RESUMEN DEL ENTORNO

Este es un ejercicio sobre la fase de reconocimiento de un sitio web vulnerable. La máquina objetivo es BeeBox VM, que es una máquina intencionalmente vulnerable en donde he abierto una página web llamada bWAPP (https://192.168.1.55) y la máquina atacante es una Kali Linux. Para realizar este ejercicio, hemos usado las siguientes herramientas: nslookup, nmap, whois, Sublist3r, Nikto, Gobuster, Dirb y SecLists repo por Daniel Miessler.

RESULTADOS DEL ESCANEO DE RED

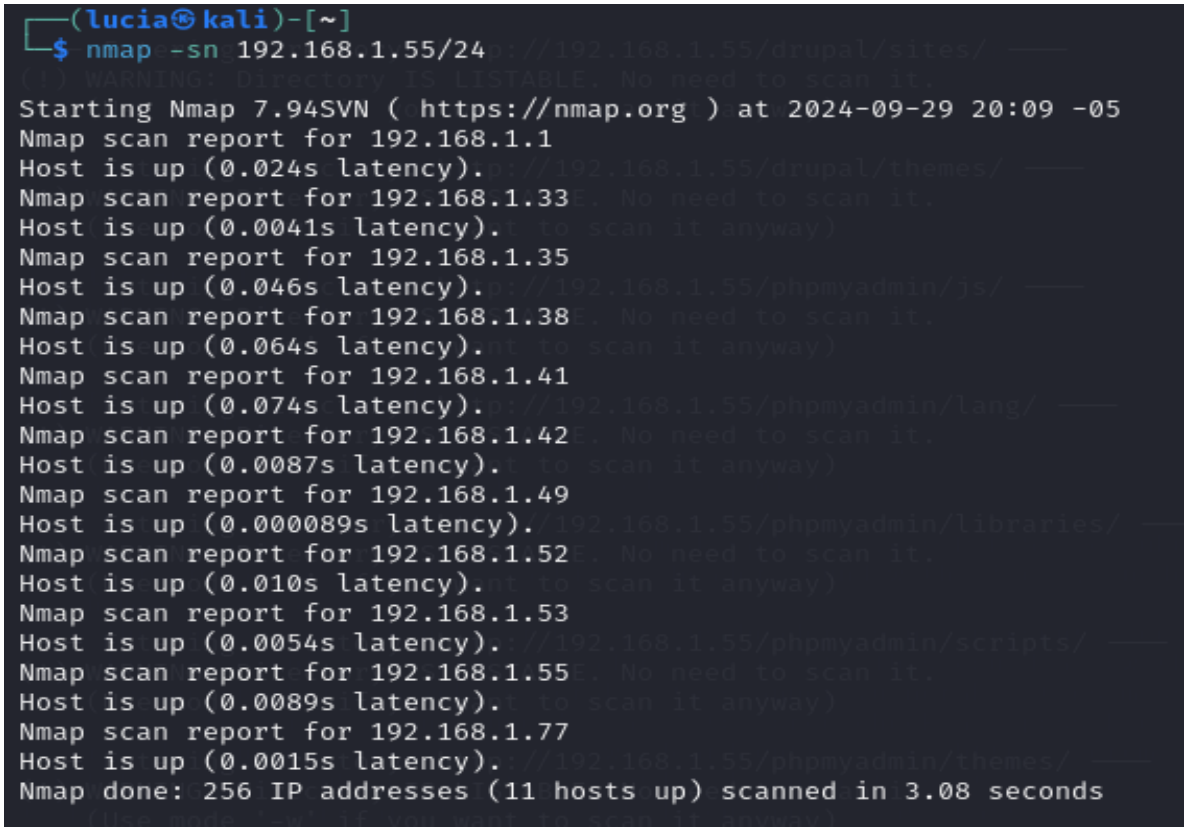
Para el escaneo de red he usado nmap desde Kali Linux hacia la dirección IP de la máquina vulnerable (192.168.1.55). Los resultados son los que se detallan a continuación:

nmap -sn 192.168.1.55/24

Se ejecuta el escaneo de red usando la versión 7.94 de nmap. Usar *192.168.1.55/24* quiere decir que estoy escaneando toda la subred de 192.168.1.55 (notación /24 : desde 192.168.1.0 hasta 192.168.255, un total de 256 direcciones).

