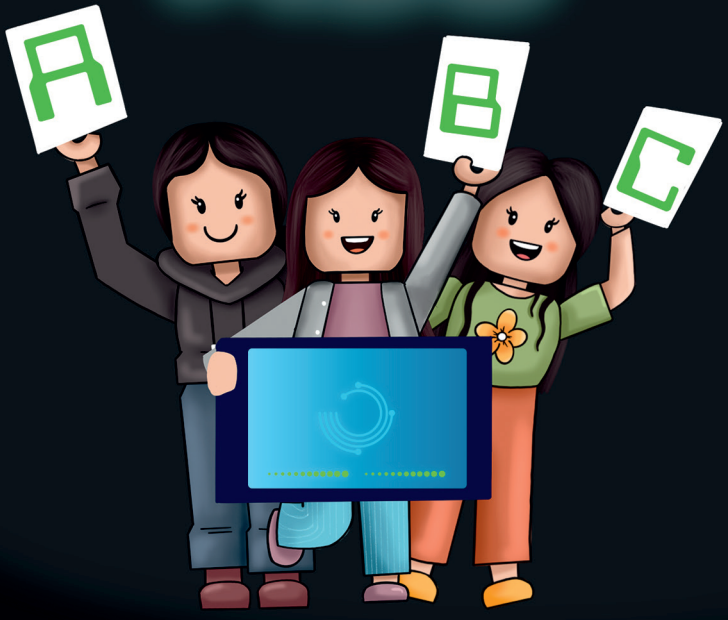
WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
ROMANIA

CyberDict FOR KIDS



Ilustrații
Alexandra Rotariu

Fraga Ţariuc

Alex Ricobon

CyberDict FOR KIDS

Ilustraţii

Alexandra Rotariu

Editura Intermedia Group

Târgu-Mureș

2025

Descrierea CIP a Bibliotecii Naţionale a României
ŢARIUC FRAGA, RICOBON ALEX
CyberDict for Kids / Fraga Ţariuc, Alex Ricobon ; il.: Alexandra Rotariu. - Târgu Mureş : Intermedia Group, 2025
ISBN 978-630-6771-02-8

I. Ţariuc Fraga, Ricobon Alex
II. Rotariu Alexandra (il.)

004
087.5

Bine ai venit în lumea fascinantă a securității cibernetice – sau cyber, cum îi spunem noi, că sună mai cool!

Acesta este **Dicționarul de Termeni Cyber**, creat special pentru copiii cu vârste între **8 și 14 ani**, care vor să descopere cum pot sa fie în siguranță online și să înțeleagă mai bine lumea digitală în care trăim.

Este un ghid prietenos, plin de explicații simple și exemple utile, unde vei învăța alături de trei prietene curajoase și super-smart: **CyberInes, ErinJoy** și **HackyFrancy**. Ele te vor însoți pe tot parcursul călătoriei și îți vor arăta cum să devii un adevărat Cyber-Expert, pas cu pas.

Acest dicționar a fost creat cu grijă de către **Asociația Women4Cyber România**, în colaborare cu **D3Cyber**, ca să aducem tehnologia mai aproape de copii – într-un mod interactiv, amuzant și ușor de înțeles.

Ce vei găsi în acest dicționar?

- Definiții clare și scurte, pe înțelesul tău
- Curiozități simpatice despre internet, tehnologie și siguranță online
- Sfaturi utile și provocări care te vor ajuta să fii mai atent, mai isteț și mai pregătit în lumea digitală
- O poveste în mai multe episoade, cu aventurile lui Ines, Erin și Francy, care transformă fiecare termen într-o lecție distractivă.

Dacă ai între 8 și 14 ani, ești curios și vrei să înveți cum să folosești internetul în siguranță, acest dicționar e făcut exact pentru tine. Iar dacă un adult citește alături de tine – fie el părinte, bunic sau profesor – s-ar putea să învețe și el ceva nou!
CyberInes, ErinJoy și HackyFrancy te așteaptă să porniți împreună în această călătorie prin alfabetul cyber. La final, vei primi un certificat de „Cyber-Expert" pentru curajul și curiozitatea ta!

Hai să începem această aventură – literă cu literă!

Cu entuziasm,

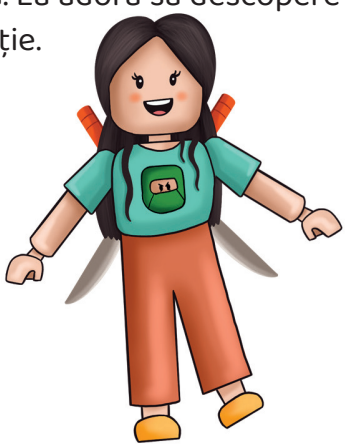
Fraga Țariuc **Alex Ricobon**

Într-o lume digitală plină de mistere, unde tehnologia întâlnește creativitatea și curajul, există trei prietene care își unesc forțele pentru a proteja internetul și pentru a te învăța cum să rămâi în siguranță în mediul online.

Ele sunt: Ines, Erin și Francesca – echipa **Cyber Explorers**!

■ **CyberInes**, la 14 ani, Ines este liderul echipei. Este sportivă, pasionată de fotbal și Formula 1, și este mereu organizată. Pentru ea, fiecare problemă cyber este ca o strategie de joc: trebuie să găsești cea mai bună soluție!

■ **ErinJoy**, 11 ani, este sufletul vesel al grupului. Dansul și jocurile, cum ar fi Roblox, o fac să fie mereu în mișcare – și la fel de curioasă în lumea digitală. Ea adoră să descopere lucruri noi și să le transforme în distracție.



HackyFrancy · HackyFrancy, 9 ani, e pasionată de coduri, jocuri și mistere digitale. Visează să devină un super hacker bun care salvează lumea de viruși și probleme cibernetice. E curajoasă, inventivă și are mereu în buzunar o glumă... sau o parolă puternică.

Împreună, ele formează o echipă de neînvins – fiecare cu stilul ei, dar unite de o misiune comună: să descopere, să protejeze și să învețe tot ce ține de siguranța digitală.

Și acum, ele te-au ales pe tine să li te alături în această aventură!

Pe măsură ce vei parcurge dicționarul, vei învăța alături de ele, vei rezolva provocări, vei afla secrete cyber și... cine știe? Poate chiar vei descoperi și tu un talent ascuns!

O misiune secretă pentru tine

Era o zi obișnuită... sau cel puțin așa părea. CyberInes își termina temele pe tabletă, ErinJoy dansa prin cameră cu căștile pe urechi, iar HackyFrancy butona concentrată un laptop cu abțibilduri cu cățeluși și coduri binare.

La un moment dat, ecranul lui HackyFrancy a pâlpâit.
Un mesaj misterios a apărut, scris cu litere verzi pe fundal negru:

> Atenție! Internetul e în pericol!
> Informații greșite, parole slabe și viruși se răspândesc mai repede ca un videoclip amuzant! Avem nevoie de voi.
>
> Formați echipa și creați Dicționarul Cyber – ca să îi învățați pe alți copii cum să se protejeze în lumea digitală.
>
> Misiunea începe ACUM.

- Asta nu e o glumă! a spus HackyFrancy, cu ochii măriți. Cineva chiar are nevoie de noi!

– E clar, e o provocare cyber! a spus CyberInes, ridicându-se în picioare. Hai să facem un plan.

– Și să-l facem super distractiv! a râs ErinJoy, începând deja să deseneze un logo pe tabletă: Cyber Explorers.

Așa a început aventura lor. Trei prietene curajoase, fiecare cu stilul ei, dar unite de aceeași dorință: să ajute copiii din toată lumea să fie mai în siguranță online.

Și ghici ce?

🎯 Acum e rândul tău!

Te invităm să faci parte din echipă. Citește fiecare termen, învață din povești, rezolvă provocările și devino și tu un Cyber-Expert!

La final, vei avea superputerea de a naviga internetul cu capul sus și parola bine setată. 🔒😉

Acces neautorizat

Definiție: este atunci când cineva accesează un sistem sau fișiere fără permisiune. Este ca și cum cineva ar intra într-o casă fără să aibă cheia.
Exemplu: Am schimbat parola WiFi-ului pentru a preveni accesul neautorizat.

Adresă IP

Definiție: adresa IP este un număr unic care identifică fiecare dispozitiv conectat la internet, la fel cum o adresă poștală indică unde locuiești.
Exemplu: Calculatorul meu are adresa IP 82.76.123.45.

Adware

Definiție: adware este un tip de program care încearcă să-ți afișeze reclame (uneori foarte enervante) pe calculator sau telefon. De multe ori, aceste reclame apar atunci când descarci aplicații gratuite din surse nesigure. Unele adware sunt inofensive, dar altele pot colecta date despre tine fără să-ți dai seama.
Exemplu: Când joc un joc gratuit, îmi apar mereu reclame enervante. Cred că are adware în el.

Amprentă digitală

Definiție: amprenta digitală este tot ce lași în urmă atunci când folosești internetul: postările, comentariile, site-urile vizitate și chiar căutările tale. Aceasta poate fi folosită pentru a înțelege cine ești sau ce preferi, așa că este important să fii atent la ce publici. Este ca urmele de pași pe care le lași pe nisip – oriunde mergi, rămâne o urmă.
Exemplu: Am realizat că toate pozele pe care le postez pe Instagram fac parte din amprenta mea digitală.

Amenințare internă / Insider Threat

Definiție: amenințarea internă este atunci când cineva din interiorul unei organizații (un angajat, de exemplu) face ceva care pune în pericol datele sau sistemele companiei, intenționat sau accidental.
Exemplu: Un angajat a descărcat fără să știe un fișier infectat, provocând o amenințare internă.

Analiza comportamentală

Definiție: analiza comportamentală este o tehnică folosită în securitatea cibernetică pentru a studia modul în care utilizatorii, programele sau dispozitivele se comportă într-un sistem. Dacă se observă ceva neobișnuit, cum ar fi un utilizator care încearcă să acceseze fișiere sensibile la o oră neobișnuită, sistemul poate alerta echipa de securitate. Este ca un profesor care observă dacă un elev se comportă diferit față de obiceiurile sale normale și întreabă ce se întâmplă.
Exemplu: Un sistem de analiză comportamentală a observat că cineva încerca să descarce multe fișiere importante fără permisiune.

Analiza jurnalelor (Log Analysis)

Definiție: Analiza jurnalelor înseamnă verificarea fișierelor în care sunt înregistrate toate activitățile unui sistem, rețele sau aplicații. Aceste fișiere, numite „loguri," sunt ca niște caiete care notează fiecare acțiune ce are loc. Experții analizează aceste jurnale pentru a găsi probleme, atacuri cibernetice sau comportamente neobișnuite. Este ca și cum ai citi un jurnal pentru a înțelege ce s-a întâmplat într-o zi.
Exemplu: Administratorul a verificat log-urile pentru a înțelege de ce rețeaua funcționa mai încet.

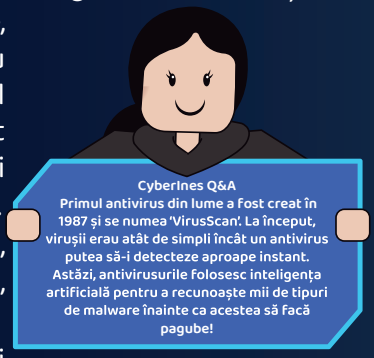
Analiza traficului (Traffic Analysis)

Definiție: analiza traficului se referă la monitorizarea datelor care circulă într-o rețea pentru a detecta activități suspecte. Este ca și cum ai verifica ce mașini intră și ies dintr-un oraș.

Exemplu: Rețeaua universității folosește analiza traficului pentru a detecta atacurile.

Antivirus

Definiție: antivirusul este un program care te ajută să îți protejezi calculatorul sau telefonul împotriva „virușilor digitali." Acesti viruși sunt programe rele care pot distruge fișiere, fura informații sau face dispozitivul tău să funcționeze mai încet. Antivirusul funcționează ca un gardian: scanează tot ce intră pe calculator, cum ar fi fișiere, jocuri sau emailuri, și elimină orice lucru periculos.



Exemplu: Când am descărcat un joc nou, antivirusul meu mi-a spus că e periculos, așa că nu l-am instalat.

CyberInes: întreabă un adult dacă ai un antivirus instalat pe dispozitivul tău. Dacă nu știi, cere ajutorul și aflați împreună!

Atac prin reutilizarea acreditivelor

Definiție: în acest tip de atac, denumit în engleză Credential Stuffing, hackerii folosesc nume de utilizator și parole furate de pe un site pentru a încerca să acceseze conturi pe alte site-uri. Acest lucru funcționează dacă oamenii folosesc aceeași parolă pentru mai multe conturi. Este ca și cum cineva ar găsi o cheie pierdută și ar încerca să deschidă toate ușile dintr-un bloc cu ea.

Exemplu: Am fost avertizat să nu folosesc aceeași parolă pe mai multe site-uri, pentru a preveni un atac de tip credential stuffing.

Atac Zero-Day

Definiție: Un atac de tip zero-day exploatează o vulnerabilitate necunoscută până atunci de către dezvoltatori. Este foarte periculos deoarece nu există o soluție imediată. Se aseamănă cu descoperirea unei uși secrete într-un castel, pe care nimeni nu știa că există, și

intrarea prin ea înainte ca regele să o blocheze.
Exemplu: Hackerii au lansat un zero-day attack asupra unei aplicații populare înainte ca dezvoltatorii să repare problema.

Autentificare

Definiție: autentificarea este procesul prin care un sistem verifică dacă tu ești persoana care spune că este. Gândește-te la ea ca la o ușă cu lacăt – pentru a intra, trebuie să arăți cheia (parola ta). Uneori, pe lângă parolă, sistemul îți mai cere și un cod trimis pe telefon sau scanarea feței tale, pentru a fi sigur că ești tu. Acest lucru face sistemul mult mai sigur și îi oprește pe hoți să îți acceseze conturile.
Exemplu: Când m-am conectat la Roblox, pe lângă parola mea, mi-au trimis un cod pe telefon. Asta e autentificare în doi pași!

Autentificare compromisă

Definiție: Broken authentication apare atunci când un sistem de autentificare (modul în care utilizatorii se conectează cu un nume de utilizator și o parolă) are probleme de securitate. Aceste probleme permit hackerilor să acceseze conturile fără permisiune, fie prin parole slabe, fie prin exploatarea unor erori din sistem. Este ca și cum cineva ar avea o cheie falsă care se potrivește la lacătul tău.
Exemplu: Un site avea o problemă de autentificare compromisa, iar parolele utilizatorilor au fost furate.

Backup

Definiție: Backup-ul este o copie de rezervă a fișierelor tale importante. Dacă, din greșeală, ștergi ceva sau dacă calculatorul tău are o problemă, poți recupera totul din backup. Este ca și cum ai avea o cutie de siguranță în care păstrezi lucruri prețioase, ca să nu le pierzi niciodată. Poți face backup pe un stick USB, pe un hard disk extern sau în cloud (spațiu de stocare pe internet).
Exemplu: Am făcut un backup al pozelor de vacanță pe un hard disk extern, ca să fiu sigur că nu le pierd.

Blue Team

Definiție: Blue Team este echipa care apără sistemele informatice de atacuri. Ei monitorizează, detectează și răspund la amenințări cibernetice, ca niște gardieni digitali. Dacă Red Team e „echipa de atac", Blue Team e „echipa de apărare".
Exemplu: Blue Team-ul a descoperit că cineva încerca să intre neautorizat în rețea și a blocat atacul imediat.

Bombă logică

Definiție: o bombă logică este un program ascuns pe calculator care rămâne inactiv până când este îndeplinită o anumită condiție, cum ar fi o dată anume sau deschiderea unui fișier. Când condiția este îndeplinită, bomba logică „explodează" și poate șterge fișiere, bloca calculatorul sau cauza alte probleme. Este ca un balon care explodează doar dacă cineva îl atinge.
Exemplu: Un atacator a introdus o bombă logică în sistem care s-a activat pe 1 aprilie.

Bomba ZIP

Definiție: o bombă ZIP este un fișier comprimat care, odată deschis, generează un volum uriaș de date care poate face sistemul inutilizabil. Este ca o cutie mică de cadouri care explodează într-o mulțime de

lucruri când o deschizi.
Exemplu: Am evitat descărcarea unui fișier ZIP suspect care putea fi o bombă ZIP.

Botnet

Definiție: Botnet-ul este ca o armată de roboți digitali controlați de un hacker. Fiecare „robot" este, de fapt, un calculator infectat cu malware, iar hackerul poate folosi aceste calculatoare pentru a face lucruri rele, cum ar fi să trimită spam sau să atace alte site-uri. Dacă ai grijă de calculatorul tău și îl protejezi, el nu va deveni parte dintr-un botnet.
Exemplu: Am citit că un hacker a folosit un botnet cu mii de calculatoare pentru a opri funcționarea unui site important.

ErinJoy Q&A
Știai că cel mai mare botnet din lume a infectat peste 30 de milioane de calculatoare? Se numea 'Storm Botnet' și era atât de puternic încât putea opri rețele întregi!

Breșă de securitate

Definiție: o breșă de securitate apare atunci când sistemele sau rețelele sunt compromise, iar datele sensibile sunt accesate sau furate fără permisiune. Acest lucru se întâmplă din cauza vulnerabilităților, atacurilor cibernetice sau erorilor umane. Este ca atunci când cineva intră pe furiș într-o clădire și fură documente importante.
Exemplu: O breșă de securitate a expus datele clienților unei companii mari.

Cal Troian

Definiție: un cal troian este un tip de program periculos (malware) care se prezintă ca ceva util sau inofensiv, dar care, odată instalat, permite hackerilor să acceseze sau să controleze calculatorul tău. Este ca un cadou care pare frumos pe dinafară, dar care ascunde ceva rău înăuntru.
Exemplu: Am descărcat un joc gratuit care conținea un cal troian, dar antivirusul meu l-a blocat.

Carantină

Definiție: carantina în securitatea cibernetică este un spațiu virtual unde fișierele suspecte sunt izolate, astfel încât să nu poată infecta calculatorul tău. Este ca un loc unde pui ceva periculos pentru a-l analiza mai târziu.
Exemplu: Antivirusul meu a pus în carantină un fișier care părea suspect.

Cloud Computing

Definiție: Cloud computing înseamnă să folosești aplicații și să salvezi fișiere pe internet, în loc să le ai doar pe calculatorul tău. Gândește-te la cloud ca la un raft invizibil, accesibil de oriunde, atâta timp cât ai conexiune la internet. Serviciile de cloud sunt folosite pentru a stoca poze, documente sau pentru a colabora cu alți oameni.
Exemplu: Am salvat tema mea de la școală în cloud, așa că o pot accesa și de pe telefon.

Command and Control (C2)

Definiție: C2 Command and Control este un sistem pe care hackerii îl folosesc pentru a controla dispozitivele infectate cu malware (cum ar fi calculatoare, telefoane sau servere). După ce un dispozitiv este

compromis, acesta se conectează la serverul C2, unde hackerii pot da comenzi, fura date sau provoca daune. Este ca un păpușar care trage sforile și controlează păpușile (dispozitivele infectate) de la distanță.
Exemplu: Hackerii au folosit un server de C2 pentru a lansa atacuri DDoS.

Controlul accesului / Access Control

Definiție: controlul accesului înseamnă să stabilești cine are voie să folosească anumite lucruri pe un calculator, o aplicație sau o rețea. Este ca o listă de invitați la o petrecere: doar cei care sunt pe listă pot intra. În lumea digitală, accesul este controlat de parole, carduri de acces sau chiar recunoaștere facială. Acest sistem ajută la protejarea informațiilor sensibile.
Exemplu: La școală, doar profesorii au acces la notele elevilor, iar eu pot accesa doar temele mele.

Cookie

Definiție: Cookie-urile sunt mici fișiere pe care site-urile web le salvează pe calculatorul tău. Ele își „amintesc" informații despre tine, cum ar fi preferințele tale sau ce produse ai pus în coșul de cumpărături online. Deși majoritatea cookie-urilor sunt inofensive și utile, unele pot urmări prea multe lucruri despre tine.
Exemplu: Site-ul pe care l-am vizitat mi-a spus că folosește cookie-uri ca să-și amintească preferințele mele.

Criminalistică digitală (Forensics)

Definiție: criminalistica digitală este procesul de investigare a unui incident cibernetic. Experții analizează dispozitivele și datele pentru a descoperi cum s-a întâmplat un atac și cine este responsabil. Este ca o investigație polițienească, dar în lumea digitală.
Exemplu: Specialiștii în forensics au analizat laptopurile pentru a găsi dovezi despre atacul hackerilor.

Criptare

Definiție: criptarea este procesul prin care informațiile sunt transformate într-un cod secret, astfel încât doar persoanele care au cheia potrivită să le poată înțelege. Este ca și cum ai pune o scrisoare într-o cutie cu lacăt și doar destinatarul are cheia. Criptarea este folosită pentru a proteja mesajele, parolele și alte date sensibile.**Exemplu:** Când trimit mesaje pe WhatsApp, ele sunt criptate, deci doar eu și prietenii mei le putem citi.

HackyFrancy Q&A:
Știai că criptarea a fost folosită încă din vremea Egiptului Antic? Faraonii scriau mesaje secrete folosind simboluri ciudate pe papirus, la fel cum facem astăzi cu codurile digitale pentru a proteja informațiile!

Criptare cu cheie publică / Public Key Encryption

Definiție: criptarea cu cheie publică este o metodă de securizare a informațiilor în care se folosesc două chei diferite: o cheie publică și o cheie privată. Cheia publică este folosită pentru a cripta (securiza) mesajele, iar cheia privată este folosită pentru a le decripta (citi). Doar persoana care are cheia privată poate accesa informațiile. Este ca un lacăt la care toată lumea are cheia de închidere, dar doar tu ai cheia pentru a-l deschide.

Exemplu: Emailurile mele sunt criptate folosind public key encryption, astfel încât doar destinatarul le poate citi.

Criptarea backup-ului

Definiție: criptarea backup-ului înseamnă protejarea copiilor de rezervă ale datelor printr-un cod secret. Astfel, dacă cineva fură aceste fișiere, nu le poate accesa fără cheie.

Exemplu: Am criptat backup-ul pozelor mele pentru a le proteja.

Cryptojacking

Definiție: Cryptojacking este un tip de atac cibernetic în care hackerii folosesc în secret calculatorul sau telefonul altcuiva pentru a mina criptomonede (cum ar fi Bitcoin). Acest lucru face dispozitivul mai lent și poate consuma multă energie. Este ca și cum cineva s-ar conecta la priză în casa ta fără să-ți ceară voie și ar folosi curentul tău pentru propriul câștig.

Exemplu: Am observat că laptopul meu mergea mai încet și antivirusul a descoperit un script de cryptojacking.

Cyberbullying

Definiție: Cyberbullying-ul este atunci când cineva folosește internetul sau rețelele sociale pentru a spune lucruri răutăcioase, a jigni sau a hărțui pe cineva. Este o formă de agresiune care poate răni foarte tare sentimentele oamenilor. Este important să fii amabil online și să vorbești cu un adult dacă cineva te face să te simți rău.

Exemplu: Am văzut că cineva i-a lăsat comentarii urâte unui coleg pe Instagram și am raportat acele mesaje.

Dark Web

Definiție: Dark web-ul este o parte ascunsă a internetului care nu poate fi accesată cu browserele normale. Este folosit uneori pentru activități ilegale, dar și pentru a comunica în siguranță în țările unde există cenzură. Nu este un loc pentru copii și trebuie evitat.
Exemplu: Am citit că dark web-ul este folosit de hackeri, dar și de jurnaliști din țări unde internetul este cenzurat.

DDoS /Distributed Denial of Service

Definiție: un atac DDoS este atunci când hackerii folosesc multe calculatoare (chiar și zeci de mii) pentru a bombarda un site web cu cereri false, astfel încât site-ul să nu mai poată funcționa. Este ca și cum toată lumea ar suna la aceeași ușă în același timp, iar proprietarul nu mai poate face față.
Exemplu: Un magazin online nu a mai funcționat o zi întreagă din cauza unui atac DDoS.

Dispozitiv de securitate (Security Token)

Definiție: Este un dispozitiv sau o aplicație care generează coduri unice pentru autentificare. Este folosit pentru a crește securitatea conturilor. Este ca un cheie electronică pe care o folosești împreună cu o cheie fizică pentru a deschide o ușă.
Exemplu: Pentru accesarea contului meu bancar folosesc un security token care generează coduri unice.

DNS Spoofing

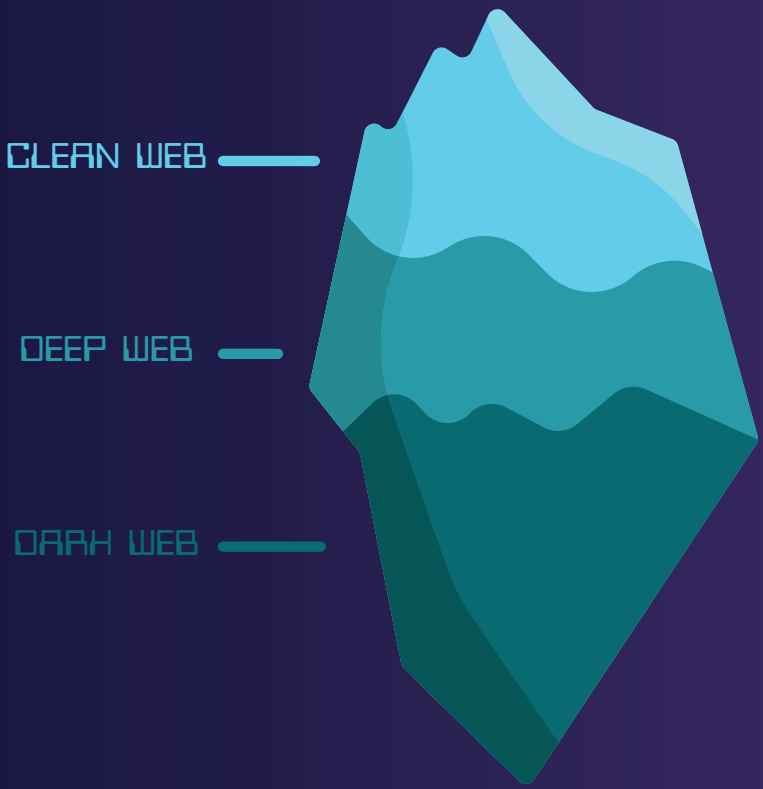
Definiție: DNS spoofing este un atac cibernetic în care hackerii păcălesc sistemele să redirecționeze utilizatorii către site-uri false care arată că cele reale, pentru a fura informații, cum ar fi parolele. Este ca o „hartă falsă" care arată ca cele reale.
Exemplu: Un atac de tip DNS spoofing m-a dus pe un site care arăta

ca banca mea, dar era fals.

