Lampiran

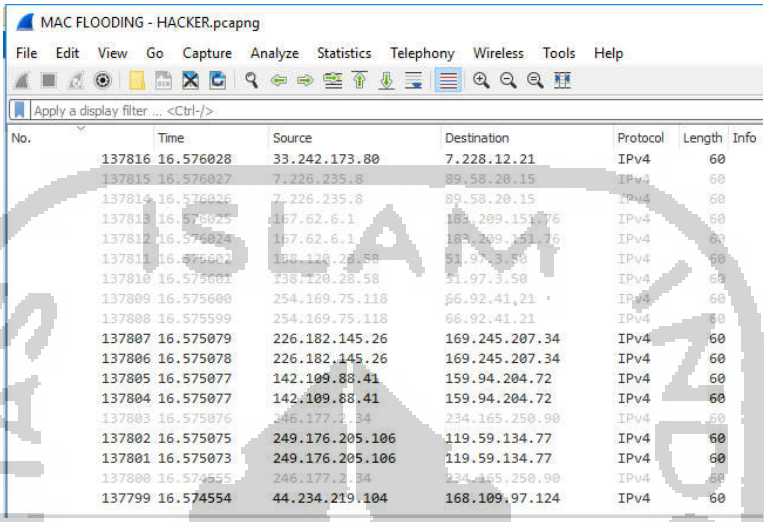
1. *Script konfigurasi Mikrotik*

```
# oct/07/2017 12:27:37 by RouterOS 6.40.2
# software id = E41R-XBFD
#
# model = 751U-2HnD
# serial number = 2B66012A93BD
/interface ethernet
set [ find default-name=ether1 ] name="ether1 - INTERNET"
set [ find default-name=ether2 ] name="ether2 - GOES TO SWITCH
A - SIEM"
set [ find default-name=ether3 ] name="ether3 - GOES TO SWITCH
B - HACKER"
set [ find default-name=ether4 ] name="ether4 - USER"
set [ find default-name=ether5 ] name="ether5 - NOT USED"
/interface wireless
set [ find default-name=wlan1 ] disabled=no mode=ap-bridge
name=\
    "wlan1 - SIEM ENV (WIFI)" ssid="SIEM ENV"
/interface wireless security-profiles
add authentication-types=wpa-psk,wpa2-psk eap-methods="" \
    management-protection=allowed mode=dynamic-keys name=KEY
\
    supplicant-identity="" wpa-pre-shared-key=SIEM1234 wpa2-
pre-shared-key=SIEM1234
/ip hotspot profile
add     dns-name=SIEM.security     hotspot-address=10.10.16.1
name=hsprof1 \
    smtp-server=10.0.0.10
/ip pool
add name=dhcp_pool0 ranges=10.10.12.10-10.10.12.254
add name=dhcp_pool1 ranges=10.10.13.2-10.10.13.254
add name=dhcp_pool2 ranges=10.10.14.2-10.10.14.254
add name=dhcp_pool3 ranges=10.10.15.2-10.10.15.254
add name=dhcp_pool4 ranges=10.10.16.2-10.10.16.254
add name=dhcp_pool5 ranges=10.0.0.200-10.0.0.254
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no interface=\
    "ether3 - GOES TO SWITCH B - HACKER" name=dhcp2
add address-pool=dhcp_pool2 disabled=no interface="ether4 -
USER" name=dhcp3
add address-pool=dhcp_pool3 disabled=no interface="ether5 -
NOT USED" name=dhcp4
add address-pool=dhcp_pool4 disabled=no interface="wlan1 -
SIEM ENV (WIFI)" name=dhcp5
add address-pool=dhcp_pool5 disabled=no interface=\
    "ether2 - GOES TO SWITCH A - SIEM" name=dhcp1
/ip hotspot
add address-pool=dhcp_pool4 disabled=no interface="wlan1 -
SIEM ENV (WIFI)"  name=hotspot1 profile=hsprof1
```

