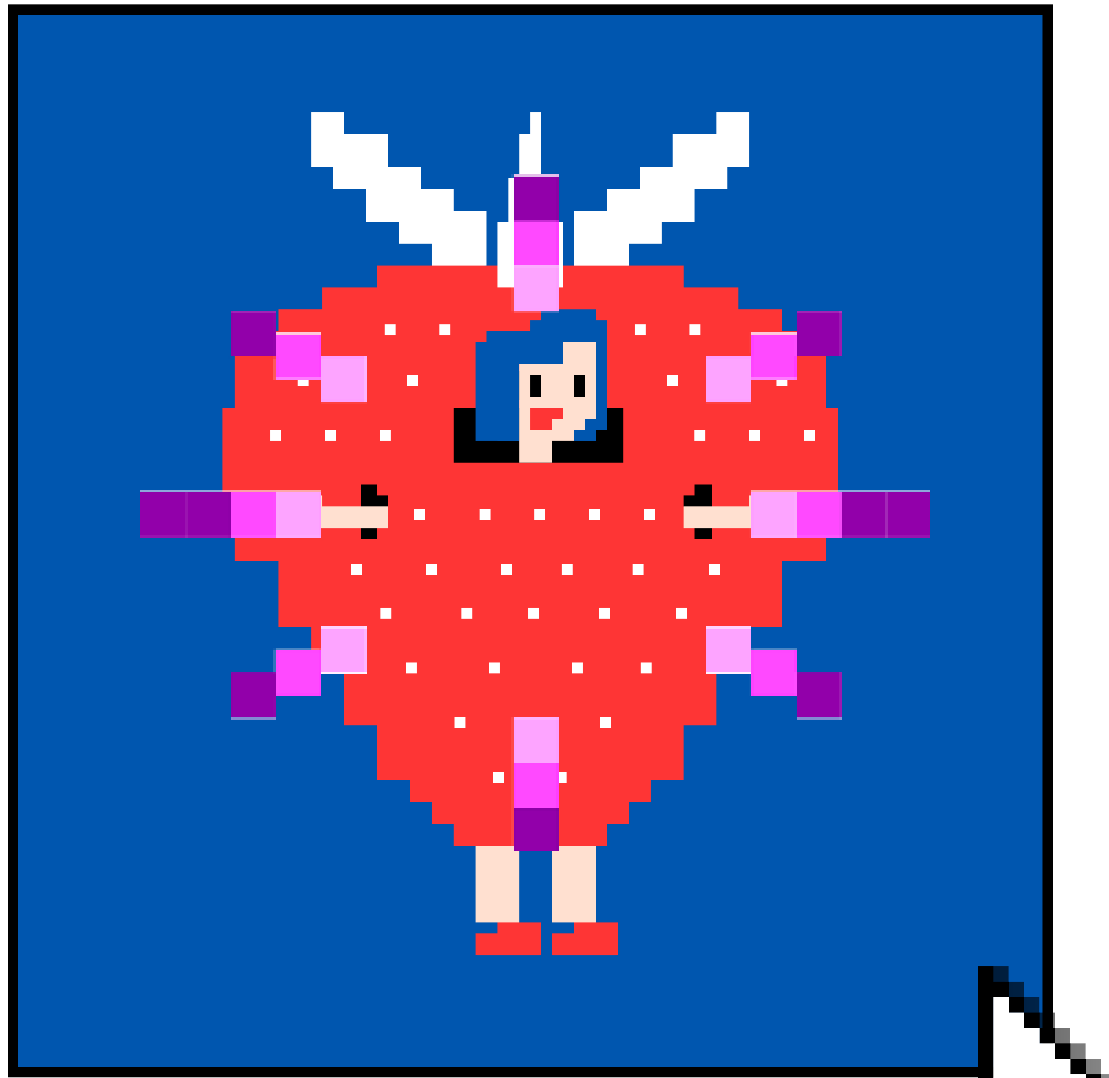
From Zero to Hero



GETTING STARTED IN CYBERSECURITY

Learn Cybersecurity on your own and beyond

AGENDA

Topics Covered

0x1-What is Cybersecurity

0x2-Cybersecurity Roadmap

0x3-CTF as a learning tool

0x4-Tips and tricks

Aldwin Tapican

Whoami:

- 3rd Year BSCS Student in NEU
- Security Researcher
- Active CTF
- Backend Developer: Django and bootstrap 5
- CBI CICS Officer and ACSS Officer

eJPT

eCMAP

CC℠

ORACLE
Certified
Specialist
Oracle Autonomous
Database Cloud
2021

ORACLE
Certified
Associate
Oracle Cloud Infrastructure
Foundations
2022

http://

aj-tap.github.io

Cybersecurity

Practice of protecting computer systems, networks, and sensitive data from theft, damage, or unauthorized access.

Offensive security

- Hack things before threat actors do
- Simulate real-world cyberattacks and attempt to breach the organization's defenses in order to identify **vulnerabilities** and **weaknesses**.

Defensive Security

- Improve security gaps before adversaries find them.
- Monitoring network traffic for suspicious activity, and implementing firewalls and other security measures to prevent unauthorized access.

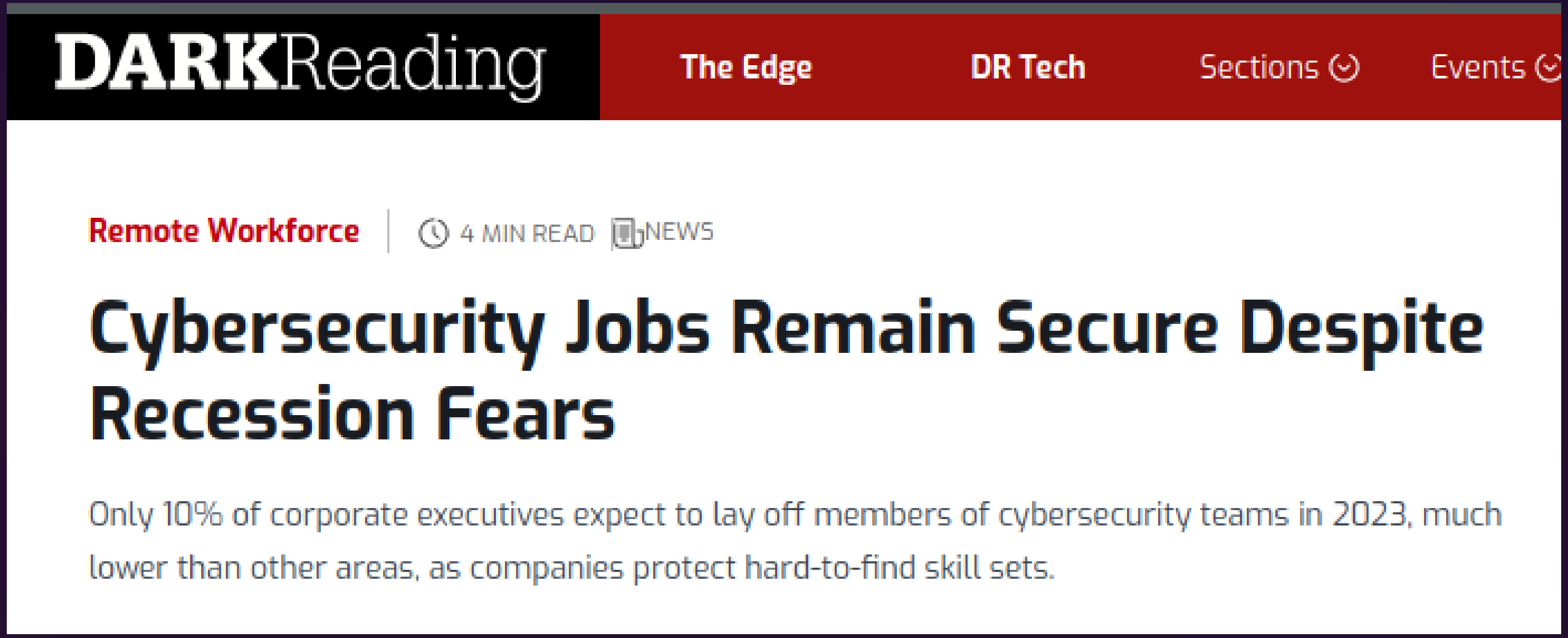
improve the organization's overall security posture

https://csrc.nist.gov/glossary/term/red_team_blue_team_approach
https://csrc.nist.gov/glossary/term/cybersecurity
https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity

WHY CYBERSECURITY?

Among the key findings of the report,
it notes that demand for cybersecurity talent is high
and continuing to grow, with a projected global
workforce gap of 3.12 million professionals

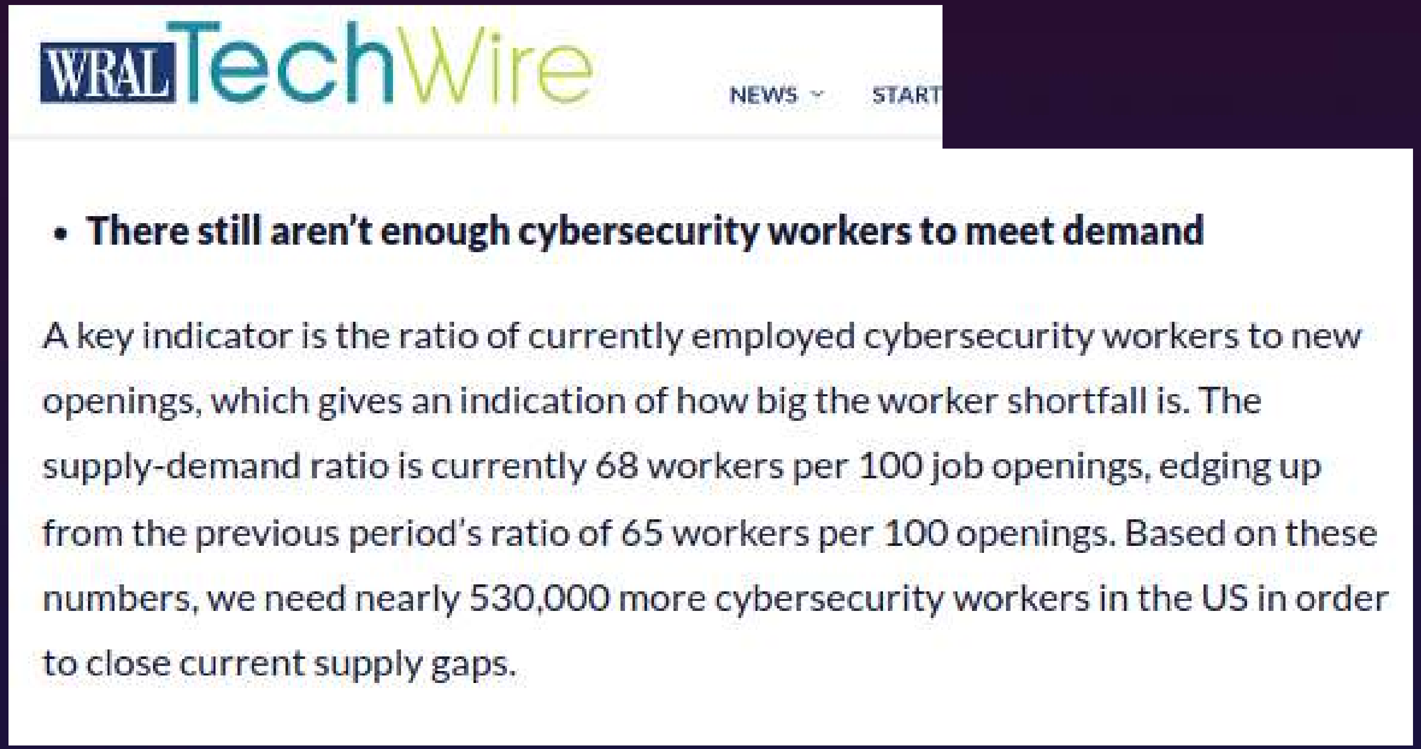
--- International Information System Security
Certification Consortium (ISC)²



Remote Workforce | 4 MIN READ | NEWS

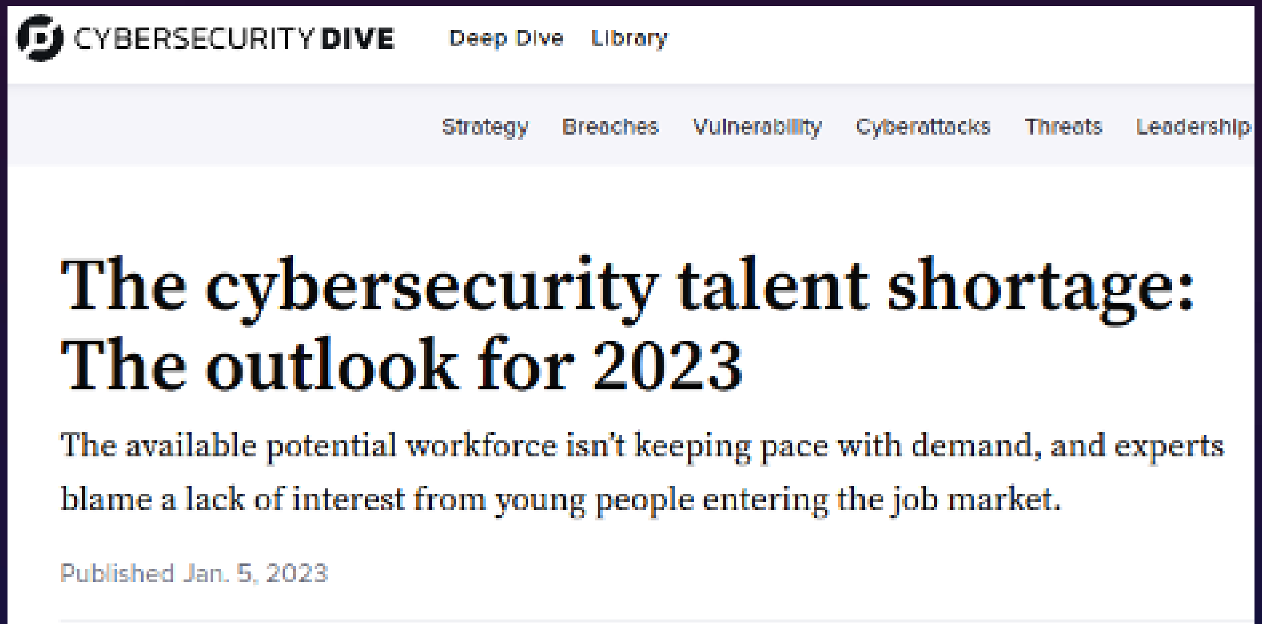
Cybersecurity Jobs Remain Secure Despite Recession Fears

Only 10% of corporate executives expect to lay off members of cybersecurity teams in 2023, much lower than other areas, as companies protect hard-to-find skill sets.



- **There still aren't enough cybersecurity workers to meet demand**

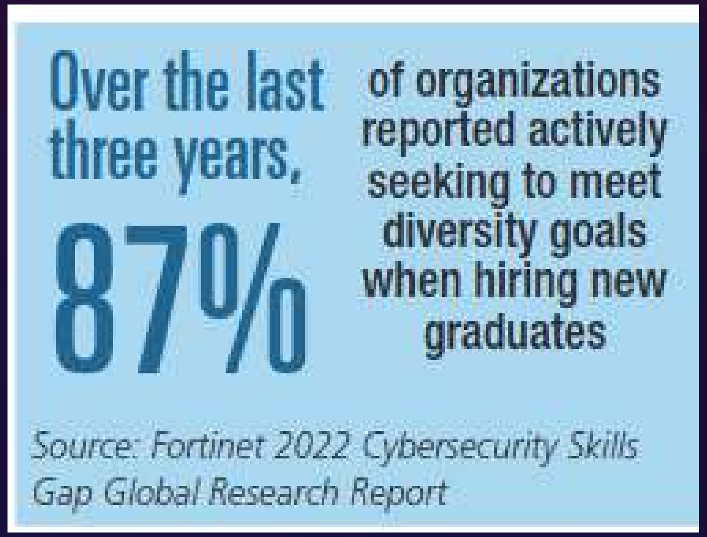
A key indicator is the ratio of currently employed cybersecurity workers to new openings, which gives an indication of how big the worker shortfall is. The supply-demand ratio is currently 68 workers per 100 job openings, edging up from the previous period's ratio of 65 workers per 100 openings. Based on these numbers, we need nearly 530,000 more cybersecurity workers in the US in order to close current supply gaps.



The cybersecurity talent shortage: The outlook for 2023

The available potential workforce isn't keeping pace with demand, and experts blame a lack of interest from young people entering the job market.

Published Jan. 5, 2023



Over the last three years, 87% of organizations reported actively seeking to meet diversity goals when hiring new graduates

Source: Fortinet 2022 Cybersecurity Skills Gap Global Research Report

https://cloud.connect.isc2.org/career-pursuers-report
https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdftechnology/information-security-analysts.htm

Careers in Cyber

Here are some reasons to consider a career in cybersecurity:

- High Salary - Security jobs have lucrative starting salaries.
- Excitement - Work in this field can involve legally hacking systems or defending against cyberattacks, which is thrilling and challenging.
- High Demand - There is an enormous gap of over 3.5 million unfilled cyber positions globally.

Incident Responder

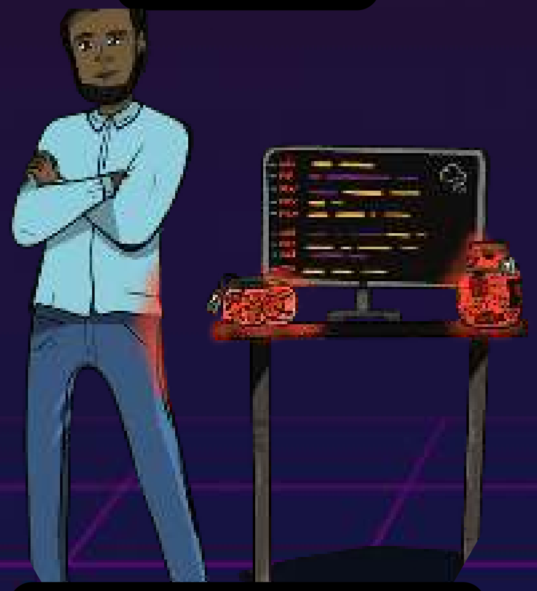
Penetration Tester

Security Analyst

Digital Forensics Examiner

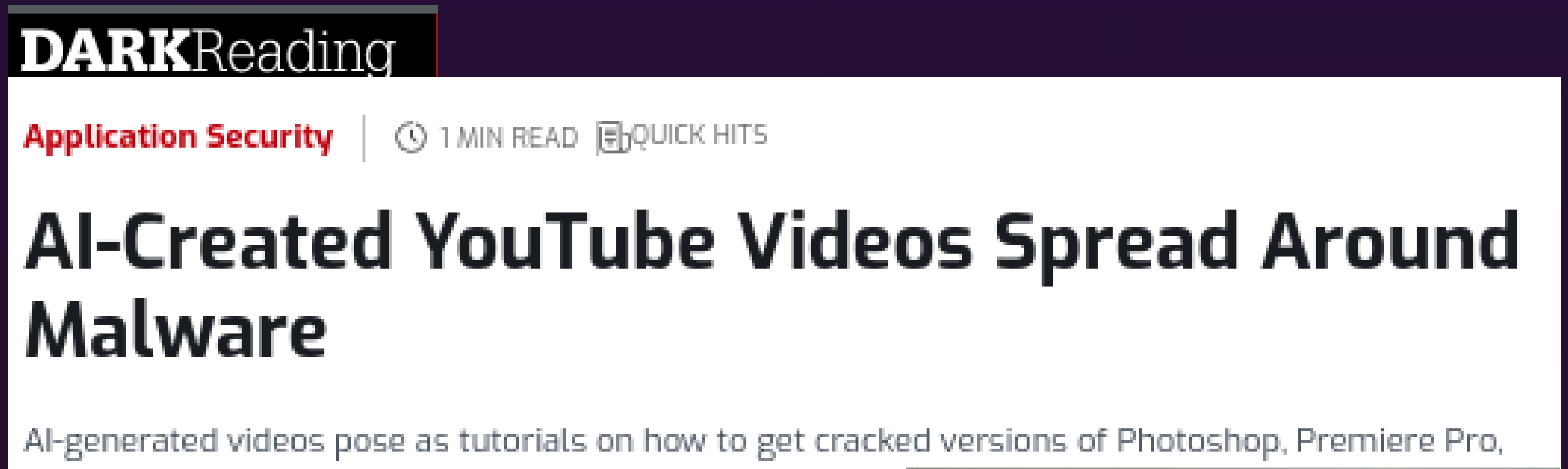
Red Teamer

Security Engineer



Malware Analyst

RECENT THREATS 2023

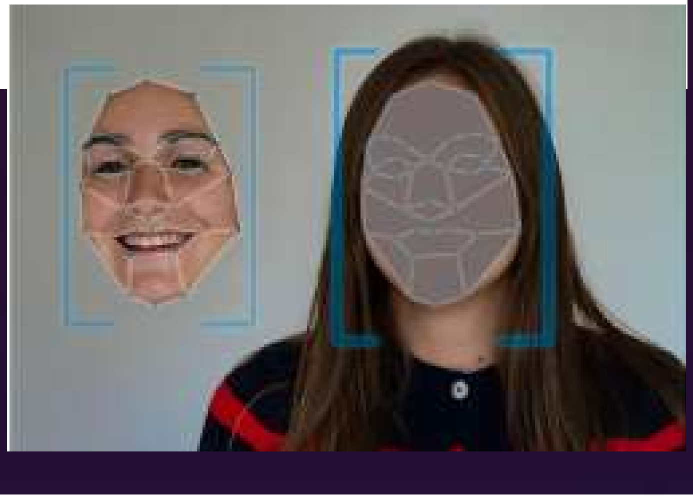


DARKReading

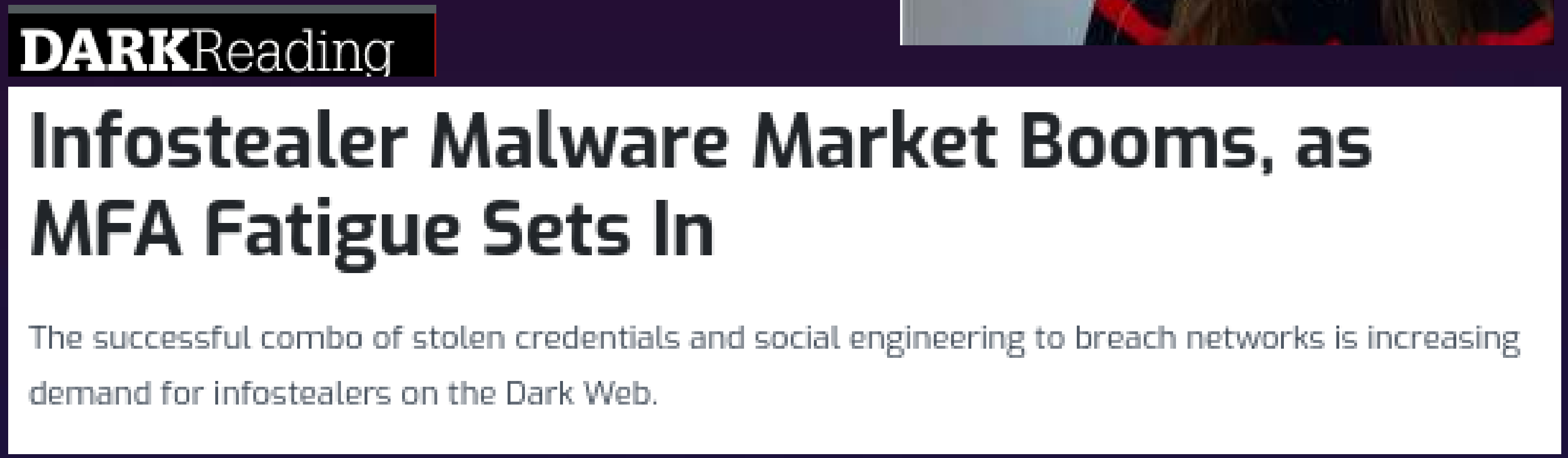
Application Security | 1 MIN READ QUICK HITS

