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.

Plataforma per al desplegament i control de servidors virtuals.

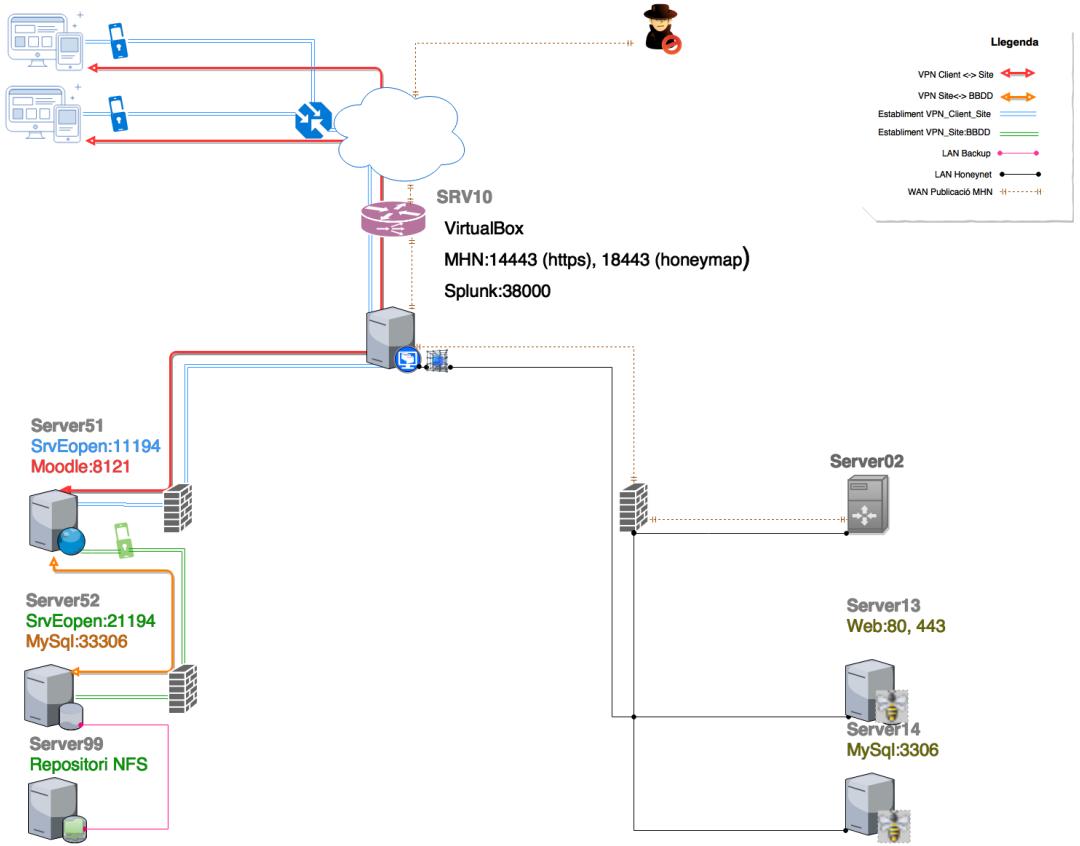
Establiment de canal segur.

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

Derivació d'atacs a entorn d'anàlisi.

Presentació i explotació de les dades capturades.

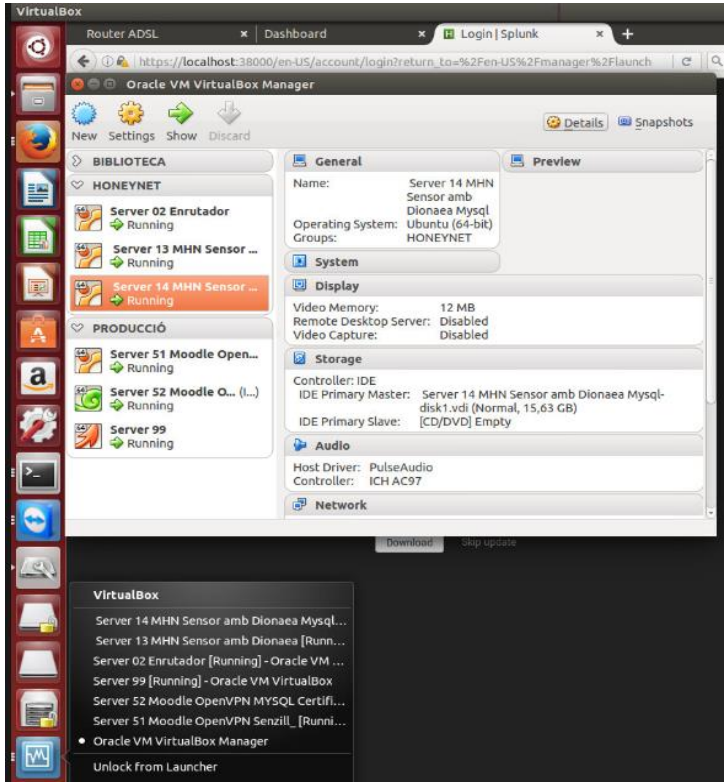
Enginyeria: arquitectura de xarxa



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.

