JURNAL FASILKOM ISSN: 2089-3353
Volume 10 No. 2 | Agustus 2020: 159-165

IMPLEMENTASI KEAMANAN JARINGAN DENGAN IPTABLES SEBAGAI FIREWALL MENGGUNAKAN METODE PORT KNOCKING

Januar Al Amien[1)]
[1]Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau
email: januaralamien@umri.ac.id

Abstrak

From the research results is necessary to to protect by closing all the information open ports on a server and give access to ports and services open only to certain users, and to give access in the form of authentication, while not authorized could not access information about the port itself. Then there is one method that can close the Port Knocking all the information about the port using iptables applications and give access rights in the form of a combination of beats that have been determined. the server will overwrite the firewall rules with new rules made under iptables configuration, and immediately open the destination port, and the client access to port of destination. This method has been successful in doing testing and may have been applied to the server by using the operating system Linux Debian 7.3 Wheezy server, the port opened port22 SSH (Secure Shell).

Keywords: *Network Security, Port Knocking, Firewall, Iptable, close port, port*

Abstract

Dari hasil penelitian Perlu adanya untuk melindungi dengan menutup semua informasi port yang terbuka pada server dan memberikan akses untuk membuka port dan layanan hanya untuk pengguna tertentu, dan memberi akses masuk berupa otentifikasi, sementara yang tidak diberi kewenangan tidak dapat mengakses informasi port itu sendiri. Maka ada satu metode Port Knocking yang bisa menutup semua informasi port dengan menggunakan Aplikasi Iptables dan memberikan hak akses berupa kombinasi ketukan yang sudah di tentukan. server akan meng-overwrite aturan firewall dengan aturan baru yang dibuat berdasarkan konfigurasi IPtables, Dan langsung membuka port tujuan, dan client dapat mengakses port tujuan. Metode ini telah berhasil di lakukan pengujian dan dapat sudah diterapkan pada server dengan menggunkan sistem operasi Debian server Wheezy 7.3 Linux, Dengan port yang di buka port22 SSH(Secure Shell).

Keywords: *Network Security, Port Knocking, Firewall, Iptable, port*

PENDAHULUAN

Port komunikasi adalah port dalam protokol TCP atau UDP (Kumar and Rai, 2012) yang merupakan anggota dari lapisan Transport dalam standar OSI (Gangane, Kakade and Professor, 2014) (Saxena, 2013). Di dalam firewall semua komunikasi masuk dan keluar terkendali. Port yang tidak penting dapat diblokir (ditutup) dan port penting dan berbahaya juga diblokir, misalnya, untuk terhubung ke Internet dan perlu mengakses server web melalui SSH untuk memperbaiki konfigurasi, sedangkan port SSH pada server dilarang menjadi dapat diakses di internet dengan firewall, tentunya hal tersebut akan sangat mengganggu. Port knocking adalah metode untuk menjalin komunikasi antar komputer dari manapun selama masing-masing komputer terhubung dalam suatu jaringan komputer (Babatunde and Al-Debagy, 2014), dengan komputer manapun yang tidak membuka port komunikasi apapun secara bebas, tetapi perangkat tersebut tetap dapat diakses dari luar, menggunakan format konfigurasi port knock (Pourvahab and Atani, 2018).

Menurut penjelasan dari (Srinivasa Rao, Rama and Naga Mani, 2011),

Kewarganegaraan (Port Knocking) adalah metode untuk membuka port dari luar jaringan firewall dengan mengirimkan paket-paket yang telah ditetapkan pada port close, setelah menerima pesanan yang benar , port dinamis akan membuka port firewall. Menurut (Al-Bahadili and Hadi, 2010), Rekayasa HPK (Hybrid Port Knocking) terdiri dari tujuh tahapan utama. Berikut ini, uraian tentang tujuh langkah: Pemantauan Lalu Lintas, Pengambilan dan analisis lalu lintas, Pemrosesan Gambar, Otentikasi Klien, Otentikasi Server, Membuktikan identitas klien, Penutupan Port.

Penjelasan (Musawi, 2016), Iptables merupakan bagian dari proyek Netfilter. Netfilter adalah sekumpulan kait kernel Linux yang berkomunikasi dengan tumpukan jaringan. Iptables adalah perintah dan struktur tabel yang berisi seperangkat aturan yang mengontrol pemfilteran paket.

Ada tiga tabel di iptables. Aturan atau rantai khusus yang Anda buat akan dimasukkan ke salah satu tabel ini. Filter tabel adalah default, dan salah satu yang paling banyak digunakan. Tabel filter berisi rantai built-in: INPUT: Proses paket masuk MAJU: Proses paket yang dirutekan melalui host, OUTPUT: Proses paket keluar.

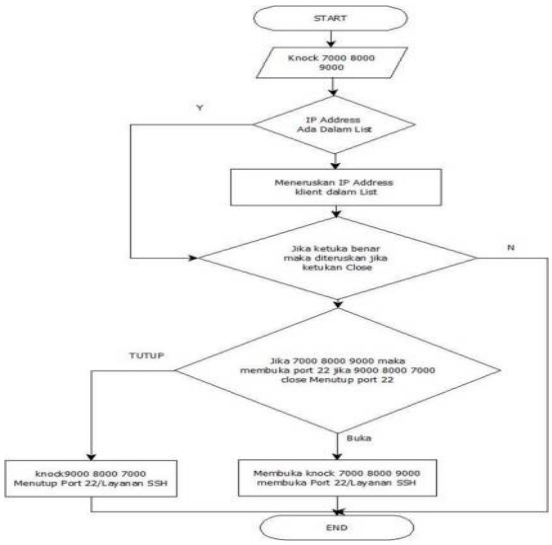
Firewall adalah perangkat lunak atau perangkat keras yang digunakan untuk melindungi jaringan dengan menganalisis data yang masuk dan keluar, berdasarkan sekumpulan aturan, apakah memiliki rangkaian berbahaya atau tidak (Alqahtani and Iftikhar, 2013).

METODE PENELITIAN

Ada Beberapa Aspek dalam network Security (Sharma, 2014).

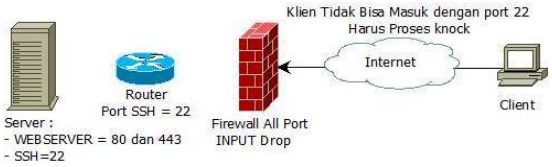
1. Confidentiality : Menjaga pembatasan resmi atas akses dan mengungkap informasi, termasuk cara untuk melindungi privasi pribadi dan informasi hak milik. Hilangnya kerahasiaan adalah mengungkap informasi yang tidak sah.
2. Integrity: Menjaga dari modifikasi atau perusakan informasi yang tidak tepat, termasuk memastikan informasi non-penyangkalan dan keaslian. Hilang nya integritas adalah modifikasi atau penghancuran informasi yang tidak sah.
3. Availability : Memastikan akses dan penggunaan informasi yang tepat waktu dan dapat diandalkan. Hilangnya ketersediaan adalah terganggunya akses atau penggunaan informasi atau sistem informasi.

A. FlowChart yang akan dibuat sebagai berikut :



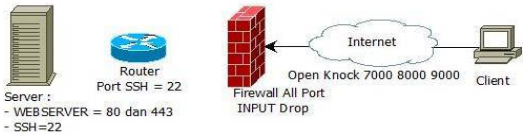
Gambar 1. Flowchart Port Koncking

B. Cara kerja Prot Knocking
   1. Gambar di bawah menunjukan si user tidak bisa masuk langsung menggunakan aplikasi SSH karena port ssh(22) sudah di block dari firewall input. lihat keterangan gambar.



Gambar 2. block dari firewall input

2. Gambar dibawah dalam proses ini user akan mengetuk terlebih dahulu dengan ketukan dengan Sequence 7000 8000 dan 9000 dalam waktu 3 detik bersamaan, pengetukan ini sudah di atur dan di konfigurasi di dalam Firewall suapaya hanya bisa membuka Port 22.



Gambar 3. ketukan open Knock 7000 8000 dan 9000

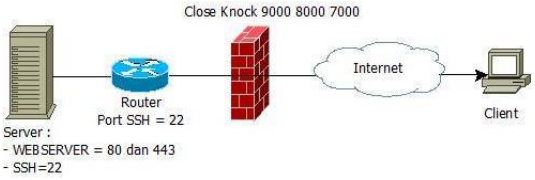
3. Proses output di firewall (port knocking daemon) mencegah upaya koneksi dan meinterpretasikan (akan meuraikan sandi dan membaca sandi) terdiri dari otentik Port Knocking Firewall melakukan tugas tertentu berdasarkan isi dari port knocking, disini firewall sudah mengizinkan klien dan sudah melakukan monitoring berdasarkan IP User dan melakukan pencatatan berupa log di dalam firewall, langkah disini user sudah bisa menggunakan aplikasi SSH (Secure Shell) untuk melakukan remote terhadap server.

Gambar 4. Membuka port ssh

4. proses user membuka aplikasi SSH dengan meremote port 22 kedalam server dan user bebas beraktifitas di dalam server.

Gambar 5. membuka ssh port 22 supaya masuk ke server

5. Closing, Sedangkan jika user/admin ingin menutup port 22, exit terlebih dahulu dari Aplikasi SSH maka ketukan yang akan di gunakan adalah 9000 8000 7000, seluruh aktifitas user akan di tutup kembali, dan Firewall melakukan proses dimana seluruh port akan tertutup kembali.

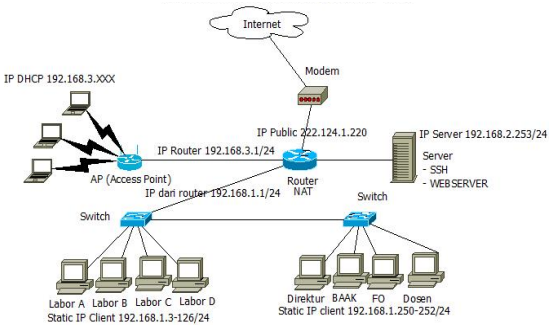


Gambar 6. Close Knock

HASIL DAN PEMBAHASAN

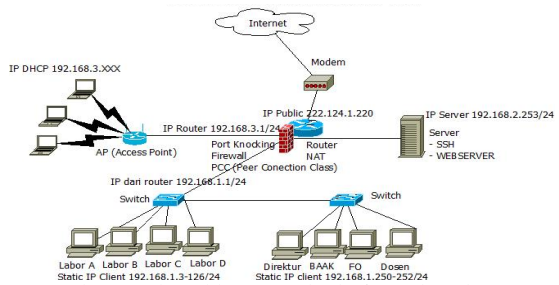
1. Topology Overview Network Systems

Dalam penerapan ini ada hal yang harus di lakukan melakukan penarapan-penerapan yang sesuai dengan kebutuhan metode Port Knocking, banyak hal yang di lakukan dalam membangun keamanan jaringan dapat di uraikan di penerapan yang akan di buat oleh seorang administrator atau pihak yang berwenang yang sudah di beri akses kedalam server.



Gambar 7. Network Topology

2. Intefare Design Of Implementation of Port knocking



Gambar 8. The addition method of port knocking on networked systems

3. Analisys Of Port Knocking
   a. Dalam langkah pertama ini disini akan melakukan konfigurasi IP Address agar bisa terhubung server ke router dalam hal ini IP address 192.168.2.253 untuk server ada pun cara konfigurasi dengan perintah nano /etc/network/interfaces
   b. eth0 adalah interface jaringan dalam bentuk fisiknya adalah ethernet satu, dengan satu alamat IP address 192.168.2.253 dengan pengelompokan IP address Class C netmask 255.255.255.0 dengan gateway 192.168.2.254 IP ini mengacu pada IP router supaya bisa berkomunikasi dengan router.
   c. Setelah konfigurasi IP address teleah selesai, lanjut dengan mengkonfiugrasi Hosts ini di maksudkan agar memberikan nama pada jaringan local dengan nama webserver nano /etc/hosts
   d. IP 127.0.0.1 adalah IP localhost ini nantinya akan di kenal di jaringan dengan penamaan webserver.
   e. *Resolv.conf* ini adalah bagaimana supaya terhubung dengan *router* ***nano /etc/resolv.conf.***
   f. Untuk mengeksekusi *netwrok interfaces* menggunakan perintah ***service networking start.***

Penambahan repository pada OS Debian atau kumpulan dari berbagai banyak sekali macam aplikasi atau suatu paket aplikasi distribusi Linux dan sekaligus juga bisa memperbaharui system perlu ada penambahan pada system di OS Debian. Dalam hal ini list repository yang di ambil dari server repo nya UI

   a. To add a repository by way membahkan library repository link UI following manner.
   b. Furthermore, the process of installing applications knock with the command apt-get install knockd.
   c. Configure knock.conf by typing a command nano /etc/knockd.conf.
   d. Further configure defult of knock by typing the command open the nano / etc / defult / knockd.
   e. At the last stage did knock command execution with the command service knockd restart.

Taking On The Firewall Configuration

   a. Closing all the input ports on the server that can not be accessed from outside into the server by typing the command open apalikasi iptables -P INPUT DROP.
   b. Open a web port for web publishing campus AMIK Mahaputra by typing the command open the application on iptables -A INPUT -p TCP -j ACCEPT -dport 80 for TCP, UDP ports to open by typing the command to open the application iptables -A INPUT -p UDP -dport 80 - j ACCEPT.
   c. For the iptables firewall can type -nL.

From the client side can Doing pegecekan IP Address with a love by the internet provider can open in a browser with www.whatismyip.com website or can Jugan with www.speedtest.net.

   a. To check on the client IP Privet can by typing ipconfig at a command prompt.
   b. The test results if the whole server ports open by clicking apikasi Zenmap in windows in the form of GUI (Grafic User Interface) that have previously been installed on the client to fill in the target column Public IP that belongs to the server, and then by typing the command column command nmap (IP public server). Continues on clicking the scan button. To open the

application results if Zenmap provide an open port.

c. The test results if the server all ports closed by clicking apikasi Zenmap in windows in the form of GUI (Grafic User Interface) that have previously been installed on the client to fill in the target column Public IP that belongs to the server, and then by typing the command column command nmap (IP public server). Keep on clicking the scan button next to the result if the application is closed Zenmap provide an open port

d. Client must be connected to the Internet first meluakukan checking the Internet connection by opening a command prompt type the ping google.com, if the replay it is already connected to the Internet

e. Further testing ping the server by typing the IP Public server with ping command at a command prompt (Public IP)

f. Further testing directly to the server remotely, in case of error means the configuration on the server running because all ports have been closed in the firewall

g. The next step the client must know the steps tapping format by typing commands open the application knock.exe -v (Public IP) to the beat already in combination with the tap 7000 8000 9000 to open a knock on the firewall. Then the server will save the IP address of the client if ketuka true then the server will open a port in accordance with the knock knock in this case 7000 8000 9000 is open SSH port22.

h. The next client opens putty applications already installed on the client by clicking the putty application and type the Public IP server in the column hostname (or IP Address) to port 22 then click ok

i. Furthermore, in this stage putty application authenticated login and enter the password

j. Once logged in user status, then malakukan authentication to root by typing sudo -s and do typing passwords

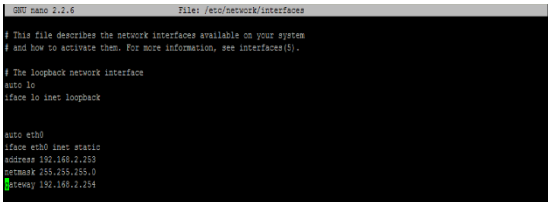
k. After that the client can perform activities on the server, in this case to check anyone who entered into the server in the form of IP Address Address complete with ports in the open, in a way to command tail -f / var / log / syslog.

l. Once the client has been doing activities in client server must follow the next steps by typing perinta exit from exit again as the root user.

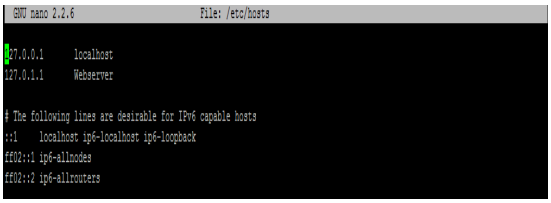
m. The next client open a command prompt return to close the tap on the server by typing a command knock.exe -v (Public IP) 9000 8000 7000.

Design Of Port Knocking

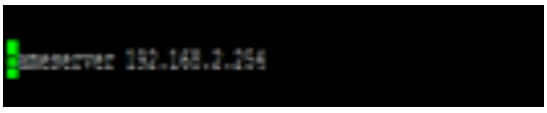
Implementation Scenarios Network Configuration on Debian OS



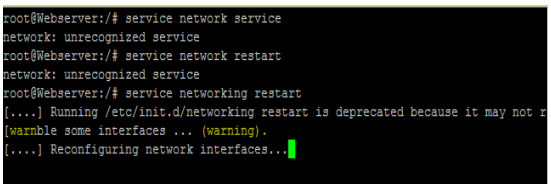
Gambar 9. Configuration IP Address



Gambar 10. Configuration Host

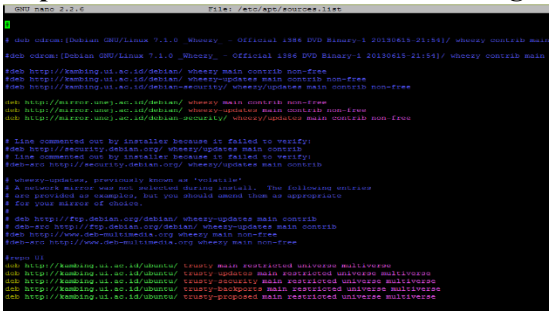


Gambar 11. Configuration Resolv.conf



Gambar 12. Execution Network

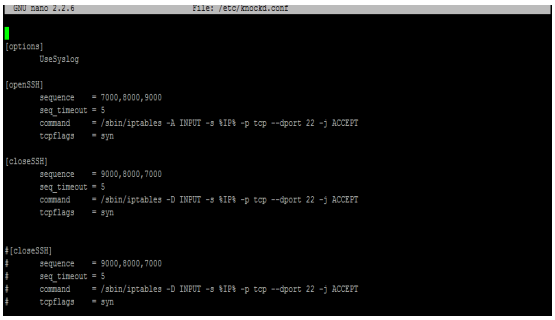
Implementation Scenarios Port Knocking



Gambar 13. Extra Repository

```
root@Webserver:/# apt-get install knockd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  knockd
0 upgraded, 1 newly installed, 0 to remove and 561 not upgraded.
Need to get 27.0 kB of archives.
After this operation, 172 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  knockd
Install these packages without verification [y/N]? Y
```

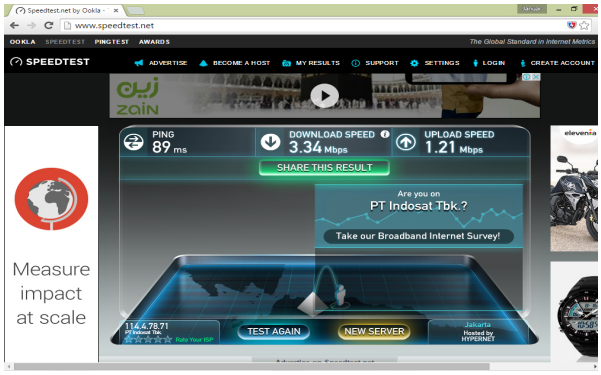
Gambar 14. Installing Applications Knock



Gambar 15. Configuration Knock

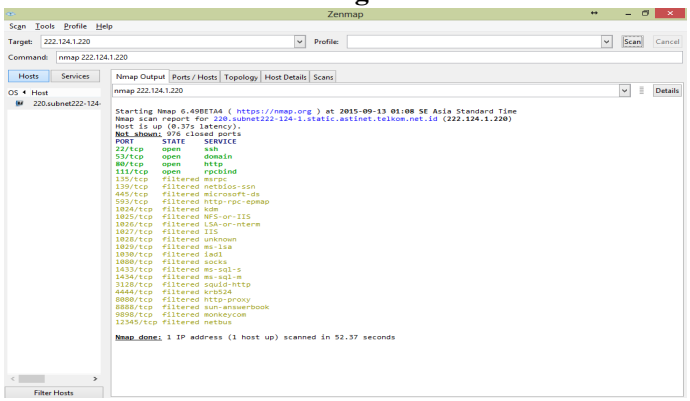
```
root@Webserver:/# nano /etc/default/knockd
root@Webserver:/# service knockd restart
[ ok ] Stopping Port-knock daemon: knockd.
[ ok ] Starting Port-knock daemon: knockd.
root@Webserver:/#
```

Gambar 16. Result Execution of Applications Knock

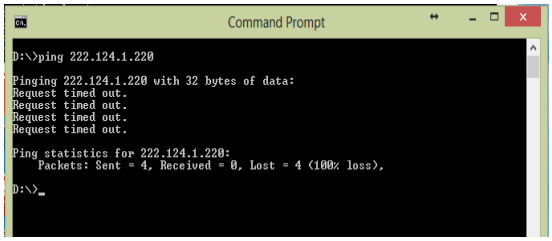


Gambar 17. Implementation Scenario Testing IPAddress in client

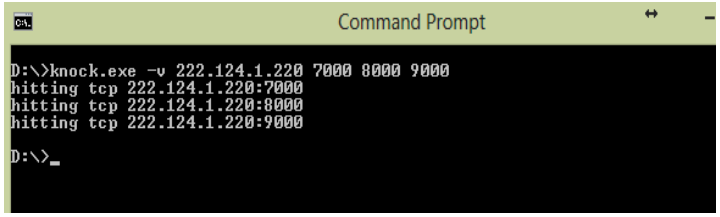
Test Result of Port Knocking



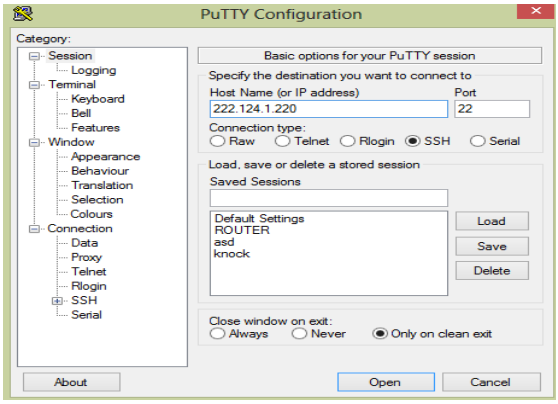
Gambar 18. Implementation Scenario Testing IPAddress in client



Gambar 19. Testing Against Server connection



Gambar 20. Tapping on the format Firewall



Gambar 21. The Test Results of Remote SSH (Secure Shell) using Putty Application

SIMPULAN DAN SARAN

Dari hasil pengamatan selama perancangan, implementasi dan proses uji coba perangkat lunak yang dilakukan, dapat diambil kesimpulan sebagai berikut:

1. Tingkat penggunaan sumber daya oleh server ketika menjalankan daemon relatif stabil, sehingga kinerja server tidak terganggu.
2. Aplikasi ini memungkinkan administrator mampu melakukan koneksi server meskipun server memblok semua port yang ada.
3. Konfigurasi baru yang di kembangkan ternyata memberikan kinerja yang cukup untuk mengamankan serangan dari luar yang memanfaatkan port.
4. Dengan atau tanpa menggunakan firewall, port yang digunakan untuk autentikasi port knocking tidak terlihat saat dilakukan stealth scanning menggunakan nmap

TERIMA KASIH

Terimakasih kepada pihak AMIK Mahaputra yang sudah membantu untuk project ini.

DAFTAR PUSTAKA

1. Al-Bahadili, H. and Hadi, A. H. (2010) 'Network Security Using Hybrid Port Knocking', *Ijcsns*, 10(8), p. 8. Available at: http://www.uop.edu.jo/download/Research/members/382_1316_Network_Security_Using_Hybrid_Port_Knocking.pdf.
2. Alqahtani, A. H. and Iftikhar, M. (2013) 'TCP / IP Attacks , Defenses and Security Tools', *Proceedings - IEEE Symposium on Security and Privacy*, 1(10), pp. 42–47. doi: 10.1109/SECPRI.1997.601338.
3. Babatunde, O. and Al-Debagy, O. (2014) 'A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)', *International Journal of Computer Trends and Technology*, 13(1), pp. 10–13. doi: 10.14445/22312803/ijctt-v13p103.
4. Gangane, S., Kakade, V. and Professor, A. (2014) 'Base of the Networking Protocol-TCP/IP Its Design and Security Aspects', *International Journal of Innovative Research in Computer and Communication Engineering (An ISO*, 3(4), pp. 3712–3718. doi: 10.15680/ijircce.2015.0304144.
5. Kumar, S. and Rai, S. (2012) 'Survey on Transport Layer Protocols: TCP & UDP', *International Journal of Computer Applications*, 46(7), pp. 975–8887.
6. Musawi, B. Q. (2016) 'Mitigating DoS / DDoS attacks using iptables', (January 2012).
7. Pourvahab, M. and Atani, R. E. (2018) 'ENHANCED SECURE WEB-KNOCKING (USING SINGLE PACKET INTERNATIONAL JOURNAL OF CURRENT LIFE SCIENCES', (January 2019).
8. Saxena, P. (2013) 'OSI Reference Model – A Seven Layered Architecture of OSI Model', *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(8), pp. 338–346.
9. Sharma, A. (2014) 'Managing the Organizational Network Security', *International Journal of Innovations in Computing*, 2(4), pp. 5–8.
10. Srinivasa Rao, C., Rama, B. R. and Naga Mani, K. (2011) 'Firewall Policy Management Through Sliding Window Filtering Method Using Data Mining Techniques', *International Journal of Computer Science & Engineering Survey*, 2(2), pp. 39–55. doi: 10.5121/ijcses.2011.2205.