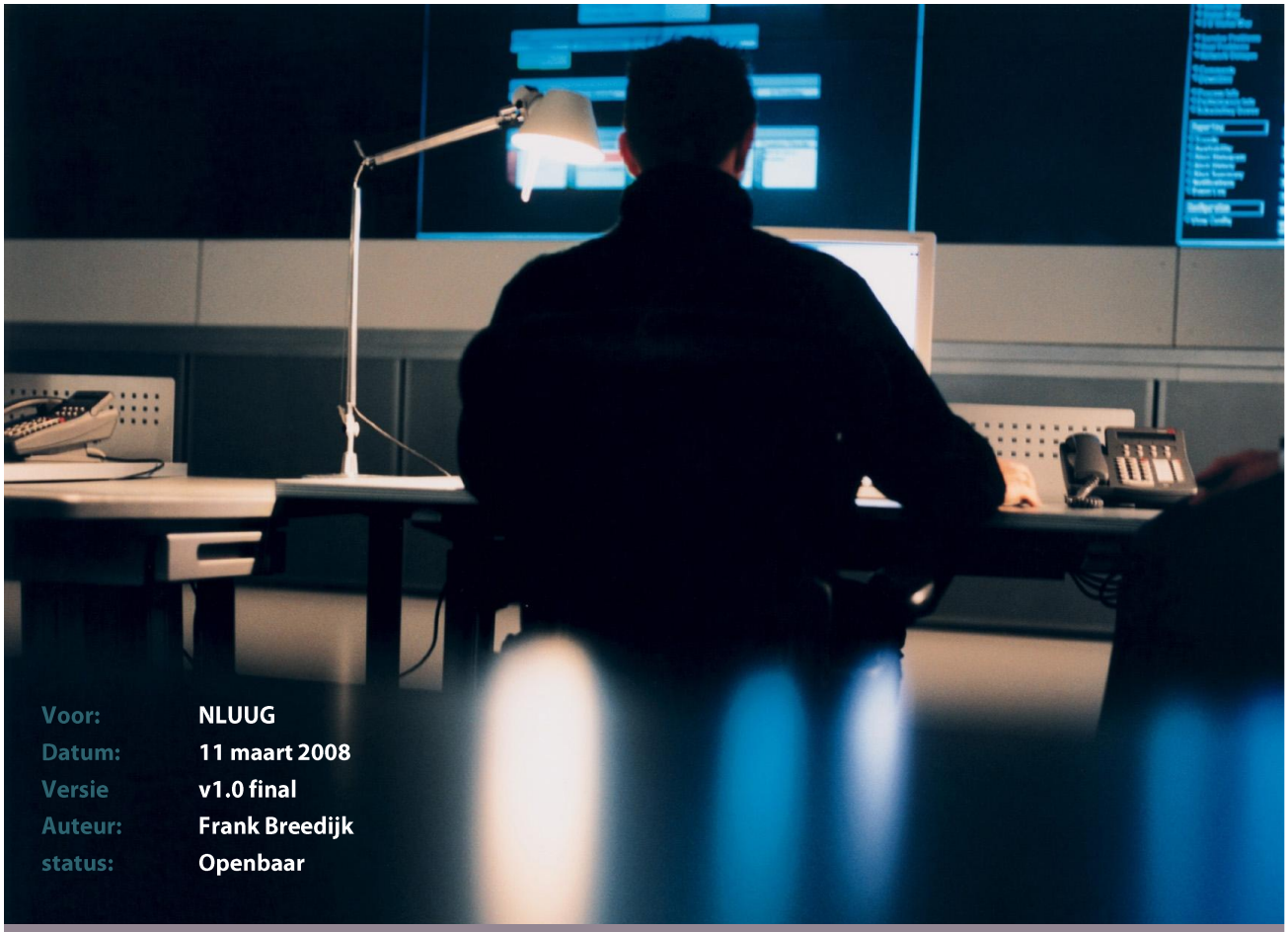
SCHUBERG PHILIS

AutoNessus

Geautomatiseerde Nessus scans met delta rapportage



Voor:	NLUUG
Datum:	11 maart 2008
Versie	v1.0 final
Auteur:	Frank Breedijk
status:	Openbaar

Schuberg Philis BV
Star Parc,Boeing Avenue 271
1119 PD Schiphol-Rijk
T +31 20 750 65 00
F +31 20 750 65 50
The Netherlands
www.schubergphilis.com

MISSION CRITICAL OUTSOURCING

Inhoudsopgave

1 Wat is het probleem?

Iedereen die wel eens met de, eens open source, vulnerability scanner Nessus heeft gewerkt, kent het probleem…. Nessus is een waardevolle tool, maar helaas ook één die de gebruiker overlaadt met, niet altijd even relevante, data. De tijd die nodig is voor het uitwerken van één enkele scan is vaak het drievoudige van de scantijd zelf.