AI-Created YouTube Videos Spread Around Malware

AI-generated videos pose as tutorials on how to get cracked versions of Photoshop, Premiere Pro, and more.



videos pretending to be
step-by-step tutorials
on how to access programs

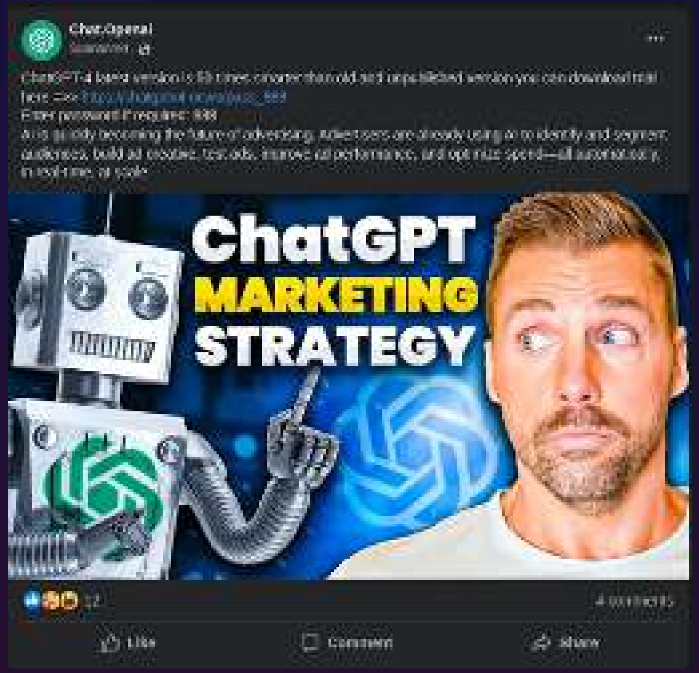


DARKReading

Infostealer Malware Market Booms, as MFA Fatigue Sets In

The successful combo of stolen credentials and social engineering to breach networks is increasing demand for infostealers on the Dark Web.

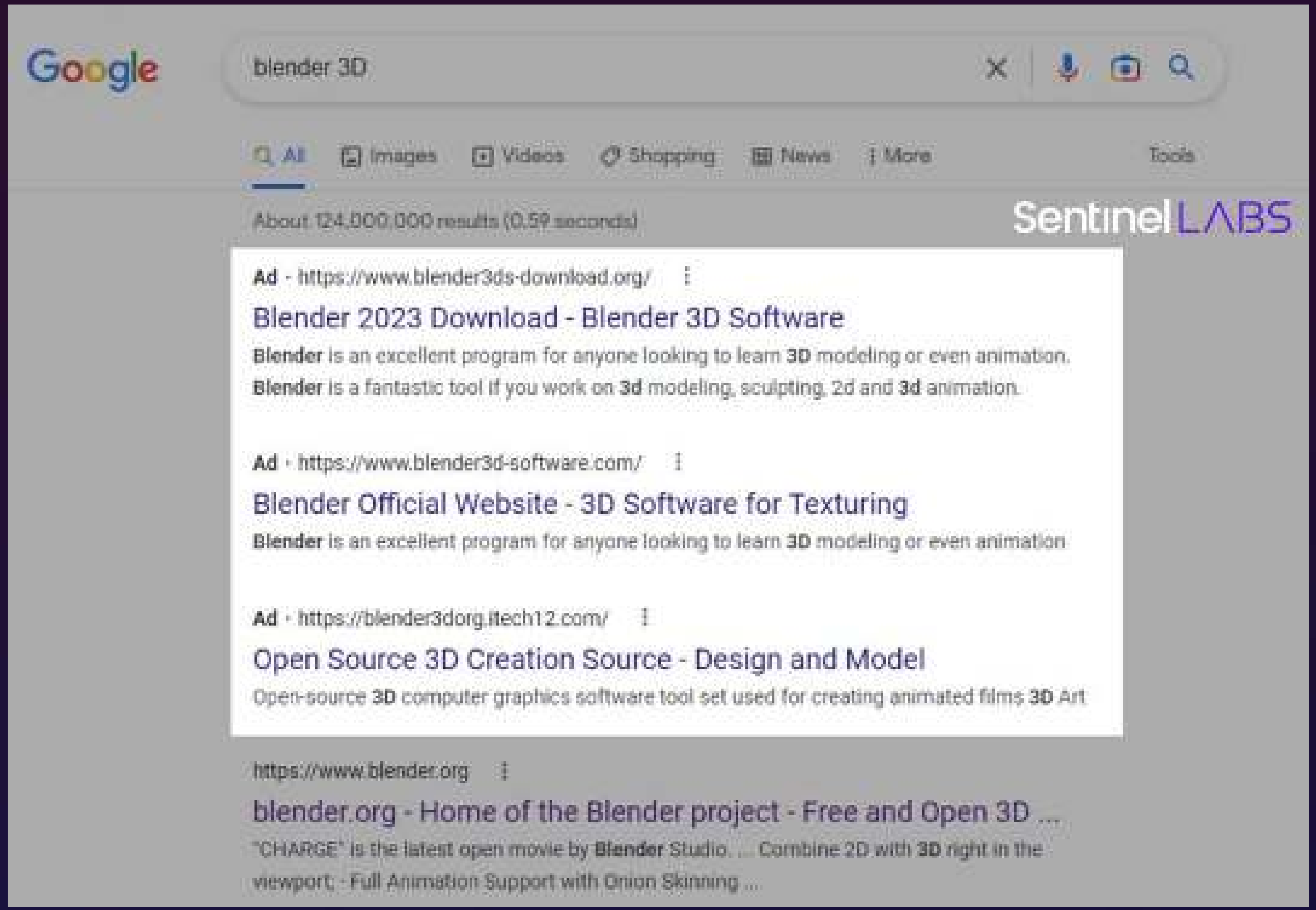
https://www.darkreading.com/application-security/ai-creating-compelling-youtube-videos-loaded-with-malware-
https://www.darkreading.com/threat-intelligence/infostealer-malware-market-booms-mfa-fatigue
https://www.sentinelone.com/blog/breaking-down-the-seo-poisoning-attack-how-attackers-are-hijacking-search-results/
https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/



Chat.Openai
Sponsored

ChatGPT-4 latest version is 59 times smarter than old and unpublished version you can download trial here ==> [illegible]
Enter password if required: 888
AI is quickly becoming the future of advertising. Advertisers are already using AI to identify and segment audiences, build ad creative, test ads, improve ad performance, and optimize spend—all automatically, in real time, at scale.

Malicious Facebook ads pretending legitimate



About 124,000,000 results (0.59 seconds)

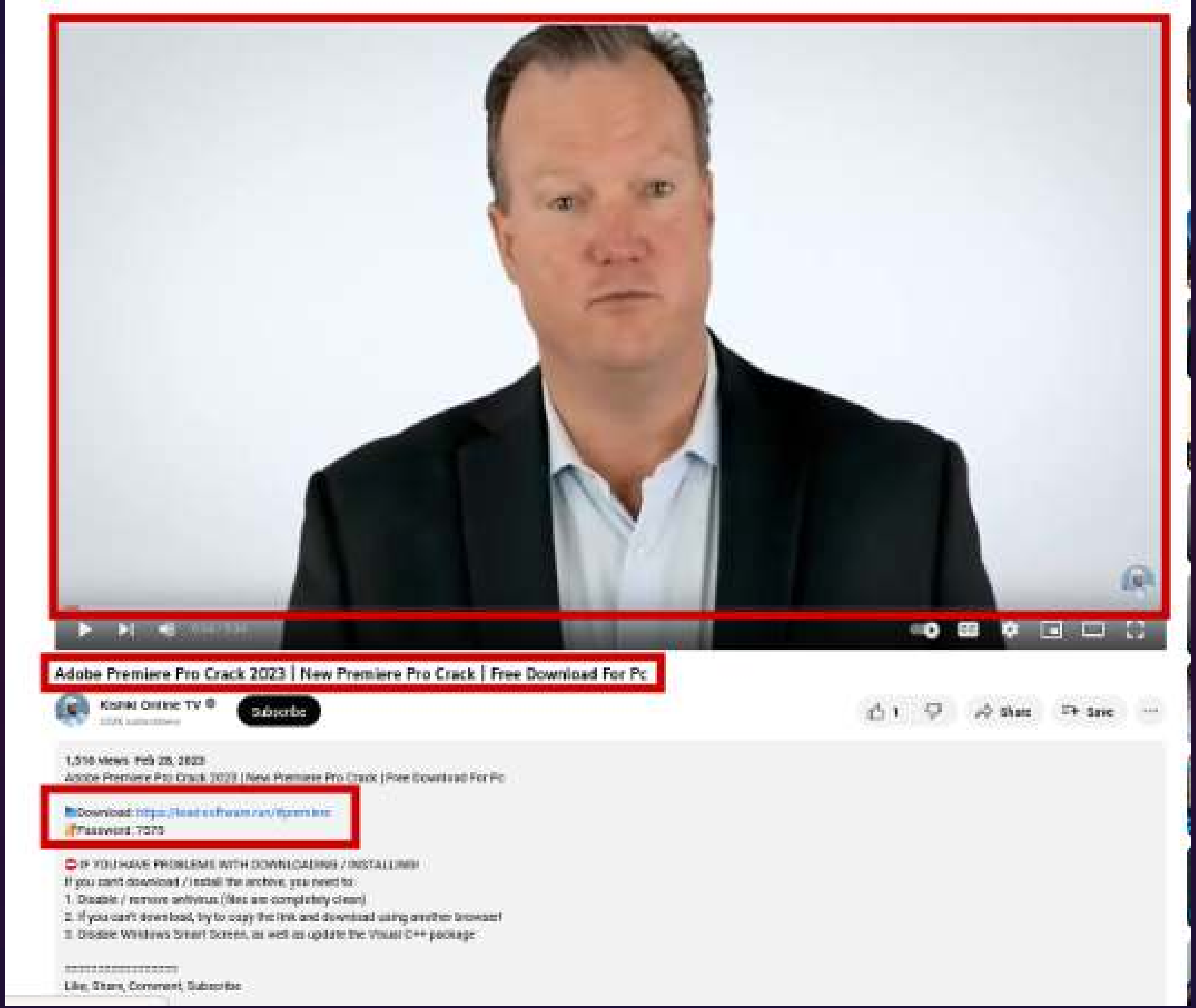
Ad · https://www.blender3ds-download.org/
Blender 2023 Download - Blender 3D Software
Blender is an excellent program for anyone looking to learn **3D** modeling or even animation. **Blender** is a fantastic tool if you work on **3d** modeling, sculpting, 2d and **3d** animation.

Ad · https://www.blender3d-software.com/
Blender Official Website - 3D Software for Texturing
Blender is an excellent program for anyone looking to learn **3D** modeling or even animation

Ad · https://blender3dorg.itech12.com/
Open Source 3D Creation Source - Design and Model
Open-source **3D** computer graphics software tool set used for creating animated films **3D** Art

https://www.blender.org
blender.org - Home of the Blender project - Free and Open 3D ...
"CHARGE" is the latest open movie by **Blender** Studio. ... Combine 2D with **3D** right in the viewport. · Full Animation Support with Onion Skinning ...

Malicious Google Search results (Sentinel Labs)



Adobe Premiere Pro Crack 2023 | New Premiere Pro Crack | Free Download For Pc

Kishki Online TV

1,516 views Feb 28, 2023

Adobe Premiere Pro Crack 2023 | New Premiere Pro Crack | Free Download For Pc

Download: https://load-software.ru/#premiere

Password: 7575

IF YOU HAVE PROBLEMS WITH DOWNLOADING / INSTALLING!

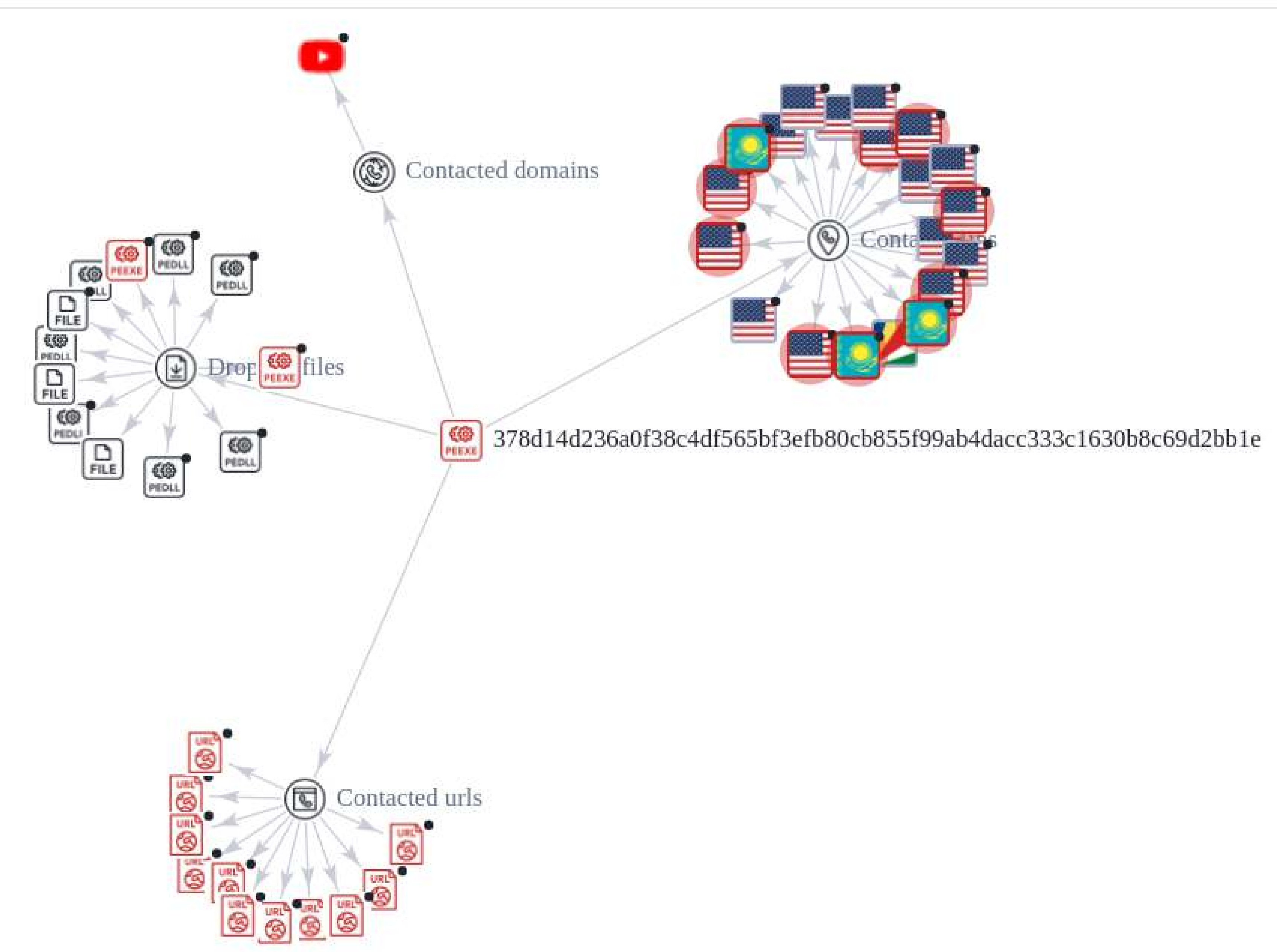
If you can't download / install the archive, you need to:

1. Disable / remove antivirus (files are completely clean)
2. If you can't download, try to copy the link and download using another browser!
3. Disable Windows Smart Screen, as well as update the Visual C++ package

==================

Like, Share, Comment, Subscribe

AI-Generated YouTube videos contain links to information-stealing malware such as Vidar, RedLine, and Raccoon.



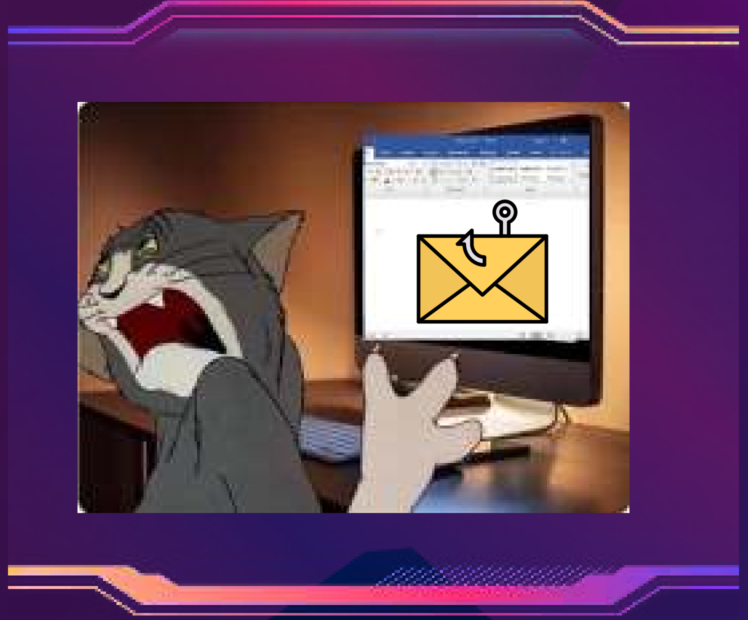
VT-Graph shows the contacted domains that have been interacted with by the malware and also malicious files that have been downloaded.

https://www.spiceworks.com/it-security/cyber-risk-management/news/youtube-malware-distribution/amp/

DEMO TIME

Typical Malware infection sequence

Victim's perspective



Threat actor's perspective

Information Stealer Malware

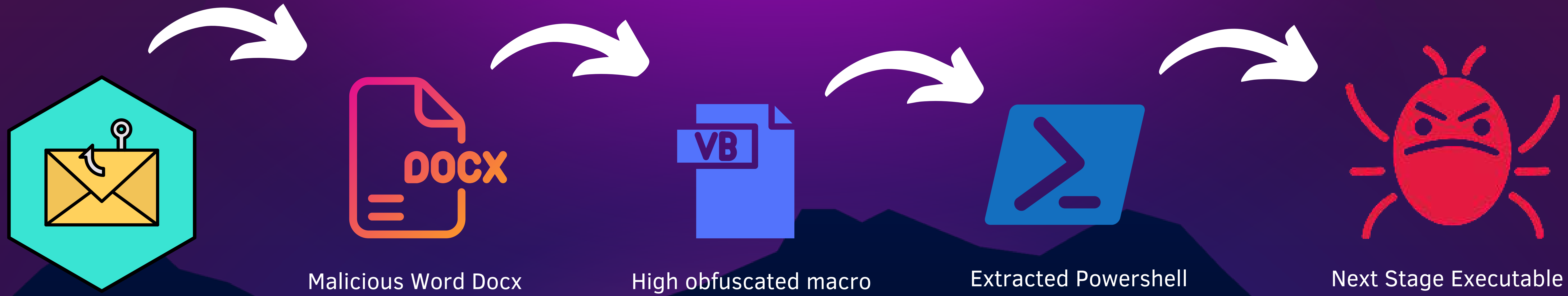
Racoon Stealer

Redline Stealer

https://blog.qualys.com/vulnerabilities-threat-research/2022/05/08/ursnif-malware-banks-on-news-events-for-phishing-attacks
https://malpedia.caad.fkie.fraunhofer.de/details/win.raccoon
https://any.run/cybersecurity-blog/raccoon-stealer-v2-malware-analysis/
https://cyberint.com/blog/research/redline-stealer/

RECAP DEMO TIME

Infection chain scenario
Malicious Word Document Pathway



Phishing Email

Malicious Word Docx
(Macro enabled)

High obfuscated macro
- Macro Executed by AutoOpen() Function.
- Macro decrypts PS script.

