



UNIVERSITÀ  
DI PARMA

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

# Sicurezza delle reti - Parte A

## Metodi di attacco e difesa

RETI DI CALCOLATORI - a.a. 2023/2024

Roberto Alfieri

# La sicurezza delle reti: sommario

## PARTE A

- ▶ I servizi di sicurezza
- ▶ Metodi e strumenti di Attacco
- ▶ Metodi e strumenti di Difesa

## PARTE B

- ▶ Crittografia applicata e OpenSSL

## PARTE C

- ▶ Protocolli di autenticazione
- ▶ Ipsec e 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

I beni da proteggere (asset) sono principalmente i dati gestiti dalla rete informatica, ma per fare ciò bisogna anche proteggere i computer ed i vari dispositivi presenti nella rete.

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:

**Autenticazione (Authentication):** un servizio che consente di accertare l'identità dichiarata da una entità (origine dei dati o peer in una comunicazione) mediante 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 (Availability):** Fornisce una protezione per garantire accessibilità di una risorsa di sistema o di rete.

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

*Riferimenti: RFC2828 di IETF e la raccomandazione X.800 di ITU*

# Metodi e strumenti di attacco ai servizi di sicurezza

Esistono diversi metodi e strumenti che un attaccante può utilizzare per violare i servizi di sicurezza a protezione di un host o di una rete.

Gli attacchi possono essere **passivi**, se l'obiettivo è la raccolta di informazioni, in modo lecito o illecito, riguardo un possibile bersaglio, oppure **attivi** quando coinvolgono l'alterazione dei dati sui dispositivi di memorizzazione o nei flussi di comunicazione.

Solitamente un attacco passivo è funzionale ad un successivo attacco attivo.

# Attacco passivo

Gli attacchi passivi includono quelle attività che consentono di raccogliere dati e informazioni di un asset bersaglio senza alcuna alterazione sui dati e sui dispositivi. L'obiettivo principale è la raccolta di informazioni sul target utili per un successivo attacco attivo.

Tipologie principali di attacco passivo:

- ▶ Scansione via rete del target e/o della rete a cui appartiene
  - ▶ Strumenti: port scanning (esempio nmap)
- ▶ Intercettazione delle comunicazioni
  - ▶ Strumenti: Sniffing (esempio tcpdump)
- ▶ Raccolta di informazioni Open Source (OSINT)
  - ▶ Strumenti: ricerca di informazioni forum, blog, siti di social network, siti di condivisione di video, wiki, record Whois e DNS di nomi di dominio registrati, metadati e file digitali, risorse web scure, dati di geolocalizzazione, indirizzi IP , i motori di ricerca delle persone e tutto ciò che può essere trovato online.

Queste attività sono il punto di partenza per un attaccante ma sono anche strumenti di difesa che possono consentire di conoscere i propri punti deboli.

# Attacco passivo: 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 passivo: OSINT

Open Source INTelligence si riferisce alla ricerca di informazioni tratte da fonti liberamente disponibili (non all'open source software).

Ricerca, esaminare, correlare le informazioni pubblicamente disponibili permette di ottenere informazioni sull'organizzazione, sui progetti, sui processi aziendali, sulle persone.

Le informazioni recuperabili tramite OSINT non sono utilizzabili soltanto per fini “negativi”

Possono essere utilmente impiegate per supportare decisioni strategiche, valutare campagne di marketing, verificare il “sentiment” e la reputazione online

Possono essere impiegate per migliorare la sicurezza dell'organizzazione

## Modalità di OSINT

✓ **Manuale:** la ricerca viene effettuata direttamente dall'operatore

Le scelte vengono fatte sul momento. Raccolta e confronto oneroso, difficilmente “scalabile” ed elevato rischio di “perdere” informazioni

✓ **Automatica:** la ricerca viene effettuata tramite strumenti parametrizzabili

Deve essere effettuata una scrematura a posteriori. Potenzialmente molto efficace, facilmente “scalabile” ed integrabile, richiede enormi investimenti (HW e SW), le tecnologie sono in rapida convergenza. Rischio di falsi positivi dovuti a AI non evoluta come analista

# Attacco attivo

Gli attacchi attivi sono quelli che si basano sull'alterazione dei dati oppure dei flussi con cui i dati sono trasmessi in rete.

