PENINGKATAN KEAMANAN JARINGAN NIRKABEL DENGAN PENDETEKSI SERANGAN BERBASIS KISMET DD-WRT

Dian Pranata[1], **Yesi Novaria Kunang**[2], **Nurul Adha Oktarini Saputri**[3]
Fakultas Ilmu Komputer, Universitas Bina Darma[2],
Email: pranatadian22@gmail.com[1], yesinovariakunang@binadarma.ac.id[2], nuruladhaos@binadarma.ac.id[3]

ABSTRACT

Network security systems become important in maintaining a network of attacks that can interfere even damage the system of connections between connected devices will be very detrimental. However, a network vulnerability requires WIDS testing that can detect attacks in the network, Wireless Intrusion Detection System (WIDS) to monitor and scan a kismet-based wireless network. Kismet is an open source tool and a program that can help monitoring a network, kismet will produce alerts in the form of output in the form of time display at the time of the attack carried out. Kismet also has an interface that can display connected networks and what networks are in the range. Kismet is able to save logs or output in new files if it is run again, it can store only different naming dates and times, regarding the kismet program the writer will conduct research on detection, attack and security which can later help and provide understanding of WIDS.

Keywords*: DD-WRT, Kismet, WIDS.*

ABSTRAK

Sistem keamanan jaringan menjadi hal yang penting dalam menjaga sebuah jaringan serangan yang bisa menggangu bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat merugikan. Namun kerentanan suatu jaringan maka dibutuhkan pengujian WIDS yang dapat mendeteksi adanya serangan dalam jaringan, Wireless Intrusion Detection System (WIDS) untuk memonitoring dan mengscan suatu jaringan wireless yang bebasis kismet. Kismet merupakan tools open source dan sebuah program yang dapat membantu memonitoring suatu jaringan, kismet nanti nya menghasilkan berupa alert berupa output berupa tampilan waktu pada saat penyerangan yang dilakukan. Kismet juga mempunyai interface yang dapat menanpilkan jaringan yang terhubung dan jaringan apa saja yang berapa di jangkaunnya. Kismet mampu menyimpan log atau ouput dalam file yang baru jika dijalankan lagi dapat penyimpanan hanya berbeda penamaannya tanggal dan waktunya saja, mengenai program kismet penulis akan melakukan penelitian mengenai pendeteksi, serangan dan keamanan yang nanti dapat membantu serta memberi pemahaman tentang WIDS.

Kata Kunci : *DD-WRT, Kismet, WIDS.*

1. PENDAHULUAN

Di zaman *modern* ini perkembangan teknologi dalam sistem informasi dan jaringan komputer sangatlah pesat. Hal ini memerlukan pengolahan jaringan yang baik agar dapat menjamin ketersediaan jaringan yang selalu tinggi. Tugas pengelola jaringan yang dilakukan oleh *administrator*, memiliki beberapa permasalahan berkaitan dengan keamanan komputer. Semakin bertambahnya pengguna semakin besar pula resiko terjadinya kerusakan, kehilangan atau penyalahgunaan pada suatu jaringan komputer.

Penerapan jaringan *nirkabel* saat ini memberikan dampak perubahan yang cukup signifikan. Penerapan jaringan nirkabel tersebut walaupun baik, namun bukan berarti tidak memunculkan masalah terutama pada jaringan *wireless*. Banyak masalah yang sering terjadi pada jaringan *wireless*, salah satunya masalah keamanan yang tentunya dapat merugikan pengguna. Permasalah tentang celah keamanan berdampak pada resiko kerugian yang besar. Untuk itu dibutuhkan suatu sistem keamanan untuk melindungi sistem dalam jaringan. [1]. Salah satu upaya pencegahan dan meningkatkan keamanan komputer adalah dengan mendeteksi jaringan menggunakan *Intrusion Detection System (IDS).*

IDS merupakan sistem deteksi untuk mendeteksi adanya trafik paket yang tidak diinginkan dalam sebuah jaringan, dan dapat berfungsi sebagai sensor peringatan dini. [2]. *Tools IDS* yang digunakan adalah *kismet* salah satu *tools* atau aplikasih *open source (IDS),* yang mempunyai *interface* yang dapat menampilkan jaringan pada jangkaunya, dan *client* mana saja yang terhubung padanya. *Kismet* mempunyai program yaitu *kismet drone, kismet server. Kismet drone* merupakan program yang ditempatkan pada *sensor wireless router. Kismet server* yang mengolah data-data yang dikumpulkan oleh *kismet drone*. [3]. Dalam penelitian ini penulis ingin menggunakan metode *spdlc (security police development life cycle* untuk metode keamanan yang baik.[4]. Berdasarkan urain di atas penulis tertarik melakukan penelitian dengan judul "Peningkatan Keamanan Jaringan *Nirkabel* Dengan Pendeteksi Serangan Berbasi *Kismet DD-WRT*". Dalam penelitian ini penulis ingin menggunakan metode *spdlc (security police development life cycle* untuk metode keamanan yang baik.

