**MHN**

**2019-2020**

AURKIBIDEA

[***AURKIBIDEA 2***](#_heading=h.30j0zll)

[***1.***](#_heading=h.1fob9te) ***Zer da mhn? 1***

[***2.***](#_heading=h.3znysh7) ***konfigurazioa 1***

[**2.1**](#_heading=h.2et92p0) **Prestatu sarea 1**

[**2.2**](#_heading=h.tyjcwt) **Instalatu zerbitzaria 1**

[**2.3**](#_heading=h.3dy6vkm) **Konfiguratu honeypotak 3**

[2.3.1](#_heading=h.1t3h5sf) Cowrie 3

[2.3.2](#_heading=h.4d34og8) Conpot 5

[***3.***](#_heading=h.2s8eyo1) ***BALIABIDEAK 8***

# Zer da mhn?

MHN-ren bitartez honeypot sare bat kudeatu dezakegu. Sare horrek zerbitzari bat izango du eta, harekin konektatuta, hainbat honeypot; azken horietako bakoitzak eremu jakin bati buruzko informazioa bilduko du. Jasotako informazio guztiarekin, zerbitzariak balizko erasotzaileen informazioa kudeatuko du.

Nabigatzailetik kontrolatu dezakegu, eta oso interfaze ikusgarria du. Besteak beste, unean uneko balizko erasoak ikusteko Munduko mapa ikusgarria dauka.

# konfigurazioa

Adi: konfigurazio honek Ubuntu 18.04 erabiltzea eskatzen du.

## Prestatu sarea

VirtualBox-en makina birtualak erabili ditugu geure honeynet-a konfiguratzeko. Sarea 192.168.0.00/24 da eta sareko txartel guztiak “*Zubi Egokitzailea*” eran jarri ditugu, biderik errazena delako makina guztietatik Internetera irten ahal izateko eta elkar konektatuta egoteko; saretik internetera irteteko router bat izango bagenu, “*Barneko sarea”* eran jarriko genituzke txartelak*.* Makina hauek sortu ditugu:

* + - “MHN zerbitzaria” 192.168.1.100 helbidean.
    - “Cowrie honeypot” bat 192.168.1.101 helbidean.
    - “Conpot honeypot” bat 192.168.1.102 helbidean.

## Instalatu zerbitzaria

*MHN zerbitzaria* makinan honako urrats hauek egingo ditugu:

* + - Instalatu Git:

apt update

apt upgrade

sudo apt install git -y

* + - Instalatu MHN:

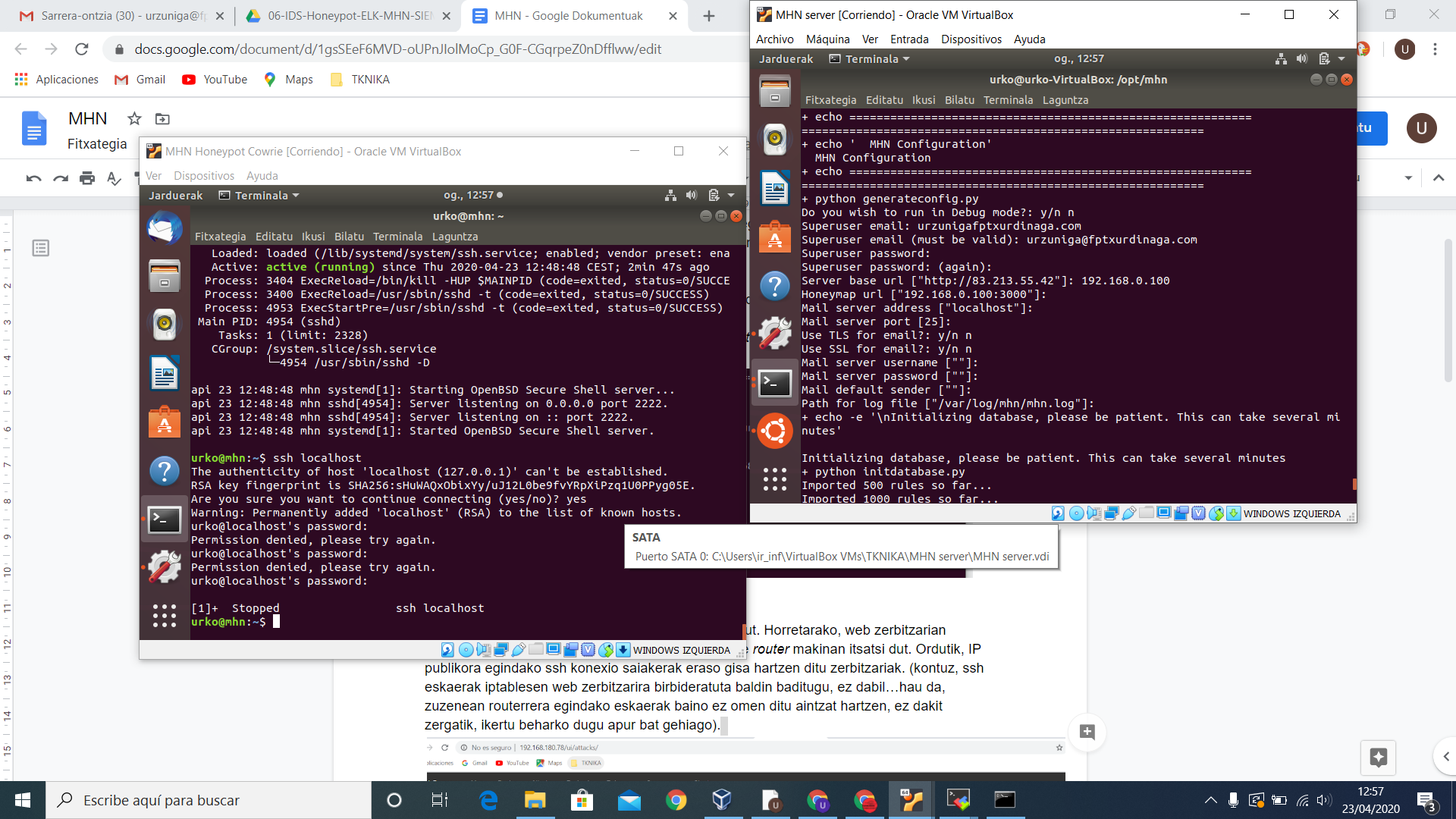
cd /opt/

sudo git clone https://github.com/pwnlandia/mhn.git

cd mhn/

