Internship Appliance Goes Wrong

Auteur: bWlrYQ

1. Recon

L'objectif est ici de retrouver le serveur qui a été joint via le protocole HTTP. En revanche les éléments fournis ont été modifiés pour nous compliquer la tâche.

L'échange HTTP ayant été retiré de la capture Wireshark on va commencer par s'intéresser à la capture au format texte en recherchant des éléments "connus" d'un échange HTTP, à savoir "GET, HTTP" et autres joyeuseries

On peut directement retrouver cet échange:

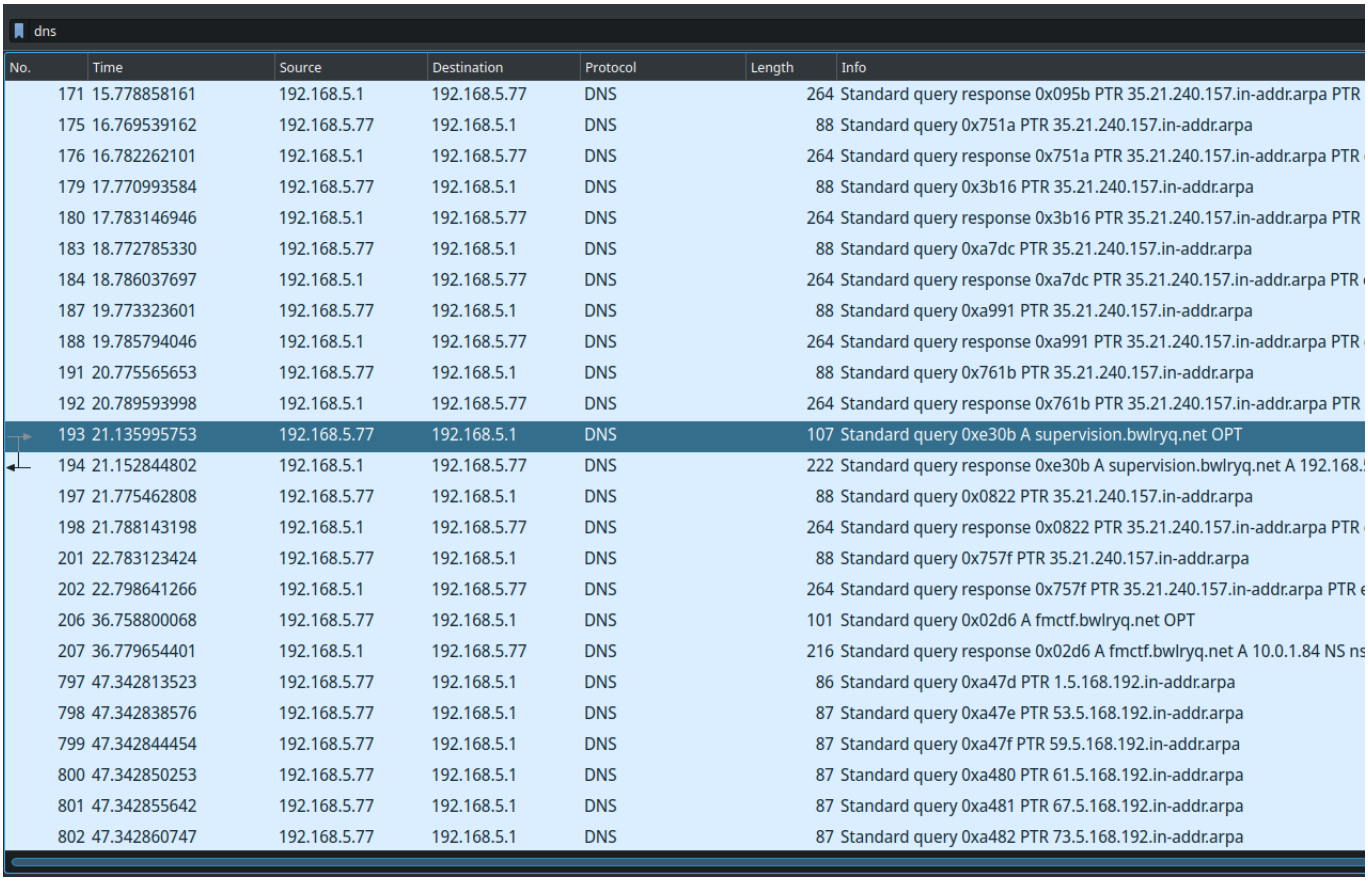
```
0000  00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00   ................
0010  45 00 00 3c ef 40 40 00 40 06 bf 90 c0 a8 05 4d   E..<.@@.@......M
0020  ?? ?? ?? ?? e1 9a 00 50 63 f0 6a 8a 00 00 00 00   ...M...Pc.j.....
0030  a0 02 ff d7 8c 19 00 00 02 04 ff d7 04 02 08 0a   ................
0040  82 2d d0 14 00 00 00 00 01 03 03 07               .-..........

0000  00 00 03 04 00 06 00 00 00 00 00 00 00 01 08 00   ................
0010  45 00 00 3c 00 00 40 00 40 06 ae d1 ?? ?? ?? ??   E..<..@.@......M
0020  c0 a8 05 4d 00 50 e1 9a bf f6 bf 1f 63 f0 6a 8b   ...M.P......c.j.
0030  a0 12 ff cb 8c 19 00 00 02 04 ff d7 04 02 08 0a   ................
0040  82 2d d0 14 82 2d d0 14 01 03 03 07               .-...-......

0000  00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00   ................
0010  45 00 00 34 ef 41 40 00 40 06 bf 97 c0 a8 05 4d   E..4.A@.@......M
0020  ?? ?? ?? ?? e1 9a 00 50 63 f0 6a 8b bf f6 bf 20   ...M...Pc.j....
0030  80 10 02 00 8c 11 00 00 01 01 08 0a 82 2d d0 14   .............-..
0040  82 2d d0 14                                       .-..

0000  00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00   ................
0010  45 00 00 8a ef 42 40 00 40 06 bf 40 c0 a8 05 4d   E....B@.@..@...M
0020  ?? ?? ?? ?? e1 9a 00 50 63 f0 6a 8b bf f6 bf 20   ...M...Pc.j....
0030  80 18 02 00 8c 67 00 00 01 01 08 0a 82 2d d0 14   .....g.......-..
0040  82 2d d0 14 47 45 54 20 2f 20 48 54 54 50 2f 31   .-..GET / HTTP/1
0050  2e 31 0d 0a 48 6f 73 74 3a 20 73 75 70 65 72 76   .1..Host: superv
0060  69 73 69 6f 6e 2e 62 77 6c 72 79 71 2e 6e 65 74   ision.bwlryq.net
0070  0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 63 75   ..User-Agent: cu
0080  72 6c 2f 37 2e 38 35 2e 30 0d 0a 41 63 63 65 70   rl/7.85.0..Accep
0090  74 3a 20 2a 2f 2a 0d 0a 0d 0a                     t: */*....
```

