



Las guías para Informes Técnicos encuadradas en la serie 900 es un compendio de guías especializadas para analistas informáticos de seguridad y personal de soporte.

Dirigida a las herramientas habituales de uso de personal técnico profesional en incidencias de seguridad, análisis de tráfico de red, vulnerabilidades y malware.

- 903 Configuración segura de asistente personal digital HP-IPAQ 6340
- 911A* Ciclo de una APT (DL)
- 911B* Recomendaciones generales ante una APT (DL)
- 912 Procedimiento de investigación de código dañino
- 920 Análisis de malware con Cuckoo Sandbox
- 951 Manual de Ethereum/Wireshark
- 952 Nessus
- 953 Recomendaciones de Empleo de la Herramienta Snort
- 954 Guía avanzada Nmap
- 955 Recomendaciones de Empleo de GnuPG v.1.4.7
- 956 Seguridad (Identificación y escape) de entornos de computación virtuales (virtualización de sistemas)
- 957 Recomendaciones de Empleo de la Herramienta TrueCrypt 7.0A
- 970 ** Uso de Cifradores IP en Redes Públicas (CONFIDENCIAL)
- 980 Arquitecturas de seguridad

Herramientas como Nessus, que ya ha sido tratado en otro de nuestros cursos, snort, nmap, etc. constituyen la columna vertebral de cualquier experto informático en seguridad y son de obligado conocimiento para quienes se dedican a la seguridad informática.

Definiciones como APT, recomendaciones, y procedimientos de investigación de código dañino nos ayudarán a poder dialogar con el personal de soporte

técnico de tu a tu y a poder sugerir procedimientos en reuniones técnicas.

Todo eso y más es lo recogido en las guías técnicas del CCN-CNI que la administración pone a disposición de empresas y usuarios con permisos especiales.