



OFFERTE PENTEST

Infrastructuur en locatiebezoek

Organisatie: Humankind
T.a.v. de heer Kranendonk
Postbus 591, 6400 AN Heerlen

Aangeboden via: SharePoint NFIR

Datum: 23 oktober 2024

Betreft: Offerte pentest infrastructuur en locatiebezoek



Dit document mag niet worden verspreid of gekopieerd zonder toestemming van NFIR B.V.



Inhoudsopgave

1	Opdrachtoomschrijving.....	2
2	Scope van de penetratietest.....	2
2.1	Black Box – Externe Infrastructuur (Timeboxed)	3
2.2	Grey Box – Interne Infrastructuur (Timeboxed).....	4
2.3	Grey Box – Locatiebezoek (Timeboxed).....	4
3	Tijdsverloop van de penetratietest.....	5
4	Rapportage en toelichting	5
5	NFIR team	6
6	Het CCV-keurmerk pentesten & Cyberveilig Nederland	6
7	Standaarden en methodieken.....	7
8	Algemene richtlijnen Cloud omgevingen.....	7
9	Start vereisten.....	8
9.1	Algemene vereiste documenten en informatie	8
9.2	Opdracht specifieke vereisten	8
9.3	Whitelisten van zes IP-adressen van NFIR	9
9.4	Pentestbox.....	9
10	Bewaartermijn gegevens.....	9
11	Tarieven en projectkosten.....	10
12	Bijlage 1: Aanvalsscenario's en zeven fasen pentest	11
12.1	Aanvalsperspectieven	11
12.2	De zeven fasen van een pentest	12



Geachte heer Kranendonk,

Op dinsdag 8 oktober 2024 spraken wij tijdens de aangename kennismaking en intake met u en John Keulen over de penetratietest die Humankind wil laten uitvoeren door NFIR. In deze offerte treft u de opdrachtschrijving, een uitwerking van de scope per te testen onderdeel, onze aanpak, de gebruikte standaarden en de vereisten voor de start van dit project. Tot slot treft u een urenrekening van de onderdelen van deze pentest met onze tarieven.

1 Opdrachtschrijving

De opdracht betreft het uitvoeren van een penetratietest binnen de infrastructuur volgens de besproken scope onderdelen tijdens de intake, met als doel het identificeren van kwetsbaarheden.

Humankind gaat de pentest rapportage gebruiken om gevonden kwetsbaarheden op te lossen. Prioritering gebeurt op basis van de CVSS-scores. De kwetsbaarheden en bijbehorende CVSS-scores worden opgenomen in de rapportage.

2 Scope van de penetratietest

De besproken scope omvat de externe infrastructuur, interne infrastructuur en locatiebezoek. Door Humankind is documentatie aangeleverd over de scope van deze pentest die tijdens de intake besproken is. Het volgende bestand is aangeleverd en bestudeerd:

- Aanvullende info tbv pentest NFIR Humankind

De verstrekte informatie in dit bestand en de verkregen informatie tijdens het intakegesprek zijn gebruikt voor de ureninschatting van deze opdracht.



2.1 Black Box – Externe Infrastructuur (Timeboxed)

Zonder enige voorkennis (met uitzondering van de IP-adressen of hostnaam), zal onderzocht worden of op de publieke IP-adressen kwetsbaarheden geïdentificeerd kunnen worden, waarbij geprobeerd zal worden om binnen te dringen in de omgeving. Gedurende het Black Box aanvalsperspectief van de infrastructuur zal geen gebruik worden gemaakt van een gebruikersaccount.

