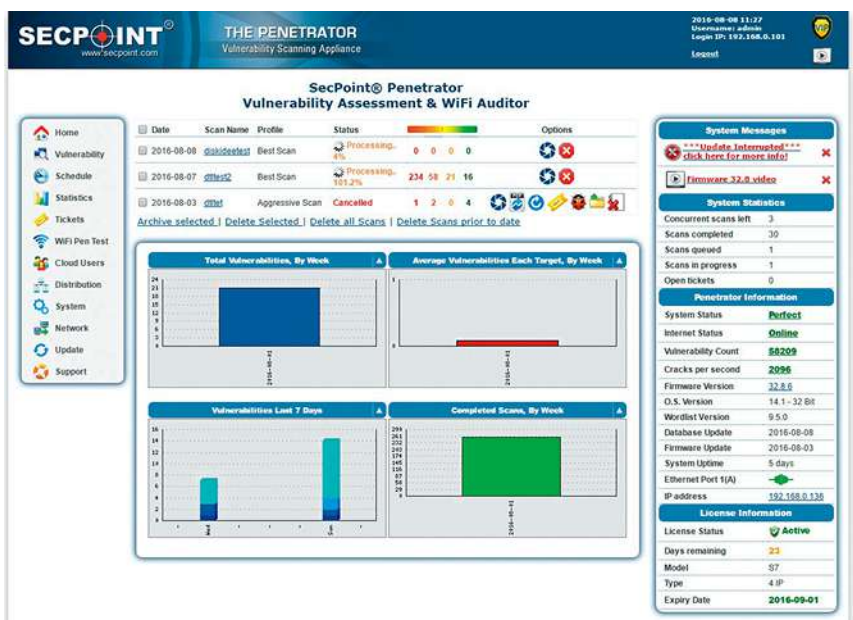
Kwetsbaarheden automatisch opsporen

Secpoint Penetrator spoort automatisch meer dan 58.000 gekende it-kwetsbaarheden op in ip-netwerken, webservers en wifinetwerken. Met de ingebouwde 'exploit'-optie kan u met een minimum aan basiskennis van it-beveiliging de hacker in uzelf loslaten. **Jozef Schildermans**

Het Deense softwarebedrijf Secpoint is sinds 1999 gespecialiseerd in de beveiliging van informaticasystemen. In het verleden testten we van dit bedrijf al de Protector, een utm firewall appliance (zie online testarchief). De Secpoint Penetrator doet, zoals ook uit de naam blijkt, net het omgekeerde: kwetsbaarheden opsporen, testen, beoordelen en, als u dat wilt, actief exploiteren. Iedereen met een basiskennis van informatica en netwerken kan de Penetrator gebruiken. Dit product kan u nog het best bekijken als een geautomatiseerd expertsysteem voor it-beveiliging met een database van meer dan 58.000 kwetsbaarheden. Secpoint vult die database overigens constant aan met nieuwe kwetsbaarheden.



VIRTUELE APPLIANCE

De eerste versies van de Penetrator werden uitsluitend als fysieke toestellen verkocht, maar u kan het product tegenwoordig ook aanschaffen in de vorm van een goedkopere virtual appliance die u op zowat elke computer kan draaien in een van de bekende virtualisatie-omgevingen. Wij testten een 4-ipversie van de virtuele appliance. Daarmee konden we vier ip-adressen gelijktijdig scannen. De adressen zelf kan u zo vaak aanpassen als u wil. Uiteraard is het niet de bedoeling en evenmin is het wettelijk om zonder toestemming niet-lokale ip-adressen te scannen. Secpoint wijst daar ook uitdrukkelijk op in zijn documentatie. Zorg eerst altijd voor schriftelijke toestemming.

De virtuele appliance kan - mits u daarvoor betaalt - maximaal 32 ip-adressen gelijktijdig scannen, op voorwaarde dat de gebruikte hardware hiervoor voldoende krachtig is. Wilt u méér gelijktijdige scans uitvoeren dan heeft u daar één van de duurdere fysieke Penetrator-appliances voor nodig. Secpoint verkoopt verder twee goedkopere versies met beperkte functies, eentje voor het scannen van wifinetwerken (Portable Penetrator) en een tweede voor het scannen van webservers (Cloud Penetrator).