sudo ./install.sh

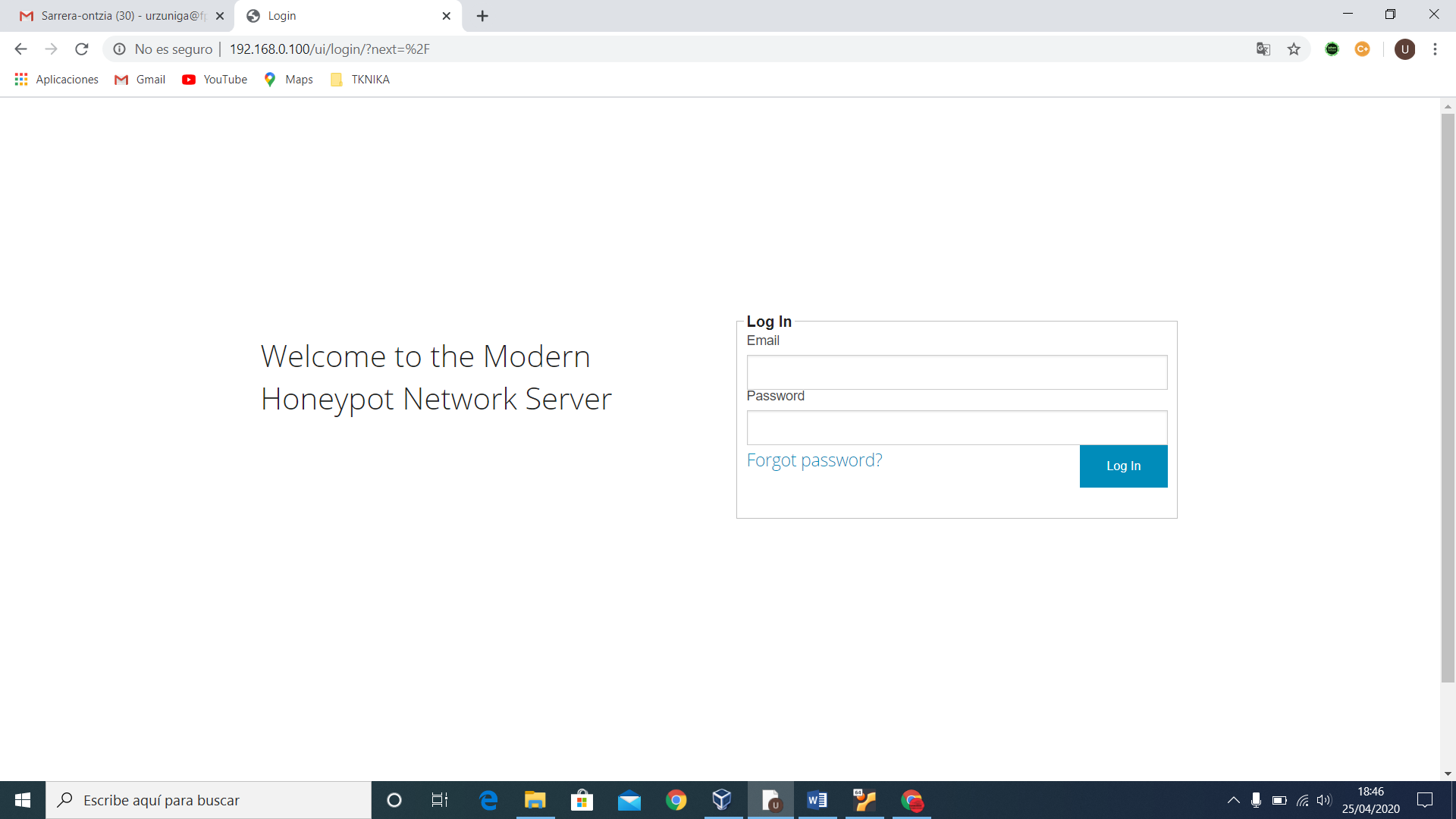
Tarte bat pasatuta (10-15 min), galdera hauek agertuko zaizkigu:



Azkenik, galdetuko digute ea SPLUNK eta ELK integratu nahi ditugun. Ezetz erantzungo dugu. Honetaz gain, UFWen MHNri dagozkion erregelak aktibatu nahi diren galdetzen du. Kasu honetan baietz erantzungo dugu.

* + - Hostalariaren nabigatzailean 192.168.0.100 ipiniko dugu.

Emaila eta pasahitza konfigurazioan jarritakoak izango dira.



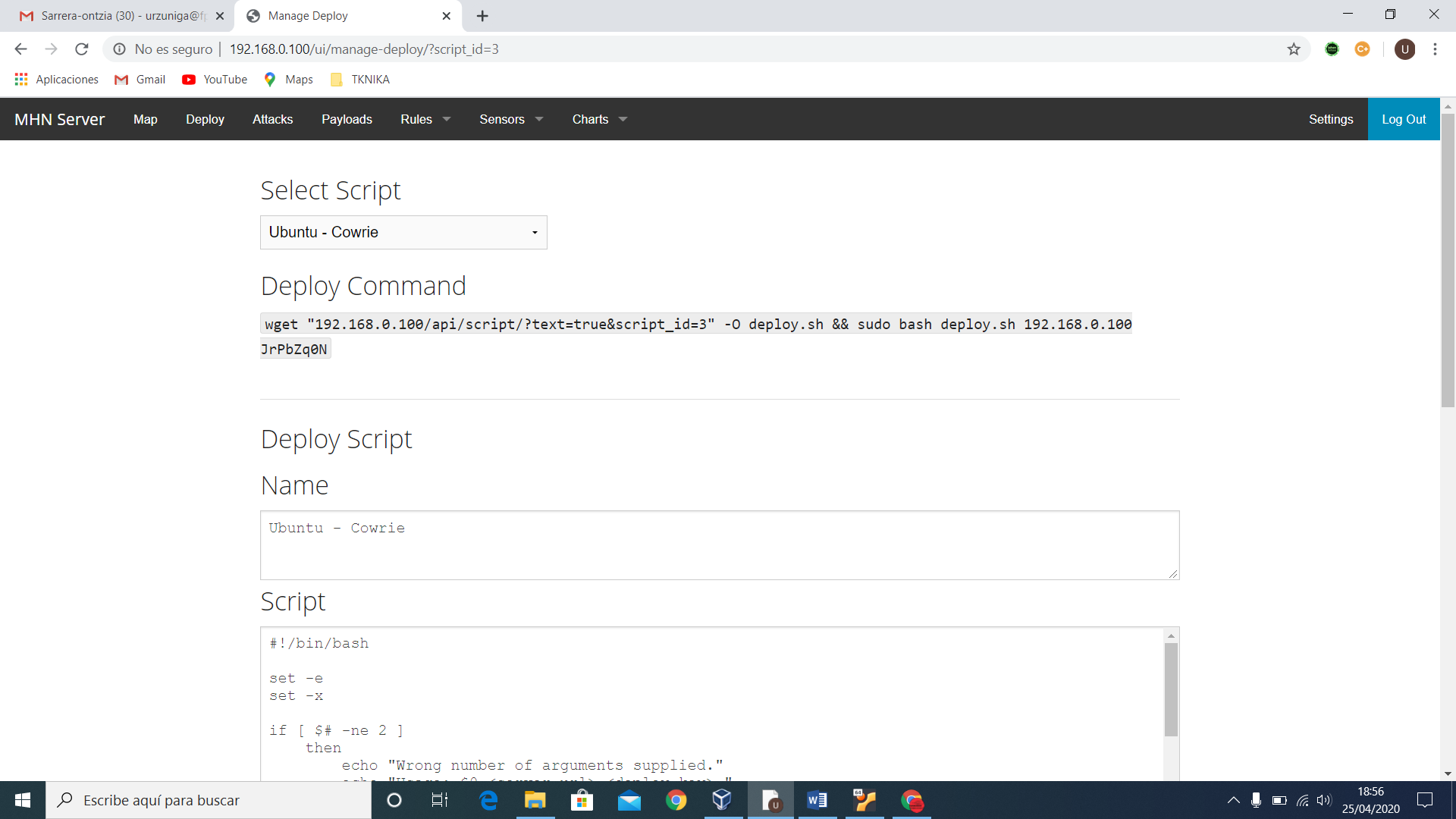
## Konfiguratu honeypotak

### Cowrie

Cowrie SSH honeypot bat da. SSH zerbitzuak kautotzeko kredentzial ahul eta errazak ditu. Behin kautotuta erasotzaileak komandoak exekutatu eta erantzunak jasoko ditu, baina alegiazkoak izango dira, pantailan ikusitakoa GNU/Linux faltsua izango baita. Honeypot hau SSH bidez erabiltzen ohi diren hiztegi bidezko indar-gordineko erasoak aztertzeko erabili daiteke, probatzen diren erabiltzaile izen eta pasahitz guztiak erregistratzen baititu.

Cowrie instalatzeko Deploy atalean “Ubuntu Cowrie” aukeratuko dugu. Deploy Command atalean agertzen den komandoa kopiatu egingo dugu.

Benetako sarerik ez badugu, 192.168.0.100 jar dezakegu berez ematen digun IP publikoaren ordez.



Cowrie instalatu baino lehen, hau instalatu nahi den Ubuntu makinan OpenSSH instalatu behar da aurretik. Hurrengo komandoa erabili daiteke:

sudo apt install openssh

Behin SSH instalatuta, aurreko pausoan kopiatutako komandoa exekutatuko dugu. Denbora tarte bat pasatu ondoren eta dena ondo joan bada honeypota prest izango dugu.

