Entrega

Propietario	Ayala Arroyo Raúl
Etiquetas	

- **Resumen del entorno:**
    - Se está realizando un análisis de reconocimiento en un entorno controlado con bWAPP en BeeBox VM, usando Kali Linux como máquina atacante.
    - La IP de BeeBox es `192.168.100.27`, identificada en el rango de red `192.168.100.0/24`.
- **Resultados del escaneo de red:**
    - Comando utilizado: `nmap -sn 192.168.100.0/24`
    - Dispositivos detectados en la red:
        - **192.168.100.1**: Huawei Technologies
        - **192.168.100.4**: Dispositivo desconocido
        - **192.168.100.6**: Dispositivo desconocido
        - **192.168.100.9**: Amazon Technologies
        - **192.168.100.14**: Apple
        - **192.168.100.27**: Oracle VirtualBox (BeeBox)
        - **192.168.100.7**: Dispositivo desconocido
- **Resultados de enumeración de servicios:**
    - Comando utilizado: `nmap -sV -p- -v 192.168.100.27`
    - Puertos abiertos encontrados en BeeBox:
        - **21/tcp**: FTP
        - **22/tcp**: SSH
        - **25/tcp**: SMTP

        - **80/tcp**: HTTP
        - **139/tcp**: NetBIOS-ssn
        - **443/tcp**: HTTPS
        - **445/tcp**: Microsoft-DS
        - **512/tcp**, **513/tcp**, **514/tcp**: Servicios de administración remota
        - **666/tcp**: Doom (posible puerto de servicio específico)
        - **8080/tcp**: HTTP alternativo
        - **8443/tcp**, **9443/tcp**: Puertos HTTPS alternativos
        - **3306/tcp**: MySQL
        - **3632/tcp**: DistCC
        - **5901/tcp**: VNC
        - **6001/tcp**: X11
        - **9080/tcp**: HTTP alternativo

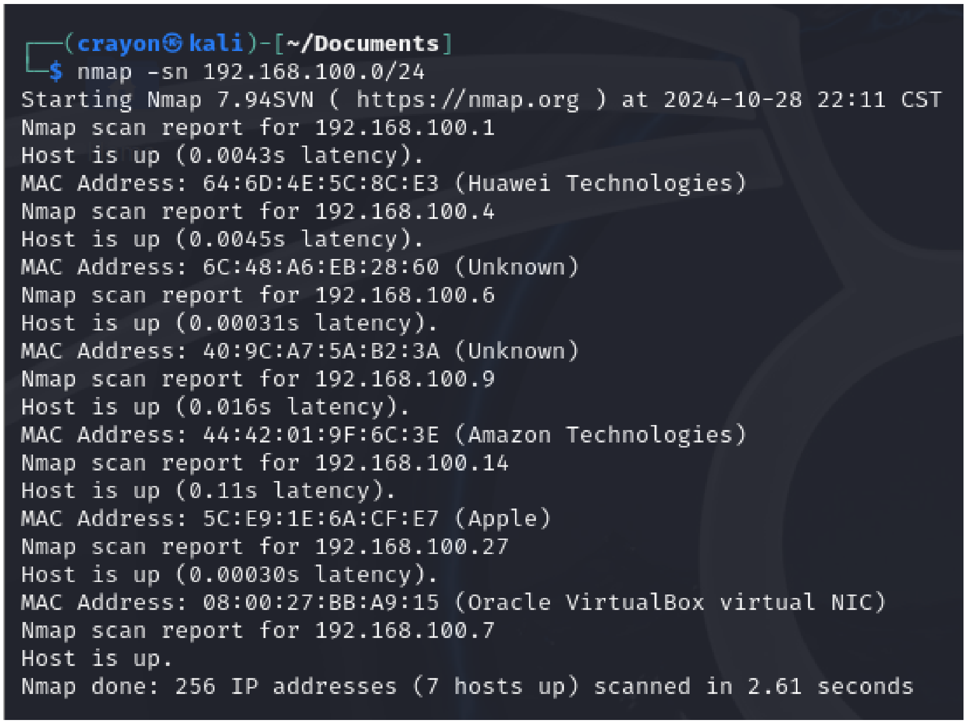
- **Información del dominio:**
    - **nslookup**: No se encontró un nombre de dominio asociado para la IP `192.168.100.27`.
    - **whois**: La IP `192.168.100.27` pertenece al rango privado `192.168.0.0/16`, que es un rango reservado para uso interno de redes privadas según RFC1918.
- **Subdominios encontrados:**
    - No se realizó un escaneo de subdominios en esta práctica (opcional si no hay un nombre de dominio).
- **Vulnerabilidades identificadas:**
    - Comando utilizado: `nikto -h 192.168.100.27`
    - **Vulnerabilidades detectadas:**
        - **ETags** en las respuestas HTTP, lo que puede filtrar información del sistema.

