Introducció a la Seguretat Informàtica

i la seva relació amb els CPDs

Frederic W. Uhlmann

Index

Introducció

Aquest treball es centra en la creació d'un petit curs introductori a diversos conceptes bàsics de la seguretat informàtica i la seva relació amb els CPDs, orientat a una persona sense coneixement del tema o un nivell de coneixement molt limitat. El propòsit és que una persona que rep aquest curs, o llegeix aquest assaig, sigui capaç d'adquirir un coneixement mínim bàsic sobre el tema i les implicacions que podria tenir.

Que es la seguretat Informatica?

Segons el NIST podem definir la seguretat informàtica o seguretat de la informació com a:

> The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[1]

Cosa que traduït seria com:

> Protegir la informació i sistemes d'informació davant d'accés i ús no autoritzat, divulgació, disrupció, modificació o destrucció per proporcionar confidencialitat, integritat i disponibilitat.

Per tant, aquesta definició ens porta directament a la següent secció.

Els pilars de la Seguretat Informàtica

A continuació veurem aquests tres pilars (sovint anomenat CIA) que pretén protegir la Seguretat Informàtica tal com les descriu el "INFOSEC Institute"[2]:

Confidencialitat (Confidentiality)

> Confidentiality revolves around the principle of 'least privilege.' This principle states that access to information, assets, etc. should be granted only on a need to know basis so that information which is only available to some should not be accessible by everyone.

En aquest aspecte doncs, tracta de protegir les dades de ser vistes per tercers, sobretot quan es tracten de secrets o dades personals. Com a exemple, imaginem una empresa farmacèutica. Aquesta empresa tindrà un molt elevat interès en què les seves dades de recerca no tinguin compromeses la seva confidencialitat i acabin en mans de competidors.

Integritat (Integrity)

---

[1] https://csrc.nist.gov/glossary/term/INFOSEC
[2] https://resources.infosecinstitute.com/topic/cia-triad/

> Integrity makes sure that the information is not tampered whenever it travels from source to destination or even stored at rest.

Amb el que volem dir que volem protegir les dades de ser canviades o manipulades per a entitats terceres. Un exemple per a veure-ho més clar podria ser el següent: un banc està molt interessat en preservar la integritat de les seves dades del saldo dels comptes del seu client, en cas que aquesta integritat es veiés compromesa, estaríem parlant del fet que els diners disponibles per a els clients poden haver sigut manipulats. Com a tal, les conseqüències tant pel banc com pel client podrien ser devastadores.

Disponibilitat (Availability)

> Availability concept is to make sure that the services of an organization are available.

Bàsicament el que es pretén és garantir que el servei en qüestió estigui disponible. Un exemple que podríem donar d'aquest punt és imaginar que Amazon cau i queda indisponible pels seus clients. Segons el temps que el servei queda inoperable, les pèrdues per a Amazon poden ser massives i fins i tot significar milions en pèrdues en el pitjor dels casos.

Black Hat vs White Hat

Es tracta de termes més aviat informals per a classificar el que la gent anomena "hackers" segons la seva intencionalitat. Es coneix les tres següents classificacions:

Black Hat

Un "hacker" és considerat Black Hat si fa les seves accions per tal d'obtenir algun benefici independentment del potencial mal que poden causar. Normalment són el tipus de "hackers" que duguen a terme activitats il·legals, prohibides o immorals.

White Hat

Un "hacker" es considera White Hat si usa els seus coneixements per tal de protegir davant d'atacs maliciosos d'una forma moral o legal. Un exemple en seria un consultor o pentester que reporta vulnerabilitats per tal que el fabricant o l'empresa propietària pugui solucionar les vulnerabilitats abans de potencialment ser atacats per algú amb intencions menys bones.

Grey Hat

Finalment tenim la classificació de Grey Hat que es refereix a aquell tipus de "hacker" que du a terme activitats tant d'un tipus com de l'altre. Un exemple em podria ser algú que treballa de consultor de dia i ven exploits al mercat negre durant la nit.

