Introduzione alla cybersecurity

Sturielet

- Come gentile quel signore ..
- Scusa ma sono di corsa, pagali e mi fai sapere
- Centrifughe al cocktail bar ..
- Si, pronto sono il tecnico dell'ufficio, mi servono …

Alessandro Curioni- Il giorno del Bianconiglio

Il calcolo del danno

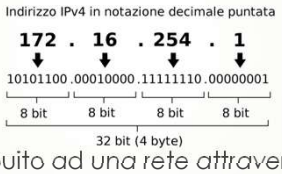
- Vulnerabilità, carenza o imperfezione in una organizzazione, in un processo, in un apparato o tecnologia
- Minaccia è la possibilità che la vulnerabilità sia attivata
- Il rischio è dato dalla gravità della minaccia per la probabilità della minaccia
- Personaggi del copione
  - hacker
  - cracker
  - lamer

Internet ?

Indirizzo IP

- 4 numeri tra 0 e 255 separati dal punto
  - 243.123.234.15
    - Il 192.xxx.xxx.xxx ed il 10.xxx.xxx.xxx sono usate per reti locali

Sono fisicamente 4 ottetti di bit (byte)



Un indirizzo viene attribuito ad una rete attraverso una maschera di rete, che dice quanti indirizzi appartengono a quella rete

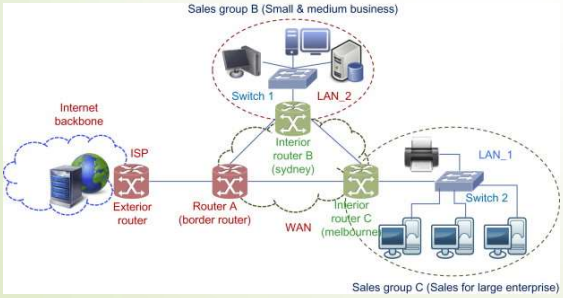
https://it.wikipedia.org/wiki/Indirizzo_IP

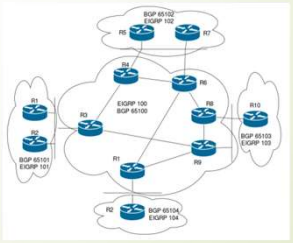
https://it.wikipedia.org/wiki/Maschera_di_sottorete

Indirizzo di broadcast

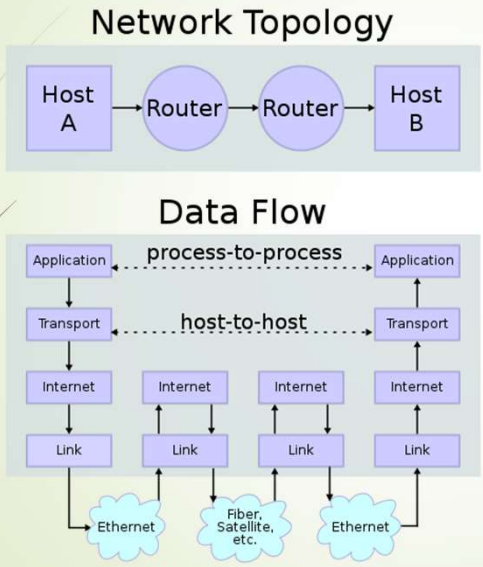
Routing

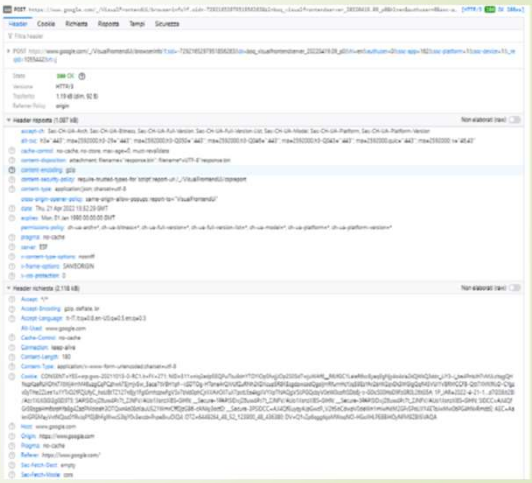
- Router indirizza il traffico da una sottorete ad un'altra
- Router ha diverse porte (interfacce)
- Diversi tipi di router
- Il router utilizza delle tabelle di indirizzamento che aggiorna scambiando informazioni sull'accessibilità della rete con i suoi vicini





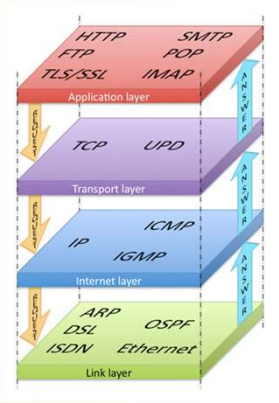
Internet ? Una torta a strati

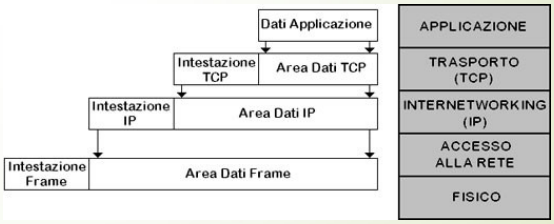




Ogni livello aggiunge un'header di suo specifico interesse.
Nel livello superiore le header di livello inferiore non hanno più significato.
Esempio di header per una pagina web non vedete traccia degli indirizzi IP …

