

Experto Universitario en Ethical Hacking



Módulo 5:

Ethical Hacking

Unidad 2:

Vulnerability Scanning / Scanning (Ports)



Presentación

En esta segunda Unidad del módulo, se expondrán tanto el proceso de búsqueda de vulnerabilidades como el escaneo de puertos y servicios.

Resolverán que puertos son necesarios escanear y utilizar una de las mejores herramientas para esa función.



Objetivos

Que los participantes logren...

- Aprender sobre los conceptos expuestos en el mundo del Hacking.
- Conocer las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades y test de penetración (Pentesting), con una filosofía enfocada en la ética profesional.
- Comprender la importancia de usar cifrado seguro en aplicaciones, abordar vulnerabilidades y potenciales ataques y amenazas, así como la correcta concientización en los usuarios.



Bloques temáticos

1. Introducción
2. Reconocimiento y búsqueda automatizada
3. Capturas de resultados
4. Ejercicios
5. Scanning

Introducción



Lo primero que un atacante o intruso haría en caso de querer lograr un objetivo y observa que de la manera sencilla no puede lograrlo, lo más probable es que recurra a la búsqueda de vulnerabilidades a través de sitios o de herramientas diseñadas para esa función.

Las mismas hoy en día están disponibles tanto a nivel comercial como públicas y las mejores cuentan con una biblioteca de vulnerabilidades muy importante.



Obviamente, el solo hecho de que un atacante disponga de un “zero-day”, no significa que la tool lo tendría, ya que se trata de actualizar la lista lo más rápido posible, para así poder evitar el uso del ataque.

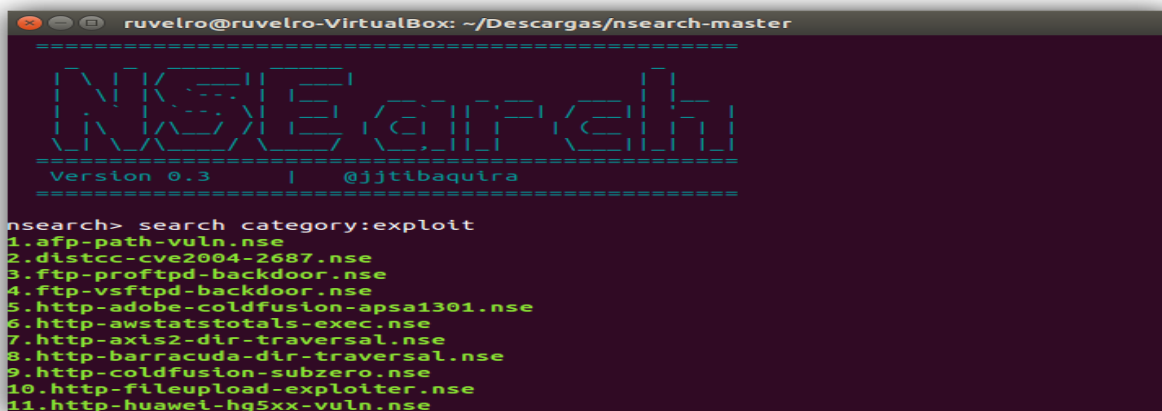
Todos los sistemas, dispositivos y hasta personas, podrían ser estudiados para lograr un objetivo, encontrar una vulnerabilidad que determine una tarea a realizar, como por ejemplo:

- INGRESO NO AUTORIZADO
- MODIFICACION DE INTEGRIDAD
- BORRADO NO AUTORIZADO
- USO DE PRIVILEGIOS
- INGENIERIA SOCIAL
- ETC

A continuación conoceremos, en primera instancia sitios web, que albergan información sobre vulnerabilidades, los cuales son un repositorio muy importante de recursos para conocer y buscar.

Luego expondremos algunas tools, preparadas para buscar vulnerabilidades, así como también son utilizadas para el uso de **Pentesting**.

Hay herramientas que no solamente sirven para poder escanear puertos y servicios, sino que dispone de opciones que ayudarían bastante en la búsqueda de vulnerabilidades.



```
ruvelro@ruvelro-VirtualBox: ~/Descargas/nsearch-master
=====
NSE
=====
Version 0.3 | @jttibaquirra
=====
nsearch> search category:exploit
1.afp-path-vuln.nse
2.distcc-cve2004-2687.nse
3.ftp-proftpd-backdoor.nse
4.ftp-vsftpd-backdoor.nse
5.http-adobe-coldfusion-apsa1301.nse
6.http-awstatstotals-exec.nse
7.http-axis2-dir-traversal.nse
8.http-barracuda-dir-traversal.nse
9.http-coldfusion-subzero.nse
10.http-fileupload-exploiter.nse
11.http-huawei-hg5xx-vuln.nse
```

Por último, se expondrán capturas de varios **Vulnerability Scanners**.

Como despedida de la unidad, se dejara un ejercicio, para enviar por mail únicamente.



