Lab 11-12 Securitate TCP/IP

- ***Arhitectura si adrese IP***
- ***Protocoale Internet***
- ***Creare retea virtuala***
- ***Atacuri - Simularea unui atac in retea***

Arhitectura si adrese IP

Arhitectura Internet consta in retele de calculatoare conectate intre ele prin routere IP (IP gateway sau proxy) care folosesc protocoale Internet pentru a comunica intre ele. Host: end-user system = terminal intr-o retea fizica. Unul sau mai multe hosturi formeaza interfata retelei.

Transmiterea pachetelor
Source Host: daca destinatarul este in aceeasi retea fizica atunci transmiterea se face in mod direct, altfel se face prin intermediul unui router. Routerul permite conexiunile exterioare.

Routere intermediare: atunci cand destinatarul nu se afla in aceeasi retea fizica, se trimite pachetul spre un router intermediar.

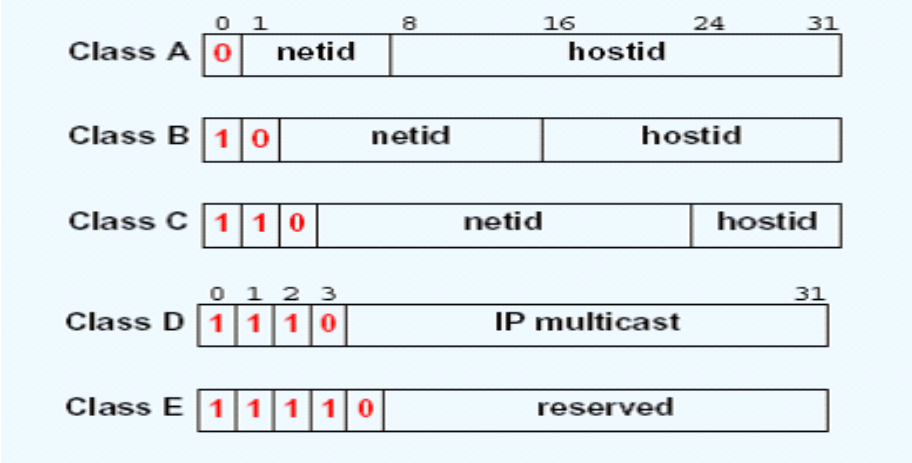
Router Final: daca destinatarul este conectat fizic cu acest router trimiterea pachetelor se face in mod direct.

Pentru a transmite un pachet routerele trebuie sa gaseasca calea (adresa corecta) a destinatarului, ceea ce se realizeaza pe baza informatiilor pe care le are din Tabloul de rutare. Tabloul de rutare: contine adresele retelelor si nu ale hosturilor (pentru a evita supra-aglomerarea).

Adrese IP (https://en.wikipedia.org/wiki/IP_address)

- Sunt de 32 de biti in binar (IPv4)
- Fiecare host are un unic IP
- Se foloseste notarea cu punct (in baza 10) exemplu: 128.230.1.12

(in binar: 10000000 11100110 00000001 00001100)
dupa o Schema de Clase bazate pe diviziunea dintre prefix si suffix.
Classless Addressing Scheme - 1990



Clasa A: 1.0.0.0 --- 126.0.0.0
B: 128.1.0.0 --- 191.255.0.0
C: 192.0.1.0 --- 223.255.255.0

D: 224.0.0.0 --- 239.255.255.255
E: 240.0.0.0 --- 255.255.255.254

Exemple: IBM 9.0.0.0, AT&T 2.0.0.0, National Institute for Physics and Nuclear Engineering Horia Hulubei 194.102.58.0/23, Institute for Atomics Physics, Magurele 46.234.114.0/24, Alexandru Ioan Cuza University 85.122.19.0/255 (see also https://ipinfo.io/AS2614 or https://db-ip.com/all/85.122.19)

Reserved address prefixes
a)10/8 10.0.0.0 - 10.255.255.255
b)172.16/12 172.16.0.0 - 172.31.255.255
c)192.168/16 192.168.0.0 - 192.168.255.255
d)169.254/16 169.254.0.0 - 169.254.255.255

Protocoale Internet

https://ro.wikipedia.org/wiki/TCP/IP
https://en.wikipedia.org/wiki/Transmission_Control_Protocol

Internet = retea unica de computere interconectate prin protocoalele (reguli) de comunicare Transmission Control Protocol / Internet Protocol, numite pe scurt TCP/IP.