De wifi- en webfuncties zijn sowieso aanwezig in de duurdere standaardversie, maar om wifinetwerken te kunnen scannen hebt u wel nog een externe Alfa awus036h wifi-antenne nodig. Die kan u apart kopen en via usb op uw pc of fysieke appliance aansluiten. Met die antenne is het bijvoorbeeld mogelijk om wep, wpa, wps en wpa2 wifisleutels te "herstellen" (lees: kraken). Deze functies hebben wij door het ontbreken van de antenne niet kunnen testen.

INSTALLATIE EN SUPPORT

Secpoint heeft op zijn website uitgebreide documentatie, compleet met video-tutorials. We slaagden er moeiteloos in het product te installeren en op te starten. De licentie wordt via het internet geactiveerd bij een server van Secpoint. Daar liep het bij ons mis. Hoewel de virtuele appliance aangaf een verbinding met het internet te kunnen maken en wij er ook in slaagden om vanaf een andere computer in een webbrowser de beheerinterface op te roepen, lukte het activeren van de licentie niet.

De Engelstalige supportafdeling van Secpoint hielp ons via e-mail vlot verder, maar zelfs dat verhielp het probleem niet.

De virtuele appliance wordt geleverd met TeamViewer. Nadat we de supportafdeling toegang hadden verleend tot onze appliance, was het probleem via een firmware-update snel verholpen. Voor volledige support voor Windows 10 hebt u namelijk de meest recente Penetrator-firmware nodig.

KWESTBAARHEDEN

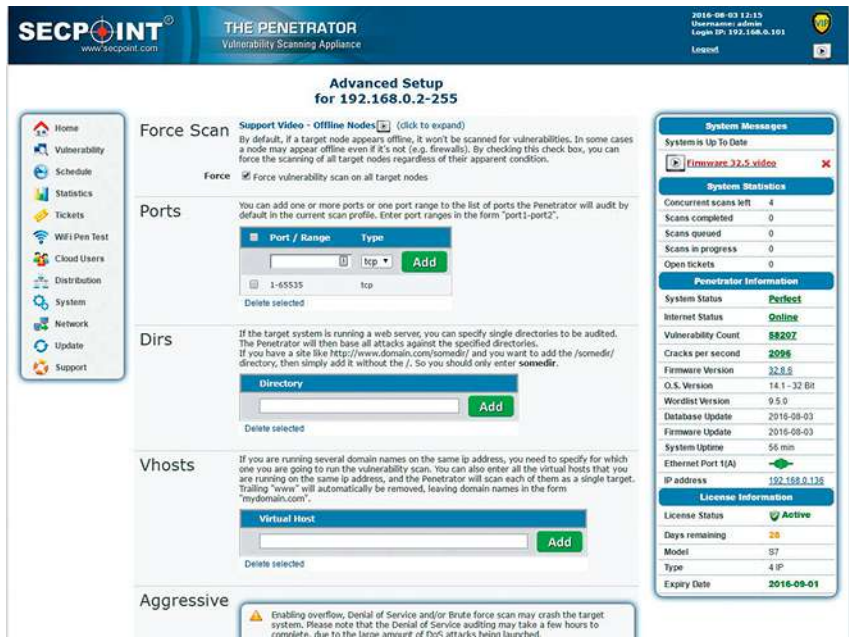
U bedient de Penetrator via een webinterface op de virtuele appliance zelf of via een webbrowser in het lokale netwerk. Het is bovendien mogelijk verschillende gebruikers met specifieke rechten toe te laten. In ingewikkeldere netwerkconfiguraties kan u verder een netwerk van 'master' en 'client' penetrators uitrollen. Het belangrijkste menu heet toepasselijk 'Vulnerability' en hier start u een kwetsbaarheid-scan op. Bij elke stap vindt u in de beheerinterface een videotutorial die u op weg helpt, maar eigenlijk wijst het zichzelf uit. U geeft uw scan een naam en een ip-adres of -bereik. U kan ook ip-adressen uit een csv-bestand importeren.

