1° PARTE

Posta elettronica

La **posta elettronica**, o email, è il **servizio più importante e antico di Internet**, che ha rivoluzionato la produttività e il modo di lavorare. Le **mailing-list**, basate sulla posta elettronica, insieme alle **USENET** NEWS, costituiscono una delle **principali forme di comunicazione globale**, permettendo discussioni su vari argomenti come software, hobby, politica e sociale. Oggi la posta elettronica è considerata uno strumento di comunicazione fondamentale. Il **servizio di posta elettronica coinvolge due programmi: il Mail User Agent** (come Thunderbird, Eudora, Microsoft Outlook) e il programma di trasporto (come **Sendmail**, Postfix, Qmail).
Il **Mail User Agent** è l'interfaccia utente che svolge **diverse funzioni**:
- La **composizione del messaggio** seguendo la sintassi definita nell'RFC822, la gestione dell'agenda elettronica e dell'indirizzario, e la gestione automatica dei campi dell'intestazione (come il destinatario e l'oggetto del messaggio).
- La **visualizzazion**e separando gli header dal corpo e gestendo gli allegati. Fornisce strumenti di archiviazione e classificazione dei messaggi, e permette l'interazione con il sistema per gestire file speciali (Postscript, PDF, PNG, ecc.).
- L'**eliminazione** avviene da parte dell'utente che può cancellare messaggi, automaticamente (filtri) o manualmente, per evitare che la mailbox diventi troppo grande e danneggi il server di posta.
Il programma di trasporto (Sendmail) svolge le seguenti funzioni:
- Il **trasferimento** quando il Mail User Agent invia il messaggio, viene passato al programma di trasporto, che interpreta l'indirizzo e provvede al trasferimento del messaggio, attivando una sessione con il server di destinazione o una macchina intermedia se il server è congestionato o irraggiungibile.
- **Invio di una notifica** all'utente quando il messaggio non viene inviato, l'utente viene informato (per ritardi o errori di sintassi). Alcuni prodotti gestiscono la ricevuta di ritorno, che non è standardizzata ma è importante nella pubblica amministrazione.
Il **programma di trasporto email**, come **Sendmail**, gestisce l'**invio** e la **ricezione** della posta utilizzando **SMTP**. Sendmail supporta anche alias e mailing list prototipali, ma per mailing list efficienti sono necessari programmi come majordomo.
Il programma popper (**POP3**) permette di interagire con il programma di trasporto direttamente da un PC connesso in rete, consentendo la gestione della posta dal PC client. Il **protocollo IMAP** offre una funzione simile ma con maggiore versatilità e sicurezza grazie a un'autenticazione più robusta.
Gli **indirizzi email** seguono il formato user@host.domain o user@domain. Per attivare correttamente la posta elettronica, il DNS deve includere la definizione del mailhost con il record MX e preferibilmente definizioni multiple per creare server di backup. Sendmail richiede anche parametri di configurazione specifici per gestire la posta per un dominio Internet.
È importante avere un **gestore di posta secondario**, situato in una rete esterna, per **salvare temporaneamente i messaggi** in caso di malfunzionamenti del server principale. Questa funzione, nota come **Mail Relay**, era utilizzata dagli spammer fino alla versione 8 di Sendmail. Dalla versione 9, il relaying è limitato agli host autorizzati elencati in una speciale tabella.

```
Received:      elenca i server che ha attraversato
Message-ID:    identificativo del messaggio
                    (B00002222000@mailhost.dom.it)
Date:          data Wed, 23 Oct 2000 10:22:00 +0100
From:          utente mittente
Subject:       soggetto
To:            utente destinatario
Cc:            utenti destinatari in carbon copy
Bcc:           utenti destinatari in Blind Carbon Copy
Mime-Version:  intestazioni MIME
```

RFC822 definisce una serie di campi di intestazione obbligatori per il corretto funzionamento della posta elettronica (immagine a sinistra

Sendmail

La configurazione di **Sendmail** è una **funzione complessa**, semplificata da uno pseudo linguaggio chiamato M4, che consente di attivare delle funzioni mediante invocazione di macro:

```
VERSIONID(`@(#)version.m4       8.9.1.1 (Berkeley) 7/2/98')
OSTYPE(linux)                                  tipo di sistema
MASQUERADE_AS(`miodominio.it')                  nome del dominio di posta
define(`confCONNECTION_RATE_THROTTLE', `2') max livello di carico accettato
                                                          sul server
define(`confMAX_DAEMON_CHILDREN', `200')     max numero di demoni contemporanei
define(`confMAX_MESSAGE_SIZE',`5000000')     max dimensione msg
define(`confMIN_FREE_BLOCKS',`100')          max dimensione libera accettata
                                                       per  /var/spool/mail
FEATURE(`smrsh')                 usa una shell con funzionalità limitate
FEATURE(`use_cw_file')          elenca i domini di posta accettati nel file
    /etc/mail/sendmail.cw
FEATURE(`always_add_domain')    aggiungi il dominio agli indirizzi che ne sono privi
FEATURE(`relay_entire_domain') effettua relaying per l'intero dominio
FEATURE(`relay_based_on_MX')      "      "      "     "  basandoti sull'MX record
FEATURE(`access_db', `hash /etc/mail/access') accetta oggetti solo dagli host
                                                        elencati nel file
```

Elenca i domini o gli host per i quali si controlla l'accesso

/etc/mail/access

```
cyberspammer.com   550 We don't accept mail from spammers
spammer@aol.com    550 We don't accept mail from spammers
150.10.1.13        REJECT
151.20.0.0         OK
193.133.108.0      OK
210.205.1.2        550 We don't accept mail from spammers
```

Elenca i domini per i quali si fa virtual hosting

/etc/mail/sendmail.cw

```
miodominio.it        dominio principale
vhost1.it            dominio di cui si fa virtualhost
vhost2.it            dominio di cui si fa virtualhost
...
```

Elenca i domini per i quali si accetta relaying

/etc/mail/relay-domains

```
miodominio.it     dominio principale
vhost1.it         dominio di cui si fa virtualhost
vhost2.it         dominio di cui si fa virtualhost
193.12.12.212     server secondario di posta
libero.it         ..domini  per l'accesso via POP3
iol.it
tiscalinet.it
tin.it
tim.it
infinito.it
email.it
```

PEC

La **Posta Elettronica Certificata (PEC)** è un sistema di comunicazione simile alla posta elettronica standard, ma con **caratteristiche di sicurezza e certificazione** della trasmissione che rendono i messaggi opponibili a terzi. Queste caratteristiche sono definite nel Decreto del Presidente della Repubblica 11 febbraio 2005 n. 68 e nei relativi documenti tecnici, tra cui:

- Regole tecniche per la formazione, trasmissione e validazione, anche temporale, della posta elettronica certificata.
- Circolare CNIPA del 24 novembre 2005 n.49.

