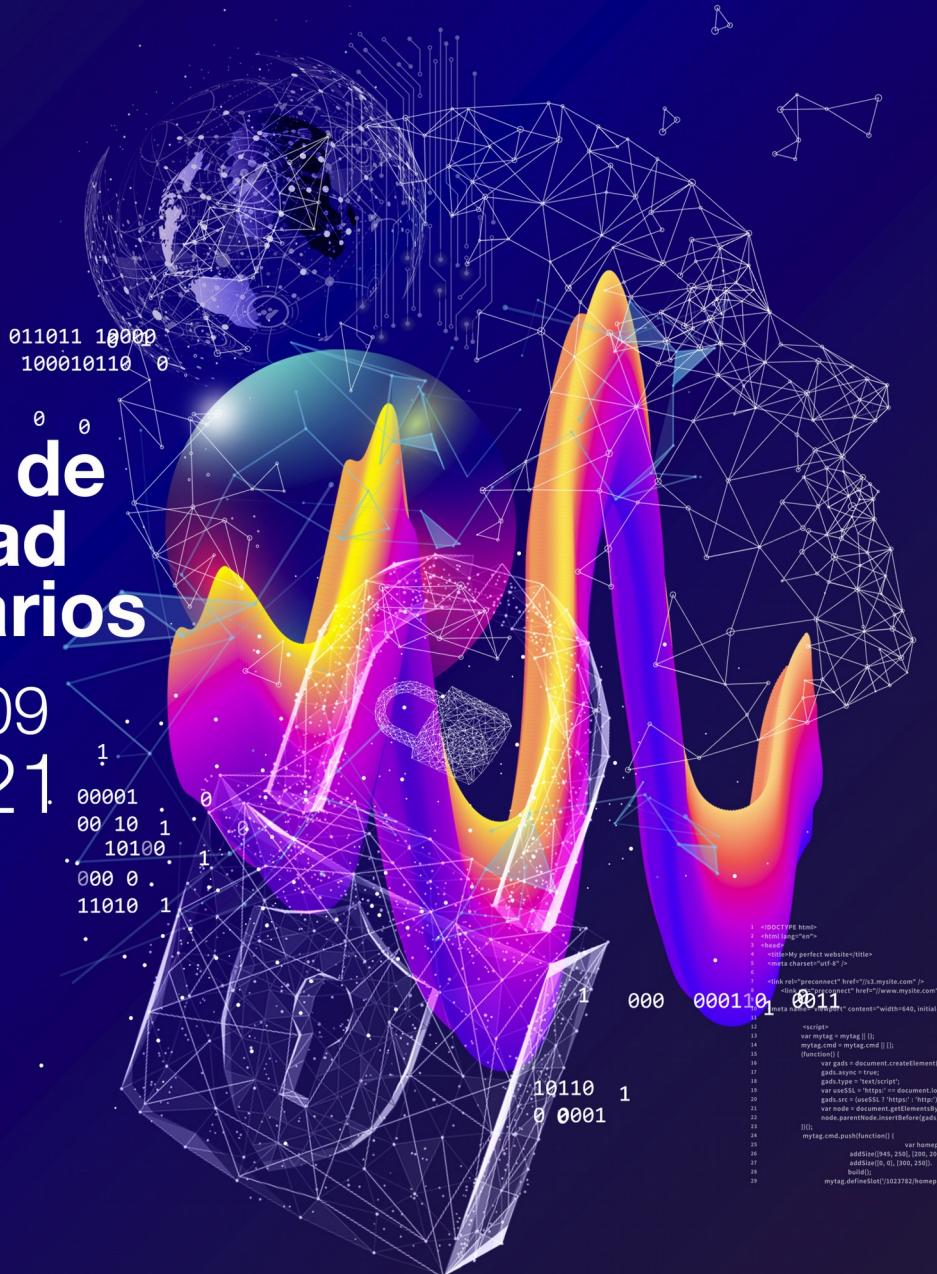




2^{do} Seminario de Ciberseguridad para funcionarios públicos

MARTES
28/09
2021





The background of the slide features the Chilean Government's official colors (blue, white, and red) and includes the logos of the Ministerio del Interior y Seguridad Pública and the CSIRT (Centro de Seguridad e Inteligencia de Redes). To the right, there is a stylized graphic of a human brain with colorful, glowing neural activity patterns.

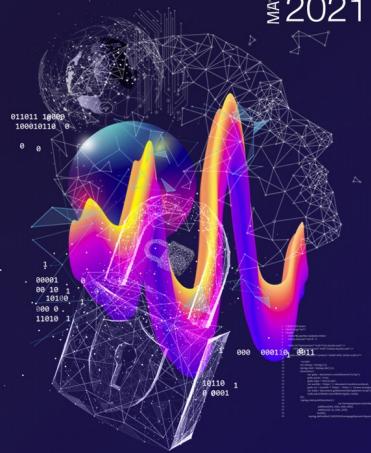
2^{do} Seminario de Ciberseguridad para funcionarios públicos

Usando un HONEY-POT (Opensource): T-POT

Miguel Kurte Araya



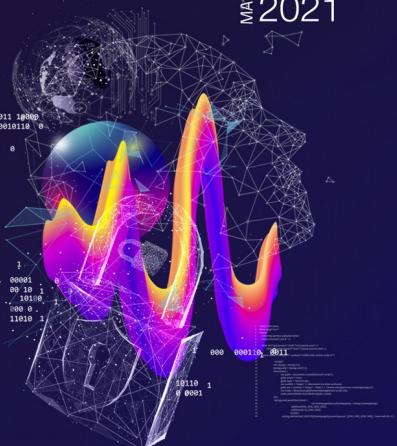
- Tabla de contenido
- ¿Qué es un HoneyPot?
- Tipos de HoneyPot
- Instalación de T-Pot
- Usando T-Pot





