CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

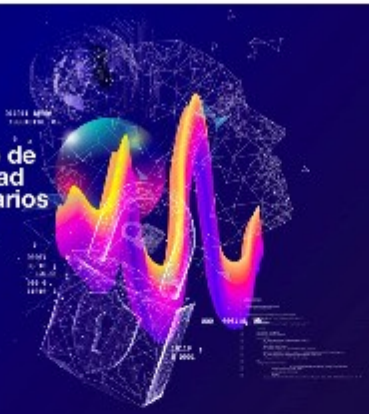
2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT



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

Miguel Kurte Araya

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

2do Seminario de Ciberseguridad para funcionarios públicos

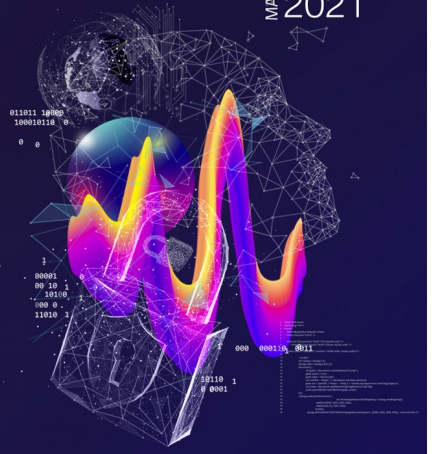
MARTES 28/09 2021

Tabla de contenido

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
MARTES 28/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

¿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.

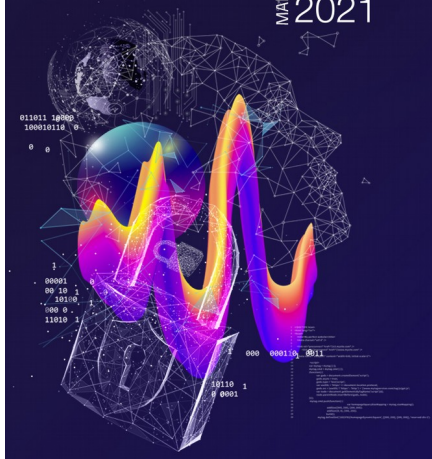
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¿Qué obtenemos con esto?