Connectionless Delivery System: Reprezinta un sistem de livrare a pachetelor care este: unreliable, best-effort, and connectionless.

Unreliable: packets may be lost, duplicated, delayed, or delivered out of order.
Connectionless: each packet is treated independently from all others.
Best-effort: the Internet software makes an earnest attempt to deliver packets.

Internet Protocol
https://ro.wikipedia.org/wiki/Internet_Protocol

Creare retea virtuala – exercitiu laborator

Se va crea o retea formata din 3 masini virtuale de tip Ubuntu (Router, C1, C2) folosind Virtual Box

Pas. 1 In Virtual Box se creeaza o masina virtuala MV base, de tip Linux (versiune Ubuntu, 32 bits, memorie alocata 512 MbRAM, HardDisk 8GB, de tip vdi, dynamically allocated).

Se porneste masina virtuala MV base pe care se instaleaza distributia de linux mentionata mai sus. Pe MV base se instaleaza pachetele traceroute, dnsutils, net-tools, iptables, wireshark, ettercap si un server FTP (necesare viitoarelor aplicatii).

Observatii: **Wireshark**: realizeaza monitorizarea traficul de date in reteaua locala (https://en.wikipedia.org/wiki/Wireshark)

Ettercap sau **netwox**: vor fi folosite pentru implementarea atacurilor (a se vedea https://www.ettercap-project.org/)

Netwox: poate fi folosit pentru a trimite pachete de diferite tipuri, avand un continut diferit
Dnsutils: poate fi folosit pentru comenzi precum dig, nslookup (a se vedea https://packages.debian.org/sid/dnsutils)

Xinetd si **telnetd**: server telnet (a se vedea https://bash.cyberciti.biz/guide/Telnetd)

Bind9: server DNS.

Iptables: (a se vedea https://en.wikipedia.org/wiki/Iptables)

Vsftpd: (a se vedea https://en.wikipedia.org/wiki/Vsftpd)

Se pot folosi comenzile:

```
sudo apt-get update
sudo apt-get install traceroute dnsutils
sudo apt-get install net-tools
sudo apt-get install iptables
sudo apt-get install wireshark
sudo apt-get install ettercap-graphical
sudo apt-get install vsftpd
```

Se inchide masina virtuala MV base folosind comanda

```
sudo poweroff
```

Pas. 2 Se realizeaza trei clone ale masinii virtuale MV base.

Clona Router: click dreapta pe MV base si se alege Clone din meniu. In fereastra Clone Virtual Machine se denumeste noua masina *MV Router*, se bifeaza *Reinitializare the MAC Address*. Alegeti Tipul clonei Linked Clone/Full Clone. Restul optiunilor pot fi lasate pe variantele default. Asemanator se creeaza Clonele C1 si C2.

Cele trei clone vor fi configurate intr-o retea, iesirea in internet realizandu-se prin MV Router.

Pas3. Configurare MV Router.

1. Se selecteaza MV *Router* si *Settings* din meniul aplicatiei VirtualBox.
2. Selectati *Network -> Adapter 1 (Enabled, Attached to: NAT)*; *Adapter2 (Enabled, Attached to: Internal Network)*;
3. Se porneste masina MV *Router*;
4. Se configureaza interfata de retea *eth1* (atasata retelei interne) cu adresa IP statica in pasii:
   a. se editati fisierul */etc/network/interfaces*
      folosind comanda
      ```
      sudo nano /etc/network/interfaces
      ```
   b. se adauga la sfarsitul fisierului urmatoarele linii:
      ```
      auto eth1
      iface eth1 inet static
      address 192.168.1.11
      netmask 255.255.255.0
      ```
5. Se salveaza fisierul si se inchide editorul de text.
6. Se activeaza interfata *eth1* prin comanda:
   ```
   sudo ifdown eth1
   sudo ifup eth1
   ```

7. Se verifica setarile prin comanda:

```
ifconfig eth1
```

(in cadrul rezultatului comenzii ar trebui sa apara

```
inet addr: 192.168.1.11 )
```

Pentru a vedea valoarea configurarilor de forward se poate utiliza comanda

```
sysctl -a | grep forward
```

8. Se activeaza `ip forwarding` intre interfetele sistemului (se seteaza optiunea de forward pentru a fi posibila retrimiterea pachetelor primite) prin pasii

a. se editeaza fisierul */etc/sysctl.conf*
(pentru editarea unui fisier se poate folosi nano)
b. se sterge caracterul **#** din fata liniei *net.ipv4.ip_forward=1*
c. se salveaza si se inchide fisierul;

Observatii: Se pot folosi comenzile `ip addr` si `ip link show` pentru a vedea cum este denumita interfata retelei locale si pentru a vedea retelele existente.