Daarna kiest u het type scan, bijvoorbeeld alleen 'populaire' poorten, alleen vaak gebruikte poorten, alle poorten, een 'stealth' scan, 'hipaa policy scan' voor compliance of een agressieve scan. Al deze scans simuleren het gedrag van een menselijke hacker en leggen de gescande services dus niet plat. Bij elk type scan kan u meer informatie bekijken door met de muis over het blauwe vraagteken ernaast te zweven.

Een scan kan uren of zelfs dagen duren, afhankelijk van het type en de hoeveelheid adressen. Wel kan u altijd de al gevonden kwetsbaarheden openen door op het blauwe wieltje ernaast te klikken. Als de scan afgelopen is, verschijnen er meer pictogrammen, bijvoorbeeld om rapporten te creëren, valse positieven aan te duiden, de scan te herhalen of tickets te creëren die u via e-mail uitstuurt en in het systeem opvolgt. Scans kunnen verder gearchiveerd of gewist worden.

RAPPORTERING

Rapporten in pdf, xml of html geeft u zelf vorm, tot en met 'branding' met eigen logo, als u een licentie kocht die dat toelaat. Volledige rapporten, samenvattingen van één pagina en rapporten zonder oplossingen zijn na afloop van de scan kant-en-klaar beschikbaar in het systeem, ook in het Frans of het Nederlands, wat bij vergelijkbare producten zelden het geval is.



Elke gevonden kwetsbaarheid krijgt bovendien een kleurcode mee: rood voor kritiek, oranje voor hoog, geel voor laag en groen voor informatief. Zowel in de interface als in de rapporten worden de resultaten verder samengevat met behulp van diagrammen. In de gedetailleerde rapporten krijgt u meer uitleg bij elke kwetsbaarheid, samen met tips om ze te verhelpen waar mogelijk. De software geeft er ook Securityfocus.com bugtraq-, CVE Mitre- en Ubuntu Security Notice-links en -id's bij als die beschikbaar zijn.

De uitgebreide rapporten kunnen zéér uitgebreid zijn. Zo besloeg het rapport over één door ons geteste webserver zo maar eventjes 391 bladzijden. Op deze server, die we verder niet zullen identificeren, vond het systeem 238 kritieke, 62 hoge, 23 lage en 16 informatieve kwetsbaarheden! Enkele kritieke kwetsbaarheden bleken na manuele controle valse positieven te zijn, maar de server vertoonde daarnaast vele echte gaten.

U kan scans op gezette tijden volgens een vast schema uitvoeren. Zodra er op een systeem twee of meer scans uitgevoerd zijn, kan u de 'vulnerability history' opvragen en op die manier controleren of in het verleden gevonden kwetsbaarheden effectief opgelost zijn. U zet de verantwoordelijke desgewenst via het ingebouwde ticketingsysteem tot actie aan.

Penetrator kan ook geautomatiseerd proberen in te breken op een systeem. In de appliance gebruikt u daarvoor een aparte applicatie, Exploits Armitage. In onze licentie was die niet geactiveerd, zodat we ze niet konden testen. Het is dan ook een functie voor geavanceerde gebruikers die de ultieme garantie willen dat hun eigen systemen niet exploiteerbaar zijn voor hackers.

CONCLUSIE

Secpoint Penetrator is een briljant preventief en curatief beveiligingsproduct dat in de toolkit van geen enkele netwerkbeheerder mag ontbreken.

Productinfo

PRODUCENT: SECPOINT, WWW.SECPOINT.COM

DISTRIBUTEUR: SECPOINT NEDERLAND, WWW.SECPOINT.NL

PRODUCT: SECPOINT PENETRATOR VULNERABILITY ASSESSMENT & WIFI AUDITOR V32.8

PRIJS: CLOUD PENETRATOR VANAF €129 VOOR 1 IP-ADRES. PORTABLE PENETRATOR VANAF €199 VOOR 1 IP. VERSIE MET 1 IP ZIJN INCLUSIEF EEN ALFA AWUS036 H WIFI-ADAPTER ; DRIE JAAR UPDATES KOST BIJVOORBEELD €349. PENETRATOR S7 VULNERABILITY SCANNER VIRTUELE APPLIANCE VANAF €199 VOOR 1 IP. PENETRATOR S7 FYSIEKE APPLIANCE VANAF €699 VOOR VIER IP'S (APPLIANCES VERKRIJGBAAR TOT UNLIMITED IP'S).