An Introduction to Intrusion Detection System

Agenda

- **Vulnerabilità dei Sistemi**
- **Intrusion Detection System**
  - Modello
  - Requisiti
  - Monitoring
  - Tipi di Analisi
- **Tipi di Attacchi**
- **Descrizione di alcuni IDS**

Definizioni

Nei sistemi di computer nel termine **sicurezza** vengono racchiusi tre significati distinti:

•**Segretezza** – un sistema sicuro non deve permettere che informazione riservata sia accessibile a persone non autorizzate.

•**Integrità** – un sistema sicuro deve mantenere l'integrità dei dati che in esso vengono conservati.

•**Disponibilità** – un sistema sicuro deve rendere disponibile l'informazione ai suoi utenti autorizzati in ogni momento.

Introduciamo alcuni termini:

•**Security policy** – Una **politica di sicurezza** è l'insieme di leggi, regole e pratiche che regolamentano le modalità con cui una qualsiasi organizzazione gestisce, protegge e distribuisce i propri servizi e le proprie informazioni.

•**Vulnerability** – Una **vulnerabilità** è un punto in cui il sistema è suscettibile di attacco, una debolezza che può essere sfruttata.

•**Threat** – Una **minaccia** è un possibile pericolo per il sistema, una potenziale violazione della sicurezza.

•**Attack** – Un **attacco** è un *minaccia intenzionale*, una azione eseguita allo scopo di violare la sicurezza.

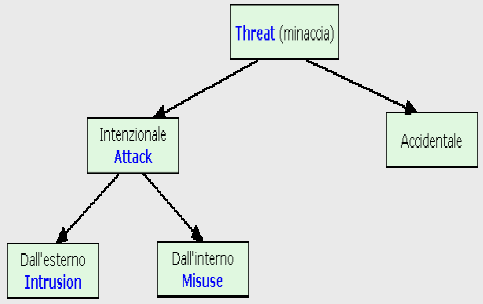
Un attacco può dividersi in intrusioni e abusi:

•**Intrusion** – Una **intrusione** è un attacco intenzionale ad un sistema (tipicamente un sistema di rete) portato *dall'esterno*.

•**misuse** – Un **abuso** è un attacco derivante da un inappropriato utilizzo dei propri permessi in un sistema. In sostanza indica un attacco portato dall'*interno.*

•**Penetration** – una penetrazione è un attacco che ha successo.

Tipologia degli attacchi:



Vulnerabilità dei sistemi

Di seguito verranno presentate alcune vulnerabilità che riguardano i protocolli di comunicazione:

Attacchi passivi

•Attacco denominato ***sniffing*** (o snooping): consiste nello spiare il traffico altrui che attraversa un elemento della rete.

Attacchi attivi

•Attacchi al ***routing*** - viene cambiato in modo illecito il corretto indirizzamento di una porzione del traffico di rete.

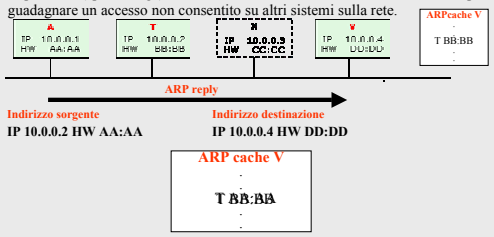
•Attacchi di tipo ***spoofing***: l'hacker dialoga con un server spacciandosi per un client autorizzato (es. *address masquerading*, attacco a 3-way handshake).

•***Denial of service*** - negazione di un servizio (in questo caso di comunicazione) offerto: un esempio è l'attacco *TCP SYN flood.*

Esempi:

ARP cache poisoning:

Permette ad una macchina su una rete locale di fingersi un'altra (sulla stessa LAN). Inquinando ("poisoning") la ARP cache della macchina vittima, un intruso potrebbe guadagnare un accesso non consentito su altri sistemi sulla rete.



Te

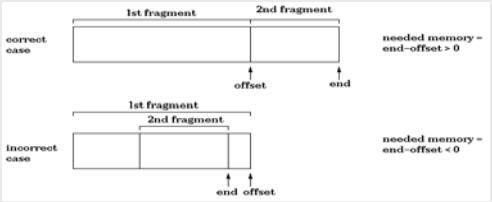
•f1.ident = f2.ident (f1 e f2 frammenti di uno stesso datagram)

•f1.offset < f2.offset

•f2.offset + f2.length < f1.offset + f1.length

Teardrop è il nome dato ad una vulnerabilità dell'algoritmo di riassemblaggio dei frammenti in un unico datagram in Linux.

Questa vulnerabilità permette ad un attaccante remoto di mandare in crash un sistema linux semplicemente spedendo due frammenti IP costruiti ad arte.



Fragment Overrun (Ping of Death)

•*Fragment overrun* è una vulnerabilità nel sistema di riassemblaggio del protocollo IP.

•Causa il crash del sistema oppure un reboot.

•L'attacco è quindi di tipo *Denial of Service*.

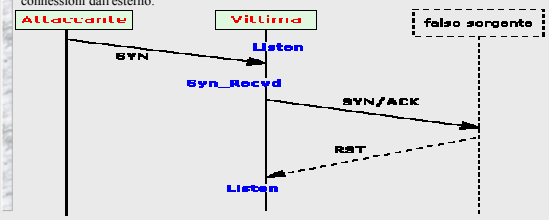
Un attacco di tipo *fragment overrun* spedisce un flusso di pacchetti, frammenti di un IP datagram, costruiti ad arte: questi pacchetti, una volta riassemblati, daranno un datagram più grande dei 65545 bytes permessi come lunghezza massima.

SYN Flood

•Questa è una vulnerabilità presente in molte implementazioni del protocollo TCP.

•Sfrutta il procedimento di instaurazione della connessione (il cosiddetto sistema *3-way handshake*).

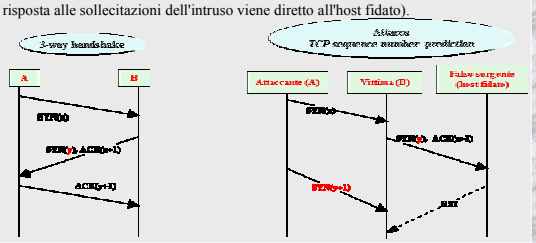
•Può causare una negazione di servizio (attacco DoS), inibendo quel sistema dall'accettare altre connessioni dall'esterno.



TCP sequence number prediction

•Vulnerabilità che permette di instaurare una connessione TCP con un host vittima fingendosi un host fidato.

•Questo permette di poter effettuare un *blind attack* (dal momento che il traffico di risposta alle sollecitazioni dell'intruso viene diretto all'host fidato).



Intrusion Detection System

Intrusion detection è una tecnologia per la sicurezza che:

•Cerca di identificare e isolare "intrusioni" verso i sistemi computerizzati.

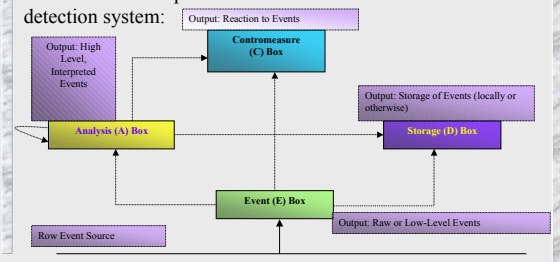
•Complementa le altre tecnologie di sicurezza (firewall).

•Rilevare e notificare attacchi espliciti

•Notifica dei nuovi attacchi imprevisti.

