(GNU/Linux) Host Intrusion Detection

breve panoramica sulle tecnologie e gli strumenti di host intrusion detection, exploit mitigation e analisi dei log su piattaforma GNU/Linux

CLUSIT Security Summit '09
26 marzo 09 - Milano

Relatore:

NETWORK enforcer SECURITY
Igor Falcomatà
Chief Technical Officer
ifalcomata@enforcer.it

Italian Security Mailing List
SIKUREZZA.ORG

< free advertising

about:

aka “koba”

- attività professionale:
  - analisi delle vulnerabilità e penetration testing
  - security consulting
  - formazione
- altro:
  - sikurezza.org
  - (Er|bz)lug

Relatore:

NETWORK enforcer SECURITY
Igor Falcomatà
Chief Technical Officer
ifalcomata@enforcer.it

Host Intrusion Detection

http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

"A host-based IDS monitors all or parts of the dynamic behaviour and the state of a computer system."

"One can think of a HIDS as an agent that monitors whether anything/anyone has circumvented the security policy that the operating system tries to enforce."

Host Intrusion Detection

the big picture

- integrity checking
  - file
  - memoria
  - kernel/driver/os/...
- log monitoring
- rootkit detection
- exploit prevention
- alerting /active responses

File integrity checking

verifica dell'integrità di file (eseguibili, config, ...)

- aide - Advanced Intrusion Detection Environment

  http://aide.sf.net
- debsums - verify installed packages against MD5

  (debian based distros)
- fcheck - IDS filesystem baseline integrity checker

  (orphaned?)
- integrit - file integrity verification program

  http://sourceforge.net/projects/integrit/
- bsign - intrusion detection using embedded hashes

  ftp://ftp.buici.com/pub/bsign/

File integrity checking

verifica dell'integrità di file (eseguibili, config, ...)

- **tripwire - file and directory integrity checker**

  http://sourceforge.net/projects/tripwire/
- **stealth - a stealthy File Integrity Checker**

  http://stealth.sourceforge.net/
- **samhain - data integrity / host intrusion alert system**

  http://www.la-samhna.de/samhain/
- **osiris - network-wide system integrity monitor**

  http://osiris.shmoo.com
- **rfc – remote filesystem checker**

  http://rfc.sourceforge.net/
- **...**

$ apt-cache show tripwire

http://www.tripwire.com/products/enterprise/ost/compare.cfm

"Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes."

"Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner."

tripwire --check

http://sourceforge.net/projects/tripwire/

root@miao-new: ~

```
Rule Name: Other configuration files (/etc)
Severity Level: 66
-------------------------------------------------------------------------------

Modified:
"/etc"

-------------------------------------------------------------------------------
Rule Name: Security Control (/etc/shadow)
Severity Level: 66
-------------------------------------------------------------------------------

Modified:
"/etc/shadow"

-------------------------------------------------------------------------------
Rule Name: Root file-system executables (/bin)
Severity Level: 100
-------------------------------------------------------------------------------

Modified:
"/bin"
"/bin/netstat"
```

tripwire 2.4.1.2

Last Update: Apr 18 2007

- **pro**
  - db e configurazione cifrati
  - facilmente scriptabile
- **contro**
  - stand-alone
  - no check memoria/os
  - sviluppo praticamente fermo da anni
  - tuning
    - /dev/shm, /tmp, /proc, ...

Basic security checks

poor man HIDS

- checksecurity - basic system security checks

  (debian based distros)
- diffmon - tool for reporting changes in system conf

  (orphaned?)
- systraq - warn when system files change

  http://mdcc.cx/systraq/
- tiger - report system security vulnerabilities

  http://www.nongnu.org/tiger/
- /etc/security (*BSD)

checksecurity --daily

(debian checksecurity package)

```
root@miao-new: ~
root@miao-new:~# checksecurity daily
There is more than one root login acounts
root:x:0:0:root:/root:/bin/bash
r00t:x:0:0:root:/root:/bin/bash
miao-new changes to setuid programs and devices:
--- setuid.today        2009-03-26 02:19:56.000000000 +0100
+++ /var/log/setuid/setuid.new.tmp      2009-03-26 02:20:24.000000000 +0100
@@ -331,0 +332 @@
+  980008  2755   1 root       root          702160 Mon May 12 20:33:24 2008 /dev/shm/
root@miao-new:~#
```

checksecurity & co

piutost che gnent l'é meii piutost

- **pro**
  - integrati nel sistema (o facilmente attivabili)
  - *plug & pray*
- **contro**
  - facilmente manomissibili
  - controlli limitati alle sole componenti critiche
    - passwd, setuid, ...
  - “Note that these [checks] are not to be considered in any way complete”

Lynis

http://www.rootkit.nl/projects/lynis.html

"Lynis is an auditing tool for Unix (specialists). It scans the system and available software, to detect security issues. Beside security related information it will also scan for general system information, installed packages and configuration mistakes."