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

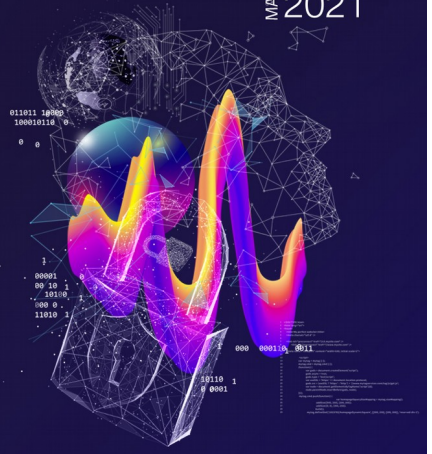


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

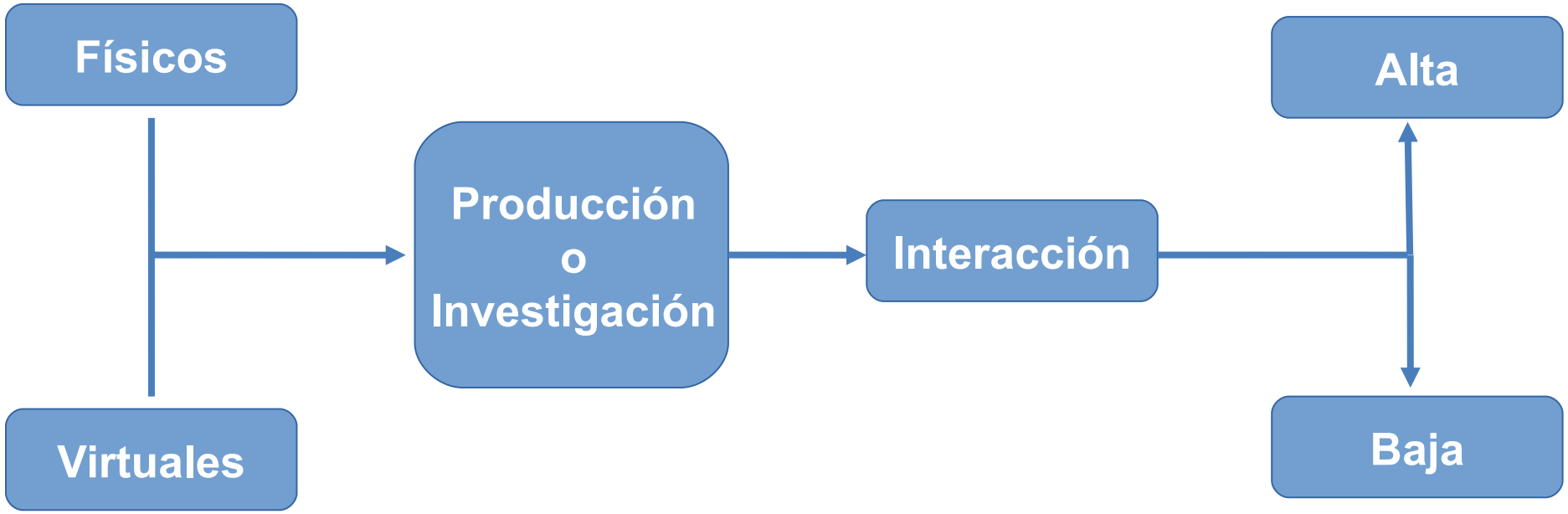
Como el Honeypot se encuentra diseñado para ser "vulnerable" el atacante intentará obtener acceso, intento que será registrado por las diferentes herramientas que cuenta el sistema.

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.

Ministerio del Interior y Seguridad Pública

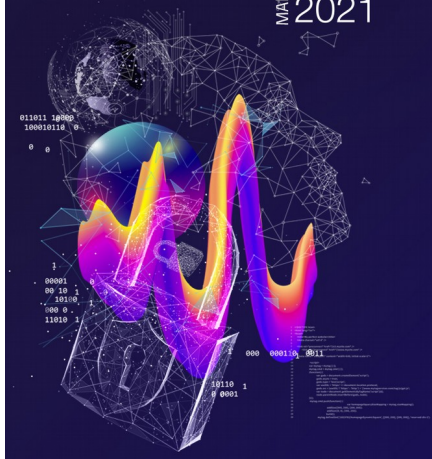
Gobierno de Chile

Tipos de HoneyPot



2do Seminario de Ciberseguridad para funcionarios públicos

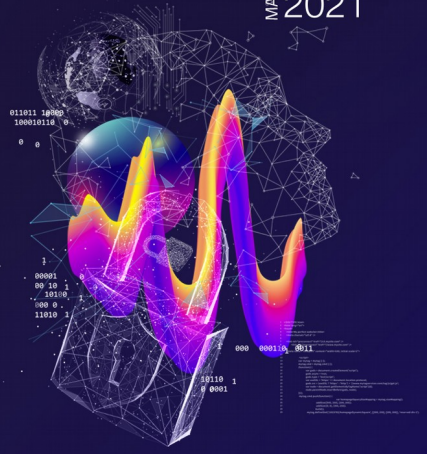
MARTES 28/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
MARTES 28/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

¿Existen riesgos?

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

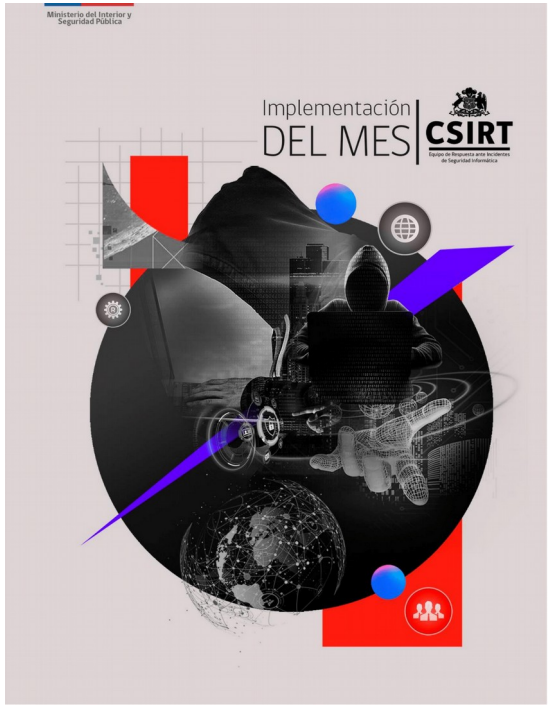
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

