

RECONOCIMIENTO DE UNA MÁQUINA VULNERABLE

05 de Noviembre de 2024

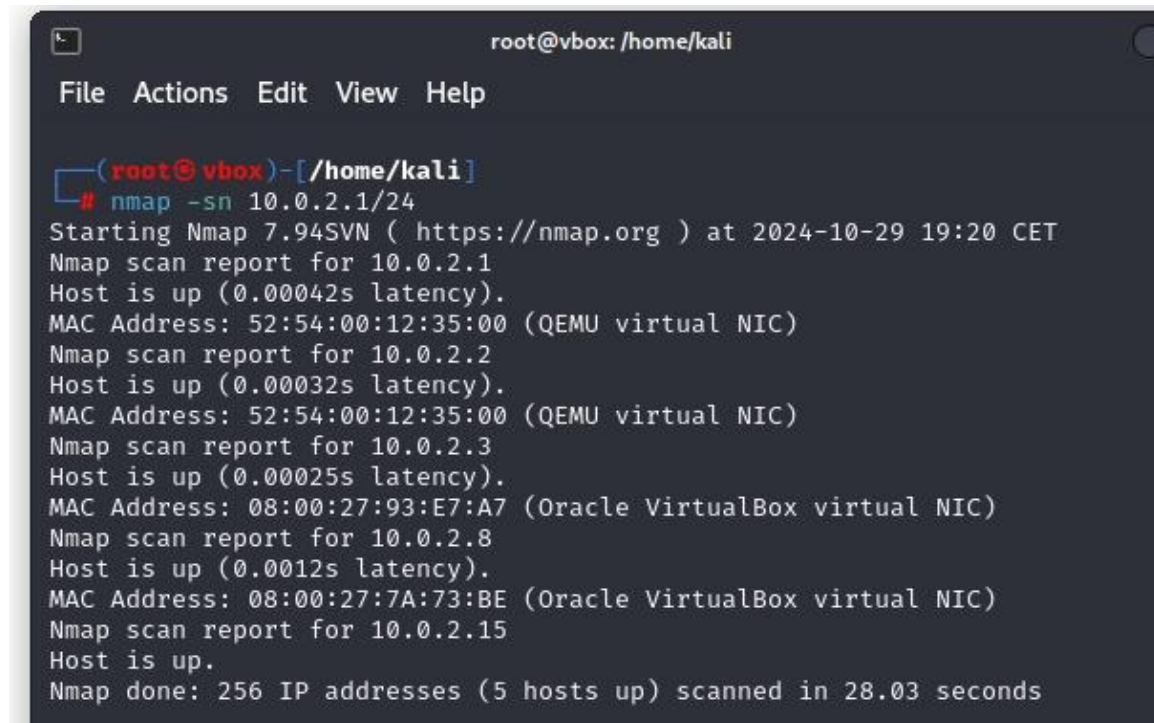
1. Resumen de Entorno

El objetivo de esta auditoría es comprobar la seguridad del sitio web BeeBox. Se comprobarán diferentes escaneo para inspeccionar los servicios activos con nmap. También se realizarán recolección de datos sobre el dominio con las herramientas nslookup y whois.

Por último se realizará un escaneo de vulnerabilidades utilizando la herramienta nikto y se hará un ataque de fuerza bruta de los directorios utilizando las herramientas gobuster y dirb.

2. Resultados de Escaneo de Red

En el escaneo de red utilizamos el comando nmap -sn para escanear la red interna 10.0.2.1/24.



```
root@vbox: /home/kali
File Actions Edit View Help

(root@vbox)-[/home/kali]
# nmap -sn 10.0.2.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 19:20 CET
Nmap scan report for 10.0.2.1
Host is up (0.00042s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00032s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00025s latency).
MAC Address: 08:00:27:93:E7:A7 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up (0.0012s latency).
MAC Address: 08:00:27:7A:73:BE (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 28.03 seconds
```

Los resultados muestran 4 ips en la red interna que se detallan a continuación:

- 10.0.2.2 => Es un software para la virtualización (QEMU)

- 10.0.2.3 => Es un software para la virtualización (QEMU)
- 10.0.2.8 => Es el ip de nuestra máquina Kali desde donde realizamos el escaneo.
- 10.0.2.15=> Es el ip de la máquina que contiene el servidor BeeBox.

