**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.2

*la Tehnologii a Securitatii Informationale*

A efectuat:

st. gr. TI-216 Rosca Dorin

A verificat: Zalesciuc Maxim

Chişinău – 2023

**Lucrare de laborator nr. 2**

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

**Scopul lucrării:** Analiza a mai multor Tipuri de atacuri în SI. Analiza tehnicilor de inginerie socială. Capturarea și analiza traficului. Simularea atacurilor DoS.

1. **Atacuri de tip Ingineria Socială**

**Exemple de atacuri de inginerie sociala:**

* **Phishing: Această metodă este una dintre cele mai utilizate și constă în trimiterea unui e-mail sau a unui mesaj text care pare a fi de la o sursă de încredere, cum ar fi o bancă sau un serviciu de e-mail. Mesajul va conține, de obicei, un link către un site fals, care imită site-ul original și solicita utilizatorului să-și introducă informațiile personale, cum ar fi numele de utilizator și parola. Aceste informații sunt apoi folosite de către atacatori pentru a accesa conturile victimelor.**
* **Vishing: Această tehnică implică folosirea telefonului pentru a suna victimele și a le solicita să dezvăluie informații confidențiale, cum ar fi numerele de carduri bancare sau parolele de la conturile online. Atacatorii se fac adesea drept angajați ai unei bănci sau ai unui serviciu de asistență pentru clienți și încearcă să-i convingă pe utilizatori să furnizeze informațiile solicitate.**
* **Social engineering prin intermediul rețelelor sociale: Atacatorii folosesc adesea rețelele sociale, cum ar fi Facebook, Instagram sau LinkedIn, pentru a se conecta cu oamenii și a le solicita să le furnizeze informații confidențiale sau să descarce software malware. Atacatorii pot folosi informațiile obținute în acest fel pentru a accesa conturile victimelor sau pentru a efectua alte activități ilegale.**
* **Watering hole attacks: Această metodă implică infectarea site-urilor web legitime cu malware și apoi așteptarea ca utilizatorii să viziteze aceste site-uri pentru a obține acces la sistemele lor. Atacatorii aleg site-uri web populare și le infectează cu software malware care poate fi utilizat pentru a accesa sistemul utilizatorilor.**
* **Atacuri prin intermediul e-mail-urilor de tip CEO Fraud: Acestea implică falsificarea adresei de e-mail a unui CEO sau a unui director și trimiterea unui mesaj fals angajaților companiei. În mesaj se solicită de obicei efectuarea unei transferuri de bani într-un cont specific, care aparține atacatorilor. Angajații care cad în această capcană transferă banii în contul specificat de către atacatori.**

Studierea metodelor și tehnicilor atacurilor de tip phishing:

Studiul metodelor și tehnicilor de phishing este important pentru a înțelege cum aceste atacuri sunt proiectate și efectuate, pentru a putea lua măsurile de protecție necesare și a evita căderea în capcana atacatorilor. Iată câteva dintre cele mai comune metode și tehnici utilizate în atacurile de phishing:

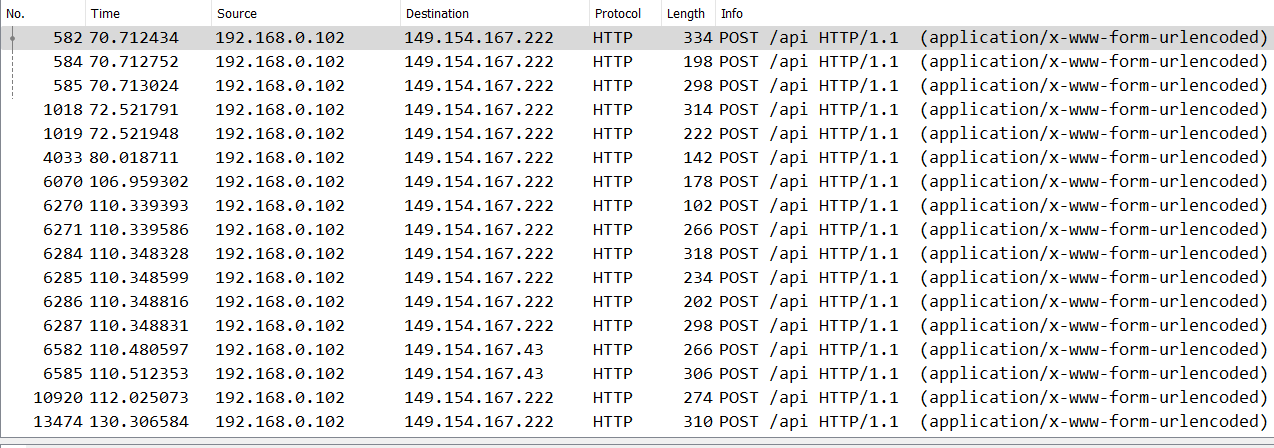
* Spoofing: Această metodă implică falsificarea adresei de e-mail sau numărului de telefon pentru a crea impresia că mesajul provine de la o sursă de încredere. Atacatorii pot, de asemenea, să creeze site-uri web sau pagini de autentificare false pentru a face ca site-ul să pară autentic.
* Spear phishing: Acest tip de phishing este personalizat și se adresează unui grup restrâns de persoane, cum ar fi angajații unei companii. Atacatorii vor cerceta în prealabil compania și vor obține informații despre angajați, astfel încât să poată crea mesaje credibile și personalizate.
* Pharming: Această metodă implică redirecționarea utilizatorilor către un site web fals sau infectat, chiar dacă utilizatorul introduce adresa corectă a site-ului în browser. Acest lucru se face prin modificarea setărilor DNS sau prin utilizarea de programe malware.
* Whale phishing: Această metodă se concentrează asupra directorilor sau altor persoane importante în cadrul unei companii. Atacatorii vor utiliza tehnici personalizate și sofisticate pentru a obține informații confidențiale sau pentru a efectua transferuri de bani.
* Angler phishing: Această metodă implică utilizarea unui eveniment de actualitate sau a unei știri importante pentru a atrage utilizatorii să acceseze un site web sau un link malicios. De exemplu, atacatorii pot trimite un e-mail sau un mesaj text care pare a fi despre o actualitate importantă și care conține un link către un site web fals.

Stabilirea recomandărilor și metodelor de protecție:

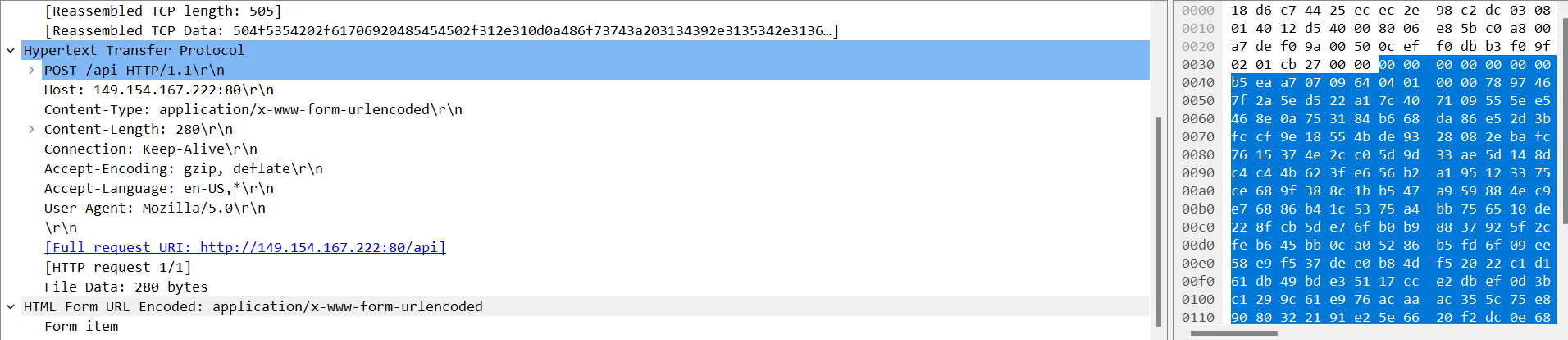
* Fiți atenți la mesajele primite prin e-mail sau mesaje text: Înainte de a face clic pe un link sau de a descărca un fișier, verificați cu atenție adresa de e-mail a expeditorului sau numărul de telefon și verificați dacă mesajul pare autentic.
* Nu dezvăluiți niciodată informații personale sau financiare sensibile: Niciodată nu ar trebui să furnizați informații precum numele de utilizator și parola, datele cardului de credit sau alte informații personale prin e-mail, mesaj text sau altfel.
* Folosiți software antivirus actualizat: Instalarea unui software antivirus actualizat pe dispozitivul dvs. poate ajuta la prevenirea atacurilor malware.
* Folosiți parole puternice și diferite pentru fiecare cont online: Folosirea unor parole puternice și diferite pentru fiecare cont online poate ajuta la prevenirea accesului neautorizat la conturile dvs. în cazul în care una dintre parole este compromisă.
* Utilizați autentificarea cu factori multipli: Autentificarea cu factori multipli (de exemplu, utilizarea unei parole și a unui cod trimis prin SMS sau o aplicație de autentificare) poate ajuta la prevenirea accesului neautorizat la conturile dvs.
* Verificați adresa site-ului web: Înainte de a introduce informații personale sau financiare pe un site web, verificați adresa site-ului și asigurați-vă că acesta este autentic.
* Fiți atenți la site-urile web false: Unele site-uri web false pot părea la fel ca cele reale. Verificați adresa site-ului și verificați dacă site-ul este autentic înainte de a introduce informații personale sau financiare.
* Actualizați software-ul și sistemul de operare: Actualizarea regulată a software-ului și a sistemului de operare pe dispozitivul dvs. poate ajuta la prevenirea vulnerabilităților de securitate.
* Educați-vă și sensibilizați alții: Învățarea metodelor și tehnicilor de phishing și informarea altora despre acestea poate ajuta la prevenirea atacurilor.

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

**Pentru a intercepta traficul din retea a fost folosita aplicatia WireShark.Din motiv ca o mare parte din pachete incerceptate erau codificate,doar o mica parte de pachete ce folosesc protocolul HTTP pot fi studiate:**

****

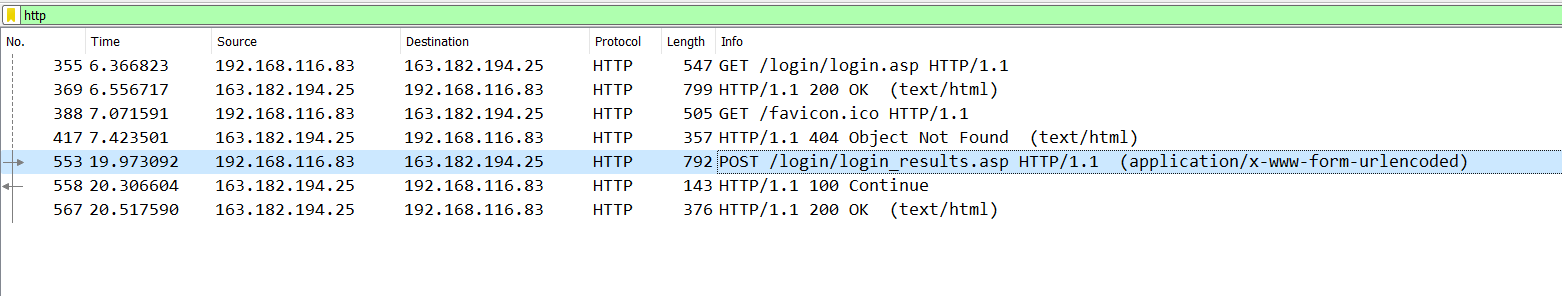
**Figura 1. Pachetele interceptate in aplicatia WireShark**

