# PROJECTE 3
# AUDITORIES DE SEGURETAT

Curs: PQTM 19. Tècnic/a en Ciberseguretat

Ivan Ricart Borges iricartb@uoc.edu

**ÍNDEX**

## 1. DESCRIPCIÓ DE L'ESCENARI

L'auditoria de seguretat es realitzarà sobre l'escenari descrit en el primer projecte, es a dir, el centre d'Estudis de Dret i Ciència Política de la Universitat Oberta de Catalunya (UOC), ubicat al edifici B3 del campus universitari Parc Mediterrani de la Tecnologia (Avda. Carl Friedrich Gauss, 5 08860 Castelldefels).

El centre està compost per un equip de 42 professors, responsables d'impartir els cursos docents relacionats amb el Dret, Ciència Política i Criminologia. Actualment hi participen més de 8794 estudiants acompanyats en el seu procés d'aprenentatge per uns 630 professors col·laboradors que donen suport docent als professors responsables.

L'activitat principal consisteix en impartir els estudis mitjançant la plataforma digital d'ensenyament en línia que ofereix la UOC, la qual, permet distribuir i organitzar els continguts docents, realitzar activitats interactives, avaluar els projectes i les pràctiques, etc. Dintre de l'organització podem classificar la tipologia de l'activitat en diferents categories relacionades amb el personal de direcció, professorat responsable, personal de gestió, personal de recerca i finalment el personal de suport.

Com a principals sistemes d'informació que fa ús el centre, podem citar l'aula virtual per gestionar els continguts docents, la biblioteca virtual per la consulta de material docent, el portal de la UOC per proporcionar informació genèrica i la possibilitat de realització de processos administratius, el sistema externalitzat Symposium per informar i gestionar les inscripcions dels assistents, unitats de disc compartits en xarxa per compartir informació, etc.

Pel que fa la infraestructura utilitzada en el centre per proporcionar els serveis descrits anteriorment i facilitar el desenvolupament de les tasques diàries, podem citar l'ús de terminals o estacions de treball pel personal docent, sala de servidors per proporcionar els serveis i emmagatzemar la informació de forma centralitzada, etc. A continuació podem observar, mitjançant la següent taula, les característiques principals de la infraestructura utilitzada.

| | | |
|---|---|---|
| Estacions de treball | Intel i5, 8 Gb RAM, Windows 10 Pro, Mcafee, etc. | |
| Servidors (CPD) | 4 Racks | Nagios, Web, DB, Backups, etc. |
| | 2 Switch Cisco Brocade | |
| | 2 Balencejadors de càrrega F5 | |
| Xarxa | Connexió de la seu de Castelldefels per fast Ethernet amb la resta de centrals (Tibidabo i Poblenou) | |
| Altres equipaments | Projectors, sala de conferencies, portàtils compartits, etc. | |

## 2. ENUMERAR LES PROVES D'AUDITORIA A REALITZAR SOBRE L'ESCENARI

A continuació enumerem les proves d'auditoria més significatives a realitzar sobre l'escenari descrit en el primer apartat.

### 2.1. POLÍTICA DE SEGURETAT

| CONTROLS | PROVES |
|---|---|
| A.5 Política de seguretat | |
| A.5.1 Política de seguretat de la informació | |
| A.5.1.1 Document de política de seguretat de la informació | Comprovar si la organització disposa d'un document de política de seguretat de la informació. |
| A.5.1.2 Revisió de la política de seguretat de la informació | Comprovar si el document de política de seguretat de la informació s'actualitza regularment o quan es produeix un canvi important. |

### 2.2. SEGURETAT FÍSICA I AMBIENTAL

| CONTROLS | PROVES |
|---|---|
| A.9 Seguretat física i ambiental<br>Prevenir els accessos físics no autoritzats, els danys i les intromissions en les instal·lacions i en la informació de la organització | |
| A.9.1 Àrees segures<br>Previndre els accessos físics no autoritzats, els danys i les intromissions en les instal·lacions i en la informació de la organització | |
| A.9.1.1 Perímetre de seguretat física | Comprovar si cada un dels punts on es troben allotjats recursos d'informació es troben degudament assegurats mitjançant portes, murs o punts amb control d'accés. Ex. sala de servidors. |
| A.9.1.2 Controls físics d'entrada | Comprovar si les àrees segures estan assegurades de tal manera que només hi pot accedir personal autoritzat. |
| A.9.1.3 Seguretat d'oficines, despatxos i instal·lacions | Comprovar si existeixen les diferents mesures de seguretat d'accés sobre oficines, despatxos, etc. |
| A.9.1.4 Protecció contra amenaces externes i d'origen ambiental | Comprovar si existeix una protecció contra elements naturals com el foc, inundacions, etc. |
| A.9.1.5 Treball en àrees segures | Comprovar si existeixen mesures de seguretat |

