Ministerul Educaţiei, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Departamentul Ingineria Software și Automatică

**Disciplina: Tehnologii ale securității informaționale**

**RAPORT**

**Lucrarea de laborator nr. 2**

A elaborat:

st. gr. TI-216  **Vlașițchi Ștefan**

A verificat: **Zalesciuc Maxim**

asit.univer,

Chişinău – 2023

Contents

[**Consideratii teoretice:** 3](#_Toc129198081)

[**1.** **Atacuri de tip Ingineria Socială** 3](#_Toc129198082)

[**2.** **Studierea atacurilor de tip man-in-the-middle** 5](#_Toc129198083)

[**3.** **Atacuri de tip DoS (Denial of Service)/DDoS (Distributed Denial of Service)** 7](#_Toc129198084)

[**4.** **Atacuri de tip forța brută (Brute-Force)** 9](#_Toc129198085)

[**Concluzie:** 11](#_Toc129198086)

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

# **Consideratii teoretice:**

1. **Atacuri de tip Ingineria Socială**

Ingineria socială este o tehnică folosită de infractori cibernetici pentru a păcăli oamenii să dezvăluie informații personale și confidentiale, pentru a instala software malware pe computere sau pentru a accesa rețele de calculatoare. Iată câteva exemple de atacuri de tip inginerie socială:

1. Phishing - infractorii cibernetici trimit email-uri sau mesaje text false, care pretind că sunt de la o organizație legitimă (cum ar fi o bancă sau un furnizor de servicii) și îi încurajează pe oameni să ofere informații personale sau să facă clic pe link-uri care conduc la site-uri false, care pot instala malware sau pot fura date.
2. Vishing - infractorii cibernetici fac apeluri telefonice false, pretinzând că sunt de la o organizație legitimă și îi conving pe oameni să ofere informații personale sau să facă transferuri de bani.
3. Pretexting - infractorii cibernetici se fac trecuți drept o altă persoană sau organizație și încearcă să obțină informații confidențiale de la oameni prin intermediul unei conversații false.
4. Baiting - infractorii cibernetici lasă dispozitive de stocare USB infectate cu malware în locuri publice, precum parcuri sau mall-uri, și așteaptă ca cineva să le găsească și să le conecteze la un computer, infectând astfel acel computer cu malware.
5. Tailgating - infractorii cibernetici urmăresc pe cineva într-o zonă securizată, cum ar fi o companie sau un aeroport, și se fac trecuți drept angajați sau vizitatori legitimi pentru a obține acces la zonele restricționate.

Acestea sunt doar câteva exemple de atacuri de tip inginerie socială. Este important să fim atenți și să avem grijă de informațiile pe care le oferim și să nu cădem în capcana infractorilor cibernetici.

Phishing-ul este o formă de atac de inginerie socială în care infractorii cibernetici trimit e-mail-uri sau mesaje text false, care pretind că sunt de la o organizație legitima, cu scopul de a păcăli oamenii să ofere informații personale și confidentiale, cum ar fi parole, numere de carduri de credit sau informații financiare.

Iată câteva metode și tehnici comune folosite în atacurile de tip phishing:

1. Spoofing - infractorii cibernetici pretind că sunt o organizație legitima prin utilizarea unei adrese de e-mail sau număr de telefon fals. De exemplu, un e-mail fals poate pretinde că este de la o bancă sau o companie cunoscută, dar adresa de e-mail a expeditorului poate fi una diferită.
2. Urgența - phishing-ul poate utiliza tacticile de urgenta sau presiune pentru a păcăli oamenii să ia o acțiune rapidă. Mesajele pot afișa un mesaj urgent care solicită un răspuns rapid, cum ar fi "contul dvs. este blocat" sau "activitatea suspectă a fost detectată".
3. Site-uri false - infractorii cibernetici creează site-uri web false, care imită aspectul și funcționalitatea unui site web legitim, cum ar fi cel al unei bănci sau a unui magazin online, pentru a obține informații de autentificare sau pentru a induce utilizatorii să introducă informații financiare.
4. Atacul "Spear Phishing" - este o tehnică de phishing care se concentrează pe un grup specific de utilizatori sau indivizi. În această metodă, atacatorii cibernetici obțin informații personale despre un grup de utilizatori și le trimit un e-mail sau o mesaj text personalizat, care pare că vine de la o persoană sau o organizație cunoscută.
5. Camuflarea link-urilor - în mesajele de phishing, link-urile pot fi camuflate astfel încât să pară că conduc la un site web legitim, dar de fapt, acestea pot duce la un site web fals, care poate instala malware sau poate fura informații personale.
6. Social Engineering - infractorii cibernetici pot folosi tehnici de manipulare sociala, cum ar fi flatarea, intimidarea sau amenințarea, pentru a obține informații personale sau pentru a determina oamenii să ia o anumită acțiune.

