Ministerul Educaţiei și Cercetării

al Republicii Moldova   
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, Infromatică și Microelectronică   
  
  
  
  
  
  
  
RAPORT

# LUCRARE DE LABORATOR NR. 3

# la Tehnologii ale securității informaționale

**Tema:** Tipuri de atacuri în SI. Analiza tehnicilor de inginerie socială. Capturarea și analiza traficului. Simularea atacurilor DoS.

A efectuat:

st. gr. TI-211 Popa Cătălin

A verificat: Octavian Răducanu

UTM, Chișinău 2023

**Tema:**

Tipuri de atacuri în SI. Analiza tehnicilor de inginerie socială. Capturarea și analiza traficului. Simularea atacurilor DoS.

**Scopul lucrării:**

1. **Atacuri de tip Ingineria Socială**

2. **Studierea atacurilor de tip man-in-the-middle**

3. **Atacuri de tip DoS (Denial of Service)/DDoS (Distributed Denial of Service)**

4. **Atacuri de tip forța brută (Brute-Force).**

**Sarcina de bază:**

* Prezentați exemple de atacuri de tip inginerie socială
* Studierea metodelor și tehnicilor atacurilor de tip phishing
* Stabilirea recomandărilor și metodelor de protecție
* Exercițiu de interceptare a traficului local și din rețea
* Instrumente recomandate: Wireshark, Ettercap,  Essential netTools
* Simularea unui atac de tip DoS
* Instrumente Recomandate: Dsniff, Kali Linux, Mașini Virtuale
* Realizarea unui atac de tip forța brută asupra unui mediu controlat
* Studierea, testarea diferitor instrumente precum ncrack, hydra, medusa
* Obținerea parolelor WiFi și studierea vulnerabilităților WPS

**1. Atacuri de tip Ingineria Socială**

**Exemple de atacuri de tip inginerie socială**

**Atacurile de inginerie socială sunt metode prin care un atacator încearcă să convingă sau să manipuleze o persoană pentru a divulga informații confidențiale sau pentru a efectua anumite acțiuni care să îi permită atacatorului să obțină acces la sisteme sau date. Iată câteva exemple comune de atacuri de inginerie socială:**

* Phishing - un atacator trimite un e-mail sau un mesaj fals, care pare să fie de la o companie sau instituție de încredere, în scopul de a convinge victima să furnizeze informații personale, cum ar fi parole sau date de card de credit.
* Spear phishing - această metodă de atac este similară cu phishing-ul, dar este mai sofisticată și se concentrează asupra unei singure persoane sau grup restrâns de persoane, cum ar fi angajații unei companii. Atacatorul folosește adesea informații personale sau detalii despre companie pentru a face mesajul să pară mai credibil.
* Vishing - atacatorul sună victima în numele unei companii sau instituții de încredere și încearcă să o convingă să dezvăluie informații personale, cum ar fi parole sau numere de card de credit.
* Pretexting - atacatorul se prezintă drept o altă persoană sau instituție, cum ar fi un coleg de muncă, un furnizor sau un reprezentant al guvernului, și încearcă să obțină informații personale sau să determine victima să efectueze o anumită acțiune.
* Baiting - atacatorul oferă ceva gratuit, cum ar fi un stick USB, pentru a atrage victima să descarce un virus sau alt program malware pe computerul lor.
* Quid pro quo - atacatorul oferă ceva în schimb pentru informațiile personale sau pentru accesul la un sistem, cum ar fi un voucher sau un discount, pentru a convinge victima să dezvăluie informații.

Acestea sunt doar câteva exemple de atacuri de inginerie socială. Atacatorii pot folosi o varietate de metode și tehnici pentru a obține informații sau acces la sisteme și date. Prin urmare, este important să fii întotdeauna atent la cererile sau mesajele suspecte și să nu dezvălui informații personale sau să efectuezi acțiuni până când nu ai verificat autenticitatea lor.

**Studierea metodelor și tehnicilor atacurilor de tip phishing**

Phishing este o metodă de atac de inginerie socială în care atacatorul trimite un mesaj fals, care pare să provină de la o sursă de încredere, cum ar fi o bancă sau o companie, în încercarea de a convinge victima să furnizeze informații personale sau să efectueze o acțiune nedorită. Iată câteva metode și tehnici comune utilizate în atacurile de phishing:

* E-mail phishing - atacatorul trimite un e-mail fals care pare să provină de la o companie sau instituție de încredere. Mesajul poate solicita victimei să furnizeze informații personale, cum ar fi numele de utilizator și parola, sau să descarce un fișier sau să acceseze un link care conduce la un site web fals.
* Smishing - atacatorul trimite un mesaj text (SMS) fals, care pare să provină de la o companie sau instituție de încredere, solicitând victimei să furnizeze informații personale sau să descarce un fișier sau să acceseze un link care conduce la un site web fals.
* Tab-uri de phishing - atacatorul creează o pagină web falsă, care arată similar cu site-ul unei companii sau instituții de încredere, în încercarea de a convinge victima să furnizeze informații personale. Această pagină web poate fi accesată prin intermediul unui link dintr-un e-mail sau un mesaj text fals.
* Pharming - atacatorul modifică setările de rețea ale victimei pentru a o redirecționa către o pagină web falsă atunci când încearcă să acceseze site-ul unei companii sau instituții de încredere. Acest tip de atac poate fi dificil de detectat, deoarece victima nu accesează în mod activ o pagină web falsă.
* Spear phishing - atacatorul personalizează mesajul phishing pentru a-l face mai credibil și mai relevant pentru victima sa. De exemplu, atacatorul poate folosi informații personale despre victima sa, cum ar fi numele sau numărul de angajat, pentru a crea un mesaj care pare să fie autentic.
* Whale phishing - acest tip de atac se concentrează asupra unei persoane importante, cum ar fi un CEO sau un oficial guvernamental. Atacatorul folosește adesea pretexte sofisticate și persoane false pentru a obține informații confidențiale sau pentru a obține acces la sisteme.

Acestea sunt doar câteva exemple de metode și tehnici utilizate în atacurile de phishing. Victimele pot fi protejate prin utilizarea de software antivirus și anti-phishing, evitând clicul pe link-uri sau descărcarea de fișiere suspecte și, în general, fiind atente la cererile suspecte sau neașteptate.

Stabilirea recomandărilor și metodelor de protecți

Iată câteva recomandări și metode de protecție împotriva atacurilor de tip inginerie socială:

* Fiți atenți la cererile suspecte sau neașteptate - Dacă primiți un e-mail sau un mesaj text care pare suspect sau neașteptat, nu furnizați informații personale sau nu efectuați acțiuni solicitate fără a verifica întâi sursa mesajului.
* Verificați adresa de e-mail sau numărul de telefon - În cazul în care primiți un mesaj care pare să provină de la o companie sau instituție de încredere, verificați cu atenție adresa de e-mail sau numărul de telefon. Adresa sau numărul pot fi similare, dar diferă cu câteva caractere, ceea ce indică faptul că mesajul este fals.
* Utilizați autentificarea cu doi factori - Autentificarea cu doi factori este o metodă eficientă de a proteja conturile online împotriva atacurilor de inginerie socială. Aceasta implică furnizarea de informații suplimentare pentru a confirma identitatea utilizatorului, cum ar fi un cod de verificare primit prin SMS sau o aplicație de autentificare.
* Instalați software de securitate - Utilizați software de securitate pentru a vă proteja împotriva atacurilor de phishing, malware sau viruși. Asigurați-vă că software-ul este actualizat și rulați verificări periodice ale sistemului.
* Fiți atenți la informațiile personale pe rețelele de socializare - Nu furnizați informații personale sensibile, cum ar fi numele complet, adresa, numărul de telefon sau informații financiare, pe rețelele de socializare. Aceste informații pot fi utilizate pentru a vă încerca identitatea sau pentru a vă ataca cu mesaje de phishing personalizate.
* Educați-vă cu privire la tehnici și metode de atac - Educați-vă cu privire la tehnici și metode de atac de inginerie socială pentru a putea recunoaște și evita astfel de atacuri. Fiți atenți la noutățile în domeniul securității cibernetice și la sfaturile de securitate din partea experților.

Acestea sunt câteva recomandări și metode de protecție împotriva atacurilor de tip inginerie socială. Este important să fii atent și să-ți protejezi informațiile personale pentru a evita astfel de atacuri.

**2. Studierea atacurilor de tip man-in-the-middle**

La prima rulare după instalarea aplicaţiei va fi afişată o interfaţă grafică simila- ră celei din Figura 1.