Los resultados me han listado un total de 11 direcciones IP, lo que quiere decir que hay 11 dispositivos activos en la red local (en la lista de IP que me arrojó también puedo reconocer que una de esas direcciones IP es la de mi máquina objetivo). “Host is up” para cada dirección IP listada indica que el dispositivo en esa dirección está encendido y “Latency” es el tiempo que tardó en responder.

Todo esto finalmente también se indica en “nmap done: 256 IP addresses(11 hosts up)” de la foto que anexo. Evidentemente, **hacer este tipo de escaneos me ha ayudado a saber qué dispositivos están conectados en la red en ese momento.**



RESULTADOS DE ENUMERACIÓN DE SERVICIOS Y PUERTOS

nmap -sV -p- 192.168.1.55

Se vuelve a usar nmap para la enumeración de puertos y servicios.
-p- : nmap debe escanear todos los puertos (1 – 65535)
-sV : nmap detecta las versiones de los servicios que están corriendo en los puertos abiertos.

El escaneo encontró puertos y servicios abiertos. Detallaré, comentaré y anexaré los principales a continuación:

PUERTO: 21/TCP STATE: OPEN SERVICE: FTP VERSIÓN : ProFTPD 1.3.1

- El puerto 21 está abierto y está ejecutando el servicio FTP (file transfer protocool) con la versión ProFTPD 1.31 . FTP es un protocolo de transferencia de archivos estándar entre un cliente y un servidor a través de una red como puede ser internet o simplemente una red local. FTP suele usar el puerto 21 para el control de la conexión. Las implicaciones de que el puerto 21 esté abierto es que cualquier dispositivo que tenga acceso a esa máquina puede intentar conectarse al servidor FTP utilizando un cliente FTP. FTP tampoco es seguro ya que las credenciales atraviesan la red en texto plano y no cifrado. Finalmente, el servicio FTP detectado está usando la versión ProFTPD 1.3.1 que es una versión antigua lanzada en 2008 que ha tenido muchas vulnerabilidades reportadas (como **CVE-2010-4221**, **CVE-2011-4130**, etc) lo que la hace susceptible a métodos de ataque básicos como suplantación de identidad, sniffing, entre otros.

PUERTO: 22/TCP STATE: OPEN SERVICE: SSH VERSION: OpenSSH 4.7

- El puerto 22 está abierto y está usando el servicio de SSH (con la versión OpenSSH 4.7). SSH o Secure Shell es un protocolo de transmisión remota y , en este caso, cualquier dispositivo que tenga acceso a la red y las credenciales correctas puede conectarse al servidor mediante SSH a través de este puerto. SSH cifra toda la comunicación entre cliente y servidor, lo que protege las credenciales de acceso y los datos transferidos. Sin embargo, un puerto 22 abierto puede ser un vector de ataque si no se configura adecuadamente. Los atacantes pueden intentar realizar ataques de fuerza bruta para adivinar contraseñas o buscar vulnerabilidades en versiones antiguas de SSH. En este caso en específico, OpenSSH 4.7 es una versión bastante desactualizada, lo que podría exponer el sistema a vulnerabilidades conocidas. Estas podrían incluir problemas como ataques de fuerza bruta, vulnerabilidades en la autenticación o explotación de bugs específicos de esa versión, por lo que se debe considerar actualizar a una versión más reciente de OpenSSH para asegurar el servicio y aplicar las últimas mejoras de seguridad.

PUERTO: 25/TCP STATE: OPEN SERVICE: SMTP VERSION: Postfix Smtpd

- El puerto 25 está abierto y está usando el servicio STMP (que es el protocolo utilizado para el envío de correos electrónicos entre servidores) con versión Postfix Smtpd. Postfix es un servidor de correo de código abierto que implementa el protocolo SMTP. Es conocido por ser rápido, seguro y fácil de configurar mientras que el Smtpd hace referencia al daemon (proceso en segundo plano) que escucha en el puerto 25 para manejar las conexiones SMTP. El riesgo en este caso está en que si el servidor no está configurado adecuadamente, los atacantes pueden usarlo para enviar spam y hacer que el servidor sea incluido en

blacklists. Asimismo, Postfix puede tener vulnerabilidades que si no se parchean pueden ser explotadas ya que sus versiones antiguas son susceptibles a ataques de ejecución de código remoto, Dos, vulnerabilidades de inyección, etc.

