sicurezza dei sistemi

quadro d'insieme

	access control	**sicurezza file system**	**autenticazione e login**	**hardening, assessment**	**auditing**
platform independent	-	-	passwords attacchi a dizionario	metodologia nessus nmap	ids, hids logging log auditing
unix **linux**	diritti root e utenti, uid, euid, gid, egid	struttura del file system unix suid	passwd gruppi pam procedura di login	ispezione di un sisetma unix bastille sudo	syslog acct log auditing
windows	handles tokens sec. descr. SRM	NTFS	SAM, winlogon	MBSA security profiles forefront	event viewer

access control

- eseguito dal kernel quando un processo accede ad una risorsa
  - input:
    - credenziali processo
    - permessi della risorsa
    - tipo di accesso richiesto
  - risultato:
    - accesso concesso o negato
- windows e linux
  - i sistemi di permessi e credenziali di windows e linux realizzano Discretionary Access Control

access control nel filesystem

- controllo di accesso quando la risorsa è un file o una directory
- i meccanismi dipendono dal sistema operativo
  - qual'è il modello dei permessi che si possono associare ai file?
    - acl? limitazioni?
  - quando viene fatto il controllo di accesso?
    - all'apertura? ad ogni accesso?
- molto importante
  - gran parte dei dati risiedono su filesystem
  - in unix "tutto è un file"

autenticazione

- fase in cui si identifca l'utente e si crea il primo processo con le credenziali opportune
- il processo che fa l'autenticazione è privilegiato e può lanciare processi con le credenziali degli utenti

policy di autenticazione

- qualcosa che so
  - password, pin, ecc.
- qualcosa che ho
  - smart card, e-token, ecc.
- qualcosa che sono
  - impronte digitali, iride, retina, viso, impronta della mano, impronta vocale, keystrokes timing
- dove sono
  - solo nella sala controllo, sono nell’atrio della ditta

vulnerabilità di password e login

- account e password di default
- password ricavate da dizionari
  - attacchi on-line: autenticazione svolta dal normale programma di login
    - log, ritardi, max numero di errori
  - attacchi off-line
    - ad esempio su versioni criptate delle password
- tool standard per testare la vulnerabilità di una password
  - detti password cracker

klain's easy-to-guess passwords

1. Passwords based on account names
   - Account name followed by a number
   - Account name surrounded by delimiters
2. Passwords based on user names
   - Initials repeated 0 or more times
   - All letters lower-or uppercase
   - Name reversed
   - First initial followed by last name reversed
3. Passwords based on computer names
4. Dictionary words
5. Reversed dictionary words
6. Dictionary words with some or all letters capitalized
7. Reversed dictionary words with some or all letters capitalized
8. Dictionary words with arbitrary letters turned into control characters
9. Dictionary words with any of the following changes: a 2 or 4, e 3, h 4, i 1, l 1, o 0, s 5 or $, z 5.
10. Conjugations or declensions of dictionary words
11. Patterns from the keyboard
12. Passwords shorter than six characters
13. Passwords containing only digits
14. Passwords containing only uppercase or lowercase letters, or letters and numbers, or letters and punctuation
15. Passwords that look like license plate numbers
16. Acronyms (such as "DPMA," "IFIPTC11," "ACM," "IEEE," "USA," and so on)
17. Passwords used in the past
18. Concatenations of dictionary words
19. Dictionary words preceded or followed by digits, punctuation marks, or spaces
20. Dictionary words with all vowels deleted
21. Dictionary words with white spaces deleted
22. Passwords with too many characters in common with the previous (current) password

proactive password selection

- si costringe l'utente a scegliere buone passwords
  - es. quando l'utente aggiorna la password si fa girare un password cracker ed eventualmente si rifiuta la password
- passwords lunghe, complesse, cambiate di frequente
  - gli utenti vedono i vincoli come un problema
    - passwords scritte sotto la tastiera o sul monitor
  - si deve trovare un compromesso anche in base alla criticità dell'account e al tipo di utenti

vulnerability assessement

- studio per individuare quali vulnerabilità sono presenti in un sistema
- automatizzato
- strumenti con database di vulnerabilità
  - il db, per ogni pacchetto software e relativa versione, fornisce le vulnerabilità note
- effettivo solo per vulnerabilità già ben note
- le vulnerabilità ben note costituiscono il pericolo maggiore
  - perché chiunque ne conosce l'exploit (via Internet)

