**PenTest: Aplicație practică realizată în Kali Linux**

**PenTest pe domeniul www.ted.com**

PROFESOR: STUDENT:

CONFERENȚIAR DR. BRÂNDAȘ CLAUDIU VALCOV BIANCA

**Cuprins**

[Etapa 1: Recunoașterea 3](#_Toc125663534)

[1.Culegere de informații folosind aplicația Maltego 3](#_Toc125663535)

[2.Culegere de informații folosind aplicația dmitry 4](#_Toc125663536)

[3. Schimbare MAC 5](#_Toc125663537)

[4. Utilizare comenzi dig și nslookup 6](#_Toc125663538)

[Etapa 2: Scanarea 7](#_Toc125663539)

[1.Scanare domeniu cu nmap 7](#_Toc125663540)

[2.Scanare domeniu cu nikto 9](#_Toc125663542)

[3. Scanare domeniu utilizând aplicația Legion 10](#_Toc125663543)

[4. Scanare subdomenii folosind wpscan 11](#_Toc125663544)

[Etapa 3: Exploatarea 14](#_Toc125663545)

[1.Exploatare versiune cu mysql\_version 14](#_Toc125663546)

[2.Exploatare servicii cu mysql\_enum 15](#_Toc125663547)

[3.Exploatare istoric de login cu mysql\_login 15](#_Toc125663548)

[4. Exploatare folosind hashdump 16](#_Toc125663549)

[5.Exploatare pe serverul de WordPress 17](#_Toc125663551)

[6. WordPress RevSlider File Upload and Execute Vulnerability 18](#_Toc125663552)

[Bibliografie 18](#_Toc125663553)

# **Etapa 1: Recunoașterea**

În acest proiect este analizat domeniul www.ted.com împreună cu toate subdomeniile acestuia (ex: blog.ted.com, ideas.ted.com).

## **1.Culegere de informații folosind aplicația Maltego**

În etapa de recunoaștere domeniul www.ted.com și subdomeniul www.blog.ted.com sunt analizate folosind instrumentul de extragere a datelor, Maltego.

În urma analizei de infrastructură și a culegerii de informații am descoperit următoarele posibile ținte care vor fi scanate în etapa următoare, și anume: adresa IP a web serverului, porturile 80 și 443, subdomeniile blog.ted.com și ideas.ted.com sunt realizate în WordPress, făcând accesibilă scanarea lor cu comanda wpscan și exploatarea în Metasploit Framework Console.

