INTRODUCERE ÎN SECURITATE CIBERNETICĂ ȘI HACKING

CONCEPTE DE HACKING ȘI CYBERSECURITY

Ramon Nastase

Securitatea Cibernetica & Ethical Hacking pe intelesul tuturor

Invata fundamentale Securitatii Cibernetice chiar si fara experienta in IT

#InvataSecuritate - De ce exista aceasta carte si ce vei invata din ea

In primul rand vreau sa te felicit si sa iti multumesc pentru faptul ca ai luat **decizia de a investii in tine** si de a deveni mai bun.

Eu sunt Ramon Nastase, autorul cartii, fondator SecuritateIT.com, unde ajut romanii sa faca reconversie profesionala in Securitate IT in mai putin de 12 luni, cu un job garantat la final, pornind de la zero.

De-a lungul a 15 ani petrecuti in industria IT am experimentat cu multe arii: Retele, Linux, Securitate, Programare, Project Management, etc. Am lucrat in industria IT la compania Atos si am obtinut numeroase certificari din domeniu, recunoscute international (Cisco CCNA Security, CCNP Security Firewall, CCNA Voice, CCNP Routing & Switching ⅔, Linux LPIC-102, CompTIA Security+).

Am creat acest ghid cu *scopul de a pune ordine in informatie* si a te ajuta sa obtii rezultate, mai repede. Pe termen lung, intentia mea este sa ajut cat mai multi romani sa traiasca in tara cu venituri din afara, prin IT. Astfel, in timp, vom pune Romania pe harta globala a tehnologiei, iar viata noastra de zi cu zi va fi mai buna.

De la acest ghid te poti astepta sa intelegi:

Securitate Cibernetica

- *Cum sa gandesti ca un Hacker*
- *Care sunt pasii unui Atac Cibernetic*
- *Cum sa Scanezi si sa vezi Traficul altora folosind Kali Linux*
- Triada CIA (Confidentiality, Integrity, Availability)
- Tipurile de Malware si Atacurile Cibernetice
- Hacking-ul etic in Retea
- Hacking-ul etic al Site-urilor web
- Despre Firewall-uri
- Concepte de Criptografie
- Despre tehnologia VPN

Retele & Internet

- cum functioneaza Internetul,
- cum comunica Dispozitivele (telefon, laptop, server etc) in Internet
- cum functioneaza retelele si de cate tipuri sunt,
- ce este un Router, Switch, adresa IP, adresa MAC, etc.

Linux & Servere

- Ce este Linux
- Cum il instalezi intr-o masina virtuala
- Comenzile de baza din terminalul Linux
- Ce este un server
- Cum sa-ti instalezi un server web pe Linux

Aceasta carte este structurata in 12 capitole care cuprind diferite teme, apartinand bazelor securitatii (Retele, Linux, Securitate).

Un lucru pe care vreau sa-l stii este faptul ca daca acum incepi pentru prima oara in IT, aceasta carte nu este alegerea cea mai potrivita.

De ce? Pentru ca ai nevoie de cunostinte (cel putin de baza) de Linux, Retelistica si (putina) programare pentru a putea intelege o parte din lucrurile pe care le explic eu aici.

In caz ca nu esti familiar cu Linux si retelele de calculatoare, le vom aborda pe scurt in capitolele viitoare.

Din acest motiv iti spun (inca de la inceput) faptul ca: **Nu poti "sparge" ceva ce nu intelegi**.

Inainte de a invata sa spargi si sa securizezi lucrurile este important sa intelegi cum functioneaza tehnologia. Avand acest lucru in minte, iti urez mult spor in ceea ce faci, trage cat mai tare pentru ca in final, vei vedea, cu munca si efor sustinut in mod constant, vei ajunge sa realizezi ceea ce ti-ai propus.

Dupa parcurgerea, cartii, in caz ca doresti sa lucram impreuna prin ghidare si mentorat saptamanal, poti aplica aici pentru o sesiune 1:1 de consultanta gratuita prin care sa-ti prezint cum te putem ajuta sa obtii rezultate mai bune, decat pe cont propriu.

Iti urez spor la treaba, iar daca ai intrebari nu ezita sa ma contactezi pe email, Facebook sau YouTube.

Ramon Nastase

Cuprins

Introducere in Securitatea IT

Ce este securitatea cibernetica?

Este aria din IT care se ocupa cu protejarea sistemelor informatice si a utilizatorilor sai. Mai exact, companiile si persoanele fizice au servere, echipamente de interconectare (router, switch, load balancer, firewall) care practic ne dau accesul din internet in retelele acestea locale.
De la companii la persoanele fizice, toti avem acces la internet prin intermediul serverelor, echipamentelor de conectare si altele. Dar acest acces la internet poate fi periculos, deoarece poate face ca sistemele noastre sa fie vulnerabile la atacuri cibernetice. Asa ca, este esential sa ne asiguram ca avem o buna securitate cibernetica pentru a proteja informatiile si datele noastre importante. Exista o varietate de metode si tehnici care ne ajuta sa ne protejam sistemele. Acestea pot include firewalls, criptarea datelor, autentificarea utilizatorilor si monitorizarea activitatilor de retea. Este important sa ne asiguram ca sistemele noastre sunt intotdeauna actualizate cu cele mai recente patch-uri si securitate, precum si sa educam utilizatorii despre cum sa fie siguri in mediul online si cum sa recunoasca si sa raporteze atacurile cibernetice. In final, securitatea cibernetica este foarte importanta pentru orice companie sau persoana care se foloseste de tehnologie. Este foarte important sa avem in vedere protejarea sistemelor informatice (retele, servere, data centere, calculatoare, imprimante, camere IP etc) si datele stocate sau generate de acestea. Educarea userilor este cruciala si sa respectam regulamentele si legile privind protectia datelor, reprezinta un alt factor important. Prin aceste moduri putem asigura un Internet siguri pentru noi si pentru colegii nostri.

Ce poti sa devii pe partea de cibernetica?

Ai mai multe optiuni cand vine vorba de profesarea in acest domeniu. Iata o parte dintre acestea:

- Analist – te uiti peste anumite rapoarte, esti atent la starea sistemelor, te uiti pe zona de raportare a retelei, a serverelor si de acolo tragi anumite concluzii, urmand sa vii cu anumite solutii pentru ceea ce ai gasit.
- Pentester – pe langa ce ofera analistul, aici se testeaza daca se poate intra in zona privata, daca exista vulnerabilitati pe care alte persoane le pot gasi cu usurinta. El aduce un plan de proiect in care isi propune sa testeze anumite severe, servicii din retea, IP-urile si bresele pe care analistul le-a sesizat.

- Cybersecurity Engineer – practic, rezolva acel bug care se afla in aplicatie. Daca vorbim de retea, poate adauga o componenta in plus de filtrare. Daca vorbim de development, unde echipa trebuie sa faca un update la sistemul de operare, el va avea grija sa le trimita mai departe lor.

Acesta poate activa in 2 zone:

- Zona de administrare a sistemelor, in care se asigura ca acestea sunt securizate si masurile de securitate sunt implementate.
- Zona de development, unde se ia in considerare si se rezolva ceea ce Pentester-ul a raportat.

Ce oportunitati de angajare ai ca *specialist in Securitate Cibernetica*?

Dupa cum am mentionat si mai sus, totul depinde de ceea ce iti doresti.
Fie ca visezi la un job cu program fix sau la un program flexibil de munca din interiorul unei cafenele, oportunitatile sunt nenumarate. Ca sa te fac sa intelegi mai bine despre ce vorbesc, hai sa intram in detalii cu fiecare dintre cele trei optiuni de a-ti exercita activitatea de administrator de retea. O sa gasesti in lista de mai jos si unele multinationalele. O companie multinationala, de regula, este inregistrata in mai multe tari fiind structurata in filiale localizate pe mai multe teritorii nationale sau chiar la nivel global. Cele mai mari companii au nevoie de specialisti de securitate cibernetica pentru a le putea gestiona sistemele informatice. Aici vorbim de companiile din telecom (Vodafone, Orange, Digi, Telekom), precum si furnizorii de servicii IT (Atos, Luxoft, Hella, Amazon, Voxility, Bitdefender, etc.) si multe alte firme atat din tara cat si din afara care sunt in (disperare) cautare de personal calificat.
Putem cataloga aceste companii si dupa industrii:

1. Medicala/Pharma
2. Financiar/Bancar
3. eCommerce
4. IT - companii de tip SaaS
5. Streaming - Netflix, Disney+, Hulu, Voyo, AntenaPlay, etc
6. Automotive
7. Big Data
8. Productie, etc.
9. Retail
10. Government

Daca privim din perspectiva startup-urilori, in Romania exista o multitudine de centre pentru dezvoltare. Intai vreau sa clarificam ce inseamna conceptul de start-up. Cu toate ca exista o multime de definitii, atat tehnice, cat si abstracte ale conceptului de start-up, nu exista o definitie unanima si complet acceptata. Termenul de startup a luat amploare abia in ultimii ani, cu toate ca este o forma de afacere ce exista de mai multe decenii. Poti face si tu parte dintr-o echipa cu un proiect startup!

Ce salarii sunt in domeniul securitatii?

Acum probabil ca te gandesti ca oricine poate castiga un salariu de peste 10.000 RON, in domeniul IT, dar din pacate nu este neaparat asa. Exista anumite job-uri cu specializari care sunt platite mai mult, iar altele care sunt platite mai putin. Pe langa asta, companiile mereu au nevoie de oameni care sunt la curent cu cele mai populare tehnologii si cu schimbarile care apar la acestea. Asta inseamna ca dupa ce esti acceptat la o firma de IT si tii pasul cu cererea de pe rolul pe care il ocupi, ai si posibilitatea de a-ti dezvolta o cariera spre beneficiul tau.

Hai sa vedem de ce nivel de pregatire ai nevoie pentru a lucra ca security analyst (adica analist de incidente de securitate).

1. Junior Security Analyst
Daca inca nu ai lucrat deloc in acest domeniu, cel mai probabil vei intra pe postul de Junior CyberSecurity Analyst. Din acest criteriu fac parte cei intre 0 – 2 ani de experienta. Stai linistit, lumea va intelege ca esti la inceput, fiind si in procesul de studiu nu vei primi responsabilitati prea mari. Iti recomand sa ai un certificat pe securitate, cea mai buna alegere este CompTIA Security+. Am tinut cont de aceste baze solide atunci cand am scris cartea. Sa stii ca asa necesita aproximativ un an de experienta in IT. Pe langa aceste cunostinte de securitate, iti recomand sa studiezi si Linux & servere la nivel mediu. Asta te va ajuta sa fii stapan pe aria securitatii, indiferent de tehnologiile cu care vei lucra. Din punct de vedere financiar apare in primul rand o diferenta in functie de locatie, dar si de experienta pe care o ai. Daca de putin timp ai pornit pe acest drum, salariul poate varia intre 4.000 – 6.000 RON, subliniez, in functie de experienta si de valoarea pe care o aduci tu la firma.

2. Middle Security Analyst
Ca sa lucrezi ca analyst de incidente de securitate, e nevoie de un minim de 2 – 4 ani de experienta in domeniu. Un nivel minim este cel de CompTIA Security+ sau o certificare

echivalenta de la un alt vendor (ex: CEH - Certified Ethical Hacker) este obligatorie din punctul meu de vedere. Clar, tinta ta aici ar fi OSCP (Offensive Security Certified Professional). De aici vei putea face tranzitia spre un job de Penetration Tester care iti permite sa devii un hacker (etic) in adevaratul sens al cuvantului. Oportunitati de cariera nenumarate, vei fi platit mult mai bine si extrem de cerut de piata (in special de cea din afara tarii)
Pe partea financiara salariile se incadreaza intre 6.500 – 9.000 RON. Efortul depus e platit! Odata ajuns Penetration Tester vei trece cu usurinta de 10.000, 15.000, chiar si 20.000 RON intr-o luna ca salariu net.

3. Senior Network Administrator
In aceasta categorie deja ai cunostinte peste medie, cunoscand OSCP-ul (iti recomand sa cauti mai multe despre aceasta certificare pe Google). Experienta necesara e clar peste 5 ani. Salariile sunt peste 10.000 RON fara certificarea OSCP si pot sa treaca de 15.000, avand aceasta certificare. E clar ca aceste sume sunt foarte bune aici in Romania!
Poti merge chiar si mai departe cu OSCE care este “doctoratul hackerilor”. E cea mai de pret certificare din industrie care te testeaza la maxim (atat dpvd. tehnic, cat si psihic).

Cum ajungi sa lucrezi in IT ca specialist de Securitate Cibernetica?

Acum urmeaza sa iti descriu pe scurt care e procesul prin care trece in general o persoana de nivel Junior, atunci cand doreste sa se angajeze. Acesti pasi au un scop orientativ, insa stiu ca e foarte probabil sa auzi anumite lucruri pentru prima data.

O mare parte dintre persoanele care imi scriu se afla in aceasta categorie junior (cu experienta mica, intre 0-2 ani). De aceea am decis ca le-ar fi folositor sa detaliez ma jos in cateva punctele cheie pasii prin care vor trece in cazul in care opteaza sa se angajeze:

1. Aplicarea CV-ului – Primul pas este desigur sa iti depui CV-ul prin mediul online, la targurile de job-uri sau chiar printr-o cunostinta care lucreaza deja acolo. Nu uita sa te informezi despre firma cu care urmeaza sa iei contactul. Pregateste si o scrisoare de intentie in care subliniezi de ce doresti sa te angajezi la ei, pe un ton formal.
2. Testul de logica – Daca esti selectat dupa criteriile folosite de firma, esti contactat pentru un scurt interviu telefonic, urmat de anumite teste de logica la firma. Aici de obicei se pune accentul pe modul de gandire al candidatului. Scopul acestor teste este ca recruiterul sa observe daca au o baza logica. Unii folosesc chiar anumite

jocuri de puzzle, betisoare de plastic sau obiecte de diferite forme care trebuie sa fie aranjate dupa un anumit fel.

3. Testul de personalitate – Daca ai trecut de acestea (poate fi tot si in aceaasi zi) are loc un test de personalitate. In acest context cel care te evalueaza este atent la soft-skill-urile pe care le ai. Unele dintre acestea pot fi: atentia la detaliu, rabdarea, perseverenta pe gasirea unei solutii, modul de reactie la o situatie descrisa. Pana in acest punct nu se deschide subiectul despre salariul de network administrator.
4. Proba practica / tehnica – In penultima etapa are loc interviul tehnic, cel de hard-skills. Aici esti testat in adevaratul sens al cuvantului: treci prin testele tehnice (practice) de network admin. Problemele primite la acest test au rolul de a verifica daca esti pregatit in zona IT, pentru a ocupa viitorul tau post. Fii pregatit, e posibil sa primesti si o “tema de casa”, unde ai la dispozitie o saptamana sa vii cu propria solutie pentru o topologie gata data.
5. Aspectul financiar – viitorul tau salar! – Daca ai ajuns pana aici, esti chemat la ultimul interviu de recrutare: cel in care are loc discutia despre salar si despre beneficiile oferite. Tot aici poti deschide subiectul si despre asteptarile tale. De exemplu poti intreba daca exista optiunea de home office (HO) de cateva ori pe luna, poti afla cum te poti dezvolta mai departe in cadrul firmei si ce career-path (traseu de cariera) poti urma pentru a ajunge pe un post superior.

Cum sa aprofundezi invatarea folosindu-te de Google?

In acesta sectiune vom discuta despre Google si cum poate acesta sa te dezvolte pe tine ca si programator. Un skill foarte important pentru majoritatea celor care lucreaza in domeniul IT este sa cunoasca metode de rezolvare a problemelor si cel mai important, sa stie ce sa caute. Este foarte important sa stii ce cauti pentru o rezolvare mai rapida a problemei iar Google este unul dintre cei mai buni prieteni ai omului cand vine vorba de rezolvarea problemei.

Nu trebuie sa te temi sa iti cauti problema si sa iti spui ca un “admin adevarat” isi rezolva singur problemele, deoarece aceasta este o conceptie gresita si trebuie eliminata, de ce trebuie sa treci prin aceeasi pasi pentru a rezolva o problema daca un om a facut deja treaba grea pentru tine. Cel mai mare avantaj al Internetului este ca prin el putem afla multe raspunsuri care devin solutii pentru problemele noastre. Google aici face partea “magica” de cautare. Acum e timpul sa iti spun si tie cum abordez eu si cum te sfatuiesc si pe tine sa abordezi o anumita situatie:

1. “Nu stiu ceva?”
2. “Caut pe Google punand intrebarea (keyword-urile corecte) – how to X.”
3. “Gasesc ceea ce ma ajuta. O aplic.”

Frumusetea in cursurile de retelistica e ca poti invata logic fara a toci si fara a memora exact totul. Ideea principala e ca Google are toate raspunsurile. Aici e fix invers in comparatie cu scoala: daca auzim “nu cautati pe Internet”, aici in IT tocmai acesta e skill-ul necesar. Nu exista IT-ist care sa nu foloseasca Google de zeci si chiar de sute de ori pe zi, nici in firmele mai mici si nici in corporatii. In cazul nostru putem spune ca orice nu cunosti in securitate, are o solutie pe Internet. Google constituie o librarie enorma de documentatie pentru limbajele de programare si pentru comenzile de retelistica, astfel cu siguranta te va ajuta sa te dezvolti pe plan profesional asa cum m-a ajutat si pe mine. Nimic nu trebuie invatat pe de rost, totul merge pe logica in programare, iar astazi ti-am explicat in detaliu ce trebuie sa faci pentru a intelege mai bine acest lucru. Ai vazut si un exemplu despre o cautare bine structurata pe Google si despre ce indicii cheie trebuie sa introduci pentru a reusi sa gasesti ceea ce iti doresti. In continuare iti voi da sfaturi si despre ce platforme de rezolvare a problemelor sa incerci prima oara pentru a gasi o solutie mai rapida. Important este in ziua de azi sa poti sa fii cat mai independent si sa gasesti singur rezolvare la obstacolele tale fara a astepta ajutor din partea celorlalti.
Asta te va ajuta sa te dezvolti pe tine, personal, si iti va oferi un avantaj in fata celorlalti competitori din industrie. Bineinteles ca exista multe alte site-uri de unde poti gasi raspunsurile. Tot ce trebuie sa faci este sa cauti pe Google, adresand intrebarea corect. Ce iti recomand este sa treci la treaba (asta daca nu ai facut-o deja).

De ce cunostinte vei avea nevoie inainte de a incepe sa studiezi si sa practici securitatea cibernetica si hacking-ul etic?

1. Fundamentele calculatoarelor (hardware, memorii, aplicatii software, etc) si sistemelor de operare (tipuri de sisteme, sistem de fisiere, utilizatori, drepturi de acces, procese, linia de comanda, etc.)
2. Fundamentele retelelor de calculatoare (adresa IP, adrese MAC, porturi, echipamente de retea, etc)
3. Fundamentele operarii pe Linux din linia de comanda
4. Intelegerea notiunilor de servere
5. Intelegerea notiunilor de virtualizare

In cazul in care nu esti familiar cu toate acestea, vom face o scurta introducere in capitolele viitoare. In continuare iti recomand sa parcurgi si cursul de Introducere in IT de pe platforma TeachBit.ro, e **gratuit**. Intra aici: https://teachbit.ro/courses/start-in-it/

I. Despre Hackeri

Propun sa vorbim despre un subiect destul de interesant din zona de Securitate Cibernetica si anume despre Hackeri. Sunt convins ca ai auzit de ei, foarte des la stiri. Tot mai des. Asta inseamna ca numarul lor creste constant ceea ce inseamna ca si oportunitatile din piata cresc (mai ales pe zona de CyberSecurity).

Inainte sa discutam mai in detaliu despre Hackeri, vreau sa-ti spun ca voi folosi des acesti termeni: ***Securitate Cibernetica*** si ***CyberSecurity***. Acestea reprezinta unul si acelasi lucru: **Stabilirea si mentinerea nivelului de securitate** a unei infrastructuri informatice (retea de calculatoare, server, laptop etc.)

Ok. Dar de ce avem nevoie de securitate cibernetica ? Pentru ca aceasta asigura buna functionare a sistemelor informatice atat pentru companii cat si pentru persoane (ca mine sau ca tine). In cazul unui incident de securitate care are ca tinta extragerea informatiilor dintr-o baza de date, atacatorul poate lua aceste informatii si le poate folosi in mai multe scopuri:

1) Le poate vinde pe piata neagra (Deep Web)
2) Le poate folosi in *scop personal* pentru a ataca cibernetic acele persoane cu scopul de a *extrage anumite informatii* bancare
3) Alte motive personal - ego, satisfactie personala... da, sunt multi care fac doar pentru asta

Ok. Acum ca am tot vorbit de rau despre Hackeri, sa vedem daca toti Hackerii sunt rai. Acum poate te intrebi: “Stai asa Ramon, cum adica? “*Daca toti Hackerii sunt rai ?”.* Un hacker nu este prin definitie... rau ?”

Ei bine iti pot spune ca nu. Termenul de Hacker (in anii ‘80) definea o persoana careia ii placea tehnologia si in mod special sa programeze (sa scrie cod). Termenul (la vremea respectiva) folosit pentru persoanele care programau virusi, care spargeau retele sau faceau orice alte lucruri ilegale era de **Cracker**.

In ziua de astazi nu prea auzi acest termen. Un Cracker (astazi) poate fi asociat cu o persoana care incearca sa sparga parole in diferite ipostaze (fie ca este vorba de cea de la Wi-Fi sau cea dintr-o baza de date).

Inainte sa inchei cu aceasta introducere mai vreau sa-ti aduc la cunostinta un termen foarte des folosit: “**Hacking**”.

Hacking-ul este procesul pe care un atacator il urmeaza cu scopul de a obtine **acces neautorizat** intr-un sistem (server, retea, laptop etc.)

Acum ca am vorbit despre aceste subiecte, sper ca ti-ai facut o imagine mai clara legata de lumea de securitate si propun sa vorbim mai multe despre Hackeri si de cate tipuri pot fi ei.

De cate tipuri poate fi un Hacker ?

Dupa cum am spus si mai devreme: NU toti Hackerii sunt rai. Dar daca nu toti sunt rai, cum ii categorisim ? De ce se mai foloseste acest termen pentru ei ?

Ei bine, lucrurile stau in felul urmator: Exista 3 categorii principale de Hackeri:

- **Black Hat** Hacker
- **Grey Hat** Hacker
- **White Hat** Hacker

Hai sa ii luam in ordine si sa discutam despre fiecare in parte:

1) Black Hat Hacker

De acest tip de Hackeri sunt absolut sigur ca ai mai auzit. Poate nu in acest format de “Black Hat” (figura 1.1) , dar sigur ai auzit de ei. Sunt acei Hackeri la care se refera toata lumea cand pomeneste acest termen. Acele persoane pe care le vezi la stiri de care se spune ca au spart serverele de la compania X, Y, Z.

Figura 1.1

Figura 1.1 de mai sus ilustreaza “logo-ul” unui astfel de Hacker de tip “Black Hat”, adica un Hacker non-etic pus pe fapte (rele). De obicei cei care sunt la **inceput** pe partea de Cyber*Security si PentTesting* se incadreaza in aceasta categorie pentru ca vor sa **invete** (si nu prea stiu ce fac).

Pana la urma, *Black Hat Hackerii*, sunt persoanele care fac lucruri intr-un **mod** total **lipsit** de **etica** si cu scopul de a se afirma, de a-si demonstra lor ca pot, bineinteles (nu in ultimul rand), de a lua diferite date extrem de valoroase (ex: datele clientilor, informatii bancare, datele strict secrete ale companiei) de la diferite organizatii.

De ce fac asta ? Pentru ca pot lua acele **date** si le pot **vinde** pe piata neagra (“Deep Web”) sau le pot folosi in scop personal (furturi, santaje etc.).

2) Grey Hat Hacker

Hackerii de tip “Grey Hat” (figura 1.2) sunt la mijloc: nici prea buni si nici prea rai. Ce inseamna asta ? Inseamna ca ei **nu sunt 100%** dedicati in a face fapte rele, respectiv in a face hacking etic (dupa cum vei vedea la punctul 3).

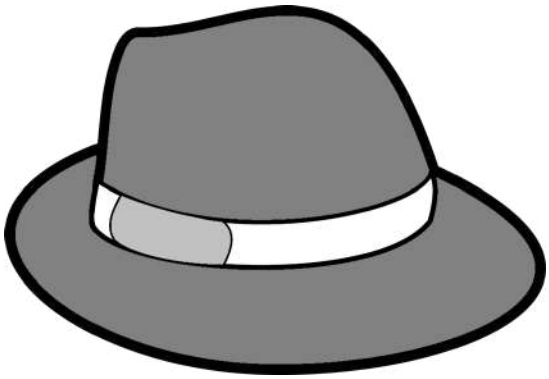


Figura 1.2

Aceste persoane sunt foarte mult axate sa invete, de multe ori ne mai gandindu-se la faptul ca fac lucrurile intr-un mod ilegal si complet non-etic (pe serverele, reteaua altcuiva fara acordul acelei persoane/organizatii).

Acum iti voi recomanda si tie, daca vrei sa inveti, fie sa-ti creezi tu proprile tale laboratoare de test in care inveti si testezi tot ce iti trece prin cap, fie iti cumperi (inchiriezi) diferite scenarii/laboratoare din Internet, fie te angajezi la o companie care sa iti ofere aceasta sansa, oportunitate astfel incat sa fi platit pentru a invata ;)
Eu am avut sansa asta, iti recomand si tie sa o incerci.

3) White Hat Hacker (aka. Ethical Hacker)

Spre deosebire de celelalte 2 categorii despre care am discutat pana acum, “White Hat Hackers” (ilustratie in figura 1.3) sunt Hackerii Etici (buni) care “sparg” anumite sisteme (retele, servere, laptop-uri, telefoane smart etc.) cu scopul de a descoperi vulnerabilitati pe care ulterior le vor anunta dezvoltatorului (sau administratorului) astfel incat sa le remedieze.

Figura 1.3

Acest tip de Hackeri, fie au fost la un moment dat “Black Hat”, fie au decis sa actioneze doar de partea binelui (intr-un format etic), astfel devenind si luptand pentru un Internet “mai curat”, fara incidente de securitate (asta fiind viziunea lor).

Acest tip de Hackeri mai pote fi numiti si “**Penetration Testers**” pentru ca ei, de fapt, asta fac, incearca sa penetreze (informatic) diferite sisteme (de securitate).

Acestia, fie lucreaza in modul freelancer (sunt liber profesionisti, colaborand cu diferite firme), fie sunt angajati intr-o firma. Ce vreau sa-ti spun cu asta este urmatorul aspect:

Pentru a putea face testele de penetrare (mai *pe romaneste Hackingul :))),* Hackerii etici trebuie sa aiba un contract care le ofera dreptul de a face asa ceva. Contractul trebuie sa fie intre ei si firma care doreste o astfel de testare (pe serverele sau reteaua lor), cu timeline-uri foarte clare (cand incepe testarea, in ce intervale de timp, pe ce zone ale companiei etc.), astfel incat sa nu fie pusa in pericol infrastructura informatica.

La sfarsitul pentestului se genereaza un **raport** (cu vulnerabilitatile gasite) care se va inmana persoanei responsabile din organizatie.

II. Concepte fundamentale despre Linux

Inainte de a trece sa discutam despre partea de Securitate si sa intram in detalii tehnice este foarte important sa ne asiguram ca intelegem elementele de baza ale acestui domeniu. Fara acestea nu vom putem acumula informatia necesara pentru a lucra cu sistemele sau a profesa in domeniu. Datorita acestui fapt, in acest capitol (si in urmatorul) vom discuta despre partea de Linux, Servere si Retele de Calculatoare. Conceptele discutate reprezinta minimul necesar acestui subiect pentru a putea merge mai departe.

Scurta introducere in Linux si linia de comanda

Aceasta sectiune iti va explica in detaliu ce este Linux si cum acest sistem de operare poate deveni cel pe care tu il folosesti cel mai mult. De fapt, termenul de “sistem de operare” nu este tocmai corect pentru a defini Linux (el este un kernel, un nucleu care face legatura cu componentele hardware), dar putem sa il numim astfel pentru o mai usoara intelegere a ceea ce acesta face si cum functioneaza.

Ce este Linux?

Linux este nucleul (kernelul) care sta la baza unei familii de sisteme de operare extrem de larga la nivel global. Linux este kernelul care “alimenteaza” in ziua de astazi sisteme de operare precum:

- Ubuntu (pentru sisteme desktop),
- Android (pentru smartphone-uri, pentru smartwatch-uri, pentru software-ul masinii etc.),
- Kali Linux (Hacking si Penetration Testing),
- CentOS (pentru partea de servere), etc.

Linux a avut ca inspiratie un alt sistem de operare si anume Unix, extrem de popular in anii ’80. Unix reprezinta o alta familie de sisteme de operare, similara cu Linux. Sisteme de operare care au la baza Unix sunt:

- macOS – OS-ul de la Apple pentru laptop-uri si Desktop-uri
- iOS – OS-ul de la Apple pentru smartphone-uri si tablete
- IBM – o parte din software-urile de la IBM sunt construite pe Unix
- pfSense – cel mai folosit firewall OS pentru securizarea retelelor

Revenind la Linux, el ca software a fost lansat in anii ’90 de catre Linus Torvalds. Poti gasi mai jos un documentar despre intreaga poveste a acestuia si cum este el inspirat din UNIX. https://www.youtube.com/watch?v=XMm0HsmOTFI

Ceea ce il face deosebit este gratuitatea, modularitatea si faptul ca oricine il poate modifica. Utilizatorii ce detin cunostintele necesare de programare ii pot adauga elemente si chiar schimba interfata grafica, facandu-l un sistem personalizat de operare.
Linux sta la baza altor sisteme de operare si interactioneaza direct cu hard-ul. Dar vei vedea in video cum functioneaza un kernel si de ce alte sisteme Linux se ajuta pentru a face calculatorul sa functioneze.

Unul dintre cele mai raspandite sisteme de operare, mai ales cand vine vorba de servere, Linux este considerat foarte stabil, fiind folosit de multi programatori si specialisti in IT. Il poti folosi chiar daca nu esti un expert in domeniu deoarece este complet gratuit si deloc greu de stapanit.

De ce este folosit Linux?

Si acum hai sa vedem de ce Linux este utlizat de atat de multa lume si in ce se foloseste el mai exact. O sa fii surprins sa afli pe ce fel de dispozitive poate fi instalat si functiona intr-un mod cat mai eficient. O parte din motivele principale pentru care Linux este atat de folosit sunt:

- Pentru ca este Gratuit – oricine il poate downloada, instala si folosi
- Pentru ca este customizabil – se poate face orice intrand in codul sursa, schimband chiar elemente din kernel
- Pentru ca este Open Source – sursa lui se afla pe un server de stocare, oricine putand lucra la codul sursa si face adaugiri. Are sute de mii de contribuitori, incluzand Microsoft, care contribuie la imbunatatirea lui.

Unde este Linux folosit?

Cand vorbim despre unde poate fi Linux folosit, afla ca in functie de ceea ce ai nevoie, sisteme de operare dezvoltate din el pot fi instalate pe:

- Desktop
- PC-uri
- Laptopuri
- Smartphonuri si tablete
- Device-uri IoT
- Mai ales servere

De fapt, peste 80% din servere folosesc Linux deoarece are mult mai putine vulnerabilitati decat Windows-ul. Contribuitorii la acest kernel gratuit nu se grabesc sa lanseze un produs nou si sa incaseze castiguri din munca lor, ceea ce inseamna ca eforturile investite in imbunatatirea Linux sunt facute in mod natural si de catre cei care se confrunta cu orice fel de probleme de securitate si functionare, zi de zi.
Daca ai Android pe telefon sau tableta , te folosesti automat de Linux pentru ca acest sistem de operare este facut in totalitate in kernelul despre care eu vorbesc aici. Multi decid sa il instaleze deoarece consuma resurse foarte putine, ceea ce este un avantaj imens fata de celelalte sisteme. Sa nu mai vorbesc de cat de stabil si rapid poate fi, in special cand folosit din linia de comanda.

Iata o lista cu 10 lucruri pe care le poti face cu Linux

1. Utilizarea Linux ca sistem de operare pentru calculatorul personal sau server.
2. Administrarea sistemului de operare si a server-ului prin intermediul liniei de comanda sau a interfetei grafice de utilizator.
3. Instalarea si administrarea aplicatiilor open-source, cum ar fi LibreOffice sau Firefox.
4. Crearea si administrarea bazelor de date, cum ar fi MySQL sau PostgreSQL.
5. Utilizarea Linux pentru programare, prin intermediul limbajelor de programare precum Python, C sau Java.
6. Utilizarea Linux pentru crearea de site-uri web si aplicatii web, prin intermediul aplicațiilor precum Apache sau Nginx.
7. Crearea si administrarea de retele, prin intermediul aplicatiilor precum iptables sau OpenVPN.
8. Utilizarea Linux pentru creativitate digitala si editare video prin intermediul aplicatiilor precum GIMP sau Blender.
9. Utilizarea Linux pentru crearea de jocuri prin intermediul aplicatiilor precum Unity sau Unreal Engine.
10. Utilizarea Linux pentru automatizarea proceselor prin intermediul scripturilor shell sau a aplicatiilor precum Ansible sau Puppet

Cum sa instalezi Linux?

In acesta sectiune vom incepe discutia despre lucrul in Sistemul de Operare (OS) Ubuntu bazat pe kernelul Linux. In cele ce urmeaza vom face primii pasi in lumea acestui minunat OS si vom invata cum sa-l instalam pe PC-ul nostru, care sunt pasii de urmat in procesul de instalare, lucrul de zi cu zi in Ubuntu, iar la sfarsit vom intra chiar si in Terminal (arma secreta a acestui OS) si vom da cateva comenzi de baza.

1) Pregatirea pentru Instalarea Linux

In acest clip trecem , pas cu pas, prin procesul de setare si instalare a unei masini virtuale in VirtualBox pe Windows. Eu folosesc Distributia de Linux, Ubuntu. Programul care face posibila virtualizarea se numeste VirtualBox. Acesta este dezvoltat de catre Oracle si il gasesti gratuit accesand urmatorul link: https://www.virtualbox.org
O alternativa a acestui program este softul de virtualizare de la VMware si anume Workstation sau Player (gratuit) pentru Windows/Linux si Fusion pentru macOS. In aceste tutoriale eu folosesc VirtualBox deoarece este o solutie relativ stabila si gratuita, astfel il poti descarca si tu de la link-ul de mai sus si te poti juca cu orice OS doresti (fie ca este vorba de Windows XP/7/8.1/10/11 sau orice alta distributie de Unix sau Linux).

Cum sa folosesi Linux fara sa-l instalezi?

In cazul in care nu vrei sa instalezi Linux, poti sa te folosesti de el intrand aici:

- https://www.onworks.net/
- https://www.tutorialspoint.com/linux_terminal_online.php

Dupa 10 minute in care nu folosesti Linux pe acest site, sesiunea va fii oprita. Joaca-te cu acestea si testeaza.

2) Procesul de instalare al Linux

In general instalarea unui Sistem de Operare (Windows, Linux, macOS etc.) nu este complicata. Selectezi cateva optiuni, Next, Next, Finish si gata ! Exact asa este si cand vine vorba de instalarea Ubuntu. Pentru inceput iti alegi:
a) Limba in care doresti sa lucrezi

Dupa care este timpul:
b) Sa partitionezi Hard Disk-ul (adica sa alegi ce dimensiune vrei sa aloci pentru Ubuntu (/), pentru utilizator (/home) etc.),
c) Sa alegi locatia (care iti va seta si data si ora specifica)
d) Iar la sfarsit vei definii un Username si o Parola.
Pentru a face lucrurile mai simple pentru tine, iti recomand sa urmaresti tutorialul acesta.
In acest clip trecem, pas cu pas, prin procesul de instalare a OS-ului Ubuntu intr-o masini virtuale in VirtualBox.

