



## PROGRAMACIÓN DE LA ASIGNATURA

<b>ASIGNATURA:</b>	LS5148 – SEGURIDAD INFORMÁTICA
<b>PROFESOR:</b>	D. CONSTANTINO MALAGÓN
<b>CURSO:</b>	2009 / 2010
<b>CUATRIMESTRE:</b>	SEGUNDO
<b>DEPARTAMENTO:</b>	INGENIERÍA INFORMÁTICA (DII)
<b>ÁREA:</b>	INGENIERÍA TELEMÁTICA
<b>GRUPOS:</b>	4IT1
<b>PLAN / CRÉDITOS:</b>	PLAN 98 – 6 CRÉDITOS

### **1.- REQUISITOS PARA CURSAR LA ASIGNATURA**

Haber cursado las asignaturas Redes y Comunicaciones de Datos I. En general conocimientos básicos de redes de comunicaciones, sistemas operativos, y conocimiento en profundidad de algún lenguaje de programación que constituyen una ventaja pero no resultan imprescindibles. Sería también muy deseable un conocimiento más o menos profundo de administración de Linux, puesto que es el entorno de trabajo elegido para la asignatura.

### **2.- DESCRIPCIÓN GENERAL DE LA ASIGNATURA. OBJETIVOS DE DOCENCIA**

El objetivo del curso es estudiar las técnicas encuadradas en lo que se ha venido a llamar Hacking Ético. Se pretende obtener una amplia visión de las amenazas y riesgos a los que están sometidos los servidores en general (aunque como ya se ha comentado se trabajará en entornos Linux) Como futuros administradores y responsables de seguridad deberemos ser capaces a su vez de implantar las medidas oportunas para minimizar los riesgos en lo que a seguridad informática se refiere.

### **3.- FORMA DE EVALUACIÓN PREVISTA**

#### **3.1.- CONVOCATORIA ORDINARIA**

- |   |     |
|---|-----|
| • Participación, Prácticas, Trabajos Escritos | 20% |
| • Examen Parcial                              | 15% |
| • Examen Final (Proyecto final de curso)      | 65% |

#### **3.2.- CONVOCATORIA EXTRAORDINARIA**

- |   |     |
|---|-----|
| • Participación, Prácticas, Trabajos Escritos | 20% |
| • Examen Final (Proyecto final de curso)      | 70% |

#### **3.3.- RESTRICCIONES**

- Es imprescindible la entrega de todos los trabajos considerados como obligatorios, tanto para la convocatoria ordinaria, como para la extraordinaria, así como obtener una calificación mínima de 5 puntos en todos y cada uno de ellos.
- Es también necesario el obtener la calificación de 4.5 o superior en el examen para poder realizar la media con los otros conceptos.

## **4.- BIBLIOGRAFÍA**

### **4.1.- BIBLIOGRAFÍA DE SEGURIDAD**

- Michael Gregg. Certified Ethical Hacker Exam Prep 2. Que editores.
- Abel Matas García. La biblia del hacker. Anaya Multimedia
- Abel Matas García. Hacking práctico. Anaya Multimedia
- Michael D. Bauer. Linux Server Security. 2<sup>nd</sup> Edition. O'Reilly.
- Brian Hatch. Hacking exposed Linux. Ed. Mcgraw-Hill.

### **4.2.- BIBLIOGRAFÍA ESPECÍFICA DE LINUX**

- Documentación de Debian. <http://www.debian.org/doc/>
- *The Linux Documentation Project*: <http://www.tldp.org/index.html>

## **5.- LOCALIZACIÓN DEL PROFESOR**

Prof. D. Constantino Malagón Luque  
Departamento de Ingeniería Informática  
Despacho 308  
E-Mail: [cmalagon@nebrija.es](mailto:cmalagon@nebrija.es)  
Web: <http://www.nebrija.es/~cmalagon>  
Tfno: 91 452 11 00 ext. 5822

## PROGRAMA DETALLADO DE LA ASIGNATURA

### LS5148 – SEGURIDAD INFORMÁTICA

#### SESIONES

1. Presentación de la asignatura.

#### INTRODUCCIÓN

2. Introducción al Hacking Ético.

#### TÉCNICAS DE OBTENCIÓN DE INFORMACIÓN, ESCANEADO DE PUERTOS Y DETECCIÓN DE VULNERABILIDADES

3. Métodos no intrusivos para la obtención de información.
4. Conceptos básicos de TCP/IP, servicios y comunicaciones.
5. Métodos intrusivos para la obtención de información. Técnicas de rastreo o sniffing. Uso de Ethereal.
6. Rastreo oculto. Detección de los sniffers funcionando en la red mediante el uso de técnicas antisniff.
7. Escaneo de puertos. Detección de sistemas operativos. Chequeo mediante ICMP de los servidores activos. Uso de Nmap.
8. Sistemas de detección de vulnerabilidades. Uso de Nessus.

#### TÉCNICAS DE INTRUSIÓN Y ATAQUE

9. Técnicas de ataque sobre conexiones seguras usando ataque MIM (Man in the Middle).
10. Intrusión por NETBIOS. Creación de sesiones nulas.
11. EXAMEN PARCIAL
12. Sniffers especializados en contraseñas y en espionaje de actividad (dsniff, webspay, urlsnarf).
13. Técnicas de obtención (craqueo) local de contraseñas. Técnicas de interceptación de contraseñas. Craqueo remoto. Caín y Abel. Uso de keyloggers.
14. Técnicas de DoS (Denegación de servicio). Inundación SYN (SYN flooding)
15. Técnicas de IP spoofing. Falsificación de las tablas ARP (ARP Spoofing)
16. Técnicas de DNS spoofing. Secuestro de sesiones DNS. Uso de DNSSpoof. Falsificación de la caché DNS.
17. Técnicas de Hijacking. Secuestro de conversaciones. Suplantación de IP. Modificación de las cabeceras TCP/IDP.
18. Suplantación de identidad. Envío de correos mediante comandos aceptados por el protocolo SMTP.

#### TÉCNICAS DE OCULTACIÓN O ANONIMATO

19. Rootkits. Ocultación por stream en particiones NTFS (ADS – Alternate Data Stream)
20. Navegación anónima. Proxys anónimos. Encadenamiento de proxys.

#### SEGURIDAD EN REDES

21. Seguridad mediante Firewalls. Concepto de DMZ. Firewall mediante iptables en Linux.
22. Puertas traseras. Técnicas para evitar los firewalls. Reverse Shell y netcat.
23. Trabajo en remoto: SSH. Redes privadas virtuales (VPN) Configurar un servidor VPN con Linux.

#### SISTEMAS DE DETECCIÓN DE INTRUSOS

24. Tipos de IDS. Arquitecturas IDS.
25. Auditorías y análisis forense.
26. Normativa legal.

27. EXAMEN FINAL ORDINARIO

28. EXAMEN FINAL EXTRAORDINARIO