

Penerapan Metode Rule Based Dalam Mendeteksi Serangan Multi Attack Pada Network Attached Storage

Ilham Faisal, Divi Handoko, Halimansyah Putra

^{1,2} Fakultas Teknik dan Komputer, Teknik Informatika, Universitas Harapan Medan, Kota Medan, Indonesia
Email: halimansyahputra@gmail.com

Abstrak

Network Attached Storage (NAS) merupakan sebuah *server* dengan sistem operasi yang dikhususkan untuk melayani kebutuhan berkas *data*. *NAS* merupakan solusi terbaik sebagai media penyimpanan dan *sharing data*. Namun, aspek keamanan data juga menjadi perhatian utama dalam penggunaan media penyimpanan *NAS*. Pengelola *NAS server* tidak dapat menjamin keamanan *data* pada *NAS server* yang dikelolanya. Dalam melindungi dan mendeteksi serangan pada *NAS*, penggunaan *firewall* sebagai keamanan sangatlah disarankan sebagai benteng awal. Metode *Rule Base* yang diimplementasikan dalam *firewall* untuk menguji seberapa besar akurasi keamanan *NAS server*, apabila *NAS* tersebut diserang dengan serangan *multi-attack* (serangan ganda). Serangan *multi-attack* dibagi menjadi dua, yaitu *brute-force attack* dan *a denial-of-service (DDoS)*. Analisis forensik juga diperlukan untuk mengetahui apakah ada *intruder* yang melakukan penyerangan, diperlukan juga *wireshark* sebagai paket *capturing* dan *snort* sebagai paket *sniffing* yang berbasis *Intrusion Detection System (IDS)* dalam pengujian serangan. Pengujian dilakukan menggunakan metode *rule based* terhadap *firewall iptables* pada *NAS* yang sangat efektif untuk memblokir serangan awal terhadap *NAS*. Dari 8 kali pengujian, akurasi *rule-based* terhadap serangan *multi-attack* pada *NAS* sebesar 84% berhasil memblokir serangan dan 16% gagal memblokir serangan. Waktu yang diberikan berupa pembatasan *limit bandwidth* masuk dan *limit-burst* yang diterapkan pada *port icmp, udp, tcp ssh* dan *ftp*. *Rule-based* berhasil memblokir serangan *multi-attack* yang ditujukan pada *NAS*. Hasil dari penerapan metode *rule-based* pada *firewall* diharapkan dapat memblokir serangan ganda pada *NAS*. Pada serangan *brute-force rule base* berhasil melakukan *drop* koneksi port aktif pada *NAS*, dan pada serangan *DDoS rule base* juga berhasil melakukan *drop* terhadap *socket flooding* pada *NAS*.

Kata Kunci: *Network Attached Storage (NAS), Multi-Attack, Metode Rule Based*

Abstract

Network Attached Storage (NAS) is a server with an operating system that is specific to serving the needs of data files. *NAS* is the best solution as a storage medium and data sharing. However, the aspect of data security is also a major concern in the use of *NAS* storage media. The *NAS server* manager cannot guarantee data security on the *NAS server* they manage. In protecting and detecting attacks on *NAS*, the use of a firewall as security is highly recommended as an initial stronghold. The *Rule Base* method is implemented in the firewall to test the accuracy of the *NAS server's* security, if the *NAS* is attacked by a *multi-attack* (multiple attacks). *Multi-attack* attacks are divided into two, namely *brute-force attacks* and a *denial-of-service (DDoS)*. Forensic analysis is also needed to find out whether there is an intruder carrying out the attack, *wireshark* is also needed as packet capturing and *snort* as packet sniffing based on the *Intrusion Detection System (IDS)* in testing attacks. The test was carried out using a *rule-based* method against the *iptables* firewall on the *NAS* which is very effective at blocking the initial attack on the *NAS*. Of the 8 times of testing, the *rule-based* accuracy against *multi-attack* attacks on *NAS* was 84% successfully blocking attacks and 16% failing to block attacks. The time given is in the form of incoming bandwidth limits and *limit-burst* which are applied to *icmp, udp, tcp ssh* and *ftp* ports. *Rule-based* managed to block *multi-attack* attacks aimed at *NAS*. The result of applying the *rule-based* method to the firewall is expected to be able to block multiple attacks on the *NAS*. In the *rule base brute-force attack* it succeeded in dropping active port connections on the *NAS*, and in the *rule base DDoS attack* it also succeeded in dropping *socket flooding* on the *NAS*.

Keywords: *Network Attached Storage (NAS), Multi-attack, Rule Based Method*

1. PENDAHULUAN

Perkembangan teknologi saat ini sangatlah pesat, banyak orang memanfaatkan *internet* sebagai media penyimpanan dengan sistem *Network Attached Storage (NAS)* berbasis *Cloud*. *Network Attached Storage (NAS)* merupakan sebuah server dengan sistem operasi yang dikhususkan untuk melayani kebutuhan berkas *data*. *NAS* dapat berbentuk perangkat yang siap pakai atau berupa sebuah piranti lunak yang akan di-*install* pada sebuah komputer agar berubah fungsi menjadi *server NAS* [1]. Selain itu, aspek keamanan data juga menjadi perhatian utama dalam penggunaan media penyimpanan *NAS*. Pengguna tidak bisa menjamin keamanan data pada *NAS Server* yang dikelola. Dikarenakan bersifat gratis dan bisa dikembangkan, kerentanan pada *NAS Server* terhadap serangan siber sangat tinggi. Untuk itu diperlukan analisis jaringan (*Network Forensic*) untuk mengamati pola serangan pada *NAS Server*.

Analisis jaringan (*Network Forensic*) yang penulis bahas dalam penelitian ini merupakan karakter dan pola serangan ganda (*Multiple-Attack*) yang menyerang sistem pada *NAS Server*. Penulis menggunakan metode *rule base* untuk mengatur aturan-aturan pada *Firewall* yang memudahkan proses verifikasi maupun autentikasi. Metode *rule base* merupakan metode yang menggunakan aturan (*rule*) sebagai representasi pengetahuan yang akan diimplementasikan dalam sistem [2]. Metode *rule base* memiliki keunggulan yang diterapkan pada domain sederhana sehingga mempermudah proses verifikasi dan validasi, namun memiliki kelemahan jika diterapkan pada *domain* dengan tingkat kompleksitas yang tinggi. Apabila sistem *rule base* tidak dapat mengenali *rules*, maka tidak ada hasil yang diperoleh (Grosan & Abraham, 2018).

Pada penelitian sebelumnya [4], membahas tentang analisis forensik serangan *brute force* yang terjadi pada *owncloud* menggunakan metode *rule-base*. Dalam penelitian ini penulis menggunakan beberapa jenis serangan (*Multiple-Attack*) untuk mengenali pola dan celah serangan yang terjadi pada *NAS Server*. Serangan yang dilakukan yaitu, *Brute Force Attack*, *A Distributed Denial of Services (DDoS Attack)*. *Brute Force Attack* merupakan serangan dengan mencoba seluruh kemungkinan kunci yang ada. Dengan kata lain semakin besar kemungkinan yang ada semakin lama pula proses pencarian solusinya [5]. Sedangkan *A Distributed Denial of Services (DDoS Attack)* merupakan suatu serangan dengan membuat lalu lintas *data* seperti membawa beban berat, sehingga tidak dapat menerima koneksi dari pengguna lain. Dengan mengirimkan *request data* ke *server* secara terus menerus dengan *bandwidth transfer data* yang besar [6].

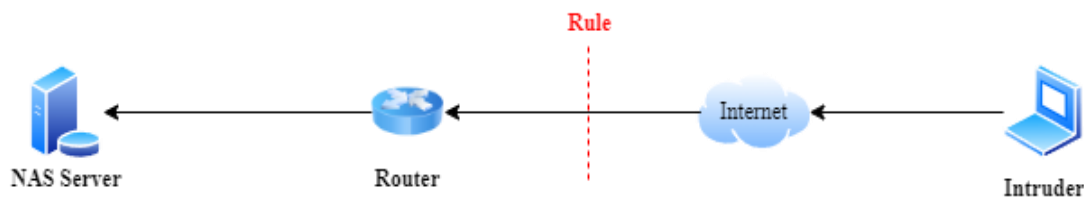
Pada penelitian ini penulis akan melakukan analisis forensik jaringan (*Network Forensic*) menggunakan tools *Network Forensic* seperti *Wireshark*, dan *Snort* terhadap *NAS Server* yang diserang menggunakan serangan ganda (*Multiple-Attack*) menggunakan *Brute Force Attack*, dan *A Distributed Denial of Services (DDoS Attack)* terhadap sistem keamanan *NAS Server* yang dilindungi oleh *Firewall* menggunakan aturan-aturan (*Rule Base*) pada sistem *NAS Server* yang diserang. Hasil akhir dari penerapan metode *rule-based* pada *firewall* diharapkan dapat memblokir ataupun membatasi jumlah *data* serangan (*hit-count*) yang masuk pada *NAS Server*. Terutama pada *port remoting server* yang sangat rentan terhadap serangan seperti *port ssh, ftp, telnet, http, dan https*. Sehingga nantinya hasil serangan yang dilakukan terblokir dan tidak efektif terhadap *NAS Server*.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Pada penelitian ini terdapat beberapa tahapan dan langkah-langkah sebelum nantinya mendapatkan hasil akurasi akhir penerapan metode dan serangan yang terjadi pada *Network Attached Storage* diantaranya adalah sebagai berikut:

1. Analisis Kebutuhan
Pada tahap ini dilakukan analisis kebutuhan perangkat dimana analisis kebutuhan ini dibagi menjadi 2 bagian, yaitu kebutuhan perangkat keras, dan kebutuhan perangkat lunak.
2. Perancangan dan Konfigurasi Sistem
Pada tahap ini dilakukan konfigurasi sistem virtualisasi yang digunakan dalam melakukan serangan sekaligus virtualisasi *Network Attached Storage*.
3. Perancangan dan Konfigurasi NAS
Pada tahap ini dilakukan proses instalasi sekaligus konfigurasi *Network Attached Storage*, pada tahap perancangan NAS dilakukan konfigurasi IP Statis dan konfigurasi firewall pada sistem NAS.
4. Perancangan dan Konfigurasi Intruder
Selanjutnya pada tahap ini dilakukan proses instalasi dan konfigurasi *intruder* (penyerang). Konfigurasi *intruder* berupa instalasi tools serangan pada *kali linux*.



