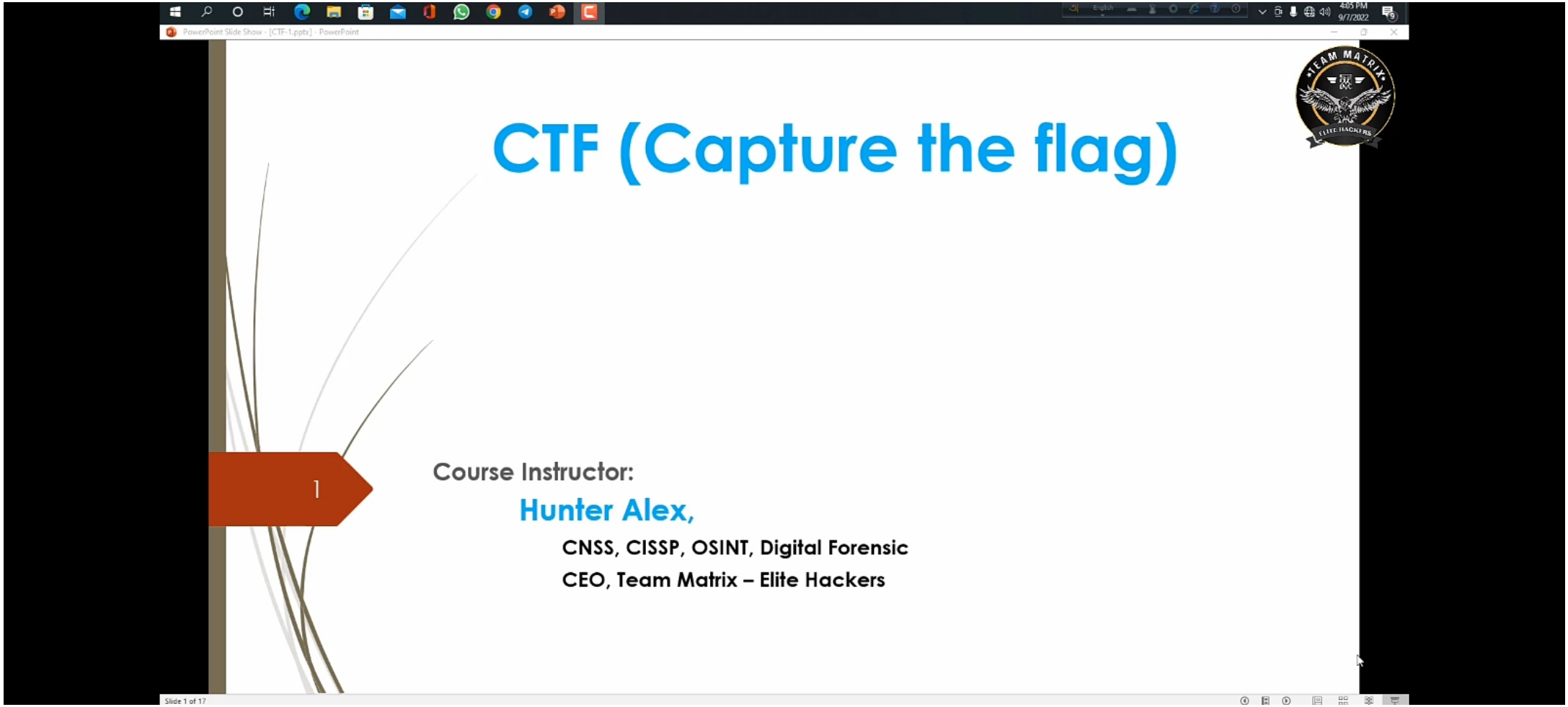
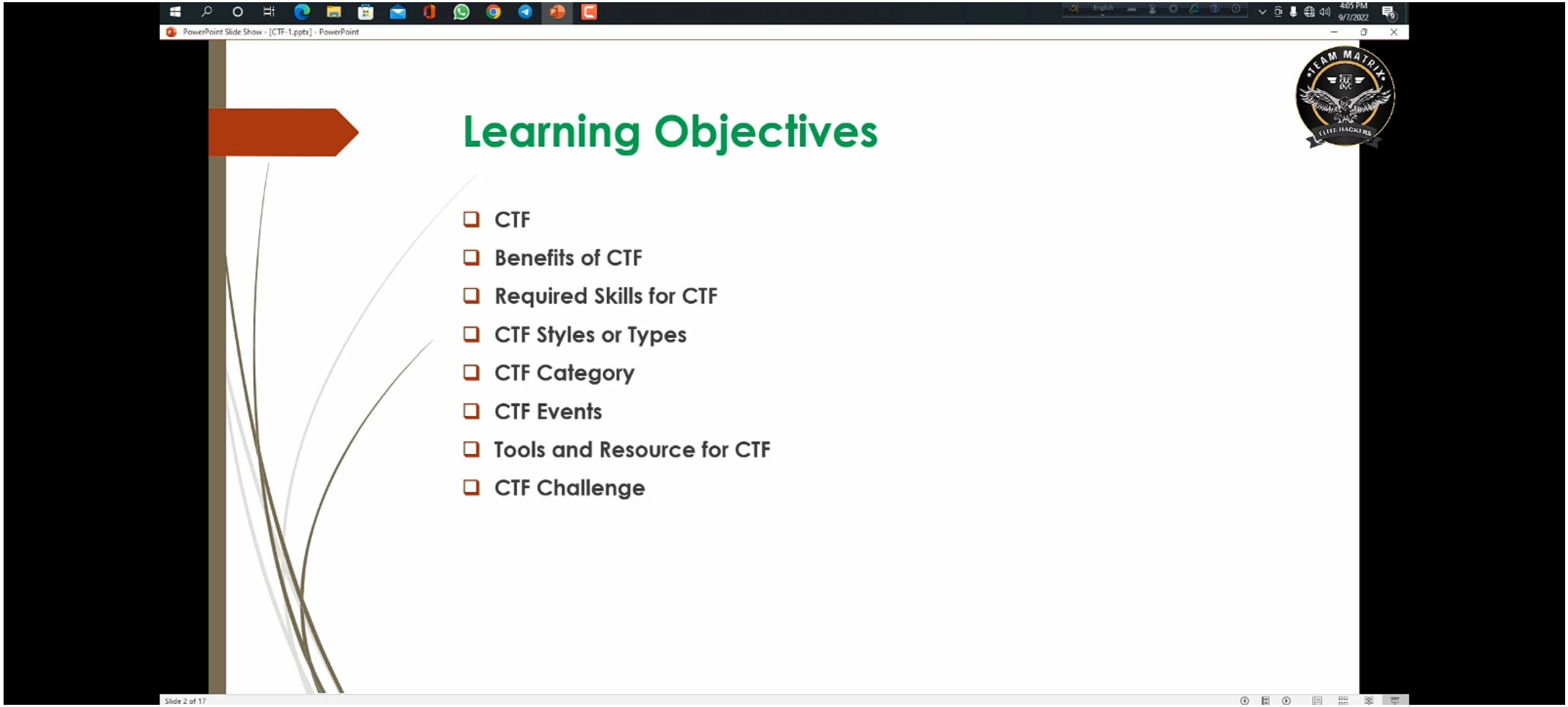

PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint
4:05 PM
9/7/2022
TEAM MATRIX
ELITE HACKERS
CTF (Capture the flag)
1
Course Instructor:
Hunter Alex,
CNSS, CISSP, OSINT, Digital Forensic
CEO, Team Matrix – Elite Hackers
Slide 1 of 17

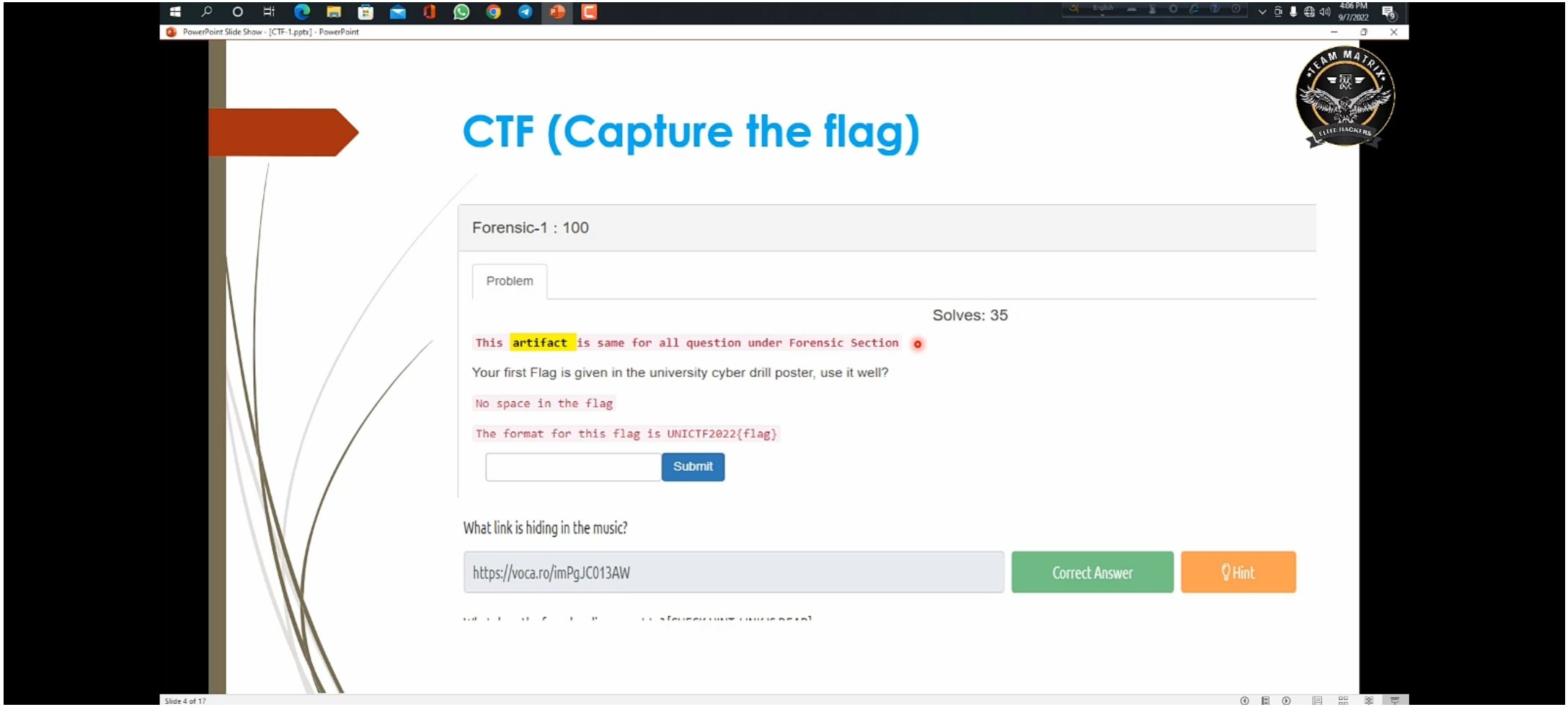

PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint
TEAM MATRIX
FLEET HACKERS
Learning Objectives
CTF
Benefits of CTF
Required Skills for CTF
CTF Styles or Types
CTF Category
CTF Events
Tools and Resource for CTF
CTF Challenge
Slide 2 of 17

PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint

CTF (Capture the flag)

- **CTF stands for Capture The Flag.**
- Capture the Flag is **a classic team game** played indoors or outdoors.
- Capture the Flag (CTF) is a special kind of information security competitions.
- A CTF is an event during which students, teachers, and professionals come together to compete against one another in an effort to test and expand cyber-security skills and awareness.
- Need to find the Flag from your Hacking Skills
- Hundreds of CTFs happen every year and that number is only growing.
- CTFs have been used since at least 1996 by hackers looking to test each others skill.

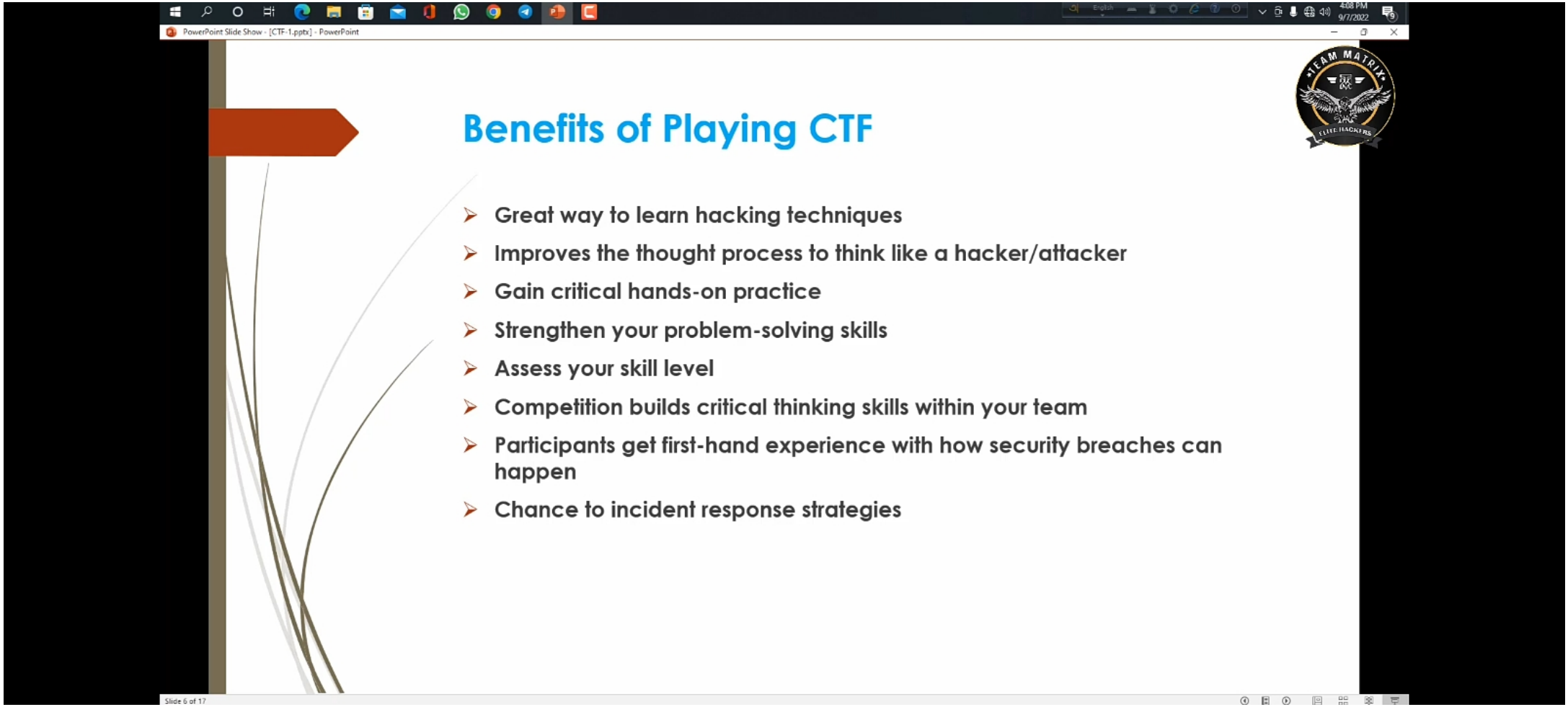
Slide 3 of 17


PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint
CTF (Capture the flag)
Forensic-1 : 100
Problem
Solves: 35
This artifact is same for all question under Forensic Section
Your first Flag is given in the university cyber drill poster, use it well?
No space in the flag
The format for this flag is UNICTF2022{flag}
Submit
What link is hiding in the music?
https://voca.ro/imPgJC013AW
Correct Answer
Hint
Slide 4 of 17

PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint

Class Requirements for CTF

- Cryptography
- Steganography
- OSINT
- LFI/RFI/RCE/CSRF
- XSS
- SQLI
- Burp Suite
- Web Attack
- Scanning and Networking
- Digital Forensic
- Kali Linux- Tools


PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint
Benefits of Playing CTF
Great way to learn hacking techniques
Improves the thought process to think like a hacker/attacker
Gain critical hands-on practice
Strengthen your problem-solving skills
Assess your skill level
Competition builds critical thinking skills within your team
Participants get first-hand experience with how security breaches can happen
Chance to incident response strategies
Slide 6 of 17

CTF Types (Styles)

There are three common types of CTFs

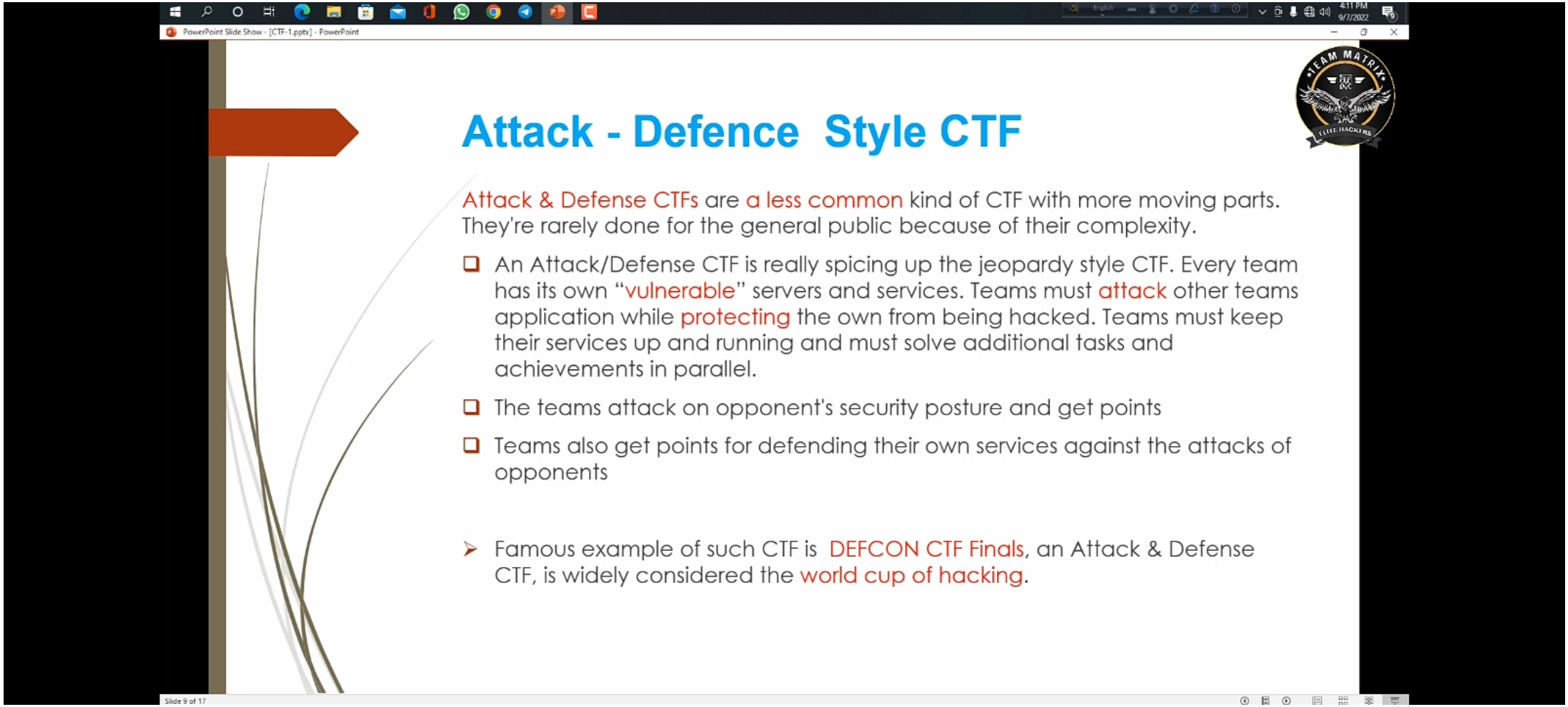
- **Jeopardy**
- **Attack-Defence**
- **Mixed Style**

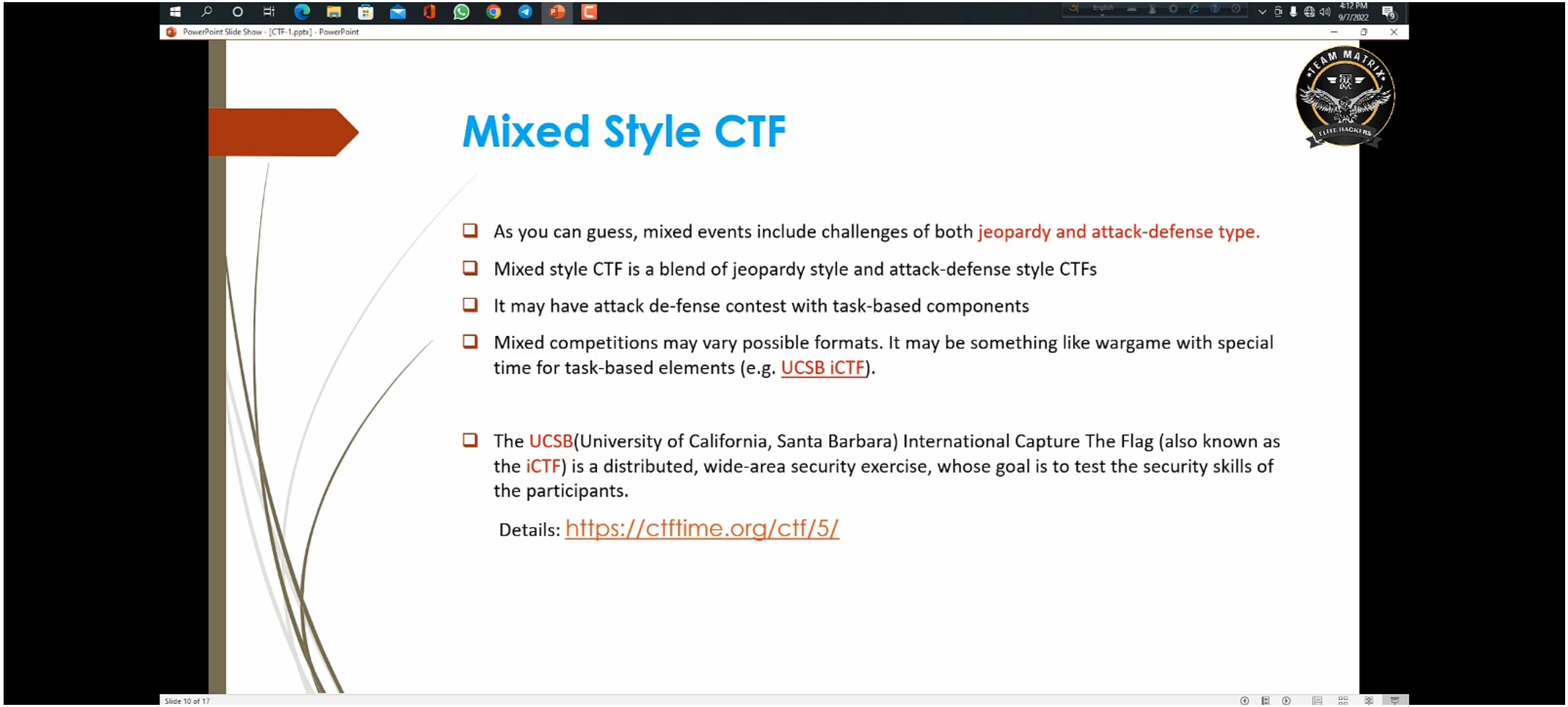
Jeopardy Style CTF

Jeopardy CTFs are the most common kind of CTF.

- Jeopardy-style CTFs have a couple of questions (tasks) in various categories.
- A team can gain some points for every solved task.
- More points for more complicated tasks, usually.
- New tasks cannot be unlocked until the previous task is completed.
- At the end of the game, the highest-scoring team or individual wins.

➢ Famous example of such CTF is DEF CON CTF Qualifier.


PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint
Attack - Defence Style CTF
Attack & Defense CTFs are a less common kind of CTF with more moving parts. They're rarely done for the general public because of their complexity.
An Attack/Defense CTF is really spicing up the jeopardy style CTF. Every team has its own "vulnerable" servers and services. Teams must attack other teams application while protecting the own from being hacked. Teams must keep their services up and running and must solve additional tasks and achievements in parallel.
The teams attack on opponent's security posture and get points
Teams also get points for defending their own services against the attacks of opponents
Famous example of such CTF is DEFCON CTF Finals, an Attack & Defense CTF, is widely considered the world cup of hacking.
Slide 9 of 17


PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint
Mixed Style CTF
As you can guess, mixed events include challenges of both jeopardy and attack-defense type.
Mixed style CTF is a blend of jeopardy style and attack-defense style CTFs
It may have attack de-fense contest with task-based components
Mixed competitions may vary possible formats. It may be something like wargame with special time for task-based elements (e.g. UCSB iCTF).
The UCSB(University of California, Santa Barbara) International Capture The Flag (also known as the iCTF) is a distributed, wide-area security exercise, whose goal is to test the security skills of the participants.
Details: https://ctftime.org/ctf/5/
Slide 10 of 17

PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint

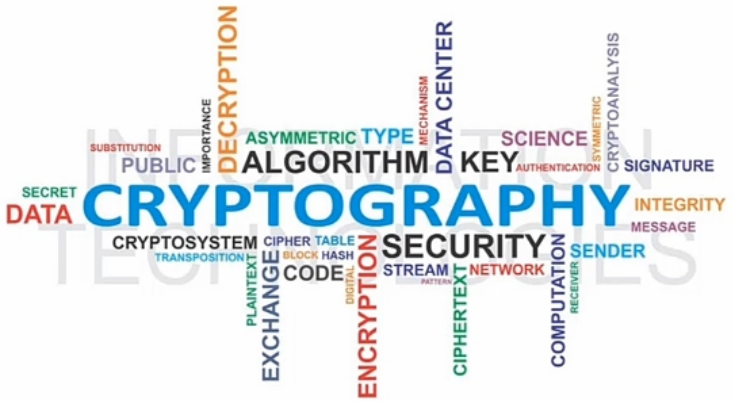
CTF Categories

- Cryptography
- Steganography
- Web Exploitation
- Forensics
- PWN Or Binary Exploitation
- Reverse Engineering
- Miscellaneous
- OSINT

Slide 11 of 17

Cryptography

- **Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.**
- **Tools :-** CyberChef, XORTool, Cryptii, dcode.fr, RSATool, hashes.com, boxentriq.com, morsecode.world and many more.



PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint

Steganography

- **Steganography means hiding secret information in any media like – text , image , audio , video.**
- **Tools:-** Steghide, Stegsolve, StegCracker, Exiftool, Sonic Visualizer, Online Stego tool and many more.

Slide 13 of 23

Web Exploitation

Web- These types of challenges focus on finding and exploiting the vulnerabilities in web applications to get a flag.

- **Learn Basic About Web Technology**

  HTTP, HTTP Request, Status Code, Cookies

  Basic HTML/CSS, PHP ,JavaScript

- **Pick a Vulnerability type and learn in deep about it, then move to another**

  XSS, SQLI, CSRF, LFI , RFI, RCE, IDOR, SSRF

- **Tools:-** Burpsuit , gobuster, nikto, hackbar ,nmap, sqlmap and many more.

Reverse Engineering

1

Course Instructor:

Hunter Alex,

CNSS, CISSP, OSINT, Digital Forensic

CEO, Team Matrix – Elite Hackers

Learning Objectives

- Reverse Engineering
- Software Reverse Engineering
- Reverse Engineering Process
- Reverse Engineering Tools
- Reverse Engineering Resources

Reverse Engineering

- Reverse → backwards, back
- Reverse → to change the direction, order, position, result, etc. of something to its opposite.
- Engineering → is the designing, testing and building of machines, structures and processes using maths and science.

Reverse Engineering

- The process of taking a piece of software or hardware and analyzing its functions and information flow so that its functionality and behavior can be understood. Malware is commonly reverse-engineered in cyber defense.
- Reverse engineering, also called backwards engineering or back engineering.

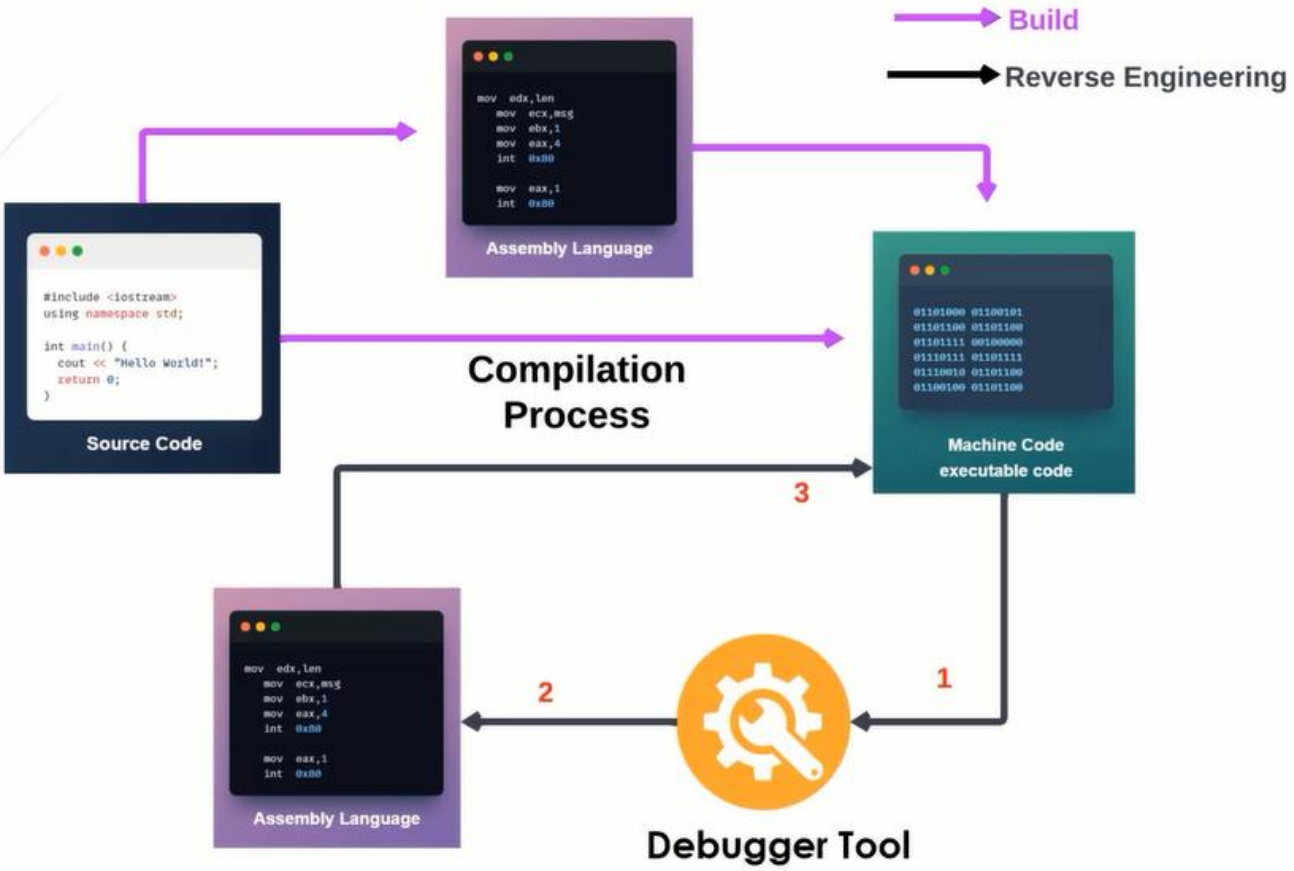
Reverse Engineering Fields

- Reverse engineering is applicable in the fields of **computer engineering, mechanical engineering, design, electronic engineering, software engineering, chemical engineering, and systems biology**.

Software reverse engineering (SRE)

- Software reverse engineering (SRE) is **the practice of analyzing a software system, either in whole or in part, to extract design and implementation information**

Software reverse engineering (SRE)



Purpose RS or SRE

- Program Bug Fixing
- Design Recovery
- Information Collection
- Extraction of the Structure
- Recover lost information.
- Corporate or Military Spying
- Competitor's intelligence
- Making Copies of the Original Product
- Parts Service or Repair
- Detect side effects.
- Failure Analysis
- Parts Improvement
- Diagnostics and Problem-Solving
- Paid App Free Use

Reverse Engineering in Cybersecurity

- Antivirus
- Malware analysis
- In the field of cyber security, the reverse engineering can be used to identify the details of a breach that how the attacker entered the system, and what steps were taken to breach the system.

