



Alessandro Cavaliere - 0522501528

02/07/2024



# CREAZIONE DI VIRTUAL MACHINE “VULNERABLE BY DESIGN”

UNIVERSITÀ DEGLI STUDI DI SALENTO

-PENTESTVM-

Esame di Penetration Testing & Ethical Hacking  
Docente: Arcangelo Castiglione

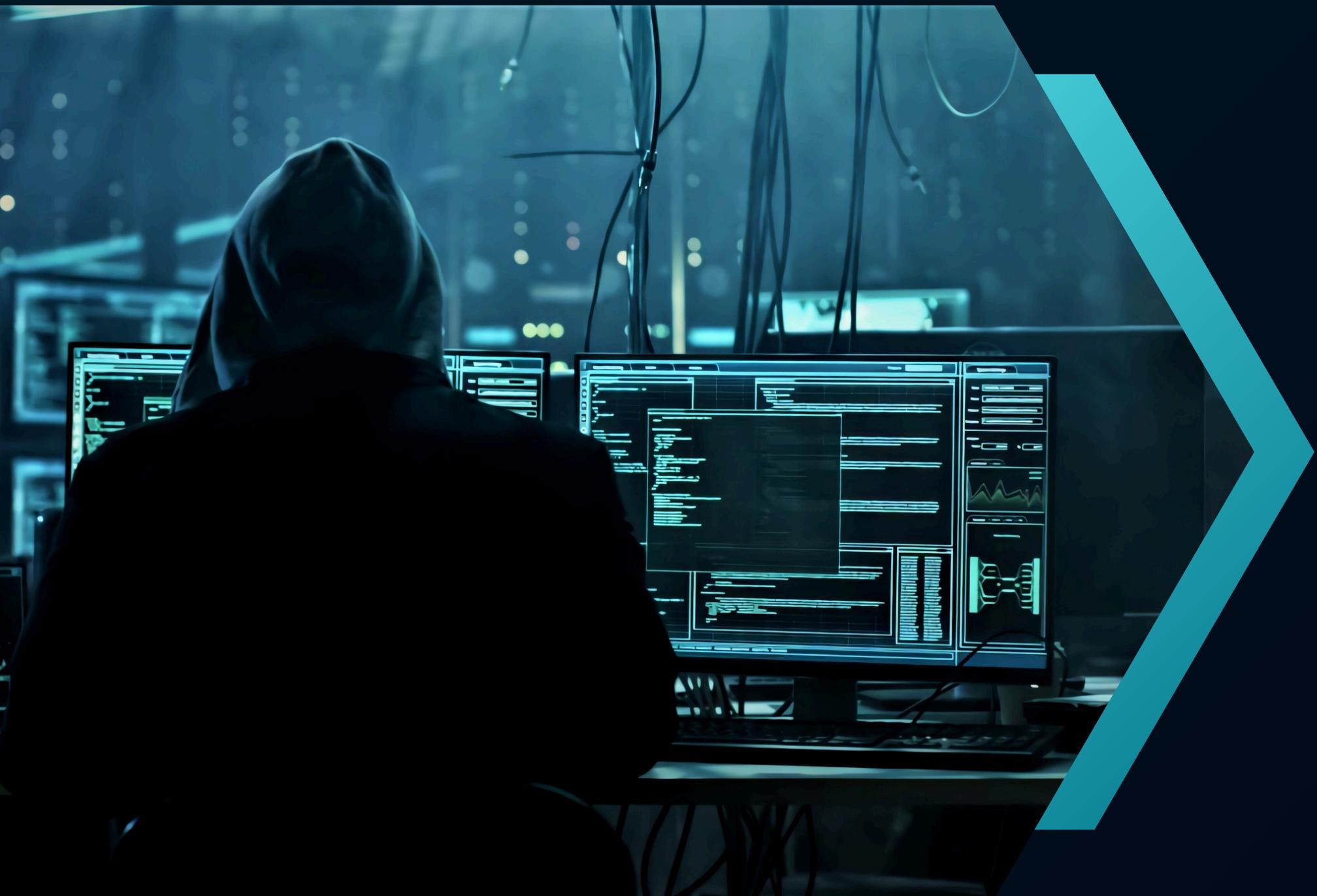
# INDICE

- OBIETTIVO DEL PROGETTO
- CONFIGURAZIONE VM
- SETUP AMBIENTE DI LAVORO
- INTRODUZIONE ALLE SFIDE CTF
- APPROFONDIMENTO DI OGNI SFIDA
- CONCLUSIONI



# OBIETTIVO DEL PROGETTO

Questo progetto ha l'obiettivo di creare una Virtual Machine 'vulnerabile by design' con tre sfide **Capture the Flag (CTF)** ospitate tramite Apache. Ogni livello rappresenta una vulnerabilità comune. I livelli saranno presentati e affrontati secondo uno schema incrementale.



