

Curso: Técnico en Seguridad de Redes y Sistemas.

Temario

1. Preparación del entorno de trabajo.
2. Modelo de capas TCP/IP.
3. Tecnologías de acceso ADSL y WiFi.
4. Redes Ethernet.
5. Tipos de tráfico.
6. Manejo de información en binario, octal y hexadecimal.
7. Control de acceso (físico y lógico).
8. Nivel de enlace.
9. Nivel de red.
10. Encabezado y direccionamiento de protocolo IP versión 4.
11. Network Address Translation (NAT).
12. Protocolo Internet Control Messaging Protocol (ICMP).
13. Protocolo Dynamic Host Configuration Protocol (DHCP).
14. Nivel de Transporte. Transport Control Protocol (TCP) y User Datagram Protocol (UDP).
15. Conceptos de Firewall.
16. Introducción a la criptografía.
17. Protocolos seguros e inseguros.
18. Qué busca y cómo opera un intruso.
19. Medidas básicas de seguridad a tener en cuenta.



<u>Ejercicios:</u>	<u>Herramientas / Comandos:</u>
<ol style="list-style-type: none"> 1. Instalación de máquinas virtuales. 2. Primeros pasos con Linux, distribución "Kali" 3. Presentación de la herramienta "Wireshark" 4. Escuchar y Capturar tráfico. 5. Analizador de protocolos. 6. Empleo de Wireshark. 7. Ejercicios de arp y de direccionamiento MAC. 8. Empleo de arpswatch. 9. Trabajos sobre rutas y direccionamiento IP. 10. Ejercicios de rutas IP 11. Ejercicios de red y subred. 12. IPSpoofing. 13. Generar tráfico de red. 14. Ejercicios con "nmap" y "Zenmap". 15. Ejercicios con "iptables". 16. Empleo de "firewalbuilder". 17. Medidas prácticas de seguridad. 	<ol style="list-style-type: none"> 1. Lynis 2. Wireshark 3. Suite "aircrack-ng" 4. Arpwach 5. Ifconfig 6. Tcpdump 7. Arpspoof 8. Yersinia 9. Ettercap 10. Ipcalc 11. Netstat 12. Route 13. Hping3 14. Fragroute 15. Fragtest 16. Nmap 17. Netcat 18. Iptables 19. Ufw 20. FWBuilder 21. OpenSSL 22. Gpg 23. Wget 24. snmpwalk