Blue Team vs Red Team

En aquesta secció es defineixen els termes de Blue Team i Red Team per tal d'entendre la diferència i quin tipus de feina fan cada un. Es tracta de dos equips que realitzen simulacions d'atac i defensa per tal d'intentar replicar escenaris reals i per un costat tancar falles de seguretat i per un altre costat poder garantir que es poden detectar certs atacs quan es reben.[3]

Blue Team

Com a Blue Team es pot entendre un equip normalment format per professionals de monitoratge i resposta d'incidents que té el rol de detectar amenaces i implementar millores per tal de minimitzar la superfície d'atac i el risc que poden implicar aquests atacs.

Red Team

Com a Red Team es pot entendre un equip que té com a objectiu la realització amb èxit d'atacs i la identificació i explotació de falles de seguretat en la defensa d'una empresa. Es pot dir que agafen el rol del potencial atacant per a detectar on estan les falles de seguretat i així poder-les solucionar.

Per tant es pot dir que el Blue team està més orientat a les tasques de protecció i monitoratge actiu dels sistemes i la seva seguretat mentre que el Red Team es centra en la detecció de vulnerabilitats en els sistemes i els entorns amb els quals treballen.
Aquest curs està orientat més aviat a la part de Red Team dins de la seguretat per tal de no repetir temes tractats en altres treballs més orientats al que tractaria un Blue Team.

Bugs, Vulnerabilitats i Exploits

A continuació s'expliquen aquests tres termes que poden resultar similars, però tenen diferències significatives entre ells. Aquests són alguns dels termes relacionats amb seguretat més usats en el dia a dia i és d'importància entendre bé del que es parla quan es fa referència a cada un d'aquests termes.

Bugs

Com tots sabem, un bug es pot definir com un error en un codi o sistema que resulta en un resultat erroni o inesperat. Per a dir-ho d'una forma més senzilla, un bug és conegut com un error informàtic.

Vulnerabilitats

Quan parlem d'una vulnerabilitat estem parlant d'un bug tal com s'ha descrit a dalt, amb la diferència que té una implicació de seguretat. Per tant podem dir que tota vulnerabilitat és un bug, però no tot bug és una vulnerabilitat.

[3] https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

Exploits

Quan parlem d'exploits, estem parlant de codis o aplicacions que fan ús d'una vulnerabilitat per a aconseguir algun fi. Un exemple d'exploit molt conegut en el sector va ser l'anomenat Eternalblue que abusava d'una vulnerabilitat en sistemes Windows per tal de fer-se amb control d'una màquina i infectar-la del ransomware conegut amb el nom de WannaCry.[4]

[4] https://risksense.com/wp-content/uploads/2018/05/White-Paper_Eternal-Blue.pdf

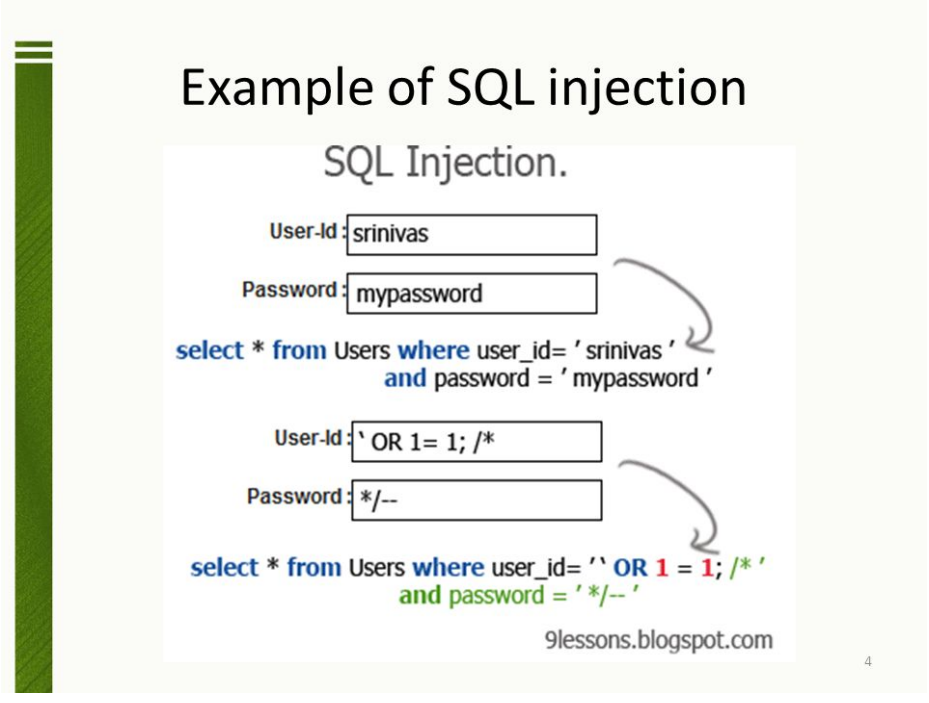
Exemples de vulnerabilitats comunes

A continuació s'expliquen breument algunes de les vulnerabilitats més comunes que ens podem trobar avui en dia. Aquestes vulnerabilitats estan majoritàriament centrades a web, ja que és el principal i més important vector d'atac a infraestructures i sistemes que podem trobar en un CPD.

SQL Injection

La SQL Injection (SQLi) tracta d'injectar codi SQL en una part del codi, normalment d'una web, que fa accessos a base de dades. D'aquesta forma es poden aconseguir coses com saltar-se un login, llistar o enumerar una base de dades sencera, aconseguir amb el control del servidor en cas que l'usuari que executi el sistema de bases de dades SQL tingui privilegis elevats en el sistema en el qual està ubicat.[5]

He pogut trobar la següent imatge per a il·lustrar millor com es du a terme un atac de tipus SQL Injection:



Cross Site Scripting

El Cross Site Scripting (XSS) és un tipus d'atac que es basa en la injecció de codi JavaScript en seccions d'una web que ho permetin. D'aquesta forma podrem des de canviar contingut d'una web de forma permanent a fer-nos amb les credencials dels usuaris d'una web. [6]

---

[5] https://owasp.org/www-community/attacks/SQL_Injection
[6] https://owasp.org/www-community/attacks/xss/

Un exemple de cas de XSS seria canviar-me el meu nom d'usuari facebook a un codi maliciós que s'executa cada vegada que algú visita el meu perfil i que m'envia les seves cookies d'autenticació, per a així a posteriori poder-me autenticar com a aquella persona. De fet, precisament aquesta aplicació és una de les més usades en el dia a dia, per tal de fer-se amb les sessions d'usuaris arbitraris.

Cal dir que hi ha diversos tipus de XSS i que és un tema molt més complex, però contingut més avançat ja queda fora de l'abast d'aquest document.

Cross Site Request Forgery

El Cross Site Request Forgery (CSRF) és un tipus d'atac que es basa a aconseguir que algú altre executi alguna funcionalitat per a nosaltres, ja sigui perquè nosaltres no tenim permisos, o perquè no volem deixar registre d'haver-hi fet una acció concreta nosaltres. Qualsevol altra raó que se'ns pugui ocórrer que necessiti algú altre executant alguna cosa per nosaltres pot ser una raó àlida.[7]

Com a exemple d'aquesta vulnerabilitat imaginem la situació en què volem canviar-nos la nota que tenim de CPD, però nosaltres no tenim permisos per a fer-ho, el millor que podríem fer és un atac de tipus CSRF. El que faríem doncs és enviar-li una web al nostre professor de, per exemple, un joc de picar talps que, per darrere, té amagada la web de canviar notes, fent-lo picar en aquells llocs de la web que ens convenen. Com podem veure, és un tipus d'atac molt complex de dur a terme, però que podria tenir un impacte significatiu, com per exemple, posar-nos una nota que no ens hem merescut.

Unrestricted File Upload

El "Unrestricted File Upload" és un tipus de vulnerabilitat que fa ús de la funcionalitat de pujades de fitxers a un servidor (per a la raó que sigui, ja sigui una foto de perfil, un treball d'universitat, etc). La vulnerabilitat es dóna quan no hi ha un control sobre el tipus de fitxer que es puja o l'extensió d'aquest fitxer. Per tant, ens permet pujar fitxers que continguin codi maliciós que el servidor pugui interpretar per tal de fer que el servidor ho executi i faci el que ens convingui. Un exemple seria pujar un fitxer amb una webshell que ens donaria control sobre el servidor amb permisos de l'usuari que executa el servidor web.[8]

Per a finalitzar aquesta secció, concloure que aquí només s'han exposat i breument explicat 4 tipus d'atac o vulnerabilitats d'entre moltíssimes. Hi ha moltes més vulnerabilitats i inclús vàries de les que s'han exposat aquí tenen diferents tipus o subclassificacions que no s'han explicat aquí. De nou, aquest curs sols serveix com una breu introducció i no és un curs exhaustiu sobre la seguretat informàtica.

[7] https://owasp.org/www-community/attacks/csrf
[8] https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Una mica sobre seguretat en AWS

Donat que AWS és un IaaS, PaaS i SaaS, segons el servei que contractem, la importància en la seguretat AWS recau sobre l'ús correcte de les configuracions, restriccions i permisos segons best practices definides per Amazon.
Com que Amazon gestiona la seva pròpia infraestructura i ens posa a disposició part d'ella, també s'assegura de la seguretat d'aquesta part, per tal sols ens queda utilitzar degudament les eines que ens posa a disposició i configurar els diversos serveis en línia amb el que proposen les best practices d'Amazon.

Per a fer-nos una idea, algunes de les configuracions o elements més importants a revisar són els permisos, usuaris i grups del IAM (Identity and Access Management) i les configuracions de seguretat dels buckets S3 (servei d'emmagatzematge de dades). Com cada compte AWS i serveis contractats és diferent, cada revisió de seguretat d'un compte AWS pot ser diferent i implicar la revisió d'unes configuracions vàries en funció dels serveis contractats.

NCCGroup ScoutSuite

NCCGroup[9], una empresa amb cert renom al sector del Regne Unit, ha desenvolupat i posat a disposició públicament una eina que ajuda amb revisar les configuracions establertes en un entorn AWS i comparar-les amb les best practices que recomana Amazon. Podem trobar aquesta eina en el següent enllaç:

- https://github.com/nccgroup/ScoutSuite

Principal font d'informació per a aspectes relacionats amb AWS

La font d'informació principal que recomano utilitzar per aspectes relacionats amb la seguretat de la configuració d'algun element AWS és la pròpia documentació que ofereix AWS que inclou moltes recomanacions de seguretat i que es pot trobar en el següent enllaç:

- https://docs.aws.amazon.com/

[9] https://www.nccgroup.com/

Relació amb els CPDs

La relació de la seguretat de la informació i els CPDs que són els centres de processament de dades, on es situen, gestionen i emmagatzemen aquestes dades, és molt òbvia. Però, per tal de donar a entendre millor aquesta relació, a continuació donaré alguns exemples del dia a dia amb els que ens podem trobar:

Un exemple podria ser l'ús d'una web. Imaginem una tenda en línia de sabates. Tot el catàleg, el codi de la web, les dades dels usuaris, etc. és informació que finalment està emmagatzemada en un CPD, i per tant, comprometre aquesta web, pot resultar en comprometre el CPD.

Un altre exemple que puc donar és una aplicació mòbil. Imaginem una aplicació de banking. Tota la informació dels usuaris, comptes corrents, diners disponibles, contrasenyes, etc. és, altre cop, informació que finalment està emmagatzemada en un CPD i, comprometent aquesta aplicació o el servidor que respon a les peticions de l'aplicació, podria resultar en comprometre el CPD.

Finalment, un exemple més aviat físic. L'accés a àrees o edificis restringits per targetes d'accés tenen els usuaris i permisos d'aquestes targetes han d'estar emmagatzemats a algun lloc, probablement un CPD, sigui propi de l'empresa o extern. Per tal, altre cop, si comprometem el sistema, podem comprometre el CPD. Inclús es pot donar el cas contrari, on comprometent el CPD, acabem comprometem els sistemes els quals en fan ús.

Per tant, finalment, qualsevol dada emmagatzemada que es pot trobar en qualsevol CPD pot ser objectiu de ser compromesa. Per tant, la seguretat de la informació i el mateix sistema en el qual es gestiona i emmagatzema aquesta informació estan molt estretament relacionats.

Algunes conclusions

Primerament, cal dir que tant aquest document com el curs que representa únicament rasca la superfície dels amplis coneixements del món de la seguretat informàtica. Donada la reduïda extensió d'aquest treball i el curs que inclou s'ha intentat fer focus en donar a conèixer conceptes molt bàsics i àmplia varietat per tal de complir amb dos objectius. Per un costat es vol aconseguir que el receptor d'aquest document o curs sigui capaç de llegir o entendre altra documentació i no anar totalment perdut. Per altre costat donar una base a partir de la qual el receptor por expandir el seu coneixement.

També, volia parlar sobre l'elevada importància que té la seguretat informàtica per a la protecció de les dades i perquè volem protegir les dades. He intentat donar exemples de situacions quotidianes amb les quals ens podem trobar en el món dels negocis i impactes que podria tenir, per tal de destacar la importància d'aquest tema i que, independentment del sector on treballem, és un tema que hem de tenir molt present.

Tot seguit, volia proposar una petita reflexió i parlar del fet que, a dia d'avui, cada vegada passem més informació de la que depenem a un format digitalitzat. Hem de ser conscients que alguns serveis bàsics i essencials com hospitals i altres serveis públics dels quals depenem fortament poden arribar a deixar de donar servei en cas d'un atac i per tant la disponibilitat d'aquest tipus de dades pot, en algunes situacions, ser literalment un tema de "vida o mort". Per tant, crec que és d'elevada importància, especialment en el nostre sector, que compartim aquests coneixements per a que tothom, ja sigui developer, sysadmin, arquitecte de xarxes o el que sigui, pugui ser un xic més conscient de la importància que té protegir degudament les dades que gestiona en el seu dia a dia.

Finalment, vull acabar les conclusions reforçant la reflexió del paràgraf anterior i dir que, tots hauríem de tenir una petita base de coneixements de seguretat, si més no, pel que fa al que a nosaltres ens afecta. Per exemple, si algú és administrador de bases de dades, potser no cal que sàpiga sobre configuracions de firewall, però considero que hauria de saber un mínim sobre seguretat en bases de dades per tal de protegir les dades que gestiona.

Fonts i recursos per aprendre més

En aquesta secció de l'assaig presento fonts i recursos que es poden utilitzar per a obtenir més coneixement sobre seguretat informàtica, ja que aquest assaig i el curs relacionat és únicament una introducció i no conté coneixements avançats.

Fonts d'informació interessants

En aquesta secció es detallen fonts d'informació genèrica que poden resultar útils per a adquirir més coneixement o mantenir-se al dia amb temes relacionats.

OWASP

Open Web Application Security Project (OWASP) és una organització sense ànim de lucre que està orientada a millorar la seguretat del software. És probablement una de les fonts més interessants, ja que tenen tota mena de documentació i inclús fan estudis tipus top 10 vulnerabilitats més presents/trobades cada any entre molta altra informació que proporcionen. En el següent enllaç podem trobar més informació:

- https://owasp.org/

SANS

SANS es dedica a entrenament i formació en ciberseguretat i és una font interessant per a informar-se sobre diversos tipus de certificacions, a part que igual que OWASP ofereixen àmplia informació en forma de documents, publicacions de blog, etc. En el següent enllaç podem trobar més informació:

- https://www.sans.org/

NIST

National Institute of Standards and Technology (NIST) és una agència d'Estats Units que en part s'encarrega de tot tema relacionat amb vulnerabilitats o seguretat de la informació i per tant ens ofereix informació útil de tota mena com publicacions, una base de dades de vulnerabilitats, etc. En el següent enllaç podem trobar més informació:

- https://www.nist.gov/

cvedetails.com

Cvedetails és bàsicament una base de dades de vulnerabilitats actuals conegudes per tota mena de fabricant i productes que es troben en el mercat. En el següent enllaç podem trobar més informació:

- https://www.cvedetails.com/

Blogs i webs d'empreses de renom del sector

A continuació poso a disposició una llista acotada d'empreses del sector, moltes de les quals tenen algun blog associat o fan publicacions a LinkedIn, que val la pena seguir. S'ha de tenir en compte que la llista no és exhaustiva i hi han moltes altres empreses del sector que poden ser d'elevat interès seguir:

- NCCGroup
- Tarlogic
- Rapid7
- Tenable
- ...

Conferencies interessants

Noconname

Conferència que es du a terme a Barcelona. És de caràcter més petit o local, però considerant que ho tenim molt a prop, és una avantatge, ja que és un esdeveniment al qual podrem assistir sense massa problema. En el següent enllaç podem trobar més informació:

- https://www.noconname.org/

Rootedcon

Conferència més important i reconeguda a escala nacional que es du a terme a Madrid. És una oportunitat molt interessant per a obtenir més coneixement i una visió més detallada sobre el sector de la seguretat a un nivell nacional. En el següent enllaç podem trobar més informació:

- https://www.rootedcon.com/

Navaja Negra

Conferència que es du a terme a Albacete i és de caràcter més aviat "Black Hat" i és coneguda per a ser un xic més centrada en temes amorals, per a dir-ho d'alguna forma. En el següent enllaç podem trobar més informació:

- https://www.navajanegra.com/

HackInParis

Conferència molt reconeguda a escala d'Europa que es du a terme a París, com ja indica el seu nom. En el següent enllaç podem trobar més informació:

- https://hackinparis.com/

Defcon

Conferència de ciberseguretat més coneguda arreu del món que es du a terme a Las Vegas. En aquesta conferència probablement es poden veure les xerrades sobre descobriments més punters del sector comparat amb totes les anteriors. En el següent enllaç podem trobar més informació:

- https://www.defcon.org/

Recursos per aprendre

WebForPentester

Es tracta d'unes màquines virtuals amb exercicis senzills i un curs en format PDF per a seguir aquests exercicis. Eina molt bàsica per a familiaritzar-se amb les tècniques emprades a la seguretat informàtica. En el següent enllaç podem trobar més informació:

- https://pentesterlab.com/exercises/web_for_pentester

Hackthebox

Plataforma per a practicar les tècniques usades en seguretat informàtica amb un model similar a l'anterior, però molt més complet i avançat. En el següent enllaç podem trobar més informació:

- https://www.hackthebox.eu/

Hackthissite

Plataforma per a practicar les tècniques usades en seguretat informàtica basades en una aplicació web, on no veurem que fa o deixa de fer el servidor que hi ha per darrere i per tant ofereix l'escenari més realista per a seguretat informàtica web. En el següent enllaç podem trobar més informació:

- https://www.hackthissite.org/