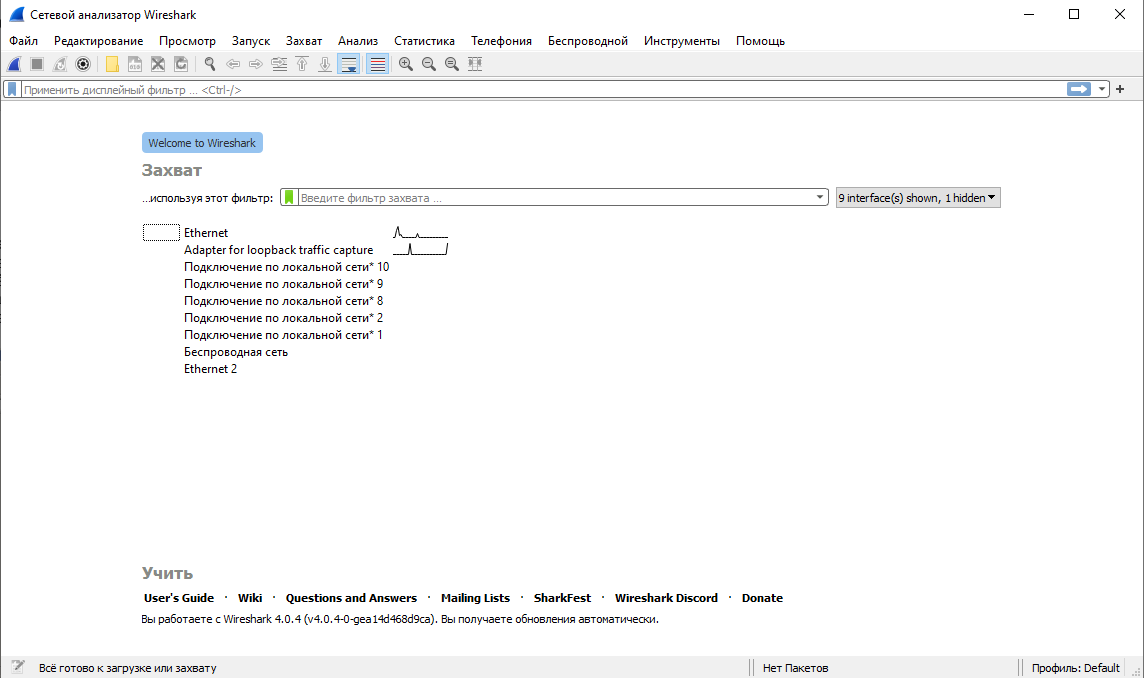


Figura 1. Aplicatia WireShark la start

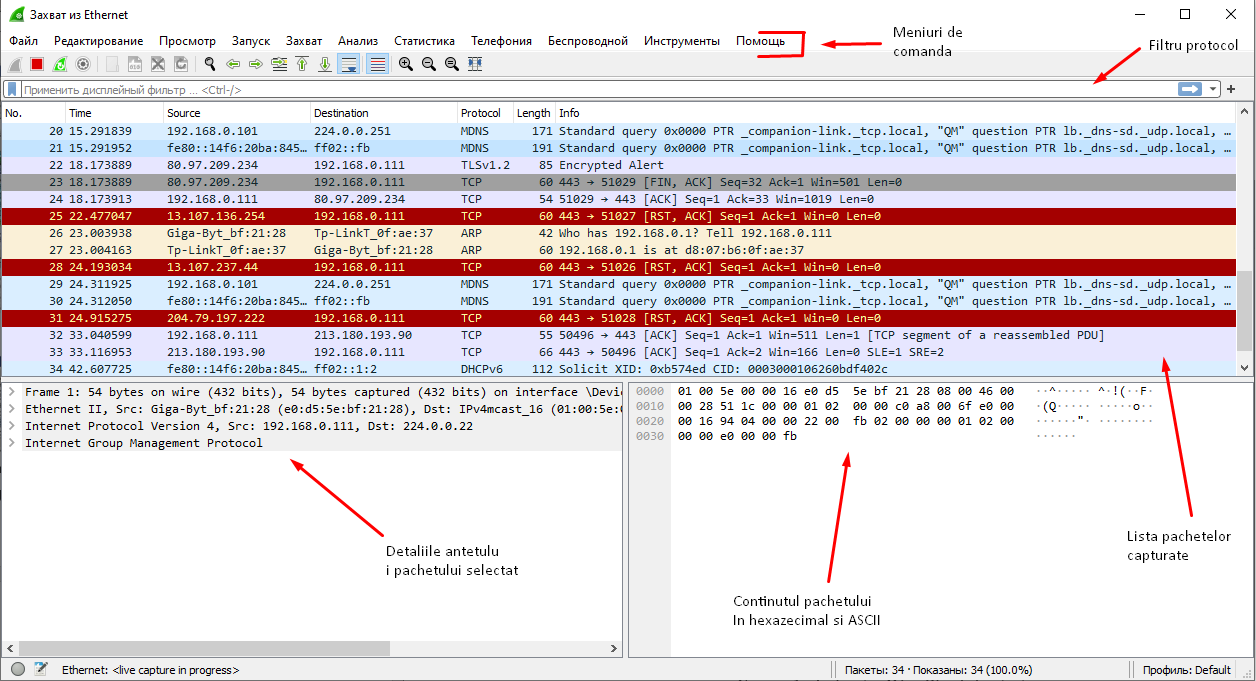


Figura 2. Interfața grafică – detalii

După cum se poate observa în Figura 2, interfaţa grafică este alcătuită din 5 componente majore:

* Meniurile de comandă: meniuri standard pentru aplicaţiile windows. De un in- teres mai mare sunt **File** şi **Capture**. Meniul File permite salvarea de capturi în

fişiere sub diverse formate, sau încărcarea unor capturi salvate anterior. Este suportat inclusiv formatul de fişier creat de către Microsoft Network Monitor (un interceptor de pachete oferit de către Microsoft).

* Fereastra de listare a pachetelor: afişează un sumar de o linie pentru fiecare pachet capturat. Ordonarea pachetelor se poate realiza dupa oricare din câm-

purile afişate pentru acestea. Sumarul afişat conţine un număr de ordine alo- cat de către wireshark (acesta nu face parte din nici un antet), momentul de timp la care s-a realizat captura, adresa sursă respectiv destinaţie a pachetu- lui, tipul protocolului şi informaţii specifice protocolului pentru pachetul curent.

* Fereastra de listare a detaliilor de antet: aceasta oferă detalii legate de pache- tul selectat în fereastra de listare a pachetelor. Informaţiile se referă la antetul Ethernet şi la datagrama IP care conţine pachetul curent. Nivelul de detalii le-

gate de Ethernet sau IP poate fi controlat prin expandarea sau ascunderea in- formaţiilor detaliate cu ajutorul semnelor „**+**” sau „**-**”. Dacă pachetul a fost transferat la nivelul transport folosind TCP sau UDP, atunci vor fi afişate detalii legate de antetul TCP sau UDP, detalii ce pot fi din nou expandate sau ascun- se ca şi în cazul IP. În final sunt oferite detalii legate de cel mai înalt protocol

folosit – cel de la nivelul Aplicaţie. Dacă protocolul este unul comun (cum ar fi HTTP) atunci antetul HTTP va putea fi expandat în detaliu până la nivelul co- menzilor şi parametrilor elementari.

* Fereastra de afişare a conţinutului pachetului: aceasta fereastră afişează con- ţinutul întregului cadru Ethernet capturat, atât hexazecimal cât şi valorile echi- valente ASCII (lucru util daca la nivelul Aplicaţie avem de-a face cu un protocol

bazat pe text, cum este HTTP sau SMPT). După cum se observă în Figura 3, detaliile selectate în fereastra de listare a detaliilor sunt evidenţiate şi din punct de vedere al conţinutului în fereastra de afişare a conţinutului pachetului (a se vedea valoarea identificatorului de sesiune).

* Filtrul de control: această casetă permite specificarea unui filtru ce va fi aplicat asupra pachetelor afişate. Astfel, dacă este specificat DNS în această case-

tă, în fereastra de listare a pachetelor vor apare exclusiv pachetele ce au fost generate de aplicaţii ce implementează acest protocol. Un astfel de exemplu a fost ilustrat în Figura 4.

