**ACADEMIA TEHNICĂ MILITARĂ “FERDINAND I”**

**FACULTATEA DE SISTEME INFORMATICE ŞI SECURITATE CIBERNETICĂ**

**Specializarea: Calculatoare şi sisteme informatice pentru apărare şi securitate naţională**

A yellow eagle with a crown and a shield

Description automatically generated

# **Proiectarea Sistemelor de Operare**

**Aplicație de Tip Port Scanner**

Îndrumător: Slt. Ing. Vaman Adina Sd. Sg. Ungureanu Andrei-Marian

Grupa C113E

Cuprins

[**Proiectarea Sistemelor de Operare** 1](#_Toc152693049)

[1. Prezentare Generala 3](#_Toc152693050)

[1.1 Utilizări Comune ale Scanerelor de Porturi 4](#_Toc152693051)

[1.2 Scannere de Porturi Consacrate 4](#_Toc152693052)

[2.Notiuni Teoretice 6](#_Toc152693053)

[3. Structura Aplicatiei 7](#_Toc152693054)

[4. Teste Functionalitati Actuale 8](#_Toc152693056)

[4.1 Scanare Normala 8](#_Toc152693057)

[4.2 Scanarea implicita 9](#_Toc152693058)

[4.3 Scanarea domeniului 10](#_Toc152693062)

[4.4 Scanarea tuturor porturilor 11](#_Toc152693063)

[4.5 Scanarea porturilor importante 11](#_Toc152693064)

[4.6 Scanarea celor mai importante porturi ale unui domeniu 11](#_Toc152693066)

[Bibliografie 13](#_Toc152693067)

# Prezentare Generala

Un port scanner este o unealtă sau aplicație de software specializată, concepută pentru a analiza și identifica porturile deschise sau disponibile pe o gazdă sau un server într-o rețea de calculatoare.

Această tehnologie esențială servește la o varietate de scopuri, de la securitate cibernetică la administrarea rețelelor și depanarea sistemelor.

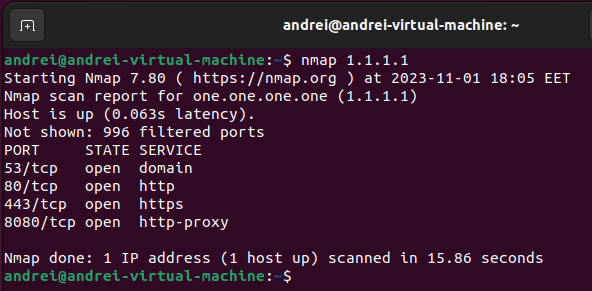
## Utilizări Comune ale Scanerelor de Porturi

* Securitate Cibernetică: Profesioniștii în securitate cibernetică utilizează scanerele de porturi pentru a identifica eventuale vulnerabilități în rețelele și sistemele informatice. Prin identificarea porturilor deschise și serviciilor care rulează pe acestea, se pot evalua potențialele amenințări și riscuri de securitate.
* Administrarea Rețelelor: Scanerele de porturi pot fi folosite de administratorii de rețea pentru a monitoriza starea rețelei și a dispozitivelor conectate. Acest lucru ajută la depistarea problemelor și la asigurarea funcționării corespunzătoare a serviciilor.
* Testarea Retelelor: Echipele de testare a securitatii folosesc scanerele de porturi pentru a evalua securitatea unei rețele sau a unui sistem prin identificarea potențialelor puncte slabe care pot fi exploatate de atacatori.
* Depanare: Scanerele de porturi pot fi utile în procesul de depanare, ajutând la identificarea problemelor de conectivitate și a erorilor de rețea prin detectarea porturilor care nu răspund sau care sunt închise necorespunzător.

