HONEYPOT

Implementació, escolta i anàlisi de resultats

Isaac Yera Caballero
iyera@uoc.edu

HONEYPOT: INTRODUCCIÓ

QUÈ ÉS UN HONEYPOT?

Un Honeypot és un software o conjunt de computadores que tenen com a objectiu:

- Simular ser dèbils i vulnerables per tal d'atreure atacants.
- Recol·lectar informació sobre atacants i tècniques utilitzades
- Desviar l'atenció dels atacants dels sistemes importants.

HONEYPOT: OBJECTIUS

- Dissenyar un conjunt de sistemes i xarxes que facilitin l'entrada d'atacants
- Implementar Honeypots (Linux i Windows) per atreure atacants.
- Implementar sistemes per extreure informació dels atacs.
- Realitzar un estudi/informe dels atacs rebuts.

HONEYPOT: DISSENY DEL SISTEMA HONEYPOT

El nostre entorn Honeypot està construït sobre quatre pilars:

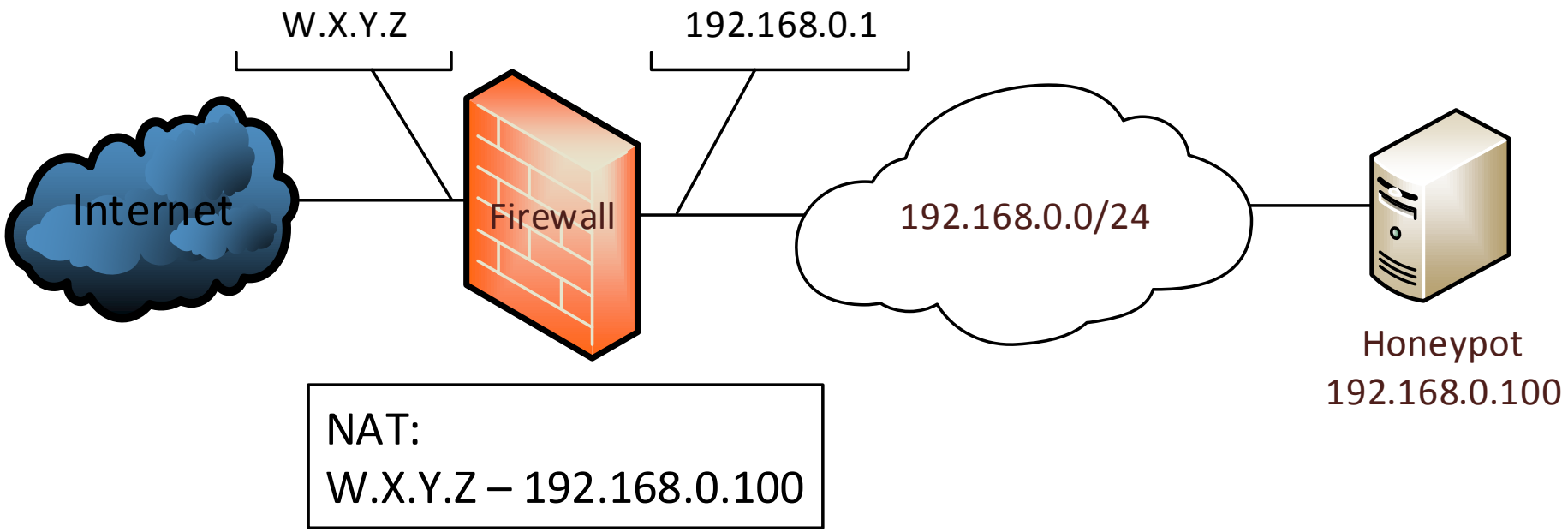
- Entorn sobre el que es dissenyarà tot el sistema Honeypot
- Estructura de xarxa
- Estructura de sistemes
- Honeypots seleccionats

HONEYPOT: DISSENY DE L'ENTORN

Per construir tot el nostre sistema de Honeypot s'ha seleccionat l'entorn en cloud de VMWare per les facilitats que aquest ens proporciona:

- Crear tantes màquines com siguin necessàries
- Crear tantes xarxes com es vulgui
- Crear firewalls virtuals

HONEYPOT: DISSENY DE LA XARXA



HONEYPOT: DISSENY DEL SISTEMA

Entre els objectius del projecte hi ha la necessitat de crear honeypot tant per entorn Linux com per a Windows i la recomanació de fer servir la distribució de Linux Honeydrive.

