Tecnologias Hackers

Rodolfo Avelino e João Eduardo Luisi

Exercício de Análise de Logs - Webservers Apache

Vocês têm em mãos uma sequência de logs coletados de um servidor web Apache que hospeda um sistema desenvolvido em PHP. O objetivo deste exercício é identificar potenciais problemas ou comportamentos suspeitos que possam indicar uma tentativa de ataque ou exploração do sistema.

Abaixo está a sequência de logs extraída:

```
172.68.11.40 - - [02/Mar/2024:05:26:34 -0300] "POST /xmlrpc.php HTTP/1.1"
301 645 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"

172.68.244.55 - - [02/Mar/2024:05:26:34 -0300] "POST /xmlrpc.php HTTP/1.1"
301 645 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"

172.68.11.107 - - [02/Mar/2024:05:26:34 -0300] "POST /xmlrpc.php HTTP/1.1"
301 645 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"

172.68.11.40 - - [02/Mar/2024:05:26:34 -0300] "POST /wp-login.php HTTP/1.1"
301 648 "http://www.tecnologiashackers.com.br/wp-login.php" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.108 Safari/537.36"
```

Com base nos logs fornecidos, que problemas ou comportamentos suspeitos vocês conseguem identificar?

Exercício 2

Vocês têm à disposição outra sequência de logs coletados de um servidor web Apache, mas desta vez em um cenário diferente. O sistema web ainda é desenvolvido em PHP, mas foi detectado um possível comportamento anômalo que pode indicar a exploração de vulnerabilidades ou outras atividades maliciosas.

Abaixo está a sequência de logs extraída:

```
192.168.1.100 - - [10/Mar/2024:14:35:12 -0300] "GET /index.php?user=admin'-- HTTP/1.1" 200 5123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"

192.168.1.101 - - [10/Mar/2024:14:35:15 -0300] "GET /index.php?user=admin' OR '1'='1' -- HTTP/1.1" 200 5321 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"

192.168.1.102 - - [10/Mar/2024:14:35:18 -0300] "GET /index.php?user=admin'; DROP TABLE users; -- HTTP/1.1" 200 5548 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"

192.168.1.103 - - [10/Mar/2024:14:35:21 -0300] "GET /index.php?user=admin'-- HTTP/1.1" 500 1024 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"

192.168.1.104 - - [10/Mar/2024:14:35:24 -0300] "GET /index.php?user=admin' AND '1'='1' -- HTTP/1.1" 500 1001 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
```

Com base nos logs fornecidos, analisem os padrões de comportamento e responda:

Qual tipo de ataque esses logs podem estar indicando?

Exercício 3

Abaixo está a sequência de logs extraída:

```
203.0.113.45 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.45 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.45 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.45 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.45 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.45 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.46 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.46 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.46 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
```

```
203.0.113.46 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200
4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.46 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200
4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.46 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200
4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"

203.0.113.46 - - [15/Mar/2024:08:10:01 -0300] "GET /index.php HTTP/1.1" 200
4876 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36"
```

Com base nesses logs:

Qual tipo de ataque vocês acreditam estar em andamento?