Este important să fim vigilenți și să verificăm întotdeauna autenticitatea unui e-mail sau a unui mesaj înainte de a oferi informații personale sau financiare. Verificarea adresei de e-mail sau a site-ului web, evitarea introducerii de informații personale sau financiare prin link-uri și încetarea imediată a oricărei acțiuni suspecte pot ajuta la prevenirea atacurilor de tip phishing

Protecția împotriva atacurilor de tip inginerie socială implică atât măsuri tehnice, cât și măsuri comportamentale. Mai jos sunt câteva recomandări și metode de protecție:

1. Educația și conștientizarea: Este important să fii conștient de tipurile de atacuri de inginerie socială și să înțelegi modul în care acestea pot fi utilizate pentru a te manipula și a obține informații confidențiale. De asemenea, este important să te educați în legătură cu metodele de protecție.
2. Verificarea identității: Înainte de a dezvălui informații confidențiale sau de a executa acțiuni solicitate, asigură-te că verifici identitatea persoanei sau entității care te contactează.
3. Utilizarea unui software de securitate: Folosește un software de securitate puternic pentru a bloca și a detecta amenințările de securitate, cum ar fi spam-ul, phishing-ul sau alte atacuri de inginerie socială.
4. Implementarea politicii de securitate: Instituie politici clare de securitate pentru compania ta, care să acopere procedurile și regulile pentru protecția informațiilor confidențiale și pentru identificarea și raportarea incidentelor de securitate.
5. Folosirea parolelor puternice: Utilizează parole puternice pentru toate conturile și evită folosirea acelorași parole pentru mai multe conturi. Schimbă parolele cu regularitate și nu le dezvălui niciodată cuiva.
6. Folosirea autentificării cu doi factori: Folosește autentificarea cu doi factori (2FA) ori de câte ori este posibil. Aceasta implică furnizarea unei parole și a unei informații suplimentare, cum ar fi un cod de securitate trimis prin SMS sau o amprentă digitală.
7. Verificarea și actualizarea sistemelor de securitate: Asigură-te că toate sistemele de securitate sunt actualizate și verificate cu regularitate pentru a detecta și a bloca amenințările de securitate.

În general, protecția împotriva atacurilor de inginerie socială implică atât măsuri tehnice, cât și măsuri comportamentale. Este important să înțelegi riscurile și să iei măsuri adecvate pentru a reduce expunerea la aceste riscuri.