2. Analsye et Wireshark

C'est un échange TCP (on le reconnaît aux trois requêtes TCP, SYN, SYN-ACK et SYN-ACK) du quel se suit une requête HTTP GET. L'adresse IP a été soigneusement effacée par notre maître de stage mais il a oublié le plus

important.

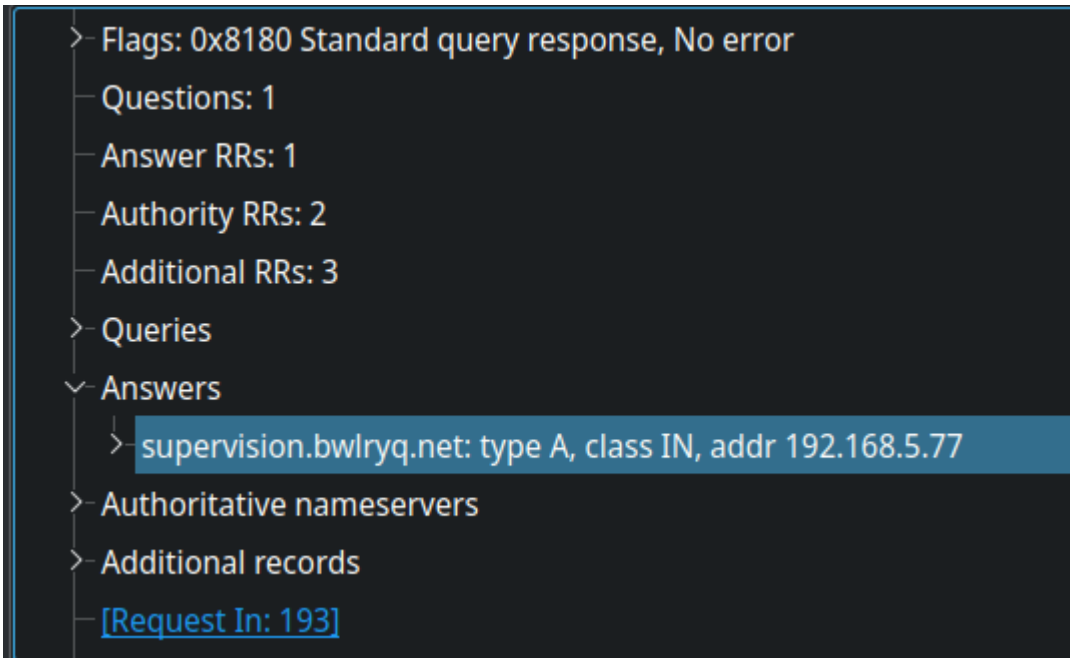
Seul l'échange HTTP a été retiré de la capture, les requêtes DNS elles, devraient toujours être présentes. Dans la requête HTTP on peut voir le nom de domaine et la machine qui a été jointe. Il nous suffit maintenant d'analyser le protocole DNS dans la capture wireshark.



