

# PcapPoisoning Forensics

Description:

How about some hide and seek heh?

Solution:

- 1) We retrieve the website data in the picoCTF webshell using wget.

```
shouvik028-picoctf@webshell:~$ strings trace.pcap
strings: 'trace.pcap': No such file
shouvik028-picoctf@webshell:~$ strings trace(1).pcap
bash: syntax error near unexpected token '('
shouvik028-picoctf@webshell:~$ strings trace.pcap
strings: 'trace.pcap': No such file
shouvik028-picoctf@webshell:~$ wget https://artifacts.picoctf.net/c/376/trace.pcap
--2023-11-16 16:23:53-- https://artifacts.picoctf.net/c/376/trace.pcap
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 3.160.22.128, 3.160.22.43, 3.160.22.92, ...
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|3.160.22.128|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 106715 (104K) [application/octet-stream]
Saving to: 'trace.pcap'

trace.pcap
100%[=====>] 104.21K --.-KB/s in 0.09s

2023-11-16 16:23:53 (1.96 MB/s) - 'trace.pcap' saved [106715/106715]

shouvik028-picoctf@webshell:~$ strings trace.pcap
username root password toorC~
!BwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
picoCTF{P64P_4N4L7S1S_SU55355FUL_f621fa37}C~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
```

- 2) Then we search for strings on the website.
- 3) We get a lot of strings and among them is our flag.

```
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
picoCTF{P64P_4N4L7S1S_SU55355FUL_f621fa37}C~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
gc2VjcmV0OiBwaWNVQRGeC~
```

Flag: picoCTF{P64P\_4N4L7S1S\_SU55355FUL\_f621fa37}