

Hacking Methodology Untuk Pengujian Keamanan Drone

Sigit Budi Prayoga¹, Fata Nidaul Khasanah^{1,*}

¹ Teknik Informatika; STMIK Bina Insani; Jl. Siliwangi No.6 Rawa Panjang Bekasi Bekasi Timur 17114 Indonesia; Telp. (021) 824 36 886 / (021) 824 36 996. Fax. (021) 824 009 24; e-mail:

* Korespondensi: e-mail: sigitbudiprayoga@gmail.com, fatanidaul.khasanah@gmail.com

* Korespondensi: e-mail: fatanidaul@gmail.com

Diterima: 7 Mei 2019 ; Review: 21 Mei 2019 ; Disetujui: 22 Juni 2019

Cara sitasi: Prayoga S, Khasanah FN. 2019. *Hacking Methodology Untuk Pengujian Keamanan Drone*. Informatics For Educators and Professionals. 3 (2): 161 – 170.

Abstrak: Saat ini perkembangan teknologi *drone* tengah populer dikalangan masyarakat dengan kecanggihan dalam fitur yang dikembangkan oleh setiap *vendor*. Dahulu *drone* hanya dimanfaatkan dalam bidang militer saja tidak seperti sekarang *drone* dapat dimanfaatkan pada bidang *photography* dan juga dapat digunakan dalam berbagai bidang seperti industri film, pertanian, lalu lintas, keamanan, dan lain sebagainya untuk memudahkan melakukan pengawasan. *Drone* memungkinkan adanya permasalahan, adanya kemungkinan celah kerentanan sehingga *drone* dapat diambil alih atau di *hack*. Dari adanya celah kerentanan keamanan pada *drone* ini muncul suatu masalah yang diakibatkan oleh *hacker* yang mempunyai niat ingin mengambil alih atau mengambil data yang ada pada *drone*. Untuk dapat mengetahui celah kerentanan maka harus dilakukan pengujian terhadap keamanan pada *drone* dengan pengujian menggunakan *hacking methodology*, uji *drone* dengan tahapan tahapan *hacking methodology* dengan *footprinting*, *scanning*, *enumeration*, *gaining access*, *denial of services* dan dari hasil pengujian ini maka dapat diketahui celah kerentanan yang terdapat pada *drone* seperti *port telnet* yang terbuka, *port http* yang terbuka *port rtsp* yang terbuka hal itu dapat membuat sistem atau data dapat eksploitasi oleh *hacker*. Lalu ketika sudah dapat diketahui hasil dari pengujian ini, maka dapat dihitung nilai resiko kerentanan yang ada pada *drone* dengan menggunakan perhitungan CVSS *calculator* versi 2 yang nanti dapat memberikan kesimpulan dari celah kerentanan yang ada pada *drone*.

Kata kunci : *Common Vulnerability Scoring System, Drone, Hacker, Hacking Methodology*

Abstract: *Currently the development of drone technology is popular among the public with sophistication in features developed by each vendor. In the past, drones were only used in the military field, unlike nowadays drones can be used in the field of photography and can also be used in various fields such as the film industry, agriculture, traffic, security, etc. to facilitate supervision. Drones allow for problems, possible vulnerability loopholes so that drones can be taken over or hacked. From the vulnerability of security vulnerabilities in this drone, a problem arises from hackers who have intentions who want to take over or retrieve data that is on a drone. To be able to find out the vulnerability gap it must be tested against the security of the drone by testing using hacking methodology, drone testing with stages of hacking methodology stages with footprinting, scanning, enumeration, gaining access, denial of services and from the results of this test it can be identified the vulnerability gap there are drones like open telnet ports, open http ports open rtsp ports that can make the system or data exploited by hackers. Then when we can know the results of this test, we can calculate the value of the vulnerability risk in the drone by using the calculation of CVSS calculator version 2 which can then provide conclusions from the vulnerability loopholes that exist in the drone.*

Keywords: *Common Vulnerability Scoring System, Drone, Hacker, Hacking Methodology*

1. Pendahuluan

Perkembangan teknologi *drone* tengah populer dikalangan masyarakat dengan kecanggihan dalam fitur yang dikembangkan oleh setiap vendor. Dahulu *drone* hanya dimanfaatkan dalam bidang militer saja tidak seperti sekarang *drone* dapat dimanfaatkan pada bidang *photography* dan juga dapat digunakan dalam berbagai bidang seperti industri film, pertanian, lalu lintas, keamanan, dan lain sebagainya untuk memudahkan melakukan pengawasan.

Drone adalah pesawat tanpa awak (*unmanned aerial vehicle*) yang mampu mengendalikan dirinya sendiri atau dikendalikan oleh pilot dari jarak jauh atau secara *remote* dengan menggunakan *remote control*. Selain itu *drone* juga dapat dikendalikan menggunakan *smartphone*. Untuk dapat menerbangkan *drone* sesuai dengan keinginan pengguna, dapat digunakan *remote control* yang menggunakan gelombang *Wi-fi* dengan frekuensi 2,4 Ghz atau 5,8 Ghz [Giffari dkk, 2016].

Drone adalah pesawat tanpa awak yang dikendalikan dengan sebuah *remote control*, di lengkapi dengan *GPS* sebagai navigasi, dan *lock position*. Namun penggunaan *drone* dengan menggunakan banyak *propeller* merupakan salah satu masalah penggunaan *drone*. Semakin banyak *propeller* yang digunakan, maka masa hidup *drone* di udara juga akan semakin berkurang. Hal ini dikarenakan baterai yang digunakan oleh wahana tersebut banyak digunakan untuk mensuplai *propeller* agar dapat berputar. Berdasarkan permasalahan tersebut maka diusulkan untuk membuat *drone* yang praktis dan efisien energi, sehingga daya tempuhnya dapat lebih lama, karena penggunaan baterai yang hemat yaitu *singrone* inovasi rancang bangun *Drone Single Propeller* sebagai wahana pemetaan lahan berbasis *UAV* [Giffari dkk, 2016].