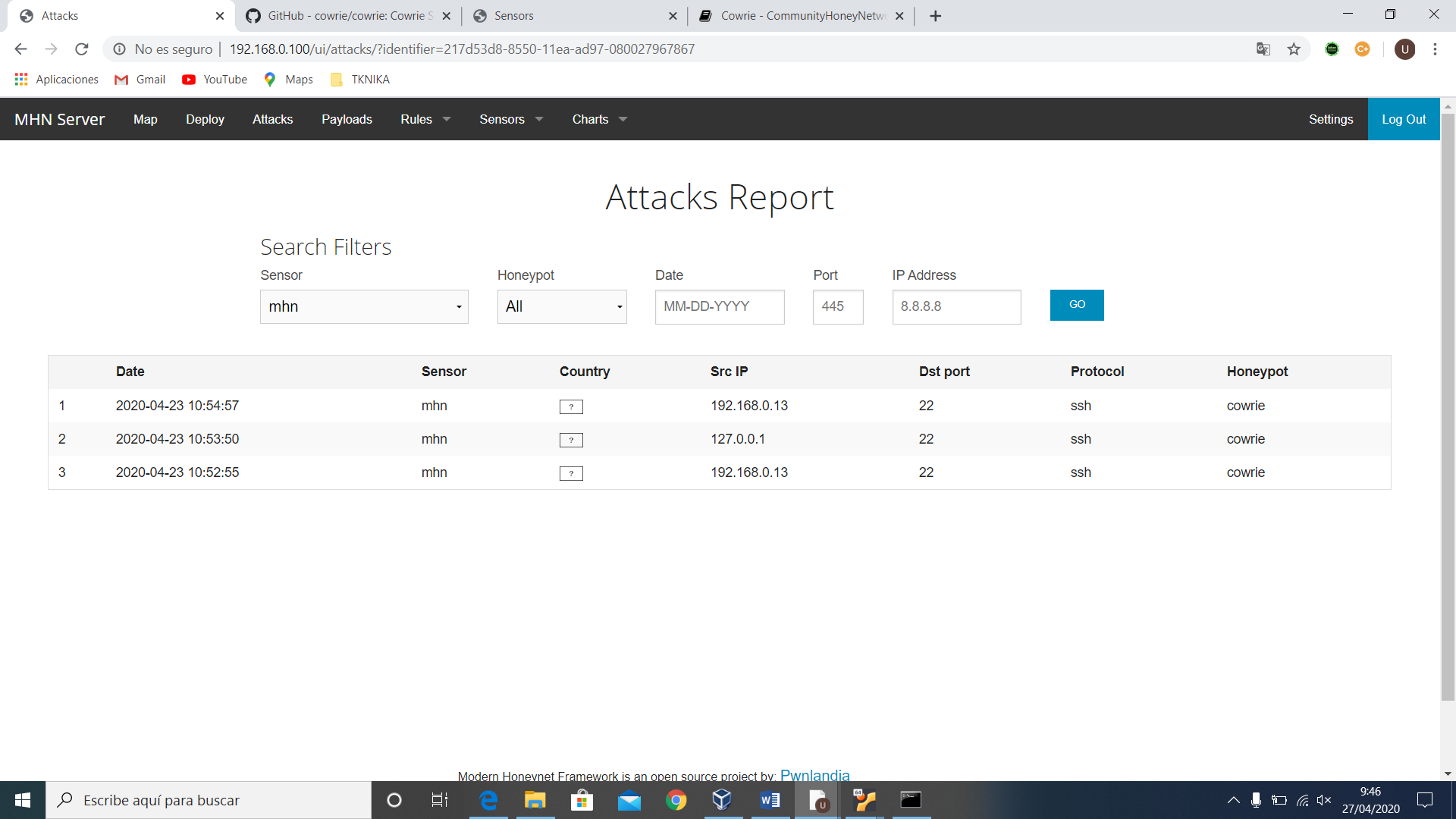
Sarean dagoen edozein makinatik SSH bidez posible izango da Cowrie makina atzitzea.

GARRANTZITSUA: Cowrie makinan bi SSH portu egongo dira irekita, 22 eta 2222. 22 portua honeypot bezala funtzionatuko du, hau da, bertara konektatuta egiten diren login saiakera guztiak erregistratuko dira. Ezinezkoa izango da makinan sartzea, root erabiltzailea erabiltzen ez bada. Cowrie makinaren kredentzialak erabilita ere ez da posible izango bertan sartzea. Root bezala sartu ahal da, baina irekitzen den SSH kontsolak ez ditu komandoak exekutatzen, eta beraz ezin da makinan kalterik egin.