Gambar 2.1 Topologi proses serangan *intruder* terhadap NAS

Keterangan :

1. *Intuder* melakukan serangan melalui jaringan internet.

2. Sebelum serangan masuk ke NAS, serangan terlebih dahulu melawati router yang telah dikonfigurasi *firewall*.
3. Pada sistem NAS ditambahkan *rule iptables* yang tujuannya melakukan *blocking* terhadap serangan *interuder*.
5. Implementasi Rule Based pada Firewall
Pada tahap ini dilakukan implementasi metode *rule based* terhadap *firewall iptables* yang terdapat pada NAS.

```
root@truenas[/home/admin]# /sbin/iptables -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j DROP
root@truenas[/home/admin]# /sbin/iptables -A INPUT -p tcp -m connlimit --connlimit-above 100 -j REJECT --reject-with tcp-reset
root@truenas[/home/admin]# /sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -m limit --limit 60/s --limit-burst 20 -j ACCEPT
root@truenas[/home/admin]# /sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -j DROP
root@truenas[/home/admin]# /sbin/iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --set
root@truenas[/home/admin]# /sbin/iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --update --second 60 --hitcount 10 -j DROP
root@truenas[/home/admin]# iptables -L --line-numbers
```

Gambar 2.2 Konfigurasi *rule based* pada NAS

Tabel 2.1 Penjelasan *rule based firewall iptables*

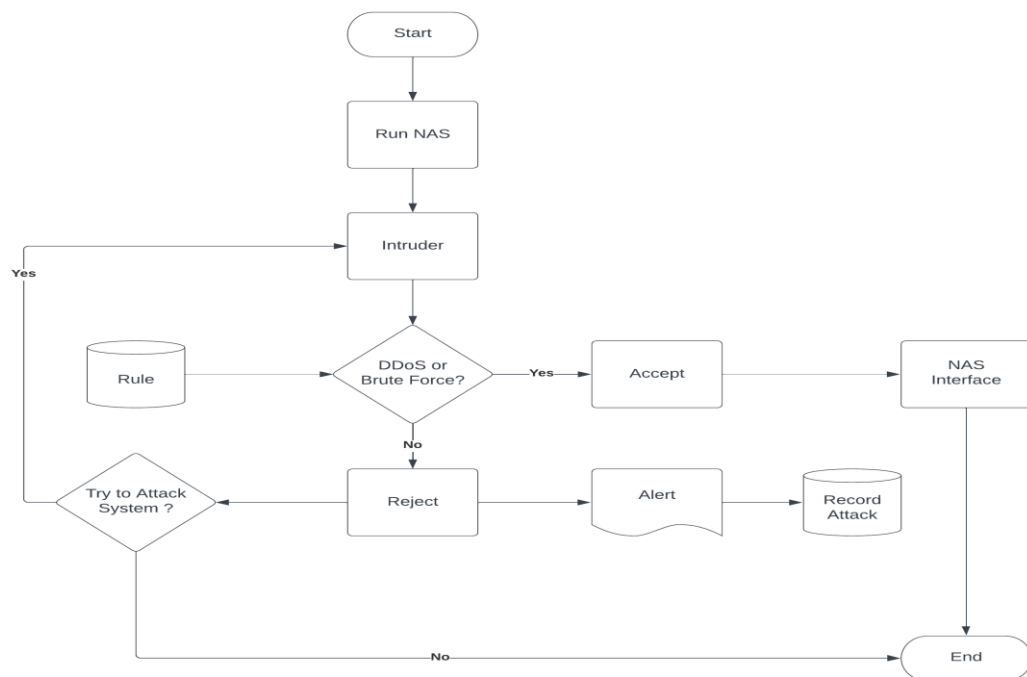
Fungsi	Rule Input	Jenis Serangan	Keterangan
Memblokir paket yang tidak valid	# /sbin/iptables -t mangle -A PREROUTING -m conntrack -ctstate INVALID -j DROP	A Denial of Services Rule	if [traffic can entered] INVALID data then connection [DROP]
Membatasi koneksi IP sumber	# /sbin/iptables -A INPUT -p tcp -m connlimit-above 100 -j REJECT --reject-with tcp-reset	A Denial of Services Rule	if [TCP/IP connection limit>100] then connection [REJECT] with TCP/IP reset
Membatasi koneksi TCP baru perdetik	# /sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -m limit --limit 60/s --limit-burst 20 -j ACCEPT # /sbin/iptables -A INPUT -p tcp -m conntrack --ctstate NEW -j DROP	A Denial of Services Rule	# if [TCP/IP bandwidth connection<60/second and max-bandwidth with burst time 20] then connection [ACCEPT] # if [TCP/IP bandwidth >60/second with burst time >20] then connection [REJECT]
Melakukan kontrol atas port SSH	# /sbin/iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --set # /sbin/iptables -A INPUT -p tcp --dport ssh -m conntrack --	Brute Force Attack Rule	# if [INPUT Chain TCP/IP user visitor focused for SSH port][22] > 60/s and >10 users then connection [DROP]

Lanjutan Tabel 2.1 Penjelasan *rule based firewall iptables*

Fungsi	Rule Input	Jenis Serangan	Keterangan
	<i>ctstate NEW -m recent --update --second 60 --hitcount 10 -j DROP</i>		
Memblokir scan open port pada NAS	<pre># /sbin/iptables -N port-scanning # /sbin/iptables -A port-scanning -p tcp --tcp-flags SYN, ACK, FIN, RST RST -m limit --limit 1/s --limit-burst 2 -j RETURN # /sbin/iptables -A port-scanning -j DROP</pre>	Port Scanning Rule	# if [Port-scanning by SYN, ACK, FIN, RST] connection forced > 1/s with burst time >2 then connection [DROP]

6. Pengujian Serangan Terhadap NAS

Pada tahap ini dilakukan pengujian serangan *intruder* terhadap NAS server.



Gambar 2.3 Flowchart pengujian serangan

2.2 Alat dan Bahan Penelitian

1. Perangkat Keras (Hardware)

Berikut merupakan spesifikasi kebutuhan perangkat keras (*hardware*) yang dibutuhkan dalam membangun sistem pada penelitian ini.

Tabel 2.2 Kebutuhan Perangkat Keras

No.	Perangkat	Spesifikasi	Detail
1.	Laptop Lenovo Ideapad 5 14ALC05	Computer Name	LAPTOP-E8856BAB
		Manuvacture	LENOVO
		System Model	82LM
		BIOS	G5CN60WW (V2.06)
		Processor	AMD Ryzen 5 5500U
		Memory	8192 MB
		Card Name	AMD Radeon(TM) Graphic
		Manuvacture	Advanced Micro Devices, Inc
		Chip Type	AMD Radeon Graphic Processor (0x164c)
		Display Memory	495 MB
		Shared Memory	3757 MB
		Current Display Memory	1920 x 1080 (32 bit) (60 Hz)
		Wifi Connection	Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
2.	Drive System	Partition ID	C
		System Type	NTFS
		Drive Space	80,8 GB Free of 174 GB
3.	Drive Storage	Partition ID	D
		System Type	NTFS
		Drive Space	209 GB Free of 300 GB
4.	Router Mikrotik h AP lite	ID	RB941-2ND-TC
		IC	7442A-9412ND
		Manuvacture	Mikrotikls SIA

2. Perangkat Lunak (Software)

Berikut merupakan spesifikasi kebutuhan perangkat lunak (*software*) yang penulis butuhkan dalam membangun dan menyerang sistem pada penelitian ini.

Tabel 2.3 Kebutuhan Perangkat Lunak

No.	Software	Detail
1.	Operating System (OS)	Windows 11 Home Single Language 64-bit (10.0, Build 22621)
		Open BSD (TrueNAS SCALE)
		Kali Linux v.2023.1

Lanjutan Tabel 2.3 Kebutuhan Perangkat Lunak

2.	Aplikasi Serangan (<i>Intruder</i>)	<i>Kali Linux v.2023.1</i>
		<i>Slowlaris v.0.2.6</i>
		<i>Hydra v.5.5</i>
3.	Aplikasi Forensik	<i>Wireshark</i>

2.3 Analisis Permasalahan

Penggunaan penyimpanan *online* dengan kapasitas yang besar tentu menarik minat berbagai kalangan. Banyak dari kalangan organisasi maupun instansi yang menggunakan *Network Attached Storage* (NAS) sebagai alternatif dari mahalnya biaya penyewaan *server* penyimpanan. Banyak pesaing bisnis yang niatnya ingin mencuri, mengambil, ataupun merusak database instansi dengan melakukan penyerangan terhadap NAS yang dikelola, ataupun user publik yang sengaja untuk mencoba-coba melakukan peretasan terhadap NAS.

Banyak terjadi upaya serangan dengan melakukan *flooding request data* pada NAS secara terus menerus yang bertujuan untuk menonaktifkan layanan sampai membuat *server* NAS tersebut *down*. Sehingga orang yang ingin membuka *database* pada NAS tidak dapat mengakses halaman loginnya. Walaupun sering terjadinya serangkaian upaya dengan melakukan usaha paksa terhadap izin akses secara ilegal pada NAS, seperti menggunakan serangan *Brute Force* dalam melakukan proses masuk secara paksa dengan cara mencari dan memperoleh hak masuk secara ilegal. Sehingga diperlukan analisa bagaimana pola serangan pada NAS tersebut dapat terdeteksi, dan bagaimana penerapan *rule base* pada *firewall* terhadap NAS bekerja jika terjadi serangan berbeda secara bersamaan.

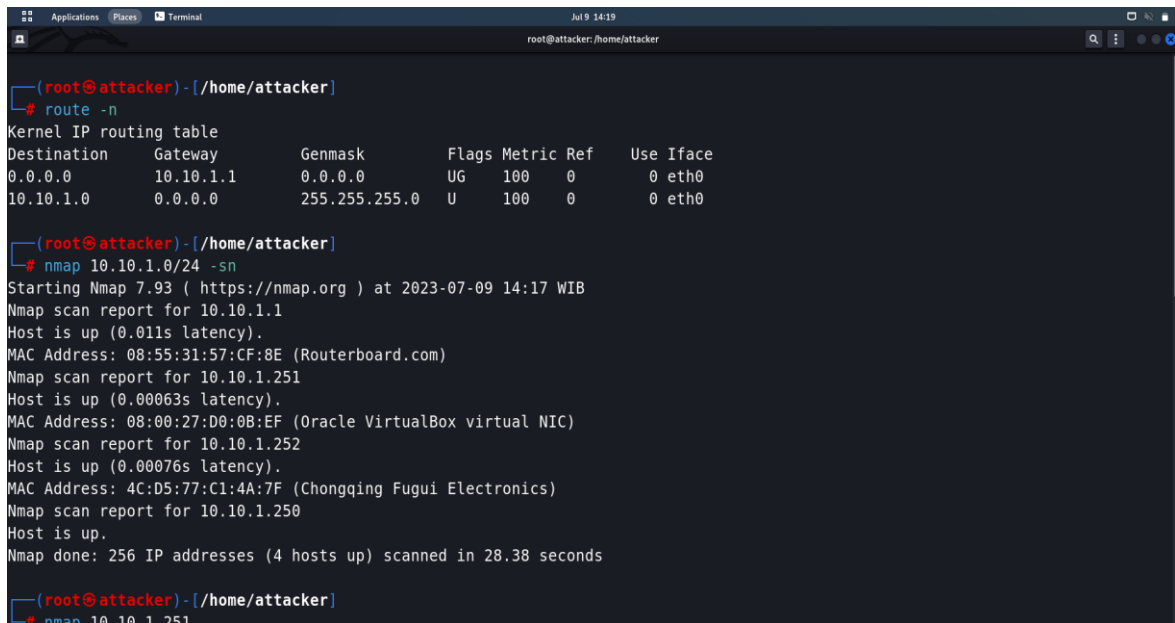
3. HASIL DAN PEMBAHASAN

Pada tahap ini, penulis melakukan serangan pada sistem *Network Attached Storage* (NAS) secara langsung. Hasil dari pengujian ini akan menampilkan bagaimana *rule base* melakukan serangkaian aturan pertahanan terhadap NAS yang diserang menggunakan serangan *Multi-Attack* (serangan ganda). Untuk mendapatkan hasil analisis yang sesuai dengan tujuan penulisan ini dilakukan beberapa skema, yaitu proses *scanning* pada *intruder* dan sistem NAS, proses *capture data*, proses klasifikasi serangan berdasarkan rule. Dari keempat tahapan diatas akan menyimpulkan bagaimana pola serangan ganda terhadap NAS *Server*, dan seberapa besar akurasi keamanan *rule base* terhadap serangan yang dilakukan terhadap NAS *Server*.

3.1 Tahap Scanning Pada Intruder

Tahap scanning ini dilakukan untuk mencari dan menentukan alamat *IP* dan *port* di jaringan *local* dalam satu jaringan *routing*. Pada *intruder*, tahapan ini dilakukan dengan menggunakan tools *Nmap* untuk mengetahui *IP Address* dan *port* aktif pada jaringan *Local Area Network* (LAN) yang dianggap terhubung ke *Network Attached Storage* (NAS). Berikut merupakan tahapan dalam melakukan *scanning route* dan *port* menggunakan *Nmap* pada *intruder*:

1. Menjalankan perintah pada *terminal kali linux*.
2. Setelah mendapatkan *IP routing table*, selanjutnya dilakukan *scanning host* aktif pada rentang *IP* tertentu.



```

(root@attacker) - [/home/attacker]
# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          10.10.1.1       0.0.0.0         UG      100    0      0 eth0
10.10.1.0        0.0.0.0         255.255.255.0   U       100    0      0 eth0

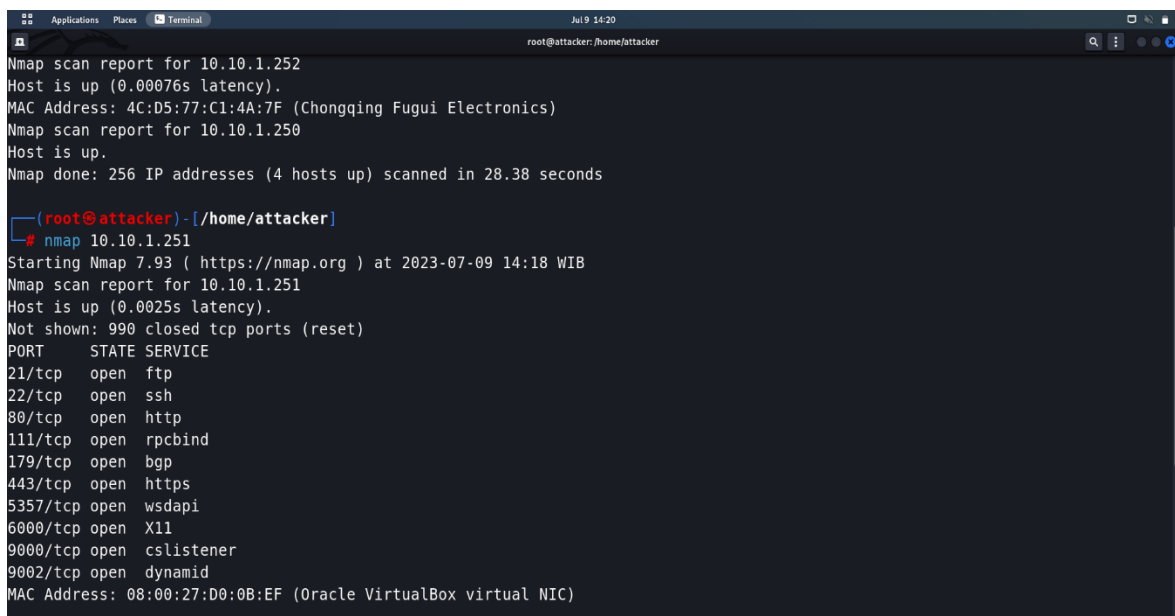
(root@attacker) - [/home/attacker]
# nmap 10.10.1.0/24 -sn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-09 14:17 WIB
Nmap scan report for 10.10.1.1
Host is up (0.011s latency).
MAC Address: 08:55:31:57:CF:8E (Routerboard.com)
Nmap scan report for 10.10.1.251
Host is up (0.00063s latency).
MAC Address: 08:00:27:D0:0B:EF (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.1.252
Host is up (0.00076s latency).
MAC Address: 4C:D5:77:C1:4A:7F (Chongqing Fugui Electronics)
Nmap scan report for 10.10.1.250
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.38 seconds

(root@attacker) - [/home/attacker]
# nmap 10.10.1.251

```

Gambar 3.1 Proses *scan route* dan *host* aktif pada *intruder*

- Setelah mendapatkan *host* aktif pada jaringan *routing*, selanjutnya *scanning port* secara menyeluruh pada jaringan *routing*.



```

Nmap scan report for 10.10.1.252
Host is up (0.00076s latency).
MAC Address: 4C:D5:77:C1:4A:7F (Chongqing Fugui Electronics)
Nmap scan report for 10.10.1.250
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.38 seconds

(root@attacker) - [/home/attacker]
# nmap 10.10.1.251
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-09 14:18 WIB
Nmap scan report for 10.10.1.251
Host is up (0.0025s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
179/tcp   open  bgp
443/tcp   open  https
5357/tcp  open  wsdapi
6000/tcp  open  X11
9000/tcp  open  cslistener
9002/tcp  open  dynamid
9003/tcp  open  dynamid
MAC Address: 08:00:27:D0:0B:EF (Oracle VirtualBox virtual NIC)

```

Gambar 3.2 Proses *nmap* terhadap jaringan *routing*

Setelah mendapatkan hasil *nmap*, terdapat satu *IP Address* dengan banyak *port* aktif. terdapat satu *IP* yang memiliki *port http* yang aktif.

3.2 Tahap serangan *intruder* terhadap NAS

Pada tahap ini dilakukan proses serangan *multi-attack* terhadap NAS, serangan pertama yaitu serangan *brute-force* dengan menggunakan *tools hydra*. Serangan *brute force* terhadap NAS ini menggunakan kombinasi *login* paksa *username* dan *password* secara acak yang telah dibuat didalam *wordlist*, biasanya *username* dan *password* yang dibuat merupakan sandi *default* untuk *login*, kombinasi huruf besar dan kecil, nama, karakter khusus, dan tanggal lahir.

Serangan kedua merupakan *A Distribution Denial of Service* (DDoS) terhadap NAS. Serangan DDoS ini bertujuan untuk melumpuhkan sistem pada NAS dengan mengirimkan paket *data* yang banyak secara terus menerus. Serangan DDoS ini menggunakan *tools Slowlaris* pada *kali linux*. Ada beberapa tahapan yang akan dilakukan untuk mendapatkan hasil yang maksimal dalam melakukan serangan ini diantaranya, serangan dilakukan tanpa *rule base* pada NAS, serangan dilakukan setelah NAS dilindungi oleh *rule base* pada *firewall*.

Secara keseluruhan, proses *login* yang berhasil maupun gagal akan tersimpan didalam *database* NAS. *Database login* berupa *log file* yang mana nantinya hanya bisa diakses melalui *CLI Linux* yang ada pada NAS.

```
root@skripsi-halim[-]# cd /var
root@skripsi-halim[/var]# ls
backups cache crash db empty lib local lock log mail opt run spool tmp trash www
root@skripsi-halim[/var]# cd log
root@skripsi-halim[/var/log]# ls
README      btmap      cron.log    error       k3s_daemon.log.2.gz  kube_router.log  messages     nginx     private  syslog      user.log  zettarepl.log
app_mounts.log  containerd.log  daemon.log  k3s_daemon.log  k3s_server_audit.log  lastlog         middlewareed.log  openvpn  proftpd  syslog.save  wsd.log
auth.log        containers     debug      k3s_daemon.log.1  kern.log            letsencrypt     multus.log      pods     samba4   sysstat     wtmp
root@skripsi-halim[/var/log]# nano auth.log
root@skripsi-halim[/var/log]#
```

Gambar 3.3 *Database log file* proses autentikasi *login* pada NAS

Pada Gambar 3.3 menampilkan proses pembukaan *log file* proses autentikasi *login* pada NAS yang tersimpan pada *folder /var/log/auth.log*.

```
GNU nano 5.4                                     syslog
Jul  9 15:30:28 skripsi-halim proftpd[89712]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:28 skripsi-halim proftpd[89711]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:28 skripsi-halim proftpd[89711]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:28 skripsi-halim proftpd[89713]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:28 skripsi-halim proftpd[89713]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:28 skripsi-halim proftpd[89714]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:28 skripsi-halim proftpd[89714]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:29 skripsi-halim proftpd[89715]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:29 skripsi-halim proftpd[89715]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:29 skripsi-halim proftpd[89716]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:29 skripsi-halim proftpd[89716]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:29 skripsi-halim proftpd[89759]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:29 skripsi-halim proftpd[89760]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:29 skripsi-halim proftpd[89760]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:29 skripsi-halim proftpd[89759]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:30 skripsi-halim proftpd[89764]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:30 skripsi-halim proftpd[89764]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:30 skripsi-halim proftpd[89763]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:30 skripsi-halim proftpd[89763]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:31 skripsi-halim proftpd[89765]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:31 skripsi-halim proftpd[89765]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:31 skripsi-halim proftpd[89766]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:31 skripsi-halim proftpd[89766]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:31 skripsi-halim proftpd[89775]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
Jul  9 15:30:31 skripsi-halim proftpd[89775]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - Maximum login attempts (1) exceeded, connection refused
Jul  9 15:30:31 skripsi-halim proftpd[89776]: 127.0.0.1 (10.10.1.250[10.10.1.250]) - USER admin (Login failed): Limit access denies login
```

Gambar 3.4 *Log file* sistem *login* gagal pada NAS

Pada Gambar 3.4 menampilkan isi *log file* autentikasi gagal *login* kedalam sistem NAS. Didalam file ini, semua proses *login* yang sukses maupun gagal akan di-*capture* dan disimpan sehingga memudahkan pengelola NAS untuk melakukan antisipasi kejahatan siber terhadap NAS yang dikelolanya.


```
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=11317 DF PROTO=TCP SPT=58188 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:42:15 skripsi-halim kernel: IN=enp0s3 OUT=
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=14036 DF PROTO=TCP SPT=58196 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:42:15 skripsi-halim kernel: IN=enp0s3 OUT=
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=45754 DF PROTO=TCP SPT=58204 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:42:15 skripsi-halim kernel: IN=enp0s3 OUT=
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=15152 DF PROTO=TCP SPT=58220 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:42:19 skripsi-halim kernel: IN=enp0s3 OUT=
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=11318 DF PROTO=TCP SPT=58188 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:42:19 skripsi-halim kernel: IN=enp0s3 OUT=
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=15153 DF PROTO=TCP SPT=58220 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:42:19 skripsi-halim kernel: IN=enp0s3 OUT=
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=45755 DF PROTO=TCP SPT=58204 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:42:19 skripsi-halim kernel: IN=enp0s3 OUT=
MAC=08:00:27:d0:0b:ef:08:00:27:5b:67:a0:08:00 SRC=10.10.1.250 DST=10.10.1.251 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=14037 DF PROTO=TCP SPT=58196 DPT=22 WINDOW=64240 RES=0x00 SYN URGF=0
Jul 9 16:45:08 skripsi-halim kernel: IN=enp0s3 OUT=
```

Gambar 3.5 Alert iptables terhadap serangan yang di-capture pada log file sistem

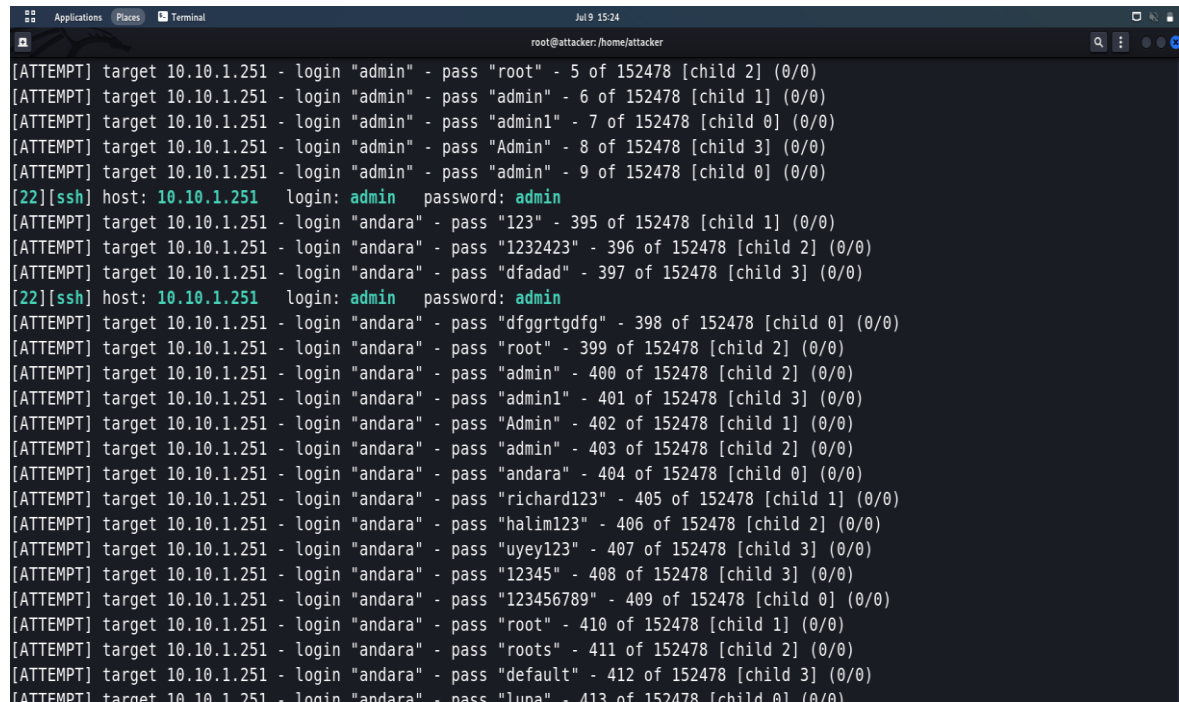
Pada Gambar 3.5 menampilkan proses *capture data* serangan terhadap port SSH yang dilakukan oleh sistem firewall iptables ketika ditambahkan rule untuk melakukan LOGDROP serangan terhadap NAS.

```
GNU nano 5.4 auth.log
Jul 9 15:18:56 skripsi-halim sshd[71877]: Invalid user andara from 10.10.1.250 port 40784
Jul 9 15:18:56 skripsi-halim sshd[71880]: error: Could not get shadow information for NOUSER
Jul 9 15:18:56 skripsi-halim sshd[71880]: Failed password for invalid user andara from 10.10.1.250 port 40808 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71878]: Invalid user andara from 10.10.1.250 port 40798
Jul 9 15:18:56 skripsi-halim sshd[71880]: Failed password for invalid user andara from 10.10.1.250 port 40808 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71878]: error: Could not get shadow information for NOUSER
Jul 9 15:18:56 skripsi-halim sshd[71878]: Failed password for invalid user andara from 10.10.1.250 port 40798 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71877]: error: Could not get shadow information for NOUSER
Jul 9 15:18:56 skripsi-halim sshd[71880]: Failed password for invalid user andara from 10.10.1.250 port 40808 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71877]: Failed password for invalid user andara from 10.10.1.250 port 40784 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71878]: Failed password for invalid user andara from 10.10.1.250 port 40798 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71881]: Invalid user andara from 10.10.1.250 port 40816
Jul 9 15:18:56 skripsi-halim sshd[71880]: Failed password for invalid user andara from 10.10.1.250 port 40808 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71877]: Failed password for invalid user andara from 10.10.1.250 port 40784 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71878]: Failed password for invalid user andara from 10.10.1.250 port 40798 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71881]: error: Could not get shadow information for NOUSER
Jul 9 15:18:56 skripsi-halim sshd[71881]: Failed password for invalid user andara from 10.10.1.250 port 40816 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71878]: Failed password for invalid user andara from 10.10.1.250 port 40798 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71881]: Failed password for invalid user andara from 10.10.1.250 port 40816 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71880]: Failed password for invalid user andara from 10.10.1.250 port 40808 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71877]: Failed password for invalid user andara from 10.10.1.250 port 40784 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71878]: Failed password for invalid user andara from 10.10.1.250 port 40798 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71881]: Failed password for invalid user andara from 10.10.1.250 port 40816 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71877]: Failed password for invalid user andara from 10.10.1.250 port 40784 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71880]: Failed password for invalid user andara from 10.10.1.250 port 40808 ssh2
Jul 9 15:18:56 skripsi-halim sshd[71880]: error: maximum authentication attempts exceeded for invalid user andara from 10.10.1.250 port 40808 ssh2 [preauth]
Jul 9 15:18:56 skripsi-halim sshd[71880]: Disconnecting invalid user andara 10.10.1.250 port 40808: Too many authentication failures [preauth]
```

Gambar 3.6 Log file autentikasi user gagal login pada port SSH

3.3 Pola serangan *multi attack* tanpa *rule*

Pada tahap ini penulis melakukan serangan *brute force* terhadap NAS yang belum diaplikasikan *rule base system*. Berikut merupakan tahapan dan pola serangan *brute force* pada NAS yang belum diaplikasikan *rule base*. Menjalankan tools *hydra* di *terminal*. Melakukan serangan terhadap *open port* SSH pada NAS Server. *Open port* SSH pada NAS terdeteksi dari hasil *nmap* dengan nilai port 22, dan *port* FTP dengan nilai port 21.



```

[ATTEMPT] target 10.10.1.251 - login "admin" - pass "root" - 5 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "admin" - 6 of 152478 [child 1] (0/0)
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "admin1" - 7 of 152478 [child 0] (0/0)
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "Admin" - 8 of 152478 [child 3] (0/0)
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "admin" - 9 of 152478 [child 0] (0/0)
[22][ssh] host: 10.10.1.251 login: admin password: admin
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "123" - 395 of 152478 [child 1] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "1232423" - 396 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "dfadad" - 397 of 152478 [child 3] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "dfggrtgdfg" - 398 of 152478 [child 0] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "root" - 399 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "admin" - 400 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "admin1" - 401 of 152478 [child 3] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "Admin" - 402 of 152478 [child 1] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "admin" - 403 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "andara" - 404 of 152478 [child 0] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "richard123" - 405 of 152478 [child 1] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "halim123" - 406 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "uyey123" - 407 of 152478 [child 3] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "12345" - 408 of 152478 [child 3] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "123456789" - 409 of 152478 [child 0] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "root" - 410 of 152478 [child 1] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "roots" - 411 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "default" - 412 of 152478 [child 3] (0/0)
[ATTEMPT] target 10.10.1.251 - login "andara" - pass "lupa" - 413 of 152478 [child 0] (0/0)

```

Gambar 3.7 Serangan *brute force* ssh dari intruder tanpa *rule*

Pada Gambar 3.7 menampilkan serangan yang dilakukan *intruder* terhadap NAS yang belum diberikan *rule* (aturan) pada *firewall*. Dimana terdapat 1 *login* ssh berwarna hijau toska yang berhasil terdeteksi proses *brute force* yang menjelaskan bahwa *login:admin* dan *password:admin* berhasil terhubung.

227	2023/190	15:19:05.685380	69.173.158.64	10.10.1.252	TCP	54 443 → 50395 [ACK] Seq=1 Ack=1 Win=12002 Len=0	
228	2023/190	15:19:05.685380	69.173.158.64	10.10.1.252	TCP	54 [TCP Previous segment not captured] 443 → 50395 [ACK] Seq=2 Ack=1 Win=12002 Len=0	
229	2023/190	15:19:05.685432	10.10.1.252	69.173.158.64	TCP	54 [TCP ACKed unseen segment] 50395 → 443 [ACK] Seq=1 Ack=2 Min=508 Len=0	
230	2023/190	15:19:05.809897	10.10.1.252	20.43.150.84	TCP	66 50967 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
231	2023/190	15:19:05.819788	20.198.119.143	10.10.1.252	TCP	54 443 → 63103 [ACK] Seq=1 Ack=1 Win=7452 Len=0	
232	2023/190	15:19:05.819865	10.10.1.252	20.198.119.143	TCP	54 [TCP ACKed unseen segment] 63103 → 443 [ACK] Seq=1 Ack=2 Win=509 Len=0	
233	2023/190	15:19:05.995519	20.198.119.143	10.10.1.252	TCP	54 [TCP Previous segment not captured] 443 → 63103 [ACK] Seq=2 Ack=1 Min=7452 Len=0	
234	2023/190	15:19:06.401741	20.43.150.84	10.10.1.252	TCP	66 443 → 50967 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128	
235	2023/190	15:19:06.401876	10.10.1.252	20.43.150.84	TCP	54 50967 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0	
236	2023/190	15:19:06.413126	10.10.1.252	20.43.150.84	TLSv1.3	359 Client Hello	
237	2023/190	15:19:06.606562	20.43.150.84	10.10.1.252	TLSv1.3	1466 Server Hello, Change Cipher Spec, Application Data	
238	2023/190	15:19:06.633065	20.43.150.84	10.10.1.252	TCP	1466 443 → 50967 [PSH, ACK] Seq=1413 Ack=306 Win=64128 Len=1412 [TCP segment of a reassembled PDU]	
239	2023/190	15:19:06.633160	10.10.1.252	20.43.150.84	TCP	54 50967 → 443 [ACK] Seq=306 Ack=2825 Win=131072 Len=0	
240	2023/190	15:19:06.811574	20.43.150.84	10.10.1.252	TCP	1466 443 → 50967 [ACK] Seq=2825 Ack=306 Win=64128 Len=1412 [TCP segment of a reassembled PDU]	
241	2023/190	15:19:06.811574	20.43.150.84	10.10.1.252	TLSv1.3	750 Application Data, Application Data, Application Data	
242	2023/190	15:19:06.811674	10.10.1.252	20.43.150.84	TCP	54 50967 → 443 [ACK] Seq=306 Ack=4933 Win=131072 Len=0	
243	2023/190	15:19:06.827811	10.10.1.252	20.43.150.84	TLSv1.3	134 Change Cipher Spec, Application Data	
244	2023/190	15:19:06.831017	10.10.1.252	20.43.150.84	TLSv1.3	134 Application Data	
245	2023/190	15:19:06.831213	10.10.1.252	20.43.150.84	TCP	1466 50967 → 443 [ACK] Seq=466 Ack=4933 Win=131072 Len=1412 [TCP segment of a reassembled PDU]	
246	2023/190	15:19:06.831213	10.10.1.252	20.43.150.84	TLSv1.3	167 Application Data	
247	2023/190	15:19:06.916345	20.43.150.84	10.10.1.252	TLSv1.3	564 Application Data, Application Data	
248	2023/190	15:19:06.916345	20.43.150.84	10.10.1.252	TCP	54 443 → 50967 [ACK] Seq=5443 Ack=1878 Win=64128 Len=0	
249	2023/190	15:19:06.916345	20.43.150.84	10.10.1.252	TLSv1.3	169 Application Data, Application Data, Application Data	
250	2023/190	15:19:06.916458	10.10.1.252	20.43.150.84	TCP	54 50967 → 443 [ACK] Seq=1991 Ack=5558 Win=130560 Len=0	
251	2023/190	15:19:06.918445	10.10.1.252	20.43.150.84	TLSv1.3	85 Application Data	
252	2023/190	15:19:07.016195	20.43.150.84	10.10.1.252	TCP	54 443 → 50967 [ACK] Seq=5558 Ack=2022 Win=64128 Len=0	
253	2023/190	15:19:07.016195	20.43.150.84	10.10.1.252	TLSv1.3	533 Application Data	
254	2023/190	15:19:07.016195	20.43.150.84	10.10.1.252	TLSv1.3	85 Application Data	
255	2023/190	15:19:07.016283	10.10.1.252	20.43.150.84	TCP	54 50967 → 443 [ACK] Seq=2022 Ack=6068 Win=130048 Len=0	
256	2023/190	15:19:07.016744	20.43.150.84	10.10.1.252	TCP	54 50967 → 443 [FIN, ACK] Seq=2022 Ack=6068 Win=130048 Len=0	