Als Security Engineer voor Schuberg Philis is de auteur verantwoordelijk voor onder andere het uitvoeren van security audits op de infrastructuren van de klanten van zijn werkgever, Schuberg Philis, hiervoor gebruikt hij onder andere Nessus. Nessus is een van de meest bekende security audit tools en de open source versie 2 en de laatste commerciële versie 3 zijn vrij verkrijgbaar.

Het voordeel van Nessus is dat het een grote hoeveelheid plug-in's bevat die een enorme hoeveelheid informatie naar boven halen, het nadeel is dat het een grote hoeveelheid plug-in's bevat die een enorme hoeveelheid informatie naar boven halen. Een simpele scan van een website (zoals te zien is in Appendix A, Voorbeeld Nessus rapport) bevat al snel tussen de 10 en 20 findings. Deze findings zijn, zeker als hetzelfde netwerk meerdere malen wordt gescand, niet altijd even relevant. Bij het uitvoeren van audits begon de auteur zich dan ook te ergeren aan het controleren van, en dus steeds weer tijd besteden aan, steeds dezelfde niet relevante bevindingen.

Als Schuberg Philis de wens externe adressen van haar klanten regelmatig te auditen, wilde waarmaken, dan moest er iets veranderen.

2 De ontstaansgeschiedenis van AutoNessus

Zoals hierboven beschreven, had Schuberg Philis de wens om de kwaliteit van haar dienstverlening te verbeteren door de externe IP adressen van al haar klanten te scannen. Daarnaast leeft onder haar engineers het credo: "Eenvoudig en repeterend werk moet je automatiseren". Dit heeft uiteindelijk geleid tot de huidige versie van AutoNessus, maar hoe is het zover gekomen?

2.1 De basis (oftewel versie 0.1)

De eerste versie van AutoNessus was niet veel meer dan een shell script welke via de crontab aangeroepen werd om een serie IP adressen te scannen en een simpele web interface om de resultaten van de scans in HTML en NBE formaat te downloaden.

2.2 Betere HTML rapportage (versie 0.2)

De gebieden voor eerste verbeteringen waren duidelijk: een betere en beter doorzoekbare rapportage dan de standaard Nessus rapportage. Daarnaast was het wenselijk de geschiedenis van diverse findings te kunnen zien.
Om dit te bereiken was het noodzakelijk het standaard NBE formaat op te splitsen in een boomstructuur bestaande uit: host/plug-in/ timestamp.

2.3 Delta rapportage (versie 0.3)

Doordat de informatie nu beschikbaar is in een boomstructuur is delta rapportage in principe mogelijk. Om goede delta's te kunnen maken werd er een status aan iedere finding toegevoegd:

- New – De finding is voor het eerst aangetroffen op dit IP adres;

- Open – De finding is opnieuw aangetroffen;
- No issue – De finding is geen echt security probleem en wordt genegeerd tot hij wijzigt;
- Hard Masked – De finding wordt altijd genegeerd.

Aangezien een aantal findings timestamps in hun output hebben was ook een ignore-diff bestand nodig met daarin regular expressions van de te negeren patronen.

2.4 De eerste grote bug (versie 0.4)

De combinatie host/plug-in bleek niet uniek te zijn, een plug-in kan op meerdere poorten tegelijk voorkomen. AutoNessus werd omgebouwd zodat hij werkt met een host/port/plug-in /timestamp boom.

2.5 Het eerste verzoek voor nieuwe features (versie 0.5)

Omdat AutoNessus nu wordt gebruikt voor een pilot klant en voor de privé machines van Schuberg Philis medewerkers, kwamen ook de eerste verbetervoorstel binnen. “Is er geen mogelijkheid om groepen findings in een keer te bewerken?” “Is het daarnaast mogelijk bepaalde findings standaard van commentaar te voorzien?” “Kun je een hosts file inlezen?”
Een nieuwe GUI, op basis van AJAX en de autoremark configuratie file waren nodig om deze wensen te realiseren.

2.6 Release (versie1.0)

De release van Autonessus is gepland op 15 mei 2008 tijdens de NLUUG .....

3 De stand van zaken

Hoe ziet AutoNessus er op dit moment uit? Welke features heeft het? Wat doet het, wat kan het?

