DMU
HACKERS

Announcements

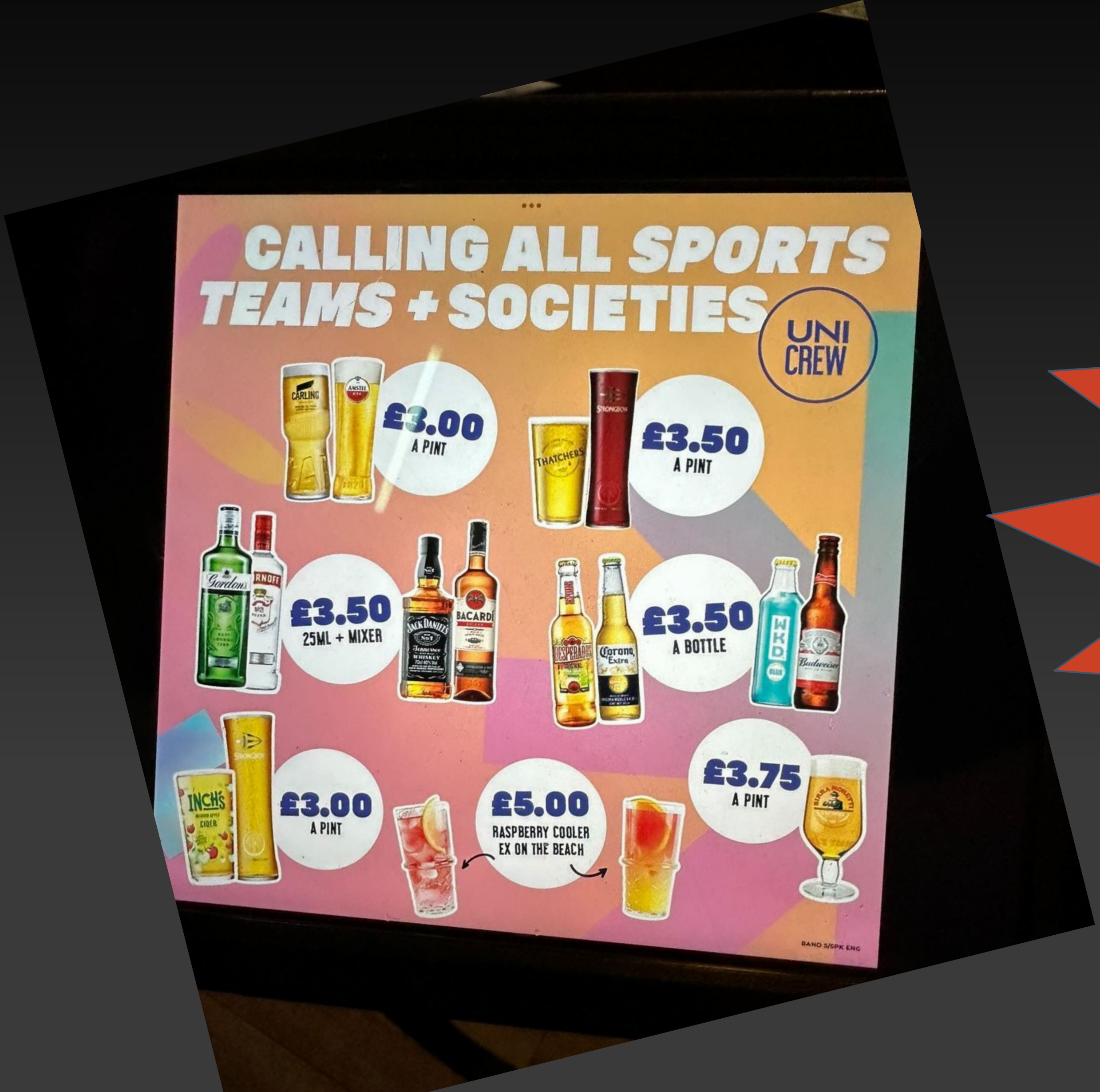
- Thank you for last week!
- Please buy your memberships if haven't already
- Soar Point QR
- Firebug cards
- CyberFirst volunteers needed - next Sat (21st Oct)

CyberFirst Days

- Free half-day session for Y8 and Y9s talking with activities related to cyber and technology
- Great for CV, something to talk about in interviews -> especially if applying for CyberFirst schemes in future…

