Planeación Didáctica

Análisis y Detección de Malware

Lectures Notes

Impartido en el
CIC y ESCOM

2024-B
26 de agosto del 2024

My Bio

Raúl Acosta Bermejo

Contacto

http://www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652

55-34-30-94-09

Formación

- Ing. Electrónica
- M. en C. CINVESTAV
- Dr. ENMP

Experiencia

- Docente
- Investigador
- Funcionario
- Desarrollo de Tecnológico

Motivación

Por qué este curso? Porque análisis?

Para el **Análisis**

Análisis vs Síntesis

- ***Análisis***.- Examen detallado de una cosa para conocer sus características o cualidades, o su estado, y extraer conclusiones, que se realiza separando o considerando por separado las partes que la constituyen.

  Identificar componentes de un todo / separarlos y examinarlos / principios fundamentales

  Varios tipos de análisis: cualitativo, cuantitativo

- **Síntesis**.- Reunir distintos elementos que estaban dispersos o separados organizándolos y relacionándolos.

  Varios tipos de síntesis: colores (aditiva, sustractiva, rojo+azul=magenta).

- **Deducción** La deducción va de lo general a lo particular.

  Es el razonamiento que conduce a una conclusión lógica a partir de la formulación de dos enunciados (generales). Aquí interviene la cuestión lógica. Ejemplo:

  Todos los mamíferos tienen cuatro patas, y Todos los perros tienen cuatro patas. Conclusión lógica: Todos los perros son mamíferos.

- **Inducción** Va de lo particular a lo general

  A partir de varios hechos o casos particulares, podemos llegar a establecer una conclusión o teoría general.

Análisis/Deducción – Síntesis/Inducción

Planeación didáctica

Definición

Definición

La planeación didáctica es diseñar un plan de trabajo que contemple los elementos que intervendrán en el proceso de enseñanza-aprendizaje organizados de tal manera que faciliten el desarrollo de las estructuras cognoscitivas, la adquisición de habilidades y modificación de actitudes de los alumnos en el tiempo.

- Es la acción que orienta y vertebra la propuesta del docente. Es una acción propia de todos los docentes, es inherente a su tarea. Es una actividad mental que realizan todos.
- Puede ser entendida como un *recorrido de enseñanza anticipatorio* que abre la posibilidad de una reflexión que redundará en un enriquecimiento de la práctica en sí, al ir desarrollándola y modificándola en función de las situaciones concretas de la sala.
- Al planificar el docente se plantea qué enseña y para qué, cómo relacionan los nuevos contenidos con los anteriores, cómo organizarlos, qué actividades son pertinentes, cómo organizar la tarea de la sala en función del espacio y dinámica de trabajo, etc.

La PD ha evolucionado con las diferentes teorías didácticas:

conductista, constructivista (Jean Piaget) .

Syllabus

Programa de estudios, curriculum, list of topics

Syllabi serve several important purposes, the most basic of which is to communicate the instructor's course design (e.g., **goals, organization, policies, expectations, requirements**) to students. Other functions commonly served by a syllabus include:

- To convey our enthusiasm for the topic and our expectations for the course
- To show how this course fits into a broader context ("the big picture")
- To establish a contract with students by publicly stating policies, requirements, and procedures for the course
- To set the tone for the course, and convey how we perceive our role as the teacher and their role as students
- To help students assess their readiness for the course by identifying prerequisite areas of knowledge
- To help students manage their learning by identifying outside resources and/or providing advice
- To communicate our course goals and content to colleagues

Diferencia de significado en ingles y español:

https://en.wikipedia.org/wiki/Syllabus

https://es.wikipedia.org/wiki/Syllabus Contrato

Table of contents (outline)

Tabla de contenido

1. Temario
   - Contenido del programa
2. Bibliografía
3. Evaluación
4. Calendario

Temario

Resumido

	Horas	Clases
1. Introducción	6	3
2. Ciberseguridad	8	4
3. Repositorios de Malware	6	3
4. Laboratorios de Malware	20	10
i. Ejemplos		
ii. Construcción de uno.		
5. Análisis de Malware	20	10
i. Análisis estático	15	7.5
a. Herramientas		
ii. Análisis Dinámico	5	2.5
a. Herramientas		

