VULNERABILITY SCANNING

Praktijkervaringen binnen een academische omgeving

Dreigingen veranderen met de minuut. Om goed inzicht te krijgen aan welke risico's een organisatie bloot staat, is regelmatig onderzoek naar kwetsbaarheden vereist. Alleen dan kunnen passende corrigerende acties genomen en verrassingen voorkomen worden. Uitdaging hierbij is het om de gevonden kwetsbaarheden op de juiste manier binnen je organisatie te laten landen. Draagvlak van de organisatie en beheerders is hierbij cruciaal.

Kwetsbaarheidsscans ofwel vulnerability scanning is het geautomatiseerd zoeken naar kwetsbaarheden in software en bijbehorende configuraties. Penetration testing gaat een stap verder en probeert actief binnen te dringen in een specifieke applicatie. Met dit artikel deel ik onze ervaringen, zoals wij die hebben opgedaan bij de implementatie en het gebruik van de Rapid7 Nexpose kwetsbaarheden scan tool bij de Wageningen UR.

Aanleiding voor de implementatie was het vaststellen van een technisch auditplan voor de centrale IT-omgeving. Hierin staan uitgangspunten opgenomen en is grofweg aangegeven wanneer welke scans en interne/externe audits uitgevoerd dienen te worden. Kwetsbaarheden tests zijn één van de aandachtspunten hierbij. Verder komt kwetsbaarheden scanning terug als kritieke controlemaatregel op bijvoorbeeld de Critical Security Controls for Effective Cyber Defense lijst van SANS[1] of in de ISO 27002 standaard. Het wordt zodoende algemeen beschouwd als een belangrijke maatregel in de bescherming van informatie.

Initieel werden alle penetration tests en vulnerability scans extern uitbesteed. Echter, om eigen kennis en ervaring te kunnen opbouwen en omdat kwetsbaarheden scanning een continue of minimaal periodiek (bijvoorbeeld maandelijks) proces dient te zijn, is besloten om deze scans zelf te gaan uitvoeren. Verder speelde het feit dat bleek dat een eenmalig rapport met een lange lijst van mogelijke kwetsbaarheden door de beheerders lastig te interpreteren is op relevantie en specifieke lokale omstandigheden. Ofwel, in hoeverre zijn de gevonden kwetsbaarheden ook daadwerkelijk uit te buiten in onze situatie? Een andere reden was de reductie van externe kosten voor kwetsbaarheden scans en de mogelijkheid om de kwetsbaarheden tool te kunnen inzetten ter ondersteuning van penetration tests.

Selectie

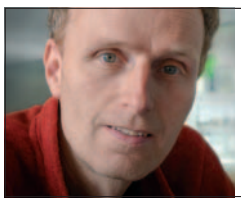
Nadat het besluit genomen was om kwetsbaarheden scanning zelf te gaan uitvoeren is onderzocht welke producten er op de markt zijn en waarin ze verschillen. Het bleek nog niet zo eenvoudig om een helder beeld te krijgen van de verschillen tussen de diverse leveranciers. De functionaliteit verschilt sterk, zo is de ene tool beperkter en enkel gericht op netwerk of webscanning en biedt de andere tooling uitgebreidere functionaliteit om het hele vulnerability managementproces te ondersteunen. De Wageningen UR heeft specifieker gekeken naar de mogelijkheden die o.a. Nessus, QualysGuard, Core Impact, Nexpose/Metasploit boden. Er is uiteindelijk gekozen voor Rapid7 Nexpose in combinatie met Metasploit. Voor specifieke applicaties zoals web-applicaties en SAP blijven aanvullende specifieke tools nodig.

