Nmap

```
nmap -sn 127.0.0.1/24
```

-sn: Realiza un escaneo de "ping" (solo detección de host) para identificar qué hosts están activos en la red.

127.0.0.1/24: Especifica el rango de IPs a escanear en la red local.

```
nmap -sV -sC -p- -O -Pn -oN nmap_results.txt
```

-sV: Detecta las versiones de los servicios que están corriendo en los puertos abiertos.

-sC: Ejecuta los scripts NSE (Nmap Scripting Engine) por defecto, que pueden proporcionar información adicional sobre vulnerabilidades y configuraciones.

-p-: Escanea todos los puertos (del 1 al 65535).

-O: Intenta detectar el sistema operativo del host.

-Pn: Desactiva el descubrimiento de hosts. Nmap procederá directamente al escaneo de puertos y servicios sin verificar si el host está en línea.

-oN nmap_results.txt: Guarda los resultados en un archivo en formato normal (nmap_results.txt).

Gobuster

```
gobuster dir -u http://example.com -w wordlist.txt -o output.txt
```

gobuster dir: Indica que estamos usando el modo de enumeración de directorios.

-u http://example.com: La URL del sitio web objetivo.

-w wordlist.txt: La ruta al archivo de lista de palabras (wordlist) que se usará para la enumeración.

-o output.txt: El archivo donde se guardará la salida del escaneo.

Nikto

```
nikto -h http://example.com -o output.txt -Format txt
```

-h http://example.com: La URL del sitio web objetivo.

-o output.txt: El archivo donde se guardará la salida del escaneo.

Format txt: El formato del archivo de salida (en este caso, texto plano).