

0xBU

Network Security

@ Boston University 2016

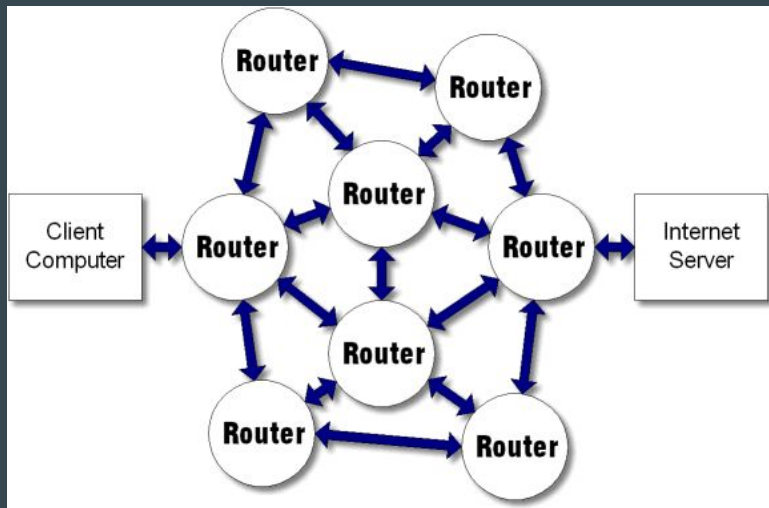
What is the Internet ($\frac{1}{3}$)

- The Internet is a set of protocols
- Request for Comments (RFCs) organized by the Internet Engineering Task Force (IETF)
 - rfc791: "Internet Protocol"
 - rfc2616: "Hypertext Transfer Protocol -- HTTP/1.1"
 - rfc1149: "A Standard for the Transmission of IP Datagrams on Avian Carriers"



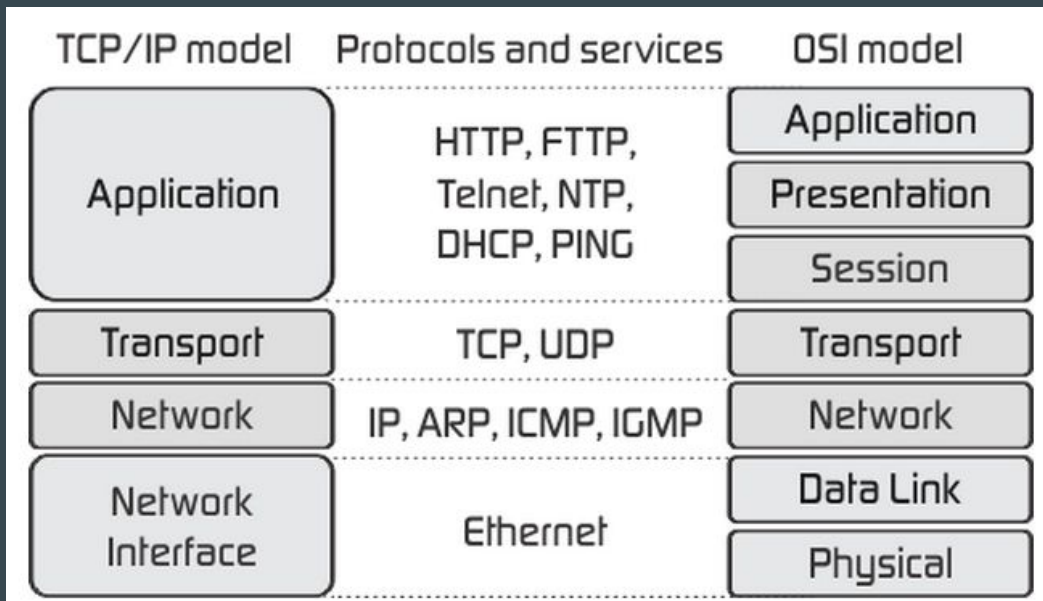
What is the Internet (2/3)

- The Internet works through a bunch of routers/hops.
 - Packets, move from one router to the other, without preserving any state.
 - The router has no clue Mary's 10 packets relate to each other.
 - Intelligence is done by the end-hosts, e.g. your browser/operating system.
 - Robust simplicity by being "dumb".



What is the Internet (3/3)

- The Internet has a layered design.
 - Each layer relies on layers below it.
 - Each layer provides a service to the layer above it.

