

# Introducción

Seguridad Ofensiva  
02/02/2024

# Algunos anuncios

- Las clases se impartirán por Google Meet
- Los clases de los miércoles se cambian a los martes
- Las clases de ayudantía quedan Mi/Ju (Fundamentos)
- 55 + 3 alumnos oficialmente inscritos
- Seminario profesionalizante

# Seguridad de la Información

- Seguridad Informática
- Ciberseguridad
- Seguridad en Cómputo
- Seguridad de las Computadoras
- Cyber
- Seguridad

Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

# Triada de la seguridad

Propiedades básicas de la información que buscamos procurar y que todo adversario buscará afectar. (CIA)

- Confidencialidad
- Integridad
- Disponibilidad (Availability)



# Ejemplo “práctico”

- Inyección SQL (permite manipular consultas a la base de datos a partir de una aplicación vulnerable. [EJEMPLO](#))
- [CVE-2023-3047](#)
- C:H
- I:H
- A:H



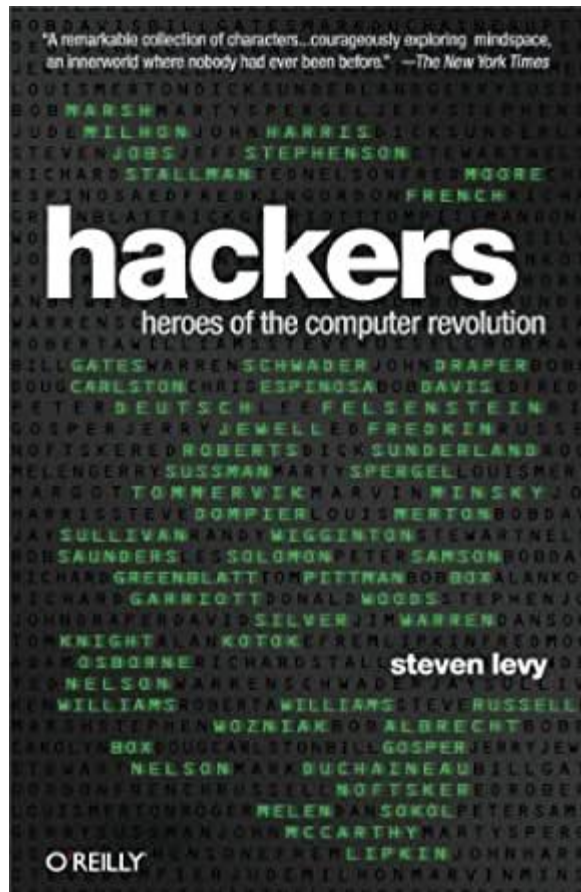
# El comienzo.