    - Falta el encabezado **X-Frame-Options**, que protege contra ataques de clickjacking.
    - Falta el encabezado **X-Content-Type-Options**, lo que podría permitir una interpretación de MIME incorrecta.
    - **Crossdomain.xml** permite cualquier origen, lo cual es un riesgo de seguridad.
    - Varios componentes desactualizados:
      - Apache/2.2.8, OpenSSL/0.9.8g, PHP/5.2.4, mod_ssl/2.2.8.
    - El método HTTP **TRACE** está habilitado, lo cual puede ser vulnerable a ataques de Cross-Site Tracing (XST).
    - **phpMyAdmin** accesible sin protección, lo que expone el servidor MySQL.
    - Índice de directorios expuesto en `/icons/` y archivos sensibles encontrados: `README`, `INSTALL.txt`, `wp-config.php`.
    - **MultiViews** está habilitado en Apache, lo que facilita ataques de fuerza bruta en nombres de archivos.
- **Directorios y archivos encontrados:**
  - Comando utilizado: `dirb http://192.168.100.27 /home/crayon/Documents/common.txt`
  - Directorios y archivos detectados:
    - **/index**: Página accesible en el servidor.
    - **/server-status**: Página de estado de Apache, que puede filtrar detalles sensibles sobre el servidor.
- **Análisis y conclusiones:**
  - El reconocimiento en el servidor BeeBox reveló varios puertos y servicios abiertos, junto con algunas vulnerabilidades potenciales, especialmente debido a software desactualizado y configuraciones de seguridad deficientes (por ejemplo, `server-status` expuesto y `phpMyAdmin` accesible).
  - Estas configuraciones podrían permitir un atacante obtener información detallada sobre la infraestructura del servidor y explotar posibles

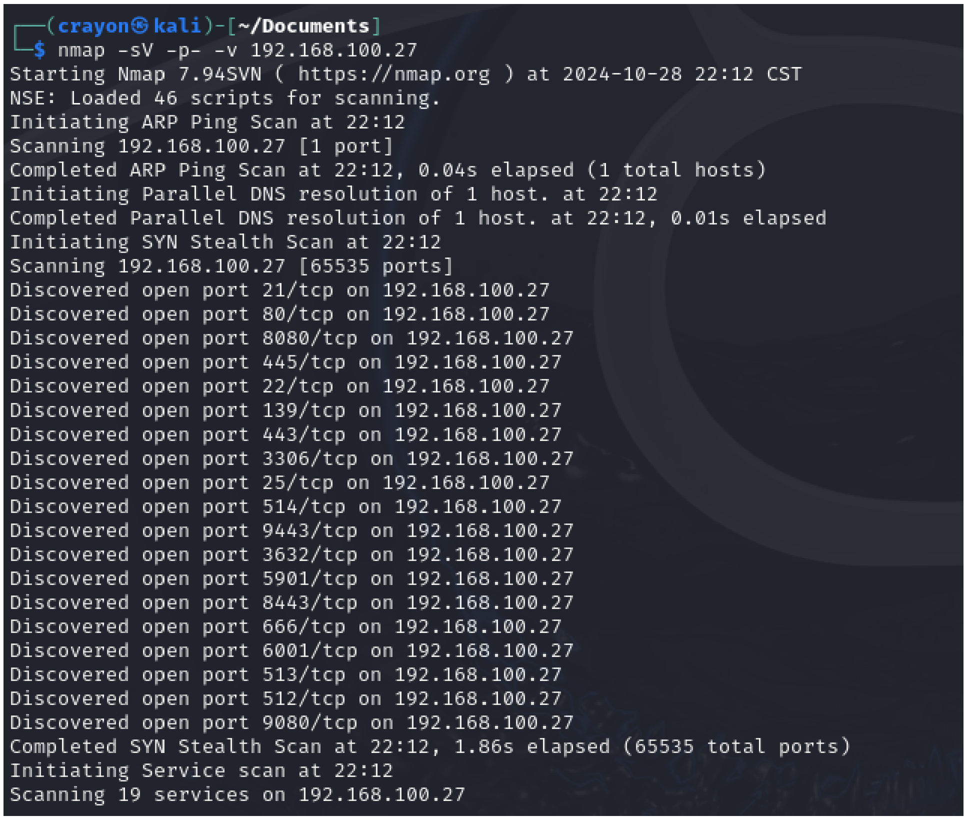
vulnerabilidades en servicios antiguos o no protegidos.