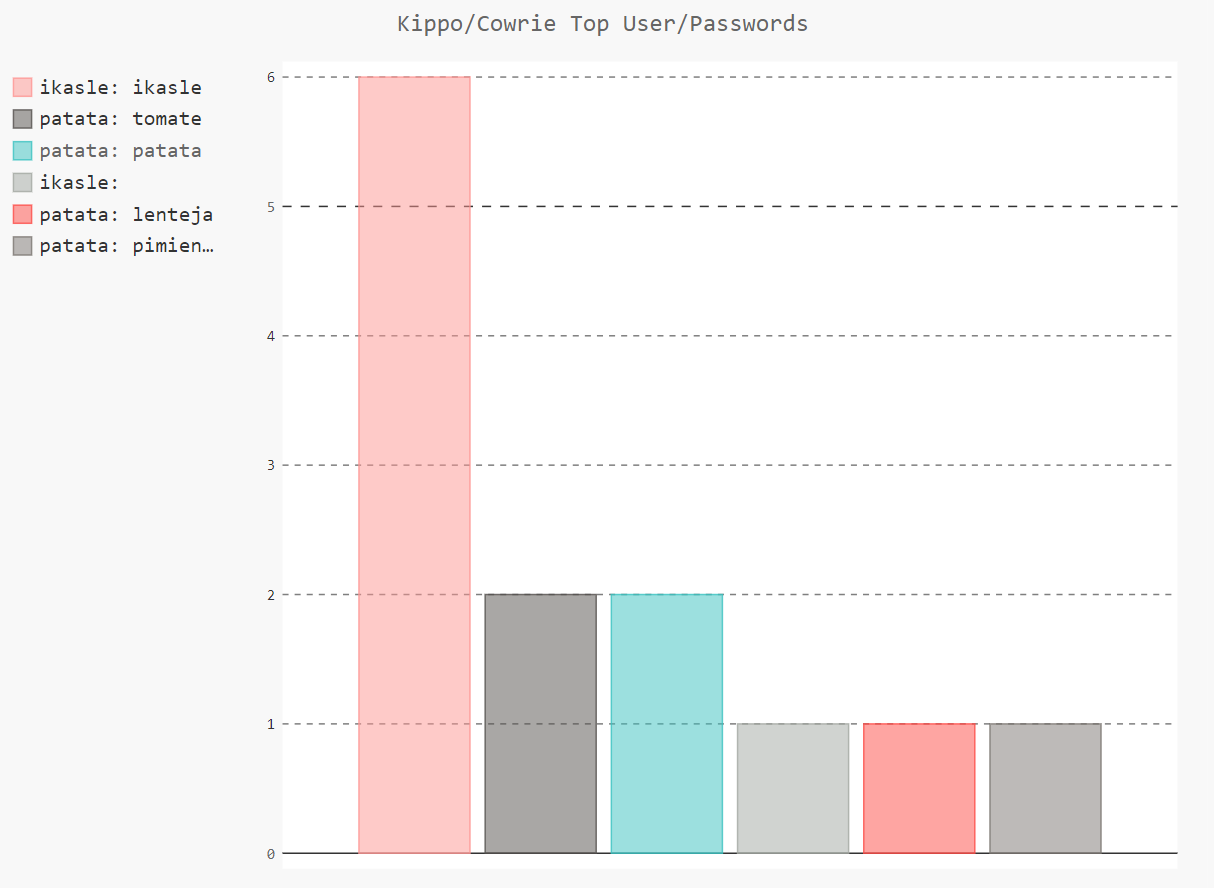
2222 portua SSH bidez Cowrie makina atzitzeko uzten den portua izango da. Portu honetan makinaren kredentzial normalekin sartu ahal izango da eta SSH modu normalean erabili ahal izango da. Portu honetara egiten diren sarrera saiakerak ez dira erregistratuko. Honeypot-a bakarrik 22 portuan egongo da.

Guzti hau horrela izanik, berebiziko garrantzia dauka Cowrie makinaren kredentzialak ahal den seguruenak izatea.

22 portura egiten diren saiakerak erregistratuta geratuko direnez, MHN-ren kontsolatik posible izango da hauek bistaratzea.



Era berean, posible izango da eraso hauen grafikoak bistaratzea. Horrela, denborarekin, indar-gordineko erasoetan gehien erabiltzen diren erabiltzaile izen eta pasahitzen datu-basea izango dugu.

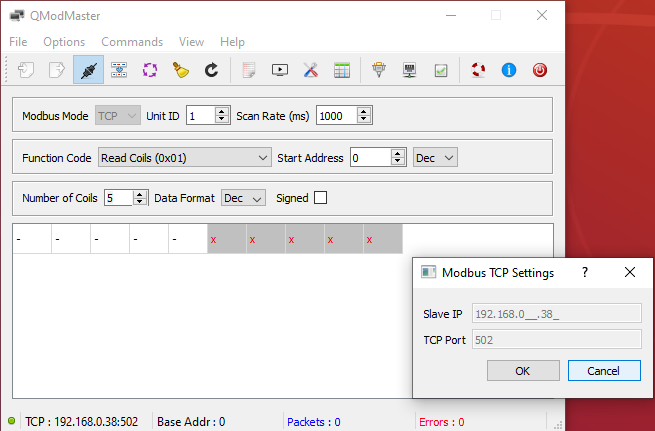


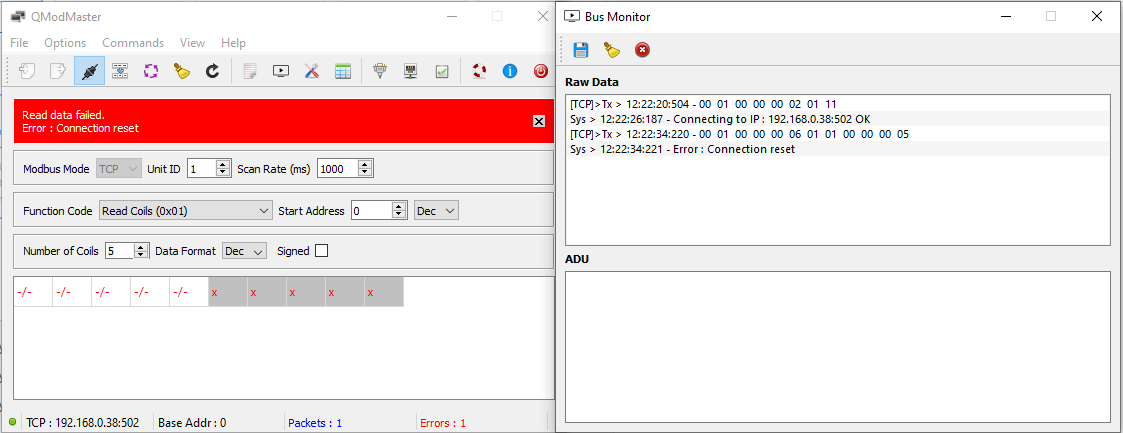
### Conpot

Conpot interakzio baxuko honeypot industrial bat da. Industriako zenbait gailu eta protokolo simulatzeko balio du. Zehazki, industriako Modbus eta S7Comm protokoloak simulatzen ditu. Honetaz gain, HTTP zerbitzari bat ere martxan jartzen du, bai eta SNMP agente bat.

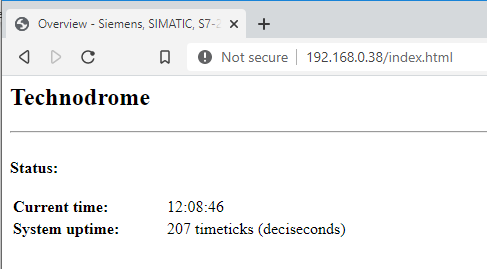
Conpot instalatzeko nahikoa da Cowrie instalatzeko jarraitu diren pauso berdinak jarraitzea. MHNren Deploy atalean Ubuntu-Conpot aukeratu, Deploy Command kuadroan agertzen den agindua Ubuntu makina garbi batean exekutatu eta instalazioa bukatu arte itxaron. Denbora tarte bat pasa ondoren instalatuta eta erabilgarri egongo da Conpot.

Modbus protokoloa probatzeko, hori erabiltzen duen edozein erreminta erabili daiteke. Besteak beste, QModMaster (<https://sourceforge.net/projects/qmodmaster/>) erreminta horietako bat da. Erreminta honen bidez Modbus protokoloa erabiltzen duen edozein gailutara TCP/IP bidez konektatu eta balioak irakurri eta idatzi daitezke gailuak baimena ematen badu. Compoten kasuan behintzat balio digitalak irakurtzea eta idaztea baimentzen da.



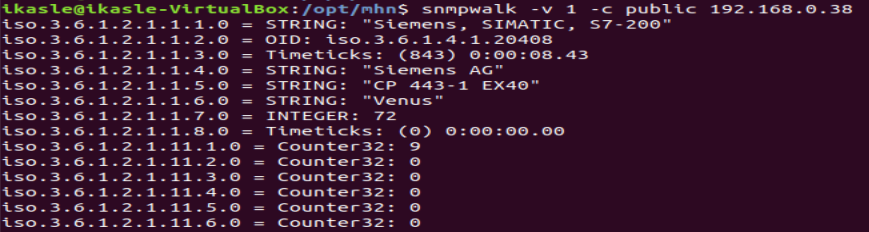


Esan bezala, Conpotek web zerbitzari bat jartzen du martxan baita ere. Zehazki, Siemens markako S7-20 ereduko PLC baten web zerbitzaria simulatzen du. Nabigatzaile batetik atzigarri uzten da.



Siemens-ekin jarraituta, Conpotek simulatzen duen PLCa 102 portua erabiltzen duen S7Comm protokoloaren bidez ere atzitu daiteke. Honetarako, noski, protokolo hau erabiltzen duen erremintaren bat erabili behar da, Snap7 (<https://sourceforge.net/projects/snap7/files/1.4.2/snap7-full-1.4.2.7z/download>), adibidez. Erreminta honen bidez PLCarekin konexioak ezarri daitezke.

