

CTF HOW TO

HARDWARE	1
• ESP32 chip board	1
• Memory	2
WEB	2
• Curl	2
• Brup Suite	2
• ffluf (url)	2
Forensics	2
PWN	3
STEGANOGRAPHY	3
• IMAGES	3
CAR	3
Helpful notes	3
Helpful links	3
CTF SPECIFIC	3
• HTH	3
• SHMOOCON steganography	4
◦ Layered QR code / QR code reconstruction	4
◦ STL file	4
◦ AWS	5
◦ PCAP	5
◦ DOCKER	6
• HACK-A-SAT	6
• THOTCON	6
◦ crypto	6
◦ RF	7
◦ Badge	7
• BATTELLE CYBER CHALLENGES	
https://solvers.battelle.org/cyber-challenge/cyber-challenge	7
◦ REVERSE ENGINEERING	7
◦ BINARY EXPLOITATION	8
◦ FORENSICS / CRYPTO	8
◦ MULTI-ARCHITECTURE SHELLCODE	9

HARDWARE

- ESP32 chip board

- How to connect to a esp32 chip board connect through UART.
 - serial connection through the usb port (micro usb / type c) if it has a FTDI chip (usb to serial). FTDI chip is usually connected to the esp32
 - Pin out esp32 chip, connect to Rx, Tx, and ground or io, gpio, and ground. Use uart to usb cable
- After plugged in, in Terminal run either
 - Picocom
 - example: `picocom /dev/ttyUSB0 -b 115200`
 - example: `picocom /dev/ttyUSB0 -b 9600`
 - `picocom (port in use) (baud rate #####)`
 - Esptool
 - Putty
 - Screen
 - Arduino IDE
 - minicom
- Helpful notes
 - Common baud rates: 9600, 1200, 2400, 4800, 19200, 38400, 57600, and 115200 bps
 - To find ports in use run in terminal `lsusb` or `ls /dev/tty*`

- Memory

- command to dump 4MB of flash to a file: `python -m esptool --port COM5 -b 115200 read_flash 0 0x4000000 flashdump.bin`
- `python3 -m esptool --port /dev/ttyUSB0 -b 9600 read_flash 0 0x4000000 flashdump.bin`
- - Esptool (port used) (bod rate) (command read flash from memory location #### to memory location ####) (name of file to create and put data in)
 - `binwalk`
 - To view strings use in terminal command `*strings*` with your .bin file `strings flashdump.bin`
 - Ghidra
 - GHex
 -

WEB

- Curl
 - Web request
- Burp Suite
- ffuf (url)
-

RF

- GQRX
- Universal Radio
- Apps to use from ZeroChaos for fox hunt and ect
 - nRF Connect
 - Flipper
 - AirGuard
 - Aruba Utilities
 - Wifi Analyzer
 - WiFiman
 - Meshtastic
 - goTenna
 - Zello
-

Forensics

-

PWN

STEGANOGRAPHY

- IMAGES

-

- https://www.aperisolve.com/979702d356135c1ceef557a17e30d9a8#google_vignette

-

CAR

- <https://github.com/LittleBlondeDevil/TruckDevil>
 - > git clone <https://github.com/LittleBlondeDevil/TruckDevil.git>
- <https://github.com/iDoka/awesome-canbus>
-

Helpful notes and tools

- Audacity
- Wireshark
- Arduinio IDE
- Ghidra
- Burp Suite
- Putty
- GHex
-

Helpful links

- <https://medium.com/quiknapp/fuzz-faster-with-ffuf-c18c031fc480>
- <https://cantreally.cyou/>
- <https://www.dcode.fr/>
- <https://gchq.github.io/CyberChef/>
- <https://python-can.readthedocs.io/en/stable/>
- <https://github.com/iDoka/awesome-canbus>

