Guía Práctica: DNSENUM - Enumeración de Subdominios y DNS

Herramienta: `dnsenum`
Estado: Preinstalada en Kali Linux

¿Qué es?

Dnsenum es una herramienta para la enumeración de DNS. Permite descubrir subdominios, realizar transferencias de zona, identificar registros MX y más. Es fundamental para el reconocimiento durante un pentest.

🔧 Requisitos

- Kali Linux
- Acceso a terminal
- Conexión a internet (si trabajas fuera de red local)

📥 Verificar instalación

```
which dnsenum
```

Si no está instalado:

```
sudo apt update
sudo apt install dnsenum
```

Comandos útiles

1. **Básico:**

```
dnsenum example.com
```

2. **Escaneo completo:**

```
dnsenum --enum example.com
```

3. **Fuerza subdominios con wordlist:**

```
dnsenum --enum --wordlist /usr/share/wordlists/dnsmap.txt example.com
```

4. **Transferencia de zona (muy sensible):**

```
dnsenum --enum --dnsserver ns1.example.com example.com
```

5. **XML output:**

```
dnsenum --xml salida.xml example.com
```

6. **Modo verbose:**

```
dnsenum --verbose example.com
```

Ejemplo completo

```
dnsenum --enum --dnsserver 8.8.8.8 --wordlist
/usr/share/wordlists/dnsmap.txt --xml resultado.xml example.com
```

Dnsenum – Comandos Avanzados

1. Enumeración completa + detección de transferencia de zona + verbose

```
dnsenum --enum --dnsserver ns1.victima.com --verbose victima.com
```

- Intenta obtener información completa.
- Prueba si el DNS permite transferencias de zona.
- Muestra todos los detalles del proceso.

---

2. Con wordlist personalizada y salida XML

```
dnsenum --enum --wordlist /usr/share/wordlists/dnsmap.txt --xml
resultado.xml victima.com
```

- Ideal para reportes.
- Puedes luego abrir `resultado.xml` con herramientas de parsing o reportes como `xsltproc`.

---

3. Combinar con DNS públicos (bypaspear resolvers internos)

```
dnsenum --dnsserver 8.8.8.8 --enum victima.com
```

- Usa servidores DNS como los de Google (8.8.8.8) para evitar firewalls internos.

---

4. Detección de subdominios + registros MX + NS

```
dnsenum --mx --enum --noreverse victima.com
```

- Extrae servidores de correo (`MX`) y servidores autoritativos (`NS`).
- `--noreverse` evita la resolución inversa si solo quieres velocidad.

---

5. Redirigir la salida a múltiples formatos

```
dnsenum --enum victima.com -o salida.txt && cat salida.txt
```

- Puedes analizar después con herramientas como `grep`, `awk`, `sed`.

---

6. Integración en scripts con múltiples dominios

```
for domain in $(cat dominios.txt); do dnsenum --enum "$domain" >>
reporte_completo.txt; done
```

- Enumeración masiva desde un archivo con múltiples objetivos.

---

7. Script con notificación sonora (Linux Desktop)

```
dnsenum --enum victima.com && paplay
/usr/share/sounds/freedesktop/stereo/complete.oga
```

- Te avisa con sonido cuando el escaneo finaliza (ideal en largos wordlists).

---

8. Combinar con otras herramientas (ej. grep para subdominios válidos)

```
dnsenum --enum victima.com | grep -E '^[a-z0-9\.-]+\.[a-z]{2,}$'
```

- Extrae solo subdominios o nombres de host válidos del output.

---

9. Exportar solo subdominios a otro archivo

```
dnsenum --enum victima.com | grep -E '^[a-z0-9\.-]+\.victima\.com' > subdominios.txt
```

Tips Avanzados

- Puedes combinar `dnsenum` con herramientas como:
  - `amass`, `sublist3r`, `fierce` para resultados cruzados.
- Usa `resolvers.txt` personalizados para evitar que te baneen los DNS públicos.
- Para analizar outputs en XML:

```
xsltproc resultado.xml -o resultado.html
```

Buenas prácticas

- Prueba transferencias solo en entornos controlados.
- Usa `--verbose` para ver más detalles.

Recursos útiles

- GitHub: https://github.com/fwaeytens/dnsenum