

ANALISI DEGLI STRUMENTI E DELLE TECNICHE PER L'IDENTIFICAZIONE DELLE INTRUSIONI

Analysis of intrusion detection tools and techniques

Corso di Laurea in Informatica
Università di Bologna

19 settembre 2003

Indice:

1	Introduzione	2
2	I Firewall	2
2.1	Firewall Design Policy.....	4
2.2	Packet Filtering Router.....	5
2.3	Problemi del Packet Filtering Routers.....	5
2.4	Application Level Gateway.....	6
2.5	Circuit Level Gateway.....	8
3	Intrusion Detection	9
3.1	Anomaly Detection.....	11
3.2	Misuse Detection.....	13
3.3	Host-Based IDS.....	15
3.4	Network-Based IDS.....	16
3.5	Caratteristiche Ibride.....	17
3.6	Risposte agli attacchi.....	18
4	Architetture degli IDS	19
4.1	Sistemi Monolitici.....	19
4.2	Sistemi Gerarchici.....	20
4.3	Sistemi Agent-Based.....	21
4.4	Sistemi Distribuiti.....	21
5	Conclusioni	22
	Appendice A: Quali porte filtrare.....	23
	Appendice B: I sistemi IDS presenti.....	26
	Riferimenti bibliografici	27

1 Introduzione

Con un accesso ad internet ormai alla portata di tutti e diffuso a livello mondiale, i problemi di sicurezza delle reti sono in costante aumento. Per un'organizzazione che sviluppa una rete privata da connettere ad Internet, la difesa delle informazioni riservate è un obiettivo primario che va ottenuto non solo applicando una robusta politica di sicurezza per impedire accessi non autorizzati, ma anche imparando in modo approfondito tutti gli elementi coinvolti nella creazione di una solida barriera di difesa contro gli attacchi degli hacker. I due principali strumenti in mano all'amministratore di rete sono i *Firewall* e gli *Intrusion Detection System*. I primi controllano le porte di accesso alla rete e formano una prima barriera ai più comuni tentativi di accesso.

I secondi identificano chi sta usando un computer senza autorizzazione o chi, possedendo un accesso legittimo, cerca di eseguire operazioni al di fuori di quelle consentite.

2 I FIREWALL

Ogni rete è differente da un'altra, per questa ragione occorre analizzarne la struttura per implementare una corretta politica di controllo e protezione, scegliendo tra le numerose soluzioni adottabili. Solitamente viene preferito un unico collegamento tra rete locale e il resto dell'Internet in modo che il traffico scambiato tra utenti interni ed esterni sia vincolato a transitare su un unico punto. L'amministratore della rete può così concentrare tutta la sua attenzione su questo passaggio obbligato per tutti i dati scambiati tra rete interna ed esterna.

Il controllo dei pacchetti in transito cerca di ottenere questi obiettivi:

- controllare i servizi a cui accedono gli utenti
- determinare in quale direzione vengono inviate le richieste di servizio
- controllare quali utenti accedono ai servizi
- controllare come ogni servizio viene utilizzato

L'insieme dei dispositivi hardware e software che permettono di monitorare i pacchetti in transito nella rete, viene definito sistema *Firewall*.

Un Firewall fornisce benefici come:

- generare allarmi in seguito a eventi speciali
- monitorare l'utilizzo di Internet, ed eventualmente bloccare connessioni a siti o reti non utili ai fini aziendali
- mascherare gli indirizzi nascondendo le reali identità degli utenti
- rappresentare la sede ideale per ospitare server accessibili pubblicamente dagli utenti esterni.

Per quanto il sistema Firewall possa essere ben studiato, non risolve tutti i problemi di sicurezza possibili. La rete interna può venir infatti compromessa dall'installazione volontaria, o non, di una *back-door*, o dall'utilizzo di una connessione *dial-up* non controllata. Risultano difficilmente identificabili gli attacchi perpetrati dagli utenti interni stessi, i quali potrebbero creare falle nella sicurezza in modi diversi:

- divenendo complici dell'hacker e compiendo volontariamente azioni tese a violare le risorse della rete
- installando sulla propria stazione un programma che agisca come Cavallo di Troia
- fornendo un accesso involontario a un hacker che si presenti come membro dell'organizzazione
- non rispettando le politiche di sicurezza adottate

Per assicurare una adeguata sicurezza per ogni necessità, un sistema Firewall può essere scomposto in più parti configurabili separatamente. Un Firewall **monolitico** è più economico e può essere realizzato tramite funzionalità di un *router* di frontiera oppure usando funzionalità di *proxy* di un *Application Gateway*. Un Firewall **composito** invece, offre maggiori possibilità di configurazioni della rete e risulta quindi più adatto a politiche di sicurezza sofisticate.

Le componenti in cui può essere scomposto un sistema Firewall sono:

- *Packet Filtering Router*;
- *Application Level Gateway*;
- *Circuit Level Gateway*;

2.1 Firewall Design Policy

L'introduzione di un firewall nella rete richiede una politica di sicurezza specifica per ogni sistema. Occorre definire le regole usate per implementare i servizi di accesso alle risorse. Solitamente si possono distinguere due modalità di approccio al problema:

- permettere ogni servizio a meno che non sia stato espressamente vietato (*Allow Everything*)
- vietare ogni servizio a meno che non sia stato espressamente permesso (*Deny Everything*)

Nel primo caso la maggioranza dei servizi passa attraverso il firewall, e vengono bloccati solo specifici servizi identificati come pericolosi. Questa politica risulta solitamente debole, lascia più possibilità ad un hacker di aggirare il sistema ed è possibile accedere a tutti i nuovi servizi momentaneamente non negati dal firewall.

Nel secondo caso al contrario vengono negati tutti i servizi e identificati e permessi solo quelli ritenuti strettamente necessari dalla politica di sicurezza compatibilmente con le esigenze dell'organizzazione. Questa politica è quella preferita in tutte le aree dove la sicurezza informatica è di vitale importanza. Spesso all'aumento della sicurezza, vi è però una diminuzione delle possibilità di utilizzo della rete. Certi servizi come FTP, RPC, non possono essere filtrati facilmente, così come altri servizi potenzialmente pericolosi potrebbero essere necessari. Occorre esaminare se la sicurezza ha la precedenza rispetto a questi servizi, o se questi servizi sono così necessari da dover accettare un rischio maggiore. Non bisogna inoltre sottovalutare il costo del sistema Firewall che prevede costi per apparati e licenze software, per gli aggiornamenti, per la manutenzione e per fornire le giuste conoscenze tecnologiche al personale interno. L'importanza delle risorse da proteggere e il danno economico dovuto a una eventuale perdita, è un fattore importante nel determinare il budget più appropriato per implementare la politica di sicurezza.

