



04 de junio de 2021
Ficha N° 6 DNSMAP
CSIRT DE GOBIERNO

Comando de la semana “DNSMAP”

I. CONTEXTO

Este documento, denominado “comando de la semana”, tiene como objetivo ilustrar sobre herramientas que pueden ser de utilidad para el lector, a objeto de ir potenciando las capacidades locales de autochequeo, detección simple de vulnerabilidades que están expuestas a internet en sus activos de información y, a su vez, la obtención de una verificación de la subsanación de aquellas que se les han sido reportadas, facilitando la interacción con el CSIRT de Gobierno. El objetivo no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por “CSIRT GOB CL”.

II. INTRODUCCIÓN

Una de las tareas regulares que en ciberseguridad se realizan es la verificación de los sitios o sistemas que están expuestos a Internet. Revisar regularmente esta información nos permite prevenir la aparición de algún dominio o subdominio que no se nos haya informado o bien que sea producto de algún problema de configuración o problema en algún paso a producción. Cualquier activo institucional que está publicado en Internet y del que los equipos no están conscientes de tal situación constituye en un potencial vector de entrada y además sin la vigilancia habitual, pues probablemente no está registrado en los sistemas de monitoreo ni está informado al CSIRT de Gobierno.

Para este caso existe un comando Linux que nos ayuda a recopilar información manera simple, con una herramienta de código abierto y, en base a sus resultados tomar decisiones de monitoreo y vigilancia, además de contratarlo con los reportes internos: DNSMAP.



¿Qué es DNSMAP?

DNSMAP¹ está destinado principalmente a ser utilizado por investigadores o encargados de ciberseguridad durante la fase de recopilación o enumeración de información de las evaluaciones de seguridad de la infraestructura. Durante la etapa de enumeración, el investigador de seguridad normalmente descubriría los bloques de red IP de la empresa objetivo, los nombres de dominio, los números de teléfono, etc.



La fuerza bruta de subdominios es otra técnica que debe usarse en la etapa de enumeración, ya que es especialmente útil cuando otras técnicas de enumeración de dominios, como las transferencias de zona², no funcionan (por cierto, rara vez se observa que las transferencias de zona se permitan públicamente en estos días).

NOTA: Dado que es importante un buen manejo de los comandos básicos de Linux, tanto para posteriores manipulaciones como para usos de la información resultante de la ejecución de los comandos, es que el comité editorial decidió que se incluya en esta edición y en las subsiguientes un anexo de comandos Linux que son de utilidad para moverse en este sistema operativo. Se sugiere dominarlos todos para facilitar el acceso y manipulación de la información. En futuras ediciones se irán incorporando nociones más avanzadas sobre el uso de estos comandos para procesamiento de archivos, procesos, y de sus usos en scripting.

Vea anexo I: Comandos básicos de Linux

¹ Fuente: <http://code.google.com/p/dnsmap/>

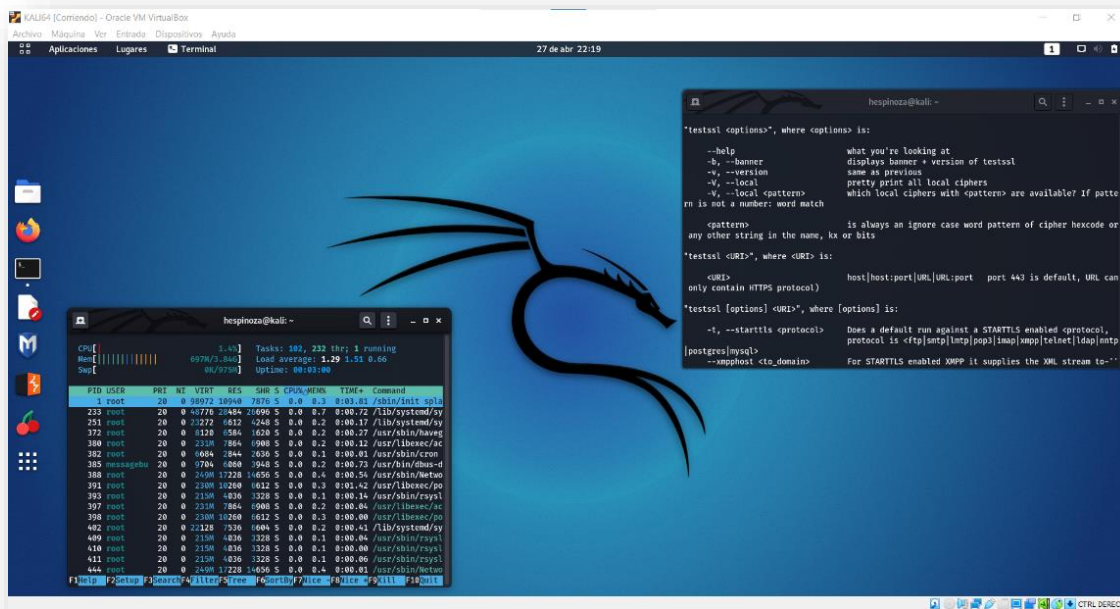
² <https://blog.nivel4.com/noticias/ejercicio-practico-como-funciona-una-transferencia-de-zona/>



