

Compromised FTP

Challenge

34 Solves

×

Compromised FTP

25

We detected some malicious activity on our FTP server. Someone has performed bruteforce attack to gain access to our FTP server. Find out the Compromised FTP account username & the attacker IP from the following.

Download Link

Alternative Links:

Link - 1

Link - 2

Link - 3

Link - 4

Link - 5

Flag Format: KCTF{username_127.0.0.1}

Author : TareqAhamed

Flag

Submit

```
Mon Jan 3 15:27:48 2022 [pid 12100] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:48 2022 [pid 12106] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 10488] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 10490] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 12054] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 12105] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 10890] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 10895] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 12089] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 12081] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:51 2022 [pid 10897] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 10899] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12105] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12108] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12110] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12083] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12095] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12097] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12099] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12100] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12112] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:52 2022 [pid 12114] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:53 2022 [pid 12116] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:53 2022 [pid 12118] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:54 2022 [pid 12054] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:54 2022 [pid 12107] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:54 2022 [pid 12108] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:54 2022 [pid 12105] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12089] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12111] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12091] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12113] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12106] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12083] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12095] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12097] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12099] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12100] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12174] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12115] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:55 2022 [pid 12117] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:56 2022 [pid 12252] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:56 2022 [pid 12255] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:56 2022 [pid 12284] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:56 2022 [pid 12286] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:56 2022 [pid 12293] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:56 2022 [pid 12298] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:56 2022 [pid 12302] [PlcmSpIp_192.168.1.7] CONNECT: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:58 2022 [pid 12107] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:58 2022 [pid 12108] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:58 2022 [pid 12103] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
Mon Jan 3 15:27:58 2022 [pid 12173] [PlcmSpIp_192.168.1.7] FAIL LOGIN: Client "::::ffff:192.168.1.7"
```

KCTF{PlcmSpIp_192.168.1.7}

KCTF{admin_192.168.1.7}

KCTF{ADMIN_192.168.1.7}

일단 그냥 대충 때려 넣어봤는데 안 됨

제일 시도가 많은 거 아닐까 싶어 exel로 합계 내봄

Aa 행 레이블	# 개수 : Column9
[a]	67
[admin]	1005
[adtec]	67
[anonymous]	67
[apc]	134

Aa 행 레이블	# 개수 : Column9
[avery]	67
[beijer]	67
[default]	67
[device]	67
[dm]	67
[dmftp]	67
[fdrusers]	67
[ftp]	134
[ftp_boot]	67
[ftpuser]	52
[Guest]	67
[httpadmin]	67
[IEleMerge]	67
[instrument]	67
[loader]	67
[localadmin]	67
[MayGion]	67
[MELSEC]	67
[nic2212]	67
[nmt]	67
[none]	67
[ntpupdate]	67
[pcfactory]	67
[PlcmSplp]	67
[qbf77101]	67
[QNUDECPU]	67
[root]	335
[se]	67
[su]	67
[supervisor]	67
[sysdiag]	67
[test]	67

Aa 행 레이블	# 개수 : Column9
[uploader]	67
[User]	335
[user1]	67
[webserver]	67
[wsupgrade]	67
<u>CONNECT:</u>	1473
<u>총합계</u>	5880

KCTF{ftp_192.168.1.7}

KCTF{User_192.168.1.7}

KCTF{root_192.168.1.7}

빈도 수 많은 거 몇 개 넣어봤는데 안 됨

그냥 username 하나하나 때려 넣어보다가 찾음

FLAG : KCTF{ftpuser_192.168.1.7}