3) Lucrul de zi cu zi in Linux

Dupa cum spuneam si la inceputul acestei sectiuni, Ubuntu este cea mai populara forma (distributie) de Linux, existenta la ora actuala, iar eu o voi folosii pe tot parcursul acestor sectiuni. In clip-ul de mai jos vorbim despre cum arata interfata grafica (GUI) din Ubuntu, testam cateva programe si vorbim pe scurt despre modurile in care putem instala acest OS pe PC/Laptop:

a) Mod Dual-Boot – exista in paralel Windows si Ubuntu, dar alegi unul din aceste 2 OS-uri in momentul in care pornesti calculatorul
b) Folosind o Masina Virtuala – eu prefer acest mod deoarece este mult mai simplu de folosit si instalat. In clip-urile viitoare iti voi arata cum poti sa instalezi un OS intr-o astfel de masina virtuala.
c) In Cloud - instalata pe serverele Amazon, Google, Microsoft, Digital Ocean, etc. E mai simplu si usor sa folosesti aceasta metoda. Necesita un abonament lunar pentru asta, dar pe masura ce incepi sa castigi experienta si sa lucrezi la un nivel mai avansat si profesionist, merita.

Comenzi de Baza in Terminalul Linux

A sosit momentul sa folosim elementul de baza care face orice distributie Linux (printre care si Ubuntu) populara si anume Terminalul. Acesta este o unealta foarte puternica, datorita functionalitatii (putem manipula sistemul mai bine fata de modul grafic) si al flexibilitatii pe care il ofera.

In acest terminal noi folosim shell-ul, un program care ia comenzile (ls, cd, pwd etc.) si le trimite mai departe OS-ului care se va ocupa de procesarea lor si intoarcerea rezultatului.

Shell-ul default (si in acelasi timp, cel pe care il folosim si noi) din Ubuntu este “bash“. Bash ne permite sa dam toate aceste comenzi si el incearca sa raspunda cu un rezultat pentru fiecare comanda introdusa de noi.

Iata cateva comenzi de baza din Linux pe care un incepator ar trebui sa le cunoasca:
1. ls: listarea fisierelor si directoarelor din directorul curent
2. cd: schimbarea directorului curent
3. mkdir: crearea unui nou director
4. touch: crearea unui fisier gol
5. rm: stergerea unui fisier sau director

6. cp: copierea unui fisier sau director
7. mv: mutarea unui fisier sau director
8. cat: afisarea continutului unui fisier
9. grep: cautarea unui sir de caractere intr-un fisier
10. sudo: obtinerea drepturilor de super-utilizator

Este important sa fie folosite cu atentie, in special comenzile de stergere (rm) si cele care necesita drepturi de super-utilizator (sudo), aka root. Pentru a afla mai multe despre aceste comenzi sau despre altele, puteti folosi man (manual) pentru a accesa documentatia. De exemplu, pentru a accesa documentatia comenzii ls, puteti folosi man ls.

```
$ls                     //listeaza continutul folder-ului curent

$cd Desktop/            //schimba folderul in care ne aflam
```

Toate aceste comenzi ne intorc un rezultat. In cazul in care am fi introdus comanda $hellothere, bash, by default, nu ar fi stiut de ea si ne-ar fi intors un mesaj de eroare, cum ca acesta comanda nu exista.
Alte comenzi utile:

```
$pwd            //ne indica unde ne aflam in toata structura de foldere

$echo "text"    //va afisa la consola cuvantul Text, il poti folosi pentru
a "printa orice cuvant doresti"

$whoami         // indica cu ce username esti logat pe Linux
```

Lucrul cu Fisiere in Ubuntu

Hai sa o luam cu inceputul. **Cum sa folosesti comenzile de mai sus?**

iata cateva exemple specifice pentru fiecare dintre comenzile de baza din Linux:

1. **ls**: Listarea fisierelor si directoarelor din directorul curent
   - ls: listarea fisierelor si directoarelor din directorul curent
   - ls -l: listarea fisierelor si directoarelor in format lung (permisiuni, proprietar, dimensiune, etc.)
   - ls -a: listarea tuturor fisierelor si directoarelor (inclusiv cele ascunse) din directorul curent

2. **cd**: Schimbarea directorului curent
   - cd Desktop: schimbarea directorului curent in "Desktop"
   - cd ..: schimbarea directorului curent in directorul parinte (directoriul care contine directorul curent)

3. **mkdir**: Crearea unui nou director
   - mkdir nou_director: crearea unui director numit "nou_director"

4. **touch**: Crearea unui fisier gol
   - touch nou_fisier.txt: crearea unui fisier gol numit "nou_fisier.txt"

5. **rm**: Stergerea unui fisier sau director
   - rm fisier.txt: stergerea fisierului numit "fisier.txt"
   - rm -r director: stergerea directorului numit "director" si a tuturor fisierelor si directoarelor continute in interiorul sau

6. **cp**: Copierea unui fisier sau director
   - cp fisier.txt fisier_copie.txt: copierea fisierului "fisier.txt" intr-un fisier nou numit "fisier_copie.txt"
   - cp -r director director_copie: copierea directorului "director" si a tuturor fisierelor si directoarelor continute in interiorul sau intr-un nou director numit "director_copie"

7. **mv**: Mutarea unui fisier sau director
   - mv fisier.txt director/: mutarea fisierului "fisier.txt" in directorul "director"
   - mv director/ director_nou/: redenumirea directorului "director" in "director_nou"

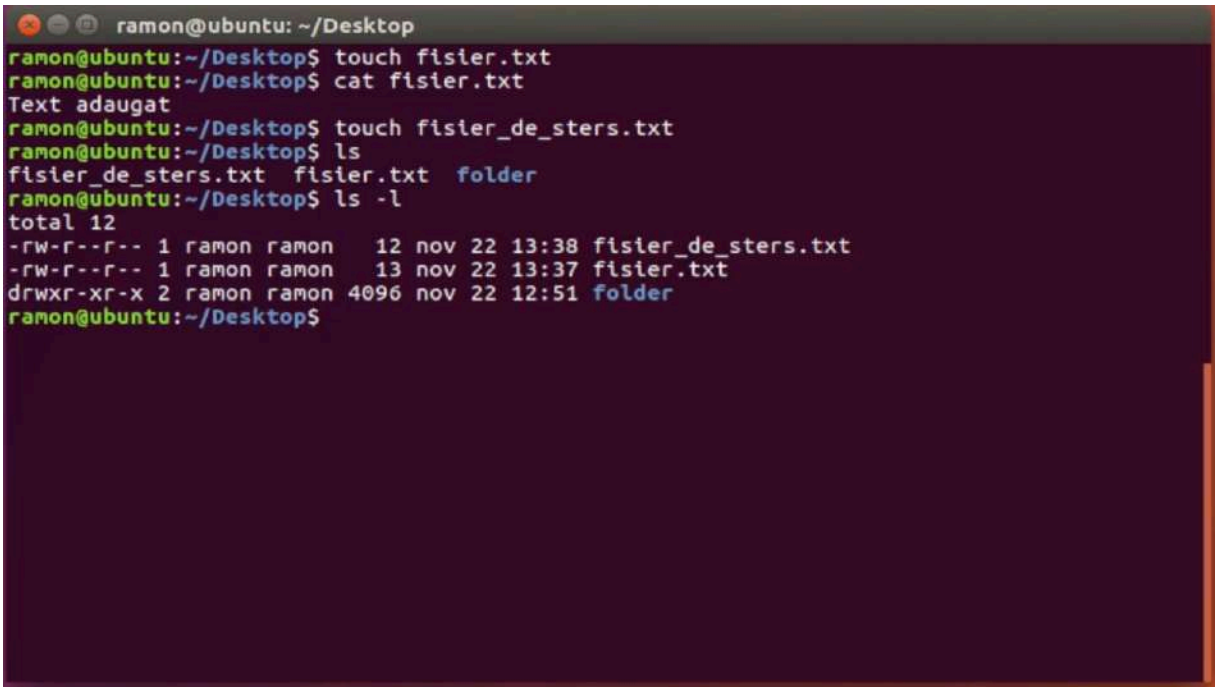
8. **cat**: Afisarea continutului unui fisier
   - cat fisier.txt: afisarea continutului fisierului "fisier.txt"

9. **grep**: Cautarea unui sir de caractere intr-un fisier
   - grep "cuvant" fisier.txt: cautarea sirului de caractere "cuvant" in fisierul "fisier.txt"

10. **sudo**: Obtinerea drepturilor de super-utilizator
    - sudo apt-get update: actualizarea listei de pachete disponibile in sistem (in distributiile bazate pe Debian/Ubuntu)
    - sudo systemctl restart apache2: repornirea serverului web Apache (daca este instalat si activat in sistem)

1) Crearea unui fisier

Pentru inceput sa vedem cum putem crea un fisier folosind terminalul in Ubuntu. Pentru a face asta trebuie sa aplicam urmatoarea comanda:
#**touch** file1.txt
Dupa cum poti sa vezi acest proces este unul extrem de simplu, la fel de simple vor fi si urmatoarele.



2) Vizionarea continutului fisierelor

Pentru a vedea continutul unui fisier avem mai multe optiuni (in functie de ce locul si informatia pe care o dorim).

#**cat** file1.txt

Comanda #***cat*** (care provine de la concatenate) ne va afisa in Terminal tot continutul fisierului, indiferent de numarul de linii pe care il are acesta. Pe langa aceasta comanda mai avem si altele care ne pot ajuta ***sa filtram rezultatul afisat***.

#**head** file1.txt

#**tail** file1.txt

Comanda #***head*** ne va arata primele *10 linii din fisier* (by default), iar comanda #***tail*** ne va afisa ultimele 10 linii din fisier. Daca adaugam argumentul **-n**, putem specifica cate linii dorim sa vedem:

#**head -n 4** file1.txt

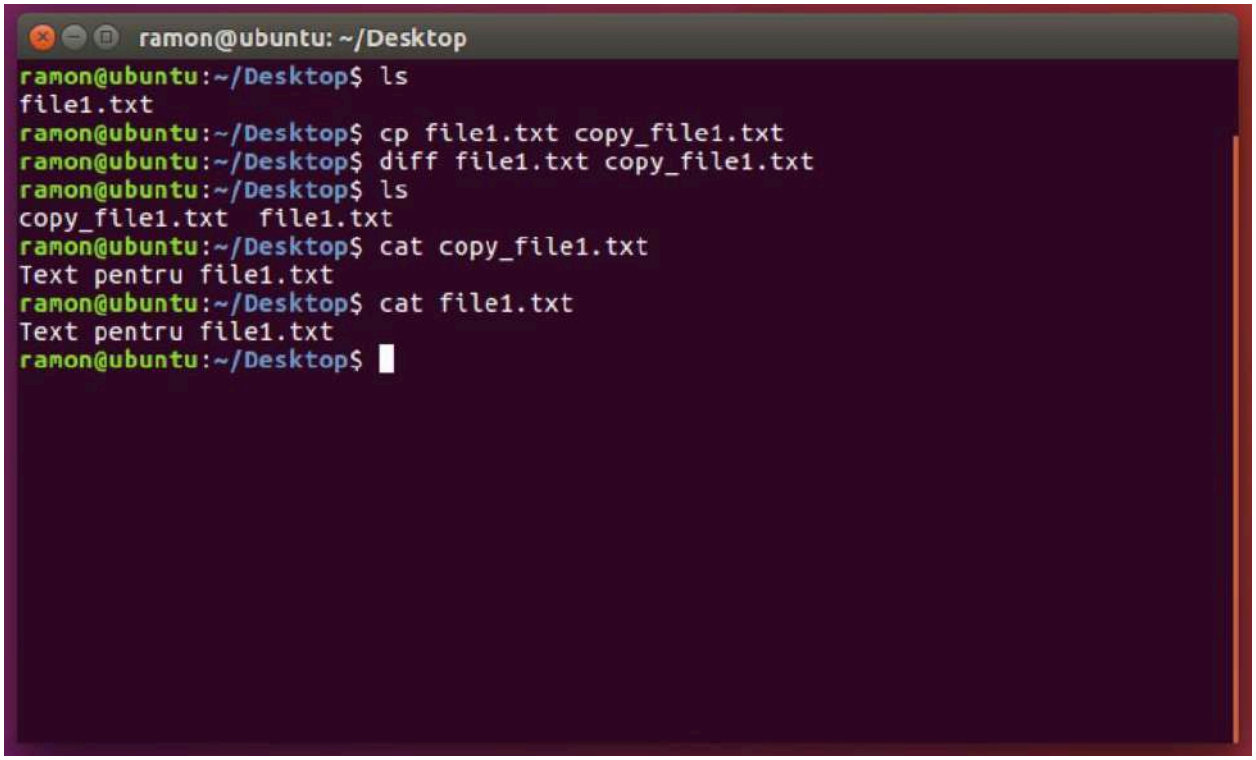
#**tail -n 4** file1.txt

Mai avem o optiune destul de interesanta pentru a vedea fisierul intr-un mod mai ordonat si segmentat. Aceasta comanda este:

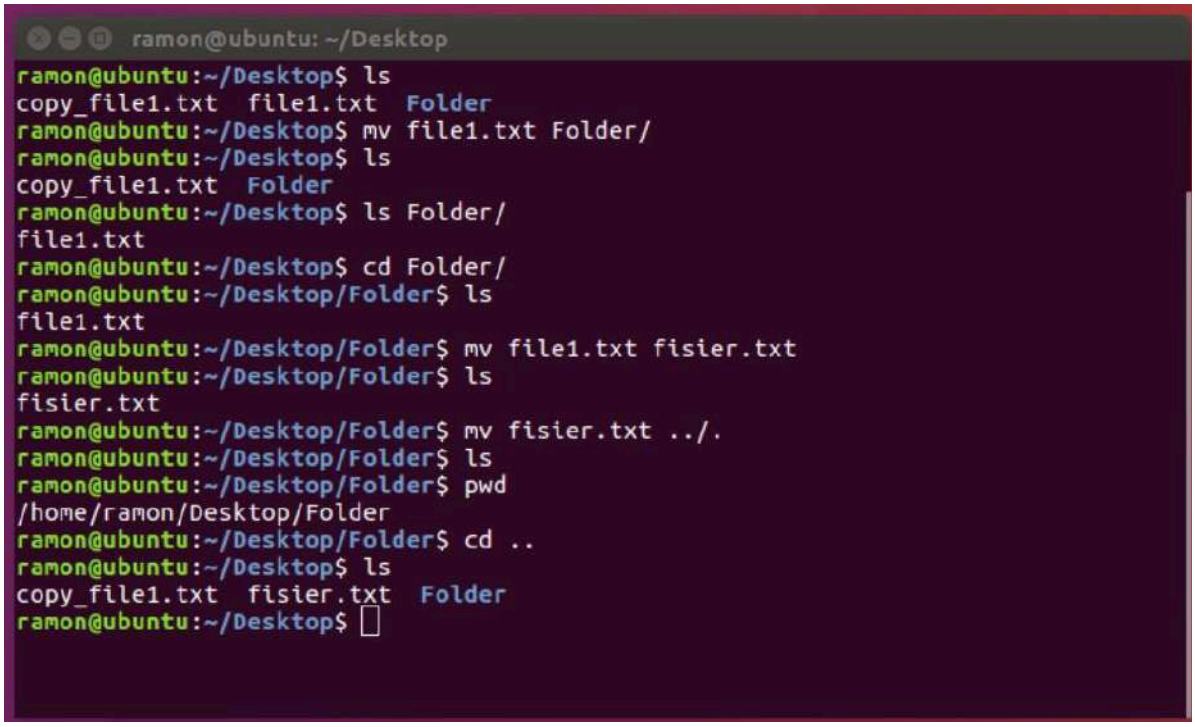
#**more** file1.txt

3) Copierea, Mutarea si Redenumirea fisierelor

Cand vine vorba de copierea, mutarea sau redenumirea unui fisier avem la dispozitie urmatoarele comenzi:
#**cp** file1.txt copy_file1.txt



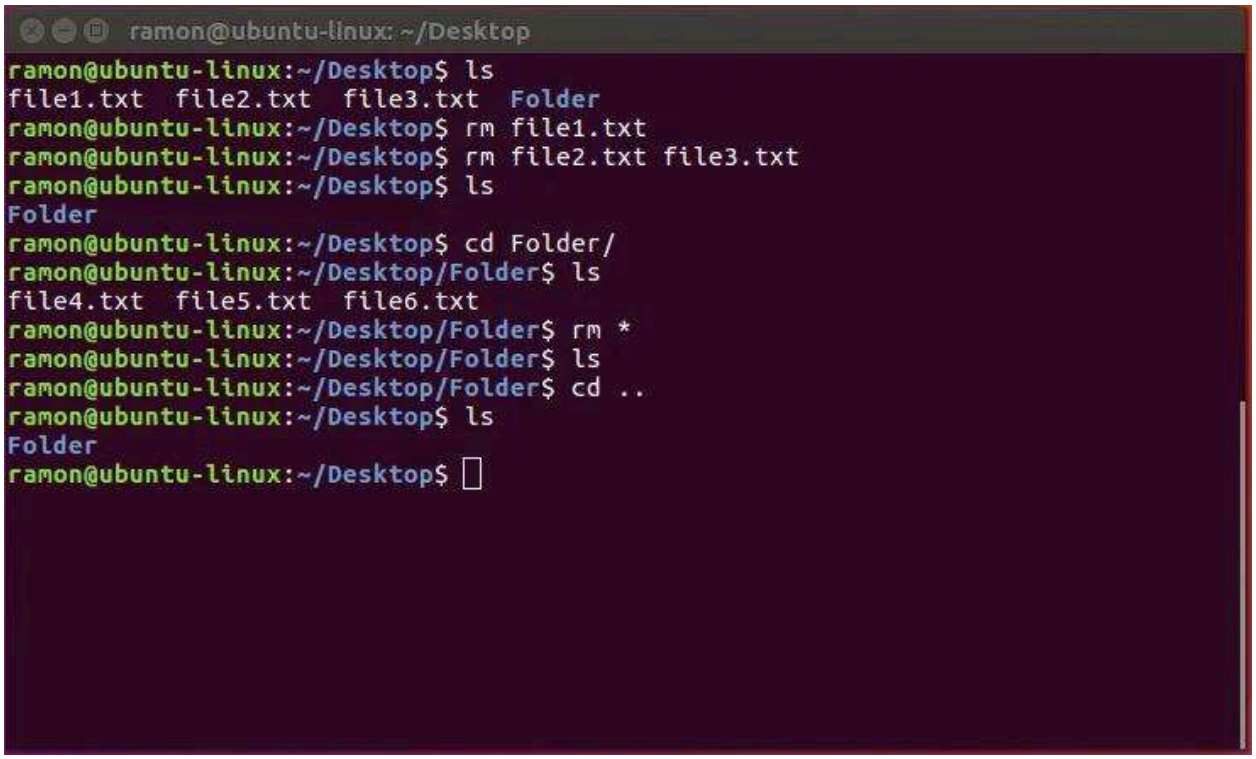
Dupa cum poti vedea, in exemplul de mai sus am folosit comanda "***#diff*** *file1.txt copy_file1.txt*". Aceasta comanda compara cele 2 fisiere si daca exista diferenta intre acestea le va afisa. In cazul de fata fisierele sunt identice, deci aceasta nu ne va afisa nimic.
#**mv** file1.txt Folder/
#**mv** file1.txt fisier.txt



Prima comanda va muta fisierul "*file1.txt*" de pe Desktop in folderul "Folder", iar cea de a 2 a comanda va redenumi fisierul nostru intr-un fisier cu numele "*fisier.txt*".

4) Stergerea fisierelor

Cand vine vorba de stergerea unui fisier lucrurile sunt extrem de simple (la fel ca si celelalte operatii discutate pana acum):
#**rm** file1.txt
#rm file2.txt file3.txt
#rm *



Prima comanda va sterge fisierul "*file1.txt*", cea de a 2-a va sterge ambele fisiere, iar cea de a 3-a **(*#rm **) va sterge tot continutul dintr-un folder.**

Lucrul cu Foldere (Directoare) in Ubuntu

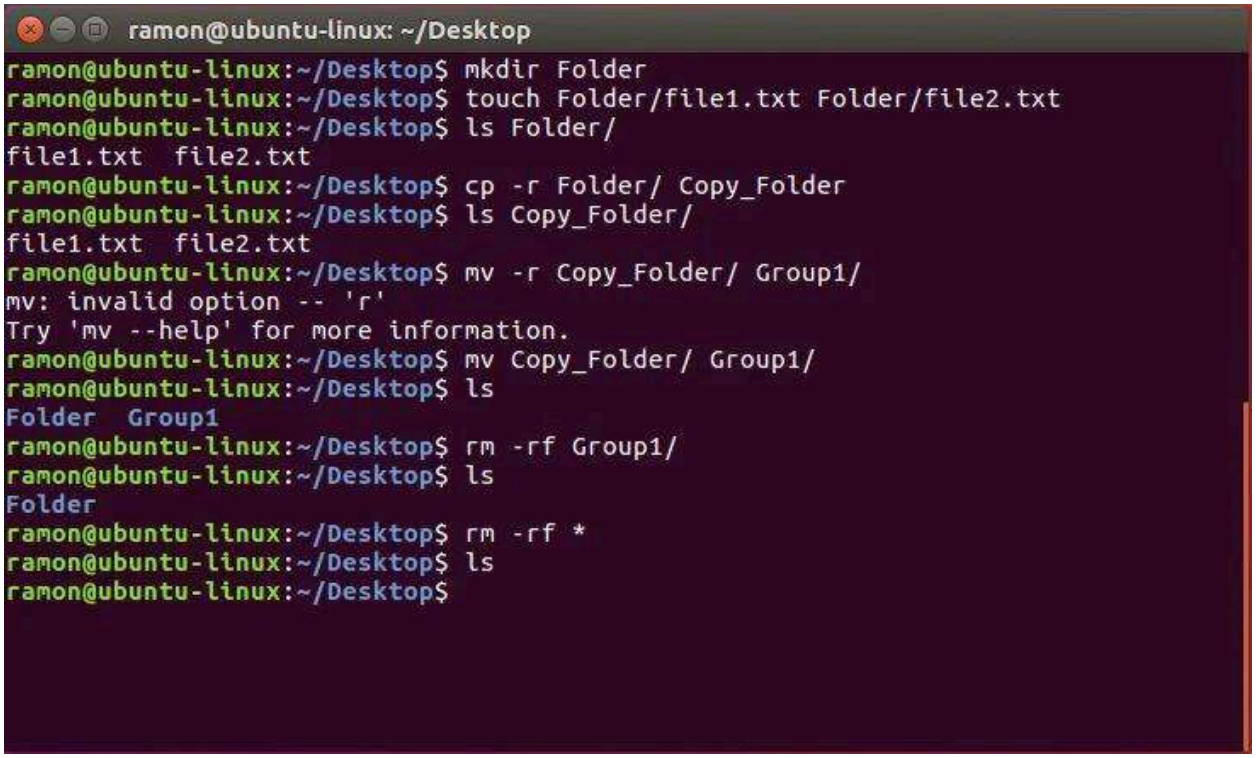
In aceasta sectiune vom vorbi despre Foldere, si mai exact cum putem crea, copia, muta, redenumii si sterge unul sau mai multe foldere.

1) Crearea unui Folder

Pentru a crea un folder din Terminal trebuie sa dam urmatoarea comanda:
#**mkdir** Folder
Atat! E un procedeu extrem de simplu (la fel ca si celelalte discutate pana acum). Singura "problema" cu toate aceste comenzi este: in ciuda faptului ca sunt simple si relativ usor de retinut, ele incep sa se adune, incep sa fie din ce in ce mai multe comenzi care trebuiesc tinute minte. *Singurul mod prin care le poti retine este sa pui in practica !*

2) Copierea, Mutarea si Redenumirea Folderelor

Pentru a copia un folder (impreuna cu continutul lui) vom folosi tot comanda ***cp***, la care vom adauga argumentul ***-r***:
#**cp -r** Folder/ Folder2/
De asemenea, mutarea si redenumirea se fac prin folosirea comenzii #***mv*** la care adaugam argumentul ***-r***:
#**mv -r** Folder/ Folder2/ *//va muta Folder in Folder2*
#**mv** Folder/ Group1/ *//va redenumi folderul*



3) Stergerea unui Folder

Pentru a sterge un folder impreuna cu tot continutul lui, trebuie sa execum urmatoarea comanda:
#**rm -rf** Folder/

Aceasta comanda il va sterge cu totul de pe disk:
-r = executa recursiv comanda (pe tot continutul folderului)

-f = forteaza stergerea

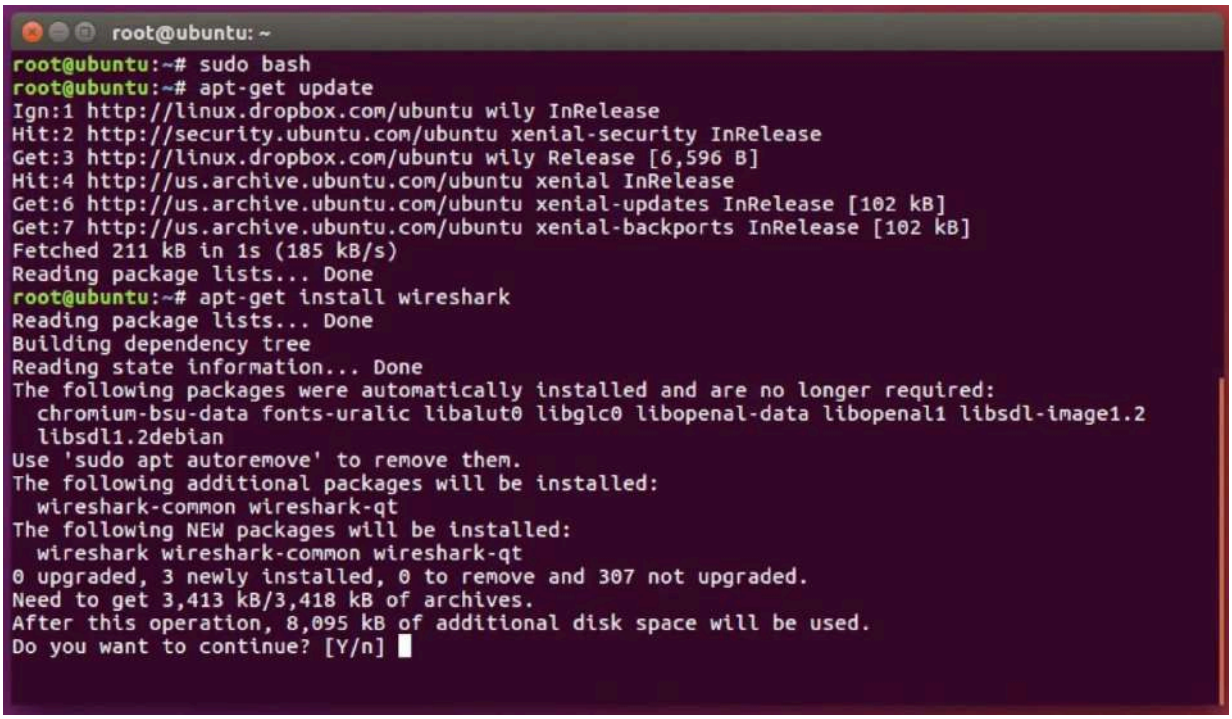
Utilitare in Linux care iti pot face "viata mai usoara"

Instalarea unui program din Terminal - APT-GET

Pentru a instala un program din terminalul Ubuntu Linux putem folosi programul "***apt-get" (sau doar "apt")***. Acest program este existent pe marea majoritatea a distributilor care au la baza **Debian** (ex: Ubuntu, Xubuntu, Kubuntu, Linux Mint, Knoppix, etc). Iata cum il putem folosi:

Exemplu: sa presupunem ca numai ce ne-am instalat Ubuntu si vrem sa instalam un program de captura de trafic din retea (ex: *Wireshark*). Tot ce trebuie sa facem este sa folosim urmatoarea comanda (si sa urmam procesul de instalare):

#**apt-get install wireshark**



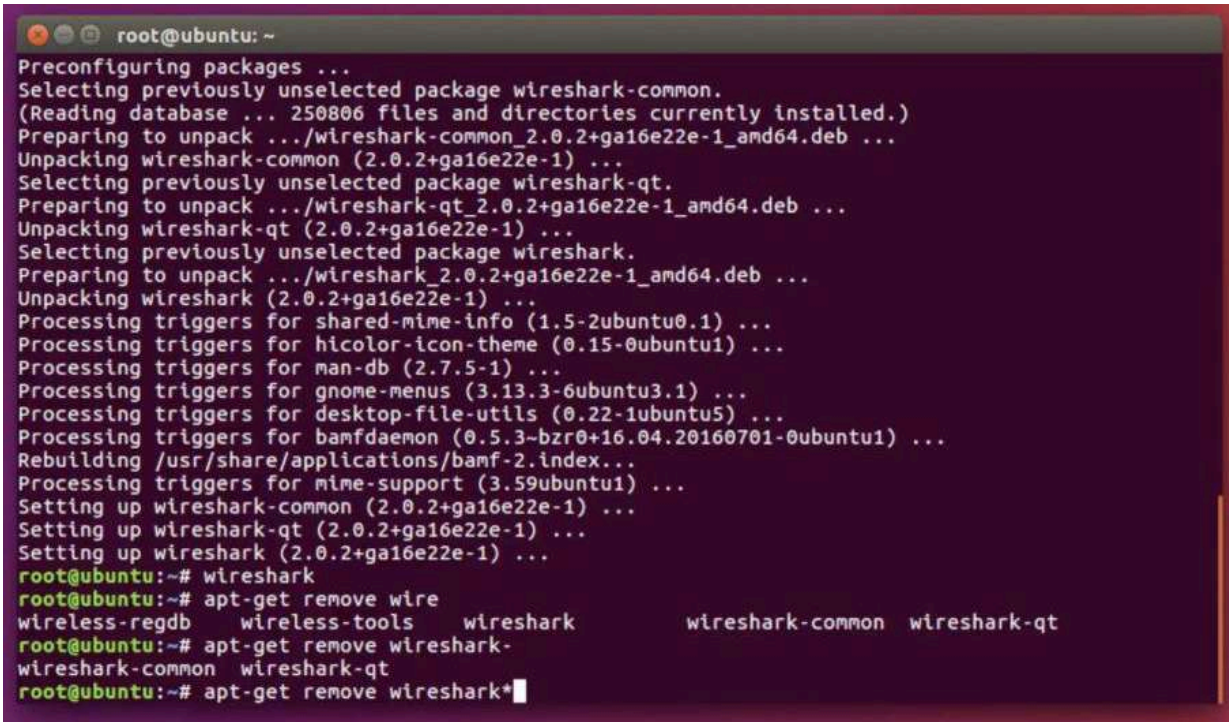
Acum, programul a fost instalat si il putem folosi astfel:

#**sudo wireshark**

Astfel se va deschide programul cu care putem captura traficul din retea. Daca dorim sa dezinstalam programul vom folosi urmatoarele comenzi:

#**apt-get remove wireshark**

#**apt-get purge wireshark** //sterge si dependintele programului



In exemplul de mai sus, poti vedea ca am instalat **Wireshark**. Ei bine, in momentul instalarii acestui program au fost **instalate si alte programe** pentru a-l putea rula cu succes pe masina Linux. Daca dorim sa-l *dezinstalam* este clar ca **nu avem nevoie** si de *programele auxiliare* instalate, astfel putem folosi * pentru a sterge si aceste programe ca in exemplul de mai jos:

#**apt-get remove** *wireshark**

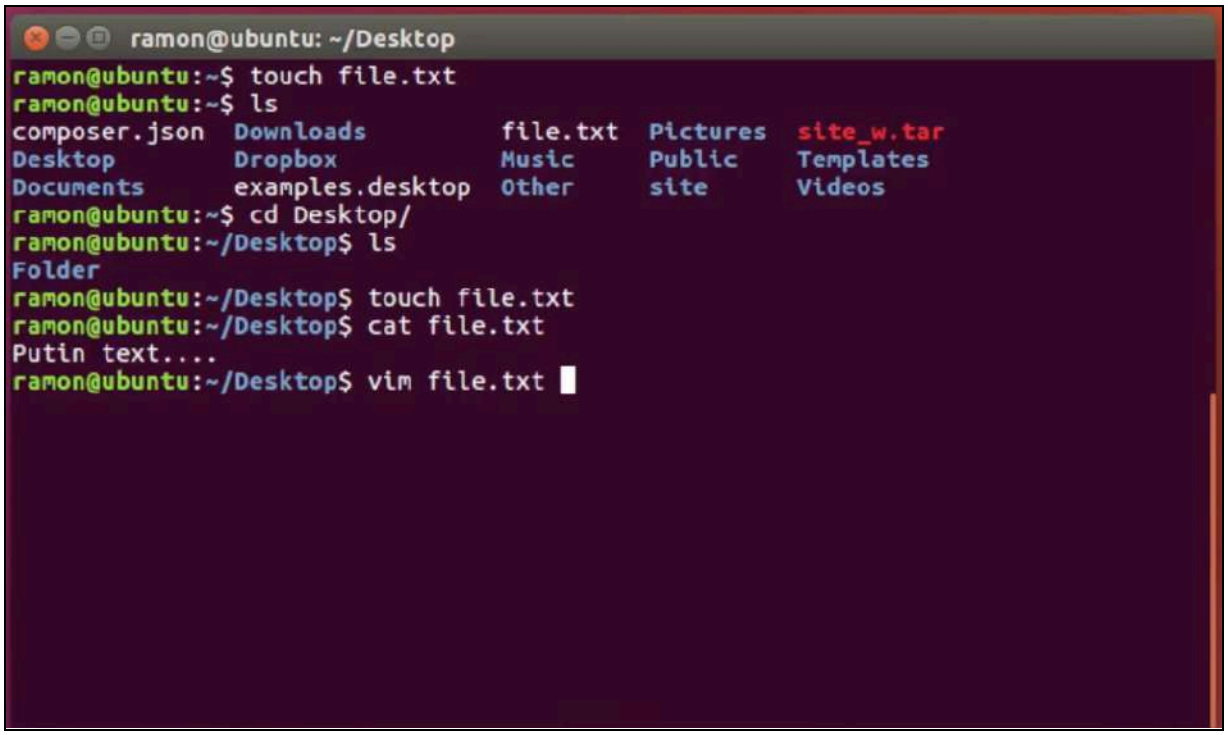
Pe langa **APT-GET**, **exista** si alte utilitare in Linux (mai exact distributile bazate pe Debian) care ne pot ajuta sa instalam programe:

- **Aptitude** (#aptitude install/remove ...)
- **DPKG**

Cum editez un fisier din terminalul Ubuntu Linux cu VIM

In orice distributie Linux vom interactiona cu **fisiere - acestea trebuie create, sterse** sau editate. Defapt, totul in Linux este un fisier si astfel trebuie sa stim cum sa le putem manipula. In sectiunea trecuta am vazut cum putem face diferite operatii cu fisier, iar acum a venit timpul sa vedem cum le putem si edita/modifica.Programul pe care il vom folosi se numeste **VIM** si este un editor text pe care *il putem folosi din* **CLI** (linie de comanda). Asta ne ofera **rapiditate si flexibilitate** cand vine vorba de administrarea unui sistem, modificare fisierelor de configurare etc. In primul rand pentru a putea folosi VIM, trebuie sa instalam programul:
#**apt-get install vim**

In al doilea rand trebuie sa ne alegem un fisier pe care dorim sa-l accesam si sa intram in el pur si simplu:
#**vim fisier.txt**

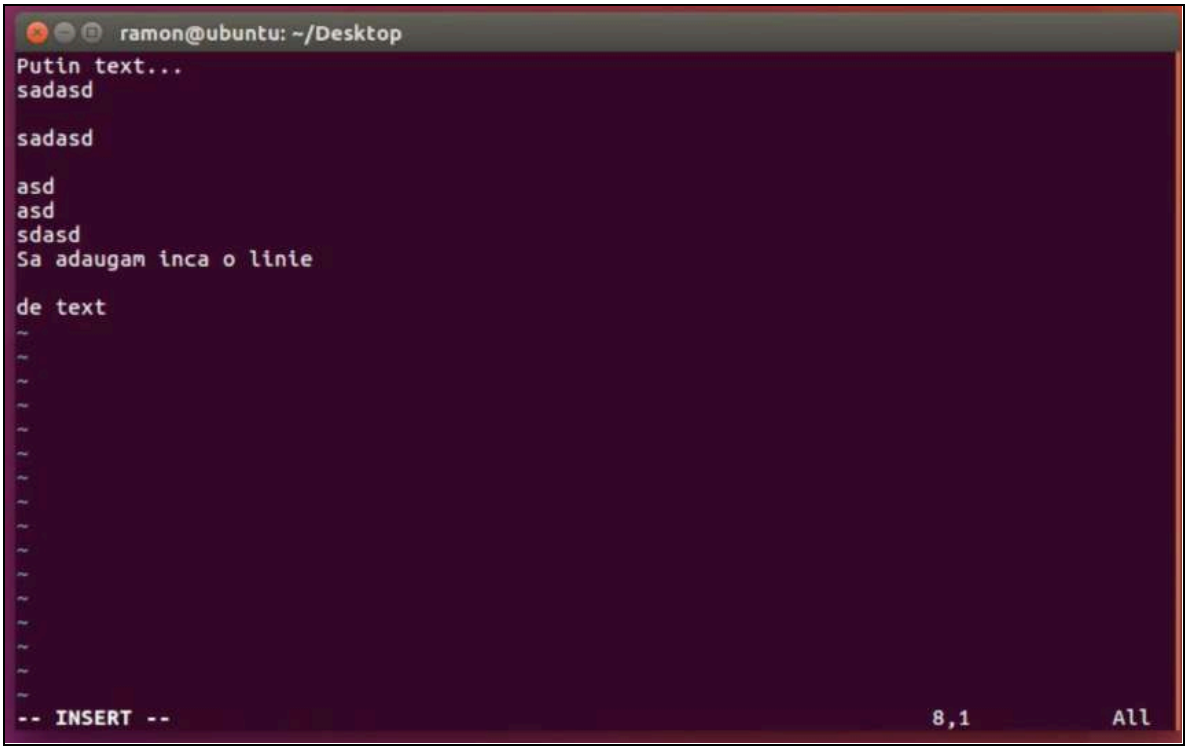


Acum am intrat in acest fisier unde avem urmatoarele optiuni:

- **Vizualizarea** (continutului) fisierului fara a-l modifica (*"miscandu-ne"* folosind *"sagetile"*
- **Modificarea** acestuia (apasand tasta **i** si introducand textul dorit)
- Iar la final **Save & Exit** sau doar **Exit fara salvarea modificarilor** facute

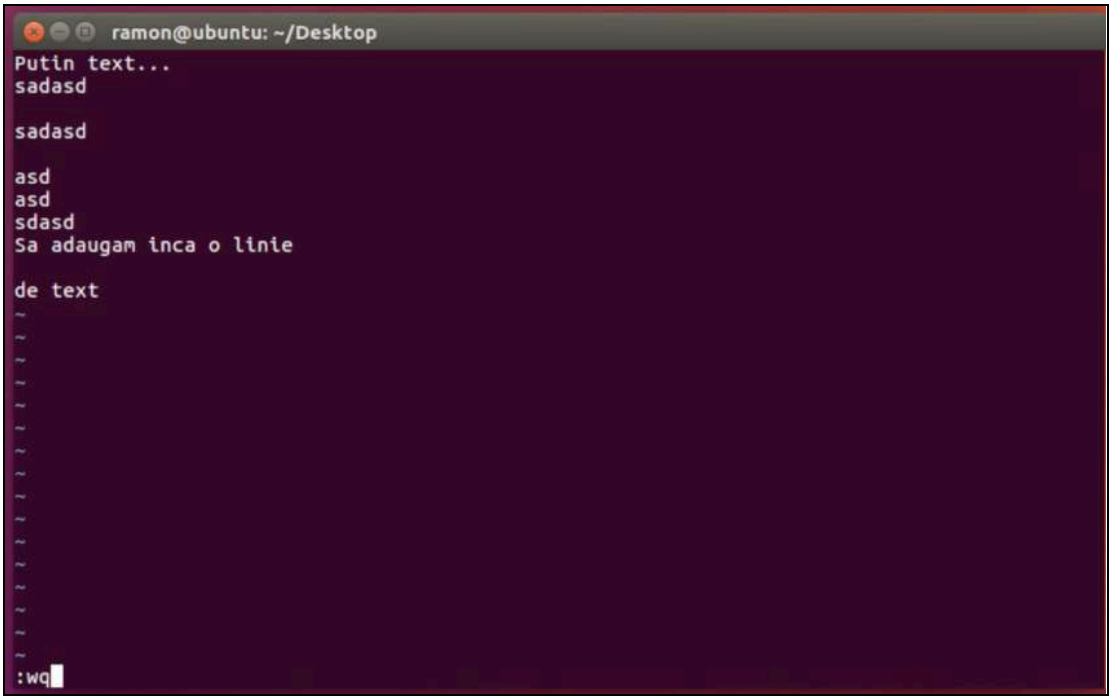
Totul simplu si usor pana aici :) Dar partea grea vine in momentul in care ne-am terminat treaba si dorim sa iesim din fisier (implicit si din editor).

