

Cyber Security - Network Attacks

[Securitate cibernetică – atacuri în rețele]

Liliana COJOCARU¹

¹ Associate Professor Ph.D., "Petre Andrei" University of Iași, Romania, e-mail: lcojocarus@yahoo.com

Konstantina Claudia CURCĂ¹

¹ Undergraduate student, "Petre Andrei" University of Iași, Romania.

Abstract

Cyber Security is a field of Computer Science that studies computer systems' and networks' vulnerabilities to attacks with the aim of obtaining information, damaging information or destroying the functionality of systems or networks. Cyber Security also studies the ways to prevent these attacks by identifying various methods to secure computer systems and networks. In this article we present the main cyberattacks, such as ARP cache poisoning, SYN flooding, DNS cache poisoning, Sniffing/Spoofing, Denial of Service, Man in the Middle, as well as the ways to secure a computer network against these attacks.

Keywords: Network Attacks; SYN flooding; ARP cache poisoning; DNS cache poisoning.

How to cite: Cojocaru, L., & Curcă, K.C. (2026). Cyber Security - Network Attacks. *Anuarul Universității "Petre Andrei" din Iași, Fascicula: Drept, Științe Economice, Științe Politice*, 36, 147-157.
<https://doi.org/10.63331/upalaw/36/14>

1. Introducere - Context și motivație

Transformarea digitală a economiei și a serviciilor publice a amplificat dependența organizațiilor de infrastructuri de comunicații reziliente. În acest context, securitatea cibernetică reprezintă ansamblul de politici, procese, tehnologii și practici menite să protejeze activele informaționale și funcțiile operaționale împotriva incidentelor intenționate sau accidentale de spargere a informațiilor private. În rețelele moderne, atacurile vizează atât protocoale fundamentale *ARP (Address Resolution Protocol)*, *IP (Internet Protocol)*, *TCP (Transmission Control Protocol)*, *DNS (Domain Name System)*, cât și componente aplicative, profitând de erori de proiectare, configurări defectuoase sau lipsa unor controale de vulnerabilitate. Complexitatea sistemelor informatice (dispozitive eterogene, servicii distribuite, cloud sau mediile hibride, internet of things) extinde aria unui atac cibernetic și impune mecanisme de apărare sofisticate.

Triada *CIA (Confidentiality, Integrity, Availability)* este un model fundamental de implementare a politicilor de apărare informațională bazată pe trei concepte fundamentale *Confidențialitate*, *Integritate* și *Disponibilitate*. Scopul fundamental al securității este protejarea acestei triade, într-o încercare de a asigura protejarea și integritatea sistemelor informatice în orice infrastructură.

În principiu, politicile de *Confidențialitate* urmăresc protejarea informațiilor față de persoanele neautorizate, ceea ce se realizează prin intermediul sistemelor de criptare, de parolare și implemmentare a accesului controlat pentru a limita sfera de vizibilitate a informațiilor. Politicile de *Integritate* urmăresc protejarea informațiilor pentru a nu fi modificate sau distruse de persoane neautorizate. Se realizează prin implementări de checksum-uri sau de semnături digitale. *Disponibilitatea* constă în asigurarea permanentă a accesului pentru persoanele autorizate. Se realizează prin efectuări periodice de backup-uri care să permită refacerea informațiilor pierdute, prin implementarea sistemelor redundante și a sistemelor de monitorizare care să permită reconstituirea informațiilor în urma unei căderi sau blocări a sistemului.

Securitatea cibernetică se aplică diferitelor tipuri de rețele informatice¹ precum *PAN (Personal Area Network)* – rețele personale, de mică distanță, folosite pentru conectarea dispozitivelor individuale, de exemplu smartphone, laptop, smartwatch, *LAN (Local Area Network)* – rețele locale, de dimensiuni restrânse, precum rețele de birou sau rețele universitare, *MAN (Metropolitan Area Network)* – rețele care acoperă o arie urbană extinsă, *WAN (Wide Area Network)* – rețele de mari dimensiuni, globale, cuprinzând inclusiv Internetul. Aceste rețele constituie mediul principal de desfășurare a atacurilor ciberneticе, deoarece fiecare strat de comunicare (fizic, legătură de date, rețea, transport, sesiune, prezentare și aplicație) introduce vulnerabilități specifice.

Astfel, *securitatea cibernetică urmărește menținerea confidențialității* (asigurarea că informația nu este accesibilă persoanelor neautorizate), *a integrității* (menținerea acurateței și completitudinii datelor), *a disponibilității* (accesul la informații și resurse atunci când este necesar), precum și *menținerea autenticității*, *responsabilității* și *nonrepudierii* (imposibilitatea ca un expeditor sau destinatar să nu recunoască ulterior implicarea într-o comunicare).

