Università degli Studi di Verona
Corso di Laurea Magistrale in Informatica

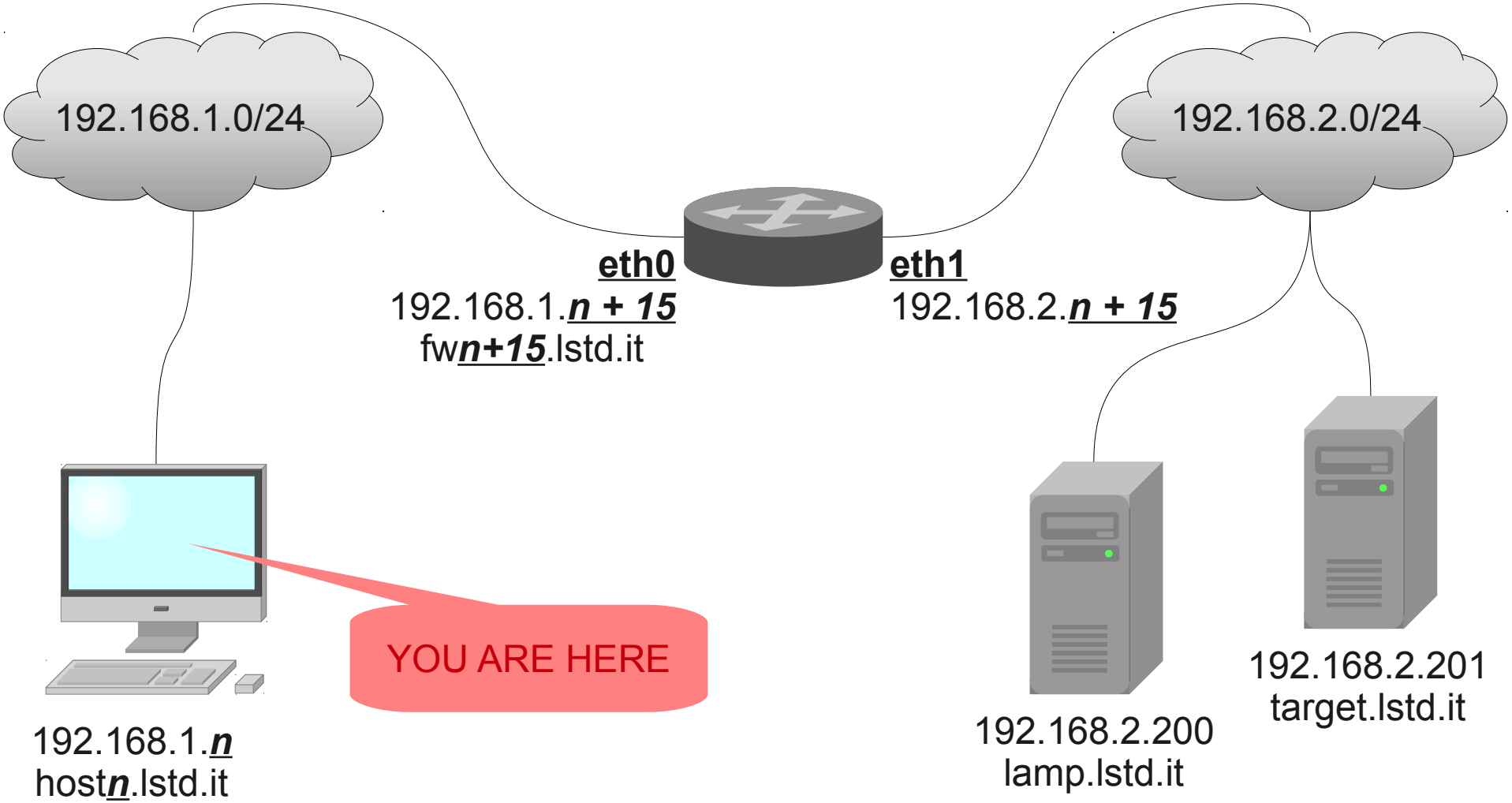
Seminario sulla sicurezza delle reti

Andrea Zwirner

andrea@linkspirit.it

@AndreaZwirner

Laboratorio: collocazione architetturale



Setup: configurazione di rete

- 15 Postazioni:
  - Indirizzo: 192.168.1.***n*** ***n*** in {1..15}
  - Subnet mask: 255.255.255.0
  - Gateway: 192.168.1.***m*** ***m*** = ***n*** + 15

- Esempio: indirizzo 192.168.1.**7**/24
  gateway 192.168.1.**22**

Setup: impostazione del gateway di default

- Linux: route del default
  route add default gw 192.168.1.***k***
- Mac OS X: route delete default
  route add default 192.168.1.***k***
- Windows: route delete 0.0.0.0 mask 0.0.0.0
  route add 0.0.0.0 mask 0.0.0.0 192.168.1.***k***
- Test: ping 192.168.2.201 (target.lstd.it)

Setup: impostazione degli hosts

- Editare come amministratore il file
  - Linux: /etc/hosts
  - Mac OS X: /private/etc/hosts
  - Windows: C:\WINDOWS\system32\drivers\etc\hosts

- Aggiungere le righe

  192.168.1.***k*** fw***k***

  192.168.2.200 lamp

  192.168.2.201 target

- Test: http://target/ oppure http://lamp/

Setup: accesso al gateway

- Il vostro gateway è sotto il vostro controllo
  - 192.168.1.***k*** fw***k***.lstd.it ***k*** in {16..30}
  - Username: root
  - Password: **WARNING**: INCIDENT RESPONSE STRATEGY NOT DEFINED
- Test: ssh root@192.168.1.***k***

Setup: accesso al gateway

- Il vostro gateway è sotto il vostro controllo
  - 192.168.1.***k*** fw***k***.lstd.it ***k*** in {16..30}
  - Username: root
  - Password: fw***k***-pwd
- Test: ssh root@192.168.1.***k***

La sicurezza informatica

- Insieme di misure di carattere organizzativo, tecnologico e procedurale mirate a garantire

  - CONFIDENZIALITÀ
  - INTEGRITÀ
  - DISPONIBILITÀ

  dell'informazione.

