PENGUJIAN KESELAMATAN RANGKAIAN TANPA WAYAR MELALUI KAEDAH SERANGAN

MOHAMAD HANAFI BIN SALLEH HUDDIN
MOHD ZAMRI MURAH

Fakulti Teknologi Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Rangkaian tanpa wayar semakin meluas penggunaan di Malaysia. Namun, penggunaan rangkaian tanpa wayar mempunyai risiko keselamatan. Kertas ini bertujuan untuk mengkaji tahap keselamatan rangkaian tanpa wayar di Universiti Kebangsaan Malaysia, terutama di bangunan Pusanika. Kami akan mengkaji tahap keselamatan rangkaian *UKM-Warga*, iaitu satu rangkaian khusus untuk warga UKM yang terdapat di Pusanika. Kami melakukan enam serangan aktif/pasif terhadap rangkaian untuk menguji tahap keselamatan rangkaian. Serangan ini meliputi serangan terhadap peranti penghala, laman log masuk, pangkalan data dan rangkaian internet. Serangan terhadap peranti penghala dan laman log masuk meliputi serangan *DDOS*. Serangan terhadap rangkaian melibatkan serangan *man-in-the-middle*. Serangan suntikan SQL terhadap laman log masuk untuk menyelinap masuk ke dalam pangkalan data UKM. Rekod semasa serangan dan selepas serangan di analisa untuk tahap keselamatan rangkaian tanpa wayar di Pusanika. Kajian kami mendapati rangkaian tanpa wayar mempunyai tahap keselamatan yang tinggi di mana enam serangan yang di laksanakan tidak berjaya menembusi rangkaian *UKM-Warga* di Pusanika.

Katakunci: rangkaian tanpa wayar, serangan, godam

1 PENGENALAN

Universiti Kebangsaan Malaysia (UKM) merupakan sebuah universiti di Malaysia yang dilengkapi dengan pelbagai kemudahan rangkaian untuk kemudahan pelajar. Ini meliputi rangkaian setempat dan rangkaian tanpa wayar. UKM menyediakan pelbagai kemudahan rangkaian yang meliputi bangunan kamsis, tempat makan, pusat kegiatan pelajar, pejabat, bilik pensyarah, bilik kuliah dan sebagainya. Amnya, setiap pelajar UKM boleh mencapai rangkaian di mana jua dan bila sahaja.

Namun isu keselamatan rangkaian merupakan satu isu terbuka. Ini kerana rangkaian Internet di UKM digunakan oleh pelbagai pihak seperti pensyarah, pentadbir dan pelajar untuk pelbagai tujuan. Isu keselamatan termasuklah gangguan rangkaian dari serangan luar dan penggodaman terhadap sistem rangkaian. Ancaman keselamatan terhadap rangkaian tanpa wayar merupakan satu isu yang penting. Rangkaian tanpa wayar terdedah kepada pelbagai serangan, dan rangkaian tanpa wayar sepatutnya mampu mengelakkan serangan-serangan tersebut.

Oleh itu, kami telah melaksanakan satu kajian terhadap kesediaan rangkaian tanpa wayar menghadapi serangan-serangan yang mungkin dilaksanakan oleh pihak penggodam. Dengan kajian ini, kami dapat melihat kesediaan rangkaian tanpa wayar dalam menghadapi serangan penggodam.

1.1 Penyataan Masalah

Rangkaian tanpa wayar *UKM-Warga* di UKM merupakan satu rangkaian tanpa wayar yang bersifat terbuka untuk penggunanya. Ia boleh digunakan oleh pelajar dan pensyarah dengan menggunakan kata masuk pengenalan diri dan kata laluan.

Oleh kerana ia bersifat terbuka, ia boleh digunakan oleh sesiapa sahaja. Ini merupakan isu keselamatan pertama di mana sesiapa sahaja boleh menceroboh rangkaian UKM-Warga dengan kaedah cuba-dan-silap, di mana penggodam boleh menggunakan satu senarai kata masuk pengenalan diri dan kata laluan.

Kedua, rangkaian ini boleh dilumpuhkan dengan serangan DDOS dan lelaki di tengah. Kemampuan rangkaian menahan dari serangan DDOS adalah penting untuk memastikan rangkaian sentiasa berfungsi dengan baik.

Akhirnya, pengguna mungkin menggunakan rangkaian untuk tujuan privasi dan sulit. Adalah penting untuk memastikan data dan privasi pengguna terlindung semasa menggunakan rangkaian.

Oleh demikian, kita boleh lihat isu keselamatan ini dari segi capaian, kebolehpercayaan dan kesulitan data.

1.2 Objektif

Kajian ini adalah untuk mengkaji tahap keselamatan rangkaian tanpa wayar di Pusanika, UKM. Ini meliputi kajian untuk mengetahui;

1. Tahap keselamatan dalam mencapai rangkaian dengan menggunakan kata pengenalan diri dan kata laluan.
2. Tahap ketahanan rangkaian dalam menghadapi serangan DDOS dan lelaki di tengah.
3. Tahap kesulitan data yang di gunakan oleh pengguna dalam rangkaian.

