

SILABUS KURIKULUM NETWORK ENGINEERING										
Sesi	Durasi	Nama sesi	Learning input	Learning output	Sub Materi	Kegiatan Berkelas	Kegiatan Mandiri	Kegiatan Eksploratif	Kegiatan Terapan	Asesmen/Evaluasi
1	5*45 Menit	Orientasi	Memberikan penjelasan terkait learning journey pelatihan, penggunaan LMS, pengenalan Praktis, Learning Output, Project dan Uji Kompetensi							
2	5*45 Menit	Network Fundamental Bagian 1: OSI Layer & Network Devices (TCP/IP)	Peserta memahami arsitektur OSI dan mengenali perangkat jaringan dasar.	Mengidentifikasi 7 lapisan OSI dan fungsinya. Menjelaskan fungsi perangkat jaringan (end device, intermediary, media). Membedakan jenis protokol jaringan.	OSI Layer (7 lapisan, fokus 3 lapisan terbawah) TCP/IP Layer Komponen jaringan (end device, intermediary device, media). Protokol jaringan dan port (TCP, UDP, HTTP, DNS, dll.)	Jigsaw Puzzle OSI Layer & Device Mapping Siswa dibagi menjadi 7 kelompok, masing-masing mendalami 1 layer dari OSI Model. Setiap kelompok: Membuat kartu peran layer: fungsi, contoh protokol, dan perangkat yang relevan. Menyusun diagram komunikasi data antar komputer dengan menempatkan layer dan perangkat pada posisi yang tepat. Lalu, perwakilan tiap kelompok membentuk tim baru (jigsaw style) dan saling menjelaskan peran layer masing-masing.	Bagaimana menurutmu model OSI membantu kita memahami cara kerja jaringan? Dari semua layer, mana yang menurutmu paling penting? Kenapa? Apa dampaknya jika salah satu layer atau perangkatnya mengalami gangguan?	Pemaparan oleh Tutor: Penjelasan 7 layer OSI dari Physical hingga Application, lengkap dengan fungsi dan protokol umum. Perbandingan TCP/IP dan OSI (singkat sebagai tambahan wawasan). Pengantar perangkat jaringan: Switch: menghubungkan perangkat dalam LAN. Router: mengarahkan lalu lintas antar jaringan. Hub vs Switch. Access Point, Modem, Network Interface Card. Diagram komunikasi data dan bagaimana data berpindah antar layer.	Simulasi & Mini Case: Pilih Perangkat yang Tepat Siswa menganalisis 3 studi kasus sederhana, misalnya: Mendesain jaringan sederhana untuk kafe. Menyambungkan dua kantor cabang. Menambahkan Wi-Fi di area sekolah. Tugas: Menentukan kebutuhan perangkat jaringan berdasarkan skenario. Menjelaskan peran setiap perangkat dalam sistem komunikasi data. Menghubungkannya dengan layer OSI yang relevan. Output: Diagram topologi. Penjelasan singkat fungsi perangkat dan lapisan OSI yang aktif.	Mini Quiz (5-7 soal) dan penilaian mini case
3	5*45 Menit	Switching dan VLAN	Peserta memahami konsep VLAN dan switching pada perangkat Mikrotik. Peserta mampu mengimplementasikan konfigurasi jaringan menggunakan VLAN.	siswa mampu: Menjelaskan fungsi VLAN dan trunking dalam jaringan. Membuat dan mengatur VLAN di switch Mikrotik. Mengatur port access dan trunk. Melakukan verifikasi dan troubleshooting VLAN.	Konsep VLAN: segmentasi, isolasi jaringan, penggunaan ID. Perintah VLAN dasar: vlan, name, switchport mode, switchport access. Konfigurasi port access dan trunk. Verifikasi dengan show vlan, show interface switching port. Studi kasus: membuat jaringan dengan 3 VLAN berbeda.	VLAN Puzzle: Slapa Terkoneksi? Siswa diberikan ilustrasi jaringan 6 PC dengan ID VLAN berbeda. Tantangan: sambungkan PC sesuai VLAN yang sama, lalu prediksi siapa yang bisa saling ping. Kartu tambahan: Access Port / Trunk Port (dengan batasan). Diskusi kelompok: kenapa PC A tidak bisa ping PC D? Solusinya apa?	