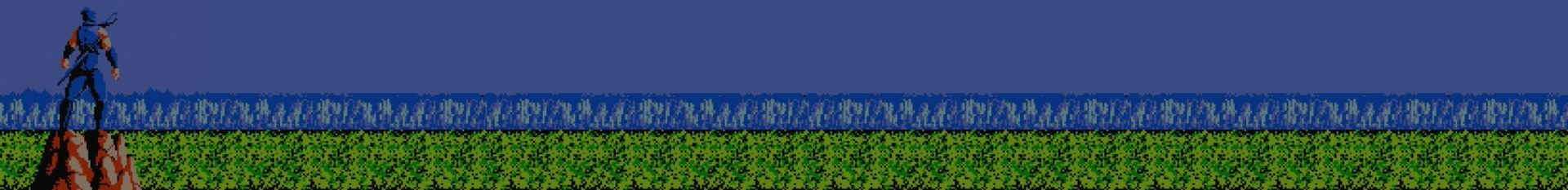
CTF Basics:

Essential Skills for First-Time Competitors

Eddie Miro



In This Talk:

- What is a CTF?
- General Skills Needed
- Categories
- Mini CTF
- Cryptography
- Steganography
- OSINT
- Reverse Engineering
- Miscellaneous
- Other Categories
- How To Prepare
- Resources

What is a CTF?

- Capture the Flag
- Solos/Teams solve challenges to earn points

Types of CTF Formats:

- Jeopardy-style:
  National Cyber League, PicoCTF
- Attack-Defense:
  DEF CON, CCDC
- Boot-to-Root:
  VulnHub, TryHackMe

General Skills Needed for CTFs

- Linux command line
- Networking (e.g., Wireshark)
- Programming (Python, Bash, etc.)
- Problem-solving and creative thinking

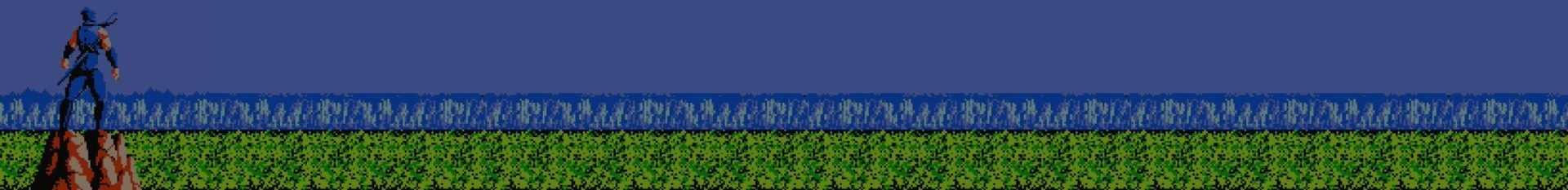
Skills to Practice:

- Googling
- Thinking outside the box
- Perseverance
- Time Management

Categories of CTF Challenges

1. Cryptography
2. Steganography
3. OSINT (Open-Source Intelligence)
4. Reverse Engineering
5. Miscellaneous (Misc)

Each type includes a challenge for you to solve!



The Eddie Miro CTF Talk CTF

Flag format: SAINT-CON-####

mirolabs.info/saintcon-2024-ctf-talk

Cryptography

What it is: Encryption, decryption, ciphers

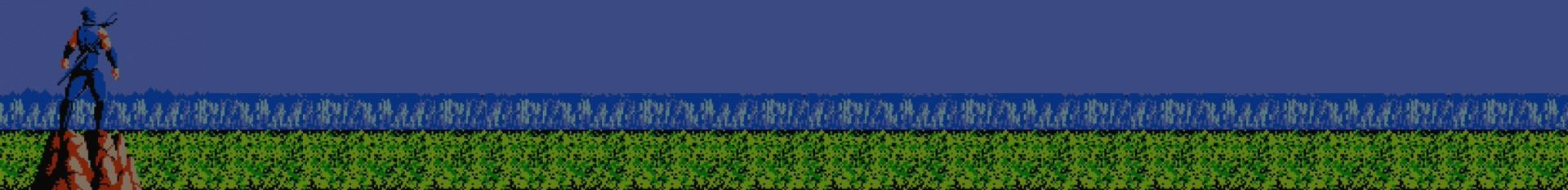
Techniques: Caesar, Vigenère, RSA, XOR, exotic/historical/obscure

Tools:
CyberChef
Cryptool
dcode.fr/en
rumkin.com/tools/cipher/

Challenge 1

Decode this Caesar cipher:

FNVAG-PBA-5357



Steganography

What it is: Hiding data within images, audio, or text

Techniques: LSB (Least Significant Bit), file formats, many more.

