

# Relatório de Incidente de Segurança

Incidente ao sistema DVWA

## Sumário Executivo

No dia 30 de junho de 2025 às 17h00, a organização tomou conhecimento de múltiplas tentativas de logins e enumeração de diretórios web contra o sistema DVWA, realizado por IPs internos - dentro da organização. O incidente tem nível de criticidade média, foi detectado em tempo real pelo software de monitoramento - Splunk Enterprise - e mitigado rapidamente sem comprometimento de dados

## Sistemas afetados e Ferramentas utilizadas

**Tipo de ataque:** Brute-force SSH e Fuzzing de Diretórios Web

**Ferramentas envolvidas:** Hydra, Dirb, Splunk

**Serviços afetados:** ssh e servidor web

## Cronologia do Incidente

**Data da ocorrência:** 2025-06-30T17:00:00.000-0300  
(30 de junho de 2025 às 17:00, UTC -03:00)

**Data de conhecimento do incidente:** 2025-06-30T17:04:00.000-0300  
(30 de junho de 2025 às 17:04, UTC -03:00)

**Atividades realizadas:**

- **Firewall bloqueia IP do atacante:** 2025-06-30T17:05:00.000-0300
- **Reset da senha da conta atacada:** 2025-06-30T17:09:00.000-0300

- **Acesso ao sistema para auditoria e verificação de integridade de dados:**  
2025-06-30T17:15:00.000-0300
- **Líder da equipe comunicado por e-mail:** 2025-06-30T17:42:00.000-0300

## Evidências do Incidente

Splunk confirmando 33 tentativas de logins ao serviço de SSH de origem do dispositivo 192.168.15.15 ao alvo *srv-vuln*

The screenshot shows a Splunk search interface titled "[T1110] - Brute Force - Linux SSH". The search query is: `index=* sourcetype="linux:audit" Failed password | rex field=message "from\s(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | stats count by src_ip where count > 10`. The time range is set to "from Jun 30 through Jul 1, 2025". The results show 33 events. The table below summarizes the data:

src_ip	host	count
192.168.15.15	srv-vuln	33

Splunk confirmando mais de 13 mil requisições que retornaram status code igual a 404 (não encontrado) e ao lado alguns exemplos de diretórios numerados, indicando uma chance muito alta de ferramenta automática de *fuzzing* (enumeração) de diretórios web

The screenshot shows a Splunk search interface titled "[T1110] - Brute Force - Web directories and files". The search query is: `index=* sourcetype="apache:access:combined" status=404 | stats count values(url) as url by src | where count > 20`. The time range is set to "from Jun 30 through Jul 1, 2025". The results show 13,840 events. The table below summarizes the data:

src	count	url
192.168.15.15	13840	<ul style="list-style-type: none"> <li>/.bash_history</li> <li>/.bashrc</li> <li>/.cache</li> <li>/.config</li> <li>/.cvs</li> <li>/.cvsignore</li> <li>/.forward</li> <li>/.git/HEAD</li> <li>/.history</li> <li>/.listing</li> <li>/.listings</li> <li>/.mysql_history</li> <li>/.passwd</li> <li>/.perf</li> <li>/.profile</li> <li>/.rhosts</li> <li>/.sh_history</li> </ul>

## Avaliação do Impacto

Incidente de criticidade média. Nenhum sistema comprometido. Tentativas foram bloqueadas.

# Causa Raiz

Ataques automatizados via Hydra e Dirb aproveitando autenticação fraca e diretórios previsíveis.

## Mitigação - Ação de resposta

### Contenção

- Bloqueio do IP do atacante via firewall

### Erradicação

- Reset de senha do usuário alvo.
- Remoção de arquivos públicos desnecessários do servidor web.

### Recuperação

- Implementação de autenticação reforçada (chave SSH + 2FA).
- Validação de regras de firewall e análise de novos acessos

## Recomendação e Atividade pós incidente

- Documentação do incidente e das ações realizadas
- Configurar rate-limit na aplicação web
- Recomendação para início do desenvolvimento de playbook automatizado via SOAR
- Atualização na política de complexidade de senha
- O incidente foi encerrado com sucesso e reforçou a importância de uma resposta estruturada