9. Se seteaza regula folosita pentru NAT (Network Address Translation)

```
(sudo) iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

10. Se instaleaza pachetul *iptables-persistent* pentru a salva regula de mai sus prin comanda `sudo apt-get install iptables-persistent`

11. Se reporneste MV *Router*.

Pas4. Configurare MV C1.

1. Se selecteaza MV *C1* si *Settings* din meniul aplicatiei VirtualBox;
2. Se selecteaza *Network -> Adapter 1 (Enabled, Attached to: **Internal Network**)*;
3. Seporneste MV *C1*;
4. Se configureaza interfata de retea *eth0* (atasata retelei interne) cu adresa IP statica in pasii:

a. editati fisierul */etc/network/interfaces*
b. adaugati la sfarsitul fisierului urmatoarele linii:

```
auto eth0
iface eth0 inet static
address 192.168.1.12
netmask 255.255.255.0
gateway 192.168.1.11
dns-nameservers 8.8.8.8 10.1.0.7 85.122.16.1
```

c. se configureaza rutarea pachetelor catre MV Router pentru acces Internet:

```
ip route add default via 192.168.1.11 dev eth0
```

d. salvati fisierul si inchideti editorul de text.

5. Se activeaza interfata *eth0* prin comenzile:

```
sudo ifdown eth0
sudo ifup eth0
```

6. Se verifica existenta conexiunii la internet prin una dintre comenzile:

```
ping www.google.com
firefox www.infoiasi.ro
```

Pas 5. Configurare MV C2
1. Se selecteaza MV *C2* si *Settings* din meniul aplicatiei VirtualBox;
2. Se selecteaza *Network -> Adapter 1 (Enabled, Attached to:* ***Internal Network****)*;
3. Se porneste MV *C2*;
4. Se configureaza interfata de retea *eth0* cu adresa IP statica in pasii:
   a. editati fisierul */etc/network/interfaces*
   b. adaugati la sfarsitul fisierului urmatoarele linii:

```
auto eth0
iface eth0 inet static
address 192.168.1.13
netmask 255.255.255.0
gateway 192.168.1.11
dns-nameservers 8.8.8.8 10.1.0.7 85.122.16.1
```

   c. se configureaza rutarea pachetelor catre MV Router pentru acces Internet:

```
ip route add default via 192.168.1.11 dev eth0
```

   d. se salveaza fisierul si inchideti editorul de text.

5. Se activeaza interfata *eth0* prin comenzile:

```
sudo ifdown eth0
sudo ifup eth0
```

6. Se verifica existenta conexiunii la internet prin una dintre comenzile:

```
ping www.google.com
firefox www.infoiasi.ro
```

Observatii 1. Varianta alternativa: https://profs.info.uaic.ro/~eonica/isec/lab10.html

2. Pasii de mai sus rulati la consola nu sunt persistenti. Setarile se pierd la urmatoarea repornire a masinilor virtuale. Pentru a preveni acest lucru pasii executati la consola pe fiecare masina pot fi copiati linie cu linie intr-un fisier pe masina respectiva.

3. Putem porni Wireshark pe una din masini. Wireshark permite vizualizarea traficul de date care trece prin reteaua locala. In aces scop se poate folosi meniul Capture. In paralel se poate rula un ping de la linia de comanda sau se poate porni Firefox din sectiunea Internet a meniului (pt. a incerca accesarea unei pagini web). In Wireshark se pot observa pachetele trimise si capturate la nivelul statiei locale.

Atacuri - Simularea unui atac in retea

Legatura cu nivelul Internet se realizeaza prin intermediul a doua protocoale de adresare: ARP (Address Resolution Protocol) si RARP (Reverse Address Resolution Protocol). ARP comunica, la cerere pe baza adresei IP a unui echipament, adresa fizica (MAC) de 6 octeti. RARP furnizează la cerere adresa IP data unui echipament cu adresa MAC. ARP și RARP se utilizeaza numai in interiorul unui LAN. Ambele folosesc o tabela de adrese (RFC 826), respectiv (RFC 903). Pe nivelul Internet, se folosesc protocoalele IP (Internet Protocol), ICMP (Internet Control Message Protocol) si IGMP (Internet Group Management Protocol).

1. Atacul ARP cache poisoning - ARP spoofing

https://en.wikipedia.org/wiki/ARP_spoofing
https://doubleoctopus.com/security-wiki/threats-and-tools/address-resolution-protocol-poisoning/

Sniffingul reprezinta procesul de capturare (intr-un fisier) si analizare a traficului cu scopul de a detecta diverse informatii trimise printr-o retea. Utilitarele folosite pentru sniffing se numesc sniffere sau analizatoare de protocoale, deoarece prin intermediul lor sunt analizate pachetele transmise prin retea, apoi sunt capturate parolele, sau alte date confidentiale. Unul dintre atacurile prin care se poate intercepta traficul dintre două calculatoare din aceeasi retea este ARP poisoning.

Un ***switch*** reprezinta un dispozitiv de retea care limiteaza capacitatea atacatorilor ce folosesc un packet sniffer de a obţine informaţii din reteaua interna. Cu toate acestea folosind ARP poisoning traficul dintre doua calculatoare poate fi interceptat chiar şi intr-o retea care foloseste switch-uri. Aceasta metoda este cunoscuta "***ca atacul omului din mijloc***". Prin acest tip de atac, statiile afectate dintr-o retea vor ajunge sa aiba intrari eronate in tabela ARP. Astfel, aceasta va contine doar corespondenta dintre adresa IP a statiilor din aceeasi retea si o singura adresa MAC (cea a statiei care a initiat atacul).

