Università di Firenze
Dipartimento di Elettronica e Telecomunicazioni

Gestione delle Reti di Telecomunicazioni

Sicurezza ?

Ing. **Tommaso Pecorella**

Ing. **Giada Mennuti**

{pecos,giada}@lenst.det.unifi.it

Sicurezza

Il sistema OSI prevede per il framework SECURITY:

Definizione di piani per la sicurezza aziendale, sia fisica che di rete.

- Integrità
- Reperibilità
- Riservatezza

Garantire il rispetto per l'accesso alle risorse della

- Gestione delle autorizzazioni

Sicurezza

In pratica, tra le altre cose:

- **Sicurezza del sistema a livello fisico**
  - Accessi non autorizzati ad aree protette
  - Badges
  - Etc.

- **Sicurezza del sistema a livello dati (intrusioni informatiche)**
  - Attacchi informatici
  - Uso improprio delle risorse informatiche
  - Etc.

… è guerra ?

"All that is necessary for evil to triumph is for good men to do nothing…"

– Edmund Burke

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

– Sun Tzu

Conosci il tuo…

Hacker

Persona che prova piacere nell'esplorare i dettagli dei sistemi programmabili e come estendere le loro capacità, in opposizione alla maggior parte degli utenti, che preferiscono imparare solo il minimo necessario.

5. Uno che programma entusiasticamente (perfino ossessivamente) o che prova piacere nel programmare piuttosto che limitarsi a teorizzare sulla programmazione.
6. Una persona capace di apprezzare (la qualità di un hack).
7. Una persona abile a programmare rapidamente.
8. Un esperto di un particolare programma, o uno che ci lavora frequentemente; come "un hacker di UNIX". (Le definizioni da 1 a 5 sono correlate, e le persone che rientrano in queste categorie possono venire riunite.)
9. Un esperto o un entusiasta di qualunque tipo. Uno potrebbe essere un hacker dell'astronomia, per esempio.
10. Uno che prova piacere nella sfida intellettuale di scavalcare o aggirare creativamente dei limiti.
11. (spregiativo) Un ficcanaso maligno che tenta di scoprire informazioni delicate frugando qua e la'. Da cui derivano "password hacker", "network hacker". (cracker) .

Conosci il tuo…

Lamer

Sono i falsi hacker, si spacciano per hacker ma che non lo sono.

Sono fanfaroni, irritanti e petulanti. Un Lamer chiede a tutti come attaccare un sito e come fare per non farsi tracciare (per non essere riconosciuto, seguito, durante un attacco), per questo si espone al ridicolo e alla possibilità di essere individuato.

Quelli che molti chiamano comunemente Hackers sono solo dei Lamers, ossia individui convinti di essere un Hacker solo perché riescono a fare dei danni a computer altrui utilizzando programmi come NetBus, BackOrifice o SubSeven e che non sarebbero assolutamente in grado di crearli personalmente. Gli Hackers con la H maiuscola non hanno bisogno di introdursi nei computer dei normalissimi utenti che navigano su Internet (sarebbe troppo facile per loro), bensì cercano di "entrare" nei sistemi più sicuri per dimostrare che sono in grado di sconfiggere le più sofisticate tecniche di sicurezza o per diffondere le proprie idee.

Conosci il tuo…

Cracker

Sono pirati-vandali informatici. Hanno le conoscenze tecniche e gli strumenti degli hackers ma li usano per infrangere le protezioni di un sistema per furto o vandalismo. La parola è stata coniata nell'85 dagli hackers per difendersi dall'uso improprio da parte dei giornalisti della parola hacker.

Di solito i crackers sono dei mediocri hacker e tendono a riunirsi in una sorta di società segrete che commettono reati. Comunità di questo genere sono fiorenti in Usa, Australia, Gran Bretagna, Germania e paesi nordici, ma il fenomeno è mondiale. Anche l'Italia è degnamente rappresentata. Sono i falsi hacker, si spacciano per hacker ma che non lo sono.

Conosci il tuo…

Phreaker

"Phone phreaker": specialista nella penetrazione di sistemi telefonici per "scomparire" nel mondo digitale ovvero per "scroccare" telefonate gratis.

The Free On-line Dictionary of Computing

alle voci "hacker", "lamer", "cracker" e "phreaking".

http://info.astrian.net/

Sicurezza fisica

Banale… forse !

- **Sistemi di allarme**
- **Badges sicuri (microprocessori)**
- **Guardie**
- **Controlli biometrici**
- **Backup: evitare che un furto diventi una falla di sicurezza.**

… non ci interessano molto !

Sicurezza Informatica

Conto gli attacchi informatici si usano *Firewall*

Un *firewall* è un:

Muro tagliafuoco. Protezione volta ad evitare che utenti non autorizzati (o programmi) penetrino in un computer o in una rete via internet (da aree non protette).