2 KAJIAN KESUSASTERAAN

Rangkaian tanpa wayar merupakan satu teknologi rangkaian yang banyak digunakan sekarang. Teknologi ini mempunyai beberapa piawai seperti 802.11a, 802.11b, 802.11n dan 802.11ac. Piawai rangkaian tanpa wayar yang banyak digunakan adalah 802.11ac dan 802.11n. Kedua piawai ini mempunyai ciri-ciri keselamatan seperti AEP[1].

Serangan terhadap rangkaian tanpa wayar boleh dilakukan secara pasif atau aktif[2]. Serangan aktif meliputi serangan DDOS dan lelaki di tengah. Serangan pasif meliputi suntikan SQL, menggodam laman log masuk dan menangkap data dalam rangkaian[3], [4].

Senarai serangan terhadap rangkaian tanpa wayar adalah dalam jadual 1.

Jadual 1. Antara jenis-jenis serangan terhadap rangkaian tanpa wayar.

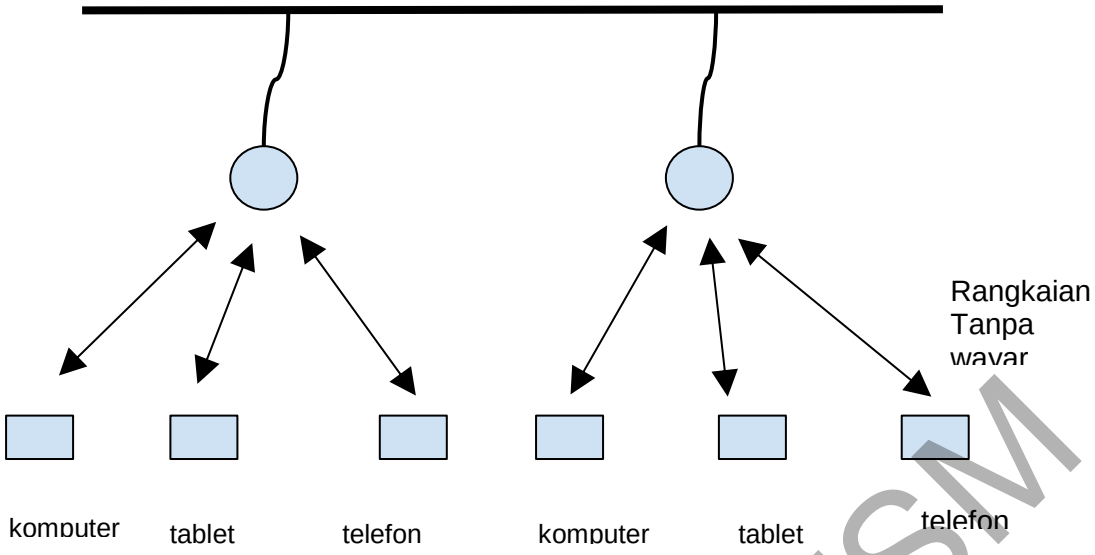
Serangan	Penerangan	Alat
war driving	mencari pusat capaian secara rambang untuk tujuan capaian dan penembusan	airmon-ng
MAC spoofing	menyamar MAC untuk tujuan mencapai satu-satu pusat capaian	SMAC
eavesdropping	menangkap dan menyahkod data trafik yang tidak dilindungi untuk mendapatkan maklumat sensitif seperti kata log masuk dan kata laluan	10 point, bold
WEP Key Cracking	menangkap trafik data untuk tujuan mendapatkan kekunci WEP	10 point, bold
Login theft	mencuri data login dari aplikasi yang menggunakan cleartext	10 point, italic

3 KAEDAH

Kajian ini melibatkan serangan terhadap rangkaian tanpa wayar *UKM-Warga*. *UKM-Warga* adalah satu rangkaian tanpa wayar untuk warga UKM. Ia bersifat terbuka dan terdapat di seluruh UKM. Kajian ini hanya melibatkan *UKM-Warga* di Pusanika, iaitu pusat khidmat pelajar. Lokasi ini dipilih kerana ianya merupakan satu lokasi yang banyak digunakan oleh pelajar, jumlah data trafik dan kemudahan melakukan serangan.

Serangan melibatkan serangan terhadap penghala, laman log masuk, rangkaian tanpa wayar dan pangkalan data. Jenis serangan meliputi DDOS, lelaki di tengah, godam laman log masuk dan suntikan SQL[5].

Serangan dilakukan dengan menggunakan Kali Linux[6]. Kali Linux adalah satu edaran Linux yang mengandungi perisian untuk tujuan penggodaman beretika.



Rajah 1. Model rangkaian tanpa wayar. Serangan boleh dilakukan terhadap penghala, trafik data, laman log masuk dan kestabilan rangkaian.