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

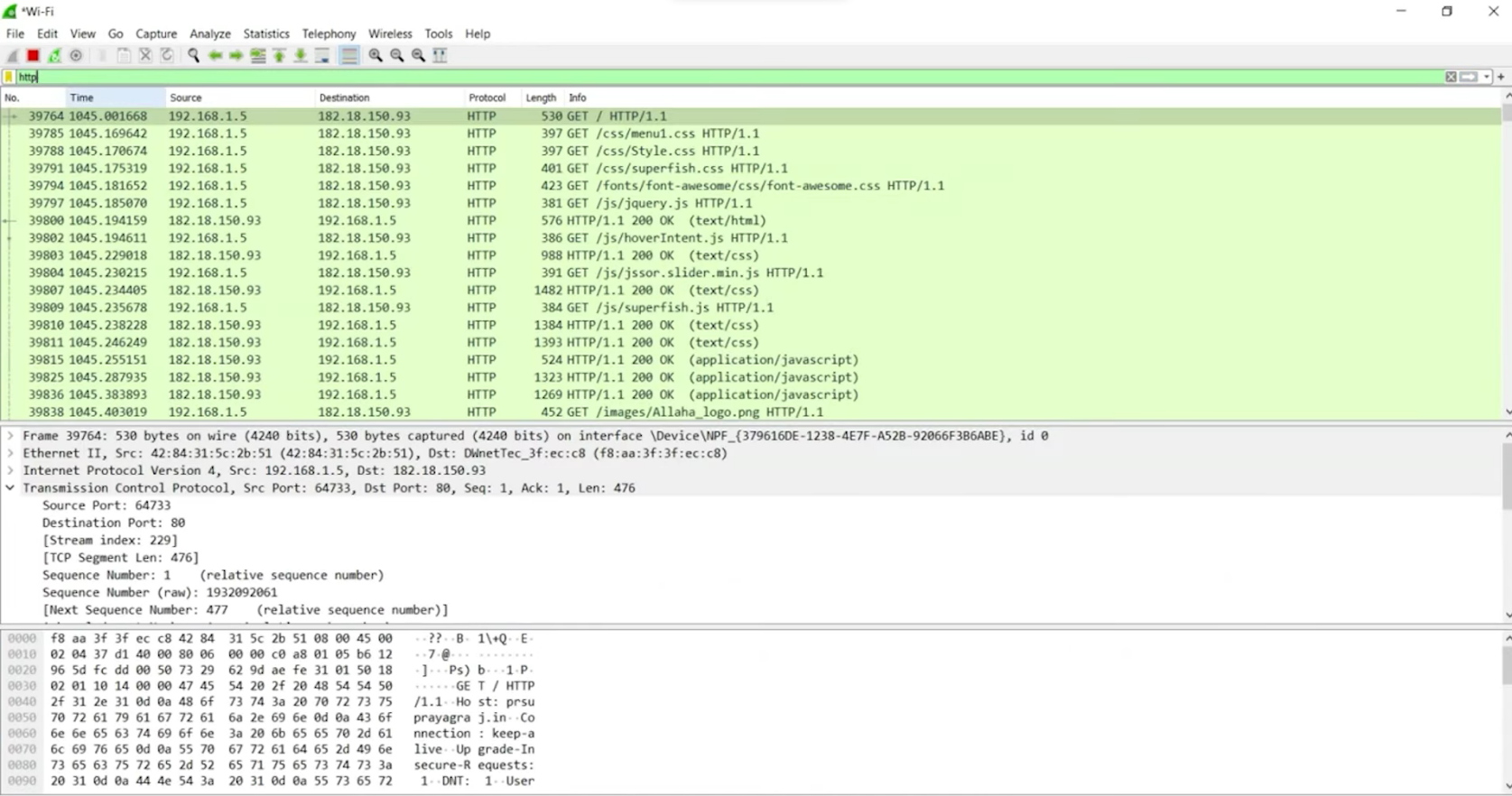


Fig 1. Exemplu de trafic in retea

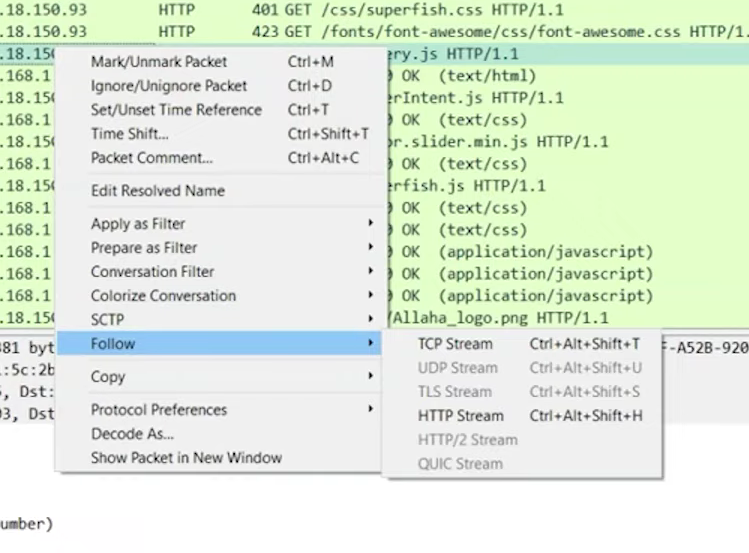


Fig 2. Metoda de a verifica datele despre un web accesat

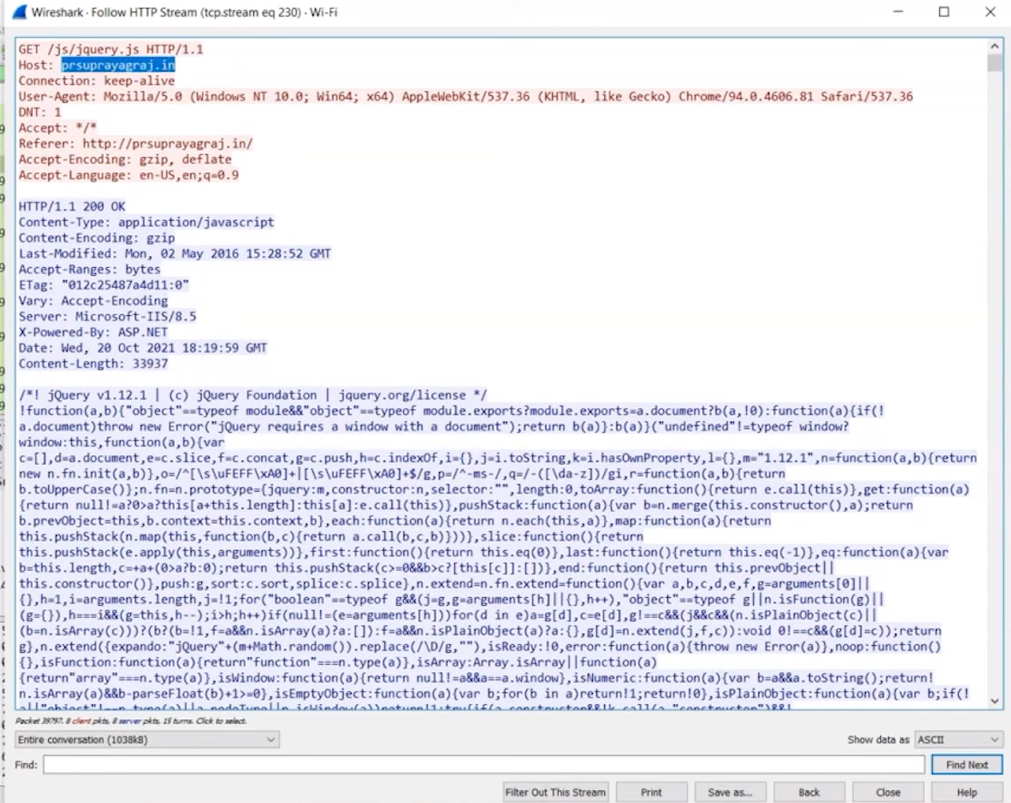


Fig 3. Informatia obtinuta despre web-ul accesat

In final cu ajutorul aplicatiiilor precum Whireshark a fost posibila verificarea traficului de internet local in urma caruia sa putut verificawebsiturile accesate dar si informatia transmisa catre acest site insa fiind protejat acesat a ramas securizata.

