Laborator 3
Faza de Recunoaștere - Enumerare Resurse și Infrastructură (footprinting)

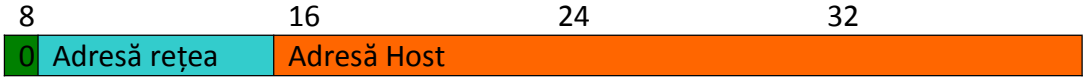
1. Reamintire adresare în Internet

Din categoria "prietenii știu de ce ..." am ajuns la concluzia că ar trebui să se facă o scurtă recapitulare a unor noțiuni precursoare pentru acestă materie.

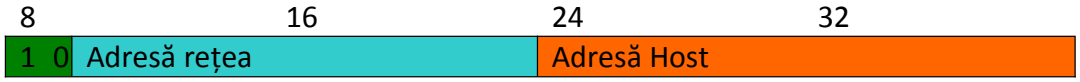
1.1. Numerotare stații în rețea

Identificarea gazdelor în Internet se face prin rezervarea unei adrese pentru fiecare, numită adresă Internet sau adresă IP. Adresele IP au o lungime de 32 biți care este împărțită într-o parte de rețea și o parte de host. Această împărțire a dus la formarea a cinci clase de adrese.

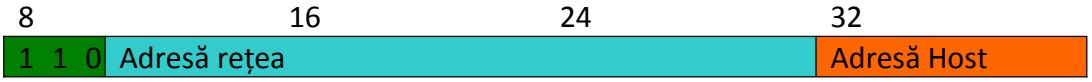
Clasa A are 7 biți pentru adresa de rețea și 24 de biți pentru adresa de host. Cel mai semnificativ bit are valoarea 0. Sunt posibile 128 de rețele de clasă A.



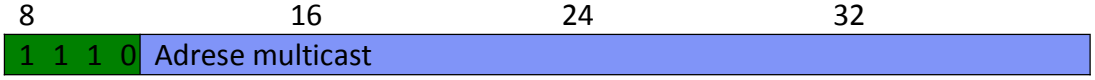
Clasa B are 14 biți pentru adresa de rețea și 16 biți pentru adresa de host. Cei mai semnificativi biți au valoarea 10. Sunt posibile 16.384 rețele de clasă B.



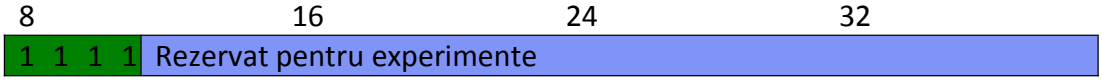
Clasa C are 21 de biți pentru adresa de rețea și 8 biți pentru adresa de host. Cei mai semnificativi 3 biți au valoarea 110. Sunt posibile 2.097.152 rețele de clasă C.



Clasa D este folosită pentru adrese de multicast. Cei mai semnificativi 4 biți au valoarea 1110.



Clasa E este rezervată pentru experimente. Cei mai semnificativi 4 biți au valoarea 1111.



O notație uzuală pentru adresele IP împarte cei 32 de biți în patru grupuri a câte 8 biți și fiecare grup este specificat prin corespondentul numeric zecimal, fiecare grup fiind separat prin punct. Aceasta este numită notația zecimală cu punct.

Adrese speciale

Adresa unde toți biții de host sunt 0 reprezintă adresa rețelei.
Adresa unde toți biții de host sunt 1 reprezintă adresa de rutare.
Adresa 0.0.0.0 reprezintă toate rețelele.
Adresa 127.0.0.1 reprezintă adresa interfeței de buclă locală.
Adresa 255.255.255.255 reprezintă adresa de rutare generală.

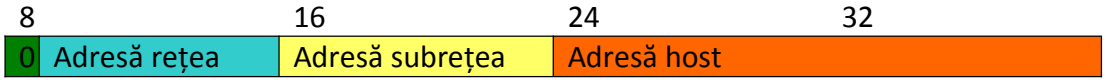
1.2. Subrețele

Din motive tehnice sau administrative, multe organizații au ales să împartă o rețea în mai multe Subrețele.
În aceste condiții, o adresă Internet poate fi interpretată astfel:

<adresă-rețea><adresă-subrețea><adresă-host>

unde *<adresă-host>* are cel puțin un bit, *<adresă-subrețea>* are lungime constantă pentru o rețea dată iar *<adresă-rețea>* este adresa de rețea corespunzătoare claselor A, B sau C. Dacă lungimea câmpului *<adresă-subrețea>* este 0 atunci rețeaua nu este împărțită în Subrețele.