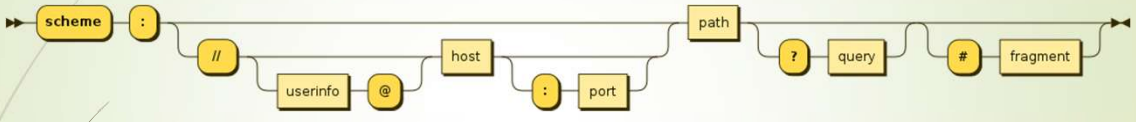
Ogni strato più protocolli

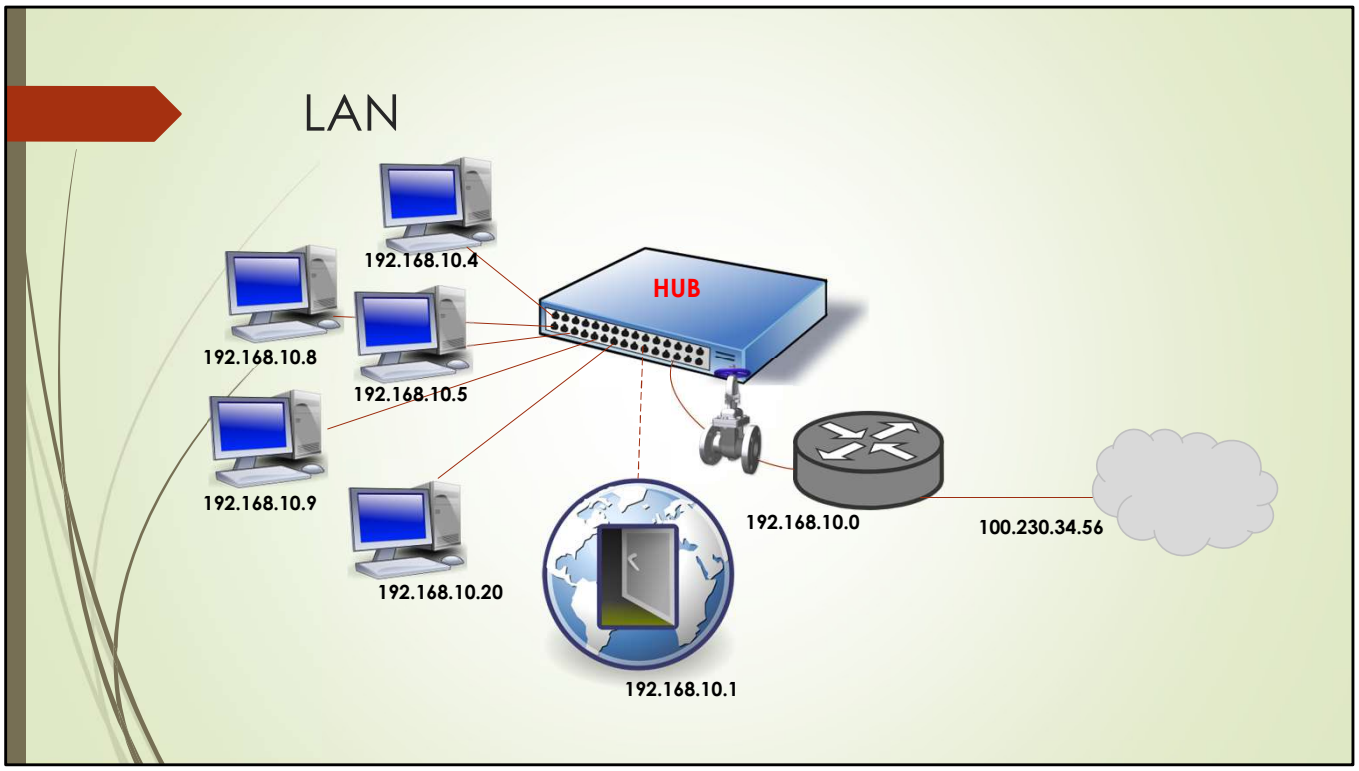




Suite_di_protocolli_Internet

URI (Uniform Resource Identifier)





Per la rete locale si usano in genere la classe A 10/8 o la classe B 192.168/16.
Il router provvede ad operare un NAT (Network Address Translaction) sull'indirizzo IP assegnato modificando l'header di pacchetto

https://it.wikipedia.org/wiki/Network_address_translation.

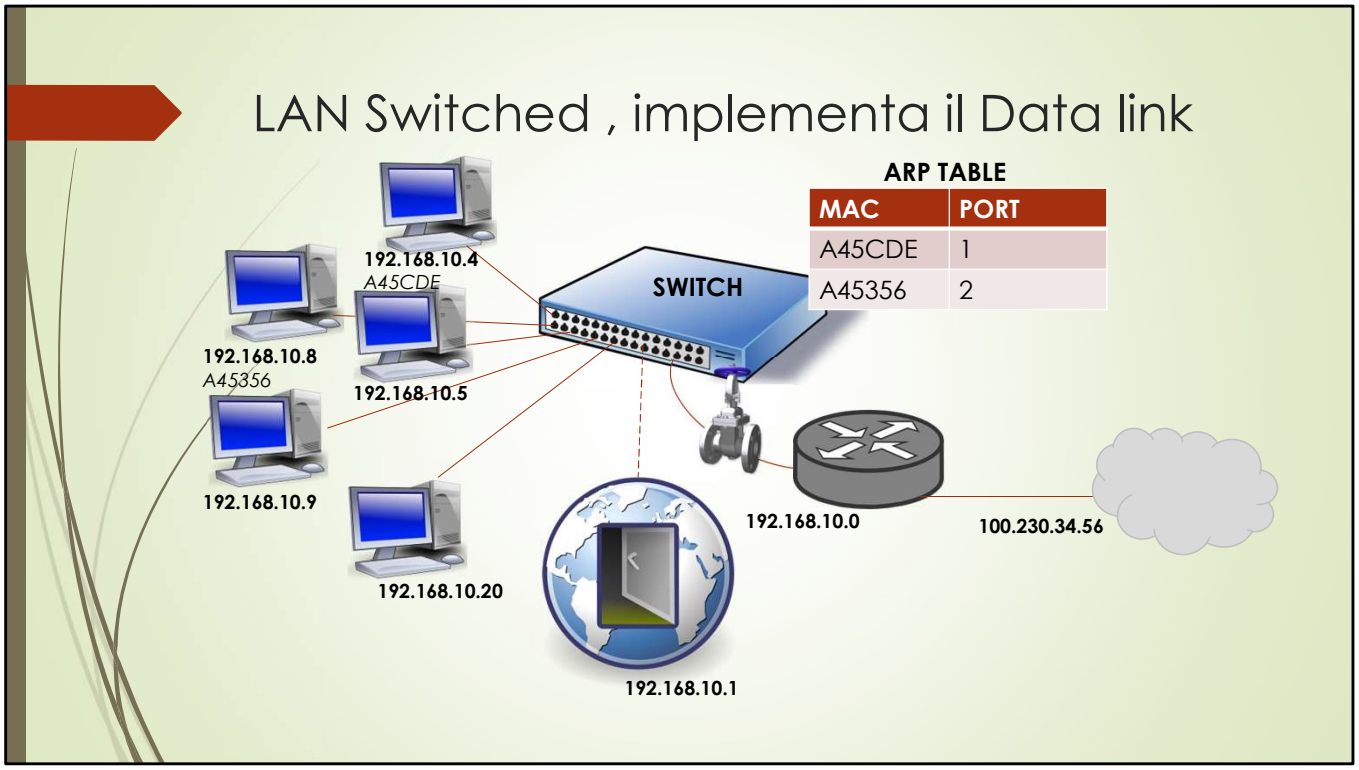
Gli indirizzi delle macchine possono essere assegnati in modo statico o dinamico, attraverso un DHCP server.

Tutto il traffico della LAN esce da un singolo IP.
Altri componenti della LAN possono essere

- Il DHCP server che assegna dinamicamente l'indirizzo IP alla singola macchina
- Il Proxy Server che gestisce il traffico di rete e gli utenti: accesso, autorizzazioni, banda usata, siti visitabili etc
- Firewall pe proteggere la rete interna

Nelle piccole LAN molte di queste funzioni vengono collassate nel router di accesso.

Il limiti dell'HUB sono che tutti i pacchetti ricevuti sulla rete vengono distribuiti su tutte le interfacce, ogni singolo host decide se il pacchetto è destinato a lui o meno, e quindi se usarlo o scartarlo.
Molto inefficiente ed insicuro.

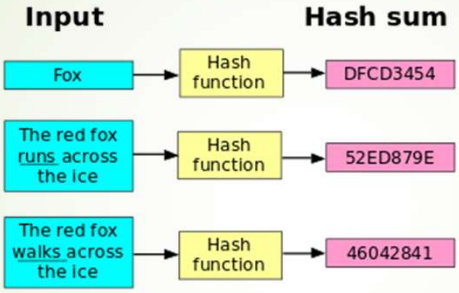


Lo switch si colloca a livello OSI 2 (Data Link). Implementa il protocollo **ARP** (Address Resolution Protocol).
Una volta che un dispositivo è collegato a uno switch, lo switch rileva il suo indirizzo MAC (Media Access Control), un codice inserito nella scheda di interfaccia di rete (NIC) del dispositivo che si collega a un cavo Ethernet che si collega allo switch.
Lo switch utilizza l'indirizzo MAC per identificare da quale dispositivo collegato vengono inviati i pacchetti in uscita e dove consegnare i pacchetti in entrata.
Quindi l'indirizzo MAC identifica il dispositivo fisico in contrapposizione all'indirizzo IP del livello di rete (Livello 3), che può essere assegnato dinamicamente a un dispositivo e cambiare nel tempo.
Quando un dispositivo invia un pacchetto a un altro dispositivo, entra nello switch e lo switch legge la sua intestazione per determinare cosa farne. Corrisponde all'indirizzo o agli indirizzi di destinazione e invia il pacchetto attravers
I Mac Address sono codice di 48 bit, 6 byte, assegnato in modo univoco dal produttore ad ogni scheda di rete, ethernet o wireless, prodotta. Sono progettati per essere globalmente unici e rappresentano quindi un singolo elemento della rete di appartenenza.
Le schede di rete

Un po di crittografia

- Hashing
- Crittografia simmetrica
- Crittografia asimmetrica
- Certificati digitali

Hashing



- https://it.wikipedia.org/wiki/Funzione_di_hash

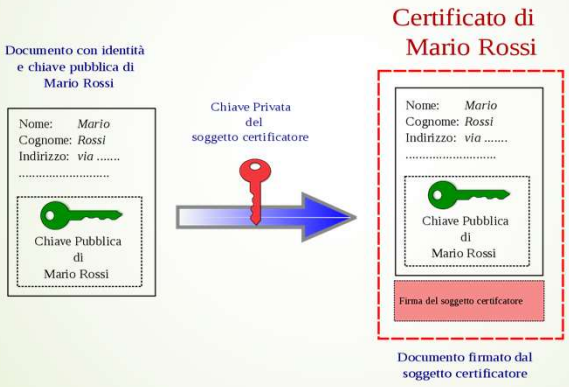
Crittografia simmetrica

https://it.wikipedia.org/wiki/Crittografia_simmetrica

Crittografia asimmetrica

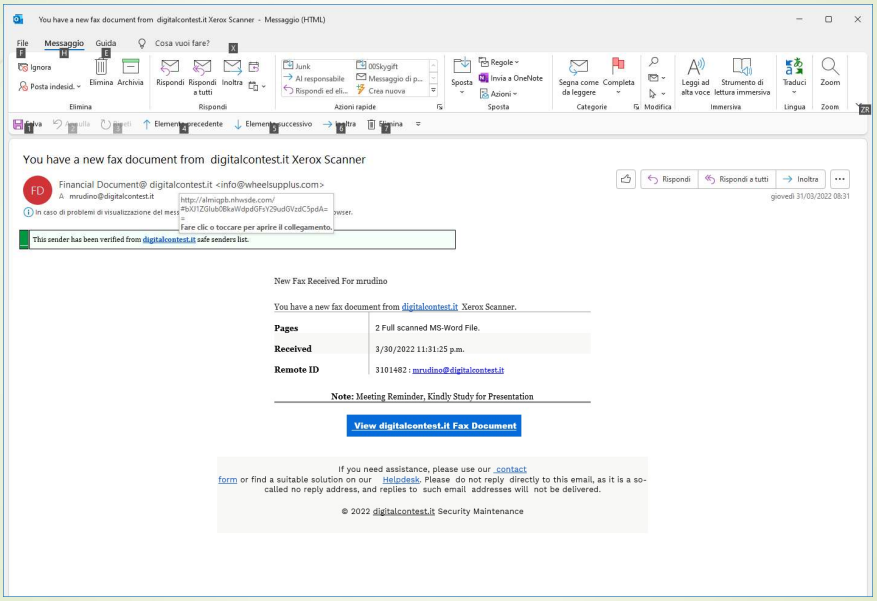
https://it.wikipedia.org/wiki/Crittografia_asimmetrica

Certificati digitali



https://it.wikipedia.org/wiki/Certificato_digitale

Phishing


You have a new fax document from digitalcontest.it Xerox Scanner - Messaggio (HTML)
You have a new fax document from digitalcontest.it Xerox Scanner
Financial Document@ digitalcontest.it <info@wheelsupplus.com>
This sender has been verified from digitalcontest.it safe senders list.
New Fax Received For mrudino
You have a new fax document from digitalcontest.it Xerox Scanner.
Pages
2 Full scanned MS-Word File.
Received
3/30/2022 11:31:25 p.m.
Remote ID
Note: Meeting Reminder, Kindly Study for Presentation
View digitalcontest.it Fax Document
If you need assistance, please use our contact form or find a suitable solution on our Helpdesk. Please do not reply directly to this email, as it is a so-called no reply address, and replies to such email addresses will not be delivered.
© 2022 digitalcontest.it Security Maintenance

Un attacco a goccia (teardrop) è un attacco DoS condotto prendendo di mira i codici di riassemblaggio della frammentazione TCP/IP. Questo attacco fa sì che i pacchetti frammentati si sovrappongano l'un l'altro sulla ricevuta dell'host; l'host tenta di ricostruirli durante il processo ma non riesce. Payload giganteschi vengono inviati alla macchina presa di mira, causando arresti anomali del sistema.
Prevenzione : usate software aggiornato

Man in the Middle

- **Session Hijacking (Dirottamento di sessione)**
  - https://pinkhatcode.com/2022/02/27/session-hijacking-tutorial-for-beginner-developers/
- **IP Spoofing**
- **Replay**
  - Si ripetono vecchi messaggi

Intercettazione

- Intercettazione passiva (WireShark)
  - Contromisure : canali sicuri (https, sftp, VPN), reti switched
- Intercettazione attiva (simulazione di EndPoint)
  - Autenticazione del peer (https)
- Reti WiFi con Access Point Open
  - evitare

Malware

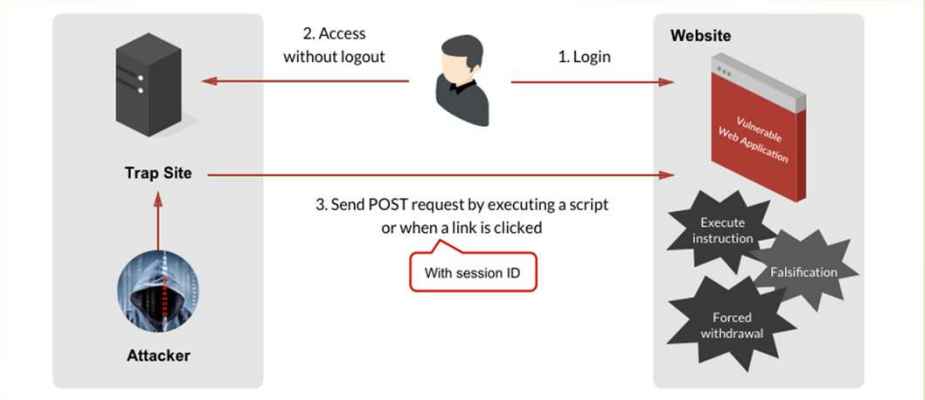
- Virus Macro
- Infector
- Boot virus
- Virus polimorfici
- Trojan (a differenza del virus non si replica)
- Mail worm
- Dropper
- Ramsonware
- Adware
- Spyware

Gestione password

- Lunghezza minima 8
- Numeri, caratteri maiuscoli, minuscoli, caratteri speciali
- Trasformate in password una vostra canzone preferita con trascodifica caratteri numeri
  - Alice guarda i gatti e i gatti guardano nel sole
    => 4g1g31ggn5!
- Validità massima password 3 mesi
- Gli utenti che non usano il sistema vanno disabilitati
- La password deve essere creata dall'utente, in contingenza gli va comunicata su un canale sicuro
- Usate sempre l'approccio una cosa che so ed una cosa che ho

i	1
a	4
e	3
s	5
h	8
o	0

Cross Site Request Forgery



Un attacco CSRF induce la vittima a fare clic su un URL che contiene una richiesta non autorizzata e malintenzionata per una particolare applicazione Web.
Il browser dell'utente invia la richiesta dannosa a un'applicazione Web mirata. La richiesta include anche eventuali credenziali relative al particolare sito web (es. cookie di sessione utente). Se l'utente è in una sessione attiva con un'applicazione Web di destinazione, l'applicazione considera questa nuova richiesta come una richiesta autorizzata inviata dall'utente.
Pertanto, l'attaccante riesce a sfruttare la **vulnerabilità CSRF dell'applicazione Web**.

Un attacco CSRF prende di mira le applicazioni Web che non riescono a distinguere tra richieste valide e richieste contraffatte controllate dall'autore dell'attacco. Esistono molti modi in cui un utente malintenzionato può provare a sfruttare la vulnerabilità CSRF.

Esempio, supponiamo che Roberto abbia un conto bancario online su mybank.com. Visita regolarmente questo sito per condurre transazioni con la sua amica Alice. Roberto non sa che mybank.com è vulnerabile agli attacchi CSRF.
Nel frattempo, un utente malintenzionato mira a trasferire 5.000 € dall'account di Roberto sfruttando questa vulnerabilità.
Per lanciare con successo questo attacco:

1. L'attaccante deve creare un URL di exploit.
2. L'attaccante deve anche indurre Roberto a fare clic sull'URL dell'exploit.
3. Roberto deve avere una sessione attiva con mybank.com.

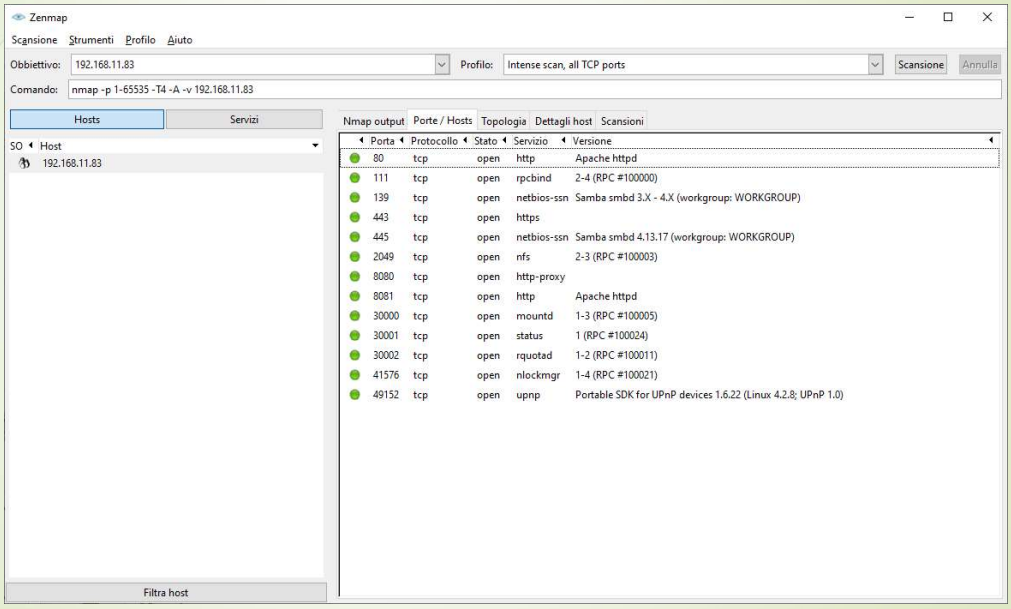
Cross Site Request Forgery - 2

- Mitigazione
  - Non utilizzare il metodo GET per richieste che comportano un cambiamento di stato, come ad esempio la modifica di dati. Controllare il campo di intestazione HTTP referer per vedere se la richiesta è stata generata da una pagina valida.
  - Verificare che il sistema sia esente da vulnerabilità di tipo cross-site scripting poiché molte delle difese CSRF possono essere evitate usando vulnerabilità di questo tipo.
  - Usare framework, librerie, moduli e in generale codice fidato che permettano allo sviluppatore di evitare l'introduzione di questa vulnerabilità.
  - Identificare quelle operazioni che possano risultare pericolose e quando un utente genera un'operazione di questo tipo inviare una richiesta addizionale di conferma all'utente, per esempio, la richiesta di una password, che deve essere verificata prima di eseguire l'operazione.
  - **Dal lato utente è buona abitudine eseguire sempre il logout da siti web sensibili prima di visitare altre pagine web.**

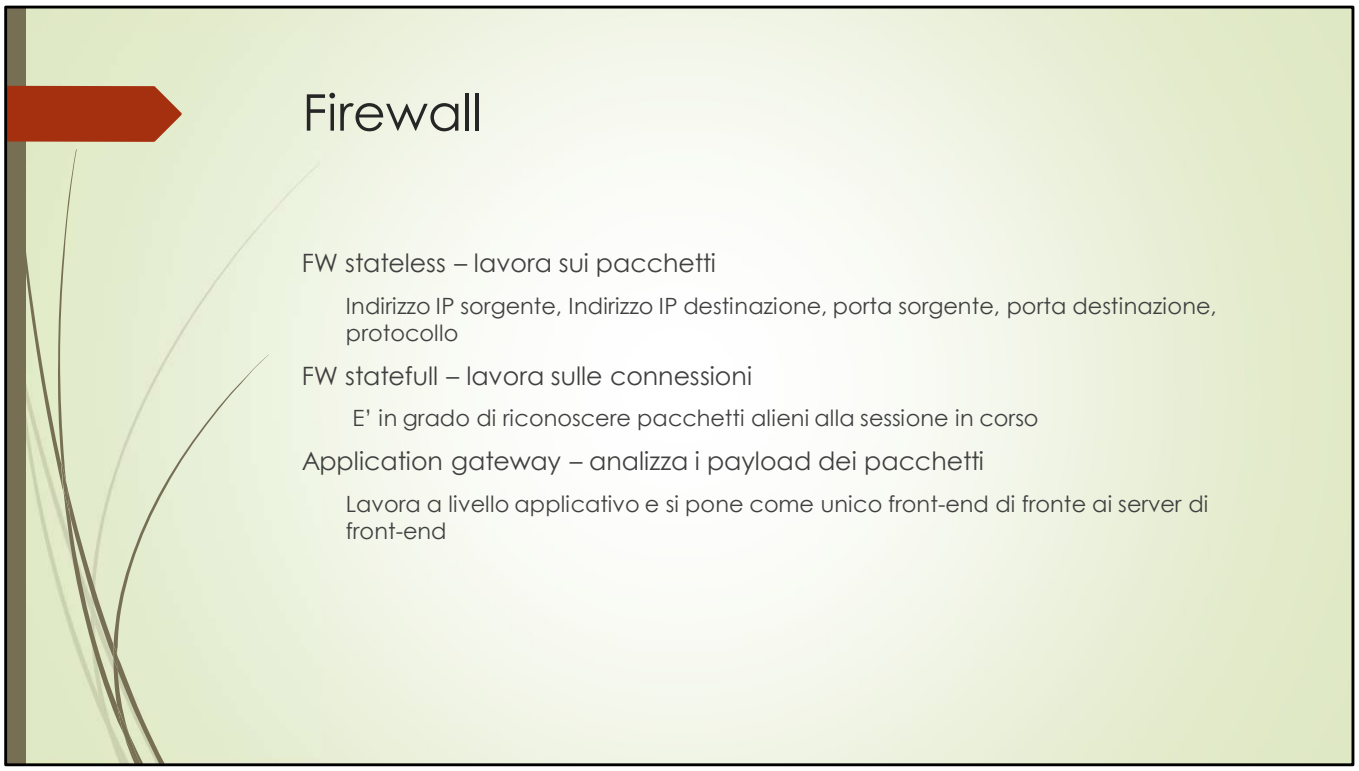
Indirizzo IP e porte

- Ad un indirizzo IP corrispondo diverse **porte** su cui rispondono dei servizi più o meno standard, come ci sono diversi negozi in un centro commerciale
- Le porte più usate sono
  - 80 http
  - 443 https
  - 20,21 FTP
  - 22 SSH
  - 23 Telnet
  - 25 SMTP
  - 161,162 SNMP
  - 143 IMAP
  - 110, (995) POP3 (over TLS)
  - …
- Elenco completo delle porte
  - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NMAP - Networking Mapping



Esempio loggato su https://corso.dcinfo.it/C_Security/Esempio scansione NMAP.txt, si riferisce ad un NAS (Network Attached Storage) all'interno di una rete locale



Packet filter firewall o stateless firewall
Un packet filter firewall o stateless firewall analizza ogni pacchetto che lo attraversa singolarmente, senza tenere conto dei pacchetti che lo hanno preceduto. In tale analisi vengono considerate solo alcune informazioni contenute nell'header del pacchetto, in particolare quelle appartenenti ai primi tre livelli del modello OSI più alcune del quarto. Le informazioni in questione sono l'indirizzo IP della sorgente, l'indirizzo IP della destinazione, la porta della sorgente, la porta della destinazione e il protocollo di trasporto. Su questi parametri vengono costruite le regole che formalizzano la policy del firewall e che stabiliscono quali pacchetti lasciar passare e quali bloccare. Questo tipo di filtraggio è semplice e leggero ma non garantisce un'elevata sicurezza. Infatti risulta vulnerabile ad attacchi di tipo IP spoofing in quanto non riesce a distinguere se un pacchetto appartenga o no ad una connessione attiva.

