WELCOME TO CLASS 3!

BLACK HAT PYTHON3

RALEIGH ISSA

GITHUB REPO

https://github.com/tiarno/bhp3_class

SUMMARY FROM LAST CLASS

- mapping an app
- word lists for enumeration
- word lists for password bruteforce
- browser tools
- `lxml` for web parsing

POLL

https://linkto.run/p/OTWCR171

WRAPPING UP BHP CHAPTER 5

Web Hacking

A NOTE ON ITERATING A QUEUE

You can't do it that way :-)

CLEAN UP `mapper.py`

- contextlib/ context manager
- thread.join()

https://pymotw.com/3/contextlib/index.html#from-generator-to-context-manager

A NOTE ON `lxml`

General notes and demo

```
from lxml import etree
url = 'http://www.textfiles.com/hacking/INTERNET'
parser = etree.HTMLParser()
tree = etree.parse(url, parser=parser)
headelem = tree.find('//h1')
print(headelem.text)
```

EXCEPTION HANDLING

https://www.pythonforthelab.com/blog/learning-not-to-handle-exceptions/

BLACK HAT PYTHON, CHAPTER 3

SOCKETS

https://github.com/crazyguitar/pysheeet/blob/master/docs/lang/python-socket.rst

SOCKET SERVER

Required:

- **create**
- **bind**

Maybe, depends on type:

- listen
- accept

```
sock_obj = socket.socket(socket_family,  # AF_INET
                         socket_type,    # SOCK_STREAM, SOCK_D
                         socket_protocol # IPPROTO_ICMP, IPPRO
                        )
```