****

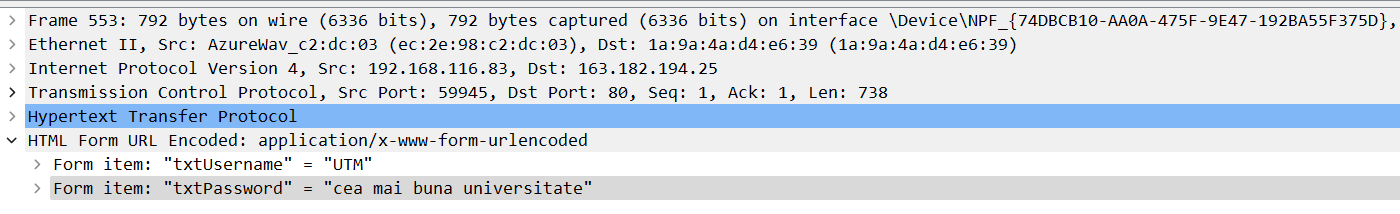
**Figura 2.Detaliile Pachetului Interceptat**

1. **Adresa MAC al calculatorului de pe care lucrez se numeste:0A-00-27-00-00-04**
2. **Numele producatorului placii de retea este:** **AzureWave Technology Inc.**
3. **Adresa IP a calculatoruui de pe care lucre este:** **192.168.56.1**
4. **Adresa MAC sursa pentru pachetele raspuns HTTP este:ec:2e:98:c2:dc:03**
5. **Adresa IP sursa pentru pachetele raspuns HTTP este:192.168.0.102**
6. **Adresele IP nu permit o diferențiere clară între o cerere HTTP și un răspuns HTTP în Wireshark.**

**Aceasta se datorează faptului că pachetele de cerere HTTP și de răspuns HTTP au aceeași adresă IP sursă și destinație, dar se disting între ele prin numerele de port utilizate. Mai exact, atunci când un client trimite o cerere HTTP către un server, aceasta va avea o adresă IP sursă care corespunde cu adresa IP a clientului și o adresă IP destinație care corespunde cu adresa IP a serverului, împreună cu un număr de port sursă care reprezintă portul utilizat de către client pentru a trimite cererea HTTP (de exemplu, portul 80 pentru conexiunile HTTP obișnuite). La rândul său, atunci când serverul trimite răspunsul HTTP înapoi către client, acesta va avea o adresă IP sursă care corespunde cu adresa IP a serverului și o adresă IP destinație care corespunde cu adresa IP a clientului, împreună cu un număr de port destinație care reprezintă portul utilizat de către client pentru a primi răspunsul HTTP (de exemplu, același port 80 pentru conexiunile HTTP obișnuite).**

