

```
root@hacklab:~/parte-02/lezione-19
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE II

LEZIONE 19

OT / ICS / SCADA Security

Sicurezza dei sistemi industriali e delle infrastrutture critiche, dove la safety viene prima di tutto.

docente **Vincenzo Calabro** fase Specializzazione: OT / ICS / SCADA

```
root@hacklab:~/lezione-19/agenda $
```

LEZIONE 19 / AGENDA

In questa lezione

// PERCORSO

- > Modello di Purdue e componenti
- > Protocolli industriali
- > Differenze IT vs OT
- > Lezione di Stuxnet
- > Segmentazione e monitoraggio

metodo obiettivi -> teoria -> strumenti -> laboratorio -> caso di studio -> etica -> verifica

```
root@hacklab:~/lezione-19/obiettivi $
```

LEZIONE 19 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – architetture e vincoli industriali
- > Applicare – recon e protocolli ICS in ambiente simulato
- > Analizzare – i rischi per la safety e la disponibilit 
- > Valutare – contromisure e segmentazione
- > Creare – un piano di hardening OT

```
root@hacklab:~/lezione-19/inquadramento $
```

LEZIONE 19 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Nei sistemi industriali la sicurezza fisica e la continuità del processo vengono prima di tutto. Vediamo protocolli, vincoli e un approccio offensivo prudente dove un errore ha conseguenze reali.

// PERCHE' CONTA

Sicurezza dei sistemi industriali e delle infrastrutture critiche, dove la safety viene prima di tutto.

```
root@hacklab:~/lezione-19/mappa-insieme $
```

LEZIONE 19 / MAPPA // INSIEME

Mappa d'insieme del modulo

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA

FONDAMENTI

- 01 Architettura OT e modello di Purdue
- 02 Protocolli industriali e debolezze
- 03 Differenze tra IT e OT
- 04 Stuxnet e infrastrutture critiche
- 05 Segmentazione e IEC 62443

APPROFONDIMENTI

- 06 Componenti di un sistema di controllo
- 07 Debolezze dei protocolli OT
- 08 Safety, disponibilit  e legacy
- 09 Zone, conduit e diodi dati
- 10 Monitoraggio passivo e anomalie

```
root@hacklab:~/lezione-19/mappa-1 $
```

LEZIONE 19 / MAPPA // FONDAMENTI

Mappa dei concetti – Fondamenti

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA



```
root@hacklab:~/lezione-19/concetto-1 $
```

LEZIONE 19 / CONCETTO 1/10

[Difesa]

Architettura OT e modello di Purdue

// SPIEGAZIONE

Il modello di Purdue stratifica gli ambienti industriali dai processi fisici alla rete IT. Componenti come PLC, RTU, HMI, SCADA e DCS controllano e supervisionano i processi: non si proteggono senza conoscerne ruolo e livello.

// ESEMPIO

> Un PLC al livello 1 comanda attuatori fisici; l'HMI al livello 2 lo supervisiona.

```
root@hacklab:~/lezione-19/concetto-2 $
```

LEZIONE 19 / CONCETTO 2/10

[Attacco/tecnica]

Protocolli industriali e debolezze

// SPIEGAZIONE

Protocolli come Modbus, DNP3, S7 e OPC nascono per affidabilità e tempo reale, non per sicurezza: spesso privi di autenticazione e cifratura. Chi raggiunge la rete OT può inviare comandi legittimi ai dispositivi.

// ESEMPIO

> Un comando Modbus write non autenticato cambia lo stato di un'uscita del PLC.

```
root@hacklab:~/lezione-19/concetto-3 $
```

LEZIONE 19 / CONCETTO 3/10

[Attacco/tecnica]

Differenze tra IT e OT

// SPIEGAZIONE

In IT contano riservatezza e integrità; in OT vengono prima safety e disponibilità: un sistema non si può spegnere o aggiornare a piacere. Sistemi legacy decennali e vincoli di continuità impongono un approccio prudente e spesso passivo.

// ESEMPIO

> Non si riavvia un PLC di linea in orario di produzione solo per applicare una patch.

```
root@hacklab:~/lezione-19/concetto-4 $
```

LEZIONE 19 / CONCETTO 4/10

[Attacco/tecnica]

Stuxnet e infrastrutture critiche

// SPIEGAZIONE

Stuxnet dimostra che il software può causare danni fisici, sabotando centrifughe mentre mostrava valori normali agli operatori. Da allora le infrastrutture critiche sono un bersaglio strategico con impatti sul mondo reale.

// ESEMPIO

> Stuxnet alterava la velocità delle centrifughe falsificando le letture mostrate agli operatori.