Extracted Powershell
Downloads/extract
next stage

Next Stage Executable
- Another malicious payload
- Malware downloads more malware from Control Server

https://malpedia.caad.fkie.fraunhofer.de/details/win.raccoon
https://any.run/cybersecurity-blog/raccoon-stealer-v2-malware-analysis/
https://cyberint.com/blog/research/redline-stealer/

RECAP DEMO TIME

Blue team

Performs :
Malware Triage and gather
Indicator of Compromise (IOCs)

Tools used:

- Windows 10 FlareVM
  - Wireshark
  - procexp
  - Sublimetext

Red Team

Performs :
Simulate the attack
Crafted a Malicious Document
and malicious payload.
Setup a Meterpreter listener.

Tools used:

- Parrot OS
  - Metasploit Framework.
  - MSF venom.
  - Python HTTP.
  - Powershell scripts.

3 Phase Cybersecurity Roadmap

Year One: The Fundamentals

Windows/Linux

- Install, Configure, Adminster
- Windows Internals
- Secure and Harden
  - CIS Benchmarks

Virtualization

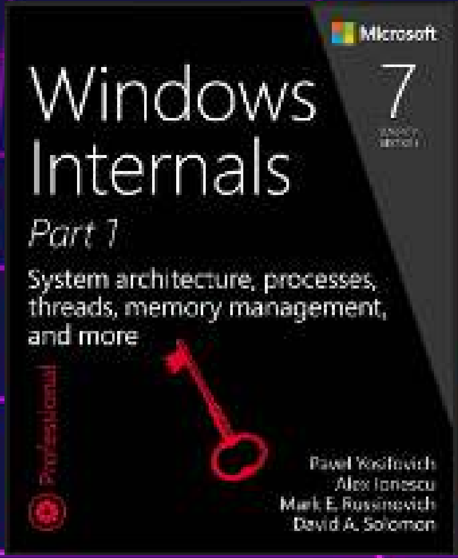
- Basics of Virtualization
- Virtualbox/Vmware/QEMU

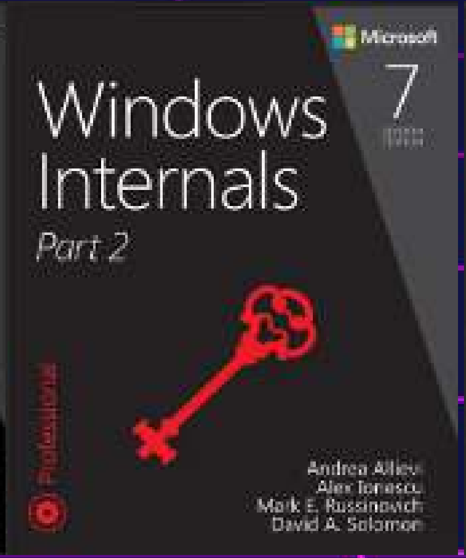
Operating Systems

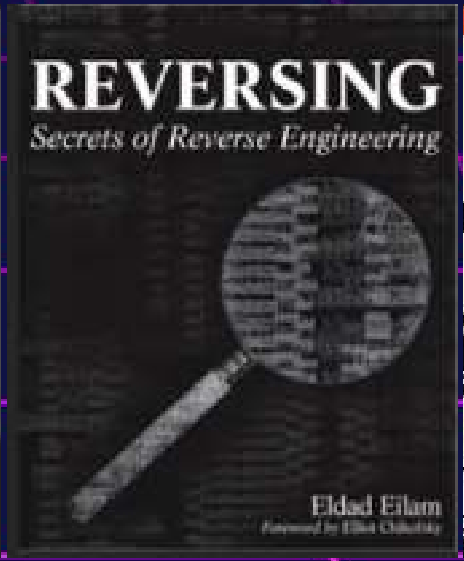
Links:

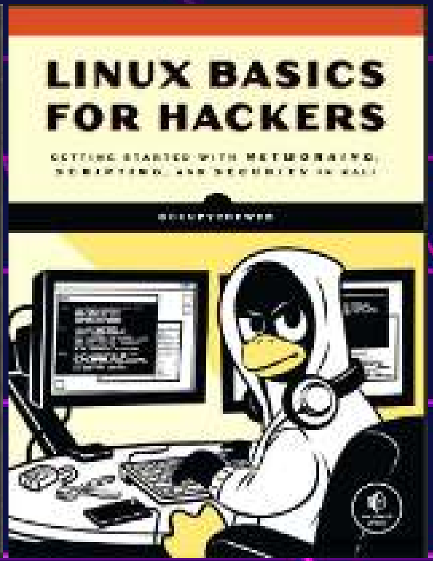
- https://tryhackme.com/room/linuxfundamentalspart1
- https://tryhackme.com/room/windowsfundamentals1xbx
- https://www.ibm.com/topics/virtual-machines
- https://linuxjourney.com/
- https://www.debian.org/doc/manuals/debian-handbook/index.en.html
- https://docs.microsoft.com/en-us/sysinternals/
- https://www.cisecurity.org/cis-benchmarks

Books:









https://www.blackhillsinfosec.com/webcast-5-year-plan-infosec/

Year One: The Fundamentals

Networking and Web Development

OSI/TCP Model

- Understand the layers make up the model.
- Common protocols like HTTP, SSH, FTP, SMB, SMTP etc.

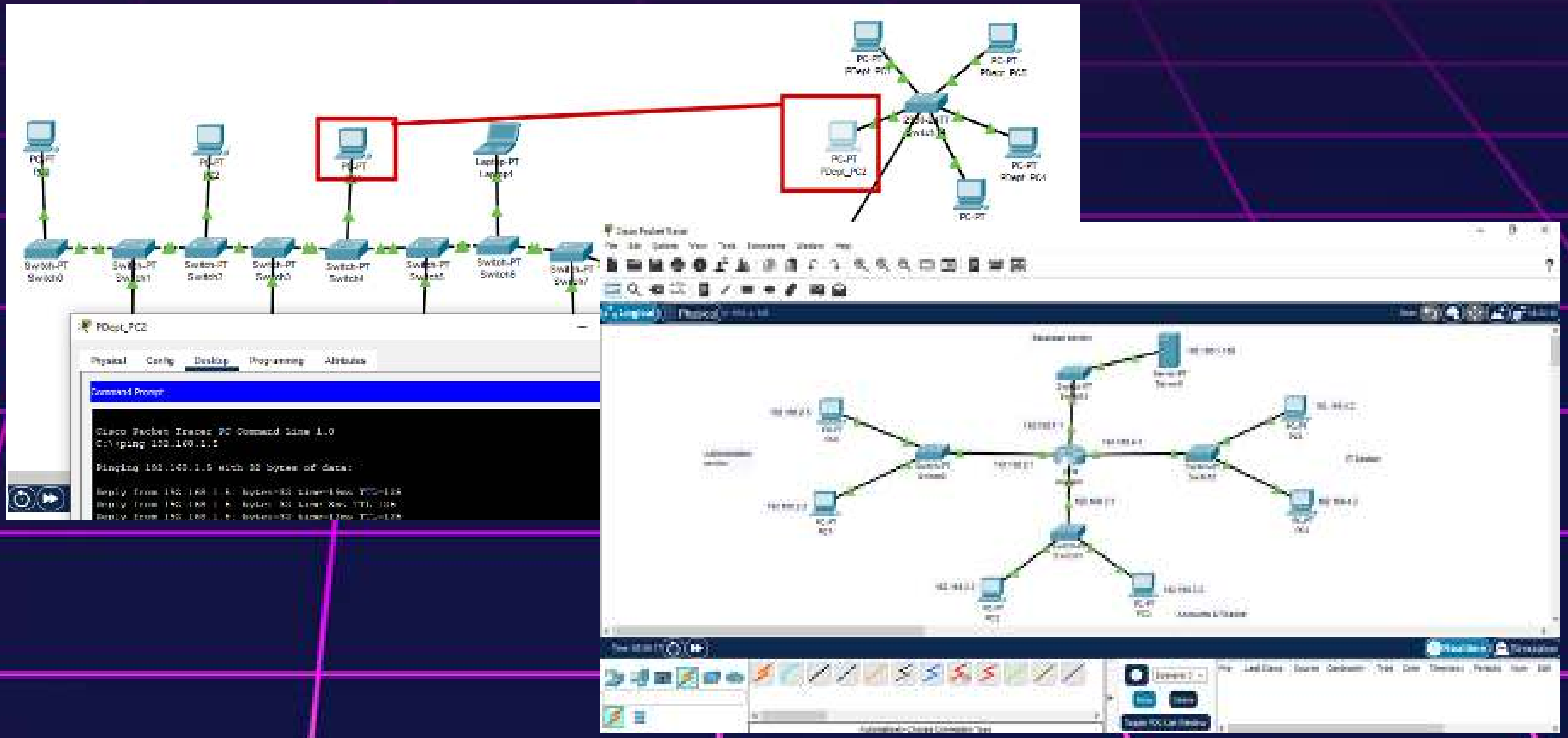
Web Development

- HTML, CSS, Javascript
- Web stacks: LAMP,MERN, Django, ASP.NET, etc.

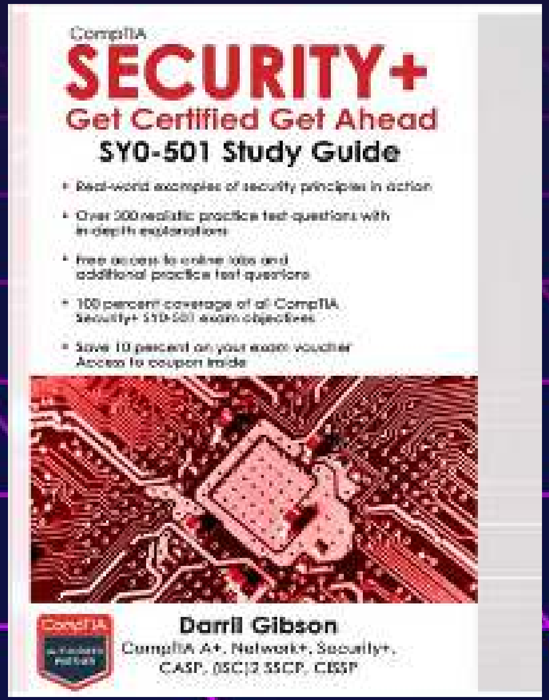
CSS HTML

Links:

- https://www.softwaretestinghelp.com/computer-networking-basics/
- https://www.guru99.com/data-communication-computer-network-tutorial.html
- https://www.netacad.com/courses/packet-tracer
- https://skillsforall.com/course/exploring-networking-cisco-packet-tracer
- https://www.netacad.com/courses/networking
- https://www.freecodecamp.org/



