

Miscellaneous 1

Introduzione

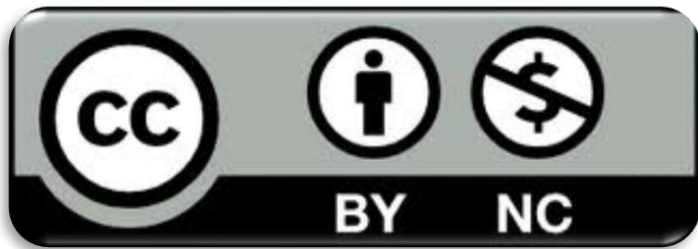


License & Disclaimer

2

License Information

This presentation is licensed under the
Creative Commons BY-NC License



To view a copy of the license, visit:

<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Cos'è una CTF?

3

- Competizioni di **offensive security** (impariamo a ragionare come gli attaccanti per difenderci meglio)
- **Gamification**, servizi “giocattolo”
- **Flag**

flag{I33t_str1ng}

Argomenti

4

- Software
 - binary exploitation
 - reverse engineering
- Crittografia
- Web
- Network
- Hardware
- Misc (tutto ciò che non ricade nelle prime categorie)

Tipologie: Jeopardy

5

- Challenge da risolvere in un tempo medio-lungo
- Punteggi statici o dinamici
- Nessuna interazione con gli altri team (~~e quasi~~)

Tipologie: Attack&Defence

6

- Macchina/e con **servizi** identici per ogni team
- Basata sul concetto di **tick**
 - SLA
 - Attacco
 - Difesa
- Tempo generalmente minore rispetto ad una Jeopardy
- Molto più dinamica

Linux

7

- Spesso useremo **Linux**, perché è il sistema operativo usato da gran parte dei server (circa l'80%) e per disponibilità di molti dei tool online
- Due opzioni principali:
 - **Ubuntu** (consigliata): bisogna installare gran parte dei tool, ma utile per imparare
 - **Kali** (sconsigliata): molti dei tool necessari sono già presenti, ma meno utile sul lungo periodo

Virtual Machine

8

- Scelta migliore se si hanno molte risorse
- Consuma molta RAM e CPU
- Facilmente rimpiazzabile

Dual Boot

9

- Scelta migliore se si ha molto spazio su disco
- Il modo intenzionale di usare Linux
- Non si sovraccaricano le risorse del PC
- Non si può usare sia Windows che Linux, bisogna riavviare se necessario

Windows Subsystem for Linux

10

- Ben integrato con Windows
- Permette di usare Windows e Linux in contemporanea
- Potrebbe essere complicato avere una GUI, se si usa una versione di Windows inferiore a Windows 10 Build 19044

Ulteriori informazioni

11

- Sul portale di formazione è presente una breve guida al setup con una VM pre-configurata con i tool utili per affrontare le challenge:
 - <https://training.olicityber.it/training/environment>

Shell

12

- Più che l'interfaccia grafica, spesso bisognerà usare il **terminale**
- Alcuni dei comandi principali sono brevemente riassunti qui:
 - <https://cheatography.com/davechild/cheat-sheets/linux-command-line/>

Shell

13

- **cd** *dir*: naviga nella cartella *dir*; **.** è la cartella corrente, **..** è la cartella superiore
- **ls** *dir*: lista i file nella cartella *dir*; senza argomenti lista i file della cartella corrente
- **mkdir** *dir*: crea la cartella *dir*

Shell

14

- **cat** *f1*: stampa il contenuto del file *f1*
- **cp** *f1 f2*: copia il file *f1* nel file *f2*
- **mv** *f1 f2*: sposta il file *f1* nel file *f2*
- **rm** *f1*: rimuove il file *f1* (attenzione: non viene spostato in un cestino)
- **file** *f1*: fornisce informazioni sul tipo del file *f1*

Shell

15

- **head** *f1* *-n N*: stampa le prime *N* righe del file *f1*
- **tail** *f1* *-n N*: stampa le ultime *N* righe del file *f1*
- **more** *f1*: mostra il contenuto del file *f1* riga per riga (l'altezza è limitata a quella del terminale)
- **strings** *f1* *-n N*: stampa le stringhe leggibili di lunghezza almeno *N* contenute nel file *f1*
- **grep** *patt f1*: cerca il pattern *patt* nel file *f1*

Shell

16

- `ssh user@host`: crea una connessione al server `host`, fornendo un terminale come utente `user`
- `nc host port`: crea una connessione TCP al server `host` sulla porta `port`
- In caso di dubbi...
 - `man cmd`: manuale del comando `cmd`
 - *Google*

Un po' di pratica

17

- Al seguente indirizzo è disponibile un gioco a livelli (**wargame**) per imparare molti dei comandi che userete molto, *e alcuni che userete poco*, in futuro:
 - <https://overthewire.org/wargames/bandit/>

Miscellaneous Introduzione