Setup

- `sudo apt install python3`
- Pwntools
 - `sudo apt-get install python3 python3-pip python3-dev git libssl-dev libffi-dev build-essential`
 - `python3 -m pip install --upgrade pip`
 - `python3 -m pip install --upgrade pwntools`
- CANBus
 - `sudo apt update`
 - `sudo apt -y install can-utils`
 - `pip install python-can`
- Visual Studio Code
 - `sudo apt-get install wget gpg`
 - `wget -qO- https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor > packages.microsoft.gpg`
 - `sudo install -D -o root -g root -m 644 packages.microsoft.gpg /etc/apt/keyrings/packages.microsoft.gpg`
 - `sudo sh -c 'echo "deb [arch=amd64,arm64,armhf signed-by=/etc/apt/keyrings/packages.microsoft.gpg] https://packages.microsoft.com/repos/code stable main" > /etc/apt/sources.list.d/vscode.list'`
 - `rm -f packages.microsoft.gpg`
 -
 - `sudo apt install apt-transport-https`
 - `sudo apt update`
 - `sudo apt install code # or code-insiders`
 -
- Hardware
 - Picocom
 - `sudo apt update`
 - `sudo apt -y install picocom`
 - Esptool
 - `sudo pip install esptool`
 - `sudo apt -y install python3-pip`
 - Putty
 - `sudo add-apt-repository universe`
 - `sudo apt update`
 - `sudo apt install -y putty`
 - Screen
 - `sudo apt-get update -y`
 - `sudo apt-get install screen -y`
 - Minicom
 - `sudo apt-get install minicom -y`

- Memory
 - Binwalk
 - sudo apt update
 - sudo apt -y install binwalk
 - Ghidra
 - sudo apt-get install openjdk-17-jdk
 - download Ghidra from its [official repository](#) page and extract it into a directory.
 - After extracting the files, please go to the directory through the cd command.
 - chmod +x ghirdRun
 - ./ghirdaRun
 - Create a desktop entry file
 - "[Desktop Entry]
 - Version=10.0
 - Type=Application
 - Terminal=false
 - Icon=/home/artemix/ghidra/support
 - Exec=sh /home/artemix/ghidra/ghidraRun.sh
 - Name=Ghidra"
 - Replace the data in the **Icon** and **Exec** fields with the location of the Ghidra icon and the launch script in your machine.
 - Save the file as "Ghidra.desktop" in the Desktop directory.
 - Right-click on the file and set it to **Allow Launching** or fire up a terminal and use the chmod command to make it executable for all users.
 - chmod a+x Ghidra.desktop
 -
 - Ghidra using snap
 - sudo apt update
 - sudo apt install snapd
 - sudo snap install ghidra
 - Ghex
 - sudo apt-get update
 - sudo apt-get install ghex -y
- Web
 - Burp
 - **Download:** [Burp Suite](#)
 -
- Wireless
 - Wireshark
 -
- JDK 17
 - Open JDK
 - sudo apt update

- sudo apt install -y openjdk-17-jdk
 - sudo apt install -y openjdk-17-jre
- Oracle JDK 17
 - sudo apt update
 - sudo apt install -y libc6-x32 libc6-i386
 - wget https://download.oracle.com/java/17/latest/jdk-17_linux-x64_bin.deb
 - sudo dpkg -i jdk-17_linux-x64_bin.deb
 - sudo update-alternatives --install /usr/bin/java java /usr/lib/jvm/jdk-17/bin/java 1
- java -version
- Wine
 -


CTF SPECIFIC

- HTH
 -
- SHMOOCON steganography
 - Layered QR code / QR code reconstruction

Stage 1: STONE

Layered QR Codes, with GeolP foo

- Each contest poster has a different QR code, overtly pointing to a dynamic URL to a LufCo site
- By changing light gray to black and dark gray to white, covert QR and URL are uncovered
- When attempted from a US IP, points to LufCo's website; use a VPN outside the US points to the next contest page



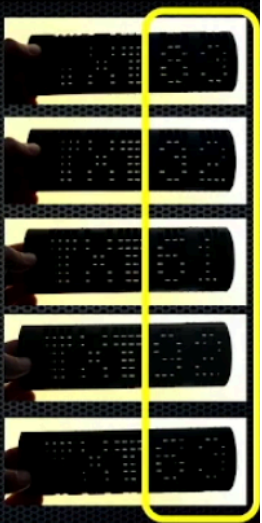
- STL file

Stage 2: WAND

Container is your wand, but hosts an STL

- Website points to DockerHub-hosted "wand" container, with script on the GitHub site to use it
- Wand shell script activates functions in the container, though the container has the payload needed for this stage
- `Shmoo.stl`, found after some directory crawling, has embedded "sun dial" stating TXT 83 32 61 **92 63** Also, "WAND" on a dial pad...

