1. Kriptografi

- **Kriptografi Simetris:** Menggunakan satu kunci untuk mengenkripsi dan mendekripsi data. Contoh algoritma: DES, 3DES, AES, Twofish, Blowfish. Penggunaannya meliputi keamanan data dalam jumlah besar, komunikasi aman, keamanan cloud, dan enkripsi basis data. openssl enc -aes-256-cbc -salt -in
- **Kriptografi Asimetris:** Menggunakan dua kunci berbeda (publik dan privat) untuk enkripsi dan dekripsi. Umumnya dianggap lebih aman, meskipun kurang efisien dibandingkan simetris. Contoh algoritma: RSA, ECC, DSA. Penggunaannya mencakup penjelajahan web, komunikasi aman, tanda tangan digital, autentikasi, dan teknologi blockchain. openssl genrsa -out private_key.pem 2048
- **Fungsi Hash:** Algoritma yang mengubah pesan berukuran variabel menjadi "sidik jari" berukuran tetap. Bersifat satu arah (irreversible) dan digunakan untuk menjaga integritas data, menyimpan password, dan menghemat waktu pengiriman data. Contoh: MD5. md5sum nama_file.txt

2. Keamanan Jaringan: Firewall, IDS, dan VPN

- **Firewall:** Bertindak sebagai filter untuk mengontrol lalu lintas jaringan, mencegah akses tidak sah, mendeteksi dan menghentikan serangan malware, serta melindungi data pengguna. iptables/ufw
- **Intrusion Detection System (IDS):** Sistem yang memantau trafik jaringan untuk mendeteksi intrusi atau aktivitas mencurigakan dan melaporkannya dalam bentuk peringatan. IDS hanya mendeteksi dan memberi peringatan, tidak mengambil tindakan aktif seperti IPS. **Contoh Alat:** Snort, Suricata.
- **Virtual Private Network (VPN):** Bekerja dengan mengenkripsi data, membuat tunneling, dan menyembunyikan IP pengguna untuk memberikan keamanan dan privasi saat mengakses internet.

3. SQL Injection

Aksi hacking yang dilakukan dengan memodifikasi perintah SQL di aplikasi klien, mengeksploitasi celah di aplikasi web yang menggunakan database. Hal ini memungkinkan akses tanpa akun, perubahan/penghapusan data, bahkan mematikan database. Jika website memiliki input SELECT * FROM users WHERE username = 'input_user' menjadi: SELECT * FROM users WHERE username = '' OR '1'='1'

4. Keamanan Cloud Computing

Bertujuan untuk meningkatkan kerahasiaan, integritas, dan ketersediaan sumber daya cloud, serta mencegah akses tidak sah, pelanggaran data, dan ancaman siber lainnya. Aspek utamanya meliputi kontrol akses, keamanan data cloud, deteksi dan respons terhadap ancaman, kepatuhan regulasi, lingkungan pengembangan yang aman, serta visibilitas dan manajemen postur cloud.

5. Forensik Digital

Cabang ilmu forensik yang khusus mengkaji bukti-bukti digital untuk mendukung investigasi kriminal atau perdata. Tujuannya adalah mengumpulkan bukti yang kuat, mengidentifikasi pelaku, memulihkan data hilang, dan menentukan keaslian bukti. Membuat image disk : sudo dd if=/dev/sda of=image.dd bs=4M conv=noerror,sync

6. Serangan Ransomware WannaCry

Menargetkan komputer berbasis Microsoft Windows, mengenkripsi data, dan meminta tebusan dalam Bitcoin. Serangan ini menyebabkan kerugian finansial besar secara global pada tahun 2017. Pencegahan utama adalah memperbarui sistem operasi dan perangkat lunak secara berkala, serta tidak mengklik tautan mencurigakan.