Stateful firewall o circuit-level gateway
Uno stateful firewall o circuit-level gateway svolge lo stesso tipo di filtraggio dei packet filter firewall e in più tiene traccia delle connessioni e del loro stato. In generale, rispetto ai packet filter firewall, offrono una maggiore sicurezza, un logging migliore e un controllo migliore sui protocolli applicativi che scelgono casualmente la porta di comunicazione (come FTP) ma sono più pesanti dal punto di vista delle performance.

Application firewall o proxy firewall o application gateway
Un application firewall o proxy firewall o application gateway opera fino al livello 7 del modello OSI filtrando tutto il traffico di una singola applicazione sulla base della conoscenza del suo protocollo. Questo tipo di firewall analizza i pacchetti nella sua interezza considerando anche il loro contenuto (payload) ed è quindi in grado di distinguere il traffico di un'applicazione indipendentemente dalla porta di comunicazione che questa utilizza. Un'altra caratteristica che lo distingue da un packet filter firewall e da uno stateful firewall è la capacità di spezzare la connessione tra un host della rete che protegge e un host della rete esterna. Infatti nelle comunicazioni svolge il ruolo di intermediario ed è quindi l'unico punto della rete che comunica con l'esterno, nascondendo così gli altri host che vi appartengono.

Esempio configurazione IP TABLE

IP TABLE firewall, Open Source in sistemi Linux

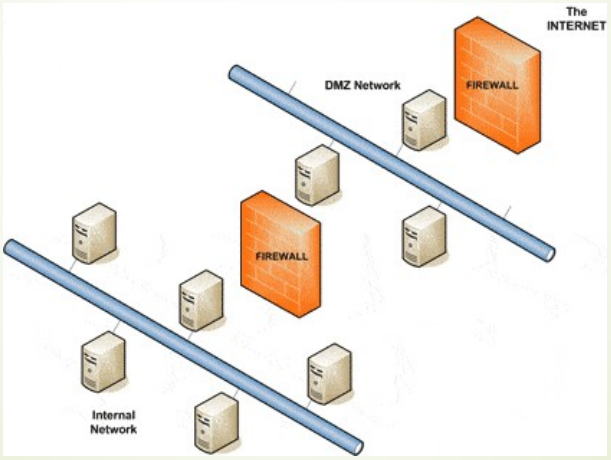
Accetto il traffico ssh e quello web dall'esterno, accetto il traffico dalla rete locale, butto via tutto il resto

- INPUT -p tcp --dport 22 ACCEPT
- INPUT -p tcp --dport 80 ACCEPT
- INPUT -p tcp --dport 443 ACCEPT
- INPUT -s 192.168.1.0/24 ACCEPT
- INPUT DROP

Per maggiori informazioni vedi ad esempio
https://wiki.archlinux.org/title/simple_stateful_firewall

Configurazione DMZ

De Militarized Zone



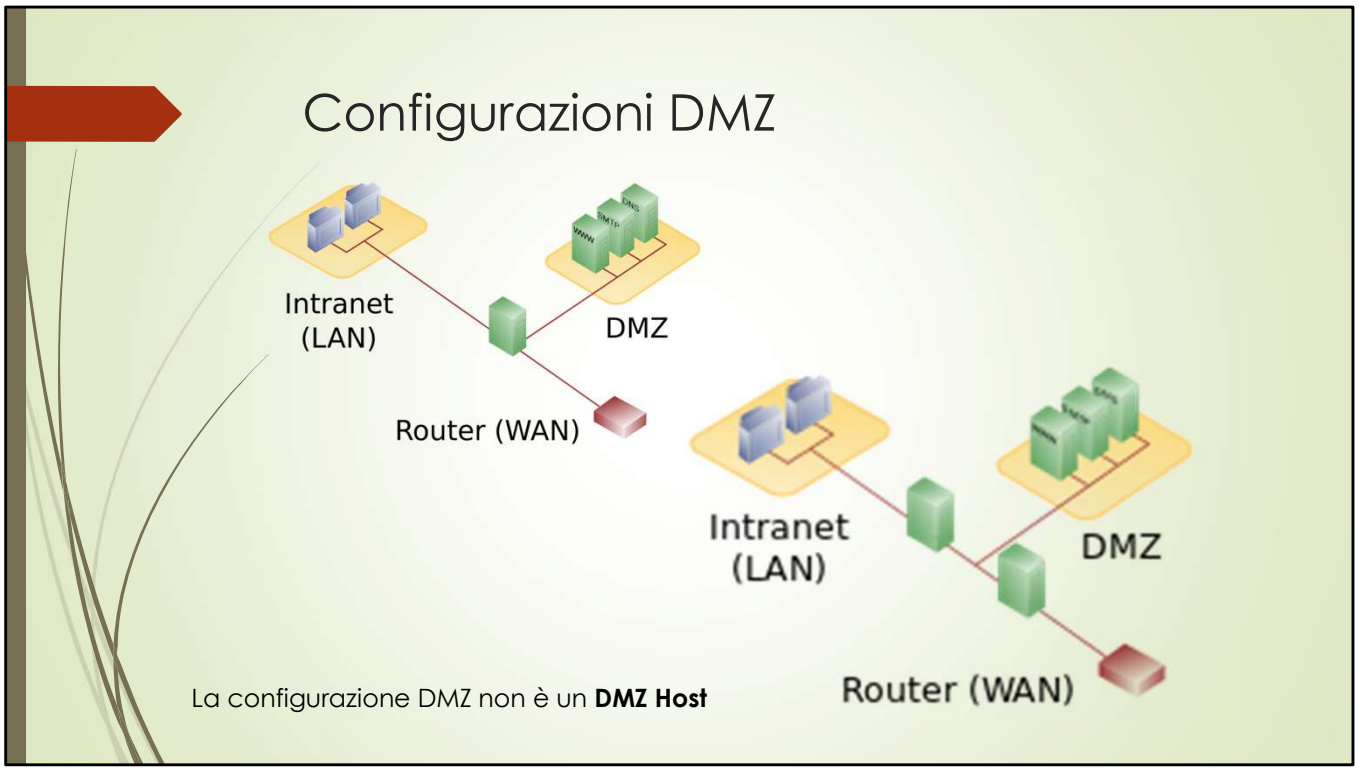
La DMZ è né sicura come la rete interna, né insicura come Internet pubblico.

Gli host più vulnerabili agli attacchi sono quelli che forniscono servizi agli utenti al di fuori della rete locale, come e-mail, Web e server DNS (Domain Name System). A causa del maggiore rischio di subire un attacco questi host, vengono inseriti in questa sottorete specifica per proteggere il resto della rete nel caso in cui qualcuno di essi venga compromesso.