Real sundial project that we pilfered:
<https://www.thingiverse.com/thing:1068443>



- Load in blender
 - Rener light hitting it

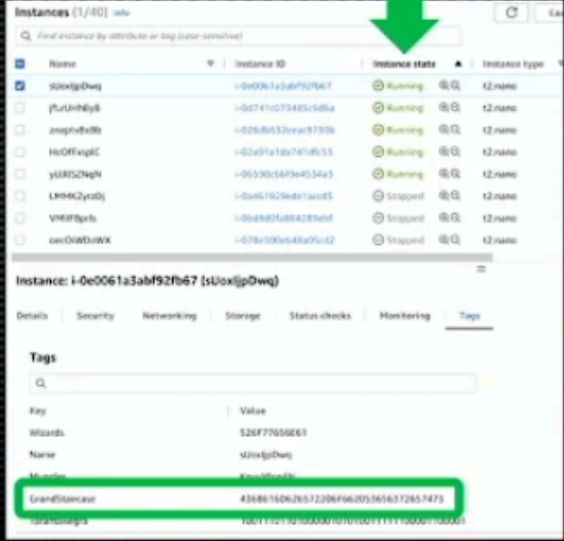
- AWS

Stage 3: CLOAK

Most unreliable AWS stack

ASCII characters emerge from each (ordered) state – on or off

- 8 AWS instances carefully starting and stopping over the course of 15 minutes
- Instances are managed by Lambdas, executed by CloudWatch every minute
 - 1 "all-on" state
 - 8 "ASCII" states: spelling `WANDSD01`
 - 1 "all-off" state
- GrandStaircase tag is used to order the instances, keyed by the book/movie names



Name	Instance ID	Instance state	Instance type
sUoxlpDwg	i-0e0061a3abf92fb67	Running	t2.nano
pUrLmHdy8	i-0e741c073485c68a	Running	t2.nano
zmprnfxDb	i-0268b652ac97306	Running	t2.nano
HeOFFagpC	i-02a9fa16d74f6c55	Running	t2.nano
yUxDSNqH	i-06390c14f9e4034e3	Running	t2.nano
LMHnC2yc0j	i-0a657029edf1aced5	Stopped	t2.nano
YH8FfpRb	i-0b48d9f884281e0f	Stopped	t2.nano
ceOWDvWK	i-078e100e648a0fcd2	Stopped	t2.nano

Key	Value
Wizards	526f770550e63
Name	sUoxlpDwg
InstanceId	i-0e0061a3abf92fb67
GrandStaircase	43686150d626572206f962059656372857473
GrandStaircase	10c1f102f121030301010100f11f1103061103061

- PCAP

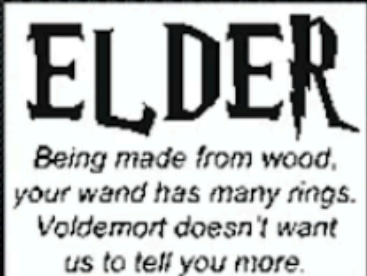
Stage 4: ELDER

RTP stream of Hedwig's Theme, with magical option data

No.	Time	Source	Destination	Protocol	Length	Info
2	0.011998	172.20.10.3	224.2.127.254	SAP/SDP	296	Announcement (v1)
3	0.011998	127.0.0.1	127.0.0.1	RTCP	88	Sender Report Source description
4	0.012998	127.0.0.1	127.0.0.1	MPEG TS	1364	PT=MPEG-II transport streams, SSRC=0xEA8028
5	0.014997	127.0.0.1	127.0.0.1	MPEG TS	1364	Audio Layer 3, 160 kb/s, 44.1 kHz (MP2T fra