Un exemplu de împărțire a unei rețele de clasă A cu o lungime a câmpului subrețea de 8 ar arăta astfel:



Din motive de simplitate și implementare eficientă, s-a considerat la un moment dat că cele mai multe organizații vor folosi o lungime a câmpului subrețea multiplu de 8. Totuși, o implementare care să suporte lungime variabilă trebuia să fie pregătită.

Pentru a suporta Subrețele, este necesar să se fie folosită încă o cantitate de 32 biți numită mască de rețea. Aceasta este o mască de biți cu biții setați în câmpurile corespunzătoare adresei de rețea și de subrețea. De exemplu, la o rețea de clasă A cu 8 biți pentru câmpul subrețea, masca de rețea ar fi 255.255.0.0.

1.3. Subrețelele și rutarea

În absența subrețelelor, există numai două tipuri posibile de rutare în IP:

- rutare către toate gazdele unei rețele specifice sau
- rutare către toate gazdele din orice rețea. Ultimul tip de rutare este folosit atunci când o gazdă nu știe în ce rețea se află.

Când sunt folosite Subrețele, situația devine puțin mai complicată. În primul rând, există posibilitatea de rutare către o subrețea specifică. În al doilea rând, rutarea către toate gazdele dintr-o rețea împărțită în Subrețele necesită mecanisme suplimentare. În fine, rutarea către toate gazdele din orice rețea trebuie interpretată ca rutare ca fiind rutare doar în interiorul rețelei originale.

Implementările trebuie deci să recunoască trei tipuri de adrese de rutare, pe lângă propriile lor adrese de host:

- *rețeaua fizică* – o adresă destinație cu toți biții de 1 (255.255.255.255) înseamnă o datagramă transmisă prin rutare în rețeaua fizică; această datagramă nu trebuie înaintată de nicio poartă;
- *rețea specifică* – adresa destinație conține o adresă de rețea validă; adresa de host are toți biții 1 (de exemplu: 36.255.255.255);
- *subrețea specifică* – adresa destinație conține o adresă de rețea validă și o adresă de *subrețea validă* unde adresa de host are toți biții 1 (de exemplu: 36.40.255.255).

1.4. Rezervarea adreselor pentru rețele private

Gazdele din organizații care utilizează IP pot fi împărțite în trei categorii:

1. gazde care nu necesită acces la gazde din alte organizații sau la Internet;
2. gazde care necesită acces la un set limitat de servicii (e-mail, FTP, etc.) care pot fi asigurate de porți la nivel de aplicație;
3. gazde care necesită acces la nivel rețea în afara organizației;

Gazdele din prima categorie pot utiliza adrese IP care nu sunt ambigue în interiorul organizației dar pot fi ambigue între organizații.

Pentru multe gazde din categoria a doua un acces extern nerestricționat poate fi nedorit din motive de securitate. Numai gazdele din categoria a treia necesită adrese IP care nu sunt ambigue la nivel global.

Multe aplicații necesită conectivitate numai în interiorul organizației și nu au nevoie de conectivitate externă pentru majoritatea gazdelor interne. În organizații foarte mari este adesea ușor de identificat un număr substanțial de gazde care folosesc TCP/IP și nu au nevoie de conectivitate externă.

Autoritatea pentru atribuirea numerelor Internet (IANA) a rezervat următoarele trei blocuri ale spațiului de adresare IP pentru rețele private:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Se va utiliza o terminologie de tipul primul bloc ca „blocul de 24 de biți", la al doilea ca „blocul de 20 de biți" și la al treilea ca „blocul de 16 biți". Primul bloc este un singur număr de clasă A în timp ce al doilea bloc este un set de 16 numere continue de clasă B și al treilea bloc este un set de 255 de numere continue de clasă C.

O organizație care decide să utilizeze adrese IP din spațiul de adresare definit în acest document poate să o facă fără niciun fel de coordonare cu IANA sau alte autorități de atribuire din Internet. spațiul de adresare poate fi deci utilizat de mai multe organizații. Adresele din spațiul de adresare privat vor fi unice doar în interiorul organizației respective.