Questi documenti definiscono gli aspetti generali del servizio e i dettagli tecnici necessari per garantire la validità del servizio e l'interoperabilità tra i diversi gestori di posta certificata. Il Codice dell'Amministrazione Digitale (CAD, Decreto Legislativo 82/2005 modificato dal Decreto Legislativo 235/2010) conferma il valore legale della PEC come strumento di trasmissione telematica.

Il **Decreto Legislativo 185/2008**, convertito con in legge, ha accelerato lo **sviluppo delle trasmissioni telematiche attraverso l'utilizzo della PEC**. L'articolo 16 del Decreto stabilisce che:
- Le nuove società devono dichiarare l'indirizzo PEC all'iscrizione nel registro delle imprese.
- I professionisti devono dichiarare l'indirizzo PEC ai rispettivi ordini entro un anno.
- Le società già esistenti devono dichiarare l'indirizzo PEC al registro delle imprese entro tre anni.
- Tutte le pubbliche amministrazioni devono dichiarare il proprio indirizzo PEC.

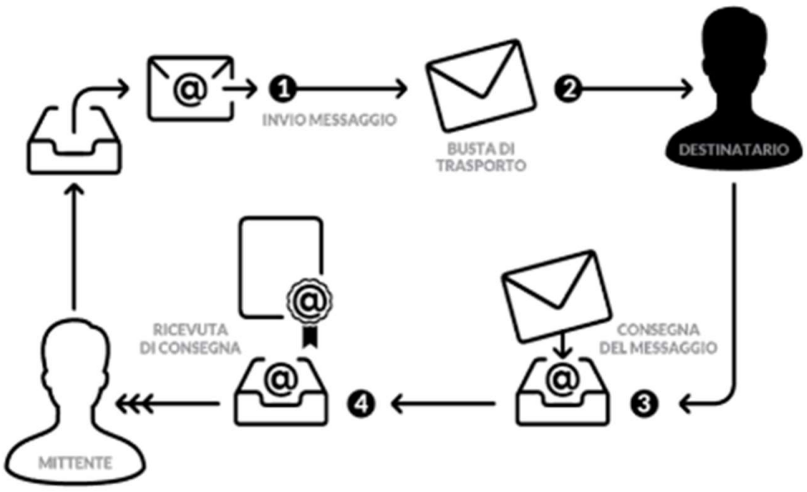
La PEC è raccomandata per:
- L'invio di documenti a Enti e Pubbliche Amministrazioni.
- La trasmissione di documenti relativi a gare d'appalto.
- La convocazione di consigli, giunte e assemblee.
- Lo scambio di documenti tra aziende con relazioni commerciali.
- La gestione delle comunicazioni all'interno di strutture con molte sedi operative.
- La gestione delle comunicazioni ufficiali all'interno di reti di aziende o commerciali.
- L'invio degli stipendi ai dipendenti.

Una trasmissione può essere considerata posta certificata solo se sia il **mittente** che il **destinatario utilizzano caselle di posta elettronica certificata** (PEC); altrimenti, il sistema fornirà solo parzialmente le funzionalità di certificazione, come la ricevuta di avvenuta consegna. I gestori di PEC devono registrare tutti i principali eventi di trasmissione per 30 mesi, fornendo prove su richiesta e utilizzando un riferimento orario allineato con gli istituti ufficiali per garantire l'ora esatta nelle registrazioni e nelle ricevute.

I **servizi di PEC** utilizzano protocolli sicuri (https per webmail, smtps, smtp starttls, pop3s, imaps) per impedire la manomissione dei messaggi da parte di terzi. L'identificazione degli utenti avviene tramite user e password o certificati digitali, e gli utenti devono fornire prova della propria identità. La falsificazione dell'identità del mittente è inibita.

Quando si invia un messaggio da una casella di posta certificata (PEC), si riceve dal proprio provider una **ricevuta di accettazione firmata**, che attesta il momento della spedizione e i destinatari, distinguendo tra quelli con PEC e senza PEC. Queste informazioni sono disponibili in formato testo e XML.

Il gestore PEC del mittente crea una **busta di trasporto**, contenente il messaggio originale e i principali dati di spedizione, firmata dal provider per garantirne l'integrità. Per mantenere l'integrità del messaggio, sia il mittente che il destinatario devono utilizzare la PEC tramite **protocolli sicuri**.



Il messaggio certificato viene consegnato al destinatario all'interno della sua busta di trasporto. Dopo la **consegna**, il provider del destinatario invia al mittente una ricevuta di consegna firmata, che attesta la consegna con data, ora e contenuto consegnato. La ricevuta di consegna include anche il messaggio originale e gli eventuali allegati, fornendo al mittente una prova firmata del contenuto recapitato con data e ora. Questa caratteristica distintiva rende la PEC superiore ai tradizionali mezzi cartacei per l'invio di documenti ufficiali

MIME

La **posta elettronica** ha subito **importanti cambiamenti** rispetto alle sue origini. Ora i messaggi sono trasmessi in diverse lingue, con caratteri accentati e alfabeti non latini. Inoltre, molti messaggi contengono **informazioni non testuali** come audio, video e file compressi.
Per gestire queste nuove esigenze, è stato **introdotto lo standard** di codifica Multipurpose Internet Mail Extensions (**MIME**), definito negli RFC1341 e RFC1521. **MIME aggiunge nuovi criteri** rispetto a quelli dell'RFC822, che continua a essere utilizzato per definire le modalità di composizione dei messaggi di posta elettronica.
L'implementazione di MIME comporta l'**aggiunta di nuovi header** senza compromettere il funzionamento di base della posta elettronica e dei meccanismi di trasporto. Di conseguenza, per gestire MIME è sufficiente **aggiornare i Mail User Agent**.

