



Explosive Cases in ICS

and
How to Prevent Them

Disclaimer

- It's all for learning and sharing the experience
- Guide through safely security assessment
- All events portrayed next are purely fictional
- **No facilites were harmed**



whoami



@S74RZ

- PT/SA more than 10 years
- Leading international team
- Masters of None:
 - Pentest
 - RE
 - AppSec
 - ICS
 - Network
 - Radio
 - HW
 - ...

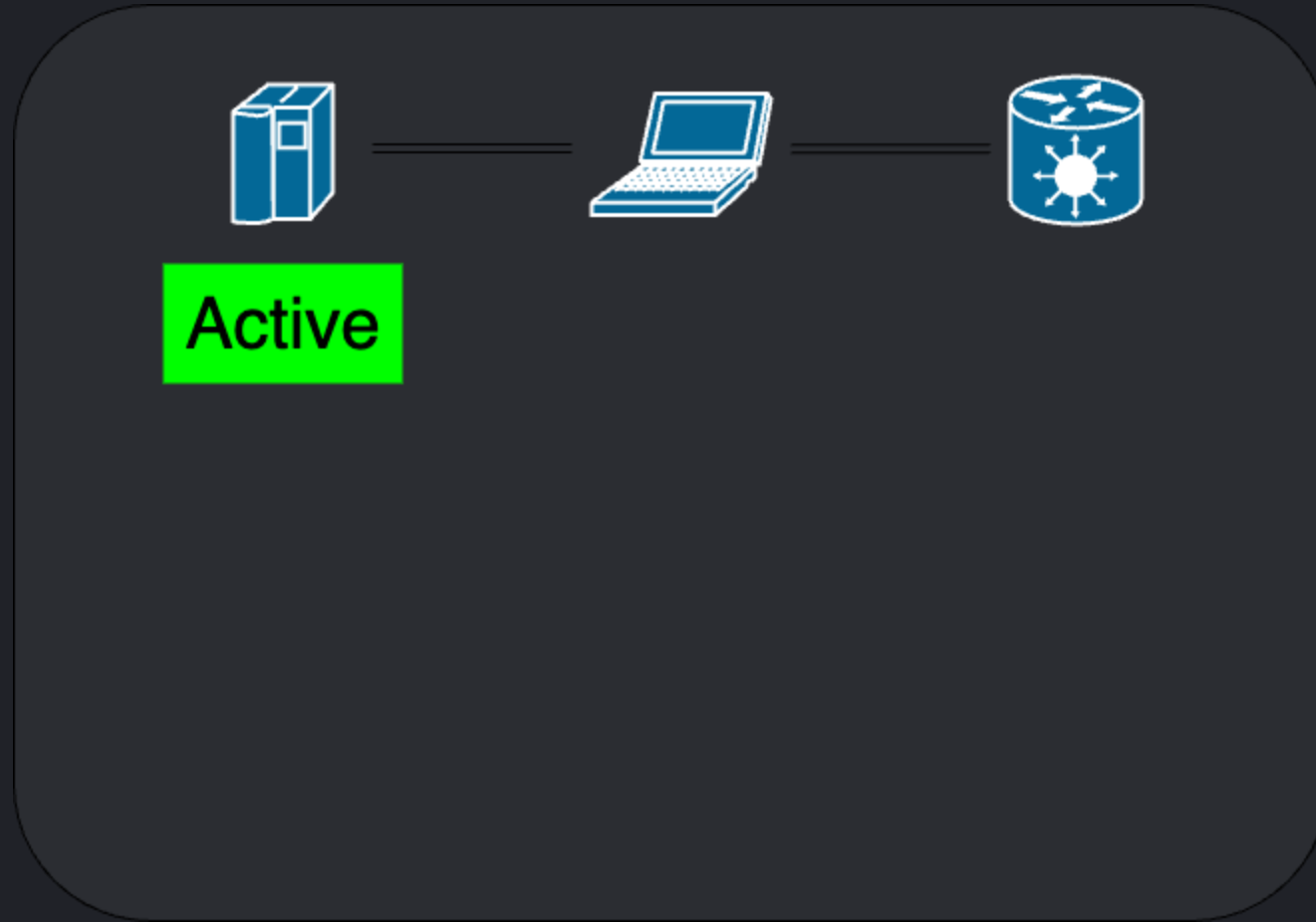
whoisHR



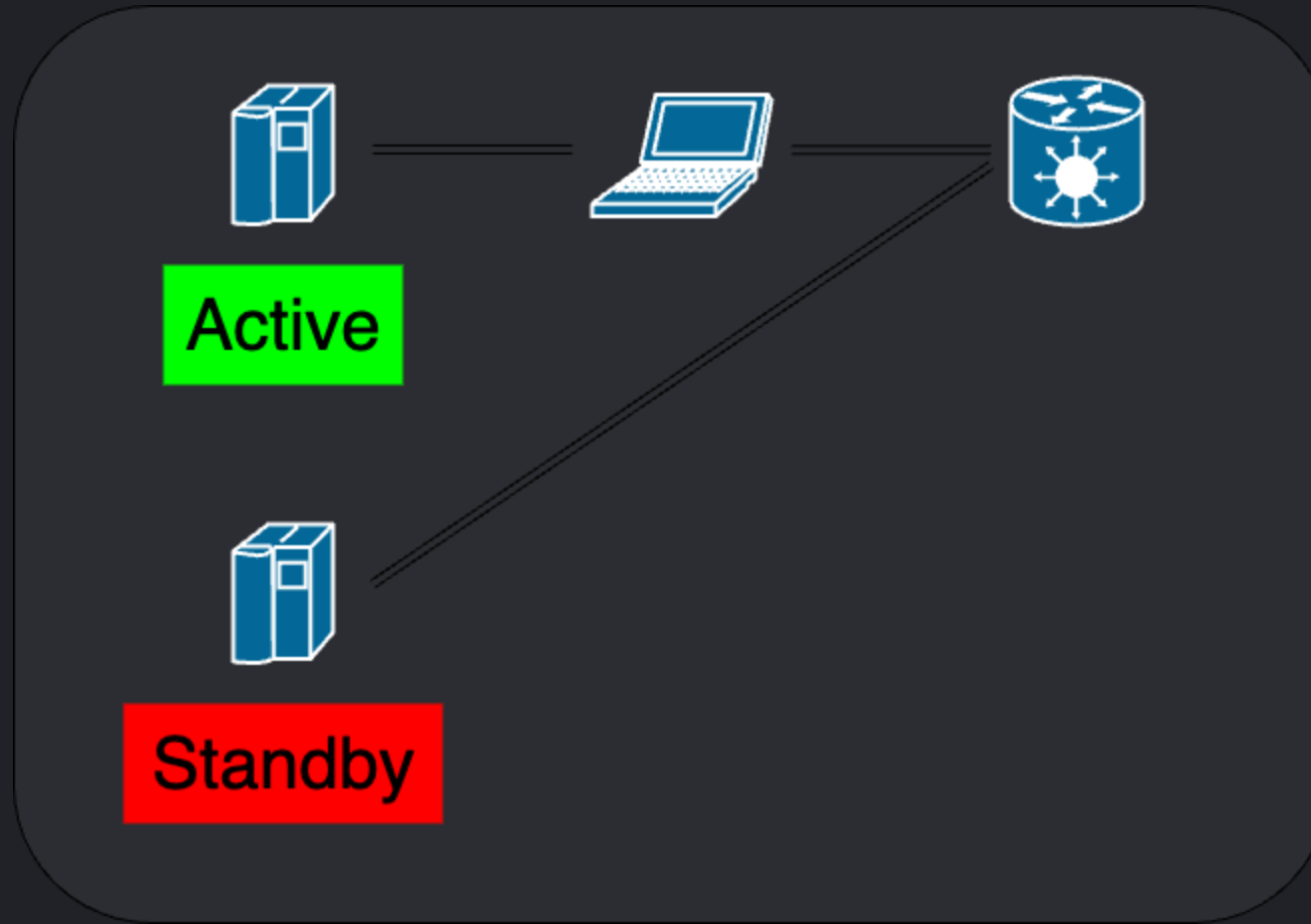
- PT/SA more than 10 years
- Leading international team
- Masters of None:
 - Pentest
 - RE
 - AppSec
 - ICS
 - Network
 - Radio
 - HW
 - ...

Case Study #0 - Personal

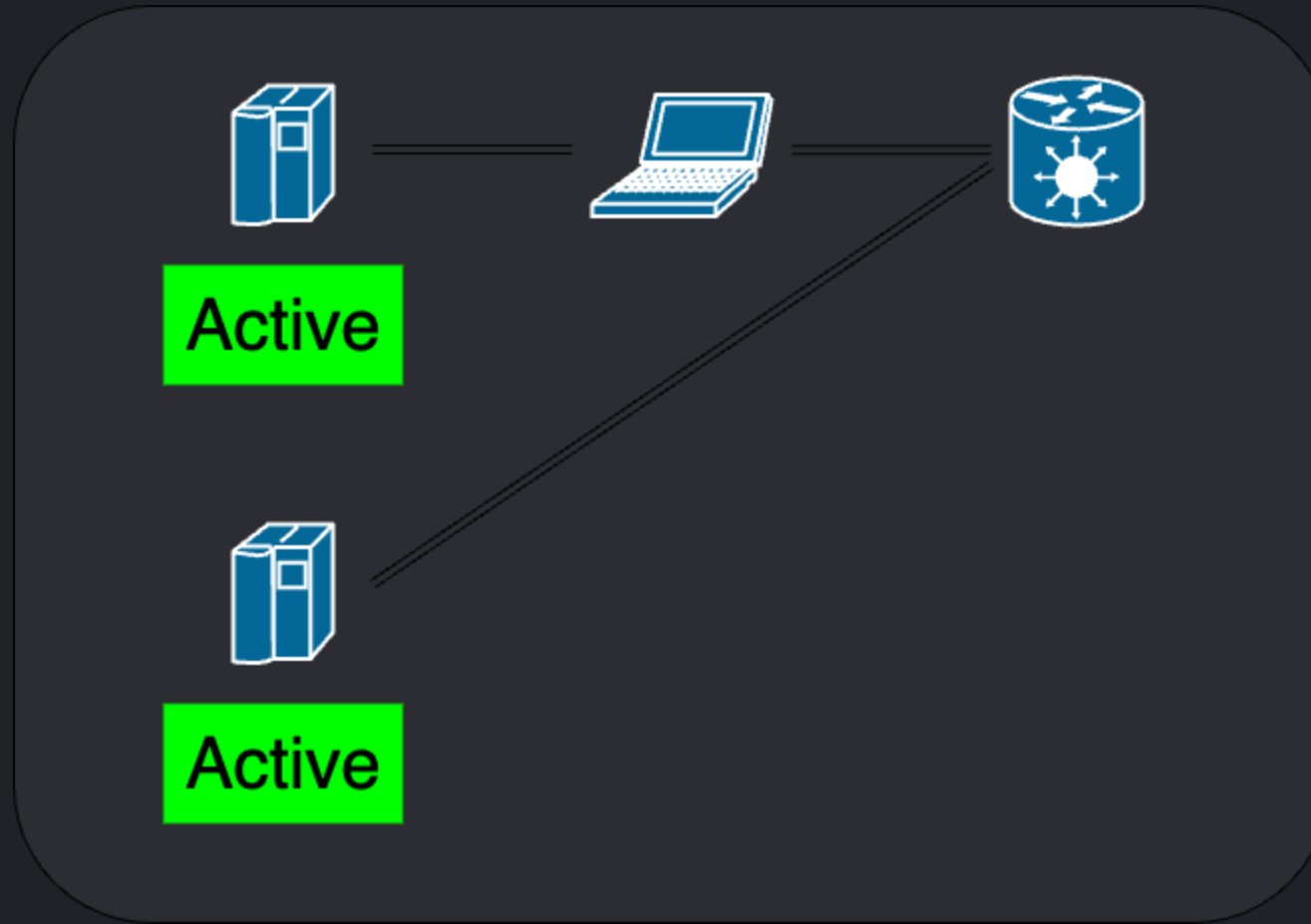
Case Study #0 - Personal



Case Study #0 - Personal



Case Study #0 - Personal



Ruleset #0

- Know your enviroment before executing any attacks
- In most cases network attack is a bad idea



