

【DNS】dnsrecon

dnsrecon 是一個用於執行域名系統 (DNS) 掃描和信息收集的工具。它提供了各種功能，用於識別目標域名的 DNS 記錄、發現子域名、枚舉主機名和 IP 地址等。以下是 **dnsrecon** 工具的一些主要功能和用途：

1. **DNS 記錄枚舉**：**dnsrecon** 可以用於查找目標域名的 DNS 記錄，包括主機 (A) 記錄、郵件 (MX) 記錄、名字伺服器 (NS) 記錄等。這有助於確定目標的 DNS 結構。
2. **子域名發現**：工具可以自動查找目標域名的子域名，這有助於擴大攻擊面，並查找潛在的安全漏洞。
3. **域名爆破**：**dnsrecon** 允許用戶執行域名爆破攻擊，以查找可能存在的域名。這對於測試域名是否可註冊或用於釣魚攻擊很有用。
4. **反向 DNS 查詢**：工具可以根據 IP 地址查詢關聯的 DNS 記錄，這有助於確定主機名和 IP 地址之間的對應關係。
5. **漏洞掃描**：**dnsrecon** 可以幫助掃描測試人員發現 DNS 伺服器的漏洞，如開放式遞歸查詢，並提供了有關 DNS 配置的重要信息。
6. **識別 DNS 伺服器**：工具可以識別給定 IP 地址的 DNS 伺服器，這有助於了解 DNS 基礎設施的配置。
7. **內容檢索**：**dnsrecon** 可用於檢索 DNS 記錄中的內容，如 TXT 記錄或 SRV 記錄。

總之，**dnsrecon** 是一個有用的工具，尤其適用於掃描、漏洞探測和域名信息收集。測試人員和安全專業人員可以使用它來確保其目標的 DNS 結構安全，同時發現潛在的風險和漏洞。然而，在使用該工具進行測試之前，應確保遵循法律和道德準則，並僅針對已經授權的目標域進行操作。

DNSRecon是一個用Python編寫的高級DNS列舉腳本。讓我們使用-d選項指定域名，-t選項指定要執行的列舉類型（在這種情況下是標準掃描），來對megacorpone.com執行dnsrecon。

```
kali@kali:~$ dnsrecon -d megacorpone.com -t std
[*] std: Performing General Enumeration against: megacorpone.com...
[-] DNSSEC is not configured for megacorpone.com
[*] SOA ns1.megacorpone.com 51.79.37.18
[*] NS ns1.megacorpone.com 51.79.37.18
[*] NS ns3.megacorpone.com 66.70.207.180
[*] NS ns2.megacorpone.com 51.222.39.63
[*] MX mail.megacorpone.com 51.222.169.212
[*] MX spool.mail.gandi.net 217.70.178.1
[*] MX fb.mail.gandi.net 217.70.178.217
[*] MX fb.mail.gandi.net 217.70.178.216
[*] MX fb.mail.gandi.net 217.70.178.215
[*] MX mail2.megacorpone.com 51.222.169.213
[*] TXT megacorpone.com Try Harder
[*] TXT megacorpone.com google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCj32hMNV3GtC0wWq5pA
[*] Enumerating SRV Records
[+] 0 Records Found
```

根據上面的輸出，我們已成功對megacorpone.com域執行了主要記錄類型的DNS掃描。

現在，讓我們嘗試使用之前為正向查找創建的list.txt文件，來對額外的主機名進行暴力破解。

```
kali@kali:~$ cat list.txt
www
ftp
mail
owa
proxy
router
```

為了執行我們的暴力破解嘗試，我們將使用-d選項來指定域名，-D選項來指定包含潛在子域字符串的文件名，以及-t選項來指定要執行的列舉類型，本例中是brt用於暴力破解

```
kali@kali:~$ dnsrecon -d megacorpone.com -D ~/list.txt -t brt
[*] Using the dictionary file: /home/kali/list.txt (provided by user)
[*] brt: Performing host and subdomain brute force against megacorpone.com...
[+] A www.megacorpone.com 149.56.244.87
[+] A mail.megacorpone.com 51.222.169.212
[+] A router.megacorpone.com 51.222.169.214
[+] 3 Records Found
```