Nuovi headers introdotti nell'RFC822 da MIME

header	significato
MIME-version	identifica la versione MIME
Content-Description	descrive il contenuto del messaggio in forma leggibile
Content-Id	identificatore del messaggio
Content-Transfer-Encoding	tipo di codifica utilizzata per la trasmissione
Content-Type	tipo di contenuto del messaggio.

Il **MIME-type** raffigurato a destra è diventato molto utilizzato da altre applicazioni Internet per identificare il tipo di contenuto associato ad un certo file, in modo da selezionare l'azione corretta da intraprendere

Esistono **tre tipi di codifica dei messaggi**:
1) R**appresentazione del Messaggio di Posta Elettronica**:
La corretta rappresentazione del messaggio di posta elettronica è cruciale per il suo buon esito, poiché i computer interpretano le informazioni in base alla loro configurazione hardware e software. La codifica più comune, ASCII, utilizza 7 bit per rappresentare l'informazione ed è utilizzata sia nei sistemi Unix che in quelli Windows, sebbene con variazioni nei caratteri speciali.
2) **Codifica dei Messaggi su MIME**:
Oltre a ASCII ed EBCDIC, esiste la codifica base64 introdotta da MIME, che rappresenta sequenze di bit utilizzando caratteri alfanumerici. Questa codifica produce linee lunghe al massimo 76 caratteri, garantendo massima compatibilità con i programmi di trasporto della posta elettronica. La codifica base64 è ideale per i file binari, superando la limitazione dei 1000 caratteri di lunghezza per ciascuna riga del messaggio.
3) **Codifica Preferita per i Messaggi di Testo**:

MIME-Types

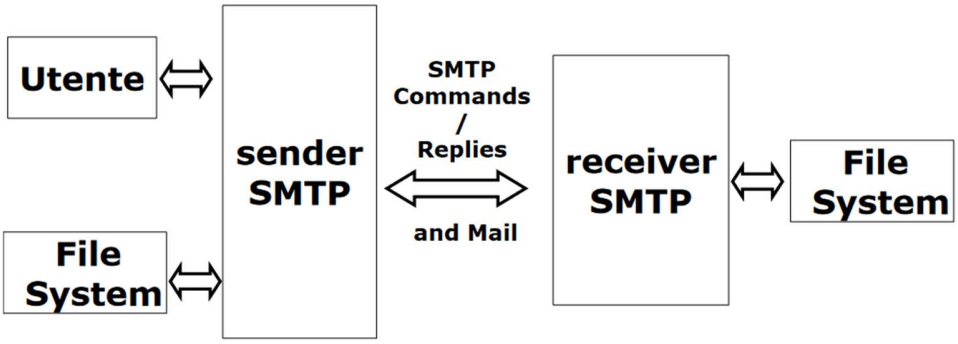
Tipo	Sottotipo	Ref.
Text	Plain	[RFC2646,RFC2046]
	RichText	[RFC2045,RFC2046]
	html	[RFC2854]
	xml	[RFC3023]
	sgml	[RFC1874]
Image	Gif	[RFC2045,RFC2046]
	Jpeg	[RFC2045,RFC2046]
Audio	Basic	[RFC2045,RFC2046]
Video	Mpeg	[RFC2045,RFC2046]
Application	Octet-stream	[RFC2045,RFC2046]
	Postscript	[RFC2045,RFC2046]
Message Rfc822		[RFC2045,RFC2046]
	Partial	[RFC2045,RFC2046]
	External-body	[RFC2045,RFC2046]
	http	[RFC2616]
	news	[RFC1036]
Multipart	Mixed	[RFC2045,RFC2046]
	Alternative	[RFC2045,RFC2046]
	Parallel	[RFC2045,RFC2046]
	Digest	[RFC2045,RFC2046]

Per i messaggi di testo, la codifica base64 può essere inefficiente. Si preferisce quindi la codifica quoted-printable encoding di MIME, utilizzando la codifica ASCII standard con un criterio per rappresentare caratteri speciali superiori a 127. L'header Content-Type, definito nell'RFC1521, specifica il tipo e il sottotipo del contenuto del messaggio, come ad esempio "video/mpeg".
Lista dei MIME-Types nell'immagine a destra

2° PARTE

SMPT (Simple Mail Transfer Protocol)

Il trasporto dei messaggi di posta elettronica avviene utilizzando il Simple Mail Transfer Protocol (SMTP), definito nel RFC 821 Il suo obiettivo è **trasferire i messaggi di posta elettronica in modo affidabile e efficiente**. Caratteristica dell'SMTP è la capacità di trasportare mail attraverso diversi ambienti di servizi di trasporto. Un servizio di trasporto fornisce un interprocess communication environment (IPCE).
L'invio di messaggi di posta elettronica avviene **indipendentemente dal tipo di rete**: consiste nello scambio di dati tra due IPCE.
Come risultato di una richiesta di posta dell'utente viene attivato un canale di comunicazione **bidirezionale** (sul port number **25**) tra il server SMTP **trasmettitore che genera i comandi** ed il server SMTP **ricevente** (che può essere il destinatario finale o un intermediario).
Le risposte SMTP sono generate dal ricevente in risposta ai comandi SMTP ed inviate al trasmettitore



scambio mail

I comandi di mail hanno una sintassi rigida, così come i codici di errore. Il dialogo è volutamente a **passi bloccanti**, uno alla volta :

- Una volta attivato il canale trasmissivo, l'SMTP-sender invia il comando **MAIL** indicando colui che invia il mail. Se il ricevente può ricevere mail risponde con **OK**
  - L'argomento del comando MAIL indica chi manda il mail (crea un **reverse-path** implementando una **return route**, sulla quale verranno istradati eventuali messaggi di errore.
- Il sender invia il comando **RCPT** identificando il recipient del mail; se il ricevente può ricevere mail per quel recipient risponde con **OK**, altrimenti risponde con un codice di **reject** del recipient (non della sessione mail). I due SMTP server possono scambiarsi diversi recipient.
  - L'argomento del comando RCPT indica chi è il destinatario del mail (crea un **forward-path** implementando una **source route**)
- Il server SMTP invia i dati della mail, **terminando con una sequenza speciale**. Se il receiver interpreta correttamente i dati, risponde con **OK**

Quando un messaggio è inviato a più utenti, viene inviata una sola copia per tutti i destinatari di uno stesso host

Ordine dei comandi

RIVEDIIIIIII HAI SOLO FATTO COPIA INCOLLA PER ORA!!