- 1950s



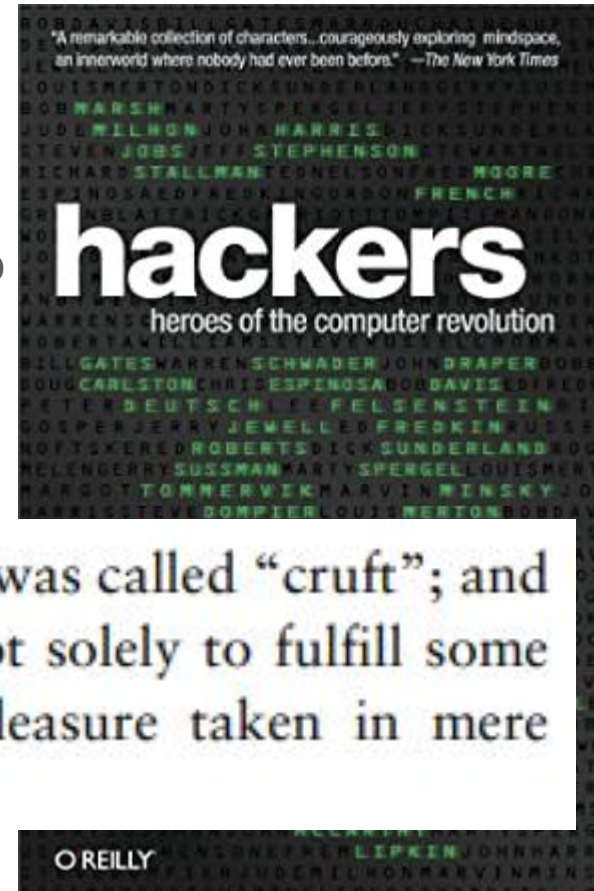
# Hackers

- 1984
- Compendio de personas pioneras en el cómputo
  - Historia
  - Ideologías
- Inteligencia Artificial - Marvin Minsky
- Etica hacker
  - Hack



# Hackers

- 1984
- Compendio de personas pioneras en el cómputo
  - Historia
  - Ideologías
- Inteligencia Artificial - Marvin Minsky
- Ética hacker



studying for courses was a “tool”; garbage was called “cruft”; and a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure taken in mere involvement, was called a “hack.”

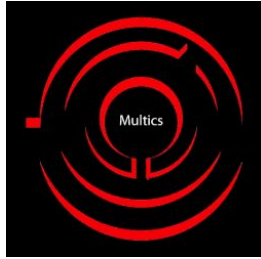


# The hacker's ethics...

- Access to computers - and anything which might teach you one thing about the way the world works - should be unlimited and total. Always yield to the Hands-On imperative!
- All information should be free.
- Mistrust authority - promote decentralization.
- **Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.**
- You can create art and beauty on a computer.
- Computers can change your life for the better.

# ¿Y la seguridad?

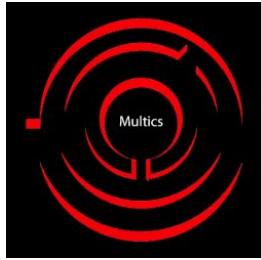
- Multics. 1964 1970 (MIT, General Electric & Bell Labs)



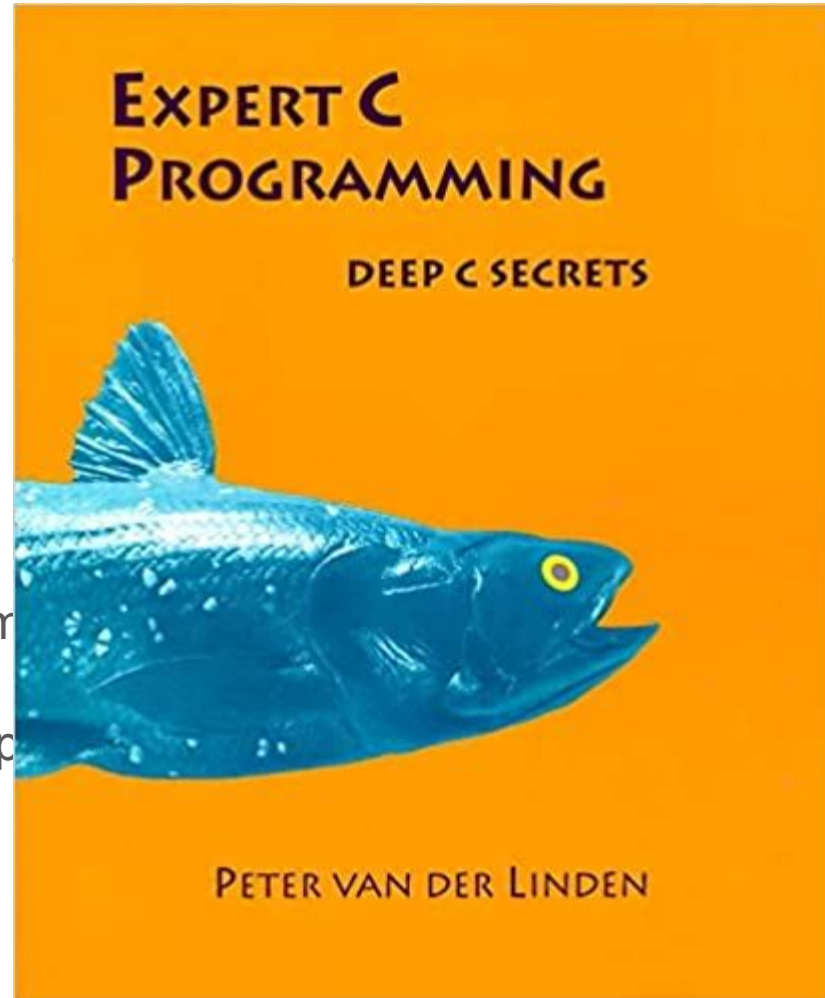
- El fracaso de MULTICS derivó en conocimiento, que sirvió para el desarrollo de UNIX.
- ¿Has escuchado hablar sobre Ken Thompson?