1. **Pachetele capturate:** ****

**Informatiile de logare:**

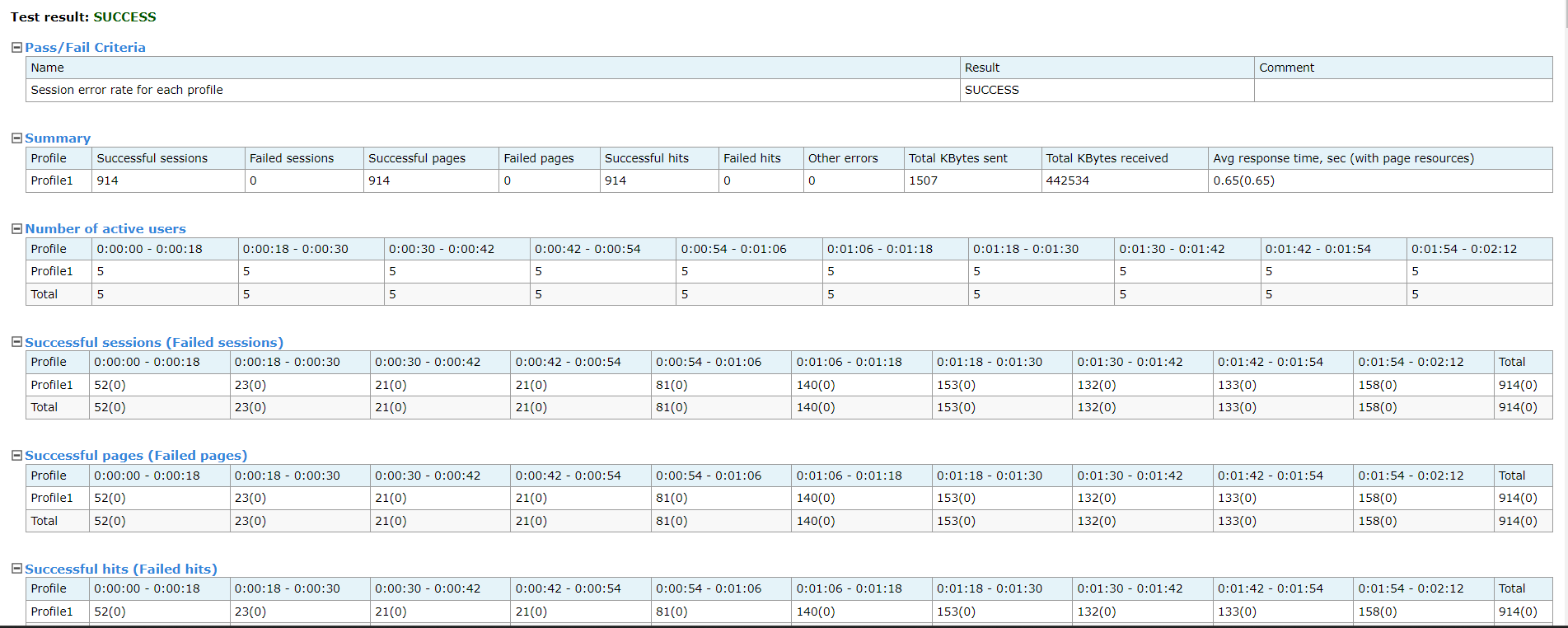
****

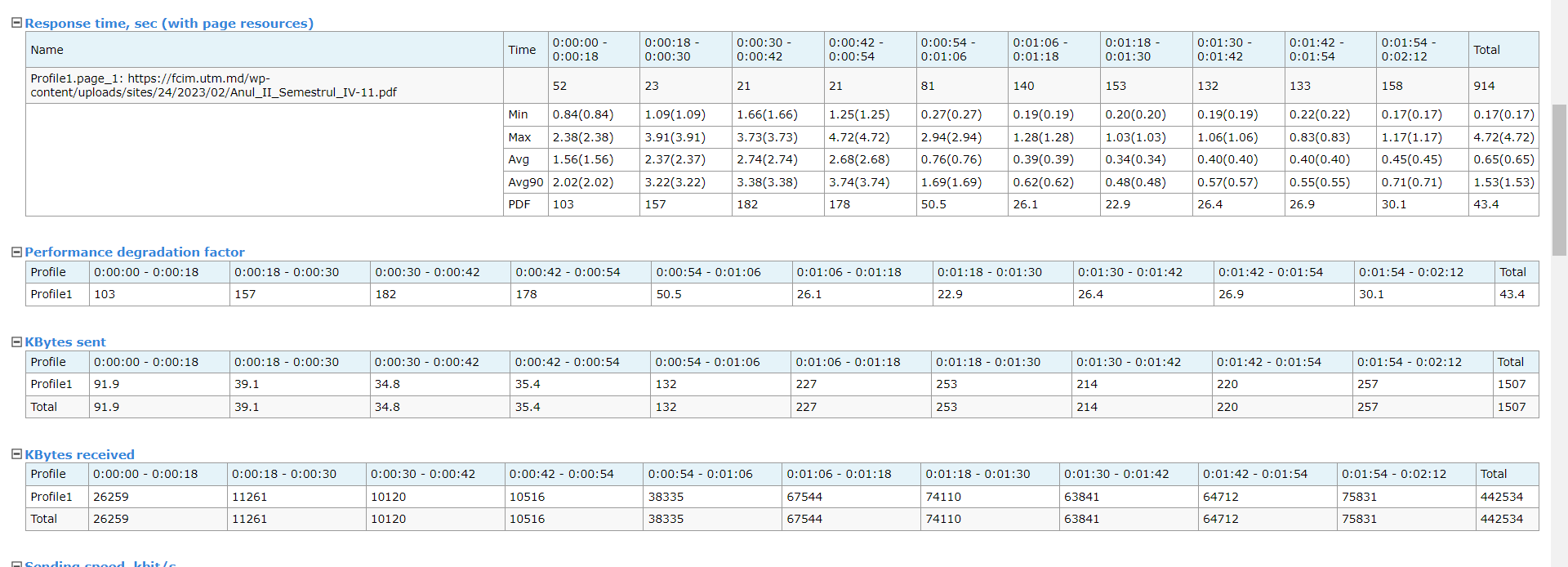
1. **Protocolul ARP (Address Resolution Protocol) este utilizat în rețelele de calculatoare pentru a găsi adresa fizică (MAC) a unui dispozitiv din rețea cunoscută deja adresa sa IP. Atunci când un dispozitiv din rețea dorește să transmită un pachet către alt dispozitiv, acesta va utiliza adresa IP a destinatarului pentru a transmite pachetul. Însă, adresa IP nu este suficientă pentru a livra pachetul la destinatar, deoarece dispozitivul trebuie să știe adresa fizică (MAC) a destinatarului pentru a transmite pachetul prin intermediul rețelei. Pentru a găsi adresa MAC a destinatarului, dispozitivul care dorește să transmită pachetul va trimite un pachet ARP către toate dispozitivele din rețea, inclusiv către destinatar. Pachetul ARP conține adresa IP a destinatarului și solicită dispozitivele din rețea să trimită înapoi adresa lor MAC dacă aceasta corespunde cu adresa IP solicitată. Când dispozitivul destinatar primește pachetul ARP, acesta va răspunde cu un pachet ARP care conține adresa sa MAC. Dispozitivul care a inițiat cererea ARP va primi răspunsul ARP și va utiliza adresa MAC primită pentru a transmite pachetul la destinatar. Informațiile obținute prin intermediul protocolului ARP sunt stocate într-un cache ARP pe fiecare dispozitiv din rețea.**
2. **Atacuri de tip DoS (Denial of Service)/DDoS (Distributed Denial of Service)**

