MODUL 5

MOBILE HACKING

5.1 Tujuan Praktikum

1. Mengetahui dan memahami definisi dan konsep *mobile hacking.*
2. Mengetahui dan memahami teknik dan *tools hacking* pada *mobile device.*
3. Mengetahui dan memahami jenis serangan *mobile hacking.*
4. Mengetahui dan memahami cara menjaga keamanan *mobile device.*
5. Mengenal kerentanan pada *mobile device.*

5.2 Alat dan Bahan

1. Laptop
2. *VirtualBox*
3. Kali Linux
4. *Ngrok*
5. *Strom Breaker*
6. *Metasploit*

5.3 Dasar Teori

5.3.1 Definisi dan Konsep Dasar Mobile Hacking

Mobile hacking adalah eksploitasi perangkat *mobile* dengan tujuan memperoleh akses ilegal ke dalam sistem perangkat untuk mencuri data, memata-matai, atau merusak perangkat itu sendiri atau praktik yang melibatkan metode dan teknik untuk mendapatkan akses tidak sah ke perangkat *mobile*,

seperti *smartphone* atau tablet. Konsep ini mencakup berbagai bentuk serangan yang dapat dilakukan oleh peretas untuk mencuri data, mengakses informasi pribadi, atau mengendalikan perangkat secara jarak jauh. Seiring dengan meningkatnya ketergantungan pada perangkat *mobile* seperti *smartphone* dan tablet, risiko terhadap ancaman *mobile hacking* pun semakin tinggi. Ponsel pintar saat ini berfungsi lebih dari sekadar alat komunikasi; mereka digunakan untuk perbankan, menyimpan data sensitif, dan mengakses sistem organisasi atau perusahaan.

Teknologi perangkat *mobile* terus berkembang dengan cepat, tetapi hal ini juga disertai dengan peningkatan dalam hal kompleksitas ancaman keamanan. *Mobile hacking* biasanya memanfaatkan kelemahan dalam perangkat keras, perangkat lunak, atau pengguna perangkat yang kurang memahami keamanan digital. Seiring dengan adopsi teknologi *Internet of Things* yang juga sering dikendalikan lewat perangkat mobile, risiko yang berkaitan dengan *mobile hacking* terus meningkat.

5.3.1.1 Tenik – Teknik Dalam *Mobile Hacking*

1. *Malware injections* merupakan metode di mana penyerang menyusupkan perangkat lunak berbahaya ke dalam perangkat *mobile*. Ini sering dilakukan melalui aplikasi berbahaya yang diunduh dari toko aplikasi tidak resmi atau melalui file yang diunduh dari internet. Setelah diinstal, *malware* dapat mengambil alih kontrol perangkat, mencuri data sensitif, atau mengubah pengaturan perangkat. Contoh *malware* ini termasuk *trojan, ransomware, dan spyware.*
2. *Zero-day exploits* adalah memanfaatkan kerentanan perangkat atau sistem operasi yang belum diketahui oleh pengembang. Karena kerentanan ini belum ditangani, penyerang dapat menggunakannya untuk mendapatkan akses tidak sah ke perangkat atau data. Teknik ini sangat berbahaya karena sering kali sulit untuk dideteksi dan bisa menyebabkan kerusakan besar sebelum ada *patch* atau solusi yang tersedia.

3. *Mobile-based phishing* adalah taktik di mana peretas menggunakan pesan teks (SMS), email, atau aplikasi palsu untuk menipu pengguna agar memberikan informasi pribadi, seperti kata sandi atau nomor kartu kredit. Misalnya, penyerang dapat mengirim pesan yang tampak resmi dari bank yang meminta pengguna untuk mengklik tautan dan mengisi detail akun mereka. Teknik ini memanfaatkan psikologi manusia untuk menciptakan rasa urgensi atau ketakutan.
4. *Botnet* adalah jaringan perangkat mobile yang telah diretas dan dikendalikan secara jarak jauh oleh penyerang. Perangkat ini dapat digunakan untuk melancarkan serangan *Distributed Denial of Service* (DDoS), di mana banyak perangkat secara bersamaan mengirimkan permintaan ke server tertentu, membuatnya tidak dapat diakses. Selain itu, botnets juga dapat digunakan untuk melakukan aktivitas jahat lainnya, seperti penyebaran *malware* atau pengambilan data secara massal.

5.3.1.2 Tools *Hacking Mobile*

1. ***Ngrok***

Ngrok merupakan alat yang digunakan untuk memaparkan *server* lokal yang berada di belakang NAT dan *firewall* ke internet publik melalui terowongan aman. Dengan menggunakan *Ngrok*, kita dapat mengarahkan akses dari internet ke dalam jaringan lokal kita. Informasi yang diberikan mencakup port tempat server web kita melakukan proses penerimaan (*listen*). Ngrok beroperasi dengan cara mengunduh dan mengeksekusi program di mesin pengguna, lalu menyediakan port layanan jaringan, yang umumnya digunakan untuk

server web. Port ini akan terkoneksi dengan layanan *cloud Ngrok*, yang menerima lalu lintas melalui alamat publik, kemudian meneruskannya ke proses Ngrok yang berjalan di mesin pengguna, dan akhirnya menuju alamat lokal yang telah ditentukan.