T-Pot, ¿qué es?

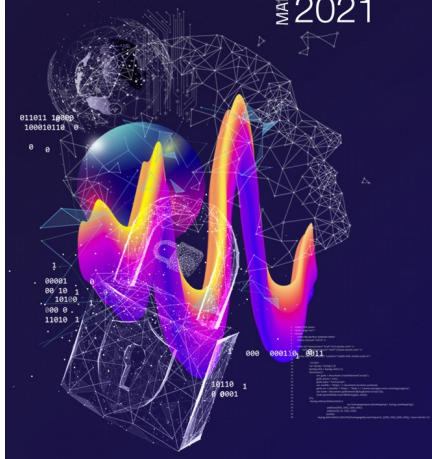
https://github.com/telekom-security/tpotce

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



2do Seminario de Ciberseguridad para funcionarios públicos

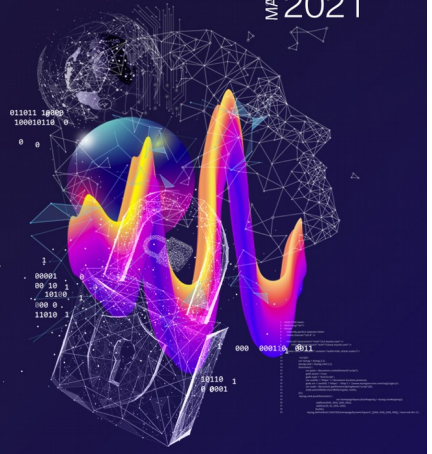
MARTES 28/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
MARTES 28/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Instalación

Requerimientos Mínimos

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

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

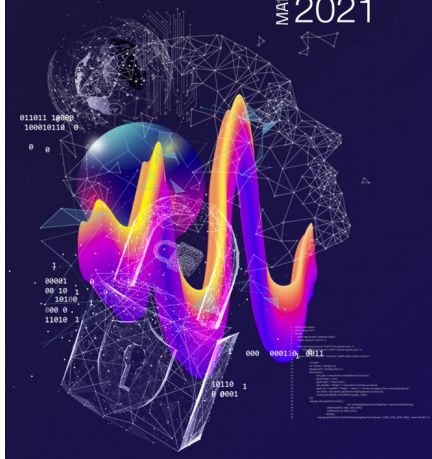
Tips

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 platadorma Intel NUC

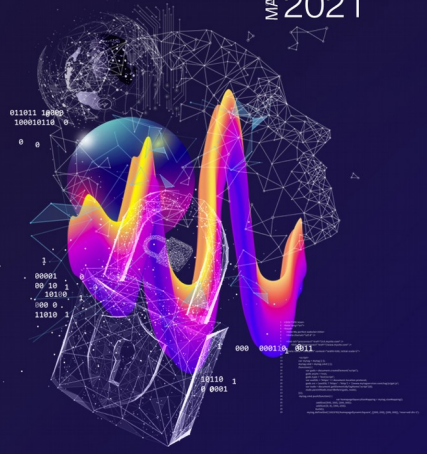
2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



CSIRT

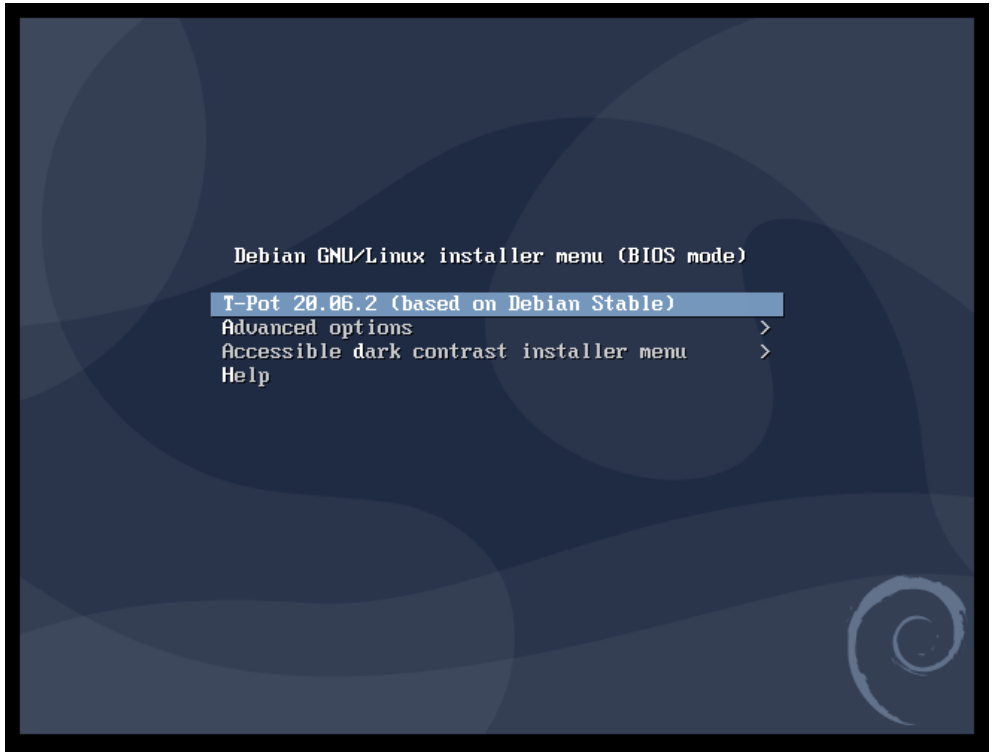
Equipo de Respuesta ante Incidentes de Seguridad Informática