PowerPoint Slide Show - [Reverse Engineering.pptx] - PowerPoint

Software

File Viewer Plus 2 License Key(s):

FA604-AFFCD-33021-04770-

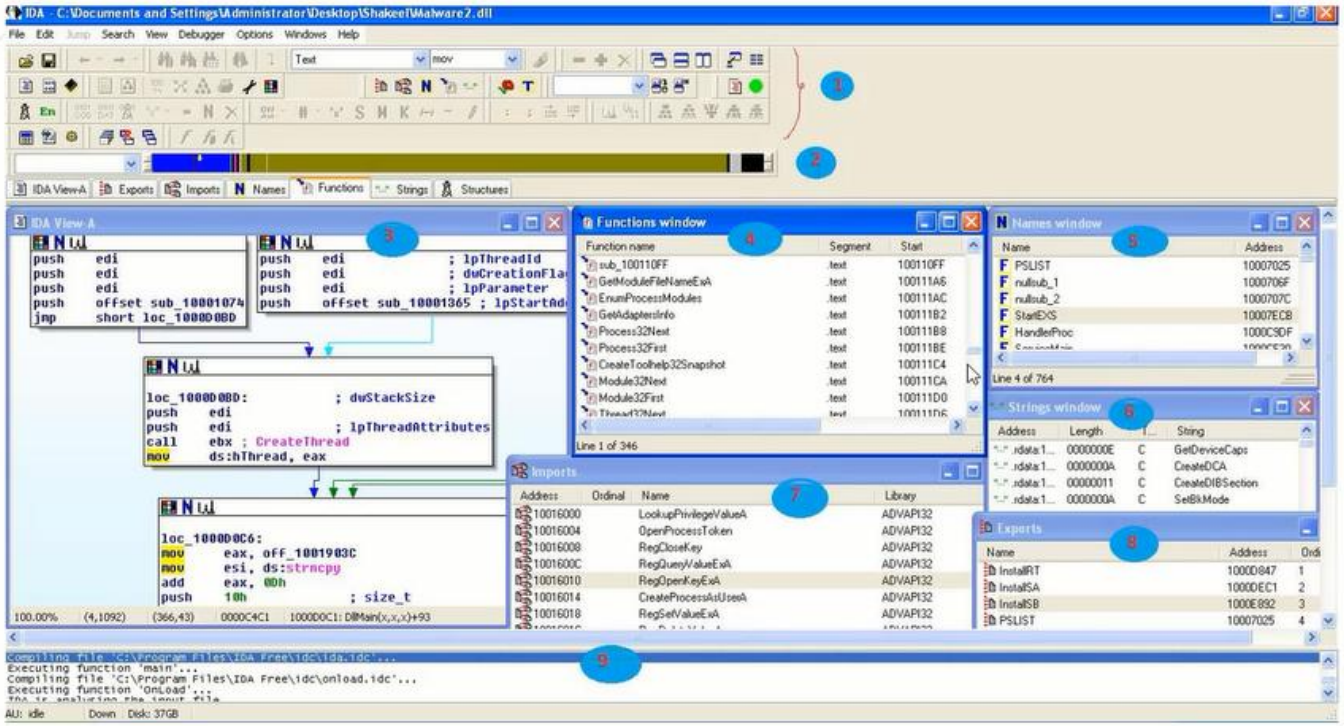
Slide 11 of 20

PowerPoint Slide Show - [Reverse Engineering.pptx] - PowerPoint

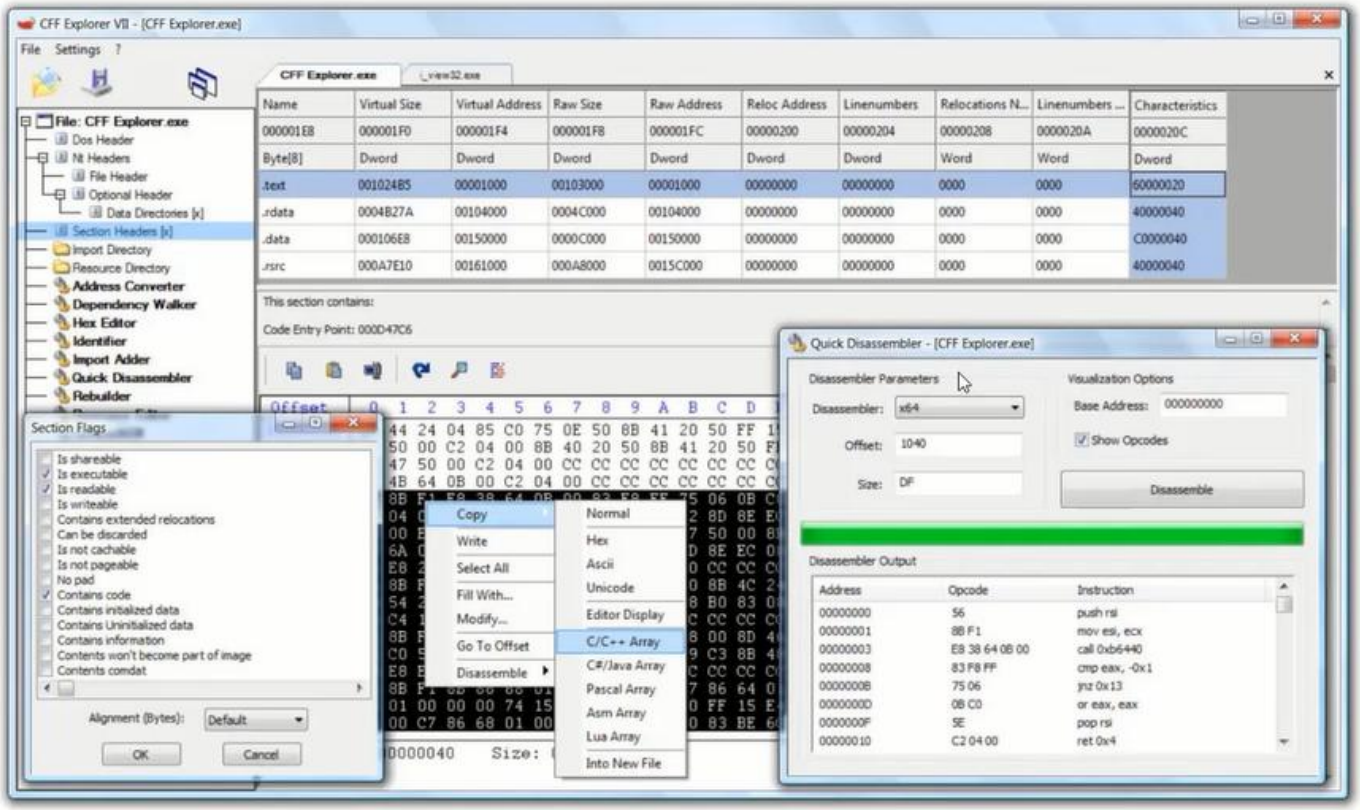
Crack Software or Apps

Slide 12 of 20

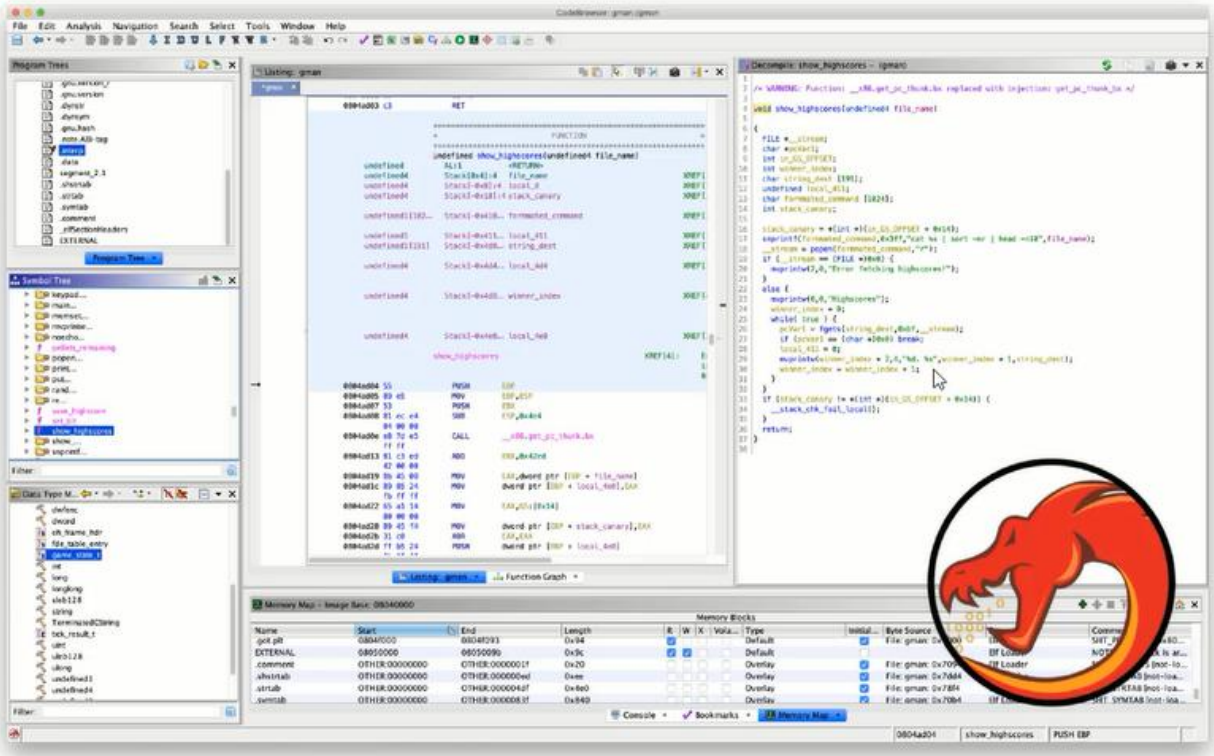
RE Tool: IDA Pro



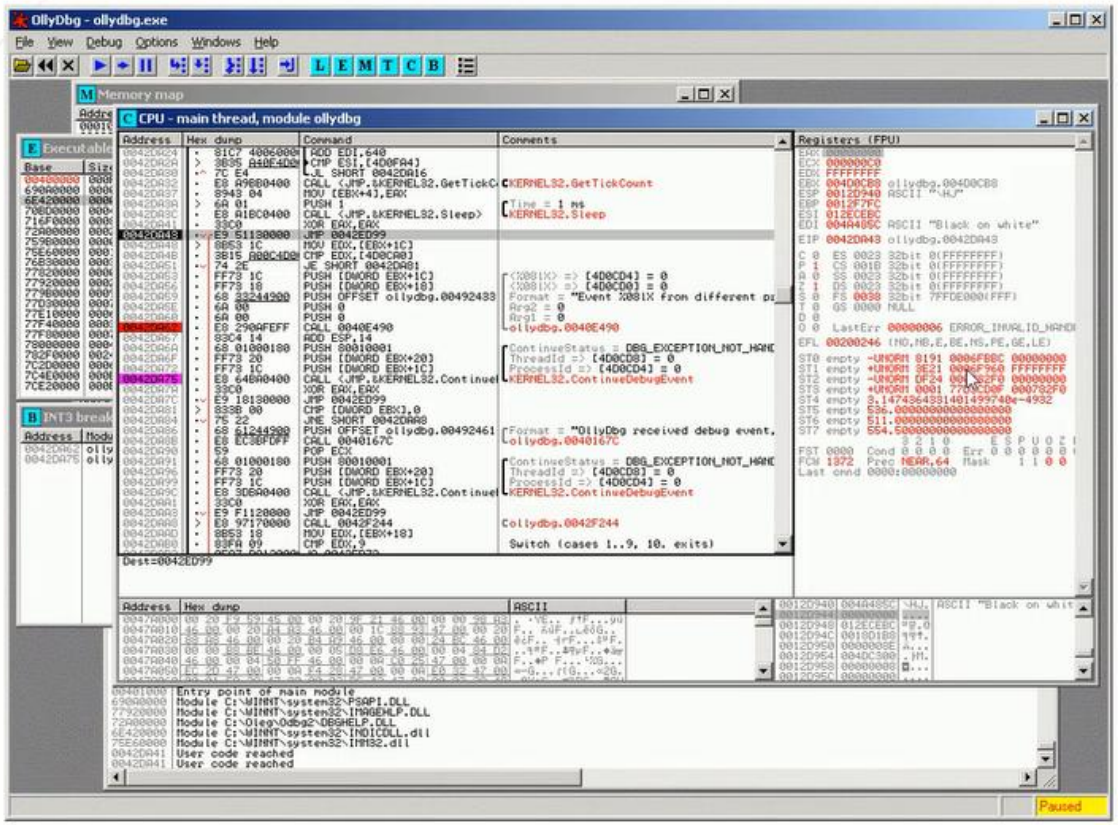
RE Tool: CFF Explorer



RE Tool: Ghidra



RE Tool: OllyDbg



Reverse Engineering Resources

- **Tools:** IDA Pro, CFF Explorer, Ghidra, OllyDbg, Itrace, radare2, apktool, and many more
- Assembly Language, Others Programing Language, Algorithm, Encryption

- **Learn**
  - https://ctf101.org/reverse-engineering/overview/
  - https://0xinfection.github.io/reversing/

Reverse Engineering - Problem Solving

- **picoCTF**
  - https://picoctf.org/
- **Tryhackme**
  - https://tryhackme.com/room/reverselfiles
  - https://tryhackme.com/room/windowsreversingintro
  - https://tryhackme.com/room/reloaded
  - https://tryhackme.com/room/brainstorm

Reverse Engineering

1

Course Instructor:

Hunter Alex,

CNSS, CISSP, OSINT, Digital Forensic

CEO, Team Matrix – Elite Hackers

Learning Objectives

- Reverse Engineering
- Software Reverse Engineering
- Reverse Engineering Process
- Reverse Engineering Tools
- Reverse Engineering Resources

Reverse Engineering

- Reverse → backwards, back
- Reverse → to change the direction, order, position, result, etc. of something to its opposite.
- Engineering → is the designing, testing and building of machines, structures and processes using maths and science.

Reverse Engineering

- The process of taking a piece of software or hardware and analyzing its functions and information flow so that its functionality and behavior can be understood. Malware is commonly reverse-engineered in cyber defense.
- Reverse engineering, also called backwards engineering or back engineering.

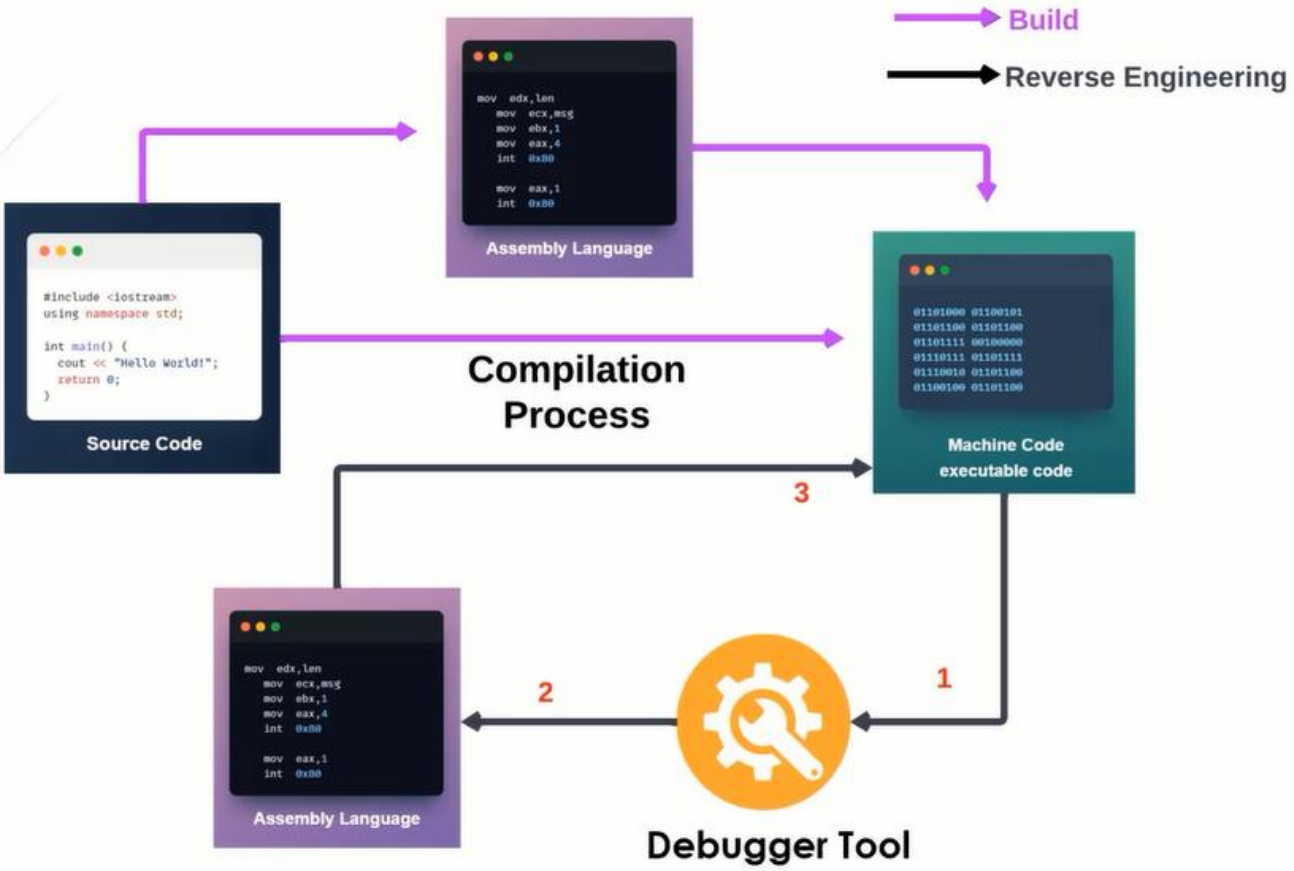
Reverse Engineering Fields

- Reverse engineering is applicable in the fields of **computer engineering, mechanical engineering, design, electronic engineering, software engineering, chemical engineering, and systems biology**.

Software reverse engineering (SRE)

- Software reverse engineering (SRE) is **the practice of analyzing a software system, either in whole or in part, to extract design and implementation information**

Software reverse engineering (SRE)



Purpose RS or SRE

- Program Bug Fixing
- Design Recovery
- Information Collection
- Extraction of the Structure
- Recover lost information.
- Corporate or Military Spying
- Competitor's intelligence
- Making Copies of the Original Product
- Parts Service or Repair
- Detect side effects.
- Failure Analysis
- Parts Improvement
- Diagnostics and Problem-Solving
- Paid App Free Use

Reverse Engineering in Cybersecurity

- Antivirus
- Malware analysis
- In the field of cyber security, the reverse engineering can be used to identify the details of a breach that how the attacker entered the system, and what steps were taken to breach the system.

PowerPoint Slide Show - [Reverse Engineering.pptx] - PowerPoint

Software

File Viewer Plus 2 License Key(s):