2. METODOLOGI PENELITIAN

Metode keamanan yang digunakan. *spdlc (security police development life cycle* adalah metode untuk keamanan. [5]. Berikut ini merupakan tahapan-tahapan di dalam metode *spdlc* identifikasi, *analisis*, *desain*, implementasi, audit, evaluasi.

2.1 *Identifikasi*

Pada tahap ini peneliti mengidentifikasi terhadap jaringan *wireless* untuk menentukan pokok dan pemecahan masalah terhadap objek yang diteliti, dan menjelaskan situasi keadaan suatu *wireless*. Pada tahap ini peneliti melakukan identifikasi *wireless* terlebih dahulu untuk menentukan serangan apa saja yang bisa menyerang *wireless* untuk mengetahui keberadaan dan keamanan, Melakukan pengujian dengan serangan paket *Mac spoofing ,ddos, Arp spoofing* dan menonitoring serangan tersebut, memonitoring serangan pada jaringan *wireless* dengan mengunakan *wireless intrusion detection system* (*WIDS*) kismet.

2.2 *Analisis*

Pada tahap analisis atau Analisa yang dikerjakan adalah pengamatan secara langsung dengan tujuan untuk mengetahui teknologi keamanan jaringan *wireless* yang digunakan saat ini, masalah-masalah apa saja yang dihadapi oleh teknologi keamanan jaringan *wireless*, dan Penanganan masalah bagaimana cara menangani masalah-masalah yang dihadapi yaitu dengan mengidentifikasi semua asset, ancaman-ancaman, *vulnerabilities* dan menetapkan resiko-resiko serta langkalangka positif untuk melindungi sistem jaringan *wireless*.

2.3 *Desain*

Pada tahap ini adalah peneliti merencanakan apa yang akan dilakukan pada jaringan yang saling berhubungan yang bertujuan melakukan pengujian *WIDS* terhadap serangan pembuatan desain topologi serangan jaringan atau skema keamanan jaringan. Desain *kismet* mempunyai program *kismet server,kismet drone,kismet server* yang menggolah data yang ditangkap dan dikumpulkan oleh *kismet drone* dan melakukan penyerangan sebagai pengujian.

2.4 *Implementasi*

Pada bab ini peneliti akan melaksanakan implementasi dengan cara melakukan instalasi dan konfigurasi *WIDS Kismet,* serangan serta dilanjutkan dengan melakukan pengujian terhadap *WIDS* yang telah dibuat.

2.5 *Audit*

Pada bab ini setelah melakukan tahap implementasi pengujian, peneliti melakukan tahap audit dan mengumpulkan hasil-hasil yang telah dilakukan dari serangan mac spoofing, ddos, arp spoofing.

2.6 *Evaluasi*

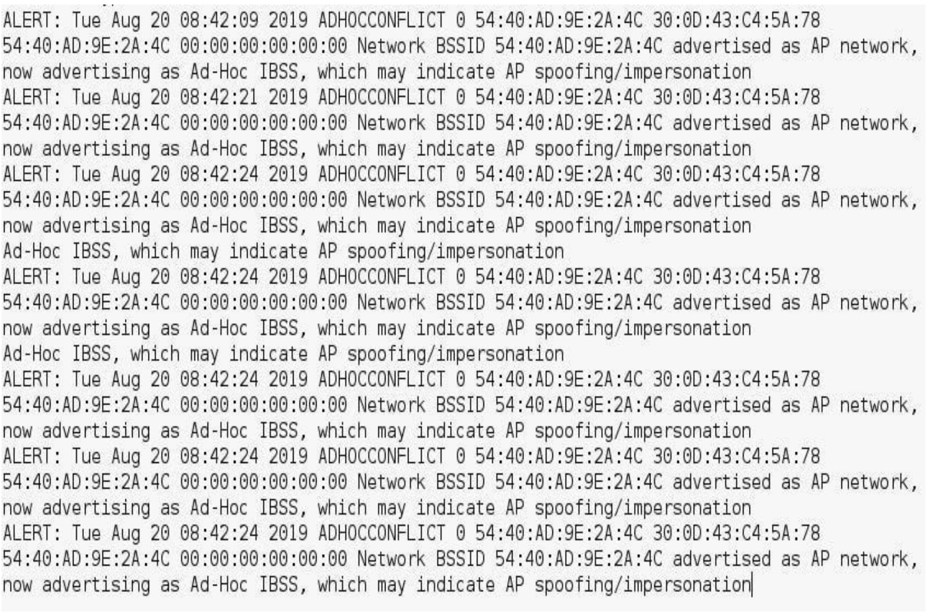
Disini penulis melakukan *vulnerability assessment*, dilakukan untuk menilai kerentanan jaringan komputer. Untuk menilai dan mengukur tingkat keamanan pada suatu jaringan. *Test* yang dilakukan pada jaringan simulasi ini mengunakan metode *penetration testing* untuk mengetahui celah keamanan yanga ada pada jaringan nirkabel.