Firewall, funzionamento

Esistono firewall Hardware o Software.

Sono identici (concettualmente) ma un firewall hardware ha meno probabilità di essere “bucato” ed è genericamente più veloce.

Problema:

vanno configurati altrimenti non servono a nulla.

Un firewall si basa su *regole di scarto*.

ogni pacchetto viene controllato e, se non soddisfa le regole di inoltro, viene scartato;

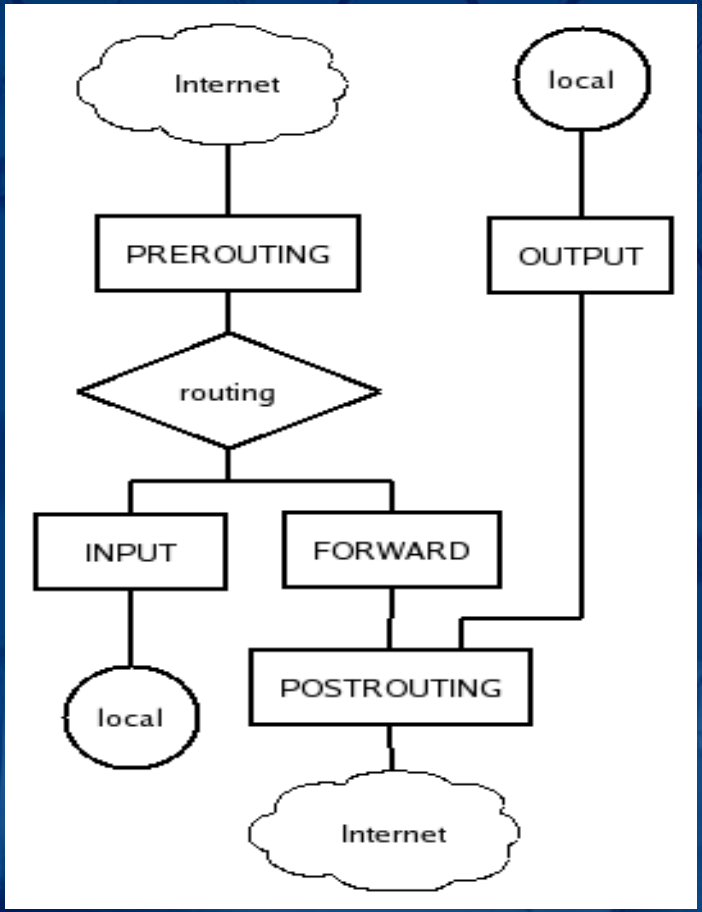
bisogna tarare bene le regole o alcuni servizi non funzioneranno più… *oppure il firewall potrebbe essere bucato.*

