UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE MATEMATICHE, FISICHE ED INFORMATICHE
Corso di Laurea in Informatica

Sicurezza delle reti - Parte A

Strumenti di attacco e difesa

RETI DI CALCOLATORI - a.a. 2022/2023

Roberto Alfieri

La sicurezza delle reti: sommario

PARTE A

- I servizi di sicurezza
- Metodi e strumenti di Attacco
- Metodi e strumenti di Difesa: architetture, policy, iniziative di comunità

PARTE B

- Crittografia applicata e OpenSSL

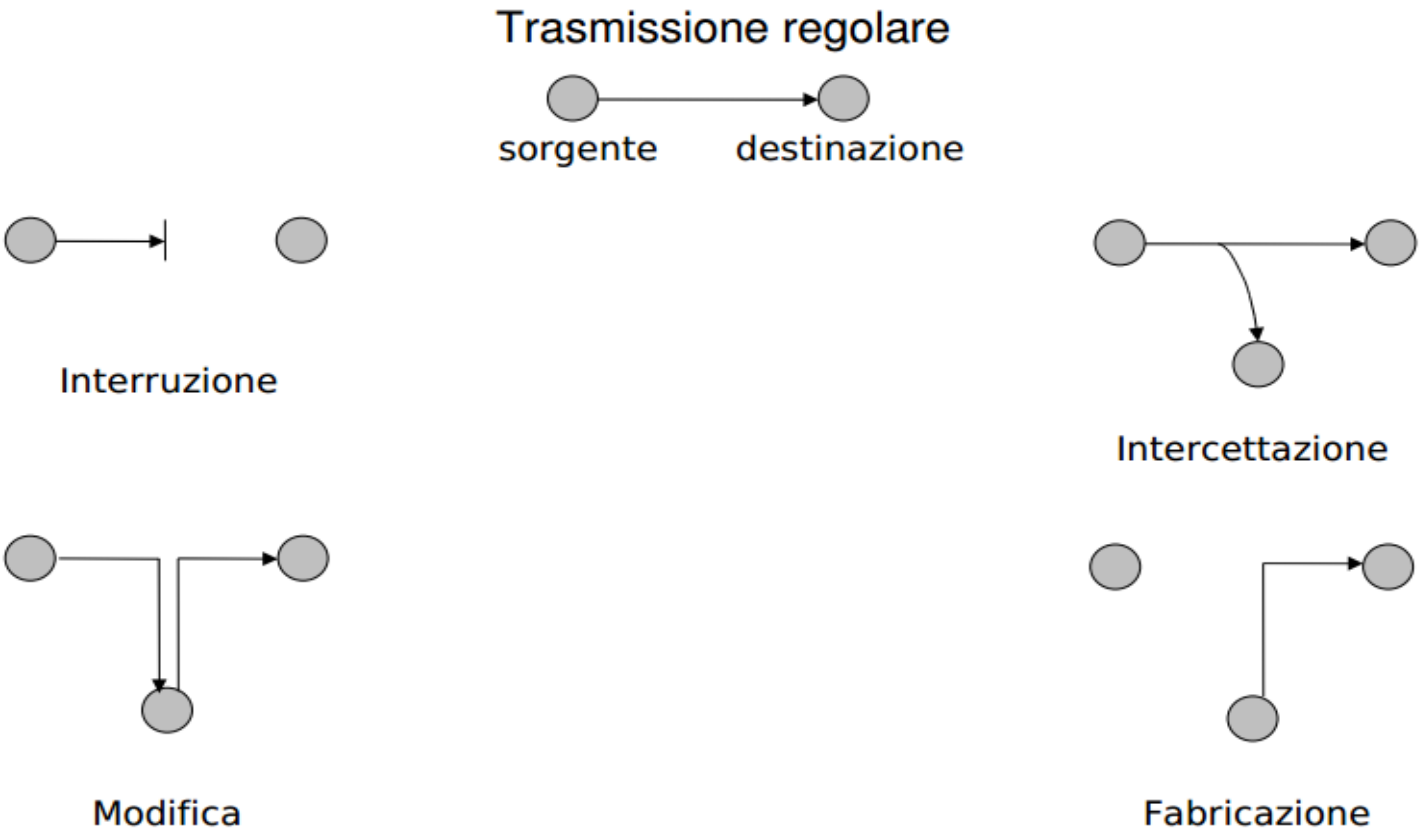
PARTE C

- Protocolli di autenticazione
- IPsec
- VPN
- Sicurezza delle reti WiFi

La sicurezza

Con il termine sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione dell'integrità logico-funzionale.

La gran parte delle minacce derivano dalla rete Internet, per cui la sicurezza informatica è un tema importante nello studio delle reti di calcolatori.



Politiche di sicurezza

La realizzazione di un sistema che garantisca una assoluta protezione da abusi è impossibile, ma è possibile attivare meccanismi di sicurezza tali da limitare e scoraggiare i tentativi.

La politica di sicurezza è ***quindi un compromesso, dettato dalle proprie necessità, tra il costo per attivarla ed il beneficio ottenuto in termini di diminuzione del rischio.***

Security services

Per proteggere un host in rete o una comunicazione occorre stabilire dei servizi di sicurezza che possono essere classificati nel seguente modo:

(vedi RFC2828 di IETF e la raccomandazione X.800 di ITU)

Autenticazione (Authentication): un servizio che consente di accertare l'identità dichiarata da una entità (origine dei dati o peer in una comunicazione) mediate la verifica di credenziali. Avviene in 2 step: Identificazione e verifica.

Autorizzazione (Authorization, Access Control): Protegge l'accesso ad una risorsa mediante l'applicazione di “Security Policy”.

Confidenzialità/Riservatezza (Data Confidentiality): Impedisce l'utilizzo delle informazioni da accessi non autorizzati.

Integrità dei dati (Data Integrity): consente di garantire che i dati acceduti non sono stati modificati.

Integrità dei sistemi (System Integrity): protegge le risorse del sistema contro modifiche, distruzioni accidentali o non autorizzate.

Non ripudio (Non-Repudiation): fornisce protezione contro il ripudio nel coinvolgimento in una comunicazione.

- non ripudio della sorgente: prova chi è il mittente dei dati in una transazione
- non ripudio della destinazione: prova che i dati sono arrivati ad uno specifico destinatario

Disponibilità (Avaliability): Fornisce una protezione per garantire accessibilità di una risorsa di sistema o di rete.

Audit (Accoutability, Traceability): Registrazione di eventi di sistema o di rete. Consente di rintracciare, ricostruire (ed eventualmente addebitare) l'utilizzo delle risorse.