```
root@hacklab:~/lezione-19/concetto-5 $
```

LEZIONE 19 / CONCETTO 5/10

[Difesa]

Segmentazione e IEC 62443

// SPIEGAZIONE

La difesa OT punta a separare: zone e conduit secondo IEC 62443, con flussi controllati tra livelli. I diodi dati impongono comunicazione unidirezionale, dall'OT verso l'IT, impedendo comandi di ritorno verso il processo.

// ESEMPIO

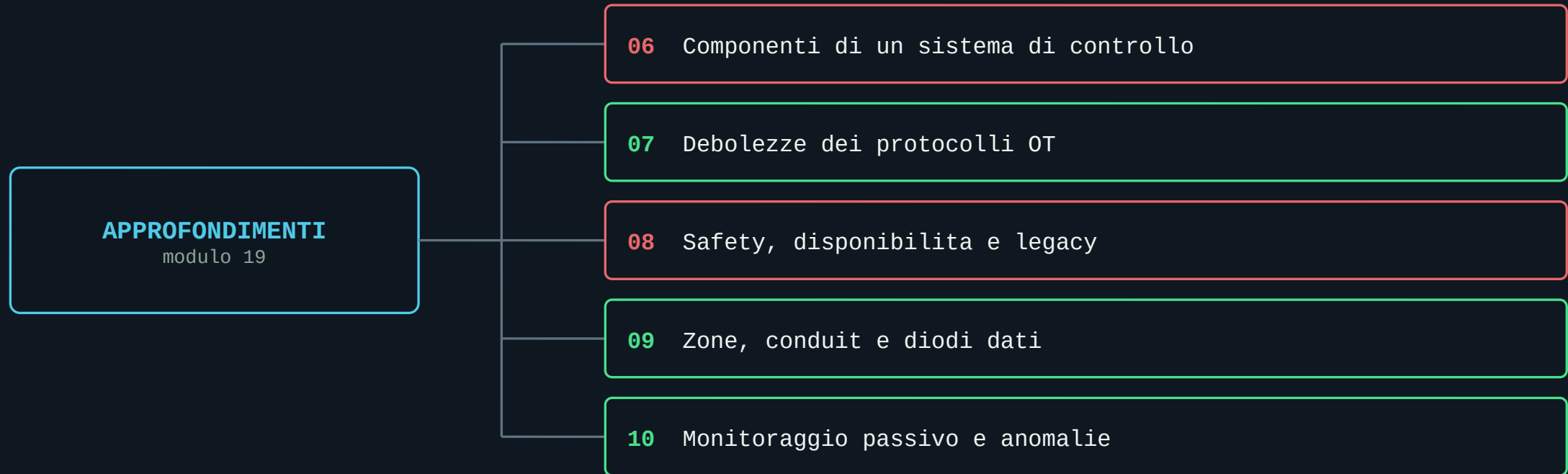
> Un diodo dati lascia uscire la telemetria ma impedisce qualsiasi comando verso i PLC.

```
root@hacklab:~/lezione-19/mappa-2 $
```

LEZIONE 19 / MAPPA // APPROFONDIMENTI

Mappa dei concetti – Approfondimenti

■ Attacco/tecnica ■ Difesa ■ Norme & metodo ■ IA



```
root@hacklab:~/lezione-19/concetto-6 $
```

LEZIONE 19 / CONCETTO 6/10

[Attacco/tecnica]

Componenti di un sistema di controllo

// SPIEGAZIONE

PLC e RTU eseguono la logica sul campo, l'HMI e l'interfaccia dell'operatore, SCADA supervisiona impianti distribuiti e il DCS controlla processi continui in un sito. Ogni componente ha esposizioni e criticita proprie.

// ESEMPIO

> Compromettere l'HMI permette di falsificare cio che l'operatore vede e comanda.

```
root@hacklab:~/lezione-19/concetto-7 $
```

LEZIONE 19 / CONCETTO 7/10

[Difesa]

Debolezze dei protocolli OT

// SPIEGAZIONE

Questi protocolli assumono una rete fidata: senza autenticazione, un messaggio ben formato viene eseguito. La difesa raramente può cifrarli sui dispositivi legacy, quindi punta su segmentazione e monitoraggio passivo del traffico.

// ESEMPIO

> Il monitoraggio passivo rileva un comando S7 anomalo verso un PLC fuori sequenza.

