Co-funded by the Erasmus+ Programme of the European Union

# Module de instruire InCyT

| | |
|---|---|
| **Securitatea informațiilor pentru angajați**<br>**Unitatea 2 Săptămâna 4**<br>**Numele unității: Programe malware și cele mai frecvente atacuri** | |
| ***Activități de învățare*** | ❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte** |
| ***Responsabil de învățare*** | Claudio Fornaro |
| ***Obiectivele activității de învățare*** | 1. Introducere în diferitele tipuri de malware<br>2. Cunoașterea celor mai comune tipuri de atacuri |
| ***Abilități de dobândit*** | • Cunoștințe de bază despre ce este malware și cele mai frecvente atacuri la sistemele informatice<br>Soft Skill 2 - SS2 |
| ***Durata activității de învățare*** | 1 săptămână |
| ***Cerințe de învățare*** | ***Ce e necesar?***<br>• Nu sunt necesare cunoștințe specifice anterioare |

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

## Informații scurte despre modul

Când vine vorba de malware, numele implică deja ceva rău intenționat. Acest termen se referă în general la software conceput în mod intenționat pentru a provoca daune de diferite tipuri, în special (dar fără a se limita la): blocarea serviciilor și comunicațiilor, interceptarea transmisiilor, furtul de informații private (personale, corporative sau guvernamentale) și de identități personale, acces neautorizat la informații sau sisteme, privarea utilizatorilor de acces la informații.
După o parte introductivă, sunt conturate conceptele fundamentale de malware, împreună cu descrierea principalelor tipuri, riscurile pe care le implică și modul în care acestea pot fi atenuate.
A doua parte a modulului își propune să ofere o imagine de ansamblu asupra celor mai frecvente atacuri pe care le poate suferi un sistem, această listă nefiind deloc completă deoarece în fiecare zi sunt descoperite noi tipuri de atacuri. Aceste atacuri sunt încercări de a obține acces la un sistem informatic sau de a întrerupe serviciile acestuia. Descrierea începe de la cele mai obișnuite și mai ușoare atacuri (phishing) până la cele mai complexe: Atacuri cu parole, Buffer Overflow, SQL Injection, Cross-site Scripting (XSS), Cross-Site Request Forgery (CSRF), File Related Attacks, Denial of Service (DoS) și Distributed Denial of Service (DDoS), Man in The Middle (MITM), ARP Spoofing sau ARP Poisoning, DNS Spoofing, Drive-by Attacks,
Reutilizarea acreditărilor, deturnarea sesiunii web, deturnarea sesiunii TCP, falsificarea IP, exploatările zero-day și consecințele scurgerii de cod.

## Conținutul materialului de învățare

În informatică, „hacker” și „cracker” sunt doi termeni care sunt folosiți pentru a indica persoanele cu cunoștințe mari de sisteme informatice. Principala diferență dintre cei doi constă în atitudinea cu care acționează. Un **hacker** (termenul s-a născut în a doua jumătate a anilor 1900 la MIT) acționează prin explorarea sistemelor pentru a înțelege mai bine cum funcționează acestea și încercând să descopere noi defecte pentru a le rezolva și, prin urmare, a crește securitatea unui sistem. Unele acțiuni pot fi doar demonstrative sau din motive etice, dar niciodată pentru profit. Un **cracker**, pe de altă parte, își folosește abilitățile în mod ilegal încercând să pătrundă în sisteme pentru a profita furând date sau într-un mod distructiv.

Hackerii încearcă în mod constant să dobândească noi cunoștințe despre sistemele informatice pentru a le înțelege mai bine sau pentru a le îmbunătăți funcțiile, performanța și securitatea. Unii dintre ei se angajează și în acțiuni demonstrative și etice, dar niciodată pentru profit. Acțiunile hackerilor sunt efectuate aproape întotdeauna fără nicio permisiune, așa că Legea îi pedepsește (cu mari diferențe între țări), din acest motiv hackerii se ascund de obicei în spatele poreclelor. Uneori, companiile înțelepte de securitate sau IT în loc să pună în judecată hackerii, adesea îi angajează pentru a profita de abilitățile și creativitatea lor înalte (eventual după ce și-au plătit o

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

parte din datoria către Justiție). Aceștia sunt apoi utilizați pentru a testa aplicații, sisteme de securitate și programe atât în producție, cât și deja pe piață, pentru a bloca atacurile și pentru a preveni problemele care ar putea apărea în viitor din cauza erorilor de sistem.

