MODUL AJAR FASE F

SISTEM KEAMANAN JARINGAN

5 TUJUAN PEMBELAJARAN

Modul 5

TP : Ethical Hacking

Idiarso, S.Kom

SISTEM INFORMASI JARINGAN DAN APLIKASI

	MODUL AJAR	SMKN 1 PUNGGELAN
	Sistem Informasi Jaringan dan Aplikasi	Fase : F
		TP : 2

I. INFORMASI UMUM

A. Identitas Modul

Nama Penyusun : Idiarso, S.Kom
Nama Sekolah : SMKN 1 PUNGGELAN
Tahun Penyusunan : 2023
Jenjang Sekolah : SMK
Alokasi Waktu : 18 Pertemuan x 4 JP (72 JP)
Elemen : Sistem Keamanan Jaringan
Capaian Pembelajaran : Pada akhir fase F peserta didik mampu memahami konsep, menerapkan, mendokumentasikan, mengomunikasikan, serta memecahkan masalah secara prosedural terkait sistem keamanan jaringan, firewall, VPN, serta menerapkan ethical hacking.

B. Kompetensi Awal

Peserta Didik telah memiliki pengetahuan awal tentang

1. Definisi dan Konsep Ethical Hacking
2. Metode yang digunakan untuk penyerangan dan pengamanan ari serangan hacking

C. Profil Pelajar Pancasila

Setelah mengikuti pembelajaran ini, Profil Pelajar Pancasila yang diharapkan muncul pada peserta didik adalah :

1. Beriman dan bertakwa kepada Tuhan YME
2. Bernalar Kritis
3. Bergotong royong
4. Mandiri
5. Kreatif

D. Sarana & Prasarana

Sarana & Prasarana yang dibutuhkan pada saat belajar dengan modul ini antara lain :

- LKPD
- Alat Tulis
- Android
- Laptop/komputer

E. Target Peserta Didik

- Peserta didik reguler/tipikal : 75 %
- Peserta didik dengan kesulitan belajar : 15 %
- Peserta didik dengan pencapaian tinggi : 10 %

F. Model Pembelajaran yang Digunakan

Pembelajaran secara discovery learning

II. KOMPONEN INTI

A. Tujuan Pembelajaran

5.1 Memahami Pengertian dan konsep ethical Hacking
5.2 Menjelaskan jenis-jenis kegiatan ethical Hacking
5.3 Menjelaskan dan manfaat dari kegiatan ethical Hacking
5.4 Menginstal system operasi linux untuk kegiatan Hacking
5.5 Melakukan pengujian untuk mencari kelebihan dan kekurangan dari berbagai system operasi dalam kegiatan hacking
5.6 Memahami konsep dari footprinting.
5.7 Memahami jenis-jenis footprinting.
5.8 Memahami proses footprinting dalam pengumpulan informasi
5.9 Menerapkan prosedur footprinting dengan cara mengumpulkan informasi dasar tentang target ,platform yang sedang berjalan dan versi web server
5.10 Membangun dan mengaplikasikan beberapa teknik footprinting footprinting best practices
5.11 Mampu menemukan kerentanan dan eksploitasi untuk meluncurkan serangan
5.12 Memahami permasalahan footprinting
5.13 Memahami konsep permasalahan footprinting.
5.14 Mengklasifikasikan jenis-jenis permasalahan footprinting
5.15 Menerapkan prosedur pengamanan pada Teknik pengunmpulan informasi
5.16 Membangun beberapa teknik pengujian jaringan
5.17 Menjelaskan berbagai teknik hacking
5.18 Menjelaskan prosedur penerapan berbagai teknik hacking
5.19 Menerapkan berbagai teknik hacking
5.20 Mengoperasikan berbagai teknik hacking.
5.21 Mendokumentasi pengoperasian berbagai teknik hacking
5.22 Mengevaluasi penggunaan tools yang ada pada kali Linux.
5.23 Mengevaluasi hasil kerentanan pada target system Operasi dan aplikasi yang digunakan.
5.24 Menyimpulkan hasil penggunaan tools pada kali linux.
5.25 Menyimpulkan efektifitas dan celah yang digunakan untuk melakukan serangan kepada target
5.26 Menjelaskan berbagai permasalahan berbagai teknik hacking
5.27 Menentukan prosedur berbagai permasalahan teknik hacking
5.28 Menerapkan pemecahan masalah berbagai teknik hacking
5.29 Memproyeksikan permasalahan berbagai teknik hacking
5.30 Menjelaskan analisis hasil berbagai hacking
5.31 Menerapkan pemecahan masalah hasil berbagai teknik hacking
5.32 Memproyeksikan permasalahan hasil berbagai teknik hacking
5.33 Menjelaskan Prosedur penanganan Hacking
5.34 Menerapkan prosedur penanaganan Hacking

5.35 Mempraktikan berbagai Teknik penanganan hacking
5.36 Memperbaiki permasalahan Hacking
5.37 Menjelaskan analisis permasalahan penanganan Hacking
5.38 Menentukan analisis permasalahan teknik hacking
5.39 Mempraktikan perbaikan permasalahan penanganan Hacking
5.40 Menjelaskan evaluasi dan alat ukur penanganan hacking
5.41 Menentukan evaluasi penanganan Hacking
5.42 Mempraktikan Tindakan data hasil penanganan hacking

B. Pemahaman Bermakna

1. Keamanan Sistem yang Ditingkatkan: Melalui praktik ethical hacking, Peserta Didik dapat mengidentifikasi kelemahan dan kerentanan dalam sistem.
2. Perlindungan Data dan Informasi: Ethical hacking membantu melindungi data dan informasi sensitif dari serangan yang berpotensi merugikan. Dengan menguji keamanan sistem, organisasi dapat mengetahui apakah data pribadi atau rahasia bisnis mereka terancam oleh ancaman eksternal atau internal. Hal ini memungkinkan mereka untuk mengambil tindakan yang diperlukan untuk melindungi integritas, kerahasiaan, dan ketersediaan informasi mereka.
3. Perbaikan Kelemahan: Melalui proses ethical hacking, kelemahan dalam sistem dapat terungkap dan dilaporkan kepada pemilik sistem. Dengan menerima laporan ini, pemilik sistem dapat melakukan perbaikan yang diperlukan untuk mengatasi kelemahan tersebut sebelum penyerang jahat memanfaatkannya. Dalam jangka panjang, ini membantu menciptakan lingkungan yang lebih aman dan dapat diandalkan.
4. Kesadaran Keamanan: Ethical hacking berperan penting dalam meningkatkan kesadaran tentang ancaman keamanan komputer dan praktik terbaik dalam melindungi sistem. Dengan membuka kelemahan dan serangan yang mungkin dilakukan oleh penyerang, ethical hackers membantu mendidik pemilik sistem dan pengguna tentang langkah-langkah yang dapat diambil untuk mengurangi risiko dan menjaga keamanan mereka.
5. Kerangka Hukum dan Etika: Salah satu aspek kunci dari ethical hacking adalah melakukan kegiatan ini dengan mengikuti kerangka hukum dan etika. Ethical hackers harus mematuhi hukum yang berlaku dan memperhatikan batasan dan izin yang diberikan oleh pemilik sistem. Mereka harus menjaga kerahasiaan data yang ditemukan selama pengujian dan melaporkannya dengan tepat kepada pihak yang berwenang.

C. Pertanyaan Pemantik

- Apa perbedaan antara ethical hacking dan hacking ilegal?
- Bagaimana proses ethical hacking dilakukan untuk mengidentifikasi kerentanan dalam sistem?
- Apa saja teknik umum yang digunakan oleh ethical hackers dalam menguji keamanan sistem?
- Apa tujuan utama dari melakukan ethical hacking?
- Bagaimana ethical hacking dapat membantu organisasi meningkatkan keamanan sistem mereka?
- Apa tanggung jawab dan kewajiban seorang ethical hacker terkait dengan hukum dan etika?
- Apa langkah-langkah yang harus diambil oleh pemilik sistem setelah menerima laporan dari ethical hacker tentang kelemahan dalam sistem mereka?

- Apa saja manfaat dan risiko yang terkait dengan menggunakan layanan ethical hacking dari pihak ketiga?
- Bagaimana ethical hacking dapat meningkatkan kesadaran tentang ancaman keamanan komputer di kalangan pengguna dan pemilik sistem?
- Apa saja bidang-bidang spesifik di mana ethical hacking sering digunakan, seperti keamanan jaringan, keamanan aplikasi, atau keamanan web?

D. Persiapan Pembelajaran

- Menyiapkan presentasi Pembelajaran
- Membuat pertanyaan yang harus dijawab oleh siswa

E. Kegiatan Pembelajaran :

KEGIATAN PEMBELAJARAN		
Pertemuan 1		
Tahapan	**Kegiatan**	**Alokasi Waktu**
Pendahuluan	1. Guru membuka pelajaran dengan memberi salam dan peserta didik menjawab salam dari guru 2. Salah satu peserta didik memimpin kegiatan berdoa sebelum pembelajaran dimulai (Profil Beriman dan bertakwa kepada Tuhan YME dan Berakhlah Mulia) 3. Guru mengecek kehadiran peserta didik 4. Peserta didik melakukan assesment diagnostik kognitif dan non kognitif. 5. Menyampaikan pertanyaan pemantik yaitu : a) Apa yang pengertian ethical hacking ? b) perbedaan antara ethical hacking dan hacking ilegal? c) Bagaimana Mengapa Hacker melakukan kegiatan peretasan ? d) Apa saja perangkat-perangkat yang paling rentan terhadap serangan ? e) Apa persamaan Hacking and Ethical Hacking ? 6. Guru memberikan gambaran tentang manfaat mempelajari materi yang akan dipelajari 7. Guru menyampaikan tujuan pembelajaran pada pertemuan yang akan berlangsung	**8 JP**

Kegiatan Inti	***Mulai dari diri*** 1. Peserta didik menggali informasi tentang definisi dan Jenis-jenis Ethical Hacking di internet (Profil bernalar kritis) 2. Peserta didik menggali informasi tentang Jenis dan tingkatan Hacker di internet (Profil bernalar kritis) 3. Beberapa peserta didik menyampaikan informasi yang didapat di internet tentang definisi Ethical Hacking ***Eksplorasi Konsep*** 4. Guru menyampaikan materi tentang manajemen Konsep Ethical Hacking. 5. Peserta didik menyimak presentasi dan video yang di berikan oleh guru tentang Ehical Hacking. ***Ruang Kolaborasi*** 6. Peserta Peserta didik membentuk kelompok untuk mendiskusikan materi tentang Sistem Operasi yang digunakan untuk kegiatan Ethical Hacking menjadi 8 kelompok diskusi sebagaimana tercantum pada LKPD 1 (Dimensi P3 kreatif: Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya). (Profil bergotong royong) ***Refleksi Terbimbing*** 7. Guru membimbing peserta didik untuk melakukan diskusi kelompok 8. Secara berkelompok, peserta didik mempresentasikan hasil pekerjaan kelompoknya 9. Kelompok lain / guru menanggapi jawaban dari kelompok yang sedang presentasi 10. Guru memberikan semangat kepada peserta didik lain untuk menjawab pertanyaan	

	Demonstrasi Kontekstual 11. Peserta didik secara mandiri mengerjakan soal yang diberikan oleh guru tentang konsep-konsep dasar Ethical Hacking (Profil mandiri) ***Elaborasi Pemahaman*** 12. Peserta didik bisa bertanya jika ada kesulitan dalam memahami materi 13. Guru membimbing peserta didik yang mengalami kesulitan dalam memahami materi	
Penutup	***Koneksi Antar Materi Peserta didik bersama*** 1. Guru bersama peserta didik menyimpulkan materi yang telah dipelajari 2. Guru memberikan penjelasan jawaban atas pertanyaan-pertanyaan yang ada 3. Peserta didik menulis rangkuman berdasarkan arahan dari guru ***Aksi Nyata*** 4. Guru memberikan motivasi kepada peserta didik 5. Guru menutup dengan memberikan salam	