https://lenst.det.unifi.it:10000/

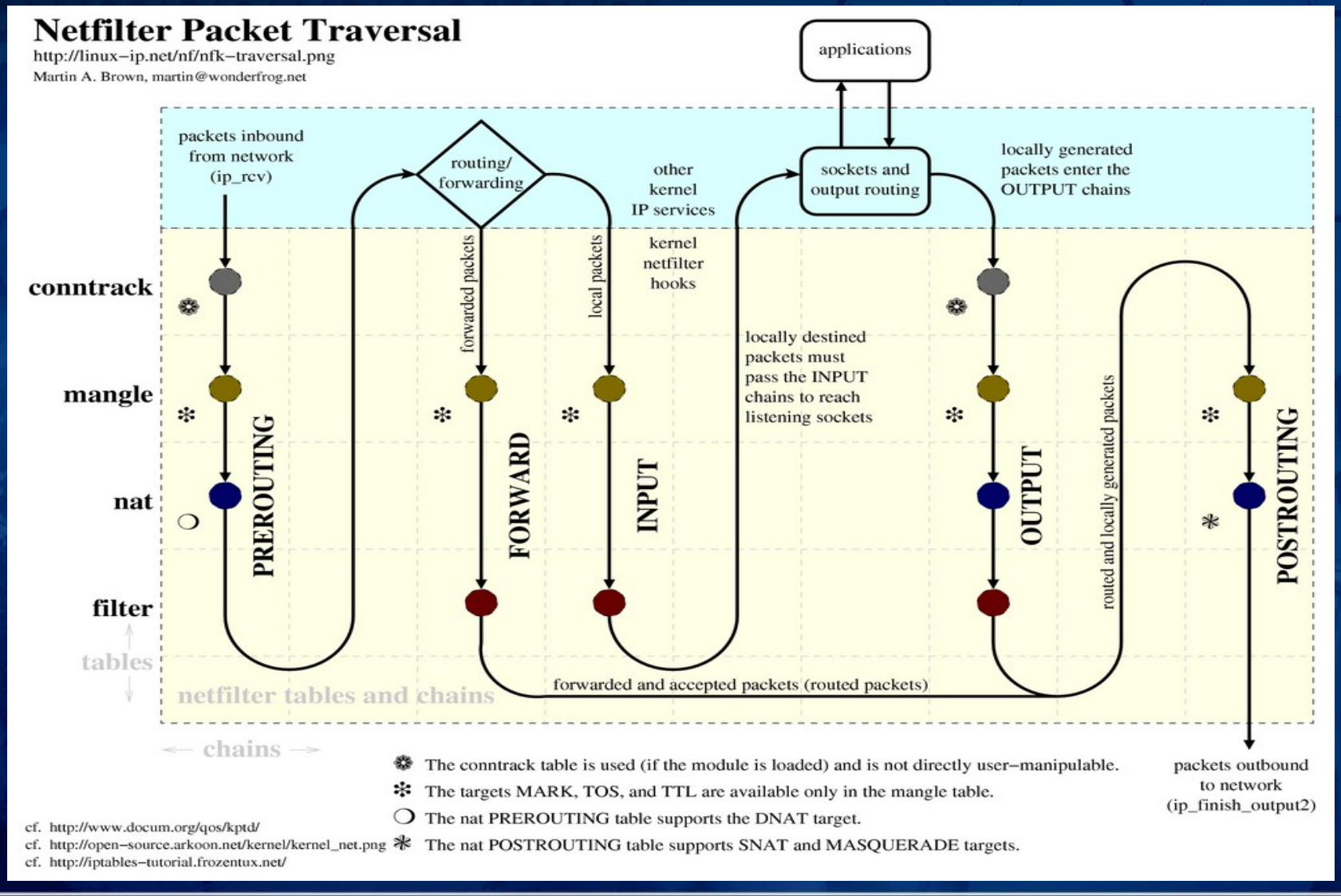
Iptables/netfilter, linux firewalling

I pacchetti all'interno del kernel di linux fanno il percorso in figura:

- Arrivano alla scheda di rete
- Attraversano la catena di PREROUTING
- Il kernel decide dove instradare il pacchetto
- A seconda della destinazione si attraversano:
  - La catena di Input
  - La catena di Forward
- Se attraversano la catena di FORWARD
  - Passano per la catena di POSTROUTING



Netfilter/Iptables



Netfilter/Iptables

Le tabelle (tables) contengono le liste di regole che vengono metchate con i pacchetti che passano nella rete. Ogni tabella definisce diversi target, ovvero l'azione finale da applicare al pacchetto.

Iptables standard tables:

- Mangle Table: serve per modificare alcuni campi dei pacchetti, per esempio il campo ToS o per marcare i pacchetti. Con sistemi compatibili si può utilizzare per la gestione del QoS. I target standard sono :
  - TOS: cambia il campo TOS
  - TTL: cambia il TTL
  - MARK: marca il pacchetto all'interno del suo flusso nel kernel

Netfilter/Iptables

- **NAT table: Network address translation, serve a modificare i cmpi di indirizzo IP dentro agli header del pacchetto. I target possibili sono:**
  - DNAT: destination address translation, si cambia l'indirizzo IP destinazione. Viene utilizzato dai firewall di frontiera per distribuire il carico su una rete con più server.
  - SNAT: source address translation. si cambia l'indirizzo IP sorgente. Viene utilizzato per mascherare una rete privata, di indirizzi non routabili dietro ad un indirizzo pubblico.
  - Masquerade: sostanzialmente la stessa cosa del SNAT

Netfilter/Iptables

- **Filter table: serve a operare il vero filtraggio dei pacchetti, decide quali passano e quali vengono bloccati. I target possibili sono:**
  - Drop: Il pacchetto viene scartato senza dare risposta al mittente.
  - Reject: il pacchetto viene scaratato inviando a destinazione una risposta di reset
  - Accept: il pacchetto continua il suo percorso all'interno del kernel
  - Log: il pacchetto genera un log (su schermo, su file...)

