

```
root@hacklab:~/parte-01/lezione-02
```

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 02

Scanning, Enumeration e Vulnerability Assessment

Dalla mappatura alla scoperta e classificazione delle vulnerabilità.

docente **Vincenzo Calabro** fase Fase 2: Scanning & Enumeration; input al Vulnerability Assessment

```
root@hacklab:~/lezione-02/agenda $
```

LEZIONE 02 / AGENDA

In questa lezione

// PERCORSO

- > Host discovery e scansione porte
- > Fingerprinting e Nmap Scripting Engine
- > Enumeration dei servizi
- > Vulnerability scanning e falsi positivi
- > Scoring e prioritizzazione (CVSS/EPSS)

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

```
root@hacklab:~/lezione-02/obiettivi $
```

LEZIONE 02 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

- > Comprendere – differenze tra scanning, enumeration e VA
- > Applicare – scansioni con Nmap+NSE e scanner
- > Analizzare – validare e distinguere i falsi positivi
- > Valutare – rischio con CVSS e prioritizzazione
- > Creare – un report di VA prioritizzato

```
root@hacklab:~/lezione-02/inquadramento $
```

LEZIONE 02 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Dopo la ricognizione si interrogano attivamente i sistemi per scoprire servizi, versioni e debolezze. La lezione mostra come trasformare un elenco di host in una mappa di vulnerabilità prioritizzata, senza confondere un vulnerability assessment con un penetration test.

// PERCHE' CONTA

Dalla mappatura alla scoperta e classificazione delle vulnerabilità.

```
root@hacklab:~/lezione-02/mappa-insieme $
```

LEZIONE 02 / MAPPA // INSIEME

Mappa d'insieme del modulo

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

FONDAMENTI

- 01 Host discovery e scansione delle porte
- 02 Fingerprinting di servizi e OS
- 03 Enumeration dei servizi di rete
- 04 Scan autenticato e falsi positivi
- 05 Scoring e prioritizzazione (CVSS/EPSS)

APPROFONDIMENTI

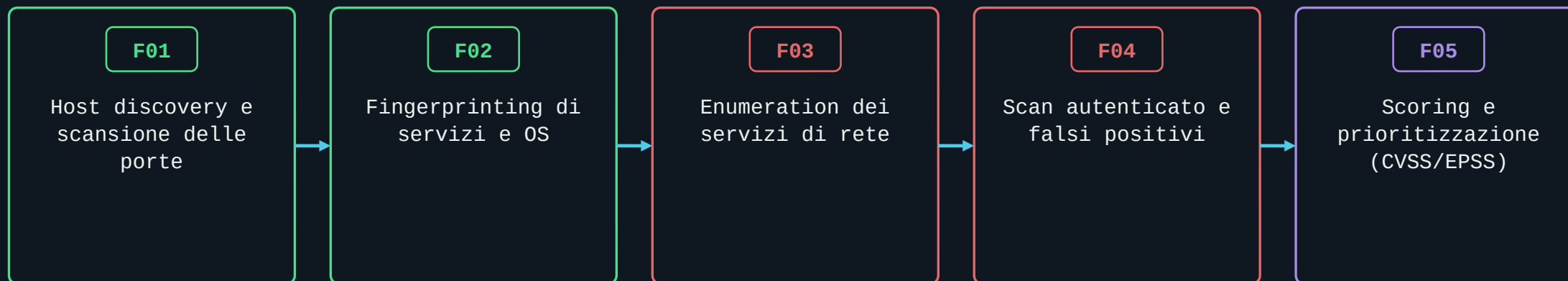
- 06 Evasione e sistemi fragili
- 07 Copertura e rischi dello scan autenticato
- 08 Validazione manuale dei finding
- 09 EPSS e rischio reale
- 10 VA e pentest sul piano operativo

```
root@hacklab:~/lezione-02/flusso-1 $
```

LEZIONE 02 / FLUSSO // FONDAMENTI

Sequenza di fasi – Fondamenti

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



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-02/concetto-1 $
```

LEZIONE 02 / CONCETTO 1/10

[Difesa]

Host discovery e scansione delle porte

// SPIEGAZIONE

La scansione individua host attivi e porte aperte distinguendo TCP, basato su handshake, e UDP, senza connessione e più incerto. Il timing regola la velocità: più aggressivo, più rilevabile e disruptivo, quindi va calibrato sullo scope.

// ESEMPIO

```
$ nmap -sS -p- -T3 10.0.0.0/24
```

```
root@hacklab:~/lezione-02/concetto-2 $
```

LEZIONE 02 / CONCETTO 2/10

[Difesa]

Fingerprinting di servizi e OS

// SPIEGAZIONE

Oltre a sapere quali porte sono aperte, serve capire quale servizio e versione girano e quale sistema operativo c'è dietro. L'Nmap Scripting Engine automatizza rilevamento di versioni, banner e controlli di vulnerabilità note.

// ESEMPIO