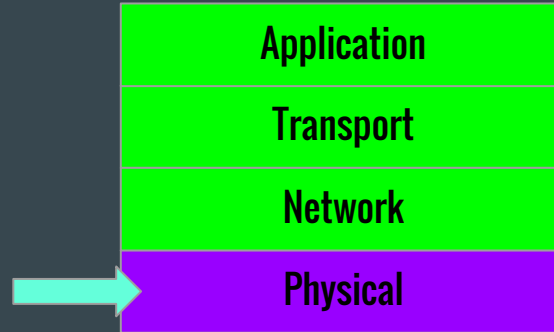


What do we want secure about the Internet?

- Confidentiality
 - No one can read our data unless we want them to.
 - Eve reading your emails =(
- Integrity
 - No one can manipulate our data unless we want them to.
 - Eve editing our emails =(
- Availability
 - We can access our data when want to
 - Eve ruining your Xbox experience =(

Physical Layer

The actual wire + transforming electricity into digital data



Physical Layer Security

- One of the hardest to secure
 - Attacker can **eavesdrop** =(
 - Attacker can **spoof** messages =(
 - The closest to the origin you can get

In an effort to alter the balance of Cold War, these men scoured the ocean floor for a five-inch diameter cable carry secret Soviet communications between military bases.

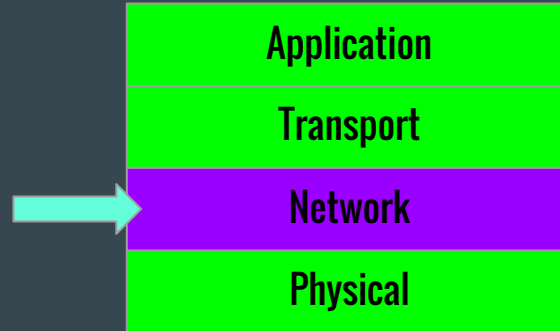
The divers found the cable and installed a 20-foot long listening device on the cable. designed to attach to the cable without piercing the casing, the device recorded all communications that occurred.

Upon their return to the United States, intelligence agents from the NSA analyzed the recordings and tried to decipher any encrypted information. The Soviets apparently were confident in the security of their communications lines, as a surprising amount of sensitive information traveled through the lines without encryption.

Upon their return to the United States, intelligence agents from the NSA analyzed the recordings and tried to decipher any encrypted information. The Soviets apparently were confident in the security of their communications lines, as a surprising amount of sensitive information traveled through the lines without encryption.

