

EJERCICIOS ANÁLISIS DE VULNERABILIDADES CON NMAP NSE Y OPENVAS

Prerrequisitos

- Kali Linux
- Metasploitable2

Ejercicio 1 - Nmap NSE

- Realizar un análisis de vulnerabilidades sobre el servicio SSH de Metasploitable2 utilizando los scripts Nmap NSE vulscan y vulners.

Comprobación de que el puerto correspondiente a SSH esta abierto..

```
(root@kali)-[/home/veronica/Documentos/red_team]
# nmap 10.0.2.8
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-14 21:10 CET
Nmap scan report for 10.0.2.8
Host is up (0.000047s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
```

NMAP NSE VULSCAN

```
(root@kali)-[/usr/share/nmap/scripts/vulscan]
# nmap -sV --script vulscan.nse 10.0.2.8 -p 22 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-14 21:34 CET
Nmap scan report for 10.0.2.8
Host is up (0.00051s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| [44077] OpenBSD OpenSSH up to 4.3 Signal privilege escalation
| [43307] OpenSSH 4.0 privilege escalation
| [41835] OpenSSH up to 4.8 privilege escalation
| [39331] OpenSSH 4.3p2 Audit Log linux_audit_record_event unknown vulnerability
| [38743] OpenSSH up to 4.6 privilege escalation
| [36382] OpenBSD OpenSSH up to 4.6 weak authentication
| [32699] OpenBSD OpenSSH 4.1 information disclosure (info debug)
| [32532] OpenBSD OpenSSH 4.5 packet.c denial of service
| [32512] OpenBSD OpenSSH up to 4.3 unknown vulnerability
| [26219] OpenBSD OpenSSH up to 4.1p1 information disclosure
| [16020] OpenBSD OpenSSH 4.5 Format String
| [2667] OpenBSD OpenSSH 4.4 Separation Monitor unknown vulnerability
| [2578] OpenBSD OpenSSH up to 4.4 Signal race condition
| [1999] OpenBSD OpenSSH up to 4.2p1 scp system privilege escalation
| [1724] OpenBSD OpenSSH 4.0 GSSAPIDelegateCredentials denial of service
| [1723] OpenBSD OpenSSH 4.0 Dynamic Port Forwarding denial of service
```

La herramienta nmap nse vulscan es muy completa, esta realiza detección de vulnerabilidades a través de distintas herramientas, la primera podemos ver arriba, vulDB, esta ha detectado en la máquina metasploitable2 vulnerabilidades relacionados con la escalada de privilegios, estos ataques explotan las vulnerabilidades de seguridad con el objetivo de elevar el acceso a una red, aplicación o sistema. La escalada de privilegios requiere a veces que el atacante obtenga el rol de administrador para realizar los ataques deseados. Cabe destacar que la lista es larga por lo que solo expongo algunos ítems.

El resultado arrojado por mitre, es bastante largo, por lo que expongo solo los resultados desde 2007, 21 tipos de vulnerabilidades en total lo que hace ver que la maquina es muy vulnerable a ataques, algunas de las vulnerabilidades encontradas son de acceso remoto, vulnerabilidad de manipulación externa como el alojamiento del caballo de troya y su ejecución e impactos desconocidos por el usuario, accesos a equipos de forma arbitraria, escuchar puertos, eludir restricciones, entre muchos otros.

```
| MITRE CVE - http
| [CVE-2010-4755]
, allow remote aut
uests to an sftp d
| [CVE-2007-4752]
privileges by caus
| [CVE-2009-2904]
ivileges via hard
| [CVE-2008-4109]
| [CVE-2008-3844]
that allows the pa
obtained these pa
| [CVE-2008-3234]
, followed by the
| [CVE-2008-1657]
| [CVE-2008-1483]
port, as demonstra
| [CVE-2007-6415]
| [CVE-2007-3102]
to an audit log vi
| [CVE-2007-2243]
```