Reconocimiento y búsqueda automática

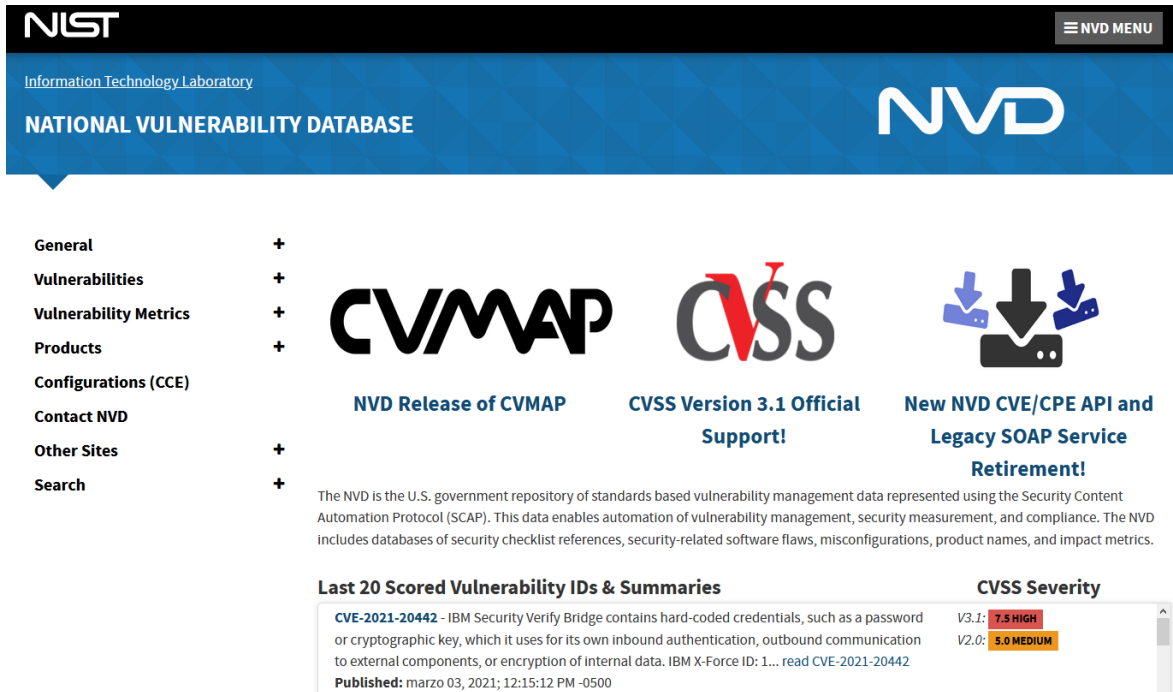
```
root@sideswipe:~# nmap -f --script vuln 192.168.206.133
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-11 12:56 ART
Nmap scan report for 192.168.206.133
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
33/tcp    open  domain
30/tcp    open  http
|_ http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.206.133
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.206.133/mutillidae/.index.php?page=set-background-color.php
| Form id: id-bad-cred-tr
| Form action: index.php?page=set-background-color.php
|
| Path: http://192.168.206.133/mutillidae/.index.php?page=html5-storage.php
| Form id: idform
| Form action: index.php?page=html5-storage.php
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
| /index/: Potentially interesting folder
|_ http-fileupload-exploiter:
|_ http-frontpage-login: false
|_ http-slowloris-check:
|_ VULNERABLE:
| Slowloris DOS attack
| State: VULNERABLE
| Description:
| Slowloris tries to keep many connections to the target web server open and hold them open as long as possible.
| It accomplishes this by opening connections to the target web server and sending a partial request. By doing
```

La explotación de una vulnerabilidad, podría llegar a ser considerada un delito de acuerdo a las leyes vigentes del país en donde es originada la técnica.

También hay que tener en cuenta que el solo hecho de haber encontrado una, puede significar que si bien existe un “agujero de seguridad”, se necesitaran conocimientos para poder aprovecharse del mismo o herramientas para tal fin.

Uso de aplicaciones de ingreso (**SSH**, **Telnet**), aplicaciones de scaneo (**Nmap**, **Autoscan**), aplicaciones de enumeración (**Hydra**, **Infiltrator**) entre otras, serían necesarias como complemento




Empecemos conociendo algunos sitios webs muy recomendados para empezar a chequear:



NIST Information Technology Laboratory **NVD**

NATIONAL VULNERABILITY DATABASE

- General +
- Vulnerabilities +
- Vulnerability Metrics +
- Products +
- Configurations (CCE)
- Contact NVD
- Other Sites +
- Search +