Netfilter/Iptables

Una regola di iptables è inseribile da riga di comando con la seguente sintassi:

iptables [-t table] comando [match] [target]

esempio: iptables -t filter -D INPUT –dport 80 -j ACCEPT

- -t filter: tabella
- -D input: catena
- --dport 80: criterio di match della regola
- -j ACCEPT: target

- **Se non si specifica una tabella si aggiunge la regola nella tabella di filter.**

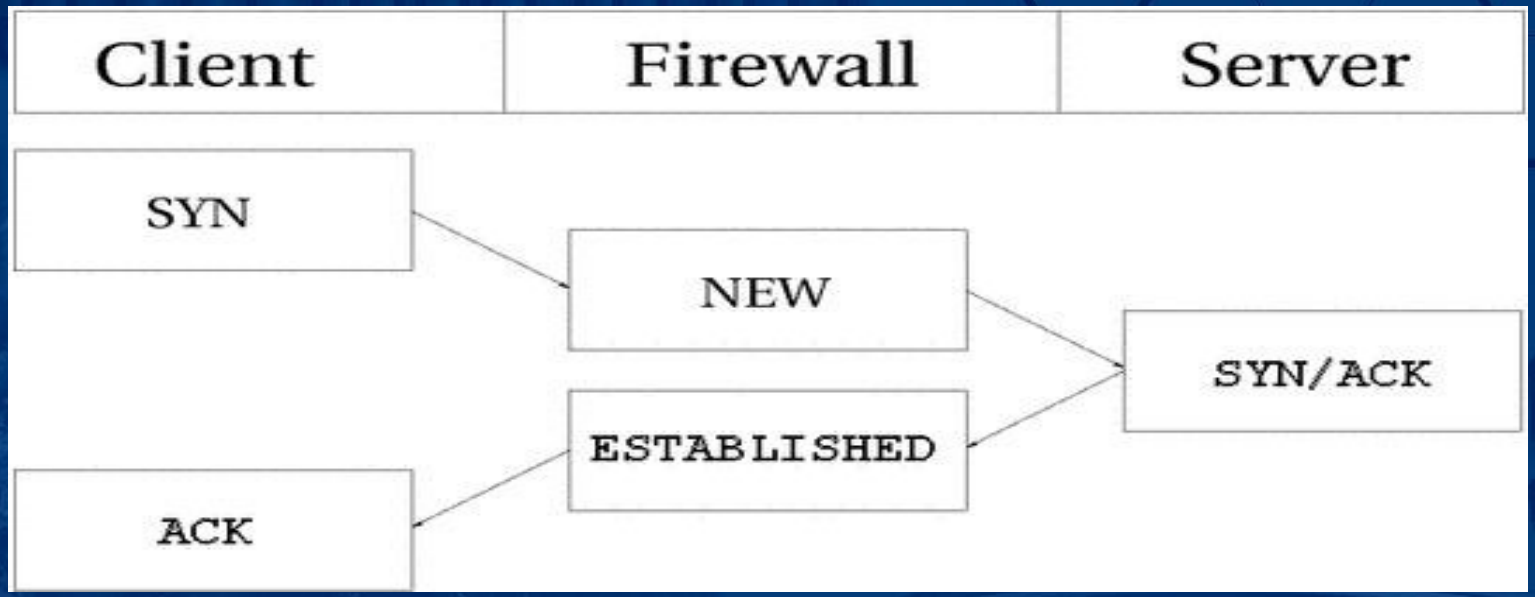
Netfilter/Iptables

Connection State Machine: Ogni connessione viene ricostruita e possiede in ogni istante uno stato. Il modulo *ip_conntrack* si occupa di questo. Una connessione (TCP, UDP, ICMP...) può essere in quattro stati differenti.

- NEW: il kernel ha visto passare pacchetti in una sola direziona
- ESTABLISHED: il kernel ha vistro traffico in entrambe le direzioni
- INVALID: nessuna delle precedenti, si è verificato un errore
- RELATED: per usi specifici, il pacchetto appartiene ad una connessione in qualche modo relazionata ad una già ESTABLISHED

Netfilter/Iptables

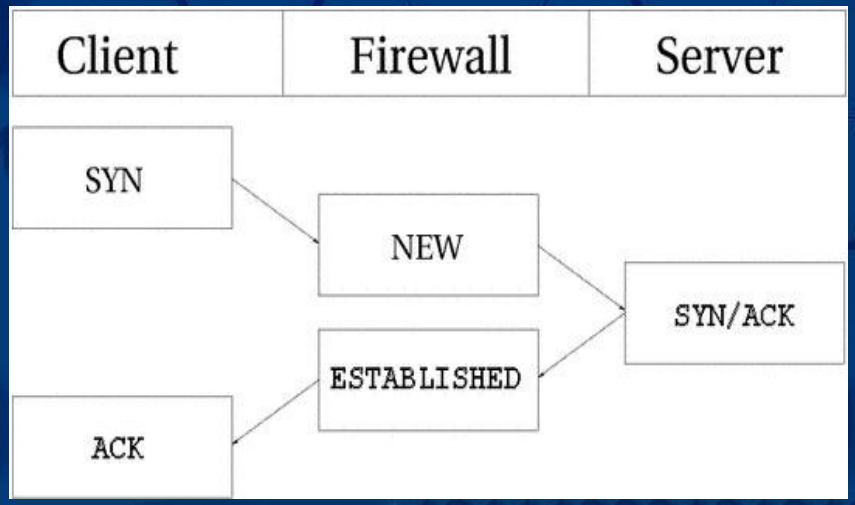
TCP connection tracking:



Come posso filtrare le connessioni verso l'interno senza impedire lo svolgimento di quelle che invece partono dall'interno?