Un *atac cibernetic* reprezintă orice acțiune deliberată menită să degradeze securitatea unui sistem, să perturbe funcționalitatea acestuia sau să obțină acces

¹ Andrew Tanenbaum, *Rețele de Calculatoare*, Editura Computer Press AGORA, 1998.

neautorizat asupra resurselor sistemului. Orice atac poate fi prevenit printr-o serie de *măsuri de control*, care sunt mecanisme preventive, detective sau corective (politici, tehnologii, proceduri) care reduc probabilitatea sau impactul unui atac.

Articolul este organizat astfel: în *Secțiunea 1* prezentăm o scurtă introducere în care sunt amintite conceptele de bază și metodologiile folosite pe parcursul articolului, împreună cu descrierea succintă a structurii lucrării. În *Secțiunea 2* prezentăm principalele atacuri la nivel de rețea și transport, împreună cu o definiție succintă a acestora. În *Secțiunea 3* descriem în detaliu atacul *ARP spoofing/poisoning*, împreună cu mecanismele de detecție și măsurile de prevenire. În *Secțiunea 4* abordăm atacul *SYN flooding*, împreună cu anomaliile specifice în traficul de date, tehnicile de protecție, precum și mecanismele de detecție și măsurile de prevenire. În *Secțiunea 5* analizăm atacul *DNS spoofing/cache poisoning*, indicatorii de compromitere și măsurile de protecție. În final în *Secțiunea 6* formulăm concluziile și direcțiile viitoare, recomandări de prioritizare a controalelor și propuneri de scenarii preventive ale atacurilor prezentate.

Prin această structură, lucrarea prezintă o trecere în revistă a conceptelor de bază ale principalelor atacuri în rețele, realizând în același timp și o analiză tehnică aprofundată a acestor atacuri și, în final, recomandări aplicabile în mediul serviciilor publice instituționale și educaționale.

2. Prezentare generală a atacurilor cibernetice

Deși protocoalele de rețea² sunt deosebit de complexe, fiecare dintre ele au anumite puncte vulnerabile, de exemplu, absența autentificării în ARP, designul handshake-ului în TCP sau lipsa integrității criptografice în rezoluția clasică DNS. De asemenea, amintim că modelul *OSI (Open Systems Interconnection)* este un model de referință folosit în informatică și telecomunicații pentru a descrie cum comunică două calculatoare sau dispozitive într-o rețea. Conform acestui model, procesul de comunicare este împărțit în 7 straturi: 1. *Stratul Fizic* care realizează transmiterea de biți prin cablu, fibră optică sau wireless; 2. *Stratul Legătură de Date* organizează biții în cadre și se ocupă de adresele *MAC (Media Access Control)*; 3. *Stratul Rețea* rutează pachetele prin rețea; 4. *Stratul Transport* asigură transferul corect al datelor; 5. *Stratul Sesiune* gestionează conexiunile și sesiunile dintre două aplicații; 6. *Stratul Prezentare* transformă datele prin criptare, compresie, conversie de format; 7. *Stratul Aplicație* care oferă interfața utilizatorului.

Atacurile cibernetice reprezintă ansamblul tehnicilor și strategiilor prin care un adversar exploatează vulnerabilitățile unui sistem informatic pentru a-i compromite securitatea. Cele mai frecvente atacuri vizează protocoale fundamentale și mecanismele de comunicare esențiale. Ele pot fi clasificate după obiectivul urmărit, precum compromiterea confidențialității (prin spionarea datelor), a integrității (prin alterarea traficului), a disponibilității (prin blocarea serviciilor) sau combinarea acestora. În cele ce urmează vom prezenta trei tipuri de atacuri³ reprezentative pentru straturile de legătură de date, rețea și transport *ARP spoofing/poisoning*, *SYN flooding* și *DNS spoofing/cache poisoning*.

Pe scurt, *ARP spoofing/poisoning* redirecționează traficul în rețele Ethernet prin falsificarea mapărilor IP (Internet Protocol) – MAC (Media Access Control). Astfel, atacatorul trimite răspunsuri ARP false pentru a redirecționa traficul în rețea, derutând

² Douglas Comer, *Computer Networks and Internets*, 6th edition, Pearson Education, 2015.

³ Robbie Myers, *Attacks on TCP/IP Protocols*, Paper Report CPSC4620 Computer Network Security, University of Tennessee, 2021.

utilizatorul care va crede că atacatorul este gateway-ul legitim, iar tot traficul trece prin dispozitivul compromis. Are loc în stratul 2 *Legătură de date*.

SYN flooding exploatează mecanismul de stabilire a conexiunii TCP three-way handshake (procesul de stabilire a conexiunii). Astfel, atacatorul trimite un număr mare de cereri SYN fără a le finaliza, ceea ce epuizează resursele serverului și blochează accesul utilizatorilor legitimi. Afectează stratul 4 *Transport* al procesul de comunicare.

