6669 Criptografía y Seguridad Informática

Penetration Test

2da. Parte

Penetration Test - Reconocimiento

- ✔No generan tráfico “sospechoso” en la red
- ✔Utilizan fuentes de información externas (ej: Google, Bing, etc)
- ✔No pueden ocasionar caídas en los servicios analizados

Penetration Test - Reconocimiento

$ dig +short zonetransfer.me NS

nsztm1.digi.ninja.

nsztm2.digi.ninja.

$ dig +short zonetransfer.me MX

0 ASPMX.L.GOOGLE.COM.

10 ALT1.ASPMX.L.GOOGLE.COM.

20 ASPMX2.GOOGLEMAIL.COM.

Penetration Test - Reconocimiento

Shodan

54.69.94.124 ec2-54-69-94-124.us-west-2.compute.amazonaws.com

City	Boardman
Country	United States
Organization	Amazon
ISP	Amazon
Last Update	2015-05-07T05:24:45.714868
Hostnames	ec2-54-69-94-124.us-west-2.compute.amazonaws.com

Shodan

22
SSH

```
SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCjbCUs2wPAK
2HzvRHLfGbJM9lOVpQlEQJbZuPJ3c/2LbYUn4v0huGfo/j
mKb6GP0tEY0K+k2kgOI4bdzsBSPOSH68vB9senDqUOv+IW
MsBf1Z9jqyJSHxUSBylAllN/MS0gWwxWhUjqyzVutaVUcF
baw1czWmOd1/XM6ig304Jxd/zYjagbfKm3RNBSwVxb3BRd
Fingerprint: a2:5d:25:be:a5:6c:92:24:59:d9:46:
```

Google Hacking

- ✔site:microsoft.com
- ✔inurl:backup
- ✔intitle:'index of'
- ✔filetype:pdf

Google Hacking

- ✔Google Hacking DataBase (GHDB)

https://www.exploit-db.com/google-hacking-database

Cabeceras de Correos Electrónicos

Delivered-To: aaaaa@sssss.com

Received: by 10.202.54.7 with SMTP id d7csp1825485oia;

Received: from mx.quickheal.com (bom04.balasai.com. [103.248.80.30])

Received: by mx.google.com with ESMTPS id tn1si15523689pac

Received: from HOPramod by mx.quickheal.com (MDaemon PRO v13.0.6)

Penetration Test - Reconocimiento

$ dig zonetransfer.me @nsztm1.digi.ninja. AXFR

dc-office.zonetransfer.me.	7200	IN	A	143.228.181.132
email.zonetransfer.me.	7200	IN	A	74.125.206.26
intns1.zonetransfer.me.	300	IN	A	167.88.42.94
intns2.zonetransfer.me.	300	IN	A	167.88.42.94
office.zonetransfer.me.	7200	IN	A	4.23.39.254
owa.zonetransfer.me.	7200	IN	A	207.46.197.32
vpn.zonetransfer.me.	4000	IN	A	174.36.59.154
www.zonetransfer.me.	7200	IN	A	217.147.180.162

Penetration Test - Reconocimiento

The Harvester


```
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [-v]
                    [-e DNS_SERVER] [-t DNS_TLD] [-n] [-c] [-f FILENAME]
                    [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company
or domain.
```

Penetration Test - Enumeración

También se la conoce como un reconocimiento activo, en esta fase empezaremos a utilizar herramientas que analizarán nuestro objetivo profundamente.

Será de suma importancia nuestro objetivo:

- ✔ Infraestructura
- ✔ Aplicaciones Web
- ✔ Aplicaciones Mobile
- ✔ Dispositivos de telecomunicaciones

Escaneo de red

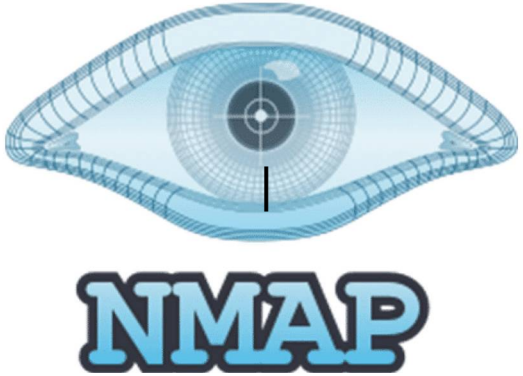
Penetration Test - Enumeración

Mapeo de Redes

- Determinar qué equipos se encuentran activos en la red
- Determinar puertos abiertos y servicios de red en ejecución
- Determinar qué sistemas operativos se están ejecutando