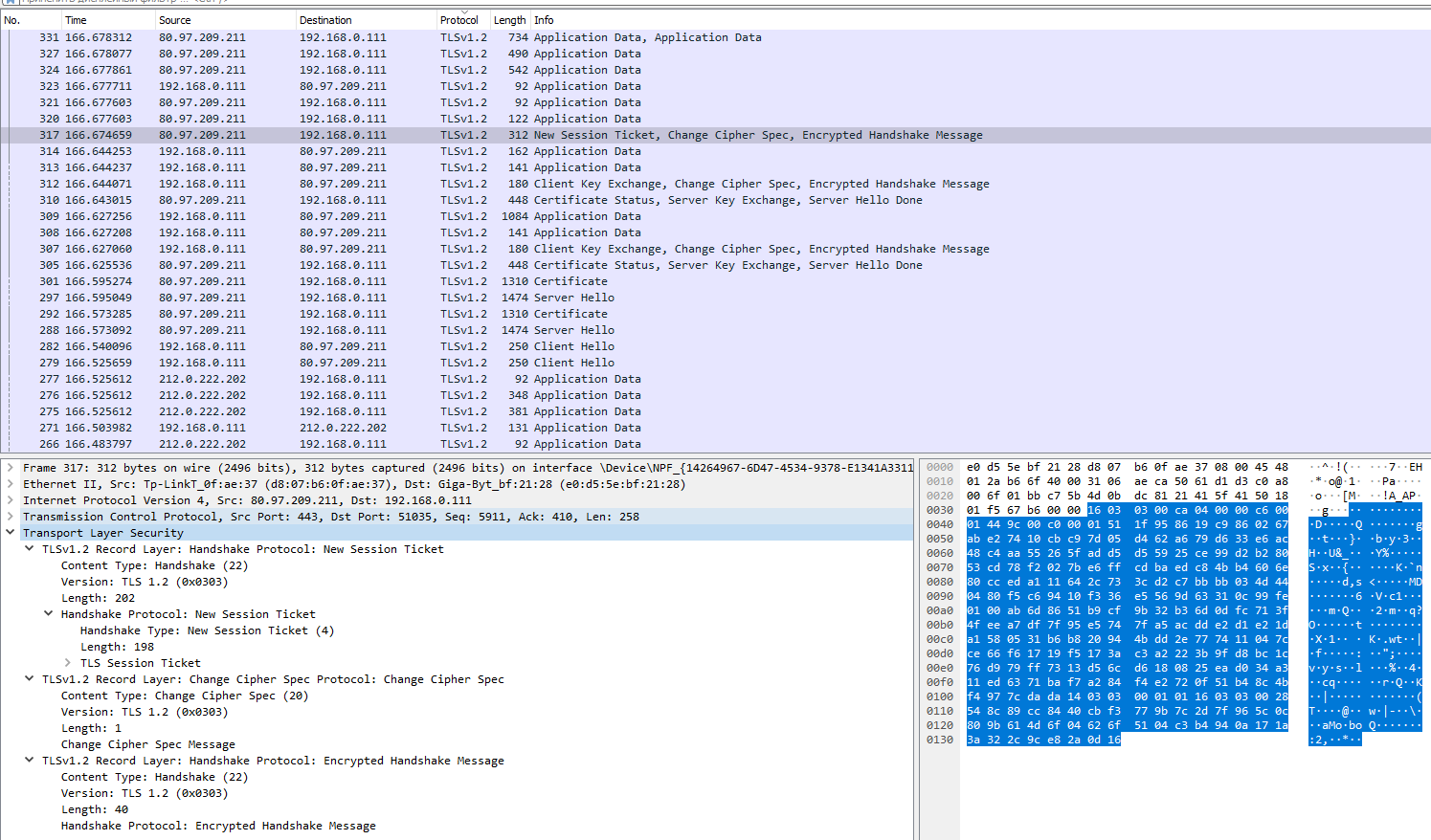


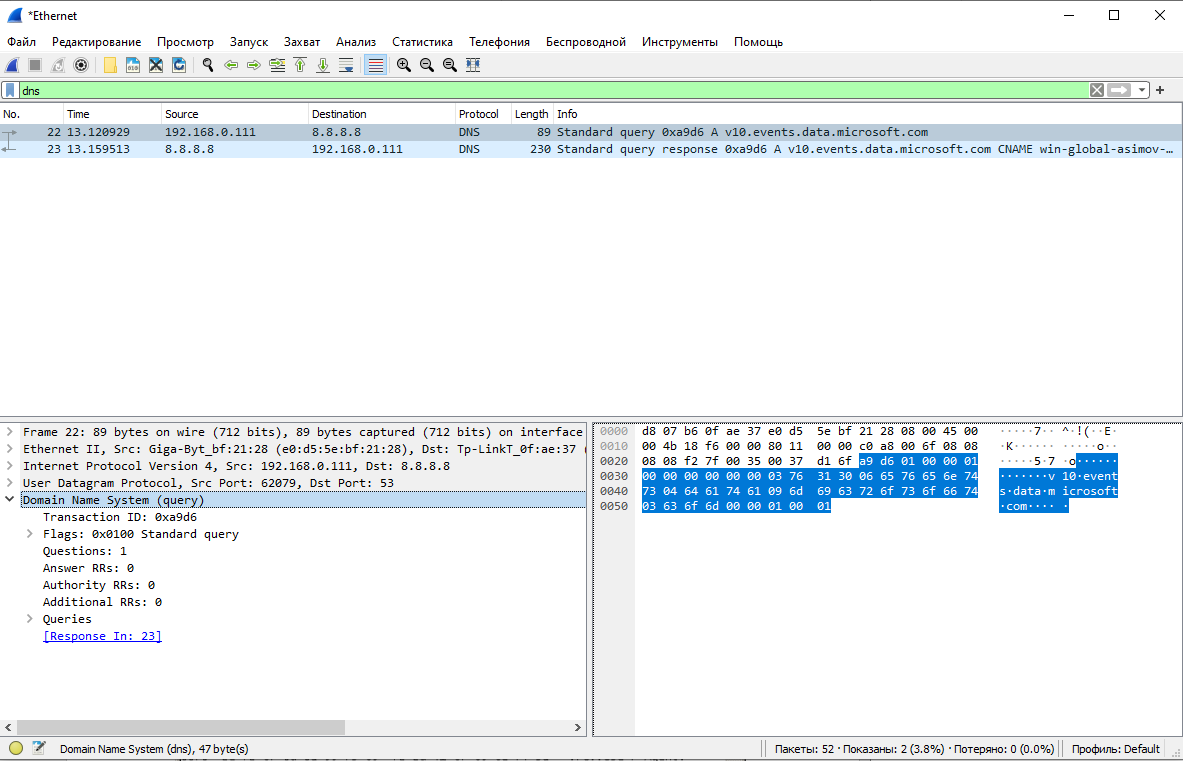
Figura 3. Exemplu

Figura 4. Protocolul DNS

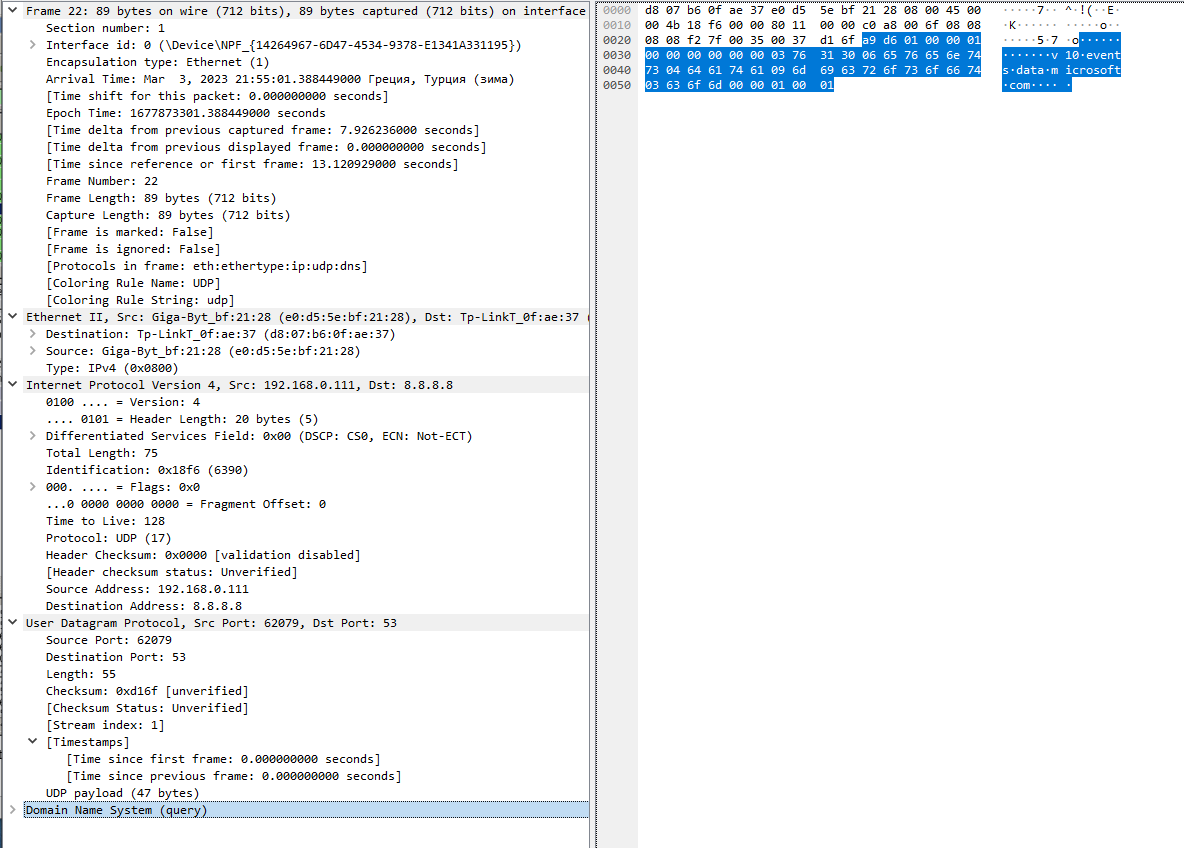


Figura 5. Toate detaliile antetului pachetului selectat

În figura 5, observăm toate detaliile antetului care aparțin pachetului selectat.

Acum voi rula pagina web <http://fcim.utm.md>. După ce pagina s-a încărcat cu succes, am apăsat butonul stop, pentru a opri capturarea. De asemenea am introdus filtrul http, pentru a găsi mult mai rapid pachetul necesar. Astfel numărul mare de pachete a fost redus doar la 2, unul dintre care fiind cel de care am avut nevoie. Astfel, am selectat pachetul conținând cererea HTTP emisă de către navigator în momentul în care a fost solicitată pagina de bază de la <http://fcim.utm.md>. Acum putem afla informații detaliate legate de acest pachet, așa cum a fost ilustrat in figura 6, unde după cum se remarcă, pot fi vizualizate date foarte detaliat legate de câmpurile antetului HTTP, ceea ce ajută la o mai bună înțelegere a protocolului în sine.

