# Sistemi SCADA

## Quale è il significato dell'acronimo SCADA?

* Supervisory Control and Data Acquisition
* Software Computation and Data Aggregation
* Superior Check and Data Addition

## Per cosa sono utilizzati i sistemi SCADA?

* Supervisione, controllo e acquisizione dati con il fine di gestire un processo
* Supervisione e controllo di un processo
* Supervisione e acquisizione dati di un processo
* Controllo di un sistema di processi

## Per cosa sta l'acronimo PLC e a cosa servono?

* "Programmable Logic Controller", computer programmabili utilizzati per il sistema di acquisizione
* "Procedural Logic Components", componenti hardware utilizzate nel sistema di trasmissione dati
* "Programmable Linked Computers", rete di strumenti utilizzata per il sistema di elaborazione

## Quali componenti fanno parte di un’architettura "standard" di un sistema SCADA?

* Sistema di elaborazione dati, sistema di trasmissione dati e sistema di acquisizione
* Sistema di controllo, elaboratore centrale e centro di connessioni
* Elaboratori periferici, sistema di trasmissione dati e centro di acquisizione
* Elaboratore centrale, sistema di acquisizione dati e centro di connessioni

## Da quanti e quali blocchi è composto l'elaboratore dei dati?

* 3: blocco gestore dati, blocco per la disponibilità dati e blocco per l'elaborazione
* 3: blocco acquisitore dati, blocco per l'elaborazione e blocco per mantenimento dato
* 2: blocco gestore dati e blocco per l'elaborazione

## Quali componenti deve mettere in comunicazione il sistema di trasmissione dati?

* Sistema di elaborazione <-> sistema di gestione dati/Sistema di elaborazione <-> sistema di acquisizione dati/Dispositivi di interazione <-> sistema di acquisizione dati/Processo <-> dispositivi di interazione
* Sistema di elaborazione <-> sistema di interazione/Processo <-> sistema di elaborazione/Sistema di acquisizione dati <-> sistema di gestione dati
* Sistema di gestione dati <-> processo/Sistema di elaborazione <-> processo/Sistema di acquisizione dati <-> dispositivi di interazione/Dispositivi di interazione <-> sistema di elaborazione

## Cosa è un servizio SCADA

* Un servizio di controllo tramite sistema SCADA. Il fornitore del servizio deve occuparsi del controllo del processo
* Un servizio di controllo tramite sistema SCADA. Il fruitore del servizio deve occuparsi del controllo del processo
* Un sistema di controllo tramite sistema SCADA. Fruitore e fornitore del servizio sono equamente coinvolti nel controllo del processo

# Attacchi Informatici

## Qual è il significato dell'acronimo DoS?

* Destruction of Service
* Duplication of Service
* Distribution of Service
* Denial of Service

## Quali sono le conseguenze di un attacco Dos/DDos?

* Installazione di software dannoso, ad insaputa della vittima
* Esaurimento delle risorse del sistema, impedendo l'esecuzione del servizio da erogare
* Intercettazione del canale di comunicazione tra server e client
* Ripetizione di comandi ricevuti, provocando danni al server vittima

## Cosa si indica con il termine malware?

* Programmi in grado di registrare tutto ciò che un utente esegue sul sistema, rendendo così possibile il furto di dati sensibili
* Software che consentono un accesso non autorizzato al sistema su cui sono in esecuzione
* Attacchi che hanno origine dalle pubblicità delle pagine web
* Qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer

## Qual è la differenza tra virus e malware?

* Con il termine virus si indica un software che infetta dei file in modo da fare copie di sé stesso, mentre con malware si indica la categoria più generale di software dannosi.
* Sono entrambi termini utilizzati indifferentemente per indicare un software che infetta dei file in modo da fare copie di sé stesso
* Con malware si indica un software che infetta dei file in modo da fare copie di sé stesso, mentre con virus si indica la categoria più generale di software dannosi.

## Cosa è un worm?

* È un pacchetto software che, modificando il sistema operativo del computer, permette l'occultamento in modo tale da nascondere le proprie tracce
* È una particolare categoria di malware in grado di auto replicarsi, sfruttando su una rete per infettare altri computer
* È un programma malevolo che falsa la sua vera identità per sembrare utile o interessante per persuadere la vittima ad installarlo.
* È un software che infetta dei file in modo da fare copie di sé stesso, integrandosi in qualche codice eseguibile del sistema vittima

## Come è effettuato un attacco replay?

* Tramite l'intercettazione e la successiva ripetizione di una trasmissione di dati valida all'interno di un canale di comunicazione
* Tramite l'intercettazione di una trasmissione di dati valida all'interno di un canale di comunicazione
* Tramite la decrittazione di una trasmissione di dati valida all'interno di un canale di comunicazione