Penetration Test - Enumeración

Nmap (Network Mapper)



- Herramienta de Código Abierto
- Permite detectar puertos abiertos
- Es extensible a través de scripts
- Corre sobre Windows, Linux, Mac y otros.
- Permite detectar versiones de software y sistemas operativos

Penetration Test - Enumeración

Nmap (defaults)

- Escanear el protocolo TCP
- Escanear los mil puertos más utilizados (nmap-services)
- Antes, verificar si el host está activo, haciendo un ping

Nmap (Opciones Comunes)

- -F Escanea sólo los cien puertos más utilizados
- -p Puerto/s a escanear
- -sU Escanea el protocolo UDP
- -sT Escanea el protocolo TCP (lo hace por defecto)
- -sP Escanea con ping (no hace escaneo de puertos)
- -Pn No hacer ping para verificar si el host está activo
- -n No intentar resolver los nombres de cada IP
- -sV Habilita la detección de versiones de software
- -O Habilita la detección de sistemas operativos
- -A Equivale a “-sV -O -sC” y algunas otras opciones

Nmap (Especificar Puertos)

```
# nmap -sT -sU -p T:80,81,U:53,154 host
```

Nmap scan report for 181.30.241.163
Host is up (0.00065s latency).

PORT	STATE	SERVICE
80/tcp	open	http
81/tcp	filtered	hosts2-ns
53/udp	open|filtered	domain
154/udp	open|filtered	netsc-prod

Vulnerabilidades

Una vulnerabilidad es un fallo en un programa o sistema informático.

Pero no cualquiera, sino un fallo de seguridad.

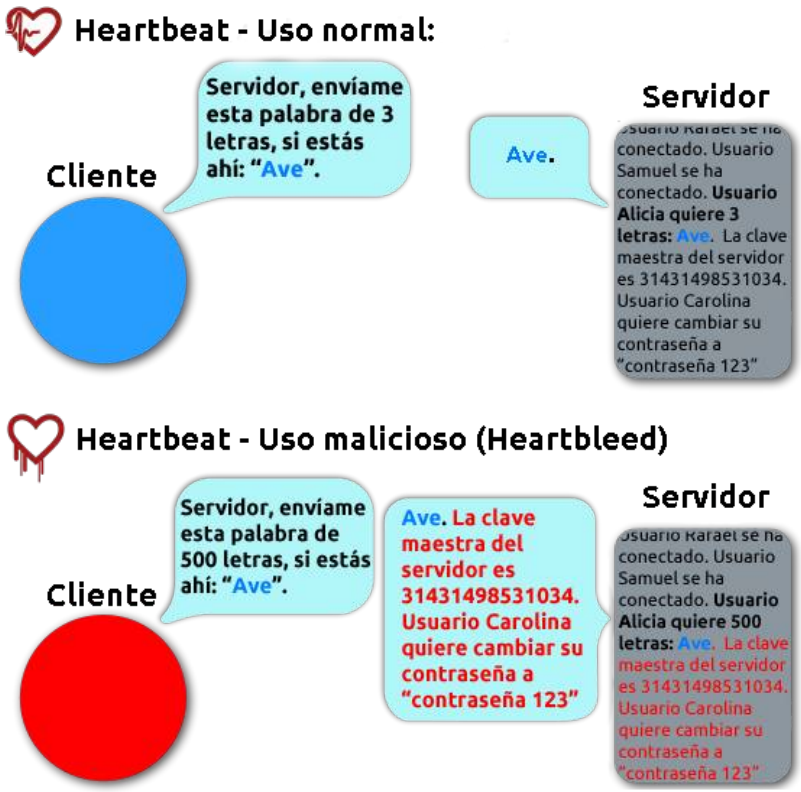
Es necesaria esta distinción puesto que **no** todos los errores de programación derivan en fallos de seguridad.

