GALILEI 2025

Intro alle CTF: Misc, Web, Crypto, Network & Rev

K!nd4SUS CyberSecurity Team - Università degli Studi di Milano

Samuele Manclossi & Andrea Lunghi

A.A. 2025/2026

TOOL NECESSARI

Per l'installazione dei tool necessari fate riferimento al documento `installazione_tool.pdf`.
I tool che useremo sono:

- Python3 + pwntools
- Wireshark
- Netcat (`nc`)
- Ghidra
- pwndbg

Inoltre, useremo le seguenti piattaforme:

- PicoCTF
- Olicyber Training

SPEEDS AND FEEDS - MISC

La prima challenge è una misc tratta da PicoCTF (dove è classificata Reverse).

> *There is something on my shop network running at `nc mercury.picoctf.net 16524`, but I can't tell what it is. Can you?*

SPEEDS AND FEEDS - MISC

Procedura di massima:

1. collegarsi tramite `nc`
2. indagare
3. risolvere tutto

Facile vero?

SPEEDS AND FEEDS - MISC

PROVIAMOCI

SPEEDS AND FEEDS - MISC

Cosa ci insegna?

- spesso per affrontare le challenge più semplici è sufficiente essere curiosi

SPEEDS AND FEEDS - MISC

Cosa ci insegna?

- spesso per affrontare le challenge più semplici è sufficiente essere curiosi
- (e avere un browser)

SPEEDS AND FEEDS - MISC

Cosa ci insegna?

- spesso per affrontare le challenge più semplici è sufficiente essere curiosi
- (e avere un browser)
- nelle misc non si sa mai cosa aspettarsi!

I GOT MAGIC - WEB

In questa challenge il sito ci permette di caricare dei file, il nostro obbittivo è leggere il file /flag.txt.

Sfortunatamente però solo immagini :((spoiler in realtà no)

I GOT MAGIC - WEB

Il nome della challange ci da un indizio.

Facciamo un po’ di ricerca!

I GOT MAGIC - WEB

Cosa succede se proviamo a caricare il seguente file PHP ?.

```
GIF89a;
<?php system(”cat /flag.txt”); ?>
```

I GOT MAGIC - WEB

E se provassimo a mettere
la doppia estensione ?

GEROGLIFICI - CRYPTO

Challenge semplice tratta da Olicyber Training

> *Ti sei mai cimentato con la crittografia più antica del mondo?*
> *Puoi collegarti al servizio remoto con:*
> `nc geroglifici.challs.olicyber.it 35000`

Ci mette a disposizione un file `script.py`

GEROGLIFICI - CRYPTO

Procedura di massima:

1. provare a leggere lo script
2. collegarsi tramite `nc` e fare qualche tentativo
3. dedurre come funziona il sistema
4. capire come romperlo
5. scrivere un programma che lo rompa al posto nostro

Pronti?

GEROGLIFICI - CRYPTO

PROVIAMOCI

`script.geroglifici.bozza.py` vi può essere utile :)

GEROGLIFICI - CRYPTO

Cosa ci rimane da questa challenge?

- non serve capire esattamente cosa fa un programma per romperlo

GEROGLIFICI - CRYPTO

Cosa ci rimane da questa challenge?

- non serve capire esattamente cosa fa un programma per romperlo
- saper scrivere qualche riga di python è utile (`pwntools` è comodo)

GEROGLIFICI - CRYPTO

Cosa ci rimane da questa challenge?

- non serve capire esattamente cosa fa un programma per romperlo
- saper scrivere qualche riga di python è utile (`pwntools` è comodo)
- un programma risolve una famiglia di problemi ← indipendemente dalla randomizzazione!

GEROGLIFICI - CRYPTO

Cosa ci rimane da questa challenge?

- non serve capire esattamente cosa fa un programma per romperlo
- saper scrivere qualche riga di python è utile (`pwntools` è comodo)
- un programma risolve una famiglia di problemi ← indipendemente dalla randomizzazione!
- (nessuno di noi vedrà più le emoji allo stesso modo)

FLAGVAULT - REV

Ci viene dato in allegato un file compilato in C.

Ci viene richiesta una password da recuperare per ottenere la flag.

Analisi Statica vs Analisi Dinamica

FLAGVAULT - REV

Cerchiamo di capire la logica del programma

FLAGVAULT - REV

E se provassimo con l’analisi dinamica ?

TR[A]IS - NETWORK

Challenge tratta da Olicyber Training

> *Ho programmato una AI fortissima per giocare a tris, ha perso solo una partita fino ad adesso, non penso succederà una seconda volta.*
> *Sito:* `http://trais.challs.olicyber.it`

Non leggete il writeup! Toglie il divertimento.
Abbiamo a disposizione un file `capture.pcapng`

TR[A]IS - NETWORK

Procedura di massima:

1. provare a interagire con il sito
2. capire cosa ci serve di recuperare dalla cattura di rete (tramite `wireshark`)
3. trovarlo
4. applicarlo
5. prenderci i punti

PROVIAMOCI

`script.geroglifici.bozza.py` vi può essere utile :)

TR[A]IS - NETWORK

Cosa abbiamo imparato?

- è importante capire con cosa stiamo interagendo per utilizzare bene il pcapng

TR[A]IS - NETWORK

Cosa abbiamo imparato?

- è importante capire con cosa stiamo interagendo per utilizzare bene il pcapng
- `wireshark` è molto comodo

TR[A]IS - NETWORK

Cosa abbiamo imparato?

- è importante capire con cosa stiamo interagendo per utilizzare bene il pcapng
- `wireshark` è molto comodo
- state attenti ai bound quando programmate!

TR[A]IS - NETWORK

Cosa abbiamo imparato?

- è importante capire con cosa stiamo interagendo per utilizzare bene il pcapng
- `wireshark` è molto comodo
- state attenti ai bound quando programmate!
- le AI possono essere forti ma non sanno barare :(

BASHINATOR REVENGE - MISC

Classica challenge in stile jail.

Ci viene dato un file bash che ci permette di eseguire dei comandi da terminale ma è presente una blacklist che limita certi caratteri.

BASHINATOR REVENGE - MISC

Un po’ di ripasso sulla shell Linux

BASHINATOR REVENGE - MISC

I glob sembrano interessanti però come potremmo sfruttarli ?

GALILEI 2025

Grazie dell'attenzione!
Qualche domanda?