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

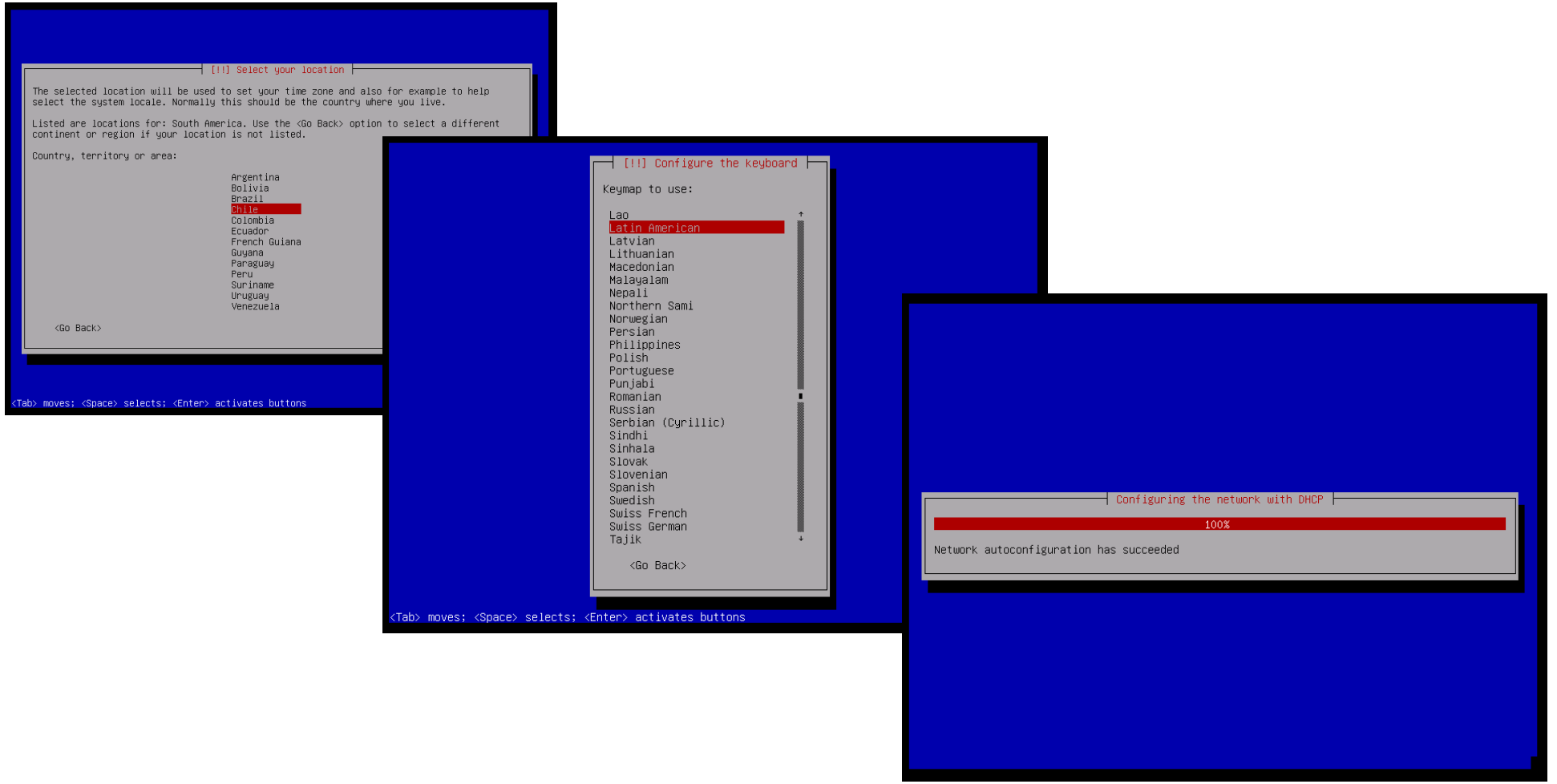
Para una máquina virtual como el ejemplo a continuación, se deberá montar el ISO y luego encender la máquina.



Ministerio del Interior y Seguridad Pública

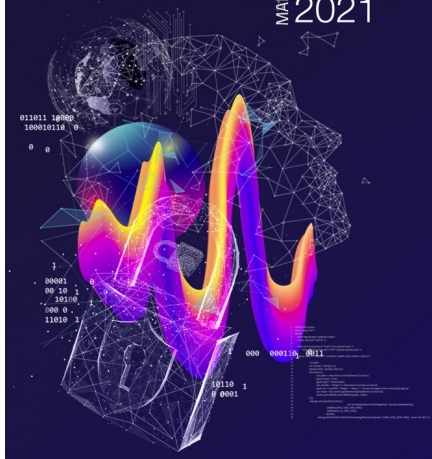
Gobierno de Chile

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.