Modello:

Il Common Intrusion Detection Framework (CIDS) definisce un insieme di componenti che insieme definiscono un intrusion detection system:

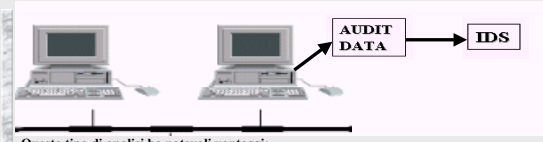


Requisiti:

Verranno elencati di seguito i requisiti base di un buon intrusion detection system:

1. Un sistema deve riconoscere qualsiasi attività o evento sospetto che potrebbe potenzialmente essere un attacco.
2. Il comportamento di un intruso dovrebbe essere rilevato al più basso livello possibile.
3. Il sistema deve essere in grado di adattarsi ai cambiamenti dei metodi di un attacco.
4. Il sistema deve essere in grado di manipolare attacchi multipli.
5. Il sistema deve essere scalabile e facilmente aggiornabile per rispecchiare i cambiamenti della rete.
6. Il sistema stesso deve in grado di proteggersi dagli attacchi.
7. Il sistema deve essere efficiente ed affidabile.

Approcci: Host based



Questo tipo di analisi ha notevoli vantaggi:

•può essere monitorata ogni attività del tipo "*chi* è acceduto a *cosa*";

•può essere investigato il comportamento di un determinato utente o di una risorsa protetta;

Ma questi IDS soffrono anche di molti difetti:

•La attività di rete non è visibile;

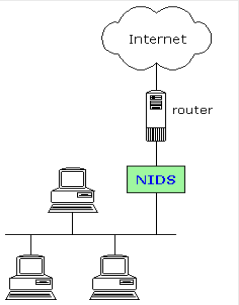
•sono fortemente dipendenti dalla piattaforma sulla quale risiedono e della quale analizzano l'attività;

•sono esposti alle vulnerabilità del sistema operativo dell'host ospite.

Network based

•Spostano la fonte di informazione dal sistema (o insieme di hosts) alla infrastruttura di rete (in figura).

•Viene infatti monitorato il traffico di rete, alla scoperta di possibili tracce di intrusioni.



Tipi di analisi:

- **Anomaly detection**
- **Misuse detection**
- **Systems integrity verifiers (SIV)**
- **Honeypots systems**

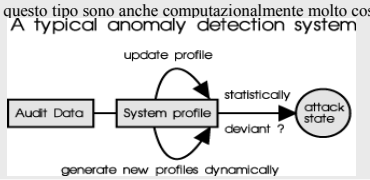
Anomaly detection

Assumono che tutte le attività intrusive sono necessariamente anomale.

Sistemi che adottano una tecnica di *anomaly detection* compiono in sostanza una analisi statistica per trovare scostamenti da un comportamento base.

Il rilevamento può essere effettuato in real-time, oppure off-line, ispezionando i log files accumulati.

Sistemi di questo tipo sono anche computazionalmente molto costosi.



Questi sistemi hanno il vantaggio di poter rilevare **nuovi** attacchi singoli o cooperativi.

Hanno, però, anche il seguente problema:

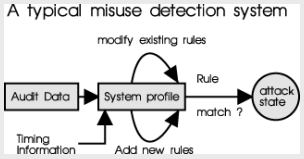
Falsi positivi: attività anomale che non sono intrusive ma che vengono rilevate come tali.

Falsi negativi: attività intrusive che non sono anomale e che quindi non vengono rilevate.

Misuse detection

L'idea dietro a questi sistemi è che esistono modi di rappresentare attacchi sottoforma di una "traccia" (o signature) lasciata all'interno del sistema.

Questo significa che, come i ben noti antivirus, possono rilevare alcuni o tutti gli attacchi noti, mentre possono poco o nulla contro quelli sconosciuti.



Pattern matching – si effettua un algoritmo di matching alla ricerca si signature all'interno dei pacchetti che fanno match con una regola contenuta nel database.

Systems integrity verifiers (SIV)

Un sistema di questo tipo ispeziona i files di sistema trovando quando un intruso (una persona non autorizzata) opera su di essi delle modifiche. Sistemi di questo tipo spesso fanno un forte utilizzo di sistemi crittografici, come l'uso di *message digest* che possono rilevare anche i più piccoli cambiamenti. Il più famoso di questi sistemi è **Tripwire.**

Honeypots systems

Detti anche ***sistemi trappola*** i quali contengono degli pseudo-servizi, il cui scopo è quello di emulare vulnerabilità ben note al solo fine di scovare ed "intrappolare" gli intrusi.

Tipi di Attacchi

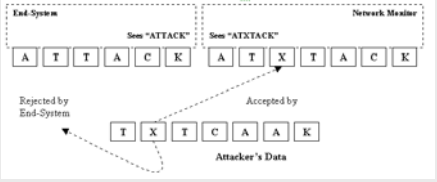
Discuteremo di tre differenti tipi di attacchi verso un network IDS sniffer-based:

- Insertion
- Evasion
- Dos

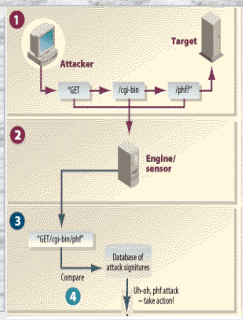
Insertion

Un IDS può accettare un pacchetto che un end-system rigetta.

Un intruso può usare quest'attacco per superare l'analisi della firma, permettendogli di far scivolare attacchi passato un IDS.

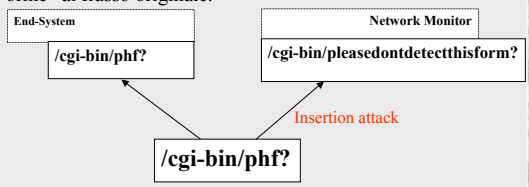


Esempio:



1. Rappresenta l'invio di una richiesta "GET/cgi-bin/phf?"
2. La richiesta viene catturata dall'IDS.
3. La richiesta, dopo essere stata ricostruita, viene confrontata con un database di signature alla ricerca di un match.
4. Reazione all'attacco.

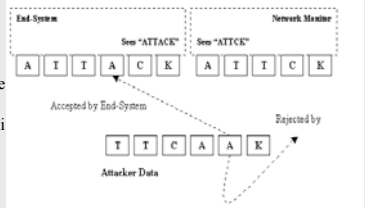
L'intruso trasmette la stessa richiesta a un webserver, ma forza l'IDS a vedere un stringa diversa, come "GET /cgi-bin/pleasedontdetectthisform?". L'intruso ha usato un attacco di tipo insertion per aggiungere "leasedontdetectt", "is", e "orme" al flusso originale.



Evasion

Un end-system può accettare un pacchetto che un IDS rigetta. Un IDS può erroneamente scartare tale pacchetto perdendo interamente il suo contenuto. Questi pacchetti stanno "evadendo" l'indagine accurata effettuata da un IDS.

L'intruso trasmette porzioni della stessa richiesta in pacchetti che l'IDS erroneamente scarta, permettendogli di rimuovere parte del flusso dalla vista di un IDS.



Attacchi Denail of Service

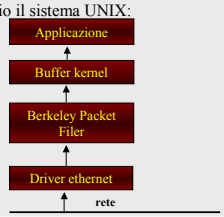
Parlare di attacchi DoS verso gli IDS significa parlare di:

- Esaurimento delle risorse CPU
- Esaurimento della memoria
- Abusare della reattività degli IDS

Esaurimento delle risorse CPU

Lo scopo consiste nell'impedire all'IDS la sorveglianza della rete. Un IDS con risorse CPU esaurite non elaborerà i pacchetti catturati abbastanza velocemente e, non appena questi pacchetti riempiono il buffer del sistema operativo, i dati catturati cominciano ad essere rifiutati o scartati.

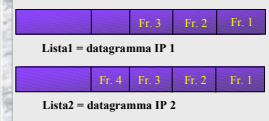
Prendiamo come esempio il sistema UNIX:



Esempio: Frammentazione IP

Per facilitare il riassemblamento, la maggior parte dei sistemi memorizzano i frammenti nell'ordine in cui i loro dati appariranno nel pacchetto finale.

Molti sistemi usano una semplice lista ordinata per memorizzare i frammenti in arrivo.



Un aggressore può trasmettere una gran quantità di traffico usando i più piccoli frammenti possibili – gran quantità di cicli CPU saranno consumati per mantenere traccia di questi minuscoli frammenti IP.

