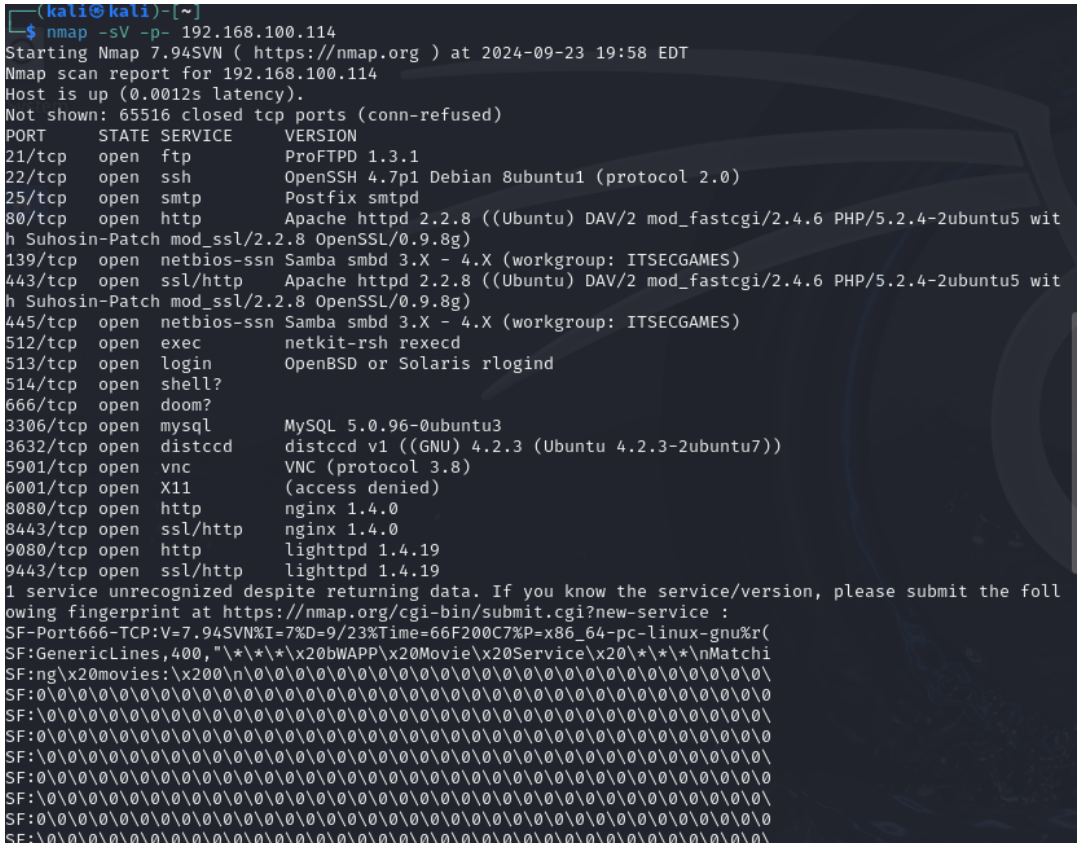
Escaneo Nmap a BEEbox



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.100.114
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 19:58 EDT
Nmap scan report for 192.168.100.114
Host is up (0.0012s latency).
Not shown: 65516 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 wit
h Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 wit
h Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell?
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3-2ubuntu7))
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
9443/tcp open  ssl/http    lighttpd 1.4.19
1 service unrecognized despite returning data. If you know the service/version, please submit the foll
owing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.94SVN%I=7%D=9/23%Time=66F200C7%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,400,"\*\*\*\x20bWAPP\x20Movie\x20Service\x20\*\*\*\nMatchi
SF:ng\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
```

1. Puertos Abiertos y Servicios Identificados:

- **21/tcp - ftp:**
    - Servicio: ProFTPD 1.3.1
- **22/tcp - ssh:**
    - Servicio: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
- **25/tcp - smtp:**
    - Servicio: Postfix smtpd
- **80/tcp - http:**
    - Servicio: Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5)
    - Con parches de seguridad Suhosin-Patch.
