Gobuster

AND ENUMERATION IN GENERAL

Τι πάει να πει enumeration

- Πρόκειται για επόμενο στάδιο του reconnaissance.

- Αφού έχουμε εντοπίσει τον στόχο (IP, services etc.), προσπαθούμε να εξαγάγουμε ό,τι πληροφορία για αυτόν μπορούμε (usernames, directories, machine/share names κτλ).

- Συνήθως γίνεται με κάποιον αυτοματοποιημένο τρόπο με εργαλεία όπως το gobuster, wpscan, nmap scripts για enumeration κ.α.

Gobuster

- Ακραίο tool, είναι γραμμένο σε golang (Παναγία μου) και κάνει uri, dns, cloud enumeration.
- Προεγκατεστημένο στα kali linux, αλλιώς εγκατάσταση μέσω

```
sudo apt install gobuster
```

- Η εντολή gobuster γενικά συντάσσεται ως εξής*:

```
gobuster MODE -u/-d URI -w WORDLIST OPTIONAL_FLAGS
```

e.g.

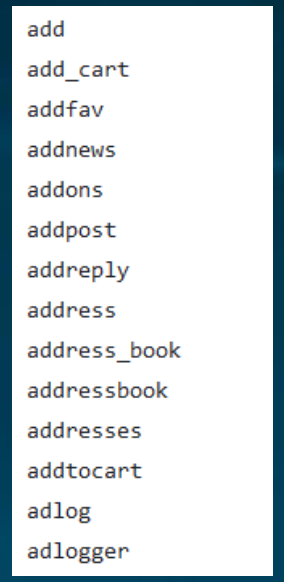
```
gobuster dir -u http://www.google.com -w ~/common.txt -t 50
```

*Η παραπάνω σύνταξη αφορά το gobuster στα kali. Στα ubuntu νομίζω διαφέρει ελαφρώς η σύνταξη. Χρησιμοποιήστε τη σημαία –help για να δείτε τη σωστή σύνταξη στα ubuntu

Wordlists

- Wordlist: Όπως λέει και το όνομα, πρόκειται για λίστα με λέξεις. Μία λέξη σε κάθε γραμμή.
- Στην περίπτωση του enumeration, τα wordlists που θα χρησιμοποιήσουμε περιέχουν τα πιο κοινώς χρησιμοποιούμενα paths σε URLs (π.χ. admin, login, register κτλ)
- Συνήθως δημιουργούνται ανάλογα με το εκάστοτε framework (π.χ. διαφορετικό wordlist θα χρησιμοποιήσεις για WordPress και διαφορετικό για Joomla enumeration)
- Σημείωση: Στα περισσότερα challenges (machines) χρησιμοποιούμε το wordlist common.txt. Στα kali, το path του wordlist είναι /usr/share/wordlists/dirb/common.txt, αλλιώς το κατεβάζουμε με την εντολή:

```
wget https://github.com/v0re/dirb/raw/master/wordlists/common.txt
```



Πιο αναλυτικά

- Το gobuster θα πάρει κάθε μία από τις λέξεις ενός wordlist και θα τις κάνει append στο url. Στη συνέχεια θα πραγματοποιήσει ένα request στο νέο URL και αν γυρίσει επιθυμητό status code (π.χ. 200), θα βγάλει στην οθόνη ότι το URL υπάρχει.
- Π.χ. για το wordlist = {stuff, hidden, secret} και το url http://www.mysite.com, το gobuster θα δοκιμάσει τα:

http://www.mysite.com/stuff, http://www.mysite.com/hidden και http://www.mysite.com/secret

Αν ο server απαντήσει πχ με 200 OK σε κάποιο από αυτά τα αιτήματα, το gobuster θα καταλάβει ότι το path υπάρχει και θα το επιστρέψει ως output.

Παράδειγμα εκτέλεσης gobuster

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir --url http://example.com -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://example.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 1256]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Gobuster Modes

Το gobuster υποστηρίζει τα ακόλουθα modes:

- dir: Αυτό χρησιμοποιούμε συνήθως και είναι αυτό που δοκιμάζει τα διαφορετικά URL paths
- dns: Χρησιμοποιείται για εύρεση subdomains (π.χ. στο google.com θα βρει το chrome.google.com)
- fuzz: Δίνει μεγαλύτερη ευελιξία στο enumeration επιτρέποντάς σου να χρησιμοποιήσεις το dummy keyword **FUZZ**, το οποίο θα αντικατασταθεί με την εκάστοτε λέξη του wordlist κατά το enumeration.
- s3/gcs: Amazon, Google cloud enumeration

Some useful flags

Κάποιες χρήσιμες σημαίες/επιλογές του gobuster φαίνονται παρακάτω:

-t *THREAD_NUM* : Πόσα threads θα χρησιμοποιήσει το gobuster (aka ταχύτητα σάρωσης). Default: 10.

-m *METHOD* : Ποια μέθοδο θα χρησιμοποιήσει το gobuster κατά το enumeration. Default: GET.

-c *COOKIE* : Το cookie που θα χρησιμοποιηθεί κατά το request. Default: None.

--status-codes(-blacklist): Καθόρισε τους positive (negative) status codes.

--exclude-length *LENGTH* : Μην εμφανίσεις URIs με περιεχόμενο μήκους LENGTH. Χρήσιμο για φιλτράρισμα των αποτελεσμάτων.

Useful material

- https://academy.hackthebox.com/module/details/77?redirect_to_section=728 (HackTheBox Academy web enumeration module)
- https://github.com/OJ/gobuster (gobuster's github page) or

https://hackertarget.com/gobuster-tutorial/ (gobuster tutorial)

- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/enumeration-ethical-hacking/ (Enumeration and its importance)