In de onderstaande tabellen wordt de scope voor dit onderdeel beschreven:

IP-adres	Omschrijving
20.23.64.252	Publieke IP-adressen Humankind
20.234.209.85	
20.31.241.172	
20.50.53.5	
20.56.239.82	
20.56.239.87	
20.71.74.225	
20.71.76.115	
20.73.35.158	
20.73.78.23	
51.124.17.132	
51.136.125.238	

Met behulp van verschillende technieken zal via een Open Source Intelligence (OSINT) onderzoek geprobeerd worden om zoveel mogelijk informatie te verkrijgen over de organisatie. Hierbij zal tevens worden achterhaald welke relevante informatie mogelijk gelekt is, waaronder potentiële logingegevens van medewerkers. De volgende domeinnamen zijn onderdeel van de scope:

Domeinnaam	Omschrijving
groeionmicrosoft.com	Domeinnamen Humankind
het-kinderatelier.nl	
humankind.nl	
kindcentra.info	
kinderdomein.nl	
kinderopvangenschede.nl	
kinderopvanghumanitas.nl	
kovdecirkel.nl	
skekinderopvang.nl	



2.2 Grey Box – Interne Infrastructuur (Timeboxed)

Met dit scenario wordt nagebootst wat de gevolgen kunnen zijn in het geval een kwaadwillende hacker toegang verkrijgt tot de interne infrastructuur (bijvoorbeeld door middel van een geslaagde phishing of social engineering aanval). Tijdens de penetratietest wordt getracht om de privileges te verhogen naar beheerdersrechten en wordt onderzocht of het mogelijk is om de kroonjuwelen van de organisatie te stelen of om ransomware uit te rollen. Er zal een pentestbox ([meer informatie over de pentestbox](#)) in uw netwerk worden geplaatst, welke door de pentesters gebruikt wordt gedurende de uitvoering. Daarnaast zullen één of meerdere gebruikersaccounts worden gebruikt. In de onderstaande tabellen wordt de scope voor dit onderdeel beschreven:

IP-range	Omschrijving/ Naam
10.4.0.0/16	Vnet-Production
10.0.0.0/16	VNet_Datacenter
10.3.0.0/16	VNet_DMZ
192.168.1.0/24	VNet_DMZ1
192.168.1.0/24	VNet_DMZ2
192.168.115.0/24	RG_Vnet_DMZ3
10.99.0.0/16	RG_VnetIsolated

Een belangrijk onderdeel van de pentest is het onderzoeken van de Microsoft Active Directory / en AzureAD configuratie op mogelijke kwetsbaarheden.

Scope	Beschrijving
Microsoft Active Directory	Domeinnaam: humanitas
Microsoft AzureAD	Tenant: 940dceee-ca16-4d7a-92b8-5c0a36ab4869

2.3 Grey Box – Locatiebezoek (Timeboxed)

Tijdens een penetratietest op locatie wordt de Wi-Fi onderzocht en kunnen ook de netwerktoegang, printers en andere randapparatuur onderdeel zijn van het onderzoek. Voorafgaand aan of tijdens het bezoek zal besproken worden welke systemen verder getest mogen worden mits voldoende tijd beschikbaar binnen dit timeboxed onderdeel. Voor de uitvoering van dit onderdeel zal 1 ethisch hacker maximaal 1 dag aanwezig zijn op locatie. Daarnaast zullen één of meerdere gebruikersaccounts worden gebruikt.

De volgende locatie is in scope:

Locatie Type	Adres
Type 3	Nader te ontvangen
Type 4	Nader te ontvangen

Voor de Wi-Fi zijn de volgende netwerken in scope:

SSID
HumanKindWS
KO091519
KovHumanitas
KovHumanitasGast
KovHumanitasIoT

Informatie over de uitvoering van de penetratietest treft u in Bijlage 1: dienstenbeschrijving pentest.



3 Tijdsverloop van de penetratietest

Hieronder treft u het tijdsverloop en de volgorde van de verschillende onderdelen van deze penetratietest. Voordat de pentest van start zal gaan, wordt altijd een startmail verstuurd door de Technical Lead. Pas na het versturen van de e-mail, zal de pentest daadwerkelijk van start gaan. De contactgegevens van de Technical Lead zullen worden gedeeld en zullen ten alle tijden beschikbaar zijn voor calamiteiten en/of vragen tijdens de opdracht.

