17 - Intrusion Detection and Cyber Forensics

Un intrusione può essere definita come:

- un insieme di azioni che tentano di compromettere l'integrità e confidenzialità di una risorsa

Intrusion detection e response

Problemi:

- le minacce sono interne ed esterne
- i log del firewall non sempre avvisano sulle intrusioni
- intrusion detection è una linea di difesa necessaria
- IDS deployment customization e management è generalmente non trivial

Intrusion detection

preso dal CERT:

- esaminare i log alla ricerca di connessioni unusuali
- cercare setuid e getuid file ovunque nel sistema
- verificare i binari di sistema per essere sicuro che non siano stati alterati
- verificare accessi non autorizzati a sistemi di monitoraggio della rete (sniffer o packet sniffer)
- esaminare tutti i file avviati da "cron" e "at"
- verificare servizi non autorizzati (verificare che /etc/inetd.conf non abbia modifiche aggiuntive)
- esaminare /etc/passwd e verificare che non siano state fatte modifiche
- verificare che i file di configurazione di sistema e di rete non abbiano subito modifiche
- controllare ovunque nel sistema per file strani o invisibili

Intrusion detection systems

Un intrusion detection system è un software o hardware il cui compito è avvisare se sono avvenute intrusioni
Falsi positivi:

- qualcosa di strano accaduto ma non è un intrusione
  Falsi negativi:
- intrusione attiva ma l'IDS non la nota
- sistema compromesso

L'obiettivo dei IDS è di minimizzare i falsi positivi ma spesso avere pochi falsi positivi implica tanti falsi negativi (e viceversa)

Caratteristiche di un buon IDS

- deve poter funzionare senza supervisione umana
- non deve essere una black box
- deve essere fault tolerant
- deve resistere alle sovversioni
- deve imporre minimo overhead nel sistema
- deve essere facile da accordare al sistema in questione
- deve adattarsi quando nuove applicazioni vengono aggiunte.

Gli IDS sono basati su modelli di intrusione:

- misuse detection: l'IDS rileva le intrusioni guardando le attività le attività che corrispondono a tecniche di intrusione conosciute o vulnerabilità di sistema
- anomaly detection: il sistema rileva le intrusioni guardando le attività diverse dal comportamento medio dell'utente o sistema

Modelli di intrusione

Misuse intrusion:

- tipicamente segue pattern molto conosciuti e può essere rilevato tramite pattern detection tramite pattern matching
- esempio: un tentativo di creare un setuid file è trovabile esaminando i log dei messaggi
  Anomaly intrusion:
- le intrusioni sono rilevate osservando deviazioni significative da un "comportamento normale"
- il modello di "comportamento normale" è derivato dall'analisi delle operazioni "normali" sul sistema.
- es: average cpu load, numero di connessioni ecc.
  Modelli più complessi:
- reti neurali
- machine learning

Anomaly vs Misuse Detection

- Misuse detection:
  - basso numero di falsi positivi, abbastanza veloce e reliable
  - impossibile rilevare attacchi "nuovi"
- Anomaly detection
  - flessibile, può migliorare le sue performance
  - difficile identificare i dati da monitorare
  - richiede training dell'applicazione

Caratteristiche degli IDS

Basati sull'origine dei dati:

- host based: audit data di un singolo host sono usati per rilevare le intrusioni
- multi-host based: audit data di molti host
- network based: network traffic data, assieme a audit data di uno o più host

Host based IDS

- tipicamente monitora sistemi, eventi e security logs
- controlla file chiave di sistema e eseguibili importanti.
- si possono usare regular expression per definire firme

Network based IDS

- analizza i pacchetti di rete
- usa un network adapter per analizzare tutto il traffico in tempo reale
- pattern o bytecode matching
- threshold crossing
- statistical anomaly detection

Vantaggi degli Host-based IDS:

- possono verificare il successo o fallimento degli attacchi
  - log verification
- monitorano specifiche attività:
  - logon/logoff activity
  - account changes
  - policy changes
- rileva attacchi che i network based IDS possono aver missato
  - keyboard attack
  - brute-force login

Vantaggi dei network-based IDS:

- lower cost of ownership
  - utilizza meno punti di detection
  - più gestibile e meno intrusivo
- rileva attacchi che gli host based systems possono missare
  - ip based dos
  - packet payload content
- più difficile rimuovere prove per un attaccante

    - usa live network traffic
    - cattura il traffico di rete
- real time detection e response
    - può fermarsi prima che il danno sia fatto
- operating system independence
    - non richiede informazioni sull'OS target
    - non deve aspettare che gli eventi vengano loggati
    - non impatta il target

Network based IDS placement

Possibile piazzamento dei network based IDS:

- fuori la DMZ, può vedere i tentativi bloccati dal firewall

Honeypot

Sono server esca o sistemi impostati per raccogliere informazioni sugli attaccanti
Sono impostati per essere facili prede per gli intrusori in confronto ai sistemi in production ma con minori modifiche in modo da loggare le attività
L'obiettivo è capire come gli intrusori cercano di guadagnare l'accesso ai sistemi

I sistemi honeypot devono apparire più generici possibile:

- limitare il traffico che gli intrusori possono mandare indietro tramite internet cosi che l'honeypot non diventi un trampolino di lancio di attacchi.
- rendere l'honeypot interessante aggiungendo dati falsi ma interessanti

Tipi di honeypot

- low interaction honeypot: abilita solo poche interazioni con un attaccante
    - tutti i servizi sono emulati
    - non vulnerabile di per se
    - meno efficace a tracciare le informazioni
- high interaction honeypot: uso del servizio o software davvero vulnerabile
    - soluzione complessa (vero OS e applicazioni)
    - un immagine di un intrusione più precisa
    - aiuta a identificare vulnerabilità sconosciute
    - prono a infezioni
    - rischio maggiore, può essere usato come attaccante