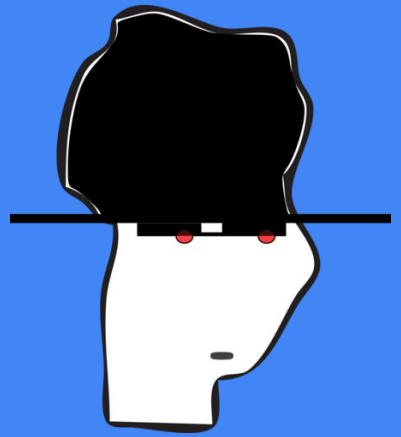
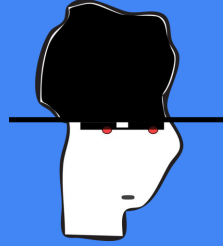


Introducción

Seguridad Ofensiva

UNC Universidad Nacional de Córdoba
FAMAF Facultad de Matemática, Astronomía, Física y Computación

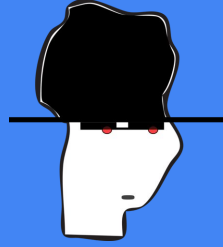
Temas



- Autenticación
- Criptografía básica
- Seguridad Web
- Tests de Intrusión / Pentesting
- ~~Reversing Network Protocols~~

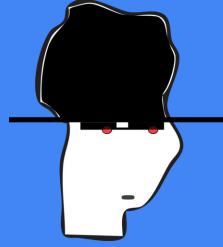
- Análisis de Binarios
- Corrupción de Memoria
- Mobile? (*)
- Forensia ? (*)
- Blockchain? (*)
- Threat Modeling

Condiciones



(L) ibre
(R) egular
(P) romocional
(O) yente : □

Disclaimer



- Voy a mezclar espagnol / inglés todo el tiempo.
- Voy a escribir sin acentos y sin ‘¿’

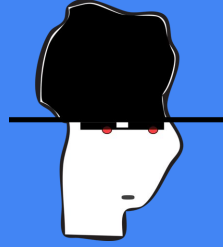
- No lo sabemos todo.

Seguridad

Porqué estudiar Seguridad Ofensiva?

CTF TIME

Porqué estudiar Seguridad Ofensiva?



Well-designed mitigation strategies need routine security tests.

The best tests simulate the techniques and methods of an intruder.

By encouraging students to use the same tools, techniques, and mindset as a hacker, we level the playing field for defenders.

Offense is the best defense.

10 COOLEST JOBS IN CYBERSECURITY

WHY THEY MAKE A DIFFERENCE AND HOW TO QUALIFY FOR THEM

Initial Jobs With Lots of Advancement Opportunities

1 DIGITAL FORENSIC ANALYST; INVESTIGATOR

"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."

You are the detective in the world of cybersecurity – searching computers and networks for evidence in the wake of an incident.

2 PENETRATION TESTER FOR SYSTEMS AND NETWORKS

"Be a hacker, but do it legally and get paid a lot of money!"

You look for security vulnerabilities in target systems and networks to help enterprises improvetheir security.

3 APPLICATION PEN TESTER

"We desperately need more of this, application security has been such a black hole for so long."

You're a programming/security wizard; test applications before deployment so they don't present opportunities for intruders.

4 SECURITY OPERATIONS CENTER (SOC) ANALYST

"The fire ranger. Catch the initial blaze, or there goes the forest."

With an eye for detail and anomalies, you see things most others miss. Active prevention, active detection, active monitoring, active response.

5 CYBER DEFENDER; SECURITY ENGINEER (ENTERPRISE AND ICS)

"A leg up on your system admin and engineering buddies; talk shop with them but you are saving the world from the bad guys, too."

Implement/tune firewalls, IPS/IDS, patching, admin. rights, monitor-ing, applicatien white listing, more

More Advanced Jobs – Open After A Few Years of Great Performance and Specialized Training

6 HUNTER; INCIDENT RESPONDER

"The secret agent of geekdom. You walk in and say 'OK I'll take it from here.'"

While everyone else is running around shouting "the system's dead," you have the sense and skills to rationally figure out why.

7 SECURITY ARCHITECT

"You get to design the solution, and not just for the perimeter."

You are very creative, on top of the game technically and the business; you design and build defensible systems and are part of a team of very adept people.

8 SECURITY SAVVY SOFTWARE DEVELOPER

"Coolest software developers"

You protect the whole dev team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.

9 MALWARE ANALYST/ REVERSE ENGINEER

"The technical elite! Only go here if you have been called. You know who you are."

Look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, what it is trying to do or has done.

10 TECHNICAL DIRECTOR/CISO

"Making decisions; making things happen. That's coolness."

Top of the tech ladder. Strategic thinking; hands-on involvement in solution design/deployment; holds the keys to tech infrastructure and ability to contribute and influence

1 CYBER FAST TRACK

"I loved Cyber-Start challenges - the coolest game I ever played."

"Taught me a lot; proved cyber-security wasn't too hard to learn."

"The most fun I have had learning."

DISCOVER IF YOU HAVE THE APTITUDE

CYBERSTART: THE GAME

- No need for cyber or IT experience
- More than 250 fun challenges protecting "real-world" bases
- Available completely online Everything you need is in the on line Field Manual and hints.
- 19 U.S. Governors launched statewide programs for their students.

SEE MORE AT CYBERSTART.US

2

CATEGORY/TOPIC	MODULES
Computer Hardware/Data	8
Linux and Windows	7
Networking	6
Programming	6
Common Attacks & Security	10
Others (Kali, Google, etc)	11

"We hire NYU cybersecurity grads only if they have hands-on mastery of these foundations" (CISO, multi $billion Silicon Valley tech leader)

MASTER THE FOUNDATIONS

CYBERSTART: ESSENTIALS

- Core technologies: how they work and are attacked
- On-line, hands-on immersion training, in 46 modules
- Progress at your own pace. Quizzes and tests on each module
- National exam to reach silver or gold levels

3 EMPLOYER INTERVIEWS BEFORE ACCEPTANCE

GET SKILLS EMPLOYERS NEED AND A COOL JOB!

- Open & Veterans' & Women's Academies
- Three SANS immersion courses and three high value GIAC certifications
- 90% job placement in 6 months
- Also available as Certificate in Applied Cyber Security (CACS) at SANS.edu and other accredited colleges and universities

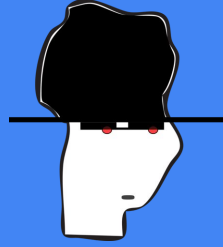
SEE MORE AT USCYBERACADEMY.SANS.EDU

"Completing the SANS Vet Success Academy not only influenced my career plans, it defined them, opening doors that were inaccessible to me otherwise. In fact, being selected into the program was a "hitting the jackpot" moment for me."

Ed Russell, USAF (ret), NTT Security

UNITED STATES CYBER ACADEMY

Porqué estudiar Seguridad Ofensiva?



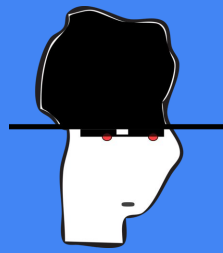
Propiedades (deseables) del Software

- Functionality
- Reliability
- Usability
- Efficiency
- Maintainability
- Portability
  (ISO/IEC 25010:2011)

Security Property	Meaning
Confidentiality	Information is only available to the people intended to use or see it.
Integrity	Information is changed only in appropriate ways by the people authorized to change it.
Availability	Apps and services are ready when needed and perform acceptably.
Authentication	A person's identity is determined before access is granted if anonymous people are not allowed.
Authorization	People are allowed or denied access to the app or app resources.
Nonrepudiation	A person cannot perform an action and then later deny performing the action.

Source: Mike Gualtieri, Principal Analyst, Forrester Research

Cuestiones Éticas & Legales

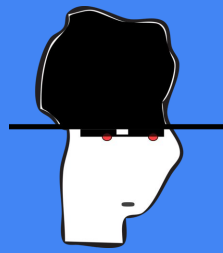


https://delitosinformaticos.com/legislacion/argentina.shtml

http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

"Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido."

Cuestiones Éticas & Legales

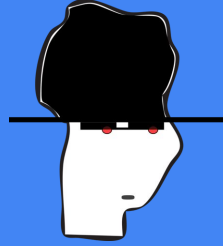


El 22 de noviembre el poder legislativo aprobó el proyecto de ley de adhesión de Argentina al Convenio de Budapest, un convenio internacional sobre ciberdelito.

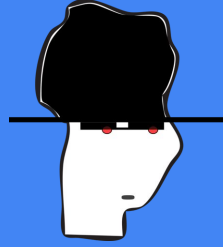
El Convenio sobre Cibercriminalidad o Convenio de Budapest fue creado en el año 2001 en la ciudad que le da nombre con el fin de homogeneizar las definiciones sobre los delitos informáticos y establecer las bases para la cooperación internacional respecto de temas relativos a la ciberseguridad.

La adhesión a este Convenio de carácter supranacional, ya cuenta con la aprobación de la Cámara de Senadores y la Cámara de Diputados. El mismo le dará a la Justicia argentina las herramientas necesarias para investigar este tipo de infracciones, por ejemplo estafas, pornografía infantil y cuestiones relativas a la propiedad intelectual. Hasta el momento el acuerdo cuenta con más de 50 países miembros.

~Breach Timeline



[World's Biggest Data Breaches & Hacks — Information is Beautiful]



Un poco de historia

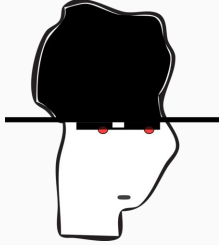
- Primeros “ataques” a telegrafía (1903), telefonía,
- Enigma (1932)
- Sistema de Tarjetas perforadas usadas para localizar judios? (1943)
- Theory and Organization of Complicated Automata. (1949) (J.V.Neuman, Malware Theory)
- Phreaking (70’s)
- …
- Ezines (80’s) (cDc , phrack …)
- The hacker’s handbook (85)
- Christmas Tree Exec “worm” (87)
- Se crea DARPA (88)
- + virus (90)
- 1st DEFCON (93)
- Movies Hackers and The Net (95)

3 Casos de Ejemplo

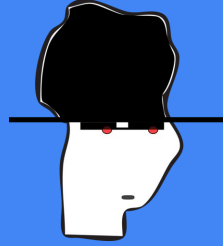
Stuxnet

Shellshock

WannaCry



Stuxnet

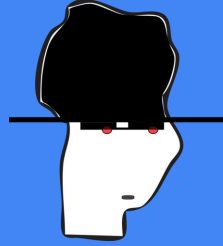


Detectado por primera vez: investigadores VirusBlockAda (17/6/2010)
Propagación: USB
Tecnología afectada: Windows, SCADA

- Equipo industrial atacado (Centrifugas en una planta de enriquecimiento de combustible)
  - Fallas imperceptibles
  - Objetivo específico: Propagarse hasta alcanzar la computadora basada Windows que se conecta con el equipo particular para sabotaje.

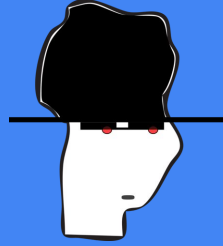
- Hay pruebas de que el ataque fue exitoso
- Representó un adelanto significativo en el desarrollo de software malicioso
- Mostró que varias suposiciones comunes acerca del área no son siempre válidas. (?)

Stuxnet



lógicos programables) —hardware para controlar un componente físico. Para programar el PLC, el administrador lo conecta a una computadora Windows estándar. Entonces por lo regular el PLC se desconecta de la computadora cuando está listo para usarse. Por ejemplo, si el administrador desea que las centrífugas funcionen a una velocidad más rápida, conecta el PLC a la computadora Windows, instala un software que se comunica con el PLC y sube las nuevas instrucciones. Supongamos que Stuxnet ha infectado la computadora conectada al PLC. El malware básicamente lleva a cabo un "ataque mediante intermediario" en contra del sistema. El administrador intenta enviar los comandos al PLC. Stuxnet los intercepta y envía sus propias instrucciones. Sin embargo, el software somete un informe falso a la computadora Windows que las instrucciones originales fueron cargadas. Al someter un informe falso, Stuxnet se esconde, convirtiéndolo más difícil de detectar.

Stuxnet fue diseñado para atacar los PLC controlados por el software Step 7 de Siemens.[14] Ade-

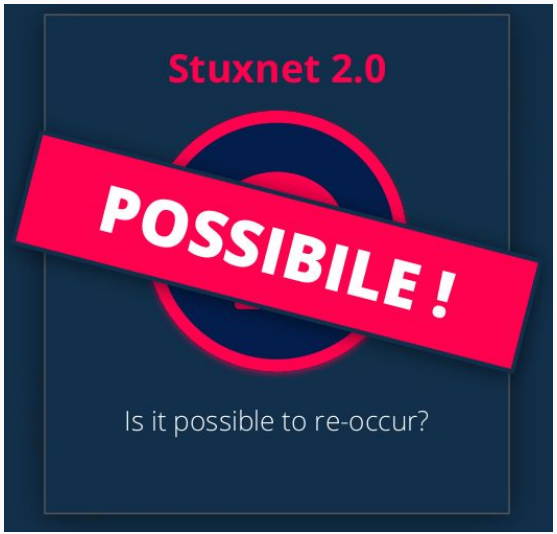


Stuxnet

5 vulnerabilidades:

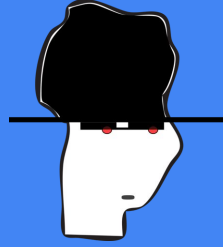
- 3 RCE (MS10-46[1] LNK, MS06-40[2] RPC, MS10-61[5] Spooler)
- 2 LPE (MS10-092[3] Task Scheduler, MS10-073[4] Kernel Drv)

DEFCON 28 Talk



“Now, over 22 million pieces of malware use that blueprint to attack organizations and states...”
-regdox.com

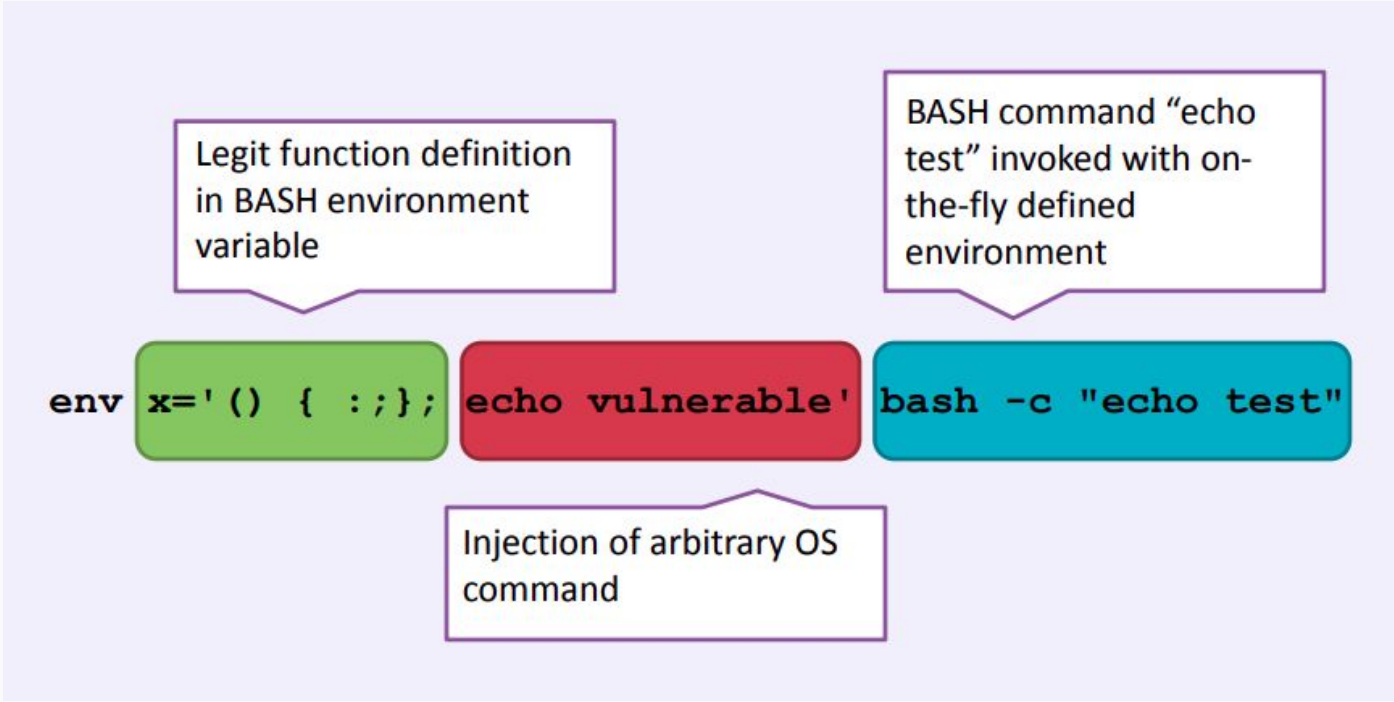
Shellshock (2014) (ver)



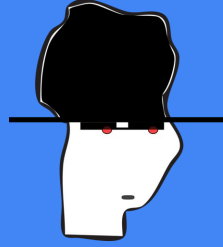
- Shellshock is effectively a Remote Command Execution vulnerability in BASH

- The vulnerability relies in the fact that BASH incorrectly executes trailing commands when it imports a function definition stored into an environment variable
- Vulnerable since version 1.03 of Bash released in **September 1989**

Shellshock (2014) (ver)



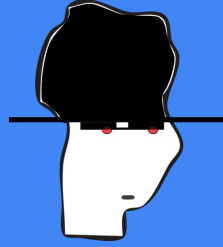
Shellshock (2014) (ver)



- RCE via Apache with mod_cgi, CGI Scripts, Python, Perl
- RCE on DHCP clients using Hostile DHCP Server
- OpenSSH RCE/Privilege escalation
- ....

WannaCry & EternalBlue(2017)

WannaCry & EternalBlue(2017)



EB

- Cyberattack exploit developed by the U.S. National Security Agency (NSA).
- leaked by the Shadow Brokers hacker group
- Affects SMB protocol
- Ejecucion de codigo.

WC

- Ransomware attack
- Impacto: Mundial
- Target: encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.

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

- Cormac Herley -