

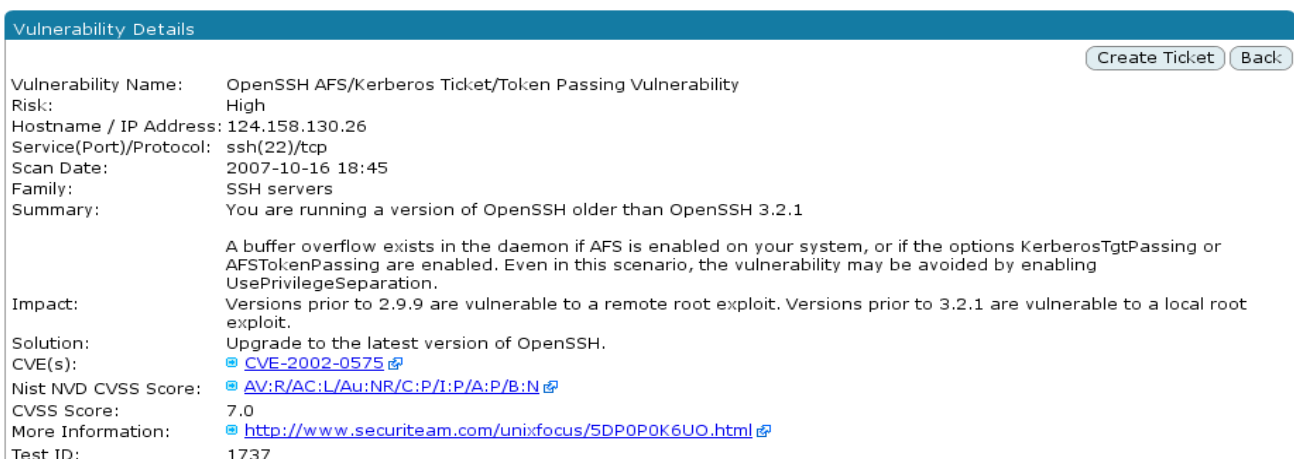
Vulnerability Scanning

Veel organisaties kennen niet of nauwelijks de status van de kwetsbaarheid in componenten en applicaties binnen hun netwerkomgevingen. Dit geldt zowel voor netwerken die in eigen beheer zijn als die uitbesteed worden. De kwetsbaarheid en het beveiligingsniveau zijn veelal onbekend. Het zijn echter juist de kwetsbaarheden die misbruikt worden door malware en hackers. Hierdoor vormen deze een direct risico voor de integriteit van het netwerk. Synchron aan anti-malware oplossingen worden dagelijks nieuwe kwetsbaarheden gevonden in netwerkcomponenten. De vulnerability database wordt met deze informatie gevuld. Door deze kwetsbaarheden te detecteren en te verhelpen neemt een organisatie een belangrijke stap in de bescherming van de netwerkonderdelen tegen malware en hackers en daarmee de beschikbaarheid van het netwerk verhogen.

Vulnerability scanners zijn voor dit doel gebouwd. Je kunt een dergelijke scan handmatig laten uitvoeren door een security consultant. Deze handmatige scan geeft een eenmalige 'snapshot' van de status van de netwerkonderdelen.

Daarnaast is het ook mogelijk een volledig geautomatiseerde vulnerability management systeem te implementeren. Daardoor kunnen naar alle vrijheid scans automatisch ingepland worden op basis van bijvoorbeeld service, locatie, datum, afdeling, functiegroep, met verschillende frequenties.

Beide varianten kunnen zowel op externe (firewall, webserver, etc) als interne omgevingen (fileserver, mailserver, intranetserver, etc) uitgevoerd worden. Er worden een rapportage opgeleverd met daarin een overzicht van de relevante kwetsbaarheden gekoppeld aan IP adres en service en er worden concrete aanbevelingen gedaan.

A screenshot of a web interface titled "Vulnerability Details". The page contains the following information:

Vulnerability Name:	OpenSSH AFS/Kerberos Ticket/Token Passing Vulnerability
Risk:	High
Hostname / IP Address:	124.158.130.26
Service(Port)/Protocol:	ssh(22)/tcp
Scan Date:	2007-10-16 18:45
Family:	SSH servers
Summary:	You are running a version of OpenSSH older than OpenSSH 3.2.1
Impact:	A buffer overflow exists in the daemon if AFS is enabled on your system, or if the options KerberosTgtPassing or AFSTokenPassing are enabled. Even in this scenario, the vulnerability may be avoided by enabling UsePrivilegeSeparation. Versions prior to 2.9.9 are vulnerable to a remote root exploit. Versions prior to 3.2.1 are vulnerable to a local root exploit.
Solution:	Upgrade to the latest version of OpenSSH.
CVE(s):	CVE-2002-0575
Nist NVD CVSS Score:	AV:R/AC:L/Au:NR/C:P/I:P/A:P/B:N
CVSS Score:	7.0
More Information:	http://www.securiteam.com/unixfocus/5DP0P0K6UO.html
Test ID:	1737

Buttons for "Create Ticket" and "Back" are visible in the top right corner.

Figuur 1: Voorbeeld gevonden kwetsbaarheid

Vulnerability Assessment

In een vulnerability assessment worden handmatig scans uitgevoerd op ad-hoc basis, door middel van een stand alone sensor en in geval van een intern scan ook een consultant voor de uitvoering en rapportage van de resultaten. Het scannen vindt plaats op basis van IP adressen of ranges. Elk IP adres met een gekoppelde server wordt gescand met behulp van de data uit de vulnerability database. Deze database wordt updated vanuit het Internet, vergelijkbaar met de bekende anti-malware systemen. Eventuele kwetsbaarheden worden geclassificeerd als hoog, midden of laag risico.