| | |
|---|---|
| | física necessàries per treballar en àrees segures. |
| A.9.1.6 Àrees d'accés públic i de càrrega i descàrrega | Comprovar si existeix un control sobre la seguretat física en les zones de càrrega i descàrrega. |
| A.9.2 Seguretat dels equips<br>Evitar danys, robatoris o circumstàncies que posin en perill els actius o que puguin provocar la interrupció de les activitats de la organització | |
| A.9.2.1 Protecció d'equips | Comprovar si els equips estan protegits davant possibles amenaces mediambientals, així com d'accessos no autoritzats. |
| A.9.2.2 Instal·lació de subministres | Comprovar si els equips estan degudament protegits contra falles elèctriques. |
| A.9.2.3 Seguretat en el cablejat | Comprovar si el cablejat està degudament protegit i assegurat. |
| A.9.2.4 Manteniment dels equips | Comprovar si els equips reben un manteniment hardware que assegura la seva integritat i disponibilitat. |
| A.9.2.5 Seguretat dels equips fora de les instal·lacions | Comprovar si els equips situats fora de les instal·lacions compleixen els requeriments sobre seguretat establerta. |
| A.9.2.6 Reutilització o retirada segura d'equips | Comprovar si tots els actius hardware i software que continguin dades sensibles són degudament eliminats o destruïts per a que no es puguin accedir. |
| A.9.2.7 Retirada de materials propietat de l'empresa | Comprovar si els actius de la organització no es poden treure sense autorització prèvia de l'encarregat. |

## 2.3. CONTROL D'ACCÉS

| CONTROLS | PROVES |
|---|---|
| A.11 Control d'accés | |
| A.11.1 Requisits de negoci per al control d'accés<br>Controlar l'accés a la informació | |
| A.11.1.1 Política de control d'accés | Comprovar si es porta a cap una política de control d'accés basada en els interessos de l'organització. |
| A.11.2 Gestió d'accés d'usuari<br>Assegurar l'accés d'un usuari autoritzat i previndre l'accés no autoritzat dels sistemes | |
| A.11.2.1 Registre d'usuaris | Comprovar si existeixen controls d'alta, modificació i |

| | |
|---|---|
| | baixa dels usuaris en els diferents sistemes de control e informació. |
| A.11.2.2 Gestió de privilegis | Comprovar si l'assignació de privilegis està restringida i controlada. |
| A.11.2.3 Gestió de contrasenyes d'usuari | Comprovar si la gestió de contrasenyes és un procès controlat. |
| A.11.2.4 Revisió dels drets d'accés d'usuari | Comprovar si la direcció revisa els permisos d'accés dels usuaris regularment. |
| A.11.3 Responsabilitats d'usuari<br>Prevenir l'accés d'usuaris no autoritzats, així com evitar que es comprometi o es produeixi el robatori de la informació | |
| A.11.3.1 Ús de contrasenya | Comprovar si s'instrueix al usuari i s'apliquen requeriments de contrasenyes conforme a les bones pràctiques. |
| A.11.4 Control d'accés a la xarxa<br>Prevenir l'accés no autoritzat als serveis en xarxa | |
| A.11.4.1 Política d'ús dels serveis en xarxa | Comprovar si els usuaris només tenen permisos per als recursos que li son necessari. |
| A.11.4.2 Autenticació d'usuari per a connexions externes | Comprovar si es porta a cap un procediment per a que un usuari fora de les instal·lacions pugui accedir als recursos. |
| A.11.4.3 Identificació dels equips en les xarxes | Comprovar si cada un dels equips connectat a la xarxa es troba registrat i localitzat. |
| A.11.4.4 Diagnòstic remot i protecció contra els ports de configuració | Comprovar si es controla l'accés físic i lògic als ports de diagnòstic i configuració. |
| A.11.4.5 Segregació en les xarxes | Comprovar si els usuaris i sistemes en la xarxa estan segregats. |
| A.11.4.6 Control de la connexió a la xarxa | Comprovar si s'estableix un control i registre sobre les connexions de cada usuari en la xarxa. |
| A.11.4.7 Control d'encaminament de xarxa | Comprovar si s'estableix un control i seguiment sobre les rutes que existeixen entre els diferents recursos. |
| A.11.5 Control d'accés al sistema operatiu<br>Previndre l'accés no autoritzat als sistemes operatius | |
| A.11.5.1 Procediments segurs d'inici de sessió | Comprovar si els accessos als sistemes operatius es controlen i son segurs. |
| A.11.5.2 Identificació i autenticació d'usuari | Comprovar si cada usuari te un identificador propi |