Netfilter/Iptables

- La connessione rimane NEW fino al pacchetto di ACK e non alla fine dell'handhake TCP
- In questo modo si possono filtrare i pacchetti *verso l'interno* lasciando uscire i pacchetti di connessioni già iniziate dall'interno, con le regole:



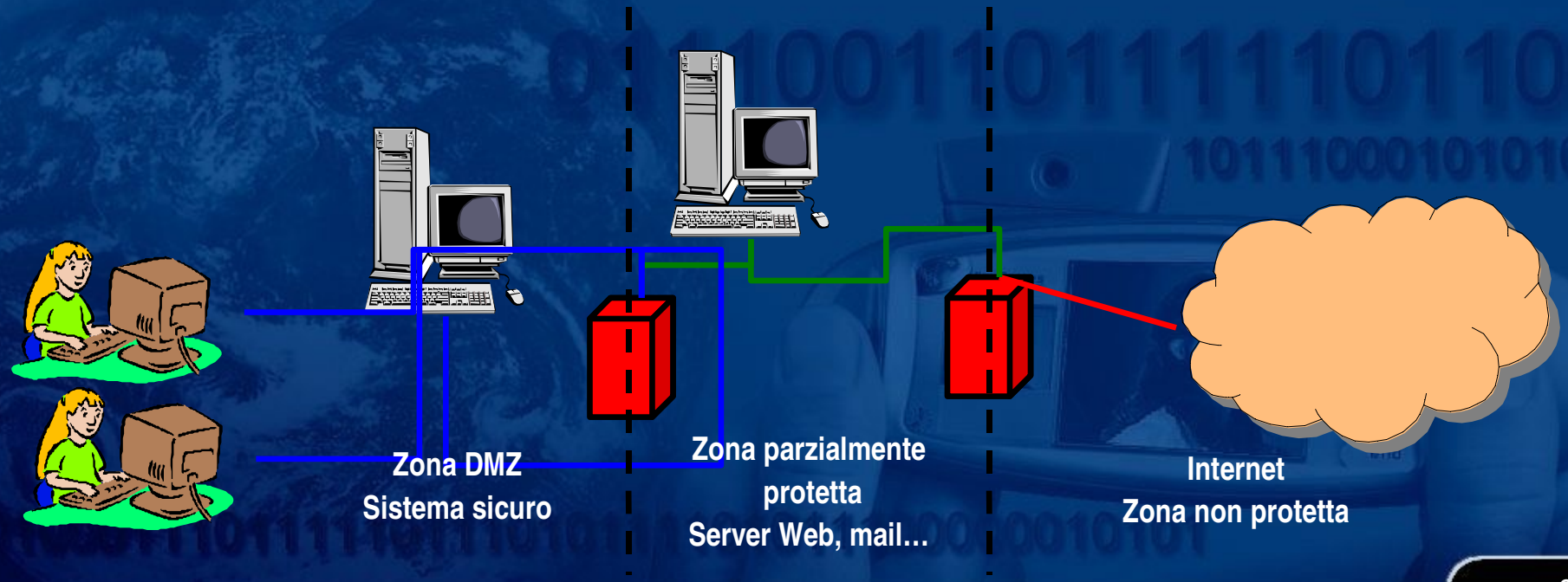
- iptabels -A OUTPUT -j ACCEPT -p tcp -m state –state NEW, ESTABLISHED
- iptabels -A INPUT -j ACCEPT -p tcp -m state –state ESTABLISHED

Zone di sicurezza

Una *qualsiasi* rete aziendale (e non) può e deve essere divisa in *zone*

Ogni zona deve rispettare ben precisi vincoli di sicurezza

- la sicurezza va garantita ai bordi della zona in modo da lasciare libertà all'interno della zona sicura



Firewall… basta ?

- La maggior parte degli attacchi informatici viene da *dentro* un'azienda.
- Un firewall è come un porta blindata… sicurissimo, a patto di non lasciare aperte le finestre !
- In un'azienda di grosse/medie dimensioni è fin troppo facile trovare una borchia di rete lasciata incustodita…

… e allora ?

Soluzione 1: si diventa paranoici (la salute ne risente)

Soluzione 2: si fa finta di niente (si rischia il licenziamento)

Soluzione 3: si installa un *allarme…* come fareste a casa vostra !