2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

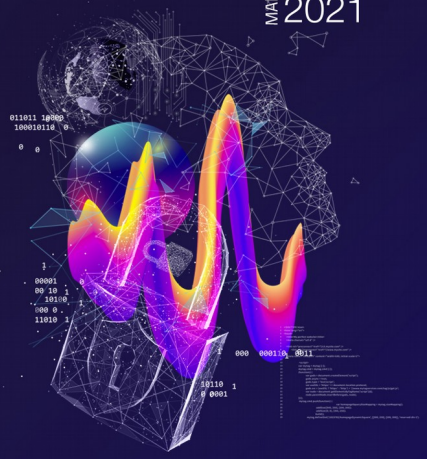


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

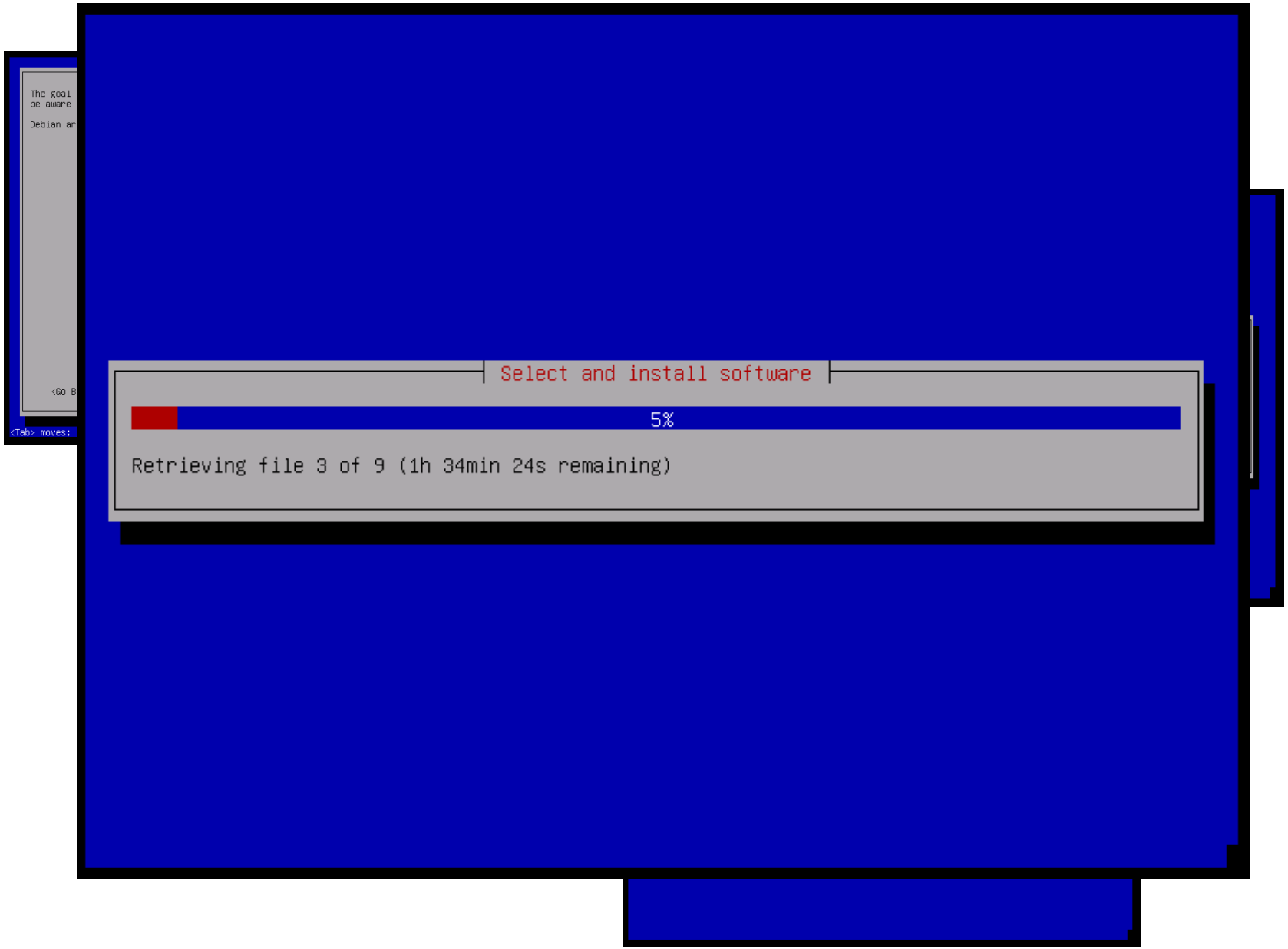


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Gobierno de Chile



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

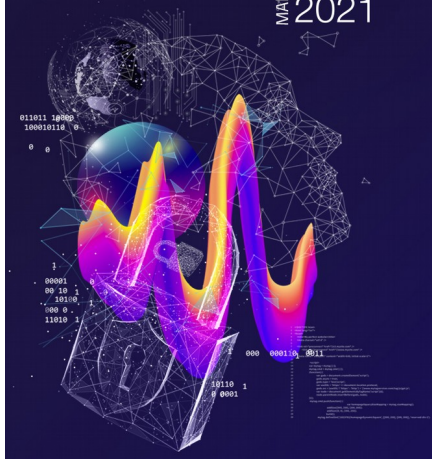
```
                    GNU GRUB  version 2.02+dfsg1-20+deb10u4

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

      Use the ↑ and ↓ keys to selec
      Press enter to boot the selec
      before booting or `c' for a c
```

```
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 addit
Get:1 http://deb.debian.org/debian bust
Fetched 902 kB in 2s (554 kB/s)
Selecting previously unselected package
(Reading database ... 27000 files and d
Preparing to unpack .../wget_1.20.1-1.1
Unpacking wget (1.20.1-1.1) ...
Setting up wget (1.20.1-1.1) ...
### Installing apt-fast
Hit:1 http://deb.debian.org/debian bust
Hit:2 http://security.debian.org/debian
Hit:3 http://deb.debian.org/debian bust
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will
  libaria2-0 libc-ares2
The following NEW packages will be inst
  aria2 libaria2-0 libc-ares2
0 upgraded, 3 newly installed, 0 to rem
Need to get 1,539 kB of archives.
After this operation, 6,098 kB of addit
Get:1 http://security.debian.org/debian
+deb10u1 [86.1 kB]
Get:2 http://deb.debian.org/debian bust
63% [2 libaria2-0 1,002 kB/1,091 kB 92%
```

```
T-Pot-Installer

[ Availability check ]

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

80%
```

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

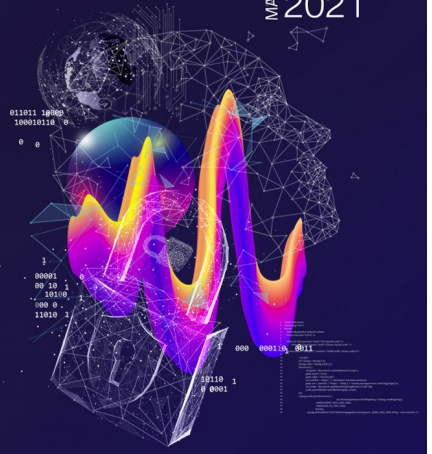


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

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 >

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

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

Sensor
-Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeypy, honeysap, honeytrap, mailoney, medpot, rdpy, 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 & rdpy
-Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

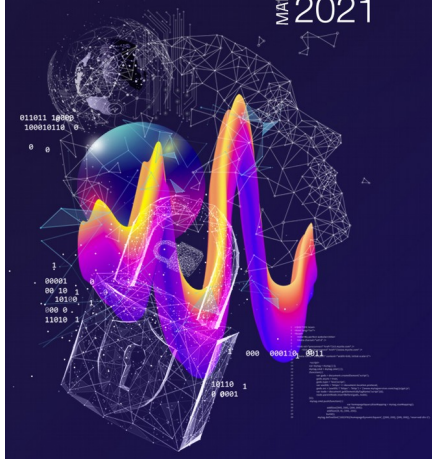
Collector
-Honeypots: heralding & honeytrap
-Tools: cockpit, cyberchef, fatt, ELK, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

NextGen
-Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, glutton, heralding, honeypy, honeysap, ipphoney, mailoney, medpot, rdpy, 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

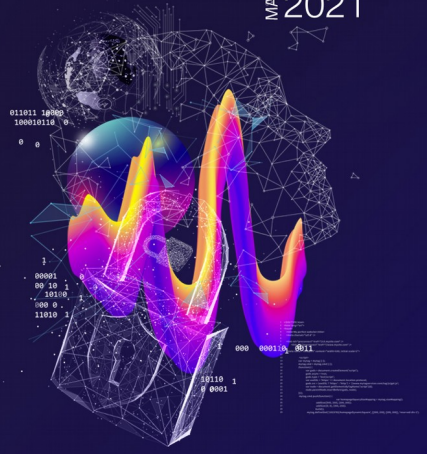
2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática



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.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

2do Seminario de Ciberseguridad para funcionarios públicos

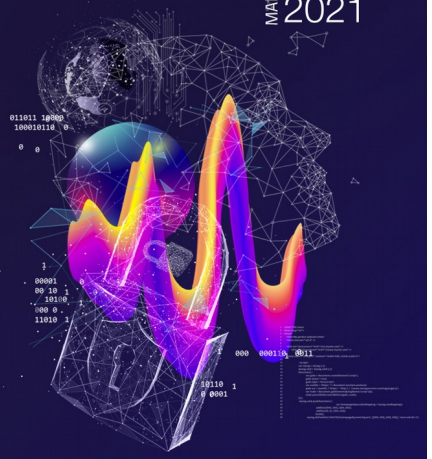
MARTES 28/09 2021

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

```
,---- [ 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
|
`----

continentalsidecar login: _
```

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

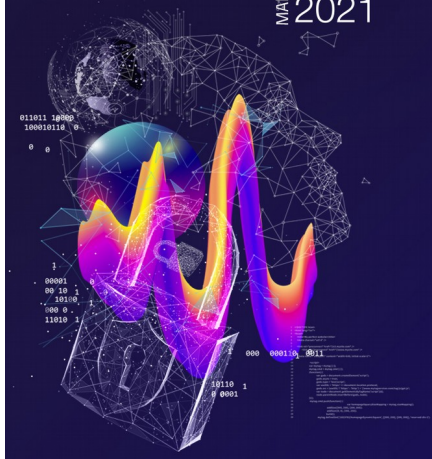
Demostración

https://181.212.41.75:64297/

https://181.212.41.75:64294/

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

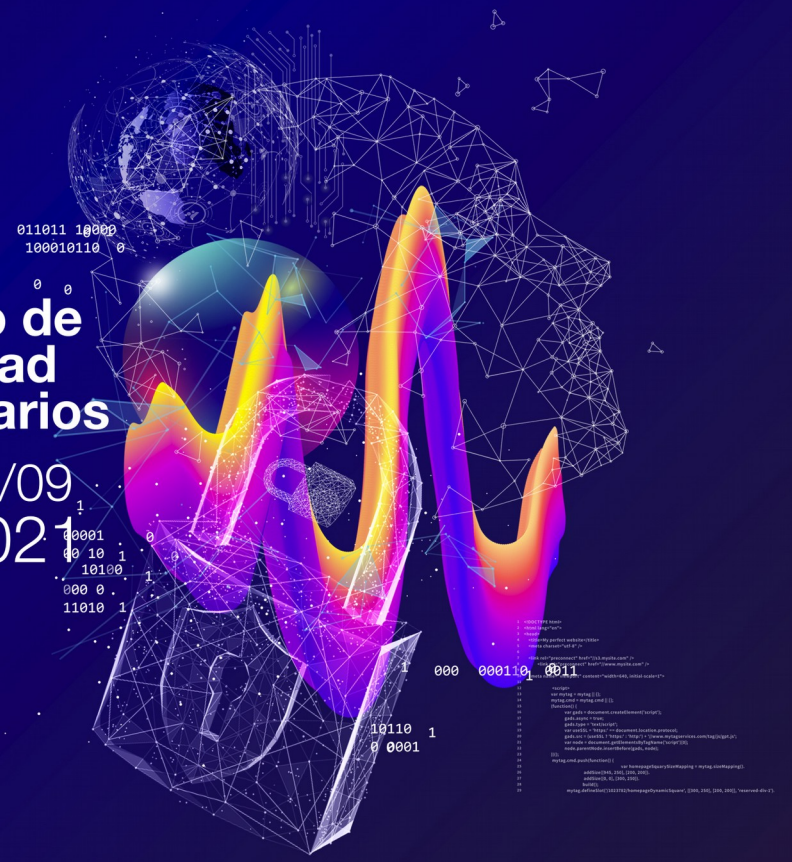


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile