CyBOK

Teaching CyBOK Through Cyber Physical Systems

Alan Mills, Jonathan White and Phil Legg

Lecturer, University of the West of England

contact@cybok.org
www.cybok.org

Welcome to the Future Funfair!

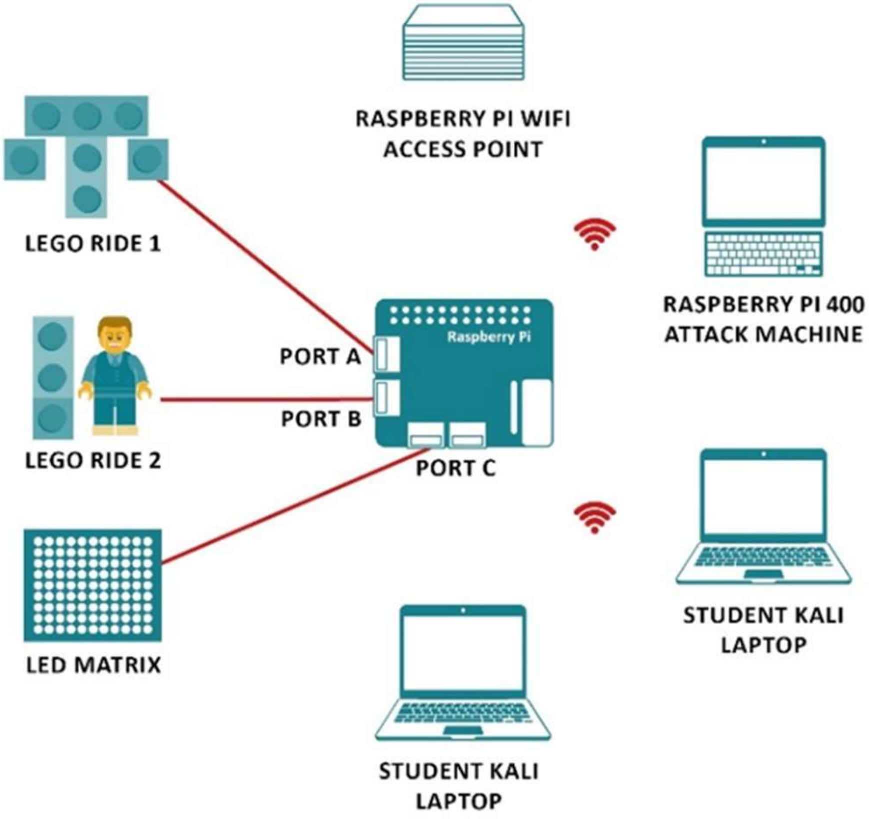
- A novel, Cyber Physical educational aide

- Created to improve knowledge of:
  - Cyber Physical Systems
  - Wider Cyber Security
  - The CyBOK

- Designed to engage students through physically observable impacts of cyber attacks

System Setup

- Key Components:
  - Raspberry Pis
  - Pi HAT
  - LEGO Spike
  - Student laptops
  - Attack Machine



System setup

Utilisation

- Two key scripts were used to orchestrate the system
  - Server script on the Pi server
  - Attack script on the student laptops