- Il primo comando deve essere HELO, tale comando può essere ri-immesso anche successivamente. Se l’argomento non è accettabile viene ritornato un errore 501 failure
- I comandi NOOP, HELP, EXPN, VRFY possono essere utilizzati ovunque nella sessione
- I comandi MAIL, SEND, SOML o SAML iniziano una transazione di mail, per l’invio del messaggio. Deve esserre seguito da uno o più comandi RCPT e dal comando DATA, nell’ordine. Dopo l’immissione del testo del messaggio deve seguire la sequenza <CRLF>.<CRLF> . Una transazione può essere abortita col comando RSET
- L’ultimo comando è QUIT, che non può essere usato un nessun altro momento della sessione

3° PARTE

4° PARTE

HTTP

cosa è

HTTP (Hypertext Transfer Protocol) è il protocollo utilizzato per il trasferimento di dati sul Web. È il fondamento della comunicazione di dati su Internet e permette la trasmissione di documenti ipertestuali, come pagine web, che possono includere testo, immagini, video e altri contenuti multimediali.

funzionamento

-Client-Server: Il client (browser) invia richieste al server.
-Connessione: Il client apre una connessione TCP al server.
-Richiesta: Il client invia una richiesta HTTP (es. GET, POST).
-Risposta: Il server elabora la richiesta e invia una risposta (es. contenuto della pagina).
-Chiusura: La connessione può essere chiusa o riutilizzata per ulteriori richieste.

versioni

le principali versioni sono:
-HTTP/0.9: La prima versione, molto semplice, usata solo per trasferire testo semplice.
-HTTP/1.0: Introduce i metodi di richiesta e le intestazioni HTTP.
-HTTP/1.1: Aggiunge miglioramenti significativi come la connessione persistente, il supporto per i proxy e le cache.
-HTTP/2: Introduce un miglioramento delle prestazioni con multiplexing delle richieste e risposte su una singola connessione TCP.
- Multiplexing: Invia più richieste simultanee su una connessione.
- Compressione degli header: Riduce la sovraccarica dei dati.
- Server Push: Invia risorse non richieste anticipatamente per velocizzare il caricamento.
-HTTP/3: Utilizza il protocollo QUIC invece di TCP, migliorando ulteriormente la velocità e l'affidabilità delle connessioni.
- Basato su QUIC: Utilizza il protocollo QUIC invece di TCP, migliorando la velocità e la connessione.
- Connessione rapida: Minimizza il ritardo.
- Sicurezza: Incorpora la crittografia end-to-end.

PAGINE WEB

pagine statiche

Le pagine web **statiche** sono file fissi memorizzati su un web server, come HTML, CSS e immagini, che vengono inviati ai browser degli utenti senza modifiche. Questo tipo di pagina è rapido da caricare e semplice da gestire, ma non offre contenuti personalizzati o interattivi.

Il web server per le pagine statiche svolge principalmente tre funzioni:

-Archivia i file delle pagine.
-Risponde alle richieste HTTP inviando questi file ai browser degli utenti.
-Gestisce errori, come inviare un errore "404 Not Found" se la pagina richiesta non è disponibile

Il web server nelle pagine statiche gestisce e risponde alle richieste HTTP inviando pagine web statiche pre-esistenti, come file HTML e risorse associate, ai browser degli utenti senza alcuna elaborazione o modifica aggiuntiva.

pagine dinamiche

Sono generate in tempo reale dal server in base alle interazioni degli utenti o ad altri dati. Utilizzano script lato server come PHP o Python per creare contenuti personalizzati e interattivi. Questo le rende ideali per siti web che necessitano di aggiornamenti frequenti e personalizzazione, come e-commerce o portali di servizi.

Il web server nelle pagine dinamiche si occupa della:

-Elaborazione delle Richieste: Quando un utente fa una richiesta per una pagina dinamica, il web server la riceve e determina quale script deve essere eseguito per generare la pagina.
-Esecuzione degli Script: Il server esegue gli script lato server, come PHP, Python o Ruby. Questi script possono interagire con database, servizi esterni, o altri componenti del sistema per raccogliere dati necessari.
-Generazione della Pagina: Basandosi sui dati raccolti e sulla logica dello script, il server genera il contenuto HTML della pagina. Questo processo può includere la personalizzazione del contenuto in base agli input dell'utente, come dati di login o preferenze.
-Invio della Risposta: Una volta che la pagina è stata generata, il server invia il contenuto HTML al browser dell'utente tramite HTTP. Questo contenuto è spesso accompagnato da CSS, JavaScript, e immagini, che aiutano a formare l'aspetto finale della pagina sul browser dell'utente.
-Gestione delle Sessioni: Per pagine che richiedono personalizzazione o mantenimento dello stato dell'utente (es. carrello della spesa), il server può anche gestire sessioni attraverso cookie o altre tecnologie.

5° PARTE

Strumenti di programmazione web

- Perl:
  -Linguaggio di programmazione ad alto livello, procedurale e interpretato
  -Molte funzionalità derivano da altri linguaggi come C e scripting Shell unix
  -Molto usato per la scrittura di Common Gateway Interfaces (CGI- tecnologia standard usata dai web server per interfacciarsi con applicazioni esterne generando contenuti web dinamici)
  -Rilasciato con licenza GPL

- PHP:
  -Acronimo di Hypertext Preprocessor
  -Linguaggio di programmazione interpretato: il testo viene scaricato dal web server ed eseguito “on the fly” dal browser
  -Ha stravolto la programmazione web consentendo di inserire nella pagina contenuti dinamici provenienti da database

- Python:
  -Linguaggio di programmazione dinamico orientato agli oggetti
  -Fornito di una estesa libreria standard
  -Estremamente veloce ed efficiente

- Javascript:
  -Sta prendendo il sopravvento nella programmazione web
  -Due tipi di programmazione:
    1. Lato client: gli script vengono eseguiti durante il caricamento della pagina web sul dispositivo dell’utente tramite le javascript virtual machine
    2. Lato server: molti sono i framework che grazie al javascript script engine permettono l’esecuzione lato server, come node.js (permette di usare javascript non solo per rendere le pagine web interattive ma anche per creare, ad esempio, un server web)
  -Linguaggio interpretato

