CTF 101: ROP the Flag

General Introduction to CTFs

By RoyalRoppers

Agenda

- Who are RoyalRoppers?
- What are CTFs?
- CTF categories
- CTFtime
- CTFs you “should” know
- How do I start?

Who are RoyalRoppers?

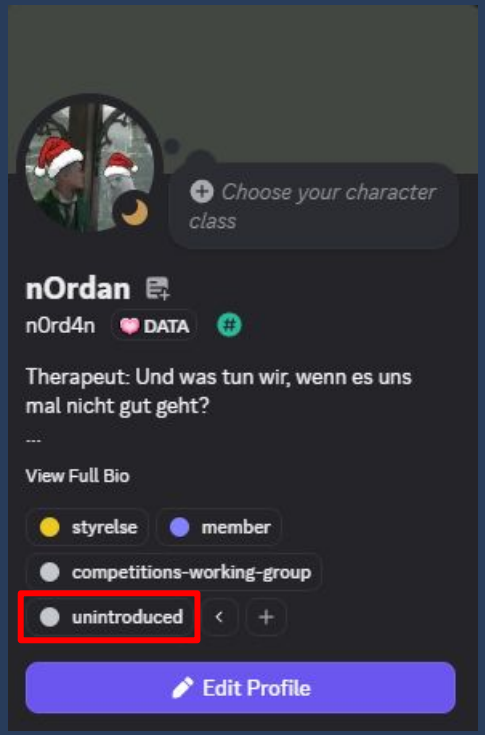
- A CTF team and an association
  - Mostly KTH students
  - Playing CTFs
  - (Hopefully) Meetups

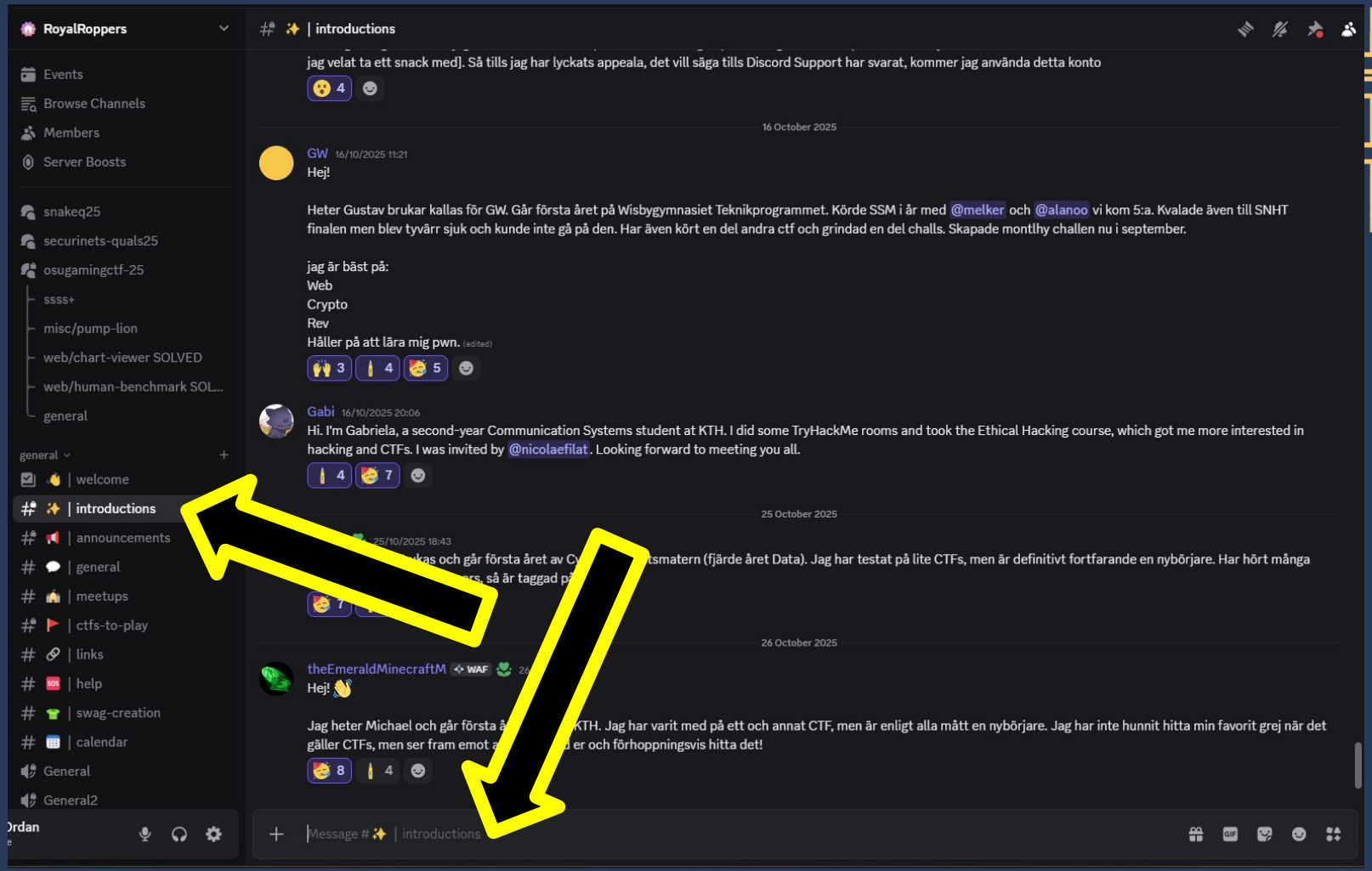
How to join RoyalRoppers?

Royal Roppers

RoyalRoppers is a Swedish student CTF team. We regularly play CTFs of all difficulty levels and have members ranging from absolute beginners to very experienced players. The majority of us live in Stockholm and we sometimes meet up to play CTFs onsite at KTH. Check out our ranking and past results on our CTFTime page.

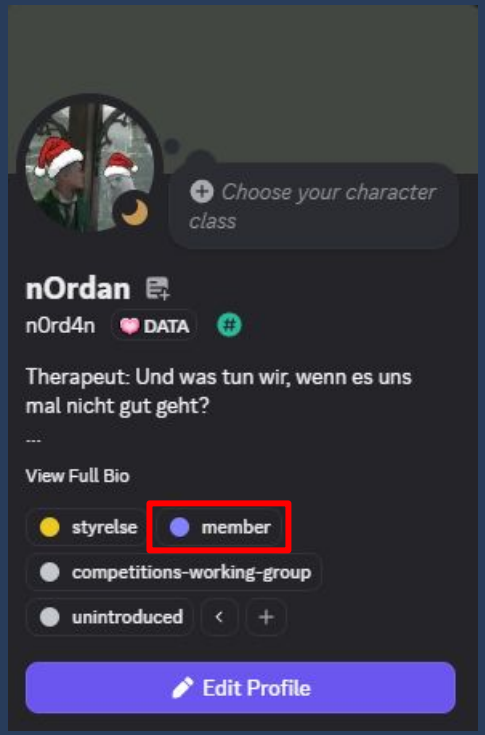
Want to play CTFs with us? Submit an application


Choose your character class
nOrdan
n0rd4n
DATA
Therapeut: Und was tun wir, wenn es uns mal nicht gut geht?
...
View Full Bio
styrelse
member
competitions-working-group
unintroduced
Edit Profile


RoyalRoppers
Events
Browse Channels
Members
Server Boosts
snakeq25
securinets-quals25
osugamingctf-25
ssss+
misc/pump-lion
web/chart-viewer SOLVED
web/human-benchmark SOL...
general
general
welcome
introductions
announcements
general
meetups
ctfs-to-play
links
help
swag-creation
calendar
General
General2
Ordan
introductions
jag velat ta ett snack med]. Så tills jag har lyckats appeala, det vill säga tills Discord Support har svarat, kommer jag använda detta konto
4
16 October 2025
GW 16/10/2025 11:21
Hej!
Heter Gustav brukar kallas för GW. Går första året på Wisbygymnasiet Teknikprogrammet. Körde SSM i år med @melker och @alanoo vi kom 5:a. Kvalade även till SNHT finalen men blev tyvärr sjuk och kunde inte gå på den. Har även kört en del andra ctf och grindad en del challs. Skapade montlhy challen nu i september.
jag är bäst på:
Web
Crypto
Rev
Håller på att lära mig pwn. (edited)
3
4
5
Gabi 16/10/2025 20:06
Hi. I'm Gabriela, a second-year Communication Systems student at KTH. I did some TryHackMe rooms and took the Ethical Hacking course, which got me more interested in hacking and CTFs. I was invited by @nicolaefilat. Looking forward to meeting you all.
4
7
25 October 2025
25/10/2025 18:43
26 October 2025
theEmeraldMinecraftM WAF
Hej!
Jag heter Michael och går första
KTH. Jag har varit med på ett och annat CTF, men är enligt alla mått en nybörjare. Jag har inte hunnit hitta min favorit grej när det gäller CTFs, men ser fram emot a
er och förhoppningsvis hitta det!
8
4
Message # | introductions


NICE


click


Choose your character class
nOrdan
n0rd4n
DATA
Therapeut: Und was tun wir, wenn es uns mal nicht gut geht?
...
View Full Bio
styrelse
member
competitions-working-group
unintroduced
Edit Profile

What are CTFs?

