

Forum:[Hack Forums](#)

Thread: [how do you hack anonymouse ftp on windows server?](#)

bdkalkun - March 29, 2019, 3:32 pm

hello guys

Quote:Not shown: 65528 filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	Microsoft ftpd
--------	------	-----	----------------

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| 03-28-19 01:07AM <DIR> 6KY2Q3B6

| 09-11-14 03:08AM <DIR> aspnet_client

| 12-15-14 09:41PM 0 ftp?????.php

| 02-12-19 11:24PM 3528005 info.zip

|_ 03-28-19 01:07AM <DIR> N2J7HJZT

| ftp-syst:

|_ SYST: Windows_NT

53/tcp	open	domain	Microsoft DNS 6.1.7601 (1DB15EC5) (Windows Server 2008 R2 SP1)
--------	------	--------	--

| dns-nsid:

|_ bind.version: Microsoft DNS 6.1.7601 (1DB15EC5)

80/tcp	open	http	Microsoft IIS httpd 7.5
--------	------	------	-------------------------

| http-methods:

| Supported Methods: OPTIONS TRACE GET HEAD POST

|_ Potentially risky methods: TRACE

|_ http-server-header: Microsoft-IIS/7.5

|_ http-title: 404 - File or directory not found.

3389/tcp	open	ms-wbt-server	Microsoft Terminal Service
----------	------	---------------	----------------------------

| ssl-cert: Subject: commonName=file

| Issuer: commonName=file

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha1WithRSAEncryption

| Not valid before: 2017-04-23T01:47:17

| Not valid after: 2017-10-23T01:47:17

| MD5: 3787 b6f8 26a2 35c3 c8a6 1c81 e682 2c98

|_SHA-1: 34fe 219a d317 0cb0 342f 076a 90d9 9077 e244 0da3

|_ssl-date: 2019-03-29T17:47:52+00:00; +7s from scanner time.

5405/tcp open netsupport NetSupport PC remote control (Name FILE)

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

i need your help to gain access to this ip...as you can see what seems to be potential starting point is ftp port because its allow anonymouse login

but i cant access uploaded file since the uploaded dir isnt in WWW
any suggestion guys?

bitkiddy - April 5, 2019, 3:53 am

If anonymous login isn't possible:

exploit-db.com

or bruteforce it with JTR, Hydra or nmap.

\$> proxychains nmap --script=brute-ftp <wordlist> <ip>

bdkalkun - April 12, 2019, 8:59 pm

(Apr 5, 2019 03:53 AM)bitkiddy Wrote: [\[CITE\]](#) If anonymous login isn't possible:

exploit-db.com

or bruteforce it with JTR, Hydra or nmap.

\$> proxychains nmap --script=brute-ftp <wordlist> <ip>
anonymouse login is allowed

bitkiddy - April 25, 2019, 5:59 am

(Apr 12, 2019 08:59 PM)bdkalkun Wrote: [\[CITE\]](#) anonymouse login is allowed
Upload a Shellcode over FTP with netcat?

F.A.S.T - April 25, 2019, 11:35 am

If you can login, just upload a backdoor to the server.

realsunjester - April 25, 2019, 11:42 am

(Apr 12, 2019 08:59 PM)bdkalkun Wrote: [\[CITE\]](#) anonymouse login is allowed
the first thing you need to do is identify the version of the ftp server. most anonymous ftp's nowadays are (probably) honeypots. i would check for open source exploits on exploit-db, cxsecurity, packetstorm, and other exploit archive sites.

if that fails, then you should get a hold of the ftp server software and attack it yourself with fuzzers and debuggers and try to find an exploit yourself.

as for people suggesting to upload a shell/backdoor, sorry but 99% of the time it wont work since you wouldn't be able to execute it on the server or access it from a web interface to use it.

plus, most anonymous accounts won't have the ability or get outside of the ftp directory (view other dirs) that it's assigned, won't have the privileges to execute files or to do anything but view files in the assigned directory.

Nexium - April 25, 2019, 11:49 am

Fun idea would be, to code a bruter ftp. Find a very big world list + text scraper and upload a ftp bruter like a miner on 100 bots, and leave it for about an week and then check for results.