3.1 Serangan DDOS terhadap penghala

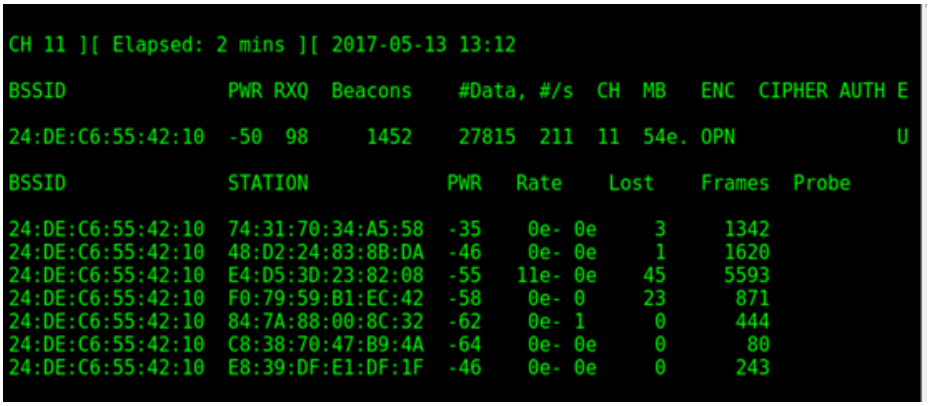
Serangan DDOS dilakukan kepada penghala. Ini bertujuan untuk melumpuhkan penghala. Jika penghala tidak berfungsi, maka seluruh rangkaian akan lumpuh.

```
CH  3 ][ Elapsed: 18 s ][ 2017-05-13 13:06

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

30:87:D9:1E:CB:28  -38       11        0    0   4  54e. OPN              Celco
1C:B9:C4:40:C0:38  -40       16        0    0   1  54e. OPN              UKM W
30:87:D9:1E:D9:18  -39        9        0    0   8  54e. OPN              Celco
1C:B9:C4:00:C0:38  -42       16      559   40   1  54e. OPN              UKM W
D0:17:C2:DC:81:35  -47       17        1    0   6  54e  WPA2 CCMP   PSK  ASUS
24:DE:C6:55:42:12  -50       11        0    0  11  54e. WPA2 CCMP   MGT  eduro
24:DE:C6:55:42:10  -51       18      857   90  11  54e. OPN              UKM-W
24:DE:C6:55:42:11  -51       13      721   59  11  54e. OPN              UKM-P
D4:CA:6D:1F:2D:BF  -51       28        0    0   1  54e. OPN              Sunne
9C:A9:E4:13:CA:70  -50       17        1    0  11  54e. WPA2 CCMP   PSK  3CA6F
D6:CA:6D:1F:2D:BF  -52       30        0    0   1  54e. WPA2 CCMP   PSK  <leng
D6:CA:6D:1F:2D:C1  -52       27        0    0   1  54e. WPA2 CCMP   PSK  <leng
D6:CA:6D:1F:2D:C0  -52       30        0    0   1  54e. WPA2 CCMP   PSK  <leng
30:87:D9:1E:CB:48  -54        6        0    0   8  54e. OPN              Celco
00:0C:46:F6:79:A8  -64       24       37    0   7  54 . OPN              tetam
30:87:D9:1E:D9:68  -62       10        0    0  13  54e. OPN              Celco
92:CD:B6:1C:21:8B  -64        5        0    0   6  54e  WPA2 CCMP   PSK  DIREC
54:8C:A0:F4:E4:F5  -65        5        0    0  11  54e. WPA2 CCMP   PSK  DIREC
```

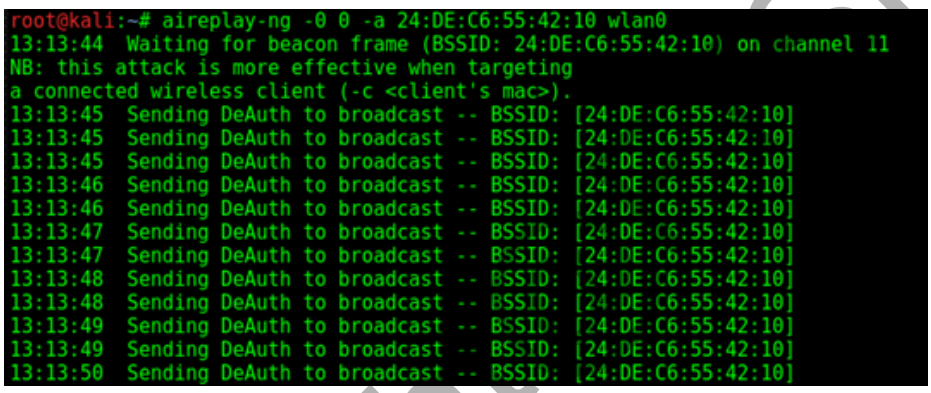
Rajah 2. Dengan menggunakan *airmon-ng*, kita boleh mendapat penghala dalam rangkaian UKM-Warga.

Setiap penghala mempunyai BSSID yang unik. Ini untuk membezakan satu penghala dengan penghala yang lain. Setiap penghala disambungkan kepada rangkaian wayar untuk capaian Internet. Sebagai contoh, satu penghala adalah **24:DE:C6:55:42:10** untuk capaian UKM-Warga. Serangan DDOS boleh dilakukan pada penghala ini.

