

BAB IV

HASIL DAN PEMBAHASAN

4.1 Penentuan Perangkat

Langkah awal dalam penelitian ini adalah menentukan perangkat-perangkat yang akan di teliti, dalam industri 4.0 ini perangkat pendukung yang berperan penting adalah router, ip cam, scada, ics, dan nas. Perangkat – perangkat itu yang nantinya akan digunakan peneliti untuk menganalisis resiko kerentanan pada perangkat pendukung industri 4.0

4.2 Pengumpulan Informasi

Perangkat-perangkat yang sudah ditentukan merupakan perangkat yang sering digunakan untuk menunjang kegiatan industri 4.0 dan pada tahapan ini kita mulai melakukan pengumpulan informasi dengan bantuan mesin pencari perangkat yaitu shodan, dengan shodan kita bisa menemukan informasi terkait IP public untuk pengujian dan penilaian terhadap perangkat-perangkat yang sudah ditentukan. Di Shodan menyediakan API yang bisa saya manfaatkan untuk mengambil sample perangkat yang menggunakan IP public untuk diteliti seberapa banyak perangkat pendukung industry 4.0 yang langsung terkoneksi IP public yang memungkinkan para pelaku kejahatan siber memanfaatkan perangkat-

perangkat tersebut. Dan berikut adalah source code yang saya buat untuk memandaatkan API shodan untuk mencari target

```
<?php

$model = $_POST['model'];

$curl = curl_init();

curl_setopt_array($curl, [
    CURLOPT_RETURNTRANSFER => 1,
    CURLOPT_URL =>
    'https://api.shodan.io/shodan/host/search?key=ON7eVr60Vrp
    xxWlVt1pFkxcU9kGNEUqi&query='.$model
]);

$res = json_decode(curl_exec($curl), true);
curl_close($curl);

for($i=0; $i<4; $i++){?>
```

Setelah proses untuk mencari model daripada perangkat yang sudah ditentukan dari situ keluarlah hasil berupa ip public yang nantinya akan saya analisis lagi dengan bantuan *tools* untuk mencari tahu kerentanan pada perangkat tersebut, ip public dari model-model perangkat yang sudah di tentukan akan di simpan dalam database sehingga tidak ada duplikasi data pada saat analisis kerentanan pada jaringan ip public nantinya.

4.3 Analisa Kerentanan Perangkat

Setelah informasi terkait IP Publik sudah didapatkan selanjutnya adalah mulai menganalisa informasi dari ip public untuk mendapatkan kerentanan apa saja yang mungkin bisa terjadi pada perangkat-perangkat pendukung industri 4.0. dari masing-masing jenis perangkat saya mengambil 40 model tiap perangkat untuk dianalisa apakah perangkat tersebut sangat beresiko diberikan ip public secara langsung tanpa ada perimeter security di depannya dan apa saja kemungkinan terburuk yang akan terjadi. Dalam hal tersebut ada yang Namanya attack surface, open port, dan cve dan berikut adalah rincian bagaimana saya mengklasifikasi kerentanan pada perangkat-perangkat tersebut.

4.3.1 Scan Open Port

Langkah awal untuk menganalisa kerentanan pada perangkat-perangkat yang sudah di dapatkan dari pengumpulan informasi yang berupa IP Publik langkah selanjutnya adalah mencari port yang terbuka pada perangkat tersebut. Disini port yang terbuka juga menjadi variable untuk menentukan kerentanan pada perangkat tersebut, semakin banyak port yang terbuka bisa membuat para pelaku kejahatan siber memanfaatkannya. Karena port-port yang terbuka tersebut mengandung informasi awal dari kerentanan perangkat tersebut, contohnya port telnet yang terbuka pada