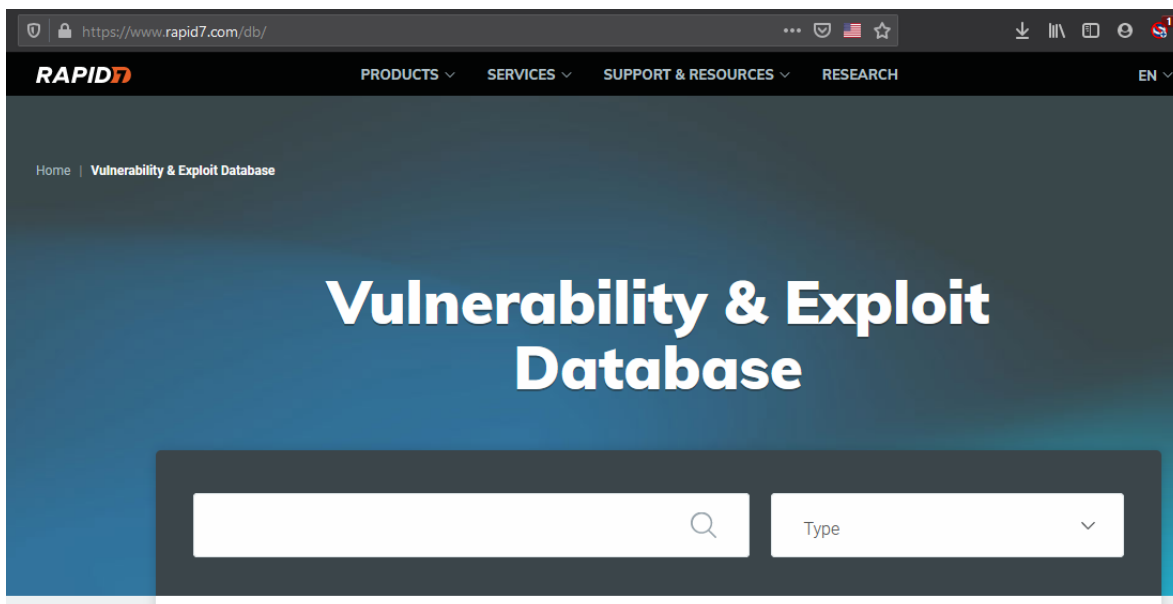
NVD Release of CVMAP **CVSS Version 3.1 Official Support!** **New NVD CVE/CPE API and Legacy SOAP Service Retirement!**

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Last 20 Scored Vulnerability IDs & Summaries **CVSS Severity**

CVE-2021-20442 - IBM Security Verify Bridge contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 1... read CVE-2021-20442	V3.1: 7.5 HIGH
Published: marzo 03, 2021; 12:15:12 PM -0500	V2.0: 5.0 MEDIUM

NIST: <http://nvd.nist.gov/>



https://www.rapid7.com/db/

RAPID7 PRODUCTS SERVICES SUPPORT & RESOURCES RESEARCH EN




Home | Vulnerability & Exploit Database

Vulnerability & Exploit Database

EXPLOIT DATABASE RAPID7 <http://www.rapid7.com/db/>



EXPLOIT
DATABASE

























  

☐ Verified ☐ Has App

Filters Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2021-03-09				bVPN 2.5.1 - 'waselvpnserv' Unquoted Service Path	Local	Windows	Mohammed Alshehri
2021-03-09				Sandboxie Plus v0.7.2 - 'SbieSvc' Unquoted Service Path	Local	Windows	Mohammed Alshehri
2021-03-09				FreeLAN 2.2 - 'FreeLAN Service' Unquoted Service Path	Local	Windows	Mohammed Alshehri
2021-03-09				Golden FTP Server 4.70 - 'PASS' Buffer Overflow (2)	Remote	Windows	1F98D
2021-03-08				GLPI 9.5.3 - 'fromtype' Unsafe Reflection	WebApps	PHP	Vadym Soroka
2021-03-08				Joomla JCK Editor 6.4.4 - 'parent' SQL Injection (2)	WebApps	PHP	Nicholas Ferreira
2021-03-08				Pingzapper 2.3.1 - 'PingzapperSvc' Unquoted Service Path	Local	Windows	Brian Rodriguez
2021-03-08				Hotel and Lodge Management System 1.0 - Remote Code Execution (Unauthenticated)	WebApps	PHP	Christian Vierschilling
2021-03-08				Configuration Tool 1.6.53 - 'OpLclSrv' Unquoted Service Path	Local	Windows	Brian Rodriguez
2021-03-08				Print Job Accounting 4.4.10 - 'OkJaSvc' Unquoted Service Path	Local	Windows	Brian Rodriguez
2021-03-05				Fluig 1.7.0 - Path Traversal	WebApps	Multiple	Lucas Souza
2021-03-05				CatDV 9.2 - RMI Authentication Bypass	Remote	Java	Christopher Ellis

EXPLOIT DATABASE OFFENSIVE SECURITY: <http://www.exploit-db.com/>

← → ↺ 🏠

🔒 <https://www.securityfocus.com/vulnerabilities>

⋮

About Contact

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
[Join the conversation >](#)