Dupa cum spuneam si mai devreme, tasta **i** ne va duce in modul "**INSERT**" care ne permite sa facem modificari in fisier.

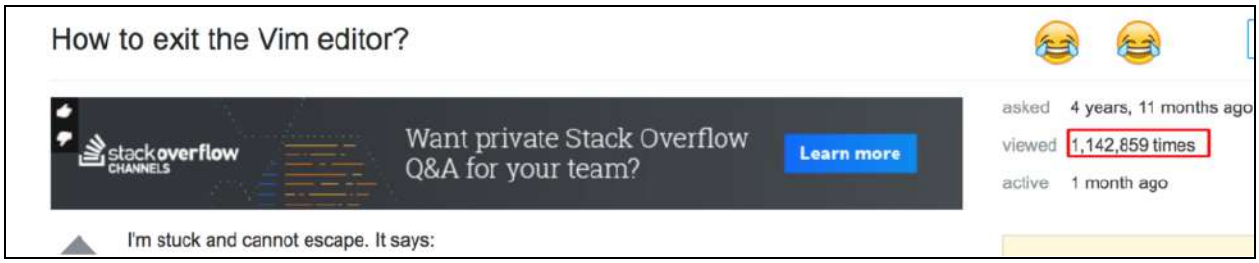


Acum daca vrem sa iesim din fisier trebuie sa urmam procedura:

1. Apasa **ESC**
2. Scrie **:q** (daca vrei *exit* din fisier)
3. Sau **:wq** (daca vrei *save & exit*)
4. Sau **:q!** (daca vrei *exit fara salvarea modificarilor*)



Iar pe langa asta, o mica gluma, iata cate persoane au avut probleme sa iasa din VIM :))



Pe scurt, despre ce este un Server

Un server este un calculator sau un sistem de calculatoare care ofera servicii de retea la alte calculatoare sau dispozitive conectate la acea retea. Acestea pot include servicii de stocare, imprimare, gazduire web, autentificare, gestionare a bazelor de date sau orice alte servicii necesare pentru a sustine activitatile utilizatorilor. Un server poate fi fizic sau virtual, si poate functiona folosind diferite sisteme de operare, cum ar fi Windows sau Linux. Acesta nu (mai) este un echipament foarte mare care costa foarte mult si care e greu de setat. Chiar si un ceas inteligent poate sa devina un server. Pana si frigiderul smart poate fi unul. Spre exemplu, Routerul tau Wireless de acasa contine un server care ofera acces la un serviciu Web. Practic un site intern, gazduit de Router care foloseste ca un mod de configurare al echipamentului.

Iata 10 tipuri de servere pe care le poti intalnii in situatii (destul de) dese:

1. **Serverul de fisiere:** stocheaza si gestioneaza fisierele utilizatorilor, permitand accesul la acestea de la mai multe computere sau dispozitive.
2. **Serverul de imprimare:** gestioneaza imprimantele conectate la retea si distribuie documente la acestea.
3. **Serverul de gazduire web:** gazduieste site-uri web si le face accesibile prin intermediul internetului.
4. **Serverul de autentificare:** verifica identitatea utilizatorilor si permite accesul la serviciile de retea.
5. **Serverul de baze de date:** stocheaza, gestioneaza si ofera acces la baze de date.
6. **Serverul de aplicatii:** ruleaza programe sau aplicatii specifice pentru utilizatori si le ofera acces la acestea prin intermediul retelei.
7. **Serverul de mail:** gestioneaza si livreaza mesajele de e-mail.
8. Serverul de streaming media: transmite continut media, cum ar fi muzica sau videoclipuri, prin intermediul retelei.
9. **Serverul de backup:** stocheaza copii de siguranta ale datelor de pe alte servere sau computere.
10. **Serverul de virtualizare:** permite crearea si gestionarea mai multor sisteme virtuale pe un singur server fizic.

Spre exemplu, in momentul in care ne conectam la google.ro, calculatorul/telefonul nostru apeleaza la serverul lor web pentru a ne afisa pagina in browser. Astfel, google.ro ne poate oferii “serviciul” de cautare online. In sectiuniile viitoare vom interactiona mai des cu ideea de server.

Instalarea unui Server web pe Linux

Un server web este un software care permite afisarea paginilor web si furnizarea de continut web catre utilizatori prin intermediul internetului. Unul dintre cele mai populare servere web este Apache HTTP Server, cunoscut sub numele de Apache. Pentru a instala Apache2 pe Ubuntu Linux, poti urma acesti pasi:

1. Deschide terminalul.
2. Actualizeaza lista de pachete cu comanda: **sudo apt update.**
3. Instaleaza Apache2 cu comanda: **sudo apt install apache2.**
4. Dupa ce instalarea este finalizata, Apache2 va fi pornit automat. Poti verifica starea sa cu comanda: **sudo systemctl status apache2.**
5. Urmatorul pas sa accesezi serverul web nou creat, introducand **adresa IP** a Linux-ului tau în browser. O poti afla folosind comanda **ifconfig** din Terminalul Linux

Acestia sunt pasii de baza pentru a instala Apache2 pe Ubuntu Linux. Odata ce Apache2 este instalat si pornit, poti accesa serverul web utilizand adresa IP a masinii tale sau domeniul asociat, pentru a verifica daca functioneaza corect. Fisierele (HTML, CSS, JavaScript) site-ului web se afla in locatia **/var/www/**. Aici poti adauga sau modifica continutul noului tau site (poti folosi teme gratuite Bootstrap de pe Google).

```
tecmint@ubuntu-20-04:~$ sudo apt install apache2
[sudo] password for tecmint:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2
0 upgraded, 1 newly installed, 0 to remove and 51 not upgraded.
Need to get 95.5 kB of archives.
After this operation, 541 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 apache2 amd64 2.4.41-4ubuntu3 [95.5 kB]
Fetched 95.5 kB in 5s (18.9 kB/s)
Selecting previously unselected package apache2.
(Reading database ... 112619 files and directories currently installed.)
Preparing to unpack .../apache2_2.4.41-4ubuntu3_amd64.deb ...
Unpacking apache2 (2.4.41-4ubuntu3) ...
Setting up apache2 (2.4.41-4ubuntu3) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
```

Exercitii

1. Creaza in folderul tau *home* urmatoarea ierarhie de fisiere si foldere (\ = folder; - = fisier):

```
\Exercitiu1
 \Retelistica
     \Switch
        - numar_porturi.jpg
        - adresaMAC
        - vitezaPort
        -numarDevice
        -versiuneOS
     \Router
 \Geografie
     \Continente
        \Europa
           \Europa de Est
              \Romania
              \Bulgaria
        \Asia
     - harta romaniei.jpg
     - harta europei.png
 \Istorie
     \Protocoale de Rutare
        - OSPF.html
        - EIGRP.pdf
     - Mihai Viteazul.jpg
     - A I Cuza.png
 \Programare
     \Python
     \C\C++
        - Introducere in algoritmi.pdf
        - Dennis Ritchie.jpg
        - tema_backtracking.c
     \JAVA
```

2. Redenumiti fisierul 'numarDevice' in 'deviceActiv'.
3. Mutati 'harta romaniei' in folderul corespunzator tarii din folderul 'Geografie'.
4. Stergeti folderul 'JAVA'.
5. Mutati intregul folder numit 'Statistica si probabilitati' (cu tot cu fisierele continute), in folderul 'Retelistica'.
6. Creati in '/home/user/Teme' un folder numit 'Imagini' in care copiati toate fisierele cu extensia .jpg din ierarhia fisierelor create la exercitiul 1.
7. In interfata grafica (cu mouse-ul), faceti acelasi lucru, de data aceasta in folderul '~/Teme/Imagini2' pe care il creati voi.
8. Stergeti fisierele, din toata ierarhia creata anterior, al caror nume se termina cu cifre.

9. Scrieti textul „Linux Rulz“ intr-un fisier, in folderul 'Downloads' din 'home', folosind interfata grafica. Apoi din linia de comanda, afisati continutul fisierului.

Avansat

NOTA #1: necesita research pe Google
NOTA #2: iti antreneaza abilitatile de rezolvare a problemelor si cele de IT-ist 🙂

1. Folositi 'ls' pentru a lista fisierele in ordinea inversa a datei in care au fost modificate.
2. Creati un alias astfel incat comanda 'grep' sa ruleze implicit in modul color. Salvati modificarea in setarile bash-ului.
3. Afisati toate alias-urile create.
4. Numarati toate fisierele din '/etc' ce incep cu litera 'a'.
5. Afisati toate fisierele din ‘/etc/’ cu extensia ‘.conf’.
6. Modificati prompt-ul utilizatorului fara privilegii in ‘#’ (in loc de ‘$’).
7. Setati prompt-ul in culoarea rosu pentru root. (HINT: http://www.cyberciti.biz/faq/bash-shell-change-the-color-of-my-shell-prompt-under-linux-or-unix/).
8. Explicati functionarea comenzilor 'pushd' si 'popd'. Cum putem afisa ierarhia de foldere, fara a o modifica?
9. Scrieti cateva randuri intr-un fisier. Apoi afisati-le in terminal, in ordine inversa.
10. Executati comanda ‘cat /dev/random’. Ce se intampla ? Ce reprezinta fisierul '/dev/random' ?
11. Afisati numele tuturor fisierelor si directoarelor din /etc/ care incep cu litera z.
12. Afisati numele tuturor fisierelor din /etc/ care incep cu litera a si au extensia .conf

III. Concepte fundamentale despre Retelistica

Scurta introducere in Retele de Calculatoare. Notiuni si principii de baza despre Retele

O retea reprezinta un ansamblu de dispozitive (PC-uri, Routere, Switch-uri etc.) interconectate, care pot comunica (schimba informatii) intre ele.

1) Dimensiunea unei retele

Retelele pot fi de mai multe tipuri:

- LAN – Local Area Network – ex: reteaua ta (prin cablu) de acasa
- MAN – Metropolitan Area Network – ex: reteaua extinsa, pe suprafata unui oras
- WAN – Wide Area Network – ex: Internetul
- WLAN – Wireless LAN – reteaua ta, wireless, de acasa
- SAN – Storage Area Network – retea dedicata sistemelor de stocare a datelor

Pe langa aceste tipuri de retele de calculatoare mai existe si altele de diferite dimensiuni sau care au total alte scopuri (ex: SAN – Storage Area Network). O retea de tip LAN este o retea relativ mica care este locala unei organizatii (si de obicei limitata din punct de vedere geometric). De exemplu reteaua ta de acasa este considerata o retea LAN pentru ca este limitata din punctul de vedere al numarului de dispozitive conectate la ea. O retea a unei scoli (desi este mai mare) va fi considerata tot LAN pentru ca leaga toate calculatoarele, serverele etc. in aceeasi retea si sunt limitati din punct de vedere geografic. Daca ar fi sa combinam mai multe retele si sa permitem interconectarea lor pe raza unui oras, atunci am forma un MAN (o retea mai extinsa, la nivelul unui oras, care ofera viteza mai ridicate de transfer de date fata de viteza “la net obijnuita”). O retea WAN este o retea este o retea de retele pentru ca se afla pe o zona geografica mai mare fata de cele enumerate mai devreme si permite extinderea pe mai multe orase, tari sau chiar continente. O retea de tipul WLAN este o retea LAN la care ne putem conecta wireless de pe telefonul mobil, tableta, laptop sau orice alt dispozitiv. Acel mediu wireless este unul separat fata de cel fizic si contine proprietati (viteza, securitate, raza de acoperire, etc.) diferite fata de acesta.

2) Componentele unei retele

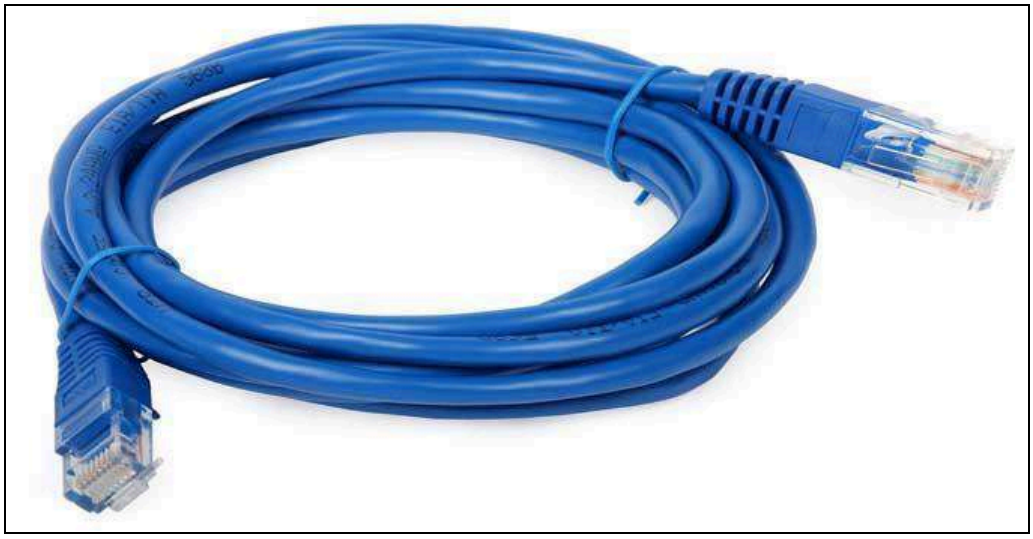
O retea este alcatuita din:

- End-device (PC, Laptop, Smartphone, Servere etc.)
- Switch – interconecteaza mai multe end-device-uri intr-o retea
- Router – interconecteaza mai multe retele
- Firewall – ne protejeaza reteaua de posbile atacuri din Internet
- Mediu de transmisie – cablu (cupru), lumina (fibra optica), wireless (aer)

Acum, propun sa discutam despre cateva elemente de retea (din cele enumerate mai sus). Primele componente ale unei retele vor fi chiar end-device-urile:

1. END-DEVICE (Dispozitiv terminal)

In general noi suntem cei care avem in componenta un dispozitiv terminal (end-device). Fiecare dintre noi avem un Laptop, PC, Server sau smartphone cu care ne conectam la Internet. Aceasta conexiune poate fi facuta prin 1 sau mai multe medii de transmisie (curent, lumina, aer). In momentul in care ne conectam cu smartphone-ul la Internet, cel mai probabil vom folosi mediul wireless. Daca folosim un Laptop, il putem conecta fie prin wireless fie prin cablu de retea (UTP).

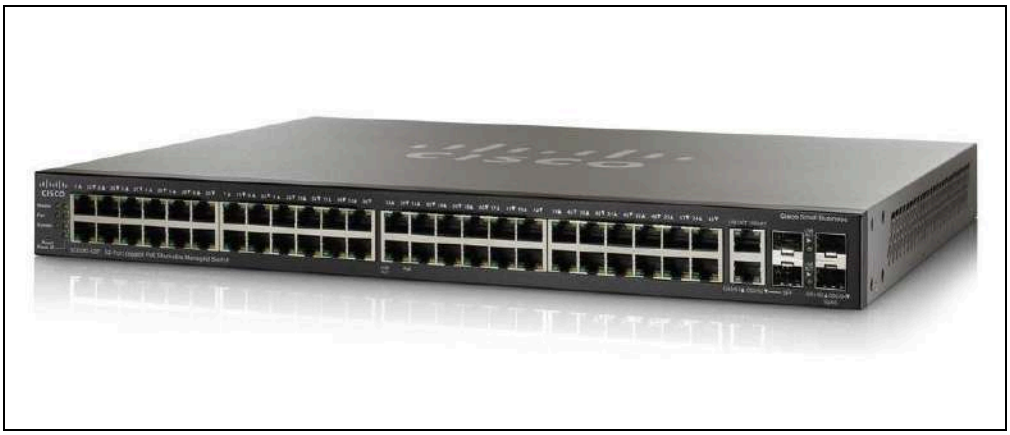


Cablu de Retea Ethernet – Figura 1.1

Conexiunea prin fibra optica are loc atunci cand dorim sa conectam mai multe echipamente de retea sau servere intre ele (ex: switch – switch, server – switch). Motivul este simplu: o legatura prin Fibra Optica poate fi mult mai rapida fata de cea prin cablu UTP sau prin Wireless.

II. SWITCH

Switch-ul este un echipament de retea care interconecteaza mai multe PC-uri (si nu numai: imprimante, telefoane IP, AP-uri, etc) la ACEEASI retea locala (LAN). El este caracterizat de un numar mare de port-uri (in general 24 sau 48) toate fiind capabile de viteze intre 100 Mbps si 1 Gbps (sau chiar 10Gbps). Switch-ul foloseste adresele MAC. (vom vorbi mai in detaliu in Capitolul 2).
Iata o imagine cu un Switch profesional Cisco:



Switch de Retea – Figura 1.2

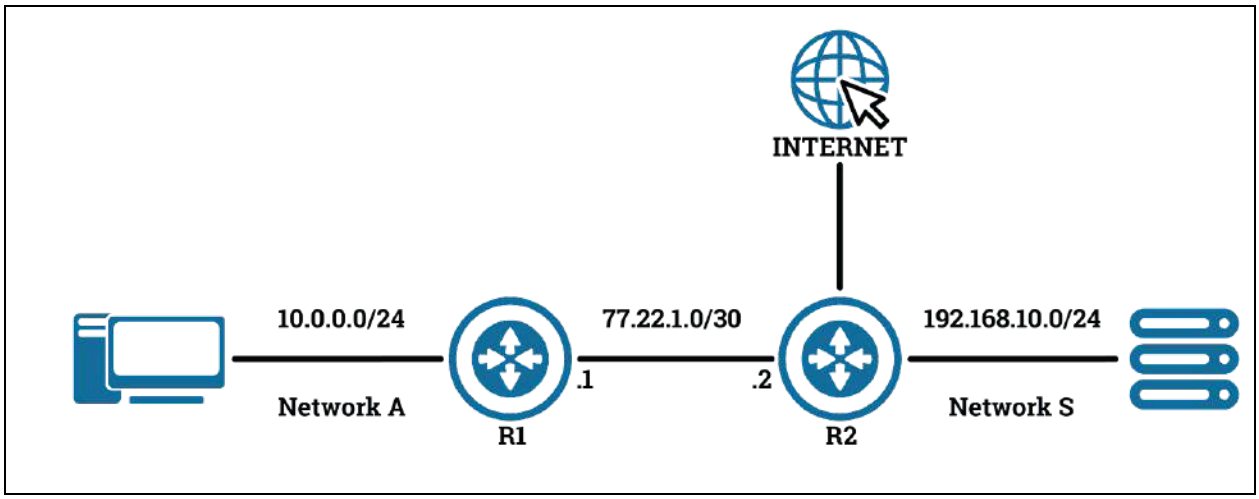
III. ROUTER

Un Router este un echipament de retea care are rolul de a interconecta mai multe retele (LAN) intr-o retea mai mare (WAN -Wide Area Network). Router-ul este dispozitivul care ne conecteaza la Internet. El se ocupa de trimiterea pachetelor, catre reteaua destinatie din Internet. In comparatie cu Switch-ul, Router-ul are mult mai putine port-uri (intre 2 – 5) la viteze asemanatoarea (100 Mbps – 10Gbps, depinde de model). Dupa cum spuneam scopul acestui echipament este sa interconecteze retelele. Toate aceste retele au nevoie de un mod de identificare si astfel Routerele foloseste adresele IP. Acesta este un Router profesional Cisco:

Router de retea – Figura 1.3

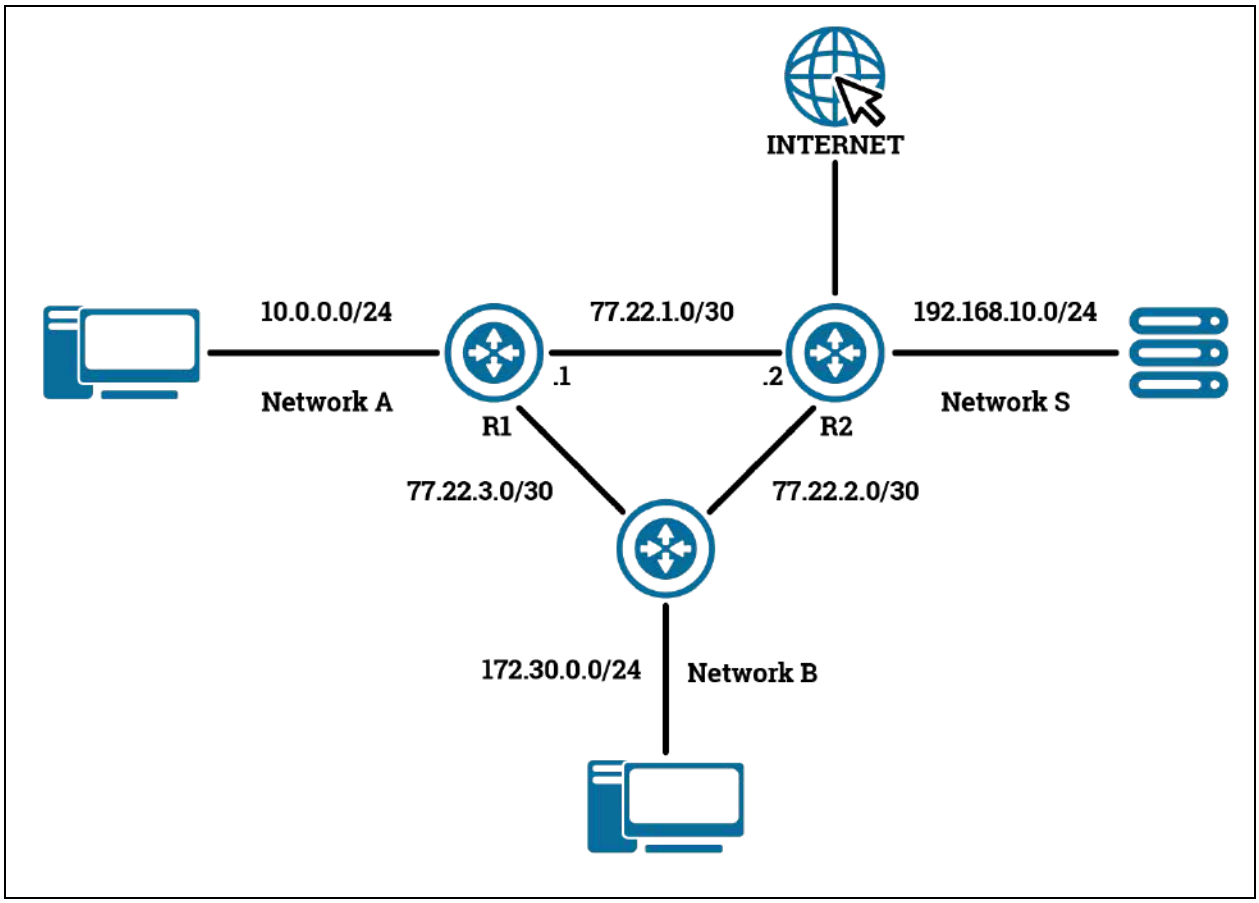
3) Cum reprezentam o retea prin Topologii Fizice si Logice

Reteaua o putem reprezenta printr-o topologie. Aceasta poate fi de 2 feluri: fizica sau logica. Topologia fizica descrie echipamentele si modul in care sunt acestea conectate, cablurile folosite. Alt exemplu avand in componenta 2 Routere, 1 PC si 1 Server. Unul dintre Routere este conectat la Internet – Exemplu #1 Topologie Logica



Topologie de reatea – Figura 1.4

Reteaua contine 1 Switch, 3 Routere, 2 PC-uri si 1 Server – Exemplu #2 Topologie Logica



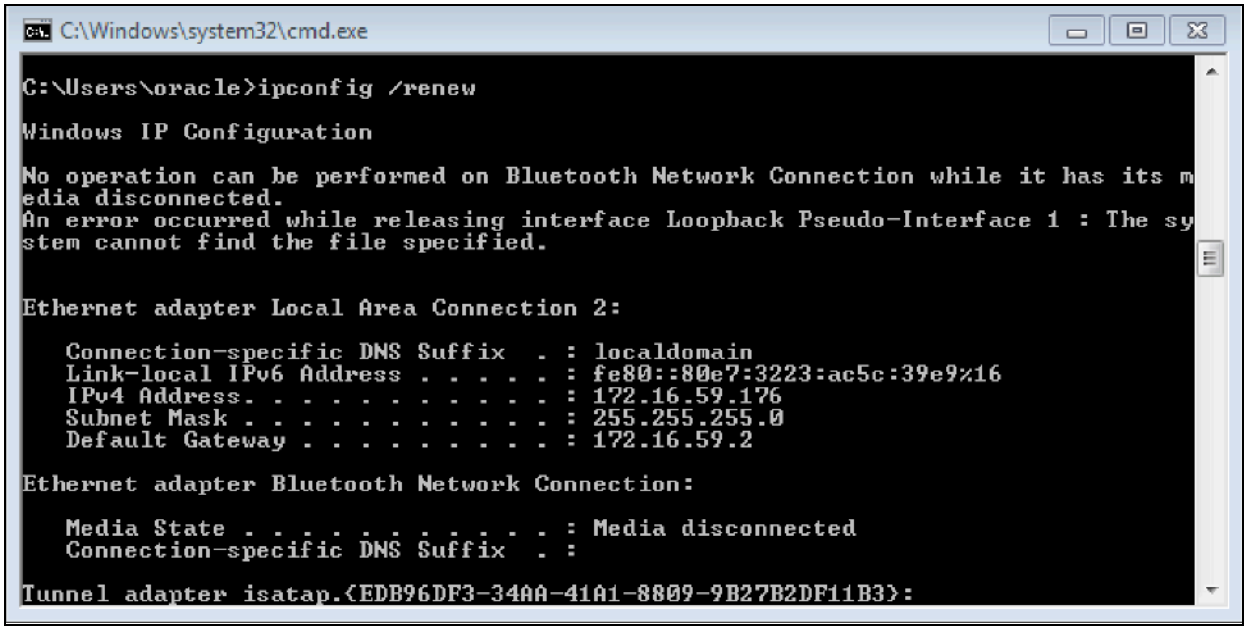
Topologie de retea – Figura 1.5

Ce este o adresa IP ?

Pentru a intelege mai bine ce este o adresa IP iti propun urmatorul exemplu: sa ne gandim la IP ca la un CNP pentru device-uri. Ce rol are CNP-ul ? De a identifica in, mod unic, fiecare persoana din Romania. Statul ne identifica prin CNP (aka IP), iar oamenii ne identifica prin Nume sau Prenume (aka. adresa MAC). IP (Internet Protocol) a fost dezvoltat in anii 1980 si foloseste 32 de biti pentru definirea unei adrese (ex: 192.168.1.1) numarul maxim de adrese IPv4 este de aproximativ ~4.2 Miliarde. In anul 2016 se estima ca numarul total de dispozitive conectate la Internet era in jur de ~30 Miliarde, numar care depaseste cu mult limita adreselor IP. Pentru asta exista adresele IPv6, care vin sa intampine aceasta problema. Daca esti curios sa citesti mai multe despre IPv6, intra aici (https://ramonnastase.ro/blog/ce-este-ipv6-si-cum-arata-o-adresa/).

Cum comunica dispozitivele in Internet cu ajutorul adresei IP?

Pentru a putea comunica, dispozitivele (PC-uri, routere, switch-uri, etc) trebuie sa aiba un identificator unic. In acest caz este vorba de IP (Internet Protocol). IP-ul este un mod de a identifica un dispozitiv intr-o retea. El trebuie sa fie unic. Nu pot exista 2 IP-uri la fel in aceeasi retea.



Linia de comanda – CMD – Windows – Figura 1.7

Exemplu de mai sus este luat din linia de comanda din Windows (cmd) folosindu-ma de comanda >ipconfig. Acesta de mai jos este alt exemplu de adresa IP:
10.0.0.1/24, unde /24 reprezinta masca de retea,
Masca de retea (Subnet Mask) determina dimensiunea retelei (adica cate dispozitive se pot afla in aceeasi retea la un moment dat – 14 – (/28), 126 – (/25), 254 – (/24), 510 – (/23) etc).
Elementele necesare unui end-device pentru a comunica cu succes in Internet:
IP-ul = identifica, in mod unic, un dispozitiv conectat intr-o retea
Masca de Retea = determina dimensiunea retelei (ca numar de IP-uri disponibile)
Default Gateway = calea de iesire din retea (de obicei spre Internet printr-un Router)
Server DNS (Domain Name Server) = „transforma" un nume de domeniu (precum google.ro) intr-o adresa IP (ex: 173.23.85.91)

Ce este Ethernet?

De aceasta tehnologie sunt absolut sigur ca ai mai auzit pentru ca: 1) am amintit putin mai devreme de ea si 2) pentru ca Routerul tau de acasa foloseste o astfel de tehnologie (la fel si PC-ul / Laptop-ul – interfata de retea).

Ethernet este cea mai raspandita tehnologie (pe echipamente de retea) din ziua de astazi datorita acestor 2 lucruri:

- viteza crescute (10/40/100 Gbps)
- forma de adresare (adresele MAC)

Fiecare port al Switch-urilor sau al Router-elor este construit pe tehnologia Ethernet si este notat diferit, in functie de viteza :

- FastEthernet – 100Mbps (aka. Fa0/1 ... Fa0/24)
- GigabitEthernet – 1000Mbps (aka Gi0/1 ... Gi0/24)

Astfel pe masura ce device-urile trimit trafic in retea, Switch-ul va invata adresele (MAC) lor sursa si le va asocia cu porturile de pe care provin (portul la care e conectat device-ul – ex: Fa0/1, Fa0/10 sau Gi0/4 etc.)

TCP, UDP, Port-uri si Aplicatii de Retea

1) TCP si UDP

In retelistica exista 2 mari protocoale care decid modul de functionare al aplicatiilor de retea, TCP si UDP. Avem de ales intre aceste 2 moduri pe operare (in functie de nevoile aplicatiei):

- Dorim ca aplicatia de retea sa functioneze fara intarziere (ex: Voce, Video – VoIP) si ne asumam pierderea unor pachete – UDP
- Suntem interesati ca aplicatia sa ne livreze tot continutul exact asa cum este el pe server (ex: pagina Web), asta implicand un mic delay – TCP

Aceste protocoale se numesc TCP (Transmission Control Protocol) si UDP (User Datagram Protocol).
TCP este considerat un protocol de incredere care garanteaza retransmiterea pachetelor in cazul pierderii acestora. El stabileste o conexiune intre client si server (numita 3 Way Handshake) folosind mesaje de sincronizare (SYN) si confirmarea (ACK) a primirii pachetelor.Dezavantajul TCP-ului este schimbul de mesaje (stabilirea unei conexiuni, terminarea ei, transmiterea de pachete SYN, confirmarea lor – ACK) care adauga un delay (timp de asteptare). Aplicatiile de retea precum HTTP (Web), FTP (Transfer de Fisiere), SSH (conexiune remote) folosesc acest protocol.

UDP este fix opusul TCP-ului (nu retransmite pachete, nu are un mod de stabilire a conexiunilor, etc.). UDP pur si simplu trimite pachetele de la o anumita sursa catre o destinatie fara sa-l intereseze starea acestora. Avantajul folosirii acestui protocol este reprezentat de latenta scazuta (delay) si permite fluiditatea aplicatiei fara intarzieri. Asadar UDP este un protocol potrivit pentru aplicatiile real-time (ex: Voce, Video) care pur si simplu au nevoie sa ajunga la destinatie cat mai repede posibil.
Metrici pentru traficul de Voce (VoIP):

- Delay: < 150 ms
    - Deschide CMD si scrie ping 8.8.8.8 pentru a vedea ce delay ai
- Pierdere de pachete: < 1%
    - 1 secunda de voce = 50 pkt de 20 ms audio fiecare => 1% din 50 = 0,5; adica la 2 secunde de audio se poate pierde maxim un pachet
- Jitter (delay variabil) – < 30ms

2) Port-urile

Un port identifica in mod unic o aplicatie de retea (server Web, DNS etc.) pe un dispozitiv dintr-o retea. Fiecare port are un identificator – un numar care poate avea o valoare de la 1 – 65535.
In momentul in care un PC trimite o cerere (pentru o pagina Web) catre un server, aceasta cerere va contine (printre altele) urmatoare informatii:
IP Sursa: PC
IP Destinatie: Server
Port Sursa: 29813 (generat random de catre Browser)
Port Destinatie: 80
Altfel spus, toate acestea reprezinta: Browser-ul (29813) PC-ului (sursa) cere pagina web (80) de la server (Destinatia).