perangkat modem di dalam port tersebut bisa membahayakan karena terkadang username dan password dari firmware telnet pada perangkat tersebut banyak di temukan di internet sehingga wajib untuk membatasi port tersebut. Untuk mencari port terbuka tersebut saya menggunakan bantuan tools yang bernama nmap dan berikut adalah contoh dari penggunaanya

```
root@mail:~ (bash)
Damaras-MacBook-Pro:~ damara$ nmap 93.171.153.65
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-21 00:20 WIB
Nmap scan report for 93.171.153.65
Host is up (0.31s latency).
Not shown: 979 closed ports
PORT      STATE      SERVICE
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    filtered  smtp
53/tcp    open      domain
80/tcp    open      http
179/tcp   open      bgp
548/tcp   filtered  afp
1026/tcp  filtered  LSA-or-nterm
1027/tcp  filtered  IIS
1028/tcp  filtered  unknown
1029/tcp  filtered  ms-lsa
1030/tcp  filtered  iad1
1031/tcp  filtered  iad2
1032/tcp  filtered  iad3
1033/tcp  filtered  netinfo
1034/tcp  filtered  zincite-a
1035/tcp  filtered  multidropper
2000/tcp  open      cisco-sccp
2875/tcp  filtered  dxmessagebase2
8291/tcp  open      unknown
9090/tcp  filtered  zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 59.94 seconds
Damaras-MacBook-Pro:~ damara$
```

4.3.2 Attack Surface

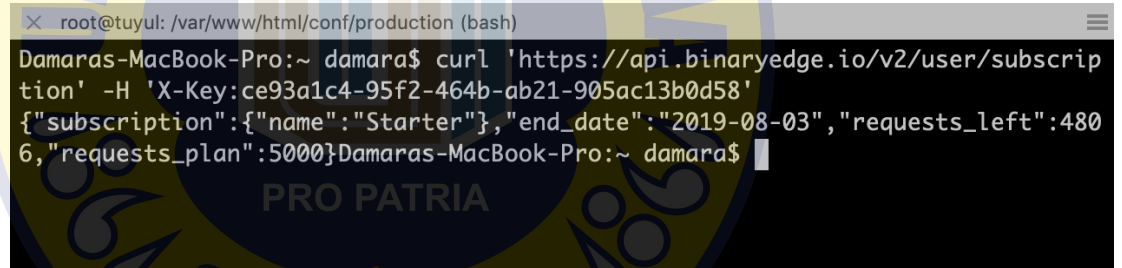
Setelah mendapatkan informasi terkait port yang terbuka disini saya bisa memilih bagian mana saja yang kemungkinan di serang oleh pelaku kejahatan siber. Disini ada beberapa bagian dari perangkat-perangkat tersebut yang bisa di simulasikan yaitu ada serangan secara brutal atau sering disebut bruteforce, mencoba default password pada semua perangkat, denial of service, serta mencoba exploit yang ada pada internet.

4.3.3 CVE dan CVSS

Selanjutnya adalah mengumpulkan informasi terkait CVE dan CVSS pada perangkat tersebut, semakin banyak CVE yang ada pada perangkat tersebut semakin perlu juga kita memperhatikan segala bagian dari kemungkinan-kemungkinan terjadinya serangan terhadap perangkat tersebut. Sehingga kita masih tetap aman dalam menggunakan perangkat tersebut tanpa menggantinya dengan merek atau tipe lain karena jika setiap ada informasi terkait exploit pada perangkat perlu di lakukan pengantian itu merupakan pemborosan tersendiri.

4.4 Library

Untuk membantu peneliti agar lebih rapih dalam menyajikan laporan kerentanan perangkat-perangkat pendukung industry 4.0 saya menggunakan bantuan dari library bernama binaryedge. Dalam libraby tersebut menyediakan banyak module yang memudahkan peneliti untuk mengumpulkan informasi terkait cve dan cvss. Cara penggunaan library ini ialah menggunakan curl sehingga menampilkan data yang masih berantakan dan akan di rapihkan pada proses selanjutnya. Berikut contoh penggunaan library binaryedge



```
root@tuyul: /var/www/html/conf/production (bash)
Damaras-MacBook-Pro:~ damara$ curl 'https://api.binaryedge.io/v2/user/subscription' -H 'X-Key:ce93a1c4-95f2-464b-ab21-905ac13b0d58'
{"subscription":{"name":"Starter"},"end_date":"2019-08-03","requests_left":4806,"requests_plan":5000}Damaras-MacBook-Pro:~ damara$
```

4.5 Pemerosesan Data Kerentanan

Setelah semua data kerentanan sudah di dapatkan langkah selanjutnya adalah memproses semuanya menjadi kesimpulan terhadap IP-IP yang telah di scan sebelumnya

