Write-Up: Null Traffic (Forensics)

Ομάδα: mousiko_gymsasio_agriniou_lt_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

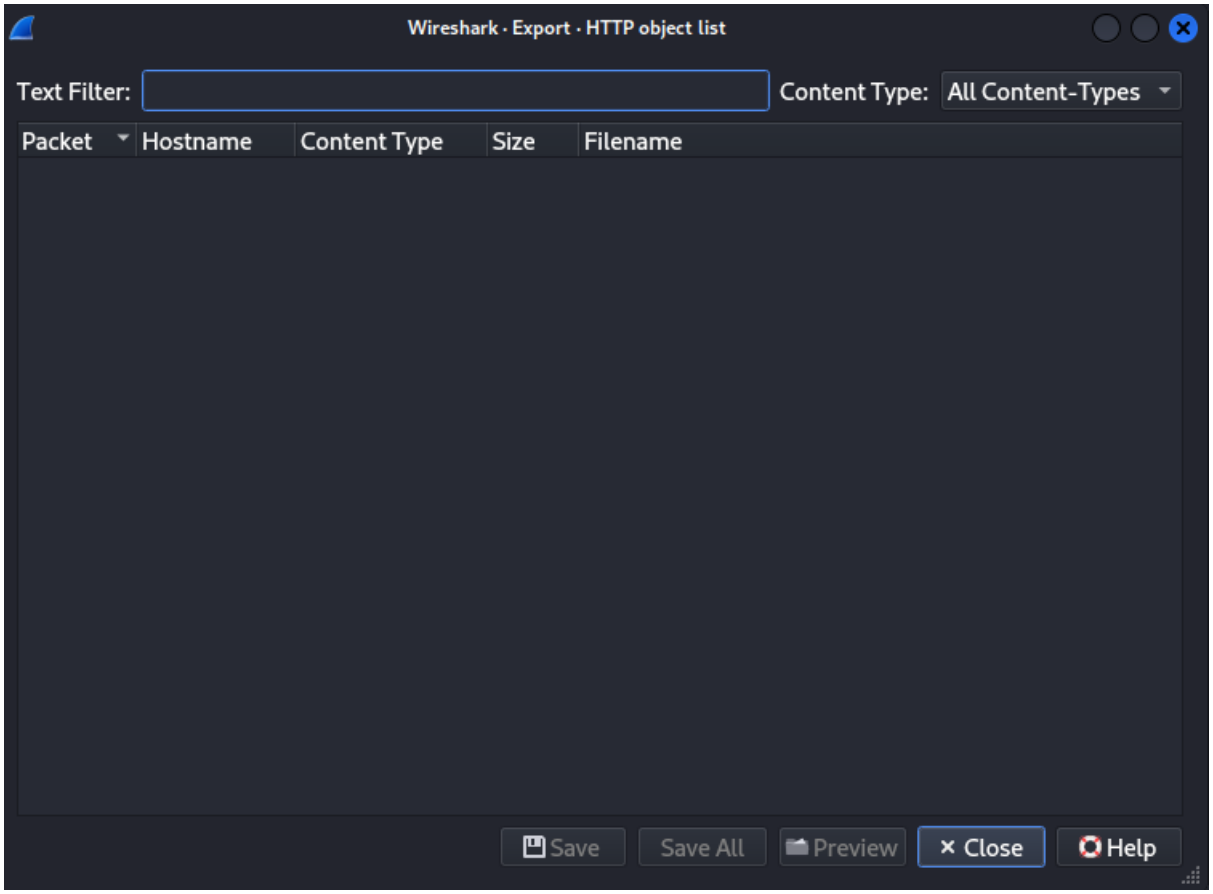
Επισκόπηση Δοκιμασίας

Η συγκεκριμένη δοκιμασία μας δίνει ένα αρχείο με επέκταση .pcap. Αυτού του είδους τα αρχεία αποθηκεύουν πακέτα στο ίντερνετ.

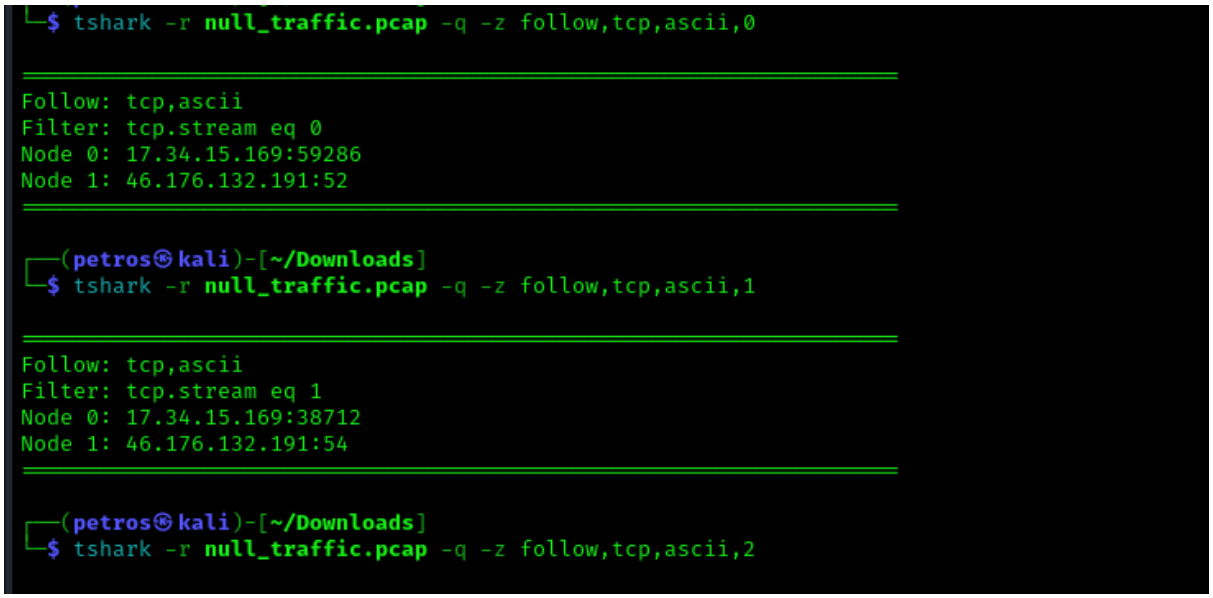
Επίλυση

Αρχική ανάλυση

Αρχικά σκέφτηκα ότι μπορεί να κατεβαίνει κάποιο αρχείο από το διαδίκτυο. Για αυτό έκανα export objects με http αλλά τίποτα.



Μετά σκέφτηκα ότι μπορεί να βρίσκονται δεδομένα μέσα σε tcp streams. Όμως η εντολή “tshark -r null_traffic.pcap -q -z follow,tcp,ascii,0” δεν μου έβγαζε αποτέλεσμα για κανένα πακέτο.



Τέλος, σκέφτηκα ότι μπορεί να υπάρχει κάποια πατέντα στα απλά δεδομένα, όπως οι πόρτες.

Εκμετάλλευση ευπάθειας

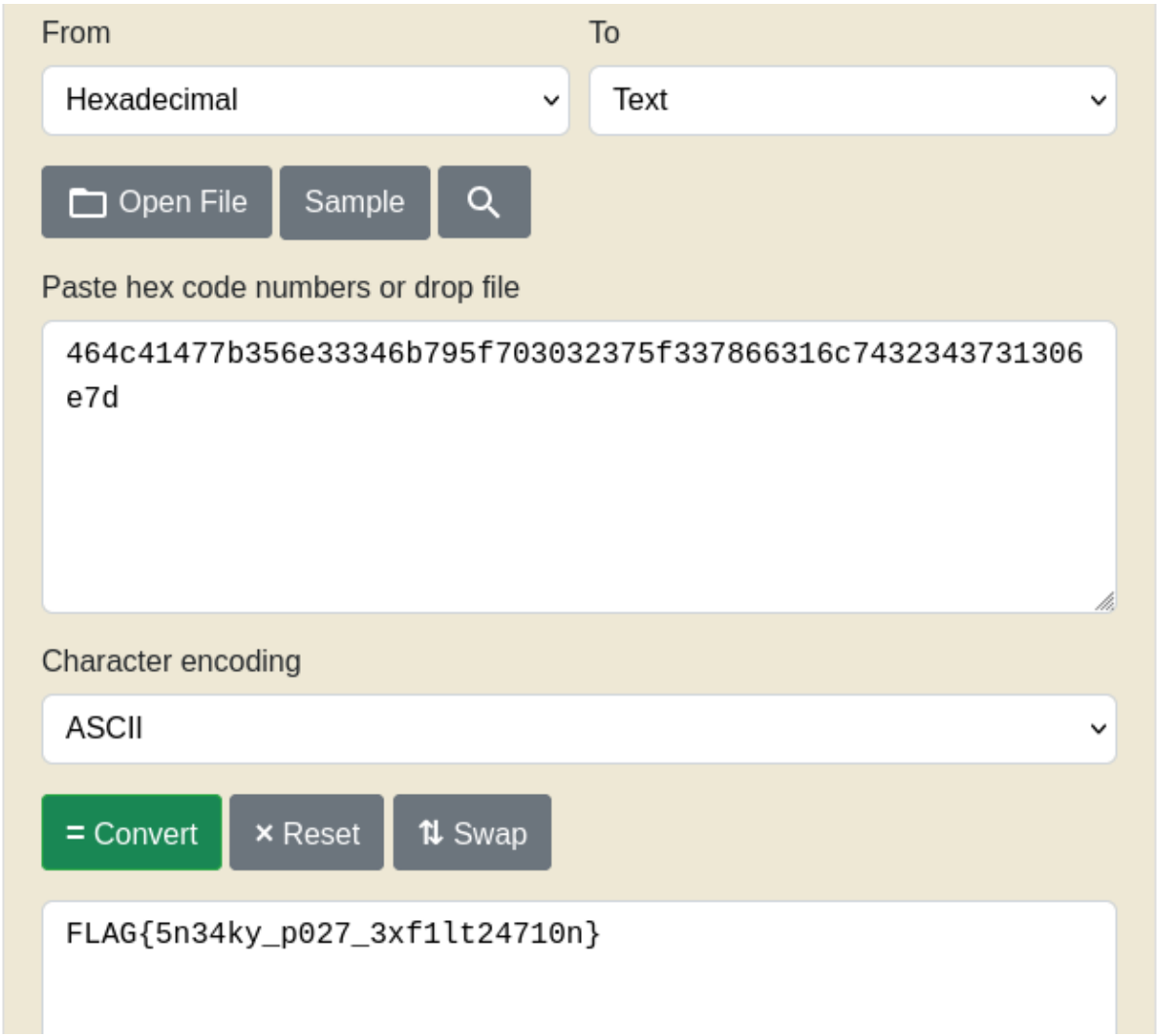
Αν βάλουμε τις destination πόρτες ως χαρακτήρες ascii θα εμφανιστεί ένα περίεργο μήνυμα.

```
dest_ports = [
    52, 54, 52, 99, 52, 49, 52, 55, 55, 98,
    51, 53, 54, 101, 51, 51, 51, 52, 54, 98,
    55, 57, 53, 102, 55, 48, 51, 48, 51, 50,
    51, 55, 53, 102, 51, 51, 55, 56, 54, 54,
    51, 49, 54, 99, 55, 52, 51, 50, 51, 52,
    51, 55, 51, 49, 51, 48, 54, 101, 55, 100
]

decoded_text = "".join([chr(p) if 32 <= p <= 126 else "_" for p in dest_ports])
print(decoded_text)
```

```
$ python3 ports.py
464c41477b356e33346b795f703032375f337866316c7432343731306e7d
```

Αρχικά, νόμιζα ότι αυτό το μήνυμα ήταν base64,αλλά τελικά είναι hexadecimal. Με έναν online Converter μετέτρεψα τους χαρακτήρες ascii σε κείμενο και πήρα την σημαία.



Σημαία

Η σημαία που βρέθηκε:

```
FLAG{5n34ky_p027_3xf1lt24710n}
```