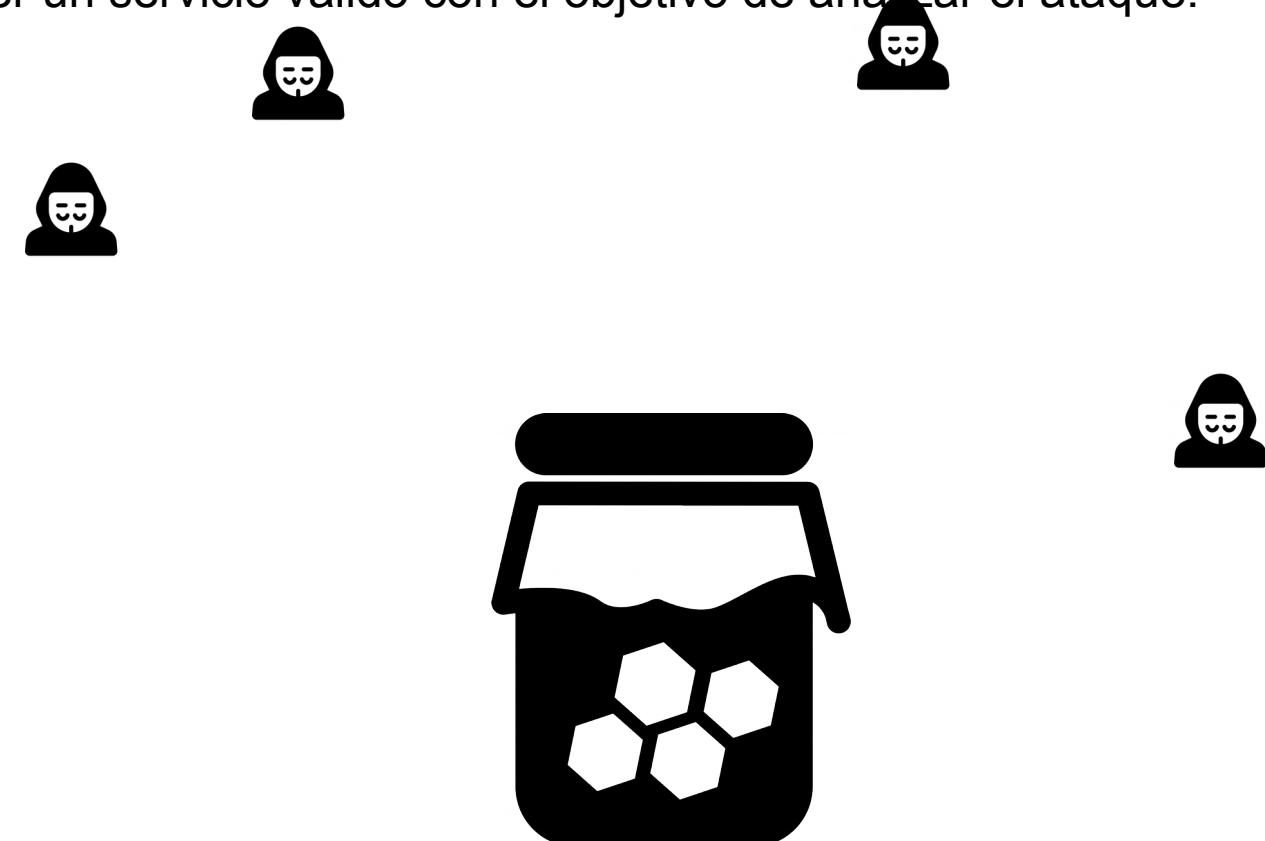
2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

MARTES
28/09
2021



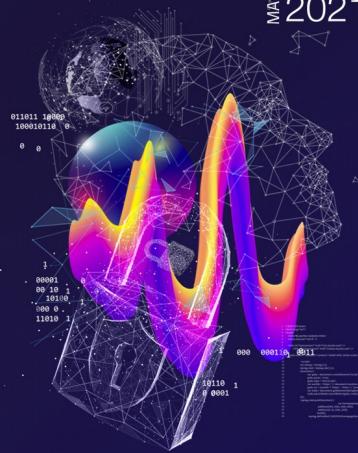
¿Qué es un Honeypot?

Sistema diseñado como señuelo o trampa contra posibles atacantes, que simula ser un servicio válido con el objetivo de analizar el ataque.





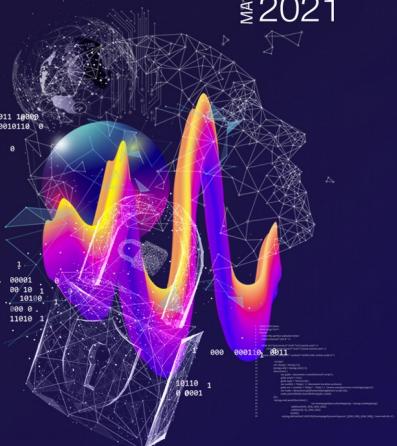
¿Qué obtenemos con esto?





2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

MARTES
28/09
2021



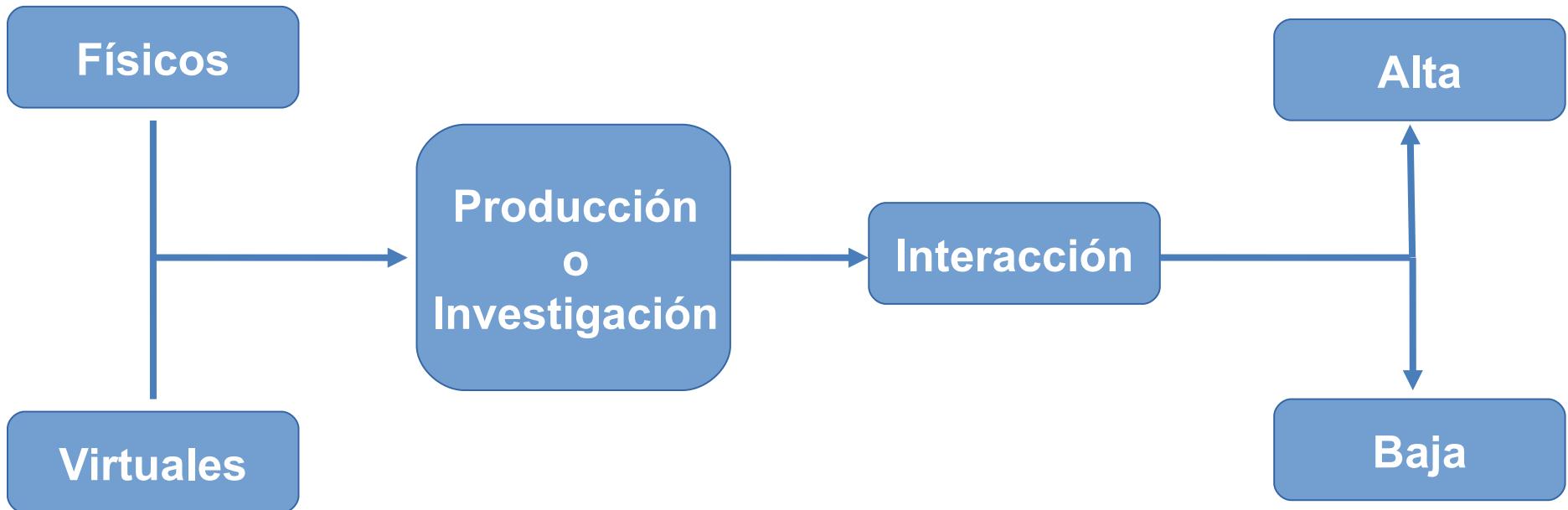
Como el Honeypot se encuentra diseñado para ser "vulnerable" el atacante intentará obtener acceso, intento que será registrado por las diferentes herramientas que cuenta el sistema.