Gli host nella DMZ possono avere solo una connettività limitata a host specifici nella rete interna, poiché il contenuto della DMZ non è sicuro come la rete interna.

Allo stesso modo, anche la comunicazione tra host nella DMZ e verso la rete esterna è limitata per rendere la DMZ più sicura di Internet e adatta a ospitare questi servizi speciali.
Ciò consente agli host nella DMZ di comunicare con la rete interna ed esterna, mentre un firewall intermedio controlla il traffico tra i server DMZ e i client di rete interni e un altro firewall eseguirà un certo livello di controllo per proteggere la DMZ dalla rete esterna .
Qualsiasi servizio fornito agli utenti sulla rete esterna può essere inserito nella DMZ. I più comuni di questi servizi sono:

- Server web
- Server di posta
- Server FTP
- Server VoIP



Firewall singolo
Diagramma di un tipico modello di rete a tre gambe che impiega una DMZ utilizzando un singolo firewall. Un singolo firewall con almeno 3 interfacce di rete può essere utilizzato per creare un'architettura di rete contenente una DMZ. La rete esterna è formata dall'ISP al firewall sulla prima interfaccia di rete, la rete interna è formata dalla seconda interfaccia di rete e la DMZ è formata dalla terza interfaccia di rete.
Il firewall diventa un singolo punto di errore per la rete e deve essere in grado di gestire tutto il traffico diretto alla DMZ e alla rete interna.
Doppio firewall
Diagramma di una tipica rete che utilizza DMZ utilizzando doppi firewall. L'approccio più sicuro. Il primo firewall (chiamato anche firewall "front-end") deve essere configurato per consentire solo il traffico destinato alla DMZ. Il secondo firewall (chiamato anche firewall "back-end")consente il traffico verso la DMZ solo dalla rete interna. Questa configurazione è considerata più sicura poiché due dispositivi dovrebbero essere compromessi. C'è ancora più protezione se i due firewall sono forniti da due fornitori diversi, perché rende meno probabile che entrambi i dispositivi soffrano delle stesse vulnerabilità di sicurezza. Uno degli svantaggi di questa architettura è che è più costoso, sia da acquistare che da gestire.

DMZ HOST
Semplici router SOHO permettono di definire un DMZ Host, ovvero un indirizzo IP su cui viene convogliato il traffico esterno. Questa non è una DMZ perché il server target non è isolato dalla LAN.

Gestire gli accessi alle risorse

- Utente appartiene a gruppo
  - Il gruppo rappresenta un insieme di utenti che hanno necessità simili di accesso alle risorse
- Le risorse hanno sempre un owner (utente/gruppo)
- I privilegi di accesso alle risorse
  - Read, Write, Execute (Traverse)

  sono dati sulla base della relazione tra l'owner e chi accede
  - Owner, Group, World
- Impostare sempre i diritti di accesso nel modo più restrittivo possibile
- Chroot è un altro strumento (https://linuxsecurity.com/features/using-chroot-securely)

Esempi di codice insicuro : file upload

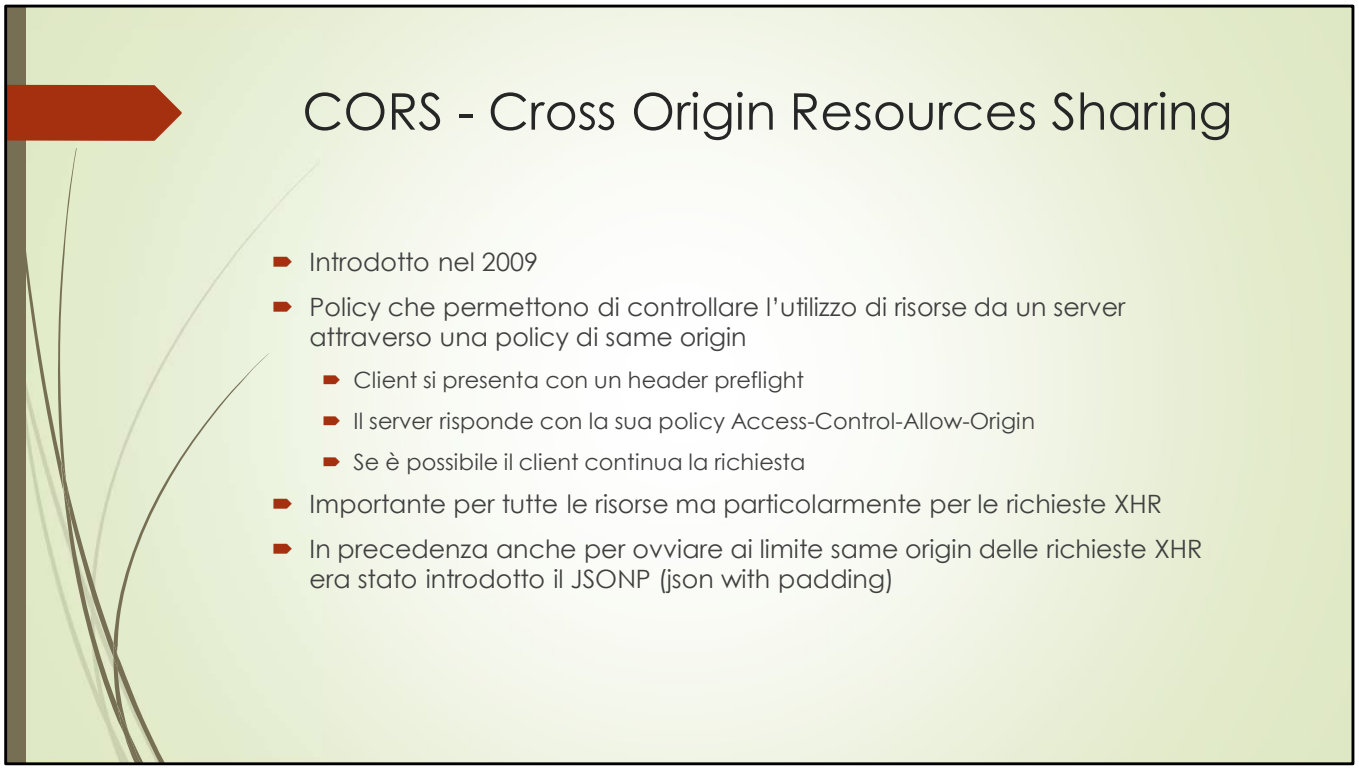
- Ogni file possiede un MIME Type
- I file multimediali contengono ei metadati che possono essere alterati con Ediftool
- Controllare il MIME Type di un file caricato è buona pratica … ma non sufficiente
- Bisogna controllare la coerenza dell'estensione con il MIME Type per evitare il MIME Type spoofing
- .. E cancellare ogni '.' presente nel nome file per evitare estensioni multiple

