**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.2

*la Tehnologii de Securitatea Informațională*

A efectuat:

st. gr. TI-214 Buza Cătălin

A verificat: Bulai Rodica

Chişinău - 2023

**Scopul lucrării:**

* 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
* Simularea unui atac de tip DoS
* 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

**Ingineria socială**

Fraudele bazate pe inginerie socială se construiesc în jurul modului în care oamenii gândesc și se comportă. Prin urmare, atacurile de inginerie socială sunt o modalitate eficientă de manipulare a comportamentului utilizatorului. Odată ce atacatorul înțelege motivația utilizatorului, îl poate înșela și manipula în mod eficient. Prin urmare, de exemplu, este mult mai ușor de convins o persoană pentru a-și comunica parola decât de a încerca spargerea parolei (cu excepția cazului în care parola este foarte slabă).

## Ingineria ****socială**** ****și**** etapele ****unui atac****

Atacurile de inginerie socială se desfășoară de obicei în una sau mai multe etape. Sunt urmați, în general, pașii de mai jos:

1. **Pregătirea terenului pentru atac**

* identificarea victimei (sau a victimelor)
* obținerea de informații generale
* decizia asupra metodei (metodelor) de atac care trebuie utilizate

2. **Înșelarea victimei**

atragerea obiectivului

* Inventarea unei povești
* preluarea controlului asupra interacțiunii

3. **Obținerea accesului la informații pe parcursul unei perioade de timp**

* extinderea poziției ocupate
* realizarea atacului
* distrugerea afacerii sau/și furtul de date

4. **Încheierea interacțiunii fără a trezi suspiciuni**

* eliminarea tuturor urmelor de malware
* acoperirea urmelor
* încheierea naturală a atacului

Acest proces poate avea loc într-un singur e-mail sau pe parcursul mai multor luni, după mai multe discuții în social media. Sau, așa cum am spus, se poate întâmpla chiar și în interacțiunea față în față. În cele din urmă, se încheie cu o acțiune pe care o realizați, cum ar fi furnizarea de informații personale sau expunerea la programe malware.

**Tipuri de atacuri de inginerie socială**

**1. Atacuri de tip phishing**

Atacatorii de phishing pretind că sunt o companie sau o persoană legitimă, de încredere, care încearcă să vă convingă să comunicați date personale și alte date de valoare.

Se poate întâmpla într-unul sau două moduri, respectiv spam phishing (atac generalizat care vizează mulți utilizatori) și spear-phishing (prin extensie whaling, care utilizează informații personalizate pentru a viza anumiți utilizatori, cum ar fi celebrități, persoane cu funcții de conducere și înalți funcționari guvernamentali).

**2. Atacuri „cu momeală”**

Momeala abuzează de curiozitatea dumneavoastră naturală pentru a vă convinge să vă expuneți unui atacator. Manipularea folosită pentru a vă exploata este, de regulă, posibilitatea de a obține ceva exclusiv sau gratuit. Acest tip de abuz implică, de obicei, infectarea dispozitivului dvs. cu programe malware.

Metodele populare de atragere includ unitățile USB lăsate în spații publice și atașamentele de e-mail care conțin detalii despre o ofertă specială sau un software gratuit falsificat.

**3. Atacuri prin pătrundere fizică**

Acest tip de atac presupune ca hackerii să apară ei înșiși, prezentându-se ca fiind o persoană de încredere pentru a obține acces neautorizate la zone sau date protejate.

Astfel de atacuri sunt cel mai des întâlnite în mediile de afaceri, cum ar fi întreprinderile, guvernele sau alte organizații. Prin urmare, infractorii pretind că sunt reprezentanții unei companii de încredere. Este posibil ca unii dintre ei să fie chiar angajați recent concediați care vor să se răzbune.

Aceștia își creează o identitate necunoscută, dar suficient de credibilă pentru a evita alte întrebări. Acest lucru necesită o mică cercetare din partea atacatorului și implică, de asemenea, un risc ridicat.

**4. Atacurile de tip pretext**

Pretexting-ul folosește identități înșelătoare ca o „scuză” pentru a crea încredere, cum ar fi să se prezinte direct drept un furnizor sau un angajat al unei unități. Această metodă presupune ca atacatorul să interacționeze mai activ cu dumneavoastră. Odată ce v-au convins că sunt autentici, vor continua să vă exploateze.

