DEFINICIÓ E IMPLEMENTACIÓ D'UN SISTEMA PER A LA PROTECCIÓ DE COMPTES D'USUARI PRIVILEGIATS

Marc Domínguez Florido

Resum— En aquest projecte dissenyarem un sistema PAM ("Privileged Account Management"), el qual ajuda a les organitzacions a gestionar i securitzar comptes privilegiades analitzant els seus requeriments tant tècnics com funcionals i implementant regles i controls.

La implementació d'aquest sistema PAM comporta determinar quina és la combinació de tècniques òptima per securitzar les dades i a continuació s'introduirà a la infraestructura interna de l'empresa Omega Peripherals, per tal d'analitzar el seu funcionament en un sistema real. També aprofitarem aquesta implementació per controlar l'accés a recursos i informació confidencial dels seus clients de manera externa, adaptant el sistema PAM segons convingui.

Paraules clau— Protecció d'infraestructura, Mecanismes de protecció, Seguretat, Autenticació, Identificació de la configuració, Procés de gestió de la configuració

Abstract— In this project we will design a PAM ("Privileged Account Management") system, which helps organizations to manage and secure privileged accounts by analyzing their technical and functional requirements and implementing rules and controls.

The implementation of this PAM system involves determining the optimal combination of techniques to secure the data and then it will be introduced to the internal infrastructure of the company Omega Peripherals, in order to analyze how it works in a real system. We will also take advantage of this implementation to control the access to resources and confidential information of their clients externally, adapting the PAM system as needed.

Index Terms— Infrastructure protection, Protection mechanisms, Security, Authentication, Configuration identification, Configuration management process

1 Introducció - Context del treball

A mesura que el nombre de comptes privilegiats ha anat creixent a les organitzacions en els darrers anys, els cibercriminals s'han adonat que son una ruta fàcil cap a aquestes organitzacions si podien aconseguir les credencials, i, malauradament, moltes organitzacions faciliten als pirates informàtics trobar credencials amb mètodes d'emmagatzematge no encriptats, insegurs i eines de gestió de contrasenyes deficients, o cap [1].

En l'última dècada, s'han produït múltiples bretxes de seguretat relacionades amb l'abús de l'accés amb privilegis. Des Terry Childs i Edward Snowden fins Yahoo! i la filtració massiva de l'Oficina d'Administració de Personal d'EE. UU., passant per la bretxa del Banc de Bangla Desh, l'atac a la xarxa elèctrica d'Ucraïna i fins i tot la molt difosa filtració de Uber: el denominador comú de cada atac va ser que les credencials amb privilegis van ser explotades i utilitzades per planificar, coordinar i executar ciberatacs. [2]

Molts atacs tenen èxit perquè l'organització no disposa de cap protecció aplicada als comptes privilegiats ni als controls d'accés, i els usuaris han de gestionar els seus propis comptes amb tots els perills que això comporta. Malauradament, molts usuaris de Tecnologies de la Informació no tenen una comprensió completa del funcionament dels comptes privilegiats, així com dels riscos associats al seu compromís i ús indegut. Això fa que ells i les seves organitzacions siguin molt més vulnerables als possibles danys monetaris i reputacionals derivats de les creixents amenaces. [3]

Recentment, s'ha produït un atac a gran escala al servei informàtic de la Universitat Autònoma de Barcelona, en el que segurament els atacants hagin accedit per la falta d'implementació de gestió de comptes privilegiades (PAM) al centre. Mitjançant aquest treball també podrem analitzar i comprendre més en detall aquest cas concret que ens afecta a tots els estudiants i aprendre com es po-

dria haver evitat la incidència.

L'organització de la resta del document és la següent: a la secció dos es recullen els objectius; a la secció tres l'estat de l'art; a la secció quatre la metodologia utilitzada al llarg del desenvolupament del projecte; a la secció cinc s'informa del detall de l'abast; a la secció sis es mostra el treball particular, on es detalla el disseny i implementació de cada un dels casos d'ús establerts a l'inici del projecte; a la secció set s'avaluen els resultats; i a la secció vuit les conclusions; per finalitzar amb els agraïments i la bibliografia emprada.

2 OBJECTIUS

L'objectiu d'aquest projecte és dissenyar un sistema PAM ("Privileged Account Management"), el qual ajuda a les organitzacions a gestionar i securitzar comptes privilegiats analitzant els seus requeriments tant tècnics com funcionals i implementant regles i controls com automatitzar el seu descobriment, emmagatzemar les seves contrasenyes en un repositori segur, rotar automàticament les contrasenyes després de cada ús, monitoritzar i reportar en funció de la seva activitat, etc. Aquest sistema PAM s'introduirà a la infraestructura interna de l'empresa Omega Peripherals, per tal d'analitzar el seu funcionament en un sistema real.

Per poder dissenyar un sistema PAM correctament, cal que sigui capaç d'abordar els principals reptes de la gestió d'accés amb privilegis [2]:

- Gestionar els comptes amb privilegis: No dependre de processos administratius manuals exhaustius i propensos a errors per rotar i actualitzar les credencials amb privilegis.
- Supervisar l'activitat amb privilegis: Supervisar i controlar de forma centralitzada les sessions amb privilegis.
- Monitoritzar i analitzar les amenaces: Fer servir eines exhaustives d'anàlisi d'amenaces i poder identificar de manera proactiva les activitats sospitoses i remeiar els incidents de seguretat.
- Controlar l'accés d'usuaris privilegiats: Evitar l'accés dels usuaris amb privilegis a les plataformes al núvol, les aplicacions de programari com a servei (SaaS), les xarxes socials, etc., degut a que creen riscos de compliment i complexitat operativa.

Aquest sistema PAM es basa en el principi del mínim privilegi, a partir del qual els usuaris només reben els nivells mínims d'accés necessaris per exercir les seves funcions laborals, això evita possibles accions no permeses i assegura les dades confidencials. En general, el principi del mínim privilegi es considera una pràctica òptima de ciberseguretat i és un pas fonamental per protegir l'accés amb privilegis a dades i actius de gran valor. A l'aplicar el principi del mínim privilegi, les organitzacions poden reduir la superfície d'atac i mitigar el risc d'usuaris interns malintencionats o de ciberatacs externs que poden ocasionar costoses filtracions de dades.