# ¿Y la seguridad?

- Multics. 1964 1970 (MIT, General Electric



- El fracaso de MULTICS derivó en conocimiento de UNIX.
- ¿Has escuchado hablar sobre Ken Thompson?

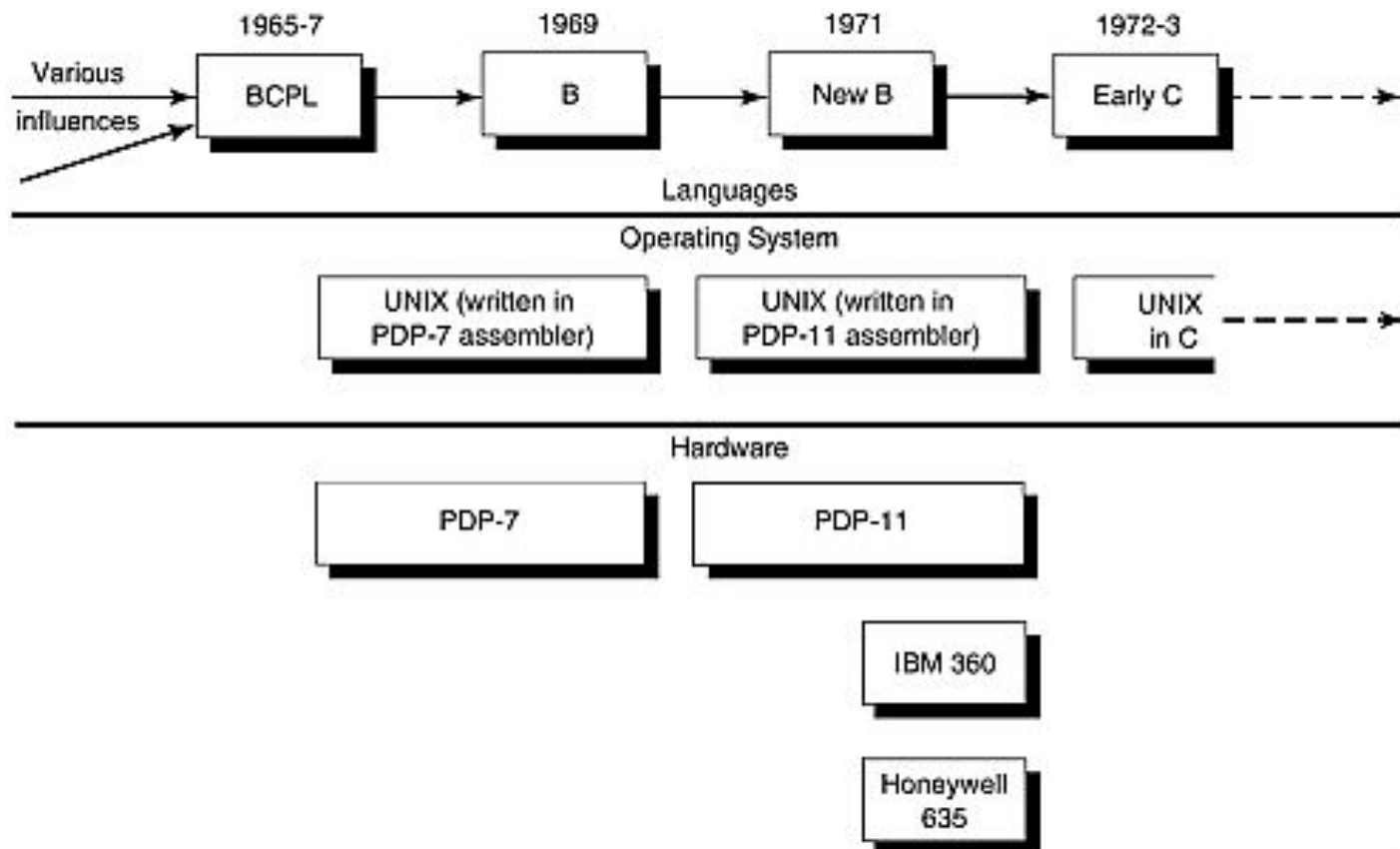


# Don't follow the leader



*C fue una mejora de Ritchie al lenguaje de programación B, desarrollado por Thompson.*

# ¿Por que C es importante?



# Los hackers vs los sistemas operativos multiusuarios

- PDP-6 - Spacewar
- La interfaz era un osciloscopio y un par de potenciómetros
- La idea de multiusuario resultaba ser un atentado
- Si existe algo lo suficientemente importante para tener contraseña, se debe ser compartido
- Fue así que comenzó la primera pelea eterna
  - Seguridad vs Hackers
- Esto ha ayudado a mantener seguridad sólida
  - Robert Morris



# Homebrew Computer Club

- California 70s - 80s
- Del MIT a Berkeley
- Steve Wozniak
- Aquí se desarrolló el cómputo moderno
- Lo ilegal era bien visto (entre los entusiastas)
  - Blue Box
  - Intrusiones a mainframes de DoD
    - WARGAMES



# The hacker's Manifesto

- Phrack 7. 1986

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++



# Chaos Computer Club

- Fundado en 1981
- Alemania
- Múltiples sedes locales
- Sus integrantes trabajaron para la KGB realizando intrusiones en equipo de US.
  - No terminó bien
- Chaos Communication Congress



```
ooooooo      oo      oooooo      oo
$$""$$"      o$"$ $      ""$ $      o$"$ $
$$o$$"      $ $ $ $      $ $      $ $ $ $
$$$$$      $ $ $ $      $ $"      $ $ $ $
$$" $ $      $$$$ $ $      o$"      $$$$ $ $
$ $ " $ $      $ $ $ $      o$ $oooo      $ $ $ $
```

```
o$ o$ $$$$ $ '$o o$' $ $ $$$$      oo o$ o$      oo
o$ $ $ $ $ $ '$o o$' $ $' o$"$ $ o$ $ $ o$"$ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $
```

-----

BOLETIN INFORMATIVO DE LOS INTEGRATES DE  
RaZa-MeXiCaNa HaCkeRs TeAm

# ¿Y el lado defensivo?

- Historia.
- Robert Tappan Morris, estudiante del MIT e hijo de Robert Morris, quien implementará el sistema de autenticación usuario, contraseña en UNIX
- Diseña un gusano que abusa de una vulnerabilidad de sendmail en 1988, toma todos los recursos de cómputo y se replica a través de red.
- El gusano de internet, o gusano Morris marca el punto de partida para los equipos de respuesta a incidentes

## ¿Y el lado de

- Historia.
- Robert Tappan
- Diseña un gu
- El gusano de



orris, quien  
a en UNIX  
mail en 1988,  
red.  
rtida para los

CERT



# **Software Engineering Institute**


## **Carnegie Mellon University**



# ¿Qué es un CERT?

Acrónimo	Nombre
CIRT	Cyber or Computer Incident Response Team
CERT	Cyber or Computer Emergency Response Team
CIRC	Cyber or Computer Incident Response Capability
CERC	Cyber or Computer Emergency Response Capability
SIRT	Security Incident Response Team
SERT	Security Emergency Response Team
SIRC	Security Incident Response Capability
SERC	Security Emergency Response Capability
IRT	Incident Response Team

# ¿Que hace un ERaI?

**Reactive Services** 

- + Alerts and Warnings
- + Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- + Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- + Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

**Proactive Services** 

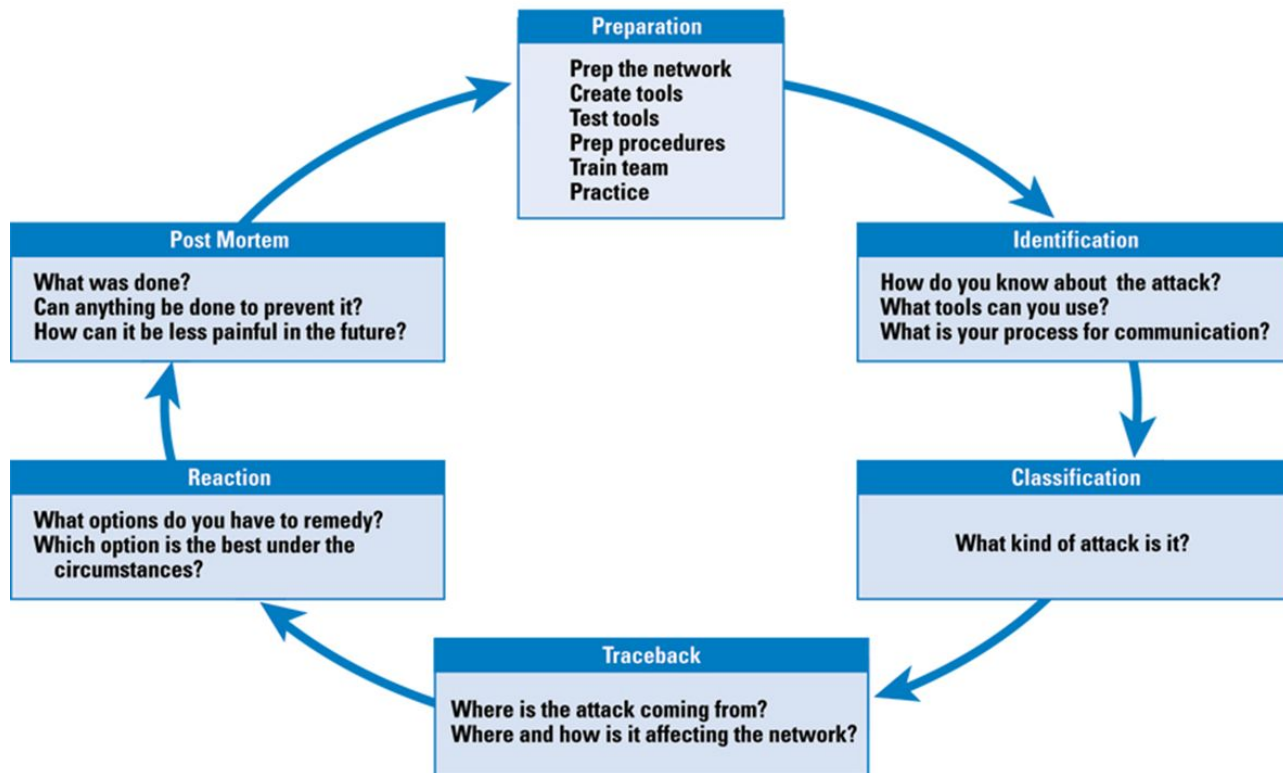
- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

**Security Quality Management Services** 

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification



# El proceso





# El presente

- Sistemas de entrenamiento, certificaciones, programas academicos, centralización
  - Nulo conocimiento de desarrollo
  - CS = Matematicas Discretas
- Diferenciación muy marcada de lado defensivo y ofensivo
  - ¿Por que ser enemigos?
- Bug Bounty
  - Aspiraciones a ser un rockstar / millonarios
- El futuro...



