Konsep Soal “Basic Steg”

Soal ini menggabungkan antara Steganografi, OSINT dan Scripting.

Pertama peserta akan diberikan file zip yang diberi nama **MrSteg.zip.** Di dalamnya sebuah gambar **nano partikel** yang diberi nama **maybe_its_a_clue.png** yang disisipi file nanozip (http://nanozip.ijat.my/) versi 0.09 yang sudah dibalik per bytenya dan file headernya diganti yang semula “**NanoZip**” menjadi “**AtomZip**” .

Peserta menggunakan konsep OSINT dan analisis file header & file extension. Salah satunya dengan menggunakan Google Images untuk mencari arti gambar maybe_its_a_clue.png setelah itu peserta mencari dan mendownload Nanozip dan mengubah file header “AtomZip” menjadi “NanoZip”. Dan mengekstrak file tersebut dengan format .nz (jika tidak menggunakan .nz tidak bisa diekstrak)

Setelah mengekstrak file Nanozip tersebut terdapat sebuah dokumen .docx yang diberi nama flaggggg.docx . Di dalamnya terdapat tulisan :

1. Perhatian : Dimohon untuk tidak disave karena akan menghilangkan konten file (kelihatan)
2. hology3{absolutrly_not_the_flag} (warna putih)
3. MRUWOIDEMVSXAZLS (warna putih) -> dig deeper (base 32)

Peserta diharapkan menggunakan steganografi untuk mencari clue selanjutnya yang disisipkan sebagai komentar di dalam styles.xml.
<!-- https://gist.github.com/rifqihz/fb64554a06e9002269d77f10df4ebc04 -->
yang merupakan link gist untuk step berikutnya.

Di gist tersebut terdapat hex file zip, peserta diharap menganalisis file header dari hex yang diberikan dan mengubahnya menjadi file zip. Di dalam file zip terdapat file readme.txt yang isinya : “Flag{its_not_da_flagggg}” dan file zip hidden diberi nama .katalist.zip

Pada tahap terakhir peserta diharapkan menggunakan teknik crack steganografi dengan wordlist yang sudah tersedia. Peserta mengekstrak file .katalist.zip yang didalamnya terdapat 8 file :

1. Indonesia.jpg (gambar bendera) (Flag tersembunyi disini)
2. flag.txt (teks hology3{FLAG} sebanyak 10000 baris)
3. random1.txt (perulangan angka 1-10 sebanyak 5000 baris)
4. random2.txt (lorem ipsum dump sebanyak 9000 baris)
5. random3.txt (keyboard dump sebanyak 10000 baris)
6. random4.txt (alfabet dump sebanyak 15000 baris)

7. random5.txt (wordlist yang digunakan untuk crack sebanyak 20000 baris)
8. random6.txt (symbol dump sebanyak 20000 baris)

Key untuk crack Indonesia.jpg : “**35.;225A>+!!294>5?>(**“ ada di random5.txt baris ke **14476**.

Hasilnya adalah secret.txt yang isinya : “AXCkoAyyzmUiiwfiSQd9nznUynzik3Lo6” (base58)
Flag : **hology3{1ts_e4sy_r1ght?}**