

Soal Pembuka

1. Untuk mendapatkan soal utama anda harus melewati halaman berikut <http://love.avc.or.id/>

Jawaban: Lakukan bypass SQL injection ('a' OR 'a'='a) setelah berhasil masuk, Show Page Source dan anda akan menemukan URL menuju soal utama.

Soal Utama

```
avc@root:~$ cat avc.txt
```

Terjadi serangan pada bank VCA . Anda sebagai ahli , akan diberi log system. Analisa log tersebut.

1. Apa yang anda temukan di log tersebut ?
2. Log itu akan merujuk pada sebuah lokasi. Dimana ?
3. Di lokasi berikutnya akan merujuk lokasi lain, dimana ?
4. Di lokasi nomor 3 akan merujuk pada lokasi baru, dimana ?
5. Di lokasi 4, anda akan menemukan document, apa isinya ?
6. Analisa isi dari dokumen tersebut, dan temukan pelaku penyerangan
7. Apa hasil analisa yang anda lakukan dipoint nomor 7 ?
8. Siapa pelaku dibalik penyerangan bank VCA ?
9. Bagaimana anda data menemukan pelaku tersebut ?
10. Buatlah rincian detail tentang informasi pelaku (Nama lengkap, alamat lengkap, jenis kelamin, foto, NIM pelaku, pekerjaan).





















We have Log File , Maybe you can chek that in here

JAWABAN:

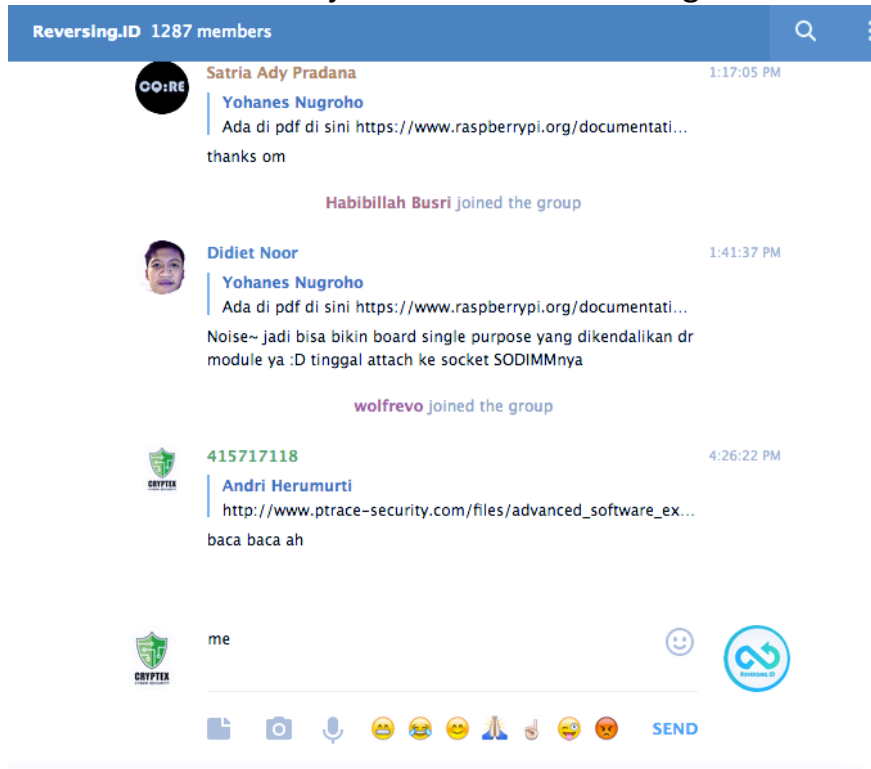
1. Setelah menganalisa log.txt ditemukan log mencurigakan sebagai berikut

```
bl0ck0ck (Wed Nov 29 21:58:20 2017) <cu9600, /dev/nmdm1B> call completed
bl0ck0ck (Wed Nov 29 22:28:34 2017) <cu9600, /dev/nmdm1B> call completed
bl0ck0ck (Wed Nov 29 22:31:47 2017) <cu9600, /dev/nmdm0B> call completed
bl0ck0ck (Thu Nov 30 16:14:13 2017) <cu9600, /dev/nmdm0B> call completed
bl0ck0ck (Thu Nov 30 18:15:29 2017) <cu9600, /dev/nmdm1B> call completed
bl0ck0ck (Thu Nov 30 18:28:15 2017) <cu9600, /dev/nmdm0B> call completed
bl0ck0ck (Thu Nov 30 19:27:09 2017) <cu9600, /dev/nmdm0B> call completed
bl0ck0ck (Mon Dec 4 13:22:01 2017) <cu9600, /dev/nmdm0B> call completed
bl0ck0ck (Sun Dec 10 18:35:42 2017) <cu9600, /dev/nmdm0B> call completed
bl0ck0ck (Sun Dec 10 18:54:49 2017) <cu9600, /dev/nmdm0B> call completed
bl0ck0ck (Sun Dec 10 20:14:28 2017) <cu9600, /dev/nmdm0B> call completed
45.77.97.16 - - [20/Oct/2017:23:22:00 +0700] "GET /login.php HTTP/1.1" 200 45
Nov 30 20:00:00 host newsyslog[10981]: logfile turned over due to size>100K
Nov 30 20:33:09 host sshd[1253]: Server listening on :: port 1818.
Nov 30 20:33:09 host sshd[1253]: Server listening on 0.0.0.0 port 1818.
Nov 30 21:38:53 host sshd[1433]: Accepted keyboard-interactive/pam for bl0ck0ck from
172.16.102.11 port 12557 ssh2
Nov 30 21:38:58 host su: bl0ck0ck to root on /dev/pts/0
Nov 30 21:45:50 host sshd[1436]: Received disconnect from 172.16.102.11 port 12557:11:
Nov 30 21:45:50 host sshd[1436]: Disconnected from 172.16.102.11 port 12557
Nov 30 21:46:06 host sshd[1506]: Accepted keyboard-interactive/pam for bl0ck0ck from
172.16.102.11 port 12387 ssh2
Nov 30 21:46:10 host su: bl0ck0ck to root on /dev/pts/0
Nov 30 21:55:30 host sshd[1607]: Accepted keyboard-interactive/pam for bl0ck0ck from
172.16.102.11 port 12467 ssh2
Nov 30 21:57:25 host su: bl0ck0ck to root on /dev/pts/2
45.77.97.16 - - [20/Oct/2017:23:22:00 +0700] "GET /login.php HTTP/1.1" 200 45
45.77.97.16 - - [20/Oct/2017:23:22:00 +0700] "GET /login.php HTTP/1.1" 200 45
45.77.97.16 - - [20/Oct/2017:23:22:00 +0700] "GET /login.php HTTP/1.1" 200 45
45.77.97.16 - - [20/Oct/2017:23:22:00 +0700] "GET /login.php HTTP/1.1" 200 45
```