History Time

1st Industrial Revolution



1760-1870

1st Industrial Revolution



New Law:

- Children can no longer work in factories
- Children can no longer work full time



1760-1870

2nd Industrial Revolution

1870-1947



2nd Industrial Revolution



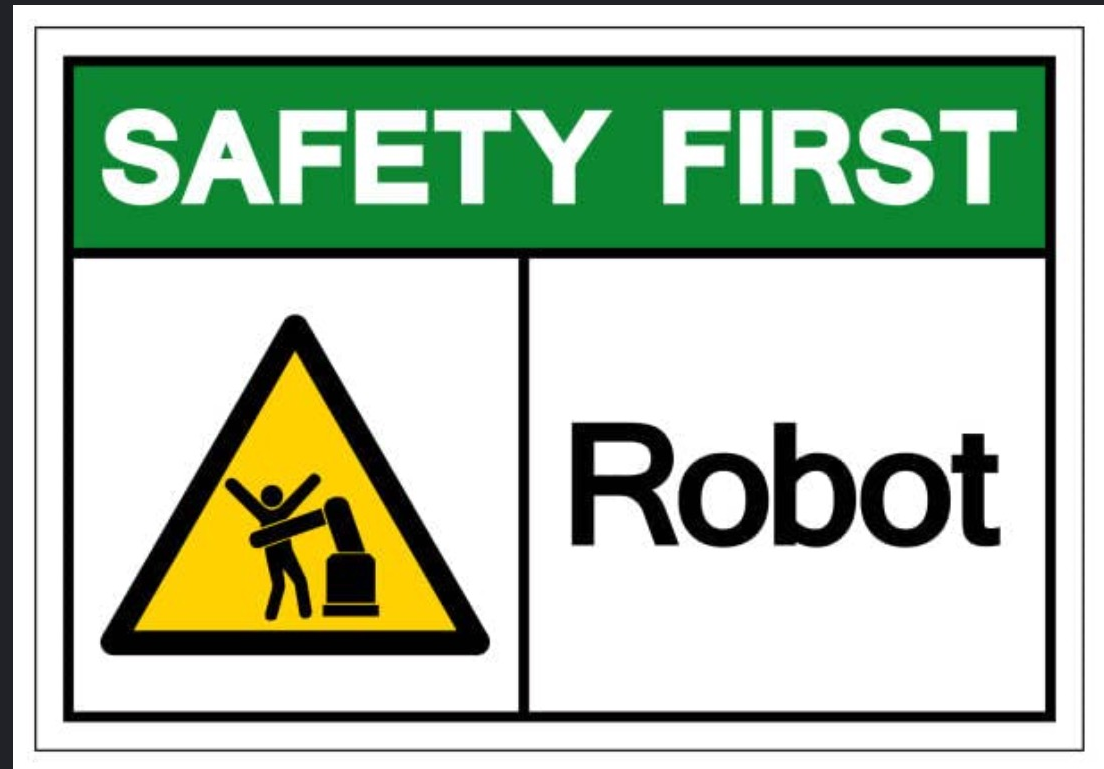
1870-1947

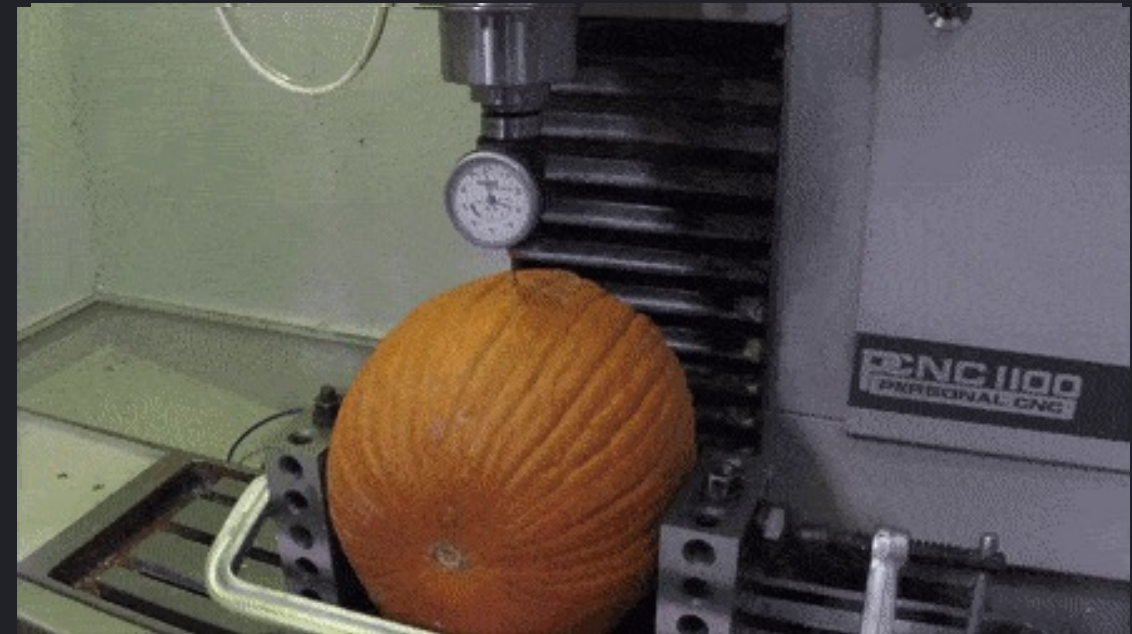


3rd Industrial Revolution



3rd Industrial Revolution





CNC/Robot fails compilations





Safety



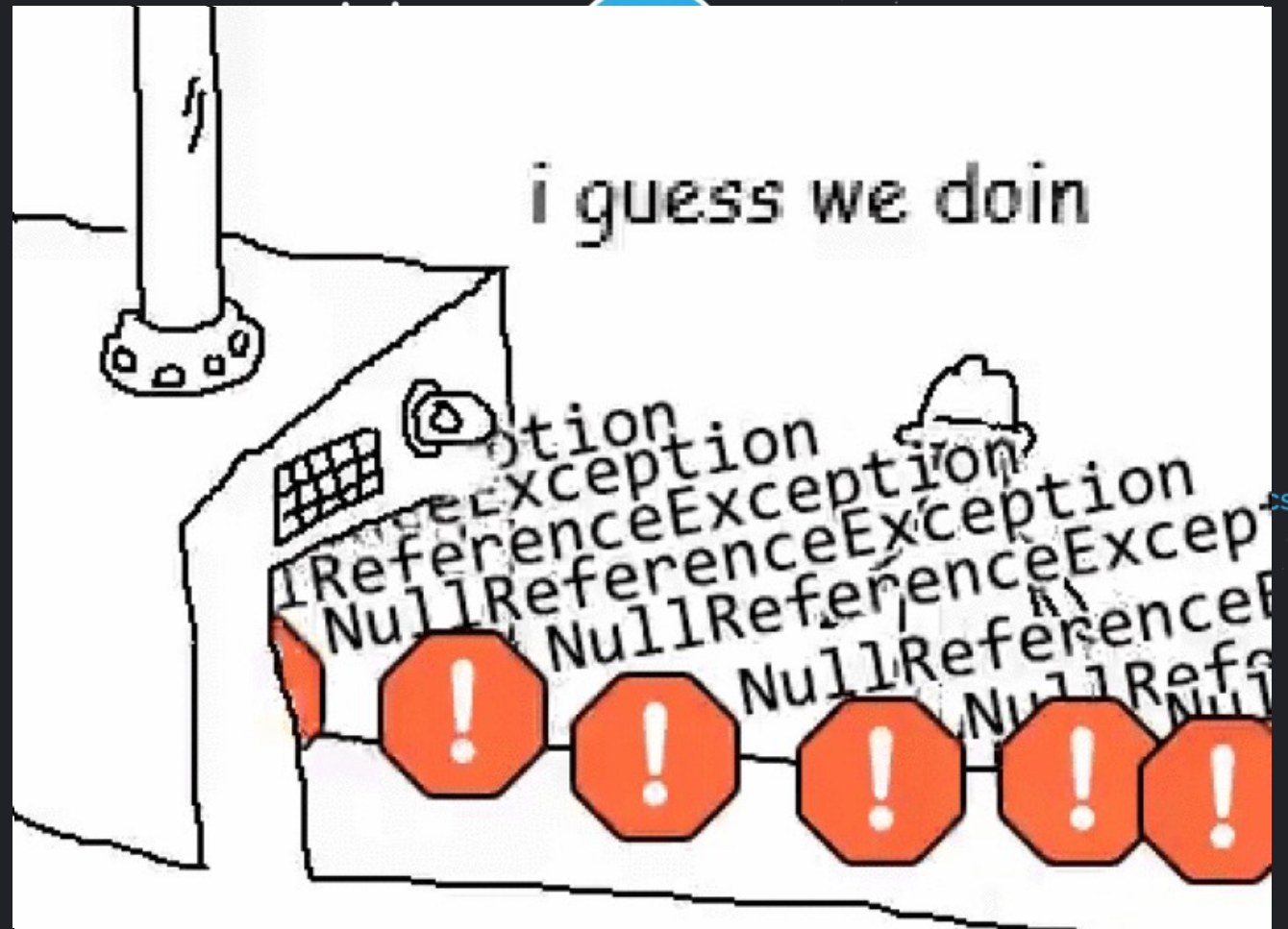
Security



Intelligence



Human-machine interaction



Case study #1 - ICS Services

"I've seen things you people wouldn't believe. Gopher, Netscape with frames, the first Browser Wars. Searching for pages with AltaVista, pop-up windows self-replicating, trying to uninstall RealPlayer. All those moments will be lost in time, like tears in rain. Time to die."



Case study #1 - ICS Services

"I've seen things you people wouldn't believe. Gopher, Netscape with frames, the first Browser Wars. Searching for pages with AltaVista, pop-up windows self-replicating, trying to uninstall RealPlayer. All those moments will be lost in time, like tears in rain. Time to die."



