Treball final de grau Seguretat informàtica

Detecció de vulnerabilitats i intrusions a les xarxes de computadors

Daniel Manau Donas Grau d'Enginyeria Informàtica Seguretat Informàtica

Consultora: Cristina Pérez Solà Professora: Helena Rifà Pous

03/01/2018



uoc.edu





Aquesta obra està subjecta a una llicència de <u>Reconeixement-NoComercial-SenseObraDerivada</u> <u>3.0 Espanya de Creative Commons</u>

TFG – Detecció de vulnerabilitats i intrusions a les xarxes de computadors



FITXA DEL TREBALL FINAL

Títol del treball:	Detecció de vulnerabilitats i intrusions a les xarxes de computadors
Nom de l'autor:	Daniel Manau Donas
Nom del consultor/a:	Cristina Pérez Solà
Nom del PRA:	Helena Rifà Pous
Data de lliurament (mm/aaaa):	01/2018
Titulació o programa:	Grau d'Enginyeria Informàtica
Àrea del Treball Final:	Seguretat informàtica
Idioma del treball:	Català
Paraules clau	Seguretat en xarxes, vulnerabilitats, intrusions

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

El problema a resoldre en aquest projecte és la detecció de les possibles vulnerabilitats que poden existir en els diferents equips d'una organització.

Cada vegada és més habitual que les organitzacions ofereixin serveis de diferents tipus mitjançant internet. Aquest tipus de serveis públics requereixen una correcta protecció per tal d'evitar accessos no autoritzats als equips i a la xarxa interna.

Per protegir aquests equips exposats necessitarem les funcions d'un sistema detector de vulnerabilitats, el qual realitzarà diferents anàlisis sobre els equips existents a la xarxa client. També inclourem un sistema de detecció d'intrusions (IDS). Aquest sistema IDS registrarà tota activitat que sigui configurada com a no autoritzada.

L'objectiu final és protegir el màxim possible les xarxes de computadors de l'organització de possibles atacs d'intrusió.

Aquestes eines seran implementades en un dispositiu Raspberry Pi 3 i mitjançant un entorn simulat realitzarem les diferents proves de vulnerabilitats.

El resultat final de les proves realitzades demostra que en la majoria d'equips que s'utilitzen en entorns reals de treball presenten greus deficiències de seguretat. Aquestes poden ser solucionades amb una correcta gestió de les actualitzacions del



fabricant del sistema operatiu i auditories periòdiques de seguretat.

Abstract (in English, 250 words or less):

In this project the problem to resolve is the correct detection of possible vulnerabilities that may exist in the different devices of an organization.

Today is very common offer different types of services through the internet in any type of organization. These types of public services require the correct protection to prevent unauthorized access to devices and the internal network.

To protect these exposed devices, we will need the functions of a vulnerability detection system, which perform different analytics on the existing computers. We will also include an intrusion detection system (IDS). This IDS will record any activity that is configured as unauthorized.

The finally goal is to protect as much as possible the computer networks of the organization of possible intrusion attacks.

These tools will be implemented on a Raspberry Pi 3 device and through a simulated environment we will perform different tests of vulnerabilities.

The final result of the tests carried out shows that in the majority of equipment that is used in real work environment they present serious security deficiencies. These can be solved with a correct management of the updates of the manufacturer of the operating system and periodically security scans.



1. Introducció
1.1 Problema a resoldre7
1.2 Objectius7
1.3 Metodologia8
1.3.1 Recursos necessaris8
1.4 Tasques a realitzar8
1.5 Planificació temporal9
1.6 Estat de l'art
2. Programari
2.1 Sistemes detectors de vulnerabilitats12
2.1.1 Nessus
2.1.2 OpenVas
2.2 Sistemes detectors d'intrusions14
2.2.1 Snort
2.3 Sistema escollit
3. Preparació equips
3.1 Preparació dispositiu
3.2 Preparació entorn simulat16
4. Personalització Snort
4.1 Regles Snort
4.2 Entorn gràfic Snort
5. Estudi vulnerabilitats 25
5. Estadi vallerabilitats
5.1 Detecció vulnerabilitats
b. Gestio remota
7. Conclusions
8. Annexos
8.1 Preparació Raspberry Pi amb Kali Linux
8.2 Instal·lació OpenVas
8.3 Instal·lació Snort
9. Referències
10 Glossari
10. Glossai i

 $\ensuremath{\mathsf{TFG}}$ – Detecció de vulnerabilitats i intrusions a les xarxes de computadors



Llistat de figures

Figura 1. Taula planificació tasques Figura 2. Diagrama de Gantt PAC 1 i PAC 2 Figura 3. Diagrama de Gantt PAC 3 i PAC 4 Figura 4. Logo Nessus vulnerability scanner Figura 5. Logo OpenVas Figura 6. Logo Snort Figura 7. Topologia de xarxa dels equips Figura 8. Configuracions equip client amb Windows 7 Enteprise Figura 9. Configuració Domini al Servidor Windows Server 2012 R2 Figura 10. Registre a snort.org Figura 11. Exemple d'actualització de regles amb PulledPork Figura 12. Accés a Snorby i el seu dashboard. Figura 13. Taules creades a la BBDD per a Snorby Figura 14. Dashboard Snorby amb alertes Snort Figura 15. Dashboard OpenVas Figura 16. Configuració tasca nova Figura 17. Configuració New Target Figura 18. Llistat de tasques creades Figura 19. Llistat tasques amb les diferents accions i percentatge completat Figura 20. Resultats escaneig Client Windows 7 Enterprise Figura 21. Vulnerabilitat TCP timestamps Figura 22. Nova tasca amb per analitzar el servidor Figura 23. Llistat de tasques Figura 24. Resultats anàlisi vulnerabilitats Servidor Figura 25. Vulnerabilitat MS15-034 HTTP.sys execució de codi remot Figura 26. Vulnerabilitats SMB Server 4013389 Figura 27. Vulnerabilitat divulgació informació LDAP Figura 28. Vulnerabilitat divulgació informació LDAP 2 Figura 29. Vulnerabilitat enumeració serveis DCE/RPC Figura 30. Vulnerabilitat enumeració serveis DCE/RPC 2 Figura 31. Teamviewer -info Figura 32. ApplePi-Baker Càrrega imatge a SD Figura 33. Parted mostra particions de la targeta SD. Figura 34. Serveis tcp Figura 35. Accés al client Greenbone de OpenVas Figura 36. Dashboard de Greenbone Security Assitant Figura 37. Configuració inicial Snort Figura 38. Procés instal·lació Snort



1. Introducció

Universitat Oberta

de Catalunya

1.1 Problema a resoldre

El problema a resoldre en aquest projecte és la detecció i gestió de les possibles vulnerabilitats que poden existir en els diferents equips d'una organització que es troben accessibles des de l'exterior.

Avui dia cada vegada és més habitual que les organitzacions ofereixin als seus clients i empleats serveis de diferents tipus mitjançant internet. Aquest tipus de serveis públics requereixen una correcta protecció per tal d'evitar accessos no autoritzats als equips i a la xarxa interna.

Per protegir aquests equips exposats a internet necessitarem les funcions d'un sistema detector de vulnerabilitats, el qual realitzarà diferents anàlisis sobre els equips existents a la xarxa client. D'aquesta forma podrem dur a terme auditories de seguretat que ens reportarà un llistat de les debilitats trobades i que exposen la seguretat de la xarxa de computadors.

Segons les deteccions del detector de vulnerabilitats estudiarem les actuacions corresponents per tal d'evitar els riscos. A part, inclourem un sistema de detecció d'intrusions (IDS). Aquest sistema IDS registrarà tota activitat que sigui configurada com a no autoritzada, i en cas de detectar alguna intrusió, poder implementar les solucions corresponents per tal de defensar-se de l'atac.

L'objectiu final és protegir el màxim possible les xarxes de computadors de l'organització de possibles atacs d'intrusió.

1.2 Objectius

Per tal d'oferir una solució al problema plantejat en l'apartat anterior en aquest projecte és pretén integrar en un equip un sistema que ofereixi una solució de detecció d'intrusions i un sistema detector de vulnerabilitats. D'aquesta forma obtindrem un dispositiu que amb les personalitzacions oportunes pugui oferir els serveis plantejats a qualsevol organització que ho requereixi. Aquest equip romandrà destinat a la seu del client i disposarà de gestió remota.

També crearem un entorn simulat per poder comprovar el correcte funcionament del sistema implementat. Aquest entorn estarà format per una màquina virtual amb Windows Server 2012 R2, que realitzarà les funcions habituals de servidor, i també per una altra màquina virtual amb Windows 7 que realitzarà les funcions de client. Per últim, i mitjançant els resultats del detector de vulnerabilitats sobre l'entorn simulat, estudiarem quines solucions s'han d'implementar per protegir els equips de possibles atacs.



1.3 Metodologia

Universitat Oberta

de Catalunya

Com a punt inicial del projecte ens documentarem amb tota la informació relacionada disponible sobre els sistemes detectors de vulnerabilitats i dels detectors d'intrusions. També recopilarem informació sobre possibles vulnerabilitats del nostre sistema simulat.

A continuació crearem el sistema simulat en dos màquines virtuals. Decidirem quines intrusions es volen detectar i crearem les regles adequades per a implementar-les al IDS.

Una vegada el nostre dispositiu sigui funcional comprovarem la funcionalitat del IDS amb les regles aplicades i elaborarem una auditoria de seguretat mitjançant el detector de vulnerabilitats. Per últim, realitzarem una proposta d'accions a dur a terme per tal de solucionar les vulnerabilitats detectades.

1.3.1 Recursos necessaris

Els recursos necessaris inclouen una màquina virtual del servidor amb el sistema simulat vulnerable Windows Server 2012 R2 i una altra amb el sistema simulat d'un equip punt de treball amb Windows 7 . Per tal de generar aquest entorn de treball necessitarem un equip, que en aquest projecte serà un Macbook Pro amb processador i5 de 2,4 Ghz, 8 Gb de RAM 1600Mhz DDR3 i disc SSD de 256 GB.

Per una altra banda l'equip a utilitzar per a la instal·lació del sistema detector de vulnerabilitats i el IDS serà una Raspberry Pi 3 [1]. Aquest equip ofereix els requeriments necessaris per dur a terme les funcions exposades i ofereix unes mides reduïdes a un cost molt baix. En aquest equip instal·larem una distribució adaptada per a processadors ARM de Kali Linux [2].

1.4 Tasques a realitzar

Les tasques que caldrà realitzar per assolir el projecte són les següents:

- Recerca d'informació eina Snort [3] (manuals i documentació específica).
- Documentació eines detector de vulnerabilitats (Nessus [4] i OpenVas [5]) per tal de decidir quina eina implementarem.
- Creació entorn simulat. Aquest estarà format per les màquines virtuals (servidor i client) amb el sistema vulnerable simulat.
- Preparació equip Raspberry Pi amb distribució Kali Linux.
- Instal·lació i posada en marxa de les eines escollides en el sistema Kali Linux.

Universitat Oberta de Catalunya

- Elecció grup de regles Snort corresponents i implementar entorn gràfic.
- Realització proves alertes d'intrusió Snort.
- Detecció de les vulnerabilitats existents en el sistema simulat.
- Realització de proposta per tal de solucionar les vulnerabilitats detectades.
- Configuració d'un servei de connexió remota per tal de gestionar el dispositiu remotament.

Simultàniament a la realització de les tasques s'anirà documentant tota la informació per a la realització dels documents a entregar.

1.5 Planificació temporal

A continuació podem veure la planificació prevista per dur a terme el projecte:

G٩	project	,		
Nom		Inici	Finalització	Durada
▼ 0	PAC 1 Pla de treball	20/09/17	06/10/17	13
	Problema a resoldre	20/09/17	22/09/17	3
	Objectius	25/09/17	25/09/17	1
	Metodologia	26/09/17	26/09/17	1
	Recursos necessaris	27/09/17	27/09/17	1
	 Tasques a realitzar 	28/09/17	29/09/17	2
	 Estat de l'art 	02/10/17	03/10/17	2
	Planificació temporal	04/10/17	06/10/17	3
▼ 0	PAC 2	09/10/17	03/11/17	20
	Documentació Snort	09/10/17	11/10/17	3
	 Documentació detectors vulnerabilitats 	12/10/17	18/10/17	5
	 Sistema escollit 	19/10/17	19/10/17	1
	Preparació Raspberry amb Kali Linux	17/10/17	19/10/17	3
	 Instalació i posada en marxa eines escollides 	20/10/17	25/10/17	4
	• Creació entorn simulat (servidor i client)	26/10/17	01/11/17	5
	Reestructurar memòria	02/11/17	03/11/17	2

V 0	PAC 3	06/11/17 01/12/17	20
	Selecció regles Snort i entorn gràfic	06/11/17 10/11/17	5
	Proves d'intrussió	13/11/17 15/11/17	3
	Detecció vulnerabilitats	16/11/17 20/11/17	3
	Proposta solució vulnerabilitats	21/11/17 24/11/17	4
	Connexió remota	27/11/17 28/11/17	2
	Reestructurar memòria	29/11/17 01/12/17	3
v e	PAC 4	04/12/17 03/01/18	23
	Finalització apartats pendents	04/12/17 15/12/17	10
	Restructuració i finalització memòria	18/12/17 03/01/18	13
v e	Presentació virtual	04/01/18 11/01/18	6
	Disseny i creació presentació virtual	04/01/18 11/01/18	6

Figura 1. Taula planificació tasques

- PAC 1 i PAC 2



Figura 2. Diagrama de Gantt PAC 1 i PAC 2

TFG – Detecció de vulnerabilitats i intrusions a les xarxes de computadors







1.6 Estat de l'art

Els entorns Kali Linux [2] estan preparats per a la realització de proves de penetració i d'auditories de seguretat amb les més de 600 eines que incorpora per defecte. Aquest entorn disposa de versions per a tot tipus de processadors de 32 bit, 64 bit i ARM. Aqueta distribució Linux disposa d'una gran comunitat d'usuaris i desenvolupadors que ofereix tota mena d'informació i millores. A la mateixa pàgina web podem trobar gran quantitat d'informació.

Snort [3] és una de les solucions de programari més utilitzades per a la identificació d'intrusions. Està disponible sota llicència OpenSource i funciona en plataformes Windows / Linux / UNIX. Disposa d'una gran quantitat de filtres ja definits i gràcies al seu constant creixement disposa de constants actualitzacions. Aquest IDS disposa d'una comunitat que ens ofereix una multitud de webs on trobar exemples de regles i configuracions.

També podem afirmar l'existència d'un gran número d'eines detectores de vulnerabilitats. D'entre aquestes eines destaquem les més utilitzades, una de pagament sota llicència (Nessus) i una altra de codi lliure (OpenVas). Nessus inicialment va estar disponible sota llicència OpenSource i es va convertir en tot un referent en eines de detecció de vulnerabilitats. En l'actualitat es va convertir a llicència privativa.

OpenVas és una variant de la eina Nessus quan aquesta va canviar el tipus de llicenciament. Disposa d'una comunitat important que aporta noves actualitzacions i a diferència de Nessus aquesta eina ofereix una versió per a processadors ARM.

Existeixen diversos projectes d'implementació del sistema IDS Snort en el dispositiu Raspberry Pi. Entre ells destaquem el projecte: Raspberry pi amb Kali Linux i Snort [6]



Universitat Oberta

de Catalunya

per obtenir un IDS portable i a baix cost. També destaquem un altre projecte que converteix una Raspberry Pi en un IDS amb Snort [7].

En resum, les eines esmentades reben el suport d'una gran comunitat d'usuaris que faciliten la publicació d'actualitzacions i ,per tant, ens facilitarà la realització del projecte plantejat per a la protecció de vulnerabilitats i detecció d'intrusions amb Snort.

2. Programari

2.1 Sistemes detectors de vulnerabilitats

Els sistemes detectors de vulnerabilitats són una de les eines més utilitzades tant per administradors de sistemes com per possibles atacants. Aquestes eines disposen d'un conjunt d'utilitats que permeten comprovar si un sistema és vulnerable a un ampli conjunt de problemes de seguretat. Una vegada detecta alguna de les possibles vulnerabilitats s'encarregarà d'informar de la seva existència i les seves possibles solucions. Dins dels detectors de seguretat destaquem les eines Nessus i OpenVas.

2.1.1 Nessus



2.1.1.1 Descripció

Nessus [4] és una eina basada en el model client-servidor que compta amb el seu propi protocol de comunicació. De la mateixa forma que els altres escàners de vulnerabilitats existents, les tasques d'exploració i proves d'atacs contra objectius són realitzats per el servidor (nessusd). Les altres tasques de control, generació d'informes i presentació

són gestionats per el client (nessus). D'aquesta forma Nessus ens permet una exploració proactiva de les deficiències de seguretat dels equips de la nostra xarxa. La major part de les alertes que reportarà Nessus es troben relacionades amb les següents deficiències:

- Utilització de servidors (daemons) no actualitzats que presenten deficiències de seguretat conegudes.
- Deficiències de seguretat relacionades amb una incorrecta configuració dels servidors.



- Deficiències de seguretat relacionades amb la implementació de la pila TCP/IP del equip remot.
- Utilització d'aplicacions des de servidors webs configurats incorrectament.
- Instal·lació de back doors, trojans, DDoS dèmons o altres serveis perillosos en sistemes de producció.

Les proves de vulnerabilitats, disponibles com a un llarg llistat de plugins, són escrits en NASL, un llenguatge de scripting optimitzat per a interaccions personalitzades a les xarxes.

En la seva última versió es troba disponible per als sistemes operatius: Microsoft Windows, macOS, Linux, FreeBSD, GPG Keys en les plataformes i386 i x86-64.

2.1.1.2 Història

Universitat Oberta

de Catalunya

Renaud Deraison va iniciar el projecte Nessus el 1998 per oferir a la comunitat un escàner remot de seguretat de codi obert. El 2005, Tenable Security, empresa de la que Renaud era cofundador, va canviar a llicència privativa del Nessus 3. En el 2008, Tenable va revisar la llicència per permetre als usuaris domèstics accedir sense restriccions als plugins i també va crear una llicència d'ús comercial.

2.1.2 OpenVas



Figura 5. Logo OpenVas

2.1.2.1 Descripció

OpenVas [5] (Open Vulnerability Assessment System) és una suite d'eines especialitzades en l'escaneig i gestió de vulnerabilitats de seguretat en sistemes informàtics. Les característiques principals són:

- Escaneig simultani de diferents nodes
- Suport SSL
- Suport WMI
- Escaneig automàtic programat
- Servidor web integrat
- Multiplataforma

Des de la versió 4.0 OpenVas permet l'actualització continua de la base de proves de vulnerabilitats de xarxa. Amb la versió 7 es va suprimir el mòdul d'administrador i el client d'escriptori per centrar-se en el seu client web.

U0C

Openvas és multiplataforma com Nessus, però en aquest cas també suporta processadors d'arquitectura ARM.

2.1.2.2 Història

Universitat Oberta

de Catalunya

OpenVas va ser inicialment anomenat GNessUS, per ser una variant de l'escàner de seguretat Nessus quan aquest va canviar el tipus de llicenciament. Va ser proposat com a sistema per dur a terme proves de penetració, pentester a l'organització Portcullis Computer Security. Després va ser anunciat com una solució de programari lliure per Tim Brown en Slashdot. Actualment és l'opció de programari lliure més completa gràcies a les continues actualitzacions de la seva base de dades de vulnerabilitats.

2.2 Sistemes detectors d'intrusions

Els sistemes IDS [9] (Intrusion Detection System) analitzen tots els datagrames IP que circulen en la xarxa amb l'objectiu de detectar el trànsit no autoritzat. Es poden implementar com a simples detectors de paquets (sniffers) per al monitoratge del trànsit d'una petita xarxa fins com a un sistema de detecció d'intrusos en temps real. Un dels IDS més reconeguts i utilitzats actualment és Snort.

2.2.1 Snort



Figura 6. Logo Snort

2.2.1.1 Descripció

Snort [3] és un NIDS de seguretat passiva, ja que, es limita a capturar els paquets i registrar-los. És open source i gràcies a la seva popularitat disposa d'una gran comunitat que col·labora en el seu desenvolupament. Algunes característiques rellevants:



- Registre en servidors de fitxers o de bases de dades de tot el trànsit capturat.
- Client IDS lleuger
- Multiplataforma
- Ofereix regles de detecció creades per la comunitat

Snort contrastarà tot el trànsit capturat amb les regles de detecció establertes per el usuari. Aquestes regles poden ser de creació pròpia, que no són res més que un conjunt de requisits on indiquem que ha d'activar una alarma si es compleixen.

2.2.1.2 Història

El 1998 va ser desenvolupat per Marty Roesch per a distribucions GNU/Linux amb el nom d'APE.

L'any 1999 és va introduir l'analitzador de signatures com a nova funcionalitat. D'aquesta forma es va començar a utilitzar com a IDS.

L'autor Marty Roesch va dedicar-se a partir d'aquell moment a temps complet en el desenvolupament de noves funcionalitats que milloressin la capacitat de configuració i facilitessin l'ús de Snort.

Marty va aconseguir fundar Sourcefire amb el finançament aconseguit. Actualment es distribueix la versió 3.0 Alpha 4.

Snort continua sent de codi lliure i promet seguir sent-ho per sempre.

2.3 Sistema escollit

Una vegada analitzats els diferents programaris possibles per dur a terme el nostre projecte, escollirem els que millor s'adaptin al maquinari escollit. Com s'indica en l'apartat "1.3.1 Recursos Necessaris" el maquinari escollit és un equip Raspberry Pi 3. Aquest dispositiu disposa d'un processador de quatre nuclis de 1,2 Ghz ARM de 64bits Cortex-A53 i 1 GB RAM.

L'arquitectura ARM del processador ens limitarà a la utilització de programari adaptat a aquests processadors.

Amb les característiques tècniques del maquinari escollit optarem per a la implementació en el projecte del següent programari:

- Sistema operatiu: Kali Linux Custom ARM for Raspberry Pi 2/3 (ref. [8]).
- Sistema detector de vulnerabilitats: OpenVas 8.0
- Sistema IDS: Snort



Universitat Oberta

de Catalunya

3. Preparació equips

3.1 Preparació dispositiu

Una vegada escollides les eines a implementar en el dispositiu realitzarem les instal·lacions oportunes. Primer realitzarem la instal·lació del sistema operatiu Kali Linux (Annex 8.1). Una vegada tenim la Raspberry operativa amb una IP assignada procedirem a instal·lar les eines OpenVas (Annex 8.2) i Snort (Annex 8.3).

A partir d'aquest moment podrem accedir al client OpenVas mitjançant la ip de l'equip i el port 9392. Snort també serà funcional quan configurem un grup de regles. A més, implementarem el framework Snorby per tal de disposar d'una interfície gràfica per visualitzar les alertes.

3.2 Preparació entorn simulat

Per a la creació de l'entorn simulat optarem per a la creació de dues màquines virtuals. Aquestes màquines han de representar els sistemes i configuracions més comuns en les organitzacions. D'aquesta manera l'estudi de les vulnerabilitats d'aquests equips seran més ajustades a la realitat. Una de les màquines virtuals realitzarà les funcions de servidor de l'organització. Aquest servidor funcionarà amb Windows Server 2012 R2, realitzarà funcions d'administració de directori actiu i DNS. També compartirà una unitat de xarxa per als treballadors a c:\Share.

L'altra màquina virtual amb Windows 7 Enterprise realitzarà les funcions d'equip client. Aquest equip disposarà d'algunes eines ofimàtiques habituals i tindrà accés a la unitat de xarxa compartida.



Figura 7. Topologia de xarxa dels equips



d l				-				
🕒 🔍 🖉 🕨 Control Panel 🕨	All Control Panel Items	m 👻 😽 Search Control	l Panel 🔰	Comput	er 🕨	 Search Computer 		٩
Control Panel Home Windows edition Device Manager © Remote settings © System protection © Advanced system settings		P	Organize Propertie Favorites Desktop Ovunloads Recent Places Libraries Documents	s System properties Uninstall or change a program Hard Disk Drives (1) Local Disk (C) Di GB free of 20.6 GB Devices with Removable Storage (1) CD Drive (0) OPRCE14 CD Drive (0) OPRCE14 CD Drive (0) OPRCE14	Map network drive »	1, .	0	
	System Rating: Processor: Installed memory (RAM): System type: Pen and Touch:	System rating is not available Intel(R) Core(TM) 15-42580 CPU @ 2.40GHz 2.4 2.00 GB 32-bit Operating System No Pen or Touch Input is available for this Displ	40 GHz lay	Music Pictures Videos Computer Network	Vetwork Location (1) there (\\92.188.1.190) (W) 9.30 08 free of 19.6 08			
	Computer name, domain, and	workgroup settings						
	Computer name:	Client	😴 Change settings					
See also	Full computer name:	Client.TFG_SEGURETAT.cat		share (\\192.1	168.1.190) (W:) Space used: Tot:	al size: 19.6 GB		
Action Center	Computer description:			Network Drive	Space free: 9.30 GB File s	ystem: NTFS		
Windows Update	Domain:	TFG_SEGURETAT.cat					5.4	5 AM
Performance Information and Tools	Windows activation			🌝 🥭 🔚			10/1	5/2017



2		Administrador del servidor		_ 0 X
E Administra	dor del servidor v	Servidor local) 🖍 Administrar Herramientas	Ver Ayuda
Panel	PROPIEDADES Para Server		[TAREAS 👻
Servidor local Todos los servidores AD DS AD DS AD DS	Nombre de equipo Dominio	Server TFG_SEGURETAT.cat	Últimas actualizaciones instaladas Windows Update Últimas actualizaciones buscadas	N N
 AD RMS DHCP DNS IIS Servicios de archivos y ▷ 	Firewall de Windows Administración remota Escritorio remoto Formación de equipos de NIC Ethernet	Privado: Activado Habilitado Deshabilitado Deshabilitado 192.168.1.190, IPv6 habilitado	Informe de errores de Windows Programa para la mejora de la experiencia Configuración de seguridad mejorada de l Zona horaria Id. del producto	del usuario N E A (U S
	Versión del sistema operativo Información de hardware	Microsoft Windows Server 2012 R2 Standard innotek GmbH VirtualBox	Procesadores Memoria instalada (RAM) Espacio total en disco	lr O 1
	<			>
	EVENTOS Todos los eventos 94 en total	 ▼ (#) ▼ (#) 	[TAREAS V
	Nombre del servidor Id.	Gravedad Origen	Registro Fecha y hora	
	SERVER 6038 SERVER 8198 SERVER 6006	Advertencia Microsoft-Windows-LSA Error Microsoft-Windows-Security-SPP Advertencia Microsoft-Windows-Winlogon	Sistema 15/10/2017 1 Aplicación 15/10/2017 1 Aplicación 15/10/2017 1	14:42:48 ^ 14:16:52 14:16:28 v
				14:48 15/10/2017

Figura 9. Configuració Domini al Servidor Windows Server 2012 R2



4. Personalització Snort

4.1 Regles Snort

Universitat Oberta

de Catalunya

Per a la utilització de regles optarem per les que ofereix la mateixa comunitat snort.org. Aquestes regles s'actualitzen regularment amb les noves amenaces a detectar. Per aquest motiu és molt recomanable actualitzar el més sovint possible l'arxiu de regles de Snort.

Aquesta tasca l'automatitzarem amb la utilització del programari PulledPork[18]. Aquesta aplicació s'encarrega de carregar les noves regles que descarrega directament des de la web oficial de Snort i aplicar-les en el nostre dispositiu.

Primerament configurarem l'arxiu snort.conf de Snort:

```
wget https://www.snort.org/downloads/snort/snort-2.9.11.tar.gz
cd /usr/local/src && wget --no-check-certificate https://www.snort.org/documents/185
-0 snort.conf
tar xvfz snort-2.9.11.tar.gz
cd snort-2.9.11
./configure --enable-sourcefire; make; sudo make install
mkdir /usr/local/etc/snort /usr/local/etc/snort/rules /var/log/snort
/var/log/barnyard2 /usr/local/lib/snort_dynamicrules
touch /usr/local/etc/snort/rules/white_list.rules
/usr/local/etc/snort/rules/black_list.rules /usr/local/etc/snort/sid-msg.map
groupadd snort && useradd -g snort snort
cp /usr/local/src/snort-2.9.11/etc/*.conf* /usr/local/etc/snort
cp /usr/local/src/snort-2.9.11/etc/*.map /usr/local/etc/snort
cp /usr/local/src/snort.conf /usr/local/etc/snort
mkdir /var/log/snort
chown snort:snort /var/log/snort
nano /usr/local/etc/snort/snort.conf
```

Dins de snort.conf modificarem aquestes línies:

```
var RULE_PATH rules
var SO_RULE_PATH so_rules
var PREPROC_RULE_PATH preproc_rules
var WHITE_LIST_PATH rules
var BLACK_LIST_PATH rules
```

output unified2: filename snort.log, limit 128



uoc.edu

Després necessitarem registrar-nos com a usuaris a snort.org per obtenir el nostre Oinkcode (codi d'usuari):

danimanau@gmail.com	
Account	Oinkcode
Oinkcode	56363bda6d36212e956a7da21c5d4dbada95e8e4
Subscription	
Receipts	Regenerate
False Positive	
	Documentation
	How to use your oinkcode

Figura 10. Registre a snort.org

A continuació les comandes per a la instal·lació i configuració de PulledPork:

cd /usr/local/src

git clone <u>https://github.org/shirkdog/pulledpork</u>

cd pulledpork

cp pulledpork.pl /urs/local/bin && cp etc/*.conf /usr/local/etc/snort

A continuació ens cal estar registrats i disposar del Oinkcode:

nano /usr/local/etc/snort/pulledpork.conf

Substituirem a la línia 19 <oinkcode> per el nostre codi.

A la línia 133 indiquem la nostra distribució:

distro=Debian-6-0

chmod +x /usr/local/bin/pulledpork.pl mkdir /usr/local/etc/snort/rules/iplists

Per actualitzar les nostres regles per les més actualitzades:

/usr/local/src/pulledpork/pulledpork.pl -c /usr/local/etc/snort/pulledpork.conf -T -1



https://github.com/shirkdog/pulledpork ----.\ --==\\ / PulledPork v0.7.3 - Making signature updates great again! `--==\\/ Copyright (C) 2009–2017 JJ Cummings, Michael Shirk ~~~-.Y|\\ / 66_ and the PulledPork Team! / _(") -| ||'--' Rules give me wings! Υ. /-| ||'-Rules give me wings! _\ 1_11 Checking latest MD5 for snortrules-snapshot-29110.tar.gz.... Rules tarball download of snortrules-snapshot-29110.tar.gz.... They Match Done! Checking latest MD5 for community-rules.tar.gz.... Rules tarball download of community-rules.tar.gz.... They Match Done! IP Blacklist download of https://talosintelligence.com/documents/ip-blacklist.... Reading IP List. Checking latest MD5 for opensource.gz.... Rules tarball download of opensource.gz.... They Match Done! Prepping rules from snortrules-snapshot-29110.tar.gz for work.... Done! Prepping rules from community-rules.tar.gz for work.... Done! Prepping rules from opensource.gz for work.... Done! Reading rules. Writing Blacklist File /usr/local/etc/snort/rules/iplists/default.blacklist.... Writing Blacklist Version 1717724772 to /usr/local/etc/snort/rules/iplistsIPRVersion.dat.... Setting Flowbit State.. Enabled 8 flowbits Done Writing /usr/local/etc/snort/rules/snort.rules.... Done Generating sid-msg.map.... Done Writing v1 /usr/local/etc/snort/sid-msg.map.... Done Writing /var/log/sid_changes.log.... Done Rule Stats... ---32928 New:-Deleted:---0 Enabled Rules:----10467 Dropped Rules:----0 Disabled Rules:---22461 Total Rules:----32928 IP Blacklist Stats... Total IPs:----2471 Done Please review /var/log/sid_changes.log for additional details Fly Piggy Fly!

[root@kali:/usr/local/src/pulledpork# /usr/local/bin/pulledpork.pl -c /usr/local/etc/snort/pulledpork.conf -T -l

Figura 11. Exemple d'actualització de regles amb PulledPork

4.2 Entorn gràfic Snort

Per facilitar la visualització i gestió de totes les dades que recull Snort implementarem un dels diversos entorns gràfics desenvolupats per la comunitat.

Escollirem el GUI que sigui més adequat per al nostre maguinari, ja que, disposem d'uns recursos més limitats que amb un ordinador/servidor habitual.

Aquest és el cas del GUI Snorby que és compatible amb el maquinari de Raspberry Pi i requereix pocs recursos per al seu funcionament.



Snorby

Per a la seva instal·lació primer instal·larem totes les dependències:

```
apt-get install libmysqlclient-dev postgresql-server-dev-9.4 libpq-dev
wget https://ftp.psu.ac.th/pub/snort/libdnet-1.12.tgz
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
tar xvfvz libdnet-1.12.tgz
cd libdnet-1.12
./configure "CFLAGS=-fPIC"
make && make install && make check
ln -s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1
cd /usr/local/src
tar xvfz daq-2.0.6.tar.gz
cd daq-2.0.6
./configure
```

make && make install

Ara iniciem la instal·lació de Snorby:

```
wget https://github.com/Snorby/snorby/archive/master.zip
gem install bundler
bundle install
bundle exec rake snorby:setup
```

Configurem l'arxiu /snorby/config/database.yml:

```
# Snorby Database Configuration
#
# Please set your database password/user below
# NOTE: Indentation is important.
#
snorby: &snorby
  adapter: mysql
  username: snorby # usuari de mysql
  password: snorby # el mateix password del nostre usuari
  host: 127.0.0.1 # IP del equip on es troba la BBDD
development:
  database: snorby
  <<* snorby
production:
  database: snorby
  <<* snorby
```

Canviem el nom l'arxiu /snorby/config/snorby_config.yml.example a snorby/config/snorby_config.yml

Finalment, podrem iniciar snorby per realitzar proves. Abans caldrà que MySQL estigui iniciat:

```
/etc/init.d/mysql start
cd /snorby
bundle exec rails server -e production
```



uoc.edu

Una vegada iniciat podrem accedir a la interfície de snorby conectant-nos a <u>http://192.168.1.108:300</u> amb les credencials <u>snorby@example.com</u> / snorby.

	Snorby Mitthread	Stack		Welcome Administrate	x Settings Log.out
Sporbu Similar Stack	Dashboard My Queue (0)	Events Sensors Search	1 ① The Snorby wor	ker is not currently running.	Administration
	Dashboard				More Options
	LAST 24 TODAY YESTERDAY TH	S WEEK THIS MONTH THIS QUARTER	THIS YEAR Updated: 11/24/17 10:39 PM UTC	TOP 5 SENSOR	
Login	0	0	0	Administrator	0
Email	HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY	LAST 5 UNIQUE EVENT	5
snorby@example.com				ANALYST CLASSIFIED	EVENTS
Password	0/0	0/0	0/0	Unauthorized Root Acces	s 0
	Sensors Seventies Protocols	Signatures Sources Destinations		Attempted Unauthorized	. 0
		Event Count vs Time By Sense	or	Denial of Service Attack	0
Wolcomo Sign In Forget Pasaward?				Policy Violation	0
Velcome, Sign in Porgol Password? Venember me				Reconnaissance	0
				Virus Intection	0
© 2017 Thread Stack. Ing - Created By: Dustin Wills Webber Snorby 2.6.3 - https://github.com/Sinorby/anorby					0

Figura 12. Accés a Snorby i el seu dashboard.

Barnyard2

Realitzarem una altra instal·lació necessària per moure les alertes generades per Snort a la BBDD i també per a millorar-ne el rendiment, es tracta del programari Barnyard2 [17].

En entorns on el IDS Snort ha de processar una gran quantitat de dades és molt possible que el rendiment es vegi afectat i finalment descarti alguns paquets de dades. Això es produeix per que Snort no processa el següent paquet fins que no finalitza l'escriptura de l'alerta a la base de dades. Aquest procés és lent, ja que, requereix una connexió TCP i un insert a la BBDD per cada alerta.

Per generar alertes més ràpidament Snort utilitza el format unified2 [17] per escriure les dades en un arxiu local.

Per per tal de traslladar aquestes dades a la base de dades utilitzarem Barnyard2 [17], que és un intèrpret open source del fitxers de sortida en format unified2.

Per instal·lar i configurar Barnyard2 utilitzarem les següents comandes:

```
cd /usr/local/src && wget https://github.com/firnsy/barnyard2/archive/master.tar.gz
tar -zxf master.tar.gz && cd barnyard2-*
autoreconf -fvi -I ./m4 && ./configure --with-mysql --with-mysql-
libraries=/usr/lib/arm-linux-gnueabihf/ && make && make install
mv /usr/local/etc/barnyard2.conf /usr/local/etc/snort
cp schemas/create_mysql /usr/local/src
nano /usr/local/etc/snort/barnyard2.conf
```

Configurarem l'arxiu barnyard2.conf modificant les línies 27, 28, 29 i 30:

```
# set the appropiate paths to the file(s) your Snort process is using.
config reference_file: /usr/local/etc/snort/reference.config
config classification_file: /usr/local/etc/snort/classification.config
config gen_file: /usr/local/etc/snort/gen-msg.map
config sid_file: /usr/local/etc/snort/sid-msg.map
```



uoc.edu

Per últim afegim al arxiu barnyard2.conf una última línia amb les dades de la BBDD:

output database: log, mysql, user=snorby password=snorby dbname=snorby host=127.0.0.1

A continuació configurarem la base de dades on s'emmagatzemen les dades recollides per Snort.

sudo service mysql start mysql -u root -p

```
create database snorby;
grant CREATE, INSERT, SELECT, DELETE, UPDATE on snorby.* to snorby@localhost;
SET PASSWORD FOR snorby@localhost=PASSWORD('snorby');
use snorby;
source /usr/local/src/create_mysql
```

Podem observar les taules creades:

show tables;



Figura 13. Taules creades a la BBDD per a Snorby



Com a últim pas per iniciar el sistema Snort amb Snorby cal iniciar els diferents components en el següent ordre:

Una vegada tots els serveis estiguin en marxa podrem observar que a Snorby ja apareixen dades sobre les alertes detectades per Snort:



Figura 14. Dashboard Snorby amb alertes Snort



Universitat Oberta

de Catalunya

5. Estudi vulnerabilitats

5.1 Detecció vulnerabilitats

Una vegada tenim el nostre dispositiu amb OpenVas connectat a la mateixa xarxa que els dispositius a escanejar ja podem iniciar la detecció a cada equip. Per això entrarem al client web mitjançant la ip 192.168.1.108:9392 i entrem al sistema.

Una vegada al dashboard anirem al menú: SCANS > TASKS > NEW TASK.

Security Assistant						Refresh every 30 Logged ir Sun	as Admin dani Logout Nov 5 01:31:31 2017 UTC
Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	Help
2 📉 🛨				Fi	ilter:	ort=name	
Tasks (3 of 3)							2
▼ Tasks by Se	everity Class (Total: 3)	*	Tasks with most H	ligh results per host	•	Tasks by status (Total: 3)	
C		High Log	No Tasks with H	igh severity found		0	Done

Figura 15. Dashboard OpenVas

Iniciarem analitzant les vulnerabilitats de l'equip simulat client amb Windows 7 i amb ip 192.168.1.200. Dins de la nova tasca crearem un nou "Target".

New Task			
Name	Client		
Comment			
Scan Targets	Client	▼ 🖬	
Alerts	0	Create a new target	
Schedule		▼ Once 🔀	
Add results to Assets	💿 yes 🔵 no		
	Apply Overrides	💿 yes 🔘 no	
	Min QoD	70 🔶 %	
Alterable Task	🔵 yes 💽 no		
Auto Delete	 Do not automatically 	delete reports	
Reports	Automatically delete	oldest reports but always keep newest 5 🚔 reports	
Scanner	OpenVAS Default	▼	
		()	
		Cre	ate

Figura 16. Configuració tasca nova

En aquesta finestra configurarem "Create a new target" amb la ip del equip de la següent manera:

TFG – Detecció de vulnerabilitats i intrusions a les xarxes de computadors



New Target			×
Name	Client		
Comment	scan win7 client		
	o Manual		192.168.1.200
Hosts	From file		Seleccionar un arxiu cap arxiu seleccionat
Exclude Hosts			
Reverse Lookup Only	🔿 Yes 💿 No		
Reverse Lookup Unify	🔿 Yes 💽 No		
Port List	All IANA assigned TCP 2012	Z	
Alive Test	Scan Config Default	_	
Credentials for authenticated checks			
SSH		on p	port 22
SMB		- 🔀	
			۱
			Create

Figura 17. Configuració New Target

Deixem per defecte els valors del llistat de ports IANA ja que és el més complet. Una vegada creada la tasca ja serà accessible des del llistat de tasques:



Figura 18. Llistat de tasques creades

Podem iniciar la tasca, aturar-la, esborrar-la o modificar-la des del menú d'accions disponibles a la dreta. Una vegada complert podrem accedir al report corresponent.





Figura 19. Llistat tasques amb les diferents accions i percentatge completat

-								
Greenbone Security Assistant							Refresh every 30 * Logged Su	in as Admin dani Logout n Nov 5 02:35:11 2017 UTC
Dashboard	Scans	Assets	SecInfo	Confi	juration	Extras	Administration	Help
2					Filter: apply_ove	severity>Error and task_id=0672c mides=0 min_qod=70 sort=nvt first=1 row	#fb-12a0-458c-8056	× ×
Results (5 of 31)							2
 Results by 5 	Severity Class (Total: 5)	*	Results vulner	ability word clou	d	•	Results by CVSS (Total: 5)	
C		Low				40 35- 30- 25- 20- 15- 16- 05- 00- NA 0 1	2 5 4 5 6	1 i i i i i i i i i i i i i i i i i i i
				_				1 - 5 of 5
Vulnerability		Sev Sev	erity	🙋 QoD 🛛 F	lost	Location	Created	
OS Detection Consolidation and Report	ting		0.0 (Log)	80% 1	92.168.1.200	general/tcp	Sun Nov 5 02:22:52 2017	
DCE/RPC and MSRPC Services Enumer	ration	S	0.0 (Log)	80% 1	92.168.1.200	135/tcp	Sun Nov 5 01:51:34 2017	
Traceroute		-	0.0 (Log)	80% 1	92.168.1.200	general/tcp	Sun Nov 5 02:08:39 2017	
TCP timestamps			2.6 (Low)	80% 1	92.168.1.200	general/tcp	Sun Nov 5 02:23:14 2017	
CPE Inventory		-	0.0 (Log)	80% 1	92.168.1.200	general/CPE-T	Sun Nov 5 02:23:17 2017	

Una vegada finalitzi la tasca ja podrem accedir als resultats:

Figura 20. Resultats escaneig Client Windows 7 Enterprise

Després d'analitzar els resultats obtinguts podem concloure que quatre dels cinc avisos ens informen que un possible atacant serà capaç d'identificar quin sistema estem utilitzant mitjançant el seu fingerprint. Aquestes alertes són inherents al sistema operatiu i no podrem oferir cap solució per a la seva ocultació a un possible atacant. Per aquest motiu el sistema OpenVas les classifica com alertes tipus log:

- OS Detection Consolidation and Reporting
- DCE/RPC and MSRPC Services Enumeration
- Traceroute
- CPE Inventory

Per una altra banda l'anàlisi ens informa d'una vulnerabilitat considerada "Low" o lleu. En aquest cas el sistema atacant podrà calcular el "uptime" (temps d'activitat) de l'equip. En la seva descripció ens informa de la seva afectació i possibles solucions:



Example of the set of the factor is that the upformed the factor is accorded in -between: Example of the factor is accorded in a delay of 1 seconds in -between: Example of the factor is accorded in a delay of 1 seconds in -between: Example of the factor is accorded in a delay of 1 seconds in -between: Example of the factor is accorded in a delay of 1 seconds in -between: Example of the factor is accorded in a delay of 1 seconds in -between: Example of the factor is accorded in a delay of 1 seconds in -between: Example of the factor is accorded in a delay of 1 seconds in -between: Example of the factor is that the upform of the renote host can sometimes be computed. Example of the factor is the factor is that the upform of the renote host can sometimes be computed. Example of the factor is the factor is that the upform of the renote host can sometimes be computed. Example of the factor is the factor is that the upform of the renote host can sometimes be computed. Example of the factor is the factor is that the upform of the renote host can sometimes be computed. Example of the factor is the factor is that the upform of the renote host can sometimes be computed. Example of the factor is the factor is that the upform of the renote host can sometimes be computed. Example of the factor is the factor is that the upform of the renote host can sometimes be computed. Example of the factor is that the upform of the renote host can sometimes be computed visible. Example of the factor is the factor i	lp									
Vulnerability Severity Optimizations To' intestamps Image: I	i401-d2fca09caf14 017 017									
Image:	Actions									
Sharper The remote hippements TCP timestamps and therefore allows to compute the uptime. Vinerability Detection Result The remote house the boats implements RPC1123. The following timestamps waves retrieved with a delay of 1 seconds in-betweens Proceed:::::::::::::::::::::::::::::::::::	8									
Vinceability Detection Result If was detected that the both implements RFC1123. The following timestamps wave restrieved with a delay of 1 seconds in-between: Proceed:: 1: 85311 Proced:: 1: 85411 Proced:: <td colspan="10">Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.</td>	Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.									
It is a detected that is host lightemasts MPC132. The Reliance of the Relianc	Vulnerability Detection Result									
Proceed: 11 (solid) Listed status Proced: 11 (solid) Listed statu										
Impact As adde effect of his feature is that the uptime of the remote host can sometimes be computed. Solution Solutio	The following timestamps were retrieved with a delay of 1 seconds in-between: Nachet 1: 863311 Nachet 2: 86547									
Solution to disable TCP timestamps on linux add the line 'net.lpv4.tcp_timestamps = 0' to /etc/systcl.conf. Execute 'syscl -p' to apply the settings at runtime. To disable TCP timestamps on linux add the line 'net.lpv4.tcp_timestamps = 0' to /etc/systcl.conf. Execute 'syscl -p' to apply the settings at runtime. To disable TCP timestamps on linux add the line 'net.lpv4.tcp_timestamps = 0' to /etc/systcl.conf. Execute 'syscl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute' netsh in to get global timestamps = 0' to /etc/systcl.conf. Execute 'syscl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute's netsh in to get global timestamps and to be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp aptions when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See alice : http://www.microsoft.com/en us/download/detalia.sapx/id=9152 Affected software/OS TCP/IPv4 implementations that implement RFC1323. Unterstamption to the tot the tot the target IP. The responses are searched for a limestamps. If found, the timestamps are reported.	Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.									
To disable TCP timestamps on linux add the line Het, by Atto, Linestamps = 0' to /etc/systL.conf. Execute 'systL -p' to apply the settings at runtime. To disable TCP timestamps on Windows Server 2008 and Vitsa, the timestamps = disabled' Starting with Windows Server 2008 and Vitsa, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SMN) segment. See also: http://www.microsoft.com/en-us/download/defails.aspx?id=9152 TCP/IPv4 Implementations that Implement RFC1323. Vincensity Turing Internet RFC1323. Vincensity Turing Internet RFC1 Turing Internet RFC1323. Vincensity Totics are fored an esent with a little dely in between to the target IP. The responses are searched for a limestamps. If found, the timestamps are reported.										
To disable TCP timestamps on Windows execute 'netsh in tcp set global (imestamps-disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id-9152 Affected Software/OS TCP/IPM Implementations that Implement RFC1323. ValenceNity Tasksh TCP timestamps, as defined by RFC1323. ValenceNity Detaction Nethod Secial IP ackets are formed and sent with a little delay in between to the target IP. The responses are searched for a limestamps. If found, the timestamps are reported.										
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See alias: http://www.microsoft.com/en-us/download/details.aspx?id=9152 Affected Software/OS TCP/IPM implementations that implement RPC1323. Vulnerability Trasight The remote hour implements TCP timestamps, as defined by RPC1323. Vulnerability Detection Method Seciel IP Sockets are forced and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.										
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SNN) segment. See also: http://www.microsoft.com/er-us/download/details.aspx?id=9152 TCP/IPv4 implementations that implement RFC1323. Vulnershilty Insight The remote hour implements TCP timestamps, as defined by RFC1323. Vulnershilty Detection Method Secial IP packets are forced and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.										
See alies: http://www.minsestrt.com/en-us/download/detalia.sapx?tid=9152 Affected Software/OS TrY/In-4 Implementations that Implement RFC1323. Vulnerability Tasjaht The remote host implements TCF Imestamps, as defined by RFC1323. Vulnerability Detection Nethod Seeaal IP advects are formed and sent with a little delay in between to the target IP. The responses are searched for a limestamps. If found, the timestamps are reported.										
Affected Software/05 TCP/IPV4 implementations that implement RFC1323. Vulnerability Taskt The remote host implements TCP timestamps, as defined by RFC1323. Vulnerability Detection Method Secial IP Sockts are forced and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.										
Vulnerability Insight The renote host implements TCP timestamps, as defined by RPC1323. Vulnerability Detection Method Social IP packets are forced and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.										
Vulnerability Detection Method Sexcal IP coactasts are forced and sent with a little delay in between to the target IP. The responses are searched for a timestamos. If found, the timestamos are reported,										
Details: TCP timestamps (0ID: 1.3.6.1.4.1.25623.1.0.80091)										
Version used: sRevision: 7176 \$										
References	References									
Other: http://www.ietf.org/rfc/rfc1323.txt										

Figura 21. Vulnerabilitat TCP timestamps

En la següent part de l'anàlisi de vulnerabilitats escanejarem el servidor simulat amb Windows 2012 server. En aquest cas tornarem a crear una nova tasca, però en aquest cas indicarem la ip del servidor (192.168.1.190) a la finestra "New target".

Name	Scan SERVER		
Comment	windows 2012 server	r2	
Scan Targets	Server	× 🖸	
Alerts			
Schedule		▼ Once 😒	
Add results to Assets	💿 yes 🔵 no		
	Apply Overrides	💿 yes 🔵 no	
	Min QoD	70 🔹 %	
Alterable Task	🔵 yes 💿 no		
Auto Delete	 Do not automatical 	ly delete reports	
Reports	Automatically delet	te oldest reports but always keep newest 5 📄 reports	
Scanner	OpenVAS Default	Y	

Name	Server	
Comment	scan Win 2012 SERVER	
	 Manual 	192.168.1.190
Hosts	 From file 	Seleccionar un arxiu cap arxiu seleccionat
Exclude Hosts		
Reverse Lookup Only	Yes 💿 No	
Reverse Lookup Unify	🔿 Yes 💽 No	
Port List	All IANA assigned TCP 2012 🔻	
Alive Test	Scan Config Default 🔻	
Credentials for authenticated checks		
SSH		on port 22
SMB		
		- -

Figura 22. Nova tasca amb per analitzar el servidor

És recomanable identificar correctament les diferents tasques per a poder reutilitzarles sobre els equips desitjats. Una vegada creada la tasca podrem accedir als resultats i a les diferents accions des del llistat de tasques.



Greenbone Security Assistant						Refresh every 30 T	l in as Admin dani Logout hu Nov 9 01:02:39 2017 UTC
Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	Help
? 📉 🗙				Fi	Iter:	rtuname	
=							
Tasks (2 of 2)							2
- Tasks by S	Severity Class (Total: 2)	*	Tasks with most High	results per host	*	Tasks by status (Total: 2)	
C		High Low	No Tasks with High 1	severity found			Done
Name		Status	Reports		Severity	Trend	Actions
Client		Dane	Total	Last	N/A		
Scan SERVER		Done	1 (2)	Nov 8 2017	N/A		
(windows 2012 server r2)			- (-)				niv to page cost
(Applied filter: min_qod=70 apply_overrides=	1 rows=10 first=1 sort=name)						1 - 2 of 2

Figura 23. Llistat de tasques

Comprovem que els resultats de l'anàlisi en el servidor ens informa de dos vulnerabilitats greus i tres vulnerabilitats més de nivell moderat.

Security Assistant							No auto-refresh	 Logged in as Ad Thu Nov 9 	dmin dani Logout 00:56:02 2017 UTC
Dashboard	Scans	Assets	SecInfo	Configuratio	n	Extras	Administration		Help
👔 Anonymous X 🔻 🚺 😫 🗮 🐺 🕲	Done				Filter: autofp=0 apply_overrides- reverse=severity levels=hr	=1 notes=1 overrides=1 res ml min_qod=70	It_hosts_only=1 first=1 rows	=100 sort-	× ×
Report: Results	(5 of 66)						II M C O	b: a132dff2-b92e-48 odified: Wed Nov 8 23:22: reated: Wed Nov 8 23:06: wner: dani	59-8db0-95ac4e4f0071 48 2017 06 2017
									1 - 5 of 5
Vulnerability				S 🔁	Severity	🙆 QoD	Host	Location	Actions
MS15-034 HTTP.sys Remote Code Execu	tion Vulnerability (rem	ote check)			10.0 (High)	95%	192.168.1.190	80/tcp	🖂 🛸
Microsoft Windows SMB Server Multiple	Vulnerabilities-Remote	(4013389)			9.3 (High)	95%	192.168.1.190	445/tcp	🔛 🛸
DCE/RPC and MSRPC Services Enumerat	tion Reporting			2	5.0 (Medium)	80%	192.168.1.190	135/tcp	🔝 🛸
Use LDAP search request to retrieve info	ormation from NT Direct	tory Services		0	5.0 (Medium)	99%	192.168.1.190	3268/tcp	🖂 🛸
Use LDAP search request to retrieve info	ormation from NT Direc	tory Services		0	5.0 (Medium)	99%	192.168.1.190	389/tcp	2
(Applied filter:autofp=0 apply_overrides=1 note	s=1 overrides=1 result_hos	its_only=1 first=1 rows=100 sort-reverse=sever	ty levels=hml min_qod=70)					1	1 - 5 of 5

Backend operation: 2.64s

Figura 24. Resultats anàlisi vulnerabilitats Servidor

La primera vulnerabilitat greu ens informa d'un error reportat per el desenvolupador del sistema operatiu, Microsoft, que disposa de solució mitjançant actualització.

Ì	Security Assistant						No auto-refresh v	Logged in as Admin dani Logo Thu Nov 9 01:01:37 2017 UT
	Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	Help
	Result: MS15-0)34 HTTP.sys Ren	note Code Executio	on Vulnerability (re	emote check)		ID: Create Modifi Owner	e87a4ds8-136d-4d9a-bbbc-3619c601231 d: Wed Nov 8 23:18:47 2017 d: Wed Nov 8 23:18:47 2017 : dani
Vuln	erability				🔢 Severity	🙆 QoD	Host	Location Actions
MS15	-034 HTTP.sys Remote Code E	xecution Vulnerability (remote o	check)		10.0 (High)	95%	192.168.1.190	80/tcp 🔀 😹
Sum This I	mary host is missing an important se	ecurity update according to Micr	rosoft Bulletin MS15-034.					
Vulne Vulne	erability Detection Result erability was detected accordin	g to the Vulnerability Detection	Method.					
Impa Succe	act essful exploitation will allow re	mote attackers to run arbitrary	code in the context of the current	user and to perform actions in th	e security context of the current user.			
Solut Solut Run V Affect Micro	tion tion type: VendorFix Windows Update and update th cted Software/OS soft Windows 8 x32/x64 Micro	ne listed hotfixes or download an	nd update mentioned hotfixes in th osoft Windows Server 2012 Micros	he advisory from the below link, h	https://technet.microsoft.com/library/securi	ty/MS15-034 e Pack 2 and prior Microso	ft Windows 7 x32/x64 Service	Pack 1 and prior
Vuln Flaw	erability Insight exists due to the HTTP protoco	ol stack 'HTTP.sys' that is trigger	red when parsing HTTP requests.					
Vuln Send Detai	erability Detection Method a special crafted HTTP GET re ils: MS15-034 HTTP.sys Remot on used: \$Revision: 6431 \$	quest and check the response e Code Execution Vulnerability ((remote check) (OID: 1.3.6.1.4.1.)	25623.1.0.105257)				
Refe	rences							
CVE	: CVE-2015-1635	2015-0545						
Othe	er: https://support.microsoft.	com/kb/3042553						
	https://technet.microsoft.	com/library/security/MS15-034						
	http://pastebin.com/ypUR	DPc4						

Figura 25. Vulnerabilitat MS15-034 HTTP.sys execució de codi remot



El segon cas greu també reporta una vulnerabilitat reportada per Microsoft que permetria als atacants executar codi en el servidor mitjançant exploit que afecta el servidor Samba.

🔊 s	reenbone ecurity Assistar	t					No auto-refresh	 Logged in as Adm Thu Nov 9 0 	nin dani Logout 1:01:05 2017 UTC	
	Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration		Help	
?	₹ . €.									
Result: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)										
Vulner	ability				Severity	🙆 QoD	Host	Location	Actions	
Microso	ft Windows SMB Serv	r Multiple Vulnerabilities-Remote (40	13389)		9.3 (High)	95%	192.168.1.190	445/tcp	2 😹	
Summ This ho	ary st is missing a critical	security update according to Microsof	t Bulletin MS17-010.							
Vulnera Vulnera	ability Detection Re bility was detected as	sult cording to the Vulnerability Detection	Method.							
Impact Success	Impact Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.									
Impact	Impact Level: System									
Solutio Solutio Run Wi	Solution Solution type: Vendorfix Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010									
Affecto Microso x32/x64	d Software/OS ft Windows 10 x32/xi Edition Service Pack	4 Edition Microsoft Windows Server 2 2 Microsoft Windows Server 2008 R2	012 Edition Microsoft Windows Serv x64 Edition Service Pack 1 Microso	ver 2016 Microsoft Windows 8.1 : ft Windows Server 2008 x32/x64	x32/x64 Edition Microsoft Windows Server Edition Service Pack 2	2012 R2 Edition Microsoft W	indows 7 x32/x64 Edition	Service Pack 1 Microsoft	t Windows Vista	
Vulner Multiple	ability Insight flaws exist due to th	way that the Microsoft Server Messa	ge Block 1.0 (SMBv1) server handl	es certain requests.						
Vulner Send th	ability Detection M e crafted SMB transa	thod tion request with fid = 0 and check the	ne response to confirm the vulnerab	pility.						
Details:	Microsoft Windows S	MB Server Multiple Vulnerabilities-Rer	note (4013389) (OID: 1.3.6.1.4.1.2	25623.1.0.810676)						
Version	used: \$Revision: 622	3\$								
Refere	nces									
CVE:	CVE-2017-0143, CV	E-2017-0144, CVE-2017-0145, CVE-2	2017-0146, CVE-2017-0147, CVE-2	017-0148						
BID:	96703, 96704, 967	5, 96707, 96709, 96706								
CERT:	CB-K17/0435, DFN	CERT-2017-0448								
Other:	https://support.mic	osoft.com/en-in/kb/4013078								
	https://technet.mic	osoft.com/library/security/MS17-010								
	https://github.com/	apid7/metasploit-framework/pull/816	57/files							

Figura 26. Vulnerabilitats SMB Server 4013389

El següent avís de seguretat de grau mitjà està relacionat amb la possibilitat d'obtenció d'informació a partir d'una consulta LDAP.

Greenbone Security Assistant						No auto-refresh 🔹	Logged in as Admin dani Logout Thu Nov 9 00:56:52 2017 UTC
Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	Help
23 😨 🐿							
Result: Use LDA	P search reques	t to retrieve inform	ation from NT Dire	ectory Services		ID: Crea Modi Own	50fd79e7-31b6-4cd4-a905-bed47edd9500 ted: Wed Nov 8 23:15:06 2017 fied: Wed Nov 8 23:15:06 2017 er: dani
Vulnerability				🔢 Severity	🙆 QoD	Host	Location Actions
Use LDAP search request to retrieve	information from NT Directory	Services		2 5.0 (Kedium)	99%	192.168.1.190	3268/tcp 🔀 🛸
Summary It is possible to disclose LDAP inform	ation.						
Description :							
The directory base of the remote ser	ver is set to NULL. This allows i	nformation to be enumerated with	out any prior knowledge of the di	rectory structure.			
Vulnerability Detection Result The following information was p NTDS Settings, CN=SERVER, CN=Serv	ulled from the server via ers,CN=Default-First-Site-	a LDAP request: Name,CN=Sites,CN=Configuration	a, DC=TFG_SEGURETAT, DC=cat				
Solution Solution type: ^O Workaround							
If pre-Windows 2000 compatibility is	not required, remove pre-Wind	dows 2000 compatibility as follows	:				
- start cmd.exe							
- execute the command : net localgr	oup 'Pre-Windows 2000 Compa	tible Access' everyone /delete					
- restart the remote host							
Vulnerability Detection Method Details: Use LDAP search request to	retrieve information from NT D	irectory Services (OID: 1.3.6.1.4.1	.25623.1.0.12105)				
Consistent dagest proceedsion 1. 5150 a							

Figura 27. Vulnerabilitat divulgació informació LDAP



Aquesta segona vulnerabilitat correspon al mateix tipus de feblesa (obtenir informació mitjançant consulta LDAP). En aquest cas aquestes consultes es realitzen pel port 389 TCP.

Security Assistant						No auto-refresh 🔹	Logged in as Adm Thu Nov 9 00	in dani Logout :58:16 2017 UTC
Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	,	lelp
23 8								
Comparison of the second								
Vulnerability				🚼 Severity	🙆 QoD	Host	Location	Actions
Use LDAP search request to retrieve i	nformation from NT Director	y Services		2 5.0 (Hedium)	99%	192.168.1.190	389/tcp	2
Summary It is possible to disclose LDAP information	ation.							
Description :								
The directory base of the remote server is set to NULL. This allows information to be enumerated without any prior knowledge of the directory structure.								
Vulnerability Detection Result								
The following information was puntly Settings, CN=SERVER, CN=Server	ulled from the server vi ers,CN=Default=First=Sit	a a LDAP request: =-Name,CN=Sites,CN=Configuration,	,DC=TFG_SEGURETAT,DC=cat					
Solution Solution type: O Workaround								
If pre-Windows 2000 compatibility is	not required, remove pre-Wi	ndows 2000 compatibility as follows :						
- start cmd.exe								
- execute the command : net localgro	oup 'Pre-Windows 2000 Com	atible Access' everyone /delete						
- restart the remote host								
Vulnerability Detection Method Details: Use LDAP search request to r Version used: \$Revision: 5190 \$	retrieve information from NT	Directory Services (OID: 1.3.6.1.4.1.2	25623.1.0.12105)					

Figura 28. Vulnerabilitat divulgació informació LDAP 2

Per últim, els serveis RPC i DCE en funcionament en el servidor poden ser enumerats mitjançant una connexió al port 135 i les consultes corresponents.

٨	Greenbone Security Assistant						No auto-refresh 🔹	Logged in as Admin dani Logou Thu Nov 9 00:58:52 2017 UT
	Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	Help
20	Result: DCE/RP	PC and MSRPC Serv	vices Enumeration	Reporting			ID: Creat Modif Owne	63ddf126-30c9-495d-ae86-c5a2bc27c5e ed: Wed Nov 8 23:14:30 2017 ed: Wed Nov 8 23:14:30 2017 r: dani
Vuine	arability				Severity	🙆 QoD Ho	ost	Location Actions
DCE/	RPC and MSRPC Services Enum	eration Reporting		8	5.0 (Hedium)	80% 19	2.168.1.190	135/tcp 🔀 🛸
Sum Distri	mary buted Computing Environment	/ Remote Procedure Calls (DCE/R	RPC) or MSRPC services running o	n the remote host can be enume	rated by connecting on port 135 a	nd doing the appropriate queri	ies.	
Vuln	erability Detection Result							
Here	is the list of DCE/RPC or	MSRPC services running on the	his host via the TCP protoco	1:				
Port	49152/tcp							
	UUID: d95afe70-a6d5-4259-1 Endpoint: ncacn_ip_tcp:19	822e-2c84dalddb0d, version 1 2.168.1.190[49152]						
Port	49153/tcp							
	UUID: 30adc50c-5cbc-46ce- Endpoint: ncacn_ip_tcp:19 Annotation: NRP server en	9a0e-91914789e23c, version 1 2.168.1.190[49153] dpoint						
	UUID: 3c4728c5-f0ab-448b- Endpoint: ncacn_ip_tcp:19: Annotation: DHCP Client Li	bdal-6ce0leb0a6d5, version 1 2.168.1.190[49153] RPC Endpoint						
	UUID: 3c4728c5-f0ab-448b- Endpoint: ncacn_ip_tcp:19 Annotation: DHCPv6 Client	bdal-6ce0leb0a6d6, version 1 2.168.1.190[49153] LRPC Endpoint						
	UUID: abfb6ca3-0c5e-4734- Endpoint: ncacn_ip_tcp:19 Annotation: Wcm Service	9285-0aee72fe8dlc, version 1 2.168.1.190[49153]						
	UUID: f6beaff7-le19-4fbb- Endpoint: ncacn_ip_tcp:19 Annotation: Event log TCP	9f8f-b89e2018337c, version 1 2.168.1.190[49153] IP						
Port	49154/tcp							
	UUID: 1a0d010f=1c33=432c=1 Endpoint: ncacn_ip_tcp:19 Annotation: IdSegSrv serv	b0f5-8cf4e8053099, version 1 2.168.1.190[49154] ice						
	UUID: 2e6035b2-e8f1-41a7- Endpoint: ncacn_ip_tcp:19 Annotation: Proxy Manager	a044-656b439c4c34, version 1 2.168.1.190[49154] provider server endpoint						
	UUID: 3a9ef155-691d-4449- Endpoint: ncacn_ip_tcp:19	8d05-09ad57031823, version 1 2.168.1.190[49154]						





<i>.</i>	Dashboard	scans		Assets		Secinto
	UUID: 86d35949-83c9-4044-b424-db36 Endpoint: ncacn_ip_tcp:192.168.1.1	3231fd0c, ver: 90[49154]	sion 1			
	UUID: 98716d03-89ac-44c7-bb8c-2858 Endpoint: ncacn_ip_tcp:192.168.1.1 Annotation: XactSrv service	24e51c4a, ver 90[49154]	sion 1			
	UUID: c36be077-e14b-4fe9-8abc-e856 Endpoint: ncacn_ip_tcp:192.168.1.1 Annotation: Proxy Manager client s	ef4f048b, ver 90[49154] erver endpoint	sion 1 t			
	UUID: c49a5a70-8a7f-4e70-ba16-1e8f Endpoint: ncacn_ip_tcp:192.168.1.1 Annotation: Adh APIs	lf193ef1, ver 90[49154]	sion 1			
Fort	49155/top					
	UUID: 0b6edbfa-4a24-4fc6-8a23-942b Endpoint: ncacn_ip_tcp:192.168.1.1	leca65d1, ver: 90[49155]	sion 1			
	UUID: 12345678-1234-abcd-ef00-0123 Endpoint: ncscn_ip_tcp:192.168.1.1 Named pipe : spoolss Win32 service or process : spoolsv Description : Spooler service	456789ab, ver: 90[49155] .exe	sion 1			
	UUID: 4a452661-8290-4b36-8fbe-7f40 Endpoint: ncacn_ip_tcp:192.168.1.1	93a94978, ver 90[49155]	sion 1			
	UUID: 76f03f96-cdfd-44fc-a22c-6495 Endpoint: ncacn_ip_tcp:192.168.1.1	0a001209, ver: 90[49155]	sion 1			
	UUID: ae33069b-a2a8-46ee-a235-ddfd Endpoint: ncacn_ip_tcp:192.168.1.1	339be281, ver 90[49155]	sion 1			
Port	: 49156/tcp					
	UUID: 50abc2a4-574d-40b3-9d66-ee4f Endpoint: ncacn_ip_tcp:192.168.1.1 Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server	d5fba076, ver: 90[49156]	sion 5			
Port	49157/tcp					
	UUID: 367abb81-9844-35f1-ad32-98f0 Endpoint: ncacn_ip_tcp:192.168.1.1	38001003, ver 90[49157]	sion 2			
Port	49158/tcp					
	UUID: 5b821720-f63b-11d0-aad2-00c0 Endpoint: ncacn_ip_tcp:192.168.1.1	4fc324db, ver: 90[49158]	sion 1			
	UUID: 6bffd098-all2-3610-9833-46c3 Endpoint: ncacn_ip_tcp:192.168.1.1	f874532d, ver 90[49158]	sion 1			
Port	49159/tcp					
	UUID: 12345778-1234-abcd-ef00-0123 Endpoint: ncacn_ip_tcp:192.168.1.1 Named pipe : lsass Win32 service or process : lsass.e Description : SAM access	456789ac, ver: 90[49159] xe	sion 1			
Note	DCE/BPC or MSBPC services running	on this host	logally ware i	dontified R	emorting this 1	ist is not on

Figura 30. Vulnerabilitat enumeració serveis DCE/RPC 2

6.2 Proposta solució vulnerabilitats

Una vegada examinades les vulnerabilitats detectades en els dos equips simulats proposarem un llistat d'accions per dur a terme per tal de corregir aquestes debilitats.

- Equip simulat Client (Windows 7 Enterprise)
 - Desactivar timestamps TCP de Windows:
 - Netsh int tcp set global timestamps=disabled
 - http://www.microsoft.com/en-us/download/details.aspx?id=9152
 - Activar Windows Update per a futures actualitzacions de seguretat importants.
- Equip simulat Servidor (Windows 2012 Server R2)
 - Instal·lació actualització KB3042553 de https://support.microsoft.com/kb/3042553
 - Instal·lació actualització KB4013078 de https://support.microsoft.com/en-in/kb/4013078
 - Desinstal·lar compatibilitat pre-Windows 2000:
 - Inici > cmd.exe
 - Net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete



- Reiniciar l'equip
- Protegir els següents ports de connexions externes mitjançant regles al Firewall:
 - Rang de ports TCP: 49152 49159. Corresponen als ports que normalment s'assignen de forma dinàmica a les aplicacions del client. També s'utilitzen en connexions peer to peer (P2P).
- Activar Windows Update per a futures actualitzacions de seguretat importants.

6. Gestió remota

L'objectiu d'aquest dispositiu que incorpora el detector de vulnerabilitats OpenVas i el IDS Snort és la seva instal·lació en les organitzacions que ho requereixin. Per aquest motiu, al estar en ubicacions externes, requerirem d'un sistema de connexió remota per tal de dur a terme les tasques de gestió i manteniment necessàries.

Utilitzarem TeamViewer per tal de portar aquesta gestió remota. La seva instal·lació i configuració en en sistema Kali Linux és el següent:

apt-get install teamviewer

Teamviewer -info

Una vegada instal·lat podem veure el codi (ID) necessari per a la connexió remota mitjançant:

Per últim configurem la contrasenya per accedir a l'equip:

sudo teamviewer passwd <password>

Amb aquestes dades ja podrem accedir a l'equip des de qualsevol dispositiu amb connexió a internet.

TFG – Detecció de vulnerabilitats i intrusions a les xarxes de computadors



7. Conclusions

Universitat Oberta

de Catalunya

Finalitzat el projecte, i amb tot el treball realitzat, crec que s'han aconseguit els objectius plantejats inicialment. També s'han adquirit els coneixements necessaris per poder dissenyar un entorn simulat així com la configuració i posada en marxa d'un dispositiu que integri les eines proposades.

Inicialment es preveia la realització de les proves de vulnerabilitats amb un únic equip simulat, però es va considerar ampliar la mostra d'equips simulats per obtenir un resultat de les deteccions de vulnerabilitats que sigui el més pròxim a un entorn real. Aquesta ampliació ha permès analitzar un equip típic que realitza les funcions de servidor d'una petita organització amb un directori actiu d'usuaris i unitats de xarxa compartides així com un altra equip punt de treball que depèn del servidor on l'usuari realitza tasques ofimàtiques i de gestió.

Observant les vulnerabilitats detectades podem concloure que el servidor a presentat moltes més vulnerabilitats crítiques. Aquest fet es correspon a que es tracta d'un sistema operatiu orientat a oferir múltiples serveis de xarxa i cadascun d'ells requereix l'obertura d'una possible via d'entrada. Per aquest motiu és rellevant la correcta configuració dels serveis que s'utilitzaran així com tancar els serveis que no siguin necessaris.

També, a partir dels resultats de l'anàlisi extraiem la gran importància de mantenir els sistemes actualitzats amb les últimes correccions dels fabricants. Una correcta configuració d'aquestes actualitzacions evitarà exposar els sistemes a vulnerabilitats crítiques ja conegudes per la comunitat i corregides per els desenvolupadors del sistema operatiu.

Per una altra banda, es va modificar la implementació del IDS Snort amb la incorporació d'una interfície d'accés mitjançant web. D'aquesta manera millorem la visualització de les dades recollides per Snort per poder afrontar més ràpidament qualsevol alerta d'intrusió detectada.

Resumint, aquest projecte ens ha permès comprovar les múltiples deficiències de seguretat que poden incorporar els nostres equips informàtics. L'aparició constant de noves vulnerabilitats ens obliga a disposar d'eines que ens ajudin a comprovar la seguretat dels nostres equips. Amb els procediments inclosos en aquest projecte disposarem d'un dispositiu que proporcionarà les eines de seguretat per detectar vulnerabilitats i intrusions a qualsevol organització que ho requereixi. D'aquesta forma millorarem la seguretat davant possibles atacs informàtics i ajudarem al desenvolupament de xarxes de computadors més segures.





Universitat Oberta de Catalunya

8. Annexos

8.1 Preparació Raspberry Pi amb Kali Linux

1.- Preparació SD:

- Formatació targeta SD amb SD Formatter a FAT.
- Descarrega imatge Kali Linux for ARM RaspberryPi (https://www.offensive-security.com/kali-linux-arm-images/)
- Càrrega imatge a SD (ApplePi-Baker):

	ApplePi-Baker v1.9.4 - ©	2014-2017 Har	ns Luijten				
	C ApplePi-Baker www.Tweaking4Al.com Icon Design by Kray Mitchell Free MacOS X application for writing IMG files, compressed or not, to SD-cards and/or USB devices. Originally intended for Raspberry Pi users, but suitable for other applications as well.						
Baking IMG recipe 14.7 Mb/s - B	TA: 5 min. 59 sec.						
Pi-Crust : Select SD-Card or USI	3 drive	Pi-Ingredie	nts : IMG Recipe	(Restore)			
/dev/disk2 (31.9GB SD Card)		Resto IMG file: Progress:	Restore to selecte SD-Card (IMG, Zip kali-2017.2-rpi3-nexmon.	id USB drive or o, 7z, GZip). .img ore			
Pi-Ingredients : NOOBS Recipe	(Prepare)	Pi-in-the-F	reezer	(Backup)			
Prep for NOOBS Create si ready for	ngle FAT32 partiton (MBR) use with NOOBS.	Real Crea	ate Backup Backup selected U SD-Card (IMG, Zip	JSB drive or o, 7z, or GZip).			
For more information visit: <u>RaspberryPi.org</u> and/or <u>Tweaking4All.co</u>	om 8 Abort	Progress:					

Figura 32. ApplePi-Baker Càrrega imatge a SD

2.- Instalació SO:

- Una vegada iniciem la Raspberry Pi amb la SD s'inicia la instal·lació del sistema operatiu.
- Una primera mesura de seguretat és canviar el password del usuari root:
 o Comanda "passwd"

Una vegada tenim el sistema operatiu instal·lat ja podrem accedir mitjançant la seva IP amb una connexió SSH.



 Expansió de partició a la totalitat de la targeta SD (32GB). La imatge del Kali Linux ve per defecte en 8Gb:

```
• Utilitzem eina Parted:
```

```
root@kali:~# parted
GNU Parted 3.2
Using /dev/mmcblk0
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) print
Model: SD SC32G (sd/mmc)
Disk /dev/mmcblk0: 31.9GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
        Start
Number
                End
                        Size
                                 Туре
                                          File system
                                                        Flags
        512B
                64.0MB
                        64.0MB
                                          fat16
                                                        lba
1
                                 primary
2
        64.0MB
                7339MB
                        7275MB
                                 primary
                                          ext4
(parted)
```

Figura 33. Parted mostra particions de la targeta SD.

Comandes:

- print: mostra particions
- resizepart > partition: 2 > end: 31900 > quit

Per a canviar la mida de les particions també es poden utilitzar altres eines amb interfície gràfica com gparted, però per tal de minimitzar recursos optem per fer ús de les eines incloses a Kali Linux.

Per últim actualitzem el llistat de paquets i repositoris amb: sudo apt-get update.

8.2 Instal·lació OpenVas

Mitjançant una connexió SSH amb la Raspberry Pi realitzarem la instal·lació del sistema detector de vulnerabilitats OpenVas.

-	Instalació Openvas:	sudo apt-get install openvas sudo openvas-setup						
-	Comprovació instal·lació correcta: openvas-check-setup							
-	Creació usuari:	sudo openvasmd –create-user=dani –role=Admin sudo openvasmd –user=dani –new-password='****'						
-	Inici i aturada servei:	sudo openvas-start sudo openvas-stop						

Amb *netstat –antp* podem veure que el servei tcp de OpenVas ja es troba disponible a la ip 192.168.1.108:9390:

uoc.edu

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Wed Sep 27 08:20:46 2017 from 192.168.1.104 [root@kali:~# netstat -antp Active Internet connections (servers and established)								
Proto Re	cv-Q Se	nd-Q	Local Address	Foreign Address	State	PID/Program name		
tcp	0	0	192.168.1.108:9390	0.0.0.0:*	LISTEN	1503/openvasmd		
tcp	0	0	192.168.1.108:80	0.0.0.0:*	LISTEN	1504/gsad		
tcp	0	0	192.168.1.108:9392	0.0.0.0:*	LISTEN	1488/gsad		
tcp	0	0	127.0.0.1:5941	0.0.0.0:*	LISTEN	420/teamviewerd		
tcp	0	0	0.0.0:22	0.0.0.0:*	LISTEN	395/sshd		
tcp	0	0	127.0.0.1:5941	127.0.0.1:60994	ESTABLISHED	420/teamviewerd		
tcp	0	0	127.0.0.1:60994	127.0.0.1:5941	ESTABLISHED	600/TeamViewer		
tcp	0	196	192.168.1.108:22	192.168.1.104:64458	ESTABLISHED	15147/sshd: root@pt		
tcp6	0 _	0	:::22	:::*	LISTEN	395/sshd		
Figura 34. Serveis top								

Una vegada finalitzat i creat un usuari ja podrem accedir mitjançant el client Greenbone Security Assistant. Per accedir utilitzarem un navegador web amb la ip de l'equip i mitjançant el port 9392.



