MATERI L1 SOC ANALYST

UNIT KOMPETENSI 1

Melakukan Deteksi Kerentanan Aset Teknologi Informasi

MEDIA PEMBELAJARAN L1 SOC ANALYST

Unit Kompetensi

Melakukan Deteksi Kerentanan Aset Teknologi Informasi (TI)

Hasil Pembelajaran

Setelah mengikuti pembelajaran peserta didik diharapkan mampu mendeteksi kerentanan pada aset TI

Indikator Hasil Belajar

- Mengidentifikasi ruang lingkup deteksi kerentanan aset TI
- Mengidentifikasi kerentanan pada aset TI

Elemen Kompetensi

1. Mengidentifikasi ruang lingkup deteksi kerentanan TI
    a. Aset TI yang akan dideteksi kerentanannya diidentifikasi berdasarkan dokumen kesepakatan
    b. Ruang lingkup deteksi kerentanan diidentifikasi berdasarkan dokumen kesepakatan
    c. Jadwal dan lokasi pelaksanaan dikoordinasikan kepada pihak terkait sesuai dokumen kesepakatan
2. Mengidentifikasi kerentanan pada aset TI
    a. Deteksi kerentanan aset TI dilaksanakan sesuai dengan tahapan *vulnerability assessment*
    b. Rekomendasi mitigasi disusun sesuai dengan laporan hasil *vulnerability assessment*

A. Security Operation Center

Apa itu *Security Operation Center?*

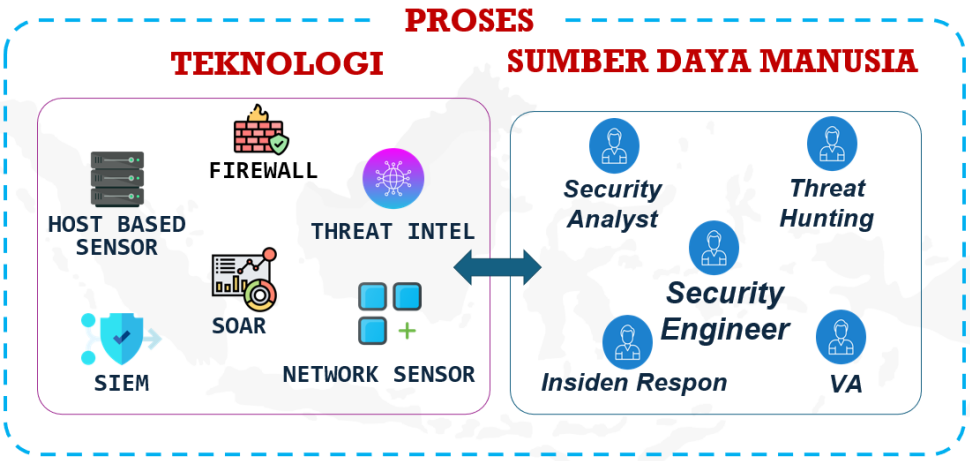
Security Operation Center (SOC) adalah sebuah bagian dari organisasi yang terdiri dari personel dan sistem sebagai pusat kegiatan pengamanan untuk meningkatkan postur keamanan organisasi. Dalam operasinya, SOC memiliki tugas untuk "memantau, mencegah, merespons, dan melaporkan" setiap aktivitas yang berhubungan dengan keamanan

Latar Belakang Pembentukan *Security Operation Center*

1. Mendeteksi aktivitas mencurigakan sebelum terjadinya insiden yang menyebabkan dampak yang lebih besar
2. Meminimalisir dampak kerugian finansial akibat insiden atau penyalahgunaan sistem elektronik
3. Meningkatkan efisiensi karena terdapat Tim khusus yang melakukan monitoring sistem elektronik sehingga Tim lainnya dapat fokus pada tugas fungsinya.
4. Prioritas insiden yang harus mendapatkan perhatian dan penanganan segera
5. Kepatuhan terhadap standard atau regulasi yang ditetapkan oleh regulator sektor
    - Peraturan Presiden (PP) Nomor 82 Tahun 2022 Tentang Pelindungan Infrastruktur Informasi Vital
    - Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
    - Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
    - PCI DSS Compliance, ISO 27001:2022
    - HIPAA, GDPR

Operasional dalam SOC

Untuk dapat beroperasi SOC terdiri dari 3 Komponen utama yaitu tata kelola, sumber daya manusia dan teknologi



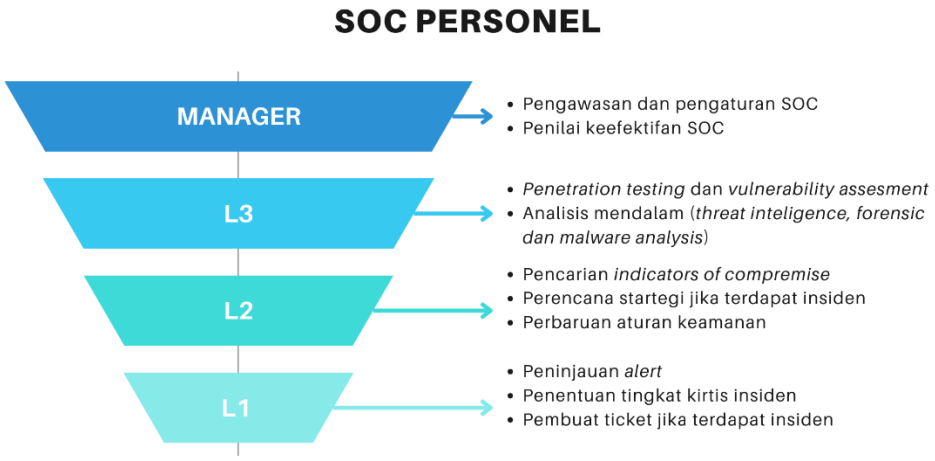
Operasional dalam SOC: Sumber Daya Manusia

Idealnya didalam SOC terdapat sumber daya manusia yang dibagi menjadi beberapa peran dengan kompetensi maupun sertifikasi yang harus dimiliki. Berikut peran SDM yang berhubungan dengan operasional SOC.

Tim	Sertifikasi
Service Desk/Call Center	SANS SEC401
L1 SOC Analyst	SANS SEC401, SEC 503, SEC 511, Regex
L2 SOC Analyst	SANS SEC401, SEC 503, SEC 511, FOR508, CISSP, Regex
L3 SOC Analyst	SANS SEC401, SEC 503, SEC 511, FOR508, SANS 610, CISSP, SANS 660
Vulnerability Assessor	SEC504, CEH, ECSA, OSCP, SEC560, SEC462, SEC460
Incident Response Team	FOR500, FOR526, SANS 610, FOR 508, Product Cert, FOR572
Malware Analyst Team	FOR500, FOR526, SANS 610
SOC Tool Support Team	SIEM Engineer, Network Engineer, Security Device Engineer, SEC555
Penetration Testing Team	OSCP, OSCE, OSEE, SANS 504, SEC462, SEC560, SEC575, OSWP, LPT Master, ECSA
Cyber Threat Intelligence Team	FOR578, CTIA
Forensic Investigators	FOR500, FOR526, SANS 610, FOR 508, FOR572, Product Cert, Investigation Theory, FOR 518
Analytic & Rule Team	SEC555, SNORT, Yara, Regex
Big Data Engineer Team	SAS Data Scientist, Certified Analytics Professional
Big Data Scientist Team	SAS Data Scientist, Certified Analytics Professional
Network Support Team	CCNA, CCNP, Network Specific Product Cert

Facilities Maintenance	CDCP, CCNA+B13B12B14:C1B13:C17

Operasional dalam SOC: SOC Analyst



1. *Tier 1 (Triage Specialist)*

   Merupakan personel yang mengawasi SOC terus menerus dan dapat dikatakan sebagai garis pertahanan pertama. Untuk menunjang tugas utama tersebut *Tier 1 SOC analyst* juga bertanggung jawab dalam meninjau peringatan keamanan yang ada. Peninjauan peringatan keamanan meliputi tingkat kekritisan insiden serta mengkonfirmasi apakah peringatan yang muncul merupakan *false positive*. Selain itu *Tier 1 SOC Analyst* harus mengetahui kekritisan insiden dan efek yang ditimbulkan agar mampu memprioritaskan penanganan insiden sesuai dengan tingkat kekritisan. *Tier 1 SOC Analyst* juga bertugas membuat *ticket* agar insiden juga dapat ditindak lanjuti personel pada *tier* berikutnya.
2. *Tier 2 (Incident Responder)*

   Tugas utamanya yaitu menindak lanjuti insiden yang dilaporkan oleh *Tier 1 SOC Analyst*. Oleh *Tier 2 SOC Analyst*, insiden akan dilakukan penilaian yang lebih mendalam seperti *indicators of compremise* (IOC), aset yang terdampak insiden serta memperbaharui aturan kemanan. *Tier 2 SOC Analyst* juga bertanggung jawab dalam merencanakan dan mengimplemantasikan strategi dalam menghadapi insiden, oleh karena itu *Tier 2 SOC Analyst* wajib memahami ruang lingkup insiden dan sistem yang terimbas. Jika *Tier 2 SOC Analyst* tidak mampu menangani insiden maka insiden akan diserahkan ke *tier* berikutnya
3. *Tier 3 (Threat Hunter)*

   Menangani insiden besar yang tidak mampu ditangani *tier* sebelumnya. Sebagai pembeda utama dari *tier-tier* sebelumnya adalah mencari kerentanan dan ancaman secara aktif sebelum terjadi inisiden.. *Tier 3 SOC Analyst* harus mampu melakukan *vulnerability assesment* dan *penetration testing* untuk melaksanakan tugas tersebut. Selain itu kemampuan *threat inteligence, forensic dan malware analysis* juga diperlukan untuk menindak

lanjuti insiden dengan tingkat kesulitan tinggi. *Tier 3 SOC Analyst* juga merekomendasikan penggunaan *tools monitoring* yang efektif untuk meningkatkan kinerja didalam SOC

4. *SOC Manager*

   Bertugas melakukan pengawasan dan pengaturan SOC. Pengaturan personel meliputi perekrutan, pelatihan, evaluasi personel. Untuk menilai keefektifan SOC yang dipimpin, SOC manager juga melakukan asesmen. SOC manajer juga bertanggung jawab atas keuangan dan penentuan *shift* personel. SOC manager langsung bertanggung jawab kepada *Chief Information Security Offcer* (CISO)

Operasional dalam SOC: Teknologi

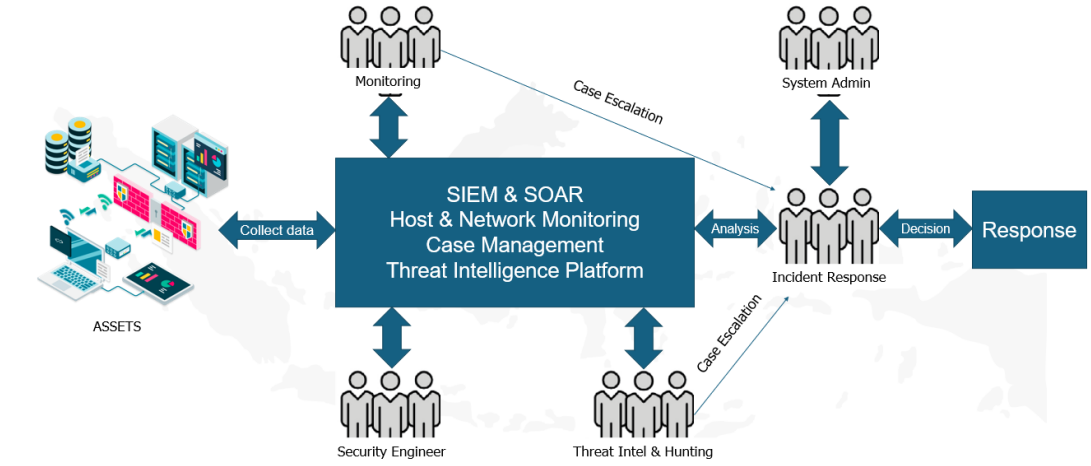
Berikut adalah daftar perangkat pencegahan ancaman keamanan siber yang membantu dalam operasional SOC

1. *Firewall*
   - Memantau lalu lintas masuk dan keluar jaringan untuk menghindari serangan dari jaringan yang tidak tepercaya.
   - Mengontrol akses berdasarkan aturan keamanan yang ditetapkan dan membatasi akses tidak sah.
   - Contoh perangkat: Cisco ASA Firewall, Fortinet FortiGate, Palo Alto Networks Next-Gen Firewall, pfSense (Open Source).
2. IDS dan IPS *(Intrusion Detection System & Intrusion Prevention System*)
   - Mendeteksi dan mencegah aktivitas mencurigakan atau tidak sah pada jaringan.
   - Contoh perangkat: Snort (Open Source IDS/IPS), Suricata (IDS/IPS berbasis open source), Cisco Firepower, Palo Alto Threat Prevention.
3. *Web Application Firewall* (WAF)
   - *Firewall* yang berfokus pada aplikasi web.
   - Melindungi situs web dari serangan seperti *SQL Injection, Cross-Site Scripting* (XSS), dan lainnya.
   - Contoh perangkat: Cloudflare WAF, AWS Web Application Firewall, Imperva WAF, ModSecurity (Open Source WAF).
4. *Hardware Security Modules* (HSM)
   - Perangkat keras untuk mengelola dan melindungi kunci kriptografi dan operasi enkripsi.
   - Menyediakan keamanan tambahan untuk mengamankan informasi sensitif.
   - Contoh Perangkat: Thales Luna HSM, Entrust nShield HSM, AWS CloudHSM, SafeNet HSM.
5. *Encryption Tools*
   - Mengamankan data dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa dekripsi yang sesuai.

- Contoh Perangkat: VeraCrypt (Disk Encryption - Open Source), BitLocker (Windows Disk Encryption), OpenSSL (Tool Enkripsi & SSL/TLS), GPG (GNU Privacy Guard - Open Source)

6. *Multi-Factor Authentication* (MFA)
   - Menggunakan lebih dari satu faktor autentikasi untuk masuk ke akun atau sistem.
   - Meningkatkan keamanan dengan menambahkan lapisan perlindungan tambahan.
   - Contoh: Google Authenticator, Microsoft Authenticator, Duo Security (Cisco MFA Solution), YubiKey (Hardware-based MFA)
7. *Antivirus/Antimalware*
   - Mendeteksi, mengidentifikasi, dan menghapus program berbahaya seperti virus, *malware, ransomware*, dan trojan sebelum merusak sistem.
   - Contoh: Windows Defender, Bitdefender Antivirus, Kaspersky Anti-Virus, Malwarebytes
8. VPN (*Virtual Private Network*)
   - Memungkinkan pengaksesan sumber daya jaringan dengan aman melalui koneksi terenkripsi.
   - Melindungi data saat dikirimkan melalui jaringan yang tidak aman, seperti internet publik.
   - Contoh: Cisco AnyConnect, OpenVPN (OpenSource VPN Solution), NordVPN Teams, WireGuard (Open Source & Fast VPN)
9. *Patch Management Tools*
   - Mengidentifikasi dan memperbarui perangkat lunak atau sistem operasi dengan patch terbaru untuk mengatasi kerentanan keamanan yang diketahui.
   - Contoh: WSUS (*Windows Server Update Services*), Qualys Patch Management, ManageEngine Patch Manager Plus, Ivanti Patch for Windows & Linux
10. EDR dan XDR (*Endpoint Detection and Response* & *Extended Detection and Response*)
    - EDR mendeteksi ancaman siber pada perangkat endpoint dan menyediakan fitur untuk mitigasi serta remidiasi.
    - XDR mengintegrasikan deteksi dan analisis pada jaringan, cloud, serta sumber daya lain dalam infrastruktur TI perusahaan.
    - Contoh: CrowdStrike Falcon (EDR/XDR), Microsoft Defender for Endpoint (EDR/XDR), SentinelOne (EDR/XDR), Palo Alto Cortex XDR

Operasional dalam SOC: Proses



Source: 11 Strategies of a World-Class Cybersecurity Operation Center

Proses dalam SOC dimulai dari pengumpulan data dari berbagai aset teknologi informasi seperti server, jaringan, *firewall*, dan *endpoint devices*. Data yang telah dikumpukan akan diolah dan dianalisi sistem SIEM & SOAR yang berfungsi untuk menonitor jaringan dan *hosts*, *case management* dan *threat intelligence platform*. SDM dalam SOC dikelompokan dalam berbagai peran diantaranya *security engineer, monitoring, threat intel & hunting, system admin* dan *incident response*. *Security engineer* bertanggung jawab untuk memastikan infrastruktur keamanan berfungsi dengan baik. Tim *Threat Intelligence & Hunting* menganalisis ancaman yang lebih kompleks dan mengeskalasikan kasus yang mencurigakan. *Monitoring* dilakukan secara terus-menerus untuk mendeteksi aktivitas anomali. Jika terdapat insiden, akan diteruskan ke Tim *Incident Response*. *Tim incident response* melakukan analisis lebih lanjut menentukan langkah respons yang akan diambil, baik berupa mitigasi, pemulihan sistem, atau tindakan lain untuk mencegah insiden selanjutnya. Tim *Incident Response* dapat meneruskan hasil analisis insiden ke *System Administrator* sebagai pengelola aset untuk melakukan mitigasi dan pemulihan sistem.

Operasional dalam SOC: Proses

Keputusan untuk mengoperasikan *Security Operations Center* (SOC) secara 24/7 bergantung pada berbagai faktor yang terkait dengan kebutuhan organisasi, ancaman keamanan, serta sumber daya yang tersedia. Faktor yang mempengaruhi apakah SOC harus beroprasi 24/7 dapat dilihat pada pertanyaan dibawah ini:

1. Apakah terdapat ancaman spesifik yang mungkin terjadi di luar jam kerja normal?
2. Apakah pengguna memiliki akses terhadap sumber daya IT di luar jam kerja?
3. Apakah organisasi bergantung pada IT selama 24/7?
4. Apakah terdapat tim SOC yang datang di luar jam kerja untuk menangani insiden?
5. Apakah terdapat *cost* untuk memenuhi kebutuhan staf 24x7?

6. Apakah terdapat sumber daya di luar SOC yang dapat memberikan respon di luar jam kerja?
7. Apakah ada toleransi terhadap keterlambatan dalam mengidentifikasi kejadian mencurigakan?
8. Apakah ada stigma organisasi yang terkait dengan tidak beroperasinya SOC sepanjang waktu?

Strategi Pembangunan SOC

1. Ketahui apa yang sedang lindungi dan alasannya
   Organisasi harus mengidentifikasi aset yang dimiliki serta memiliki tingkat prioritas dalam pengamanan dengan memperhitungkan nilai resiko. Bentuk aset yang perlu diidentifikasi dapat berupa infrastuktur jaringan, data pengguna, dan layanan aplikasi.
2. Berikan otoritas kepada SOC untuk menjalankan tugas
   Otoritas SOC dalam mendeteksi, menganalisis dan merespons ancaman dapat berupa akses terhadap data, koordinasi dengan bagian lain organisasi serta akses dalam pengambilan keputusan cepat ketika terjadi insiden.
3. Bangun struktur SOC sesuai dengan kebutuhan organisasi
   Setiap organisasi memiliki karakteristik yang berbeda dan dapat mempengaruhi aset yang dilindungi. Dalam membangun SOC, organisasi dapat mempertimbangkan regulasi yang ada, skala bisnis, pembiayaan, dan ancaman yang mungkin terjadi.
4. Rekrut dan kembangkan staf berkualitas
5. Prioritaskan respons terhadap insiden
   SOC harus memiliki prosedur yang terstruktur dan efisien untuk menilai keparahan insiden agar dapat memprioritaskan insiden dengan tingkat kerugian paling besar.
6. Kenali ancaman dengan *Threat Intelligence*
   Threat Intelligence dapat dimanfaatkan SOC dalam mengenali pola serangan maupun IoC sehingga mampu mencegah serangan sebelum terjadi.
7. Pilih dan kumpulkan data yang tepat
8. Manfaatkan alat yang tepat untuk mendukung kinerja analis
9. Komunikasikan dengan jelas, kolaborasi , dan berbagi informasi dengan baik
   SOC akan sering berhubungan dengan bagian lain dalam organisasi ketika terjadi insiden seperti kepada tim infrastruktur, tim tanggap insiden siber dan pimpinan organisasi. Kecepatan dan ketepatan komunikasi menjadi kunci dalam memastikan insiden ditangani dengan cepat dan tepat.
10. Ukur kinerja untuk meningkatkan performa

Efektifitas SOC dapat diukur dengan mengukur waktu SOC dapat mendeteksi suatu insiden (MTTD) dan waktu yang diperlukan SOC untuk merespons insiden (MTTR)

11. Perluas fungsi SOC untuk meningkatkan efektivitasnya

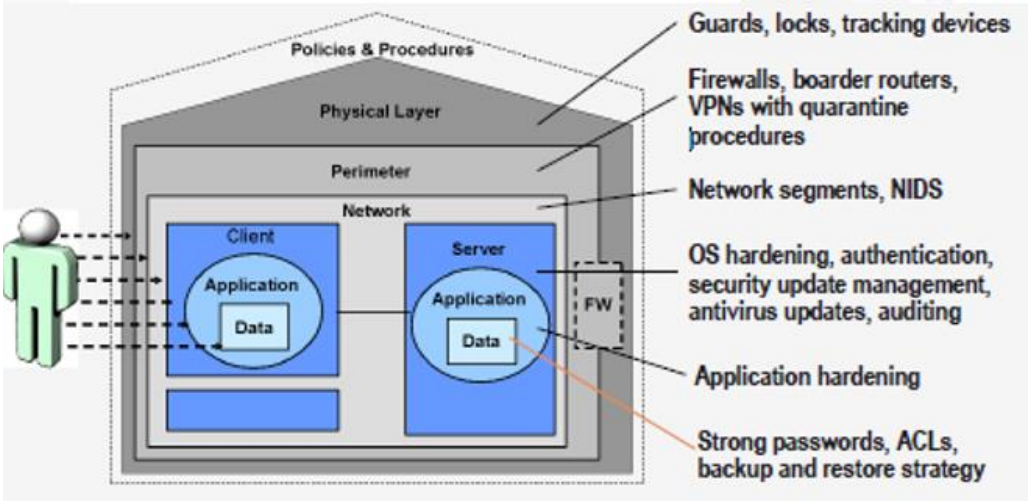
Faktor Keberhasilan SOC

1. Memahami proses bisnis yang menjadi ruang lingkup *monitoring*
2. Komunikasi & memahami ekspektasi *Top Level Management* dengan adanya SOC
3. Memahami proses rinci mengenai tanggap insiden
4. Memahami aset yang dimonitoring dan tingkat kritikalitas aset

B. Security Assessment

Konsep Defense-In-Depth

Konsep keamanan informasi yang menggunakan beberapa lapisan kontrol keamanan yang ditempatkan di seluruh sistem teknologi informasi (TI).



Apa itu Security Assessment

Security Assessment adalah proses menilai secara menyeluruh keamanan suatu sistem atau organisasi untuk mengidentifikasi risiko, kerentanan, dan celah yang dapat dieksploitasi oleh penyerang siber

Latar Belakang Pembentukan Security Operation Center

6. Mendeteksi kelemahan dalam sistem
7. Mengevaluasi tingkat keparahan kelemahan pada sistem
8. Merekomendasikan perbaikan dan tindakan pencegahan
9. Prioritas insiden yang harus mendapatkan perhatian dan penanganan segera

Mengapa Perlu Security Assessment?

Security Assessment diperlukan untuk menjawab pertanyaan ”Apakah sistem kita aman?”, menyediakan *baseline* keamanan sistem, menemukan konfigurasi yang salah ataupun pembaruan keamanan yang terlewat, mengetahui kelemahan yang tidak teridentifikasi, memastikan kepatuhan seluruh pegawai terhadap *security policy* dan kepatuhan organisasi terhadap regulasi dan perundangan-undangan.

Berikut contoh sertifikat *security assessment*

Perencanaan Security Assessment

Fase Assessment	Elemen yang Harus Direncanakan
Sebelum-*assessment*	• Ruang Lingkup • *Goals* • Waktu/Jadwal • Aturan Dasar
Saat *Assessment*	• Pemilihan Teknologi • Melakukan *Assessment* • Pengelompokan Hasil
Penyiapan Hasil *Assessment*	• Menghitung estimasi risiko dari kelemahan yang didapatkan • Membuat rencana remediasi/perbaikan • Mengidentifikasi kerentanan baru yang belum di terapkan kontrolnya • Menentukan rencana perbaikan/*update* di keseluruhan sistem secara berkala
Melaporkan Temuan	• Menyusun laporan hasil akhir *asssessment*

	• Mengungkapkan hasil temuan • Menentukan jadwal *assessment* selanjutnya

Alur Kerja Tim ITSA

Pra Pelaksanaan	*Stakeholder* mengirimkan surat permohonan ITSA -> *Stakeholder* mengisi dokumen koordinasi -> Kesepakatan dan Penandatanganan NDA -> Pemberian surat perintah kepada Tim ITSA
Pelaksanaan	Pemberian surat perintah kepada Tim ITSA -> *Kick-off meeting* -> ITSA **(Diskusi Tim -> Proses *Research* Tim -> Proses Analisis dan *Assessment* -> *Meeting* Progres pengerjaan ITSA)** -> Paparan Hasil ITSA
Pasca Pelaksanaan	Paparan Hasil ITSA -> Penyerahan Laporan Hasil ITSA -> *Stakeholder* melakukan perbaikan -> Tim ITSA melakukan verifikasi hasil perbaikan -> Penyerahan laporan verifikasi perbaikan -> ITSA Selesai

Tipe Security Assessment

Terdapat 3 tipe *security assessment,* yaitu

Tipe	Penjelasan
Vulnerability Assessment	• Proses untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan prioritas tingkat kerentanan keamanan pada ekosistem TI berdasarkan risiko • Fokus pada kerentanan yang telah diketahui • Dilakukan menggunakan *tools* otomatis • Tidak memerlukan kemampuan *expertise* yang tinggi
Penetration Testing	• Simulasi serangan siber pada sistem komputer atau jaringan untuk memvalidasi apakah kerentanan dapat dieksploitasi dan

	mendapatkan akses tidak sah ke data atau sistem • Fokus kepada kerentanan, baik yang diketahui maupun belum diketahui • Membutuhkan kemampuan *expertise* yang tinggi • Memerlukan aspek legal secara hukum untuk menghindari hal-hal yang tidak diinginkan
IT Security Auditing	• Proses evaluasi dan penilaian sistematis terhadap keamanan sistem informasi, untuk mengidentifikasi potensi kerentanan, kelemahan, dan ketidaksesuaian terhadap standar keamanan yang ditetapkan • Fokus kepada kepatuhan *policy* dan prosedur • Digunakan sebagai bukti/*evidence* untuk regulator

C. Vulnerability

RFC 4949 INTERNET SECURITY GLOSSARY

Kelemahan dalam desain, implementasi, operasi dan manajemen sistem yang dapat dimanfaatkan dan dieksploitasi penyerang untuk melanggar kebijakan keamanan sistem dan mengganggu operasi.

Tipe:

1. Weakness:
   Kelemahan dalam desain atau spesifikasi yang dapat dieksploitasi dan berdampak pada kerusakan data
2. Vulnerability:
   Kelemahan spesifik yang tereksploitasi dalam implementasi, dapat berupa cacat pada konfigurasi yang berdampak pada penolakan layanan
3. Backdoor:
   Kerentanan yang dibuat dengan sengaja dalam operasi dan manajemen, yang dapat berdampak pada eskalasi hak istimewa

ISO 27002 (*Information security, cybersecurity and privacy protection — Information security controls*)

Management of technical vulnerability

1. *Control*
   Informasi tentang kerentanan teknis sistem informasi yang digunakan harus diperoleh, paparan organisasi terhadap kerentanan tersebut harus dievaluasi dan tindakan yang tepat harus diambil
2. Tujuan
   Mencegah eksploitasi kerentanan

3. Tahapan
   Melakukan identifikasi kerentanan
4. Melakukan evaluasi kerentanan
   Mengambil tindakan yang tepat untuk mengatasi kerentanan

D. Dokumen Kesepakatan

Dokumen kesepakatan adalah dokumen tertulis yang memuat perjanjian antara dua pihak atau lebih untuk:

1. Menyatakan persetujuan bersama
2. Menjelaskan hak dan kewajiban
3. Membuat kerangka kerja

Jenis Dokumen Kesepakatan:

1. *Surat Perjanjian* (SP)
   Surat perjanjian atau SP adalah dokumen hukum yang mengikat dua pihak atau lebih dalam suatu kesepakatan tertentu. SP biasanya mencamtumkan hak, kewajiban, dan konsekuensi hukum jika salah satu melanggar kesepakatan. Dalam *Security Assessment*, SP bisa digunakan untuk perusahaan yang ingin bekerja sama dengan pihak ketiga untuk melakukan evaluasi keamanan sistem. SP akan mencakup ruang lingkup kerja, metode pengujian keamanan, serta tanggung jawab masing-masing pihak.
2. *Memorandum of Understanding* (MoU)
   MoU adalah dokumen yang menjelaskan kesepahaman antara dua pihak sebelum perjanjian resmi dibuat. MoU bersifat tidak mengikat secara hukum, tetapi dapat menjadi dasar untuk perjanjian lebih lanjut. Dalam *Security Assessment*, MoU bisa digunakan ketika dua organisasi ingin berkolaborasi dalam audit keamanan tanpa langsung masuk ke kontrak formal. Misalnya, sebuah perusahaan bisa menandatangani MoU dengan penyedia layanan keamanan sebelum menentukan cakupan detail dan tanggung jawab dalam perjanjian lebih lanjut.
3. *Non-Disclosure Agreement* (NDA)
   NDA adalah perjanjian yang mengatur kerahasiaan informasi antara dua pihak. Pihak yang menerima informasi tidak boleh membocorkan atau menggunakan informasi tersebut untuk kepentingan pribadi atau pihak lain. NDA sangat penting dalam penilaian keamanan, auditor atau penilai keamanan akan memiliki akses ke informasi sensitif perusahaan, seperti arsitektur sistem, data pengguna, atau kelemahan keamanan. NDA memastikan bahwa informasi tersebut tetap rahasia dan tidak disalahgunakan.
4. *Service Level Agreement* (SLA)
   SLA adalah perjanjian yang mendefinisikan tingkat layanan yang harus dipenuhi oleh penyedia layanan kepada pelanggan, termasuk standar

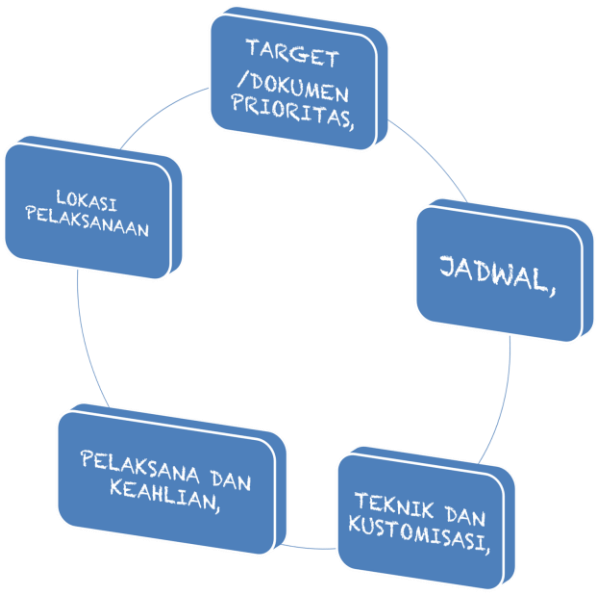
performa, keandalan, dan konsekuensi jika layanan tidak terpenuhi. SLA bisa digunakan antara perusahaan dan penyedia layanan keamanan untuk memastikan bahwa layanan keamanan yang diberikan memenuhi standar tertentu. SLA bisa mencakup:

- Waktu respons terhadap insiden keamanan
- Tingkat keberhasilan dalam mendeteksi ancaman
- Jaminan pemulihan setelah serangan siber

Kriteria Dokumen Kesepakatan:

1. Jelas dan mudah dipahami
2. Lengkap, mencakup hak dan kewajiban, jangka waktu, dan mekanisme penyelesaian
3. Tertulis dan ditandatangani

Kandungan Dokumen Kesepakatan:

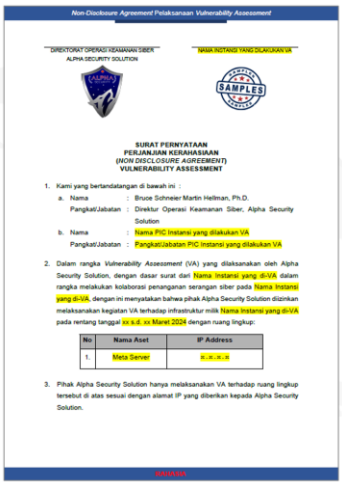


4. Target/Dokumen Prioritas
   Semakin banyak aset yang dilakukan VA, semakin banyak waktu yang diperlukan
5. Jadwal
   Dilaksanakan sesuai kesepakatan. Baiknya dilaksanakan ketika *low traffic.*
6. Teknik & Kustomisasi
   White Box, mendapatkan seluruh informasi mengenai sistem
   Grey Box, mendapatkan sebagian informasi mengenai sistem (IP, URL, Framework)
   Black Box, berperan sebagai pihak eksternal, peretas atau hacker, Tidak membutuhkan informasi apa pun
7. Pelaksana & Keahlian

Daftar nama pelaksana dan keahlian yang dimiliki pelaksana

8. Lokasi Pelaksanaan
   On site, Remote

Contoh Dokumen Kesepakatan


Non-Disclosure Agreement Pelaksanaan Vulnerability Assessment

DIREKTORAT OPERASI KEAMANAN SIBER
ALPHA SECURITY SOLUTION

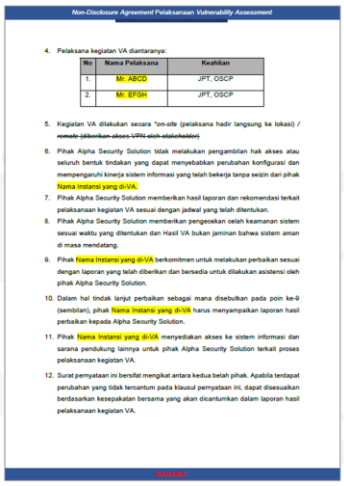
NAMA INSTANSI YANG DILAKUKAN VA

SURAT PERNYATAAN
PERJANJIAN KERAHASIAAN
(*NON DISCLOSURE AGREEMENT*)
VULNERABILITY ASSESSMENT

1. Kami yang bertandatangan di bawah ini :
   a. Nama : Bruce Schneier Martin Hellman, Ph.D.
      Pangkat/Jabatan : Direktur Operasi Keamanan Siber, Alpha Security Solution
   b. Nama : Nama PIC Instansi yang dilakukan VA
      Pangkat/Jabatan : Pangkat/Jabatan PIC Instansi yang dilakukan VA
2. Dalam rangka *Vulnerability Assessment* (VA) yang dilaksanakan oleh Alpha Security Solution, dengan dasar surat dari Nama Instansi yang di-VA dalam rangka melakukan kolaborasi penanganan serangan siber pada Nama Instansi yang di-VA, dengan ini menyatakan bahwa pihak Alpha Security Solution dizinkan melaksanakan kegiatan VA terhadap infrastruktur milik Nama Instansi yang di-VA pada rentang tanggal xx s.d. xx Maret 2024 dengan ruang lingkup:

No	Nama Aset	IP Address
1.	Meta Server	x..x..x..x

3. Pihak Alpha Security Solution hanya melaksanakan VA terhadap ruang lingkup tersebut di atas sesuai dengan alamat IP yang diberikan kepada Alpha Security Solution.


Non-Disclosure Agreement Pelaksanaan Vulnerability Assessment

4. Pelaksana kegiatan VA diantaranya:

No	Nama Pelaksana	Keahlian
1.	Mr. ABCD	JPT, OSCP
2.	Mr. EFGH	JPT, OSCP

5. Kegiatan VA dilakukan secara *on-site (pelaksana hadir langsung ke lokasi) / ~~remote (diberikan akses VPN oleh stakeholder)~~*
6. Pihak Alpha Security Solution tidak melakukan pengambilan hak akses atau seluruh bentuk tindakan yang dapat menyebabkan perubahan konfigurasi dan mempengaruhi kinerja sistem informasi yang telah bekerja tanpa seizin dari pihak Nama Instansi yang di-VA.
7. Pihak Alpha Security Solution memberikan hasil laporan dan rekomendasi terkait pelaksanaan kegiatan VA sesuai dengan jadwal yang telah ditentukan.
8. Pihak Alpha Security Solution memberikan pengecekan celah keamanan sistem sesuai waktu yang ditentukan dan Hasil VA bukan jaminan bahwa sistem aman di masa mendatang.
9. Pihak Nama Instansi yang di-VA berkomitmen untuk melakukan perbaikan sesuai dengan laporan yang telah diberikan dan bersedia untuk dilakukan asistensi oleh pihak Alpha Security Solution.
10. Dalam hal tindak lanjut perbaikan sebagai mana disebutkan pada poin ke-9 (sembilan), pihak Nama Instansi yang di-VA harus menyampaikan laporan hasil perbaikan kepada Alpha Security Solution.
11. Pihak Nama Instansi yang di-VA menyediakan akses ke sistem informasi dan sarana pendukung lainnya untuk pihak Alpha Security Solution terkait proses pelaksanaan kegiatan VA.
12. Surat pernyataan ini bersifat mengikat antara kedua belah pihak. Apabila terdapat perubahan yang tidak tercantum pada klausul pernyataan ini, dapat disesuaikan berdasarkan kesepakatan bersama yang akan dicantumkan dalam laporan hasil pelaksanaan kegiatan VA.


Non-Disclosure Agreement Pelaksanaan Vulnerability Assessment

13. Surat pernyataan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Depok, 28 Mei 2024

Direktur Operasi Keamanan Siber
Alpha Security Solution

Balai Sertifikasi Elektronik

Bruce Schneier Martin Hellman, Ph.D.

Kepala Divisi Teknologi Informasi
Nama Instansi yang di-VA

Balai Sertifikasi Elektronik

Nama PIC Instansi yang dilakukan VA

E. Vulnerability Assesment

Vulnerability Assessment merupakan bentuk penilaian risiko (*Risk Assessment*) yang ditinjau dari sisi kerentanan terhadap sistem atau infrastruktur.

1. *Vulnerability Assesment*
   Fokus kepada identifikasi kelemahan saat ini pada aset dan kontrol yang diterapkan, di mana penyerang bisa melakukan eksploitasi dan menyebabkan kerusakan
2. *Risk Assesment*
   Fokus kepada identifikasi ancaman potensial pada organisasi, dihadapkan dengan kerentanan, lalu memitigasinya

Tahapan VA:

1. *Reconnaissance*
   Tahapan awal untuk mengumpulkan data tentang target, seperti teknologi yang digunakan, jumlah perangkat terkoneksi, hingga arsitektur jaringan target.
   OSINT untuk mencari informasi mengenai target
   - Google Dorking
     inurl:gacor intext:gacor site:go.id
   - DNSDumpster
   - MXToolbox

- Shodan
- Whois

2. *Scanning*
   Proses pengumpulan informasi tambahan yang lebih detail mengenai target menggunakan teknik ***reconnaissance* aktif** untuk mendeteksi target aktif, *port*, dan *service* pada jaringan.
   NMAP untuk *scanning*:
   - Port
   - Service
     nmap -sV -O x.x.x.x
     nmap -F x.x.x.x

3. *Enumeration*
   Pencarian data yang lebih spesifik atau ketika sudah berhasil masuk pada *service* tententu, seperti mengidentifikasi *user* atau *resource* yang berelasi dengan sistem target.
   - Identifying and listing the users, networks, and resources
     nmap --script smb-enum-users.nse -p 445 x.x.x.x
     nmap --script vuln x.x.x.x
   - Dirbuster

4. *Vulnerability Analysis*
   Tahapan deteksi dan analisis terhadap kerentanan yang ditemukan, dilakukan berdasarkan pengalaman penguji atau menggunakan *VA tools* seperti Nessus, OWASP Zap, Acunetix, dll.
   - *Install* Nessus
   - *Scanning* to Metasploitable
   - *OWASP ZAP*

F. Rekomendasi Mitigasi

1. *Common Weakness Enumeration* (CWE)
   
   Sistem yang mengklasifikasikan berbagai jenis kelemahan yang ditemukan pada perangkat keras dan perangkat lunak, untuk membantu memahami, mengklasifikasi, dan menggambarkan jenis masalah keamanan yang mungkin muncul dalam sistem TI.

2. *Common Vulnerabilities and Exposures* (CVE)

Sistem standar internasional yang memberikan identifikasi untuk setiap kerentanan perangkat keras dan perangkat lunak yang ditemukan. Ini membantu dalam pelaporan, pelacakan, dan pertukaran informasi tentang kerentanan.

3. *National Vulnerability Database* (NVD)

Menyediakan database komprehensif tentang kerentanan keamanan siber, kerentanan perangkat lunak, dan informasi keamanan terkait lainnya, untuk membantu mengidentifikasi, memahami, dan mengatasi kerentanan dalam perangkat lunak dan perangkat keras

4. *Security Advisory* BSSN

Pemberitahuan resmi yang dikeluarkan BSSN untuk memberikan informasi tentang ancaman keamanan siber, kerentanan perangkat lunak, atau tindakan keamanan yang perlu diambil oleh organisasi atau individu untuk melindungi sistem dan data mereka dari potensi serangan.

G. Laporan Hasil VA

Contoh *outline* laporan hasil VA:

1. Tim ITSA BSSN
   a. Pendahuluan
      a) Dasar
      b) Maksud dan Tujuan
      c) Metodologi dan skenario
         Alur Kerja
         Acuan Kerentanan yang dinilai
      d) Teknik pengujian
         BlackBox
         Grey Box
      e) Penilaian risiko kerentanan

f) Syarat dan ketentuan
g) Kemungkinan Dampak

b. Hasil Kegiatan
a) Rekomendasi
b) Hasil temuan Kerentanan (PoC)

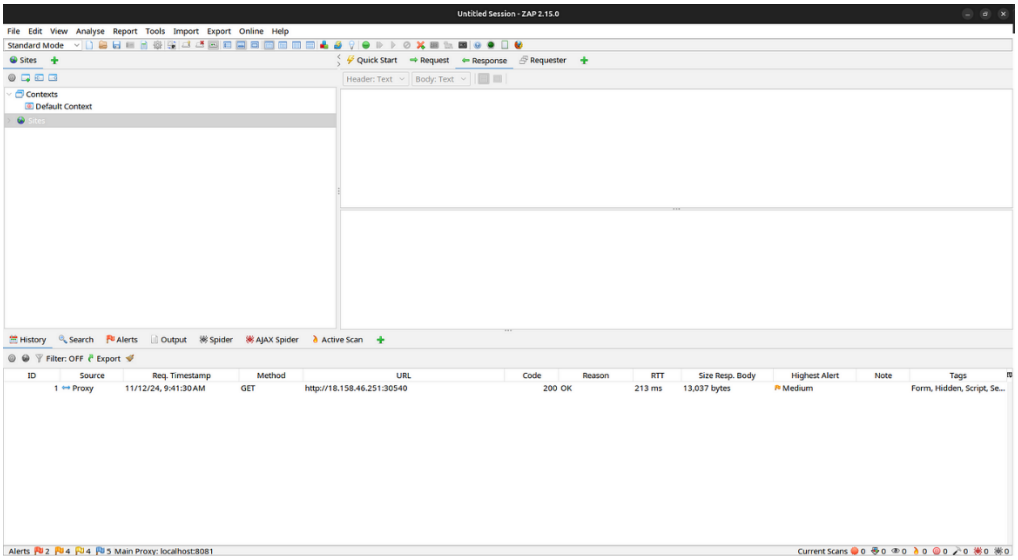
2. EC-Council / Purplesec
   a. *Executive Summary*
   b. *Scan Results*
   c. *Methodology*
   d. *Findings*
   e. *Risk Assessment*
   f. *Recommendations*