2. *Network forensic Mac Flooding*

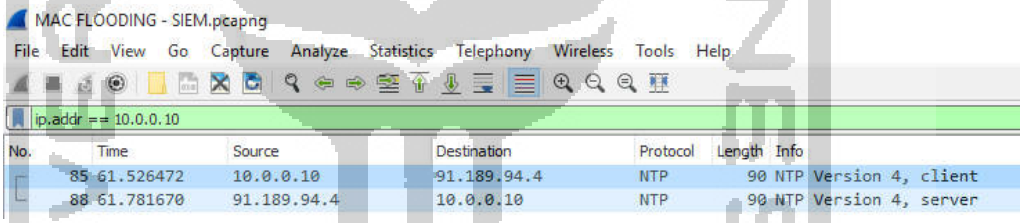
- Trafik *Mikrotik - hacker*

  Terpantau adanya trafik yang *source* dan *destination* IP yang *random*

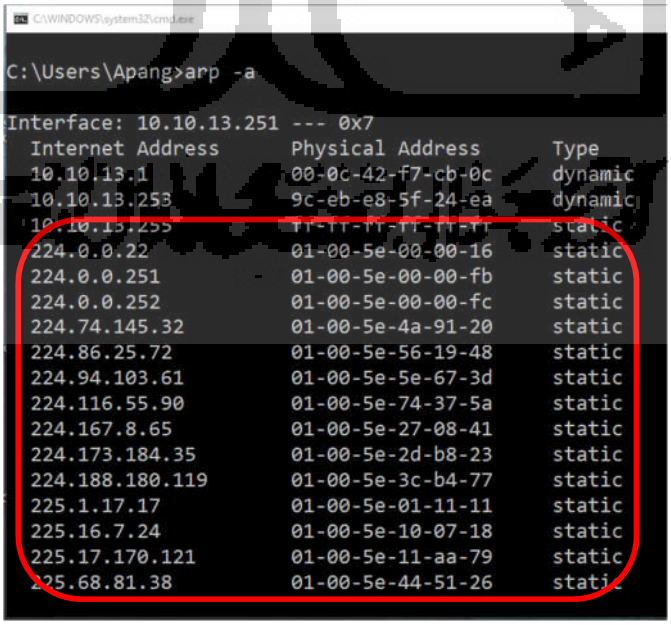


- Trafik *Mikrotik - SIEM*

  Tidak terlihat komunikasi hanya trafik *SIEM* menghubungi *NTP Server*



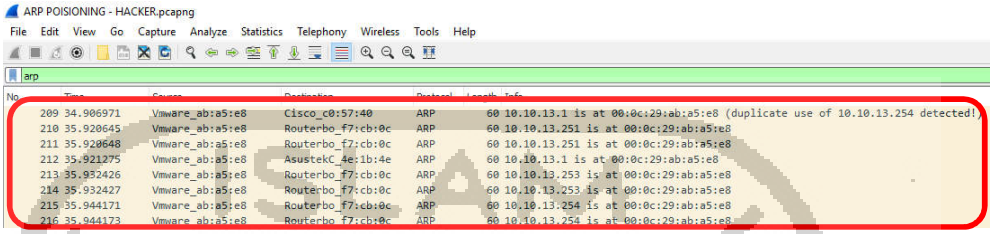
- Dari sisi *user table arp* bertambah lebih banyak karena adanya *mac flooding* di jaringan tersebut.



3. *Network forensic Arp Poisioning*

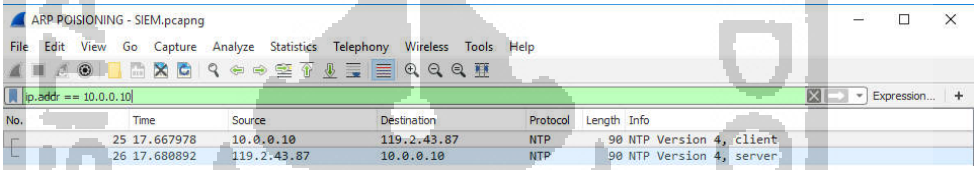
- Trafik *Mikrotik - hacker*

  Terlihat adanya *arp reply* yang memberikan *mac address* yang sama untuk IP yang berbeda yaitu: *00:0c:29:ab:a5:e8*



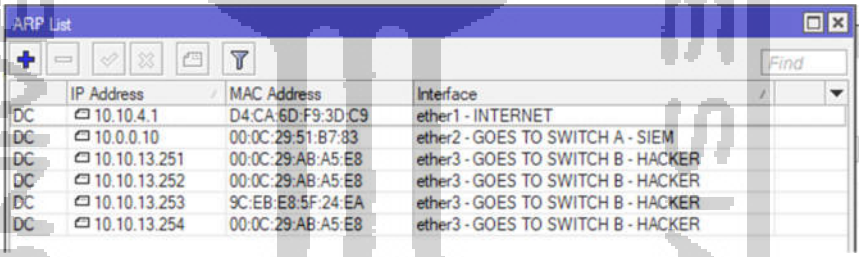
- Trafik *Mikrotik* ke *SIEM*

  Tidak terlihat komunikasi hanya trafik *SIEM* menghubungi *NTP Server*



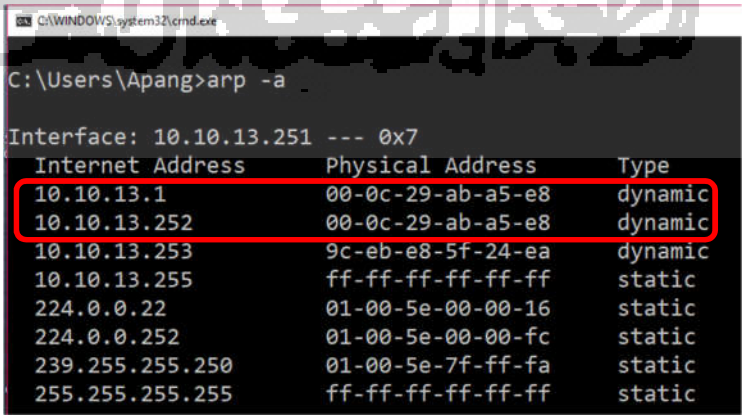
- Aktifitas *Mikrotik*

  Terlihat *arp table Mikrotik* menunjukan IP yang berbeda tapi menggunakan *mac address* yang sama yaitu *00:0c:29:ab:a5:e8*



- *End User Windows*

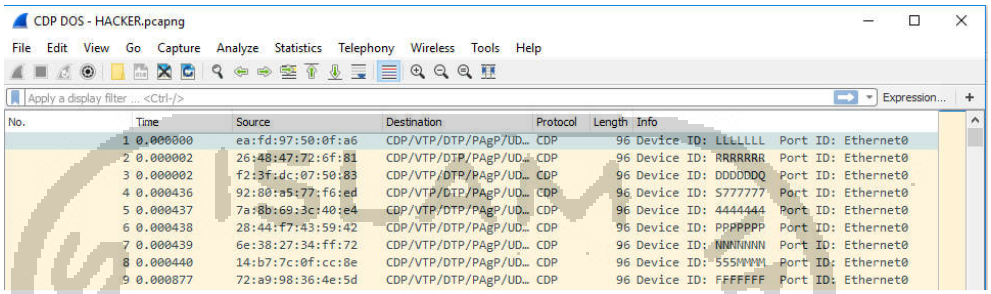
  Terlihat *arp table end user* menunjukan *mac address gateway* menggunakan *mac address* yaitu *00:0c:29:ab:a5:e8* yang merupakan mac *address hacker*



4. *Network forensic CDP Flooding*

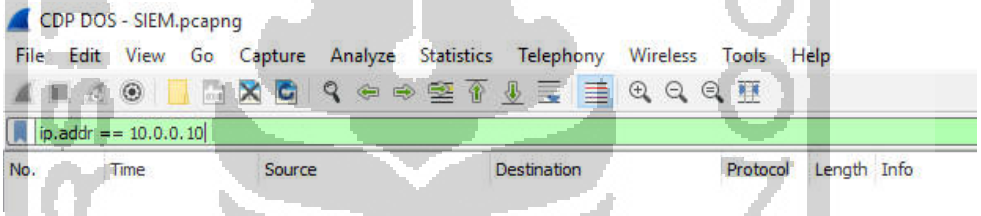
- Trafik *Mikrotik – hacker*

  Terlihat adanya trafik *cdp* dengan menggunakan *mac address* dan *device id* yang *random*