Mocht er tijdens de opdracht kritieke bevindingen worden gevonden, zal de Technical Lead direct telefonisch contact opnemen om samen met de opdrachtgever de gevonden kwetsbaarheid op te lossen. Gelijk na het telefonisch contact zal de bevinding direct in het deelportaai worden gezet en met de opdrachtgever worden gedeeld. De besproken bevinding zal in het eindrapport ook worden beschreven. Zodra de technische uitvoering is afgerond, zal de Technical Lead hierover een e-mail sturen.

Hackers hebben bij een aanval in principe oneindig de tijd om ongeautoriseerde toegang te verkrijgen tot de IT-infrastructuur van uw organisatie. Onze ethisch hackers hebben niet oneindig de tijd, want dat zou de uitvoering van het black box aanvalsscenario te kostbaar maken. Om die reden wordt de uitvoering van een black box altijd timeboxed uitgevoerd. Wij calculeren aan de hand van de grootte van de scope een redelijke hoeveelheid tijd waarbinnen de aanval uitgevoerd wordt en de technische weerbaarheid getoetst wordt.

Vanwege het ontbreken van informatie zullen alle onderdelen Timeboxed uitgevoerd worden, waardoor de uren voor de uitvoering van dit onderdeel gemaximeerd zijn op een vastgestelde hoeveelheid uren.

4 Rapportage en toelichting

De bevindingen tijdens deze opdracht worden gedocumenteerd in een heldere en volledige rapportage. Indien deze pentest bestaat uit verschillende onderdelen, zullen de bevindingen per onderdeel worden gerapporteerd. De rapportage wordt altijd geschreven door een gecertificeerd ethisch hacker. De rapportage zal op uw verzoek worden uitgebracht in de Nederlandse taal. De rapportage zal worden opgeleverd op een voor uw organisatie gecreëerde beveiligde SharePoint deelopgeving. Wij verzoeken u in de tabel onder 'Algemene vereiste documenten en informatie voor de start' aan te geven wie toegang mag krijgen tot dit deelportaai t.b.v. de rapportage. De opleverdatum van de rapportage zal tijdig aan u worden doorgegeven.

Een standaard onderdeel van onze pentest dienstverlening is het toelichten van de bevindingen naar aanleiding van de opgeleverde pentest rapportage. Deze toelichting wordt enorm gewaardeerd door onze opdrachtgevers, omdat de accountmanager en de technical lead samen alle betrokken personen informeren over de belangrijkste gevonden kwetsbaarheden. Er is ruimte om vragen te stellen en te discussiëren over de mogelijke oplossingsrichting. Door deze aanpak vergroot de opdrachtgever de kans dat iedereen betrokken is en blijft in de fase waarin de kwetsbaarheden moeten worden opgelost.



5 NFIR team

De pentest zal worden uitgevoerd door eigen medewerkers van NFIR. NFIR is in het bezit van een POB vergunning van het Ministerie van Veiligheid en Justitie (nummer 1672). Alle NFIR-medewerkers hebben Korpschef toestemming en worden jaarlijks onderworpen aan een integriteitsonderzoek. Met deze status van betrouwbaarheid onderscheidt NFIR zich van vele andere cyber securityspecialisten. Het pentest team bestaat uit zeer gecertificeerde, creatieve en ervaren ethische (white hat) hackers, gedreven projectcoördinatoren en betrokken account manager.

Onze vakkundige en professionele ethische hackers hebben ruime ervaring, creativiteit en actuele vakkennis. Ze zijn in het bezit van diverse certificeringen, waaronder [OSCP](#), [OSWP](#), [OSEP](#), [OSWE](#), [CPTS](#), [CBBH](#), en [eWPT](#).



