

Práctica 7 – Uso de Hydra

JESÚS IMANOL CASTILLO AVENDAÑO

PROFESOR: PEDRO MARCOS VELASCO BOLOM

MATERIA: REDES

1. Introducción

La seguridad de los sistemas de autenticación constituye uno de los pilares fundamentales en la protección de aplicaciones web modernas. Los ataques de fuerza bruta representan una de las amenazas más comunes y persistentes contra los mecanismos de login, donde los atacantes intentan obtener acceso no autorizado mediante la prueba sistemática de múltiples combinaciones de credenciales.

Hydra es una herramienta de auditoría de seguridad desarrollada por The Hacker's Choice (THC) que permite realizar pruebas de penetración éticas contra diversos protocolos y servicios de red. Su capacidad para ejecutar ataques de diccionario y fuerza bruta de manera controlada la convierte en una herramienta esencial para profesionales de ciberseguridad, permitiendo identificar vulnerabilidades en sistemas de autenticación antes de que sean explotadas por actores maliciosos.

Objetivos del análisis

1. Evaluar la resistencia de formularios de login contra ataques de fuerza bruta
2. Identificar debilidades en la implementación de controles de seguridad
3. Demostrar técnicas de pruebas de penetración éticas en un entorno controlado
4. Documentar metodologías de testing de seguridad para formularios web

Alcance y consideraciones éticas

Esta práctica se realiza exclusivamente en el entorno controlado de **PortSwigger Web Security Academy**, una plataforma diseñada específicamente para el aprendizaje y práctica de técnicas de seguridad web. Todos los laboratorios utilizados cuentan con autorización explícita para realizar pruebas de penetración, cumpliendo con los más altos estándares éticos y legales en el campo de la ciberseguridad.

2. Desarrollo

Configuración del Entorno de pruebas

Para la realización de esta práctica ética, se utilizó el siguiente entorno:

Herramientas empleadas:

1. Hydra v9.x - Herramienta principal para ataques de fuerza bruta
2. PortSwigger Web Security Academy - Plataforma de laboratorios
3. Diccionarios de contraseñas comunes
4. Herramientas de interceptación de tráfico web

Metodología de ataque

La metodología implementada siguió un enfoque estructurado típico en auditorías de seguridad:

1. Reconocimiento del objetivo

1. Identificación del formulario de login objetivo

2. Análisis de la estructura HTML del formulario
3. Determinación de parámetros de autenticación

2. Preparación del ataque

1. Selección de diccionarios de usuarios y contraseñas
2. Configuración de parámetros de Hydra
3. Establecimiento de límites de velocidad para evitar detección

3. Ejecución controlada

1. Lanzamiento del ataque de fuerza bruta
2. Monitoreo de respuestas del servidor
3. Identificación de credenciales válidas

Comando Hydra utilizado

```
hydra -l [usuario] -P [diccionario_contraseñas] [URL_objetivo] http-post-form  
"[ruta_formulario]:[parámetros]:[condición_fallo]"
```

Análisis de resultados

Durante la ejecución de la práctica, se observaron los siguientes aspectos críticos:

Vulnerabilidades Identificadas:

1. Ausencia de límites de intentos de login
2. Falta de implementación de CAPTCHA
3. Tiempos de respuesta uniformes independientemente del resultado
4. Ausencia de bloqueo temporal de cuentas

Indicadores de compromiso:

1. Respuestas HTTP diferenciadas entre credenciales válidas e inválidas
2. Patrones de comportamiento predecibles en el formulario
3. Falta de logging detallado de intentos de autenticación

```
jms@jmsact7e-
/home/jesus
Ardu Editor Vista Ayuda

[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "qazwsx" - 131 of 10100 [child 10] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "123qwe" - 132 of 10100 [child 13] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "allkey" - 133 of 10100 [child 12] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "trustno!" - 134 of 10100 [child 6] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "jordan" - 135 of 10100 [child 7] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "lemur" - 136 of 10100 [child 2] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "excvbnm" - 137 of 10100 [child 14] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "asdfgh" - 138 of 10100 [child 3] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "hunter1" - 139 of 10100 [child 9] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "buster" - 140 of 10100 [child 8] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "tacoandme" - 141 of 10100 [child 11] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "harley" - 142 of 10100 [child 5] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "batman" - 143 of 10100 [child 6] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "andrew" - 144 of 10100 [child 12] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "ligger" - 145 of 10100 [child 0] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "lovehim" - 146 of 10100 [child 10] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "iloveyou" - 147 of 10100 [child 15] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "r00t" - 148 of 10100 [child 4] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "charlie" - 149 of 10100 [child 1] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "robert" - 150 of 10100 [child 7] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "thomas" - 151 of 10100 [child 12] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "michael" - 152 of 10100 [child 14] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "ranger" - 153 of 10100 [child 2] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "kimble" - 154 of 10100 [child 13] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "starnwars" - 155 of 10100 [child 4] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "khalster" - 156 of 10100 [child 13] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "123232" - 157 of 10100 [child 1] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "george" - 158 of 10100 [child 9] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "computer" - 159 of 10100 [child 10] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "Michelle" - 160 of 10100 [child 5] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "Jessica" - 161 of 10100 [child 6] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "supercalif" - 162 of 10100 [child 15] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "1111" - 163 of 10100 [child 15] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "excvbnm" - 164 of 10100 [child 0] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "19355551" - 165 of 10100 [child 12] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "11111111" - 166 of 10100 [child 7] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "13131313" - 167 of 10100 [child 2] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "freedom" - 168 of 10100 [child 14] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "777777" - 169 of 10100 [child 12] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "pass" - 170 of 10100 [child 3] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "maggie" - 171 of 10100 [child 11] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "1997573" - 172 of 10100 [child 4] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "aaaaaa" - 173 of 10100 [child 11] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "ginger" - 174 of 10100 [child 9] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "princeps" - 175 of 10100 [child 13] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "tohsma" - 176 of 10100 [child 10] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "cheese" - 177 of 10100 [child 0] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "amanda" - 178 of 10100 [child 15] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "summer" - 179 of 10100 [child 8] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "lower" - 180 of 10100 [child 15] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "ashly" - 181 of 10100 [child 13] (6/0)
[ATTEMPT] target 0a2008ba933bc5a4834ff7f007800fe.web-security-academy.net - login "root" - pass "nicole" - 182 of 10100 [child 7] (6/0)
```