**5. Atacuri de acces „tailgating”**

Tailgating (sau piggybacking) este încearcarea de a intra într-o zonă cu acces restricționat pe urmele unui angajat autorizat.

Practic, atacatorii încearcă să vă convingă că și ei sunt autorizați să se afle în zona respectivă. De fapt, și pretextarea poate juca un rol în acest caz.

**6. Atacuri quid pro quo**

Aceasta înseamnă literalmente „o favoare pentru o favoare”, ceea ce, în contextul phishing-ului, înseamnă un schimb de informații personale în schimbul unor recompense sau compensații. Cel mai frecvent, ofertele sau cadourile oferite pentru participarea la studii de cercetare vă pot expune la acest tip de atac.

Exploatarea vine din entuziasmul pentru ceva valoros obținut cu o investiție mică. În cele din urmă, însă, atacatorul pur și simplu colectează datele fără nicio recompensă pentru dvs.

**7. Atacurile de falsificare de DNS și de otrăvire a memoriei cache**

DNS spoofing manipulează browserul și serverele web pentru a vă redirecționa către site-uri web periculoase atunci când introduceți un URL legitim. Odată infectată, redirecționarea va continua, cu excepția cazului în care datele de rutare greșite sunt șterse din sistemele implicate.

Pe de altă parte, atacurile de otrăvire a memoriei cache DNS vă infectează în special dispozitivul cu instrucțiuni de rutare pentru ca URL-ul legitim sau mai multe URL-uri să se conecteze la site-uri web suspecte.

**8. Atacuri de tip „scareware”**

Scareware este un tip de malware folosit pentru a vă speria și a vă determina să întreprindeți o acțiune. Acest tip de malware înșelător folosește avertizări alarmante care raportează false infecții cu malware sau afirmă că unul dintre conturile dumneavoastră a fost compromis.

Ca efect, scareware vă obligă să cumpărați software de securitate cibernetică fraudulos sau să dezvăluiți informații private, cum ar fi datele de identificare ale contului dumneavoastră.

**9. Atacurile de tip „watering hole”**

Aceste atacuri infectează pagini web bine cunoscute cu programe malware pentru a avea un impact asupra unui număr mare de utilizatori în același timp. Este nevoie de o planificare atentă din partea atacatorului pentru a găsi vulnerabilități în anumite site-uri. Aceștia caută punctele slabe existente care nu sunt cunoscute și nu au fost corectate (aceste vulnerabilități sunt considerate exploatări de tip zero-day)

Este posibil să constate că un site web nu și-a actualizat infrastructura pentru a remedia problemele cunoscute. Proprietarii de site-uri web aleg de obicei să amâne actualizările de software pentru a păstra versiunile de software pe care le știu stabile. Aceștia le vor schimba atunci când versiunea mai nouă va avea un istoric dovedit de stabilitate a sistemului.

Prin urmare, hackerii exploatează acest comportament pentru a viza punctele slabe recent remediate.

**10. Metode neobișnuite de inginerie socială**

***phishing pe bază de fax***: atunci când un client al unei bănci primește un e-mail fals care pretinde că provine de la bancă și care îi cere clientului să confirme codul de acces, metoda de confirmare nu a fost cea obișnuită prin e-mail sau internet. În schimb, clienții erau rugați să tipărească formularul din e-mail, apoi să completeze datele lor și să trimită formularul prin fax la numărul de telefon al atacatorului.

***distribuția tradițională de malware prin poștă***: în Japonia, atacatorii cibernetici au folosit un serviciu de livrare la domiciliu pentru a distribui CD-uri infectate cu un spyware troian. CD-urile au fost livrate clienților unei bănci japoneze. În acest caz, adresele clienților fuseseră furate anterior din baza de date a băncii.

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

Atacurile de tip phishing sunt o metodă comună utilizată de hackeri pentru a obține informații sensibile, cum ar fi parole sau date bancare. Aceste atacuri implică crearea unor site-uri web sau e-mail-uri false care imită site-uri web sau e-mail-uri legale, cu scopul de a convinge utilizatorii să furnizeze informații personale.