Con esa información podemos bloquear la IP del atacante para evitar un daño mayor, recopilar información para realizar análisis forense o bien tomar alguna acción legal, obtener información de métodos de ataque.





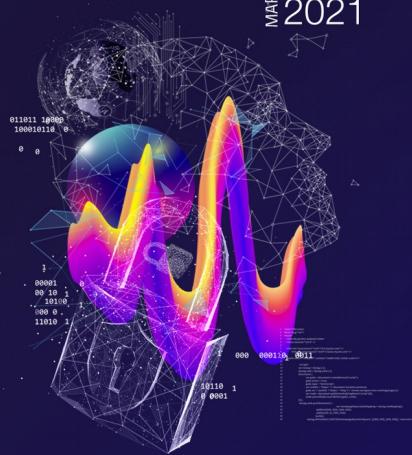
Tipos de HoneyPot



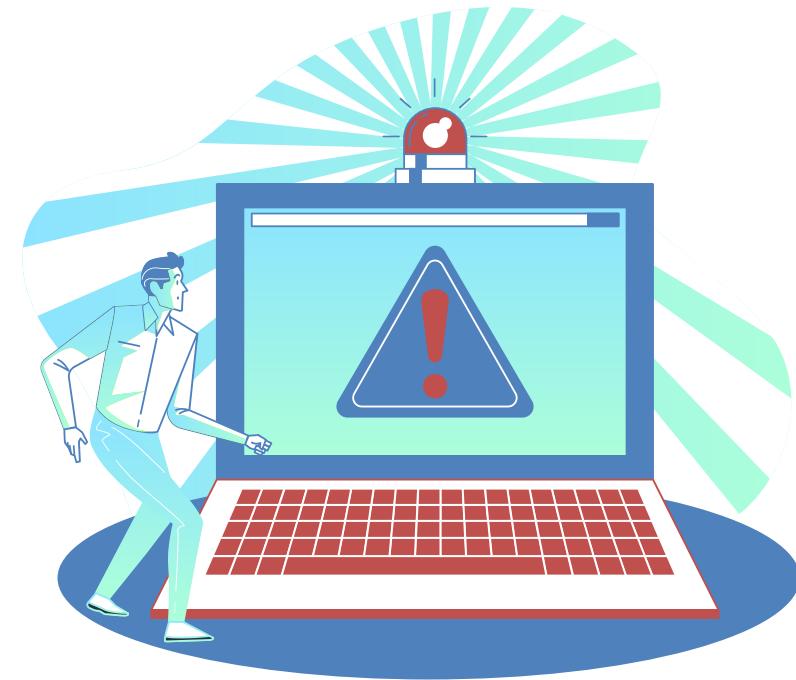


2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

MARTES
28/09
2021



¿Existen riesgos?



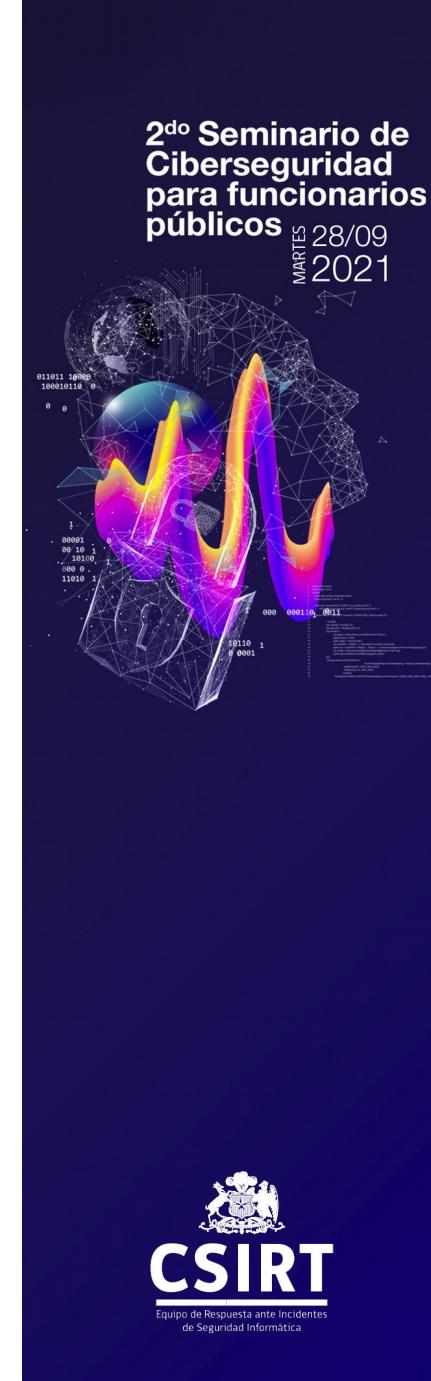
- Se recomienda implementar en red totalmente aislada
- Nunca descuidar su función y dejar de monitorearla



T-Pot, ¿qué es?