3) Aplicatii de Retea

Iata cateva protocoale des intalnite ale aplicatiilor de retea:
HTTP

- Descriere: folosit pentru traficul Web (transporta fisierele HTML de la server la client)
- Port: 80
- Protocol de Transport: TCP

HTTPS

- Descriere: folosit pentru traficul Web intr-un mod securizat
- Port: 443
- Protocol de Transport: TCP

FTP

- Descriere: permite transferul de fisiere intre un client si un server
- Port: 20/21
- Protocol de Transport: TCP

DNS

- Descriere: gaseste IP-ul unui nume de domeniu (ex: google.ro -> 173.253.81.9)
- Port: 53
- Protocol de Transport: UDP (client), TCP (server)

Telnet

- Descriere: permite conexiunea nesecurizata de la distanta catre un echipament (Switch, Router)
- Port: 23
- Protocol de Transport: TCP

SSH

- Descriere: permite conexiunea securizata de la distanta catre un echipament (Switch, Router)
- Port: 22
- Protocol de Transport: TCP

DHCP

- Descriere: aloca in mod dinamic adrese IP, masca si default gateway device-urilor din retea
- Port: 67/68
- Protocol de Transport: UDP

Concluzii

Conceptele invata pana acum despre retelele de calculatoare te vor ajuta sa intelegi si mai bine partea de securitate cibernetica. In urmatoarele sectiuni vei invata mai multe despre aspectele securitatii si cel al hacking-ului in retea si Internet.

IV. Procesul de Hacking

In general cand vorbim de Hacking exista o structura foarte bine gandita in spate. Nu vrem sa gasim un server si sa “sarim” direct pe el pentru ca avem prea putine informatii despre acesta pe moment si ne expunem la riscul de a fi prinsi daca nu luam in calcul cei 5 pasi existenti in acest proces.

Cum se desfasoara procesul de Hacking ?

Sper ca observi ca am spus “*procesul de Hacking*”, proces care poate dura si cateva zile, saptamani, chiar luni (depinde de tinta si de riscul existent). Acest proces, cum am spus si mai devreme, este alcatuit din 5 pasi (figura 2.1):

1. **Reconnaissance -** Information Gathering
2. **Scanning**
3. **Gaining Access**
4. **Maintaining Access**
5. **Covering Tracks**

Figura 2.1

Iar acum haide sa luam pe rand si sa discutam despre fiecare in parte:

1) Reconnaissance - "*Information Gathering*"

Unul dintre cele mai importante lucruri pe care Hackerii il fac in momentul in care s-au decis ca vor sa atace un sistem (server, retea etc.) este sa acumuleze cat mai multe date despre el.

Gandeste-te in felul urmator: in momentul in care vrei sa pleci intr-o vacanta intr-un loc/tara in care nu ai mai fost, ce faci ? Cel mai probabil iti faci temele de casa. Adica te interesezi de acea locatie. Cauti pe Google diferite lucruri (ce poti face acolo, cum este vremea/mancarea, review-urile localurilor din zona etc.). Cu alte cuvinte **te informezi despre tinta ta**.

Exact prin acest proces trece si un Hacker in momentul in care decide sa atace un sistem. Exista diferite metode prin care poti afla mai multe despre un site/server, una dintre cele mai simple metode este sa cauti pe Google informatii despre acesta.

Printr-o comanda simpla precum **nslookup** (sau **dig**) poti afla cu adresa IP a unui site, iar prin comanda whois poti afla mult mai multe informatii despre acel domeniu.

>**nslookup** google.ro
>**whois** google.ro

Termenul de Reconnaissance (sau de Information Gathering) vine de la ideea de a cerceta, de a te informa despre un anumit subiect inainte de a trece la actiune. Mai pe scurt, practic inseamna **documentare** inainte de **actiune**.

Ca interval de timp acest proces este cel mai "costisitor". De ce ? Pentru ca un atacator trebuie sa fie foarte bine informat, trebuie sa cunoasca lucrurile in amanunt pentru ca altfel (asa cum am spus si la pasul #5) isi risca propria libertate.

2) Scanning - "*Scanarea sistemului*"

Urmatorul pas in "Procesul de Hacking" este **scanarea**. Odata ce un Hakcer are mai multe informatii despre tinta sa va incepe sa afle si mai multe informatii (de data aceasta tehnice).
Si cum va face asta ? Folosind diferite unelte (precum Nmap) cu care se pot scana retele, servere si care ii ofera informatii mult mai clare despre topologia retelei, despre echipamentele folosite, sistemul de operare etc.

De ce sunt acestea importante ? De ce este important sa stie un Hacker daca un anumit server web ruleaza pe Windows sau pe Linux ? Pentru ca odata ce are aceasta informatie poate sa mearga mai departe (la pasul 3), cu un mic research pe Google, sa descopere anumite vulnerabilitati existente si sa incerce sa profite de ele cu scopul de obtine acces in acel sistem (sau de a extrage anumite date).

Despre scanare si diferitele metode prin care putem face asta vom vorbi mai pe larg in capitolul 6. Cu ajutorul acestor date acumulate din urma scanarii, Hackerul va trece la pasul #3.

3) Gaining Access - "*Obtinerea Accesului*"

Avand temele facute (a facut research, a scanat retelele/serverele, a aflat informatii din diferite surse - Google, Facebook, Forumuri - despre tinta), Hackerul poate incepe atacul. Atacul trebuie gandit foarte bine pentru a fi in modul stealth (fara a declansa alarme si - daca se poate - fara a generea prea multe log-uri).

Exista foarte multe **tool-uri** (*Burp Suite, SQLmap, Metasploit* etc.) care pot fi folosite pentru a genera un atac cibernetic, totul depinde de tehnologie si obiectiv.

Obtinerea accesului se poate face in mai multe moduri si din mai multe puncte de vedere:

- Obtinere acces la nivel de **root** pe un server Linux
- Obtinere acces la **panoul de administrare** al unui site
- Obtinere acces pe un anumit **echipament** din **retea** (Router, Firewall, Switch etc.)
- Obtinere acces pe un **end-device** din retea (smartphone, tableta, laptop etc.)

Odata ce Hackerul are acces pe unul dintre elementele enumerate mai devreme, el este infiltrat in retea si astfel poate obtine foarte multe informatii despre organizatia in care se afla (digital).

Vom discuta in capitolul 5 mai multe despre tipuri de atacurile cibernetice si cum le putem face. Totodata in **cursul de Securitate** (iti mai aduci aminte de surpriza din capitolul 1 ? ;) iti arat pas cu pas cum poti face aceste atacuri cibernetice indiferent ca este vorba de retea, wireless, servere sau site-uri.

4) Maintaining Access

Odata intrat in retea, Hacker are optiunea de a-si mentine accesul. In foarte multe situatii cand au fost sparte diferite servere ale marilor companii (Yahoo, Google, Microsoft etc.), Hackerii si-au lasat mereu “portite deschise” pentru a intra inapoi in sistem.

Aceste portite se numesc “**backdoor**” si sunt lasate intentionat de catre Hackeri (sau chiar de catre dezvoltatorii de software ale unor aplicatii pe care tu si eu le folosim zi de zi) pentru a avea acces ulterior in sistem.

Astfel ei pot extrage in mod constant date, pot urmarii ce se intampla in organizatii, pot detine “controlul din spate”, urmand ca ulterior sa faca ceva cu aceste date (de obicei ele sunt vandute pe piata neagra din Deep Web).

Dupa acest proces, urmeaza pasul #5 care este extrem de important.

5) Covering Tracks - “Acoperirea Urmelor”

Acest proces este unul foarte important (cel de “Acoperire a urmelor lasate”). Un proces pe care foarte multi Hackeri (mai ales cei care sunt la inceput de drum) il omit. Pur si simplu nu sunt atenti (sau constienti) sa-si acopere urmele si ajung sa fie prinsi (in Romania de DIICOT, SRI sau STS) si pedepsiti in instanta pentru faptele savarsite.

Repet, faptul ca, **accesul neautorizat** intr-un sistem poate duce la consecinte grave din punct de vedere penal:

- confiscarea bunurilor informatice - laptop-uri, hard disk-uri externe etc.
- punerea sub supraveghere
- sau chiar arestul, acestea fiind doar cateva dintre consecinte.

Pentru a nu lasa astfel de urme ca sa poata fi descoperiti, intervine un element cheie, *SA INTELEGI CUM FUNCTIONEAZA TEHNOLOGIA*.

La ce ma refer ? Ma refer la faptul ca este extrem de important sa intelegi cum functioneaza “acel server de baze de date, acel server de mail sau web” - atat din punctul de vedere al modului in care il configurezi, cat si din punctul de vedere al monitarizarii si jurnalizarii (log-uri) acestuia.

De asemenea este important sa stii cum sa functioneaza sistemul de operare **Windows** sau **Linux**.“Cum sunt creati userii ? Unde sunt stocate datele acestora ? Datele de logare? Ce se intampla in momentul in care te loghezi pe un astfel de sistem ? Unde se scriu acele log-uri ?” etc.

Hackingul (profesionist, etic si sigur) nu este pentru toate lumea si de aceea trebuie sa fii foarte bine pregatit pentru ca in anumite situatii libertatea ta poate fi pusa in joc.

Inca un lucru foarte important pe care vreau sa-l retii este faptul ca nimeni, **NIMENI**, nu face “Hacking” **de la el de acasa**. Este foarte important sa-ti ascunzi urmele pe cat de mult poti. Asta inseamna sa schimbi locatia in care te afli, sa folosesti servicii VPN (despre care vom discuta in capitolul 10) si/sau Tor pentru criptarea si anonimizarea traficului.

Cum stergem urmele dintr-un sistem ?

Acum hai sa vedem cateva metode prin care iti poti acoperi urmele lasate odata ce ai intrat intr-un sistem (retea, server, laptop etc.)

a) **Stergerea Log-urilor din diferite aplicatii (web, mail etc.)**
b) **Stergerea Log-urilor userilor**
c) **Stergerea logurilor din diferite sisteme de monitorizare**

Fiecare sistem are diferite moduri de monitorizare a acestuia cu scopul de a face debuging sau troubleshooting in cazul aparitiei unei probleme.

Pentru a face toate acestea nu este necesar, ca un Hacker, sa merga pas cu pas, din fisier in fisier, sa caute si sa stearga ultimele jurnalizari (log-uri). Ci poate folosi diferite scripturi existente (in Internet) ale altor persoane cu care isi poate curata urmele.

Iata **aici** un exemplu de program pentru **Windows** (de asemenea se mai poate folosi si EventViewer).

Iar pentru **Linux** se pot da urmatoarele comenzi:

#**rm ./bash_history** - pentru stergerea comenzilor date de catre utilizatorul curent

#**vim /var/log/messages** - loc in care se pot sterge logurile

sau in orice alt fisier din **/var/log**, depinde cu ce aplicatie s-a incercat exploatarea. Mai exista un alt mod prin care putem sterge logurile folosind Meterpreter (o aplicatie destinata PenTesterilor, despre care vorbesc si iti arat cum sa faci in **cursul de CyberSecuritate**).

6) (Pentru cei etici) Raportarea

Un alt pas foarte important, mai ales in procesul de Ethical Hacking este #6, **Reporting (Rapotarea)**, pasul in care Hackerul genereaza un raport asupra vulnerabilitatilor gasite (si exploatate), modurile prin care acestea pot fi remediate si alte informatii care sa duca la solutionarea si securizarea sistemului.

Acestia au fost cei 5 pasi (6 pentru Ethical Hackers) care constituie **procesul de Hacking.** In urmatorul capitol vom incepe discutia despre cele 3 elementele fundamentale care stau la baza securitatii cibernetice.

V. Instalarea si folosirea OS-ului Kali Linux

Daca esti curios sa afli cum se fac atacurile cibernetice, atunci ai ajuns la capitolul potrivit pentru ca acum iti voi arata un tutorial de instalare a Kali Linux (distributia de Linux folosita de Hackeri).

Ce este Kali Linux ?

Kali Linux este **distributia de Linux** (cea mai) folosita de catre **Hackeri** si **Pentesteri** profesionisti datorita numarului de programe preinstalate existente pe aceasta. In Kali Linux poti gasi extrem de multe programe axate pe partea de securitate si pe partea de testare a vulnerabilitatii sistemului. Indiferent ca vorbim de scanari, atacuri DoS, atacuri Web sau orice alt tip de atac, Kali este alegerea perfecta pentru oricine doreste sa invete securitate. In figura 3.1 de mai jos poti sa vezi logo-ul oficial al acestei distributii de Linux. Denumirea de Kali vine de la zeul razboiului din mitologia hindusa.

Figura 3.1

Desi, la inceput poate parea putin greu de utilizat, acest lucru nu trebuie sa te descurajeze din a persevera si din a invata constant lucruri noi. De ce spun ca e greu de utilizat ? Pai in primul rand este vorba de Linux, iar daca nu ai mai interactionat cu Linux pana acum (din Terminal) s-ar putea sa ti se para destul de dificil, la inceput.

In al 2-lea rand este vorba de numarul mare de programe de PentTesting existente pe Kali. Acestea sunt dificil de folosit (mai ales la inceput), daca nu stii care este scopul lor (practic ce face tehnologia din spatele acelui tool) si daca nu stii sintaxa acestuia (dar aceasta se poate invata - la fel ca si celelalte).

Pasii de instalare Kali Linux in Masina Virtuala

Cand vine vorba de instalarea oricari distributii de Linux (deci si Kali) avem 2 optiuni:

- **Instalare Dual-Boot**
  - Linux, respectiv Windows se afla instalat pe partitii diferite
  - Cele 2 OS-uri ruleaza pe rand
  - Necesita reboot-ul laptopului/desktop-ului pentru a alege OS-ul dorit
- **Instalare in Masina Virtuala**
  - Linuxul vine instalat intr-o aplicatie (Virtual Box) si poate fi folosit in acelasi timp cu Windows
  - Nu necesita reboot, iar cele 2 OS-uri pot fi utilizate simultan
  - Consuma mai multe resurse (CPU & RAM) pentru ca acestea trebuie alocate catre 2 OS-uri in acelasi timp

Personal prefer a 2-a metoda pentru ca este mult mai simpla si rapida. In plus, iti spun din proprie experienta, daca folosesti prima varianta foarte des, vei omite sa intri in Linux si vei spune “Lasa, alta data. Acum nu am chef sau dau restart”. Dar cu varianta a 2-a nu prea ai scuze :D.

Pentru a instala Kali Linux avem nevoie sa trecem prin cativa pasi. In primul rand avem nevoie de programul **VirtualBox** (sau un alt program de virtualizare - ex: VMware Workstation) si de imaginea **OS-ului Kali Linux** asa cum poti vedea in figura 3.2.

Iti recomand sa selectezi **versiunea pe 64 de biti**, iar downloadarea sa o faci folosind Torrent pentru ca va fi mult mai rapida.

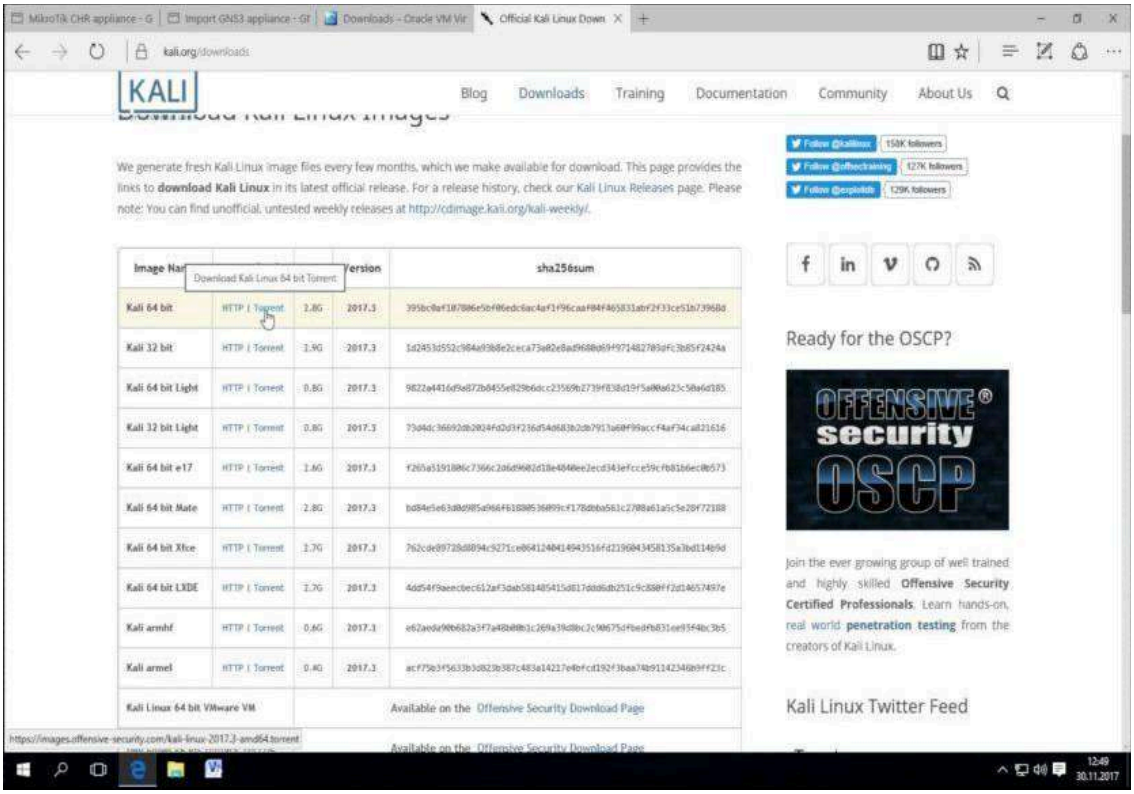


Figura 3.2

Urmatorul pas, dupa descarcarea imaginii OS-ului Kali Linux si al programului de virtualizare **Virtualbox** revine **procesului de instalare:**

1. Crearea unei masini virtuale - vezi **AICI** cum poti face asta.
2. Inceperea procesului de instalare - dupa cum poti vedea in figurile 3.3 si 3.4.

Procesul este unul simplu, iar cu ajutorul **acestui tutorial** sunt convins ca vei putea sa duci la capatat toata instalarea si sa incepi sa te joci cu Kali ;)

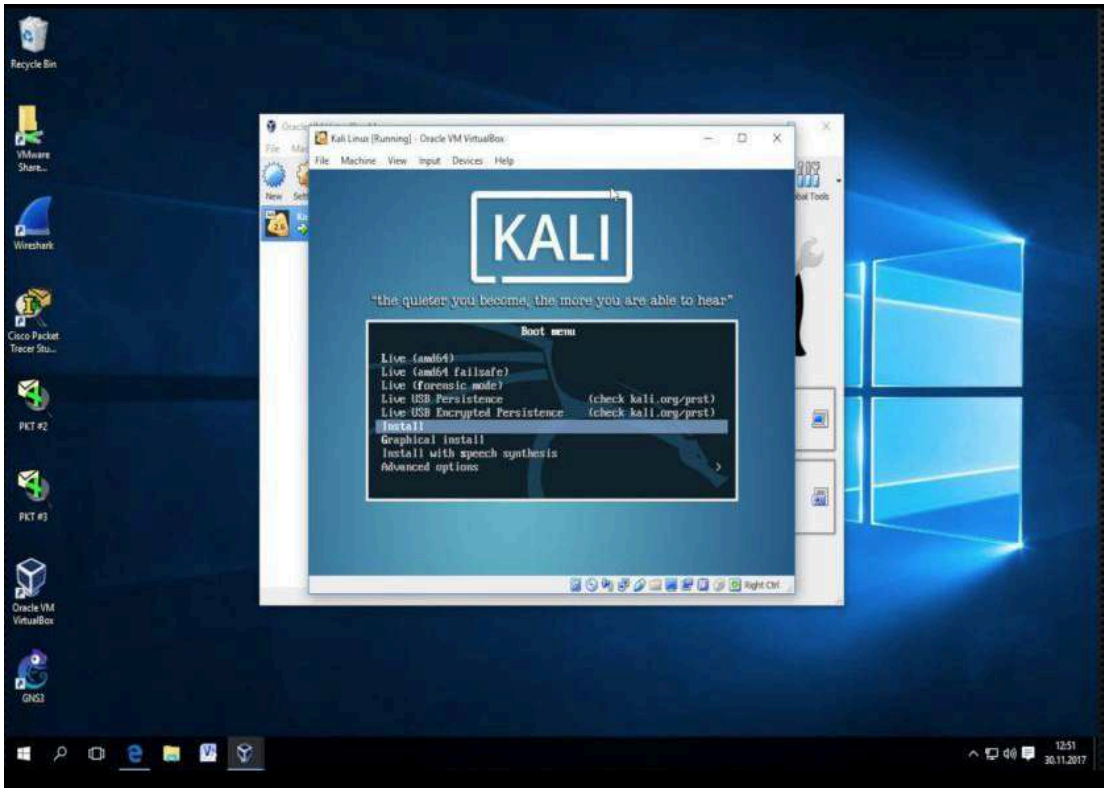


Figura 3.3

Daca vrei sa testezi Kali fara sa-l instalezi atunci poti opta pentru optiunea **Live**. Singura problema este ca de fiecare data cand vei porni masina virtuala ti se vor sterge setarile/munca pe care ai depus-o pana in acel moment. Daca scrii un script si esti in modul Live, acesta la reboot va fi sters, nu va fi salvat !

Si aici iti recomand sa mergi pe instalarea clasica pentru ca toate datele tale sa fie salvate pe disk.

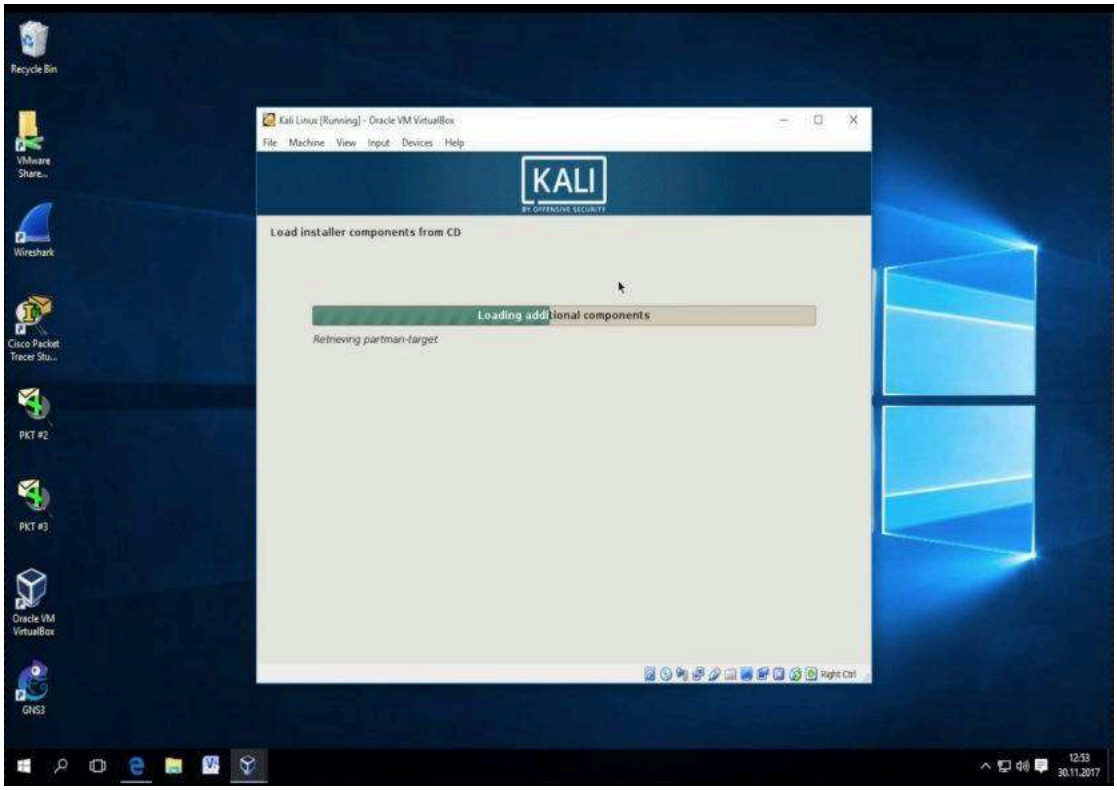


Figura 3.4

In continuarea procesului de instalare (figura 3.4), in mare parte trebuie sa mergi **next -> next -> finish**, iar apoi sa astepti putin pana cand totul este gata. Daca nu te descurci la un moment dat (intervin anumite setari pe care nu le intelegi sau iti apare o eroare) te incurajez MAXIM sa faci **research pe Google**.

In ultimii ani am constat ca un skill, o abilitate, tot mai necesara in ziua de astazi este cea de **a cauta pe Google**. Probabil ca te amuza ceea ce spun eu aici, dar vreau sa stii ca vorbesc cat se poate de serios. Iti spun din proprie experienta ca acesta abilitate m-a scos de foarte multe ori din incurcatura, indiferent de situatia in care m-am aflat (construirea site-ului, terminarea proiectelor din timpul facultatii, documentarea si nu in ultimul rand gasirea forumurilor cu subiecte de interes pentru mine).

Deci, daca iti apare o eroare la instalare sau in orice alta situatie. *Don't panic. Think for yourself. And search on Google :)*

Aaa.... si apropo, **userul default** pentru Kali Linux e **root** cu parola **toor**. Acum te-am scapat eu de o cautare ;)

Prezentare Distributie Kali Linux

Acum, dupa ce ai terminat cu instalarea si ai reusit sa pornesti si sa intri in Desktop, propun sa mergem mai departe si sa-ti prezint pe scurt Kali-ul astfel incat sa intelegi si sa identifci o parte din uneltele pe care le ai la dispozitie (in functie de obiectivul tau). Dupa cum poti sa vezi in figura 3.5, ne aflam in starea default a Kali-ului, mai exact pe Desktop. In partea stanga ai o bara cu o parte din unelte, dar sus de tot (pe pozitia a 2-a) poti sa vezi terminalul (cel mai probabil cea mai importanta componenta pe care iti recomand sa o stapanesti cat mai bine ;).

Figura 3.5

Mergand in stanga sus, avem un meniu fooooarte interesant :D. Meniul cu aplicatiile de PenTesting pe care le putem folosi (cu unele chiar ai experimentat din capitolele anterioare). Dupa cum poti sa vezi in figura 3.6, avem de unde alege (ba chiar mai mult, ele sunt puse in diferite categorii, iar aici intervenim noi - sa alegem cele mai eficiente programe pe interesul nostru).

Aceste aplicatii sunt defapt programe de “Hacking” care pot fi folosite atat cu intentii bune cat si mai putin bune. Totul depinde de tine acum sa le folosesti in scopuri cat mai bune (psss.... Ethical Hacking).

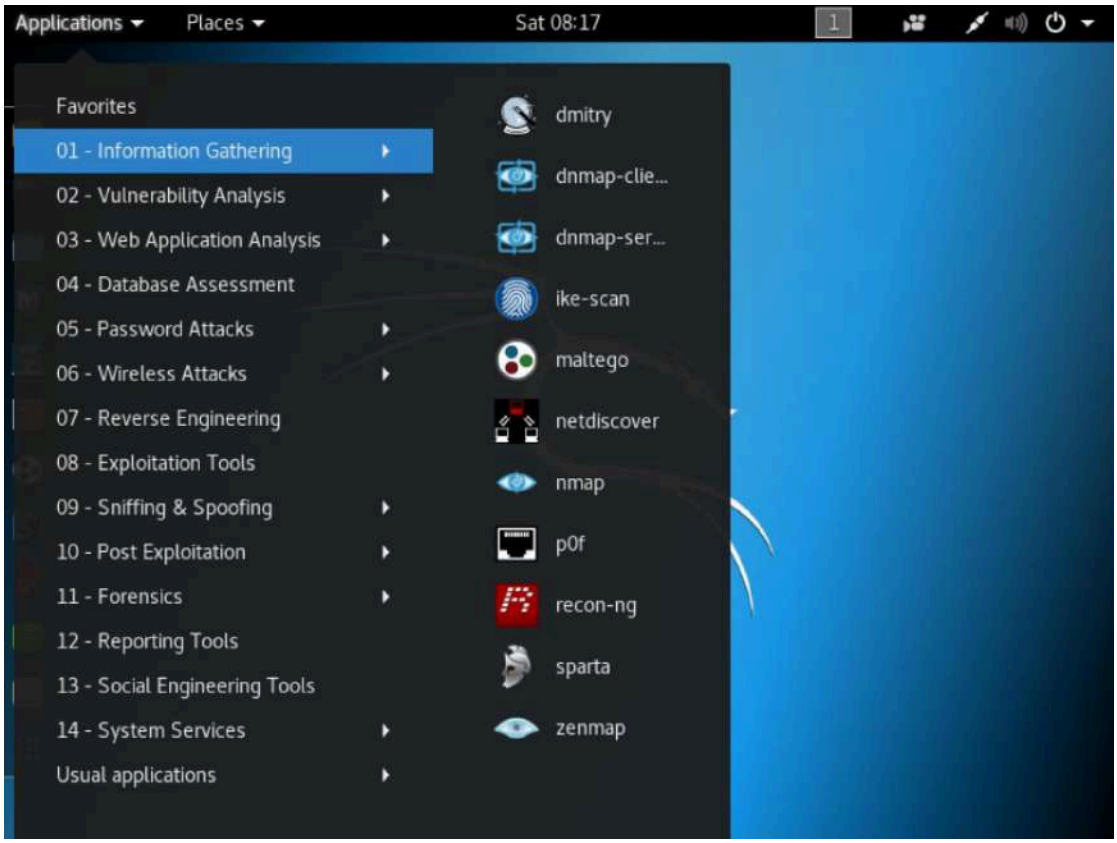


Figura 3.6

Si dupa cum poti sa vezi, chiar prima categorie se numeste “*Information Gathering*”, **exact** ca **primul pas** din *Procesul de Hacking* (despre care am vorbit mult mai in detaliu in capitolul 2). Aceste tool-uri pe care le vezi in figura 3.6 ne ajuta sa obtinem mai multe informatii despre tinta noastre. Pe unele dintre ele chiar le-am folosit sau le-am mentionat (nmap, zenmap).
Un lucru pe care vreau sa-l retii este faptul ca, in momentul in care apesi pe unul dintre aceste programe (oricare ar fi ele) se pot intampla aceste 2 lucruri:

1. Se deschide programul cu interfata GUI
2. Se deschide un terminal care ruleaza programul si iti afiseaza informatii de tip “help” ale acestuia

In primul caz, poate fi destul de intuitiv ce poti face cu el, iti vei da seama pe parcursul folosirii (exemple de **programe GUI in Kali**: *Yersinia, Maltego, Burp suite, Wireshark* etc.).

In al 2-lea caz, s-ar putea sa nu fie atat de evident inca de la prima utilizare, pentru ca, dupa cum spuneam si mai devreme, ti se va deschida un terminal cu un fel de meniu help/descriere a acelui tool. In ambele cazuri (mai ales in cazul 2) este important sa inveti acel program. Sa intelegi ce fac ele cu adevarat si “cu ce sa mananca”.
In figura 3.7 de mai jos poti sa vezi la ce ma refer mai exact:

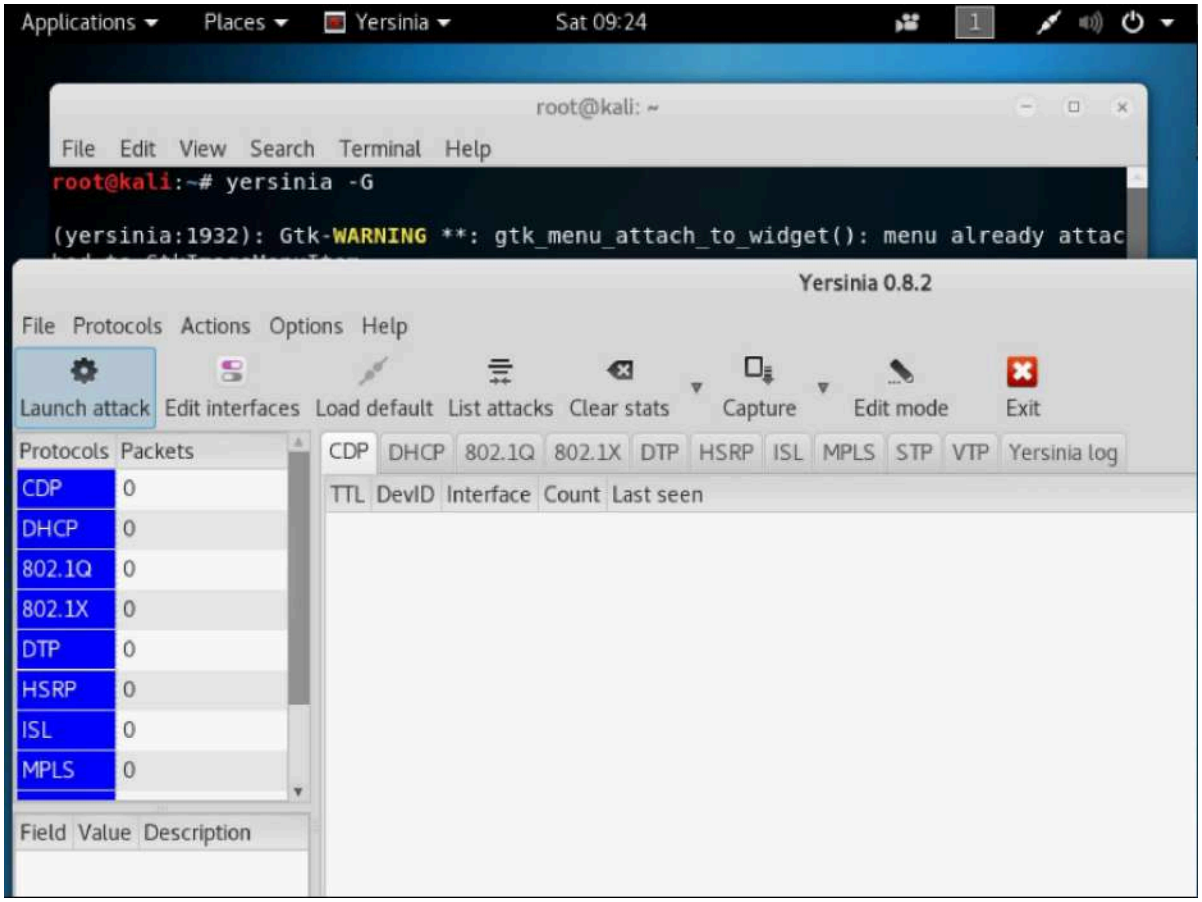


Figura 3.7

Yersinia este un tool grafic cu ajutorul caruia putem face foarte usor atacuri de tip MITM (mai ales daca in retea exista echipamente Cisco - Routere, Switch-uri nesecurizate). Yersinia are si o varianta in terminal care este mult mai puternica si customizabila. Pentru a porni versiunea GUI a Yersinia trebuie sa dam urmatoarea comanda:

```
#yersinia -G
```

De aici, te las pe tine sa experimentezi cu acest program :D .Tot ce pot sa-ti spun este ca, in partea stanga, vor aparea numarul de pachete capturate de tipul respectiv (statistica care iti da si un indiciu clar pe ce tip de atac sa te focusezi).