Case study #1 - ICS Services

"I've seen things you people wouldn't believe. Gopher, Netscape with frames, the first Browser Wars. Searching for pages with AltaVista, pop-up windows self-replicating, trying to uninstall RealPlayer. All those moments will be lost in time, like tears in rain. Time to die."



```
import socket
socked_fd = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
socked_fd.connect(('192.168.1.128', 5555))
socked_fd.send(b'\x41')
```

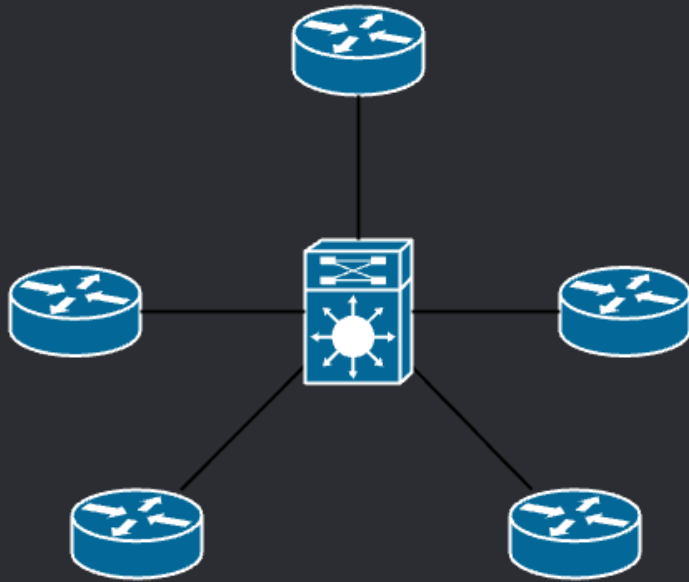
SCANNING

Ruleset #1

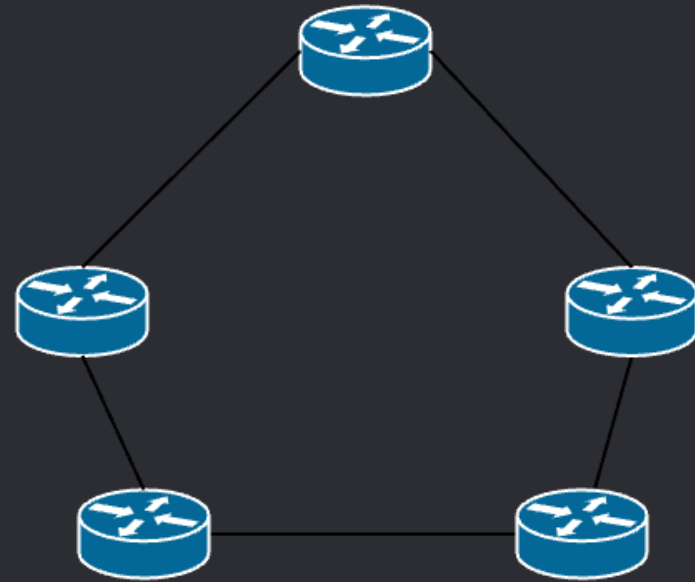
- All actions on a testbed first
- ARP/ICMP scan after
- TCP connect scan is always better than SYN scan
- Blind scan for only known ports (ssh, smb, rdp etc.)
- Don't even think about -sV