Come funziona

- Definizione di politiche di accesso a servizi e informazioni
  - autenticazione → chi è chi
  - autorizzazione → chi può fare cosa
- Difesa perimetrale
- Difesa interna

Di cosa parliamo oggi

- Rilevazione delle anomalie e gestione degli allarmi da parte di
  - Host sotto attacco
  - Apparati di rete
- Configurazione di IPS
- Definizione di politiche di filtraggio
- Configurazione e verifica di firewall

Netfilter

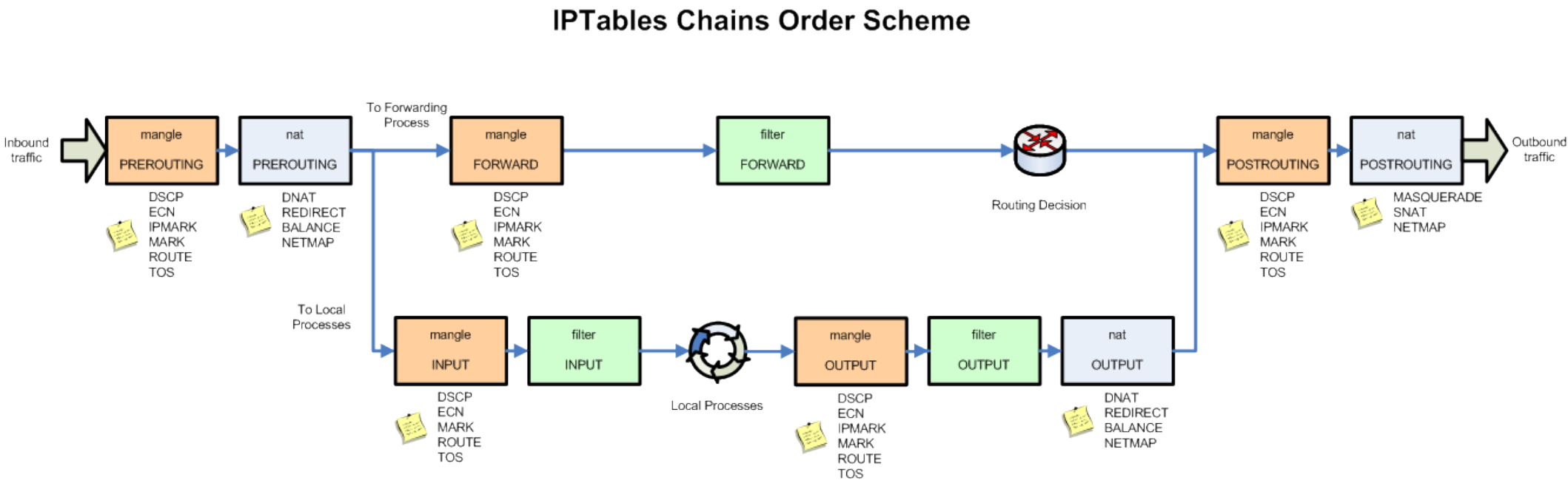
- Strumento di filtraggio disponibile nel kernel Linux
  - ipchains (kernel 2.2)
  - iptables (kernel 2.4 e successivi)

- Funzionalità
  - Filtraggio stateless e statefull
  - Manipolazione di pacchetti
  - Address and port translation (NAT, DNAT, SNAT, etc)
  - QoS e policy-based routing con tc ed iproute2
  - Filtering a layer 7 (L7-filter)

