PEN TESTING

BETAALBAAR, NAUWKEURIG EN ON-DEMAND

Maak kennis met onze Pen Testing, een uitgebreid penetratietestplatform dat de nieuwste kennis, methodologieën, technieken en veelgebruikte tools van meerdere consultants in één platform integreert. Pen Testing is ontworpen om netwerkpenetratietests betaalbaarder, nauwkeuriger, sneller en consistenter te maken, zonder menselijke fouten. Ons eigen framework groeit continu op basis van ons onderzoek en ontwikkeling, waardoor we de manier waarop penetratietests worden uitgevoerd, kunnen moderniseren.

WAT IS GEAUTOMATISEERDE PENETRATIETESTING?

Pen Testing is een geautomatiseerd penetratietestplatform dat de kennis, methodologie, processen en tools van een hacker combineert in een enkel, inzetbaar SaaS-platform voor organisaties van alle groottes. Met Pen Testing kunnen organisaties op elk gewenst moment een penetratietest uitvoeren binnen hun omgeving, waarmee ze voldoen aan zowel compliance-eisen als aan beveiligingsbest practices. Dit platform, ontwikkeld en onderhouden door Vonahi Security, is gebaseerd op een framework dat continu verbetert.

Traditioneel gezien staan organisaties voor verschillende uitdagingen bij het zoeken naar een penetratietest, zoals beschikbaarheid, ervaring en achtergrond, evenals lage kwaliteit van de opgeleverde resultaten die niet effectief de kritieke problemen en herstelstrategieën communiceren die organisaties moeten volgen om hun algehele cyberrisico te verminderen. Door meerdere jaren ervaring, certificeringen en industriële bijdragen, inclusief talrijke tools, lost Pen Testing een cruciale behoefte op voor organisaties in een voortdurend veranderend dreigingslandschap.

GEVALIDEERD DOOR EXPERTS

Door de kennis, vaardigheden, logica en tools van talrijke consultants te combineren in één oplossing, is Pen Testing de perfecte oplossing om consistent te voldoen aan de behoeften van je organisatie voor kwaliteitsresultaten.

- **Geen planningsconflicten meer.**
- **Een volledige penetratietest, wanneer je maar wilt en zo vaak je maar wilt.**
- **Ontwikkeld op een framework en methodologie die veranderen en verbeteren naarmate de bedreigingen in de industrie toenemen.**
- **Ondersteund door meer dan 10 jaar ervaring en consultants die OSCP-, CISSP-, CEH- en OSCE-gecertificeerd zijn.**

REAL-TIME ACTIVITEITSTRACKING

Een belangrijke stap bij het beoordelen van het risico voor je organisatie is het vermogen om kwaadaardige activiteiten binnen je omgeving te detecteren en erop te reageren. Pen Testing maakt een apart logbestand voor elke activiteit die wordt uitgevoerd, zodat je onze activiteiten kunt correleren met je monitoring- en loggingsoplossingen.

VOLDOEN AAN COMPLIANCE EN BEST PRACTICES

Door de mogelijkheid te hebben om op elk gewenst moment en zo vaak als je wilt een kwalitatieve netwerkpenetratietest uit te voeren, kan je organisatie er zeker van zijn dat het continu voldoet aan beveiligingsbest practices en nalevingsvoorschriften.

PEN TESTING

ONZE GEAUTOMATISEERDE PENETRATIETESTMETHODOLOGIE

Pen Testing combineert meerdere methodologieën die voorheen handmatig werden uitgevoerd tot een geautomatiseerde aanpak om consequent maximale waarde te bieden aan organisaties.

EGRESS FILTERING TESTING

Voer automatisch egress filtering uit om ervoor te zorgen dat je organisatie effectief onnodig uitgaand verkeer beperkt. Onbeperkte uitgaande toegang kan een kwaadwillende actor in staat stellen gegevens uit de omgeving van je organisatie te exfiltreren via traditionele methoden en ongecontroleerde poorten.

AUTHENTICATIE AANVALLEN

Bij de ontdekking van gebruikersaccountgegevens zal Pen Testing automatisch proberen deze gegevens te valideren en bepalen waar ze het meest bruikbaar zijn. Dit is een gangbaar proces dat zowel door kwaadwillende aanvallers als penetratietesters wordt uitgevoerd tijdens privilege-escalatie.

PRIVILEGE ESCALATIE EN LATERALE BEWEGING

Met een geldige set inloggegevens zal Pen Testing proberen waardevolle gebieden binnen je organisatie te identificeren. Dit wordt uitgevoerd via verschillende methoden, waaronder het gebruik van Vonahi's Leprechaun-tool, die helpt bij het identificeren van gevoelige doelen.

DATA EXFILTRATIE

Het verlies van kritieke data uit je organisatie is een zeer ernstig probleem. Als toegang tot vertrouwelijke en/of gevoelige data kan worden verkregen, zal Pen Testing deze activiteit simuleren en loggen om je organisatie te helpen de gebieden te versterken die data-exfiltratie zouden moeten beperken.

GESIMULEERDE MALWARE

Met verhoogde toegang zal Pen Testing proberen kwaadaardige code op externe systemen te uploaden om de anti-malwaremaatregelen van de organisatie te testen.

TIJDIGE RAPPORTAGE

Pen Testing genereert een managementsamenvatting, een technisch rapport en een kwetsbaarheidsrapport binnen 48 uur na voltooiing van de penetratietest. Onze gedetailleerde resultaten stellen je netwerkteam in staat om onze activiteiten te vergelijken met monitoring- en waarschuwingscontroles.

NEEM DIRECT CONTACT MET ONS OP OM MEER TE WETEN TE KOMEN

info@heiper.nl