Case study #2.1 - Networks

Case study #2.1 - Networks

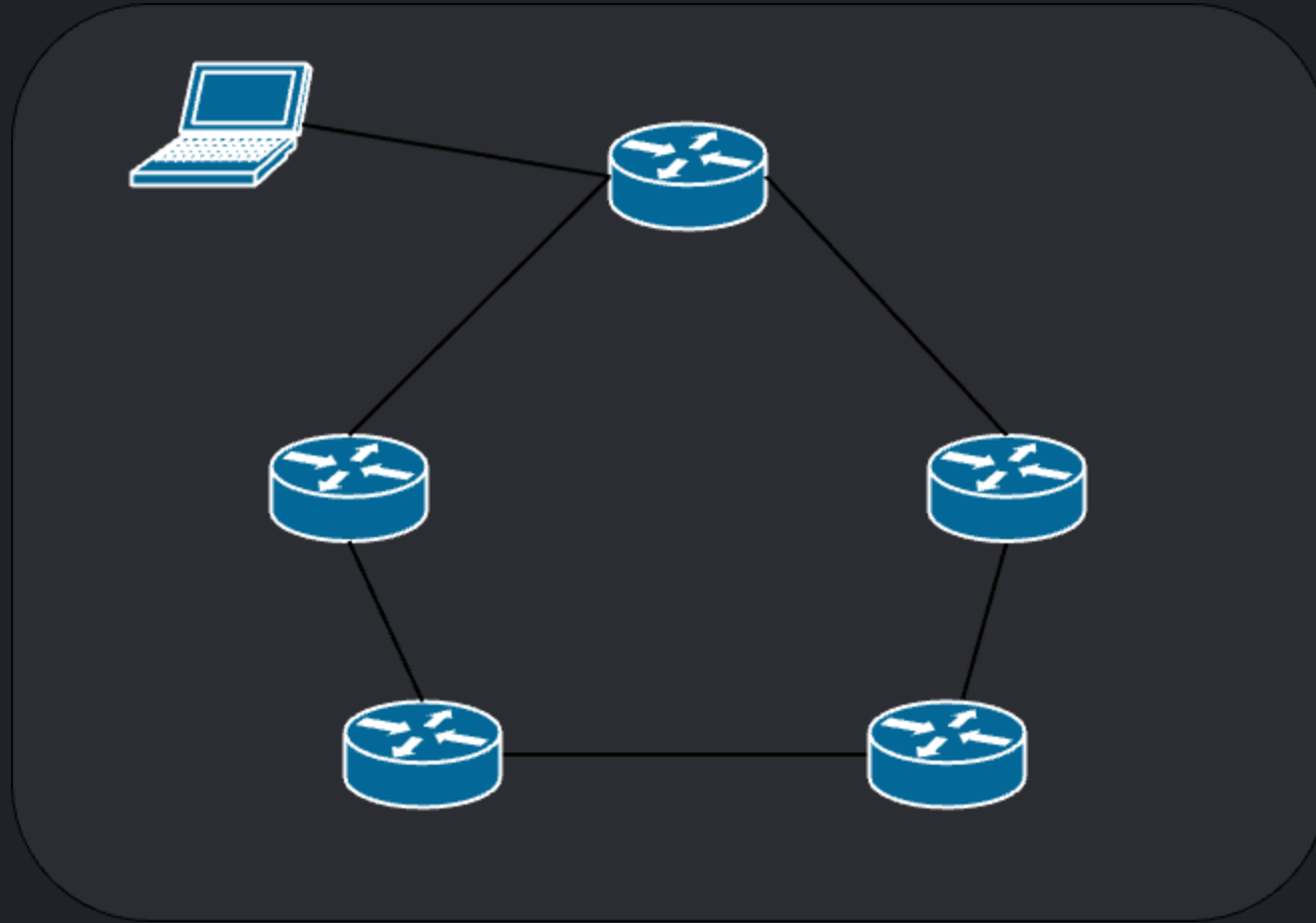


Star topology

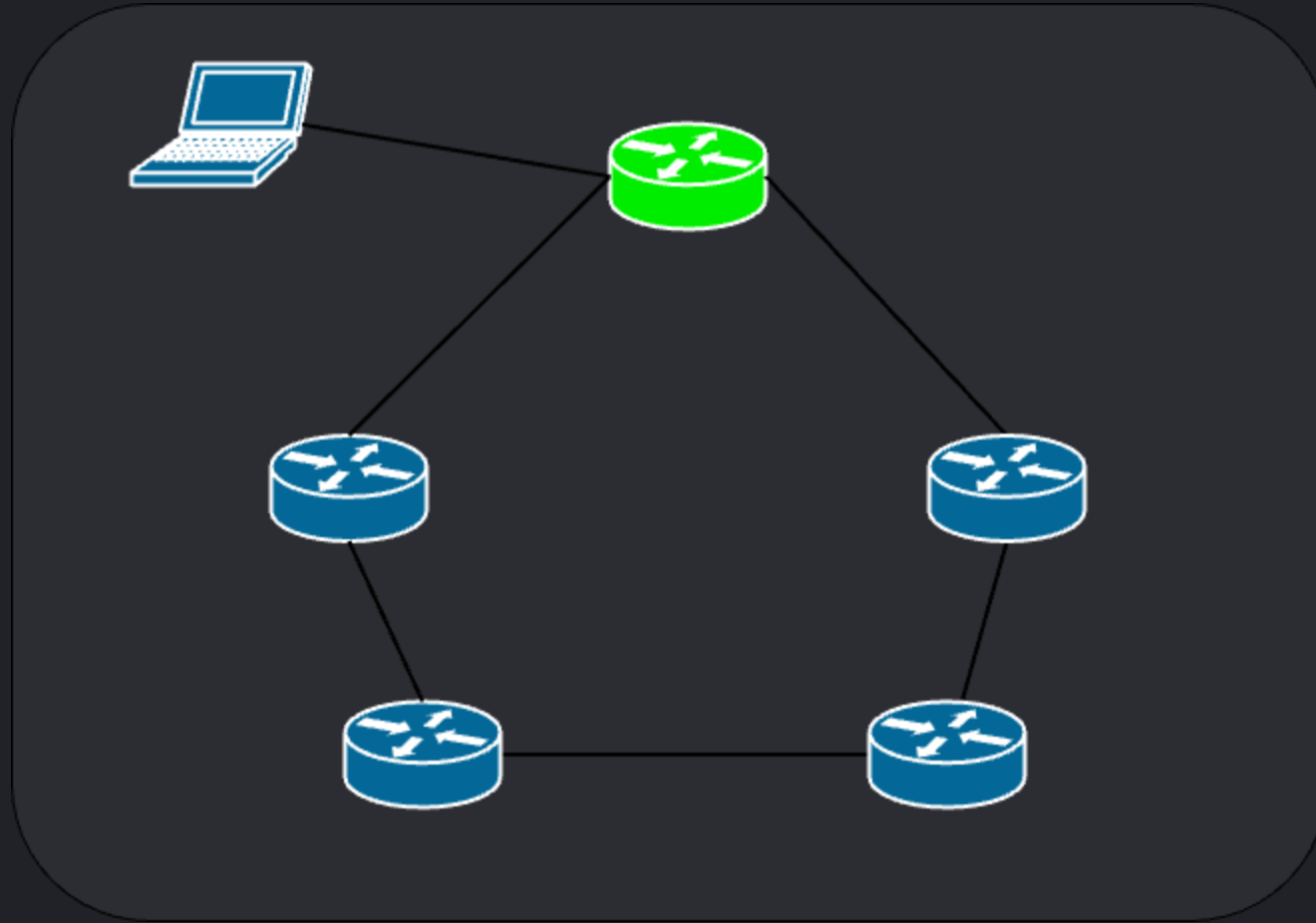


Ring topology

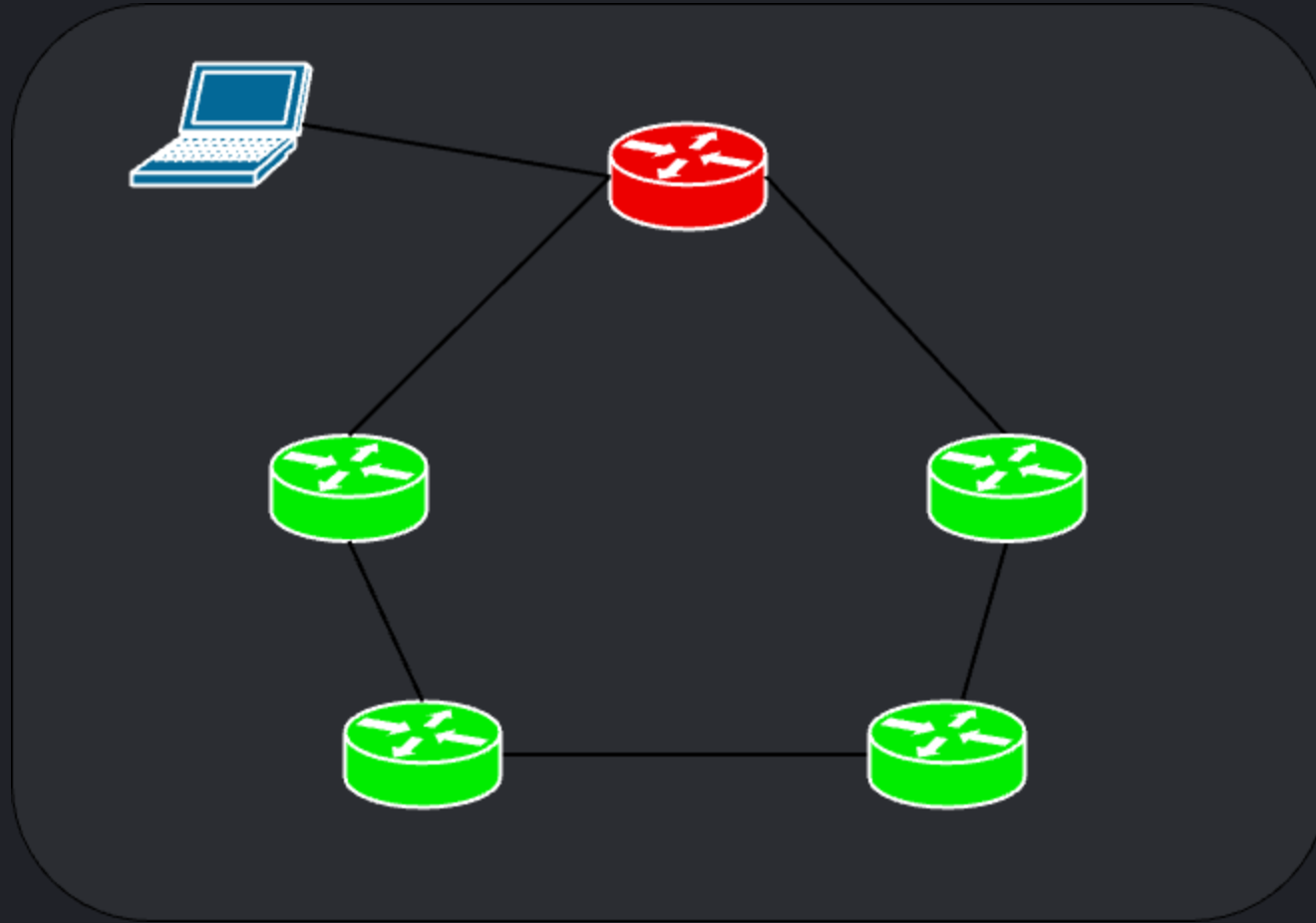
Case study #2.1 - Networks



Case study #2.1 - Networks



Case study #2.1 - Networks



Case study #2.2 - Networks

```
20 packets transmitted, 0 packets received, 100.0% packet loss
ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254): 56 data bytes
ping: sendto: No route to host
ping: sendto: No route to host
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
64 bytes from 192.168.2.254: icmp_seq=2 ttl=128 time=0.608 ms
64 bytes from 192.168.2.254: icmp_seq=3 ttl=128 time=0.431 ms
64 bytes from 192.168.2.254: icmp_seq=4 ttl=128 time=0.608 ms
64 bytes from 192.168.2.254: icmp_seq=5 ttl=128 time=0.773 ms
```

Case study #2.2 - Networks



Case study #2.2 - Networks



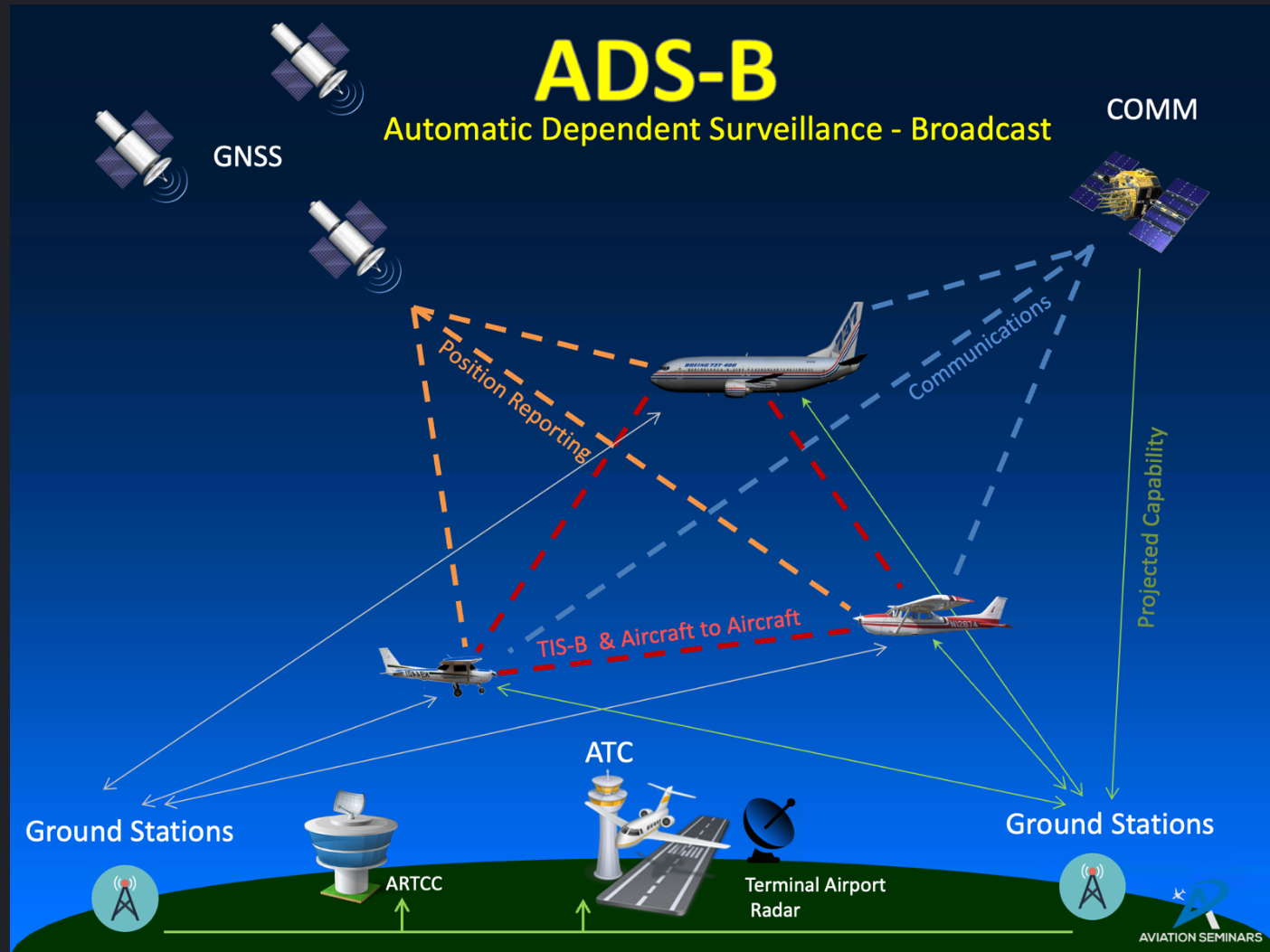
Otherwise...

Ruleset #2

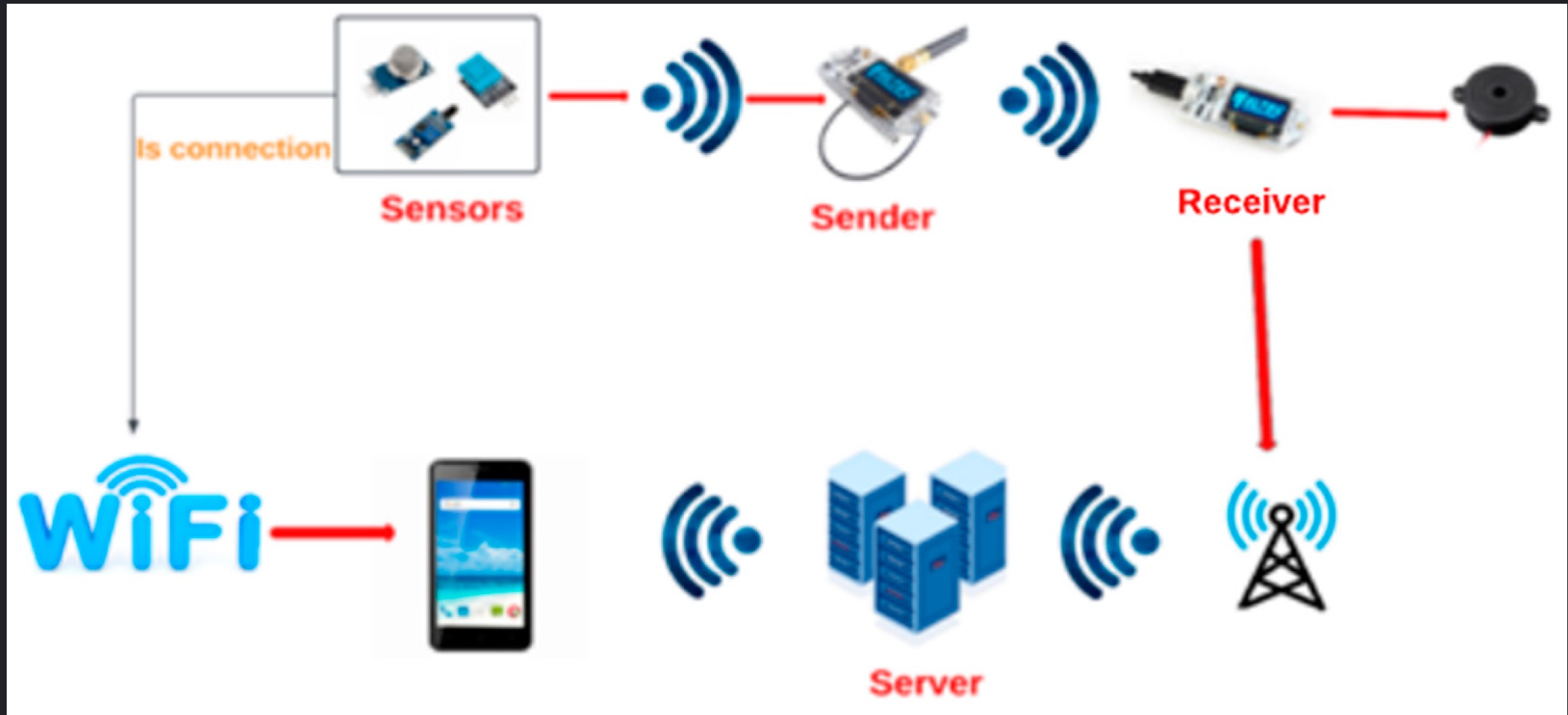
- Make sure it really works before anything
- Collect all network information first
- Do u remember that network attacks is a bad idea?