- Attacks were launched from the student laptops, via the attack machine

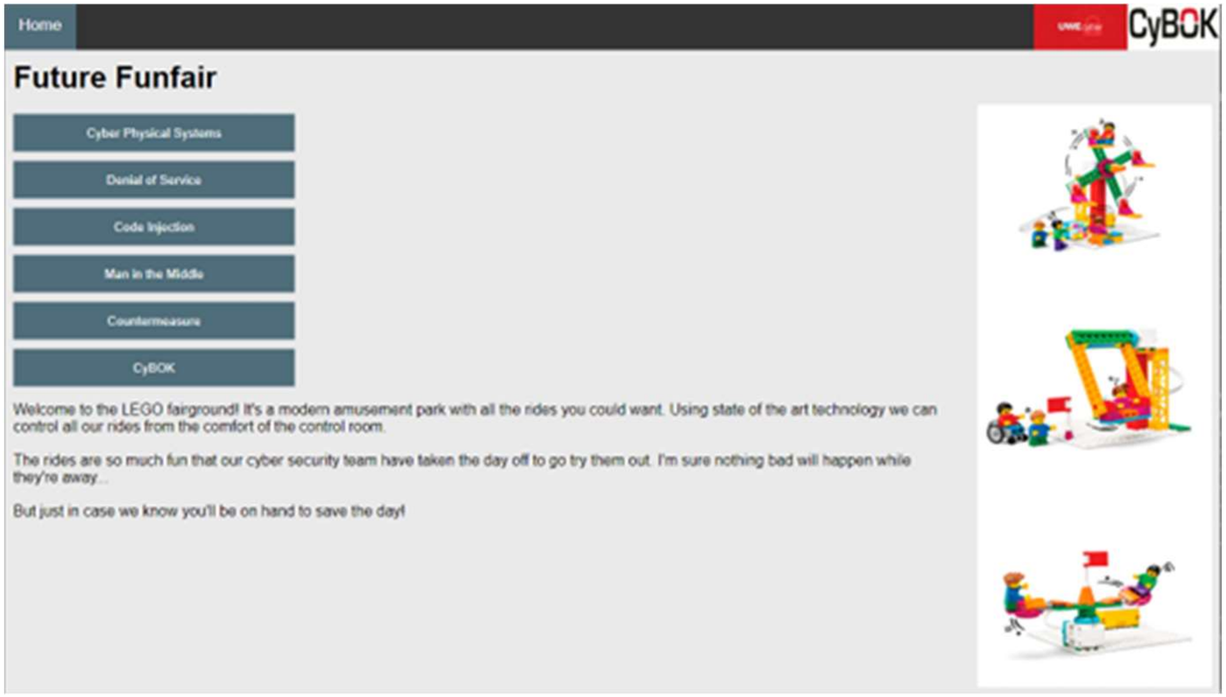
- This enabled observation of attack traffic, without breaking the engagement flow

- Students used a combination of traffic analysis, observation of the LEGO rides and the UI to understand and counter the attacks

UI

- A UI was created to help guide students through:
  - Different attacks
  - Associated countermeasures
  - Cyber Physical Systems
  - CyBOK

- As countermeasures were deployed via the UI we ensured engagement with this element



Future Funfair

Welcome to the LEGO fairground! It's a modern amusement park with all the rides you could want. Using state of the art technology we can control all our rides from the comfort of the control room.

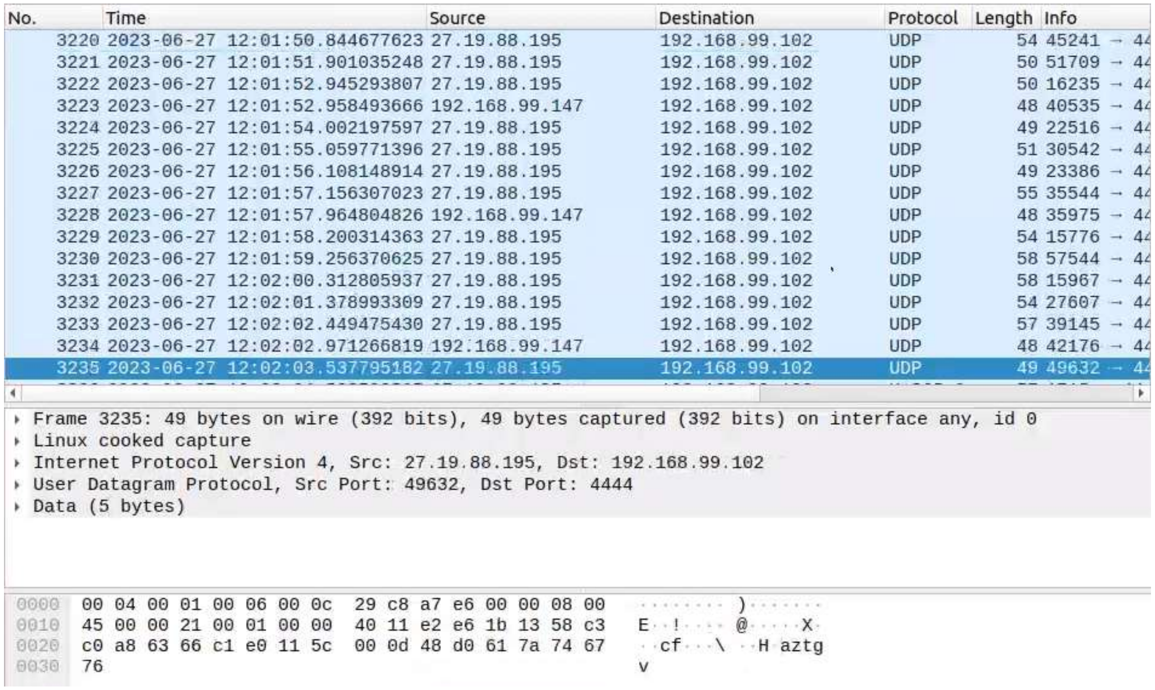
The rides are so much fun that our cyber security team have taken the day off to go try them out. I'm sure nothing bad will happen while they're away...

But just in case we know you'll be on hand to save the day!

UI splash page

Attacks

- Three attacks could be launched:
  - Code Injection
  - Denial of Service
  - Man in the Middle
- Each attack had a dedicated page on the UI to provide an attack profile
- All material was taken from or referenced the CyBOK



No.	Time	Source	Destination	Protocol	Length	Info
3220	2023-06-27 12:01:50.844677623	27.19.88.195	192.168.99.102	UDP	54	45241 → 44
3221	2023-06-27 12:01:51.901035248	27.19.88.195	192.168.99.102	UDP	50	51709 → 44
3222	2023-06-27 12:01:52.945293807	27.19.88.195	192.168.99.102	UDP	50	16235 → 44
3223	2023-06-27 12:01:52.958493666	192.168.99.147	192.168.99.102	UDP	48	40535 → 44
3224	2023-06-27 12:01:54.002197597	27.19.88.195	192.168.99.102	UDP	49	22516 → 44
3225	2023-06-27 12:01:55.059771396	27.19.88.195	192.168.99.102	UDP	51	30542 → 44
3226	2023-06-27 12:01:56.108148914	27.19.88.195	192.168.99.102	UDP	49	23386 → 44
3227	2023-06-27 12:01:57.156307023	27.19.88.195	192.168.99.102	UDP	55	35544 → 44
3228	2023-06-27 12:01:57.964804826	192.168.99.147	192.168.99.102	UDP	48	35975 → 44
3229	2023-06-27 12:01:58.200314363	27.19.88.195	192.168.99.102	UDP	54	15776 → 44
3230	2023-06-27 12:01:59.256370625	27.19.88.195	192.168.99.102	UDP	58	57544 → 44
3231	2023-06-27 12:02:00.312805937	27.19.88.195	192.168.99.102	UDP	58	15967 → 44
3232	2023-06-27 12:02:01.378993309	27.19.88.195	192.168.99.102	UDP	54	27607 → 44
3233	2023-06-27 12:02:02.449475430	27.19.88.195	192.168.99.102	UDP	57	39145 → 44
3234	2023-06-27 12:02:02.971266819	192.168.99.147	192.168.99.102	UDP	48	42176 → 44
3235	2023-06-27 12:02:03.537795182	27.19.88.195	192.168.99.102	UDP	49	49632 → 44

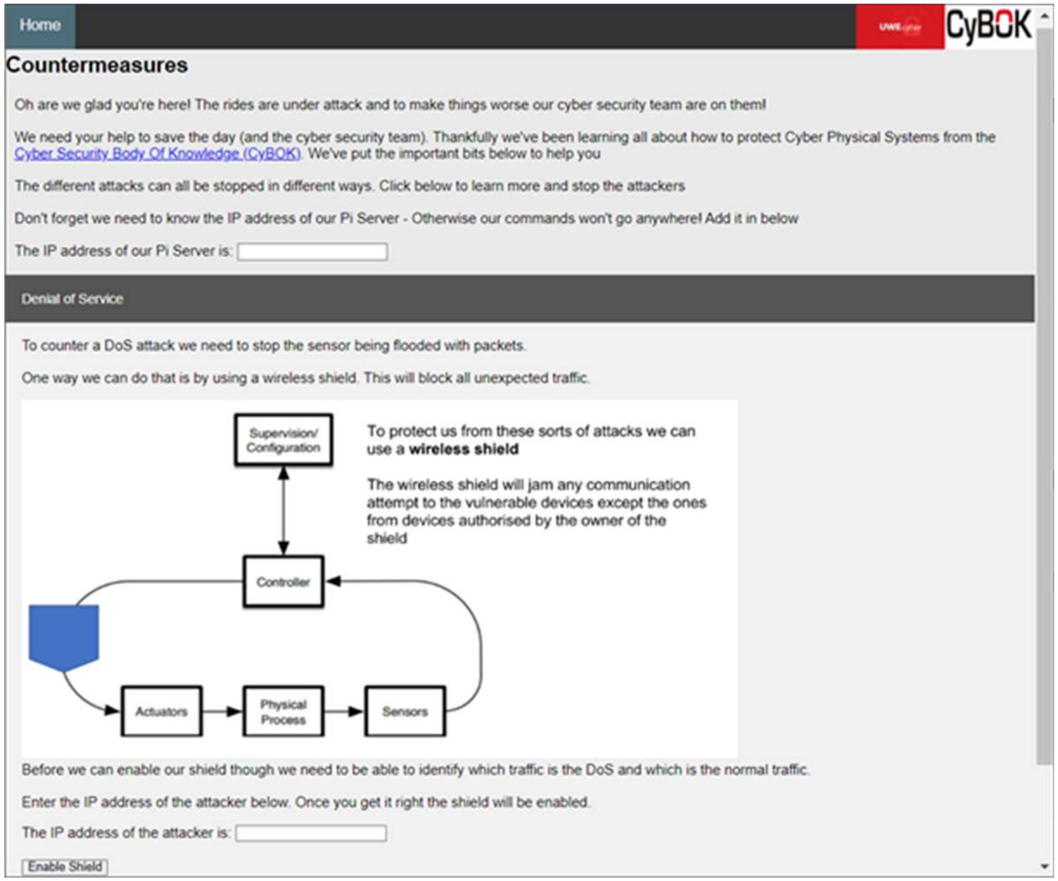
```
▸ Frame 3235: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 27.19.88.195, Dst: 192.168.99.102
▸ User Datagram Protocol, Src Port: 49632, Dst Port: 4444
▸ Data (5 bytes)
```

```
0000  00 04 00 01 00 06 00 0c  29 c8 a7 e6 00 00 08 00   ·········)······
0010  45 00 00 21 00 01 00 00  40 11 e2 e6 1b 13 58 c3   E··!····@·····X·
0020  c0 a8 63 66 c1 e0 11 5c  00 0d 48 d0 61 7a 74 67   ··cf···\··H·aztg
0030  76                                                 v
```