Orice organizație care are nevoie de adrese unice la nivel global trebuie să le obțină de la o autoritate de atribuire din Internet. Unei organizații care necesită adrese IP pentru conectivitate externă nu i se va atribui niciodată adrese din spațiul de adresare privată.

Pentru a utiliza adrese private, o organizație trebuie să determine ce gazde nu au nevoie de conectivitate externă în viitorul apropiat. Asemenea gazde vor fi denumite gazde private și vor utiliza spațiul de adresare privată definit în acest document. Gazdele private pot comunica cu toate celelalte gazde din interiorul organizației, publice sau private. În orice caz ele nu pot avea conectivitate IP cu gazde externe.

Toate celelalte gazde vor fi denumite publice și vor utiliza adrese unice globale. Gazdele publice pot comunica cu alte gazde în interiorul organizației, fie ele publice sau private și pot avea conectivitate IP cu gazde publice externe. Gazdele publice nu pot avea conectivitate cu gazde private aparținând altor organizații. Schimbarea unei gazde din publică în privată sau invers implică o schimbare de adresă IP.

Deoarece adresele private nu au însemnătate la nivel global, informațiile de rutare despre rețelele private nu vor trebui propagate pe legăturile dintre organizații iar pachetele cu adresa sursă și adresa destinație private nu trebuie comutate pe asemenea legături.

Ruterele din rețele care nu folosesc spațiul de adresare privată, în special cele ale furnizorilor de Internet, trebuie configurate să respingă (să filtreze) informațiile de rutare cu privire la rețele private. Dacă un ruter primește astfel de informații, respingerea lor nu trebuie tratată ca o eroare a protocolului de rutare.

Referiri indirecte la asemenea adrese ar trebui să fie conținute în interiorul organizației. Exemple evidente de astfel de referiri sunt înregistrările de resursele DNS și alte informații referitoare la adresele private interne. În particular, furnizorii de servicii Internet trebuie să ia măsuri pentru a preveni scurgeri de acest fel.

2. *Protocolul Internet, versiunea 6*

IP versiunea 6 (IPv6) este succesoarea versiunii 4 (IPv4). Schimbările de la IPv4 la IPv6 se pot împărți în următoarele categorii:

1. Posibilități de extindere a spațiului de adresare - IPv6 mărește dimensiunea adresei IP de la 32 de biți la 128 de biți, pentru a suporta mai multe nivele de ierarhie a adresării, un număr mai mare de noduri adresabile și autoconfigurare simplă a adreselor.

2. Simplificarea formatului antetului - Câteva câmpuri ale antetului IPv4 au fost eliminate sau făcute opționale pentru a reduce costurile de procesare ale antetului și pentru a limita costul lățimii de bandă.
3. Suport îmbunătățit pentru extensii și opțiuni - Schimbările în modul de codificare a antetului IP permit o avansare mai eficientă, mai puține limite asupra lungimii opțiunilor și mai multă flexibilitate pentru introducerea unor noi opțiuni în viitor.
4. Posibilitatea de etichetare a traficului - O nouă posibilitate este adăugată pentru a permite etichetarea pachetelor aparținând unor fluxuri particulare de trafic pentru care emițătorul cere tratare specială, cum ar fi calitatea serviciilor non-default sau servicii de timp real.
5. Posibilități de autentificare și confidențialitate - În IPv6 au fost specificate extensii pentru a suporta autentificarea, integritatea datelor și (opțional) confidențialitatea datelor.

2.1. Adresarea IPv6

Adresele IPv6 sunt identificatori de 128 de biți pentru interfețe și seturi de interfețe. Există trei tipuri de adrese:

- Unicast – un identificator pentru o singură interfață. Un pachet trimis la o adresă unicast este livrat la interfața identificată de acea adresă.
- Anycast – un identificator pentru un set de interfețe (tipic aparținând unor noduri diferite). Un pachet trimis la o adresă anycast este livrat la una din interfețele identificate de acea adresă (cea mai apropiată, în concordanță cu distanța măsurată de protocolul de rutare).
- Multicast – un identificator pentru un set de interfețe (tipic aparținând unor noduri diferite). Un pachet trimis la o adresă multicast este livrat tuturor interfețelor identificate de acea adresă.

Nu există adrese de broadcast în IPv6, funcționalitatea lor fiind înlocuită cu adresele de multicast.