Case study #3 - Radio

Case study #3 - Radio



Case study #3 - Radio



Case study #3 - Radio



Case study #3 - Radio



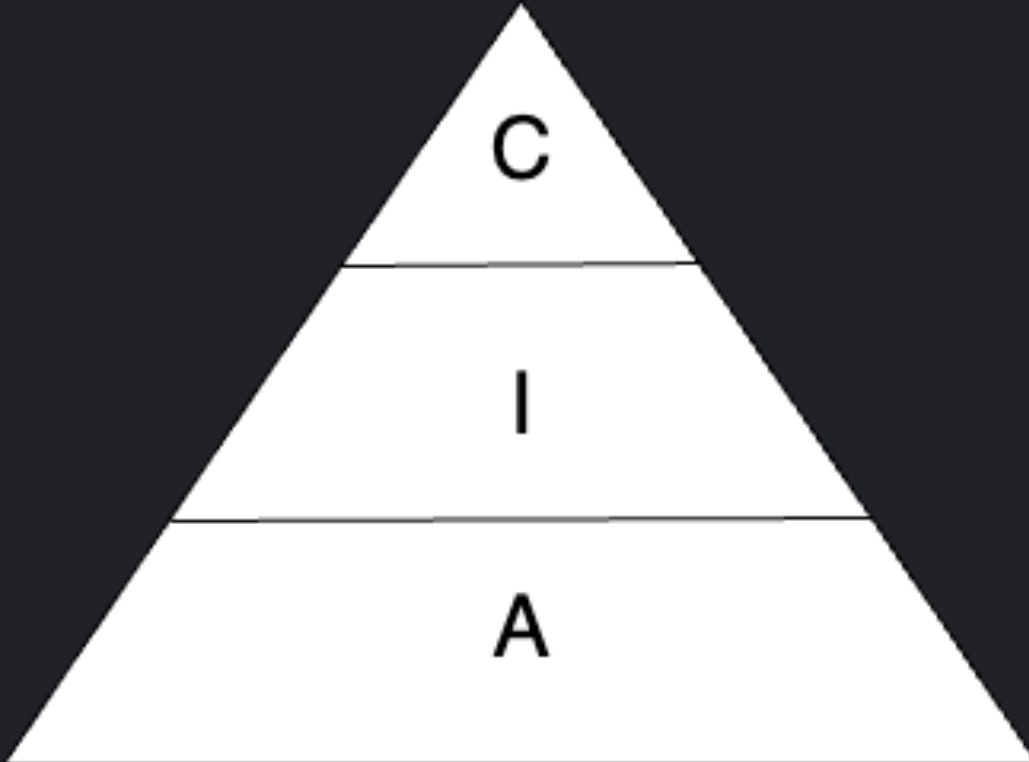
Ruleset #3

- Always remember you are not alone there
- Radio may be more unpredictable than networks
- Make all tests with radio in the isolated area