Iată câteva metode și tehnici utilizate în atacurile de tip phishing:

* **E-mail-uri false** - Phishing-ul prin e-mail-uri este unul dintre cele mai comune tipuri de atacuri de phishing. Hackerii trimit e-mail-uri false care par să fie de la bănci, furnizori de servicii sau alte companii legitime. E-mail-ul poate conține link-uri către site-uri web false, unde utilizatorul este apoi rugat să furnizeze informații personale.
* **Site-uri web false** - Hackerii pot crea site-uri web false care imită site-uri web legitime. Aceste site-uri pot fi folosite pentru a obține informații personale sau pentru a distribui malware.
* **Phishing prin SMS** - Aceasta este o formă relativ nouă de atacuri de phishing care implică trimiterea de mesaje SMS false. Utilizatorii sunt rugați să furnizeze informații personale sau să descarce anumite aplicații, care pot conține malware.
* **Spear phishing** - Această formă de atacuri de phishing se concentrează asupra unor utilizatori specifici, cum ar fi angajații unei companii. Hackerii cercetează în prealabil victima și apoi trimit un e-mail fals sau un mesaj cu un link spre un site fals, cu scopul de a obține informații confidențiale.
* **Tab fishing** - Acesta este un tip de atac de phishing care implică redirectionarea utilizatorului către un site web fals atunci când face clic pe un link. Site-ul fals poate fi făcut să arate exact ca un site web legitm, astfel încât utilizatorul să fie indus în eroare și să furnizeze informații personale.
* **Social Engineering** - Aceasta este o tehnică de manipulare psihologică utilizată pentru a convinge utilizatorii să furnizeze informații personale. Hackerii pot utiliza această tehnică prin intermediul e-mail-urilor false sau prin intermediul site-urilor web false pentru a induce utilizatorii să dezvăluie informații sensibile.
* **URL-uri falsificate** - Hackerii pot crea URL-uri falsificate care par să fie legitime, pentru a convinge utilizatorii să acceseze un site web fals. Aceste URL-uri falsificate pot fi trimise prin e-mail-uri, mesaje SMS sau prin intermediul rețelelor de socializare.
* **Atacuri de tip Man-in-the-Middle (MitM)** - Aceasta este o tehnică de interceptare a traficului de rețea, prin care hackerii pot obține acces la informații personale și financiare. În cazul atacurilor de phishing, hackerii pot utiliza această tehnică pentru a intercepta datele furnizate de utilizatori către site-uri web sau aplicații.
* **Atacuri prin intermediul browser-ului** - Aceste atacuri implică folosirea vulnerabilităților din browser-ul utilizatorului pentru a instala malware sau pentru a accesa informații personale și financiare.
* **Phishing prin intermediul rețelelor de socializare** - Această tehnică implică crearea de conturi false pe rețelele de socializare, cu scopul de a obține informații personale și financiare de la utilizatori.

Pentru a evita atacurile de phishing, este important să fii conștient de aceste metode și tehnici. Este important să nu furnizezi niciodată informații personale prin intermediul unor e-mail-uri sau site-uri web suspecte. În plus, folosește mereu parole puternice și actualizează-le frecvent, iar pentru a verifica autenticitatea unui site web, asigura-te că adresa URL începe cu "https" și are un lacăt verde în bara de adrese.

**Stabilirea recomandărilor și metodelor de protecție împotriva ingineriei sociale**

* Educație și conștientizare - Este important să înțelegi cum funcționează tehnica de inginerie socială și să fii conștient de diferitele tehnici de manipulare utilizate de hackeri și infractori cibernetici. Ar trebui să fii sceptic în ceea ce privește cererile de informații personale sau financiare și să eviți să dai clic pe link-uri sau să descarci atașamente din e-mail-uri suspecte.
* Autentificare în doi factori (2FA) - 2FA este o metodă de autentificare suplimentară care necesită o informație suplimentară pe lângă parolă pentru a accesa un cont. De exemplu, un cod de verificare trimis prin SMS sau prin intermediul unei aplicații autentificare. Acest lucru face mai dificilă accesarea conturilor de către infractori cibernetici chiar dacă aceștia au obținut parola ta.
* Software de securitate - Instalează software de securitate pe dispozitivele tale și asigură-te că acestea sunt actualizate în mod regulat. Software-ul de securitate poate detecta și bloca site-urile web și e-mail-urile suspecte, precum și alte amenințări cibernetice.
* Verificarea site-urilor web - Asigură-te că verifici întotdeauna URL-ul site-urilor web înainte de a furniza informații personale sau financiare. Verifică dacă site-ul web utilizează protocolul HTTPS și dacă este emis un certificat SSL valid.
* Politici de securitate - Companiile ar trebui să aibă politici de securitate solide și să ofere formare angajaților lor în ceea ce privește tehnici de protecție împotriva ingineriei sociale. Aceste politici ar trebui să includă reguli stricte privind accesul la informații sensibile și să ofere instrucțiuni clare cu privire la gestionarea și protejarea datelor confidențiale.
* Audituri de securitate - Companiile ar trebui să efectueze audituri de securitate regulate pentru a detecta vulnerabilitățile din sistemul lor și pentru a implementa măsuri de protecție adecvate.