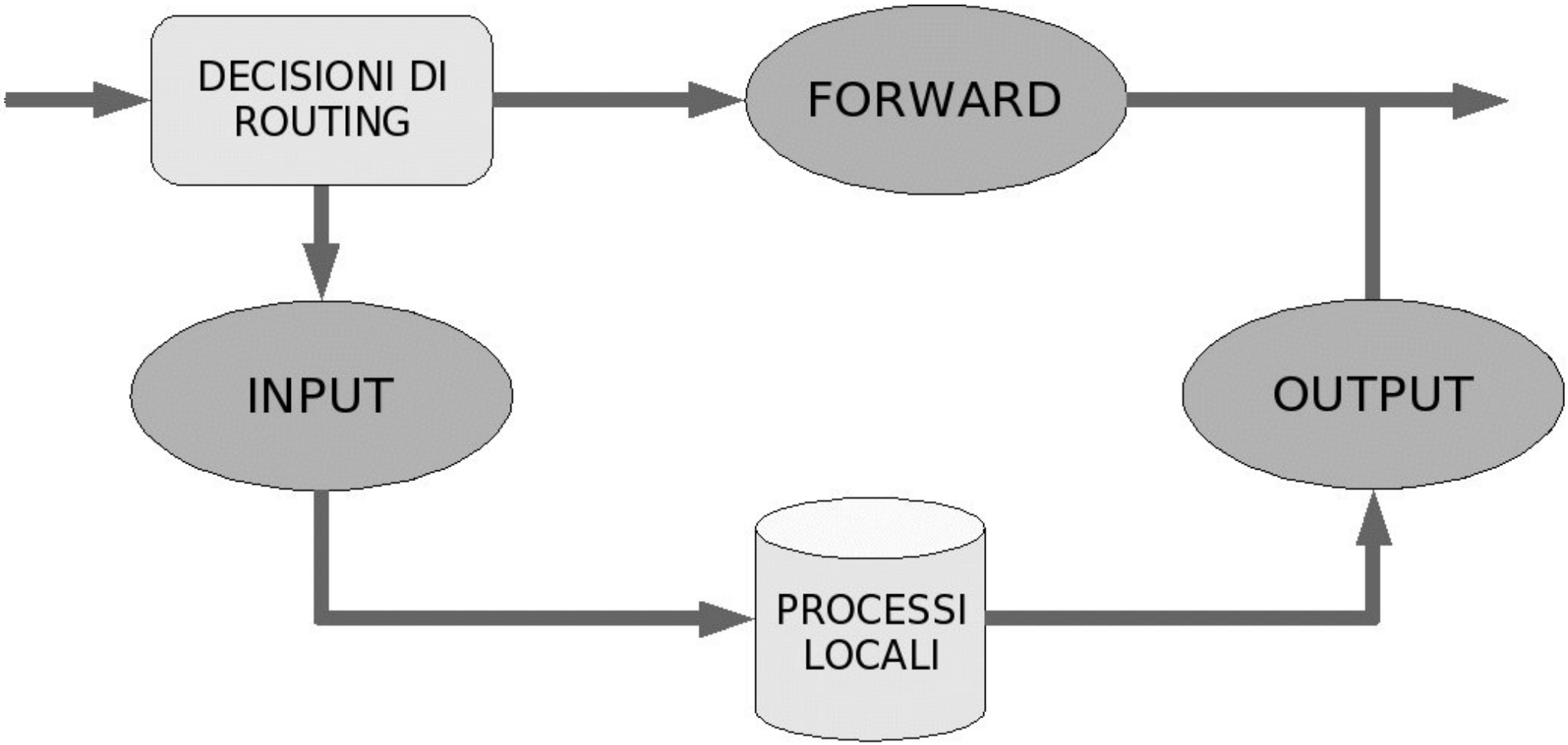
La struttura di Netfilter

- Basata su tabelle
- Le tabelle sono suddivise in catene
- Le catene sono composte da regole

Linux Iptables Firewall Schema



Particolare: la tabella di filtraggio



La tabella filter

- Effettua il filtraggio del traffico
- INPUT
  - Pacchetti in ingresso, destinati all'host locale (userspace)
- FORWARD
  - Pacchetti in transito, non destinati all'host locale
- OUTPUT
  - Pacchetti in uscita, generati dall'host locale

La tabella nat

- Permette di effettuare attività di NAT (D/S-NAT, redirezione porte, etc)
- PREROUTING
  - Pacchetti in transito prima della decisione di routing
- POSTROUTING
  - Pacchetti in transito dopo della decisione di routing
- OUTPUT / INPUT (ker 2.6.34)
  - Pacchetti in uscita / entrata

La tabella mangle

- Permette di alterare i pacchetti in transito (QoS) nelle fasi di:
  - PREROUTING
  - INPUT
  - FORWARD
  - OUTPUT
  - POSTROUTING
- To mangle: rovinare, storpiare, fare scempio
- Non dev'essere usata per il filtraggio

Applicazione delle regole da parte di Netfilter

- Per ogni pacchetto in transito in una catena
- Le regole della catena vengono scorse in ordine di inserimento
- Alla prima corrispondenza
  - Viene eseguita l'azione definita (*target*) per la regola
  - Il controllo torna alla tabella (non per LOG)
- In assenza di corrispondenze, viene applicata la regola di default (*default policy*)

Visualizzazione delle tabelle

iptables [-t tabella] -n [-v] [--line-numbers] -L [<CATENA>]

- tabella: filter (default), nat, mangle
- CATENA: INPUT, OUTPUT, FORWARD, etc

- Esempio: iptables -nL INPUT

Svuotamento delle catene

iptables -F <CATENA>

- Esempio: iptables -F INPUT

Impostazione della policy di default

iptables -P <CATENA> <AZIONE>

- CATENA: INPUT, OUTPUT, FORWARD
- AZIONE (target)
  - ACCEPT accetta il pacchetto
  - DROP scarta il pacchetto

Esempio 1

Impostazione di default policy

Impostare a DROP la default policy della catena di INPUT

Definizione di regole: aggiunta

- Aggiunta (accodamento) di una regola ad una catena

iptables -A <CATENA> [opzioni] -j AZIONE

- AZIONE
  - ACCEPT
  - DROP
  - QUEUE manda il pacchetto in user-space
  - RETURN termina l'attraversamento della catena
  - LOG logga il pacchetto (--log-prefix)

Definizione di regole: gestione

- Rimozione di una regola da una catena

iptables -D <CATENA> [opzioni] -j AZIONE

- Inserimento/Sostituzione/Rimozione della ***k***-esima regola

Inserimento:	iptables	-I	***k*** [...]
Sostituzione:	iptables	-R	***k*** [...]
Rimozione:	iptables	-D	***k***

Definizione di regole: opzioni

Opzioni

- --protocol, -p <protocollo>
- --syn Si tratta di pacchetto SYN
- --source, -s <indirizzo>[/<maschera>]
- --destination, -d <indirizzo>[/<maschera>]
- --source-port, --sport <porta>[:<porta>]
- --destination-port, --dport <porta>[:<porta>]
- --in-interface, -i <interfaccia>
- --out-interface, -o <interfaccia>

- Operatore not: “!” – attenzione a spaziarlo

Esempio 2

Come evitare di chiudersi fuori

Impostare permesso di accesso da proprio IP

Impostare a DROP la default policy della catena di INPUT

Esercizio 1

Proteggere il firewall

Impedire accesso SSH al proprio firewall da parte degli altri

Impedire che gli altri possano utilizzare il proprio firewall come gateway (per raggiungere target)