2. IP yang ditemukan yaitu 45.77.97.16 memiliki hostname **lapangan-basket.com** maka ini akan merujuk ke lapangan basket.
3. Di lapangan basket peserta melakukan simulasi investigasi di tempat dengan menelusuri daerah sekitar dan mendapatkan sebuah flashdisk yang diduga milik pelaku. Setelah dianalisa muncul kode **base64** yang setelah di encode akan merujuk pada suatu tempat. Masing-masing tim memiliki tempat yang berbeda.
=ogMgkWY05WYsBibhJXarJXYQBSakBibhtGbhd2ZulGdgEWehNHIn5WYyFmQ
=oQMgkWY05WYsBibhJXarJXYQBSakBibhtGbhd2ZulGdgEWehNHIn5WYyFmQ
=KEWZyFGIn5War9WbzBSakBibhtGbhd2ZulGdgEWehNHIn5WYyFmQ
=oAbh52bpNXyUjXZ05Wagcmb1RWZnBSakBibhtGbhd2ZulGdgEWehNHIn5WYyFmQ
=oQbvtWatFE11JXYiBCah5WY0BSakBibhtGbhd2ZulGdgEWehNHIn5WYyFmQ
=oAbh52bpNXyUjXZ05Wagcmb1RWZnBCduVWblNXyBSakBibhtGbhd2ZulGdgEWehNHIn5WYyFmQ
4. Di lokasi 4 tim memiliki lokasi berbeda. Di lokasi ini tersebar di beberapa area seperti Dom atas amikom, dom bawah, parkiran timur, basement unit 6, gazebo.
5. Disana peserta akan menemukan dokumen di lokasi 4 berisi DVD Drive. Didalam dokumen tersebut memberikan petunjuk. Terdapat ratusan file berekstensi **.txt** yang ternyata file tersebut adalah file gambar. Peserta hanya perlu mengganti semua ekstensi menjadi **.jpg** dan menganalisisnya lagi. Jika diperhatikan maka seluruh file memiliki date modified 6 tahun yang lalu. Dan hanya 1 file saja yang memiliki date modified 8 jam yang lalu. Disinilah ketika diganti ekstensinya akan memberikan gambar seperti berikut (gambar dibawah simulasi lealui drive cloud):

	wallpaper-1547294.txt		Amikom Virus	...	413 KB	5 years ago
	wallpaper-1679292.txt		Amikom Virus	...	592 KB	5 years ago
	wallpapers (2).txt		Amikom Virus	...	690 KB	6 years ago
	wallpapers (12).txt		Amikom Virus	...	412 KB	6 years ago
	wallpapers (14).txt		Amikom Virus	...	480 KB	6 years ago
	wallpapers (25).txt		Amikom Virus	...	1.5 MB	6 years ago
	wallpapers (69).txt		Amikom Virus	...	62 KB	8 hours ago
	Zack_stock_7_by_da_toss_stock.txt		Amikom Virus	...	1.9 MB	5 years ago
	Zebra_1.txt		Amikom Virus	...	4 MB	7 years ago
	Zebra_2.txt		Amikom Virus	...	1000 KB	7 years ago

6. Foto tersebut menunjukkan Screenshot terduga



7. Untuk mencari tahu siapa orang yang berada diatas maka perlu join ke Group bernama Reversing.ID dan mencari history chat yang diduga sebagai pelaku. Setelah itu akan didapatkan sebuah nomor telepon yaitu 085842991925. Maka akan melakukan pencarian nomor telepon tersebut melalui google dork dan social media.

8. Pelaku tersebut bernama Nanda Reynaldi

9. Dengan melakukan information gathering melalui nomor telepon yang didapatkan itu. Dan mengumpulkan informasi yang ternyata nomor tersebut terhubung dengan beberapa akun media social pelaku,

10. Dirinci.....

Sekian. Terimakasih