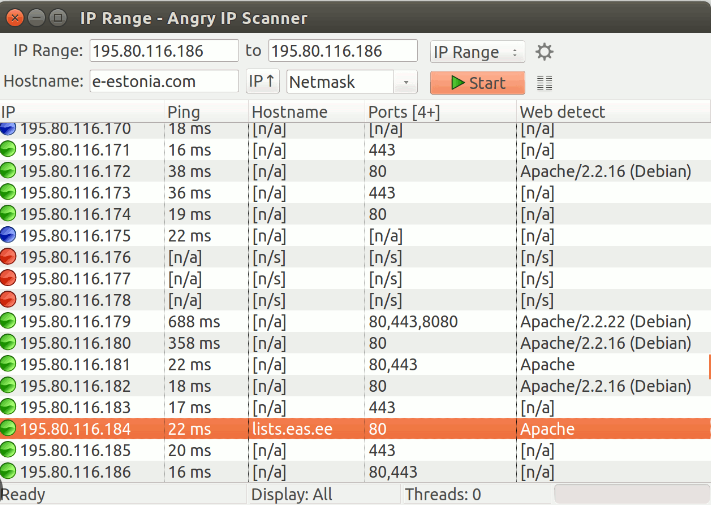
## 1.2 Scannere de Porturi Consacrate

Există mai multe scanere de porturi consacrate și recunoscute în industrie, care sunt utilizate pe scară largă în domeniul securității cibernetice și administrării rețelelor.

* Nmap (Network Mapper): Nmap este unul dintre cele mai cunoscute și puternice scanere de porturi. Acesta oferă o gamă variată de funcționalități, inclusiv scanări de porturi, recunoaștere de servicii, detectare de vulnerabilități și mai mult. Este disponibil pentru diverse platforme și este adesea folosit în testele de securitate.



* Angry IP Scanner: Angry IP Scanner este o aplicație simplă și ușor de utilizat, potrivită pentru scanări rapide ale porturilor. Acesta oferă o interfață prietenoasă pentru utilizator și funcționalități de bază pentru a identifica porturile deschise



* Masscan: Masscan este un scaner de porturi de înaltă viteză, specializat în scanări rapide ale rețelelor. Este cunoscut pentru performanța sa și este folosit în principal în testele de penetrare pentru identificarea rapidă a porturilor deschise.
* ZENMAP: Acesta este un frontend grafic pentru Nmap, care face utilizarea Nmap mai accesibilă pentru utilizatorii care preferă o interfață utilizator prietenoasă. Cu ZENMAP, puteți efectua scanări de porturi și analiza rezultatele într-un mod mai intuitiv.

# 

# 2.Notiuni Teoretice

Această aplicație se concentrează pe porturile de rețea (network ports), care joacă un rol vital în gestionarea cererilor de intrare și ieșire pe un canal fizic conectat la rețea.

Sistemul de operare atribuie fiecărei cereri (request) un număr de port pentru a facilita gestionarea lor. Un număr de port poate varia între 0 și 65535 (2 la puterea 16).

Există porturi implicite, cum ar fi portul 21 pentru protocolul FTP sau portul 80 pentru HTTP. Acestea se numesc "porturi well-known" și au valori cuprinse între 0 și 1023. Porturile din intervalul 1024 până la 49151 sunt cunoscute drept "porturi înregistrate" (registered) și pot fi alocate de către IANA (Internet Assigned Numbers Authority) pentru servicii specifice, la cerere. Porturile din intervalul 49152 până la 65535 sunt considerate "porturi dinamice" și pot fi utilizate de către orice tip de serviciu.

Este important de menționat că un port este întotdeauna asociat cu un protocol specific. Portul este specificat după adresa IP sau numele domeniului, urmat de două puncte.

Un port poate fi în mod activ în "ascultare" (listening port) pentru trafic de rețea, așteptând cereri de conexiuni de intrare pe acel port specific.

Scanarea porturilor dintr-o rețea este o metodă utilizată pentru a identifica porturile deschise și pentru a determina dacă acestea permit transmiterea sau primirea de pachete în rețea. Această metodă implică, de asemenea, trimiterea de pachete pe porturi specifice pentru a observa răspunsurile primite și pentru a identifica eventualele vulnerabilități. Protocolurile folosite pentru scanarea de porturi sunt TCP și UDP.

# Structura Aplicatiei

Pentru proiectul meu am ales să folosesc limbajul de programare C și compilatorul GCC (GNU Compiler Collection).

Această alegere s-a bazat pe multiple motive, care definesc atât direcția proiectului, cât și rezultatele pe care le urmăream să le obțin.