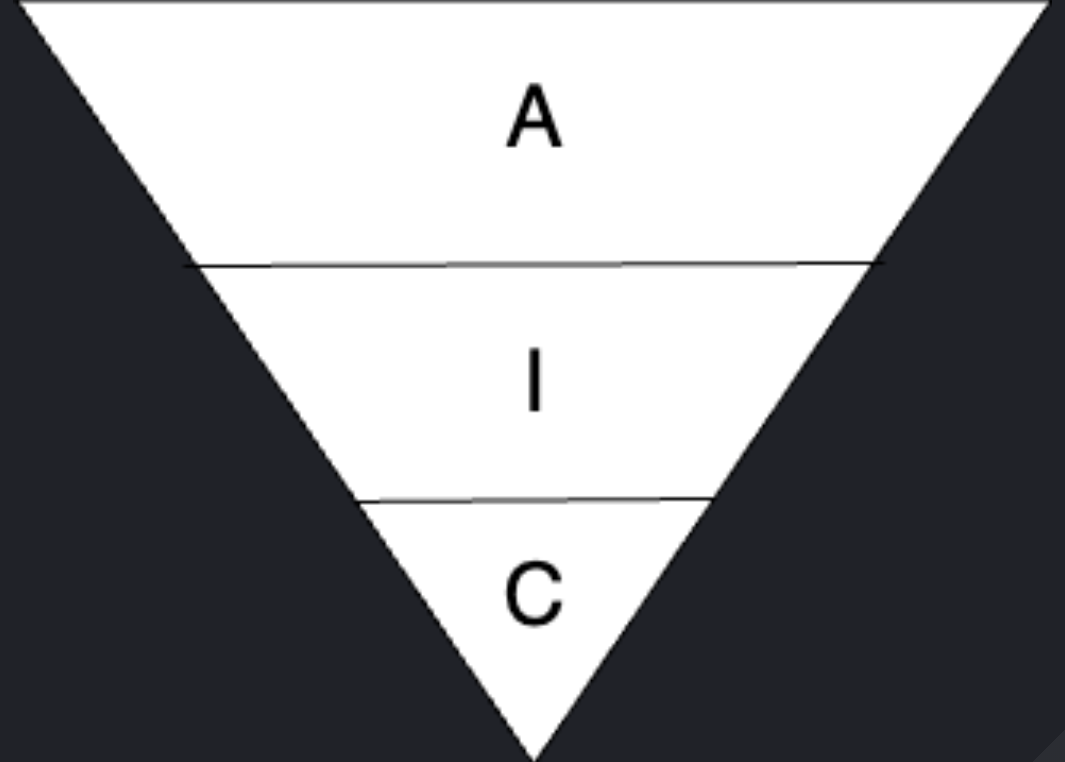


CIA

- **Corporate**



- **ICS**



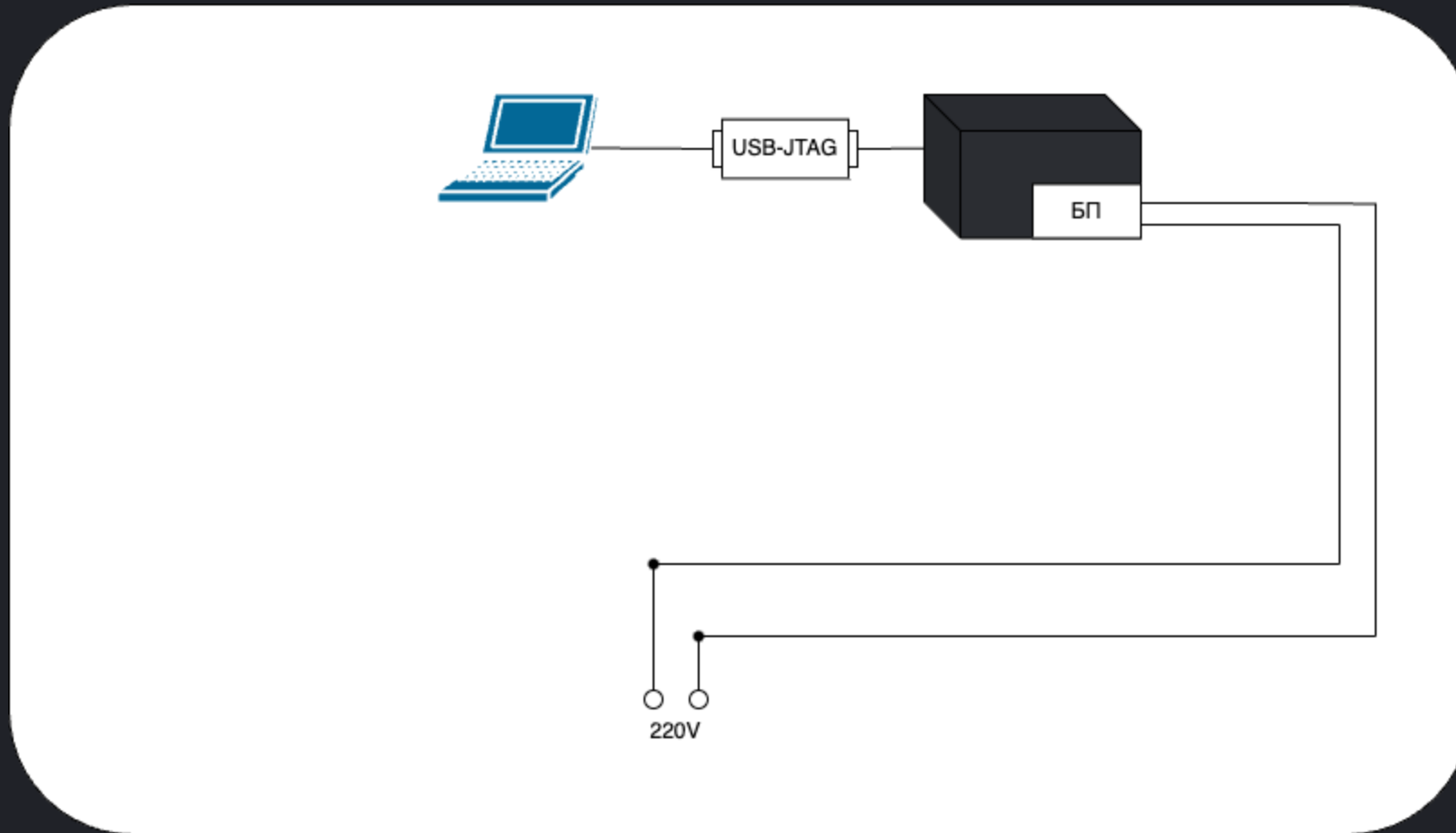
Case study #4 - HW



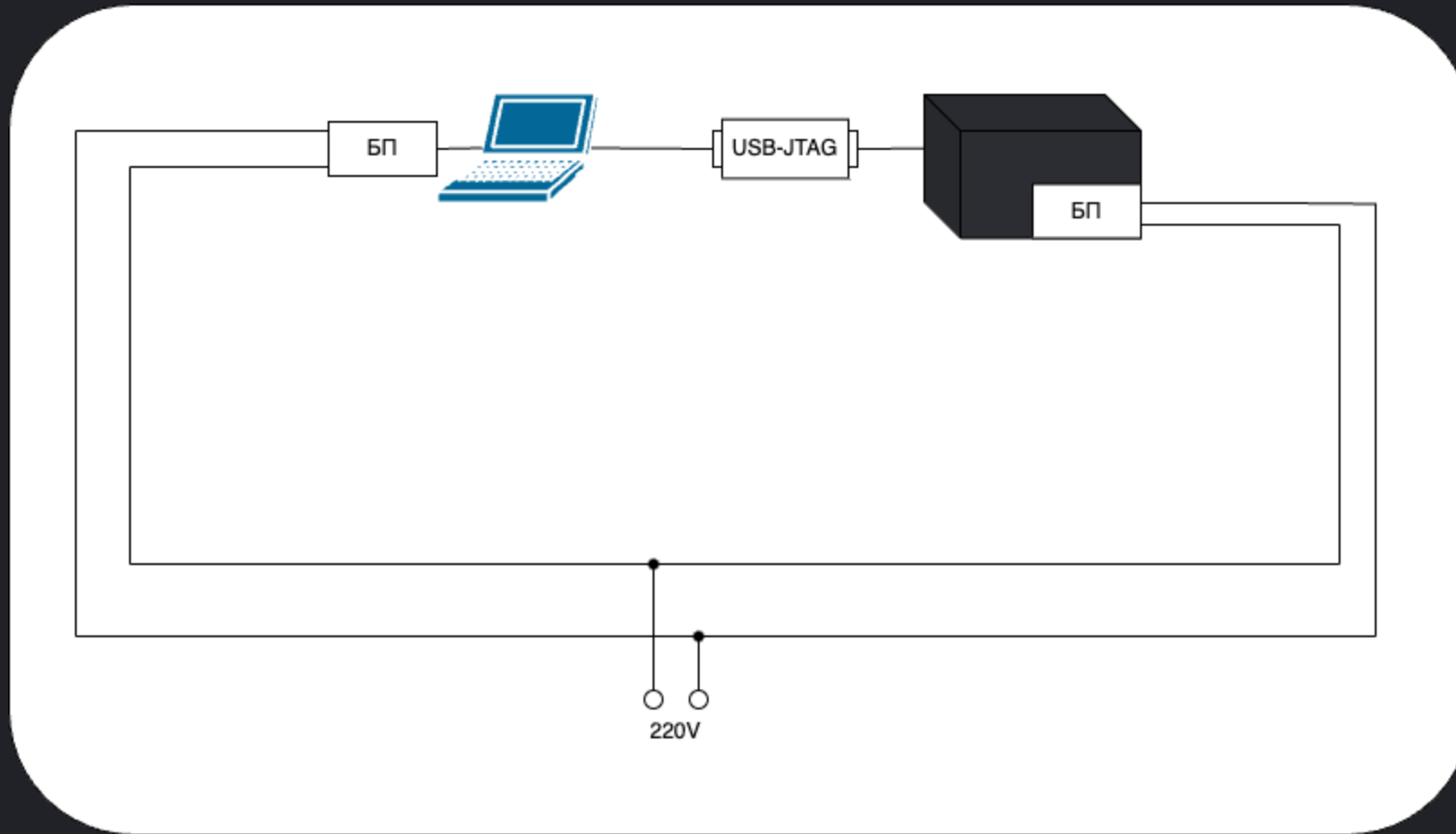
Case study #4 - HW



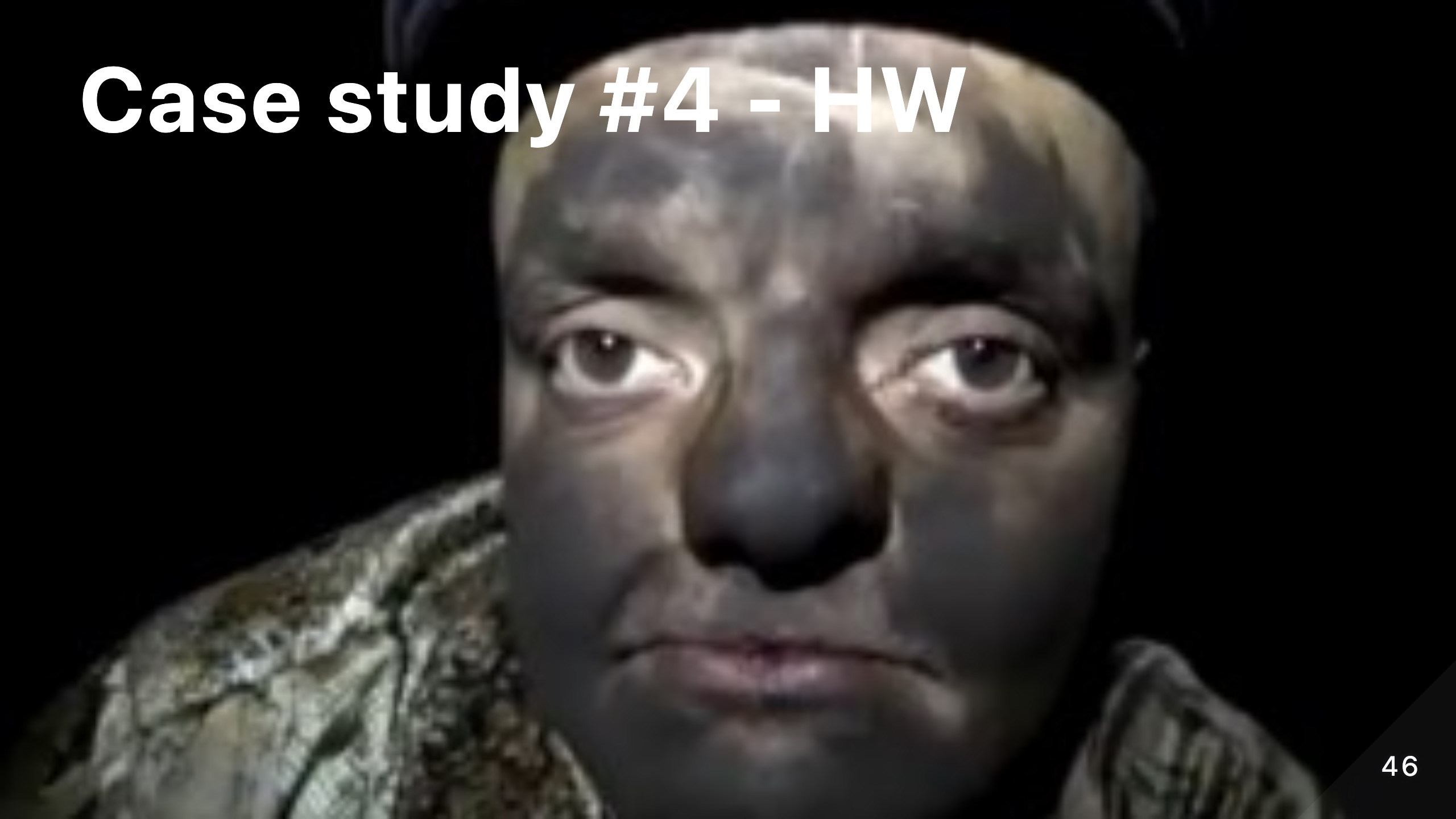
Case study #4 - HW



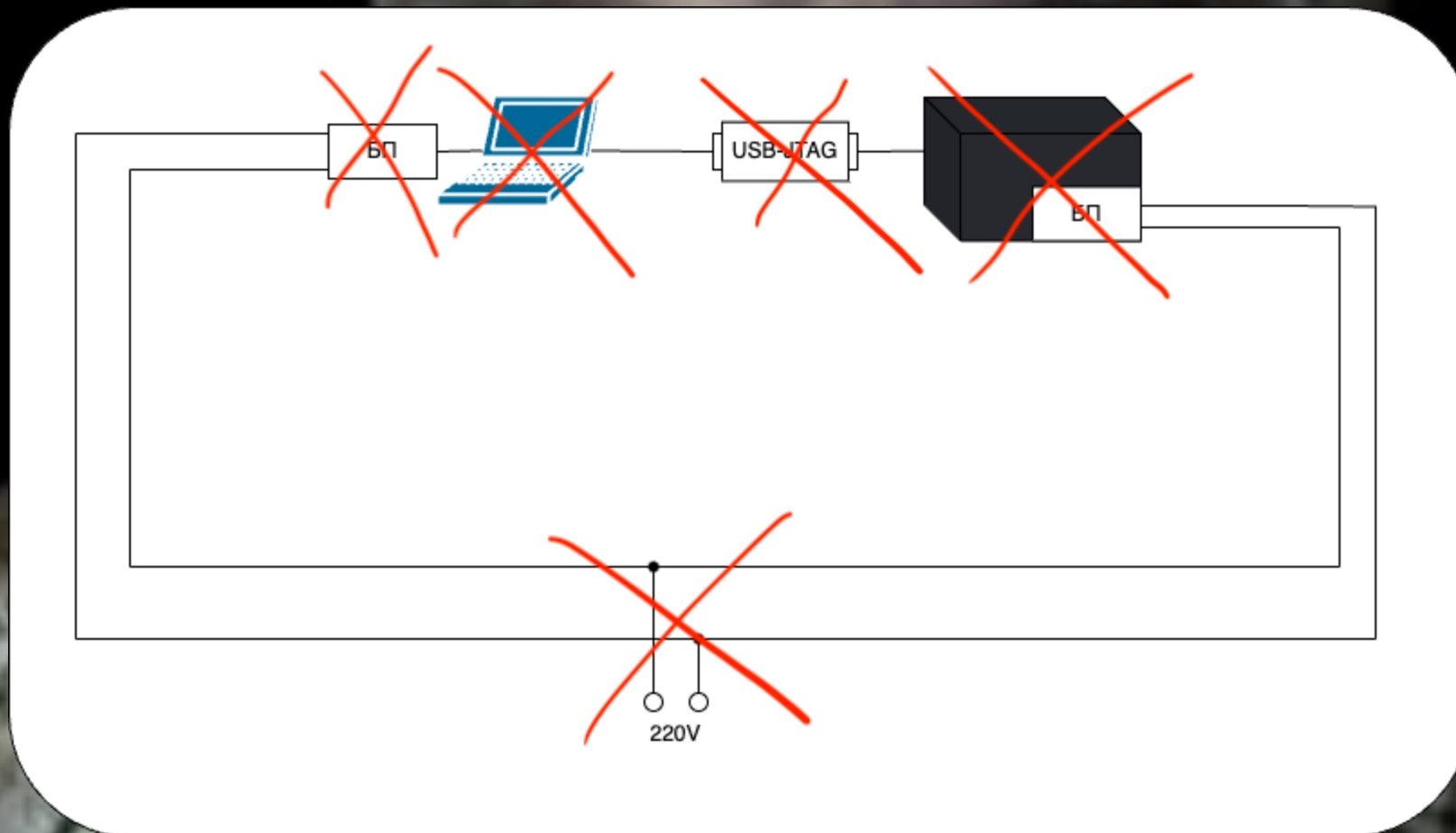
Case study #4 - HW



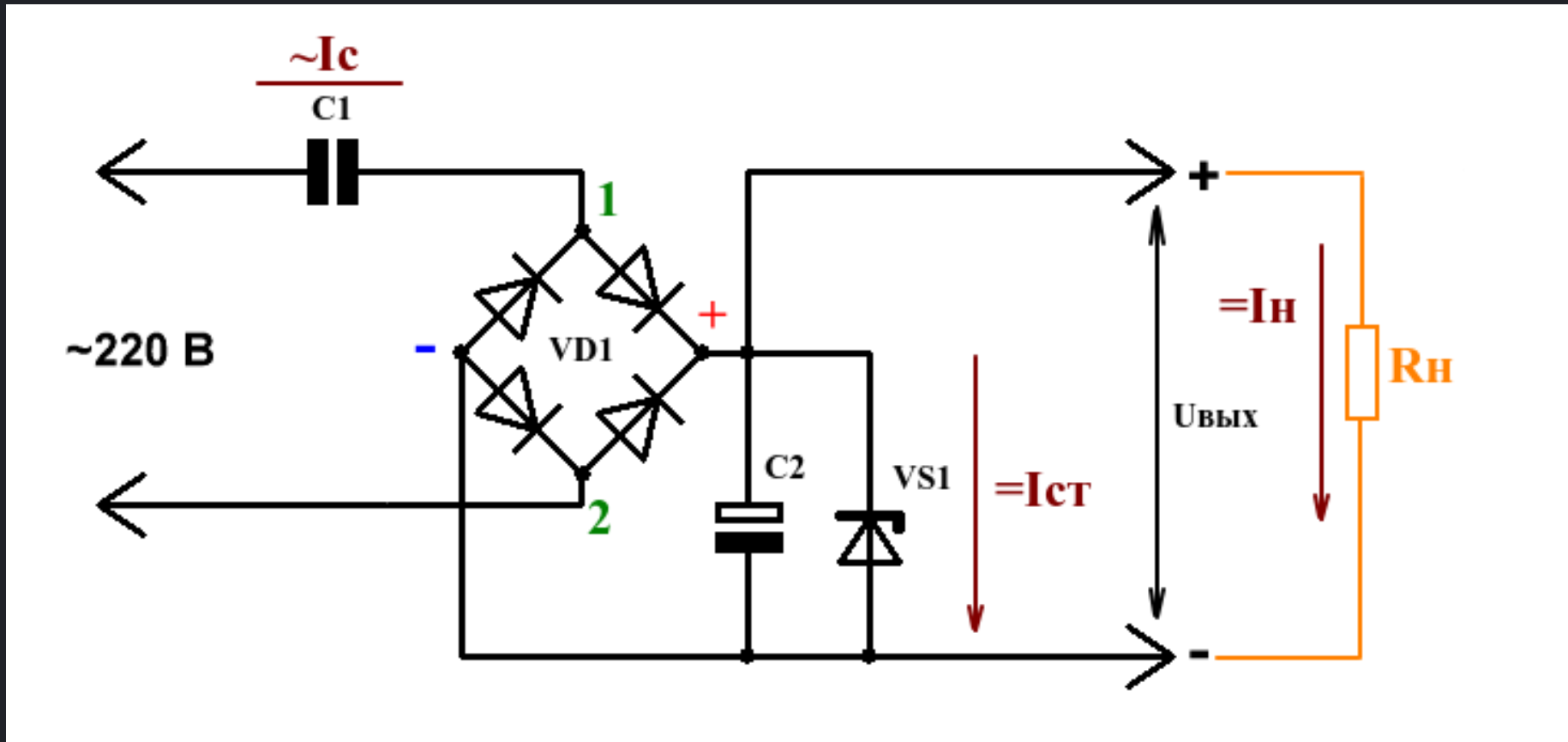