2. ***Storm-Breaker***

Strom-Breaker adalah alat rekayasa sosial yang kuat yang memungkinkan peretas mengakses lokasi, kamera, mikrofon korban. Namun, dengan menggunakan *storm-breaker* untuk beberapa pekerjaan seperti melacak dan mencatat alamat IP, mengakses *feed* kamera, mengakses *feed* mikrofon, dan mengetahui lokasi perangkat yang tepat

3. ***Metasploit***

Metasploit merupakan *framework* yang digunakan untuk keamanan dan *hacker* dalam menguji keamanan sistem melalui penetration testing, termasuk pada perangkat *mobile*. Dalam konteks *mobile hacking*, *Metasploit* dapat digunakan untuk mengeksploitasi perangkat *Android* dengan memanfaatkan celah keamanan pada aplikasi atau sistem operasi, misalnya melalui pembuatan aplikasi berbahaya (APK) yang mengandung *payload* seperti Meterpreter untuk akses jarak jauh. Selain itu, *Metasploit* bisa melakukan serangan *Man-in-the-Middle* (MitM) untuk mencegat dan memanipulasi data di

jaringan WiFi, serta mengeksploitasi kerentanan aplikasi *mobile*. Meskipun sering dikaitkan dengan *hacking*. *Metasploit* sebenarnya berfungsi sebagai alat untuk membantu peneliti dan perusahaan mengidentifikasi serta memperbaiki celah keamanan sebelum disalahgunakan oleh pihak lain.

5.3.2 Jenis Ancaman dan Serangan *Mobile Hacking*

Ada banyak jenis ancaman yang dapat menargetkan perangkat *mobile*, dan masing-masing ancaman tersebut bisa memiliki dampak yang merugikan baik bagi pengguna pribadi maupun organisasi besar. Berikut adalah beberapa ancaman paling umum yang dihadapi oleh perangkat *mobile*:

1. *Mobile malware* adalah perangkat lunak berbahaya yang dirancang khusus untuk menyerang perangkat *mobile*. Ancaman ini dapat bervariasi dalam jenis dan fungsi, tetapi umumnya bertujuan untuk melakukan aktivitas merugikan bagi pengguna, seperti mencuri data atau merusak perangkat.
2. *Trajon* adalah jenis *malware* yang berpura-pura sebagai aplikasi yang sah. Namun, saat diunduh dan di-*install*, *trojan* dapat melakukan aktivitas jahat di latar belakang, seperti mencuri data pengguna, mengambil alih kontrol perangkat, atau menginstal perangkat lunak berbahaya lainnya. Pengguna sering kali tidak menyadari bahwa mereka telah terpengaruh hingga kerusakan sudah terjadi.
3. *Spyware* adalah aplikasi yang dirancang untuk mengumpulkan informasi pribadi pengguna tanpa sepengetahuan mereka. Ini termasuk data sensitif seperti kata sandi, kontak, pesan, atau lokasi geografis. *Spyware* dapat membahayakan privasi pengguna dan digunakan untuk penipuan identitas atau pencurian data.
4. *Ransomware* adalah jenis *malware* yang mengenkripsi file di perangkat pengguna dan meminta tebusan untuk membuka akses kembali. Serangan ini bisa sangat merusak, terutama jika data penting dikunci dan tidak ada cara untuk memulihkannya tanpa membayar tebusan.

5. *Wi-Fi Hacking* Perangkat mobile yang terhubung ke jaringan Wi-Fi publik rentan terhadap serangan *Man in the Middle* (MitM). Dalam serangan ini, peretas dapat memantau dan mengubah data yang dikirimkan antara perangkat dan *server*. Pengguna yang tidak menyadari kerentanan ini mungkin melanjutkan aktivitas sensitif, seperti perbankan online, yang dapat disadap oleh peretas.
6. *Man in the Middle Attack* Serangan ini terjadi ketika peretas mencegat komunikasi antara dua pihak. Dalam konteks *mobile*, ini sering terjadi melalui jaringan Wi-Fi publik atau koneksi *bluetooth* yang tidak aman. Peretas dapat menyusup ke dalam komunikasi dan mengubah data yang dikirim, membuat pengguna percaya bahwa mereka sedang berkomunikasi dengan pihak yang sah.
7. *Phishing dan SMiShing* di perangkat *mobile* sering dilakukan melalui pesan teks (SMiShing) atau *email* yang tampak resmi tetapi sebenarnya berisi tautan berbahaya. Jika pengguna mengklik tautan tersebut, mereka akan diarahkan ke situs *web* palsu yang dirancang untuk mencuri informasi *login* atau data pribadi lainnya. Taktik ini memanfaatkan kepercayaan pengguna dan tampilan otoritas.
8. *Exploit Operating System*, Kerentanan dalam sistem operasi seperti *Android* atau *iOS* dapat menjadi pintu masuk bagi peretas. Misalnya, bug dalam kode dapat memungkinkan peretas untuk menjalankan kode berbahaya di perangkat tanpa sepengetahuan pengguna. Banyak eksploitasi yang dieksploitasi dalam serangan besar berasal dari sistem operasi yang belum diperbarui dengan patch keamanan terbaru.
9. *SIM swapping* adalah teknik di mana peretas memanipulasi penyedia layanan telekomunikasi untuk memindahkan nomor telepon korban ke kartu SIM yang mereka kendalikan. Setelah mendapatkan kontrol atas nomor telepon tersebut, peretas dapat mengakses akun yang menggunakan autentikasi dua faktor berbasis SMS, seperti akun bank atau akun media sosial, sehingga meningkatkan risiko pencurian identitas.

5.3.3 Cara Mencegah Serangan Mobile Hacking

Untuk melindungi perangkat *mobile* dari ancaman *hacking*, pengguna perlu menerapkan berbagai langkah keamanan yang dirancang untuk mencegah atau memitigasi dampak serangan. Beberapa langkah pencegahan penting meliputi:

1. Menginstal Aplikasi dari Sumber Resmi: Hanya mengunduh aplikasi dari toko aplikasi resmi seperti *Google Play Store* dan *Apple App Store*. Aplikasi yang diunduh dari sumber tidak tepercaya lebih cenderung mengandung *malware* atau aplikasi berbahaya.
2. Perbarui Sistem dan Aplikasi Secara Rutin: Pengembang sistem operasi dan aplikasi sering kali merilis pembaruan yang mencakup patch keamanan untuk memperbaiki kerentanan yang ditemukan. Pengguna harus memastikan bahwa perangkat mereka selalu diperbarui untuk melindungi dari *exploit* terbaru.
3. Gunakan VPN Saat Mengakses Jaringan Publik: *Virtual Private Network* (VPN) mengenkripsi lalu lintas internet pengguna, yang membuatnya lebih sulit bagi peretas untuk melakukan serangan *Man in the Middle* (MitM) saat perangkat terhubung ke Wi-Fi publik.
4. Aktifkan Fitur Autentikasi Dua Faktor (2FA): Autentikasi dua faktor memberikan lapisan perlindungan tambahan terhadap akun penting dengan meminta kode verifikasi tambahan setelah pengguna memasukkan kata sandi. Kode ini biasanya dikirim melalui SMS, email, atau aplikasi autentikasi seperti *Google Authenticator*.
5. Nonaktifkan Wi-Fi, bluetooth, dan NFC Ketika Tidak Digunakan: Beberapa serangan, terutama yang melibatkan bluetooth dan Wi-Fi, dapat dilakukan pada perangkat *mobile* yang memiliki koneksi tersebut aktif secara terus-menerus. Sebaiknya matikan koneksi yang tidak sedang digunakan untuk mengurangi peluang serangan.
6. Gunakan Aplikasi Keamanan *Mobile*: Aplikasi keamanan *mobile*, seperti *anti-virus* dan *anti-malware*, bisa membantu mendeteksi dan mencegah instalasi *malware* pada perangkat. Aplikasi ini juga memberikan perlindungan terhadap *phishing* dan situs *web* berbahaya.

5.3.4 Solusi Serangan *Mobile Hacking*

Jika perangkat *mobile* diretas atau dicurigai telah disusupi, ada beberapa langkah yang bisa diambil untuk mengamankan kembali perangkat dan mengurangi kerugian:

1. Hapus Aplikasi yang Mencurigakan: Jika perangkat menunjukkan perilaku aneh atau aplikasi yang mencurigakan diidentifikasi, segera hapus aplikasi tersebut. Aplikasi yang jarang digunakan juga sebaiknya dihapus untuk mengurangi risiko serangan di masa depan.
2. Reset Pengaturan Pabrik: Pada kasus di mana perangkat sudah tidak dapat diakses atau perangkat lunak jahat terlalu sulit untuk dihapus, mereset perangkat ke pengaturan pabrik bisa menjadi solusi terakhir. Namun, tindakan ini akan menghapus semua data di perangkat, jadi pastikan untuk melakukan backup terlebih dahulu.
3. Mengubah Kata Sandi dan Kredensial Penting: Setelah serangan, penting untuk segera mengubah semua kata sandi yang terkait dengan perangkat dan aplikasi penting, seperti akun email, akun media sosial, dan akun perbankan.
4. Laporkan kepada Pihak Berwenang atau Penyedia Layanan: Jika serangan melibatkan informasi pribadi yang penting, segera laporkan insiden tersebut kepada penyedia layanan terkait, seperti bank atau penyedia layanan telekomunikasi. Jika serangan melibatkan pencurian identitas, hubungi pihak berwenang setempat.