Een Vulnerability Assessment levert een 'snapshot' van de situatie. Elke keer dat een scan uitgevoerd is, wordt het resultaat echter niet automatisch gerelateerd aan de resultaten van een vorige scan. De frequentie van deze scans en het opvolgen van de aanbevelingen bepaalt uiteindelijk de kracht van deze dienst.

Automatisch Vulnerability Management

In de geautomatiseerde versie wordt wel gebruik het differentiatie verschil met eerdere scans aangetoond. Er wordt met trendanalyses de verbetering (of verslechtering) per afdeling/lokatie/functie/servicegroep uitgelicht ten opzichte van het algemene kwetsbaarheidniveau.



Figuur 2: Screenshots van verschillende grafieken met vulnerabilites en trendanalyse

In een geautomatiseerde omgeving wordt gebruik gemaakt van één of meerdere sensoren en een centraal management platform. Het platform is gekoppeld aan het Internet voor de updates van de vulnerability database. Deze database en scan opdrachten worden door het platform aan de sensor(en) doorgegeven. De resultaten worden verzameld en verwerkt in rapportages. In een gedistribueerde WAN netwerk omgeving kunnen meerdere sensoren gebruikt worden, waarbij WAN vertragingen en firewall kwesties vermeden worden.

De rapporten in het management platform zijn interactief en door op verschillende lijnen en punten te klikken, kan de gebruiker direct inzoomen op informatiedetails. Toegangsrechten zijn aanpasbaar aan de gebruikersrollen en aangetoonde kwetsbaarheden kunnen toegekend worden aan individuele IT engineers voor de ticketing en verbetering.

Doordat men direct scans kan activeren of met een hoge frequentie kan laten uitvoeren acteert de oplossing feitelijk als een 'virtuele hacker'. Daarmee verdwijnt de noodzaak voor het inhuren van externe consultants voor kostbare hacking en penetratie activiteiten.

vulnerability Scan Summary Results								
Location	Total	High	Medium	Low	Score	Trend	Report	Compliant
Beyond Security HQ	10117 (9824)	315 (309)	2745 (2686)	7057 (6829)	91.60 (96.79)	▼ 5.19		<input type="checkbox"/>
Multi Country DMZ	54 (0)	2 (0)	10 (0)	42 (0)	92.87 (100.00)	▼ 7.13		<input type="checkbox"/>
Beyond Security Asia	9184 (8933)	287 (282)	2603 (2557)	6294 (6094)	91.03 (98.00)	▼ 6.97		<input type="checkbox"/>
Multi Country DMZ #2	183 (0)	0 (0)	21 (0)	162 (0)	98.42 (100.00)	▼ 1.58		<input type="checkbox"/>
Beyond Security IL	9001 (8933)	287 (282)	2582 (2557)	6132 (6094)	83.64 (96.00)	▼ 12.36		<input type="checkbox"/>
Israel Test Scan	19 (0)	0 (0)	4 (0)	15 (0)	81.45 (100.00)	▼ 18.55		<input type="checkbox"/>
Beyond Security DEV	21 (7)	0 (0)	1 (0)	20 (7)	97.52 (100.00)	▼ 2.48		<input type="checkbox"/>
IL Batch 1	7 (7)	0 (0)	0 (0)	7 (7)	100.00 (100.00)	0.00		<input checked="" type="checkbox"/>
Internal Scan	14 (0)	0 (0)	1 (0)	13 (0)	95.04 (100.00)	▼ 4.96		<input type="checkbox"/>
Beyond Security Sales	22 (22)	3 (3)	4 (4)	15 (15)	99.40 (99.34)	▲ 0.06		<input type="checkbox"/>
IL Batch 2	22 (22)	3 (3)	4 (4)	15 (15)	99.40 (99.34)	▲ 0.06		<input type="checkbox"/>
Ramat Hayal	8939 (8904)	284 (279)	2573 (2553)	6082 (6072)	56.17 (84.67)	▼ 28.50		<input type="checkbox"/>
C6 Server Farm	8667 (8904)	249 (279)	2509 (2553)	5909 (6072)	55.16 (53.96)	▲ 1.20		<input type="checkbox"/>
TLV DMZ	244 (0)	34 (0)	59 (0)	151 (0)	58.81 (100.00)	▼ 41.19		<input type="checkbox"/>
Internal Scan	28 (0)	1 (0)	5 (0)	22 (0)	54.55 (100.00)	▼ 45.45		<input type="checkbox"/>
Beyond Security Europe	19 (8)	0 (0)	7 (2)	12 (6)	78.33 (93.70)	▼ 15.37		<input type="checkbox"/>
Know-Market	9 (0)	0 (0)	3 (0)	6 (0)	72.93 (100.00)			<input type="checkbox"/>
Smart-Forward test	8 (8)	0 (0)	2 (2)	6 (6)	81.03 (81.03)	0.00		<input type="checkbox"/>
mario	2 (0)	0 (0)	2 (0)	0 (0)	81.03 (100.00)			<input type="checkbox"/>
Beyond Security NA	819 (856)	26 (27)	120 (124)	673 (705)	92.82 (92.40)	▲ 0.42		<input type="checkbox"/>
Beyond Security McLean	604 (578)	23 (23)	99 (91)	482 (464)	89.56 (89.68)	▼ 0.12		<input type="checkbox"/>

Figuur 3: Screenshots van systeem 'downdrill', en trendanalyse