Análisis Forense de Sistemas Comprometidos

The Pope // Undersec Security Team

pope@undersec.com

Undercon 0x07 – Diciembre 2.003

Qué os voy a contar…

- 1. Introducción
- 2. Saber que nos han comprometido
- 3. Posibles causas de la intrusión
- 4. Motivación del AF
- 5. Potencial del AF
- 6. Medidas a priori
- 7. Referencias

1. Introducción

- AF: ¿qué es? ¿para qué sirve?
- **Cuando** nos entren, querremos…
    - Alerta temprana
    - Máxima información
    - No perder servicio
    - Mínimo coste

2. Cómo saber que nos han comprometido

- Alteración de los ficheros (md5, tamaño, contenido…). HIDS: Tripwire, Tiger…
- Tráfico de red anormal. NIDS: snort
- Actividad sospechosa en los logs. HIDS
- Notificaciones externas. CERTs

3. Causas de la intrusión

- Fallo técnico: culpa del SW.

  Parcheo, auditorías, otras medidas.
- Fallo técnico/humano: mala configuración.

  ¿A quién no le ha pasao? ;-)
- Fallo humano: ingeniería social.

  Formar y concienciar a users y admins.

4. Motivación del AF

- Conocer el error para no repetirlo.
- Conocer el alcance del ataque.
- ¿Medidas legales?

- Problema: cuesta tiempo (➔ €) y, sobre todo, *tiempo de servicio*.

5. Potencial del AF

- En qué nos apoyamos:
  - Correlación de logs
  - Datos *unallocated* en los discos
  - mac-times: **timeline**

Potencial del AF: ejemplo de timeline

- RedHat 7.1
- *adduser hax0r*

```
Ejecución de "adduser hax0r":
   TAMAÑO      TIPO/PERISOS    UID           GID     I-NODE FICHERO
       7 .a. l/lrwxrwxrwx   root   root     158994   /usr/sbin/adduser -> useradd
   52348 .a. -/-rwxr-xr-x   root   root     159006   /usr/sbin/useradd
      96 .a. -/-rw-------   root   root     40163    /etc/default/useradd
Modificación de gshadow, group y lastlog:
   TAMAÑO      TIPO/PERISOS    UID           GID     I-NODE FICHERO
     400 m.. -/-rw-------   root   root     28263    /etc/gshadow-
     400 m.. -r--------   root   root     28264    <hda1.dd-dead-28264>
     484 m.. -/-rw-------   root   root     26151    /etc/group-
  146584 m.c -/-rw-r--r--   root   root     12050    /var/log/lastlog
Creación del home y copia de skel:
   TAMAÑO      TIPO/PERISOS    UID           GID     I-NODE FICHERO
    4096 m.c d/drwx------ hax0r    hax0r    63361    /home/hax0r
     124 .a. -/-rw-r--r--   root   root     40166    /etc/skel/.bashrc
     124 mac -/-rw-r--r-- hax0r    hax0r    63364    /home/hax0r/.bashrc
     224 .a. -/-rw-r--r--   root   root     40165    /etc/skel/.bash_profile
     224 mac -/-rw-r--r-- hax0r    hax0r    63363    /home/hax0r/.bash_profile
Lectura de opciones PAM, y solicitud de password:
   TAMAÑO      TIPO/PERISOS    UID           GID     I-NODE FICHERO
     210 .a. -/-rw-r--r--   root   root     60254    /etc/pam.d/other
     211 .a. -/-rw-r--r--   root   root     60256    /etc/pam.d/passwd
     637 .a. -/-rw-r--r--   root   root     60255    /etc/pam.d/system-auth
   14764 .a. -/-rwxr-xr-x   root   root     6039     /lib/security/pam_cracklib.so
    5046 .a. -/-rwxr-xr-x   root   root     6040     /lib/security/pam_deny.so
   13137 .a. -/-rwxr-xr-x   root   root     6041     /lib/security/pam_env.so
   13858 .a. -/-rwxr-xr-x   root   root     6047     /lib/security/pam_limits.so
   10874 .a. -/-rwxr-xr-x   root   root     6060     /lib/security/pam_stack.so
   46971 .a. -/-rwxr-xr-x   root   root     6064     /lib/security/pam_unix.so
      19 .a. l/lrwxrwxrwx   root   root     44255    /lib/libpam_misc.so.0 -> libpam_misc.so.0.74
   12191 .a. -/-rwxr-xr-x   root   root     44254    /lib/libpam_misc.so.0.74
      17 .a. l/lrwxrwxrwx   root   root     44248    /lib/libpwdb.so.0 -> libpwdb.so.0.61.1
  133705 .a. -/-rwxr-xr-x   root   root     44247    /lib/libpwdb.so.0.61.1
      15 .a. l/lrwxrwxrwx   root   root     174499   /usr/lib/libcrack.so.2 -> libcrack.so.2.7
   70446 .a. -/-rwxr-xr-x   root   root     174498   /usr/lib/libcrack.so.2.7
   13536 .a. -/-r-s--x--x   root   root     159701   /usr/bin/passwd
Aplicación de libcrack:
   TAMAÑO      TIPO/PERISOS    UID           GID     I-NODE FICHERO
    1024 .a. -/-rw-r--r--   root   root     175310   /usr/lib/cracklib_dict.hwm
   42116 .a. -/-rw-r--r--   root   root     175312   /usr/lib/cracklib_dict.pwi
  828334 .a. -/-rw-r--r--   root   root     175311   /usr/lib/cracklib_dict.pw
Modificación de shadow y passwd:
   TAMAÑO      TIPO/PERISOS    UID           GID     I-NODE FICHERO
     856 m.. -/-rw-------   root   root     28261    /etc/shadow-
    1044 m.. -/-rw-------   root   root     28123    /etc/passwd-
    1044 m.. -rw-r--r--   root   root     28265    <hda1.dd-dead-28265>
```

6. Medidas a priori

- Jamás FAT32.
- Logs adecuados.
- HIDS: integridad de archivos, revisión (automática) de logs.
- Seguridad perimetral: NIDS, ¿ADS?
- Si puede ser, RAID1.

7. Referencias

- http://voodoo.somos lo peor.com/ forensics /bookmarks
- http://www.sleuthkit.org
- http://www.honeynet.org

pope@undersec.com

¿Preguntas?