

## Aanval- en penetratietest



*U heeft beveiligings-technieken geïnstalleerd zoals Firewalls, Intrusion detection/protection, en encryptie van gevoelige bedrijfsgegevens. Uw medewerkers veranderen iedere maand hun wachtwoord en de ingang tot uw bedrijfspand en datacenter worden nauwlettend in de gaten gehouden door een gedisciplineerde receptioniste. En toch heeft u af en toe het angstige gevoel dat de beveiliging misschien niet adequaat en volledig is ingericht.*

*ISSX kan u helpen.*

### ISSX, Experts in IT Security

ISSX ontstaat in 2007 met als achtergrond IT infrastructuur en applicatie beveiliging. ISSX is een snelgroeiend bedrijf met als primaire focus (technische) informatie beveiliging. ISSX richt zich zowel op onderzoek als op beveiliging voor alle segmenten door gebruik te maken van eigen kennis en innovatie. Zowel overheid-, financiële-, medische-, als juridische instellingen zijn vanaf het begin belangrijke klanten.

Op dit moment is ISSX één van de meeste gespecialiseerde bedrijven op het gebied van (technische) informatie beveiliging.

ISSX heeft ruime ervaring in het uitvoeren van penetratie testen (ethical hacking), systeem audits en risico analyses en BCP. Wij hebben penetratietesten en security audits uitgevoerd voor een groot aantal klanten, waaronder financiële instellingen, medische instellingen, overheidsinstellingen en juridische instellingen.

### Wat is een penetratietest?

Een penetratietest is vaak een onderdeel van een audit. Het netwerk, systemen, zoals firewalls, web servers en mail servers en (web) applicaties van een organisatie worden aangevallen op een manier zoals een hacker dat ook zou doen.

Een penetratie test bestaat globaal gezien uit twee delen: een vulnerability assessment en een uitgebreide (handmatige) test met diepgang. Tijdens de vulnerability assessment wordt met diverse automatische tools gezocht naar bekende kwetsbaarheden. In het tweede deel wordt niet alleen gezocht naar bekende kwetsbaarheden, maar ook naar minder bekende kwetsbaarheden of combinaties van kwetsbaarheden.

De primaire focus is access control. Lukt het een potentiële aanvaller om:

- toegang te krijgen tot vertrouwelijke of geheime informatie;
- Uw bedrijf substantiële financiële schade en/of reputatieschade toe te brengen;
- de bedrijfscontinuïteit van uw bedrijf in gevaar te brengen;
- een anderszins nieuwswaardig voorval te creëren;
- de veiligheid van klanten, bezoekers en/of personeel van uw bedrijf in gevaar te brengen.



*“Bent u zich bewust van de gevaren binnen uw eigen (online) omgeving?”*



*Mochten er tijdens het testen ernstige beveiligingsrisico's worden geconstateerd dan neemt ISSX deze direct op met de opdrachtgever. ISSX kan dan assisteren met het oplossen.*

## Focus penetratietest

De focus van de ISSX penetratietest ligt op de volgende onderdelen:

- Het **profileren** van beschikbare informatie welke gerelateerd kan worden aan de applicatie en/of het bedrijf welke misbruikt kan worden door kwaadwillende aanvallers.
- **Kwetsbaarheid analyse** (externe audit, penetratietest, DDoS test) van de eerder genoemde omgevingen waarin wordt gekeken of de aan het internet gekoppelde systemen welke deel uitmaken van eerder genoemde omgeving ongewenste kwetsbaarheden bevatten.
- **Beoordeling** van de infrastructuur welke wordt gebruikt om de applicatie(s) te faciliteren.
- Bepalen welke services draaien op de systemen, welk operating systeem wordt gebruikt, waar het systeem staat (intern / extern) etc.
- **Manipulatie** van gegevens / data.
- **Manipulatie** / penetratie van de management interfaces.
- **Manipulatie** van de applicaties in de backend
- **Manipulatie / verzamelen** van data direct van de database door gebruik te maken van applicatie hacking technieken zoals SQL-injection, enumeration van data etc. in relatie tot lijsten zoals de SANS top-20, OWASP-10 etc.

## Doelstellingen penetratietest

ISSX heeft de penetratietest ontworpen om de volgende doelstellingen te halen:

- De scope van deze penetratie test is het identificeren en verifiëren van verdachte services, applicaties, mogelijke manieren om data te verzamelen, of het penetreren van de eerder genoemde infrastructuren.
- Er wordt extern of intern getest tegen systemen.
- Verschillende scan en penetratie pogingen zullen worden uitgevoerd om zwakheden in security (tegen)maatregelen, applicaties en databases te identificeren. Dit zal resulteren in een identificatie van kwetsbaarheden op de gevonden internet (en intranet) toegankelijke systemen.
- Analyseren en verwerken van de resultaten in een rapport en het opnemen van “Best-Practice” aanbevelingen. Het rapport wordt overgedragen aan het management en er zal kennisoverdracht / technische discussie plaatsvinden met technische en/of functionele beheerders.

## Deliverables

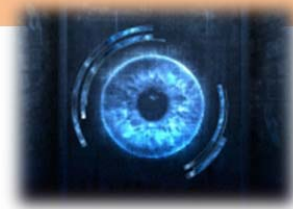
Na het uitvoeren van de penetratietest levert ISSX de volgende zaken op:

- Rapport met de resultaten en aanbevelingen
- Het rapport moet begrijpbaar en leesbaar zijn door zowel management als IT technici en zal bestaan uit:
  - Management samenvatting
  - Inleiding en beschrijving opdracht
  - (technische) bevindingen en aanbevelingen (met details in bijlagen)
- Management presentatie met aansluitend een technische sessie / discussie waarbij de resultaten en aanbevelingen gepresenteerd en besproken worden.