Mitjançant aquest sistema PAM, serem capaços d'evitar incompliments de seguretat i proporcionar accés ràpid a aquells que ho necessitin quan ho necessitin eliminant l'amenaça d'accés no autoritzat degut a l'augment de l'accés a les dades i als recursos crítics. [2]

3 ESTAT DE L'ART

Efectuant una simple exploració de mercat, podem trobar diferents gestors de comptes privilegiats, els quals s'identifiquen en funció de dos criteris:

- Ability to Execute: Avalua l'eina en funció de característiques que ofereix el producte, com la seva viabilitat o la experiència d'usuari.
- Completeness of Vision: Avalua l'eina en funció de les seves estratègies de ventes, marketing i oferta.

Les eines més encertades segons aquests criteris són CyberArk, One Identity i Thycotic, en ordre de classificació.

A més d'aquesta comparativa inicial, l'empresa Omega recomana fer servir l'eina One Identity, des d'un punt de vista estratègic, degut a les següents raons:

- Omega disposa d'un acord de col·laboració més estret amb One Identity.
- Facilita la integració al sistema degut a l'estructura interna de l'empresa.
- El cost de desplegament és més reduït degut a l'acord de col·laboració esmentat, el qual proporciona llicències gratuites.

En base a aquesta aportació per part de l'empresa, hem decidir seleccionar One Identity com l'eina que farem servir per implementar el nostre sistema PAM durant la següent fase del nostre projecte de fi de grau, ja que forma part de les més rellevants, compleix tots el requeriments i és la opció preferent de l'empresa on implemen-

- *E-mail de contacte: marcdom3@gmail.com*
- *Menció realitzada: Tecnologies de la Informació*
- *Treball tutoritzat per: Juan Antonio Martínez (Departament d'Enginyeria de la Informació i de les Comunicacions)*
- *Curs 2021/22*

tarem el sistema, Omega Peripherals.

4 METODOLOGIA

Per aconseguir els objectius, es seguirà una metodologia fonamentada en el Gannt de seguiment, i suportada per Jira com a eina, degut a que és la que acostumen a fer servir a l'empresa Omega Peripherals i considerem que és la més adequada per comprendre el seu funcionament i adaptar-se a la seva manera de realitzar les tasques.

Aquesta metodologia consisteix en vàries fases:

- Anàlisi, per tal de determinar com enfocar el problema i quins punts concrets volem millorar;
- planificació i selecció de solucions;
- plantejament de l'arquitectura, considerant tot el programari i llenguatge recomanat per l'empresa;
- implementació de les tècniques escollides, seguint una organització clara i un bon estil de codificació;
- configuració del sistema, vetllant pel sincronisme entre sistema i tècniques escollides;
- proves, per tal de comprovar la correcta implementació i corregir errors i inconsistències detectades;
- i possibles cicles de millora, amb la possibilitat de controlar les versions i millorar la funcionalitat global del sistema.

5 DETALL DE L'ABAST

Omega, és una empresa integradora de solucions tecnològiques especialitzada en serveis avançats associats a les noves Tecnologies de la Informació. Des de 1993 ha promogut la cooperació amb els seus clients a través de la innovació en processos, mitjans i tecnologies contribuint al canvi, la productivitat i la competitivitat en els negocis.

Un cop definits tots els mètodes que es puguin desenvolupar per millorar la seguretat dels comptes, es determinarà quina és la combinació de tècniques òptima per securitzar les dades i s'implementarà a la infraestructura interna de l'empresa Omega Peripherals, per tal d'analitzar el seu funcionament en un sistema real, millorar la protecció de la seva infraestructura i aplicacions i mantenir la confidencialitat de les dades sensibles.

La realització d'aquest projecte comporta la configuració bàsica d'un sistema PAM, el qual serà adoptat per l'empresa en un futur proper amb la intenció d'aprofundir en algunes funcionalitats i afegir complexitat a la estructura.

6 TREBALL PARTICULAR

6.1 Disseny del sistema PAM

L'eina seleccionada per a la implementació del nostre sistema PAM, One Identity Safeguard, consta dels següents components:

- Safeguard for Privileged Passwords (SPP) automatitza, controla i assegura el procés de concessió de credencials privilegiades amb administració d'accés basada en rols i fluxos de treball automatitzats.
- Safeguard for Privileged Sessions (SPS) permet controlar, monitoritzar i gravar sessions amb privilegis d'administradors, proveïdors remots i altres usuaris d'alt risc.

Ambdós components poden ser desplegats en format d'appliance físic o bé en format d'appliance virtual desplegable mitjançant imatge OVA. En el nostre cas, hem optat per aquesta segona opció perquè ofereix més versatilitat a un cost més reduït.

En el nostre cas, farem servir dues màquines virtuals, una destinada a la gestió de contrasenyes (SPP) i una altra destinada a la gestió de sessions (SPS).

6.2 Desenvolupament

Seguidament, detallem l'aplicació i resolució de cada un dels vuit casos d'ús establerts a l'inici del projecte i corresponents als requeriments funcionals que ha de complir el nostre sistema.

Per tal de disposar de diferents actius per la seva configuració, Omega Peripherals ens proporciona tres màquines virtuals, corresponents a una màquina client Windows, una màquina client Linux, i una altra màquina Windows amb Active Directory (AD) integrat per a la definició d'usuaris i emmagatzemament de credencials. Aquestes tres màquines formen part de les particions de Windows Server, Linux Server i Directory respectivament.

6.2.1 Donar d'alta un sistema

El funcionament d'aquest cas d'ús representa la creació d'actius en el sistema i la creació de comptes, inclòs el necessari per vincular l'actiu destí amb Safeguard per permetre el descobriment de comptes.

Primer de tot, cal afegir els actius que disposem a Safeguard per la seva posterior configuració, indicant a quina partició correspon cadascun.

