Folosirea tool-urilor Nmap si Wireshark

Studenta:Podeanu Stefania Adriana

Nmap

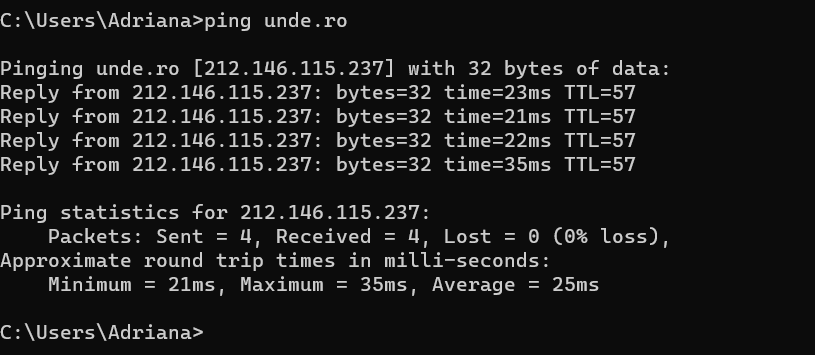
Nmap este un tool gratuit pentru a putea scana traficul de pe o retea, hosturile logate la aceasta .Este capabila sa colecteze informatii si sa detecteze vulerabiltatile dintr-o retea.

Acesta se bazeaza pr scanarea fiecarei adrese IP din retea si detalierea informatiilor despre aceasta astfel incat se poate determina cand aceasta este compromisa .

De asemenea identifica vulnerabilitatile unui server web si poate crea o harta digitala pentru o folosire mai usoara si facila pentru a raporta eventualele probleme intalnite pe parcursul trimiterii pachetelor catre un alt utilizator.

Pasi de utilizare nmap:

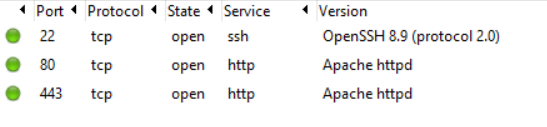
1. Am intrat in cmd si am scris comanda ping pentru a afla adresa ip a unui site oarecare, am folosit pentru primul exemplu site-ul unde.ro.



1. Odata aflata adresa ip, cu ajutorul aplicatiei Nmap am scanat traficul de pe reteaua acestei adresa ca sa putem vedea si utilizatorii logati/porturile si protocoalele folosite:



Exemple de porturi deschise pentru adresa ip: 192.168.1.1



TCP (protocol de control al transmisiei) este un protocol folosit pentru transmiterea datelor care au nevoie de confirmare de primire.Acest protocol asigura livrarea ordonata a unui flux de octeti de la un program.

HTTPeste un protocol folosit pentru traficul web.

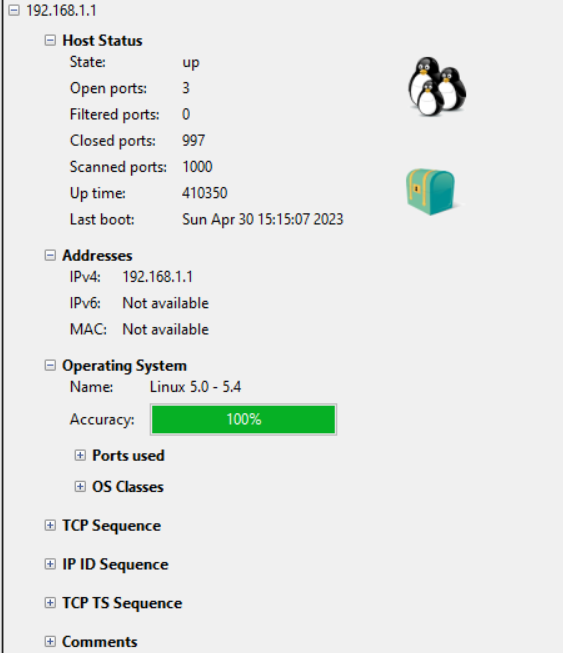
**DNS** este un system distribuit de nume utilizat pentru identificarea calculatoarelor din Internet.

**ICMP** este un protocol din suita TCP/IP care foloseste semnalizarea si diagnosticarea problemelor din retea.

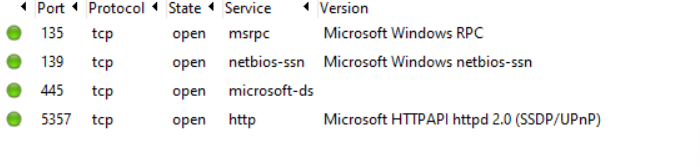
Pentru serviciul de **SSH** care are la baza protocolul **TCP** s-au implement serviciile de catre **OpenSSH** s-a folosit portul 22.

Iar serviciul de **HTTP** a fost implementat de catre Apache httpd folosind protocolul **TCP** ambele avand porturile deschise s-au folosit porturile 80 si 443.

Observam ca pentru adresa de mai sus host-ul are sistemul de operare Linux:

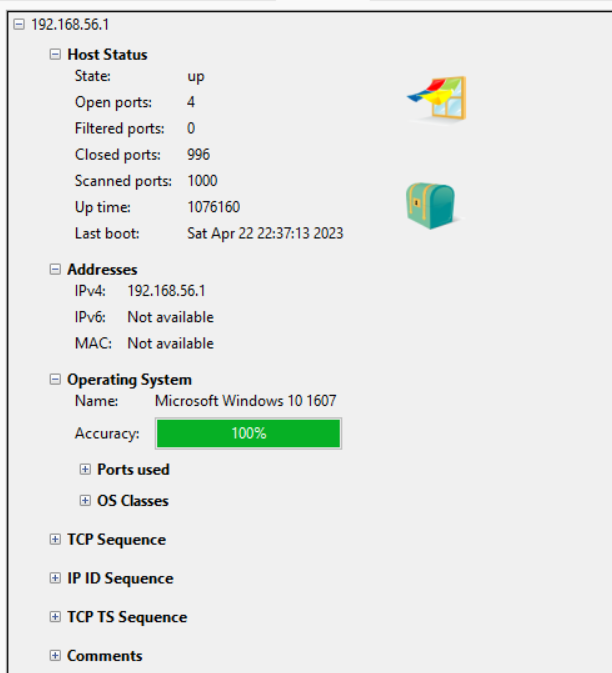


Exemple de porturi deschise pentru adresa IP: 192.168.56.1

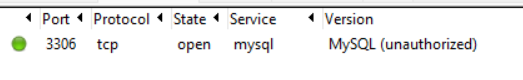


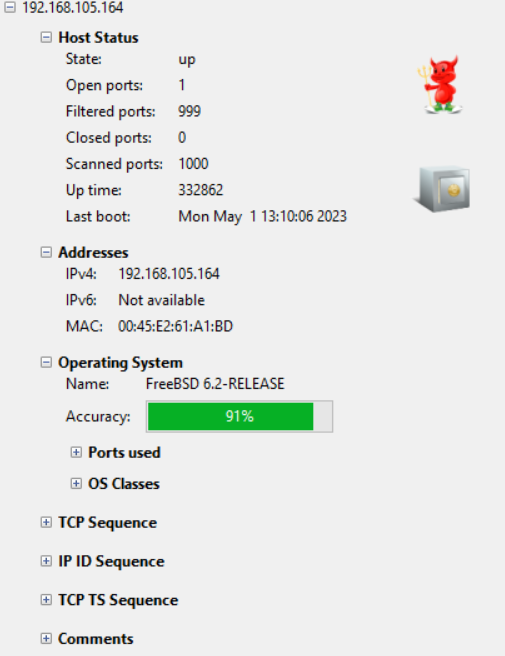
S-a folosit protocolul tcp pentru toate serviciile porturilor deschise din imaginea anterioara(135,139,445, 5357).De asemenea exista unele diferente deoarece fiecarui port ii corespunde un serviciu specific de exemplu:msrpc,netbios-ssn oferite de Microsoft Windows.

Pentru aceasta adresa IP hostul foloseste sistemul de operare:Microsoft Windows 10 .