2.2 Packet Filtering Router

Il Packet Filtering Router agisce come prima linea di difesa. E' un router che confronta ogni pacchetto con una politica o un insieme di regole prima di farlo procedere verso la destinazione tramite l'interfaccia corretta.

Solitamente vengono applicati filtri in base a

- Indirizzo IP di partenza
- Indirizzo IP di destinazione
- Porta TCP/UDP di partenza
- Porta TCP/UDP di destinazione

Le più comuni politiche di filtraggio rifiutano i pacchetti ICMP, UDP, e i pacchetti SYN/ACK in arrivo che attivano una sessione. Si possono filtrare pacchetti anche sulla base dei *flag* contenuti nell'intestazione dei pacchetti IP ed in base all'interfaccia di rete fisica a cui arriva il pacchetto. L'appendice A riporta un elenco delle porte e dei servizi ad esse associati.

2.3 Problemi del Packet Filtering Routers

Con l'uso del Packet Filtering Router, all'aumento della sicurezza consegue una chiusura delle porte, e quindi una diminuzione dei servizi disponibili. Ma questo non è il solo problema:

- Non capiscono gli *Application Layer Protocols*. Non possono controllare gli accessi a sottoparti dei protocolli, come per esempio i comandi PUT o GET in FTP.
- Sono stateless: non mantengono informazioni riguardo la sessione o la applicazione che sta comunicando nella rete.
- Hanno funzionalità molto limitate nel manipolare informazioni all'interno del pacchetto
- Non offrono funzionalità di valore aggiunto come HTTP Object Caching, URL Filtering, e funzionalità di autenticazione, visto che non possono capire i protocolli usati a questi scopi.

- Non possono limitare le informazioni passate dall'interno della rete locale ai servizi del server firewall
- Hacker potrebbero riuscire ad avere accesso ai servizi del server firewall
- Hanno pochi sistemi di controllo degli eventi, e pochi meccanismi di allarmi. Può essere difficile testare la rete per definire le funzionalità permesse e quelle negate

2.4 Application Level Gateway

Per contrastare le debolezze del Packet Filtering Router i firewall hanno bisogno di un software che effettui il trasferimento e il filtraggio delle connessioni per i servizi come TELNET E FTP. Una applicazione di questo tipo viene chiamata *proxy service* mentre l'host sul quale è in uso viene chiamato *Application Gateway*.

Supponendo che un utente necessiti di una connessione TELNET O FTP a un altro computer della rete interna, egli dovrà mandare la richiesta di collegamento al Application Gateway, eventualmente autenticarsi con una password e, se tutto rispetta i criteri di sicurezza, sarà il Application Gateway a inoltrare la connessione all'host di destinazione e a registrarne l'attività.

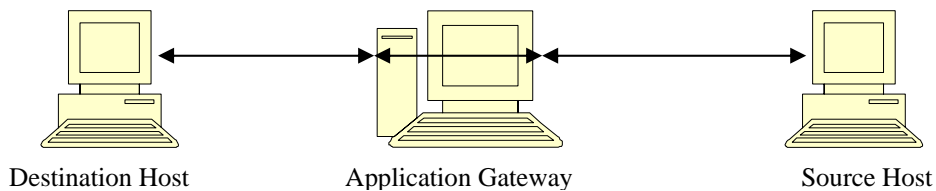
I benefici di questo approccio sono numerosi:

- i proxy services permettono solo i servizi attraverso i quali c'è un proxy. Se un Application Gateway contiene i proxy per FTP e TELNET, allora solo questi due servizi saranno permessi all'interno della sottorete protetta. Tutti gli altri servizi saranno bloccati
- I protocolli possono essere capiti e filtrati. Per esempio si possono impedire solo alcuni comandi come FTP PUT, per non autorizzare solo le scritture via FTP
- possono manipolare i pacchetti
- si possono nascondere informazioni quali nomi e indirizzi degli host interni
- vengono mantenute informazioni riguardo alle comunicazioni
- si riducono i costi perché software e hardware di autenticazione e logging possono essere posizionati solo negli Application Gateway
- si riduce la complessità delle regole di filtraggio, il Packet Filtering Router potrebbe permettere solo traffico destinato al Application Gateway

- prevedono funzionalità di valore aggiunto come HTTP Object Caching e URL filtering e politiche di autenticazione e logging più sicure
- permettono verifiche delle comunicazioni avvenute e allarmi di fronte a eventi pericolosi
- evitano comunicazioni dirette tra l'esterno e l'interno della rete

Permangono comunque anche alcuni svantaggi

- Il proxy server introduce un ritardo nelle prestazioni dovuto al controllo dei dati.
- È necessario un proxy per ogni protocollo che passa attraverso il firewall
- Non sono previsti proxy per UDP, RPC, e altri servizi fra i protocolli più comuni.
- Spesso si rende necessaria una modifica ai client o alle procedure dei client, che devono comunicare non direttamente con l'host ma con un Application Gateway. Si rende perciò più complicato il processo di configurazione.
- Non protegge dalle vulnerabilità presenti nel sistema operativo né dai bug software



2.5 Circuit Level Gateway

Il Circuit Level Gateway è un passaggio veloce e senza controlli attraverso il firewall basato su regole predefinite mantenute nel TCP/IP kernel. Questo tipo di proxy server offre una connessione controllata tra sistemi interni ed esterni. Le richieste internet attraversano un circuito virtuale esistente tra client interni e il proxy server, che successivamente trasmette queste richieste all'esterno, cambiando l'indirizzo IP. Gli utenti esterni vedranno solo l'IP del proxy server, e sarà questo a ricevere il traffico dall'esterno e a rimandarlo indietro al client. In questo modo dall'esterno risulta impossibile vedere la rete interna. Una volta che vengono controllati i permessi di trasmissione tra l'host di partenza e quello di destinazione, i pacchetti attraversano il firewall senza ulteriori controlli.

I vantaggi di questo sistema sono:

- una maggiore velocità rispetto al Application Gateway, dovuta al minor controllo
- protezione di una rete, impedendo connessioni a uno specifico computer esterno o interno
- protezione degli indirizzi IP dagli utenti esterni

Gli svantaggi sono:

- non può controllare gli accessi a sottoparti dei protocolli all'infuori del TCP
- non può eseguire controlli sicuri sui protocolli di alto livello
- ha limitata capacità di generare log ed allarmi
- non offre servizi come Http Object Caching, URL filtering e autenticazione.