Cercate di evitare di chiudervi fuori :-)

Estensioni per il matching

-m <match> [--match-options]

- Moduli che estendono le capacità di matching
- Ogni modulo ha le proprie specifiche opzioni aggiuntive

Tipologie di indirizzi

-m addrtype --src-type <TIPO>, --dst-type <TIPO>

- Basati sulle tabelle di routing

- Tipi di indirizzi:
  - UNSPEC — non specificato (e.g. 0.0.0.0)
  - LOCAL, PROHIBIT
  - UNICAST, BROADCAST
  - …

Commenti

-m comment – comment “questa regola non serve a nulla”

Limiti

-m limit --limit <quantità>/second /minute /hour /day

- Un pacchetto corrisponde fintanto che il numero di pacchetti che corrispondono alla regola spera il limite

- L'opzione --limit-burst indica il numero massimo d pacchetti da lasciar passare prima di attivare il matching

MAC address

-m mac --mac-source XX:XX:XX:XX:XX:XX

MAC address

-m mac --mac-source XX:XX:XX:XX:XX:XX

A chi viene in mente qualcosa?

MAC address

-m mac --mac-source XX:XX:XX:XX:XX:XX

Italians: spaghetti, pizza, mandolino, ARP spoofing!

Scenario d'attacco

- L'attaccante avvelena la tabella ARP del client sostituendo il MAC del gateway con il proprio
- Il client inizia ad inviare all'attaccante le comunicazioni per target
- L'attaccante le inoltra al gateway (includendovi il proprio MAC address), affinché questo le inoltri a sua volta a target
- Il traffico di ritorno passa quindi di nuovo nelle mani dell'attaccante

Esercizio 2

ARP spoofing mitigation (dei poveri)

Implementare un sistema lato firewall che

impedisca agli altri host di rete di

intercettare il proprio traffico con target

Mitigare non è risolvere

- In questo caso per mitigare gli effetti dell'ARP spoofing creiamo un DOS

- La perdita in disponibilità di servizio sembra comunque un costo trascurabile in cambio del beneficio in confidenzialità ed integrità

Ispezione degli stati

-m state --state <STATO>

- STATI
  - NEW

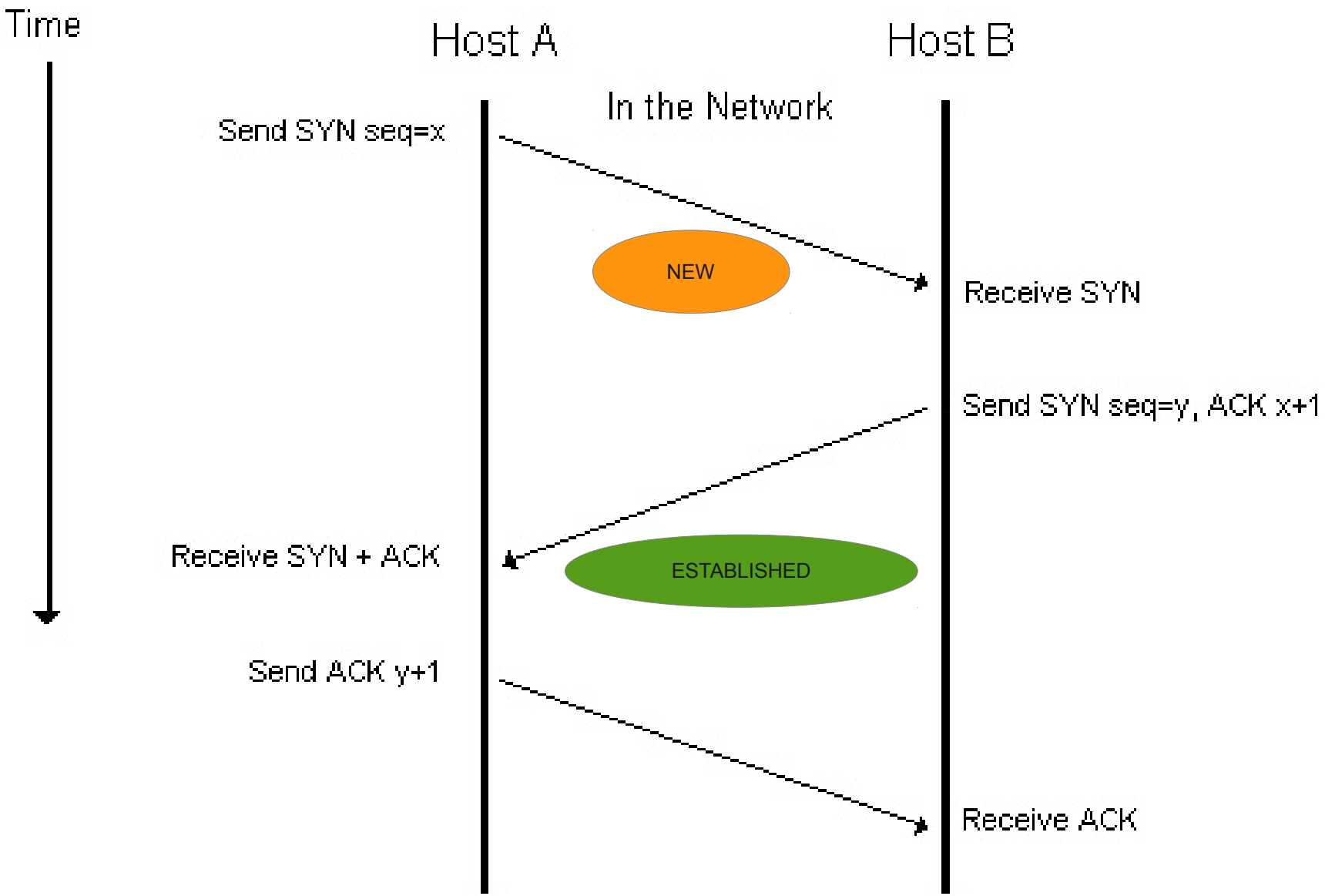
    Pacchetto SYN dell'handshaking di connessione o primo pacchetto di connessione stateless.