Drive-by Download

Definiție: un drive-by download este un tip de atac cibernetic în care un fișier periculos este descărcat automat pe calculatorul tău atunci când vizitezi un site infectat, fără ca tu să-ți dai seama. Hackerii folosesc aceste fișiere pentru a instala malware sau a fura informații. Este ca și cum ai trece pe lângă cineva care îți pune ceva în geantă fără să observi.

Exemplu: Am fost atenționat că un site pe care voiam să-l vizitez poate descărca malware printr-un drive-by download.



E

Endpoint Detection and Response (EDR)

Definiție: EDR este o tehnologie care monitorizează dispozitivele conectate la o rețea pentru a detecta și răspunde rapid la amenințările cibernetice. Este ca o cameră de supraveghere pentru laptopul sau telefonul tău.
Exemplu: EDR-ul a blocat un fișier suspect înainte să infecteze rețeaua.

Escaladarea privilegiilor / Privilege Escalation

Definiție: escaladarea privilegiilor este o tehnică folosită de hackeri pentru a obține mai mult control asupra unui sistem decât ar trebui să aibă. De exemplu, cineva care are acces limitat la un calculator poate găsi o metodă de a obține acces complet pentru a schimba setări sau a fura informații. Este ca și cum ai avea cheie doar pentru camera de zi, dar reușești să găsești o cale să intri în toată casa.
Exemplu: Un atac de tip privilege escalation le-a permis hackerilor să acceseze toate fișierele companiei.

Evaluarea riscurilor

Definiție: evaluarea riscurilor este procesul prin care o companie identifică ce amenințări ar putea să îi afecteze sistemele și decide cum să le prevină. Este ca o verificare periodică a casei pentru a te asigura că totul e în siguranță.
Exemplu: Echipa IT face evaluarea riscurilor lunar pentru a identifica problemele de securitate.

Evaluarea vulnerabilităților

Definiție: Evaluarea vulnerabilităților este procesul prin care un sistem sau o rețea este verificată pentru a descoperi probleme de securitate care ar putea fi exploatate de hackeri. Scopul este să

găsești și să repari aceste puncte slabe înainte ca cineva să le folosească împotriva ta. Este ca atunci când verifici o clădire pentru a vedea dacă există ferestre sparte sau uși descuiate care trebuie reparate.
Exemplu: Echipa noastră IT face evaluări regulate ale vulnerabilităților pentru a preveni atacurile.

Evil Twin Attack

Definiție: este un atac în care un hacker creează o rețea WiFi falsă care pare legitimă. Când te conectezi, hackerul poate intercepta informațiile tale. Este ca și cum ai merge la un restaurant fals care arată ca cel original.
Exemplu: Când sunt într-o cafenea, mă asigur că rețeaua WiFi este cea oficială, pentru a evita un atac Evil Twin.

Exfiltrarea de date / Data Exfiltration

Definiție: exfiltrarea de date înseamnă furtul de date dintr-un calculator sau dintr-o rețea fără permisiune. Hackerii găsesc o metodă de a copia informații importante, cum ar fi parole, fișiere sau date personale, și le trimit în afara sistemului. Este ca și cum cineva ar fura un jurnal din camera ta și l-ar scoate pe fereastră fără să-ți dai seama.
Exemplu: Școala mea a prevenit un atac prin care se incerca exfiltrarea de date datorită sistemului avansat de monitorizare si protecție.

Exploit

Definiție: Exploit-ul este o metodă folosită de hackeri pentru a profita de o slăbiciune într-un program sau sistem, astfel încât să poată fura date sau să preia controlul. Este ca și cum ai găsi o ușă lăsată întredeschisă și ai intra fără permisiune.
Exemplu: Un hacker a folosit un exploit dintr-un joc pentru a accesa datele jucătorilor.

F

Falsificarea emailurilor (Email Spoofing)

Definiție: este atunci când un hacker trimite un email care pare să vină de la o sursă de încredere (cum ar fi banca ta), dar de fapt este fals. Scopul este să te păcălească să dai informații sensibile.
Exemplu: Am primit un email care părea de la banca mea, dar era spoofing. Am verificat adresa expeditorului și era falsă.

Firewal

Definiție: un firewall este un program sau un dispozitiv care protejează calculatorul tău de atacuri din exterior, blocând accesul neautorizat. Este ca un gardian care decide ce informații pot intra și ieși din rețea.
Exemplu: Firewall-ul meu blochează orice încercare de acces neautorizat la rețeaua mea de acasă.

Firmware

Definiție: Firmware-ul este un tip special de software care controlează componentele fizice ale unui dispozitiv, cum ar fi imprimanta sau routerul. Este ca un creier care îi spune dispozitivului ce să facă.
Exemplu: Am actualizat firmware-ul routerului meu pentru a îmbunătăți securitatea rețelei WiFi.

Full Disk Encryption (FDE)

Definiție: Full Disk Encryption este o tehnologie care protejează toate datele de pe un calculator sau un dispozitiv, transformându-le într-un cod secret. Doar cineva care știe parola corectă poate decripta și accesa datele. Este ca și cum ai pune un lacăt foarte sigur pe un cufăr care conține toate lucrurile tale importante.
Exemplu: Telefonul meu folosește full disk encryption pentru a proteja fotografiile și mesajele mele.

Furt de identitate / Identity Theft

Definiție: furtul de identitate este atunci când cineva îți fură informațiile personale (cum ar fi numele sau numărul cardului) și le folosește pentru a se da drept tine sau a face cumpărături.
Exemplu: Un hacker a folosit datele mele pentru a comanda lucruri online – asta se numește furt de identitate.

Furtul de credențiale / Credential Theft

Definiție: Este procesul prin care hackerii fură informațiile de conectare, cum ar fi numele de utilizator și parolele, pentru a accesa conturile victimelor.
Exemplu: Am schimbat imediat parola după ce am aflat despre o tentativă de credential theft.

GDPR (General Data Protection Regulation)

Definiție: GDPR este o lege europeană care protejează datele personale ale oamenilor. Ea obligă companiile să colecteze și să folosească informațiile tale în mod responsabil și să-ți ceară permisiunea înainte de a le folosi.
Exemplu: Un site mi-a cerut să accept termenii GDPR înainte să-mi creez un cont.

Geolocalizare

Definiție: geolocalizarea înseamnă să folosești tehnologia pentru a determina unde te afli pe glob. Este folosită de aplicații precum hărțile sau jocurile care depind de locația ta.
Exemplu: Am folosit geolocalizarea pe telefon ca să găsesc cel mai apropiat restaurant.

Geolocalizare limitată(Geofencing)

Definiție: Geofencing este o tehnologie care creează o „zonă virtuală" pe hartă în jurul unui loc fizic. Când un dispozitiv, cum ar fi telefonul tău, intră sau iese din acea zonă, este trimis un mesaj sau se activează o anumită funcție. Este ca o barieră invizibilă care știe când ai trecut peste ea.
Exemplu: Am primit o notificare pe telefon când am intrat într-un magazin, datorită geofencing-ului.

Guvernanță

Definiție: guvernanța în securitatea cibernetică se referă la regulile și procedurile care ajută o organizație să își protejeze informațiile și să se asigure că totul funcționează în siguranță. Este ca un set de reguli pentru a păstra ordinea într-un oraș digital.

Exemplu: Compania mea are reguli stricte de guvernanță pentru a preveni accesul neautorizat la datele clienților.

H

Hacker

Definiție: un hacker este o persoană care folosește cunoștințele despre computere pentru a accesa sisteme sau date. Unii hackeri ajută companiile să își îmbunătățească securitatea (hackeri buni sau „white hat"), iar alții o folosesc pentru a face rău (hackeri răi sau „black hat").
Exemplu: Un hacker bun a ajutat o companie să descopere o problemă de securitate în aplicația lor.

Hashing

Definiție: hashing-ul este un proces prin care datele sunt transformate într-o serie de caractere unice, numite hash. Este folosit pentru a verifica dacă datele nu au fost modificate. Gândește-te la el ca la o „amprentă digitală" a fișierelor.
Exemplu: Parolele mele sunt stocate sub formă de hash, astfel încât nimeni să nu le poată citi.

Honeypot

Definiție: un honeypot este un sistem sau un site special creat pentru a atrage hackerii și a-i păcăli să interacționeze cu el. Scopul este să se descopere cum acționează hackerii sau să îi țină ocupați departe de sistemele reale. Este ca o capcană pentru urși, în care pui miere ca să atragi urșii, dar nu îi lași să ajungă la stupul adevărat.
Exemplu: Cercetătorii au folosit un honeypot pentru a înțelege cum lucrează un nou tip de malware.

Host-based Firewal

Definiție: Un host-based firewall este un program instalat direct pe un calculator sau un dispozitiv care monitorizează și controlează traficul de rețea ce intră și iese din acel dispozitiv. Acesta protejează calculatorul de atacuri cibernetice și blochează accesul programelor

suspecte. Este ca o ușă cu vizor pe care o poți închide sau deschide pentru a decide cine poate intra în casă și cine nu.

Exemplu: Laptopul meu folosește un host-based firewall pentru a bloca atacurile locale.

Pauză Cyber: Aventurile lui CyberInes, ErinJoy și FranByte în Lumea Digitală

Într-o dimineață strălucitoare, CyberInes, ErinJoy și FranByte se întâlniră în laboratorul lor super-secret, numit „Fortăreața Codurilor". Era un loc plin de ecrane, lumini colorate și sunete de taste apăsate rapid. Cele trei eroine aveau o misiune specială: să protejeze lumea digitală de pericolele ascunse și să-i învețe pe toți despre securitatea cibernetică.

CyberInes, lidera grupului, își verifică panoul de comandă.

- Avem o alertă din Rețeaua Pixelia! Cineva a plantat un virus care încetinește toate serverele din oraș! spuse ea, cu privirea concentrată.

- Un virus?! Bleah, asta sună nasol! exclamă ErinJoy, cea mai veselă dintre ele, care dansa în timp ce ajusta antenele lor WiFi. Ne apucăm de treabă?

- Absolut! interveni FranByte, expertă în gadgeturi digitale. Dar fiți atente. Dacă virusul a fost plantat cu un Trojan Horse, s-ar putea să fie o capcană.

- Corect. Să activăm firewall-ul nostru pentru protecție suplimentară, spuse CyberInes, tastând rapid pe tastatură.

Cele trei intrară în lumea virtuală prin portalul lor special.

Rețeaua Pixelia era un loc vibrant, plin de pixeli plutitori și pachete de date care circulau rapid. Dar astăzi, totul era încet. Un nor negru de cod malefic plutea peste un server central.


WARNING
VIRUS DETECTED
VIRUS ALERT!

- Asta arată ca un caz clasic de Distributed Denial of Service (DDoS), observă FranByte.Cred că hackerii au supraîncărcat serverul.

- Atunci trebuie să resetăm serverul și să eliminăm virusul, spuse ErinJoy, ridicând o baghetă digitală numită Intrerupător de Coduri.

Când se apropiară de server, o ușă imensă, decorată cu simboluri misterioase, apăru în fața lor.

- Hmm, asta pare o poartă cu authentication (autentificare), spuse CyberInes. Dar uitați-vă la asta – e falsă! E un Trojan Horse în spatele ușii. Dacă intrăm, activăm un alt atac.

- Nu-i nimic, am un plan! exclamă FranByte. Folosim un honeypot ca să-i păcălim pe atacatori să-și dezvăluie locația.

ErinJoy zâmbi strengareste.

- Îmi place cum gândești! Și, cu un singur clic, honeypot-ul lor a fost activat, iar hackerii au fost prinși în flagrant.

Cu serverele curățate și hackerii opriți, Rețeaua Pixelia era din nou funcțională.

- Trebuie să învățăm pe toată lumea despre password hygiene (igiena parolelor) și să-i avertizăm să nu deschidă atașamente suspecte, spuse CyberInes.

- Și să folosim mereu Two-Factor Authentication (2FA) pentru conturi importante, adăugă FranByte.

- Am câștigat încă o bătălie, dar lumea digitală are mereu nevoie de eroi ca noi! spuse ErinJoy, făcând un mic dans al victoriei.

Așa se termină aventura celor trei eroine: CyberInes, ErinJoy și FranByte. Împreună, ele nu doar că protejează lumea digitală, ci și îi ajută pe toți să înțeleagă importanța securității cibernetice – cu zâmbete și voie bună!

Incident (Incident de securitate)

Definiție: Un incident de securitate este un eveniment care afectează negativ funcționarea unui sistem, a unei rețele sau a datelor unei organizații. Acesta poate include atacuri cibernetice, pierderi de date, infectări cu malware sau acces neautorizat. Este ca atunci când cineva încearcă să intre în casa ta fără permisiune sau lasă o ușă deschisă și lucrurile dispar.
Exemplu: Un incident de securitate a avut loc când un hacker a accesat un server și a descărcat fișiere importante.

Information Security (InfoSec)

Definiție: InfoSec este procesul de protejare a informațiilor importante, fie că sunt stocate pe un calculator, trimise prin internet sau scrise pe hârtie. Scopul este de a preveni ca aceste informații să fie furate, schimbate sau pierdute. Este ca o cutie de valori în care îți păstrezi obiectele prețioase pentru a fi în siguranță.
Exemplu: Compania mea se concentrează pe InfoSec pentru a proteja informațiile clienților.

Inginerie socială (Social Engineering)

Definiție: social engineering înseamnă să manipulezi sau să păcălești oamenii pentru a obține informații sensibile, cum ar fi parolele sau datele cardurilor. Hackerii nu atacă tehnologia, ci încrederea oamenilor. Este ca și cum cineva te-ar convinge să îi dai cheia casei spunând că e un prieten al familiei.
Exemplu: Un hacker mi-a trimis un mesaj prefăcându-se că este prietenul meu, dar încerca să-mi fure parola.

Inteligența artificială în securitate cibernetică

Definiție: inteligența artificială (AI) este folosită pentru a detecta și preveni atacurile cibernetice. AI poate învăța cum arată comportamentul normal într-un sistem și poate recunoaște rapid orice activitate suspectă, oprind atacurile mai repede decât un om. Este ca un paznic foarte inteligent care observă orice mișcare neobișnuită și acționează imediat.
Exemplu: Compania mea folosește AI pentru a detecta tentativele de phishing în emailuri.

Interceptarea traficului de rețea (Network Sniffing)

Definiție: Network sniffing este o tehnică prin care hackerii sau specialiștii în securitate analizează datele care circulă într-o rețea. Dacă rețeaua nu este protejată, cineva poate vedea informații sensibile, cum ar fi parolele sau mesajele trimise. Este ca și cum ai asculta conversațiile oamenilor care vorbesc într-o cameră, fără să fii invitat.
Exemplu: Un hacker a folosit network sniffing pe o rețea WiFi nesecurizată pentru a captura parolele utilizatorilor care se conectau.

IoT (Internet of Things)

Definiție: Internetul Lucrurilor (IoT) se referă la toate dispozitivele conectate la internet, cum ar fi ceasurile inteligente, frigiderele inteligente sau becurile controlate prin telefon. Aceste dispozitive fac viața mai ușoară, dar trebuie protejate pentru a nu fi hackuite.
Exemplu: Ceasul meu inteligent este un dispozitiv IoT și îl folosesc pentru a-mi monitoriza pașii zilnici.

Jailbreaking

Definiție: Jailbreaking înseamnă să modifici un dispozitiv, cum ar fi un telefon, pentru a elimina restricțiile impuse de producător. Acest lucru îți permite să instalezi aplicații și să faci modificări care nu sunt aprobate oficial. Dar, odată făcut, dispozitivul devine mai vulnerabil la atacuri. Este ca și cum ai sparge un lacăt pus de fabrică pe o cutie, astfel încât să poți folosi tot ce se află înăuntru cum vrei tu, chiar dacă nu era planificat așa.
Exemplu: Prietenul meu a făcut jailbreak la telefonul său pentru a descărca aplicații care nu sunt disponibile în magazinul oficial, dar acum are probleme de securitate.

JavaScript

Definiție: JavaScript este un limbaj de programare folosit pentru a face paginile web interactive și dinamice. Cu ajutorul lui, site-urile pot să răspundă la acțiunile utilizatorilor, cum ar fi apăsarea unui buton, completarea unui formular sau chiar rularea de jocuri direct în browser. Este ca „motorul" care dă viață unui site, transformându-l dintr-o simplă pagină statică într-o experiență captivantă.
Exemplu: Când apeși pe un buton și apare un mesaj de tipul 'Mulțumim pentru înscriere!', acel mesaj este afișat cu ajutorul JavaScript. Cod simplu de exemplu:

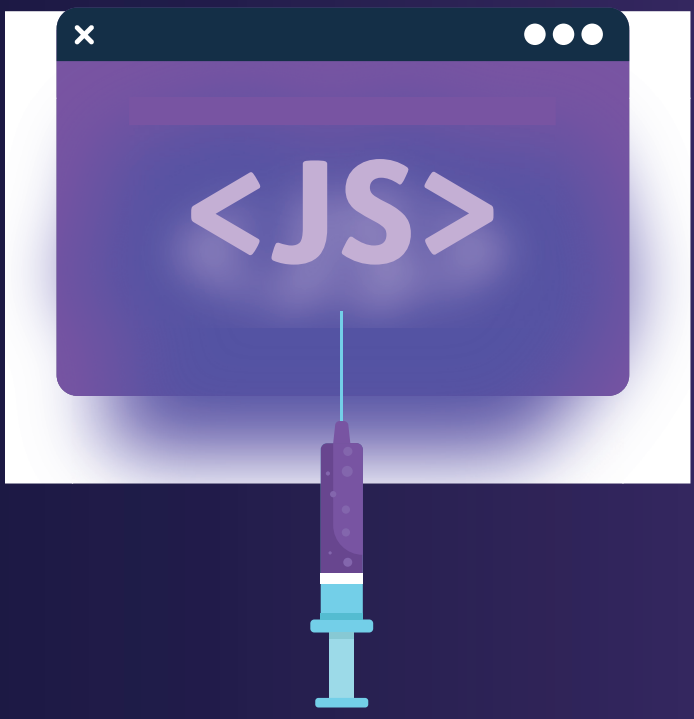
```
document.getElementById("buton".addEventListener("click,function() {
alert("Mulțumim pentru înscriere!");
});
```

JavaScript Injection

Definiție: este un tip de atac în care un hacker introduce cod malițios JavaScript într-un site web pentru a fura informații sau a prelua controlul asupra site-ului. Este ca și cum cineva ar adăuga instrucțiuni periculoase pe o listă de lucruri de făcut.
Exemplu: Un atac de tip JavaScript injection a făcut ca site-ul să afișeze reclame false.

JSON Web Token (JWT)

Definiție: JSON Web Token este un mod sigur de a transmite informații între două părți (de exemplu, între un utilizator și un server). Informațiile sunt codificate într-un format special care poate fi verificat pentru a vedea dacă nu a fost modificat. Este ca un bilet de acces care dovedește că ai permisiunea să intri undeva, iar semnătura specială de pe bilet arată că este autentic și nu a fost falsificat.
Exemplu: Aplicația mea de școală folosește JWT pentru a mă autentifica rapid și sigur.



H

Kernel

Definiție: Kernel-ul este partea centrală a unui sistem de operare, responsabilă de gestionarea resurselor și a comunicării dintre hardware și software. Este ca un dirijor care face ca totul să funcționeze armonios.
Exemplu: Kernel-ul calculatorului meu s-a actualizat pentru a repara o problemă de securitate.

Kernel Exploitation

Definiție: Kernel Exploitation este un tip de atac în care hackerii vizează nucleul (kernel-ul) sistemului de operare, care controlează toate funcțiile importante ale unui calculator. Dacă reușesc, pot prelua controlul total asupra dispozitivului. Este ca și cum cineva ar găsi cheia centrală a unei clădiri și ar putea accesa fiecare cameră fără restricții.
Exemplu: Un exploit de kernel a permis hackerilor să preia controlul unui server.

Key Exchange

Definiție: Key exchange este procesul prin care două persoane sau sisteme împart în siguranță o cheie secretă pe care o folosesc pentru a cripta și decripta mesaje. Este ca un schimb de secrete pe care doar ei le pot înțelege.
Exemplu: Aplicațiile de mesagerie folosesc key exchange pentru a face conversațiile private.

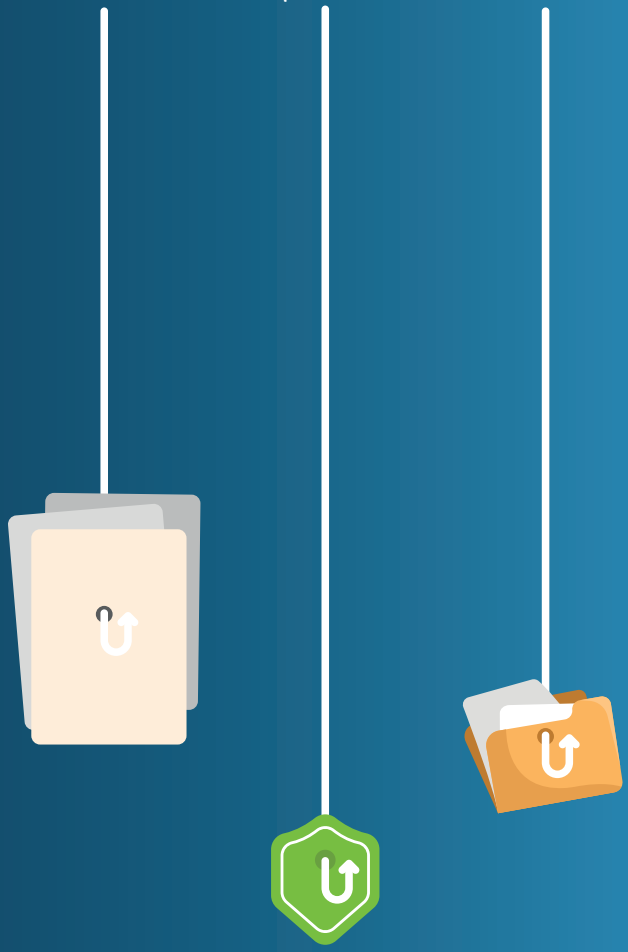
Keylogger Attack

Definiție: un keylogger attack este un tip de atac cibernetic în care un program rău intenționat numit „keylogger" este instalat pe calculatorul unei persoane. Acest program înregistrează tot ce tastezi, inclusiv parolele, mesajele și alte informații personale și le trimite hackerului. Este ca și cum cineva ar sta în spatele tău și ar nota

fiecare cuvânt pe care îl scrii.
Exemplu: Un keylogger a fost detectat pe calculatorul unui angajat care a descărcat un fișier suspect.

Keystroke Dynamics

Definiție: este o metodă de autentificare care analizează modul în care tastezi – cât de repede apeși pe taste și în ce ordine. Este un mod unic de identificare.
Exemplu: Aplicația folosește keystroke dynamics pentru a verifica dacă sunt eu cel care introduce parola.



L

LAN (Local Area Network)

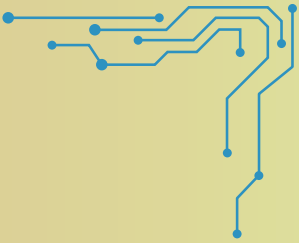
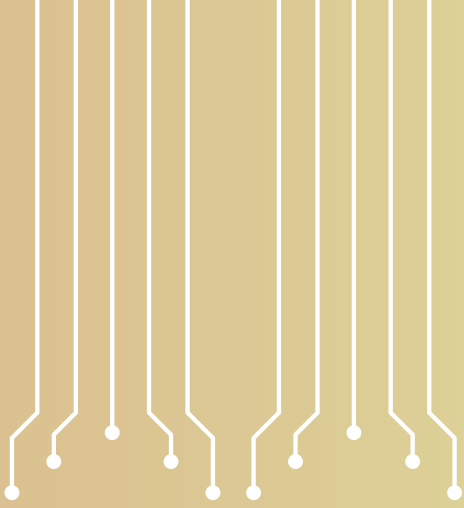
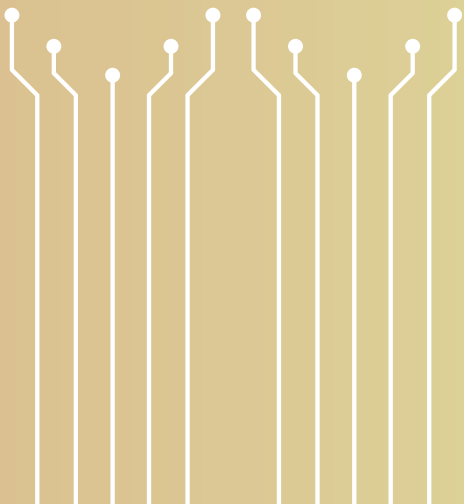
Definiție: LAN este o rețea de calculatoare și dispozitive conectate între ele într-un spațiu mic, cum ar fi o casă, o școală sau un birou. Aceasta permite dispozitivelor să comunice și să partajeze informații, cum ar fi fișiere sau imprimante. Este ca o mică echipă de prieteni care lucrează împreună într-o cameră și își împărtășesc resursele.
Exemplu: în rețeaua LAN a școlii, pot folosi imprimanta fără să mă conectez la internet.

Lanț de aprovizionare (Supply Chain)

Definiție: lanțul de aprovizionare reprezintă toate firmele și procesele implicate în crearea și livrarea unui produs sau serviciu. De exemplu, dacă cumpărăm un joc video, lanțul de aprovizionare include dezvoltatorii care l-au creat, fabricile care au făcut CD-urile, companiile care le-au transportat și magazinele care le vând.
Exemplu: Lanțul de aprovizionare al unui telefon include: minerii care extrag metale rare, fabricile care asamblează piesele și magazinele care îl vând.

