Hacking Ético

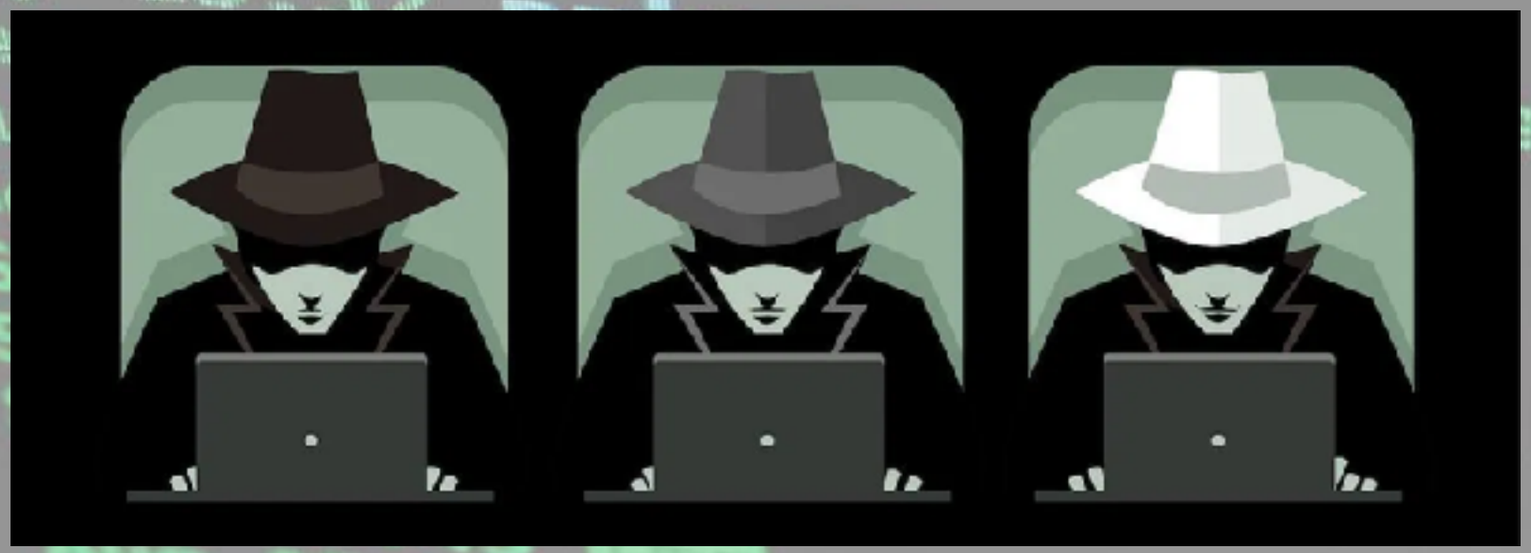
Francisco Martín Vázquez
Auditor de Ciberseguridad y Hacking Ético

Definición de Hacker

- Persona entusiasta de la tecnología que disfruta resolviendo problemas utilizando soluciones creativas y eficientes
- Disfrutan aprendiendo los detalles de la tecnología y como ampliar sus capacidades y funcionalidades
- En el ámbito tecnológico suelen ser personas con conocimientos en sistemas operativos, redes, programación o electrónica que utilizan sus conocimientos para conseguir saltar las medidas de seguridad y acceder a sistemas, redes o información protegida
- El término hacker se acuñó por un grupo de pioneros del MIT (Instituto Tecnológico de Massachusetts) y proviene de “hack”, el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionasen

Tipos de Hacker

- "White Hat" Hackers: (Los buenos) Su trabajo es localizar vulnerabilidades en un sistema para estudiar y corregir los fallos encontrados
- "Black Hat" Hackers: (Los malos, crackers) Son ciberdelincuentes, utilizan sus conocimientos para realizar actividades ilícitas con el objetivo de vulnerar y extraer información confidencial, principalmente con fines económicos aunque pueden tener otras motivaciones: políticos, sociales, etc.



Actividades Hacking Ético

- El Hacking Ético es una actividad legal realizada por profesionales de la seguridad y se rige por un estricto código deontológico y unas normas de conducta
- El objetivo es poner a prueba la efectividad de las medidas de seguridad en los sistemas de una compañía
- En este sentido las actividades se puede centrar en buscar vulnerabilidades y fallos de seguridad en diferentes ámbitos:
  - Seguridad Física:
    - Seguridad en accesos físicos: Lockpicking, sistemas de alarma, sistemas de vigilancia, etc.
  - Ingeniería Social
    - Ataques dirigidos a las personas: Llamadas telefónicas, Phishing, etc.
  - Seguridad en Tecnología
    - Pentest: Actividades dedicadas a la identificación y explotación de brechas de seguridad en el perímetro tecnológico de una compañía.
    - Análisis de Vulnerabilidades
    - Explotación de vulnerabilidades
  - CiberInteligencia
  - Análisis Forense

Cualificación

- Profesionales altamente cualificados técnicamente.
- Preferentemente perfiles técnicos: Informática, telecomunicaciones, electrónica, etc.
- Áreas de conocimiento:
  - Computación
  - Sistemas Operativos
  - Redes y Comunicaciones
  - Programación
  - Electrónica (Hardware)
  - Inteligencia (Ciberinteligencia)

Red Team: Equipo Multidisciplinar

El equipo ideal de Hacking ético o “Red Team” debería estar formado por profesionales con diferentes perfiles dentro del ámbito de la seguridad:

- Pentest
  - Especialista en pentest de aplicaciones Web, Cloud, Micro servicios, etc.
  - Especialista en pentest de sistemas: SSOO (Windows, UNIX), BBDD, Virtualización, Contenedores redes, routers, etc.
- Especialista en CiberInteligencia, medios, redes sociales, etc.
- Especialista en Ingeniería Social, seguridad física, etc.
- Especialista en Análisis Forense, ciberincidentes
- Analista de Malware, ingeniería inversa, etc.
- Especialista en desarrollo, BBDD, exploiting, desarrollo Seguro
- Especialista en Red y Comunicaciones: Redes de datos (TCP,IP, VPN, MPLS, etc), Firewalls, IDS, Redes inalámbricas (WiFi), Comunicaciones móviles (2G,3G, 4G, SS7, etc)
- Especialista en Hardware, electrónica, dispositivos IoT, etc.
- Especialista en seguridad de dispositivos móviles y aplicaciones móviles

Técnicas y Herramientas

- Actualmente existe una gran cantidad de herramientas accesibles en el Mercado (libres y comerciales)
- Aunque las herramientas son útiles y necesarias, no son suficientes para el desarrollo de la actividad
- Las herramientas automáticas a veces fallan y no tienen inteligencia
- La clave está en el factor humano
- Otra de las claves para el éxito en las tareas de hacking ético es desarrollar y utilizar una buena metodología
- Los integrantes del equipo deben de tener altas capacidades de aprendizaje que les permitan adaptarse a los continuos cambios y avances en materia de tecnología

Técnicas y Herramientas (SW)

- Herramientas de análisis de red:
  - Escáneres: nmap, tcpScan, hping, etc.
  - Analizadores de tráfico: tcpdump, wireshark, scappy, ettercap, Cain&Abel, etc.
  - Airodump, aircrack-ng, wifite, etc.
- Análisis de Vulnerabilidades:
  - Escáneres de Vulnerabilidades: Nessus, Rapid7, Qradar, Acunetix, OpenVAS, Retina, NetSparker, Nikto, WebInspect, etc.
  - Análisis y Explotación de Vulnerabilidades:
    - Vulnerabilidades Web: OWASP Zap, Burp Suite, Acunetix
    - Frameworks Explotacion: Metasploit, Empire, Core Impact, Inmunity Canvas, BeeF, routerexploit, etc.
    - Análisis Credenciales: Medusa, THC Hydra, John The Ripper, OCL Hashcat, OphCrack, Cain&Abel, FuzzDB, SecList, etc.
- Ingeniería Inversa (Análisis Malware)
  - Radare2, OllyDBg, WinDBG, Inmunity Debugger, IDA Pro, Cucko SandBox, etc.
- Análisis Forense: Encase, SleuthKit, Volatility, etc.
- Otros: Virtual Box, VMWare, Dynamips, GCC, MinGW, PowerShell, Shell Scripting, Python, Perl, etc.

Técnicas y Herramientas (HW)

- Herramientas de análisis de red:
  - AirSPy, HackRF, Wifi Pineapple, SDR, OsmoCom, etc…
- Análisis de Vulnerabilidades:
  - Raspbery Pi, Orange Pi, SBCs en general.
  - Bad USB, Rubber Ducky, Key loggers HW, etc
- Ingeniería Inversa (Análisis Malware)
  - USB RS232 ports, Sonda Lógica, Osciloscopio, Bus Pirate, etc
  - Arduino, programadores/lectores EEPROM, Microcontroladores, etc.

¡GRACIAS!