    La connessione non ha ancora visto pacchetti in entrambe le direzioni

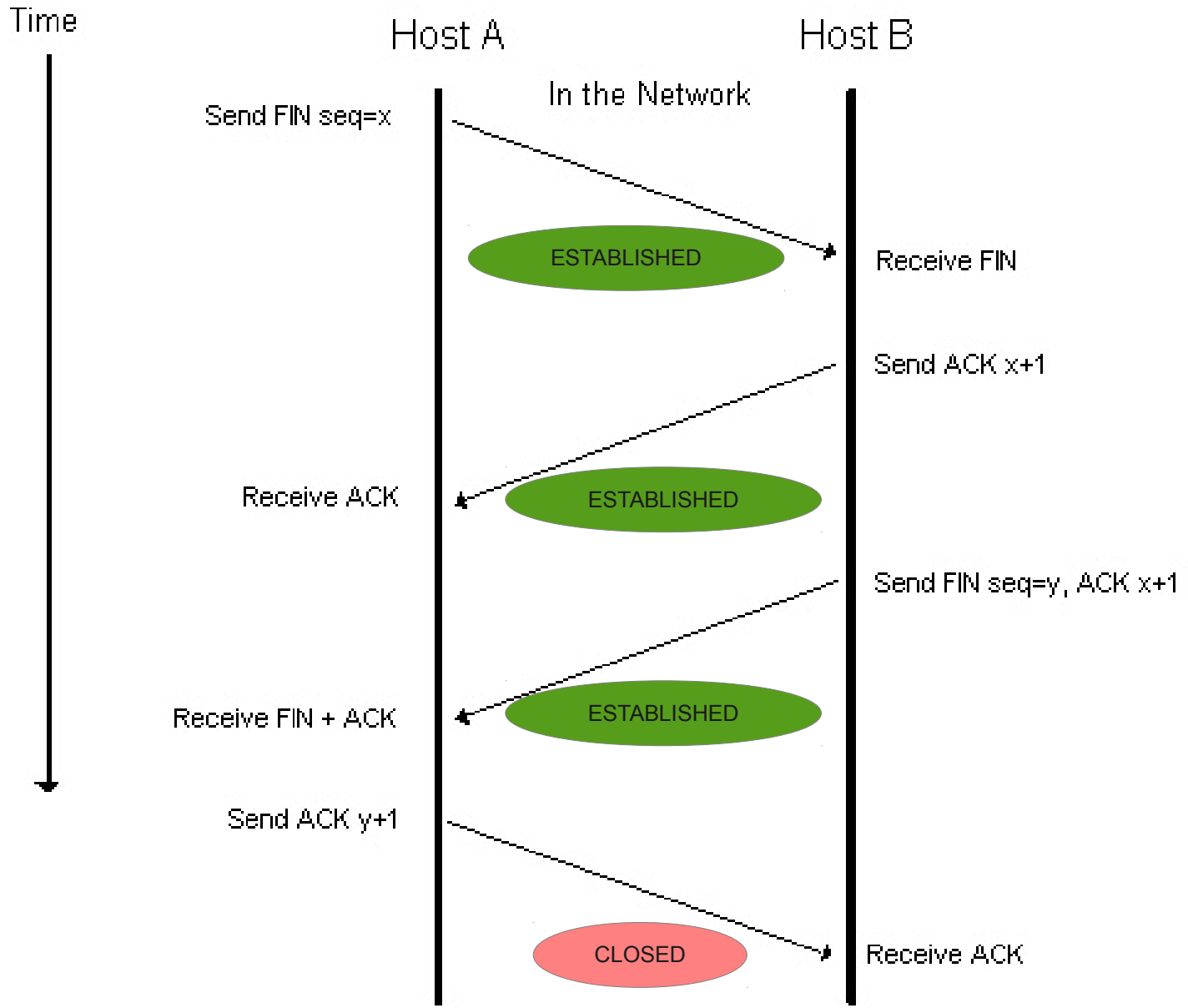
  - ESTABLISHED

    Pacchetto appartenente ad una connessione attiva (dal primo pacchetto della seconda direzione)

Handshake a 3 vie ed ispezione degli stati



Handshake a 4 vie ed ispezione degli stati



Ispezione degli stati

-m state --state <STATO>

- STATI
  - RELATED

    Pacchetti non facenti parte di una connessione, ma ad essa collegati (e.g. FTP data transfer, ICMP error, etc)

  - INVALID

    Nessuno degli altri.

    Non necessariamente malevolo: errori di rete, risorse per il tracciamento delle connessioni sature, etc