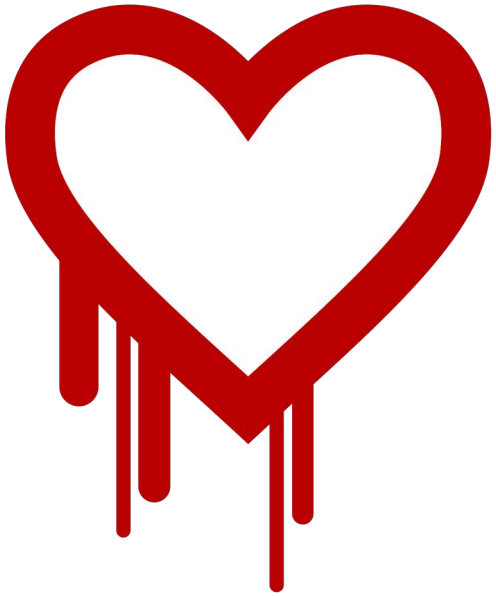
Penetration Test - Enumeración

Vulnerabilidades conocidas

- ✔ Heartbleed
- ✔ BEAST
- ✔ CRIME
- ✔ Poodle
- ✔ EternalBlue
- ✔ BlueKeep

Heartbleed


Heartbeat - Uso normal:
Servidor, envíame esta palabra de 3 letras, si estás ahí: "Ave".
Cliente
Ave.
Servidor
conectado. Usuario Samuel se ha conectado. Usuario Alicia quiere 3 letras: Ave. La clave maestra del servidor es 31431498531034. Usuario Carolina quiere cambiar su contraseña a "contraseña 123"
Heartbeat - Uso malicioso (Heartbleed)
Servidor, envíame esta palabra de 500 letras, si estás ahí: "Ave".
Cliente
Ave. La clave maestra del servidor es 31431498531034. Usuario Carolina quiere cambiar su contraseña a "contraseña 123"
Servidor
conectado. Usuario Samuel se ha conectado. Usuario Alicia quiere 500 letras: Ave. La clave maestra del servidor es 31431498531034. Usuario Carolina quiere cambiar su contraseña a "contraseña 123"



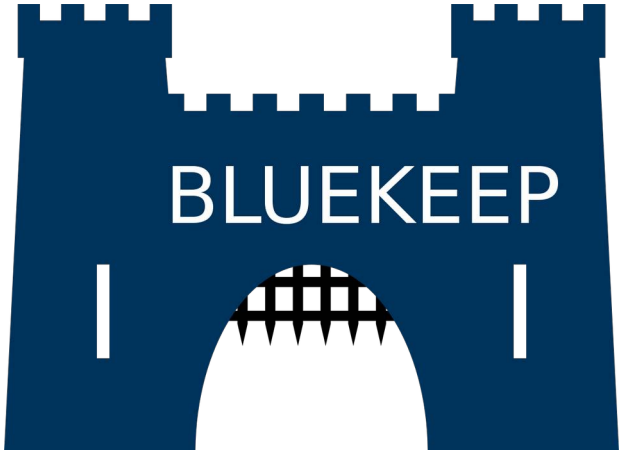
EternalBlue (MS17-010)

EternalBlue aprovecha una vulnerabilidad en la implementación del protocolo Server Message Block (SMB) de Microsoft.

Esta vulnerabilidad se debe a que la versión 1 del servidor SMB (SMBv1) acepta en varias versiones de Microsoft Windows paquetes específicos de atacantes remotos, permitiéndoles ejecutar código en el ordenador en cuestión.

BlueKeep

BlueKeep es una vulnerabilidad de seguridad que se descubrió en la implementación del Protocolo de escritorio remoto (RDP) de Microsoft, que permite la posibilidad de ejecución remota de código



Common Vulnerability & Exposure (CVE)

CVE es una lista de información registrada sobre vulnerabilidades de seguridad conocidas.

Es definido y es mantenido por The MITRE Corporation.

Cada referencia tiene:

- ✔ Número de identificación CVE-ID
- ✔ Descripción de la vulnerabilidad.
- ✔ Que versiones del software están afectadas.
- ✔ Posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad.
- ✔ Referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación.

Penetration Test - Enumeración

- Heartbleed (CVE-2014-0160)
- BEAST (CVE-2011-3389)
- CRIME (CVE-2012-4929)
- Poodle (CVE-2014-3566)
- EternalBlue (CVE-2017-0144)
- BlueKeep (CVE-2019-0708)

Common & Vulnerability Scoring System (CVSS)

CVSS es un estándar de la industria gratuito y abierto para evaluar la gravedad de las vulnerabilidades de seguridad del sistema informático.

CVSS intenta asignar puntajes de gravedad a las vulnerabilidades, lo que permite a los respondedores priorizar las respuestas y los recursos de acuerdo con la amenaza

Penetration Test - Enumeración

CWE (Common Weakness Enumeration)

- Identifica las debilidades “comunes” en el software
- Asocia debilidades con tipos de ataque
- Muestra ejemplos de código vulnerable y soluciones posibles

Escaneo de Vulnerabilidades

El escaneo de vulnerabilidades nos permite rápidamente detectar vulnerabilidades conocidas en el equipo/servicio objetivo.