Honeydrive destaca per ser una distribució de Linux que compte amb una gran varietat de softwares per crear Honeypots.

HONEYPOT: DISSENY DEL HONEYPOT

Entre la gran varietat de softwares per crear Honeypots que ens aporta Honeydrive, s'han seleccionat les següents eïnes:

- Dionaea → Capacitat de emular entorns Linux i windows
- DionaeaFR → Capacitat de extreure informació dels atacs rebuts per Dionae
- Kippo → Capacitat per emular SSH
- KippoGraph → Capacitat de extreure informació dels atacs rebuts per Kippo

HONEYPOT: DISSENY DEL HONEYPOT

Amb les eines Honypot seleccionades s'han emulat els següents serveis vulnerables:

- Dionaea:
  - *Windows:*
    - Ms SQL Server (MsSQL) (port 1433 TCP)
    - WINS (port 42 TCP)
    - NetBios (port 139 TCP)
    - Ms Active Directory / SMB (port 445 TCP)
  - *Linux:*
    - HTTP (port 80 i 443 TCP)
    - FTP (port 21 TCP)
    - TFTP (port 69 UDP)
    - Telnet (Port 23 TCP)
    - MySQL (port 3306 TCP)
  - *Altres:*
    - Sip
- Kippo:
  - *Linux:*
    - SSH (port 22 TCP)