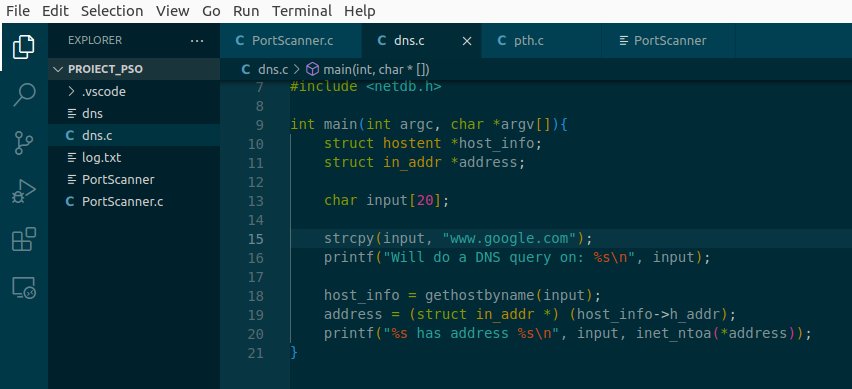
În primul rând, limbajul C este cunoscut pentru performanța sa remarcabilă și controlul precis asupra resurselor hardware. Acest lucru este de o importanță critică pentru un scaner de porturi, deoarece necesită manipularea conexiunilor și a porturilor într-un mod eficient și precis.

În plus, am avut nevoie de facilități solide pentru lucru cu socket-uri și funcționalități de rețea, pentru a construi și gestiona conexiunile și pentru a realiza scanarea porturilor.

Pentru a implementa multiprocesarea, am folosit biblioteca de fire POSIX (Pthreads) disponibilă în C. Am creat fire separate pentru a efectua scanarea porturilor și am gestionat comunicarea și sincronizarea între acestea.

Utilizarea firelor a adus un avantaj semnificativ în ceea ce privește performanța și eficiența proiectului meu de scaner de porturi. Aceasta a permis scanarea rapidă și paralelă a unui mare număr de porturi.

Un port scanner este o aplicație care explorează o adresă IP sau un domeniu pentru a identifica porturile deschise și serviciile care rulează pe acestea. Din aceasta cauza este nevoie de o componenta care sa traduca numele de domenii in adrese IP. Acest lucru se efectueaza cu ajutorul serverului DNS.



Rezultatul:

# 

# Teste Functionalitati Actuale

# Scanare Normala

* Argc =2

În acest mod, aplicația este destinată scanării porturilor pentru un singur IP specificat în linia de comandă.

Se afișează un mesaj care indică intervalul de porturi care urmează a fi scanate (de la 0 la NUM\_THREADS \* PORTS\_PER\_THREAD) pentru IP-ul specificat.

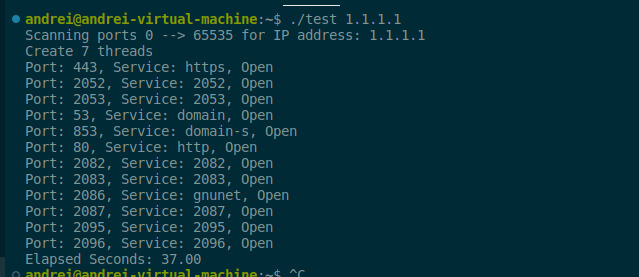
Aplicația creează NUM\_THREADS fire de execuție, fiecare fir de execuție fiind responsabil de scanarea unui interval de porturi.

Fiecare fir de execuție utilizează funcția scanPort pentru a încerca să stabilească o conexiune la fiecare port în intervalul specificat.

Dacă o conexiune este stabilită cu succes, aplicația indică că portul este deschis și afișează informații despre port (numărul portului și serviciul asociat).

Apoi, conexiunea este închisă, și firul de execuție se termină.

După ce toate firele de execuție au terminat scanarea, aplicația afișează timpul total petrecut pentru scanare.



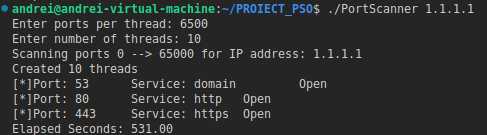
# Scanarea implicita

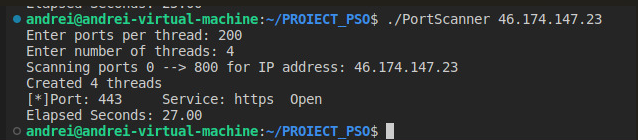
# În implementarea implicită a scanării porturilor, programatorul este solicitat să introducă doi parametri esențiali: numărul de porturi ce vor fi scanate în cadrul unui singur fir de execuție și numărul total de fire de execuție ce vor fi create. Acestă configurație va dicta domeniul porturilor care vor fi supuse scanării.

# Scanarea propriu-zisă se va realiza asupra intervalului de porturi cuprins între 1 și NUM\_THREADS \* PORTS\_PER\_THREAD. Fiecare fir de execuție va emite informații în terminal cu privire la descoperirea unui port deschis în timpul procesului de scanare.