"Lynis does not fix things automatically, it reports only"

./lynis --no-colors -Q

non propriamente un HIDS, però...

```
root@miao-new: ~
================================================================================

  -[ Lynis 1.2.4 Results ]-

  Tests performed: 93
  Warnings:
  ----------------------------
   - [03:34:13] Warning: No password set on GRUB bootloader [test:BOOT-5121] [impact:M]
   - [03:34:16] Warning: Multiple users with UID 0 found in passwd file [test:AUTH-9204] [impact:H]
   - [03:34:25] Warning: Root can directly login via SSH [test:SSH-7412] [impact:M]
   - [03:34:26] Warning: No running NTP daemon or available client found [test:TIME-3104] [impact:M]
================================================================================
  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat
================================================================================
  Hardening index : [27]     [#####               ]
================================================================================
  Lynis 1.2.4
  Copyright 2007-2009 - Michael Boelen, http://www.rootkit.nl/
================================================================================


root@miao-new:~/lynis-1.2.4#
```

Lynis

Examples of audit tests:

- Available authentication methods
- Expired SSL certificates
- Outdated software
- User accounts without password
- Incorrect file permissions
- Firewall auditing
- ...

System integrity checking

controllo dell'integrità del sistema (os/mem/kernel/..)

- **(known) malware**
  - backdoor
  - trojan
  - rootkit
- **hidden activities**
  - processi
  - directory
  - socket
  - moduli kernel

Rootkit Hunter

http://www.rootkit.nl/projects/rootkit_hunter.html

"This tool scans for rootkits, backdoors and local exploits by running tests like:

- MD5 hash compare
- Look for default files used by rootkits
- Wrong file permissions for binaries
- Look for suspected strings in LKM and KLD modules
- Look for hidden files
- Optional scan within plaintext and binary files"

chkrootkit

http://www.chkrootkit.org/

"chkrootkit is a tool to locally check for signs of a rootkit. It contains:

- system binaries for rootkit modification.
- interfaces is in promiscuous mode.
- checks for lastlog/wtmp/utmp deletions.
- checks for signs of LKM trojans."

Quando si parla di LKM...

(Loadable Kernel Module)

- se un attaccante ha accesso privilegiato al kernel -> BINGO
- servono livelli ridondanti di sicurezza, come ad esempio le capabilities, RBAC, LSM, (...)
- detection signature based
  - falsi positivi
  - falsi negativi

Quando si parla di LKM...

non esiste un metodo di detection efficace al 100%

- limiti concettuali
  - p. es. controllo syscall vs controllo VFS
- non signature based
  - detecting hiding techniques (userspace)
  - execution path analysis
  - anomaly detection
- monitoraggio real-time passivo vero e proprio
  - “host snort” (?)
- inferenza/analisi
  - kstat (R.I.P.)

avoid being r00ted?

"In kernel space, nobody can hear you scream"

- **Linux Security Modules (LSM)**
  - SELinux - http://en.wikipedia.org/wiki/Selinux
  - AppArmor - http://en.wikipedia.org/wiki/AppArmor
  - ..
- **Role-Based Access Control (RBAC)**
  - http://en.wikipedia.org/wiki/RBAC
- **prevention of arbitrary code execution**
  - PAX - http://en.wikipedia.org/wiki/Pax
  - Exec Shield - http://en.wikipedia.org/wiki/Exec_Shield
  - SSP - http://en.wikipedia.org/wiki/Stack-smashing_protection
- **hardening**

grsecurity

http://www.grsecurity.net/

- prevention of arbitrary code execution
  - PAX + various
  - kernel
  - userspace
- Role-Based Access Control (RBAC)
- security auditing
- randomization
- enforcement
- ...

log analysis

gestione dei log

- raccolta & salvataggio
  - locale
  - remota
- analisi
  - real-time
  - batch / cronjobs
  - manuale (HA HA HA)
- correlazione