4.5.1 Pemindaian IP dengan Shodan

Data yang pertama kali di cari adalah model dari perangkat yang sudah ditentukan dengan api shodan, model yang di cari akan

mengeluarkan beberapa data seperti IP dan port yang terbuka, namun pada proses ini saya hanya menyimpan data IP yang telah dicari dengan bantuan shodan

```
root@tuyul: /var/www/html/conf/production (bash)
{"ip": 248070224, "isp": "TPG Internet", "port": 5060, "hostnames": ["14-201-64-80.tpgi.com.au"], "location": {"city": "Elsternwick", "region_code": "07", "area_code": null, "longitude": 145.0, "country_code3": "AUS", "country_name": "Australia", "postal_code": "3185", "dma_code": null, "country_code": "AU", "latitude": -37.88329999999999}, "timestamp": "2019-07-23T03:55:54.507554", "domains": ["tpgi.com.au"], "org": "TPG Internet", "data": "SIP/2.0 200 OK\r\nVia: SIP/2.0/UDP nm;rport=26810;received=16.45.193.13;branch=foo\r\nCall-ID: 50000\r\nFrom: <sip:nm@nm>;tag=root\r\nTo: <sip:nm2@nm2>;tag=foo\r\nCSeq: 42 OPTIONS\r\nAllow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, SUBSCRIBE, NOTIFY, REFER, OPTIONS\r\nAccept: application/sdp, application/simple-message-summary, message/sipfrag;version=2.0\r\nSupported: replaces, 100rel, timer, noferensub\r\nAllow-Events: message-summary, refer\r\nUser-Agent: TP-Link SIP Stack V1.0.0\r\nContent-Type: application/sdp\r\nContent-Length: 380\r\n\r\nv=0\r\no=- 3772842953 3772842953 IN IP4 14.201.64.80\r\ns=pjmedia\r\nnc=IN IP4 14.201.64.80\r\nnm=audio 60120 RTP/AVP 0 8 9 110 2 18 96\r\na=rtpmap:60121 IN IP4 14.201.64.80\r\na=rtpmap:0 PCMU/8000\r\na=rtpmap:8 PCMA/8000\r\na=rtpmap:9 G722/16000\r\na=rtpmap:110 G726-32/8000\r\na=rtpmap:2 G721/8000\r\na=rtpmap:18 G729/8000\r\na=sendrecv\r\na=ptime:0\r\na=rtpmap:96 telephone-event/8000\r\na=fmtp:96 0-15\r\n", "asn": "AS7545", "transport": "udp", "ip_str": "14.201.64.80"}, {"info": "SIP end point; Status: 200 OK", "_shodan": {"id": null, "options": {}}, "ptr": true, "module": "sip", "crawler": "5faf2928ceb560cb4276cc1b4660b2d763cc6397"}, {"hash": 1593737594, "os": null, "ip": 248046037, "isp": "TPG Internet", "port": 5060, "hostnames": ["14-200-225-213.tpgi.com.au"], "location": {"city": "Mckinnon", "region_code": "07", "area_code": null, "longitude": 145.05, "country_code3": "AUS", "country_name": "Australia", "postal_code": "3204", "dma_code": null, "country_code": "AU", "latitude": -37.91669999999999}, "timestamp": "2019-07-23T03:55:51.420361", "domains": ["tpgi.com.au"], "org": "TPG Internet", "data": "SIP/2.0 200 OK\r\nVia: SIP/2.0/UDP nm;rport=26810;received=223.16.242.217;branch=foo\r\nCall-ID: 50000\r\nFrom: <sip:nm@nm>;tag=root\r\nTo: <sip:nm2@nm2>;tag=foo\r\nCSeq: 42 OPTIONS\r\nAllow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, SUBSCRIBE, NOTIFY, REFER, OPTIONS\r\nAccept: application/sdp, application/simple-message-summary, message/sipfrag;version=2.0\r\nSupported: replaces, 100rel, timer, noferensub\r\nAllow-Events: message-summary, refer\r\nUser-Agent: TP-Link SIP Stack V1.0.0\r\nContent-Type: application/sdp\r\nContent-Length: 386\r\n\r\nv=0\r\no=- 3772842950 3772842950 IN IP4 14.200.225.213\r\ns=pjmedia\r\nnc=IN IP4 14.200.225.213\r\nnt=0 0\r\nnm=audio 60928 RTP/AVP 9 110 18 0 8 2 96\r\na=rtpmap:60929 IN IP4 14.200.225.213\r\na=rtpmap:9 G722/16000\r\na=rtpmap:110 G726-32/8000\r\na=rtpmap:18 G729/8000\r\na=rtpmap:0 PCMU/8000\r\na=rtpmap:8 PCMA/8000\r\na=rtpmap:2 G721/8000\r\na=sendrecv\r\na=ptime:0\r\na=rtpmap:96 telephone-event/8000\r\na=fmtp:96 0-15\r\n", "asn": "AS7545", "transport": "udp", "ip_str": "14"}
Damaras-MacBook-Pro:~ damara$ curl 'https://api.shodan.io/shodan/host/search?key=0N7eVr60VrpXXwLVt1pFxcU9kGNEUqi&query=tp-link'
```