Un esempio di spoofing del MIME type

```
//The URL I am uploading to.
$uploadUrl = 'http://localhost/test/upload-script.php';
//Attempting to upload a PHP file.
$badFile = 'C:\wamp64\www\test\file.php';
 $ch = curl_init($uploadUrl);
 curl_setopt($ch, CURLOPT_POST, true);
 curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
//Set the MIME type of the PHP file to image/jpeg
$badFile = new CURLFile($badFile, 'image/jpeg');
$postFields = array( 'user_file' => $badFile, );
 curl_setopt($ch, CURLOPT_POSTFIELDS, $postFields);
$result = curl_exec($ch);
 echo $result;
```

Esempi di codice insicuro : XSS

- XSS (Cross Site Scipting) è una tecnica di iniezione di codice javascript dento le pagine di un utente
- XSS si presta a divesi tipi di attacchi, esempio
  - Session hijacking, basato sulla cattura dei cookies dell'utente
  - Keylogger
  - …
- Sempre sanificare l'input (php: htmlspecialchars)
- Sanificare l'output in JS



Esempio :
Accedendo a https://corso.dcinfo.it/C_CORS/json.html si visualizza una risposta jsonr elativa ad una request XHR dallo stesso dominio

Accedendo alla stesa pagina da un altro dominio https://collaudo.digitalcontest.it/corso/C_CORS/json.html la pagina viene bloccata per la configurazione dei CORS

La pagina https://collaudo.digitalcontest.it/corso/C_CORS/json_CORS.html invece invoca un php che imposta in mod permissivo le policy di risposta

header ("Access-Control-Allow-Origin:*");

Alternativa è l'utilizzo di **jsonp** (Json with padding) che trasforma la risposta in una chiamata a callback con i dati

SQL Injection

- Questo tipo di attacco sfrutta la possibilità di inserire nella get o nella post di accesso ad un sito delle parti di istruzioni SQL
- La vulnerabilità può permettere di
  - Loggarsi in modo fraudolento ad un sito
  - Enumerare il contenuto di un DB
  - Accedere alle tabelle
  - Modificare il contenuto delle tabelle
  - Cancellare tabelle del DB
- Contromisure
  - Utilizzare mysql_real_escape_string per sanificare l'input
  - Utilizzare query con Prepared Statement
  - Evitare *raw sql query*
  - Definire gli utenti in base al progetto e con i minimi diritti di accesso necessari (?DROP TABLE ?)

Vedere esempio su https://corso.dcinfo.it/C_SQLInjection/

CVE – CWE

- **C**ommon **V**ulnerabilities and **E**xposures
  - Vecchio sito in https://cve.mitre.org/ in corso di migrazione su www.cve.org
- Espone le vulnerabilità conosciute dei software
- Da consultare prima di utilizzare un software

- Common Weakness Enumeration (cwe.mitre.org)
  - Da conoscere la lista delle TOP25 vulnerabilitò che si possono introdurre nel software
  - Aggiornato annualmente

CWE TOP25 1-12

[1]	CWE-787	Out-of-bounds Write
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[3]	CWE-125	Out-of-bounds Read
[4]	CWE-20	Improper Input Validation
[5]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[7]	CWE-416	Use After Free
[8]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[9]	CWE-352	Cross-Site Request Forgery (CSRF)
[10]	CWE-434	Unrestricted Upload of File with Dangerous Type
[11]	CWE-306	Missing Authentication for Critical Function
[12]	CWE-190	Integer Overflow or Wraparound

CWE TOP25 13-25

[13]	CWE-502	Deserialization of Untrusted Data
[14]	CWE-287	Improper Authentication
[15]	CWE-476	NULL Pointer Dereference
[16]	CWE-798	Use of Hard-coded Credentials
[17]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
[18]	CWE-862	Missing Authorization
[19]	CWE-276	Incorrect Default Permissions
[20]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
[21]	CWE-522	Insufficiently Protected Credentials
[22]	CWE-732	Incorrect Permission Assignment for Critical Resource
[23]	CWE-611	Improper Restriction of XML External Entity Reference
[24]	CWE-918	Server-Side Request Forgery (SSRF) (http://capec.mitre.org/data/definitions/664.html)
[25]	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')

ISO27001 – SoA (Statement of Applicability)

Documento di sintesi per il controllo della sicurezza informatica

- 14 aree di controllo
- 114 obiettivi di controllo

ISO/IEC 27001:2013 Annex A controls
5 Security Policies
6 Organisation of information security
7 Human resource security
8 Asset management
9 Access control
11 Physical and environmental security
12 Operations security
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance

Viene presentato a lezione un esempio reale di SoA

KPI (Key Perfomance Indicator)

- **Maximum acceptable outage (MAO):** tempo di interruzione tale da rendere l'erogazione del prodotto o del servizio inaccettabile.
- **Minimum business continuity objective (MBCO):** livello minimo di erogazione di servizi e/o prodotti durante l'interruzione tale da consentire all'organizzazione di raggiungere comunque i suoi obiettivi aziendali.
- **Recovery Point Objective** (**RPO)** rappresenta la quantità di dati prodotti ma non ancora sincronizzati, in caso di incidente o disastro, su un archivio (storage o file) di sicurezza. Indica quindi il massimo tempo che deve intercorrere tra la generazione di un'informazione e la sua *messa in sicurezza* (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema potrebbe perdere a causa di guasto improvviso.
- Il **Recovery Time Objective** (**RTO**) è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo. È in pratica la massima durata, prevista o tollerata, del *downtime* occorso.
- **Recovery Point Actual** e **Recovery Time Actual** misurano le stesse cose nel sistema in esercizio

BIA (Business Impact Analisys)

- I servizi vengono analizzati in termini di
  - impatto finanziario;
  - impatto reputazionale;
  - impatto legale/contrattuale;
  - impatto sugli obiettivi di business.
- Per ogni servizio vengono definiti i KPI obiettivo
- I servizi vengono pesati rispetto alla loro criticità determinata dall'impatto precedente
- Si calcola per i servizi i KPI actual
- Si determinano i piani di intervento per avvicinare i KPI actual ai KPI obiettivo