4. ATACURI CIBERNETICE

Preliminarii

Impactul atacurilor cibernetice este tot mai mare, influențând sistemele informatice, economiile statelor și societatea per ansamblu. Astfel, în tema 4, "Atacuri cibernetice", vor fi tratate subiecte în care vor fi clasificate atacurile cibernetice comune, ce au loc în rețea și asupra aplicațiilor moderne. Vor fi analizate diverse caracteristici ale atacurilor cibernetice prin analiza și discutarea exemplelor relevante.

Scopul:

- s*tudierea și analiza atacurilor cibernetice comune cu scopul implementării cerințelor de securitate adecvate pentru prevenirea, detectarea și răspunsul la incidente în cadrul organizațiilor.*

Obiectivele educaționale:

- *identificarea și clasificarea atacurilor cibernetice;*
- *analiza impactului atacurilor cibernetice asupra securității rețelelor de comunicații electronice;*
- *analiza impactului atacurilor cibernetice asupra aplicațiilor utilizate în cadrul organizațiilor.*

Finalitățile de referință:

- *înțelegerea contextului în care au loc atacurile cibernetice;*
- *cunoașterea caracteristicilor definitorii ale atacurilor în rețea și ale atacurilor asupra aplicațiilor;*
- *aplicarea cunoștințelor dobândite pentru identificarea atacurilor cibernetice;*
- *prevenirea atacurilor cibernetice răspândite.*

Modalitățile de evaluare

Evaluarea masteranzilor se va efectua în baza testelor formative realizate pe parcursul semestrului de studiu, care vor conține întrebări de tip grilă, întrebări deschise și studii de caz. De asemenea, masteranzii vor îndeplini sarcini practice individuale sau de grup și vor prezenta oral o temă relevantă domeniului de securitate cibernetică. La finele semestrului masteranzii vor susține un examen care va acoperi toate temele din acest suport de curs.

4.1. Atacuri în rețea

Infrastructurile critice, cum ar fi rețelele de energie, comunicațiile, transportul și serviciile financiare, sunt ținte frecvente ale atacurilor cibernetice. Un atac cibernetic asupra acestor sisteme poate avea consecințe devastatoare, inclusiv întreruperi ale serviciilor esențiale, pierderi financiare masive și chiar riscuri pentru siguranța publică.

Companiile pierd miliarde de dolari anual din cauza atacurilor cibernetice. Costurile includ nu doar pierderi directe, cum ar fi furtul de bani sau proprietate intelectuală, ci și costuri indirecte, cum ar fi pierderea încrederii clienților, amenzile de reglementare și cheltuielile pentru recuperarea datelor și sistemelor.

Atacurile cibernetice pun în pericol datele personale și confidențiale ale utilizatorilor. Aceste date pot fi utilizate pentru furtul de identitate, fraudă și alte activități ilicite.

Prin studierea atacurilor cibernetice, organizațiile pot implementa măsuri de securitate mai eficiente pentru a preveni pierderile financiare, ajută la dezvoltarea de strategii și tehnologii pentru protejarea infrastructurii critice de stat și la dezvoltarea unor metode de

protecție a datelor, la implementarea unor politici de securitate pentru a proteja confidențialitatea informațiilor [15].

Odată cu utilizarea tot mai multă a Internetului, un loc cu totul aparte îl au atacurile asupra rețelelor de comunicații electronice, deoarece dacă este afectat un singur dispozitiv riscurile pentru organizație nu sunt atât de mari, pe când dacă exploatând o singură vulnerabilitate a rețelelor de comunicații electronice pot fi afectate simultan mii de dispozitive terminale, atunci riscurile de securitate și impactul acestor atacuri este unul colosal. Cele mai comune atacuri în rețele sunt bazate pe inundare, interceptare și impersonare, sau reprezintă un mix dintre aceste atacuri [16]. Cel mai cunoscut atac de inundare este desigur DoS (Denial of Service) și DDoS (Distributed Denial of Service), de interceptare a comunicațiilor sunt Packet Sniffer-ele și atacurile MitM (Man in the Middle) și de impersonare sunt falsificarea adresei logice IP, a adresei fizice MAC, a tabelului ARP și a serviciului DNS.

4.1.1. Atacuri de inundare

Atacuri DoS/DDoS

Pentru a înțelege mai bine atacurile DoS/DDoS se va examina drept exemplu un profesor la ore care este asaltat de către un student pentru a răspunde la o anumită întrebare. Studentul insistă să se discute mai detaliat un anumit subiect sau o neclaritate apărută și astfel profesorul trebuie să răspundă la acea întrebare, iar un student timid nu mai poate să întrebe profesorul, fiindcă acesta este concentrat pentru a răspunde studentului care a avut mai mult curaj. Un alt exemplu relevant poate fi un ”flash mob” organizat la universitate pentru a promova o anumită idee, de salvare a planetei de exemplu. În acest caz, doi prieteni nu vor mai putea discuta în continuare un anumit subiect, deoarece vocile care vor scanda anumite replici în jur îi vor încurca să continue o discuție privată, ei vor fi ”forțați” oarecum să se implice în activitatea colectivă. Aceste două exemple reflectă foarte bine cum au loc atacurile de tip DoS și DDoS (figura 4.1). Primul exemplu reflectă cum are loc un atac de tip DoS prin care un sistem informatic nu poate răspunde utilizatorilor autorizați, deoarece este asaltat de cereri din partea atacatorului, iar în cel de-al doilea exemplu este prezentat un model după care au loc atacurile DDoS, când un sistem informatic trebuie să răspundă la cererile ce vin din multiple surse și nu poate furniza servicii utilizatorilor autorizați. Majoritatea atacurilor de astăzi sunt de tip DDoS, adică sunt utilizate sute și mii de calculatoare zombi pentru a cauza refuzul serviciului și a inunda un anumit dispozitiv cu cereri false.

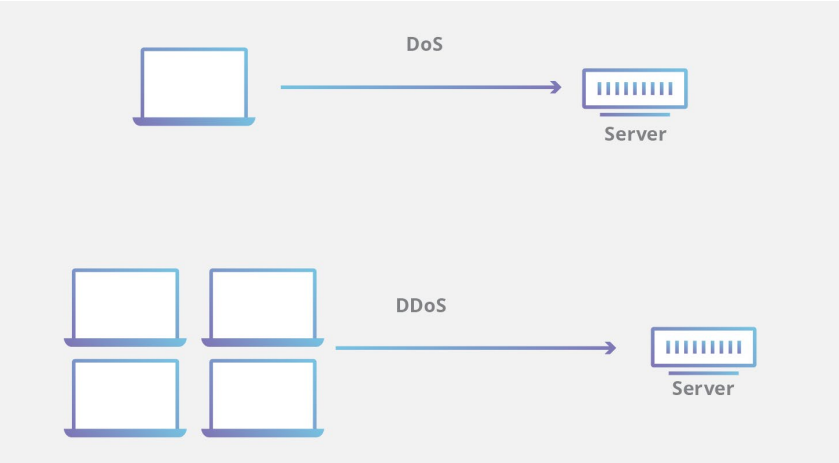

Fig. 4.1. Atacuri DoS și DDoS

Există diferite tipuri de atacuri DoS. Un atac *ping flood* folosește mesaje de control pe internet, prin protocolul ICMP care este un protocol de nivel de rețea ce face parte din suita protocoalelor TCP/IP, pentru a inunda o victimă cu pachete, după cum este reprezentat în

figura 4.2. ICMP este în mod normal utilizat pentru diagnosticarea rețelei, cum ar fi stabilirea dacă un sistem gazdă este activ sau pentru a determina calea folosită de un pachet pentru a ajunge la gazdă. Utilitarul ping trimite o cerere de ecou ICMP către o gazdă. Gazda răspunde cu un mesaj de răspuns ecou ICMP, indicând că este activ. Într-un atac ping flood, mai multe calculatoare trimit simultan un număr mare de solicitări ICMP, copleșind un server (precum și rețeaua) în măsura în care acesta nu poate răspunde suficient de repede și va renunța la conexiunile legitime cu alți clienți, refuzând orice conexiuni noi. O hartă în timp real a atacurilor DDoS la nivel mondial poate fi analizată accesând www.digitalattackmap.com.

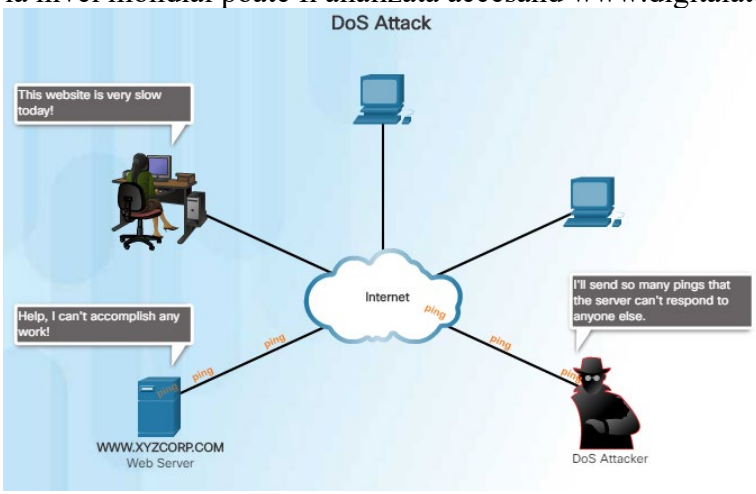

Fig. 4.2. Cereri ICMP în atacurile Dos/DDoS [3]

O altă versiune a atacului DoS păcălește dispozitivele să răspundă la solicitări false adresate unei victime. Acest tip de atac mai este numit *atac smurf*, un atacator transmite o solicitare ping către toate calculatoarele din rețea, dar schimbă adresa de la care a venit cererea pe adresa calculatorului victimei (această uzurpare a identității altui calculator sau dispozitiv se numește spoofing sau impersonare). Acest lucru face să pară că calculatorul victimei cere un răspuns. Fiecare dintre calculatoare trimite apoi un răspuns către calculatorul victimei, astfel încât acesta este rapid copleșit de numărul mare de cereri, apoi se blochează sau devine indisponibil utilizatorilor legitimi.

O altă variație a atacurilor DoS este *atacul prin inundare SYN* (figura 4.3), care profită de procedurile de inițiere a unei sesiuni între două dispozitive. În condițiile rețelei, folosind TCP/IP, un dispozitiv contactează un server de rețea cu o solicitare, cum ar fi pentru a afișa o pagină web sau pentru a deschide un fișier. Această solicitare utilizează un mesaj de control, numit mesaj de sincronizare SYN, pentru a inițializa conexiunea. Serverul răspunde cu propriul său SYN împreună cu o confirmare (ACK) că a primit cererea inițială, numită SYN+ACK. Serverul așteaptă apoi un răspuns ACK de la dispozitiv, care indică faptul că a primit SYN al serverului. Pentru a permite o conexiune lentă, serverul ar putea aștepta o perioadă de timp pentru răspuns. Când dispozitivul răspunde, transferul de date poate începe.

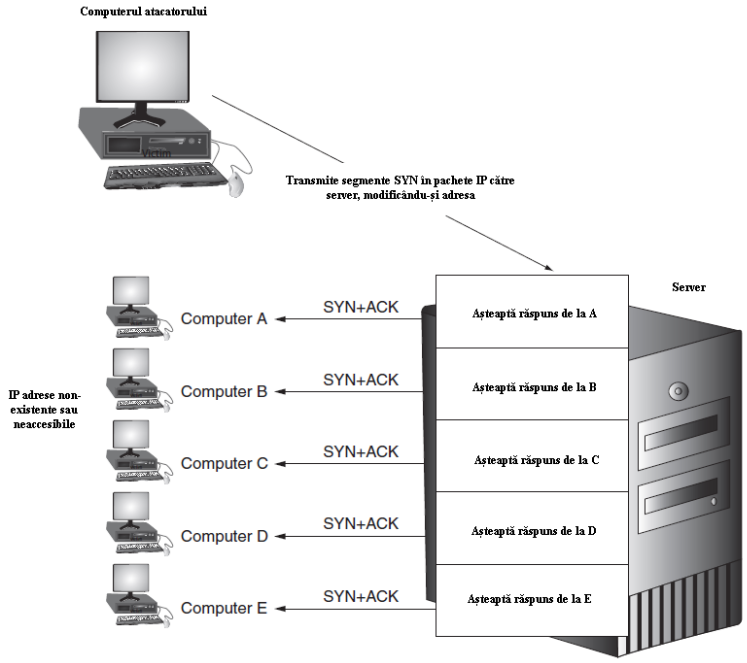

Fig. 4.3. Atacuri de inundare SYN

Într-un atac SYN flood împotriva unui server web atacatorul trimite segmente SYN în pachete IP către server. Cu toate acestea, atacatorul modifică adresa sursă a fiecărui pachet cu adrese care nu există sau nu pot fi contactate. Serverul ține ”linia ocupată” și așteaptă un răspuns (care nu vine) în timp ce primește mai multe cereri false și păstrează mai multe căi deschise pentru răspunsuri. După o perioadă scurtă de timp, serverul își epuizează resursele și nu mai poate răspunde solicitărilor legitime sau nu mai poate funcționa corect.

Simptomele care definesc atacurile DoS [17] (pentru un utilizator legitim) includ următoarele:

- incapacitatea de a accesa un site web;
- întârziere în accesarea serviciului online;
- întârzieri mari în deschiderea fișierelor pe site-urile web;
- creșterea volumului de e-mailuri spam;
- degradarea performanței serviciilor de rețea.

Este mai dificil a preveni atacul DDoS decât atacul DoS obișnuit. În cazul acestui atac, mai multe calculatoare din diferite regiuni geografice devin parte a atacului fără ca proprietarul calculatorului să cunoască acest lucru. Atacurile DDoS sunt efectuate în moduri diferite. Mai jos sunt enumerate principalele tipuri de atacuri DdoS:

- atacurile la nivel de aplicație bazate pe conexiune, adică HTTP, DNS, servere web și altele;
- atacurile volumetrice fără conexiune de la mai multe botnet-uri;
- atacurile de epuizare a tabelului de stare;
- toate tehnicile utilizate în atacurile DoS.

4.1.2. Atacuri de interceptare

Packet Sniffer

Ascultarea online este similară cu spionarea unei persoane din lumea reală. Infractorii cibernetici examinează tot traficul de rețea care trece prin placa interfeței de rețea, indiferent cui i se adresează traficul. Rău-făcătorii analizează infrastructura de rețea folosind aplicații software, hardware sau o combinație a ambelor [18]. După cum se arată în figura 4.4, sniffing inspectează tot traficul de rețea sau filtrele pe baza unui anumit protocol, serviciu sau chiar set

de caractere, cum ar fi un ID de utilizator sau o parolă. Unii analizatori de trafic de rețea pot inspecta întregul trafic și chiar îl pot modifica parțial sau total. Există aspecte pozitive în sniffing. Administratorii de rețea pot folosi astfel de dispozitive pentru a analiza traficul de rețea, pentru a identifica problemele de lățime de bandă și pentru a depana alte probleme ale infrastructurii rețelei. Securitatea fizică joacă un rol important în prevenirea instalării sniffer-urilor de trafic în rețeaua internă a unei organizații.

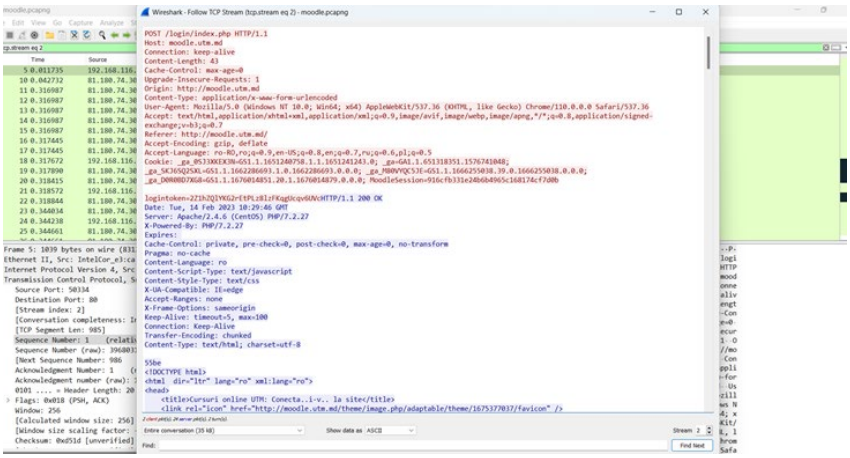

Fig. 4.4. Analizator de traffic, Wireshark

Man-in-the-Middle

Presupunem că Ana, o elevă de liceu, este în pericol să primească o notă proastă la matematică. Profesorul ei, dl Ciobanu, trimite o scrisoare părinților Anei prin care le solicită o întrevedere cu privire la pregătirea insuficientă a fetei. Cu toate acestea, Ana așteaptă corespondența și ia scrisoarea din cutia poștală înainte ca părinții ei să vină acasă. Ea o înlocuiește cu o scrisoare falsă de la dl Ciobanu care o complimentează pentru rezultatele ei la matematică, apoi îi transmite profesorului o scrisoare falsă din partea părinților, prin care aceștia refuză întrevederea cu profesorul. Într-un final, părinții sunt fericiți pentru performanțele Anei, iar profesorul este nedumerit de ce părinții au refuzat întrevederea, fiind dezinteresați de situația școlară a fiicei lor.

Atacurile „man-in-the-middle” bazate pe tehnologie sunt efectuate prin rețele, însă utilizează aceleași procedee ca în situația descrisă mai sus. Acest tip de atac face să pară că două calculatoare comunică între ele, când de fapt ele trimit și primesc date, care sunt interceptate de un calculator terță, sau „omul din mijloc” [19]. În figura 4.5, calculatorul victimei și serverul comunică fără să cunoască că un atacator le interceptează transmisiunile de date.

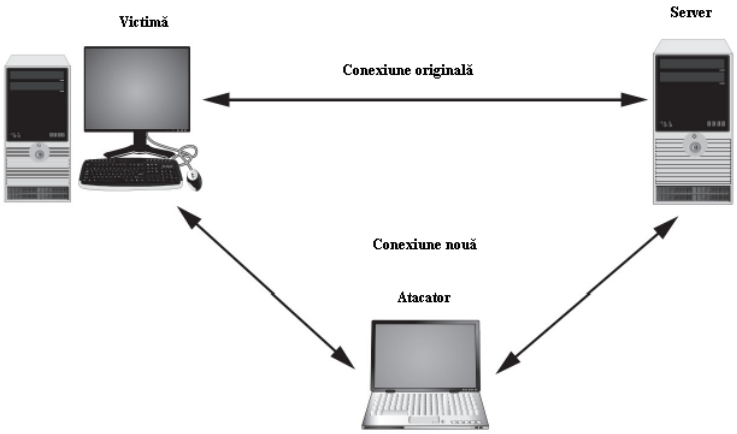

Fig. 4.5. Reprezentare grafică atac MitM

Atacurile MitM sunt atacuri active de interceptare a comunicațiilor față de atacurile pasive de Packet Sniffer, care fac același lucru, însă nu modifică conținutul pachetelor interceptate.

Atacuri de reluare

Un atac de reluare este similar cu un atac pasiv de interceptare, așa ca Packet Sniffer. În timp ce un atac pasiv trimite transmisia imediat, un atac de reluare face o copie a transmisiei înainte de a trimite destinatarului. Informațiile ce conțin acreditările de conectare sunt utilizate mai târziu de către atacator pentru a se conecta la sistemele la care are acces victima.

Un atac mai sofisticat profită de comunicațiile dintre un dispozitiv de rețea și un server. Mesajele administrative care conțin solicitări specifice de rețea sunt frecvent trimise între un dispozitiv de rețea și un server. Când serverul primește mesajul, îi răspunde expeditorului cu un alt mesaj administrativ. Fiecare dintre aceste transmisii este criptată pentru a împiedica un atacator să vadă conținutul, de asemenea, includ un cod care arată dacă conținutul a fost manipulat. Serverul citește codul, iar dacă recunoaște că mesajul a fost modificat, nu răspunde. Folosind un atac de reluare, un atacator poate captura mesajul trimis de pe dispozitivul de rețea către server. Mai târziu, atacatorul poate trimite mesajul original către server, iar serverul poate răspunde, crezând că a venit de la dispozitivul valabil.

4.1.3. Atacuri de spoofing/falsificare

Spoofing-ul reprezintă atacurile de uzurpare a identității prin care atacatorii exploatează relația de încredere dintre două sisteme [20]. Dacă două sisteme acceptă autentificarea unică, este posibil ca un utilizator conectat la un sistem să nu fie nevoit să se autentifice din nou pentru a accesa celălalt sistem. Un criminal cibernetic ar putea profita de acest lucru și ar putea trimite unuia dintre sistemele de încredere un pachet similar cu pachetele trimise de celălalt sistem. Deoarece există o relație de încredere între sisteme, sistemul-țintă completează cererea fără autentificare.

Există câteva tipuri de atacuri de falsificare comune:

- ***Falsificarea adresei MAC*** – presupune preluarea adresei fizice a unui dispozitiv legitim și utilizarea acesteia pentru conectarea la o rețea sau pentru a transmite pachete de date.
- ***Falsificarea adresei IP –*** un atacator trimite pachete cu adresa IP a unei surse false pentru a-și ascunde adresa.
- ***Falsificarea ARP*** (Address Resolution Protocol) – protocol care traduce adresele IP în adrese MAC pentru transmiterea datelor într-o rețea locală. În spoofingul ARP, un atacator trimite mesaje ARP false printr-o rețea locală pentru a-și asocia adresa MAC cu adresa IP a unui utilizator de încredere din infrastructura de rețea.

- ***Falsificarea DNS*** (Domain Name Service) – utilizat pentru a asocia nume de domenii cu adrese IP. Falsificarea DNS implică schimbarea serverului DNS pentru a reatribui un anumit nume de domeniu unei adrese IP false aflate sub controlul atacatorului.

Otrăvirea este actul de introducere a unei substanțe care dăunează sau distruge funcționalitatea unui organism. Două tipuri de atacuri injectează „otravă" într-un proces normal de rețea pentru a facilita un atac și realizează spoofing, acestea sunt falsificarea ARP și falsificarea DNS.

Falsificarea ARP

TCP/IP necesită ca adresele IP logice să fie atribuite fiecărei gazde dintr-o rețea. Cu toate acestea, o rețea LAN Ethernet utilizează adresa fizică (MAC) pentru a trimite pachete. Pentru ca o gazdă care utilizează TCP/IP într-o rețea Ethernet să găsească adresa MAC a altui dispozitiv pe baza adresei IP, aceasta utilizează protocolul de rezoluție a adresei (ARP). Dacă adresa IP pentru un dispozitiv este cunoscută, dar adresa MAC nu este, calculatorul trimite un pachet ARP la toate calculatoarele din rețea și spune: „Dacă este adresa ta IP, trimite-mi înapoi adresa ta MAC". Calculatorul cu acea adresă IP trimite înapoi un pachet cu adresa MAC, astfel încât pachetul să poată fi adresat corect. Aceste adrese IP și MAC sunt stocate într-un cache ARP pentru referințele viitoare. În plus, toate celelalte calculatoare care aud răspunsul ARP memorează acele date în cache. Un atacator poate modifica adresa MAC din memoria cache ARP, astfel încât IP corespunzător să îi fie atribuit altui calculator. Acest lucru este cunoscut sub numele de intoxicație cu ARP. Succesul atacului se datorează faptului că nu există proceduri de autentificare pentru a verifica cererile ARP. Atacurile ARP sunt utilizate ca vectori de atac în atacurile MitM, DoS/DDoS, furtul datelor și blocarea accesului la Internet.

Falsificarea DNS

Predecesorul internetului de astăzi a fost o rețea cunoscută sub numele de ARPAnet. Această rețea a fost finalizată în 1969 și a conectat între ele calculatoare individuale localizate în patru locații diferite (Universitatea California din Los Angeles, Stanford Institutul de Cercetare, Universitatea din California din Santa Barbara și Universitatea din Utah) cu o conexiune de 50 Kbps. Comunicarea dintre aceste calculatoare era realizată inițial prin atribuirea unui număr de identificare fiecărui calculator (adrese IP nu existau). Cu toate acestea, pe măsură ce numărul calculatoarelor conectate la rețea a crescut, a devenit mai dificil pentru oameni să-și amintească cu exactitate numărul de identificare al fiecăruia calculator. Ceea ce era necesar, era un sistem de nume care să permită alocarea calculatoarelor dintr-o rețea atât adrese numerice, cât și nume mai prietenoase, care pot fi citite de om, compuse din litere, numere și simboluri speciale. La începutul anilor 1970, fiecărui calculator dintr-o anumită locație a început să li se atribuie nume simple dispozitivelor de rețea și, de asemenea, să se gestioneze propriul tabel-gazdă care conținea mapările numelor cu numerele calculatorului. Cu toate acestea, pentru că fiecare locație încerca să mențină propriul său tabel-gazdă local, acest lucru a dus la inconsecvențe între locații. Când a fost dezvoltată suita TCP/IP, conceptul de tabel-gazdă a fost extins la un sistem de nume ierarhice pentru potrivirea numelui calculatorului cu numărul acestuia, cunoscut sub numele de Domain Name System (DNS), care stă la baza rezoluției numelui la adresa IP de astăzi.

Datorită rolului important pe care îl joacă, DNS este ținta atacurilor. La fel ca otrăvirea cu ARP, otrăvirea DNS înlocuiește o adresă DNS, astfel încât calculatorul să fie redirecționat automat la alt dispozitiv. În timp ce otrăvirea ARP înlocuiește o adresă MAC frauduloasă pentru o adresă IP, otrăvirea DNS înlocuiește un nume simbolic cu o adresă IP frauduloasă. Înlocuirea unei adrese IP frauduloase se poate face în două locații diferite: tabelul-gazdă local sau serverul DNS extern. TCP/IP încă folosește tabele-gazdă stocate pe calculatorul local. Aceasta este numit sistem de nume de tabel-gazdă TCP/IP. Un tabel tipic de gazdă locală este reprezentat în figura 4.6 și se află în directorul /etc/ în UNIX, Linux și Mac OS X și în directorul Windows\System32\drivers\etc din Windows. Când un utilizator introduce un nume simbolic,

TCP/IP verifică mai întâi tabelul-gazdă local pentru a determina dacă există o intrare. Dacă nu există nici o intrare, atunci este utilizat sistemul DNS extern. Atacatorii pot vedea fișierul gazdelor locale pentru a crea intrări noi care vor redirecționa utilizatorii către site-ul fraudulos, astfel încât, de exemplu, când utilizatorii intră pe www.paypal.com, aceștia sunt direcționați către site-ul asemănător al atacatorului.

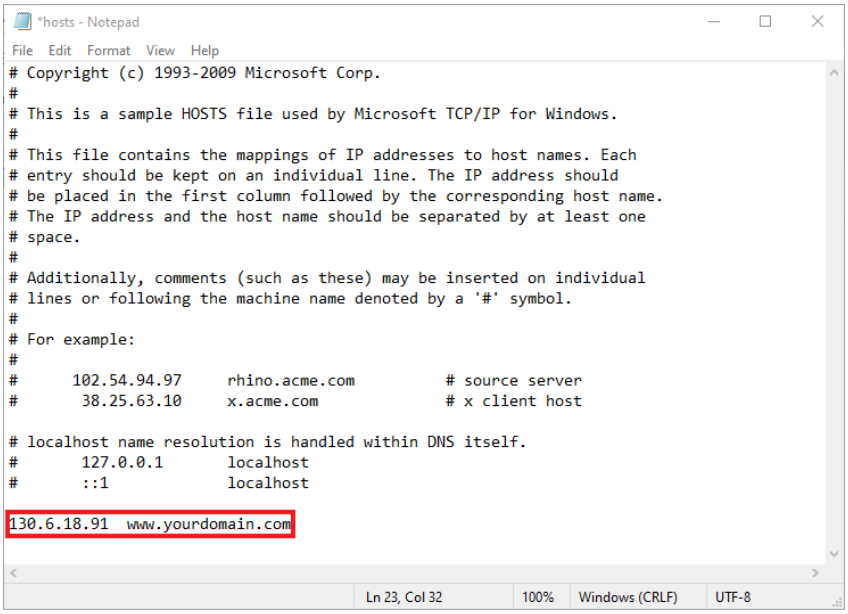

Fig. 4.6. Fișierul local

O a doua locație care poate fi atacată este serverul DNS extern [8]. În loc să încerce să pătrundă într-un server DNS pentru a-i schimba conținutul, atacatorii folosesc o abordare mai simplă. Deoarece serverele DNS fac schimb de informații între ele (cunoscute ca transferuri de zonă), atacatorii vor încerca să exploateze un defect de protocol și să convingă serverul DNS autentic să facă acest lucru prin a accepta intrări DNS frauduloase trimise de pe serverul DNS al atacatorului. Dacă serverul DNS o face și nu validează corect răspunsurile DNS pentru a se asigura că provin de la o autoritate sursă, va stoca intrările frauduloase local și le va servi utilizatorilor, răspândindu-le pe alte servere DNS. Un exemplu de atac de otrăvire DNS de la un atacator care are un nume de domeniu www.evil.net cu propriul server DNS, ns.evil.net este reprezentat în figura 4.7.

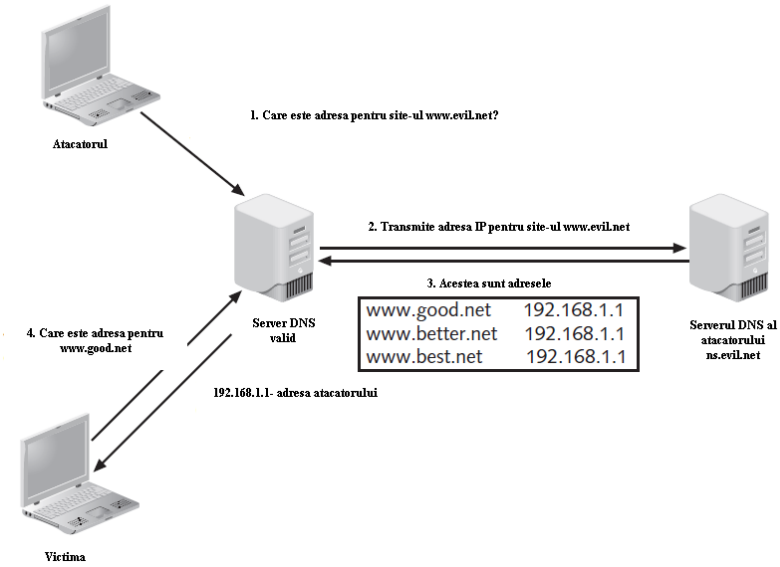

Fig. 4.7. Otrăvirea DNS, server extern

Otrăvirea DNS este deseori utilizată de guvernele statelor totalitare pentru a limita accesul cetățenilor la resursele Internet care nu sunt acceptate de către autorități, ca de exemplu în cazul Chinei.

4.1.4. Atacuri asupra drepturilor de acces

Drepturile de acces sunt privilegiile de a accesa resursele hardware și software care le sunt acordate utilizatorilor. De exemplu, Sofiei i se pot acorda drepturi de acces pentru a citi un fișier, în timp ce Elizei i se acordă drepturi de acces pentru a adăuga conținut la fișier. Două dintre cele mai comune atacuri care vizează drepturile de acces sunt *escaladarea privilegiilor* și *accesul tranzitiv*.

Escaladarea privilegiilor

Sistemele de operare și multe aplicații au capacitatea de a restricționa privilegiile unui utilizator în accesarea funcțiilor sale specifice. Escaladarea privilegiilor este exploatarea unei vulnerabilități software pentru a obține acces la resursele pe care utilizatorul în mod normal nu le poate accesa.

Există două tipuri de escaladare a privilegiilor:

- Primul se referă la folosirea unui utilizator cu un privilegiu mai scăzut al escaladării privilegiilor pentru a-și acorda acces la funcțiile rezervate utilizatorilor cu privilegii mai mari (numită și escaladarea verticală a privilegiilor).
- Al doilea tip de escaladare a privilegiilor se referă la un utilizator cu privilegii restricționate care accesează diferite funcții restricționate ale unui utilizator similar; adică Mia nu are privilegii pentru a accesa un program de salarizare, dar folosește privilegii de escaladare pentru a accesa contul lui Ion care are aceste privilegii (privilegiul orizontal de escaladare).

Accesul tranzitiv

Accesul tranzitiv este definit ca o relație cu proprietate, astfel încât dacă o relație există între A și B și există și o relație între B și C, atunci există o relație și între A și C. Tranzitivul este adesea folosit în matematică în ceea ce privește mărimea: dacă A este mai mic decât B și B este mai mic decât C, apoi se poate spune că A este mai mic decât C. Când se înlocuiește încrederea cu dimensiunea, accesul tranzitiv înseamnă că dacă Alice are încredere în Bob și Bob are încredere în Carol, atunci și Alice are încredere în Carol (numită încredere tranzitivă).

În tehnologie, această încredere tranzitivă poate duce la acces tranzitiv, în care sistemul 1 poate accesa Sistemul 2 și deoarece Sistemul 2 poate accesa Sistemul 3, atunci Sistemul 1 poate accesa Sistemul 3. Cu toate acestea, intenția poate să nu fie ca Sistemul 1 să acceseze Sistemul 3, ci Sistemul 1 să poată accesa numai Sistemul 2. Acest lucru apare involuntar și accesul neautorizat poate duce la riscuri serioase de securitate. Atacatorii pot profita de accesul tranzitiv care are loc ori de câte ori accesul este construit prin sisteme succesive, aici intervenind efectul de cascadă menționat anterior.

4.2. Atacuri asupra aplicațiilor

Actualmente, utilizarea aplicațiilor web a devenit o activitate uzuală pentru utilizatorii din întreaga lume, indiferent de educația pe care o au și activitatea pe care o desfășoară. Internetul care este supranumit ”rețeaua internațională a rețelelor interconectate” este parte indispensabilă a activităților cotidiene, profesionale și personale. Cel mai des utilizat model de rețea este client-server [21] ilustrat în figura 4.8.

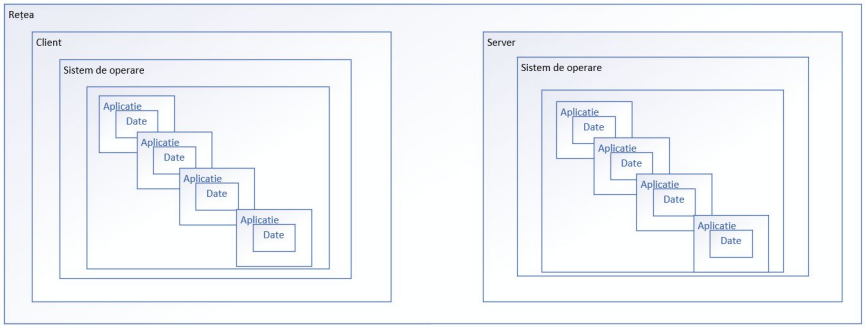

Fig. 4.8. Modelul client-server al rețelelor

Practic, fiecare element ilustrat în figura 4.8 este vulnerabil la atacurile cibernetice, reprezentând vectori de atac, însă în această temă vor fi analizate cu precădere atacurile asupra aplicațiilor web. Atacurile asupra aplicațiilor web pot avea loc asupra clientului, asupra serverului sau asupra ambelor părți.

4.2.1. Atacuri pe partea de server a aplicațiilor web

Serverele oferă diverse servicii clienților prin aplicațiile web care rulează pe acestea. O caracteristică importantă a aplicațiilor web bazate pe servere este că oferă conținut dinamic în baza cererii primite de la utilizator, ca de exemplu notificările meteo transmise utilizatorilor de către un anumit site web. Acest proces se realizează prin cereri de tip HTTP (Hypertext Transport Protocol) inițiate de browser-ul utilizatorului către server. Aplicațiile web specifice apelează la bazele de date prin rețeaua internă și returnează serverului informația solicitată, astfel încât informația să poată fi returnată browser-ului client în mod dinamic (figura 4.9).

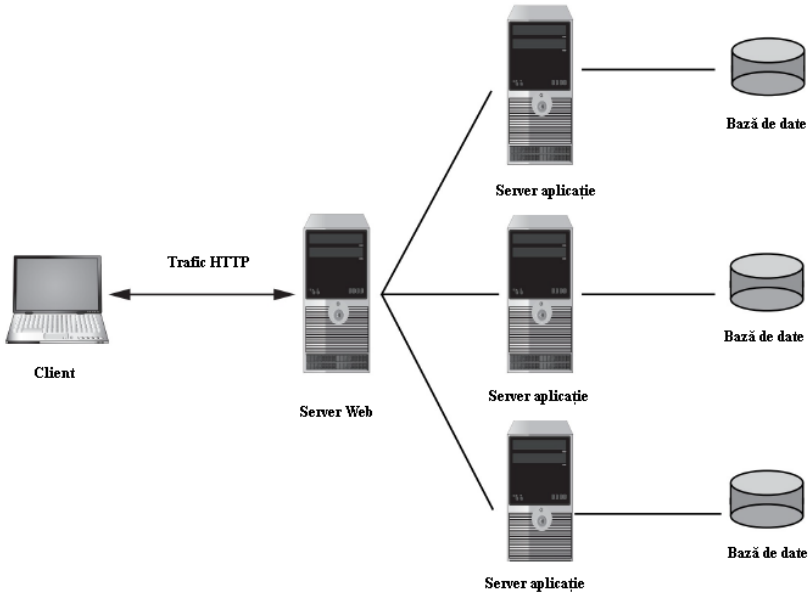

Fig. 4.9. Infrastructura aplicațiilor web bazate pe server

Se consideră o procedură mult mai complicată securizarea aplicațiilor web de pe partea de server, deoarece acestea sunt proiectate din start ca fiind dinamice, astfel încât să accepte intrări de pe partea clientului, ca de exemplu un site web meteo va accepta introducerea codului clientului pentru a cunoaște datele meteo din regiunea dorită. Majoritatea altor aplicații ar respinge astfel de cereri, anume intrările din partea clienților și reprezintă amenințarea cea mai comună de securitate, deoarece datele introduse de acesta pot avea deseori rezultate neașteptate. Susceptibilitatea aplicațiilor web la atacurile de tip zero-day este mult mai mare decât a aplicațiilor de pe partea de client, deoarece acestea pot duce la întreruperea activității serverului. O altă vulnerabilitate sunt cererile de tip HTTP, care de obicei sunt ignorate de către dispozitivele intermediare de rețea, dar care sunt vectori des exploatați pentru atacurile asupra aplicațiilor. Cele mai comune atacuri ale aplicațiilor pe partea de server sunt: *cross-site scripting, injectarea SQL, injectarea XML și atacurile de traversare a căii (Path Traversal).*

Cross-site scripting (XSS cross site scripting)

Cross-site scripting este o vulnerabilitate în aplicațiile web. Include trei participanți: infractorul, victima și site-ul web. Exploatează o vulnerabilitate a unui site web sau a unei aplicații web în următoarele moduri:

- redirecționând URL-uri ascunse care exploatează vulnerabilitățile de scripting între site-uri sau de falsificare a cererilor de pe mai multe site-uri;
- transmiterea de către atacator prin e-mail a unui link care exploatează vulnerabilitate prin care se trimit acreditări/ID-uri de sesiune/cookie-uri către atacator;
- site-ul web permite rularea scripturilor la intrarea utilizatorului, caseta de căutare fiind un vector comun de atac.

Un exemplu din mediul real descoperit de către un hacker etic descrie un atac XSS prin care site-ul web nu ar trebui să permită introducerea și procesarea scriptului în URL, deoarece în acest caz un atacator poate acționa acest site în contextul securității. Acesta este un exemplu de adresă URL:

```
www.gossamer-threads.com/form/user.cgi?url=”><script>alert(“XSS
vulnerability”)</sc...
```

Făcând clic pe această adresă URL, se deschide site-ul web, deoarece URL conține un script special. Când utilizatorul va introduce numele de utilizator și parola, atacatorul va putea să fure acreditările. Partea critică a codului este:

```
..ds.com/forum/user.cgi?url=”><script>alert(“XSS
vulnerability”)</script>”&from=rate...
```

Aceasta și este vulnerabilitatea de falsificare a cererilor între site-uri. Codul introdus conține elementul iframe inserat pentru a crea un ecran de conectare fals și pentru a colecta detalii de conectare și parole (figura 4.10):

```
.../user.cgi?url=”><iframe%20src=”http://www.stationx.net/linksql.html%20sc
rolling=”No”%20align=”MIDDLE”%20width=”100%”%20height=”3000”&20frameborder=
”No”></iframe><!--&from=rate
```

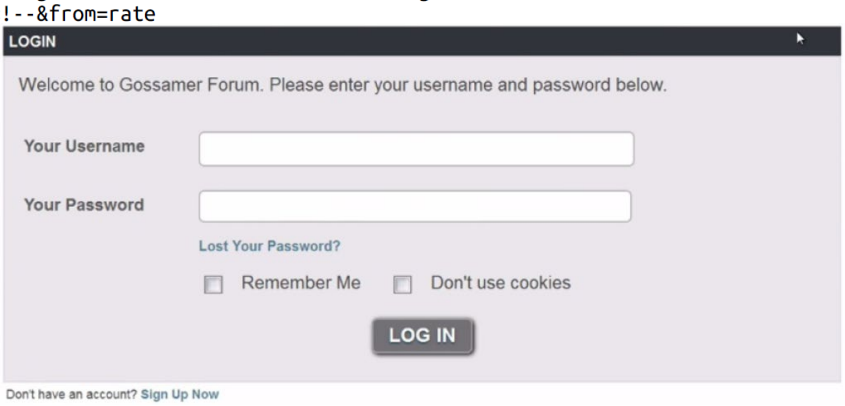

Fig. 4.10. Fereastră de autentificare falsă

Aplicațiile web, după cum a fost specificat anterior, sunt dinamice, adică sunt concepute pentru a personaliza conținutul pentru utilizator, în dependență de ceea ce se solicită. Răspunsurile personalizate tipice sunt descrise în tabelul 4.1.

Tabelul 4.1. Răspunsuri personalizate

Intrări utilizator	***Variabile care conțin intrările***	***Răspunsul aplicației web***	***Exemplu de cod***
Căutare termen	search_term	Este returnat termenul căutat	“Search results for search_term”
Intrare incorectă	user_input	Mesaj de eroare care conține intrarea incorectă	“user_input is not valid”
Nume utilizator	Name	Răspuns personalizat	“Welcome back name”

Atacurile XSS apar când un atacator profită de aplicațiile web care acceptă intrări ale utilizatorului, fără a le valida, apoi prezintă răspuns utilizatorului [8]. Un exemplu tipic de atac XSS sunt site-urile de vânzări online care acceptă recenzii/comentarii de la cumpărători. Astfel, atacatorul introduce un comentariu care de fapt conține un script ascuns sau redirecționează către site-ul atacatorului, iar un utilizator oarecare făcând clic pe acel comentariu, i se descarcă în mod automat scriptul și i se fură toate informațiile sensibile salvate în browser-ul utilizatorului, utilizate ulterior pentru atacurile de impersonare.

Injectarea SQL

Injectarea SQL este un alt atac comun asupra aplicațiilor web care utilizează bazele de date relaționale SQL. Acest atac vizează serverele SQL prin introducerea comenzilor rău intenționate [8]. Cel mai tipic exemplu este autentificarea utilizatorului pe un anumit site, folosind numele de utilizator și parola prin formularul de autentificare ce permite, de asemenea, în cazul când utilizatorul a uitat numele sau parola, să introducă un email pe adresa căruia va fi transmis link-ul de resetare (figura 4.11).

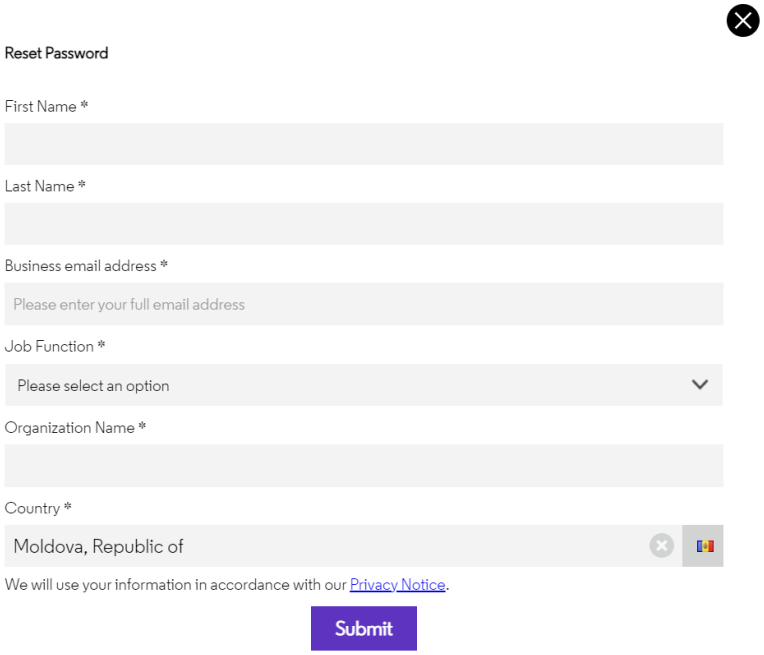

Fig. 4.11. Formular de resetare credențiale

Email-ul introdus este comparat cu cel stocat în baza de date. Dacă adresa de e-mail introdusă de utilizator în formular este stocată în variabila $EMAIL, atunci instrucțiunea SQL de bază pentru a prelua adresa de e-mail stocată este:

SELECT fieldlist FROM table WHERE field = '$EMAIL'

Clauza WHERE este menită să limiteze interogarea bazei de date pentru a afișa informații numai când condiția este considerată adevărată (adică atunci, când adresa de e-mail din $EMAIL se potrivește cu o adresă din baza de date). Un atacator care folosește un atac SQL ar începe prin a introduce mai întâi o adresă de e-mail fictivă care include ghilimele doar la sfârșitul adresei introduse, ca parte a datelor, cum ar fi *ion.turcanu@fakemail.com"*. Dacă este afișat mesajul "*E-mail Address Unknown*", acesta indică faptul că intrarea utilizatorului este filtrată corect și că un atac SQL nu poate fi executat pe site. Cu toate acestea, dacă este afișat mesajul de eroare "*Server Failure"*, înseamnă că intrarea utilizatorului nu este filtrată și toate intrările utilizatorului sunt trimise direct în baza de date. Mesajul "Server Failure" se datorează unei erori de sintaxă creată de ghilimele adăugate: adresa de e-mail fictivă introdusă va fi procesată ca *ion.turcanu@fakemail.com* ' ' (cu două ghilimele simple) și serverul va genera mesajul de eroare.

Injectarea XML

Injectarea XML exploatează vulnerabilitățile limbajului de marcare, care este o metodă de adăugare a adnotărilor la text astfel, încât completările pot fi distinse de textul însuși. Limbajul de marcare hipertext (HTML) este un astfel de limbaj de marcare ce utilizează anumite cuvinte (etichete) încorporate între paranteze (< >) pe care un browser web îl folosește apoi pentru a afișa text într-un anumit format.

Un alt limbaj de marcare este XML (Extensible Markup Language). Însă există câteva diferențe semnificative între XML și HTML. În primul rând, XML este conceput să transporte date în loc să indice cum să fie afișate. De asemenea, XML nu are un set predefinit de etichete; în schimb, utilizatorii își definesc propriile etichete. Un atac de injectare XML este similar cu un atac de injectare SQL; un atacator care descoperă că site-ul web nu filtrează datele introduse de utilizator poate injecta etichete și date XML în baza de date. Un tip specific de atac de injectare XML este o injectare XPath, care încearcă să exploateze Interogări XML Path Language (XPath) care sunt construite din intrarea utilizatorului.

Atacurile de traversare a căii

Atacurile de traversare a căii (Path Traversal) / Command Injection poate fi lansat printr-o vulnerabilitate din aplicația web program care acceptă intrarea utilizatorului, o vulnerabilitate în software-ul sistemului de operare al serverului web sau o configurație greșită de securitate pe server. Când se utilizează intrarea de la utilizator ca vector de atac, poate fi introdus un șir lung de caractere, cum ar fi http://../../../../../../../../, unde ../ parcurge un nivel de director în sus. De exemplu, un browser care solicită o pagina web dinamică compilată (dynamic.asp) de pe un server web (www.server.net) pentru a prelua un fișier (display.html) și a-l afișa ar genera cererea folosind adresa URL http://www.server.net/ dynamic.asp? view= display.html. Cu toate acestea, dacă intrarea utilizatorului ar fi permisă, însă nu va fi validată corespunzător, atacatorul ar putea crea intrarea http://www.server.net/dynamic.asp ?view=. ./../../../../TopSecret.docx care ar putea afișa conținutul unui document confidențial.

Directorul rădăcină este un director specific în sistemul de fișiere al unui server web. Utilizatorii care accesează serverul sunt de obicei restricționați să acceseze directorul rădăcină sau sub-directoriile acestuia. De exemplu, directorul rădăcină implicit al Internet Information Services Microsoft Serverul web (IIS) este C:\Inetpub\wwwroot. Utilizatorii au acces la acest director și subdirectoare sub această rădăcină (C:\Inetpub\wwwroot\news) dacă s-a obținut permisiunea, dar nu are acces la alte directoare din sistemul de fișiere, cum ar fi *C:\Windows\System32*. Calea parcursă de atacator este ilustrată în figura 4.12.

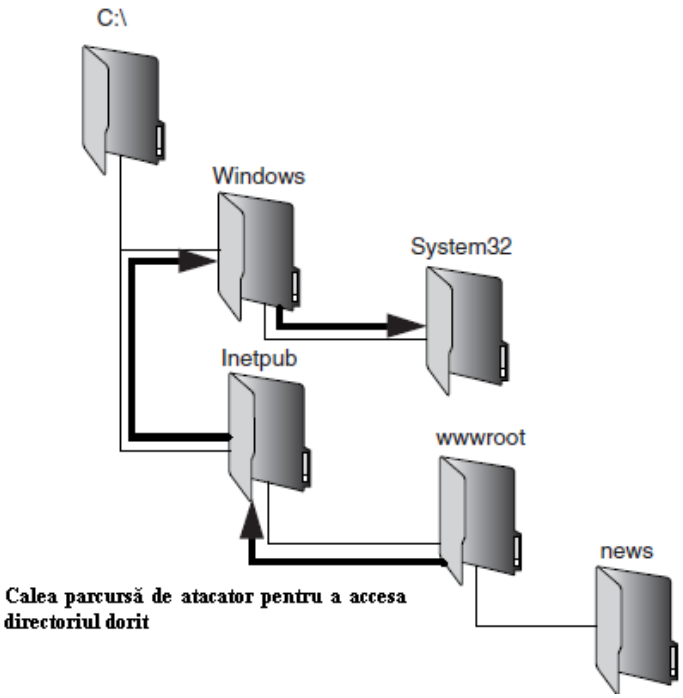

Fig. 4.12. Calea parcursă de atacator

4.2.2. Atacuri pe partea de client a aplicațiilor web

Atacurile pe partea de server exploatează vulnerabilitățile serverului pe când atacurile pe partea de client exploatează vulnerabilitățile aplicațiilor client care interacționează cu serverele compromise, adică atacul survine în momentul conexiunii client-server [8]. Un exemplu de atac pe partea clientului are ca rezultat compromiterea calculatorului unui utilizator prin vizualizarea unei pagini web, chiar dacă nu se face clic pe conținut. Acest tip de atac, cunoscut sub numele de descărcare *drive-by*, este o amenințare serioasă. Atacatorii identifică mai întâi un server web vulnerabil și injectează un conținut prin exploatarea serverului prin aplicații vulnerabile de scripting. Aceste vulnerabilități permit atacatorului să obțină acces

direct la serverul sistemului de operare de bază, apoi injectează un conținut nou în site-ul web compromis. Pentru a evita detectarea vizuală, atacatorii creează adesea un *iFrame* cu zero pixeli, care este un element HTML ce permite încorporarea unui alt document HTML. iFrame-ul de zero pixeli este invizibil pentru utilizatori și dacă calculatorul victimei permite descărcarea automată, atunci scriptul rău intenționat se va executa pe dispozitivul utilizatorului. Acest tip de atac funcționa cu succes în browser-ele mai vechi, însă nu este la fel de eficient și în versiunile mai noi ale browser-elor.

Cele mai comune atacuri ale aplicațiilor pe partea de client includ: *manipularea antetului (header), cookie, ataşamentele, extensiile (add-ons) maliţioase, deturnarea sesiunii (session hijacking).*

Manipularea antetului

Manipularea antetului se referă la antetul HTTP care este format din câmpuri ce conțin informații despre caracteristicile datelor transmise. Câmpurile de antet sunt compuse din numele câmpului, două puncte și valoarea câmpului, cum ar fi lungimea conținutului: 49. Deși antetul HTTP, numele câmpurilor și valorile pot fi orice șiruri specifice aplicației, a fost standardizat de Internet Engineering Task Force (IETF) un set de bază de câmpuri. Un atacator poate modifica anteturile HTTP pentru a crea un atac folosind manipularea antetului HTTP. Manipularea antetului nu reprezintă atacuri propriu-zise, ci sunt mai degrabă utilizate de către atacator ca vector de atac pentru atacurile XSS și permite transmiterea conținutului rău intenționat utilizând un site compromis.

Cookies

Cookies reprezintă fișiere stocate de către server, cu anumite date ale utilizatorului mai des solicitate, chiar pe dispozitivul acestuia, pentru ca următoarea dată când utilizatorul va accesa un site, serverul să poată accesa acest fișier pentru a cunoaște anumite preferințe și a returna conținutul dinamic. Astfel, serverul nu va mai trebui să solicite aceleași informații de la utilizator ori de câte ori acesta va accesa site-ul. Cookie-urile pot stoca, de asemenea, orice informații de identificare personală (nume, adresă de e-mail, adresa de serviciu, numărul de telefon și așa mai departe) care a fost furnizat la vizitarea site-ului; cu toate acestea, un site web nu poate obține acces la informațiile private stocate în calculatorul local.

Cookies se clasifică astfel:

- *cookie primar* care salvează informațiile despre vizita utilizatorului pe site-ul accesat în prezent;
- *cookie terțiar* care conțin informații stocate local, suplimentare ce vin de la site-urile de publicitate sau noutăți, utilizate pentru a personaliza conținutul afișat utilizatorului ca și publicitate;
- *cookie de sesiune* stocat în memoria de acces aleatoriu (RAM) și sunt stocate doar pe durata vizitei site-ului. Aceste cookies sunt șterse odată ce utilizatorul a închis browser-ul sau după o anumită perioadă de timp;
- *cookie persistent* care este opusul cookie de sesiune și este stocat pe unitatea de stocare permanentă a calculatorului;
- *cookie flash* poate stoca mult mai mult conținut decât cookie obișnuite de până la 100 KB, de 25 ori mai mult decât alte cookie.

Cookie-urile pot prezenta atât riscuri de securitate, cât și de confidențialitate. Cookie-urile primare pot fi furate și utilizate pentru a uzurpa identitatea utilizatorului, în timp ce cookie-urile terțiare pot fi folosite pentru a urmări navigarea sau obiceiurile de cumpărare a unui utilizator. Când mai multe site-uri web sunt deservite de o singură organizație de marketing, cookie-urile pot fi folosite pentru a urmări obiceiurile de navigare pe toate site-urile clientului. Aceste organizații pot urmări obiceiurile de navigare de la o pagină la alta pe toate site-urile clienților lor și să știe care pagini sunt vizualizate, cât de des sunt vizualizate și adresa

IP (Internet Protocol) a calculatorului. Aceste informații pot fi folosite pentru a deduce elementele de care poate fi interesat utilizatorul și să direcționeze publicitatea către utilizator.

Atașamente

Atașamentele la email sau ca și conținut al site-urilor sunt des utilizate pentru a infecta cu malware calculatorul utilizatorului, conținând adesea o linie de subiect atractivă, ceea ce îi determină chiar și pe utilizatorii experimentați să le acceseze, ca de exemplu linia de subiect: ”*Ești chiar tu în acest video?*”

Deturnarea sesiunii (session hijacking)

Este important ca atunci când un utilizator accesează o aplicație web securizată, cum ar fi o librărie online, să poată fi verificată identitatea acestuia, astfel încât să împiedice un impostor să preia cărțile comandate de victimă. Această verificare se realizează printr-un token de sesiune, care este un șir aliator atribuit acelei interacțiuni dintre utilizator și aplicația web accesată. Când utilizatorul se conectează la serverul web al librăriei online cu numele și parola sa, serverul de aplicații web atribuie un simbol de sesiune unic, cum ar fi *64aa9DACOqgoipxwQDdywr*. Fiecare solicitare ulterioară din browser-ul web al utilizatorului către aplicația web conține simbolul de sesiune care verifică identitatea utilizatorului până când acesta se deconectează. ***Deturnarea sesiunii*** este atacul prin care hackerul va încerca impersonarea utilizatorului prin utilizarea token-ului de sesiune atribuit de către server acestui utilizator. Un scenariu care reflectă acest tip de atac este reprezentat în figura 4.13.

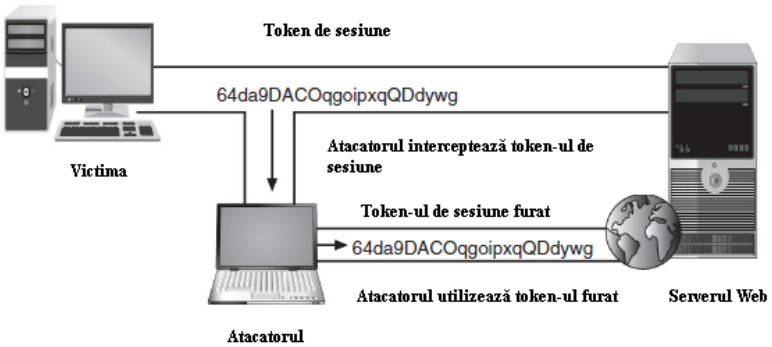

Fig. 4.13. Exemplu de deturnare a sesiunii

Unul dintre cele mai comune moduri de obținere a token-ului de sesiune sunt atacurile XSS sau alte atacuri prin care se fură cookies de sesiune, care mai apoi este utilizat pentru impersonarea utilizatorului.

Extensiile din browser pot fi de 2 tipuri:

- pentru a îmbunătăți experiența de navigare a utilizatorului și a rula conținuturi de diferit tip, de exemplu Java, Adobe Flash player, Apple QuickTime și Adobe Acrobat Reader; în acest caz va fi afectat doar conținutul specific în care este plasat;
- a doua categorie este formată din instrumente care adaugă funcționalitate browser-ului web și pot face următoarele: crea bare de instrumente suplimentare pentru browser web, schimba meniurile browser-ului, procesa conținutul fiecărei pagini web care este încărcată.

Există riscuri de securitate când se utilizează extensiile, deoarece atacatorii pot crea extensii malițioase pentru a lansa atacuri împotriva calculatorului utilizatorului.

4.2.3. Atacuri imparțiale

Există însă și atacuri care pot afecta atât aplicațiile pe partea de server, cât și pe partea de client. Multe dintre aceste atacurile sunt concepute pentru a „depăși” zonele de memorie cu instrucțiuni date de atacatori. Această categorie de atacuri include *atacuri de depășire a*

tamponului (Buffer Overflow), atacuri de depășire a numărului întreg (Integer Overflow) și atacuri arbitrare/ atacuri de execuție de cod la distanță.

Buffer Overflow

Buffer Overflow este un atac complex, iar pentru a înțelege mai bine cum are loc va fi prezentat un exemplu tipic din viața cotidiană: o profesoară verifică un test de examinare lung, scris pe hârtie și marchează răspunsurile incorecte cu un pix roșu. Pentru că ea este frecvent întreruptă de către elevi, profesoara pune o riglă la întrebarea test pe care în prezent o evaluează pentru a indica „punctul de întoarcere" sau punctul de la care ar trebui să reia notarea. Presupunem că doi studenți vicleni intră în biroul ei în timp ce ea notează examenele și în timp ce un elev îi distrage atenția, al doilea elev împinge rigla în jos de la întrebarea 4 la întrebarea 20. Când profesoara revine la notare, va relua „punctul de întoarcere" greșit și nu se va uita la răspunsurile întrebărilor 4-19. Acest scenariu este similar cu modul în care un atacator încearcă să compromită un calculator utilizând atacul ***buffer overflow***. Un buffer de stocare pe calculator conține de obicei locația de memorie a software-ului, program care a fost executat când o altă funcție a întrerupt procesul; memoria tampon de stocare conține „adresa de retur" unde procesorul calculatorului ar trebui să reia execuția programului, odată ce noul proces s-a încheiat. Un atacator își poate înlocui propria „adresă de întoarcere" pentru a indica o zonă diferită din memoria calculatorului care conține codul malware introdus. ***Un atac de depășire a memoriei tampon are loc când un proces încearcă să stocheze date în RAM dincolo de limitele unui buffer de stocare cu lungime fixă.*** Aceste date suplimentare se revarsă în memoria adiacentă locației (o depășire a tamponului). Deoarece tamponul de stocare conține de obicei „adresa de return", un atacator poate depăși buffer-ul cu o nouă adresă către codul malware al atacatorului. Un atac de depășire al tamponului este reprezentat în figura 4.14.

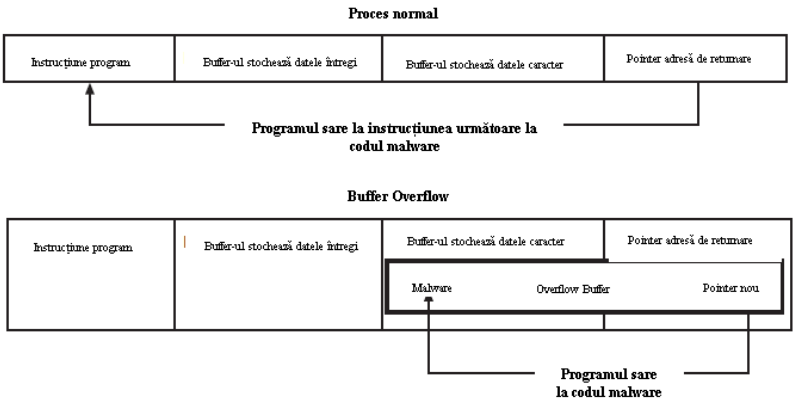

Fig. 4.14. Buffer Overflow

Integer Overflow

Integer Overflow reprezintă atacuri de manipulare cu diapazonul numerelor întregi, cum ar fi de exemplu un ceas digital care poate afișa orele doar de la 1 la 12. Apare întrebarea: ce se întâmplă când timpul trece de 12:59? Ceasul va „trece" la cea mai mică valoare a sa, adică la 1 din nou. Pe un calculator, depășirea numerelor întregi este condiția care apare când în rezultatul unei operații aritmetice, cum ar fi adunarea sau înmulțirea, se depășește dimensiunea maximă a diapazonului numerelor întregi. Când are loc această depășire a numărului întreg, valoarea interpretată se deplasează de la valoarea maximă la valoarea minimă.

! De exemplu, un număr întreg de 8 biți are o valoare maximă de 127 și o valoare minimă de -128. Dacă valoarea 127 este stocată într-o variabilă și i se adaugă 1, suma depășește valoarea maximă pentru tipul numerelor întregi și se transformă în -128.

Acest tip de atac poate fi folosit în următoarele situații:

- Un atacator ar putea folosi un atac de depășire a numerelor întregi pentru a crea o situație de depășire a tamponului.

- Un program care calculează costul total al articolelor achiziționate ar folosi numărul unităților vândute înmulțite cu costul pe unitate. Dacă s-a introdus un număr care depășește numărul de articole vândute, costul total ar putea avea ca rezultat o valoare negativă și un rezultat negativ, indicând faptul că o rambursare se datorează clientului.
- O valoare pozitivă mare într-un transfer bancar ar putea să devină o valoare negativă, care ar putea apoi inversa fluxul de bani: în loc să adauge această sumă în contul victimei, ar putea să retragă suma și ulterior să o transfere în contul atacatorului. Un exemplu relevant a acestui tip de atac de depășire a numărului întreg ar fi retragerea 1 USD dintr-un cont care are soldul 0 USD, ceea ce ar putea cauza un nou sold de 4.294.967.295 USD!

Atacuri arbitrare/ atacuri de execuție de cod la distanță

Atacurile arbitrare/ atacurile de execuție de cod la distanță reprezintă atacuri comune prin care are loc executarea unui anumit cod de la distanță, cod ce putea fi inserat în orice tip de atașament deschis de către utilizator și care permite atacatorului să aibă aceleași drepturi de acces ca și victima, să acceseze, să modifice sau să șteargă fișiere precum și alte acțiuni neautorizate.

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. De ce atacurile asupra rețelelor reprezintă o prioritate pentru infractorii cibernetici?
2. Prin ce diferă atacurile DoS? Care este scopul acestor atacuri și ce ar putea reprezenta o motivație pentru atacatori?
3. Explicați cum diferă atacurile de interceptare a comunicațiilor electronice.
4. Care sunt cele patru clase principale de atacuri asupra rețelelor?
5. Prin ce se deosebesc atacurile pe partea de server de atacurile pe partea de client?
6. Care este scopul și motivația atacatorilor de a iniția atacuri asupra serverelor? Analizați literatura și enumerați cât mai multe exemple relevante și specificați scopul acestora.
7. În ce cazuri sunt inițiate atacurile de depășire a numerelor întregi? Care sunt posibilele cauze ale acestor atacuri?
8. Descrieți atacurile de tip Buffer Overflow și explicați de ce aceste atacuri sunt inițiate împotriva serverelor Web.
9. De ce dispozitivele de securitate nu pot opri atacurile asupra aplicațiilor web?
10. Descrieți printr-un exemplu concret tipurile de cookie și cum pot fi utilizate acestea pentru atacurile de securitate.