Mergand mai departe, in figura 3.8 de mai jos poti sa vezi o alta categorie care contine diferite tool-uri (unele din le-am folosit - *ettercap, Wireshark, macchanger*) care au scopul de a asculta, respectiv capta traficul intr-un atac cibernetic de tip MITM (Man-In-The Middle):

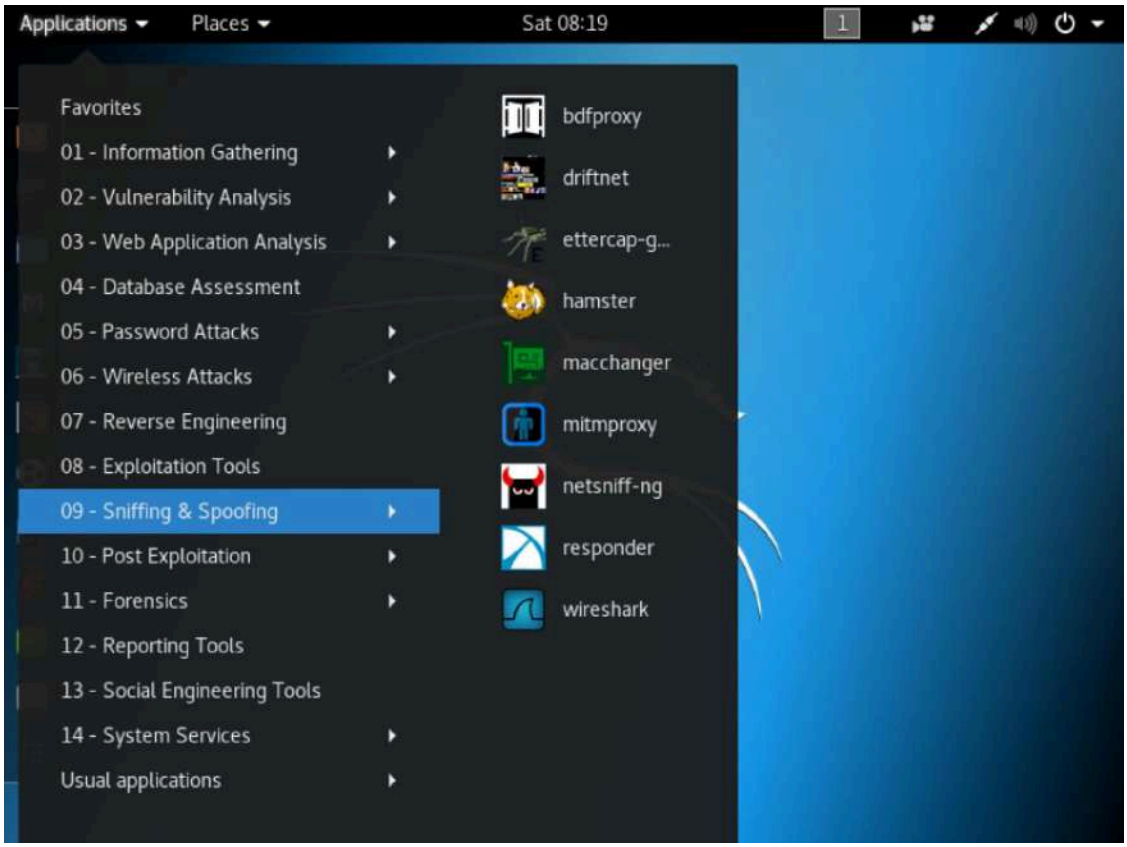


Figura 3.8

Acesta a fost doar o scurta introducere pe partea de Kali Linux. Daca vrei sa inveti mult mai multe elemente practice de PenTesting si CyberSecurity atunci te invit sa te inscrii la cursul de Introducere in CyberSecurity si Hacking de **AICI**.

VI. C.I.A.

Introducere in Securitate Cibernetica

In acest capitol vom incepe discutia despre cele 3 elementele care alcatuiesc notiunea de Securitate Cibernetica. Practic vom acoperi bazele acesteia.

Foarte multe persoane cand vorbeste despre Securitate Cibernetica, *se gandesc doar la criptarea datelor*. Acest lucru nu este neaparat corect, pentru ca securitatea cibernetica implica mai mult decat atat (defapt sunt 3 elemente cheie, cunoscute drept **CIA**). Acest CIA este o triada formata din 3 elemente cheie:

- **Confidentialitate**
- **Integritate**
- **Availability** (Disponibilitate)

Fiecare dintre aceste 3 elemente asigura, intr-un fel sau altul, ca datele noastre **nu au fost vazute**/citite (Confidentialitate), **nu au fost modificate** (Integritate) si sunt **accesibile** la orice ora (Availability).

1) Confidentialitatea Datelor

Cand vorbim de **confidentialitatea** datelor ne vom referi mereu la **criptarea** lor cu *scopul* de a le face **indescifrabile**. Acest proces de criptare necesita algoritmi, cu formule matematice foarte complexe, care sa asigure ca datele criptate nu pot fi citite.

Astfel daca vrei sa-ti criptezi un fisier pe telefon, pe laptop sau sa criptezi o comunicatie prin Internet intre 2 retele, lucrurile se pot face in 2 moduri (depinde de situatie):

1. **Simetrica** - folosind *o singura cheie* (PSK - aka. **parola**)
2. **Asimetrica** - folosind *o pereche de chei* (una **publica**, iar cealalta **privata**)

a) Criptarea Simetrica

Criptarea simetrica este **cea mai folosita forma de criptare din Internet**, fiind in acelasi timp rapida si sigura.

Motivul pentru care este atat de raspandita este faptul ca **necesita o singura cheie** (numita **PSK** - **P**re-**S**hared **K**ey) care va fi folosita atat pentru **criptarea datelor**, cat si pentru **decriptarea** acestora. Gandeste-te la aceasta cheie, ca fiind cea de la intrarea in casa ta (cu ea poti **descuia** usa, dar o poti si **incuia)**.

Si acum, iata un caz obijnuit in care folosesti un astfel de **PSK** pentru a cripta datele (sau traficul). Este vorba de conexiunea ta **Wireless**. Da, *in momentul in care te conectezi pentru prima* data la o retea wireless (**WLAN**) iti va cere o parola (care este PSK-ul).

Acea **cheie** (parola) este folosita atat pentru **autentificarea** in retea, cat si pentru **criptarea** mesajelor.

Acum ca ai inteles care e treaba cu criptarea simetrica, propun sa mergem mai departe si sa vedem cativa algoritmi care fac posibila securizarea datelor folosind o singura cheie:

- **DES**
- **3DES**
- **AES**
- **Blowfish**
- **RC4**

b) Criptarea Asimetrica

Cand vine vorba de criptarea asimetrica, lucrurile stau putin diferit. **Complexitatea** acestei criptari este **mult peste** cea simetrica (*1024, 2048 sau chiar 4096 de biti* vs 128, 192, 256), dar si *consumul de resurse hardware este mult mai mare*. Pe langa asta, **criptarea asimetrica** foloseste **o pereche de chei** - una **publica** si una **privata**.

Cheia privata este menita sa fie... privata, iar cea publica poate fi distribuita catre oricine. Criptarea asimetrica se face astfel:

Orice **criptez** cu cheia **PUBLICA**, pot decripta **DOAR** cu cheia **PRIVATA** (astfel obtinem confidentialitatea datelor).

Orice **criptez** cu cheia **PRIVATA**, pot decripta **DOAR** cu cheia **PUBLICA** (astfel obtinem o **semnatura digitala** care are scopul de a autentifica).

Vom discuta *mai multe despre criptare* in *capitolul 8, Introducere in Criptografie.*

2) Integritatea Datelor

Deci, practic, ce inseamna integritatea datelor ?
Intregritatea datelor asigura ca un fisier poate fi transferat dintr-un punct A intr-un punct B fara alterarea (sau modificarea) continutului acestuia. Ea este obtinuta in urma unui procedeu numit hashing.

Sa presupunem ca avem un fisier PDF caruia dorim sa-i asiguram integritatea in urma transferului prin Internet. Pentru a face acest lucru posibil avem nevoie de HASH-ul acestui fisier PDF.

Hash-ul unui fisier ajuta la stabilirea integritatii acestuia. In momentul in care dorim sa trimitem un fisier prin Internet, pe tot parcursul drumului poate suferi modificari (pierderea de pachete, alterarea informatiei, un hacker ii schimba continutul).

Iata si cativa algoritmi de stabilire a integritatii datelor:

- MD5 - 128 bits
- SHA1 - 160 bits
- SHA2 - 256 bits
- SHA3 - 384 bits (standardul curent)
- SHA5 - 512 bits

Mai multe despre Hashing si integritatea datelor discutam in capitolul 9, Introducere in Criptografie.

3) Availability / Disponibilitatea Datelor

Ce rost ar avea ca datele noastre sa fie criptate si hash-uite daca ele nu pot fi accesate ? Cum am putea sa ne folosim de date daca serverele, reteaua (sau curentul :D) ar fi down? Raspunsul este simplu: nu am putea sa le folosim. Atunci, un atac care are drept tinta intreruperea disponibilitatii datelor poate fi considerat o amenintare la adresa securitatii cibernetice a unei companii/organizatii ? Bineinteles.

Pentru a combate astfel de incidente de securitate care au legatura cu disponibilitatea datelor, avem mai multe optiuni pe care le putem implementa:

- **Redundanta** - la nivel de retea, server, UPS-uri etc.

- **Backup**

Aceste 2 elemente stau la baza asigurarii disponibilitatii datelor. Acum haide sa luam primul element:

a) Redundanta

Am scris la un moment dat pe blog, un articol despre Redundanta in care ma refeream la redundanta la nivel de retea. Exista mai multe tipuri de redundanta, dar mai intai sa vedem *ce reprezinta Redundanta* ?

Redundanta asigura ca pentru orice componenta critica care asigura functionarea companiei (de retea, server, alimentare electrica, etc.) sa avem cel putin un inlocuitor activ.
Asta inseamna ca daca avem un singur Router care este conectat la Internet, pentru a asigura redundanta (in cel mai bun caz) vom avea nevoie de *2 conexiuni la 2 provideri de Internet* diferiti si de *2 Routere* care se conecteaza la acesti provideri.

Cand vine vorba de redundanta la nivel de Server putem sa ne gandim la 2 sau mai multe servere care *ofera aceleasi servicii* (ex: web, baze de date etc.), sau ne putem referi chiar la discurile de stocare (HDD sau SSD) care pot fi "legate" impreuna pentru a asigura redundandata folosind o tehnologie numita **RAID** (**R**edundant **A**rray of **I**ndependent **D**isks).

b) Backup

Cu totii stim cat de importante sunt **backup-urile**, atat cele la nivel de hard-disk (SSD) cat si cele la nivel de site-uri web, fisiere de configurare, cod etc. Backup-urile recurente ne pot "salva pielea" foarte des pentru ca reprezinta o copie a tot ce avem noi live pe un sistem.

Spre exemplu, in cazul unui atac de tip Ransomware (care) in cazul in care nu vrem sa platim suma ceruta de catre hackeri, singura optiune pe care o avem este cea a backup-ului (mai exact cea a restaurarii unei copii deja existente care va readuce acel sistem din nou la viata.

Din pacate, in acest caz, daca **backup-urile nu sunt facute** destul de **des** (*cel putin saptamanal daca nu chiar zilnic*) atunci se va ajunge la o pierdere partiala a modificarilor facute cel mai recent.

Ce am discutat noi pana acum reprezinta elementele de baza care compun securitatea la nivel de date (atat cele care **circula** prin Internet, cat si cele care "**stau**" stocate pe un hard disk/SSD).

Ca un **rezumat** a celor discutate, vreau sa retii faptul ca:

1. **CIA** (**C**onfidentialitatea - criptarea -, **I**ntegritatea, **D**isponibilitatea) stau la **baza** Securitatii Cibernetice
2. Exista 2 moduri prin care se poate face **Criptarea** datelor (**Simetric** si **Asimetric**)
3. Integritatea datelor se stabileste printr-un **Hash** (care este o valoare unica pentru orice secventa de informatii)
4. Este important ca datele sa fie SI **Disponibile**, fapt care se poate asigura folosind elemente de **Backup** si **Redundanta**

VII. Tipuri de MALWARE si Atacuri Cibernetice

In acest capitol incepem discutia despre **tipurile de malware**-uri, iar mai tarziu vom discuta despre **Atacuri Cibernetice**. Pentru inceput vom discuta despre *Virusi, Trojeni, Viermi, Ransomware* si alte tipuri de programe care au fost concepute cu rea intentie. Dar inainte de toate acestea sa raspundem la urmatoarea intrebare:

1) Ce este un Malware ?

Un **malware** (aka. **malicious software**) este un *program conceput cu intentii rele* (aka. software malitios care vrea sa ne fure, distruga sau corupa datele stocate pe dispozitivele noastre).

Figura 5.1

Foarte multa lume foloseste **termenul generic de virus**, care nu este neaparat corect pentru ca pot exista mai multe *tipuri de programe periculoase.*

Iata mai jos (doar) o partea dintre acestea:
1) *Virusi*
2) *Troieni*
3) *Viermi*
4) *Ransomware*
5) *Spyware*
6) *Adware*
7) si multe, multe altele (Rootkit, time bombs, backdoor, etc.)

Iata in imaginea de mai jos extrasa de pe Wikipedia, proportia (in 2011) a malware-ului din Internet. De atunci si pana acum multe lucruri sau schimbat, dar este interesant ca avem o astfel de ierarhie cu cele mai intalnite tipuri de malware-uri.

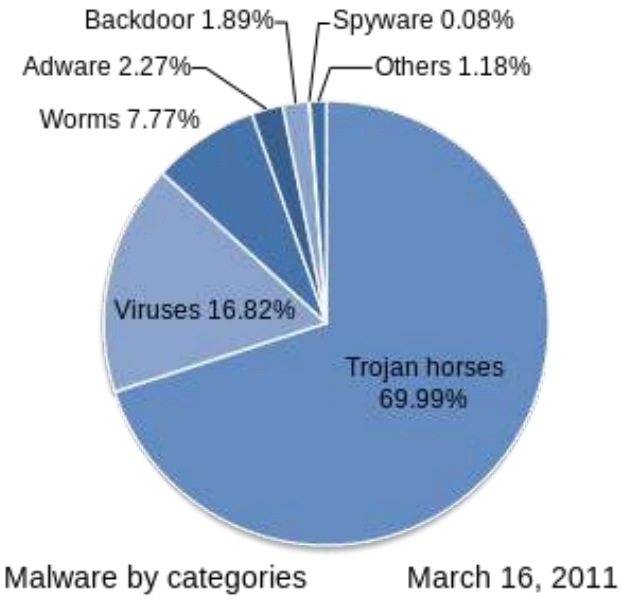


Figura 5.2

Si acum sa luam cateva dintre aceste malware-uri si sa discutam mai in detaliu despre ele:

1) Virusi

Un virus este un program cu care totii suntem obisnuiti. Fie ca am avut calculatorul infectat cu un virus sau ca am auzit/vazut la altcineva, stim ca acesti virus pot fi cu adevarat periculosi pentru noi (si mai ales pentru datele noastre stocate pe calculator - elementul cel mai important pentru noi).
Programatorii de virusi profita de vulnerabilitatile existente pe diferite sisteme de operare (in mod special Windows) si scriu software care sa profite de acestea (si de utilizatorii acestor dispozitive).

2) Trojeni

Un troian este un tip de program conceput sa para in folosul celui care il foloseste, dar in spate exista un cod malitios care are cu totul alte intentii. Aceste tipuri de programe se intalnesc cel mai des in Internet (dupa cum ai putut vedea si in imaginea de mai sus) si sunt folosite pentru ca sunt usor de mascat in fata unui utilizator neexperimentat. Astfel in momentul (primei) rularii programului, troianul este instalat si se va ascunde, facandu-si treaba "in liniste". Termenul de troian vine de la povestea calului troian din mitologia greaca, expusa in filmul Troia.

3) Viermi

Un vierme (**worm**) este o *forma de malware* care odata ce infecteaza un dispozitiv (PC, laptop, server etc.) va face tot posibilul sa se extinda si sa infecteze altele din retea. Astfel un worm reuseste sa **incetineasca** device-urile conectate la retea (prin consumul de resurse CPU si RAM) si chiar si reteaua pentru ca, calculatoarele infectate vor genera un consum anormal de trafic.

4) Ransomware

Un tip de malware tot mai popular in ultima perioada este ransomware-ul, a carui **scop este sa cripteze** hard disk-ul (sau SSD-ul) victime si sa ceara o **rascumparare** in bani acesteia pentru cheia de decriptare.

5) Adware

Sunt programe care odata instalate pe un dispozitiv (sau in browser) va incepe sa afiseze reclame (enervante).

6) Spyware

Sunt programe concepute cu scopul de a extrage anumite date de la utilizatori. Acestea nu sunt gandite sa ingreuneze (prin consumul de resurse) sau sa afecteze in vreun fel victima, ci pur si simplu sa extraga date si sa le trimita catre "serverele mama" (cele care au initiat "spionajul").

In primul rand trebuie sa fii constient de existenta unor astfel de programe dupa care trebuie sa iei masuri de protectie/prevenire impotriva lor.
In aceasta situatie programele de tip **anti-virus** sunt foarte bine venite pentru ca ele contin baze de date foarte mari (numite **semnaturi**) care verifica fiecare program/fisier aflat pe sistemul tau de operare (fie el Windows, Linux sau Mac).

Acum poate stii si tu ca pe Windows exista cel mai mare numar de programe malware (virusi, trojeni, ransomware etc). De ce ? Pentru ca Windows este cel mai utilizat sistem de operare la nivel mondial, iar Hackerii au ce sa “fure”. De aceea focusul principal al atacatorilor si al companiilor care se ocupa cu Securitatea Cibernetica este pe Windows.

Mac-ul si Linux-ul nu sunt nici ele ferite de malware, doar ca numarul lor nu este atat de mare. Acestea au fost concepute si cu un grad de securitate mai mare in minte si opereaza complet diferit fata de Windows.

2) Exemple de Atacuri Cibernetice

In acesta sectiune a capitolului 5, vom vorbi despre **Atacurile Cibernetice** si vom vedea cateva exemple de **Atacuri Cibernetice** (si *metode de Hacking*) din Internet. Aceste metode de hacking sunt foarte des intalnite, iar fiecare dintre ele serveste un scop anume.

Ce este un Atac Cibernetic ?

Un **atac cibernetic** este un mijloc prin care o persoana (cu rele intentii) **profita de vulnerabilitatile** existente pe un anumit sistem (server, calculator, echipament de retea, aplicatie etc.)

Iata in lista de mai jos cateva atacuri foarte des intalnite in Internet:

1) **MITM** - **M**an **i**n **t**he **M**iddle
2) **DoS** - **D**enial **o**f **S**ervice
3) **DDoS** - **D**istributed **D**enial **o**f **S**ervice, link atacuri: http://www.digitalattackmap.com/
4) **SQLi** - SQL injection
5) **XSS** - Cross-Site Scripting

Pe langa acestea, exista mult mai multe in lumea Internetului, dar pentru a exemplifica cateva ne vom focusa doar pe primele 3, urmand ca in capitolul 7 sa vorbim si despre ultimele doua pentru ca in mare au legatura cu **vulnerabilitatile site**-urilor (tehnologiilor) web.

Deci hai sa luam primul tip de atac, MITM, si sa discutam mai in detaliu despre el (si sa-ti arat cateva moduri in care poti face astfel de atacuri - dar te rog, fa-le intr-un mod etic), dupa care vom merge mai departe cu discutia si vom discuta despre DoS si DDoS.

Dupa toate acestea, in capitolul 6 vom discuta despre securitatea Web si despre celelalte tipuri de atacuri: SQL injections si XSS.

Ce este MITM (Man In The Middle) ?

MITM este un tip de atac cibernetic cu scopul de a asculta traficul utilizatorilor conectati la aceeasi retea.

Ce inseamna asta ? Inseamna ca daca mergi la o cafenea, in oras, cineva se poate conecta cu tine la acelasi Wi-Fi, iar din doar cateva comenzi iti poate vedea toate conversatiile de pe Facebook, Google etc.

Asta asa pe scurt, dar nu-ti fa probleme pentru ca lucrurile nu sunt chiar atat de simple. De ce ? Pentru ca marea majoritate a conexiunilor noastre in Internet sunt securizate (**HTTPS in loc de HTTP** ;)), in schimb asta nu insemna ca nu poate exista cineva care sa-ti asculte traficul.

Pentru a evita astfel de situatii, iti recomand ca in locurile publice sa folosesti un VPN (despre care vorbim mai multe in capitolul 9). In figura 5.3 poti vedea un exemplu de atac MITM:

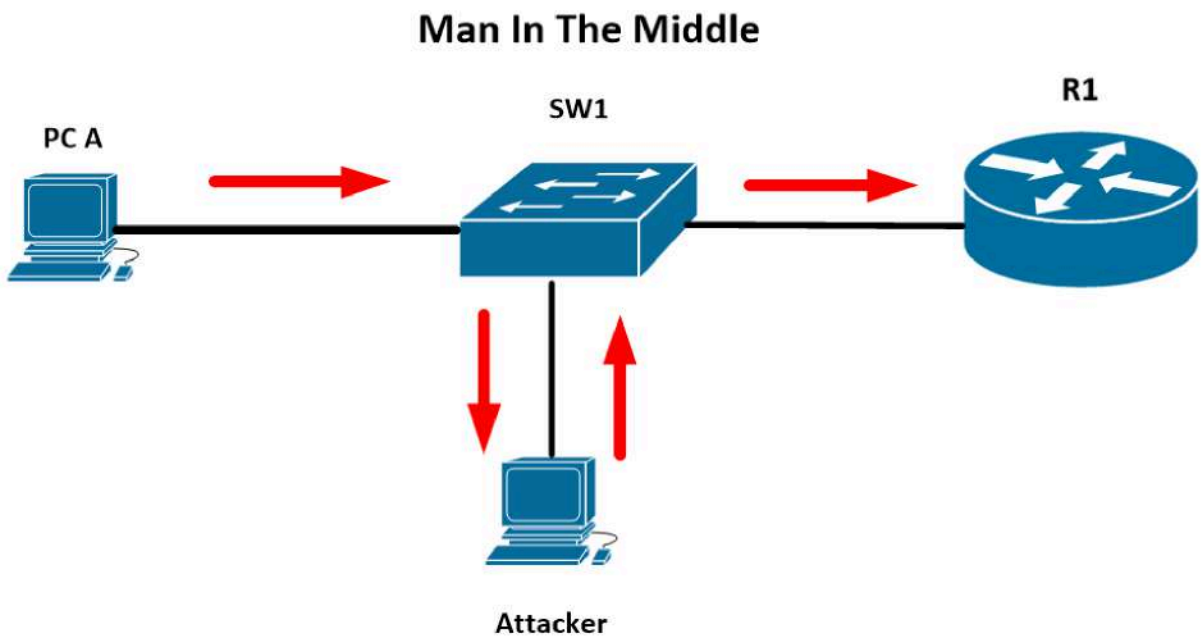


Figura 5.3

Exista mai multe moduri prin care se poate face MITM (iti voi enumera mai jos doar cateva dintre multele posibilitati):

- **MAC Spoofing**
- **ARP Spoofing**
- **Rogue DHCP Server**
- **STP Attack**
- **DNS Poisoning**

Acestea sunt o parte dintre cele mai des intalnite. In cele ce urmeaza voi discuta despre o parte dintre acestea si iti voi da si cateva exemple practice despre cum se fac.

1) MAC Spoofing

Termenul de spoofing vine de la a insela, iar in acest caz se refera la inselarea a cel putin unui device din retea prin faptul ca un anumit calculator se da drept un alt calculator (sau chiar Router) folosindu-se de adresa MAC a acestuia.

Acest lucru se poate face foarte usor folosind un program care schimba adresa ta MAC cu cea a unui PC pentru a vedea traficul acestuia. Ai aici un exemplu pe Windows 10 despre cum sa-ti schimbi adresa MAC, dar in opinia mea procesul este unul complex in comparatie cu cel de pe Linux:

```
# ifconfig eth0 down
# macchanger -m 00:d0:70:00:20:69 eth0
# ifconfig eth0 up
```

Mai intai oprim interfata (eth0 in acest exemplu), dupa care folosim comanda **macchanger,** aceasta este cea care ne ajuta cu **schimbarea adresei MAC**, iar argumentul **-m** ne lasa sa specificam o adresa. Pentru verificare foloseste comanda: **#ifconfig**

PS: daca vrei sa generezi un MAC aleatoriu, atunci foloseste: #**macchanger -r eth0**

2) ARP Spoofing

ARP Spoofing functioneaza intr-un mod similar cu MAC spoofing, doar ca atacatorul se foloseste de protoclul ARP pentru a informa (gresit) intreaga retea cu privire la faptul ca el detine adresa MAC X (care defapt este cea a Routerului).

Astfel toate device-urile din retea, care doresc sa ajunga in Internet, vor trimite traficul catre atacator (care il va redirecta catre Router). In aceasta situatie atacatorul poate sa vada tot traficul care trece prin el folosind un program de captura de trafic precum Wireshark.

In figura 5.4 de mai jos poti vedea cum are loc acest proces:

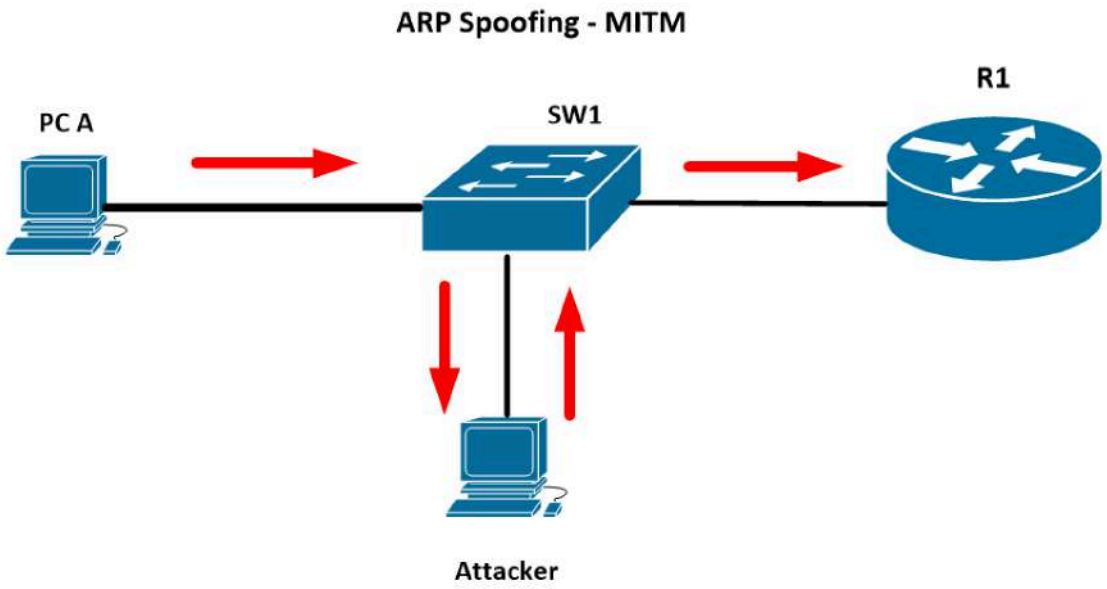


Figura 5.4

Pentru a initia un astfel de atac mai intai trebuie sa **pornim rutarea pe Linux**, astfel incat traficul sa poata fi trimis de la victima la Router si invers (prin noi, “atacatorii”):

```
# echo “1” > /proc/sys/net/ipv4/ip_forward
# cat /proc/sys/net/ipv4/ip_forward
```

Acum urmeaza **redirectarea traficului** pe portul pe care dorim sa ascultam:

```
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8181
```

Dupa care trebuie sa instalam programul:

```
# sudo apt-get update
# sudo apt-get install dsniff
```

Iar acum putem da comanda pentru inceperea atacului:

```
# sudo arpspoof -i eth0 -t 192.168.1.3 192.168.1.1
# sudo arpspoof -i eth0 -t 192.168.1.1 192.168.1.3
```

- *-i eth0*: reprezinta interfata pe care vom incepe atacul
- *-t 192.168.1.3*: reprezinta IP-ul victimei (device-ul care dorim sa-l atacam -- SCHIMBA cu un IP din reteaua ta)
- *192.168.1.1*: reprezinta IP-ul Routerului (SCHIMBA IP-ul Routerului cu cel din reteaua ta)

Practic aceste 2 comenzi trimit pachete false catre cele 2 dispozitive informandu-le ca traficul trebuie sa treaca prin atacator. Acum tot ce trebuie sa faci este sa deschizi Wireshark si sa observi cum trece traficul victimei “prin tine”.

Aici mai e nevoie si de un element care va facilita **DECRIPTAREA** traficului. De ce ? Pentru ca o mare parte din traficul existent in Internet este criptat.

Acest tool pe care il vom folosi se numeste **SSLstrip** (scoate elementul de securitate, SSL), iar comanda pentru decriptarea traficului HTTPS in HTTP este:

```
# sudo python sslstrip.py -l 8181
```

Aceasta comanda va asculta traficul pe portul 8181 si va incerca sa-l decripteze. Dupa asta poti sa pornesti Wireshark si sa vezi traficul decriptat (totusi iti sugerez sa pornesti Wireshark si cand traficul este criptat pentru a vedea diferenta).

PS: la o simpla cautare pe Google vei gasi SSL strip ;)

Pentru a scrie rezultatul intr-un fisier (din terminal) poti sa folosesti un tool similar cu Wireshark care se numeste Ettercap. Odata ce il instalezi pe Linux poti da urmatoarea comanda:

```
# sudo ettercap –i eth0 –T -w /root/scan.txt –M arp /192.168.1.3 /
```

Aceste argumente reprezinta:

- *-i eth0*: interfata pe care se asculta traficul
- -T : to launch command execution over the terminal
- -M : Man in middle mode
- -w : scrierea datelor intr-un fisier
- 192.168.1.3: IP-ul victimei

3) Rogue DHCP Server

Acest tip de atac se refera la crearea unui Server DHCP neautorizat in retea care sa ofere adrese IP valide, dar care ofera ca adresa IP a gateway-ului, adresa atacatorului. Astfel fiecare dispozitiv din retea (care a solicitat o adresa IP in mod dinamic) va trimite traficul catre atacator, care ulterior va redirectiona catre Router. Intre timp, tot traficul poate fi **decriptat** (folosind **SSL Strip**) si ascultat folosind **Wireshark**.

Acest atac se poate face folosind (pe Windows) un program care permite crearea serverului DHCP, iar pe Linux poti sa folosesti **serverul dhcpd**. Pe langa toate acestea mai ai nevoie sa adaugi si o ruta statica default pentru a **redirectiona** tot traficul catre Routerul din retea (aka. Gateway).

Iata pasii:

1. Porneste rutarea pe Kali
    a. **# echo “1” > /proc/sys/net/ipv4/ip_forward**
2. Instaleaza serverul DHCP
    a. # sudo **apt-get install isc-dhcp-server**
3. Configureaza serverul DHCP
    a. **# nano /etc/dhcp/dhcpd.conf**
4. Adauga o ruta statica catre Routerul tau
    a. # sudo **ip route add default via** 192.168.1.1
5. Porneste SSL Strip
6. Captureaza traficul

Cum te protejezi de atacurile MITM ?

Da, exista o solutie pentru toate aceste atacuri. De fapt mai multe solutii, dar iti voi spune de una relativ simpla, pe care o poti folosi incepand de astazi. Ea se numeste VPN (Virtual Private Network) si iti va cripta traficul fara ca cineva (aflat la mijloc) sa ti-l poata decripta. Vom discuta mai multe despre VPN-uri in capitolul 10.

O alta solutie se aplica in cazul Switch-urilor din retea si anume se refera la DHCP Snooping sau DAI (Dynamic ARP Inspection) care sunt diferite mecanisme prin care se obtine incredere in anumite dispozitive din retea. Iar in cazul in care cineva doreste sa incalce asta, atunci va fi penalizat prin excluderea lui completa din retea (inchiderea portului direct de pe switch).

Ce este DoS (Denial of Service) ?

DoS este o forma de atac cibernetic cu scopul de a **intrerupe** (pentru o perioada de timp) **functionarea** unui anumit serviciu de pe un **server**, avand **o singura sursa de trafic** (atacul este facut de pe un singur calculator).
DoS-ul are loc prin trimiterea a unui numar impresionant de trafic catre un serviciu "targhetat" cu scopul de a-l intrerupe. Astfel primind foarte multe cereri, un server web spre exemplu, nu ar face fata si s-ar "bloca" pe moment => intreruperea serviciului (in cazul acesta "picarea" site-ului web). Iata un exemplu de atac in figura 5.5:

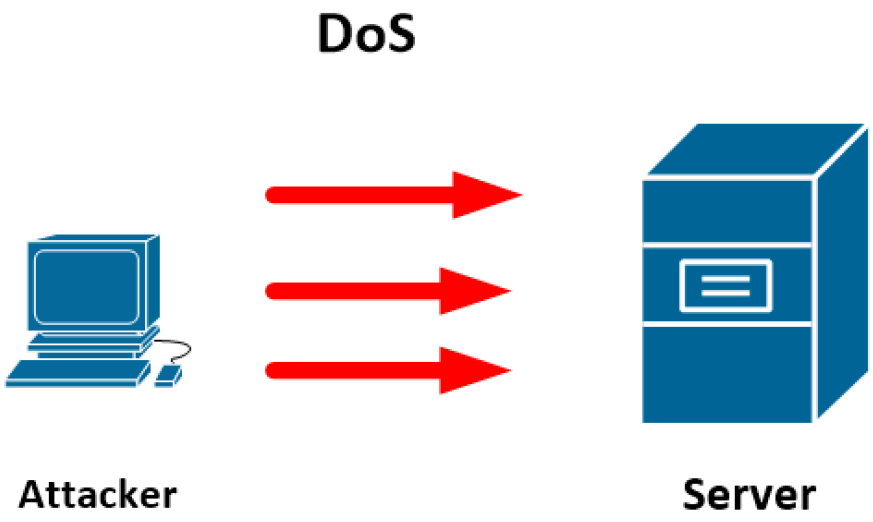


Figura 5.5

Ce este DDoS (Distributed Denial of Service) ?

DDoS este o forma de atac cibernetic cu scopul de a **intrerupe** (pentru o perioada de timp) **functionarea** unui anumit serviciu de pe un **server** sau a unei **retele** intregi, avand **foarte multe surse de trafic** din Internet.

DDoS-ul **are loc** prin intermediul mai multor **calculatoare** **"infectate"** cu malware care (puse cap la cap) trimit un numar impresionant de Gbps (*10,40, 100+ Gbps* - depinde foarte mult de numarul de calculatoare) in trafic. Aceste calculatoare se afla in **intreaga lume** si *nu au o locatie specifica*, acesta fiind unul dintre motive pentru care DDoS este foarte greu de combatut. Ba, chiar recent (in februarie 2018), a avut loc cel mai mare atac DDoS din istorie, catalogand 1.5 Tbps (adica 1500 Gbps). Wow !