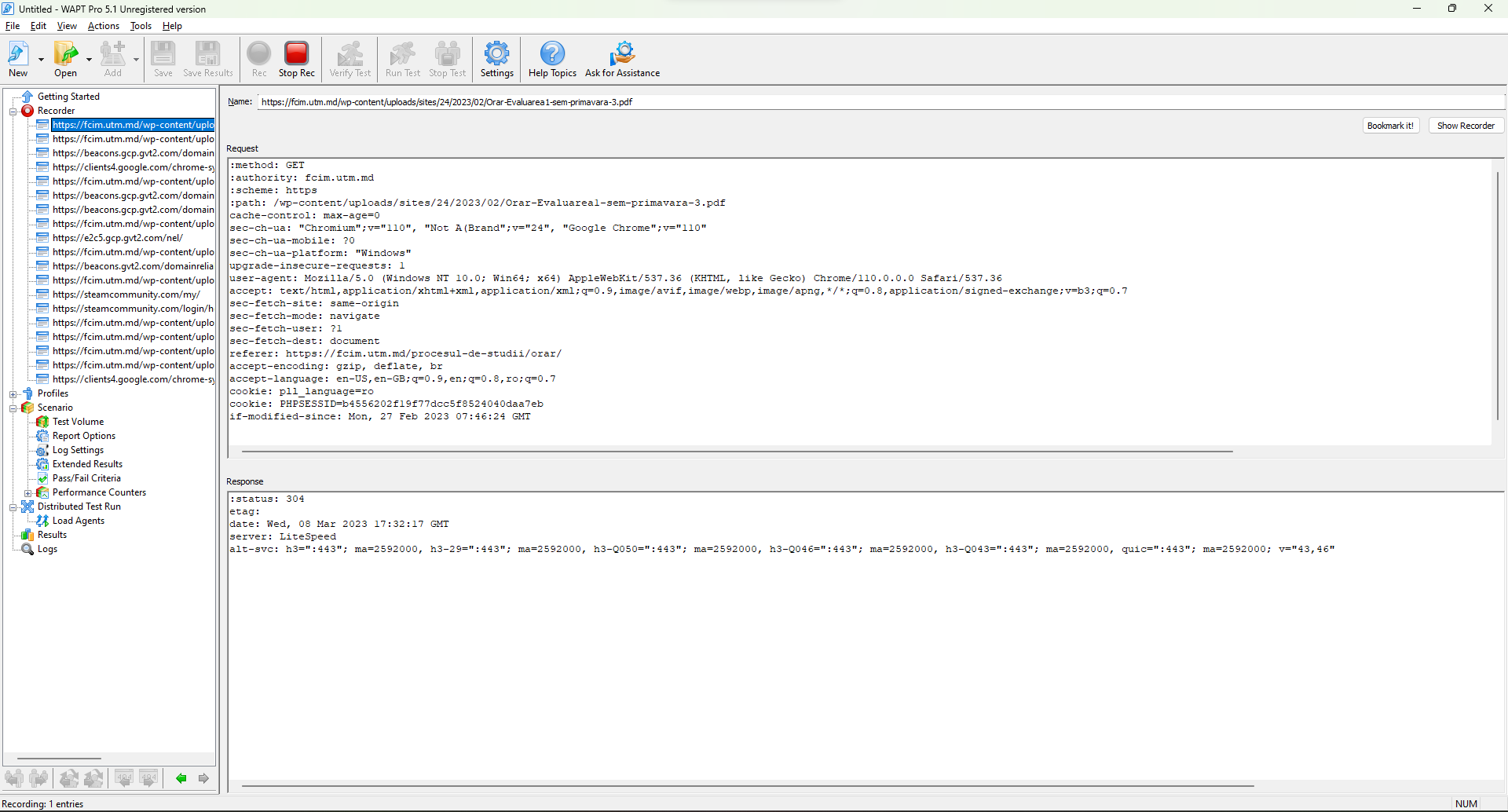
1. **Atacuri de tip DoS (Denial of Service)/DDoS (Distributed Denial of Service)**

