Journal of Technology and Informatics (JoTI)
Vol 1, No.1, Oktober Tahun 2019
E-ISSN 2686-6102

Upaya Penetrasi dengan Enumeration menggunakan Hydra

Andre Arta Kurniawan[1] **Yahya Nugroho** [2]
Program Studi/Jurusan Teknik Komputer, Institut Bisnis dan Informatika Stikom Surabaya,
Email: [1]andrearta1@gmail.com, [2]yahya.nvf31@gmail.com

Abstrak: Internet di jaman sekarang sudah dapat dikatakan sebagai menjadi suatu kebutuhan untuk beberapa orang yang bergerak dalam teknologi internet. Namun di sisi lain ancaman terhadap internet juga akan semakin terus bertambah. Salah satu kejahatan yang ada pada internet adalah *cyber-crime* atau kejahatan internet dan kejahatan internet juga dapat dilakukan oleh siapa saja salah satunya *hacker.* Apabila seorang *hacker* berhasil meretas sebuah jaringan atau *server* maka tak diragukan lagi *hacker* tersebut dapat mengakses seluruh jaringan dan menggunakan setiap data yang ada, maka dari itu diperlukan seorang *network administrator* yang handal dalam menangani sebuah jaringan atau sebuah *server.* Pada jurnal ini mengamati langkah yang dilakukan oleh *Attacker* mendapatkan akses ke *user* menggunakan *tools hydra* , lama *cracking password user* membutuhkan rata-rata waktu sekitar 4 jam.

Kata Kunci: *cyber-crime, hacker, cracking password,enumeration, hydra*

Abstract: Today's internet can be said to be a necessity for some people who are engaged in internet technology. But on the other hand the threat to the internet will also continue to grow. One of the crimes that are on the internet is cyber-crime or internet-crime and internet-crime can also be done by anyone, one of them is a hacker. If a hacker succeeds in hacking a network or server then the hacker is undoubtedly able to access the entire network and use every available data, therefore a reliable network administrator is required to handle a network or a server. In this journal observing the steps taken by the Attacker gain access to the user using the hydra tools. In this journal observing the steps taken by the Attacker to gain access to the user using the Hydra tools, the length of cracking the user password requires an average of about 4 hours.

Keywords: *cyber-crime, hacker, cracking password,enumeration, hydra*

PENDAHULUAN

Di era teknologi internet yang sudah sangat maju ini memang sangat penting dibutuhkannya sebuah keamanan dalam sebuah jaringan, karena mengingat seiring majunya teknologi internet jumlah *cyber-crime* juga akan terus meningkat. Sebuah jaringan akan memerlukan *network administrator* yang handal dalam menangani sebuah jaringan, terutama dalam urusan keamanan jaringan. *Network administrator* harus bisa mengatasi apabila suatu waktu jaringan yang dikontrolnya mengalami serangan *hacker.* Tujuan dari keamanan komputer sendiri adalah melindungi informasi komputer yang berada di dalamnya. [1]

Sebuah jaringan tanpa kemanan pun juga sangat berbahaya apabila jaringan tersebut setiap harinya diakses dan digunakan. Terlebih para *hacker* akan dengan mudah masuk kedalam jaringan dan menyerang sebuah server. Dengan tidak adanya keamannya pada sistem maka akan banyak para *Hacker* yang dengan mudah dapat mengambil alih sistem yang dibangun. [2] Ada berbagai jenis macam serangan yang dapat dilakukan oleh para *hacker* yang dapat digunakan untuk menyerang sebuah server, salah satunya dengan *penetration.* Dengan melakukan *penetration, hacker* akan berusaha masuk melalui celah keamanan yang terbuka dari server tersebut. Dan apabila *hacker* berhasil masuk ke

dalam server dan mendapatkan akses penuh terhadap server maka bukan tidak mungkin lagi *hacker* dapat dengan mudah dapat mengakses setiap data yang terdapat di dalam server tersebut. Kebocoran data dan informasi merupakan hal yang fatal. Data-data tersebut dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. [3]

Namun, bagi sebagian orang bekerja untuk sebuah jaringan atau *network administrator*, mereka akan melakukan sendiri *penetration* ke dalam jaringan mereka sendiri sehingga kegiatan tersebut disebut dengan *penetration testing.*

Pada jurnal ini, upaya penetrasi dilakukan dengan cara menyelundup ke *user* akses terlebih dahulu, dengan cara enumeration. Enumeration merupakan salah satu usaha dari attacker untuk mendapatkan hak ases dengan mencoba berbagai kemungkinan *password* dari generator hash. Enumeration dapat dilakukan dengan menggunakan beberapa tolos yang opensource seperti hydra, medusa, dan John The Ripper. Jurnal ini menerapkan tools hydra untuk men-*cracking* password.

METODOLOGI PENETRATION

Teknik *Penetration*

Dalam melakukan *penetration* seorang *network administrator* harus melakukan beberapa tahapan untuk kemudian menganalisa apakah *server* tersebut masih memiliki celah keamanan atau tidak. Jika masih ditemukan celah kemanan maka *server* tersebut masih diperlukan solusi untuk memperbaiki celah kemanan. Keamanan jaringan ini dapat bertujuan untuk agar pemilik sistem informasi dapat menjaga sistem informasinya tidak ditembus atau disusupi oleh orang lain yang pada akhirnya dapat merusak sistem. [4] Untuk menerapkan teknologi yang aman perlu adanya perancangan sebuah sistem keamanan jaringan yang bagus. [5]

Tujuan lain dalam melakukan *penetration* adalah menentukan dan mengetahui kemungkinan – kemungkinan yang dapat terjadi apabila seorang *hacker* melakukan serangan terhadap *server*, serta dampak yang dihasilkan dari hasil eksploitasi *server* yang dilakukan oleh *hacker.*

Adapun tahapan yang harus dilakukan untuk melakukan *penetration* adalah sebagai berikut :

1. *Footprinting* = umunya digunakan untuk mengumpulkan informasi sebanyak mungkin mengenai target yang akan diserang baik itu *server* maupun jaringan yang akan diserang. Dengan melakukan *footprinting*, *attacker* akan berusaha untuk mendapatkan informasi sebanyak mungkin mengenai target yang akan diserang, mulai dari *IP Addresses*, *name server*, hingga informasi mengenai *server*.
2. *Scanning* = dengan melakukan *scanning*, *attacker* akan mengumpulkan *port list* yang terbuka. Dari *port list* yang terbuka, *attacker* akan mengetahui dari mana *attacker* bisa menyerang
3. *Enumeration* = dengan melakukan *enumeration*, *attacker* akan mencari *user account* yang aktif atau *valid* dari target. Dengan memanfaatkan *user* ini *attacker* akan mencoba masuk kedalam *server*.
   Enumeration merupakan salah satu cara oleh *attacker* untuk mendapatkan informasi mengenai *username*, nama mesin, dan *resource* jaringan.
   Salah satu *tools* yang bisa digunakan untuk melakukan *enumeration* ini adalah dengan menggunakan medusa, hydra, john the ripper, dan lain-lain. Pada jurnal ini, penerapannya menggunakan *tools hydra* pada linux.
   - Hydra merupakan salah tools yang disedikan oleh Kali Linux, untuk men-*cracking* password sesuai dengan *wordlist user* dan *password* . Beberapa contoh 10.000 *wordlist* dari *password* disajikan pada tabel berikut,

Tabel 1 *Wordlist* dari *Generate Pasword*

No	Password
1	A1!%1
2	A%AA1
3	A%AzA
4	AA%1z@

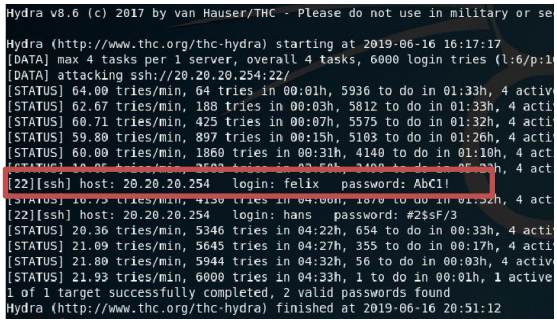
Tabel 2 *Wordlist* dari *User*

No	User.lst	Nama user
1	User 1	felix
2	User 2	bukcy
3	User 3	james

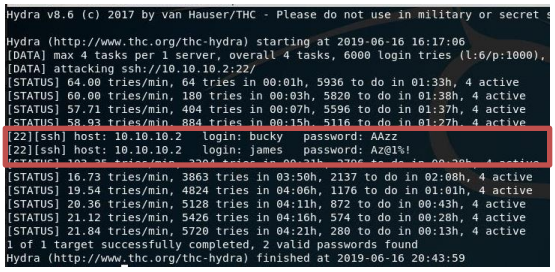
Sintak yang digunakan pada hydra sebagai berikut :

```
hydra -L /root/JoTi/user.lst
-P /root/JoTi/password.lst
10.10.10.2 -t 4 ssh -->>
SSH-server
hydra -L /root/JoTi/user.lst
-P /root/JoTi/password.lst
20.20.20.253 -t 4 ssh -->>
user1
hydra -L /root/JoTi/user.lst
-P /root/JoTi/password.lst
20.20.20.254 -t 4 ssh -->>
user2
```

dari sintak tersebut terlihat kemungkinan *password* yang cocok dari user tersebut. Cepat tidaknya kinerja dari hydra tergantung dari spek *resource* yang digunakan oleh Attacker dan kompleksitas dari *password*.



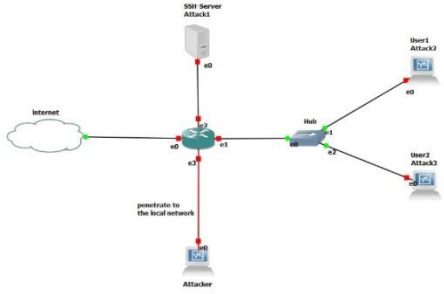
Gambar 1 Enumeration User : felix dengan Hydra



Gambar 2 Enumeration User bucky dan james dengan hydra

4. *Gaining Access* = Setelah data – data yang diperlukan telah terkumpul, *attacker* akan mencoba untuk masuk ke dalam *server* atau mengakses *server* tersebut
5. *Privilege Escalation* = Dengan *user* – *user* yang ada, *attacker* akan mencoba masuk ke dalam *server*. Jika terdapat *user* yang dapat digunakan masuk ke dalam *server*, maka selanjutnya *attacker* akan mencoba untuk mendapatkan *full-access* terhadap *server* tersebut.
6. *Covering Tracks* = Setelah mendapatkan *full-access* terhadap *server* maka selanjutnya *attacker* akan menghapus *logs* yang ada agar tidak dicurigai.
7. *Backdooring* = Terakhir, *attacker* akan mencoba untuk membuat *user* baru dengan tujuan ketika *attacker* akan mengakses kembali *server* tersebut *attacker* akan masuk dengan *user* yang telah dibuatnya.
8. *Denial* of *Service* = Atau yang lebih sering dikenal dengan *DoS attack*, serangan ini juga merupakan serangkaian dari *penteration attack*, dimana ketika seorang *attacker* gagal menyerang maka *attacker* akan melakukan Teknik *DoS attack*.

HASIL DAN PEMBAHASAN



Gambar 3. Topologi yang digunakan untuk *penetration*

Dari ilustrasi Gambar 3. Rancangan topologi yang digunakan. Pada topologi jaringan, *Attacker* akan mencoba melakukan *penetration* dari dalam jaringan langsung atau jaringan lokal. Nantinya *attacker* akan mencoba untuk *cracking password* dari *user* dan SSH-*Server* yang terdapat pada jaringan tersebut.

Pada hasil percobaan *cracking password*, *password* yang digunakan terdiri atas berbagai macam kombinasi *password* hingga panjang karakter yang digunakan.

Attacker pada percobaan menggunakan sistem operasi Kali Linux v2019.2 dan *tools* yang digunakan untuk melakukan *cracking password* adalah menggunakan *hydra.*

Tabel 3. Lama Waktu *Cracking Password*

	Password	Mulai	Akhir	Lama
User 1	AAzz Az@1%!	16:17:06	20:43:59	04:26:53
User 2	AbC1! #2$sF/3	16:17:17	20:51:12	04:33:55
User 3	AA%!@A Aik@1%!!	16:17:13	20:57:06	04:39:53

Dari hasil tabel 3. *Password* yang digunakan adalah hasil *generate random passoword* dengan menggunakan *tools* yang ada pada *Kali Linux. Password* yang digunakan pun juga kombinasi antara panjang karakter yang digunakan dengan jenis karakter yang digunakan.

Lama waktu hasil percobaan adalah dari *attacker* melakukan *cracking password* ke setiap *user* dan SSH-*Server* pada jaringan tersebut. Dan dari hasil pada tabel 1. menunjukkan semakin panjang karakter dan jenis password yang digunakan beragam maka waktu yang diperlukan semakin lama.

KESIMPULAN DAN SARAN

Penetrasi yang dilakukan dengan cara enumeration, untuk mendapatkan *password* dari *user* bisa dilakukan dengan cara mencari kemungkinan kecocokan dari password dan *user* menggunakan hydra selama 4 jam. Hal ini tergantung dari kompleksitas dari *password* dan *resource* yang digunakan *attacker*.

DAFTAR PUSTAKA

[1] R. Pangalila, A. Noertjahyana y J. Andjarwirawan, Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra, *Jurnal Infra*, Vols. %1 de %2 Vol 3, No 2, 2015.

[2] Y. Yunanri , I. Riadi y A. Yudhana, «Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST), *Annual Research Seminar (ARS)*, Vols. %1 de %2Vol 2, No 1, 2016.

[3] M. Dahlan, A. Latubessy y M. Nurkamid, Analisa Keamanan Web Server Terhadap Serangan Possibility Sql Injection Studi Kasus: Web Server UMK, *Pros iding SNATIF*, 2015.

[4] D. C. Angir, A. Noertjahyana y J. Andjarwirawan, Vulnerability Mapping pada Jaringan Komputer di Universitas X, *Jurnal Infra*, Vols. %1 de %2Vol 3, No 2, 2015.

[5] A. Amarudin, Desain Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking, *Jurnal TEKNOINFO*, Vols. %1 de %2Vol. 12, No. 2, 2018.