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=[illegible] TTL=128
Reply from 192.168.1.5: bytes=32 time=[illegible] TTL=128
Reply from 192.168.1.5: bytes=32 time=[illegible] TTL=128
```



CompTIA
SECURITY+
Get Certified Get Ahead
SY0-501 Study Guide

- Real-world examples of security principles in action
- Over 300 realistic practice test questions with in-depth explanations
- Free access to online labs and additional practice test questions
- 100 percent coverage of all CompTIA Security+ SY0-501 exam objectives
- Save 10 percent on your exam voucher Access to coupon inside

Darril Gibson
CompTIA A+, Network+, Security+, CASP, (ISC)2 SSCP, CISSP

Year One: The Fundamentals

Programming skills and Knowledge

- Powershell/bash scripts
    - Automate your daily tasks
- Start Simple with Python
- Go
- Javascript
- C++
- Develops intuition

Programming languages

Links:

- https://learn-bash.org/
- https://www.learnpython.org/
- https://www.learn-c.org/
- https://www.learn-cpp.org/
- https://nodejs.dev/en/learn/
- https://dev.java/learn/
- https://learn.microsoft.com/en-us/training/modules/introduction-to-powershell/

Books:

2ND EDITION
HACKING
THE ART OF EXPLOITATION
JON ERICKSON
Black Hat Go
Go Programming for Hackers and Pentesters
2ND EDITION
Black Hat Python
Python Programming for Hackers and Pentesters
CORY ALTHOFF
the self-taught
PROGRAMMER
the definitive guide to programming professionally
2ND EDITION
AUTOMATE THE BORING STUFF WITH PYTHON
PRACTICAL PROGRAMMING FOR TOTAL BEGINNERS
AL SWEIGART

https://www.blackhillsinfosec.com/webcast-5-year-plan-infosec/

Year Two: Cybersecurity Concepts

Security Concepts

- Information Security Terminologies
- CIA Triad Model
- Attacks, threats, vulnerabilities, risk

Security Standards

- National Information Security Technology (NIST) Standard Specification
  - RMF
  - Cybersecurity Framework
- CIS (Center for Internet Security)

Security Fundamentals

Links:

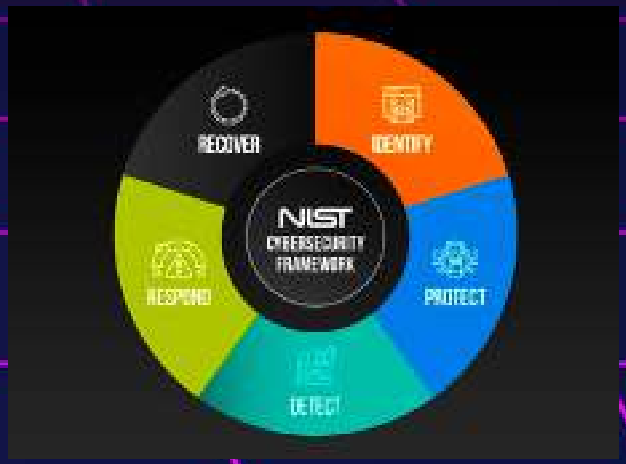
- https://csrc.nist.gov/glossary
- https://www.nist.gov/cyberframework
- https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html
- https://www.cisecurity.org
- https://owasp.org/Top10/

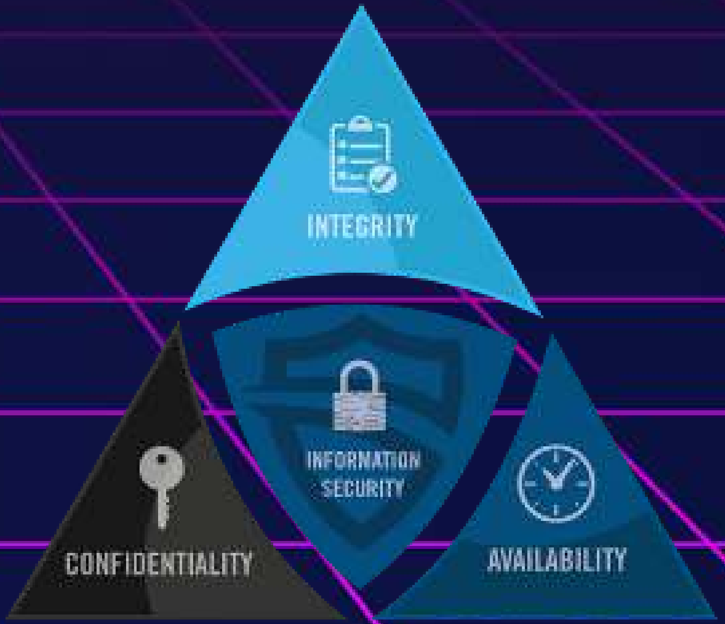
NIST SP 800-53 R5 HIGH BASELINE

SCF SECURE CONTROLS FRAMEWORK

NIST CYBERSECURITY FRAMEWORK

ISO ISO 27001 / 27002





https://allabouttesting.org/complete-list-of-cyber-security-standards/

Year Two: Cybersecurity Concepts

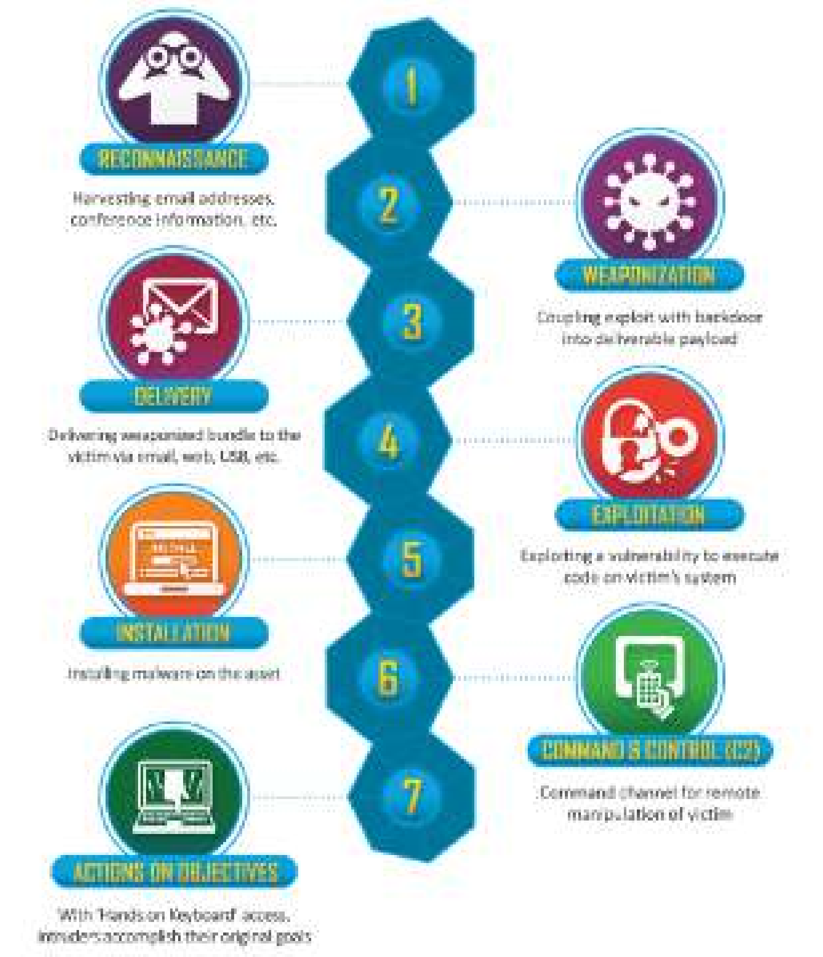
Pentesting Fundamentals

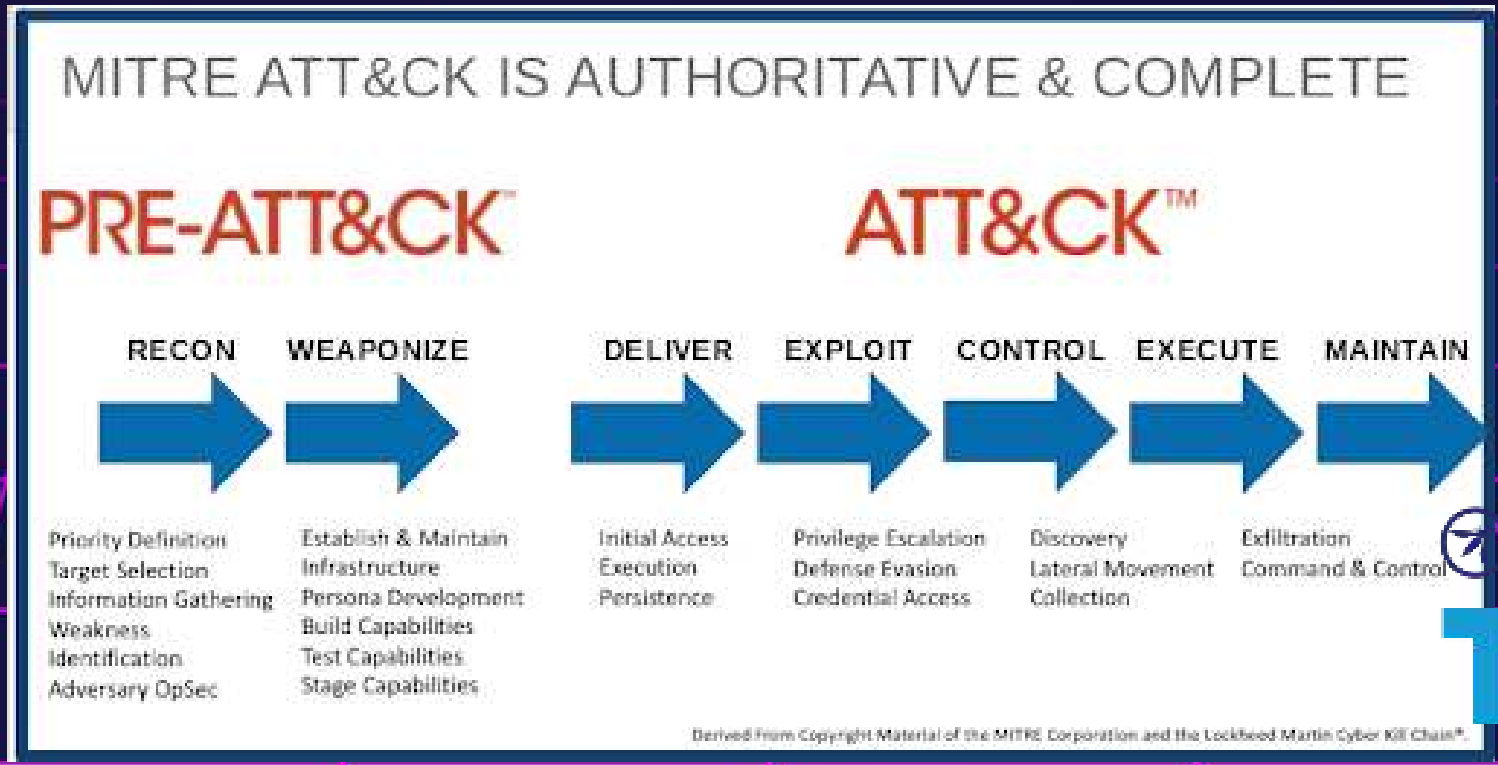
- PTES
- MITRE ATTACK
- Cyber Kill Chain
- OWASP Top 10
- OWASP Security Testing Guide
- Analyze open source reports pentest
- Understand Common Security suite and tools.

Frameworks/Methodology

Links:

- http://www.pentest-standard.org/index.php/Main_Page
- https://attack.mitre.org/
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.unifiedkillchain.com/
- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- https://owasp.org/www-project-top-ten/
- https://github.com/Sector443/awesome-list-of-public-pentesting-reports


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals



MITRE ATT&CK IS AUTHORITATIVE & COMPLETE

PRE-ATT&CK™		ATT&CK™				
RECON	WEAPONIZE	DELIVER	EXPLOIT	CONTROL	EXECUTE	MAINTAIN
Priority Definition Target Selection Information Gathering Weakness Identification Adversary OpSec	Establish & Maintain Infrastructure Persona Development Build Capabilities Test Capabilities Stage Capabilities	Initial Access Execution Persistence	Privilege Escalation Defense Evasion Credential Access	Discovery Lateral Movement Collection	Exfiltration Command & Control	

Derived From Copyright Material of the MITRE Corporation and the Lockheed Martin Cyber Kill Chain®.

https://www.blackhillsinfosec.com/webcast-5-year-plan-infosec/

Year three: Getting hands dirty

Attack & Defend

- Approach your learning with directness.
  - Gain an understanding of how adversaries operate and how to detect them. (Adversary Simulation)
  - Learn how Malware Operates and Types
  - Setup vulnerable server and attack it.
- CTFs
  - Participate, Identify your weak spots and improve!

Autodidact learning + Practice

Links:

- https://book.hacktricks.xyz/welcome/readme
- https://portswigger.net/web-security
- https://github.com/digininja/DVWA
- https://www.vulnhub.com/
- https://github.com/ashemery/exploitation-course
- https://github.com/redcanaryco/atomic-red-team

Practices on platforms:

VULNHUB
VULNERABLE BY DESIGN

Try Hack Me

picoCTF

HACKTHEBOX

Year four: Career hunt

Connect with professionals in the industry and submit a job application.

- LinkedIn, JobStreet, Facebook groups, university career fairs, webinars, and conferences.
- Volunteer works in Org
- Create a personal project, publish writeups, showcase your talent.
- Create a meaningful connection.
  - 50 meaningful > 1000 connections in linkedin
- Softskills Don't forget it ;)

Plaforms:

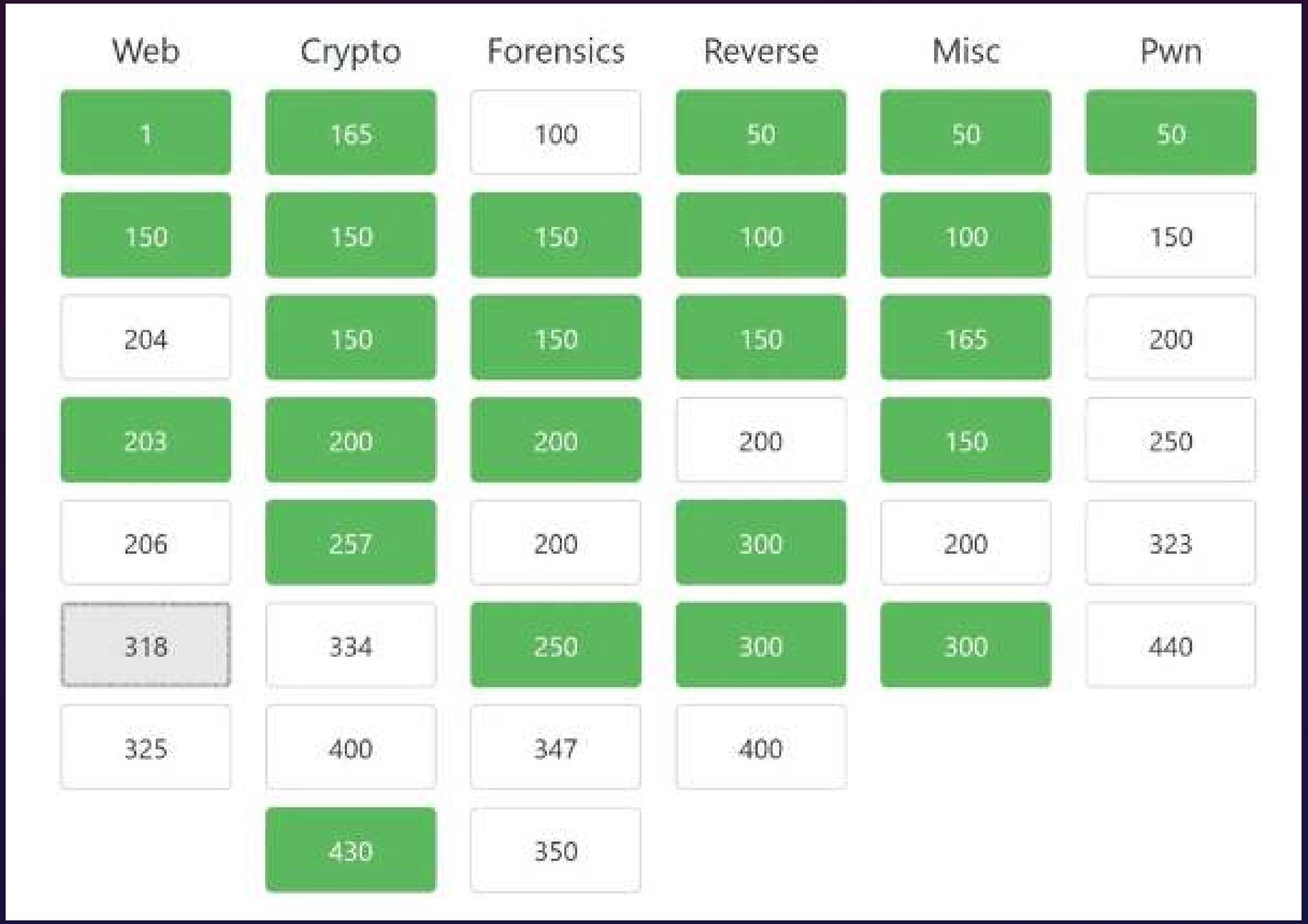
indeed®

JobStreet.com

CTF: How the Best Hackers Learn Their Craft

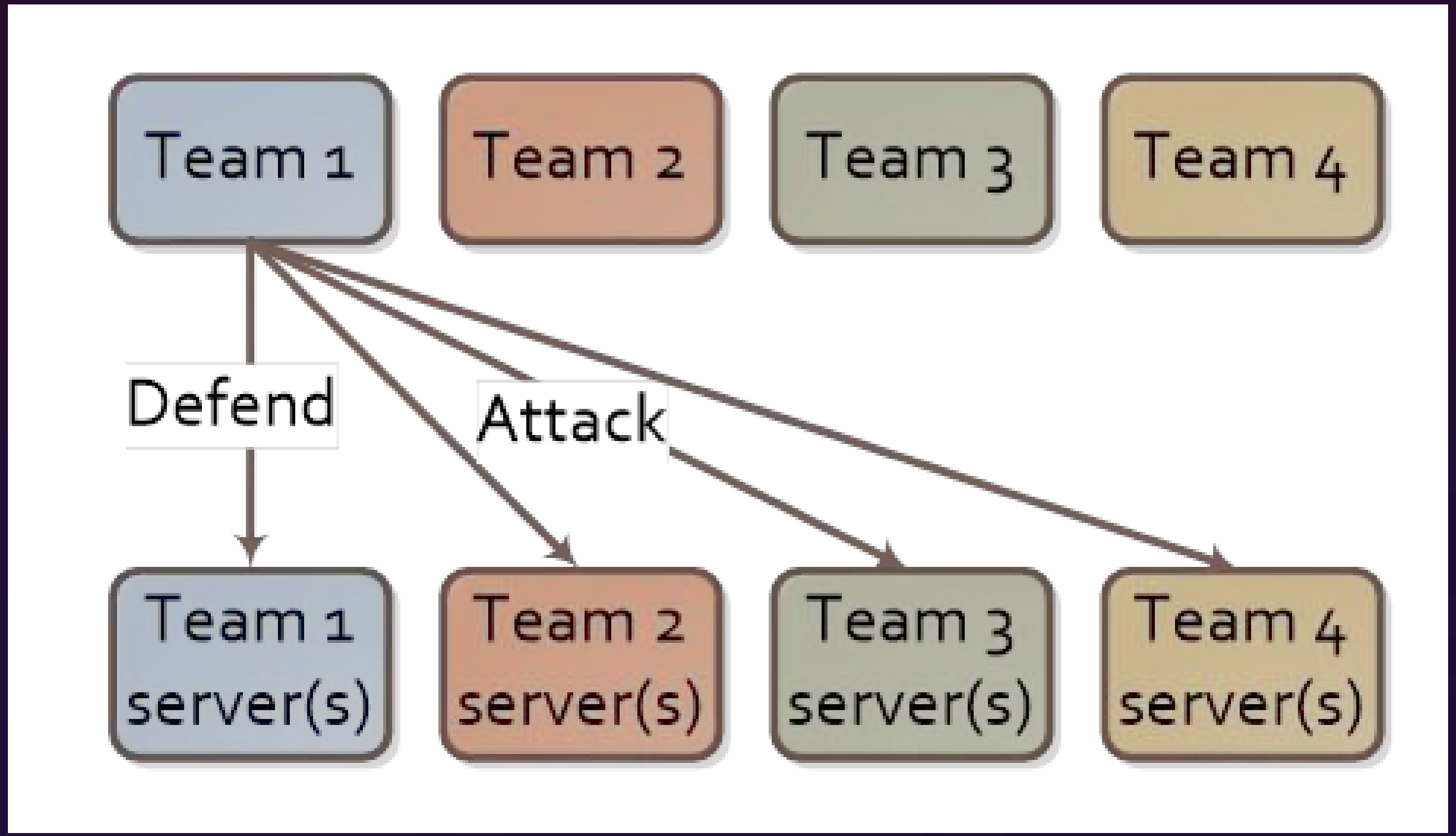
Capture The Flag 101

Jeopardy Style



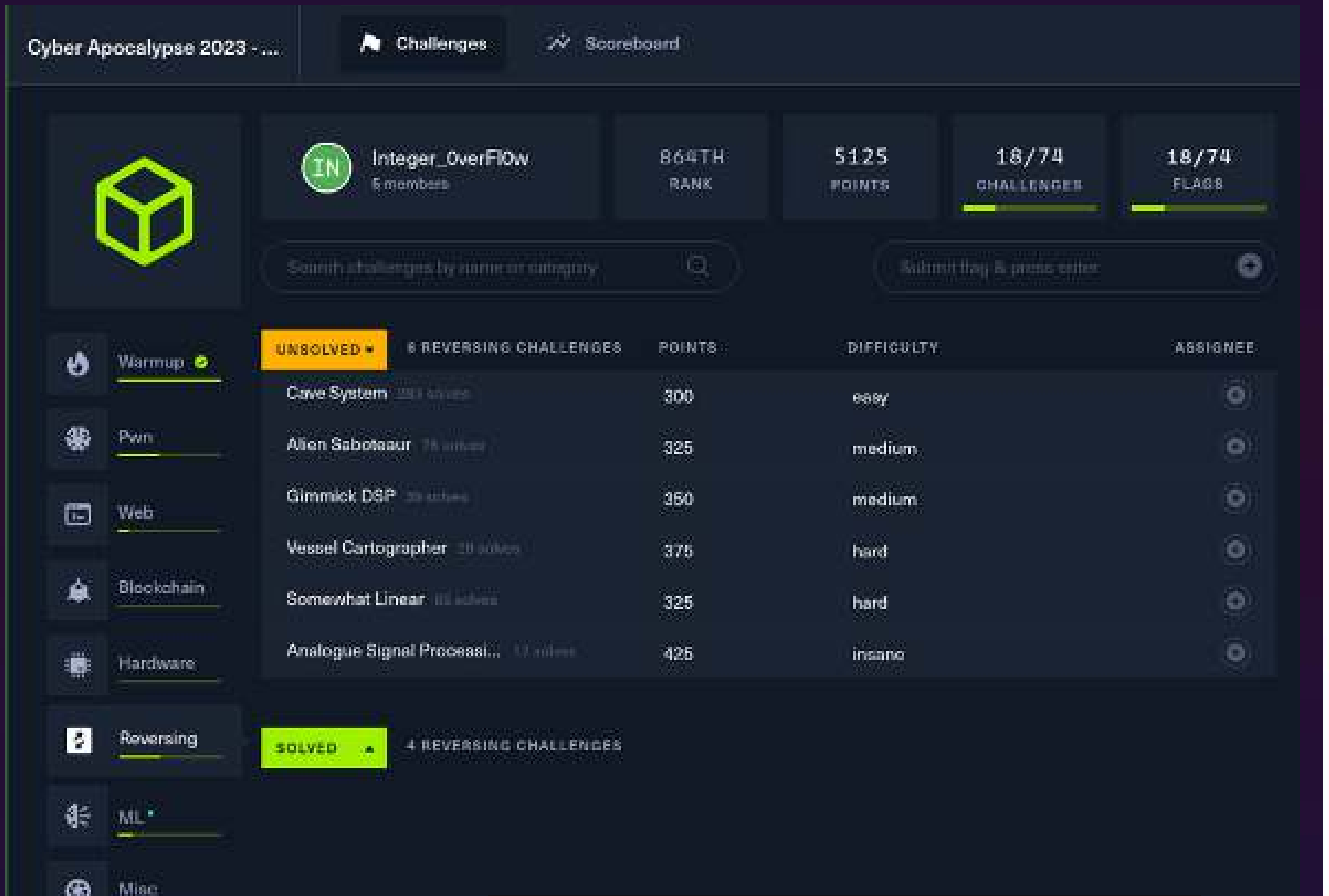
Web	Crypto	Forensics	Reverse	Misc	Pwn
1	165	100	50	50	50
150	150	150	100	100	150
204	150	150	150	165	200
203	200	200	200	150	250
206	257	200	300	200	323
318	334	250	300	300	440
325	400	347	400		
	430	350			

Attack-Defense



https://ctf101.org/

Typical Jeopardy CTF Page



Cyber Apocalypse 2023 - ...

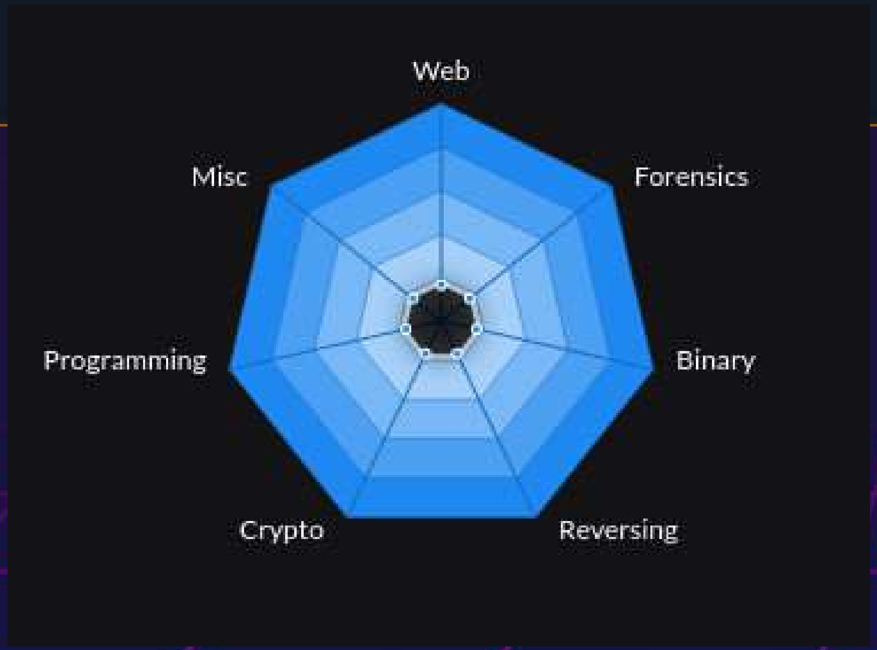
Integer_OverFl0w
5 members

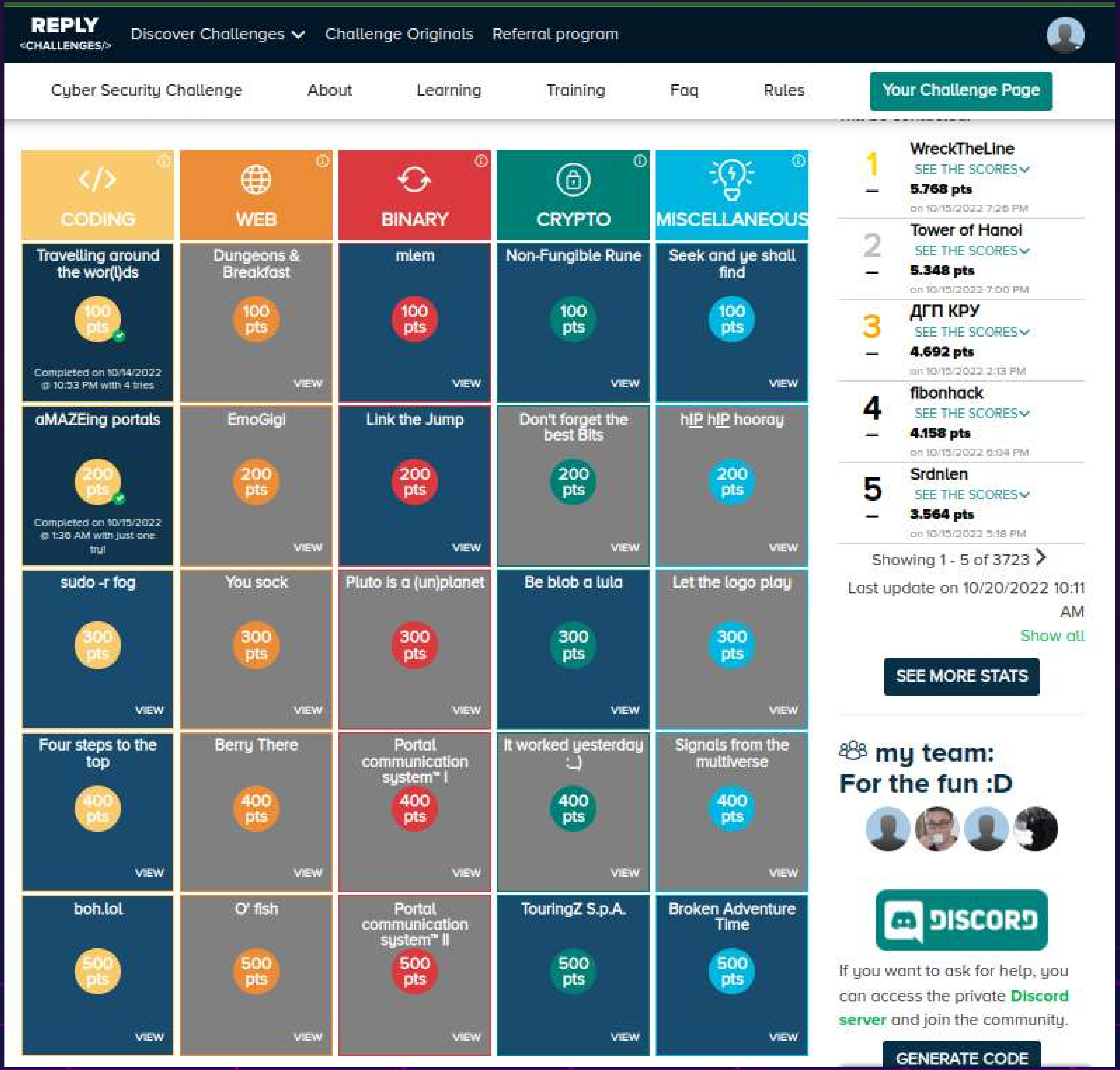
864TH	5125	18/74	18/74
RANK	POINTS	CHALLENGES	FLAGS

Search challenges by name or category
Submit flag & press enter
Warmup
Pwn
Web
Blockchain
Hardware
Reversing
ML
Misc
Show More

UNSOLVED ▾ 6 REVERSING CHALLENGES	POINTS	DIFFICULTY	ASSIGNEE
Cave System 233 solves	300	easy	
Alien Saboteaur 78 solves	325	medium	
Gimmick DSP 39 solves	350	medium	
Vessel Cartographer 20 solves	375	hard	
Somewhat Linear 65 solves	325	hard	
Analogue Signal Processi... 17 solves	425	insane	

SOLVED ▴ 4 REVERSING CHALLENGES





CODING	WEB	BINARY	CRYPTO	MISCELLANEOUS
Travelling around the wor(l)ds 100 pts Completed on 10/14/2022 @ 10:53 PM with 4 tries	Dungeons & Breakfast 100 pts VIEW	mlem 100 pts VIEW	Non-Fungible Rune 100 pts VIEW	Seek and ye shall find 100 pts VIEW
aMAZEing portals 200 pts Completed on 10/15/2022 @ 1:36 AM with just one try!	EmoGigi 200 pts VIEW	Link the Jump 200 pts VIEW	Don't forget the best Bits 200 pts VIEW	hIP hIP hooray 200 pts VIEW
sudo -r fog 300 pts VIEW	You sock 300 pts VIEW	Pluto is a (un)planet 300 pts VIEW	Be blob a lula 300 pts VIEW	Let the logo play 300 pts VIEW
Four steps to the top 400 pts VIEW	Berry There 400 pts VIEW	Portal communication system™ I 400 pts VIEW	It worked yesterday :_) 400 pts VIEW	Signals from the multiverse 400 pts VIEW
boh.lol 500 pts VIEW	O' fish 500 pts VIEW	Portal communication system™ II 500 pts VIEW	TouringZ S.p.A. 500 pts VIEW	Broken Adventure Time 500 pts VIEW

1	WreckTheLine	SEE THE SCORES 5.768 pts on 10/15/2022 7:26 PM
2	Tower of Hanoi	SEE THE SCORES 5.348 pts on 10/15/2022 7:00 PM
3	ДГП КРУ	SEE THE SCORES 4.692 pts on 10/15/2022 2:13 PM
4	fibonhack	SEE THE SCORES 4.158 pts on 10/15/2022 6:04 PM
5	Srdnlen	SEE THE SCORES 3.564 pts on 10/15/2022 5:18 PM

Showing 1 - 5 of 3723

Last update on 10/20/2022 10:11 AM

Show all

SEE MORE STATS

my team:
For the fun :D

DISCORD

If you want to ask for help, you can access the private Discord server and join the community.

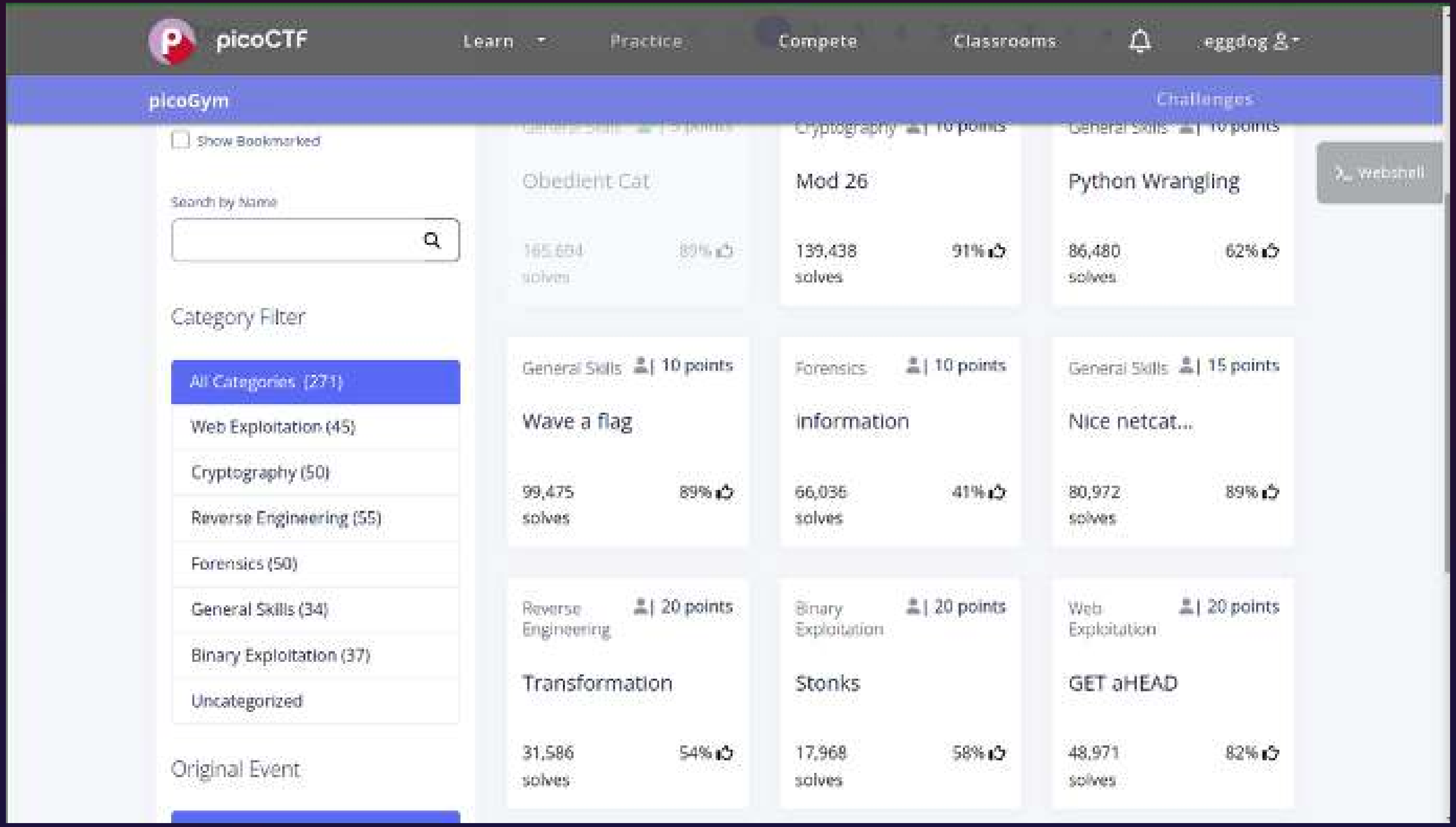
GENERATE CODE

Gamified learning

https://ctf101.org/

Where to find these CTF

PicoCTF



picoCTF Learn Practice Compete Classrooms eggdog

picoGym Challenges

□ Show Bookmarked

Search by Name

Category Filter

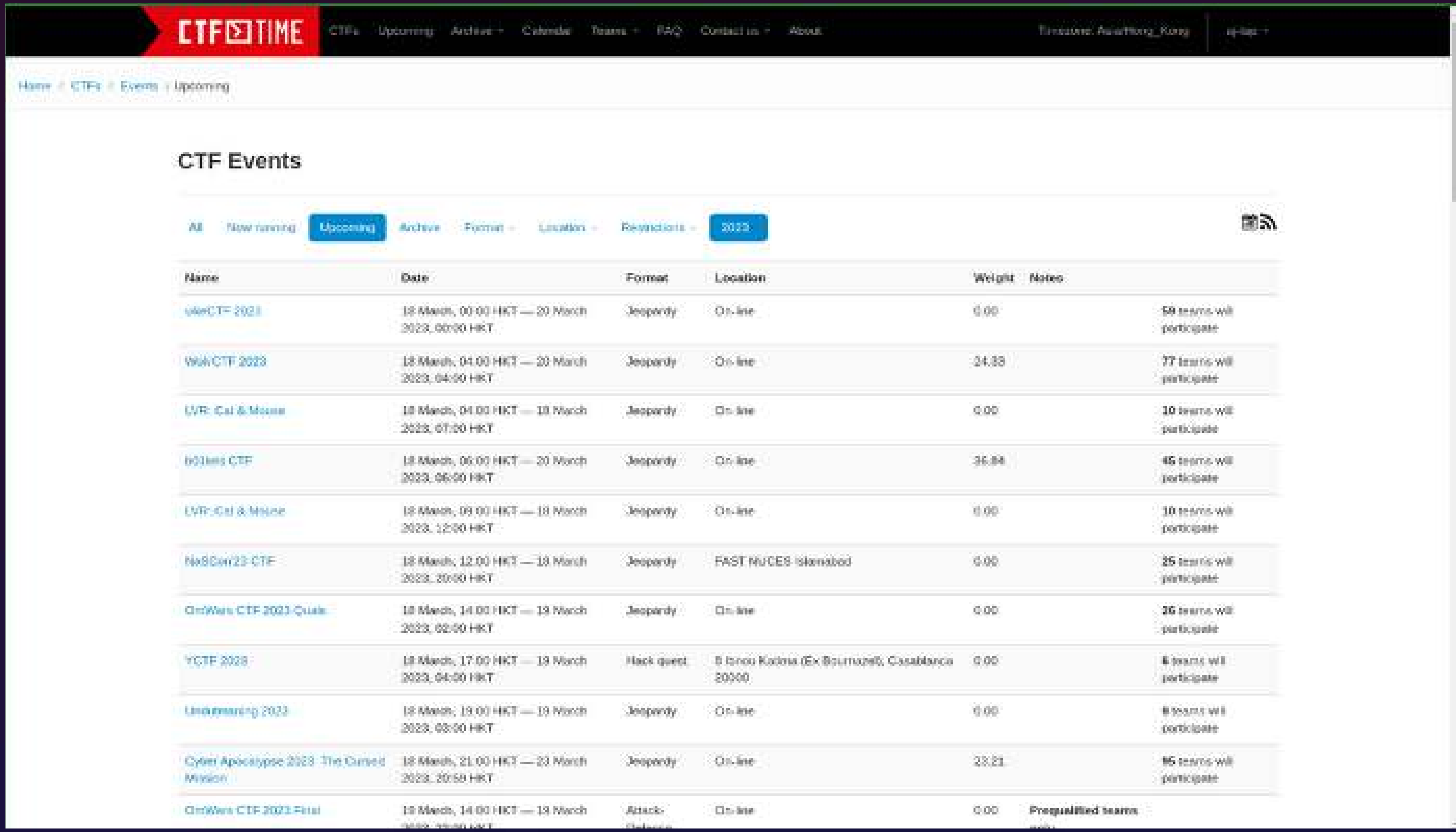
- All Categories (271)
- Web Exploitation (45)
- Cryptography (50)
- Reverse Engineering (55)
- Forensics (50)
- General Skills (34)
- Binary Exploitation (37)
- Uncategorized

Original Event

Webshell

Category	Points	Name	Solves	Rating
General Skills	5 points	Obedient Cat	165,604 solves	89%
Cryptography	10 points	Mod 26	139,438 solves	91%
General Skills	10 points	Python Wrangling	86,480 solves	62%
General Skills	10 points	Wave a flag	99,475 solves	89%
Forensics	10 points	information	66,036 solves	41%
General Skills	15 points	Nice netcat...	80,972 solves	89%
Reverse Engineering	20 points	Transformation	31,586 solves	54%
Binary Exploitation	20 points	Stonks	17,968 solves	58%
Web Exploitation	20 points	GET aHEAD	48,971 solves	82%

CTF Time



CTFTIME CTFs Upcoming Archive Calendar Teams FAQ Contact us About Timezone: Asia/Hong_Kong

Home / CTFs / Events / Upcoming

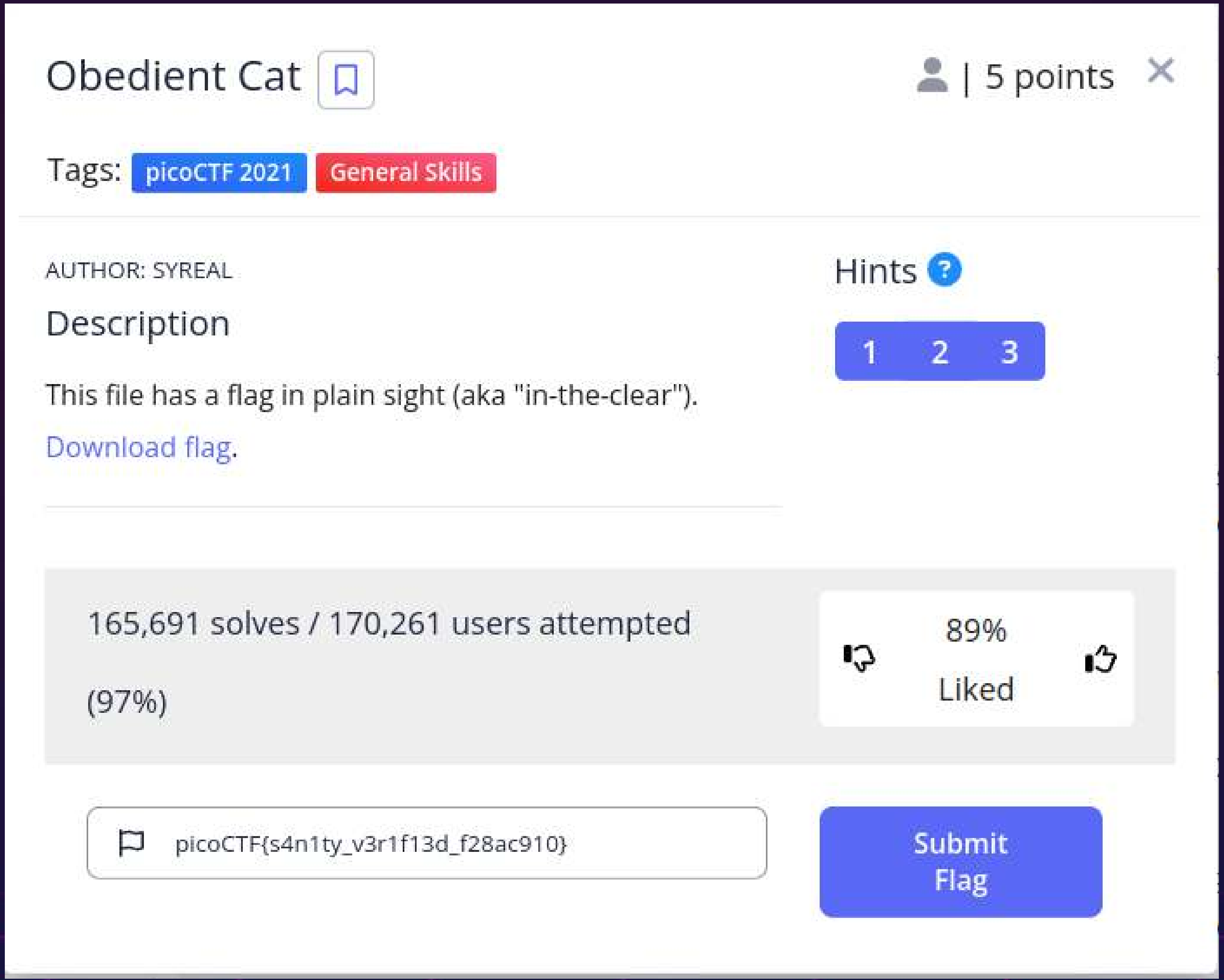
CTF Events

All Now running Upcoming Archive Format Location Restrictions 2023

Name	Date	Format	Location	Weight	Notes
ukeCTF 2023	18 March, 00:00 HKT — 20 March 2023, 00:00 HKT	Jeopardy	On-line	0.00	**59** teams will participate
WolvCTF 2023	18 March, 04:00 HKT — 20 March 2023, 04:00 HKT	Jeopardy	On-line	24.33	**77** teams will participate
LVR: Cat & Mouse	18 March, 04:00 HKT — 18 March 2023, 07:00 HKT	Jeopardy	On-line	0.00	**10** teams will participate
b01lers CTF	18 March, 06:00 HKT — 20 March 2023, 06:00 HKT	Jeopardy	On-line	36.84	**45** teams will participate
LVR: Cat & Mouse	18 March, 09:00 HKT — 18 March 2023, 12:00 HKT	Jeopardy	On-line	0.00	**10** teams will participate
NaSCon'23 CTF	18 March, 12:00 HKT — 18 March 2023, 20:00 HKT	Jeopardy	FAST NUCES Islamabad	0.00	**25** teams will participate
CitWars CTF 2023 Quals	18 March, 14:00 HKT — 19 March 2023, 02:00 HKT	Jeopardy	On-line	0.00	**26** teams will participate
YCTF 2023	18 March, 17:00 HKT — 19 March 2023, 04:00 HKT	Hack quest	8 Ibnou Kadma (Ex Bournazel), Casablanca 20000	0.00	**6** teams will participate
Undermining 2023	18 March, 19:00 HKT — 19 March 2023, 03:00 HKT	Jeopardy	On-line	0.00	**8** teams will participate
Cyber Apocalypse 2023: The Cursed Mission	18 March, 21:00 HKT — 23 March 2023, 20:59 HKT	Jeopardy	On-line	23.21	**95** teams will participate
CitWars CTF 2023 Final	18 March, 14:00 HKT — 18 March	Attack-Defense	On-line	0.00	**Prequalified teams**

https://play.picoctf.org/practice
https://ctf101.org/

CTF Examples Question



Obedient Cat

5 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

This file has a flag in plain sight (aka "in-the-clear").

Download flag.

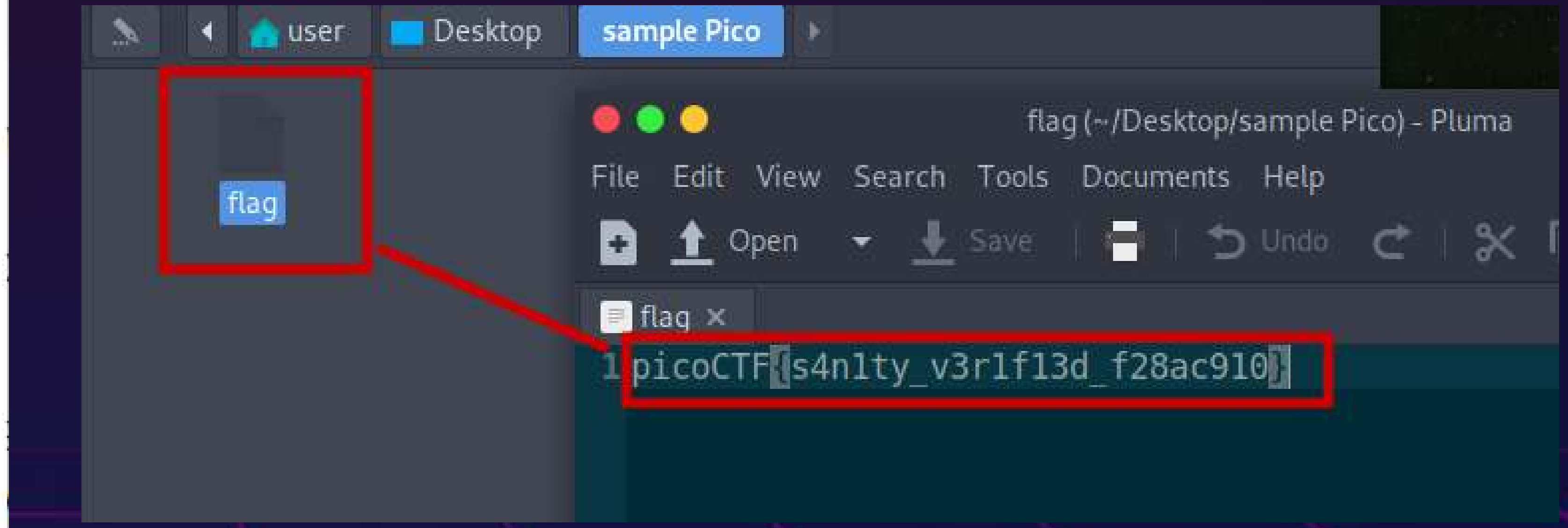
Hints

165,691 solves / 170,261 users attempted (97%)

89% Liked

picoCTF{s4n1ty_v3r1f13d_f28ac910}

- Title
- Short description
- Attachment
- Inputflag



flag (~/Desktop/sample Pico) - Pluma

flag