vulnerability scanners

- nmap
  - scanning delle porte
  - versione OS, uptime
- nessus
  - scanning delle porte
  - identificazione delle versioni dei server
  - matching su un db di vulnerabilità
  - check “locale” con login ssh
- tiger
  - verifica configurazioni e stato del sistema dall’interno
- http://sectools.org/vuln-scanners.html

hardening

- attività che consiste nel configurare una macchina in modo che sia difficile da espugnare
- prevede principalmente
  - agire sulla configurazione di sistema, servizi, applicazioni, utenze, privilegi, ecc.
- tipicamente abbinata a...
  - dei sistemi di log auditing
  - una corretta politica di mantenimento

hardening: metodologia e strumenti

- l'hardening richiede grosse competenze tecniche e un aggiornamento costante rispetto alle minacce
  - basato spesso su "best practices"
- un hardening efficace è molto difficile fare manualmente
- si usano strumenti automatici che guidano la configurazione di un sistema hardened

hardening: gruppi e utenze

- avviare solo le utenze strettamente indispensabili appartenenti alle seguenti categorie
  - user accounts (gli utenti)
  - system accounts (account per amministrazione)
    - molto pericolosi (es. root)
    - preferibilmente non accessibili dall'esterno
  - application accounts
    - particolari system accounts con privilegi limitati
- bloccare il login di tutti gli account che non fanno capo ad una persona
- se ci sono più persone che devono compiere operazioni privilegiate usare il meccanismo dei gruppi

hardening: servizi

- solo i servizi strettamente indispensabili
- meno servizi ? meno vulnerabilità
- attenzione maggiore a servizi di rete
- per i servizi rimasti considera...
  - ... di far girare un servizio con una utenza limitata
    - cioé un application account
  - ... jailing (vedi nel seguito) se possibile
  - ... considera il serivizio come “critico” e applica una politica adeguata
    - monitorare in maniera stringente i relativi security alert
    - tempestività nell'applicare le patch di sicurezza

hardening: servizi privilegiati

- i servizi/comandi privilegiati utilizzabili dall'utente sono pericolosi
- spesso il software gira con diritti maggiori rispetto a quelli dell'utente che lo usa
  - server (web, email, ecc.) permettono a "utenti remoti" di effettuare operazioni sul sistema in cui gira
  - programmi con diritti privilegiati (passwd, ping, ecc.) permettono di effettuare operazioni normalmente non ammesse per l'utente comune

hardening: servizi privilegiati

- le credenziali dei processi permettono di eseguire operazioni relative al servizio... e potenzialmente molto altro
  - es. un web server può girare come root o nobody
- non possiamo fidarci del server (o dei programmatori)
  - bugs (es. buffer overflow)

hardening: servizi privilegiati

- è veramente necessario tali servizi/comandi siano privilegiati?
  - considerare l'uso di un application account con privilegi limitati
  - considera l'uso di wrapper di sicurezza che verificano e limitano gli input a tale comando/servizio
    - richiede programmazione, tipicamente in C

hardening: schema di un wrapper

Initialize string constants such as the full path to the real program, maximum string lengths, the allowed character mask, and the allowed environment variable list

Check that an environment exists (used by interactive programs)

Check that USER & uid can be found in user db (paranoid option)

For i=1 to argc

- rewrite each character using a character mask
- if string length > predetermined value, error out

For i=1 to length of envp

- drop any variable not in predetermined list
- rewrite each character using a character mask
- if string length > predetermined value, error out
- if variable is suppose to be the user name but isn't, error out (paranoid option)

Create the new environment variable array

Execve real program with new environment and safe argument strings

hardening: permessi

- Elimina, se possibile, file e directory scrivibili da tutti gli utenti
  - sono fonte di potenziali interferenze tra gli utenti
  - questo controllo dovrebbe essere fatto periodicamente
    - si può usare un IDS come tripwire per questo (vedi seguito)

hardening: security patches

- kernel, software di sistema e applicazioni sono sicuramente affetti da bug di sicurezza
  - un bug diventa problematico solo dopo che ne viene diffusa l'esistenza
- applicazione di pach di sicurezza o upgrade
  - fondamentale la tempestività rispetto all'annuncio
- la patch potrebbe tardare ad apparire, nel frattempo considera...
  - spegnimento del servizio
  - riduzione dei privilegi
  - wrapping

hardening: security patches

- per software open la patch è spesso più rapida da ottenere ma richiede la ricompilazione dell'applicazione
  - la preparazione di un pacchetto binario che include la patch può richiedere tempo
  - la compilazione di un pacchetto software può richiedere un po' di esperienza di programmazione C
- per software proprietari possiamo solo confidare nel vendor per una patch binaria

hardening: log auditing periodico

- attivare meccanismi di auditing che permettano di avere una verifica continua nel tempo
  - log auditing come logwatch, lire, swatch, logsurf
  - Intrusion Detection Systems

logging

- attività di registrazione di eventi relativi a...
  - comportamento degli utenti
  - servizi
  - applicazioni
  - anomalie
  - ecc.
- la registrazione degli eventi è sollecitata
  - dai processi che implementano servizi o applicazioni
  - dal kernel in presenza di anomalie o eventi particolari

logging e policy

- è necessario proteggere i log da manomissioni
  - obiettivo di un hacker è quello di essere invisibile quindi spesso sono oggetto di modifica
- una buona politica di sicurezza dovrebbe…
  - proteggere l'integrità dei log
    - monitoraggio della taglia, compressione, rotazione, consolidation in un log server, protezione dalla scrittura (hardening del log server).
  - far sì che vengano loggati tutti gli eventi "**interessanti**"
    - accurata configurazione del logging
  - far sì che le informazioni "**critiche**" contenute nei log vengano prontamente comunicate all'amministratore perché possa prendere adeguate misure reattive
    - log auditing

log auditing

- una attività di verifica periodica dei log in modo da individuare tentativi di intrusione
- il log auditing “a occhio” è improponibile
- tools automatici di reporting periodico
  - scanning periodico delle nuove righe dei log (a partire dall'ultimo scan)
  - email con report
  - possibilità di fare scanning su log da varie fonti
    - es. web server, firewalls, ecc.
- tool automatici di analisi “al volo”
  - monitor costante dei file di log e analisi delle nuove linee
  - **azione reattiva tempestiva**

problemi del log auditing

- tutti gli strumenti basati su regole vanno “tarati” per le esigenze del caso
  - appena installato le configurazioni di default daranno falsi postivi e falsi negativi
- la taratura...
  - richiede risorse umane
    - la taratura viene fatta da un “amministratore”
  - complessa e quindi può contenere errori
  - si basa sull'esperienza e quindi richiede tempi lunghi
    - il sistema non sarà efficace sin da subito

IDS
intrusion detection systems

- un sistema hw/sw in grado di rilevare un utilizzo non autorizzato delle risorse di un sistema informatico
- obiettivi
  - tempestività nella rilevazione dell'intrusione
  - accuratezza nella rilevazione dell'intrusione
    - nessuno o pochi falsi positivi
    - nessuno o pochi falsi negativi (più pericolosi!)
  - semplicità di configurazione
  - eventuale risposta immediata all'attacco

host based IDS (HIDS)

- verifica l'integrità di file critici o la presenza di processi estranei in esecuzione su un sistema
- verifica periodicamente
  - non è una verifica in “tempo reale”
- uso di funzioni hash e regole
- necessario un aggiornamento delle conoscenze dell'IDS quando il sistema viene aggiornato

IDS e configurazioni

- le regole (policy) secondo cui un IDS rivela sono configurabili
- la configurazione di un IDS deve essere adeguata all'uso che si fa del sistema
  - in un sistema su cui si creano frequentemente nuove utenze è noioso avere un controllo sul file /etc/passwd
    - falso positivo
  - molti falsi positivi rendono difficile individuare nei log i veri attacchi

IDS e configurazioni

- ma configurazioni troppo lasche possono non rilevare una intrusione!
  - in un sistema su cui si creano frequentemente nuove utenze è noiso avere un controllo sul file /etc/passwd ma un hacker spesso crea un sua utenza
    - falso negativo

IDS statistici (anomaly detection)

- gli IDS statistici si avvalgono di meccanismi di apprendimento
- non richiedono configurazione
- considerano legittimo il comportamento standard della rete o di un utente

- comportamento difficilmente prevedibile
- alto numero di falsi positivi
- a fronte di falsi negativi è difficile modificare il comportamento dell'IDS
- considerati poco affidabili
- sono diffusi IDS ibridi (statistici+regole)

ids e antivirus

- un antivirus è un sistema integrato di rilevamento delle intrusioni
  - periodicamente controlla il filesystem
  - blocca la chiamata a particolari system call
  - verifica il traffico di rete (network ids/fw)
  - effettua altre verifiche specifiche per i virus
    - comportamenti anomali degli eseguibili (es. automodifica per i virus mutanti)