

ESTABLIMENT D'UN SITE SEGUR AMB HONEYNET ADJACENT

Desplegament virtualitzat en entorn stand alone

Coneix el teu enemic i coneix-te a tu mateix i podràs lluitar mil batalles sense perdre. (L'art de la Guerra, Sun Wu Tzu, 544/496 AC)

- Alumne: Josep Caballé i Ràmia
- Consultor: Jordi Guijarro Olivares
- Període: Setembre 2016/Gener 2017

Precedents: qüestionament metodològic

Apareixen dubtes raonables en qüestionar-se la seguretat pel que fa a la compartició de dades confidencials:

- COM: s'utilitza una eina adient, el canal és segur....?
- QUI: accessos no autoritzats, control d'activitats, suplantació d'identitat... ?
- ON: es desen les dades, des de quins dispositius s'hi accedirà... ?
- VALOR: signatura digital, *timestamp*, certificació... ?
- FINS: quant de temps seran publicades, es podrà recuperar contingut...?



Resposta: creació d'un entorn segur

Establiment d'un *site* -DeepTicies- basat en eines de programari lliure, que un cop integrades, ofereixin una plataforma assegurada, accessible per a multitud de clients.



VirtualBox

Plataforma per al desplegament i control de servidors virtuals.



Establiment de canal segur.



Gestió del *site* amb control d'usuaris i continguts.

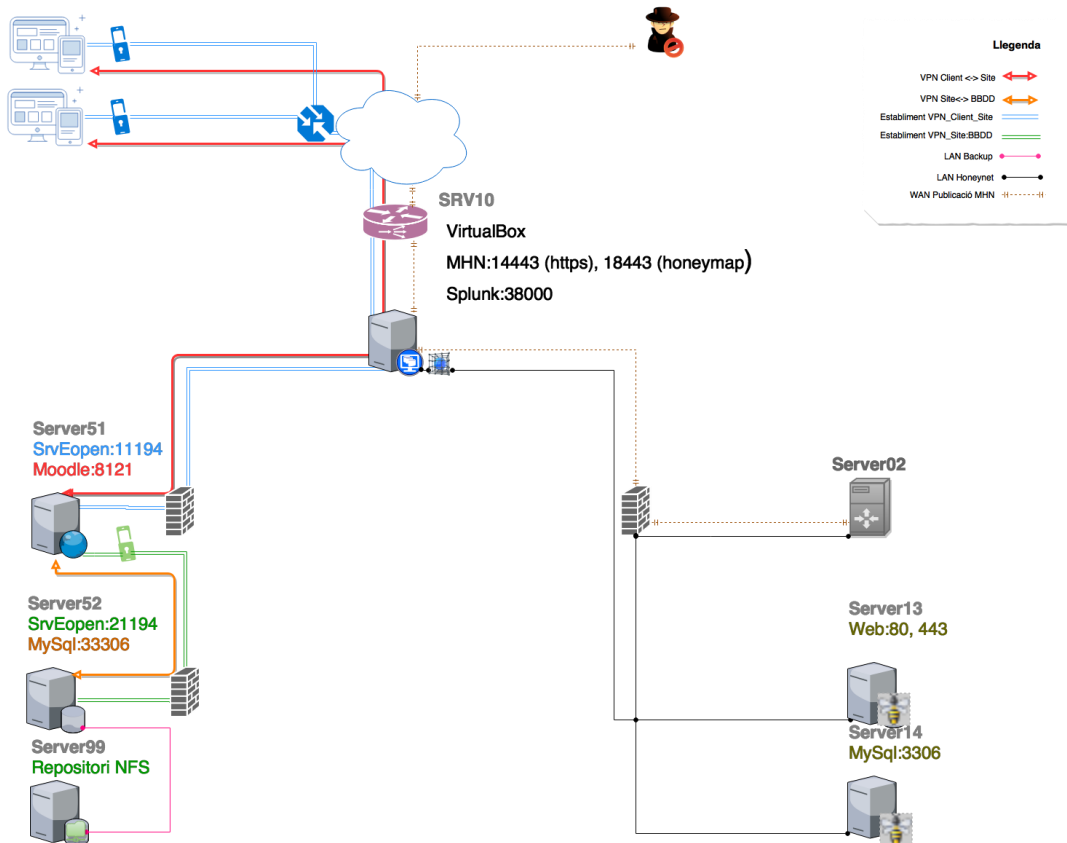


Derivació d'atacs a entorn d'anàlisi.



Presentació i explotació de les dades capturades.

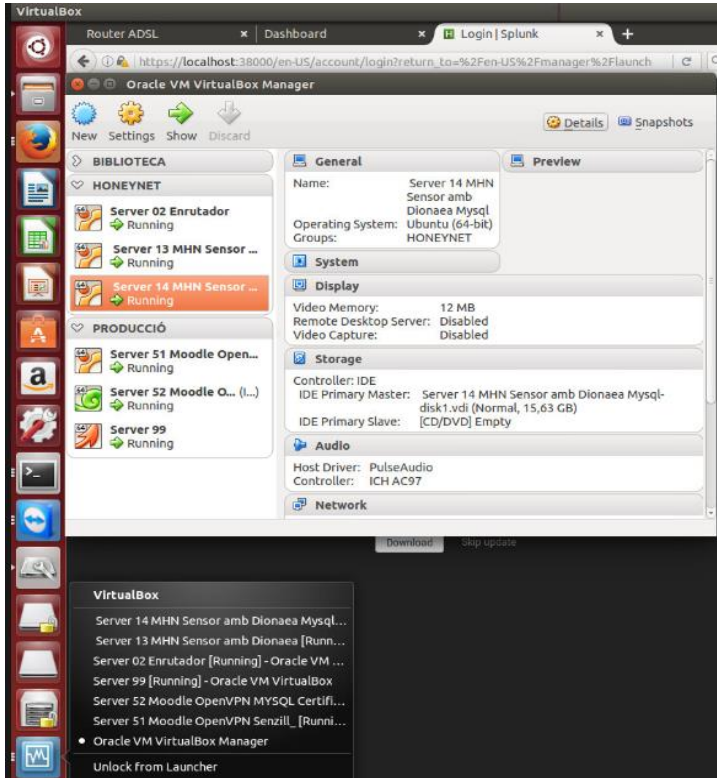
Enginyeria: arquitectura de xarxa



Es creen dos entorns de treball, per a donar accés als clients lícits i ciberatacants:

- Legal (inferior esquerra): comunicacions segures, validació usuaris i securització de dades.
- Esquer (inferior dret): desviació activitats malicioses, captura de dades i anàlisi.

Entorn lògic: disposició de les VM's



Dins una sola màquina física s'ubica el host i els sis servidors virtuals, tots ells amb els serveis assegurats, *hardering*.

- SRV10: VirtualBox Host, MHN Host, Splunk
- Server51: Moodle, iptables
- Server52: MySql, iptables
- Server99: NFS, Backup
- Server02: Routing, iptables
- Server13: Honeypot, Sensor:Dionaea WEB

OpenVPN: establiment del canal segur



Client - Site

Site - BBDD

```
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.18.0.1 P-t-P:10.18.0.2 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

tun1 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.28.0.6 P-t-P:10.28.0.5 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

kuse@Server51:/etc/openvpn$
```

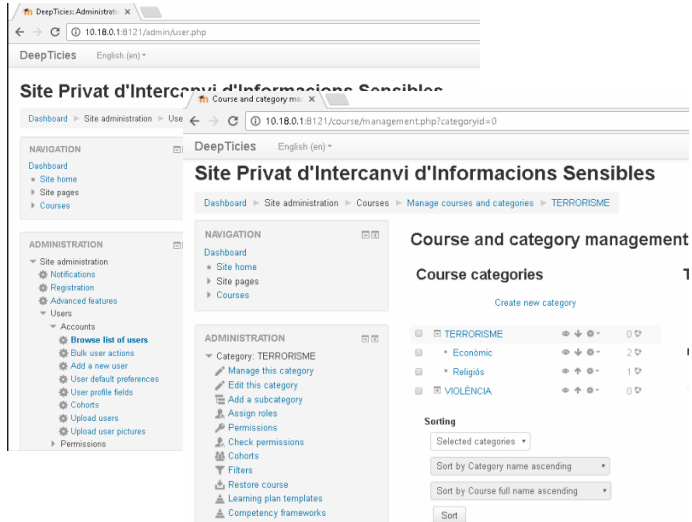
```
tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.28.0.1 P-t-P:10.28.0.2 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

kuse@Server52:~$
```

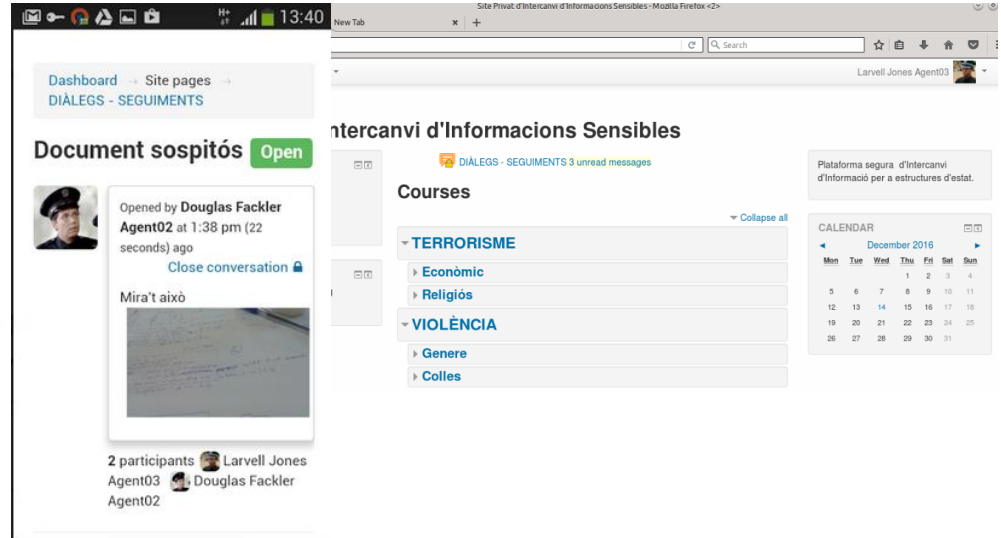
Per tal de poder accedir al portal DeepTicies caldrà tenir establerts dos canals de comunicació, túnels.

Moodle: accés al portal

Un cop validat l'usuari a la plataforma disposarà dels recursos pertinents segons els rols assignats.



This screenshot shows the Moodle administrator interface. The browser address bar displays '10.18.0.18121/admin/user.php'. The page title is 'Site Privat d'Intercanvi d'Informacions Sensibles'. The left sidebar contains navigation and administration menus. The main content area is titled 'Course and category management' and shows a tree structure of course categories: 'TERRORISME' (with sub-categories 'Econòmic' and 'Religiós'), and 'VIOLÈNCIA'. A 'Sorting' section at the bottom allows filtering by category name or course name.



This screenshot shows the Moodle user interface. The browser address bar displays 'Site Privat d'Intercanvi d'Informacions Sensibles - Mozilla Firefox'. The page title is 'Intercanvi d'Informacions Sensibles'. The left sidebar contains navigation and administration menus. The main content area is titled 'Document sospitós' and shows a document titled 'Document sospitós' opened by 'Douglas Fackler Agent02' at 1:38 pm. The document content is a blurry image of a document. Below the document, it shows '2 participants' and lists 'Larvell Jones Agent03' and 'Douglas Fackler Agent02'. The right sidebar contains a 'Courses' section with a list of categories: 'TERRORISME', 'Econòmic', 'Religiós', 'VIOLÈNCIA', 'Gènere', and 'Colles'. A 'CALENDAR' section shows a calendar for December 2016.

Des del nivell d'administració, gestionant aules i rols, entre moltes altres possibilitats...

...fins al nivell d'usuari consultant la interfície personalitzada o, entre d'altres enviant missatges des del mòbil.

Moodle: registre de seguretat i *backup*

Totes les activitats, de cada usuari, realitzades dins la plataforma són registrades i és possible fer-ne consulta. Així com exportar el registre en diferents formats.