KEGIATAN PEMBELAJARAN		
Pertemuan 2		
Tahapan	**Kegiatan**	**Alokasi Waktu**
Pendahuluan	1. Guru membuka pelajaran dengan memberi salam dan peserta didik menjawab salam dari guru 2. Salah satu peserta didik memimpin kegiatan berdoa sebelum pembelajaran dimulai (Profil Beriman dan bertakwa kepada Tuhan YME dan Berakhlah Mulia) 3. Guru mengecek kehadiran peserta didik 4. Guru menyampaikan tujuan pembelajaran yang ingin dicapai 5. Guru menyampaikan pertanyaan pemantik o Apa saja Sistem Operasi dan perangkat yang digunakan untuk kegiatan hacking ? 6. Mengaitkan kejadian sehari-hari dengan materi 7. Memberikan gambaran tentang manfaat mempelajari materi dalam kehidupan sehari-hari	8 JP
Kegiatan Inti	***Mulai dari diri*** 1. Peserta didik menggali informasi tentang perangkat dan Sistem Operasi yang digunakan untuk kegiatan Ethical Hacking. (Profil bernalar kritis) 2. Peserta didik menyampaikan informasi yang didapat diinternet tentang Sistem Operasi yang digunakan untuk kegiatan Ethical Hacking. ***Eksplorasi Konsep*** 3. Guru menyampaikan materi tentang Sistem Operasi yang banyak digunakan untuk kegiatan Ethical Hacking dan mencontohkan cara menginstalnya di perangkat komputer. 4. Peserta didik menyimak materi yang di berikan oleh guru tentang cara instalasi sistem operasi yang digunakan untuk kegiatan Ethical Hacking. ***aksi nyata*** 8. Peserta didik menginstal Sistem operasi kali linux pada mesin Virtual secara mandiri menggunakan perangkat komputer yang telah disediakan	

	9. Peserta didik diminta untuk menagkap layar dan menuangkannya dalam bentuk file presentasi maupun video yang nanti akan digunakan untuk ruang elaborasi dan diskusi secara kelompok sebagaimana tercantum pada LKPD 2 ***Refleksi Terbimbing*** 5. Secara mandiri, peserta didik berusaha mengikuti langkah-langkah yang telah diberikan guru diawal 6. Guru dan mengawasi dan membantu memecahkan masalah yang dihadapi peserta didik dalam proses penginstalan . 7. Guru memberikan semangat kepada peserta didik lain untuk saling membantu dalam proses Instalasi dan membantu memecahakan permasalahan yang dihadapi ***Demonstrasi Kontekstual*** 8. Peserta didik mempresentasikan hasil dari proses instalasi sistem operasi kali linux untuk kegiatan Ethical Hacking dan langkah-langkah penginstalannya secara berkelompok. (Profil gotong royong) 9. Peserta didik membuat laporan hasil diskusi dengan menyertakan file hasil karya/hasil diskusi dalam bentuk PPt atau Video, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan ***Elaborasi Pemahaman*** 10. Peserta didik bisa bertanya jika ada kesulitan dalam memahami materi 11. Guru membimbing peserta didik yang mengalami kesulitan dalam memahami materi	

Penutup	***Koneksi Antar Materi*** 1. Peserta didik bersama guru menyimpulkan hasil diskusi untuk pembelajaran hari ini 2. Guru memberikan penjelasan jawaban atas pertanyaan yang ada 3. Peserta didik menulis rangkuman berdasarkan arahan dari guru ***Aksi Nyata*** 4. Guru memberikan motivasi kepada peserta didik 5. Guru menutup dengan memberikan salam	

KEGIATAN PEMBELAJARAN		
Pertemuan 3		
Tahapan	**Kegiatan**	**Alokasi Waktu**
Pendahuluan	1. Guru membuka pelajaran dengan memberi salam dan peserta didik menjawab salam dari guru 2. Salah satu peserta didik memimpin kegiatan berdoa sebelum pembelajaran dimulai (Profil Beriman dan bertakwa kepada Tuhan YME dan Berakhlah Mulia) 3. Guru mengecek kehadiran peserta didik 4. Guru menyampaikan tujuan pembelajaran yang ingin dicapai 5. Guru menyampaikan pertanyaan pemantik o Bagaimana kita mengoptimalkan kinerja Sistem Operasi kali linux di mesin virtual ? o Apakah kalian sudah banyak mengenal perintah dasar linux ? 6. Mengaitkan kejadian sehari-hari dengan materi 7. Memberikan gambaran tentang manfaat mempelajari materi dalam kehidupan sehari-hari	8 JP
Kegiatan Inti	***Mulai dari diri*** 1. Peserta didik menggali informasi tentang Optimalisasi kali linux & perintah dasar Kali linux untuk kegiatan Ethical Hacking. (Profil bernalar kritis)	

	2. Peserta didik menyampaikan informasi yang didapat diinternet tentang Optimalisasi kali linux & perintah dasar Kali linux untuk kegiatan Ethical Hacking. ***Eksplorasi Konsep*** 3. Guru menyampaikan materi tentang Optimalisasi kali linux & perintah dasar Kali linux untuk kegiatan Ethical Hacking . 4. Peserta didik menyimak materi yang di berikan oleh guru tentang Optimalisasi kali linux & perintah dasar Kali linux yang digunakan untuk kegiatan Ethical Hacking. ***aksi nyata*** 10. Peserta didik megoperasikan Sistem operasi kali linux pada mesin Virtual secara mandiri menggunakan perangkat komputer yang telah disediakan 11. Peserta didik diminta untuk menagkap layar dan menuangkannya dalam bentuk file presentasi maupun video yang nanti akan digunakan untuk ruang elaborasi dan diskusi. ***Refleksi Terbimbing*** 5. Secara mandiri, peserta didik berusaha mengikuti langkah-langkah yang telah diberikan guru diawal 6. Guru dan mengawasi dan membantu memecahkan masalah yang dihadapi peserta didik dalam proses penginstalan . 7. Guru memberikan semangat kepada peserta didik lain untuk saling membantu dalam proses Pengerjaan dan optimalisasi dan membantu memecahakan permasalahan yang dihadapi ***Demonstrasi Kontekstual*** 8. Peserta didik mempresentasikan hasil dari proses Optimalisasi dan perintah dasar linux sistem operasi kali linux untuk kegiatan Ethical Hacking secara berkelompok. (Profil gotong royong) 9. Peserta didik membuat laporan hasil diskusi dengan menyertakan file hasil karya/hasil diskusi dalam bentuk PPt	

	atau Video, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan ***Elaborasi Pemahaman*** 10. Peserta didik bisa bertanya jika ada kesulitan dalam memahami materi 11. Guru membimbing peserta didik yang mengalami kesulitan dalam memahami materi	
Penutup	***Koneksi Antar Materi*** 1. Peserta didik bersama guru menyimpulkan hasil diskusi untuk pembelajaran hari ini 2. Guru memberikan penjelasan jawaban atas pertanyaan yang ada 3. Peserta didik menulis rangkuman berdasarkan arahan dari guru ***Aksi Nyata*** 4. Guru memberikan motivasi kepada peserta didik 5. Guru menutup dengan memberikan salam	

KEGIATAN PEMBELAJARAN		
Pertemuan 4		
Tahapan	**Kegiatan**	**Alokasi Waktu**
Pendahuluan	1. Guru membuka pelajaran dengan memberi salam dan peserta didik menjawab salam dari guru 2. Salah satu peserta didik memimpin kegiatan berdoa sebelum pembelajaran dimulai (Profil Beriman dan bertakwa kepada Tuhan YME dan Berakhlah Mulia) 3. Guru mengecek kehadiran peserta didik 4. Guru menyampaikan tujuan pembelajaran yang ingin dicapai 5. Guru menyampaikan pertanyaan pemantik o Bagaimana kita Melacak IP Address seseorang ? o Dalam proses pengumpulan informasi target, apa yang kalianlakukan ? 6. Mengaitkan kejadian sehari-hari dengan materi 7. Memberikan gambaran tentang manfaat mempelajari materi dalam kehidupan sehari-hari	8 JP
Kegiatan Inti	***Mulai dari diri*** 1. Peserta didik menggali informasi tentangpengumpulan informasi target menggunakan tools yang ada. (Profil bernalar kritis) 2. Peserta didik menyampaikan informasi yang didapat diinternet tentang pengumpulan informasi untuk kegiatan Ethical Hacking. ***Eksplorasi Konsep*** 3. Guru menyampaikan materi keystroke loggers dan spyware serta potensi ancaman yang ditimbulkannyamenggunakan Melacak IP Address seseorang secara aktive dan pasive dan mencontohkan penggunaan ping & nslookup 4. Peserta didik menyimak materi yang di berikan oleh guru tentang Information Gathering untuk kegiatan Ethical Hacking.	

	aksi nyata 12. Peserta didik megoperasikan Sistem operasi kali linux pada mesin Virtual secara mandiri menggunakan perangkat komputer yang telah disediakan 13. Peserta didik diminta untuk menagkap layar dan menuangkannya dalam bentuk file presentasi maupun video yang nanti akan digunakan untuk ruang elaborasi dan diskusi. ***Refleksi Terbimbing*** 5. Secara mandiri, peserta didik berusaha mengikuti langkah-langkah yang telah diberikan guru diawal 6. Guru dan mengawasi dan membantu memecahkan masalah yang dihadapi peserta didik dalam proses penginstalan . 7. Guru memberikan semangat kepada peserta didik lain untuk saling membantu dalam proses Pengerjaan dan optimalisasi dan membantu memecahakan permasalahan yang dihadapi ***Demonstrasi Kontekstual*** 8. Peserta didik mempresentasikan hasil dari proses information Gathering untuk kegiatan Ethical Hacking secara berkelompok. (Profil gotong royong) 9. Peserta didik membuat laporan hasil diskusi dengan menyertakan file hasil karya/hasil diskusi dalam bentuk PPt atau Video, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan ***Elaborasi Pemahaman*** 10. Peserta didik bisa bertanya jika ada kesulitan dalam memahami materi 11. Guru membimbing peserta didik yang mengalami kesulitan dalam memahami materi	

Penutup	***Koneksi Antar Materi*** 1. Peserta didik bersama guru menyimpulkan hasil diskusi untuk pembelajaran hari ini 2. Guru memberikan penjelasan jawaban atas pertanyaan yang ada 3. Peserta didik menulis rangkuman berdasarkan arahan dari guru ***Aksi Nyata*** 4. Guru memberikan motivasi kepada peserta didik 5. Guru menutup dengan memberikan salam	