*Hackerii adevărați* au o reputație de experți și sunt foarte respectați în comunitatea lor. Competițiile sunt organizate cu scopul de a „piercing" un sistem sau program în cel mai scurt timp posibil. Aceste competiții se numesc hackathon-uri și sunt adesea sponsorizate de giganții industriei computerelor.

Termenul de „cracker" este atribuit lui Richard Stallman (o figură cunoscută a mișcării software liber, creatorul proiectului GNU și membru al comunității hackerilor din anii 1970). A vrut să evite abuzul termenului de „hacker", diferențiind cine a acționat fără nicio dorință de a vătăma și cine, dimpotrivă, acționează pentru a avea profit sau doar pentru a da un prejudiciu. Un cracker este un criminal cibernetic care încearcă să atace sistemele informatice într-un mod neautorizat și ilegal, cu răutate, încercând să profite fraudulos de ele exploatând vulnerabilități necunoscute și rezolvate încă. Crackerii sunt adesea implicați în spionaj industrial, furt de date și blocarea rețelelor și site-urilor web, vandalism etc.

Termenii hacker și cracker au limite subtile care îi împart. De exemplu, o intruziune poate fi considerată un act ilegal pentru unii oameni și nu pentru alții, iar Legea reflectă aceste opinii; dar acest document nu este despre aspecte etice sau legislative. În schimb, trebuie să avem în vedere că astăzi, din păcate, cei doi termeni sunt considerați sinonimi.
**În acest document, vom folosi cu nefericire termenul mai comun și mai folosit hacker pentru ambele categorii, fiind siguri că cititorul înțelept va fi destul de capabil să distingă între un *hacker* și un *cracker*.**

„Hackeri" pot fi clasificați aproximativ în mai multe categorii, cele mai utilizate sunt următoarele.

**Hackerii Black Hat** își folosesc cunoștințele în scopuri rău intenționate sau criminale, având grijă să nu fie urmăriți.

**Hackerii White Hat** testează sistemele pentru a identifica posibilele vulnerabilități și pentru a le elimina pentru a preveni accesul nedorit. Adesea sunt experți în securitate plătiți în acest scop.

**Hackerii de pălărie gri** sunt asemănătoare pălăriilor albe, dar deseori efectuează cercetări asupra vulnerabilităților sistemului fără autorizație și, odată ce aceste vulnerabilități sunt descoperite, le folosesc pentru a forța vânzătorii să remedieze problema, de obicei gratuit. Unii vânzători îi răsplătesc cu bani, alții îi pun în judecată.

**Hackerii sinucigași** sunt de obicei mai puțin competenți decât pălăriile negre/albe, dar acționează din motive ideologice și nu au niciun interes să-și ascundă identitatea.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

**Hackerii sponsorizați de stat** sunt plătiți de un guvern pentru a lansa atacuri cibernetice împotriva unei alte țări; au acces la resurse mari oferite de stat, precum și la protecție împotriva urmăririi penale pentru infracțiunile comise. Acționează pentru a scădea informații confidențiale, planuri sau proiecte, sau pentru a crea tulburări generalizate și a dauna populației, Armatei, conducerii Guvernului, spitalelor, uzinelor de producere a energiei, apă și alimentare cu energie electrică etc. Aceste acțiuni sunt considerate război adevărat.

**Copiii cu scenarii** nu au sau nu au dobândit încă abilități grozave, de obicei folosesc scripturi și instrumente create de alți hackeri. Toți hackerii înainte de a dobândi abilități grozave sunt niște script kiddies.

**Teroriștii cibernetici** sunt indivizi sau grupuri cu intenții ostile care, în general, urmăresc să creeze haos într-o țară; sunt similari cu hackerii sponsorizați de stat, dar nu au (încă) un guvern care să-i sprijine sau sprijinul nu este evident.

## Programe malware

Malware este acronimul lui "**mal**icious soft**ware**", un termen generic care identifică orice program rău intenționat dăunător unui sistem. Malware este software-ul creat de hackeri pentru a-și atinge obiectivele: să câștige bani, să fure date, să întrerupă activitățile etc.

Unul dintre cele mai comune programe malware este așa-numitul **cal troian** (sau pur și simplu **troian**), un program care pare un software util și adesea acționează ca atare, dar poartă o funcție ascunsă care este executată pentru a face împreună cu cea normală activată atunci când aplicația este a început. Acestea sunt adesea programe shareware sau programe sparte care sunt distribuite modificate pentru a transporta calul troian. În alte cazuri, este doar un malware cu un nume înșelător care îl face să pară un software util. Troienii sunt adesea răspândiți prin e-mailuri sau prin descărcarea de programe prin Web și, de obicei, nu se răspândesc singuri pe alte computere. Exemple de coduri rău intenționate sunt *keyloggers* (programe care fură parole și le trimit hackerului), *backdoors* (programe care funcționează ca un server terminal și care permit hackerului de la distanță să acceseze computerul în anumite moduri ocolind procedurile normale de autentificare), *criptominerii* (programe care minează criptomonede), *boți* (prescurtare de la roboți, folosiți, de exemplu, pentru un atac distribuit de denial of service).

**Rootkits** sunt software instalat de malware care încearcă să ascundă prezența unui malware în sine de la detectare; realizează acest lucru prin modificarea sistemelor de operare.

Malware-ul care infectează alt software poate fi un virus sau un vierme. Acestea își iau numele de la modul în care se răspândesc, mai degrabă decât de la orice fel de comportament specific. Un **virus** de computer este un software similar cu calul troian, dar poate produce copii ale lui însuși prin infectarea (introducându-se în) alt software, inclusiv fișierele sistemului de operare. Virusul este răspândit în alte sisteme atunci când software-ul infectat este copiat și rulat pe aceste

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

sisteme.

Similar cu un virus este un **vierme**, acesta este un software de sine stătător care funcționează pe un computer și infectează alte computere prin intermediul rețelei, dar fără a infecta fișiere.

Un **ransomware** este un tip de malware care restricționează accesul la dispozitivul pe care îl infectează, necesitând plata unei răscumpărare pentru a elimina restricția. Principalele tipuri de ransomware sunt: 1) Ransomware de *blocare a ecranului* care blochează ecranele cu o acuzație intimidantă de comportament ilegal și cerând victimelor să plătească o taxă; 2) *Ransomware bazat pe criptare,* unde software-ul rău intenționat un anumit tip de fișiere (imagini, documente) sau toate fișierele de pe o mașină infectată. Când se realizează criptarea completă, un pop-up informează de obicei utilizatorul că (toate) fișierele au fost criptate și că trebuie plătită o taxă pentru a le recupera, de obicei în criptomonedă. Exemple de ransomware bazat pe criptare sunt CryptoLocker și WannaCry. O variantă cunoscută sub numele de **Wiper** arată ca un ransomware, dar doar distruge datele, chiar dacă este adesea necesară o plată.

**Greyware** sunt o categorie diferită de malware: aceste programe pot înrăutăți performanța computerelor și pot provoca riscuri de securitate, se comportă într-un mod enervant sau nedorit, dar de obicei sunt mai puțin periculoase (ceea ce este o părere relativă) decât categoriile anterioare de malware. Spyware (de ex. keylogger, programe care înregistrează toate tastele apăsate pe tastatură), adware (ferestre de reclame pe ecran sau în browser, dialer frauduloase etc.), Programe potențial nedorite (PUP-uri, aplicații pe care utilizatorul le-a instalat doar din cauza o greșeală într-o fereastră de acord în timpul instalării unui alt program) sunt forme tipice de greyware. Pot fi programe de sine stătătoare sau pluginuri pentru alte programe, de exemplu browsere. Ei se limitează uneori la modificarea setărilor altor programe, de exemplu pentru a aduce utilizatorul la un anumit site de anunțuri sau pentru a afișa o pagină de anunțuri de fiecare dată când browserul este pornit sau ocazional.

**Antivirusuri**

Pe măsură ce motoarele antivirus își îmbunătățesc puterea de a detecta malware, se utilizează o combinație de diferite tehnici pentru a încerca să evite detectarea și analiza. Programele malware mai recente sunt capabile să adopte contramăsuri sofisticate, cum ar fi:

- analizarea și detectarea prin amprentare a mediului pentru a adopta metode specifice de ascundere;
- încercarea de a se înfunda pentru a încurca detectarea antivirus pe baza semnăturii malware;
- adoptarea unei evadari bazate pe timp pentru a păcăli detectarea unui comportament anormal, malware-ul este în mod normal inactiv și se activează singur în perioade foarte specifice (de exemplu în timpul procesului de boot) sau în urma anumitor acțiuni întreprinse de utilizator.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

O tehnică de evaziune foarte greu de descoperit este programul *malware fără fișiere* sau *amenințările volatile avansate*. Acest tip de malware rulează în memorie și nu necesită un fișier pentru a funcționa. Utilizează instrumentele de sistem existente pentru a-și desfășura activitatea. Absența oricărui fișier în sistemul de fișiere le face destul de dificil de detectat și analizat, cu excepția, parțial, a acelor instrumente de monitorizare care verifică utilizarea resurselor și comportamentul sistemului. Creșterea acestui tip de atacuri este foarte mare.

**Riscuri**

Software-ul vulnerabil poate fi exploatat pentru a obține privilegii sau pentru a ocoli apărarea, până când problema este corectată; acesta este principalul motiv pentru care software-ul ar trebui să fie actualizat, în special sistemul de operare. Firewall-urile și sistemele de detectare a intruziunilor monitorizează tiparele de trafic pe LAN.

Regula celui mai mic privilegiu spune că utilizatorii și programele nu ar trebui să aibă mai multe privilegii decât au nevoie, altfel malware-ul poate profita de acest lucru..

**Atenuare**

Software-ul antivirus blochează și, eventual, elimină unele tipuri de malware, ele pot oferi protecție în timp real împotriva instalării software-ului malware pe un computer și o scanare completă a fișierelor și a configurației (de exemplu, registrul Windows) în căutarea potențialelor amenințări.

Firewall-urile personale analizează orice conexiune la rețea și pot identifica activități neobișnuite.

Sandboxing rulează o aplicație izolată de restul sistemului, unele aplicații pot rula o anumită aplicație, în timp ce în sistemele mai complexe o mașină virtuală ar putea fi mai potrivită.

Scanările de vulnerabilități ale site-urilor web sunt efectuate de unele software antivirus împotriva unei liste de site-uri periculoase bine-cunoscute și împiedică conectarea la acestea.

Segregarea rețelei împarte o rețea în părți și permite doar acel trafic între ele despre care se știe că este legitim, astfel încât software-ul rău intenționat să se răspândească în rețea. Tehnicile moderne de rețea definită de software sunt capabile să implementeze această segregare.

Izolarea „decalajului” sau „rețeaua paralelă” aduce segregarea rețelei la limită, izolând complet o porțiune a rețelei și oferind controale îmbunătățite asupra intrării și ieșirii de software și date din lumea exterioară. Nici această soluție nu este cea definitivă, întrucât software-ul și datele trebuie să intre în sistemul izolat, de exemplu pentru corecție. Un exemplu binecunoscut de încălcare a unei rețele izolate este faimosul malware **Stuxnet** care a fost introdus în mediul țintă prin

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

intermediul unităților USB uitate „ocazional” în apropiere, preluat de personalul fabricii și introdus în computerele fabricii pentru a vedea conținutul. Stuxnet are trei module: un vierme care controlează atacul; un fișier link care execută automat viermele atunci când este introdus într-un computer Windows; și o componentă rootkit responsabilă pentru ascunderea tuturor fișierelor și proceselor rău intenționate, pentru a preveni detectarea. Alte modalități de traversare a golurilor de aer analizează emisiile electromagnetice, termice și acustice.

## Cele mai comune tipuri de atacuri

Această parte descrie unele dintre cele mai comune atacuri la un sistem informatic. Nu este și nu poate fi complet deoarece varietatea de atacuri este extrem de mare, fiecare are multe variante și multe atacuri și variante sunt create și descoperite (și rezolvate) în fiecare zi. Aceasta înseamnă că scopul acestei părți nu este de a oferi o clasificare completă, ci de a oferi o idee despre nivelul ridicat de cunoștințe necesar atât pentru comiterea, cât și pentru a contracara atacurile..

### Phishing

Atacurile de tip phishing sunt foarte frecvente și ușor de efectuat. Acestea constau în trimiterea de e-mailuri care par să provină de la un expeditor de încredere, cum ar fi un coleg sau o bancă, cu scopul de a păcăli victima să facă un anumit tip de operațiune.

Atacatorul încearcă să convingă victima să deschidă un atașament sau furnizează un link care duce la o pagină foarte asemănătoare cu cea inițială, de exemplu o pagină de pornire a unei bănci, dar creată de atacator, apoi să îi ceară victimei să-și introducă acreditările. Pentru a optimiza acest tip de atac există o serie întreagă de tehnici care fac parte din așa-numita inginerie socială, deoarece, în acest caz, vulnerabilitatea sistemului informatic urmează să fie identificată în utilizatorul însuși, care este înșelat și neintenționat. oferă acreditările sale.

Pentru a vă apăra împotriva acestor atacuri, este necesară o inspecție atentă a legăturii (este aproape imposibil să distingem între L minuscul „l”, un I mare „I” și cifra „1” sau să observați diferența dintre . it și .lt într-o adresă URL). Mai mult, trebuie să știți că companiile serioase nu pun niciodată link-uri în e-mailul lor care să aducă la o pagină de conectare.

### Atacurile cu parole

Pentru a obține parole de la o victimă, un hacker poate încerca ingineria socială, așa cum s-a văzut în paragraful anterior, sau poate lansa un atac cu parolă. Parolele sunt de obicei stocate ca hashuri, iar hashurile sunt foarte greu de inversat. Există în esență două cazuri: parola criptată este disponibilă sau este necunoscută și acest tip de atac poate fi efectuat în moduri diferite:

- **Atacul de forță brută:** în acest caz programul va încerca toate combinațiile posibile de

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

caractere dintr-un set;

- **Atacă cu dicționar:** programul va testa o secvență de parole utilizate în mod obișnuit (dicționar);
- **Atacă cu fișiere curcubeu:** un tabel curcubeu este un tabel precalculat care listează ieșirea funcțiilor hash ale parolei. Utilizarea unei derivații cheie care folosește o sare face ca acest atac să fie imposibil.

Managerii de sistem ar trebui să testeze în mod regulat fișierele de parole ale utilizatorilor sistemelor lor cu programe capabile să efectueze atacuri cu parole, atât prin forță brută, cât și prin dicționar.

Pentru a se proteja împotriva acestor atacuri, un sistem ar trebui să verifice calitatea parolei înainte de a permite utilizatorului să o seteze, necesitând utilizarea unui număr minim de caractere (de exemplu, 10) din seturi diferite (litere mari și mici, cifre, caractere de punctuație). ). Dacă parola introdusă este incorectă pentru unele încercări ulterioare, este oportun să adoptați o politică de blocare a contului sau de întârziere la următoarea încercare, împiedicând astfel atacatorul să încerce rapid multe combinații.

**Buffer Overflow**

Buffer overflow (sau depășire) apare atunci când trimiteți mai mulți octeți la un buffer decât poate stoca acesta, acești octeți depășesc bufferul destinat să-i rețină și modifică alți octeți sau, în funcție de sistemul de operare și tipul de fișier, chiar injectează codul mașinii executabil. În timp ce sistemele de operare moderne pot împiedica rularea unui fișier executabil cu date și coduri amestecate, acest lucru nu este adevărat pentru sistemele de operare mai simple, adesea găsite în sistemele încorporate, unde în multe cazuri nu există deloc un sistem de operare..

**Injecție SQL**

Un atac foarte comun este SQL Injection. Limbajul SQL este folosit în bazele de date relaționale; prin urmare, aceste tipuri de atacuri vizează furtul de informații. În esență, datorită naturii interpretate a interogării SQL, codul SQL rău intenționat este trimis către o pagină web despre care se știe că folosește o interogare SQL pentru a aduna datele pentru a le prezenta utilizatorului. Codul SQL rău intenționat modifică (uneori doar adăugând alte părți sintactice) interogarea SQL predefinită care rezultă este o interogare modificată care expune alte date decât cele pentru care a fost scrisă interogarea originală.

Deși prevenirea acestui tip de atacuri nu este complexă (de exemplu împiedicarea accesului la alte tabele ale bazei de date în afară de cele necesare pentru a efectua interogarea originală), injectarea SQL este încă unul dintre cele mai frecvente atacuri..

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

**Cross-site Scripting (XSS)**

Într-un cross-site scripting (XSS), scripturile executabile rău intenționate sunt injectate în codul unei aplicații web de încredere (plugin) sau al unei pagini de site web, cu rezultatul că sunt descărcate de alte persoane (spectatori). Când serverul trimite înapoi pagina web compromisă, browserul web al utilizatorului consideră că aceasta a fost livrată dintr-o sursă de încredere și apoi codul injectat nu este identificat ca fiind rău intenționat. Conținutul activ este de obicei un script (cod de programare care este executat de browser) care poate permite unui atacator să obțină acces la conținutul paginii sensibile, cookie-uri de sesiune sau alte informații pe care browserul le păstrează în numele utilizatorului. Cu atacurile XSS, este posibil să furați date sensibile ale tuturor utilizatorilor care accesează site-uri infectate. De exemplu, furtul SESSIONID-ului unei sesiuni de site (care se află în cookie-urile browserului utilizatorului care la rândul lor sunt folosite pentru a evita ca fiecare conexiune la același site să necesite autentificare dincolo de prima), ar putea permite unui impostor să ocolească faza de autentificare și operează ilicit în numele utilizatorului.

**Cross-Site Request Forgery (CSRF)**

Un CSRF este o solicitare http involuntară (dorită de atacator) către un site web efectuată de un utilizator deja autentificat pe acel site web; site-ul web în acest moment va executa cererea fără alte verificări, permițând atacatorului să-și efectueze atacul. Acest tip de atac permite modificarea datelor utilizatorului sau efectuarea de tranzacții nedorite, precum achiziții nedorite, dacă ar fi de exemplu un site de comerț electronic. Atacatorul trebuie să aibă cunoștințe foarte bune despre site-ul în cauză pentru a efectua un atac CSRF.

Un exemplu de atac CSRF este efectuat prin schimbarea unei adrese URL. De exemplu, codul sursă al paginii web este analizat de către malware pentru a găsi linkul „Schimbare parolă” și a verifica dacă este folosită metoda http GET, apoi se poate forma o nouă legătură cu o nouă parolă (aleasă de atacator) și trimis victimei, de exemplu printr-un atașament de e-mail. Dacă se face clic pe link și se întâmplă ca victima să fie deja autentificată pe site, este activată o procedură ascunsă de începere a schimbării parolei, dând efectiv contul hackerului. Metodele bune de schimbare a parolei cer să inserați și vechea parolă (și metoda GET nu este folosită). Mai mult, utilizarea unei metode CAPTCHA (un test pentru a verifica dacă utilizatorul este un om sau un computer) este destul de eficientă.

**Atacurile legate de fișiere**

Există multe tipuri de atacuri asupra fișierelor. Cele mai cunoscute vulnerabilități sunt:

- **Referințe nesigure la obiecte directe:** apare atunci când o aplicație solicită o resursă de la un server apelând-o pe numele ei, dar permițând utilizatorului să o modifice pe aceasta din

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

urmă, pentru a solicita o altă resursă.

- **Includerea fișierelor locale (LFI):** exploatează vulnerabilitatea funcțiilor GET și POST ale limbajului PHP pentru a insera fișiere rău intenționate în cod.
- **Traversarea căii:** permite unui utilizator rău intenționat să acceseze directoare cu acces limitat și să execute comenzi. Adesea, acestea sunt folosite în urma unui LFI pentru a pătrunde adânc în sistem și pentru a obține privilegiile necesare.

Pentru a vă proteja împotriva acestor tipuri de atacuri, este important să preveniți încărcarea fișierelor pe servere, să dezactivați execuția codului de la distanță, să restricționați accesul PHP la sistemul de fișiere și să actualizați periodic software-ul.

## Denial of Service (DoS) și Distributed Denial of Service (DDoS)

Poate cele mai cunoscute atacuri de rețea, atacurile DoS constau practic în trimiterea multor pachete pentru a bloca posibilitatea de a primi alte pachete, împiedicând astfel accesul la mașină pentru utilizatorii obișnuiți, blocând serviciile oferite.

Diferența dintre un atac DoS și un atac DDoS constă în faptul că în primul caz se folosește o singură gazdă pentru a efectua atacul, în timp ce în al doilea atacul este efectuat cu mai multe gazde (numite zombi) în același timp. Aceste gazde au fost infectate anterior de un malware și la comanda atacatorului pornesc conexiunea la mașina victimă.

Printre atacurile DoS, ne putem aminti:

- **Syn-Flood**: constă în trimiterea unui număr mare de cereri de conectare. Mașina care primește o solicitare (un pachet SYN) de la un client va răspunde clientului prin trimiterea unui mesaj, alocarea unor resurse pentru această conexiune și așteptarea pachetului de confirmare (care nu va ajunge niciodată). Prin urmare, cererea de conectare rămâne activă până când apare un timeout. Dacă au fost pornite toate conexiunile posibile, serviciul oferit de aparat nu va mai fi disponibil. Timeout-ul are loc în câteva secunde, dar rata uriașă de solicitări menține mașina înfundată.
- **Smurf**: acest atac este o combinație de falsificare IP și solicitări ICMP. IP spoofing se referă la trimiterea unui pachet IP în care IP-ul expeditorului este falsificat. Prin trimiterea continuă a cererilor de eco ICMP (mesajul trimis prin comanda ping, folosit pentru a verifica dacă o mașină este accesibilă) pentru a difuza adrese IP după ce a înlocuit adresa IP a expeditorului cu adresa IP a victimei, mașina victimă va primi un răspuns pentru fiecare solicitare. de la orice gazdă activă în rețea, blocând astfel conexiunea (flood). Pentru a preveni apariția acestor atacuri, este posibil să dezactivați în routere redirecționarea adreselor IP de difuzare.
- **Ping of death**: constă în trimiterea unui pachet fragmentat cu o dimensiune IP totală mai mare decât maximul permis unei mașini victimă, odată ce mașina reasamblează pachetul poate suferi depășiri de buffer..

Este obișnuit ca un atac DDoS să folosească o rețea botnet care este mii sau milioane de computere infectate cu malware, care, la comanda atacatorului, execută un atac Syn-Flood la

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

unison pe un server victimă..

**Man in The Middle (MITM)**

Prin MITM ne referim la o întreagă tipologie de atacuri care au ca scop interceptarea, analizarea și retransmiterea unei comunicări între două părți care cred că comunică direct între ele.

Acest tip de atac este efectuat de obicei folosind IP spoofing: sniffer-ii de rețea interceptează o conexiune și noi pachete create prin schimbarea adresei IP a expeditorului și destinatarului, astfel încât expeditorul să trimită date atacatorului care, la rândul său, le va retrimite către destinatarului și invers.

Există multe modalități de a vă apăra împotriva acestor tipuri de atacuri; cea mai eficientă și utilizată astăzi este adoptarea criptării *end-to-end*, în care subiecții finali efectuează criptarea/decriptarea și toate sistemele intermediare pot vedea doar datele criptate.

**ARP Spoofing or ARP Poisoning**

Protocolul de rezoluție a adresei (ARP) permite comunicațiilor de rețea să ajungă la un anumit dispozitiv din rețeaua locală. Este folosit pentru a mapa adresele IP la adresele Media Access Control (MAC) (utilizate pentru a identifica gazdele dintr-o rețea LAN). O gazdă trebuie să folosească protocolul ARP pentru a cunoaște adresa MAC a routerului/gateway-ului pentru a se conecta la Internet. Fiecare gazdă menține un cache ARP pentru a mapa perechea IP/MAC deja solicitată și cunoscută. Dacă gazda nu cunoaște adresa MAC pentru o anumită adresă IP locală, trimite un pachet de solicitare ARP de difuzare, întrebând toate celelalte gazde din rețeaua locală care au adresa IP. Gazda cu acea adresă IP va răspunde, furnizând astfel adresa MAC.

Un atac de falsificare/otrăvire ARP poate fi clasificat ca un atac MITM de rețea locală. Atacatorul trebuie să aibă acces la rețeaua locală și o scanează pentru a determina adresele IP ale routerului și ale altei gazde. Atacatorul trimite răspunsuri ARP falsificate care fac routerul și gazda să creadă că adresa MAC a atacatorului este cea a gazdei și, respectiv, a routerului. Acest lucru păcălește atât routerul, cât și stația de lucru să se conecteze la mașina atacatorului, în loc să se conecteze unul la celălalt. Pe măsură ce cele două dispozitive își actualizează intrările în cache ARP, gazda și routerul comunică cu atacatorul în loc să fie direct unul cu celălalt.

**DNS Spoofing**

Sistemul de nume de domeniu (DNS) este sistemul de denumire utilizat pentru a converti numele de Internet (mai corect FQDN - Nume distinctive complet calificate, de exemplu, www.server.net) în adresa IP corespunzătoare. Sistemul este ierarhic și descentralizat cu unele servere de nivel superior. De fiecare dată când un sistem încearcă să ajungă la o resursă de rețea, se realizează o conexiune la un server DNS pentru a converti numele resursei într-o adresă IP. Înregistrările de

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

resurse conțin de obicei informații administrative și alte date utilizate, de exemplu, de serverele de e-mail.

Un hacker va dori să modifice înregistrările DNS pentru a trimite trafic către un site web fals sau „falsificat” în loc de cel legitim. Mașina falsificată ar putea apoi să facă atacuri MITM, falsificare etc. Pentru a preveni falsificarea DNS, serverele DNS trebuie menținute la zi.

**Atacurile de tip drive-by**

Într-un atac drive-by, codul rău intenționat este încorporat într-un site web nesigur. Când pagina infectată este vizitată, scriptul este executat automat pe computerul victimei și îl compromite, nu este nevoie să faceți nimic pe site sau să introduceți vreo informație. În acest caz, utilizarea unui antivirus actualizat și decent și/sau a unui firewall personal este singura protecție, deoarece pot detecta din baza lor de date dacă un site este nesigur înainte ca un utilizator să îl viziteze.

**Reutilizarea acreditărilor**

Necesitatea de a avea acreditări pentru mai multe servicii îi determină pe utilizatori să refolosească unele dintre parolele lor. Odată ce un atacator are o listă de nume de utilizator și parole ale site-urilor web sau serviciilor compromise (de exemplu, obținute de pe Dark Web), este posibil ca același utilizator să folosească aceeași pereche utilizator/parole pe alte sisteme. Acest lucru va reduce foarte mult numărul de parole de verificat cu un atac de dicționar. Pentru a contrasta acest tip de atac, aceleași contramăsuri adoptate pentru a contracara atacurile cu parole sunt eficiente. Atunci când sunt necesare multe parole complexe, unii oameni consideră că managerii de parole sunt folositori.

**Deturnarea sesiunii web**

Un atac de tip Session Hijacking constă în exploatarea token-urilor de sesiune, utilizate de browserul web ca mecanisme de control al sesiunii. Serverul web trebuie să relaționeze diferite conexiuni de la același utilizator, deoarece pentru fiecare pagină web este creată o conexiune TCP pentru fiecare element (text, imagini etc.). Cea mai utilizată metodă se bazează pe un token pe care Web Server-ul îl trimite browserului client după o autentificare cu succes a clientului. Un token de sesiune este doar un identificator, un șir unic lung și poate fi folosit pentru a evita necesitatea efectuării unei proceduri de autentificare pentru fiecare conexiune. Acest atac este efectuat prin furtul sau prezicerea unui token de sesiune valid pentru a obține acces neautorizat la serverul web.

**Deturnarea sesiunii TCP**

Conexiunile TCP trebuie să garanteze livrarea pachetelor în ordinea succesivă corectă, pentru a

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

realiza acest lucru utilizează pachete de confirmare și numere de secvență. Aceste pachete de confirmare sunt doar numere care sunt incrementate într-un fel după strângerea de mână inițială în trei căi. Scopul hijacker-ului de sesiune TCP este de a crea o stare în care clientul și serverul nu pot face schimb de date; permițându-i să formeze pachete acceptabile pentru ambele capete, care imită pachetele reale. Astfel, atacatorul poate prelua controlul asupra sesiunii. Dacă secvența poate fi prezisă, un atacator poate trimite pachete falsificate care sunt recunoscute ca fiind valide de la gazda victimei.

**IP Spoofing**

O falsificare a IP este de obicei efectuată cu un atac DoS: un număr mare de conexiuni blochează serverul legitim și, în același timp, un server fals își setează adresa IP cu numărul serverului legitim. Prin urmare, utilizatorul este condus către serverul fals care trimite mesaje cu o adresă IP care indică faptul că mesajul provine de la o gazdă de încredere.

Blind Hijacking: În cazurile în care rutarea sursei este dezactivată, deturnarea sesiunii poate folosi și deturnarea oarbă în cazul în care își injectează datele rău intenționate în comunicațiile interceptate în sesiunea TCP. Se numește orb pentru că nu poate vedea răspunsul; deși piratatorul poate trimite datele sau comenzile, practic ghicește răspunsurile clientului și serverului.

**Exploatare zero-day**

Strict vorbind, exploatarea zero-day nu este un atac specific, deoarece infractorii cibernetici află despre o vulnerabilitate care tocmai a fost descoperită în anumite software și sisteme de operare și apoi vizează organizațiile care folosesc acel software înainte ca o soluție să devină disponibilă..

**Scurgere de cod**

Codul sursă al aplicațiilor poate conține uneori informații sensibile și oferă informații valoroase pentru un atac cibernetic, pe lângă valoarea economică intrinsecă a codului în sine.

## Întrebări:

În fisier separat.

## Atasamente:

În fisier separat.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

## Referințe:

Fiecare subiect are propria sa pagină pe Wikipedia, uneori deja prea amănunțită pentru scopurile acestui curs; cărțile sunt prea specializate și sunt utile doar după o pregătire foarte profundă pe tema specifică.

1. Programe malware sau software rău intenționat
   URL: https://www.malwarebytes.com/malware
2. Securitate cibernetică pentru toată lumea.
   https://www.avast.com/c-malware
3. Ce sunt amenințările de securitate cibernetică?
   URL: https://www.imperva.com/learn/application-security/cyber-security-threats/
4. 21 de amenințări de top pentru securitatea cibernetică și cum poate ajuta inteligența contra amenințărilor
   URL: https://www.exabeam.com/information-security/cyber-security-threat/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.