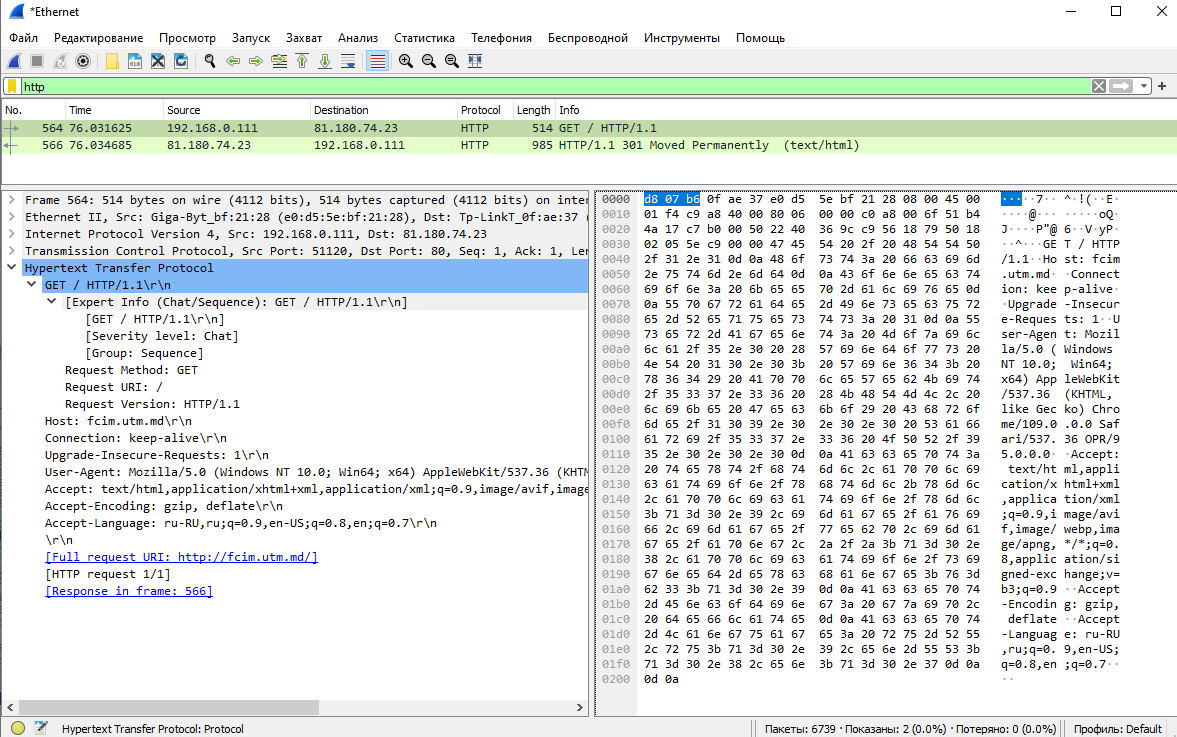


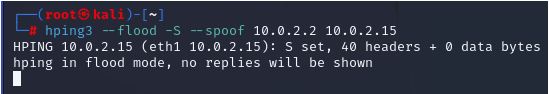
Figura 6. Informatii detaliate dupa deschiderea fcim.utm

**3. Atacuri de tip DoS (Denial of Service)/DDoS (Distributed Denial of Service)**

**Un atac DoS (Denial of Service) este un tip de atac cibernetic prin care se încearcă blocarea sau perturbarea accesului la un sistem sau serviciu online pentru utilizatori legitimi. Acest lucru se face prin inundarea sistemului sau serviciului cu trafic fals sau neautorizat, astfel încât acesta să devină inaccesibil sau să funcționeze foarte încet.Un atac DoS poate fi realizat prin utilizarea unor programe specializate numite "botnet" sau prin trimitera unui număr mare de cereri către un server în același timp. Aceste acțiuni pot duce la supraîncărcarea serverului și la blocarea accesului pentru utilizatorii legitimi.**

**Pentru a realiza un DoS atac, am folosit unelta hping3.**

**hping3 este o unealtă de rețea capabilă să trimită pachete ICMP/UDP/TCP personalizate și să afișeze răspunsurile țintă, asemenea ping-ului, care afișează răspunsurile ICMP. Această unealtă se ocupă de fragmentare și de corpul și dimensiunea arbitrare a pachetelor și poate fi folosită pentru transferul de fișiere sub protocoalele suportate. Folosind hping3, puteți testa regulile de firewall, efectua scanarea porturilor (spoofed), testa performanța rețelei folosind diferite protocoale, face descoperirea Path MTU, efectua acțiuni similare cu traceroute sub diferite protocoale, identifica sistemele de operare de la distanță, efectua auditul stivelor TCP/IP, etc. hping3 poate fi scriptabil folosind limbajul Tcl. În figura 7, observăm cum am folosit unelta respectivă.**



**Figura 7. hping3**

Pentru a realiza atacul respectiv, avem nevoie de adresa IPv4 și adresa Default Gateway. Ele pot fi aflate prin introducerea comenzii ipconfig în cmd. În figura 8, este arătat exemplu de afișare a datelor.

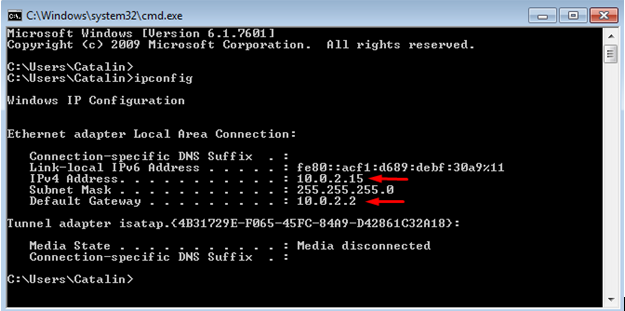


Figura 8. Informații internet

După introducerea comenzii, putem verifica cu ajutorul comenzii ping, pentru a observa legătura și dacă are loc transmiterea de date. În figura 9, putem observa că la încercarea creării legăturii cu google.com, ne dă respins, astfel înseamnă că deja are loc atacul DoS.

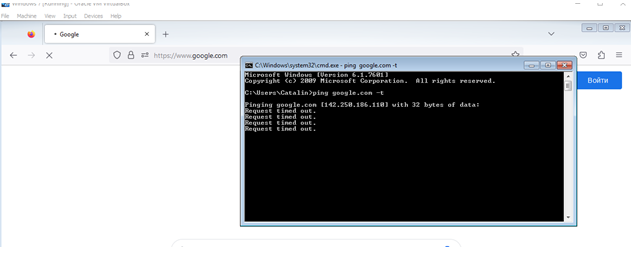


Figura 9. Atac DoS

După încetarea atacului, în figura 10 se observă că a apărut legătura și astfel victima poate folosi din nou internetul.