Toate valorile de zero și de unu sunt legale pentru orice câmp, doar dacă sunt excluse în mod specific.

Adresele IPv6 de toate tipurile sunt atribuite interfețelor, nu nodurilor. Din moment ce fiecare interfață aparține unui singur nod, oricare din adresele unicast ale interfețelor acelui nod pot fi utilizate ca un identificator pentru nodul respectiv.

O adresă unicast IPv6 se referă la o singură interfață.

Există trei forme convenționale pentru reprezentarea adreselor IPv6 ca șiruri de text:

1. Forma preferată este **x:x:x:x:x:x:x:x**, unde fiecare „x” reprezintă o valoare hexazecimală de 16 biți. Exemple:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

De notat că nu este necesar a se scrie zerourile care prefixează un câmp individual, dar trebuie să fie cel puțin o valoare numerică în fiecare câmp (cu excepția cazului descris la punctul 2).

2. Datorită metodei de rezervare a unor stiluri de adrese IPv6, va fi normal ca adresele să conțină șiruri lungi de biți de zero. Pentru a face scrierea adreselor ce conțin biți de zero mai ușoară, o sintaxă specială este disponibilă pentru a comprima zerourile. Semnul „::” indică grupuri multiple de 16 biți ce conțin zerouri. Acest semn poate apărea doar o dată într-o adresă. De asemenea poate fi folosit pentru a comprima zerourile de început sau de sfârșit dintr-o adresă. De exemplu următoarele adrese:

1080:0:0:0:8:800:200C:417A – o adresă de unicast
FF01:0:0:0:0:0:0:43 – o adresă de multicast
0:0:0:0:0:0:0:1 – adresă de loopback

0:0:0:0:0:0:0:0 – adresă nespecificată

pot fi reprezentate ca:

1080::8:800:200C:417A

FF01::43

::1

::

3. O formă alternativă care este câteodată mai convenabilă când avem de-a face cu un mediu mixt ce conține noduri IPv4 și IPv6 este x:x:x:x:x:x:d.d.d.d, unde „x" reprezintă valorile hexazecimale ale primelor 6 câmpuri de câte 16 biți iar „d" reprezintă valorile zecimale ale ultimelor 4 câmpuri de câte 8 biți. Exemple:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

sau în forma comprimată:

::13.1.68.3

::FFFF:129.144.52.38

Tipul specific al unei adrese IPv6 este indicat de primii biți ai acesteia. Câmpul de lungime variabilă ce cuprinde acești biți este denumit prefix de format.

Pentru început jucați-vă cu arping de Thomas Habets, (trebuie să-l aduceți, compilați și instalați și pe stațiile din laborator.

Deoarece am văzut laboratorul trecut că documentația de nmap se pare că este prea stufoasă aveți un rezumat și câteva exemple ca să fiu sigur că îl puteți utiliza pentru RedBlue.

3. NMAP

Nmap („Network Mapper") este utilizat pentru explorarea rețelei și audit de securitate

Tot ceea ce nu este o opțiune (sau argument al ei) în linia de comandă a Nmap este tratat ca o specificare a unei ținte. Cel mai simplu caz este specificarea adresei IP sau a numelui calculatorului care urmează a fi scanat. Dacă se dorește scanarea completă a unei rețele pentru calculatoare adiacente.

De exemplu, *192.168.10.0/24* va scana cele 256 de calculatoare între

192.168.10.0 și *192.168.10.255*

11000000 10101000 00001010 00000000 și 11000000 10101000 00001010 11111111

Dat fiind numele *www.xxx.xxx* cu adresa IP *205.217.153.62*, specificația *www.xxx.xxx/16* va scana cele 65.536 adrese IP între *205.217.0.0* și *205.217.255.255*.

Cea mai mică valoare permisă este /1, care va scana jumătate din adresele IPv4 din Internet. Cea mai mare este 32, care va scana doar calculatorul specificat prin nume sau IP deoarece toți biții sunt fixați.

-iL <fisierdeintrare>(Preluare dintr-un fișier)

Citește specificațiile țintelor din fișierul de intrare. Serverul DHCP poate exporta o listă de 10.000 de IP pe care le-a atribuit.

-iR <număr de tinte>(Alegere de tinte aleatoare)

Numarul de ținte comunica Nmapului cate ținte aleatoare sa genereze.