- **Recomendación**: Implementar actualizaciones en el software y deshabilitar o restringir el acceso a recursos sensibles como `phpMyAdmin`, `server-status`, y habilitar encabezados de seguridad para mitigar riesgos comunes.

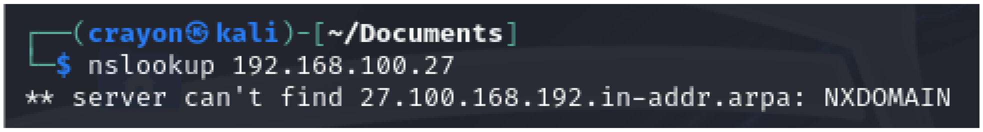
Capturas de pantalla:



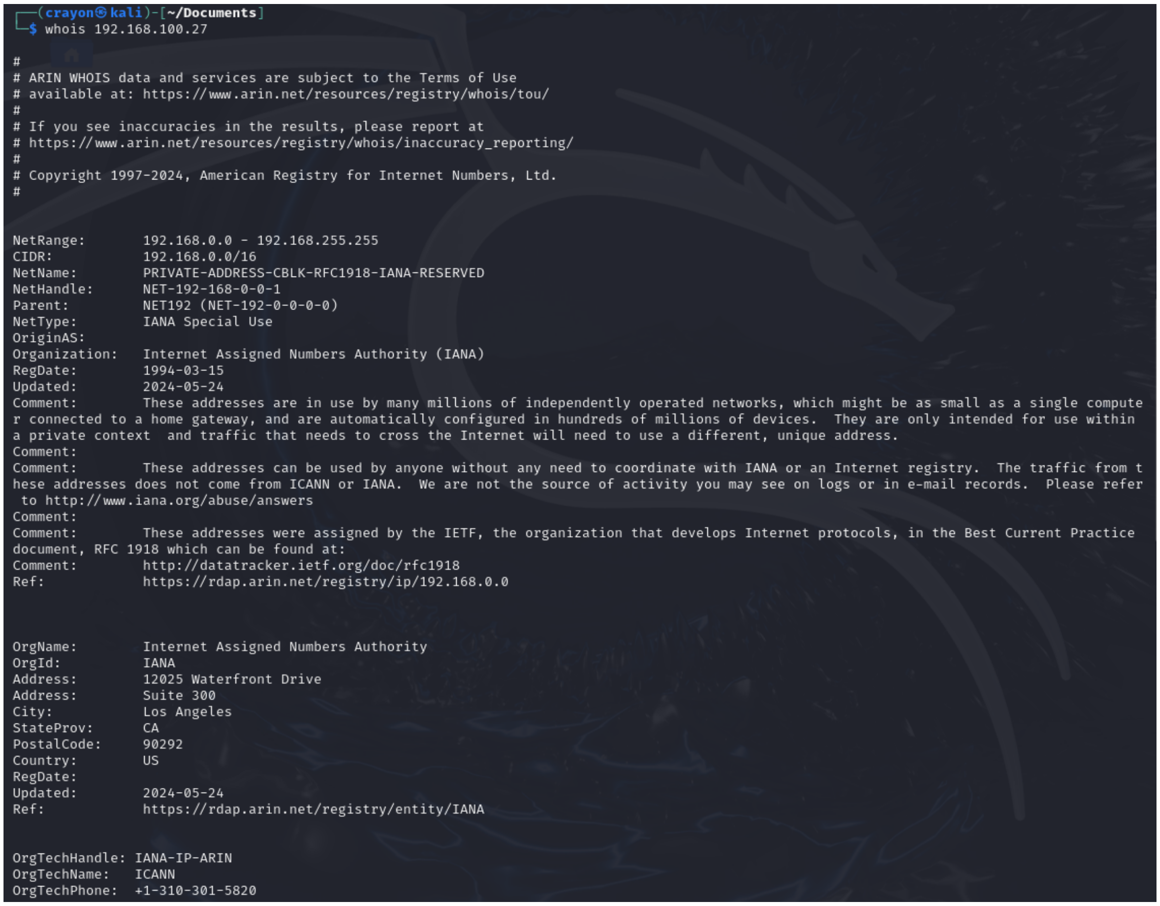
```
┌──(crayon㉿kali)-[~/Documents]
└─$ nmap -sn 192.168.100.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-28 22:11 CST
Nmap scan report for 192.168.100.1
Host is up (0.0043s latency).
MAC Address: 64:6D:4E:5C:8C:E3 (Huawei Technologies)
Nmap scan report for 192.168.100.4
Host is up (0.0045s latency).
MAC Address: 6C:48:A6:EB:28:60 (Unknown)
Nmap scan report for 192.168.100.6
Host is up (0.00031s latency).
MAC Address: 40:9C:A7:5A:B2:3A (Unknown)
Nmap scan report for 192.168.100.9
Host is up (0.016s latency).
MAC Address: 44:42:01:9F:6C:3E (Amazon Technologies)
Nmap scan report for 192.168.100.14
Host is up (0.11s latency).
MAC Address: 5C:E9:1E:6A:CF:E7 (Apple)
Nmap scan report for 192.168.100.27
Host is up (0.00030s latency).
MAC Address: 08:00:27:BB:A9:15 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.7
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.61 seconds
```