3.1 ‘Two Tier’ architectuur

De AutoNessus architectuur bestaat uit twee lagen:

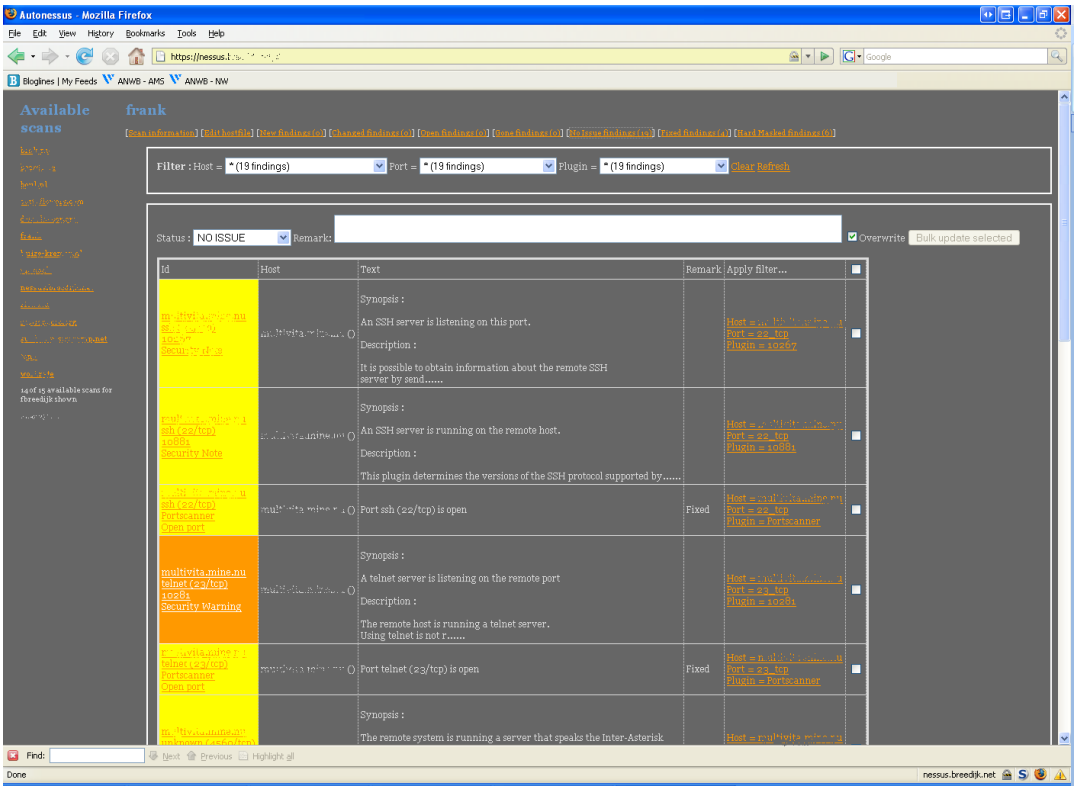
- De scanning laag, deze bestaat uit een installatie van de Nessus deamon op een machine;
- De applicatie laag, hier vind de aansturing van de scanners, het bereken van de delta’s en het presenteren van de resultaten plaats.

Het is mogelijk de scanning tier en de applicatie tier op een machine te installeren, maar je zou ook vanuit een applicatie tier meerdere scanning machines aan kunnen sturen, bijvoorbeeld een scanner in de DMZ en een scanner in de applicatie tier van een infrastructuur.

3.2 Web GUI

De web interface van AutoNessus kan worden gebruikt voor de meest voorkomende taken:

- Aanpassen van de status van findings;
- Aanpassen van opmerkingen bij de status;
- Aanpassen van de hosts file;
- ‘Bulk update’ scherm voor het aanpassen van meerdere findings in een keer;
- Dynamische filters op basis van host/netwerk, poort en/of plug-in;
- Ophalen van rapporten in verschillende formaten.



3.3 Verschillende status codes

AutoNessus kent zeven statussen met ieder hun eigen betekenis:

- ‘New’ – Voor het eerst aangetroffen finding;
- ‘Changed’ – Een finding die ooit veranderd is of na Gone of Fixed weer aangetroffen. Deze status blijft tot hij handmatig wordt aangepast of de finding verdwijnt;
- ‘Open’ – De finding is vaker aangetroffen maar niet gewijzigd;
- ‘Gone’ – De finding is niet meer aangetroffen;
- ‘No Issue’ – De finding is niet van belang en blijft No Issue tot hij wijzigt (en dus CHANGED wordt);
- ‘Fixed’ – De finding is opgelost en zou niet meer terug moeten komen;
- ‘Hard Masked’ – De gebruiker heeft ervoor gekozen de finding nooit meer te zien.