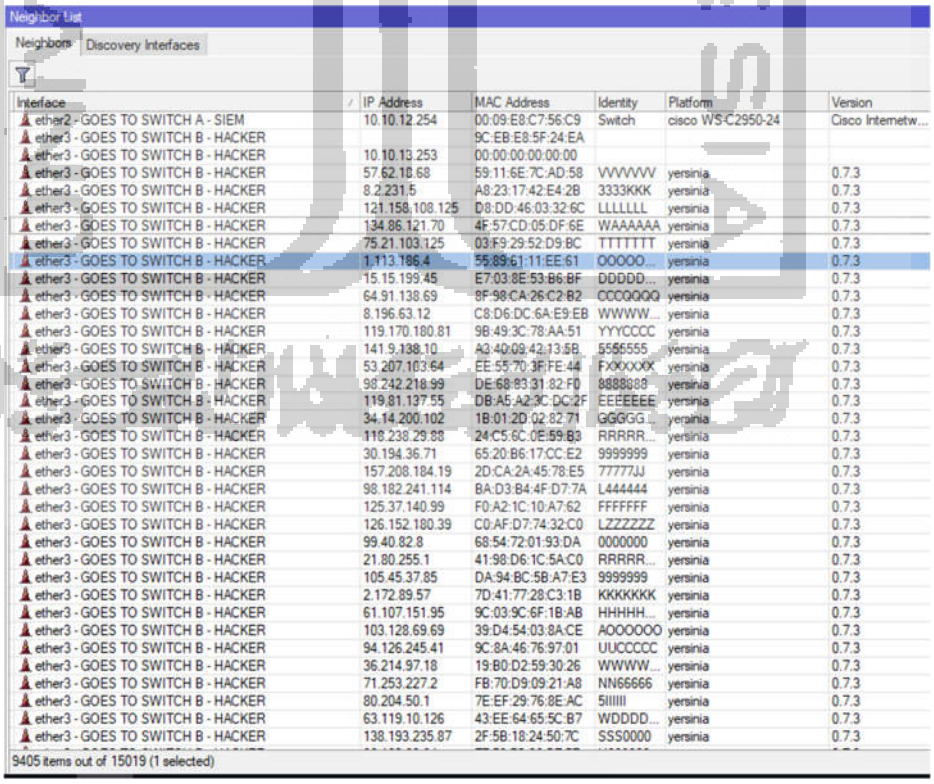
- Trafik *Mikrotik - SIEM*

  Tidak ada aktifitas komunikasi antara *SIEM* dan Mikrotik



- Aktifitas *Mikrotik*

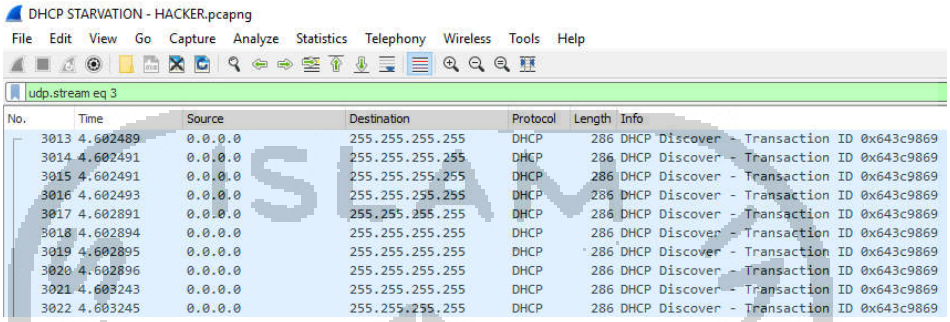
  Terlihat *Mikrotik table neighbor list* berisi 15019 efek serangan *CDP Flooding*



5. *Network forensic DHCP Starvation*

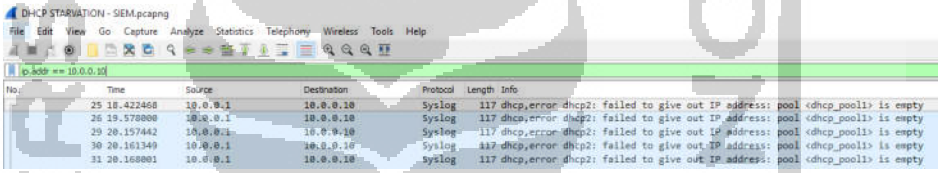
- Trafik *Mikrotik - hacker*

  Terlihat adanya paket *DHCP Discover* yang dikirim dalam jumlah yang banyak hasil serangan dari *yersinia*



