V1.2

Security profiel vulnerability scan

Door middel van een kwetsbaarheden (vulnerabilities) scan zoek je in een netwerk naar systemen met een “bug”. Dit kan zijn dat je gevoelige data kunt inzien zonder dat je daar toestemming voor hebt. Ook kan het betekenen dat bijvoorbeeld de werking van een systeem of een applicatie kan worden verstoord of zelfs niet meer bereikbaar is.

De reden dat een bedrijf een kwetsbaarheden scan wil laten uitvoeren is vaak preventief. Het bedrijf checkt of er mogelijk zwakke plekken gevonden kunnen worden. Ook na grote wijzigingen in het netwerk of het in gebruik nemen van een nieuwe applicatie is een kwetsbaarheden scan een goede manier om de security te testen.

Het verschil met een penetratietest is dat een kwetsbaarheden scan snel en breed naar een systeem kijkt om mogelijke lekken op te sporen. De software doet geen poging om het lek te dichten of uit te buiten. Een kwetsbaarheden scan geeft een goede indicatie van de beveiliging van een systeem of applicatie en kan op maandelijkse basis worden uitgevoerd zonder verdere kosten. Een penetratietester probeert om een kwetsbaarheid uit te buiten en voert een veel dieper onderzoek uit.
Bij een kwetsbaarheden scan is de rapportage vaak geautomatiseerd, bij een pentest opgesteld door de tester.
De vulnerability scan wordt uitgevoerd door middel van Tenable Nessus, een welbekende scan met een professionele gratis versie.

Voordat de scan wordt geconfigureerd en uitgevoerd wordt het security profiel voor de Nessus van het bedrijf ingevuld. Het profiel bestaat uit een stappenplan wat inzicht geeft in de specifieke omstandigheden van het bedrijf.

Alle profielen beginnen met de formulering van het hoofddoel, het ***waarom*** van de specifieke test. Dit kan variëren van een preventieve scan tot een scan om een specifieke poort te controleren.

## Stap 1: Bepaal je doelen

Bepaal in samenspraak met de klant welke doelen je met de scant bereiken. Stel hier vast welke onderdelen worden getest en welke kwetsbaarheid wordt onderzocht. Dit is in veel gevallen een algemene scan, maar kan voor een bedrijf ook een specifiek systeem zijn. Bijvoorbeeld op Server X de ftp-poort of een scan op een wat verouderde router.

**Onderzoeksvragen**
Nadat het bereik van de test is geformuleerd kan je ene of meerdere onderzoeksvragen beschrijven. Je formuleert de onderzoeksvragen in overleg met de klant. Voorbeelden zijn:

- Zijn er op de gescande systemen kwetsbaarheden gevonden die niet bekend zijn bij het ICT team?
- Op systeem X is een nieuwe security policy geïmplementeerd, zijn er specifieke kwetsbaarheden naar voren gekomen?
- Hackers een maand geleden getracht systeem Y binnen te dringen, zijn op systeem (nog) open poorten te vinden?
- Systeem A heeft een netwerkverbinding naar een systeem van een externe leverancier, zijn er kwetsbaarheden te vinden op dat externe systeem?

Als stap 1 volledig is doorlopen is in kaart gebracht wat het doel van de test is en welke systemen worden gescand. De klant heeft via de onderzoeksvragen kenbaar kunnen maken waar de prioriteiten liggen.

**Details uitvoering scan**

In stap 2 bepaal je welke systemen worden gescand met welke scan. Betreft het één IP-adres of een range aan IP-adressen? Dit is de scope van de scan en is definitief. Per vermeld systeem wordt aangegeven op welk risico de scan specifiek is gericht. Dit is in de meeste gevallen een preventieve scan, wat wel het “laaghangend fruit” wordt genoemd. De scan geeft een algemeen overzicht hoe het met de security is gesteld. Een penetratietest kan vervolgens testen of de gevonden kwetsbaarheid uitgebuit (lees gehackt) kan worden

| Profiel securitytest 1 vulnerability scan | | | |
|---|---|---|---|
| Stappenplan | | Input voor opdrachtformulering – detaillering | |
| Bedenk waarom je een vulnerability test wilt | Wat is het **hoofddoel** van de vulnerability testen? | | |
| Stap 1: Bepaal je doelen | Onderdelen | Welk kwetsbaarheden wilt u laten controleren? | |
| Bepaal wat je wilt laten onderzoeken. | Server systemen | | |
| | Netwerkcomponenten | | |
| | Client systemen | | |
| Vulnerability scan onderzoeksvragen | | | |
| Onderzoeksvraag 1 | | | |
| Onderzoeksvraag 2 | | | |
| Onderzoeksvraag 3 | | | |
| Stap 2: detaillering bereik | Scan | Systemen | |
| Bepaal welke scans je wilt toepassen | Basic network | Welk systeem | |
| | ….. | | |
| | ….. | | |
| | ,….. | | |
| | IP-adres | FQDN | Poorten |
| Systeem A | | | |
| Systeem B | | | |
| Systeem C | | | |