Tipologie principali di attacco attivo:

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

# 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).
- **NINVIO 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)

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

- **NTP reflection** (vedi spoofing)

# Attacco attivo: sfruttamento delle vulnerabilità

La vulnerabilità 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 **vulnerabilità** si presenta ovunque ci sia un difetto di progettazione, codifica, installazione e configurazione del software. Esempi di vulnerabilità: <https://csirt.gov.it>

Un 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.

**Patch** : Quando viene scoperta una vulnerabilità lo sviluppatore rilascia un aggiornamento del software (**patch**), che porta alla risoluzione della vulnerabilità di sicurezza.

**Zero-day** è il nome delle vulnerabilità di cui ancora non è stata rilasciata una Patch. Zero-day exploit si riferisce a exploit di vulnerabilità zero-day.

# 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.
- ▶ **Cross site scripring (XSS)** è una vulnerabilità che affligge siti web dinamici che impiegano un insufficiente controllo dell'input nei form.
- ▶ **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](#))

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.

# Common Weakness Enumeration (CWE)

CWE <https://cwe.mitre.org/> è una lista di debolezze di sicurezza mantenuta da Mitre Corporation <https://www.mitre.org/> (organizzazione no-profit) in cui ogni tipologia di debolezza viene classificata attribuendo un identificativo numerico univoco.

Esempi delle debolezze più rilevanti nel 2022

- CWE-787 : Out-of-bounds Write
- CWE-79 : Cross-site Scripting
- CWE-89 : SQL Injection
- CWE-20 : Improper Input Validation
- CWE-125 : Out-of-bounds Read
- CWE-78 : OS Command Injection
- CWE-416 : Use After Free
- CWE-22 : Path traversal



# Common Vulnerabilities ean Exposures (CVE)

Mitre Corporation gestisce anche il dizionario CVE (Common Vulnerabilities and Exposures) in cui sono classificate ed enumerate le singole vulnerabilità e falle di sicurezza note pubblicamente.

Esistono diversi elenchi delle vulnerabilità più sfruttate nel 2022.

Ad esempio:

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a>

In questo elenco la vulnerabilità più sfruttata nel 2022 è la [CVE-2018-13379](#)

Denominata «Fortinet FortiOS SSL VPN Path Traversal Vulnerability»

Appartenente al CWE-22

( Improper Limitation of a Pathname to a Restricted Directory - 'Path Traversal' )

Organizzazioni come GARR-CERT diffondono regolarmente avvisi riguardo nuove vulnerabilità:

<https://www.cert.garr.it/en/alert-en/security-alerts/archive/listing>

# CVSS

Il Common Vulnerability Scoring System (CVSS) è una norma tecnica aperta per valutare la gravità delle vulnerabilità di sicurezza di un sistema informatico.

CVSS assegna un punteggio di gravità alle vulnerabilità, consentendo a chi si occupa di rispondere all'emergenza di stabilire la priorità di risposte e risorse in base al livello di minaccia.

I punteggi vengono calcolati con una formula che dipende da diverse metriche che approssimano la facilità e l'impatto di un exploit. Il punteggio è espresso in una scala da 0 a 10, dove 10 indica il livello di vulnerabilità più grave. (Wikipedia)

Esistono diverse versioni di CVSS per calcolare lo score; le versioni più recenti sono CVSS3 e CVSS2.

Diverse organizzazioni calcolano in CVSS per le nuove vulnerabilità, tra cui [NIST](#)

Nell'esempio della vulnerabilità [CVE-2018-13379](#) NIST ha calcolato:

CVSS3: 9.8/10    CVSS2: 9.1/10

# OWASP Top10

Un'altra lista molto nota di debolezze è la [Top10](#) che l'Open Web Application Security Project ( [OWASP](#) ) stila ogni anno.