Quadcopter merupakan salah satu jenis dari *Unmanned Aerial Vehicle (UAV)*, yaitu robot yang dapat terbang dengan empat baling-baling disetiap ujungnya. Untuk menerbangkan *quadcopter* pada umumnya digunakan *remote control* atau *smartphone*. Namun diperlukan keahlian dan pengalaman khusus untuk dapat menerbangkan *quadcopter*. Berdasarkan permasalahan tersebut maka perlu dikembangkan inovasi dari sistem kendali navigasi pada *quadcopter* agar lebih mudah digunakan. Sistem yang dibuat pada penelitian ini dibuat menggunakan salah satu bagian dari *natural user interface* berupa gerakan tubuh dari pengguna yang akan dideteksi menggunakan *Kinect*. Dari hasil pengujian yang telah dilakukan didapatkan hasil persentase ketepatan gerakan yang berhasil dilakukan pengguna untuk mengendalikan *quadcopter* sebesar 100%. Selain itu juga diperoleh hasil dari kecepatan gerakan *roll*, *pitch*, dan *yaw* pada *quadcopter* berbanding lurus dengan nilai input dari gerakan pengguna yang berarti kecepatan *quadcopter* dapat diatur sesuai gerakan yang diberikan oleh pengguna. Untuk *delay* yang dihasilkan sistem ini pada saat pengguna menggerakkan tubuh hingga *quadcopter* mengikuti instruksi adalah sebesar 0,05 detik [Wildani dkk, 2018].

Common Vulnerability Scoring System (CVSS) adalah standar industri yang bebas dan terbuka untuk menilai tingkat keparahan kerentanan keamanan sistem komputer. *CVSS* mencoba untuk menetapkan skor keparahan untuk kerentanan, memungkinkan responden untuk memprioritaskan tanggapan dan sumber daya sesuai ancaman. Skor dihitung berdasarkan rumus yang bergantung pada beberapa metrik yang memperkirakan kemudahan eksploitasi dan dampak eksploitasi [Attila dkk, 2016].

Drone memungkinkan adanya permasalahan, adanya kemungkinan celah kerentanan sehingga mengakibatkan *drone* dapat diambil alih atau di *hack*. Untuk dapat mengetahui celah kerentanan ini harus dilakukan pengujian. Setelah diketahui celah kerentanan yang ada pada *drone* maka memungkinkan adanya tindakan pengambilalihan *drone* dan tindakan pengambilan data yang dilakukan oleh *hacker*. Untuk dapat mengetahui celah kerentanan ini harus dilakukan pengujian terhadap keamanan pada *drone* dengan menggunakan *tools airmon-ng*, *airodump-ng*, *aircrack-ng*, *zenmap*, *xhydra* dan lain-lain. Hal tersebut bertujuan untuk mengetahui celah celah kerentanan yang ada pada *drone*.

Berdasarkan permasalahan yang terdapat pada *drone*, maka pada penelitian ini untuk mengetahui celah kerentanan maka dilakukan pengujian, setelah itu lakukan eksploitasi, lalu hitung nilai resiko kerentanan dengan perhitungan *Common Vulnerability Scoring System (CVSS)*. Dalam penelitian ini menggunakan sistem operasi *kali linux* yang di dalamnya terdapat *tools* yang handal untuk melakukan pengujian keamanan pada *drone*. Dari adanya celah keamanan pada *drone* ini muncul suatu masalah yang diakibatkan oleh oknum (*hacker*) yang mempunyai niat yang ingin mengambil alih atau ingin mengambil data dan merusak sistem

yang ada pada *drone*. Dan dari pengujian ini dilakukan penyerangan melalui *telnet*, penyerangan menggunakan teknik *bruteforce* untuk mengetahui *login* dan *password* untuk masuk kedalam sistem lalu mengambil file berupa gambar atau video. Dan dari masalah tersebut diharapkan muncul sebuah sistem yang dapat mengamankan *drone* dari serangan *hacker* agar nanti nya dapat lebih aman disaat digunakan oleh pengguna *drone* itu sendiri.

2. Metode Penelitian

Hacking methodology mengacu pada pendekatan langkah demi langkah yang digunakan oleh penyerang untuk menyerang sasaran seperti jaringan komputer. Tidak ada pendekatan langkah demi langkah spesifik yang digunakan oleh semua *hacker*. Seperti biasa diharapkan ketika sebuah kelompok beroperasi di luar peraturan seperti dilakukan *hacker*, peraturan tidak berlaku dengan cara yang sama. Tahapan-tahapan nya adalah sebagai berikut: *Footprinting, Scanning, Enumeration, Gaining access, Denial of service* [Oriyano, 2014:15].

Tahap *footprinting* adalah proses menggali informasi sebanyak-banyaknya dari target (*drone*). Jika menggunakan aplikasi berbasis *web* seperti *whois*, penerapan *footprinting* juga menggunakan aplikasi lain atau bisa juga menggunakan seperti aplikasi *zenmap*. Pada penelitian ini penulis menggunakan aplikasi *zenmap*. Tahap ini adalah yang pertama dalam pengujian penetrasi, intinya adalah mengumpulkan sebanyak mungkin informasi tentang target *drone*, *IP address*, dan lain-lain.