Mengapa VLAN diperlukan dalam jaringan skala besar? Apa perbedaan antara port access dan trunk? Bagaimana cara mendeteksi kesalahan konfigurasi VLAN?	Tutor menjelaskan: Apa itu VLAN: segmentasi logis, ID VLAN, manfaat keamanan dan efisiensi. Perintah dasar: vlan [id], name, interface, switchport mode access/trunk, switchport access vlan [id]. Perbedaan access vs trunk. Perintah verifikasi: show vlan brief, show interfaces switchport.	Konfigurasi 3 VLAN pada Switch. Langkah: Buat topologi: 1 switch, 3 PC untuk 3 VLAN berbeda. Konfigurasi VLAN: VLAN 10: PC1, VLAN 20: PC2, VLAN 30: PC3. Konfigurasi port: Interface PC1 → access vlan 10, Interface PC2 → access vlan 30, Interface PC3 → access vlan 30. Uji komunikasi: pastikan antar VLAN tidak saling ping. Buat 1 switch tambahan sebagai trunk port dan ulangi ping.	Kuis Konsep VLAN (5 soal)
4	5*45 Menit	Routing Dasar (IPv4/IPv6)	Siswa memahami konsep IP Address, subnet mask, dan cara melakukan subnetting. Siswa mampu menghitung pembagian jaringan berdasarkan kebutuhan IP yang berbeda.	siswa mampu: Menjelaskan pengertian IP Address, subnet mask, dan pembagian kelas IP. Menghitung jumlah host, subnet, dan rentang IP menggunakan teknik subnetting. Menentukan IP dan subnet yang sesuai untuk berbagai kebutuhan jaringan. Membedakan IP publik dan IP privat.	IPv4 addressing: struktur, kelas A-B-C. Subnet mask dan pembagian jaringan. Teknik subnetting: perhitungan jumlah host dan subnet. Konsep CIDR (Classless Inter-Domain Routing). IP publik vs IP privat. Studi kasus perhitungan subnet untuk kantor cabang.	IP Puzzle Race Tiap kelompok diberikan kartu IP Address acak dan skenario kebutuhan jaringan (misalnya: "Kantor A butuh 30 host", "Lab komputer butuh 30 perangkat"). Mereka harus: Mengelompokkan IP berdasarkan kelas (A, B, C). Menentukan mana yang publik vs privat. Mencocokkan IP dengan subnet yang tepat.	Kenapa IP Address tidak bisa dibagikan sembarangan? Apa dampak jika subnetting tidak tepat dalam jaringan besar? Pernahkah kalian mengalami konflik IP di sekolah atau rumah?	menjelaskan: Struktur IP Address (IPv4), kelas A/B/C. Subnet mask, pengertian dan penggunaannya. Teknik subnetting: hitung jumlah host, subnet, dan rentang IP. CIDR notation (misal: /24, /26). IP publik vs privat. Studi kasus kantor cabang: pembagian IP antar divisi. Lathan langsung: Hitung kebutuhan subnet untuk 4 departemen, Tentukan alamat IP yang efisien menggunakan teknik CIDR.	Perencanaan Alokasi IP Tiap tim mendapat studi kasus: "Sebuah kantor kecil memiliki 4 departemen dengan kebutuhan: 50, 25, 10, dan 5 perangkat. Rancang alokasi IP-nya dengan subnetting yang tepat." Tugas: Hitung subnet dan mask untuk tiap divisi. Tentukan rentang IP yang digunakan. Gunakan CIDR notation dan tentukan network address + broadcast. Visualisasikan dalam bentuk tabel atau sketsa jaringan sederhana. Output: Lembar kerja perhitungan, Tabel IP allocation per divisi.	Kuis (5 soal)
			Siswa memahami struktur alamat IPv6 dan cara penggunaannya dalam konfigurasi jaringan modem. Siswa mampu menerapkan IPv6 di perangkat Cisco secara sederhana.	siswa mampu: Menjelaskan perbedaan antara IPv4 dan IPv6. Mengidentifikasi jenis-jenis alamat IPv6 (global, link-local, multicast). Mengatur alamat IPv6 pada interface Cisco. Menggunakan perintah dasar untuk melihat dan menguji konfigurasi IPv6.	Struktur alamat IPv6: 128-bit, heksadesimal, notasi prefix. Jenis alamat: Global Unicast, Link Local, Multicast. Konfigurasi dasar IPv6: ipv6 address, ipv6 enable. Verifikasi: show ipv6 interface, ping ipv6. Lathan konfigurasi jaringan IPv6 sederhana di Packet Tracer.	Tebak Alamat IPv6 Siswa dibagi kelompok, tiap kelompok menerima potongan alamat IPv6 (dalam kartu heksadesimal). Tantangan: Susun alamat dengan benar berdasarkan jenis (global/link-local/multicast). Jelaskan fungsi dari prefix, e.g., /64, /128. Kelompok tercepat dan tepat dapat poin.	Apa manfaat utama IPv6 dibanding IPv4 dalam jaringan modern? Mengapa kita perlu memahami jenis-jenis alamat IPv6? Apa potensi kesulitan saat transisi dari IPv4 ke IPv6?	Tutor menjelaskan: Struktur alamat IPv6: 128-bit, dibagi dalam 8 blok heksadesimal. Perbedaan IPv4 vs IPv6: panjang, jumlah alamat, NAT, keamanan. Jenis alamat: Global Unicast: alamat publik. Link-local: alamat lokal otomatis (/EUI64). Multicast: komunikasi ke banyak perangkat. Dasar konfigurasi: ipv6 address 2001::1::1/64, ipv6 enable, show ipv6 interface, ping ipv6.	Konfigurasi IPv6 di Packet Tracer Topologi: 1 Router Cisco, 2 PC. Langkah: Konfigurasi alamat IPv6 pada router dan PC. Router: 2001::1::1/64, PC1: 2001::2::1/64, gateway 2001::1::1. Verifikasi: ping dari PC ke router, show ipv6 interface brief di router. Output: Screenshot CLI konfigurasi dan hasil ping. Penjelasan fungsi setiap alamat dan hasil pengujian.	
5	5*45 Menit	Layanan Jaringan (DHCP, DNS, NAT, QoS)	Siswa memahami dan menerapkan konfigurasi layanan DHCP, NAT, dan static routing pada perangkat Mikrotik untuk mendukung skenario jaringan yang lebih kompleks.	siswa mampu: Mengaktifkan dan mengelola DHCP Server di Mikrotik. Mengatur NAT untuk akses internet melalui gateway. Membuat static route untuk komunikasi antar jaringan berbeda. Menguji dan menganalisis hasil konfigurasi secara langsung.	DHCP Server: pool IP, lease, pengaturan DNS. NAT (masquerade) prinsip dan konfigurasi dasar. Static routing: pengantar routing dan skenario dua jaringan. Uji koneksi dan pemantauan routing table. Studi kasus: jaringan dengan dua router dan satu jalur internet.	"Bangun Dua Dunia" Siswa dibagi per kelompok kecil dan diberi peta skenario: Dua jaringan (Jaringan A dan B) yang harus dihubungkan dengan dua router, di mana hanya satu router yang terhubung ke internet. Tantangan: Bagaimana NAT bekerja jika hanya satu router terhubung ke internet? Mengapa kita perlu membuat routing secara manual antara dua jaringan? Tiap kelompok harus: Mendesain alur IP. Menentukan posisi NAT dan routing. Menyusun flow komunikasi antar jaringan.	Apa peran DHCP dalam mempermudah konfigurasi client? Bagaimana NAT bekerja jika hanya satu router terhubung ke internet? Mengapa kita perlu membuat routing secara manual antara dua jaringan?	Tutor menjelaskan dan mendemonkan: DHCP Server: pengaturan IP pool, DNS, lease time. NAT: fungsi masquerade, gateway, port mapping. Static Routing: route list, gateway, distance. Monitoring: IP leases, routing table, test ping antar jaringan. Studi kasus 2 router: subnet A → subnet B → internet. Drill cepat: Apa hasil ping jika tidak ada route antar jaringan? Di mana seharusnya NAT ditempatkan?	Praktik Jaringan Dua Router Tiap kelompok: Konfigurasi DHCP Server di kedua router. NAT di router yang terkoneksi ke internet. Routing statis antar jaringan. Pengujian: Ping dari subnet A ke B. Akues internet dari subnet B melalui router A. Verifikasi NAT dan routing table.	Output: Screenshot konfigurasi DHCP, NAT, dan routing. Skema topologi IP. Log pengujian ping dan hasil traceroute. Ringkasan fungsi tiap bagian (DHCP, NAT, route).