<https://github.com/telekom-security/tpotce>

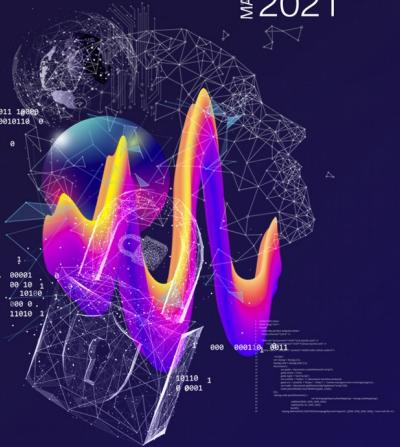
<https://www.csirt.gob.cl/estadisticas/la-implementacion-del-mes-no-2/>





2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

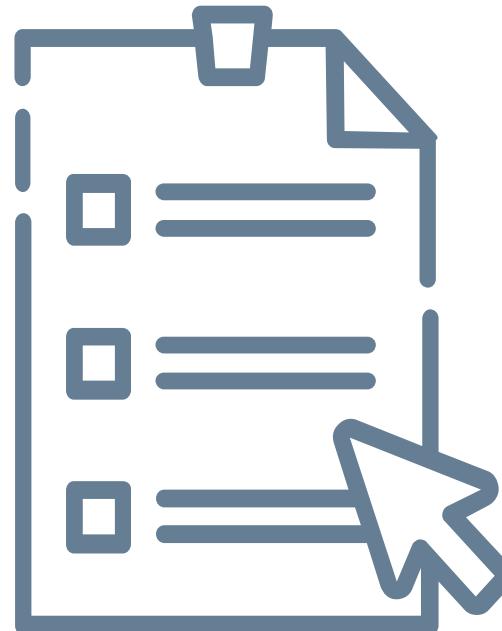
MARTES
28/09
2021

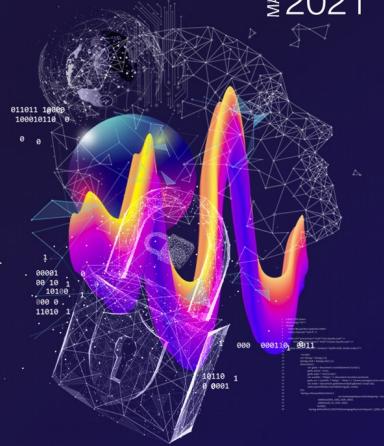


Instalación

Requerimientos Mínimos

- ✓ 8 GB RAM / 4 CPU
- ✓ 128 GB SSD
- ✓ Network via DHCP
- ✓ Conexión a internet (sin proxy)

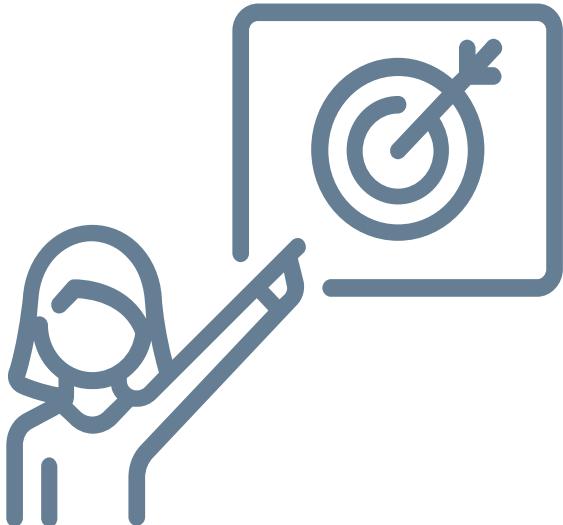




Tips

Para una máquina virtual la interfaz de red debe estar configurada en modo promiscuo

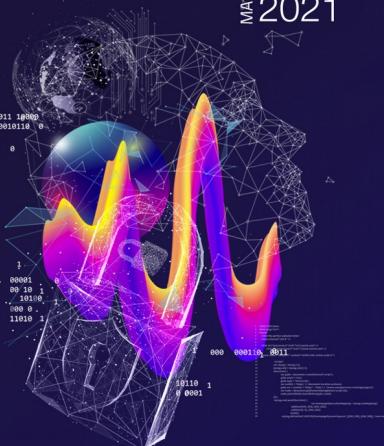
Para una instalación en un host físico es posible que no se detecte algún hardware como las tarjetas de red, por lo que se deberán cargar de forma manual, esto debido a que se han realizado pruebas limitadas en la plataforma Intel NUC





2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

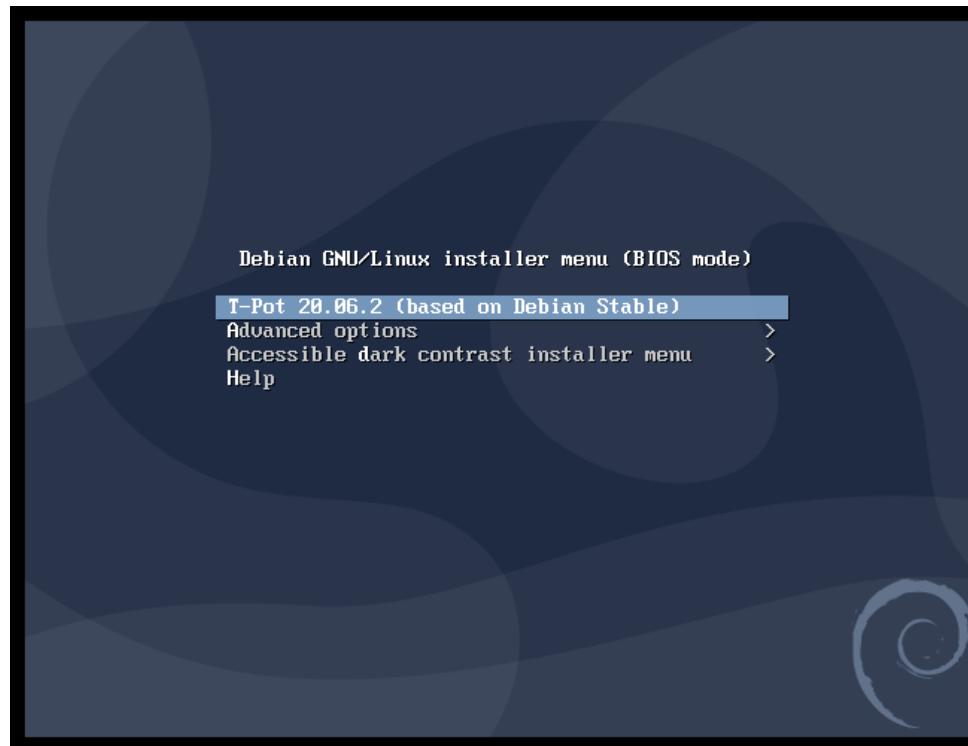
MARTES
28/09
2021



Descargar ISO desde <https://github.com/telekom-security/tpotce/releases>

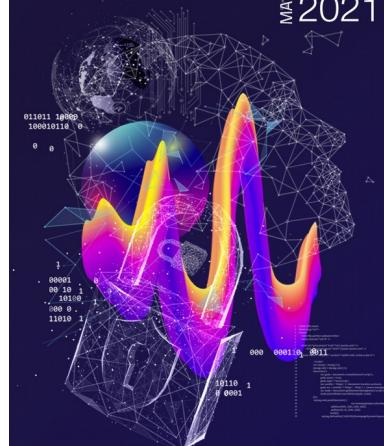
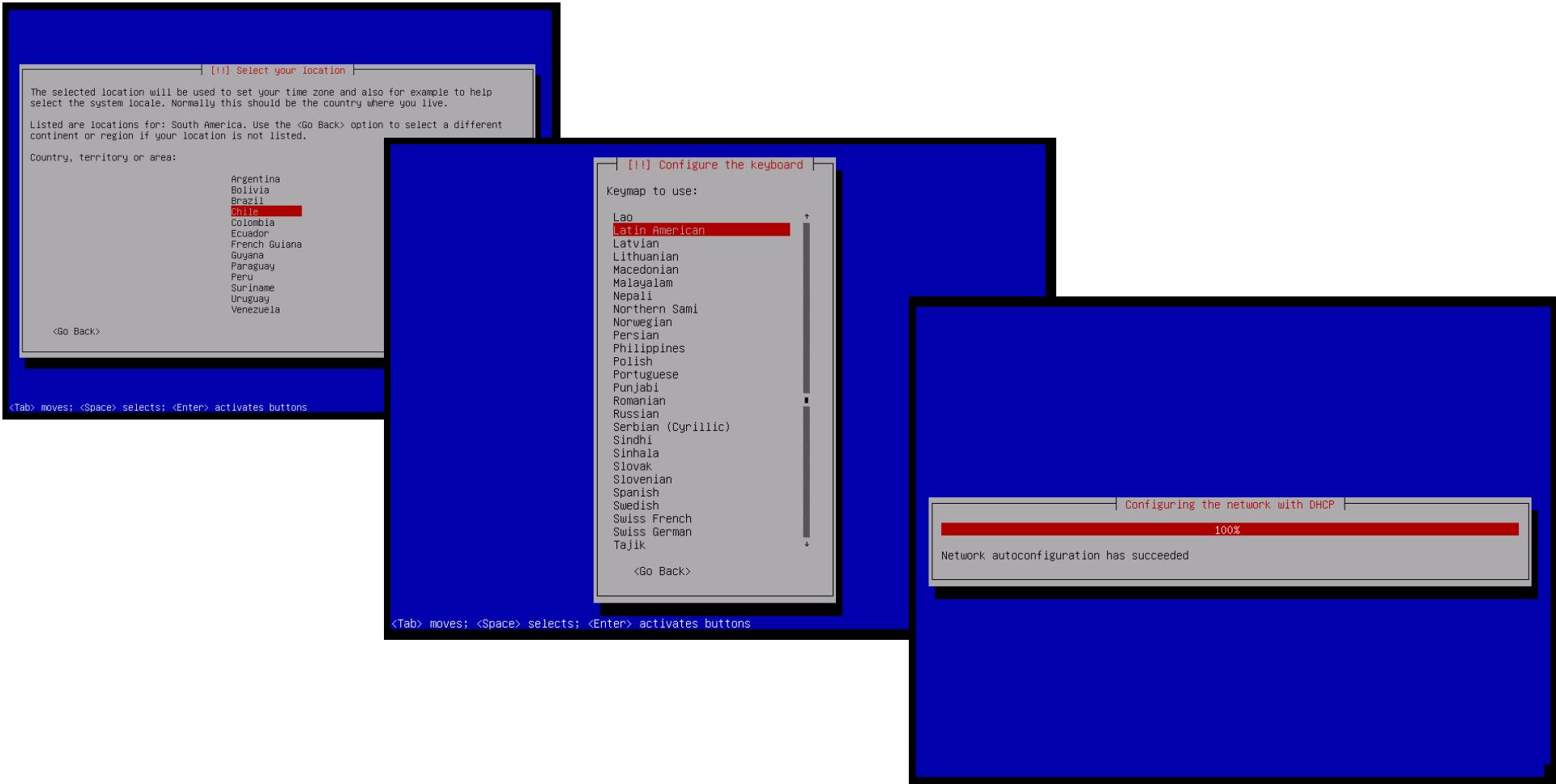
O bien crearla siguiendo los pasos indicados en el manual disponible en el sitio web del CSIRT

Para una máquina virtual como el ejemplo a continuación, se deberá montar el ISO y luego encender la máquina.