Esta herramienta, securityfocus, detecto un desbordamiento de bufer de token al igual que IBM, lo mismo para exploir DB.

```
SecurityFocus - https://www.securityfocus.com/bid/:
[4560] OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow Vulnerability

IBM X-Force - https://exchange.xforce.ibmcloud.com:
[8896] OpenSSH Kerberos 4 TGT/AFS buffer overflow

Exploit-DB - https://www.exploit-db.com:
[21402] OpenSSH 2.x/3.x Kerberos 4 TGT/AFS Token Buffer Overflow Vulnerability
[3303] Portable OpenSSH ≤ 3.6.1p-PAM / 4.1-SUSE Timing Attack Exploit
[2444] OpenSSH ≤ 4.3 p1 (Duplicated Block) Remote Denial of Service Exploit
```

OpenVas, ha detectado muchas mas vulnerabilidades, una lista de mas de 30 que no están expluestas en su totalidad, entre estas, la vulnerabilidad de desbordamiento de bufer, vulnerabilidad de divulgación de información, vulnerabilidad de secuestro de sesión de conexiones, actualización de información y aviso de seguridad.

```
OpenVAS (Nessus) - http://www.openvas.org:
[902488] OpenSSH 'sshd' GSSAPI Credential Disclosure Vulnerability
[900179] OpenSSH CBC Mode Information Disclosure Vulnerability
[881183] CentOS Update for openssh CESA-2012:0884 centos6
[880802] CentOS Update for openssh CESA-2009:1287 centos5 i386
[880746] CentOS Update for openssh CESA-2009:1470 centos5 i386
[870763] RedHat Update for openssh RHSA-2012:0884-04
[870129] RedHat Update for openssh RHSA-2008:0855-01
[861813] Fedora Update for openssh FEDORA-2010-5429
[861319] Fedora Update for openssh FEDORA-2007-395
[861170] Fedora Update for openssh FEDORA-2007-394
[861012] Fedora Update for openssh FEDORA-2007-715
[840345] Ubuntu Update for openssh vulnerability USN-597-1
[840300] Ubuntu Update for openssh update USN-612-5
[840271] Ubuntu Update for openssh vulnerability USN-612-2
[840268] Ubuntu Update for openssh update USN-612-7
```

Securitytracker, ha detectado vulnerabilidades como el acceso remoto arbitrario, una vulnerabilidad muy peligrosa que permite a usuarios remotos el acceso a información confidencial , ejecutar código arbitrario, una vulnerabilidad que da a los usuarios privilegios elevados, otra que niega el acceso a dispositivos de manera remota, entre otros.

```
SecurityTracker - https://www.securitytracker.com:
[1028187] OpenSSH pam_ssh_agent_auth Module on Red Hat Enterprise Linux Lets Remote Users Execute Arbitrary C
[1026593] OpenSSH Lets Remote Authenticated Users Obtain Potentially Sensitive Information
[1025739] OpenSSH on FreeBSD Has Buffer Overflow in pam_thread() That Lets Remote Users Execute Arbitrary Cod
[1025482] OpenSSH ssh-keysign Utility Lets Local Users Gain Elevated Privileges
[1025028] OpenSSH Legacy Certificates May Disclose Stack Contents to Remote Users
[1022967] OpenSSH on Red Hat Enterprise Linux Lets Remote Authenticated Users Gain Elevated Privileges
[1021235] OpenSSH CBC Mode Error Handling May Let Certain Remote Users Obtain Plain Text in Certain Cases
[1020891] OpenSSH on Debian Lets Remote Users Prevent Logins
[1020730] OpenSSH for Red Hat Enterprise Linux Packages May Have Been Compromised
[1020537] OpenSSH on HP-UX Lets Local Users Hijack X11 Sessions
[1019733] OpenSSH Unsafe Default Configuration May Let Local Users Execute Arbitrary Commands
[1019707] OpenSSH Lets Local Users Hijack Forwarded X Sessions in Certain Cases
```