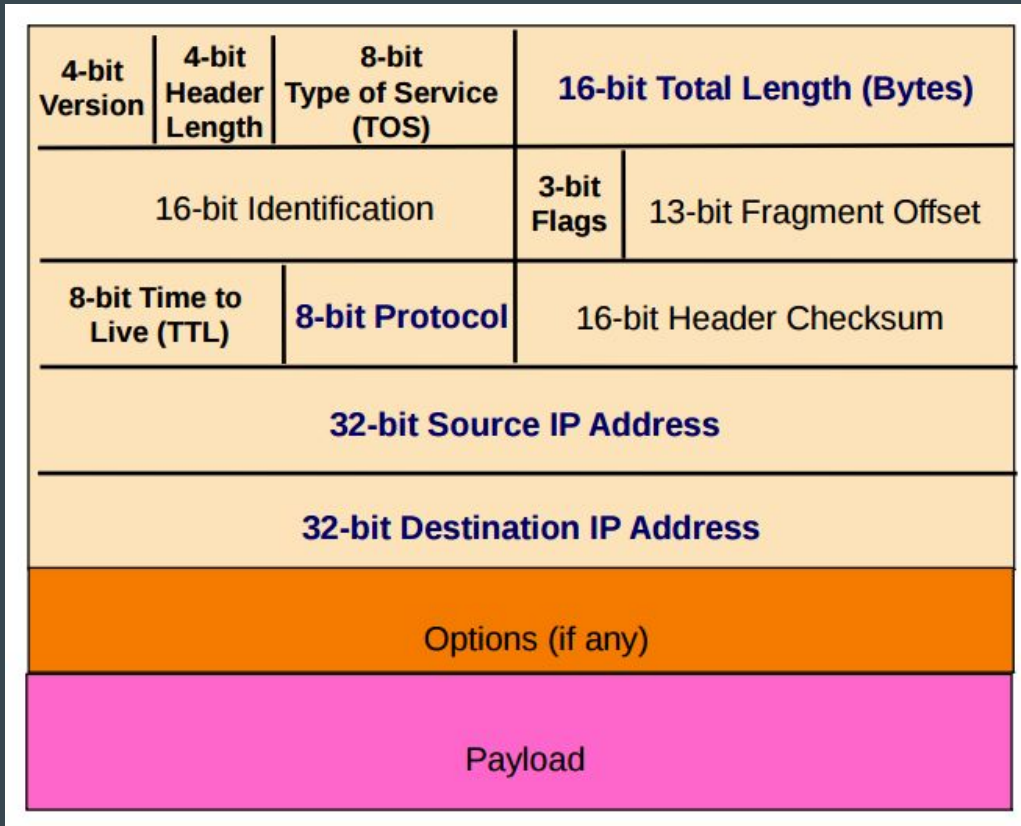
Network Layer

Transmitting digital packets, to
communicate with other computers



IP Packet

- Maximum size: 65,535 bytes
- May fragment (split) into multiple pieces if a router decides
- “Best effort” protocol
 - Packets may be lost
 - Packets may be corrupted
 - Packets may be out of order
 - ???
- Payload can be anything!



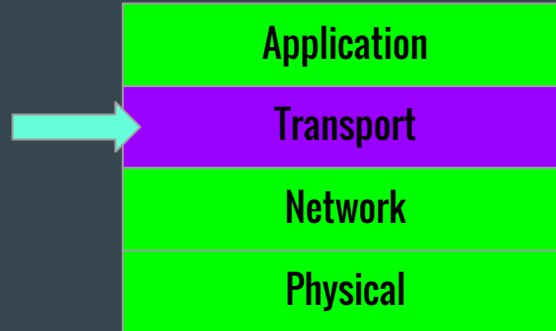
IP Packet Security

- Can set arbitrary source address
 - “Spoofing” - receiver has no idea who you are
 - Can send unwelcome return traffic to the spoof source address
- Can set arbitrary destination address
 - Enables “scanning” - brute force searching for hosts



Transport Layer

Transmitting digital packets, to communicate with other computer



Transport Protocols

UDP - Fast. Unreliable. Simple.

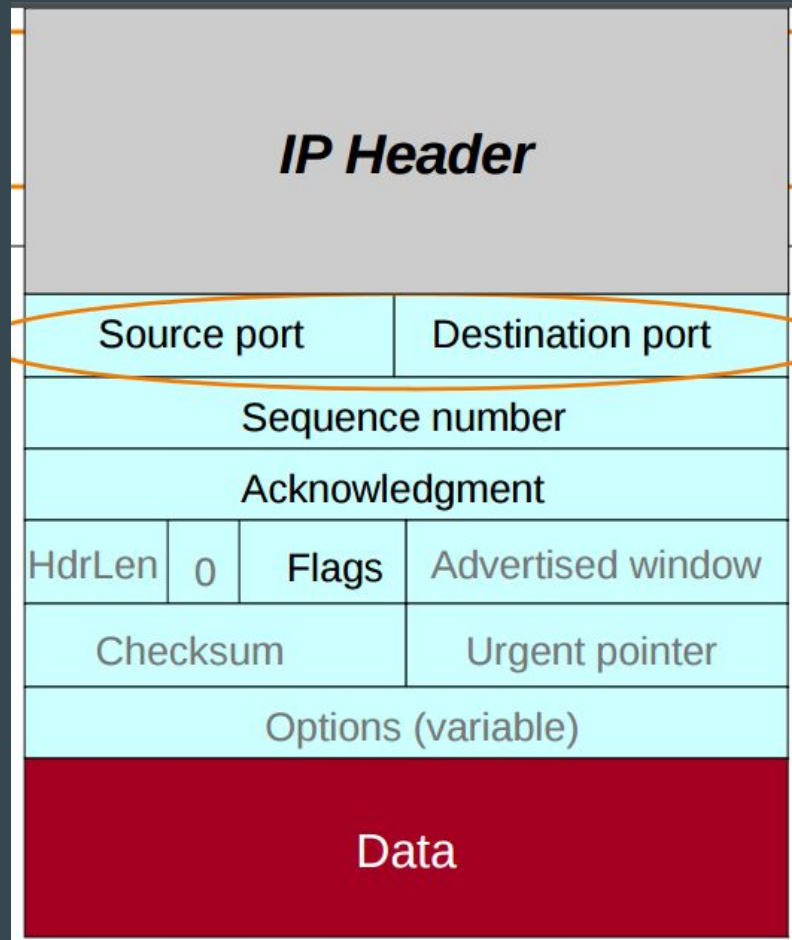


TCP - Slow. Reliable. Complex.