```
picoCTF{s4n1ty_v3r1f13d_f28ac910}
```

https://play.picoctf.org/practice

CTF SAMPLE CHALLENGE

File attachment name: WindowsXP.jpg

Category: OSINT

Description:
What information can you possible get with just one photo?

Flags to capture:

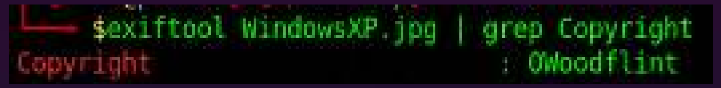
- What is this users avatar of?
- What city is this person in?
- What is his personal email address?
- What site did you find his email address on?
- Where has he gone on holiday?
- What is this persons password?

https://tryhackme.com/room/ohsint

CTF CHALLENGE RECAP

Understand the problem by researching.

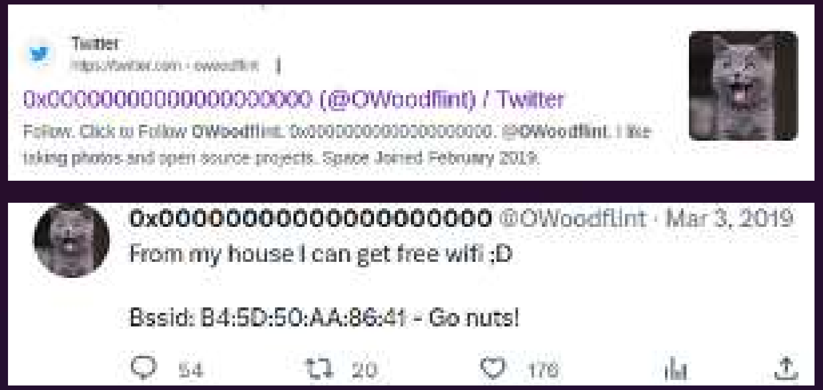
- Google
  - **We search OSINT and stumble a Methodology called OSINT framework**
  - **We learn that Photos Contains Metadata.**