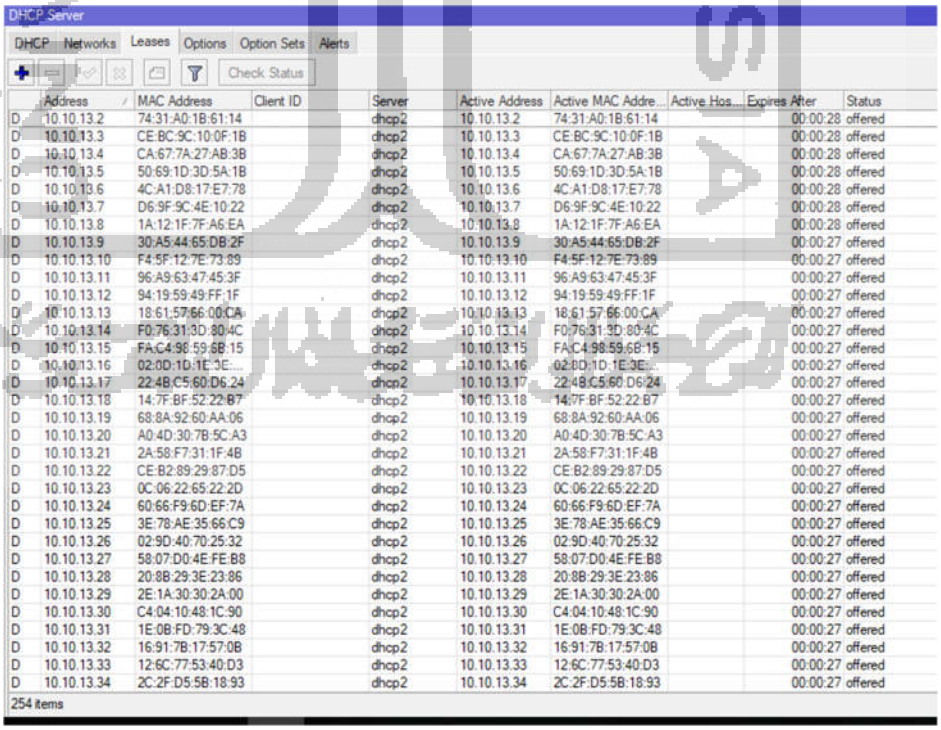
- Trafik *Mikrotik - SIEM*

  Terjadi komunikasi antara *Mikrotik – SIEM* dalam bentuk *syslog dhcp, error dhcp2: failed to give out IP address: pool <dhcp_pool1> is empty*



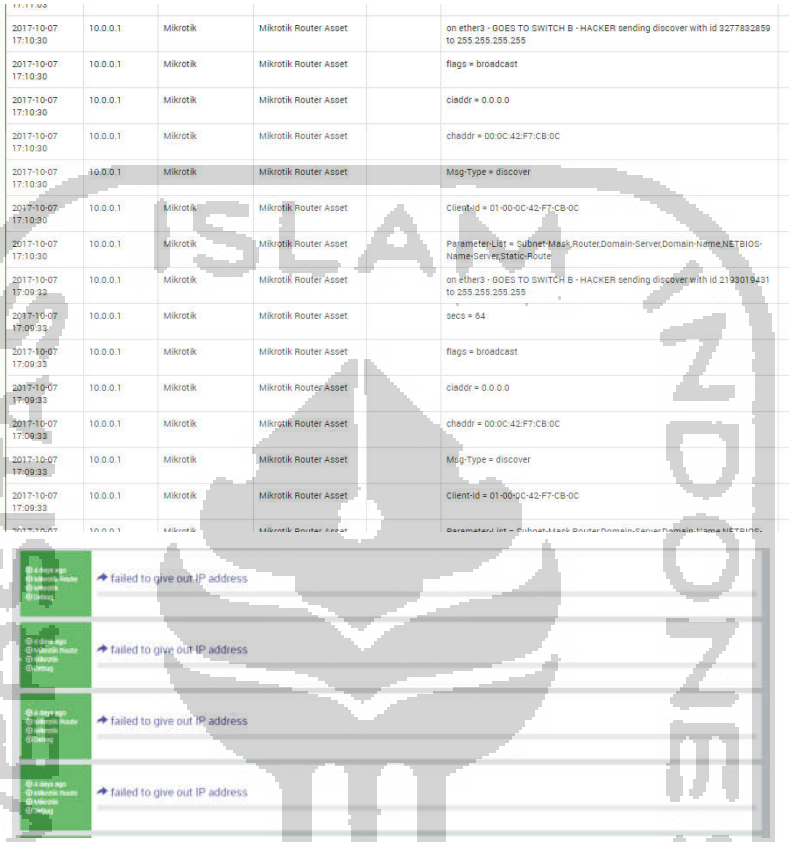
- Aktifitas *Mikrotik*

  Mikrotik melakukan *DHCP Offer* sampai IP poolnya habis



- Aktifitas *SIEM*

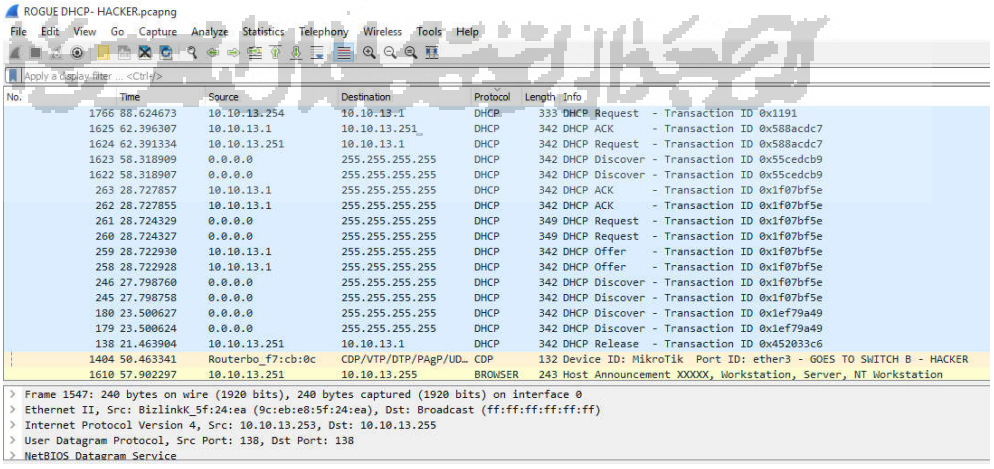
  SIEM menunjukan *log* bahwa *Mikrotik* gagal menyewakan alamat IP karena *pool dhcp* habis yang dikirimkan oleh *Mikrotik*



6. *Network forensic DHCP Rogue*

- Trafik *Mikrotik - hacker*

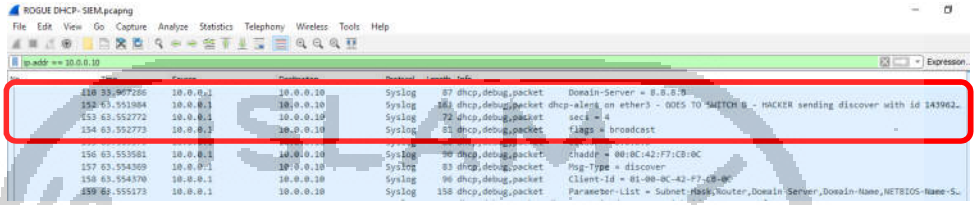
  Adanya trafik *dhcp server* dan terlihat permintaan alamat IP dari klien dalam bentuk *DHCP Discover*.



No.	Time	Source	Destination	Protocol	Length	Info
1766	88.624673	10.10.13.254	10.10.13.1	DHCP	333	DHCP Request - Transaction ID 0x1191
1625	62.396307	10.10.13.1	10.10.13.251	DHCP	342	DHCP ACK - Transaction ID 0x588acdc7
1624	62.391334	10.10.13.251	10.10.13.1	DHCP	342	DHCP Request - Transaction ID 0x588acdc7
1623	58.318909	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x55cedcb9
1622	58.318907	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x55cedcb9
263	28.727857	10.10.13.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1f07bf5e
262	28.727855	10.10.13.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1f07bf5e
261	28.724329	0.0.0.0	255.255.255.255	DHCP	349	DHCP Request - Transaction ID 0x1f07bf5e
260	28.724327	0.0.0.0	255.255.255.255	DHCP	349	DHCP Request - Transaction ID 0x1f07bf5e
259	28.722930	10.10.13.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1f07bf5e
258	28.722928	10.10.13.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1f07bf5e
246	27.798760	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1f07bf5e
245	27.798758	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1f07bf5e
180	23.500627	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1ef79a49
179	23.500624	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1ef79a49
138	21.463904	10.10.13.251	10.10.13.1	DHCP	342	DHCP Release - Transaction ID 0x452033c6
1404	50.463341	Routerbo_f7:cb:0c	CDP/VTP/DTP/PAgP/UD…	CDP	132	Device ID: MikroTik Port ID: ether3 - GOES TO SWITCH B - HACKER
1610	57.902297	10.10.13.251	10.10.13.255	BROWSER	243	Host Announcement XXXXX, Workstation, Server, NT Workstation

- Trafik *Mikrotik - SIEM*

  Terlihat adanya komunikasi dalam bentuk *syslog* dengan isi *dhcp alert* yang menunjukan adanya *dhcp server* lain dalam satu jaringan yang sama. *dhcp debug, packet dhcp-alert on ether3 – GOES TO SWITCH B -HACKER sending discover with id 143962..*



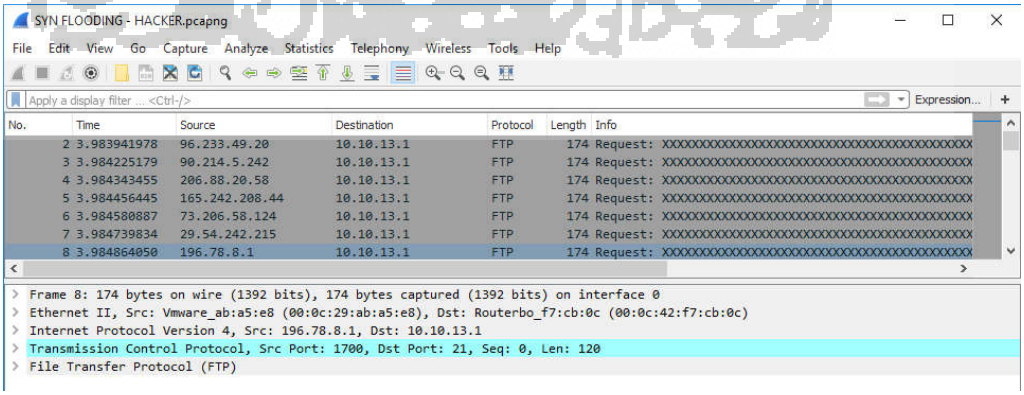
- Aktifitas *SIEM*

  SIEM menunjukan *log dhcp alert*

7. *Network forensic SYN Flooding*

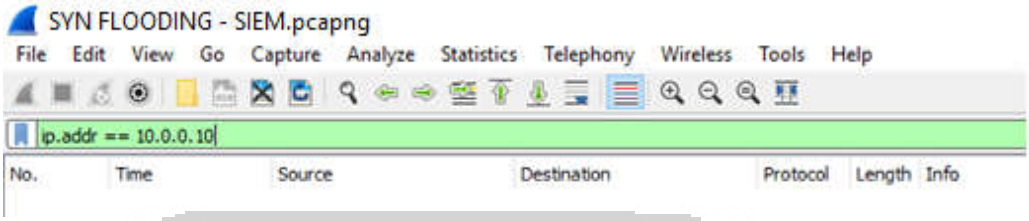
- Trafik *Mikrotik – hacker*

  Terlihat adanya trafik *syn flooding* yang dilakukan oleh *hacker* dengan menggunakan alamat *Ip address* dengan *source ip* yang *random,* dari gambar yang dilihat dibawah ini proses *syn flooding* di lakukan pada protokol *FTP*



- Trafik *Mikrotik - SIEM*

  Tidak ada aktifitas komunikasi antara *SIEM* dan Mikrotik



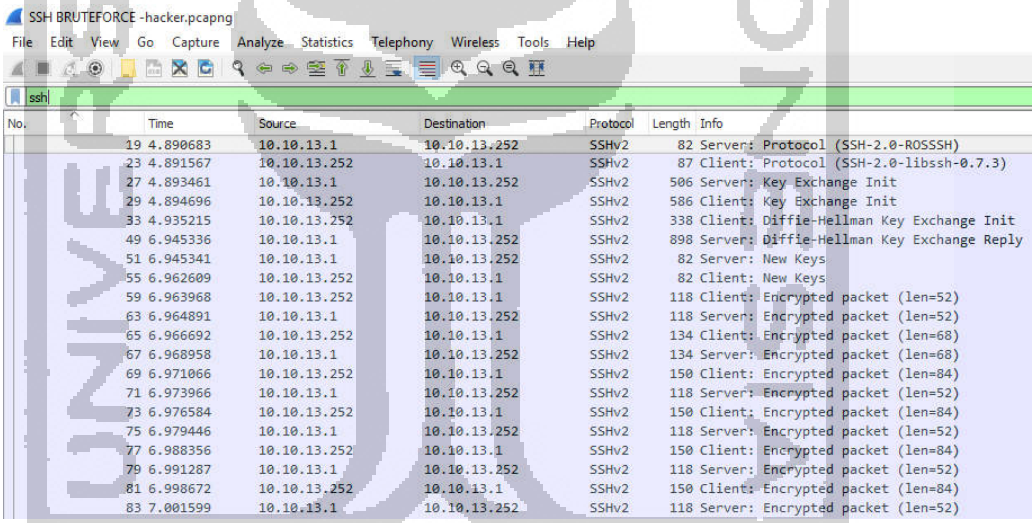
- Aktifitas *Mikrotik*

  Mikrotik dalam kondisi tidak bisa diakses dengan *Winbox* karena serangan *SYN Flooding*

8. *Network forensic SSH Brute Force*

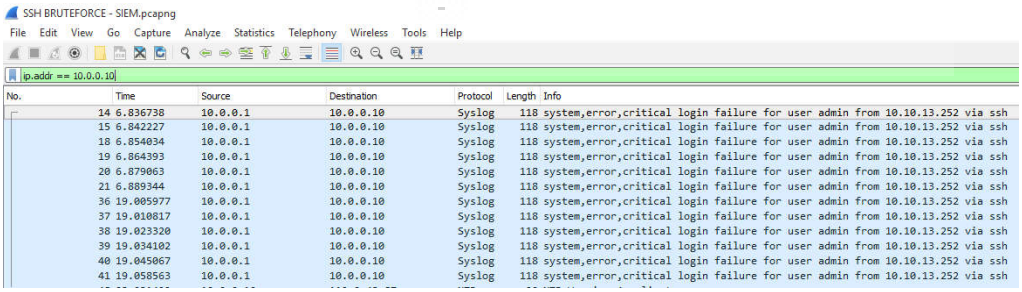
- Trafik *Mikrotik - hacker*

  Terlihat adanya komunikasi percobaan *login ssh* yang dilakukan beberapa kali



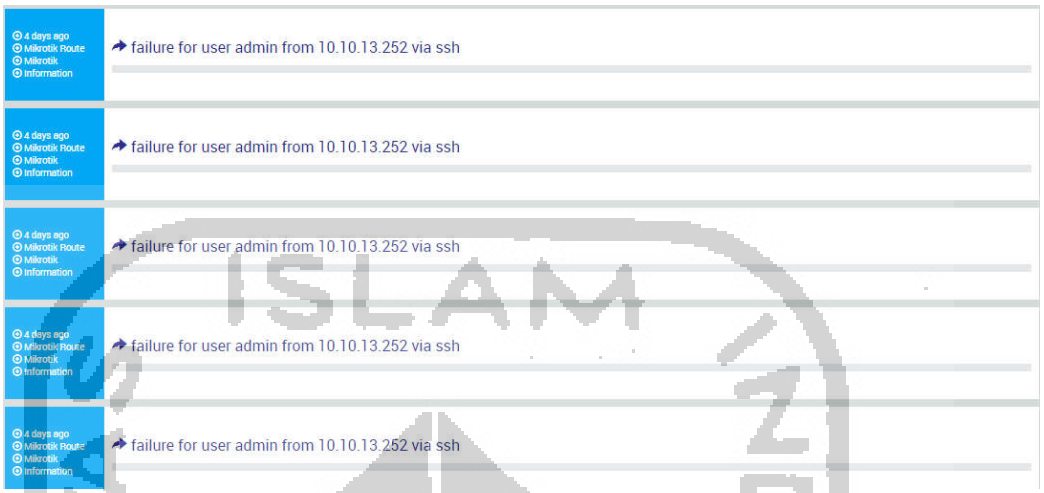
- Trafik *Mikrotik - SIEM*

  Terjadi komunikasi antara *Mikrotik – SIEM* dalam bentuk *syslog system, error, critical login failure for user a0dmin from 10.10.13.252 via ssh*



- Aktifitas *SIEM*

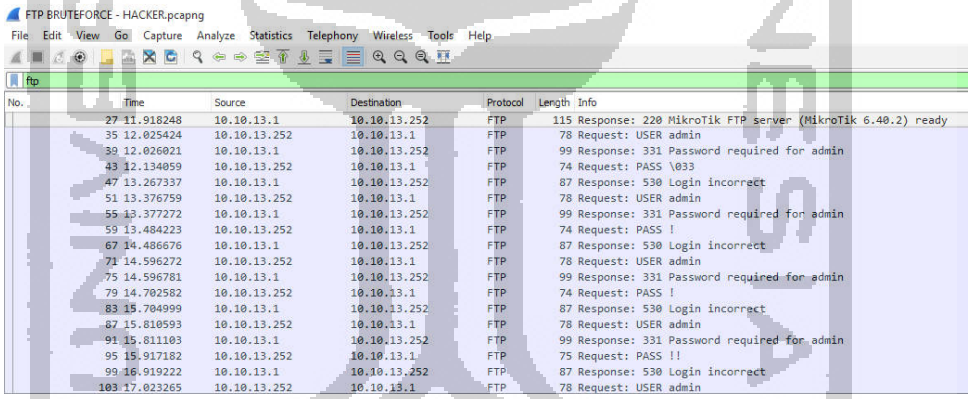
  SIEM menunjukan adanya percobaan *login user admin via ssh*



9. *Network forensic FTP Brute Force*

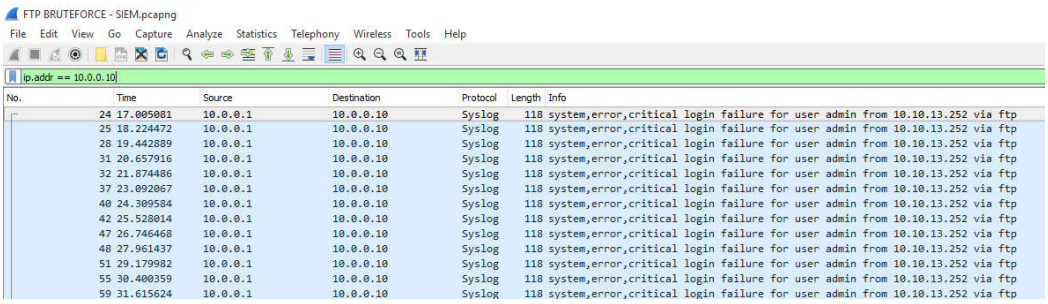
- Trafik *Mikrotik – hacker*

  Terlihat adanya komunikasi percobaan *login ftp* yang dilakukan beberapa kali



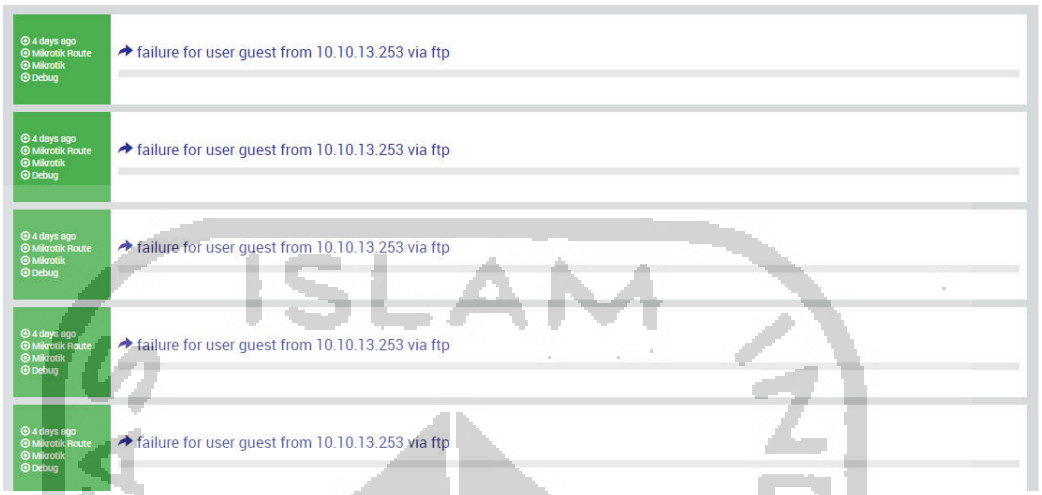
- Trafik *Mikrotik - SIEM*

  Terjadi komunikasi antara *Mikrotik – SIEM* dalam bentuk *syslog system, error, critical login failure for user a0dmin from 10.10.13.252 via ftp*



- Aktifitas *SIEM*

  SIEM menunjukan adanya percobaan *login user admin via ftp*



10. Kuisioner Pre-Assessment Indeks KAMI Diskominfo Kota Tegal

KUESIONER INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

DINAS KOMUNIKASI DAN INFORMASI KOTA TEGAL

2017

DATA PENGISI KUESIONER

Instansi	:	Dinas Komunikasi dan Informatika Kota Tegal
Nama	:	Khairul Fahmi, M Kom
NIP	:	19860827 201101 1010
Jabatan	:	Pranata Komputer Pertama
Nomor Kontak	:	0857 1829 5334
Email	:	fahmikhair@gmail.com

Tanda Tangan dan Cap Instansi :

Form Checlist

- I. Aspek Peran TIK ☐
- II. Aspek Tata Kelola ☐
- III. Aspek Risiko ☑
- IV. Aspek Kerangka Kerja ☑
- V. Aspek Pengelolaan Aset ☑
- VI. Aspek Teknologi ☑

KUESIONER ASPEK PERAN TIK

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengukur tingkat peran dan kepentingan TIK dalam instansi anda. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Minim
- 1 = Rendah
- 2 = Sedang
- 3 = Tinggi
- 4 = Kritis

No	Karakteristik Instansi	Status				
		0	1	2	3	4
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis				✓	
2	Jumlah staff/pengguna dalam instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis				✓	
3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi Instansi anda				✓	
4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda		✓			
5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda		✓			
6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda				✓	
7	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional				✓	

8	Tingkat sensitifitas pengguna sistem TIK di Instansi anda			✓		
9	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya			✓		
10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda				✓	
11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK			✓		
12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi			✓		

KUESIONER ASPEK TATA KELOLA KEAMANAN INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
1	Apakah pimpinan instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	√			
2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		√		
3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?		√		
4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	√			
5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	√			
6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	√			
7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	√			
8	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	√			
9	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?			√	

10	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	✓			
11	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	✓			
12	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?		✓		
13	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	✓			
14	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	✓			
15	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	✓			
16	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	✓			
17	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	✓			
18	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?	✓			
19	Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	✓			
20	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	✓			

KUESIONER ASPEK PENGELOLAAN RISIKO KEAMANAN INROMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian;\
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?				
2	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	√			
3	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	√			
4	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	√			
5	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?		√		
6	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?				
7	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	√			

8	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	✓			
9	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	✓			
10	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	✓			
11	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	✓			
12	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?				
13	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	✓			
14	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	✓			
15	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	✓			

KUESIONER ASPEK KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian;\
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
PENYUSUNAN DAN PENGELOLAAN KEBIJAKAN & PROSEDUR KEAMANAN INFORMASI					
1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?		√		
2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?		√		
3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	√			
4	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	√			
5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	√			
6	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	√			
7	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	√			
8	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	√			
9	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	√			

10	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?		√		
11	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?		√		
12	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?		√		
13	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?				
14	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?				
15	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?				
16	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?				
PENGELOLAAN STRATEGI DAN PROGRAM KEAMANAN INFORMASI					
17	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?				
18	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?				
19	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?				
20	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?				
21	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?				
22	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?				

23	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	✓			
24	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	✓			
25	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?	✓			
26	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	✓			

KUESIONER ASPEK PENGELOLAAN ASET INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
PENGELOLAAN ASET INFOMASI					
1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?		√		
2	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?			√	
3	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut		√		
4	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?		√		
5	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?		√		
6	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?		√		
7	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda		√		
8	Tata tertib penggunaan komputer, email, internet dan intranet		√		
9	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI		√		
10	Peraturan pengamanan data pribadi		√		
11	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya		√		
12	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi		√		

13	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	✓			
14	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	✓			
15	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	✓			
16	Prosedur *back-up* ujicoba pengembalian data (*restore*)		✓		
17	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	✓			
18	Proses pengecekan latar belakang SDM	✓			
19	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	✓			
20	Prosedur penghancuran data/aset yang sudah tidak diperlukan	✓			
21	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	✓			
22	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	✓			
23	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	✓			
24	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	✓			
PENGAMANAN FISIK					
25	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	✓			
26	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	✓			
27	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?			✓	
28	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?			✓	

29	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	√			
30	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?			√	
31	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?				
32	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?				
33	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)				
34	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?				