```
root@hacklab:~/lezione-19/concetto-8 $
```

LEZIONE 19 / CONCETTO 8/10

[Attacco/tecnica]

Safety, disponibilit  e legacy

// SPIEGAZIONE

In OT un test invasivo pu  mettere a rischio persone e impianti: la priorit    non interrompere ne destabilizzare. Si privilegiano tecniche passive, finestre concordate e repliche di laboratorio dei sistemi legacy.

// ESEMPIO

> La scansione attiva di un PLC fragile si prova prima su un gemello di laboratorio.

```
root@hacklab:~/lezione-19/concetto-9 $
```

LEZIONE 19 / CONCETTO 9/10

[Difesa]

Zone, conduit e diodi dati

// SPIEGAZIONE

IEC 62443 organizza l'impianto in zone con requisiti omogenei e conduit che ne regolano le comunicazioni. I diodi dati garantiscono fisicamente l'unidirezionalita, elemento chiave per esporre dati senza aprire vie di comando.

// ESEMPIO

> La zona di processo comunica con l'IT solo tramite un conduit monitorato e un diodo dati.

```
root@hacklab:~/lezione-19/concetto-10 $
```

LEZIONE 19 / CONCETTO 10/10

[Difesa]

Monitoraggio passivo e anomalie

// SPIEGAZIONE

Dove non si può intervenire attivamente si osserva: il monitoraggio passivo del traffico OT apprende il comportamento normale e segnala le deviazioni. In reti stabili e ripetitive come quelle industriali l'anomaly detection è particolarmente efficace.

// ESEMPIO

> Un nuovo dispositivo che parla Modbus sulla rete OT fa subito scattare un'anomalia.

```
root@hacklab:~/lezione-19/strumenti $
```

LEZIONE 19 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Nmap (script ICS)

Wireshark (dissettori ICS)

simulatori PLC/Modbus

Shodan

// NOTA OPERATIVA

> Ogni strumento si usa in ambiente virtualizzato e isolato, solo su bersagli di proprietà o autorizzati. Output e artefatti vanno protetti e, a fine ingaggio, gestiti o distrutti.

```
root@hacklab:~/lezione-19/lab-1 $
```

LEZIONE 19 / LABORATORIO 1

Laboratorio 1

\$ Modbus in simulatore (impatto di un comando)

// PROCEDURA

[1] Interroga e manipola un dispositivo Modbus in simulatore osservando l'impatto

[!] Verifica: Perché un comando legittimo può essere pericoloso?

```
root@hacklab:~/lezione-19/lab-2 $
```

LEZIONE 19 / LABORATORIO 2

Laboratorio 2

\$ Segmentazione OT (zone e conduit)

// PROCEDURA

[1] Progetta una segmentazione a zone e conduit per una rete industriale

[!] Verifica: Come si isola l'OT dall'IT senza bloccare i processi?

```
root@hacklab:~/lezione-19/caso-di-studio $
```

LEZIONE 19 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Stuxnet (2010): attacco a SCADA/ICS, con implicazioni per la safety e la supply chain.

// ANALISI RICHIESTA

- > Ricostruisci la dinamica dei fatti con metodo e tracciabilità
- > Individua errori, cause radice e punti di decisione critici
- > Proponi contromisure, controlli e lezioni apprese

```
root@hacklab:~/lezione-19/etica $
```

LEZIONE 19 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] I test su OT reali possono rischiare la safety e vite umane: solo simulatori o autorizzazione formale rigorosa.

```
root@hacklab:~/lezione-19/ricapitolazione $
```

LEZIONE 19 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Architetture e vincoli industriali
- > Recon e protocolli ICS in ambiente simulato
- > I rischi per la safety e la disponibilit 
- > Contromisure e segmentazione
- > Un piano di hardening OT

```
root@hacklab:~/lezione-19/verifica $
```

LEZIONE 19 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Perché un comando legittimo può essere pericoloso in OT?
- ? Come si isola l'OT dall'IT senza bloccare i processi?
- ? Perché la safety viene prima della sicurezza informatica?

// VALUTAZIONE

Relazione di valutazione del rischio OT con piano di hardening.

// LETTURE

NIST SP 800-82; MITRE ATT&CK for ICS; IEC 62443.

lezione 19 completata

\$ next

OT / ICS / SCADA Security

[!] Le competenze di questa lezione si impiegano esclusivamente in contesti legali, autorizzati e deontologicamente corretti, entro lo scope e con autorizzazione scritta.

root@hacklab:~# _

```
root@hacklab:~/contatti $
```

CONTATTI / RISORSE

Restiamo in contatto



Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.