- **139/tcp y 445/tcp - netbios-ssn:**
    - Servicio: Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)

- **443/tcp - https:**
    - Servicio: Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5)
- **512/tcp - exec:**
    - Servicio: netkit-rsh rexecd
- **513/tcp - login:**
    - Servicio: OpenBSD or Solaris rlogind
- **514/tcp - shell:**
    - Servicio: no identificado
- **666/tcp - doom:**
    - Servicio no identificado, posiblemente un puerto personalizado para algún servicio específico.
- **3306/tcp - mysql:**
    - Servicio: MySQL 5.0.96-0ubuntu3
- **3632/tcp - distccd:**
    - Servicio: distccd v1 (GNU) 4.2.3 (Ubuntu 4.2.3-2ubuntu7)
- **5901/tcp - vnc:**
    - Servicio: VNC (protocol 3.8)
- **6001/tcp - X11:**
    - Servicio: access denied (Acceso denegado, lo cual indica que hay un servicio X11, pero no está permitido el acceso).
- **8080/tcp - http:**
    - Servicio: nginx 1.4.0
- **8443/tcp - https:**
    - Servicio: nginx 1.4.0
- **9080/tcp - http:**
    - Servicio: lighttpd 1.4.19
- **9443/tcp - https:**
    - Servicio: lighttpd 1.4.19

Múltiples Servicios Web:

- Hay varios servicios HTTP y HTTPS corriendo en diferentes puertos (80, 443, 8080, 8443, 9080, 9443), cada uno con diferentes versiones de servidores web (Apache, nginx, lighttpd).

Servicios de Red y Compartición de Archivos:

- Los puertos 139 y 445 están relacionados con Samba, lo que sugiere que se podría estar compartiendo archivos en la red local.

Servicio de Base de Datos:

- El puerto 3306 indica que hay un servidor MySQL corriendo, lo que podría ser un punto crítico de acceso si no está protegido adecuadamente.

Servicio VNC:

- El puerto 5901 indica que hay un servidor VNC (control remoto) activo, lo cual puede ser un vector de ataque si no está adecuadamente protegido con autenticación.

Servicios de Shell Remoto y Ejecución Remota:

- Los puertos 512, 513 y 514 sugieren que hay servicios de ejecución remota (rexec, rlogin, rsh), que son potencialmente peligrosos si no están adecuadamente configurados.
- Hay un puerto (666/tcp) cuyo servicio y versión no pudieron ser reconocidos por nmap. Esto podría requerir una investigación más detallada para identificar si es un servicio personalizado o una posible puerta trasera.

Uso de whois:

```
└─$ whois 192.168.00.114

#
# 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 computer connected to a home gateway, and are automatically configured i
n hundreds of millions of devices.  They are only intended for use within a private context  and traff
ic 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 I
nternet registry.  The traffic from these 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/abus
e/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet pro
tocols, 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
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# 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.
#
```

Información General:

- **Rango de IPs:** 192.168.0.0 - 192.168.255.255
- **CIDR:** 192.168.0.0/16
- **Designación:** PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
- **NetName:** NET-192-168-0-0-1
- **Organización: Internet Assigned Numbers Authority (IANA)**

Uso de Nikto:

Resumen del escaneo

- **Target IP:** La dirección IP del servidor objetivo, en este caso 192.168.100.114.
- **Target Hostname:** El nombre de host del objetivo, que no se ha resuelto en este escaneo específico.
- **Target Port:** Puerto 80, que es el puerto estándar para HTTP.

- **Start Time:** Fecha y hora de inicio del escaneo, en este caso 2024-09-23 20:21:31 (GMT-4).

Información del servidor

- **Server:** La cabecera del servidor muestra que el servidor web utiliza Apache 2.2.8 en un sistema operativo Ubuntu, con módulos adicionales como mod_fastcgi/2.4.6, PHP 5.2.4 con un parche de seguridad Suhosin-Patch, y mod_ssl con OpenSSL 0.9.8g.

Vulnerabilidades y advertencias detectadas:

1. **Servidor web vulnerable a ETags:**
    - Se encontró una vulnerabilidad relacionada con el manejo de las cabeceras ETags, que puede permitir la enumeración de archivos o el rastreo de usuarios.
2. **Falta de encabezado X-Frame-Options:**
    - No se detectó el encabezado X-Frame-Options, lo que permite ataques de Clickjacking.
3. **No se encontraron Directivas de Opciones (Option Directives):**
    - No hay restricciones específicas en la configuración del servidor, por lo que puede haber rutas potencialmente accesibles.
4. **crossdomain.xml contiene una entrada comodín:**
    - El archivo crossdomain.xml permite acceso a todas las rutas (*), lo cual es un riesgo de seguridad.
5. **Método HTTP TRACE activo:**
    - El método HTTP TRACE está habilitado, lo cual puede permitir ataques de tipo Cross Site Tracing (XST).
6. **Apache MultiViews y lista de directorios:**
    - Hay archivos comunes como index.bak e index.html, que podrían ser accesibles y exponer información.
7. **Versiones desactualizadas:**
    - El servidor Apache, OpenSSL y PHP están utilizando versiones obsoletas y vulnerables:
        - Apache 2.2.8 es obsoleto y tiene múltiples vulnerabilidades conocidas.

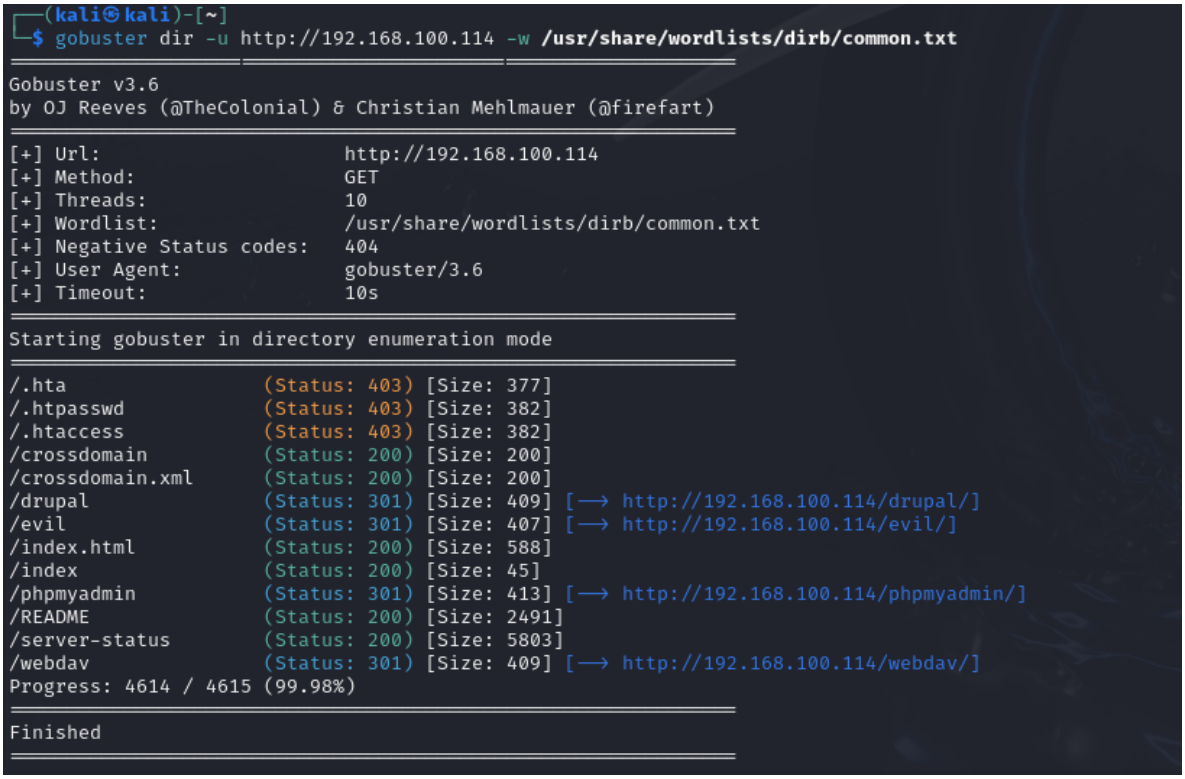
        - OpenSSL 0.9.8g tiene vulnerabilidades conocidas.
        - PHP 5.2.4-2ubuntu5 también está desactualizado y vulnerable.

8. **Configuración insegura de mod_ssl:**
    - mod_ssl y versiones inferiores son vulnerables a desbordamientos de buffer, lo que podría permitir la ejecución de código remoto.
9. **Exposición de server-status:**
    - La URL /server-status está habilitada, revelando información interna del servidor. Esto puede ser aprovechado para un reconocimiento más detallado por parte de un atacante.
10. **Archivos potencialmente peligrosos:**
    - Se han encontrado archivos y directorios expuestos, como /phpmyadmin, /icons/, y /README que pueden proporcionar información adicional al atacante.

Recomendaciones generales:

- **Actualizar el software:** Se recomienda actualizar Apache, PHP y OpenSSL a versiones más recientes que no sean vulnerables.
- **Deshabilitar métodos HTTP inseguros:** Deshabilitar el método HTTP TRACE y asegurarse de que solo los métodos necesarios estén permitidos.
- **Proteger archivos y directorios sensibles:** Asegurarse de que archivos como phpmyadmin, /server-status, /icons/, etc., no estén accesibles públicamente.
- **Configurar encabezados de seguridad:** Añadir encabezados de seguridad como X-Frame-Options, X-Content-Type-Options, y Strict-Transport-Security para mitigar ataques comunes.

Uso de GoBuster:



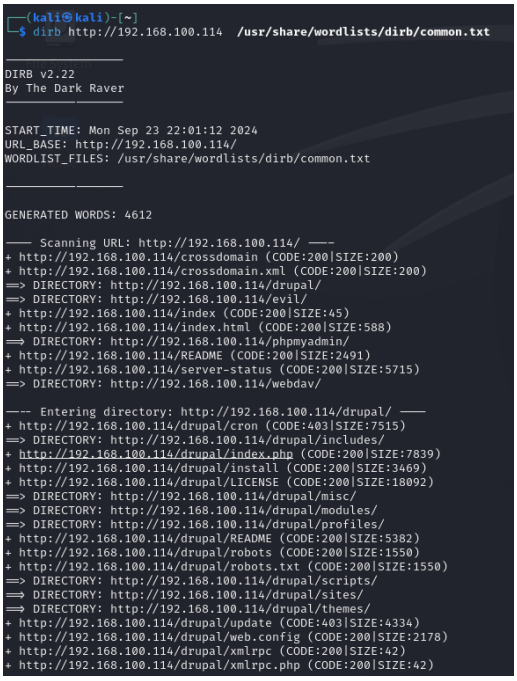
1. **Archivos Protegidos (Código 403 - Forbidden):**
    - /.hta
    - /.htpasswd
    - /.htaccess Estos archivos suelen ser archivos de configuración y protección de servidores web, como reglas de acceso o credenciales. El estado 403 indica que existen, pero no se permite el acceso a ellos.
2. **Archivos Encontrados (Código 200 - OK):**
    - /crossdomain: Archivo encontrado con un tamaño de 200 bytes.
    - /crossdomain.xml: Archivo con un tamaño de 200 bytes. Suele ser utilizado por aplicaciones Flash para definir permisos de acceso de dominio cruzado.
    - /index.html: Página principal del servidor web, tamaño 588 bytes.
    - /index: Similar al archivo index.html, con un tamaño de 45 bytes.
    - /README: Archivo README con un tamaño de 2491 bytes. Puede contener información sobre la configuración del servidor o las aplicaciones instaladas.
    - /server-status: Tamaño de 5803 bytes. Suele proporcionar detalles del estado y configuración del servidor Apache.

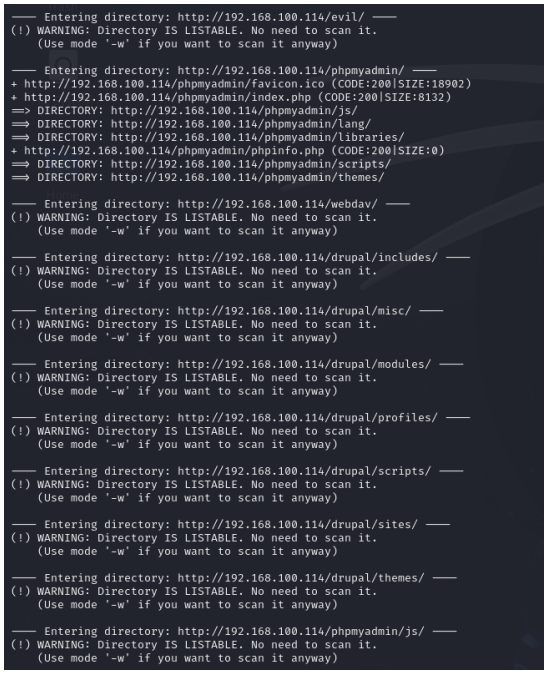
3. **Directorios Encontrados con Redirección (Código 301 - Moved Permanently):**
    - /drupal/ (Redirige a http://192.168.100.114/drupal/): Posible instalación de Drupal.
    - /evil/ (Redirige a http://192.168.100.114/evil/): Directorio inusual, posiblemente una carpeta de pruebas o con contenido específico para el entorno.
    - /phpmyadmin/ (Redirige a http://192.168.100.114/phpmyadmin/): Interfaz de administración de bases de datos MySQL. Debe protegerse adecuadamente.
    - /webdav/ (Redirige a http://192.168.100.114/webdav/): Posible implementación de WebDAV, un protocolo para la manipulación de archivos en el servidor a través del navegador.
4. **Directorios y Archivos Interesantes:**
    - /.hta, /.htpasswd, /.htaccess: Aunque no se permite su acceso, estos archivos indican que hay medidas de seguridad aplicadas en el servidor.
    - phpmyadmin: La presencia de phpMyAdmin en el servidor representa un potencial vector de ataque si no está debidamente asegurado.
    - server-status: Si este archivo es accesible públicamente, podría proporcionar información valiosa sobre la configuración del servidor y las solicitudes HTTP recientes.

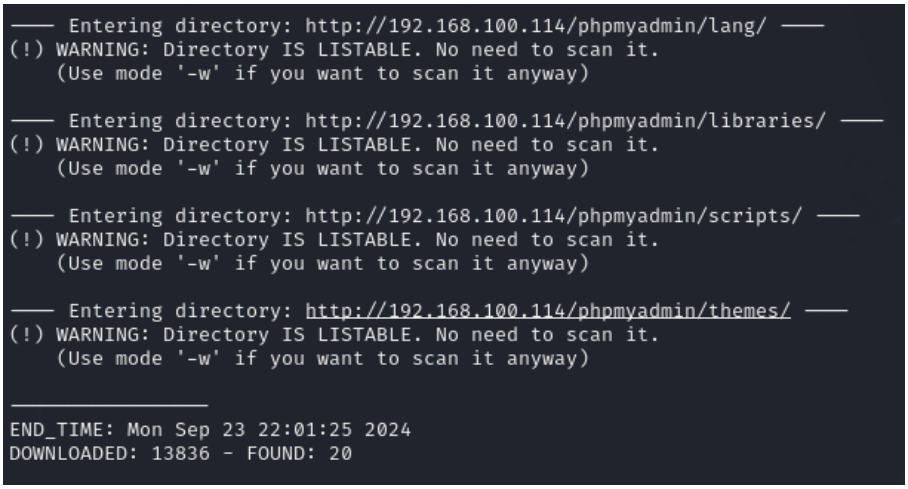
Conclusión:

- **Vulnerabilidades Potenciales:**
    - La presencia de phpmyadmin sin protección puede exponer la base de datos a ataques si no está configurado correctamente.
    - server-status puede ser una fuente de información sensible si no se restringe su acceso.

Uso de DirB:







.- **Archivos y Directorios Principales Encontrados:**

- **Archivos:**
  - crossdomain.xml (Código: 200)
  - README (Código: 200)
  - server-status (Código: 200)

- **Directorios:**
    - /drupal/ (Código: 200)
    - /evil/ (Código: 200)
    - /phpmyadmin/ (Código: 200)
    - /webdav/ (Código: 200)

.- **Directorios Específicos Explorados:**

- **/drupal/:**
    - Encontró varios archivos y subdirectorios:
        - cron (Código: 403)
        - index.php (Código: 200)
        - install (Código: 200)
        - Varios otros subdirectorios (includes, misc, modules, etc.) están listables, por lo que dirb recomienda usar el modo -w si se desea profundizar en el escaneo.
- **/phpmyadmin/:**
    - Encontró varios archivos y subdirectorios:
        - favicon.ico (Código: 200)
        - index.php (Código: 200)
        - phpinfo.php (Código: 200)
        - Varios subdirectorios (js, lang, libraries, etc.) están listables, también recomendando el uso de -w.
- **/webdav/:** El directorio es listable.

.- **Directorios Listables (avisos):**

- Se detectaron múltiples directorios en los que el servidor permite listar su contenido sin restricciones (opción de listable). Esto puede ser una vulnerabilidad, ya que permite ver el contenido de los directorios sin necesidad de conocer los nombres de los archivos.

.- **Conclusiones del escaneo:**

- **Directorios sensibles:** Se encontraron directorios como /phpmyadmin/ y /drupal/ que podrían ser objetivos para ataques específicos si no están adecuadamente protegidos.
- **Archivos interesantes:** Archivos como README y server-status pueden contener información útil sobre la configuración del servidor.
- **Recomendación de profundizar el escaneo:** Para los directorios listables, usar el modo -w para obtener más detalles si se desea realizar una auditoría más profunda.

Resumen del Entorno Analizado

a. **Dirección IP Objetivo:** 192.168.100.114
    - Esta dirección IP es parte del rango de direcciones privadas (192.168.0.0/16), comúnmente utilizada en redes internas.

b. **Características Generales:**
    - El sistema parece estar configurado en un entorno de red local, posiblemente una red de pruebas o de desarrollo debido a la cantidad de servicios y puertos abiertos.

c. **Servicios Identificados:**
    - **Servidores Web:**
        - Múltiples instancias de servidores web corriendo:
            - Apache en puertos 80 y 443.
            - nginx en puertos 8080 y 8443.
            - lighttpd en puertos 9080 y 9443.
        - Esto sugiere que el sistema podría estar sirviendo diferentes aplicaciones web o entornos de desarrollo en distintos puertos.
    - **Servicios de Red y Compartición de Archivos:**
        - Samba (139, 445): Indica que se pueden estar compartiendo archivos en la red local, posiblemente con fines de colaboración o desarrollo.
    - **Servicios de Administración y Control Remoto:**
        - SSH (22): Acceso remoto seguro.
        - VNC (5901): Control remoto gráfico.

        - rsh, rlogin, rexec (512, 513, 514): Servicios de acceso remoto potencialmente inseguros, obsoletos o no recomendados.
    - **Servicio de Base de Datos:**
        - MySQL (3306): Base de datos relacional. Esto indica que podrían estar almacenándose datos de aplicaciones o pruebas en el entorno.

d. **Observaciones Críticas:**
    - **Multiplicidad de Servicios Web y Puertos:**
        - Hay muchos servicios web escuchando en diferentes puertos, lo cual podría facilitar el acceso no autorizado si alguno de estos servicios tiene vulnerabilidades no parchadas.
    - **Riesgo de Exposición de Datos:**
        - Servicios como Samba y MySQL, si no están adecuadamente protegidos, podrían exponer datos sensibles.
    - **Uso de Servicios Obsoletos/Inseguros:**
        - Los servicios rsh, rlogin, y rexec son conocidos por ser inseguros. Deberían ser deshabilitados o reemplazados por alternativas más seguras como SSH.

e. **Posibles Propósitos del Entorno:**
    - **Desarrollo o Pruebas:**
        - La diversidad de servicios y configuraciones sugiere que este entorno podría ser una plataforma de pruebas o desarrollo para diferentes aplicaciones y tecnologías.
    - **Entorno de Pruebas de Seguridad:**
        - La combinación de múltiples servicios, incluyendo servicios potencialmente inseguros, sugiere que podría ser un entorno para pruebas de seguridad o CTF (Capture The Flag).

f. **Recomendaciones Generales:**
    - Revisar la configuración de cada servicio para asegurar que no hay vulnerabilidades conocidas.
    - Deshabilitar servicios innecesarios, especialmente aquellos considerados inseguros.
    - Implementar medidas de seguridad adicionales, como cortafuegos y reglas de acceso restrictivas.

Resultados de Enumeración de Servicios y Subdominios Encontrados:

1. Servicios Enumerados:

Basado en el escaneo previo con nmap y los resultados de gobuster:

1. **Servicios de Red y Web:**
    - **HTTP (Apache)**: Corriendo en puertos 80 y 443 con versiones 2.2.8 y módulos adicionales (DAV/2, mod_fastcgi, PHP/5.2.4, Suhosin-Patch).
    - **HTTP (nginx)**: Corriendo en puertos 8080 y 8443 con versión 1.4.0.
    - **HTTP (lighttpd)**: Corriendo en puertos 9080 y 9443 con versión 1.4.19.
    - **FTP (ProFTPD)**: Corriendo en el puerto 21 con versión 1.3.1.
    - **SSH (OpenSSH)**: Corriendo en el puerto 22 con versión 4.7p1.
    - **SMTP (Postfix)**: Corriendo en el puerto 25.
    - **MySQL**: Corriendo en el puerto 3306 con versión 5.0.96.
    - **Samba**: Compartición de archivos corriendo en los puertos 139 y 445.
    - **phpMyAdmin**: Interfaz para la administración de bases de datos MySQL encontrada en el directorio /phpmyadmin/.
2. **Servicios de Control y Administración Remota:**
    - **VNC**: Corriendo en el puerto 5901 con protocolo 3.8.
    - **exec, login, shell**: Servicios de ejecución remota (512, 513, 514).
    - **distccd**: Servicio de compilación distribuida en el puerto 3632.
3. **Servicios No Identificados o Personalizados:**
    - **666/tcp (doom?)**: Servicio no identificado que puede requerir una investigación adicional.

2. Directorios y Subdominios Encontrados con GoBuster:

1. **Directorios Encontrados en el Escaneo de gobuster:**
    - **/drupal/**: Posible instalación de Drupal. Esto sugiere un subdominio potencial como drupal.192.168.100.114.
    - **/evil/**: Directorio que podría contener contenido o aplicaciones específicas del entorno. Sin embargo, no hay suficiente información para determinar su función.

- **/phpmyadmin/**: Interfaz de administración de MySQL, comúnmente asociada con el subdominio phpmyadmin.192.168.100.114.
