



# EUSK@LERT: INFORME PRELIMINAR

## INTRODUCCIÓN

Se ha instalado una infraestructura *Eusk@lert*<sup>1</sup> completa en la Escuela Politécnica Superior de Mondragón Unibertsitatea en Arrasate. La arquitectura montada está basada en el modelo de *The HoneyNet Project*<sup>2</sup> (ver Anexos), que consta de un sensor (cliente HoneyMole), un servidor de túneles encriptados (servidor HoneyMole), un IDS Snort<sup>3</sup> (HoneyWall) y un *honeypot* que integra Nepenthes<sup>4</sup> y Honeytrap<sup>5</sup>. El sensor escucha en una dirección IP pública concreta y reenvía al *honeypot* todo el tráfico dirigido a la misma a través de un túnel encriptado. Snort se encuentra entre ambos elementos registrando todas las alertas y sesiones, mientras Nepenthes y Honeytrap manejan las conexiones (el primero emulando servicios y vulnerabilidades conocidas y el segundo monitorizando el resto de puertos) y capturan gusanos, troyanos y malware en general.

Se ha sometido la infraestructura a un período de prueba. La dirección IP pública utilizada en el testeo no ofrece ningún servicio público válido ni conocido para ningún usuario, de lo que se deduce que la mayor parte de las conexiones externas dirigidas a dicha dirección son maliciosas. Snort ha registrado detalladamente múltiples sesiones con destino a la IP anteriormente citada. Además, el *honeypot* ha sido víctima de varios intentos de descarga de malware, de los que alguno ha sido exitoso. Este conjunto de información importante ha sido obtenida sin que la seguridad del sistema haya corrido riesgo alguno: la emulación de servicios de Nepenthes impide que la infraestructura pueda ser comprometida y usada como puente para intrusiones a la red interna. Asimismo, el test ha demostrado la robustez de *Eusk@lert*: ha funcionado ininterrumpidamente durante varios días soportando múltiples conexiones y captando varios virus de diferente naturaleza.

Tal y como se ha demostrado durante el período de prueba, ninguna red está a salvo de las amenazas que constantemente provienen de Internet. Sin embargo, poseer cierto conocimiento e información sobre los ataques de los que se es víctima ayuda enormemente a tomar medidas para reducir al mínimo el impacto causado por dichas amenazas. *Eusk@lert* provee esta información, lo que le convierte en un sistema de una gran validez para el cumplimiento de los objetivos propuestos al inicio.

## CONEXIONES Y SESIONES CAPTURADAS

Durante el período de prueba se han registrado multitud de conexiones dirigidas a muchos puertos diferentes. Algunos de ellos están reservados para determinados servicios emulados por Nepenthes. En el resto de puertos corren servicios que no están siendo emulados por el *honeypot*, pero cuyas conexiones sí están siendo aceptadas por Honeytrap, permitiendo de este modo el registro de los mensajes y malware enviados a través de ellas. Tener un conocimiento exhaustivo sobre los puertos del sistema interno hacia

---

<sup>1</sup> [www.euskalert.net](http://www.euskalert.net)

<sup>2</sup> [www.honeynet.org](http://www.honeynet.org)

<sup>3</sup> [www.snort.org](http://www.snort.org)

<sup>4</sup> [nepenthes.mwcollect.org](http://nepenthes.mwcollect.org)

<sup>5</sup> [honeytrap.mwcollect.org](http://honeytrap.mwcollect.org)



los que se establecen conexiones externas y sobre los servicios que corren en ellos es vital porque éstos son ofrecidos por aplicaciones cuyas vulnerabilidades suelen ser explotadas durante los ataques.

Las gráficas que se presentan a continuación muestran las conexiones y sesiones (o intentos de establecerlas) registradas a o desde determinados servicios del *honeypot* durante varios días:

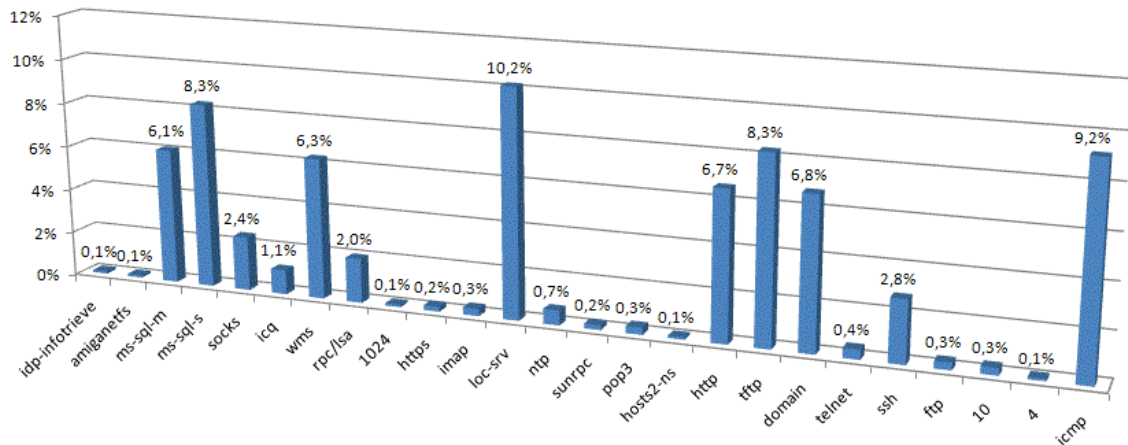


Figura 1: Sesiones relacionados con determinados servicios.

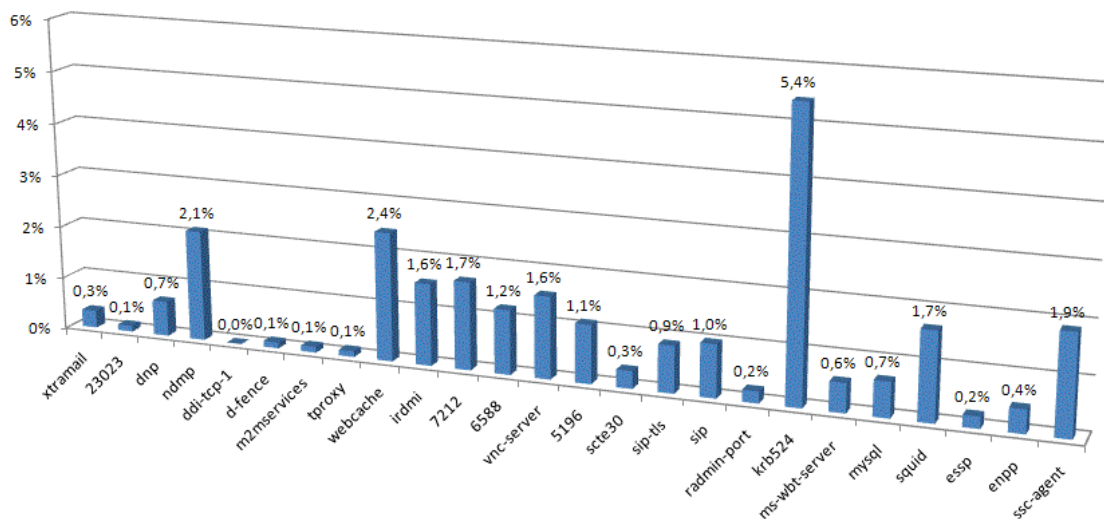


Figura 2: Sesiones relacionados con otros servicios.

Como puede observarse, existen multitud de conexiones a diversos puertos que en teoría no debían existir puesto que esa dirección IP no ofrece ningún servicio que sea público. Es posible que muchas aplicaciones que ofrecen servicios en los puertos implicados en las conexiones de las gráficas tengan ciertas vulnerabilidades explotables por un atacante. *Eusk@lert* alerta sobre servicios que pueden ser potenciales víctimas de ataques facilitando trabajo a los administradores de sistemas. Como ejemplo, basta fijarse en las grandes cantidades de tráfico registrado en los servicios tftp y loc-srv en la Figura 1, y en krb524 en la Figura 2. Estos puertos son lo utilizados por el gusano Win32/Lovsan – más conocido



como Blaster – para propagarse en Internet y lanzar sus ataques. Una correcta eliminación de las vulnerabilidades que afectan a dichos servicios contribuye a minimizar los daños causados por este y otros gusanos y a ralentizar su propagación en Internet.

## INFECCIONES DE VIRUS

Tal y como se ha expuesto en el anterior apartado, muchas de las conexiones externas tienen como objetivo infectar el equipo al que van dirigidas. Estas infecciones están causadas por virus que pueden ser gusanos, troyanos, puertas traseras, herramientas DoS etc. Nepenthes se encarga de capturar ese malware para su posterior análisis.

A continuación se presentan los virus que se han sido detectados por Nepenthes y el porcentaje en el que de incidencias de los mismos:

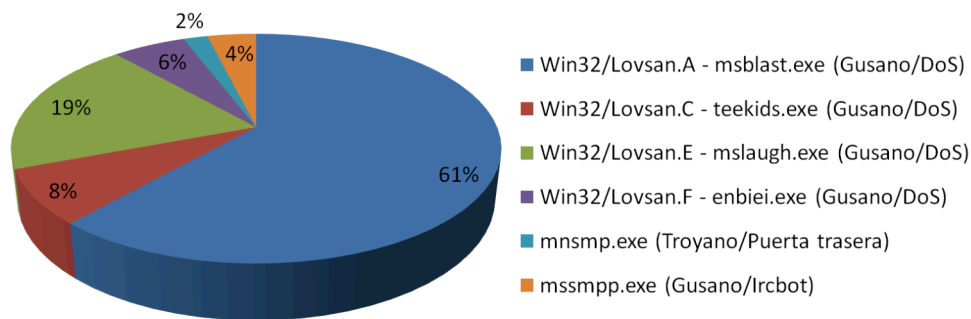


Figura 3: Virus detectados por Nepenthes.