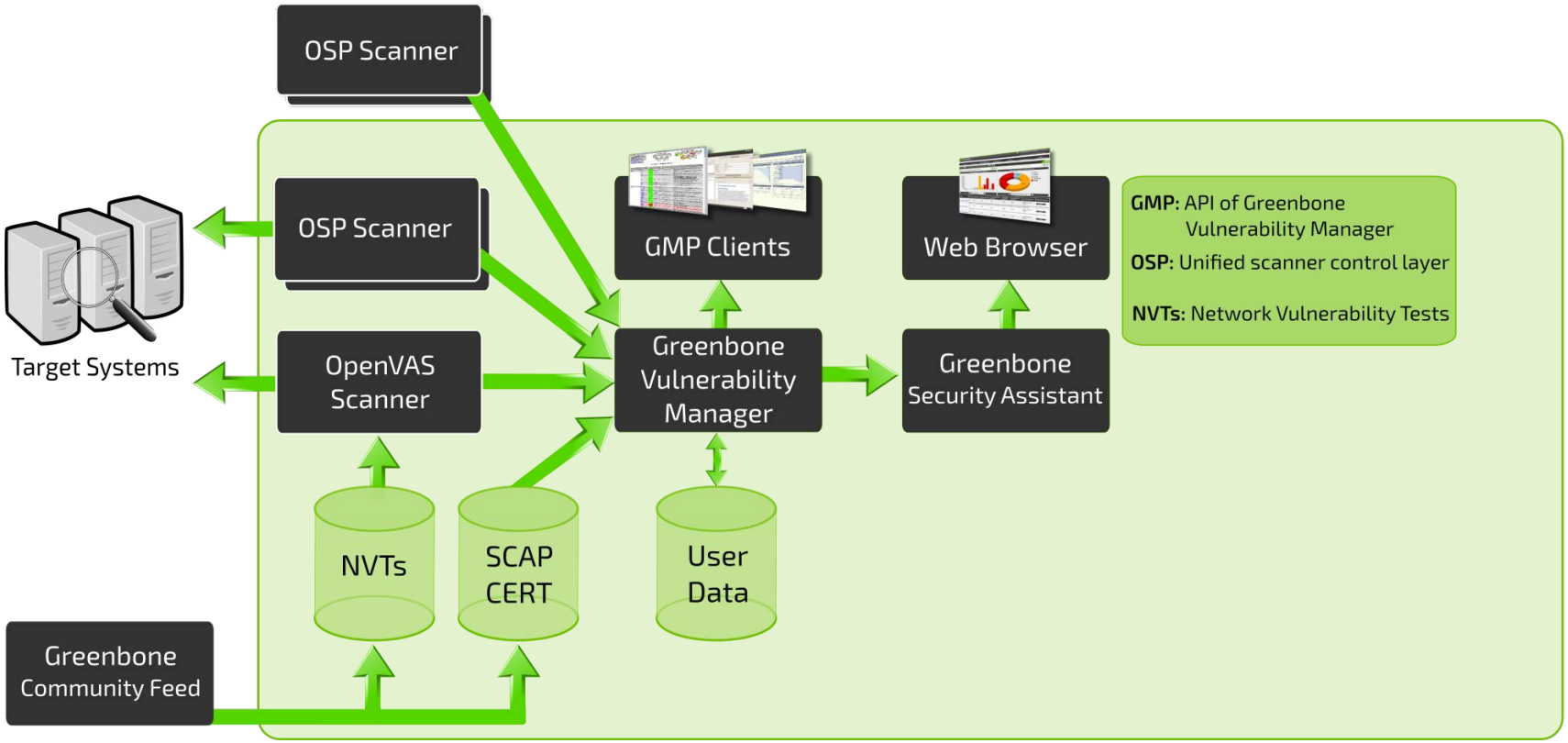
Los sistemas que realizan estos escaneos nos darán el nombre de la vulnerabilidad, criticidad, descripción, host asociado, puerto y protocolo, recomendaciones, CVE asociado, entro otros datos de interés.

Scanners de vulnerabilidades conocidos:

- ✔ Nessus
- ✔ OpenVAS
- ✔ Acunetix
- ✔ Burp
- ✔ OWASP ZAP
- ✔ Entre otros.

Penetration Test - Enumeración

OpenVAS



Exploit Database

Exploit Database es mantenida por Offensive Security y es un proyecto sin fines de lucro que se ofrece como un servicio público de seguridad ofensiva.

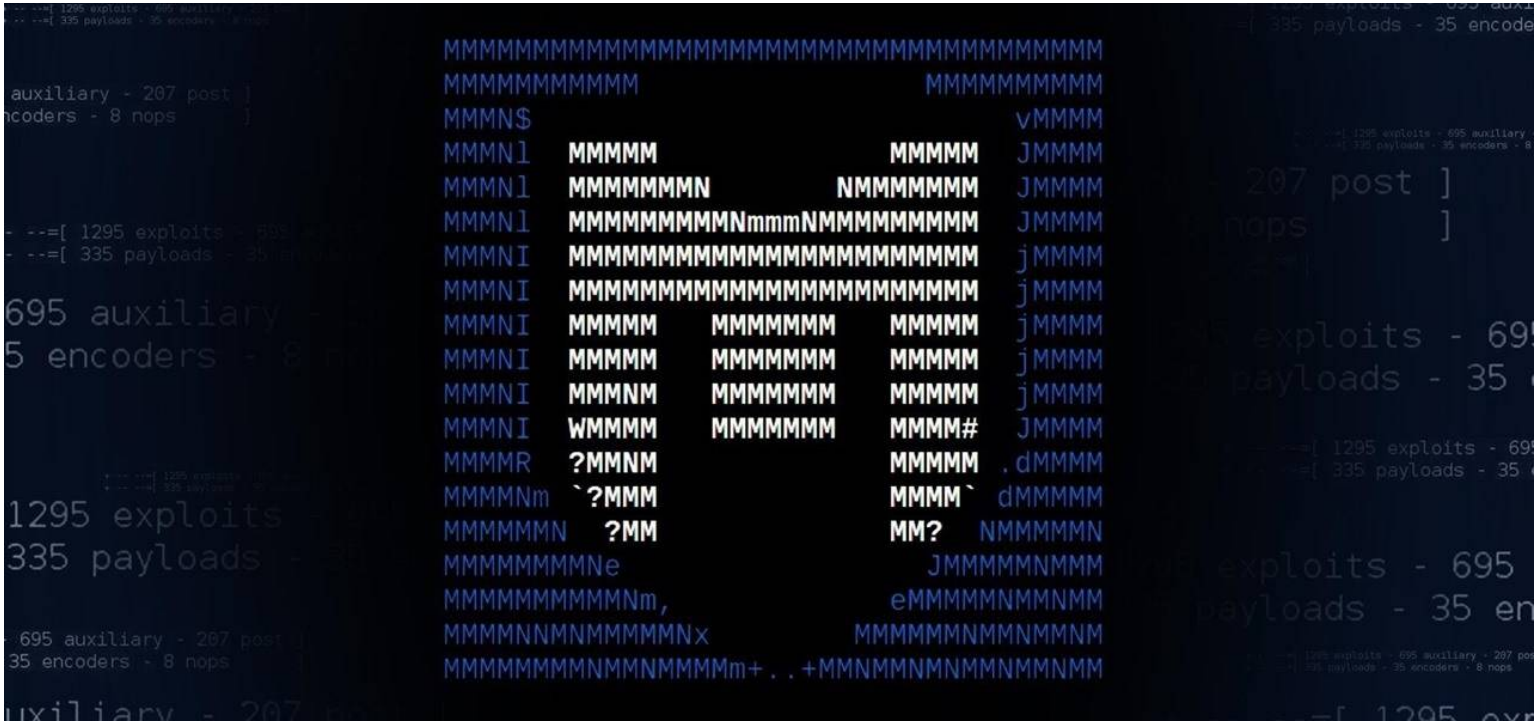
Penetration Test – Ganar Acceso

Exploit Database

```
root@kali:~# searchsploit eternalblue
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)                                        | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)                    | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)                              | windows_x86-64/remote/42030.py
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Penetration Test – Ganar Acceso

Metasploit



Metasploit

Metasploit es un proyecto de código abierto de seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en el proceso de "Pentesting".

Su subproyecto más conocido es el Metasploit Framework, una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Inicialmente fue creado utilizando el lenguaje de programación de scripting Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.

Metasploit

Dispone de diversos módulos, entre ellos:

- ✔ exploits
- ✔ payloads
- ✔ auxiliaries
- ✔ post
- ✔ encoders