Pentru adresa: 192.168.105.164 protocolul folosit este TCP pe portul deschis 3306 si ofera serviciul de mysql implementat de MYSQL, sistemul de operare al acestui host este FreeBSD 6.2-RELESE



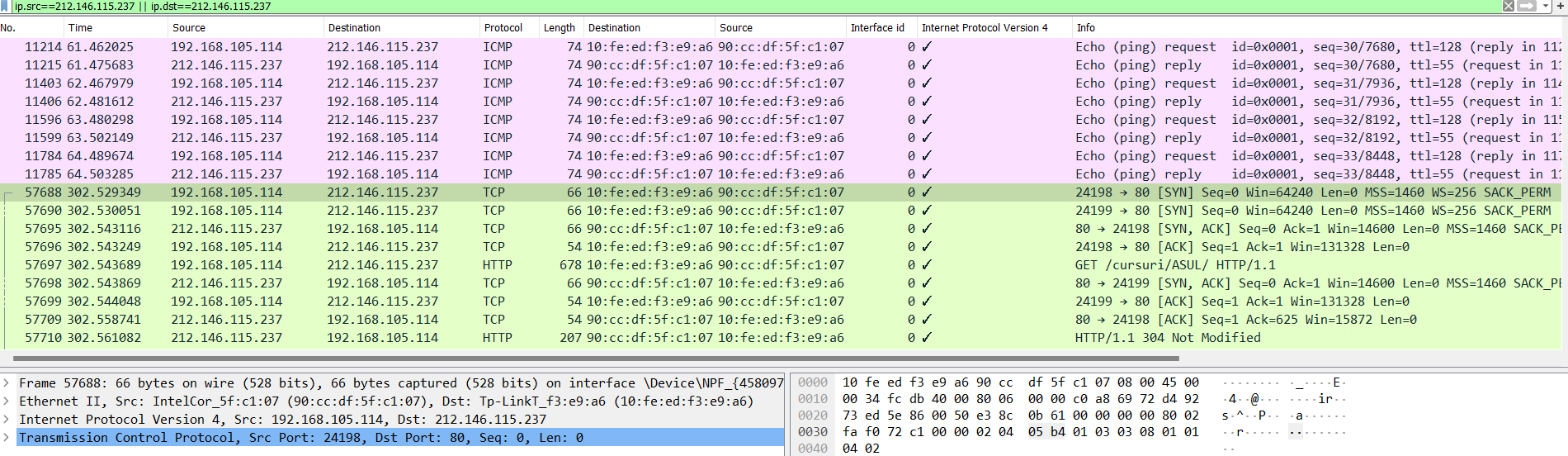


Pentru adresa: protocolul folosit

Wireshark

Wireshark este cel mai cunoscut sniffer de retea. Acesta ajuta la gasirea pachetelor transmise in retea de la un calculator catre un server sau un alt utilizator.Wireshark poate fi utilizat pentru a asculta tipul de conexiune in timp real si poate o crea o schema specifica de trafic a pachetelor pe retea.

O alta utilitate a acestui tool o reprezinta filtrarea pachetelor folosind diverse filtre alese de catre utilizator.



In imaginea de mai sus se observa una din caracteristicile principale ale acestei aplicatii si anume filtrarea traficului pe retea care contine atat adresa sursa cat si adresa destinatie ip-ul: 212.106.115.237.

Odata pus acest filtru se poate vedea ca majoritatea protocoalelor folosite in prima parte sunt de tip ICMP in care cu ajutorul comenzii ping se fac diverse request-uri si replay-uri pentru conexiunea la server.

O data stabilita conexiunea intre cele doua device-uri, informatia este transferata catre nivelul transport iar acesta le directioneaza mai departe sub forma de pachete .Pentru a se putea realiza aceasta comunicare se foloseste o metoda denumita Positive Acknowledgement with Re- transmission (PAR).

Unitatea de date folosita intr-un protocol se numeste segment care utilizeaza metoda Positive Acknowledgement with Re- transmission (PAR) care verifica daca segmentul este deteriorat atunci cand acesta se primeste. Tot acest proces are la baza sa trei segmente principale denumite SYN, ACK si FIN.

Dupa ce a fost stabilita conexiunea se incearca o conectare asa ca se trimite un request de tip SYN(Synchronize Sequence Number), iar raspunsul este primit sub forma unui ACK(Acknowledgement) care cere informatie despre conectarea la server prin introducerea utilizatorului si a parolei.

Datele sunt preluate prin metoda get si se stabileste conexiunea cu site-ul unde.ro.

Ca sa se incheie sesiunea de transmitere de segmente se foloseste FIN.