- Music is streamed, but not hiding any information (this year)
- Inspecting the often-overlooked Overflow field in the IP header reveals a GIF, one nibble at a time

Pointer: 5
0011 = Overflow; 3



- <https://cantreally.cyou/posts/shmoogon-shmooganography/>

- DOCKER

Stage 5: RESURRECTION

Docker layering

- Take container received in Stage 2, unpacking it to reveal internal layers

```
docker pull $(IMAGE):$(PHASE1TAG)
mkdir validate
docker save -o validate/phase12-4A4B.mod.tar $(IMAGE):$(PHASE1TAG)
tar -xvf phase12-4A4B.mod.tar
```

Space after comma is 1, no space is 0.

```
ead5a1990f9bf86eadafcb463920", "sha256:6c72ac497917fc267b4cd9b1f7ec9003405fbc70e5f3bf33ac", "sha256:17ef1685390cb7943eedb67d753ab6c7492769b9706117885", "sha256:712a7a8763188b5bfb68e2db29978b4220bcc19bf60b3a59df", "sha256:ad65b013ecba06a381d0dd300e54eef22179495af6c40677e6c", "sha256:4d4d3b62c882944c06290fe5fc67388cf9960dede89d60711a9a", "
```

- HACK-A-SAT

- THOTCON

- crypto

- Find the flag in the text string: f33_qn_E0G
 - Hint: Rot & Decay
 - Apply ROT13
 - flag{s33_da_R0t}
- Find the flag hidden in this text. Think Bacon:
01100010010_01001310011101100_00001400010001100_0101000101010111
 - Its binary but in a weird format
 - flag{n0t_k3v1n_b4c0n_l0lz}
- In the hands of an allied spy, you've found a small piece of paper with a strange sequence of characters: 'RmxhZ3tiYXNINjRfaXNfZWfZeX0='. What could it mean?
 - Base 64 encoding (give away is the "=")
 - base64_is_easy
- Ykj pynih fgl iak weru tlmt utut hor dp oyu ytd? Smisu nn ia eeco ayhc sr heme. ftuo{so1o_t0_so_n0k}
 - -
- Ftue ue FTAFOAZ 0jO agd fiqxrft kqmd. lq tabq kag tmhq mz mymluzs fuyq mzp qzvax xqmdzuzs eayqftuzs zqi. Rxms{d0f12_ue_ea_qmek}
 - ROT [A-Z]+12
 - This is THOTCON 0xC our twelfth year. We hope you have an amazing time and enjoy learning something new. Flag{r0t12_is_so_easy}
- Ace of Base
TGVzcyBjcnlwdG8sIG1vcmUgZW5jb2RpbmcuIGZsYWd7MV9zYXdfdGgzX3MxZ259==
 - Base 64 encoding (give away is the "=")
 - Less crypto, more encoding. Flag{1_saw_th3_s1gn}
- Cracking the Code A cryptic message, "nzdpmphz", has found its way to you. The circumstances surrounding the receipt of this message suggest that it holds an important secret, but it appears to be encrypted. Your task is to decrypt this mystery text, which will serve as the flag.
 - Caesar cipher with a shift of 1 to the right
 - mcology

- RF

- Find the Signal
 - Search for radio peak that is transmitting. This one was transmitting on 99.1
 - Morse code can be heard. Translate the morse code

- m0rs3c0d3

- Badge

- esptool can be installed with `pip install esptool`
- Dump memory
 - command to dump all 4MB of flash to a file: `python -m esptool --port COM5 -b 115200 read_flash 0 0x400000 flashdump.bin`
- found badge flags as strings: `flag{welcome_to_the_8bit_world}` and `flag{lets_fight!}`
- To view strings use in terminal command `*strings*` with your .bin file `strings flashdump.bin`

