
50 Oefeningen Cyberbeveiliging (NL)

- | | | | |
|----|--|----|--|
| 01 | Fundamenten & Netwerkbeveiliging | 06 | Besturingssysteem- en Systeemhardening |
| 02 | Aanvalstechnieken & Social Engineering | 07 | Webapplicatiebeveiliging (OWASP Top 10) |
| 03 | Malware & Dreigingsanalyse | 08 | Penetratietesten en Ethisch Hacken |
| 04 | Cryptografie & Databeveiliging | 09 | Hoofdstuk 9: Incidentrespons en Monitoring |
| 05 | Identiteits- en Toegangsbeheer (IAM) | 10 | Hoofdstuk 10: Continuïteit, Cloud en Beveiligingscultuur |

Fundamenten & Netwerkbeveiliging

1 Oefening 1: CIA-triade in de praktijk

Scenario: Een webshop verwerkt creditcardbetalingen en toont productvoorraden. Bepaal voor klantgegevens, voorraadaantallen en de uptime van de betaalpagina welk element van de CIA-triade primair beschermd moet worden en formuleer per onderdeel één beheersmaatregel.

Toepassingsnotitie: Gebruik dit scenario om risicobeoordelingen uit te voeren op basis van vertrouwelijkheid, integriteit en beschikbaarheid bij online diensten.

2 Oefening 2: Poort- en protocolidentificatie

Tijdens een netwerkscan zie je poorten 21, 22, 80 en 443 openstaan. Benoem per poort het standaardprotocol. Geef aan welke twee protocollen ongecodeerde gegevens verzenden en welk beveiligd alternatief verplicht moet worden gesteld.

Toepassingsnotitie: Direct inzetbaar bij firewall-configuraties en het uitschakelen van verouderde, onveilige netwerkdiensten.

3 Oefening 3: Subnetting en netwerksegmentatie

Een organisatie gebruikt 192.168.1.0/24 voor alle apparaten. Deel dit netwerk logisch op in drie afzonderlijke VLAN's: Beheer, Medewerkers en Gasten. Beschrijf per VLAN het toegangsbeleid naar het interne databaseserver-segment.

Toepassingsnotitie: Toepassen om laterale bewegingen van aanvallers binnen een intern netwerk in te perken volgens het zero-trust principe.

4 Oefening 4: DNS-spoofing en verificatie

Een medewerker voert de URL van het bedrijfsportaal in, maar wordt omgeleid naar een frauduleuze pagina op een afwijkend server-IP-adres. Leg uit hoe DNS-cache poisoning dit veroorzaakt en beschrijf hoe de implementatie van DNSSEC via cryptografische validatie dit aanvalsscenario voorkomt.

Toepassen bij het beveiligen van bedrijfsresolvers en het valideren van DNS-records tegen omleidingsaanvallen.

5 Oefening 5: Firewall-regelanalyse

Inspecteer de regel: 'ALLOW ANY ANY ANY'. Leg uit waarom deze regel een auditfout oplevert. Herschrijf de regel volgens het principe van minimale privileges voor een webserver die uitsluitend HTTPS-verkeer van internet mag ontvangen.

Toepassingsnotitie: Essentiële controle bij het auditen en aanscherpen van perimeter- en ingress-firewallregels.

Aanvalstechnieken & Social Engineering

6 Oefening 6: Phishing e-mail header-inspectie

Een binnengekomen factuur-e-mail claimt van 'directie@bedrijf.nl' te zijn. De Received-SPF status is 'Fail' en DKIM ontbreekt. Bepaal of het bericht legitiem is en formuleer de DMARC-beleidsregel (reject/quarantine) die deze e-mail had moeten tegenhouden.

| Detecteren van spoofing en beveiligen van bedrijfsdomeinen tegen impersonatie.

7 Oefening 7: Brute-force en credential stuffing detectie

In de auth.log staan binnen 3 minuten 5.000 mislukte inlogpogingen voor account 'admin' vanaf 50 verschillende IP-adressen. Analyseer of dit een gerichte brute-force of credential stuffing aanval betreft en noem twee verdedigingsmaatregelen op applicatieniveau.

| Logboekanalyse en implementatie van rate limiting en multi-factor authenticatie.

8 Oefening 8: Man-in-the-Middle (MitM) op openbare Wi-Fi

Een thuiswerker logt in op een openbaar hotelnetwerk zonder VPN. Beschrijf hoe een kwaadwillende met ARP-spoofing sessiecookies kan onderscheppen. Benoem twee methoden waarmee de medewerker de vertrouwelijkheid van het dataverkeer kan waarborgen.

| Veilig werken op afstand en afdwingen van encrypted tunnels via VPN/TLS.