La lista del 2021 è la seguente:

- A01:2021 Broken Access Control
- A02:2021 Cryptographic Failures
- A03:2021 Injection
- A04:2021 Insecure Design
- A05:2021 Security Misconfiguration
- A06:2021 Vulnerable and Outdated Components
- A07:2021 Identification and Authentication Failures
- A08:2021 Software and Data Integrity Failures
- A09:2021 Security Logging and Monitoring Failures
- A10:2021 Server Side Request Forgery (SSRF)

# 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](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

*Il termine SPAM deriva da una scena dei [Monty Python](https://www.youtube.com/watch?v=zLih-WQwBSc) <https://www.youtube.com/watch?v=zLih-WQwBSc>*

# Metodi e strumenti di difesa

## **Architettura e politiche di sicurezza**

- ▶ Perimetro, superficie d'attacco
- ▶ Firewall Packet filter e Firewall Proxy (system integrity), IDS, IPS (availability)
- ▶ Auditing di sicurezza (utenti, sistemi e reti)

## **Iniziative di comunità**

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

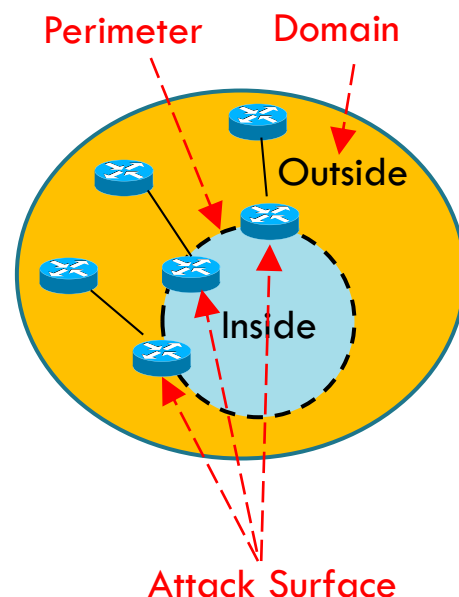
## **Rinforzo di autenticazione e riservatezza : strumenti crittografici**

- ▶ 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

22

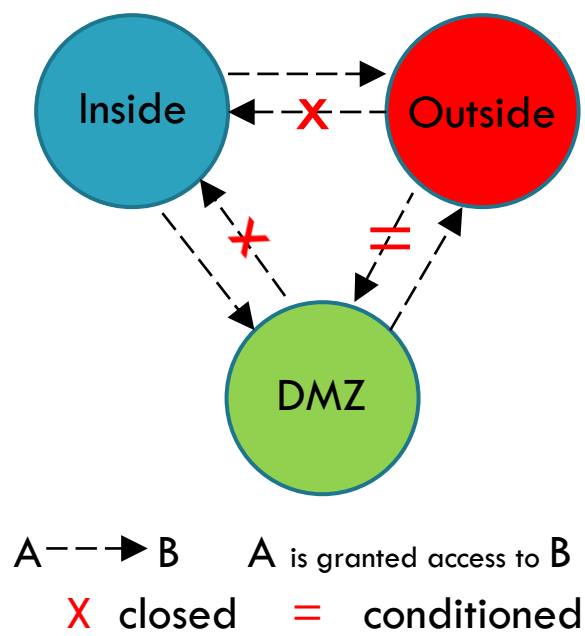
- A **security domain** is a set of entities/resources to be managed as a unique administration area according to a common security policy (security enforcement rules)
- A **security perimeter** is the secured boundary between the external and internal side of a security domain
  - e.g., an internal 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



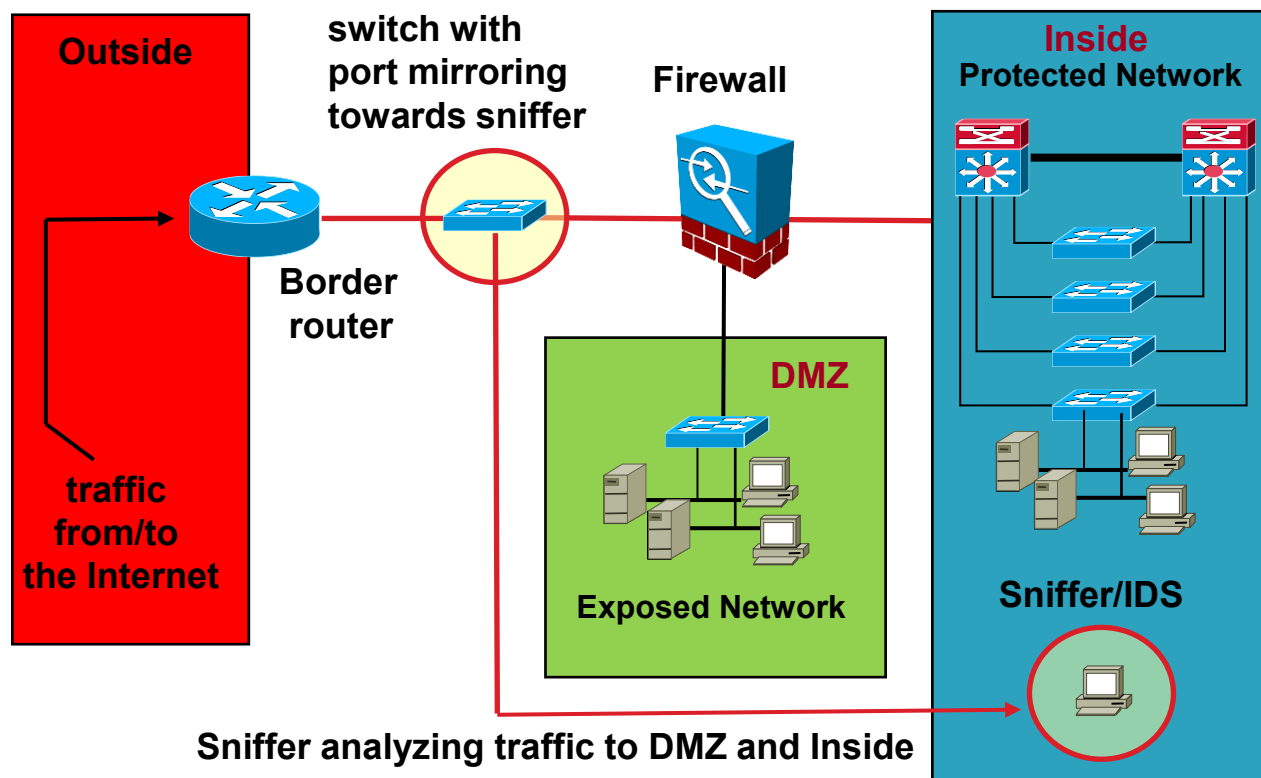
# Security Domains

23

- 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:

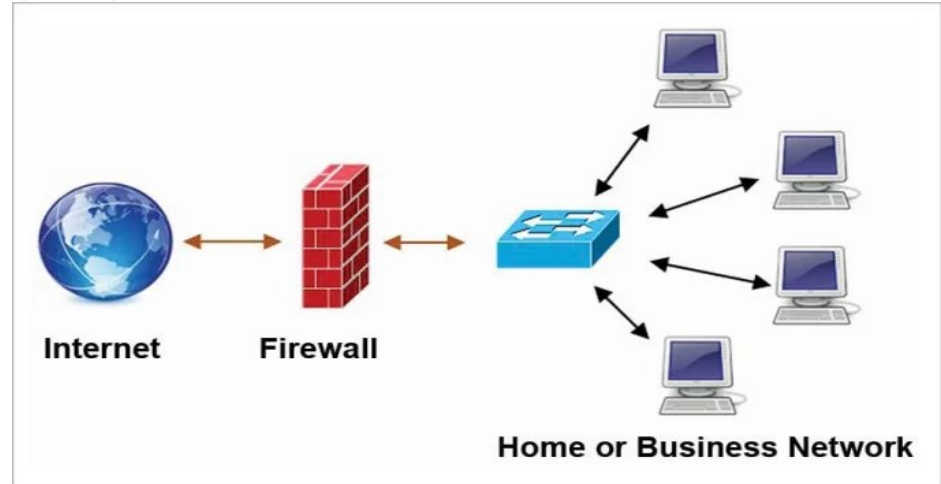
- **Outside** (all the world outside - the Internet): trust degree 0
- **Inside** (the internal organization to be protected and hidden): degree of trust 100
- **DMZ** (the set of internal machines that expose services outside): degree of trust  $0 < x < 100$