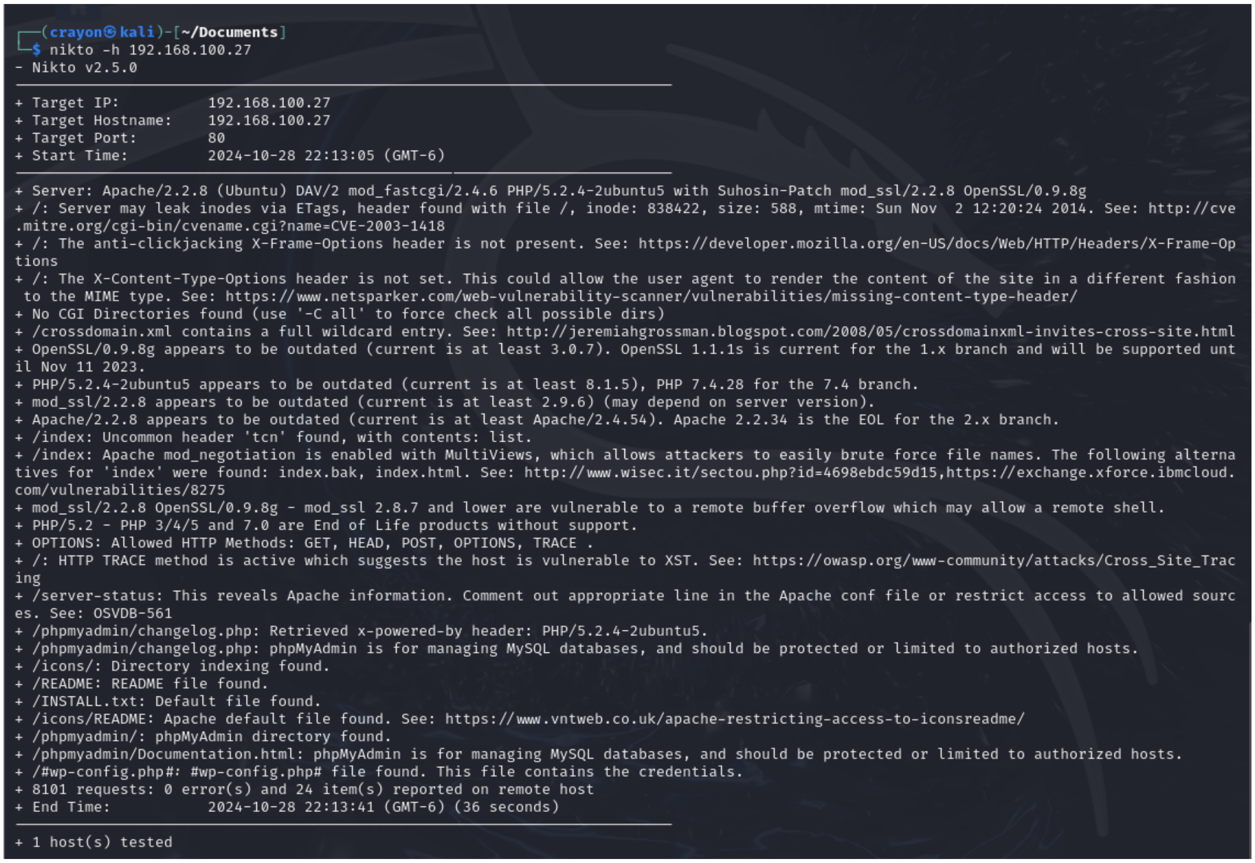
```
┌──(crayon㉿kali)-[~/Documents]
└─$ nmap -sV -p- -v 192.168.100.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-28 22:12 CST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 22:12
Scanning 192.168.100.27 [1 port]
Completed ARP Ping Scan at 22:12, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:12
Completed Parallel DNS resolution of 1 host. at 22:12, 0.01s elapsed
Initiating SYN Stealth Scan at 22:12
Scanning 192.168.100.27 [65535 ports]
Discovered open port 21/tcp on 192.168.100.27
Discovered open port 80/tcp on 192.168.100.27
Discovered open port 8080/tcp on 192.168.100.27
Discovered open port 445/tcp on 192.168.100.27
Discovered open port 22/tcp on 192.168.100.27
Discovered open port 139/tcp on 192.168.100.27
Discovered open port 443/tcp on 192.168.100.27
Discovered open port 3306/tcp on 192.168.100.27
Discovered open port 25/tcp on 192.168.100.27
Discovered open port 514/tcp on 192.168.100.27
Discovered open port 9443/tcp on 192.168.100.27
Discovered open port 3632/tcp on 192.168.100.27
Discovered open port 5901/tcp on 192.168.100.27
Discovered open port 8443/tcp on 192.168.100.27
Discovered open port 666/tcp on 192.168.100.27
Discovered open port 6001/tcp on 192.168.100.27
Discovered open port 513/tcp on 192.168.100.27
Discovered open port 512/tcp on 192.168.100.27
Discovered open port 9080/tcp on 192.168.100.27
Completed SYN Stealth Scan at 22:12, 1.86s elapsed (65535 total ports)
Initiating Service scan at 22:12
Scanning 19 services on 192.168.100.27
```