-exclude<host1[,host2][,host3],...>(Se exclud de la scanare calculatoarele/rețelele specificate ca argument)

-excludefile <fișier_de_excludere>(listă de excludere dintr-un fișier)

3.1 Descoperirea gazdelor

Este adesea numită scanare ping, dar trece cu mult de simplul stadiu al pachetelor ICMP care solicita un răspuns asociate unui ping.

Utilizatorii pot trece de pasul care implică ping-ul cu o scanare de tip listă (-sL) sau dezactivând ping-ul (-P0), sau angrenând alte combinații arbitrare de probe multiport TCP SYN/ACK, UDP și ICMP.

Scopul acestor teste este sa solicite răspunsuri care sa demonstreze dacă o adresa IP este cu adevărat activa (este folosita de un dispozitiv din rețea).

Dacă nu sunt furnizate opțiuni de descoperire a gazdelor, Nmap trimite un pachet TCP ACK destinat portului 80 și un pachet de interogare ICMP cu solicitare de răspuns la fiecare mașină țintă.

O excepție la acestea este ca scanarea ARP este folosita pentru orice țintă dintr-o rețea locală. Pentru utilizatori neprivilegiați cu conturi shell pe sisteme UNIX, sunt trimise pachete SYN în locul celor ack folosind apelul de sistemconnect().

Opțiunea -P* (care selectează tipul ping-ului) poate fi combinată.

Se pot mari șansele de penetrare a unor firewall-uri stricte trimițând mai multe probe folosind diferite porturi/flaguri (indicatori din pachetele) TCP și coduri ICMP.

Descoperirea **ARP (-PR)** este executata implicit împotriva țintelor dintr-o rețea locala chiar dacă se specifica alta opțiune-P*, deoarece este aproape întotdeauna mai rapida și mai eficienta.

-sL(Scanarea de tip lista)

Scanarea de tip listă este o forma degenerată de descoperire a gazdelor care listează fiecare host al rețelei specificate, fără a trimite nici un pachet țintelor.

în mod implicit, Nmap realizează totuși o rezoluție inversa DNS pentru a afla și numele țintelor.

??? - informații utile ne pot oferi simplele nume ale gazdelor.

-sP(Scanare ping)

Aceasta opțiune spune Nmapului sa realizeze numai o scanare ping (descoperirea gazdelor) și apoi să afișeze hosturile disponibile care răspund la scanare.

Acest pas este mai intruziv decât scanarea de tip listă și poate fi folosita adesea în același scop. Permite o descoperire a țintelor din rețea fără a atrage prea mult atenția.

Cunoscând câte gazde sunt active este o informație mult mai valoroasa unui atacator decât simpla listă furnizată de scanarea de tip listă a fiecărei adrese IP și a numelor gazdelor.

Opțiunea **–sP** trimite un pachet ICMP cu solicitare de răspuns și un pachet TCP la portul 80 în mod implicit. Când se executa de către un utilizator neprivilegiat, un pachet SYN este trimis la portul 80 al țintei. Când un utilizator privilegiat încearcă sa scaneze ținte dintr-o rețea locala, solicitări ARP (-PR) sunt utilizate, doar dacă

-send-ip(adresa IP de expediere) a fost specificat.

-P0(fără ping)

Aceasta opțiune nu mai realizează faza de descoperire.

Implicit, Nmap realizează scanarea avansată cum ar fi scanarea de porturi, detecția versiunii și a sistemului de operare doar pentru hosturile găsite active.

Dezactivarea descoperirii gazdelor cu -P0 face ca Nmap sa încerce tehnicile avansate de scanare pentru fiecare adresa IP specificata ca țintă.

-PS [listadeporturi](Ping TCP SYN)

Aceasta opțiune trimite un pachet TCP gol cu flagul SYN setat. Portul de destinație implicit este 80 dar un alt port poate fi specificat ca parametru.

Chiar o listă separată prin virgula de porturi poate fi specificată (de exemplu-PS22,23,25,80,113,1050,35000),caz în care pachetele de test vor fi trimise la fiecare port în paralel.

Flagul SYN sugerează țintei ca dorim sa stabilim o conexiune. în mod normal portul destinație va fi închis și un pachet RST (de resetare) este trimis înapoi.
dacă se întâmplă ca portul sa fie deschis, țintă va face cel de-al doilea pas dintr-un protocol în trei pași) răspunzând cu un pachet TCP SYN/ACK.

-PA [lista_de_porturi](Ping TCP ACK)

ping-ul TCP ACK este similar cu ping SYN.
Un pachet ACK pretinde ca transporta date în cadrul unei conexiuni ACK deja stabilite, dar nu exista nici o astfel de conexiune.
Așadar țintele trebuie sa răspundă întotdeauna cu un pachet RST, dezvăluindu-și existenta în cadrul acestui proces.
Opțiunea –PA folosește același port implicit ca probele SYN și de asemenea poate prelua o listă de porturi destinație în același format.

-PU [lista_de_porturi](Ping UDP)

Alta opțiune de descoperire a gazdelor este ping-ul UDP, care trimite un pachet gol (doar dacă optiunea--data-lengthnu este specificata) UDP la portul specificat.
listă de porturi are același format cu cel discutat anterior la opțiunile-PS și –PA (implicit portul 31338).
După trimiterea pachetului de test către un port închis al țintei, trebuie sa se obțină un pachet ICMP de port indisponibil.
Acest lucru semnalizează Nmapul ca mașină este activa și disponibila.

-PE;-PP;-PM(Tipuri de ping ICMP)

Nmap poate trimite pachete standard ICMP de tipul 8 (solicitare de răspuns) către adresa IP țintă, așteptând un pachet de tip 0 (răspuns) în schimb de la hosturile disponibile.
multe gazde și firewall-uri blochează aceste pachete, în loc sa răspundă în conformitate cuRFC1122.
Standardul ICMP (RFC792) specifică de asemenea solicitarea amprentei de timp, a informațiilor și a măștii de rețea corespunzătoare codurilor 13,15 și 17.
Solicitările de amprenta de timp și masca de rețea pot fi trimise cu ajutorul optiunilor-PP, respectiv-PM.
Un răspuns amprenta de timp (ICMP cod 14) sau un răspuns masca de rețea (cod 18) dezvăluie un host disponibil.

-PR(Ping ARP)

Unul dintre cele mai comune scenarii de utilizare ale Nmap-ului o reprezintă scanarea unei întregi rețele locale (LAN).
în multe LAN-uri, în special în cele care folosesc spațiul privat de adrese specificat în RFC1918, mare majoritate a adreselor IP nu sunt utilizate la un moment dat.
Dacă primește un răspuns, Nmap nici nu mai ia în în considerare ping-urile bazate pe IP din moment ce știe deja ca hostul este activ.
Acest lucru face scanarea ARP mult mai rapida și mai corecta decât scanările bazate pe IP.

-n(Nu se realizează rezoluția DNS)

Transmite Nmap-ului ca niciodată sa nu realizeze rezoluția inversă DNS pentru IP-urile active găsite.
Din moment ce DNS este adesea lent, aceasta opțiune poate mari viteza de scanare.

-R(rezoluție DNS pentru toate țintele)

Transmite Nmapului ca întotdeauna să realizeze rezoluția DNS pentru IP-urile țintă.

3.2 Bazele scanării de porturi

Simpla comandă nmap țintă scanează mai mult de 1660 de porturi TCP ale țintei.
Nmap împarte porturile în sase stări:

- **open (deschis) -** O aplicație accept în mod activ conexiuni TCP sau pachete UDP la respectivul port.
- **closed (închis) -** Un port închis este accesibil (primește și răspunde la un pachet de proba trimis de Nmap), dar nu exista nici o aplicație care sa asculte la el. Pot fi folositoare în dezvăluirea stării hostului sau ca parte a detecției sistemului de operare.
- **filtered (filtrat)** Nmap nu poate determina dacă portul este deschis datorita unui filtru de pachete care împiedica pachetele sa ajungă la portul destinație. Filtrarea poate proveni de la un firewall dedicat, din regulile unui router sau dintr-un firewall software al țintei. Deoarece furnizează foarte puține informații Nmap va retrimite de câteva ori pachetele de test pentru cazul în care pachetul s-a pierdut din cauza congestionării rețelei și nu din cauza filtrării.â
- **unfiltered (nefiltrat) -** Starea nefiltrata înseamnă ca portul este accesibil, dar Nmap nu poate determina dacă portul este închis sau deschis. Numai scanarea ACK, folosita pentru maparea regulilor din firewall, clasifica portul în aceasta stare.
- **open|filtered (deschis|filtrat) -** Nmap plasează porturi în aceasta categorie când nu poate determina dacă portul este deschis sau filtrat. Acestea apar pentru tipurile de scanări în care porturile deschise nu oferă nici un răspuns.
- **closed|filtered (închis|filtrat) -** Aceasta stare este folosita când Nmap este în imposibilitatea de a determina dacă portul este închis sau filtrat. Este folosit doar de scanarea IPID Idle. Aceste stări nu sunt proprietăți intrinsece ale porturilor, dar descriu modul în care sunt văzute de Nmap.