- **/webdav/**: Implementación de WebDAV, sugiere un subdominio o aplicación de compartición de archivos.

Conclusiones:

-**Exposición de Servicios Múltiples:**

- El sistema en la IP 192.168.100.114 tiene múltiples servicios corriendo en diferentes puertos, lo que aumenta la superficie de ataque. Entre estos servicios se encuentran varios servidores web (Apache, nginx, lighttpd), FTP, SSH, y Samba, entre otros. Esta diversidad sugiere un entorno de pruebas o desarrollo que necesita una gestión cuidadosa de la seguridad.

- **Servicios Web Multiplicados:**

- La presencia de varios servidores web en diferentes puertos (80, 443, 8080, 8443, 9080, 9443) indica que podrían estar sirviendo diferentes aplicaciones o versiones de una misma aplicación. Es crucial asegurar que todos estos servicios estén actualizados y correctamente configurados para evitar vulnerabilidades conocidas.

- **Archivos Sensibles y Configuraciones Inseguras:**

- Se encontraron archivos sensibles como .htaccess y .htpasswd, que aunque no son accesibles directamente, su existencia revela configuraciones potencialmente críticas. Además, la posibilidad de listar directorios (Directory is LISTABLE) puede exponer el contenido de ciertas carpetas si no se configura correctamente el servidor web.

- **Exposición de Herramientas de Administración:**

- La detección de phpMyAdmin y servicios de administración remota como VNC (puerto 5901) y SSH indica que se debe prestar especial atención a la protección con contraseñas fuertes y la limitación de acceso. phpMyAdmin, en particular, es un objetivo común de ataques si no está adecuadamente protegido.

- **Riesgos de Seguridad Elevados:**

- La combinación de servicios obsoletos (como OpenSSH 4.7p1 y ProFTPD 1.3.1) y servicios inseguros (como rsh, rlogin, rexec) sugiere que el sistema puede ser vulnerable a ataques conocidos. Estos servicios deberían actualizarse o deshabilitarse si no son absolutamente necesarios.

- **Evidencia de Entorno de Pruebas o Desarrollo:**

- La diversidad de servicios y puertos abiertos, junto con directorios como /evil/ y /webdav/, sugieren que este entorno es posiblemente una plataforma de pruebas o

desarrollo. En un entorno productivo, estos servicios y configuraciones serían un riesgo inaceptable.

- **Potenciales Subdominios y Directorios:**

- Se encontraron directorios que podrían correlacionarse con subdominios, como /drupal/, /phpmyadmin/, y /webdav/. Aunque no se realizó un escaneo específico de subdominios, la presencia de estos directorios sugiere la posible existencia de subdominios con aplicaciones específicas.

Recomendaciones:

1. **Revisión y Actualización de Servicios:**
    - Actualizar todos los servicios a sus versiones más recientes y asegurarse de que están configurados con las mejores prácticas de seguridad. Especial atención a servicios como OpenSSH, ProFTPD y phpMyAdmin.
2. **Eliminar o Proteger Servicios Innecesarios:**
    - Deshabilitar servicios inseguros o no utilizados, como rsh, rlogin, y rexec. También se recomienda revisar la necesidad de tener múltiples servidores web en diferentes puertos.
3. **Restricciones de Acceso:**
    - Implementar reglas de firewall estrictas para limitar el acceso a servicios como phpMyAdmin, VNC, y MySQL, permitiendo solo conexiones desde direcciones IP de confianza.
4. **Auditoría de Configuraciones:**
    - Revisar configuraciones de seguridad en archivos como .htaccess y en servicios de web. Asegurar que no hay archivos de configuración o información sensible accesible públicamente.
5. **Monitoreo y Pruebas de Seguridad:**
    - Implementar monitoreo continuo de los servicios y realizar pruebas de penetración periódicas para identificar y mitigar nuevas vulnerabilidades.