Esercizio 3

Correzione del problema riscontrato nell'Esempio 2

Impostare a DROP la default policy della catena di INPUT

facendo in modo da non chiudersi fuori e che le risposte

alle richieste inviate possano raggiungere il firewall

Filtraggio a layer 7

- Richiede modulo aggiuntivo *L7-filter*

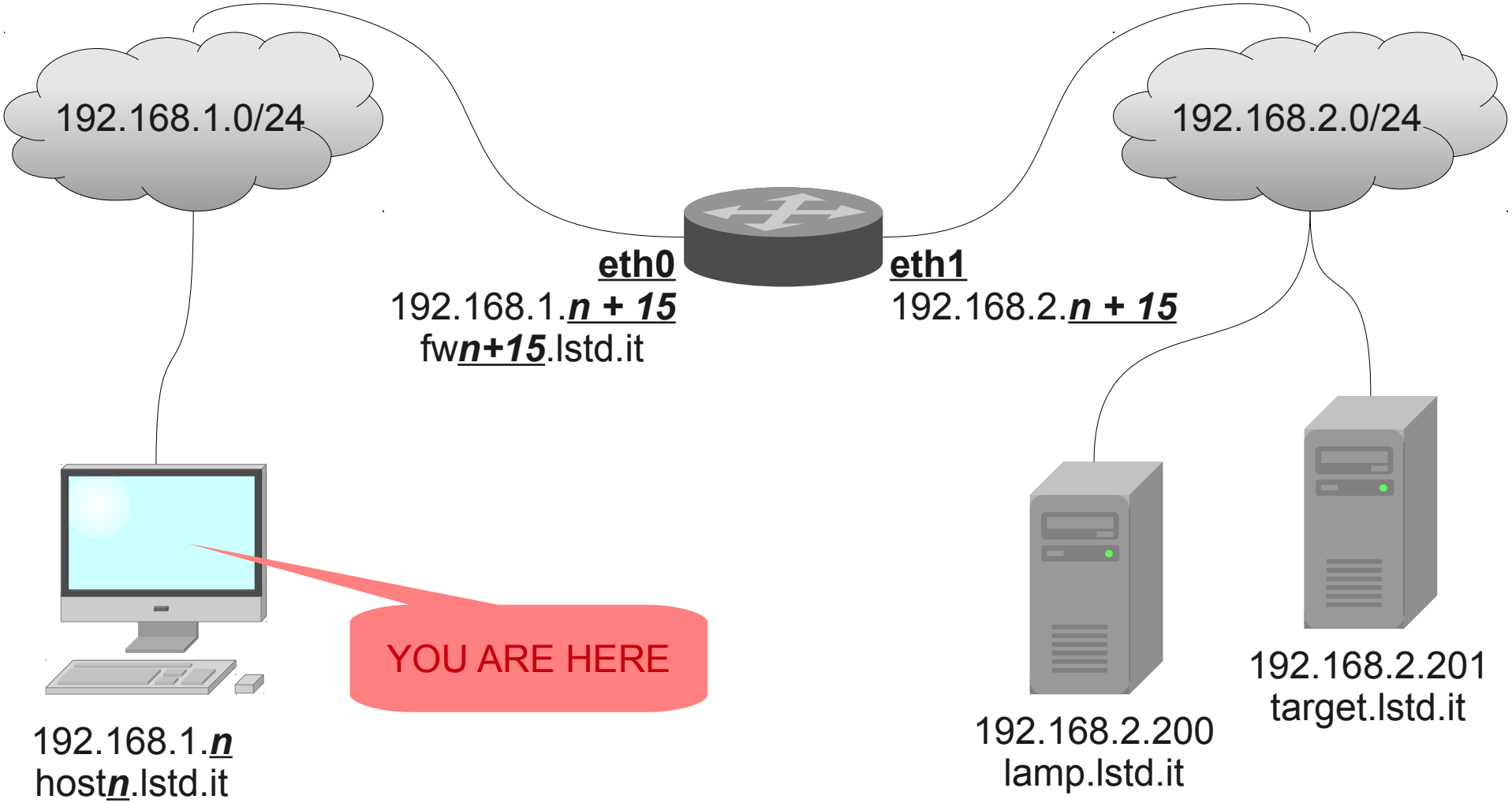
-m layer7 --l7proto <protocollo>

- I protocolli sono quelli che ci si può aspettare (http, ftp, tenlet, etc) a cui si aggiungono
  - unset: pacchetti iniziali per cui non è ancora stata rilevato il protocollo
  - unknown: protocollo sconosciuto