Metodi di attacco

Attacco passivo:

- Raccolta di informazioni su possibili obiettivi
  - network monitor, port scanning, ..
- Intercettazione delle comunicazioni (Confidentiality attacks)
  - eavesdropping, Sniffing

Attacco attivo:

- Fabbricazione dell'identità di un'altra entità (Authentication attacks)
  - Spoofing, Man in the Middle
- Interruzione/compromissione di servizi (Avaliability attacks)
  - Denial of Service (DoS), Distributed DoS (DDoS)
- Sfruttamento di bugs nel software installato (System Integrity and Authentication attacks)
  - Applicazione degli Exploit noti
- Diffusione di Vulnerabilità intenzionali (System Integrity attacks)
  - Virus, Worms, BOT, Trojan
- Ingegneria Sociale
  - Phishing

Attacco passivo (e difesa): Sniffing e scanning

Sniffing: Analizzare il traffico di rete utilizzando un analizzatore di protocollo.

E' necessario un accesso privilegiato all'interfaccia di rete.

Possono essere orientati ad analizzare una sequenza di pacchetti

- Esempi di strumenti: **tcpdump e wireshark**

Scanning: testare un intervallo di indirizzi IP e numeri di porta per vedere quali servizi o sistemi sono presenti ed attivi.

- Esempio di strumento : **nmap**

nmap è uno tool open-source per la network exploration e l'auditing.

https://nmap.org/man/it/

Opzioni significative: https://nmap.org/book/port-scanning-options.html

-sP (ping scan)

-sT (TCP connect() - default)

-sS (TCP syn, richiede i priv. di root)

-A rileva versione

-p seleziona le porte da testare (per default vengono scansionate le 1000 porte più popolari)

Esempi:

nmap 192.168.0.0/24

nmap -A 192.168.0.254 -p 22,8001-8060

Attacco attivo: Spoofing (fabbricazione)

E' un tipo di attacco informatico dove viene impiegata la falsificazione dell'identità (spoof)

Quando la falsificazione non avviene in campo informatico si parla di social engineering

User account spoofing: usare nome utente e password di un altro utente senza averne il diritto. Può avvenire utilizzando strumenti come sniffer e password crackers

I password cracker possono essere off-line come John the Ripper http://www.openwall.com/john/ , oppure on-line, come Hydra

IP Address spoofing: Si basa sul fatto che la maggior parte dei routers all'interno di una rete controllino solo l'indirizzo IP di destinazione e non quello sorgente. Finalità:

- superare le tecniche difensive basate sull'autenticazione dell'indirizzo
- Realizzare attacchi DDoS. Vedi ad esempio "NTP reflection"

MAC Address forging: il MAC address viene modificato impersonando l'indirizzo della vittima. Diversi sistemi di autenticazione/autorizzazione sono basati su MAC address.

- Autenticazione verso DHCP server
- Sessioni attive su Captive Portal (session Hijacking)

ARP Spoofing / Poisoning: Consiste nell'inviare intenzionalmente e in modo forzato risposte ARP contenenti dati inesatti. In questo modo la tabella ARP di un host conterrà dati alterati. Ettercap è un tool per attacco di tipo **man-in-the-middle**, basato su ARP poisoning.

Attacco attivo: Denial of Service (DoS)

Causano la perdita dell'utilizzo di una risorsa sovraccaricandola, ma non ne permettono l'accesso all'attaccante. Gli attacchi possono essere

- diretti (l'attaccante interagisce direttamente con la vittima)
- indiretti (l'attaccante sfrutta terze parti).

I principali attacchi sono:

- **FLOODING**
  - **Ping floods:** invio di ICMP echo request in numero maggiore a quelli gestibili dal sistema attaccato; l'aggressore invia un grosso flusso di traffico ICMP echo verso una serie di indirizzi di broadcast attribuendosi come indirizzo sorgente quello della vittima.
  - **TCP SYN Floods:** Funziona se un server alloca delle risorse dopo aver ricevuto un SYN, ma prima di aver ricevuto un messaggio ACK (vedi nmap -sS).
- **INVIO DI PACHETTI MALFORMATI**
  - **Ping di grandi dimensioni (ping of death)**: può causare buffer overflow con conseguente blocco del servizio o, nei casi più gravi, crash del sistema.
  - **UDP bombs:** costruiti con valori illegali in certi campi. In certi sistemi operativi la ricezione di pacchetti imprevisti può causare crash
- **ATTACCHI DA PIU' HOST: DDOS (Distributed DoS)** https://www.garrnews.it/index.php/ricerche/236

E' una variante di DoS realizzato utilizzando numerose macchine attaccanti che insieme costituiscono una "botnet" controllate da un una unica entità, il botmaster

Attacco attivo: le vulnerabilità

La vulnerabilità https://it.wikipedia.org/wiki/Vulnerabilit%C3%A0_informatica può essere intesa come una componente di un sistema, in corrispondenza alla quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema.

La v**ulnerabilità** si presenta ovunque ci sia un difetto di progettazione, codifica, installazione e configurazione del software.

Esempi di vulnerabilità: https://csirt.gov.it

Un exploit https://it.wikipedia.org/wiki/Exploit è un frammento di codice, una sequenza di comandi, o un insieme di dati, che prendono vantaggio da una **vulnerabilità** per acquisire privilegi di accesso, eseguire codice o creare DoS su di una risorsa.

Attacco attivo: gli exploit

I più comuni tipi di exploit prendono vantaggio da:

- **Buffer overflow (Stack o Heap):** si basa sul fatto che un programma potrebbe non controllare in anticipo la lunghezza dei dati in arrivo, ma si limita a scrivere il loro valore in un buffer di lunghezza prestabilita, confidando che l'utente (o il mittente) non immetta più dati di quanti esso ne possa contenere.

- **Code injection**: Questo exploit sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno (ad esempio all'interno di una query SQL, oppure attraverso Remote File Inclusion: http://it.wikipedia.org/wiki/Remote_File_Inclusion)

Spesso, quando gli exploit vengono pubblicati, la vulnerabilità viene eliminata attraverso una Patch che produce una nuova versione del software.

Vedi ad esempio: https://www.cert.garr.it/alert/security-alerts

Attacco attivo: Malware

Un qualsiasi software creato allo scopo di causare danni a un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito.
http://it.wikipedia.org/wiki/Malware

- Virus Sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto.
- Worm questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet.
- Trojan software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore
- Spyware Software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato.

Attacco attivo: Ingegneria sociale e spam

.

- Ingegneria sociale. lo studio del comportamento individuale di una persona al fine di carpire informazioni utili. http://it.wikipedia.org/wiki/Social_engineering
  - Phishing E' un tipo di ingegneria sociale attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili.

