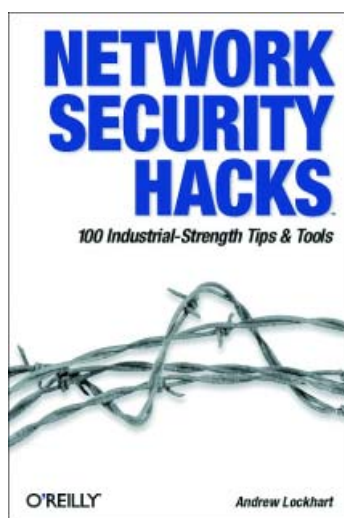


NGN - leden
de duiken in
de boeken

Wie bij wil blijven moet
regelmatig in de boeken
duiken. Welke boeken moe-
ten nu weer eens onder de
loep worden genomen?

BookROM Up To Date



Network Security Hacks

Auteur: Andrew Lockhart
Uitgever: O'Reilly
ISBN: 0596006438
Taal: Engels
Pagina's: 298
Prijs: \$ 24,95
JIF: ●●●
Recensent: Dimitry Schoenmakers

In het boek Network Security Hacks heeft de auteur Andrew Lockhart samen met enkele open source collega's 100 tips in iets minder dan 300 bladzijden bijeen gebracht, voor een ieder die de beveiliging van zijn/haar netwerk op een hoger niveau wil brengen. Mits deze gebaseerd is op een UNIX, Linux of BSD-variant, of u bereid bent dergelijke systemen in uw netwerk op te nemen, want slechts één hoofdstuk wordt aan het Windows besturingssysteem gewijd. Overigens worden daarin wel degelijk nuttige tips (10 stuks) gegeven.

Naast het Windows Host Security hoofdstuk bestaat het boek uit nog zeven hoofdstukken. De volgorde daarvan is mij niet geheel logisch gebleken. Namelijk in hoofdstukken 1, 2, 3 en 6 ligt de nadruk op preventie. En in hoofdstukken 4, 5 en 7 op detectie van pogingen tot inbraak danwel op geslaagde inbraakpogingen. Wel weer logisch wordt tot slot in hoofdstuk 8 kort ingegaan op herstel na het ontdekken van een indringer.

Hoofdstukken 1 en 2 beginnen wel netjes bij het begin. Eerst dienen namelijk de afzonderlijke systemen beveiligd te zijn, alvorens aan het netwerk begonnen kan worden. Daartoe behandelt hoofdstuk 1 - Unix Host Security - in 20 tips het dichtspijkeren van Unix, Linux & BSD systemen. En hoofdstuk 2 - Windows Host Security - bespreekt hetzelfde, maar dan voor het Windows 2000 (server) besturingssysteem. Overigens worden beide onderwerpen uitgebreid behandeld in overige boeken uit de O'Reilly Hacks serie, zoals: 'BSD Hacks' en 'Windows Server Hacks'

Hoofdstuk 3 - Network Security - is het meest uitgebreide hoofdstuk met 23 tips. Deze tips zijn er op gericht zoveel mogelijk gaten in je netwerk te dichten. Vrijwel vanzelfsprekend komen hierbij diverse firewall tips aan de orde, maar ook zaken als het veilig delen van bestanden in Unix.

Hoofdstuk 4 - Logging - behandelt voornamelijk diverse methodes voor het opzetten van Remote Logging. Zodanig in geval van een beveiligingslek het een stuk moeilijker wordt voor de

indringer de logbestanden aan te passen (7 tips).

Logbestanden vertellen maar een deel van wat er op het netwerk gebeurt. Of juist teveel. Daarom is het dagelijks lezen van deze logbestanden in de praktijk nauwelijks haalbaar. In Hoofdstuk 5 - Monitoring and Trending - wordt daarop middels een zestal tips ingesprongen. Deze tips hebben tot doel inzicht te geven in het hoe een netwerk met behulp van software actief te monitoren is en in het ontdekken en tonen van bepaalde trends in het netwerkverkeer.

In de vorige hoofdstukken is het netwerk steeds verder dichtgetimmerd. Hoofdstuk 6 - Secure Tunnels - daarentegen beschrijft in 15 tips hoe toch veilige verbindingen met andere systemen en netwerken gelegd kunnen worden. En wel met het opzetten van IPSec, virtual network interfaces en VPN's, op en tussen de diverse besturingssystemen.

Hoofdstuk 7 - Network Intrusion Detection - is het logische vervolg op hoofdstuk 5. Bij het ontdekken van vreemde waarden tijdens het monitoren of schadelijke trends, zou het prettig zijn als er automatisch alarm geslagen wordt. En daarom heeft de auteur 14 tips opgenomen om dit tot stand te brengen.

Het onderwerp van hoofdstuk 8 - Recovery and Response - kan, zoals de auteur het zelf schrijft, niet in de 5 tips beschreven worden. Maar zijn slechts een leidraad om een idee te kunnen vormen wat er gedaan kan

worden nadat een inbraak heeft plaatsgevonden..

Ondanks de in mijn ogen ietwat onlogische volgorde van hoofdstukken is het een prima boek met prima uitgewerkte tips. Daarom kan ik het iedereen aanbevelen die netwerkbeveiliging hoog op zijn/haar lijstje heeft staan.

GroupWise 6.5 administrator's guide

Auteur: Tay Kratzer
 Uitgever: Que Publishing
 ISBN: 0789729822
 Taal: Engels
 Pagina's: 948
 Prijs: \$ 59,99
 JIF: ●●●●
 Recensent: Frank Heemsbergen

Toen Novell WordPerfect kocht is uit WordPerfect Office GroupWise ontstaan. Nog steeds wordt de naamgeving uit WP-office gebruikt zoals 'wpdomain' en 'ofuser'. Inmiddels is GroupWise aanbeldt bij versie 6.5



en ook voor deze versie heeft Tay Kratzer een administrator's guide geschreven.

Gezien het aantal pagina's moet het boek een complete indruk achterlaten. Het boek beslaat 948 bladzijden welke zijn onderverdeeld in 31 hoofdstukken. De 31 hoofdstukken zijn weer ingedeeld in 5 delen.

In het eerste deel wordt de basis van het GroupWise-systeem bijgebracht. Zo wordt in hoofdstuk 2 aan de hand van een basis-installatie de architectuur uitgelegd. Het synchronisatieproces van de GroupWise-directory wordt zeer duidelijk uitgebeeld in hoofdstuk 3.

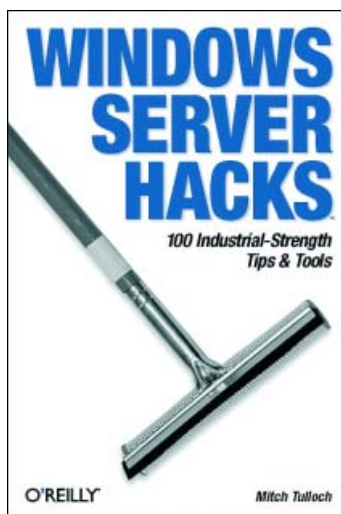
Het tweede deel geeft een introductie in de beheer-mogelijkheden zoals consoleOne. De drie hoofdstukken in dit deel geven een overzicht van de beheertools voor het gehele GroupWise-systeem en beschrijven de GroupWise-utilities.

Deel 3 behandelt de verschillende agents die GroupWise gebruikt. Achtereenvolgens worden de POA, MTA, GWIA en de webaccess-agent beschreven. De hoofdstukken hebben steeds dezelfde opbouw, eerste wordt de werking uitgelegd, vervolgens de installatie, configuratie, console, logfiles, http-monitor en afgesloten met enkele nuttige tips van de schrijver. Dit deel wordt afgesloten met een hoofdstuk over de client waarin 5 verschillende 'unattended'-installaties worden behandeld.

Het vierde deel heeft terecht de titel 'Practical Administration' meegekregen. Uitgelegd wordt onder andere: het verhuizen van gebruikers naar een ander postkantoor, waarin een handig stappenplan wordt doorlopen. Verder wordt het opzetten en beheren van een document management systeem beschreven. Ook de tool 'Gwcheck' wordt niet vergeten in dit deel.

Het vijfde en laatste deel is het dikste en beschrijft voornamelijk het troubleshooten van de GroupWise-omgeving. Het opbouwen van een GroupWise-systeem inclusief detailontwerp wordt behandeld. Er wordt dieper ingezoomd in de berichtenstroom zodat je kunt bepalen waar een bericht zich bevindt. Het beveiligen van berichten en het herstellen van verwijderde gebruikers (postbussen) wordt ook in aparte hoofdstukken vermeld. Voor het geval dat al deze troubleshoot-tips niet helpen wordt in het laatste hoofdstuk van het boek de GroupWise back-up en restore behandeld.

Ondanks dat het boek als een dikke pil oogt bevat het geen lange verhalen, de procesbeschrijvingen zijn duidelijk en goed te volgen. Tussen de tekst worden regelmatig nuttige tips vermeld. De hoofdstukken zijn veelal in dezelfde opbouw geschreven, dit leest wel prettig. In mijn ogen is dit boek compleet en goed te gebruiken als naslagwerk, een ideaal boek voor de systeembeheerder.



Windows Server Hacks

Auteur: Mitch Tulloch
 Uitgever: O'Reilly
 ISBN: 0596006470
 Taal: Engels
 Pagina's: 357
 Prijs: \$ 24,95
 JIF: ●●●●
 Recensent: Steven Hoogslag

Een club van 28 Hackers publiceert '100 Industrial-Strength Tips & Tools' in dit prettig ingedeelde en goed lezende boek. De trucs behelzen het doen van aanpassingen aan Windows 2000 en 2003 servers en netwerken, voornamelijk met VBScripts en batch files. Volgens de auteur die de hacks verzamelde gaat dit boek in op dat deel van het MS-Windows server-onderhoud dat met de GUI niet of slecht te bereiken is. Alle broncode staat uitgeschreven in het boek. Dat is goed gedaan want zo kun je de inhoud rustig bestuderen en toch je beeldscherm-pauzes in acht nemen. Gelukkig staat de code ook klaar voor download op de website van de uitgever. De link naar <http://www.oreilly.com/catalog/wins->

vrhks/ scheelt tikwerk en wellicht ook fouten. Overigens is via deze link ook een eigen indruk van het boek te krijgen; er staan enkele stukken uit het boek geplaatst.

De honderd tips in dit boek staan verdeeld in de volgende hoofdstukken: 1 General Administration, 2 Active Directory, 3 User Management, 4 Networking Services, 5 File and Print, 6 Internet Information Server, 7 Deployment, 8 Security, 9 Patch Management, 10 Backup and Recovery.

Met twee-kleurendruk en een duidelijke opmaak is de indeling goed uitgewerkt. Het werken met iconen voor moeilijkheidsgraad en gevaarlijke situaties is prima gedaan.

Hier als voorbeeld enkele hack-beschrijvingen uitgelicht:

Hack 6 bespreekt een VBS script waarmee op afstand een Windows 2000 systeem kan worden afgesloten, eventueel met parameters.

Hack 12 behandelt een script om Event-Logs te verzamelen en beheren.

Hack 14 laat je configuratie-informatie op afstand verzamelen naar een HTML pagina.

Hack 45 zorgt voor opstart met de juiste netwerkparameters op het werk, thuis en op locatie.

Hack 54 gaat in op het klonen en back-ups maken van de IIS Metabase.

Hack 60 demonstreert hoe meerdere sites op poort 80 kunnen draaien door het aanpassen van Socket Pooling.

Hack 66 vertelt hoe je Windows componenten als Freecell kunt verwijderen met een opdracht vanaf de DOS prompt.

Hack 82 toont hoe je vanaf DOS prompt de geplaatste patches en hotfixes kunt opvragen.

Hack 90-100 leggen uit wat nodig is om een gecrashte server te kunnen

herbouwen. Vooral het deel dat je moet doen vóórdat de server crasht is heel leerzaam want met tijdige maatregelen is herstelwerk een stuk beter te doen.

Hack 92 beschrijft bijvoorbeeld het geautomatiseerd groeperen en op tape plaatsen van System-State backups van remote servers, iets dat in een serverpark erg handig kan zijn.

De meeste hacks kunnen in Notepad worden ingetikt in de vorm van batch-file of VBS script en de resultaten kunnen vaak in Notepad worden uitgelezen. Door zo te werken kan veel op afstand en geautomatiseerd worden gedaan.

Waarom geen JIF van 5 bollen? Het leek er even op, maar gaandeweg blijkt de inhoud toch wat 'hap-snap'; een complete index van relevante Windows Server-parameters bijvoorbeeld wordt ons onthouden. Het boek is niet in het Nederlands vertaald, en enkele hacks lijken erbij gesleept om de 100 te halen...

Dit boek zit in elkaar zoals het hoort, is goed geschreven, maakt gebruik van internet als publicatie-hulp en zit bovenal vol met zaken die op een dag van pas zullen komen als je MS-Windows Servers en netwerken beheert. Ook maakt het je nog eens alert op de alternatieve beheersmogelijkheden vanaf DOS-prompt en via VBScript.

Een echte aanrader voor wie onder de motorkap van een MS-Windows Server aan het werk wil.

De JIF zit als volgt in elkaar:

- Zo worden boeken zelden geschreven.
- Goede en vlot geschreven uitgave. Relevante informatie.
- Een "krappe voldoende" voor dit boek.
- Nee, nee, nee! Het had zo mooi kunnen zijn.
- In één woord: vreselijk.