4.5.2 Mengolah IP Pada Database

Setelah proses yang di hasilkan shodan saya hanya mengambil informasi terkait IP dari model perangkat yang saya cari namun

dengan tampilan yang masih raw membuat susah untuk saya mencari IP pada hasilnya dan akhirnya saya proses dengan script php yang akan mengkstrasi hasilnya kedalam database

```
<?php

date_default_timezone_set("Asia/Jakarta");

include "config.php";

$model =
strtoupper($_POST['model']);

$id_shodan = "";

$t = date("Y-m-d H:i:s");

$r = mysqli_query($conn, "select
* from shodan where model = '$model'");

$c = mysqli_num_rows($r);

if($c > 0){

$h = mysqli_fetch_assoc($r);

$id_shodan = $h['id'];

}else{

mysqli_query($conn, "insert
into shodan (model, tgl_update) values ('$model',
'$t')");

$q = mysqli_query($conn,
"select * from shodan where model = '$model'");

$w = mysqli_fetch_assoc($q);

$id_shodan = $w['id'];

}
```



```
</div>
```

4.5.3 Melempar Data IP ke Library

Setelah proses mengolah data IP yang didapat dari shodan dan menyimpannya pada database, langkah selanjutnya adalah melempar hasil IP tersebut ke library binaryedge untuk mencari tau port yang terbuka, attack surface, cve dan cvss. Sama seperti proses pencarian IP di shodan cara yang saya gunakan untuk mencari celah kerentanan pada IP-IP tersebut dengan bantuan script PHP sebagai berikut

```
<div id="collapse<?= $i ?>"
class="collapse" aria-
labelledby="heading<?= $i ?>"
data-parent="#accordionExample">
<div
class="card-body">
<?php
$ips =
$respl['matches'][$i]['ip_str'];
$q =
mysqli_query($conn, "select * from
edbinary where ips = '$ips'");
$qq =
mysqli_num_rows($q);
if($qq
> 0){
```

```

= mysqli_fetch_assoc($q);
//
print_r($s);

$resps = json_decode($s['file_json'],
true);
}else{

$curls = curl_init();

curl_setopt_array($curls, [
CURLOPT_RETURNTRANSFER => 1,
CURLOPT_HTTPHEADER => ["X-Key:ce93a1c4-
95f2-464b-ab21-905ac13b0d58"],
CURLOPT_URL =>
'https://api.binaryedge.io/v2/query/sco
re/ip/'. $ips
]);
//
$resps = json_decode(curl_exec($curls),
true);

$resps = curl_exec($curls);

curl_close($curls);

= mysqli_query($conn, "insert into
edbinary (id_shodan, ips, file_json,

```

```
tgl_update) values ('$id_shodan',
'$ips', '$resps', '$t');"

$resps = json_decode($resps, true);
}
?>
```

4.5.4 Membuat Tampilan Aplikasi

Agar hasil dari penelitian saya dapat mudah dibaca dan dipahami maka saya buat tampilan aplikasi untuk mencari resiko kerentanan pada perangkat pendukung industry 4.0