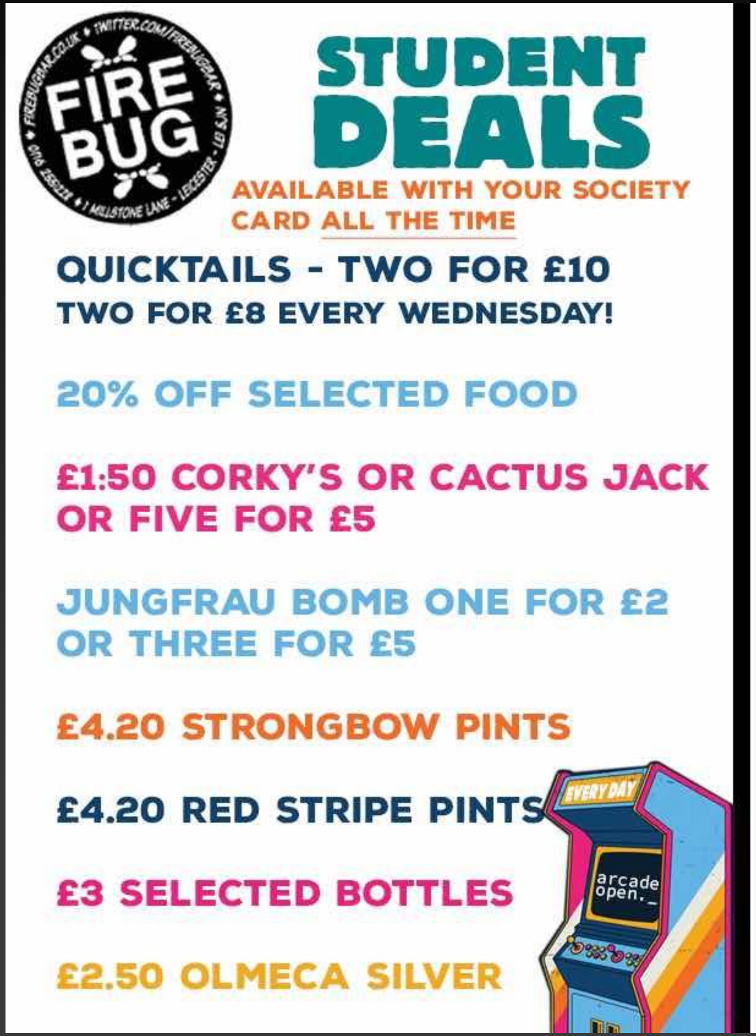
1st Session - Next Saturday (21st October) 9am-3pm
Contact: CyberFirst@dmu.ac.uk (Sarah De'Ath)

Soar Deals - QR Code



Burgers and Pizzas FROM £7!

Firebug Deals


FIRE BUG
EVERY DAY
arcade open._

STUDENT DEALS

AVAILABLE WITH YOUR SOCIETY CARD ALL THE TIME

QUICKTAILS - TWO FOR £10
TWO FOR £8 EVERY WEDNESDAY!

20% OFF SELECTED FOOD

£1:50 CORKY'S OR CACTUS JACK
OR FIVE FOR £5

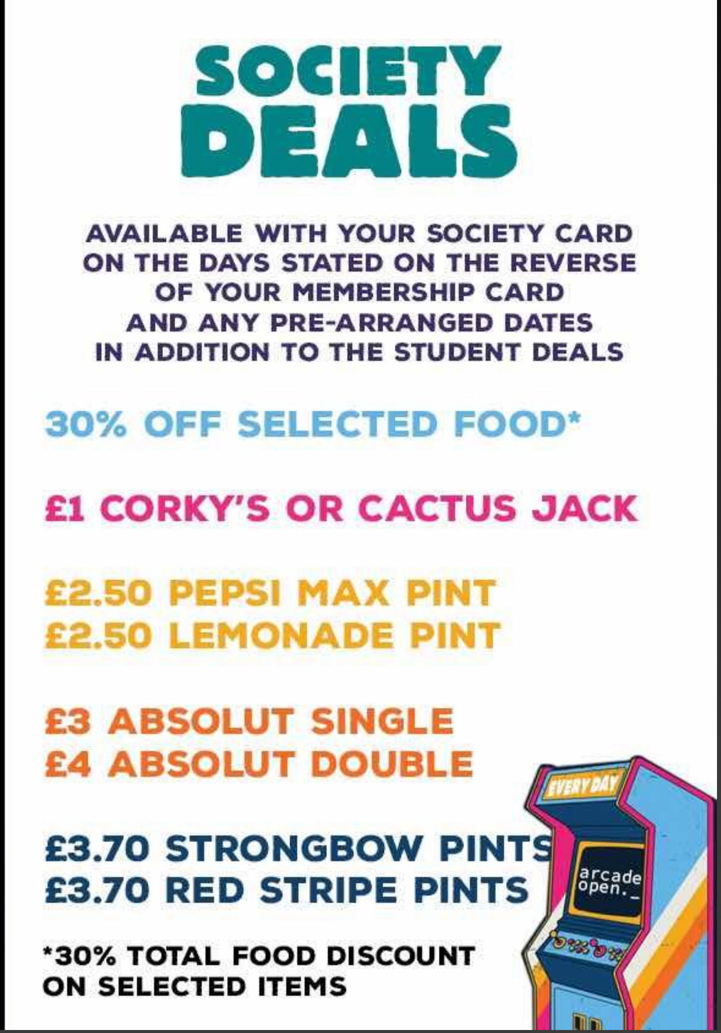
JUNGFRAU BOMB ONE FOR £2
OR THREE FOR £5