KUESIONER ASPEK TEKNOLOGI DAN KEAMANAN INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
PENGAMAN TEKNOLOGI					
1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	√			
2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?				√
3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	√			
4	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	√			
5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	√			
6	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	√			
7	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	√			
8	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	√			
9	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	√			
10	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	√			

11	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	✓			
12	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	✓			
13	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	✓			
14	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	✓			
15	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*, dan penarikan akses?	✓			
16	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	✓			
17	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	✓			
18	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	✓			
19	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	✓			
20	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	✓			
21	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	✓			
22	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	✓			
23	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	✓			
24	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	✓			

11. Kuisioner Post-Assessment Indeks KAMI Diskominfo Kota Tegal

POST KUESIONER INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

DINAS KOMUNIKASI DAN INFORMASI KOTA TEGAL

2017

DATA PENGISI KUESIONER

Instansi	:	Dinas Komunikasi dan Informatika Kota Tegal
Nama	:	Khairul Fahmi, M. Kom
NIP	:	19860827 201101 1016
Jabatan	:	Pranata Komputer Pertama
Nomor Kontak	:	085718295374
Email	:	fahmikhairul@gmail.com

Tanda Tangan dan Cap Instansi :

7 oktober 2017

Form Checlist

I. Aspek Peran TIK	☑
II. Aspek Tata Kelola	☑
III. Aspek Risiko	☑
IV. Aspek Kerangka Kerja	☑
V. Aspek Pengelolaan Aset	☑
VI. Aspek Teknologi	☑

KUESIONER ASPEK PERAN TIK

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengukur tingkat peran dan kepentingan TIK dalam instansi anda. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Minim
- 1 = Rendah
- 2 = Sedang
- 3 = Tinggi
- 4 = Kritis

No	Karakteristik Instansi	Status				
		0	1	2	3	4
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis				√	
2	Jumlah staff/pengguna dalam instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis				√	
3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi Instansi anda				√	
4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda		√			
5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda		√			
6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda				√	
7	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional		√			

8	Tingkat sensitifitas pengguna sistem TIK di Instansi anda			✓		
9	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya			✓		
10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda				✓	
11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK			✓		
12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi			✓		

KUESIONER ASPEK TATA KELOLA KEAMANAN INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	✓			
2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		✓		
3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?		✓		
4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	✓			
5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	✓			
6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	✓			
7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	✓			
8	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	✓			
9	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?			✓	

10	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	✓				
11	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	✓				
12	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?		✓			
13	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	✓				
14	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	✓				
15	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	✓				
16	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	✓				
17	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	✓				
18	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?	✓				
19	Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	✓				
20	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	✓				

KUESIONER ASPEK PENGELOLAAN RISIKO KEAMANAN INROMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian;\
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	√			
2	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	√			
3	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	√			
4	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	√			
5	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?		√		
6	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	√			
7	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	√			

8	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	✓			
9	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	✓			
10	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	✓			
11	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	✓			
12	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	✓			
13	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	✓			
14	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	✓			
15	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	✓			

KUESIONER ASPEK KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian;\
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
PENYUSUNAN DAN PENGELOLAAN KEBIJAKAN & PROSEDUR KEAMANAN INFORMASI					
1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?		✓		
2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?		✓		
3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	✓			
4	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	✓			
5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	✓			
6	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	✓			
7	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	✓			
8	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	✓			
9	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	✓			

10	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?		✓		
11	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?		✓		
12	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?		✓		
13	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	✓			
14	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	✓			
15	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	✓			
16	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	✓			
PENGELOLAAN STRATEGI DAN PROGRAM KEAMANAN INFORMASI					
17	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	✓			
18	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	✓			
19	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	✓			
20	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	✓			
21	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	✓			
22	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	✓			

23	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	✓				
24	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	✓				
25	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?	✓				
26	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	✓				

KUESIONER ASPEK PENGELOLAAN ASET INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
PENGELOLAAN ASET INFOMASI					
1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?		√		
2	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?			√	
3	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut	√			
4	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	√			
5	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	√			
6	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	√			
7	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	√			
8	Tata tertib penggunaan komputer, email, internet dan intranet	√			
9	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	√			
10	Peraturan pengamanan data pribadi	√			
11	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	√			
12	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	√			

13	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	✓				
14	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	✓				
15	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	✓				
16	Prosedur *back-up* ujicoba pengembalian data (*restore*)	✓	✓			
17	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	✓				
18	Proses pengecekan latar belakang SDM	✓				
19	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	✓				
20	Prosedur penghancuran data/aset yang sudah tidak diperlukan	✓				
21	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	✓				
22	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	✓				
23	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	✓				
24	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	✓				
PENGAMANAN FISIK						
25	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	✓				
26	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	✓				
27	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?				✓	
28	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?				✓	

29	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	✓			
30	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?			✓	
31	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	✓			
32	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	✓			
33	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	✓			
34	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	✓			

KUESIONER ASPEK TEKNOLOGI DAN KEAMANAN INFORMASI

INDEKS KEAMANAN INFORMASI (KAMI) KOTA TEGAL

Kuisioner ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instasi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan atau Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi Keamanan Informasi	Status			
		0	1	2	3
PENGAMAN TEKNOLOGI					
1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	√			
2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?				√
3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	√			
4	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	√			
5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?			√	
6	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?				√
7	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?				√
8	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?				√
9	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?				√
10	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	√			

11	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	✓				
12	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	✓				
13	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	✓				
14	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	✓				
15	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?		✓			
16	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	✓				
17	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	✓				
18	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	✓				
19	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	✓				
20	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?					✓
21	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	✓				
22	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	✓				
23	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	✓				
24	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	✓				