SOCKET CLIENT

- connect

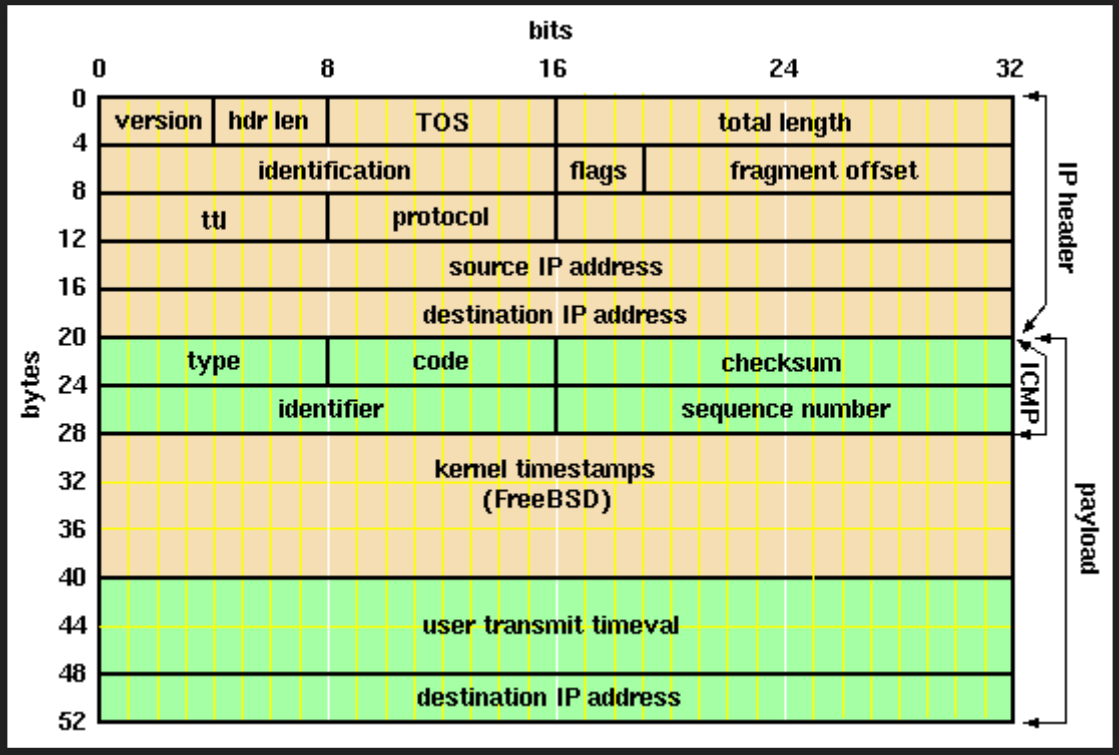
SOCKET COMMUNICATION

- send
- recv
- sendto
- recvfrom

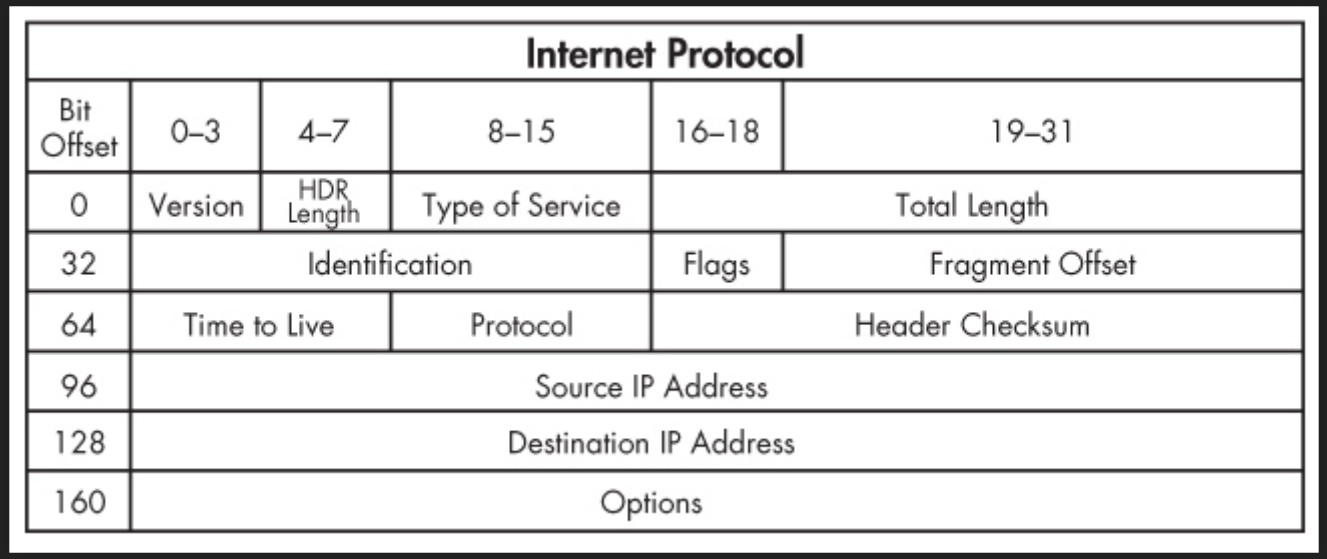
LET'S CODE!

`sniffone.py`

IP PACKET


bits
0
8
16
24
32
bytes
0
4
8
12
16
20
24
28
32
36
40
44
48
52
version
hdr len
TOS
total length
identification
flags
fragment offset
ttl
protocol
source IP address
destination IP address
type
code
checksum
identifier
sequence number
kernel timestamps
(FreeBSD)
user transmit timeval
destination IP address
IP header
ICMP
payload

IP HEADER



Internet Protocol					
Bit Offset	0–3	4–7	8–15	16–18	19–31
0	Version	HDR Length	Type of Service	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source IP Address				
128	Destination IP Address				
160	Options				

CODE

- c_ip.py
- struct_ip.code
- c_icmp.py
- struct_icmp.py

`struct` PACKAGE

https://docs.python.org/3/library/struct.html

HEADER PARTS

```
1.      B (ver, hdrlen)
2.      B tos
3.      H total len
4.      H identification
5.      H flags + frag offset
6.      B ttl
7.      B protocol
8.      H checksum
9.      4s src ip
10.     4s dst ip
```

HIGH NYBBLE

We have one byte and want the high-order nybble:

0	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**>> 4**
0	0	0	0	0	1	0	1	

LOW NYBBLE

We have one byte and want the low-order nybble:

0	1	0	1	0	1	1	0	&F
0	0	0	0	1	1	1	1	
0	0	0	0	0	1	1	0	

PYTHON CODE

```
>>> m = 66
>>> m
66
>>> bin(m)
'0b1000010' # or 0100 0010
>>> bin(m>>4)
'0b100'     # or 0100
>>> bin(m&0xF)
'0b10'      # or      0010
```

```
"{0:016b}".format(0x1234)
f"{0x1234:016b}"


>>> '{0:08b}'.format(0x45)
'01000101'
>>> '{0:04b}'.format(0x45>>4)
'0100'
>>> '{0:04b}'.format(0x45&0xF)
'0101'
```

TEST IT OUT:

- `ipheader0.py`

ICMP HEADER

Destination Unreachable Message		
0–7	8–15	16–31
Type = 3	Code	Header Checksum
Unused		Next-hop MTU
IP Header and First 8 Bytes of Original Datagram's Data		

ICMP HEADERS

- ping
- traceroute

https://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/icmp-code.html

TEST IT OUT:

- `ipheader1.py`

IPADDRESS PACKAGE

https://docs.python.org/3/library/ipaddress.html

UDP SCANNER

- how it works
- UDP packet to unused port
  - network unreachable (from router)
  - host unreachable (from router)
  - port unreachable !

TEST IT OUT

- `scanner.py`

READING 1

https://docs.python.org/3/library/struct.html#format-characters

https://docs.python.org/3.5/library/ctypes.html#ctypes.

http://www.firewall.cx/networking-topics/protocols/icmp-protocol/153-icmp-destination-unreachable.html

YOUR JOB

- Pick your favorite method to define headers
- Add an IP and ICMP class to your `bhp3_class/packets/__init__.py` file
- Create your own network UDP scanner in your `bhp3_class/packets` module

FEEDBACK PLEASE!

- tim@reachtim.com
- discord: https://discord.gg/WR23qUj