Selectiecriteria

- bewezen technologie en dus geen nieuwkomer op de markt
- grote, actuele en gevalideerde kennisbank van kwetsbaarheden
- bij voorkeur mogelijkheid voor lokale installatie
- goede mogelijkheden tot rapportages op verschillende niveaus (management maar ook detail en achtergrond informatie over de bevindingen en praktische instructies hoe de kwetsbaarheden op te lossen zijn)
- mogelijkheden voor goede en snelle support en partnership met de producent en leverancier
- prijs
- weinig false positives
- mogelijkheid om te valideren dat kwetsbaarheden daadwerkelijk uit te buiten zijn
- stabiliteit en betrouwbaarheid van de tool ten aanzien van verstoringen op gescande omgevingen

Implementatie

Na de keuze voor de tooling diende deze geïnstalleerd te worden en geconfigureerd te worden op basis van onze eigen wensen. Hieronder een toelichting op een aantal van onze keuzes en aandachtspunten waar wij tegen aan liepen. Nadruk ligt hierbij op de ervaringen met Nexpose en minder op Metasploit.



Raoul Vernède. Raoul is werkzaam als security manager bij Wageningen UR.
Hij is te bereiken via raoul.vernede@wur.nl

Installatie van Nexpose en Metasploit werd gedaan op een eigen managed Linux server en verliep relatief makkelijk. De integratie tussen Nexpose en Metasploit werkt jammer genoeg nog niet optimaal.

Scans kunnen uitgevoerd worden als externe non-authenticated scans (oogpunt van externe hacker) met een beperkte resultaat. Anderzijds kunnen de scans draaien met de toegangcredentials van de servers (geauthentiseerde scans) en zo extra en meer diepgaande informatie vergaren.

Wij hebben er voor gekozen om al onze scans authenticated te draaien. Het is dan natuurlijk cruciaal dat de wachtwoorden zorgvuldig beschermd worden binnen de scantool en tijdens het inlogproces. Een optie hierbij is om een apart specifiek account voor de scantool te gebruiken waarbij het wachtwoord periodiek gewijzigd wordt. Check in hoeverre de vulnerability applicatie is gepentest door de leverancier of voer zelf een penetratietest uit. Zorg er verder natuurlijk voor dat updates op OS- en Rapid7-niveau snel uitgerold worden.

in hoeverre zijn de gevonden kwetsbaarheden ook daadwerkelijk uit te buiten

Al onze fysieke en virtuele servers in beide datacentra van zowel de productie als ook OTA (ontwikkel-, test- en acceptatie) omgevingen worden maandelijks gescand. Het scannen gebeurt overdag omdat bij eventuele problemen direct ingegrepen kan worden. Wij scannen niet tegen bepaalde standaard policies, zoals die bijvoorbeeld in de bankenwereld vaker gehanteerd worden (bijvoorbeeld PCI). In de planning van de scans houden wij rekening met de maandelijkse updates van Microsoft. Zodoende gebruiken we Nexpose ook om te controleren of alle updates en patches zijn uitgerold. Tussen het scannen van de OTA en de productie omgeving zit een week; mogelijke verstoringen zoals datacorruptie door SQL-injection komen dan vroegtijdig aan het licht. Bedoeling is om op een later tijdstip ook de decentrale servers buiten de datacentra te gaan scannen. In geval van ontdekking van ernstige nieuwe kwetsbaarheden (denk aan Heartbleed) dient tussentijds gescand te worden.

Bij de inrichting van Nexpose is het mogelijk IP-ranges automatisch in kaart te brengen (via discovery). Er is geen integratie met bijvoorbeeld Active Directory of DNS om servers automatisch te provisionen. Er is een koppeling met VMware mogelijk maar dit werkt alleen voor virtuele machines.

Het ontbreken van een dergelijke integratie veroorzaakt voor ons veel administratief werk. Feitelijk importeren we nu uit de CMDB een serverlijst in Nexpose. Het blijkt hierbij in de praktijk wel lastig om de serverlijst (of asset-lijst) in Nexpose up-to-date te houden. Heeft men wel een up-to-date CMDB, dan kan Nexpose gebruikt worden om rogue apparaten te ontdekken en om de CMDB op correctheid te checken.