Revenind, vreau sa stii ca o astfel de retea de calculatoare infectata cu malware poarta denumirea de **Botnet**. Iata mai jos un exemplu de Botnet care poate servi mai multe scopuri malefice (trimiterea de mail-uri tip spam/ a programelor de tip malware sau a unui numar insemnat de Gbps cu scopul de a face DoS) - figura 5.6:

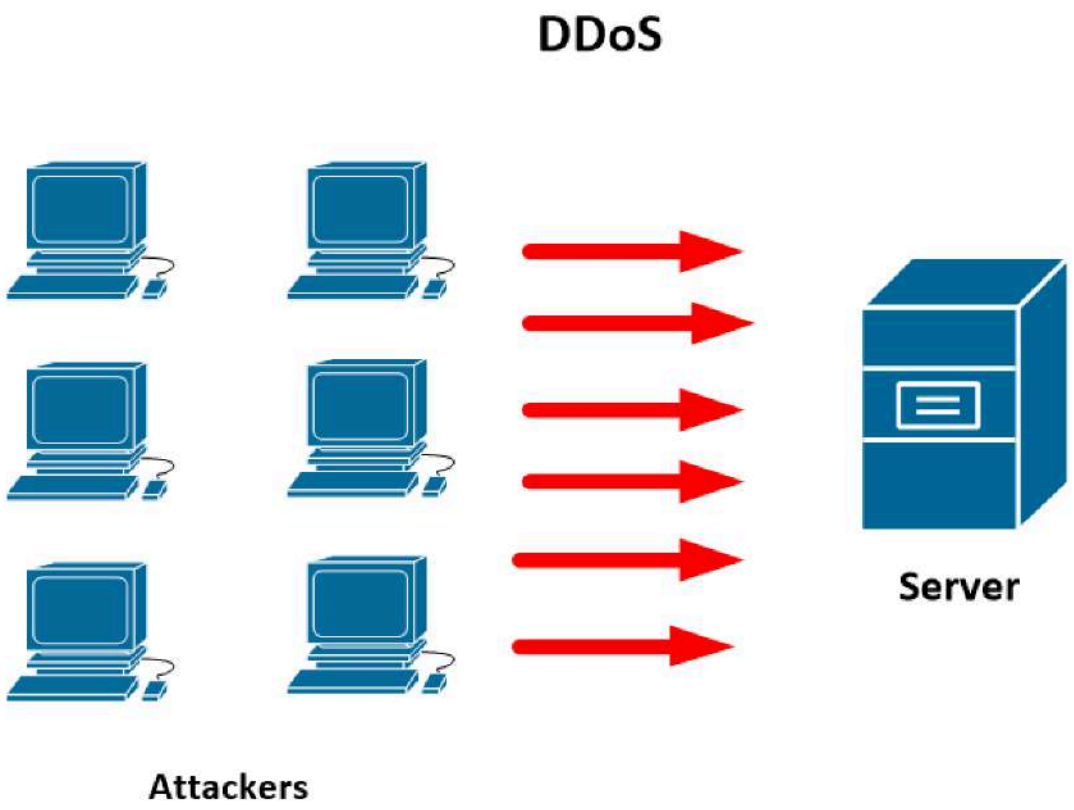


Figura 5.6

Pe langa aceste atacuri care au legatura cu reteaua, mai exista si atacuri care tin de "*spargerea*" *parolelor*:
1) **Brute Force**
2) **Dictionary Attack**
3) **Rainbow table**

1) Brute Force

Brute Force este o forma de atac cibernetic care are scopul de a obtine acces neautorizat in sistem (panoul de administrare al unui site, server, echipament de retea etc.).

Prin aceasta tehnica se foloseste "forta bruta", adica atacatorul incearca sa **ghiceasca** (nimereasca) **parola**, cu un minim de logica in spate.

De foarte multe ori aceasta tehnica duce la esec si renuntarea din partea atacatorului, dar sunt si multe cazuri in care se obtine accesul in sistem pentru ca acestuia *nu i s-a schimbat parola default* (care de multe ori este "*admin*" sau "12345678")

2) Dictionary attack

Un **atac pe baza de dictionar** (Dictionary attack) merge *putin mai targetat pe sistemul victima* pentru ca sunt cunoscute mai multi factori externi care tin de acea organizatie/persoana.

Astfel cu ajutorul unor tool-uri se pot genera sute, chiar mii de cuvinte care pot fi incercate pentru a obtine accesul in sistem. **Dezavantajul** acestui tip de atac este ca poate dura mult timp (depinde numarul de cuvinte si de securitatea sistemului), iar dictionarul nu garanteaza succesul atacului.

Un simplu mod prin care putem **combate** aceste tipuri de atacuri este sa folosim un numar maxim (de obicei 3) de incercari de logare (autentificare) in sistem.

3) Rainbow table

Al 3-lea tip de atac se numeste "**Rainbow table**" care are scopul de a "**descifra**" un **hash**. Mai stii ce este un hash ? In cazul in care nu, iti voi rezuma pe scurt (in capitolul 9 vorbim mai in detaliu despre asta).

Un **hash** este o *valoare unica* a unui cuvant (sau a oricarei combinatii dintre litere/cifre etc.). *Orice combinatie* de litere, cifre, cuvinte/fraze din aceasta lume va genera o **valoare unica**. Ei bine, acum gandeste-te la parola ta in momentul in care o introduci in contul de Facebook, Google etc.

Toate companiile **nu stocheaza direct parola ta** in baza lor de date (pentru ca implica un risc dpvd al securitatii), ci vor stoca acest **hash** (al parolei). In momentul in care un atacator *"fura" baza de date*, o fura cu ***username***-urile si *hash*-urile ***parolelor*** (si nu cu parola in *clear text*).

Astfel atacatorul va recurge la o lista de hash-uri pentru a descifra parolele "hash-uite" din baza de date furate. Aceasta lista se numeste "rainbow table" si incearca sa afle care este parola.

Si acum poate te intrebi, "De ce se fac lucrurile asa ?". Raspunsul e simplu: pentru ca procedeul de hash este ireversibil, adica odata generat hash-ul nu putem sa-l introducem prin aceeasi formula matematica si sa obtinem parola.

Astfel atacatorul isi incearca norocul cu lista lui de hash-uri (rainbow table) care sunt asociate unor parole.

In urmatorul capitol vom trece la primul pas spre generarea unui atac cibernetic, mai exact, vom vorbi despre Scanare. De asemenea, spre sfarsitul capitolului iti voi arata cum poti sa faci un atac de pin DoS folosind (Kali) Linux.

VIII. Scanarea Retelei si a Serverelor

Sunt sigur ca ai auzit de multe ori de conceptul de scanare a unei retele (sau a unui server). Well, in acest capitol vom discuta mai in detaliu despre tot acest concept si despre cum poti **scana retele si server** din doar cateva comenzi din (Kali) Linux sau Windows.

Ce inseamna sa "Scanez o Retea de Calculatoare" ?

Inainte sa trecem la a vedea cum pot sa scanez o retea, vreau sa-ti explic ce inseamna aceasta scanare. La ce ma refer cand spun am scanat reteaua X.Y.Z.A ? Ma refer la faptul ca am folosit un anumit program (in acest caz **Nmap**) cu ajutorul caruia am aflat care sunt dispozitivele conectate la retea in momentul de fata.

Nu doar ca am aflat care sunt aceste dispozitive (afland adresa lor **IP** si **MAC**-ul), ci putem afla si alte informatii precum:

- Tipul dispozitivului
- Sistemul de operare si versiunea folosita
- Porturile deschise
- Aplicatile care ruleaza pe acele porturi
- etc.

Avand aceste informatii, ne putem folosi de ele pentru a intelege mai bine cum este structurata reteaua, pentru a scana si, ulterior, a testa reteaua si serverele de vulnerabilitati (intr-un mod etic), pentru a ne asigura ca toate dispozitivele sunt up & running. Acestea , bineinteles, sunt doar cateva motive pentru care scanarea retelei si a device-urilor din ea are sens.

Cum Scanez o Retea ?

Scanarea retelei (si a componentelor ei) se face foarte usor, folosind Nmap. Nmap vine de la Network Mapper si ne ajuta sa "mapam" reteaua intr-un output (din terminal) destul de usor de inteles.
Programul pe care il folosesc in exemplul de mai jos (pentru scanarea retelei) se numeste **Nmap**. Nmap (pe Windows, programul cu interfata grafica se numeste **Zenmap**) este un tool gratuit extrem de folosit de hackeri si de ethical hackeri.

Cu ajutorul lui putem descoperi dispozitivele conectate la retea, porturile deschise de pe acestea si chiar si Sistemul lor de Operare.

Iata cateva exemple de comenzi pe care le putem da cu Nmap pentru a atinge diferite scopuri:

1) Scanare la nivel de retea cu Nmap

 # nmap -sP *192.168.1.0/24* -- scanare pe baza de ICMP (ping), afisand numarul de dispozitive din retea (aka **PING SCAN**)

 # nmap -sS *192.168.1.0/24* -- scanarea intregii retele cu scopul de a gasi porturile deschise (TCP, folosind SYN) de pe fiecare dispozitiv (aka. **PORT SCAN**)

In figura 6.1 de mai jos poti vedea in detaliu informatiile despre o parte din echipamentele conectate la retea (mai exact Routerul cu IP-ul 192.168.1.1 si un alt dispozitiv cu IP-ul 192.168.1.3). Pe langa faptul ca a descoperit ca aceste dispozitive sunt conectate la retea, Nmap a mai descoperit si porturile deschise pe aceste echipamente.

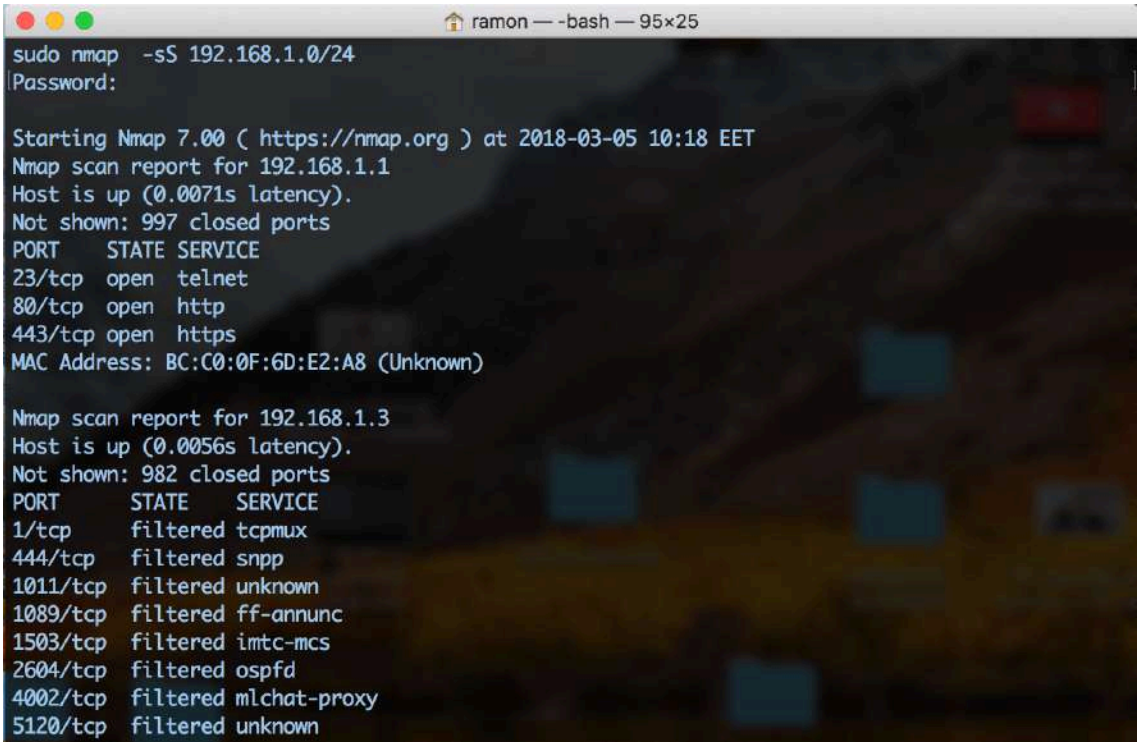


Figura 6.1

Dupa cum poti sa vezi, Routerul (192.168.1.1) are deschise 3 servicii destul de importante care pot fi vulnerabile si exploatate. Spre exemplu, portul 23 reprezinta Telnet ceea ce inseamna ca ne putem conecta de la distanta la acesta, putand chiar sa avem acces la CLI (linia de comanda).

De asemenea, portul 80, respectiv 443, care identifica traficul Web sunt deschise (deci ne putem conecta prin browser si putem incerca sa obtinem acces pe acest Router). Acum sper ca ai inteles rolul si puterea scanarii ;)

2) Scanare folosind Nmap la nivel de dispozitiv (server, laptop, telefon etc.)

 # nmap -A *192.168.1.1* -- scaneaza un singur device pentru *obtinerea serviciilor* (porturilor) si a sistemului de operare (aka. **OS SCAN**)

 # nmap -sT 192.168.1.254 -- scaneaza folosind pachete TCP

 # nmap -sU 192.168.1.1 -- scaneaza folosind pachete UDP

In figura 6.2 poti vedea rezultatul primei comenzi la care am mai adaugat si **-sS** pentru scanarea TCP a porturilor:

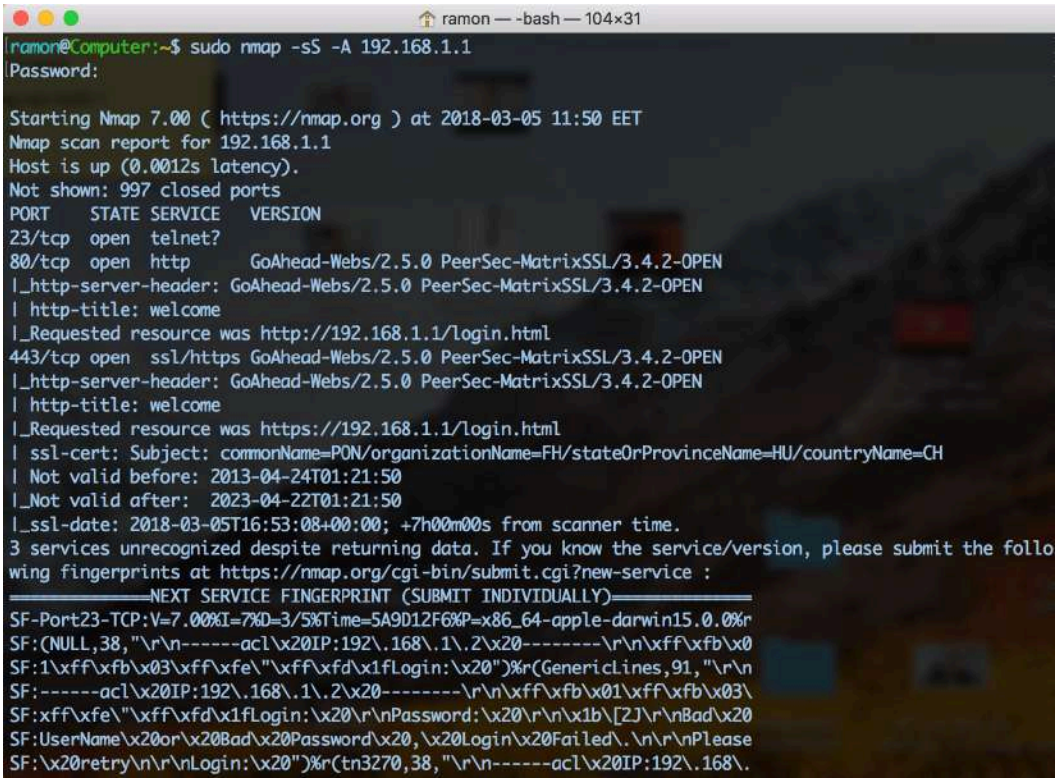


Figura 6.2

Daca vrei sa obtii (mai multe) informatii in timp real legate de scanare, atunci iti recomand sa adaugi **-v** la orice tip de comanda Nmap doresti. De asemenea, mai poti apasa si pe "Space" pentru a obtine date legate de progresul scanarii (vei vedea X% finalizat si timpul estimat).

Alte exemple de scanare folosind Nmap:

nmap -F 192.168.1.0/24 -- scaneaza fiecare device din retea pentru top 100 cele mai folosite porturi

nmap -sS -p 80,443,23,22,25 192.168.1.1 -- scaneaza device-ul pentru porturile date cu argumentul -p folosind pachete TCP SYN

nmap -F -oN *rezultat_scanare.txt* 192.168.1.0/24 -- scaneaza reteaua rapid si stocheaza rezultatul in fisierul rezultat_scanare.txt (foarte util in cazul unui script - Python)

3) Hping3

Un alt tool foarte util pe care il mai putem folosi pe langa Nmap este **hping3**. **Hping3** este un **generator de trafic**, similar cu ping, dar cu mult mai multe functionalitati. Este capabil sa trimita (pe langa trafic ICMP - ping) pachete de tipul TCP, UDP sau RAW-IP customizate (cu orice specificatie ii dam noi legat de aceste protocoale).

Spre exemplu putem trimite un packet TCP ACK sau FIN pentru a vedea cum reactioneaza serverul sau firewall-ul pe care dorim sa-l testam. Mai jos gasesti o lista cu lucrurile pe care le poti face cu acest tool.

Practic, hping3 ne ajuta sa facem face urmatoarele lucruri:

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

Iata cateva **exemple de folosire a hping3**:

 # hping3 -h -- pentru a afla mai multe despre argumentele disponibile

 # hping3 -1 *IP_VICTIMA* -- se trimite un ping (ICMP) normal (figura 6.3)

 # hping3 --traceroute -V -1 *IP_VICTIMA* -- se trimite un singur pachet de tip traceroute pentru a vedea pe unde merge acesta

 # hping3 -V -S -p 80 *IP_VICTIMA* -- se trimit pachete de tip TCP SYN pe portul 80 pentru a vedea daca raspunde aplicatia

In figura 6.3 de mai jos poti am facut cateva teste si poti vedea o parte exemplele enuntate mai sus:

```
root@rn-s-1vcpu-1gb-fra1-01:~# hping3 -1 hackthissite.org
HPING hackthissite.org (eth0 198.148.81.137): icmp mode set, 28 headers + 0 data bytes
len=42 ip=198.148.81.137 ttl=51 id=9426 icmp_seq=0 rtt=169.2 ms
len=42 ip=198.148.81.137 ttl=51 id=10767 icmp_seq=1 rtt=169.0 ms
len=42 ip=198.148.81.137 ttl=51 id=12684 icmp_seq=2 rtt=168.9 ms
^C
--- hackthissite.org hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 168.9/169.0/169.2 ms
root@rn-s-1vcpu-1gb-fra1-01:~# hping3 -V -S -p 80 hackthissite.org
using eth0, addr: 46.101.143.160, MTU: 1500
HPING hackthissite.org (eth0 198.148.81.136): S set, 40 headers + 0 data bytes
len=44 ip=198.148.81.136 ttl=53 DF id=43320 tos=0 iplen=44
sport=80 flags=SA seq=0 win=65535 rtt=163.0 ms
seq=4116557452 ack=513609534 sum=32e9 urp=0

len=44 ip=198.148.81.136 ttl=50 DF id=44497 tos=0 iplen=44
sport=80 flags=SA seq=1 win=65535 rtt=162.9 ms
seq=3555362188 ack=2032411494 sum=f5c4 urp=0

DUP! len=42 ip=198.148.81.136 ttl=50 id=45735 tos=10 iplen=40
sport=80 flags=A seq=1 win=0 rtt=890.9 ms
seq=4294967295 ack=2032411494 sum=2b36 urp=0
```

Figura 6.3

 # hping3 -c 1 -V -p 80 -s 5050 -A *IP_VICTIMA*

-- acest tip de scanare trimite un singur pachet TCP de tip ACK (-A) si ne ajuta sa ne dam seama daca un device este up in retea in momentul in care nu raspunde la ping (acesta fiind blocat de catre un firewall).

Argumentele comenzii (figura 6.4) reprezinta:

- **-c 1**: se trimite un singur pachet
- **-V**: verbose (afiseaza in timp real rezultatul scanarii)
- **-p 80**: portul destinatie este 80 (HTTP)
- **-s 5050**: portul sursa este 5050 (poate fi orice altceva)
- **-A**: se trimit pachete de tip TCP ACK

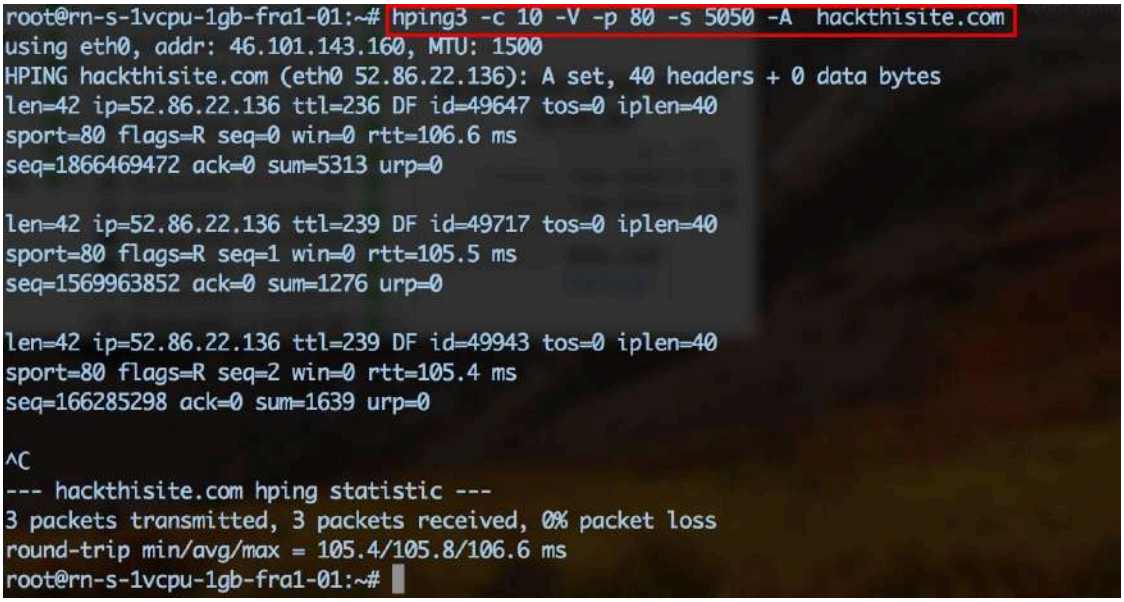


Figura 6.4

Daca dorim sa **ne acoperim urmele** (sa fim **anonimi**, sa nu se stie de unde provine scanarea/atacul) putem adauga argumentul **--rand-source:**

 # hping3 -c 1 -V -p 80 -s 5050 -A --rand-source *IP_VICTIMA*

Hping3 iti ofera posibilitatea sa fii foarte specific cu ceea ce faci. Spre exemplu daca folosim scanari de tipul TCP la nivel de server atunci ne putem folosi de mesajele TCP-ului (precum SYN, ACK, FIN, RST, URG etc.).
Revin cu ce am spus si la inceputul acestei carti: ESTE FOARTE IMPORTANT SA INTELEGI CUM FUNCTIONEAZA TEHNOLOGIA. In acest caz ma refer in mod special la modelul OSI, la protocolul TCP, la porturi etc.

In **capitolul 7** vom discuta despre **Firewall**, cum functioneaza acestea si vei vedea ca acest tip de scanare se potriveste in cazul lor pentru ca firewall-urile by default blocheaza tot traficul din Internet.

Dar cu **pachete trimise customizat** (un TCP ACK neasteptat spre exemplu) putem sa surprindem firewall-ul sau aplicatia (ex: server web) si sa ne dea un raspuns cu ajutorul caruia putem afla mai multe informatii despre el (un server pe Windows raspunde intr-un mod diferit fata de unul pe Linux etc. - exemplu de remote OS fingerprinting).

In continuare iti sugerez sa te joci cu aceste programe Nmap si hping3 sa faci putin mai mult research astfel incat sa le intelegi utilitatea si modul lor de functionare.

Cu **hping3** mai putem face si atacuri de tip **DoS** (despre care am vorbit in capitolul 5), in care facem flood catre un anumit dispozitiv:

```
# hping3 -V -c 2000000 -d 100 -S -w 64 -p 443 -s 591 --flood --rand-source IP_VICTIMA
```

Iar argumentele acestei comenzi reprezinta:

- --flood: trimite pachetele cat mai repede posibil
- --rand-source: genereaza adrese IP sursa diferite pentru fiecare pachet
- -V: cat mai explicit (ofera informatii in timp real)
- -c --count: numarul total de pachete
- -d --data: marimea pachetelor
- -S --syn: pachete TCP de tip SYN
- -w --win: window size (default 64)
- -p --destport: portul destinatie
- -s --baseport: portul sursa (by default este aleatoriu)

Acestea au fost doar cateva exemple. Acum tu poti incepe sa te joci cu acest tool (iti recomand sa folosesti Kali Linux si sa incepi cu reteaua ta locala). In loc de IP_VICTIMA poti da IP-ul Routerului tau sau a unui telefon/laptop/server din reteaua ta.

PS: in cazul in care folosesti Linux (si nu Kali Linux) poti instala Nmap sau hping3 folosind comanda:

```
# sudo apt-get install nmap hping3
```

De ce vrem sa Scanam Reteaua ?

Pentru ca mai departe putem folosi aceste informatii pentru a ne decide focusul, cand vine vorba de penetration testing. Pe ce ne focusam ? Care este tinta cea mai vulnerabila din retea si ce aplicatii exista pe ea de care sa putem profita ? Pentru un Hacker (fie el etic sau nu) raspunsul la aceste intrebari este extrem de important.

De ce ? Pentru ca, daca nu este foarte bine informat despre retea si despre componentele existente in ea, Hacker-ul isi va pierde timpul cu anumite parti care nu pot fi exploatate si va risca sa fie detectat.

Acest proces de scanare face parte din ciclul de Penetration Testing care este compus din 5 etape (figura 6.5) si despre care vorbesc mult mai pe larg in cursul de *Introducere in Securitate Cibernetica si Hacking*, la care iti ofer acces **GRATUIT** la primul capitol pentru ca ai facut investitia in aceasta carte.

Figura 6.5

VII. Securitatea Web

In acest capitol vom vorbi pe scurt despre securitatea web si despre cateva atacuri pe care trebuie sa le ai in minte. Sunt absolut sigur ca de foarte multe ori ai auzit la TV, la radio sau in diferite parti ca site-ul companiei X a fost spart, site-ul organizatiei Y a fost pus jos, iar Hackerii au inlocuit site-ul principal cu o pagina falsa care avea un anumit mesaj.

Ei bine, vreau sa iti spun ca in mare (Hackerii mai putin experimentati), toti cauta la foarte multe site-uri 1 - 2 vulnerabilitati foarte cunoscute de care ei pot sa profite. Exista foarte multe tool-uri care ii ajuta sa gaseasca relativ usor aceste vulnerabilitati, iar ulterior ii ajuta sa le si exploateze.

O parte dintre aceste vulnerabilitati (la nivel de site-uri web) sunt extrem de bine prezentate si documentate in topul **OWASP** (**O**pen **W**eb **A**pplication **S**ecurity **P**roject). OWASP-ul este o organizatie non-profit care se ocupa cu imbunatatirea securitatii a aplicatiilor software si web.

Ei au un **top 10 celebru** in sfera Securitatii Cibernetice la nivelul aplicatiilor web si sunt cele mai des raportate/intalnite incidente de securitate din anii precedenti. **OWASP** organizeaza chiar si **evenimente** locale (chiar si la noi in tara), astfel creandu-se o comunitate de oameni pasionati de securitate cibernetica.
Daca auzi la un moment dat de un astfel de eveniment si ai ocazia sa mergi, iti recomand sa faci acest pas pentru ca vei vedea, in primul rand ca merita experienta, iar in al doilea rand, faptul ca inveti o gramada de lucruri de la foarte multi oameni.

Spre exemplu, iata in figura 7.1 o lista a celor mai des intalnite incidente de securitate web care au avut loc in anul 2017 (in comparatie cu anul 2013):

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Figura 7.1

Dupa cum poti sa vezi, in mare parte, este vorba de aceleasi tipuri de vulnerabilitati, top-ul modificandu-se foarte putin intr-o perioada de 3 ani. Voi lua doar o parte dintre aceste atacuri si iti voi explica ce reprezinta fiecare si cum le poti face si tu pe propriul site.

Iata atacurile despre care vom discuta in continuare:

- SQL injection
- XSS
- Security Misconfiguration (folosirea HTTP in loc de HTTPS, neschimbarea parolei default)

Acum hai sa incepem discutia despre atacurile web cu primul atac/vulnerabilitate (si cel mai des intalnit) din lista de mai sus:

1) SQL injection

Cand vorbim de SQL injection, vorbim in primul rand de baze de date, iar in al doilea rand de un atac (o vulnerabilitate) la nivelul acestora. Hai sa vedem ce este SQL. **SQL** (**S**tructured **Q**uery **L**anguage) este un limbaj de interogare cu bazele de date. Acesta este folosit pentru a comunica direct cu baza de date prin diferite comenzi adresate acesteia. Exista mai multe tipuri/forme de SQL, dar la baza lucrurile sunt la fel. Poti sa vezi aici un tutorial despre bazele de date (MySQL) pe Linux.

Practic SQL injection (figura 7.2) este un mod prin care un Hacker poate accesa o baza de date intr-un mod neautorizat si pot extrage informatii extrem de importante (date despre persoane, username-uri & parole, date de contact precum email-uri sau informatii bancare, etc.). Acest lucru se intampla in general datorita unei erori de programare.

Figura 7.2

Unde au loc atacurile de tip SQL injection ? Cel mai adesea acestea au loc in momentul in care atacatorul gaseste “o casuta” in care poate introduce date. Spre exemplu, gandeste-te la o casuta de tip search in care oricine poate scrie orice.

Daca codul din spate (cel mai des fiind PHP) nu este scris cum trebuie, atunci Hackerul poate sa introduca comenzi SQL care interactioneaza direct cu baza de date, astfel reusind sa extraga diferite informatii.

Acum vreau sa te gandesti ca in momentul in care interactionezi cu un “input form” (o casuta in care poti scrie si trimite catre server ceva), in spate se intampla acest lucru:

```
SELECT * FROM ? WHERE ? LIKE '%';
```

Adica, limbajul PHP va genera o astfel de comanda pentru a interactiona (si cauta) cu baza de date. Unde apare *'%'*, va fi inlocuit cu ceea ce introduci tu in acel input form.

Iata un exemplu de cod SQL care poate fi introdus intr-un astfel de camp (ATENTIE: nu va functiona pentru orice site. Iti sugerez sa folosesti aplicatia bWAPP si sa testezi pe ea):

```
' OR 1=1;--
```

Poti incerca pe acest site sa introduci in loc de username si parola comanda SQL de mai sus.

SQLmap este un tool foarte bun pe care il poti folosi pentru a **testa vulnerabilitatile** la nivel de baze de date pe un site. SQLmap va face toate aceste incercari ca injectie SQL **automat** pentru tine (ba chiar va incerca sa sparga si hash-ul parolelor pe care le va gasi in baza de date).

De asemenea, iti recomand sa downloadezi si sa-ti instalezi **bWAPP**, care este o aplicatie web care contine peste 100 de vulnerabilitati clasice (printre care si OWASP top 10). Poti exersa pe aceasta masina virtuala (la care te vei conecta prin browser -> pui adresa IP a masinii virtuale in browserul tau) fara a avea probleme ulterior (mai stii ce vorbeam in capitolul 1... despre hackeri ?). In cazul in care doresti sa-ti instalezi bWAPP pe Kali (sau orice alta distributie de Linux sau Windows) iti recomand sa urmaresti acest tutoriale.

2) XSS (Cross-Site Scripting)

Cand vine vorba de SQL injection, dupa cum ai vazut, atacatorul merge direct la site si incearca sa obtina acces in baza de date a acestuia, astfel incat sa poata sa extraga date confidentiale (useri si parole, informatii bancare, adrese de mail etc.). In cazul XSS lucrurile se intampla altfel. Focusul atacatorului se indreapta spre utiizator (cel care acceseaza site-ul), moment in care se foloseste de un script pentru a-l ataca.

XSS presupune injectarea unui malware (script malitios de data aceasta) in site (fara a-l afecta in vreun fel), iar la accesarea site-ului de catre utilizator, acest cod va fi executat direct in browser. Codul este scris in JavaScript, limbaj care este executat de catre browser.

Cel mai simplu mod prin care se poate face asta este prin injectarea codului malitios intr-un comentariu sau intr-un script care poate fi rulat automat.
De exemplu, Hackerul poate incorpora un link catre un script JavaScript rau intentionat intr-un comentariu pe un blog.

Atacurile de tip **XSS** (Cross-site scripting) pot deteriora in mod semnificativ reputatia site-ului prin plasarea informatiilor utilizatorilor la risc fara a lasa urme cum ca raul a avut loc. Acum, aflandu-se in aceasta situatie, orice informatie delicata pe care un utilizator o trimite catre site (cum ar fi datele persoanele, informatiile bancare sau alte date private) - poate fi deturnata prin intermediul script-urilor de pe site-uri fara ca proprietarii site-ului sa realizeze că exista o problema.

O parte din atacurile care pot sa aiba loc in urma unui atac de tip XSS:

- **Furarea de cookie-uri** - duplicarea unui cookie poate duce la duplicarea sesiunii de pe site-ul valid catre un site fals al atacatorului care poate fura datele utilizatorului
- **Keylogger** - trimiterea catre atacator a tuturor literelor tastate de catre utilizator
- **Phishing** - manipularea utilizatorului spre a lua o actiune de care nu este constient, urmand ca datele sale sa fie expuse

Astfel dupa ce un atacator incearca un atac de tip XSS (de obicei pe orice site care are o sectiune de comentarii, search sau input de date, etc.), datele victimei (ex: sesiunea web curenta in care se afla, cookie-urile) pot fi furate si folosite de catre hacker pentru a accesa diferite pagini/resurse ale acesteia. Astfel, atacatorul nu are nevoie de userul sau

de parola victimei pentru ca are deja cookie-urile. Folosind XSS, el a reusit sa faca un alt tip de atac cunoscut sub denumirea de **Session Hijacking**.

NOTE: **Iata aici un site** foarte bun pe care poti sa inveti mai multe despre atacurile web. Site-ul a fost conceput pentru a educa dezvoltatorii de software web pentru a fi constienti de vulnerabilitatile existente si pentru a le arata cum sa le rezolve.

3) Security Misconfiguration

O alta problema care este intalnita foarte des, iar din pacate o mare parte a lumii o omite, este cea legata de parole. DA, in anul 2018 inca ne punem problema asta. Foarte multe persoane nu iau in serios politicile de securitatea care vizeaza parolele si (in primul rand) schimbarea celor default, iar in al doilea rand schimbarea cu o parola complexa (de peste 8 caractere) cu caractere alfanumerice.

Fiecare caracter in plus pe care il adaugam unei parole creste intr-un mod dramatic complexitatea si in acelasi timp dificultatea de spargere (sau ghicire) a acesteia.

Deci, sfatul meu, desi pare banal, este sa-ti reevaluezi username-urile si parolele tale de pe diferite sisteme si treci la actiune pentru a le schimba. Daca mai poti sa adaugi inca un factor de autentificare pe langa parola, ar fi grozav.

Spre exemplu poti folosi autentificarea biometrica (pe baza de amprenta) sau cea pe baza de user, parola si token (in general SMS) pe telefon care este mult mai sigura fata de varianta clasica.

Vom discuta in capitolul 8 (Criptografie) mai multe detalii despre diferitele forme de autentificare. Pana atunci treci la actiune ! :D Pe langa asta vreau sa te uiti la figura 7.3, unde poti sa vezi o lista cu **userii si parolele default**. Aici poti sa gasesti site-ul cu userii si parolele default ale mai multor vendori de echipamente de retea.

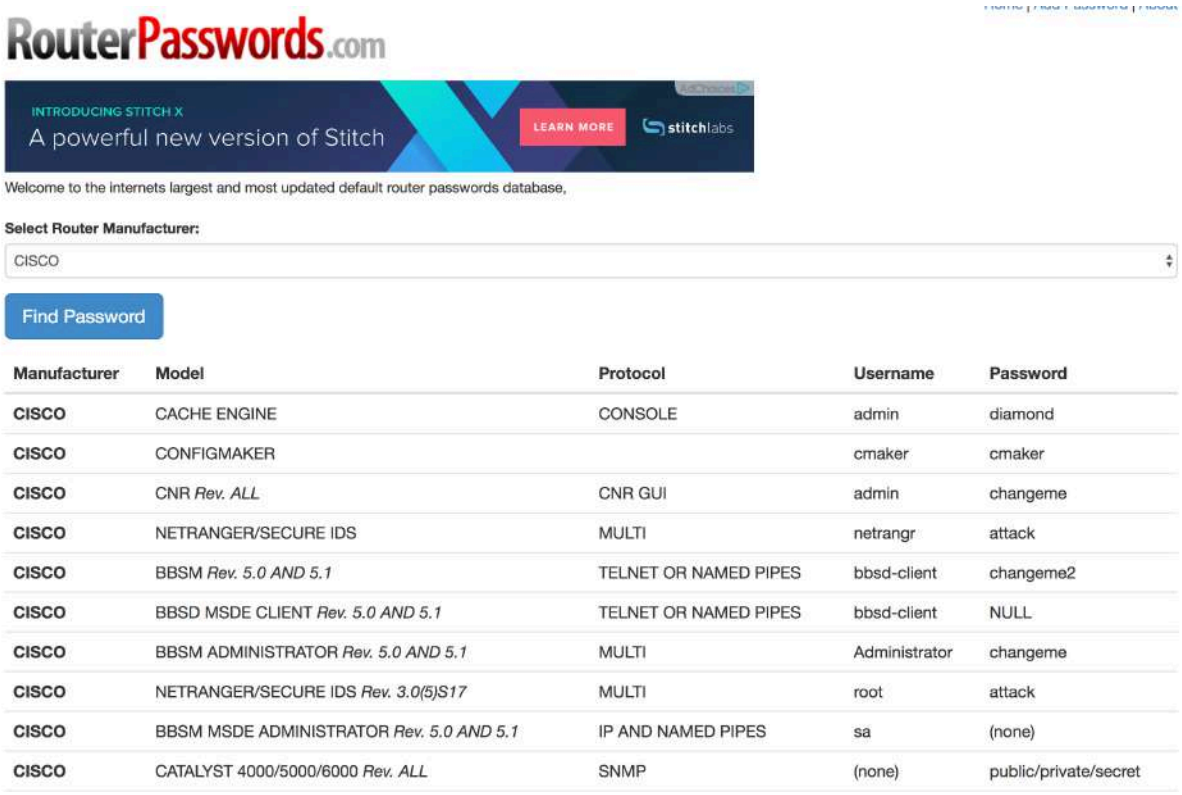


Figura 7.3

O alta problema care inca apare pe foarte multe site-uri poarta denumirea de Directory Listing si se refera la faptul ca un Hacker poate intra pe site-ul tau (mai exact pe partea din spate a site-ului) si se poate plimba din folder in folder astfel ca el ajunge la un moment dat sa aiba acces la informatii private site-ului.

Asta in cazul unui business online care vinde produse educative (carti, cursuri, etc.) poate fi o catastrofa pentru ca Hackerii ii pot accesa site-ul si pot merge din folder in folder pentru cautarea, descarcarea si chiar stergerea produselor educative de pe site.

Aici intervine elementul de securitate la nivel de foldere si fisiere si ma refer la oprirea accesului neautorizat bazat pe drepturi de acces. Fiecare fisier, folder in parte (indiferent ca vorbim de Windows, Linux sau Mac) are un set de reguli de acces asupra lui. Astfel administratorii pot permite sau restrictiona accesul in functie de necesitati si de nivelul de confidentialitate al fisierului.

Pentru ca tot suntem la *capitolul de securitate* la nivelul site-urilor web, propun sa mergem mai departe si sa vorbim despre unul dintre cele mai folosite platforme pentru site-urile web. Este vorba despre WordPress:

4) WordPress

WordPress (figura 7.4) este cea mai folosita platforma de creare si gestionare a site-urilor web din lume. El este un **CMS** (**C**ontent **M**anagement **S**ystem), o platforma de gestionare a continutului. Astfel, prin intermediul lui oricine isi poate creea un blog, un site sau un magazin online multifunctional. In prezent peste 27.5% din topul 10 milionane de site-uri la nivel mondial il folosesc. Fiind atat de utilizat la nivel mondial, iti dai seama ca este in interesul Hackerilor (mai ales pentru ca acesta platforma contine numeroase bug-uri si vulnerabilitati care, in ultimul timp, de la versiune la versiune au fost diminuate).

Figura 7.4

Un alt motiv pentru care WordPress este atat de folosit se datoreaza numarului de pluginuri existente care pot fi folosite pentru a imbunatatii site-ul, experienta utilizatorului, etc. Astfel persoana care gestioneaza un site/blog folosind un astfel de CMS, NU are nevoie de cunostinte de programare pentru ca plugin-urile se ocupa (in mare) de tot ce e necesar. In marketplace-ul WordPress exista peste 50.000 de plugin-uri gratuite, iar pe langa acestea mai intervin si cele platite care au fost dezvoltate de diferite companii.

Un alt aspect foarte interesant legat de WordPress este faptul ca el este OpenSource. Asta inseamna ca este dezvoltat de o comunitate de programatori la care oricine poate lua parte.

Ca tehnologii de functionare, WordPress are nevoie de **LAMP** (*Linux, Apache, MySQL, PHP*). Fiecare dintre aceste componente este critica in functionarea unui site. Daca nu esti familiar cu LAMP iti voi explica pe scurt ce reprezinta fiecare componenta in parte:

1. **Linux** - OS-ul pe care va functiona site-ul, motivul fiind simplu: un OS flexibil, stabil si mult mai securizat fata de Windows
2. **Apache** - Serverul web folosit pentru gazduirea site-ului, cel mai raspandit in Internet
3. **MySQL** - Baza de date folosita de catre WordPress pentru a stoca informatiile site-ului (articole, useri, comentarii si orice alt tip de continut care necesita stocare)
4. **PHP** - Limbajul de programare care interactioneaza cu fiecare componenta (baza de date, serverul web si OS-ul). PHP este un limbaj de programare web folosit pe partea de backend (ceea ce noi nu vedem cand accesam un site)

Iata **aici un tutorial** scurt in care iti arat cum poti sa-ti faci un site in doar 10 minute. Este important sa treci prin procesul de instalare pentru a intelege (pe scurt) cum functioneaza WordPress-ul. Acum hai sa mergem la urmatorul tool care te va ajuta sa testezi dpvd. security, site-ul tau:

WPScan

WPScan este un tool de scanare (si bineinteles de spargere) a unui site construit pe WordPress. El este open source, deci poate fi folosit de catre oricine doreste sa-si testeze site-ul de vulnerabilitati. Acest tool iti poate oferi foarte multe informatii despre site-ul tau:

- Versiunea de WordPress folosita (un indicator foarte bun)
- Plugin-urile instalate
- Potentiale vulnerabilitati existente pe site, care pot fi ulterior exploatate
- Aflarea userilor existenti pe site
- Efectuarea de atacuri de tip Brute Force prin folosirea unui dictionar pentru aflarea parolei

Acum hai sa trecem la treaba si sa-ti arat cum poti sa faci aceste scanari despre care vorbeam mai devreme folosind **WPScan**. In cele ce urmeaza iti voi arata cateva exemple de scanare pe care le poti face folosind acest tool. Atentie, faci **scanare** (deci **Reconnaissance**), *nu ataci site-ul*.
De multe ori scanarea poate fi perceputa ca testand activ sistemul sa vezi ce poti gasi prin el. Poti compara acest concept cu cel in care cineva (strain) doreste sa “vada” ce ai tu prin casa. Intra pe usa (fara ca tu sa fi acasa) si incepe sa se uite prin lucrurile tale, dar nu ia nimic, cu scopul de a folosi acele informatii mai tarziu.

Face o scanare “non-intrusiva” (figura 7.5):

```
# wpscan --url www.example.com
```

Enumereaza plugin-urile instalate:

```
# wpscan --url www.example.com --enumerate p
```

Ruleaza toate tool-urile de enumerare cu scopul de a afla cat mai multe informatii:

```
# wpscan --url www.example.com --enumerate
```

Enumera userii existenti pe site:

```
# wpscan --url www.example.com --enumerate u
```

Acestea sunt cateva posibilitati de folosire a tool-ului WPScan. In figura 7.5 de mai jos am dat prima comanda pe un site bazat pe WordPress (a carei identitate nu o voi publica) pentru a vedea ce informatii putem sa aflam despre el. Mentionez ca eram autorizat sa fac o astfel de scanare pe acest site.

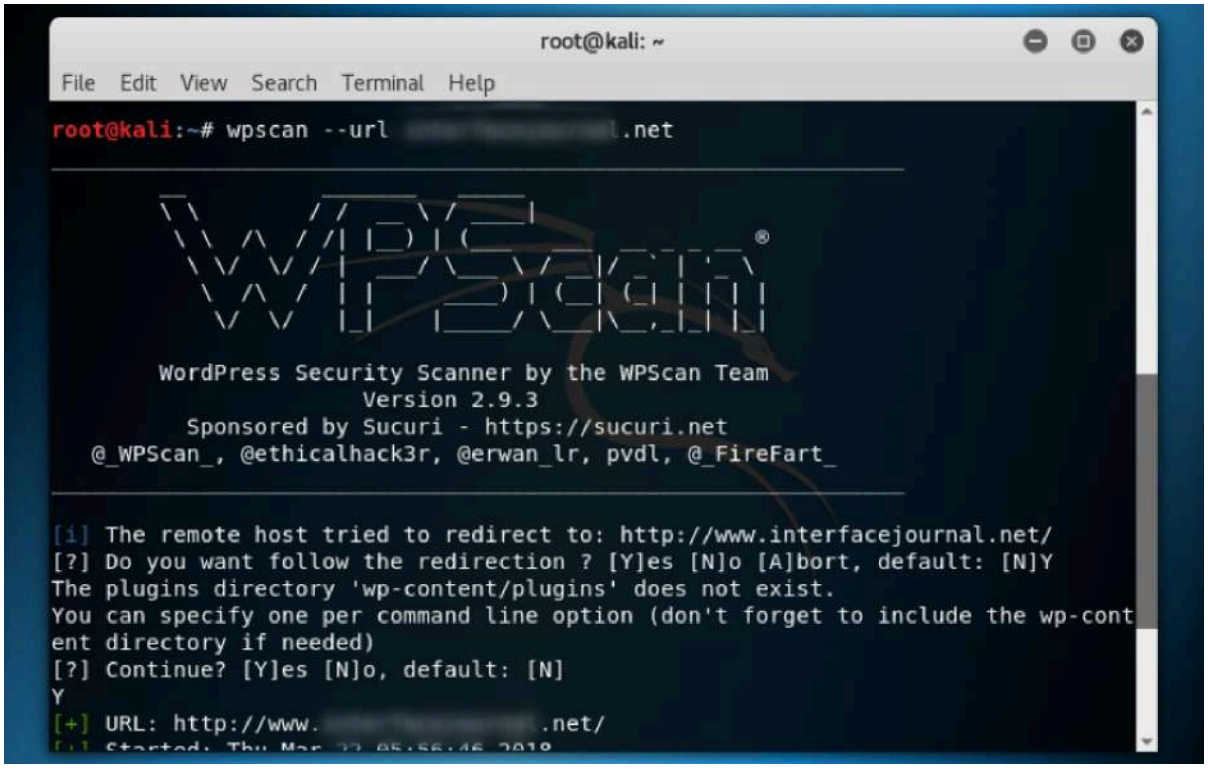


Figura 7.5

:

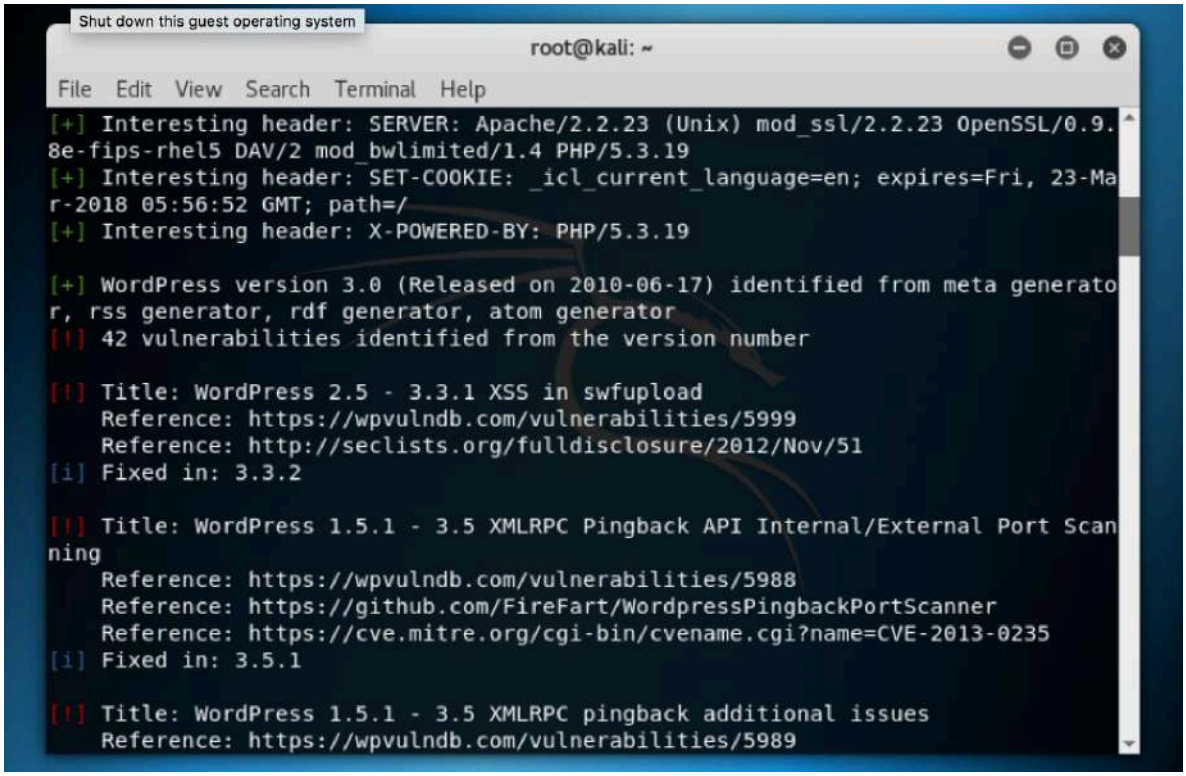


Figura 7.6

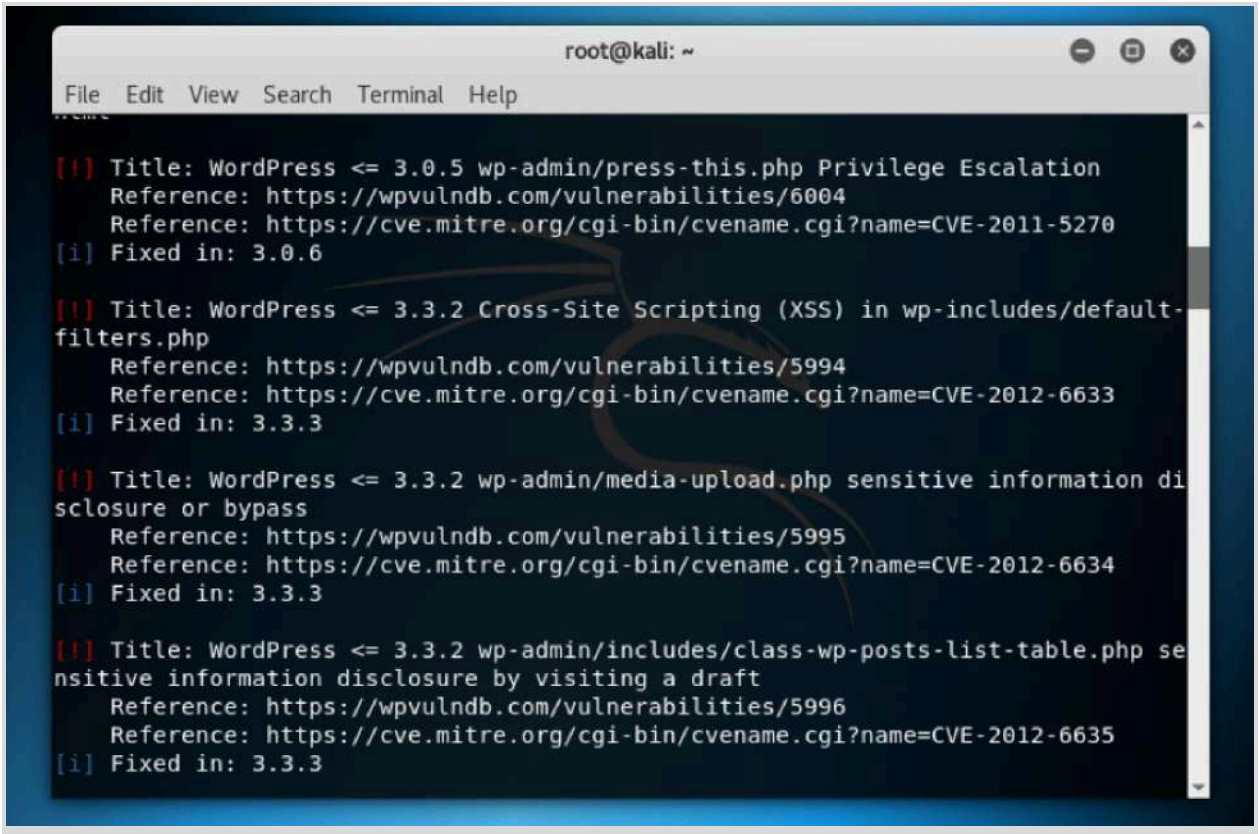


Figura 7.7

In figurile 7.6, respectiv 7.7, poti sa vezi continuarea comenzii date. Si iata, dintr-o simpla scanare cate vulnerabilitati am gasit pe acest site (el in mod cert are nevoie de un update). Dupa cum vezi sunt multe vulnerabilitati care pot fi exploatate folosind diferite metode. Mai mult decat atat, existe si aceste **CVE**-uri (**C**ommon **V**ulnerability and **E**xposures) care descriu vulnerabilitatea si modul in care ea poate fi exploatata.

Pentru ca tot vorbim de *WordPress si de vulnerabilitati* pana la urma, **AICI** poti sa vezi o baza de date care contine toate **vulnerabilitatile cunoscute** si facute **publice** pentru fiecare versiune in parte. Pe langa asta vreau sa-ti spun ca toate atacurile despre care am vorbit in acest capitol se aplica si cazul WordPress-ului. Din pacate *SQLi, XSS, Directory Traversal* sunt cateva (din multe) atacuri care se pot face relativ usor pe aceasta platforma. Cu WPScan tot ce faci este sa le descoperi mult mai repede.

Important e sa le **constientizezi**, sa-ti scanezi in mod frecvent site-ul (tau sau al unui client), sa descoperi vulnerabilitati noi si sa faci astfel incat sa le rezolvi cat mai repede posibil.

5) Google Hacking

Cred ca ai avut o reactie putin diferita cand ai vazut titlul acestui subiect: “Wow ! pot sa hackuiesc Google-ul ?” sau “pot sa fac hacking cu Google ?”. Pot sa-ti spun ca da, in a 2-a situatie (desi nici prima nu e exclusa :D). Te poti folosi de Google pentru a descoperi diferite site-uri care au anumite **pagini indexate** in motorul de cautare. Astfel, folosind cateva keyword-uri specifice de cautare, Google iti poate oferi exact ceea ce cauti (**site-uri** care sa contina exact **URL-ul** pe care tu il cauti cu un **plugin vulnerabil**, o pagina cu **informatii** despre *baza de date* cum ar fi *userul, parola* si numele bazei de date, etc.).

Da, administratorii site-urilor nu sunt atenti (probabil nu sunt nici macar constienti) de faptul ca site-ul lor poate “**scapa informatii**” pretioase pe Google, astfel fiind extrem de expus la atacuri din Internet.

Din nou, iti dau aceasta informatie pentru ca o poti folosi in scopuri etice (pentru a cerceta si testa site-ul tau sau cel al unui client). Nu uita faptul ca accesul neautorizat intr-un sistem va fi sanctionat penal si poti face cativa ani de inchisoare pentru asa ceva (cunosc cateva persoane care au patit asta...).

Acum ca ti-ai reamintit acest lucru, iata cateva exemple prin care poti face research. Prin aceasta cautare, Google ne va afisa site-uri care au ca plugin WordFence (un plugin care se ocupa cu securizarea site-ului - firewall, virus scanner etc.)

```
inurl:”/wp-content/plugins/wordfence/”
```

Acesta a fost doar un exemplu (in figura 7.8). Desigur tu poti sa inlocuiesti continutul de cautare dupa “**inurl:**” cu orice doresti tu, in functie de interesul tau actual. In figura

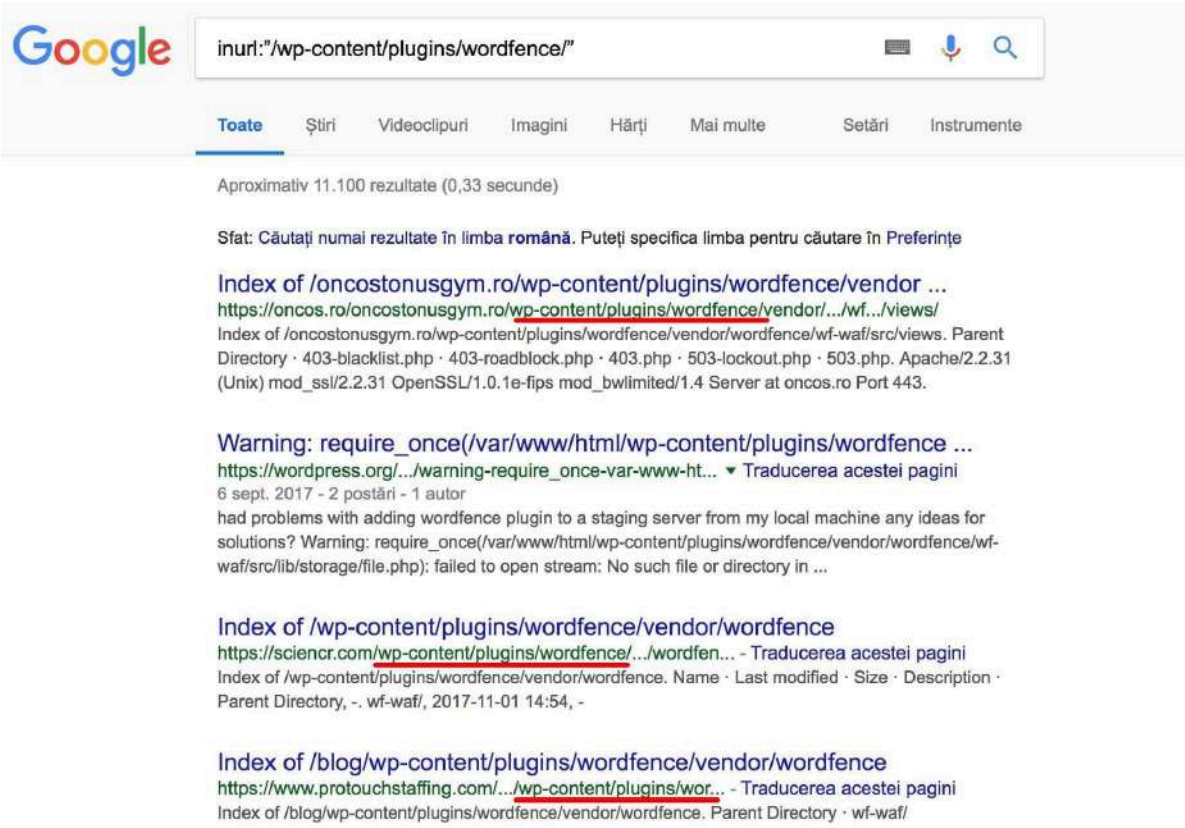


Figura 7.8

Prin urmatoarea comanda in Google Search vei putea sa vezi diferite site-uri in functie de versiunea de WordPress pe care o folosesc. Ulterior poti sa folosesti WPScan si sa afli mai multe detalii legate de vulnerabilitatile existe pe acesta, dupa care poti incerca sa profiti (etic) de ele. Vei vedea ca sunt foarte multe versiuni de WordPress foarte vechi, extrem de vulnerabile. Ce iti recomand eu tie este sa iei legatura cu adminul site-ului, sa-l faci constient de faptul ca este expus la un risc masiv si sa-l rogi sa te lase sa-i demonstrezi asta (adica sa-i ataci site-ul :D).

```
inurl:"wordpress readme.html"
```

Iata, in figura 7.9, cateva site-uri cu versiuni vechi de WordPress (la data scrierii acestei carti, *Martie 2018*, versiunea cea mai recenta este **4.9.4**):

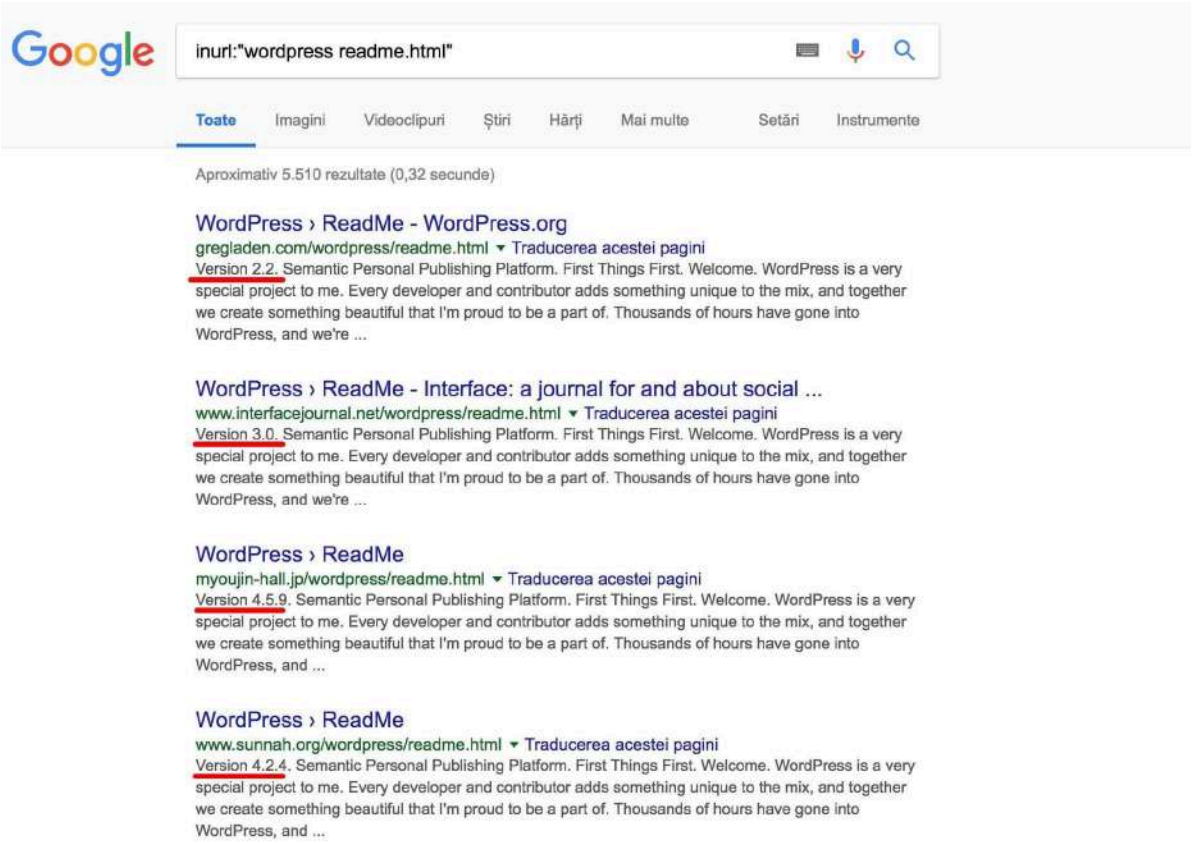


Figura 7.9

In continuare iti recomand sa cercetezi si tu. Sa te joci (intr-un mediu izolat sau intr-unul in care ai acces/permisiune) cu toate uneltele despre care am vorbit in acest capitol. Asadar, mult spor ! :)

IX. Firewall

Incepem un nou capitol interesant in care vorbim despre Firewall-uri si cum functioneaza acestea. Un lucru vreau sa-ti spun: atat timp cat vei lucra cu orice inseamna servere, retele, site-uri web (mai ales din punct de vedere CyberSecurity), te rog sa fii sigur ca **te vei intalni cu Firewall-uri.**

Ce este un Firewall ?

La fel ca si un Router sau un Switch, un **firewall** este un echipament de retea care are scopul de a securiza (proteja) reteaua de potentialii atacatori (hackeri) din Internet.

Prin securizarea retelei, ma refer in mod special la **filtrarea pachetelor** (adresa IP sursa/destinatie, porturi, filtrare URL etc.) cu scopul de a nu permite accesul unei persoane neautorizate in retea.

By default, **firewall-ul blocheaza tot traficul** din extern in intern si ramane la latitudinea administratorului sa configureze politicile de acces in retea, necesare companiei. *Cum face asta ?* Vei afla in cele ce urmeaza ;)

Un lucru pe care vrea sa-l retii: **NU exista securitate perfecta**, iar un Firewall nu este suficient pentru a securiza reteaua, ci el este o componenta importanta care ajuta la securizarea accesului extern (adica din Internet in LAN).

Pe langa acest element de retea mai sunt multe alte componente care trebuiesc luate in calcul cand vine vorba de securitate. Dupa cum poti sa vezi in figura 8.1, firewall-ul conecteaza toate echipamentele la Internet (deci practic ia locul Routerului in aceasta situatie). Scopul lui, in acest caz, este sa le protejeze de potentialele atacuri din Internet, care la un moment dat pot incerca sa exploateze anumite vulnerabilitati pe sisteme. Firewall-ul functioneaza la **nivelul 4** (by default), dar poate fi configurat sa functioneze si la **nivelul 7** (din modelul OSI).

Ce inseamna asta ? Inseamna ca se poate “uita adanc” in pachet. Poate chiar sa **vada** ce URL incerci sa accesezi si sa ti-l blocheze, poate chiar sa scaneze programul pe care incerci sa-l descarci si sa-si dea seama daca este virusat sau nu.

Asta se aplica in cazul firewall-urilor perfomante si scumpe, adesea numite **UTM** (Unified Threat Management).

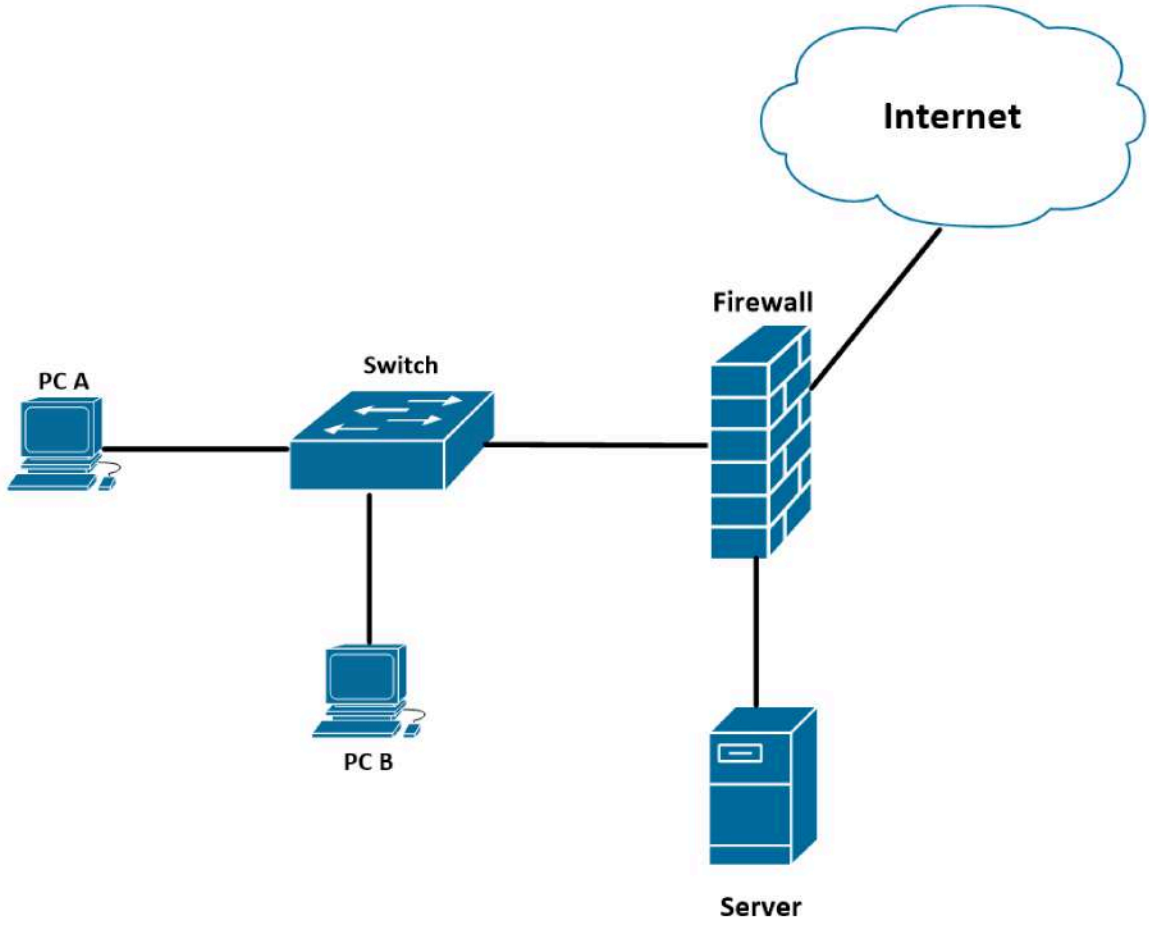


Figura 8.1

Cum functioneaza zonele de Securitate ale unui Firewall ?

Firewall-ul functioneaza pe baza de zone de securitate. Practic fiecare interfata a unui firewall reprezinta o zona de securitate. Noi putem creea mai multe astfel de zone si sa includem una sau mai multe interfate in ele. Aceste zone de securitate, de obicei, se impart in 3 categorii:

- **INSIDE** - zona care cuprinde reteaua interna (LAN)
- **OUTSIDE** - zona care cuprinde reteaua externa organizatiei (de obicei Internetul)
- **DMZ** - zona speciala care contine servere

Fiecarei zone in parte, firewall-ul ii va aloca un **nivel de securitate** (definit printr-un numar intre 0 - 100) care influenteaza comportamentul acestuia.

Spre exemplu: daca avem o zona de **INSIDE** cu un nivel de securitate de **100** si o zona de **OUTSIDE** cu un nivel de securitate de **0**, atunci **ORICE** trafic din INSIDE va fi **lasat** (de catre firewall) **sa treaca** in OUTSIDE (aka. Internet), dar traficul care vine din *OUTSIDE in INSIDE* va fi **oprit,** astfel fiind nevoie de reguli speciale (aka. invatare dinamica - statefull - a traficului) care trebuiesc a fi configurate pe firewall.

DMZ-ul (**D**emilitarized **Z**one) reprezinta o zona speciala in care sunt plasate echipamentele care necesita acces din Internet. In cea mai mare parte a timpului in aceasta categorie se incadreaza serverele (Web, Fisiere, VPN etc.). Acestea sunt resursele publice ale companiei la care, teoretic oricine are acces.

Aceste servere le izolam intr-o zona speciala (DMZ) astfel incat daca acestea ajung sa fie corupte, restul retelei sa nu sufere (Hackerul sa nu poata patrunde in LAN - reteaua interna companiei).

DMZ-ul are un **nivel de securitate mai mic** (30 dupa cum poti sa vezi si in figura 8.2) fata de cel al LAN-ului, dar mai mare fata de cel al Internetului. Astfel oricine din DMZ poate accesa Internetul si invers datorita unor regului din firewall despre vom vorbi imediat. In figura 8.2 poti sa vezi cum arata aceste zone de securitate.