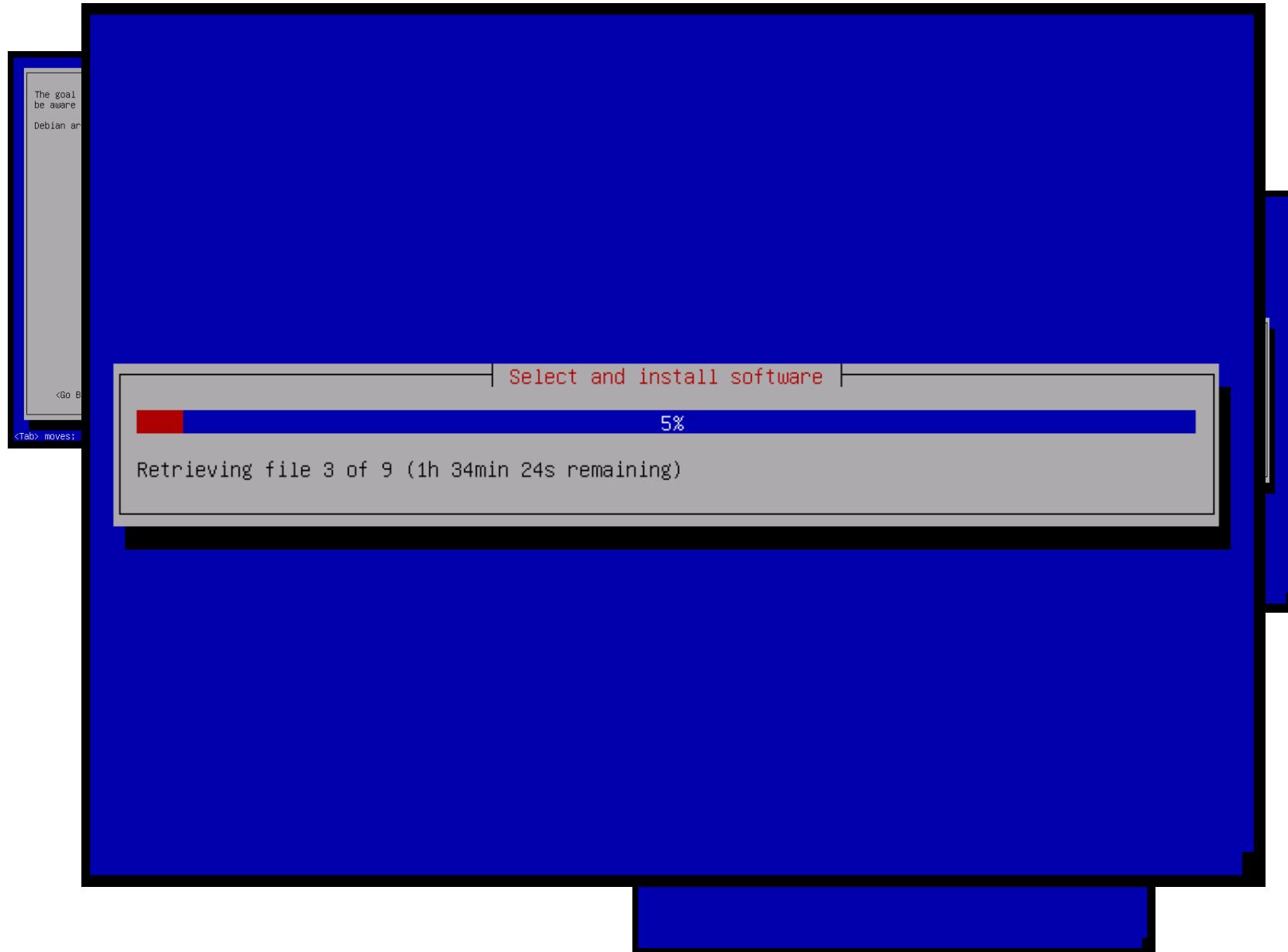
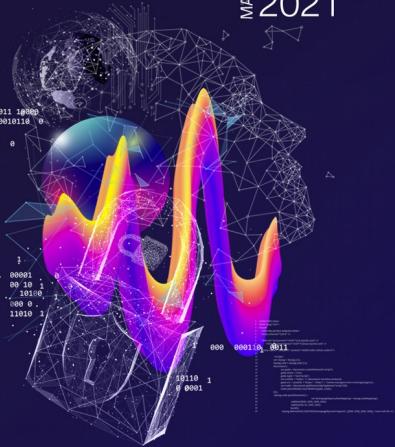
Luego, como la mayoría de las instalaciones de Debian, se debe seleccionar la Ubicación, el tipo de teclado y luego pasará a la configuración de la red, en este caso se realiza de forma automática gracias al DHCP.





2^{do} Seminario de Ciberseguridad para funcionarios públicos

MARTES
28/09
2021





```
GNU GRUB version 2.02+dfsg1-20+deb10u4

*Debian GNU/Linux
Advanced options for Debian GNU/Linux

Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
curl is already the newest version (7.64.0-4+deb10u2).
sudo is already the newest version (1.8.27-1+deb10u3).
The following NEW packages will be installed:
  wget
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 902 kB of archives.
After this operation, 3,335 kB of additional space will be used.
Get:1 http://deb.debian.org/debian/bust/main wget amd64 1.20.1-1.1
Fetched 902 kB in 2s (554 kB/s)
Selecting previously unselected package wget (Reading database ... 27000 files and directories currently installed).
Preparing to unpack .../wget_1.20.1-1.1 ...
Unpacking wget (1.20.1-1.1) ...
Setting up wget (1.20.1-1.1) ...
Press enter to boot the selected entry. Press 'c' for a complete manual boot or 'd' for a direct boot.
Hit:1 http://deb.debian.org/debian/bust/main wget amd64 1.20.1-1.1
Hit:2 http://security.debian.org/debian-security/bust/main libaria2-0 amd64 0.8.1-1+b1
Hit:3 http://deb.debian.org/debian/bust/main libcurl3-openssl4 amd64 7.64.0-4+b1
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libaria2-0 libcurl3-openssl4
The following NEW packages will be installed:
  aria2 libaria2-0 libcurl3-openssl4
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,539 kB of additional space will be used.
After this operation, 6,098 kB of additional space will be used.
Get:1 http://security.debian.org/debian-security/bust/main libaria2-0 amd64 0.8.1-1+b1 [86.1 kB]
Get:2 http://deb.debian.org/debian/bust/main libcurl3-openssl4 amd64 7.64.0-4+b1 [1,002 kB]
63% [2 libaria2-0 1,002 kB/1,091 kB 92%]
```

T-Pot-Installer

[Availability check]

Now checking: https://listbot.sicherheitstacho.eu

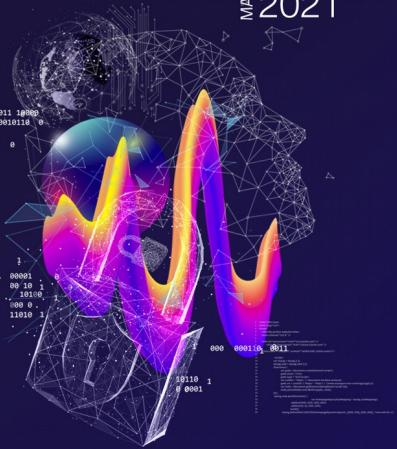
80%





2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

MARTES
28/09
2021



T-Pot-Installer

[Choose Your T-Pot Edition]