Bij de inrichting van Nexpose hebben wij er voor gekozen om een verbinding te maken tussen de verschillende teams en beheerders en anderzijds de servers die zij beheren. Dit is voor ons cruciaal. Hierdoor is het makkelijker om de bevindingen van de scans (via specifieke rapportages) terug te koppelen aan de verantwoordelijke teams (bijvoorbeeld database, web, etc.) met hun technische beheerders. De beheerder kent de servers die hij beheert en kan de bevindingen interpreteren en eventueel corrigerende maatregelen nemen. Beheerders hebben het vaak erg druk met het uitrollen van nieuwe functionaliteit en andere dagelijkse werkzaamheden. Hierdoor ontstaat het risico dat de resultaten van de scan (te) lang blijven liggen.

De DNS naamgeving van onze servers bestaat uit een letter/nummer combinatie. Daarnaast staat er in de CMDB ook een korte beschrijving, maar deze kan standaard jammer genoeg niet ingelezen worden. Voor de beheerders is het vaak lastig om enkel aan deze server-ID vast te stellen om welk type server het gaat. Wij hebben er daarom voor gekozen om via een API van Nexpose deze aanvullende gegevens uit onze CMDB in te lezen. Voor het ontwikkelen en testen van deze interface is een aparte Nexpose omgeving nodig. Hierbij dienen vooraf heldere afspraken gemaakt te worden over het licentiegebruik.

De initieel gevonden aantallen gelijke kwetsbaarheden over diverse servers is relatief groot. Er is daarom besloten om de gevonden kwetsbaarheden niet automatisch om te zetten in tickets van ons eigen service management system (dit zou kunnen via e-mail of XML). Ook is er voor gekozen om niet het ticketsysteem binnen Nexpose te gebruiken. Dit zou tot verwarring kunnen leiden bij de beheerders. Bevindingen uit Nexpose worden via het standaard changeproces verder afgewikkeld. De beheerder van de server is verantwoordelijk om gevonden kwetsbaarheden te analyseren en corrigerende maatregelen te initiëren.

Het bleek jammer genoeg, dat het scannen van virtual appliances binnen onze Citrix omgeving niet mogelijk is. Tevens bleek door een bug het juist scannen van Microsoft SharePoint omgevingen voorlopig niet mogelijk te zijn. Ernstige tekortkomingen van Nexpose.

Wat heel handig is binnen Nexpose is de mogelijkheid om tijdsgebonden ontheffingen te registreren. Kwetsbaarheden die om specifieke redenen niet van toepassing zijn of later opgepakt worden, kunnen zodoende tijdelijk verwijderd worden uit de rapportages. Goedkeuring van de door de beheerders aangevraagde ontheffingen gebeurt centraal door de security manager.

Het blijkt binnen Nexpose niet mogelijk te zijn om op een webserver alle aanwezige websites automatisch te detecteren en af te scannen. Een IP-adres kan verbonden zijn aan meerdere hostnames en verder bemoeilijken loadbalancers en reverse proxy ook detectie. Enige oplossing is om alle relevante URL's en IP-adressen uit de CMDB of andere bron in te voeren in Nexpose. Een optie is ook om de gegevens via een aparte crawler tool te verzamelen. Doordat bij ons de CMDB op dit punt niet compleet is, worden wij gedwongen om onze interne en externe DNS-gegevens uit te lezen en om te zetten. Commerciële partijen zullen waarschijnlijk scherper hebben welke externe websites ze hosten maar binnen een academische omgeving bestaan er eenvoudig weg te veel sites. Aan de andere kant is het ook voor ons cruciaal om grip te krijgen op deze sites en verouderde omgevingen te upgraden, dan wel af te sluiten. Mogelijk biedt Metasploit meer functionaliteit dan Nexpose ten aanzien van web applicatie scanning.