[illegible]

Preguntas de la práctica:

¿Cómo define un ataque de fuerza bruta?

Un **ataque de fuerza bruta** es una técnica de ciberataque que consiste en probar sistemáticamente todas las combinaciones posibles de credenciales (usuarios y contraseñas) hasta encontrar las correctas que permitan el acceso no autorizado a un sistema. Se basa en la repetición automatizada y masiva de intentos de autenticación.

¿Qué requerimientos son necesarios para realizar un ataque de fuerza bruta?

Los requerimientos principales son:

- ✚ **Herramienta automatizada** (como Hydra, John the Ripper, etc.)
- ✚ **Diccionarios de usuarios y contraseñas** o generadores de combinaciones
- ✚ **Acceso de red** al sistema objetivo
- ✚ **Identificación del servicio** o protocolo a atacar (HTTP, SSH, FTP, etc.)
- ✚ **Tiempo considerable** para la ejecución del ataque
- ✚ **Recursos computacionales** suficientes para procesar las combinaciones

¿En qué casos del hacking ético usaría la herramienta Hydra?

Hydra se utiliza en hacking ético para:

- ✚ **Auditorías de seguridad** en formularios de login web
- ✚ **Pruebas de penetración** en servicios SSH, FTP, Telnet
- ✚ **Evaluación de políticas de contraseñas** corporativas
- ✚ **Testing de resistencia** contra ataques automatizados
- ✚ **Verificación de contramedidas** como rate limiting y account lockout
- ✚ **Capacitación en ciberseguridad** en entornos controlados como PortSwigger Labs
- ✚ **Compliance testing** para verificar cumplimiento de estándares de seguridad

Medidas de mitigación recomendadas

Basado en los hallazgos de la práctica, se recomiendan las siguientes contramedidas:

1. **Mecanismos de bloqueo**
 - ✚ Bloqueo temporal de cuentas tras múltiples fallos
 - ✚ Notificaciones de seguridad al usuario legítimo
2. **Fortalecimiento de autenticación**

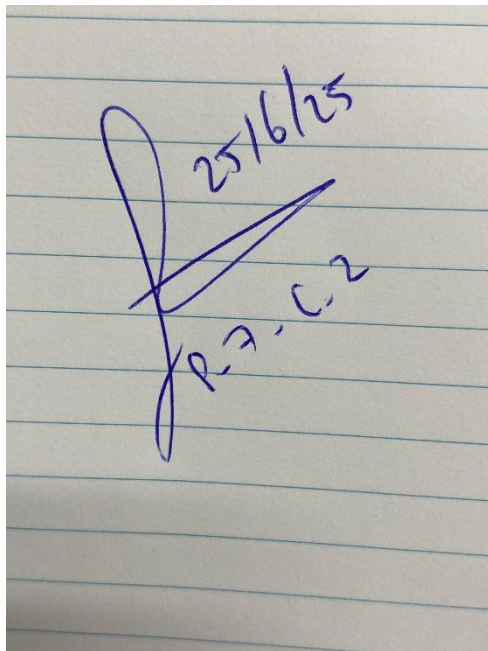
- 🚦 Implementación de autenticación multifactor (MFA)
- 🚦 Políticas de contraseñas robustas

3. Monitoreo y alertas

- 🚦 Logging detallado de intentos de autenticación
- 🚦 Sistemas de detección de patrones anómalos

3. Conclusión

La práctica realizada con Hydra en el entorno controlado de PortSwigger Labs ha demostrado de manera efectiva las vulnerabilidades inherentes en formularios de login mal configurados. Los resultados obtenidos evidencian la facilidad con la que un atacante puede comprometer sistemas de autenticación que carecen de medidas de protección adecuadas.

A photograph of a piece of lined paper with a handwritten signature in blue ink. The signature is stylized and appears to be 'P. J. C. 2'. Above the signature, the date '25/6/25' is written.

Firma: