Sicurezza delle reti

Giuseppe Augiero

Agenda

- Sicurezza informatica
- Crittologia
- Stack Tcp/Ip
- Firewall
- Ids/Ips
- Tipologie di attacchi
- Aspetti Legislativi
- Sicurezza di Linux
- (In)Sicurezza di Windows
- Wireless


Sicurezza informatica

Sicurezza informatica

- In ambito informatico con la parola “Sicurezza” si intende la *sicurezza dell’informazione*.

- La sicurezza informatica definisce *le regole per il controllo dell’accesso all’informazione e alle risorse*.

Principi di base

Occorre garantire:

- **Confidenzialità**: solo chi e' autorizzato conosce l'informazione.
- **Integrità**:l'informazione non può essere manomessa da chi non e' autorizzato.
- **Disponibilità**: l'informazione e' disponibile per chi ha l'autorizzazione ad usarla.
- **Non ripudiabilità**: il mittente non può disconoscere la paternità del messaggio, cioè non può negare di aver inviato il messaggio.

Costo della sicurezza

- Esiste un conflitto tra sicurezza e facilità di utilizzo di un computer.
- La sicurezza è considerata un costo e non un beneficio.

- Non si comprende il valore dei dati da proteggere.
- Quanto costa non adottare la "sicurezza"?

Costi vivi

I costi associati alla sicurezza sono:

- Selezionare, formare e mantenere personale qualificato.
- Acquistare tecnologia hardware e software.
- Aggiornamento della tecnologia.
- Aumento della complessità operativa ed organizzativa, incremento dell'overhead e degrado delle performance del sistema (dovuti alla tecnologia).

  Tuttavia questi costi sono inferiori al costo che l'organizzazione sosterrebbe in caso di compromissione del sistema.

Dinamicità

- La sicurezza non ha uno sviluppo statico ma è un processo iterativo.

Da dove iniziare?

- La definizione della politica di sicurezza non può che partire da una analisi dei rischi.
- L'analisi dei rischi deve individuare i punti critici.
- I prunti critici rappresentano elementi di ridotta robustezza dell'infrastruttura informatica.

Robustezza informatica

- La robustezza di un componente è la capacità di non danneggiare il sistema in cui è inserito quando vengono violate le specifiche del componente stesso.
- Violazione delle specifiche significa:
  - input diversi da quelli specificati
  - risorse diverse da quelle specificate

Essere sicuri

E’ inutile cercare di essere impenetrabili, occorre essere costosi (tempo e danaro) da penetrare.

- Per proteggere un bene non si dovrebbe mai spendere di più del valore reale del bene stesso.
- La sicurezza di un sistema può essere paragonata ad una catena. La misura del livello di sicurezza dell’intero sistema è determinato dalla robustezza dell’anello più debole della catena.

Sicurezza relativa

- La nozione di sicurezza è un qualcosa di relativo e non di assoluto. Non esiste un sistema sicuro in assoluto.
- La sicurezza è un concetto relativo. “Il sistema A è più sicuro del sistema B”. Il corretto quesito da porsi dovrebbe essere: “Il sistema è sufficientemente sicuro da sostenere il mio business?”

Usabilità

- **Sicurezza ed usabilità sono spesso in antitesi.** Il sistema più usabile è quello privo di misure di sicurezza. Un sistema completamente sicuro è un sistema che opera localmente, staccato dalla rete, collocato in un bunker, senza finestre, con un plotone di guardie armate e cani ringhiosi dietro del filo spinato e con un sistema di sorveglianza con telecamere. Sistema davvero sicuro, ma chi vorrebbe lavorare in tali condizioni ?
- Bisogna trovare il giusto equilibrio tra usabilità e produttività da un lato e sicurezza dall'altro.

Tre politiche per la sicurezza

- Tre sono le politiche fondamentali per la robustezza:
  - controlli nell'accesso agli oggetti
  - controlli di identificazione
  - politiche di crittografia
    - per l'identificazione dei soggetti
    - per la confidenzialità dei dati

Risk Assestment

- Il concetto di risk assessment è fondamentale per sviluppare una difesa adeguata.
- Identificazione dei beni.
- Identificazione delle vulnerabilità.
- Identificazione delle minacce e della loro probabilità.
- Identificazione delle contromisure.
- Analisi costi e benefici.
- Sviluppo di politiche e procedure di sicurezza.

Asset

Per identificare e dare una priorità ai beni (asset) informativi aziendali e per sviluppare un'analisi di costo/beneficio è necessario rispondere alle seguenti domande:

- Cosa si vuole salvaguardare?
- Perché si vuole salvaguardare il bene?
- Quale è il suo valore?
- Quali sono le minacce?
- Quali sono i rischi?
- Quali sono le conseguenze della perdita?
- Quali sono i possibili scenari?
- Quale sarà il costo associato alla perdita delle informazioni o del sistema?