Takeaways

- Meten is weten; begin met scannen op kwetsbaarheden
- Wees niet verbaasd en word niet ontmoedigd als veel tot heel veel kwetsbaarheden gevonden worden
- Prioriteer, maak keuzes en begin met de belangrijkste kwetsbaarheden
- Besteed veel aandacht aan de manier van presenteren; goede overzichtelijke rapporten zijn cruciaal
- Zorg dat verantwoordelijkheden ten aanzien van het verhelpen van kwetsbaarheden helder zijn over de hele software-stack heen
- Realiseer je dat je nooit klaar bent

Resultaten

Inmiddels draait Rapid7 tooling bijna een jaar en is het een goed moment om terug te kijken naar de gemaakte keuzes en ervaringen.

Bij het scannen worden initieel substantiële hoeveelheden kwetsbaarheden gevonden. Deze variëren van urgente tot minder belangrijke aandachtspunten. Indien men de kwetsbaarheden optelt per server ontstaan er enorme aantallen. Doordat ergens bijvoorbeeld een update mist die meerdere bugs verhelpt, kunnen er veel kwetsbaarheden ontstaan. Voor een drukke beheerder werken de grote aantallen kwetsbaarheden afschrikkend. De beheerder wil weten wat er moet gebeuren en is niet zo zeer geïnteresseerd hoeveel kwetsbaarheden dat oplost. De insteek bij Nexpose, maar waarschijnlijk ook bij andere tools, is echter enkel kwetsbaarheden en niet zozeer een overzicht van oorzaken en te ondernemen acties. Het is dus belangrijk om passende rapporten te maken voor de beheerders.

Bij het scannen van onze servers werden relatief veel verouderde "client"-software (denk aan Adobe reader, diverse browsers, Java) op servers gevonden. Dit gaat tegen ons beleid in. Deze software dient verwijderd te worden of in uitzonderingsgevallen, indien nodig voor het functioneren van de server, geüpdate te worden.

Het aanpassen van bestaande standaard rapporten dan wel het maken van nieuwe passende rapporten is best lastig. Het is echter wel cruciaal voor de bruikbaarheid voor en draagvlak bij de beheerders. En de wensen zijn verschillend; de ene beheerder wil het zo en de ander zo. Denk ook goed na welke rapporten er voor het management gemaakt dienen te worden. Nexpose biedt hierin echter veel mogelijkheden. Wees er alert op dat overzichtsrapporten door bijvoorbeeld teamcoördinatoren ook geïnterpreteerd kunnen worden als een soort controlerapporten van hun werkwijze. Dit kan weerstand opleveren.

Het is verstandig om productieverstoringen te vermijden om in principe eerst de OTA-omgeving en pas naderhand de productieomgeving te scannen. Wij scanden na het uitkomen van de Heartbleed kwetsbaarheid direct alle servers. Maar door een bug in de meest recente update van de engine werden echter veel van onze servers onbereikbaar. Dit leverde veel extra werk op en zorgde voor de nodige kritiek op Nexpose.

Maak een onderscheid in specifieke kwetsbaarheden die een individuele beheerder kan oppakken en anderzijds in meer generieke kwetsbaarheden. Denk bij deze laatste categorie aan zaken als de generieke instellingen van de TLS/SSL versie,

self-signed certificates, SMB configuratie of het gebruik van verouderde ciphers. Doordat de impact op de hele omgeving bij aanpassing groot en complex is, dienen dit soort zaken als project opgepakt te worden. Deze bevindingen kunnen wel gebruikt worden om de huidige dan wel toekomstige (bijvoorbeeld server 2012) configuratie template van een standaard managed server verder aan te scherpen.

Doordat de applicatiebeheerders bij de Wageningen UR per domein/kolom (verticaal) en de systeembeheerders per OS (Linux/Windows) (horizontaal) zijn ingedeeld, is het belangrijk om te bepalen wie welke kwetsbaarheid oppakt. In vele gevallen is het helder, maar zeker bij overlappende zaken dient er helderheid van verantwoordelijkheden te zijn. Als voorbeeld hier het punt dat Apache Tomcat op Linux machines normaal gesproken automatisch meeloopt met de updates, maar dat er ook installaties zijn op Windows machines waarbij dat niet het geval is.

