Nombre: Christian Jiménez
Fecha: 3/01/21
Pais: Bolivia

SCRIPTS DE NMAP

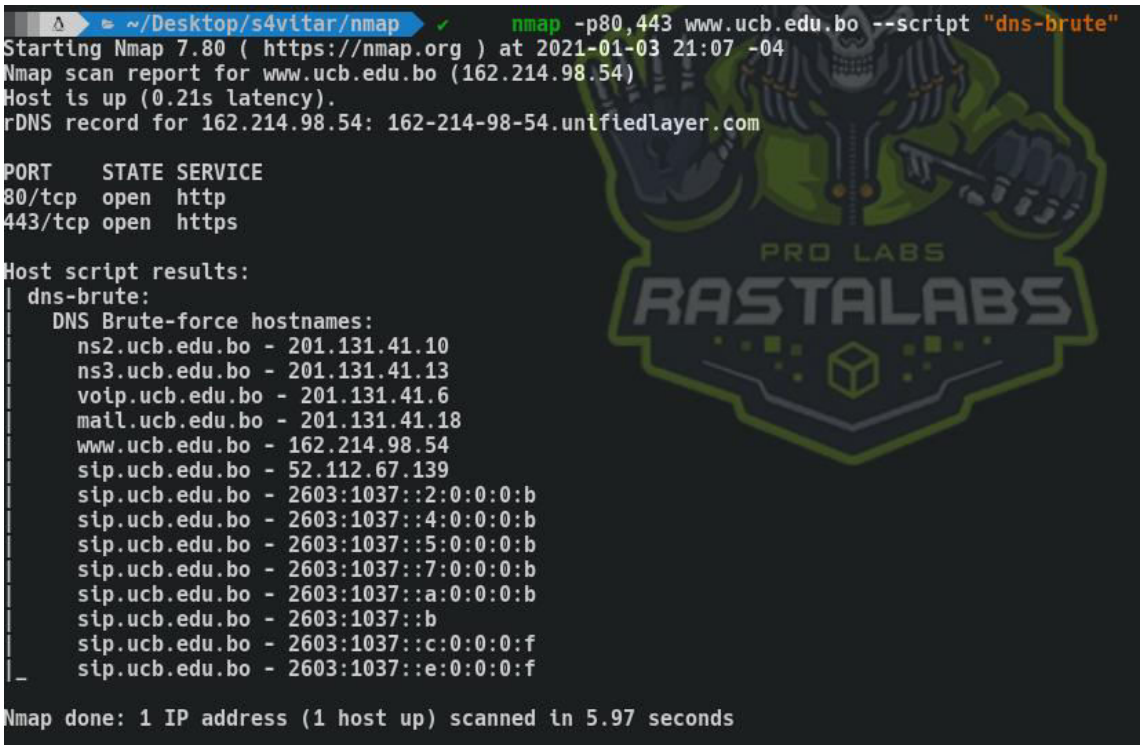
Buscando en internet encontré ciertos scripts de nmap que dan buena información a los atacantes:

1. Dns-brute
2. Http-enum
3. Http-grep
4. Ssh-brute
5. Http-wordpress-enum
6. Mysql-empty-password
7. Http-waf-detect

A continuación, se explicará cada uno:

DNS-BRUTE

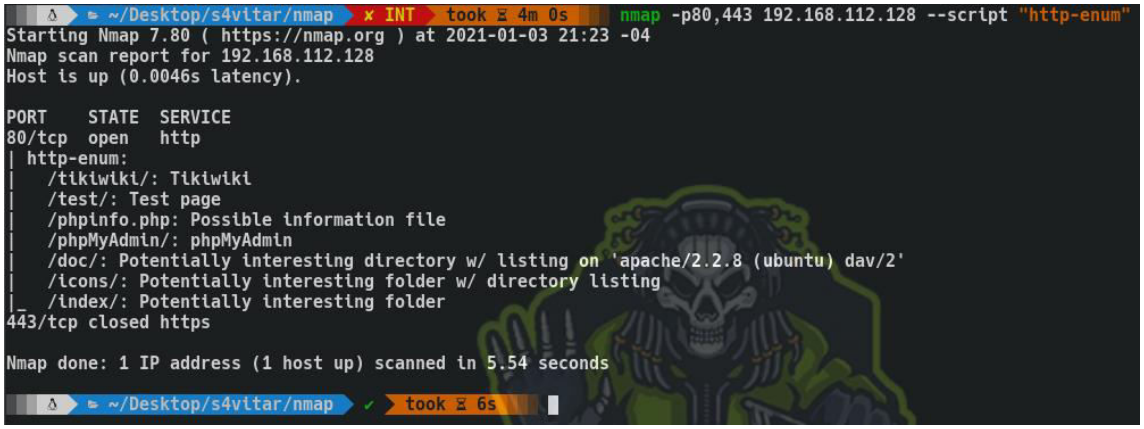
Enumera subdominios y sus direcciones IP de servidor correspondientes.



HTTP-ENUM

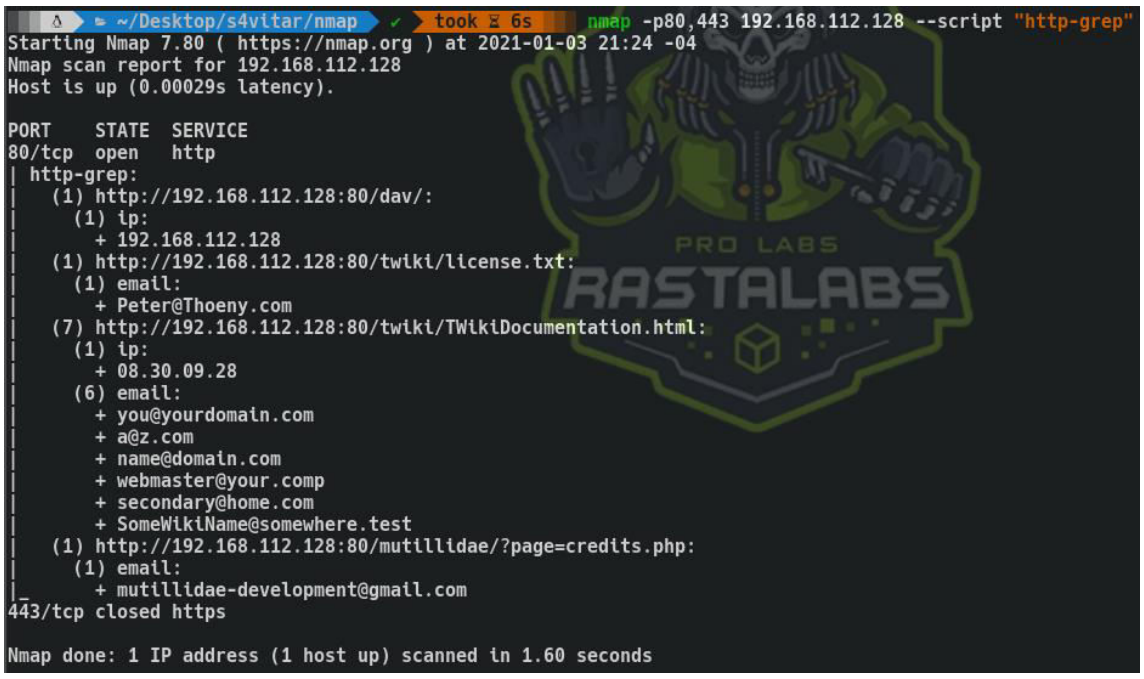
Envía más de 2000 consultas al servidor web, intentando acceder a archivos y/o directorios específicos de aplicaciones web populares. Si el servidor devuelve el código " 200 OK " o " 401 Autenticación requerida " a cualquiera de las consultas significará que el archivo o directorio deseado está disponible en el servidor.

Nombre: Christian Jiménez
Fecha: 3/01/21
Pais: Bolivia



HTTP-GREP

Busca información útil en la página dada. De forma predeterminada, devuelve las direcciones de correo electrónico y las direcciones IP que se encuentran en todas las subpáginas descubiertas por el script. Podemos dar el script en la subpágina del argumento http-grep.url que queremos buscar.



SSH-BRUTE

Se utiliza para romper las contraseñas de servicios SSH con la entrada de texto predictivo. De forma predeterminada, utiliza su propia base de datos, más bien una extensa base de datos de usuarios y contraseñas. Sin embargo, puede pasar nuestras cartas al script usando los argumentos userdb y passdb.

Nombre: Christian Jiménez
Fecha: 3/01/21
Pais: Bolivia

```
~/Desktop/s4vitar/nmap  x INT  took ⧖ 18s   nmap -p22 192.168.112.128 --script "ssh-brute"
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-03 21:28 -04
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
```

HTTP-WORDPRESS-ENUM

Verifica qué temas y complementos se han instalado en el sitio escaneado. Solo para páginas con CMS WordPress.

```
~/Desktop/s4vitar/nmap  x INT  took ⧖ 9s   nmap -p80,443 192.168.112.128 --script "http-wordpress-enum"
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-03 21:30 -04
Nmap scan report for 192.168.112.128
Host is up (0.00037s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

MYSQL-EMPTY-PASSWORD

Comprueba si es posible iniciar sesión en el servidor MySQL a la cuenta raíz o anónima utilizando una contraseña vacía.

```
~/Desktop/s4vitar/nmap  ✓     nmap -p3306 192.168.112.128 --script "mysql-empty-password"
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-03 21:32 -04
Nmap scan report for 192.168.112.128
Host is up (0.00042s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-empty-password:
|_  root account has empty password

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Nombre: Christian Jiménez
Fecha: 3/01/21
Pais: Bolivia

```
~/Desktop/s4vitar/nmap ✓ took ⧖ 1m 40s mysql -u root -h 192.168.112.128
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 19
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

HTTP-WAF-DETECT

Está diseñado para ayudarnos a conocer la presencia de un firewall de aplicaciones web. Probará el servidor web objetivo con varias solicitudes. Primero, enviará una solicitud web normal y registrará la respuesta del servidor. Luego, enviará otra solicitud con una carga útil (URL mal formada) y comparará las respuestas. Este método de detección de WAF está lejos de ser perfecto y puede variar según el tipo de servidor web y el producto WAF.

```
~/Desktop/s4vitar/nmap ✓ took ⧖ 1m 31s nmap -p80 --script "http-waf-detect" --script-args="http-waf-detect.aggro,http-waf-detect.detectBodychanges" 192.168.112.128
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-03 21:39 -04
Nmap scan report for 192.168.112.128
Host is up (0.00049s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

En este caso no se cuenta con un WAF.

Saludos s4itar que este año todas tus metas y objetivos se cumplan bien hack, gracias por tu aporte a la comunidad. ¡Eres un Crack!