TCP Packet

- Reliable
 - In-order packets!
 - Packet-loss detection!
- Connections
- Contained in payload of an IP packet
- Payload can be anything!



TCP (Transportation Layer)

"Hi, I'd like to hear a TCP joke."

"Hello, would you like to hear a TCP joke?"

"Yes, I'd like to hear a TCP joke."

"OK, I'll tell you a TCP joke."

"Ok, I will hear a TCP joke."

"Are you ready to hear a TCP joke?"

"Yes, I am ready to hear a TCP joke."

... (it goes on)

TCP Security

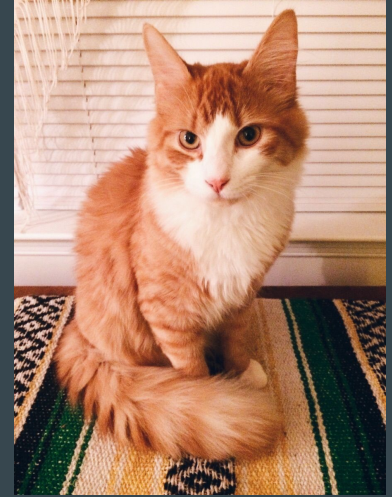
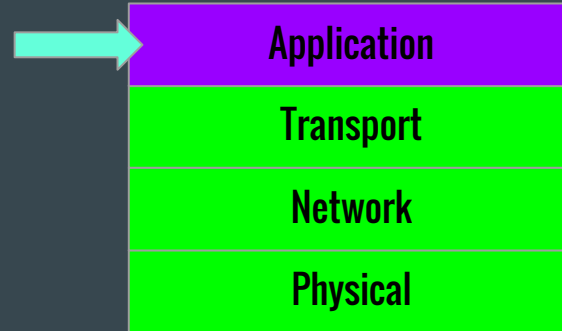
- The world is full of cheaters
 - Receiver can get data to come to them faster
- An attack simply needs to know the source and destination ports, and sequence numbers to disrupt your connection
- The same is true for injecting data, “session hijacking”

If an attacker sees (or guesses) your TCP data, then you're gonna have a bad time



Application Layer

Everything else we need, including cat pics



DNS (Application Layer)

People like to remember names, not IP addresses.

DNS (Domain Name System) is a distributed system to map names to IP addresses. DNS is at the application layer of the Internet stack.

- A single root server, and a set of top-level domain (TLD) servers
 - Websites are actually "google.com." <-- Note the `.` Try it for yourself!
 - The `.` is the root server.
 - The '.com' is the TLD.
- More local (i.e. faster) DNS servers get information from the TLDs.
 - And pass that information on to you.

DNS Packet/Protocol

- rfc 882, 883, 1034, 1035, 1035....
- DNS Spoofing:
 - All that tells a client they should accept a response is that the response has the same original **ident** field.
 - 16 bits of entropy, only 64K combinations, easily bruted.
 - Where can we get more entropy?
 - DNS uses UDP for transportation (recall layers)
 - UDP consists of a **source port**, destination port, a checksum, length, and the data
 - Randomize the source port that a client is using!
 - Still guessable. Easily manipulated with by a man-in-the-middle attack. But, best we got.

UDP
(transport)

DNS
(application)

Src Port	Dest Port
Checksum	Length

0 15 16 32

Ident	Flags
# of Questions	# of Answers
# of Authorities	# of Additional

Questions
Answers
Authority
Additional

HTTP

- Human readable
- **Requests** receive **Responses**
- Requests do “verbs”, GET, POST, DELETE, ...
- Responses send a status and response message
- Body data can be anything

GET /doc/test.html HTTP/1.1

Host: www.test101.com

Accept: image/gif, image/jpeg, */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0

Content-Length: 35

bookId=12345&author=Tan+Ah+Teck

Request Line

Request Headers

Request
Message
Header

A blank line separates header & body

Request Message Body

HTTP/1.1 200 OK

Date: Sun, 08 Feb xxxx 01:11:12 GMT

Server: Apache/1.3.29 (Win32)

Last-Modified: Sat, 07 Feb xxxx

ETag: "0-23-4024c3a5"

Accept-Ranges: bytes

Content-Length: 35

Connection: close

Content-Type: text/html

<h1>My Home page</h1>

Status Line

Response Headers

Response
Message
Header

A blank line separates header & body

Response Message Body

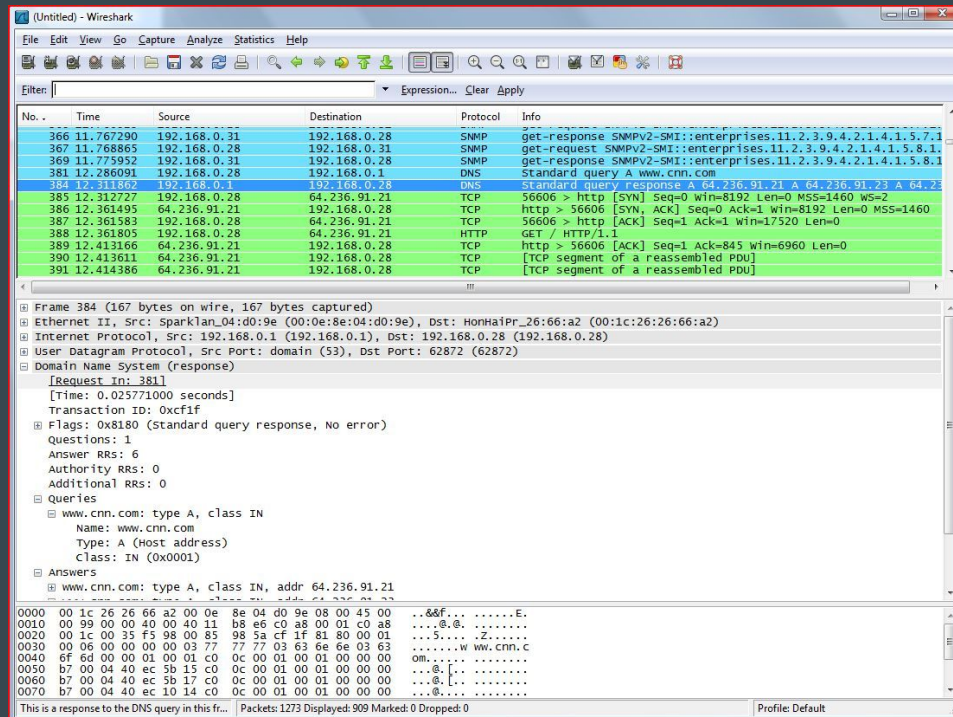
In Summary

- The Internet is a set of protocols, distributed networks, and layers
 - Physical (Ethernet)
 - Network (IP - “No guarantee.. I try my best”)
 - Transport (TCP, UDP)
 - Application (HTTP, FTP, Halo, BitTorrent, everything else)
- Network security is primarily focused on:
 - Confidentiality
 - Integrity
 - Availability
- A lot of the web is insecure if an attacker can view your data packets

H4CK3r T00LZ

Capture and Hack Data

- Wireshark
 - Record and modify all sorts of data
 - Not just web!
 - Industry standard, one of the best tools
 - Ton of fun, easy to use, modifiable
 - Give it a try yourself, and see what data your computer is sending and receiving
- aircrack-ng
 - Hack weak WiFi networks
 - Really does work



Scan the Internet/network

- nmap
 - Scan a network or machine for “info”
 - What’s running on it?
 - What version of things is it using?
 - Is it easily hackable?
- shodan
 - Global nmaping
 - Easily searchable

nmap cheatsheet:

<https://www.eugenekolo.com/blog/i-can-n/>

```
$ nmap eugenekolo.com
```

Nmap scan report for eugenekolo.com
(104.28.8.239)

Not shown: 996 filtered ports

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
8080/tcp	open	http-proxy
8443/tcp	open	https-alt

The screenshot shows the Shodan search engine interface with the search term 'bu.edu'. The results are categorized into 'TOP COUNTRIES', 'TOP SERVICES', 'TOP ORGANIZATIONS', and 'TOP PRODUCTS'. The 'TOP COUNTRIES' section shows a map of the United States with 214 results. The 'TOP SERVICES' section lists SMTP (80), HTTP (71), HTTPS (42), FTP (8), and 587 (6). The 'TOP ORGANIZATIONS' section lists Boston University (212), Massachusetts Institute of ... (1), and Ecommerce Corporation (1). The 'TOP PRODUCTS' section lists Apache httpd (106), Sendmail (68), Postfix smtpd (18), ProFTPD (5), and tnftp (3).

