# Subdomain Enumeration 2

بص بقي يامعلم احنا هنتعلم انهارده طرق Advanced اكتر عشان نقدر نجيب domains اكتر

## Bulid Apache Server on your Machine

---

- بص بقي انا عاوز دلوقتي نتعلم ازاي نشغل سيرفر الاباتشي وهعرفك ليه بعدين

```
sudo systemctl start apache2.server
```

```
sudo systemctl enable apache2.server
```

- كده انت شغلت السيرفر معني كده ان جهازك بقي عباره عن سيرفر ويب بس طبعا برايفت خاص بيك انت بس يعني اي حد هيحاول يفتحه مش هيعرف ده علي جهازك انت بس عاوز تخليه بابليك في اداة زي ngrok مثلا بتديك public ip بس ده مش موضوعنا دلوقتي
- المهم ده عباره عن سيرفر ويب حلو اوي طيب فين ملفات الويب او المسار بتاعه اللي بيجيب ملفات الويب منه اقولك الكالي عملالك ملف افتراضي هو بيجيب منه `var/www/html/` هو الdir ده والملف الرئيسي اللي هو `index.html`
- يعني اللي مكتوب ف الindex.html هو اللي هتلاقيه لما تفتح الlocalhost عشان تشوف بقي اللي مكتوب فالفايل وتفتح تكتب فالمتصفح `localhost/` او تكتب الip اللي هو `127.0.0.1` اكيد انت عارف الكلام احنا درسناه قبل كده
- حد هيجي يقولي ياعم هو كل شويه هروح اكتب localhost او الip دول تقال اوي وانا بكسل
- اقولك تعالي نغير الهوست نخليه حاجه تانيه

-اول حاجه نخش علي المسار الخاص بالهوستات اللي هو `nano etc/hosts`

```
 GNU nano 8.2                                /etc/hosts
127.0.0.1       localhost
127.0.0.1       tantawy
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

-بص هنا عملت هتلاحظ ان ال127.0.0.1 ip جمبيه localhost وده الاسم الافتراضي

-هنا بقي انا ضيفت نفس الip بس لدومين تاني باسم tantawy

-فاكر قبل كده لما قولتلك ان السيرفر ممكن يشيل اكتر من دومين هو بالظبط ده كده جهازك عباره عن سيرفر وانت بتحطلو اكتر من دومين

-وكده نكون طبقنا علي الVirtual Host فاكره؟ اللي هو كان معناه ان السيرفر يقدر يشيل اكتر من Domain واكتر من Subdomain يعني ممكن تلاقي موقعين علي نفس السيرفر بالsubdomains بتوعهم اقولك اه عادي

-وطبعا لو كتبت `tantawy/` فالمتصفح هيفتح عادي

## ffuf Tool and Internal Subdomain Finder

- طبعا احنا عرفنا الVirtual Host وعرفنا ان ممكن سيرفر يشيل اكتر من Subdomian بس خلي بالك لأني بيكون في subdomains داخليه بمعني ان مينفعش انت تدخل للsubdomain الا لما تكون انت متصل بالشبكه بتاعت الشركه عندهم اصلا
- بص خليني اديك مثال حلو انت دلوقتي بتحاول تطلع الSubdomains بتوع فيسبوك فا لقيت ده مثلا `help.facebook.com` ده عادي لو حطيتو فالبراوزر هيشتغل عادي بس تعالي وانت بتدور فالsubdomains طلعلك `admin.facebook.com` تفتكر انه هيفتح؟ اكيد لأ لازم تكون من المهندسين بتوع الفيسبوك وتكون لاقط من الشبكه بتاعت الفيس فالشركه نفسها عشان يفتح.....طب انا كا هاكر افتحو ازاي؟ هقولك بس اتقل نتعلم ازاي نجيب subdomains الأول بالffuf
- فكرة الffuf انها بتعمل Fuzzing وبتخمن اسم الsubdomain عن طريق اني بديلو wordlist وهو يشتغل بقي ومن اشهر الwordlists فالموضوع ده هيا Seclists
- فال ffuf انا بحطله كلمة FUZZ فالحته اللي عاوزه يخمنلي فيها

```
ffuf -u http://FUZZ.mars.com -w wordlist/seclists/dicovery/dns
```

- هنا عملت `FUZZ.mars.com` لأني طبيعي الsubdomain بيكون حاجه وبعد كده mars.com صح؟ فا انا بقولو خمنلي الحته دي
- ودي طريقه عاديه لو عاوز اجيب الsubdomains العاديين

```
ffuf -u http://mars.com "Host: FUZZ.mars.com" -w wordlist/seclists/dicovery/dns
```

- دي بقي بص انا قولتلو هنا ايه `"Host: FUZZ.mars.com"` يعني قولتلو ياباشا ابعتلي طلب للسيرفر وجرب تعمل Fuzzing ف خانه الhost فالريكويست ودي تفيدني بأنها ممكن تطلعلي Internal Subdomains عن الطريقه الاولي

*ملحوظه: يفضل انك متحطش الdomain بتاع الموقع وتحط الip بتاعه وتقدر تجيب الip من انك تعمل ping علي الموقع او من اداة Dig او nslookup*

*ملحوظه تانيه: لو عاوز تفلتر شوية حاجات بتطلعلك وانت بتعمل fuzzing ممكن تستخدم*

*fc => filter by status code-*

*fs => filter by size-*

*دول تقدر تستعملهم عشان ساعات ال ffuf بتطلعلك شوية هبل كده فا لو في حاجات طلعلتلك شوف ال status code او الsize بتاعهم واكتبهم مش هيطلعولك تاني*

## Exploiting Internal Subdomain

- مثلا افترض وانت بتعمل Fuzzing طلعلك subdomain باسم admin.mars.com وجيت تحطو فالبراوزر مشتغلش وده الطبيعي لأني من اسمه باين انه خاص بال Admins بس
- فكر معايا اقدر افتحه ازاي؟

- بص يامعلم انت اول حاجه لازم تجيب ip الموقع وده هتجيبو من خلال انك ممكن تعمل ping علي الموقع او ممكن تستخدم اداة زي dig مثلا `dig +short mars.com` او nslookup
- جبت الip؟ تمام كده عاوز تاخدو وتاخد الdomain الرئيسي والsubdomain اللي معاك اللي انت جبته اللي هو `admin` دلوقتي انت معاك
  -ايبي الموقع 128.154.16.5
  -الدومين mars.com
  -الsubdomain اللي هو admin
- عاوز بقي تاخد ال domain مع ال subdomain وتركبهم علي بعض `adamin.mars.com` وتاخد الip مع الsubdomain وتخزنهولي ف ملف ال `etc/hosts` اللي فتحناه وعرفنا بيعمل ايه فوق لو تفتكر وتحط الip وجمبيه الsubdomain زي ماوريتك فالصوره
- وجرب بقي افتح ال subdomain عادي من البراوزر لو فتح او نزل حاجه يبقي فل عليك فشخ ولو مفتح مفيش مشكله حاول تاني مع internal subdomain تاني وان شاء الله يفتح معاك