Todos ellos han intentado descargarse a Nepenthes, siendo las variantes A, C y D de Win32/Lovsan los que lo han conseguido. Como puede observarse, estos gusanos son los que más incidencias han tenido durante el período de prueba del sistema, siendo el más destacado Win32/Lovsan.A. Cabe resaltar que los gusanos no infectan el *honeypot*, puesto que éste no presenta las vulnerabilidades necesarias para hacerlo sino que únicamente simula tenerlas.

## VIRUS DESTACADOS

Los virus más detectados y algunas de sus características aparecen en la siguiente tabla. Para más información consulte [alerta-antivirus.red.es/portada/buscar.php](http://alerta-antivirus.red.es/portada/buscar.php):

NOMBRE	ALIAS	TIPO	GRAVEDAD
<a href="#">Win32/Lovsan.A</a>	W32/Lovsan.worm, MSBlast, Exploit-DcomRpc (variant), W32.Blaster.Worm, Win32.Poza, WORM_MSBLAST.A, W32/Blaster-A, W32/Lovsan.A, Poza, Win32.Poza, MsBlaster, Blaster	Gusano (DoS)	Alta
<a href="#">Win32/Lovsan.E</a>	W32/Lovsan.worm.e, W32/Lovsan.E, Worm.Blaster.E, W32/Blaster.E	Gusano (DoS)	Media
<a href="#">mssmpp.exe</a>		Gusano (Ircbot)	Alta

## CONCLUSIONES

Como ya se ha comentado anteriormente en este informe, la obtención de información sobre los ataques que se producen en Internet es crucial para la seguridad de las redes corporativas. Es necesario saber qué está pasando. Ya existen observatorios a nivel mundial que ofrecen información sobre ataques. Entonces, ¿por qué es necesario desplegar una infraestructura como *Eusk@lert*? Porque es muy importante conocer las particularidades locales de los ataques que, en la mayoría de las ocasiones, presentan diferencias con el comportamiento global de los ataques a nivel mundial.

Como ejemplo, en las siguientes figuras se muestran los puertos más atacados tanto en el nodo de *Eusk@lert* (Figura 4) instalado en la Escuela Politécnica Superior como en la red *Leurre.com* (Figura 5).

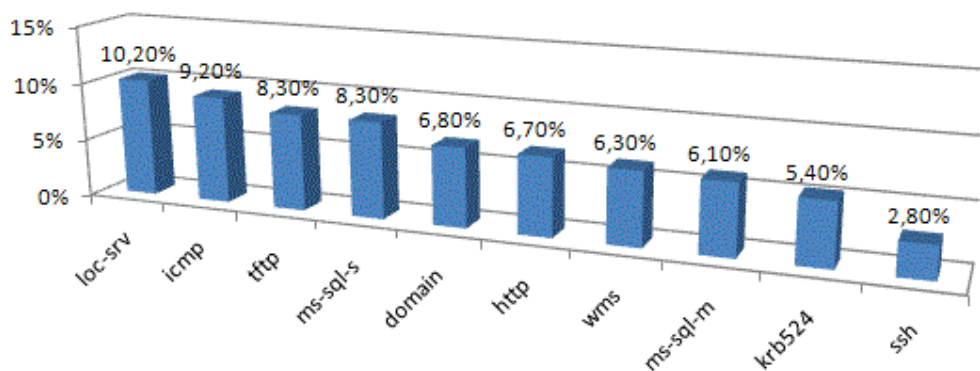


Figura 4: Servicios más atacados en *Eusk@lert*.

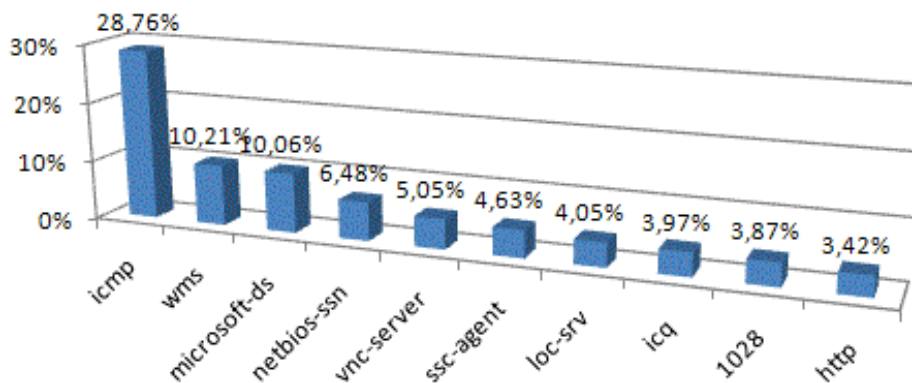


Figura 5: Servicios más atacados en *Leurre.com*.