```
$ nmap -sV -O --script=default 10.0.0.5
```

```
root@hacklab:~/lezione-02/concetto-3 $
```

LEZIONE 02 / CONCETTO 3/10

[Attacco/tecnica]

Enumeration dei servizi di rete

// SPIEGAZIONE

L'enumerazione estrae informazioni utili dai servizi esposti: condivisioni e utenti da SMB, community string da SNMP, utenti validi da SMTP, export da NFS, struttura da LDAP. Spesso rivela percorsi d'attacco senza bisogno di exploit.

// ESEMPIO

```
$ enum4linux -a 10.0.0.5
```

```
root@hacklab:~/lezione-02/concetto-4 $
```

LEZIONE 02 / CONCETTO 4/10

[Attacco/tecnica]

Scan autenticato e falsi positivi

// SPIEGAZIONE

Uno scan non autenticato vede cio che vede un estraneo; quello autenticato, con credenziali, ispeziona patch e configurazioni dall'interno con molta piu precisione. Capire la differenza aiuta a spiegare perche nascono i falsi positivi e come ridurli.

// ESEMPIO

> Uno scanner segnala una CVE per versione, ma la patch backport dell'OS l'ha gia corretta.

```
root@hacklab:~/lezione-02/concetto-5 $
```

LEZIONE 02 / CONCETTO 5/10

[IA]

Scoring e prioritizzazione (CVSS/EPSS)

// SPIEGAZIONE

Le vulnerabilità si identificano con CVE, si classificano per tipo con CWE e si valutano per gravità con CVSS; EPSS stima invece la probabilità di sfruttamento reale. Combinarli, anche con aiuto dell'IA, permette un triage che non si ferma al solo punteggio tecnico.

// ESEMPIO

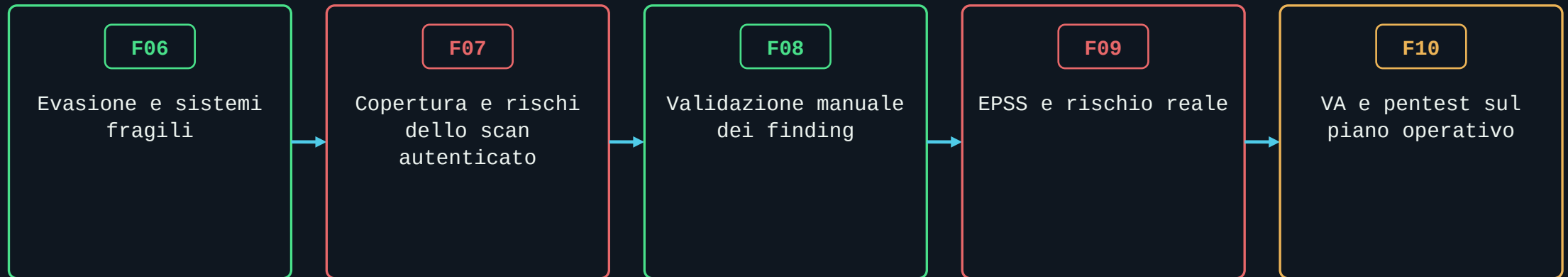
> CVSS 9.8 ma EPSS 2% contro CVSS 7.5 ed EPSS 70%: la seconda ha priorità operativa.

```
root@hacklab:~/lezione-02/flusso-2 $
```

LEZIONE 02 / FLUSSO // APPROFONDIMENTI

Sequenza di fasi – Approfondimenti

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



> Le fasi si susseguono: l'esito di ciascuna alimenta la successiva.

```
root@hacklab:~/lezione-02/concetto-6 $
```

LEZIONE 02 / CONCETTO 6/10

[Difesa]

Evasione e sistemi fragili

// SPIEGAZIONE

Frammentazione, rallentamento e scansioni mirate possono eludere il rilevamento, ma aumentano tempi e complessità. Su sistemi fragili come legacy e OT anche una semplice scansione può causare malfunzionamenti: va concordata e sorvegliata.

// ESEMPIO

> Uno scan UDP aggressivo manda in crash un vecchio PLC industriale.

```
root@hacklab:~/lezione-02/concetto-7 $
```

LEZIONE 02 / CONCETTO 7/10

[Attacco/tecnica]

Copertura e rischi dello scan autenticato

// SPIEGAZIONE

Lo scan con credenziali offre copertura profonda su patch, software installato e configurazioni, ma richiede account dedicati e comporta il rischio di esporre quelle credenziali. Vanno protette e revocate a fine attività.

// ESEMPIO

> Un account di sola lettura dedicato allo scanner, disabilitato al termine dell'ingaggio.