III. PASO A PASO

PASO 1: Un entorno adecuado para trabajar.

Primero debe contar con una distribución de Kali³ Linux funcionando ya sea en una máquina física o en una máquina virtual⁴⁵.



PASO 2: Instalar el comando.

Una vez que se cuenta con este sistema operativo de manera funcional podemos instalar el comando “DNSMAP”; en general este ya viene preinstalado en la distribución KALI⁶, pero si no fuere así puede instalarlo con los siguientes comandos, **previamente tomando privilegios de usuario “root”**:

```
apt-get install dnsmap
```

³ <https://www.kali.org/downloads/>

⁴

https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0

⁵ <https://www.virtualbox.org/wiki/Downloads>

⁶ <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>



PASO3: Verificar su instalación.

Una vez que se instalado podemos verificar y explorar las múltiples opciones que ofrece para su ejecución:

```
#dnsmmap
dnsmmap 0.35 - DNS Network Mapper





usage: dnsmmap <target-domain> [options]

options:
-w <wordlist-file>
-r <regular-results-file>
-c <csv-results-file>
-d <delay-millisecs>
-i <ips-to-ignore> (useful if you're obtaining false positives)
```

Paso 4: Ponerlo en marcha para verificar nuestra infraestructura.

Algunos ejemplos de ejecución básica para nuestros primeros pasos:

EJEMPLOS

- 1) Buscar sitios o sistemas web asociados al dominio example.com:
 `dnsmmap example.com`
- 2) Buscar sitios o sistemas web asociados al dominio example.com, en base a un diccionario de palabras preestablecidas, y escribiendo el resultado en un archivo de texto denominado domainbf_results.txt, en el directorio /tmp:
 `dnsmmap example.com -w yourwordlist.txt -r /tmp/domainbf_results.txt`
- 3) Buscar sitios o sistemas web asociados al dominio example.com, escribiendo el resultado en el directorio /tmp y teniendo en consideración retardo de 3000ms entre solicitudes:
 `dnsmmap example.com -r /tmp/ -d 3000`
- 4) Buscar sitios o sistemas web asociados al dominio example.com, escribiendo el resultado en el directorio /tmp y teniendo en consideración retardo de 3000ms entre solicitudes:
 `dnsmmap example.com -r ./domainbf_results.txt`






Que se ve en una consola KALI después de la ejecución más simple:

Vista de un ejemplo: Ejecución del comando:

```
#dnsmap csirt.gob.cl
```

```
root@V: ~  
# (root@V) ~  
# dnsmap csirt.gob.cl  
dnsmap 0.35 - DNS Network Mapper  
  
[+] searching (sub)domains for csirt.gob.cl using built-in wordlist  
[+] using maximum random delay of 10 millisecond(s) between requests  
  
eventos.csirt.gob.cl  
IP address #1: 163.247.175.10  
  
mp.csirt.gob.cl  
IP address #1: 163.247.70.133  
  
www.csirt.gob.cl  
IP address #1: 163.247.175.10  
  
[+] 3 (sub)domains and 3 IP address(es) found  
[+] completion time: 13 second(s)  
  
# (root@V) ~  
#
```

En este ejemplo podemos visualizar que existen al dominio csirt.gob.cl los siguientes activos:

-  Eventos.csirt.gob.cl
-  Mp.csirt.gob.cl
-  www.csirt.gob.cl

Estos activos los podemos contrastar con los que nos han reportado y si están bajo el esquema de vigilancia y monitoreo adecuado.

