Temario: Taller 10 – InSecurityLand: de la A la Z en pentesting

Introducción a las pruebas de seguridad (PenTesting)
• Fases generales
• Metodologías
• Evolución de las metodologías
• Fases críticas
• Vulnerabilidades
• Descubrimiento
• Fuentes de consulta e información
• Fuentes de información en la web profunda
• Frameworks de explotación
Pruebas Tradicionales
• Herramientas automatizadas
• Mejora del desempeño de las herramientas automatizadas
• Scripting 1
• Pruebas manuales
• Desarrollo de Scripts
• Fuzzing
• Pruebas Manuales
Tecnologia Traidicional
• Pruebas de Escritorio y compromiso físico
• Pruebas en infraestructura Cliente/Servidor
• Explotación
• Pruebas a webapps
Tecnología Moderna
• Pentestiing a tecnología cloud
• API testing
• Disección de Malware
• Evasión de controles de seguridad
Trofeos o huevos dorados
• Niveles de compromiso
• Escalamiento de privilegios
• RAT - configuración de plataformas de adminsitración remota sin autenticación