- Spam http://it.wikipedia.org/wiki/Spam Lo spamming è l'invio di messaggi indesiderati (generalmente commerciali). Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica
  - Più dell'80% delle email inviate oggi nel mondo è Spam.
  - Il termine SPAM deriva dai Monty Python https://www.youtube.com/watch?v=zLih-WQwBSc

Strumenti di difesa

Architettura di sicurezza

- Perimetro, superficie d'attacco
- Firewall Packet filter e Firewall Proxy (system integrity)
- IDS, IPS (availability)

Policy per l'utente e l'amministratore di sistema

- Password Policy (authentication)
- Analisi del traffico e dei Log file (auditing)
- Ethical Hacking

Iniziative di comunità

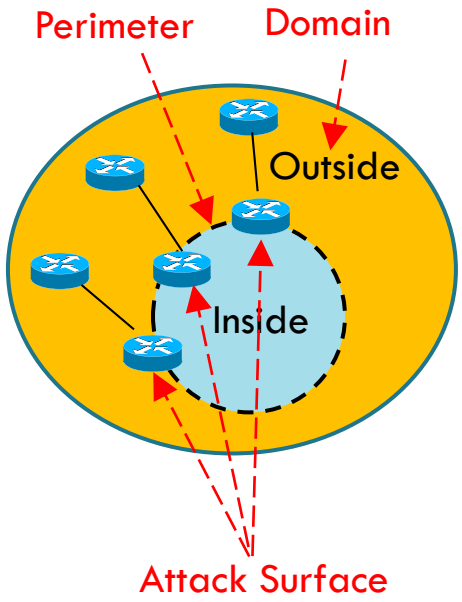
- Vulnerability Alerts e scan
- Computer Emergency Response Team (CERT)
- Normative

Rinforzo di autenticazione e riservatezza : strumenti crittografici

- Tools: crittografia simmetrica e asimmetrica, Message Digest, certificati
- Servizi: autenticazione (authentication, non repudiation), cifratura (data confidentiality), firma digitale (Data Integrity).

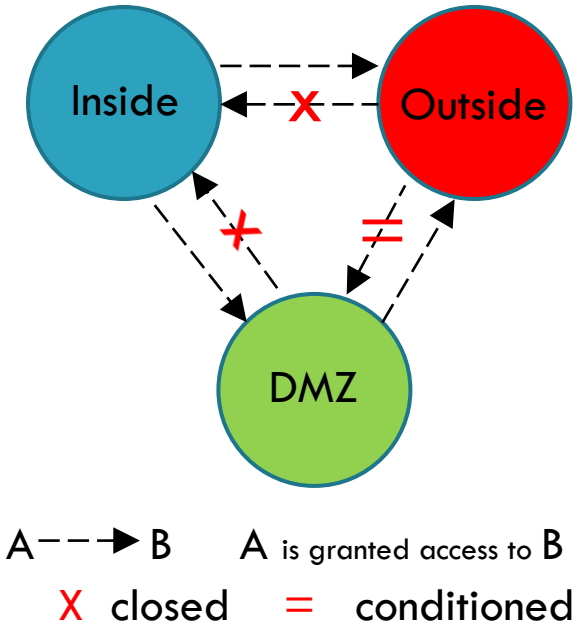
Domains, perimeter and attack surface

- A **security domain** is a set of entities/resources to be managed as a unique administration area according to a common security policy (security enforcement rules)
- A **security perimeter** is the secured boundary between the external and internal side of a security domain
  - e.g., an internal network and its public facing side, typically the Internet
  - The perimeter can be protected by several security devices
- The **attack surface** of a security domain is the sum of the different points ("attack vectors") where an unauthorized entity ("attacker") can try to enter data to or extract data or do any kind of unauthorized or hostile activity.
  - **Keeping the attack surface as small as possible** is a fundamental basic security measure

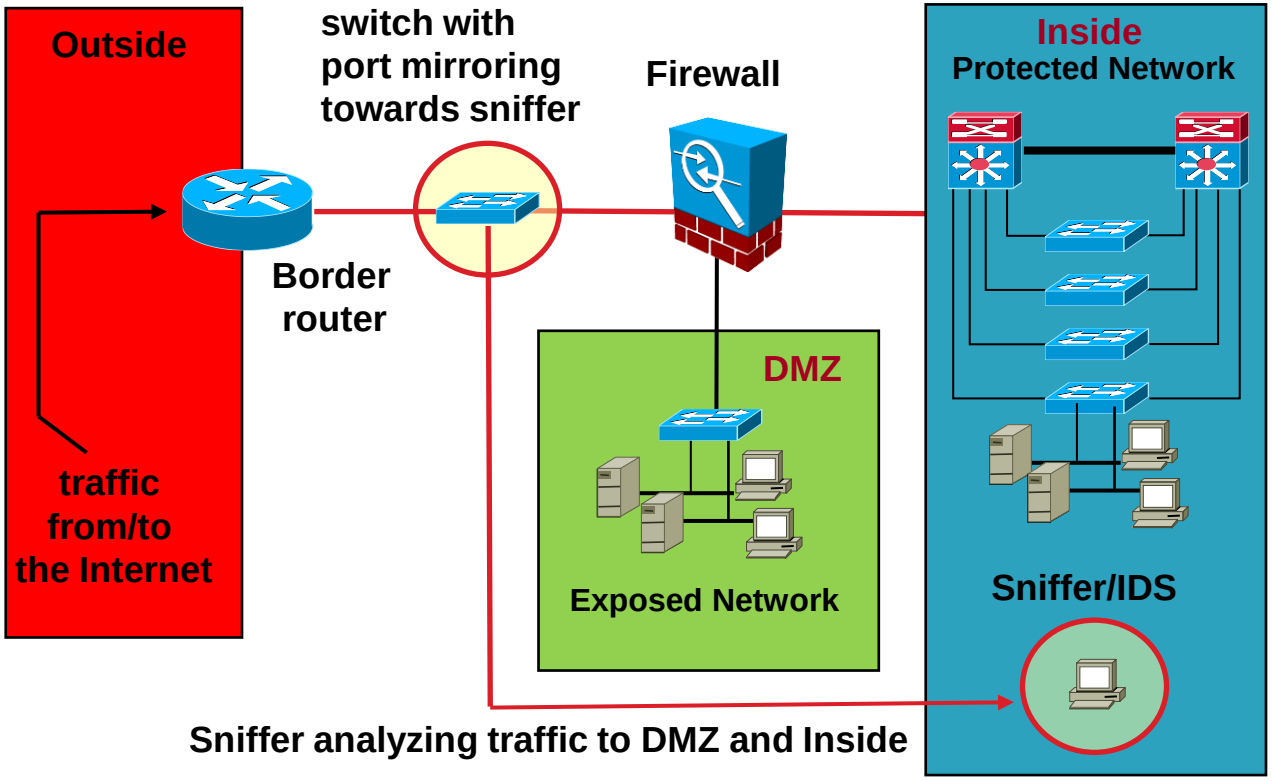


Security Domains

- Each security domain is assigned a **degree of trust** or **security level**
- Such degree defines and characterizes its visibility rules (access rights) with respect to the others
  - A domain with a higher degree of trust can have fuller visibility than those with a lower degree
  - Vice versa, visibility is blocked unless specific exceptions (filtering / visibility rules) are defined
    - DMZ and INSIDE have full visibility of OUTSIDE
    - INSIDE has full visibility of DMZ
    - Any other access is not granted