A continuació, a cada màquina client i a la màquina AD creem dos comptes d'administrador, els quals disposen de tots els permisos del sistema i serviran per accedir remotament al sistema mitjançant petició de sessió; tres

comptes d'usuari bàsics; un compte de servei genèric, que formarà part d'un nou grup d'usuaris anomenat *ServiceAccounts* i el qual només podrà sol·licitar descobriment de la contrasenya; i un compte de vinculació, necessari per establir i comprovar la connexió entre les màquines virtuals i Safeguard. [4] [5]

A més, per a les màquines Windows, també configurem el Firewall del sistema per permetre tres regles entrants predefinides necessaries, canviem la política de seguretat local per evitar permisos conflictius que puguin afectar al nostre sistema dins dels nostres clients i habilitem la connexió remota per RDP. [6]

Per tal de facilitar la selecció d'actius a l'hora d'establir polítiques de sol·licitud d'accés, afegim les màquines Windows a un nou grup d'actius anomenat *Windows RDP* i, de la mateixa manera, afegim la màquina Linux a un altre nou grup d'actius anomenat *Linux SSH*, de manera que els actius que pertanyin a aquests grups podran ser accedits per connexió remota.

Posteriorment afegim els tres actius de les tres corresponents particions a Safeguard, especificant les IPs de cada màquina virtual i establint connexió amb el compte de vinculació creat anteriorment.

6.2.2 Afegir un compte privilegiat

La integritat dels comptes és molt important en aquest sistema i una manera d'identificar els comptes propis de cada actiu de manera senzilla és fent servir una política de detecció de comptes; la qual serà la mateixa pels tres actius, s'executarà diàriament i comptarà amb dues regles de detecció, una per detectar els comptes d'administrador i una altra per detecter les comptes de servei. [7]

Aquestes regles tenen una restricció de propietat per grup, és a dir, cadascuna busca els usuaris en un grup d'usuaris especificat i definit dins del directori de cada màquina, sent *Administrators* i *ServiceAccounts* aquests dos grups.

A diferència de la resta, la partició de Directory permet filtrar la cerca especificant la ubicació concreta dins del directory i seleccionant el grup d'usuaris directament.

Un cop finalitzada la configuració de la política, podem iniciar el procés de detecció de comptes i recuperarles al perfil de contrasenyes de cada partició corresponent.

6.2.3 Accés a la infraestructura local

Aquest cas d'ús es centra en una de les implementacions que conformen el detall de l'abast del projecte, la qual tracta la gestió de comptes de la infraestructura interna de l'empresa Omega Peripherals.

Una vegada l'usuari inicia sessió i s'identifica correctament, pot seleccionar la màquina client a la que vol accedir per sessió. Aquesta connexió podrà ser per SSH si la màquina seleccionada és Linux o per RDP si la màquina seleccionada és Windows. Una vegada indiqui el temps que vol estar fent servint la màquina i especifiqui el motiu de l'ús, el sistema iniciarà la connexió a la màquina remotament i de manera transparent fent servir el compte d'administrador vinculat a l'usuari, és a dir, sense la necessitat de demanar credencials ni que en cap moment l'usuari les conegui.

Una altra opció que pot escollir l'usuari és el descobriment de contrasenya del compte de servei d'una de les màquines, de tal manera que, una vegada s'introdueixi la durada i el motiu, el sistema proporcionarà una clau temporal per poder realitzar una connexió remota. Aquesta opció, però, necessita d'una aprovació per part d'un usuari aprovador, el qual té la possibilitat de permetre o no l'accés a l'usari.

Amb qualsevol d'aquestes opcions, l'usuari pot aconseguir accedir de manera remota i transparent a la infraestructura interna de l'empresa Omega Peripherals.

6.2.4 Accés a sistemes de clients externs

Aquest cas d'ús es centra en l'altra implementació que conforma el detall de l'abast del projecte, la qual tracta el control de l'accés a recursos dels clients de manera externa de l'empresa Omega Peripherals.

De manera implícita a les polítiques de connexió RDP i SSH establertes a Safeguard i que es detallen al cas d'ús *Iniciar una sessió privilegiada*, qualsevol rang d'IPs es podrà connectar al servidor de Safeguard, ja que la connexió es realitza de manera transparent.

La connexió amb els clients és una VPN to VPN contínua, on un router enruta al servidor quan l'usuari vol accedir al sistema.

A mode de millora de cara al futur, seria més segur i òptim establir un rang determinat d'IPs per permetre l'accés al servidor, però de moment, per la correcta funcionalitat definida del nostre sistema és més que suficient aquesta configuració.

6.2.5 Accés a comptes compartits

Aquest cas d'ús tracta l'accés als comptes únics que poden ser utilitzats per qualsevol membre de l'empresa autoritzat, com podrien ser comptes per comunicar-se amb els proveïdors, comptes de xarxes socials, etc.

En el nostre cas i de manera similar a com creem actius al primer cas d'ús, crearem un compte de xarxa social a Facebook dins d'un actiu diferent i concret per aquest tipus de comptes.

En aquest cas i de la mateixa manera que sol·licitem el

descobriment de les contrasenyes dels comptes de serveis genèrics, aquestes comptes compartides només poden sol·licitar l'accés mitjançant descobriment de contrasenya i necessiten l'aprovació d'un usuari autoritzat per poder accedir a l'actiu desitjat. [8]

A diferència de les comptes de serveis, però, aquestes comptes permeten l'accés simultani de fins a cinc usuaris de l'empresa.

6.2.6 Autenticació amb contrasenya

Aquest cas d'ús tracta la identificació dels diferents tipus d'usuari que poden accedir al sistema, els quals es classifiquen en si fan servir un compte local o un compte d'Active Directory.

Per una banda, si volem accedir amb un compte local, primer hem de crear un usuari local de Safeguard i assignar-li tots els permisos disponibles per tenir accés a tots els recursos. [9]

Per una altra banda, si volem accedir amb un compte d'Active Directory, primer afegim un nou proveïdor d'identitat de tipus Active Directory per vincular amb l'actiu corresponent a la partició Directory. Comprovem la connexió amb el compte de vinculació i acceptem. A continuació, creem un nou usuari seleccionant el nou proveïdor d'identitat i assignem només permisos d'Auditor (només lectura). Per l'accés al sistema amb comptes d'Active Directory, afegim autenticació de dos factors, funcionalitat que actualment es troba en desenvolupament.