3. HASIL DAN PEMBAHASAN

Pada bab ini setelah melakukan tahap implementasi pengujian, peneliti melakukan tahap audit dan mengumpulkan hasil-hasil yang telah dilakukan dari serangan mac spoofing, ddos, arp spoofing . Dan dapat dilihat pada gambar dibawah

Pada gambar dibawah adalah hasil serangan yang dilakukan oleh serangan mac spoofing yang berupa log file alert kismet, pcapdump, nettxt, dari hasil pengujian serangan mengunakan serangan mac spoofing.

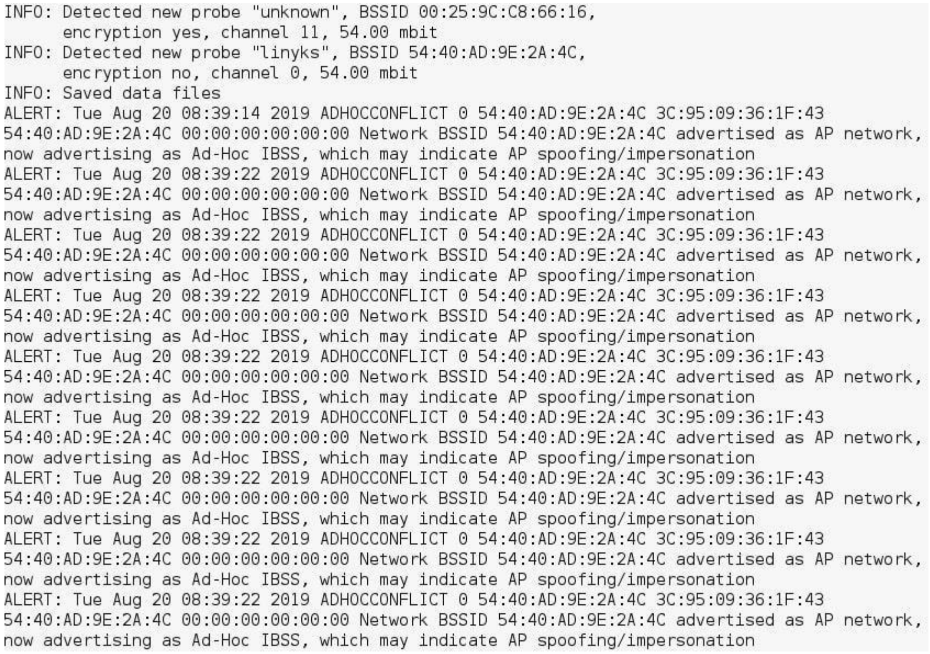
Gambar 1. Hasil Alert serangan mac spoofing



```
ALERT: Tue Aug 20 08:42:09 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 30:0D:43:C4:5A:78
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:42:21 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 30:0D:43:C4:5A:78
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:42:24 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 30:0D:43:C4:5A:78
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:42:24 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 30:0D:43:C4:5A:78
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:42:24 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 30:0D:43:C4:5A:78
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:42:24 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 30:0D:43:C4:5A:78
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:42:24 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 30:0D:43:C4:5A:78
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
```

Pada gambar diats bisa dilihat hasil alert kismet dengan mengunakan serangan mac spoofing, dalam melakukan penyerangan ini penyerang melakukan pengujian serangan terhadap server terlebih dahulu. Dimana mac AP 54:40:AD:9E:2A:4C menuju mac server korban 30:0D:43:C4:5A:78 terindikasih andanya terjadinya serangan mac spoofing.:

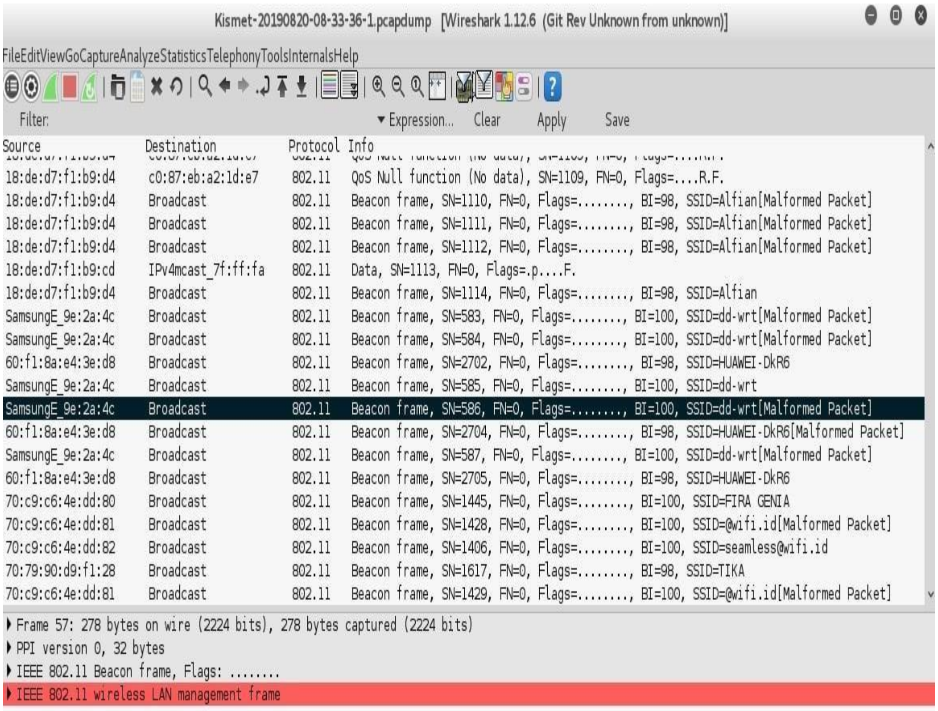
Gambar 2. Hasil Alert serangan mac spoofing



```
INFO: Detected new probe "unknown", BSSID 00:25:9C:C8:66:16,
      encryption yes, channel 11, 54.00 mbit
INFO: Detected new probe "linyks", BSSID 54:40:AD:9E:2A:4C,
      encryption no, channel 0, 54.00 mbit
INFO: Saved data files
ALERT: Tue Aug 20 08:39:14 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
```

