Desmitificando la caja negra

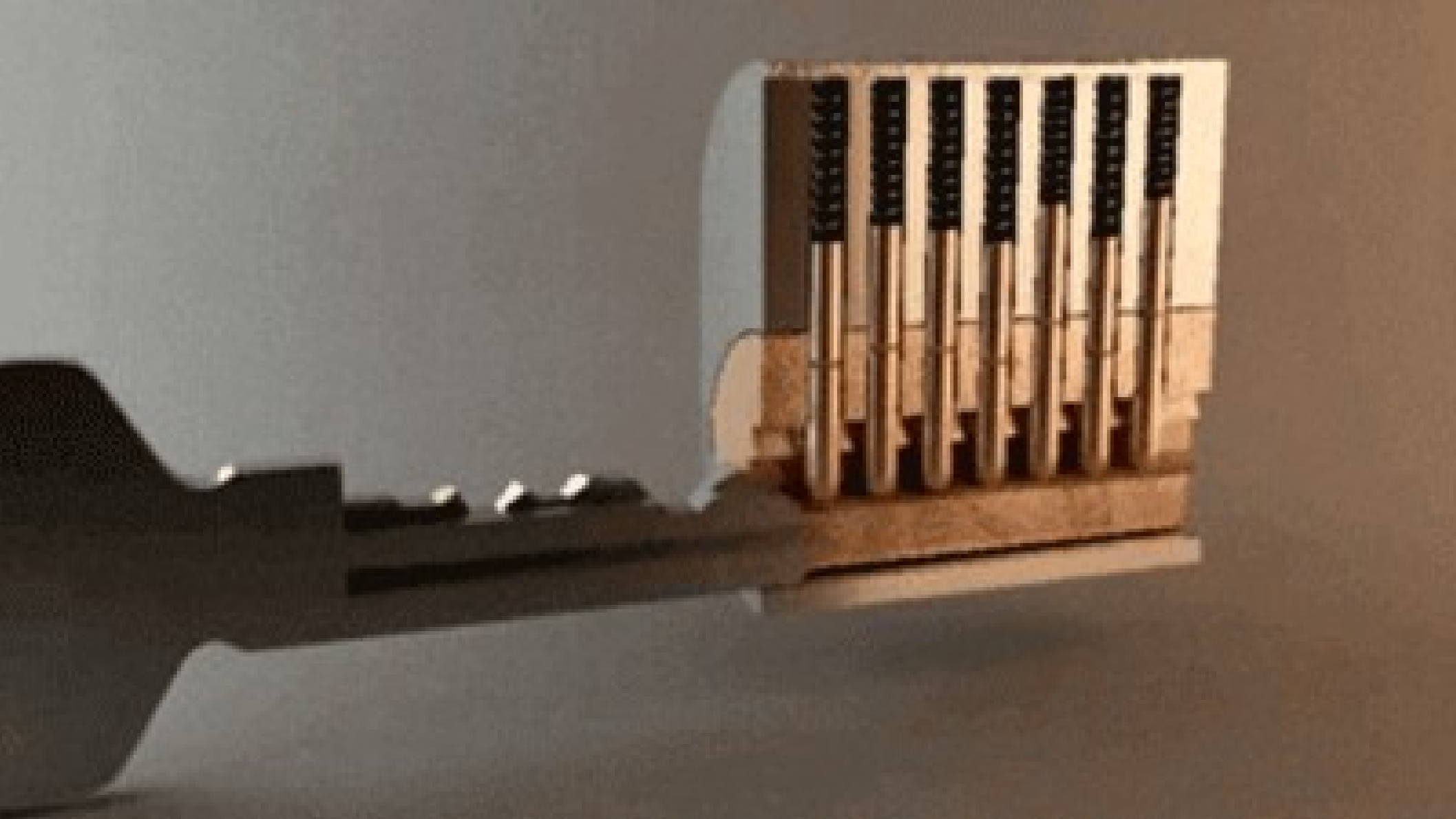
Quién soy?

