

CTF на физтехе

часть 4 (web [part 1])

Basic knowledge

IP - Internet Protocol

IP-адрес - уникальный сетевой
адрес узла в компьютерной сети,
построенной по протоколу IP

IPv4 - 32 bit; IPv6 - 128 bit

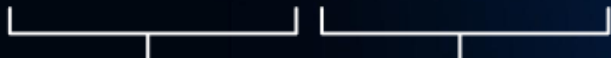
IPv4 address explain

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1



10101100 .00010000 .11111110 .00000001



One byte = Eight bits



Thirty-two bits (4 x 8), or 4 bytes

IP-packet

Октет	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Версия			IHL			Тип обслуживания								Длина пакета																	
4	Идентификатор															Флаги			Смещение фрагмента													
8	Время жизни (TTL)							Протокол								Контрольная сумма заголовка																
12	IP-адрес отправителя																															
16	IP-адрес получателя																															
20	Параметры (от 0 до 10-и 32-х битных слов)																															
	Данные																															

Establishing connection

- Подключаемся по IP-адресу
- Адрес один, программ много

Как достучаться до конкретной программы на компьютере?

Port

Port - номер от 1 до 65536.

Программа открывает порт 5555 =>
при подключении по \$IP:5555 мы
сможем общаться с программой

Standard ports: 21, 22, 53, 80, ...

Nmap

Утилита для сканирования сетей.
Позволяет получить список хостов,
портов и соответствующих служб.

```
$ nmap -sV -O host
```

```
$ nmap -sP ip/mask
```

TCP/IP stack

4	Прикладной уровень	HTTP, RTSP, FTP, DNS
3	Транспортный уровень	TCP, UDP, SCTP
2	Сетевой уровень	IP
1	Канальный уровень	Ethernet, IEEE 802.1

TCP

- установка соединения
- порты

handshake:

- SYN: host -> server
- SYN, ACK: server -> host
- ACK: host-> server

TCP

"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."

"Ok, I am about to send the TCP joke. It will last 10 seconds, it has two characters, it does not have a setting, it ends with a punchline."

"Ok, I am ready to get your TCP joke that will last 10 seconds, has two characters, does not have an explicit setting, and ends with a punchline."

"I'm sorry, your connection has timed out. Hello, would you like to hear a TCP joke?"

UDP

- тоже порты
- соединение не устанавливается => пакеты могут теряться или приходить в неправильном порядке

I'd tell you a UDP joke, but you might not get it.

Ping

- проверка доступности хоста
- ICMP протокол

`nmap -Pn host # or(-P0)`

Vuln example:

- ping of death
`ping -l 65510 example.com`
- SYN-flood

Netcat power

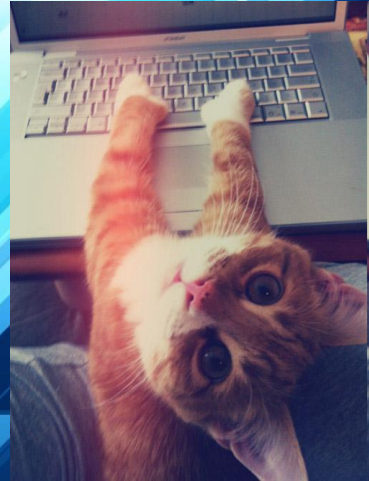
\$ nc host port # Connect TCP

\$ nc -u host port # Connect UDP

\$ nc -l host port # Listen port

\$ man 1 nc

netstat - check network connections



DNS

dom.example.org.



1. Какой ip у
www.k-max.name.

resolver

/etc/nsswitch.conf
/etc/resolv.conf

192.168.1.1

9. Забирай ip

2. Знаешь ip хоста
www.k-max.name. ?



192.168.1.1

Первичный
DNS-сервер
клиента

3. Знаешь ip хоста www.k-max.name. ?

4. Нет, но должен знать сервер 1

5. Знаешь ip хоста www.k-max.name. ?

6. Нет, но должен знать сервер 2

7. Знаешь ip хоста www.k-max.name. ?

8. Конечно, вот он.



Корневой
DNS-сервер



DNS-сервер
домена name.



DNS-сервер
домена k-max.name.