- AJAX:
  -Acronimo di Asynchronous Javascript and XML
  -Tecnica di sviluppo software web per creare applicazioni più dinamiche e interattive.
  -Si basa sullo scambio di dati in background fra web browser e server, consentendo l’aggiornamento dinamico di una pagina web senza esplicito ricaricamento da parte dell’utente
  -Ci sono molti framework che facilitano la programmazione Ajax:
    1. JQuery
    2. Dojo

E-commerce

- Finanza Elettronica:
  -Trading online, applicazione ormai molto importante in rete, ha dato la possibilità di operare anche a borse chiuse e con speciali incentivi, diminuendo i costi delle transazioni in modo drastico

- Telemarketing:
  -L'utilizzo di tecnologie ipermediali consente la creazione di siti web con stile sofisticato, aggiornamento in tempo reale delle informazioni e aumento dell'affidabilità e disponibilità.
  -Messaggi pubblicitari più ricercati e appropriati per l'utente grazie al ruolo crescente dell'Augmented reality e Virtual reality.

- Banner e animazioni:
  -Una delle fonti principali di guadagno in rete sono i banner animati inseriti nelle pagine web
  -Viene utilizzata la tecnica animated GIF, che consente di salvare più immagini e visualizzarle in sequenza

- Commercio elettronico:
  -Internet offre una impressionante immediatezza nello scambio di informazioni, una maggior potenzialità nell'illustrare i prodotti ed una maggior versatilità e sicurezza nelle transazioni
  -Le aziende si muovono verso il commercio online per massimizzare i profitti, aumentare nuovi affari, massimizzare la sicurezza e minimizzare i costi

- Secure web:
  -La crescente diffusione di Internet impone l'adozione di tecnologie Web Sicure. Possibili violazioni:
    1. Estensibilità del server: l'aggancio con database può compromettere la sicurezza del sistema
    2. Estensibilità del browser: l'uso di Java, javascript e VBScript può estendere le funzionalità del browser e compromettere la sicurezza del sistema
    3. Distruzione del servizio: denial-of-service attacks

  -Un server sicuro necessità di 3 interventi fondamentali:
    1. Sicurezza del server e dei dati: occorre essere certi dell'impossibilità di manipolazione dei dati e del server web
    2. Sicurezza dei dati mentre transitano dal server all'utente: Occorre essere sicuri che le informazioni sensibili (login/password, dati finanziari) non possono essere alterati
    3. Sicurezza del computer dell'utente: occorre essere certi che programmi e informazioni scaricate dall'utente non danneggiano il suo computer

  -Requisiti essenziali per un sito web sicuro:
    1. Accesso al server: controllato da un firewall
    2. Autenticazione (server ⇐=>Browser)
    3. Confidenzialità
    4. Integrità
    5. Non ripudiabilità

-Crittografia: Ogni volta che un utente scarica dalla rete programmi da installare sul computer, si espone a possibili attacchi o violazioni della privacy, perciò sono importanti degli strumenti di anonimizzazione che mascherano l'utente finale

1. SSL (secure socket layer)è un encryption system a doppia chiave pubblica e privata usata nei server per garantire la privacy durante le trasmissioni attraverso Internet
   →Permette ai server di criptare le informazioni sensibili in testo cifrato prima dell'invio ai client, evitando così la lettura da parte di terzi
   →Ogni server per poter inviare la propria chiave pubblica ai client deve possedere un certificato X.509. Ogni certificato contiene:
   - Chiave pubblica
   - Nome ed indirizzo associato con il server
   - Un numero si serie o data di pubblicazione del certificato
   - Data di fine validità del certificato
     →I certificati sono pubblicati dalle certificate authority (CA):
     E' un ente terzo che assegna certificati ai server, per farlo ne verifica l'identità e se è valida, firma digitalmente il certificato con la propria chiave pubblica; attraverso la propria chiave privata la CA garantisce che il certificato è valido

6° PARTE

TLS

- Trasport Layer Security
- Protocollo standard IETF (Internet Engineering Task Force)
- Consente alle applicazioni client/server di comunicare attraverso una rete in modo tale da prevenire la manomissione dei dati, la falsificazione e l'intercettazione
- Oper sopra al livello Transport
- evoluzione del protocollo SSL
- All'inizio utilizza la porta 80 e poi usa la 443

Il funzionamento del protocollo può essere suddiviso in 3 fasi principali:

- Negoziazione fra le parti dell'algoritmo da utilizzare
- Scambio delle chiavi e autenticazione
- Cifratura simmetrica e autenticazione dei messaggi