Bibliography

Referencias

Additional bibliography

Bibliografía

Links

Bibliografía

Oficial

Grupo 1

Referencias básicas e iniciales

- Malware Analyst's Cookbook and DVD, Tools and Techniques for fighting malicious code
  - Autores: Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard.
  - Edición y/o Editorial: Wiley Publishing Inc, 2011.
- Practical Malware Analysis
  - Autores: Michael Sikorski, Andrew Honig.
  - Edición y/o Editorial: Wiliam Pollock, 2012.
- Malware Data Science
  - Autores: Joshua Saxe, Hillary Sanders
  - Edición y/o Editorial: No Starch Press, 2018.

Bibliografía

Oficial

Grupo 2

Referencias complementarias

- HACKING EXPOSED MALWARE & ROOTKITS:
  MALWARE & ROOTKITS SECURITY SECRETS & SOLUTIONS
  - Autores: Michael DAVIS, Sean BODMER, Aaron LEMASTERS.
  - Edición y/o Editorial: McGraw Hill. 2nd edition 2017.
- Malware: Fighting Malicious Code
  - Autores: ByEd Skoudis,Lenny Zeltser.
  - Edición y/o Editorial : Pearson, 2003.
- Rootkits: Subverting the Windows Kernel
  - Autores: Greg Hoglund, James Butler.
  - Edición y/o Editorial: Addison Wesley Professional.

Bibliografía

Oficial

Grupo 2

Referencias complementarias

- The Ghidra book
  - Autores:.
  - Edición y/o Editorial:.

Bibliografía

Oficial

Grupo 3

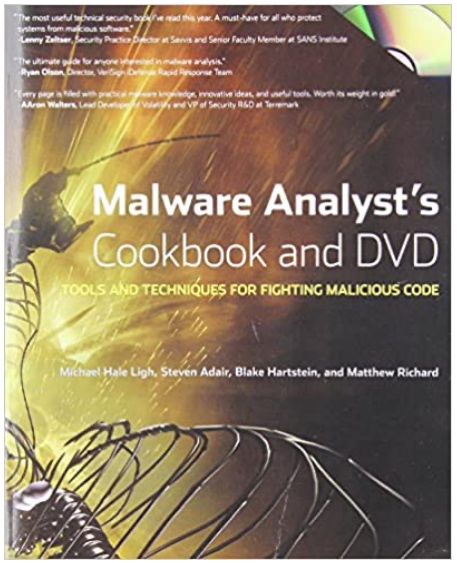
Varios libros de Seguridad en Redes y SO

1. Learning Linux Binary Analysis
   "elfmaster" O'Neill, Packt Publishing, 2016.
2. “Hacking Exposet No. 7: Network security secrtes and solutions”
   Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill, 2012 .
3. “A Guide to Kernel Exploitation”
   Enrico Perla, Massimiliano Oldani, Ed. Elsevier
4. Hacking, The art of exploitation
   Jon Erickson, No starch Press, 2008 2nd edition.
5. Linux 101 Hacks (eBook Free)
6. Linux Sever Hacks