6	5*45 Menit	Layanan Jaringan (DHCP, DNS, NAT, QoS)	Siswa memahami konsep Quality of Service (QoS) dan pentingnya pengaturan prioritas trafik jaringan. Siswa mampu menerapkan konfigurasi QoS menggunakan Flow Simple Queue dan PCQ di Mikrotik untuk memastikan distribusi bandwidth yang efisien.	siswa mampu: Menjelaskan fungsi dan manfaat QoS dalam jaringan. Membedakan metode pengelolaan bandwidth: Simple Queue vs Queue Tree. Membuat konfigurasi Simple Queue dan menerapkan PCQ untuk pembagian bandwidth otomatis. Menganalisis efektivitas konfigurasi QoS melalui uji kecepatan dan monitoring.	Pengantar Quality of Service (QoS): delay, jitter, throughput. Simple Queue: limit at, max limit, target address. PCQ (Per Connection Queue): penggunaan untuk manajemen bandwidth multi-user. Studi kasus penerapan QoS: prioritas trafik untuk video call dan download. Pengujian hasil konfigurasi menggunakan bandwidth test dan Torch.	"Lomba Berebut Bandwidth" (Simulasi Kompetisi Trafik) Siswa dibagi menjadi 3 tim: Tim A = Video call, Tim B = Download file besar, Tim C = browsing email. Semua tim mencoba akses internet secara bersamaan tanpa QoS → diamati efeknya (siapa yang lambat). Lalu, guru aktifkan Simple Queue dengan PCQ → ulangi simulasi dan bandingkan hasilnya.	Siapa yang "kalah" dalam berebut bandwidth sebelum QoS diaktifkan? Apa manfaat adanya pembagian bandwidth otomatis? Bagaimana persaanmu jika kamu pengguna video call dalam kondisi jaringan padat?	Tutor menjelaskan dan mendemonkan: Konsep dasar QoS: delay, jitter, throughput. Fungsi Simple Queue dan parameter penting (limit at, max limit, target). Penerapan PCQ (Per Connection Queue) dan penggunaannya. Studi kasus: memprioritaskan video call vs download. Pilih monitoring: Bandwidth Test, Torch, Queue List. Lathan singkat: Identifikasi parameter Simple Queue dan cocokkan dengan fungsinya.	Praktik Konfigurasi QoS di Mikroik Tiap tim melakukan: Konfigurasi Simple Queue untuk satu IP. Konfigurasi PCQ untuk jaringan multi-user. Melakukan simulasi trafik (via speedtest, download, ping). Monitoring penggunaan bandwidth. Menganalisis dampak: sebelum dan sesudah QoS.	Output: Screenshot konfigurasi queue. Catatan hasil pengujian dan interpretasi. Grafik penggunaan bandwidth.

7	5*45 Menit	Wireless LAN	Siswa memahami prinsip kerja jaringan nirkabel (wireless LAN) dan perbedaan dengan jaringan kabel. Siswa mampu mengkonfigurasi WLAN menggunakan perangkat Mikrotik. Siswa mengenali tantangan dan praktik terbaik dalam penyebaran jaringan wireless di lingkungan indoor.	Siswa mampu: Menjelaskan prinsip dasar jaringan WLAN dan perbedaannya dengan LAN kabel. Mengidentifikasi komponen utama jaringan wireless seperti Access Point (AP), SSID, dan keamanan jaringan. Melakukan konfigurasi wireless interface di Mikrotik RouterOS. Mengatur SSID, mode wireless, dan tingkat keamanan (WPA/WPA2). Menguji koneksi dan performa jaringan WLAN secara lokal.	Konsep dasar wireless: frekuensi, sinyal, SSID, channel, dan interferensi. Mikrotik wireless mode: AP Bridge, Station, Station Bridge. Konfigurasi wireless interface di Mikrotik. Pengaturan keamanan jaringan WLAN (WPA2, password, MAC filtering). Praktik penyebaran AP indoor: lokasi, hambatan fisik, jangkauan. Troubleshooting dasar koneksi WLAN.	*WLAN Detective: Sinyal di Balik Tembok* Siswa diberi peta layout ruangan (kelas/lab/rumah). Mereka harus: Menetakan lokasi potensial Access Point (AP) Memprediksi jangkauan sinyal & potensi interferensi Lalu, mereka melakukan uji lapangan sinyal dengan ponsel/laptop di 3 titik: Dekat AP Di balik dinding Di ujung ruangan	Di titik mana sinyal paling lemah? Kenapa? Apa yang bisa mengganggu kualitas koneksi WLAN?	