Diverse softwareleveranciers leveren beperkte of soms geen ondersteuning dan wel willen geen garanties afgeven dat hun applicatie functioneert op een geüpdate versie van het OS of de middleware. Denk hierbij bijvoorbeeld aan nieuwere versies van Java, Tomcat Apache of Oracle. Enkel tegen extra kosten en/of na langere tijd worden de pakketten aangepast. Zeker voor specialistische onderzoek en onderwijs-software van deels kleine leveranciers zorgt dit voor beperkingen om tijdig te kunnen upgraden en zodoende kwetsbaarheden te verhelpen.

Binnen Metasploit Pro is er de mogelijkheid om (nep-)phishing e-mail campagnes te simuleren. Het inrichten van zo'n campagne werkt handig en geeft heldere overzichten of de ontvangers de mail ontvangen hebben, op de link geklikt hebben en of ze inderdaad een wachtwoord ingevuld hebben. De tool is ook in staat om eenvoudig bijvoorbeeld een bedrijfsspecifieke OWA (Outlook Web Access) site te klonen. Naar de kopie site kan dan verwezen worden in de nep-phishing mail. Wageningen UR heeft rond de 5000 nep-phishing mails verstuurd. Hiervan gaven een substantieel aantal ontvangers daadwerkelijk ook hun wachtwoord af. Dit was hoger dan verwacht en zorgde ervoor dat er een bewustwordingscampagne gestart is voor eindgebruikers. Phishing mails zijn iets waarvan managers en beslissers de impact makkelijk snappen. Zodoende lukt het om informatiebeveiliging hoger op de agenda te krijgen.

onderscheidt kwetsbaarheden die een individuele beheerder kan oppakken van de generieke

Het verdere gebruik van Metasploit is bij Wageningen UR nog relatief beperkt en wij zouden waarschijnlijk grotendeels ook uit de voeten kunnen met de community versie. De integratie met Nexpose is slechts beperkt en levert nog weinig meerwaarde.

Op basis van de opgedane ervaring en kaders dienen de security eisen helder en formeel vastgelegd te worden in een vulnerability management policy. Hierin dienen zaken te zijn opgenomen als periodiciteit, vorm van scannen, omgang met uitzonderingen en ontheffingen, opvolging van bevindingen et cetera.

Conclusies

Wees niet te ambitieus en realiseer je dat voor de beheerder kwetsbaarheden extra werk betekent. Er ontstaat daarom initieel weerstand en de roep om veel extra menskracht. Maar wees realistisch en probeer te focussen op de meest belangrijke kwetsbaarheden en stapje voor stapje verder te komen. Verschillen tussen beheerders over de belangrijkheid en invulling van veilige servers komen ook aan het licht. Voor de ene beheerder is functionaliteit en tevreden gebruikers belangrijker dan security, en vice versa. Gebruik van een kwetsbaarheden tool zorgt dus ook voor het vergroten van de bewustwording bij beheerders. Blijf herhalen en uitleggen; het duurt enige tijd voordat beheerders de resultaten uit de scantool systematisch gaan gebruiken. De tool is enkel een hulpmiddel; de beheerders en een bijbehorend proces moeten het verschil gaan maken.

- **gebruik tool is lastiger dan gedacht**
- **problemen doken op waarover niet van te voren nagedacht**
- **meer ook een proces met mensen**
- **extra werk levert weerstand op**
- **last van beperkingen tool en support**
- **meer aandacht en draagvlak uiteindelijk voor security**
- **mogelijkheid om snel te kunnen scannen op specifieke kwetsbaarheden**

Links

[1] SANS Critical Security Controls for Effective Cyber Defense: http://www.sans.org/critical-security-controls