Penetratietesten met Rootsec

#ROOTSEC

Wie zijn wij?

Rootsec is een gerenommeerd IT-security bedrijf uit Almere. Onze kernactiviteiten zijn het uitvoeren van penetratietesten en het leveren van beveiligingsexpertise in de vorm van bijvoorbeeld audits, consultancy en trainingen.

Deze whitepaper moet u zien als een kijkje in onze keuken. Onze penetratietest keuken.

Bij Rootsec voeren wij dagelijks penetratietesten uit voor bedrijven in de meest uiteenlopende sectoren. Dit doen wij inmiddels al 10 jaar met veel plezier, energie en technisch vernuft.
Maar hoe wordt een penetratietest nou precies uitgevoerd?
En wat kunt u, de ontvangende partij, nou precies met de resultaten?

Dit en meer vertellen wij u in deze whitepaper.

#ROOTSEC

Wat is een penetratietest

Wij definiëren een penetratietest als een gecoördineerde aanval op uw systemen met als doel uw beveiliging te breken. Want op het moment dat wij uw beveiliging kunnen omzeilen dan kunnen kwaadwillende dat ook, met alle gevolgen van dien.

Het doel van een penetratietest

Het voornaamste doel van een penetratietest is het verkrijgen van inzicht in de kwetsbaarheden en risico's van de onderzochte systemen. Naast het verkrijgen van inzicht is een penetratietest ook geschikt voor het uiteindelijk verbeteren van de beveiliging op basis van de bevindingen.

Samen met u gaan we de dialoog aan om de scope te bepalen. Gedurende dit gesprek zullen ook de onderzoeksvragen vorm krijgen.

Enkele voorbeelden van onderzoeksvragen vindt u hieronder.

Onderzoeksvragen

- *Is het mogelijk voor een kwaadwillende om op ongeautoriseerde wijze toegang te verkrijgen tot de gespecificeerde doelobjecten?*
- *Is het mogelijk om, eenmaal binnengedrongen, toegang te verkrijgen tot vertrouwelijk materiaal, wijzigingen aan te brengen of om anderszins schade aan te richten?*
- *Wat is de ernst van aangetroffen kwetsbaarheden? Hoe en met welke prioriteit dienen deze te worden verholpen?*
- *Zijn er kwetsbaarheden c.q. zwakke plekken die door de leverancier/ ontwikkelaar moeten worden verholpen?*

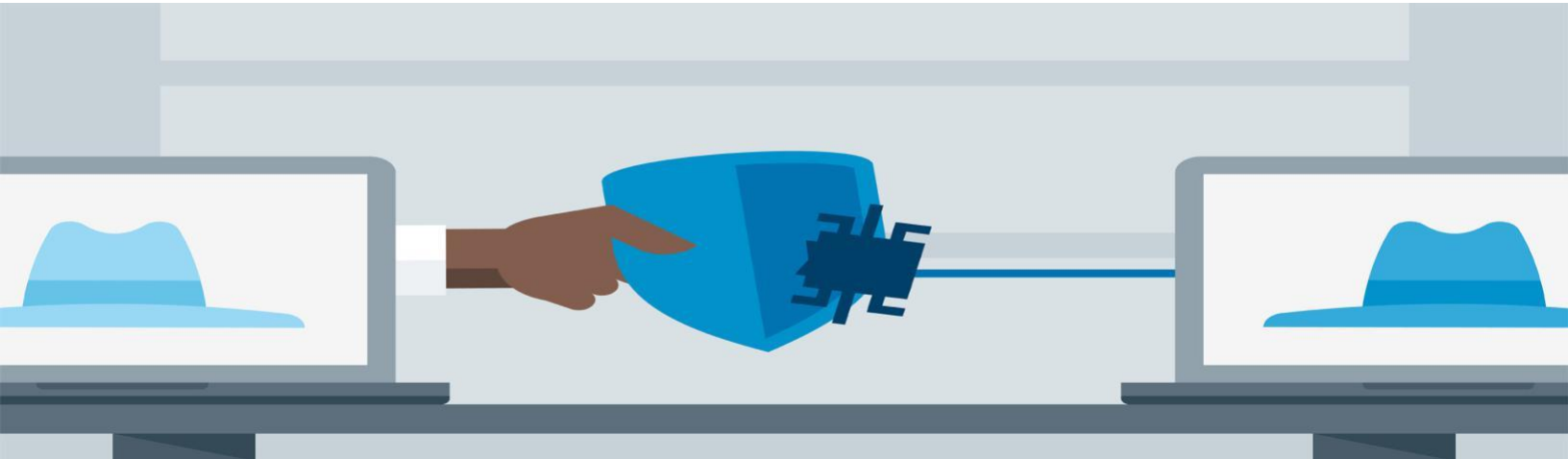
Soorten penetratietesten

Zodra we samen met u de scope en de onderzoeksvragen hebben bepaald, gaan we aan de slag met de test.
Afhankelijk van hetgeen we gaan testen, kiezen we samen met u uit één van de onderstaande methodes, of een combinatie hiervan.