Fig 4. Simulatrea unui tip de atac DoS

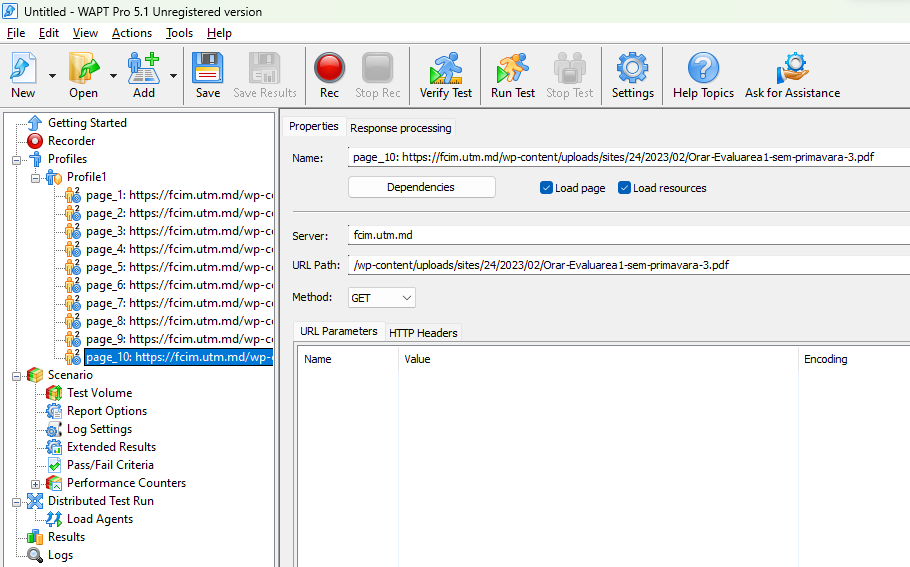
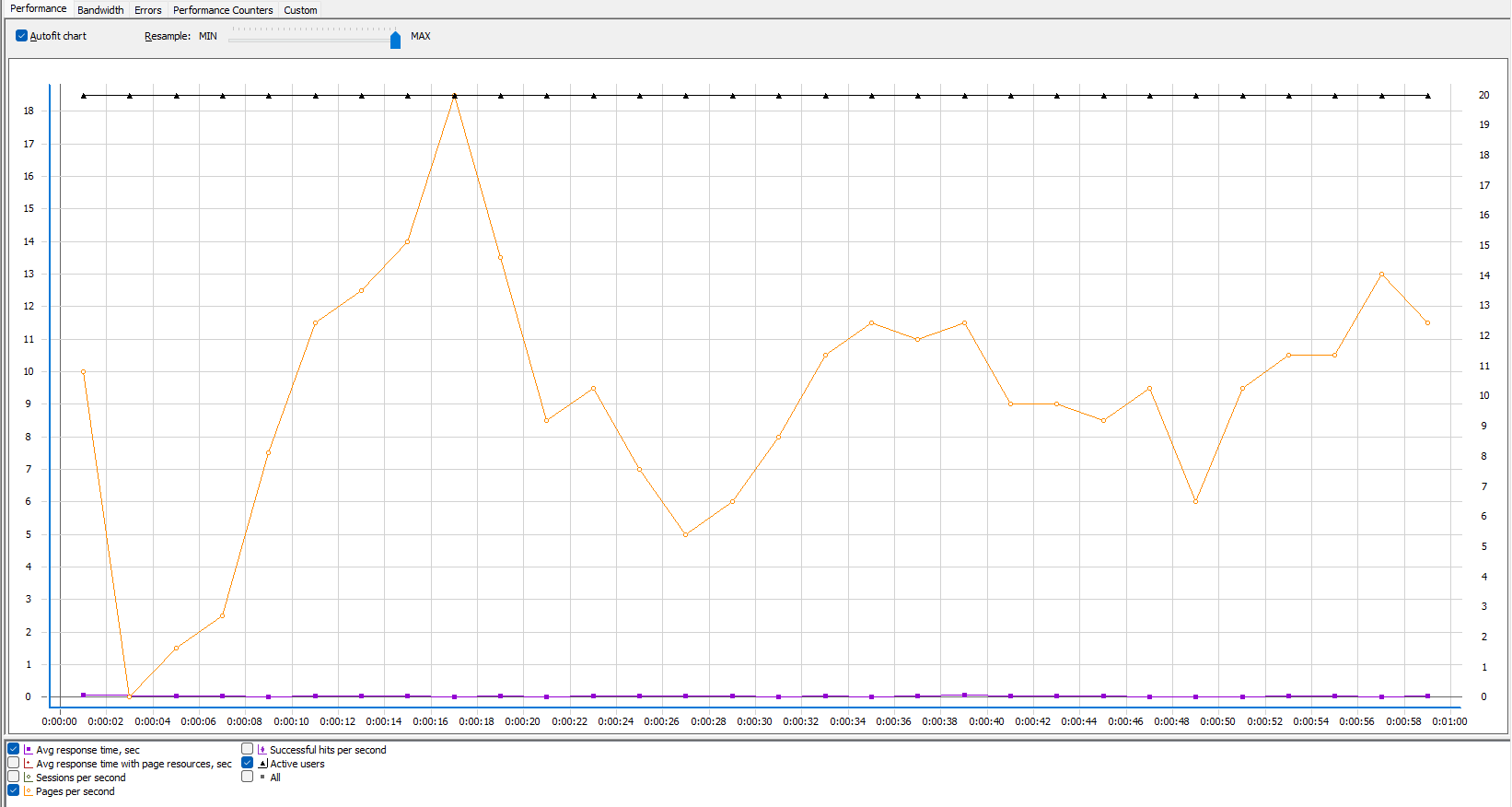
****