En qualsevol dels dos casos, afegim el nou usuari al grup d'usuaris anomenat *Requesters*, per tal de que pugui fer sol·licituds d'accés per sessió o per contrasenya; i vinculem el compte local amb un dels comptes d'administrador descoberts perquè es redirigeixi al compte amb privilegis a l'iniciar una connexió remota.

6.2.7 Iniciar una sessió privilegiada

Cada actiu pot disposar d'una o més polítiques de sol·licitud d'accés, les quals han de complir una sèrie de característiques. Cada política estarà vinculada a una assignació, que són un conjunt de normes que controlen les peticions d'accés per sessió o per descobriment de contrasenya. [10]

Sabent això, creem una nova assignació anomenada *Session Requests*, la qual restringeix l'accés del sistema als usuaris autoritzats, en el nostre cas al grup d'usuaris *Requesters* i requereix un motiu de sol·licitud d'accés, que pot ser *Petició de sessió SSH, Petició de sessió RDP* o *Petició de contrasenya.* [11]

També ens interessa crear grups d'actius per determinar el tipus de connexió permès per cada actiu. Creem dos grups d'actius, un per poder determinar a quines màquines Windows es podrà accedir per connexió RDP, i un altre que identifica les màquines Linux que permeten la connexió SSH.

L'accés a aquests dos grups d'actius es gestiona amb les polítiques de sol·licitud de sessions per RDP i SSH respectivament, a les quals no establim aprovacions ni revisions de la sol·licitud, de manera que qualsevol usuari autoritzat pot sol·licitar de manera immediata una connexió remota. Durant el procés de sol·licitud, l'usuari ha d'especificar un motiu d'accés i pot seleccionar fins a set dies de durada màxima de la connexió. També establim que l'accés es basa en un compte vinculat, el qual cal associa el compte de l'usuari amb el seu corresponent compte d'administrador.

Per tal d'aprofitar les funcionalitats de les eines del nostre sistema PAM, definim una política de connexió de sessió en el component *Safeguard for Privileged Sessions* per enllaçar-la i aprofitar-la en la implementació de les polítiques de sol·licitud de sessions. En aquesta política de connexió, cal especificar el rang de IPs permesa per la connexió, on especifiquem que acceptem totes les IPs sense filtre per simplificar el cas d'ús quatre. També indiquem que és l'usuari qui introdueix la IP destí, de manera que afegim una simple manera d'assegurar que per permetre la connexió l'usuari ha de saber on cal connectar-se.

Seguidament, dins de la política de connexió també associem algunes de les polítiques que ens permet crear Safeguard, com les de *Audit*, *Usermapping* i *Channel.*

Establim la configuració per defecte de les polítiques de *Audit*, que emmagatzema les activitats registrades dels administradors; i *Usermapping,* que descriu qui pot utilitzar un nom d'usuari específic per accedir al servidor remot.

Per últim, creem una simple política de *Channel* per a cada tipus de connexió, la qual ens permet llistar els canals permesos i restringir l'accés a les IPs especificades. També es pot determinar en quines hores del dia està disponible l'accés i si s'habilita la monitorització del canal.

De RDP, permetem l'accés al canal de *Drawing*, dedicat a la interfaç gràfica de l'usuari i al canal de *Clipboard*, el porta-retalls de l'usuari. Ambdós canals no tenen restricció temporal ni de IPs i habiliten la monitorització.

De SSH, només permetem el canal de terminal (*Shell*) sense restricció temporal ni de IPs i habilitant la monitorització.

6.2.8 Revelar contrasenya

Per aquest últim cas d'ús, necessitarem definir tres noves assignacions, corresponents a la sol·licitud de contra-

senya de comptes Linux, Windows i Directory i en els tres casos especifiquem el grup d'usuaris *Requesters* com els usuaris autoritzats per sol·licitar contrasenyes. [10]

De la mateixa manera que en la sol·licitud de sessions, per poder revelar la contrasenya d'un compte, cal crear una nova política de sol·licitud d'accés, enfocada a l'accés per contrasenya. [8]

Creem tres nous grups de comptes, corresponents als comptes que permeten descobriment de contrasenya, un per cada partició i afegirem a cada grup els comptes de servei de cada partició, ja que aquests seran els únics comptes sobre els que podrem sol·licitar el descobriment de contrasenya.

A diferència de la política d'accés per sessions, en aquesta política sí que requerim aprovacions de la sol·licitud per part d'algun membre del grup d'usuaris aprovadors, de manera que qualsevol usuari que sol·liciti l'accés mitjançant contrasenya necessitarà l'aprovació d'almenys un membre d'aquest grup.

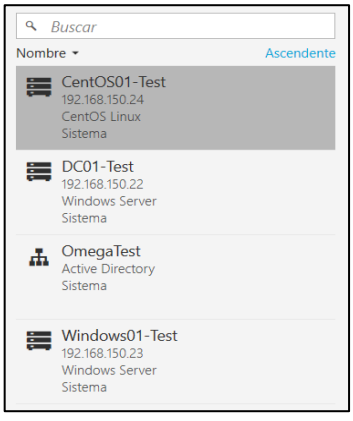
7 RESULTATS

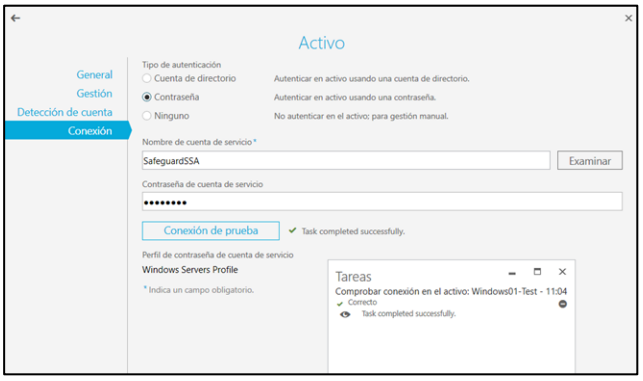
En aquesta secció, documentarem els resultats obtinguts en base a les aplicacions dels casos d'ús realitzats en el nostre projecte. Amb l'objectiu d'evitar redundància, només mostrarem els resultats de la màquina client Windows anomenada *Windows01-Test*, a excepció de la connexió SSH del cas d'ús set, que està destinada a màquines Linux.