Vulnerabilities (Page 1 of 3411) 1 2 3 4 5 6 7 8 9 10 11 Next >

Vendor: Select Vendor

Title: Select Title

Version: Select Version

Search by CVE

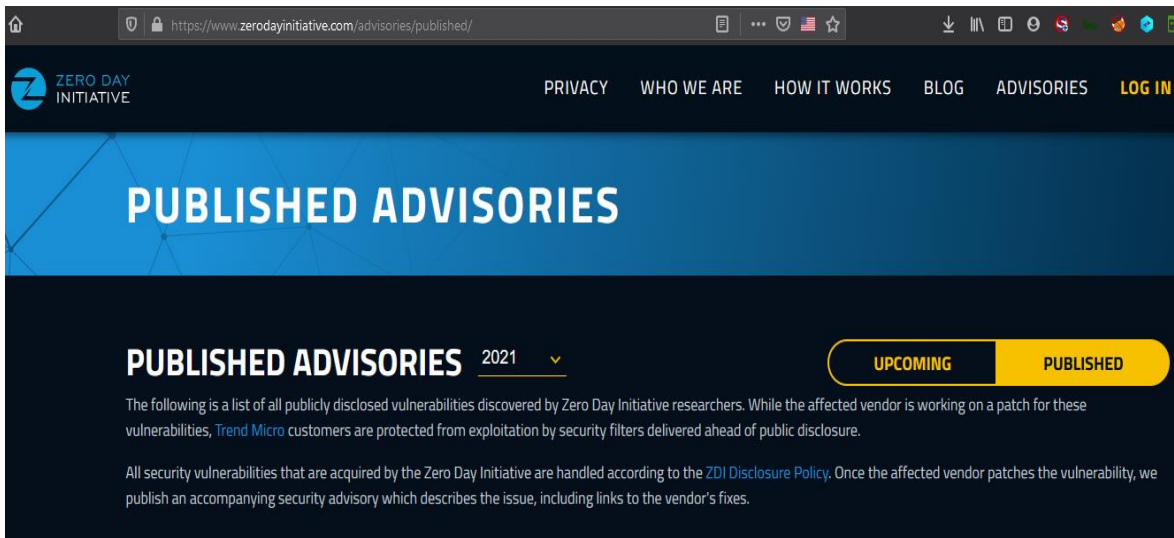
CVE:

Submit

Jenkins Credentials Binding Plugin CVE-2019-1010241 Information Disclosure Vulnerability
2019-07-26
<http://www.securityfocus.com/bid/109320>

Qualcomm Components CVE-2019-2307 Integer Underflow Vulnerability
2019-07-26
<http://www.securityfocus.com/bid/109383>

<http://www.securityfocus.com/vulnerabilities>



The screenshot shows the 'PUBLISHED ADVISORIES' page of the Zero Day Initiative. It features a navigation bar with links like 'PRIVACY', 'WHO WE ARE', 'HOW IT WORKS', 'BLOG', 'ADVISORIES', and 'LOG IN'. The main heading is 'PUBLISHED ADVISORIES' with a dropdown for the year '2021'. Below this, there are two tabs: 'UPCOMING' and 'PUBLISHED'. The text explains that the list contains publicly disclosed vulnerabilities discovered by Zero Day Initiative researchers, and that Trend Micro customers are protected from exploitation by security filters delivered ahead of public disclosure. It also mentions that all security vulnerabilities are handled according to the ZDI Disclosure Policy.

<http://www.zerodayinitiative.com/advisories/published/>

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-200

[Log In](#) [Register](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

Enter a CVE id, product, vendor, vulnerability type...

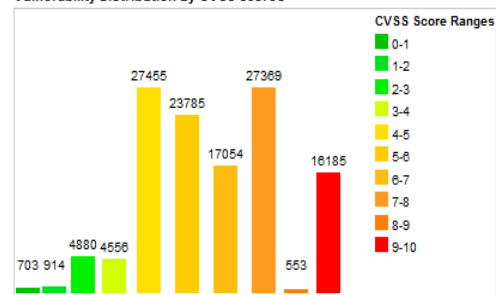
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

Weighted Average CVSS Score: 6.6

Vulnerability Distribution By CVSS Scores



<http://www.cvedetails.com/>

El seguimiento de las buenas prácticas en lo que se refiere a la seguridad informática nos dicen que no hay nada 100% seguro pero que a partir de una serie de reglas se pueden detener y/o prevenir muchas acciones que perjudicarían a los activos a proteger.

Hay que entender que el uso de los scanners de vulnerabilidades no van proteger de ningún tipo de ataque pero si nos ADVIERTEN y PREVIENEN sobre ellos, ya que gracias a ellos podremos saber o medir el nivel de seguridad que tienen nuestros sistemas, por eso se recomienda el uso de ellos de una manera continua para así evitar daños mayores.