DNS spoofing/cache poisoning constă în compromiterea integrității rezoluției de nume pentru a devia utilizatorii către resurse malițioase. Astfel, atacatorul introduce răspunsuri DNS false într-un server DNS cache redirecționând utilizatorii către site-uri malițioase atunci când tastează nume de domenii legitime. Are loc în stratul 7 *Aplicație* al modelului OSI.

Pe lângă aceste atacuri, literatura de specialitate menționează frecvent și alte atacuri, precum: *DoS (Denial of Service)* care afectează stratul 3 *Rețea* și constă în blocarea disponibilității unui serviciu prin supraîncărcarea rețelei sau serverului cu trafic excesiv, *Man-in-the-Middle* prin care atacatorul se interpune între două entități (victime) și interceptează, modifică sau redirecționează traficul dintre aceste două entități, care cred că comunică direct între ele (dar de fapt ele sunt ascultate de către atacator), *IP Sniffing/Spoofing* constă în capturarea pachetelor de date (sniffing) sau falsificarea acestora (spoofing), pentru a extrage informații, pentru a compromite autenticitatea acestora sau pentru a perturba traficul de date în stratul 3 *Rețea*.

Toate aceste atacuri afectează triada *Confidențialitate, Integritate și Disponibilitate* prin expunerea datelor private, capturarea parolelor prin sniffing, modificarea neautorizată a datelor sau mesajelor sau prin blocarea accesului la resurse.

În secțiunile următoare vom descrie pe larg mecanismele tehnice de funcționare ale fiecărui atac, pașii de execuție, impactul asupra triadei CIA împreună cu metodele de detecție și prevenție pentru fiecare atac.

3. Atacul ARP Spoofing / Poisoning

*ARP (Address Resolution Protocol)*⁴ este protocolul utilizat în rețelele Ethernet pentru a asocia adresele IP cu adresele fizice MAC ale interfețelor de rețea. Funcționarea normală a ARP presupune menținerea unui tabel (ARP cache) pe fiecare dispozitiv, unde sunt stocate aceste mapări IP-MAC pentru a permite transmiterea corectă a pachetelor în rețea. *ARP spoofing* sau *ARP poisoning* este o tehnică prin care un atacator trimite pachete ARP falsificate într-o rețea locală, asociind adresa sa MAC cu adresa IP a unei gazde/victime, cum ar fi gateway-ul implicit (de exemplu, routerul) permițând astfel redirecționarea oricărui trafic destinat adresei IP către adresa MAC a atacatorului. Astfel, traficul destinat gateway-ului este redirecționat către atacator, care poate să îl intercepteze, modifice sau blocheze.

Fluxul unui atac ARP spoofing urmează, în general, următorii pași: 1. Atacatorul se conectează la aceeași rețea locală cu victima și gateway-ul; 2. Atacatorul trimite mesaje ARP Reply false către victimă, anunțând că „IP-ul gateway-ului este la MAC-ul meu”; 3. Victima actualizează cache-ul ARP cu informația falsă; 4. Traficul legitimat pentru gateway este redirecționat prin atacator; 5. Atacatorul poate intercepta traficul (sniffing, exfiltrare

⁴ Rajwinder Kaur, Gurjot Singh, Suman Khurana, "A Security Approach to Prevent ARP Poisoning and Defensive Tools", in *International Journal of Computer and Communication System Engineering (IJCCSE)*, Vol. 2(3), 2015, pp. 431-437.

parole, cookie-uri), modifica pachetele (integritate compromisă, ex. injectare malware), bloca traficul (DoS local).

ARP poisoning utilizează tehnica Man-in-the-Middle pentru a otrăvi rețeaua, precum este prezentat în Figura 1.