£4.20 STRONGBOW PINTS

£4.20 RED STRIPE PINTS

£3 SELECTED BOTTLES

£2.50 OLMECA SILVER


EVERY DAY
arcade open._

SOCIETY DEALS

AVAILABLE WITH YOUR SOCIETY CARD ON THE DAYS STATED ON THE REVERSE OF YOUR MEMBERSHIP CARD AND ANY PRE-ARRANGED DATES IN ADDITION TO THE STUDENT DEALS

30% OFF SELECTED FOOD*

£1 CORKY'S OR CACTUS JACK

£2.50 PEPSI MAX PINT
£2.50 LEMONADE PINT

£3 ABSOLUT SINGLE
£4 ABSOLUT DOUBLE

£3.70 STRONGBOW PINTS
£3.70 RED STRIPE PINTS

*30% TOTAL FOOD DISCOUNT ON SELECTED ITEMS

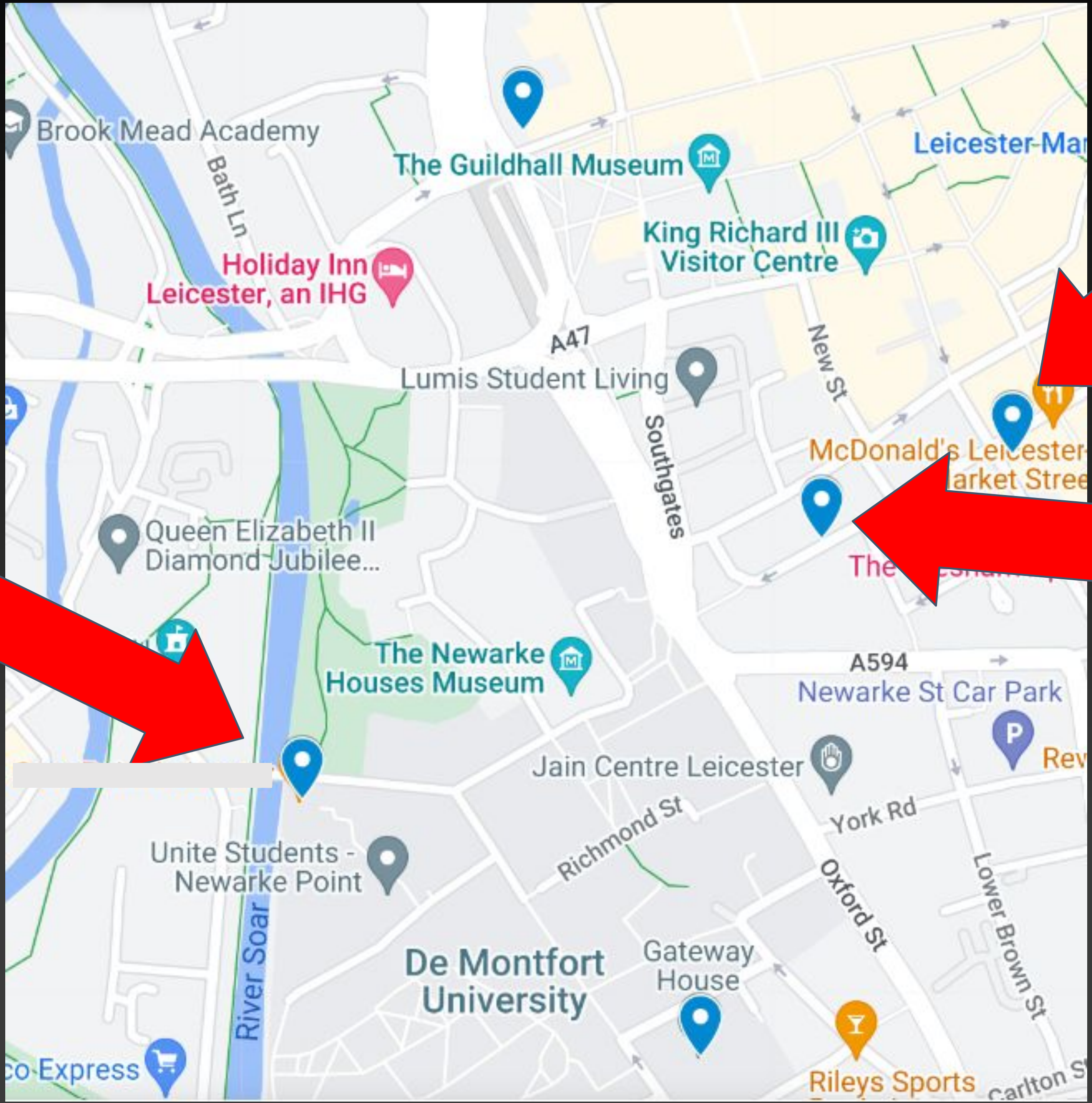
Burger + Chips = £5ish

Bug Box = £3ish

DMU HACKERS

Social

THE SOAR POINT



FIREBUG
BAR . VENUE . FOOD

oddbar

DMU HACKERS

hackers.dmu

@dmuhackers

DMU HACKERS

Basic Web Exploitation

Don't do illegal shit

URL Parameters

- For GET requests, data is included in the URL as a parameter
- Parameters are given after ‘?’ and can be joined together with ‘&’
- They are formatted parameter=value

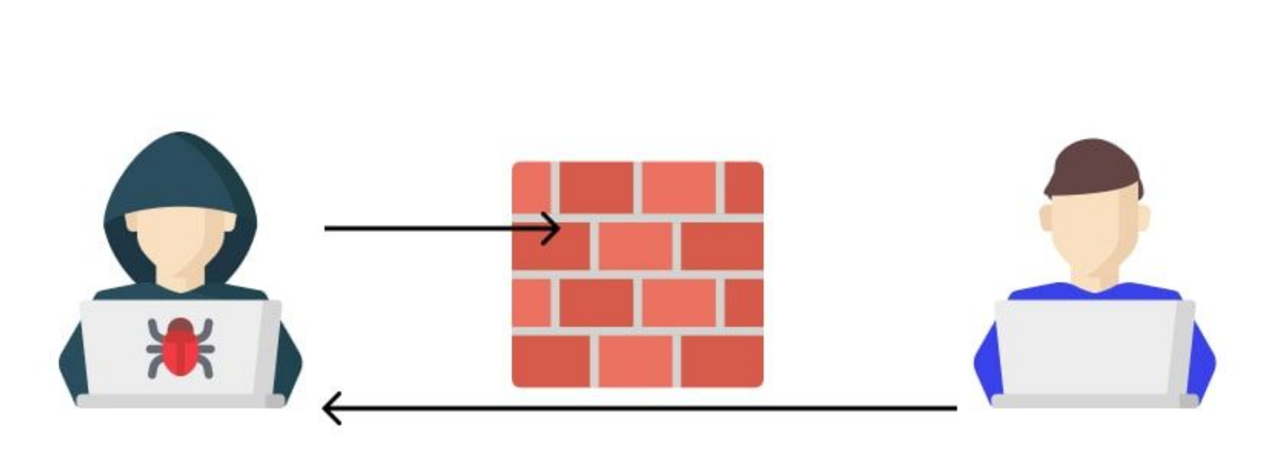
E.g.
https://dmuhackers.com/index.php?colour=blue&size=big

Reverse Shells

- A reverse shell allows an attacker to connect to and control a victim's machine by sending a payload to that will then connect back to the attacker's listener.
- Most web servers use a PHP backend, so if we’re wanting to exploit a web server, we’ll need a php reverse shell.

Reverse Shells

- Many different reverse shells available in all sorts of languages - https://revshells.com