Modelli di sicurezza

Esistono 3 approcci di base per sviluppare un modello di sicurezza:

- "By Obscurity" (occultamento)
- Difesa perimetrale
- Difesa in profondità

Per conseguire la sicurezza, in generale le aziende impiegano una combinazione dei tre approcci.

Analisi del rischio

- Comprensione delle insicurezze.
- Definizione di priorità.
- Implementazione di Sistemi Esperti.

- Occorre effettuare un Trade-Off !!!

Politiche di sicurezza

- Fornire linee guida.
- Soluzioni implementabili.
- Accettabile da parte di tutti.
- Controllare che siano rispettate (audit)
- Responsabilizzare.
- Scegliete gli obiettivi per valutare il trade-off.
- Facilità di utilizzo.
- Valutare i costi.

Progettare la sicurezza

- Minimi privilegi.
- Prevedere diversi livelli.
- Prevedere diversi sistemi di sicurezza.
- Centralizzare la gestione.
- Concentrare l'attenzione sui punti deboli.
- Fail-over.
- Partecipazione di tutti gli utenti.

Audit

- Analisi dei log non e' una operazione banale.

- Le ragioni di analisi possono essere:

  - controllo delle operazioni effettuate.

  - controllo del rispetto delle politiche di sicurezza.

  - Ricerca di segni di intrusione.

Azioni da intraprendere

- Prevention: E’ necessario implementare delle misure per prevenire lo sfruttamento delle vulnerabilità.
- Detection: E’ importante rilevare prontamente il problema; prima si rileva il problema, più semplice è la sua risoluzione.
- Response: bisogna sviluppare un piano appropriato di intervento in caso di violazione con individuazione delle responsabilità e le azioni da intraprendere.

Da chi dobbiamo difenderci

- Hackers.
- Crackers.
- Ricercatori di informazioni.
- Procutatori di Denial of Service.
- Virus e Cavalli di Troia.

Motivazioni

- Furto.
- Modifica delle informazioni.
- Odio.
- Motivazioni politiche/religiose.
- Sfida intellettuale.

Crittologia

Crittologia

- La crittologia è «l'arte e la scienza della scritture segrete».

- La crittologia si divide in due branche: la crittografia (che studia come proteggere i messaggi) e la crittanalisi (come violarli).

Cifratura

- Il senso ultimo della crittografia è quello di rendere illegibile un testo in chiaro (una sequenza di lettere oppure di numeri) a chi non è stato autorizzato dall'autore, mediante un'operazione nota come cifratura.

Decifratura

- Un testo realizzato secondo i principi della crittografia si chiama testo cifrato e perché sia riportato nella sua forma in chiaro il destinatario deve compiere un'operazione che si chiama decifrazione.
- La stessa operazione (la decifrazione) attuata da chi non è autorizzato a leggere il messaggio si chiama decrittazione .

Segretezza

- Il livello di segretezza dipende dal cifrario utilizzato (il codice) e dalla complessità della chiave di cifratura che determina il modo in cui un messaggio viene cifrato

Chiave di cifratura

In generale gli algoritmi di cifratura fanno uso di chiavi

- Il termine chiave si riferisce all'insieme delle informazioni necessarie all'algoritmo crittografico per cifrare e decifrare i dati
- In generale una chiave è una sequenza di bit e la sicurezza della chiave è espressa in termini della sua lunghezza.
- La sicurezza dei sistemi crittografici dipende dalla robustezza dell'algoritmo e dalla sicurezza della chiave.
- La chiave di cifratura nella crittologia moderna è creata attraverso algoritmi matematici.

Brute force

- Tanto più è robusto l'algoritmo e complessa la chiave di cifratura che esso genera, più sicuro sarà il messaggio, anche di fronte a un attacco di forza bruta, cioè l'esplorazione di tutte le combinazioni matematiche che permettono di risalire alla chiave.

L’alba della crittografia

- Nel corso della storia sono state sviluppate numerose tecniche crittografiche per garantire la segretezza delle comunicazioni scritte.
- Giulio Cesare fu tra i primi uomini di stato a elaborare un proprio cifrario per comunicare coi suoi generali.

Spie, segreti, codici cifrati

- L'esigenza di segretezza in ambito militare ha fatto sì che la crittografia fosse per lungo tempo considerata appannaggio di generali, diplomatici e spioni.