7.1 Donar d'alta un sistema

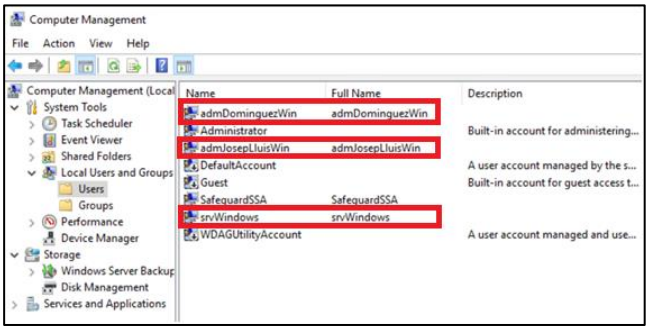
Per aquest primer cas d'ús, cal afegir els quatre actius del nostre sistema: un per cada partició més l'actiu Windows que conté l'Active Directory anomenat *DC01-Test.*

Un cop configurat l'usuari i els seus permisos a l'actiu, és moment de comprovar la connexió des de Safeguard.

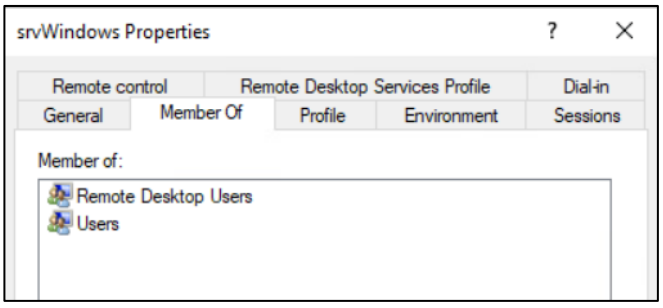




Un cop comprovada la connexió, podem afegir els usuaris que farem servir per la màquina Windows01-Test: un compte de servei i dos comptes d'administrador, de la mateixa manera que hem creat el compte de vinculació.



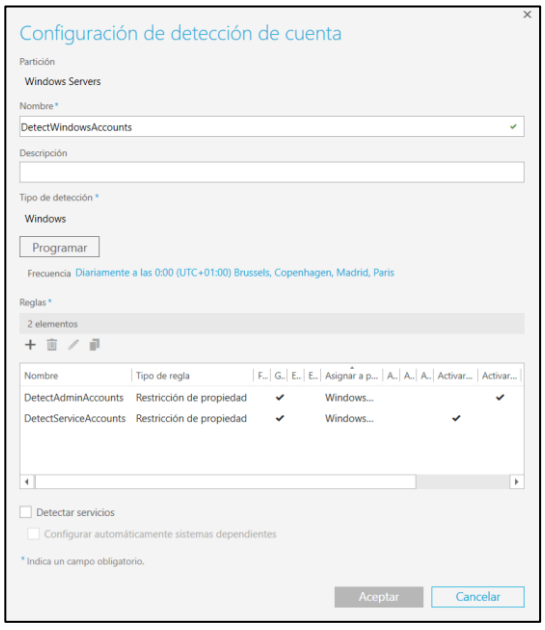
Els usuaris administradors han de pertànyer al grup d'usuaris *Administrators* per disposar de tots els permisos i els comptes de servei han de pertànyer al grup d'usuaris *Remote Desktop Users*, per tal de poder recuperar la contrasenya per connexió RDP.



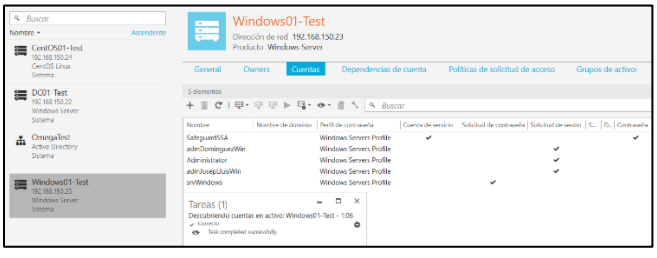
A més, per tal d'afegir seguretat, podem configurar que l'usuari hagi de modificar la contrasenya del compte de servei després de cada correcte login, per tal d'assegurar una major seguretat en el sistema.

7.2 Afegir un compte privilegiat

Primer de tot, definim la política de detecció de comptes amb les dues regles per recuperar els comptes d'administrador i de servei respectivament.



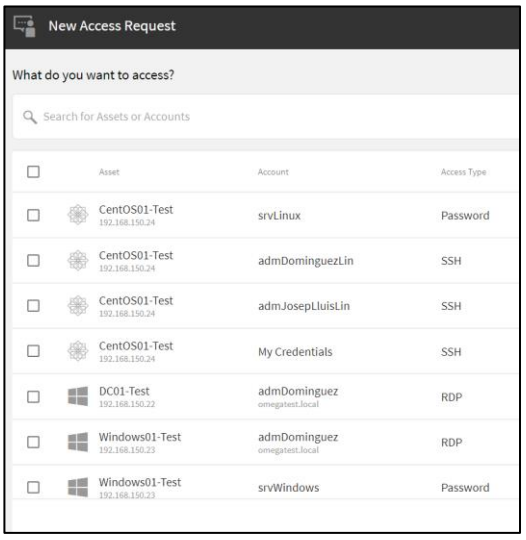
Seguidament, i fent servir les regles mencionades per la detecció de comptes, podem iniciar la pròpia detecció des de *Detectar comptes* un cop fem clic dret a l'actiu *Windows01-Test*.



