UNIVERSIDAD TÉCNICA DE COTOPAXI

SISTEMAS DE INFORMACIÓN

CONTROL Y AUDITORÍA INFORMÁTICA

TEMA: Evaluación de vulnerabilidades en sistemas de autenticación usando THC-HYDRA

Integrantes:

- Alay Jonathan
- Cisneros Diego
- Espin Anthony
- Zela Cesar

curso: 7°mo

fecha: 10/07/2025

INFORME

1. Introducción

En el presente informe se detalla el análisis de seguridad y control sobre mecanismos de autenticación en aplicaciones web, como parte de las prácticas de la asignatura Control y Auditoría Informática. El enfoque de este estudio fue el uso de la herramienta THC-HYDRA, que forma parte de la distribución Kali Linux, para realizar pruebas de penetración sobre formularios de inicio de sesión desarrollados en Django (Python) y sobre una página de acceso a un sistema real de una institución educativa.

2. Objetivos

Objetivo general:
Evaluar la robustez de los mecanismos de autenticación frente a ataques de fuerza bruta mediante el uso de herramientas de auditoría informática.

Objetivos específicos:

1. Simular un ataque de fuerza bruta usando THC-HYDRA contra un login desarrollado en Django.

2. Identificar posibles vulnerabilidades en el sistema de autenticación de una plataforma escolar.

3. Analizar los resultados y proponer medidas de mejora en seguridad.

3. Metodología

Para el desarrollo de esta práctica de auditoría informática se implementó un enfoque práctico-experimental centrado en la evaluación de vulnerabilidades de autenticación. Se trabajó tanto en un entorno de pruebas desarrollado por los estudiantes como en una plataforma real bajo autorización académica. La metodología seguida se detalla a continuación:

1. **Diseño de entorno de pruebas**:
   Se desarrolló una pequeña aplicación web en el framework **Django**, utilizando Visual

Studio Code como entorno de desarrollo. Esta aplicación contenía un formulario de login básico, sin mecanismos de defensa avanzados como captcha, restricciones por intentos fallidos o validaciones de seguridad robustas. Este entorno permitió recrear una situación real pero controlada, ideal para probar herramientas de auditoría.

2. **Selección y configuración de herramienta de ataque**:
   Se utilizó la herramienta **THC-HYDRA**, una utilidad incluida en Kali Linux ampliamente utilizada para realizar ataques de fuerza bruta sobre protocolos como HTTP, FTP, SSH, entre otros. En este caso, se configuró para atacar el formulario de login vía HTTP POST, especificando el endpoint del formulario, los parámetros (usuario y contraseña), y un diccionario con credenciales comunes o predefinidas.

3. **Pruebas sobre sistema real (plataforma educativa)**:
   Adicionalmente, se identificó un formulario de login de una institución educativa (con fines exclusivamente académicos). La intención fue observar cómo se comportaba una plataforma real ante múltiples intentos de autenticación. En este escenario no se intentó obtener acceso real, sino simplemente verificar si existían mecanismos de defensa como bloqueos de IP, respuestas HTTP específicas (403, 429), redirecciones o bloqueos progresivos.

4. **Recolección y análisis de resultados**:
   Durante la ejecución de los ataques simulados, se documentaron los comportamientos observados en ambas plataformas. Se analizaron los códigos de respuesta HTTP, la cantidad de intentos permitidos, el tiempo de respuesta del servidor, y si existían limitaciones que detuvieran el ataque. Además, se tomaron capturas de pantalla y logs como evidencia del proceso.

5. **Evaluación y documentación**:
   Finalmente, se elaboró el presente informe en el que se describe el proceso completo, los resultados obtenidos y las respectivas recomendaciones de seguridad que deberían aplicarse para evitar este tipo de vulnerabilidades en entornos productivos.

¿Qué es?

THC-HYDRA (también conocida simplemente como **Hydra**) es una herramienta de código abierto utilizada en pruebas de penetración para realizar ataques de fuerza bruta y de diccionario sobre distintos servicios que requieren autenticación, tales como HTTP, FTP, SSH, Telnet, entre otros. Forma parte del conjunto de herramientas de auditoría incluidas en distribuciones como **Kali Linux**.

¿Para qué sirve?

Esta herramienta sirve para evaluar la seguridad de los sistemas de autenticación, detectando si una aplicación web o servicio permite múltiples intentos de acceso sin medidas de protección. THC-HYDRA es ampliamente utilizada por profesionales de seguridad informática

para identificar vulnerabilidades relacionadas con contraseñas débiles, falta de límites en intentos de acceso, y ausencia de mecanismos anti-bot o CAPTCHA.

¿Cómo funciona?
THC-HYDRA funciona enviando múltiples combinaciones de usuario y contraseña (extraídas de diccionarios de texto) a un formulario de autenticación o servicio remoto, a gran velocidad. El atacante configura el tipo de servicio (por ejemplo, HTTP POST para logins web), el archivo de usuarios, el archivo de contraseñas y la dirección del formulario. Hydra intenta conectarse y validar las credenciales una por una, registrando si alguna combinación resulta exitosa. Su velocidad y compatibilidad con múltiples protocolos la convierten en una herramienta eficaz pero que, si no se controla, puede vulnerar la seguridad de sistemas mal protegidos.

4. Resultados

Entorno Django (entorno de pruebas):

- THC-HYDRA logró enviar múltiples combinaciones de usuario y contraseña sin restricción.
- No existían bloqueos temporales ni captcha.
- El login aceptaba múltiples intentos por segundo, lo que lo hacía vulnerable a ataques de fuerza bruta.

Plataforma de la institución educativa:

- Hydra logró enviar varias peticiones antes de recibir respuestas de error HTTP 403 y redirecciones inesperadas.
- No se logró obtener acceso pero se evidenció que no había límite claro de intentos fallidos.
- El sistema no notificaba al usuario sobre actividad sospechosa.

5. Análisis y conclusiones

1. Primero, se recomienda la implementación de **mecanismos de validación adicionales**, como el uso de *CAPTCHA*, especialmente luego de varios intentos fallidos de acceso. Esta medida dificulta significativamente los ataques automatizados y protege el sistema de fuerza bruta.

2. En segundo lugar, es fundamental configurar un **sistema de bloqueo temporal por múltiples intentos fallidos**, ya sea por cuenta de usuario o por dirección IP. Esto permite mitigar ataques sostenidos y da tiempo para que el equipo técnico actúe en caso de detección de actividad inusual.
3. Como tercera recomendación, se sugiere habilitar y revisar periódicamente los **logs de acceso y autenticación** del sistema. Un monitoreo constante de estos registros facilita la detección de patrones sospechosos, como múltiples intentos desde una misma IP o intentos secuenciales con diferentes usuarios.
4. Finalmente, se aconseja implementar **delays o retardos progresivos** entre cada intento fallido de inicio de sesión. Esta técnica reduce la velocidad con la que un atacante puede probar combinaciones, y en combinación con las anteriores, fortalece significativamente la protección contra ataques automatizados.