3. Resultados de Enumeración de Servicios

En la enumeración de servicios utilizamos el comando `nmap -sV -p- 10.0.2.15`

```

root@vbox: /home/kali
File Actions Edit View Help
nmap -sV -p- 10.0.2.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 19:26 CET
Nmap scan report for 10.0.2.8
Host is up (0.0011s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp?
80/tcp    open  http         Apache httpd 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)
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 with 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?
513/tcp   open  login?
514/tcp   open  shell?
666/tcp   open  doom?
3306/tcp  open  mysql?
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

```

Se detectó una lista de puertos abiertos en los cuales en varios se especificaba el servicio, esta lista se detalla a continuación:

- 22/tcp => detectado como abierto con la versión OpenSSH 4.71p1
- 80/tcp - 443/tcp => detectado como abierto con la versión de Apache httpd 2.2.8
- 139/tcp - 445/tcp => detectado como abierto con la versión de Samba smbd 3. X - 4. X
- 3632/tcp => detectado como abierto con la versión distccd v1 (GNU) 4.2.3

- 5901/tcp => detectado como abierto con la versión VNC(protocol 3.8)
- 8080/tcp - 8443/tcp => detectados como abierto con la versión nginx 1.4.0
- 9080/tcp - 9443/tcp => detectados como abiertos con la versión lighttpd 1.4.19

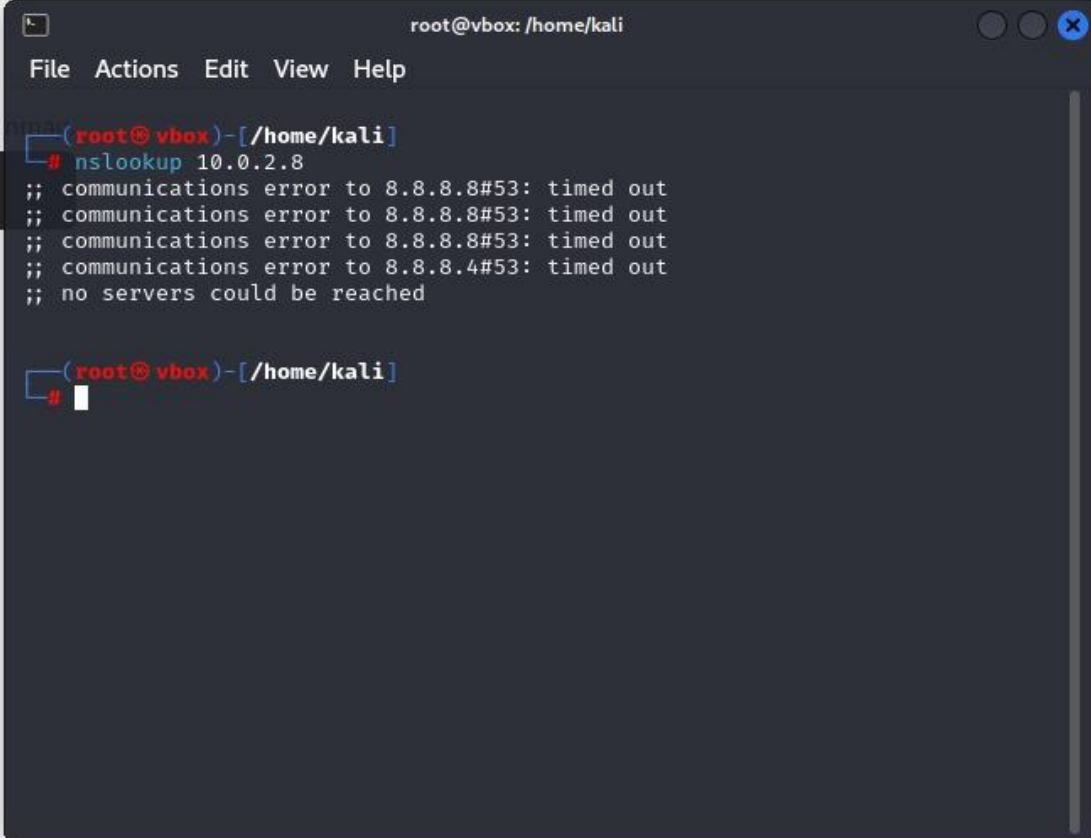
Los puertos 21/tcp, 25/tcp, 512/tcp, 513/tcp, 514/tcp, 666/tcp se detectaron abiertos pero sin especificación del servicio.