Esaurimento della memoria

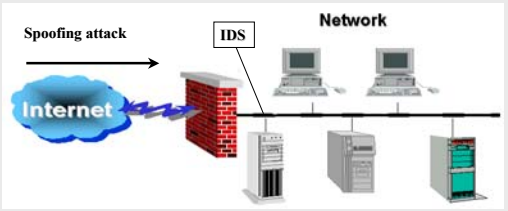
Gli IDS richiedono ovviamente memoria per operare. Un aggressore che può forzare un IDS a consumare tutte le risorse di memoria disponibili può rendere il sistema non operativo.

Esempi di allocazioni di memoria attaccabili includono:

- il TCB teardown di TCP
- il riassemblamento TCP

Abusare della reattività degli IDS

In alcune circostanze, l'IDS stesso può diventare uno strumento di attacchi denial of service. Se l'IDS possiede delle capacità di contromisure reattive, ed è vulnerabile ad attacchi che creano falsi positivi, può essere forzato a reagire agli attacchi che in realtà non sono avvenuti.



Descrizione di alcuni IDS

Verranno presentati tools di ricerca come:

- Emerald
- NetStat
- Bro

Prodotti commerciali come:

- RealSecure

E prodotti open-source come:

- Snort

Emerald

Emerald (Event Monitoring Enabling Responces to Anomalous Live Disturbances) rappresenta un intrusion detection che associa entrambe le tecniche di monitoring, ossia *anomaly detection* (deviazioni dal normale comportamento del sistema) e *misuse detection* (signature note di attacchi).

L'approccio gerarchico fornisce tre livelli di analisi effettuato da tre sistemi di monitor :

- ***Service monitors*****:** effettua il rilevamento a livello di componenti individuali e servizi di rete all'interno di un dominio, operazioni di log, ed effettua analisi statistiche e di signature locali.
- ***Domain monitors***: integra le informazioni dei service monitors per fornire una vista delle intrusioni a livello domain-wide.
- ***Enterprice monitors***: effettua analisi inter-domain per rilevare minacce da una prospettiva globale.

NetStat

NetStat esplora l'uso dell'analisi a *transizione di stato* per effettuare rilevamenti in real-time.

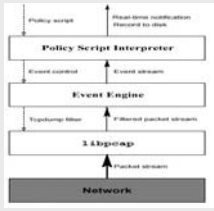
Componenti:

- ***Preprocessore***: filtra e manipola i dati in una forma che sia indipendente dall'audit-file.
- ***Una base di conoscenza*** (che include una base di fatti e di regole): le regole memorizzano le regole per le transizioni di stato che rappresentano sequenze predefinite di intrusioni, mentre i fatti memorizzano i cambiamenti di stato del sistema dinamicamente in base alla possibile intrusione.
- ***Un motore inferenziale***: identifica qualunque cambiamento di stato significativo ed aggiorna la base dei fatti. Inoltre notifica al decision engine una possibile violazione della sicurezza.
- ***Decision engine***: notifica all'amministratore di sistema circa gli eventi significativi o intraprende un'azione in risposta ad un tentativo di intrusione.

Bro

Bro è un toll di ricerca sviluppato dalla Lawrence Livemore National Laboratory. È stato sviluppato, in parte, per esplorare le problematiche sulla robustezza degli IDS, valutando quali caratteristiche rendono un IDS capace di resistere ad attacchi diretti ad esso stesso.

Architettura:



RealSecure

RealSecure rappresenta un IDS che opera in real-time. Usa un'architettura a tre livelli costituita dalla seguenti componenti:

- ***Network-based recognition engine***: gira su workstation dedicate ed effettua rilevamenti di intrusi e contromisure a livello di rete.
- ***Host-based recognition engine***: analizza i log fornito dall'host ospite per riconoscere attacchi e determinare se l'attacco ha avuto successo o meno.
- ***Administrator's module***: è una console di gestione che riceve tutti report generati dagli engine e monitora lo stato di ciascuno per una semplice gestione e configurazione.