*Leurre.com* es una red de sistemas trampa con más de 50 nodos desplegados a nivel mundial. Uno de estos nodos está ubicado en la Escuela Politécnica Superior de Mondragón Unibertsitatea. Esta red se dedica a recopilar información sobre ataques en Internet. Como se puede observar comparando las dos figuras, los comportamientos observados en ambos entornos presentan bastantes diferencias.

También se han comparado los resultados extraídos hasta ahora en *Eusk@lert* con los resultados proporcionados por otros observatorios públicos y en todos los casos se han observado diferencias notables, respaldando la necesidad de observar los procesos locales, para poder responder antes y mejor a los ataques.

## ANEXOS

La Figura 6 representa la arquitectura genérica de la infraestructura Honeynet. Además, integra HoneyMole con el fin de facilitar la distribución de sensores remotos y el intercambio de información mediante procedimientos seguros -túneles encriptados- a través de redes públicas. Este modelo es genérico, por lo que prevé la instalación de múltiples *honeypots* que pueden ser de diferente naturaleza. Esto no es necesario, tal y como demuestra el uso de un solo *honeypot* en el sistema *Eusk@lert*, pero puede implementarse en un futuro gracias a la escalabilidad que ofrece el modelo.

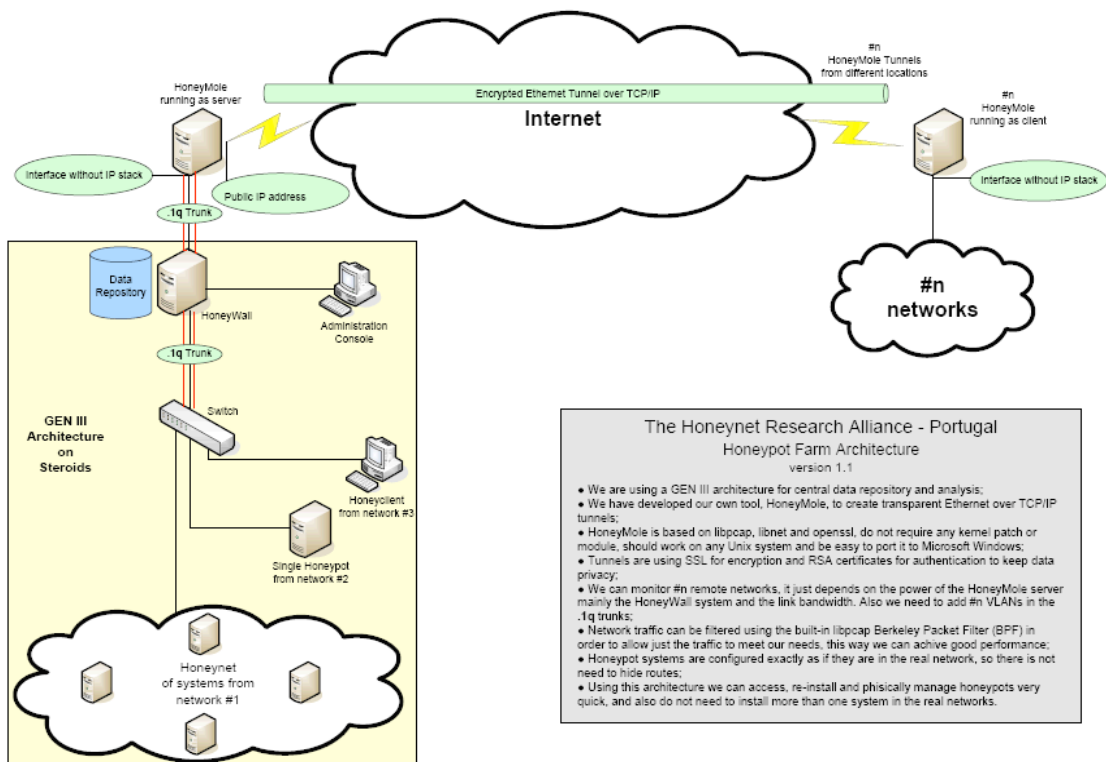


Figura 6: Arquitectura Honeynet + Honeymole