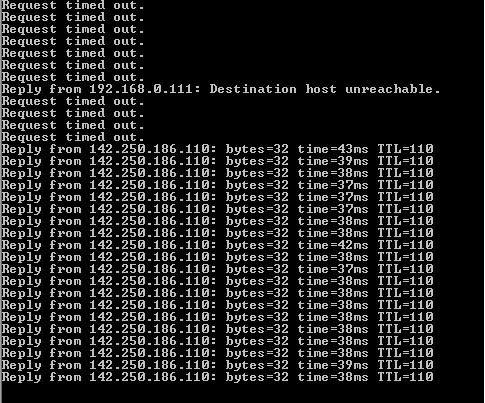


Figura 10. Încetarea atacului

**4. Atacuri de tip forța brută (Brute-Force)**

Un atac de tip forță brută este o metodă de securitate cibernetică în care un atacator încearcă să obțină acces neautorizat la un sistem sau la un cont folosind o metodă de încercare și eroare, încercând toate posibilele combinații de parole sau de alte informații de autentificare până când găsește o combinație corectă.

De exemplu, un atacator poate încerca toate combinațiile posibile de caractere pentru a ghici o parolă sau poate încerca să ghicească un cod PIN prin încercarea tuturor combinațiilor posibile de cifre. Atacurile de tip forță brută pot fi efectuate manual sau pot fi automate folosind programe special concepute, cunoscute sub numele de "crackere" sau "exploituri".

Atacurile de tip forță brută pot fi foarte eficiente împotriva parolelor slabe sau a altor forme de autentificare slabă, dar pot fi și timp consumator și pot necesita resurse semnificative pentru a fi efectuate. Pentru a preveni atacurile de tip forță brută, este important să se folosească parole și alte forme de autentificare puternice și să se implementeze măsuri de securitate suplimentare, cum ar fi blocarea temporară a conturilor după un număr specific de încercări eșuate de autentificare.

Pentru a realiza atacul de tip forță brută, am folosit hydra, care deja este implimentată în kali linux. Hydra este un cracker de conectare paralelizat care acceptă numeroase protocoale de atac. Este foarte rapid și flexibil, iar modulele noi sunt ușor de adăugat.Acest instrument face posibil ca cercetătorii și consultanții de securitate să arate cât de ușor ar fi să obții acces neautorizat la un sistem de la distanță.

Logotipul al putem observa în figura 11.



Figura 11. Hydra

Pentru a realiza sarcina, am folosit 2 mașini virtuale pe calculatoare diferite, pentru a realiza într-un mod sigur. Mai întâi am instalat pe calculatorul victimă un SSH (Secure Shell). Acesta este un protocal care permite comunicarea între două calculatoare. În figura 12 este reprezentată comanda folosită pentru a realiza acest past.

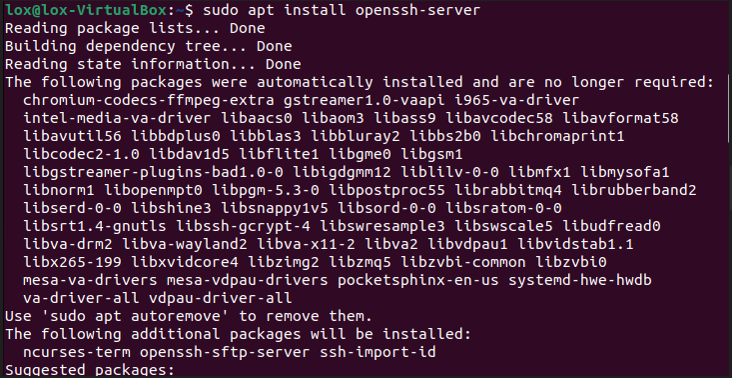


Figura 12. Creare SSH

În figura 13 se vede că serverul SSH este activ.

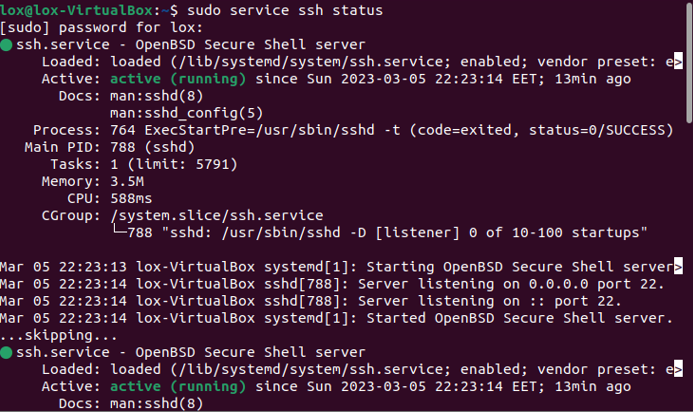


Figura 13. SSH status

În pasul următor am avut nevoie de a afla ip la victimă. Astfel am folosit comanda prezentă în figura 14.

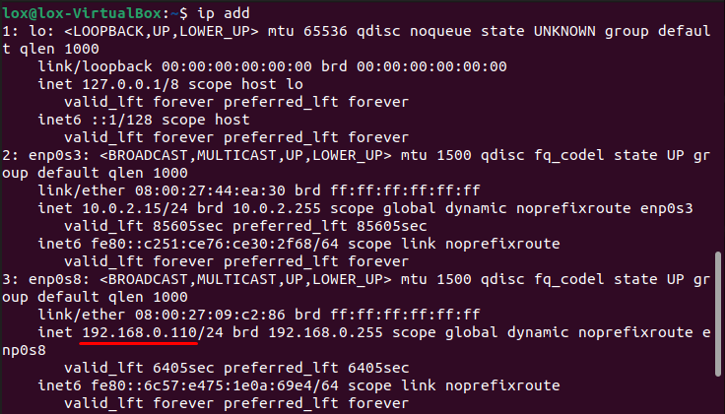


Figura 14. IP adresă

Ulterior, am trecut la calculatorul sursă și am verificat conexiunea cu victima. Folosind comanda ping, cum este ilustrat în figura 15.

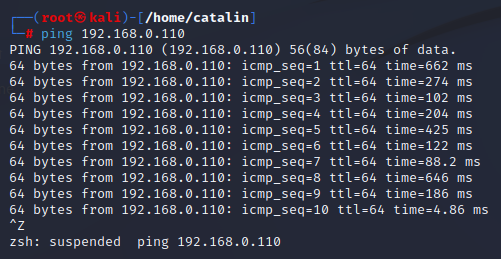


Figura 15. Verificare conexiune

Observăm că are loc schimbul de date, deci legătura dintre calculatoare există.

În pasul următor, am creat un file cu câteva parole simple, pentru a le verifica în calculatorul victimei dacă există coincidențe. Filul pass.txt este ilustrat în figura 16.

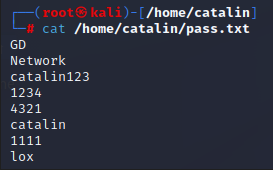


Figura 16. Creare parole

Deci, deja este totul pregătit pentru a realiza atacul. Pentru aceasta, vom folosi comanda reprezentată în figura 17.

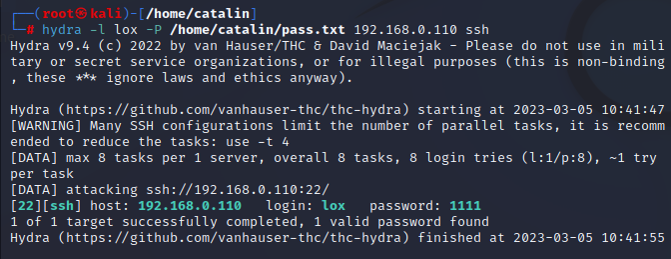


Figura 17. Creare atac

Din figura 17, observăm ca atacul a avut loc cu succes, ulterior avem și o coincidență în login și parolă. Respectiv, atacul a fost cu succes. Pentru a verifica eficiența, am schimbat parola de pe calculatorul victimă, pentru a observa dacă sunt schimbări, rezultatul este în figura 19.

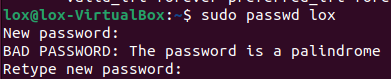


Figura 18. Schimb parolă

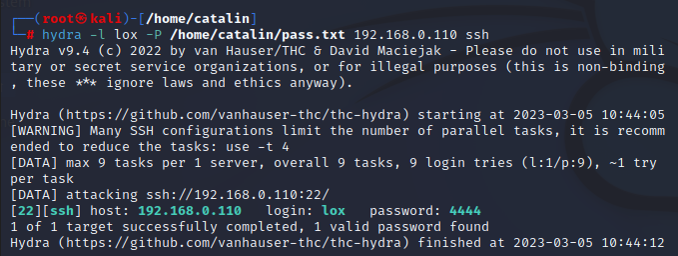


Figura 19. Schimb de parolă

Observăm că parola din 1111, a fost schimbată în 4444. Deoarece în fileul nostru create cu parole aproximative este parola respectivă, rezultă că atacul din nou a fost realizat cu succes.

Acum, vom folosi datele respective pentru a ne loga și verifica dacă sunt corecte.

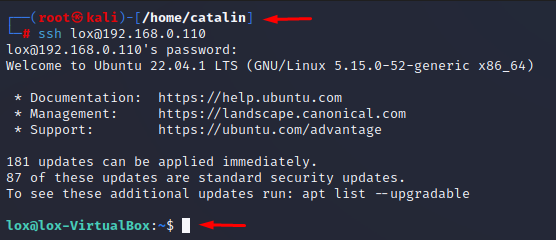


Figura 20. Logare

În figura 20, observăm că la moment, ne-am logat cu succes în calculatorul victimei. Ulterior, voi crea un file, pentru a demonstra că el va apărea la victimă în calculator, pasul respectiv este reprezentat în figura 21.

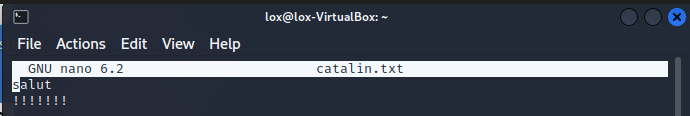


Figura 21. Creare file nou

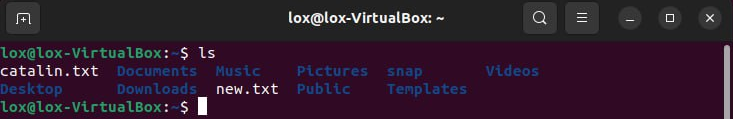
Acum voi verifica pe calculatorul victimă dacă el a fost creat.



Figura 22. File nou

Observăm în figura 22, că filul creat este prezent, respectiv totul funcționeză perfect.

Acesta a fost doar un exemplu simplu de a crea un file nou, dar dacă cineva obține controlul asupra calculatorului nostru, poate realiza fapte mult mai rele, deoarece toate datele sunt posibile de accesat pentru el.

**Concluzie**

În urma realizării lucrării de laborator respective, am studiat și realizat câteva tipuri de atacuri, cum ar fi: atacuri de tip ingineria socială, studierea atacurilor de tip man-in-the-middle, atacuri de tip DoS și atacuri de tip forță brută. A fost o sarcină destul de interesantă și a fost un proces educativ, deoarece am înțeles cât nesiguri suntem dacă, nu ne asigurăm cu sisteme de protecție și folosim parole destul de simple. Dacă utilizatorul nu se protejează corespunzător, atunci el foarte ușor poate fi atacat iar datele lui vor fi folosite de atacator. Trebuie să ne asigurăm cât mai bine pentru siguranța noastră și a datelor noastre. De asemenea, este important să nu comunicăm nimănui datele noastre, cum ar fi IP sau parole, deoarece având acest parametru, atacatorul ne poate realiza un atac foarte rapid.

**Bibliografie**

1. DoS Attack - <https://medium.com/geekculture/simple-but-powerful-denial-of-service-dos-attack-8c7dfd60045f> [Sursă electronică]

2. Brute Force Attack - <https://gtrekter.medium.com/brute-force-attack-with-hydra-and-kali-linux-3c4ede55d119> [Sursă electronică]

3. Brute Force Attack - <https://www.youtube.com/watch?v=0Ld4_C-jBDM> [Sursă video]