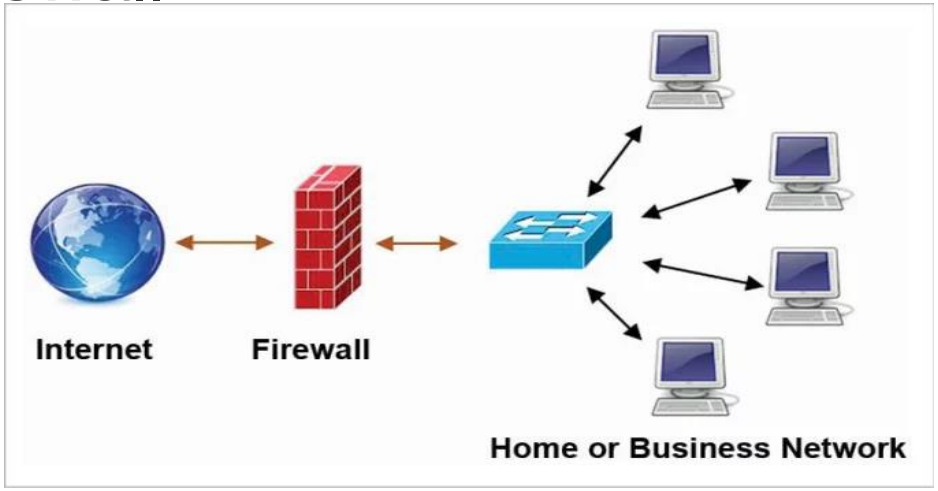
Basic security architecture



- In a common network architecture there are at least three domains:
  - **Outside** (all the world outside - the Internet): trust degree 0
  - **Inside** (the internal organization to be protected and hidden): degree of trust 100
  - **DMZ** (the set of internal machines that expose services outside): degree of trust 0 <x <100

Firewall

Per firewall si intende una entità hardware o software che si pone tra internet e la rete (o l'host) che si vuole proteggere.



Il firewall svolge una funzione di filtro, consentendo il transito solamente alle connessioni ritenute lecite mediante una opportuna “Policy”. Obiettivi principali:

- Monitorare, limitare, autenticare l'accesso alla rete da proteggere nei confronti di accessi provenienti dall'esterno (Internet).
- Monitorare, limitare, autenticare l'accesso all'esterno (Internet) da parte dell'utenza interna.

Servizi di sicurezza: system integrity, availability, audit.

I firewall possono essere di 2 tipi:

- I packet filter: agiscono ai livelli 3 e 4

- I proxy: agiscono a livello applicazione.

Firewall a filtro di pacchetti

Questo filtro analizza tutti i pacchetti in transito e applica azioni del tipo permit/deny sulla base di politiche basate sugli indirizzi IP e le porte di provenienza e/o di destinazione.

Obiettivi:

- Rendere visibili ad internet solamente i servizi di rete destinati ad un accesso pubblico (protezione dei servizi intranet e dei servizi “inconsapevoli”)
- Bloccare il traffico indesiderato (es: P2P, ..)
- Strumento per la gestione delle emergenze (bloccare un host ostile o contaminato da virus).

Agisce a livello di pacchetti IP, ma deve leggere anche i primi byte del livello 4 per leggere le porte TCP o UDP.

Può essere realizzato dai Router mediante un modulo aggiuntivo o da HW specifico.

Per Linux esiste il modulo **IPtables** che può essere applicato ad una interfaccia di rete.

ACL sul Router

Il router è un apparato di rete posto solitamente tra LAN e internet, che svolge il compito di gestione dei singoli pacchetti per il loro instradamento.

La gran parte dei router possono essere configurati per svolgere anche la funzionalità di Packet filter.

Il sistema operativo IOS dei router Cisco consente la definizione di ACL (Access Control List) che possono essere applicate alle interfacce del router.

In questo esempio viene creata una ACL sul traffico entrante che consente l'accesso ai soli server WEB ed EMAIL, bloccando il resto. L'ACL è poi applicata all'interfaccia opportuna. Esempio:

```
access-list 140 permit tcp any host "webserver"   eq www
access-list 140 permit tcp any host "mailserver"  eq smtp
access-list 140 permit tcp any host "mailserver"  eq pop3
access-list 140 permit tcp any host "mailserver"  eq imap
access-list 140 deny   ip any any log

interface  eth 0
  ip access-group 140 in
```

IPtables

Il pacchetto software IPtables consente di applicare ACL per il Packet filtering sulle interfacce di Sistemi Linux. IPtables lavora sulle 3 tabelle filter, nat, mangle sulle quali possiamo creare catene (chains) di regole ACL.

La tabella **Filter** (tabella di default) server per il packet filter

Le tabelle **NAT** (SNAT e DNAT) servono per le regole di NATting

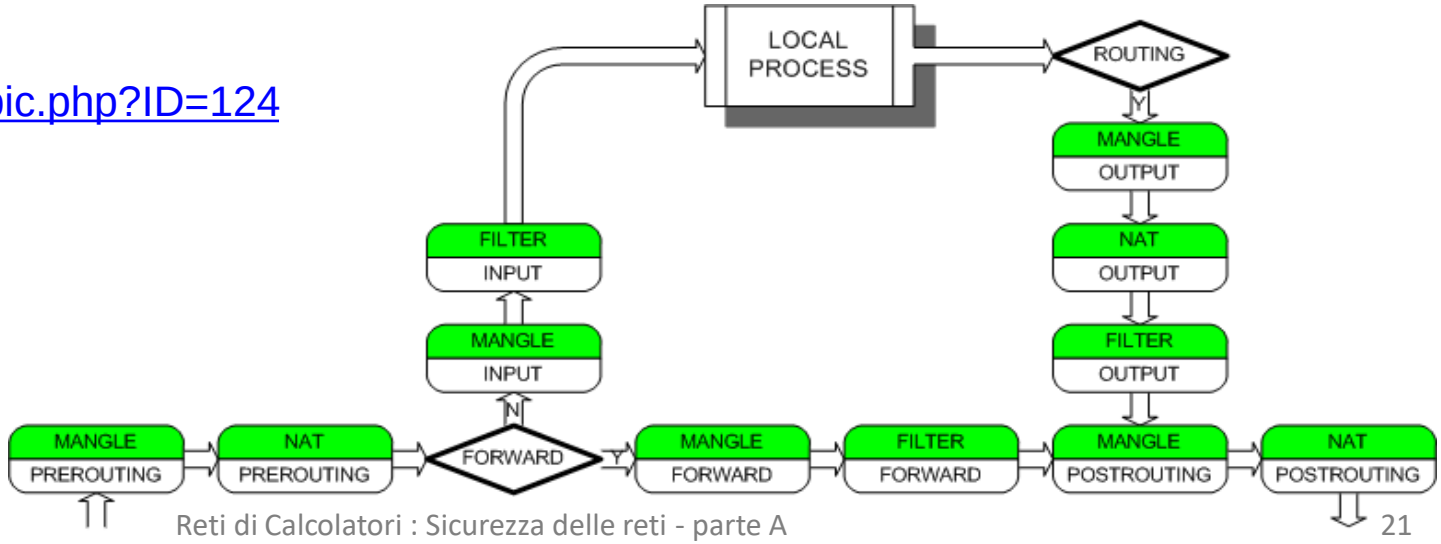
La tabella **Mangle** server per modificare alcuni parametri nell'header pacchetto