Pada langkah ini *scanning* berfungsi untuk menentukan *host* mana yang tinggal di jaringan dan apa yang mereka lakukan, yang paling populer adalah *nmap* dan *supercan*. Pemindaian dapat dengan mudah diambil oleh sistem deteksi, walaupun ada beberapa cara untuk menghindari hal ini dengan pemindaian spesifik. Terdapat identifikasi *service* apa saja yang berjalan di dalam *drone*. Pada tahap *scanning* ini meliputi analisis dan *scanning* terhadap *service* apa saja yang dijalankan pada sistem. Penulis juga menggunakan *zenmap* untuk mengetahui informasi-informasi *port-port* yang terbuka atau tertutup dan mengetahui *service* yang tersedia pada *drone*.

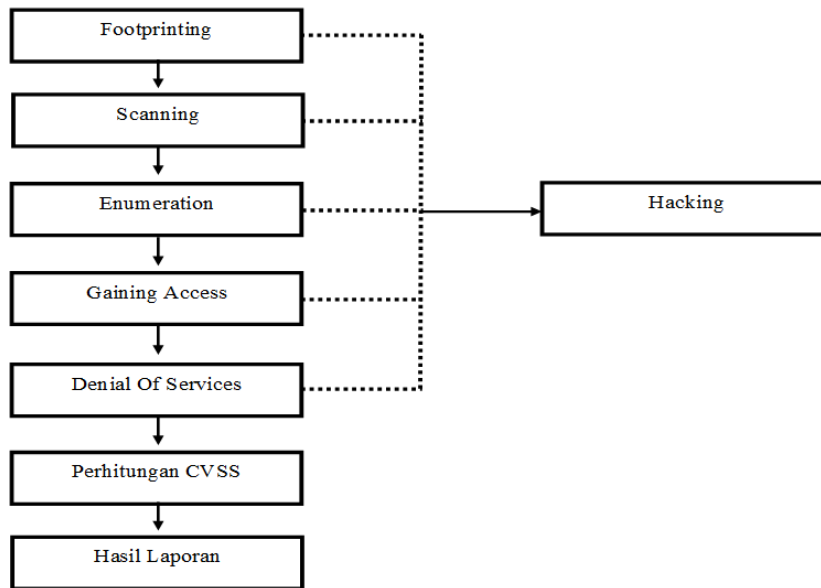
Tahap *enumeration* adalah mencari *poorly protected password*. Penulis mencoba menggali informasi berupa *username* dan *password* terlemah yang digunakan untuk akses kedalam sistem. Menggunakan aplikasi *xhydra* yang terdapat *Wordlist*. *Wordlist* merupakan kumpulan-kumpulan *username* dan *password* yang terdaftar dan bersifat umum digunakan pada penelitian ini penulis menggunakan *Rockyou.txt*.

Tahap *gaining access*, merupakan langkah untuk mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses target dan masuk kedalam sistem. Ketika sudah masuk dan diambil alih *hacker* dapat melihat data data yang ada pada file sistem yang terdapat di *telnet* atau bisa juga *monitoring* video secara langsung dari *drone* melalui *web browser*.

Denial of services merupakan jenis serangan ke sebuah sistem dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer atau sistem yang diserang tersebut. Pada penelitian ini tahapan *denial of services* yaitu menyerang *drone* dengan bertujuan untuk mengirim paket data yang banyak sehingga daya pada *drone* berkurang atau mengakibatkan *drone* hilang kendali. Pada tahapan ini penulis memakai aplikasi *mdk3* yang berbasis CLI (*command line interfaces*).

Perhitungan *CVSS (Common Vulnerability Scoring System)* adalah sebuah proses untuk menghitung celah kerentanan pada suatu sistem, dan dari perhitungan itu dihitung menggunakan rumus yang akan menghasilkan kesimpulan dari nilai kerentanan dan dampak dari eksploitasi. Pada penelitian ini penulis menggunakan perhitungan *CVSS calculator* versi 2 untuk menghitung celah kerentanan yang terdapat pada *drone*.

Hasil laporan, tahap ini merupakan tahap terakhir dimana kerentanan yang ditemukan dianalisa kemudian disajikan dalam bentuk laporan analisa keamanan *drone* menggunakan metode *hacking methodology*. Berikut diagram alur tahapan dari pengujian keamanan *drone* menggunakan *hacking methodology*.



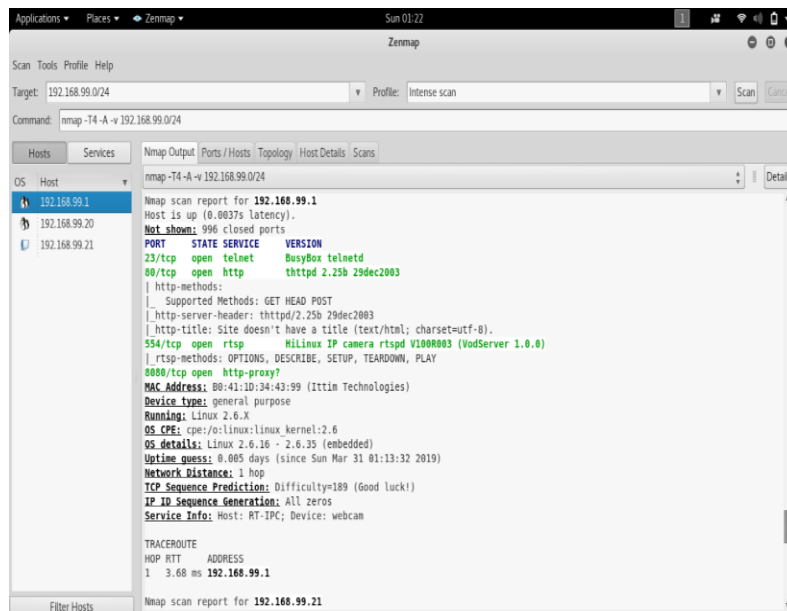
Sumber : Hasil Penelitian (2019)

Gambar 1. Diagram Alur Penelitian

3. Hasil dan Pembahasan

3.1. Tahap *Footprinting*

Tahap *footprinting* adalah proses menggali informasi sebanyak-banyaknya dari target (*drone*). Jika menggunakan aplikasi berbasis *web* seperti *whois*, penerapan *footprinting* juga menggunakan aplikasi lain atau bisa juga menggunakan seperti aplikasi *Zenmap*. Pada penelitian ini penulis menggunakan aplikasi *zenmap*. Tahap ini adalah yang pertama dalam pengujian penetrasi, intinya adalah mengumpulkan sebanyak mungkin informasi tentang target tentang *drone*, *IP address*, dan lain-lain. Tahapan *footprinting* dilakukan dengan menggunakan *tools Zenmap*. Proses untuk melakukan *footprinting* adalah dengan memasukkan alamat IP atau *IP address*.



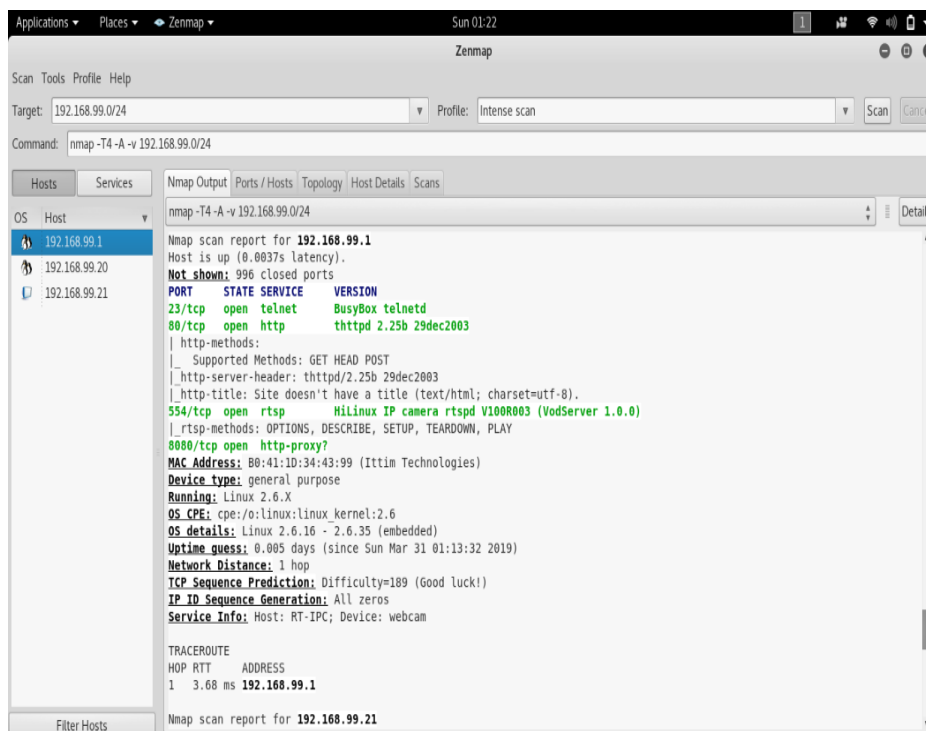
Sumber : Hasil Penelitian (2019)

Gambar 1. Hasil *Footprinting*

Dari hasil *footprinting* tersebut terlihat *mac address* yang dipakai oleh *drone*, sistem operasi yang digunakan, *services* apa yang berjalan, *detail log* aktif.

3.2. Tahap *scanning*

Tahap *scanning*, pada langkah ini *scanning* berfungsi untuk menentukan *host* mana yang tinggal di jaringan dan apa yang mereka lakukan, yang paling populer adalah *Nmap* dan *supercan*. Pemindaian dapat dengan mudah diambil oleh sistem deteksi, walaupun ada beberapa cara untuk menghindari hal ini dengan pemindaian spesifik. Terdapat identifikasi *service* apa saja yang berjalan di dalam *drone*. Pada tahap *scanning* ini meliputi analisis dan *scanning* terhadap *service* apa saja yang dijalankan pada sistem. Penulis juga menggunakan *Zenmap* untuk mengetahui informasi-informasi *port-port* yang terbuka atau tertutup dan mengetahui *service* yang tersedia pada *drone*. Melakukan tahapan *scanning* dengan menggunakan *tools Zenmap* dengan memasukkan *IP address* 192.168.99.0/24



Sumber :Hasil Penelitian (2019)

Gambar 2. Hasil *Scanning*

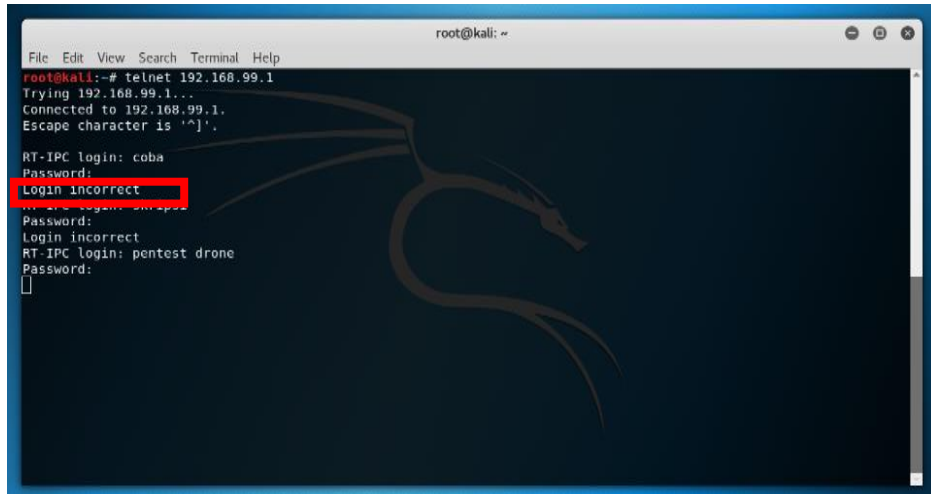
Hasil *scanning* pada pada gambar 2 menunjukkan jenis atau celah kerentanan yang ada pada *drone*, yaitu terdapat jenis celah-celah kerentanan. Beberapa jenis celah-celah kerentanan berdasarkan hasil *scanning* meliputi *port 23 telnet open*, *port 80 http open*, *port 554 rstp open*, *port 8080 http-proxy open*.

3.3. Tahap *Enumeration*

Tahap *enumeration* adalah mencari *poorly protected password*. Pada tahap ini hal yang dilakukan yaitu dengan mencoba menggali informasi berupa *username* dan *password* terlemah yang digunakan untuk akses kedalam sistem. Menggunakan aplikasi *xhydra* yang terdapat *Wordlist*. *Wordlist* merupakan kumpulan-kumpulan *username* dan *password* yang terdaftar dan bersifat umum digunakan pada penelitian ini penulis menggunakan *Rockyou.txt*.

Melakukan pengujian pada *telnet* yang terdapat pada *drone* dengan tahapan *Enumeration*. Berikut ini tampilan *telnet* ketika belum diketahui *login* dan *password*, untuk dapat mengetahui *login* dan *password* pada *telnet* ini harus dilakukan pengujian dengan menggunakan *tools xhydra*.

Dari hasil pengujian sebelumnya menunjukkan *hacker* memasukkan beberapa kata pada *menu login* dan *password* dan mencoba beberapa kali namun tidak berhasil masuk ke sistem, untuk dapat masuk dan mengetahui *login* dan *password telnet* maka harus dilakukan pengujian *hacking login* dan *password* dengan menggunakan *bruteforce* pada aplikasi *xhydra*.



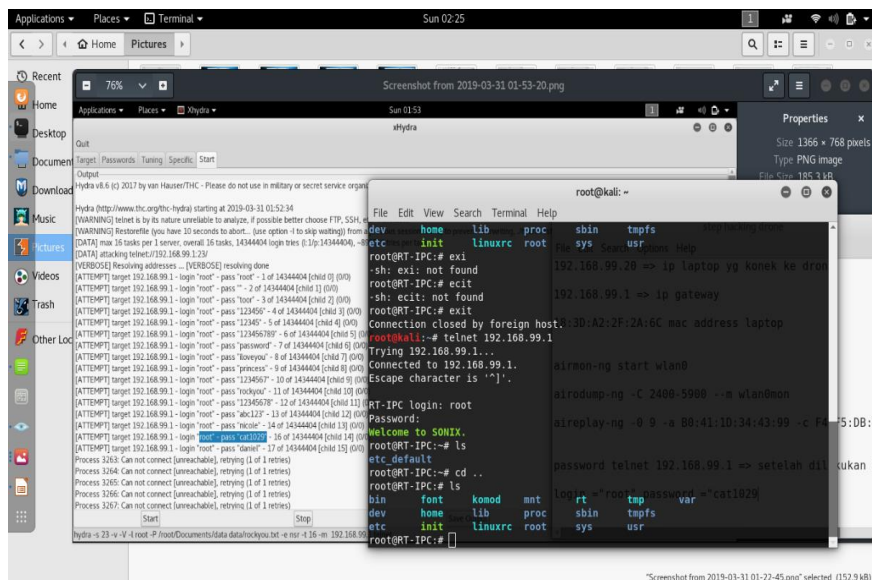
Sumber :Hasil Penelitian (2019)

Gambar.3 Tampilan Tidak Dapat Login

3.4. Tahap *Gaining Access*

Tahap *gaining access*, merupakan langkah untuk mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses target dan masuk ke dalam sistem. Ketika sudah masuk dan diambil alih *hacker* dapat melihat data data yang ada pada file sistem yang terdapat di *Telnet* atau bisa juga *monitoring* video secara langsung dari *drone* melalui *web browser*.

Ketika sudah mendapatkan informasi tentang *login* dan *password*, maka lakukan tahapan *Gaining access* dengan masuk ke *telnet* dengan masukan *command telnet* 192.168.99.1 dan *login* dengan ketik *login* "root" dan *password* "cat1029".



Sumber :Hasil Penelitian (2019)

Gambar 4. Berhasil Masuk Sistem Telnet

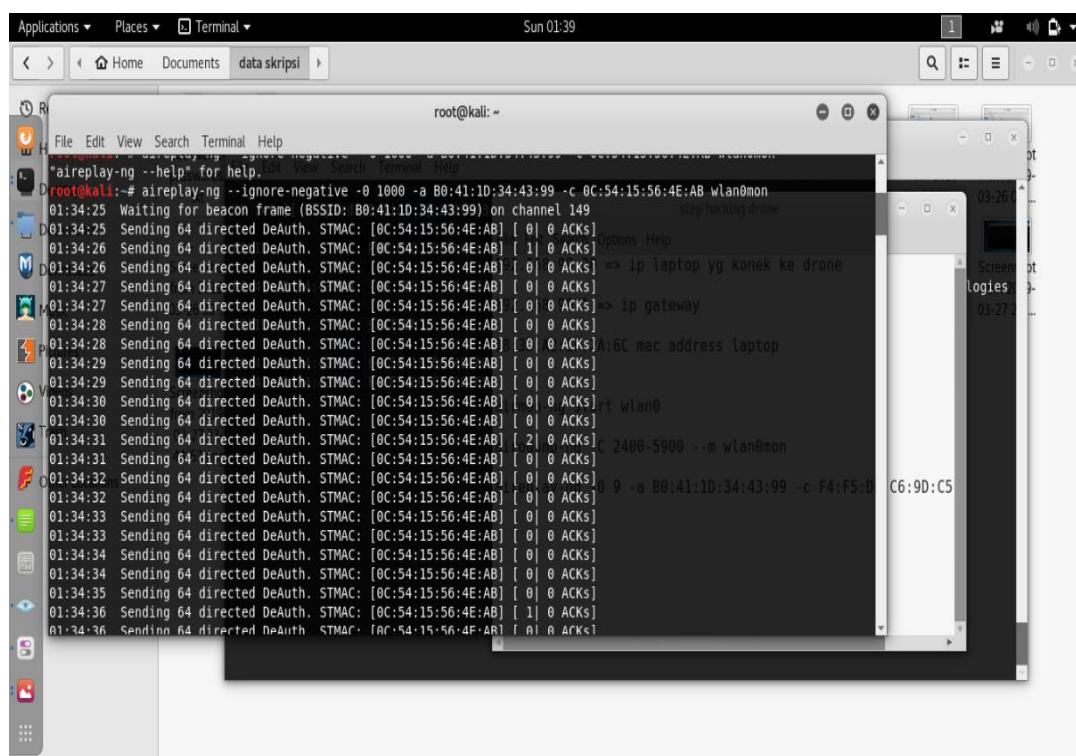
Pada gambar 4 dapat diketahui file atau data-data yang ada pada file sistem *telnet*, *hacker* dapat dengan mudah membaca isi file yang terdapat di dalamnya misalnya informasi *cpu* yang digunakan versi sistem yang digunakan, *firmware* dan lain-lain.

3.5. Tahapan *Denial Of Services*

Tahap *denial of services*, adalah jenis serangan terhadap sebuah komputer atau sistem dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer atau sistem yang diserang tersebut.

Pada penelitian ini tahapan *Denial of Services* (DoS) yaitu menyerang *drone* dengan bertujuan untuk mengirim paket data yang banyak sehingga daya pada *drone* berkurang atau mengakibatkan *drone* hilang kendali. Pada tahapan ini penulis memakai aplikasi *mdk3* yang berbasis CLI (*command line interfaces*).

Melakukan pengujian dengan tahapan *Denial of services*, lalu lakukan pengujian dengan *DoS* dengan menggunakan *command Aireplay-ng --ignore-negative -o 1000 -a B0:41:1D:34:43:99 -c 0C:54:15:56:4E:AB wlan0mon*.



```

root@kali:~# aireplay-ng --help for help.
root@kali:~# aireplay-ng --ignore-negative -o 1000 -a B0:41:1D:34:43:99 -c 0C:54:15:56:4E:AB wlan0mon
01:34:25 Waiting for beacon frame (BSSID: B0:41:1D:34:43:99) on channel 149
01:34:25 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:26 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [1] 0 ACKS
01:34:26 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:27 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:27 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:28 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:28 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:29 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:29 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:30 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:30 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:31 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [2] 0 ACKS
01:34:31 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:32 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:32 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:33 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:33 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:34 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:34 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:35 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS
01:34:36 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [1] 0 ACKS
01:34:36 Sending 64 directed DeAuth. STMAC: [0C:54:15:56:4E:AB] [0] 0 ACKS

```

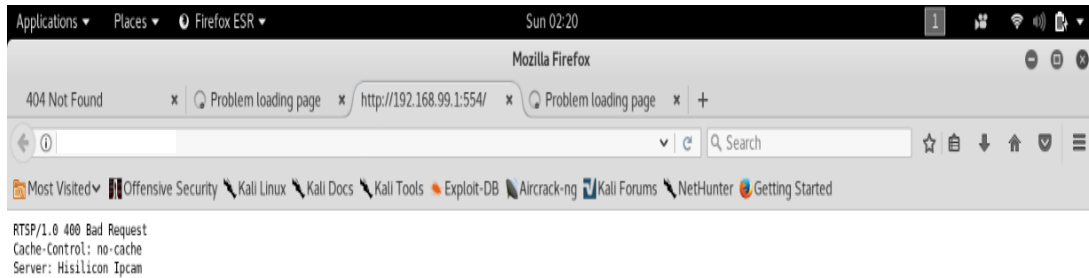
Sumber :Hasil Penelitian (2019)

Gambar 5. Hasil Serangan *DoS*

Dari hasil pada gambar 5 teknik *DOS* bertujuan untuk mengirimkan *packet* ke alamat *mac address drone* yang bertujuan untuk mengurangi *resources* dari sistem yang terdapat pada *drone* atau membuat *drone* menjadi tidak stabil.

3.6. Pengujian *Port Real Time Streaming Protocol*

Setelah itu lakukan pengujian pada *port Real Time Streaming Protocol* (*RTSP*) dengan memasukan alamat IP atau *IP address* di *browser*.



Sumber :Hasil Penelitian (2019)

Gambar 6. Hasil pengujian RTSP

Dari hasil pengujian pada gambar 6 tersebut dapat diketahui bahwa *services RTSP* yang ada pada *web server* tidak dapat muncul dalam *web browser*. Namun terdapat celah kerentanan *port RTSP* itu dapat di *sniffing* atau *monitoring* oleh *hacker* dengan itu maka harus dilakukan pengujian terhadap *port RTSP*.

3.7. Pengujian Dengan Deauth / Aireplay

Lakukan *deauth* pada target (*drone*) yang bertujuan untuk memutus koneksi *handphone user* agar tidak bisa terhubung ke *wireless drone*.

```
root@kali:~# aireplay-ng -0 9 -a B0:41:1D:34:43:99 -c F4:F5:DB:C6:9D:C5 wlan0mon01:31:34 Wa
iting for beacon frame (BSSID: B0:41:1D:34:43:99) on channel 149
01:31:34 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 1| 0 ACKs]
01:31:35 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 0| 0 ACKs]
01:31:35 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 0| 0 ACKs]
01:31:36 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 0| 0 ACKs]
01:31:36 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 0| 0 ACKs]
01:31:37 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 0| 0 ACKs]
01:31:37 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 0| 0 ACKs]
01:31:38 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 5| 0 ACKs]
01:31:39 Sending 64 directed DeAuth. STMAC: [F4:F5:DB:C6:9D:C5] [ 4| 4 ACKs]
root@kali:~#
```

Sumber :Hasil Penelitian (2019)

Gambar 7. Hasil deauth atau aireplay

Tujuan dari adanya proses *deauth* atau *aireplay* tersebut yaitu untuk mengirim paket data yang dapat mengakibatkan *user* atau target agar tidak dapat terhubung ke *wireless* pada *drone*.

3.8. Perhitungan Dengan CVSS Calculator Version 2

Perhitungan kerentanan pada pengujian saat ini dilakukan dengan memakai *tools* yang berbasis *web* yaitu dengan menggunakan *tools Common Vulnerability Scoring System (CVSS) Calculator Version 2*.

Common Vulnerability Scoring System versi 2 juga telah menetapkan skala penilaian berdasarkan nilai yang diperoleh dari perhitungan CVSS. Terdapat tiga kategori untuk status celah kerentanan, yaitu *low*, *mdedium* dan *high*. Tabel 1 menunjukkan dasar kategori kerentanan berdasarkan skala nilai yang diperoleh.

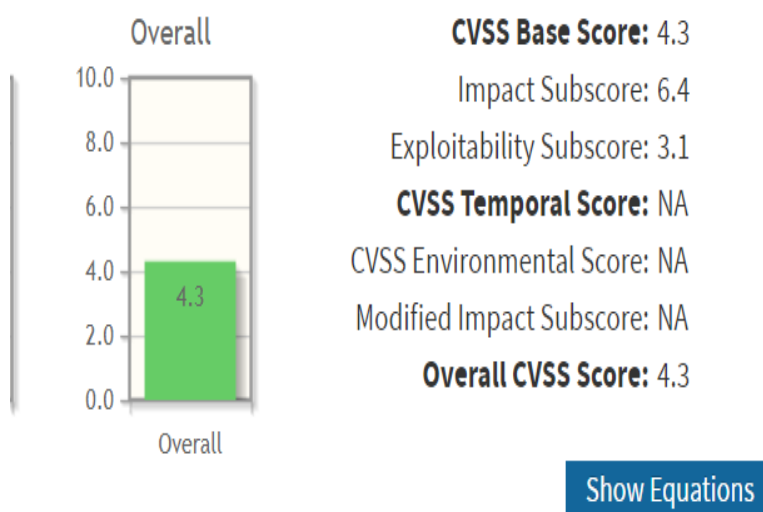
Tabel 1. NVD Vulnerability Severity Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

Sumber: National Vulnerability Database (2019)

Dari hasil perhitungan menggunakan CVSS akan diketahui celah kerentanan yang terdapat pada *drone* melalui jaringan *local* atau dalam satu jaringan hal itu sangat rentan untuk di *hack*, dan terdapat kemudahan dalam kerumitan akses dan dari indikator yang dipilih yaitu sangat mudah, dan terdapat juga celah kerentanan pada keamanan *root access* pada sistem *telnet*, terdapat celah kerentanan dari *port* atau *services* yang terbuka seperti *HTTP*, *RTSP*, *telnet*.

Berikut adalah tampilan dari hasil perhitungan secara keseluruhan dengan menggunakan perhitungan *CVSS Calculator version 2*.



Sumber :Hasil Penelitian (2019)

Gambar 9. Hasil Perhitungan CVSS

Dari hasil perhitungan kerentanan dengan menggunakan *tools CVSS Calculator version 2* dapat diketahui hasilnya yaitu *CVSS Base Score* dengan nilai 4.3, *impact subscore* dengan nilai 6.4 dan *exploitability subscore* dengan nilai 3.1.

Berdasarkan tabel 1 menunjukkan bahwa kerentanan yang terjadi pada *drone* masuk ke dalam kategori *medium* berdasarkan hasil perhitungan *base score* yang diperoleh 4.3.

3.9. Keamanan Yang Digunakan

Keamanan yang digunakan pada *drone* ini meliputi data video dan gambar yang tersembunyi didalam *telnet*, fungsi *remote* atau mengendalikan hanya bisa di *control* pada *controller* yang ada pada *remote controller*, tidak dapat di *control* melalui *handphone* , disaat menguji dengan memasukan *IP address* 192.168.99.1 :80 menggunakan *web browser* melalui *port* atau *services http* tidak dapat masuk ke *web server*, ketika menguji menggunakan *web server* dengan memasukan *IP address* 192.168.99.1 :23 *port* atau *services telnet* tidak dapat masuk kedalam *web server* yang ada pada *drone*.

3.10. Perbandingan Dari Hasil Penelitian

Sebelum dilakukannya pengujian terhadap *drone* maka belum dapat diketahui celah kerentanan yang ada pada *drone*, dan setelah dilakukannya pengujian dengan menggunakan *Hacking Methodology* maka dapat diketahui celah kerentanan yang ada pada *drone*.

Tabel 1. Perbandingan Dari Hasil Penelitian

No	Aspek Yang di uji	Sebelum Diuji	Setelah Diuji	Hasil Yang Diharapkan	Hasil Pengujian
1	<i>Drone</i>	Tidak diketahui celah kerentanan	Dapat diketahui celah kerentanan	Dapat dieksploitasi	Berhasil
2	<i>Telnet</i>	Tidak diketahui aman atau tidak	<i>Port</i> terbuka	Dapat masuk ke sistem	Berhasil
3	<i>RTSP</i>	Tidak diketahui celah kerentanan	<i>Port</i> terbuka	Dapat di <i>sniffing</i>	Berhasil
4	<i>HTTP</i>	Tidak diketahui celah kerentanan	<i>Port</i> terbuka	Dapat masuk ke <i>webserver</i>	Tidak Berhasil

Sumber : Hasil Penelitian (2019)

3.11 Hasil Akhir Perbandingan

Berdasarkan dari hasil akhir perbandingan pengujian yang berdasarkan dari perbandingan hasil penelitian maka dapat diketahui, *drone* setelah di uji dapat diketahui celah kerentanan yang ada pada *drone* terdapat celah kerentanan seperti *port 23 (TELNET)*, *80 (HTTP)*, *554 (RTSP)*. Dari adanya celah kerentanan pada *telnet* maka file sistem dapat masuk ke sistem dan melakukan eksploitasi. Dan dari adanya celah kerentanan pada *HTTP* hal ini dapat menyebabkan *login user* dan *password* dapat di *hack* dengan menggunakan teknik *bruteforce*, namun pada penelitian ini file sistem tidak ada di dalam *webserver* pada *services HTTP*. Dari celah yang terdapat pada *RTSP* maka *drone* dapat di *sniffing* oleh *hacker*.

4. Kesimpulan

Berdasarkan hasil pengamatan dan penelitian dalam pengujian keamanan *drone* menggunakan *hacking methodology* maka dapat diambil kesimpulan sebagai berikut: 1) Dari adanya pengujian dengan tahapan *Footprinting, Scanning Enumeration, Gaining access, Denial of services*, maka hasil dari celah kerentanan pada *drone* dapat diketahui. Terdapat celah kerentanan yang dapat dieksploitasi seperti pada *Telnet, RTSP, HTTP*. Celah-celah nya yaitu *hacker* dapat masuk ke sistem dan dapat melakukan eksploitasi, *drone* dapat di *sniffing*, *drone* dapat diserang dengan serangan *DoS*. 2) Mengetahui hasil pengujian eksploitasi pada *drone* dari adanya pengujian dengan mengambil alih *drone* dan data data yang terdapat pada *drone port Telnet, RTSP, HTTP* dengan menggunakan tahapan *Hacking Methodology*. 3) Mengetahui nilai resiko dari celah kerentanan pada *drone* yang dapat diketahui dengan perhitungan CVSS. Hasil perhitungan pada *drone* secara keseluruhan dengan menggunakan CVSS yaitu dengan nilai 4.3.

Referensi

- Angir, D. C., Noertjahyana, A., & Andjarwirawan, J. 2015. Vulnerability Mapping Pada Jaringan Komputer Di Universitas X. *Jurnal Infra*, 3(2), Pp.44-P.50.
- Attila, H., Kiss, F., & Erdosi, P. M. 2016. The Common Vulnerability Scoring System (CVSS) Generations – Usefulness And Deficiencies, (January), 137–154.
- Giffari, M., Pradana, A., Prasakti, R., Worsito, S. B., & Fajaryati, N. 2016. Single Propeller Drone (Singrone): Inovasi Rancang Bangun Drone Single Propeller Sebagai Wahana Pemetaan Lahan Berbasis Unmanned Aerial Vehicle (UAV).
- Harihanto, Riska, & Nurmanina, A. (2013). Informan Perempuan Lebih Dominan Mengakses Internet Setiap Hari Dengan Waktu Sekitar 2 - 3 Jam Dalam Sehari , Sedangkan Informan Laki-Laki Cenderung Jarang Mengakses Internet Dengan Waktu 1 Jam . *Sociology*, 1(4), 37–49.
- Humphreys, E. (2017). Information Security Risk Management (Isri) | Rapid7. Rapid7.
- Jamaludin. (2016). Teknik Keamanan Jaringan Wireless Lan Pada Parnet Salsabila Computer Net. *Jurnal & Penelitian Teknik Informatika*, 1(1), 67–74.
- Juliharta, I. G. P. K. (2015). Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing. *Jurnal Sistem Dan Informatika*, 10(1), 149–158.
- Kaur, M. G. (2017). Penetration Testing – Reconnaissance With Nmap Tool, 8(3), 844–846.