[INT] Test de Penetración

Se realizan pruebas ofensivas contra los mecanismos de defensa de una infraestructura, estos pueden ir desde el ámbito físico hasta el software.

Hackers

- Sombrero negro: Hackers, sacan beneficio
- Sobrero gris: hacen ambas
- Sobrero Blanco: muestra y enseñan como hacer hacking

Not Hackers

- Script Kiddies: utilizan programas escritos de otros para penetrar algún sistema, red o web.
- Newbie: Es un principiante inofensivo en busca de información sobre hacking
- Lammer: Persona que se cree hacker pero no tienen los conocimientos para comprender que esta sucediendo cuando usa algún programa hecho para hackear.

Certificaciones

CEH

Hay 2, el teorical y el practical:

- Theorical: Examen con preguntas, se necesita acertar el 70% para aprobar
- Practical: 20 Retos de todo tipo en 6 horas, tiene que resolverse 14 para aprobar

Cuestan 550€. Se recomiendan las siguientes herramientas:

- NMAP
- SQLMap
- Hydra
- Wireshark
- Veracrypt
- Hashcalc
- Dirb
- Steghide
- WPSCAN
- Hashcat John Nikto
- Searchsploit

eJPTv2

35 retos en 50 horas sin restricciones de software, cuesta de 300 a 900€.

OSCP

Válida por 3 años, de 1600 a 5500€. De las más importantes

Modalidades de hacking

Hay 3 modalidades básicas

- Caja blanca: La empresa da información muy detallada, es usual cuando se ha detectado una brecha concreata en un lugar concreto
- Caja Negra: Una auditoría completa, no se da acceso, o se da acceso solo a las instalaciones. Estas suelen ser las más cuantiosas, hay una tasa fija, que son las horas que se va a tardar y una cuota, que es lo que encuentra el pentester. Antiguamente habían contratos mal hechos con clausulas mal redactadas del nivel de: “Se considera la auditoría finalizada al encontrar un usuario administrador”, lo que hace que esta cueste como si fuera del tiempo indicado inicialmente, durando esta una fracción del tiempo. Las empresas en general, con estos tipos de auditorías, buscan asegurarse de que su infraestructura es segura.
- Caja Gris: Cuando se tiene acceso a algunas cosas como un usuario y contraseña para las redes Wifi de la organización

Fases

Un test de penetración completo suele tener las siguientes fases:

1. Reconocimiento enumeración
2. Análisis de vulnerabilidades
3. Explotación
4. Reporting

Reconocimiento y Enumeración

Tenemos dos fases iniciales:

- FootPrinting: Información que se puede obtener de forma pasiva. Se trata de obtener información basada en datos públicos.
    - Se debe hacer una instantánea de los elementos observables de la red local (IP activas, protocolos usados, topología, si hay IDS, IPS o FireWalls)
- FingerPrinting: Información que se puede obtener de forma activa.
    - Una vez identificadas las máquinas disponibles se escanean con el fin de obtener información sobre el SO, Servicios activos y las versiones de IDS o Firewall.

Tras obtener datos en las fases iniciales siguen las siguientes fases:

1. Enumeración: Tras obtener toda la información posible, se buscan posibles vectores de ataque,

siendo preferibles los menos detectables.
2. Acceso: Se realiza el acceso al sistema mediante la explotación de vulnerabilidades.
3. Mantenimiento de acceso

Red Team vs Blue Team

Tenemos 2 tipos de equipos, los de defensa y los de ataque:

- Blue Team: Bloquea, detecta y previene ataques informáticos
- Red Team: Escanea, detecta y explota vulnerabilidades.
- Pruple Team: Pueden hacer las dos cosas pero son excesivamente caros.

Pentesting adicionales

- Ingeniería social: Obtención de información a través de la manipulación de las personas.
- Wardriving: Obtención de acceso a una red de forma inalámbrica desde fuera de la propia empresa
- Equipo Robado: comprobación de la información contenida en los dispositivos.