La tabella **Filter** ha 3 catene di Default applicate su una interfaccia di rete:

- **INPUT** per il processamento dei pacchetti destinati all'host
- **OUTPUT** per i pacchetti provenienti dall'host
- **FORWARD** per i pacchetti che devono attraversare il firewall.

Riferimenti:

http://openskill.info/topic.php?ID=124



Esempi IPtables

#accetta i pacchetti entrati di connessioni gia stabilite (SYN=0)
iptables -A INPUT -p ALL -m state --state ESTABLISHED -j ACCEPT

#accetta i pacchetti entranti dei servizi interni http, 81 (vh1), ssh e 3000 (ntopng)
iptables -A INPUT -p tcp --dport http -i enp0s3 -j ACCEPT
iptables -A INPUT -p tcp –dport 81 -i enp0s3 -j ACCEPT
iptables -A INPUT -p tcp –dport 3000 -i enp0s3 -j ACCEPT
iptables -A INPUT -p tcp --dport ssh -i enp0s3 -j ACCEPT

#accetta e registra sul sistema di log i pacchetti entranti verso il servizio telnet
iptables -A INPUT -p tcp --dport 23 -i enp0s3 -j LOG --log-prefix "TELNET"

#tutto il resto viene scartato
iptables --policy INPUT DROP

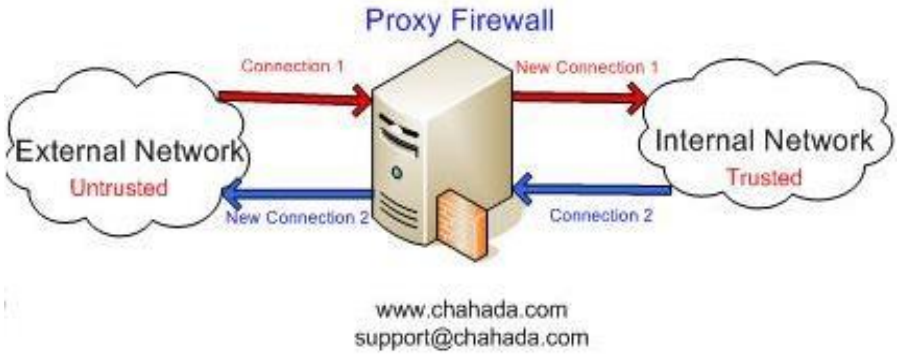
iptables -nvL

Firewall Basati su Proxy

Il Proxy è un programma applicativo con funzione di tramite tra client e server.
In modo implicito o esplicito il client deve rivolgersi al proxy per poter raggiungere il server.
Occorre un Proxy specifico per ogni applicazione.

Obiettivi:

- Mettere in comunicazione client e server che non hanno visibilità diretta (ad esempio se il client è in una rete intranet)
- Migliorare le prestazioni (es: Web Caching)
- Servizi di sicurezza
  - Auditing (tracciamento delle attività)
  - Autenticazione e Autorizzazione



Esempi:

- **Proxy Web** (Vedi Squid https://it.wikipedia.org/wiki/Squid)
- **Proxy SMTP** (MTA con **antiVirus e antiSpam** posizionato all'ingresso/uscita della LAN)
- **socat** (https://linux.die.net/man/1/socat) è un tool command-line che consente di connettere due flussi TCP e può quindi essere utilizzato per realizzare un servizio Proxy.

Antivirus

L'Antivirus (AV) è un software atto a prevenire, rilevare ed eventualmente eliminare programmi dannosi. Un AV ha anche una funzione preventiva, impedendo che un virus possa entrare in un sistema ed infettarlo.

Il metodo più utilizzato per individuare virus in un file è attraverso le signatures (firma).

Il programma AV calcola la firma (signature) di un file da analizzare (e.g. Hash MD5 dell'intero file) e lo confronta con le firme di virus noti presenti all'interno di un archivio. Se la firma corrisponde il file è sicuramente un virus.

Esistono anche tecniche euristiche, di solito usate in modo complementare alle firme, che cercano di individuare virus non noti all'AV attraverso la ricerca di pattern sospetti.

Può essere installato

- sul PC: scan dei dischi dell'host e dei nuovi file salvati
- sul MailServer: scan delle mail in entrata e in uscita

The best antivirus software for Windows Home User:

https://www.av-test.org/en/antivirus/home-windows/

Tecniche Antispam

Link utili: http://it.wikipedia.org/wiki/Spam

Black list https://www.cert.garr.it/it/documentazione/articoli-tecnici/30-blacklist

Lista di server classificati spammers che viene attivata sul mail server rifiutando mail che provengono da host inclusi in questa lista. L'amministratore del mailserver può costruire manualmente una propria lista o può avvalersi di servizi in Internet che distribuiscono automaticamente le liste.

Gray-List: Si basano sul fatto che i mailer usati dagli spammer generalmente tentano l'invio di una email una sola volta: Il GrayListing consiste nel rigetto della ricezione della mail al primo tentativo, che verrà accettata ad un successivo tentativo, dopo un tempo stabilito (tipicamente 300 sec.)

White List. Liste di mittenti “Fidati” su cui non vengono effettuati controlli antispam. Include gli host accettati da Gray-list e host inseriti manualmente dall'amministratore.

Filtri Bayesiani: Sono filtri che cercano di classificare le mail in arrivo assegnando un punteggio numerico a frasi o modelli che si presentano nel messaggio. Ogni messaggio riceve quindi un punteggio compressivo (tra 0 e 1) che, dopo aver stabilito una soglia, ci consente di classificare il messaggio. Il filtro richiede un addestramento con mail spam e no-spam con cui viene creato un database di riferimento.