6 Het CCV-keurmerk pentesten & Cyberveilig Nederland

Brancheorganisatie Cyberveilig Nederland zet zich in voor het vergroten van kwaliteit en transparantie in de cybersecuritysector. Het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) heeft in samenwerking met Cyberveilig Nederland een certificeringsschema opgesteld om de kwaliteit te waarborgen voor afnemers van penetratietesten. Het doel van het certificeren van de pentest is het verminderen van faal- en risicokosten bij afnemers die kunnen optreden als de vermeende kwaliteit van de pentest niet aanwezig is. Door certificatie kunnen afnemers een gerechtvaardigd vertrouwen hebben dat de geleverde pentest, voorzien van het certificatiemerk, voldoet aan de vooraf gestelde eisen. Met dit keurmerk bent u ervan verzekerd dat de uitvoering van uw pentest voldoet aan de belangrijkste kwaliteitseisen. NFIR is in december 2021 door KIWA Nederland gecertificeerd. Jaarlijks vindt er een heraudit plaats.

Meer informatie over het CCV-keurmerk treft u [hier](#). Meer informatie over Cyberveilig Nederland treft u [hier](#).





7 Standaarden en methodieken

- [Penetration Testing Execution Standard \(PTES\)](#): Standaard ten behoeve van infrastructuur pentesten.
- [Common Vulnerability Scoring System \(CVSS\)](#): Wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.
 - Het scoresysteem werkt op basis van acht verschillende basisparameters, die samen de risicoscore bepalen.
 - Deze parameters vormen zogenaamde vector strings en kunnen gebruikt worden om te herleiden waarop de scores gebaseerd zijn. Dit herleiden kan eenvoudig gereproduceerd worden door op de vector string te klikken.
 - Informatieve bevindingen zijn afwijkingen van de best practices op het gebied van beveiliging die, hoewel ze een minimaal onmiddellijk risico veroorzaken, in de toekomst een grotere bedreiging kunnen vormen.



8 Algemene richtlijnen Cloud omgevingen

Bij het testen van de Microsoft Cloud omgevingen van de klant worden de richtlijnen van Microsoft gevolgd. Deze richtlijnen beschrijven welke omgevingen getest mogen worden en welke acties zijn toegestaan.

Zie voor meer informatie de volgende website: [Microsoft Cloud Penetration Testing Rules of Engagement](#)



9 Start vereisten

9.1 Algemene vereiste documenten en informatie

De volgende documenten en informatie zijn vereist voor het uitvoeren van deze opdracht:

- Een getekende versie van deze pentest offerte
- De getekende vrijwaringsverklaring. Deze wordt als bijlage bij deze offerte meegestuurd
- Eén of meerdere contactpersonen van uw organisatie die beschikbaar is/zijn tijdens de pentest zodat de technical lead eventuele kritieke bevindingen direct kan doorgeven:

Prio	Naam	E-mailadres	Mobiel nummer

- Gegevens van de personen die na afloop van de pentest de rapportage dienen te ontvangen:

Naam	E-mailadres

9.2 Opdracht specifieke vereisten

- Ten behoeve van de Black Box – Externe Infrastructuur (Timeboxed)
- Ten behoeve van de Grey Box – Interne Infrastructuur
 - Twee gebruikersaccounts met de standaard gebruiksrechten binnen de Microsoft ActiveDirectory/AzureAD omgeving.
 - Een netwerkaansluiting voor de NFIR pentestbox, waarbij alle objecten binnen de scope te benaderen zijn.
 - Graag doorgeven of de pentestbox gebruik kan maken van een dynamisch of statisch IP-adres, indien benodigd voor DHCP reservering kan een MAC adres aangeleverd worden.
 - Indien statisch zijn de volgende gegevens benodigd: IP-adres, subnetmasker, default-gateway en DNS servers.
 - Een overzicht van de actieve systemen binnen de /16 subnets.
- Ten behoeve van de Grey Box – Locatiebezoek (Timeboxed)
 - De adresgegevens van de Type 3 en 4 locaties
 - Voor beide locaties een rustige werkplek waarbij toegang is tot het netwerk en Wi-Fi-netwerken.
- Voor de start van deze pentest dient u in de firewall de onderstaande IP-adressen van NFIR te whitelisten, zodat de firewall NFIR niet blokkeert en de pentest onnodig stil komt te liggen.

IPv4	IPv6
136.144.183.82	2a01:7c8:aac7:318::1
95.170.71.93	2a01:7c8:bb06:10e:5054:ff:fe6d:b24e
93.119.0.143	2a01:7c8:bb0a:7f:5054:ff:fe3b:73dd



9.3 Whitelisten van zes IP-adressen van NFIR

Veel organisaties vragen zich af waarom NFIR verzoekt om zes IP-adressen te whitelisten in de firewall als vereiste voor de start van de pentest. Ook wordt soms gesuggereerd dat hierdoor het testen van de technische weerbaarheid niet meer representatief zou zijn. De reden dat wij dit vragen is om te voorkomen dat onze IP-adressen geblokkeerd worden door de Intrusion Prevention / Detection (IPS/IDS) modules van uw firewall zodra wij de IT-infrastructuur gaan onderzoeken. Dit zou zeer waarschijnlijk gebeuren doordat de (scanning) tools die wij gebruiken verzoeken afvuren op uw firewall en als malafide verkeer worden herkend. Als u onze IP-adressen niet zou whitelisten, dan zou de pentest stil komen te liggen doordat uw firewall onze externe IP-adressen blokkeert. Deze blokkade moet dan steeds vrijgegeven worden door een beheerder en deze kostbare tijd van de pentest gaat dan verloren. Indien uw firewall geen modules heeft die blokkades uitvoeren op basis van het ontvangen netwerkverkeer, dan hoeft er geen actie te worden ondernomen. Het is uiteraard niet de bedoeling om extra poorten open te zetten voor onze IP-adressen. Dit zou wél een vertekend beeld opleveren van de technische weerbaarheid van uw extern beschikbare infrastructuur.

9.4 Pentestbox

Naast het testen van de externe infrastructuur, zullen onze ethisch hackers tijdens het interne gedeelte van de test gebruiken maken van een zogenaamde pentestbox die fysiek in uw netwerk geplaatst zal worden. Voorheen kwamen de ethisch hackers van NFIR hiervoor fysiek naar uw kantoorlocatie, tegenwoordig wordt dit op afstand gedaan met een pentestbox. Met de pentestbox simuleren onze ethisch hackers dat zij de test uitvoeren alsof zij op uw locatie zijn om zo het netwerk van binnenuit te kunnen testen. De pentestbox dient de mogelijkheid te hebben om te communiceren met de volgende IP-adressen en poorten:

IP	Poort	Omschrijving
95.170.71.93	51821/udp	VPN verbinding
93.92.99.155	443/tcp	SIEM - Logging

Daarnaast moet de pentestbox in staat zijn om verbinding te maken met het internet in het algemeen, voor het downloaden van tools of het updaten van packages.

De pentestbox zal na afronding van de opdracht eerst door NFIR volledig opgeschoond worden alvorens deze ontkoppeld en vrij van data geretourneerd mag worden. [Meer informatie over de pentestbox](#)

10 Bewaartermijn gegevens

Tijdens de uitvoering van deze opdracht wordt onderzoeksdata gegenereerd. Deze onderzoeksdata wordt één jaar bewaard op een beveiligde omgeving van NFIR BV. Na één jaar wordt de onderzoeksdata verwijderd, tenzij sprake is van een zwaarwegend belang en/of op verzoek van de opdrachtgever. De rapportage van deze opdracht zal 1 maand na de rapportage toelichting gearchiveerd worden, zodat deze beschikbaar is voor hertesten, toekomstige opdrachten en/of een eventueel IT-Security incident.



11 Tarieven en projectkosten

Op basis van de in deze offerte beschreven scope en uw aangeleverde documentatie is een urenrekening gemaakt. In de onderstaande tabel treft u de werkzaamheden, het (fixed) aantal uren en onze tarieven.

Beschrijving van de pentest werkzaamheden	Uren	Uurtarief	Subtotaal
Black Box - Externe Infrastructuur (Timeboxed)	28	€ 175,00	€ 4.900,00
Grey Box - Interne Infrastructuur (Timeboxed)	101	€ 175,00	€ 17.675,00
Grey Box - Locatiebezoek (Timeboxed)	28	€ 175,00	€ 4.900,00
Totaal incl. rapportage en een toelichting meeting van de belangrijkste bevindingen van deze pentest. Exclusief een uit te voeren hertest.	157		€ 27.475,00

De geldigheidsduur van deze offerte bedraagt 30 dagen na offertedatum. Op deze aanbieding zijn de Algemene Verkoopvoorwaarden NFIR (v2.1 maart 2024) van toepassing. Deze zijn als bijlage bij deze offerte toegevoegd. Dit project wordt gefactureerd direct bij oplevering van de rapportage. Alle genoemde tarieven zijn excl. BTW. Deze offerte is 30 dagen geldig. De betalingstermijn is 14 dagen netto.

Mochten er naar aanleiding van deze offerte nog vragen zijn of heeft u de behoefte aan een toelichting, dan vernemen wij dat uiteraard graag. Indien u akkoord gaat met deze offerte, dan verzoeken wij u de getekende versies van deze offerte en de vrijwaringsverklaring retour aan te bieden op de door NFIR aangeboden beveiligde SharePoint omgeving. Zodra wij uw officiële akkoord ontvangen, zullen wij de werkzaamheden samen met u definitief inplannen.

Nogmaals dank voor uw aanvraag en wij kijken er naar uit om deze opdracht te mogen uitvoeren.

Met vriendelijke groet,

Voor akkoord,

NFIR B.V.
S. van den Braak
Accountmanager
23 oktober 2024

Humankind
Naam:
Functie:
Datum:



12 Bijlage 1: Aanvalsscenarios en zeven fasen pentest

12.1 Aanvalsperspectieven

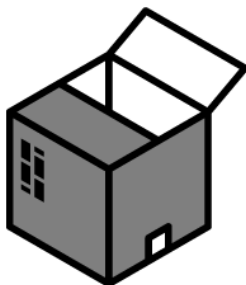
Een pentest kan worden uitgevoerd vanuit verschillende perspectieven, waarbij het resultaat (gedeeltelijk) afhankelijk is van het gekozen aanvalsperspectief. Tijdens een intakegesprek bepalen wij samen de scope van de pentest en adviseren wij over de wijze waarop wij voor uw organisatie de meest waardevolle pentest kunnen uitvoeren.

- **Black Box:** Bij een Black Box aanvalsscenario wordt vooraf minimale informatie verstrekt door de opdrachtgever. De ethische hackers zullen als 'buitenstaanders' opereren zonder voorkennis. De pentesters gebruiken diverse technieken, waaronder Open Source Intelligence (OSINT) om zwakke plekken te ontdekken.
- **Grey Box:** Een Grey Box aanvalsscenario zit tussen een Black en White box in. Er wordt 'beperkt' informatie gedeeld die gebruikt wordt om een omgeving te onderzoeken. De ethisch hackers zullen gebruik maken van een gebruikersaccount voor het onderzoeken van de infrastructuur of applicatie
- **White Box:** Bij een White Box aanvalsscenario (ook wel Crystal box genoemd), wordt vooraf alle informatie verstrekt om gericht op zoek te gaan naar kwetsbaarheden. Denk hierbij aan de informatie die ook bij Grey Box pentesting wordt opgevraagd. Aanvullend hierop wordt gebruik gemaakt van broncode, logbestanden en toegang tot de server. Daarnaast kan er gebruik gemaakt van de mogelijkheid om een eigen testomgeving op te zetten.