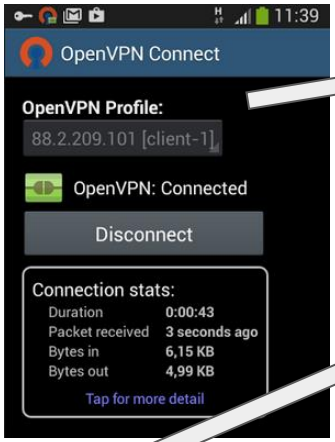
Entorn lògic: disposició de les VM's



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$
```

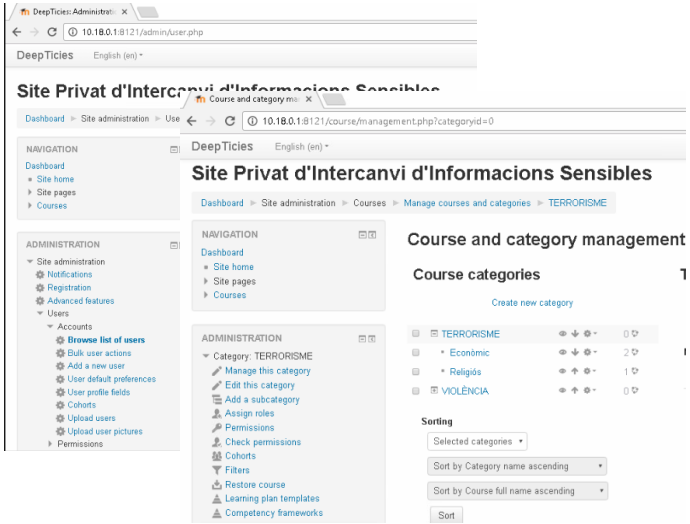
```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.28.0.1  P-t-P:10.28.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 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:~$
```

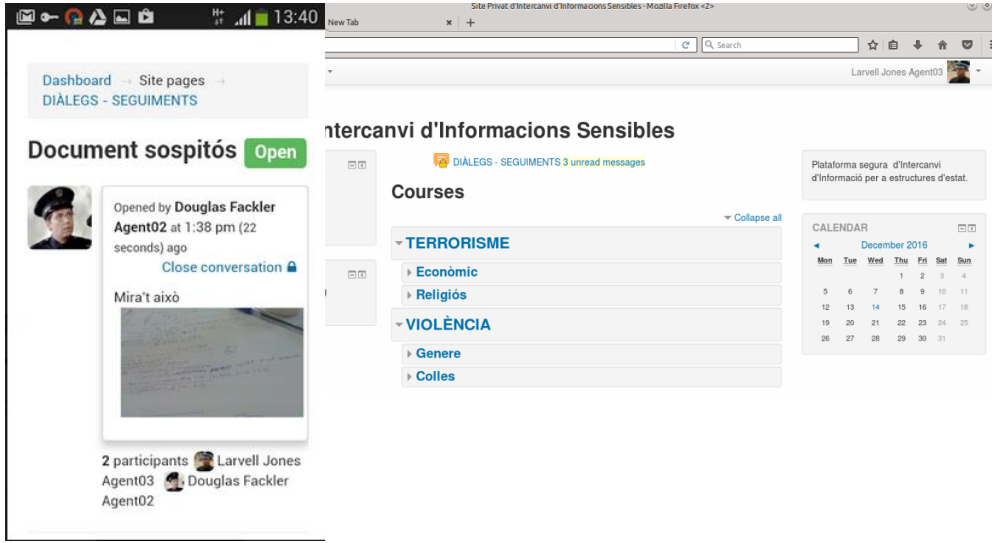
Per tal de poder accedir al portal DeepTicies caldrà tenir establerts dos canals de comunicació, túnels.

Moodle: accés al portal

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



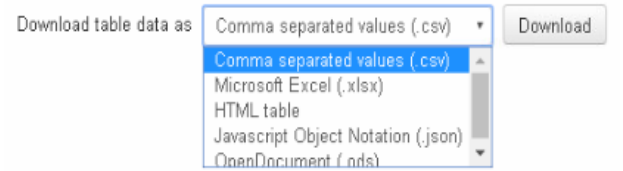
Des del nivell d'adminstració, gestionant aules i rols, entre moltes altres possibilitats...

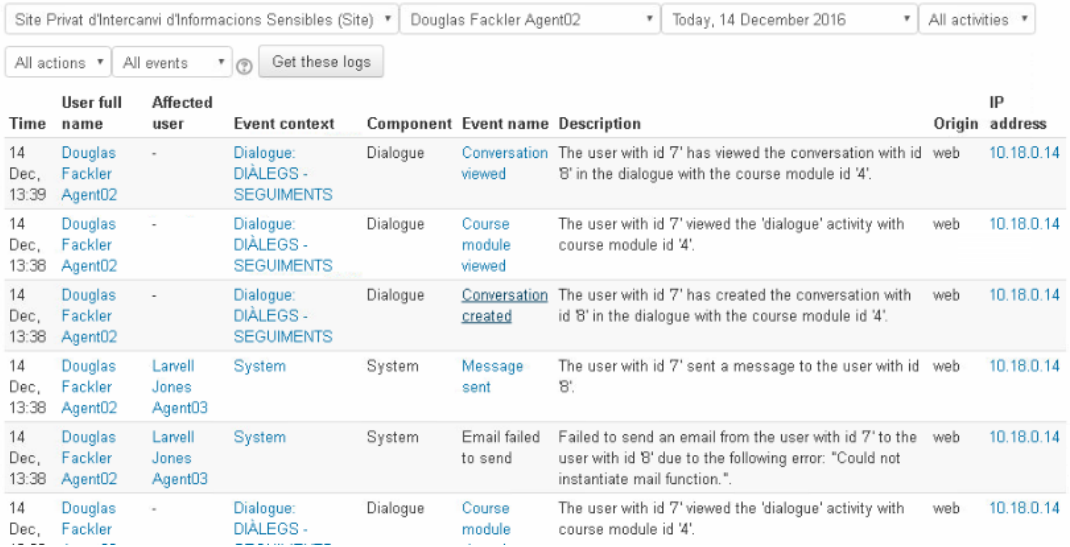