PUERTO: 80/TCP STATE: OPEN SERVICE: HTTP VERSION: Apache httpd 2.2.8

- El puerto 80 está abierto y está usando el servicio HTTP (Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertexto) con la versión Apache httpd 2.2.8. El puerto 80 es el puerto estándar utilizado para las conexiones HTTP, que es el protocolo utilizado para la comunicación en la web sin cifrado. Este puerto es comúnmente utilizado por servidores web para servir contenido a los navegadores de los usuarios. Apache HTTP Server es uno de los servidores web más utilizados en Internet. La versión 2.2.8 es una versión bastante antigua (lanzada en 2008) y presenta algunas implicaciones de seguridad como inyección de código o ataques de denegación de servicio. Esto significa que un atacante puede explotar estas vulnerabilidades, por lo que es vital migrar a una versión más reciente de apache y revisar y ajustar su configuración.

PUERTO 139/TCP STATE: OPEN SERVICE: netbios – ssn VERSION: samba smbd 3.X – 4.X

- El puerto 139 está abierto ejecutando el servicio netbios – ssn con una versión samba smbd dentro del rango 3.X – 4.X. *El puerto 139* es utilizado por el protocolo NetBIOS Session Service, que permite la comunicación entre computadoras en una red local. Es comúnmente utilizado en entornos de red de Windows para el intercambio de archivos y la impresión, así como para otras funciones de red. Que este puerto esté significa que está escuchando y aceptando conexiones entrantes.
  Samba es un software que permite la interoperabilidad entre sistemas Unix/Linux y sistemas Windows. Proporciona servicios de archivos e impresión para clientes de Windows a través de la implementación del protocolo SMB (Server Message Block) y las versiones de Samba en el rango de 3.X a 4.X son utilizadas para ofrecer soporte para el intercambio de archivos y recursos en red entre sistemas Windows y Unix/Linux. Sin embargo, las versiones de Samba 3.X y 4.X han tenido vulnerabilidades de seguridad que podrían ser explotadas si no se actualizan (como **CVE-2015-5370** y **CVE-2017-7494**). Un puerto 139 abierto también podría permitir a un atacante acceder a recursos compartidos en el servidor. Si no se configura adecuadamente, esto podría facilitar la transferencia de datos no autorizada o la ejecución de comandos. Finalmente, una configuración inadecuada de Samba puede exponer archivos y recursos a usuarios no autorizados. Es por ello que también es esencial revisar las configuraciones de Samba para asegurar que se estén aplicando las políticas de seguridad adecuadas.

PUERTO 443/TCP STATE: OPEN SERVICE: SSL/ HTTP VERSION: Apache httpd 2.2.8

Indica que el puerto 443 en el servidor está abierto y está utilizando Apache httpd 2.2.8 como servidor web para HTTPS (SSL/HTTP). Recordemos que Apache httpd 2.2.8 es una versión bastante antigua.

PUERTO 445/TCP STATE: OPEN SERVICE: netbios -ssn VERSION: Samba smbd 3.X – 4.X

El puerto 445 en tu servidor está abierto y está ejecutando un servicio relacionado con NetBIOS a través de Samba con una versión que anteriormente indiqué que está desactualizada.

PUERTO 512/TCP STATE: OPEN SERVICE: exec VERSION: netkit-rsh rexecd

El puerto 512 que está abierto en el servidor y está ejecutando el servicio exec con la versión netkit-rsh rexecd. El servicio rexec puede ser vulnerable a varios tipos de ataques, como la ejecución remota de código y ataques de interceptación, especialmente si no se usa de manera segura.

PUERTO 513/TCP STATE: OPEN SERVICE: login?

PUERTO 514/TCP STATE: OPEN SERVICE: Shell?

PUERTO 666/TCP STATE: OPEN SERVICE: doom?

