# HTB: Data

Writeup técnico por Sérgio Muniz

| OS | DIFFICULTY | STATE |
| --- | --- | --- |
| Linux | Easy | Active |

## 0. Metadados da Máquina

- Plataforma: Hack The Box
- Nome da máquina: **Data**
- Sistema operacional: Linux
- Nível de dificuldade: Easy
- Endereço IP do alvo: `10.129.234.47`
- Estado da máquina: Em andamento
- Data da execução: `2025-11-23`
- Autor: `Sérgio Muniz`

## 1. Visão Geral / TL;DR

- Vetor de acesso inicial: ...
- Vulnerabilidade principal: ...
- Foothold: ...
- Escalação de privilégios: ...
- Flags `user` e `root`: ...
- Impacto em ambiente real: ...

## 2. Reconhecimento e Enumeração Inicial

### 2.1. Preparação do ambiente de trabalho

- Estrutura de diretórios: `scans/`, `loot/`, `web/`, `exploit/`, `notes/`.
- Variáveis: `$IP`, `$BOX`, `$TS`, `$WORK`.

```
New-Item -ItemType Directory -Path "$HOME/ctf/env" -Force | Out-Null
$IP = "10.129.234.47"; $BOX = "Data"; $TS = Get-Date -Format "yyyy-MM-dd_HH-mm-ss"; $WORK = "$HOME/ctf/$IP/${BOX}_$TS"; New-Item -ItemType Directory -Path "$WORK/sc
```

### 2.2. Mapeamento de portas e serviços expostos

```
PS [10.10.14.149] /home/smss/ctf/10.129.234.47/Data_2025-11-23_15-18-15 > nmap -Pn -sS -p- -n --min-rate 10000 -vvv -oA "$WORK/scans/full_tcp_allports" $IP
```

Portas identificadas:

| Porta | Protocolo | Serviço | Observações |
| --- | --- | --- | --- |
| 22 | tcp | ssh | OpenSSH exposto para acesso remoto autenticado |
| 3000 | tcp | http (app web) | Redireciona para `/login` |

As demais 65.533 portas foram reportadas como fechadas (`reset`).

```
PS [10.10.14.149] /home/smss/ctf/10.129.234.47/Data_2025-11-23_15-18-15 > nmap -Pn -sCV -p 22,3000 -n -vvv -oA "$WORK/scans/targeted_22_3000" $IP
```

22/tcp: `OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)` → indica **Ubuntu 18.04 Bionic**.

3000/tcp: serviço HTTP retornando `400 Bad Request` para entradas inválidas e `302 Found` para `/login`, com cabeçalhos de segurança básicos e cookie `redirect_to=%2F`. Forte indicação de painel web autenticado na porta 3000.

## 3. Enumeração de Serviços Web (HTTP/HTTPS)

### 3.1. Análise exploratória

- Contexto da aplicação: ...
- Funcionalidades visíveis: ...
- Pontos que chamam atenção: ...

### 3.2. Enumeração automatizada

```
# Comando
```

- Endpoint 1: ...
- Endpoint 2: ...

### 3.3. Funcionalidades e hipóteses de vulnerabilidade

- Pontos de entrada (GET/POST, uploads, APIs): ...
- Comportamentos suspeitos: ...
- Hipóteses: SQLi, LFI, RCE, XSS, etc.: ...

## 4. Foothold (Comprometimento Inicial)

### 4.1. Vulnerabilidade explorada

- Tipo: ...
- Endpoint/parâmetro afetado: ...
- Referências (CVE / artigo / PoC): ...

### 4.2. Cadeia de exploração

```
# Comando
```

- Construção do payload: ...
- Execução e obtenção de shell: ...
- Estabilização da shell: ...

### 4.3. User flag

- Usuário comprometido: ...
- Caminho de `user.txt`: ...

```
# Comando
```

## 5. Enumeração Pós-Foothold

### 5.1. Sistema

- SO e kernel: ...
- Usuários e grupos: ...
- Sudo / cron / serviços: ...

```
# Comando
```

### 5.2. Artefatos sensíveis

- Configs em `/etc`, `/var/www`, `/opt`: ...
- Credenciais, chaves, tokens: ...
- Scripts internos interessantes: ...

```
# Comando
```

## 6. Escalação de Privilégios

### 6.1. Vetor identificado

- Categoria (SUID, sudo, serviço, kernel, etc.): ...
- Evidências: ...
- Referências: ...

### 6.2. Execução

```
# Comando
```

- Passos principais: ...
- Riscos e limitações: ...

### 6.3. Root flag

- Confirmação de contexto `root`: ...
- Caminho de `root.txt`: ...

```
# Comando
```

## 7. Pós-Exploração e Análise

- Dados adicionais relevantes: ...
- Possível movimento lateral / persistência: ...
- Avaliação de risco (CIA): ...
- Medidas de hardening: ...

## 8. Lições Aprendidas

- Conceitos novos: ...
- Ferramentas/técnicas que funcionaram bem: ...
- Erros e caminhos mortos úteis para lembrar: ...

## 9. Apêndice

### 9.1. Linha do tempo de comandos

```
# Comando
```

### 9.2. Referências

- Writeups externos: ...
- Artigos / advisories: ...
- Cheatsheets / docs de ferramentas: ...