- Cyber security competitions
- Find flags to “prove” that you solved a challenge
- 2 types of CTFs
  - Jeopardy-style
  - Attack & Defense
- Why?
  - Learn and get experience
  - Fun!

Example flag: CTF101{th1s_1s_a_flag}

CTF categories

- Cryptography (Crypto)
- Web
- Reversing (Rev)
- Binary Exploitation (Pwn)
- Forensics
- Hardware
- Open Source Intelligence (OSINT)
- Misc

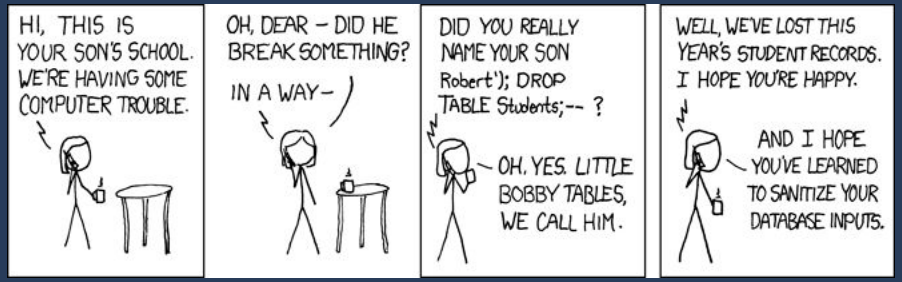
Cryptography (Crypto)

- Decoding or breaking encryption methods
- Classical Ciphers - Caesar, Vigenère, Substitution, etc.
- Modern - RSA, AES, ECC, etc.
- Hash Functions - MD5, SHA-256, etc.
- Useful tools:
  - SageMath
  - SymPy
  - dcode.fr
  - CyberChef

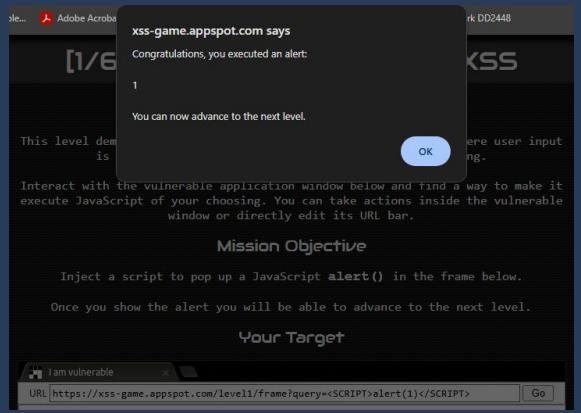
Example: EblnyEbccref → (Rot 13) → RoyalRoppers

Web Exploitation

- Vulnerabilities in websites or web applications
- Examples:
  - SQL injections
  - Command injections
  - Path traversal
  - Server-Side Template Injection (SSTI)
  - Cross-Site Request Forgery (CSRF)
  - Server-Side Request Forgery (SSRF)
  - Cross-Site Scripting (XSS)
  - Weird language-specific behaviors
  - XS-Leaks (side channels)
  - … *many* more
- Tools:
  - Burp Suite / Caido
  - Python + requests
  - fuzzers, sqlmap (*)

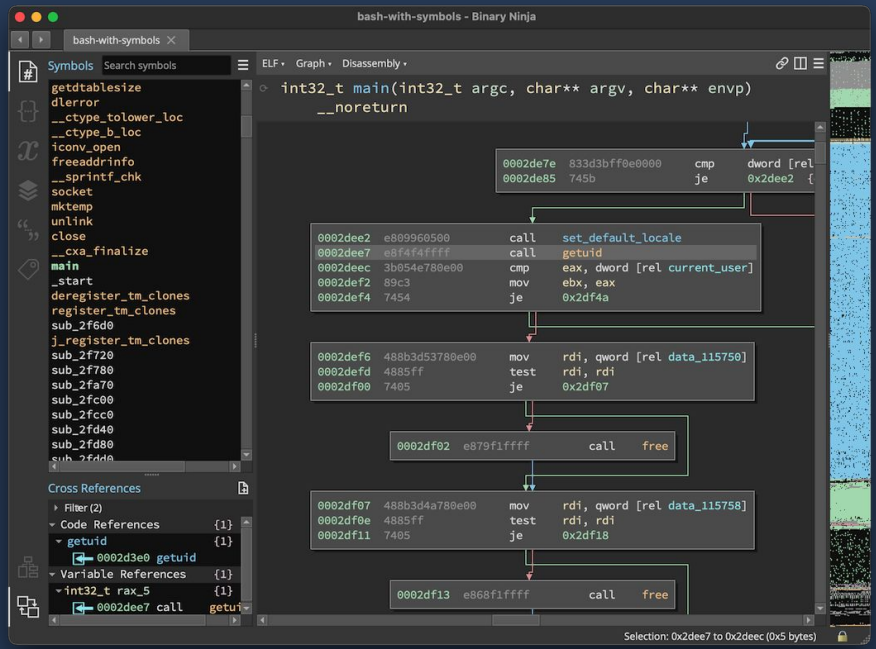



```
» ('b' + 'a' + + 'a' + 'a').toLowerCase()
← "banana"
```



Reverse Engineering (Rev)

- Analyze programs to understand behaviours
- Reverse binaries
- Tools:
  - Ghidra (Made by NSA)
  - Binary Ninja (also online)
  - IDA



Binary Exploitation (Pwn)

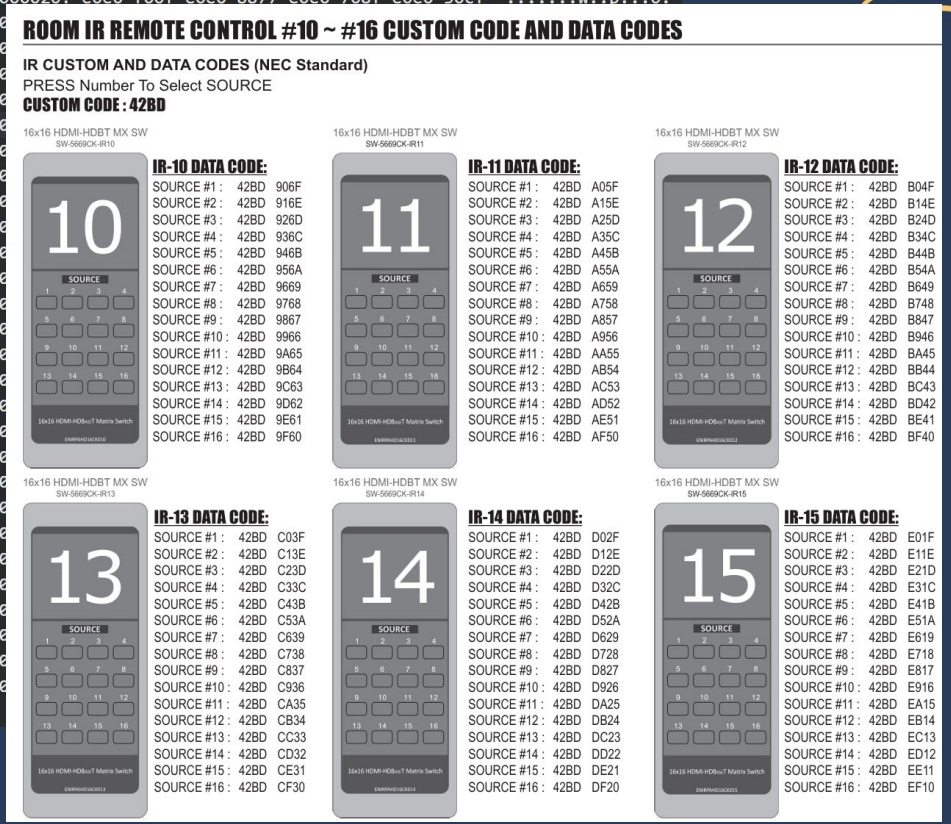
- Exploiting vulnerabilities in programs to execute arbitrary code or gain control
- Examples:
  - Format String vulnerabilities
  - Buffer/Heap overflows
  - ROP
  - Use after free
- Tools:
  - gdb + gef/pwndbg
  - x64dbg
  - pwntools

```c
#include <stdio.h>
#include <windows.h>

void win()
{
    printf("[!] Exploit executed successfully!\n");
    unsigned char shellcode[1000];
    SIZE_T size = sizeof(shellcode); // Size of the shellcode
    LPVOID lpAllocationStart = VirtualAlloc(NULL, size, MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE);
    if (lpAllocationStart == NULL) {
        printf("Memory allocation failed\n");
        return;
    }
    printf("[+] Enter shellcode: ");
    gets(shellcode);
    memcpy(lpAllocationStart, shellcode, size);
    printf("[+] Content of shellcode: %s\n", lpAllocationStart);      Elad Beber, 3 weeks ago • windows re
    ((void (*)())lpAllocationStart)();

}

void lose()
{
    printf("Exploit failed\n");
}

void vuln()
{
    char buffer[8];
    printf("[+] Enter a payload\n");
    gets(buffer);
    printf("[+] Content of buffer: %s\n", buffer);
}

void dump_win_address() {
    FILE *f = fopen("win.txt", "w");
    if (f == NULL) {
        printf("Error opening file!\n");
        return;
    }
    fprintf(f, "0x%p", win);
    fclose(f);
}

int main() {
    dump_win_address();
    vuln();
    lose();
    return 0;
}
```