Esempi:

- Spamassassin http://spamassassin.apache.org/ (liste White e Black, filtri Bayesiani)

Auditing di sicurezza informatica

Un audit di sicurezza informatica è un'analisi sistematica con l'obiettivo di verificare i controlli di sicurezza, politiche e procedure in atto e convalidare il loro efficace funzionamento in base al rischio.

Gli elementi oggetto di valutazione di un audit di sicurezza informatica sono:

- **personale aziendale**, ovvero le modalità utilizzate dai dipendenti per raccogliere, condividere e archiviare informazioni sensibili.
- I componenti del **sistema informatico** e ambiente in cui è ospitato
- **applicazioni e software** (incluse le patch di sicurezza messe a punto dagli amministratori di sistema)
- **vulnerabilità della rete** interna ed esterna

Passaggi principali dell'auditing:

- Definizione degli asset: elenco dettagliato di risorse, dati sensibili, apparecchiature informatiche e relativa valutazione del rischio informatico
- Valutazione del personale
- Monitoraggio dei sistemi e delle reti
- Identificazione delle vulnerabilità
- Risposte al rischio, aumento delle protezioni

Audit del personale

La sicurezza dei sistemi e delle reti dipende anche dal comportamento degli utenti e degli amministratori di sistema. Occorre annotare e registrare quali dipendenti abbiano accesso alle informazioni sensibili e quanti di loro siano preparati in maniera adeguata.

Il rischio principale riguarda il furto delle credenziali per l'accesso ai sistemi aziendali.

La password è una delle forme di identificazione più semplici ed utilizzate ed è quindi uno dei principali bersagli degli attacchi.

I metodi più utilizzati sono:

1) Intercettazione. L'utilizzo di un canale non cifrato consente la cattura delle password sulla rete.
2) Furto. Alcuni utenti tendono a scriverla su un supporto magnetico per non dimenticarla.
3) Tentativi di indovinare la password (password cracker basati su dizionari)
4) Phishing.

I risultati dell'audit sul personale vengono utilizzati per programmare un **piano di formazione del personale**

Auditing di sistema

L’audit di sicurezza informatica richiede la definizione dell’elenco dei sistemi, la loro classificazione in base al rischio informatico e l’attribuzione del ruolo di amministratore.

L’amministratore di sistema deve definire un programma di audit attraverso il quale viene definita la gestione e l'analisi degli eventi, con i seguenti obiettivi:

- **(Early) warning:** Individuare rapidamente eventuali attacchi in corso.
- **Trouble-shooting:** mantenere uno storico degli eventi per tracciare le attività.

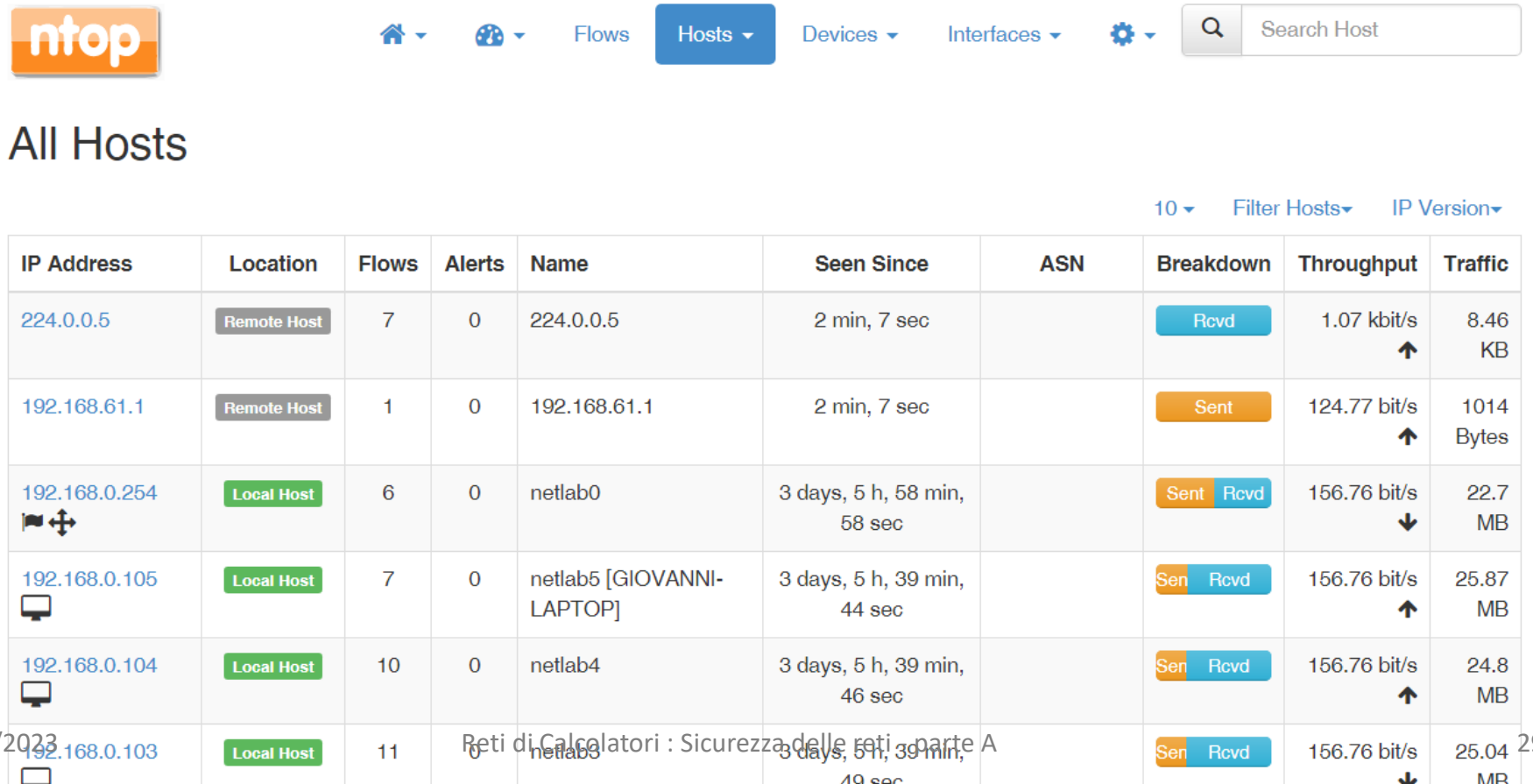
rsyslog è lo strumento base per l’audit di sistema in ambiente Linux.

Consente ai processi interni di generare eventi classificati in categorie (KERN, USER, MAIL, DAEMON, AUTH, LPR, CRON, LOCAL0-7) e priorità (EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG). Per ogni evento è possibile definire una azione come scrivere su file (tipicamente nella directory /var/log) , inviare mail o attivare script.

Audit della rete

Consiste nella raccolta e analisi sistematica del traffico di rete e per la rilevazione in tempo reale di minacce provenienti dalla rete. E' necessaria la nomina di un amministratore di rete.

Strumenti utili sono i **Network Monitor** (esempio **ntop** , dotato di una console web, vedi figura), gli **Intrusion Detection Systems** (IDS), gli **Honeypot** e i **Vulnerability Scanners.**



IP Address	Location	Flows	Alerts	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
224.0.0.5	Remote Host	7	0	224.0.0.5	2 min, 7 sec		Rcvd	1.07 kbit/s ↑	8.46 KB
192.168.61.1	Remote Host	1	0	192.168.61.1	2 min, 7 sec		Sent	124.77 bit/s ↑	1014 Bytes
192.168.0.254	Local Host	6	0	netlab0	3 days, 5 h, 58 min, 58 sec		Sent Rcvd	156.76 bit/s ↓	22.7 MB
192.168.0.105	Local Host	7	0	netlab5 [GIOVANNI-LAPTOP]	3 days, 5 h, 39 min, 44 sec		Sen Rcvd	156.76 bit/s ↑	25.87 MB
192.168.0.104	Local Host	10	0	netlab4	3 days, 5 h, 39 min, 46 sec		Sen Rcvd	156.76 bit/s ↑	24.8 MB
192.168.0.103	Local Host	11	0	netlab3	3 days, 5 h, 39 min, 49 sec		Sen Rcvd	156.76 bit/s ↓	25.04 MB

IDS (Intrusion Detection System)

IDS è un dispositivo software/Hardware per identificare accessi non autorizzati a host o LAN.

L'IDS generalmente si appoggia su un Data-Base per memorizzare le regole utilizzate per individuare le violazioni di sicurezza.

Gli IDS sono classificabili nel seguente modo:

Host IDS (HIDS): analizzano file di log e file system sull'Host.

TRIPWIRE è un esempio di HIDS. Si basa sulla differenza tra lo stato analizzato ed uno stato iniziale.

Network IDS (NIDS): analizzano il traffico di rete.

SNORT è un esempio di NIDS che può funzionare anche come sniffer / packet logger.

Quando un IDS rileva una intrusione invia una notifica all'amministratore via e-mail o con un messaggio alla console (continuous monitoring e auditing).

Intrusion Prevention System (IPS)

Gli IPS sono un'estensione degli strumenti di IDS: quando rilevano un tentativo di intrusione sono abilitati a bloccare gli accessi considerati pericolosi.

IPS può mandare un allarme (come un IDS), ma anche interagire con un firewall per eliminare pacchetti malevoli, resettare le connessioni e/o bloccare il traffico da un indirizzo IP attaccante.

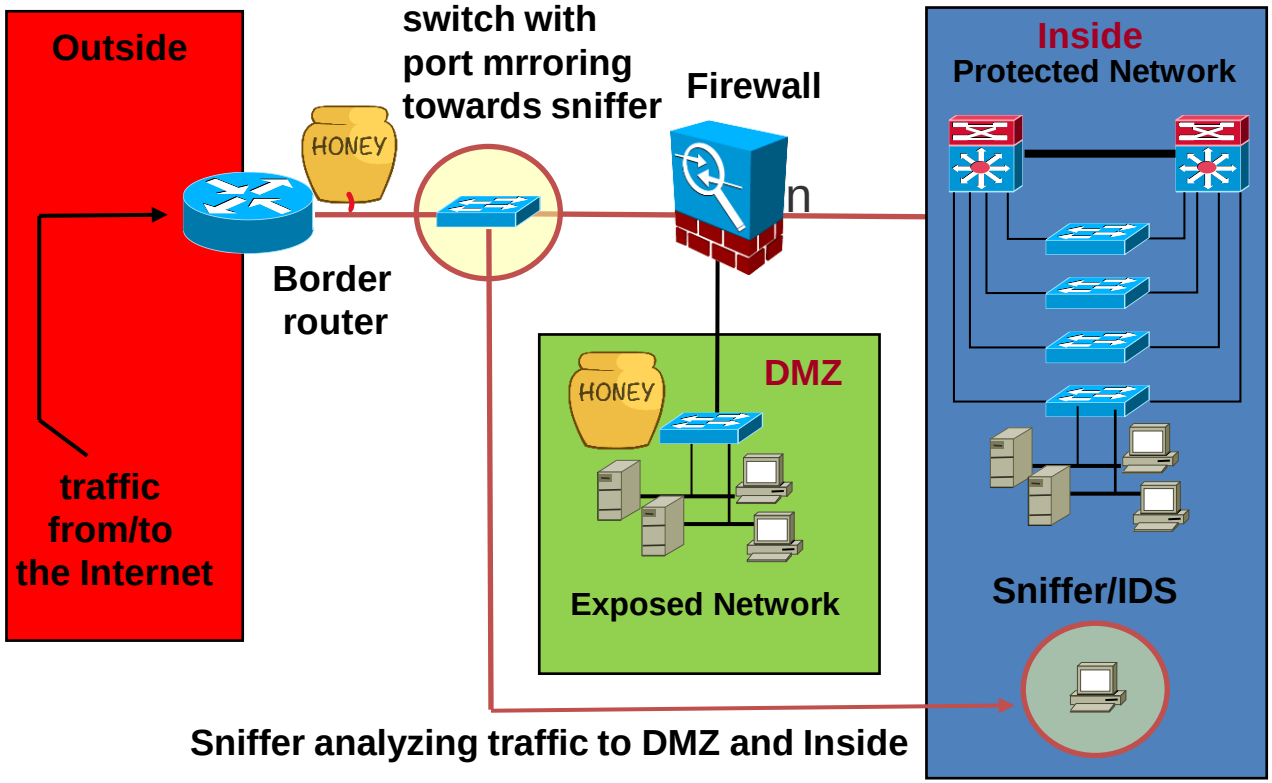
Strumenti utili: **fail2ban** http://guide.debianizzati.org/index.php/Fail2ban

Fail2ban è pensato per prevenire attacchi “brute force” via ssh bloccando temporaneamente gli indirizzi IP che provano a violare la sicurezza di un sistema.

Il programma effettua il parsing di alcuni file di log che contengono informazioni relative ad accessi falliti. Se il numero di accessi falliti supera una certa soglia l’indirizzo IP del client viene bloccato attraverso una regola di iptables.

Honeypot

Un honeypot è un sistema o componente hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi. Consiste in un computer o un sito che sembra essere parte della rete, ma che in realtà è ben isolato e non ha contenuti sensibili o critici.
Consente di rilevare attività malevole senza coinvolgere la rete interna.