Intrusion Detection System (IDS)

Un IDS è un sistema automatico che fa monitoring dell'attività di rete alla ricerca di *patterns* che indichino la presenza di attività non lecite

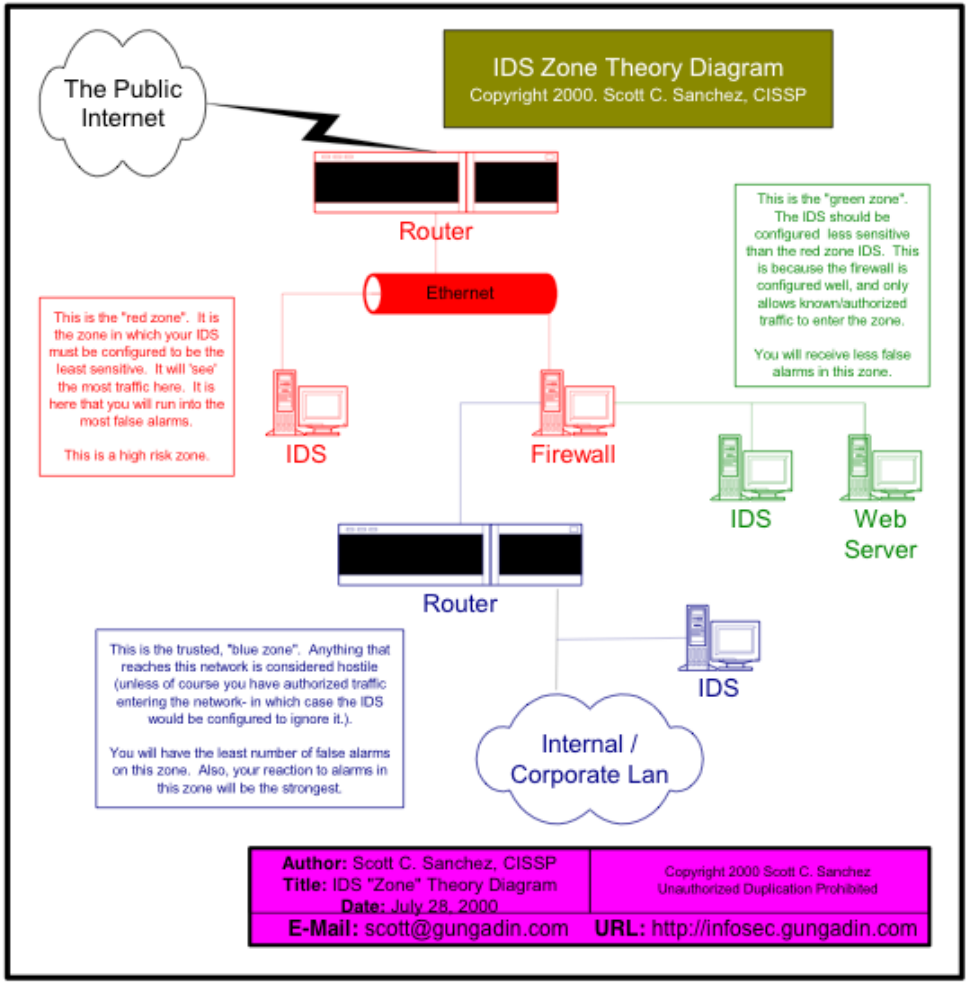
Esempio:

- Port scanning
- Frammenti di pacchetti sospetti
- Pacchetti mal formati
- Tentativi di DoS (Denial of Service)
- Generici attacchi ben conosciuti (lamers !)
- Uso di programmi "proibiti" (P2P come Napster, Kazaaa, eDonkey, etc.)
- Accesso a siti proibiti (filtraggio di indirizzi, es. porn browsing)
- Eccetera…

ATTENZIONE

non difende da un hacker !

Posizione degli IDS



Requisiti di un IDS

- Facile da usare (???)
- Altamente configurabile e modulare
- Espandibile
- Interfaccia grafica
- *Invisibile*

non installereste mai un allarme con una freccia sopra con su scritto “allarme”, premere qui per disattivare…

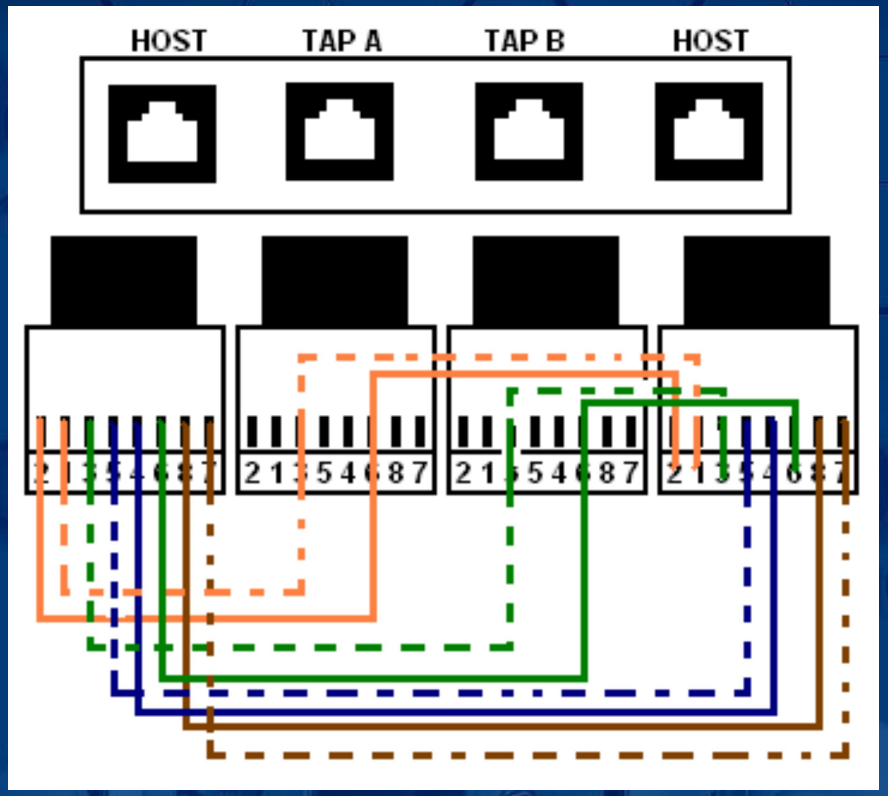
Tap Ethernet passivi

Un tap Ethernet passivo è un dispositivo di ascolto passivo, cioè permette di “vedere” il traffico in transito senza essere visibili

L’IDS verrà connesso ai tap A e B. Potrà essere raggiunto tramite rilocazione fisica del network administrator o tramite una rete dedicata.

ATTENZIONE

La macchina connessa ai tap A e B è invisibile a chiunque… perfetto per lo sniffing !



… e guerra sia.

“la storia dell’informatica è una battaglia tra i programmatori, che creano programmi sempre più idiot-proof e Dio, che crea idioti sempre migliori. E’ inutile notare che Dio sta vincendo”

– Gray Lensman

Esiste una battaglia simile tra gli Hacker e gli addetti alla sicurezza. E’ inutile dire che gli Hacker stanno vincendo, anche perché gli addetti alla sicurezza continuano a giocare in difesa e con il catenaccio…

Nuove frontiere dell'hacking

… noto un IDS, si può escogitare un attacco che lo eviti.

- Attacchi distribuiti
- Attacchi "lenti"
- Uso di risorse legittime per scopi illeciti
- Eccetera

Problema maggiore: l'uso di attacchi distibuiti o lenti
-> pochi allarmi per host, bassa visibilità, IDS ingannato.

IDS…
paralysis by analysis

Un IDS può generare una grandissima mole di allarmi…

Soluzione 0:

si leva l'IDS…

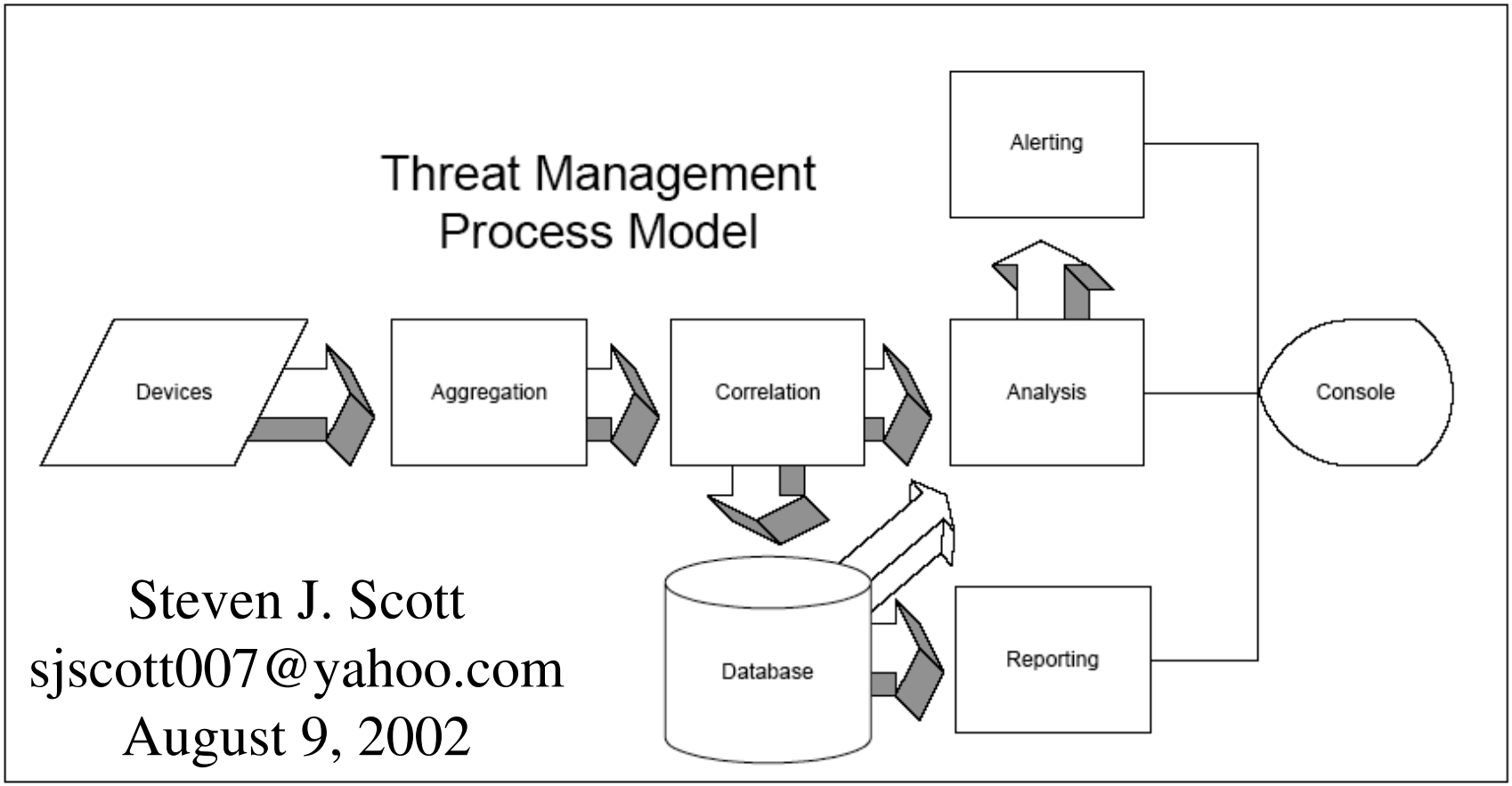
Soluzione 1:

si tara l'IDS su livelli di sicurezza inferiore

Soluzione 2:

si filtrano gli allarmi…

Aggregazione e filtraggio



Steven J. Scott
sjscott007@yahoo.com
August 9, 2002

IDS, tipi diversi:

- **Misuse Detection: si confrontano i pacchetti con un database di firme di attacchi.**
  - + Facile da gestire, i database esistono.
  - - Facile da aggirare, basta cambiare qualche bit dell'attacco.
  - - 0-day attack.
- **Anomaly detection: l'IDS si accorge di comportamenti anomali**
  - + Si accorge anche degli 0-day
  - - Quali sono i comportamenti anomali?

IDS, tipi diversi:

- **On-Line:**
  - Generazione degli alert in base ad eventi correnti
  - Alto peso computazionale (migliaia di regole per migliaia di exploit?)
  - Trigger di reazioni (self defending networks)
- **Off-Line (batch)**
  - Registrazione di eventi su log
  - Analisi degli stessi periodicamente
  - Risultato non istantaneo
  - Possibilità di history

IDS, problemi:

- Banda a disposizione: non sempre si riescono a raccogliere tutti i pacchetti
- Carico computazionale: l'analisi pacchetto per pacchetto e l'analisi trasversale di gruppi di pacchetti (per esempio per individuare un DOS) è molto costosa in termini di memoria e di processore
- Falsi positivi
- Traffico crittografato

IDS, scopi:

- **Gli IDS servono sostanzialmente per due scopi:**
  - Disaster Recovery
  - Individuazione dei responsabili
- **In reti wireless in particolare:**
  - Il disaster recovery è importante per tenere sotto controllo la rete che è accessibile anche dall'esterno e quindi naturalmente prona ad attacchi
  - I responsabili possono essere non identificabili

IDS distribuiti

L'ultima frontiera in quanto a IDS consiste nell'integrare:

3. IDS "classici"
4. IDS sui singoli PC
5. analisi di tool di monitoring (RMON, SNMP)
6. altro

e attraverso analisi di sistemi esperti (database, regole, etc.) filtrare gli allarmi inoffensivi da quelli potenzialmente pericolosi, nonché di generarne di nuovi in caso di allarmi "globalmente" sospetti.

L'obbiettivo è quello di presentare all'addetto alla NS solo gli allarmi significativi e di farlo con la dovuta tempestività.

Nota a margine: ricordarsi sempre di Dio e degli idioti…