Pentru a simula atac de tip Ddos,a fost ulilizata aplicatia WAPT PRO

Rezultatele simularii atacului:

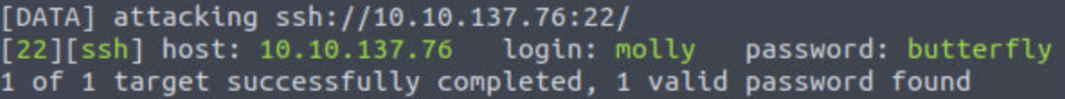






1. Atacuri de tip forta Bruta

Pentru a efectua atacul de tip forta bruta a fost folosita aplicatia Hydra



1. **Concluzie:**

În urma lucrării de laborator desfășurate, am putut înțelege importanța cunoașterii tipurilor de atacuri în sistemele informatice și a tehnicilor de inginerie socială, pentru a putea identifica și preveni astfel de atacuri. Am analizat diverse exemple de atacuri, cum ar fi phishing-ul, vishing-ul, social engineering-ul prin intermediul rețelelor sociale și CEO Fraud. De asemenea, am învățat despre metodele și tehnicile utilizate în atacurile de phishing, cum ar fi spoofing-ul, spear phishing-ul și pharming-ul. O altă parte importantă a lucrării a fost analiza traficului și simularea atacurilor DoS, care ne-au ajutat să înțelegem modul în care se pot bloca sau perturba sistemele informatice prin suprasolicitarea resurselor acestora. Am învățat că este important să se ia măsuri de protecție, cum ar fi utilizarea de firewall-uri, actualizarea software-ului și monitorizarea traficului, pentru a preveni astfel de atacuri. În concluzie, cunoașterea și înțelegerea tipurilor de atacuri în sistemele informatice și a tehnicilor de inginerie socială, precum și luarea măsurilor de protecție adecvate, sunt esențiale pentru asigurarea securității și protejarea datelor personale și a informațiilor confidențiale