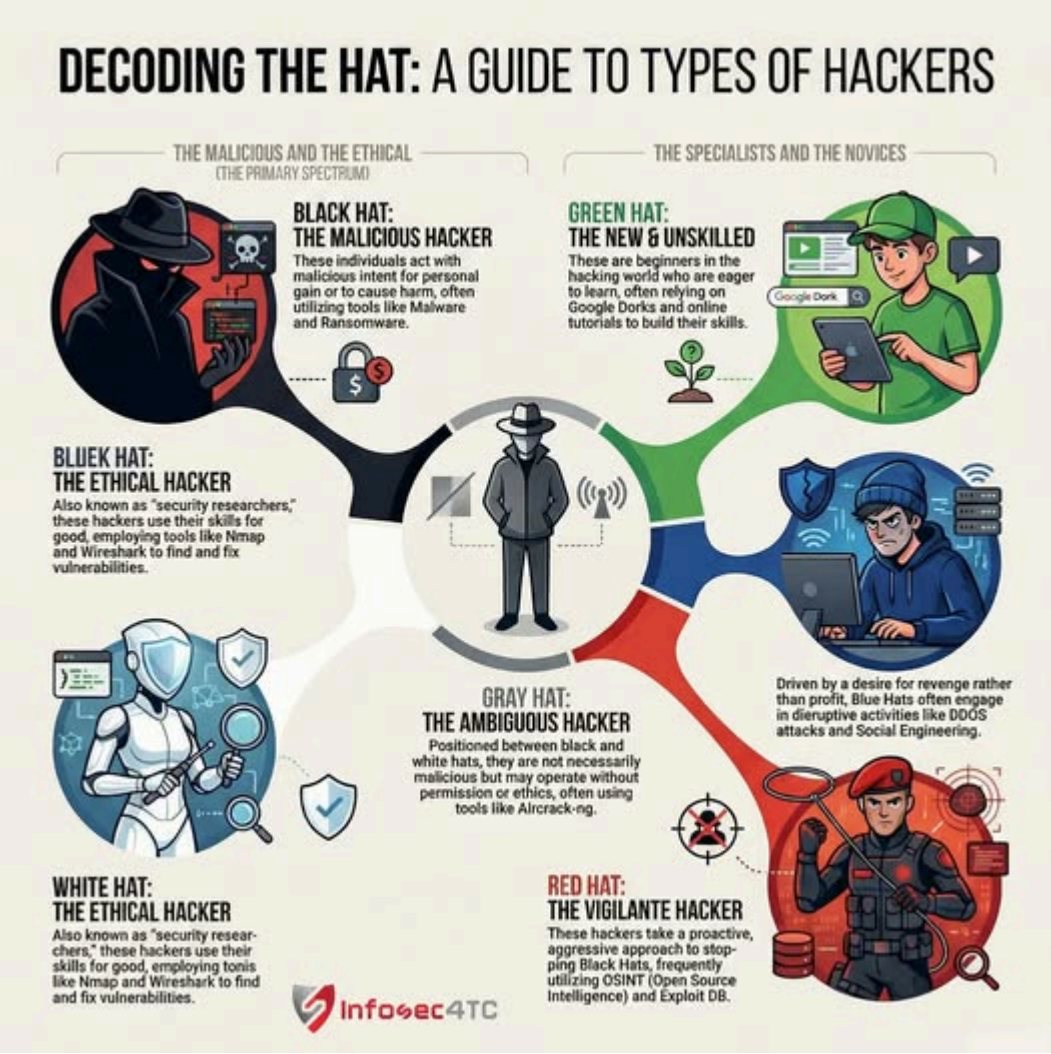
Universidad de Buenos Aires
Facultad de Ciencias Económicas

Los Colores del Hacking

Material de Estudio



Traducción y Comentarios

DECODIFICANDO LOS SOMBREROS: GUÍA DE TIPOS DE HACKERS

1. Black Hat (Sombrero Negro) – *El hacker malicioso*

Definición:

Son individuos con intenciones deliberadamente maliciosas. Utilizan conocimientos técnicos para obtener beneficios personales o causar daño.

Características principales:

- Acceden de forma no autorizada a sistemas de información.
- Roban datos, instalan malware o realizan fraudes.
- Buscan lucro personal, sabotaje o extorsión.

Desde la mirada de TI y la administración:

- Representan un riesgo crítico para la **seguridad de la información**.
- Obligan a las organizaciones a invertir en **controles de acceso, auditorías y ciberseguridad**.
- Impactan directamente en la **continuidad operativa** y en la **reputación institucional**.

---

2. White Hat (Sombrero Blanco) – *El hacker ético*

Definición:

También conocidos como *security researchers* (investigadores de seguridad), utilizan sus habilidades para identificar y corregir vulnerabilidades de manera legal y autorizada.

Características principales:

- Trabajan para organizaciones o como consultores.

- Realizan pruebas de seguridad (*penetration testing*).
- Ayudan a mejorar la protección de los sistemas.

Herramientas mencionadas:

- **Nmap** (Network Mapper – Mapeador de Redes): herramienta para descubrir dispositivos y servicios en una red.
- **Wireshark**: analizador de tráfico de red (packet analyzer).

Desde la mirada de TI y la administración:

- Son clave para la **gestión del riesgo tecnológico**.
- Aportan valor en auditorías de sistemas, cumplimiento normativo y gobernanza de TI.
- Contribuyen a la **toma de decisiones informadas** sobre inversiones en tecnología.

---

3. Blue Hat (Sombrero Azul) – *El evaluador externo*

Definición:

Hacker ético que no pertenece de forma permanente a la organización, pero es invitado para evaluar sistemas antes de su lanzamiento.

Características principales:

- Detectan fallas de seguridad en etapas previas a la puesta en producción.
- Suelen participar en pruebas de productos o sistemas nuevos.

Desde la mirada de TI y la administración:

- Reducen costos futuros al prevenir incidentes.
- Mejoran la calidad y confiabilidad de los sistemas de información.
- Aportan una **visión externa e independiente**.

---

4. Gray Hat (Sombrero Gris) – *El hacker ambiguo*

Definición:

Se ubican entre los *black hat* y los *white hat*. No siempre actúan con intención maliciosa, pero pueden violar normas sin autorización explícita.

Características principales:

- Acceden a sistemas sin permiso, pero sin buscar necesariamente dañar.
- Informan vulnerabilidades después de encontrarlas, a veces de forma informal.

Herramientas mencionadas:

- **Aircrack-ng**: conjunto de herramientas para auditoría de redes Wi-Fi.

Desde la mirada de TI y la administración:

- Plantean dilemas éticos y legales.
- Evidencian la necesidad de **políticas claras de seguridad y compliance**.
- Demuestran que la falta de controles formales genera zonas grises de riesgo.

---

5. Red Hat (Sombrero Rojo) – *El hacker vigilante*

Definición:

Actúan de manera agresiva contra *black hats*, utilizando tácticas ofensivas para detenerlos.

Características principales:

- No priorizan la legalidad, sino el objetivo de frenar ataques.
- Utilizan técnicas similares a las de atacantes maliciosos.

Herramientas mencionadas:

- **OSINT** (Open Source Intelligence – Inteligencia de Fuentes Abiertas): recolección de información pública.
- **Exploit DB** (Exploit Database – Base de Datos de Explotaciones): repositorio de vulnerabilidades conocidas.

Desde la mirada de TI y la administración:

- Refuerzan el debate sobre **justicia, legalidad y control** en TI.

- No son un modelo recomendable para organizaciones formales.
- Destacan la importancia de respuestas institucionales y no individuales.

---

6. Green Hat (Sombrero Verde) – *El principiante*

Definición:

Personas nuevas en el hacking, con entusiasmo por aprender y desarrollar habilidades técnicas.

Características principales:

- Siguen tutoriales, cursos y laboratorios prácticos.
- Cometen errores por falta de experiencia.

Desde la mirada de TI y la administración:

- Representan el **capital humano en formación**.
- Subrayan la necesidad de capacitación formal en seguridad informática.
- Bien orientados, pueden convertirse en futuros *white hats*.

---

7. Script Kiddie – *El usuario sin habilidades profundas*

Definición:

Individuos con conocimientos técnicos limitados que utilizan herramientas desarrolladas por otros.

Características principales:

- Ejecutan ataques sin comprender completamente su funcionamiento.
- Motivaciones comunes: curiosidad, revancha o notoriedad.

Ejemplos de ataques mencionados:

- **DDoS** (Distributed Denial of Service – Denegación de Servicio Distribuida).
- **Social Engineering** (Ingeniería Social): manipulación de personas para obtener información.

Desde la mirada de TI y la administración:

- Aunque técnicamente simples, pueden generar interrupciones operativas.

- Refuerzan la importancia de la **concientización del usuario** y la educación organizacional.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.