Required: 8GB RAM, 128GB SSD

Recommended: 8GB RAM, 256GB SSD

STANDARD

Honeypots, ELK, NSM & Tools

SENSOR

Just Honeypots, EWS Poster & NSM

INDUSTRIAL

Conpot, RDPY, Vnclowpot, ELK, NSM & Tools

COLLECTOR

Heralding, ELK, NSM & Tools

NEXTGEN

NextGen (Glutton, HoneyPy)

MEDICAL

Dicompot, Medpot, ELK, NSM & Tools

< OK >



Standard

- Honeypots: adbhone, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeysap, honeytrap, mailoney, medpot, rdp, snare & tanner
- Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

Sensor

- Honeypots: adbhone, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeypy, honeysap, honeytrap, mailoney, medpot, rdp, snare & tanner
- Tools: cockpit, ewsposter, fatt, p0f & suricata
- Since there is no ELK stack provided the Sensor Installation only requires 4 GB of RAM.

Industrial

- Honeypots: conpot, cowrie, dicompot, heralding, honeysap, honeytrap, medpot & rdp
- Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

Collector

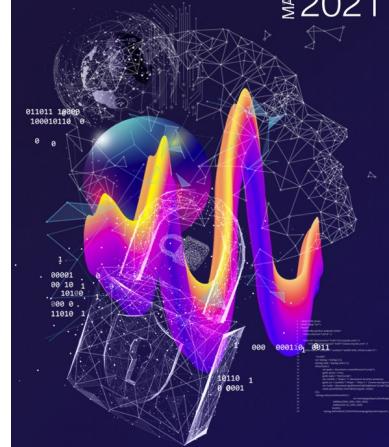
- Honeypots: heralding & honeytrap
- Tools: cockpit, cyberchef, fatt, ELK, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

NextGen

- Honeypots: adbhone, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, glutton, heralding, honeypy, honeysap, ipponey, mailoney, medpot, rdp, snare & tanner
- Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

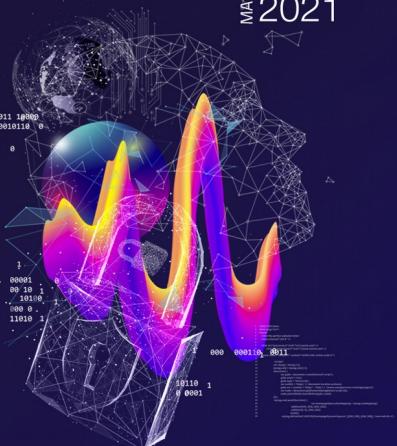
Medical

- Honeypots: dicompot & medpot
- Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata



2^{do} Seminario de
Ciberseguridad
para funcionarios
públicos

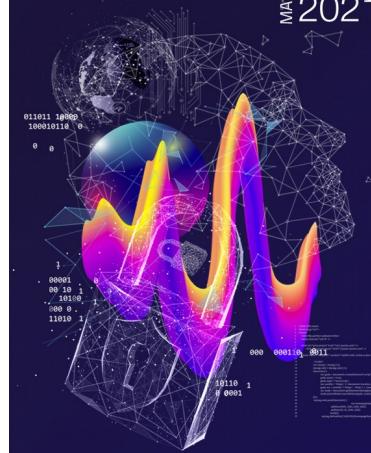
MARTES
28/09
2021



- Cockpit** for a lightweight, webui for docker, os, real-time performance monitoring and web terminal.
- Cyberchef** a web app for encryption, encoding, compression and data analysis.
- ELK stack** to beautifully visualize all the events captured by T-Pot.
- Elasticsearch Head** a web front end for browsing and interacting with an Elastic Search cluster.
- Fatt** a pyshark based script for extracting network metadata and fingerprints from pcap files and live network traffic.
- Spiderfoot** a open source intelligence automation tool.
- Suricata** a Network Security Monitoring engine.