Forensics

- Looking at data
- Different kinds of data:
  - Memory dumps
  - Network traffic
  - Unusual file formats

```
00000000: e0e0 40bf e0e0 8877 e0e0 708f e0e0 708f  ..@....w..p...p.
00000010: e0e0 f00f e0e0 20df e0e0 20df e0e0 10ef  ...... ... .....
00000020: e0e0 f00f e0e0 8877 e0e0 708f e0e0 30cf  .......w..p...0.
```



ROOM IR REMOTE CONTROL #10 ~ #16 CUSTOM CODE AND DATA CODES

IR CUSTOM AND DATA CODES (NEC Standard)
PRESS Number To Select SOURCE
CUSTOM CODE : 42BD

16x16 HDMI-HDBT MX SW
SW-5669CK-IR10

IR-10 DATA CODE:

SOURCE #1 :	42BD	906F
SOURCE #2 :	42BD	916E
SOURCE #3 :	42BD	926D
SOURCE #4 :	42BD	936C
SOURCE #5 :	42BD	946B
SOURCE #6 :	42BD	956A
SOURCE #7 :	42BD	9669
SOURCE #8 :	42BD	9768
SOURCE #9 :	42BD	9867
SOURCE #10 :	42BD	9966
SOURCE #11 :	42BD	9A65
SOURCE #12 :	42BD	9B64
SOURCE #13 :	42BD	9C63
SOURCE #14 :	42BD	9D62
SOURCE #15 :	42BD	9E61
SOURCE #16 :	42BD	9F60

16x16 HDMI-HDBT MX SW
SW-5669CK-IR11

IR-11 DATA CODE:

SOURCE #1 :	42BD	A05F
SOURCE #2 :	42BD	A15E
SOURCE #3 :	42BD	A25D
SOURCE #4 :	42BD	A35C
SOURCE #5 :	42BD	A45B
SOURCE #6 :	42BD	A55A
SOURCE #7 :	42BD	A659
SOURCE #8 :	42BD	A758
SOURCE #9 :	42BD	A857
SOURCE #10 :	42BD	A956
SOURCE #11 :	42BD	AA55
SOURCE #12 :	42BD	AB54
SOURCE #13 :	42BD	AC53
SOURCE #14 :	42BD	AD52
SOURCE #15 :	42BD	AE51
SOURCE #16 :	42BD	AF50

16x16 HDMI-HDBT MX SW
SW-5669CK-IR12

IR-12 DATA CODE:

SOURCE #1 :	42BD	B04F
SOURCE #2 :	42BD	B14E
SOURCE #3 :	42BD	B24D
SOURCE #4 :	42BD	B34C
SOURCE #5 :	42BD	B44B
SOURCE #6 :	42BD	B54A
SOURCE #7 :	42BD	B649
SOURCE #8 :	42BD	B748
SOURCE #9 :	42BD	B847
SOURCE #10 :	42BD	B946
SOURCE #11 :	42BD	BA45
SOURCE #12 :	42BD	BB44
SOURCE #13 :	42BD	BC43
SOURCE #14 :	42BD	BD42
SOURCE #15 :	42BD	BE41
SOURCE #16 :	42BD	BF40

16x16 HDMI-HDBT MX SW
SW-5669CK-IR13

IR-13 DATA CODE:

SOURCE #1 :	42BD	C03F
SOURCE #2 :	42BD	C13E
SOURCE #3 :	42BD	C23D
SOURCE #4 :	42BD	C33C
SOURCE #5 :	42BD	C43B
SOURCE #6 :	42BD	C53A
SOURCE #7 :	42BD	C639
SOURCE #8 :	42BD	C738
SOURCE #9 :	42BD	C837
SOURCE #10 :	42BD	C936
SOURCE #11 :	42BD	CA35
SOURCE #12 :	42BD	CB34
SOURCE #13 :	42BD	CC33
SOURCE #14 :	42BD	CD32
SOURCE #15 :	42BD	CE31
SOURCE #16 :	42BD	CF30

16x16 HDMI-HDBT MX SW
SW-5669CK-IR14

IR-14 DATA CODE:

SOURCE #1 :	42BD	D02F
SOURCE #2 :	42BD	D12E
SOURCE #3 :	42BD	D22D
SOURCE #4 :	42BD	D32C
SOURCE #5 :	42BD	D42B
SOURCE #6 :	42BD	D52A
SOURCE #7 :	42BD	D629
SOURCE #8 :	42BD	D728
SOURCE #9 :	42BD	D827
SOURCE #10 :	42BD	D926
SOURCE #11 :	42BD	DA25
SOURCE #12 :	42BD	DB24
SOURCE #13 :	42BD	DC23
SOURCE #14 :	42BD	DD22
SOURCE #15 :	42BD	DE21
SOURCE #16 :	42BD	DF20

16x16 HDMI-HDBT MX SW
SW-5669CK-IR15

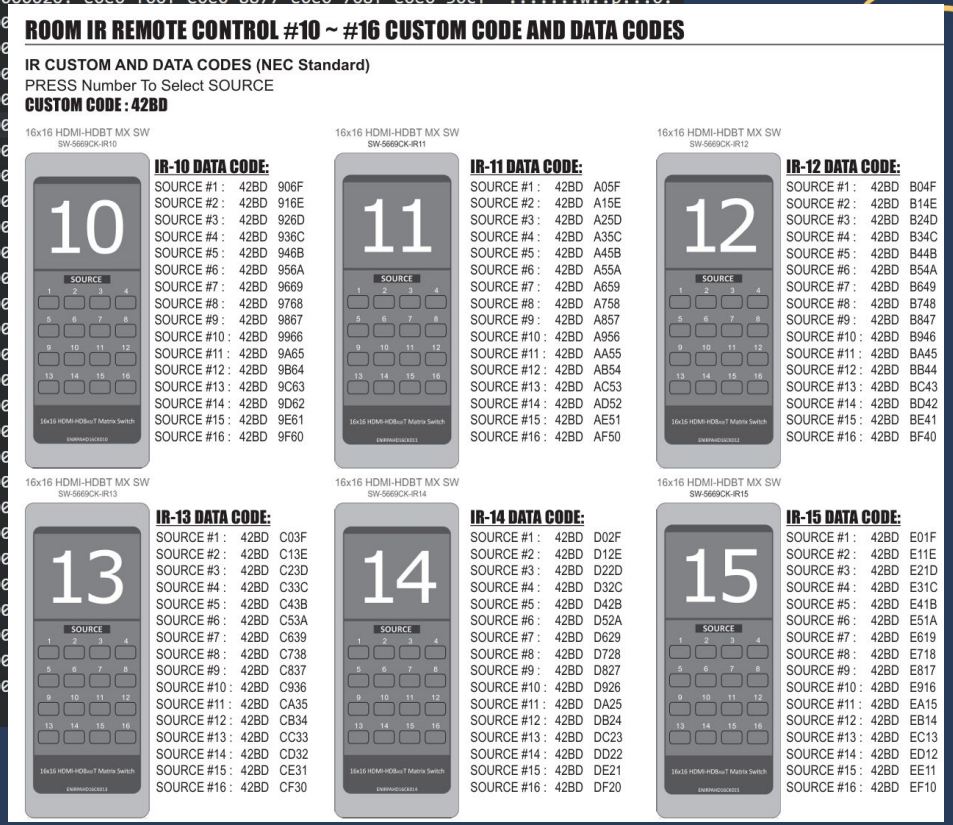
IR-15 DATA CODE:

SOURCE #1 :	42BD	E01F
SOURCE #2 :	42BD	E11E
SOURCE #3 :	42BD	E21D
SOURCE #4 :	42BD	E31C
SOURCE #5 :	42BD	E41B
SOURCE #6 :	42BD	E51A
SOURCE #7 :	42BD	E619
SOURCE #8 :	42BD	E718
SOURCE #9 :	42BD	E817
SOURCE #10 :	42BD	E916
SOURCE #11 :	42BD	EA15
SOURCE #12 :	42BD	EB14
SOURCE #13 :	42BD	EC13
SOURCE #14 :	42BD	ED12
SOURCE #15 :	42BD	EE11
SOURCE #16 :	42BD	EF10

Forensics

- Looking at data
- Different kinds of data:
  - Memory dumps
  - Network traffic
  - Unusual file formats
- Tools:
  - Strings, Binwalk, Foremost
  - Wireshark
  - 010 editor
  - Volatility

```
00000000: e0e0 40bf e0e0 8877 e0e0 708f e0e0 708f  ..@....w..p...p.
00000010: e0e0 f00f e0e0 20df e0e0 20df e0e0 10ef  ...... ... .....
00000020: e0e0 f00f e0e0 8877 e0e0 708f e0e0 30cf  .......w..p...0.
```



ROOM IR REMOTE CONTROL #10 ~ #16 CUSTOM CODE AND DATA CODES

IR CUSTOM AND DATA CODES (NEC Standard)
PRESS Number To Select SOURCE
CUSTOM CODE : 42BD

16x16 HDMI-HDBT MX SW
SW-5669CK-IR10

IR-10 DATA CODE:

SOURCE #1 :	42BD	906F
SOURCE #2 :	42BD	916E
SOURCE #3 :	42BD	926D
SOURCE #4 :	42BD	936C
SOURCE #5 :	42BD	946B
SOURCE #6 :	42BD	956A
SOURCE #7 :	42BD	9669
SOURCE #8 :	42BD	9768
SOURCE #9 :	42BD	9867
SOURCE #10 :	42BD	9966
SOURCE #11 :	42BD	9A65
SOURCE #12 :	42BD	9B64
SOURCE #13 :	42BD	9C63
SOURCE #14 :	42BD	9D62
SOURCE #15 :	42BD	9E61
SOURCE #16 :	42BD	9F60

16x16 HDMI-HDBT MX SW
SW-5669CK-IR11

IR-11 DATA CODE:

SOURCE #1 :	42BD	A05F
SOURCE #2 :	42BD	A15E
SOURCE #3 :	42BD	A25D
SOURCE #4 :	42BD	A35C
SOURCE #5 :	42BD	A45B
SOURCE #6 :	42BD	A55A
SOURCE #7 :	42BD	A659
SOURCE #8 :	42BD	A758
SOURCE #9 :	42BD	A857
SOURCE #10 :	42BD	A956
SOURCE #11 :	42BD	AA55
SOURCE #12 :	42BD	AB54
SOURCE #13 :	42BD	AC53
SOURCE #14 :	42BD	AD52
SOURCE #15 :	42BD	AE51
SOURCE #16 :	42BD	AF50

16x16 HDMI-HDBT MX SW
SW-5669CK-IR12

IR-12 DATA CODE:

SOURCE #1 :	42BD	B04F
SOURCE #2 :	42BD	B14E
SOURCE #3 :	42BD	B24D
SOURCE #4 :	42BD	B34C
SOURCE #5 :	42BD	B44B
SOURCE #6 :	42BD	B54A
SOURCE #7 :	42BD	B649
SOURCE #8 :	42BD	B748
SOURCE #9 :	42BD	B847
SOURCE #10 :	42BD	B946
SOURCE #11 :	42BD	BA45
SOURCE #12 :	42BD	BB44
SOURCE #13 :	42BD	BC43
SOURCE #14 :	42BD	BD42
SOURCE #15 :	42BD	BE41
SOURCE #16 :	42BD	BF40

16x16 HDMI-HDBT MX SW
SW-5669CK-IR13

IR-13 DATA CODE:

SOURCE #1 :	42BD	C03F
SOURCE #2 :	42BD	C13E
SOURCE #3 :	42BD	C23D
SOURCE #4 :	42BD	C33C
SOURCE #5 :	42BD	C43B
SOURCE #6 :	42BD	C53A
SOURCE #7 :	42BD	C639
SOURCE #8 :	42BD	C738
SOURCE #9 :	42BD	C837
SOURCE #10 :	42BD	C936
SOURCE #11 :	42BD	CA35
SOURCE #12 :	42BD	CB34
SOURCE #13 :	42BD	CC33
SOURCE #14 :	42BD	CD32
SOURCE #15 :	42BD	CE31
SOURCE #16 :	42BD	CF30

16x16 HDMI-HDBT MX SW
SW-5669CK-IR14

IR-14 DATA CODE:

SOURCE #1 :	42BD	D02F
SOURCE #2 :	42BD	D12E
SOURCE #3 :	42BD	D22D
SOURCE #4 :	42BD	D32C
SOURCE #5 :	42BD	D42B
SOURCE #6 :	42BD	D52A
SOURCE #7 :	42BD	D629
SOURCE #8 :	42BD	D728
SOURCE #9 :	42BD	D827
SOURCE #10 :	42BD	D926
SOURCE #11 :	42BD	DA25
SOURCE #12 :	42BD	DB24
SOURCE #13 :	42BD	DC23
SOURCE #14 :	42BD	DD22
SOURCE #15 :	42BD	DE21
SOURCE #16 :	42BD	DF20

16x16 HDMI-HDBT MX SW
SW-5669CK-IR15

IR-15 DATA CODE:

SOURCE #1 :	42BD	E01F
SOURCE #2 :	42BD	E11E
SOURCE #3 :	42BD	E21D
SOURCE #4 :	42BD	E31C
SOURCE #5 :	42BD	E41B
SOURCE #6 :	42BD	E51A
SOURCE #7 :	42BD	E619
SOURCE #8 :	42BD	E718
SOURCE #9 :	42BD	E817
SOURCE #10 :	42BD	E916
SOURCE #11 :	42BD	EA15
SOURCE #12 :	42BD	EB14
SOURCE #13 :	42BD	EC13
SOURCE #14 :	42BD	ED12
SOURCE #15 :	42BD	EE11
SOURCE #16 :	42BD	EF10

Hardware

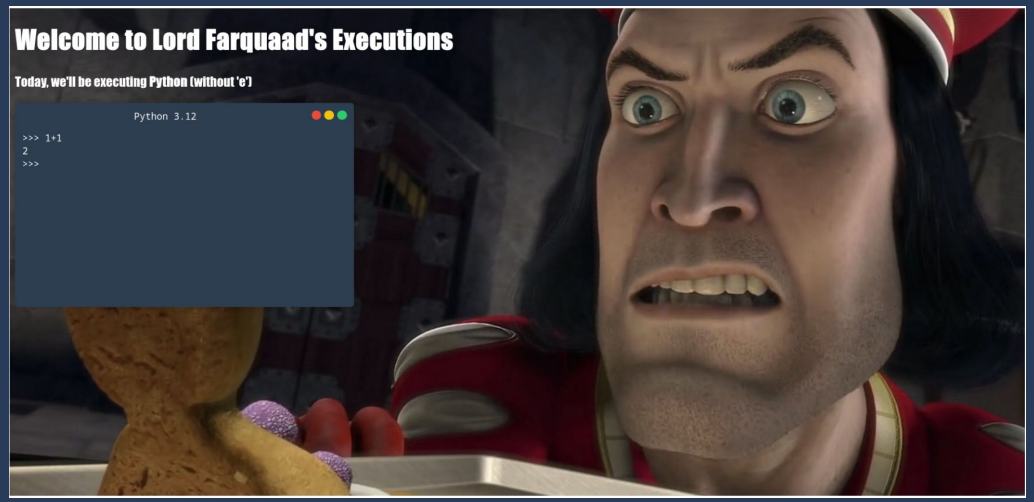
- Interact with real or simulated hardware
- Knowledge in different categories needed

Open Source Intelligence (OSINT)

- Find publicly accessible information online
- Things to find:
  - Locations
  - Names
  - Contacts
  - Online Accounts
- Tools:
  - Google Lens
  - AI
  - 360° Panorama Viewer
  - Google Street View
  - OpenStreetMap
  - Social Media

Misc

- Challenges that don’t fit into other categories
- Examples
  - AI/LLM
  - Custom puzzles
  - PyJail
  - Linux Shell “Jail”
  - Other sandbox escapes (e.g., Nix)



CTFtime

CTFs you “should” know

Swedish CTFs

- Säkerhets-SM

Undutmaningen
(FRA/MUST/SÄPO)

Crate CTF (FOI)

MidnightSun CTF

LA CTF 2025
(University of California - USA)

KalmarCTF 2025
kalmarunionen - Denmark

DEF CON CTF
(Nautilus Institute - USA)

ENOWARS 9
(Technische Universität Berlin - Germany)

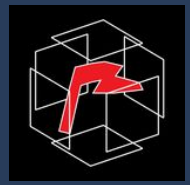
PlaidCTF 2025
(Plaid Parliament of Pwning, Carnegie Mellon University - USA)

Crypto CTF 2025
ASIS - Iran

DownUnderCTF 2025
(Collection of CTF teams - Australia)

snakeCTF 2025
(University of Udine - Italy)

Google Capture The Flag 2025
(Google Security Team)



BuckeyeCTF 2025
The Ohio State University - USA

smileyCTF 2025
(.;;;. - USA)

TAMUctf 2025
Texas A&M University - USA

osu!gaming CTF 2025
(Project Sekai - N/A)

LakeCTF Quals 25-26
(EPFL - Switzerland)

SEC-T

SECURITY FEST

Security Fest

Midnight Sun Conference

How do I start?

How do I start?

1. You are here. Good start!
2. Play! Play! Play!
3. Solve together with others!
4. Feel free to ask other people for help!
5. Have fun!