A continuación, un listado de scanners de vulnerabilidades a nivel software (conocidos y discontinuos):

Programa
Acunetix Web Vulnerability Scanner
App Scanner
AppScan
AppSpider
AVDS
BlueClosure BC Detect
Burp Suite
Contrast
Detectify
edgescan
GamaScan
GFI LANguard Network Security scanner
GoLismero
Grabber
Grendel-Scan
IKare
Indusface Web Application Scanning
ISS Internet Scanner
Microsoft Baseline Security Analyzer (MBSA)
Nessus
Netsparker
Nexpose
NeXpose Community Edition
Nikto2
nmap
N-Stealth
OpenVAS
Owasp ZAP

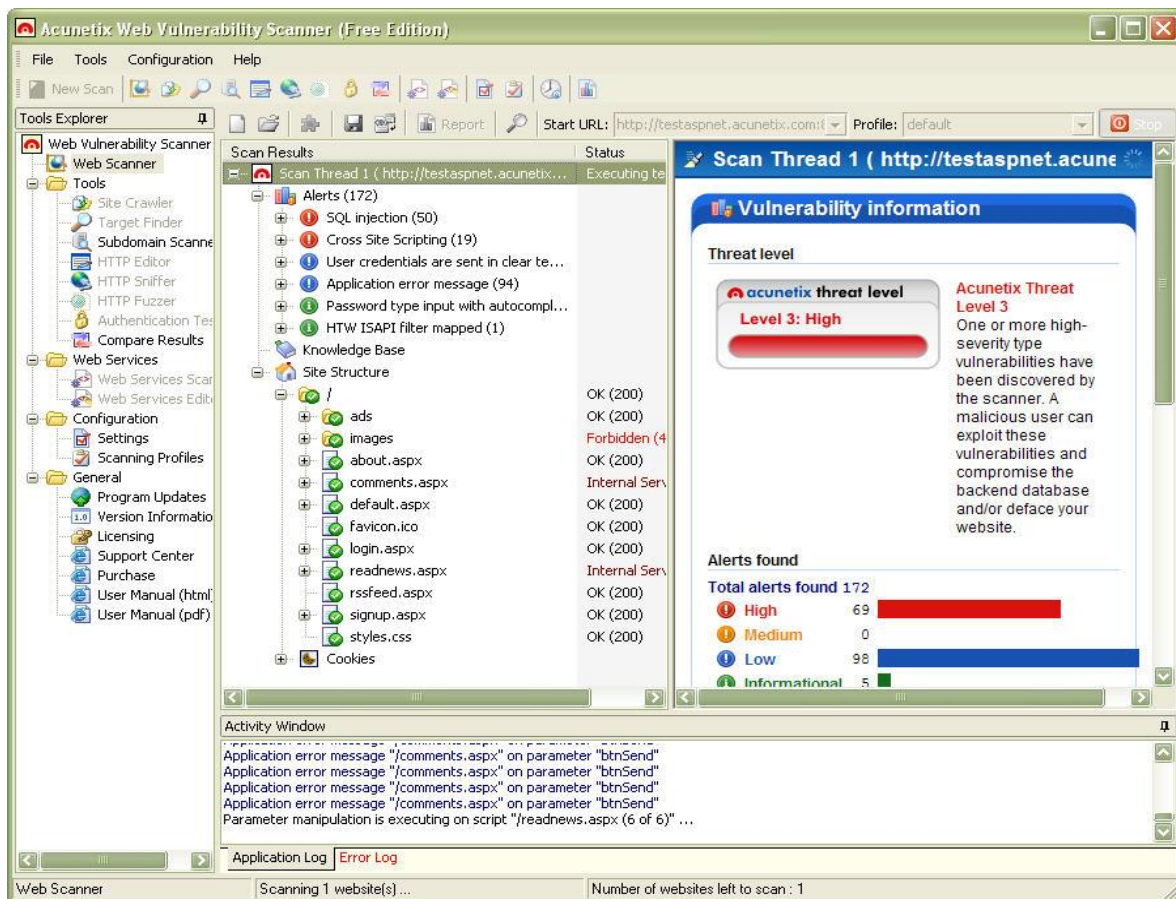
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
 (1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

ParosPro
Pengowin
Proxy.app
Qualys FreeScan
QualysGuard
Ratproxy
Retina
Retina CS Community
Retina Network Security Scanner
SAINT Network Vulnerability Scanner
SecureCheq
Securus
Sentinel
Skipfish
SOATest
sqlmap
Tinfoil Security
Trustkeeper Scanner
uniscan
Vega
w3af
Wapiti
Watchfire Rational Appscan
WebApp360
WebCookies
WebInspect
WebReaver
WebScanService
WebScarab
Websecurify Suite
Wikto
wpscan
Xenotix XSS Exploit Framework