Atac asupra lanțului de aprovizionare (Supply Chain Attack)

Definiție: : un supply chain attack este atunci când hackerii nu atacă direct o companie mare, ci păcălesc sau infectează o firmă mai mică, care lucrează cu aceasta. Apoi, prin acea firmă, ajung să acceseze informațiile sau sistemele companiei mari. Este ca și cum cineva ar ascunde un pachet periculos într-o livrare trimisă de o firmă de curierat pe care o cunoști.
Exemplu: Hackerii au atacat o companie care făcea actualizările unui program pe care îl folosește școala, iar programul a fost infectat.

Macros

Definiție: macrocomenzile sunt instrucțiuni sau seturi de comenzi care sunt înregistrate pentru a automatiza sarcinile repetitive într-un program, cum ar fi Word sau Excel. Ele ajută utilizatorii să economisească timp, dar, uneori, hackerii pot folosi macrocomenzi pentru a rula cod rău intenționat pe calculatorul unei victime. Este ca un robot care face o muncă pentru tine, dar dacă cineva îl controlează, ar putea face ceva rău.
Exemplu: Antivirusul meu a blocat o macro suspectă dintr-un fișier Word.

Macro Virus

Definiție: un macro virus este un tip de malware care folosește macrocomenzi – scripturi automate din programe precum Word sau Excel – pentru a se răspândi și a cauza probleme. Acest tip de virus poate șterge fișiere, modifica documente sau trimite mesaje infectate altor utilizatori. Este ca și cum ai primi un manual fals care conține instrucțiuni greșite care strică lucrurile.
Exemplu: Am deschis un fișier Word dintr-un email suspect, iar un macro virus mi-a infectat calculatorul și a trimis fișierul infectat prietenilor mei.

Malware

Definiție: Malware este un program rău intenționat creat pentru a cauza probleme pe calculatorul sau telefonul tău. Poate șterge fișiere, fura informații sau încetini dispozitivul. Tipuri comune de malware sunt virușii, troienii și ransomware-ul.
Exemplu: Am descărcat un fișier suspect, iar antivirusul meu a detectat că era malware.

Malware criptat

Definiție: Encrypted malware este un program rău intenționat care este ascuns în spatele unui cod secret (criptare) pentru a nu fi detectat de antivirusuri. Criptarea îl face greu de recunoscut până când se „dezarmează" și începe să afecteze calculatorul. Este ca un cadou frumos împachetat, dar care ascunde ceva periculos înăuntru.
Exemplu: Antivirusul meu a detectat un malware criptat care încerca să se instaleze pe calculator.

MITM (Man-in-the-Middle Attack)

Definiție: este un tip de atac în care hackerul interceptează informațiile transmise între două persoane sau sisteme fără ca acestea să știe. Este ca și cum cineva ar asculta conversația ta fără permisiune.
Exemplu: Un atac MITM poate intercepta parolele dacă te conectezi la o rețea WiFi nesigură.

Mașină virtuală / Virtual Machine

Definiție: o mașină virtuală este un program special care permite unui calculator să funcționeze ca și cum ar fi mai multe calculatoare în același timp. Practic, creezi un „calculator în interiorul calculatorului" pentru a testa lucruri noi, fără să afectezi sistemul principal. Este ca o cameră de joacă separată în care poți face experimente fără să strici restul casei.
Exemplu: Am folosit o mașină virtuală pentru a instala un joc vechi care nu funcționa pe calculatorul meu modern.

Multifactor Authentication (MFA - Autentificare multifactor)

Definiție: MFA este un mod sigur de a te conecta la conturile tale. Pe lângă parolă, trebuie să mai folosești un alt mod de verificare, cum ar fi un cod trimis pe telefon. Este ca și cum ai avea două lacăte la o ușă.
Exemplu: Am activat MFA pe contul meu de email, așa că trebuie să

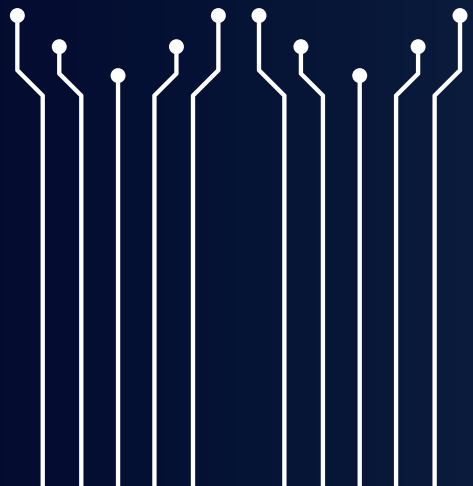
introduc și un cod din telefon.

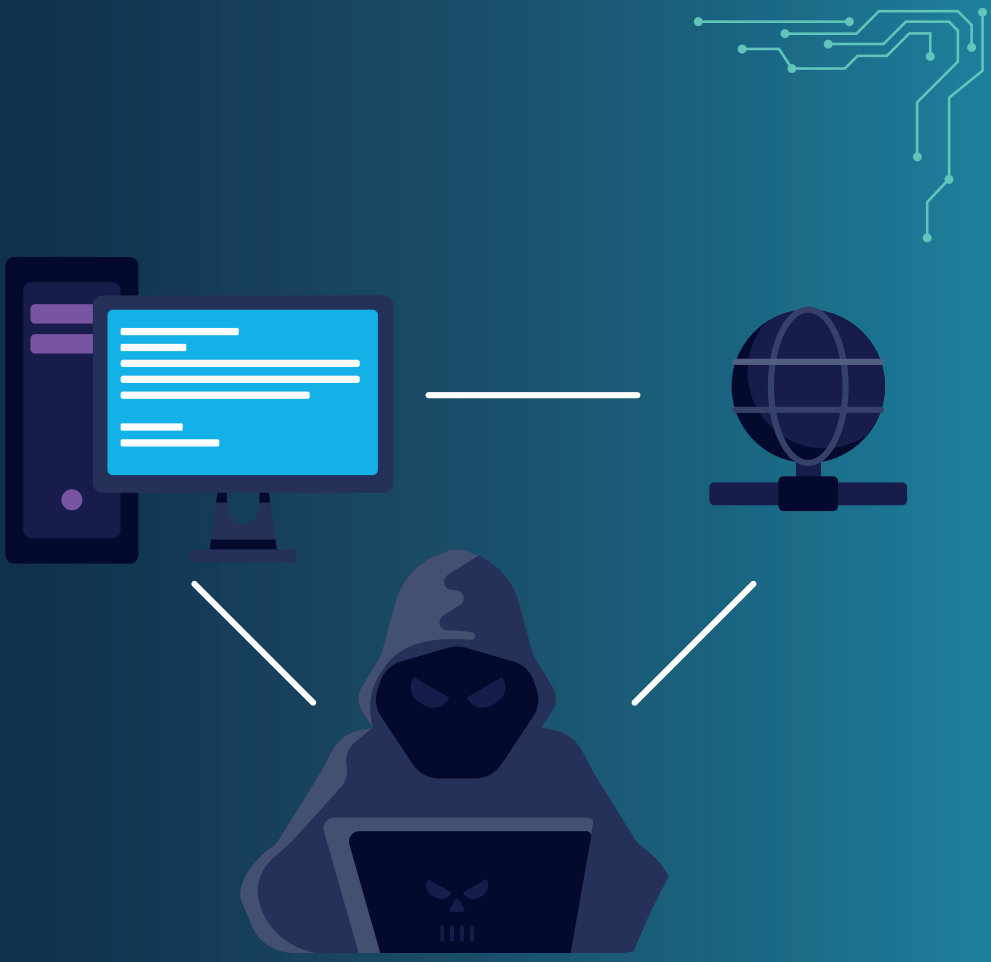
Mișcare laterală

Definiție: mișcarea laterală este o strategie folosită de hackeri după ce obțin acces într-un sistem. În loc să atace direct, ei se deplasează „lateral" prin rețea, încercând să acceseze alte computere, servere sau fișiere pentru a descoperi mai multe informații valoroase. Este ca un intrus care intră într-o clădire și încearcă să se plimbe prin diferite camere pentru a găsi lucruri importante.
Exemplu: Hackerii au folosit mișcarea laterală pentru a ajunge la serverul principal al companiei.

Mobile Device Management (MDM)

Definiție: MDM este o tehnologie folosită de companii pentru a controla și proteja dispozitivele mobile, cum ar fi telefoanele și tabletele, care sunt folosite de angajați. Cu MDM, companiile pot să instaleze aplicații, să actualizeze software-ul, să șteargă datele de la distanță dacă dispozitivul este pierdut și să asigure securitatea informațiilor. Este ca un „supervizor digital" care are grijă ca toate dispozitivele să fie sigure și funcționale.
Exemplu: Tabletele de la școală sunt gestionate printr-un sistem MDM care blochează jocurile în timpul lecțiilor.





NIDS (Network Intrusion Detection System)

Definiție: NIDS este un sistem care monitorizează rețeaua și alertează administratorii dacă detectează activități suspecte. Este ca un sistem de alarmă pentru rețea.
Exemplu: Rețeaua școlii folosește NIDS pentru a detecta accesul neautorizat.

Next-Generation Firewall (NGFW Firewall de generație următoare)

Definiție: NGFW este un firewall avansat care oferă mai mult decât protecția tradițională a rețelei. Pe lângă blocarea accesului neautorizat, el poate analiza traficul în detaliu, detecta atacuri complexe și opri aplicațiile periculoase. Este ca un portar foarte inteligent care nu doar verifică cine intră, ci și ce aduce cu el și ce face după ce intră.
Exemplu: Compania a instalat un NGFW pentru a detecta și bloca atât virușii obișnuiți, cât și atacurile mai avansate.

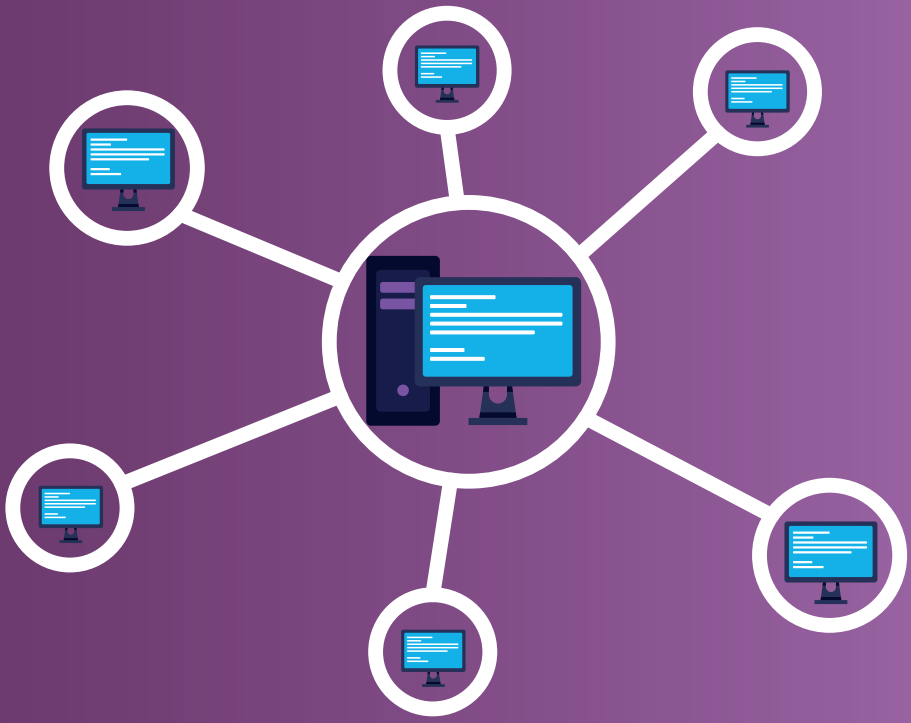
NIS2 (Network and Information Security Directive 2)

Definiție: NIS2 este o lege europeană care cere companiilor să-și protejeze mai bine rețelele și datele pentru a preveni atacurile cibernetice. Este ca o regulă care spune că toată lumea trebuie să aibă lacăte puternice la ușile digitale.
Exemplu: Compania tatălui meu a implementat reguli noi pentru securitate, conform NIS2.

Non-repudiation (Nonrepudiere)

Definiție: nonrepudierea este un concept în securitatea cibernetică care asigură că nimeni nu poate nega faptul că a trimis un mesaj, a făcut o acțiune sau a accesat un sistem. Cu ajutorul semnăturilor digitale sau al altor metode de verificare, se creează dovezi clare despre cine a făcut o anumită activitate. Este ca atunci când primești un pachet și semnezi pentru el – acea semnătură arată că l-ai primit, iar tu nu poți nega acest lucru mai târziu.

Exemplu: Când am trimis un email important semnat digital, am folosit nonrepudierea pentru a dovedi că eu am fost cel care l-a trimis și că mesajul nu a fost modificat.



OAuth (Open Authorization)

Definiție: OAuth este un sistem care permite aplicațiilor să folosească informațiile tale fără să îți ceară parola. Este folosit, de exemplu, când te conectezi la un site cu contul tău de Google sau Facebook.
Exemplu: Am folosit OAuth pentru a mă conecta la o aplicație nouă folosind contul meu de Google.

Obfuscation (Ofuscarea)

Definiție: ofuscarea este procesul de a ascunde informațiile sau codurile într-un format greu de înțeles pentru oameni. Scopul este să protejezi datele sau să ascunzi ce face un program, astfel încât să fie mai dificil pentru hackeri să le descifreze. Este ca și cum ai scrie un mesaj secret folosind un cod complicat pe care doar tu și prietenii tăi îl înțelegeți.
Exemplu: Dezvoltatorii unui joc au folosit ofuscarea pentru a ascunde codul, astfel încât nimeni să nu-l poată modifica sau copia fără permisiune.

Open Redirect

Definiție: Open Redirect este o vulnerabilitate de securitate care apare atunci când un link de pe un site legitim te redirecționează către un alt site, fără să te avertizeze. Hackerii pot folosi această tehnică pentru a te păcăli să accesezi pagini periculoase care arată ca și cum ar fi de încredere. Este ca atunci când cineva îți dă indicații greșite intenționat, ca să te ducă într-un loc periculos.
Exemplu: Am dat clic pe un link de pe un email care părea sigur, dar era un Open Redirect și m-a trimis pe un site fals unde mi-au cerut parola.

OSINT (Open Source Intelligence)

Definiție: OSINT înseamnă să colectezi informații din surse publice, cum ar fi site-uri web sau rețele sociale, pentru a afla mai multe despre o persoană sau o organizație. Este ca atunci când cauți pe Google pentru a găsi detalii despre un subiect sau despre cineva, folosind doar datele pe care le poți vedea fără să încalci reguli.

Exemplu: Poliția a folosit OSINT pentru a găsi indicii despre o persoană dispărută, verificând profilurile de pe rețelele sociale și articolele online.

Patch Management (Gestionarea actualizărilor)

Definiție: patch management este procesul de instalare a actualizărilor pentru software, care repară vulnerabilitățile și îmbunătățesc securitatea. Este ca și cum ai repara o gaură într-un gard pentru a împiedica hoții să intre.
Exemplu: Calculatorul meu îmi cere mereu să instalez actualizările pentru a corecta problemele de securitate.

Password Cracking

Definiție: Password cracking este procesul prin care hackerii încearcă să ghicească sau să spargă parolele pentru a accesa conturi, fișiere sau sisteme. Ei folosesc programe speciale care încearcă mii sau milioane de combinații de litere, cifre și simboluri până găsesc parola corectă. Este ca atunci când cineva încearcă toate combinațiile posibile pentru a descuia un lacăt.
Exemplu: Antivirusul meu a prevenit o încercare de password cracking asupra contului meu.

Password Manager

Definiție: un password manager este o aplicație care te ajută să creezi, să stochezi și să folosești parole puternice pentru toate conturile tale. În loc să ții minte multe parole, trebuie să ții minte doar una singură, pentru aplicație.
Exemplu: Folosesc un password manager ca să nu mai uit parolele conturilor mele.

Penetration Testing

Definiție: testarea de penetrare este un proces prin care experții în securitate încearcă să „atace" un sistem, o rețea sau o aplicație, dar

în mod controlat și cu permisiune, pentru a descoperi punctele slabe. Scopul este să găsească vulnerabilitățile înainte ca hackerii reali să le exploateze. Este ca atunci când verifici lacătele și ferestrele casei tale încercând să vezi dacă cineva ar putea intra fără cheie.
Exemplu: Compania noastră a angajat o echipă de testare de penetrare pentru a descoperi problemele de securitate ale site-ului nostru înainte de lansare.

Pharming

Definiție: pharming este un tip de atac cibernetic în care hackerii modifică setările unui site web sau ale rețelei tale, astfel încât să te redirecționeze către un site fals, chiar dacă ai introdus corect adresa web. Site-ul fals arată ca unul real, dar este creat pentru a fura informații, cum ar fi parolele sau datele cardului tău. Este ca și cum cineva ar schimba indicatoarele rutiere pentru a te conduce la o destinație greșită, fără să-ți dai seama.
Exemplu: Deși am tastat adresa corectă a băncii, un atac pharming m-a dus pe un site fals.

Phishing

Definiție: Phishing este o metodă folosită de hackeri pentru a păcăli oamenii să le ofere informații personale, cum ar fi parolele sau datele cardului de credit. De obicei, acest lucru se face prin emailuri sau mesaje care par să vină de la surse de încredere, dar sunt false. Este ca și cum cineva ar trimite o scrisoare falsă care arată oficială, dar care este menită să te păcălească.
Exemplu: Am primit un email care părea să fie de la banca mea, dar prietenii mi-au spus că era phishing.

Pretexting

Definiție: pretexting este o tehnică folosită de hackeri pentru a păcăli o persoană să ofere informații confidențiale. Atacatorul creează o poveste falsă (un „pretext") și se prezintă ca o persoană de încredere, cum ar fi un angajat al unei companii sau un prieten. Este ca atunci când cineva se dă drept un polițist fals pentru a te convinge să îi dai

informații importante.
Exemplu: Un hacker a folosit pretexting, pretinzând că este de la suport tehnic, ca să-mi ceară parola.

Principiul minimului privilegiu (Least Privilege)

Definiție: principiul minimului privilegiu spune că o persoană sau un program ar trebui să aibă acces doar la informațiile și resursele de care are nevoie pentru a-și face treaba, nimic mai mult. Acest lucru ajută la prevenirea greșelilor și a atacurilor cibernetice, deoarece limitează ce poate face fiecare utilizator sau aplicație. Este ca atunci când le permiți prietenilor să intre doar în camera de zi a casei tale, dar nu și în camerele private.
Exemplu: Angajații noștri au acces doar la fișierele care sunt relevante pentru departamentul lor.

Privitul peste umăr (Shoulder Surfing)

Definiție: este o metodă simplă de a fura informații, cum ar fi parole, uitându-te la ecranul sau tastatura altcuiva.
Exemplu: Am observat pe cineva încercând să facă shoulder surfing în timp ce introduceam parola pe telefon.

Protecția Dispozitivelor (Endpoint Protection)

Definiție: Endpoint protection se referă la măsurile de securitate care protejează calculatoarele, telefoanele sau tabletele conectate la internet împotriva virușilor și atacurilor. Este ca un scut digital care îți protejează dispozitivele.
Exemplu: : La școală, calculatoarele din laborator au un sistem de endpoint protection pentru a opri virușii.

Protocoale nesecurizate

Definiție: protocoalele nesecurizate sunt metode de comunicare pe internet care nu protejează datele transmise între dispozitive. Acest lucru înseamnă că informațiile, cum ar fi parolele sau mesajele, pot fi interceptate și citite de hackeri. Este ca și cum ai trimite o scrisoare fără plic, iar oricine o vede poate citi ce ai scris.
Exemplu: Nu mă conectez la site-uri care folosesc HTTP, deoarece este un protocol nesecurizat.

Purple Team

Definiție: Purple Team este o echipă care combină Red Team (atac) și Blue Team (apărare). Ei lucrează împreună ca să testeze și să îmbunătățească securitatea. Gândește-te la Purple Team ca la o echipă de antrenori care îi ajută pe „atacatori" și „apărători" să devină mai buni împreună.
Exemplu: Purple Team-ul a analizat atacurile simulate și a învățat Blue Team cum să răspundă mai repede data viitoare.

QR Code (Quick Response)

Definiție: un cod QR este un tip special de cod de bare pătrat, care poate fi scanat cu telefonul pentru a accesa rapid informații, cum ar fi un link, un text sau date de contact. Este ca o „ușă magică" digitală care te duce direct la informațiile de care ai nevoie fără să tastezi nimic.
Exemplu: Am scanat un cod QR de pe afișul unui film și am ajuns imediat pe site-ul unde puteam cumpăra bilete.

QR Code Spoofing

Definiție: QR code spoofing este un atac în care un hacker folosește un cod QR fals pentru a te trimite pe un site periculos sau pentru a fura informații. Deși codul arată ca unul legitim, te poate duce într-un loc periculos.
Exemplu: Am verificat de două ori un cod QR înainte să îl scanez, pentru a mă asigura că nu e un atac.

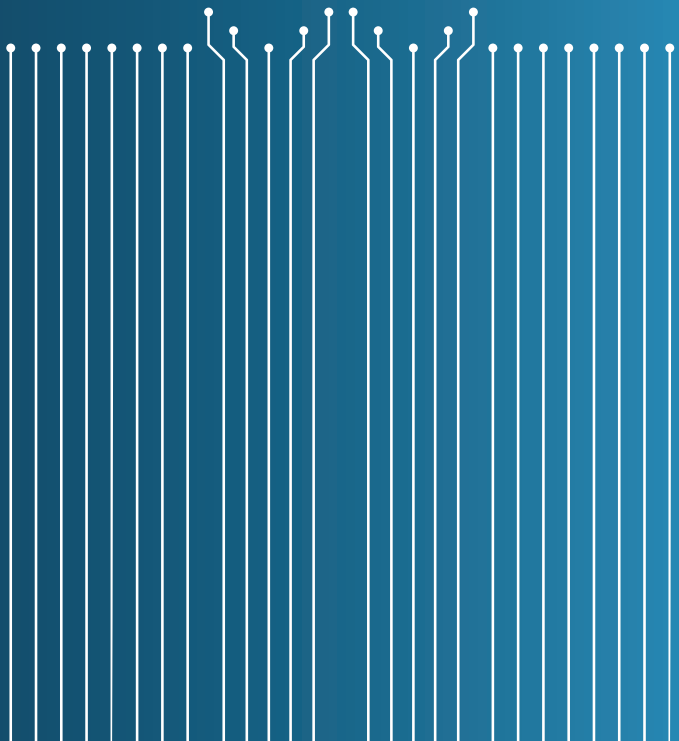
Query Injection

Definiție: Query Injection este un tip de atac cibernetic în care un hacker introduce cod rău intenționat într-un câmp de căutare sau formular de pe un site web. Scopul este să păcălească site-ul să execute comenzi pe care nu ar trebui să le accepte, cum ar fi să dezvăluie informații confidențiale din baza de date. Este ca și cum cineva ar modifica un bilet de tren pentru a călători într-un loc diferit, fără să plătească.
Exemplu: Un atac de tip query injection a fost folosit pentru a obține parolele utilizatorilor unui site.

Quantum Security

Definiție: în securitatea cibernetică, cuvântul "quantum" este folosit pentru a descrie tehnologii bazate pe fizica cuantică, cum ar fi calculatoarele cuantice sau criptografia cuantică. Acestea folosesc proprietățile particulelor extrem de mici (cum ar fi fotonii) pentru a rezolva probleme complexe sau pentru a crea metode de securitate mult mai sigure. Este ca și cum ai folosi „magie științifică" pentru a face comunicațiile aproape imposibil de spart.

Exemplu: Cercetătorii lucrează la criptografia cuantică, care va face mesajele digitale atât de sigure încât hackerii nu le vor putea descifra, nici măcar cu un supercomputer.



RaaS - Ransomware ca Serviciu

Definiție: RaaS este modalitatea în care hackerii creează programe ransomware și le oferă altor persoane pentru a lansa atacuri. Aceștia își împart câștigurile, iar oricine poate folosi ransomware-ul fără să știe să îl creeze. Este ca și cum ai închiria un instrument periculos pentru a face rău altora.
Exemplu: Un atacator fără cunoștințe avansate a folosit RaaS pentru a lansa un atac ransomware și a bloca calculatoarele unei companii.

Ransomware

Definiție: ransomware este un tip de malware care blochează accesul la fișierele tale și îți cere bani (ransom) pentru a le debloca. Este ca și cum cineva ți-ar încuia camera și ți-ar cere bani pentru a-ți da cheia.
Exemplu: Am citit despre un spital care a fost victima unui atac ransomware și nu a mai putut accesa datele pacienților până nu a plătit recompensa cerută de atacatori.

Răspuns la incidente

Definiție: este procesul prin care o echipă gestionează un atac cibernetic sau o problemă de securitate. Ei detectează ce s-a întâmplat, opresc atacul și repară pagubele.
Exemplu: Echipa de răspuns la incidente a lucrat rapid pentru a opri atacul asupra rețelei școlii.

Red Team

Definiție: Red Team este un grup de experți care simulează atacuri cibernetice asupra unei organizații pentru a găsi punctele slabe ale sistemului de securitate. Scopul lor este să îmbunătățească apărarea testând-o. Este ca o echipă de „actori răi" care joacă rolul atacatorilor pentru a ajuta „echipa bună" să devină mai puternică.
Exemplu: Red Team-ul a simulat un atac cibernetic pentru a testa cât de bine răspunde echipa de securitate.

Reducerea riscurilor / Risk Mitigation

Definiție: Reducerea riscurilor este procesul prin care sunt luate măsuri pentru a reduce sau elimina amenințările care pot afecta un sistem sau o organizație. Aceasta poate include utilizarea firewall-urilor, criptarea datelor sau instruirea utilizatorilor. Este ca și cum ai pune plasă la geamuri pentru a preveni pătrunderea insectelor.
Exemplu: Am implementat autentificarea în doi pași ca parte a strategiei de risk mitigation.

Remote Access Trojan (RAT)

Definiție: RAT este un program malițios care le permite hackerilor să acceseze și să controleze calculatorul tău de la distanță, ca și cum ar fi în fața lui.
Exemplu: Am citit că un RAT a fost folosit pentru a spiona computerele unei organizații.

Role-Based Access Control (RBAC)

Definiție: RBAC este o metodă de securitate în care accesul la fișiere sau aplicații este acordat în funcție de rolul utilizatorului, cum ar fi student, profesor sau administrator.
Exemplu: În biblioteca școlii, doar profesorii pot accesa baza de date cu notele elevilor.