Cifratura digitale

- In un mondo interconnesso dagli apparati di comunicazione digitale, la crittografia è una componente fondamentale della vita quotidiana anche se non ce ne rendiamo conto.
- Usiamo la crittografia al bancomat o quando guardiamo la pay-tv, ci colleghiamo a un sito web sicuro per le operazioni bancarie o compriamo qualcosa su Internet, quando parliamo al telefono cellulare.

Simmetria vs Asimmetria

La crittografia può essere classificata in base al tipo di chiave impiegata:

- Crittografia a chiave segreta o simmetrica.
- Crittografia a chiave pubblica o asimmetrica .

La maggior parte delle applicazioni fanno uso di uno o di entrambi i tipi di crittografia.

- Le funzioni hash non usano la chiave.

Chiave simmetrica

- La crittografia a chiave simmetrica usa la stessa chiave per cifrare e decifrare i messaggi.
- Ogni coppia di utenti condivide la stessa chiave per effettuare lo scambio dei messaggi.
- Essendo in grado di cifrare e decifrare un messaggio, ciascun partner assume che l'altra entità sia la stessa entità alla quale ha comunicato la chiave (Autenticazione).
- Affinché questo schema funzioni la chiave deve essere mantenuta segreta tra i due partner.
- La sicurezza dell'algoritmo a chiave simmetrica è direttamente legata alla protezione e distribuzione della chiave segreta

Simmetria

Gli algoritmi a chiave simmetrica sono generalmente classificati in:

- block cipher che operano su blocchi di dimensioni fisse (64 bit). I messaggi di lunghezza maggiore sono suddivisi in blocchi, elaborati e quindi concatenati secondo un qualche criterio.
- stream cipher che elaborano i dati un byte alla volta.

Gli algoritmi block cipher sono più adatti per cifrare dati a lunghezza fissa, mentre gli algoritmi stream cipher sono più adatti per cifrare dati a lunghezza variabile (traffico di rete)

Algoritmi chiave simmetrica

Principali algoritmi block cipher:

- Data Encryption Standard (DES) (56 bits)
- Triple DES (3DES) (168 bits)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA) (128 bits
- CAST-128
- Blowfish

Principali algoritmi stream cipher:

- Ron's Cipher 4 (RC4)
- Software-Optimized Encryption Algorithm (SEAL)

Pro e contro

Principali vantaggi:

- Velocità del processo di cifratura
- Semplicità d'uso

Principali svantaggi:

- Necessità di cambiare frequentemente le chiavi segrete
- Distribuzione delle chiavi, cioè la necessità di inviare la chiave segreta in un canale sicuro diverso da quello di comunicazione
- Gestione delle chiavi (crescita quadratica).
- Non garantisce la non ripudiabilità.

Chiave asimmetrica

La crittografia a chiave pubblica o asimmetrica prevede l'utilizzo di una coppia di chiavi, correlate tra loro, per ciascun partner; una pubblica, nota a tutti, ed una privata nota solo al proprietario, mantenuta segreta e protetta (smart card).

- Ciò che viene codificato con la prima chiave può essere decodificato con l'altra e viceversa.
- E' virtualmente impossibile derivare la chiave privata conoscendo la chiave pubblica.

Asimmetria

La crittografia a chiave pubblica garantisce le seguenti funzioni:)

- **Confidenzialità**: nel caso in cui il mittente voglia inviare un messaggio non decifrabile da altri in un canale insicuro, è sufficiente che codifichi il messaggio in chiaro con la chiave pubblica del destinatario e lo trasmetta. Il destinatario potrà decodificare il messaggio con la sua chiave privata
- **Autenticazione**: nel caso in cui il mittente voglia firmare il documento in modo che possa rivendicarne la proprietà, è sufficiente che al documento applichi la sua chiave privata. Il destinatario potrà leggere il contenuto e verificarne la provenienza con il solo ausilio della chiave pubblica del mittente.

Funzione Hash

Una funzione hash trasforma un messaggio di lunghezza arbitraria in output di lunghezza fissa (impronta)

- Non utilizza la chiave
- Garantisce l'integrità del messaggio

Carattesistiche principali di una funzione hash:

- Coerenza: ad input uguali corrispondono sempre output uguali.
- Casualità: output uniformemente distribuito.
- Univocità: la probabilità che due messaggi generino la medesima impronta è nulla.
- Non invertibile: è impossibile risalire al messaggio originale dall'impronta.
- Minime variazioni sul messaggio comportano variazioni significative sull'impronta
- Computazionalmente poco onerosa

Firma Digitale

Una firma digitale è un "digest" in codice che viene accodato ad un documento e viene utilizzato per comprovare l'identità del mittente e l'integrità del documento.

- Le firme digitali si basano su una combinazione di tecniche crittografiche a chiave asimmetrica e funzioni hash non invertibili.

