RENCANA PELAKSANAAN PEMBELAJARAN		
Nama Sekolah	:	MTs Ahmad Yani Jabung
Nama Guru	:	Muhammad Badrul Huda, S.Pd
Mata Pelajaran	:	Informatika
Kelas/Semester	:	IX - A / 2
Alokasi Waktu	:	2 x 40 Menit`

1. Identifikasi

Peserta didik: Siswa kelas IX diasumsikan telah memahami dasar-dasar jaringan komputer dan konsep keamanan data. Kesiapan belajar difokuskan pada pemahaman etika penggunaan teknologi sebelum mendalami perkakas spesifik.
Materi Pelajaran: Perkakas peretasan
Dimensi Profil Lulusan: Keimanan dan Ketakwaan terhadap Tuhan YME, Penalaran Kritis, Komunikasi, Cinta kepada Ilmu Pengetahuan, Cinta kepada Bangsa dan Negeri

2. Desain Pembelajaran

Capaian Pembelajaran: Peserta didik mampu mengidentifikasi dan menjelaskan fungsi dasar perkakas yang digunakan untuk pengujian keamanan (penetration testing) secara etis dan bertanggung jawab.
Lintas Disiplin Ilmu: Pendidikan Kewarganegaraan (Etika Digital dan Hukum Siber), Bahasa Indonesia (Penyusunan Laporan dan Komunikasi Ilmiah), Matematika (Analisis data dan algoritma enkripsi dasar)
Kemitraan Pembelajaran: Praktisi Keamanan Siber Lokal (sebagai narasumber), Komunitas IT/Ethical Hacking, Institusi Kepolisian (untuk konteks hukum)
Tujuan Pembelajaran:

1. Menjelaskan perbedaan antara peretasan etis (ethical hacking) dan peretasan ilegal (black hat hacking) dengan mengaitkannya pada nilai ketakwaan.
2. Mengidentifikasi minimal tiga jenis perkakas dasar yang digunakan untuk menganalisis keamanan jaringan (misalnya Nmap, Wireshark).
3. Menganalisis potensi risiko dan manfaat dari penggunaan perkakas pengujian keamanan.
4. Mengomunikasikan hasil analisis risiko secara lisan dan tertulis dengan jelas (Komunikasi dan Penalaran Kritis).

Topik Pembelajaran: Konsep dasar Ethical Hacking, Pengenalan Perkakas Penetration Testing (Nmap & Wireshark sebagai contoh), dan Regulasi Keamanan Siber di Indonesia.
Model: Problem-Based Learning, Project-Based Learning (simulasi studi kasus)
Metode: Diskusi Kelompok, Studi Kasus (Simulasi), Presentasi, Demonstrasi

3. Pengalaman Belajar

Kegiatan Awal:

- Guru memulai pelajaran dengan salam, doa, dan pengecekan kehadiran (Keimanan dan Ketakwaan).
- Guru melakukan Asesmen Awal tentang pemahaman siswa mengenai privasi data dan hukum siber.
- Guru menyampaikan relevansi materi dalam konteks keamanan siber nasional (Cinta Bangsa dan Negeri).

Kegiatan Inti:

- Orientasi Masalah: Siswa diberikan studi kasus tentang celah keamanan pada jaringan simulasi.

- Pengumpulan Data: Siswa mengidentifikasi jenis perkakas yang dapat digunakan untuk mendeteksi celah tersebut (misalnya, Nmap untuk scanning port).
- Diskusi Kelompok: Siswa membahas etika penggunaan perkakas tersebut dan menyusun kode etik kelompok (Penalaran Kritis).
- Demonstrasi/Simulasi: Guru mendemonstrasikan fungsi dasar perkakas analisis jaringan (misalnya, Nmap scanning pada IP lokal yang aman).
- Pengembangan dan Penyajian Hasil: Kelompok merumuskan rekomendasi tindakan pencegahan dan pertahanan sistem berdasarkan hasil analisis (Komunikasi).
- Penguatan Konsep: Guru menekankan bahwa penggunaan perkakas harus legal, beretika, dan berorientasi pada pertahanan sistem.

Kegiatan Penutup:

- Refleksi Siswa: Siswa menjawab pertanyaan reflektif yang diberikan guru.
- Kesimpulan: Guru dan siswa merangkum poin penting tentang tanggung jawab digital dan etika (Cinta kepada Ilmu Pengetahuan).
- Tindak Lanjut: Pemberian tugas mandiri untuk mencari undang-undang ITE yang relevan.
- Penutup: Doa bersama.

4. Asesmen Pembelajaran

Asesmen Awal: Tanya jawab lisan mengenai Undang-Undang ITE dan konsep *firewall*.
Asesmen Proses: Observasi kerja kelompok, penilaian keaktifan diskusi (Penalaran Kritis), dan ketaatan pada etika kelompok.
Asesmen Akhir: Laporan Analisis Studi Kasus (termasuk rekomendasi etis) dan Tes Tertulis (esai pendek).

Jabung, 9 Februari 2026

Mengetahui,

Kepala Madrasah	**Guru Mata Pelajaran**,
Muroihatul Jannah, M.Pd	**Muhammad Badrul Huda, S.Pd**

Lampiran 1. LKPD (Lembar Kerja Peserta Didik)

Nama	:	.....
Kelas	:	IX -
Materi	:	Perkakas peretasan

Langkah Kerja:

1. Persiapan: Pastikan semua komputer berada dalam jaringan lokal simulasi yang aman.
2. Akses Perkakas: Akses perkakas analisis jaringan yang telah disiapkan (misalnya, Nmap versi lab).
3. Identifikasi Target: Tentukan alamat IP dari perangkat yang ditargetkan (misalnya, IP router simulasi).
4. Eksekusi Perintah: Jalankan perintah dasar untuk memindai port terbuka (Contoh: `nmap -sT [IP Address]`).
5. Analisis Hasil: Catat port yang terbuka dan jelaskan potensi risiko yang ditimbulkan dari port tersebut (Penalaran Kritis).
6. Pelaporan Etis: Buat draf rekomendasi pertahanan untuk menutup celah yang ditemukan, fokus pada aspek Keamanan Data.

Pertanyaan Reflektif:

1. Bagaimana pengetahuan tentang perkakas peretasan dapat memperkuat pertahanan keamanan data pribadi Anda?
2. Jika Anda menemukan celah keamanan, apa langkah etis dan legal pertama yang harus Anda lakukan berdasarkan prinsip Keimanan?
3. Jelaskan mengapa pengembangan ilmu pengetahuan dalam bidang keamanan siber sangat penting bagi kemajuan bangsa dan negara.

Lampiran 2. Bahan Ajar

A. Ringkasan Materi

Perkakas peretasan (hacking tools) adalah perangkat lunak yang dirancang untuk menganalisis dan menguji keamanan sistem. Dalam konteks pendidikan dan profesional, perkakas ini digunakan secara etis (Ethical Hacking atau Pen Test) untuk menemukan kelemahan sebelum dieksploitasi oleh pihak tak bertanggung jawab. Contoh perkakas populer adalah Nmap (pemindai jaringan) dan Wireshark (analis lalu lintas jaringan). Penggunaan perkakas ini harus didasari izin dan tujuan yang sah, mematuhi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Tujuan utama mempelajari perkakas ini adalah untuk meningkatkan pertahanan siber, bukan melakukan kejahatan. Pemahaman yang kuat tentang etika digital adalah fondasi untuk menjadi profesional keamanan siber yang bertanggung jawab dan berkontribusi pada keamanan data nasional.

B. Sumber Belajar Tambahan

Video Pembelajaran: https://www.youtube.com/watch?v=J_jA2x3S1D8 (Pengantar Ethical Hacking dan Pentesting)
Artikel/Simulasi: https://www.kominfo.go.id/content/detail/3953/undang-undang-nomor-11-tahun-2008-tentang-informasi-dan-transaksi-elektronik/0/regulasi (Teks UU ITE untuk referensi hukum)

Lampiran 3. Instrumen Asesmen

A. Daftar Pertanyaan/Soal Tes

1. Jelaskan perbedaan prinsip antara "Black Hat Hacker" dan "White Hat Hacker" berdasarkan etika kerja.
2. Apa fungsi utama dari perkakas Nmap dan Wireshark dalam konteks pengujian keamanan jaringan?

3. Andi menemukan celah keamanan pada situs layanan publik. Ia ingin membuktikan kelemahannya dengan memasuki sistem. Apakah tindakan Andi etis? Jelaskan jawaban Anda menggunakan penalaran kritis dan kaitkan dengan UU ITE.
4. Sebutkan dua langkah konkret yang dapat Anda lakukan untuk melindungi perangkat pribadi Anda setelah mengetahui cara kerja dasar perkakas peretasan.
5. Bagaimana Penalaran Kritis membantu seorang *ethical hacker* dalam menganalisis potensi ancaman siber?

B. Rubrik Penilaian Kinerja

Aspek yang Dinilai	Skor 1 (Kurang)	Skor 2 (Cukup)	Skor 3 (Baik)	Skor 4 (Sangat Baik)
Persiapan Kerja dan Pemahaman Konsep	Tidak mampu menjelaskan perbedaan hacker etis dan ilegal; persiapan alat/data tidak dilakukan.	Mampu menjelaskan perbedaan dasar tetapi tidak mengaitkannya dengan etika/hukum; persiapan kurang lengkap.	Mampu menjelaskan perbedaan etis secara baik dan mengaitkannya dengan tanggung jawab; persiapan lengkap.	Mampu menjelaskan perbedaan secara komprehensif, mengaitkan dengan dimensi Keimanan, dan alat/data disiapkan secara mandiri dan cermat.
Proses Analisis (Penalaran Kritis)	Tidak mampu melakukan langkah analisis atau mendeteksi risiko pada studi kasus.	Mampu melakukan analisis dasar, tetapi hasil penemuan risiko kurang logis atau tidak didukung data.	Mampu menganalisis data hasil simulasi dengan baik dan menyusun temuan risiko yang logis.	Mampu menganalisis secara mendalam, mengidentifikasi akar masalah, dan menyajikan penalaran kritis yang kuat mengenai potensi eksploitasi.
Hasil dan Rekomendasi (Komunikasi)	Laporan hasil analisis tidak diserahkan atau tidak memiliki rekomendasi pertahanan.	Laporan diserahkan, rekomendasi pertahanan kurang jelas atau tidak relevan dengan temuan.	Laporan jelas, rekomendasi pertahanan disajikan secara logis dan efektif.	Laporan sangat informatif, rekomendasi pertahanan disajikan dengan sangat jelas, persuasif, dan mencerminkan komitmen terhadap keamanan data (Cinta Bangsa).
Sikap Kerja dan Etika	Melanggar prosedur kerja, tidak menunjukkan sikap bertanggung jawab terhadap etika penggunaan alat.	Kurang fokus pada etika, perlu diingatkan berkali-kali tentang batas legalitas penggunaan perkakas.	Bekerja sesuai prosedur dan selalu mengedepankan etika dan batasan hukum yang dipelajari.	Bekerja dengan sangat disiplin, menunjukkan inisiatif untuk memastikan semua kegiatan legal, dan menegaskan prinsip etika digital (Keimanan dan Ketakwaan).