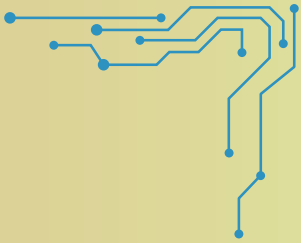
Rootkit

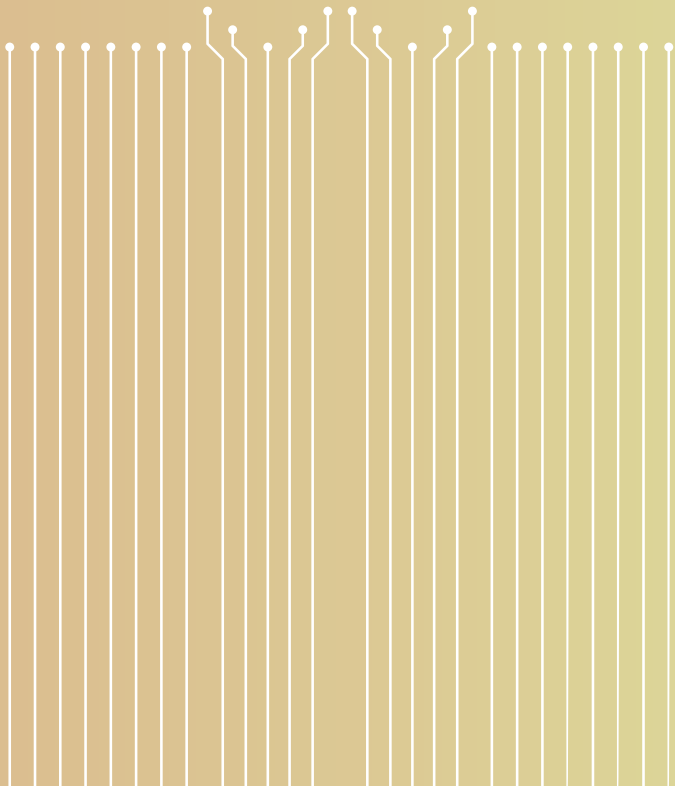
Definiție: Rootkit-ul este un tip de malware care se ascunde adânc în sistemul de operare al calculatorului, făcându-l greu de detectat. Hackerii îl folosesc pentru a prelua controlul complet asupra unui dispozitiv.
Exemplu: Un rootkit poate rămâne ascuns mult timp, așa că antivirusul meu verifică constant sistemul.

Rogue Access Point

Definiție: Un rogue access point este un dispozitiv WiFi care nu este autorizat și care poate fi instalat de hackeri sau chiar din greșeală. Acesta poate fi folosit pentru a intercepta datele utilizatorilor care se conectează la el. Este ca un „pod fals" care te duce într-o direcție greșită.

Exemplu: Hackerii au instalat un rogue access point într-o cafenea pentru a fura datele celor care s-au conectat la rețeaua WiFi.





Sandboxing

Definiție: Sandboxing-ul este o metodă de securitate prin care un program sau fișier este izolat într-un mediu controlat pentru a verifica dacă este sigur. Este ca o cutie de nisip unde poți testa ceva fără riscul de a strica totul.
Exemplu: Am folosit sandboxing pentru a testa un fișier descărcat de pe internet înainte să îl deschid.

Segmentarea rețelei

Definiție: segmentarea rețelei înseamnă să împarți o rețea mare în părți mai mici, astfel încât un atac să nu poată afecta toate zonele. Este ca și cum ai avea mai multe camere separate cu uși închise într-o casă.
Exemplu: Segmentarea rețelei școlii înseamnă că laboratoarele și birourile profesorilor sunt separate digital.

Semnătura virusului

Definiție: o semnătură de virus este un cod unic folosit de antivirusuri pentru a identifica un virus specific. Este ca o amprentă digitală a virusului.
Exemplu: Antivirusul meu a găsit un fișier cu o semnătură care corespundea unui virus cunoscut.

Server

Definiție: Un server este un calculator special sau un program care oferă servicii altor calculatoare sau dispozitive conectate la o rețea. El poate trimite fișiere, stoca date sau găzdui site-uri web. Este ca o bibliotecă mare unde poți merge să împrumuți cărți sau să obții informații, dar în loc de cărți, serverul oferă fișiere și servicii digitale.
Exemplu: Când accesez un site web, calculatorul meu cere informații de la un server care găzduiește acel site.

Session Hijacking

Definiție: Este un atac în care hackerii fură informațiile legate de o sesiune activă a unui utilizator pe un site web (cum ar fi un cookie de autentificare). După ce obțin aceste informații, ei pot accesa contul victimei ca și cum ar fi utilizatorul autentic. Este ca și cum cineva ar lua locul tău într-o coadă după ce ai obținut un bilet de acces.
Exemplu: Un atac de session hijacking mi-a compromis contul de pe un site nesecurizat.

Securitate Wireless

Definiție: : securitatea wireless înseamnă protejarea rețelelor WiFi împotriva accesului neautorizat și a atacurilor cibernetice. Aceasta include folosirea parolelor puternice, criptarea datelor și alte măsuri care să împiedice hackerii să se conecteze la rețea sau să fure informații. Este ca o poartă cu lacăt pentru rețeaua ta, care permite doar persoanelor autorizate să intre.
Exemplu: Am setat o parolă puternică pentru rețeaua mea WiFi pentru a crește securitatea.

Securitate cibernetică (Cybersecurity)

Definiție: Securitatea cibernetică înseamnă să protejezi calculatoarele, rețelele și informațiile de hackeri sau programe periculoase. Este ca o combinație de lacăte digitale și paznici care au grijă ca totul să fie în siguranță. Implică folosirea unui antivirus, a parolelor puternice și a altor măsuri care te ajută să te protejezi în lumea online.
Exemplu: Profesorul meu ne-a explicat cum să fim în siguranță online folosind reguli de securitate cibernetică.

Securitatea aplicațiilor

Definiție: securitatea aplicațiilor înseamnă protejarea programelor și aplicațiilor împotriva atacurilor, astfel încât utilizatorii să fie în siguranță atunci când le folosesc. Aceasta include verificarea codului, aplicarea actualizărilor și utilizarea unor măsuri de protecție pentru a

preveni ca hackerii să exploateze punctele slabe ale aplicațiilor. Este ca și cum ai pune lacăte și alarme pe fiecare ușă și fereastră a unei clădiri pentru a te asigura că nimeni nu poate intra fără permisiune.
Exemplu: Dezvoltatorii noștri testează fiecare aplicație pentru a se asigura că este protejată.

Securitatea infrastructurii critice

Definiție: este protecția rețelelor și sistemelor care sunt esențiale pentru societate, cum ar fi energia electrică, apa, spitalele și transportul. Dacă acestea sunt atacate de hackeri, pot apărea probleme mari pentru toată lumea. De aceea, aceste sisteme trebuie să fie protejate foarte bine.
Exemplu: Sistemele care controlează alimentarea cu energie electrică sunt protejate împotriva atacurilor pentru a preveni penele de curente.

Securitatea rețelei

Definiție: securitatea rețelei înseamnă să protejezi rețeaua de calculatoare împotriva accesului neautorizat și a atacurilor. Este ca un zid digital care apără rețeaua.
Exemplu: Routerul meu folosește o parolă puternică pentru securitatea rețelei.

SIEM (Security Information and Event Management)

Definiție: SIEM este o tehnologie folosită de companii pentru a monitoriza activitățile din rețea și a detecta problemele de securitate. Este ca o cameră de supraveghere digitală care te anunță imediat dacă ceva pare suspect.
Exemplu: Compania folosește SIEM pentru a detecta activități neobișnuite în rețea.

Smishing

Definiție: Smishing este un tip de atac cibernetic similar cu phishing-ul, dar realizat prin mesaje SMS. Hackerii trimit mesaje care par să vină de la surse de încredere, cum ar fi bănci sau companii, cerând să accesezi un link sau să oferi informații personale. Este ca și cum ai primi o scrisoare falsă în cutia poștală, care te păcălește să oferi detalii importante.
Exemplu: Am primit un SMS care pretindea că este de la un curier, cerându-mi să accesez un link pentru a confirma livrarea – era un atac de smishing.

Spam

Definiție: Spam-ul este o serie de mesaje nedorite sau nesolicitate, de obicei trimise în masă. Poate fi enervant, iar uneori poate conține linkuri periculoase.
Exemplu: Am primit o mulțime de emailuri spam care îmi promiteau câștiguri mari, dar le-am șters.

SQL Injection

Definiție: SQL Injection este un tip de atac cibernetic în care hackerii introduc coduri rău intenționate într-un formular online sau într-un câmp de căutare. Scopul este să păcălească baza de date a site-ului pentru a dezvălui informații sensibile sau pentru a permite acces neautorizat. Este ca și cum cineva ar folosi o frază secretă pentru a deschide o ușă care nu ar trebui să fie deschisă.
Exemplu: Un hacker a folosit SQL injection pentru a accesa datele utilizatorilor unui site web nesecurizat.

Spyware

Definiție: Spyware este un tip de program care se instalează pe calculatorul sau telefonul tău fără să știi și urmărește ce faci. Poate colecta parole, date bancare sau alte informații personale.
Exemplu: Am descărcat un joc de pe un site necunoscut, iar antivirusul meu a detectat că avea spyware.

Spyware Detector (Detector de spyware)

Definiție: este un program care identifică și elimină spyware-ul de pe calculatorul sau telefonul tău. Este ca un câine de pază care detectează spionii ascunși.
Exemplu: Am instalat un spyware detector care m-a ajutat să șterg un program periculos.

SSL/TLS (Secure Socket Layer/ Transport Layer Security)

Definiție: SSL și TLS sunt protocoale care securizează conexiunile dintre calculatorul tău și un site web. Dacă vezi un lacăt lângă adresa unui site, înseamnă că folosește aceste protocoale pentru a proteja datele tale.
Exemplu: Când fac cumpărături online, mă asigur că site-ul folosește SSL/TLS pentru a-mi proteja informațiile.

Steganografie

Definiție: steganografia este arta de a ascunde informații într-o imagine, fișier audio sau alt tip de fișier, astfel încât să nu fie detectate. Este ca o scrisoare secretă ascunsă într-un desen.
Exemplu: Hackerii au ascuns un mesaj periculos într-o fotografie folosind steganografie.

Suprafața de atac (Attack Surface)

Definiție: suprafața de atac reprezintă toate punctele prin care un hacker ar putea încerca să intre într-un calculator sau într-o rețea. De exemplu, dacă folosești aplicații vechi, cu erori, sau nu ai un antivirus, le dai mai multe „uși deschise" hackerilor. Cu cât ai mai puține vulnerabilități, cu atât este mai greu să fii atacat.
Exemplu: Am închis aplicațiile pe care nu le mai folosesc și am instalat actualizări, ca să reduc suprafața de atac a calculatorului meu.

Sistem de rezervă (Failover System)

Definiție: Un failover system este un sistem de rezervă care intră automat în funcțiune dacă sistemul principal se defectează. Scopul lui este să mențină funcționarea continuă a unui site, a unei aplicații sau a unui serviciu, fără întreruperi. Este ca atunci când ai o lanternă cu baterii de rezervă: dacă primele baterii se descarcă, cele de rezervă se activează imediat.

Exemplu: Sistemul nostru de email are un failover care preia funcționarea în cazul unei probleme tehnice.

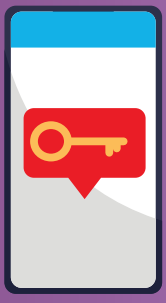
Tokenizare

Definiție: tokenizarea este o metodă de securitate prin care informațiile sensibile, cum ar fi un număr de card de credit, sunt înlocuite cu un cod unic numit „token." Acest token nu conține datele reale și nu poate fi folosit în afara sistemului care l-a creat. Este ca atunci când primești un jeton la o garderobă cand îți lași hainele – jetonul reprezintă hainele tale, dar nu spune nimic despre ele.
Exemplu: Când plătesc online, datele cardului meu sunt tokenizate pentru a fi în siguranță.

Threat Hunting

Definiție: este un proces proactiv în care specialiștii caută semne de atacuri cibernetice în rețelele unei organizații, chiar înainte ca acestea să aibă loc.
Exemplu: Echipa noastră de securitate face threat hunting pentru a preveni atacurile.


Username
Login



URL (Uniform Resource Locator)

Definiție: URL este adresa unui site web sau a unei resurse online. Este ceea ce scrii în bara de adrese a browserului pentru a accesa un site. URL-ul indică unde se află site-ul pe internet, la fel cum o adresă poștală arată unde este o casă.
Exemplu: Adresa URL a site-ului Asociației Women4Cyber România este www.women4cyber.ro .

URL Spoofing

Definiție: este un atac în care un hacker creează un link fals care pare să fie legitim, dar te redirecționează către un site periculos. Acest site poate arăta ca unul real, cum ar fi banca ta, dar este folosit pentru a fura informații personale, cum ar fi parole sau detalii despre carduri. Este ca atunci când cineva îți dă o hartă falsă care te conduce într-un loc greșit.
Exemplu: Am verificat linkul din email înainte de a da clic, ca să evit un atac de tip URL spoofing.

User Account Control (UAC)

Definiție: UAC este o funcție de securitate în Windows care îți cere permisiunea înainte de a face modificări importante pe calculator. Este ca atunci când un portar te întreabă dacă ești sigur că vrei să intri într-o zonă restricționată, pentru a preveni accesul neautorizat.
Exemplu: Calculatorul meu m-a întrebat prin UAC dacă sunt sigur că vreau să instalez un program nou.

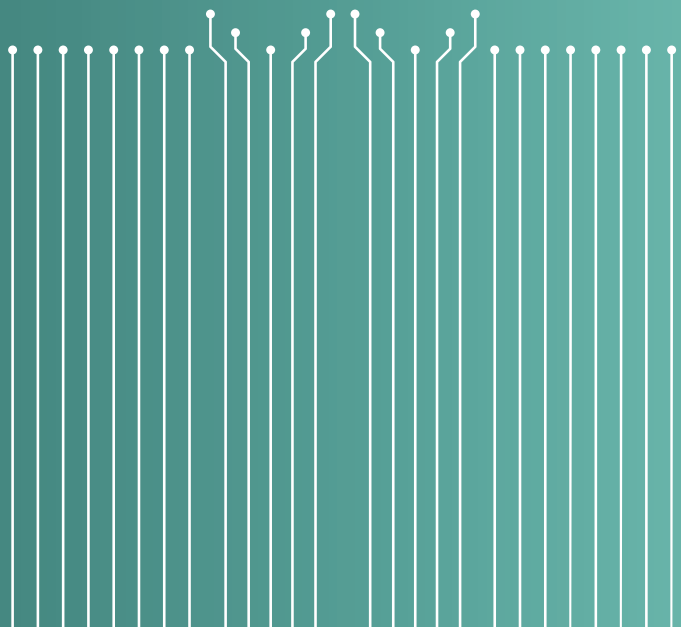
User Behavior Analytics (UBA - Analiza comportamentului utilizatorilor)

Definiție: UBA este o tehnologie care monitorizează ce fac utilizatorii pe un sistem sau o rețea, pentru a detecta comportamente

neobișnuite. Dacă cineva încearcă să acceseze fișiere importante la o oră ciudată sau face ceva ce nu ar trebui, UBA poate semnala acest lucru pentru a preveni un atac. Este ca un profesor care observă dacă un elev se comportă diferit și întreabă ce s-a întâmplat.
Exemplu: Sistemul UBA a detectat că un cont de utilizator descărca multe fișiere neobișnuite, ceea ce ar putea însemna un atac cibernetic.

Unified Threat Management (UTM)

Definiție: UTM este un sistem care combină mai multe instrumente de securitate într-un singur dispozitiv sau software, cum ar fi firewall, antivirus, filtrare web și detectarea atacurilor. Este ca un „super-paznic" care protejează rețeaua ta de toate tipurile de pericole.
Exemplu: Compania folosește un dispozitiv UTM pentru a proteja rețeaua de viruși, atacuri cibernetice și site-uri periculoase.



V

Vector de atac

Definiție: un vector de atac este calea prin care hackerii pot pătrunde într-un sistem sau rețea. Poate fi un email fals, o aplicație nesigură sau chiar un stick USB infectat. Este ca o cale de acces pe care un hoț o folosește – poate fi o ușă deschisă, o fereastră sau chiar o gaură mică în gard.
Exemplu: Un hacker a folosit un vector de atac printr-un email de phishing pentru a accesa rețeaua companiei.

Verificarea integrității

Definiție: este procesul de verificare a faptului că un fișier sau un sistem nu a fost modificat fără autorizație. Este ca atunci când verifici dacă o scrisoare primită este exact așa cum a fost trimisă, fără să fie deschisă sau schimbată pe drum.
Exemplu: Sistemul meu de backup face o verificare a integrității pentru fiecare fișier salvat.

Virtual Private Cloud (VPC)

Definiție: Un Virtual Private Cloud (VPC) este un spațiu securizat creat într-un cloud public (cum ar fi Amazon Web Services sau Google Cloud), care funcționează ca o rețea privată. Acesta permite companiilor să își stocheze datele și aplicațiile într-un mediu sigur, izolat de restul internetului. Este ca și cum ai avea propriul apartament într-o clădire mare, cu uși încuiate pe care doar tu le poți deschide.
Definiție: Compania noastră folosește un VPC pentru a păstra informațiile clienților în siguranță, deși este găzduit pe un cloud public.

Virus

Definiție: un virus informatic este un program rău intenționat creat pentru a infecta calculatoare sau alte dispozitive. El se răspândește

de la un fișier la altul, uneori chiar de la un calculator la altul și poate cauza probleme cum ar fi ștergerea fișierelor, încetinirea sistemului sau chiar distrugerea datelor. Este ca un virus real care se răspândește între oameni, dar acesta „infectează" calculatoare.
Definiție: Am descărcat un fișier de pe un site nesigur, iar acesta conținea un virus care mi-a blocat calculatorul.

Voice Over IP (VoIP)

Definiție: VoIP este o tehnologie care permite oamenilor să facă apeluri telefonice folosind internetul în loc de liniile telefonice tradiționale. Practic, vocea ta este transformată în semnale digitale care sunt trimise prin rețea, făcând apelurile mai rapide și mai ieftine. Este ca și cum ai folosi un walkie-talkie, dar cu ajutorul internetului.
Exemplu: Am mutat aplicația noastră într-un VPC pentru a proteja mai bine datele utilizatorilor.

Voice Phishing (Vishing)

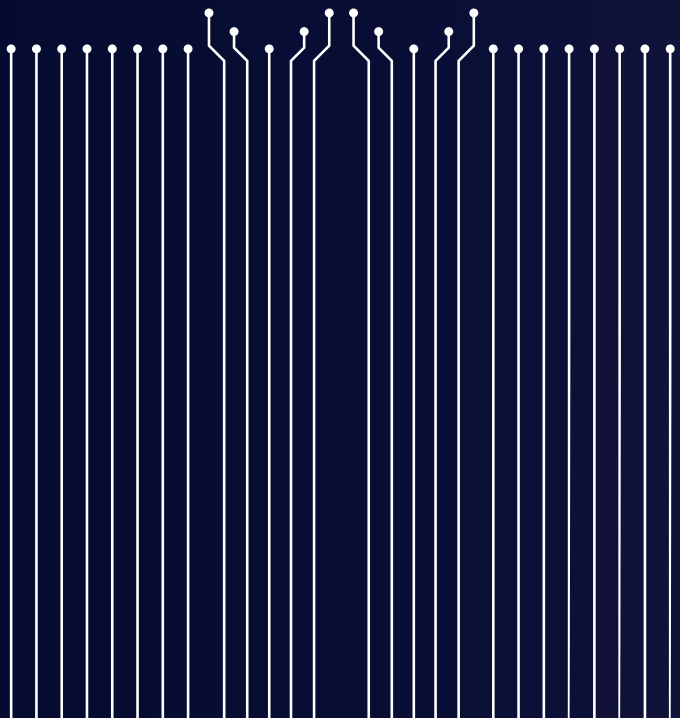
Definiție: Vishing este un tip de atac cibernetic în care hackerii încearcă să păcălească oamenii prin apeluri telefonice. Ei pretind că sunt de la o bancă, un serviciu de suport sau o altă organizație de încredere și cer informații confidențiale, cum ar fi parole, coduri PIN sau detalii ale cardului de credit. Este ca și cum cineva ar suna și s-ar da drept polițist fals pentru a te face să-i dai cheia casei.
Exemplu: Am primit un apel de la cineva care pretindea că este de la bancă, dar încerca să mă păcălească.

VPN (Virtual Private Network)

Definiție: un VPN este o conexiune sigură care ascunde locația și activitatea ta pe internet, protejându-te de hackeri. Este ca un tunel invizibil între tine și site-urile pe care le vizitezi.
Exemplu: Folosesc un VPN pentru a mă conecta la internet când folosesc rețele WiFi publice.

Vulnerability Disclosure

Definiție: Vulnerability disclosure este procesul prin care cineva descoperă și raportează o problemă de securitate (o vulnerabilitate) dintr-un sistem, aplicație sau rețea. Această raportare ajută dezvoltatorii să repare problema înainte ca hackerii să o exploateze. Este ca atunci când găsești o gaură în gardul școlii și le spui profesorilor pentru ca ei să o repare înainte să intre cineva fără permisiune.
Exemplu: Un cercetător a descoperit o vulnerabilitate într-o aplicație și a trimis un raport detaliat companiei pentru ca aceasta să poată rezolva problema.



Virtual Private Cloud

Watering Hole Attack

Definiție: un Watering Hole Attack este un tip de atac cibernetic în care hackerii infectează un site pe care victimele obișnuiesc să îl viziteze des. Când acestea accesează site-ul, dispozitivele lor sunt infectate cu malware. Este ca și cum cineva ar otrăvi un loc unde animalele vin să bea apă, știind că vor ajunge acolo.
Exemplu: Hackerii au infectat un site popular cu un watering hole attack pentru a viza utilizatorii.

Web Application Firewall (WAF)

Definiție: un WAF este un tip special de firewall care protejează aplicațiile web de atacuri cibernetice. Acesta funcționează monitorizând și filtrând traficul care vine către și pleacă de la aplicația web, oprind atacuri precum SQL Injection, Cross-Site Scripting (XSS) sau DDoS. Este ca un portar digital care verifică fiecare persoană înainte să intre într-o clădire, asigurându-se că nimeni nu are intenții rele.
Exemplu: Magazinul online al companiei mele folosește un WAF pentru a bloca atacurile care încearcă să fure datele cardurilor de credit ale clienților.

Web Scraping

Definiție: Web scraping este procesul prin care un program colectează automat informații de pe site-uri web, cum ar fi texte, imagini sau prețuri. Aceasta poate fi folosită pentru lucruri utile, cum ar fi compararea prețurilor, dar uneori este făcută fără permisiune și poate încălca regulile unui site. Este ca și cum ai copia toate informațiile de pe o pagină dintr-o revistă pentru a le folosi mai târziu.
Exemplu: O companie de marketing a folosit web scraping pentru a colecta informații despre produse.

WiFi Sniffing

Definiție: WiFi sniffing este o tehnică folosită de hackeri pentru a intercepta datele care circulă pe o rețea WiFi. Ei pot urmări traficul de internet al utilizatorilor, încercând să fure informații precum parole sau date personale. Este ca și cum cineva ar asculta conversațiile dintre tine și prietenii tăi fără să-ți dai seama.
Exemplu: Mă conectez doar la rețele WiFi securizate pentru a evita atacurile de tip sniffing.

Wireless Intrusion Prevention System (WIPS)

Definiție: WIPS este un sistem de securitate care monitorizează rețelele WiFi pentru a detecta și opri accesul neautorizat sau atacurile periculoase. Este ca un gardian digital care veghează asupra rețelei tale wireless și alertează imediat dacă cineva încearcă să se conecteze fără permisiune.
Exemplu: Compania folosește WIPS pentru a preveni accesul neautorizat la rețeaua WiFi.

Worm

Definiție: un worm este un tip de program rău intenționat (malware) care se răspândește singur de la un calculator la altul, fără să aibă nevoie de ajutorul utilizatorilor. El se înmulțește automat și poate provoca multe probleme, cum ar fi încetinirea rețelei sau blocarea calculatoarelor. Este ca un vierme real care sapă tunele printr-un măr, distrugându-l complet.
Exemplu: Un worm s-a răspândit prin rețeaua școlii, dar antivirusul a oprit infectarea.

XDR (Extended Detection and Response)

Definiție: XDR este o tehnologie avansată de securitate care combină date din mai multe surse, cum ar fi calculatoare, rețele și servere, pentru a detecta și răspunde mai rapid la atacuri cibernetice. Este ca o echipă de detectivi care lucrează împreună, adunând informații din diferite locuri pentru a rezolva un caz mai repede și mai eficient.
Exemplu: Folosim XDR pentru a avea o imagine completă a amenințărilor cibernetice din rețea.

XML Injection

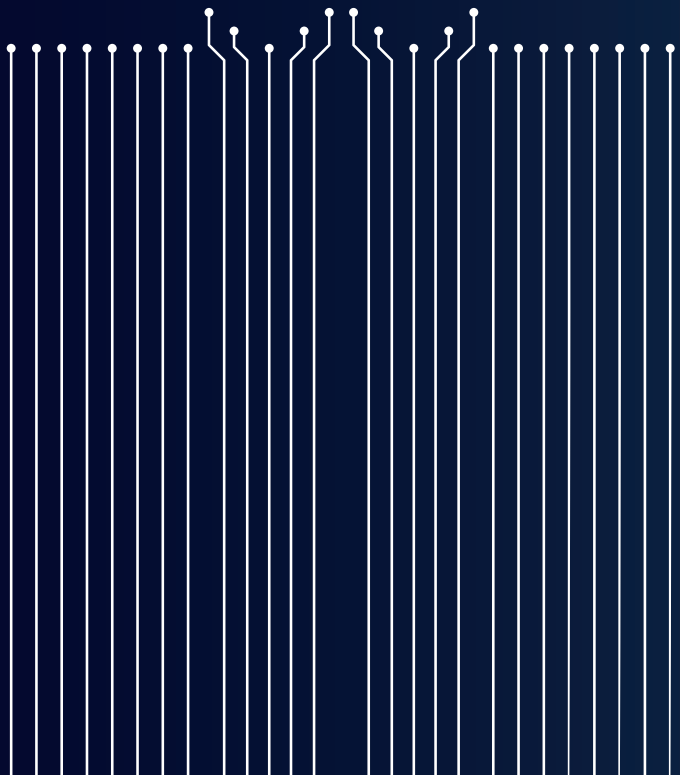
Definiție: XML Injection este un atac în care un hacker introduce cod XML malițios într-un câmp de input al unei aplicații pentru a manipula sistemul și a obține acces neautorizat la date. Este ca și cum cineva ar adăuga comenzi suplimentare într-o listă de sarcini pe care o trimiți colegului tău.
Exemplu: Un atac de XML Injection a permis unui hacker să acceseze baza de date a unei aplicații, modificând cererile transmise serverului.

XSS (Cross-Site Scripting)

Definiție: XSS este un tip de atac cibernetic în care un hacker introduce cod rău intenționat într-un site web. Acest cod este rulat de utilizatorii care vizitează site-ul, fără să știe, și poate fura informații sensibile, cum ar fi datele de autentificare sau parolele. Este ca și cum cineva ar ascunde o scrisoare falsă în cutia ta poștală, care pare să fie de la cineva de încredere.
Exemplu: Un atac XSS a fost folosit pentru a afișa mesaje rău intenționate pe un forum, care furau informațiile de conectare ale utilizatorilor.

YouTube Phishing

Definiție: YouTube phishing este un atac în care hackerii trimit linkuri false prin comentarii sau mesaje private pe YouTube pentru a fura datele utilizatorilor.
Exemplu: Un hacker mi-a trimis un link fals pe YouTube care părea să fie un concurs, dar era phishing.



Z

Zero-Day Exploit

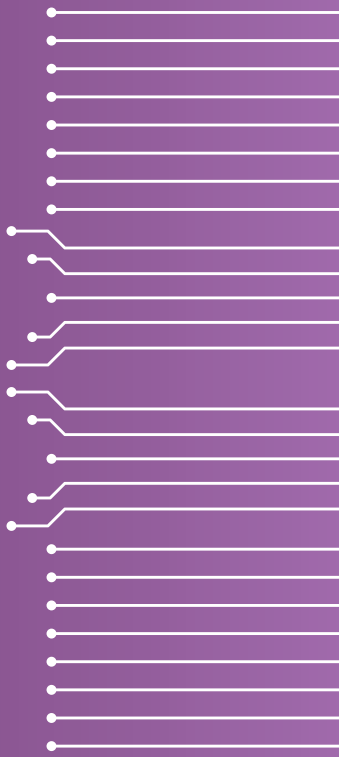
Definiție: un Zero-Day Exploit este o vulnerabilitate necunoscută dintr-un program sau sistem, pe care hackerii o descoperă și o folosesc înainte ca dezvoltatorii să aibă timp să o repare. Este ca și cum cineva ar găsi o ușă secretă într-o casă despre care nimeni nu știa și ar intra fără să fie observat.
Exemplu: Un hacker a folosit un Zero-Day Exploit pentru a prelua controlul unui joc popular înainte ca echipa să repare problema.

Zero Trust Security (Securitate de tip Zero Trust)

Definiție: Zero Trust este un model de securitate care presupune că nimeni din rețea nu este de încredere implicit și verifică constant accesul fiecărui utilizator sau dispozitiv. Se aseamănă cu o fortăreață în care fiecare persoană trebuie să arate un permis special de fiecare dată când vrea să intre, chiar dacă este deja cunoscută.
Exemplu: Organizația noastră implementează Zero Trust Security pentru a proteja datele sensibile.

Zombie Network (Rețea zombie)

Definiție: este o rețea formată din calculatoare infectate (zombie) care sunt controlate de la distanță de un hacker. Acestea sunt utilizate pentru atacuri masive, cum ar fi cele de tip DDoS. Se aseamănă cu o armată de roboți controlați de la distanță, care fac ceea ce le spune hackerul.
Exemplu: Un atac DDoS a fost lansat folosind o rețea zombie formată din mii de calculatoare infectate.



Q&A
Și
FUN FACTS

CyberInes Q&A

Știai că prima Red Team oficială a fost formată în anii '70 în armata SUA, ca să testeze siguranța bazelor militare? De atunci, conceptul a fost preluat de companii private și s-a transformat într-o adevărată disciplină de securitate cibernetică.

Culoarea Purple din Purple Team simbolizează colaborarea: roșul (Red Team) combinat cu albastrul (Blue Team). Purple Team nu este o echipă separată, ci o metodă prin care atacatorii și apărătorii lucrează împreună ca să învețe mai repede.

Știai că există competiții internaționale de tip Capture The Flag (CTF) în care echipele Red, Blue și Purple se întrec să atace și să apere sisteme virtuale? Mulți experți și-au început cariera participând la astfel de concursuri.

Știai că prima rețea considerată "străbunica" internetului de azi se numea ARPANET? A fost creată în 1969 ca să lege computerele unor universități americane, iar primul mesaj transmis a fost doar „LO" – rețeaua a căzut înainte să termine cuvântul "LOGIN"!

Știai că un firewall poate fi hardware sau software? Firewall-ul hardware e un aparat special conectat la rețea, iar cel software este un program instalat pe calculator.

Știai că termenul "cookie" în informatică vine de la "magic cookie", un mic pachet de date folosit pentru identificare? Nu are nicio legătură cu prăjiturile adevărate!

Știai că în multe școli din lume se organizează cursuri speciale despre cum să creezi parole sigure și cum să recunoști phishingul? Securitatea cibernetică începe de mic!

CyberInes și Misterul Camerei Video

CyberInes naviga liniștită pe internet când a observat ceva ciudat: camera video de pe birou clipea, deși nu o pornise. A tresărit și a pus mâna pe telefon.

— ErinJoy, vino repede! Cred că cineva încearcă să-mi acceseze camera!

În câteva minute, ErinJoy și HackyFrancy au intrat în cameră cu laptopurile pregătite.

— Să vedem... — a spus HackyFrancy, conectând cablul. — Uite! O adresă IP suspectă încearcă să trimită imagini către un server străin.

— Închide conexiunea imediat! — a spus ErinJoy hotărâtă.

CyberInes s-a uitat speriată la cameră.

— Cum e posibil să intre așa ușor?

— E simplu, Ines — i-a explicat ErinJoy calm. — Camera avea parola din fabrică, „admin". Niciun dispozitiv nu trebuie lăsat fără parolă sigură.

— Îmi pare rău că nu am verificat mai devreme... — a spus Ines.

— Important e că acum ai învățat — a zâmbit HackyFrancy. Schimbăm parola, activăm firewall-ul camerei și totul va fi bine!

După ce au securizat dispozitivul, CyberInes a respirat ușurată. A promis că de acum înainte nu va lăsa niciun gadget fără protecție.


PAROLA MEA
123456
Password:

Q&A
Și
FUN FACTS

HackyFrancy Fun Fact

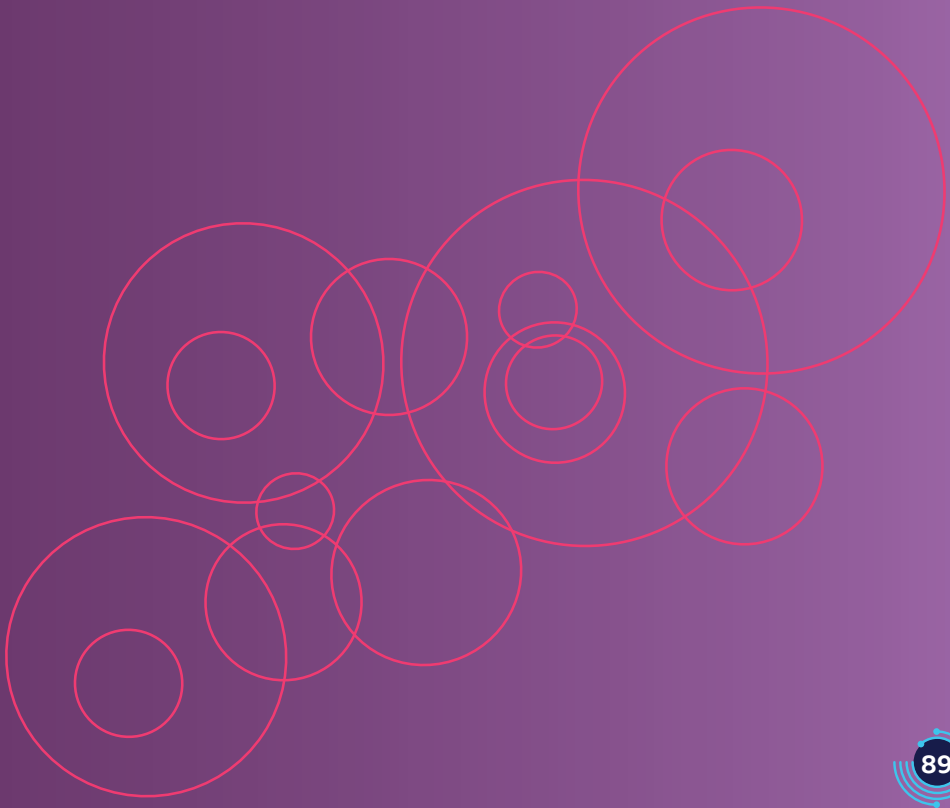
Există hackeri etici care câștigă bani ajutând companiile să găsească vulnerabilități. Se numește bug bounty, iar unii tineri experți au câștigat sute de mii de dolari descoperind probleme de securitate în aplicații cunoscute!

În 2016, un atac DDoS uriaș a blocat accesul la mari site-uri ca Twitter și Netflix. A fost cauzat de mii de camere video infectate cu malware care au format o rețea de atac numită Mirai Botnet.

În 1999, a apărut primul virus care s-a răspândit prin email – se numea Melissa. Atât de mulți oameni au deschis fișierul infectat încât unele servere de email au fost complet blocate.

Cel mai mare atac de tip phishing din istorie a vizat milioane de conturi Google. Google a reușit să blocheze campania în doar câteva ore datorită sistemelor automate de protecție.

Există un virus numit Stuxnet care a fost descoperit în 2010 și a afectat echipamente industriale reale, nu doar computere. Este considerat unul dintre cele mai sofisticate atacuri cibernetice.



HackyFrancy și Aplicația Fantomă

Într-o după-amiază ploioasă, HackyFrancy se plimba prin aplicațiile telefonului când a observat ceva ciudat. O aplicație cu nume bizar - „SuperFlashBank++" - era instalată, deși ea nu-și amintea s-o fi descărcat.

— Hm... foarte ciudat, n-am instalat eu așa ceva! - a spus Francy, încruntându-se.

A apăsat pe iconiță, dar aplicația a cerut imediat datele cardului bancar.

— Asta miroase a capcană! - a zis ea și a chemat-o repede pe CyberInes.

— Ines, ai pățit vreodată să ți se instaleze ceva fără să vrei?

— Da! Când am descărcat un joc gratuit de pe un site dubios... - a răspuns Ines rușinată.

HackyFrancy a conectat telefonul la laptopul ei și a început investigația.

— Exact ce bănuiam! Aplicația nu vine din magazinul oficial și a fost instalată printr-un fișier .apk de pe un site necunoscut. În plus, trimite date către un server din altă țară.

— Doamne! Dar dacă aș fi introdus datele cardului? - s-a speriat Ines.

— Ți-ar fi golit contul în câteva minute. De aceea trebuie să instalăm aplicații doar din magazine oficiale și să nu oferim niciodată date bancare dacă ceva pare dubios.

CyberInes a dat din cap, iar HackyFrancy a continuat:

— Și uite încă un sfat: activează autentificarea cu doi pași pe contul tău bancar. Dacă cineva îți află parola, tot nu va putea face nimic

fără codul de pe telefon.
Au șters aplicația fantomă și au instalat un antivirus pentru telefon.

— Mulțumesc, Francy! - a spus Ines ușurată.

— Cu plăcere! - a zâmbit HackyFrancy. - E mai bine să fim curioase, dar și atente. Tehnologia e grozavă, dacă o folosim în siguranță!

Q&A
Și
FUN FACTS

ErinJoy Fun Fact

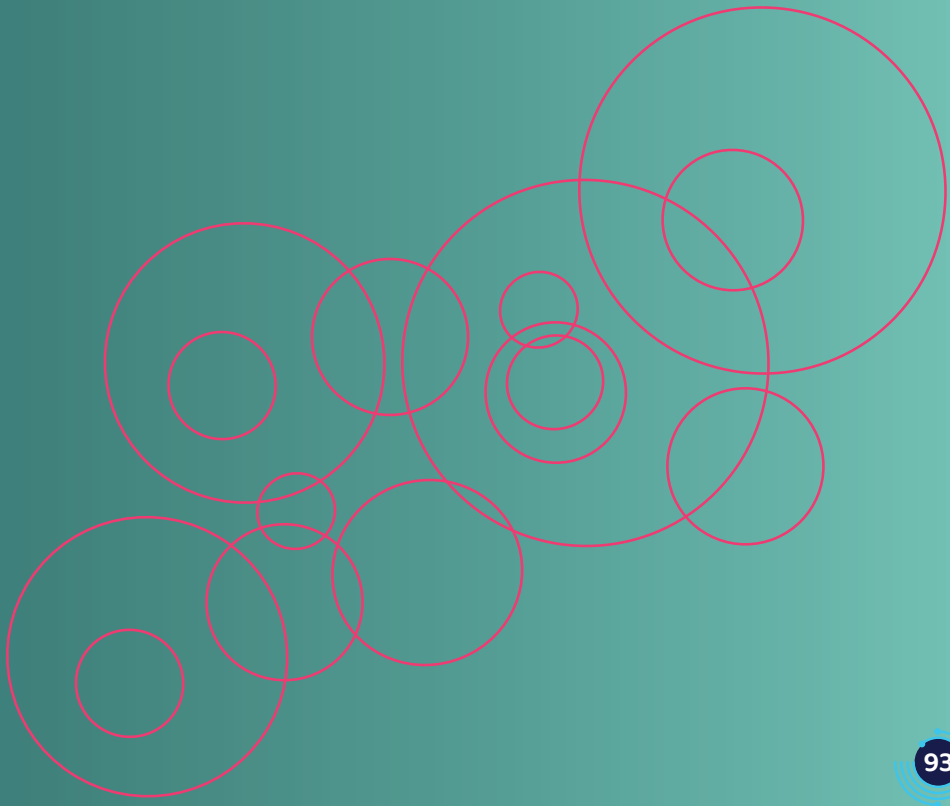
Știai că parola cea mai folosită în lume rămâne „123456”? Specialiștii recomandă parole lungi și unice, dar mulți oameni încă preferă combinații ușor de ghicit. Tocmai de aceea atacatorii le pot sparge în câteva secunde.

Green Team este mai puțin cunoscută, dar extrem de importantă: ei se asigură că aplicațiile sunt proiectate securizat de la început, ca să fie mai greu de spart. Este ca și cum ai construi o casă cu uși blindate încă din prima zi!

Emoji-urile au apărut prima dată în Japonia în anii ’90 și au devenit populare în toată lumea. Astăzi, există mii de emoji, inclusiv cu teme de securitate digitală, cum ar fi 🔒 și 🛡️.

Prima parolă computerizată a fost inventată în anii '60 de un cercetător care lucra la MIT. El a vrut să împiedice colegii să îi deschidă fișierele fără permisiune.

Cuvântul "spam" a devenit popular datorită unui sketch comic cu Monty Python, unde personajele tot repetau "spam" până ce nimeni nu mai putea vorbi. Așa apar și mesajele nedorite: mereu, mereu, mereu.



ErinJoy și Parola Invizibilă

Era târziu seara, iar ErinJoy lucra la un proiect despre siguranța conturilor online. Dintr-odată, un mesaj pop-up a apărut pe ecran: „Parola ta trebuie schimbată imediat!"

— Asta pare suspect... - a murmurat ErinJoy, închizând fereastra cu un click hotărât.

A doua zi, le-a povestit totul prietenelor ei.

— Ai făcut bine că nu ai dat clic pe link - a spus HackyFrancy. Era o tentativă de phishing!

— Ce ai de gând să faci acum? - a întrebat CyberInes.

— Vreau să-mi creez o parolă invizibilă, adică atât de sigură încât nimeni să nu o poată ghici! - a răspuns ErinJoy cu un zâmbet.

S-au așezat toate trei în jurul tabletei și au început să combine idei: un cuvânt preferat, un număr special și un simbol surpriză.

— Ce părere aveți de „Siriu$Planet92!"? - a întrebat ErinJoy.

— Perfect! - au spus fetele în cor.

În seara aceea, ErinJoy a salvat parola în managerul ei digital și a adormit liniștită, știind că nimeni nu avea să o descopere.

Fraga Ţariuc **Alex Ricobon**

CyberDict FOR KIDS

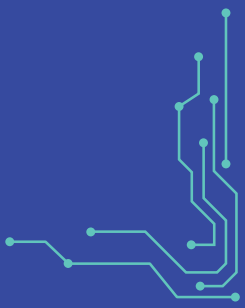
Illustrations

Alexandra Rotariu

București,
2025

Welcome to the fascinating world of cybersecurity - or "cyber," as we like to call it, because it sounds cooler!

This is the **Cyber Dictionary**, specially created for children **aged 8 to 14** who want to learn how to stay safe online and better understand the digital world we live in.
It's a friendly guide, full of simple explanations and helpful examples, where you'll learn alongside three brave and super-smart friends: **CyberInes, ErinJoy,** and **HackyFrancy**. They will accompany you throughout this journey and show you how to become a true Cyber Expert, step by step.
This dictionary was carefully created by the **Women4Cyber Romania Association**, in collaboration with **D3Cyber**, to bring technology closer to children – in a fun, interactive, and easy-to-understand way.



What will you find in this dictionary?

- Clear and short definitions, in words you can understand
- Fun facts about the internet, technology, and online safety
- Useful tips and challenges to help you become more attentive, smarter, and better prepared in the digital world
- Story told in episodes, with the adventures of Ines, Erin, and Francy, that turns every term into a fun lesson.

If you're between 8 and 14 years old, you're curious, and you want to learn how to use the internet safely, this dictionary is made just for you. And if an adult is reading along with you – whether it's a parent, grandparent, or teacher – they might learn something new too!

CyberInes, ErinJoy, and HackyFrancy are waiting for you to join them on this journey through the cyber alphabet. At the end, you'll receive a "Cyber Expert" certificate for your courage and curiosity!

Let's start this adventure – letter by letter!

With enthusiasm,

Fraga Țariuc **Alex Ricobon**

In a digital world full of mysteries, where technology meets creativity and courage, there are three friends who join forces to protect the internet and teach you how to stay safe online.

They are: Ines, Erin, and Francesca – the Cyber Explorers Team!

- **CyberInes** is 14 years old and the team leader. She's sporty, passionate about football and Formula 1, and always organized. For her, every cyber problem is like a game strategy: you need to find the best solution!

- **ErinJoy**, 11 years old, is the cheerful heart of the group. She loves dancing and playing games like Roblox, and she's always curious about the digital world. She loves discovering new things and turning them into fun.

HackyFrancy, 9 years old, loves codes, games, and digital mysteries. She dreams of becoming a good super-hacker who saves the world from viruses and cyber problems. She's brave, inventive, and always has a joke... or a strong password in her pocket.

Together, they form an unbeatable team – each with her own style, but united by a shared mission: to discover, protect, and learn everything about digital safety.
And now, they have chosen you to join them on this adventure! As you go through the dictionary, you'll learn alongside them, solve challenges, discover cyber secrets and... who knows? Maybe you'll discover a hidden talent too!

A Secret Mission for You

It was a regular day... or at least it seemed like it. CyberInes was finishing her homework on her tablet, ErinJoy was dancing around her room with headphones on, and HackyFrancy was focused on a laptop covered with stickers of puppies and binary codes.

Suddenly, HackyFrancy's screen flickered. A mysterious message appeared, written in green letters on a black background:

Attention! The internet is in danger!
False information, weak passwords, and viruses
are spreading faster than a funny video!
We need your help
Form a team and create the Cyber Dictionary
to teach other kids how to protect
themselves in the digital world.

The mission starts NOW.

"This isn't a joke!" said HackyFrancy, eyes wide. "Someone really needs us!"

"It's clearly a cyber challenge!" said CyberInes, standing up. "Let's make a plan."

"And let's make it super fun!" laughed ErinJoy, already drawing a logo on her tablet: Cyber Explorers.

And so their adventure began. Three brave friends, each with her own style, but united by the same desire: to help children all over the world stay safer online.

And guess what?

🎯 Now it's your turn!

We invite you to join the team. Read each term, learn from the stories, solve the challenges, and become a Cyber Expert too!

By the end, you'll have the superpower to surf the internet with your head held high and a strong password in place. 🔓😉

A

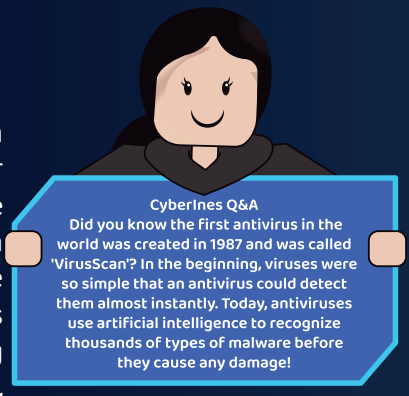
Access Control

Definition: Access control means deciding who can see or use certain data or systems. It's like using keys or badges at school – some doors are only for teachers. In the cyber world, access control makes sure only the right people can get to sensitive information.
Example: Only the teacher has access to edit grades in the school's computer system.

Adware

Definition: Adware is a type of program that tries to show you ads (sometimes very annoying ones) on your computer or phone. These ads often appear when you download free apps from unsafe sources. Some adware is harmless, but others might collect your data without you knowing.
Example: When I play a free game, I always see annoying ads. I think it has adware in it.

Antivirus



Definition: An antivirus is a program that helps protect your computer or phone against "digital viruses." These viruses are bad programs that can destroy files, steal information, or make your device run slower. The antivirus works like a guard: it scans everything coming into your computer, like files, games, or emails, and removes anything dangerous.
Example: When I downloaded a new game, my antivirus told me it was dangerous, so I didn't install it.
CyberInes says: Ask an adult if you have an antivirus installed on your device. If you're not sure, ask them to help you find out!

Application Security

Definition: Application security means protecting programs and apps from attacks, so users are safe when using them. This includes checking the code, applying updates, and using protection measures to stop hackers from exploiting weaknesses. It's like putting locks and alarms on every door and window of a building to make sure no one can enter without permission.

Example: Our developers test every app to make sure it's secure.

Artificial Intelligence in Cybersecurity

Definition: Artificial intelligence (AI) is used to detect and prevent cyberattacks. AI can learn what normal behavior looks like in a system and quickly recognize any suspicious activity, stopping attacks faster than a human could. It's like a super-smart guard who notices every unusual move and acts right away.

Example: My company uses AI to detect phishing attempts in emails.

Attack Surface

Definition: The attack surface represents all the points through which a hacker could try to enter a computer or network. For example, if you use old, buggy apps or don't have antivirus software, you're giving hackers more "open doors." The fewer vulnerabilities you have, the harder it is to be attacked.

Example: I closed the apps I no longer use and installed updates to reduce my computer's attack surface.

Attack Vector

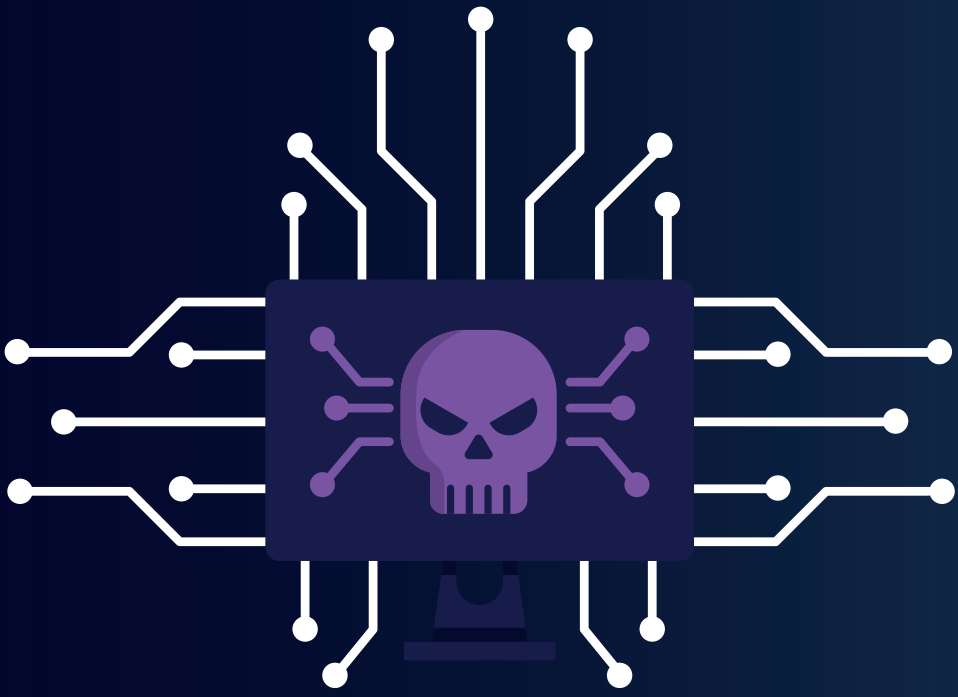
Definition: An attack vector is the path that hackers use to enter a system or network. It could be a fake email, an unsafe app, or even an infected USB stick. It's like an entry point a thief might use—a door left open, a window, or a small hole in the fence.

Example: A hacker used an attack vector through a phishing email to access the company's network.

Authentication

Definition: Authentication is the process by which a system checks if you are who you say you are. Think of it like a locked door – to enter, you need to show the key (your password). Sometimes, besides the password, the system also asks for a code sent to your phone or a face scan to make sure it's really you. This makes the system much more secure and stops bad guys from getting into your accounts.

Example: When I logged into Roblox, besides my password, they sent me a code to my phone. That's called two-step authentication!




Username
Login

Backup

Definition: A backup is a copy of your important files. If you accidentally delete something or your computer has a problem, you can get everything back from your backup. It's like having a safety box where you keep precious things so you never lose them. You can make backups on a USB stick, an external hard drive, or in the cloud (internet storage).

Example: I made a backup of my vacation photos on an external hard drive so I wouldn't lose them.

Behavioral Analysis

Definition: Behavioral analysis is a technique used in cybersecurity to study how users, programs, or devices behave in a system. If something strange is noticed, like a user trying to access sensitive files at odd hours, the system can alert the security team. It's like a teacher noticing if a student is acting differently than usual and asking what's going on.

Example: A behavioral analysis system noticed someone trying to download many important files without permission.

Blue Team

Definition: The Blue Team is the team that defends computer systems from attacks. They monitor, detect, and respond to cyber threats like digital guardians. If the Red Team is the "attack team," the Blue Team is the "defense team."

Example: The Blue Team discovered someone trying to enter the network without permission and stopped the attack immediately.

Botnet

Definition: A botnet is like an army of digital robots controlled by a hacker. Each "robot" is actually a computer infected with malware, and the hacker can use these computers to do bad things, like send spam or attack other websites. If you take care of your computer and protect it, it won't become part of a botnet.

Example: I read that a hacker used a botnet with thousands of computers to take down an important website.

ErinJoy Q&A

Did you know the biggest botnet in the world infected over 30 million computers? It was called the 'Storm Botnet' and it was so powerful that it could shut down entire networks!

Broken Authentication

Definition: Broken authentication happens when a login system has security problems. These problems allow hackers to access accounts without permission, either by using weak passwords or by exploiting bugs. It's like someone having a fake key that fits your lock.

Example: A website had a broken authentication problem, and users' passwords were stolen.

Clickbait

Definition: Clickbait is a trick used on the internet to make you click on something with a shocking or exciting title – even if the content isn't true or important. It's like a flashy fishing lure trying to catch your attention.

Example: I saw a title saying "You won't believe what happened next!" but it was just clickbait.

Cloud Computing

Definition: Cloud computing means using apps and saving files on the internet instead of just on your own computer. Think of the cloud like an invisible shelf that you can reach from anywhere with internet. It's used to store photos, documents, or work with other people.

Example: I saved my homework in the cloud so I could open it from my phone too.

Command and Control (C2)

Definition: C2 is a system used by hackers to control devices infected with malware (like computers or phones). Once a device is infected, it connects to the C2 server, where hackers can give commands, steal data, or cause harm. It's like a puppeteer controlling infected devices from far away.

Example: Hackers used a C2 server to launch DDoS attacks.

Cookie

Definition: A cookie is a small file that websites save on your device to remember things like your preferences or login info. Cookies help websites work better, but they can also be used to track what you do online.

Example: When I visited a site, it asked me to accept cookies so it could remember my settings.

Credential Stuffing Attack

Definition: In this type of attack, called Credential Stuffing, hackers use stolen usernames and passwords from one site to try to access accounts on other sites. This works if people use the same password for many accounts. It's like someone finding a lost key and trying it on every door in a building.

Example: I was warned not to use the same password on multiple sites to prevent a credential stuffing attack.

Credential Theft

Definition: Credential theft is the process where hackers steal login information, like usernames and passwords, to access victims' accounts.

Example: I changed my password immediately after learning about a credential theft attempt.

Critical Infrastructure Security

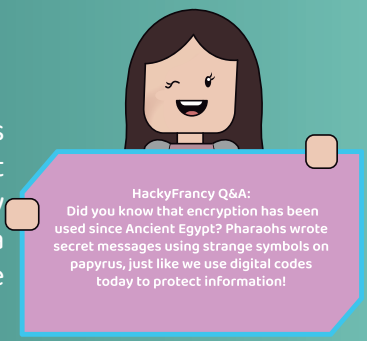
Definition: This means protecting networks and systems that are essential for society, like electricity, water, hospitals, and transport. If hackers attack these, it can cause big problems for everyone. That's why these systems need to be very well protected.

Example: Systems that control electricity supply are protected from attacks to prevent power outages.

Cryptography

Definition: Cryptography is the process of turning information into a secret code so only people with the right key can understand it. It's like putting a letter in a locked box and only the person with the key can open it.

Example: When I send messages on WhatsApp, they're encrypted, so only my friends and I can read them.



Cyberbullying

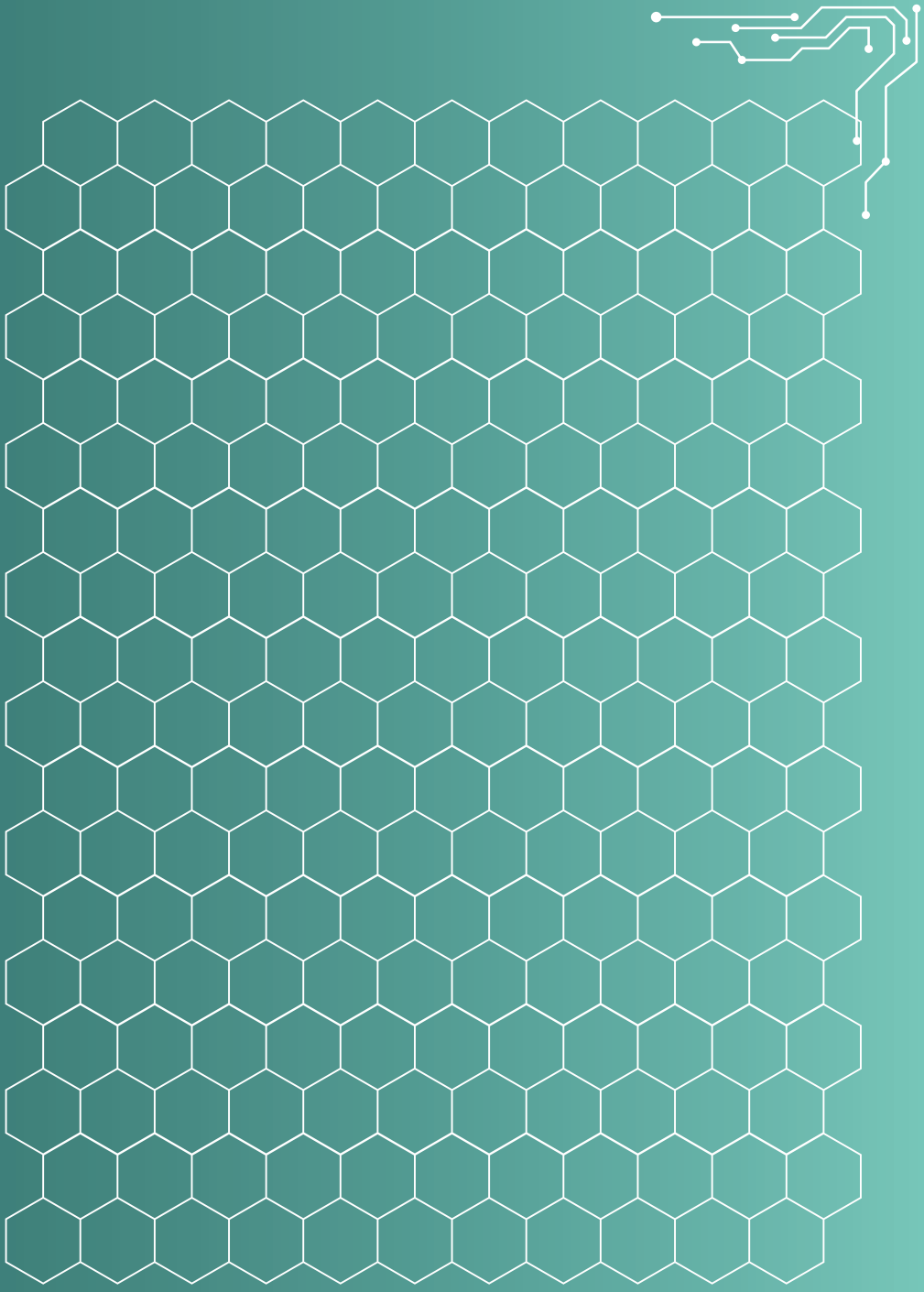
Definition: Cyberbullying is when someone is mean to others online – by sending hurtful messages, spreading rumors, or posting embarrassing photos. It's a serious problem and it's never okay. If it happens to you or someone you know, talk to an adult.

Example: My friend was upset because someone was bullying her online, so we told the school counselor.

Cybersecurity

Definition: Cybersecurity means protecting your devices, information, and internet accounts from hackers and viruses. It's like having a super shield that keeps out digital danger. Cybersecurity includes strong passwords, antivirus software, safe internet use, and more.

Example: Our teacher gave us a lesson about cybersecurity and how to stay safe online.



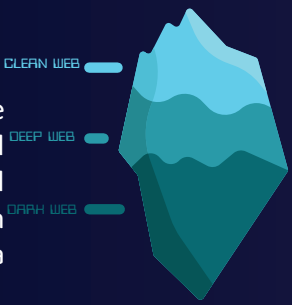
DDoS / Distributed Denial of Service

Definition: A DDoS attack is when hackers use many computers (even tens of thousands) to flood a website with fake requests, so the site can no longer function. It's like everyone ringing the same doorbell at the same time, and the owner can't keep up.
Example: An online store was down for a whole day because of a DDoS attack.

Data Exfiltration

Definition: Data exfiltration means stealing data from a computer or network without permission. Hackers find a way to copy important information, like passwords, files, or personal data, and send it outside the system. It's like someone stealing a diary from your room and sneaking it out the window without you noticing.
Example: My school prevented an attack trying to perform data exfiltration thanks to an advanced monitoring and protection system.

Dark Web



Definition: The dark web is a hidden part of the internet that cannot be accessed with normal browsers. It is sometimes used for illegal activities, but also for secure communication in countries where censorship exists. It is not a place for children and should be avoided.
Example: I read that the dark web is used by hackers, but also by journalists from countries where the internet is censored.

Digital Footprint

Definition: A digital footprint is everything you leave behind when you use the internet: your posts, comments, visited websites, and

even your searches. This can be used to understand who you are or what you like, so it's important to be careful about what you share. It's like the footprints you leave in the sand – everywhere you go, you leave a trace.
Example: I realized that all the photos I post on Instagram are part of my digital footprint.

Digital Forensics

Definition: Digital forensics is the process of investigating a cyber incident. Experts analyze devices and data to figure out what happened and who was responsible. It's like a detective story, but in the digital world.
Example: The forensics experts checked the laptops to find clues about the hackers.

DNS Spoofing

Definition: DNS spoofing is a cyberattack where hackers trick systems into redirecting users to fake websites that look like the real ones, to steal information such as passwords. It's like a "fake map" that sends you to dangerous places.
Example: A DNS spoofing attack led me to a website that looked like my bank, but it was fake.

Drive-by Download

Definition: A drive-by download is a type of cyberattack where a dangerous file is automatically downloaded onto your computer when you visit an infected website, without you noticing. Hackers use these files to install malware or steal information. It's like walking past someone who puts something in your bag without you seeing.
Example: I was warned that a site I wanted to visit could download malware through a drive-by download.

E

Email Spoofing

Definition: Email spoofing is when a hacker sends an email that looks like it comes from a trusted source (like your bank), but it's actually fake. The goal is to trick you into giving sensitive information.
Example: I received an email that looked like it was from my bank, but it was spoofing. I checked the sender's address and it was fake.

Encrypted Backup

Definition: An encrypted backup means protecting your backup files with a secret code. That way, if someone steals the files, they can't open them without the key.
Example: I encrypted the backup of my photos to keep them safe.

Encrypted Malware

Definition: Encrypted malware is a malicious program that is hidden behind a secret code (encryption) to avoid being detected by antivirus software. Encryption makes it hard to recognize until it "unpacks" and starts affecting the computer. It's like a nicely wrapped gift hiding something dangerous inside.
Example: My antivirus detected an encrypted malware trying to install itself on my computer.

Endpoint Detection and Response (EDR)

Definition: EDR is a technology that monitors devices connected to a network to quickly detect and respond to cyber threats. It's like a surveillance camera for your laptop or phone.
Example: The EDR blocked a suspicious file before it infected the network.

Endpoint Protection

Definition: Endpoint protection refers to the security measures that protect computers, phones, or tablets connected to the internet from viruses and attacks. It's like a digital shield that protects your devices.
Example: At school, the computers in the lab have an endpoint protection system to stop viruses.

Evil Twin Attack

Definition: This is an attack where a hacker creates a fake WiFi network that looks legitimate. When you connect, the hacker can intercept your information. It's like going to a fake restaurant that looks exactly like the original.
Example: When I'm in a café, I make sure the WiFi network is the official one to avoid an Evil Twin attack.

Exploit

Definition: An exploit is a method used by hackers to take advantage of a weakness in a program or system, so they can steal data or take control. It's like finding a door left ajar and entering without permission.
Example: A hacker used an exploit in a game to access players' data.

F

Failover System

Definition : A failover system is a backup system that automatically takes over if the main system breaks down. Its purpose is to keep a website, app, or service running without interruption. It's like a flashlight with backup batteries: if the first ones die, the backup ones take over.

Example: Our email system has a failover that takes over if there's a technical issue.

Firewall

Definition : A firewall is a program or device that protects your computer from outside attacks by blocking unauthorized access. It's like a guard who decides what information can enter and leave the network.

Example: My firewall blocks any unauthorized attempts to access my home network.

Firmware

Definition : Firmware is a special type of software that controls the physical components of a device, such as a printer or router. It's like a brain that tells the device what to do.

Example: I updated my router's firmware to improve the WiFi network's security.

Full Disk Encryption (FDE)

Definition : Full Disk Encryption is a technology that protects all the data on a computer or device by turning it into a secret code. Only someone who knows the correct password can decrypt and access the data. It's like putting a very strong lock on a chest containing all your important things.

Example: My phone uses full disk encryption to protect my photos and messages.

GDPR (General Data Protection Regulation)

Definition: GDPR is a European law that protects people's personal data. It requires companies to collect and use your information responsibly and ask for your permission before using it.
Exemplu: A website asked me to accept the GDPR terms before I could create an account.

Geofencing

Definition: Geofencing is a technology that creates a "virtual zone" on a map around a physical place. When a device, like your phone, enters or leaves that zone, a message is sent or a specific function is activated. It's like an invisible barrier that knows when you cross it.
Example: I received a notification on my phone when I entered a store, thanks to geofencing.

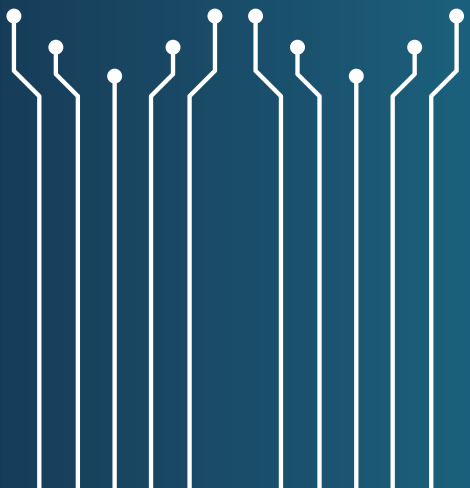
Geolocation

Definition: Geolocation means using technology to determine where you are on the globe. It's used by apps like maps or games that depend on your location.
Example: I used geolocation on my phone to find the nearest restaurant.

Governance

Definition: Governance in cybersecurity refers to the rules and procedures that help an organization protect its information and ensure everything operates safely. It's like a set of rules to keep order in a digital city.

Example: My company has strict governance rules to prevent unauthorized access to customer data.



H

Hacker

Definition: A hacker is a person who uses computer knowledge to access systems or data. Some hackers help companies improve their security (good hackers or "white hats"), while others use it to cause harm (bad hackers or "black hats").
Example: A good hacker helped a company discover a security problem in their app.

Hashing

Definition: Hashing is a process where data is transformed into a unique string of characters called a hash. It is used to verify that data has not been changed. Think of it as a "digital fingerprint" of files.
Example: My passwords are stored as hashes so that no one can read them.

Honeypot

Definition: A honeypot is a system or website specially created to attract hackers and trick them into interacting with it. The goal is to learn how hackers operate or to keep them busy away from real systems. It's like a bear trap where you put honey to attract bears but don't let them reach the real hive.
Example: Researchers used a honeypot to understand how a new type of malware works.

Host-based Firewal

Definition: A host-based firewall is a program installed directly on a computer or device that monitors and controls the network traffic coming in and out of that device. It protects the computer from cyberattacks and blocks access to suspicious programs. It's like a

door with a peephole that you can open or close to decide who can enter the house and who cannot.

Example: My laptop uses a host-based firewall to block local attacks.

Cyber Break: The Adventures of CyberInes, ErinJoy, and HackyFrancy in the Digital World

On a bright morning, CyberInes, ErinJoy, and HackyFrancy met in their super-secret lab called "The Fortress of Codes." It was a place full of screens, colorful lights, and the sound of fast typing. The three heroines had a special mission: to protect the digital world from hidden dangers and teach everyone about cybersecurity.

CyberInes, the leader of the group, checked her control panel.

"Alert from the Pixelia Network! Someone planted a virus that's slowing down all the servers in the city!" she said, her eyes focused.

"A virus?! Ew, that sounds gross!" exclaimed ErinJoy, the most cheerful of them, dancing as she adjusted their WiFi antennas. "Shall we get to work?"

"Absolutely!" replied HackyFrancy, the expert in digital gadgets.

"But be careful. If the virus came in through a Trojan Horse, it might be a trap."

"Good point. Let's activate our firewall for extra protection," said CyberInes, typing quickly on her keyboard.

The three of them entered the virtual world through their special portal. The Pixelia Network was a vibrant place, full of floating pixels and fast-moving data packets. But today, everything was slow. A dark cloud of malicious code hovered over a central server.

"This looks like a classic case of Distributed Denial of Service (DDoS)," observed HackyFrancy. "I think hackers overloaded the server."


WARNING
VIRUS DETECTED
VIRUS ALERT!

"Then we need to reset the server and remove the virus," said ErinJoy, lifting a digital wand called the Code Switch.

As they approached the server, a giant door decorated with mysterious symbols appeared in front of them.

"Hmm, this looks like an authentication gate," said CyberInes. "But look at this—it's fake! There's a Trojan Horse behind the door. If we go in, it will trigger another attack."

"No worries, I have a plan!" exclaimed HackyFrancy. "We'll use a honeypot to trick the attackers into revealing their location."

ErinJoy grinned mischievously.

"I like how you think!" And with one click, their honeypot was activated, and the hackers were caught red-handed.

With the servers clean and the hackers stopped, the Pixelia Network was fully operational again.

"We need to teach everyone about password hygiene and warn them not to open suspicious attachments," said CyberInes.

"And always use Two-Factor Authentication (2FA) for important accounts," added HackyFrancy.

"We won another battle, but the digital world will always need heroes like us!" said ErinJoy, doing a little victory dance.

And so ends the adventure of the three heroines: CyberInes, ErinJoy, and HackyFrancy. Together, they not only protect the digital world but also help everyone understand the importance of cybersecurity—with smiles and good vibes!

Identity Theft

Definition: Identity theft is when someone steals your personal information (like your name or card number) and uses it to pretend to be you or make purchases.
Example: A hacker used my information to order things online — that's called identity theft.

Incident Response

Definition: Incident response is the process used by a team to handle a cyberattack or security issue. They detect what happened, stop the attack, and fix the damage.
Example: The incident response team worked quickly to stop the attack on the school's network.

Information Security (InfoSec)

Definition: InfoSec is the process of protecting important information, whether it's stored on a computer, sent over the internet, or written on paper. The goal is to prevent this information from being stolen, changed, or lost. It's like a safe where you keep your valuable things to protect them.
Example: My company focuses on InfoSec to protect our customers' information.

Insider Threat

Definition: An insider threat happens when someone inside an organization (like an employee) does something that puts the company's data or systems at risk, either by accident or on purpose.
Example: An employee accidentally downloaded an infected file, causing an insider threat.

Integrity Checking

Definition: This is the process of checking that a file or system has not been changed without permission. It's like checking if a letter you received is exactly the same as when it was sent, without being opened or tampered with on the way.
Example: My backup system performs integrity checking for each saved file.

IoT (Internet of Things)

Definition: The Internet of Things (IoT) refers to all devices connected to the internet, such as smartwatches, smart fridges, or light bulbs controlled via phone. These devices make life easier but must be protected to prevent hacking.
Example: My smartwatch is an IoT device, and I use it to track my daily steps.

IP Address

Definition: An IP address is a unique number that identifies every device connected to the internet, like a postal address shows where you live.
Example: My computer's IP address is 192.168.100.101.

Jailbreaking

Definition: Jailbreaking means modifying a device, like a phone, to remove the restrictions set by the manufacturer. This allows you to install apps and make changes that aren't officially approved. However, once done, the device becomes more vulnerable to attacks. It's like breaking a factory-installed lock on a box so you can use everything inside however you want—even if it wasn't meant to be used that way.
Example: My friend jailbroke his phone to download apps that aren't available in the official store, but now he's having security issues.

JavaScript

Definition: JavaScript is a programming language used to make web pages interactive and dynamic. With it, websites can respond to user actions like clicking a button, filling out a form, or even playing games right in the browser. It's like the "engine" that brings a website to life, turning a simple static page into an engaging experience.
Example: When you click a button and see a message like "Thank you for signing up!", that message appears thanks to JavaScript. Here is a simple example:

```
document.getElementById("button".addEventListener("click,function() {
alert("Thank you for signing up!");
});
```

JavaScript Injection

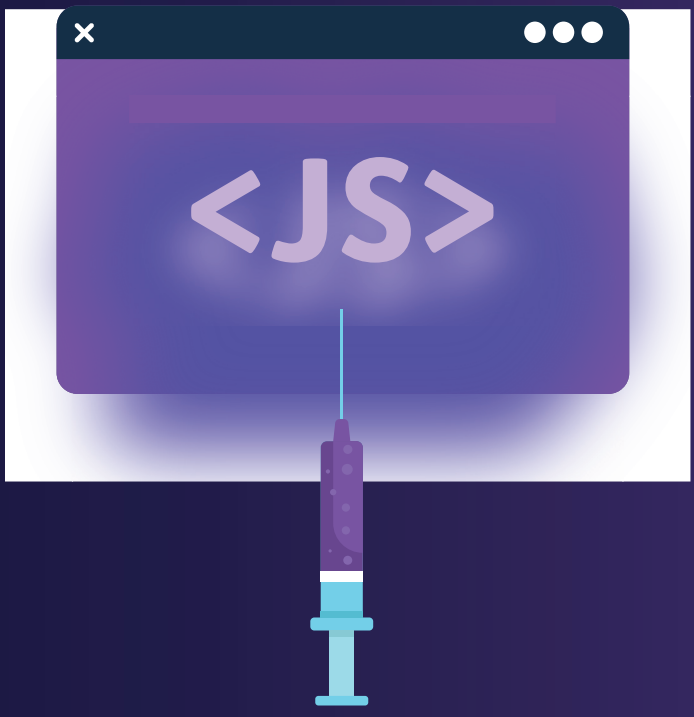
Definition: This is a type of attack where a hacker inserts malicious JavaScript code into a website to steal information or take control of the site. It's like someone adding dangerous instructions to a to-do list.

Example: A JavaScript injection attack caused the website to display fake ads.

JSON Web Token (JWT)

Definition: A JSON Web Token is a secure way to send information between two parties (for example, between a user and a server). The information is encoded in a special format that can be verified to ensure it hasn't been altered. It's like an access ticket that proves you're allowed in, and the special signature on the ticket shows that it's authentic and hasn't been forged.

Example: My school app uses JWT to log me in quickly and securely.



H

Kernel

Definition: The kernel is the core part of an operating system, responsible for managing resources and communication between hardware and software. It's like a conductor making sure everything works in harmony.
Example: The kernel on my computer was updated to fix a security issue.

Kernel Exploitation

Definition: Kernel exploitation is a type of attack where hackers target the kernel—the core of the operating system that controls all major functions of a computer. If successful, they can take full control of the device. It's like someone finding the master key to a building and being able to enter every room without restriction.

Example: A kernel exploit allowed hackers to take control of a server.

Key Exchange

Definition: Key exchange is the process through which two people or systems securely share a secret key that they will use to encrypt and decrypt messages. It's like a secret handshake that only they understand.
Example: Messaging apps use key exchange to keep conversations private.

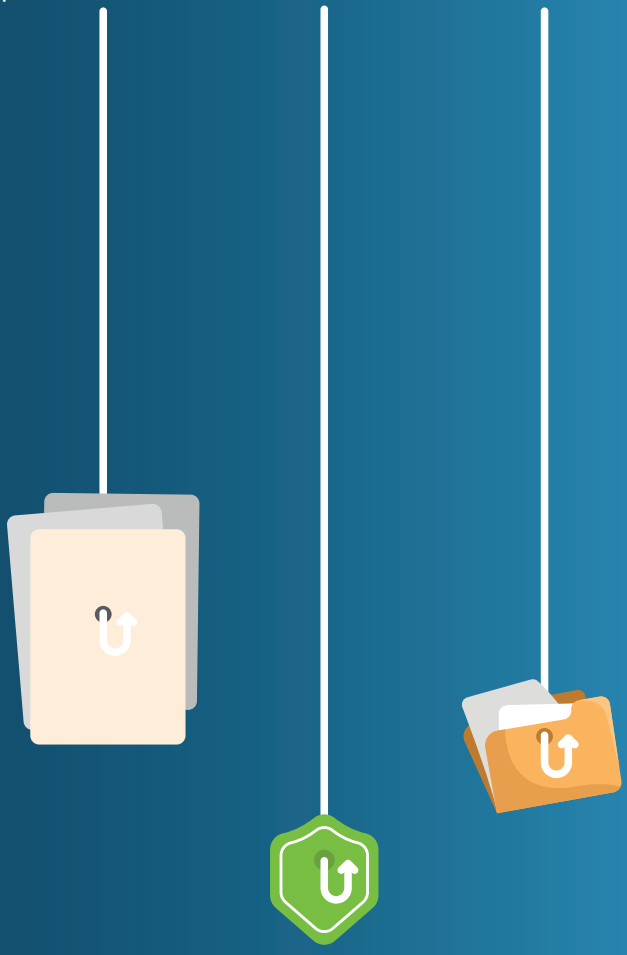
Keylogger Attack

Definition: A keylogger attack is a type of cyberattack in which a malicious program called a "keylogger" is installed on someone's computer. This program records everything you type, including passwords, messages, and other personal info, and sends it to a hacker. It's like someone standing behind you and writing down every

word you type.
Example: A keylogger was found on an employee's computer after they downloaded a suspicious file.

Keystroke Dynamics

Definition: This is a method of authentication that analyzes how you type—how fast you press the keys and in what order. It's a unique way to identify someone.
Example: The app uses keystroke dynamics to check if I'm the one typing my password.



LAN (Local Area Network)

Definition: A LAN is a network of computers and devices connected to each other within a small area, such as a home, school, or office. It allows devices to communicate and share information, such as files or printers. It's like a small team of friends working together in one room and sharing their resources.
Example: In my school's LAN, I can use the printer without connecting to the internet.

Lateral Movement

Definition: Lateral movement is a strategy hackers use after gaining access to a system. Instead of attacking right away, they move "sideways" through the network to access other computers, servers, or files and find valuable information. It's like an intruder entering a building and quietly exploring different rooms to find something important.
Example: The hackers used lateral movement to reach the company's main server.

Log Analysis

Definition: Log analysis means checking the files where all system, network, or app activities are recorded. These files, called "logs," are like notebooks that write down every action. Experts analyze these logs to find problems, cyberattacks, or unusual behavior. It's like reading a journal to figure out what happened in a day.
Example: The administrator checked the logs to understand why the network was running slowly.

Logic Bomb

Definition: A logic bomb is a hidden program on a computer that stays inactive until a certain condition is met, like a specific date or opening a file. When triggered, the logic bomb "explodes" and can delete files, lock the computer, or cause other problems. It's like a balloon that pops only if someone touches it.

Example: An attacker planted a logic bomb in the system that activated on April 1st.

Macros

Definition: Macros are instructions or sets of commands recorded to automate repetitive tasks in programs like Word or Excel. They help save time, but sometimes hackers use macros to run malicious code on a victim's computer. It's like a robot doing your work, but if someone controls it, it could do something harmful.
Example: My antivirus blocked a suspicious macro from a Word document.

Macro Virus

Definition: A macro virus is a type of malware that uses macros—automatic scripts in programs like Word or Excel—to spread and cause harm. This virus can delete files, change documents, or send infected messages to others. It's like receiving a fake instruction manual that breaks things instead of helping.
Example: I opened a Word file from a suspicious email, and a macro virus infected my computer and sent the infected file to my friends.

Malware

Definition: Malware is a malicious program created to cause problems on your computer or phone. It can delete files, steal information, or slow down your device. Common types of malware include viruses, trojans, and ransomware.
Example: I downloaded a suspicious file, and my antivirus detected it was malware.

MITM (Man-in-the-Middle Attack)

Definition: This is a type of cyberattack where a hacker secretly intercepts the communication between two people or systems. It's like someone listening to your conversation without permission.
Example: A MITM attack can steal passwords if you connect to an unsafe WiFi network.

Multifactor Authentication (MFA)

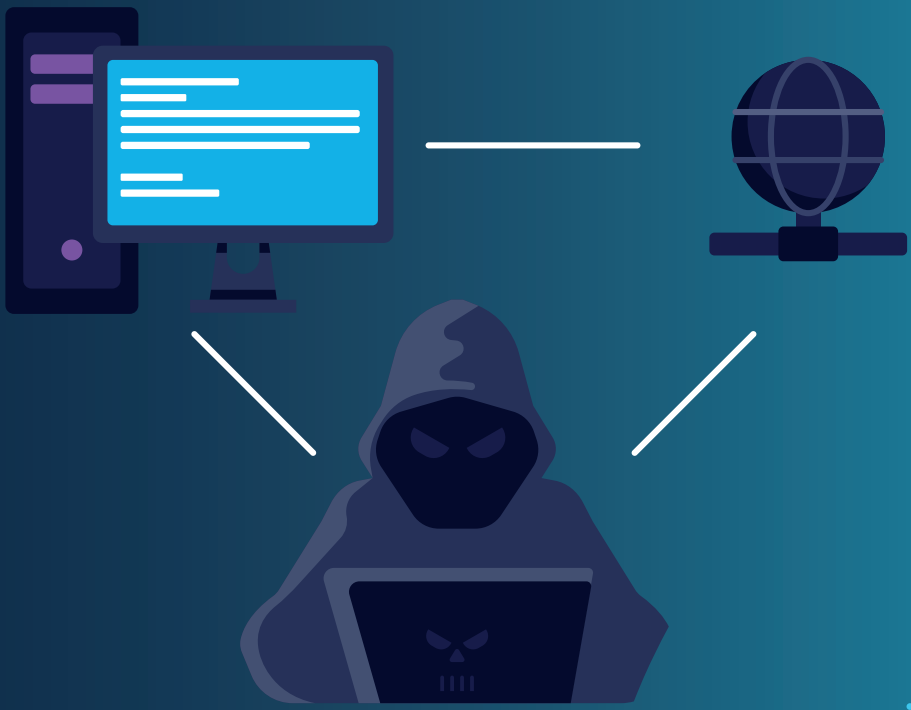
Definition: MFA is a secure way to log into your accounts. Besides your password, you also need to use another way to verify your identity, like a code sent to your phone. It's like having two locks on a door.

Example: I activated MFA on my email account, so now I also have to enter a code from my phone.

Mobile Device Management (MDM)

Definition: MDM is a technology used by companies to control and protect mobile devices like phones and tablets used by employees. With MDM, companies can install apps, update software, wipe data remotely if a device is lost, and keep information safe. It's like a digital supervisor making sure all devices are secure and working properly.

Example: The school tablets are managed through an MDM system that blocks games during class time.



Next-Generation Firewall (NGFW)

Definition: An NGFW is an advanced firewall that offers more than traditional network protection. Besides blocking unauthorized access, it can analyze traffic in detail, detect complex attacks, and stop dangerous applications. It's like a very smart doorman who not only checks who comes in but also what they bring and what they do inside.
Example: The company installed an NGFW to detect and block both regular viruses and advanced attacks.

NIDS (Network Intrusion Detection System)

Definition: NIDS is a system that monitors the network and alerts administrators if it detects suspicious activity. It's like an alarm system for the network.
Example: The school's network uses NIDS to detect unauthorized access.

NIS2 (Network and Information Security Directive 2)

Definition: NIS2 is a European law that requires companies to better protect their networks and data to prevent cyberattacks. It's like a rule that says everyone must have strong locks on their digital doors.
Example: My dad's company implemented new security rules according to NIS2.

Network Security

Definition: Network security means protecting the computer network from unauthorized access and attacks. It's like a digital wall that defends the network.

Example: My router uses a strong password for network security.

Network Segmentation

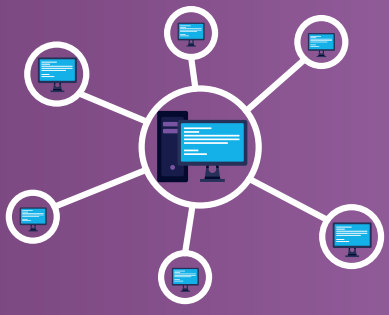
Definition: Network segmentation means dividing a big network into smaller parts so that an attack can't affect the whole system. It's like having several separate rooms with closed doors in a house.
Example: Segmenting the school's network means the labs and teachers' offices are digitally separated.

Network Sniffing

Definition: Network sniffing is a technique used by hackers or security experts to analyze data moving through a network. If the network is not protected, someone could see sensitive information, like passwords or messages being sent. It's like secretly listening to people's conversations in a room without being invited.
Example: A hacker used network sniffing on an unsecured WiFi network to capture the passwords of users who were logging in.

Non-repudiation

Definition: Non-repudiation is a cybersecurity concept that ensures no one can deny sending a message, performing an action, or accessing a system. Using digital signatures or other verification methods, clear proof is created about who did a certain activity. It's like signing for a package—you can't later say you didn't receive it.
Example: When I sent an important digitally signed email, I used non-repudiation to prove it was really me who sent it and that the message wasn't changed.



OAuth (Open Authorization)

Definition: OAuth is a system that allows apps to use your information without asking for your password. It's used, for example, when you sign in to a website using your Google or Facebook account.
Example: I used OAuth to sign in to a new app using my Google account.

Obfuscation

Definition: Obfuscation is the process of hiding information or code in a format that's hard to understand for humans. The purpose is to protect data or to hide what a program does, making it harder for hackers to figure it out. It's like writing a secret message using a complicated code that only you and your friends understand.
Example: The developers of a game used obfuscation to hide the code so that no one could modify or copy it without permission.

Open Redirect

Definiție: Open Redirect is a security vulnerability that happens when a link on a trusted website redirects you to another site without warning. Hackers can use this technique to trick you into visiting dangerous pages that look trustworthy. It's like someone giving you the wrong directions on purpose to lead you to a risky place.
Exemplu: I clicked on a link in an email that looked safe, but it was an Open Redirect and took me to a fake site where they asked for my password.

OSINT (Open Source Intelligence)

Definition: OSINT means collecting information from public sources, such as websites or social media, to find out more about a person or an organization. It's like searching on Google to find details about a topic or someone, using only the data that is publicly visible without breaking any rules.

Example: The police used OSINT to find clues about a missing person by checking social media profiles and online articles.

Password Cracking

Definition: Password cracking is the process where hackers try to guess or break passwords to access accounts, files, or systems. They use special programs that try thousands or millions of combinations of letters, numbers, and symbols until they find the right password. It's like trying all possible combinations to unlock a padlock.
Example: My antivirus stopped a password cracking attempt on my account.

Password Manager

Definition: A password manager is an app that helps you create, store, and use strong passwords for all your accounts. Instead of remembering many passwords, you only need to remember one—for the app.
Example: I use a password manager so I don't forget the passwords to my accounts.

Patch Management

Definition: Patch management is the process of installing software updates that fix vulnerabilities and improve security. It's like fixing a hole in a fence so thieves can't get in.
Example: My computer always asks me to install updates to fix security issues.

Penetration Testing

Definition: Penetration testing is a process where security experts try to "attack" a system, network, or app—but in a controlled and authorized way—to discover weaknesses. The goal is to find vulnerabilities before real hackers do. It's like checking your house's locks and windows to see if someone could get in without a key.
Example: Our company hired a penetration testing team to find security problems on our website before launch.

Pharming

Definition: Pharming is a type of cyberattack where hackers change the settings of a website or your network to redirect you to a fake site—even if you type the correct web address. The fake site looks real but is made to steal your information, like passwords or credit card numbers. It's like someone changing road signs to send you to the wrong place without you knowing.
Example: Even though I typed the correct bank address, a pharming attack took me to a fake website.

Phishing

Definition: Phishing is a method used by hackers to trick people into giving away personal information, like passwords or credit card details. This is usually done through emails or messages that look like they come from trusted sources, but are actually fake. It's like someone sending you an official-looking letter that's really a trick.
Example: I got an email that looked like it was from my bank, but my friends told me it was phishing.

Pretexting

Definition: Pretexting is a technique used by hackers to trick someone into giving away confidential information. The attacker creates a fake story (a "pretext") and pretends to be a trusted person, like a company employee or a friend. It's like someone pretending to be a fake police officer to get important information from you.
Example: A hacker used pretexting by pretending to be tech support and asked me for my password.

Principle of Least Privilege

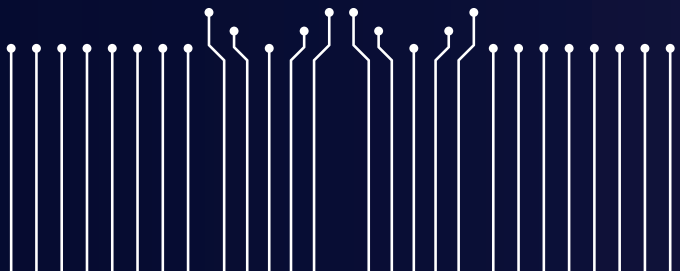
Definition: The principle of least privilege says that a person or program should have access only to the information and resources they need to do their job—nothing more. This helps prevent mistakes and cyberattacks by limiting what each user or app can do. It's like allowing your friends into your living room but not into your private rooms.
Example: Our employees only have access to the files that are relevant to their department.

Privilege Escalation

Definition: Privilege escalation is a technique hackers use to get more control over a system than they should have. For example, someone with limited access to a computer might find a way to get full access to change settings or steal information. It's like having a key only for the living room but managing to get into the whole house.
Example: A privilege escalation attack allowed hackers to access all the company's files.

Public Key Encryption

Definition: Public key encryption is a way of securing messages where you use two keys: a public one (that everyone can see) and a private one (only you have). It's like a mailbox: anyone can drop a letter in, but only you have the key to open and read it.
Example: My school uses public key encryption so only the principal can read certain emails.



Purple Team

Definition: A Purple Team is a group that combines the Red Team (attack) and the Blue Team (defense). They work together to test and improve security. Think of the Purple Team as a team of coaches helping both "attackers" and "defenders" get better.

Example: The Purple Team analyzed simulated attacks and taught the Blue Team how to respond faster next time.

QR Code (Quick Response)

Definition: A QR code is a special type of square barcode that can be scanned with a phone to quickly access information, such as a link, a message, or contact details. It's like a digital "magic door" that takes you straight to the information you need without typing anything.
Example: I scanned a QR code from a movie poster and instantly got to the website where I could buy tickets.

QR Code Spoofing

Definition: QR code spoofing is an attack where a hacker uses a fake QR code to send you to a dangerous website or to steal information. Even though the code looks legitimate, it can lead you somewhere unsafe.
Example: I double-checked a QR code before scanning it to make sure it wasn't part of an attack.

Query Injection

Definition: Query Injection is a type of cyberattack where a hacker inserts malicious code into a search field or form on a website. The goal is to trick the site into executing commands it shouldn't, like revealing confidential data from its database. It's like someone changing a train ticket to travel somewhere else without paying.
Example: A query injection attack was used to get users' passwords from a website.

Quantum Security

Definition: In cybersecurity, the word "quantum" is used to describe technologies based on quantum physics, like quantum computers or quantum cryptography. These use the properties of tiny particles (such as photons) to solve complex problems

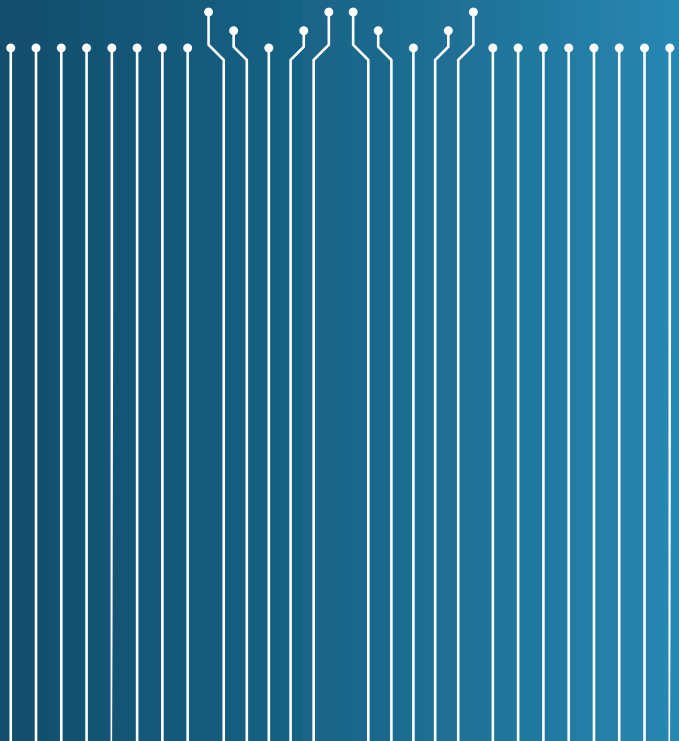
or to create much more secure methods of protection. It's like using "scientific magic" to make communications nearly impossible to break.

Example: Researchers are working on quantum cryptography, which will make digital messages so secure that even a supercomputer won't be able to decode them.

Quarantine

Definition: In cybersecurity, quarantine is a special area where suspicious files are isolated so they don't infect your computer. It's like putting something dangerous in a box until you can investigate it.

Example: My antivirus quarantined a file that looked suspicious.



RaaS – Ransomware as a Service

Definition: RaaS is a way for hackers to create ransomware programs and offer them to others to launch attacks. They share the profits, and anyone can use the ransomware without knowing how to create it. It's like renting a dangerous tool to harm others.
Example: An attacker with little technical knowledge used RaaS to launch a ransomware attack and lock a company's computers.

Ransomware

Definition: Ransomware is a type of malware that locks your files and demands money (a ransom) to unlock them. It's like someone locking your room and asking for money to give you the key.
Example: I read about a hospital that was hit by a ransomware attack and couldn't access patient records until they paid the ransom demanded by the attackers.

Red Team

Definition: A Red Team is a group of experts who simulate cyberattacks on an organization to find weaknesses in its security. Their goal is to improve defenses by testing them. It's like a group of "bad actors" helping the "good team" get stronger.
Example: The Red Team simulated a cyberattack to test how well the security team responds.

Remote Access Trojan (RAT)

Definition: A RAT is a malicious program that allows hackers to access and control your computer remotely, as if they were sitting right in front of it.
Example: I read that a RAT was used to spy on the computers of an organization.

Risk Assessment

Definition: Risk assessment is the process a company uses to identify which threats might affect its systems and decide how to prevent them. It's like regularly checking your house to make sure everything is safe.
Example: The IT team does a monthly risk assessment to identify security problems.

Risk Mitigation

Definition: Risk mitigation is the process of taking actions to reduce or eliminate threats that can affect a system or organization. This can include using firewalls, encrypting data, or training users. It's like putting a screen on windows to keep bugs out.
Example: We implemented two-factor authentication as part of our risk mitigation strategy.

Role-Based Access Control (RBAC)

Definition: RBAC is a security method where access to files or applications is given based on a user's role, like student, teacher, or administrator.
Example: In the school library system, only teachers can access the database with students' grades.

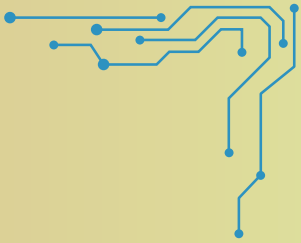
Rogue Access Point

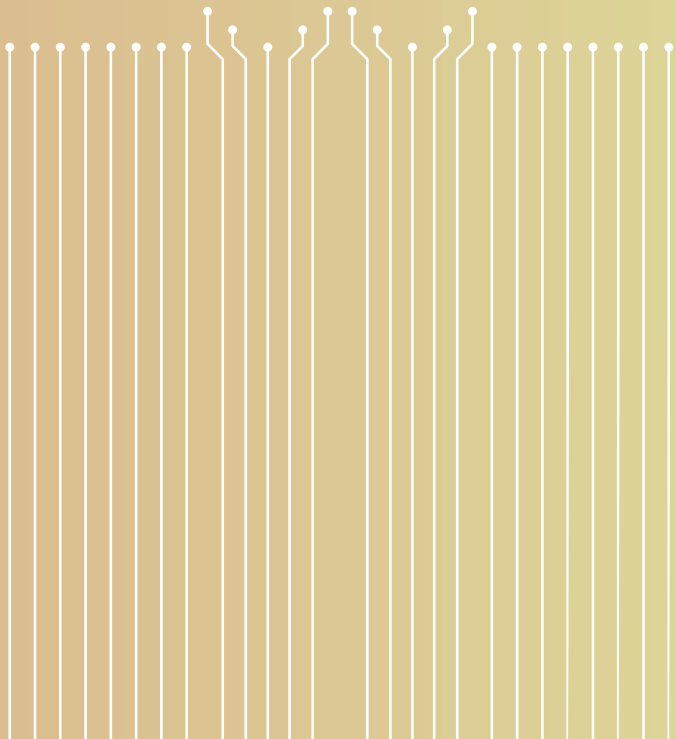
Definition: A rogue access point is a WiFi device that is not authorized and may be set up by hackers or by accident. It can be used to intercept data from users who connect to it. It's like a "fake bridge" that leads you the wrong way.
Example: Hackers set up a rogue access point in a café to steal data from people who connected to the WiFi network.

Rootkit

Definition: A rootkit is a type of malware that hides deep inside a computer's operating system, making it hard to detect. Hackers use it to take full control over a device.

Example: A rootkit can stay hidden for a long time, so my antivirus constantly scans the system.





S

Sandboxing

Definition: Sandboxing is a security method where a program or file is isolated in a controlled environment to check if it's safe. It's like a sandbox where you can test something without risking damage to everything else.
Example: I used sandboxing to test a file I downloaded from the internet before opening it.

Security Breach

Definition: A security breach happens when systems or networks are compromised and sensitive data is accessed or stolen without permission. This can happen because of vulnerabilities, cyberattacks, or human mistakes. It's like someone sneaking into a building and stealing important documents.
Example: A security breach exposed the data of a big company's customers.

Security Incident

Definition: A security incident is an event that negatively affects the functioning of a system, network, or an organization's data. It can include cyberattacks, data loss, malware infections, or unauthorized access. It's like when someone tries to enter your house without permission or leaves a door open and things go missing.
Example: A security incident occurred when a hacker accessed a server and downloaded important files.

Security Token

Definition: It is a device or an app that generates unique codes for authentication. It is used to increase account security. It's like an electronic key you use together with a physical key to open a door.
Example: To access my bank account, I use a security token that generates unique codes.

Server

Definition: A server is a special computer or program that provides services to other computers or devices connected to a network. It can send files, store data, or host websites. It's like a big library where you can go to borrow books or get information—but instead of books, the server provides digital files and services.
Example: When I visit a website, my computer asks for information from a server that hosts that site.

Session Hijacking

Definition: This is an attack where hackers steal the information from an active session on a website (like an authentication cookie). Once they have this info, they can access the victim's account as if they were the real user. It's like someone taking your place in line after you've already gotten a ticket.
Example: A session hijacking attack compromised my account on an unsecured site.

Shoulder Surfing

Definition: Shoulder surfing is a simple way to steal information like passwords by looking at someone's screen or keyboard.
Example: I noticed someone trying to shoulder surf while I was entering my phone password.

SIEM (Security Information and Event Management)

Definition: SIEM is a technology used by companies to monitor network activity and detect security problems. It's like a digital surveillance camera that alerts you right away if something seems suspicious.
Example: The company uses SIEM to detect unusual activity in the network.

Smishing

Definition: Smishing is a type of cyberattack similar to phishing, but it's done through text messages. Hackers send messages that seem to come from trusted sources, like banks or companies, asking you to click a link or give personal information. It's like getting a fake letter in your mailbox that tricks you into giving away important details.
Example: I got an SMS that looked like it was from a delivery company asking me to click a link—it was a smishing attack.

Social Engineering

Definition: Social engineering means tricking or manipulating people into giving away sensitive information like passwords or credit card details. Hackers don't attack the technology, they attack people's trust. It's like someone convincing you to give them the key to your house by pretending to be a family friend.
Example: A hacker sent me a message pretending to be my friend, but they were trying to steal my password.

Spam

Definition: Spam is a bunch of unwanted or unsolicited messages, usually sent in bulk. It can be annoying and sometimes contains dangerous links.
Example: I got lots of spam emails promising big prizes, but I deleted them.

Spyware

Definition: Spyware is a type of program that installs itself on your computer or phone without you knowing and watches what you do. It can collect passwords, bank data, or other personal information.
Example: I downloaded a game from an unknown site, and my antivirus detected that it had spyware.

Spyware Detector

Definition: This is a program that finds and removes spyware from your computer or phone. It's like a guard dog that detects hidden spies.
Example: I installed a spyware detector that helped me delete a dangerous program.

SQL Injection

Definition: SQL Injection is a type of cyberattack where hackers insert malicious code into an online form or search box. The goal is to trick the site's database into revealing sensitive information or allowing unauthorized access. It's like someone using a secret phrase to open a door that shouldn't be opened.
Example: A hacker used SQL injection to access user data on an unsecured website.

SSL/TLS (Secure Socket Layer / Transport Layer Security)

Definition: SSL and TLS are protocols that secure the connections between your computer and a website. If you see a lock next to a site's address, it means it uses these protocols to protect your data.
Example: When I shop online, I make sure the site uses SSL/TLS to protect my information.

Steganography

Definition: Steganography is the art of hiding information in an image, audio file, or another type of file so that it can't be detected. It's like a secret letter hidden in a drawing.
Example: Hackers hid a dangerous message inside a photo using steganography.

Supply Chain

Definition: The supply chain includes all the companies and processes involved in creating and delivering a product or service. For example, if we buy a video game, the supply chain includes the developers who made it, the factories that produced the discs, the companies that transported them, and the stores that sell them.
Example: The supply chain of a smartphone includes miners who extract rare metals, factories that assemble the parts, and stores that sell the final product.

Supply Chain Attack

Definition: A supply chain attack happens when hackers don't target a big company directly but instead trick or infect a smaller company that works with the big one. Through the smaller company, they gain access to the larger company's systems or information. It's like someone hiding something dangerous in a delivery sent by a courier company you trust.
Example: Hackers attacked a company that provided software updates to the school, and the program became infected.

Threat Hunting

Definition: Threat hunting is a proactive process where specialists search for signs of cyberattacks in an organization's networks, even before the attacks actually happen.
Example: Our security team does threat hunting to prevent attacks.

Tokenization

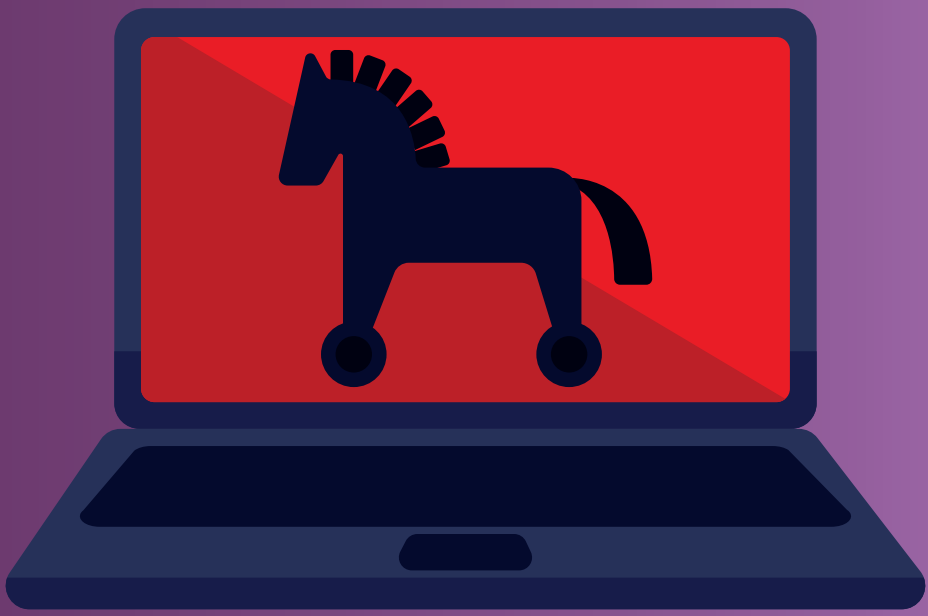
Definition: Tokenization is a security method in which sensitive information, such as a credit card number, is replaced with a unique code called a "token." This token does not contain the actual data and cannot be used outside the system that created it. It's like when you get a token at a coat check— the token represents your coat, but it doesn't reveal anything about it.
Example: When I pay online, my card data is tokenized to keep it safe.

Traffic Analysis

Definition: Traffic analysis is about monitoring the data that moves through a network to detect suspicious activity. It's like checking what cars come in and out of a city.
Example: The university's network uses traffic analysis to detect attacks.

Trojan Horse

Definition: A Trojan horse is a dangerous program (malware) that pretends to be something useful or safe, but once installed, it lets hackers access or control your device. It's like a pretty gift that hides something bad inside.
Example: I downloaded a free game that had a Trojan horse in it, but my antivirus stopped it.



Unauthorized Access

Definition: This is when someone enters a system or opens files without permission. It's like someone entering a house without having the key.
Example: I changed my WiFi password to prevent unauthorized access.

Unsecured Protocols

Definition: Unsecured protocols are ways of communicating on the internet that don't protect the data sent between devices. This means that information like passwords or messages can be intercepted and read by hackers. It's like sending a letter without an envelope—anyone can read it.
Example: I don't connect to websites that use HTTP because it's an unsecured protocol.

Unified Threat Management (UTM)

Definition: UTM is a system that combines several security tools into a single device or software, such as firewall, antivirus, web filtering, and intrusion detection. It's like a "super guard" that protects your network from all kinds of threats.
Example: The company uses a UTM device to protect its network from viruses, cyberattacks, and dangerous websites.

URL (Uniform Resource Locator)

Definition: A URL is the address of a website or an online resource. It's what you type in the browser's address bar to access a site. The URL shows where the website is located on the internet, just like a postal address shows where a house is.
Example: The URL of the Women4Cyber Romania Association website is www.women4cyber.ro.

URL Spoofing

Definition: This is an attack where a hacker creates a fake link that appears to be legitimate but redirects you to a dangerous website. That site may look real—like your bank's website—but is used to steal personal information such as passwords or credit card details. It's like someone giving you a fake map that leads you to the wrong place.
Example: I checked the link in the email before clicking it to avoid a URL spoofing attack.

User Account Control (UAC)

Definition: UAC is a security feature in Windows that asks for your permission before making important changes to your computer. It's like a security guard asking if you're sure you want to enter a restricted area, to prevent unauthorized access.
Example: My computer asked me through UAC if I was sure I wanted to install a new program.

User Behavior Analytics (UBA)

Definition: UBA is a technology that monitors what users do on a system or network in order to detect unusual behavior. If someone tries to access important files at a strange hour or does something they shouldn't, UBA can signal this to help prevent an attack. It's like a teacher noticing when a student acts differently and asking what's going on.
Example: The UBA system detected that a user account was downloading many unusual files, which could indicate a cyberattack.

V

Virtual Machine

Definition: A virtual machine is a special program that allows a computer to act like it's several computers at once. You create a "computer inside a computer" to test new things without affecting the main system. It's like a separate playroom where you can experiment without messing up the rest of the house.
Example: I used a virtual machine to install an old game that doesn't work on my modern computer.

Virtual Private Cloud (VPC)

Definition: A Virtual Private Cloud (VPC) is a secure space created within a public cloud (like Amazon Web Services or Google Cloud) that works like a private network. It allows companies to store their data and applications in a safe environment, isolated from the rest of the internet. It's like having your own locked apartment in a big building.
Example: Our company uses a VPC to keep customer data safe, even though it's hosted on a public cloud.

Virus

Definition: A computer virus is a malicious program designed to infect computers or other devices. It spreads from file to file, sometimes even from one computer to another, and can cause problems like deleting files, slowing down the system, or destroying data. It's like a real virus that spreads among people, but this one infects computers.
Example: I downloaded a file from an unsafe website, and it contained a virus that locked up my computer.

Virus Signature

Definition: A virus signature is a unique code used by antivirus programs to identify a specific virus. It's like a digital fingerprint

of the virus.
Example: My antivirus found a file with a signature that matched a known virus.

Vishing

Definition: Vishing is a type of cyberattack where hackers try to trick people through phone calls. They pretend to be from a bank, tech support, or another trusted organization and ask for confidential information like passwords, PINs, or credit card details. It's like someone calling and pretending to be a fake police officer to get you to hand over your house key.
Example: I got a phone call from someone claiming to be from the bank, but they were trying to scam me.

Voice Over IP (VoIP)

Definition: VoIP is a technology that allows people to make phone calls using the internet instead of traditional phone lines. Basically, your voice is turned into digital signals that are sent over the network, making calls faster and cheaper. It's like using a walkie-talkie, but with the help of the internet.
Example: Our team uses VoIP to make international calls more efficiently.

VPN (Virtual Private Network)

Definition: A VPN is a secure connection that hides your location and online activity, protecting you from hackers. It's like an invisible tunnel between you and the websites you visit.
Example: I use a VPN when connecting to the internet through public WiFi networks.

Vulnerability Assessment

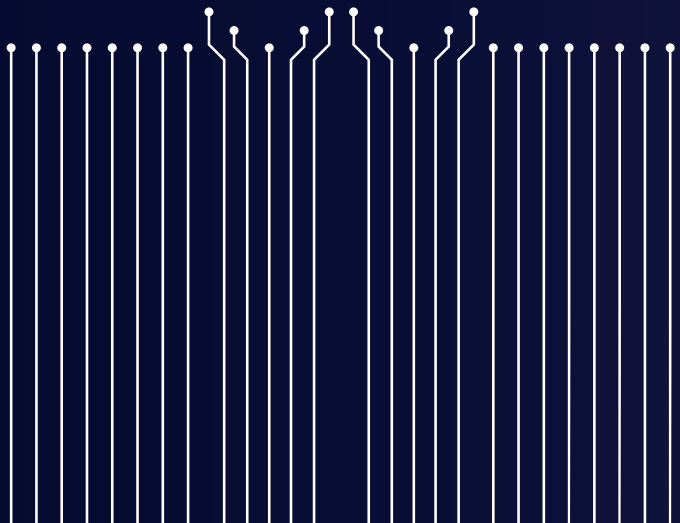
Definition: Vulnerability assessment is the process of checking a system or network to find security problems that hackers could exploit. The goal is to find and fix these weak points before someone uses them against you. It's like inspecting a building to see if there are broken windows or unlocked doors that need fixing.

Example: Our IT team regularly performs vulnerability assessments to prevent attacks.

Vulnerability Disclosure

Definition: Vulnerability disclosure is the process by which someone discovers and reports a security issue (a vulnerability) in a system, app, or network. This report helps developers fix the issue before hackers can exploit it. It's like finding a hole in the school fence and telling the teachers so they can fix it before someone sneaks in.

Example: A researcher discovered a vulnerability in an app and sent a detailed report to the company so they could fix it.



Watering Hole Attack

Definition: A watering hole attack is a type of cyberattack where hackers infect a website that their targets often visit. When people access the site, their devices get infected with malware. It's like someone poisoning a waterhole where animals go to drink, knowing they'll show up there.
Example: Hackers infected a popular site with a watering hole attack to target its users.

Web Application Firewall (WAF)

Definition: A WAF is a special type of firewall that protects web applications from cyberattacks. It works by monitoring and filtering the traffic that goes to and from the web application, blocking attacks like SQL Injection, Cross-Site Scripting (XSS), or DDoS. It's like a digital guard checking everyone before they enter a building, making sure no one has bad intentions.
Example: My company's online store uses a WAF to block attacks that try to steal customers' credit card data.

Web Scraping

Definition: Web scraping is the process where a program automatically collects information from websites, like text, images, or prices. It can be used for helpful things, like comparing prices, but sometimes it's done without permission and may break the site's rules. It's like copying all the info from a magazine page to use later.
Example: A marketing company used web scraping to collect product information.

WiFi Sniffing

Definition: WiFi sniffing is a technique used by hackers to intercept data traveling through a WiFi network. They can monitor internet traffic and try to steal information like passwords or personal data. It's like someone secretly listening to your conversations with friends.
Example: I only connect to secure WiFi networks to avoid sniffing attacks.

Wireless Intrusion Prevention System (WIPS)

Definition: WIPS is a security system that monitors WiFi networks to detect and stop unauthorized access or dangerous attacks. It's like a digital guard watching over your wireless network and alerting you if someone tries to sneak in.
Example: The company uses WIPS to prevent unauthorized access to the WiFi network.

Wireless Security

Definition: Wireless security means protecting WiFi networks from unauthorized access and cyberattacks. It includes using strong passwords, encrypting data, and other measures to stop hackers from connecting to the network or stealing information. It's like a locked gate for your network that only lets authorized people in.
Example: I set a strong password for my WiFi network to improve its security.

Worm

Definition: A worm is a type of malicious software (malware) that spreads on its own from one computer to another without needing any help from users. It multiplies automatically and can cause lots of problems, like slowing down networks or crashing computers. It's like a real worm digging tunnels through an apple, destroying it completely.
Example: A worm spread through the school's network, but the antivirus stopped the infection.

XDR (Extended Detection and Response)

Definition: XDR is an advanced cybersecurity technology that combines data from different sources—like computers, networks, and servers—to detect and respond to cyber threats more quickly. It's like a team of detectives working together, gathering clues from all over to solve a mystery faster and better.
Example: We use XDR to get a full picture of the cyber threats in our network.

XML Injection

Definition: XDR is an advanced cybersecurity technology that combines data from different sources—like computers, networks, and servers—to detect and respond to cyber threats more quickly. It's like a team of detectives working together, gathering clues from all over to solve a mystery faster and better.
Example: We use XDR to get a full picture of the cyber threats in our network.

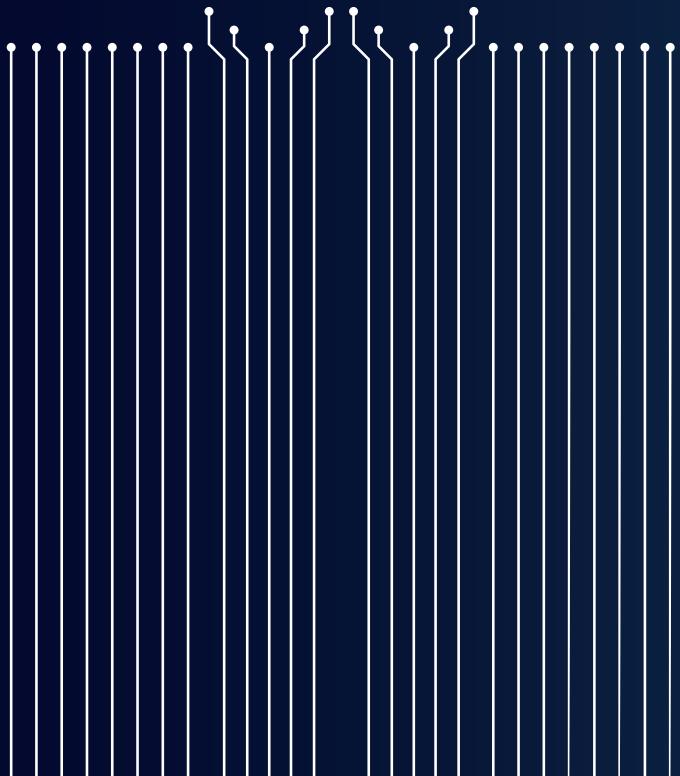
XSS (Cross-Site Scripting)

Definition: XSS is a type of cyberattack where a hacker inserts malicious code into a website. This code runs without the visitor knowing, and it can steal sensitive information like login details or passwords. It's like someone sneaking a fake letter into your mailbox that looks like it's from someone you trust.
Example: An XSS attack was used to display malicious messages on a forum that stole users' login information.

YouTube Phishing

Definition: YouTube phishing is an attack where hackers send fake links through comments or private messages on YouTube to steal users' information.

Example: A hacker sent me a fake link on YouTube that looked like a contest, but it was phishing.



Z

Zero-Day Exploit

Definition: A Zero-Day Exploit is an unknown vulnerability in a program or system that hackers discover and use before developers have time to fix it. It is like someone finding a secret door in a house that no one knew about and entering unnoticed.
Example: A hacker used a Zero-Day Exploit to take control of a popular game before the team could fix the problem.

Zero-Day Attack

Definition: A zero-day attack takes advantage of a vulnerability that developers didn't know about. It's very dangerous because there's no immediate solution. It's like discovering a secret door in a castle that no one knew existed and using it to sneak in before the king can lock it.
Example: Hackers launched a zero-day attack on a popular app before the developers could fix the problem.

Zero Trust Security

Definition: Zero Trust is a security model that assumes no one inside the network is trusted and constantly verifies the access of each user or device. It is like a fortress where every person must show a special pass every time they want to enter, even if they are already known.
Example: Our organization is implementing Zero Trust Security to protect sensitive data.

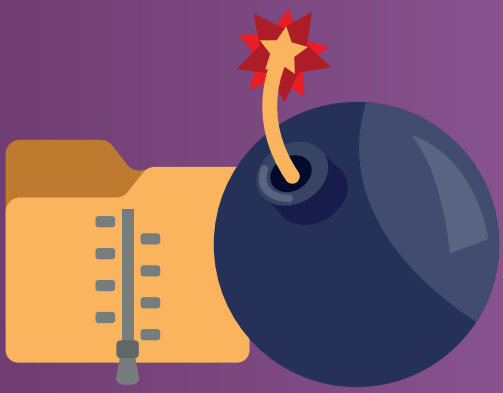
ZIP Bomb

Definition: A ZIP bomb is a compressed file that, when opened, expands into a huge amount of data that can crash the system. It's like a small gift box that explodes into a mountain of stuff when you open it.
Example: I avoided downloading a suspicious ZIP file that could have been a ZIP bomb.

Zombie Network

Definition: A zombie network is a network made up of infected computers (zombies) controlled remotely by a hacker. They are used for massive attacks, such as DDoS attacks. It is like an army of robots controlled remotely, doing whatever the hacker commands.

Example: A DDoS attack was launched using a zombie network made up of thousands of infected computers.



Q&A and FUN FACTS

CyberInes Q&A

Did you know that the first official Red Team was formed in the 1970s in the US military to test the security of military bases? Since then, the concept has been adopted by private companies and has turned into a true cybersecurity discipline.

The color purple in the Purple Team symbolizes collaboration: red (Red Team) combined with blue (Blue Team). The Purple Team isn't a separate team but rather a method where attackers and defenders work together to learn faster.

Did you know there are international Capture The Flag (CTF) competitions where Red, Blue, and Purple teams compete to attack and defend virtual systems? Many experts started their careers by participating in these contests.

Did you know that the first network considered the "grandmother" of today's internet was called ARPANET? It was created in 1969 to connect computers of American universities, and the first message ever sent was just "LO"—the network crashed before completing the word "LOGIN"!

Did you know that a firewall can be hardware or software? Hardware firewalls are special devices connected to the network, while software firewalls are programs installed on the computer.

Did you know that the term "cookie" in computing comes from "magic cookie," a small packet of data used for identification? It has nothing to do with real cookies!

Did you know that in many schools around the world, there are special lessons about how to create strong passwords and recognize phishing? Cybersecurity starts when you're young!

CyberInes and the Mystery of the Webcam

CyberInes was calmly browsing the internet when she noticed something strange: the webcam on her desk was blinking, even though she hadn't turned it on. She jumped up and grabbed her phone.

— ErinJoy, come quickly! I think someone is trying to access my camera!

Within minutes, ErinJoy and HackyFrancy rushed in with their laptops ready.

— Let's see... — said HackyFrancy, plugging in a cable. — Look! A suspicious IP address is trying to send images to a foreign server.

— Close the connection immediately! — ErinJoy said firmly.

CyberInes stared at the camera, worried.

— How is it possible for someone to get in so easily?

— It's simple, Ines, — ErinJoy explained calmly. — The camera still had the factory password, "admin." No device should be left without a strong password.

— I'm sorry I didn't check sooner... — Ines said softly.

— What matters is that you've learned now, — HackyFrancy smiled.

— We'll change the password, enable the camera firewall, and everything will be fine!

After they secured the device, CyberInes breathed a sigh of relief. She promised that from now on, she wouldn't leave any gadget unprotected.


MY PASSWORD
123456
Password:

Q&A and FUN FACTS

HackyFrancy Fun Fact

There are ethical hackers who earn money by helping companies find vulnerabilities. This is called bug bounty, and some young experts have earned hundreds of thousands of dollars discovering security problems in well-known applications!

In 2016, a huge DDoS attack blocked access to major sites like Twitter and Netflix. It was caused by thousands of video cameras infected with malware that formed an attack network called the Mirai Botnet.

In 1999, the first virus to spread by email appeared—it was called Melissa. So many people opened the infected file that some email servers were completely shut down.

The biggest phishing attack in history targeted millions of Google accounts. Google managed to block the campaign within a few hours thanks to automated protection systems.

There is a virus called Stuxnet that was discovered in 2010 and affected real industrial equipment, not just computers. It's considered one of the most sophisticated cyberattacks ever.

HackyFrancy and the Phantom App

On a rainy afternoon, HackyFrancy was browsing through the apps on her phone when she noticed something strange. An app with a weird name — SuperFlashBank++ — was installed, even though she didn't remember downloading it.

— Hm... very strange, I didn't install this! — Francy said, frowning. She tapped the icon, but the app immediately asked for her bank card details.

— This smells like a trap! — she said and quickly called CyberInes.

— Ines, have you ever had something installed without your permission?

— Yes! When I downloaded a free game from a shady website... — Ines replied, embarrassed.

HackyFrancy connected her phone to her laptop and started investigating.

— Just as I suspected! The app isn't from the official store and was installed via an .apk file from an unknown site. Also, it's sending data to a server in another country.

— Oh no! What if I had entered my card details? — Ines was scared.

— They would have emptied your account within minutes. That's why we must only install apps from official stores and never give out banking details if something seems suspicious.

CyberInes nodded, and HackyFrancy continued:

— Here's another tip: enable two-factor authentication on your bank account. Even if someone finds out your password, they still can't do anything without the code from your phone.

They deleted the phantom app and installed antivirus software on the phone.

— Thanks, Francy! — Ines said, relieved.

— You're welcome! HackyFrancy smiled. It's good to be curious, but also careful. Technology is great if we use it safely!

Q&A and FUN FACTS

ErinJoy Fun Fact

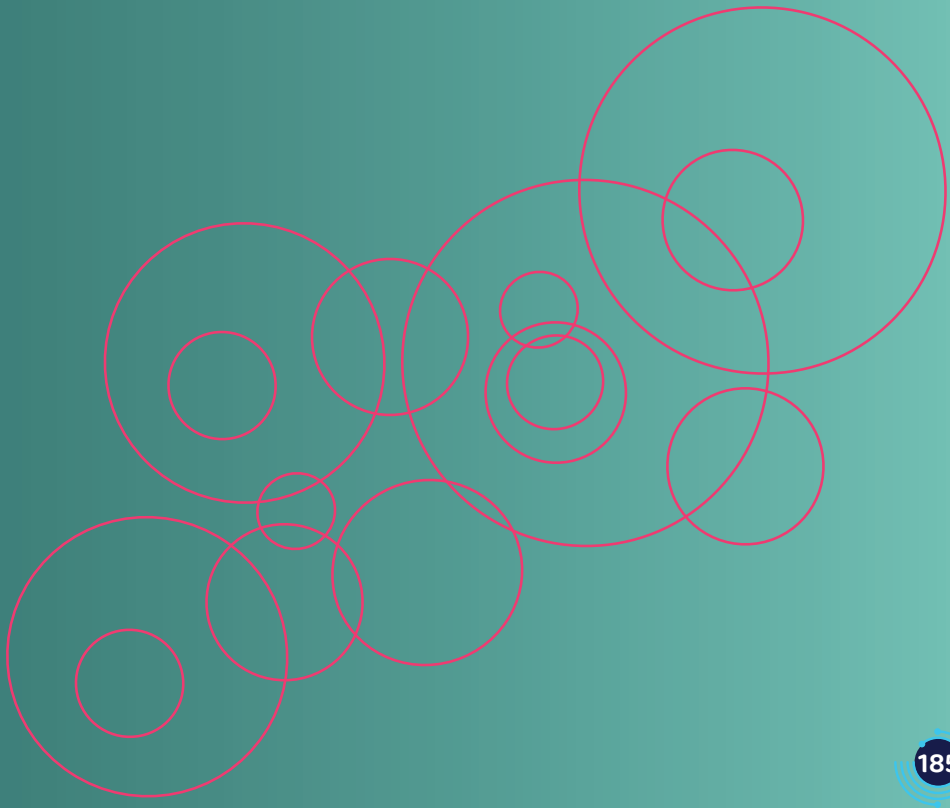
Did you know that the most used password in the world is still "123456"? Specialists recommend long and unique passwords, but many people still prefer combinations that are easy to guess. That's exactly why attackers can crack them in just a few seconds.

The Green Team is less known but extremely important: they make sure applications are designed securely from the start so they're harder to break into. It's like building a house with armored doors right from day one!

Emojis first appeared in Japan in the 1990s and became popular worldwide. Today, there are thousands of emojis, including ones about digital security, like and .

The first computer password was invented in the 1960s by a researcher working at MIT. He wanted to prevent his colleagues from opening his files without permission.

The word "spam" became popular thanks to a Monty Python comedy sketch where characters kept repeating "spam" until nobody could talk anymore. That's exactly how unwanted messages feel: over and over again.



ErinJoy and the Invisible Password

It was late in the evening, and ErinJoy was working on a project about keeping online accounts safe. Suddenly, a pop-up message appeared on her screen:

"You must change your password immediately!"

— This looks suspicious... ErinJoy murmured, closing the window with a determined click.

The next day, she told her friends everything.

— You did the right thing by not clicking the link, said HackyFrancy. That was a phishing attempt!

— What are you going to do now? — asked CyberInes.

— I want to create an invisible password, so strong that no one could ever guess it! — ErinJoy replied with a smile.

The three of them sat around the tablet and started combining ideas: a favorite word, a special number, and a surprise symbol.

— What do you think about "Siriu$Planet92!"? — ErinJoy asked.

— Perfect! — the girls said together.

That evening, ErinJoy saved her password in her digital manager and went to sleep peacefully, knowing no one would ever discover it.

CUPRINS

TABLE OF CONTENTS

CyberDict

Certificat de Cyber-Expert

se acorda lui

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

pentru curajul si curiozitatea ta!

Fraga Țariuc

Women4Cyber România

Alex. Ricobon

D3 Cyber

CyberDict

Cyber-Expert Certification

This certification is awarded to

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

for your courage and curiosity!

Fraga Țariuc

Women4Cyber România

Cyber Dict

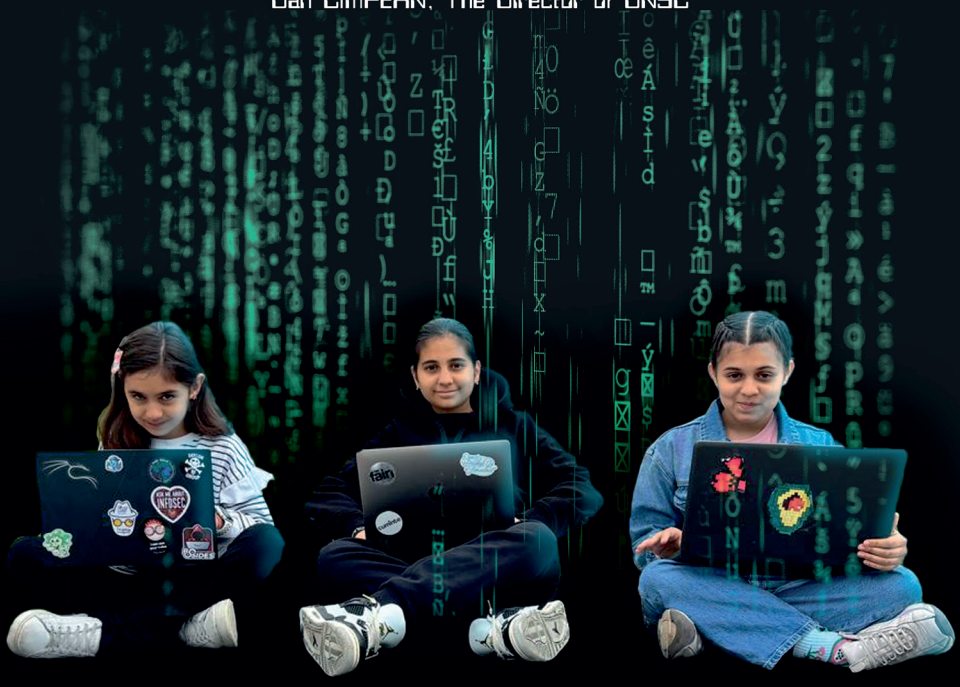
Alex. Ricobon

D3 Cyber

Directoratul Național de Securitate Cibernetică (DNSC) sprijină această inițiativă, având în vedere prezența constantă a unor termeni din domeniul cyber în media. Considerând importanța conștientizării și educării generației tinere, expusă cel mai frecvent la sfera digitală, apreciem utilitatea și potențialul acestui dicționar. El se adresează tuturor generațiilor și se dorește a fi o punte între acestea. Îl recomandăm, întrucât reprezintă o sursă de încredere privind definițiile-cheie și va fi în continuă actualizare. Dan CÎMPEAN, Directorul DNSC

The National Directorate of Cyber Security (DNSC) supports this initiative, given the constant presence of cyber terms in the media. Considering the importance of awareness and education of the younger generation, most frequently exposed to the digital sphere, we appreciate the usefulness and potential of this dictionary. It is addressed to all generations and aims to be a bridge between them. We recommend it, as it represents a reliable source of key definitions and will be continuously updated.

Dan CÎMPEAN, The Director of DNSC



978-630-6771-02-8

Editura Intermedia Group