Otro ejemplo:

```
#dnsmap digital.gob.cl
```



Cuyo resultado encuentra los siguientes activos:

-  biblioteca.digital.gob.cl
-  chat.digital.gob.cl
-  logs.digital.gob.cl
-  mail.digital.gob.cl
-  prueba.digital.gob.cl
-  sc.digital.gob.cl
-  soporte.digital.gob.cl
-  stats.digital.gob.cl
-  test.digital.gob.cl
-  vpn.digital.gob.cl
-  www.digital.gob.cl

Lo que visto en la consola de KALI se vería así, donde además se aprecia el direccionamiento IP asignado al activo encontrado:

```
root@V: ~  
(root@V) - [~]  
# dnsmap digital.gob.cl  
dnsmap 0.35 - DNS Network Mapper  
  
[+] searching (sub)domains for digital.gob.cl using built-in wordlist  
[+] using maximum random delay of 10 millisecond(s) between requests  
  
biblioteca.digital.gob.cl  
IP address #1: 52.41.239.29  
IP address #2: 52.10.54.195  
IP address #3: 44.235.176.128  
  
chat.digital.gob.cl  
IP address #1: 52.32.73.124  
  
logs.digital.gob.cl  
IP address #1: 52.34.55.222  
  
mail.digital.gob.cl  
IPv6 address #1: 2800:3f0:4003:c02::79  
  
mail.digital.gob.cl  
IP address #1: 172.217.192.121
```



Junto a dnsmap viene incluido un script en bash⁷, denominado dnsmap-bulk, cuya función es facilitar el uso de dnsmap cuando se quiere analizar un listado de dominios, permitiendo escribir el resultado en un directorio especificado por el usuario.

```
—# more8 /usr/bin/dnsmap-bulk
#!/bin/bash
# Version 0.1
# Copyright 2009 gnutizen.org, by pagvac
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License along
# with this program; if not, write to the Free Software Foundation, Inc.,
# 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

if [[ $# -ne 1 && $# -ne 2 ]]
then
    echo "usage: `basename $0` <domains-file> [results-path]";
    echo "e.g.:";
    echo "`basename $0` domains.txt";
    echo "`basename $0` domains.txt /tmp/";
    exit
fi
for i in `cat $1`
do
    if [[ $# -eq 1 ]]
    then
        dnsmap $i
    elif [[ $# -eq 2 ]]
    then
        dnsmap $i -r $2
    fi
done
```

⁷ [https://en.wikipedia.org/wiki/Bash_\(Unix_shell\)](https://en.wikipedia.org/wiki/Bash_(Unix_shell))

⁸ [https://es.wikipedia.org/wiki/More_\(comando\)](https://es.wikipedia.org/wiki/More_(comando))



Algunos ejemplos de esta herramienta complementaria:

Ejecución en vacío para desplegar la ayuda incorporada en el comando mismo:

```
root @ kali: ~ # dnsmap-bulk
```

```
uso: dnsmap-bulk.sh <archivo-de-dominios> [ruta de resultados]
```

Por ejemplo:

Procesar con dnsmap-bulk un listado de dominios que tengo escritos en un archivo denominado domains.txt:

```
root @ kali: ~ # dnsmap-bulk domains.txt
```

Procesar con dnsmap-bulk un listado de dominios que tengo escritos en un archivo denominado domains.txt y dejar los resultados en un directorio “/tmp”:

```
root @ kali: ~ # dnsmap-bulk domains.txt /tmp/
```

Estudie las múltiples opciones que tiene el comando para obtener resultados específicos o redirigir la salida a un archivo, para su inclusión en informes posteriores.

En caso de cualquier inquietud no dudes en consultarnos a soc-csirt@interior.gob.cl.



