

CTF Warfare

An introduction to attack defense CTFs

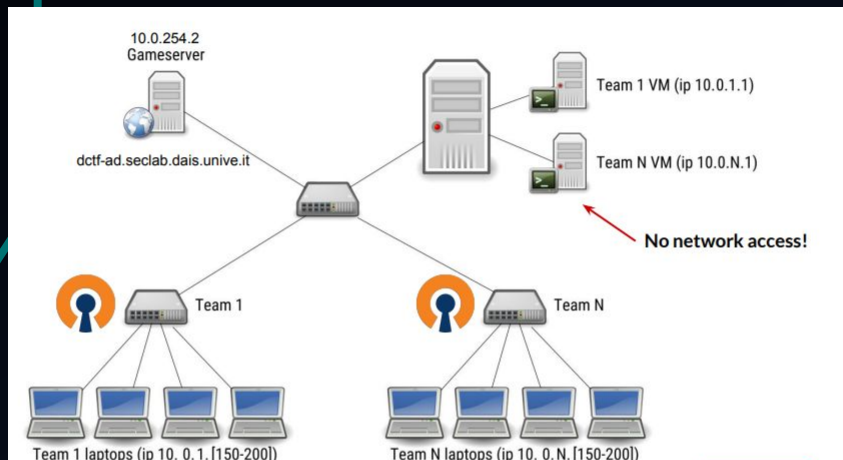
Cos'è una Ctf?

Le CTF (Capture The Flag) sono competizioni informatiche progettate per sfidare le abilità e le conoscenze dei partecipanti nel campo della sicurezza informatica.

Ci sono diversi tipi di CTF:

- 1. Jeopardy**
- 2. Attack and Defence**
- 3. King of the Hill**

Attack and Defense: Come funzionano?



Ogni squadra ha un server con dei servizi attivi

Il server di gioco si occupa di calcolare i punteggi di ogni squadra

Un server è dedicato invece per fare test e le sue flag non contano nei punti

Come si vince?

ENOWARS 7				HowTo A/D CTF	Scoreboard	Setup	Contact	Teams	Login
Round 478	asocialnetwork	bollwerk	phreaking	yvm	granulizer	oldschool	steinsgate		
	AICanaries C4T BuT S4D	AICanaries FaKappa	AICanaries	AICanaries ECSC Team France	AICanaries	AICanaries TeamItaly	AICanaries C4T BuT S4D		
1	C4T BuT S4D	1285.76 (-0.05) -692.86 (+0.00) 5142.86 (+0.00)	1772.84 (-0.80) -367.86 (+0.00) 6378.57 (+0.00)	18958.88 (-0.55) -1300.00 (+0.00) 4785.71 (+0.00)	408.82 (-0.03) -2400.00 (+0.00) 6521.43 (+0.00)	4399.00 (-0.23) -407.14 (+0.00) 6750.00 (+0.00)	533.31 (-0.02) -1242.86 (+0.00) 6335.71 (+0.00)	5478.38 (-0.67) -585.71 (+0.00) 6742.86 (+0.00)	68497.70 (-2.36)
2	TeamItaly	3268.76 (+9.42) -1521.43 (-3.57) 5021.43 (+14.29)	2237.60 (+1.20) -550.00 (+0.00) 6428.57 (+14.29)	3790.92 (+14.91) -2885.71 (-7.14) 6264.29 (+14.29)	1305.22 (+0.45) -2664.29 (-7.14) 6592.86 (+14.29)	12896.12 (+6.40) -385.71 (+0.00) 6785.71 (+14.29)	1513.18 (+0.80) -1100.00 (+0.00) 5928.57 (+14.29)	3466.92 (+4.41) -1675.00 (-3.57) 6728.57 (+14.29)	61446.59 (+116.16)
3	Bushwhackers	845.89 (+1.17) -1471.43 (-3.57) 4828.57 (+14.29)	2994.30 (-1.19) -178.57 (+0.00) 6278.57 (+14.29)	5105.63 (+8.72) -2342.86 (-14.29) 5357.14 (+14.29)	374.86 (+0.57) -2307.14 (-3.57) 6450.00 (+14.29)	1114.41 (+7.21) -1378.57 (+0.00) 6114.29 (+14.29)	388.01 (+1.15) -2775.00 (-3.57) 6200.00 (+14.29)	5005.41 (+1.77) -817.86 (+0.00) 3771.43 (+14.29)	43557.09 (+94.40)
4	Czech Cyber Team	62.13 (-0.26) -735.71 (+0.00) 6435.71 (+14.29)	308.30 (-0.19) -221.43 (+0.00) 6764.29 (+14.29)	3212.73 (-4.24) -2971.43 (-7.14) 6635.71 (+14.29)	1551.06 (-1.13) -1057.14 (-3.57) 6707.14 (+14.29)	0.00 (+0.00) -142.86 (+0.00) 6707.14 (+14.29)	167.48 (-0.09) -2350.00 (-3.57) 5100.00 (+14.29)	98.81 (-0.07) -1053.57 (+0.00) 6071.43 (+14.29)	41289.81 (+79.73)
5	aetruria	635.19 (+0.64) -585.71 (+0.00) 5885.71 (+14.29)	1063.03 (+1.91) -321.43 (+0.00) 6664.29 (+14.29)	1927.01 (+9.48) -2992.86 (-7.14) 6528.57 (+14.29)	386.21 (+1.04) -2539.29 (-7.14) 6221.43 (+14.29)	1309.33 (+4.66) -2900.00 (+0.00) 6528.57 (+14.29)	1067.23 (+2.43) -900.00 (+0.00) 6357.14 (+14.29)	1805.34 (+4.84) -2071.43 (-0.00) 6657.14 (+14.29)	40725.47 (+110.71)
6	CyberSecurityAustria	293.82 (+0.73) -650.00 (+0.00) 6221.43 (+14.29)	239.23 (-0.01) -2560.71 (-10.71) 5785.71 (+14.29)	5064.37 (+1.06) -2785.71 (-7.14) 6200.00 (+14.29)	166.67 (-0.60) -2453.57 (-7.14) 6735.71 (+14.29)	1373.50 (+0.68) -357.14 (+0.00) 6692.86 (+14.29)	338.09 (+0.55) -2400.00 (+0.00) 6354.29 (+14.29)	0.00 (+0.00) -1807.14 (+0.00) 6542.86 (+14.29)	36604.25 (+77.41)
7	The Flat Network Society	827.58 (+1.56) -50.00 (+0.00) 5957.14 (+14.29)	2701.68 (+1.47) -617.86 (+0.00) 6371.43 (+14.29)	0.00 (+0.00) -2978.57 (-7.14) 6664.29 (+14.29)	465.14 (+10.64) -2589.29 (-21.43) 6385.71 (+14.29)	1674.63 (+4.47) -800.00 (+0.00) 6792.86 (+14.29)	664.71 (+2.46) -2903.57 (-7.14) 3535.71 (+7.14)	349.16 (+1.60) -2985.71 (-7.14) 6557.14 (+14.29)	36022.18 (+72.19)
8	SKSD	143.94 (+1.17) -1639.29 (-3.57) 5664.29 (+14.29)	1046.25 (+1.12) -1089.29 (+0.00) 6671.43 (+14.29)	0.00 (+0.00) -2392.86 (-7.14) 5528.57 (+14.29)	1175.45 (+0.54) -2375.00 (-3.57) 6542.86 (+14.29)	375.46 (+8.09) -2150.00 (+0.00) 6728.57 (+14.29)	206.64 (+0.00) -46.43 (+0.00) 6742.86 (+14.29)	447.21 (+1.96) -2360.71 (-3.57) 6771.43 (+14.29)	35991.39 (+95.02)
9	Blue Water	157.80 (+0.00) -1453.57 (+0.00)	1058.83 (+0.00) -1596.43 (-3.57)	183.51 (+56.38) -2850.00 (-7.14)	0.00 (+0.00) -2603.57 (-7.14)	374.32 (-0.11) -992.86 (+0.00)	601.76 (+0.00) -1996.43 (-7.14)	381.89 (+0.00) -1546.43 (-3.57)	35918.81 (+127.70)

Tulip- flow analyzer

The screenshot displays the Tulip flow analyzer interface. At the top, there is a search bar with 'regex' and a dropdown menu set to 'Trademark'. The current view shows 'Last 5 ticks' and 'Current: 4501'. A 'Close filters' button is visible. Below this, an 'Intersection filter' section contains various tags like FLAG-IN, FLAG-OUT, BLOCKED, SURICATA, ENEMY, RCE, MEME, Sqli, PHP-RCE, PATH TRAVERSAL, AUTH, PATH TRAVERSAL, CRYPTO, PHP-LFI, SSRF, INJECTION, BOF, and STARRED. A list of network events follows, each with a heart icon, a 'Trademark:5000' label, a timestamp, and a duration. The selected event at 09:16:04.877 is expanded to show details:

- Suricata**
 - Message: ICC - Modern Firefox UA observed
 - Rule ID: 1500006
 - Action taken: allowed
- Meta**
 - Source: /traffic/capture-2022-06-16_07:14:39.pcap
 - Tags: [flag-out, suricata, enemy]
 - Source - Target: 10.254.0.1:45204 - 10.60.4.1:5000
- 09:16:04:877 0ms (Plain Hex Web PythonRequest)
- Copy
- POST /api/products/11/download?/api/login HTTP/1.1
- Host: 10.60.4.1:5000
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:100.0) Gecko/2
- Accept-Encoding: gzip, deflate
- Accept: */*
- Connection: keep-alive
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 0
- 09:16:04:906 29ms (Plain Hex Web PythonRequest)

Destructive Farm

The screenshot shows a web browser window with the URL 127.0.0.1:1337. The page title is "S4D Farm". There are two tabs: "front" and "+". The browser's address bar shows the URL and various icons. The page content is divided into three main sections:

- Filter flags:** A section with several input fields and a "FILTER" button. The "Exploit" field contains "[neo] kek.py". The "Team" field contains "Team #4". There are also fields for "Since" (containing "MSK"), "Until" (containing "MSK"), and "Status". A "Checksystem response" field is also present. A "SUBMIT" button is located below the filter fields.
- Submit manually:** A section with a text input field labeled "Text with flags" and a "SUBMIT" button. Below the input field, it says "flag format: [A-20-9]{(1)}=".
- 270 flags total:** A table showing a list of flags. The table has columns for "Exploit", "Team", "Flag", "Time", "Status", and "Checksystem response". The first few rows of the table are as follows:

Exploit	Team	Flag	Time	Status	Checksystem response
[neo] kek.py	Team #4	KF24N2L7KSRAUMK5TSTZU8GR4TTS6FZ=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KFNDEERRA6NIO2Y0XJ2I5MCS4V1ZDJZG=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	K8RNVWGBLB7B7EQ6HLIRTE2AK91FFPAH=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KE9CC9S95007M18GPDV7G3F5TELYM7N=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KY4UMBUYAL53ED1YFK29D1SGOC9S3V0=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KPS6TJXJECNMTEJOV7KWVCN29AMIKGR=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KACH8COONFDGESVDN68H5D5MCRXRKRX=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	K7DN28BYXSHXMZ5TLYYKWL67BNEAK3=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	K7RVSXR5T9FMKTG9I2A128U69IOLFU=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	K57MOS01STB0S04SFJDFCUBSLDT2UXY=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KMX3SGOXYJZBPF182XOESUFVJ45IM34=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KM65H0ABQYNBXC8ZXH9P8CLO7G9CVW=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	K5C6V4LBV27G087FVQYVYIKCR59T5LU=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KFLBPT077G1K5BZ10T\$W21U5XJM8M=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out
[neo] kek.py	Team #4	KANUC1HLT4Y8J204YPRCNC52VF2TZQ0=	December 24th 2020, 17:03:16	SKIPPED	timeout: timed out

AsocialNetwork

asocialnetwork

[Home](#)

[Login](#)

[Register](#)

Username

Password

Login

AsocialNetwork

[asocialnetwork](#) [Home](#) [Profile](#) [Messages](#) [Friends](#) [Logout](#)

Profile

[Edit Profile Picture](#)

Lontra



Leave a message on Lontra's wall

In rooms:

AsocialNetwork

[asocialnetwork](#) [Home](#) [Profile](#) [Messages](#) [Friends](#) [Logout](#)

Profile

[Edit Profile Picture](#)

Lontra



Leave a message on Lontra's wall



Lontra

FLG{Viva_L_amicizia_<3}

7:16:59 PM 10/16/2023



Lontra

Ciao Mondo odio i castori!!!

7:16:36 PM 10/16/2023

In rooms:

AsocialNetwork

[asocialnetwork](#) [Home](#) [Profile](#) [Messages](#) [Friends](#) [Logout](#)

Profile

[Edit Profile Picture](#)

Castoro



Leave a message on Castoro's wall

In rooms:

AsocialNetwork

asocialnetwork

Home

Profile

Messages

Friends

Logout

Friends

Requests



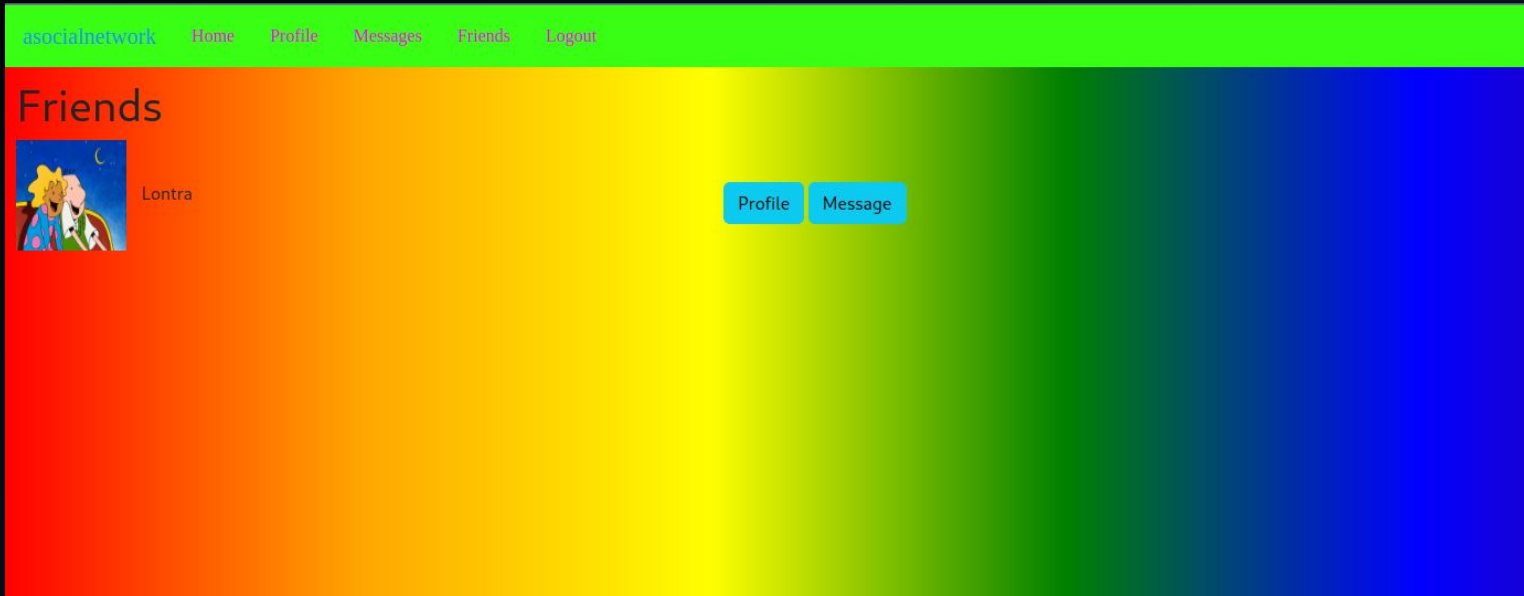
Lontra

Cancel



Ma guardiamo il codice...

AsocialNetwork



AsocialNetwork

asocialnetwork Home Profile Messages Friends Logout

Profile

Lontra



In rooms:

Leave a message on Lontra's wall



Lontra

FLG{Viva_L_amicizia_<3}

7:16:59 PM 10/16/2023



Lontra

Ciao Mondo odio i castori!!!

7:16:36 PM 10/16/2023