Search results for 'bu.edu' include:

- 128.197.10.17** (cs-mx1.bu.edu) - Boston University, Added on 2016-02-24 23:35:39 GMT, United States, Boston. Details: 220 cs-mx1.bu.edu ESMTP Postfix, 250-cs-mx1.bu.edu, 250-PIPELINING, 250-SIZE 50000000, 250-VRFY, 250-ETRN, 250-STARTTLS, 250-ENHANCEDSTATUSCODES, 250-8BITIME, 250 DSN.
- 128.197.228.172** (relay72.bu.edu) - Boston University, Added on 2016-02-23 19:44:38 GMT, United States, Boston. Details: 220 relay72.bu.edu ESMTP Sendmail 8.14.3/8.14.3; Tue, 23 Feb 2016, 250-relay72.bu.edu Hello xxx.xxx.xxx.xxx [xxx.xxx.xxx.xxx] (may b, 250-ENHANCEDSTATUSCODES, 250-8BITIME, 250-SIZE 104857600, 250-DSN, 250-ETRN, 250-DELIVERY, 250 HELP.
- 128.197.128.22** (iss3.bu.edu) - Boston University, Added on 2016-02-23 17:29:03 GMT, United States, Boston. Details: 220 iss3.bu.edu ESMTP Postfix, 250-iss3.bu.edu, 250-PIPELINING, 250-SIZE 128000000, 250-VRFY.

Play with HTTP

- Burpsuite
 - Intercept, modify, create, send, receive and more HTTP packets
- Postman
 - Create, send, and receive HTTP packets
 - More so for web development
- Firefox/Browser plugins
 - Modify packets
 - Chrome doesn't let you I believe?

Play with HTTP

Burp

Postman

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Size
http://0b7bd624bab7.mdseclabs.net	GET	/addressbook/32/		200	2
http://0b7bd624bab7.mdseclabs.net	POST	/addressbook/32/De...		200	3

addressbook

- admin
- app
- auth
- bank
- cclookup
- employees
- error
- feedback
- filestore
- search
- settings
- shop
- updates
- https://0b7bd624bab7.mdseclabs.net

http://0b7bd624bab7.mdseclabs.net/addressbook

- Add to scope
- Spider this branch
- Actively scan this branch
- Passively scan this branch
- Engagement tools
- Compare site maps
- Expand branch
- Expand requested items
- Delete branch
- Copy URLs in this branch
- Copy links in this branch
- Save selected items
- Site map help

1.1
bs.net
Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101
ion/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
q=0.5
accept-encoding: gzip, deflate
Proxy-Connection: keep-alive
Referer: http://0b7bd624bab7.mdseclabs.net/labs/lab.ashx?lab=7

Type a search term 0 matches

Builder API Library

No environment

Request Headers

GET https://echo.getpostman.com/headers

Params Send Save

Authorization Headers Body Pre-request Scripts Tests Generate Code Reset

my-sample-header Lorem ipsum dolor sit amet Presets

Body Cookies Headers Tests Status 200 OK Time 1828 ms

Pretty RAW Preview JSON Save Response

```
{
  "headers": {
    "Host": "echo.getpostman.com",
    "cache-control": "no-cache",
    "user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36",
    "my-sample-header": "Lorem ipsum dolor sit amet",
    "postman-token": "4438cec0-6944-0c19-25b4-6eaca04766f4",
    "accept": "*/json",
    "accept-encoding": "gzip, deflate, sdch",
    "accept-language": "en-US,en;q=0.8,en;q=0.6",
    "cookie": "sails.sid=s%3A2nQ5pqiDKCFN8kaZthw1ErUrhbg4GeOy.38Pu1zKagegi17NF3ob0Q1j0ZqMaGx1zSRs3PvtHByG4"
  }
}
```

Demos

Live @ 0xBU

Next week

Challenge1: `ssh tiny@pwnable.kr -p2222 (pw:guest)`

Challenge2: <http://web2014.picoctf.com/injection4/>

__libc_fini