Figura 35. Accés al client Greenbone de OpenVas

Per accedir al portal web amb una IP fixa des de qualsevol equip dins de la mateixa xarxa seguirem els passos següents:

- Modificació dels serveis greenbone-security-assitant.service, openvasmanager.service, openvas-scanner.service amb l'ordre sed per reemplaçar la IP local 127.0.0.1 amb la IP que desitgem, en aquest cas 192.168.1.108:
 - sed –e 's/127.0.0.1/192.168.1.108/g' greenbone-securityassistant.service openvas-manager.service openvasscanner.service -i
- Després reiniciarem els serveis i daemons:



- systemctl daemon-reload
- systemctl restart greenbone-security-assistant.service openvasmanager.service openvas-scanner.service

Actualització de NVT (net vulnerability test) disponibles per al scanner:

- openvasmd –update && openvasmd –rebuild
- service openvas-scanner restart

Una vegada finalitzat totes les configuracions comprovem l'accés al client Greenbone:



Figura 36. Dashboard de Greenbone Security Assitant

8.3 Instal·lació Snort

Amb *sudo apt-get install snort* s'inicia la instal·lació. Ens demana el rang de IP de la nostra xarxa:



Figura 37. Configuració inicial Snort

uoc.edu



Universitat Oberta de Catalunya

```
root@kali:~# sudo apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
libblas-common libgfortran3 libjim0.76 libpcre16-3 libpoppler64 libqgsttools-p1 libqt5multimedia5-plugins
libqt5multimediaquick-p5 libqt5multimediawidgets5 libwireshark8 libwiretap6 libwsutil7 rename sgml-base xml-core
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
   libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries snort-rules-default
[Suggested packages:
   snort-doc
The following NEW packages will be installed:
   libdag2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 304 not upgraded.
Need to get 2102 kB of archives
After this operation, 5999 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive-4.kali.org/kali kali-rolling/main armhf libdag2 armhf 2.0.4-3+b1 [60.6 kB]
Get:2 http://archive-4.kali.org/kali kali-rolling/main armhf libdumbnet1 armhf 1.12-7+b1 [23.2 kB]
Get:3 http://archive-4.kali.org/kali kali-rolling/main armhf snort-common-libraries armhf 2.9.7.0-5 [594 kB]
Get:4 http://archive-4.kali.org/kali kali-rolling/main armhf snort-rules-default all 2.9.7.0-5 [341 kB]
Get:5 http://archive-4.kali.org/kali kali-rolling/main armhf snort-common all 2.9.7.0-5 [243 kB]
Get:6 http://archive-4.kali.org/kali kali-rolling/main armhf snort armhf 2.9.7.0-5 [750 kB]
Get:7 http://archive-4.kali.org/kali kali-rolling/main armhf snort armhf 2.9.7.0-5 [750 kB]
Get:7 http://archive-4.kali.org/kali kali-rolling/main armhf oinkmaster all 2.0-4 [90.6 kB]
Fetched 2102 kB in 1s (1610 kB/s)
Preconfiguring packages .
Selecting previously unselected package libdaq2.
(Reading database ... 157728 files and directories currently installed.)
Preparing to unpack .../0-libdaq2_2.0.4-3+b1_armhf.deb ...
Unpacking libdaq2 (2.0.4-3+b1)
Selecting previously unselected package libdumbnet1:armhf.
Preparing to unpack .../1-libdumbnet1_1.12-7+b1_armhf.deb ...
Unpacking libdumbnet1:armhf (1.12-7+b1) ..
Selecting previously unselected package snort-common-libraries.
Preparing to unpack .../2-snort-common-libraries_2.9.7.0-5_armhf.deb ...
Unpacking snort-common-libraries (2.9.7.0-5) ..
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../3-snort-rules-default_2.9.7.0-5_all.deb ...
Unpacking snort-rules-default (2.9.7.0-5) ..
Selecting previously unselected package snort-common.
Preparing to unpack .../4-snort-common_2.9.7.0-5_all.deb ...
Unpacking snort-common (2.9.7.0-5) ...
Selecting previously unselected package snort.
Preparing to unpack ... /5-snort_2.9.7.0-5_armhf.deb ...
Unpacking snort (2.9.7.0-5) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../6-oinkmaster_2.0-4_all.deb ...
Unpacking oinkmaster (2.0-4) ...
Setting up oinkmaster (2.0-4) ...
Setting up snort-common (2.9.7.0-5)
Setting up short-common (2.9.7.0-3) ...
Setting up libdaq2 (2.0.4-3+b1) ...
Processing triggers for libc-bin (2.24-17) ...
Processing triggers for systemd (234-3) ...
Setting up libdumbnet1:armhf (1.12-7+b1)
Processing triggers for man-db (2.7.6.1-2)
Setting up snort-common-libraries (2.9.7.0-5) ...
Setting up snort (2.9.7.0-5) ...
update-rc.d: We have no instructions for the snort init script.
update-rc.d: It looks like a network service, we disable it. Processing triggers for libc-bin (2.24-17) ...
Processing triggers for systemd (234-3)
```

Figura 38. Procés instal·lació Snort

Una vegada instal·lat, podem configurar les seves opcions i regles a l'arxiu: *sudo nano /etc/snort/snort.conf*

Les regles creades per nosaltres o les descarregades aniran ubicades a: /etc/snort/rules

Les alertes que produeix Snort es registren a l'arxiu "alert" dins de /var/log/snort

Per executar Snort: *snort –c /etc/snort/snort.conf –l /var/log/snort* on *–c* indica l'arxiu de regles i *–l* el directori on ubiquem el log.



Universitat Oberta de Catalunya



9. Referències

[1] Raspberry Pi 3 Model B [En línia] [Data: 30 / octubre / 2017] https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

[2] Kali Linux [En línia] [Data: 30 / octubre / 2017] https://www.kali.org/downloads/

[3] Snort [En línia] [Data: 30 / octubre / 2017] https://www.snort.org

[4] Nessus [En línia] [Data: 22 / octubre / 2017] https://www.tenable.com/products/nessus-vulnerability-scanner

[5] OpenVas [En línia] [Data: 20 / octubre / 2017]: http://www.openvas.org

[6] Detecting malware through DNS queries: a Kali Pi / Snort Project [En línia] [Data: 2 / gener / 2015] https://www.securityforrealpeople.com/2015/01/detecting-malware-through-dnsqueries.html

[7] Turn your Raspberry Pi into a Snort IDS [En línia] [Data: 25 / octubre / 2016] https://blog.holdenkilbride.com/index.php/2016/10/25/turn-your-raspberry-pi-into-asnort-ids/

[8] Kali Linux Custom ARM Images [En línia] [Data: 3 / novembre / 2017] https://www.offensive-security.com/kali-linux-arm-images/

[9] IDS Sistema de detección de intrusos [En línia] [Data: 30 / novembre / 2017] https://es.wikipedia.org/wiki/Sistema de detección de intrusos

[10] OpenVas en Linux [En línia] [Data: 30 / maig / 2014] https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

[11] Steps to Install and configure Snort on Kali Linux [En línia] [Data: 2 / desembre / 20141

https://techcyberz.wordpress.com/2014/12/02/steps-to-install-and-configure-snort-onkali-linux/

[12] How to use OpenVas to audit [En línia] [Data: 22 / novembre / 2016] https://komunity.komand.com/learn/article/how-to-use-openvas-to-audit-the-security-ofyour-network-22/

TFG - Detecció de vulnerabilitats i intrusions a les xarxes de computadors

[13] OpenVas self-fingerprint [En línia] [Data: 27 / agost / 2014] http://kinomakino.blogspot.com.es/2014/08/openvas-self-fingerprint-maquillandoal.html

[14] OpenVas vulnerability scanner on the Raspberry Pi [En línia] [Data: 27 / novembre / 2017]

https://cromwell-intl.com/linux/raspberry-pi/openvas.html

[15] How to install Snorby in Kali [En línia] [Data: 21 / novembre / 2014] <u>http://www.ylabs.co.kr/index.php?document_srl=37892&mid=board_net_forensics&list</u> <u>Style=viewer</u>

[16] Administración de sistemes operatives Snort-BASE [En línia] [Data: gener / 2015] <u>http://adminso.es/index.php/Snort-BASE</u>

[17] Aumentando el rendimiento de Snort con Barnyard2 [En línia] [Data: 30/ març / 2011]

http://www.hackplayers.com/2011/03/aumentando-el-rendimiento-de-snort-con.html

[18] Actualización automática de reglas Snort con PulledPork [En línia] [Data: 27/ gener / 2017]

http://www.securityartwork.es/2017/01/27/actualizacion-automatica-reglas-snort-pulledpork/



10. Glossari

DNS: Servidor que s'encarrega de la traducció dels noms de les web a direccions IP.

Firewall: Programa o hardware informàtic configurable per al bloqueig i filtratge del trànsit d'una xarxa.

GUI: Interfície gràfica d'usuari. Representa la informació mitjançant l'ús de gràfics i imatges per tal de presentar la informació a l'usuari.

IDS: Sistema de detecció d'intrusions. Aquests sistemes es basen en l'anàlisi del trànsit de dades i la detecció de patrons coneguts per activar les alarmes corresponents.

LDAP: Protocol lleuger d'accés a directoris. És un protocol a nivell d'aplicació que permet l'accés a un servei de directori ordenat i distribuït.

Linux: És un dels termes utilitzats per englobar la combinació d'un kernel (nucli) amb el sistema GNU. El seu codi font pot ser utilitzat, modificat i redistribuït lliurement per qualsevol sota els termes de la llicència pública general de GNU (GPL) i altres tipus de llicències lliures.

MySQL: Sistema de gestió de bases de dades relacionals desenvolupat sota llicència dual (GPL i llicència comercial) per Oracle Corporation. És considerada com la base de dades open source més popular del mon.

Open source: Expressió amb la que es coneix el programari distribuït i desenvolupat sota el paradigma del programari lliure. Habitualment dóna referència a l'accés total al codi font d'un programari.

RAM: Memòria utilitzada com a memòria de treball per al programari instal·lat en un ordinador. Les seves sigles provenen de l'anglès Randorm-Access Memory.

Root: Compte d'usuari amb privilegis d'administrador.

Sniffer: Programa informàtic que registra tota la informació que envien els equips en una xarxa.

SSH: Secure Shell o intèrpret d'ordres segura, és el nom del protocol i del programa que l'implementa. La seva funcionalitat radica en proporcionar accés a màquines remotes mitjançant una xarxa. Permet gestionar completament l'ordinador mitjançant l'intèrpret d'ordres.



VirtualBox: Programari de virtualització que permet la creació de màquines virtuals operatives. Desenvolupat per Oracle Corporation.

VM: Inicials de Virtual Machine. Referent a la capacitat d'instal·lar un sistema operatiu dins d'un altre.