Osvdb, ha detectado vulnerabilidades relacionadas con la saturación de conexión remota, en su mayoría las vulnerabilidades halladas se relación con la conexión remota, por lo que el acceso, control y robo de información de la maquina analizada se hace muy fácil para un atacante.

```
OSVDB - http://www.osvdb.org:
[92034] GSI-OpenSSH auth-pam.c Memory Management Authentication Bypass
[90474] Red Hat / Fedora PAM Module for OpenSSH Incorrect error() Function Calling Local Privilege Escalation
[90007] OpenSSH loggingracetime / maxstartup Threshold Connection Saturation Remote DoS
[81500] OpenSSH gss-serv.c ssh_gssapi_parse_ename Function Field Length Value Parsing Remote DoS
[78706] OpenSSH auth-options.c sshd auth_parse_options Function authorized_keys Command Option Debug Message Information Disclosure
[75753] OpenSSH PAM Module Aborted Conversation Local Information Disclosure
[75249] OpenSSH sftp-glob.c remote_glob Function Glob Expression Parsing Remote DoS
[75248] OpenSSH sftp.c process_put Function Glob Expression Parsing Remote DoS
[72183] Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure
[70873] OpenSSH Legacy Certificates Stack Memory Disclosure
[69658] OpenSSH J-PAKE Public Parameter Validation Shared Secret Authentication Bypass
```