# Cu scopul de a optimiza viteza scannerului, un mecanism de gestionare a timpului de așteptare pentru răspuns a fost implementat. Această abordare are ca obiectiv minimizarea timpului total necesar scanării, oferind în același timp eficiență în identificarea porturilor deschise.

Exemple:

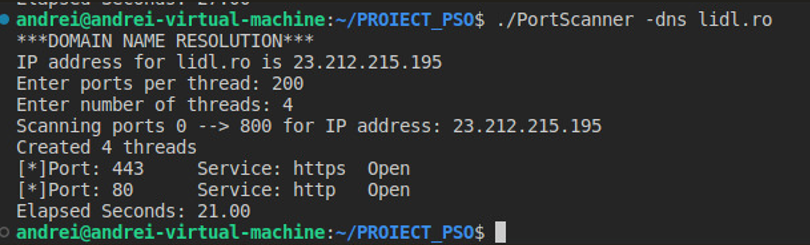




# Scanarea domeniului

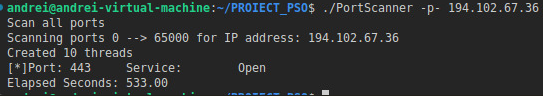
Segmentul de cod se ocupă de rezolvarea numelui de domeniu la adresa IP. Procesul începe cu afișarea unui mesaj de notificare și apoi se alocă dinamic spațiu pentru o copie a numelui de domeniu. După copierea numelui de domeniu în spațiul alocat, se efectuează rezolvarea propriu-zisă a numelui de domeniu la adresa IP.

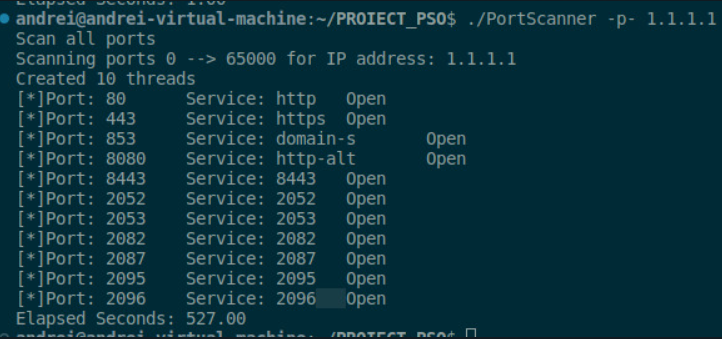
Dacă rezolvarea este reușită, se afișează adresa IP și se apelează o funcție principală (mainFunction) cu adresa IP rezolvată. În caz de eșec al rezolvării, se afișează un mesaj de eroare.



# Scanarea tuturor porturilor

Scaneaza toate porturile unei retele. Creeaza 10 fire de executie in care aloca cate 6500 de porturi, ultimul avand sansa sa le scaneze pe toate. Acest proces este costisitor si poate dura mult timp, este echivalentul ***nmap –p-*** .

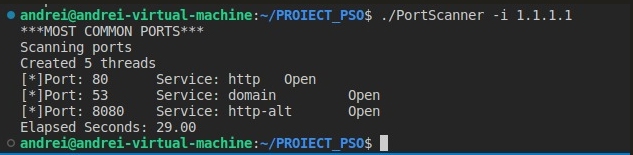




# Scanarea porturilor importante

Similar funcționării implicite a instrumentului nmap, utilizarea opțiunii -i în cadrul proiectului curent va implica scanarea celor mai semnificative 1002 de porturi, alegere determinată de echipa de dezvoltare a nmap. În cadrul acestei abordări, se vor aloca cinci fire de execuție, fiecare responsabil cu scanarea a 200 de porturi, având în vedere vectorul predefinit de porturi relevante, MOST\_COMMON\_PORTS\_1002.

Acest set de porturi a fost selecționat pentru a reflecta importanța lor în contextul securității și funcționării generale a rețelelor informatice.



# Scanarea celor mai importante porturi ale unui domeniu

Analog cu funcționarea implicită a nmap, condiția specificată în codul furnizat are ca scop scanarea celor mai semnificative 1002 de porturi. Această condiție este activată atunci când opțiunile din linia de comandă corespund cu -dns și -i în oricare ordine. Mai explicit, dacă primul argument este -dns și al doilea argument este -i, sau dacă ordinea acestora este inversată, atunci se inițiază un proces de rezolvare a numelui de domeniu la adresa IP, urmat de scanarea celor mai frecvent utilizate 1002 de porturi.