```
root@hacklab:~/lezione-02/concetto-8 $
```

LEZIONE 02 / CONCETTO 8/10

[Difesa]

Validazione manuale dei finding

// SPIEGAZIONE

Uno scanner propone, l'analista dispone: ogni risultato rilevante va confermato manualmente per escludere falsi positivi e dimostrare l'impatto reale. E il passaggio che trasforma un elenco automatico in evidenza affidabile.

// ESEMPIO

> Si verifica una presunta SQL injection con una singola query controllata prima di riportarla.

```
root@hacklab:~/lezione-02/concetto-9 $
```

LEZIONE 02 / CONCETTO 9/10

[Attacco/tecnica]

EPSS e rischio reale

// SPIEGAZIONE

EPSS stima la probabilit  che una vulnerabilit  venga sfruttata nel breve periodo, aggiungendo al 'quanto e grave' il 'quanto e probabile'. Prioritizzare con EPSS evita di rincorrere punteggi alti ma improbabili, concentrando le risorse dove conta.

// ESEMPIO

> Si corregge prima una CVE con exploit pubblico ed EPSS elevato, pur con CVSS medio.

```
root@hacklab:~/lezione-02/concetto-10 $
```

LEZIONE 02 / CONCETTO 10/10

[Norme & metodo]

VA e pentest sul piano operativo

// SPIEGAZIONE

Operativamente il VA è ampio, automatizzato e ripetibile, pensato per il monitoraggio continuo; il pentest è mirato, manuale e dimostrativo, pensato per provare l'impatto. Confonderli porta ad aspettative sbagliate nel contratto e nel report.

// ESEMPIO

> Un VA mensile su tutta la rete, un pentest annuale sulle applicazioni critiche.

```
root@hacklab:~/lezione-02/strumenti $
```

LEZIONE 02 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Nmap+NSE

Nessus

OpenVAS

Masscan

Nikto

enum4linux

// 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-02/lab-1 $
```

LEZIONE 02 / LABORATORIO 1

Laboratorio 1

\$ Scanning ed enumeration (Nmap+NSE su Metasploitable)

// PROCEDURA

[1] Esegui Nmap+NSE su Metasploitable ed enumera i servizi esposti

[!] Verifica: Cosa distingue uno scan SYN da uno connect?

```
root@hacklab:~/lezione-02/lab-2 $
```

LEZIONE 02 / LABORATORIO 2

Laboratorio 2

\$ Vulnerability assessment e triage (OpenVAS, lista per CVSS)

// PROCEDURA

[1] Lancia OpenVAS

[2] valida un finding e costruisci la lista per CVSS

[!] Verifica: Perché un VA produce falsi positivi?

```
root@hacklab:~/lezione-02/caso-di-studio $
```

LEZIONE 02 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Compromissione resa possibile da una vulnerabilità nota ma non prioritizzata (anticipo del caso Equifax).

// 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-02/etica $
```

LEZIONE 02 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] La scansione genera traffico rilevabile e disruptivo: solo entro scope e finestre concordate.

```
root@hacklab:~/lezione-02/ricapitolazione $
```

LEZIONE 02 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

- > Differenze tra scanning, enumeration e VA
- > Scansioni con Nmap+NSE e scanner
- > Validare e distinguere i falsi positivi
- > Rischio con CVSS e prioritizzazione
- > Un report di VA prioritizzato

```
root@hacklab:~/lezione-02/verifica $
```

LEZIONE 02 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

- ? Perché uno scan autenticato cambia i risultati?
- ? Come nasce un falso positivo e come si valida?
- ? Quando un VA non è ancora un penetration test?

// VALUTAZIONE

Report di VA prioritizzato + prova pratica di scansione.

// LETTURE

Doc. Nmap/NSE; NIST SP 800-115; specifiche CVSS.

lezione 02 completata

\$ next

Scanning, Enumeration e Vulnerability Assessment

[!] 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

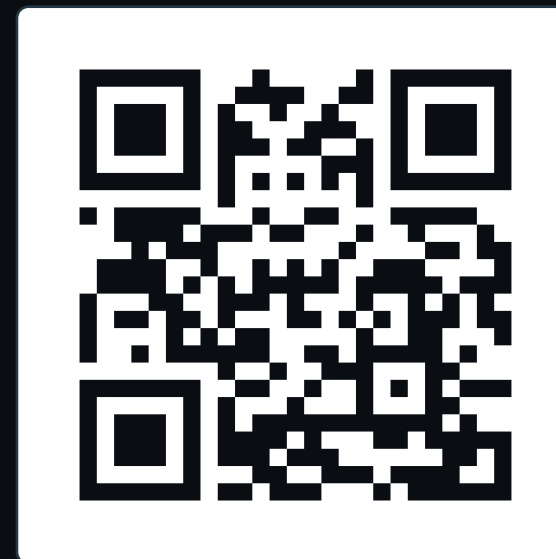


Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it



Inquadra il QR con la fotocamera
per aprire il sito.