- Especialista en Ciberseguridad
- Trabajo como Miembro del Equipo de respuesta de Incidentes de ENTEL
- Investigador de Seguridad
- @MDiazCL

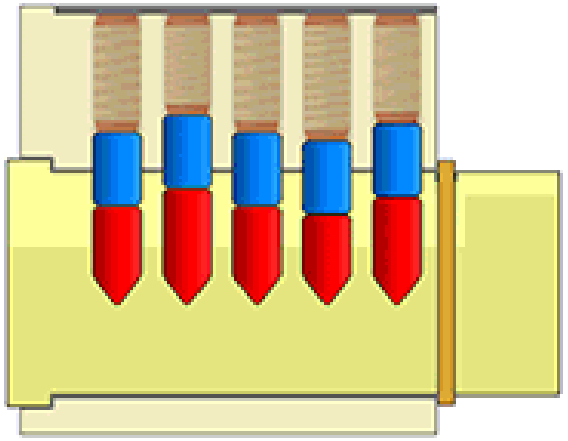
Introducción

- Soy curioso, desde ~~chico~~ joven
- Siempre me interesó empujar los límites de las cosas y hasta dónde pueden llegar
- Cuando uno entiende como funcionan las cosas, puedes alterar ese entendimiento y adaptarlo para lo que tú quieras.

¿Cómo funciona?



Así nació
lockpicking



Hablemos de hacking (computacional)

- Herramientas automáticas hay muchas (yey!)
- ScriptKiddies!
- Entender es la clave, si no somos monitos que nos creemos hackers.

...vamos a ver como funcionan

Revisemos algunas técnicas y herramientas

(pasamos a las slides negras)

Nmap descripción

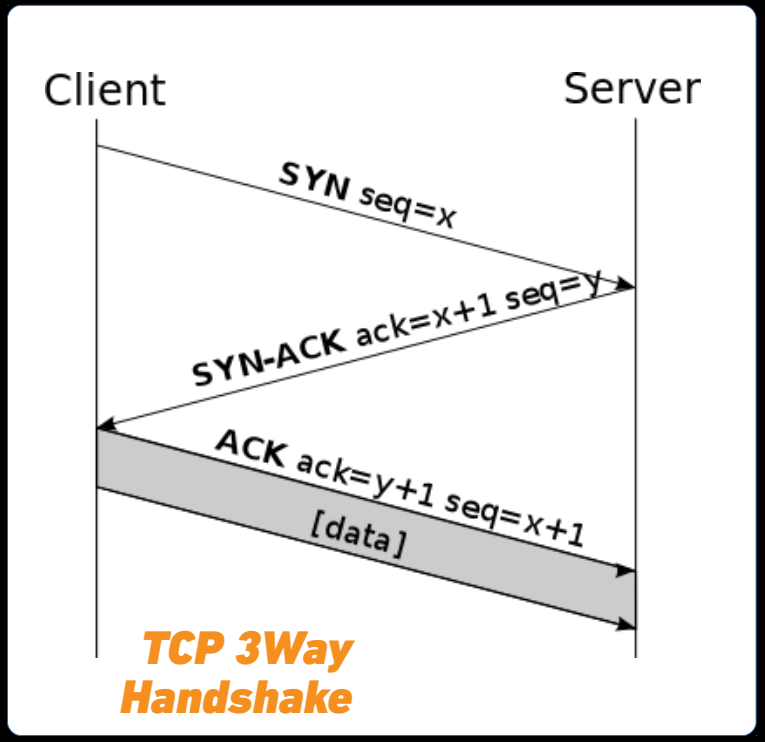
Características

- Escáner de puertos abiertos
- Scripts de identificación (aux)
- Mapeador de red (tracert)