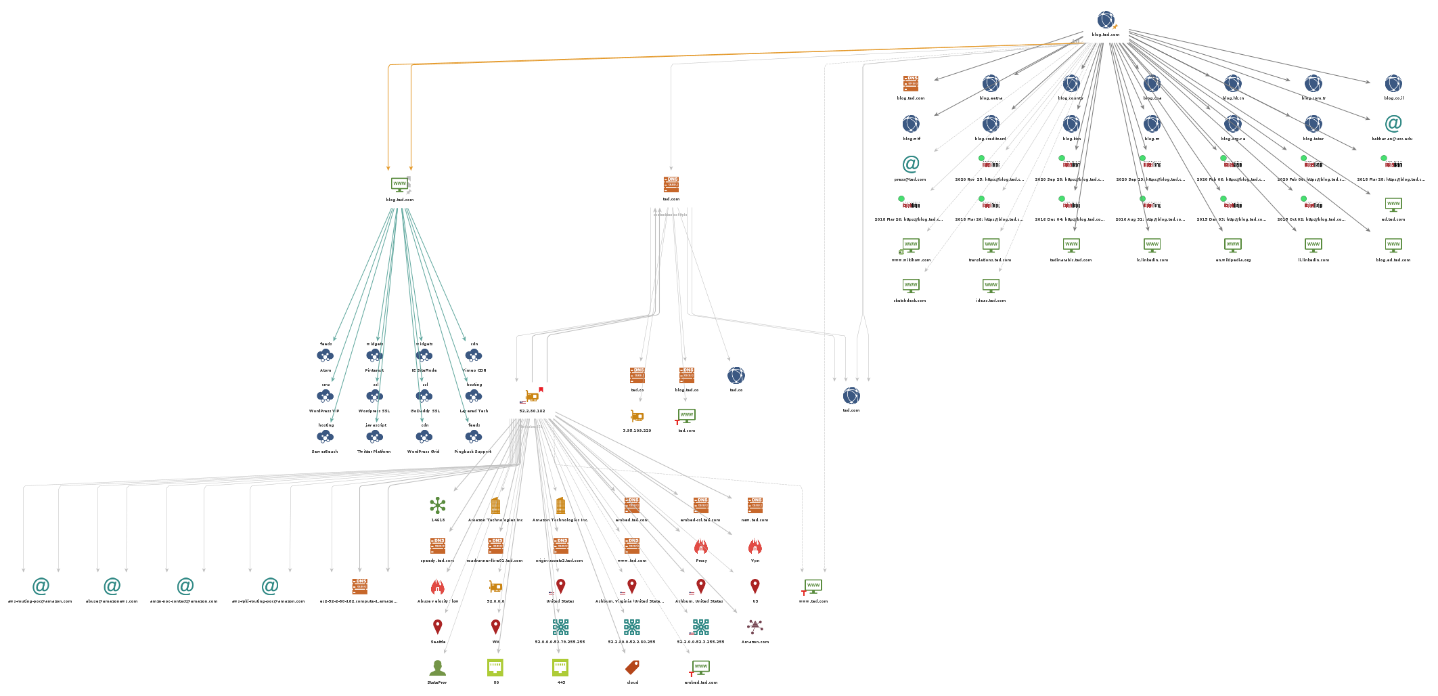
****

Figura 1. Infrastructură domeniu www.ted.com



Figura 2. Infrastructură subdomeniu blog.ted.com

## **2.Culegere de informații folosind aplicația dmitry**

O imagine care conține text

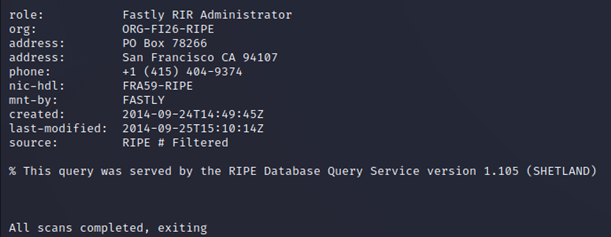
Descriere generată automat

Figura 3. Analiză website folosind aplicația dmitry

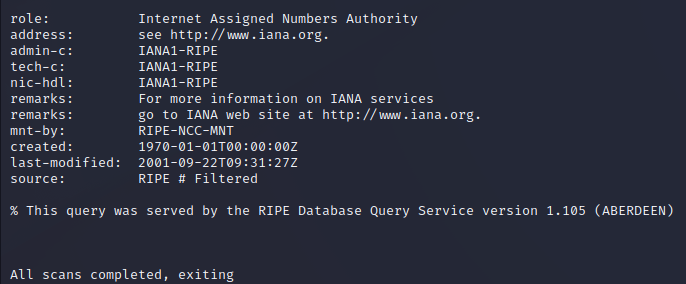
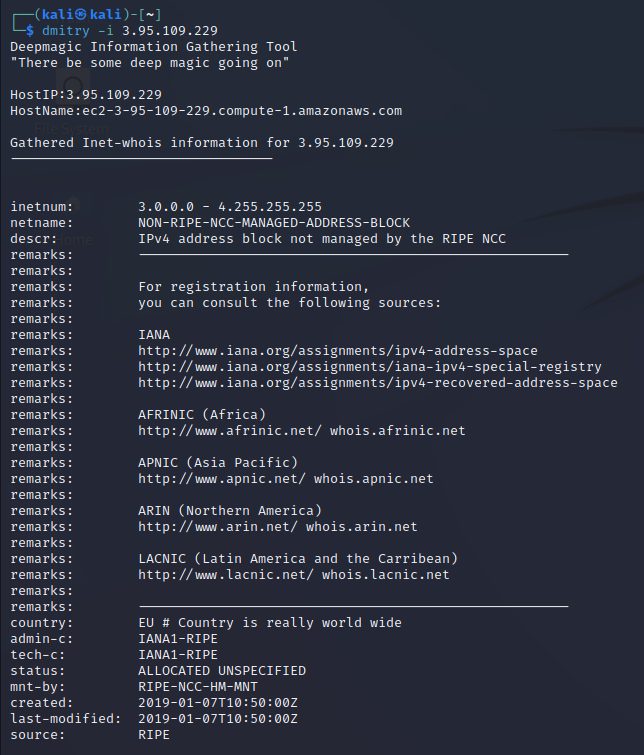