| | |
|---|---|
| | que li serveixi per autenticar-se en els diferents sistemes. |
| A.11.5.3 Sistema de gestió de contrasenyes | Comprovar si els sistemes de gestió de contrasenyes son segurs i robustos. |
| A.11.5.4 Ús dels recursos del sistema | Comprovar si es controla l'accés a certes aplicacions o programes que puguin invalidar la seguretat dels recursos. |
| A.11.5.5 Desconnexió automàtica de sessió | Comprovar si les sessions inactives durant un període indefinit es tanquen soles. |
| A.11.5.6 Limitació de temps de connexió | Comprovar si s'estableix per certes aplicacions crítiques la limitació d'ús de temps. |
| A.11.6 Control d'accés a les aplicacions i a la informació<br>Prevenir l'accés no autoritzat a la informació que contenen les aplicacions | |
| A.11.6.1 Restricció d'accés a la informació | Comprovar si s'estableix un control per restringir l'accés a la informació de certes aplicacions. |
| A.11.6.2 Aïllament de sistemes sensibles | Comprovar si els entorns sensibles estan aïllats i tenen accés restringit. |

## 2.4. GESTIÓ DE LA CONTINUÏTAT

| CONTROLS | PROVES |
|---|---|
| A.14 Gestió de la continuïtat | |
| A.14.1 Aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci | |
| A.14.1.1 Seguretat de la informació en el procés de la gestió de la continuïtat del negoci | Comprovar si la organització ha creat un pla de continuïtat del negoci. |
| A.14.1.2 Continuïtat del negoci i avaluació de riscos | Comprovar si s'avaluen els possibles esdeveniments que provoquen interrupcions en els processos de negoci. |
| A.14.1.3 Desenvolupament e implementació de plans de continuïtat | Comprovar si la organització ha desenvolupat un pla per la restauració i disponibilitat dels processos del negoci. |
| A.14.1.4 Marc de referència per a la planificació de la continuïtat del negoci | Comprovar si la organització estableix un procediment de referencia per a la continuïtat del negoci. |
| A.14.1.5 Proves, manteniment i reavaluació dels plans de continuïtat del negoci | Comprovar si els plans de continuïtat es proven i s'actualitzen regularment. |

## 2.5. ENGINYERIA SOCIAL

L'enginyeria social és una tècnica que pot ser utilitzada per aconseguir informació de caràcter confidencial d'una organització, es basa principalment en aprofitar-se de la bona voluntat de les persones i el desconeixement en els temes de seguretat informàtica. Una persona malintencionada que utilitzi aquesta tècnica podria obtindre tot tipus d'informació d'una empresa, l'atac consisteix en fer-se passar per algú de confiança per aconseguir la informació que es persegueix i amb aquesta, l'atacant podria comprometre fins i tot, la seguretat total del sistema. Les eines de comunicació utilitzades per realitzar la explotació poden ser diverses, presencial, telefònicament, correu electrònic, sms, etc. Es important comentar que el hacker **Kevin Mitnick** (considerat el hacker més famós del món degut a la quantitat de delictes informàtics que va realitzar en la seva època utilitzant aquest mètode), reconeix que la seguretat més dèbil és la persona humana i que les empreses han de proporcionar recursos per conscienciar a les persones sobre aquests tipus d'atacs i les conseqüències que poden tindre dintre d'una organització. Degut a la gravetat d'aquest tipus d'atac, l'utilitzarem en aquest projecte per auditar al personal de gestió de la universitat, farem un atac telefònic i un altre mitjançant correu electrònic per obtindre les seves credencials del correu electrònic corporatiu, per dur-ho a terme ens farem passar per un responsable de la empresa de hosting que gestiona els correus electrònics.

### 2.5.1. ATAC MITJANÇANT COMUNICACIÓ TELEFÒNICA

Per dur a terme l'atac, hem redactat en un foli en blanc la nostra conversa i la hem utilitzat per mantindre una conversació amb el personal de gestió de la universitat. Per tindre major credibilitat, la redacció ha respòs les següents preguntes:

| | |
|---|---|
| Qui Som ? | Marc Llauradó, responsable del servei hosting del correu electrònic *Dynamo Hosting* |
| Perquè contactem ? | Per fer una millora al vostre perfil de correu electrònic |
| Quin cost te ? | Totalment gratuït |
| Quines millores proporciona ? | Servei d'intel·ligència artificial amb autoaprenentatge per facilitar les tasques diàries mitjançant recordatoris de veu |
| Que necessitem ? | El vostre usuari i la contrasenya d'accés al correu |
| Quan tardara la actualització ? | Un parell de dies |
| Com ens acomiadem ? | Gràcies per confiar amb nosaltres, estem aquí a la vostra disposició |

A continuació podem veure la redacció que hem utilitzat per realitzar aquest tipus d'atac.

*Hola bon dia, sóc Marc Llauradó, responsable del servei hosting Dynamo Hosting i per tant de gestionar els correus electrònics corporatius de la vostra organització, contacto amb vostè per oferir-li la possibilitat de fer una millora totalment gratuïta al vostre perfil d'usuari, la millora consisteix en introduir capacitats d'intel·ligència artificial amb autoaprenentatge per facilitar les tasques diàries mitjançant notificacions textuals i de veu, aquesta actualització només tardaria un parell de dies i ho recomano a tots els meus clients perquè els resultats han sigut totalment satisfactoris, si està d'acord només m'ha de proporcionar el compte d'usuari i la contrasenya, Gràcies per confiar amb nosaltres, estem aquí a la vostra disposició.*

L'atac l'hem realitzat sobre quatre persones diferents de l'organització, les dues persones de secretaria Àngels Huguet i Teresa Puigdomenech, la responsable de contabilitat Anna Civic i la responsable d'administració Gloria Canals.

| EMPLEAT | DIA I HORA | RESPOSTA DE L'ATAC |
|---|---|---|
| Àngels Huguet | 11/11/2019 10:00h | Ho sento molt Marc, però ara mateix tinc pressa si vol pot trucar en un altre moment |
| Teresa Puigdomenech | 12/11/2019 10:00h | Gràcies per la informació Marc, però actualment no necessito aquesta actualització, pot ser en un altre moment |
| Anna Civic | 13/11/2019 10:00h | Gràcies Marc, en un principi no necessito més recordatoris, actualment utilitzo altre eines de notificació, encarà així podries enviar-m'ho per correu electrònic |
| Gloria Canals | 14/11/2019 10:00h | Gràcies Marc, però per poder fer aquesta actualització primer ho hauria de comentar amb el personal informàtic |

Com podem veure les respostes han sigut adequades i no s'ha pogut explotar l'atac, però hem insistit mitjançant correu electrònic sobre les empleades Àngels Huguet i Anna Civic degut a les seves respostes.

### 2.5.2. ATAC MITJANÇANT CORREU ELECTRÒNIC

De forma similar al apartat anterior, hem realitzat el mateix tipus d'atac però una mica modificat per proporcionar més confiança, hem utilitzat el correu electrònic com a mitjà de comunicació i hem clonat la pàgina web d'identificació del usuari del correu electrònic mitjançant la eina SET. Per dur a terme aquest tipus d'atac hem utilitzat un servidor de correu propi i hem falsificat la direcció d'origen (defecte d'implementació de protocol SMTP sense mecanismes de protecció) mitjançant l'adreça mllaurado@dynamohosting.com. A continuació podem veure la redacció que hem utilitzat per realitzar aquest tipus d'atac.

*Hola bon dia, sóc Marc Llauradó, responsable del servei hosting Dynamo Hosting i per tant de gestionar els correus electrònics corporatius de la vostra organització,* ***com ja he comentat telefònicament****, contacto amb vostè per oferir-li la possibilitat de fer una millora totalment gratuïta al vostre perfil d'usuari, la millora consisteix en introduir capacitats d'intel·ligència artificial amb autoaprenentatge per facilitar les tasques diàries mitjançant notificacions textuals i de veu, aquesta actualització només tardaria un parell de dies i ho recomano a tots els meus clients perquè els resultats han sigut totalment satisfactoris, si està d'acord només* ***ha de validar-se al seu correu electrònic mitjançant l'enllaç:***

*http://www.dynamohosting.dhmodules.com*

*Gràcies per confiar amb nosaltres, estem aquí a la vostra disposició.*

Com podem veure anteriorment, s'utilitza el domini dhmodules.com amb subdomini dynamohosting per enganyar a la víctima de que la direcció URL es confiable. La pàgina web clonada permet emmagatzemar la informació d'usuari i contrasenya i un cop introduïda aquesta informació reenviar al usuari cap a la pàgina web original. L'atac l'hem realitzat sobre les empleades Àngels Huguet i Anna Civic.

| EMPLEAT | DIA I HORA | RESPOSTA DE L'ATAC |
|---|---|---|
| Àngels Huguet | 15/11/2019 10:00h | Ha introduït l'usuari ahuguet@edcp.uoc.edu i contrasenya ahuguet071272 |
| Anna Civic | 15/11/2019 10:00h | Sense resposta |

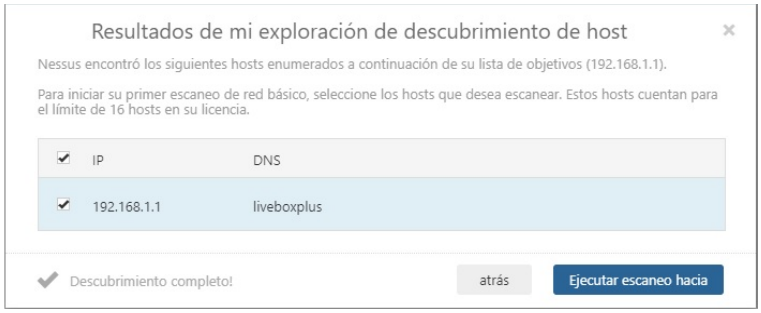
Com podem veure la empleada Àngels Huguet ha accedit a introduir la informació del seu compte d'usuari i aquesta ha sigut emmagatzemada al servidor del atacant. Hem de pensar que tindre el control d'un perfil de correu electrònic corporatiu és molt perillós per la quantitat d'informació de caràcter confidencial que pot ser interceptada i per la possibilitat d'utilitzar aquest compte de correu electrònic per enganyar a altres persones de dintre de l'organització. Resumint, el resultat d'aquesta auditoria ens indica que l'organització ha de proporcionar mecanismes per conscienciar als seus empleats sobre aquests tipus d'atacs, explicar com es poden identificar i com s'ha d'actuar davant d'una amenaça d'aquest estil.

## 3. EXPLORACIÓ DE VULNERABILITATS AMB NESSUS

*Nessus* és un escàner remot de vulnerabilitats que permet identificar tots els serveis proporcionats per una màquina remota i determinar si aquests estan protegits sobre tots els exploits coneguts. Segons la pàgina oficial de Nessus, es a dir, http://www.nessus.org, aquest és l'escàner de vulnerabilitats més popular del món que és utilitzat en més de 75.000 organitzacions d'arreu del món.

He realitzat una exploració de vulnerabilitats sobre el meu router livebox, amb direcció IPv4 192.168.1.1, per dur-ho a terme he fet ús de l'escàner de vulnerabilitats Nessus, concretament la última versió estable 8.8.0.


Un cop iniciat Nessus, he introduït la direcció IPv4 del router i he començat el escaneig.


| Severity | CVSS | Plugin | Name |
|---|---|---|---|
| MEDIUM | 6.4 | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 5.8 | 50686 | IP Forwarding Enabled |
| MEDIUM | 5.0 | 12217 | DNS Server Cache Snooping Remote Information Disclosure |
| MEDIUM | 5.0 | 57608 | SMB Signing not required |
| MEDIUM | 5.0 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| LOW | 3.3 | 10663 | DHCP Server Detection |
| INFO | N/A | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | 45590 | Common Platform Enumeration (CPE) |

Nessus ha trobat 37 vulnerabilitats, de les quals cinc són de gravetat mitjana, farem referencia a elles degut a la seva importància.

| VULNERABILITATS | DESCRIPCIÓ |
|---|---|
| 51192 - SSL Certificate Cannot Be Trusted | No es pot confiar amb el certificat x.509 del servidor. Això pot succeir principalment a que la cadena de certificats enviada pel servidor podrien no descendir d'una autoritat púbica de confiança o bé contenen un certificat no vàlid. |
| 50686 - IP Forwarding Enabled | El host remot te habilitat el reenviament IP, un atacant podria explotar això per enrutar paquets mitjançant aquest host i potencialment ometre alguns firewalls, enrutadors, etc. Degut a que el dispositiu escanejat és un enrutador, farem cas omís d'aquesta vulnerabilitat. |
| 12217 - DNS Server Cache Snooping Remote Information Disclosure | El servidor DNS remot és vulnerable a atacs de cache, aquest respon a les consultes dels dominis de tercers que no tenen establert el bit de recursivitat, això pot permetre que un atacant remot determini quins dominis s'han resolt recentment. |
| 57608 - SMB Signing not required | No es necessari firmar en el servidor SMB remot. Un atacant remot no autenticat podria explotar això per realitzar atacs man-in-the-middle contra el servidor SMB. |
| SSL Medium Strength Cipher Suites Supported (SWEET32) | El host remot admet l'ús de xifratge SSL amb xifratge de força mitjana (longitud de claus de 64 bits a 112 bits o enc. 3DES). |

## 4. OPINIÓ PERSONAL

He de reconèixer que ser coordinador és una tasca complicada, has de programar les reunions, vetllar per l'assoliment de les tasques, ser flexible per fer front les possibles situacions inesperades, unificar la informació, però també haig de dir que els membres d'aquest grup fan que tot això sigui fàcilment assumible, assistint a les hores indicades a les reunions, permetent la comunicació en qualsevol moment del dia i aportant cada un d'ells els seus coneixements per facilitar el desenvolupament de les tasques. La enginyeria social és un atac molt perillós per les organitzacions degut a que s'aprofita de la bona voluntat de la persona humana i els desconeixements d'aquest en temes de seguretat, per tant, les organitzacions han de posar mitjans per conscienciar als seus treballadors de la existència d'aquest i les conseqüències que en poden derivar, personalment, crec que cada cop més les organitzacions són més conscients i la efectivitat d'aquests atacs s'han vist reduïts al llarg del temps. En referencia a la tasca d'exploració de vulnerabilitats, haig de dir que les eines actuals han millorat considerablement durant el pas dels anys i cada cop son molt més professionals, el fet d'utilitzar la arquitectura client-servidor fan que aquestes aplicacions puguin estar centralitzades en una organització i que siguin interoperables entre diferents arquitectures. Personalment l'aplicació Nessus m'ha sorprès gratament per la quantitat d'informació que maneja (més de 75.000 plugins), per l'arquitectura que utilitza, segmentant clarament la part del client i la del servidor, per la qualitat dels informes d'exploració de vulnerabilitats amb una explicació de la causa de la vulnerabilitat, les possibles solucions a efectuar per evitar la seva existència i les referencies relacionades, tot això fa que l'aplicació sigui un referent a seguir dintre del seu àmbit. També haig de dir que he tingut que utilitzar una màquina amb millors prestacions per poder instal·lar Nessus, la instal·lació és molt senzilla però es necessita bastanta capacitat de disc dur i de processament per agilitzar el temps d'espera.

## 5. FONTS D'INFORMACIÓ

### Recursos

*Fitxer PDF auditories i test de penetració del Webinar número 8*

*Grabació del Webinar número 8 realitzat el 07/11/2019 per Antoni Martínez, professor del curs Tècnic en Ciberseguretat PQTM 19.*

### Escenari

*Descripció de l'escenari per fer auditories*

Projecte 1

### Auditories

*Informació sobre auditories relacionades amb la informàtica*

https://www.academia.edu/31621729/APUNTES_DE_AUDITORÍA_INFORMÁTICA

### Nessus

*Pàgina oficial - Informació genèrica de l'eina.*

http://www.nessus.org

*Informació detallada de l'eina Nessus.*

https://es.scribd.com/document/386071484/Nessus-pdf

*Web de Tenable on podem trobar els requisits de Hardware, de Software, llicenciament, etc.*

https://docs.tenable.com/nessus/Content/GettingStarted.htm

*Pàgina web de Tenable sobre el procés d'instal·lació del Nessus en entorn Windows:*

https://docs.tenable.com/nessus/Content/InstallNessusWindows.htm