Penjelasan dan demo oleh tutor: Prinsip dasar WLAN: SSID, frekuensi, channel, mode wireless Perbedaan AP Bridge, Station, Station Bridge Pengaturan keamanan (WPA2, MAC filtering) Mini drill: Cocokkan jenis mode wireless dengan fungsinya Kuis cepat tentang keamanan WLAN dan konfigurasi SSID Praktik penyebaran AP Indoor: lokasi, hambatan, jangkauan Troubleshooting umum WLAN	Praktik: Konfigurasi WLAN Mikrotik Indoor Tiap kelompok: Mengatur wireless interface Mikrotik menjadi AP Menentukan SSID dan channel yang digunakan Menetapkan mode keamanan (WPA2, password) Menguji koneksi wireless (device client terhubung ke SSID) Melakukan uji kecepatan koneksi lokal dan ping	Output: Screenshot konfigurasi wireless interface Ringkasan lokasi AP & hasil pengujian sinyal Log ping dan hasil kecepatan lokal
8	5*45 Menit	Network Planning	Memetakan kebutuhan & KPI jaringan sekolah. Menyusun desain logis (VLAN, IP, routing) dan fisik (topologi kabel & Wi-Fi). Menetapkan kapasitas, keamanan dasar, dan rencana keandalan. Menyusun rencana implementasi, uji terima, dan paket dokumentasi.	Peserta mampu: • Menghasilkan daftar kebutuhan & KPI layanan jaringan. • Menyusun VLAN & IP plan (VLSM) untuk 25 segmen dengan margin pertumbuhan 230% (optional IPv6). • Membuat diagram logis & fisik awal yang konsisten. • Menetapkan kebijakan ACL, QoS, dan baseline keamanan L2. • Menghitung BOM dan estimasi biaya tingkat tinggi (3 tahun). • Menyusun rencana implementasi, uji, dan rollback yang terukur.	Konteks SMK, pemangku kepentingan, SLA/KPI (uptime, latensi, throughput). Estimasi trafik & pertumbuhan. Layanan: LMS, CCTV, Wi-Fi, Internet, VoIP (rencana). Desain Logis (VLAN & IP Plan). Desain Fisik & Kapasitas. Keamanan, QoS & Keandalan. Implementasi, Uji & Dokumentasi				Studi kasus "SMK Nusantara": 2 gedung (3 lantai), 6 lab, 300 siswa, 50 guru, Internet 300 Mbps, LMS lokal, 10 CCTV, target uptime 99%. Tugas: Rumuskan kebutuhan, KPI, dan asumsi kapasitas puncak (gunakan margin 30%).	Produk: 1-halaman Requirements & KPI Sheet. Format: kuis cepat (5 soal).
9	5*45 Menit	Praktek Industri: pengembangan proyek sekolah								
10	5*45 Menit	Praktek Industri: pengembangan proyek sekolah								
11	5*45 Menit	Microteaching & desiminasi								
12	5*45 Menit	Presentasi Hasil Proyek	Peserta mempresentasikan hasil proyek sekolah							
13	5*45 Menit	Uji Kompetensi/Sertifikasi								

SILABUS KURIKULUM CYBER OPS

Sesi	Durasi	Nama Sesi	Tujuan Sesi (singkat)	Learning Output	Sub Materi (singkat)	Kegiatan Praktek/Simulasi	Aasesmen
1	5*45 Menit	Orientasi Program & Setup Lab	Menyklarakan tujuan, aturan main, dan kesiapan lab daring.	Peserta siap mengikuti kelas, akses lab berhasil, paham alur & rubrik.	Gambaran Cyber Ops; etika & AUP; alur 3 pertemuan; rubrik & bukti artefak; setup VM/cloud lab.	Uji akses platform, import VM/akun lab, uji koneksi, pengalaman repository tugas.	Pre-test; cek kelayakan lab (screenshot); komitmen learning contract.
2	5*45 Menit	Threat Landscape & Dasar Jaringan	Memahami ancaman & fondasi jaringan.	Dapat memetakan risiko dasar di lingkungan SMK.	OA triad, model OSI/TCP-IP; topologi LAN/DWAN; segmentasi VLAN; kebijakan dasar keamanan.	Rancang topologi sekolah sederhana; uji ping/traceroute; simulasi VLAN di Packet Tracer/GNS3.	Kuis konsep; unggah diagram topologi + rationale.
3	5*45 Menit	Perimeter Security: Firewall/NAT/ACL	Mengamankan batas jaringan.	Menyusun ruleset minimal aman untuk skenario sekolah.	Stateful vs stateless; NAT/port-forward; DMZ; priorities & urutan rule; logging.	Konfigurasi rules di pfSense/OPNsense (lab); uji lalu lintas diblokir/dibukir; audit log.	Review ruleset (peer + instruktur); bukti log sukses/tolak.
