Introduzione

CYBERSECURITY

- Insieme di tecnologie utilizzate per ridurre il rischio di attacchi informatici

Viene spesso presa sottogamba.

CVE-2021-44228

CVE-2022-0609

```
cursor.execute(
"SELECT * FROM users WHERE username=" +
username + " AND password=" + password)
```

```
print(subprocess.check_output(f"ping {ipaddr}",
shell=True))
```

```
eval(input())
```

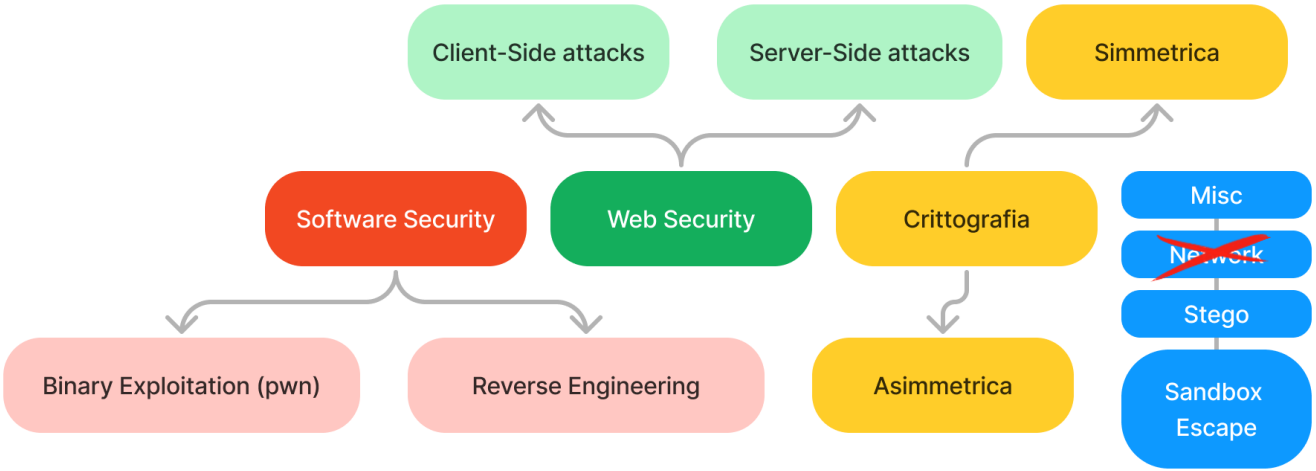
COSA È UNA CTF?

- Competizione di cybersecurity
- Ideata per la quarta edizione di DEFCON
- Jeopardy/attack-defense
- Flags!

JDUV4E6AGE47UNN336X4ED4HYL74S2VF

flag{l337_str1ng}

Argomenti


Client-Side attacks
Server-Side attacks
Simmetrica
Software Security
Web Security
Crittografia
Misc
Network
Stego
Sandbox Escape
Binary Exploitation (pwn)
Reverse Engineering
Asimmetrica

LINUX!

Viene utilizzato da gran parte dei server
Quantità (e qualità) di tool maggiore

OPZIONI

UBUNTU

Consigliato, ideale per iniziare ad usare Linux.

KALI

Non consigliato.

OPZIONI

VM

Utilizzabile solo se si hanno tante risorse

Lenta

DUAL BOOT

Scelta migliore se si ha tanto spazio sul disco

Ha i suoi pro e contro

WSL

Più leggero rispetto alle precedenti opzioni.
Permette di usare Windows e Linux in contemporanea

SHELL!

Verrà utilizzata più spesso rispetto alla GUI

LINUX CMDLINE CHEATSHEET

https://cheatography.com/davechild/cheat-sheets/linux-command-line/

SETUP

https://training.olicyber.it/training/environment

ALTRI COMANDI UTILI

BINWALK Permette di cercare file dentro altri file	**EXIFTOOL** Permette di leggere i medatati delle immagini	**STRINGS** Printa tutte le stringhe presenti in un file
ZSTEG Recupera informazioni nascoste in file .bmp e .png	**FILE** Permette di determinare il tipo di un file	**STEGHIDE** Permette di recuperare informazioni da vari file

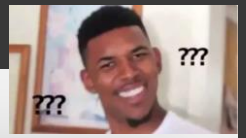
python™

Un linguaggio di programmazione estremamente versatile che offre numerosi vantaggi.

PYTHON

- **Linguaggio interpretato o compilato???**
- Parecchio lento!
- Principale linguaggio per scrivere exploit
- Fa un po' schifo...

```
help(*open("flag"))
```




```
@print\r@set\r@open\r@input\rclass\x0ca:pass
```

LIBRERIE UTILI

REQUESTS Invio di richieste HTTP/S	**PWNTOOLS** Framework che permette di scrivere exploit facilmente	**CRYPTODOME** Primitive di crittografia a basso livello
BASE64 Implementazione di diverse codifiche (base64, base32, ...)	**JSON** Parsing/dumping di stringhe in formato JSON	**FLASK** Micro framework per lo sviluppo web

Una stringa che identifica altre stringhe (???)

Introduzione alle regex

https://regexone.com/

Piattaforma per testarle

https://regex101.com/

FINE

Salvatore Abello, 5IB

salvatore.abello2005@gmail.com
https://github.com/salvatore-abello