Funzionamento

Creazione di una firma digitale (Mittente “Alice”)

- “Alice”crea la coppia chiave pubblica/chiave privata.
- “Alice” comunica la propria chiave pubblica al destinatario “Bob”.
- “Alice” scrive un messaggio e crea il digest con la funzione hash non invertibile.
- “Alice” codifica il digest del messaggio con la propria chiave privata ottenendo così la firma digitale.
- “Alice” appende al documento originale la firma digitale così ottenuta ed invia il tutto a “Bob”.
- Le firme digitali si basano su una combinazione di tecniche crittografiche a chiave asimmetrica e funzioni hash non invertibili.

Firma Digitale

La firma digitale offre 3 servizi di sicurezza di base:

- Autenticazione
- Integrità
- Non Ripudio

Lo scopo principale della firma digitale è di identificare il mittente del messaggio e di garantire che il documento non sia stato modificato dal suo stato originale al momento della firma.

L'unico modo per garantire la sicurezza della firma digitale è di garantire che lo scambio iniziale delle chiavi pubbliche avvenga in modo sicuro. E' questa la ragione fondamentale dell'esistenza dei certificati digitali.

Pro e contro

Principali vantaggi:

- Distribuzione delle chiavi semplificata

Principali svantaggi:

- Gli algoritmi a chiave pubblica sono "processor-intensive"
- Generalmente inadatta per cifrare grandi masse di dati

Molte tecnologie fanno un uso ibrido dei metodi di cifratura simmetrica e asimmetrica, impiegando gli algoritmi a chiave asimmetrica per rendere sicuro lo scambio della chiave simmetrica utilizzando quest'ultima per il processo di cifratura di grosse moli di dati.

Algoritmi asimmetrici

Principali algoritmi :

- Diffie-Hellman
- Rivest, Shamir, Adleman (RSA)
- Digital Signature Algorithm (DSA) / ElGama
- Elliptic Curve Cryptosystem (ECC)

Tipi di rete

- **Reti Broadcast**:

  Le *reti broadcast* sono dotate di un unico "canale" di comunicazione che è condiviso da tutti gli elaboratori.

- **Reti Punto-Punto**:

  Le *reti punto a punto* consistono di un insieme di connessioni fra coppie di elaboratori.

Estensioni delle reti

- Reti Personali:

  PAN
- Reti Locali:

  LAN
- Reti Metropolitane:

  MAN
- Reti Geografiche:

  WAN

Stack Tcp/Ip

- Lo stack Tcp/IP nasce per esigenze militari di affidabilità e non di sicurezza.
- L'attuale versione (4) dello stack Tcp/ip non offre funzionalità di sicurezza.
- E' facile falsificare informazioni di trasporto di un datagram Ip (ip sorgente, destinazione, tos)
- Il payload più essere letto da chiunque ne venga in possesso.

Network Address Traslation

- Il Nat permette di modificare l'indirizzo Ip dei pacchetti che transitano su un router.
- Perché utilizzare il nat ?
- Nat crea un falso senso di sicurezza.

Firewall

- E’ un sistema di protezione perimetrale tra due reti (p.es.lan e Internet).
- Un firewall, è un dispositivo che connette una rete fidata “trusted” (presumibilmente sicura) con una rete non fidata “untrusted” (potenzialmente insicura).
- Tutto il traffico da e verso Internet deve passare da un unico nodo (il firewall).
- Il firewall non deve essere visibile.

I punti di forza

- Centralizza le politiche di sicurezza.
- Centralizza i log e i messaggi di allarme.
- Previene il foot-printing.
- Permette di usare sistema di strong security.

Tipologie

- Packet filters e screening routers.
- Application gateways e proxy servers.
- Stateful inspection.
- Soluzioni ibride.

Packet Filter

Un packet filtering firewall semplicemente esamina l'intestazione di ciascun pacchetto (IP) e decide se lasciarlo transitare o di bloccarlo in funzione delle regole definite dall'amministratore del firewall.

Vantaggi:

- Economicità e funzioni di packet filtering svolte anche a livello di router.

Svantaggi:

- Reporting degli eventi limitato
- Non controllano lo stato della connessione, ma solo i singoli pacchetti.

Stateful Packet Inspection

- Mantengono informazioni sullo stato della connessione
  - Mantenendo una tabella delle connessioni correnti e dei loro eventi, sono in grado di rilevare sequenze anomale che potrebbero rappresentare degli attacchi.

Stateful Packet Inspection

Aspetti negativi

- Non effettuano controlli profondi a livello applicazione.
- Non permettono controlli sull'autenticazione utente.