Malware Analyst's Cookbook and DVD

Tools and Techniques for fighting malicious code

Tabla de Contenido



Practical Malware Analysis

Michael Sikorski, Andrew Honig

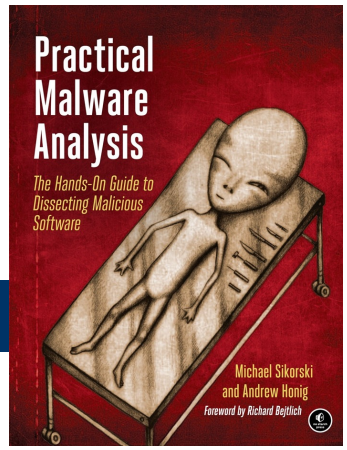


Tabla de Contenido

Malware Data Science

Joshua Saxe with Hillary Sanders

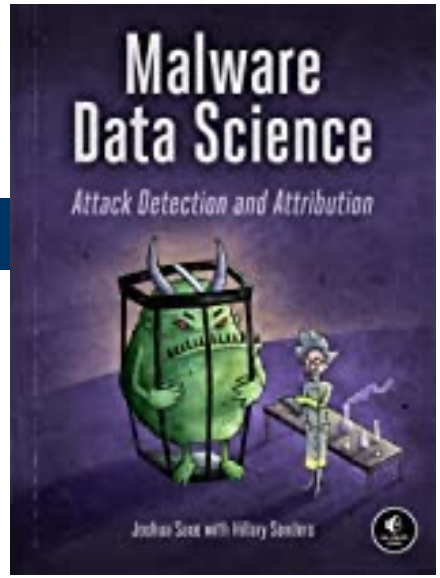


Tabla de Contenido

HACKING EXPOSEDTM MALWARE & ROOTKITS: MALWARE & ROOTKITS SECURITY SECRETS & SOLUTIONS

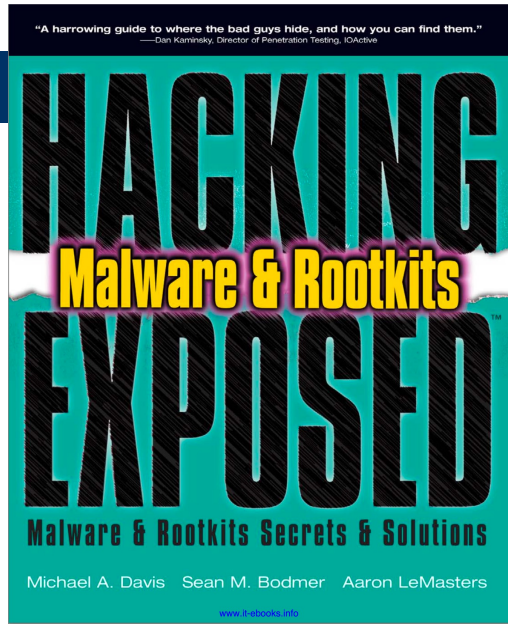


Tabla de Contenido

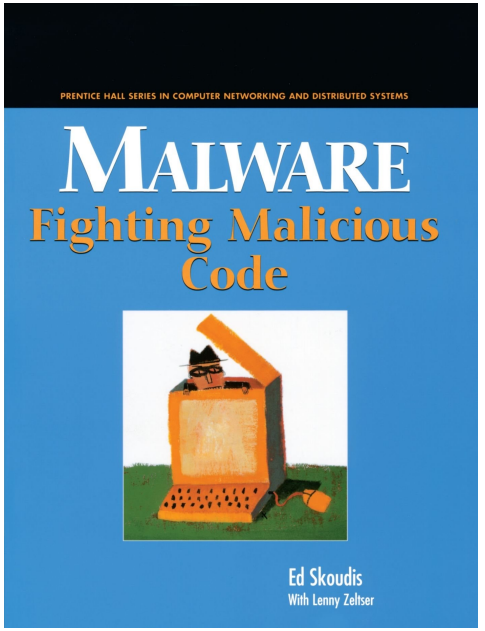
Links

- https://www.amazon.com/vdp/1dc539c017864ef28bbadf539dc61ae8?ref=dp_vse_rvc_0

Malware: Fighting Malicious Code

Ed Skoudis,Lenny Zeltser

Tabla de Contenido



Rootkits: Subverting the Windows Kernel

Greg Hoglund, James Butler

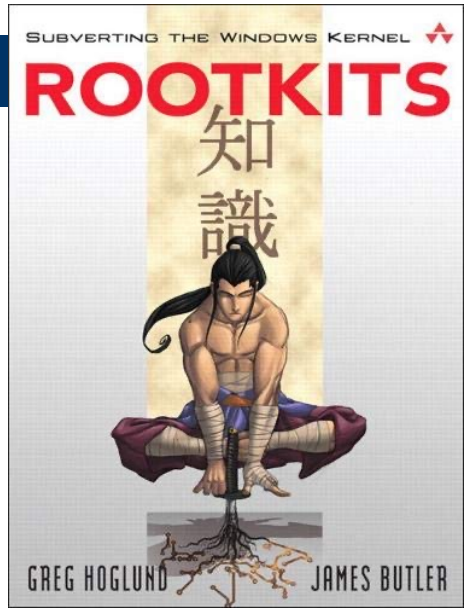


Tabla de Contenido

Modern Malware FOR DUMMIES

Lawrence C. Miller, CISSP

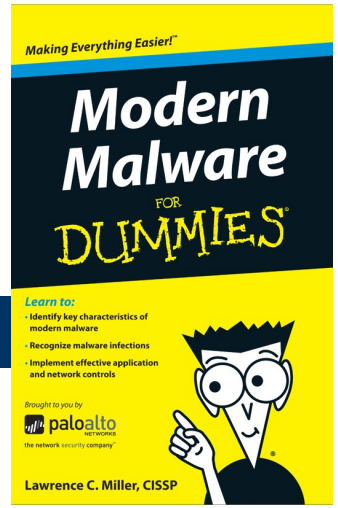


Tabla de Contenido

E-learning

Cursos en linea

Links

1. Curso: Sam Bowne
   i. CNIT 126: Practical Malware Analysis
   ii. Fall 2021 Sam Bowne, Tue 6:10 - 9 pm.
   iii. https://samsclass.info/126/126_F21.shtml
2. Cursos: Class central

   Malware analysis Courses and Certifications
   i. https://www.classcentral.com/course/youtube-malware-analysis-63978
3. Cursos: INE
   i. https://ine.com/learning/courses/malware-analysis

Un gran etcétera que evoluciona.

Grading policy

Mecanismo de Evaluación

Elementos

Exámenes, prácticas, etc.

y porcentajes

Elementos de la evaluación

Estáticos o dinámicos

Elementos Clásicos

- Exámenes / Exams
- Participación
- Prácticas
- Proyectos / Projects
- Ejercicios extra-clase
- Tareas / Homeworks

Elementos de la evaluación

Para este curso

Semestre 2024-A

- La mayor parte de la evaluación 80%

  Prácticas de Laboratorio.

  - Laboratorio de Malware ver 1.
  - Laboratorio de Malware ver 2.
  - Laboratorio de Malware ver 3.

  Aprox. dos por parcial.