**Jeff McJunkin** @jeffmcjunkin · 17h

Offense in depth: Having more than one way (multiple tools and approaches) to solve any particular offensive problem.

At some point your favorite toys *\*will\** be taken away. Be able to solve the problem regardless.

(Or, as @TimMedin says: *\*Use\** the tools, but don't *\*be\** a tool)

academicos,

- Diferenciación muy marcada de lado defensivo y ofensivo
  - ¿Donde no debo trabajar?
- Bug Bounty
  - Aspiraciones a ser un rockstar / millonarios
- El futuro...
  - Aprender: Explotación de binarios, lenguaje ensamblador de 64 bits, semántica de lenguajes de programación, fuzzing, algoritmos y criptografía.



**Jeff McJunkin** @jeffmcjunkin · 17h

Offense in depth: Having more than one way (multiple tools and approaches) to solve any particular offensive problem.

At some point your favorite toys *\*will\** be taken away. Be able to solve the problem regardless.

(Or, as @TimMedin says: *\*Use\* the tools, but don't *\*be\** a tool*)

academicos,



**LiveOverflow** @LiveOverflow · 14 mar.

what the fuck is this @VICE "reporting"

SIVO



youtube.com

**I Hunt Down Internet Trolls | Super Users**

Meet TikTok's Masked Vigilante, who has made it his mission to track down and expose online bullie...

4 bits, semántica de lenguajes



**Jeff McJunkin** @jeffmcjunkin · 17h

Offense in depth: Having more than one way (multiple tools and approaches) to solve any particular offensive problem.

Hackers 1980



Let me  
create an editor

Hackers 2022



How do I exit Vim??

academicos,

Be able to solve the

\* a tool

...

SIVO

s made it  
line bullie...

4 bits, semántica de lenguajes



**Jeff McJunkin** @jeffmcjunkin · 17h

Offense in depth: Having more than one way (multiple tools and approaches) to solve any particular offensive problem.

Hackers 1980

Hackers 2022

Be able to solve the

academicos,



**vx-underground** @vxunderground · 11 ene.

We've added a new paper to our AV Tech paper collection:

An Empirical Assessment of Endpoint Security Systems Against Advanced Persistent Threats Attack Vectors Part III by @kpatsak & @Sneakid2

[vx-underground.org/av.html](https://vx-underground.org/av.html)

Let me  
create an editor

How do I exit Vim??

s made it  
line bullie...

4 bits, semántica de lenguajes



Jeff Mc  
Offense  
approach

Hack



creat

imgflip.com



S,

de lenguajes

# ¿Qué esperar del curso?

- Aprenderás a ser un buen sysadmin, soñarás con la terminal y harás herramientas que se verán bien en tu Github.
- Haremos mucho uso de lo básico, sistemas operativos, redes, CS.
- Serán profesionales en la materia, tanto en lo técnico como en lo que respecta a tecnología.
- De tener éxito el curso, buscar que se perpetúe el curso en la facultad de ciencias. Siendo ustedes los herederos y encargados de educar generaciones futuras :)

# Ejercicios opcionales

- Intentar realizar los ejercicios de programación del PDF adjunto, el cual se utilizó como preparación de un curso para semestres anteriores.
- Una vez intentados los ejercicios, pensar en lo siguiente: ¿Cuales son mis deficiencias?, quizás no sea tu culpa, pero es momento de cubrirlas ;)
- Ver las películas:
  - Wargames (1983)
  - Hackers (1995)