H. OWASP Zap

OWASP ZAP (Zed Attack Proxy) adalah alat sumber terbuka yang kuat yang dirancang untuk pengujian keamanan aplikasi web. Dibuat oleh Open Web Application Security Project (OWASP), ZAP membantu mengidentifikasi kerentanan umum, termasuk injeksi SQL, *cross-site scripting* (XSS), dan lainnya. Alat ini banyak digunakan oleh pengembang, profesional keamanan, dan penguji karena antarmuka yang ramah pengguna serta fitur yang lengkap, yang mencakup pemindai otomatis, pemindaian pasif, dan alat pengujian manual.

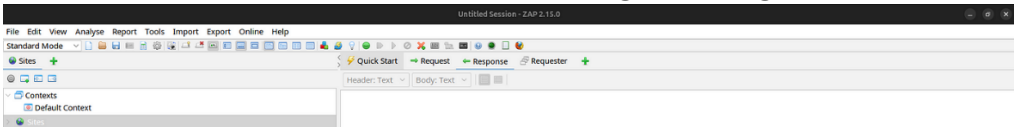
ZAP tersedia untuk berbagai sistem operasi seperti Windows, macOS, dan Linux. Langkah-langkah instalasi meliputi:

- Mengunduh versi yang sesuai dari halaman unduhan OWASP ZAP pada laman, https://www.zaproxy.org/download/
- Untuk Windows: jalankan *installer* dan ikuti petunjuk.
- Untuk macOS: ekstrak *file* yang diunduh dan pindahkan ke folder Aplikasi.
- Untuk Linux: ekstrak *file* dan jalankan *executable* ZAP.
- Setelah terinstal, pengguna perlu mengatur *proxy* browser ke localhost:8080 (*proxy default* ZAP) untuk merekam lalu lintas jaringan.

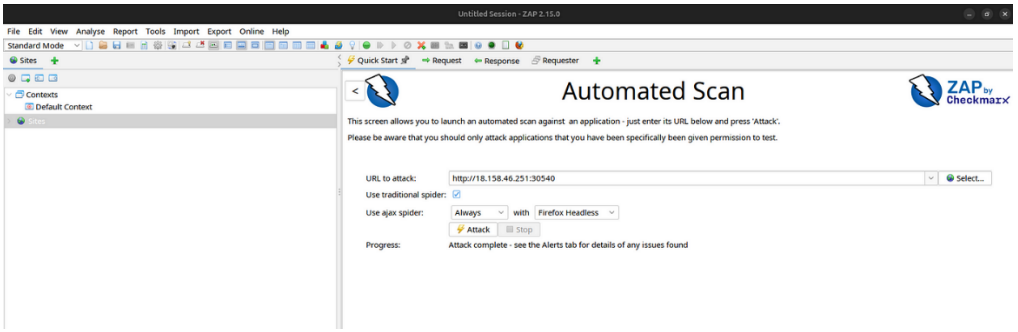


Pemindaian Otomatis Dasar:

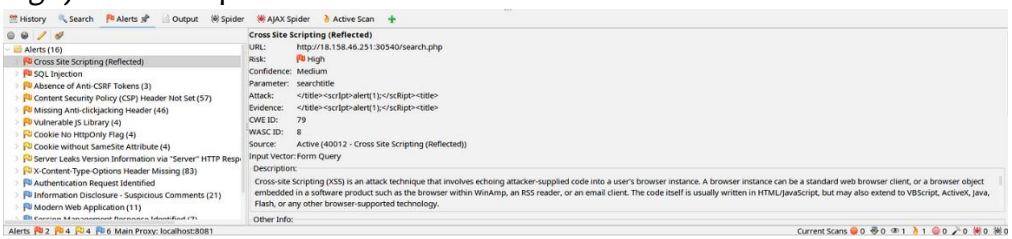
- Buka ZAP dan pastikan browser sudah dikonfigurasi dengan *proxy* ZAP.



- Di tab "*Quick Start*", masukkan URL aplikasi web yang ingin dipindai, lalu klik "*Attack*" untuk memulai pemindaian otomatis dasar.

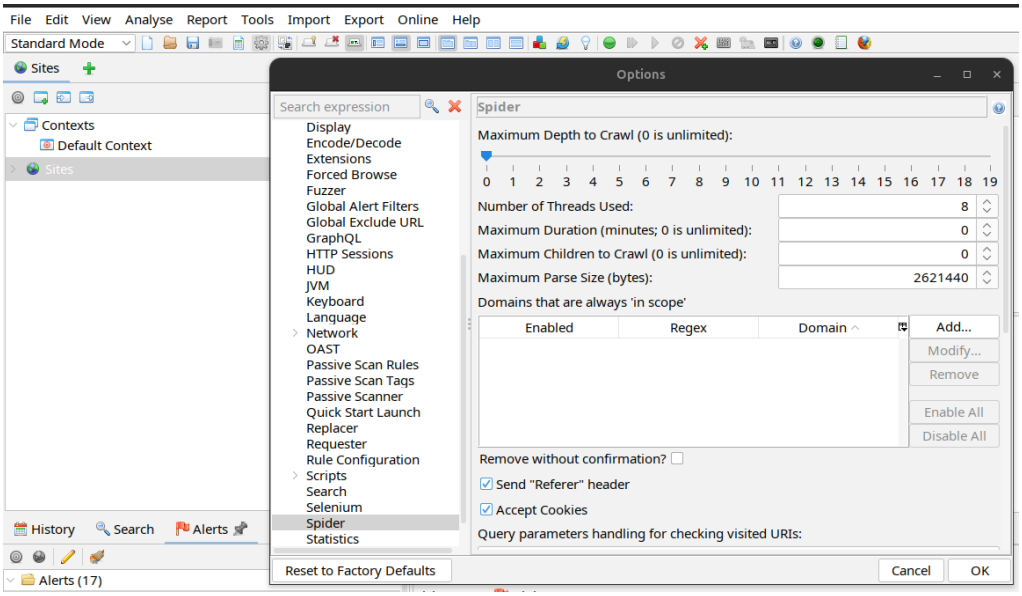


- ZAP akan melakukan *spidering* untuk menemukan halaman dan sumber daya, lalu memindai kerentanan umum seperti XSS dan injeksi SQL.
- Hasilnya ditampilkan di tab "*Alerts*" dengan tingkat risiko (*Low, Medium, High*) dan saran perbaikan.