Model / Merks

Masukan Model / Merk perangkat target. Ex: TP-LINK. NB: Jangan gunakan spasi

Cari

Check IP anda disini

Masukan IP perangkat anda. Ex: 80.211.184.148. NB: Menggunakan pattern IP pada umumnya

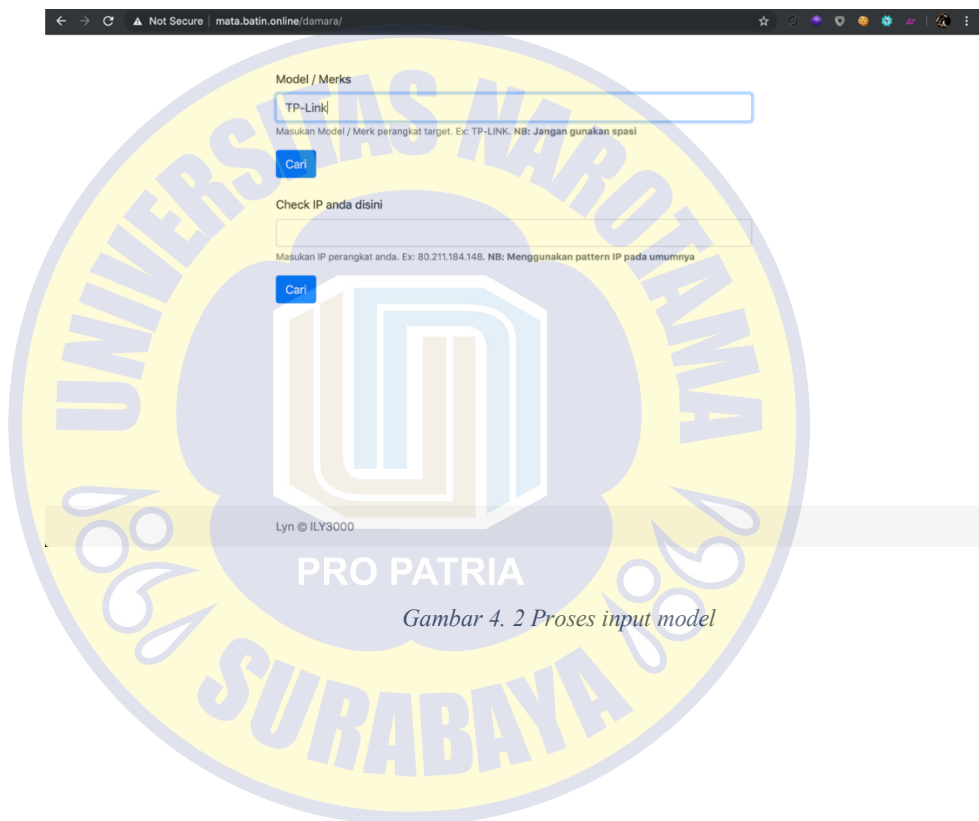
Cari

Lyn © ILY3000

Gambar 4. 1 Halaman depan

4.6 Hasil

Setelah semua proses sudah di jalankan langkah terakhir adalah mencari perangkat-perangkat yang sudah di tentukan dengan menggunakan web aplikasi yang telah saya buat berikut adalah contoh penggunaannya



Gambar 4. 2 Proses input model

Back

Model / Merk perangkat Target: TP-Link

#0	Domains: Domains not Available / IP: 117.102.139.18
#1	Domains: satnet.net / IP: 186.71.139.219
#2	Domains: tpgi.com.au / IP: 115.64.237.110
#3	Domains: Domains not Available / IP: 203.63.194.240

Lyn @ILY300

Gambar 4. 3 Hasil dari proses crwaling data

Back

Model / Merk perangkat Target: TP-Link

#0	Domains: Domains not Available / IP: 117.102.139.18
#1	Domains: satnet.net / IP: 186.71.139.219
#2	Domains: tpgi.com.au / IP: 115.64.237.110
#3	Domains: Domains not Available / IP: 203.63.194.240

Score	Open Port	Score CVE	Hackable	
2.9	5060;	0	NEGATIVE	Detail

Lyn @ILY300

Gambar 4. 4 Field dari baris yang didapat