Network traffic during the Denial of Service attack

Countermeasures

- Once the attack was identified students could launch a countermeasure against it
- Mitigations, graphics and language used were all taken from the CyBOK
- The attack would continue but no longer have an impact on the running system(s)



Countermeasures

Oh are we glad you're here! The rides are under attack and to make things worse our cyber security team are on them!

We need your help to save the day (and the cyber security team). Thankfully we've been learning all about how to protect Cyber Physical Systems from the Cyber Security Body Of Knowledge (CyBOK). We've put the important bits below to help you

The different attacks can all be stopped in different ways. Click below to learn more and stop the attackers

Don't forget we need to know the IP address of our Pi Server - Otherwise our commands won't go anywhere! Add it in below

The IP address of our Pi Server is: ▭

Denial of Service

To counter a DoS attack we need to stop the sensor being flooded with packets.

One way we can do that is by using a wireless shield. This will block all unexpected traffic.

To protect us from these sorts of attacks we can use a **wireless shield**

The wireless shield will jam any communication attempt to the vulnerable devices except the ones from devices authorised by the owner of the shield

Before we can enable our shield though we need to be able to identify which traffic is the DoS and which is the normal traffic.

Enter the IP address of the attacker below. Once you get it right the shield will be enabled.

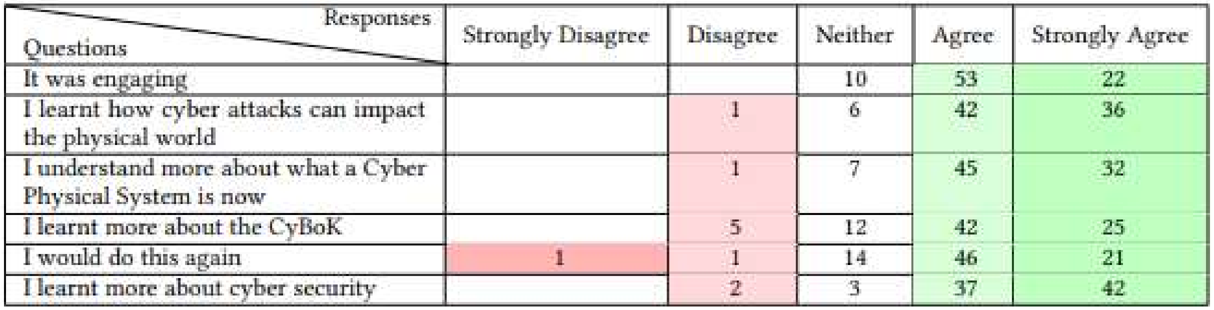
The IP address of the attacker is: ▭

UI Countermeasures page - Denial of Service section

Results

- The activity was run at the Unlock Cyber event at UWE

- Students were asked to take part in a short, anonymised survey after the activity



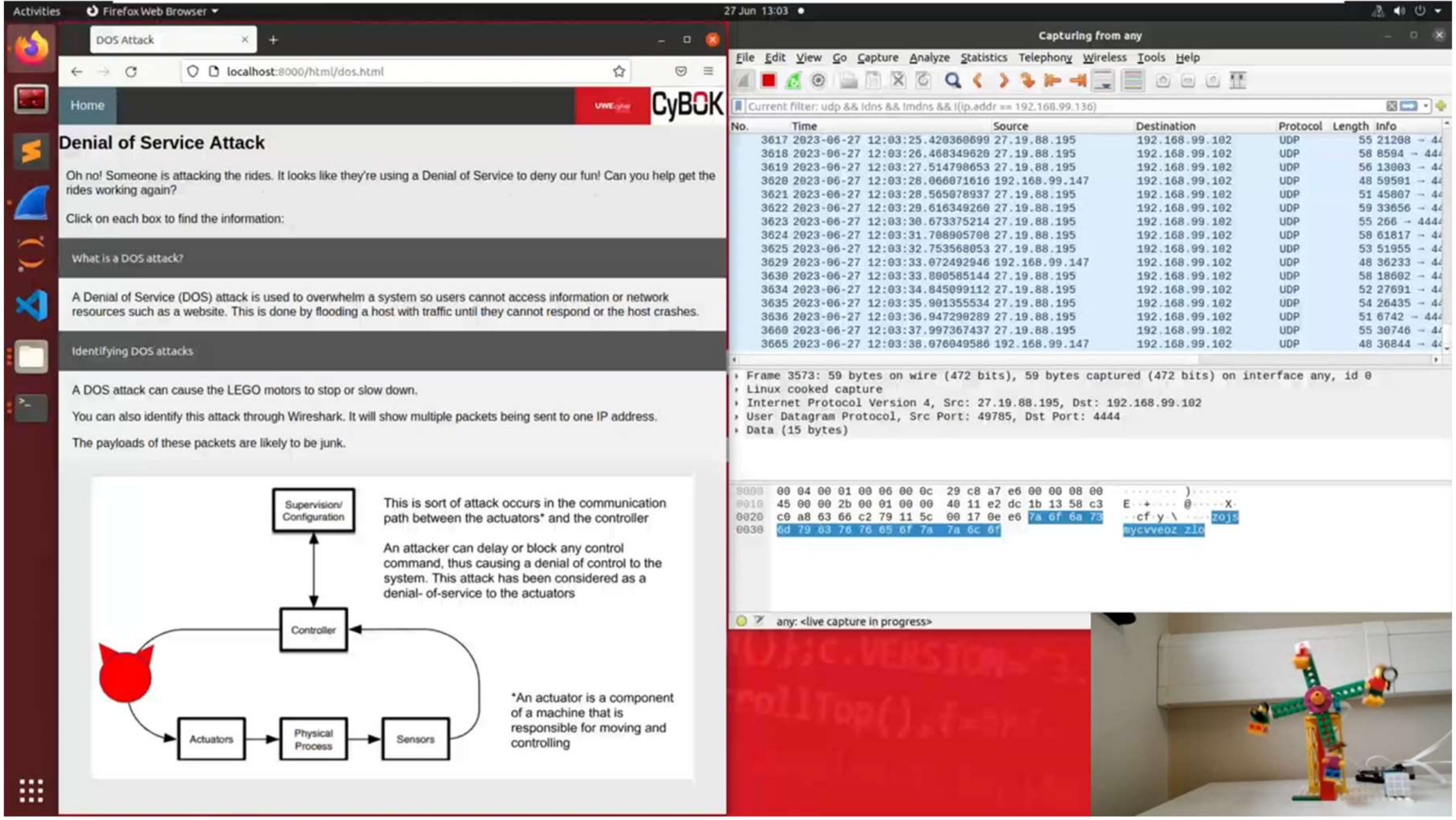
Responses Questions	Strongly Disagree	Disagree	Neither	Agree	Strongly Agree
It was engaging			10	53	22
I learnt how cyber attacks can impact the physical world		1	6	42	36
I understand more about what a Cyber Physical System is now		1	7	45	32
I learnt more about the CyBoK		5	12	42	25
I would do this again	1	1	14	46	21
I learnt more about cyber security		2	3	37	42

Survey questions and responses

Extended support

- To support wider outreach all material has been made available on the UWE website
- We have also put together videos and supporting documentation which will be hosted by the CyBOK
- These videos provide a walkthrough of the system and allow schools without access to LEGO Spike kits to observe the attacks

Extended support



Activities
Firefox Web Browser
27 Jun 13:03
DOS Attack
localhost:8000/html/dos.html
Home
CyBOK
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Supervision/ Configuration
Controller
Actuators
Physical Process
Sensors

Denial of Service Attack

Oh no! Someone is attacking the rides. It looks like they're using a Denial of Service to deny our fun! Can you help get the rides working again?

Click on each box to find the information:

What is a DOS attack?

A Denial of Service (DOS) attack is used to overwhelm a system so users cannot access information or network resources such as a website. This is done by flooding a host with traffic until they cannot respond or the host crashes.

Identifying DOS attacks

A DOS attack can cause the LEGO motors to stop or slow down.

You can also identify this attack through Wireshark. It will show multiple packets being sent to one IP address.

The payloads of these packets are likely to be junk.

This is sort of attack occurs in the communication path between the actuators* and the controller

An attacker can delay or block any control command, thus causing a denial of control to the system. This attack has been considered as a denial- of-service to the actuators

*An actuator is a component of a machine that is responsible for moving and controlling

```
Current filter: udp && !dns && !mdns && !(ip.addr == 192.168.99.136)

No.  Time                          Source          Destination     Protocol Length Info
3617 2023-06-27 12:03:25.420360699 27.19.88.195    192.168.99.102  UDP      55 21208 → 44
3618 2023-06-27 12:03:26.468349620 27.19.88.195    192.168.99.102  UDP      58 8594 → 444
3619 2023-06-27 12:03:27.514798653 27.19.88.195    192.168.99.102  UDP      56 13003 → 44
3620 2023-06-27 12:03:28.066071616 192.168.99.147  192.168.99.102  UDP      48 59501 → 44
3621 2023-06-27 12:03:28.565078937 27.19.88.195    192.168.99.102  UDP      51 45807 → 44
3622 2023-06-27 12:03:29.616349260 27.19.88.195    192.168.99.102  UDP      59 33656 → 44
3623 2023-06-27 12:03:30.673375214 27.19.88.195    192.168.99.102  UDP      55 266 → 4444
3624 2023-06-27 12:03:31.708905708 27.19.88.195    192.168.99.102  UDP      58 61817 → 44
3625 2023-06-27 12:03:32.753568053 27.19.88.195    192.168.99.102  UDP      53 51955 → 44
3629 2023-06-27 12:03:33.072492946 192.168.99.147  192.168.99.102  UDP      48 36233 → 44
3630 2023-06-27 12:03:33.800585144 27.19.88.195    192.168.99.102  UDP      58 18602 → 44
3634 2023-06-27 12:03:34.845099112 27.19.88.195    192.168.99.102  UDP      52 27691 → 44
3635 2023-06-27 12:03:35.901355534 27.19.88.195    192.168.99.102  UDP      54 26435 → 44
3636 2023-06-27 12:03:36.947290289 27.19.88.195    192.168.99.102  UDP      51 6742 → 444
3660 2023-06-27 12:03:37.997367437 27.19.88.195    192.168.99.102  UDP      55 30746 → 44
3665 2023-06-27 12:03:38.076049586 192.168.99.147  192.168.99.102  UDP      48 36844 → 44

› Frame 3573: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface any, id 0
› Linux cooked capture
› Internet Protocol Version 4, Src: 27.19.88.195, Dst: 192.168.99.102
› User Datagram Protocol, Src Port: 49785, Dst Port: 4444
› Data (15 bytes)

0000  00 04 00 01 00 06 00 0c  29 c8 a7 e6 00 00 08 00   ········ )·······
0010  45 00 00 2b 00 01 00 00  40 11 e2 dc 1b 13 58 c3   E··+···· @·····X·
0020  c0 a8 63 66 c2 79 11 5c  00 17 0e e6 7a 6f 6a 73   ··cf·y·\ ····zojs
0030  6d 79 63 76 76 65 6f 7a  7a 6c 6f                  mycvveoz zlo

any: <live capture in progress>
```

Video clip – Denial of Service attack video

Further details

- https://go.uwe.ac.uk/legofunfair
- https://github.com/uwe-cyber/Future_Funfair
- https://www.unlockcyber.com/mission/

- Alan Mills

- Jonathan White

- Phil Legg

Closing comment

CyBOK