4	5*45 Menit	Network Monitoring & Packet Analysis	Mendeteksi anomali lalu lintas.	Mampu capture & analisis PCAP sederhana.	Wireshark filter; Netflow; IDS (Zeek/Suricata) konsep; SPAN/mirroring.	Capture skenario scan; identifikasi handshake, DNS, HTTP; analisis alert IDS sampel.	Laporan temuan (IOC, timeline, rekomendasi).
5	5*45 Menit	Endpoint Security & Hardening	Memperkuat host Windows/Linux.	Menerapkan baseline hardening & logging host.	CIS benchmark konsep; patch mgmt; host firewall; Sysmon/auditd; AV/EDR konsep.	Terapkan kebijakan local firewall; instal & konfigurasi Sysmon/auditd; uji event berisiko rendah.	Checklist hardening; bukti log event kunci.
6	5*45 Menit	Identity & Access Management (IAM)	Mengontrol akses berbasis identitas.	Merancang kebijakan IAM dasar (RBAC, MFA, least privilege).	AD/LDAP konsep; RBAC/ABAC; password & MFA; prinsip Zero Trust; audit akses.	Buat struktur pengguna/kelompok; setel kebijakan password; simulasi MFA pada layanan lab; audit hak akses.	Dokumen kebijakan IAM; screenshot penerapan; kuis singkat.
7	5*45 Menit	Secure Network Services & Web	Mengamankan layanan inti sekolah.	Mengonfigurasi layanan web/dns yang aman dasar.	Hardening DNS/DHCP; HTTPS/TLS dasar; reverse proxy; header keamanan; WAF konsep.	Deploy Nginx/reverse proxy (lab); aktifkan TLS; uji header keamanan & redirect; review log akses.	Bukti konfigurasi + hasil uji (report otomatis/manual).
8	5*45 Menit	Vulnerability Management & Basic Pentest	Menemukan & memprioritaskan celah.	Melakukan pemindaian dan menyusun rencana perbaikan.	Etika pentest; Nmap/Nikto; membaca CVE/CVSS; OWASP Top 10 ringkas.	Scan target lab (DVWA/Metasploitable); klasifikasi temuan; rancang mitigasi/patch.	Laporan VA (temuan → prioritas → aksi).
9	5*45 Menit	Incident Response (IR) & Forensik	Menangani insiden awal.	Menulis playbook IR & melakukan triage log.	Fase IR; chain of custody; sumber log (endpoint, network, auth); MITRE ATT&CK mapping; SIEM konsep (WashU/ELSI).	Simulasi insiden (phishing/malware rendah risiko); kumpulkan log; buat rule deteksi sederhana; post-incident review.	Playbook IR + laporan insiden singkat; peta ATT&CK.
10	5*45 Menit	Proyek Sekolah: Desain & Kickoff	Merancang implementasi nyata di SMK.	RPP + modul "Cyber Ops Dasar" siap pilot.	Tujuan & indikator; KI & etika; skenario lab hemat perangkat; rubrik penilaian siswa; rencana diseminasi internal.	Susun RPP & modul praktikum; rancang lab mini (topologi, tools, SOP); setup repo Git untuk artefak.	RPP disetujui (review instruktur); rencana proyek terdokumentasi.
11	5*45 Menit	Microteaching & Diseminasi	Uji ajar dan dapatkan umpan balik.	M/deliver microteaching 20-30 menit dengan demonstrasi lab.	Teknik demonstrasi daring; manajemen kelas; adaptasi device terbatas; strategi diseminasi ke MGMP.	Microteaching via VC; rekam sesi; peer-feedback terstruktur.	Rubrik microteaching (konten, demo, interaksi); rencana diseminasi.
12	5*45 Menit	Presentasi Hasil Proyek	Memaparkan hasil pilot & dampak.	Menyajikan artefak, metrik, dan perbaikan.	KPI proyek; bukti pembelajaran siswa; lesson learned; rencana scale-up.	Presentasi + demo singkat artefak (lab, SOP, modul); tanya jawab panel.	Rubrik presentasi; validasi artefak proyek.
13	5*45 Menit	Uji Kompetensi (Teori + Pratik)	Mengukur penguasaan akhir.	Lulus standar kompetensi Cyber Ops dasar untuk pengajar.	Teori (40%): konsep inti; Pratik (60%): konfigurasi, monitoring, IR mini.	Captstone: konfigurasi firewall, tangkap & analisis trafik, triage log, susun rencana respon.	Skor ujian; portofolio artefak; umpan balik individu.