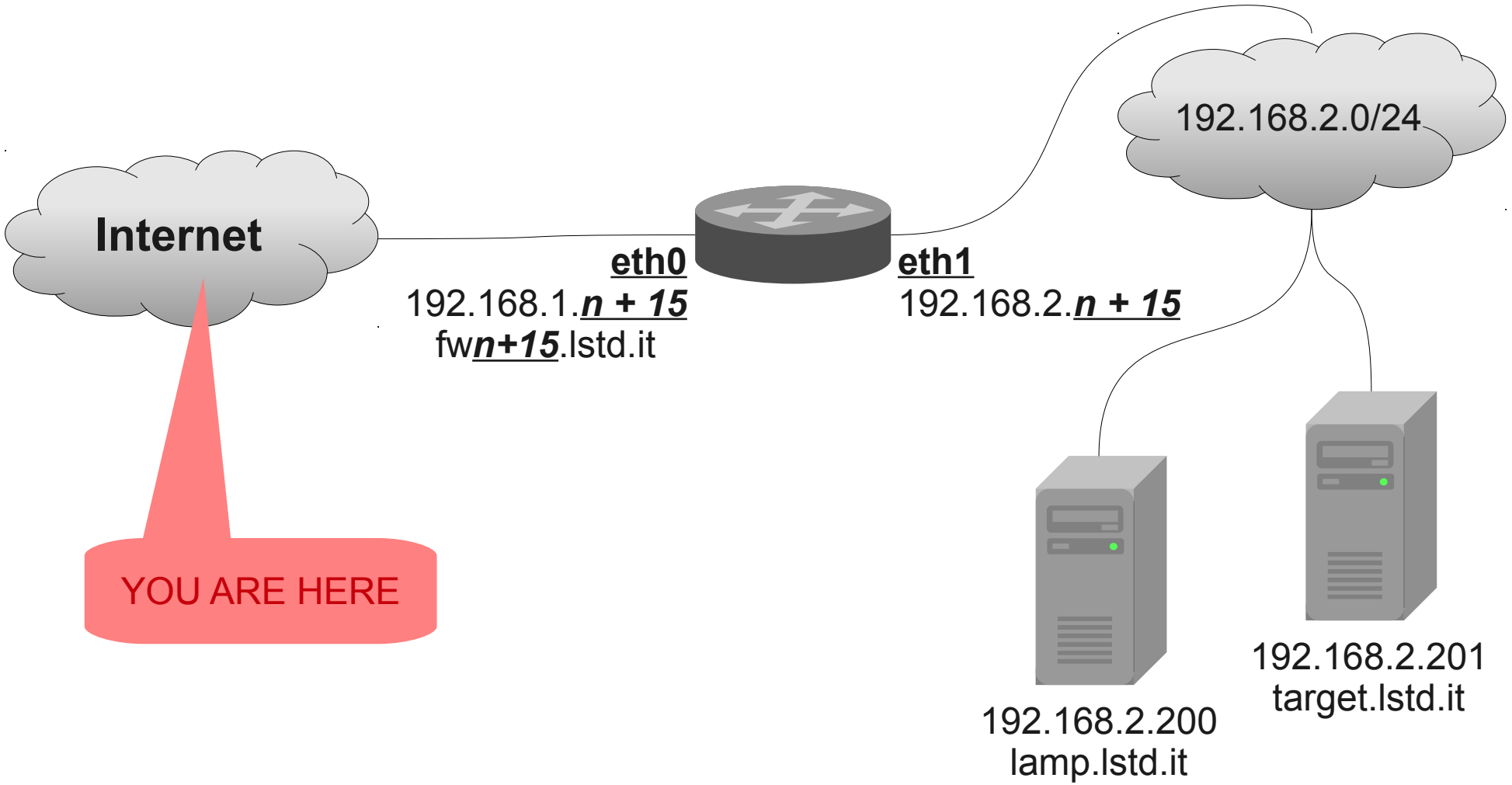
Progettazione di un sistema IDS

- Formalizzazione dei comportamenti attesi
- Identificazione delle anomalie
- Definizione (ed implementazione) delle modalità di rilevazione delle anomalie
- Gestione degli allarmi
- Messa in atto di strategie di difesa

Laboratorio: collocazione architetturale



Laboratorio: rivisitazione architetturale



Formalizzazione dei comportamenti attesi

- Ricezione di richieste da Internet verso il server su porte standard 80, 443, 21, 22, e con protocolli standard
- Ricezione di risposte alle richieste dal server verso Internet
- Invio di richieste dal server solo verso server prestabiliti (DNS, updates, API, etc)
  - Di difficile implementazione, ma estrema efficacia
- Previsione dei range entro cui staranno i volumi di richieste e di traffico di rete in ingresso ed uscita

Formalizzazione dei comportamenti attesi

- Indirizzamenti del traffico in transito sulle interfacce fisiche e virtuali confacenti il contesto architetturale
  - Traffico host, di rete locale, di reti note, di altre reti

Identificazione delle anomalie

- Ricezione di connessioni su porte diverse dalle predefinite
- Ricezione di richieste che fanno uso di protocolli inattesi
- Ricezione di risposte a richieste non transitate
- Volumi di richieste e/o traffico fuori dai range prestabiliti
- Ricezione di traffico con indirizzamenti non conformi

Identificazione delle anomalie

- Invio di richieste verso destinazioni inattese da parte del server

Modalità di rilevazione delle anomalie

- Analisi del traffico di rete
- Analisi dei log di sistemi ed apparati
- Analisi dei log di servizi ed applicazioni
- Correlazione delle informazioni ottenute

Allarmi

- Mail, sms, piccioni viaggiatori, segnali di fumo, etc
- Possono avere fine informativo o attivare processi di incident handling / response / investigation

Messa in atto di strategie di difesa

- Sbattere fuori chi pare “ci abbia provato”

Messa in atto di strategie di difesa

- Sbattere fuori chi pare “ci abbia provato”
- Fermandosi qui, sul lungo periodo si perde
- L'arrocco non è una strategia di difesa efficace
  - Impedisce di osservare il comportamento dell'attaccante e di comprenderne i fini
  - Informa l'attaccante sulle nostre strategie di rilevazione
  - Lo indirizza nella ricerca di nuovi metodi di attacco, che prima o poi andranno a buon fine

Messa in atto di strategie di difesa

- Proiezione dell'attaccante in rete honeypot
- Analisi delle attività svolte
  - Comprenderne il background
  - Valutarne la motivazione e, soprattutto, i fini
- Estremamente efficaci quando coinvolgono contesti differenti
  - E' possibile rilevare il montare della minaccia in ambiti specifici

Log-Based IDS

- Fanno uso dei log come fonte di informazione per la rilevazione di anomalie
- Sono semplici ed economici da implementare
- Quasi ogni cosa produce log, che possono essere correlati
  - Visibilità delle attività di sistema (kernel, demoni, servizi)
  - Visibilità del livello applicativo

Log-Based IDS: OSSEC

- Esistono diversi LIDS, fra cui OSSEC

  - Multipiattaforma e sicuro (chroot, least privilege)
  - Ha centinaia di template per l'analisi dei log ed è facilmente estensibile
  - Scalabile e Client/Server (correlazione di log da diverse fonti: router, firewall, server, sonde, etc)

Log-Based IDS domestici

- Noi però ne scriveremo uno manualmente :-)