3.4 Eigen hosts file

AutoNessus heeft, onafhankelijk van DNS, een eigen hosts file per geconfigureerde scan. Via deze file kunnen in de web interface van AutoNessus namen aan IP adressen toegekend worden.

4 Een case, Schuberg Philis

Sinds de zomer van 2007 gebruikt Schuberg Philis AutoNessus voor het regelmatig uitvoeren van vulnerability scans op de infrastructuren van haar klanten. Dit gebeurt tussen de één keer per maand en één keer per twee weken, afhankelijk van de klant.

Voor AutoNessus bleek het niet praktisch om dit soort audits met deze regelmaat uit te voeren.

Voorheen was voor een handmatige audit snel een halve tot een hele dag werk gemoeid. Door gebruik te maken van AutoNessus heeft Schuberg Philis een behoorlijke efficiëntie verbetering bereikt.

De eerste scan van een infrastructuur en het verwerken daarvan duurt vaak nog anderhalf tot twee uur, afhankelijk van de grootte van de infrastructuur, maar het verwerken van de resultaten van een vervolgscan kost, zeker als de laatste echte bevindingen opgelost zijn, vaak niet meer dan 30 minuten uitgaande van een /24 netwerk.

Schuberg Philis gebruikt AutoNessus voornamelijk voor interne kwaliteitsborging. Dit betekent dat zij, als standaard onderdeel van haar dienstverlening, een reguliere scan van de externe IP adressen van haar klanten uitvoert en deze informatie gebruikt om de beveiliging van deze infrastructuren op het benodigde niveau te houden.

Het audit gedeelte van het vulnerability management proces van Schuberg Philis ziet er als volgt uit.
In overleg met de klant en het klantenteam wordt besloten waanneer de eerste scan wordt uitgevoerd.
De Security Engineer plant de scan in AutoNessus in.
Als de scan start, wordt via de 'prescan hook' in AutoNessus een waarschuwing naar het monitoring systeem gestuurd, dit om de engineers te waarschuwen dat er een scan in opkomst is.
Na de scan wordt via de 'postscan hook' een recovery message naar het monitoring systeem gestuurd.
De samenvatting van de scan wordt naar de engineers gemaild. De eerst volgende werkdag bekijkt de Security Engineer de findings en schrijft een kort rapport voor zijn collega's waarin de bevindingen logisch gegroepeerd staan.
De Security Engineer en de teamleider maken samen met de klant afspraken over hoe de findings worden opgelost.
De Customer Operations Manager rapporteert over de voortgang via de maandelijkse service rapportage.
Deze cyclus wordt elke maand herhaald.

5 De toekomst

Door AutoNessus als open source te releasen, wordt de toekomst van het programma in de handen van de open source gemeenschap gelegd. Open source maken is voor Schuberg Philis geen sterfhuis constructie, binnen Schuberg Philis is en blijft AutoNessus een belangrijke tool. Schuberg Philis zal de tool dan ook nog verder ontwikkelen en de ontwikkeling door derden blijven volgen en steunen.

In ieder geval staan er nog een aantal punten open:

- Verbetering van de GUI;
- Het uitbreiden van de GUI zodat alle aspecten van de tool via de GUI beheerd kunnen worden;
- Het vervangen van de flat file 'database' door een echte, relationele, database.

6 Meer informatie?

Meer informatie is te vinden op http://www.AutoNessus.com. Hier is vanaf 15 mei een download link te vinden.

Appendix A Voorbeeld Nessus rapport

Network Vulnerability Assessment Report

05.02.2008

Sorted by host names

Session name: www.**********.com	**Start Time:** 05.02.2008 14:32:32
	Finish Time: 05.02.2008 14:49:12
	Elapsed: 0 day(s) 00:16:39

Total records generated:	12
high severity:	0
Medium severity:	1
informational:	11

www.**********.com

Service	Severity	Description
http (80/tcp)	**Info**	Port is open
http (80/tcp)	**Medium**	Synopsis : This web server leaks a private IP address through its HTTP headers. Description : This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. There is a known issue with IIS 4.0 doing this in its default configuration. See also : http://support.microsoft.com/support/kb/articles/Q218/1/80.ASP See the Bugtraq reference for a full discussion. Risk factor : Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) Plugin output : This web server leaks the following private IP address : 123.123.123.123 CVE : CVE-2000-0649 BID : 1499
http (80/tcp)	**Info**	Synopsis : A web server is running on the remote host. Description : This plugin attempts to determine the type and the version of the remote web server. Risk factor : None

		Plugin output : The remote web server type is : Microsoft-IIS/6.0
http (80/tcp)	**Info**	The following Acrobat files (.pdf) are available on the remote server : /downloads/route.pdf /downloads/ advertentie%20Technology%20Office%20Co-ordinator.pdf /downloads/Corporate%20Story.pdf /downloads/Annual%20Report%202006.pdf You should make sure that none of these files contain confidential or otherwise sensitive information. An attacker may use these files to gain a more intimate knowledge of your organization and eventually use them do perform social engineering attacks (abusing the trust of the personnel of your company). Solution : sensitive files should not be accessible by everyone, but only by authenticated users.
http (80/tcp)	**Info**	The remote host appears to be running a version of IIS which allows remote users to determine which authentication schemes are required for confidential webpages. Specifically, the following methods are enabled on the remote webserver: - IIS NTLM authentication is enabled Solution : None at this time Risk factor : Low CVE : CVE-2002-0419 BID : 4235
general/udp	**Info**	For your information, here is the traceroute from 62.93.230.13 to 127.0.0.1 : 62.93.230.13 62.4.95.97 64.125.26.70
general/tcp	**Info**	127.0.0.1 resolves as www.**********.com.
http (80/tcp)	**Info**	Synopsis : Some information about the remote HTTP configuration can be extracted. Description : This test gives some information about the remote HTTP protocol – the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem Solution : None. Risk factor : None Plugin output : Protocol version : HTTP/1.1 SSL : no Pipelining : yes Keep-Alive : no

		Headers : Set-Cookie: ARPT=WMMVYUS10.200.1.136CKMOJ path=/ Content-Length: 4209 Content-Type: text/html Content-Location: http://www.**********.com/index.html Last-Modified: Tue, 27 Nov 2007 09:30:21 GMT Accept-Ranges: bytes ETag: "34795421d830c81:6e7" Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Date: Tue, 05 Feb 2008 13:36:38 GMT
http (80/tcp)	**Info**	Synopsis : The remote web server contains a 'robots.txt' file. Description : The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks. See also : http://www.robotstxt.org/wc/exclusion.html Solution : Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material. Risk factor : None Contents of robots.txt : # /robots.txt for www.**********.com #---------- # Monday 15 October 2007 18:00 GMT+1, Schuberg Philis BV # # MISSION CRITICAL # OUTSOURCING # #---------- # A nice catch-all for our friendly bots User-agent: * # no need to gather info from the style sheet Disallow: /styles.css # and there's nothing useful in our images dir either Disallow: /images Other references : OSVDB:238

http (80/tcp)	**Info**	Synopsis : It is possible to enumerate web directories. Description : This plugin attempts to determine the presence of various common dirs on the remote web server. Risk factor : None Plugin output : The following directories were discovered: /News, /customers, /downloads, /images, /scripts, /style While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards Other references : OWASP:OWASP-CM-006
http (80/tcp)	**Info**	Here is the Nikto report: Unknown option: generic --- - Nikto 2.02/2.03 - cirt.net + Target IP: 127.0.0.1 + Target Hostname: 127.0.0.1 + Target Port: 80 + Virtual Host: www.**********.com + Start Time: 2008-02-06 14:38:10 --- + Server: Microsoft-IIS/6.0 + OSVDB-0: Retrieved X-Powered-By header: ASP.NET + OSVDB-630: IIS may reveal its internal IP in the Content-Location header via a request to the root file. The value is "http://192.168.0.1/index.html". + OSVDB-630: IIS may reveal its internal IP in the Location header via a request to the /images directory. The value is "http://192.168.0.1/images/". - /robots.txt - contains 2 'disallow' entries which should be manually viewed. (GET) + 4347 items checked: 4 item(s) reported on remote host + End Time: 2008-02-06 14:39:48 (98 seconds) --- + 1 host(s) tested
general/tcp	**Info**	Information about this scan : Nessus version : 2.2.9 (Nessus 2.2.10 is available - consider upgrading) Plugin feed version : 200801311935 Type of plugin feed : Registered (7 days delay) Scanner IP : 172.16.0.1 WARNING : no port scanner was enabled during the scan. This may lead to incomplete results Port range : (?) Thorough tests : no Experimental tests : no

		Paranoia level : 1 Report Verbosity : 2 Safe checks : no Optimize the test : yes Max hosts : 4 Max checks : 20 Scan Start Date : 2008/2/5 14:32 Scan duration : 994 sec