Hardening&Armoring di un sistema informatico

Paolo PAVAN

anno 2002

Hardening e Armoring

- Sono termini che si riferiscono a tutte quelle procedure necessarie per irrobustire un sistema, superando le limitazioni e le insicurezze intrinseche che accompagnano l'installazione standard dei sistemi operativi.

Procedura di Hardening

- Sicurezza disica del Sistema (BIOS)
- Scelta dei software/pacchetti durante l'installazione
- Pianificazione e Sicurezza del Filesystem
- Controllo della password
- Controllo dell'ambiente di root (superuser)
- Gestione sicura degli utenti (accesso al sistema)
- Kernel Hardening
- Analisi delle vulnerabilità note (SANS Insitute)
- Applicazione delle patch
- Implementazione della Crittografia nel sistema
- Controllo della risorse del sistema
- Auditing del sistema: analisi dei log
- Auditing della rete: Intrusion Detection
- Portscan e penetration test
- Firewalling di un host
- Gestione e utilizzo dei Backup

Sicurezza fisica del Sistema (BIOS)

- E’ quella che si riferisce all’accesso fisico diretto al sistema:
  - sicurezza dei locali
  - Serrature per PC
  - Sicurezza del Bios
  - Sicurezza al boot

Scelta dei software/pacchetti durante l'installazione

- Nell'installazione dei sistemi vale una regola fondamentale:
  - "non installare mai software che non saranno utilizzati"
- Installare solo ciò che è espressamente necessario e non aggiungere servizi inutili e potenzialmente dannosi per la sicurezza.

Pianificazione e Sicurezza del Filesystem

- Valutare le necessità di spazio e pianificare con accuratezza le partizioni implementando se possibile:
  - Journaling Filesystem
  - Sistemi RAID (1 o 5)
  - Crittografia del filesystem

Controllo delle password

- Installare sistemi per la verifica della qualità della password:
- Impostare password sicure:
  - ⇨usare almeno 8 caratteri
  - ⇨usare caratteri maiuscoli e minuscoli
  - ⇨usare uno o più caratteri non alfanumerici
  - ⇨usare uno o più numeri
- Scadenza della password adozione di OTP

Controllo dell'ambiente di root (superuser)

- E' l'account più preso di mira sul sistema perché è quello che consente di effettuare sul sistema qualsiasi operazione.
- Utilizzare molta cautela quando si lavora come utente root
- Utilizzare sudo per emulare alcune funzioni di root.

Gestione sicura degli utenti (accesso al sistema)

- Implementazione di shadow password o PAM
- Inibire l'accesso console al sistema se possibile
- Monitorare gli accessi utente al sistema
- Impostare agenti automatici per il controllo delle attività degli utenti.

Disabilitazione e filtro dei servizi

- Disabilitare i servizi non utilizzati specie quelli critici per la sicurezza
- Impostazione di wrapper per limitare ad alcuni soggetti l'uso delle applicazioni sul sistema
- Monitoraggio completo di servizi ad accesso esterno
  - http e ftp
- Installazione di sistemi di rilevamento delle intrusioni (portscan).

Kernel Hardening

- Aggiornamento costante del kernel alla più recente release stabile
- Disabilitazione degli elementi inclusi non necessari
- Disabilitazione dei moduli per evitare LKM rootkit
- Installazione di patch per la sicurezza
  - Selinux
  - Grsecurety
  - Openwall
  - Lids

Analisi delle vulnerabilità note (SANS Insitute)

- Verifica delle versioni di kernel e degli applicativi installati
- Controllo del sistema installato con un portscanner o meglio un IDS
  - Nessus
  - Nmap
  - Vlad (SANS) e Vetes
- Verifica sulla base dei rapporti del SAN Institute.

Applicazione delle patch

- Applicazione di tutte le patch disponibili appena possibile
- Verifica della provenienza delle patch (checksum)
- Aggiornamento costante del sistema sia per i driver/Kernel che per i software (Apache/Web server, Sendmail/posta, Bind/DNS)

Implementazione della Crittografia nel sistema

- Installazione di sistemi sicuri per il controllo remoto tramite crittografazione dei dati in transito
  - SSH (Secure Shell)
- Uso di https: http+SSL
- Uso di stunnel/sslwrap per l'invio e la consultazione della posta
- Uso di PGP o certificati email
- Impostazione di connessioni in VPN (Ipsec o vtund)

Controllo della risorse del sistema

- Controllo delle risorse del sistema
- analisi dei carichi di lavoro:
  - memoria, dischi e processore
- analisi dei processi attivi
- verifica per attività sospette o carichi di lavoro fuori dalla norma.
- Monitoraggio delle sessioni in rete (netstat)

Auditing del sistema: analisi dei log

- Analisi degli eventi sul sistema:
  - controllo dei file di log
- Monitoraggio di:
  - attività di sistema basso livello (hardware-kernel)
  - attività di sistema alto livello: software e applicativi
  - utenti e accessi ai serivizi (http, ftp e posta)

Auditing della rete: Intrusion Detection

- Monitoraggio e registrazione degli accessi non autorizzati al sistema
- Attività di controllo attivo per tentativi di attacco (portsentry)
- Implementazione di un IDS in modalità di packet sniffer (snort sensor).

Portscan e penetration test

- Conduzione di scansioni per verificare i servizi attivi o le eventuali risposte dei servizi anti intrusione
- Esecuzione di approfonditi penetration test alla ricerca delle vulnerabilità dei servizi offerti.

Firewalling di un host

- Operazione di protezione di un host secondo la politica:
  - “Negare tutto e permettere solo ciò che è necessario”
- Attivare espliciti sistemi (software) per inibire l’accesso a parti del sistema evitare attacchi di tipo DoS e registrare operazioni anomale.
  - Abilitazione del firewall solo per pacchetti in ingresso di tipo non SYN (non si accettano nuove connessioni ma solo quelle in risposta alle nostre richieste con bit ACK attivo).

Gestione e utilizzo dei Backup

- Impostare sempre una corretta politica di backup, anche in presenza di sistemi RAID/Clustering
- Predisporre i corretti livelli di backup (totale o incrementale - pool di cassette)
- Predisporre le corrette procedure di gestione e conservazione delle cassette
- Preventivare delle prove di restore dei dati.