Capturas de resultados

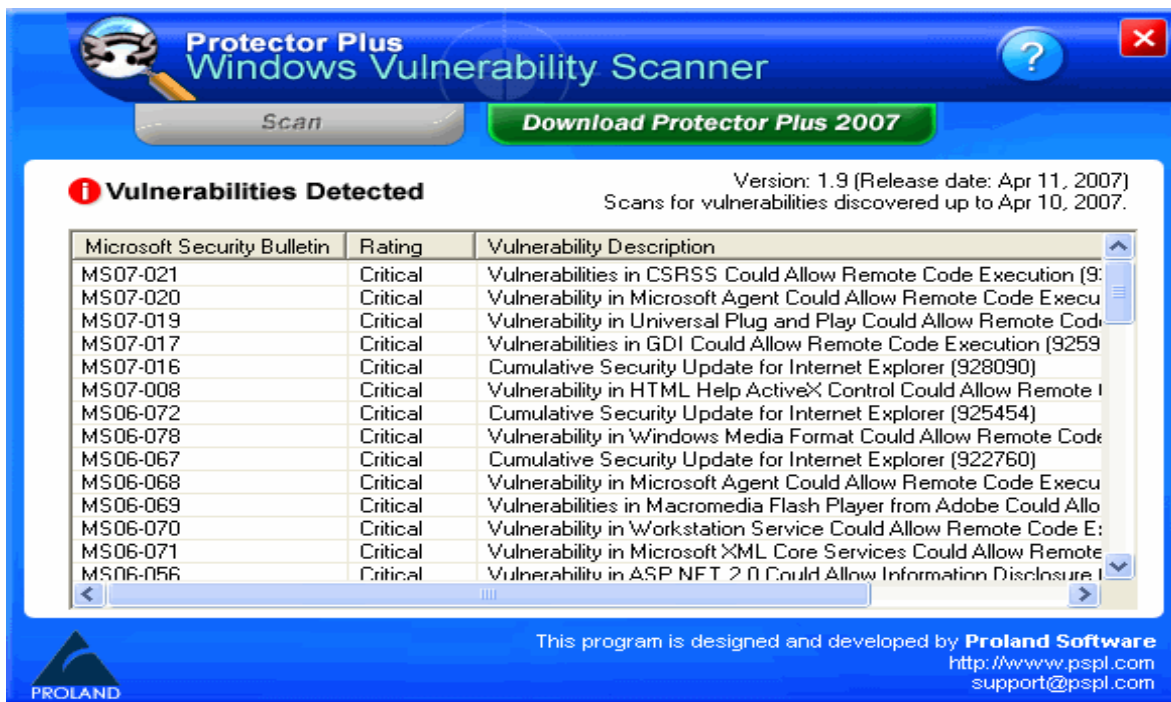
Cada captura, puede ser parecida o distinta, y está en el profesional de seguridad, comprender y descartar si es un falso positivo.

En el escenario más real posible, podemos encontrarnos con miles de vulnerabilidades o posibles vulnerabilidades, no existe una biblioteca en el mundo que nos permita hacer todo automatizado para el descarte, por eso el trabajo manual es importante

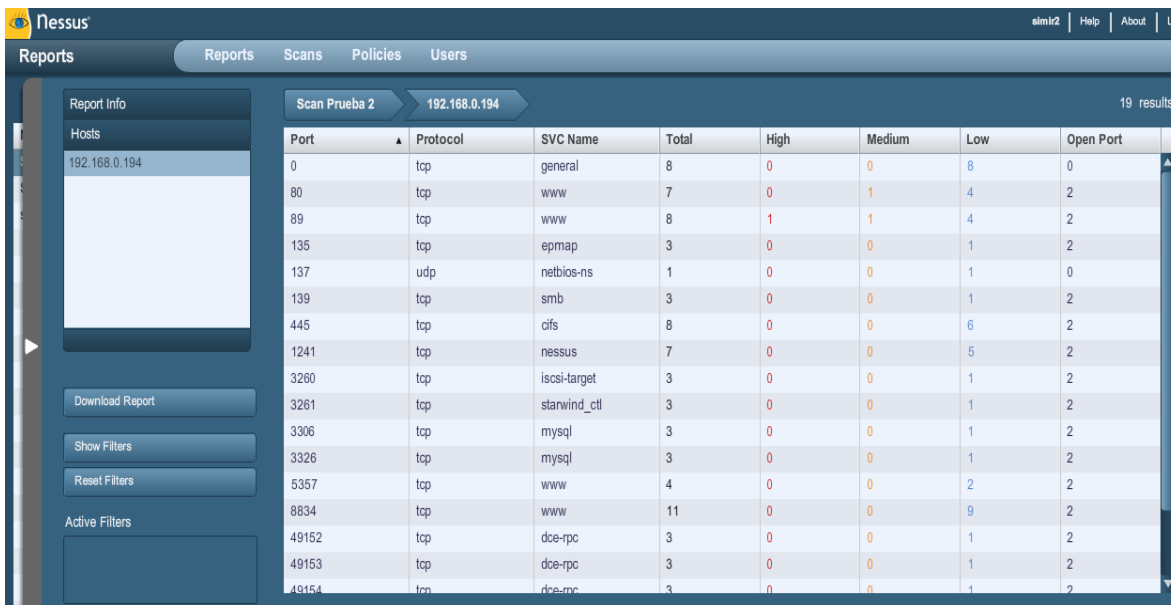


Esta es la aplicación ACUNETIX, notaremos en el resultado, que ha encontrado vulnerabilidades SQL y XSS entre otras, también nos muestra la estructura del objetivo.

Esa misma data, sirve para poder realizar otras pruebas.



Una “aplicación discontinua” que expone los códigos de vulnerabilidades encontrados junto con la descripción y nivel de criticidad.



Acá la aplicación **NESSUS** expone los puertos involucrados, junto con el servicio y nivel de criticidad.



```
root@kali:~/usr/share/nmap/scripts# nmap --script vulscan -sV 192.168.135.131
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-07 23:53 -03
Nmap scan report for 192.168.135.131
Host is up (0.0040s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| vulscan: VulDB - https://vuldb.com:
| [43110] vsftpd up to 2.0.4 Memory Leak denial of service
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial
of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different
vulnerability than CVE-2010-2632.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [82285] Vsftpd CVE-2004-0042 Remote Security Vulnerability
| [72451] vsftpd CVE-2015-1419 Security Bypass Vulnerability
| [51013] vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
| [48539] vsftpd Compromised Source Packages Backdoor Vulnerability
| [46617] vsftpd FTP Server 'ls.c' Remote Denial of Service Vulnerability
| [41443] Vsftpd Webmin Module Multiple Unspecified Vulnerabilities
| [30364] vsftpd FTP Server Pluggable Authentication Module (PAM) Remote Denial of Service Vulnerability
| [29322] vsftpd FTP Server 'deny_file' Option Remote Denial of Service Vulnerability
| [10394] Vsftpd Listener Denial of Service Vulnerability
| [7253] Red Hat Linux 9 vsftpd Compiling Error Weakness
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [68366] vsftpd package backdoor
| [65873] vsftpd vsf_filename_passes_filter denial of service
| [55148] VSFTPD-WEBMIN-MODULE unknown unspecified
| [43685] vsftpd authentication attempts denial of service
| [42593] vsftpd deny_file denial of service
| [16222] vsftpd connection denial of service
| [14844] vsftpd message allows attacker to obtain username
| [11729] Red Hat Linux vsftpd FTP daemon tcp_wrapper could allow an attacker to gain access to server
|
| Exploit-DB - https://www.exploit-db.com:
| [17491] VSFTPD 2.3.4 - Backdoor Command Execution
| [16270] vsftpd 2.3.2 - Denial of Service Vulnerability
```

Uso del NMAP, en conjunto con el script=vulscan, donde expone todos los CVE.

Es cansador pero necesario comprender que la recolección de datos es importante, no es cuestión de tirar una tool y rezar que encuentre algo, puede haber escenarios que no se encuentre absolutamente nada, quizás por medidas de seguridad del cliente, algún **WAF** o **Firewall** instalado en la red, son cientos de escenarios, no hay manera de adivinar que nos podemos encontrar en un ambiente **BlackBox**.

Ejercicio 1 Unidad 2



Wordpress, tuvo muchos inconvenientes de vulnerabilidades a lo largo de los años, la idea es explicar una de las mismas, y quien se anima demostrar alguna a través de capturas en el ejercicio.

La idea es exponer el mismo en el foro de la unidad y debatir.

Para poder realizar este ejercicio, recomendamos el uso de la herramienta **WPSCAN**, que se encuentra dentro de Kali Linux.

```
WPSecan®
WordPress Security Scanner by the WPScan Team
Version 2.9.2
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdL, @_FireFart_

[!] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]Y
[!] Updating the Database ...
[!] Update completed.
```

En caso de ser necesario, el instructor tiene un tutorial de la misma para que se lo puedan solicitar.

Para los que no tienen conocimientos, lo ideal sería instalar en una virtual, un **Wordpress**.

En este caso, les paso un procedimiento sencillo:

<https://www.pedrosuarezweb.com/instalar-wordpress-en-local/>

LOCAL es una aplicación que les permitirá instalar WP de una manera muy sencilla, sin depender de ninguna herramienta adicional.

Scanning (de Puertos)

PORT SCANNING



El término escaneo de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones.

Detecta si un puerto está abierto, cerrado, o protegido por un firewall.

Utilizado para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos.

Nos da la posibilidad de detectar el sistema operativo que está ejecutando la máquina/objetivo según los puertos que tiene abiertos.

Y muy utilizado por administradores de sistemas para analizar posibles problemas de seguridad, así como también utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.

Prácticas de escaneo (utilizar la tools NMAP)

Obtener información sobre puertos y detección del sistema operativo de un sistema o host.

```
(root@kali)-[/home/kali]
# nmap -sS -Pn -sV -O 192.168.1.36
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 08:55 EST
Nmap scan report for 192.168.1.36
Host is up (0.0012s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:6C:01:FC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::~ cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008::r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: LABORATORIO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 132.03 seconds
```

nmap -sS -Pn -sV -O < objetivo >

Donde < objetivo > puede ser una dirección IP simple, un nombre de máquina o una dirección de red.

-sS exploración TCP SYN (conocida también como medio-abierta, o análisis sigiloso)

-P0 opción que nos permite desactivar los pings ICMP.

-sV opción que habilita la detección de versión del sistema operativo

-O es una bandera que intenta identificar el sistema operativo remoto

Otras opciones:

-A habilita la detección tanto del sistema operativo como de la versión

-v al utilizar el parámetro **-v** dos veces obtendremos mayor detalle del análisis (verbosity)

Obtener una lista de posibles servidores WEB con un puerto específico abierto (80)

nmap -sT -p 80 -oG - 192.168.1.* | grep open

Podemos cambiar el valor del parámetro **-p** para definir el número del puerto a buscar.
Busquemos en “man nmap” las diferentes formas de especificar rangos de direcciones.

Encontrar todas las direcciones IP activas en la red

nmap -sP 192.168.0.*

Otra opción es:

nmap -sP 192.168.0.0/24 para el rango de red completo.

Ping a un rango de direcciones IP

nmap -sP 192.168.1.100-254

NMAP acepta una amplia variedad de notaciones de direccionamiento, múltiples objetivos/rangos, etc.

Encontrar direcciones IP no utilizadas en una red definida

nmap -T4 -sP 192.168.2.0/24 && egrep “00:00:00:00:00:00” /proc/net/arp

Explorar en búsqueda del virus Conficker en la red LAN (Ejemplo)

nmap -PN -T4 -p139,445 -n -v --script=smb-check-vulns --script-args safe=1 192.168.0.1-254

Podemos reemplazar el rango 192.168.0.1-254 con el rango de la red que queremos verificar.

Cuántos dispositivos Linux y Windows hay en la red?

nmap -F -O 192.168.0.1-255 | grep “Running: ” > /tmp/os; echo “\$(cat /tmp/os | grep Linux | wc -l) Linux device(s)”; echo “\$(cat /tmp/os | grep Windows | wc -l) Window(s) devices”

Probablemente se requieran privilegios de root para ejecutar esta exploración.

Utilizar un señuelo mientras se analizan los puertos para evitar ser detectados por el sysadmin

nmap -sS 192.168.0.10 -D 192.168.0.2

Explora en búsqueda de puertos abiertos en la máquina (192.168.0.10) mientras establece una dirección señuelo (192.168.0.2). Esto mostrará la dirección señuelo en lugar de nuestra dirección real en los registros de seguridad del objetivo. La dirección señuelo debe ser de una máquina activa. Verifiquemos los registros de seguridad del objetivo en /var/log/secure para asegurarnos que funciona.

Números de puertos utilizados por un AD (Active Directory) para tener en cuenta en el escaneo

Número de puerto	Propósito
389	Directorio, replicación, confianza, autenticación, políticas de grupo
636	Directorio, replicación, confianza, autenticación, políticas de grupo (comunicación SSL)
3268	Directorio, replicación, confianza, autenticación, políticas de grupo (Catálogo global)
3269	Directorio, replicación, confianza, autenticación, políticas de grupo (Comunicación SSL)

La deducción posible que uno puede hacer, es que conociendo suficientemente bien los números de puertos más conocidos o utilizados, se pueden obtener a través de los mismos, información relevante para un Ethical Hacking.



Recomendamos no practicar estas técnicas en redes o máquinas que no nos pertenecen o a las cuales no tenemos autorización.

Si bien el escaneo de puertos no es considerado un delito, se recomienda que lo hagan en ambientes propios o seguros.



APORTE: listado de los puertos mas buscados y conocidos

Top 10 TCP ports	TCP effectiveness of --top-port values
<ul style="list-style-type: none"> • 80 (http) • 23 (telnet) • 22 (ssh) • 443 (https) • 3389 (ms-term-serv) • 445 (microsoft-ds) • 139 (netbios-ssn) • 21 (ftp) • 135 (msrpc) • 25 (smtp) 	<ul style="list-style-type: none"> • --top-ports 10: 48% • --top-ports 50: 65% • --top-ports 100: 73% • --top-ports 250: 83% • --top-ports 500: 89% • --top-ports 1000: 93% • --top-ports 2000: 96% • --top-ports 3674: 100%

En la primer columna se exponen los más encontrados y en la segunda, la opción más recomendable para usar con NMAP junto a su efectividad.

Tener en cuenta que se disponen de 65535 puertos, tanto en TCP como UDP

Port Specification		
Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range
-p	nmap 192.168.1.1 -p U:53,T:21-25,80	Port scan multiple TCP and UDP ports
-p-	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
--top-ports	nmap 192.168.1.1 --top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la “X” el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy **IMPORTANTE** que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.



Bibliografía utilizada y sugerida

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU.

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México.

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España.

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU.

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU.

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado)