BAB II

TINJAUAN PUSTAKA

Dalam proses pengerjaan penelitian ini, penulis mendapatkan beberapa referensi dari penelitian – penelitian terdahulu yang dapat membantu penulis menyelesaikan penelitian ini.

Pada penelitian yang dilakukan oleh Royan Firdaus (2020), beliau membuat sistem jaringan yang terdiri dari 3 PC, yang mana PC 1 sebagai web server, PC 2 sebagai honeypot server, dan PC 3 sebagai *attacker*. Beliau mensimulasikan serangan dari *attacker* berupa *port scanning* dan *hacking* menuju honeypot server yang dianggap *attacker* sebagai web server. Dalam proses simulasi tersebut, honeypot berhasil mencegah serangan melalui *port scanning* dan menampilkan log terkait dengan serangan yang terjadi. Dari penelitian beliau membuktikan bahwa honeypot dapat mencegah serangan *port scanning* sekaligus juga menampilkan log yang berisi informasi mengenai port mana yang diserang dan ip *address* dari *attacker* [5].

Selanjutnya pada penelitian yang dilakukan oleh Wahyu Adi Sulaksono dan Cosmas Eko Suharyanto (2020), beliau mengimplementasikan honeypot menggunakan cowrie pada sebuah server yang terletak di SMKN 5 Batam. Server tersebut divirtualisasikan menjadi virtual *private* server yang digunakan sebagai web server dan *cloud storage* oleh SMKN 5 Batam. Setelah mengimplementasikan honeypot, beliau melakukan pengujian penyerangan honeypot untuk mengetahui apakah honeypot telah terpasang dengan baik. Beliau melakukan serangan pada port 22 yang kemudian serangan tersebut berhasil digagalkan oleh honeypot. Hasil dari penelitian beliau bahwa honeypot pada server di SMKN 5 Batam telah berhasil diimplementasikan yang mana honeypot ini berguna untuk meningkatkan keamanan server dan juga menekan biaya pengeluaran karena honeypot sendiri bersifat *open source* [6].

Selanjutnya pada penelitian yang dilakukan oleh Rosi Dermawati dan M. Hasim Siregar (2020), beliau menggunakan honeypot *Dionaea* yang dipasang di labor jaringan Fakultas Teknik Universitas Islam Kuantan Singingi. Honeypot *Dionaea* yang telah terpasang ini akan memproses semua *traffic* yang masuk ke dalam sistem jaringan dan informasi *traffic* tersebut akan tersimpan dalam *database*. Beliau kemudian menguji honeypot *Dionaea* yang telah terpasang dengan mengirimkan *malware*. Honeypot *Dionaea* memproses *malware* tersebut yang berada dalam *traffic* yang masuk ke dalam sistem jaringan. Informasi *malware* tersebut kemudian dianalisis menggunakan *tools online* virustotal.com. Beliau mendapatkan hasil bahwa *malware* tersebut merupakan jenis worm yang memanfaatkan kerentanan dalam layanan Microsoft Windows Server. Dari hasil pengujian tersebut, honeypot *Dionaea* dapat digunakan untuk memantau *traffic* pada sistem jaringan dan penggunaan *tools online* seperti virustotal.com untuk menganalisis *malware* yang didapat dari honeypot *Dionaea*[7].

Selanjutnya pada penelitian yang dilakukan oleh Nur Fitriana dan Fata Nidaul Khasanah (2018), beliau menggunakan honeyd sebagai solusi dari keamanan jaringan *wireless*. beliau merancang sistem jaringan dimana *packet* data yang masuk akan melalui proses pengecekan. Setelah pengecekan, *packet* tersebut akan dibandingkan dengan *network traffic rules* yang beliau buat. Jika hasil dari pembandingan tersebut terdapat *alert*, maka *packet* akan dialihkan menuju honeyd dan jika tidak terdapat *alert*, maka *packet* akan diteruskan menuju server. Beliau melakukan pengujian terhadap honeyd yang telah diimplementasikan dengan melakukan serangan Dos *attack*, FTP *attack*, dan ICMP *attack*. Hasil dari serangan tersebut kemudian masuk ke dalam log honeyd dan beliau melakukan pengamatan bahwa rata – rata serangan FTP *attack* lebih cepat terdeteksi dalam waktu 2 detik kemudian DoS *attack* dalam waktu 2,33 detik dan terakhir ICMP *attack* dalam waktu 5 detik [8].

Selanjutnya pada penelitian yang dilakukan oleh Kurnia Elviani (2021), beliau melakukan implementasi honeyd pada jaringan *wireless* di Fakultas Teknik Universitas Islam Kuantan Singingi. Jaringan ini terdiri dari 1 *access point* yang

terhubung dengan ISP, PC client, PC penguji yang terhubung dengan *device* mikrotik pada Fakultas Teknik. Setelah melakukan implementasi honeyd pada jaringan Fakultas Teknik, beliau menguji jaringan tersebut dengan melakukan serangan berupa *port scanning*, TCP *flood*, dan HTTP *flood*. Hasil dari pengujian serangan tersebut membuktikan bahwa honeyd berhasil menghentikan serangan *attacker* dan menyimpan informasi serangan pada *file* log honeyd. Hasil analisis dari informasi yang terdapat pada file log honeyd dapat digunakan untuk meningkatkan keamanan jaringan [9].

Selanjutnya pada penelitian yang dilakukan oleh Rendyanto Adi Kurniawan, Rakhmadhany Primananda (2023), beliau mengimplementasikan honeyd dan virtual server openstack pada linux Ubuntu 18.04 yang dijalankan melalui VirtualBox. Lalu terdapat PC *attacker* yang disambungkan melalui *access point* menuju server honeyd dan server OpenStack. Setelah itu, beliau mensimulasikan serangan DoS menuju honeyd yang nantinya hasil serangan tersebut dianalisis menggunakan algoritma K-Means. Algoritma ini akan mengelompokkan hasil serangan DoS menjadi tiga level serangan yaitu *low*, *medium*, *high* dengan menggunakan parameter kerapatan waktu dan ukuran paket. Hasil yang didapat beliau bahwa honeyd dapat mencegah serangan DoS dan menyimpan informasi serangan sehingga dapat dianalisis menggunakan algoritma K-Means [10].

Selanjutnya pada penelitian yang dilakukan oleh Fakhrul Efendi, Devie Ryana Suchendra, Setia Juli Irzal Ismail (2023), beliau merancang jaringan yang terdiri dari *database*, web server berbasis html dan php, dan honeypot *snare tanner* sebagai *detector* serangan yang dijalankan melalui VMWare. Setelah itu beliau mulai melakukan implementasi honeypot *snare tanner*, Postgresql, PHP, dan Docker pada jaringan yang telah dibuat. Setelah implementasi, beliau melakukan pengujian jaringan yang dibuat dengan melakukan serangan SQL *injection*, XSS *attack*, dan *Password Brute Force attack*. Dari pengujian tersebut didapatkan hasil bahwa seluruh serangan yang dilakukan dapat terdeteksi oleh honeypot dan

kombinasi *user password* dari serangan *Password Brute Force attack* dapat terekam oleh honeypot [11].

Selanjutnya pada penelitian yang dilakukan oleh Nur Rohman Rosyid, Budi Bayu Murti, Brama Prayudha, Arul Ferian Ramadloni, Lukman Subekti (2022), beliau mengimplementasikan honeypot dan Yara pada jaringan lokal beliau. Topologi yang ada pada jaringan lokal beliau terdiri dari jaringan honeypot, MQTT broker, server proaktif, dan jaringan lokal (LAN). Jaringan honeypot akan memindai setiap *packet* yang masuk menuju honeypot untuk dibandingan dengan hash *malware* yang ada pada folder /binaries honeypot. Jika hasilnya *packet* tersebut merupakan *malware* maka informasi serangan *malware* tersebut akan disimpan dalam *database* MongoDB. *Packet* yang berisi *malware* akan diteruskan menuju server proaktif dan diproses oleh Yara untuk mengidentifikasikan jenis *malware* tersebut. Hasil dari penelitian beliau bahwa honeypot dapat dikombinasikan dengan Yara sebagai mekanisme keamanan proaktif yang mana honeypot berfungsi untuk mencegah *malware* dan menyimpan informasi serangan *malware* tersebut dan Yara akan memindai spesifikasi dari *malware* [12].

Tabel 2. 1 Tabel Perbandingan Penelitian Terdahulu

Nama Peneliti	Royan Firdaus	Wahyu Adi Sulaksono dan Cosmas Eko Suharyanto	Rosi Dermawati dan M. Hasim Siregar
Judul	ANALISIS DAN IMPLEMENTASI HIGH INTERACTION HONEYPOT PADA SERVER	IMPLEMENTASI HONEYPOT SEBAGAI SISTEM KEAMANAN JARINGAN PADA VIRTUAL PRIVATE SERVER	IMPLEMENTASI HONEYPOT PADA JARINGAN INTERNET LABOR FAKULTAS TEKNIK UNIKS MENGGUNAKAN DIONAEA SEBAGAI KEAMANAN JARINGAN
Implementasi	Jaringan Lokal (LAN)	Virtual Private Server SMKN 5 Batam	Jaringan Internet Labor Fakultas Teknik UNIKS
Honeypot	PenTBox Honeypot	Honeypot Cowrie	Honeypot Dionaea
Uji Serangan	Port Scanning menggunakan Nmap	Port 22 *login attack* menggunakan putty	Malware *attack* (*Computer Worm*)

Nama Peneliti	Nur Fitriana dan Fata Nidaul Khasanah	Kurnia Elviani	Rendyanto Adi Kurniawan, Rakhmadhany Primananda
Judul	HONEYPOT MENGGUNAKAN HONEYD SEBAGAI SOLUSI KEAMANAN JARINGAN DARI AKTIVITAS SERANGAN	ANALISA DAN IMPLEMENTASI HONEYPOT HONEYD PADA JARINGAN WIRELESS DI FAKULTAS TEKNIK UNIVERSITAS ISLAM KUANTAN SINGINGI	PENGELOMPOKKAN SERANGAN DOS PADA HONEYPOT MENGGUNAKAN ALGORITMA K-MEANS
Implementasi	Jaringan Lokal (LAN)	Jaringan Wireless Fakultas Teknik UNIKS	Jaringan Lokal (LAN)
Honeypot	Honeypot Honeyd	Honeypot Honeyd	Honeypot Honeyd
Uji Serangan	DoS *attack*, FTP *attack*, ICMP *attack*	*Scanning port* menggunakan Net Scan, TCP *flood* dan HTTP *flood* menggunakan LOIC	DoS *attack* menggunakan LOIC

Nama Peneliti	Fakhrul Efendi, Devie Ryana Suchendra, Setia Juli Irzal Ismail	Nur Rohman Rosyid, Budi Bayu Murti, Brama Prayudha, Arul Ferian Ramadloni, Lukman Subekti
Judul	PENERAPAN KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT SNARE & TANNER BERBASIS WEB SECARA LOW INTERACTION PADA LAYANAN WEB SERVER	DETEKSI MALWARE PADA JARINGAN LOKAL BERBASIS HONEYPOT DAN YARA
Implementasi	Jaringan Lokal (LAN)	Jaringan Lokal (LAN)
Honeypot	Honeypot Snare & Tanner	Honeypot Dionaea
Uji Serangan	SQL *injection*, XSS *attack*, *Password Brute Force attack*	Malware *attack*