Dari hasil gambar diatas bisa dilihat hasil *alert kismet* dengan mengunakan serangan *mac spoofing*, dalam melakukan penyerangan ini, kismet mampu menampilkan jaringan mana saja yang berhasil dideteksinya. Pengujian serangan mac spoofing terhadap client yang terhubung. Dimana mac AP 54:40:AD:9E:2A:4C menuju mac client 3C:95:09:36:1F:43. Dan kismet mampu mendeteksi alert serangan tersebut berindikasih serangan spoofing :

Gambar 3. Hasil serangan mac spoofing pcapdump

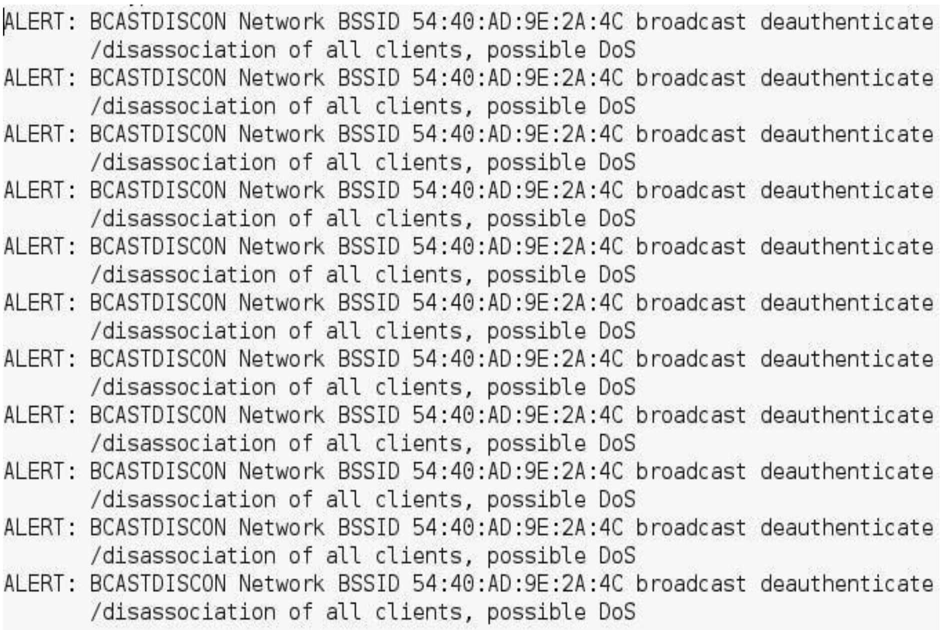


```
Source              Destination         Protocol  Info
18:de:d7:f1:b9:d4   c0:87:eb:a2:1d:e7   802.11    QoS Null function (No data), SN=1109, FN=0, Flags=....R.F.
18:de:d7:f1:b9:d4   Broadcast           802.11    Beacon frame, SN=1110, FN=0, Flags=........, BI=98, SSID=Alfian[Malformed Packet]
18:de:d7:f1:b9:d4   Broadcast           802.11    Beacon frame, SN=1111, FN=0, Flags=........, BI=98, SSID=Alfian[Malformed Packet]
18:de:d7:f1:b9:d4   Broadcast           802.11    Beacon frame, SN=1112, FN=0, Flags=........, BI=98, SSID=Alfian[Malformed Packet]
18:de:d7:f1:b9:cd   IPv4mcast_7f:ff:fa  802.11    Data, SN=1113, FN=0, Flags=.p....F.
18:de:d7:f1:b9:d4   Broadcast           802.11    Beacon frame, SN=1114, FN=0, Flags=........, BI=98, SSID=Alfian
SamsungE_9e:2a:4c   Broadcast           802.11    Beacon frame, SN=583, FN=0, Flags=........, BI=100, SSID=dd-wrt[Malformed Packet]
SamsungE_9e:2a:4c   Broadcast           802.11    Beacon frame, SN=584, FN=0, Flags=........, BI=100, SSID=dd-wrt[Malformed Packet]
60:f1:8a:e4:3e:d8   Broadcast           802.11    Beacon frame, SN=2702, FN=0, Flags=........, BI=98, SSID=HUAWEI-DkR6
SamsungE_9e:2a:4c   Broadcast           802.11    Beacon frame, SN=585, FN=0, Flags=........, BI=100, SSID=dd-wrt
SamsungE_9e:2a:4c   Broadcast           802.11    Beacon frame, SN=586, FN=0, Flags=........, BI=100, SSID=dd-wrt[Malformed Packet]
60:f1:8a:e4:3e:d8   Broadcast           802.11    Beacon frame, SN=2704, FN=0, Flags=........, BI=98, SSID=HUAWEI-DkR6[Malformed Packet]
SamsungE_9e:2a:4c   Broadcast           802.11    Beacon frame, SN=587, FN=0, Flags=........, BI=100, SSID=dd-wrt[Malformed Packet]
60:f1:8a:e4:3e:d8   Broadcast           802.11    Beacon frame, SN=2705, FN=0, Flags=........, BI=98, SSID=HUAWEI-DkR6
70:c9:c6:4e:dd:80   Broadcast           802.11    Beacon frame, SN=1445, FN=0, Flags=........, BI=100, SSID=FIRA GENIA
70:c9:c6:4e:dd:81   Broadcast           802.11    Beacon frame, SN=1428, FN=0, Flags=........, BI=100, SSID=@wifi.id[Malformed Packet]
70:c9:c6:4e:dd:82   Broadcast           802.11    Beacon frame, SN=1406, FN=0, Flags=........, BI=100, SSID=seamless@wifi.id
70:79:90:d9:f1:28   Broadcast           802.11    Beacon frame, SN=1617, FN=0, Flags=........, BI=98, SSID=TIKA
70:c9:c6:4e:dd:81   Broadcast           802.11    Beacon frame, SN=1429, FN=0, Flags=........, BI=100, SSID=@wifi.id[Malformed Packet]

▸ Frame 57: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits)
▸ PPI version 0, 32 bytes
▸ IEEE 802.11 Beacon frame, Flags: ........
▸ IEEE 802.11 wireless LAN management frame
```