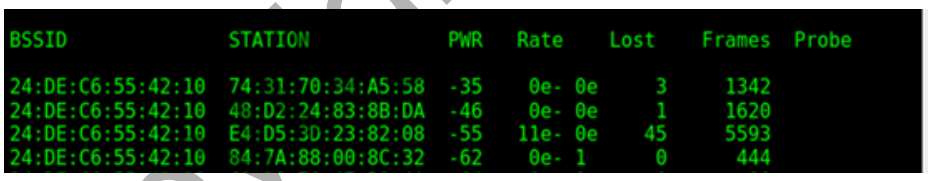
Terdapat 2 penghala untuk rangkaian UKM-Warga iaitu **24:DE:C6:55:42:10** dan **1C:B9:C4:00:C0:38**. BBSID lain merujuk kepada hot-spot atau capaian tanpa wayar yang lain.



Rajah 2. Serangan DDOS terhadap penghala UKM-Warga **24:DE:C6:55:42:10**. Terdapat sejumlah pengguna yang mencapai penghala ini.



Rajah 3. Serangan DDOS terhadap penghala **24:DE:C6:55:42:10** sedang dijalankan.



Rajah 4. Pengguna pada **24:DE:C6:55:42:10** selepas serangan DDOS. Sebilangan pengguna telah tersingkir. Ini menandakan rangkaian berjaya dilumpuhkan dengan serangan DDOS.

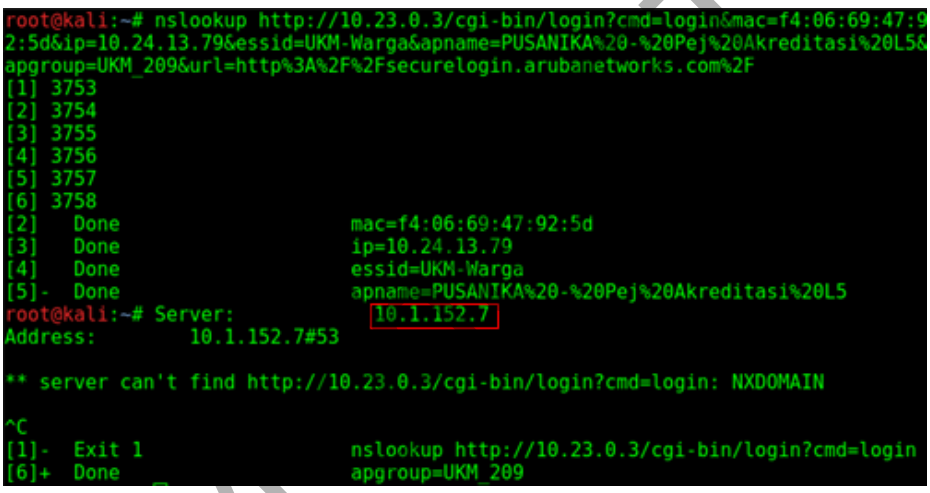
Dari serangan yang dijalankan, adalah didapati penghala UKM-Warga adalah terdedah kepada serangan DDOS. Akibat dari serangan DDOS, pengguna akan tidak boleh mencapai rangkaian.

3.2 Serangan terhadap laman log masuk UKM-Warga

Pengguna perlu log masuk sebelum dapat menggunakan UKM-Warga. Laman log masuk ini memerlukan kata pengenalan diri dan kata laluan. Serangan boleh dilakukan pada laman log masuk untuk menguji sama ada laman log masuk boleh dilumpuhkan.

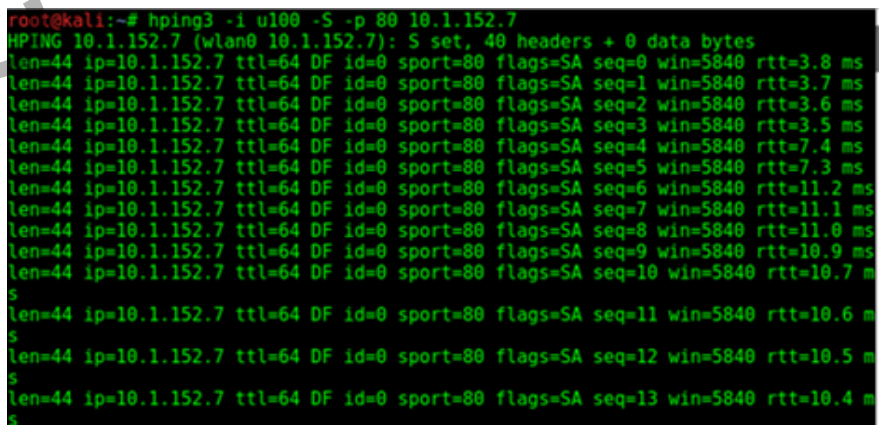
Rajah 5. Laman log masuk UKM-Warga.

Laman log masuk UKM-Warga ditempatkan kepada satu pelayan lain. Kita boleh gunakan *nslookup* untuk mencapai IP pelayan ini.

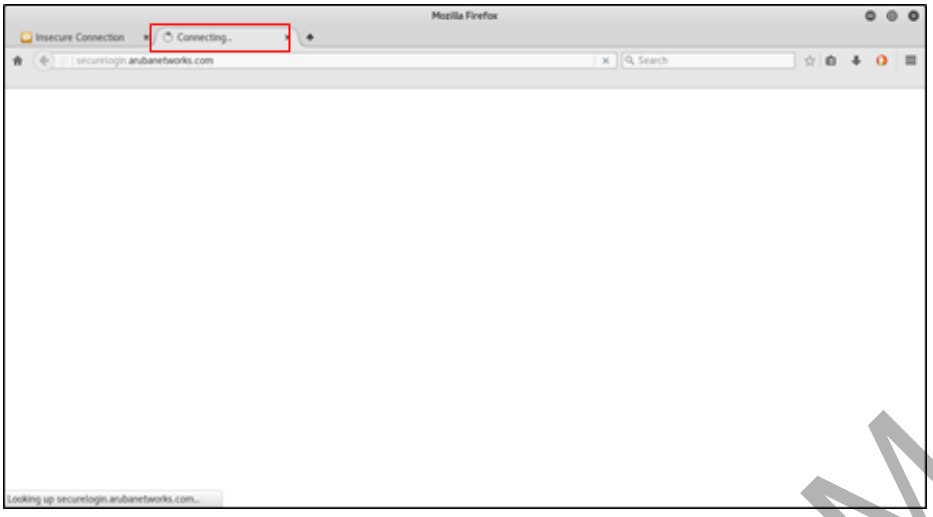


Rajah 6. Menggunakan *nslookup* untuk mendapatkan IP laman log masuk UKM-Warga.

Berdasarkan nslookup, kita dapati IP laman log masuk adalah **10.1.152.7**. Serangan boleh dilakukan pada pelayan ini. Jika serangan berjaya, laman ini akan lumpuh dan akan gagal untuk melayan pengguna untuk log masuk.



Rajah 6. Serangan *hping* terhadap pelayan log masuk UKM-Warga .



Rajah 7. Laman log masuk UKM-Warga gagal dipaparkan semasa serangan *hping* .

Kajian mendapati, laman log masuk mudah dilumpuhkan dengan serangan hping. Bila ini berlaku, pengguna tidak akan dapat log masuk untuk mencapai rangkaian. Serangan ini telah berjaya menghalang pengguna dari mencapai laman log masuk UKM-Warga.

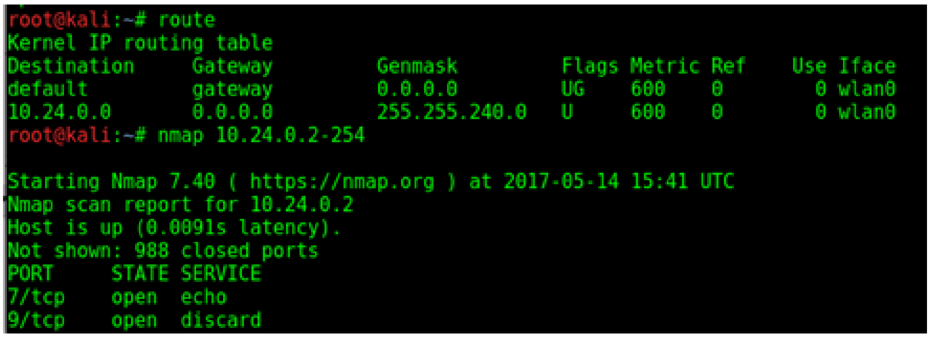
3.3 Serangan lelaki di tengah dalam rangkaian tanpa wayar terbuka

Serangan lelaki di tengah adalah serangan yang melibatkan penangkapan data. Kajian ini dilakukan di Pusanika, di mana ia merupakan satu pusat khidmat untuk pelajar dan pensyarah. Untuk memudahkan pelajar dan pensyarah, terdapat beberapa rangkaian tanpa wayar terbuka untuk digunakan.

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
30:87:D9:1E:CB:28	-38	11	0	0	4	54e.	OPN			Celco
1C:B9:C4:40:C0:38	-40	16	0	0	1	54e.	OPN			UKM W
30:87:D9:1E:D9:18	-39	9	0	0	8	54e.	OPN			Celco
1C:B9:C4:00:C0:38	-42	16	559	40	1	54e.	OPN			UKM W
30:87:D9:1E:CB:48	-54	6	0	0	8	54e.	OPN			Celco
00:0C:46:F6:79:A8	-64	24	37	0	7	54 .	OPN			tetam
30:87:D9:1E:D9:68	-62	10	0	0	13	54e.	OPN			Celco
24:DE:C6:55:42:10	-51	18	857	90	11	54e.	OPN			UKM-W
24:DE:C6:55:42:11	-51	13	721	59	11	54e.	OPN			UKM-P
D4:CA:6D:1F:2D:BF	-51	28	0	0	1	54e.	OPN			Sunne
9C:A9:E4:13:CA:70	-50	17	1	0	11	54e.	WPA2	CCMP	PSK	3CA6F
D6:CA:6D:1F:2D:BF	-52	30	0	0	1	54e.	WPA2	CCMP	PSK	<leng
D6:CA:6D:1F:2D:C1	-52	27	0	0	1	54e.	WPA2	CCMP	PSK	<leng
D6:CA:6D:1F:2D:C0	-52	30	0	0	1	54e.	WPA2	CCMP	PSK	<leng
D0:17:C2:DC:81:35	-47	17	1	0	6	54e	WPA2	CCMP	PSK	ASUS
24:DE:C6:55:42:12	-50	11	0	0	11	54e.	WPA2	CCMP	MGT	eduro
92:CD:B6:1C:21:8B	-64	5	0	0	6	54e	WPA2	CCMP	PSK	DIREC
54:8C:A0:F4:E4:F5	-65	5	0	0	11	54e.	WPA2	CCMP	PSK	DIREC