## Methode van testen

De ISSX penetratietest bestaat uit 4 fases:

- *Internet verkenning*
- *Vulnerability scan*
- *Applicatie penetratietest*
- *Analyse en documentatie*



### Internet verkenning

Tijdens deze fase zal ISSX (gedetailleerde) informatie proberen te verkrijgen over de netwerk infrastructuur. Deze informatie kan gebruikt worden door een hacker om een lay-out van het netwerk te maken.

Alle verzamelde informatie wordt helder gedocumenteerd en bevat tevens de bron van de data. De volgende stappen worden uitgevoerd tijdens deze fase:

- Probeer informatie te verzamelen van Internet resources; onderzoek internet resources voor infrastructuur informatie. Bronnen bevatten o.a., maar zijn niet gelimiteerd tot: corporate websites, vendor websites, partner websites, artikelen, nieuwsgroepen, chat rooms en andere elektronische methodes.
- Probeer Domain Name System (DNS) transfers en queries; het uitvoeren van DNS en reverse DNS queries en transfers in een poging om informatie te verzamelen over de (interne) systemen.
- Host Enumeration; basis scans en verkenning in een poging om het netwerk te en de systeem functionaliteit te doorgronden.
- 

In sommige gevallen, uiteraard na overleg met de opdrachtgever, kan ISSX gebruik maken van technieken als social engineering en dumpster diving om eventuele processen en procedures rondom de applicaties te testen.

### Verkenning netwerk / Vulnerability scan

Tijdens deze fase zal ISSX o.a. poortscans uitvoeren om de "live" hosts te detecteren, gevolgd door gedetailleerde scans voor het detecteren van mogelijke vulnerabilities. Deze fase bevat tevens het detecteren van eventuele koppelingen naar 3<sup>e</sup> partijen en penetratietesten.

ISSX voert vulnerability scans uit tegen de systemen en netwerken. Het scan proces bevat de volgende testen/scans:

- Systeem identificatie; identificeer het type device en het OS.
- Service discovery; identificeer services welke mogelijk reageren op aanvragen op o.a. servers, routers, firewalls en werkstations.
- In-depth service probing; ontdekte services worden grondig getest om mogelijke toegangspunten tot een systeem te ontdekken.
- Vulnerability identificatie; test voor bekende vulnerabilities op bereikbare systemen door gebruik te maken van standaard tools en methodes.
- (D)DoS test; verificatie of systemen en netwerken niet crashen onder de load van een distributed packet flood aanval.
- 

ISSX zal proberen de vulnerabilities te verifiëren en te exploiteren op de systemen om zo "trofeeën" te verzamelen als bewijs. De methodes van exploiteren worden gedetailleerd uitgelegd in het eind rapport.



*Uiteraard kunnen de penetratietesten ook op het interne netwerk worden uitgevoerd. De stappen blijven hetzelfde, er wordt alleen van binnen uit getest.*

## Applicatie penetratietesten

ISSX zal proberen zwakheden te identificeren in de specifieke applicaties. ISSX voert deze penetratie test uit door te testen zonder kennis en toegang tot de applicatie (black box).

Tijdens deze testen wordt heel specifiek gekeken naar het gedrag van de applicaties (o.a. XSS en SQLi), mogelijke zwakheden en of het bijv. mogelijk is in te loggen met standaard accounts.

De focus van de applicatie penetratietesten ligt op de OWASP top 10:

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

## Analyse en documentatie

ISSX zal alle verzamelde data zorgvuldig analyseren en verwerken in het eind rapport. Dit rapport wordt opgeleverd als een beveiligde PDF file en in een aantal geprinte versies.

ISSX levert tevens een CDROM met alle "raw" data welke is verzameld in de testen.

Het eindrapport bevat de volgende zaken:

- Management samenvatting
- Informatie verzameling / Omschrijving netwerk, systemen en applicaties
- Reconnaissance profiel samenvatting
- Vulnerability analyse
- Penetratie test analyse
- Overzicht resultaten van systeem discovery en security scans
- Overzicht resultaten van security scans
- Aanbevelingen met prioriteiten
- Gedetailleerde omschrijving van gevonden zaken

De resultaten en de deliverables worden besproken tijdens een technische sessie.

## Prijs en vervolg

Elk traject begint met een vrijblijvend intake gesprek waarbij wij met u verkennen wat er exact nodig is en in hoeverre ISSX de ideale partner zou zijn. Op basis van dit gesprek kunnen wij u een begroting en voorstel op maat aanleveren. U weet exact waar u aan toe bent.

Transparantie is bij ISSX overal terug te vinden. Neem contact met ons op via [info@issx.nl](mailto:info@issx.nl) of 033-4779529 om een afspraak voor een intake gesprek te maken of kijk op onze website (<http://www.issx.nl>) voor meer informatie.



*"Beveiliging: Ga niet alleen op de buitenkant af. ISSX kan u ook helpen met o.a. het testen van de beveiliging van uw WLAN, Third Party connecties, onveilige poorten en protocollen op uw netwerk, interne security audits, review (security) architectuur, opleidingen, juiste inrichting interne machines en bewustwording medewerkers."*