- Tareas y trabajos extra-clase 20%

Calendar

Calendario

Por Ciclo Escolar

Calendarización de las Clases

Por semestre

Lo más importante

- El detalle estáen un archivo Excel que se comparte.
- Para este semestre 2024-B

  Se tienen:

  - 5 meses.
  - 21 semanas - 2 de vacaciones (Navidad y Fin de año)
  - Días inhabiles (asueto): 2 que afectan clase en lunes.
  - 37 clases efectivas.

Sección de Comentarios

Y aclaración de dudas

Casos extremos

Normatividad

Darse de Baja

Reglamento de Estudios de Posgrado.

Gaceta Politécnica
Número Extraordinario
1358

15 de septiembre
2017

Artículo 29. El alumno podrá solicitar por escrito la baja a una unidad de aprendizaje o la baja temporal del programa, de acuerdo con lo previsto en el Reglamento General de Estudios.

Cuando el alumno recurse una unidad de aprendizaje no procederá la baja de la misma.

Reglamento General de Estudios del Instituto Politécnico Nacional.

Gaceta Politécnica
Número Extraordinario
866

13 de junio 2011

Artículo 54. El alumno podrá solicitar la baja de unidades de aprendizaje en las que se encuentre inscrito en el periodo escolar, siempre y cuando mantenga la carga mínima de créditos establecidos en su plan de estudio.

Tratándose de una misma unidad de aprendizaje procederá la baja en un máximo de dos ocasiones.

En ambos casos, el alumno deberá presentar la solicitud por escrito ante la Subdirección de Servicios Educativos e Integración Social o el Colegio de Profesores de su unidad académica, según corresponda, durante las primeras tres semanas de haber iniciado el periodo escolar.

Cuando el alumno esté recursando una unidad de aprendizaje no procederá la baja de la misma.

Para el alumno que curse un programa académico en las modalidades educativas diferentes a la escolarizada, se sujetará a lo previsto en los lineamientos correspondientes.

Para este ciclo escolar el límite es el
13 de septiembre del 2024

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652