Anexo I: Comandos Básicos de Linux

Comandos básicos

Los comandos son esencialmente los mismos que cualquier sistema UNIX. En las tablas que se presentan a continuación se tiene la lista de comandos más frecuentes.

| Comando/Sintaxis | Descripción | Ejemplos |
|--------------------------------------|---------------------------------------|------------------------------|
| cat <i>fich1</i> [... <i>fichN</i>] | Concatena y muestra un archivos | cat /etc/passwd |
| | archivos | cat dict1 dict2 dict |
| cd [<i>dir</i>] | Cambia de directorio | cd /tmp |
| chmod <i>permisos fich</i> | Cambia los permisos de un archivo | chmod +x miscript |
| chown <i>usuario:grupo fich</i> | Cambia el dueño un archivo | chown nobody miscript |
| cp <i>fich1...fichN dir</i> | Copia archivos | cp foo foo.backup |
| diff [-e] <i>arch1 arch2</i> | Encuentra diferencia entre archivos | diff foo.c newfoo.c |
| du [-sabr] <i>fich</i> | Reporta el tamaño del directorio | du -s /home/ |
| file <i>arch</i> | Muestra el tipo de un archivo | file arc_desconocido |
| find <i>dir test acción</i> | Encuentra archivos. | find . -name ``.bak" – print |
| grep [-cilmv] <i>expr archivos</i> | Busca patrones en archivos | grep mike /etc/passwd |
| head -count <i>fich</i> | Muestra el inicio de un archivo | head prog1.c |
| mkdir <i>dir</i> | Crea un directorio. | mkdir temp |
| mv <i>fich1 ...fichN dir</i> | Mueve un archivo(s) a un directorio | mv a.out prog1 |
| mv <i>fich1 fich2</i> | Renombra un archivo. | mv .c prog_dir |
| less / more <i>fich(s)</i> | Visualiza página a página un archivo. | more muy_largo.c |
| | less acepta comandos vi. | less muy_largo.c |
| ln [-s] <i>fich acceso</i> | Crea un acceso directo a un archivo | ln -s /users/mike/.profile . |



| | | |
|-------------------------------|---------------------------------------|------------------------------|
| <code>ls</code> | Lista el contenido del directorio | <code>ls -l /usr/bin</code> |
| <code>pwd</code> | Muestra la ruta del directorio actual | <code>Pwd</code> |
| <code>rm fich</code> | Borra un fichero. | <code>rm foo.c</code> |
| <code>rm -r dir</code> | Borra un todo un directorio | <code>rm -rf prog_dir</code> |
| <code>rmdir dir</code> | Borra un directorio vacío | <code>rmdir prog_dir</code> |
| <code>tail -count fich</code> | Muestra el final de un archivo | <code>tail prog1.c</code> |
| <code>vi fich</code> | Edita un archivo. | <code>vi .profile</code> |

Comandos Linux/Unix de manipulación de archivos y directorios:

| Comando/Sintaxis | Descripción | Ejemplos |
|--|--|---|
| <code>at [-lr] hora [fecha]</code> | Ejecuta un comando mas tarde | <code>at 6pm Friday miscript</code> |
| <code>cal [[mes] año]</code> | Muestra un calendario del mes/año | <code>cal 1 2025</code> |
| <code>date [mmdhmm] [+form]</code> | Muestra la hora y la fecha | <code>Date</code> |
| <code>echo string</code> | Escribe mensaje en la salida estándar | <code>echo "Hola mundo"</code> |
| <code>finger usuario</code> | Muestra información general sobre un usuario en la red | <code>finger nn@maquina.aca.com.co</code> |
| <code>id</code> | Número id de un usuario | <code>id usuario</code> |
| <code>kill [-señal] PID</code> | Matar un proceso | <code>kill 1234</code> |
| <code>man comando</code> | Ayuda del comando especificado | <code>man gcc man -k printer</code> |
| <code>passwd</code> | Cambia la contraseña. | <code>passwd</code> |
| <code>ps [axiu]</code> | Muestra información sobre los procesos que se están ejecutando en el sistema | <code>ps -ux</code> |
| <code>who / rwho</code> | Muestra información de los usuarios conectados al sistema. | <code>who</code> |



Comandos Linux/Unix más frecuentes:

| Linux | DOS | Significado |
|-----------|-----------|---|
| cat | type | Ver contenido de un archivo. |
| cd, chdir | cd, chdir | Cambio el directorio en curso. |
| chmod | attrib | Cambia los atributos. |
| clear | cls | Borra la pantalla. |
| ls | dir | Ver contenido de directorio. |
| mkdir | md, mkdir | Creación de subdirectorio. |
| more | more | Muestra un archivo pantalla por pantalla. |
| mv | move | Mover un archivo o directorio. |
| rmdir | rd, rmdir | Eliminación de subdirectorio. |
| rm -r | deltree | Eliminación de subdirectorio y todo su contenido. |