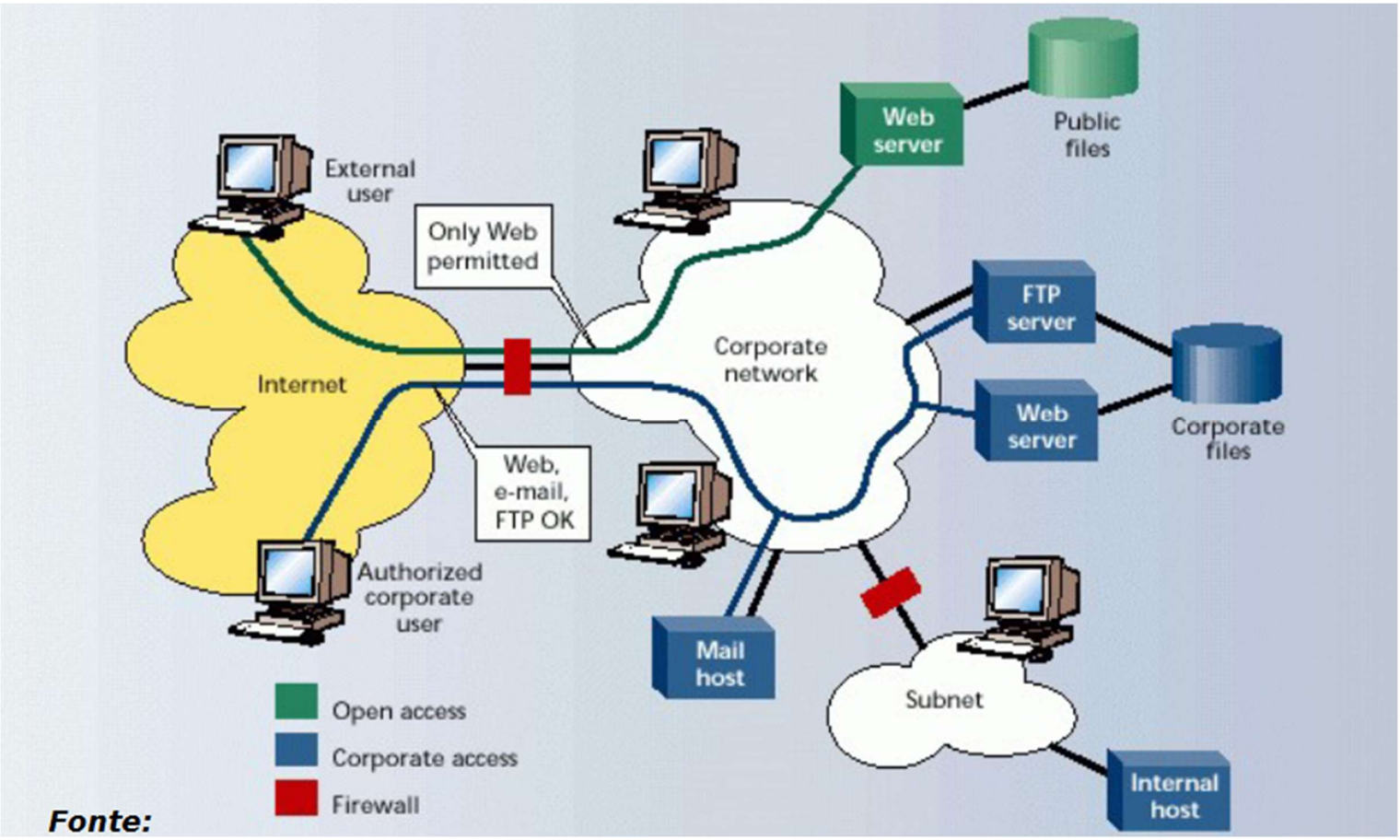
TLS 1.3

- Rispetto al TLS 1.2 sono state introdotte diverse migliorie nella generazione delle chiavi e nell'uso degli algoritmi crittografici
- Vengono supportati i nuovi protocolli di handshake (round trip time, tempo necessario all'invio del segnale e alla ricezione dell'acknowledgement dello stesso)
- Rimosse funzioni obsolete
- Aggiunte funzionalità che rafforzano la sicurezza delle transizioni

Sicurezza di rete

Importanza crescente:

- Aumento degli intrusori
- Aumento degli attacchi
- Esigenza di confidenza sempre crescente nelle tecnologie ipermediali e di rete
- Le tecniche di protezione devono essere accessibili ai più
- Attenzione ai costi



- On-line help

1) **Confidenzialità**
    a) Le informazioni possono essere lette solo da che ne ha diritto
2) **Integrità**
    a) Le informazioni possono essere modificate solo da chi ne ha diritto
3) **Disponibilità**
    a) Le informazioni possono essere lette/scritte quando necessario; le risorse devono poter essere usate solo da chi ne ha diritto
4) **Tracciabilità**
    a) Individuazione di chi ha invocato un'operazione
5) **Accountability**
    a) Quanto è utilizzata una risorsa
6) **Auditability**
    a) Poter verificare l'efficacia dei meccanismi utilizzati
7) **Forensics**
    a) Poter provare che certi attacchi hanno avuto luogo
8) **Privacy**
    a) Chi/come e se può usare le proprie informazioni personali

Attacco ad un sistema informatico

Definizione

Sequenza di azione eseguite per ottenere il controllo di un sistema informatico

Conseguenza

è possibile raccogliere informazioni, modificare informazioni, impedire ad altri di accedere alle informazioni

- Automatizzabile/non automatizzabile
- Ogni attacco è in realtà un attacco al SO

Fasi di un attacco

1) raccolta informazioni [giorni/mesi]
2) Individuazione delle **vulnerabilità** [giorni/mesi]
3) Ricerca o costruzione di un **programma** (exploit) **che sfrutti la vulnerabilità** [giorni/mesi]
4) Esecuzione dell'exploit
5) Installazione di strumenti per il controllo
6) Cancellazione delle tracce dell'attacco
7) Accesso (modifica) ad un **sottoinsieme** delle informazioni

Vulnerabilità

Definizione

Difetto in un componente del sistema

Conseguenze

Sfruttando il difetto riesco a generare un **comportamento inatteso** del componente; questo comportamento permette di violare le proprietà di sicurezza

Classificazione

- Vulnerabilità **procedurale** (nel modo in cui si fa)
- Vulnerabilità **organizzativa** (nelle persone che fanno)
- Vulnerabilità **degli strumenti informatici** (nello strumento hardware e/o software che si usa)

Vulnerabilità degli strumenti informatici

- **Specifica**
  - Il componente è, inutilmente, più generale del necessario
- **Implementazione**
  - L'errore è stato commesso nello sviluppo del componente
- **Strutturale**
  - l'errore nasce quando si integrano i componenti che costituiscono il sistema complessivo)

Analisi del rischio

- Cercare di garantire che ci sia una giustificazione ai costi della sicurezza
- E' importante **eliminare** quei rischi che possono provocare **attacchi dannosi**
- Comprende:
  - analisi della vulnerabilità
  - analisi degli attacchi
  - analisi degli impatti
  - analisi delle minacce
  - individuazione rischio accettabile ed introduzione delle contromisure

Analisi degli impatti

- Per ogni attacco si deve stabilire la perdita dell'azienda dovuta all'attacco in esame
- Dipende dai:
  - Dati e dalle risorse che possono essere acceduti a seguito dell'attacco
  - Dai processi aziendali che utilizzano quelle risorse e dati
- alcune perdite:
  - Non sono quantificabili
  - Sono difficilmente quantificabili

Analisi delle minacce

- Per ogni attacco è necessario determinare
  - Chi **ha interesse** ad eseguire l'attacco
  - Chi **dispone delle risorse** necessarie per l'attacco
- Un attacco può essere eseguito solo se l'intersezione tra i due insiemi è vuota

Contromisure

- Per ogni vulnerabilità esiste almeno una contromisura in grado di eliminarla
- La contromisura può essere di tipo
  - **Tecnico**
    - modifico un'applicazione
  - **Organizzativo**
    - divieto di usare un'applicazione
  - **Personale**
    - controlli su una persona, formazione

- Ogni contromisura ha un costo
    - **Tecnico**
        - Prima si risolve un problema minor impatto sui costi avrà
    - **Organizzativo**
        - più complesso eseguire certe operazioni

Rischio residuo

- Scelte le contromisure da applicare può rimanere un certo rischio detto **residuo**
- Accettare la presenza del rischio residuo significa accettare l'uso di un sistema anche con rischio non nullo

Esempi di attacchi

Virus

- Il modo per difendersi da questa vera e propria catastroge che può colpire chiunque in qualsiasi momento è solo l'uso di un **software antivirus**
- Il software va costantemente **aggiornato**, altrimenti perde di efficacia

Trojan Horse

- La difesa contro questo subdolo strumento è solo quella di scaricare il software in modo molto attento, cercando ove possibile di verificare l'integrità del codice mediante firma digitale
- Impossibile accorgersi della presenza di un Trojan Horses, a men0 che ci si tenga informati

Hoax e catene

- SOno pericolosi quanto i virus, ma innocui
- Minano la fiducia della gente nella rete
- Inducono a comportamenti fastidiosi e scorretti

SPAM

- L'unica difesa dallo SPAM si ha usando dei mail user agents che filtrino questi messaggi
- E' importante per chi amministra dei sistemi di posta elettronica di non essere oggetto involontario di invio di SPAM, altrimenti si sprecano importanti risorse o si finisce in liste di prescrizione in cui i siti vengono da molti **filtrati**

7° PARTE

HTTP e sicurezza

Il **World wide web** viene soprannominato “World Wild Web”, vista la diffusione ed i diversi ambienti applicativi che si basano su di esso, le applicazioni principali che costituiscono una potenziale esposizione in termini di sicurezza sono:

- **Cookies**
- **Uso di programmi esterni**
- **Interfacce verso DB**

Cookies

Sono stati introdotti con l’ormai obsoleto browser “Netscape 2.0”, sono stringhe di caratteri ASCII che vengono passate da un server web al browser dell’utente(**Firefox, Chrome, Safari** ecc) una volta ricevuto il **cookie** il client lo invia al server ogni volta che accede ad un determinato sito , vengono utilizzati per tenere traccia delle scelte che vengono effettuate da un utente, utile per orientare al meglio la pubblicità di un bene o un servizio piuttosto che un altro

eTrust

i cookies però oltre che ad essere un potente strumento per fare pubblicità mirata, pongono problemi riguardo all'effettivo rispetto della privacy di un utente, **eTrust** è un programma creato dalla **Electronic Frontiers Foundation**, per definire uno standard per la **privacy online**, i siti con il logo eTrust sono conformi al progetto che riguarda la tutela dei dati personali degli utenti

Interazione con i database

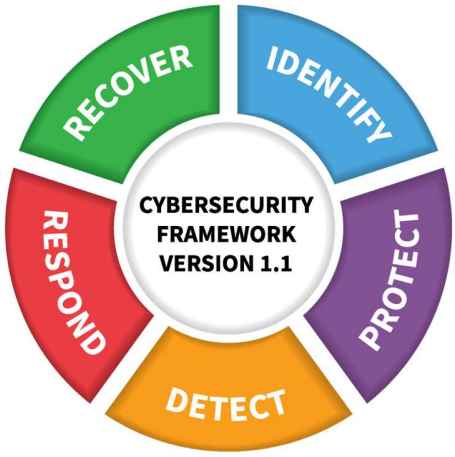
L’interazione con i database viene effettuata tramite determinate procedure chiamate Common Gateway Interfaces, tramite cui si possono costruire pagine web, dinamicamente tramite l’interazione con un database, i linguaggi che vengono usati più frequentemente sono:

- PHP4
- Perl
- C
- TCL/TK
- Python

Sono un problema per la sicurezza perché comportano l’esecuzione di programmi esterni che potrebbero avere degli exploit. se siete curiosi degli exploit → https://www.exploit-db.com/

NIST Cybersecurity Framework

fornisce linee guida e best practice a cui le organizzazioni del settore privato possono attenersi per migliorare la sicurezza delle informazioni e la gestione dei rischi per quanto riguarda la cybersecurity



Detect

Sviluppo e implementazione di strumenti per identificare attività anomale o incidenti di sicurezza, alcune attività chiave sono:

- rilevazione di anomalie ed eventi insoliti
- Monitoraggio continuo
- Capacità di rispondere ad un incidente
- Gestione delle informazioni e degli eventi di sicurezza
- Analisi del comportamento degli utenti

Protect

sono le misure di sicurezza utili a proteggere risorse e dati critici, i punti chiave sono:

- Controllo degli accessi
- addestramento e consapevolezza
- Sicurezza dei dati
- Protezione delle informazioni dei processi e delle procedure
- Manutenzione
- Tecnologie di protezione
- Piano in caso di incidenti di sicurezza (Disaster Recovery)

Respond

Questo punto riguarda la gestione degli incidenti di sicurezza e risposta immediata, per mitigare il più possibile gli effetti negativi di un attacco:

- Piano in caso di incidenti di sicurezza (Disaster Recovery) ← fa parte di entrambi i punti
- Mitigazione degli incidenti
- Comunicazione
- **Miglioramento della Postura digitale**: insieme di politiche e tecnologie messe in campo da un'organizzazione per mitigare i rischi informatici
- reports legali e regolatori

- Analisi post incidente
- Recovery Planning

Recover

consiste nel ripristino delle normali attività e nella prevenzione di attacchi futuri, le attività chiave di questo punto sono:

- Recovery Planning
- Miglioramenti in base alla “lezione imparata”
- Ripristino dei dati e dei sistemi
- Analisi post incidente
- Aggiornamenti alla policy e alle procedure
- Cambio di comunicazione

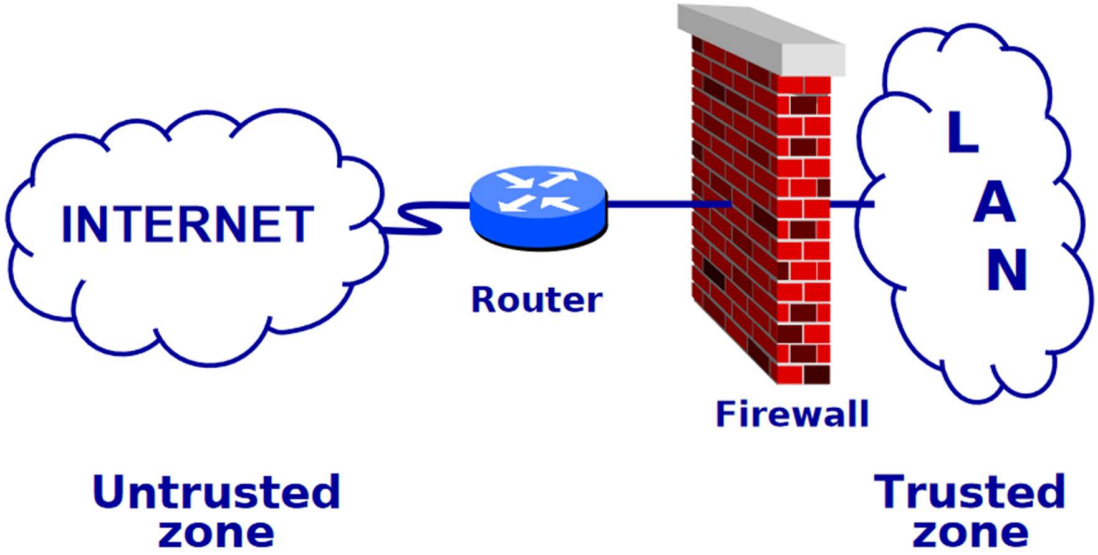
Firewall

Un **Firewall(o muro di fuoco)** è un sistema che ha lo scopo di controllare il traffico fra 2 o più reti, permette di monitorare il traffico in **Entrata/Uscita dalle reti**

- **Access Control:** protegge informazioni le risorse e dagli accessi non autorizzati sia dall’interno sia dall’esterno di una Intranet
- viene posto al confine tra la intranet e Internet
- permette di configurare delle policy per decidere cosa può passare e cosa no

suddivide tutti gli utenti delle reti in **Trusted** e **Untrusted**, l’accesso dalla rete esterna viene forzato a passare per il firewall e viene sottoposto alle regole del firewall, anche gli utenti che fanno della rete devono attraversare il firewall per andare in internet.

Ogni **Socket(combinazione di IP e Porta)** che viene aperto in **Entrata/Uscita** viene verificato in base alle regole definite nel firewall, la configurazione migliore e più sicura è quella che nega tutto tranne ciò che è permesso (**Default Deny o Whitelist**)



La parte Trusted della rete ***NON È SOTTOPOSTA AL CONTROLLO DEL FIREWALL*** per aumentare l'efficacia del firewall è consigliabile separare la rete in ambienti diversi(mettendoci davanti un firewall), ad esempio separare i reparti: Amministrazione, Contabile ecc ecc

Firewall: Packet FIltering

È un filtro di pacchetti livello software, analizza l'intestazione dei pacchetti e decide "che farsene", in base anche alle regole configurate nel firewall in particolare prende in considerazione:

- **Header IP:**
  - mittente
  - destinatario
  - protocollo
  - flag e altre opzioni
- **Header TCP/UDP**:
  - porta mittente
  - porta destinatario
  - flag TCP(SYN, ACK)

e può effettuare una tra le 3 seguenti opzioni:

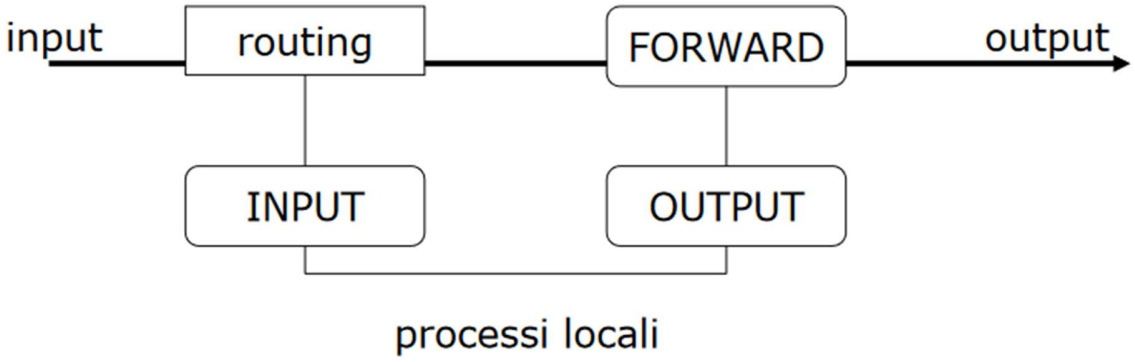
- **ACCEPT**: il pacchetto rispetta tutte le regole imposte e può procedere
- **DENY**: rifiutare il pacchetto eliminandolo dando una giustificazione come host unreachable
- **DROP**: scarta il pacchetto senza motivarne il perchè

il kernel dove viene eseguito il packet filtering, ha una tabella di filtraggio chiamata "filter" dove il tool iptables inserisce o rimuove le regole di filtraggio, il filtraggio viene effettuato in

- **INGRESSO:**
  - sapendo da quale interfaccia arriva il pacchetto, mantenendo protetto il sistema locale
- **USCITA:**
  - gestisco il traffico generato localmente

nella tabella filter ci sono di default 3 liste di regole:

- **INPUT**
- **OUTPUT**
- **FORWARD**



Funzionamento

COMING SOON

Audit

La fase di controllo e analisi dei processi di gestione dei sistemi utilizzati, vengono interrogati i log dei sistemi operativi, delle applicazioni e degli utenti allo scopo di prevenire e rilevare attacchi e intrusioni, da parte di malintenzionati, la cadenza con il quale avviene questo controllo dipende dal grado di sicurezza che si vuole ottenere, dallo spazio di archiviazione che si vuole dedicare ad i log ecc, un'azione che potrebbe destare dei sospetti è un accesso da parte di un utente ad un'ora insolita

Sistemi automatici

Sono software che in automatico eseguono operazioni di audit, alcuni si basano sulla conoscenza degli attacchi più comuni, altri sull'identificazione di attività anomale del sistema

- Nessus
- OpenVAS