White box penetratietest:
Een penetratietest waarbij de tester volledig inzicht heeft in alle aspecten van de systeemarchitectuur.

Grey box penetratietest:
Een penetratietest waarbij de tester over gedeeltelijke informatie beschikt.

Black box penetratietest:
Een penetratietest met minimale voorkennis.



Wanneer een penetratietest?

Weet u niet zeker of een Penetratietest nodig is voor uw situatie? Dan kunt u altijd vrijblijvend contact met ons opnemen en we denken graag met u mee.
Er zijn echter diverse “standaard” redenen om een penetratietest te laten uitvoeren, hierbij kunt u denken aan:

- U zit in de acceptatiefase van een nieuwe applicatie of een nieuw systeem;
- U heeft recentelijk significante wijzigingen aangebracht aan uw systeem of applicatie;
- Als een periodieke test welke u elk jaar of tweejaarlijks laat uitvoeren;
- Als u reden heeft om te geloven dat de beveiliging van uw systeem minder goed is dan gedacht. Bijvoorbeeld het bekend worden van een

Project timeline

Ons proces

Ondanks dat elke penetratietest een unieke aanpak vereist, hanteren wij bij Rootsec wel een vast proces om zodoende een hoge mate van efficiëntie en kwaliteit te waarborgen. In het onderstaande model ziet u hoe wij stapsgewijs te werk gaan bij het opzetten en uitvoeren van een penetratietest.

1e FASE	2e FASE	3e FASE	4e FASE
			
Onderzoek	**Scannen**	**Hacktest**	**Documenteren**
In samenspraak met u bepalen we middels onderzoeksvragen de scope van het project.	Nadat we de te gebruiken methodiek hebben bepaald, scannen we met geautomatiseerde tools het doelobject.	Nadat we de omgeving hebben gescand gaan we over op manuele hacking om uw omgeving aan te vallen.	Onze penetratietester documenteert al zijn bevindingen en de resultaten worden aan u gepresenteerd.

Handmatig testen

In het model hierboven ziet u dat wij bij Rootsec een duidelijk onderscheid maken tussen het scannen met een diversiteit aan tooling en manuele hacking. Een kwaadwillende zal nooit enkel vertrouwen op tooling. Daarom zullen onze penetratietesters altijd proberen om middels manuele hacking (100% handmatig) toegang te verkrijgen tot uw vitale data of systemen.

Rootsec is ervan overtuigd dat de juiste inzet van een goed geselecteerde toolset bijdraagt aan het versnellen van de werkzaamheden maar niet als vervanger kan dienen van een penetratietest.

Samenwerking

Belangrijk om te weten is dat wij als uitvoerende partij altijd nauw samenwerken met u, de klant. Samen met u bepalen we de scope, de onderzoeksvragen en het type penetratietest. Samen met u bekijken we vervolgens de resultaten en zorgen we ervoor dat u weet welke stappen u dient te ondernemen om op het gewenste IT-security niveau te komen.

Rapportage

Wij hebben lang nagedacht over de beste manier van rapporteren. De ‘traditionele manier’ via een pdf vol met bevindingen en aanbevelingen is altijd de norm geweest. Maar wij zijn van mening dat een statische rapportage niet past in een dynamische omgeving als die van IT-security. Het is daarom dat wij **Rootdash** hebben ontwikkeld, een interactief en dynamisch platform. Wanneer u een penetratietest laat uitvoeren bij Rootsec dan presenteren wij de resultaten hiervan op Rootdash. Zo heeft u snel overzichtelijk wat de huidige status van uw IT-beveiliging is, welke bevindingen per direct opgelost dienen te worden en natuurlijk hoe deze opgelost moeten worden.

Ons interactieve platform geeft u alle tools om intern aan de slag te gaan. Per bevinding ontvangt u van ons een beschrijving van het risico, waar het zich bevindt en hoe het opgelost kan worden. In helder Nederlands en zonder overbodig moeilijke vaktaal. En heeft u toch nog vragen? Stel deze dan op Rootdash en één van onze IT-experts zal uw vraag z.s.m. beantwoorden. Wij zien Rootdash daarom niet enkel als een rapportage platform maar ook als een monitoring tool. Heeft u een kwetsbaarheid opgelost? Dan wordt dat bijgewerkt in Rootdash en zodoende heeft u altijd een **actueel overzicht** van uw IT-security status.

En wilt u toch iets tastbaars? Dan draait u via het platform met slechts een enkele klik een PDF uit. Wilt u Rootdash graag een keer in actie zien? Vraag dan gratis een demo aan en laat u overtuigen.

Toch liever een PDF zoals u gewend bent? Dan kunnen we dit tegen een meerprijs voor u realiseren.

Adres	Telefoon	Contact
Rootsec B.V.	036 760 04 51	Brian de Leeuwe
P.J. Oudweg 4	06 225 665 47	b.deleeuwe@rootsec.nl
1314CH Almere		