PUERTO 3306 /TCP STATE: OPEN SERVICE: mysql VERSION: MySQL 5.0.96 – 0ubuntu3

PUERTO 3632/TCP STATE: OPEN SERVICE: distccd VERSION: distccd V1 4.2.3

PUERTO 5901/TCP STATE: OPEN SERVICE: vnc VERSION: VNC (protocool 3.8)

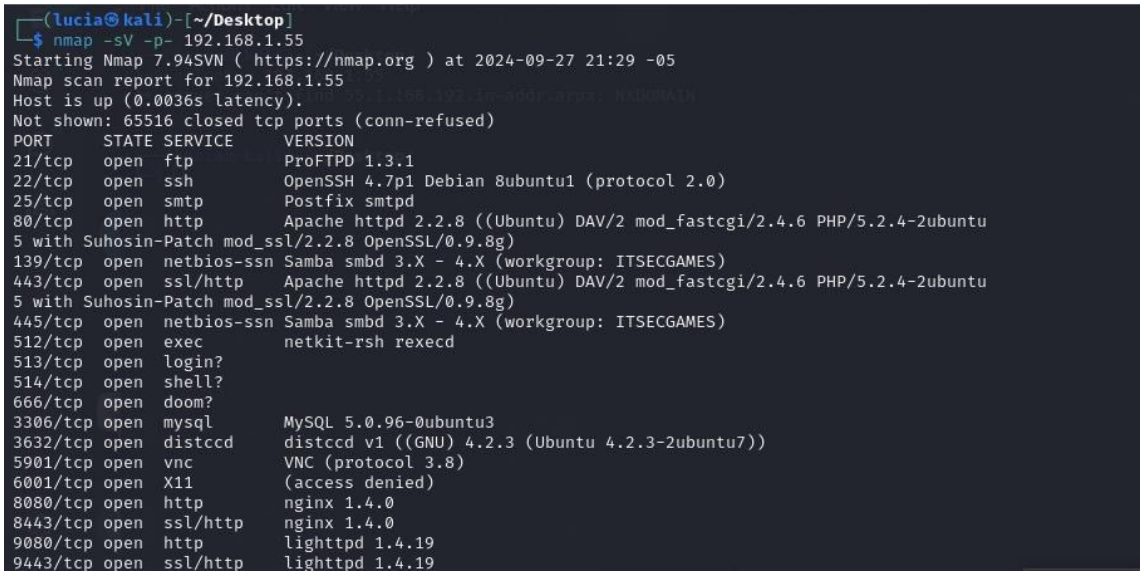
PUERTO 6001/TCP STATE: OPEN SERVICE: X11 VERSION: Access denied

PUERTO 8080/TCP STATE: OPEN SERVICE: http VERSION: nginx 1.4.0

PUERTO 8443/TCP STATE: OPEN SERVICE: ssl/http VERSION: nginx 1.4.0

PUERTO 9080/TCP STATE: OPEN SERVICE: http VERSION: lighttpd 1.4.19

PUERTO 9443 /TCP STATE: OPEN SERVICE: ssl/httpd VERSION: lighttpd 1.4.19



INFORMACIÓN DEL DOMINIO

WHOIS 192.168.1.55

```
┌──(lucia㉿kali)-[~]
└─$ whois 192.168.1.55

#
# 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 sm
ay, and are automatically configured in hundreds of millions of devices.  They are only intended for use within a pr
 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 regist
e from ICANN or IANA.  We are not the source of activity you may see on logs or in e-mail records.  Please refer to
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the
n 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


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

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

#
# 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.
```

NSLOOKUP 192.168.1.55

```
┌──(lucia㉿kali)-[~]
└─$ nslookup 192.168.1.55
** server can't find 55.1.168.192.in-addr.arpa: NXDOMAIN
```

CONTEXTO: La dirección IP 192.168.1.55 pertenece al rango de direcciones 192.168.0.0 - 192.168.255.255, que se encuentran en la categoría de direcciones IP privadas (está dentro de la clase C según teoría de redes), lo que significa que este tipo de direcciones son utilizadas en redes locales y no son enrutables a través de Internet.