log analysis

analisi dei log

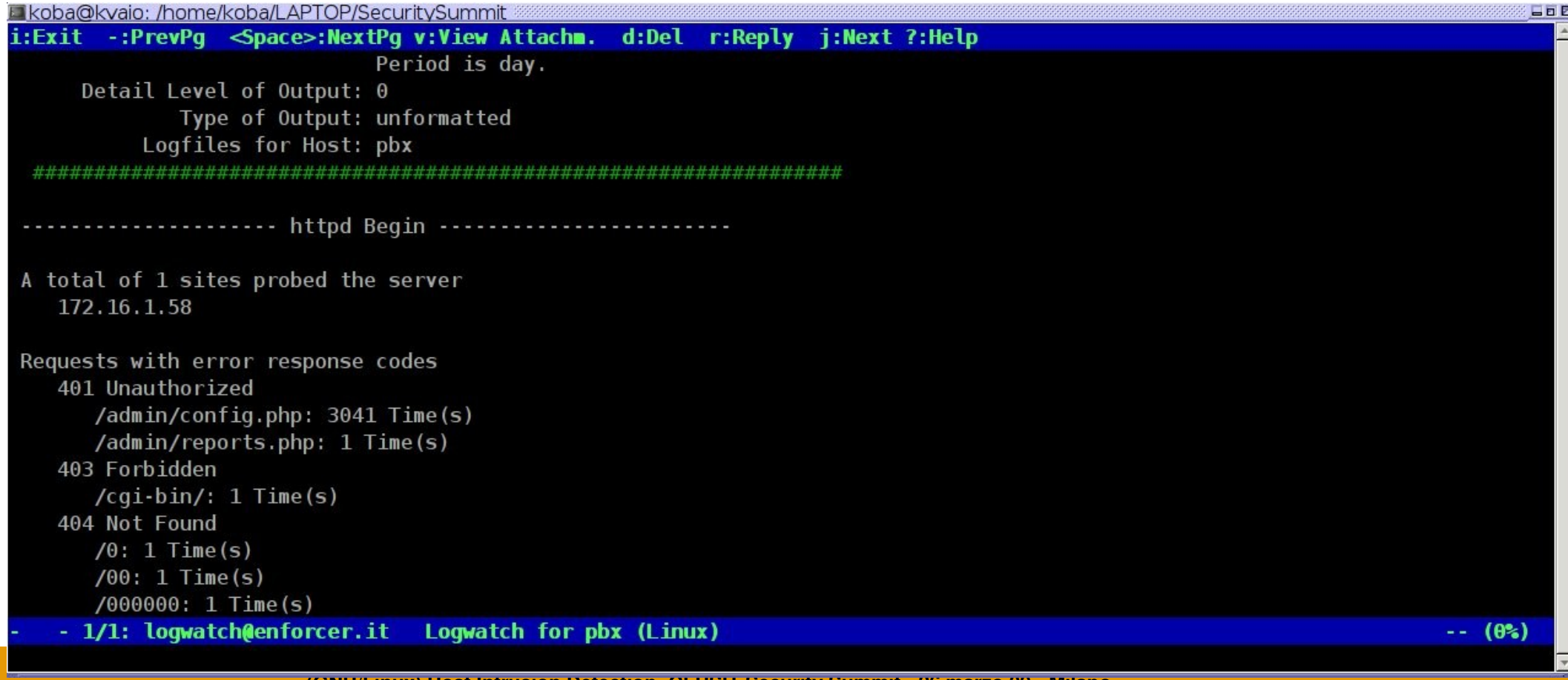
- **pattern specifici**
  - failed logins
  - error / warning / critical
  - known vulns (p. es. *cgi-scanning*, ...)
  - violazione policy
- **anomaly detection**
- **alerting / active responses**
- **statistiche / riepilogo**
  - analisi *umana* a posteriori
  - variazioni statistiche evidenti (cpu/mem/net/..)

log analysis

da semplici script ...

- **logcheck - mails anomalies in the system logfiles**

http://logcheck.org/



Appl Level log analysis

- **Intrusion Detection for Apache**
  an Apache log security analyzer written in PHP

  http://sourceforge.net/projects/phpida/
- **apache-scalp - a log analyzer for the Apache web server that aims to look for security problems**