FA604-AFFCD-33021-04770-

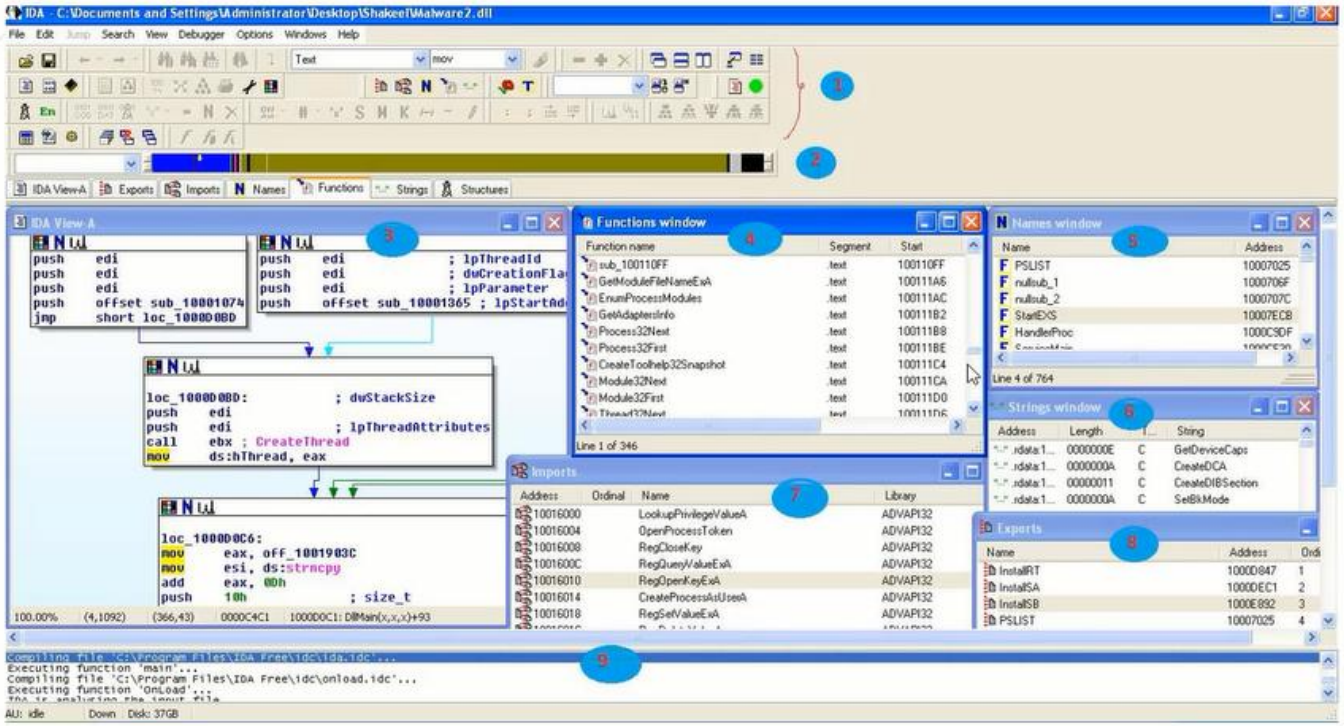
Slide 11 of 20

PowerPoint Slide Show - [Reverse Engineering.pptx] - PowerPoint

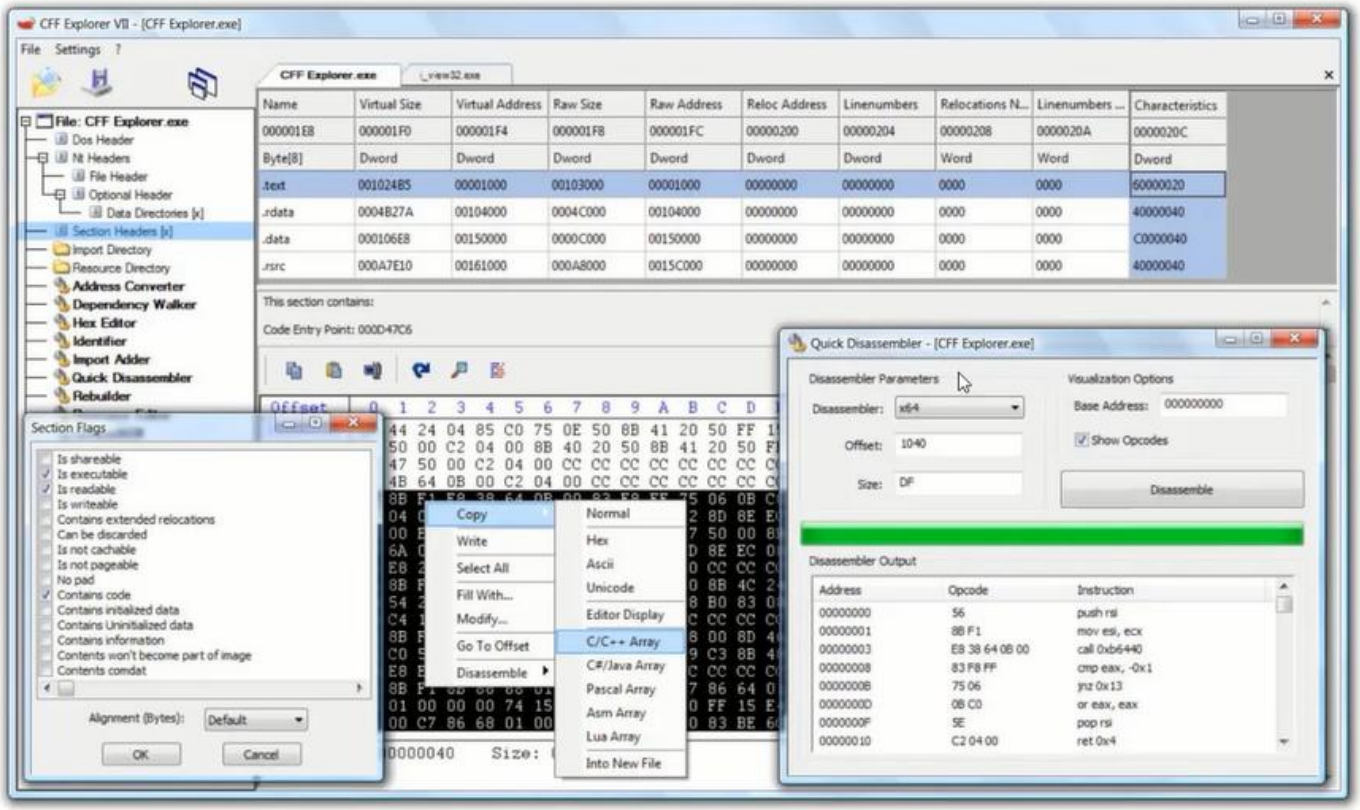
Crack Software or Apps

Slide 12 of 20

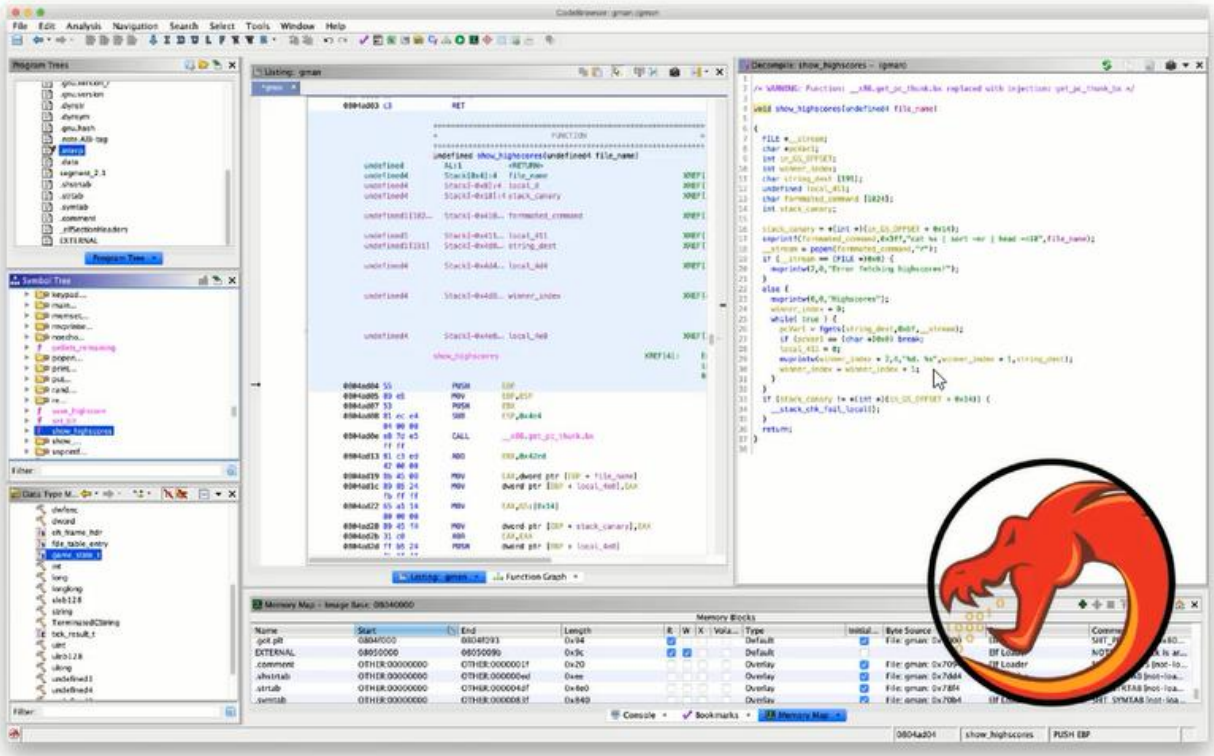
RE Tool: IDA Pro



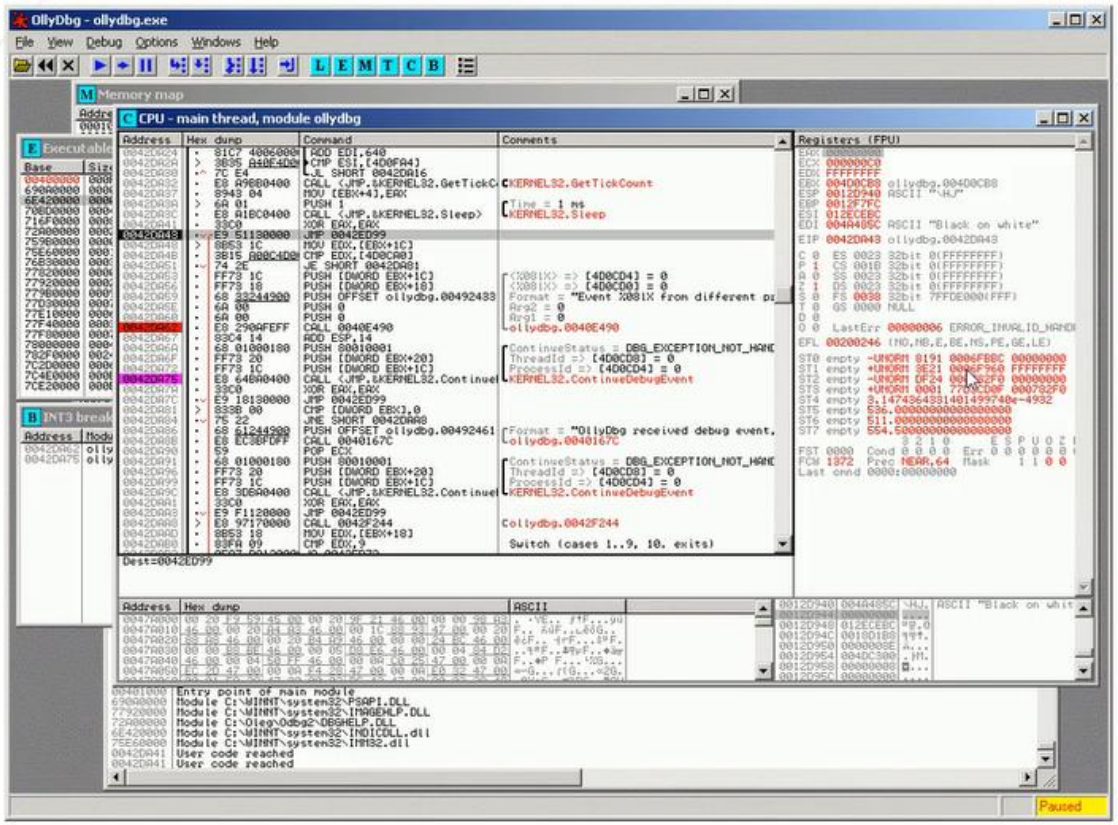
RE Tool: CFF Explorer



RE Tool: Ghidra



RE Tool: OllyDbg



Reverse Engineering Resources

- **Tools:** IDA Pro, CFF Explorer, Ghidra, OllyDbg, Itrace, radare2, apktool, and many more
- Assembly Language, Others Programing Language, Algorithm, Encryption

- **Learn**
  - https://ctf101.org/reverse-engineering/overview/
  - https://0xinfection.github.io/reversing/

Reverse Engineering - Problem Solving

- **picoCTF**
  - https://picoctf.org/
- **Tryhackme**
  - https://tryhackme.com/room/reverselfiles
  - https://tryhackme.com/room/windowsreversingintro
  - https://tryhackme.com/room/reloaded
  - https://tryhackme.com/room/brainstorm

PWN Or Binary Exploitation

- Binaries, or executables, are machine code for a computer to execute. For the most part, the binaries that you will face in CTFs are Linux ELF files or the occasional windows executable. Binary Exploitation is a broad topic within Cyber Security which really comes down to finding a vulnerability in the program and exploiting it to gain control of a shell or modifying the program's functions.

- Binary Exploitation Details → https://ctf101.org/binary-exploitation/overview/

Binary Exploitation

Binaries, or executables, are machine code for a computer to execute. For the most part, the binaries that you will face in CTFs are Linux ELF files or the occasional windows executable. Binary Exploitation is a broad topic within Cyber Security which really comes down to finding a vulnerability in the program and exploiting it to gain control of a shell or modifying the program's functions.

Common topics addressed by Binary Exploitation or 'pwn' challenges include:

- Registers
- The Stack
- Calling Conventions
- Global Offset Table (GOT)
- Buffers
  - Buffer Overflow
- Return Oriented Programming (ROP)
- Binary Security
  - No eXecute (NX)
  - Address Space Layout Randomization (ASLR)
  - Stack Canaries
  - Relocation Read-Only (RELRO)
- The Heap
  - Heap Exploitation
- Format String Vulnerability

Buffer Overflow

- **A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer.**
- A Buffer Overflow is a vulnerability in which data can be written which exceeds the allocated space, allowing an attacker to overwrite other data.

BUFFER OVERFLOW ATTACKS

Binary Exploitation

Binaries, or executables, are machine code for a computer to execute. For the most part, the binaries that you will face in CTFs are Linux ELF files or the occasional windows executable. Binary Exploitation is a broad topic within Cyber Security which really comes down to finding a vulnerability in the program and exploiting it to gain control of a shell or modifying the program's functions.

Common topics addressed by Binary Exploitation or 'pwn' challenges include:

- Registers
- The Stack
- Calling Conventions
- Global Offset Table (GOT)
- Buffers
  - Buffer Overflow
- Return Oriented Programming (ROP)
- Binary Security
  - No eXecute (NX)
  - Address Space Layout Randomization (ASLR)
  - Stack Canaries
  - Relocation Read-Only (RELRO)
- The Heap
  - Heap Exploitation
- Format String Vulnerability

Difference Between Binary Exploitation and Reverse Engineering

- Binary exploitation is intended to change the behavior of the binary, and reverse engineering is designed to understand how it works.
- Binary exploitation requires some reverse engineering; reverse engineering doesn't necessarily require binary exploitation.