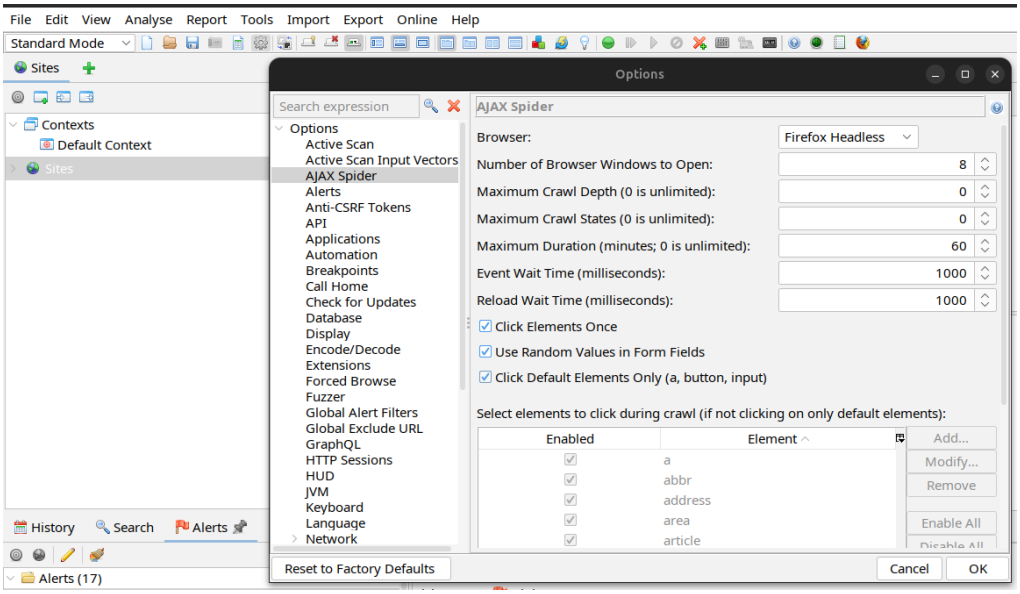


Untuk pemindaian yang lebih mendalam:

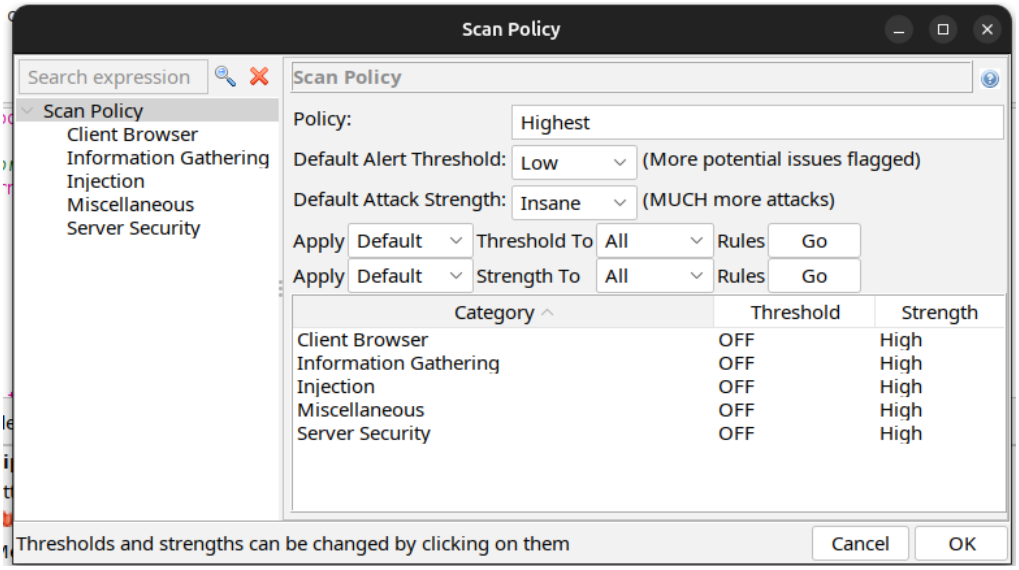
- Tingkatkan kedalaman perayapan: Di menu *Tools* > *Options* > *Spider*, atur "*Maximum Depth to Crawl*" ke nilai lebih tinggi (misalnya 5) untuk menjelajahi situs lebih dalam.



- Aktifkan AJAX *Spidering*: Untuk situs berbasis JavaScript atau aplikasi satu halaman (SPA), aktifkan AJAX *Spider* di *Tools* > *Options* > AJAX *Spider* agar ZAP dapat mendeteksi konten dinamis.



- Atur kebijakan pemindaian: Di *Analyze* > *Scan Policy Manager*, pilih atau buat kebijakan baru, lalu atur semua kategori (*Injection, Authentication*, dll.) ke tingkat "*High*" untuk cakupan maksimal.
- Jalankan pemindaian penuh dengan klik kanan pada situs di tab "*Sites*" dan pilih "*Attack*" > "*Active Scan*".



I. Nmap

Nmap adalah sebuah alat *open-source* yang digunakan untuk eksplorasi jaringan dan audit keamanan. Nmap berguna untuk menemukan *host* dan layanan di dalam jaringan komputer dengan mengirimkan paket-paket khusus dan menganalisis responsnya. Nmap banyak digunakan oleh administrator jaringan, peneliti keamanan, dan *ethical hacker* untuk mengidentifikasi perangkat yang aktif di jaringan, *port* terbuka, serta layanan yang berjalan.

- Melakukan *ping scan*
  Bertujuan untuk mengetahui perangkat yang aktif di dalam jaringan tanpa melakukan pemindaian *port*
  ' nmap -sn <ip/subnet> '
- Melakukan pemindaian *port* pada *host*
  ' nmap *<ip address>* ' atau jika ingin memindai *port* tertentu dapat menggunakan ' nmap -p 22,80,443 *<ip address>* '
- Melakukan pemindaian yang lebih mendalam
  Untuk mendapatkan informasi lebih detail mengenai layanan yang berjalan pada *port* terbuka bisa dilakukan dengan *command* ' nmap -sV *<ip address>* '
- Melakukan pemindaian OS
  ' nmap -O <ip address> '
- Melakukan pemindaian *stealth* (menghindari dari deteksi)
  Untuk menghindari deteksi oleh *firewall*, atau IDS bisa menggunakan SYN *Stealth* yaitu ' nmap -sS <ip address> '
- Menyimpan hasil *scan* ke *file*

' nmap -oN <nama file> *<ip address>* '

J. DirBuster

DirBuster adalah alat berbasis GUI yang digunakan untuk menemukan direktori dan file tersembunyi di dalam sebuah situs web melalui *brute-force*. DirBuster dikembangkan oleh OWASP dan sangat berguna bagi pentester untuk menemukan direktori yang tidak terindeks atau *file* yang sensitif di server web. Bekerja dengan mengirimkan sejumlah permintaan HTTP ke server target berdasarkan daftar kata (*wordlist*) yang telah ditentukan. Jika server merespons dengan kode status HTTP tertentu misalnya 200, maka berarti direktori atau *file* tersebut ada.

DirBuster bisa digunakan melalui CLI dengan *menginstal* dirb, dapat digunakan dengan
' dirb <nama domain> <direktori *wordlist*> '
Biasanya, setelah menjalankan hal tersebut kita mendapatkan hasil *scan* yang berupa
+ http://example.com/admin (CODE:200|SIZE:1234)
+ http://example.com/backup (CODE:403|SIZE:298)
+ http://example.com/index.html (CODE:200|SIZE:5120)