## Quali sono le dinamiche di un attacco Man in the Middle?

* L'attaccante si intromette di un canale di comunicazione tra due vittime, intercettando la trasmissione dati e, se necessario, modificandola
* L'attaccante si finge fruitore di un servizio, rispondendo in maniera non autorizzata alle richieste effettuate dalla vittima
* L'attaccante, tramite l'ausilio di macchine controllate da lui, impedisce l'erogazione di un servizio, attaccando i sistemi della vittima

## Cosa si indica con il termine "phishing"

* Una tecnica di ingegneria sociale, con cui si tenta di acquisire dati sensibili, attraverso l'utilizzo fraudolento di una e-mail o un sito web
* Un attacco mirato a reindirizzare il traffico di un sito web ad un altro sito web
* Un attacco con cui si intercetta una comunicazione della vittima per poi riutilizzarla in maniera dannosa, senza decrittarne il contenuto
* Una tecnica di ingegneria, con cui si tenta di modificare i dati di un utente, intercettando il canale di comunicazione su cui sono trasmessi i dati

## Qual è la differenza tra un attacco replay ed un attacco MitM?

* Un attacco replay può avvenire anche in modo asincrono quando la comunicazione è ormai terminata, mentre il MitM avviene in tempo reale
* Un attacco MitM può avvenire anche in modo asincrono quando la comunicazione è ormai terminata, mentre quello replay avviene in tempo reale
* Nessuna, possono avvenire entrambi solo in tempo reale
* Nessuna, possono avvenire entrambi sia in tempo reale che in modo asincrono

# Sistemi di difesa

## Che cosa è un IDS (Intrusion Detection System)?

* Un dispositivo software o hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali
* È un componente di difesa perimetrale di una rete informatica che blocca gli accessi non autorizzati.
* Una tecnica di difesa informatica che permette di prevenire attacchi da parte di entità non autorizzate

## Cosa è un IPS (Intrusion Prevention System)? Per cosa si differenzia da un IDS?

* Sono dei componenti software attivi utilizzati per la sicurezza informatica. Come gli IDS, controllano il traffico e le attività di sistema, ma a differenza loro sono posizionati inline e sono abilitati a prevenire e bloccare le intrusioni identificate
* Sono dei componenti software passivi utilizzati per la sicurezza informatica. Controllano il traffico e le attività di sistema, ma non sono abilitati a prevenire e bloccare le intrusioni identificate
* Sono dei componenti hardware utilizzati per la sicurezza informatica come supporto agli IDS. Entrambi i sistemi monitorano il traffico di rete, senza effettuare azioni preventive

## Qual è la differenza tra un IDS e un firewall?

* Un firewall definisce una serie di regole che un pacchetto deve rispettare per transitare nella rete locale, un IDS ne controlla solo lo stato, confrontandolo con situazioni pericolose già successe o definite dall'amministratore della rete
* Un firewall controlla il traffico di rete, avvisando l'amministratore in caso di pacchetti anomali, mentre un IDS blocca tutti i pacchetti che ritiene dannosi
* Il firewall può essere posizionato solo in un router, mentre l'IDS può essere implementato su qualsiasi nodo della rete
* Un firewall riesce ad individuare un attacco anche se effettuato all'interno di una rete locale, mentre un IDS solamente se l'attacco proviene dall'esterno

# Minacce del mondo SCADA

## Che tipo di attacco è Stuxnet?

* Worm
* Virus
* DoS
* Man in the Middle

## Quale fu il primo impianto SCADA attaccato da Stuxnet? Quali componenti furono prese di mira?

* Un impianto nucleare, furono compromessi i PLC responsabili del controllo delle centrifughe per il trattamento di uranio
* Un impianto di distribuzione di gas, furono compromessi i dispositivi di controllo presenti nei nodi di scambio
* Un impianto di produzione di armi, furono compromessi i sistemi per il controllo qualità dei materiali
* Un impianto energetico, furono compromessi i PLC utilizzati per la gestione della distribuzione elettrica

## Quante furono le vulnerabilità sfruttare da Stuxnet per riuscire nell'attacco?

* 4, tutte allo zero-day
* 5, di cui 2 allo zero-day
* 3, di cui 1 allo zero-day e 1 conosciuta, ma non patchata
* 4, di cui 2 allo zero-day e 2 conosciute, ma non patchate

## Che tipo di attacco è Dragonfly?

* Una combinazione di attacchi phishing, malware e watering hole
* Una combinazione di attacchi whaling e worm
* Una combinazione di attacchi Dos e MitM
* Una combinazione di attacchi replay, shadow server e virus

## Quali tecnica è utilizzata per dar via all'attacco?

* Spear phisnig, inviando file .pdf corrotti alle vittime
* MitM, dirottando tutto il traffico su di un shadow server
* infetto DoS, sovraccaricando l íntero sistema da colpire
* Replay, con cui si colpisce il software HMI utilizzato per il controllo da remoto