5. COMPROBACION Y EXPLOTACION DE VULNERABILIDADES A NIVEL DE CREDENCIALES POR DEFAULT Y DEBILES

5.1 BUSQUEDA DE VULNERABILIDADES EN PROCESOS DE AUTENTICACIÓN

Comando:

Internet: **nmap -v -Pn -sV -p** *a,b,c,... direccion_IP_o_nombre_DNS* **--script** auth,"not *brute* and not *flood* and not *http*" **-oA** *nombre_archivo*
LAN : **nmap -v -sV -p** *a,b,c,... direccion_IP_o_nombre_DNS* **--script** auth,"not *brute* and not *flood* and not *http*" **-oA** *nombre_archivo*

Parámetros:

-Pn ---> Indica que no se realice el "ping"
-sV ---> Permite identificar el software que atiende en cada puerto abierto
-p *a,b,c...* ---> corresponde a la lista de los puertos que previamente se encontraron en estado de "abiertos"
direccion_IP_o_nombre_DNS ---> La dirección IP o el nombre DNS del host a escanear
--script auth,"not *brute* and not *flood* and not *http*" ---> Permite indicar que se realice la búsqueda de vulnerabilidades a nivel de credenciales default y débiles exceptuando ataques de fuerza bruta (brute y flood) y aquellos referidos a http (https, web en general).
-oA *nombre_archivo* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").

MISCELANEOS

1. TECNICAS DE ESCANEO DE PUERTOS

-sS (TCP SYN scan) **--->** escaneo por defecto para usuario root, utilizando SYN TCP. No culmina la conexión de tres vías.

-sT (TCP connect scan) ---> completa la conexión de 3 vías de TCP

-sU (UDP scans) ---> escaneo basado en UDP. Se puede combinar en simultaneo con -sS

-sA (TCP ACK scan) ---> determina que puertos están filtrados por algún firewall.

Open-Sec
Autores: William Marchand/Walter Cuestas A.
@WilliamMarchand/@wcu35745

They run automated tools, we have ETHICAL HACKERS!

Open-Sec

NMAP Básico - 1
Summary Sheet

Objetivo: Proveer de un instructivo para la aplicación básica de Ethical Hacking con NMAP.

1. OBTENCION DE INFORMACION PUBLICA Y BASICA

1.1 OBTENCION DE LISTA DE SERVIDORES EXPUESTOS HACIA INTERNET MEDIANTE DNS

Comando:
nmap -v --script dns-brute **--script-args** dns-brute.domain=*dominio.dom* **-oA** *nombre_archivo*

Parámetros :
--script dns-brute ---> es el nombre del script que lleva a cabo la labor
--script-args dns-brute.domain=*dominio.dom* ---> es el parámetro que permite indicar el dominio DNS a analizar
-oA *nombre_archivo* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").

1.2 VALIDACIÓN DE DIRECCIONES IP EN BASE DE DATOS WHOIS

Comando:
nmap -Pn -v *IP_address_public* **--script** whois-ip **--script-args** whodb=lacnic **-oA** *nombre_archivo*

Parámetros :
--script whois-ip ---> es el nombre del script que lleva a cabo la labor
--script-args whodb=lacnic ---> indica que la búsqueda se debe realizar en la base de datos Whois de LACNIC que es la que corresponde para Latino América y Caribe
-oA *nombre_archivo* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").

1.3 OBTENCION DE DIRECCIONES DE CORREO ELECTRONICO

Comando:
nmap -p80 **--script** http-google-email.nse *IP_address_public* **--script-args=**http-google-email.domain="*nombre_dominio*" **-oA** *nombre_archivo*

Parámetros :
--script http-google-email.nse ---> es el nombre del script que lleva a cabo la labor
--script-args http-google-email.domain="*nombre_dominio* " ---> indica que la búsqueda se debe realizar econ respecto al dominio.
-oA *nombre_archivo* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").

Nota:
Es posible que tenga que descargar el script desde www.nmap.org y adecuar el código, además de asegurarse de la actualización del archivo *shortport.lua (https://svn.nmap.org/nmap/nselib/shortport.lua)*

2. BÚSQUEDA DE PUERTOS Y SERVICIOS

2.1 ESCANEO DE PUERTOS

Comando:
nmap -v -Pn --reason -iL *lista-hosts* **-oA** *nom_file*
nmap -v -Pn --reason --port-ratio 0 **-iL** *lista-hosts* **-oA** *nom_file*
nmap -v -Pn --reason -p 1-65535 **-iL** *lista-hosts* **-oA** *nom_file*

Parámetros :
-Pn ---> Parámetro que evita la ejecución de un "ping" para verificar sí el host a escanear está activo o no. Sí el escaneo es en una LAN,puede ser recomendable permitir el ping default.
--reason ---> Permite conocer la razón para reportar el estado de cada puerto (abierto, cerrado, filtrado).
-iL ---> Permite especificar el nombre de un archivo de texto que contenga las direcciones IP o nombres DNS de hosts a escanear.
--port-ratio 0 ---> El escaneo default solamente consulta el estado de los 1000 puertos más usados. La indicación del port-ratio en cero (0) permite incrementar la cantidad de puertos a 4243. Estos ratios de uso son propios de NMAP, no guardan relación con el entorno del escaneo.
-p 1-65535 ---> Permite especificar el escaneo de los 65535 puertos posibles.
-oA *nom_file* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").

2.2 ESCANEO DE SERVICIOS

Comando:
Internet : **nmap -v -Pn -sV -O -p** *a,b,c,...* *direccion_IP_o_nombre_DNS* **-oA** *nombre_archivo*
LAN : **nmap -v -sV -O -p** *a,b,c,...* *direccion_IP_o_nombre_DNS* **-oA** *nombre_archivo*

Parámetros :
-Pn ---> Indica que no se realice el "ping"
-sV ---> Permite especificar a la herramienta que se requiere identificar el software que atiende en cada puerto abierto
-O ---> Le específica a la herramienta que debe intentar la identificación del sistema operativo base del host escaneado. IMPORTANTE: Linux: Solamente funciona si es ejecutada como administrador del sistema desde el cual se ejecuta la herramienta.
-p a,b,c... ---> corresponde a la lista (enumeración) de los puertos que previamente se encontraron en estado de "abiertos"
-oA *nombre_archivo* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").

3. ANÁLISIS DE VULNERABILIDADES

3.1 BUSQUEDA DE VULNERABILIDADES

Comando:
Internet : **nmap -v -Pn -sV -p** *a,b,c,...* *direccion_IP_o_nombre_DNS* **--script** "vuln and not *dos* and not *slow*" **-oA** *nombre_archivo*
LAN : **nmap -v -sV -p** *a,b,c,...* *direccion_IP_o_nombre_DNS* **--script** "vuln and not *dos* and not *slow*" **-oA** *nombre_archivo*

Parámetros:
-Pn ---> Indica que no se realice el "ping"
-sV ---> Permite especificar a la herramienta que se requiere identificar el software que atiende en cada puerto abierto
-p *a,b,c...* ---> corresponde a la lista (enumeración) de los puertos que previamente se encontraron en estado de "abiertos"
--script "vuln and not *dos*" ---> Permite indicar que se realice la búsqueda e identificación de vulnerabilidades comúnes y de exploits/técnicas de explotación de carácter público (1). Al mismo tiempo, se está previniendo que se genere una denegación de servicios durante su labor indicando que cualquier opción relacionada a explotación de DoS no sea ejecutada (not *dos*)
-oA *nombre_archivo* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").
(1) Se debe instalar el exploitdb.nse o vulscan.nse

4. COMPROBACION Y EXPLOTACION DE VULNERABILIDADES EN SERVIDORES DE BASES DE DATOS

4.1 BUSQUEDA DE VULNERABILIDADES

Comando:
MS SQL : **nmap -v -sV -p** 1433 *direccion_IP_o_nombre_DNS* **--script** "*ms-sql* and not *dos* and not *brute*",exploitdb **-oA** *nombre_archivo*
MySQL : **nmap -v -sV -p** 3306 *direccion_IP_o_nombre_DNS* **--script** "*mysql* and not *dos* and not *brute*",exploitdb **-oA** *nombre_archivo*
Oracle : **nmap -v -sV -p** 1521 *direccion_IP_o_nombre_DNS* **--script** oracle-enum-users,exploitdb **--script-args** oracle-enum-users.sid=ORCL,qchars=6 **-oA** *nombre_archivo*

Parámetros:
-Pn ---> Indica que no se realice el "ping"
-sV ---> Permite especificar a la herramienta que se requiere identificar el software que atiende en cada puerto abierto
-p *a,b,c...* ---> corresponde a la lista (enumeración) de los puertos que previamente se encontraron en estado de "abiertos"
--script "*ms-sql* and not *dos* and not *brute*", **--script** "*ms-sql* and not *dos* and not *brute*" ---> Permite indicar que se realice la búsqueda e identificación de vulnerabilidades comúnes y de exploits/técnicas de explotación de carácter público en el servidor de base de datos correspondiente. Al mismo tiempo, se está previniendo que se genere una denegación de servicios durante su labor indicando que cualquier opción relacionada a explotación de DoS no sea ejecutada (not *dos*) y cualquier ataque de diccionario y/o fuerza bruta (not *brute*).
--script oracle-enum-users,exploitdb **--script-args** oracle-enum-users.sid=ORCL,qchars=6 --->
Para el caso de Oracle se está aplicando una forma diferente tomando como base el hecho que la exposición del TNS Listener no siempre representa una vulnerabilidad y, además, que las vulnerabilidades referidas al este servicio son más frecuentes en ataques de diccionario y/o fuerza bruta. Por esas razones, al encontrar al Listener activo y expuestos sin filtros, las opciones se limitan a identificar la versión exacta para buscar exploits/técnica de explotación y realizar un ataque de diccionario con nombres de usuarios default de Oracle y el nombre de instancia más común.
-oA *nombre_archivo* ---> parámetro que permite especificar la generación de reporte en 3 formatos (XML, NMAP (texto) y GNMAP ("grepeable").