# CONFIGURAZIONE VM

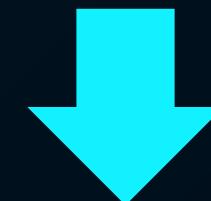
(Software di Virtualizzazione)

## Download Virtual Box



(Sistema operativo scelto)

## Download ISO Debian



(NAT Network + Host-only)

## VirtualBox Networking

Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Host-only	+	+	+	-	-
Internal	-	-	+	-	-
Bridged	+	+	+	+	+
NAT	+	<a href="#">Port forward</a>	-	+	<a href="#">Port forward</a>
NATservice	+	<a href="#">Port forward</a>	+	+	<a href="#">Port forward</a>



# SETUP AMBIENTE DI LAVORO



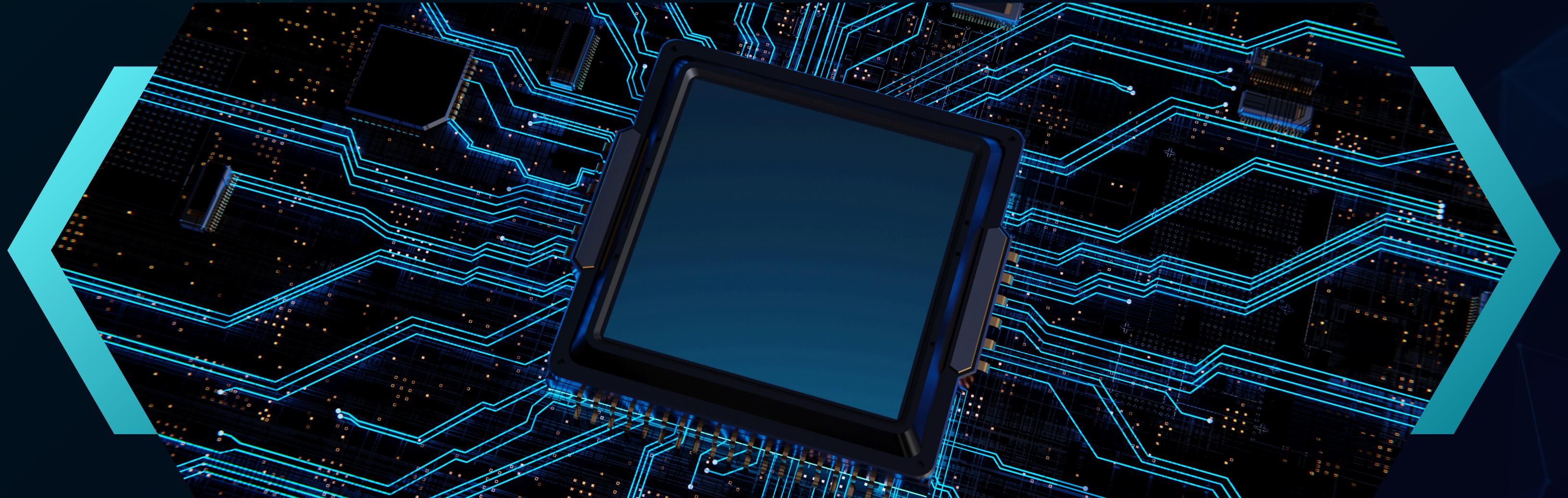
Installazione di SSH



Installazione di PHP 7



Installazione di Apache



# INTRODUZIONE ALLE SFIDE CTF



- 1 **Livello 1 - Race is Fun :)**
  - 2 **Livello 2 - PHP Injection**
  - 3 **Livello 3 - Privilege Escalation**
- 

# LIVELLO 1

## RACE IS FUN :)

CTF Web - Access Control

Il livello 1 coinvolge dei file PHP  
vulnerabili alla **RACE CONDITION**

Dimostrazione Pratica:

Accedere a <http://192.168.56.106/>

The screenshot shows a web browser window with the URL [192.168.56.106/index.php](http://192.168.56.106/index.php). The page title is "Level1 - Race is Fun :)". Below the title, there is a message: "You currently have 100\$ in your account." and "You transferred a total of 0\$ to Level1.". To the right, there is a form titled "Create a new payment" with a text input field containing "0" and a blue "Submit Query" button. At the bottom left, there is a link "Go here if you want a new account.".



# LIVELLO 2

## PHP INJECTION

CTF Web

Il livello 2 sfrutta una vulnerabilità di iniezione PHP all'interno di un form di inserimento per ottenere una **REMOTE CODE EXECUTION**

Dimostrazione Pratica:

Accedere a <http://192.168.56.106/>

**Livello 2 - PHP Injection**

You can view the source code [here](#)

Put some code

Send



# LIVELLO 3

## PRIVILEGE ESCALATION

CTF Software

Il livello 3 sfrutta una errata configurazione di un software con bit setuid acceso per elevare i suoi privilegi a root, ottenendo una **PRIVILEGE ESCALATION**.

Dimostrazione Pratica:

Ottener Reverse Shell dal Livello 2.

```
(galexela㉿kali)-[~]
$ nc -lnvp 9000
listening on [any] 9000 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.106] 58744
bash: cannot set terminal process group (557): Inappropriate ioctl for device
bash: no job control in this shell
www-data@vulnbox:/var/www/html$
```



# RISULTATO

## FLAG OTTENUTA!

```
cat /root/root.txt  
connection: XCB error: 3 (BadWindow), sequen  
Congratulations !! You've pwned the VM and allothe g3 levels.  
qt.qpa.xcb: QXcbConnection: XCB error: 3 (BadWindow), sequen  
Here's the flag → FLAG{P3n_735t_3x4M_2_0_2B4}
```

Una volta completati tutti e 3 i livelli CTF, potremo ottenere la **FLAG** nascosta all'interno di un file accessibile solo dall'utente root

N.B: Il file in questione è stato creato solo come Proof Of Concept.

# CONCLUSION

Ogni sfida è stata pensata per mettere alla prova le competenze di sicurezza informatica degli utenti, dalla scoperta di vulnerabilità fino all'esecuzione di **exploit** efficaci per ottenere il controllo del sistema.

Nell'ambito del penetration testing, essendo quest'ultimo una disciplina che richiede competenze **pratiche**, questo tipo di progetto fornisce una piattaforma pratica per apprendere e migliorare le competenze di sicurezza informatica (in un ambiente sicuro), ma contribuisce anche alla preparazione per situazioni reali di **attacco** e **difesa**.



# GRAZIE PER L'ATTENZIONE

ALESSANDRO CAVALIERE