IngramMicro
FlexibleServices

INGRAM MICRO

Basic Penetration Test (BPT)

Het Ingram Micro Cyber Security Center of Excellence team is opgericht met de visie om te helpen het Cyber Security potentieel te ontsluiten. Het team, dat gevestigd is in Utrecht, biedt een reeks gespecialiseerde Cyber Security consultancy- en trainingsoplossingen aan onze Business en Channel Partners.

Met een services portfolio bestaande uit technische assessments, consultancy en managed security services zijn we in een zeer sterke positie om onze channel partners te helpen om elke cyber security deal te winnen. We doen dit door onze partners volledig te ondersteunen bij complexe security vraagstukken en de mogelijkheid te bieden om zelf cyber security diensten (door) te ontwikkelen en verder te laten groeien om zo lucratieve white-labelled beveiligingsdiensten aan te bieden aan eindklanten.

INGRAM MICRO

Cyber Security Center

IngramMicro
FlexibleServices

Penetration Testing (PT) is het proces van het evalueren van de huidige beveiligingsstatus van een systeem of netwerk om kwetsbaarheden op te sporen die een aanvaller zou kunnen gebruiken om ongeautoriseerde toegang tot systemen en informatie te verkrijgen. Dit proces omvat de identificatie van zwakke plekken in de beveiliging die het gevolg kunnen zijn van een onjuiste beveiligingsconfiguratie van systemen of toepassingen en bekende of onbekende kwetsbaarheden in hardware- of softwaresystemen.

De scope van Basic Penetration Testing omvat in scope IT-assets van de organisatie. De IT-assets omvatten firewalls, routers, VPN, IDS/IPS, webservers, applicatieservers, databaseservers, enz. Penetratietesten geven inzicht in de huidige staat van beveiliging van de organisatie, ontdekken mogelijke manieren om door te dringen en testen de effectiviteit van de beveiligingsmaatregelen.

In plaats van een simpele opsomming van alle individuele kwetsbaarheden in elke IT-asset, is onze aanpak het vinden van de systematische problemen in de organisatie die tot deze problemen hebben geleid. We gebruiken vaak een steekproefmethodologie in onze aanpak om ons te richten op de hoofdoorzaken en de belangrijkste saneringsstappen te prioriteren. Bij het uitvoeren van Basic Penetration Testing zijn onze testen gerelateerd aan de veilige controles die zijn ontworpen om de eventuele negatieve impact op de productieomgeving van de organisatie te beperken.

Bij het leveren van de dienst Basic Penetration Testing gebruikt Ingram Micro een combinatie van geautomatiseerde en handmatige scanmethoden en maken we gebruik van commerciële en publiekelijk beschikbare hulpmiddelen, evenals aangepaste scripts en toepassingen die in huis zijn ontwikkeld.

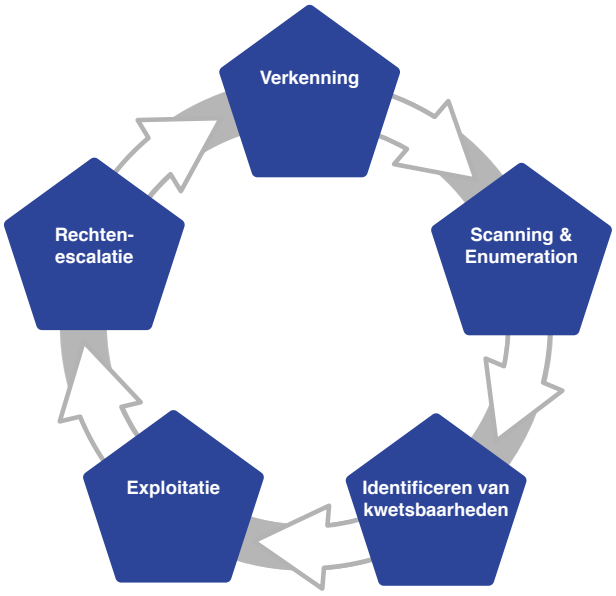
Het Basic Penetration Testing proces bestaat uit de volgende stappen:

- Verkenning: het verzamelen van voorlopige gegevens of inlichtingen over de doelorganisatie. De gegevens worden verzameld om de aanval beter te kunnen plannen. De informatie die in deze stap wordt verzameld, omvat IP-adres ranges, openbare e-mailadressen, websites en andere.
- Scanning & Enumeration: het verzamelen van meer informatie over de aangesloten systemen, lopende applicaties en de diensten in het netwerk van de organisatie. Informatie zoals type en versie van het besturingssysteem, gebruikersaccounts, e-mailadressen, serviceversies en releasenummers worden ook verzameld.
- Identificeren van kwetsbaarheden: op basis van de informatie die in de vorige twee fasen is verzameld, identificeren we zwakke diensten die in het netwerk draaien of applicaties die bekende kwetsbaarheden hebben.
- Exploitatie: gebruikmakend van direct beschikbare code of een aangepaste code om geïdentificeerde kwetsbaarheden te gebruiken om toegang te krijgen tot het kwetsbare systeem.

IngramMicro
FlexibleServices

IngramMicro
FlexibleServices

- Rechtenescalatie: in sommige gevallen biedt de bestaande kwetsbaarheid alleen toegang op een laag niveau, zoals normale gebruikerstoegang met beperkte rechten. In deze stap zullen we proberen om volledige administratieve toegang te krijgen op de machine.



Na afronding van de Basic Penetration Test wordt een gedetailleerd rapport gestuurd met daarin het volgende:

- Managementsamenvatting: samenvatting van het doel van deze beoordeling, evenals een korte uitleg van de bedreigingen waaraan de organisatie wordt blootgesteld vanuit een zakelijk perspectief.
- Bevindingen: een gedetailleerde, technische uitleg van de bevindingen van de beoordeling, samen met stappen en bewijzen van de bevindingen.
- Conclusie & aanbevelingen: in dit hoofdstuk vindt u de laatste aanbevelingen en een samenvatting van de kwesties die tijdens de beveiligingsbeoordeling zijn gevonden.

Meer weten over onze Cyber Security Assessment services?
Neem contact op met het Ingram Micro Cyber Security Center of Excellence (COE) via cs-coe-weur@ingrammicro.com of met uw Account Manager.

IngramMicro
FlexibleServices