Fig 5. Selectarea websitului propus pentru atac.

****

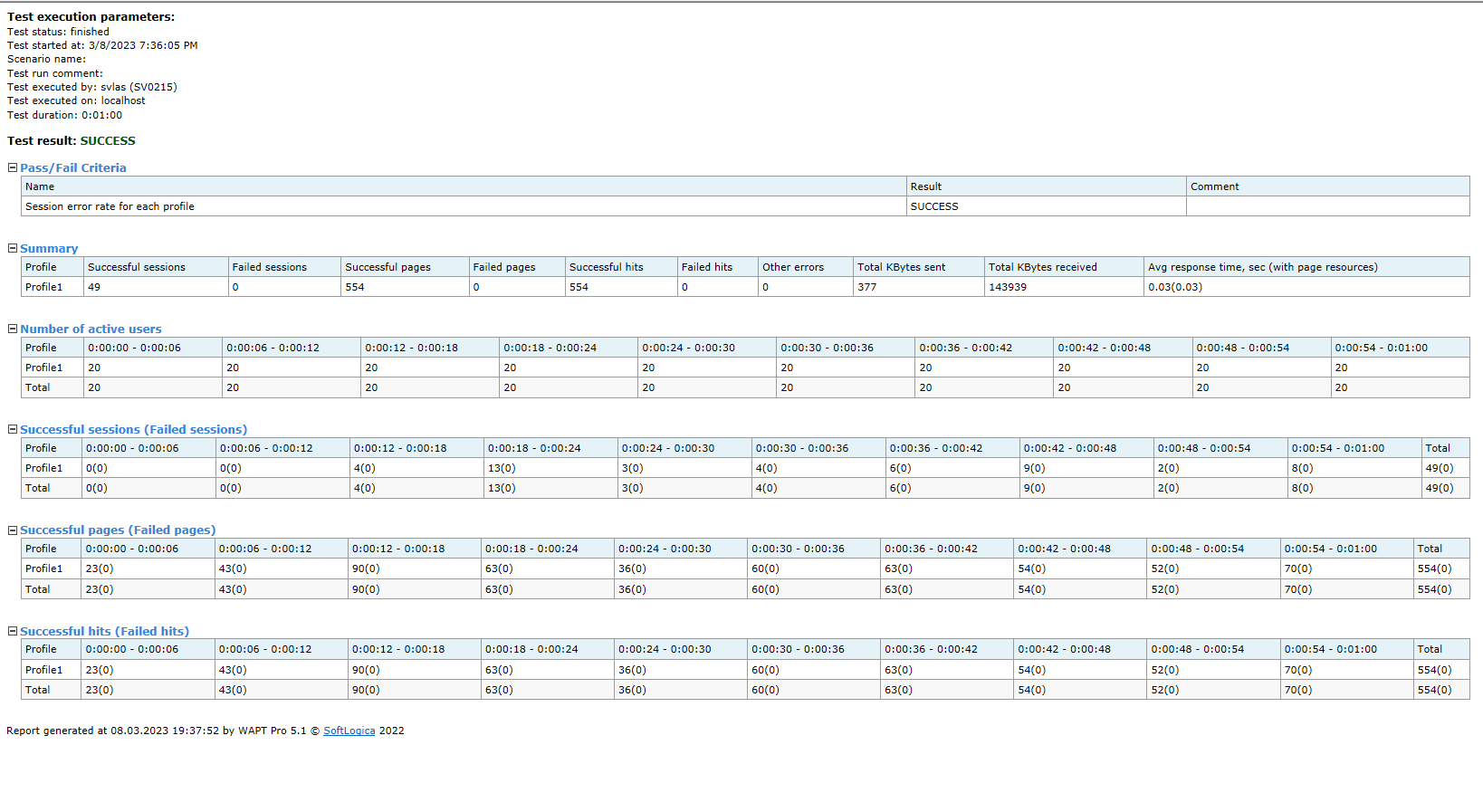
****Fig 6.1. Verificarea rezultatelor obtinut

