Hola futuros hackers!

Les comparto por acá herramientas con las que pueden practicar:

1. Hack the box: Trae una serie de máquinas vulnerables con diferentes sistemas operativos, algunas de estas máquinas aparecen en los laboratorios de la certificación OSCP
2. TryHackMe: Es la plataforma que utiliza el profe para este curso, lo que me gusta de esta es que está gamificada hasta cierto punto y tiene prácticas reales
3. Metasploitable: Es una máquina intencionalmente vulnerable que puedes ejecutar en un entorno virtual, si quieres practicar con metasploit esta puede ser la opción de primera mano
4. OWASP Broken: Después de hack the box, esta es mi favorita para practicar, consiste en una serie de aplicaciones web vulnerables, todas las vulnerabilidades encontradas son conocidas y públicas.

El cracking de contraseñas es el proceso de recuperar contraseñas a partir de datos almacenados o transmitidos mediante diversos métodos, con el objetivo de acceder a sistemas, cuentas o archivos protegidos. A continuación, te presento una descripción general de los métodos comunes de cracking de contraseñas, las herramientas utilizadas y las medidas de defensa.

**Métodos Comunes de Cracking de Contraseñas**

1. **Ataque de Fuerza Bruta**:
   * Probar todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta.
   * **Herramientas**: John the Ripper, Hydra, Hashcat.
2. **Ataque de Diccionario**:
   * Usar una lista de contraseñas comunes o palabras del diccionario.
   * **Herramientas**: John the Ripper, Hydra, Hashcat.
3. **Ataque de Rainbow Tables**:
   * Usar tablas precomputadas de hashes y sus contraseñas correspondientes.
   * **Herramientas**: Rainbow Crack, Ophcrack.
4. **Ataque de Phishing**:
   * Engañar a los usuarios para que revelen sus contraseñas mediante correos electrónicos fraudulentos o sitios web falsos.
   * **Herramientas**: Social Engineering Toolkit (SET), Gophish.
5. **Ataque de Ingeniería Social**:
   * Manipular a las personas para que divulguen sus contraseñas a través de interacciones personales o telefónicas.
6. **Sniffing**:
   * Interceptar y capturar tráfico de red para obtener contraseñas transmitidas en texto claro.
   * **Herramientas**: Wireshark, tcpdump.
7. **Keylogging**:
   * Registrar las pulsaciones de teclas de un usuario para capturar sus contraseñas.
   * **Herramientas**: Spyrix Keylogger, Actual Keylogger.
8. **Exploits y Vulnerabilidades**:
   * Aprovechar vulnerabilidades en software o hardware para obtener contraseñas.
   * **Herramientas**: Metasploit, exploits específicos.

**Herramientas de Cracking de Contraseñas**

1. **John the Ripper**:
   * Herramienta de código abierto para pruebas de contraseñas, especialmente eficaz con hashes.
   * Soporta múltiples tipos de hash y técnicas de cracking.
2. **Hashcat**:
   * Conocida como la herramienta de recuperación de contraseñas más rápida del mundo.
   * Soporta muchos algoritmos de hashing y se puede ejecutar en GPU para mayor velocidad.
3. **Hydra**:
   * Herramienta para ataques de fuerza bruta contra servicios de red.
   * Soporta múltiples protocolos como HTTP, FTP, SSH, y más.
4. **Ophcrack**:
   * Utiliza tablas arco iris para crackear hashes LM y NTLM.
   * Especialmente útil para recuperar contraseñas de Windows.
5. **Cain & Abel**:
   * Herramienta de recuperación de contraseñas para Windows.
   * Puede realizar sniffing de redes, ataques de diccionario, ataques de fuerza bruta, ataques de tablas arco iris y más.
6. **Medusa**:
   * Herramienta de fuerza bruta rápida y masivamente paralela.
   * Soporta muchos protocolos y servicios.

**Medidas de Defensa**

1. **Uso de Contraseñas Fuertes**:
   * Utilizar contraseñas largas y complejas con una combinación de letras, números y caracteres especiales.
2. **Autenticación Multifactor (MFA)**:
   * Implementar MFA para añadir una capa adicional de seguridad.
3. **Políticas de Expiración de Contraseñas**:
   * Establecer políticas para cambiar contraseñas regularmente.
4. **Hashing Seguro**:
   * Almacenar contraseñas usando algoritmos de hashing seguros como bcrypt, scrypt o Argon2.
5. **Salting**:
   * Añadir sal (salt) a las contraseñas antes de hashearlas para prevenir ataques de tablas arco iris.
6. **Educación y Concienciación**:
   * Capacitar a los usuarios sobre la importancia de la seguridad de las contraseñas y los riesgos de phishing y ingeniería social.

**Ejemplo de Uso de John the Ripper**

1. **Crackeo Básico de Contraseñas**:
   * Ejecutar John the Ripper en un archivo de hash:

sh

Copy code

john --wordlist=/path/to/wordlist.txt /path/to/hashfile

1. **Generar Hashes**:
   * Crear un hash para probar:

sh

Copy code

john --stdin --format=raw-md5 --pot=hashes.pot

**Ejemplo de Uso de Hashcat**

1. **Crackeo Básico de Contraseñas**:
   * Ejecutar Hashcat con un archivo de hash y una lista de palabras:

sh

Copy code

hashcat -m 0 -a 0 /path/to/hashfile /path/to/wordlist.txt

Implementar medidas de seguridad robustas es fundamental para proteger sistemas y datos sensibles contra intentos de cracking de contraseñas.

4o