Resumen de Clases de Direcciones IP

Clase	Rango	Uso	IP Privada	IP Pública
A	1.0.0.0 - 126.255.255.255	Redes grandes	No hay	10.1.1.1
B	128.0.0.0 - 191.255.255.255	Redes medianas a grandes	172.16.0.0 - 172.31.255.255	128.100.0.1
C	192.0.0.0 - 223.255.255.255	Redes pequeñas	192.168.0.0 - 192.168.255.255	192.0.2.1
D	224.0.0.0 - 239.255.255.255	Multicast	No hay	224.0.0.1
E	240.0.0.0 - 255.255.255.255	Reservada para experimentos	No hay	255.255.255.255

- En ese sentido, la consulta WHOIS que realizamos a la dirección IP 192.168.1.55 nos sugiere que se trata de una dirección IP privada utilizada dentro de una red local. Esto significa que **no tiene un registro público en internet** y esto lo podemos reforzar con los resultados de la consulta nslookup que hicimos a dicha dirección IP, que nos mostró **"** server can't find 55.1.168.192.in-addr.arpa: NXDOMAIN**"** ya que `NXDOMAIN` es un código de respuesta que significa "Non-Existent Domain". Indica que no hay registros DNS disponibles para la dirección IP que estoy consultando.

SUBDOMINIOS ENCONTRADOS

Debido al contexto anterior, no es posible encontrar subdominios asociados a registros públicos de DNS.

VULNERABILIDADES IDENTIFICADAS

Habemus realizado un escaneo con **nikto**, que es una herramienta de código abierto utilizada para realizar escaneos de vulnerabilidades en servidores web cuyo principal función es identificar configuraciones incorrectas, archivos sensibles expuestos y posibles problemas de seguridad en aplicaciones y servidores web. Dicho esto, el comando que ejecuté en la terminal de Kali Linux fue el siguiente:

nikto -h 192.168.1.55

LOS RESULTADOS FUERON LOS SIGUIENTES

Puerto del objetivo: 80

- Se identificó al servidor **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** con módulos adicionales como **DAV/2**, **mod_fastcgi**, **mod_ssl**, y que utiliza **PHP 5.2.4** con el parche de seguridad Suhosin, y una versión antigua de **OpenSSL**.

- **Vulnerabilidad CVE-2003-1418:** Es una vulnerabilidad conocida en la que los números de inodos(cualquier fichero o carpeta alojado en tu cuenta de hosting) se pueden filtrar a través de ETags(uno de los varios mecanismos que HTTP proporciona para la validación de caché web). Un atacante podría usar esta información para obtener metadatos de archivos específicos o deducir información sobre la arquitectura del servidor.
- **No se ha encontrado la cabecera X-Frame-Options**, la cual previene ataques de "clickjacking"
- **La cabecera X-Content-Type-Options no está configurada**. Esto podría permitir que un navegador interprete incorrectamente el tipo de contenido, lo que podría derivar en ataques de tipo Cross-Site Scripting (XSS)
- **El archivo crossdomain.xml contiene una entrada comodín (wildcard),** lo que significa que permite que cualquier dominio realice solicitudes desde tu servidor. Esto puede facilitar ataques de Cross-Site Request Forgery (CSRF) o Cross-Site Scripting (XSS).
- **El módulo mod_ssl, que permite el uso de SSL/TLS en Apache**, **está desactualizado**. Versiones anteriores pueden tener vulnerabilidades críticas.
- **La versión de PHP instalada (5.2.4) está desactualizada.**
- **La versión de OpenSSL (0.9.8g) está desactualizada y contiene vulnerabilidades.**
- **Se encontró una cabecera inusual tcn en la respuesta de la página index.** Esto puede indicar que la negociación de contenido de Apache está habilitada, lo que podría facilitar ataques de enumeración de archivos.
- **El módulo mod_negotiation de Apache está habilitado con la opción MultiViews**, lo que permite a los atacantes probar múltiples nombres de archivos fácilmente, facilitando ataques de fuerza bruta.
- **Las versiones antiguas de mod_ssl son vulnerables a desbordamientos de búfer remoto**, lo que puede permitir la ejecución remota de código y comprometer el servidor
- **Las versiones PHP 3, 4, 5 y 7.0 han alcanzado su fin de vida útil (EOL) y ya no reciben actualizaciones ni soporte**. Esto significa que cualquier vulnerabilidad encontrada en estas versiones no será corregida.
- **El servidor acepta varios métodos HTTP, incluyendo TRACE, que puede ser explotado en ataques de Cross-Site Tracing (XST).**
- **El método HTTP TRACE está habilitado, lo que sugiere que el servidor podría ser vulnerable a ataques de Cross-Site Tracing (XST).**
- **La página /server-status revela información detallada sobre el estado de Apache, incluyendo rutas, procesos, y actividad en tiempo real.** Esta información puede ser utilizada por atacantes para planificar futuros ataques.
- **Se ha encontrado el archivo README, el cual generalmente contiene información sobre el sistema y las configuraciones**. Dejar este archivo expuesto podría dar información valiosa a los atacantes.
- **Se ha encontrado el archivo INSTALL.txt, un archivo predeterminado que usualmente contiene instrucciones de instalación del software**. Este archivo también puede ofrecer información útil a los atacantes.
- **Se ha encontrado el directorio phpMyAdmin, lo que significa que la herramienta está expuesta públicamente.** phpMyAdmin debe ser protegida para evitar accesos no autorizados.
- **Se encontró el archivo Documentation.html de phpMyAdmin, el cual es parte de la instalación estándar.** Como phpMyAdmin es una herramienta crítica, debe estar protegida.
- **Se ha encontrado el archivo wp-config.php, el cual contiene las credenciales de la base de datos de WordPress**. Este archivo es crítico para la seguridad del sitio.

```
┌──(lucia㉿kali)-[~]
└─$ nikto -h 192.168.1.55
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.55
+ Target Hostname:    192.168.1.55
+ Target Port:        80
+ Start Time:         2024-09-30 00:51:04 (GMT-5)
---------------------------------------------------------------------------
+ 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 Ope
+ /: Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov  2 13
cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
ps://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/crossdomai
+ 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
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ 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.
+ 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 bran
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
d: index.bak, index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud
+ 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 a
+ 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-commu
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or rest
+ /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
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /INSTALL.txt: Default file found.
```