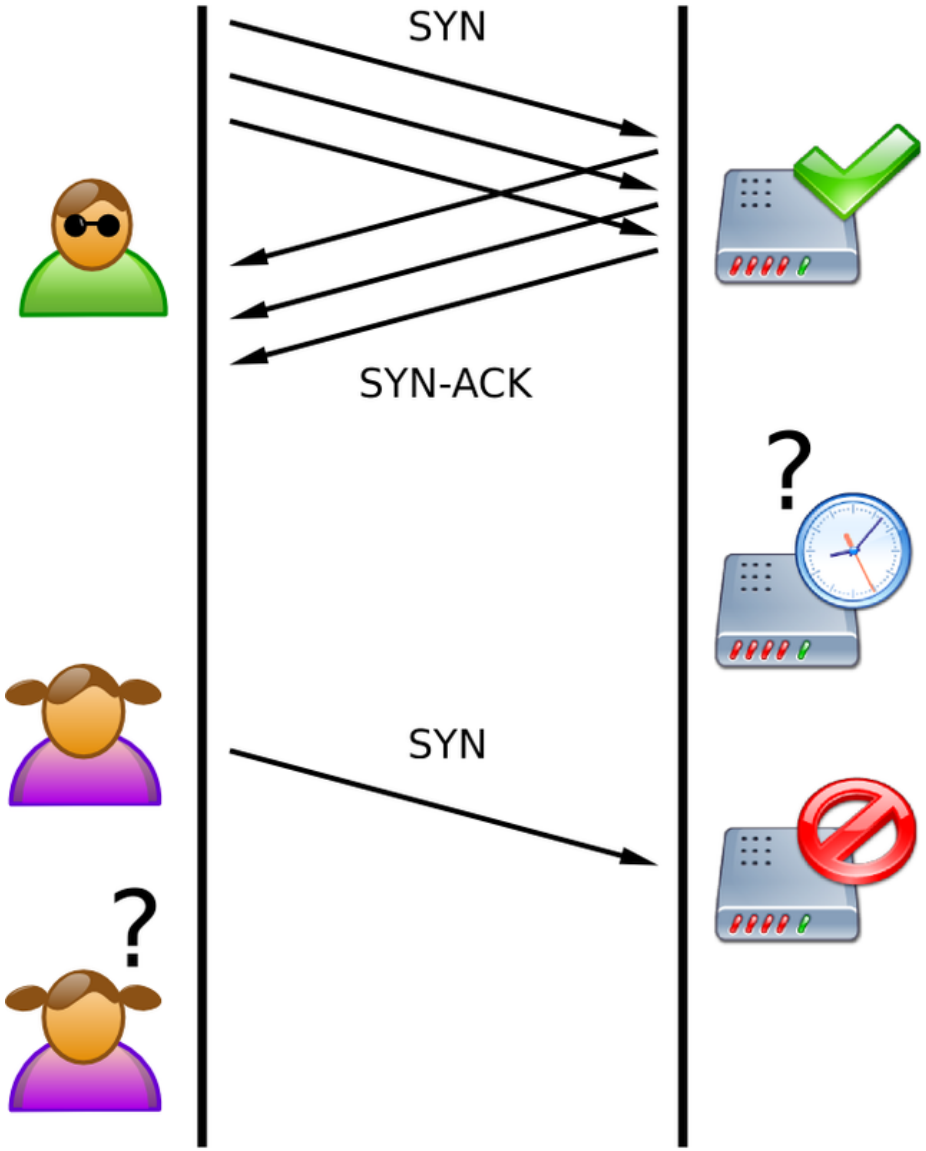
- Ingredienti:
  - iptables (-j LOG --log-prefix “ETICHETTA “)
  - bash, cat, grep, awk, sed, wc, etc :-)
  - iptables (-j DROP)

Esercizio 4

Rilevazione di anomalie

Rilevare la ricezione di connessioni su porte diverse dalle predefinite e l'invio di richieste verso destinazioni inattese da parte dei server lamp e target.

Caso di studio: SYN Flood (half-open attack)



Caso di studio: SYN Flood (half-open attack)

- Attacco di tipo Denial of Service
- Saturazione delle risorse lato server (troppe connessioni in fase di handshaking)
- Mitigazione:
  - Troppe richieste SYN sono sicuramente un'anomalia, bisogna solo definire il “troppe”

Esercizio 5A – semplice

Mitigazione di SYN flood e DOS agli attaccanti

Bloccare gli attacchi di tipo SYN flood verso target ed interrompere il servizio agli host che hanno effettuato tentativi di SYN Flood

Esercizio 5B – medio

Bloccare host che effettuano port scan

Rilevare il port scan su lamp ed interrompere il servizio all'host che lo genera

Migliori pratiche di gestione di firewall

- Documentare ogni regola o insieme di regole
- Revisionare periodicamente le regole e rimuovere le regole non più inutilizzate
- Documentare ogni regola o insieme di regole
- Revisionare periodicamente le regole e rimuovere le regole non più inutilizzate

Migliori pratiche di gestione di firewall

- Restringere il più possibile i permessi di accesso / transito
  - Utilizzare DROP come default policy (ove possibile), quindi aggiungere eccezioni
  - In particolare, chiudere le porte non presidiate da demoni!
  - Evitare l'uso di “ANY” (0.0.0.0) nelle regole di apertura
- Preferire la semplicità alla complessità
  - L'approccio blocco tutto lo favorisce
- Ottimizzare le regole per performance

Migliori pratiche di gestione di firewall

- Fare backup regolare delle regole di filtraggio
- Centralizzare i log del filtraggio su host dedicato ed inaccessibile
  - Verifiche automatizzate
  - Analisi di incident response (shit happens)
- Mantenere il firewall aggiornato (!)
  - Se non sono disponibili aggiornamenti, cambiare firewall
  - Se non c'è budget, trovare budget.

Università degli Studi di Verona
Corso di Laurea Magistrale in Informatica

Seminario sulla sicurezza delle reti

Andrea Zwirner

andrea@linkspirit.it

@AndreaZwirner