ETHICAL HACKING

Strategi Pencegahan Ancaman Siber

Ethical hacking adalah aktivitas pengujian keamanan sistem komputer, jaringan, atau aplikasi secara legal, terkontrol, dan berizin, dengan tujuan menemukan celah keamanan sebelum disalahgunakan oleh pihak yang tidak bertanggung jawab.

White Hat

- Bekerja secara legal dan profesional.
- Menguji sistem untuk tujuan perlindungan.
- Biasanya bekerja di instansi pemerintah, perusahaan, atau sebagai konsultan keamanan.

Grey Hat

- Berada di antara White Hat dan Black Hat.
- Tidak selalu berniat jahat, namun sering melanggar aturan atau izin.
- Tidak mengikuti prosedur hukum dan etika secara penuh

Black Hat

- Menyerangtanpa izin.
- Mencuri data, merusak sistem, atau melakukan penipuan.
- Mengancam keamanan dan stabilitas digital.
- Menyembunyikan jejak serangan untuk menghindari pelacakan.

Ethical hacking berperan penting dalam:

- Mengidentifikasi celah keamanan sejak dini
- Memberikan rekomendasi perbaikan sistem
- Mendukung keberlanjutan sistem digital
- Kesiapan menghadapi serangan siber

Tips Praktis Keamanan Digital untuk Semua Orang

🔐 Gunakan password kuat dan berbeda pada setiap akun

📲 Aktifkan autentikasi dua faktor (2FA)

🎣 Waspada terhadap phishing dan pesan mencurigakan

🔄 Perbarui sistem dan aplikasi secara rutin

📶 Hindari penggunaan Wi-Fi publik tanpa perlindungan

DISKOMINFOS PROVINSI BALI
PROGRAM LITERASI KESADARAN KEAMANAN SIBER
Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?
Ayo berlangganan KABAR LENTERA (GRATIS !) di https://balikom.info/kabarlentera

SECURITY IS INCOMPLETE WITHOUT U #JagaRuangSiber
LENTERA SIBER
SAYA NETIZEN CERDAS

DISKOMINFOS.BALIPROV.GO.ID | diskominfosbali | diskominfos_bali | lenterasiber | balikom.info/link/lenterasiber
TLP: CLEAR

Balai Besar Sertifikasi Elektronik
Dokumen ini telah ditandatangani secara elektronik (TTE).
Scan/Klik QR Code untuk informasi TTE.
Upload file pada https://tte.komdigi.go.id/verifyPDF untuk cek keaslian file.
BANGGA BUATAN INDONESIA
BANGGA BERWISATA DI INDONESIA