El puerto 6001/tcp esta abierto, sin embargo, el servicio negó el acceso.

4. Información del Dominio

Se utilizó el comando nslookup 10.0.2.15 para recaudar información del dominio, pero no logró comunicarse con el DNS

on



```
root@vbox: /home/kali
File Actions Edit View Help

(root@vbox)-[/home/kali]
# nslookup 10.0.2.8
;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.4#53: timed out
;; no servers could be reached

(root@vbox)-[/home/kali]
#
```

Por otro lado se utilizó el comando whois 10.0.2.15

```
ra de servicios.
rec File Actions Edit View Help root@vbox: /home/kali
-5 (root@vbox)-[/home/kali]
-# whois 10.0.2.8
#
# ARIN WHOIS data and services are subject to the Terms of Use
-5 # 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/
CC #
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
oku #
#
NetRange: 10.0.0.0 - 10.255.255.255
CIDR: 10.0.0.0/8
NetName: PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
is: NetHandle: NET-10-0-0-1
Parent: ()
< NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate:
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently
cto operated networks, which might be as small as a single computer connected to
a home gateway, and are automatically configured in hundreds of millions of d
eices. They are only intended for use within a private context and traffic
```

En la información del dominio encontramos que nos lo da IANA, esto es debido a que estamos en una red interna de la máquina virtual. La información que nos da, es que esta dirección es pertenece a un puerta independiente de un hogar. Lo cual nos hace pensar que la BeeBox es de uso doméstico

6.Vulnerabilidades Identificadas

En el análisis de vulnerabilidades se utilizo el comando nikto -h 10.0.2.15

```
root@vbox: /home/kali
File Actions Edit View Help
- (root@vbox)-[/home/kali]
-# nikto -h 10.0.2.8
- Nikto v2.5.0
+ Target IP: 10.0.2.8
+ Target Hostname: 10.0.2.8
+ Target Port: 80
+ Start Time: 2024-10-29 19:39:31 (GMT1)
+ 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 19:20:24 2014. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1410
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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
+ /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 alternatives 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 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 3.0.72). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.56). Apache 2.2.34 is the EOL for the 2.x branch.
+ 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_Tracing
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. 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.
+ /php-config.php: php-config.php file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time: 2024-10-29 19:40:00 (GMT1) (29 seconds)
+ 1 Host(s) tested
- (root@vbox)-[/home/kali]
-#
```

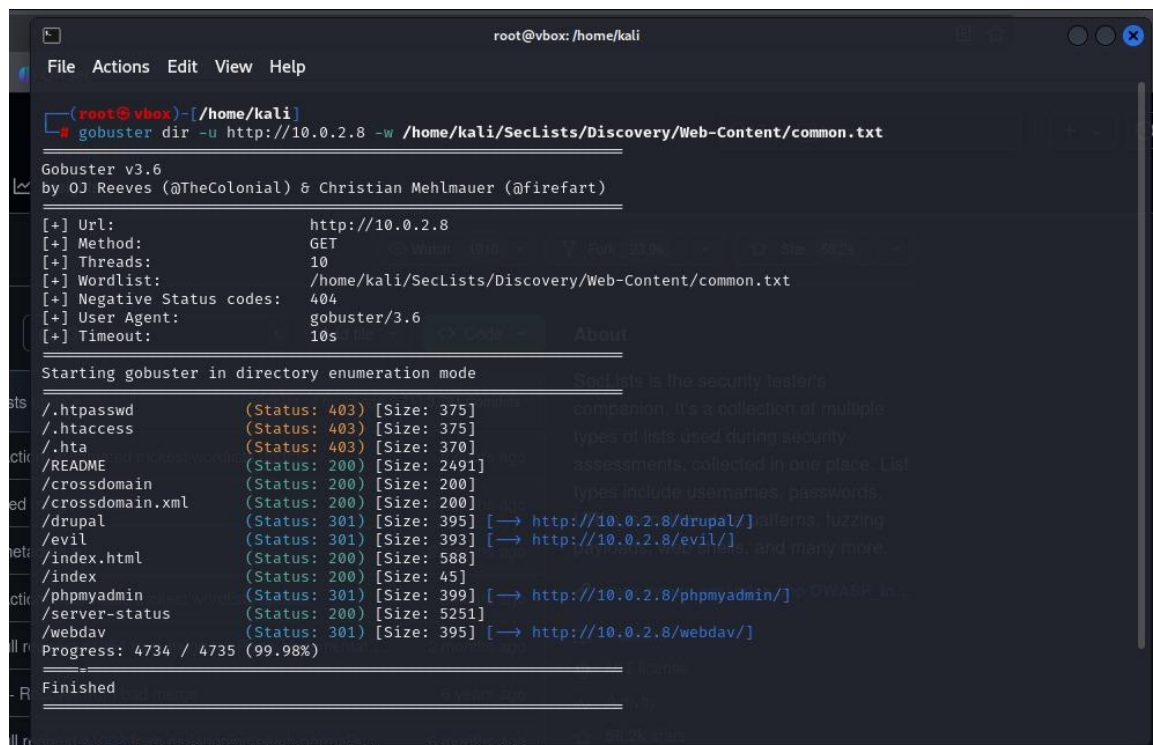
El escaneo de vulnerabilidades dio como resultado una amplia lista, la cual se detalla a continuación:

- Apache 2.2.8 CVE-2003-1418 => En OpenBSD permite a los atacantes remotos obtener información sensible a través de el encabezado ETag, que revela el número de inodo, o el límite MIME multiparte, que revela los ID de los proceso hijos (PID). Nivel de riesgo mediano(4.3)
- El encabezado X-Content-Type-Options no esta configurado, lo que permite que cualquiera pueda renderizar cualquier contenido en la web.
- Apache mod_negotiation esta habilitado en vista multiples, lo que ocasiona que los atacantes puedan realizar facilmente ataques de fuerza bruta a directorios.

Las demás vulnerabilidades se pueden resolver actualizando y parcheando el sistema a las últimas versiones, o a las versiones más estables. Como se indica en la imagen del escaneo, estan desactualizadas.

6. Directorios y Archivos Encontrados

Para la fuerza bruta de directorios usamos el comando gobuster dir -u junto con una seclist de common.txt.



```
root@vbox: /home/kali
File Actions Edit View Help
(root@vbox)-[/home/kali]
gobuster dir -u http://10.0.2.8 -w /home/kali/SecLists/Discovery/Web-Content/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.0.2.8
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.htpasswd (Status: 403) [Size: 375]
/.htaccess (Status: 403) [Size: 375]
/.hta (Status: 403) [Size: 370]
/README (Status: 200) [Size: 2491]
/crossdomain (Status: 200) [Size: 200]
/crossdomain.xml (Status: 200) [Size: 200]
/drupal (Status: 301) [Size: 395] [→ http://10.0.2.8/drupal/] allerns, fuzzing
/evil (Status: 301) [Size: 393] [→ http://10.0.2.8/evil/] and many more
/index.html (Status: 200) [Size: 588]
/index (Status: 200) [Size: 45]
/phpmyadmin (Status: 301) [Size: 399] [→ http://10.0.2.8/phpmyadmin/]
/server-status (Status: 200) [Size: 5251]
/webdav (Status: 301) [Size: 395] [→ http://10.0.2.8/webdav/]

Progress: 4734 / 4735 (99.98%)

Finished
```

Se detectaron todos los directorio del web site, incluido los domains y los index. Así como también el server status y el servidor php. La lista de los dominios junto con el directorio de phpadmin implica un gran peligro para el host, debido a que el acceso los archivos de administrador podría garantizarle un escalada de privilegios y permanencia en la red.

Los directorios de index, podrían utilizarse para cargar código malicioso para quienes visite el website, por lo que podría ser una brecha peligrosa para los usuarios.

7. Conclusión

En conclusión el web site es sumamente vulnerables a múltiples ataques, desde diferentes formas. La recomendación inmediata es actualizar todos los servicios a su versión mas reciente y volver a hacer una auditoría lo antes posibles para confirmar posibles brechas de seguridad de nuevo. Debe actualizarse el sistema en menos de 24 horas debido a la gravedad de todos los posibles ataques y brechas existentes. Por último se recomienda configurar un firewalls para filtrar los puertos tpc donde se utilizan servicios, y cerrar aquellos puertos que no se utilizen para minimizar riesgos de ataque, como por ejemplo podría ocurrir con el FTP.