3.3 Tehnici de scanare de porturi

Chiar dacă Nmap încearcă sa producă cele mai precise rezultate, trebuie ținut cont de faptul ca el se bazează pe pachetele returnate de mașină țintă (sau firewall-ul din fata lui).

-sS(Scanare TCP SYN)

Scanarea SYN este implicită. Poate fi executata rapid, scanând mii de porturi pe secunda într-o rețea fără firewall. Scanările SYN sunt relativ invizibile, din moment ce nu stabilesc niciodată o conexiune TCP.

-sT(Scanare TCP connect())

Scanarea TCP Connect() este implicita când SYN nu reprezinta o opțiune viabilă. Acesta este cazul în care utilizatorul nu beneficiază de posibilitatea de trimitere a pachetelor brute sau scanează rețele IPv6. în locul scrierii pachetelor brute asa cum o fac majoritatea tipurilor de scanare, Nmap cere nivelelor inferioare ale sistemului de operare sa stabilească o conexiune cu mașină țintă și portul dorit realizând un apel de sistem connect().

-sU(Scanare UDP)

DNS, SNMP și DHCP (porturile înregistrate 53, 161/162 și 67/68) sunt trei dintre cele mai comune porturi. Deoarece scanarea UDP este în general lentă și mai dificilă decât TCP, unii experți în securitate ignora aceste porturi. Porturile închise reprezintă adesea o problemă și mai mare. în mod uzual trimit înapoi un mesaj de eroare ICMP inaccesibil. Nmap detectează rata de limitare și încetinește scanarea în conformitate cu aceasta pentru a preveni inundarea rețelei cu pachete inutile pe care mașină țintă le va ignora.

-sN;-sF;-sX(Scanări TCP Null, FIN, și Xmas)

Aceste trei tipuri de scanare exploatează o portiță din TCP RFC pentru a diferenția intre porturile deschise și cele închise .

Există trei tipuri de scanări:

1. Scanare Null (-sN): Nu setează nici un bit (flagul header tcp este 0)
2. Scanare FIN (-sF): Setează doar bitul TCP FIN.
3. Scanare Xmas (-sX): Setează flagurile FIN, PSH și URG

Principalul avantaj al acestor tipuri de scanare este acela că se pot strecura prin anumite firewall-uri non-statefull și routere cu filtrare de pachete. Alt avantaj al acestor tipuri de scanare este ca sunt și mai discrete decât o scanare SYN deși multe IDSuri moderne pot fi configurate sa le detecteze.
Nu toate sistemele respecta RFC 793. Unele trimit un răspuns RST la probe indiferent dacă portul este deschis sau nu. Acest lucru face ca porturile sa fie marcate ca fiindinchise (closed).

-sA(Scanare TCP ACK)

Aceasta scanare e diferita de celelalte discutate pana acum în sensul în care nu poate determina niciodată un port deschis sau deschis|filtrat
Este folosita pentru a verifica regulile firewall-ului.

-sW(Scanare TCP Window)

Scanarea Window (fereastra) este asemănătoare cu scanarea ACK, cu excepția ca exploatează un detaliu de implementare a anumitor sisteme pentru a diferenția porturile deschise de cele închise.

-sM(Scanarea TCP Maimon)

Scanarea TCP Maimon este denumita astfel după descoperitorul ei, Uriel Maimon 1996). Tehnica este similara cu scanările Null, FIN și Xmas cu excepția ca proba este FIN/ACK. Oricum, s-a observat faptul ca multe sisteme derivate din BSD ignora pachetul dacă portul este deschis.