NMAP NSE VULNER

La herramienta vulner detecto vulnerabilidades CVE y SSV, relacionadas con la conexión remota, algunas son vulnerabilidades como la baja complejidad de acceso, evasión de autenticación de directiva, vulnerabilidades que pueden ser explotadas por atacantes y que facilitan la denegación del servicio por parte de estos, entre otros.





```
(veronica@kali)-[/usr/share/nmap/scripts]
$ nmap -sV --script vulners 10.0.2.8 -p 22 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-14 23:10 CET
Nmap scan report for 10.0.2.8
Host is up (0.0031s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|   SECURITYVULNS:VULN:8166 7.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|   CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
|   CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
|   SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
|   CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
|   CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
|   CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
|   CVE-2008-5161 2.6 https://vulners.com/cve/CVE-2008-5161
|   CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
|   CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
|_ SECURITYVULNS:VULN:9455 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

Ejercicio 2 – OpenVAS

Realizar un análisis de vulnerabilidades sobre el equipo Metasploitable2 utilizando OpenVAS.

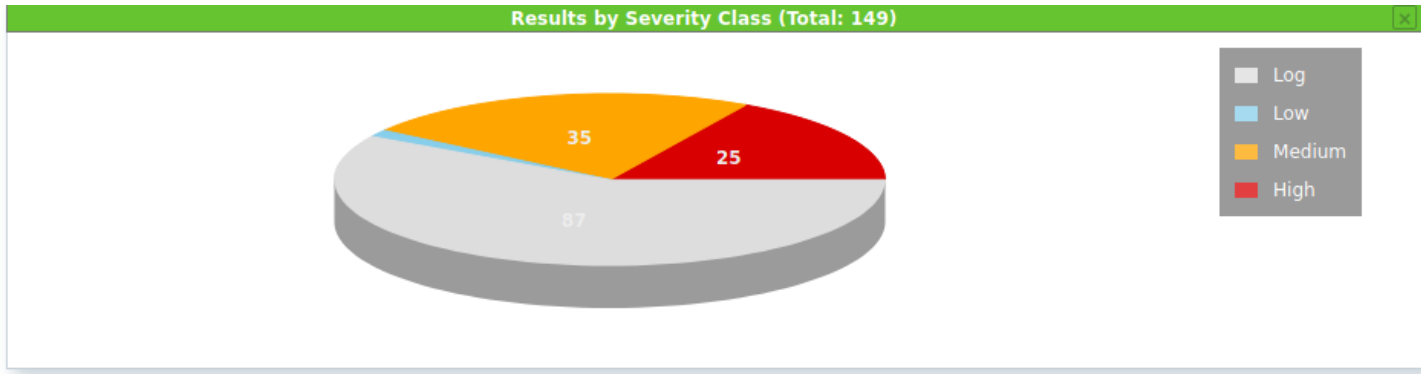
Iniciamos el análisis de vulnerabilidades de la maquina metasploitable2 exponiendo su composición. En este caso, esta maquina posee sistemas operativos en parte Ubuntu, linux y debian.

Name	Title
 cpe:/o:debian:debian_linux	
 cpe:/o:linux:kernel	
 cpe:/o:canonical:ubuntu_linux:8.04	
 cpe:/o:canonical:ubuntu_linux	

Abajo se expone un pequeño resumen de lo analizado en la maquina metasploitable2, esto es, una vez analizados todos los ítems se encontraron varias vulnerabilidades de las que halaremos mas adelante, 25 son de alta gravedad, 35 media y 2 de baja gravedad y 87 inicio de sesión.

