DINSDAG 16 JUNI 2009 – DE REEHORST EDE

BLACK HATS SESSION PART VII

GEHACKT?

INCIDENT RESPONSE & IT FORENSICS

MET SPREKERS: WALTER BELGERS - MADISON GURKHA › ROLAND VERGEER - DIGITAL INTELLIGENCE › ARNOUD ENGELFRIET - ICTRECHT › MARNIX KAART EN ERWIN VAN EIJK - NEDERLANDS FORENSISCH INSTITUUT


Walter Belgers


Roland Vergeer


Arnoud Engelfriet


Marnix Kaart


Erwin van Eijk

Deze zevende editie van de welbekende Black Hats sessies wordt georganiseerd door Array Seminars en Madison Gurkha en staat volledig in het teken van Incident Response & IT Forensics.

Ging het programma van de vorige editie in op de duistere en criminele kant van het Hacken: HACKING FOR PROFIT, deze keer gaan we in op gevolgen: GEHACKT! En wat nu?

Het wordt CSI Ede op 16 juni. Walter Belgers van Madison Gurkha zal een presentatie geven over incident response "light". Hoe kunt u eenvoudig incident response onderzoek doen met freeware tools? Roland Vergeer (Digital Intelligence) geeft een mooi voorbeeld uit de praktijk over een forensisch onderzoek naar een interne fraude (die niet intern bleek te zijn), Arnoud Engelfriet (ICTRecht) gaat in op bewijsvoering in een rechtszaak, wat de criteria zijn voor computervredebreuk of denial-of-service en wat er dus nodig is om een aangifte te kunnen doen of een civiele zaak om schadevergoeding te kunnen beginnen. Het Nederlands Forensisch Instituut zal een lezing over forensisch onderzoek geven.

BESTEMD VOOR Ú

De bijeenkomst wordt georganiseerd voor beheerders van systemen, netwerken en applicaties, security officers, interne auditors en andere geïnteresseerden. Na dit seminar heeft u geleerd hoe u zelf eenvoudig incident response kunt doen en wat er bij een volledig forensisch onderzoek komt kijken. Ook leert u waar u aan moet denken als u een onderzoek voor de rechter wilt brengen.

PROGRAMMA DINSDAG 16 JUNI 2009

09.30 Opening door de dagvoorzitter

09.50 Incident response "light"
Walter Belgers, Madison Gurkha
Een systeem gedraagt zich raar. Er komen meldingen van derden over inbraakpogingen. Wat zou er aan de hand zijn? In deze lezing zullen simpele (freeware) tools de revue passeren, waarmee incident response kan worden gedaan. Hoe is de aanval in zijn werk gegaan? Welke sporen vind ik nog op de disk of in het geheugen? Zijn er rootkits achtergebleven? Een "light" onderzoek probeert antwoorden op die vragen te vinden maar heeft niet als doel een uitgebreid forensisch onderzoek te doen.

10.50 Pauze en informatiemarkt

11.10 Opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk
Arnoud Engelfriet, ICTRecht
Hacks en cracks worden steeds subtieler, maar de wet is en blijft een bot instrument. De Wet Computercriminaliteit is in 2006 grondig herzien, waarbij met name de regels rond virussen en DDoS-aanvallen aangescherpt zijn. Ook het meesurfen bij de buren is nu vaak strafbaar, hoewel nog niet duidelijk is wanneer nu precies. Maar voordat we weten of een XSS exploit nu "binnendringen in een geautomatiseerd werk is", zijn er nog wel een paar proefprocessen nodig. Wat houden die wetten en regels nu in? Hoe kan digitaal bewijs daarbij worden ingezet? En hoe voorkom je dat jij het proefproces wordt?

12.10 Vendorsessies

12.40 Lunch en informatiemarkt

13.40 Forensisch onderzoek in hacking zaken
ir. Marnix Kaart en ir. Erwin van Eijk CISSP, Nederlands Forensisch Instituut
Het NFI krijgt regelmatig het verzoek onderzoek te doen in zaken die betrekking hebben op hacking of pogingen daartoe. Meer dan eens is het aangeleverde materiaal van matige kwaliteit en dit heeft over het algemeen een negatieve invloed op de bewijswaarde. Voorbeelden hiervan zijn het ontbreken van een goede audittrail, gebrek aan mogelijkheden tot integriteitscontrole van aangeleverde logbestanden, onduidelijkheid over de betrouwbaarheid van datum- en tijdsinstellingen, onvolledige informatie met betrekking tot de aanwezige infrastructuur, etc. Deze presentatie beoogt de toehoorders meer inzicht te geven in randvoorwaarden waar bewijsmateriaal aan dient te voldoen. Ook worden er enkele praktische methoden en technieken gedemonstreerd waarmee bewijsmateriaal van goede kwaliteit verzameld kan worden ten tijde van een incident. De nadruk zal hierbij liggen op het vastleggen van netwerkverkeer en geheugenacquisitie. Er wordt uitgelegd op welke wijze dit materiaal een bijdrage kan leveren aan het forensisch onderzoek.

14.40 Vendorsessies

15.10 Pauze en informatiemarkt

15.30 Digitale criminelen gesnapt
Roland Vergeer, Digital Intelligence
Bij cybercrime is niets wat het lijkt. Een eenvoudig geval van interne fraude kan uiteindelijk uitmonden in een onderzoek, waarbij meerdere organisaties gecompromitteerd blijken te zijn. Aan de hand van een recente zaak laat Roland Vergeer zien hoe een digitaal forensisch onderzoek verloopt, en welke verrassingen de onderzoeker en zijn opdrachtgever kunnen tegenkomen. Aan bod komen onder andere de werkwijze van hackers, de gebruikte onderzoeksmethodiek, en gemaakte fouten bij beide partijen.

Array SEMINARS

Madison Gurkha
Your Security is Our Business

Sponsor: TSTC
TSHUKUDU TECHNOLOGY COLLEGE

GEHACKT?

INCIDENT RESPONSE & IT FORENSICS

TOPSPREKERS OP DE BLACK HATS SESSION PART VII

Roland Vergeer heeft ruim 15 jaar ervaring met digitale criminaliteit. Als technisch directeur bij een internet provider kreeg hij als een van de eersten te maken met digitale criminaliteit. In latere jaren deed hij als onderzoeker voor een vooraanstaand onderzoeksbureau onderzoek naar gehackte organisaties, digitale bedrijfsspionage, en digitale fraude. Als enthousiast en kundig trainer geeft Roland onder andere (maatwerk)trainingen in forensics, internet rechercheren, en cybercriminaliteit.

Arnoud Engelfriet is ICT-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij is partner bij juridisch adviesbureau ICTRecht. Zijn site www.lusmentis.com is één van de grootste sites in Nederland over internetrecht, met onder andere de gids "De Wet Computercriminaliteit". In de jaren negentig onderhield hij de alt.security.pgp FAQ. Zijn RSA-in-four-lines-of-Perl shirt bleek niet kookwasbestendig.

Walter Belgers is partner en Principal Security Consultant bij Madison Gurkha. Hij voert security audits uit, maar geeft ook geregeld trainingen zoals security awareness en spreekt graag op conferenties en bijeenkomsten. Walter heeft voor Madison Gurkha een tweedaagse cursus opgezet rondom incident response met eenvoudige hulpmiddelen. Naast zijn werk houdt Walter van driften, lockpicken en zeilen.

ir. Marnix Kaart is sinds 2007 werkzaam als forensisch onderzoeker bij het NFI. Hier doet hij forensisch onderzoek aan computers en netwerken met als speciale aandachtspunt Incident Response en onderzoek op plaats-delict (PD). Voor zijn aanstelling bij het NFI was hij werkzaam als onderzoeker bij de Technische Universiteit Delft waar hij onderzoek heeft gedaan naar internettopologie metingen.

ir. Erwin van Eijk CISSP is sinds 1998 werkzaam als forenisch onderzoeker bij het NFI. Hij heeft zich gespecialiseerd in het forensisch onderzoek aan gedistribueerde systemen en computernetwerken. Omdat goed forensisch onderzoek vereist dat het basismateriaal in orde is, houdt hij zich ook bezig met het specificeren van methoden voor het vastleggen en analyseren van netwerkdata.

GA SNEL NAAR WWW.ARRAYSEMINARS.NL VOOR ONLINE AANMELDEN!

INFORMATIE

DATUM EN TIJD
Dinsdag 16 juni 2009. De Black Hats Sessie start om 09.30 uur en duurt tot ongeveer 16.30 uur. Registratie is mogelijk vanaf 08.30 uur.

PLAATS
Hotel en Congrescentrum De Reehorst
Bennekomseweg 24
6717 LM EDE GLD
Tel: 0318-750300

AANMELDEN
Aanmelden is uitsluitend online mogelijk op www.arrayseminars.nl. Na uw online aanmelding ontvangt u een e-mail met uw ticketnummer. Deze bevestigingsmail met het ticketnummer is uw toegangsbewijs tot het seminar en dient u te tonen bij het seminar.

KOSTEN
De kosten voor deelname aan het seminar bedragen € 285,- (excl. BTW) per persoon. Documentatie, lunch en koffie zijn inbegrepen. Abonnees van LAN Magazine en Infosecurity ontvangen € 35,- korting. Werkt u bij een gemeente of provincie? Dan kunt u BTW terugvorderen via het BTW compensatiefonds.

VROEGBOEKVOORDEEL EN GROEPSKORTING
Als u zich uiterlijk vijf weken voor het evenement registreert, wordt u beloond met 10% vroegboekkorting. Meldt u op dezelfde dag meerdere personen van één bedrijf aan voor hetzelfde evenement, dan geldt vanaf vier deelnemers een aantrekkelijke korting.

ANNULEREN
Annuleren dient uitsluitend schriftelijk te geschieden. U kunt annuleren tot drie weken voor het evenement plaatsvindt. Er wordt echter wel € 75,- (excl. BTW) administratiekosten in rekening gebracht. Annuleren is niet meer mogelijk vanaf drie weken voordat het evenement plaatsvindt. Vervanging door een ander dan de aangemelde persoon is te allen tijde mogelijk.

MEER INFORMATIE
Alle informatie over dit seminar en de complete agenda van de e venementen vindt u op www.arrayseminars.nl. U kunt zich hier ook online registreren. Voor meer informatie over het programma en de registratie kunt u contact opnemen met Array Seminars, telefoonnummer 0172-469030.

GEHACKT? – INCIDENT RESPONSE & IT FORENSICS MAG U NIET MISSEN!

FOLDERCODE A913

Array SEMINARS

Computable

INFOSECURITY
INZICHT IN INFORMATIEBEVEILIGING