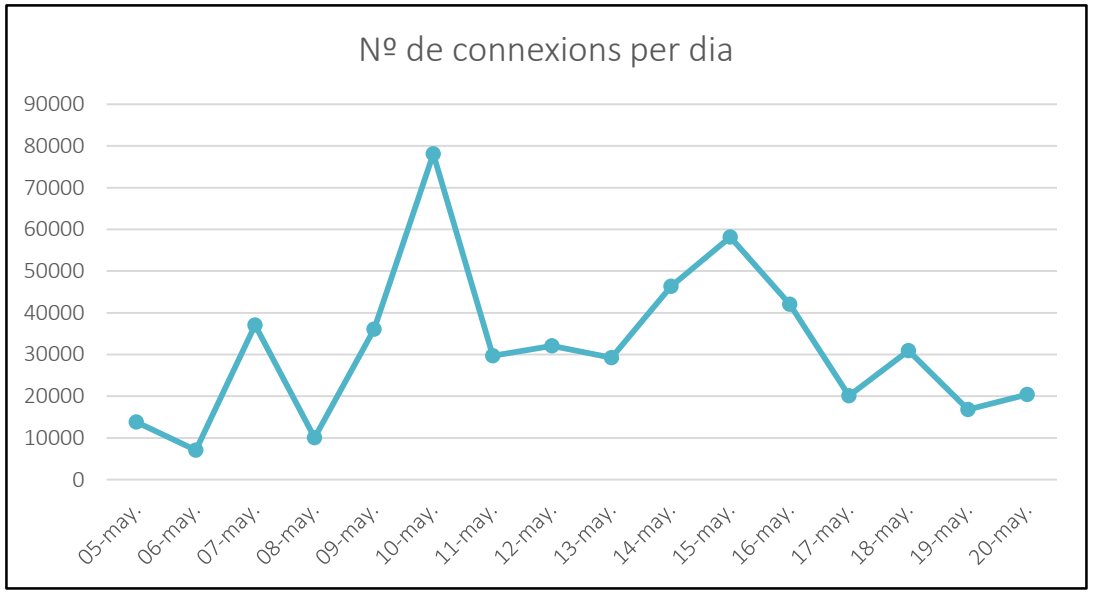
HONEYPOT: RESULTAT DELS ATACS

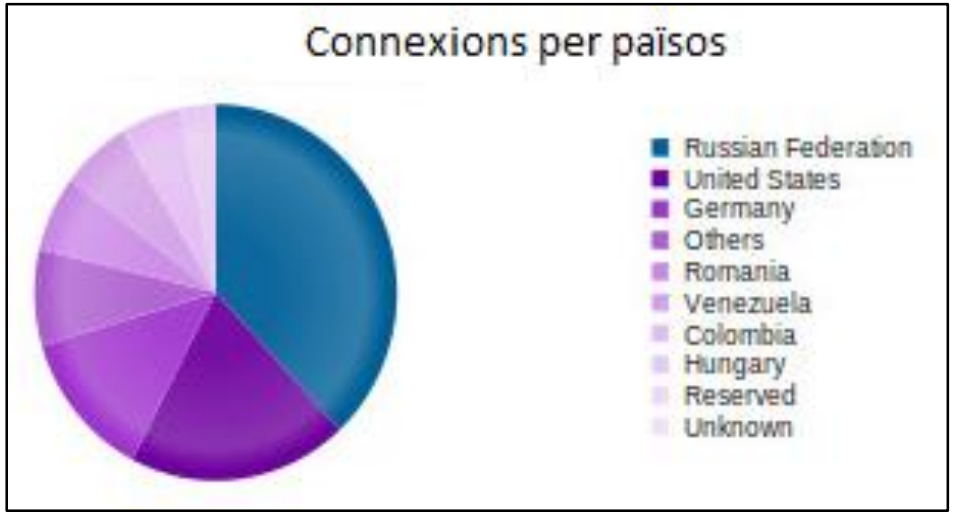
Amb els dissenys esmentats s'ha creat un entorn Honeypot que ha estat rebent connexions i atacs durant 15 dies, obtenint dades sobre:

- Nº de connexions totals, per servei i per país d'origen
- Serveis emulats que han rebut més connexions i/o atacs
- Nº d'atacs en funció del servei objectiu.
- Atac o vulnerabilitat més explotat

