Vulnerability Assesment e hardening

Automatic vulnerability assesment

- studio automatizzato per individuare quali vulnerabilità sono presenti in un sistema: **configurazioni o bug software**
- caratteristiche
  - altamente automatizzato, fino alla creazione dei report
    - intervento umano limitato
  - eseguito su base periodica
  - efficace **solo per vulnerabilità già ben note per prodotti diffusi e per errori di configurazione tipici**
  - **inefficace per software custom**
  - poco costoso (rispetto al penetration test)
- strumenti con **database di vulnerabilità**
  - il db, per ogni software e relativa versione, fornisce le vulnerabilità note
- **le vulnerabilità ben note costituiscono il pericolo maggiore**
  - perché l'exploit è noto

Automatic vulnerability assesment

- studio automatizzato per individuare quali vulnerabilità sono presenti in un sistema: **configurazioni o bug software**
- caratteristiche
  - altamente automatizzato, fino alla creazione dei report
    - intervento umano limitato
  - eseguito su base periodica
  - efficace **solo per vulnerabilità già ben note per prodotti diffusi e per errori di configurazione tipici**
  - **inefficace per software custom**
  - poco costoso (rispetto al penetration test)
- strumenti con **database di vulnerabilità**
  - il db, per ogni software e relativa versione, fornisce le vulnerabilità note
- **le vulnerabilità ben note costituiscono il pericolo maggiore**
  - perché l'exploit è noto

Manual vulnerability assessment

- Manual vulnerability assessment refers to the process of evaluating the security vulnerabilities in a system, network, or application.
- In other words, the process of finding vulnerabilities or potential vulnerabilities
- Main tasks:
  - Check running processes and services
  - Check filesystem and process permissions
  - Check users' permissions
  - Network check
    - Open ports
    - Firewall
  - Log check

Hardening

- Hardening in the context of cybersecurity refers to the process of securing a system by reducing its surface of attack
- This involves mitigating potential security risks to make the system more resistant to attacks.
  - The security risks are discovered by the vulnerability assessment
- Hardening can include measures like updating software to remove known vulnerabilities, configuring security settings to eliminate unnecessary functions or services, strengthening password policies, applying security patches, and implementing network security controls.
- The goal of hardening is to make it more difficult for attackers to exploit vulnerabilities in a system, thereby improving its overall security posture.

Hardening

- In other words, the goal of hardening is to fix the problems discovered by the vulnerability assessment
- Main tasks are about:
  - Services
    - Ensuring that only critical services are running
    - Securing configurations
  - Firewall configurations
  - Patch the source code
  - Updates
    - In some cases, a simple upgrade of the operating system can patch vulnerabilities

hardening: metodologia

- Basic Principles
  - Simplicity
  - Open Design
  - Compartmentalization
  - Minimum Exposure
  - Least Privilege
  - Minimum Trust and Maximum Trustworthiness
  - Secure, Fail-SafeDefaults
  - CompleteMediation
  - NoSinglePointofFailure
  - Traceability

hardening: azioni tipiche

- eliminare utenze, gruppi, servizi, eseguibili inutili
- minimizzare i diritti di utenze, gruppi, servizi, eseguibili
- isolare servizi, utenze e risorse mediante permessi DAC, permessi MAC, containerizzazione, virtualizzazione
- proteggere eseguibili critici mediante wrapping per filtrare input non fidati
- proteggere servizi critici mediante firewall e proxy applicativi
- adottare adeguate politiche di patching, logging, auditing

hardening: wrapping

- è un software per filtrare gli input ad un processo prima che arrivino a questo
  - esso stesso lancia il processo che non deve poter essere lanciato direttamente dagli utenti non fidati
- richiede programmazione, tipicamente in C
  - prima considerare alternative standard di confinamento e minimizzazione dei privilegi
  - considerare l'uso di sudo, è una sorta di wrapper generico

hardening: strumenti

- un hardening efficace è molto difficile fare manualmente
- si usano **strumenti automatici** che guidano/suggeriscono la configurazione del sistema
- tools famosi
  - lynis
  - bastille (obsoleto)
  - MBSA

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 scoperta l'esistenza
- applicazione di patch 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
- 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 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.
- es. logwatch

SIEM: Security Information Event Manager

- il log auditing è ora parte di prodotti integrati: i SIEM
- integrano
  - collezionamento da moltissime fonti (scalano)
  - motore di correlazione di eventi
  - regole puntuali o statistiche per sollevare allarmi
  - strumenti di analisi (business intelligence)
  - Programmabilità
  - gestione incidenti
- costo non trascurabile
  - di acquisizione e di gestione
- MSSP: Managed Security Service Provider
  - servizi che forniscono funzionalità SIEM outsourced
- Wazuh!