Tools:
Steghide
zsteg
binwalk
ExifTool
georgeom.net/StegOnline
aperisolve.com

Challenge 2

Extract hidden text from image

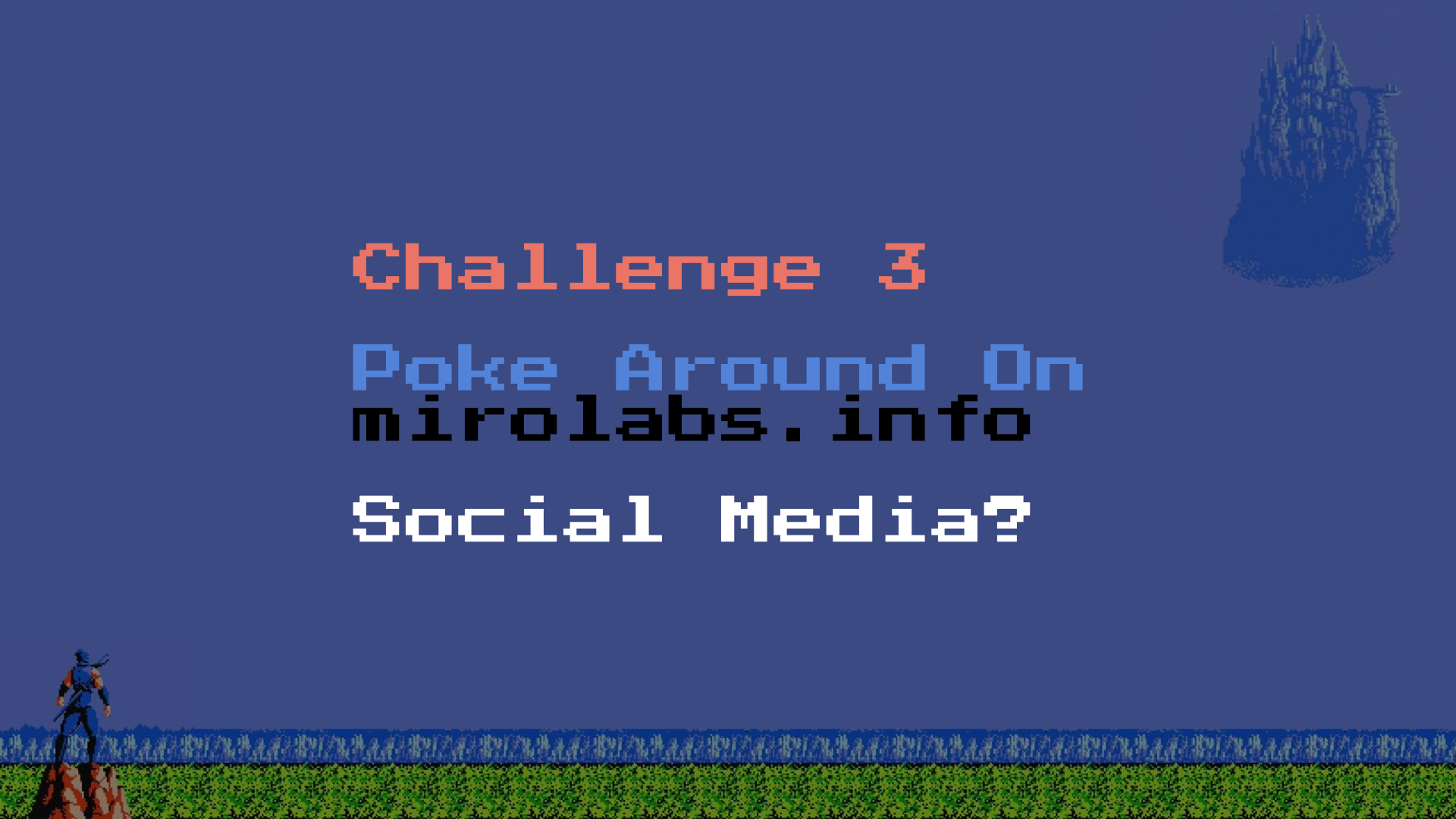
github.com/c1ph0r/SaintCon-2024/blob/main/steganography.png

OSINT
(Open-Source Intelligence)

What it is: Gathering publicly available information to solve challenges.

Techniques: Google dorking, social media analysis, WHOIS lookups, public database searching, Geolocation analysis.

Tools:Maltego, theHarvester, SpiderFoot, Shodan, OSINT Framework, Reverse Image Search,


Challenge 3
Poke Around On
mirolabs.info
Social Media?

Reverse Engineering

What it is: Understanding a program's inner workings

Techniques: Tools like Ghidra, IDA Pro

Tools: Ghidra, IDA Pro, Radare2, x64dbg

Challenge 4

Analyze a simple Python program to find the flag.

github.com/c1ph0r/SaintCon-2024/blob/main/reverse_engineering.py

Miscellaneous

What it is: Challenges that don't fit into other categories, often creative or unconventional.

Techniques: Could involve puzzles, trivia, out-of-the-box thinking, or unique tools.

Tools: Google, ChatGPT

Challenge 5

Password is the 4 digit number for the RFC that covers the Hyper Text Coffee Pot Control Protocol

mirolabs.info/misc

Other Categories (Not Covered)

- Binary Exploitation (Pwn)
- Forensics
- Web Exploitation
- Mobile Exploitation
- Networking/Packet Challenges
- Hardware Challenges
- Log Analysis Challenges
- Physical Security Challenges

How to Prepare for a CTF

Practice platforms: Hack The Box, TryHackMe, OverTheWire, CryptoPals, VulnHub, picoGym

CTFTime.org for events

Essential tools: Kali Linux, Burp Suite, Wireshark, Ghidra, Python, pwntools

POWERED BY CYBER SKYLINE

Supported by

CROWDSTRIKE · CIPHER TECH SOLUTIONS · amazon · TANIUM · ISACA · women in CYBERSECURITY WiCyS · CompTIA · BLACK GIRLS HACK

Increase mission preparedness

CYBER SKYLINE Enterprise

Continuous cyber skills development for your team.

Identify technical talent

CYBER SKYLINE TalentScreen

Streamline recruiting process and drive better interviews.

Ranked gameplay

CYBER SKYLINE Competition

Competition environment for college & professionals.

Grow your students' cyber skills

CYBER SKYLINE Lab Kit

Supplemental learning material for cybersecurity education.