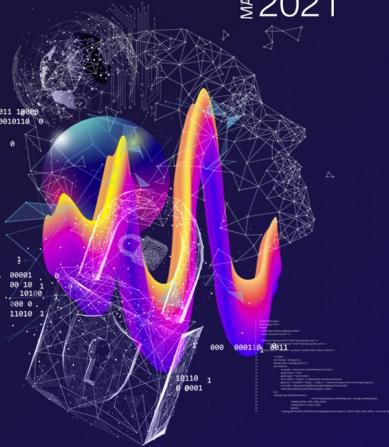
```
[ 0%] [ 25%] [ 50%] [ 75%] [ 100%]
09/23 18:46:30 [NOTICE] Download complete: /var/cache/apt/apt-fast/libalgorithm-merge-perl_0.08-3_amd64.deb
### Getting update info for deb1.deb
[DL:574KiB] [#5705e5 18MiB/51MiB(36%)] [#f51b71 3.0MiB/4.7MiB(64%)] [#a5231b 16KiB/25KiB(63%)] [#07d62a
16KiB/567KiB(2%)] [#2dd842 0B/144KiB(0%)]
Hit:1 http://deb.debian.org/debian [DL:578KiB] [#5705e5 18MiB/51MiB(37%)] [#f51b71 3.2MiB/4.7MiB(68%)] [#a5231b 16KiB/25KiB(63%)] [#07d62a
16KiB/567KiB(14%)] [#2dd842 48KiB/144KiB(33%)]
Hit:2 http://security.debian.org/debian-security [DL:578KiB] [#5705e5 18MiB/51MiB(37%)] [#f51b71 3.2MiB/4.7MiB(68%)] [#a5231b 16KiB/25KiB(63%)] [#07d62a
16KiB/567KiB(14%)] [#2dd842 48KiB/144KiB(33%)]
Hit:3 http://deb.debian.org/debian [DL:554KiB] [#5705e5 19MiB/51MiB(37%)] [#f51b71 3.3MiB/4.7MiB(70%)] [#a5231b 16KiB/25KiB(63%)] [#07d62a
16KiB/567KiB(16%)] [#2dd842 112KiB/144KiB(77%)]
Reading package lists...
### Upgrading packages.
09/23 18:46:34 [NOTICE] Verification finished successfully. file=/var/cache/apt/apt-fast/libhavoc1_1.9.1-7_amd64.deb
info: Trying to set 'doc'
info: Loading answer for deb1.deb
09/23 18:46:34 [NOTICE] Download complete: /var/cache/apt/apt-fast/libhavoc1_1.9.1-7_amd64.deb
info: Trying to set 'deb1.deb'
[DL:570KiB] [#5705e5 19MiB/51MiB(38%)] [#f51b71 3.5MiB/4.7MiB(73%)] [#07d62a 112KiB/567KiB(19%)] [#2dd842
112KiB/144KiB(77%)] [#e5f1e2 0B/244KiB(0%)]
[apt-fast 18:41:54]
[apt-fast 18:41:54] Working...
09/23 18:46:34 [NOTICE] Verification finished successfully. file=/var/cache/apt/apt-fast/libblas3_3.8.0-2_amd64.deb
W: --force-yes is deprecated.
Reading package lists...
Building dependency tree
09/23 18:46:34 [NOTICE] Download complete: /var/cache/apt/apt-fast/libblas3_3.8.0-2_amd64.deb
Reading state information
[DL:559KiB] [#5705e5 20MiB/51MiB(39%)] [#f51b71 3.5MiB/4.7MiB(75%)] [#07d62a 144KiB/567KiB(25%)] [#e5f1e2
16KiB/244KiB(6%)] [#fe7698 32KiB/116KiB(27%)]
Calculating upgrade...
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
W: --force-yes is deprecated.
09/23 18:46:36 [NOTICE] Verification finished successfully. file=/var/cache/apt/apt-fast/libvolume-key1_0.3.12-2+b1_amd64.deb
### Installing T-Pot dependencies
09/23 18:46:36 [NOTICE] Download complete: /var/cache/apt/apt-fast/libvolume-key1_0.3.12-2+b1_amd64.deb
[apt-fast 18:41:56]
[apt-fast 18:41:56] Working...
09/23 18:46:36 [NOTICE] Verification finished successfully. file=/var/cache/apt/apt-fast/libblockdev-crypto2_2.20-7+deb10u1_amd64.deb
09/23 18:46:36 [NOTICE] Verification finished successfully. file=/var/cache/apt/apt-fast/libblockdev-crypto2_2.20-7+deb10u1_amd64.deb
09/23 18:46:36 [NOTICE] Download complete: /var/cache/apt/apt-fast/libblockdev-crypto2_2.20-7+deb10u1_amd64.deb
```





2^{do} Seminario de Ciberseguridad para funcionarios públicos

MARTES
28/09
2021



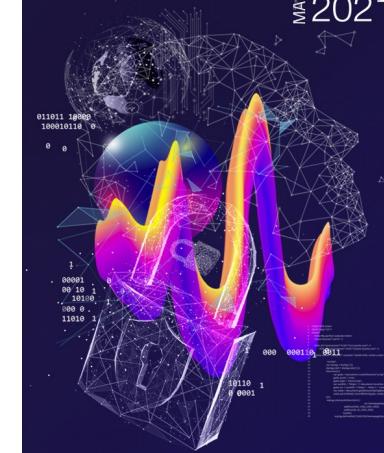
```
---- [ continentalsidecar ] [ Fri Sep 24 2021 ] [ 16:04:37 ]
| IP: 192.168.3.25 (186.107.184.133)
| SSH: ssh -l tsec -p 64295 192.168.3.25
| WEB: https://192.168.3.25:64297
| ADMIN: https://192.168.3.25:64294
|
----[br]
continentalsidecar login: _
```



Demostración

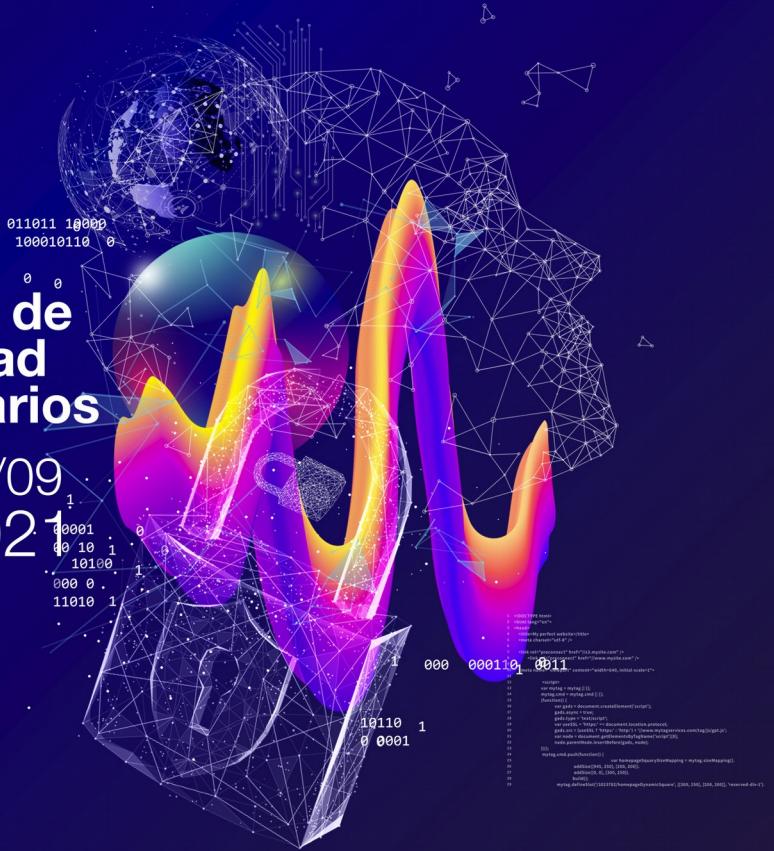
<https://181.212.41.75:64297/>

<https://181.212.41.75:64294/>



2º Seminario de Ciberseguridad para funcionarios públicos

MARTES
28/09
2021



CSIRT
<https://www.csirt.gob.cl/>
Teatinos 92 piso 6
Santiago, Chile