Circuit Level

- Operano a livello sessione della pila ISO/OSI
- Normalmente non includono l'autenticazione utente.
- Richiedono la configurazione, per ogni applicazione, del proxy, tipo browser web.
- Un esempio è il SOCKS: supporta i protocolli TCP e UDP. La versione 5 supporta anche l'autenticazione utente.

Application Gateway

- Utilizzano un set di proxy, uno per ogni applicazione
- Possono richiedere o no la connessione iniziale
- Possono forzare l'autenticazione utente
- Funzionano da intermediari e ogni sessione è sempre il risultato di due connessioni:
  - Client Firewall
  - Firewall Server
- Consente al Firewall di riscrivere l'IP header
- Non attaccabile con procedimenti basati su routing

Rovescio della medaglia:

- Prestazioni condizionate dalla profondità e complessità dei controlli

Limiti di un Firewall

- Non protegge contro virus e trojan
- Non protegge contro nuovi (sconosciuti) attacchi
- Non protegge contro le connessioni che non lo attraversano (modem)
- Non protegge da cattive o inesistenti policy
- Non protegge da attacchi interni (75%-80%)
- Non protegge da attacchi fisici
- Non può fungere da unico punto di difesa

Le regole

- Definizione di una lista in cui ogni elemento (regola) definisce se un particolare tipo di traffico deve passare o non passare.
- Possibilità di utilizzare operatori relazionali.
- E' importante l'ordine delle regole !

“La filosofia del gioco”

- Il design delle policy di un firewall può seguire uno dei seguenti approcci:

  - permetto, e nego tutto il resto

    (+ sicuro)

  - nego, e permetto tutto il resto

    (- sicuro)

Le regole d'oro

- **Stealth rule:**

  E' buona norma inserire come all'inizio della lista, una regola che rende il firewall invisibile.

- **Clean Up rule:**

  Alla fine della lista occorre inserire una regola che neghi tutto il traffico non permesso (drop su catch-all).

Antispoofing e Rfc 1918

Architettura di un firewall

- Il firewall può essere un prodotto hardware o software.
- Se il firewall è software occorre "*bastionizzare*" la macchina su cui gira.
- In generale la configurazione di un firewall e' una operazione complessa.

Intrusion Detection System

Un IDS è un sistema atto ad individuare le intrusioni. E' un sistema hardware e/o software, posizionato in punti strategici del sistema, che analizza eventi sospetti al fine di individuare eventuali attacchi ("intrusion signatures").

I sistemi IDS sono classificati in:

- **Network-Based IDS (NIDS):** impiegati per controllare il traffico di un intero dominio di collisione.
- **Host-Based IDS (HIDS):** progettati per proteggere un singolo sistema.

Network Ids

Un Network IDS è usualmente costituito da sniffer o sensori che vedono il traffico sul mezzo trasmissivo ed un motore (engine) per l'analisi e la gestione.

I sensori operano in modalità promiscua vedendo tutto il traffico. Non appena individuano qualcosa di sospetto inviano un messaggio di notifica alla stazione di analisi, che in base alla configurazione può inviare un alert, resettare la connessione, interagire con il firewall o router per modificare le regole di filtro.

Host Ids

Un Host IDS funziona in modo analogo ad uno scanner antivirus.

Il software IDS gira sul sistema da proteggere come un processo in background. Tale processo continuamente cerca di individuare attività sospette come ad esempio se vengono passati comandi strani attraverso richieste HTTP o se si effettuano modifiche al file system.

Quando l'IDS rileva l'attività sospetta, può tentare di terminare la sessione e/o inviare un alert all'amministratore del sistema.

Falsi positivi

I principali problemi inerenti l'impiego degli IDS riguardano le situazioni di "falsi positivi" e di "falsi negativi".

Si ha un "falso positivo" quando l'IDS rileva un attacco in situazione di traffico legittimo.

D'altra parte la situazione di "falso negativo" si presenta in occasione di un reale attacco non rilevato dall'IDS. Tale situazione non è facilmente rilevabile, se non a posteriori, analizzando le evidenze dei sistemi che hanno subito l'attacco.

Legge sulla privacy (196/2003)

- La legge sulla Privacy, cita in modo esplicito l'obbligo di adottare delle misure minime di sicurezza per i dati ed i sistemi che trattano elettronicamente tali dati.
- L'articolo 34 e l'allegato B indicano quali sono tali misure minime e la loro attuazione.

Misure minime

- Sinteticamente tali misure minime riguardano
  - Sistemi di autenticazione, tali da controllare l'accesso alle informazioni.
  - Sistemi di salvataggio periodico dei dati e loro ripristino.
  - Sistemi che mantengano l'integrità dei dati e degli strumenti informatici (Antivirus).
  - Sistemi per impedire accessi non autorizzati tramite Rete.
  - Gestione e manutenzione degli strumenti informatici utilizzati, sia Hardware che Software.