Bypassing File Uploads

- Checks are usually in place to limit what types of files can be uploaded by a website user
- For example, a check that a user has uploaded and image (.png) instead of a malicious script (.php)

Bypassing File Uploads

- Can use tools like Burpsuite to intercept and change MIME type:

✗ `Content-type: application/x-php`

✓ `Content-type: image/jpeg`

- Can also change to an alternative extension:

PHP	.php, .phtml, .php3, .php4, .php5 and .inc
ASP	.asp, .aspx
PERL	.pl, .pm, .cgi, .lib
JSP	.jsp, .jspx, .jsw, .jsv, .jspf

Today's Box…

Ignore the fact it's Christmas themed!

Advent of Cyber 2 [2020] - Day 2 (The Elf Strikes Back!)
c
https://tryhackme.com/room/adventofcyber2

Advent of Cyber 2 [2020] - Day 2 (The Elf Strikes Back!)

https://tryhackme.com/room/adventofcyber2

Tips:

- ID task - uses URL parameters
- Copy file into your own directory:
  `cp /usr/share/webshells/php/php-reverse-shell.php /root/`
  Use TAB to autocomplete!
- When uploading, change from `‘All Supported Types’` to `‘All Files’`
- To read a file, `cat <directory>`

EXTENSION: OWASP Juice Shop

https://tryhackme.com/room/owaspjuiceshop

Demonstration

Resources

- https://revshells.com - great for CTFs - enter IP/port and it does all the hard work for you
- File Upload Bypassing - Hackers Grimoire - Great quick reference page!
- File Upload - HackTricks - More In-Depth Step-By-Step checklist

Pub time!