În general, o abordare proactivă în ceea ce privește securitatea informatică și educarea cu privire la tehnicile de inginerie socială sunt cele mai bune metode pentru a te proteja împotriva atacurilor cibernetice.

**Exercițiu de interceptare a traficului local și din rețea**

Wireshark este un instrument de analiză a traficului de rețea open source, care permite utilizatorilor să intercepteze, să filtreze și să analizeze traficul de rețea. Acest instrument poate fi utilizat pentru a înțelege mai bine cum funcționează traficul de rețea și pentru a identifica problemele de performanță sau de securitate în rețea. În exercițiul de interceptare a traficului local și din rețea, utilizarea Wireshark poate fi utilă pentru a obține informații despre traficul de rețea care circulă prin rețeaua locală.

Cele cinci componente majore ale instrumentului Wireshark sunt următoarele și acestea sunt arătate în figura 1:

* Meniuri de comandă - Acestea sunt meniurile principale ale aplicației Wireshark și conțin opțiuni pentru a porni sau opri captura de pachete, pentru a aplica filtre și pentru a exporta datele capturate.
* Filtru protocol - Wireshark permite utilizatorilor să filtreze pachetele în funcție de diferite protocoale, cum ar fi HTTP, DNS sau TCP/IP. Acest filtru poate fi folosit pentru a limita numărul de pachete capturate și pentru a se concentra pe un protocoal specific.
* Lista pachetelor capturate - Aceasta este o listă de pachete capturate care afișează informații precum adresa IP sursă și destinație, protocolul și dimensiunea pachetului. Utilizatorii pot selecta un pachet din această listă pentru a vedea informații detaliate despre acel pachet.
* Detaliile antetului pachetului selectat - Acesta afișează informații detaliate despre antetul pachetului selectat, cum ar fi adresa IP sursă și destinație, numărul de secvență și de confirmare pentru protocoalele TCP și informații despre controlul de flux.
* Conținutul pachetului în format hexadecimal și ASCII - Această componentă afișează conținutul pachetului în format hexadecimal și ASCII. Această informație poate fi utilă pentru a identifica tipul de informații care circulă în rețea și poate fi utilizată pentru a detecta probleme de securitate, cum ar fi parole sau date personale necriptate.

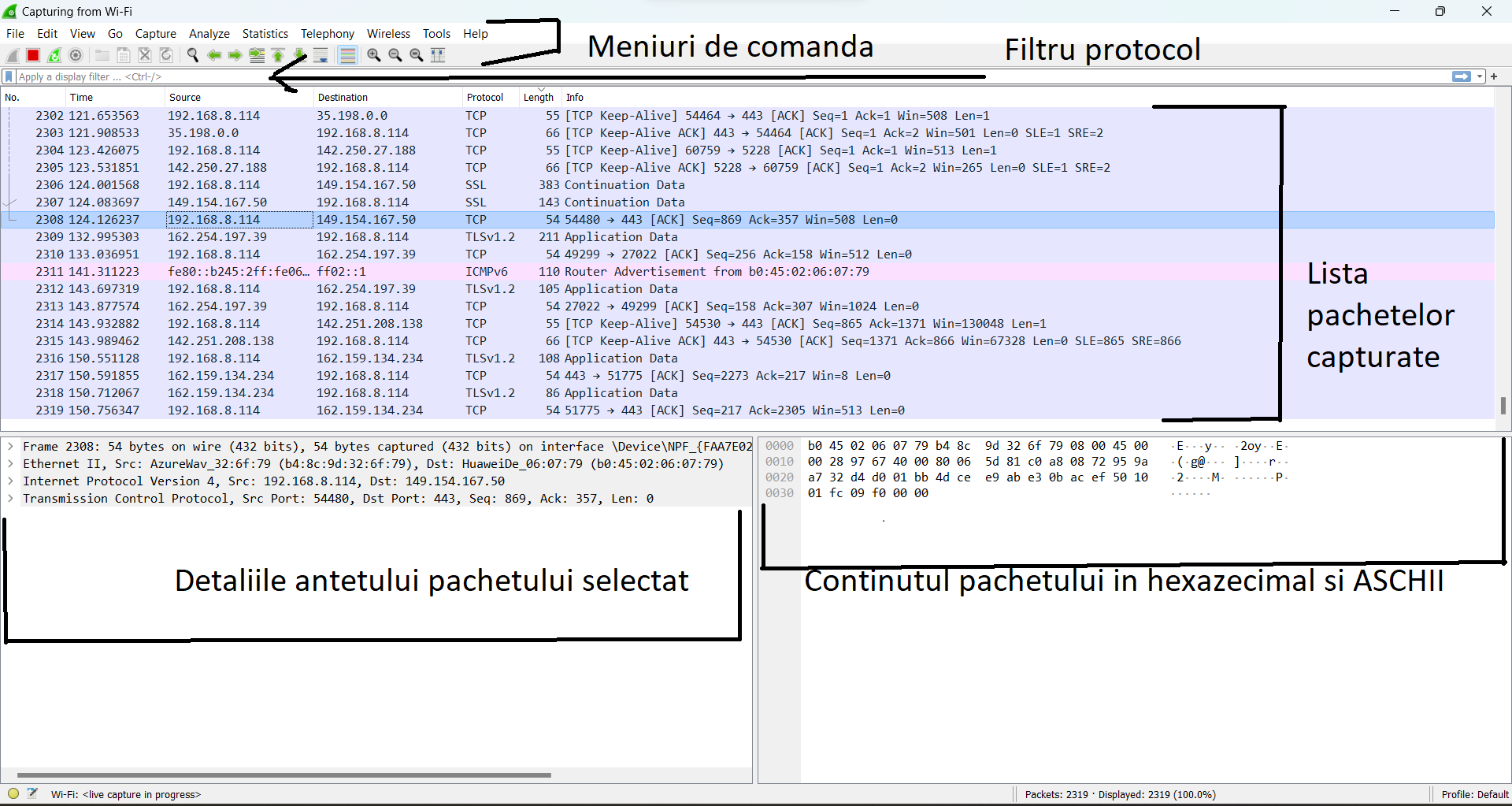


Figura 1- Instrumentul de captare a pachetelor

**Simularea unui atac de tip DoS**

Atacurile de tip DoS (Denial of Service) și DDoS (Distributed Denial of Service) sunt două tipuri de atacuri cibernetice care vizează să împiedice accesul la un serviciu sau la o resursă online prin inundarea cu trafic sau cereri false.

Un atac DoS implică trimiterea unui număr mare de cereri la un server sau la o resursă online, astfel încât să devină supraîncărcat și să nu mai poată gestiona cererile legitime. Acest tip de atac este efectuat de obicei de la un singur dispozitiv, care trimite o cantitate mare de trafic către ținta sa.

Un atac DDoS, pe de altă parte, implică utilizarea a numeroase dispozitive (de obicei, aparate botnet) pentru a trimite trafic sau cereri către ținta. Acest lucru face ca atacul să fie mult mai puternic și mai dificil de contracarat decât un atac DoS.

Printre obiectivele frecvente ale atacurilor de tip DoS și DDoS se numără site-uri web, servere de jocuri online, servere de email și alte resurse online.

Pentru a preveni și a contracara aceste tipuri de atacuri, este important să se ia măsuri de securitate cibernetice adecvate, cum ar fi utilizarea de firewall-uri, îmbunătățirea infrastructurii rețelei și folosirea de servicii de protecție împotriva atacurilor DDoS.

Într-o experiență simulată de securitate cibernetică, am folosit sistemul de operare Kali Linux instalat pe o mașină virtuală și am atacat o altă mașină virtuală cu sistemul de operare Windows 10. Scopul meu a fost să întrerup conexiunea la internet a mașinii țintă prin efectuarea unui atac de tip DOS (Denial of Service).

Pentru a îndeplini acest obiectiv, am urmat instrucțiunile dintr-un articol care era plasat pe pagina cu sarcina laboratorului de pe platforma Medium, disponibil la adresa <https://medium.com/geekculture/simple-but-powerful-denial-of-service-dos-attack-8c7dfd60045f.> Pas cu pas, am parcurs procesul descris acolo pentru a crea un atac DOS care să blocheze accesul la internet al mașinii țintă, precum e arătat în figura 2.

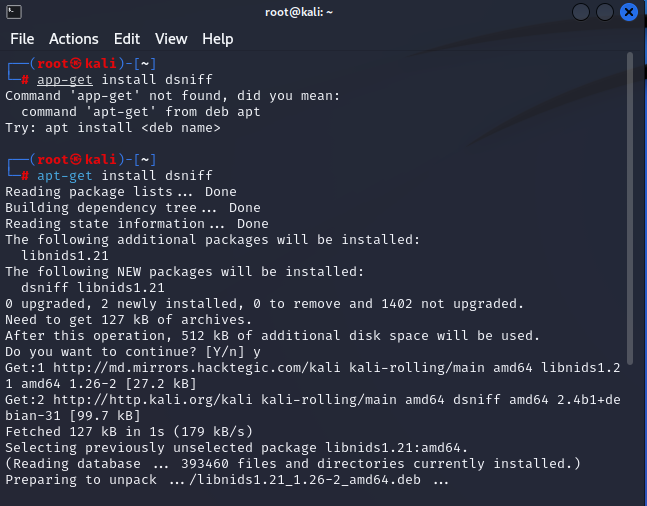


Figura 2- Realizarea pașilor din linkul plasat în terminalul Kali Linux

În primul rând, am verificat adresa IP a mașinii țintă utilizând comanda "ipconfig" pe linia de comandă a sistemului de operare Windows 10 și totodată am verificat dacă dispozitivul este conectat la internet deschizând browserul Microsoft Edge, în figura 3 este arătat că mașina virtuală avea acces la internet înainte de atac. Am utilizat această adresă IP pentru a trimite mai apoi pachete de date către mașina țintă. Am deschis apoi terminalul Kali Linux și am început să creez un număr mare de pachete de date utilizând o comandă specifică din Kali Linux.

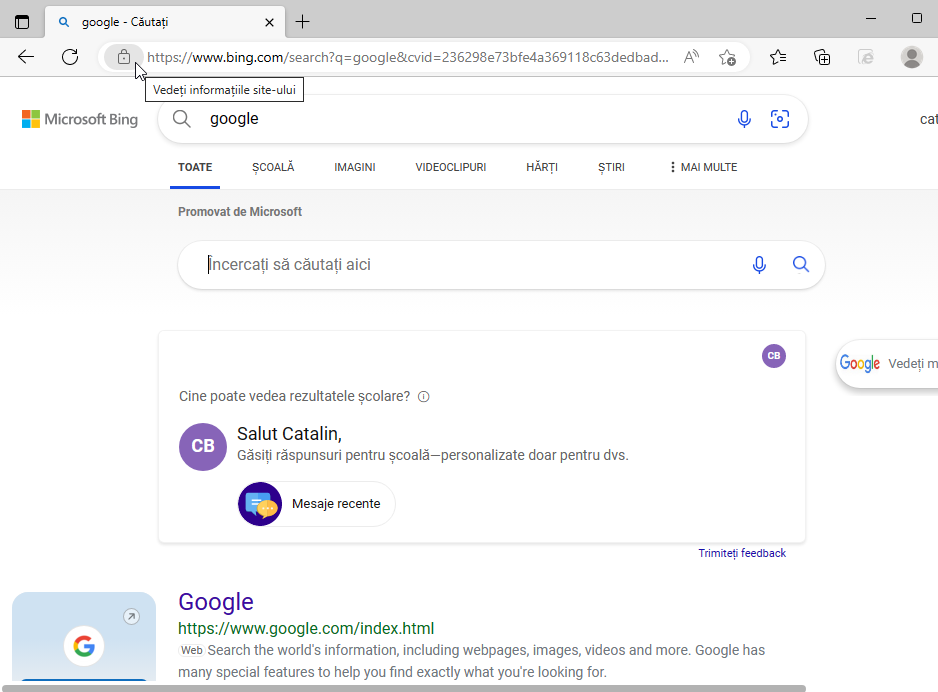


Figura 3- Verificarea conectivității la internet a mașini virtuale înainte de atac

Apoi, am folosit o altă comandă pentru a trimite aceste pachete de date într-un mod continuu către adresa IP a mașina țintă în figura 4 este văzută această comandă.

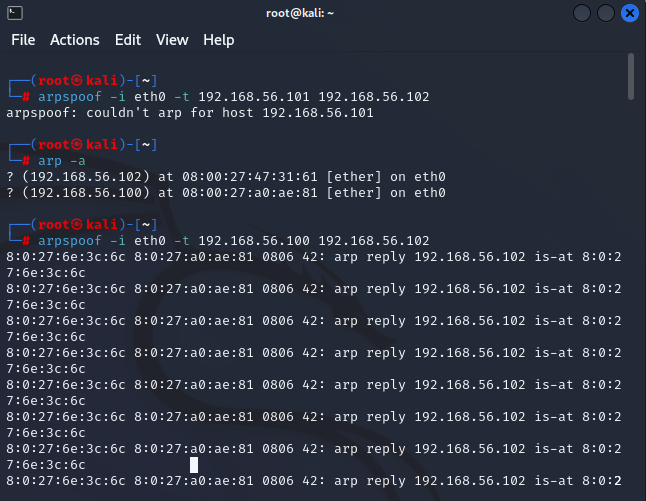


Figura 4- Trimiterea continuă a pachetelor către mașina țintă

Acest flux constant de pachete de date către mașina țintă a creat o supraîncărcare de trafic care a dus la blocarea conexiunii la internet a mașinii țintă. În figura 5 este reprezentat consecințele atacului DoS.

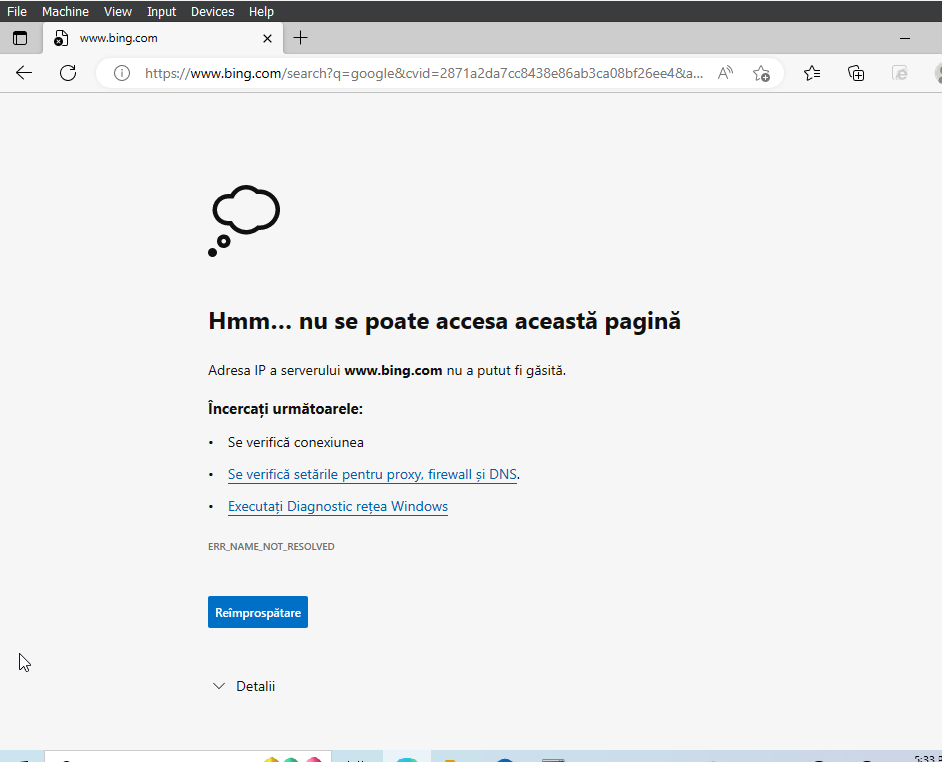


Figura 5- Starea mașini virtuale după atac

În scop educativ, vom încerca să efectuăm un atac de tip brute-force pentru a sparge parola unei mașini virtuale care rulează sistemul de operare Windows 10. Pentru a efectua acest atac, vom folosi sistemul de operare Kali Linux, instalat pe o mașină virtuală separată.

În primul rând, trebuie să verificăm dacă mașina virtuală țintă poate fi accesată din rețeaua noastră. Pentru aceasta, vom rula comanda "ping" pentru a trimite pachete către adresa IP a mașinii țintă și a vedea dacă primim un răspuns.

Dacă primim un răspuns, vom folosi comanda "Medusa" pentru a efectua atacul brute-force. Această comandă este deja preinstalată în sistemul de operare Kali Linux și poate fi folosită pentru a ataca servicii care necesită autentificare.

Pentru a folosi comanda Medusa, vom specifica mai întâi protocolul de autentificare pe care vrem să îl atacăm, adresa IP a mașinii țintă, portul de serviciu și lista de utilizatori și parole posibile.

De exemplu, dacă vrem să atacăm protocolul SMB (Server Message Block) pentru a sparge parola unui utilizator pe mașina virtuală țintă, vom rula următoarea comandă:

medusa -h <adresa-IP-țintă> -u <utilizatori.txt> -p <parole.txt> -M smbnt

În această comandă, "<adresa-IP-țintă>" reprezintă adresa IP a mașinii virtuale țintă, "utilizatori.txt" și "parole.txt" sunt fișierele text care conțin lista de utilizatori și parole posibile, iar "smbnt" specifică protocolul SMB folosit de mașina țintă.

Dacă comanda Medusa găsește o combinație validă de utilizator și parolă, vom vedea un mesaj de succes și vom putea accesa serviciul dorit cu aceste credențiale. Este important de menționat că acest atac poate dura mult timp și poate necesita resurse considerabile, așa că ar trebui efectuat numai într-un mediu de testare și cu permisiunea proprietarului mașinii virtuale țintă. În figura 6 este reprezentat un exemplu de atac brute-force realizat de către mine.

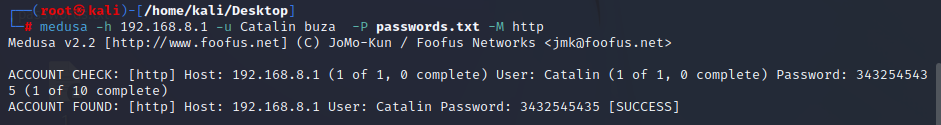


Figura 6 – Atac forță brută reușit

Concluzie:

În concluzie, lucrarea nr. 2 la Tehnologii de Securitate Informațională a oferit o perspectivă cuprinzătoare asupra atacurilor cibernetice și a tehnicilor folosite pentru a le efectua. Am studiat diverse tipuri de atacuri, inclusiv ingineria socială și phishing-ul, care se bazează pe manipularea oamenilor pentru a obține acces neautorizat la sisteme și informații. De asemenea, am învățat despre metodele și tehnicile utilizate în atacurile de tip DoS și brute-force.

Pentru a proteja sistemele noastre împotriva acestor atacuri, am discutat despre recomandări și metode de protecție, cum ar fi autentificarea cu doi factori și utilizarea de parole puternice. De asemenea, am efectuat un exercițiu de interceptare a traficului local și din rețea, care ne-a arătat cât de ușor poate fi accesată informația în timp ce circulă pe rețea.

Pentru a înțelege mai bine modul în care se efectuează atacurile, am testat diferite instrumente precum ncrack, hydra și medusa, care ne-au arătat cum se poate efectua un atac de tip brute-force pentru a sparge parolele sistemelor protejate.

În general, această lucrare ne-a ajutat să înțelegem importanța securității informaționale și cât de important este să ne protejăm informațiile și sistemele împotriva atacurilor cibernetice. Cu cât suntem mai bine informați și pregătiți, cu atât suntem mai în siguranță în lumea digitală în care trăim.