Pada gambar diatas merupakan hasil serangan mac spoofing dimana hasil pcapdump menujukan adanya serangan dengan mac 54:40:AD:9E:2A:4C dengan melakukan broadcast mengunakan protokol 801.11 menuju ssid dd-wrt yang dilakukan penyerang :

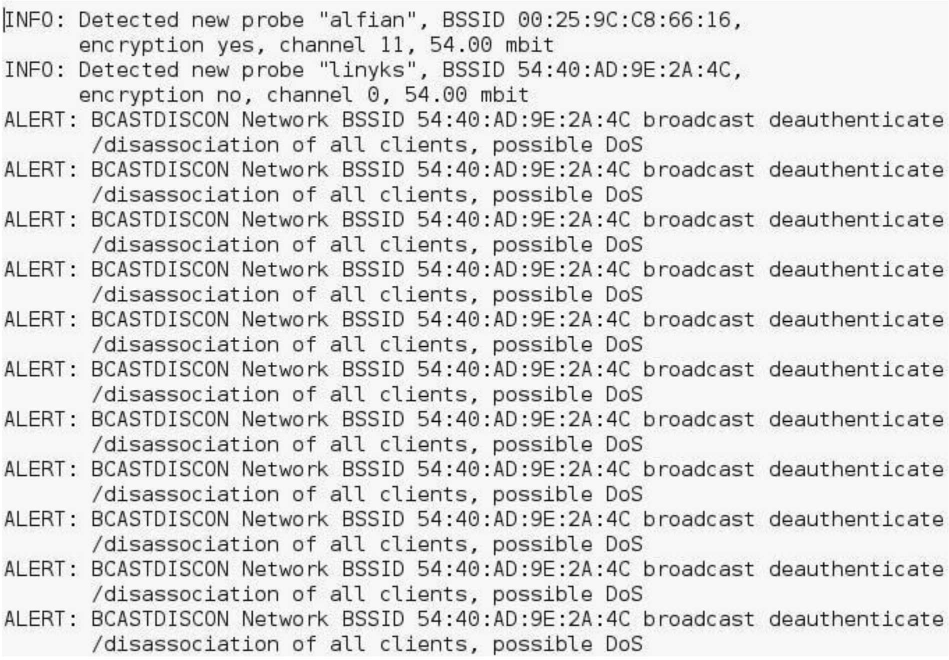
Gambar 4. Hasil alert serangan ddos



```
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
```

Berdasarkan pada gambar diats ini kismet dengan mengunakan serangan ddos, dalam melakukan penyerangan ini penyerang melakukan pengujian serangan terhadap server terlebih dahulu. Dan mampu mendeteksi serangan berupa alert dengan network bssid AP 54:40:AD:9E:2A:4C adanya broadcast yang berindikasih terjadinya serangan ddos :