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \\Device\\NPF{32C01734-C0E0-420A-8000-000000000000}
> Ethernet II, Src: Routerbo_57:c:f8e (08:55:31:57:c:f8e), Dst: Chongqin_c1:4a:7f (4c:d5:77:c1:4a:7f)
> Internet Protocol Version 4, Src: 13.107.42.12, Dst: 10.10.1.252
> Transmission Control Protocol, Src Port: 443, Dst Port: 50959, Seq: 1, Ack: 1, Len: 0
```

```
0000 4c d5 77 c1 4a 7f 08 55 31 57 cf 8e 08 00 45 00 L.w.J.U 1w...E
0010 00 28 2e 44 0a 00 79 06 90 0f 0d 6b 2a 0c 0a 0a .(.D@.y...k*...
0020 01 fc 01 bb c7 0f c8 a2 7f 61 66 e6 60 c0 50 10 .....af~.P
0030 40 01 53 e1 00 00 @.S...
```

wireshark Wi-Fi28AW71.pcapng

Packets: 1178 · Discarded: 1178 (100.0%)

Profile

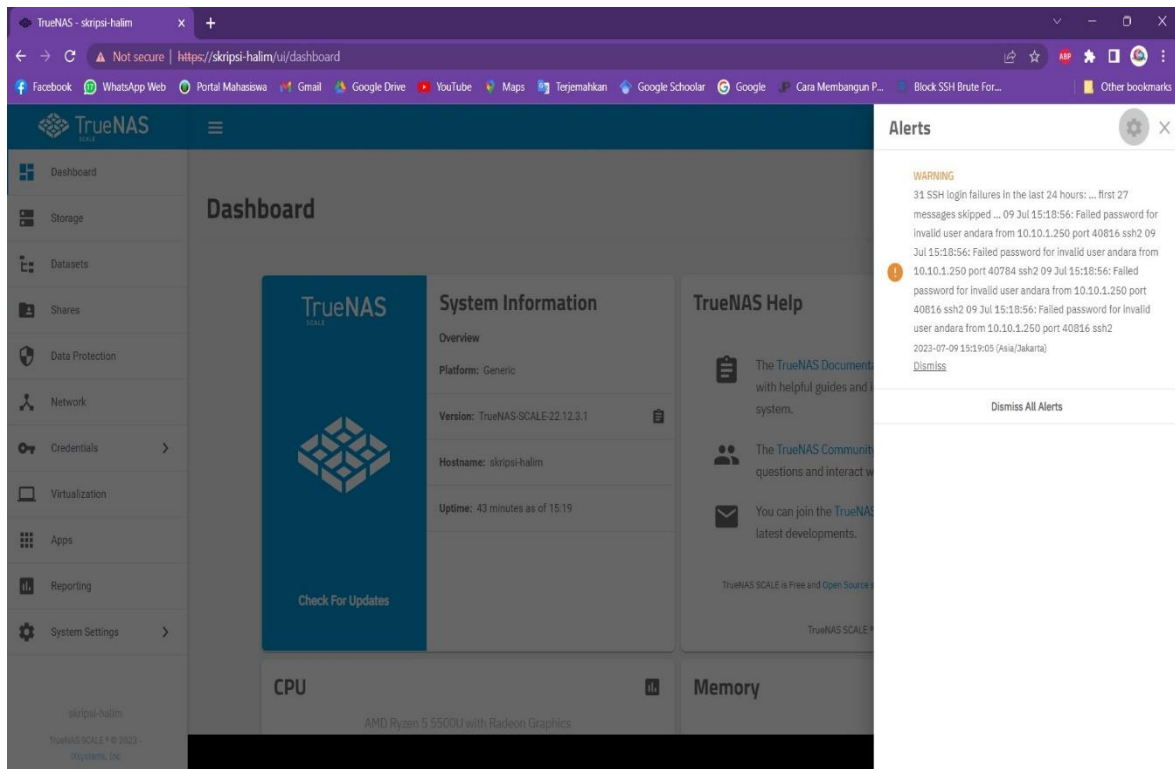
Gambar 3.8 Hasil *wireshark* serangan *brute force ssh* terhadap NAS tanpa *rule*

```

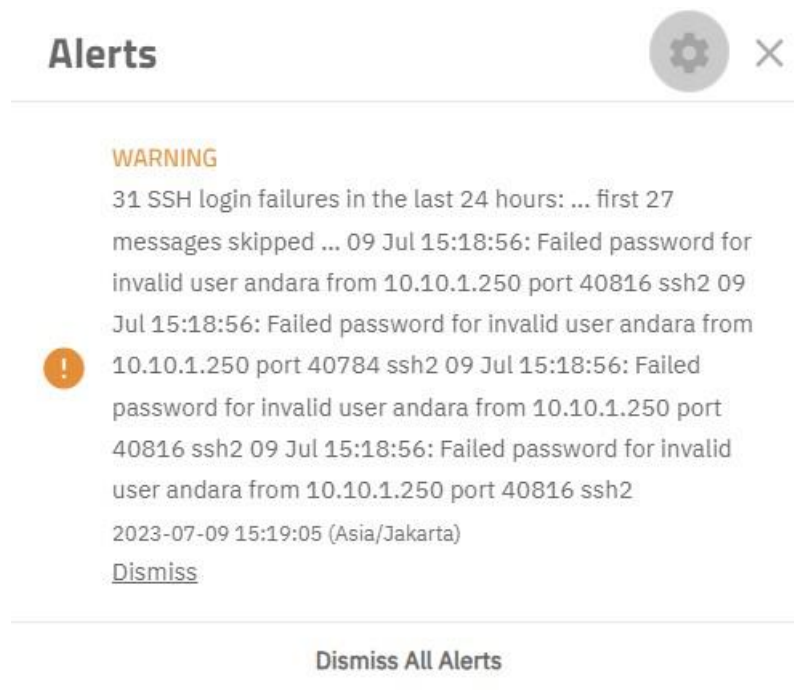
07/09-15:19:00.713488 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.8.8:53 -> 10.10.1.252:65147
07/09-15:19:00.721443 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.721555 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.875819 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.888331 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.888331 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.888331 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.888331 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.888331 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.888331 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.888331 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.888331 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 13.107.42.12:443 -> 10.10.1.252:50958
07/09-15:19:00.888331 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 13.107.42.12:443 -> 10.10.1.252:50958
07/09-15:19:00.888462 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 10.10.1.252:50958 -> 13.107.42.12:443
07/09-15:19:00.888548 [[*] [1:1000001:0] ICMP Accessed [[*] [Priority: 0] {ICMP} 10.10.1.252 -> 8.8.8.8
07/09-15:19:00.888863 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.888967 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.889109 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.889354 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.889474 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:00.899894 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.899894 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.900546 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 10.10.1.252:50966 -> 20.205.243.166:443
07/09-15:19:00.905383 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:443 -> 10.10.1.252:54633
07/09-15:19:00.925400 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:54633 -> 8.8.4.4:443
07/09-15:19:01.130909 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:52028 -> 8.8.8.53
07/09-15:19:01.142667 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 8.8.4.4:443 -> 10.10.1.252:50965
07/09-15:19:01.142815 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 10.10.1.252:50965 -> 8.8.4.4:443
07/09-15:19:01.143126 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 10.10.1.252:50965 -> 8.8.4.4:443
07/09-15:19:01.223243 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 10.10.1.252:52028 -> 8.8.4.4:53
07/09-15:19:01.247349 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 20.205.243.166:443 -> 10.10.1.252:50966
07/09-15:19:01.247469 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 10.10.1.252:50966 -> 20.205.243.166:443
07/09-15:19:01.247746 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 10.10.1.252:50966 -> 20.205.243.166:443
07/09-15:19:01.281811 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.8.8:53 -> 10.10.1.252:52028
07/09-15:19:01.305724 [[*] [1:1000002:0] UDP Accessed [[*] [Priority: 0] {UDP} 8.8.4.4:53 -> 10.10.1.252:52028
07/09-15:19:01.305791 [[*] [1:1000001:0] ICMP Accessed [[*] [Priority: 0] {ICMP} 10.10.1.252 -> 8.8.4.4
07/09-15:19:01.693712 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 8.8.4.4:443 -> 10.10.1.252:50965
07/09-15:19:01.693712 [[*] [1:1000003:0] TCP Accessed [[*] [Priority: 0] {TCP} 8.8.4.4:443 -> 10.10.1.252:50965

```

Gambar 3.9 Hasil *snort* serangan *brute force* terhadap NAS tanpa *rule*



Gambar 3.10 NAS server memberikan alert serangan pada port SSH



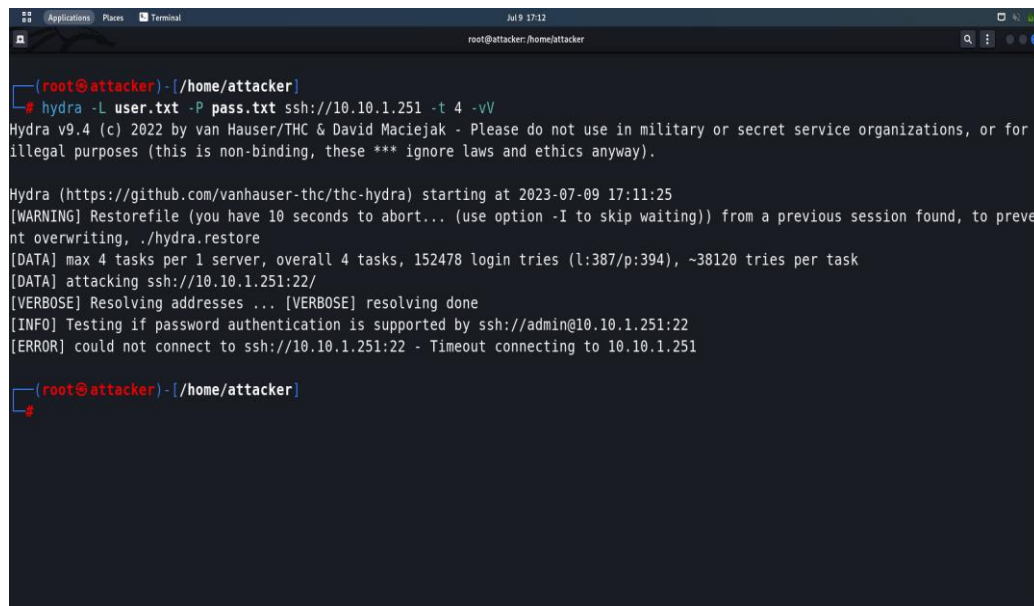
Gambar 3.11 Alert NAS server terhadap serangan pada port SSH

Pada Gambar 3.8 – 3.9 menampilkan *capture* paket data serangan menggunakan wireshark dan paket *sniffing* menggunakan *snort IDS* yang terjadi pada satu jaringan *router* yang terhubung ke NAS server. Sedangkan pada Gambar 3.10 – 3.11 menampilkan sistem *default* yang tersedia dalam NAS server secara

langsung menampilkan *alert* adanya serangan yang terjadi pada *port ssh*, meskipun penulis belum menerapkan *rule* terhadap NAS.

3.4 Pola serangan *multi attack* dengan *rule*

Pada tahap ini, penulis melakukan serangan berdasarkan *rule* yang sudah dikonfigurasi menggunakan *firewall iptables*. Berikut merupakan tahapan pola serangan sekaligus hasil pengujian terhadap NAS yang telah dilindungi oleh *rule*. Menjalankan tools *hydra* di *terminal* dan melakukan serangan terhadap *port SSH* pada NAS. *Open port SSH* pada NAS terdeteksi setelah di *nmap* dengan nilai *port 22*.



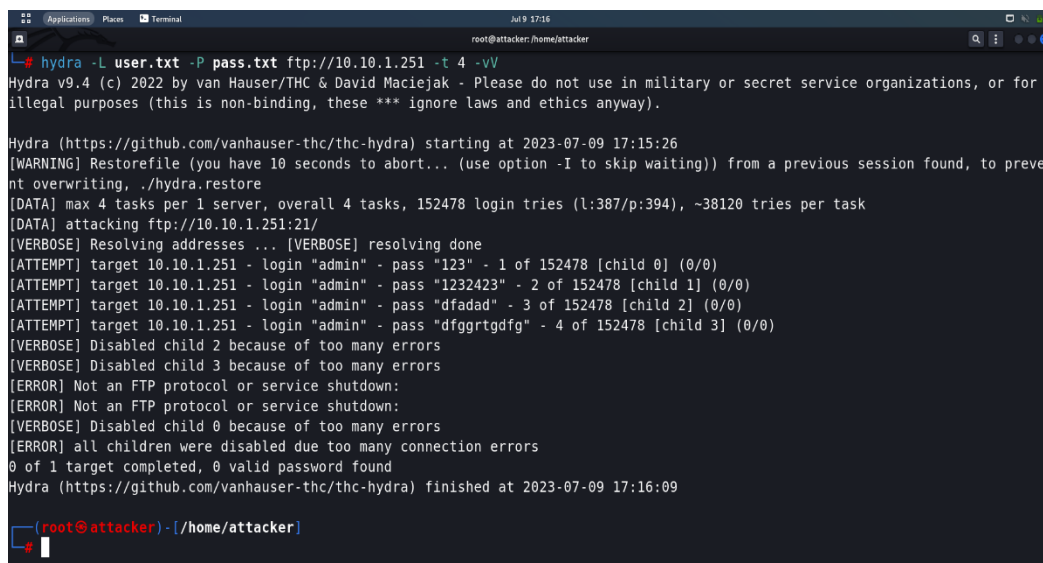
```
(root@attacker) - [/home/attacker]
# hydra -L user.txt -P pass.txt ssh://10.10.1.251 -t 4 -vv
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-09 17:11:25
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 152478 login tries (l:387/p:394), ~38120 tries per task
[DATA] attacking ssh://10.10.1.251:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://admin@10.10.1.251:22
[ERROR] could not connect to ssh://10.10.1.251:22 - Timeout connecting to 10.10.1.251

(root@attacker) - [/home/attacker]
```

Gambar 3.12 Proses Serangan *Brute Force* pada *Intruder*

Pada Gambar 4.19 menampilkan proses *serangan brute force* terhadap NAS yang terblokir akibat adanya *rule* yang di *input* pada *firewall iptables* NAS. Koneksi pada *port SSH* menampilkan hasil "*Timeout connecting to NAS IP*".



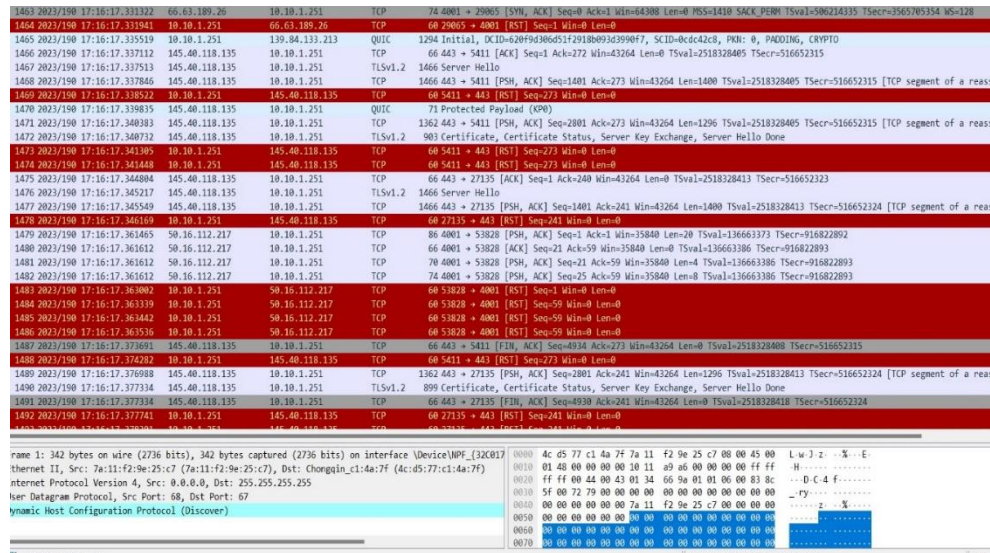
```
(root@attacker) - [/home/attacker]
# hydra -L user.txt -P pass.txt ftp://10.10.1.251 -t 4 -vv
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-09 17:15:26
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 152478 login tries (l:387/p:394), ~38120 tries per task
[DATA] attacking ftp://10.10.1.251:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "123" - 1 of 152478 [child 0] (0/0)
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "1232423" - 2 of 152478 [child 1] (0/0)
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "dfadad" - 3 of 152478 [child 2] (0/0)
[ATTEMPT] target 10.10.1.251 - login "admin" - pass "dfggrtgdfg" - 4 of 152478 [child 3] (0/0)
[VERBOSE] Disabled child 2 because of too many errors
[VERBOSE] Disabled child 3 because of too many errors
[ERROR] Not an FTP protocol or service shutdown:
[ERROR] Not an FTP protocol or service shutdown:
[VERBOSE] Disabled child 0 because of too many errors
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-09 17:16:09

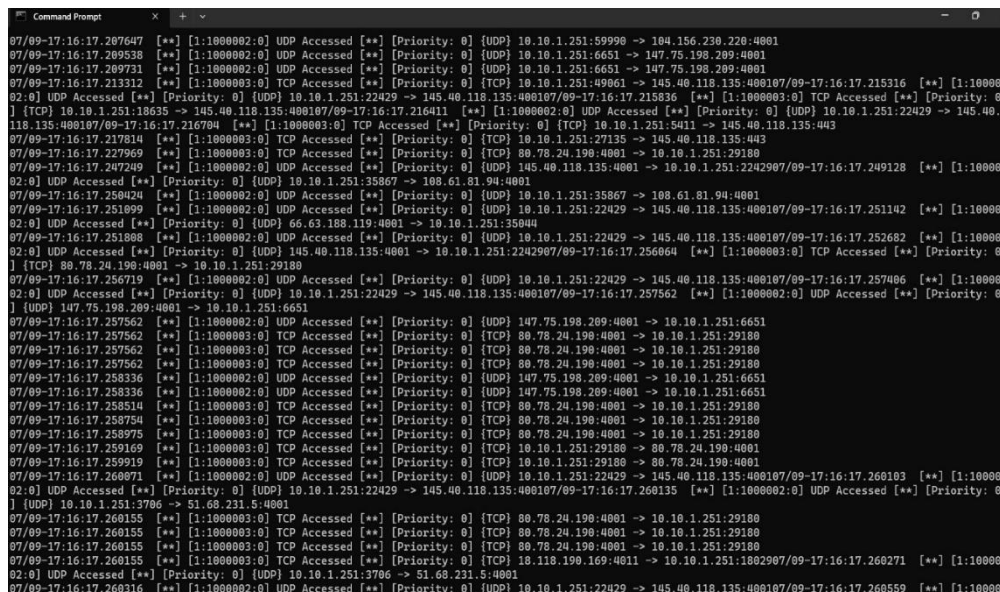
(root@attacker) - [/home/attacker]
```

Gambar 3.13 Serangan *brute force* terhadap *port FTP* pada NAS dengan *rule*

Pada Gambar 3.13 menampilkan proses serangan *brute force* yang dilakukan *intruder* terhadap *port FTP* pada NAS yang sudah diberikan *rule* pada *firewall iptables*. Hasil diatas menampilkan serangan yang masuk dan dideteksi oleh *firewall iptables* secara langsung diblokir aksesnya pada *port 21 (FTP port)*.



Gambar 3.3 Hasil *wireshark* serangan *brute force port ftp* dengan *rule*



Gambar 3.4 Hasil *snort* serangan *brute force port ftp* dengan *rule*

Pada Gambar 3.14 – 3.15 menampilkan hasil *capture data* pada *wireshark* dan *packet sniffing* menggunakan *snort IDS* terhadap serangan *brute force port ftp* pada NAS.

4. KESIMPULAN

Dari hasil serangan diatas, maka penulis mendapatkan hasil akurasi *rule based* terhadap serangan *multi-attack* yang diperoleh dari *data* 8 kali serangan yang dikumpulkan dan dikonversi kedalam nilai persen yang terlebih dahulu mencari nilai presisi menggunakan rumus sebagai berikut:

$$\text{Presisi} = (\text{TP}) / \text{TP} + \text{FP}$$

Keterangan:

TP = True Positive: Jumlah *data* serangan yang terdeteksi oleh sistem (*hasil wireshark*)

FP = False Positive: Jumlah serangan yang salah terdeteksi oleh sistem (aktivitas normal yang didefenisikan sebagai serangan)

Nilai Presisi yang didapatkan yaitu :

$$\text{Presisi} = 8 / 8 + 1 = 0,888889$$

Kemudian penulis mencari nilai dari sensitivitas dari *data* serangan yang diperoleh dari pengujian menggunakan rumus sebagai berikut:

$$\text{Sensitivitas} = (\text{TP}) / \text{TP} + \text{FN}$$

Keterangan:

TP = True Positive: Jumlah *data* serangan yang terdeteksi oleh sistem (*hasil wireshark*)

FN = False Negative: Jumlah serangan yang sebenarnya terjadi tetapi tidak terdeteksi oleh sistem (serangan yang didefenisikan sebagai aktivitas normal)

Nilai Sensitivitas yang didapatkan yaitu :

$$\text{Sensitivitas} = 8 / 8 + 2 = 0,8$$

Kemudian pada fase akhir penulis mencari nilai F1-Score menggunakan rumus sebagai berikut :

$$\text{F1-Score} = 2 * (\text{Presisi} * \text{Sensitivitas}) / (\text{Presisi} + \text{Sensitivitas}) * 100$$

Nilai F1- Score yang didapatkan yaitu :

$$\text{F1-Score} = 2 * (0,888889 * 0,8) / (0,888889 + 0,8) = 0,842105 * 100 = 84 \%$$

Berdasarkan penelitian dan analisis keseluruhan yang telah dilakukan pada NAS *server*, dapat disimpulkan bahwa:

1. IP pada NAS *server* yang diuji bersifat *random*, dikarenakan NAS menggunakan IP DHCP sebagai IP *interface*-nya.
2. *Rule base* pada *firewall* sangat berpengaruh pada serangan *multi-attack* yang diterima pada NAS, dikarenakan jika tidak ada aturan pada *firewall* maka sistem pada NAS ini sangat rentan diserang oleh serangan *brute-force* dan *a denial of service* (DDoS).
3. Akurasi *rule-based* terhadap serangan *multi-attack* pada NAS didapatkan sebesar 84% berhasil memblokir serangan dan 16% gagal memblokir serangan yang diperoleh dari nilai *true positive* (TP) yang merupakan *data* dari 8 kali pengujian dengan perbandingan 100%. Terdapat nilai *false positive* (FP) yang merupakan 1 paket lalu lintas *data* normal yang salah didefenisikan oleh sistem sebagai serangan. Dan terdapat nilai *false negative* (FN) yang merupakan 2 paket lalu lintas *data* serangan yang sebenarnya terjadi tetapi salah didefenisikan oleh sistem sebagai lalu lintas normal.
4. *Rule base* berhasil memblokir serangan *multi-attack*.
5. *Database* pada sistem NAS hanya dibuka menggunakan CLI *linux*, tidak dari *interface* NAS.

REFERENCES

- [1] K. I. Santoso and M. A. Muin, "Implementasi Network Attached Storage (NAS) Menggunakan NAS4Free untuk Media Backup File," *Scientific Journal of Informatics*, vol. 2, no. 2, p. 123, 2018, doi: 10.15294/sji.v2i2.5078.
- [2] M. A. P. Subali and C. Fatichah, "Kombinasi Metode Rule-Based dan N-Gram Stemming untuk Mengenali Stemmer Bahasa Bali," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 2, p. 219, 2019, doi: 10.25126/jtiik.2019621105.
- [3] C. Grosan and A. Abraham, "Rule-Based Expert Systems.," *Intelligence Systems Reference Library*, vol. 17, pp. 655–697, 2018, doi: 10.1007/978-3-642-21004-4_7.
- [4] M. Kadapi, "FORENSIC SERANGAN BRUTE FORCE PADA PUBLIC CLOUD DENGAN METODE RULE BASE," Universitas Sriwijaya, 2021.
- [5] I. Gunawan, "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss," *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, vol. 1, no. 1, pp. 52–55, 2016, doi: 10.30743/infotekjar.v1i1.48.
- [6] B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS Attacks and Desirable Defense Mechanism in a Cloud Computing Environment," *Neural Computing & Application*, vol. 28, no. 12, pp. 3655–3682, 2018, doi: 10.1007/s00521-016-2317-5.
- [7] T. M. Diansyah, I. Faisal, A. Perdana, B. O. Sembiring, and T. H. Sinaga, "Analysis of Using Firewall and Single Honeypot in Training Attack on Wireless Network," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Dec. 2017. doi: 10.1088/1742-6596/930/1/012038.
- [8] Y. Mulyanto, Herfandi, and R. C. Kirana, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR)," *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401.
- [9] N. P. D. R. R. Ida Ayu Mas Putri Mahalini, Ida Bagus Kusuma, Dewantara, N. M. Mahardika, Listartha, I. M. E. Saskara, and G. A. Jude, "ANALISIS KELAYAKAN TOOLS DENGAN METODE PENYERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) MENGGUNAKAN FL00D3R, DDOS-RIPPER, DAN RAVEN-STORM," *Jurnal Teknologi Informasi*, vol. 6, no. 2, Dec. 2022.
- [10] I. P. A. E. Pratama and P. A. Dharmesta, "Implementasi Wireshark Dalam Melakukan Pemantauan Protocol Jaringan (Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana)," *Mantik Penusa*, vol. 3, no. 1, pp. 94–99, 2019.
- [11] M. Fldr, D. A. N. Raven-storm, M. Mahardika, I. M. E. Listartha, G. Arna, and J. Saskara, "Analisis Kelayakan Tools Dengan Metode Penyerangan Distributed Denial of Service (Ddos)," vol. 6, no. 2, pp. 278–285, 2022.
- [12] P. Bedi and A. Dua, "Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet," *Procedia Comput Sci*, vol. 171, pp. 1810–1818, 2020, doi: 10.1016/J.PROCS.2020.04.194.
- [13] A. Ligeza, *Logical Foundations for Rule-Based Systems*, 2nd editio. Springer, 2020.
- [14] I. H. Sembodo, "Password Cracking menggunakan Brute Force Attack IF2211 Strategi Algoritma," 2019.