6º Centro de Telemática de Área
O portal da Telemática no Pantanal

PROCEDIMENTO OPERACIONAL PADRÃO

Remoção de Rootkits

Março de 2010

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DCT - C I T EX
6º CENTRO DE TELEMÁTICA DE ÁREA
(Centro de Informática Nr 9/1993)

PROCEDIMENTO OPERACIONAL PADRÃO

Remoção de Rootkits

1. FINALIDADE

Este POP tem por finalidade proteger servidores de rede usando ferramentas chkrootkit e rkhunter.

2. DEFINIÇÃO

. Rootkit são ferramentas que hackers usam para entrar em um sistema e não serem descobertos. Muitas pessoas tem suas máquinas invadidas e usadas para fins ilicitos.

3. PROCEDIMENTOS

Antes de iniciar, certifique-se que as farramentas estejam instaladas, conforme o Anexo.

a. **Ferramenta chkrootkit**

1) Para usar a ferramenta, estando como root, digite chkrootkit

2) Para rodar o chkrootkit em outro dispositivo digite chkrootkit -p /media/dispositivo

3) Para maiores informações digite chkrootkit -h

4) Caso o chkrootkit encontre algo, ele mostrará um INFECTED na linha correspondente. Deve-se proceder a remoção do rootkit.

b. **Ferramenta rkhunter**

1) Para usar a ferramenta estando como root digite rkhunter -c

2) Para maiores informações digite rkhunter -h

3) Os arquivos em cor verde – not found e ok – estão normais.

4) Os arquivos que tiverem WARNING estão comprometidos – sairá na cor vermelha. Deve-se proceder a remoção do rootkit.

5) O rkhunter irá gerar um log em /var/log/rkhunter.log

6) Caso tenha suspeita que seu sistema esteja infectado, deverá usar um livecd e rodar as ferramentas a partir do livecd.

Anexo

7) Para baixar a ferramenta chkrootkit entre no site http://www.chkrootkit.org/

8) Para instalar a ferramenta, estando como root, digite apt-get install chkrootkit

3) Para baixar a ferramenta entre no site http://rkhunter.sourceforge.net/

4) **Para instalar a ferramenta estando como root digite** apt-get install rkhunter

5) Solução proprietaria para servidor de arquivos kaspersky veja logo abaixo:

http://brazil.kaspersky.com/products/empresas/security_apps_file_servers.php

http://usa.kaspersky.com/products_services/business/components/anti-virus_samba_server.php

Kaspersky Anti-Virus for Samba Server is designed to protect file storage areas on Samba Servers, which emulate Windows file servers under the Linux operating system. Thus, Windows-based users within a heterogeneous network are provided with safe and transparent access to data stored on Linux file servers. Kaspersky Anti-Virus is easily integrated with the Samba Server and does not require the Samba Server or parts of the operating system to be re-compiled.

1. **Functions**

- Anti-Virus Protection
- Easy Administration
- System Requirements

Detects and disinfects viruses, spyware and other malware

Real-time protection for file The application intercepts requests for access to Samba file storage areas, analyzes the files being accessed for malicious code and disinfects or deletes infected objects. Suspicious objects are quarantined pending further analysis.

On demand file system scanning. The application scans specified areas for infected and suspicious objects at the specified times (or on demand). It analyzes objects and disinfects, deletes or quarantines objects for further analysis.

Antivirus scanning optimization. The iChecker™ technology significantly reduces the time required for duplicate scans of each object by only scanning those files that have been modified since the latest scan.

Quarantine. Infected, suspicious and damaged objects detected in the file system can be moved to the quarantine folder, where they are processed according to administrator defined rules.

Backup storage. The solution saves copies of infected objects in a backup storage area before they are treated and/or deleted, making it possible to restore an object on demand in the event that disinfection fails.

Easy administration

Remote administration. Kaspersky Anti-Virus for Samba Server can be configured either traditionally via the application's configuration file or using the Web interface.

Antivirus database updates. Antivirus database updates can be downloaded from Kaspersky Lab's servers via the Internet or from local update servers on demand or automatically on schedule. Administrators can choose the type of antivirus databases to be used: standard (detection of true malware only) or extended (databases used to detect potentially hostile software – e.g., spyware, adware, etc.). Kaspersky Lab antivirus databases are updated hourly.

2. System Requirements

Hardware Requirements

- Pentium class CPU
- At least 32MB of RAM
- At least 100MB available HDD space for installation

Anexo A – folha 2/2

Software Requirements

32-bit platforms:

- RedHat Enterprise Linux Advanced Server 4 UPD3 (kernel: 2.6.9-34EL (i386))
- RedHat Linux 9.0. (kernel: 2.4.20-8)
- SUSE Linux Enterprise Server 9.0 SP3. (kernel: 2.6.5-7.97)
- SUSE Linux Professional 10.1. (kernel: 2.6.16.13-4)
- Debian GNU/Linux 3.1 R2. (kernel: 2.4.27-2)
- Mandriva 2006. (kernel: 2.6.12-12mdksmp)
- FreeBSD 4.11. (kernel: GENERIC/SMP)
- FreeBSD 5.4. (kernel: GENERIC/SMP)
- FreeBSD version 6.1. (kernel: GENERIC/SMP)

64-bit platforms:

- RedHat Enterprise Linux Advanced Server 4 UPD3 (kernel: 2.6.9-34EL (amd64))
- RedHat Fedora Core 5. (kernel: 2.6.15-1.2054_FC5)
- SUSE Linux Professional 10.1. (kernel: 2.6.16.13-4)
- SUSE LES 9 SP3. (kernel: 2.6.5-7.97)

- Samba Server Version 2.2.6 or higher
- Interpreter of the Perl language version 5.0 or higher