- Útil para muchos escenarios! Sobretodo para comenzar

```
# nmap -A -T4 scanme.nmap.org 207.68.200.30

Starting Nmap 5.00 ( http://nmap.org ) at 2009-07-13 16:22 PDT
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 994 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
|  ssh-hostkey: 1024 03:5f:d3:9d:95:74:8a:d0:8d:70:17:9a:bf:93:84:13 (DSA)
|_ 2048 fa:af:76:4c:b0:f4:4b:83:a4:6e:70:9f:a1:ec:51:0c (RSA)
53/tcp    open   domain  ISC BIND 9.3.4
70/tcp    closed gopher
80/tcp    open   http    Apache httpd 2.2.2 ((Fedora))
|_ html-title: Go ahead and ScanMe!
113/tcp   closed auth
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)

Interesting ports on 207.68.200.30:
Not shown: 991 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.0.6001
88/tcp    open  kerberos-sec Microsoft Windows kerberos-sec
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds Microsoft Windows 2003 microsoft-ds
464/tcp   open  kpasswd5?
49158/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49175/tcp open  msrpc        Microsoft Windows RPC
Running: Microsoft Windows 2008|Vista

Host script results:
|  smb-os-discovery: Windows                                  nterprise 6001 Service Pack 1
|  LAN Manager: Windows                                       6.0
|  Name: MSAPPLELAB\AP
|_ System time: 200
|  nbstat: NetBIO                                             wn>, NetBIOS MAC:
00:1a:a0:9a:a3:90
|  Name: APPLELAB2K8<00
|_ Name: MSAPPLELAB<00>                                       ive>

TRACEROUTE (using port 135/tcp)
HOP RTT    ADDRESS
[Cut first 8 lines for
9   36.88  ge-10-0.hsa1                                       05.6)
10  36.61  unknown.Leve
11  41.21  207.68.200.3

Nmap done: 2 IP addresses (2 hosts up) scanned in 120.26 seconds
```

Nmap *funcionamiento*



- ***Concepto:*** *Puerto, dirección IP, flujo*
- ***Analogía:*** *Patio de comidas*

- *nmap -sS -vv <host>*
- *nmap -sS -vv -O <host>*
- *nmap -sS -vv -p <ports> <host>*
- *nmap -sS --script <nse> <host>*

```
    29 12.542957576  192.168.1.158    64.233.186.94    TCP      74 56380 → 80 [SYN] Seq=0 Win=29200
    30 12.552121427  64.233.186.94    192.168.1.158    TCP      74 80 → 56380 [SYN, ACK] Seq=0 Ack=
    31 12.552232765  192.168.1.158    64.233.186.94    TCP      66 56380 → 80 [ACK] Seq=1 Ack=1 Win
```

Nmap *demo*

SQLMap descripción

Características

- *Detector de SQLInjections*
- *Capaz de detectar y explotar*
- *De facil uso*
- *Letal contra sitios web vulnerables, arma de doble filo para los niños.*

```
[15:24:09] [INFO] the back-end DBMS
web application technology: Nginx, P
back-end DBMS: MySQL 5.0
[15:24:09] [INFO] fetching tables fo
[15:24:10] [INFO] the SQL query used
[15:24:10] [INFO] retrieved: artists
[15:24:11] [INFO] retrieved: carts
[15:24:11] [INFO] retrieved: categ
[15:24:12] [INFO] retrieved: feature
[15:24:13] [INFO] retrieved: guestbo
[15:24:13] [INFO] retrieved: picture
[15:24:17] [INFO] retrieved: product
[15:24:21] [INFO] retrieved: users
Database: acuart
[8 tables]
+----------+
| artists  |
| carts    |
| ca       |
| fe       |
| gu       |
| pi       |
| pr       |
| users    |
+----------+
```

SQLMap *funcionamiento*

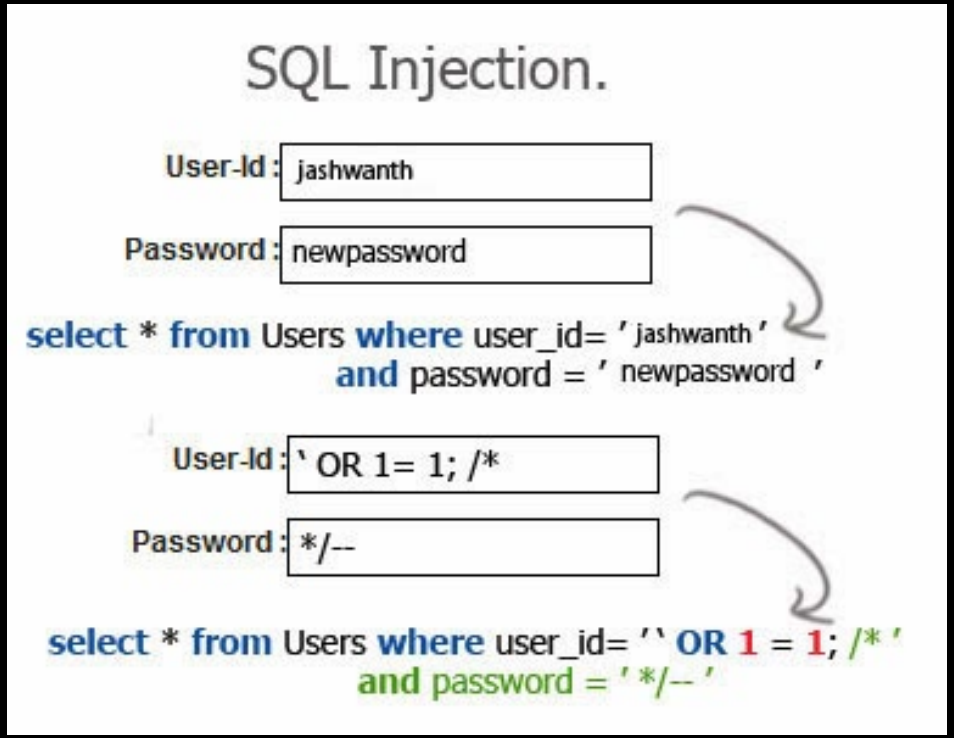
- ***Concepto:*** *URL, QuerySQL,*
- ***Analogía:*** *Patio de comidas*

- *sqlmap -u “<test_url”>*
- *sqlmap -u “<test_url”> --data=”<post_data”>*

```
String SQLQuery ="SELECT Username, Password
 FROM users WHERE Username='" + Username +
   "' AND Password='" + Password +"'";

Statement stmt = connection.oreateStaement();
ResultSet rs = stmt.executeQuery(SQLQuery);
while (rs.next()) { … }
```

SQLMap *funcionamiento*

- ***Concepto:*** *URL, QuerySQL,*
- ***Analogía:*** *Conversación*



- *sqlmap -u "<test_url">*
- *sqlmap -u "<test_url">*
  --data="<post_data">

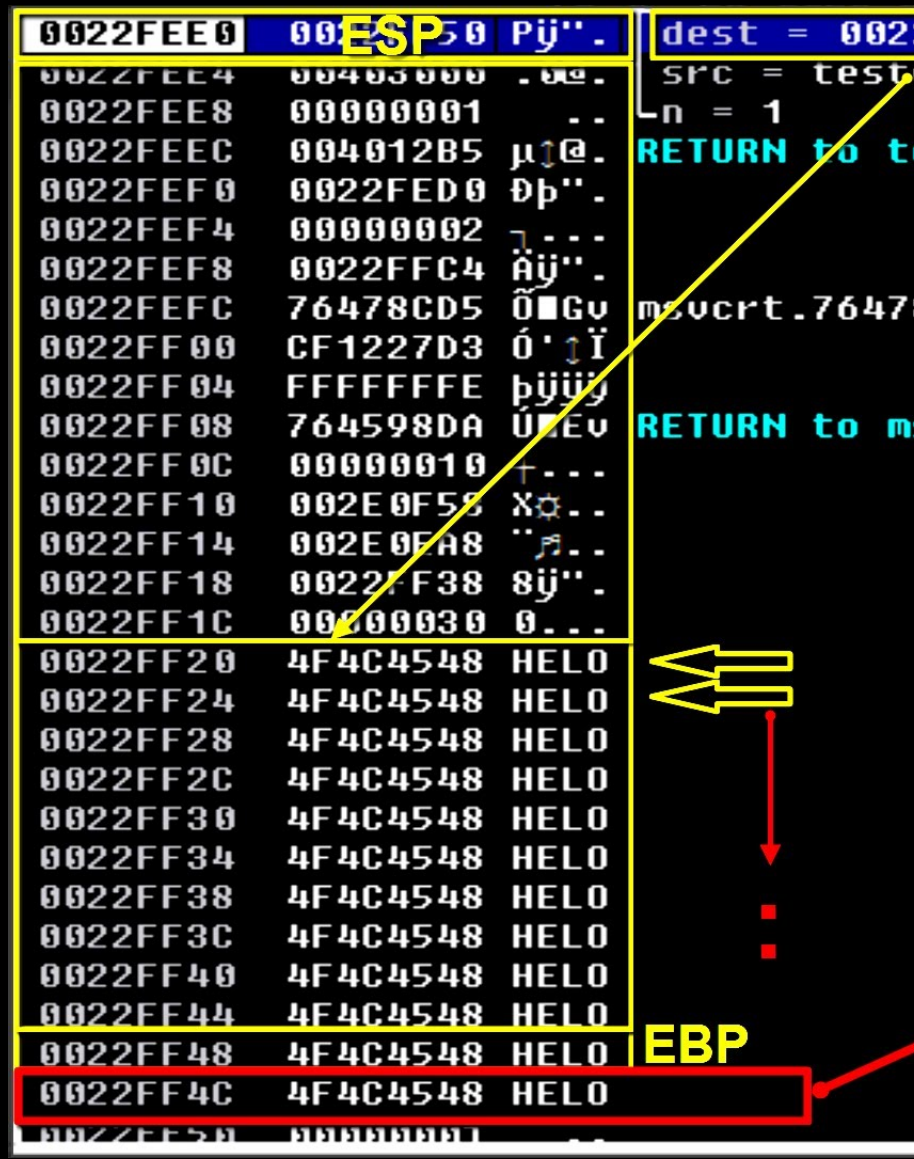
```
String SQLQuery ="SELECT Username, Password
 FROM users WHERE Username='" + Username +
  "' AND Password='" + Password +"'";

Statement stmt = connection.oreateStaement();
ResultSet rs = stmt.executeQuery(SQLQuery);
while (rs.next()) { … }
```

SQLMap *demo*

BufferOverflow *descripción*

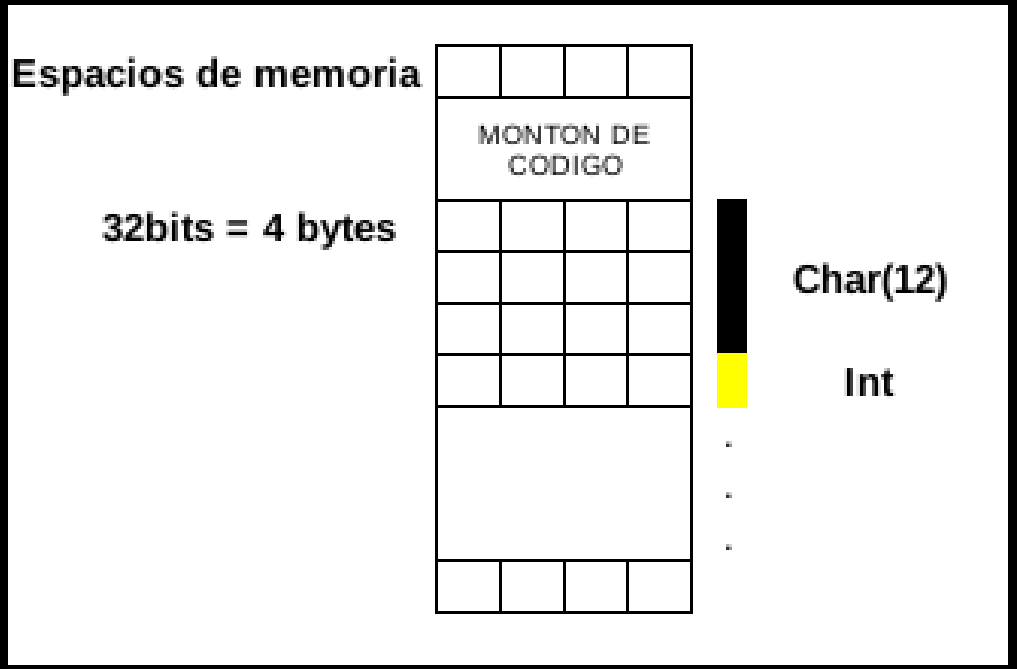
Características

- *Carga código en la memoria*
- *Es una forma de explotación antigua, pero muy utilizada*
- *Potente ataque cuando se encuentra algún software vulnerable*



BufferOverflow

```
int main (int argc, char **argv)
{
   Char c[12];
   strcpy(argv[1]);
   Int x = 1
   return 0;
}
```



BufferOverflow demo

Invitación a seguir estudiando
Algunos temas para ustedes

- Intercambio de llaves Diffie-Hellman
- Firewall, IDS/IPS
- Protocolos: HTTP, SSH, TELNET, DNS, etc...
- Logs de Datos (ELK)
- Full-Stack (Front-end, Back-end)
- Networking
- CTFs!
- Reversing de código
- Threat Hunting

Gracias por su atención!

(los gif son lo mejor)