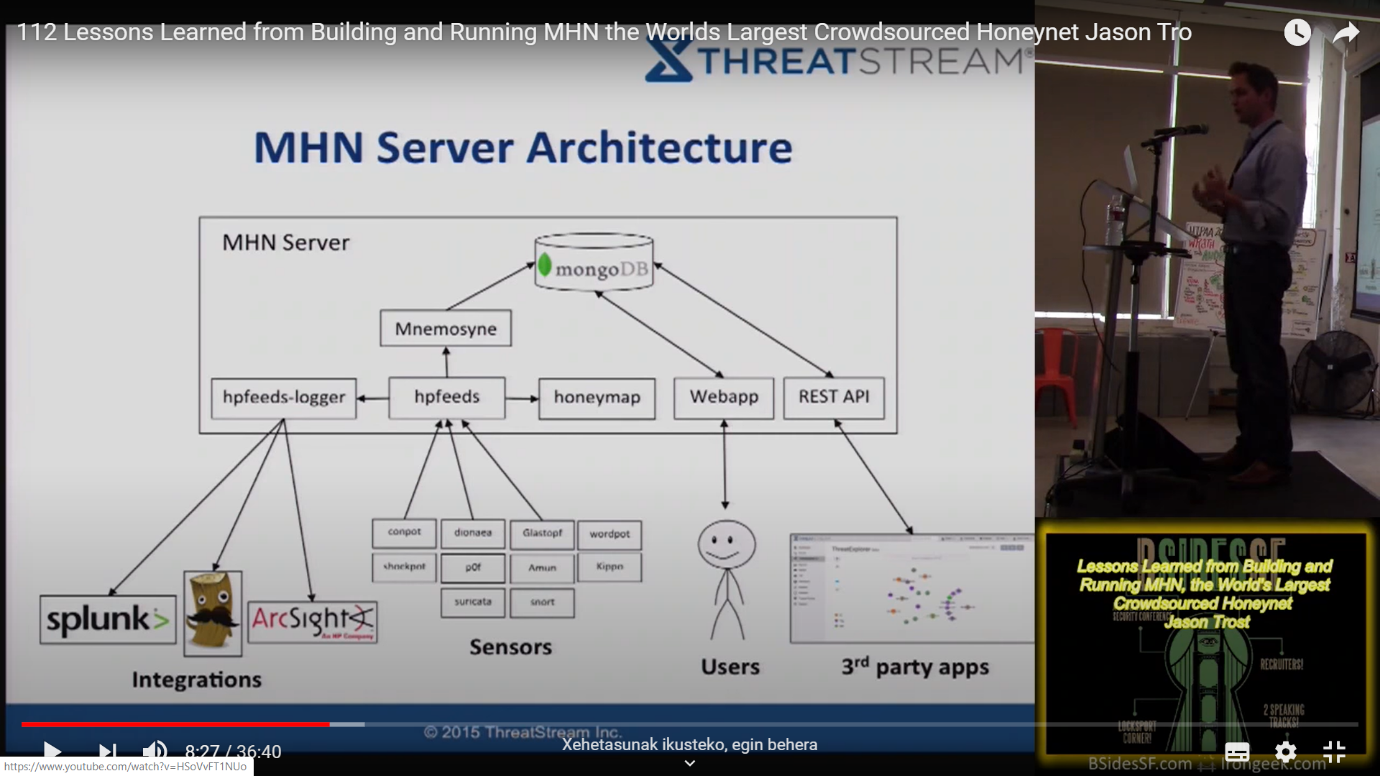
Bukatzeko, Conpotek SNMP protokoloa ere simulatzen du. Horrela, snmpwalk komandoarekin simulatutako gailuari buruzko informazioa jaso daiteke.



Compoten gertatzen diren eraso guztiak MHN-n erregistratuta geratzen dira. Horrela, besteak beste, eraso mota eta iturburua zein izan den jakin daiteke.

# BALIABIDEAK

* + - Arkitektura orokorraren eskema, [bideo honetatik](https://www.youtube.com/watch?v=Zd1Br8TW1mk) hartua:



* + - MHN zerbitzaria instalatu eta Dionaea honeypota hedatu. [Azalpen idatzia](https://zeltser.com/modern-honey-network-experiments/).
    - MHN zerbitzaria instalatu eta Snort honeypota hedatu. [Bideoa](https://www.youtube.com/watch?v=vUj9W0w7MdA).
    - Zerbitzariaren ohiko erroreak nola konpondu. [Gida](https://github.com/pwnlandia/mhn/wiki/MHN-Troubleshooting-Guide).