Dacă un sistem doreste sa transmita un pachet catre un alt sistem aflat in aceeasi retea, acesta verifica tabela ARP. Daca nu este gasita maparea dorita, sistemul apeleaza la protocolul ARP transmitind o cerere ARP prin retea. Cererea contine adresa IP dorita. Fiecare sistem receptioneaza aceasta cerere si verifica daca se potriveste cu propria adresa IP. Daca da, sistemul implicat va trimite un mesaj de raspuns care contine adresa de nivel legatura de date. Sursa cererii va adauga si aceasta informatie in propria tabela ARP.

Toate nodurile retelei vor detine cate un cache ARP in care vor fi stocate adresele MAC impreuna cu IP-urile corespunzatoare. Chiar daca gazda nu a initiat nici o cerere, in cazul in care primeste un reply ARP, aceasta va face actualizarea propriului cache ARP cu informatia primita (posibil eronata).

Astfel, atacul ARP poisoning redirectioneaza traficul dintre statiile din reteaua locala si routerul de iesire din LAN (gateway) prin staţia atacatorului. Acest lucru este realizat prin trimiterea de pachete ARP (de tip cerere - raspuns) cu informatii eronate. Cauza este faptul ca protocolul ARP nu face autentificare.

Tema 1 *Implemetati si demonstrati cum functioneaza un astfel de atac si precizati care pot fi consecintele.*

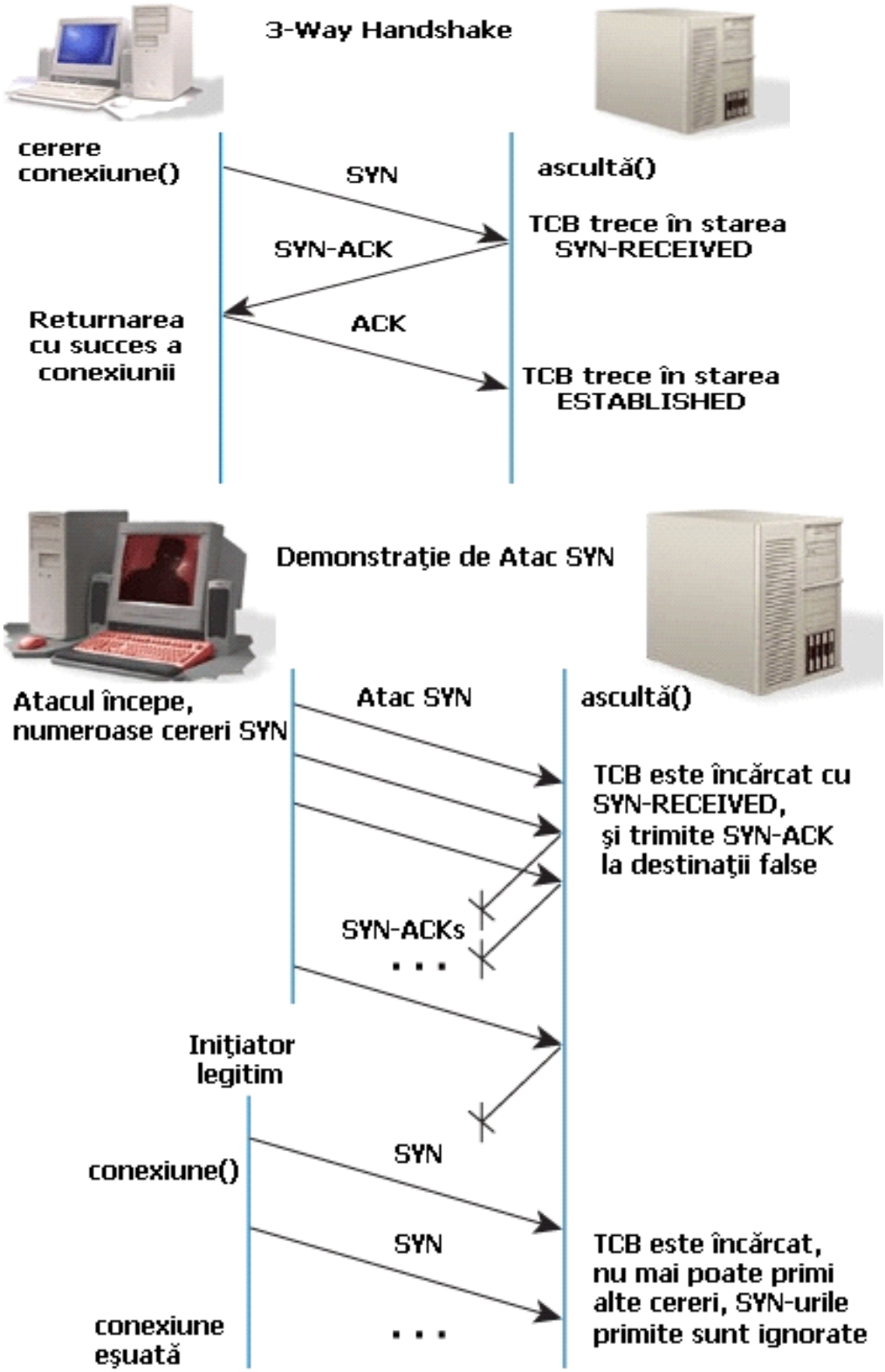
Observatie: Vizualizarea tabelei ARP se poate face prin intermediul comenzii `arp -a` sau `ip neighbour`.

2. Atacul SYN Flooding

https://en.wikipedia.org/wiki/SYN_flood

Un atac de tip SYN Flood se bazeaza pe principiile de funcționare ale comunicarii in retea, in trei pasi (three-way handshake) astfel: in timpul operatiunii un client initiaza comunicarea prin transmiterea catre server a unui pachet TCP/SYN, avertizand serverul ca doreste sa comunice. Serverul, odata ce primeste pachetul, creeaza o conexiune pentru a comunica cu clientul si trimite o confirmare si o referinta la canalul de comunicare.

Clientul, la randul sau, trimite inapoi o confirmare de primire, si incepe comunicarea cu serverul. In cazul in care clientul nu raspunde cu cea de a doua confirmare, serverul presupune ca aceasta nu a ajuns la destinatie si retrimite pachetul.



Un atac de tip SYN Flood abuzeaza de acest mecanism prin trimiterea mai multor pachete TCP/SYN (fiecare cu o origine falsa, specificata). Fiecare pachet forteaza serverul sa creeze o noua conexiune si sa continue transmiterea confirmarilor. In scurt timp, serverul va utiliza toate resursele proprii, cu conexiunile pe jumatate deschise.
Starea SYN-RECEIVED este folosita pentru a indica faptul ca o conexiune este pe jumatate deschisa si cererea conexiunii este sub semnul intrebarii. Aceasta stare conduce catre un potential atac DoS (Denial of Service). Pentru a evita aceasta situatie sistemele de operare aloca un parametru denumit `backlog` care seteaza un numar maxim de conexiuni simultane ce pot fi in starea SYN-RECEIVED. Dimensiunea cozii in care sunt plasate cererile este stabilita de sistem. Acest parametru se verifica prin comanda:

```
$ sysctl -q net.ipv4.tcp_max_syn_backlog
```

Pentru a verifica stadiul cozii se ruleaza comanda:

```
$ netstat -na
```

Aceasta permite aflarea conexiunilor in curs (SYN-RECEIVED) asociate unui port in stadiul "*listen*". Dupa analizarea celor 3 pasi, statusul conexiunii va fi ESTABLISHED.

Tema 2 *Explicati cum functioneaza atacul SYN Flooding. Implementati atacul si identificati pachetele atacatorului. In timpul derularii atacului, pe masina atacatorului rulati din nou comanda $ netstat -na si comparati rezultatele cu cele dinainte de atac.*

3. Atacul DNS Server Cache Poisoning

https://en.wikipedia.org/wiki/DNS_spoofing

Un atac DNS Server Cache Poisoning este un tip de atac DDoS (Distributed Denial of Service) care se bazeaza pe utilizarea unor servere de tip „open recursive DNS resolver", accesibile in mod public, pentru a supraincarca un sistem informatic victima cu trafic de tip răspuns DNS.

DNS (Domain Name Server) face legatura dintre hostnames si adresele IP si invers. Cand un server DNS primeste o cerere acesta va cauta numele cerut in propriul cache (care este pastrat o anumita perioada de timp). Daca rezultatul este negativ, va interoga alte servere, pentru rezolvarea numelui, primind un raspuns din partea lor. Acest raspuns poate fi falsificat, caz in care serverul care a facut cererea va pastra in propriul cache informatia falsa pana la expirarea perioadei de timp alocate, fiind astfel victima a unui atac.

Observatii 1. Se poate goli cache-ul serverului DNS inaintea atacului prin comanda

```
$ sudo rndc flush
```

2. Pentru a vedea daca atacul a reusit se poate utiliza `wireshark` sau se poate analiza cache-ul server-ului prin comenzile:

```
$ sudo rndc dumpdb -cache
$ sudo cat / var/cache/bind/dump.db
```

3. Pentru simularea unui astfel de atac este necesara instalarea si configurarea unui server DNS pe masina Router, ceea ce se realizeaza prin instalarea pachetului `bind9` pe Router.

Tema 3 *Implementati un atac DNS Server Cache Poisoning si prezentati observatiile efectuate.*

Tema 4 **Observator de trafic in retea**

https://www.tcpdump.org/pcap.html

Mesajele de redirectare ICMP (Internet Control Message Protocol) sunt utilizate de catre rutere pentru a actualiza informatiile de rutare pe masinile gazda. La primirea unui astfel de mesaj se modifica tabelul de rutare, disponibil prin comanda `route` (fara a se efectua validarea datelor).

Programele pentru monitorizarea pachetelor pot fi scrise utilizand biblioteca `pcap`. Pachetele monitorizate pot fi puse intr-un buffer pentru a fi analizate mai tarziu.

Descarcati fisierul `sniffex.c` de la adresa http://www.tcpdump.org/sniffex.c
compilati si rulati acest fisier. Implementati monitorizarea pachetelor de retea (bufferul retelei).

Descrieti secventa de functii din biblioteca `pcap` necesare pentru a implementa monitorizarea pachetelor din retea. Notati observatiile legate de drepturile pe care trebuie sa le aiba initiatorul actiunii de monitorizare. Ce se intampla daca nu are aceste drepturi, ce poate face fara drepturi de root?

Modificati programul `sniffer` pentru a intercepta pachete de tip ICMP si TCP intre doua masini specificate.

Aratati cum se poate utiliza `sniffex` pentru a intercepta datele de login in cazul unei conexiuni `telnet` in reteaua monitorizata.

Observatii Tema

1. Se va implementa doar unul din cele 3 tipuri de atac sau "observatorul" (tema 4). Se va puncta doar una din cele 4 teme. Tema se va prezenta in cadrul primului laborator din 2022. Pe langa implementare se vor preciza timpii de execuție, idei de a proteja reteaua impotriva tipului de atac ales (si simulat), observatii privind esecul unui atac, etc.

2. Se va folosi ca mediu de lucru doar VirtualBox/VMware si nu un mediu real. Configurati o retea locala compusa din 3 masini virtuale cu o versiune de Linux instalata, dintre care una este atacatorul, alta este victima iar a treia este observatorul.

Cateva aplicatii utile: *wireshark* - pentru a monitoriza traficul din reteaua locala, *ettercap/netwox* /(*netwag* pentru interfata greafica), *dnsutils* - in vederea interogarii DNS-ului (dig/nslookup), pentru a face actualizari dinamice (*nsupdate*) RFC2136, *xinetd* - server telnet, *bind9* - server DNS.