Status	Task	Severity	High	Medium	Low	Log	False Pos.
Done	Immediate scan of IP 10.0.2.8	10.0 (High)	25	35	2	87	0

En cuanto a los resultados arrojados por la herramienta describe que la maquina se encuentra vulnerable a ataques tanto físicos, locales como remotos, del total de 149 vulnerabilidades detectadas 25 son muy peligrosas y de alta gravedad, en la tabla de abajo se puede ver cuales son, y estas son las únicas de las que hablaremos por ahora.



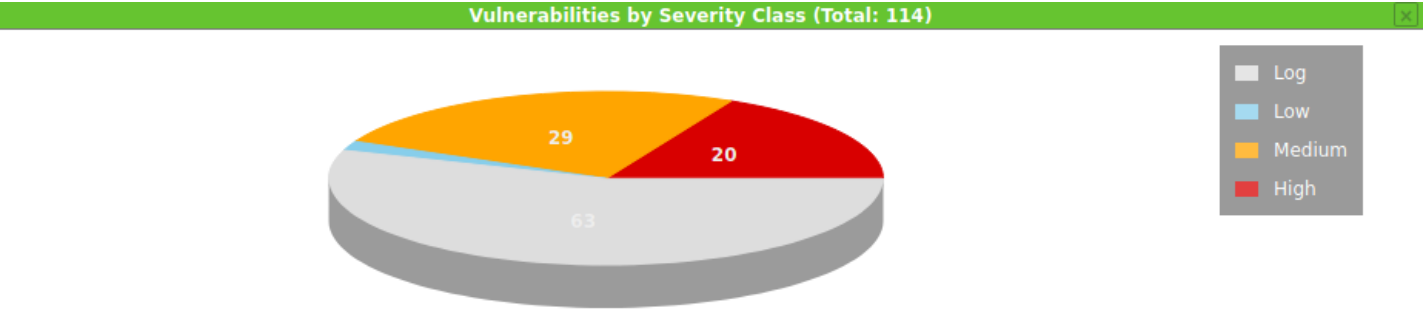
En cuanto al primer ítem OS END OF LIFE DETECTION, el sistema operativo utilizado llegó al final de su vida útil por lo que debe ser actualizado de manera que no se vuelva un problema, en cuanto al Twiki (ítem 3) El host está ejecutando TWiki y es propenso a Cross-Site Scripting (XSS) y vulnerabilidades de ejecución de comandos, distributed ruby ; los sistemas que utilizan Distributed Ruby (dRuby/DRb), que está disponible en las versiones de Ruby 1.6 y posteriores, pueden permitir que los sistemas no autorizados ejecuten comandos distribuidos., uno de los más peligrosos hallados y que posee una puntuación perfecta en gravedad es rlogin el cual permite acceso a root sin contraseña, de aquí en adelante, la puntuación según la gravedad de la vulnerabilidad va disminuyendo hasta llegar a 0.

Vulnerability		Severity ▼
OS End Of Life Detection	🔒	10.0 (High)
Possible Backdoor: Ingreslock	🔒	10.0 (High)
Twiki XSS and Command Execution Vulnerabilities	🔒	10.0 (High)
The rexec service is running	🔒	10.0 (High)
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	🔒	10.0 (High)
rlogin Passwordless Login	🔒	10.0 (High)
DistCC Remote Code Execution Vulnerability	🔒	9.3 (High)
VNC Brute Force Login	🔒	9.0 (High)
PostgreSQL weak password	🔒	9.0 (High)
MySQL / MariaDB weak password	🔒	9.0 (High)

Vulnerability		Severity ▼
SSH Brute Force Logins With Default Credentials Reporting	🔒	7.5 (High)
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	🔒	7.5 (High)
FTP Brute Force Logins Reporting	🔒	7.5 (High)
rsh Unencrypted Cleartext Login	🔒	7.5 (High)
vsftpd Compromised Source Packages Backdoor Vulnerability	🔒	7.5 (High)
Check for Backdoor in UnrealIRCd	🔒	7.5 (High)
vsftpd Compromised Source Packages Backdoor Vulnerability	🔒	7.5 (High)
FTP Brute Force Logins Reporting	🔒	7.5 (High)
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	🔒	7.5 (High)
Test HTTP dangerous methods	🔒	7.5 (High)

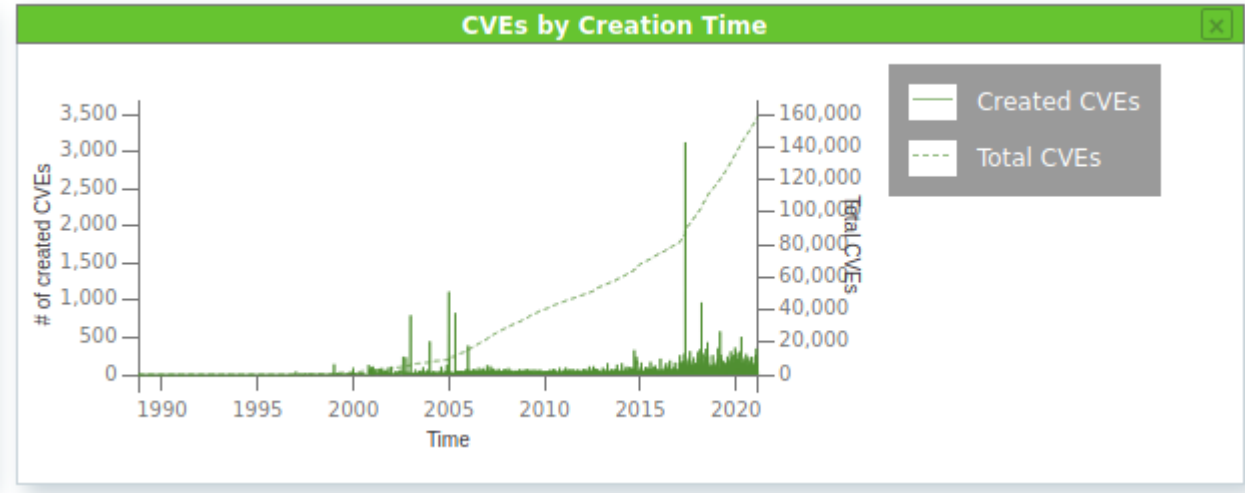
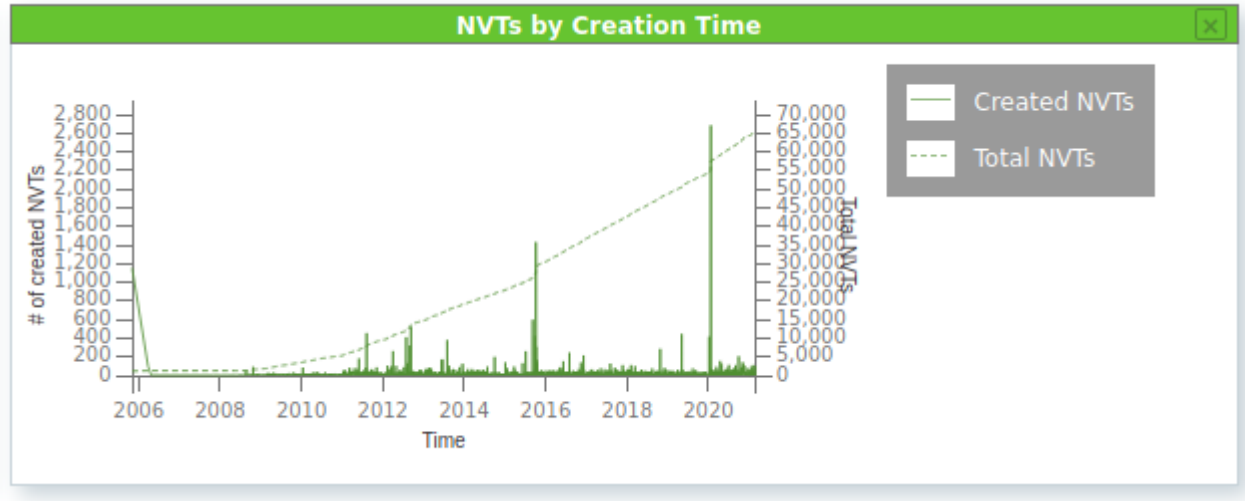
En el grafico de abajo se puede notar las vulnerabilidades según la gravedad, esta lista es la misma que la expuesta anteriormente a diferencia de que posee un orden distinto y mas información acerca de la vulnerabilidad como ser el CVE, fechas y como mitigar el problema, además de que este análisis es mas restrictivo que el arrojado por los resultados.

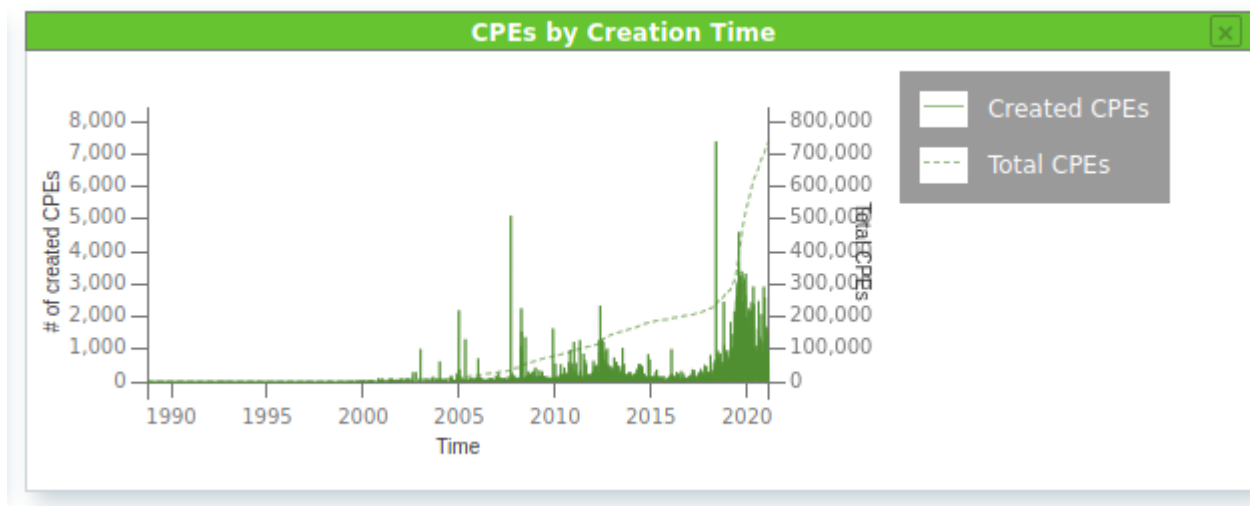
Como se puede ver 20 vulnerabilidades son consideradas altamente peligrosas, 29 parcialmente, y asi sucesivamente.



Se pueden clasificar las vulnerabilidades en categorías, esta herramienta permite esta segmentación, el NVT es un test de vulnerabilidades que evalúa dispositivos conectados a la red. La CVE es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID. La CPE se considera un estándar de la industria que se utiliza para proporcionar una forma uniforme de mostrar información sobre sistemas operativos, hardware y software.

Teniendo en cuenta esto exponemos abajo la cronología de creación o aparición de estas vulnerabilidades, esto como se ve va en aumento inminente, por ende mitigar las vulnerabilidades inmediatamente son detectadas es muy importante para mantener la seguridad informática y de la información.





- Generar un informe y subirlo a classroom.

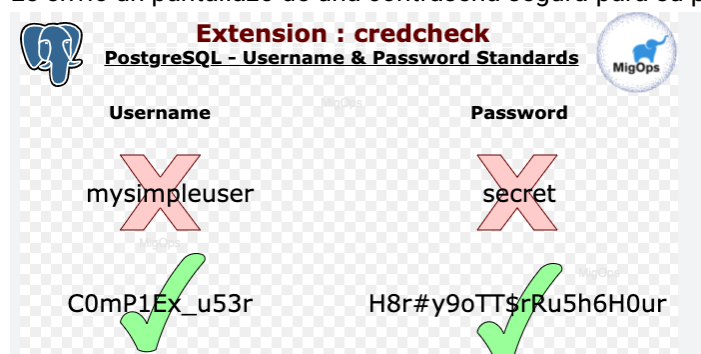
SUBIDO AL CLASSROOM

Ejercicio 3 - Caso Real

- Imagina que un cliente te solicita información por correo detallada de alguna de las vulnerabilidades de tus informes. En base a esto, desarrolla una explicación detallada de la vulnerabilidad que elijas.

Estimado Señor Mersan,

Por este medio me comunico teniendo en cuenta su consulta acerca de posibles ataques a los que puede que estén expuestos, le comento con mayor detalle, que sabiendo el tipo de conexiones de sus máquinas, las cuales se encuentran en red y el hecho de que sus informáticos mencionaron que la contraseña tanto de sus servidores locales como la de las máquinas en red son débiles, esta puede ser una vulnerabilidad para fácil acceso por parte de intrusos, en su servidor principal hallamos que la contraseña era 1234, lo cual es muy fácil de pensar para cualquier atacante experimentado, esta vulnerabilidad lleva el nombre de CONTRASEÑA DEBIL DE POSTGRESQL, PostgreSQL es el que permite la protección de los datos de su compañía, por lo que sus datos podrían estar expuestos, y caso algún usuario externo no autorizado quisiera ingresar a su hardware podrá hacerlo. Por todo esto es conveniente el cambio inmediato de su contraseña a una mas fuerte para mayor seguridad, también es valido el otorgamiento de permisos desde usuario a superusuario. Adicionalmente, realizar el mismo procedimiento con sus demás dispositivos corporativos. Le envío un pantallazo de una contraseña segura para su protección.



Sin otro particular,

Me despido atentamente.

Ejercicio 4 - Nmap NSE y OpenVAS

- ¿Véis algún resultado de OpenVAS que concuerden con los de los scripts de Nmap NSE utilizados? Poned algún ejemplo (uno o dos) de CVE's si es así, y si no, razonad el por qué.

No encontré coincidencias de lo detectado por nmap y openvas, puede que yo no lo haya revisado bien, pero teniendo en cuenta sus funciones, nmap escanea puertos de manera abierta hallando en el camino vulnerabilidades de manera profunda, y por otro lado, openvas es un sistema abierto de evaluación de vulnerabilidades, este es un asistente de seguridad de aplicaciones web y además ofrece soluciones para mitigar estas vulnerabilidades, mientras nmap posee fortalezas en el escaneo de herramientas y redes.