```
└─ $exiftool WindowsXP.jpg | grep Copyright
Copyright                       : OWoodflint
```

Using Exiftool that we learn from OSINT framework we extract metadata of the file

- Copyright:OWoodflint



Twitter
https://twitter.com › owoodflint

0x00000000000000000000 (@OWoodflint) / Twitter

Follow. Click to Follow OWoodflint. 0x00000000000000000000. @OWoodflint. I like taking photos and open source projects. Space Joined February 2019.

0x00000000000000000000 @OWoodflint · Mar 3, 2019
From my house I can get free wifi ;D

Bssid: B4:5D:50:AA:86:41 - Go nuts!

What is this users avatar of?
Answer: Cat

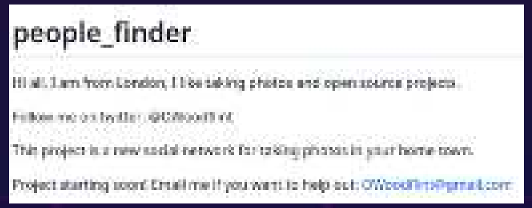
Simple google search of Owoodflint will reveal his accounts.

- He tweeted a Bssid which near in his house.

A406
London
Ilfor

What city is this person in?
Answer: London

By researching again we find out there is concept called "Wardriving" and based from OSINT Framework.
Wigle is a database of wireless access points and cell tower locations



people_finder

Hi all, I am from London, I like taking photos and open source projects.

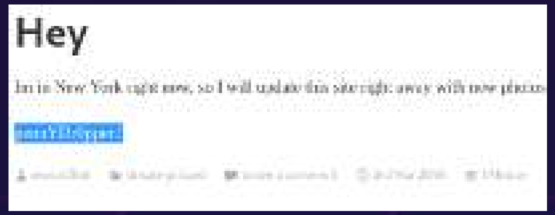
Follow me on twitter: @OWoodflint

This project is a new social network for taking photos in your home town.

Project starting soon! Email me if you want to help out: OWoodflint@gmail.com

What is his personal email address?
Answer: OWoodflint@gmail.com

Looking to his github account we can find that he accidentally leaked his email in one of repository.



Hey

Im in New York right now, so I will update this site right away with new photos

pennYDr0pper.!

What is this persons password?
Answer: pennYDr0pper.!

Where has he gone on holiday?
Answer: OWoodflint@gmail.com

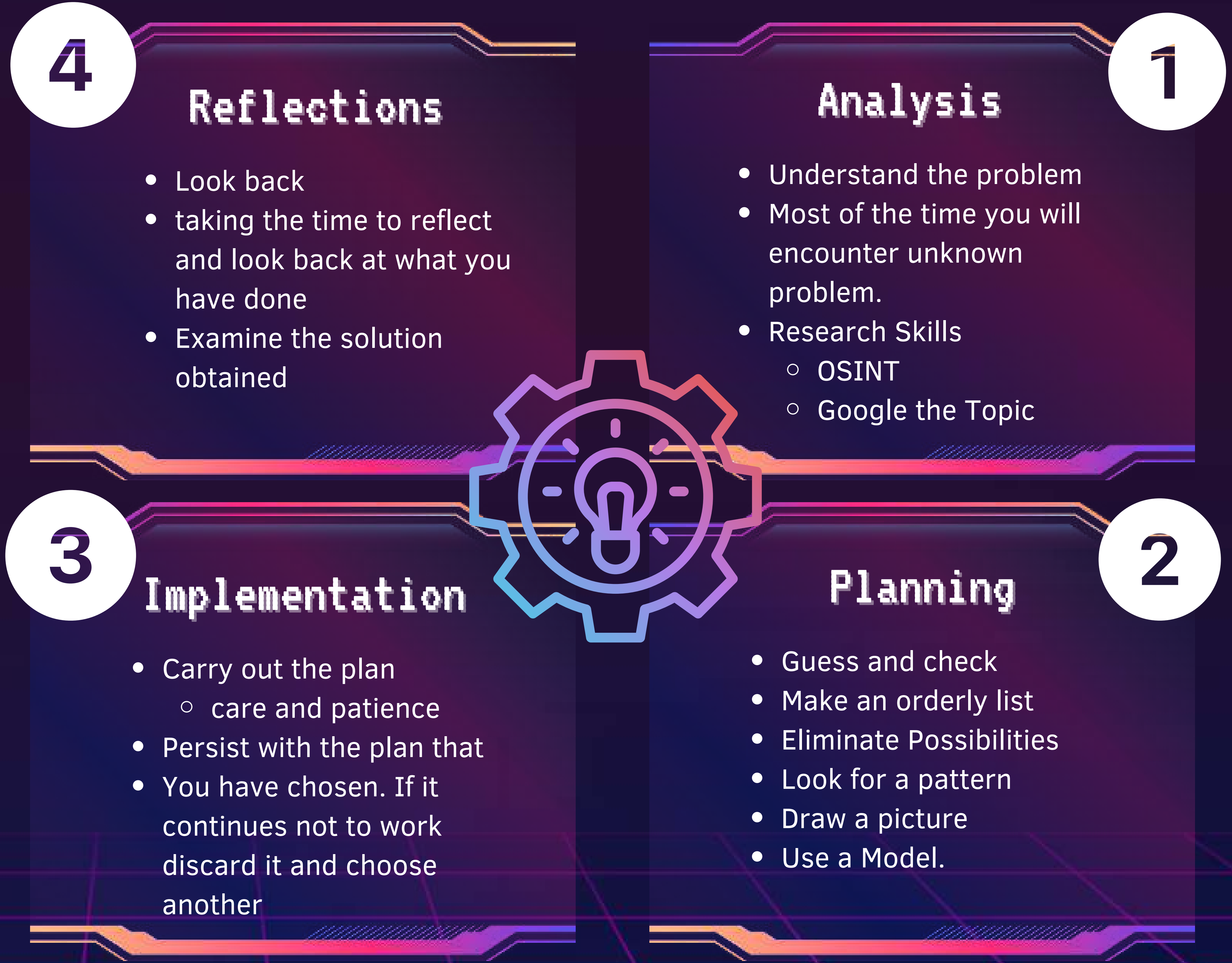
We also found his OWoodflint's wordpress flag.

While doing the problem you constantly researching new topics we don't know and learn new concepts, techniques and methodologies.

CTF Learning Process

Principles of CTF

- Applied, deliberate practice
- Autodidactic Learning
- Creative Problem solving



1

Analysis

- Understand the problem
- Most of the time you will encounter unknown problem.
- Research Skills
  - OSINT
  - Google the Topic

2

Planning

- Guess and check
- Make an orderly list
- Eliminate Possibilities
- Look for a pattern
- Draw a picture
- Use a Model.

3

Implementation

- Carry out the plan
  - care and patience
- Persist with the plan that
- You have chosen. If it continues not to work discard it and choose another

4

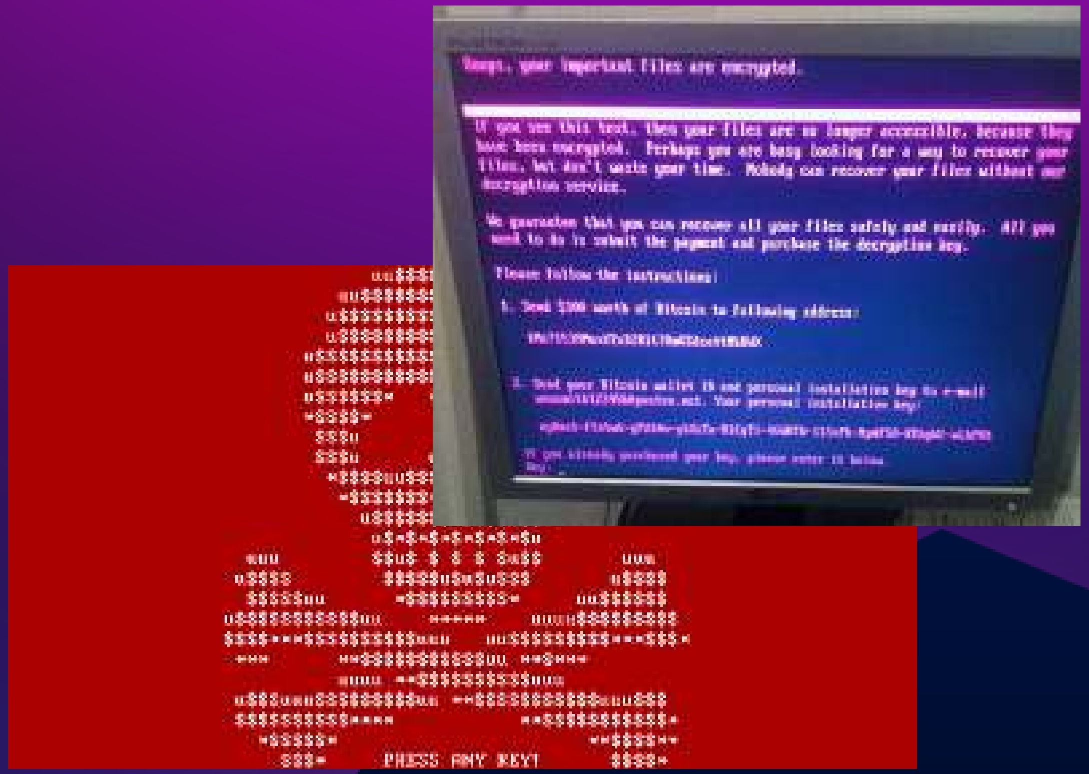
Reflections

- Look back
- taking the time to reflect and look back at what you have done
- Examine the solution obtained

https://math.berkeley.edu/~gmelvin/polya.pdf
https://www.rsaconference.com/library/presentation/how-the-best-hackers-learn-their-craft

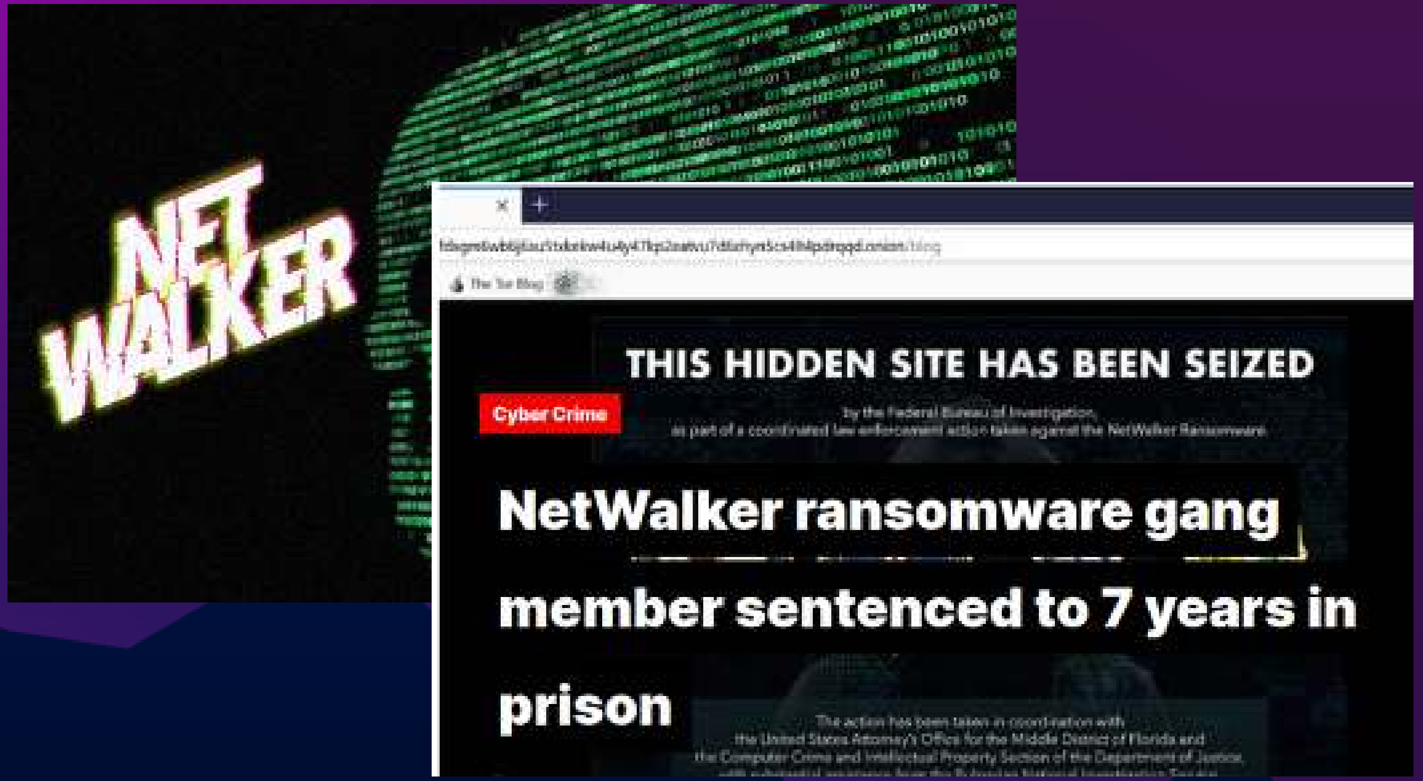
OSINT SKILLS CAN BE USED TO PROFILE CYBERCRIMINALS

Authorities soon tracked Sokolovsky's phone through Germany and eventually to The Netherlands, with his female companion helpfully documenting every step of the trip on her Instagram account.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   [illegible]

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   [illegible]@posteo.net. Your personal installation key:

   [illegible]

If you already purchased your key, please enter it below.
Key:
```

Researchers who analyzed the malware found that it contained metadata that pointed to the use of a Russian-made programming tool called "Pelles C". The metadata also contained a reference to a file path that contained the username of the developer who created the malware.



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
as part of a coordinated law enforcement action taken against the NetWalker Ransomware.

NetWalker ransomware gang member sentenced to 7 years in prison

The action has been taken in coordination with
the United States Attorney's Office for the Middle District of Florida and
the Computer Crime and Intellectual Property Section of the Department of Justice,

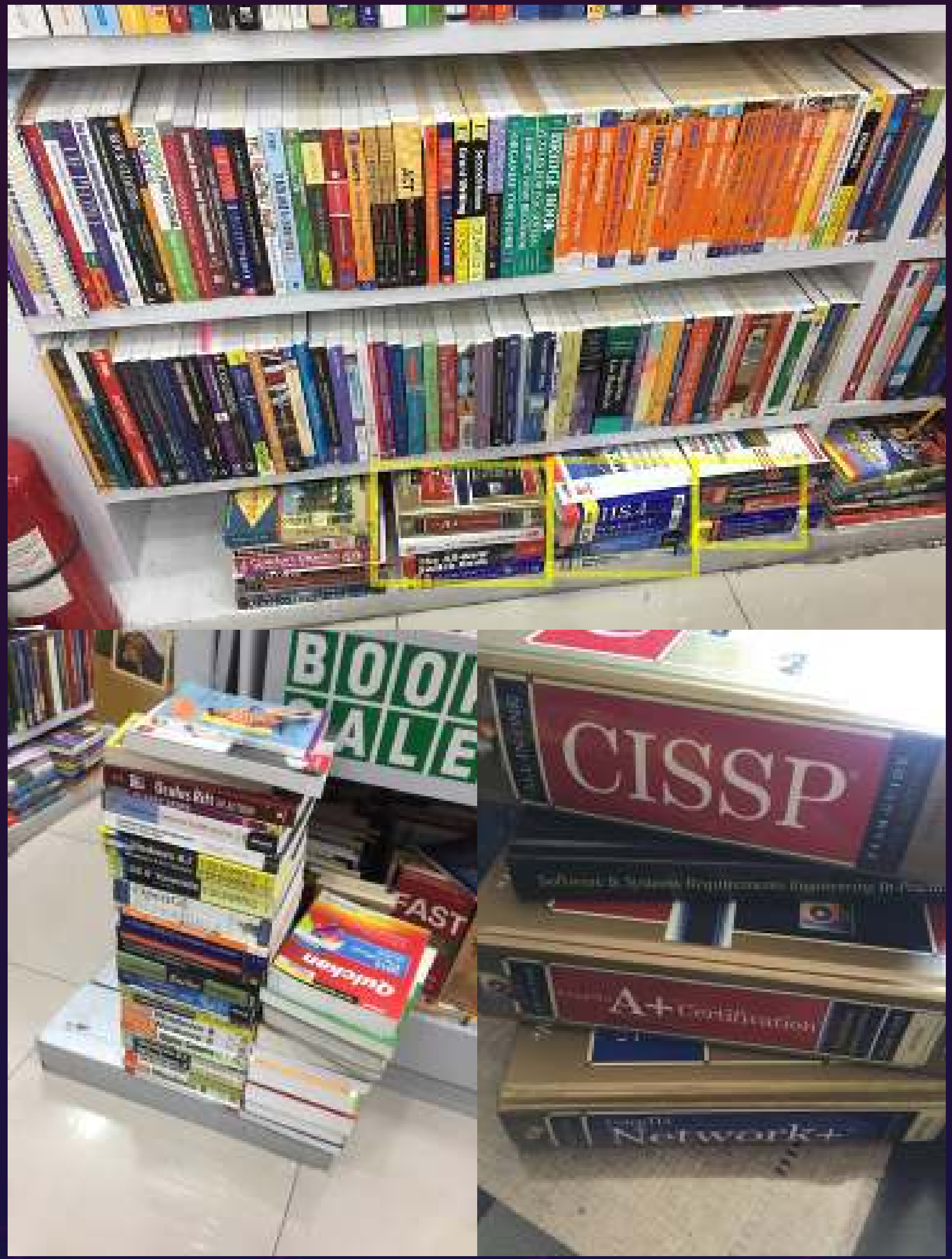
"based on internet protocol addresses, data gleaned from US investigations into various Apple, Google, Microsoft, and Mega.nz accounts, aliases, email addresses, and personal information revealed on social media platforms, the Defendant was identified by the Canadian authorities," court documents revealed.

https://darknetdiaries.com/transcript/54/
https://darknetdiaries.com/episode/58/
https://www.hackread.com/netwalker-ransomware-gang-member-imprisoned/
https://krebsonsecurity.com/2022/10/accused-raccoon-malware-developer-fled-ukraine-after-russian-invasion/
https://www.pcmag.com/news/us-indicts-ukrainian-for-raccoon-stealer-malware-that-hit-millions-of-computers

Tips and tricks

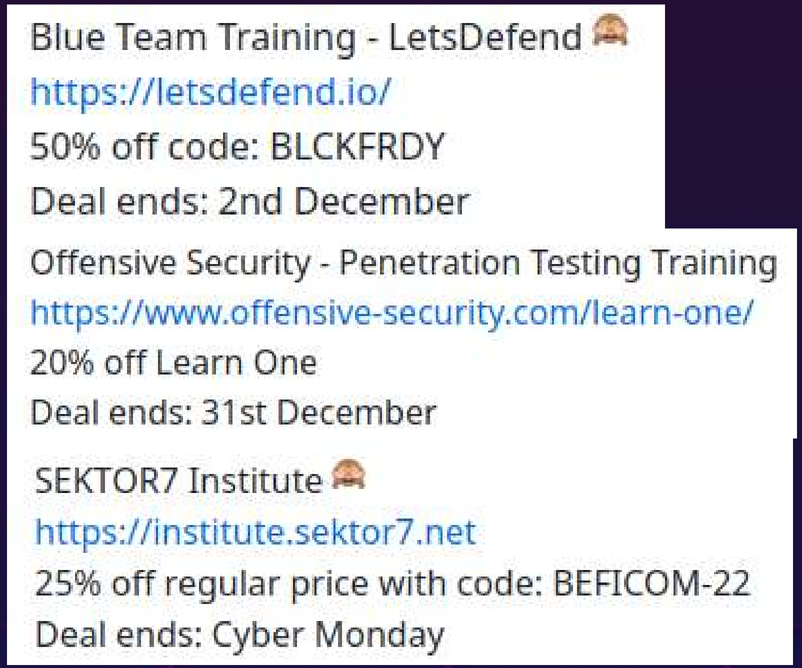
https://github.com/s0md3v/be-a-hacker#how-to-avoid-burnouts

GATHERING RESOURCES



Used book sale

- Cost effective
- Supplementary material
- Exam objectives remain the same
- Familiarity with older technologies
- Historical information



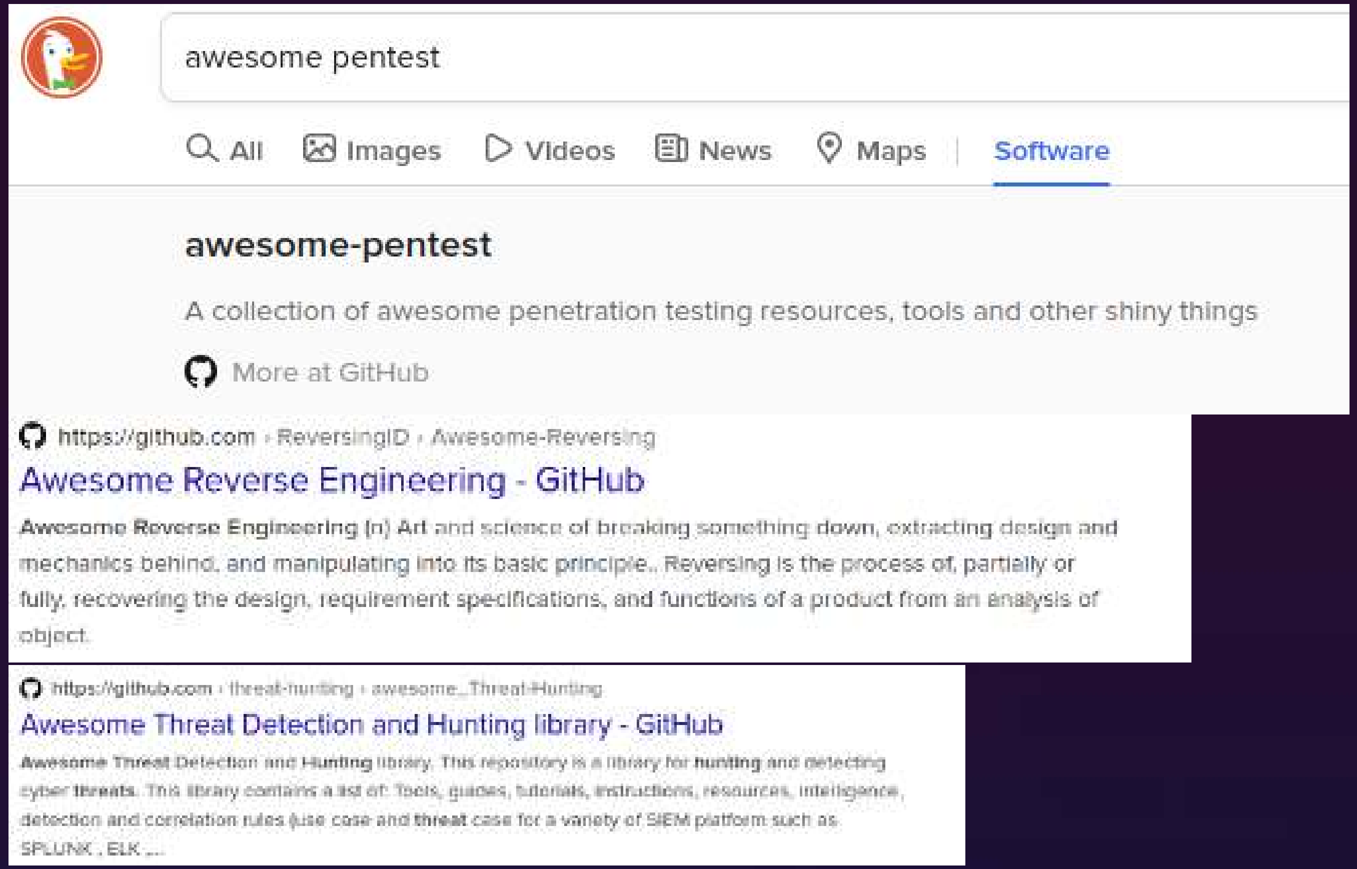
Blue Team Training - LetsDefend 🙈
https://letsdefend.io/
50% off code: BLCKFRDY
Deal ends: 2nd December

Offensive Security - Penetration Testing Training
https://www.offensive-security.com/learn-one/
20% off Learn One
Deal ends: 31st December

SEKTOR7 Institute 🙈
https://institute.sektor7.net
25% off regular price with code: BEFICOM-22
Deal ends: Cyber Monday

Black Friday sales

- discounted Prices/Certifications/Training
- https://github.com/0x90n/InfoSec-Black-Friday



awesome-pentest

A collection of awesome penetration testing resources, tools and other shiny things

More at GitHub

https://github.com › ReversingID › Awesome-Reversing

Awesome Reverse Engineering - GitHub

Awesome Reverse Engineering (n) **Art** and science of breaking something down, extracting design and mechanics behind, and manipulating into its basic principle.. Reversing is the process of, partially or fully, recovering the design, requirement specifications, and functions of a product from an analysis of object.

https://github.com › threat-hunting › awesome_Threat-Hunting

Awesome Threat Detection and Hunting library - GitHub

Awesome Threat Detection and **Hunting** library. This repository is a library for **hunting** and detecting cyber **threats**. This library contains a list of: Tools, guides, tutorials, instructions, resources, intelligence, detection and correlation rules (use case and **threat** case for a variety of SIEM platform such as SPLUNK , ELK ,...

Google dorking or just simply search

Awesome <Topics> you can Currated list.

HOW TO STAY UPDATED

RSS Feed

convenient way to stay up-to-date with multiple websites and sources of information without having to visit each site individually.

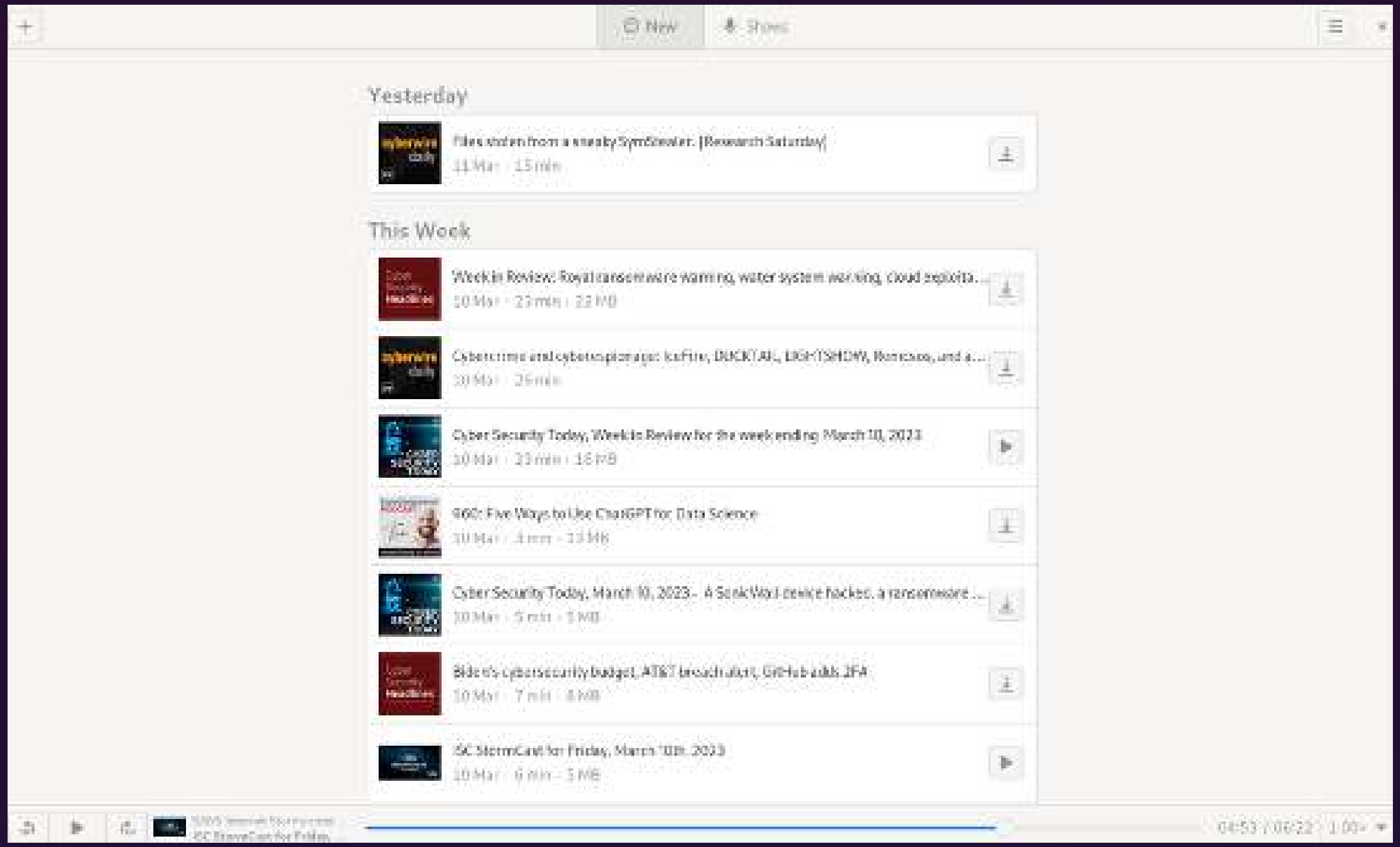
Twitter

Twitter is a great platform for staying up-to-date with the latest news and developments in the field of information security (InfoSec).

InfoSec Communities

Communities are typically focused on helping people learn about security, providing a platform for security professionals to network and collaborate, or sharing the latest security news and developments.

HOW TO STAY UPDATED



Yesterday

Files stolen from a sneaky SymStealer. [Research Saturday]
11 Mar · 15 min

This Week

Week in Review: Royal ransomware warning, water system warning, cloud exploits...
10 Mar · 23 min · 22 MB

Cybercrime and cyberespionage: IceFire, DUCKTAIL, LIGHTSHOW, Remcos, and a...
10 Mar · 26 min

Cyber Security Today, Week in Review for the week ending March 10, 2023
10 Mar · 23 min · 16 MB

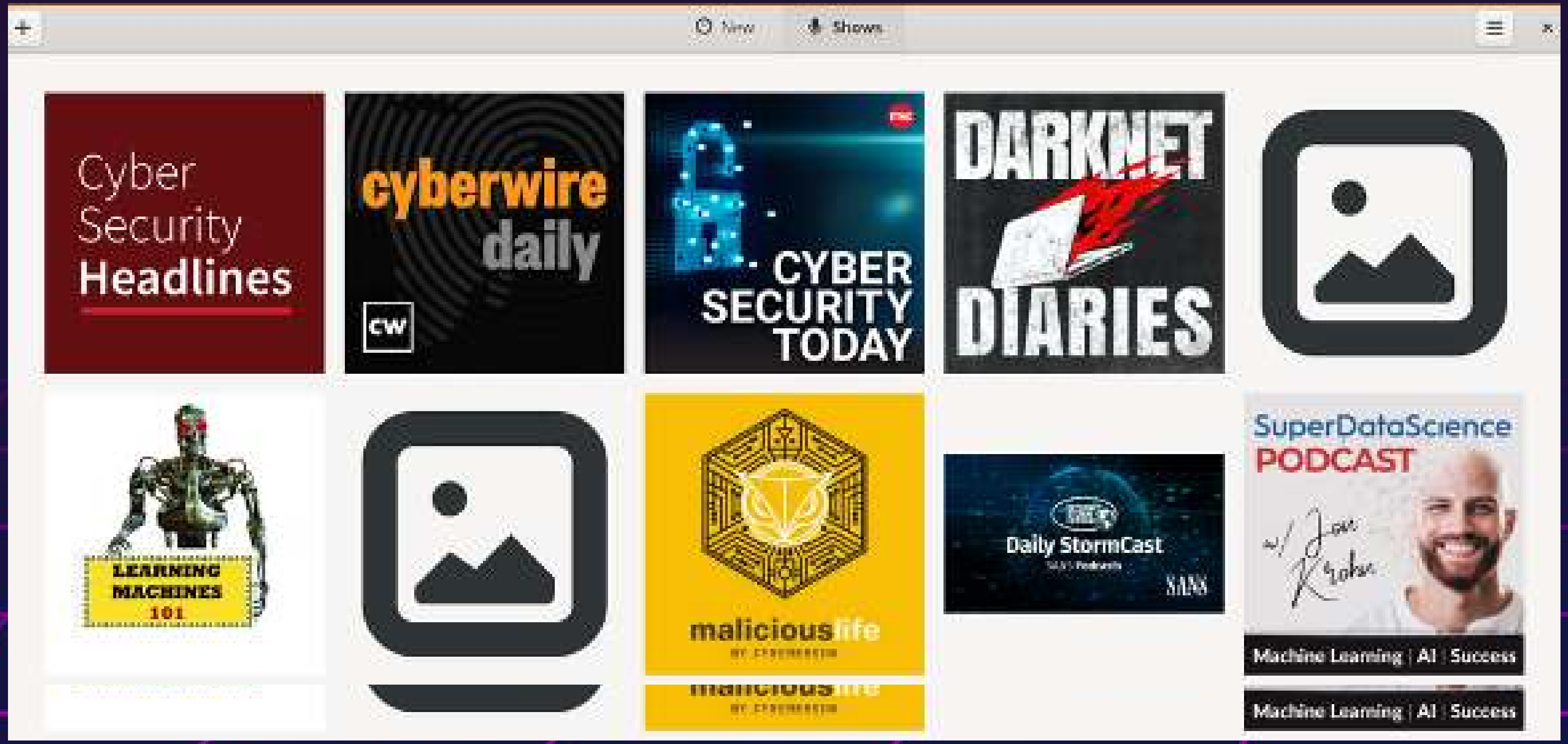
960: Five Ways to Use ChatGPT for Data Science
10 Mar · 3 min · 13 MB

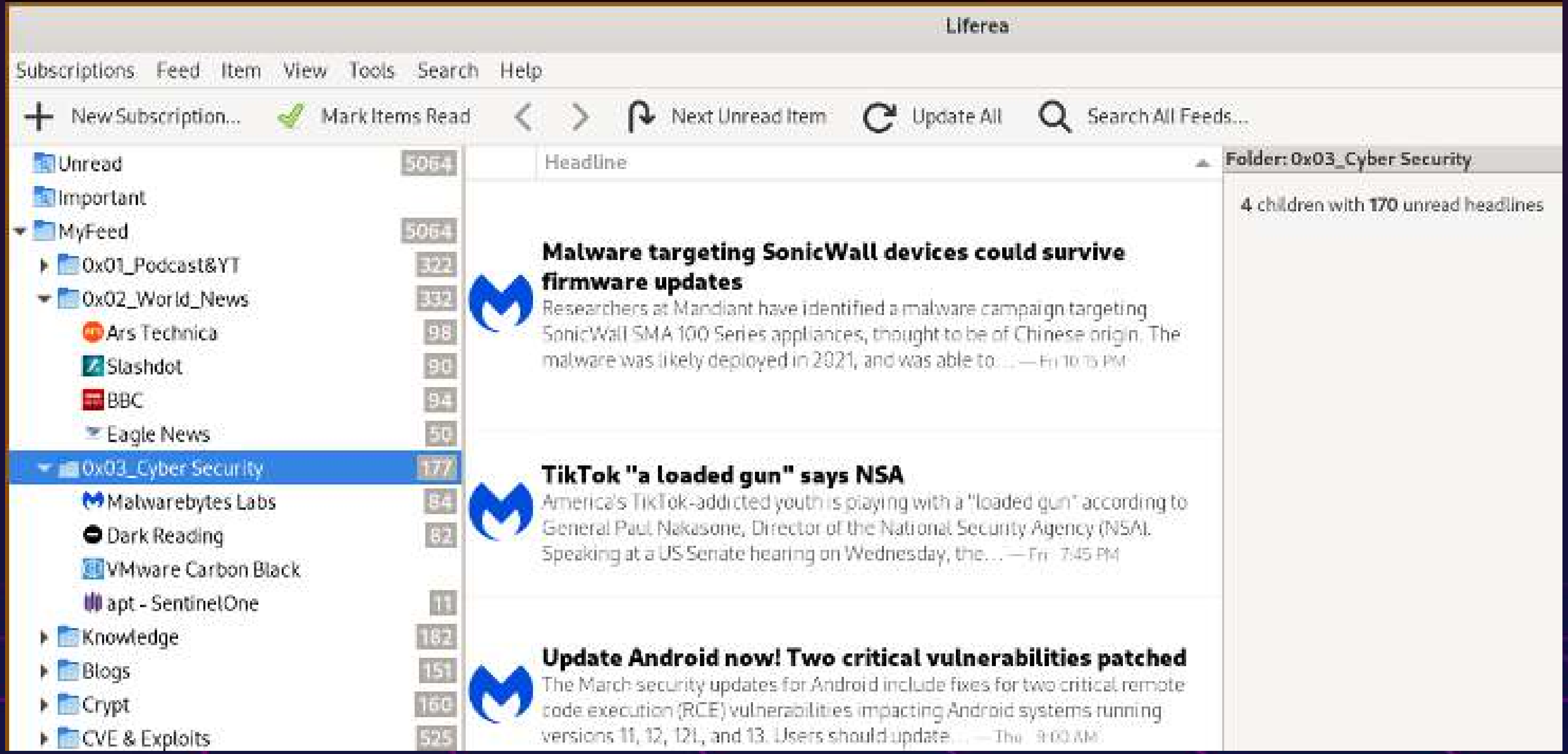
Cyber Security Today, March 10, 2023 - A SonicWall device hacked, a ransomware ...
10 Mar · 5 min · 5 MB

Biden's cybersecurity budget, AT&T breach alert, GitHub adds 2FA
10 Mar · 7 min · 8 MB

ISC StormCast for Friday, March 10th, 2023
10 Mar · 6 min · 5 MB

RSS feeds are a great way to stay updated on the latest content from websites you follow without having to visit each website individually




Liferea
Subscriptions Feed Item View Tools Search Help
New Subscription... Mark Items Read Next Unread Item Update All Search All Feeds...
Headline

Unread	5064
Important	
MyFeed	5064
0x01_Podcast&YT	322
0x02_World_News	332
Ars Technica	98
Slashdot	90
BBC	94
Eagle News	50
0x03_Cyber Security	177
Malwarebytes Labs	84
Dark Reading	82
VMware Carbon Black	
apt - SentinelOne	11
Knowledge	182
Blogs	151
Crypt	160
CVE & Exploits	525

Malware targeting SonicWall devices could survive firmware updates
Researchers at Mandiant have identified a malware campaign targeting SonicWall SMA 100 Series appliances, thought to be of Chinese origin. The malware was likely deployed in 2021, and was able to… — Fri 10:15 PM

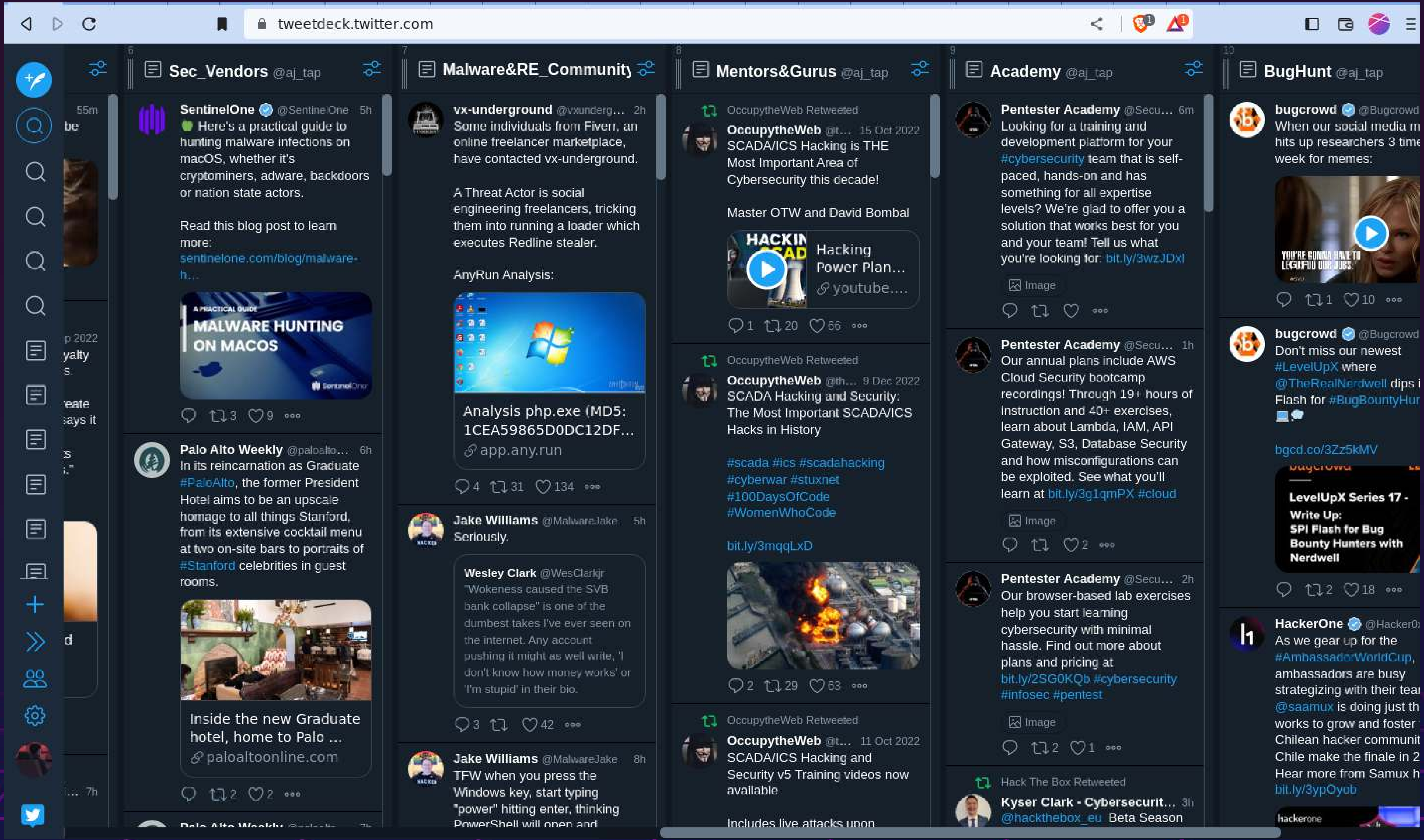
TikTok "a loaded gun" says NSA
America's TikTok-addicted youth is playing with a "loaded gun" according to General Paul Nakasone, Director of the National Security Agency (NSA). Speaking at a US Senate hearing on Wednesday, the… — Fri 7:45 PM

Update Android now! Two critical vulnerabilities patched
The March security updates for Android include fixes for two critical remote code execution (RCE) vulnerabilities impacting Android systems running versions 11, 12, 12L, and 13. Users should update… — Thu 9:00 AM

Folder: 0x03_Cyber Security

4 children with 170 unread headlines

HOW TO STAY UPDATED



Sec_Vendors @aj_tap

SentinelOne @SentinelOne 5h
Here's a practical guide to hunting malware infections on macOS, whether it's cryptominers, adware, backdoors or nation state actors.

Read this blog post to learn more:
sentinelone.com/blog/malware-h...

3 9

Palo Alto Weekly @paloalto... 6h
In its reincarnation as Graduate #PaloAlto, the former President Hotel aims to be an upscale homage to all things Stanford, from its extensive cocktail menu at two on-site bars to portraits of #Stanford celebrities in guest rooms.

Inside the new Graduate hotel, home to Palo ...
paloaltoonline.com

2 2

Malware&RE_Community

vx-underground @vxunderg... 2h
Some individuals from Fiverr, an online freelancer marketplace, have contacted vx-underground.

A Threat Actor is social engineering freelancers, tricking them into running a loader which executes Redline stealer.

AnyRun Analysis:

Analysis php.exe (MD5: 1CEA59865D0DC12DF...
app.any.run

4 31 134

Jake Williams @MalwareJake 5h
Seriously.

> **Wesley Clark** @WesClarkjr
> "Wokeness caused the SVB bank collapse" is one of the dumbest takes I've ever seen on the internet. Any account pushing it might as well write, 'I don't know how money works' or 'I'm stupid' in their bio.

3 42

Jake Williams @MalwareJake 8h
TFW when you press the Windows key, start typing "power" hitting enter, thinking PowerShell will open and

Mentors&Gurus @aj_tap

OccupytheWeb Retweeted
OccupytheWeb @t... 15 Oct 2022
SCADA/ICS Hacking is THE Most Important Area of Cybersecurity this decade!

Master OTW and David Bombal

Hacking Power Plan...
youtube....

1 20 66

OccupytheWeb Retweeted
OccupytheWeb @th... 9 Dec 2022
SCADA Hacking and Security: The Most Important SCADA/ICS Hacks in History

#scada #ics #scadahacking #cyberwar #stuxnet #100DaysOfCode #WomenWhoCode

bit.ly/3mqqLxD

2 29 63

OccupytheWeb Retweeted
OccupytheWeb @t... 11 Oct 2022
SCADA/ICS Hacking and Security v5 Training videos now available

Includes live attacks upon

Academy @aj_tap

Pentester Academy @Secu... 6m
Looking for a training and development platform for your #cybersecurity team that is self-paced, hands-on and has something for all expertise levels? We're glad to offer you a solution that works best for you and your team! Tell us what you're looking for: bit.ly/3wzJDxl

Image

Pentester Academy @Secu... 1h
Our annual plans include AWS Cloud Security bootcamp recordings! Through 19+ hours of instruction and 40+ exercises, learn about Lambda, IAM, API Gateway, S3, Database Security and how misconfigurations can be exploited. See what you'll learn at bit.ly/3g1qmPX #cloud

Image

2

Pentester Academy @Secu... 2h
Our browser-based lab exercises help you start learning cybersecurity with minimal hassle. Find out more about plans and pricing at bit.ly/2SG0KQb #cybersecurity #infosec #pentest

Image

2 1

Hack The Box Retweeted
Kyser Clark - Cybersecurit... 3h
@hackthebox_eu Beta Season

BugHunt @aj_tap

bugcrowd @Bugcrowd
When our social media m
hits up researchers 3 time
week for memes:

1 10

bugcrowd @Bugcrowd
Don't miss our newest #LevelUpX where @TheRealNerdwell dips i
Flash for #BugBountyHur

bgcd.co/3Zz5kMV

LevelUpX Series 17 - Write Up: SPI Flash for Bug Bounty Hunters with Nerdwell

2 18

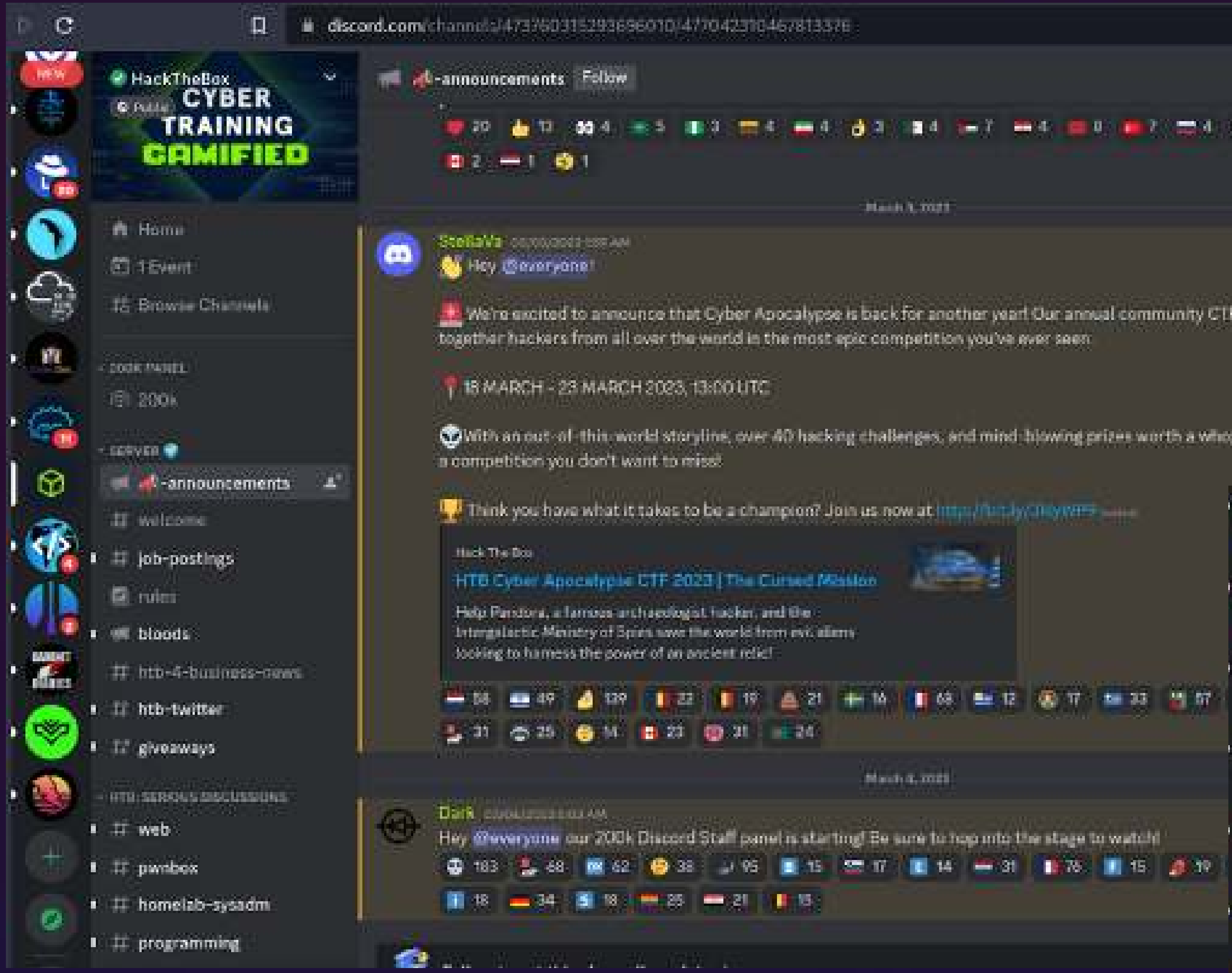
HackerOne @Hacker0
As we gear up for the #AmbassadorWorldCup, ambassadors are busy strategizing with their tea
@saamux is doing just th
works to grow and foster
Chilean hacker communit
Chile make the finale in 2
Hear more from Samux h
bit.ly/3ypOyob

social media dashboard application that allows users to manage and organize their Twitter accounts.

HOW TO STAY UPDATED

several communities dedicated to information security (InfoSec).

Network with people :)



March 3, 2023

StellaVa

Hey @everyone!

We're excited to announce that Cyber Apocalypse is back for another year! Our annual community CTF is ready to bring together hackers from all over the world in the most epic competition you've ever seen

18 MARCH - 23 MARCH 2023, 13:00 UTC

With an out-of-this-world storyline, over 40 hacking challenges, and mind-blowing prizes worth a whopping $35,000, this is a competition you don't want to miss!

Think you have what it takes to be a champion? Join us now at http://bit.ly/3KyWFF

Hack The Box

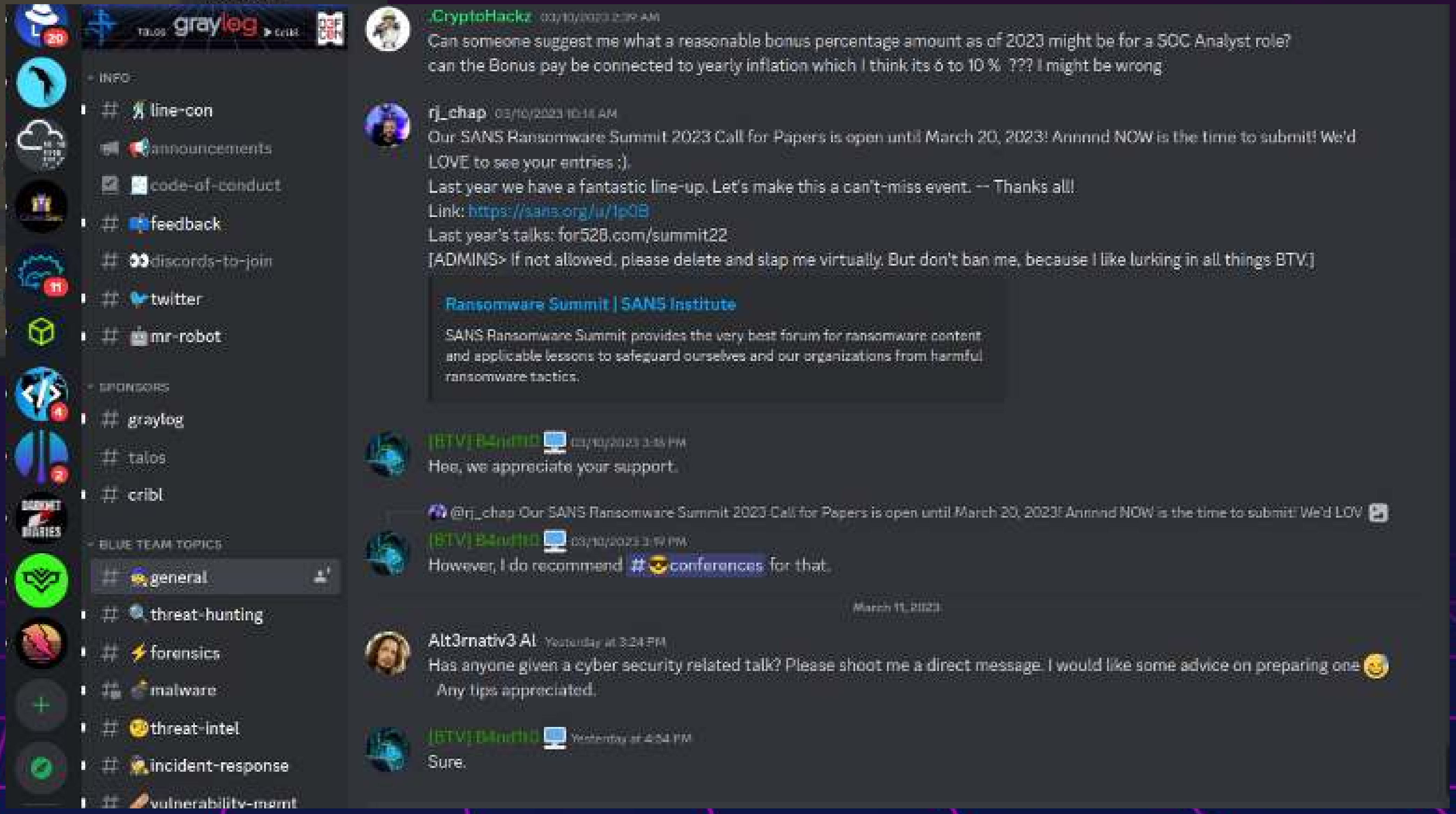
HTB Cyber Apocalypse CTF 2023 | The Cursed Mission

Help Pandora, a famous archaeologist, hacker, and the Intergalactic Ministry of Spies save the world from evil aliens looking to harness the power of an ancient relic!

March 4, 2023

Dark

Hey @everyone our 200k Discord Staff panel is starting! Be sure to hop into the stage to watch!



.CryptoHackz 03/10/2023 2:39 AM

Can someone suggest me what a reasonable bonus percentage amount as of 2023 might be for a SOC Analyst role?
can the Bonus pay be connected to yearly inflation which I think its 6 to 10 % ??? I might be wrong

rj_chap 03/10/2023 10:14 AM

Our SANS Ransomware Summit 2023 Call for Papers is open until March 20, 2023! Annnnd NOW is the time to submit! We'd LOVE to see your entries :).
Last year we have a fantastic line-up. Let's make this a can't-miss event. -- Thanks all!
Link: https://sans.org/u/1p0B
Last year's talks: for528.com/summit22
[ADMINS> If not allowed, please delete and slap me virtually. But don't ban me, because I like lurking in all things BTV.]

Ransomware Summit | SANS Institute

SANS Ransomware Summit provides the very best forum for ransomware content and applicable lessons to safeguard ourselves and our organizations from harmful ransomware tactics.

[BTV] B4nd1t0 03/10/2023 3:18 PM

Hee, we appreciate your support.

@rj_chap Our SANS Ransomware Summit 2023 Call for Papers is open until March 20, 2023! Annnnd NOW is the time to submit! We'd LOV

[BTV] B4nd1t0 03/10/2023 3:19 PM

However, I do recommend #😎conferences for that.

March 11, 2023

Alt3rnativ3 AI Yesterday at 3:24 PM

Has anyone given a cyber security related talk? Please shoot me a direct message. I would like some advice on preparing one 😊
Any tips appreciated.

[BTV] B4nd1t0 Yesterday at 4:54 PM

Sure.

HOW TO RETAIN LEARNIGS

Zettelkasten

note-taking method that involves creating small, interconnected notes or "slips" that can be linked together to form a knowledge graph.

Note-taking apps

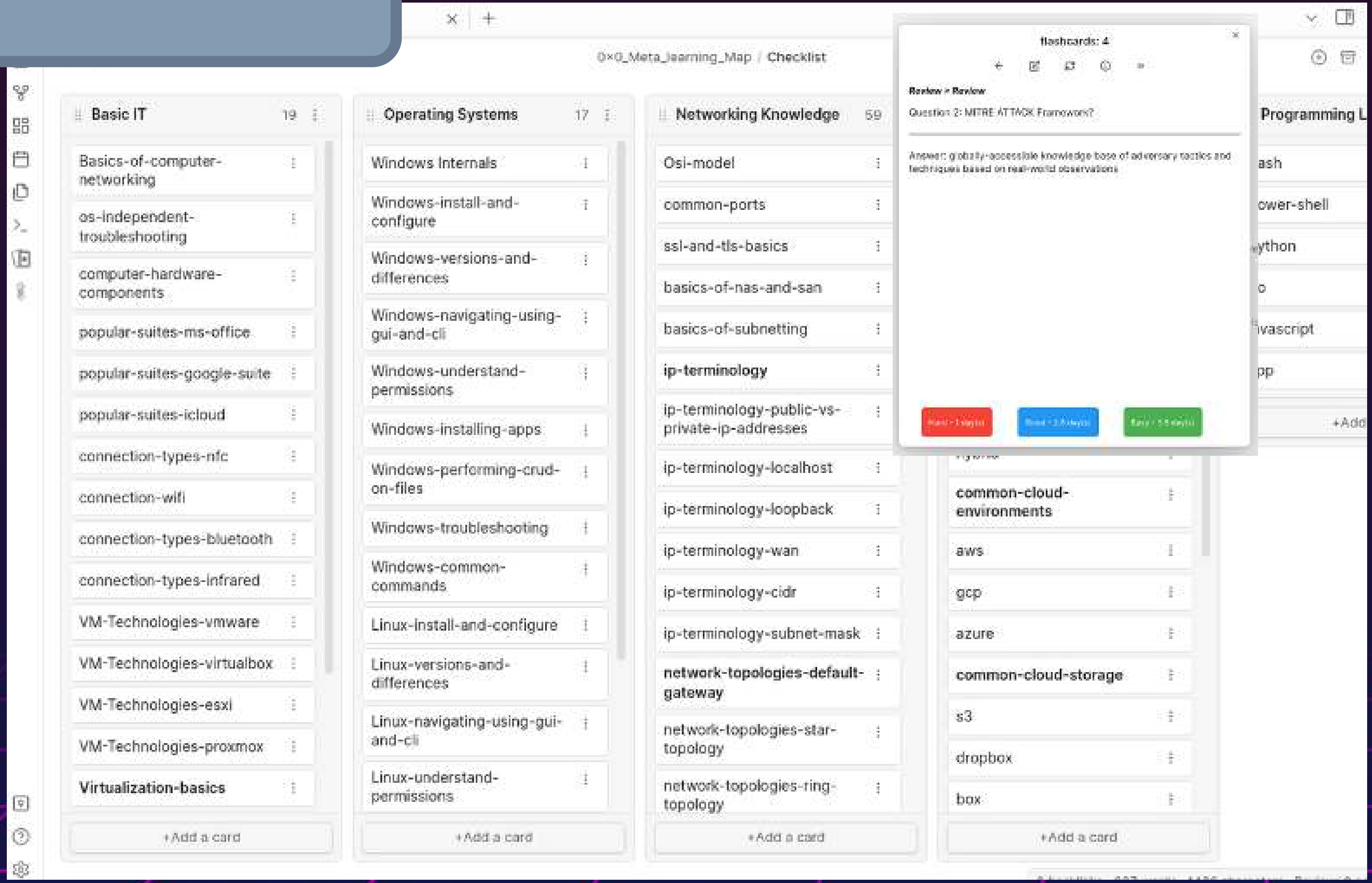
Such as Obsidian, Notion, Evernote, TiddlyWiki and Roam Research

Spaced Repetition

learning technique that uses flashcards to help you remember and recall information. which involves repeating information at increasingly spaced intervals to improve memory retention.

YOUR ROADMAP TEMPLATE

Ultra learning MD notebook template



0x0_Meta_learning_Map / Checklist

Basic IT 19

- Basics-of-computer-networking
- os-independent-troubleshooting
- computer-hardware-components
- popular-suites-ms-office
- popular-suites-google-suite
- popular-suites-icloud
- connection-types-nfc
- connection-wifi
- connection-types-bluetooth
- connection-types-infrared
- VM-Technologies-vmware
- VM-Technologies-virtualbox
- VM-Technologies-esxi
- VM-Technologies-proxmox
- Virtualization-basics

+Add a card

Operating Systems 17

- Windows Internals
- Windows-install-and-configure
- Windows-versions-and-differences
- Windows-navigating-using-gui-and-cli
- Windows-understand-permissions
- Windows-installing-apps
- Windows-performing-crud-on-files
- Windows-troubleshooting
- Windows-common-commands
- Linux-install-and-configure
- Linux-versions-and-differences
- Linux-navigating-using-gui-and-cli
- Linux-understand-permissions

+Add a card

Networking Knowledge 59

- Osi-model
- common-ports
- ssl-and-tls-basics
- basics-of-nas-and-san
- basics-of-subnetting
- ip-terminology
- ip-terminology-public-vs-private-ip-addresses
- ip-terminology-localhost
- ip-terminology-loopback
- ip-terminology-wan
- ip-terminology-cidr
- ip-terminology-subnet-mask
- network-topologies-default-gateway
- network-topologies-star-topology
- network-topologies-ring-topology

+Add a card

- common-cloud-environments
- aws
- gcp
- azure
- common-cloud-storage
- s3
- dropbox
- box

+Add a card

Programming L

- ash
- ower-shell
- ython
- o
- ivascript
- pp

+Add

flashcards: 4

Review > Review

Question 2: MITRE ATTACK Framework?

Answer: globally-accessible knowledge base of adversary tactics and techniques based on real-world observations

- Contains plugins and templates that can help you retain your learning

Notebook template:
https://drive.google.com/file/d/1xNAuePD9SM7mwrnMdRDeIgnbWy6msbcy/view?usp=sharing

RSS feedlist:
https://drive.google.com/file/d/1YJgF3mjue0juiRr6uJLqNBE3sUvwUFLF/view?usp=share_link

How to use it.

1. Download the obsidian note taking app
   a. https://obsidian.md
2. Download and extract the template
3. Open as vault and specify the template directory

Tutorial in setting up your own:
https://www.youtube.com/watch?v=E6ySG7xYgjY

THANK YOU FOR LISTENING

GuideM Training Center

Cybersecurity live training
courses such as Cyber Defense, Threat Hunting,
Digital Forensics, Memory Analysis and some
https://www.facebook.com/guidemtraining

Association of Computer Science Student

ACSS Be part of our team we will conduct
CTF competitions, hackthons and webinars.

JOIN
TODAY
WE ARE LOOKING FOR
COMPUTER SCIENCE STUDENTS
WHO WANT TO BECOME AN OFFICER
IN OUR ORGANIZATION
ACSS
ASSOCIATION OF COMPUTER
SCIENCE STUDENTS
bit.ly/ACSSRecForm