Любитель
экспериментов
www.k-max.name

DNS attacks examples

DNS Amplification

DNS Cache Poisoning

HTTP-request

<http://example.com/>

nc example.com 80

GET / HTTP/1.1

Host: example.com

Python requests

```
import requests  
r = requests.get("http://example.com/ex.php?p1=c1&p2=c2")  
print r.status_code  
print r.text
```

```
import requests  
payload = {"p1" : "c1", "p2" : "c2"}  
r = requests.post("http://example.com/ex.php",  
data=payload)  
print r.status_code  
print r.text
```

HTTP-headers

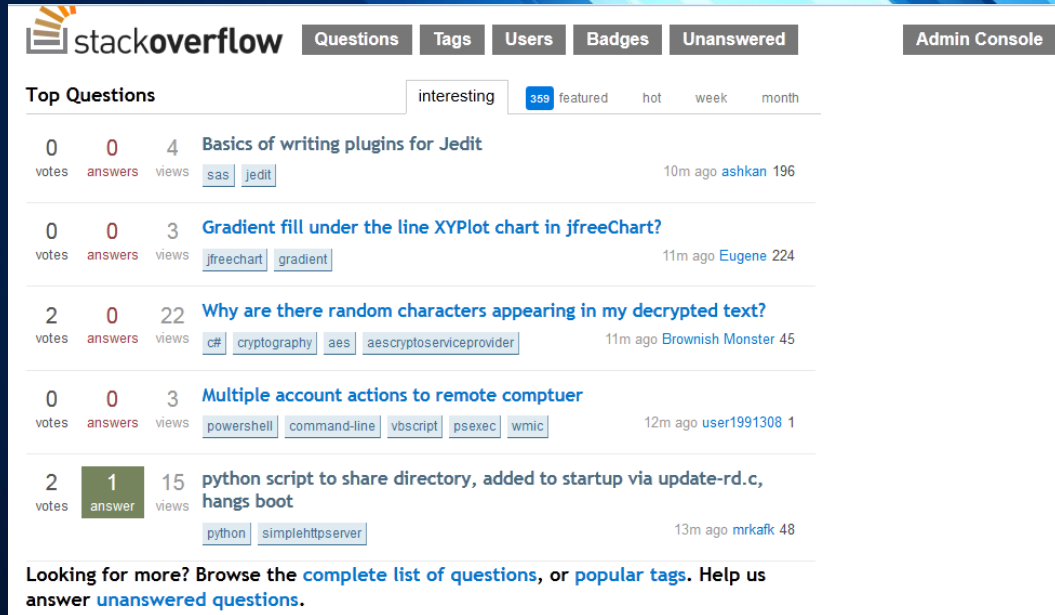
Server: Apache/2.2.11 (Win32) PHP/5.3.0
Last-Modified: Sat, 16 Jan 2010 21:16:42 GMT
Content-Type: text/plain; charset=windows-1251
Content-Language: ru

```
print requests.get("http://example.com").headers()  
$ curl -I example.com
```

HTTP header injection

Your IP is not authorised to use this function.

X-Forwarded-For: 127.0.0.1



The screenshot shows the Stack Overflow homepage with the 'Top Questions' section. The page has a dark blue header with the Stack Overflow logo and navigation links: Questions, Tags, Users, Badges, Unanswered, and Admin Console. Below the header, there's a filter bar for 'Top Questions' with tabs for 'interesting', '369 featured', 'hot', 'week', and 'month'. The main content area lists five questions with their respective statistics (votes, answers, views) and tags. The first question is 'Basics of writing plugins for Jedit' with 0 votes, 0 answers, and 4 views. The second is 'Gradient fill under the line XYPlot chart in jfreeChart?' with 0 votes, 0 answers, and 3 views. The third is 'Why are there random characters appearing in my decrypted text?' with 2 votes, 0 answers, and 22 views. The fourth is 'Multiple account actions to remote computer' with 0 votes, 0 answers, and 3 views. The fifth is 'python script to share directory, added to startup via update-rd.c, hangs boot' with 2 votes, 1 answer, and 15 views. At the bottom, there's a link to 'Browse the complete list of questions, or popular tags. Help us answer unanswered questions.'

votes	answers	views	question	tags	time ago	author	score
0	0	4	Basics of writing plugins for Jedit	jas	10m ago	ashkan	196
0	0	3	Gradient fill under the line XYPlot chart in jfreeChart?	jfreechart	11m ago	Eugene	224
2	0	22	Why are there random characters appearing in my decrypted text?	c#	11m ago	Brownish Monster	45
0	0	3	Multiple account actions to remote computer	powershell	12m ago	user1991308	1
2	1	15	python script to share directory, added to startup via update-rd.c, hangs boot	python	13m ago	mrkafk	48

Looking for more? Browse the [complete list of questions](#), or [popular tags](#). Help us answer [unanswered questions](#).