Tipologie di attacchi

Ip Spoofing

- Lo spoofing si basa sulla supposizione da parte dei servizi offerti dal TCP e dall'UDP che un indirizzo IP sia valido. L'host di un hacker puo' tuttavia utilizzare un routing del codice IP di origine per presentarsi al server nelle vesti di un client valido. Un Hacker può impiegare il routing dell'IP di origine per specificare un percorso diretto verso una destinazione e un percorso di ritorno verso l'origine.

Sniffing

- Gli attacchi a sniffer passivo rappresentano il primo passo prima che un hacker esegua un dirottamento attivo o un attacco IP spoofing. Per iniziare un attacco sniffing, un hacker ottiene user-ID e la password di un utente legittimo e utilizza le informazioni dell'utente per accedere a una rete distribuita.

TCP hijack

- Questo attacco rappresenta la più grave minaccia per i server connessi a Internet. Anche se presenta analogie con l'attacco al numero di sequenza, questo attacco ottiene l'accesso alla rete costringendo la rete ad accettare il suo indirizzo IP come se fosse un indirizzo fidato e dunque l'hacker non è costretto a provare indirizzi IP per trovare quello giusto. L'idea dell'attacco è che l'hacker acquisisce il controllo di un computer che si collega con la rete che rappresenta il suo obbiettivo.

DoS

- DoS è la sigla di **denial of service**, letteralmente *negazione del servizio*. In questo tipo di attacco si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio.

Malware

- Si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche *codice maligno.*

Virus

- Nell'ambito dell'informatica un virus è un frammento di software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente.

Vulnerabilità

- Una vulnerabilità è una componente implicita di un sistema che ne rappresenta un punto debole.
- Ne esistono principalmente di due tipi:
  - *Vulnerabilità software (bug software)*
  - *Vulnerabilità dei protocolli*

Iptables

- Iptables e’ parte integrante di netfilter.
- Netfilter e’ il framework di manipolaggio pacchetti che mette a disposizione il kernel di Linux.
- Supporto kernel 2.4 e 2.6
- Successore di ipfwadm e ipchains

Come installare Ipt

- Iptables e' parte integrante del kernel 2.4 e 2.6.
- Per usare le funzionalità di iptables occorre attivare il supporto dal Kernel.
- Ricompilazione del Kernel.

Architettura

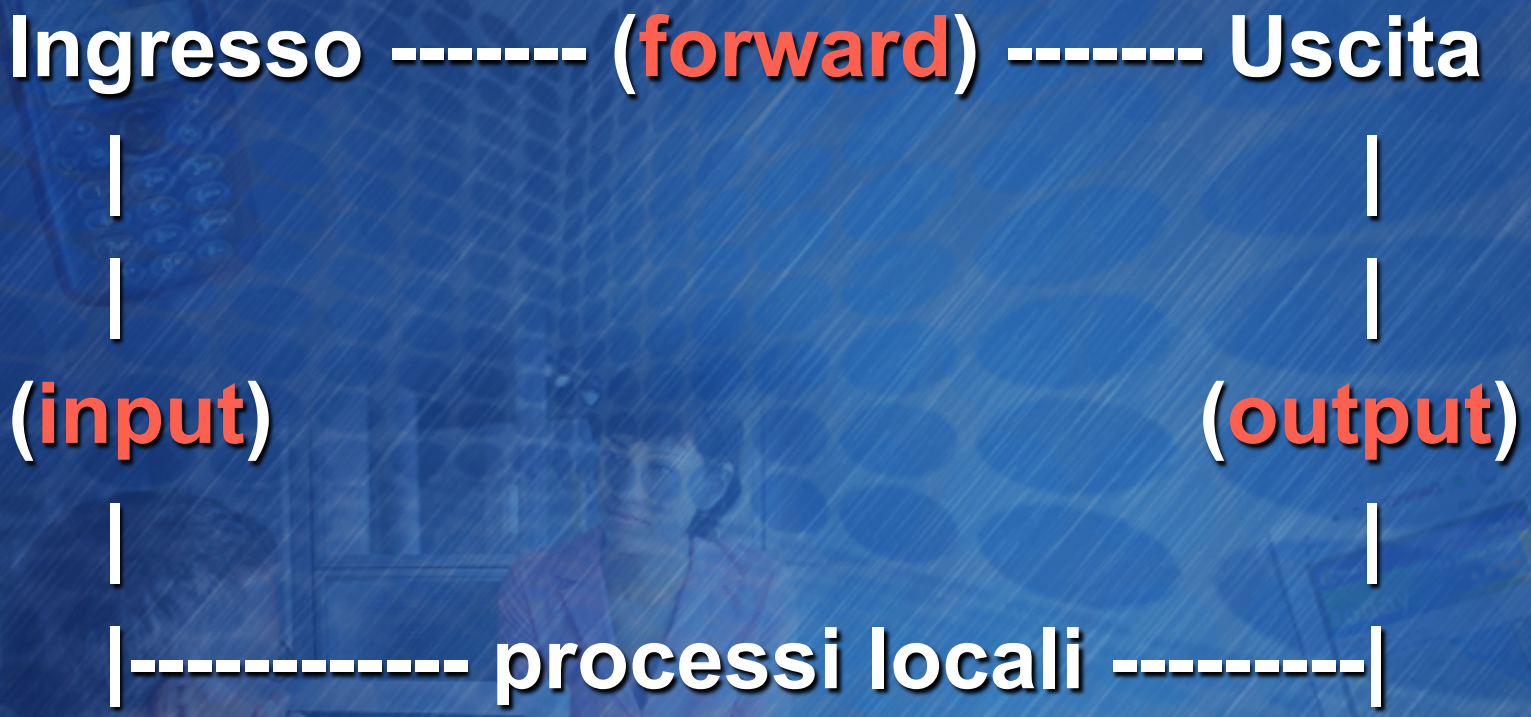
Di default iptable e' composto da tre tabelle:

- Filter
- Nat
- Mangle

Ogni tabella contiene più catene.

Ogni catene e' una lista di regole ordinate.

Filter



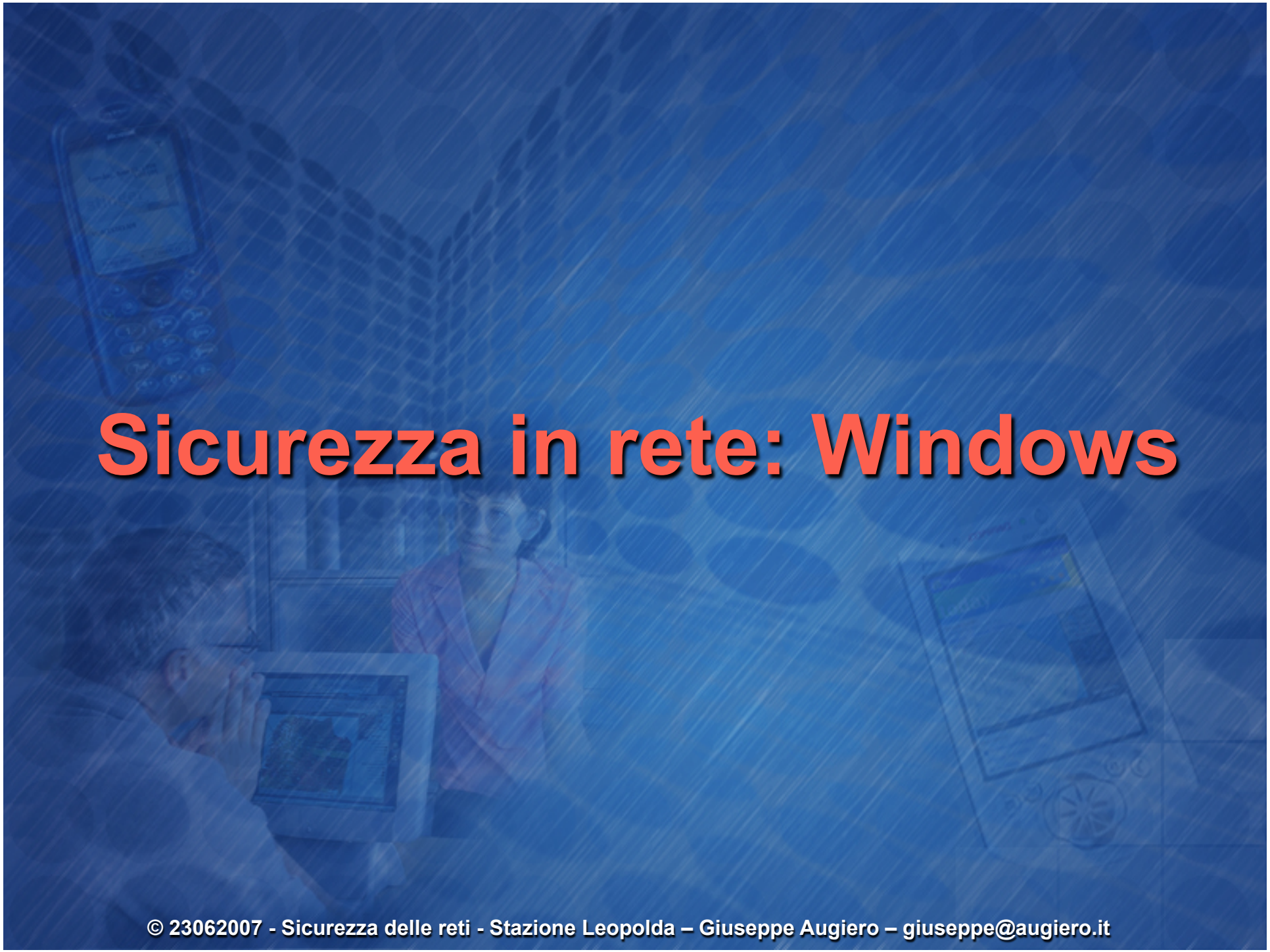
Le policy

- Di default esistono tre catene (Input/ Output/Forward).
- Una catena e' un insieme di regole
- Ogni regola definisce cosa bisogna fare con il traffico identificato.
- Se non esiste una regola per il traffico viene applicata la policy generale della catena.

Azioni da intraprendere

- Accept
- Drop (timeout)
- Reject

- Il traffico in drop o reject può essere monitorizzato e loggato.



Sistemi Windows

- Microsoft Windows rappresenta il sistema operativo che vanta il numero maggiore di installazioni.
- I tipici attacchi sono spesso legati alle vulnerabilità del sistema operativo e ai servizi che di default vengono lasciati attivi sulla macchina.
- Occorre creare una cultura della sicurezza.

Consigli della nonna

- Aggiornare il sistema operativo e i suoi applicativi.
- Installare e utilizzare un firewall.
- Installare un antivirus.
- Installare un antimalware.
- Eliminare i servizi non indispensabili.
- Utilizzare un browser alternativo.
- Eliminare utenti inutili.
- Associare a ogni utente una password robusta.

WiFi

- La necessità di mobilità e copertura in spazi aperti o mal raggiunti dai canonici cavi hanno favorito lo sviluppo di tecnologie wireless.
- Esistono diverse metodologie di trasmissione dati via etere, quali ad esempio GPRS, Bluetooth e 802.11.
- La tecnologia 802.11 è comunemente chiamata Wireless Ethernet o WIFI.

Standard 802.11b/g

- La tecnologia Wireless Lan più diffusa è basata sullo standard IEEE 802.11b.
- La wireless Lan viene vista logicamente come una rete Ethernet tradizionale.
- In particolare il protocollo 802.11 definisce lo strato fisico e il l livello mac per le reti wireless.
