PERKAKAS PERETAS

Kelompok: _____

Anggota : 1. _____

2. _____

3. _____

TUJUAN PEMBELAJARAN

Setelah mengikuti pembelajaran, peserta didik diharapkan mampu:

1. Peserta didik mampu menjelaskan keamanan data dan informasi.
2. Peserta didik mampu menjelaskan ancaman terhadap keamanan data yang dapat terjadi ketika menggunakan perangkat lunak.
3. Peserta didik mampu menganalisis dan mengevaluasi ancaman kejahatan di internet.

PEMBERIAN STIMULUS

Perhatikan video berikut ini

MERUMUSKAN MASALAH

Buatlah pertanyaan yang muncul dipikiranmu setelah menonton video di atas.

Buatlah jawaban sementara dari pertanyaan kamu di atas

MENGUMPULKAN DATA

Kerjakanlah soal-soal berikut dengan memilih jawaban di samping!

Peretas yang menggunakan keahlian mereka untuk mencari celah keamanan atau potensi kerawanan untuk meningkatkan keamanan sistem. Peretas ini meminta izin ketika akan melakukan penetrasi ke sistem dan akan memberikan peringatan dini tentang potensi ancaman. Peretas ini termasuk pakar keamanan siber yang berusaha keras untuk melindungi sistem yang menggunakan etika dalam bekerja.

Peretas yang menggunakan keahlian mereka untuk merusak, tidak memiliki etika yang baik, serta melakukan penetasi tanpa izin dan ilegal. Dia sering mencuri, mengeksploitasi, dan menjual data untuk mendapatkan keuntungan pribadi.

Peretas yang merupakan kategori tengah. Mereka mungkin berusaha untuk memperbaiki dan mengeksploitasi kelemahan sistem dengan tanpa mendapatkan keuntungan finansial. Namun, pekerjaan mereka tetap akan menjadi hal yang tidak legal jika tidak memberitahukannya ke pemilik sistem

Jodohkanlah pernyataan berikut dengan jenis perkakas peretasnya!

Perangkat lunak yang menempel pada perangkat lunak lain dan mampu mereplikasi diri sendiri	Trojan horse
Perangkat lunak yang tidak perlu menempel ke program lain agar dapat berfungsi dan dirancang untuk mengeksploitasi kelemahan sistem tertentu	Ransomware
Malware yang tampak seperti aplikasi perangkat lunak jinak, tetapi perangkat lunak ini membawa komponen yang jahat di dalamnya	Virus
Peretasan yang melakukan manipulasi pengguna, seperti meminta orang untuk mengeluarkan informasi atau melakukan tugas yang melanggar protokol keamanan.	Worm
Target dihubungi melalui surel, telepon, atau pesan teks oleh seseorang yang menyamar dari lembaga yang sah agar memberikan data sensitif seperti informasi pribadi, detail data perbankan atau kartu kredit dan kredensialnya	Spyware
Memikat pengguna internet untuk masuk ke situs web palsu dan mencuri data pribadi penggunanya	Pharming
Malware yang dapat memantau dan merekam aktivitas pengguna di komputer atau perangkat seluler, termasuk mencatat penekanan tombol pada keyboard	Phising
Malware yang mampu mengenkripsi file di komputer atau perangkat seluler dan menampilkan pesan menuntut pembayaran kunci untuk mendekripsi file	Rekayasa sosial

MENGUMPULKAN DATA

Kelompokkanlah contoh-contoh perkakas peretas ke jenisnya dengan benar!

Virus	Worm	Ransomware	Spyware

Tempelkanlah nama-nama berikut ke kotak di atas sesuai jenisnya!

MENGOLAH DATA

Dari aktivitas sebelumnya, buatlah penjelasan mengenai video yang sudah kamu tonton tadi

Apa jenis *malware* yang meretas Pusat Data Nasional Sementara sehingga beberapa aktivitas instansi pemerintahan di Indonesia lumpuh.

Berilah penjelasan!

Apa nama malware yang menyerang PDNS tersebut!

VERIFIKASI

Pada tahap ini satu kelompok akan mempresentasikan mengenai permasalahan yang ada dari video

MERUMUSKAN KESIMPULAN

Apakah kesimpulan dari pembelajaran kita hari ini?

LATIHAN

Kerjakanlah latihan berikut!

Kasus I

Kasus yang terjadi pada tahun 2016 menargetkan karyawan Crelan Bank. Pelaku menyamar menjadi CEO Crelan Bank dan mengirimkan e-mail kepada karyawan untuk mengirimkan e-mail ke rekeningnya. Karyawan tersebut tidak curiga karena mereka berasumsi e-mail tersebut benar-benar dikirimkan oleh CEO Crelan Bank. Kasus ini terkuak setelah Crelan Bank melakukan internal audit dan melaporkan kerugian sebesar 75 juta dolar.

Apakah perkakas peretas yang digunakan pelaku?

Jelaskan alasannya!

Kasus II

Kasus BSI bermula pada 8 Mei 2023 ketika para nasabah tidak dapat melakukan transaksi. Awalnya, BSI mengumumkan bahwa gangguan tersebut terkait dengan pemeliharaan sistem. Namun, masalah tak kunjung selesai dalam beberapa hari. Kemudian pada 10 Mei, BUMN membuat pernyataan bahwa BSI terkena serangan cyber. Hal itu disusul oleh klaim LockBit yang mengaku bertanggung jawab atas kejadian tersebut. LockBit menuntut tebusan Rp200 miliar lebih dengan ancaman membocorkan 1,5 TB data pelanggan. Tawar menawar gagal. BSI akhirnya memilih untuk fokus memulihkan sistem mereka dan menjamin tidak ada data yang bocor.

Apakah perkakas peretas yang digunakan pelaku?

Jelaskan alasannya!