7. Pentest Vulnerability, Pentesting Method (terutama web) & Vuln Assessment

- **Penetration Testing (Pentest):** Serangan resmi pada sistem komputer untuk mengevaluasi keamanan sistem atau jaringan, mengidentifikasi kerentanan dan risikonya.
  Contoh Metode Web Pentest: Mencoba input `' OR '1'='1` untuk SQL Injection, mengunggah file berbahaya untuk *Remote Code Execution*, atau mencoba ID yang berbeda di URL untuk IDOR.
  Contoh Alat: Burp Suite, OWASP ZAP
- **Vulnerability Assessment (Penilaian Kerentanan):** Proses identifikasi, pelacakan, dan pengelolaan perbaikan kerentanan pada sistem atau jaringan.
  Contoh Alat: Nessus, OpenVAS.
  Laporan Singkat: "Ditemukan kerentanan SQL Injection dengan CVSS 9.8 pada `/login.php` dan kerentanan *outdated library* pada server Apache."

8. SOC SIEM

- **Security Operations Center (SOC):** Pusat operasi keamanan yang bertanggung jawab untuk memantau, mendeteksi, menganalisis, dan menanggapi insiden keamanan siber.**COntoh:** Menganalisis *alert* dari SIEM, melakukan *threat hunting*, merespons insiden.
- **Security Information and Event Management (SIEM):** Perangkat lunak yang digunakan SOC untuk mengumpulkan dan menganalisis data keamanan dari berbagai titik di jaringan guna mengidentifikasi pola atau aktivitas mencurigakan.
  Contoh Koriografi di SIEM: "Jika ada 5 percobaan login gagal diikuti 1 login berhasil dari IP yang sama dalam 1 menit, hasilkan alert 'Brute Force Berhasil'."
  Contoh Log yang Dikumpulkan: Log autentikasi, log firewall, log web server, log sistem operasi.

9. Enumeration, Scanning, Exploit

- **Enumeration:** Proses mengumpulkan informasi lebih spesifik tentang sistem atau jaringan, seperti daftar komputer, username, user group, port, OS, nama mesin, sumber daya jaringan, dan layanan. Informasi ini membantu mengidentifikasi celah keamanan. nmap --script smb-enum-users -p 445 192.168.1.100
- **Scanning (Active Scanning):** P emindaian aktif terhadap target untuk mengidentifikasi kerentanan dan celah keamanan yang dapat dimanfaatkan penyerang. Contoh alat: Nmap, Nikto. # Scan port TCP umum pada host 192.168.1.100 nmap 192.168.1.100 # Scan versi layanan dan OS detection nmap -sV -O 192.168.1.100
- **Exploit:** Seperangkat perintah, data, atau perangkat lunak yang memanfaatkan kerentanan untuk aktivitas jahat, membuka peluang bagi peretas. Exploit dapat membahayakan kerahasiaan atau ketersediaan sebuah sistem. msf6 > use exploit/windows/smb/ms17_010_eternalblue (menggunakan *exploit* WannaCry)