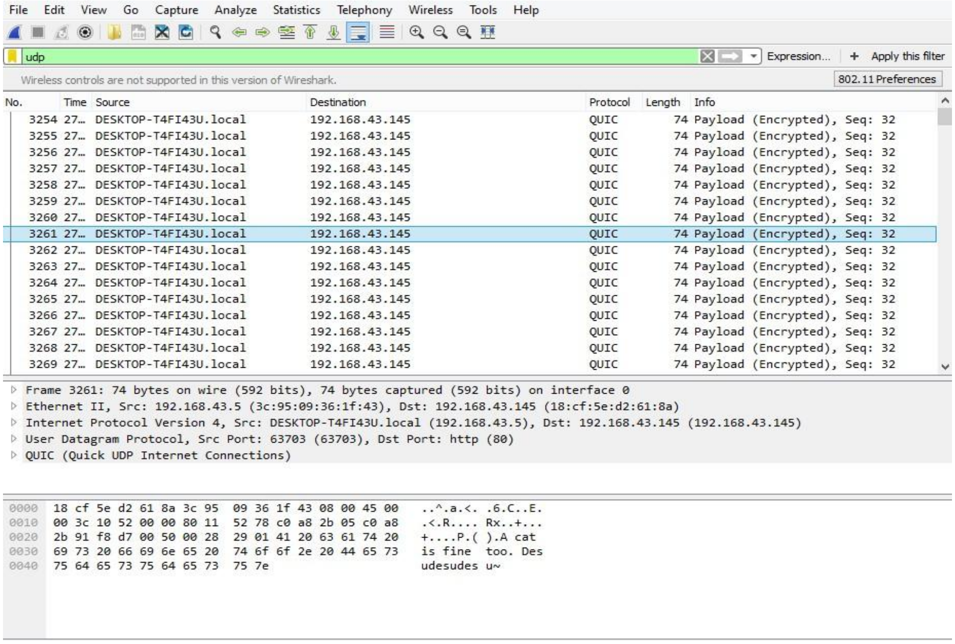
Gambar 5. Hasil alert serangan ddos



```
INFO: Detected new probe "alfian", BSSID 00:25:9C:C8:66:16,
      encryption yes, channel 11, 54.00 mbit
INFO: Detected new probe "linyks", BSSID 54:40:AD:9E:2A:4C,
      encryption no, channel 0, 54.00 mbit
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID 54:40:AD:9E:2A:4C broadcast deauthenticate
       /disassociation of all clients, possible DoS
```

Dari hasil gambar diatas bisa dilihat hasil alert kismet dengan mengunakan serangan ddos, dalam melakukan penyerangan ini, kismet mampu menampilkan jaringan mana saja yang berhasil dideteksinya. Yang bisa dilihat pada pada info berhasil mendeteksi ap linyks dengan bssid 54:40:AD:9E:2A:4C dan ap ddwrt dengan bssid54:40:AD:9E:2A:4C. Pada gambar dibawah . Pengujian serangan ddos dilakukan terhadap client yang terhubung, dengan network bssid 54:40:AD:9E:2A:4C adanya broadcast yang berindikasih terjadinya serangan ddos :

Gambar 6. Hasil serangan ddos pcapdump



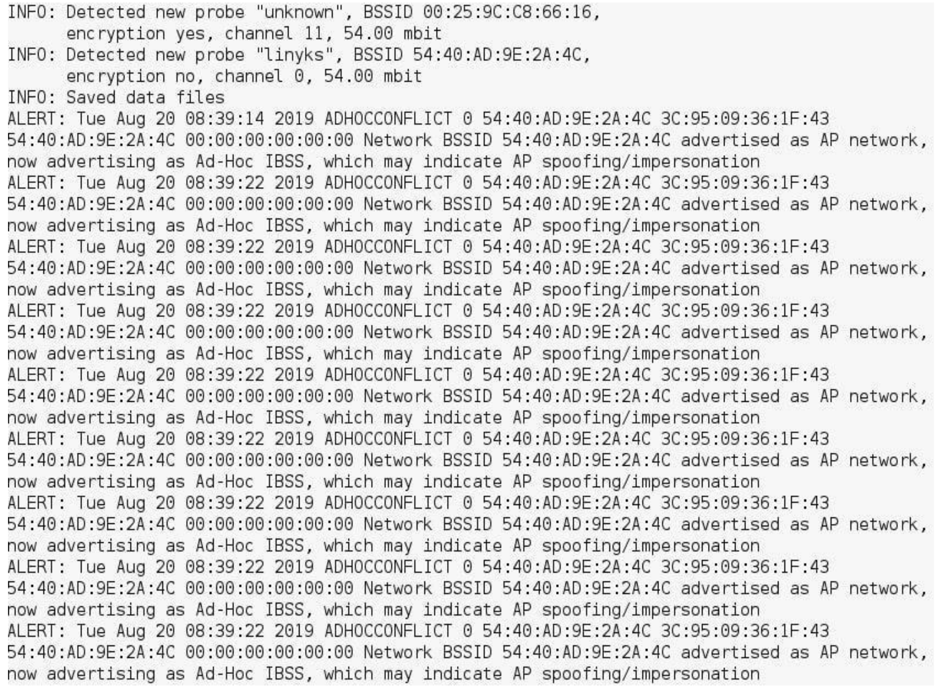
```
No.   Time Source                 Destination      Protocol Length Info
 3254 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3255 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3256 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3257 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3258 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3259 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3260 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3261 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3262 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3263 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3264 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3265 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3266 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3267 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3268 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
 3269 27… DESKTOP-T4FI43U.local   192.168.43.145   QUIC         74 Payload (Encrypted), Seq: 32
```

```
▷ Frame 3261: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▷ Ethernet II, Src: 192.168.43.5 (3c:95:09:36:1f:43), Dst: 192.168.43.145 (18:cf:5e:d2:61:8a)
▷ Internet Protocol Version 4, Src: DESKTOP-T4FI43U.local (192.168.43.5), Dst: 192.168.43.145 (192.168.43.145)
▷ User Datagram Protocol, Src Port: 63703 (63703), Dst Port: http (80)
▷ QUIC (Quick UDP Internet Connections)
```

```
0000  18 cf 5e d2 61 8a 3c 95  09 36 1f 43 08 00 45 00   ..^.a.<. .6.C..E.
0010  00 3c 10 52 00 00 80 11  52 78 c0 a8 2b 05 c0 a8   .<.R.... Rx..+...
0020  2b 91 f8 d7 00 50 00 28  29 01 41 20 63 61 74 20   +....P.( ).A cat
0030  69 73 20 66 69 6e 65 20  74 6f 6f 2e 20 44 65 73   is fine  too. Des
0040  75 64 65 73 75 64 65 73  75 7e                     udesudes u~
```

Pada gambar diatas merupakan hasil serangan *ddos* dimana hasil pcapdump menujukan adanya serangan menuju ip 192.168.43.145 protokol Quic adalah protokol udp yang dilakukan penyerang :

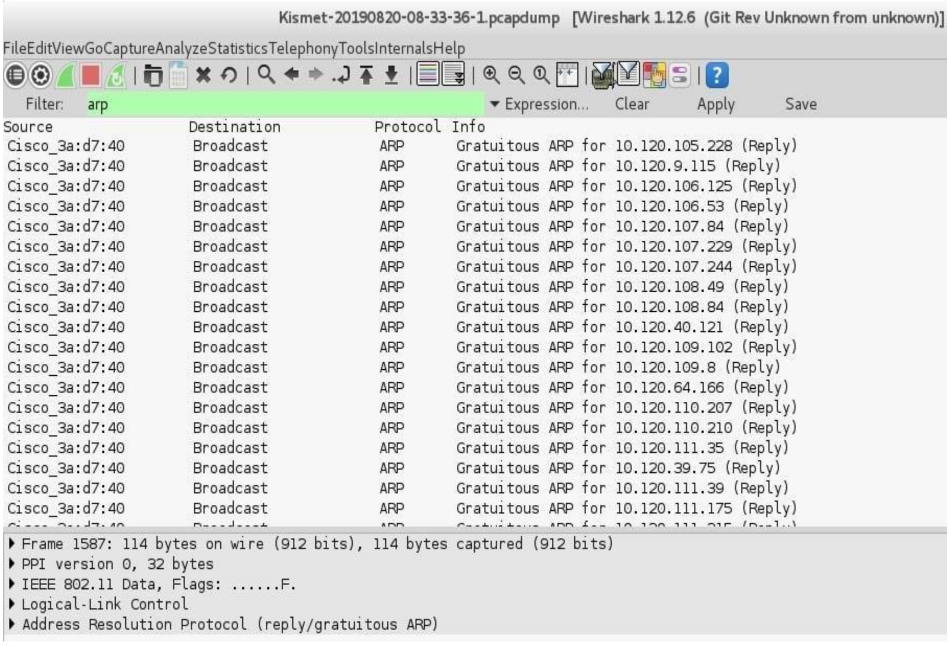
Gambar 7. Hasil alert serangan arp spoofing



```
INFO: Detected new probe "unknown", BSSID 00:25:9C:C8:66:16,
      encryption yes, channel 11, 54.00 mbit
INFO: Detected new probe "linyks", BSSID 54:40:AD:9E:2A:4C,
      encryption no, channel 0, 54.00 mbit
INFO: Saved data files
ALERT: Tue Aug 20 08:39:14 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
ALERT: Tue Aug 20 08:39:22 2019 ADHOCCONFLICT 0 54:40:AD:9E:2A:4C 3C:95:09:36:1F:43
54:40:AD:9E:2A:4C 00:00:00:00:00:00 Network BSSID 54:40:AD:9E:2A:4C advertised as AP network,
now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
```

Pada gambar diatas bisa dilihat hasil alert kismet dengan mengunakan serangan arp spoofing, dalam melakukan penyerangan ini penyerang melakukan pengujian serangan terhadap server terlebih dahulu. Dimana mac AP 54:40:AD:9E:2A:4C menuju mac server korban 3C:95:09:36:IF:43 indikasih andanya terjadinya serangan mac spoofing :

Gambar 8. Hasil serangan pcapdum arp spoofing



Filter: arp

```
Source          Destination     Protocol Info
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.105.228 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.9.115 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.106.125 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.106.53 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.107.84 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.107.229 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.107.244 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.108.49 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.108.84 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.40.121 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.109.102 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.109.8 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.64.166 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.110.207 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.110.210 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.111.35 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.39.75 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.111.39 (Reply)
Cisco_3a:d7:40  Broadcast       ARP      Gratuitous ARP for 10.120.111.175 (Reply)
```

```
▸ Frame 1587: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
▸ PPI version 0, 32 bytes
▸ IEEE 802.11 Data, Flags: ......F.
▸ Logical-Link Control
▸ Address Resolution Protocol (reply/gratuitous ARP)
```

Pada gambar diatas merupakan hasil serangan arp spoofing dimana hasil pcapdump menujukan adanya serangan arp spoofing dimana melakukan broadcast dengan protolol arp yang dilakukan penyerang.

Tabel 1. Tabel deteksi

no	Jenis serangan	Informasi yang didapatkan	Pendeteksi oleh kismet	Hasil deteksi alert
1	Mac spoofing	Kismet membaca traffic serangan yang menuju jaringan	dideteksi	Hasil alert memberitahukan adanya indikasih serangan spoofing
2	Ddos	Kismet membaca traffic serangan yang menuju jaringan	dideteksi	Hail alert memberitahukan adanya serangan ddos
3	Arp spoofing	Kismet membaca traffic serangan yang menuju jaringan	dideteksi	Hasil alert memberitahukan adanya serangan sniffing dengan serangan arp poison
4	Malware	Kismet membaca traffic serangan yang menuju jaringan	dideteksi	Hasil alert tidak terdeteksi

Pada penyerangan dengan mengunakan seranggan *mac spoofing,ddos,arp spoofing,* dan *malware* hasil dideteksi yang bisa dilihat pada tabel diatas dari seranganserangan yang telah dilakukan dengan *panetration testing* ,dapat dihasilkan suatu analisis bahwa suatu keamanan untuk mencegah *user* yang tidak memiliki hak. Agar tidak dapat bergabung ke dalam jaringan. :

4. KESIMPULAN

Berdasarkan dari hasil penelitian dan pembahasan yang telah di uraikan pada bab sebelumnya, penelitian berjudul " Peningkatan Keamanan Pada Jaringan *Wireless* Berbasis *Kismet DD-WRT*" maka penulis dapat menyimpulkan bahwa. Dengan adanya *Wireless Intrusion Detection System (WIDS)* menggunakan tools dapat mengetahui terjadi serangan pada jaringan, Kismet berhasil mencurigai serangan dijaringan wireless karena wireless intrusion detection system (*WIDS*) tersebut berhasil mendeteksi adanya serangan, Mendapatkan hasil berupa vurnability serangan yang nanti bisa digunakan sebagai memantau komputer target, Berdasarkan hasil jaringan wireless intrusion detection system (*WIDS*) yang dihubungkan berhasil mendeteksi serangan mac spoofing, ddos dan arp spoofing.

DAFTAR PUSTAKA

[1] Muis Rajab (2010). "Analisis Dan Perancangan Wireless Lan Security menggunakan Wpa2-Radius". Diambil dari : http://103.229.202.68/dspace/bitstream/123456789/21423/1/muis%20rajab-fst.pdf pada 5 Januari 2018

[2] Andi Nurhidayat (2015). "Wireless intrusion detection system using open source tool". Diambil dari : https://fti.uajy.ac.id/sentika/publikasi/makalah/2015/21.pdf pada Januari 2018

[3] Mohmad Gifar Perkasa (2015). "The Implmentasi Wireless Ids (Intrusion Detection System) For Network Securty Monitoring Bases On Kismet " Diambil dari: https://fti.uajy.ac.id/sentika/publikasi/makalah/2015/21.pdf pada Januari 2018

[4] Abdullah, Syukri. (2012). "Pengertian Jaringan Komputer". Diambil dari http://www.itartikel.com/2012/04/pengertianjaringankomputer.html pada 22 September 2018.

[5] Wagito. (2007). Jaringan Komputer Teori dan Implementasi Berbasis *Linux.* Yogyakarta : Gava Media.

[6] Prasetyo, Eko. 2014. Data Mining, Yogyakarta: Andi.

[7] Romadhon, Pearl Pratama. (2014). "Analisis kinerja jaringan LAN menggunakan metode QoS dan RMA pada PT Pertamina EP Uber Ramba (Persero)". *Skripsi*. Palembang: Fakultas Ilmu Komputer Universitas Bina Darma.