9 Oefening 9: Social engineering via pretexting

Iemand belt de servicedesk: 'Ik ben directeur Jansen, mijn laptop is gecrasht, reset direct mijn wachtwoord naar Welkom2024!'. Identificeer de beïnvloedingstechnieken en formuleer het verificatieprotocol dat de servicedeskmedewerker verplicht moet volgen.

| Inrichten van weerbare helpdeskprocedures tegen identiteitsfraude en manipulatie.

10 Oefening 10: DDoS-mitigatie en verkeersanalyse

De serverbelasting stijgt plotseling naar 100% door miljoenen SYN-pakketten zonder ACK van willekeurige bronadressen. Benoem dit type aanval en leg uit hoe SYN-cookies en een cloud-scrubbing center de dienstverlening kunnen herstellen.

| Bescherming van webinfrastructuur tegen netwerkuitputting en denial-of-service.

Malware & Dreigingsanalyse

11 Oefening 11: Ransomware-infectieketen in kaart brengen

Zet de volgende stappen in chronologische volgorde: data-exfiltratie, phishing-mail geopend, uitschakelen schaduwkopieën, versleuteling van bestanden, laterale beweging via SMB. Bepaal bij welke stap een offline back-up de reddende maatregel is.

| Inzicht krijgen in ransomware-playbooks en het belang van geïsoleerde back-ups.

12 Oefening 12: Trojaanse paarden versus virussen en wormen

Drie systemen zijn besmet: Systeem A downloadde een illegale rekenmachine-app; Systeem B werd besmet doordat malware zelfstandig over het LAN sprong; Systeem C raakte geïnfecteerd via een macro in een Word-bestand. Classificeer A, B en C als worm, Trojaans paard of virus.

| Accurate triage en malwareclassificatie tijdens incident response.

13 Oefening 13: Statische versus dynamische bestandsanalyse

Je ontvangt een verdacht executable-bestand. Noem twee eigenschappen die je inspecteert tijdens statische analyse (zonder uitvoeren). Leg uit waarom dynamische analyse altijd in een geïsoleerde sandboxomgeving moet plaatsvinden.

| Veilig onderzoeken van verdachte bestanden binnen een SOC- of analistenomgeving.

14 Oefening 14: Indicatoren van compromittering (IoC)

Na een incident vind je een onbekende SHA256-hash, een uitgaande verbinding naar een verdacht IP in Rusland, en een gewijzigde registersleutel (Run-key). Benoem welke van deze items netwerk-IoC's zijn en welke host-IoC's, en leg uit hoe je ze deelt via MISP.

| Opstellen en distribueren van threat intelligence en detectie-regels.

15 Oefening 15: Command & Control (C2) communicatiedetectie

Een intern werkstation verstuurt exact elke 60 seconden een HTTP POST-verzoek van 128 bytes naar een onbekend extern domein. Verklaar het concept 'beaconing' en noem twee netwerkmonitoring-maatregelen om dergelijk C2-verkeer op te sporen.

| Detecteren van gecompromitteerde interne systemen die verbinding houden met aanvallers.

Cryptografie & Databeveiliging

16 Oefening 16: Symmetrische versus asymmetrische encryptie

Je moet 50 GB aan databases versleutelen voor archivering én een veilige sleuteluitwisseling doen over internet. Bepaal wanneer je AES gebruikt en wanneer RSA/ECC. Leg uit waarom asymmetrische cryptografie ongeschikt is voor bulkdata-encryptie.

| Selecteren van de juiste cryptografische algoritmen voor data-in-transit en data-at-rest.

17 Oefening 17: Hashing en wachtwoordbeveiliging

Een ontwikkelaar stelt voor wachtwoorden op te slaan als MD5(wachtwoord). Beargumenteer waarom dit onveilig is (collision attacks, rainbow tables). Herschrijf het voorstel met een modern alternatief (bijv. bcrypt of Argon2) en leg de werking van een 'salt' uit.

| Veilige opslag van authenticatiegegevens conform moderne normen.

18 Oefening 18: Digitale handtekeningen en integriteit

Persoon A stuurt een contract naar Persoon B. Beschrijf stapsgewijs hoe Persoon A het document ondertekent met een privésleutel en hoe Persoon B met de publieke sleutel verifieert dat de inhoud niet is gewijzigd (integriteit) en echt van A komt (authenticiteit).

| Inrichten en begrijpen van PKI-gebaseerde integriteitscontroles en contractondertekening.