Case study #4 - HW



Case study #4 - HW

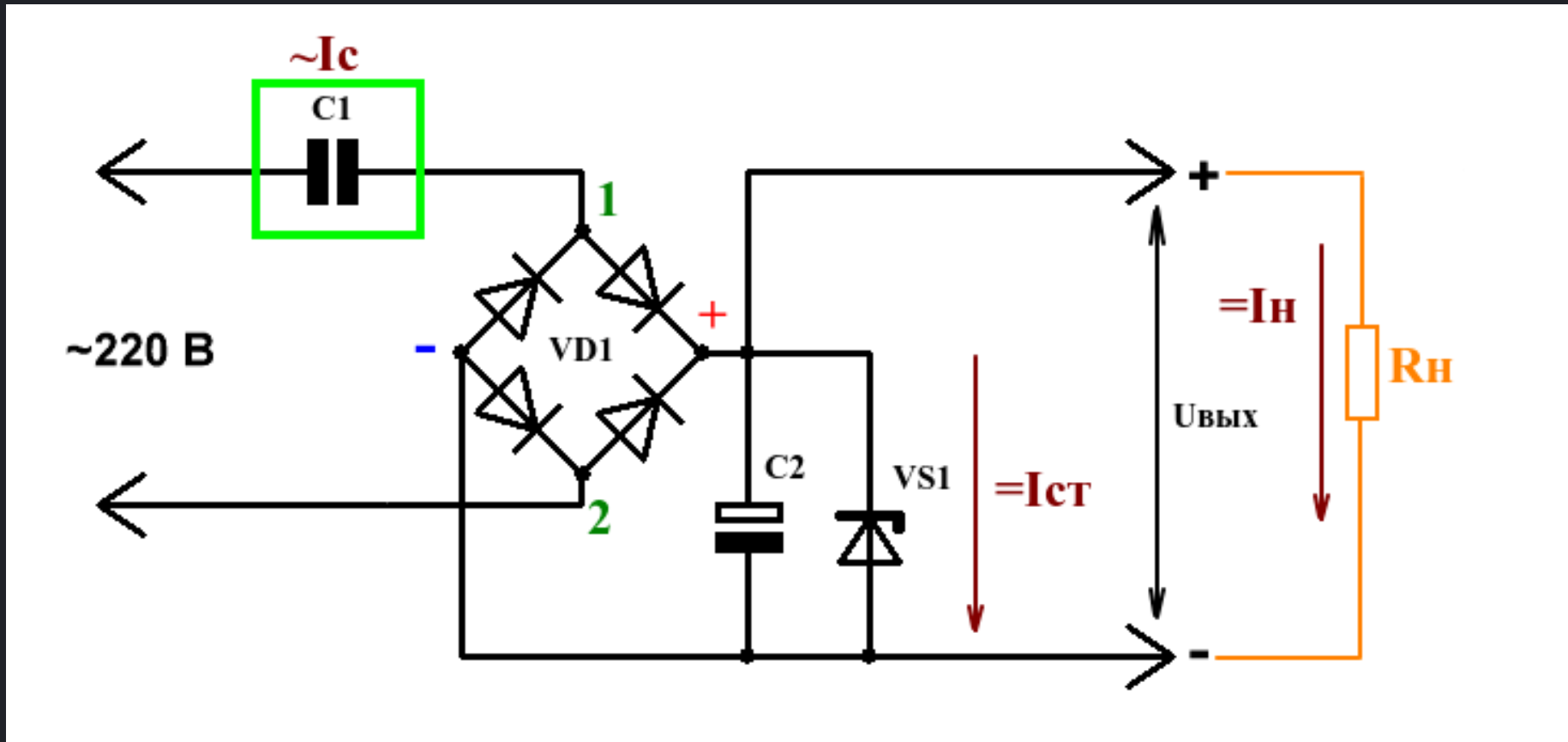


Case study #4 - HW



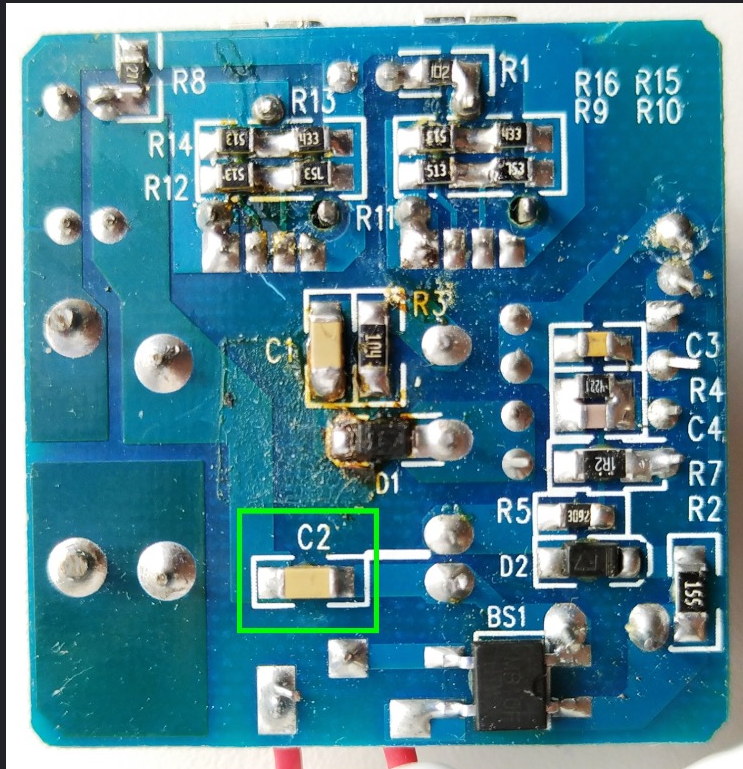
Without galvanic isolation

Case study #4 - HW

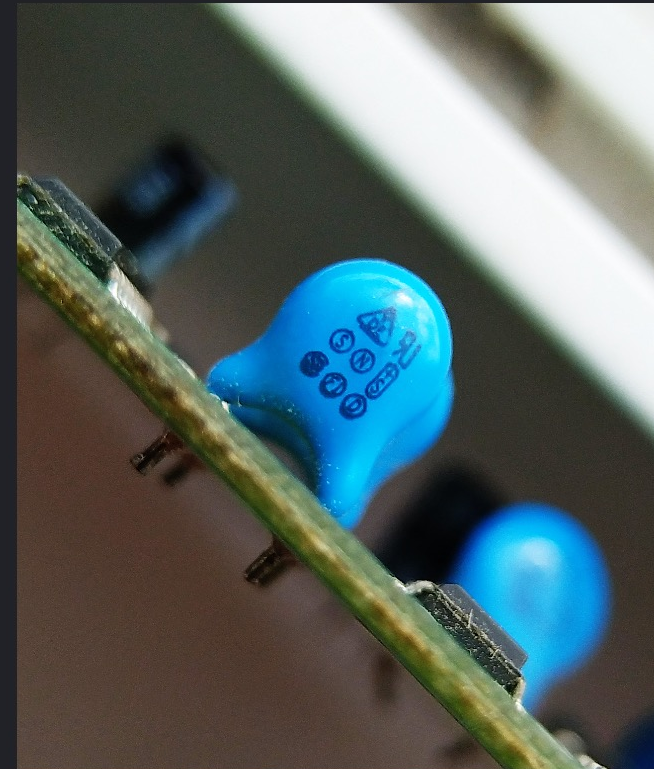


Without galvanic isolation

Case study #4 - HW

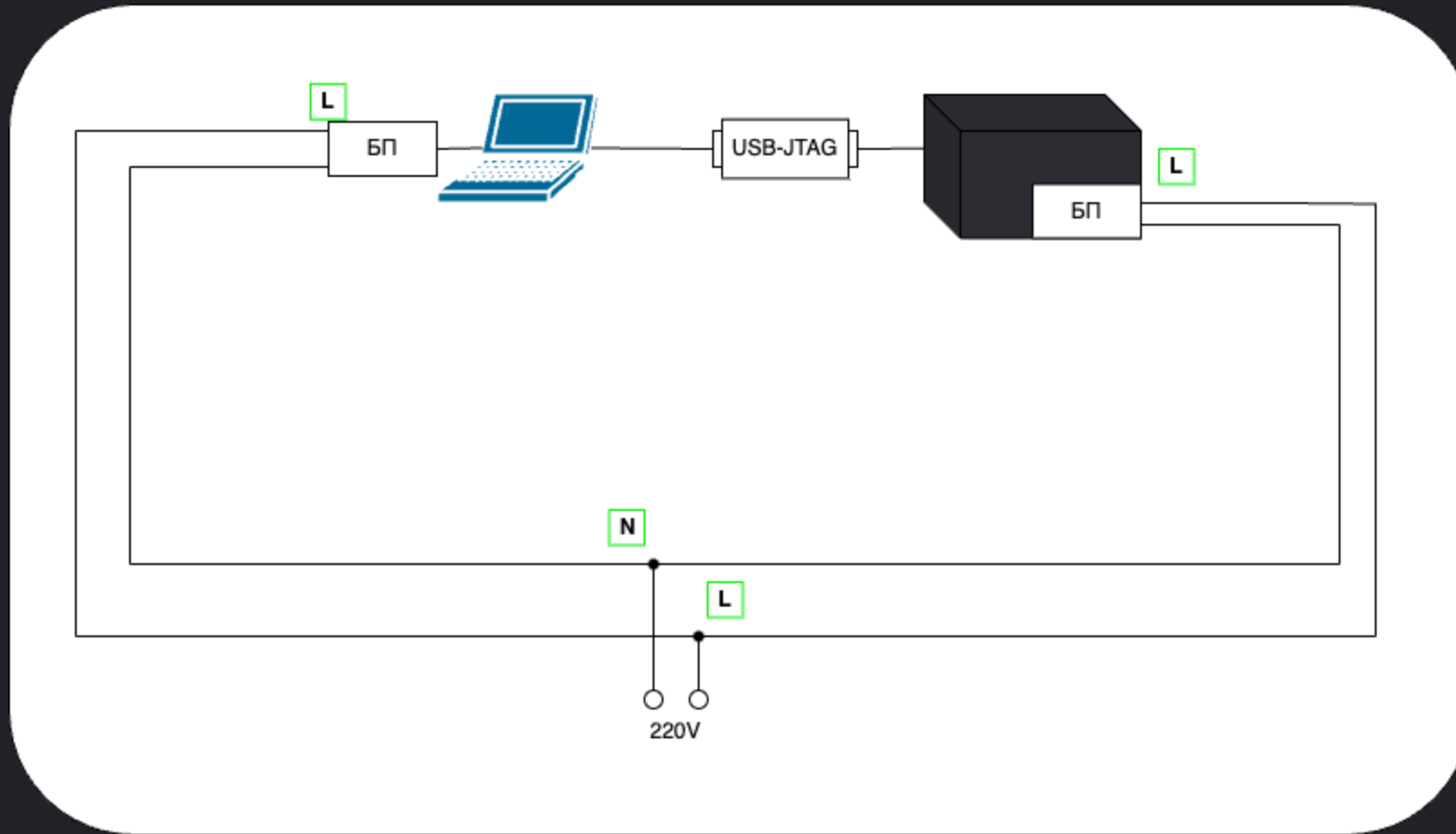


SMD Capacitor

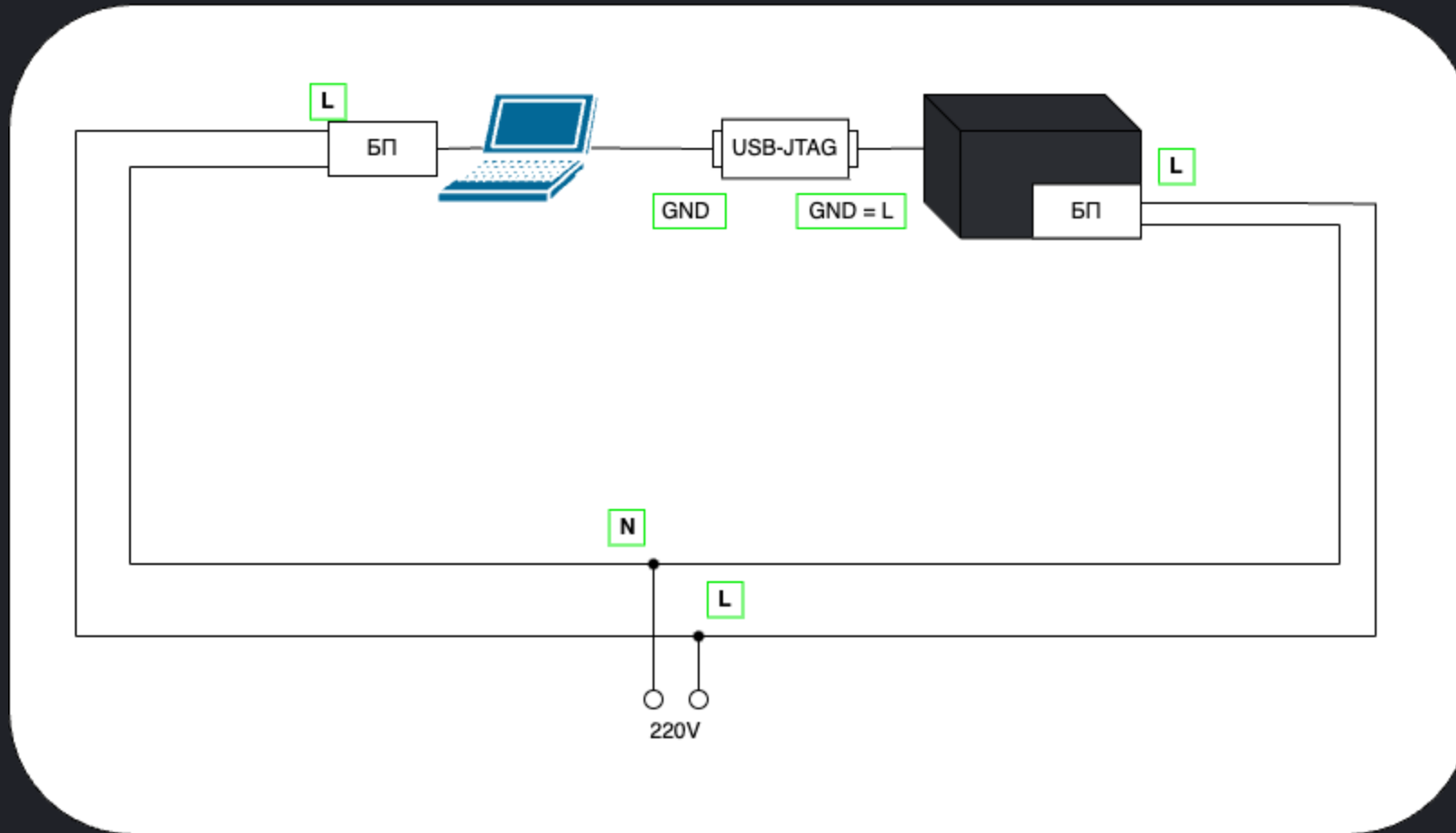