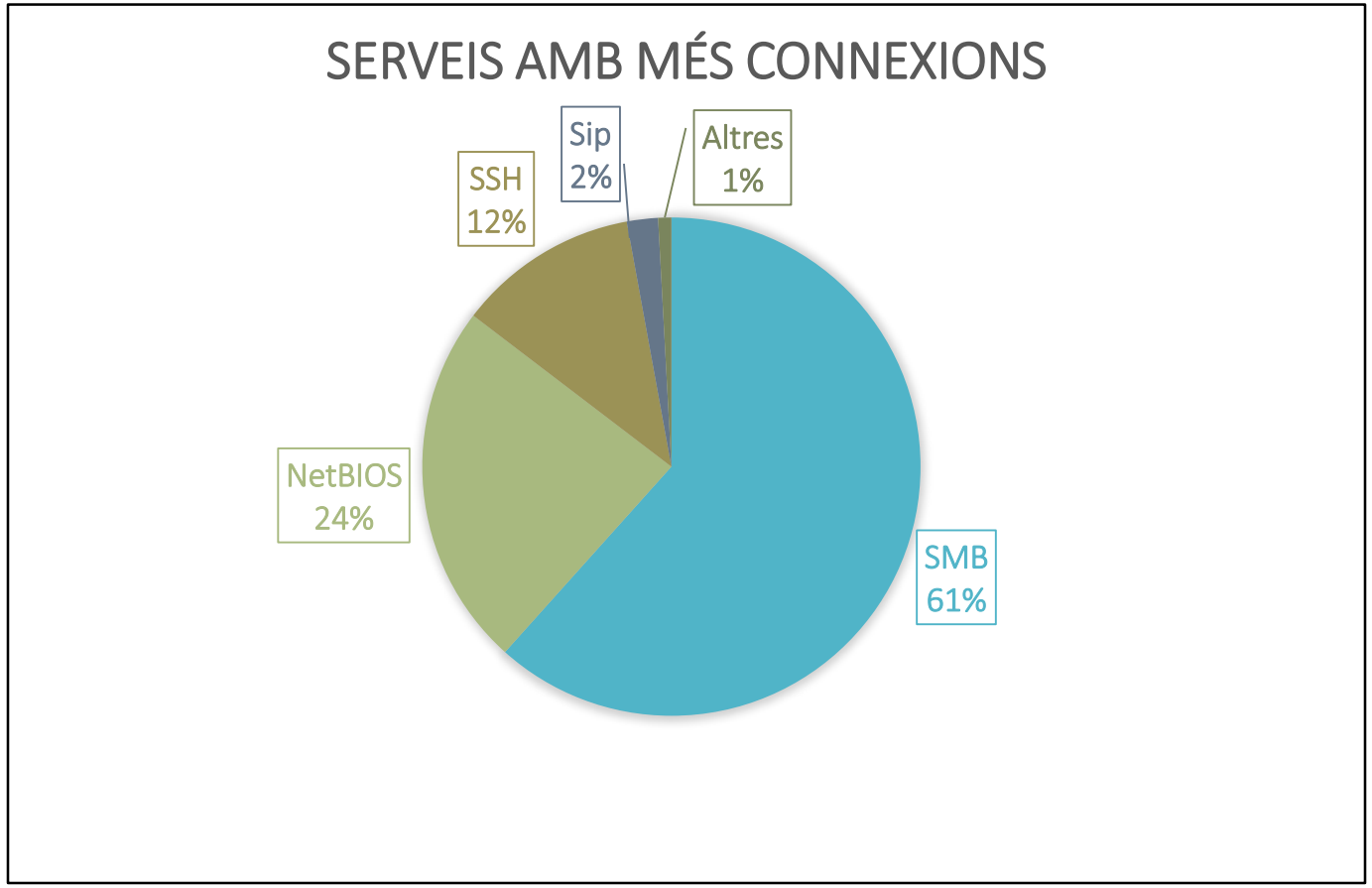
HONEYPOT: RESULTAT DELS ATACS

Número de connexions per dia i com es distribueixen aquestes connexions per països



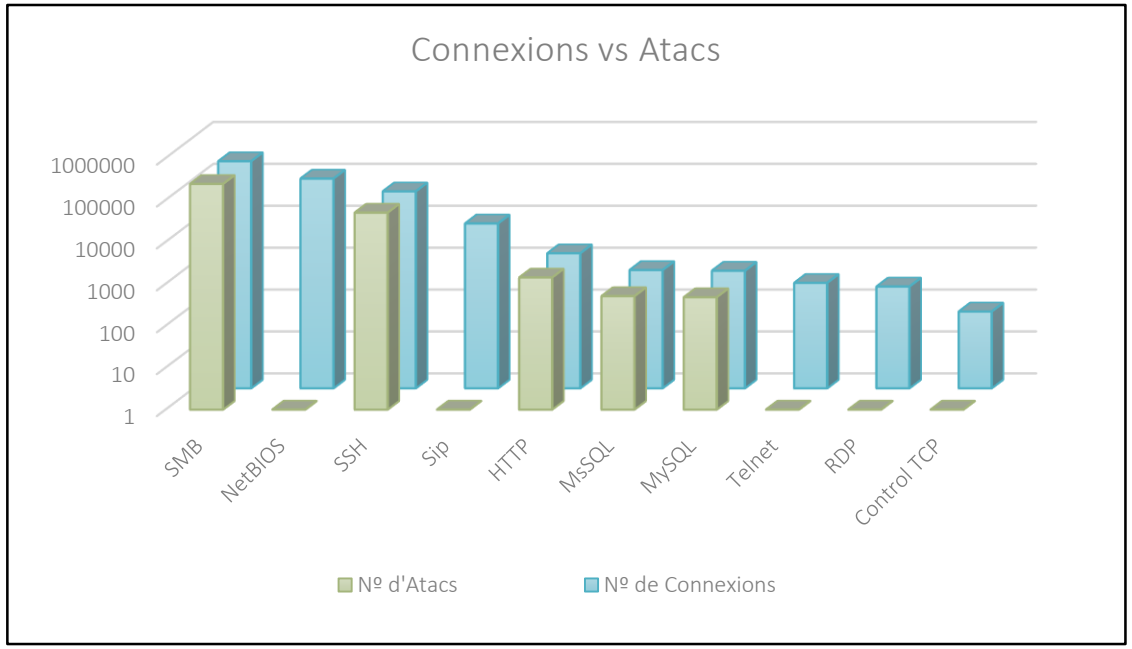


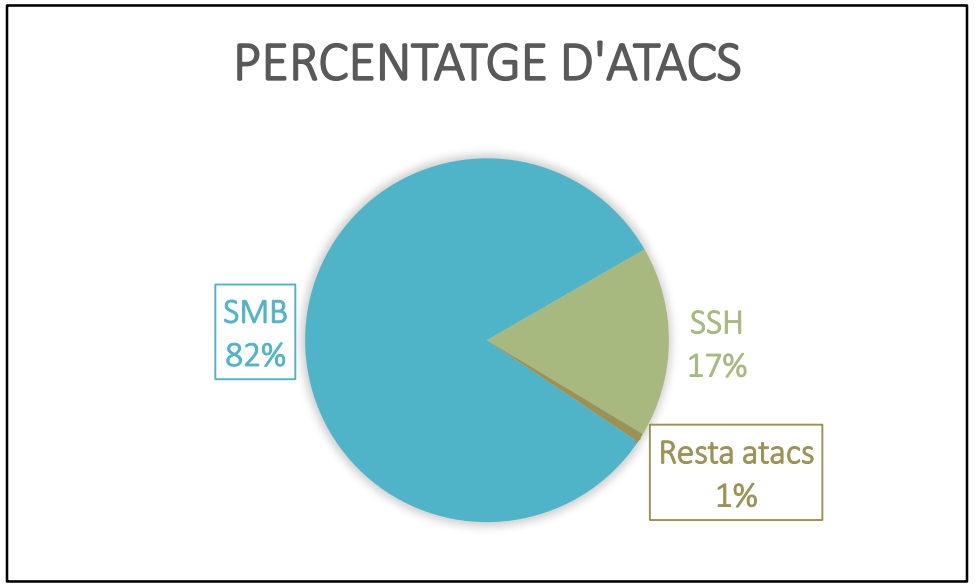
HONEYPOT: RESULTAT DELS ATACS



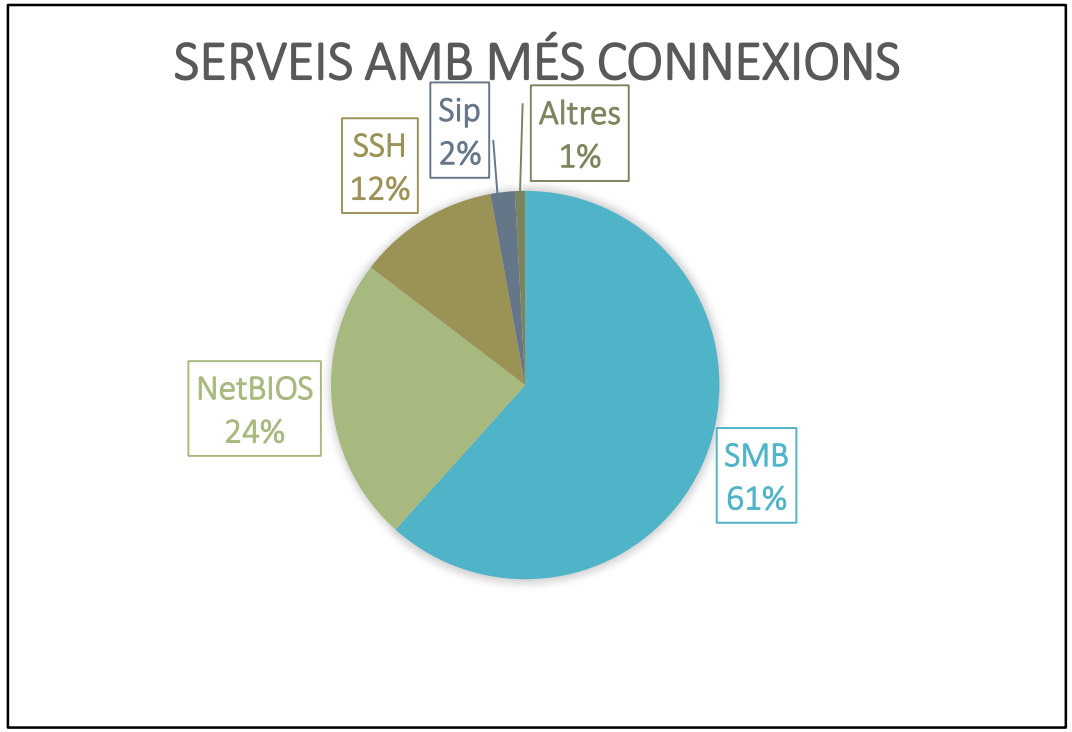
HONEYPOT: RESULTAT DELS ATACS

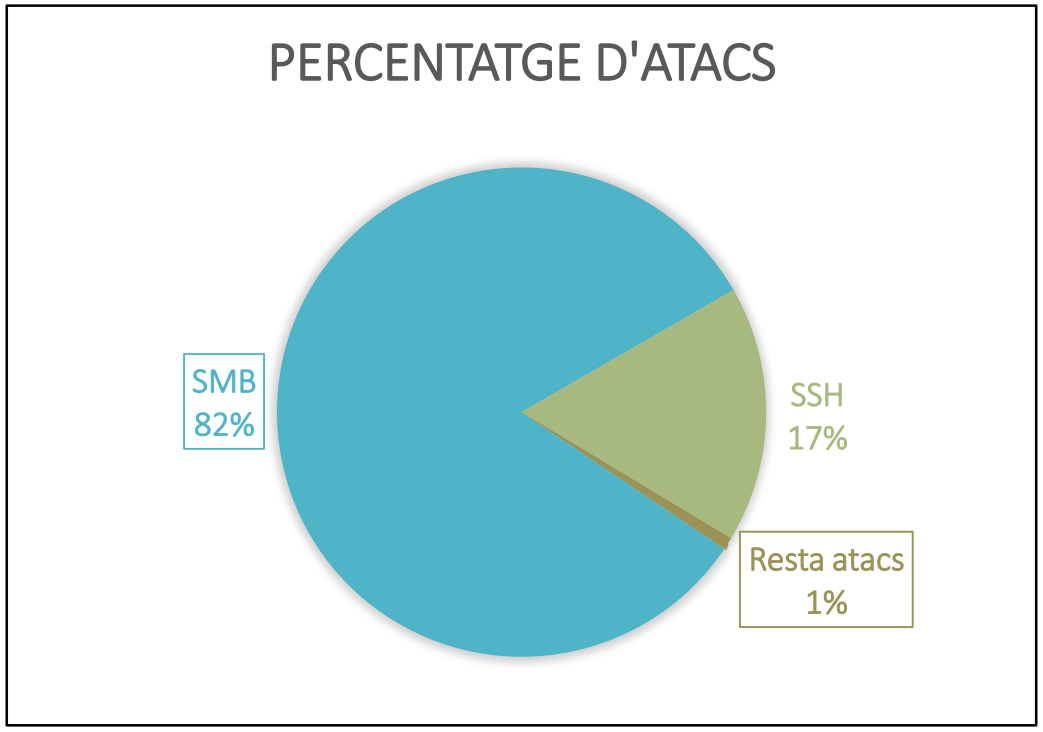
SERVEIS AMB MÉS ATACS





HONEYPOT: RESULTAT DELS ATACS





HONEYPOT: RESULTAT DELS ATACS

ATACS MÉS UTILITZATS

El 99% dels atacs se'ls reparteixen dos servies SMB i SSH. I els atacs fets servir han sigut preferentment

- SSH: força bruta per esbrinar la combinació user:pass
- SMB: explotar la vulnerabilitat MS08-067

HONEYPOT: CONCLUSIONS

- A internet hi ha milers d'aranyes dedicades a localitzar serveis amb deficiències de seguretat.
- Les deficiències detectades per les aranyes són fetes servir per comprometre les màquines afectades.
- L'objectiu dels atacs han sigut entorns Linux i Windows, però per cada atac a Linux Windows rep 5.

Moltes Gràcies

Isaac Yera Caballero
iyera@uoc.edu