19 Oefening 19: SSL/TLS-handshake en certificaatvalidatie

Een gebruiker bezoekt een interne applicatie en ziet: 'NET::ERR_CERT_AUTHORITY_INVALID'. Leg uit hoe de Public Key Infrastructure (PKI) en de certificeringsinstantie (CA) de vertrouwensketen opbouwen, en waarom deze fout optreedt bij self-signed certificaten.

| Probleemoplossing en beheer van TLS-verbindingen en interne CA-vertrouwenslijsten.

20 Oefening 20: Data in Rust versus Data in Beweging

Een laptop bevat gevoelige patiëntendossiers en synchroniseert deze dagelijks met een cloudopslag. Welke versleutelingstechnologie (bijv. BitLocker/LUKS) beschermt de data bij diefstal van het apparaat, en welk protocol beschermt de data tijdens de upload?

| Voldoen aan privacywetgeving (AVG) door adequate end-to-end encryptie.

Identiteits- en Toegangsbeheer (IAM)

21 Oefening 21: Multi-Factor Authenticatie (MFA) Typologie

Categoriseer de volgende verificatiemethoden in de juiste authenticatiefactoren: SMS-code, vingerafdrukscan, pincode en hardwarebeveiligingssleutel. Bepaal welke combinatie voldoet aan sterke MFA.

Inzicht verwerven in de drie pijlers van authenticatie om kwetsbaarheden zoals zwakke single-factor logins effectief te elimineren.

22 Oefening 22: Role-Based Access Control (RBAC) Ontwerp

Ontwerp een matrix voor een marketingmedewerker, systeembeheerder en financiële controller met de acties Lezen, Schrijven en Uitvoeren op drie bronsystemen volgens het least-privilege principe.

Beheerders leren granulaire toegangsrechten inrichten zonder onnodige privilegeverlening binnen bedrijfsnetwerken.

23 Oefening 23: Principle of Least Privilege Audit

Onderzoek een lijst met actieve domeinaccounts waarbij 15 van de 40 gebruikers lokale administratorrechten bezitten. Formuleer een saneringsvoorstel en beleidsregel om dit terug te dringen.

Vermindert het aanvalsoppervlak bij endpoint-compromittering door overtollige beheerdersrechten systematisch af te bouwen.

24 Oefening 24: Single Sign-On (SSO) en SAML-Flows

Breng de interactie in kaart tussen Gebruiker, Identity Provider (IdP) en Service Provider (SP) tijdens een SAML/OIDC-aanmeldpoging. Wijs aan waar tokenverificatie plaatsvindt.

Begrijpen hoe centrale identiteitsverificatie werkt en waar kwetsbaarheden in sessieafhandeling kunnen ontstaan.

25 Oefening 25: Wachtwoordbeleid en Credential Lifecycle

Vergelijk een traditioneel 90-dagen rotatiebeleid met 8 tekens tegen een beleid met 16+ tekens wachtwoordzinnen zonder verplichte rotatie conform NIST SP 800-63B.

Moderniseert wachtwoordbeveiliging door gebruiksvriendelijke, cryptografisch sterke authenticatiemethoden te stimuleren.

Besturingssysteem- en Systeemhardening

26 Oefening 26: Windows Endpoint Hardening en GPO

Definieer drie Group Policy Objects (GPO) om PowerShell execution policies te beperken, autorun uit te schakelen en SMBv1 te deactiveren op alle Windows-werkstations.

Minimaliseert misbruik van ingebouwde beheertools door aanvallers tijdens post-exploitation fasen.

27 Oefening 27: Linux Bestandsrechten en Permissiematrix

Analyseer bestandspermissie 4755 op een custom scriptbestand. Bepaal waarom het SUID-bit hier een risico vormt voor privilege-escalatie en corrigeer dit naar een veilige waarde.

Voorkomt ongeautoriseerde rechtenverhoging door foute bestandsrechten en risicovolle binaire configuraties op Linux-systemen.

28 Oefening 28: Patchbeheer en Vulnerability Prioritering

Rangschik drie kwetsbaarheden op prioriteit voor implementatie: CVSS 9.8 (intern archiefsysteem), CVSS 7.5 (publiek bereikbare webserver met actieve exploit) en CVSS 5.3 (lokaal werkstation).

Ontwikkelt risicogebaseerde besluitvorming voor patchmanagement in plaats van uitsluitend te sturen op CVSS-basisgetallen.

29 Oefening 29: Poorten en Onnodige Services Uitschakelen

Bekijk een lijst met actieve luisterende netwerkpoorten op een server (21, 22, 23, 80, 445). Bepaal welke verouderde protocollen onmiddellijk gestopt moeten worden en beargumenteer waarom.

Verkleint het aanvalsoppervlak door verouderde en onversleutelde netwerkdiensten structureel te ontmantelen.

30 Oefening 30: Host-Based Intrusion Detection (HIDS)

Beschrijf hoe een bestandsintegriteitsmonitor (FIM) wijzigingen in /etc/passwd of C:\Windows\System32\drivers\etc\hosts signaleert aan de hand van hashvergelijkingen.

Stelt beheerders in staat ongeautoriseerde configuratiewijzigingen of rootkit-installaties direct op te sporen.

Webapplicatiebeveiliging (OWASP Top 10)

31 Oefening 31: SQL-Injectie (SQLi) Detectie en Mitigatie

Bekijk een kwetsbare inlogquery met ongefilterde gebruikersinvoer. Schrijf de string om naar een geparametriseerde query (prepared statement) om SQLi te neutraliseren.

Essentieel voor ontwikkelaars en analisten om datalekken via ongefilterde database-invoer te voorkomen.

32 Oefening 32: Cross-Site Scripting (XSS) Typologie

Koppel drie scenario's aan het juiste type XSS: kwaadaardig script opgeslagen in forumcommentaren, script ingevoegd via zoekbalk-URL, en script uitgevoerd via client-side JavaScript DOM-manipulatie.

Inzicht bieden in sessiekaping en browser-manipulatie om passende contextuele output-encoding toe te passen.

33 Oefening 33: Cross-Site Request Forgery (CSRF) Preventie

Leg uit waarom het SameSite=Strict cookie-attribuut en unieke formuliertekens voorkomen dat een ongeautoriseerde geldtransactie namens een ingelogde gebruiker wordt verzonden.

Voorkomt dat aanvallers misbruik maken van actieve browsersessies voor ongeoorloofde transacties.

34 Oefening 34: Insecure Direct Object References (IDOR)

Een gebruiker wijzigt in de browser URL /factuur?id=1024 naar /factuur?id=1025 en ziet andermans factuur. Benoem het kwetsbaarheidstype en definieer de vereiste backend-toegangscontrole.

Leert hoe strikte validatie op serverniveau vereist is bij het opvragen van objecten via gebruikersinvoer.

35 Oefening 35: Beveiligingsheaders (CSP, HSTS) Configureren

Formuleer een Content Security Policy (CSP) header die het laden van scripts van externe, niet-vertrouwde domeinen blokkeert, en voeg een geldige HSTS-header toe voor HTTPS-afdwinging.

Biedt diepgaande verdediging op browserniveau tegen injectie-aanvallen en downgrading van verbindingen.

Penetratietesten en Ethisch Hacken

36 Oefening 36: Verkenningfase (OSINT) en Reikwijdte

Lijst drie legitieme openbare bronnen (zoals DNS WHOIS, openbare certificaattransparantielogs en Shodan) op om subdomeinen van een doelwitorganisatie passief in kaart te brengen.

| Begrijpen welke informatie publiek zichtbaar is voor aanvallers tijdens de initiële verkenningfase.

37 Oefening 37: Poortscantechnieken en Nmap-Flag Logica

Vergelijk een TCP SYN-scan (-sS) met een volledige TCP Connect-scan (-sT). Leg uit welke scan stiller is in standaard verbindingslogs en waarom dit zo is.

| Verbeter kennis over netwerktraffic-generatie en detectiemechanismen in intrusion detection systemen.

38 Oefening 38: Kwetsbaarheidsscanning versus Penetratietest

Benoem twee fundamentele verschillen tussen een geautomatiseerde kwetsbaarheidsscan (zoals OpenVAS/Nessus) en een handmatige penetratietest gericht op bedrijfslogica.

| Helpt organisaties en studenten de juiste diepgang en verwachtingen te bepalen voor beveiligingstests.

39 Oefening 39: Regels van Betrokkenheid (Rules of Engagement)

Definieer drie cruciale onderdelen van een Rules of Engagement (RoE) document, waaronder expliciete testperiode, afgebakend IP-bereik en escalatieprocedures bij ontdekte breaches.

| Waarborgt dat beveiligingstesten juridisch compliant, transparant en zonder operationele schade verlopen.

40 Oefening 40: Ethische Rapportage en Risicoclassificatie

Stel de inhoudsopgave en risicomatrix op voor een bevinding: beschrijf Kwetsbaarheid, Impact, Reproductiestappen en Concreet Hersteladvies voor het management en technisch team.

| Vertaalt technische zwakheden naar bruikbare herstelacties en heldere risico-inzichten voor belanghebbenden.

Hoofdstuk 9: Incidentrespons en Monitoring

41 Oefening 41: SIEM-Logaggregatie en Gebeurteniscorrelatie

Onderzoek hoe firewall-logs, Active Directory-authenticaties en endpoint-gebeurtenissen gecorreleerd worden tot een bruikbare beveiligingswaarschuwing. Bepaal welke regels afwijkend gedrag onderscheiden van operationele ruis.

Toepassing: Verlaag 'alert fatigue' door alleen gecorreleerde afwijkingen met hoge betrouwbaarheid prioritair door te zetten naar analisten.

42 Oefening 42: Incidentresponsfasen en Triage

Wijs vijf praktijkscenario's toe aan de juiste fase: Voorbereiding, Detectie & Analyse, Inperking, Uitroeiing, Herstel of Lessen. Definieer de eerste handeling bij het constateren van actieve exfiltratie.

Toepassing: Snelle triage voorkomt overhaaste acties die vluchtig forensisch bewijsmateriaal op getroffen hosts overschrijven.

43 Oefening 43: Netwerkisolatie en Inperkingsstrategieën

Vergelijk het direct afsluiten van een server met het plaatsen van de host in een geïsoleerd quarantaine-VLAN. Beoordeel wanneer actieve netwerkcommunicatie tijdelijk moet worden getolereerd voor onderzoek.

Toepassing: Kies isolatietechnieken die verdere laterale beweging blokkeren zonder direct het werkgeheugen van de getroffen host te wissen.

44 Oefening 44: Vluchtige Gegevens en Forensische Acquisitie

Rangschik systeemgeheugen (RAM), swap-bestanden, netwerkaansluitingen en vaste opslag op volgorde van vluchtigheid. Bepaal hoe een RAM-dump veilig wordt vastgelegd zonder actieve malware-artefacten te verstoren.

Toepassing: Borg forensische integriteit door vluchtige data veilig te stellen voordat systemen opnieuw worden opgestart.

45 Oefening 45: Post-Incident Evaluatie en Lessen (Lessons Learned)

Stel na een gesimuleerde ransomware-aanval een actiepuntenlijst op voor procesverbetering. Identificeer hiaten in responstijd, communicatielijnen en back-upintegriteit.

Toepassing: Veranker evaluatieresultaten direct in playbooks en detectieregels om herhaling van hetzelfde aanvalsvector type te voorkomen.

Hoofdstuk 10: Continuïteit, Cloud en Beveiligingscultuur

46 Oefening 46: Back-upstrategieën en de 3-2-1 Regel

Toets een back-upbeleid aan het 3-2-1 principe: 3 kopieën, 2 verschillende media, 1 externe/onveranderlijke (immutable) locatie. Analyseer hoe offline of write-once media beschermen tegen ransomware.

Toepassing: Voorkom dat back-ups tijdens een aanval simultaan worden versleuteld door immutability en air-gapping af te dwingen.

47 Oefening 47: Cloud Shared Responsibility Model

Categoriseer taken zoals OS-patching, netwerkconfiguratie, identiteitsbeheer en fysieke datacenterbeveiliging per servicemodel. Bepaal wie verantwoordelijk is voor data-encryptie in een SaaS-oplossing.

Toepassing: Elimineer blinde vlekken in cloudbeheer door contractuele en operationele verantwoordelijkheden eenduidig toe te wijzen.

48 Oefening 48: Schaduw-IT en Cloud Storage Permissies

Onderzoek de risico's van publiek toegankelijke object-opslag (zoals open S3-buckets of blob storage). Bepaal hoe beleid en Cloud Access Security Brokers (CASB) schaduw-IT inzichtelijk maken.

Toepassing: Blokkeer standaard publieke leestoegang op bucketniveau om datalekken door configuratiefouten te verhinderen.

49 Oefening 49: Ketenveiligheid en Derdepartijenrisico (Supply Chain)

Beoordeel de risico's van open-source dependencies en leverancierstoegang tot interne netwerken. Stel basiseisen op voor een Software Bill of Materials (SBOM) en periodieke vendor assessments.

Toepassing: Beperk ketenrisico's door continue controle op bekende kwetsbaarheden in externe componenten voorafgaand aan productie.

50 Oefening 50: Security Awareness en Veilige Cultuur

Ontwerp een heldere no-blame meldingsprocedure voor werknemers die per ongeluk op een verdachte koppeling hebben geklikt. Vergelijk de effectiviteit van interactieve simulaties met passieve jaarlijkse cursussen.

Toepassing: Stimuleer vroege melding van potentiële incidenten door medewerkers te belonen voor alertheid in plaats van te bestraffen.