Site Privat d'Intercanvi d'Informacions Sensibles (Site) Douglas Fackler Agent02 Today, 14 December 2016 All activities

All actions All events Get these logs

Time	User full name	Affected user	Event context	Component	Event name	Description	Origin	IP address
14 Dec, 13:39	Douglas Fackler Agent02	-	Dialogue: DIÀLEGS - SEGUIMENTS	Dialogue	Conversation viewed	The user with id '7' has viewed the conversation with id '8' in the dialogue with the course module id '4'.	web	10.18.0.14
14 Dec, 13:38	Douglas Fackler Agent02	-	Dialogue: DIÀLEGS - SEGUIMENTS	Dialogue	Course module viewed	The user with id '7' viewed the 'dialogue' activity with course module id '4'.	web	10.18.0.14
14 Dec, 13:38	Douglas Fackler Agent02	-	Dialogue: DIÀLEGS - SEGUIMENTS	Dialogue	Conversation created	The user with id '7' has created the conversation with id '8' in the dialogue with the course module id '4'.	web	10.18.0.14
14 Dec, 13:38	Douglas Fackler Agent02	Larvell Jones Agent03	System	System	Message sent	The user with id '7' sent a message to the user with id '8'.	web	10.18.0.14
14 Dec, 13:38	Douglas Fackler Agent02	Larvell Jones Agent03	System	System	Email failed to send	Failed to send an email from the user with id '7' to the user with id '8' due to the following error: "Could not instantiate mail function."	web	10.18.0.14
14 Dec, 13:38	Douglas Fackler Agent02	-	Dialogue: DIÀLEGS - SEGUIMENTS	Dialogue	Course module viewed	The user with id '7' viewed the 'dialogue' activity with course module id '4'.	web	10.18.0.14

Download table data as

Comma separated values (.csv)
Comma separated values (.csv)
Microsoft Excel (.xlsx)
HTML table
Javascript Object Notation (.json)
OpenDocument (.ods)

Download

DeepTicies English (en)

Josep Caballé i Ràmia SysAdmin

Backup course: DeepTicies

Dashboard > Front page settings > Backup

NAVIGATION

Dashboard
Site home
Site pages
Courses

1. Initial settings > 2. Schema settings > 3. Confirmation and review > 4. Perform backup > 5. Complete

The backup file was successfully created.

Continue

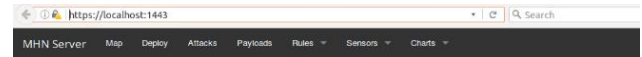
La pròpia eina també disposa d'una senzilla funció de realització de còpia de seguretat.

MHN: resposta als atacs



Qualsevol petició que no s'inscriu dins l'estàndard apuntat fins ara no tindrà resposta, excepte les fetes als ports 80, 443 i 3306, que seran derivades a la xarxa esquer, gestionada pel programari Modern Honey Network.

Aquesta xarxa presentarà un entorn simulat i anirà recollint els rastres deixat per les activitats dels cibercriminals



Attack Stats

Attacks in the last 24 hours: **281**

TOP 5 Attacker IPs:

- 211.147.118.113 (79 attacks)
- 116.7.104.165 (53 attacks)
- 211.147.112.141 (31 attacks)
- 139.196.212.102 (30 attacks)
- 60.222.217.239 (12 attacks)

TOP 5 Attacked ports:

- 3306 (190 times)
- 80 (91 times)

TOP 5 Honey Pots:

- dionaea (281 attacks)

TOP 5 Sensors:

- Server14 (190 attacks)
- Server13 (91 attacks)

Attacks Report

Search Filters

Sensor	Honeypot	Date	Port	IP Address	
All	All	MM-DD-YYYY	443	8.8.8.8	Go

Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot	
1	2016-12-14 22:19:12	Server14		111.121.193.223	3306	mysql	dionaea
2	2016-12-14 21:42:23	Server13		180.97.106.37	80	http	dionaea
3	2016-12-14 20:56:15	Server14		125.88.146.10	3306	mysql	dionaea
4	2016-12-14 20:49:09	Server13		92.0.181.214	80	http	dionaea
5	2016-12-14 18:41:54	Server14		139.182.37.156	3306	mysql	dionaea

Splunk: anàlisi de dades recol·lectades

El programari Splunk facilita la generació d'informes i filtratge de dades, a part que la seva integració amb els *honeypots* desplegats és total.