Dalam investigasi SIEM ditemukan pola brute force login yang berhasil login setelah 5 kali gagal. Tindakan pertama yang tepat adalah:
Investigasi credential reuse dan lokasi login user
Saat melakukan threat hunting, Anda menemukan adanya proses aneh yang berjalan di endpoint, dengan nama mirip layanan Windows namun berlokasi di folder non-standar. Teknik MITRE ATT&CK apa yang kemungkinan relevan, dan apa langkah pertama Anda?
Persistence – mengumpulkan hash file dan membandingkan dengan reputasi
Setelah investigasi MITRE ATT&CK mapping, Anda mendapati serangan mengeksekusi PowerShell script encoded. Teknik ATT&CK mana yang cocok?
Defense Evasion – Obfuscated Files or Information
Tim SOC menemukan alert file integrity pada file web aplikasi yang jarang diubah, muncul mendadak di jam malam. Tidak ada deployment tercatat. Apa langkah investigasi paling tepat?
Analisis hash file baru dan korelasikan dengan log akses
Seorang admin mencatat log jaringan menunjukkan transfer data sangat besar ke server asing di luar jam kerja. Analisis apa yang perlu diprioritaskan?
Menganalisis PCAP untuk memeriksa isi transfer dan proses yang terlibat
Seorang peneliti keamanan mendapati checksum file sistem operasi berubah tanpa adanya pembaruan resmi. Mengapa deteksi perubahan ini penting, dan apa konsekuensinya jika diabaikan?
Menunjukkan potensi modifikasi berbahaya, dan bisa menjadi pintu masuk backdoor
Seorang analis SOC menemukan pola login berhasil dari IP luar negeri setelah terjadi beberapa kali login gagal dalam waktu sangat singkat. Log mana yang paling relevan untuk dianalisis lebih lanjut, dan tindakan mitigasi apa yang sebaiknya diambil?
Menganalisis log autentikasi, lalu memaksa reset kata sandi pengguna tersebut
Seorang analis SOC menerima alert SIEM terkait login dari luar negeri, tetapi setelah dikonfirmasi ternyata user sedang perjalanan dinas resmi. Situasi ini disebut:
False positive
Ketika Wazuh menerima log dari web server, muncul pattern scanning dengan user-agent yang aneh. Apa tindakan hunting yang tepat?
Mencatat IP asal dan melakukan analisis payload untuk rule tambahan
Dalam skenario SOC, serangan fileless malware sering luput dari signature-based detection. Mekanisme log apa yang harus dioptimalkan untuk mendeteksi jenis serangan ini?
Log eksekusi proses dan event command line
Seorang pentester menemukan form login tanpa rate limit. Apa resiko utama dari temuan tersebut?
Potensi brute force login sangat mudah dilakukan
Dalam pengujian file disclosure, peneliti berhasil melakukan permintaan ke file /etc/passwd dan mendapat respons 200 OK. Risiko utama dari temuan ini adalah:
Server tidak menolak akses file sensitif, membuka peluang enumerasi user
Anda mengintegrasikan VulnVM dengan Wazuh untuk memonitor kerentanan. Saat Wazuh agent diinstal pada VulnVM, hasil vulnerability assessment menunjukkan CVSS tinggi pada port yang jarang digunakan. Tindakan terbaik selanjutnya?
Validasi exposure port di firewall dan rencanakan patching
Seorang operator SOC menerima ratusan alert setiap hari, banyak di antaranya berlevel rendah dan tidak relevan. Strategi yang dapat digunakan untuk mengurangi alert fatigue adalah:
Menyempurnakan rule / aturan korelasi dan menambahkan prioritisasi berbasis risiko
Dalam pengetesan file disclosure, Anda mencoba permintaan ke file backup lama /backup/config.bak dan mendapatkan HTTP 302 Redirect ke halaman login. Apa yang dapat Anda simpulkan?
File mungkin ada tetapi dibatasi otorisasi
Dalam proses threat hunting, bagaimana membantu menurunkan false positive dari alert yang sering muncul?
Membuat hipotesis berbasis TTP attacker dan menyempurnakan rule korelasi
Apa alasan vulnerability scanner harus dijalankan secara berkala meskipun ada SIEM?
Kerentanan baru muncul terus, SIEM sendiri tidak menguji sistem
Ketika menggunakan Wazuh untuk mendeteksi perubahan mendadak pada file konfigurasi sistem, apa langkah paling tepat sebelum melakukan remediasi?
Memeriksa rule FIM dan melakukan verifikasi apakah perubahan memang sah
Apa risiko jika laporan pentest tidak memuat rekomendasi mitigasi yang jelas?
Temuan tidak diatasi dan potensi serangan tetap terbuka
Dalam konteks web pentest, mengapa kelemahan IDOR berbahaya? **Membiarkan attacker mengakses atau memodifikasi objek lain tanpa otorisasi**