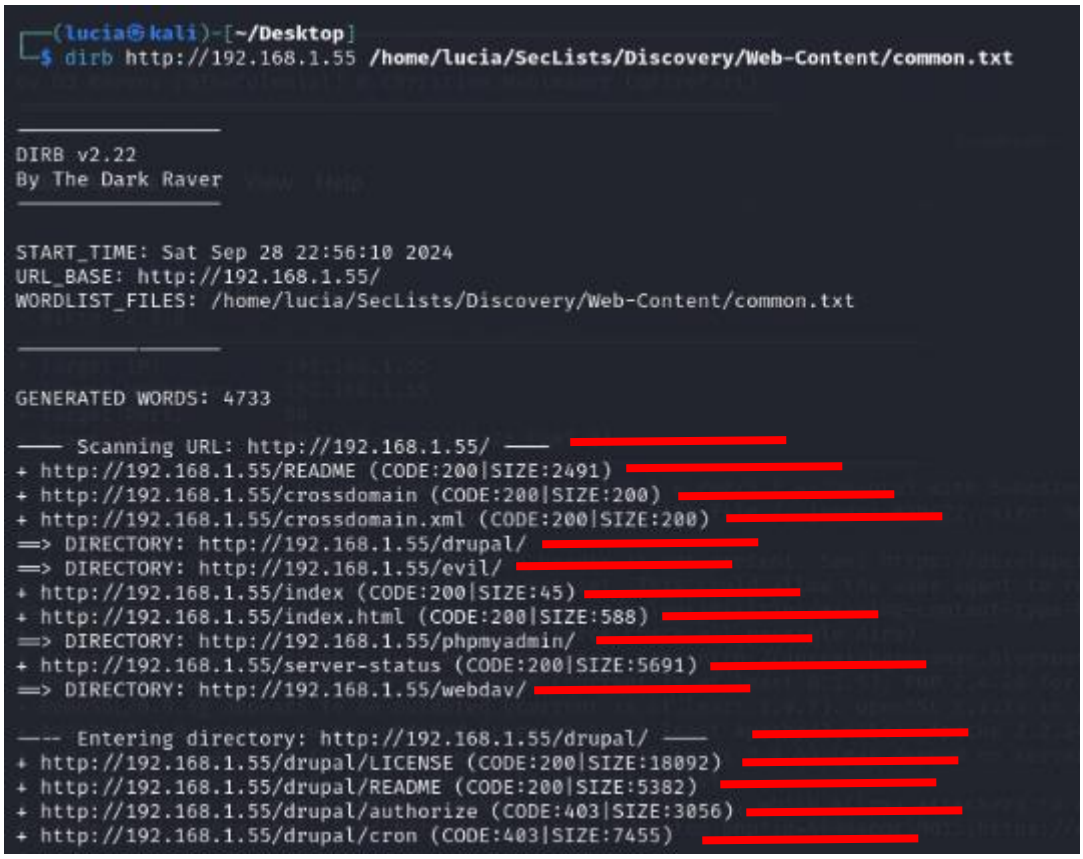
```
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /INSTALL.txt: Default file found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsrea
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limite
+ /#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:       2024-09-30 00:51:28 (GMT-5) (24 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

DIRECTORIOS Y ARCHIVOS ENCONTRADOS

CON GOBUSTER se encontraron los siguientes directorios que señalo con color rojo:

```
┌──(lucia㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.55 -w /home/lucia/SecLists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.55
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/lucia/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 374]
/.htpasswd           (Status: 403) [Size: 379]
/.htaccess           (Status: 403) [Size: 379]
/README              (Status: 200) [Size: 2491]
/crossdomain         (Status: 200) [Size: 200]
/crossdomain.xml     (Status: 200) [Size: 200]
/drupal              (Status: 301) [Size: 403] [--> http://192.168.1.55/drupal/]
/evil                (Status: 301) [Size: 401] [--> http://192.168.1.55/evil/]
/index.html          (Status: 200) [Size: 588]
/index               (Status: 200) [Size: 45]
/phpmyadmin          (Status: 301) [Size: 407] [--> http://192.168.1.55/phpmyadmin/]
/server-status       (Status: 200) [Size: 6898]
/webdav              (Status: 301) [Size: 403] [--> http://192.168.1.55/webdav/]
Progress: 4734 / 4735 (99.98%)
===============================================================
Finished
===============================================================
```

Con dirb se descubrieron las siguientes urls con su correspondiente código http y el tamaño de respuesta:



```
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/phpmyadmin/ ----
+ http://192.168.1.55/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.1.55/phpmyadmin/index.php (CODE:200|SIZE:8132)
==> DIRECTORY: http://192.168.1.55/phpmyadmin/js/
==> DIRECTORY: http://192.168.1.55/phpmyadmin/lang/
==> DIRECTORY: http://192.168.1.55/phpmyadmin/libraries/
+ http://192.168.1.55/phpmyadmin/phpinfo.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.1.55/phpmyadmin/scripts/
==> DIRECTORY: http://192.168.1.55/phpmyadmin/themes/

---- Entering directory: http://192.168.1.55/webdav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/drupal/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/drupal/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/drupal/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/drupal/profiles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/drupal/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/drupal/sites/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/drupal/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/phpmyadmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/phpmyadmin/lang/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/phpmyadmin/libraries/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/phpmyadmin/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.55/phpmyadmin/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Sep 28 22:56:40 2024
DOWNLOADED: 14199 - FOUND: 21
```

END_TIME: Sat Sep 28 22:56:40 2024 DOWNLOADED: 14199 - FOUND: 21

DOWNLOADED 14199: Significa que Dirb ha hecho 14,199 solicitudes HTTP a diferentes rutas basadas en la lista de palabras que estaba utilizando (en este caso, el archivo common.txt que formaba parte del comando que ejecuté, SecLists repo por Daniel Miessler)

FOUND 21: significa que se encontraron 21 rutas (archivos o directorios) válidas, es decir, que dieron una respuesta significativa del servidor, como código 200 o 403.

ANÁLISIS Y CONCLUSIONES

- La etapa de escaneo de red con nmap mostró diversos puertos abiertos que pueden ser usados como vectores de ataque y también hacen uso de servicios con versiones desactualizadas y vulnerables a las técnicas de hacking más básicas.
- La consulta WHOIS y nslooup reveló que se trata de IP privada en una red local y no hay registros públicos en internet.
- El análisis realizado con Nikto nos indica que la mayoría de vulnerabilidades están asociadas a versiones obsoletas y malas configuraciones.
- El análisis hecho con gobuster y dirb arrojó directorios expuestos que pueden ser usados como vectores de ataques y también pueden revelar información sensible.