Fig 6.2. Verificarea rezultatelor obtinute

Scopul atacului nu a fost atins fiind prea putine dispositive care au atacat de acea operativitatea websitului nu a fost influentata

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

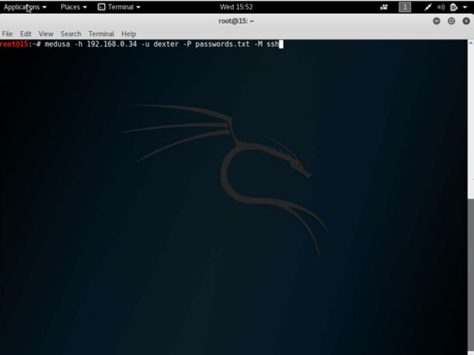
****

Fig 7. Exemplu de atac asupra unui dispozitiv

****

Fig 8. Dispozitivul urmarit

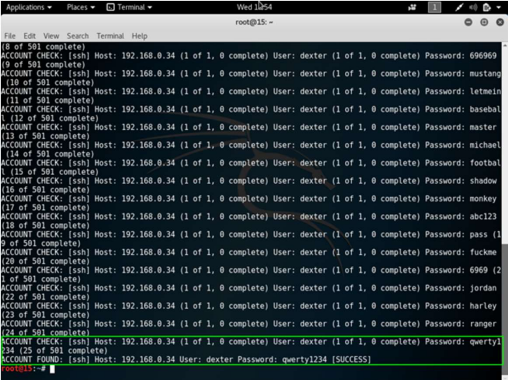


Fig 9. Procesul de apargere al parolei

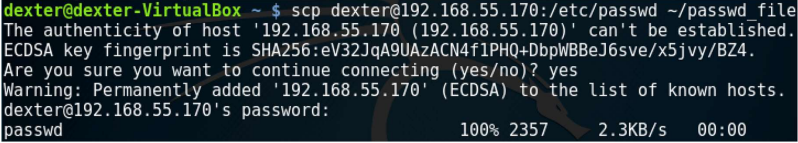
****

Fig 10. Rezultatul obtinut

In exemplu anterior s-a facut un atac de tip brut-force asupra unui alt dispozitiv pentru aceasta sa folosit o aplicatie externa si cu ajutorul adresei IP si un sir de comenzi sa reusit intro perioada de timp de a divulga parola dispozitivului aceste tipuri de atacuri pot fi utilizate si pentru alte tipuri deparole precum cele de pe situri web , internet si altele.

# **Concluzie:**

În concluzie, pot afirma că am atins cu succes scopul propus de a studia tipurile de atacuri în securitatea informațională, analizând tehnicile de inginerie socială, capturând și analizând traficul. Aceste activități au fost efectuate în scopul de a învăța și de a ne informa cu privire la metodele de combatere a acestor atacuri și de a le utiliza în mod responsabil, fără a încălca informația privată a unei persoane. În final, am învățat cum să ne apărăm și să evităm să devenim victime ale unuia dintre tipurile de atacuri studiate. Această experiență ne va fi cu siguranță utilă în cariera noastră de ingineri în tehnologii informaționale și în protejarea informațiilor sensibile ale clienților noștri.