Y-Capacitor

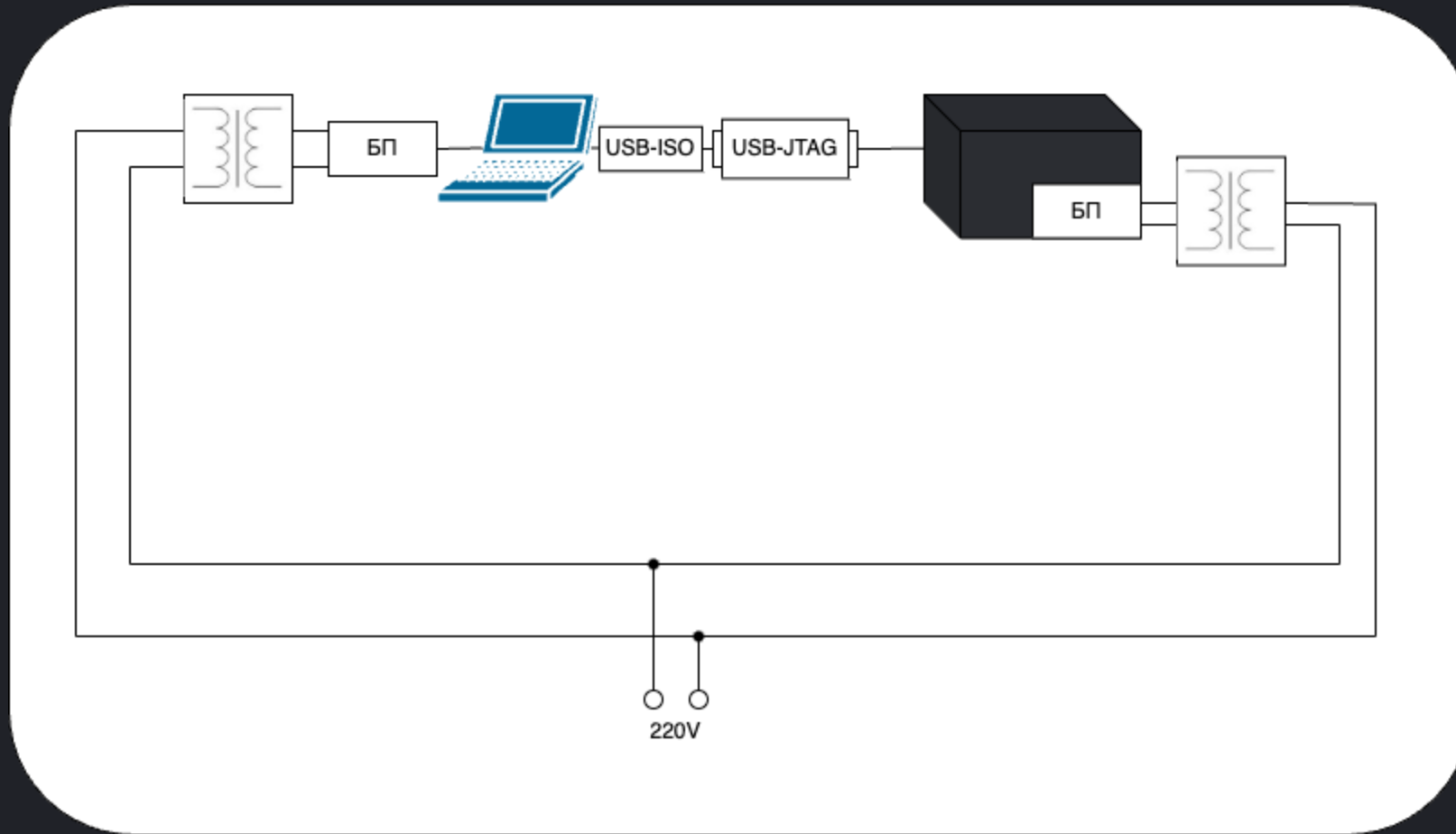
Case study #4 - HW



Case study #4 - HW



Ruleset #4



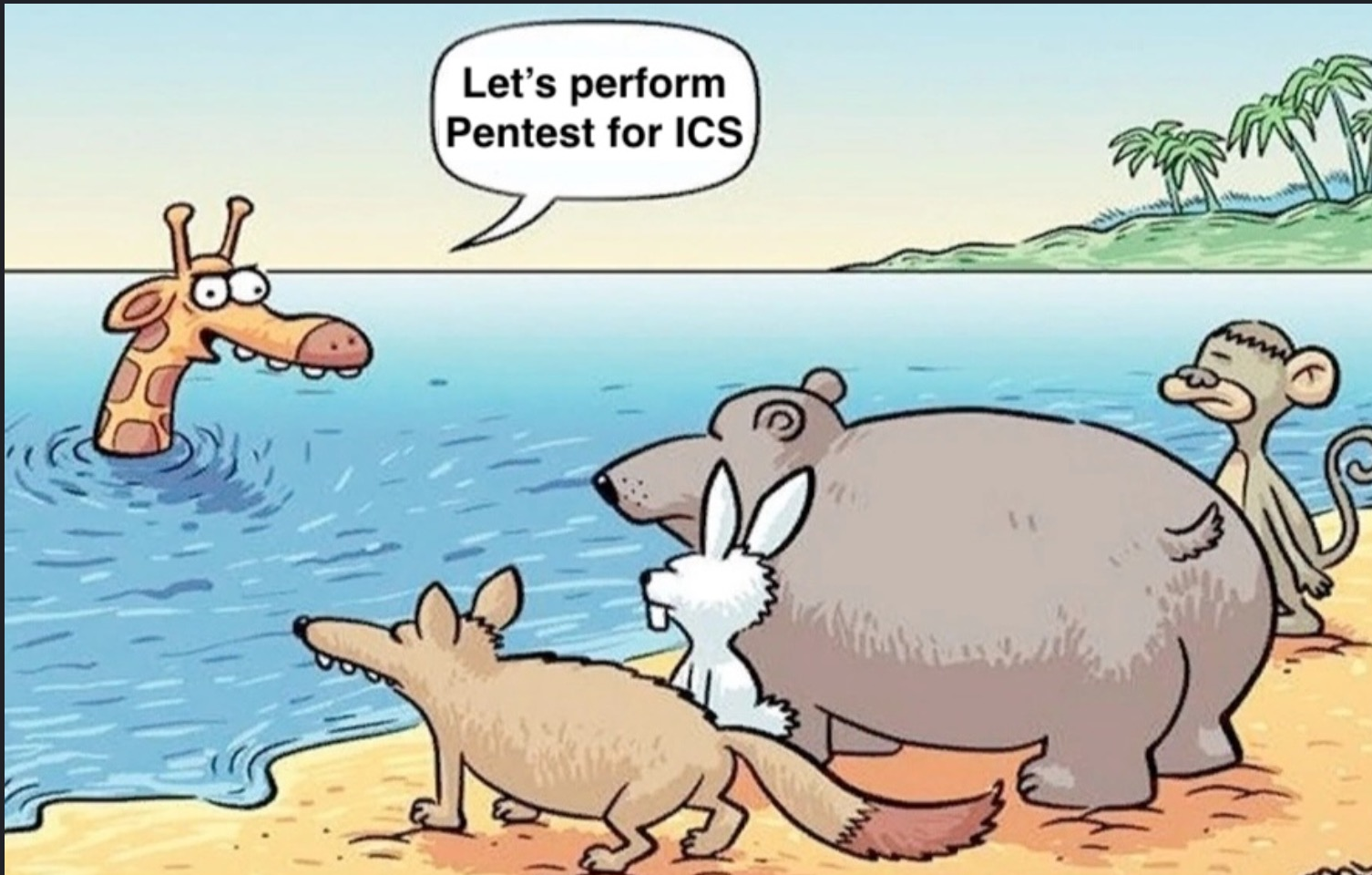
Ruleset #4

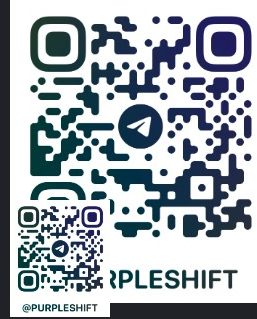
- Unplug your laptop during anytype of debugging (just in case)
- Use standalone Isolation transformer



Conclusion

- Just follow the rules





Questions?
Let's share!