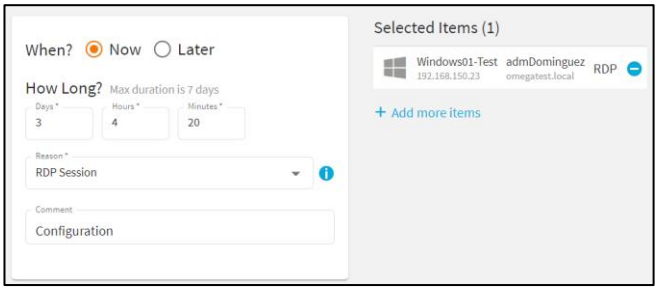
Podem observar que ha recuperat correctament quatre nous comptes, entre els quals trobem els dos comptes d'administrador *admDominguezWin* i *admJosepLluisWin* i el compte de servei *srvWindows*, que eren els comptes que volíem recuperar.

7.3 Accés a la infraestructura local

Una vegada ens identifiquem correctament com usuari, podem sol·licitar accés als diferents actius configurats: connexió RDP pels actius Windows, connexió SSH pels actius SSH, o descobriment de la contrasenya de les comptes de servei.



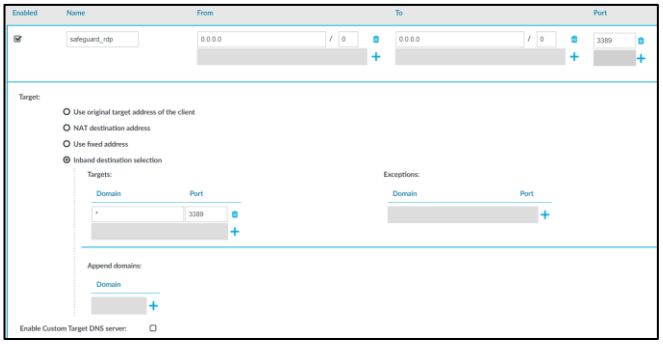
Un cop seleccionat l'actiu, hem d'especificar la duració, el motiu de la connexió i un comentari opcional.



7.4 Accés a sistemes de clients externs

Al tractar aquest cas d'ús de manera implícita a l'haver establert un mètode de selecció de destinació en banda o *inband* durant la configuració del SPS , podem crear una única política de connexió i permetre als usuaris finals accedir a qualsevol servidor, incloent el nom del servidor de destinació al vostre nom d'usuari. [12]

D'aquesta manera, indiquem que el client amb permís d'accés al servidor pot tenir qualsevol IP i que la IP del servidor a la qual es sol·licita l'accés també pot ser qualsevol introduint 0.0.0.0 en els dos casos.



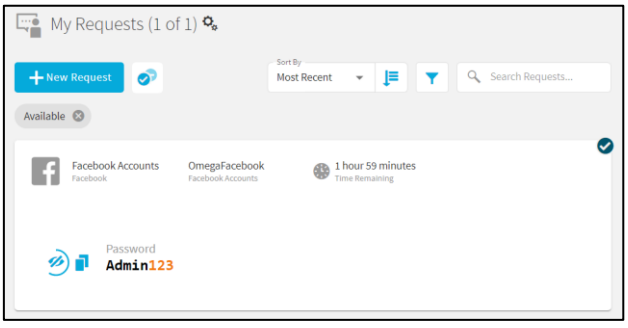
En altres paraules, facilitem la implementació d'aquest cas d'ús, ja que no tenim en compte la IP origen i permetem l'accés a qualsevol client. Tot i això, s'origina un des-

avantatge de seguretat, de manera que de cara a futures millores caldrà limitar l'accés als clients autoritzats.

7.5 Accés a comptes compartits

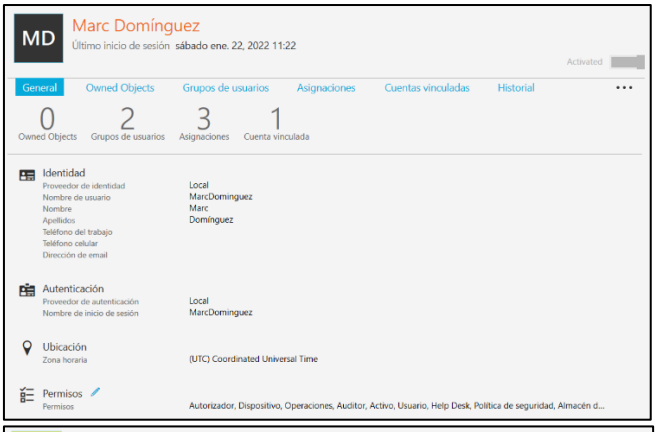
Una vegada creat l'actiu *Facebook Accounts* amb el seu corresponent compte local *OmegaFacebook*, creem l'assignació *Facebook Password Requests* i una política de sol·licitud de contrasenya bàsica, on indiquem el tipus d'accés per contrasenya i el requeriment d'aprovació de la sol·licitud.

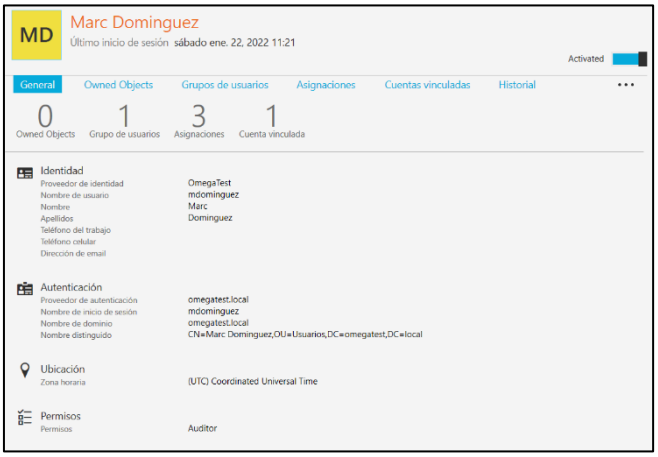
Un cop finalitzada la configuració, podem sol·licitar la contrasenya, i un cop sigui aprovada, la podrem visualitzar com s'observa a continuació.



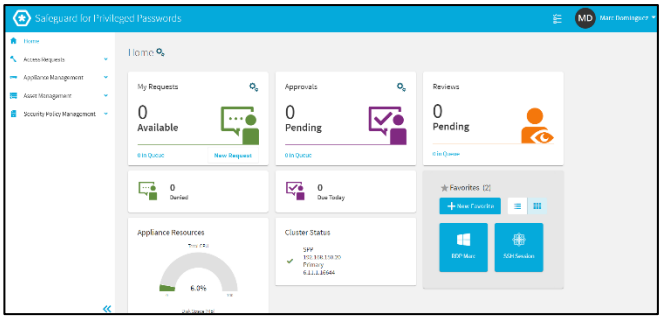
7.6 Autenticació amb contrasenya

Primer de tot, creem un usuari local i un usuari d'Active Directory.



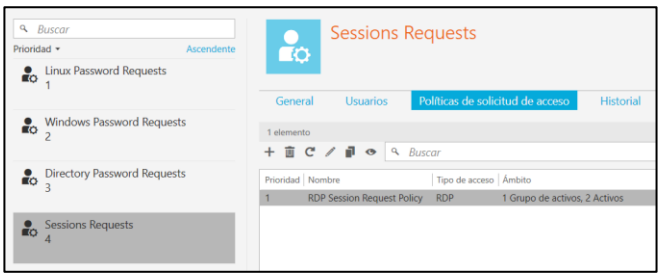


Una vegada configurem adequadament els usuaris, podem iniciar sessió fent servir les credencials assignades al compte de l'usuari i accedir al sistema.

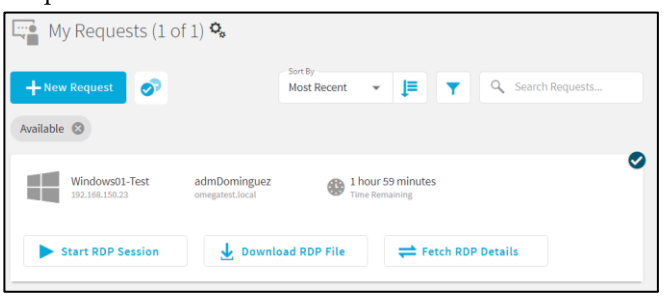


7.7 Iniciar una sessió privilegiada

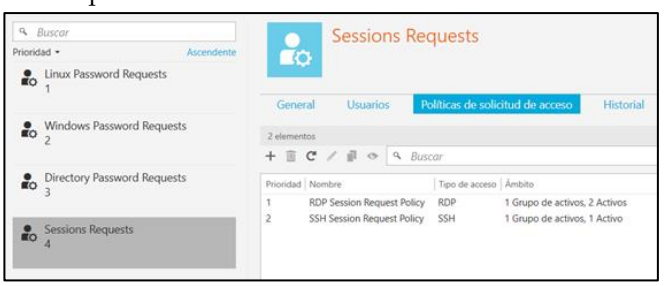
Després de la configuració, la política d'accés per sessions RDP queda establerta de la següent manera:



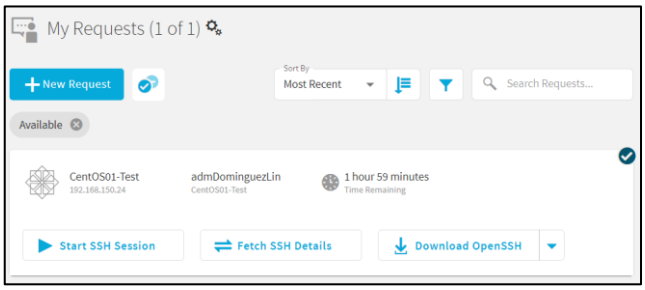
Si accedim com a usuari, podem sol·licitar l'accés a la màquina Windows e iniciar la sessió RDP.



Per la part de SSH, també configurem la política d'accés per sessions SSH.

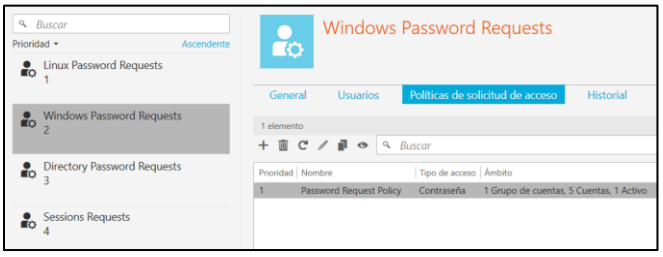


Si accedim com a usuari, també podem sol·licitar l'accés a la màquina Linux e iniciar la sessió SSH.

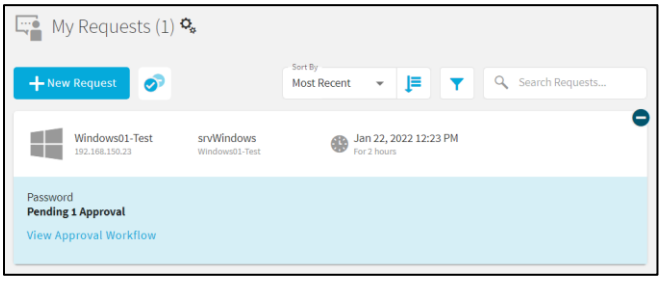


7.8 Revelar contrasenya

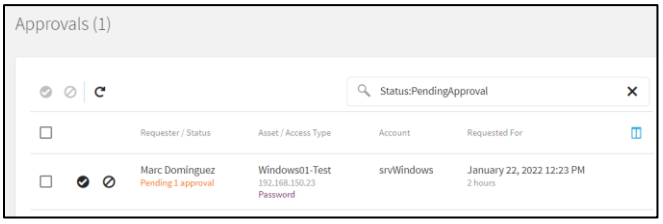
Després de la configuració, la política d'accés per contrasenya queda establerta de la següent manera:



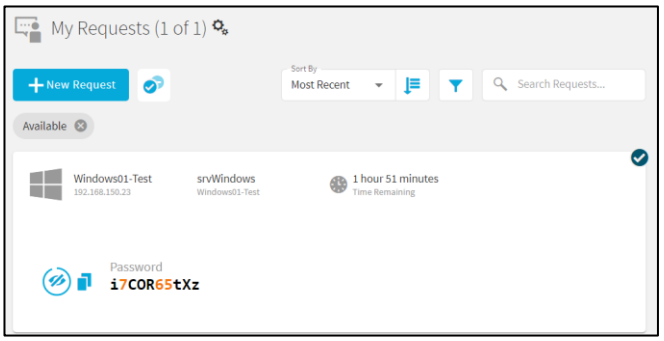
Si accedim com a usuari, podem sol·licitar el descobriment de la contrasenya de servei de la màquina Windows.



