Nmap como herramienta de seguridad

Situación de la maquina servidor:

Ubuntu 12.04 LTS (AMD64) Utilizamos xampp 5.6.32 / PHP 5.6.32 (https://www.apachefriends.org/es/download.html)

Para que la máquina servidor sea capaz de verse con el host hay que añadir una tarjeta de red (HOST-ONLY) a la máquina y encenderla con mediante:

```
ifup (nombre de la tarjeta, que lo podremos obtener mediante ifconfig -a)
```

Una vez tenemos todo instalado procedemos a utilizar Nmap.

Por supuesto hay que tener iniciado el servidor para poder escanear las características:

```
/opt/lampp/xampp start
```

Nmap, mediante su poderosa y flexible característica denominada NSE (Nmap Scripting Engine) permite a los usuarios escribir (y compartir) scripts sencillos para automatizar una amplia diversidad de tareas de red.

Ejemplos de cosas que podemos hacer con nmap:

1ºUn simple uso de nmap IP(192.168.56.20) nos muestra la información de los

```
puertos que están abiertos:
port      state   service
21/tcp    open    ftp
80/tcp    open    http
443/tcp   open    https
3306/tcp  open    mysql
```

2º nmap -A habilita la detección de sistema operativo y versión.

Starting Nmap 7.60 (https://nmap.org) at 2017-11-11 13:30 CET Nmap scan report for 192.168.56.20 Host is up (0.0022s latency). Not shown: 996 closed ports PORT STATE SERVICE VERSION 21/tcp open ftp ProFTPD 1.3.4c 80/tcp open http Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2m PHP/5.6.32 mod_perl/2.0.8-dev Perl/v5.16.3) |_http-server-header: Apache/2.4.29 (Unix) OpenSSL/1.0.2m PHP/5.6.32 mod_perl/2.0.8-dev Perl/v5.16.3 | http-title: Welcome to XAMPP |_Requested resource was http://192.168.56.20/dashboard/ 443/tcp open ssl/http Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2m PHP/5.6.32 mod_perl/2.0.8-dev Perl/v5.16.3) |_http-server-header: Apache/2.4.29 (Unix) OpenSSL/1.0.2m PHP/5.6.32

mod_perl/2.0.8-dev Perl/v5.16.3 | http-title: Welcome to XAMPP |_Requested resource was https://192.168.56.20/dashboard/ | ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE | Not valid before: 2004-10-01T09:10:30 |_Not valid after: 2010-09-30T09:10:30 |_ssl-date: TLS randomness does not represent time 3306/tcp open mysql MariaDB (unauthorized) Service Info: OS: Unix

Pero no solo eso, también nos permite saber la versión de ftp y el pgrama utilizado para mantener el servidor (ProFTPD 1.3.4c) al igual pasa con nuestro servidor que Apache --> 2.4.29 y sus versiones de PHP -->5.6.32 openSSL --> 1.0.2 (criptografía) Perl --> 5.16.3 por supuesto todo esto sobre linux. Muestra también que tipo de BBDD estamos utilizando, en nuestro caso MariaDB

3º nmap -n -Pn 192.168.56.20 -p- --script=vuln

Se procede a escanear el objetivo de evaluación. La opción “-n” no realiza una resolución al DNS. La opción “-Pn” trata a todos los hosts como en funcionamiento. La opción “-p-” define el escaneo de los 65535 puertos TCP, y la opción –script=vuln define la utilización de todos los Scripts NSE incluidos en la categoría “vuln”.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-11 12:40 CET
Nmap scan report for 192.168.56.20
Host is up (0.0014s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_sslv2-drown:
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /icons/: Potentially interesting folder w/ directory listing
|   /img/: Potentially interesting folder w/ directory listing
|_  /webalizer/: Potentially interesting folder w/ directory listing
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
443/tcp  open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /icons/: Potentially interesting folder w/ directory listing
|   /img/: Potentially interesting folder w/ directory listing
|_  /webalizer/: Potentially interesting folder w/ directory listing
| http-sql-injection:
|   Possible sqli for queries:
|     https://192.168.56.20/dashboard/javascripts/?C=D%3bO%3dA%27%20OR%20sqlspider
|     https://192.168.56.20/dashboard/javascripts/?C=N%3bO%3dD%27%20OR%20sqlspider
|     https://192.168.56.20/dashboard/javascripts/?C=S%3bO%3dA%27%20OR%20sqlspider
|_    https://192.168.56.20/dashboard/javascripts/?C=M%3bO%3dA%27%20OR%20sqlspider
```

```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_sslv2-drown:
3306/tcp open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 34.08 seconds
```

A destacar vulnerabilidades encontradas:

sqli, se refiere a sql injection, una explotación de vulnerabilidad centrada en consultas de la base de datos de una aplicación. En este caso nmap nos muestra un pposible objetivo de sqli en nuestro servidor

```
http-sql-injection:
|   Possible sqli for queries:
|     https://192.168.56.20/dashboard/javascripts/?C=D%3bO%3dA%27%20OR%20sqlspider
```

ssl-dh es referido a ssl Diffie-Hellman, es un protocolo de criptografía, establece claves entre partes que no han tenido contacto previo, para ello cada parte elige dos números públicos y uno secreto. Utilizando una formula matemática cada uno realiza una serie de operaciones con sus dos números públicos y el secreto. Ambos se pasan el resultado el uno al otro. Entonces ambos utilizan por seperado una formula matemática que combina esos dos números transformados con su número secreto y al final ambos llegarán a un resultado que será la clave compartida.

Nmap nos avisa que escuchando de forma ilega podríamos tener problemas utilizando este protocolo. Abrimos : https://weakdh.org en donde te muestra datos y posibles soluciones. Por lo que por ahora podemos decir que nmap es válido para encontrar, al menos, ciertos problemas en nuestro servidor y poder solucionarlos. Podemos comprobar como Diffie-Hellman tiene una vulnerabilidad: Logjam attack

```
ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
```