Figura 4. Analiză adresă IP folosind dmitry

**O imagine care conține text

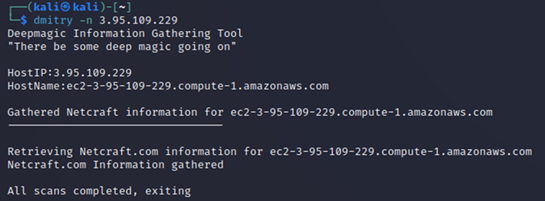
Descriere generată automat**

Figura 5. Analiză folosind comanda dmitry -n

O imagine care conține text

Descriere generată automat

Figura 6. Descoperire subdomenii existente cu dmitry -s

## **3. Schimbare MAC**

O imagine care conține text

Descriere generată automat

Figura 7. Schimbarea mac-ului plăcii de rețea cu o adresă random

## **4. Utilizare comenzi dig și nslookup**

Pentru a obține adresa IP a domeniului pe care o vom folosi în comanda nmap vom utiliza comenzile dig și nslookup. Din imaginile de mai jos putem vedea că IP-ul pentru www.ted.com este 146.75.122.133, iar pentru blog este 192.0.66.44.



Figura 8. Comandă dig pentru aflare IP

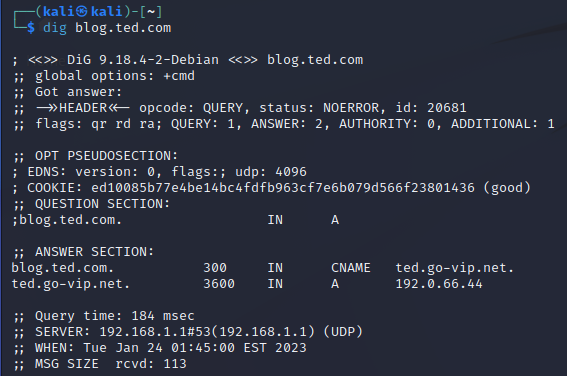


Figura 9. Comandă dig pe blog.ted.com

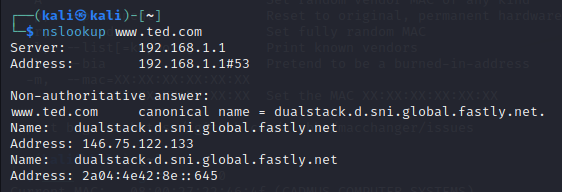


Figura 10. Comandă nslookup pentru aflare IP

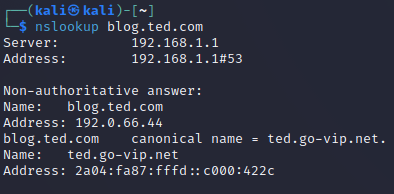


Figura 11. Comandă nslookup pe blog.ted.com

# **Etapa 2: Scanarea**

Pentru scanare vom analiza vulnerabilitățile descoperite în etapa de recunoaștere. Se vor folosi comenzile nmap -A -sV -Pn, nikto, wpscan pentru subdomenii și aplicața Legion. În urma scanării am descoperit că porturile 80 și 443 sunt deschise pentru serviciile http și ssl/https.

## **1.Scanare domeniu cu nmap**

# **O imagine care conține text Descriere generată automat**

O imagine care conține text

Descriere generată automat

Figura 12. Scanare cu nmap – port 80 deschis

O imagine care conține text

Descriere generată automatO imagine care conține text

Descriere generată automat

Figura 13. Scanare cu nmap - port 443 deschis

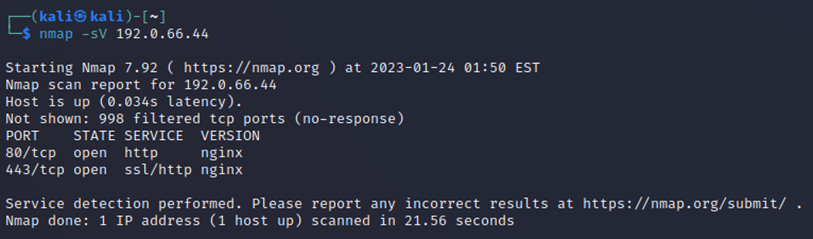


Figura 14. Scanare server cu nmap -sV

## **2.Scanare domeniu cu nikto**

În urma scanării cu nikto am găsit mai multe vulnerabilități, precum:

* The anti-clickjacking X-Frame-Options header is not present.

Headerul de raspuns HTTP X-Frame-Options poate fi folosit pentru a indica dacă unui browser ar trebui să i se permită sau nu să redea o pagină într-un <frame>,<iframe> sau <object> . Site-urile pot folosi acest lucru pentru a evita atacurile de tip clickjacking, asigurându-se că conținutul lor nu este încorporat în alte site-uri.

Există două modalități principale de a preveni clickjacking-ul:

* Trimiterea antetelor de răspuns HTTP X-Frame-Options adecvate care indică browserului să nu permită încadrarea din alte domenii
* Utilizarea codului defensiv în interfața de utilizare.
* Configurați serverul web pentru a include un header X-Frame-Options și un header CSP cu directivă frame-ancestors.
* The X-XSS-Protection header is not defined.

Prin această vulnerabilitate site-ul este expus unor atacuri de tip cross-site scripting, iar soluția pentru a remedia această vulnerabilitate ar fi setarea pe modul block a XSS-Protection (X-XSS-Protection: 1; mode=block) în fișierul de configurare al serverului.

* The X-Content-Type-Options header is not set.

Headerul http „X-Content-Type-Options” lipsă permite unui browser să efectueze sniffing MIME atunci când antetul Content-Type nu este setat sau valoarea acestuia pare nepotrivită. Cu alte cuvinte, atunci când browserul primește răspuns de la serverul web, încearcă să-și dea seama singur care este tipul de conținut și cum să-l gestioneze. În anumite circumstanțe, acest lucru poate duce la probleme grave de securitate (un atac de tip cross-site scripting). Soluția ar fi configurarea serverullui web pentru a include un header „X-Content-Type-Options” cu valoarea „nosniff” (anti MIME sniffing header).

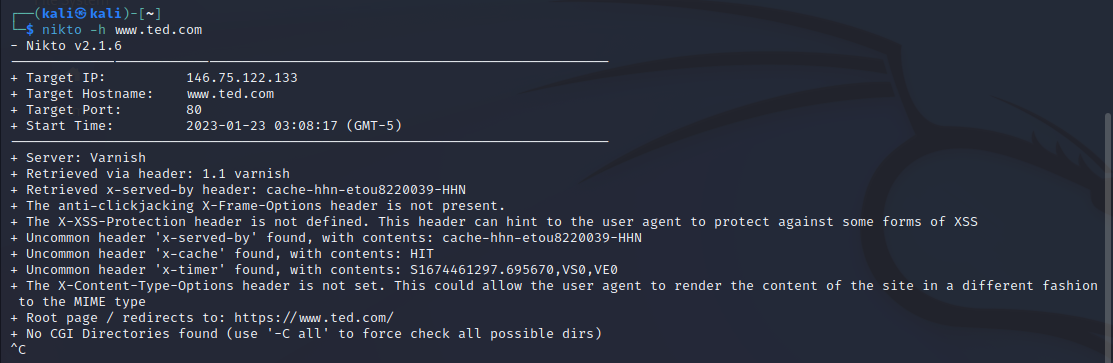


Figura 15. Scanare domeniu cu nikto -h

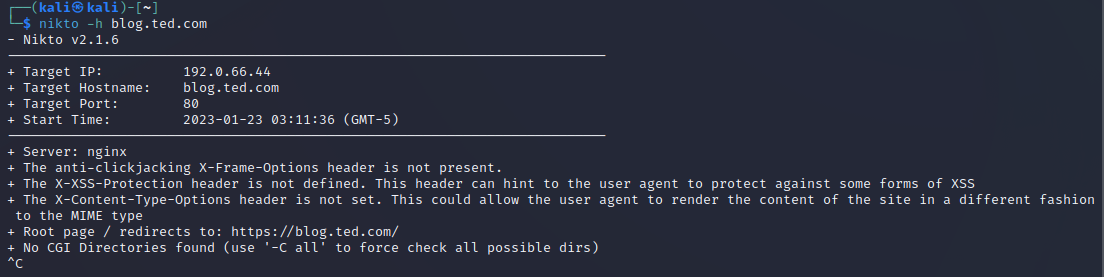


Figura 16. Scanare subdomeniu blog.ted.com cu nikto -h

## **3. Scanare domeniu utilizând aplicația Legion**

În continuare vom folosi aplicația Legion pentru a scana domeniul www.ted.com să vedem dacă putem descoperii mai multe, dar putem vedea și aici că doar porturile 80 și 443 sunt deschise și sunt afișate câteva pagini care numai sunt disponibile.

O imagine care conține text, monitor, captură de ecran, negru

Descriere generată automat

Figura 17. Scanare domeniu cu aplicația Legion

O imagine care conține text, captură de ecran, monitor

Descriere generată automat

Figura 18. Aplicația Legion - Pagini nedisponibile

## **4. Scanare subdomenii folosind wpscan**

Pentru website-ul www.ted.com doar subdomeniile blog.ted.com și ideas.ted.com sunt realizate în WordPress. În urma scanării lor cu wpscan am descoperit că în ideas.ted.com avem acces la wp-admin, fereastra de login este deschisă și că conectarea este posibilă doar dacă se cunosc username-ul și parola puse de administrator.

O imagine care conține text

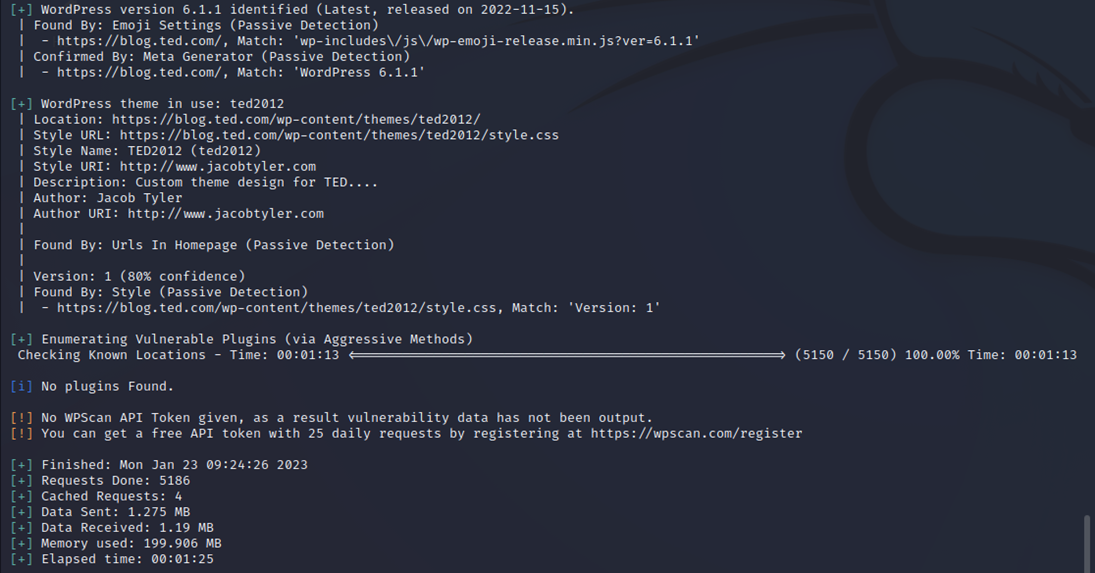
Descriere generată automat

Figura 19. Scanare subdomeniu blog.ted.com cu wpscan

O imagine care conține text

Descriere generată automatO imagine care conține text

Descriere generată automat

Figura 20. Scanare subdomeniu ideas.ted.com cu wpscan

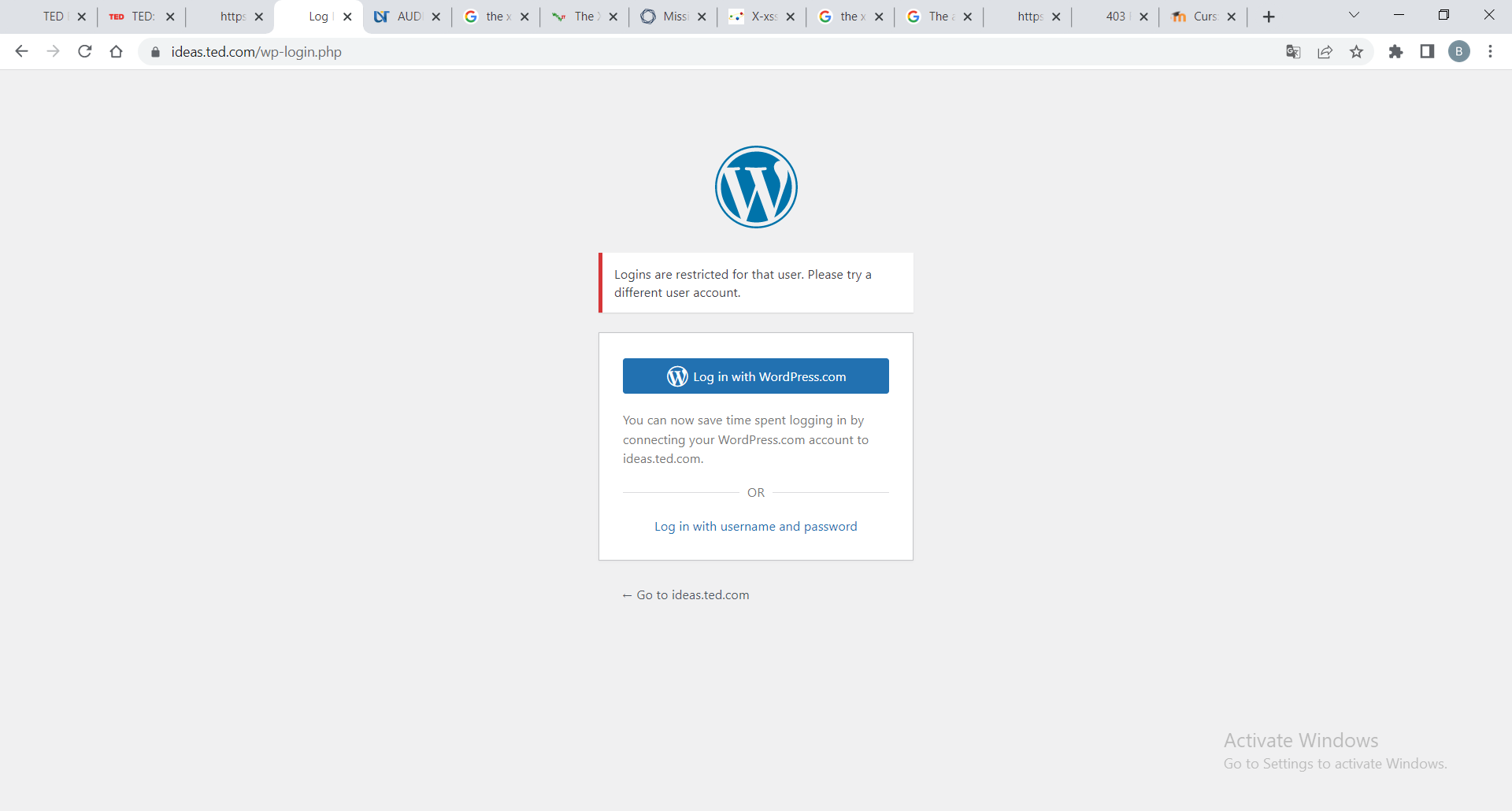


Figura 21. În wp-admin fereastra de login e deschisă

O imagine care conține text

Descriere generată automat

Figura 22. Fișierul robots.txt

# 

# **Etapa 3: Exploatarea**

După scanarea serverului 146.75.122.133 cu nmap -sV vom încerca exploatarea acestuia pe Metasploit Framework Console. Am încercat să aflu versiunea, istoricul de login, ce servicii rulează, iar cu IP-ul subdomeniilor am încercat să exploatez backup-ul bazei de date pentru a-mi face o copie a backup-ului pe local.

## **1.Exploatare versiune cu mysql\_version**

Introducem comanda info pentru a vedea ce parametrii ne cere.

Setăm parametrul RHOSTS cu 146.75.122.133 și dăm exploit.

O imagine care conține text

Descriere generată automat

Figura 23. Exploatare server mysql

## **2.Exploatare servicii cu mysql\_enum**

Setăm parametrul RHOSTS cu 146.75.122.133, username-ul cu root și dăm exploit pentru a vedea ce servicii rulează pe server.

O imagine care conține text

Descriere generată automat

Figura 24. Explotare mysql\_enum

## **3.Exploatare istoric de login cu mysql\_login**

Introducem comanda info pentru a vedea ce parametrii ne cere.

Setăm parametrul RHOSTS cu 146.75.122.133, username-ul cu guest și dăm exploit pentru a vedea dacă poate vedea istoricul de login, dar conexiunea a eșuat.

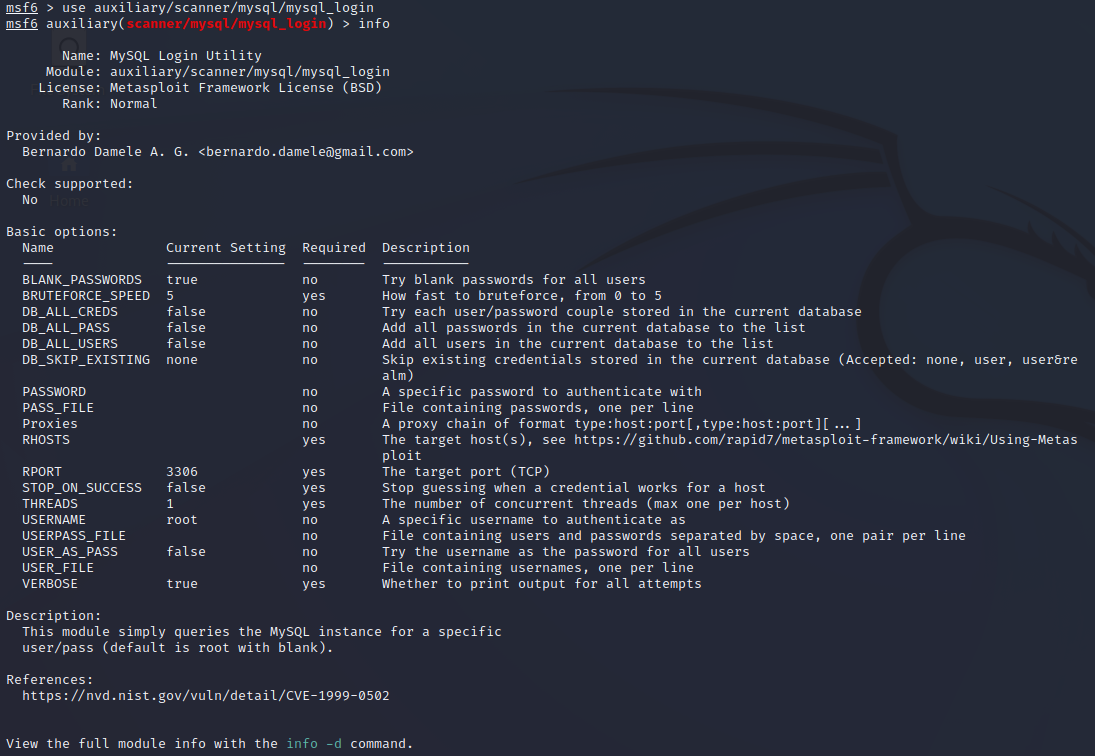


Figura 25. Info parametrii

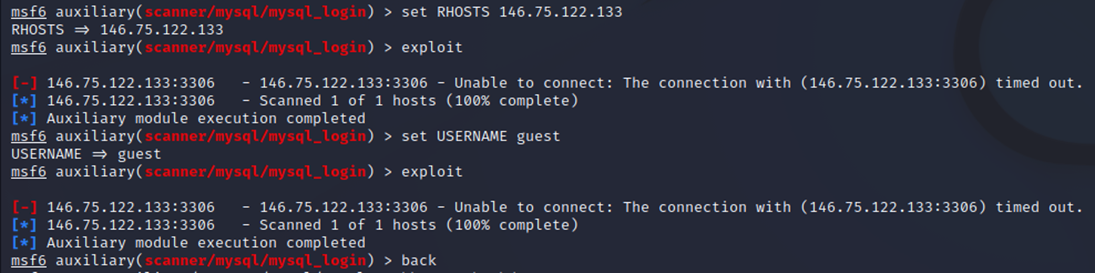


Figura 26. Exploatare cu mysql\_login

## **4. Exploatare folosind hashdump**

Încercăm acest exploit pentru a descărca hash-urile parolei conturilor de pe sistemul țintă. Aceste hashuri vor fi folosite mai târziu în încercările de spargere a parolelor, cu scopul final de a obține nume de utilizator și parole suplimentare. Setăm parametrul RHOSTS cu 146.75.122.133 și dăm exploit.

## O imagine care conține text Descriere generată automat

Figura 27.Exploatare cu hashdump

## **5.Exploatare pe serverul de WordPress**

În această încercare de exploatare a backup-ului bazei de date am folosit adresa IP de la subdomenile blog.ted.com și ideas.ted.com.

Setăm parametrul RHOSTS cu 192.0.66.44 și dăm exploit. Iar ca rezultat exploatarea nu a reușit pentru că nu avem access de login în WordPress.



Figura 28. Căutare comenzi cu wordpress

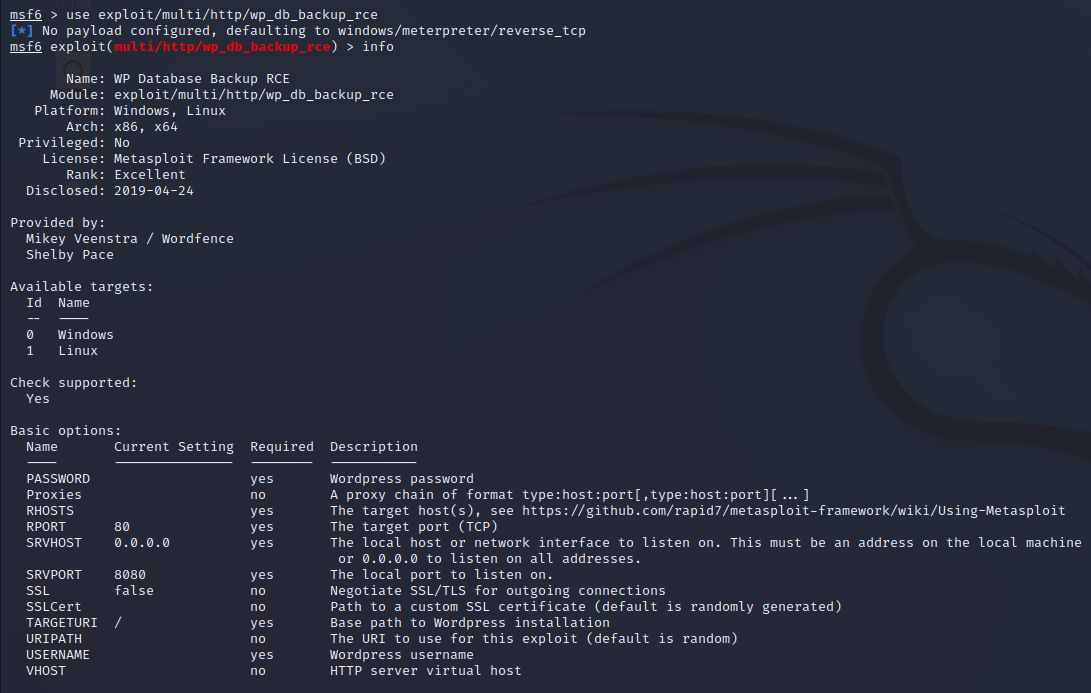


Figura 29. Info parametrii ceruți pentru execuția exploitului

O imagine care conține text

Descriere generată automat

Figura 30. Rezultat exploatare - Acces nepermis

## **6. WordPress RevSlider File Upload and Execute Vulnerability**

Acest modul exploatează o vulnerabilitate arbitrară de încărcare a codului PHP în pluginul WordPress ThemePunch Slider Revolution (RevSlider), versiunile 3.0.95 și anterioare. Vulnerabilitatea permite încărcarea arbitrară a fișierelor și executarea codului de la distanță. . Iar ca rezultat exploatarea nu a reușit, deoarece serverul returnează eroarea 404.

O imagine care conține text

Descriere generată automat

Figura 31. Rezultat exploatare - Serverul a returnat 404

# Bibliografie:

*Clickjacking X Frame Options Header Missing.* (2023). Retrieved from Valency Networks: https://www.valencynetworks.com/kb/clickjacking-x-frame-options-header-missing.html

*Clickjacking: X-Frame-Options header.* (2023). Retrieved from Acunetix: https://www.acunetix.com/vulnerabilities/web/clickjacking-x-frame-options-header/

TED. (2023). *TED: Ideas worth spreading.* Retrieved from TED: https://www.ted.com/

*TED Blog.* (2023). Retrieved from TED Blog: https://blog.ted.com/

*TED: Explore ideas worth spreading.* (2023). Retrieved from TED Ideas: https://ideas.ted.com/

*X-Content-Type-Options Header Missing.* (2023). Retrieved from scan repeat: https://scanrepeat.com/web-security-knowledge-base/x-content-type-options-header-missing

*X-xss Protection Header Missing.* (2023). Retrieved from Valency Networks: https://www.valencynetworks.com/kb/x-xss-protection-header-missing.html