–Phishing: consiste en engañar al usuario para robarle información confidencial, claves de acceso, etc., haciéndole creer que eres tal persona, empresa o un servicio

(Método: ingeniería social, aprovecharse de estados emocionales de la persona, o necesidades de la persona, como hacerle creer que va a conseguir un trabajo o un iphone, con correos electrónicos (como cebo). Normalmente se roba información pero también se puede utilizar malware para sabotear sistemas).

–Phishing general/tradicional/Bulk/Spray and pray: enviar de forma masiva correos electrónicos a usuarios, haciéndose pasar por entidades de confianza como bancos con el fin de engañar al usuario y conseguir información. Ej: URL es correcta pero el enlace apunta a otro sitio.

–Vishing: como phishing tradicional pero por teléfono.

--Smishing: como phishing tradicional pero por mensajes de texto (SMS/Whatsapp/Facebook).

--URL Phishing: hacer parecer que una URL maliciosa parezca la de una entidad confiable. Se suele entrar o sin querer al introducir mal el URL o simplemente porque el usuario cree que es correcto lo que ha buscado pero en verdad tiene caracteres que no se ven sencillamente.

—--<a href=”192.168.1.234”>Banco Santander</a>

—--<a href=”www. caixa.es”>Caixa</a>

—--DNS: ip verdadera / ip falsa (servidor DHCP/DNS/WEB), registros que lleven a otros sitios.

--Whaling: phishing pero a persona con un alto rango, la información que se quiere obtener se explota de una forma más individualizada.

–SQL Injection: el atacante lo que hace es inyectar código SQL malicioso en la base de datos de la víctima, y fuerza a la base de datos a ejecutar esa sentencia. Las sentencias pueden destruir las tablas de la BD o extraer información privada como contraseñas.

—-select\* from usuarios where usuario=’admin(variable nombre)’ and clave=’1234(variable clave)’

–Exploiting: Es un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad en un software o hardware. Su uso principal es utilizar payloads que permiten al que ataca acceso o control al software o hardware atacado. Los payloads pueden ser usados por varios exploits y un mismo exploit por varios payloads.

–Auditing: Es un proceso para analizar todas las vulnerabilidades posibles de un sistema de una organización o entidad, es decir un análisis de las medidas de ciberseguridad para conocer los riesgos reales a los que se enfrenta una empresa y que se puede hacer para solucionar todos estos riesgos.