- BATTELLE CYBER CHALLENGES

<https://solvers.battelle.org/cyber-challenge/cyber-challenge>

- REVERSE ENGINEERING

- Keepin' It Real:
 - Our engineers have managed to recover an old control system, but they can't figure out how to get the thing to work! Device documentation says that it shipped with some kind of client software that is no longer available. Luckily, they were able to recover the system firmware image...
 -
- What the... Frob?:
 - What the... Frob?
 -
- Humpty Dumpty's Fall:
 - Humpty Dumpty sat on a wall.... you know the rest. Can you figure out how the kings men and horses botched the repair on poor humpty?
 -
- The Legend of the Headless Horseman:
 - A mysterious figure has been terrorizing the village of Sleepy Hollow. He rides a massive horse, swings a might scythe and has been collecting heads from any who draw near. A group of locals, Ichabod Crane, Katrina Van Tassel and Abraham "Brom Bones" Van Brunt have been working to discover the secret behind this mysterious menace, but just as they were on the verge of putting the pieces together, the Headless Horseman struck!
 -
- Feed the Magical Goat:
 - Once upon a time, there was a little reverse engineer who found a special bell. When the bell was struck, they say a magical billy goat appeared looking for food. Everyone knows billy goats will

eat anything, but this is all the little reverse engineer had lying around.

•

○ BINARY EXPLOITATION

■ Holy Grail of ROP:

- The ROP God has tasked King Arthur with finding the function called "holy_grail". You must aid him on his quest! But be warned, the way is guarded by a text-based sorcerer whom loves old British comedy movies, and just to make things harder, you're going to have to find "holy_grail" 3 times! ...Or was it 5 times? Use your pwning knowledge to answer the sorcerer's questions and ROP your way to the holy grail and bring this holy relic home for the glory of England!

•

■ Ghosted:

- You're trying to save some money on your flight home so you've decided to fly Ghost Airlines, unfortunately their chatbot AI is being very unhelpful and is totally ignoring you! Can you figure out a way around the ghosting and hack your way home?

•

○ FORENSICS / CRYPTO

■ The Thanksgiving Bandits:

- Last year, the notorious Thanksgiving Bandits struck for the third time. They stole over 1,000 potatoes that were meant to be mashed for the annual Thanksgiving Day feast. Two years ago, they burgled 400 pounds of cranberries, and they took 104 pumpkin pies the year before that. No one knows how they pull off such masterful heists or what they do with their score, but everyone agrees that they must be stopped at all costs.

•

■ Dragons and Dwarves:

- A wise dragon decided that dwarves were too easily stealing his treasure while he slept. To thwart these villains he has placed his prized possessions inside a magic portal that transmutes the valuables into worthless junk unless one knew the magic pass phrase.