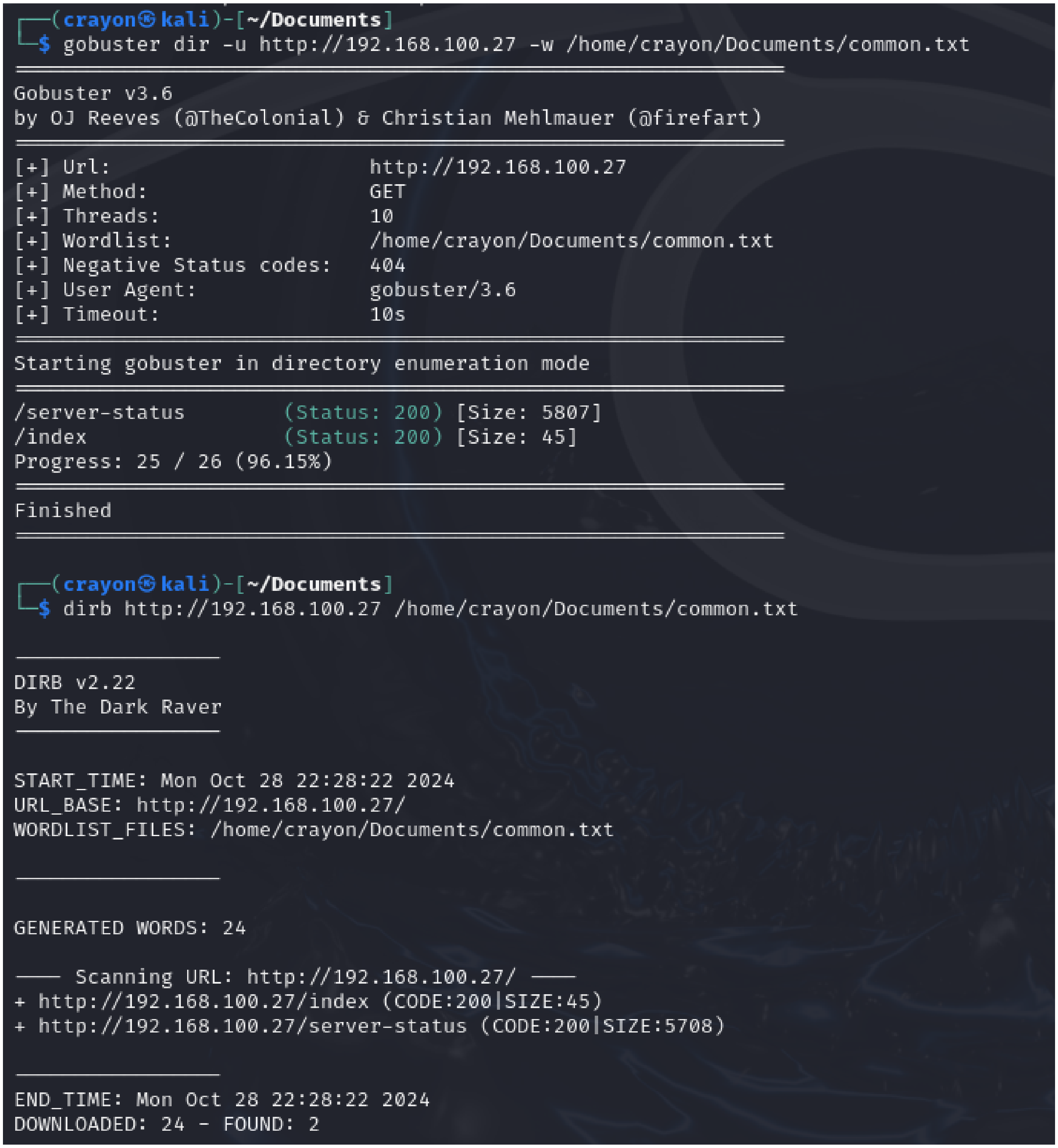
```
┌──(crayon㉿kali)-[~/Documents]
└─$ nslookup 192.168.100.27
** server can't find 27.100.168.192.in-addr.arpa: NXDOMAIN
```



```
┌──(crayon㉿kali)-[~/Documents]
└─$ whois 192.168.100.27

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#


NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2024-05-24
Comment:        These addresses are in use by many millions of independently operated networks, which might be as small as a single compute
r connected to a home gateway, and are automatically configured in hundreds of millions of devices.  They are only intended for use within
a private context  and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment:        These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry.  The traffic from t
hese addresses does not come from ICANN or IANA.  We are not the source of activity you may see on logs or in e-mail records.  Please refer
 to http://www.iana.org/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice
document, RFC 1918 which can be found at:
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0



OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2024-05-24
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
```



```
┌──(crayon㉿kali)-[~/Documents]
└─$ nikto -h 192.168.100.27
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.100.27
+ Target Hostname:    192.168.100.27
+ Target Port:        80
+ Start Time:         2024-10-28 22:13:05 (GMT-6)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ /: Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov  2 12:20:24 2014. See: http://cve
.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Op
tions
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion
 to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ OpenSSL/0.9.8g appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported unt
il Nov 11 2023.
+ PHP/5.2.4-2ubuntu5 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alterna
tives for 'index' were found: index.bak, index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.
com/vulnerabilities/8275
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Trac
ing
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sourc
es. See: OSVDB-561
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /INSTALL.txt: Default file found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2024-10-28 22:13:41 (GMT-6) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
┌──(crayon㉿kali)-[~/Documents]
└─$ gobuster dir -u http://192.168.100.27 -w /home/crayon/Documents/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.100.27
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/crayon/Documents/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 200) [Size: 5807]
/index                (Status: 200) [Size: 45]
Progress: 25 / 26 (96.15%)
===============================================================
Finished
===============================================================

┌──(crayon㉿kali)-[~/Documents]
└─$ dirb http://192.168.100.27 /home/crayon/Documents/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Oct 28 22:28:22 2024
URL_BASE: http://192.168.100.27/
WORDLIST_FILES: /home/crayon/Documents/common.txt

-----------------

GENERATED WORDS: 24

---- Scanning URL: http://192.168.100.27/ ----
+ http://192.168.100.27/index (CODE:200|SIZE:45)
+ http://192.168.100.27/server-status (CODE:200|SIZE:5708)

-----------------
END_TIME: Mon Oct 28 22:28:22 2024
DOWNLOADED: 24 - FOUND: 2
```