URL encoding

\$ = %24

& = %26

/ = %2F

...

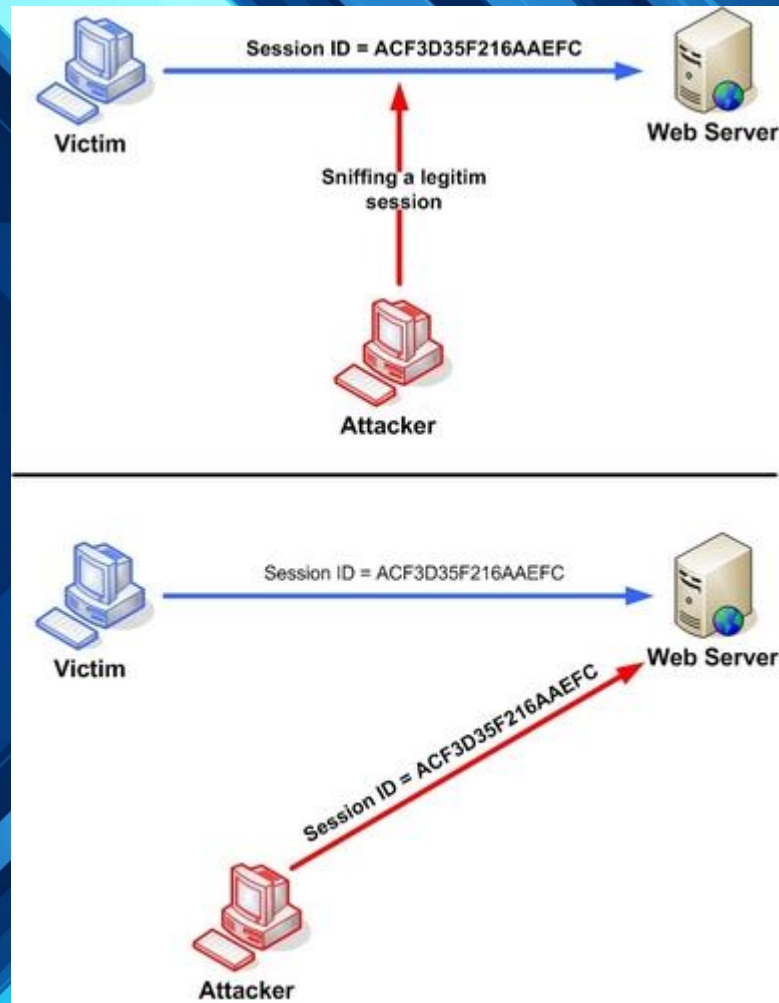
<http://www.url-encode-decode.com>

Cookies

- Web-server -> cookie -> client
- аутентификация пользователя;
- хранение персональных предпочтений и настроек пользователя;
- отслеживание состояния сеанса [en] доступа пользователя;
- ведение статистики о пользователях.



Session hijacking attack



Capturing traffic

Capture

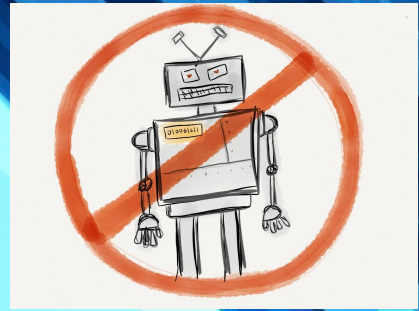
- wireshark
- tcpdump
- tshark

Analyze

- wireshark
- tshark
- network miner

<http://bit.ly/1vCVU1t>

Robots exclusion standard



- google cache => секретная инфа может быть сохранена в кэше гугла
- robots.txt - файл ограничения доступа к содержимому роботам на http-сервере
- Файл всегда лежит в корне домена (т.е. <http://google.com/robots.txt>)