PWN Or Binary Exploitation - Problem Solving

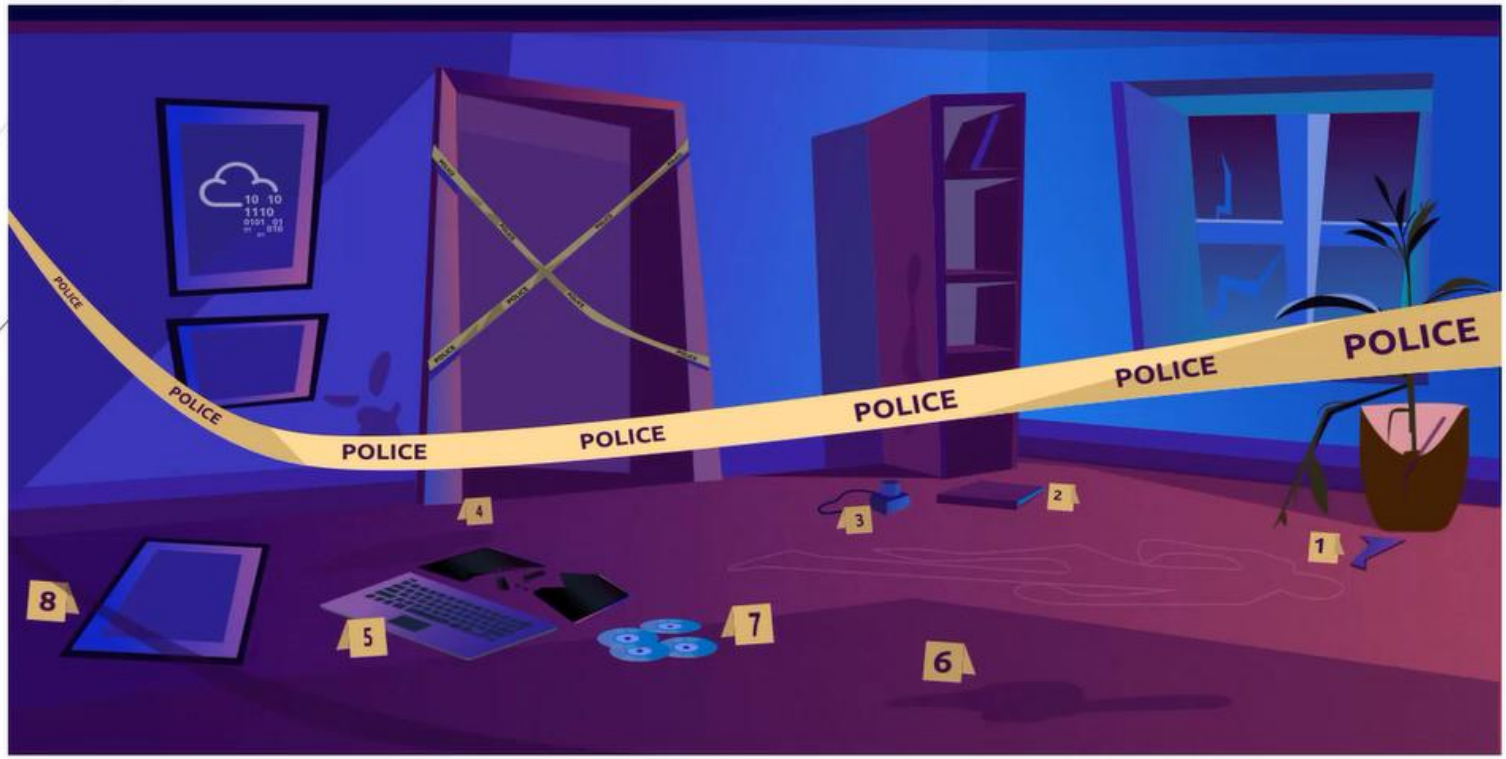
- **Tools:-** pwntools, ltrace , strings , gdb , radare 2, Ghidra and many more

- **Tryhackme**
  - https://tryhackme.com/room/pwn101
  - https://tryhackme.com/room/introtopwntools
  - https://tryhackme.com/room/binaryheaven

- **picoCTF**
  - https://picoctf.org/

- **Reference**
  - https://ctf101.org/binary-exploitation/what-is-a-format-string-vulnerability/
  - https://owasp.org/www-community/attacks/Format_string_attack
  - https://www.rapidtables.com/convert/number/hex-to-ascii.html

Digital Forensics | Networking



Forensics or Digital Forensics

Networking

- Forensics is the application of science to investigate crimes and establish facts. With the use and spread of digital systems, such as computers and smartphones, a new branch of forensics was born to investigate related crimes: computer forensics, which later evolved into, *digital forensics*.

- More formally, digital forensics is the application of computer science to investigate digital evidence for a legal purpose. Digital forensics is used in two types of investigations:

  1. **Public-sector investigations** refer to the investigations carried out by government and law enforcement agencies. They would be part of a crime or civil investigation.
  2. **Private-sector investigations** refer to the investigations carried out by corporate bodies by assigning a private investigator, whether in-house or outsourced. They are triggered by corporate policy violations.

Forensics or Digital Forensics

- In CTF "Forensic" challenges can include file format analysis, steganography, memory dump analysis or network packet capture analysis.
- **Networking, Steganography**
- **Details:** https://ctf101.org/forensics/overview/
- **Tools:-** Autopsy, hexeditor, foremost, binwalk, Wireshark, and many more

Digital Forensics - Problem Solving

- **Tryhackme**
  - https://tryhackme.com/room/btautopsye0
  - https://tryhackme.com/room/wireshark
- **picoCTF**
  - https://picoctf.org/

OSINT

Open Source Intelligence

Open-source intelligence, also known as OSINT, refers to gathering information from publicly available sources, such as social media, company websites, and news articles. Much data can be collected about a company or person through open-source intelligence.

OSINT Techniques

In a cybersecurity context, OSINT can be used to recon a target before performing a penetration test or to generate a report of the information a company is leaking through public sources. Cybercriminals use OSINT to collect information on a target before attacking; also, OSINT can be used to help guess a user's password. Many people use passwords that relate to themselves.

OSINT Defensive Techniques

OSINT can also be used in a defensive manner. Open source intel can be used to keep up with cybersecurity trends and the techniques cyber criminals are using right now. There are many websites that provide OSINT about cyber attack trends reported by cybersecurity professionals. Also, when a company is receiving unusual internet traffic, OSINT can be used to determine if the usual traffic is coming from a known malicious IP address (An IP address is a four part number that identifies the source of a network connect

OSINT - Problem Solving

- **Tryhackme**
  - https://tryhackme.com/room/ohsint
- **CTF Academy**
  - https://ctfacademy.github.io/osint/challenge1/index.htm

Keeber 1

"You have been applying to entry-level cybersecurity jobs focused on reconnaissance and open-source intelligence (OSINT). Great news! You got an interview with a small cybersecurity company; the Keeber Security Group. Before interviewing, they want to test your skills through a series of challenges oriented around investigating the Keeber Security Group.

The first step in your investigation is to find more information about the company itself. All we know is that the company is named Keeber Security Group and they are a cybersecurity startup. To start, help us find the person who registered their domain."

Miscellaneous | Misc

- Many challenges in CTFs will be completely random and unprecedented, requiring simply logic, knowledge, and patience to be solved. There is no sure-fire way to prepare for these, but as you complete more CTFs you will be able to recognize and hopefully have more clues on how to solve them.

- Example
  - https://github.com/ctfs/write-ups-2014/tree/master/ructf-2014-quals/misc-100
  - https://github.com/ctfs/write-ups-2014/tree/master/olympic-ctf-2014/crypting

CTF Events

- **DEF CON CTF - CTF World Cup**
  - Details: https://defcon.org/html/links/dc-ctf.html
- **CSAW CTF**
  - Details: https://ctf.csaw.io/
- **iCTF:** the International Capture The Flag Competition
  - Details: https://shellphish.net/ictf/

Bangladesh CTF Events

Bangladesh's cybersecurity platform BGD e-GOV CIRT – Events List

- **Cyber Drill For University Students**
- **Cyber Drill For Financial Institutes**
- **National Cyber Drill Bangladesh**

❑ **Details**

https://www.cirt.gov.bd/

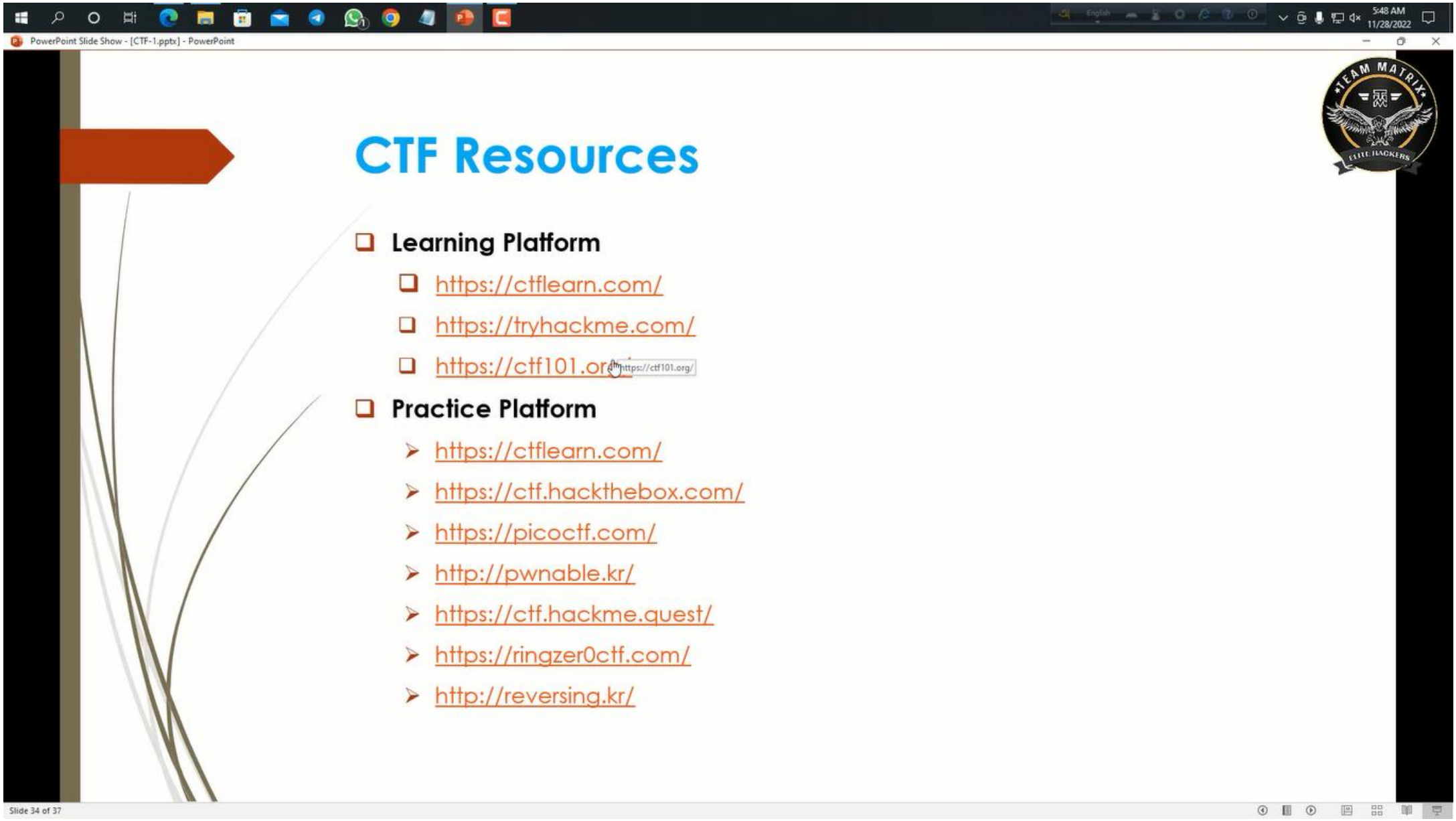
https://cyberdrill.cirt.gov.bd

CTF Events Tracker

- **Worldwide security CTF tracking site**
  - https://ctftime.org/ctfs/
  - https://ctftime.org/event/list/upcoming
  - https://ctf.hackthebox.com/

CTF Ranking

- **Global Ranking**
  - https://ctftime.org/stats/


PowerPoint Slide Show - [CTF-1.pptx] - PowerPoint
5:48 AM
11/28/2022
CTF Resources
Learning Platform
https://ctflearn.com/
https://tryhackme.com/
https://ctf101.org/
https://ctf101.org/
Practice Platform
https://ctflearn.com/
https://ctf.hackthebox.com/
https://picoctf.com/
http://pwnable.kr/
https://ctf.hackme.quest/
https://ringzer0ctf.com/
http://reversing.kr/
Slide 34 of 37

CTF Resources

- **GitHub**
  - https://github.com/JohnHammond/ctf-katana
  - https://github.com/ctfs/
  - https://github.com/p4-team/ctf/
- **YouTube Channel**
  - John Hammond
  - Hacker Joe
  - LiveOverflow
  - ShmooCon
  - IppSec
  - OWASP

CTF Resources

- **Writeup**
  - https://ctftime.org/writeups

CTF (Capture the flag)

By Team Matrix Elite Hackers

1.0 CTF

- ❑ CTF stands for Capture The Flag.
- ❑ Capture the Flag (CTF) is a special kind of information security competitions.
- ❑ A CTF is an event during which students, teachers, and professionals come together to compete against one another in an effort to test and expand cyber-security skills and awareness.

1.1 Class Requirements for CTF

- ❑ Cryptography
- ❑ Steganography
- ❑ OSINT
- ❑ LFI/RFI
- ❑ XSS
- ❑ SQLI
- ❑ Burp Suite
- ❑ Scanning and Networking
- ❑ Digital Forensic
- ❑ Kali Linux

1.2 There are three common types of CTFs

- ❑ **Jeopardy**
- ❑ **Attack-Defence**
- ❑ **Mixed Style**

1.3 CTF Categories

- ➢ **Cryptography**
- ➢ **Steganography**

- **Web Exploitation**
- **Forensics**
- **PWN Or Binary Exploitation**
- **Reverse Engineering**
- **Miscellaneous**
- **OSINT**

2.0 Cryptography

2.1 Hash Tools

- **Hash Analyzer -Kali Linux Tool**

  Hashid, Hash-identifier

- **Hash Analyzer - Online Tools:**
  - https://www.tunnelsup.com/hash-analyzer/
  - https://hashes.com/en/tools/hash_identifier
  - https://www.dcode.fr/hash-identifier
- **Hash Encoder/Decoder**
  - **Offline Tools - Hashcat, hash generator, BCTextEncoder, BlueCode**
  - https://gchq.github.io/CyberChef
  - https://md5hashing.net/
  - https://www.dcode.fr/hash-function

2.2 Cipher (or Cypher) Tools

- **Cipher Identifier**
  - https://www.dcode.fr/cipher-identifier
- **Shift Cipher**
  - https://www.dcode.fr/shift-cipher
- **Symbol Cipher**
  - https://www.dcode.fr/symbols-ciphers

❑ Encode/Decode

- https://cryptii.com
- https://gchq.github.io/CyberChef
- https://www.boxentriq.com/code-breaking/atbash-cipher
- https://morsecode.world
- https://www.dcode.fr/langage-brainfuck
- https://cryptii.com/pipes/binary-decoder
- https://github.com/hellman/xortool/

3.0 Steganography

3.1 Steganography Resource (Tools)

❑ Web Tools (Online Tools)

Steganography - A list of useful tools and resources

- https://0xrick.github.io/lists/stego/

Ultimate steganography solver website

- https://www.aperisolve.com/

Steganographic Encoder/Decoder

- https://futureboy.us/stegano/decinput.html

Steganography Online - Image

- https://stylesuxx.github.io/steganography/

❑ Text

Unicode Text - A web tool for unicode steganography , it can encode and decode text.

- https://www.irongeek.com/i.php?page=security/unicode-steganography-homoglyph-encoder

❑ Audio Analyzer

Sonic Visualiser

- https://www.sonicvisualiser.org/

Audacity - Multi-track audio editor

- https://www.audacityteam.org/

❑ Image Kali Linux Tools

Steghide — is a steganography program that hides data in various kinds of image and audio files.

- **http://steghide.sourceforge.net/**

Kali Linux >> sudo apt-get update, sudo apt install steghide

Binwalk - Binwalk is a tool for searching binary files like images and audio files for embedded files and data.

- **https://github.com/ReFirmLabs/binwalk**

Exiftool — Read and write meta information in files

- **https://linux.die.net/man/1/exiftool**

Pngtools — For various analysis related to PNGs

- **https://www.madebymikal.com/category/pngtools/**

Zsteg — PNG/BMP analysis

- **https://github.com/zed-0xff/zsteg/**

StegCracker — Steganography brute-force utility to uncover hidden data inside files.

- **https://github.com/Paradoxis/StegCracker**

❑ Image Windows Tools

OpenStego

- **https://www.openstego.com**

Stegsolve — Apply various steganography techniques to images

- **https://github.com/eugenekolo/sec-tools/tree/master/stego/stegsolve/stegsolve**
- **https://github.com/zardus/ctf-tools/blob/master/stegsolve/install**

HxD - Freeware Hex Editor and Disk Editor

- **https://mh-nexus.de/en/hxd/**

ExifTool - Read, Write and Edit Meta Information!

- **https://exiftool.org/**

QR Code Scanner

- **https://qrcodescan.in/**

Cryptography & Steganography Problem Solving

❑ Tryhackme – CTF collection Vol.1

- https://tryhackme.com/room/ctfcollectionvol1

✓ Task: 2,3,4,6,7,8,9,11,13,14,15,16,17,19,20

4.0 Web Exploitation

❑ picoCTF

- https://picoctf.org/

❑ Tryhackme

- https://tryhackme.com/room/learncyberin25days
- https://tryhackme.com/room/adventofcyber2
- https://tryhackme.com/room/adventofcyber3

5. Reverse Engineering

❑ Tools

- IDA Pro, CFF Explorer, Ghidra, OllyDbg, Itrace, radare2, apktool, and many more

❑ Learn

- https://ctf101.org/reverse-engineering/overview/
- https://0xinfection.github.io/reversing/

Problem Solving

❑ picoCTF

- https://picoctf.org/

❑ Tryhackme

- https://tryhackme.com/room/reverselfiles
- https://tryhackme.com/room/windowsreversingintro
- https://tryhackme.com/room/reloaded
- https://tryhackme.com/room/brainstorm

6. PWN Or Binary Exploitation

- ❑ **Details**
  - https://ctf101.org/binary-exploitation/overview/

- ❑ **Tools**
  - pwntools, Itrace , strings , gdb , radare 2, Ghidra and many more

Problem Solving

- ❑ **Tryhackme**
  - https://tryhackme.com/room/pwn101
  - https://tryhackme.com/room/introtopwntools
  - https://tryhackme.com/room/binaryheaven
- ❑ **picoCTF**
  - https://picoctf.org/
- ❑ **Reference**
  - https://ctf101.org/binary-exploitation/what-is-a-format-string-vulnerability/
  - https://owasp.org/www-community/attacks/Format_string_attack
  - https://www.rapidtables.com/convert/number/hex-to-ascii.html

7. Forensics or Digital Forensics

- ❑ **Details**
  - https://ctf101.org/forensics/overview/
- ❑ **Tools**
  - **Autopsy, hexeditor, foremost, binwalk, Wireshark, and many more**

Problem Solving

- ❑ **Tryhackme**
  - https://tryhackme.com/room/btautopsye0
  - https://tryhackme.com/room/wireshark

- ❑ **picoCTF**
  - https://picoctf.org/

8. OSINT Open-Source Intelligence

- **Tryhackme**
  - https://tryhackme.com/room/ohsint
- **CTF Academy**
  - https://ctfacademy.github.io/osint/challenge1/index.htm

9. Miscellaneous | Misc

- **Many challenges in CTFs will be completely random and unprecedented, requiring simply logic, knowledge, and patience to be solved. There is no sure-fire way to prepare for these, but as you complete more CTFs you will be able to recognize and hopefully have more clues on how to solve them.**
- **Example**
  - https://github.com/ctfs/write-ups-2014/tree/master/ructf-2014-quals/misc-100
  - https://github.com/ctfs/write-ups-2014/tree/master/olympic-ctf-2014/crypting

10. CTF Events

- **DEF CON CTF** - **CTF** World Cup
  - Details: https://defcon.org/html/links/dc-ctf.html
- **CSAW CTF**
  - Details: https://ctf.csaw.io/
- **iCTF:** the International Capture The Flag Competition
  - Details: https://shellphish.net/ictf/

11. Bangladesh CTF Events

- **Details**
  - https://www.cirt.gov.bd/
  - https://cyberdrill.cirt.gov.bd

12. CTF Events Tracker

- ❑ **Worldwide security CTF tracking site**
  - ➢ https://ctftime.org/ctfs/
  - ➢ https://ctftime.org/event/list/upcoming
  - ➢ https://ctf.hackthebox.com/

13. CTF Ranking

- ❑ **Global Ranking**
  - ➢ https://ctftime.org/stats/

14. CTF Resources

- ❑ **Learning Platform**
  - ❑ https://ctflearn.com/
  - ❑ https://tryhackme.com/
  - ❑ https://ctf101.org/
- ❑ **Practice Platform**
  - ❑ https://ctflearn.com/
  - ❑ https://ctf.hackthebox.com/
  - ❑ https://picoctf.com/
  - ❑ http://pwnable.kr/
  - ❑ https://ctf.hackme.quest/
  - ❑ https://ringzer0ctf.com/
  - ❑ http://reversing.kr/
- ❑ **GitHub**
  - ❑ https://github.com/JohnHammond/ctf-katana
  - ❑ https://github.com/ctfs/
  - ❑ https://github.com/p4-team/ctf/

- **YouTube Channel**
  - John Hammond
  - Hacker Joe
  - LiveOverflow
  - ShmooCon
  - IppSec
  - OWASP
- **Writeup**
  - https://ctftime.org/writeups

Team Matrix Elite Hacker

- **Facebook: https://www.facebook.com/teammatriix**
- **Google Site: https://sites.google.com/view/teammatrix**
- **Telegram Channel: https://t.me/teammatrixs**
- **YouTube Channel: https://www.youtube.com/c/TeamMatrixEliteHackers**
- **Phone: +8801303818319**