...fins al nivell d'usuari consultant la interfície personalitzada o, entre d'altres enviant missatges des del mòbil.

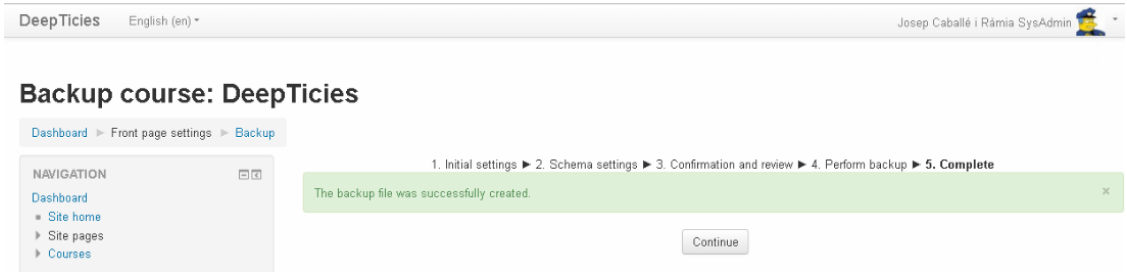
Moodle: registre de seguretat i *backup*

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.





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,	Douglas Fackler	-	Dialogue: DIÀLEGS -	Dialogue	Course module	The user with id '7' viewed the 'dialogue' activity with course module id '4'.	web	10.18.0.14

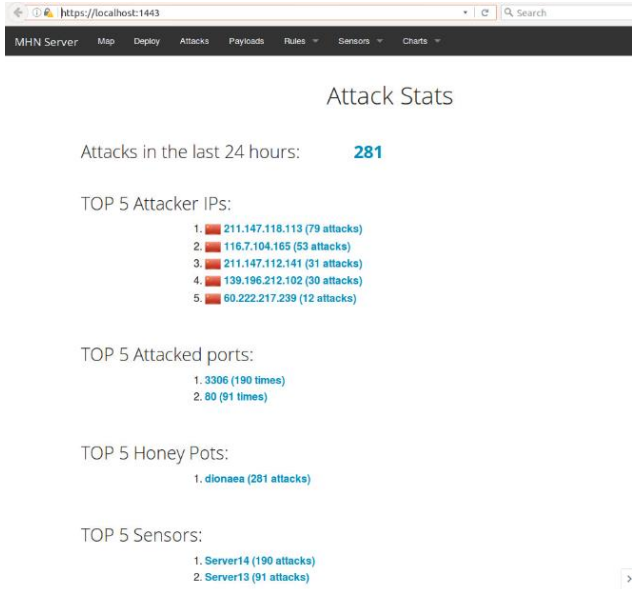


La pròpia eina també disposa d'una senzilla funció de realització de còpia de seguretat.

MHN: resposta als atacs

Qualsevol petició que no s'inscrigui 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 recol·lectant els rastres deixat per les activitats dels cibercriminals



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.