- Il livello superiore non si accorge della trasmissione via wireless.

Reti ad hoc

- Una rete ad hoc è composta solo da terminali wireless.
- Non supporta l'accesso alla rete cablata e non necessiata di un punto di accesso.
- Non esiste una struttura.
- Ogni nodo può comunicare con gli altri.

Reti Strutturate

- Le reti strutturate sono divise in celle o BSS (Basic Service Set).
- Le celle sono connesse a una rete che offre servizi chiamata DS (Distribution System).
- Se le zone degli AP si sovrappongono è possibile effettuare il roaming del terminale.

Beacon & Probe Packet

- Quando un dispositivo wireless 802.11 vuole accedere in una BSS, il nodo deve ricevere informazioni di sincronizzazione da un punto di accesso.
- *Scansione passiva*: la stazione attende che arrivi dal punto di accesso il pacchetto di sincronizzazione (Beacon Packets)
- *Scansione attiva*: la stazione tenta di localizzare un punto di accesso inviando dei pacchetti sonda (Probe Packets).

Wep

- Lo standard 802.11 definisce una cifratura opzionali dei dati trasmessi chiamata Wired Equivalent Privacy (WEP).
- Debolezza della cifratura: e' possibile ricavare la chiave di cifratura wep dall'osservazione del traffico di rete.
- Debolezza intrinseca: lo store delle chiavi.
- Falsa sensazione di sicurezza.

Protezione di una rete wireless

- Cambiare il SSID di default
- Utilizzare SSID non descrittivi
- Disabilitare il broadcast SSID
- Cambiare la password
- Aggiornare il firmware
- Utilizzare il Wep
- Abilitare il Mac Filtering
- Spegnere l'Ap quando non serve
- Minimizzare l'intensità del segnale
- Cambiare la community di SNMP
- Non usare Dhcp
- Usare una Vlan separata

Domande????

- Giuseppe Augiero
- giuseppe@augiero.it

Grazie!!!!!!