Jornadas Técnicas de RedIRIS 2025
Toledo. 20-22 de mayo de 2025

CAPTURAS CON MIEL

Casos prácticos de detección de ciberataques en la UPC

Daniel GUASCH MURILLO, Jordi Enric MARTINEZ OSORIO, David RAYA MARCOS

Universitat Politècnica de Catalunya
daniel.guasch@upc.edu, jordi.enric.martinez@upc.edu, david.raya@upc.edu

Línea temática: Seguridad y privacidad

Resumen:

La Seguridad en las redes , tanto públicas como privadas, de las universidades abarca todos sus ámbitos de actuación. Disponer de datos reales del tráfico en estas redes proporciona una información útil aplicable en cada uno de estos ámbitos. En la docencia permiten ilustrar al estudiantado la importancia del diseño, la planificación y la configuración de los elementos y procesos que conforman la infraestructura TIC. Las trazas de tráfico permiten obtener patrones detallados de los ataques recibidos necesarios para la investigación en ciberseguridad. Y a partir de esta información los servicios TIC pueden optimizar la gestión de la red, configurando óptimamente los equipos troncales.

Este trabajo pone de manifiesto el potencial del uso combinado de honeypots y sniffers para identificar y analizar problemas de ciberseguridad en una red universitaria mediante la descripción de dos ciberataques realizados contra la Universitat Politècnica de Catalunya (UPC) en 2024. Es el resultado de la colaboración entre el profesorado del Departament d'Enginyeria Telemàtica (ENTEL) y los Servicios TIC de la Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú (EPSEVG) de la UPC.

El análisis se ha realizado mediante un honeypot y un sniffer, implementados con software libre. Ambos están basados en la distribución Linux Debian. Sobre esta, el honeypot ejecuta una la plataforma T-Pot, mientras que el sniffer dispone de una interfaz alimentada con un port mirror del honeypot desde el router troncal de la EPSEVG. Se han definido reglas específicas en los cortafuegos, tanto el troncal de la UPC como el local de la EPSEVG, para que el honeypot sea completamente accesible desde las redes externas a la UPC (Internet). Esta arquitectura permite realizar un análisis a dos niveles de detalle, ataques y tráfico. Así como obtener información cuando el honeypot está inestable, o saturado, debido a los ataques que recibe.

El primer ataque presentado fue reportado el 2024/05/29 en un post de @elhackernet, en la plataforma X, y realizado por el grupo de hackers UserSec según se informaba en la web de High Society. Se trataba de un ataque de diccionario al servicio FTP y, a pesar de lo que pensaban los hackers implicados, no tuvo éxito. El segundo ataque descrito se realizó el 2024/10/03 y consistió en un ataque distribuido de denegación de servicio (DDNS) contra el servicio DNS. Mientras que el caso anterior fue un ataque indiscriminado contra entidades de países occidentales, este fue dirigido específicamente contra el honeypot. El motivo fue que la identidad del honeypot quedo al descubierto en el ataque de UserSec del mes de mayo. La información obtenida de ambos ataques se ha publicado parcialmente y usado para optimizar los equipos de la UPC.

Palabras claves:
ciberseguridad, honeypot, caso práctico, universidad

Abstract:

Security in universities' networks, both public and private, covers all areas of action. Having real traffic data on these networks provides valuable information applicable to each of these areas. In teaching, they allow students to illustrate the importance of designing, planning and configuring the elements and processes that make up the ICT infrastructure. Traffic traces allow detailed patterns of attacks received necessary for cybersecurity research. And based on this information, ICT services can optimise network management, optimally configuring the backbone equipment.

This work highlights the potential of the combined use of honeypots and sniffers to identify and analyse cybersecurity problems in a university network by describing two cyberattacks carried out against the Universitat Politècnica de Catalunya (UPC) in 2024. It is the result of the collaboration between the teaching staff of the Department of Telematic Engineering (ENTEL) and the ICT Services of the Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú (EPSEVG) of the UPC.

The analysis has been carried out by the combined use of a honeypot and a sniffer, implemented with free software. Both are based on the Debian Linux distribution. On top of this, the honeypot runs on the T-Pot platform, while the sniffer has an interface powered by a honeypot port mirror from the EPSEVG trunk router. Specific rules have been defined in the firewalls, both the UPC trunk and the local EPSEVG, so that the honeypot is fully accessible from networks external to the UPC (Internet). This architecture allows for analysis at two levels of detail, attacks and traffic. As well as obtaining information when the honeypot is unstable, or saturated, due to the attacks it receives.

The first attack presented was reported on 2024/05/29 in a @elhackernet post, on the X platform, and carried out by the hacker group UserSec as reported on the High Society website. It was a dictionary attack on the FTP service and, despite what the hackers involved thought, it was unsuccessful. The second attack described was performed on 2024/10/03 and consisted of a distributed denial-of-service (DDNS) attack against the DNS service. While the previous case was an indiscriminate attack against entities in Western countries, this one was specifically directed against the honeypot. The reason was that the identity of the honeypot was exposed in the UserSec attack in May. The information obtained from both attacks has been partially published and used to optimise the UPC's equipment.

Keywords:
cybersecurity, honeypot, case study, university