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)

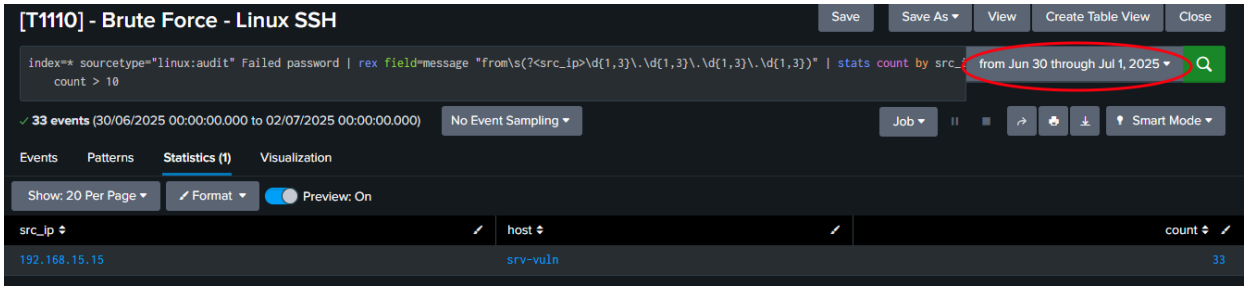
Atividades realizadas:

- **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

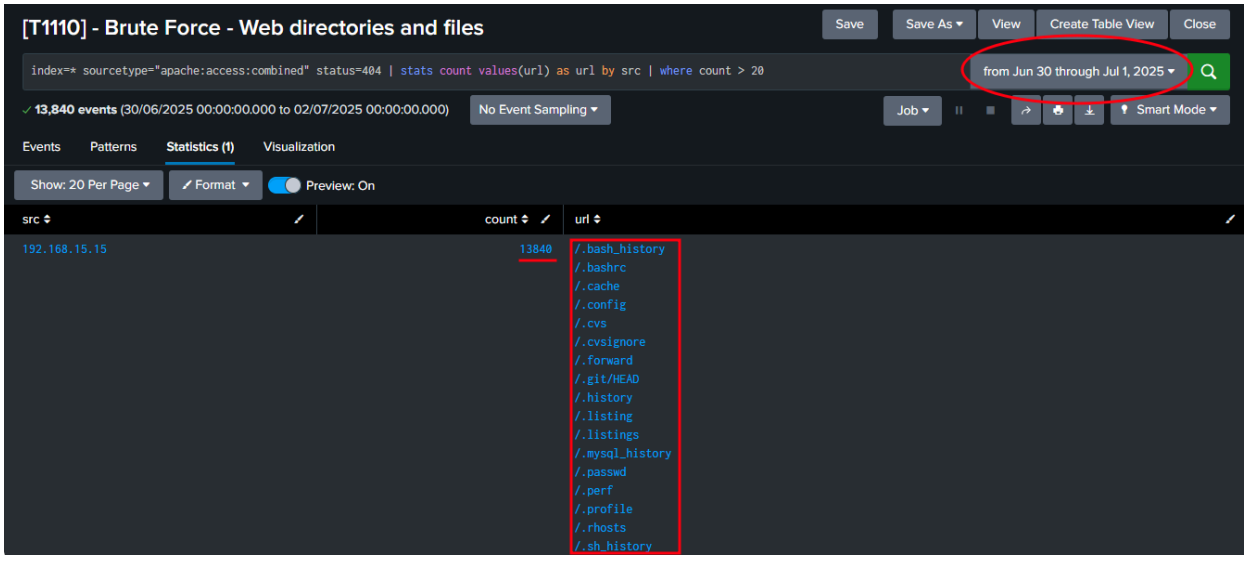
- **Acesso ao sistema para auditoria e verificação de integridade de dados:** 2025-06-30T17:15:00.000-0300
- **Líder da equipe comunicado por e-mail:** 2025-06-30T17:42:00.000-0300

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*



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



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