heeft de aanbieder de MASTG aangeboden over desbetreffende onderdeel. |  |  |
| Voorafgaand aan start van het onderzoek is de volledige lijst aan exacte onderzoeksobjecten, aanvalsperspectief en onderdelen bekend en vastgelegd. | Een lijst met exacte onderzoeksobjecten, aanvalsperspectief en scope onderdelen is opgenomen bij de scopebeschrijving. |  |  |
| Voorafgaand aan start van het onderzoek is geverifieerd dat de lijst aan objecten toebehoord aan de opdrachtgever of toestemming is gegeven door de rechthebbende derde partij voor het uitvoeren van de pentest. | 1. De objecten zijn op basis van open bronnen (whois, domeinregistratie, publisher) eigendom van opdrachtgever. 2. Rechthebbende derde partij heeft schriftelijk toestemming overlegd voor het uitvoeren van de pentest. |  |  |
| Voorafgaand aan start van het onderzoek is de wettelijke kader gevalideerd van de locaties waar de systemen fysiek zijn gelokaliseerd. De pentest wordt uitgevoerd volgens de wettelijke kaders aldaar van toepassing. | Er is een overzicht van de locaties van de te testen objecten. Indien een object in het buitenland is gelocaliseerd, is vastgesteld onder welke voorwaarden een pentest wel of niet uitgevoerd mag worden in desbetreffende land. |  |  |
| Voorafgaand aan de start van het onderzoek is de scope voorgelegd aan opdrachtgever en bevestigd. | Er is een document (fysiek, pdf, e-mail) waaruit blijkt dat de scope uit hoofd 2.2 in zijn geheel aan opdrachtgever voorgelegd. Deze heeft deze bevestigd in schrift of met een handtekening. |  |  |
| Voorafgaand aan de pentest is afgesproken en vastgelegd in welke taal de rapportage dient te worden geschreven. | Er zijn afspraken opgenomen over de taal van de rapportage. |  |  |
| Een plan van aanpak bevat het doel van de penetratietest en eventuele secundaire doelstelling(en) indien deze naar voren zijn gekomen in het intakegesprek. | Er is een doelstelling opgenomen, welke gevalideerd zijn door de deelnemers van het intakegesprek. |  |  |
| Er dient een vrijwaringsverklaring te worden getekend tussen opdrachtgever en opdrachtnemer voor het uitvoeren van de penetratietest, in deze vrijwaringsverklaring is specifiek verwezen naar de scope | Er is een getekende vrijwaringsverklaring aanwezig |  |  |
| Het "assume breach" principe bij pentesten (penetratietesten) is een benadering waarbij men ervan uitgaat dat een aanvaller al toegang heeft gekregen tot het netwerk. In plaats van te proberen binnen te komen (zoals niet MIAUW-pentests), focust men zich op het beperken van schade, het ontdekken van de aanwezigheid van de aanvaller, en het herstellen van systemen. Dit principe is bedoeld om organisaties beter voor te bereiden op het geval dat een beveiligingsincident plaatsvindt. | In de rapportage wordt beschreven dat er is gewerkt conform 'assume breach', waarbij ook een opsomming aanwezig is van maatregelen die zijn genomen om dat mogelijk te maken. |  |  |
| Bij een bevinding wordt een waarde op basis van het Common Vulnerability Scoring System 4.0 of hoger. | Er wordt bij iedere bevinding een CVSS-score versie 4.0 geleverd. |  |  |
| De CVSS-scores dienen te worden berekend op basis van de Base Metrics, aangevuld met de Supplemental Metrics, Environmental (Modified Base Metrics - Vulnerable System Impact Metrics, Subsequent System Impact Metrics) en Threat Metrics. | Door de CVSS-strings uit de rapportage via https://www.first.org/cvss/calculator/4.0 te raadplegen. In de CVSS-strings die zijn opgenomen in de rapportage, zijn ook waarden gedefinieerd onder supplemental, environmental en threat metrics. |  |  |
| De rapporteur dient alle scanresultaten, producties en andere resultaten versleuteld op te slaan en ter beschikking te hebben voor opdrachtgever. Alle resultaten worden gehasht, zodat de inhoud van de bestanden geverifieerd kunnen worden. Partijen maken afspraken over de bewaartermijnen. | Bewijslast is beschikbaar en kunnen worden opgevraagd. De hashwaarde van de opgevraagde bestanden komen overeen met de rapportage. |  |  |
| Alle scans worden uitgevoerd tegen scope-objecten waarvan vooraf is vastgesteld dat deze niet extra beschermd worden door een firewall met rate-limiting, een Web application Firewall (WAF) of andere maatregelen in de communicatielijn welke een verstorende werking kunnen hebben op de scanresultaten. | Er is bewijs beschikbaar dat de configuratie van eventuele tussen liggende objecten zijn aangepast of andere beschermende maatregelen buiten werking zijn gesteld. Daarnaast levert de onderzoeker bewijs aan dat is gecontroleerd dat met andere parameters (bijvoorbeeld IP-adres of intensiteit van scanning) is gevalideerd dat extra beschermende maatregelen voor het onderzoek niet functioneerden tijdens het onderzoek. |  |  |
| Alle gedetecteerde en geïdentificeerde toegangswegen waarmee verbonden kan worden met een onderzocht scope-object worden gedocumenteerd, ook indien deze niet direct tot misbruik geleid hebben | Er is een overzicht van de gedetecteerde en geïdentificeerde toegangswegen. |  |  |
| De rapportage bevat een genummerde inhoudsopgave van hoofdstukken en sub-hoofdstukken |  |  |  |
| De rapportage bevat een hoofdstuk methodiek waarin beschreven wordt langs welke lijnen het onderzoek uitgevoerd wordt - waarbij benoemd wordt dat het onderzoek uitgevoerd wordt volgens de zeven fasen van de Pentest Execution Standard (PTES) (https://www.pentest-standard.org/index.php/Main\_Page). De zeven fasen zijn: 1. Interacties vóór de betrokkenheid (Pre-engagement Interactions)  2. Informatie verzamelen (Intelligence Gathering) 3. Modellering van bedreigingen (Threat Modeling) 4. Kwetsbaarheidsanalyse (Vulnerability Analysis) 5. Exploitatie (Exploitation) 6. Post-exploitatie(Post Exploitation) 7. Rapportage(Reporting) | De indeling van de hoofdstukken in de rapportage komt overeen met de standaard. |  |  |
| De rapportage bevat een subhoofdstuk binnen het hoofdstuk methodiek - waarin beschreven wordt dat de bevindingen welke door onderzoekers gedaan worden, geclassificeerd worden middels het Common Vulnerability Scoring System (laatste beschikbare versie) en worden voorzien van een zogenoemde CVSS-vector string teneinde terug te kunnen leiden hoe de calculatie van de score tot stand gekomen is. | De rapportage bevat een uitleg over CVSS en hoe deze terug te herleiden zijn naar een CVSS-berekening. |  |  |
| De rapportage bevat een hoofdstuk over het document (documentbeheer) - in dit hoofdstuk wordt tenminste gedefinieerd: Opdrachtgever, projectnummer/naam, start- en einddatum van project, rapporteurs, reviewers, document classificatie, versie-nummer van het document en de handtekening van de verantwoordelijke rapporteur | De rapportage bevat de componenten over documentbeheer. |  |  |
| De rapportage bevat een hoofdstuk over versie-beheer - in dit hoofdstuk wordt tenminste gedefinieerd (per versie): Versie, Datum, Auteur en Versie-omschrijving | De rapportage bevat de componenten over versiebeheer. |  |  |
| De rapportage bevat een hoofdstuk inzake de distributielijst - in dit hoofdstuk wordt tenminste gedefinieerd: Versie, datum, naam, organisatie en verspreidingsmethode | De rapportage bevat een overzicht over de distributie in de verschillende versies. |  |  |
| De rapportage bevat een hoofdstuk waarin de aanleiding van het onderzoek beschreven is, hierbij wordt minimaal beschreven: of er sprake is van een timeboxed test en indien dit het geval is, wat de maximering van de uren betreft, welke onderdelen niet (volledig) konden worden getest en waarom niet, een algemene beschrijving van de te testen omgevingen van opdrachtgever | De inleiding bevat informatie over de minimale randvoorwaarden waaronder de penetratietest wordt uitgevoerd. Daarnaast is ook opgenomen in de rapportage of er bepaalde onderdelen niet getest konden worden en wat daarvan de oorzaak is. |  |  |
| Een doelstelling is opgenomen die overeenkomt met hetgeen dat tijdens de intake naar voren is gekomen. | De doelstelling komt overeen met hetgeen dat is afgesproken met opdrachtgever. |  |  |
| De rapportage bevat een genummerde lijst van bevindingen en verwijst naar de invidiuele bevindingen | Er is een lijst, waarin alle bevindingen worden voorzien van een nummer dat verwijst naar de individuele bevindngen. |  |  |
| De rapportage bevat een managementsamenvatting | De rapportage bevat een managementsamenvatting |  |  |
| De managementsamenvatting bevat een start- en einddatum van het onderzoek | Er is duidelijk wanneer het onderzoek is begonnen en wanneer het is afgerond. |  |  |
| De managementsamenvatting bevat een overzicht van de gebruikte standaarden tijdens het onderzoek | De managementsamenvatting bevat een overzicht van de gebruikte standaarden tijdens het onderzoek. |  |  |
| De managementsamenvatting bevat een overzicht van de door opdrachtgever aangeleverde CIA-scores per scope-object indien deze door opdrachtgever zijn opgeleverd | De managementsamenvatting bevat een overzicht van de door opdrachtgever aangeleverde CIA-scores per scope-object indien deze door opdrachtgever zijn opgeleverd. |  |  |
| De managementsamenvatting bevat een root-cause analyse op basis van de informatie verkregen uit het onderzoek en de bevindingen | De managementsamenvatting bevat een root-cause analyse op basis van de informatie verkregen uit het onderzoek en de bevindingen. |  |  |
| De managementsamenvatting bevat een overzicht van de door rapporteur aangetroffen kwetsbaarheden (aantal bevindingen per risico-categorie) - op basis van het Common Vulnerability Scoring System - CVSS (nieuwste beschikbare versie) - waarbij de volgende categorieen worden gehanteerd: Kritiek, Hoog, Gemiddeld, Laag en Informatief (zoals gedefineerd door FIRST) | De managementsamenvatting bevat een overzicht van de door rapporteur aangetroffen kwetsbaarheden (aantal bevindingen per risico-categorie) - op basis van het Common Vulnerability Scoring System - CVSS (nieuwste beschikbare versie) - waarbij de volgende categorieen worden gehanteerd: Kritiek, Hoog, Gemiddeld, Laag en Informatief (zoals gedefineerd door FIRST) |  |  |
| De rapportage bevat een overzicht van de scope-objecten, waarbij per scope-object aangegeven wordt of deze getest is en indien er afwijkingen zijn wordt er per scope-object beschreven wat deze afwijkingen behelsen. | De rapportage bevat een overzicht van de scope-objecten, waarbij per scope-object aangegeven wordt of deze getest is en indien er afwijkingen zijn wordt er per scope-object beschreven wat deze afwijkingen behelsen. |  |  |
| De beschreven scope dient overeen te komen met het Plan van Aanpak | De beschreven scope dient overeen te komen met het Plan van Aanpak. |  |  |
| De rapportage bevat een (sub)hoofdstuk waarin beschreven is dat er middels het assume breach principe getest wordt en hoe de validatie van het toepassen van het principe vastgesteld is door opdrachtnemer. | De rapportage bevat een (sub)hoofdstuk waarin beschreven is dat er middels het assume breach principe getest wordt en hoe de validatie van het toepassen van het principe vastgesteld is door opdrachtnemer. |  |  |
| De rapportage bevat een tijdlijn waarin aangegeven wordt welke acties er op welk moment in de tijd (tijdens de testperiode) uitgevoerd zijn. | De rapportage bevat een tijdslijn van de werkzaamheden. |  |  |
| De rapportage bevat een hoofdstuk bevindingen | De rapportage bevat een hoofdstuk bevindingen |  |  |
| In de rapportage dient er per opgenomen bevinding een scope-object te worden gedefineerd - dit scope-object dient direct herleidbaar te zijn naar het systeem, de omgeving of applicatie (of directe URL) waarbinnen de kwetsbaarheid zich bevindt. | De bevindingen zijn direct herleidbaar naar het systeem, de omgeving, applicatie of URL waarin de kwetsbaarheid is aangetroffen. |  |  |
| In de rapportage dient er per opgenomen bevinding een CVSS-score te worden gedefineerd, tezamen met een CVSS-classificatie volgens de standaard (https://www.first.org/cvss/v4.0/specification-document - 6. Qualitative Severity Rating Scale) en indien van toepassing wordt in de berekening de weging meegenomen vanuit de door opdrachtgever verstrekte CIA-scores. | De bevindingen zijn voorzien van een geldige CVSS berekening, die via de standaard (vector string) nagerekend kunnen worden. |  |  |
| In de rapportage dient er per opgenomen bevinding een CVSS-vector string te worden verstrekt, volgens de standaard (https://www.first.org/cvss/v4.0/specification-document - 7 Vector String). Indien van toepassing wordt in de berekening de weging meegenomen vanuit de door opdrachtgever verstrekte CIA-scores. | De bevindingen zijn voorzien van een geldige CVSS vector string, die via de standaard nagerekend kunnen worden. |  |  |
| In de rapportage dient er per opgenomen bevinding een beschrijving van de kwetsbaarheid te worden opgenomen, waarbij indien beschikbaar gerefereerd wordt naar externe bronnen (zoals bijvoorbeeld CVE-nummers, public advisories) | De kwetsbaarheden zijn beschreven met verwijzingen naar externe bronnen, waarin de exacte kwetsbaarheid is beschreven. |  |  |
| In de rapportage dient er per opgenomen bevinding een bevestiging van de kwetsbaarheid te worden opgenomen, waarbij expliciet opgenomen staat hoe de kwetsbaarheid kan worden gereproduceerd, of er gebruik gemaakt is van een publieke exploit, of er door middel van misbruik van de kwetsbaarheid toegang is verkregen tot het systeem en/of beschikbare informatie. | De rapporteur toont per bevinding aan hoe de kwetsbaarheid misbruikt kan worden op een wijze dat de stappen ook reproduceerbaar zijn en welke tools daarbij zijn gebruikt. |  |  |
| In de rapportage dient er per opgenomen bevinding een mogelijke impact te worden beschreven. Daarbij dient ook rekening te worden gehouden met de impact op omliggende omgevingen/systemen welke een relatie hebben tot het scope-object | De rapporteur geeft per bevinding aan wat de mogelijke impact is van de kwetsbaarheid op het systeem en/of binnen het netwerk. |  |  |
| In de rapportage dient er per opgenomen bevinding een aanbeveling te worden geschreven inzake hoe een kwetsbaarheid kan worden opgelost. Daarbij dient er (indien deze van toepassing is) een klikbare (link) te worden opgenomen naar een individuele toevoeging in de Common Weakness Enumaration (CWE) database welke bij de kwetsbaarheid hoort. | Er is in de rapportage per opgenomen bevinding een aanbeveling opgenomen. Hierin hoort te staan hoe een kwetsbaarheid kan worden opgelost. Daarbij dient er (indien deze van toepassing is) een klikbare (link) te worden opgenomen naar een individuele toevoeging in de Common Weakness Enumaration (CWE) database welke bij de kwetsbaarheid hoort. |  |  |
| De rapportage bevat een hoofdstuk waarin bijlages opgenomen worden | De rapportage bevat een hoofdstuk waarin bijlages opgenomen worden |  |  |
| De rapportage bevat een hoofdstuk waarin een verklarende woordenlijst opgenomen wordt. | De rapportage bevat een hoofdstuk waarin een verklarende woordenlijst opgenomen wordt. |  |  |
| De rapportage bevat een hoofdstuk waarin gebruikte hulpmiddelen tijdens het onderzoek opgenomen wordt. | De rapportage bevat een hoofdstuk waarin gebruikte hulpmiddelen tijdens het onderzoek opgenomen wordt. |  |  |
| Er dient per gebruikt hulpmiddel een beschrijving van het hulpmiddel te worden opgenomen | Er dient per gebruikt hulpmiddel een beschrijving van het hulpmiddel te worden opgenomen |  |  |
| Er dient per gebruikt hulpmiddel een specifiek versienummer te worden opgenomen welke overeenkomt met de versie van het ingezette hulpmiddel | Er dient per gebruikt hulpmiddel een specifiek versienummer te worden opgenomen welke overeenkomt met de versie van het ingezette hulpmiddel |  |  |
| Er dient per gebruikt hulpmiddel een publieke referentie (URL) te worden opgenomen waar het specifieke hulpmiddel kan worden verkregen (download/informatie website) | Er dient per gebruikt hulpmiddel een publieke referentie (URL) te worden opgenomen waar het specifieke hulpmiddel kan worden verkregen (download/informatie website) |  |  |
| De rapportage bevat een hoofdstuk waarin een lijst met ALLE door opdrachtnemer ontvangen documenten (inclusief bestandsnaam) worden opgenomen. | De rapportage bevat een hoofdstuk waarin een lijst met ALLE door opdrachtnemer ontvangen documenten (inclusief bestandsnaam) worden opgenomen. |  |  |
| Bij alle ontvangen documenten dient een beschrijving te worden opgenomen van het specifieke document | Bij alle ontvangen documenten dient een beschrijving te worden opgenomen van het specifieke document |  |  |
| Bij alle ontvangen documenten dient een SHA1-hash te worden berekend en opgenomen te worden | Bij alle ontvangen documenten dient een SHA1-hash te worden berekend en opgenomen te worden |  |  |
| De rapportage bevat een hoofdstuk waarin een lijst met ALLE door opdrachtnemer ontvangen bestanden (inclusief bestandsnaam) worden opgenomen. | De rapportage bevat een hoofdstuk waarin een lijst met ALLE door opdrachtnemer ontvangen bestanden (inclusief bestandsnaam) worden opgenomen. |  |  |
| Bij alle ontvangen bestanden dient een beschrijving te worden opgenomen van het specifieke bestand | Bij alle ontvangen bestanden dient een beschrijving te worden opgenomen van het specifieke bestand |  |  |
| Bij alle ontvangen bestanden dient een SHA1-hash te worden berekend en opgenomen te worden | Bij alle ontvangen bestanden dient een SHA1-hash te worden berekend en opgenomen te worden |  |  |
| De rapportage bevat een hoofdstuk waarin een lijst met de door opdrachtgever verstrekte accounts zijn opgenomen | De rapportage bevat een hoofdstuk waarin een lijst met de door opdrachtgever verstrekte accounts zijn opgenomen |  |  |
| Bij elk opgenomen account dient het bijbehorende scope-object te worden beschreven | Bij elk opgenomen account dient het bijbehorende scope-object te worden beschreven |  |  |
| Bij elk opgenomen account dient een beschrijving en rol/een korte beschrijving van permissies te worden opgenomen | Bij elk opgenomen account dient een beschrijving en rol/een korte beschrijving van permissies te worden opgenomen |  |  |
| De rapportage bevat een hoofdstuk waarin de scan-output van de uitgevoerde scans opgenomen is. | De rapportage bevat een hoofdstuk waarin de scan-output van de uitgevoerde scans opgenomen is. |  |  |
| Bij elk opgenomen scan-resultaat dient het scope-object te worden gedefineerd | Bij elk opgenomen scan-resultaat dient het scope-object te worden gedefineerd |  |  |
| Bij elk opgenomen scan-resultaat dient de ruwe scan-output te worden opgenomen | Bij elk opgenomen scan-resultaat dient de ruwe scan-output te worden opgenomen |  |  |
| De rapportage bevat een hoofdstuk waarin een lijst met alle door opdrachtnemer gecreerde/gegenereerde informatie wordt opgenomen - voorbeelden hiervan zijn state-files (Burp), Nessus scans, nmap scans, testssl.sh scans en elke andere output behorende tot het onderzoek | De rapportage bevat een hoofdstuk waarin een lijst met alle door opdrachtnemer gecreerde/gegenereerde informatie wordt opgenomen - voorbeelden hiervan zijn state-files (Burp), Nessus scans, nmap scans, testssl.sh scans en elke andere output behorende tot het onderzoek |  |  |
| Bij alle bestanden die behoren tot het bewijsmateriaal dient een SHA1-hash te worden berekend en opgenomen te worden | Bij alle bestanden die behoren tot het bewijsmateriaal dient een SHA1-hash te worden berekend en opgenomen te worden |  |  |
| De rapportage bevat een hoofdstuk waarin de checklists opgenomen zijn voor de standaarden die van toepassing zijn op het onderzoek | De rapportage bevat een hoofdstuk waarin de checklists opgenomen zijn voor de standaarden die van toepassing zijn op het onderzoek |  |  |
| Afhankelijk van de in het onderzoek gedefineerde checklists dient er per standaard een checklist te worden opgenomen - binnen deze checklist dient elke test te worden afgevinkt, waarbij er drie verschillende statussen mogelijk zijn:  1. Getest. 2. Niet getest.  3. Valt niet te testen (functionaliteit afwezig).  Indien er een bevinding is, dient deze bij de invidiuele check te worden opgenomen als afwijking. Indien een check niet getest is, dient dit als rood te worden gemarkeerd en dient toelichting te worden gegeven waarom een test niet uitgevoerd is. | Afhankelijk van de in het onderzoek gedefinieerde checklists dient er per standaard een checklist te worden opgenomen - binnen deze checklist dient elke test te worden afgevinkt, waarbij er drie verschillende statussen mogelijk zijn:  1. Getest. 2. Niet getest.  3. Valt niet te testen (functionaliteit afwezig).  Indien er een bevinding is, dient deze bij de invidiuele check te worden opgenomen als afwijking. Indien een check niet getest is, dient dit als rood te worden gemarkeerd en dient toelichting te worden gegeven waarom een test niet uitgevoerd is. |  |  |
| In de rapportage wordt een hoofdstuk opgenomen waarin beschreven word of er scope-objecten ten tijden van het onderzoek technisch niet bereikaar waren, daarbij wordt beschreven welke scope-objecten dit betroffen en hoe is vastgesteld dat deze objecten technisch niet benaderbaar/bereikbaar waren. | In de rapportage wordt een hoofdstuk opgenomen waarin beschreven word of er scope-objecten ten tijden van het onderzoek technisch niet bereikbaar waren, daarbij wordt beschreven welke scope-objecten dit betroffen en hoe is vastgesteld dat deze objecten technisch niet benaderbaar/bereikbaar waren. |  |  |

Aldus naar waarheid opgemaakt te [Plaatsnaam] op [Datum]

[Handtekening]

[Naam Auditor]