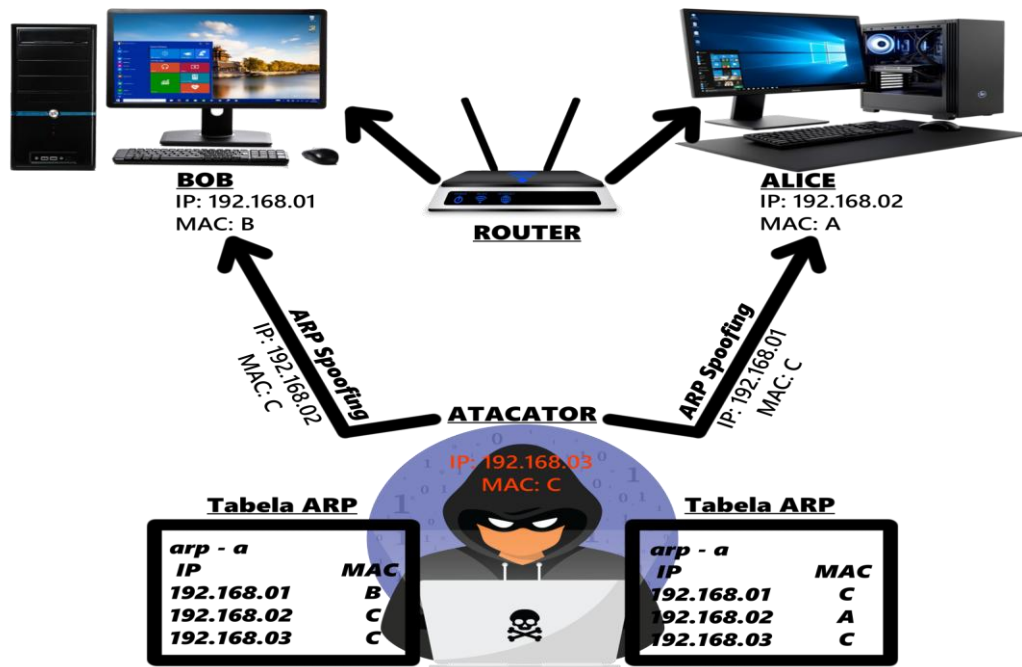


Figura 1. ARP spoofing într-o rețea LAN: atacatorul modifică alternativ adresele MAC ale victimelor Alice și Bob.

În cazul acestui atac, triada CIA este afectată astfel: atacatorul poate citi traficul în clar, parole, date sensibile (Confidențialitatea), datele pot fi modificate în timpul traficului (Integritatea), iar în cazul în care atacatorul nu mai redirecționează pachetele, victima pierde conexiunea (Disponibilitatea). Detectarea unui atac ARP se bazează pe identificarea anomaliilor în tabelele ARP, anume prin detectarea adreselor IP diferite cu același MAC, detectarea pachetelor ARP suspecte folosind instrumente precum Wireshark (un analizor de trafic de rețea utilizat pentru capturarea și inspectarea pachetelor transmise printr-o rețea) sau IDS (Intrusion Detection Systems, software de detectare a activităților malițioase în traficul de date) sau compararea tabelor ARP între mai multe gazde.

În Figura 2 este prezentat un traffic ARP consistent, în care fiecare adresă IP este asociată cu o singură adresă MAC. Într-un scenariu de spoofing, în trafic ar apărea duplicate sau inconsecvențe (IP-uri diferite cu aceeași adresă MAC sau cu diverse adrese MAC).

Prevenirea unui atac ARP spoofing se poate realiza prin folosirea dispozitivelor de tip VPN (Virtual Private Network) care permit conectarea la internet printr-un tunel criptat și care să împiedice conectarea unui posibil atacator. Alte metode constau în folosirea comutatoarelor de tip switch (dispozitive de rețea care limitează capacitatea atacatorilor să folosească pachete sniffer de capturare a informațiilor), configurarea statică sau dinamică (prin intermediul dispozitivelor de tip switch) a tabelor ARP sau criptarea traficului prin folosirea unor protocoale de comunicare securizate unde toate datele sunt criptate.

Time	Source	Destination	Protocol	Length	Info
17 1.965267	SeikoEpson_b9:68:2c	Broadcast	ARP	60	ARP Announcement for 192.168.0.164
256 15.335992	Intel_71:8d:65	SeikoEpson_b9:68:2c	ARP	42	Who has 192.168.0.164? Tell 192.168.0.133
257 15.349552	SeikoEpson_b9:68:2c	Intel_71:8d:65	ARP	42	192.168.0.164 is at dc:cd:2f:b9:68:2c
262 15.933863	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
263 15.933883	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
1605 52.038696	SeikoEpson_b9:68:2c	Broadcast	ARP	60	ARP Announcement for 192.168.0.164
1858 59.193174	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
1859 59.193194	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
2305 88.836409	Intel_71:8d:65	SeikoEpson_b9:68:2c	ARP	42	Who has 192.168.0.164? Tell 192.168.0.133
2306 88.919763	SeikoEpson_b9:68:2c	Intel_71:8d:65	ARP	42	192.168.0.164 is at dc:cd:2f:b9:68:2c
2560 102.009703	SeikoEpson_b9:68:2c	Broadcast	ARP	60	ARP Announcement for 192.168.0.164
2570 102.813010	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
2571 102.813029	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
3122 123.263356	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
3123 123.263370	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
3908 143.723100	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
3909 143.723119	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
4175 151.980752	SeikoEpson_b9:68:2c	Broadcast	ARP	60	ARP Announcement for 192.168.0.164
4467 164.152354	Intel_71:8d:65	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
4468 164.152393	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
4759 184.732791	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
4760 184.732827	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
4986 202.054139	SeikoEpson_b9:68:2c	Broadcast	ARP	60	ARP Announcement for 192.168.0.164
5080 205.102698	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
5081 205.102718	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
5320 225.421788	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
5321 225.421802	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
5683 245.931720	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
5684 245.931735	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
5915 252.025206	SeikoEpson_b9:68:2c	Broadcast	ARP	60	ARP Announcement for 192.168.0.164
6607 266.691546	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
6608 266.691567	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
7095 291.271950	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
7096 291.271970	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65
7243 301.996155	SeikoEpson_b9:68:2c	Broadcast	ARP	60	ARP Announcement for 192.168.0.164
7363 311.552120	TpLinkTechno_3a:a4:...	Intel_71:8d:65	ARP	42	Who has 192.168.0.133? Tell 192.168.0.1
7364 311.552140	Intel_71:8d:65	TpLinkTechno_3a:a4:...	ARP	42	192.168.0.133 is at e0:c2:64:71:8d:65

Figura 2. Prezintă un trafic ARP normal în rețea (captură în Wireshark), fiecărei adrese IP îi corespunde o singură adresă MAC.

4. Atacul SYN Flooding

Protocolul *TCP (Transmission Control Protocol)*⁵ utilizează un mecanism specific de stabilire a unei conexiuni numit *three-way handshake*, care funcționează astfel: într-o primă fază clientul transmite un pachet *SYN (synchronize)* către server, operație la care serverul răspunde cu *SYN-ACK (synchronize-acknowledge)*, după care clientul finalizează cu un *ACK (acknowledge)*, iar conexiunea devine activă (Figura 3). Într-un atac *SYN flooding* atacatorul trimite un volum mare de pachete SYN către server folosind adrese IP deteriorate care determină serverul să trimită o replică de tip SYN-ACK, fără să finalizeze transmisia prin trimiterea unui pachet final de tip ACK. Astfel, serverul își lasă porturile pe jumătate deschise, alocând resurse pentru conexiuni care nu vor fi niciodată finalizate, epuizându-și memoria și tabelele de conexiuni. Ca urmare a atacului, serverul nu va mai putea răspunde cererilor legitime ale utilizatorilor autorizați (care nu se vor mai putea conecta la server), ducând în cele din urmă la un *Denial of Service*.

⁵ Mitko Bogdanoski, Tomislav Shuminoski, Aleksandar Risteski, "Analysis of the SYN Flood DoS Attack", in *International Journal of Computer Network and Information Security*, Vol. 8, 2013, pp. 1-11.

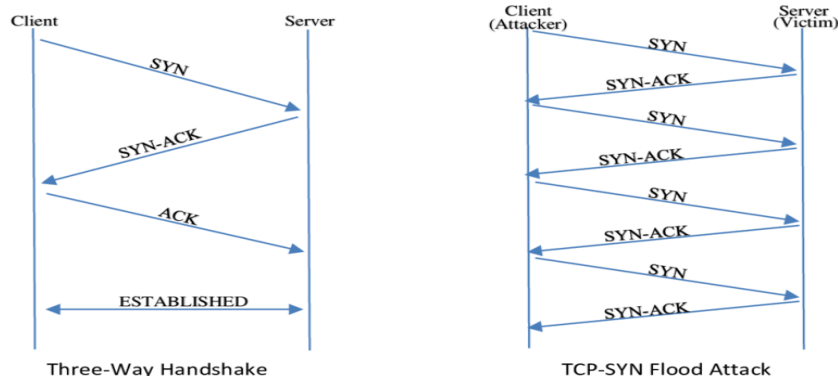


Figura 3. TCP three-way handshake versus atac SYN flooding

Fluxul unui atac SYN flooding urmează următorii pași: 1. Atacatorul trimite sute de cereri SYN către server, uneori cu adrese IP false (IP spoofing); 2. Serverul răspunde fiecărei cereri cu SYN-ACK și rezervă resurse; 3. Atacatorul nu răspunde printr-un ACK final, forțând serverul să rămână cu conexiunile în așteptare (semi-deschise), caz în care intră într-o stare de tip SYN-Received (folosită pentru orice conexiune pe jumătate deschisă, Figura 4; 4. După ce tabelul de conexiuni al serverului se umple, acesta nu mai poate răspunde utilizatorilor legitimi.

```
root@ubuntu:/home/azabo# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                  :::*                    LISTEN
tcp6       0      0 :::22                  :::*                    LISTEN
tcp6       0      0 192.168.0.3:21         15.148.8.57:1158       SYN_RECV
tcp6       0      0 192.168.0.3:21         141.123.60.109:60938   SYN_RECV
tcp6       0      0 192.168.0.3:21         140.253.11.140:1165    SYN_RECV
tcp6       0      0 192.168.0.3:21         125.175.250.192:60948  SYN_RECV
tcp6       0      0 192.168.0.3:21         81.74.240.155:1152     SYN_RECV
tcp6       0      0 192.168.0.3:21         250.208.39.57:60939    SYN_RECV
tcp6       0      0 192.168.0.3:21         121.26.124.155:1151    SYN_RECV
tcp6       0      0 192.168.0.3:21         64.87.88.43:60941     SYN_RECV
tcp6       0      0 192.168.0.3:21         106.0.23.64:1156      SYN_RECV
tcp6       0      0 192.168.0.3:21         66.253.255.138:1162    SYN_RECV
tcp6       0      0 192.168.0.3:21         175.113.180.100:60951  SYN_RECV
tcp6       0      0 192.168.0.3:21         218.68.79.178:1157     SYN_RECV
tcp6       0      0 192.168.0.3:21         135.219.175.172:1159   SYN_RECV
tcp6       0      0 192.168.0.3:21         56.219.87.42:60953     SYN_RECV
tcp6       0      0 192.168.0.3:21         8.12.17.163:1153       SYN_RECV
tcp6       0      0 192.168.0.3:21         6.217.149.253:60947    SYN_RECV
tcp6       0      0 192.168.0.3:21         8.155.151.16:1161      SYN_RECV
tcp6       0      0 192.168.0.3:21         83.150.161.20:60940    SYN_RECV
tcp6       0      0 192.168.0.3:21         215.172.115.161:60942  SYN_RECV
tcp6       0      0 192.168.0.3:21         155.169.100.195:60945  SYN_RECV
tcp6       0      0 192.168.0.3:21         218.106.219.43:60949   SYN_RECV
tcp6       0      0 192.168.0.3:21         157.212.21.250:1150    SYN_RECV
tcp6       0      0 192.168.0.3:21         3.159.115.57:60943     SYN_RECV
tcp6       0      0 192.168.0.3:21         203.243.0.218:1160     SYN_RECV
tcp6       0      0 192.168.0.3:21         214.29.253.195:60946   SYN_RECV
tcp6       0      0 192.168.0.3:21         61.249.92.86:1155      SYN_RECV
tcp6       0      0 192.168.0.3:21         215.130.249.47:60950   SYN_RECV
tcp6       0      0 192.168.0.3:21         186.43.16.250:1163     SYN_RECV
tcp6       0      0 192.168.0.3:21         172.131.186.98:1154    SYN_RECV
tcp6       0      0 192.168.0.3:21         66.94.107.89:60944     SYN_RECV
tcp6       0      0 192.168.0.3:21         128.170.1.74:1164      SYN_RECV
tcp6       0      0 192.168.0.3:21         105.46.255.151:60952   SYN_RECV
```

Figura 4. Simularea unui atac SYN flooding în care se observă multitudinea de stări SYN-Received provocate de adresele IP aleatoare ale atacatorului (Foreign address) menite să provoace un Denial of Service.

Principalul impact al acestui atac asupra triadei CIA este provocat de Denial of Service. Dacă utilizatorii nu pot accesa datele, acestea devin indisponibile, ceea ce afectează Disponibilitatea datelor, serviciul devenind inaccesibil. În mod indirect vor fi afectate atât Confidențialitatea, cât și Integritatea datelor.

Detectarea unui atac SYN flooding se realizează prin monitorizarea tabelului de conexiuni (detectarea unui număr mare de conexiuni SYN semi-deschise în starea SYN-

Received), prin detectarea creșterilor exagerate ale numărului de pachete SYN comparativ cu pachetele ACK, utilizarea analizorului Wireshark sau a instrumentelor de tip IDS (Sistem de Detecție a Intruziunilor) și IPS (Sistem de Prevenire a Intruziunilor) pentru a monitoriza traficul de rețea și a identifica atacurile cibernetice.

Un atac SYN flooding poate fi prevenit prin folosirea unor SYN cookies (mecanisme prin care serverul nu alocă resurse până când clientul nu trimite un ACK final), prin reducerea temporizatorului SYN-received, prin folosirea de firewall-uri și proxy-uri (dispozitive care filtrează și distribuie traficul), prin limitarea numărului de cereri SYN acceptate per secundă sau prin filtrarea IP spoofing, ducând la blocarea pachetelor provenite de la adrese inexistente sau nealocate.

5. Atacul DNS Cache Poisoning

DNS (Domain Name System)⁶ este protocolul responsabil pentru traducerea numelor de domenii (ex. *www.google.com*) în adrese IP corespunzătoare (ex. *64.233.191.255*). În momentul în care am introdus în bara de adrese a unui browser o astfel de adresă, acesta va încerca să identifice în baza de date a serverelor DNS adresa IP asociată numelui de domeniu furnizat, se conectează la adresa IP găsită și vizualizează informațiile (pagina web) corespunzătoare (mecanism reprezentat în Figura 5). Pentru eficiență, serverele DNS păstrează aceste mapări în memoria cache (DNS cache). Operația de identificare a adreselor IP se face prin intermediul unui *DNS resolver*. Când un server DNS primește o cerere, acesta va căuta numele cerut în propriul cache. În cazul în care nu îl găsește, va interoga alte servere, pentru rezolvarea numelui, primind un răspuns din partea lor. Mai mult, un DNS resolver salvează răspunsurile referitoare la adresa IP căutată pentru o anumită perioadă de timp. În acest fel, resolver-ul poate răspunde la interogările viitoare mult mai rapid, fără a fi nevoie să comunice cu numeroasele servere implicate în procesul tipic de rezoluție DNS.

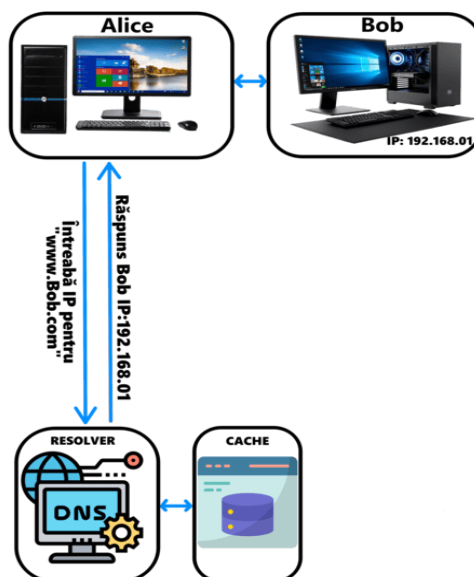


Figura 5. Funcționarea protocolului DNS - responsabil pentru determinarea adresei IP asociată unui site web.

⁶ Osama Alsad, Qasem Abu Al-Haija, "DNS Cache Poisoning Attack Detection: A Systematic Review", in *Proceedings of the 7th IET Smart Cities Symposium*, 2023, pp. 426-432.

DNS cache poisoning (sau *DNS spoofing*) este un atac de tip *DDoS* (*Distributed Denial of Service*) prin care atacatorul falsifică răspunsurile primite de un DNS resolver de la serverele interogate. Adresele IP falsificate vor fi păstrate în memoria cache a resolver-ului până la expirarea perioadei de timp alocate, devenind victimă a unui atac de tip DNS cache poisoning.

Astfel, atunci când utilizatorii cer rezoluția unui domeniu legitim, DNS resolver-ul va returna o adresă IP falsă, direcționând traficul către un server controlat de atacator (Figura 6).

Mecanismul de funcționare al unui atac DNS poisoning⁷ urmează următorii pași:

1. Utilizatorul solicită rezoluția unui domeniu (ex. *www.google.com*);
2. Serverul DNS interoghează alte servere pentru rezoluție;
3. Atacatorul trimite un răspuns fals mai rapid decât serverul legitim, conținând o adresă IP controlată de el;
4. Serverul DNS stochează această mapare falsă în cache;
5. Utilizatorii care solicită același domeniu vor fi redirecționați către serverul atacatorului.

Deoarece acest atac redirecționează utilizatorii către site-uri false controlate de către atacator, datele transmise de către utilizatori devin vizibile pentru atacant, conducând atât la compromiterea Confidențialității și a Integrității datelor private, cât și la compromiterea Disponibilității deoarece serviciile legitime devin inaccesibile pentru utilizatori, care ajung doar pe serverul atacatorului.

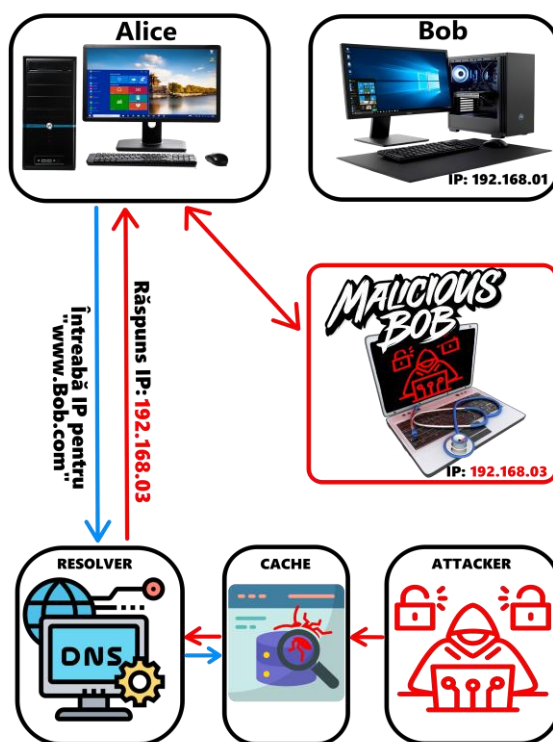


Figura 6. Funcționarea atacului DNS cache poisoning: Alice este forțată de către atacator să acceseze o adresă IP greșită pentru site-ul *www. Bob.com*, conducând-o către un site fake *www. Bob.com*.

⁷ Sooel Son, Vitaly Shmatikov, *The Hitchhiker's Guide to DNS Cache Poisoning*, Paper Report, University of Texas, 2010, https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf.

Detectarea unui atac DNS poisoning se poate realiza printr-o monitorizare a cache-ului DNS prin verificarea periodică a intrărilor DNS, prin compararea răspunsurilor DNS folosind mai multe servere DNS resolver și compararea răspunsurilor primite, sau prin folosirea instrumentelor IDS/IPS (menite să detecteze răspunsurile suspecte), sau a capturilor de trafic cu Wireshark.

Un atac DNS poisoning poate fi prevenit prin folosirea extensiilor de securitate *DNSSEC (Domain Name System Security Extensions)* cu rolul de a adăuga semnături digitale răspunsurilor DNS, permițând verificarea autenticității acestora, folosirea tehnicilor de validare și semnare a datelor DNS, configurarea serverelor DNS pentru a utiliza surse de încredere, monitorizarea continuă și validarea multiplă a rezoluțiilor DNS, reducerea timpului de stocare a răspunsurilor primite de la serverele interogate, utilizarea criptării interogărilor DNS cu rol de a împiedica interceptarea și modificarea interogărilor DNS.

Concluzii

Studiul atacurilor cibernetice la nivel de rețea evidențiază faptul că securitatea informatică nu mai poate fi privită ca un aspect opțional, ci ca o necesitate fundamentală. Analiza atacurilor ARP spoofing/poisoning, SYN flooding, DNS cache poisoning, dar și a altor tehnici precum Denial of Service și Man-in-the-Middle, demonstrează că vulnerabilitățile rețelelor provin adesea din protocoale esențiale, concepute inițial fără mecanisme avansate de protecție.

Impactul acestor atacuri asupra triadei *Confidențialitate, Integritate, Disponibilitate* constă în compromiterea confidențialității datelor prin interceptări și redirectionări ale mesajelor, în alterarea integrității informațiilor prin injectarea de informații și date false sau prin supra-aglomerarea traficului în rețele, conducând în final la indisponibilitatea serviciilor prin supra-încărcarea și blocarea acestora.

În același timp, studiul metodelor de detecție și prevenție arată că există soluții concrete și eficiente, de la tehnologii clasice (tabele ARP statice, SYN cookies, filtrare IP) la mecanisme moderne (DNSSEC, criptare end-to-end, IDS/IPS avansate sau folosirea comutatoarelor switch). Totuși, niciuna dintre aceste soluții nu este suficientă, astfel încât securitatea trebuie abordată și printr-o strategie stratificată și proactivă, care să combine măsuri tehnice, bune practici organizaționale și o educație continuă a utilizatorilor.

În concluzie, securitatea cibernetică este un domeniu dinamic, aflat într-o continuă luptă între metodele de atac și mecanismele de apărare⁸. O rețea protejată nu înseamnă doar implementarea unor soluții tehnologice, ci și o înțelegere profundă a riscurilor, o monitorizare permanentă și o adaptare constantă la noile amenințări.

În acest articol am realizat o prezentare sistematică a trei atacuri principale la nivel de legătură de date, rețea și transport, anume ARP spoofing/poisoning, SYN flooding și DNS spoofing/cache poisoning. Am prezentat mecanismele de funcționare, de protecție și apărare, precum și consecințele acestora asupra *Confidențialității, Integrității și Disponibilității* datelor.

References

Osama Alsad, Qasem Abu Al-Haija, "DNS Cache Poisoning Attack Detection: A Systematic Review", in *Proceedings of the 7th IET Smart Cities Symposium 2023*, pp. 426-432.

⁸ William Stallings, *Network Security Essentials: Applications and Standards*, 6th edition, Pearson Education, 2020.

- Mitko Bogdanoski, Tomislav Shuminoski, Aleksandar Risteski, "Analysis of the SYN Flood DoS Attack", in *International Journal of Computer Network and Information Security*, Vol. 5(8), 2013, pp. 1-11.
- Douglas Comer, *Computer Networks and Internets*, 6th edition, Pearson Education, 2015.
- Rajwinder Kaur, Gurjot Singh, Suman Khurana, "A Security Approach to Prevent ARP Poisoning and Defensive tools", in *International Journal of Computer and Communication System Engineering*, Vol. 2(3), 2015, pp. 431-437.
- Andrew Lockhart, *Network Security Hacks*, O'Reilly Media Press, 2007.
- Robbie Myers, *Attacks on TCP/IP Protocols*, Paper Report CPSC462o Computer Network Security, University of Tennessee, 2021.
- Soel Son, Vitaly Shmatikov, *The Hitchhiker's Guide to DNS Cache Poisoning*, Paper Report, University of Texas, 2010,
https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf.
- William Stallings, *Network Security Essentials: Applications and Standards*, 6th edition, Pearson Education, 2020.
- Andrew Tanenbaum, *Rețele de Calculatoare*, Editura Computer Press AGORA, 1998.