•

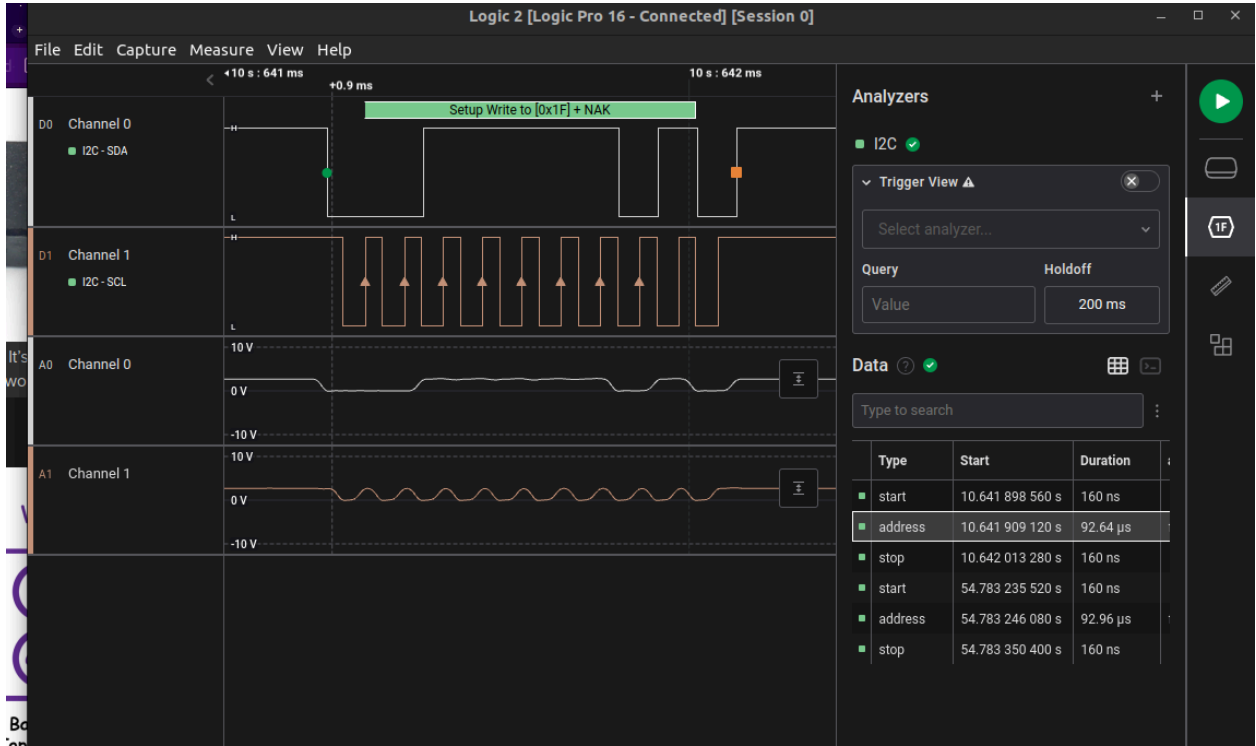
○ MULTI-ARCHITECTURE SHELLCODE

■ Unicorns Undercover:

- You arrive at the meeting location. It's dark The handoff is scheduled to take place at 10 p.m. The unicorns arrive, but you don't see the flag. They approach you and the first one says, "push eax, call joke." The second says, "jalr blankstare." They

stare at each other. They stare at you. They aren't speaking the same language.

Logic analyzer



	name	type	start_time	duration	ack	address	read	data
I2C	start		5.78338656	1.60000001e-07				
I2C	address		5.78339712	0.00012096	true	0x1F	false	
I2C	data		5.78352432	0.00010976	true			0x42
I2C	data		5.78364016	0.00010992	true			0x44
I2C	data		5.78375616	0.00010976	true			0x47
I2C	data		5.783872	0.00010976	true			0x49
I2C	data		5.783988	0.00010976	true			0x49
I2C	data		5.78410384	0.00011088	true			0x4D
I2C	data		5.7842208	0.00010976	true			0x4F
I2C	data		5.7843368	0.00010976	true			0x3F
I2C	stop		5.78445792	1.6e-07				
I2C	start		5.79451088	1.6e-07				
I2C	address		5.79452144	0.00012128	true	0x1F	true	
I2C	data		5.79471984	9.568e-05	true			0x4B
I2C	data		5.79488128	9.456e-05	true			0x4B
I2C	data		5.79504176	9.232e-05	true			0x55
I2C	data		5.79519984	9.248e-05	true			0x78
I2C	data		5.79535824	9.44e-05	true			0x36
I2C	data		5.79551888	9.2e-05	true			0x76
I2C	data		5.79567728	9.392e-05	true			0x73
I2C	data		5.7958384	9.152e-05	false			0x30

I2C	stop	5.79600112	1.6e-07
I2C	start	15.2575363	1.60000001e-07
I2C	stop	15.2575906	1.6e-07
I2C	start	15.2589378	1.59999998e-07
I2C	stop	15.2707021	1.60000001e-07
I2C	start	15.2720619	1.6e-07
I2C	stop	15.2733035	1.59999998e-07
I2C	start	15.2734474	1.6e-07
I2C	stop	15.2751781	1.60000001e-07

- Car hacking village 2024

- R

- K:

- Ou