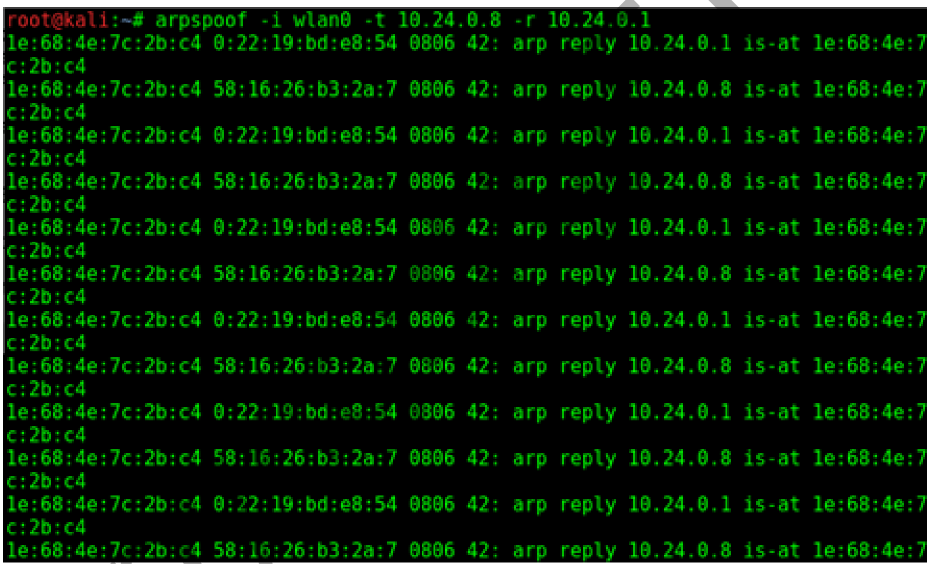
Rajah 7. Rangkaian tanpa wayar terbuka di Pusanika iaitu Celcom, UKM-Warga, tetamu-UKM, UKM-Pelajar. Rangkaian tanpa wayar terbuka adalah rangkaian di mana data trafik tidak disulitkan semasa trafik.

Serangan lelaki di tengah boleh dilakukan pada rangkaian terbuka. Ia memerlukan IP mangsa dan IP penghala. Dengan menyamar sebagai IP mangsa, penyerang boleh menerima data trafik yang dilakukan antara IP mangsa dan IP penghala.



Rajah 7. Mendapatkan IP penghala menggunakan *route* dan mendapat IP mangsa dengan menggunakan *nmap*.

Dengan menggunakan *route*, kita memperoleh IP penghala pada 10.24.0.1. Selanjutnya, kita mengimbas dengan *nmap* untuk mencari IP mangsa. Katakan kita memperoleh IP mangsa 10.24.0.11. Selanjutnya kita mengguna *arpspoof* untuk melakukan serangan lelaki di tengah. Dengan arpspoof, segala data dari IP mangsa kepada IP penghala akan juga dihantar kepada IP penyerang. Ini membolehkan penyerang menangkap data trafik mangsa.



Rajah 8. Serangan lelaki di tengah sedang dijalankan di mana IP mangsa adalah 10.24.0.8 dan IP penghala adalah 10.24.0.1.

Hasil dari serangan adalah penangkapan data yang beraku antara IP mangsa dan IP penghala.

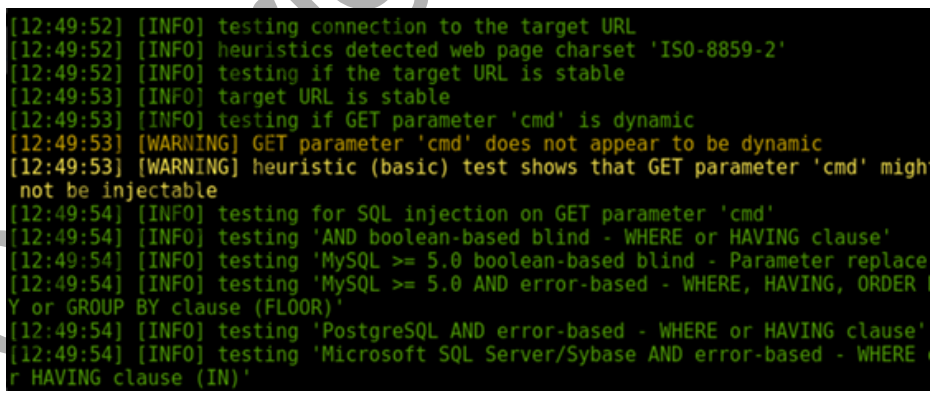
Rajah 9. Data yang ditangkap semasa sesi serangan lelaki di tengah.

Kita mendapati serangan ini membolehkan kita untuk mendapatkan kata pengenalan diri dan kata laluan untuk lama web. Ini merupakan satu isu keselamatan yang besar.

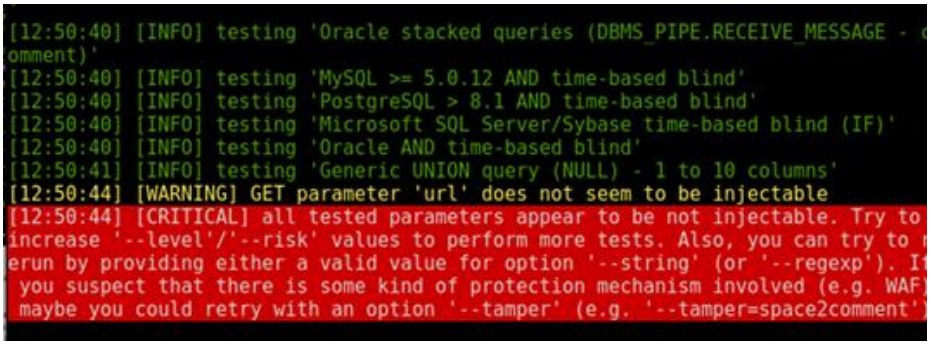
3.4 Serangan pangkalan data

Pangkalan data merupakan sistem penting dalam satu-satu organisasi. Ia menyimpan pelbagai maklumat peribadi dan sulit setiap entiti organisasi. Keselamatan pangkalan data dari dicerobohi adalah penting.

Serangan terhadap pangkalan data UKM boleh dilakukan dengan menggunakan *sqlmap* dan suntikan SQL.



Rajah 10. Serangan *sqlmap* terhadap pangkalan data UKM.



Rajah 11. Serangan *suntik SQL* terhadap pangkalan data UKM.

Kajian mendapati bahawa kedua serangan gagal menggodam sistem pangkalan data di UKM.

3.4 Serangan laman log masuk menggunakan kaedah *brute force*

Laman log masuk UKM-Warga memerlukan kata pengenalan diri dan kata laluan. Satu kaedah untuk menggodam laman log masuk ialah kaedah *brute force*. Dalam kaedah ini, ia melibatkan kaedah cuba dan salah. Langkah pertama adalah mendapat senarai kata pengenalan diri yang digunakan. Untuk laman log masuk UKM-Warga, kata pengenalan diri lazimnya nombor matrik atau nombor pekerja. Kiat boleh gunakan *google* untuk mendapatkan senarai kata pengenalan diri.

Rajah 12. Senarai kata pengenalan diri dari hasil pencarian google.

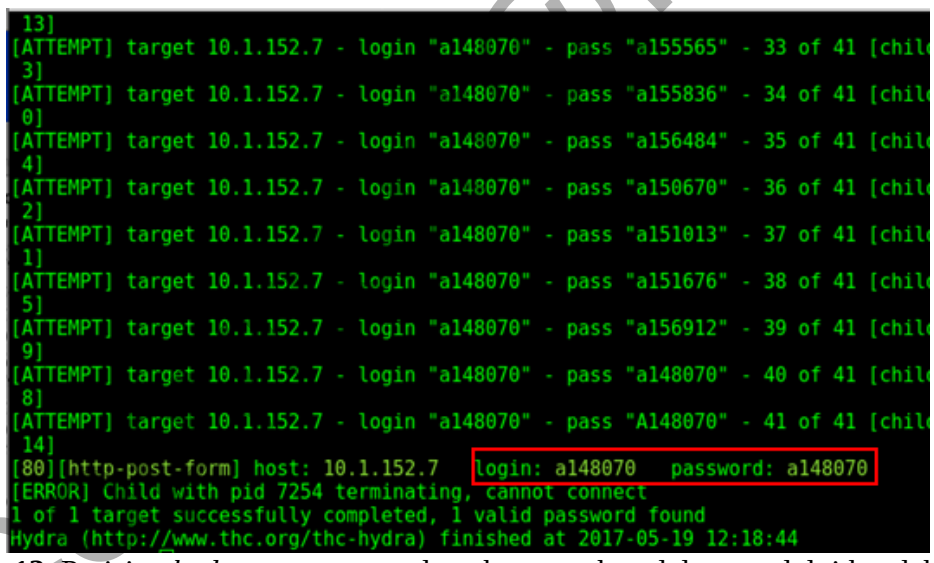
Fail yang diperolehi mempunyai nama dan nombor matrik. Ia boleh digunakan sebagai kata pengenalan diri untuk log masuk UKM-Warga.

Bil	Matrik	Nama	Tahun
1		Afzan Adam (Dr.)	
2	A157582	MOHAMAD NORIZAL BIN ABDULLAH	1
3	A160774	MOHD EMIR ASHRAF BIN MAZUAN	1
4	A161085	LEE HUI ZHI	1
5	A161198	TAN SIN MIN	1
6	A155441	NURADLIN MASTURA BINTI MOHD ZUDI	2
7	A155816	PUA SZE KIAT	2
8	A156443	AZAMUDDIN HAZIQ BIN SAMSUDIN	2
9	A150652	PANG XIN YI	3
10	A151000	GOO MIAO LING	3
11	A151529	NUR 'IN BALQIS BINTI JOHAR	3
12	A156657	SHALINI A/P ALAGRISAMY	3

Bil	Matrik	Nama	Tahun
1		Azizi Abdullah (Dr.)	
2	A157756	SITI NUR ATHIRAH BINTI MOHD AZMEY	1
3	A160796	NUR HIDAYAH BINTI ABD MALIK	1
4	A161088	WONG KIM JIE	1
5	A161204	LIM JIE MIN	1
6	A155565	NUR HIDAYAH BINTI RIZUAN	2
7	A155836	FAEQA ADILAH BINTI MOHD ANUAR	2
8	A156484	NUR AZMIN BINTI AMIR	2
9	A150670	NUR NABILAH BINTI MOHD NAZMI	3
10	A151013	MUNIRAH BINTI MAZLAN	3
11	A151676	IZLYN ADLINA BINTI AHMAD AKMAL	3
12	A156912	NURUL FIRZANA BINTI ZAINAL RASHID	3

Rajah 13. Fail yang mengandungi nombor matrik pelajar. Ia boleh digunakan sebagai kata pengenalan diri.

Selanjutnya, kita boleh menggunakan perisian *hydra* untuk melakukan proses log masuk secara *brute force*.



Rajah 13. Perisian *hydra* mampu mendapatkan satu kata laluan melalui kaedah *brute force*.

3.5 Kesimpulan

Kami telah melakukan serangan aktif dan pasif terhadap rangkaian tanpa wayar UKM-Warga. Kami dapati rangkaian ini mudah terdedah kepada serangan DDOS, lelaki di tengah dan laman log masuk melalui kata laluan. Kami juga dapati serangan terhadap pangkalan data dengan menggunakan *sqlmap* dan suntikan SQL tidak berhasil.

4 Keputusan dan perbincangan

Kajian ini melibatkan lima serangan terhadap rangkaian tanpa wayar UKM-Warga di Pusanika, UKM. Kami mendapati rangkaian tanpa wayar UKM-warga mudah terdapat kepada beberapa serangan. Hasil serangan ini boleh melumpuhkan rangkaian dan menyulitkan pengguna untuk menggunakan rangkaian.

Rangkaian UKM-Warga mudah terdedah kepada serangan DDOS dan hping. Serangan ini boleh melumpuhkan rangkaian. Juga, kaedah serangan lelaki di tengah boleh digunakan untuk mendapatkan data sulit pengguna.

Untuk mengelakkan serangan *hping* dan *DDOS*, disarankan agar penghala menggunakan kemampuan untuk mengelakkan kedua serangan ini. Kebanyakan penghala terkini mempunyai kemampuan sediaada untuk menyekat serangan DDOS dan hping.

Untuk mengelakkan serangan lelaki di tengah, rangkaian boleh menggunakan kaedah penyulitan data antara penghala dan pengguna. Ia akan menyebabkan data tidak boleh dibaca dengan mudah open penyerang.

serangan	sasaran	kesan	impak
DDOS	penghala	melumpuhkan rangkaian, pengguna tidak boleh log masuk	tinggi.
lelaki di tengah	aliran data trafik antara mangsa dan penghala	mendapat maklumat sulit dan privasi	tinggi.
serangan pangkalan data	pangkalan data	mendapatkan maklumat sulit	gagal dilakukan.
serangan kata laluan	laman log masuk	mampu masuk ke dalam sistem	tinggi
serangan hping	penghala	gagal memaparkan laman log masuk	tinggi

Jadual. 13. Jenis serangan dan impak.

5 Kesimpulan

Tahap keselamatan rangkaian UKM-Warga adalah baik. Namun, penambah baikan perlu dilakukan untuk memastikan data pengguna selamat dan rangkaian tidak mudah dilumpuhkan.

RUJUKAN

[1] M. S. Gast, *802.11ac: A Survival Guide: Wi-Fi at Gigabit and Beyond*. "O'Reilly Media, Inc.," 2013.
[2] T. Karygiannis and L. Owens, "Wireless network security," *NIST Spec. Pub.*, vol. 800, p. 48, 2002.
[3] M. Alamanni, *Kali Linux Wireless Penetration Testing Essentials*. Packt Publishing Ltd, 2015.
[4] F. T. Sheldon, J. M. Weber, S. M. Yoo, and W. D. Pan, "The Insecurity of Wireless Networks," *IEEE Security Privacy*, vol. 10, no. 4, pp. 54–61, Jul. 2012.
[5] G. Weidman, *Penetration testing : a hands-on introduction to hacking*. San Francisco, CA: No Starch Press, 2014.
[6] J. Muniz, *Web Penetration Testing with Kali Linux*. Packt Publishing Ltd, 2013.