Com podem observar, encara no podem recuperar la contrasenya perquè necessitem l'aprovació d'un usuari aprovador, tal i com està configurat. Per tal de testejar la funcionalitat, iniciem sessió com un usuari definit com a aprovador per veure la petició.

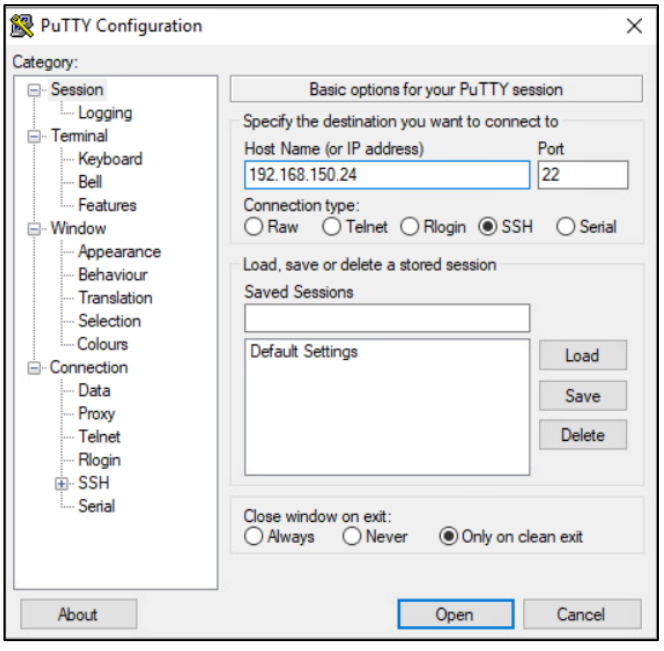


Aquí tenim les dades de la petició, i tenim la opció d'acceptar l'accés o denegar-lo. L'acceptem i retornem a l'usuari sol·licitant.



Ara ja podem obtenir la contrasenya temporal, que farem servir per accedir a l'actiu *Windows01-Test*. Per tal de poder iniciar sessió correctament, cal especificar el directori arrel de la màquina en el nom d'usuari, en aquest cas *WIN01TEST*, degut a que el compte genèric és local.

Per accedir al sistema amb el compte de servei de Linux, cal fer servir Putty, un client SSH per terminal, on amb la IP i la contrasenya de srvLinux podem accedir al sistema.



8 Conclusió

Durant la realització d'aquest projecte hi ha hagut dies intensos i no tan intensos de feina, però sempre s'ha mantingut una càrrega de treball setmanal similar, per tal de mantenir-se sobre la planificació establerta.

Malgrat aquesta planificació inicial, en les darreres setmanes vam prendre la decisió de juntar els documents de configuració i test en un de sol, ja que vam considerar més pràctic provar el funcionament de la configuració una vegada estava implementat.

Podem dir que la organització ha estat bastant adequada, ja que hem mantingut actualitzats els documents

en tot moment, classificant-los segons la fase i/o tasca en la que ens trobàvem i mantenint l'ordre mitjançant el software Jira.

En quant al desenvolupament del treball, hem completat els casos d'ús identificats a l'inici del projecte i, de cara al futur, es contemplen possibles millores d'alguns apartats per reforçar alguns aspectes del sistema i afegir funcionalitats opcionals que poden ser interessants per aquest sistema PAM.

Amb la realització d'aquest projecte, hem après que aquest sistema és més que rellevant i, considerem, necessari, per tal de mantenir la seguretat i la integritat de les credencials i dades sensibles de qualsevol empresa.

Sense anar més lluny, l'atac informàtic patit per la UAB, possiblement es podria haver evitat si la universitat comptés amb un sistema de protecció de comptes d'usuari privilegiats o un altre sistema similar; de manera que podem observar una possible aplicació d'una situació realista i molt recent.

AGRAÏMENTS

Agraeixo al meu tutor de l'empresa Omega Peripherals, Josep Lluís Masmitjà, per guiar-me en el projecte i facilitar-me la feina.

També agraeixo al meu tutor del TFG de la Universitat Autònoma de Barcelona, Juan Antonio Martínez, per ajudar-me en la redacció dels informes i per la seva atenció i disponibilitat.

BIBLIOGRAFIA

[1] P. Fisher, Trends in Privileged Access Management for the Digital Enterprise, KuppingerCole, 2020.

[2] J. Carson, Privileged Account Management for dummies, CISSP, 2017.

[3] C. Software, "CyberArk Software," 22 Julio 2021. [Online]. Available: https://www.cyberark.com/es/what-is/privileged-access-management/.

[4] R. Technologies, "How to create Sudo User in centOS," [Online]. Available: https://docs.rackspace.com/support/how-to/create-sudo-user-in-centos/.

[5] «Preparing Unix-based systems,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.11.1/administration-guide/134#TOPIC-1693940.

[6] «Preparing Windows systems,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.12.1/administration-guide/136#TOPIC-1738390.

[7] «Adding an Account Discovery job,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.12.1/administration-guide/55#TOPIC-1738064.

[8] «Adding password release request policies,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.12.1/evaluation-guide/4#TOPIC-1737875.

[9] «Adding a user,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.12.1/administration-guide/117#TOPIC-1738312.

[10] «Writing entitlements,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.12.1/evaluation-guide/4#TOPIC-1737872.

[11] «Adding session request policies,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.12.1/evaluation-guide/5#TOPIC-1737878.

[12] «Configuring the destination selection method,» [En línia]. Available: https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-sessions/6.12.0/evaluation-guide/3#TOPIC-1740664.