

SusPaquet

Auteur: bWlrYQ

1. Recon

La capture semble de prime abord tout à fait banale, il n'y a que des protocoles de base en revanche on peut remarquer que le buffer ICMP n'est pas celui par défaut et qu'il change à chaque echo request.

192 19.680271869

10.0.1.84

10.0.1.76

ICMP

196 19.885251888

10.0.1.84

10.0.1.76

ICMP

198 20.103520123

10.0.1.84

10.0.1.76

ICMP

202 20.306936895

10.0.1.84

10.0.1.76

ICMP

206 20.510670122

10.0.1.84

10.0.1.76

ICMP

0000 00 03 00 01 00 06 08 00 27 4a d8 9b 08 00 08 00 'j'.....

0010 45 00 00 54 76 a6 00 00 40 01 ed 63 0a 00 01 54 E·Tv· @·c·T

0020 0a 00 01 4c 00 00 cb b6 2d 7c 00 01 89 86 3d 63 ...L· -|· =c

0030 00 00 00 00 93 37 02 00 00 00 00 00 55 55 55 557·UUUU

0040 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU

0050 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 UUUUUUUU UUUUUUUU

196 19.885251888

10.0.1.84

10.0.1.76

ICMP

198 20.103520123

10.0.1.84

10.0.1.76

ICMP

202 20.306936895

10.0.1.84

10.0.1.76

ICMP

206 20.510670122

10.0.1.84

10.0.1.76

ICMP

0000 00 03 00 01 00 06 08 00 27 4a d8 9b 00 00 08 00 'j'.....

0010 45 00 00 54 76 c9 00 00 40 01 ed 40 0a 00 01 54 E·Tv· @·@·T

0020 0a 00 01 4c 00 00 18 2a 9c 93 00 01 89 86 3d 63 ...L·*=c

0030 00 00 00 00 7f 57 05 00 00 00 00 00 ff ff ff ffW·

0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

198	20.103520123	10.0.1.84	10.0.1.76	ICMP
202	20.306936895	10.0.1.84	10.0.1.76	ICMP
206	20.510670122	10.0.1.84	10.0.1.76	ICMP

0000	00 03 00 01 00 06 08 00	27 4a d8 9b 08 00 08 00 'J'.....
0010	45 00 00 54 76 fb 00 00	40 01 ed 0e 0a 00 01 54	E·Tv· @·····T
0020	0a 00 01 4c 00 00 6b 25	c3 41 00 01 89 86 3d 63	··L·k% ·A·····c
0030	00 00 00 00 02 ae 08 00	00 00 00 00 33 33 33 33	······ ···3333
0040	33 33 33 33 33 33 33 33	33 33 33 33 33 33 33 33	33333333 33333333
0050	33 33 33 33 33 33 33 33	33 33 33 33 33 33 33 33	33333333 33333333

Quand on regarde encore plus le charset utilisé est celui de l'hexadécimal, on peut essayer de décoder ça en prenant la première lettre du buffer à chaque fois.

2. Décodage et flag

On peut faire ce sympathique one-liner 😊

```
tshark -r susPaquet.pcapng -Y '(ip.src==10.0.1.76 && icmp)' -x | grep "^0050" |
cut -d ' ' -f 3 | cut -c1 | tr -d '\n' | xxd -r -p
```

Et voilà:

```
mika@bwlryg ~/D/c/r/S/solve [main ✚1] ./rw
$ tshark -r ./susPaquet.pcapng -Y '(ip.src==10.0.1.76 && icmp)' -x | grep "^0050" | cut -d ' ' -f 3 | cut -c1 | tr -d '\n' | xxd -r -p
FMCTF{IcMp_1sNt_CompLicAtEd_!!!}
```

Flag: FMCTF{IcMp_1sNt_CompLicAtEd_!!!}

Note: mes compliments à ceux qui le feront à la main, vous avez du courage 😊))