# Architettura di sicurezza

## 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.

## Architettura di sicurezza

# 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.

# Architettura di sicurezza 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

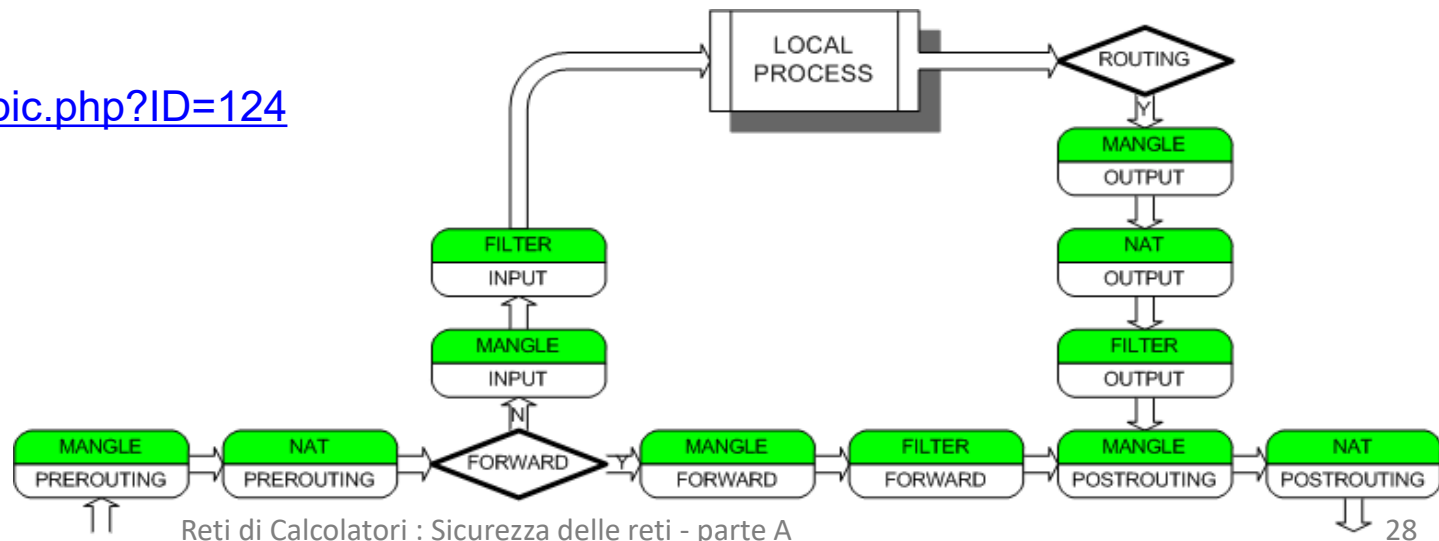
La tabella **Mangle** server per modificare alcuni parametri nell'header pacchetto

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>



# Architettura di sicurezza

## Esempi IPtables

#accetta i pacchetti entranti di connessioni già 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
```

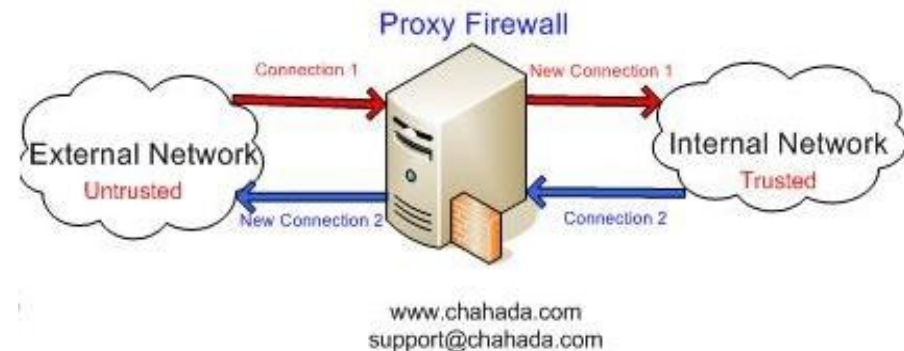
```
iptables -nvL
```

# 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)

# 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).



## Architettura di sicurezza

# 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>

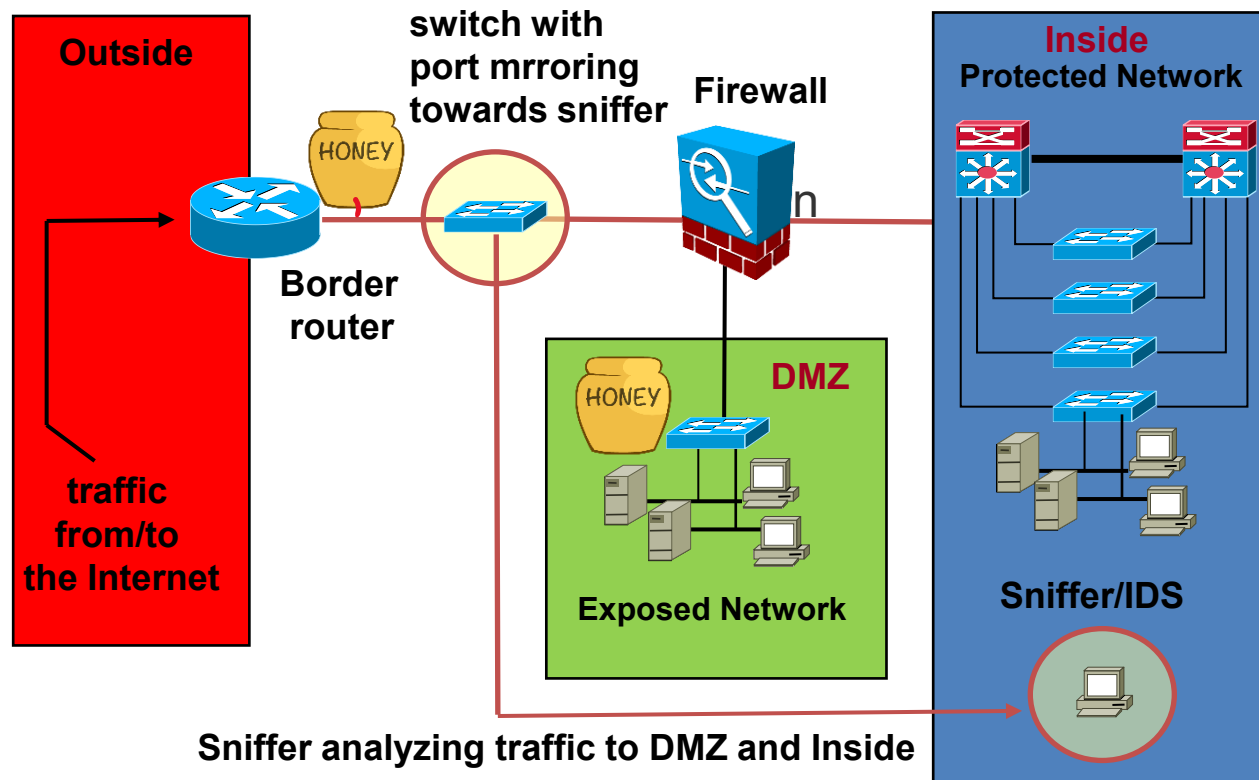
Fail2ban è pensato per prevenire attacchi “brute force” via ssh bloccando temporaneamente gli indirizzi IP che provano a violare la sicurezza di un sistema.

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.

# Architettura di rete 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 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

# Auditing 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.

# Auditing di rete

## 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. Strumenti utili sono i **Network Monitor** come [ntop](#) , dotato di una console web, vedi figura.



Flows

Hosts

Devices

Interfaces



Search Host

### All Hosts

10

Filter Hosts

IP Version

IP Address	Location	Flows	Alerts	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
<a href="#">224.0.0.5</a>	Remote Host	7	0	224.0.0.5	2 min, 7 sec		Rcvd	1.07 kbit/s ↑	8.46 KB
<a href="#">192.168.61.1</a>	Remote Host	1	0	192.168.61.1	2 min, 7 sec		Sent	124.77 bit/s ↑	1014 Bytes
<a href="#">192.168.0.254</a> 	Local Host	6	0	netlab0	3 days, 5 h, 58 min, 58 sec		Sent Rcvd	156.76 bit/s ↓	22.7 MB
<a href="#">192.168.0.105</a> 	Local Host	7	0	netlab5 [GIOVANNI-LAPTOP]	3 days, 5 h, 39 min, 44 sec		Sent Rcvd	156.76 bit/s ↑	25.87 MB
<a href="#">192.168.0.104</a> 	Local Host	10	0	netlab4	3 days, 5 h, 39 min, 46 sec		Sent Rcvd	156.76 bit/s ↑	24.8 MB
<a href="#">192.168.0.103</a> 	Local Host	11	0	netlab3	3 days, 5 h, 39 min, 49 sec		Sent Rcvd	156.76 bit/s ↓	25.04 MB
<a href="#">192.168.0.102</a> 	Local Host	8	0	netlab2	3 days, 5 h, 39 min, 57 sec		Sent Rcvd	156.76 bit/s ↓	26.08 MB
<a href="#">192.168.0.101</a> 	Local Host	7	0	netlab1	3 days, 5 h, 58 min, 57 sec		Sent Rcvd	156.76 bit/s ↓	25.58 MB

# 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 e Qualys (commerciale) - 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

**Nessus** Scans Policies richk

INFN  
CURRENT RESULTS: AUGUST 26 AT 3:50 PM

Configure Audit Trail Launch Export Filter Vulnerabilities

Hosts > 192.135.11.16 > Vulnerabilities 25

<input type="checkbox"/>	Severity	Plugin Name	Plugin Family	Count
<input type="checkbox"/>	MEDIUM	Apache Server ETag Header I...	Web Servers	1
<input type="checkbox"/>	MEDIUM	PHP expose_php Information...	Web Servers	1
<input type="checkbox"/>	INFO	RPC Services Enumeration	Service detection	4
<input type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	2
<input type="checkbox"/>	INFO	Apache Banner Linux Distrib...	Web Servers	1
<input type="checkbox"/>	INFO	Backported Security Patch D...	General	1
<input type="checkbox"/>	INFO	Common Platform Enumerati...	General	1
<input type="checkbox"/>	INFO	Device Type	General	1
<input type="checkbox"/>	INFO	Ethernet Card Manufacturer ...	Misc.	1
<input type="checkbox"/>	INFO	HTTP Methods Allowed (per ...	Web Servers	1
<input type="checkbox"/>	INFO	HTTP Server Type and Version	Web Servers	1
<input type="checkbox"/>	INFO	HyperText Transfer Protocol (...)	Web Servers	1

**Host Details**

IP: 192.135.11.16  
MAC: 7c:5cf8:ce:c9:80  
OS: Linux Kernel 2.6  
Start: August 26 at 12:22 PM  
End: August 26 at 12:36 PM  
Elapsed: 13 minutes  
KB: Download

**Vulnerabilities**

Donut chart showing vulnerability counts: 1 Medium (orange), 24 Info (blue).

# Auditing di rete

## Cyber Threat Intelligence (CTI)

La Threat Intelligence, consiste nell'attività di raccolta di informazioni riguardo potenziali minacce provenienti da varie fonti; i dati vengono memorizzati, correlati e processati da processi automatici di Threat intelligence che possono generare allarmi (alert) o attivare delle azioni (Active Response).

Esempi di sorgenti delle informazioni possono essere EDR (Endpoint Detection and Response) ovvero agenti su dispositivi quali PC, , oppure Honeypot , network monitor e NIDS (Network Intrusion Detection System).

Il collettore e analizzatore dei dati è tipicamente un **SIEM** (Security Information and Event Management).

L'organizzazione delle fonti e la gestione del SIEM può essere operata da un centro operativo denominato **SOC** (Security Operation Center).