KEGIATAN PEMBELAJARAN		
Pertemuan 5		
Tahapan	**Kegiatan**	**Alokasi Waktu**
Pendahuluan	1. Guru membuka pelajaran dengan memberi salam, dan peserta didik menjawab salam dari guru. 2. Salah satu peserta didik memimpin kegiatan berdoa sebelum pembelajaran dimulai (Profil Beriman dan bertakwa kepada Tuhan YME dan Berakhlah Mulia). 3. Guru mengecek kehadiran peserta didik. 4. Peserta didik melakukan asesmen diagnostik kognitif dan non-kognitif. 5. Peserta didik melakukan aktivitas pengulangan materi sebelumnya secara singkat. 6. Guru memperkenalkan topik "Advanced Network Scanning and Evasion Techniques" dan menjelaskan manfaat serta tujuan pembelajaran pada pertemuan ini 7. emberikan gambaran tentang manfaat mempelajari materi dalam kehidupan sehari-hari	8 JP
Kegiatan Inti	***Mulai dari diri*** 1. Guru memberikan gambaran umum tentang network scanning dan pentingnya dalam persiapan serangan. 2. Peserta didik mempelajari penggunaan proxy dalam serangan sebagai metode untuk menyembunyikan identitas asli. 3. Guru memperkenalkan CEH Scanning Methodology sebagai pendekatan sistematis untuk melakukan scanning jaringan. 4. Peserta didik diajak memahami teknik pengujian sistem live dan	

	bagaimana menerapkan teknik ini dalam proses scanning. 5. Guru menjelaskan berbagai teknik scanning yang digunakan oleh attacker, seperti banner grabbing, vulnerability scanning, dan penggambaran diagram jaringan. 6. Peserta didik mempelajari teknik IDS evasion yang digunakan untuk menghindari deteksi oleh sistem Intrusion Detection System. 7. Guru menjelaskan tentang countermeasures yang dapat diimplementasikan untuk melawan teknik scanning yang dilakukan oleh attacker. 8. Peserta didik mempelajari konsep proxy chaining dan bagaimana menggunakan serangkaian proxy untuk mengenkripsi dan menyembunyikan aktivitas mereka. 9. Guru menjelaskan teknik HTTP tunneling dan SSH tunneling sebagai cara untuk menyembunyikan serangan atau melakukan akses ke sistem yang terkunci. ***aksi nyata*** 14. Peserta didik megoperasikan Sistem operasi kali linux pada mesin Virtual secara mandiri menggunakan perangkat komputer yang telah disediakan 15. Peserta didik mempraktikan Scanning network menggunakan tools yang ada pada kali linux 16. Peserta didik diminta untuk menagkap layar dan menuangkannya dalam bentuk file presentasi maupun video yang nanti akan digunakan untuk ruang elaborasi dan diskusi. ***Refleksi Terbimbing*** 10. Secara mandiri, peserta didik berusaha mengikuti langkah-langkah yang telah diberikan guru diawal 11. Guru dan mengawasi dan membantu memecahkan masalah yang dihadapi peserta didik dalam proses pen Guru memfasilitasi diskusi tentang penggunaan teknik scanning dan teknik evasi dalam serangan, serta dampak dan risiko yang terkait. 12. Guru memberikan semangat kepada peserta didik lain untuk saling membantu dalam proses Pengerjaan dan optimalisasi dan membantu memecahkan permasalahan yang dihadapi	

	Demonstrasi Kontekstual 1. Peserta didik berbagi pemahaman, pertanyaan, dan pengalaman terkait materi yang telah dipelajari. 2. Peserta didik mempresentasikan hasil dari proses information Gathering untuk kegiatan Ethical Hacking secara berkelompok. (Profil gotong royong) 3. Peserta didik membuat laporan hasil diskusi dengan menyertakan file hasil karya/hasil diskusi dalam bentuk PPt atau Video, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan ***Elaborasi Pemahaman*** 4. Peserta didik bisa bertanya jika ada kesulitan dalam memahami materi 5. Guru membimbing peserta didik yang mengalami kesulitan dalam memahami materi	
Penutup	***Koneksi Antar Materi*** 1. Guru mengajukan pertanyaan refleksi terkait pembelajaran hari ini. 2. Peserta didik memberikan tanggapan dan kesimpulan mereka tentang materi "Advanced Network Scanning and Evasion Techniques". 3. Guru memberikan penjelasan atau pemahaman tambahan jika diperlukan. 4. Aksi Nyata 5. Guru memberikan motivasi kepada peserta didik 6. Guru menutup dengan memberikan salam II.	

KEGIATAN PEMBELAJARAN		
Pertemuan 6		
Tahapan	**Kegiatan**	**Alokasi Waktu**

1. Pendahuluan	2. Guru membuka pelajaran dengan memberi salam dan peserta didik menjawab salam dari guru 3. Salah satu peserta didik memimpin kegiatan berdoa sebelum pembelajaran dimulai (Profil Beriman dan bertakwa kepada Tuhan YME dan Berakhlah Mulia) 4. Guru mengecek kehadiran peserta didik 5. Guru menyampaikan tujuan pembelajaran yang ingin dicapai 6. Guru menyampaikan pertanyaan pemantik: Apa yang dimaksud dengan Enumerasi dalam konteks keamanan sistem dan jaringan? Mengapa Enumerasi menjadi tahap penting dalam pengujian keamanan? Apa saja teknik yang digunakan dalam Enumerasi untuk mengumpulkan informasi tentang sistem dan jaringan? Mengapa penting untuk melakukan Enumerasi terhadap services dan ports yang berjalan dalam suatu sistem? 7. Mengaitkan kejadian sehari-hari dengan materi 8. Memberikan gambaran tentang manfaat mempelajari materi dalam kehidupan sehari-hari	**8 JP**
Kegiatan Inti	***Mulai dari diri*** 9. Peserta didik menggali informasi tentangpengumpulan informasi target menggunakan tools yang ada. (Profil bernalar kritis) 10. Peserta didik menyampaikan informasi yang didapat diinternet tentang pengumpulan informasi untuk kegiatan Ethical Hacking. ***Eksplorasi Konsep*** 11. Guru menyampaikan materi keystroke loggers dan spyware serta potensi ancaman yang ditimbulkannyamenggunakan Melacak IP Address seseorang secara aktive dan pasive dan mencontohkan penggunaan ping & nslookup 12. Peserta didik menyimak materi yang di berikan oleh guru tentang Enumerasi untuk kegiatan Ethical Hacking. ***aksi nyata*** 17. Peserta didik megoperasikan Sistem operasi kali linux pada mesin Virtual secara mandiri menggunakan perangkat komputer yang telah disediakan 18. Peserta didik diminta untuk mempraktikan Enumerasi menggunakan kali linux, menagkap layar untuk kegiatan	

	pembuatan tugas penilaian dan menuangkannya dalam bentuk file presentasi maupun video yang nanti akan digunakan untuk ruang elaborasi dan diskusi. ***Refleksi Terbimbing*** 13. Secara mandiri, peserta didik berusaha mengikuti langkah-langkah yang telah diberikan guru diawal 14. Guru dan mengawasi dan membantu memecahkan masalah yang dihadapi peserta didik dalam proses Enumerasi . 15. Guru memberikan semangat kepada peserta didik lain untuk saling membantu dalam proses Pengerjaan dan optimalisasi dan membantu memecahakan permasalahan yang dihadapi ***Demonstrasi Kontekstual*** 16. Peserta didik mempresentasikan hasil dari Enumerasi untuk kegiatan Ethical Hacking secara berkelompok. (Profil gotong royong) 17. Peserta didik membuat laporan hasil diskusi dengan menyertakan file hasil karya/hasil diskusi dalam bentuk PPt atau Video, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan ***Elaborasi Pemahaman*** 18. Peserta didik bisa bertanya jika ada kesulitan dalam memahami materi 19. Guru membimbing peserta didik yang mengalami kesulitan dalam memahami materi	
Penutup	***Koneksi Antar Materi*** 1. Peserta didik bersama guru menyimpulkan hasil diskusi untuk pembelajaran hari ini 2. Guru memberikan penjelasan jawaban atas pertanyaan yang ada 3. Peserta didik menulis rangkuman berdasarkan arahan dari guru ***Aksi Nyata*** 4. Guru memberikan motivasi kepada peserta didik 5. Guru menutup dengan memberikan salam	

KEGIATAN PEMBELAJARAN		
Pertemuan 8		
Tahapan	**Kegiatan**	**Alokasi Waktu**
Pendahuluan	1. Guru membuka pelajaran dengan memberi salam dan peserta didik menjawab salam dari guru 2. Salah satu peserta didik memimpin kegiatan berdoa sebelum pembelajaran dimulai (Profil Beriman dan bertakwa kepada Tuhan YME dan Berakhlah Mulia) 3. Guru mengecek kehadiran peserta didik 4. Guru menyampaikan tujuan pembelajaran yang ingin dicapai pada pertemuan 9 5. Guru menjelaskan pengertian tentang Metasploit Framework. 6. Guru membahas jenis-jenis Metasploit Framework yang umum digunakan. 7. Peserta didik diajak untuk berdiskusi mengenai pengalaman atau pengetahuan mereka terkait Sistem yang pernah terkena virus sehingga sistem mereka terkena Hack. 8. Mengaitkan kejadian sehari-hari dengan materi 9. Memberikan gambaran tentang manfaat mempelajari materi dalam kehidupan sehari-hari	8 JP
Kegiatan Inti	***Mulai dari diri*** 10. Peserta didik menggali informasi Metasploit Framework serta potensi ancaman yang ditimbulkannya. (Profil bernalar kritis) Peserta didik menyampaikan informasi yang didapat diinternet tentang Metasploit Framework dan jenis jenis sistem yang bisa terkena serangan. ***Eksplorasi Konsep*** Guru menyampaikan materi Metasploit Framework dan jenis jenispenggunaanya menggunakan tools yang ada pad kali linux. 11. Peserta didik menyimak materi yang di berikan oleh guru tentang Metasploit Framework untuk kegiatan Ethical Hacking.	

	aksi nyata 19. Peserta didik megoperasikan Metasploit Framework secara mandiri menggunakan perangkat komputer yang telah disediakan 20. Peserta didik diminta untuk menagkap layar dan menuangkannya dalam bentuk file presentasi maupun video yang nanti akan digunakan untuk ruang elaborasi dan diskusi. ***Refleksi Terbimbing*** 12. Secara mandiri, peserta didik berusaha mengikuti langkah-langkah yang telah diberikan guru diawal 13. Guru dan mengawasi dan membantu memecahkan masalah yang dihadapi peserta didik dalam proses praktik tentang Metasploit Framework **.** 14. Guru memberikan semangat kepada peserta didik lain untuk saling membantu dalam proses Pengerjaan dan optimalisasi dan membantu memecahakan permasalahan yang dihadapi ***Demonstrasi Kontekstual*** 15. Peserta didik mempresentasikan hasil dari proses instalasi tambahan dalam kalilinux dan penggunaan Metasploit Framework untuk kegiatan Ethical Hacking secara berkelompok. (Profil gotong royong) 16. Peserta didik membuat laporan hasil diskusi dengan menyertakan file hasil karya/hasil diskusi dalam bentuk PPt atau Video, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan ***Elaborasi Pemahaman*** 17. Peserta didik bisa bertanya jika ada kesulitan dalam memahami materi 18. Guru membimbing peserta didik yang mengalami kesulitan dalam memahami materi	

Penutup	***Koneksi Antar Materi*** 6. Peserta didik bersama guru menyimpulkan hasil diskusi untuk pembelajaran hari ini 7. Guru memberikan penjelasan jawaban atas pertanyaan yang ada 8. Peserta didik menulis rangkuman berdasarkan arahan dari guru ***Aksi Nyata*** 9. Guru memberikan motivasi kepada peserta didik 10. Guru menutup dengan memberikan salam	

A. Asesmen

1. **Formatif :** Soal Diskusi dan Tes Formatif (Terlampir)
2. **Diagnostik :** Non-kognitif (Terlampir)

B. Pengayaan & Remidial

Terlampir

C. Refleksi Peserta Didik dan Guru

- Apa ada kendala pada kegiatan pembelajaran?
- Apakah semua peserta didik aktif selama mengikuti kegiatan pembelajaran?
- Apa saja kesulitan yang dihadapi peserta didik selama mengikuti kegiatan pembelajaran?
- Apakah kesulitan yang dialami peserta didik dapat teratasi?
- Apa level pencapaian rata-rata peserta didik dalam kegiatan pembelajaran ini?
- Apakah seluruh peserta didik dapat tuntas dalam pelaksanaan pembelajaran?
- Apa strategi yang harus dipilih supaya peserta didik dapat menuntaskan kompetensi?

I. LAMPIRAN

A. LKPD

a) Tes formatif

Soal Latihan LKPD 1
Silahkan jawab pertanyaan-pertanyaan berikut ini dengan bahasa kamu sendiri! 1. Apa yang dimaksud dengan ethical hacking dan mengapa hal ini penting dalam konteks keamanan informasi? 2. Bagaimana perbedaan antara ethical hacking dan hacking biasa?

3. Apa tujuan utama dari ethical hacking dan bagaimana hal ini membantu organisasi meningkatkan keamanan sistem mereka?

4. Apa langkah-langkah yang biasanya dilakukan oleh seorang ethical hacker dalam menjalankan aktivitasnya?

5. Apa peran penting yang dimainkan oleh persetujuan tertulis (written consent) dalam praktik ethical hacking?

11. Apa saja metode atau pendekatan yang biasanya digunakan oleh ethical hacker untuk mengidentifikasi dan mengeksploitasi kerentanan dalam sistem?
12. Apa tindakan yang diambil oleh seorang ethical hacker setelah menemukan kerentanan dalam sistem yang diuji?
13. Apa kode etik atau prinsip-prinsip penting yang harus diikuti oleh seorang ethical hacker dalam menjalankan tugasnya?
14. sebutkan jenis-jenis Hacker ?
15. Apa perbedaan Hacker dan Cracker ?

Kunci jawaban dan norma penilaian		
No	**Kunci Jawaban**	**Skor**
1	Ethical hacking adalah praktik penggunaan keterampilan dan pengetahuan dalam bidang keamanan informasi untuk secara legal dan etis mengidentifikasi dan menguji kerentanan dalam sistem, dengan tujuan meningkatkan keamanan sistem tersebut. Hal ini penting karena membantu organisasi mengidentifikasi celah keamanan yang dapat dieksploitasi oleh penyerang jahat, sehingga langkah-langkah pencegahan dapat diambil untuk melindungi sistem dan data.	10
2	Perbedaan antara ethical hacking dan hacking biasa terletak pada niat dan izin yang diperlukan. Ethical hacking dilakukan dengan izin tertulis dan tujuan yang jelas untuk meningkatkan keamanan sistem. Sementara hacking biasa dilakukan tanpa izin atau niat jahat untuk merusak, mencuri data, atau menyebabkan kerugian.	10
3	Tujuan utama dari ethical hacking adalah untuk mengidentifikasi kerentanan keamanan yang mungkin ada dalam sistem, mengevaluasi tingkat risiko yang terkait, dan memberikan rekomendasi perbaikan. Dengan melakukan aktivitas ethical hacking secara teratur, organisasi dapat meningkatkan keamanan	10

	sistem mereka, mengurangi risiko serangan, dan melindungi data sensitif mereka.	
4	Seorang ethical hacker biasanya melakukan langkah-langkah seperti pengumpulan informasi (information gathering), pemindaian kerentanan (vulnerability scanning), pengujian penetrasi (penetration testing), dan analisis keamanan (security analysis). Mereka juga dapat menggunakan teknik-teknik seperti social engineering, uji coba serangan (exploitation testing), dan analisis kode untuk menemukan kerentanan dalam sistem.	10
5	Persetujuan tertulis (written consent) penting dalam praktik ethical hacking karena membantu memastikan bahwa aktivitas tersebut dilakukan secara legal dan dengan izin dari pemilik sistem. Hal ini melindungi ethical hacker dari tuntutan hukum dan memastikan transparansi dalam aktivitas yang dilakukan.	10
6	Ethical hacker menggunakan berbagai metode dan pendekatan, termasuk pemindaian kerentanan, analisis kode, social engineering, uji coba serangan, dan uji penetrasi. Tujuannya adalah untuk mengidentifikasi kerentanan dalam sistem, baik melalui celah teknis, kelemahan konfigurasi, atau kelemahan manusia dalam organisasi.	10
7	Setelah menemukan kerentanan dalam sistem yang diuji, seorang ethical hacker akan membuat laporan yang menyertakan detail tentang kerentanan tersebut, potensi dampaknya, dan rekomendasi perbaikan. Selanjutnya, tindakan perbaikan dapat diambil oleh tim keamanan IT atau departemen terkait untuk memperbaiki kerentanan yang telah diidentifikasi.	10
8	Seorang ethical hacker diharapkan mengikuti kode etik yang meliputi prinsip-prinsip seperti mendapatkan izin tertulis sebelum melakukan pengujian, menjaga kerahasiaan data yang ditemukan selama pengujian, tidak merusak sistem, dan memberikan laporan yang jujur dan lengkap tentang temuan dan rekomendasi. Prinsip-prinsip ini bertujuan untuk memastikan bahwa ethical hacking dilakukan dengan integritas dan tanggung jawab.	10
9	Ada beberapa jenis hacker yang dapat dikenali berdasarkan motivasi, metode, dan aktivitas mereka. Berikut adalah beberapa jenis hacker yang umum dikenal: 1. White Hat Hacker: Juga dikenal sebagai ethical hacker, mereka bekerja untuk meningkatkan keamanan sistem dengan izin dan	10

	tujuan yang jelas. Mereka melakukan pengujian penetrasi, analisis keamanan, dan membantu organisasi mengidentifikasi dan memperbaiki kerentanan. 2. Black Hat Hacker: Merupakan hacker dengan niat jahat dan melanggar hukum. Mereka menjalankan serangan untuk mencuri data, merusak sistem, atau memperoleh keuntungan pribadi. Mereka sering kali terlibat dalam kegiatan ilegal seperti peretasan, penipuan, atau pencurian identitas. 3. Grey Hat Hacker: Grey hat hacker berada di antara white hat hacker dan black hat hacker. Mereka tidak memiliki izin resmi untuk melakukan serangan, tetapi mereka juga tidak memiliki niat jahat. Mereka dapat menemukan kerentanan dalam sistem dan mengungkapkannya kepada pemilik sistem tanpa izin, dengan tujuan memperbaiki keamanan. 4. Script Kiddie: Script kiddie adalah hacker amatir yang menggunakan alat dan skrip yang telah dikembangkan oleh orang lain tanpa pemahaman mendalam tentang cara kerjanya. Mereka cenderung mencoba mengeksploitasi kerentanan yang sudah diketahui tanpa memahami secara penuh tentang hacking itu sendiri. 5. Hacktivist: Hacktivist adalah hacker yang melakukan serangan dengan tujuan politik atau sosial. Mereka menggunakan keterampilan hacking untuk mempengaruhi opini publik atau memperjuangkan tujuan tertentu, seperti mengungkap skandal atau melawan tindakan yang dianggap tidak adil. 6. State-Sponsored Hacker: Jenis hacker ini bekerja untuk negara atau badan intelijen dengan tujuan melakukan serangan atau pengintaian terhadap negara atau organisasi lain. Mereka memiliki sumber daya yang kuat dan sering kali beroperasi dalam skala yang besar.	
10	Perbedaan antara hacker dan cracker terletak pada niat, tujuan, dan aktivitas mereka: 1. Hacker: Seorang hacker adalah seseorang yang memiliki	10

	pengetahuan dan keterampilan teknis dalam bidang keamanan informasi. Mereka menggunakan pengetahuan ini untuk memahami sistem, melindungi sistem, atau meningkatkan keamanan secara legal. Hacker dapat dibagi menjadi white hat, grey hat, dan hacktivist, tergantung pada niat dan aktivitas mereka. 2. Cracker: Cracker, di sisi lain, adalah seseorang yang meretas atau melanggar sistem dengan niat jahat atau tanpa izin. Mereka melakukan aktivitas ilegal, seperti mencuri data, merusak sistem, atau mendapatkan keuntungan pribadi. Cracker juga dikenal sebagai black hat hacker. Dalam rangka mencapai tujuan mereka, cracker sering kali melanggar hukum dan melakukan serangan yang merugikan individu atau organisasi. Mereka bertujuan untuk mendapatkan akses yang tidak sah, merusak sistem, mencuri informasi sensitif, atau melakukan aktivitas kriminal lainnya. Di sisi lain, hacker yang baik (white hat hacker) menggunakan pengetahuan dan keterampilan mereka untuk melindungi sistem dan membantu meningkatkan keamanan. Penting untuk dicatat bahwa penggunaan istilah "hacker" dan "cracker" dapat bervariasi tergantung pada konteks dan persepsi. Dalam penggunaan umum, istilah "hacker" sering kali mengacu pada orang yang melakukan kegiatan jahat, sedangkan dalam komunitas keamanan informasi, istilah "hacker" dapat merujuk pada orang dengan pengetahuan dan keterampilan yang luas dalam bidang teknologi dan keamanan informasi.	
	Total	100

b) Lembar Observasi

Tugas Kelompok 2
Buatlah kelompok yang terdiri dari 2 orang. erikut adalah langkah-langkah untuk menginstal Kali Linux di VirtualBox: Unduh Kali Linux ISO:

- Kunjungi situs resmi Kali Linux (https://www.kali.org/downloads/) dan unduh file ISO terbaru dari Kali Linux.
- Pilih versi yang sesuai dengan arsitektur dan kebutuhan Anda (32-bit atau 64-bit).

Buat Mesin Virtual di VirtualBox:

- Buka VirtualBox dan klik tombol "New" untuk membuat mesin virtual baru.
- Berikan nama untuk mesin virtual, misalnya "Kali Linux", dan pilih jenis sistem operasi sebagai "Linux" dan versi sebagai "Debian" (jika tidak ada pilihan Debian, pilih yang sesuai).
- Tentukan jumlah memori yang ingin dialokasikan untuk mesin virtual (disarankan minimal 2 GB).
- Pilih opsi "Create a virtual hard disk now" dan lanjutkan.

Konfigurasi Virtual Hard Disk:

- Pilih jenis file virtual hard disk sebagai "VDI" (VirtualBox Disk Image).
- Pilih opsi alokasi ruang pada hard disk, misalnya "Dynamically allocated" yang akan mengalokasikan ruang hard disk sesuai kebutuhan saat digunakan.
- Tentukan ukuran hard disk virtual (disarankan minimal 20 GB).
- Klik "Create" untuk membuat virtual hard disk.

Konfigurasi Pengaturan Mesin Virtual:

- Pilih mesin virtual "Kali Linux" yang baru dibuat pada panel VirtualBox.
- Klik tombol "Settings" untuk mengatur pengaturan mesin virtual.
- Pada tab "System", pastikan "Processor" ditetapkan pada jumlah CPU yang diinginkan.
- Pada tab "Storage", pilih ikon "Empty" di bagian "Controller: IDE" dan di sebelah kanan, pilih ikon CD/DVD.
- Klik ikon folder di bagian "Attributes" dan pilih file ISO Kali Linux yang sudah diunduh.
- Klik "OK" untuk menyimpan pengaturan.

Mulai Instalasi Kali Linux:

- Klik "Start" untuk memulai mesin virtual.
- Setelah mesin virtual dimulai, pilih opsi "Install" atau "Graphical install" untuk memulai proses instalasi Kali Linux.
- Ikuti panduan instalasi yang ditampilkan di layar, termasuk pengaturan bahasa, lokasi, dan pengaturan pengguna.
- Saat diminta, pilih partisi disk yang tersedia untuk instalasi Kali Linux atau buat partisi baru jika diperlukan.
- Tunggu hingga proses instalasi selesai.

Selesaikan Instalasi:

- Setelah proses instalasi selesai, restart mesin virtual.
- Setelah mesin virtual reboot, Anda akan melihat layar login Kali Linux.
- Masukkan informasi login yang telah Anda buat selama proses instalasi.
- Selamat! Anda sekarang memiliki Kali Linux yang terinstal di VirtualBox.

Pastikan untuk mencatat dan mengambil screenshot dari tiap langkah yang dilewati untuk bahan presentasi dan diskusi nantinya

Tugas Kelompok 2.1

Silahkan jawab pertanyaan-pertanyaan berikut ini dengan bahasa kamu sendiri!

1. Apa itu sistem operasi virtualisasi, dan bagaimana penggunaannya dalam kegiatan ethical hacking?
2. Sebutkan lima tools virtualisasi populer digunakan ?
3. Apa perbedaan antara tipe hypervisor tumpukan penuh (bare-metal) dan tipe hypervisor hosted?
4. Bagaimana VirtualBox memfasilitasi virtualisasi dan bagaimana ia dapat digunakan untuk kegiatan ethical hacking?
5. Berikan contoh fitur keamanan penting yang disediakan oleh Kali Linux untuk kegiatan ethical hacking

Kunci jawaban dan norma penilaian

No	Kunci Jawaban	Skor
1	Sistem operasi virtualisasi adalah teknologi yang memungkinkan pengguna untuk menjalankan beberapa sistem operasi yang terisolasi secara simultan pada satu komputer fisik. Dalam kegiatan ethical hacking, virtualisasi dapat digunakan untuk membuat lingkungan terisolasi yang aman untuk menguji dan mengembangkan teknik keamanan, melakukan penetrasi tes, atau menjalankan alat-alat hacking tanpa merusak sistem operasi utama.	20
2	a) VirtualBox: Platform virtualisasi cross-platform yang dapat diinstal di berbagai sistem operasi. b) VMware Workstation: Program virtualisasi yang populer dengan fitur-fitur canggih untuk penggunaan profesional. c) Hyper-V: Platform virtualisasi bawaan di sistem operasi Windows yang mendukung virtualisasi tingkat server.	20

	d) KVM (Kernel-based Virtual Machine): Infrastruktur virtualisasi di Linux yang memanfaatkan kernel Linux. e) Parallels Desktop: Platform virtualisasi yang dirancang khusus untuk sistem operasi macOS.	
3	Tipe hypervisor tumpukan penuh (bare-metal hypervisor) adalah hypervisor yang berjalan langsung pada perangkat keras fisik dan mengelola langsung sistem operasi tamu. Tipe hypervisor hosted, di sisi lain, berjalan di atas sistem operasi host dan menggunakan sumber daya perangkat keras melalui sistem operasi tersebut. Tipe hypervisor tumpukan penuh memiliki kinerja yang lebih baik karena tidak ada lapisan tambahan, sementara tipe hypervisor hosted lebih fleksibel dan mudah digunakan karena bergantung pada sistem operasi host.	20
4	VirtualBox adalah platform virtualisasi populer yang memungkinkan pengguna untuk menjalankan sistem operasi tamu di dalam sistem operasi host. Ia menyediakan lingkungan terisolasi yang aman untuk melakukan kegiatan ethical hacking, di mana pengguna dapat menginstal sistem operasi seperti Kali Linux dan menggunakan tools hacking yang tersedia di dalamnya. VirtualBox menyediakan fitur seperti snapshotting (pencitraan), jaringan terlarang, dan konfigurasi yang fleksibel untuk mendukung kegiatan ethical hacking.	20
5	Kali Linux, sebagai distribusi Linux khusus untuk kegiatan ethical hacking, menyediakan banyak fitur keamanan yang berguna. Beberapa contoh fitur penting yang disediakan oleh Kali Linux adalah: a) Metasploit Framework: Framework yang kuat untuk pengeksplorasian keamanan dan pengujian penetrasi. b) Aircrack-ng: Tool untuk menguji keamanan jaringan nirkabel dan pemulihan kunci WEP dan WPA. c) Wireshark: Alat penganalisis paket	20
	Total	100

Tugas Kelompok 3 (pertemuan ke 3)
Silahkan jawab pertanyaan-pertanyaan berikut ini dengan bahasa kamu sendiri! 1. Apa yang dimaksud dengan optimalisasi dalam konteks Kali Linux? 2. Mengapa penting untuk mengoptimalkan Kali Linux? 3. Apa perintah untuk melihat direktori saat ini di Kali Linux?

4. Bagaimana cara membuat direktori baru di Kali Linux?
5. Bagaimana cara membuat file kosong di Kali Linux?
6. Apa perbedaan antara perintah "kill" dan "pkill" dalam Linux, dan bagaimana cara menggunakannya secara efektif untuk menghentikan proses yang berjalan?
7. Jelaskan perbedaan antara sistem file ext3 dan ext4 dalam Linux, serta keuntungan dan kelemahannya masing-masing.
8. Bagaimana cara mengoptimalkan penggunaan CPU dalam Linux menggunakan perintah dan teknik yang tersedia?
9. Jelaskan perintah "cron" dalam Linux dan bagaimana cara menggunakannya untuk menjalankan tugas terjadwal secara otomatis
10. Apa yang dimaksud dengan "swappiness" dalam Linux dan bagaimana cara mengkonfigurasinya untuk mengoptimalkan penggunaan swap space?

Kunci jawaban dan norma penilaian		
No	**Kunci Jawaban**	**Skor**
1	Optimalisasi dalam konteks Kali Linux mengacu pada proses mengoptimalkan kinerja dan efisiensi sistem operasi untuk meningkatkan kecepatan, responsifitas, dan penggunaan sumber daya yang lebih baik.	10
2	Mengoptimalkan Kali Linux penting karena dapat meningkatkan produktivitas dan efektivitas dalam kegiatan ethical hacking. Dengan memaksimalkan kinerja sistem, pengguna dapat menjalankan aplikasi dan tools dengan lebih cepat dan responsif, serta menghindari masalah kinerja yang menghambat aktivitas.	10
3	Bagaimana cara membuat direktori baru di Kali Linux? Jawaban: Perintahnya adalah mkdir. Contoh penggunaannya adalah mkdir nama_direktori untuk membuat direktori baru dengan nama yang Anda tentukan.	10
4	Perintahnya adalah cd. Misalnya, cd nama_direktori akan memindahkan Anda ke direktori dengan nama yang Anda tentukan.	10
5	Perintahnya adalah touch. Misalnya, touch nama_file akan membuat file baru dengan nama yang Anda tentukan	10
6	Perbedaan antara perintah "kill" dan "pkill" dalam Linux adalah sebagai berikut: "kill" digunakan untuk menghentikan proses dengan mengirimkan sinyal ke proses tersebut berdasarkan ID proses (PID).	10

	"pkill" digunakan untuk menghentikan proses berdasarkan nama proses atau pola nama proses	
7	Perbedaan antara sistem file ext3 dan ext4 dalam Linux adalah sebagai berikut: Ext3 adalah sistem file berbasis jurnal (journaling file system) yang memungkinkan pemulihan cepat setelah kegagalan sistem. Ext4 adalah pengembangan dari Ext3 dengan peningkatan performa, kehandalan, dan kapasitas. Ext4 memiliki batas ukuran file yang lebih besar, dukungan untuk metadata yang lebih baik, alokasi blok yang lebih efisien, dan peningkatan kinerja pada operasi pembacaan/tulisan.	10
8	Untuk mengoptimalkan penggunaan CPU dalam Linux, beberapa perintah dan teknik yang dapat digunakan antara lain: Menggunakan perintah "nice" atau "renice" untuk mengatur prioritas eksekusi proses. Memantau penggunaan CPU dengan perintah "top" atau "htop" untuk mengidentifikasi proses yang memakan sumber daya. Menonaktifkan atau mematikan layanan yang tidak diperlukan untuk mengurangi beban CPU.	10
9	Perintah "cron" dalam Linux digunakan untuk menjalankan tugas terjadwal secara otomatis. Untuk menggunakannya, Anda perlu menambahkan entri pada file crontab dengan menggunakan sintaks yang sesuai dengan jadwal yang diinginkan.	10
10	"Swappiness" dalam Linux adalah kecenderungan sistem untuk menggunakan swap space saat memori fisik hampir penuh. Untuk mengoptimalkan penggunaan swap space, Anda dapat mengatur nilai swappiness yang lebih rendah untuk mengurangi penggunaan swap dan memaksimalkan penggunaan memori fisik.	10
	Total	100

Tugas Kelompok 4 (pertemuan ke 4)
Silahkan jawab pertanyaan-pertanyaan berikut ini dengan bahasa kamu sendiri! 1. Apa perbedaan antara passive dan active information gathering dalam konteks hacking, dan berikan contoh teknik yang mewakili masing-masing pendekatan tersebut? 2. Jelaskan perbedaan antara teknik Open Source Intelligence (OSINT) dan Social

Engineering dalam information gathering, serta bagaimana Kali Linux dapat digunakan untuk mendukung kedua teknik tersebut.

3. Apa itu DNS enumeration dan bagaimana Kali Linux dapat digunakan untuk melakukan teknik ini dalam upaya information gathering?
4. Jelaskan peran alat Nmap dalam information gathering dan bagaimana cara menggunakannya secara efektif di Kali Linux.
5. Bagaimana cara mengidentifikasi rentang alamat IP yang aktif dalam suatu jaringan menggunakan Kali Linux, dan sebutkan alat-alat yang dapat digunakan untuk tujuan ini.
6. Jelaskan peran alat Recon-ng dalam information gathering dan bagaimana cara menggunakannya di Kali Linux.
7. Apa itu "Google Dorking" dan bagaimana Kali Linux dapat digunakan untuk melakukan pencarian terfokus menggunakan dork-dork Google?
8. Bagaimana teknik WHOIS dapat digunakan untuk mendapatkan informasi tentang domain dan entitas yang terkait di Kali Linux?
9. Jelaskan perbedaan antara teknik "scanning" dan "enumeration" dalam information gathering, serta alat-alat yang dapat digunakan untuk masing-masing teknik tersebut di Kali Linux.
10. Bagaimana Kali Linux dapat digunakan untuk mengumpulkan informasi dari jaringan sosial (social media) sebagai bagian dari proses information gathering dalam hacking?

Kunci jawaban dan norma penilaian		
No	**Kunci Jawaban**	**Skor**
1	Passive information gathering adalah pendekatan di mana penyerang mengumpulkan informasi tanpa berinteraksi langsung dengan target. Contohnya adalah memantau aktivitas online target atau mencari informasi publik tentang target. Active information gathering melibatkan interaksi langsung dengan target, seperti melakukan scanning jaringan atau mencoba mendapatkan informasi melalui teknik social engineering.	10
2	Teknik Open Source Intelligence (OSINT) melibatkan pengumpulan informasi dari sumber publik, seperti mesin pencari, situs web, atau media sosial, untuk mendapatkan wawasan tentang target. Social Engineering adalah teknik manipulasi psikologis untuk memperoleh informasi dari individu secara tidak sah. Kali Linux dapat digunakan dengan alat-alat seperti Maltego untuk mendukung OSINT dan alat-alat seperti Social Engineering	10

	Toolkit (SET) untuk mendukung social engineering.	
3	DNS enumeration adalah teknik untuk mengumpulkan informasi tentang domain, subdomain, dan host yang terkait dengan target. Kali Linux menyediakan alat seperti "dnsenum" dan "dnsrecon" yang dapat digunakan untuk melakukan teknik ini..	10
4	Nmap adalah alat yang sangat berguna dalam information gathering. Ia dapat digunakan untuk melakukan pemindaian jaringan, mendeteksi port terbuka, mengidentifikasi sistem operasi yang digunakan, dan bahkan melakukan pemetaan topologi jaringan. Dalam Kali Linux, Anda dapat menggunakan perintah "nmap" untuk mengakses fungsi-fungsi ini.	10
5	Untuk mengidentifikasi rentang alamat IP yang aktif dalam suatu jaringan menggunakan Kali Linux, Anda dapat menggunakan alat-alat seperti "netdiscover" atau "arp-scan". Alat-alat ini akan memindai jaringan dan menampilkan daftar alamat IP yang aktif.	10
6	Recon-ng adalah alat pengumpulan informasi yang kuat yang dapat digunakan dalam information gathering. Ia menyediakan berbagai modul yang dapat digunakan untuk mengumpulkan informasi dari berbagai sumber. Di Kali Linux, Anda dapat mengakses Recon-ng melalui perintah "recon-ng".	10
7	"Google Dorking" adalah teknik menggunakan operator dan sintaksis khusus dalam mesin pencari Google untuk melakukan pencarian terfokus dan mendapatkan informasi yang tersembunyi atau tidak terindeks. Kali Linux menyediakan alat-alat seperti "googledorks" yang dapat membantu dalam pelaksanaan teknik ini.	10
8	Teknik WHOIS melibatkan mencari informasi tentang domain dan entitas yang terkait melalui database WHOIS. Di Kali Linux, Anda dapat menggunakan perintah "whois" untuk mengakses informasi ini.	10
9	Scanning adalah teknik untuk mengidentifikasi layanan dan port yang aktif di suatu jaringan, sementara enumeration adalah teknik untuk mengumpulkan informasi lebih lanjut tentang sistem dan jaringan yang terdeteksi. Dalam Kali Linux, alat-alat seperti "Nmap" dapat digunakan untuk melakukan scanning, sementara alat-alat seperti "enum4linux" atau "smbmap" dapat digunakan untuk melakukan enumeration	10
10	Kali Linux dapat digunakan untuk mengumpulkan informasi dari jaringan sosial dengan menggunakan alat-alat seperti	10

	"theHarvester" atau "Maltego". Alat-alat ini dapat digunakan untuk mencari informasi publik dari platform media sosial tentang target yang relevan dengan proses information gathering dalam hacking.penggunaan swap dan memaksimalkan penggunaan memori fisik.	
	Total	100

Tugas Kelompok 5 (pertemuan ke 5)

1. Apa itu scanning network?
2. Mengapa scanning network penting dalam konteks keamanan informasi?
3. Apa perbedaan antara scanning network dan footprinting?
4. Apa saja tujuan dari melakukan scanning network?
5. Apa teknik-teknik umum yang digunakan dalam scanning network?
6. Bagaimana cara mendeteksi adanya sistem yang aktif dalam jaringan?
7. Apa itu banner grabbing dalam konteks scanning network?
8. Apa peran IDS (Intrusion Detection System) dalam menghadapi scanning network?
9. Bagaimana cara melindungi jaringan dari scanning network yang berpotensi menjadi serangan?
10. Apa pentingnya melakukan scanning network sebagai bagian dari pengujian penetrasi atau penilaian keamanan sistem?

JAWABAN

Berikut adalah jawaban terkait scanning network:

1. Scanning network adalah proses yang dilakukan untuk mengidentifikasi sistem, layanan, dan konfigurasi jaringan yang berpotensi menjadi sasaran serangan.
2. Teknik-teknik yang umum digunakan dalam scanning network meliputi port scanning, vulnerability scanning, service enumeration, dan OS fingerprinting.
3. Scanning network membantu dalam mengidentifikasi sistem yang aktif dalam jaringan, membuka port yang terbuka, dan layanan yang berjalan.
4. NetBIOS enumeration adalah proses mengumpulkan informasi tentang sistem, pengguna, dan berbagai sumber daya yang terhubung dalam jaringan menggunakan protokol NetBIOS.
5. Enumerasi sistem menggunakan default passwords adalah teknik untuk mencoba login ke sistem menggunakan kata sandi default atau umum yang sering digunakan.

6. SNMP enumeration adalah proses mengumpulkan informasi tentang perangkat jaringan yang diatur untuk mengelola melalui protokol SNMP.
7. UNIX/Linux enumeration adalah proses mengumpulkan informasi tentang sistem operasi UNIX atau Linux yang terhubung dalam jaringan, termasuk pengguna, grup, direktori, dan layanan yang berjalan.
8. LDAP enumeration adalah proses mengumpulkan informasi tentang direktori dan entitas yang terkait yang diatur menggunakan protokol LDAP.
9. NTP enumeration adalah proses mengumpulkan informasi tentang server NTP (Network Time Protocol) yang terhubung dalam jaringan, termasuk versi perangkat lunak, zona waktu, dan sinkronisasi waktu.
10. SMTP enumeration adalah proses mengumpulkan informasi tentang server SMTP (Simple Mail Transfer Protocol) yang terhubung dalam jaringan, termasuk daftar alamat email yang valid.

Tugas Kelompok 6 (pertemuan ke 6)

Silahkan jawab pertanyaan-pertanyaan berikut ini dengan bahasa kamu sendiri!

1. Berikut adalah beberapa pertanyaan pemantik yang dapat digunakan untuk memulai diskusi tentang Enumerasi:
2. Apa yang dimaksud dengan Enumerasi dalam konteks keamanan sistem dan jaringan?
3. Mengapa Enumerasi menjadi tahap penting dalam pengujian keamanan?
4. Apa saja teknik yang digunakan dalam Enumerasi untuk mengumpulkan informasi tentang sistem dan jaringan?
5. Mengapa penting untuk melakukan Enumerasi terhadap services dan ports yang berjalan dalam suatu sistem?
6. Bagaimana NetBIOS Enumerasi dapat membantu dalam mengidentifikasi dan memetakan sistem dan sumber daya?
7. Mengapa penggunaan password default atau umum yang belum diubah merupakan risiko yang serius?
8. Apa peran SNMP dalam Enumerasi dan bagaimana tekniknya digunakan untuk mengumpulkan informasi tentang perangkat jaringan?
9. Bagaimana Enumerasi pada sistem UNIX/Linux dapat membantu dalam mendapatkan informasi tentang pengguna, grup, dan sumber daya lainnya?
10. Apa yang dimaksud dengan Enumerasi LDAP dan bagaimana tekniknya digunakan

untuk mengumpulkan informasi tentang direktori dan entitas dalam sistem?

11. Mengapa Enumerasi pada server NTP dan SMTP penting dalam pengujian keamanan?
12. Bagaimana Enumerasi DNS digunakan untuk mengumpulkan informasi tentang domain, server DNS, dan catatan DNS terkait?
13. Apa saja langkah-langkah yang dapat diambil untuk mengurangi risiko Enumerasi dalam sistem dan jaringan?
14. Apa peran pengujian Enumerasi dalam mengidentifikasi kerentanan potensial dalam sistem?

Bagaimana pengujian Enumerasi dapat membantu dalam meningkatkan keamanan sistem dan melindungi dari serangan Enumerasi yang berbahaya?

Jawaban

1. Apa yang dimaksud dengan Enumerasi dalam konteks keamanan sistem dan jaringan?

Enumerasi adalah proses pengumpulan informasi tentang sistem, jaringan, dan entitas terkait dengan tujuan mengidentifikasi dan memetakan sasaran yang akan diserang. Ini melibatkan mengumpulkan data tentang layanan yang berjalan, port yang terbuka, pengguna, grup, sumber daya, konfigurasi, dan informasi penting lainnya.

2. Mengapa Enumerasi menjadi tahap penting dalam pengujian keamanan?

Enumerasi penting dalam pengujian keamanan karena memberikan wawasan mendalam tentang infrastruktur, konfigurasi, dan potensi kerentanan dalam sistem dan jaringan. Informasi yang dikumpulkan melalui Enumerasi dapat membantu penyerang untuk merencanakan serangan yang lebih efektif. Oleh karena itu, melalui pengujian Enumerasi, organisasi dapat mengidentifikasi kerentanan potensial dan mengambil langkah-langkah untuk memperbaikinya sebelum penyerang dapat mengeksploitasi mereka.

3. Apa saja teknik yang digunakan dalam Enumerasi untuk mengumpulkan informasi tentang sistem dan jaringan?

Beberapa teknik yang digunakan dalam Enumerasi meliputi:

- Scanning port: Mengidentifikasi port yang terbuka dan layanan yang berjalan di sistem.
- Enumerasi NetBIOS: Mencari informasi tentang sistem dan sumber daya dalam jaringan menggunakan protokol NetBIOS.
- Enumerasi menggunakan password default: Menguji apakah sistem masih

menggunakan password default atau umum yang belum diubah.

- Enumerasi SNMP: Mengumpulkan informasi tentang perangkat jaringan menggunakan protokol SNMP.
- Enumerasi UNIX/Linux: Mengumpulkan informasi tentang pengguna, grup, dan sumber daya dalam sistem UNIX/Linux.
- Enumerasi LDAP: Mencari informasi dalam direktori menggunakan protokol LDAP.
- NTP Enumeration: Mengumpulkan informasi tentang server NTP dan konfigurasi waktu.
- SMTP Enumeration: Mengumpulkan informasi tentang server SMTP dan alamat email yang valid.
- DNS Enumeration: Mengumpulkan informasi tentang domain, server DNS, dan catatan DNS terkait.

4. Mengapa penting untuk melakukan Enumerasi terhadap services dan ports yang berjalan dalam suatu sistem?

Enumerasi terhadap services dan ports yang berjalan dalam suatu sistem penting karena memberikan wawasan tentang layanan yang terekspos dan port yang terbuka. Informasi ini dapat membantu penyerang untuk memahami keadaan sistem dan mengidentifikasi kerentanan yang mungkin ada. Dengan memahami layanan dan port yang berjalan, organisasi dapat mengambil langkah-langkah untuk memperkuat keamanan sistem dengan menutup port yang tidak perlu dan memastikan bahwa layanan yang berjalan memiliki konfigurasi yang aman.

5. Bagaimana NetBIOS Enumerasi dapat membantu dalam mengidentifikasi dan memetakan sistem dan sumber daya?

NetBIOS Enumerasi digunakan untuk mengumpulkan informasi tentang sistem dan sumber daya dalamjaringan yang menggunakan protokol NetBIOS. Dengan melakukan NetBIOS Enumerasi, penyerang dapat mengidentifikasi sistem yang aktif dalam jaringan, mengumpulkan informasi tentang pengguna, grup, sumber daya bersama, dan melakukan pemetaan jaringan. Informasi ini dapat digunakan untuk merencanakan serangan yang lebih terarah dan mengidentifikasi kerentanan potensial dalam sistem.

6. Mengapa penggunaan password default atau umum yang belum diubah merupakan risiko yang serius?

Penggunaan password default atau umum yang belum diubah merupakan risiko yang serius karena penyerang dapat dengan mudah menebak atau mencari password tersebut. Jika password default atau umum digunakan, sistem menjadi rentan terhadap serangan brute force atau serangan kata sandi lainnya. Penyerang dapat memperoleh akses tidak sah ke sistem dan merusak integritas, kerahasiaan, dan ketersediaan data yang sensitif. Oleh karena itu, penting bagi organisasi dan pengguna untuk mengubah password default dan memilih password yang kuat untuk

melindungi sistem mereka.

7. Apa peran SNMP dalam Enumerasi dan bagaimana tekniknya digunakan untuk mengumpulkan informasi tentang perangkat jaringan?

SNMP (Simple Network Management Protocol) digunakan untuk memantau dan mengelola perangkat jaringan. Dalam konteks Enumerasi, SNMP dapat digunakan untuk mengumpulkan informasi tentang perangkat jaringan seperti router, switch, dan printer. Teknik SNMP Enumerasi melibatkan mengirim permintaan SNMP ke perangkat jaringan dan menganalisis responsenya. Informasi yang dikumpulkan melalui SNMP Enumerasi dapat mencakup versi perangkat lunak, konfigurasi, pengguna, dan statistik jaringan lainnya. Hal ini memungkinkan penyerang untuk memahami lebih lanjut tentang infrastruktur jaringan dan mengidentifikasi potensi kerentanan.

8. Bagaimana Enumerasi pada sistem UNIX/Linux dapat membantu dalam mendapatkan informasi tentang pengguna, grup, dan sumber daya lainnya?

Enumerasi pada sistem UNIX/Linux melibatkan mengumpulkan informasi tentang pengguna, grup, dan sumber daya lainnya dalam sistem. Dengan melakukan Enumerasi ini, penyerang dapat memperoleh daftar pengguna yang ada, hak akses, dan sumber daya bersama yang dapat dieksplorasi lebih lanjut. Informasi ini dapat membantu penyerang dalam merencanakan serangan yang ditargetkan terhadap pengguna atau sistem tertentu dan mengidentifikasi celah keamanan dalam konfigurasi pengguna dan grup.

9. Apa yang dimaksud dengan Enumerasi LDAP dan bagaimana tekniknya digunakan untuk mengumpulkan informasi tentang direktori dan entitas dalam sistem?

Enumerasi LDAP melibatkan penggunaan protokol LDAP (Lightweight Directory Access Protocol) untuk mengumpulkan informasi tentang direktori dan entitas dalam sistem. Dalam Enumerasi LDAP, penyerang dapat mencari dan mengambil informasi dari direktori, seperti pengguna, grup, atribut entitas, dan hak akses. Informasi ini dapat membantu penyerang dalam memahami struktur direktori, hierarki pengguna, dan hubungan entitas dalam sistem.

10. Mengapa Enumerasi Countermeasures dan PenTesting diperlukan dalam konteks keamanan sistem dan jaringan?

Enumerasi Countermeasures (langkah-langkah pencegahan) dan PenTesting (pengujian penetrasi) diperlukan dalam konteks keamanan sistem dan jaringan untuk melindungi sistem dari serangan Enumerasi dan mengidentifikasi kerentanan yang ada. Enumerasi Countermeasures melibatkan penerapan tindakan keamanan yang efektif, seperti menutup port yang tidak perlu, mengatur kebijakan kata sandi yang kuat, mengimplementasikan pemantauan jaringan, dan mengupdate sistem secara teratur. Sementara itu, PenTesting melibatkan melakukan pengujian keamanan secara aktif untuk mengidentifikasi kerentanan dalam sistem dan jaringan. Melalui kombinasi Enumerasi Countermeasures dan PenTesting, organisasi dapat meningkatkan

keamanan sistem dan jaringan mereka serta mengurangi risiko serangan Enumerasi.

Tugas Kelompok 7 (pertemuan ke 7)

Silahkan jawab pertanyaan-pertanyaan berikut ini dengan bahasa kamu sendiri!

Apa yang dimaksud dengan keystroke loggers dan spyware?

Apa tujuan utama dari penggunaan keystroke loggers dan spyware oleh penyerang?

Apa saja jenis-jenis keystroke loggers dan spyware yang sering digunakan?

Bagaimana cara kerja keystroke loggers dalam mencuri informasi pengguna?

Apa perbedaan antara keyloggers dan spyware?

Apa saja teknik anti-keylogger yang dapat digunakan untuk melindungi sistem dari serangan tersebut?

Bagaimana pentingnya keamanan keystroke dan spyware dalam menjaga privasi dan keamanan data?

Bagaimana cara mendeteksi keberadaan keystroke loggers dan spyware di dalam sistem?

Apa langkah-langkah yang dapat diambil untuk mencegah serangan keystroke loggers dan spyware?

Bagaimana cara melindungi diri dari pencurian password menggunakan keyloggers?

JAWABAN

1. Keystroke loggers adalah perangkat lunak atau perangkat keras yang merekam setiap ketukan tombol yang dilakukan pengguna pada keyboard, sedangkan spyware adalah jenis perangkat lunak yang mengumpulkan informasi tentang pengguna tanpa izin atau pengetahuan mereka.
2. Tujuan utama penggunaan keystroke loggers dan spyware oleh penyerang adalah

mencuri informasi sensitif, seperti kata sandi, nomor kartu kredit, dan data pribadi lainnya.

3. Jenis-jenis keystroke loggers dan spyware meliputi perangkat lunak berbahaya, trojan, keyloggers berbasis perangkat keras, dan spyware berbasis peramban web.
4. Keystroke loggers mencuri informasi pengguna dengan merekam dan menyimpan setiap ketukan tombol yang dilakukan pengguna pada keyboard, termasuk kata sandi dan pesan yang diketik.
5. Perbedaan antara keyloggers dan spyware adalah fokus utama keyloggers pada merekam ketukan tombol, sedangkan spyware lebih luas dalam mencuri informasi pengguna dan melacak aktivitas online mereka.
6. Teknik anti-keylogger meliputi penggunaan perangkat lunak keamanan yang dapat mendeteksi dan menghapus keyloggers, penggunaan virtual keyboard untuk menghindari keystroke loggers, dan penggunaan kebijakan keamanan yang ketat.
7. Keamanan keystroke dan spyware penting untuk melindungi privasi dan keamanan data pengguna. Informasi yang dicuri oleh keyloggers dan spyware dapat digunakan untuk pencurian identitas, penipuan finansial, dan pelanggaran privasi pribadi.
8. Deteksi keberadaan keystroke loggers dan spyware dapat dilakukan dengan menggunakan perangkat lunak anti-spyware dan memantau aktivitas yang mencurigakan di sistem.
9. Langkah-langkah pencegahan termasuk menginstal perangkat lunak keamanan yang mutakhir, menghindari mengklik tautan atau lampiran yang mencurigakan, dan menjaga sistem operasi dan perangkat lunak selalu diperbarui.
10. Untuk melindungi diri dari pencurian password menggunakan keyloggers, disarankan untuk menggunakan autentikasi dua faktor, menggunakan password yang kuat dan unik, serta menghindari memasukkan informasi sensitif di komputer yang tidak dipercaya.

Tugas Kelompok 8 (pertemuan ke 8)

1.Buatlah langkah langkah systemHacking menggunakan metasploit framework

2. kumpulkan tugas tersebut dalam bentuk File Presentasi dan Video

3. Tugas Presentasi dikumpulkan melalui form yang ada di grup Google classroom

4. Tugas Video diupload menggunakan youtube kalian masing masing

5. Hasil harus bisa mencantumkan system Operasi yang telah terkena Hacking

6. Tuliskan pengalamanmu menggunakan metasploit windows dan Linux dan apa tantangan diantara keduanya

Contoh penggunaan Metasploit:

erikut adalah contoh penggunaan Metasploit Framework (msfconsole) untuk melakukan beberapa tindakan umum dalam uji penetrasi:

1. Membuka Metasploit Console:
   ```
   msfconsole
   ```

2. Menampilkan modul yang tersedia:
   ```
   show modules
   ```

3. Memilih modul eksploit:
   ```
   use exploit/[nama_modul]
   ```

4. Menampilkan opsi konfigurasi untuk modul yang dipilih:
   ```
   show options
   ```

5. Mengatur nilai opsi konfigurasi:
   ```
   set [nama_opsi] [nilai]
   ```

6. Menjalankan eksploitasi:
   ```
   exploit
   ```

7. Menampilkan sesi yang berhasil didapatkan:
   ```
   ```

```
sessions
```

8. Memilih sesi yang aktif:
```
sessions -i [nomor_sesi]
```

9. Menggunakan shell interaktif pada sesi:
```
sessions -i [nomor_sesi]
```
Kemudian, dapat menjalankan perintah shell seperti di dalam sistem target.

10. Mengakhiri sesi:
```
sessions -K
```

11. Keluar dari Metasploit Console:
```
exit
```
```

Perlu diingat bahwa contoh-contoh di atas hanya mengilustrasikan beberapa tindakan umum yang dapat dilakukan dengan Metasploit Framework. Ada banyak modul dan opsi lain yang tersedia dalam Metasploit yang dapat digunakan untuk skenario uji penetrasi yang lebih spesifik dan kompleks. Disarankan untuk mempelajari lebih lanjut dokumentasi Metasploit Framework untuk memahami seluruh kemampuan dan penggunaannya dengan baik.

| **Tugas Kelompok 9 (pertemuan ke 9 )** |
| --- |
| |

| **Tugas Kelompok 10 (pertemuan ke 10 )** |
| --- |
| |
```

Tugas Kelompok 11 (pertemuan ke 11)

Norma penilaian

No	Aspek penilaian	Skor maks
1	Hasil diskusi	40
2	Kerjasama kelompok	30
3	Tepat waktu	20
	Total skor	90

c) Pengayaan dan Remidi

Soal Remidi
Silahkan jawab pertanyaan-pertanyaan berikut ini dengan bahasa kamu sendiri! 1. Apa kegunaan sistem operasi virtualisasi dalam konteks ethical hacking, dan berikan contoh implementasinya. 2. Apa kelebihan Kali Linux sebagai sistem operasi untuk ethical hacking, dan sebutkan satu contoh fitur keamanannya. 3. Apa perbedaan antara jenis virtualisasi "paravirtualization" dan "full virtualization"? 4. Sebutkan dua tools populer yang tersedia di Kali Linux untuk analisis keamanan jaringan

Kunci jawaban dan norma penilaian		
No	**Kunci Jawaban**	**Skor**
1	Sistem operasi virtualisasi memiliki peran penting dalam ethical hacking dengan memberikan lingkungan yang terisolasi untuk menguji dan mengembangkan teknik keamanan. Contoh implementasinya adalah penggunaan virtualisasi untuk menjalankan Kali Linux sebagai sistem operasi tamu yang secara khusus dirancang untuk kegiatan ethical hacking. Dalam lingkungan virtual, peneliti keamanan dapat melakukan penetrasi tes, menjalankan alat-alat hacking, dan melakukan eksperimen tanpa mempengaruhi sistem operasi utama atau jaringan yang ada.	25
2	Kali Linux memiliki beberapa kelebihan sebagai sistem operasi untuk ethical hacking: Tools dan aplikasi yang disertakan: Kali Linux menyediakan sejumlah besar tools dan aplikasi hacking yang telah terintegrasi secara default. Tools ini mencakup berbagai kategori, seperti analisis jaringan, penetrasi tes, forensik digital, pemulihan kata sandi, dan banyak lagi. Keberadaan tools yang lengkap ini memudahkan praktisi ethical hacking untuk menjalankan berbagai jenis serangan dan penelitian keamanan. Fokus pada keamanan: Kali Linux dikembangkan dengan fokus utama pada keamanan dan pengujian penetrasi. Distribusi ini dirancang untuk memberikan lingkungan yang aman dan terisolasi untuk aktivitas hacking dan pengujian keamanan. Kali Linux juga memastikan pembaruan rutin untuk menjaga kehandalan dan keamanan sistem operasinya. Contoh fitur keamanan dalam Kali Linux: Salah satu contoh fitur keamanan yang signifikan dalam Kali Linux adalah Metasploit Framework. Metasploit Framework adalah platform pengujian penetrasi yang kuat yang menyediakan berbagai alat dan eksploitasi yang dapat digunakan untuk menguji kelemahan sistem, mengembangkan serangan, dan mengelola siklus hidup eksploitasi. Dengan Metasploit Framework, pengguna Kali Linux dapat melakukan pengujian penetrasi yang	25

	komprehensif dan mengidentifikasi celah keamanan dalam sistem yang dituju.	
3	Paravirtualisasi adalah jenis virtualisasi di mana sistem operasi tamu dimodifikasi agar sadar akan lingkungan virtualisasi dan berinteraksi secara langsung dengan hypervisor. Hal ini memungkinkan kinerja yang lebih baik dan efisien, tetapi memerlukan modifikasi pada sistem operasi tamu. Di sisi lain, full virtualization adalah jenis virtualisasi di mana sistem operasi tamu tidak perlu dimodifikasi, dan hypervisor mengelola akses ke perangkat keras secara virtual. Full virtualization memberikan tingkat kompatibilitas yang lebih tinggi, tetapi dapat memiliki overhead kinerja yang lebih besar dibandingkan dengan paravirtualisasi.	25
4	a) Wireshark: Wireshark adalah alat penganalisis paket jaringan yang dapat digunakan untuk memantau, menganalisis, dan merekam lalu lintas jaringan. Wireshark dapat membantu dalam mengidentifikasi celah keamanan, mengeksplorasi serangan jaringan, dan memahami komunikasi jaringan yang terjadi. b) Nmap: Nmap (Network Mapper) adalah scanner jaringan yang kuat yang digunakan untuk pemetaan port dan pengintaian jaringan. Nmap memungkinkan pengguna untuk menemukan host yang aktif, mengeksplorasi layanan yang berjalan di host tersebut, dan mengidentifikasi kerentanan yang mungkin ada dalam jaringan.	25
	Total	100

Soal Pengayaan

- Dalam kegiatan ethical Hacking sangat penting pemilihan sistem operasi yang akan kita gunakan, carilah sistem operasi yang lain selain kali linux dan sertakan deskripsi singkat tentang penggunaan kelebihan dan kekurangannya jika dibandingkan dengan Kali Linux
- Carilah Aplikasi untuk mode Virtualisasi Selain Virtualbox dan sertakan deskripsi singkat tentang penggunaan kelebihan dan kekurangannya

3. Pembelajaran remedial dan pengayaan

a) Remedial

Remedial dilaksanakan setelah diadakan penilaian pengetahuan bagi peserta didik yang mendapat nilai di bawah KKM dengan memberi tugas berupa:

- Mengulang Pendalaman Materi terkait rincian materi yang sulit
- Memanfaatkan peserta didik yang nilainya paling baik dan mempunyai kemampuan lebih untuk melakukan tutor sebaya
- Mengulang Melakukan Evaluasi dengan materi yang sama

b) Pengayaan

Peserta didik yang mendapat nilai di atas KKM diberikan pengayaan berupa:

- Memberikan tugas baru yang sepadan
- Mengembangkan materi yang sudah dikuasai dan membandingkan dari berbagai sumber belajar.

Mengetahui Kepala SMK Negeri 1 Punggelan	Banjarnegara, 19 Juni 2023 Guru Mata Pelajaran,
Drs. Supriyadi **NIP. 19660128 199302 1 002**	**Idiarso, S.Kom** NIP.19830804 202221 1 006

A. Bahan Bacaan

MATERI

Pengenalan dasar Ethical Hacking

I. Pengertian Cyber Ethics

Cyber ethics adalah suatu aturan tak tertulis yang dikenal di dunia IT. Suatu nilai-nilai yang disepakati bersama untuk dipatuhi dalam interaksi antar pengguna teknologi khususnya teknologi informasi. Tidak adanya batas yang jelas secara fisik serta luasnya penggunaan IT di berbagai bidang membuat setiap orang yang menggunakan teknologi informasi diharapkan mau mematuhi cyber ethics yang ada.

Cyber ethics memunculkan peluang baru dalam bidang pendidikan, bisnis, layanan pemerintahan dengan adanya kehadiran internet. Sehingga memunculkan netiket/nettiquette yaitu salah satu etika acuan dalam berkomunikasi menggunakan internet,berpedoman pada IETF (the internet engineering task force), yang menetapkan RFC (netiquette guidelies dalam request for comments)

II. Karakteristik Dunia Maya

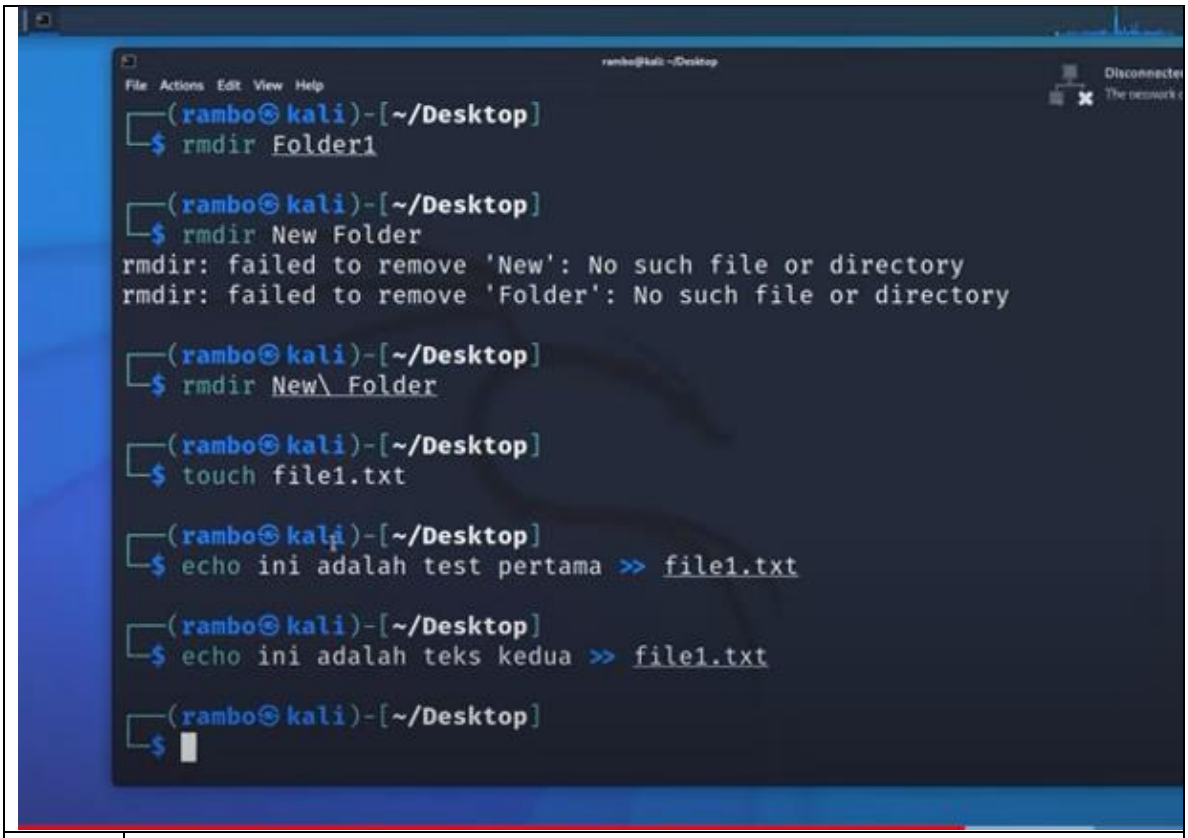
Internet identik dengan cyberspace atau dunia maya. Dysson (1994) cyberscape merupakan suatu ekosistem bioelektronik di semua tempat yang memiliki telepon, kabel coaxial, fiber optic atau elektomagnetik waves. Hal ini berarti bahwa tidak ada yang tahu pasti seberapa luas internet secara fisik.

Karakteristik dunia maya (Dysson : 1994) sebagai berikut :

1. Beroperasi secara virtual / maya
2. Dunia cyber selalu berubah dengan cepat
3. Dunia maya tidak mengenal batas-batas territorial
4. Orang-orang yang hidup dalam dunia maya tersebut dapat melaksanakan aktivitas tanpa harus menunjukkan identitasnya
5. Informasi di dalamnya bersifat public

LINK:	https://www.academia.edu/38111869/etika_profesi_docx

LINK:	https://drive.google.com/drive/u/0/search?q=ethical%20hacking
LINK	https://www.edureka.co/blog/ethical-hacking-using-kali-linux/



LINK:	Optimaslisasi Kali Linux https://www.youtube.com/watch?v=4yZ3qEvJFeg&list=PLGpswQpApOmNQDKPqCpDT8qXdjY-yucDm&index=3
LINK:	Perintah dasar Linux https://www.youtube.com/watch?v=lyBihzENPww&list=PLGpswQpApOmNQDKPqCpDT8qXdjY-yucDm&index=4 Information Gathering https://www.youtube.com/watch?v=CmlVYXGuXig&list=PLGpswQpApOmNQDKPqCpDT8qXdjY-yucDm&index=7&t=7s&pp=iAQB Melacak Email Address dengan theHarvester & Hunter.io https://www.youtube.com/watch?v=tX0rOVmucuw&list=PLGpswQpApOmNQDKPqCpDT8qXdjY-yucDm&index=8&t=368s

	Membuat Tool Email Scraper dengan Python https://www.youtube.com/watch?v=EcNsPGQMOj4&list=PLGpswQpApOmNQDKPqCpDT8qXdjY-yucDm&index=9 Melacak Username dengan Sherlock https://www.youtube.com/watch?v=7MoRUnNYKyc&list=PLGpswQpApOmNQDKPqCpDT8qXdjY-yucDm&index=10

K3LH

K3 (Kesehatan dan Keselamatan Kerja) merupakan suatu usaha dan prosedur agar kesehatan dan keselamatan pekerja serta orang lain yang memasuki tempat kerja terjamin dari bahaya yang dapat menimpa mereka. K3LH dalam menggunakan computer

1. Aturlah posisi tempat duduk anda dengan nyaman serta gunakan kursi yang memiliki sandaran.
2. Aturlah agar layar komputer tidak terlalu terang dan terlalu gelap.
3. Posisikan jarak mata dengan layar komputer 40 - 75 cm.
4. Pastikan ruangan memiliki penerangan yang cukup.
5. Posisikan telapak tangan anda tidak menekuk saat mengetik di komputer.
6. Istirahatkan mata anda 5-15 menit setiap satu jam sekali atau jika mata anda sudah merasa lelah, pijatan pada sekitar mata juga membantu.
7. Istirahatkan badan anda 5-15 menit dan lakukan gerakan peregangan.
8. Istirahatkan tangan anda 5-15 menit saat merasa lelah dan lakukan pijatan.
9. Usahakan meja kerja anda cukup lebar untuk meletakkan peralatan dan perlengkapan kerja anda.
10. Pastikan tidak ada air minum yang tumpah saat anda mengoperasikan komputer.
11. Posisikan kepala, leher, dan punggung tegak.
12. Mengatur secara rapi kabel-kabel pada komputer agar tidak mengganggu pekerjaan.

B. Glosarium

Man-in-the-middle (MITM) Attack : Serangan di mana penyerang memasuki komunikasi antara dua pihak dan mampu membaca, memodifikasi, atau menginterupsi data yang dikirimkan.

Password Cracking : Proses mencoba mendapatkan kata sandi dengan menggunakan metode seperti brute force, dictionary attack, atau rainbow table.

Session Hijacking : Serangan di mana penyerang mengambil alih sesi yang sedang berlangsung antara pengguna dan server untuk mendapatkan akses yang tidak sah.

Wireless Hacking : Proses mengamati, menganalisis, atau mencoba mendapatkan akses tidak sah ke jaringan nirkabel.

Cryptography : Praktik dan metode pengamanan data menggunakan teknik enkripsi untuk melindungi kerahasiaan dan integritas data.

Hypervisor : Perangkat lunak yang memungkinkan pengguna menjalankan beberapa sistem operasi yang terisolasi (mesin virtual) pada satu mesin fisik.

Host Machine : Mesin fisik yang menjalankan hypervisor dan memungkinkan mesin virtual untuk beroperasi.

Guest Machine: Mesin virtual yang berjalan di dalam lingkungan virtual dan menjalankan sistem operasi tamu.

Snapshot: Salinan atau gambaran (image) dari mesin virtual pada titik waktu tertentu yang dapat digunakan untuk memulihkan atau mengembalikan mesin virtual ke kondisi tersebut.

Virtual Switch: Komponen virtual yang digunakan untuk menghubungkan mesin virtual dengan jaringan fisik atau mesin virtual lainnya.

LAMPIRAN

1. Asesmen Diagnostik

a. Non-Kognitif

Informasi apa saja yang ingin digali?	**Pertanyaan kunci yang ingin ditanyakan**
Aktivitas peserta didik selama belajar di rumah	1. Apa saja kegiatanmu sepanjang hari di rumah? 2. kapan waktu paling tepat untuk belajar? 3. Sebutkan 5 hal dari yang paling menyenangkan sampai yang paling tidak menyenangkan ketika sedang belajar? 4. Aplikasi apa saja yang biasa dan bisa dipakai untuk kegiatan belajar?

Informasi apa saja yang ingin digali?	Pertanyaan kunci yang ingin ditanyakan
Aktivitas di rumah mendukung minat dan bakat peserta didik	1. Apa hobimu? 2. Apakah hobimu yang berkaitan dengan program keahlian Pengembangan Perangkat Lunak dan Gim?

LEMBAR ASESMEN DIAGNOSTIK NON KOGNITIF

ASESMEN DIAGNOSTIK NON KOGNITIF

a. Coba amati lingkungan saat ini, lalu pilih emoji berikut yang mewakili perasaanmu. (lingkari pada gambar)

b. Apa saja kegiatanmu sepanjang hari di rumah?
c. Kapan waktu paling tepat untuk belajar?
d. Sebutkan 5 hal dari yang paling menyenangkan sampai yang paling tidak menyenangkan ketika sedang belajar?
e. Aplikasi apa saja yang biasa dan bisa dipakai untuk kegiatan belajar?
f. Apa hobimu?
g. Apakah hobimu yang berkaitan dengan program keahlian Pengembangan Perangkat Lunak dan Gim?