dns

No.	Time	Source	Destination	Protocol	Length	Info
171	15.778858161	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0x095b PTR 35.21.240.157.in-addr.arpa PTR
175	16.769539162	192.168.5.77	192.168.5.1	DNS	88	Standard query 0x751a PTR 35.21.240.157.in-addr.arpa
176	16.782262101	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0x751a PTR 35.21.240.157.in-addr.arpa PTR
179	17.770993584	192.168.5.77	192.168.5.1	DNS	88	Standard query 0x3b16 PTR 35.21.240.157.in-addr.arpa
180	17.783146946	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0x3b16 PTR 35.21.240.157.in-addr.arpa PTR
183	18.772785330	192.168.5.77	192.168.5.1	DNS	88	Standard query 0xa7dc PTR 35.21.240.157.in-addr.arpa
184	18.786037697	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0xa7dc PTR 35.21.240.157.in-addr.arpa PTR
187	19.773323601	192.168.5.77	192.168.5.1	DNS	88	Standard query 0xa991 PTR 35.21.240.157.in-addr.arpa
188	19.785794046	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0xa991 PTR 35.21.240.157.in-addr.arpa PTR
191	20.775565653	192.168.5.77	192.168.5.1	DNS	88	Standard query 0x761b PTR 35.21.240.157.in-addr.arpa
192	20.789593998	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0x761b PTR 35.21.240.157.in-addr.arpa PTR
193	21.135995753	192.168.5.77	192.168.5.1	DNS	107	Standard query 0xe30b A supervision.bwlryq.net OPT
194	21.152844802	192.168.5.1	192.168.5.77	DNS	222	Standard query response 0xe30b A supervision.bwlryq.net A 192.168.
197	21.775462808	192.168.5.77	192.168.5.1	DNS	88	Standard query 0x0822 PTR 35.21.240.157.in-addr.arpa
198	21.788143198	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0x0822 PTR 35.21.240.157.in-addr.arpa PTR
201	22.783123424	192.168.5.77	192.168.5.1	DNS	88	Standard query 0x757f PTR 35.21.240.157.in-addr.arpa
202	22.798641266	192.168.5.1	192.168.5.77	DNS	264	Standard query response 0x757f PTR 35.21.240.157.in-addr.arpa PTR
206	36.758800068	192.168.5.77	192.168.5.1	DNS	101	Standard query 0x02d6 A fmctf.bwlryq.net OPT
207	36.779654401	192.168.5.1	192.168.5.77	DNS	216	Standard query response 0x02d6 A fmctf.bwlryq.net A 10.0.1.84 NS ns
797	47.342813523	192.168.5.77	192.168.5.1	DNS	86	Standard query 0xa47d PTR 1.5.168.192.in-addr.arpa
798	47.342838576	192.168.5.77	192.168.5.1	DNS	87	Standard query 0xa47e PTR 53.5.168.192.in-addr.arpa
799	47.342844454	192.168.5.77	192.168.5.1	DNS	87	Standard query 0xa47f PTR 59.5.168.192.in-addr.arpa
800	47.342850253	192.168.5.77	192.168.5.1	DNS	87	Standard query 0xa480 PTR 61.5.168.192.in-addr.arpa
801	47.342855642	192.168.5.77	192.168.5.1	DNS	87	Standard query 0xa481 PTR 67.5.168.192.in-addr.arpa
802	47.342860747	192.168.5.77	192.168.5.1	DNS	87	Standard query 0xa482 PTR 73.5.168.192.in-addr.arpa

On peut voir la query DNS pour supervision.bwlryq.net, on peut donc regarder la réponse pour obtenir l'IP du serveur.



Le flag est donc FMCTF{192.168.5.77}