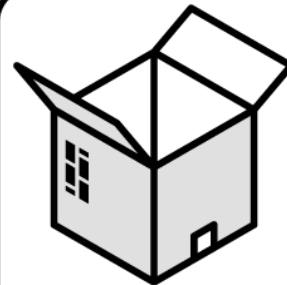
Uiteraard is het mogelijk om een combinatie te maken van verschillende aanvalsperspectieven, om een zo compleet mogelijk beeld van de technische weerbaarheid van uw digitale omgeving te verkrijgen. Daarnaast kan de pentest als een Timeboxed variant worden uitgevoerd, waarbij binnen een vooraf afgesproken aantal uur zo veel mogelijk getest zal worden. Tijdens het intake gesprek wordt de scope vastgesteld, de gewenste (en passende) aanvalsperspectieven besproken en een vorm gekozen waarop de pentest wordt uitgevoerd.



Black Box
Zero Knowledge



Grey Box
Some Knowledge



White Box
Full Knowledge



12.2 De zeven fasen van een pentest

Er zijn zeven fasen tijdens een penetratietest. Deze zeven fasen zijn:

ID	Fase	Omschrijving
1	Informatie verzamelen	Deze fase bestaat uit het verzamelen van zoveel mogelijk informatie uit openbare bronnen (OSINT) en informatie die wordt aangeleverd door de opdrachtgever, zoals netwerktekeningen en een IP-nummerplan.
2	Informatie analyseren	Gedurende deze fase wordt de informatie gewaardeerd en wordt daarmee vastgesteld welke informatie relevant is voor de penetratietest om bijvoorbeeld een aanvalsmethodiek en mogelijke bedreigingen in kaart te brengen.
3	Kwetsbaarheden analyse	Nadat alle informatie is verzameld, wordt in deze fase gezocht naar kwetsbaarheden in systemen en applicaties. Hierbij wordt zowel met automatische tooling als op creatieve wijze handmatig gezocht naar kwetsbaarheden. Tijdens deze fase wordt gebruik gemaakt van diverse internationale standaarden zoals OWASP Top 10, PTES, en OWASP MAS.
4	Exploitatie	Tijdens de exploitatie fase is toegang verkrijgen tot het systeem het doel. De verzamelde informatie wordt gebruikt om op een zorgvuldige wijze aanvallen uit te voeren, met als doel de geïdentificeerde kwetsbaarheden te bevestigen.
5	Post-exploitatie	In de post-exploitatie fase wordt vastgesteld wat de waarde is van het gecompromitteerde systeem. Dit is afhankelijk van de gevonden data en of deze bruikbaar is om het netwerk verder te compromitteren.
6	Rapporteren	Alle bevindingen worden samengebracht in een compleet en helder uitgewerkt rapport. Dit rapport bevat een beschrijving van de bevindingen, een scoresysteem (CVSS) waarbij de kwetsbaarheden een classificatie krijgen, de mogelijke impact van de kwetsbaarheden, en aanbevelingen die uw organisatie helpen met het oplossen van de gevonden kwetsbaarheden.
7	Hertest	Op basis van de aanbevelingen kunnen de gevonden kwetsbaarheden door uw eigen organisatie (of externe partij) worden opgelost. Zodra de kwetsbaarheden zijn opgelost, wordt NFIR veelal gevraagd dit te controleren middels een korte hertest. Er wordt dan onderzocht en gerapporteerd of de kwetsbaarheden daadwerkelijk zijn opgelost. Een hertest kan alleen worden begroot na voltooiing van de initiële penetratietest en als duidelijk is hoeveel kwetsbaarheden hertest moeten worden.