  http://code.google.com/p/apache-scalp/
- **..**

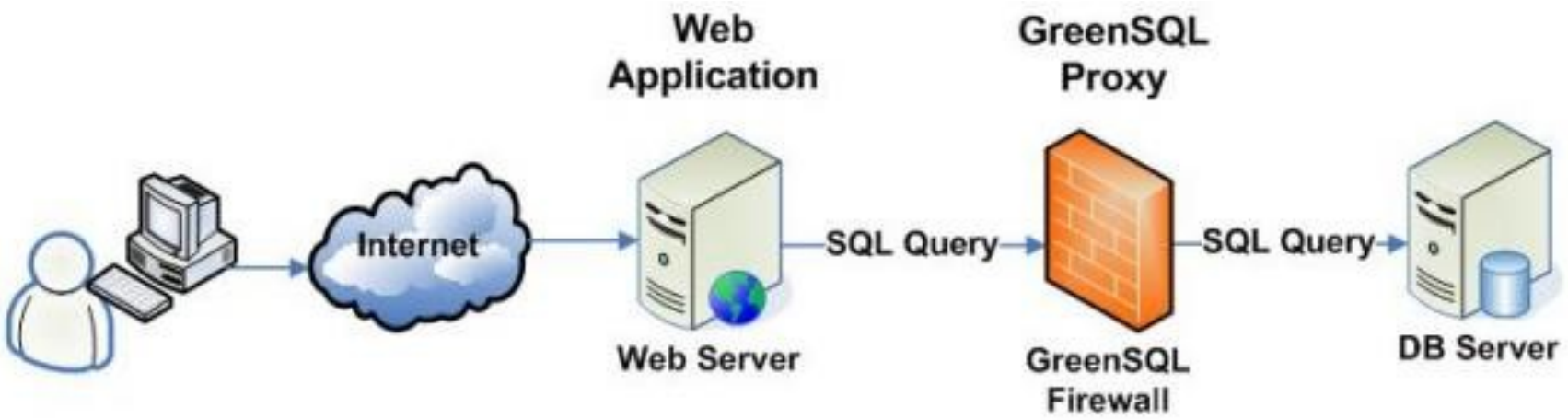
App Level IDS / IPS / something?

- **modsecurity – web application firewall / ips / ids**

  http://www.modsecurity.org

- **GreenSQL - a database firewall used to protect databases from SQL injection attacks (MySQL)**

  http://www.greensql.net



..a sistemi di SIM complessi

http://en.wikipedia.org/wiki/SIM

"Security information management (SIM) is the industry-specific term in computer security referring to the collection of data (typically log files; e.g. eventlogs) into a central repository for trend analysis"

"SIM products generally comprise software agents running on the computers that are to be monitored, communicating with a centralized server acting as a "security console"

OSSEC

http://www.ossec.net/

"OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.

"It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows."

Prelude-LML

http://www.prelude-ids.com

"Prelude-LML is a signature-based log analyzer monitoring your log file and received syslog messages for suspicious activity."

"It handle events generated by a large set of components, including but not limited to: APC Emu, BigIP, Cisco PIX, Clamav, Dell-OM, Grsecurity, Honeyd, ipchains, Netfilter, ipfw, Nokia ipso, Apache ModSecurity, [..]"

Snare

http://www.intersectalliance.com/projects/index.html

"SNARE (System iNtrusion Analysis and Reporting Environment) Agents are a series of audit collection and forwarding tools, that facilitate centralised audit and log collection on Linux, Solaris, AIX, Irix, Windows, and other operating systems and services."

OSSIM

http://www.ossim.net/

"Ossim stands for Open Source Security Information Management. Its goal is to provide a comprehensive compilation of tools which, when working together, grant a network/security administrator with detailed view over each and every aspect of his networks/hosts/physical access devices/server/etc..."

webografia

- http://www.linuxworld.com/news/2007/031207-top-5-security.html
  Top 5 open source security tools in the enterprise, Eric Hines
- http://ossec.net/ossec-docs/auscert-2007-dcid.pdf
  Log Analysis using OSSEC, Daniel Cid
- http://sectools.org/ids.html
  Top 5 Intrusion Detection Systems, Fyodor
- http://www.sage.org/pubs/12_logging/
  Building a Logging Infrastructure, Abe Singer, Tina Bird

- **Moottoori di ricerca**

webografia

LKM / kernel

- “Abuse of the Linux Kernel for Fun and Profit”, Phrack 50
- “Weakening the Linux Kernel”, Phrack 52
- “Sub proc_root Quando Sumus (Advances in Kernel Hacking)”, Phrack 58
- “Linux on-the-fly kernel patching without LKM”, Phrack 58
- “Indetectable Linux Kernel Modules”, SpaceWalker
- “(nearly) Complete Linux Loadable Kernel Modules”, Pragmatic
- 5 Short Stories about execve, Phrack 59
- Kernel Function Hijacking, Silvio Cesare
- Runtime Kernel KMEM Patching, Silvio Cesare
- Progetto Caronte, BFi 4
- oMBRa LKM, BFi 8
- KSEC & KSTAT, BFi 9
- HKS: Hacking Kernel Structures, BFi 11
- Kernel Hacking: Nuove Tecniche per l’Occultamento, BFi 11
- Smashing the Kernel for Fun and Profit, BFi 11abc

(GNU/Linux) Host Intrusion Detection

Domande?

(to be continued...)

CLUSIT Security Summit '09
26 marzo 09 - Milano

Relatore:

NETWORK enforcer SECURITY
Igor Falcomatà
Chief Technical Officer
ifalcomata@enforcer.it

Italian Security Mailing List
SIKUREZZA.ORG

< free advertising