--scanflags(Scanare TCP personalizată)

Opțiunea permite crearea propriilor tipuri de scanare prin specificarea flagurilor TCP.
Se poate folosi orice combinație intre URG, ACK, PSH, RST, SYN, andFIN.
De exemplu,--scanflags URGACKPSHRSTSYNFIN setează toți biții, deși nu este foarte folositor pentru scanare.

3.4 Detecția serviciilor și a versiunilor

Dacă se executa nmap pe o mașină și el raportează ca porturile 25/tcp, 80/tcp și 53/udp sunt deschise. Folosind baza de datenmap-services de aproximativ 2.200 servicii cunoscute, Nmap va raporta ca respectivele porturi corespund unui server de mail (SMTP), unui server web (HTTP) și respectiv unui server DNS (53).

Aceasta recunoaștere este de obicei corectă – majoritatea serviciilor care asculta la portul TCP 25 sunt servere de mail.

După ce porturile TCP și/sau UDP sunt descoperite folosind una dintre metodele de scanare, detecția versiunii interoghează acele porturi pentru a determina mai multe despre ce se rulează la ele de fapt.

Nmap încearcă sa determine protocolul serviciului (ex: ftp, ssh, telnet, http), numele aplicației (ex: ISC Bind, Apache httpd, Solaris teletin), numărul versiunii, numele hostului, tipul mașinii (ex: printer, router), familia de sisteme de operare (ex: Windows, Linux) și câteodată și alte informații diverse cum ar fi dacă exista un server X deschis la conexiuni.

Când servicii RPC sunt descoperite, evaluatorul RPC din Nmap (-sR) este automat folosit pentru a determina programul RPC și numărul versiunii.

Unele porturi UDP sunt lăsate în starea deschis|filtrat (open|filtered) după o scanare UDP care nu a putut determina dacă porturile sunt deschise sau filtrate.

Detecția versiunii va încerca sa obțină un răspuns de la aceste porturi (asa cum o face cu porturile deschise), și sa sa le schimbe starea în deschis dacă reușește.
Porturile TCPdeschis|filtrat (open|filtered)sunt tratate în aceeași maniera. Opțiunea –A activează detecția versiunii printre altele.

3.5 Exemple de utilizare

Nmap adresă numerică stație

nmap -v www.xxx.xxx
Aceasta linie de comanda scanează toate porturile TCP rezervate de pe mașina www.xxx.xxx. Opțiunea –v activează modul de afișare În timp real a rezultatelor.

nmap -sS -O www.xxx.xxx/24
Lansează o scanare SYN împotriva tuturor celor 255 mașini din rețeaua de clasa C unde își are locul gazda. De asemenea încearcă determinarea sistemului de operare a fiecărui host activ. Acesta lansare necesita privilegii root din cauza scanării SYN și a detectării sistemului de operare.

nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127
Lansează enumerarea gazdelor și o scanare TCP În prima jumătate a celor 255 de subretele 198.116 de clasa B. Testează dacă sistemul execută sshd, DNS, pop3d, imapd sau portul 4546. Pentru fiecare dintre porturile găsite deschise, detecția versiunii este pusa În funcțiune pentru a se determina aplicația care execută.

nmap -v -iR 100000 -P0 -p 80
Cere Nmap-ului sa aleagă aleator 100.000 ținte și sa le scaneze În căutarea serverelor web (portul 80). Enumerarea gazdelor este dezactivata cu -P0 din moment ce trimiterea unui cuplu de probe pentru a determina dacă hostul este activ este o pierdere de timp atâta vreme cat se cauta un singur port al fiecărei ținte.

nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20
Scanează după servere web (fără ping) și salvează rezultatele În formatul pentru comanda grep și În formatul XML.

host -l www.xxx.xxx | cut -d -f 4 | nmap -v -iL -
Realizează un transfer de zona DNS pentru a găsi toate hosturile din www.xxx.xxx și apoi furnizează adresele Nmap-ului. Comanda de mai sus este valabila pentru un sistem Linux

Temă de laborator
- Testați fiecare comandă cu diverse combinații de parametri (când acest lucru este posibil).

Temă pe acasă:
Pornind de la analiza anterioară(tema 2) creati o o harta cu informațiile extrase cu nmap-ul pentru fiecare stație din graful de la tema 2
Cei care nu stau în cămin deconectează legătura cu isp-ul și fac analiză pe calculatoarele din rețeau locală (mama, tata, desktop etc) până se obișnuiesc apoi oricum vor face pe caz real în redblue.