3 INTRUSION DETECTION

Col termine *Intrusion Detection System (IDS)* si definisce un sistema software o hardware in grado di determinare se è in corso una violazione della rete. Mentre il firewall semplicemente chiude tutte le porte e mantiene aperte quelle che sono state scelte perché necessarie, l'*Intrusion Detection System* è in grado di accorgersi se qualcuno sta tentando una intrusione o sta commettendo operazioni illegittime, avendo a disposizione informazioni sul traffico di rete, sui log degli host e sulle system call. A fronte di un determinato attacco, inoltre, un IDS reagisce avvisando con un allarme l'amministratore o con una appropriata risposta che lo renda inoffensivo. In altre parole il firewall può essere visto come un muro che protegge le strutture interne e controlla solo un certo numero di porte prestabilite, ma non è in grado di accorgersi di una violazione che aggiri questo muro, né controlla quello che succede all'interno dello stesso. Un IDS è uno strumento essenziale da affiancare al firewall in quanto:

- rivela gli attacchi che falliscono
- rivela gli attacchi interni
- rivela gli attacchi che superano il firewall

Un buon sistema IDS deve avere queste caratteristiche:

1. Deve funzionare continuamente anche senza una supervisione umana. Il sistema deve essere abbastanza affidabile da permettergli di funzionare nel background del sistema osservato. Il suo funzionamento interno dovrebbe essere esaminabile dall'esterno.
2. Deve essere *fault tolerant*, ossia deve restare attivo anche in caso di crash del sistema senza perdere le informazioni di base al riavvio.
3. Deve sfruttare solo il minor numero di risorse del sistema per non rallentarlo eccessivamente
4. Deve accorgersi dei cambiamenti dal normale comportamento
5. Deve essere facilmente adattabile al sistema da proteggere: per potersi adeguare alla struttura e alle esigenze dei differenti sistemi
6. Deve far fronte ai cambiamenti dei criteri del sistema e quindi adattarsi a differenti profili ed esigenze variabili nel tempo.
7. Deve essere difficile da aggirare.

Tra gli avvisi che vengono segnalati dall'IDS si possono distinguere i falsi positivi (*false positive*), i falsi negativi (*false negative*) e gli errori indotti dal sovvertimento dell'IDS (*subversion errors*).

Falsi positivi: avvengono quando il sistema classifica una azione come anomala, segnalandola come intrusione, quando invece risulta essere una azione legittima. Questi tipi di errori, che verranno ignorati dai gestori dell'IDS, devono essere minimizzati in modo da evitare inutili perdite di tempo per controlli superflui. Inoltre un numero eccessivo di questi avvisi finirebbero per nascondere le vere infrazioni che verrebbero ignorate o non rilevate in tempo dagli operatori.

Falsi negativi: avvengono quando l'azione di intrusione è stata commessa ma il sistema non se ne è accorto considerandola come azione legittima. Questi tipi di errori sono più seri rispetto agli errori falsi positivi, in quanto danno un ingannevole senso di sicurezza. Visto che le intrusioni vengono commesse, ma gli operatori non vengono avvisati, essi considereranno sicuro un sistema che non lo è e quindi eviteranno ulteriori controlli. In questo caso l'IDS renderebbe addirittura meno sicuro il sistema che non se non ci fosse.

Errori di sovversione: avvengono invece quando un intruso riesce a modificare le operazioni dell'IDS in modo che produca avvisi falsi negativi.

Gli errori di sovversione sono più complessi e si legano agli errori falsi negativi. Un intruso potrebbe sfruttare la conoscenza del sistema interno dell'IDS per alterare la sua configurazione e permettere di eseguire operazioni illecite. Con questo modo l'intruso può violare il sistema in esecuzione. Questo tipo di attacco può essere scoperto da un operatore che controlli i file di log dell'IDS ma avrebbe l'impressione che l'IDS continui a funzionare correttamente. Un altro tipo di errore di sovversione si ha quando si imbroglia il sistema nel tempo. Visto che l'IDS osserva i comportamenti del sistema in un lungo lasso di tempo, è possibile eseguire una serie di operazioni che singolarmente non appaiono come minacce, ma che prese tutte insieme lo sono. L'IDS infatti aggiorna continuamente la sua nozione di "normalità" nell'uso del sistema, in modo da essere sempre compatibile con le necessità del sistema che cambiano nel tempo. Sfruttando questa caratteristica, certe azioni leggermente illegittime, eseguite da un intruso in un lungo lasso di tempo, potrebbero venir considerate dall'IDS come legittime anche nel caso in cui tutte insieme esse siano parti di un tentativo di intrusione. L'IDS quindi accetterà le singole azioni sospette ma non si accorgerà che esse insieme sono una minaccia al sistema..

Esistono vari tipi di IDS che affrontano il problema da differenti prospettive. Ogni approccio ha i suoi meriti e i suoi difetti. Il tipo di attività monitorata dipende dal tipo di IDS che si usa. Si classificano i sistemi IDS basandosi

- Su modelli di intrusione
 - Rilevamento delle anomalie (*Anomaly Detection*)
 - Rilevamento dei comportamenti sospetti (*Misuse Detection*)
- Sulla posizione del sistema di monitoraggio
 - Host Based IDS
 - Network Based IDS
 - Hybrid Characteristics

3.1 Anomaly Detection

Questo sistema di rilevamento viene anche definito come *profile-based detection* ossia rilevamento basato sui profili. Questo sistema necessita infatti la creazione di profili per ogni gruppo di utenti, che definiscano i comportamenti base, i servizi, i programmi di cui necessitano per svolgere le loro mansioni. Viene stabilita quindi una linea base per le attività che normalmente l'utente esegue durante il suo lavoro. La creazione e l'aggiornamento di questi profili rappresentano una significativa parte del lavoro per implementare un anomaly-based IDS e la qualità di essi è direttamente legata alle probabilità di successo che avrà il IDS nell'identificare gli attacchi.

Tra le metodologie più comuni per la creazione di questi profili ci sono

- La campionatura statistica (*Statistical sampling*)
- L'approccio basato su regole (*Rule-based approach*)
- Le reti neurali (*Neural network*)

Anomaly Detection with Statistical Sampling: utilizza un approccio statistico per la creazione dei profili e quindi il sistema emette allarmi quando si accorge di una variazione dal normale stato definito. Viene definito un parametro (*standard deviation*) che misura la normale variazione dal profilo permessa prima che venga generato un allarme. Variando questo valore è possibile controllare la sensibilità del IDS permettendo quindi ad esempio di regolare il numero di falsi positivi generati. Il punto debole di

questo sistema sta nel fatto che, se cambiano nel tempo le attività necessarie degli utenti, questi generano falsi allarmi.

Anomaly Detection with the Rule-Based Approach: invece di avvalersi di un metodo statistico per definire la normalità, l'Anomaly Detection System può avvalersi di regole che definiscano il normale comportamento dell'utente. L'Anomaly Detection with the Rule-Based Approach analizza il normale comportamento di ogni utente per un periodo di tempo e successivamente crea le regole che corrispondono a questi comportamenti. Qualsiasi altra attività verrà quindi considerata anomala e genererà un allarme. Questi sistemi generalmente si aggiornano per venire incontro alle piccole variazioni nei comportamenti degli utenti. La definizione di normalità viene continuamente aggiustata in base ai cambiamenti nelle abitudini e nelle operazioni dell'utente. Il punto debole di questo sistema sta nel fatto che un attaccante può gradualmente istruire il sistema fino a che il suo attacco risulti normale nuovo comportamento all'interno della rete.

Anomaly Detection with Neural Networks. Le reti neurali sono una forma di intelligenza artificiale nella quale si cerca di simulare l'attività dei neuroni biologici come quelli del cervello umano. I sistemi Anomaly Detection with Neural Networks vengono istruiti con un enorme quantità di dati e regole sulle relazioni tra essi che andranno a definire le connessioni tra i neuroni. Una volta che il sistema è istruito il traffico di rete è usato come stimolo per le reti neurali per determinare quale tipo di traffico è considerato normale.

Vantaggi del Anomaly Detection:

- Possono rilevare molti attacchi interni o furti di account. Un eventuale intruso non può sapere con certezza quali azioni può compiere un determinato utente e quali no, e rischia quindi di eseguire attività che generano allarmi.
- Non basano gli allarmi sulla rivelazione di un attacco conosciuto, ma sul cambiamento del profilo definito di normalità. In questo modo rivelano anche gli attacchi sconosciuti, o quelli che vengono usati per la prima volta, o che ancora non sono stati pubblicati.

Svantaggi:

- Un lungo periodo di addestramento
- La mancanza di protezione durante l'addestramento. Ad esempio un attacco durante questo periodo verrebbe considerato come una normale attività legittima di un utente e rimarrebbe quindi radicata nel sistema
- La difficoltà di definire la "normalità" che può variare talmente rapidamente nel tempo da rendere troppo oneroso l'aggiornamento dei profili.
- Se l'IDS non si aggiorna in tempo rispetto al cambiamento dei profili, lancerà inevitabili errori falsi positivi.
- La presenza di errori falsi negativi se una azione intrusiva appare nella normalità dei comportamenti. Ad esempio se un gruppo di utenti necessita di una grande numero di attività, è possibile che tra esse ce ne sia qualcuna che comporti una vulnerabilità. La rilevazione di questo attacco può risultare molto difficile se non impossibile.
- La difficoltà di capire gli allarmi. Non esiste una relazione diretta tra un allarme e il tipo di attacco, spetta quindi all'amministratore determinare di cosa si tratti.

3.2 Misuse Detection

Questo sistema di rilevamento viene anche definito come *signature-based detection* ossia basato su un set di regole (firme) che definiscono uno specifico traffico come pericoloso in base a una uguaglianza con certi modelli che si sanno venir usati dai malintenzionati per ottenere un accesso. Un gruppo di esperti ingegneri di reti vanno alla continua ricerca di attacchi e vulnerabilità per sviluppare le regole per ogni firma che le dovrà identificare e bloccare. Una buona definizione di queste firme permette di ridurre la possibilità di falsi positivi e contemporaneamente di minimizzare i falsi negativi. Come detto per individuare un attacco, un signature-based IDS esamina i dati che gli arrivano, ma talvolta gli attacchi vengono effettuati in molte parti più piccole, e portati avanti per più tempo. Il sistema IDS deve quindi stabilire una finestra temporale entro la quale un attacco può essere determinato. Questa quantità di tempo viene definita **Event Horizon**. Durante questo lasso di tempo il sistema deve mantenere le informazioni sugli stati del sistema. L'event horizon è quindi un parametro che può essere variato dall'amministratore per personalizzare la sicurezza di una rete. In alcuni casi questa

finestra temporale comincia al momento del login dell'utente e finisce col suo logoff, in altri casi, può invece essere necessario un event horizon di settimane. In ogni caso è importante evidenziare che non è possibile mantenere tutte le informazioni degli stati per un tempo indefinito.

Vantaggi:

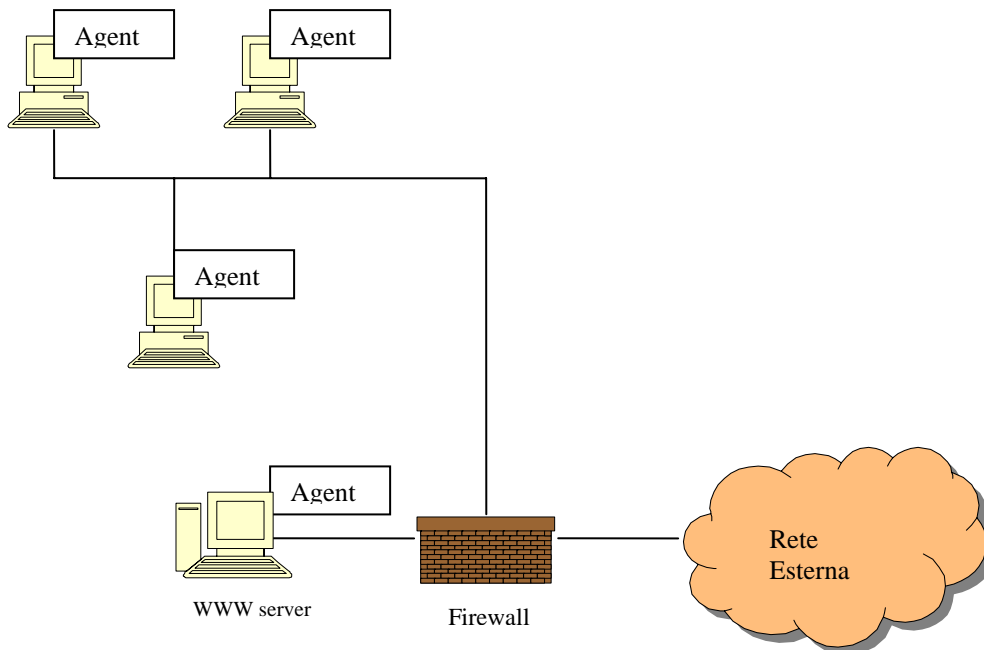
- Le firme sono basate su attività di intrusione conosciute, si può quindi essere sicuri di rilevarle
- Gli attacchi identificati sono ben definiti. Ogni attacco ha una firma e quindi un nome e un documento di identificazione all'interno del database delle firme. Gli utenti hanno la consapevolezza della capacità dell'IDS nell'intercettazione degli attacchi e possono verificare gli aggiornamenti nel database delle firme.
- Il sistema è facile da capire, esiste una corrispondenza uno-a-uno tra gli allarmi e gli attacchi.
- Gli attacchi sono individuati immediatamente dopo l'installazione, non c'è un periodo di addestramento come per gli Anomaly-Based IDS

Svantaggi:

- L'aggiornamento del database delle firme è una procedura che va effettuata continuamente.
- L'inabilità di determinare attacchi sconosciuti non presenti nel database delle firme. Anche se questo non vuol dire, comunque, che tutti i nuovi attacchi violeranno il sistema. Gli sviluppatori delle firme, cercano di creare definizioni flessibili in modo che vengano rilevati classi di attacchi simili.
- Si possono verificare falsi negativi quando gli attacchi aggirano il sistema
- Il mantenimento delle informazioni sugli stati (Event Horizon) può richiedere grosse quantità di memoria.

3.3 Host-Based IDS

Gli Host-Based IDS rilevano le intrusioni controllando le informazioni a livello dell'host ed esaminano aspetti quali le system call, i log, i messaggi di errore, le modifiche ai file e ai documenti. La figura sotto rappresenta un tipico Host-Based IDS.



Vantaggi:

Questo tipo di approccio non prevede un controllo della rete e di conseguenza non ne rallenta la velocità. Ha il grande pregio di poter controllare che l'host non subisca attacchi, potendo contare su un ampio insieme di controlli e informazioni del sistema.

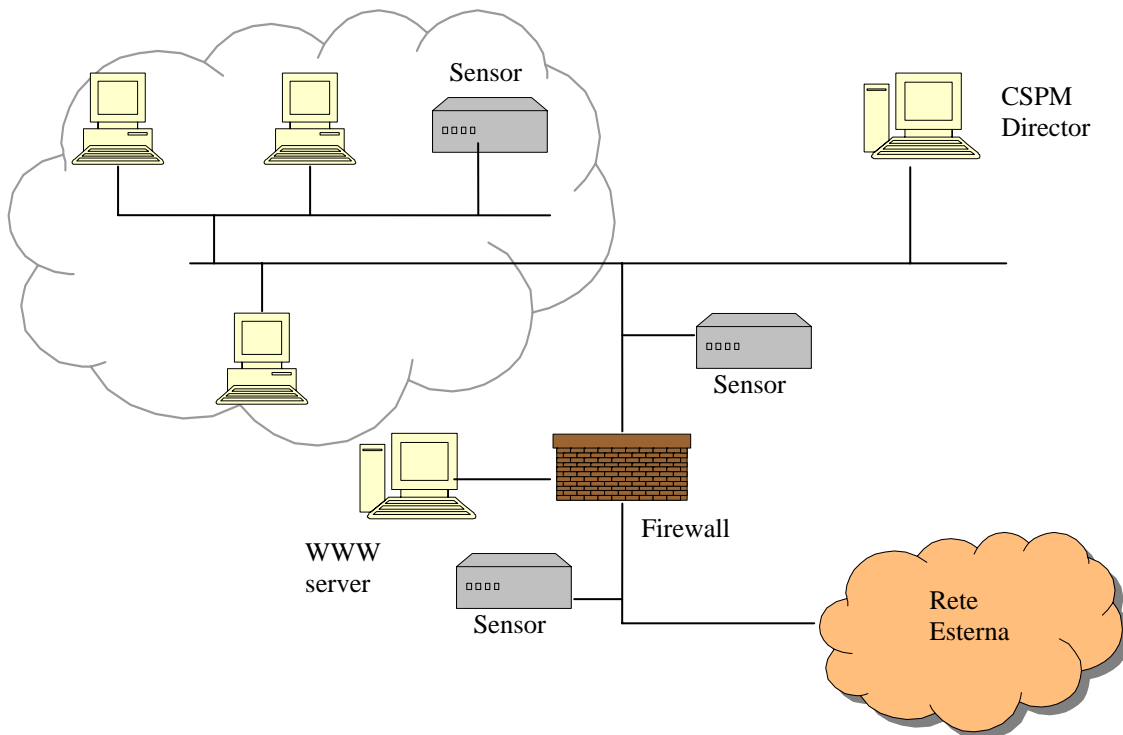
Svantaggi:

- Un visione della rete ristretta, che non permette l'identificazioni di certi tipi di attacchi. Ad esempio attacchi diretti ai protocolli di rete di basso livello non vengono rilevati in quanto l'informazione non è disponibile fino a che non raggiunge un livello superiore.
- L'IDS deve essere presente su ogni componente della rete, spetta quindi all'amministratore installarlo in tutti i computer.

- Dipende dal sistema operativo. Qualche volta i produttori di IDS scelgono di supportare solo certi sistemi operativi, per cui se alcuni computer hanno sistemi operativi diversi, la rete non risulta adeguatamente controllata.
- Utilizzo delle risorse. La presenza dell'IDS può rallentare il sistema in mano all'utente.
- Quando un Host-Based IDS subisce un attacco, deve comunicarle l'intrusione a un sistema centrale di raccolta dati. Se l'attaccante riesce a bloccare il traffico di rete dell'host, questo non riesce a comunicare l'intrusione. Inoltre il traffico di rete diretto alla centrale, può essere a sua volta bersaglio di un attacco.

3.4 Network-Based IDS

Una Network-Based IDS esamina, con l'uso di sensori esterni, i pacchetti per localizzare gli attacchi alla rete. L'IDS analizza i pacchetti della rete e li paragona alle firme del database delle attività intrusive. Una intero insieme di computer può essere monitorato da una macchina dedicata che ascolta il traffico di rete. Il sistema può essere completamente nascosto con l'uso di una scheda dire rete che ascolta la rete ma non trasmette mai.



Vantaggi:

- Ampia visione della rete. Osservando il traffico destinato a più host, un sensore è in grado di accorgersi anche di attacchi distribuiti su più host.
- Non deve essere in funzione su tutti i sistemi operativi degli host con una conseguente maggior velocità di installazione e un minor lavoro per gli amministratori.

Svantaggi:

- Sfruttamento della banda di rete con conseguente decremento di velocità.
- Il traffico codificato non viene rilevato dai sensori dell'IDS, in quanto con corrisponde alle firme del database.
- Riasssemblamento dei frammenti: i pacchetti di rete hanno una dimensione massima, se una connessione necessita di mandare dati che eccedono questa quantità, i dati devono essere spezzati in più pacchetti. Quando l'host riceve i pacchetti frammentati, li riassume nel dato originale. Così deve fare anche il sensore dell'IDS per esaminare i pacchetti e il problema riguarda il corretto ordine con cui vengono riassemblati, visto che alcuni sistemi operativi partono dal primo pacchetto e vanno verso l'ultimo e altri dall'ultimo verso il primo. Un tipo di attacco prevede di mandare frammenti che si sovrappongono per cercare di aggirare il Network-Based IDS.

3.5 Caratteristiche Ibride

I sistemi ibridi combinano le funzionalità dei differenti IDS per creare un sistema che fornisca più funzionalità di uno tradizionale. Sistemi ibridi possono incorporare sistemi diversi come Anomaly e Misuse Detection, altri possono incorporare differenti localizzazioni per il monitoraggio come Host-Based e Network-Based IDS. La maggiore difficoltà nel costruire questi sistemi ibridi sta nel riuscire a far convivere le varie componenti in armonia e a indicare le informazioni all'utente finale in modo ossia facile da capire.

Vantaggi:

I vantaggi dei sistemi ibridi dipendono dalle diverse tecnologie che vengono combinate. L'unione di Host-Based e Network-Based IDS fornisce una chiara visione della rete così come una dettagliata analisi a livello dell'host. L'unione degli approcci Anomaly e Misuse Detection può produrre un signature-based IDS che può individuare attacchi precedentemente sconosciuti.

Svantaggi:

Gli svantaggi sono una maggiore difficoltà nel far lavorare insieme le differenti tecnologie e nel fornire messaggi chiari all'utente. Inoltre ogni sistema richiede di essere esaminato per studiarne i punti forti e deboli.

3.6 Risposte agli attacchi

Il IDS ideale dovrebbe essere capace di riconoscere e neutralizzare gli attacchi, prevenire ulteriori attacchi, e rafforzare il sistema per prevenire che si riverifichino una seconda volta. Nelle attuali implementazioni degli IDS possono essere riconosciute varie capacità di reazione:

- **Tracciamento dell'attacco:** il sistema cerca passivamente e indirettamente di raccogliere informazioni utili all'identificazione della provenienza dell'attacco
- **Fuga:** il IDS riconfigura un altro sistema (come un firewall o un router) per escludere l'intruso, oppure usa tecniche per far cadere ogni tentativo di connessione
- **Raccolta di informazioni avanzate:** aumenta il livello di informazioni memorizzate riguardo agli eventi che attorniano un attacco in modo da analizzarle successivamente

L'uso di queste tecniche di risposte è abbastanza limitato per via dei problemi inerenti i falsi positivi, ritardi nel riconoscimento degli attacchi, e il rischio di una risposta automatica verso una operazione legittima. Per questo motivo molti sistemi si limitano a registrare le attività e a segnalarle al personale amministrativo. Ma talvolta le risposte automatiche sono necessarie quando il volume o la necessaria velocità di risposta superano le capacità umane.

4 ARCHITETTURA DEGLI IDS

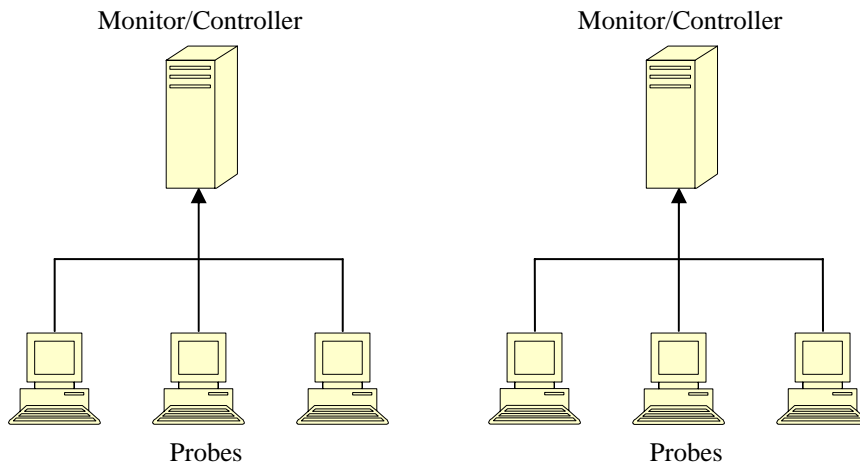
Un Intrusion Detection System è formato da una serie di elementi comuni:

- **Sensori, sonde:** questi moduli sono i primi elementi che raccolgono le informazioni di un IDS. Esaminano il traffico di rete, i file di log, il comportamento del sistema, e comunicano gli eventi agli IDS monitors
- **Monitor:** ricevono la comunicazione degli eventi dai sensori, li confrontano con i modelli di comportamento presenti nel IDS, ed eventualmente producono un allarme. Gli allarmi indicano una possibile falla nella sicurezza e possono essere mandati a monitor di livello più alto o alla unità di risposta
- **Unità di risposta (*resolver*):** ricevono le segnalazioni sulle possibili violazioni dai monitor e determinano una appropriata risposta automatica o una segnalazione agli operatori.
- **Controller:** facilitano la configurazione e la coordinazione dei componenti specialmente per gli IDS distribuiti. Inoltre offrono un unico punto per l'amministrazione e le interrogazioni al IDS.

In molte architetture di IDS alcune di queste parti sono spesso parte di un unico componente, come ad esempio nel caso degli IDS monolitici.

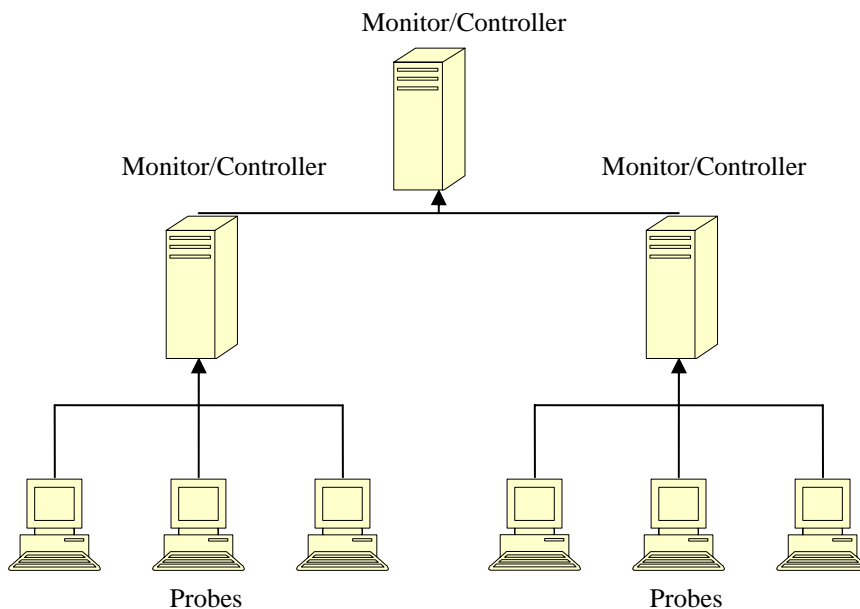
4.1 Sistemi monolitici

L'architettura più semplice di un IDS è l'utilizzo di una singola applicazione che contiene un sensore, un monitor, una unità di risposta e un controller in un unico blocco. Sistemi monolitici più avanzati prevedono l'uso indipendente di più sensori, monitor e resolver, ognuno dei quali implementa specifiche tecniche. La maggiore debolezza di questa architettura sta nel fatto che non è possibile bloccare un attacco composto da sequenze di operazioni distribuite su più computer, in quanto l'architettura non offre cooperazione tra gli IDS.



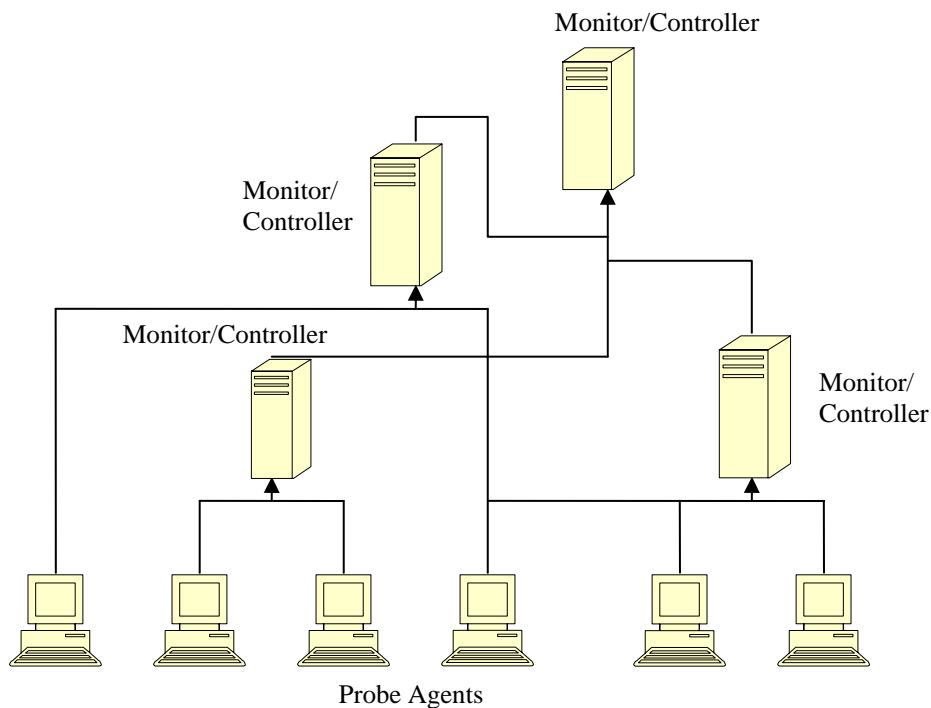
4.2 Sistemi Gerarchici

Al vertice del sistema gerarchico trova posto una unità di risposta e controller. Sotto a questo, una o più componenti monitor, con sonde ausiliari distribuite attraverso il sistema protetto. L'uso di un controllo centralizzato permette a informazioni provenienti da differenti sottosistemi di essere correlati, rilevando attacchi distribuiti.



4.3 Sistemi Agent-Based

Architetture più recenti di IDS dividono il sistema in più unità funzionali distinte: sensori, monitor, revolver e controller. Questi possono essere distribuiti su molti sistemi con ogni componente che riceve informazioni da componenti sottostanti e manda informazioni a componenti di livello più alto. I sensori informano i monitor che informano a loro volta unità di risposta o monitor di più alto livello. Questa architettura permette una grande flessibilità nel posizionamento e nella applicazione di componenti individuali. Inoltre questa architettura permette maggiore resistenza a sovraccarichi e attacchi, una facile estensione della rete e più livelli di informazioni attraverso la struttura.



4.4 Sistemi distribuiti

L'architettura dei sistemi descritta fino ad ora considerava gli attacchi in termini di eventi su un singolo elemento del sistema. Con i sistemi distribuiti invece si può pensare tutto un sistema come una singola unità. In reti particolarmente ampie e complesse, è possibile in questo modo considerare intere sottoreti come singoli sistemi elementari, permettendo una maggiore possibilità di espansione della rete e una capacità di identificare attacchi distribuiti su larga scala.

5 Conclusioni

Il campo degli Intrusion Detection è stato, e sarà in futuro, sviluppato rapidamente. Differenti tecniche e soluzioni caratterizzano la struttura degli IDS presenti, ed esistono molti progetti ancora in fase di sviluppo che porteranno innovazioni su questo segmento della sicurezza delle reti. Ma ancora ci sarà molto da fare prima di poter parlare di reti realmente sicure.

Appendice A: Quali porte filtrare

La decisione di quali porte vanno filtrate dipende dalla politica di sicurezza adottata. La lista seguente contiene alcune delle porte considerate vulnerabili e che sono solitamente bloccate o filtrate da un firewall sia in ingresso che in uscita.

Porta 7: echo. Le politiche di comunicazione standard non necessitano del servizio, dato che esso accetta, semplicemente, le risposte ai dati inviati dalle richieste di connessione TCP o UDP. Questa porta può venir usata per attacchi di tipo Denial of Service che mirano a mettere fuori uso il sistema.

Porte 11 e 15: systa e netstat. Forniscono in ambiente Unix informazioni sullo stato dei processi, degli utenti e del sottosistema della rete.

Porta 19: chargen. Può essere usato per creare un loop infinito che passi dati tra il servizio echo e il servizio chargen stesso.

Porta 21: FTP. Se le politiche di comunicazione non necessitano dell'impiego del protocollo FTP, è consigliabile disabilitarlo. Nel caso fosse indispensabile, è meglio prendere qualche accorgimento quale:

- ridurre il limite massimo di connessioni contemporanee, che potrebbe essere sfruttato da un hacker per sovraccaricare il sistema
- impedire le connessioni FTP anonime
- modificare il banner del daemon FTP che fornisce dati utili per un attacco come tipo, versione del daemon e piattaforma utilizzata.
- impostare permessi per operazioni di upload e download per ogni utente

Porta 23: Telnet. Può essere sfruttata per portare gravi attacchi visto che le password vengono passate in chiaro e che sono possibili comandi remoti. Nel caso non servisse è consigliabile disabilitare l'impiego di questo servizio. In caso contrario sarà necessario controllare questo servizio con accorgimenti simili a quelli adottati per FTP o con l'uso di wrapper TCP che assicura un miglior controllo delle connessione e degli accessi.

Porta 25: SMTP. Il daemon SMTP resta sempre attivo in attesa dell'arrivo della posta elettronica e risulta quindi molto esposto a attacchi di vario genere. E' opportuno modificare il banner del daemon che potrebbe divulgare informazioni utili per un attacco, ed è possibile gestire il servizio con un wrapper TCP. Per evitare un utilizzo fraudolento si può configurare il servizio in modo che operi come un gateway per l'indirizzamento della posta elettronica operante all'interno del dominio locale e fare quindi in modo che il daemon non accetti richieste di indirizzamento provenienti dall'esterno. Esiste poi una procedura più avanzata denominata SMTP-NAT-DMZ che permette un maggiore controllo del traffico sulla porta SMTP. La procedura NAT (Network Address Translation), eseguita dal firewall o dal router di accesso, traduce gli indirizzi IP interni in indirizzi Internet e viceversa. Per fare in modo che possa essere raggiunto dall'esterno, per le operazioni di trasferimento dei messaggi, il firewall traduce l'indirizzo Internet nell'indirizzo interno del server SMTP. La soluzione DMZ (De-Militarized Zone) introduce un'altra rete, all'esterno del firewall, distinta rispetto alla rete locale interna. In questo modo un attacco al server SMTP non darebbe accesso alla rete locale interna.

Porta 53: DNS. Contiene i nomi e le informazioni degli host può quindi essere usato per un attacco. Se necessario, il servizio Domain Name Service, va utilizzato tramite un provider Internet o situando il server all'esterno del firewall di protezione come in una zona "smilitarizzata". Può essere poi utile modificare il daemon DNS in modo che non visualizzi all'esterno alcuna informazione.

Porta 67: bootp. Consente a una workstation senza dischi di conoscere il proprio indirizzo IP tramite richiesta di propagazione. Il server bootp controlla questo processo in risposta a una query su un database usando l'indirizzo hardware o MAC della workstation. E' importante attivare un elenco degli indirizzi MAC dei nodi che possono ricevere risposte dal server bootp.

Porta 67: TFTP. Se non utilizzato il daemon TFTP andrebbe disabilitato. Data la mancanza di funzionalità di sicurezza chiunque potrebbe accedere ai file pubblici.

Porta 79: Finger. Il servizio può essere utilizzato facilmente per estrapolare informazioni importanti per eseguire un attacco. Non essendo strettamente necessario sarebbe utile disattivarlo.

Porta 80: HTTP .Il punto debole del HyperText Transfer Protocol è l'attacco alle pagine web. Per assicurare una maggior sicurezza alla rete si può posizionare il server Web in una zona smilitarizzata o almeno mantenere estesi registri di sistema e configurare un sistema di bloccaggio della porta.

Porte 109, 110: POP . Il Post Office Protocol può consentire agli hacker di carpire informazioni, eseguire login e attivare una sessione telnet. Se non è possibile disattivare queste porte si può gestire il servizio, con maggiore sicurezza, con un wrapper TCP

Porte 111, 135, 137, 139, 838: portmap, loc-serv, nbservice, nbdgram, nbsession. E' importante filtrare gli accessi a queste porte provenienti dall'esterno della rete locale

Porta 161: SNMP . Il Simple Network Management Protocol può fornire importanti informazioni a un hacker come tipo di dispositivo, connessioni e processi attivi nella rete. Per evitare questo problema è sufficiente impedire l'accessibilità remota dall'esterno della rete locale.

Porte da 512 a 520. Questi servizi se impropriamente configurati possono permettere una moltitudine di attacchi, dal reperimento di informazioni, a spoofing degli indirizzi, a Denial of Service. Come contromisura è importante bloccare queste porte con firewall router o port blocker.

Porta 540: UUCP. Incorpora una serie di programmi per il trasferimento di file e la trasmissione di comandi su sistemi Unix. Normalmente disabilitato, se necessario può essere controllato con un wrapper TCP, impedendone l'accesso dall'esterno della rete locale o rendendone possibile l'utilizzo solo in certi momenti.

Le porte elencate fanno parte delle prime 1024 porte considerate ben note. Ma gli attacchi possono coinvolgere una qualsiasi delle 65000 porte a disposizione. Le restanti porte devono essere controllate periodicamente, possono essere utilizzate da programmi specifici utili all'azienda, o da Cavalli di Troia che aprono la strada agli hacker. Occorre quindi controllare queste porte periodicamente e, se inaspettatamente si riscontrano porte aperte, si devono bloccare e controllare file e registro di sistema alla ricerca di Troiani. E' sempre necessario avere quindi software anti-troiani aggiornati e controllare l'accesso alle porte anche con un semplice firewall software che richieda all'utente l'apertura di una di esse in caso di bisogno.

Appendice B: I sistemi di IDS presenti

I principali IDS del mercato sono:

- | | | |
|-----------------|----------------|---|
| - Cisco | Secure IDS | http://www.cisco.com |
| - ISS | RealSecure | http://www.iss.net |
| - Axent | Intruder Alert | http://www.axent.com |
| - Intrusion.com | Secure Net Pro | http://www.intrusion.com |
| - Enterasys | Dragon | http://www.enterasys.com/ids |
| - NFR Security | NID e HID | http://www.nfr.net |
| - Marty Roesch | Snort | http://www.snort.org |

Riferimenti bibliografici

- [Chi01] Chirillo J., *Hacker: la difesa*, Milano, McGraw-Hill, 2001.
- [Chi01] Chirillo J., *Hacker: l'attacco*, Milano, McGraw-Hill, 2001.
- [MSK01] McClure S., Scambray J., Kurtz G., *Hacker 2.0: nuove tecniche di protezione dei sistemi*, Milano, Apogeo, 2001.
- [Gol99] Gollmann D., *Computer Security*, Chichester, John Wiley & Son, 1999
- [ESC01] Ellis J., Speed T., Carrasco E., *The Internet Security Guidebook from planning to deployment*, San Diego, Academic Press, 2001
- [Cin99] Cinotti M., *Internet security : architetture, protocolli e applicazioni per la sicurezza delle reti e dei dati*, Milano, Hoepli, 1999
- [Kla98] Klander L., *Hacker Proof: sicurezza in rete*, Milano, McGraw-Hill, 1998
- [Car02] Carter E., *Cisco secure intrusion detection system*, Indianapolis, Cisco Press, 2002
- [Gur01] Gurley, *Intrusion detection*, Indianapolis, Macmillan Thecnical, 2001
- [Gra00] Robert Graham, "Network Intrusion Detection Systems", 2000, <http://www.robertgraham.com/pubs/network-intrusion-detection.html>.
- [Pri01] Katherine Price, "Intrusion Detection Pages", 2001, <http://www.cerias.purdue.edu/coast/intrusion-detection/welcome.html>
- [Coh96] Fred Cohen, "Intrusion Detection and Response", 1996, <http://all.net/journal/ntb/ids.html>
- [Dek97] Marcel Dekker, "Security of the Internet", 1997, http://www.cert.org/encyc_article/tocencyc.html