Auditing di rete

Identificazione delle vulnerabilità

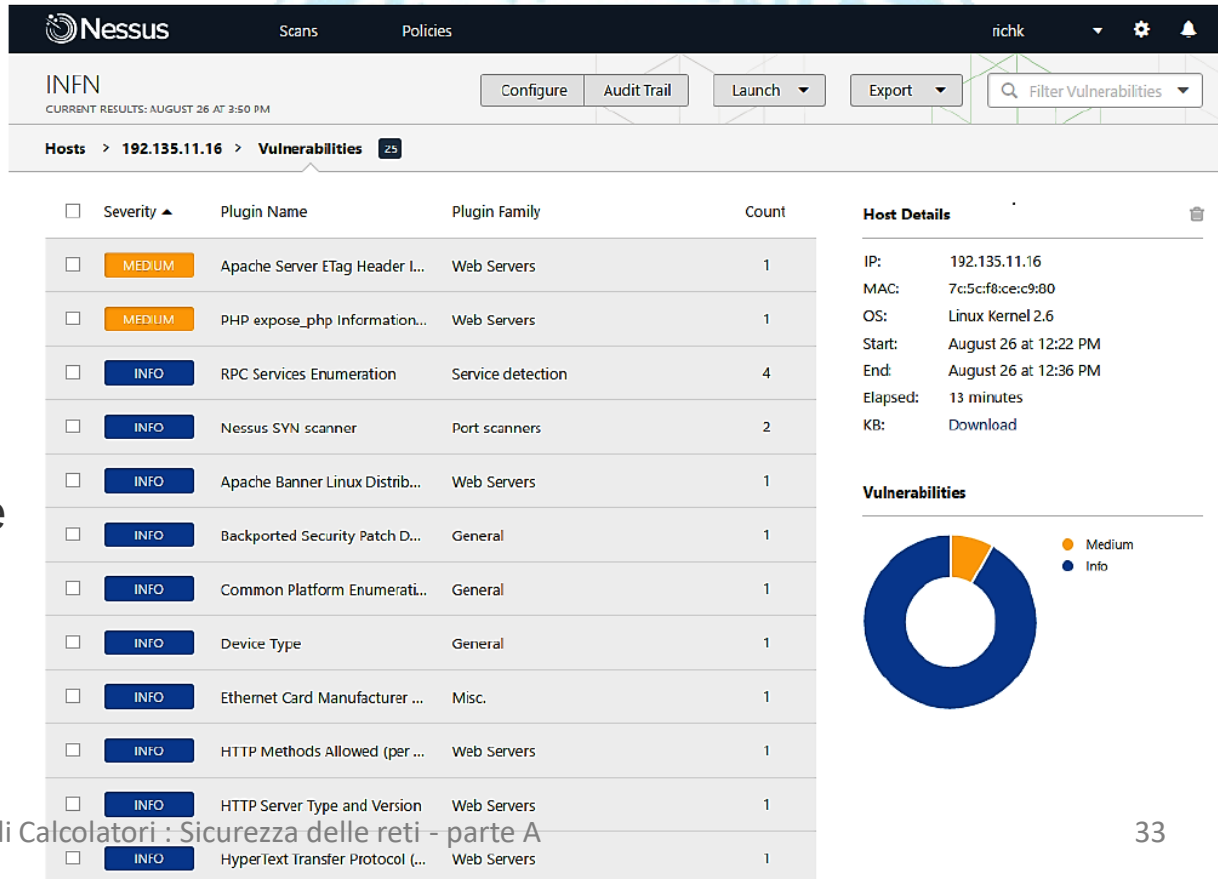
Un vulnerability scanner è un programma progettato per ricercare e mappare le debolezze di un singolo computer o degli host di una rete.

Identifica le vulnerabilità dovute a software con bugs o non aggiornato, configurazioni errate all'interno di servizi applicativi, web server, firewall router, ecc

Scanner più utilizzati: Nessus (commerciale) e openVAS (opensource).

Funzionamento:

1 ricerca host attivi
2 port scanning per ogni host
3 ricerca vulnerabilità tramite test non invasivi
4 identificazione vulnerabilità tramite confronto con database
5 Generazione di un report



Vulnerabilità: Dizionari e Alert

Le vulnerabilità note vengono censite in dizionari da organizzazioni internazionali, indicando il software interessato, l'impatto e i rimedi da applicare.

Il dizionario più noto è il «Common Vulnerabilities and Exposures» (CVE) mantenuto dalla MITRE Corporation e finanziato dal Dipartimento della Sicurezza interna degli Stati Uniti. Vedi https://cve.mitre.org/

La severità delle vulnerabilità è misurata con «Common Vulnerability Scoring System" (CVSS) che assegna ad ogni vulnerabilità un punteggio tra 0 e 10

Vedi https://it.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

https://nvd.nist.gov/vuln-metrics/cvss

Diverse organizzazioni pubblicano quotidianamente le nuove vulnerabilità attraverso «Vulnerability Alert»

Vedi ad esempio i Security Alert del GARR: https://www.cert.garr.it/alert/security-alerts

Alcune organizzazioni forniscono strumenti per il Vulnerability scanning

Vedi ad esempio GARR SCARR https://scarr.garr.it/

CERT – Computer Emergency Response Team

Un CERT (o CSIRT – Computer Security Incident Response Team) è un Servizio offerto all'interno di una comunità di utenti Internet per la gestione di emergenze in seguito ad attacchi informatici.

L'assistenza tecnica avviene attuando piani immediati di incident response in caso di attacco e attraverso la massiccia diffusione di informazioni per la prevenzione di incidenti informatici.

CERT rilevanti in Italia :

https://cert-agid.gov.it/ (AGID)

https://www.cert.garr.it/ (Garr)

https://csirt.gov.it (Agenzia per la Cybersicurezza Nazionale)

Standard e normative di sicurezza informatica

Gli standard di sicurezza informatica sono metodologie che permettono alle organizzazioni di attuare tecniche di sicurezza finalizzate a minimizzare la quantità e la pericolosità delle minacce alla sicurezza informatica.

Vedi https://it.wikipedia.org/wiki/Standard_di_sicurezza_informatica

Normative per la sicurezza informatica

Uno degli standard di sicurezza più ampiamente utilizzato è **l'ISO 27001** del 2013 che include un elenco di 114 controlli e che prevede una **certificazione per le aziende**.

Nel 2017 AGID (Agenzia per l'Italia Digitale) ha emanato le «Misure minime di sicurezza ICT» che **le pubbliche amministrazioni** devono adottare.

Normative per la protezione dei dati

Nel 2016 l'Agenzia dell'Unione Europea per la Cybersecurity, ENISA, ha emanato il **regolamento generale sulla protezione dei dati** (GDPR), adottato in Italia attraverso un regolamento emanato dal «Garante per la protezione dei dati personali» a cui si deve attenere chi tratta i dati personali. L'articolo 34 descrive le misure minime da adottare in caso di trattamento di dati personali con strumenti elettronici.