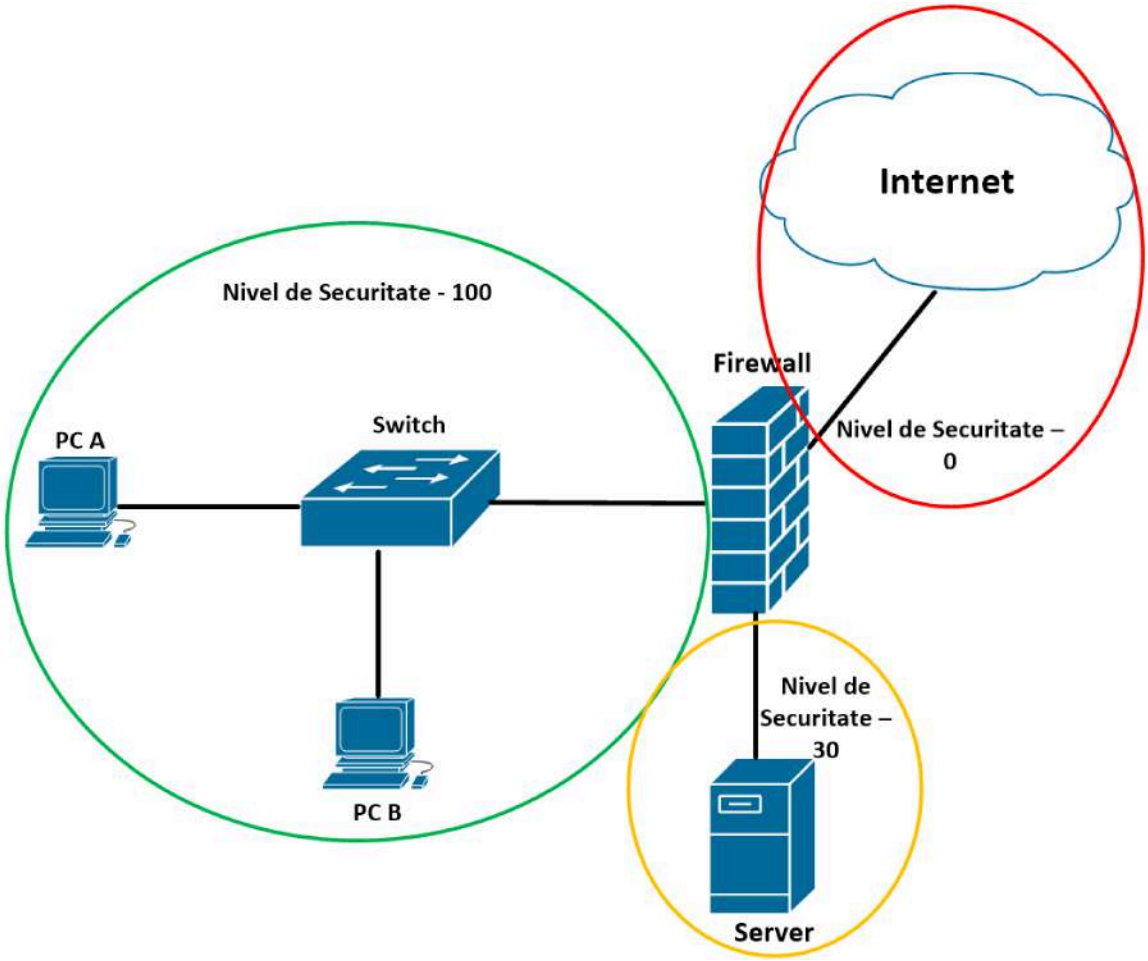


Figura 8.2

Poate la un moment dat te-ai intrebat: "*oare ce face firewall-ul asta 'in spate'* ? Adica cum functioneaza el defapt ?". Iar eu iti voi raspunde in cele ce urmeaza in sectiunea despre ACL-ul (practic acesta e "ingredientul" secret care ne protejeaza noua retelele... si DA, chiar si Routerul tau Wireless are un mini-firewall incorporat care foloseste ACL-uri :D)

ACL (Access Control List)

ACL-ul este componenta care sta la baza modului se functionare a unui firewall. Este componenta esentiala cand vine vorba de **protejarea** si **filtrarea traficului** (de obicei cel din Internet)

Un **ACL (Access Control List)** reprezinta un set de reguli cu scopul de a bloca sau permite accesul dintr-o retea la o anumita resursa. Aceste reguli sunt setate pe Routere sau pe Firewall-uri.

“ACL-urile stau la **baza *conceptului de securitate*** (limitare a accesului) intr-o sau dintr-o retea (ex: Din Internet in reteaua Interna - LAN sau invers)."

Gandeste-te la acest concept, ca la un Bodyguard care sta la intrarea unui club in care se organizeaza o petrecere privata. Acesta va avea o lista cu toti invitatii la acea petrecere.

Pe masura ce oamenii incearca sa intre in locatie, bodyguard-ul ii va verifica pe fiecare in parte; se va uita pe lista (**ACL**) si va decide pentru fiecare persoana daca are voie in club sau nu. Practic daca te afli pe lista vei fi lasat sa intri (permit) la petrecere, iar daca nu apari pe lista, nu vei avea acces (**deny**) inauntru.

Pentru inceput trebuie sa ne gandim ce tip de trafic (aka. reguli) vrem sa permitem in reteaua noastra, urmand ca apoi sa includem aceste reguli in ACL. Dupa cum vom vedea mai jos, aceste **reguli pot varia**: de la *permiterea unei retele intregi* sa acceseze o alta retea, la *permiterea sau respingerea accesului a unui singur PC* la un server pe un anumit port (ex: SSH - 22, Web - 80).

Dupa ce o astfel de lista de acces este creata si sunt adaugate reguli de ***permit*** *sau* ***deny,*** va fi pusa in functie (cum ? setand-o pe o interfata a Firewall-ului sau a Routerului pe o anumita directie - **IN** sau **OUT**). **IN**(side) reprezinta traficul care **intra** in Firewall, iar **OUT**(side) reprezinta traficul care **iese** din Firewall.

In mod normal, exista 2 tipuri principale de ACL-uri care pot fi setate (atat pe Firewall-uri cat si pe Routere sau servere Linux):

- **ACL Standard**
- **ACL Extended**

1) ACL Standard

Scopul ACL-urilor de tip Standard este sa faca filtrarea traficului dupa ***IP-ul sursa*** **!** Cel mai usor mod de a intelege este printr-un exemplu (precum cel din figura 8.3 si apropo, poti inlocui in mintea ta aceste Routere cu Firewall-uri, nu conteaza, ideea este sa intelegi conceptul):

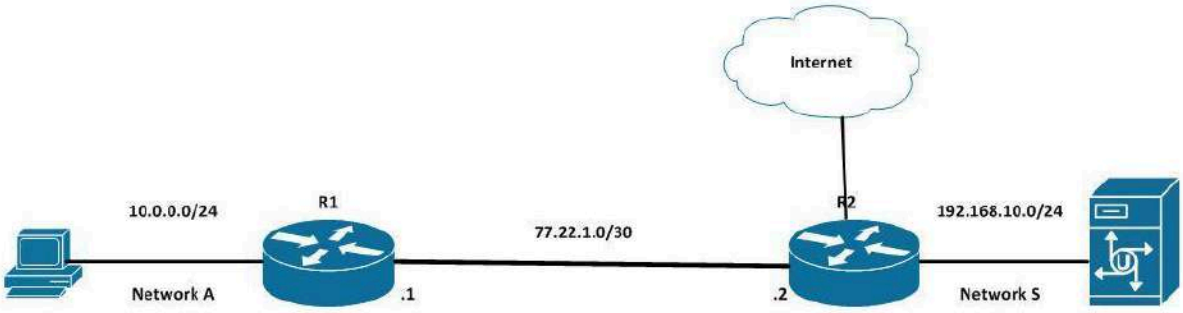


Figura 8.3

Sa spunem ca (din motive de securitate) PC-ului din reteaua A, cu IP-ul 10.0.0.8, nu ii vom da voie sa acceseze server-ul din reteaua S. Astfel tot ce trebuie sa facem este sa cream o lista de acces in care sa specificam acest lucru. Regulile acestei liste vor arata astfel:

#**deny** 10.0.0.8
#**permit any**

Aceasta regula va fi setata pe R2, pe **interfata cea mai apropiata** de server (in cazul acesta, cea direct conectata la server) in **directia OUT**. Am adaugat cea de a 2-a linie (permit any) deoarece, by default, la finalul fiecarui ACL apare o regula "implicita de deny" (#deny any). Noi dorim sa oprim traficul de la PC la server si sa **permitem in rest orice alt tip de trafic**.

ATENTIE: nu trebuie sa cunosti (sau sa retii) sintaxa pe care ti-o voi prezenta in acesta sectiune a cartii. Comenzile provin din linia de comanda pentru echipamentele Cisco, dar vreau tot ce vreau de la tine este **sa INTELEGI CONCEPTUL** si modul de functionare al acestor ACL-uri. *De ce ?* Pentru ca te vei intalni cu ele, foarte des. Fie ca le vei configura, fie ca doresti sa treci de ele este foarte important **sa stii cum functioneaza**.

2) ACL Extended

Scopul ACL-urilor de tip Extended este sa faca filtrarea traficului dupa:

- ***IP Sursa***
- ***IP Destinatie***
- ***Port Sursa***
- ***Port Destinatie***
- ***Protocol (IP, TCP, UDP etc.)***

Astfel, acest tip de liste ne ofera o flexibilitate mult mai mare cand vine vorba de control. Putem controla orice flux de trafic indiferent de sursa, destinatia si aplicatia folosita.

Iata cateva scenarii practice

Pe scurt, practic ACL-urile au nevoie de urmatoarele informatii pentru a le putea pune in practica:

1. Lista impreuna cu regulile de **permit/deny** in functie de nevoi
2. Interfata pe care dorim sa aplicam aceste reguli
3. Directia traficului (IN/OUT) de pe interfata

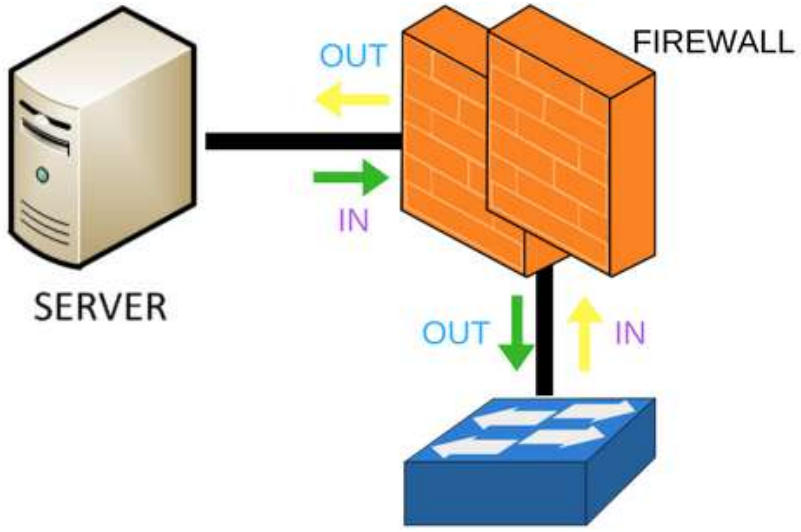
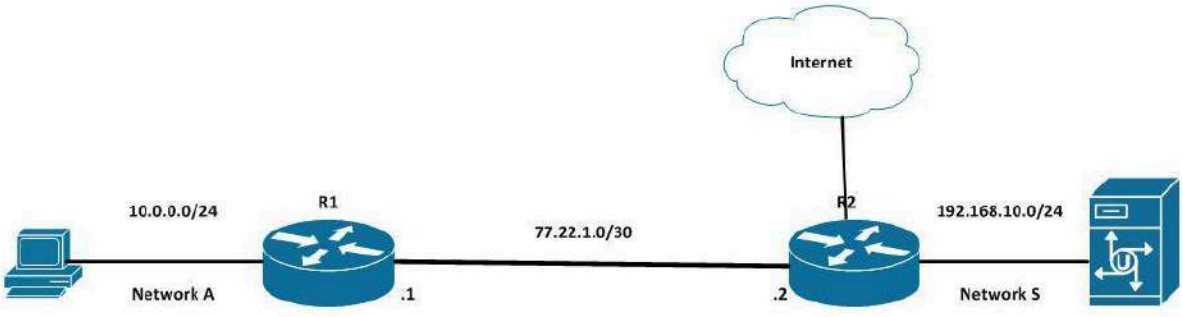


Figura 8.4

Dupa cum poti sa vezi si in figura 8.4, traficul trimis din reteaua Switch-ului va **INTRA (IN)** pe interfata Firewall-ului si va **IESII (OUT)** pe interfata conectata la Server. Exact opusul se intampla atunci cand server-ul raspunde celui care l-a contactat. Acum sa reluam imaginea din figura 8.3



Scenariu #1: Sa presupunem ca dorim sa oprim PC-ul (*10.0.0.8*) din retea A de a trimite orice tip de trafic catre Server. In cazul acesta avem nevoie de **o regula** care filtreaza dupa IP-ul sursa (ACL Standard). Regulile vor arata astfel:

#**deny host** 10.0.0.8
#**permit any**

Cum verificam setarile ? In primul rand vom genera trafic ICMP (ping) de la PC1 catre server (192.168. si dupa cum putem vedea in figura de mai jos, acesta nu merge. Iata si dovada ca R2 a blocat traficul. Rezultatul comenzii **#show access-list** ne indica faptul ca avem **8 matches** pe regula de deny pentru PC (figura 8.5) !

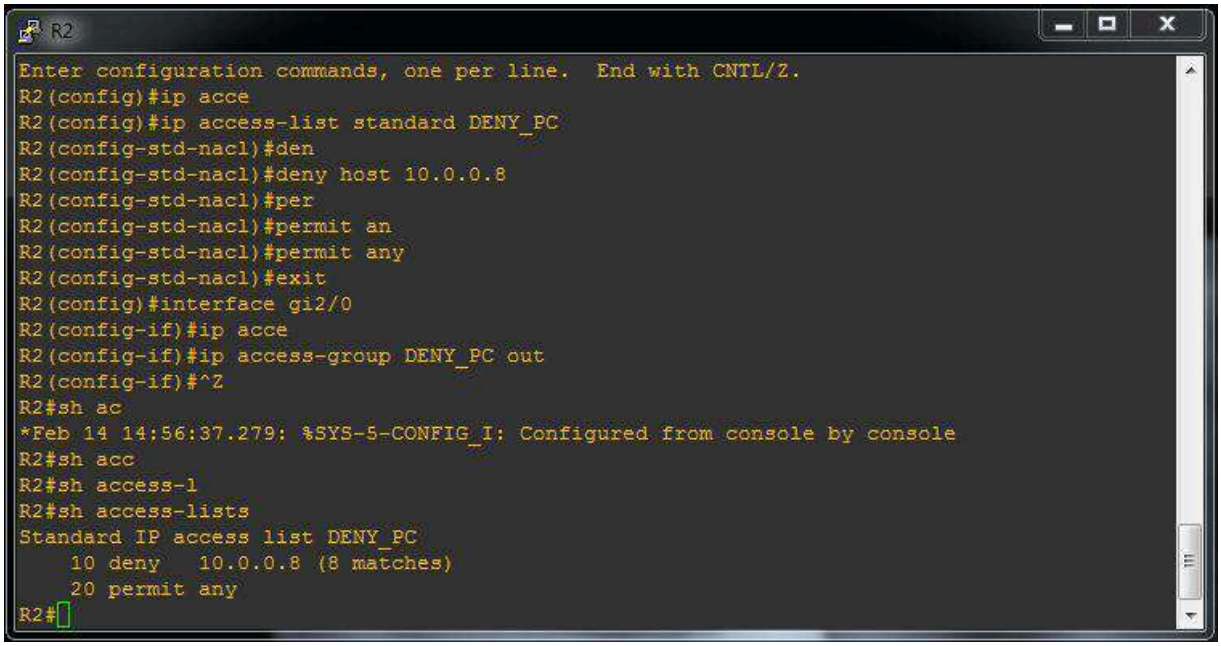


Figura 8.5

Scenariu #2: Sa presupunem ca dorim sa oprim orice tip de trafic Web (**HTTP - 80** - si **HTTPS - 443**) din reteaua PC-ului catre Internet. In cazul acesta avem nevoie de **o regula mai specifica** (de un *ACL Extended*). Regulile vor arata astfel:

#**deny tcp host** 10.0.0.8 **any eq** 80
#**deny tcp host** 10.0.0.8 **any eq** 443
#**permit ip any any**
Astfel, primele 2 reguli vor bloca traficul Web (port-urile 80 si 443) pentru PC catre any (orice destinatie), iar ultima regula va permite orice alt tip de trafic de la orice sursa la orice destinatie.

Aceasta regula ***va fi setata cat mai aproape de sursa*** (pe R1 interfata legata la PC) in ***directia IN***. Acum vom genera trafic web (din consola PC-ului catre Server - 192.168.10.10):

La fel ca mai sus, in figura 8.6 poti sa vezi faptul ca traficul web a fost **blocat (6 matches) prima linie din lista:**

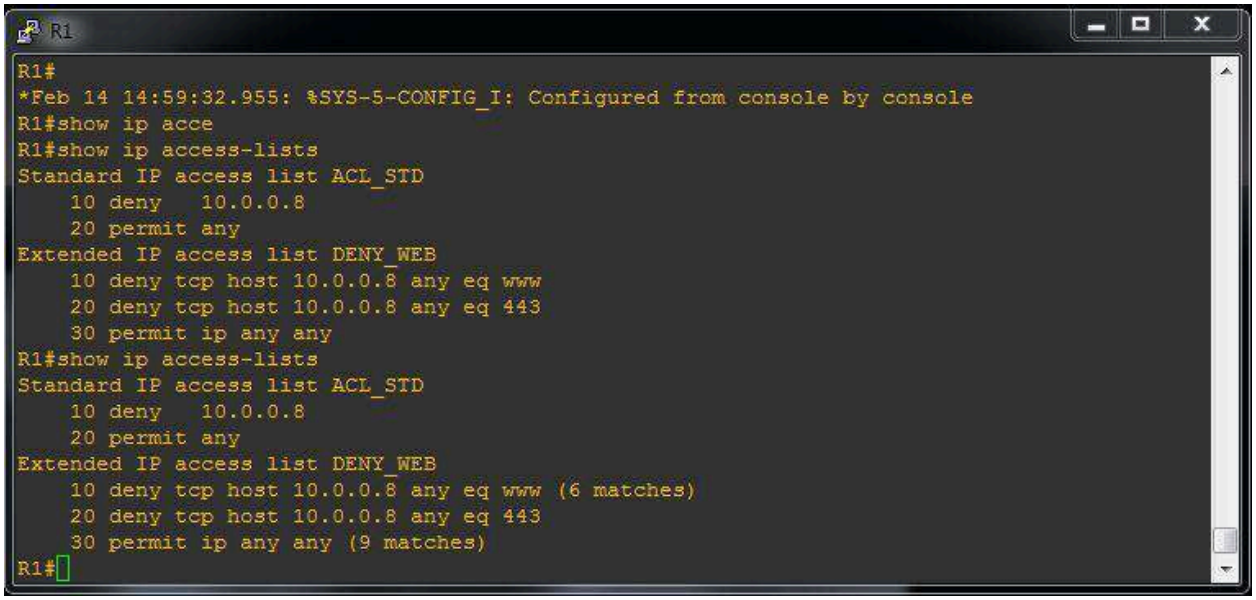


Figura 8.6

Alte exemple (ACL Standard):

#deny 192.168.99.0/24 -- va permite tot range-ul /24

#permit 85.1.245.5 -- va permite doar acest IP

#deny 172.16.0.0/17 -- va permite reteaua 172.16.0.0/17

Alte exemple (ACL Extended):

#permit ip 172.30.0.0/24 any -- permite traficul de la sursa 172.30.0/24 catre orice destinatie

#permit tcp host 10.45.21.5 eq 22 any -- permite orice trafic SSH de return de la 10.45.21.5

#deny udp 172.16.0.0/24 85.98.2.0/23 eq 53 -- blocheaza traficul DNS (port 53 UDP) de la reteaua 172.16.0.0/24 la 85.98.2.0/23

Daca vrei sa vezi un scenariu practic **in GNS3** am creat acest tutorial pentru a vedea cum poti sa blochezi traficul pe un **PC** catre un server **Web** (Linux).

Solutii de Firewall-uri existente pe piata

Cand vorbim despre diferitele tipuri de firewall-uri de pe piata avem o gama variata din care sa alegem (totul depinde de competentele noastre si de bugetul nostru). Exista doua mari categorii in acest sens:

1. ***Vendor specific*** - Cisco ASA, Palo Alto, Checkpoint, Fortinet etc.
2. ***Open Source*** - pfSense, OPNSense, IP Fire etc.

In mare, toate aceste firewall-uri **functioneaza intr-un mod similar** (conceptul la baza este acelasi), doar ca fiecare vendor/dezvoltator vine cu **elementele** sale de **diferentiere** care il fac unic (*inteligenta artificiala pentru detectia de malware, anti-virus, anti-spam incorporta, filtrare la nivel de URL,* etc.). In prezent piata tinde sa mearga tot mai mult spre Palo Alto, datorita inovatiilor in materie de tehnologie pe firewall-urile lor, iar un vendor cunoscut pe partea de retelistica (Cisco), ramanand in urma la acest capitol cu al sau firewall, ASA (Adaptive Security Appliance).

Daca iti doresti o solutie ieftina (chiar gratuita), buna si rapid de implementat, atunci una dintre variante poat fi chiar aceste firewall-uri Open Source despre care vom vorbi in cele ce urmeaza.

In aceasta sectiune vom vorbi mult mai in detaliu despre solutile Open Source, iar ca exemplu principal vom alege **OPNSense** (figura 8.7) datorita interfetei mai prietenoase.

Figura 8.7

Pentru inceput haide sa vorbim pe scurt despre **pfSense**:

pfSense

pfSense este cea mai cunoscuta optiune de firewall open source existenta pe piata. Este folosita de multe companii (chiar si de corporatii) pentru protejarea retelelor, in mod special a traficului care vine din Internet. La baza acestui Firewall sta o distributie de Unix, FreeBSD, cunoscuta in comunitate ca find una foarte securizata si reliable. In figura 8.8 poti vedea logo-ul acestui Firewall, iar in figura 8.9 de mai jos poti vedea cum arata **interfata** de configurare (**GUI)** a acestui Firewall.

Figura 8.8

Dupa cum poti sa vezi, marele avantaj este fix acesta, ca exista o interfata grafica din care se pot face setarile firewall-ului. Pe langa aceasta interfata, bineinteles, exista si una in linie de comanda (care de multe ori poate compensa lipsurile celei grafice - din browser). In figura de mai jos poti vedea dashboard-ul principal al acestui OS, care la o prima vedere pare putin cam aglomerat.

Toate aceste firewall-uri Open Source (pfSense, OPNSense, IP Fire etc.) le vei putea **instala** pe **propriul laptop**, intr-o *masina virtuala* sau chiar pe un calculator cu 2 interfete (una care va fi utilizata pentru LAN, iar cealalta pentru WAN - conexiunea cu Internetul). Acest calculator (sau laptop mai vechi) il vei putea folosi pe post de “Router / Firewall” care sa te conecteze la Internet si bineinteles sa-ti protejeze reteaua.

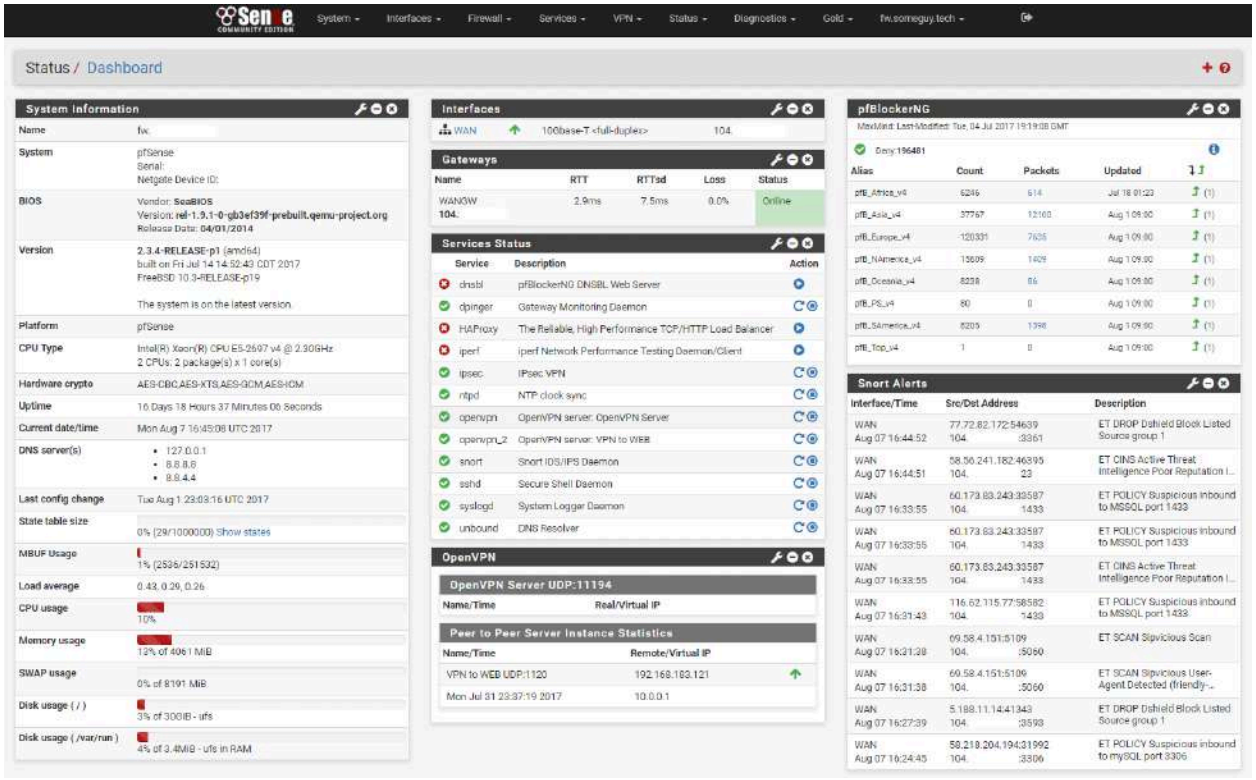


Figura 8.9

Acum vom discuta despre OPNSense, o varianta de firewall Open Source, care provine (la baza) din pfSense (defapt este un fork - o copie - a acestuia, in stadiul initial).

OPNSense

OPNSense este o alta alternativa de Firewall Open Source existent pe piata (pe care eu o prefer mai mult, datorita interfetei si design-ului mai user-friendly), iar noi il vom folosi pentru a ilustra functionalitatea sa in acest capitol. De **AICI** poti descarca ultima versiune a acestui OS, pe care ulterior o vei putea instala intr-o masina virtuala (recomandarea mea). Selecteaza ***amd64*** (daca ai procesorul pe 64-bit), image type: ***dvd*** (asta in cazul in care o vei instala local pe o masina virtuala), iar apoi poti selecta ce mirror doresti tu (serverul de la care se va downloada fisierul de instalare).

Dupa ce ai descarcat imaginea OS-ului ai 2 optiuni:

- *Instalare clasica* (similar cu ce am facut in cazul Kali Linux)
- *Rulare **Live*** - fara necesitatea de a instala OS-ul (NU vor fi salvate setarile)

La inceput oricum se va face rularea Live a OS-ului (adica nu va fi nevoie sa instalezi OPNSense-ul pentru a-l putea folosi). Dupa ce ai pornit masina virtuala cu imaginea ISO a OPNSense-ului, vei ajunge la un moment dat la setarea interfetelor (exact ca in figura 8.10):

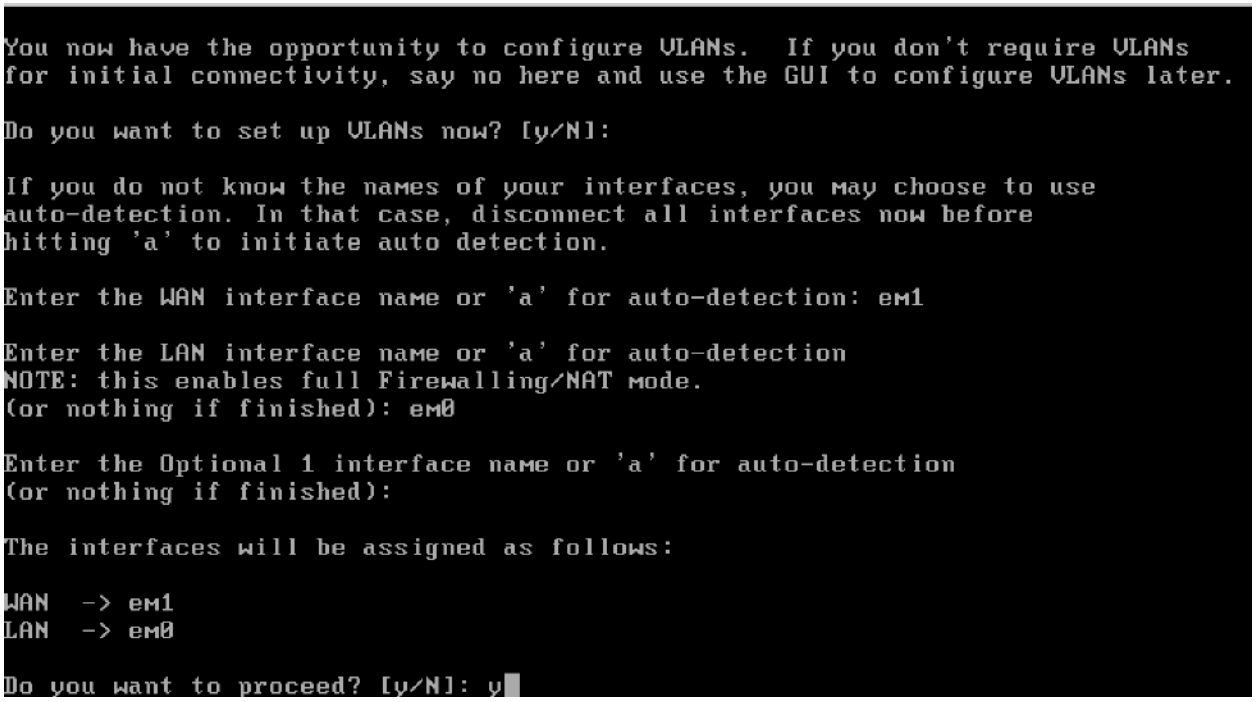


Figura 8.10

Aici, dupa cum poti sa vezi, setam 2 interfete:

- **WAN** - pentru conexiunea cu Internetul
- **LAN** - pentru conexiunea din reteaua locala (catre Internet)

Acest aspect este foarte important datorita regulilor setate in background (in spate se seteaza ACL-uri si politici de NAT pentru a mentine un nivel inalt de securitate si functionalitatea Internetului). Dupa setarea celor 2 interfete (care trebuie sa existe inca inainte de pornirea masinii virtuale - **ASIGURA-TE** ca ai configurate **2** astfel de **Interfete** - de preferat in retelel diferite).

Acum haide sa ne logam in consola Firewall-ului cu userul ***root*** si parola ***opnsense*** (figura 8.11):

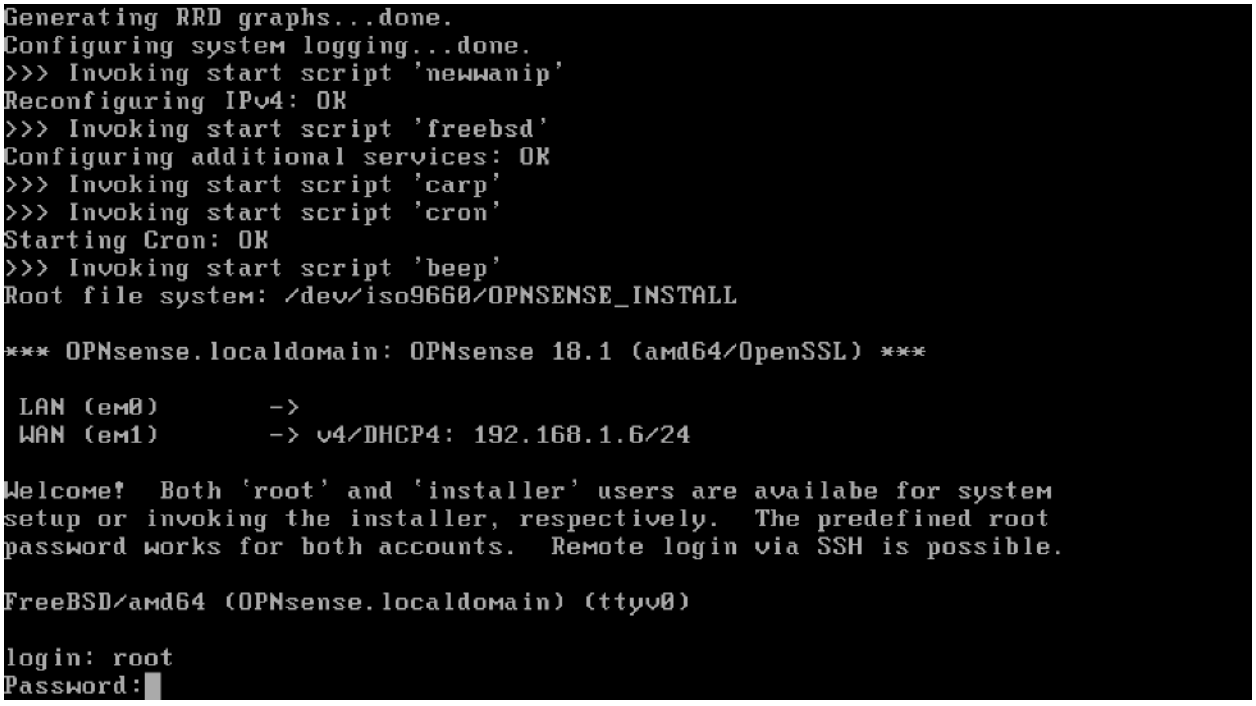


Figura 8.11

Dupa ce am introdus datele de logare vom accesa meniul din CLI (Command Line Interface) a Firewall-ului nostru care arata similar cu cel din figura 8.12 de mai jos:

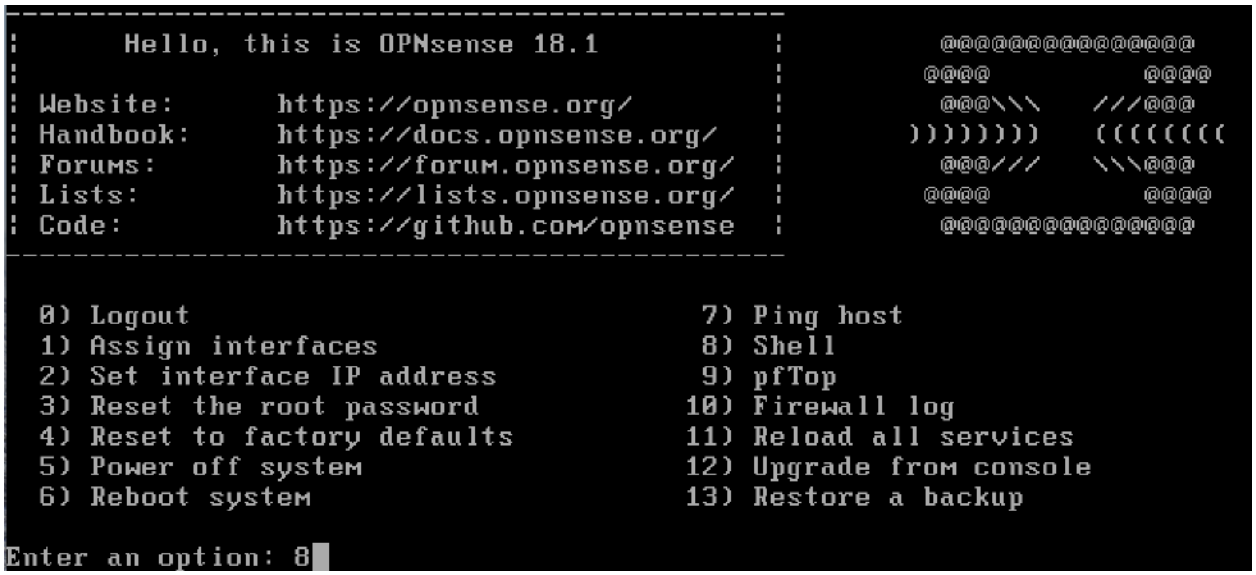


Figura 8.12

In acest stadiu avem mai multe optiuni (testarea conectivitatii, setarea interfetelor, modificarea parolei userului root si cel mai important, accesarea shell-ului - aka. Linia de

comanda din FreeBSD). Astfel noi vom introduce 8 si vom avea acces la linia de comanda. Fiind un OS care are la baza Unix inseamna ca linia de comanda este similara cu cea din Linux (comenzi precum - *cd, ls, mv, find, grep, ps* - apar si aici - figura 8.13). Bineinteles ca exista si comenzi care difera, acestea fiind specifice distributiei.

```
root@OPNsense:~ # ls
.cshrc          .login          .profile        .vimrc
root@OPNsense:~ # cd ..
root@OPNsense:/ # ls
.cshrc          boot            home            net             sys
.profile        conf            lib             proc            tmp
.rr_moved       dev             libexec         rescue          usr
COPYRIGHT       entropy         media           root            var
bin             etc             mnt             sbin
root@OPNsense:/ # ifconfig em1
em1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=98<VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:0c:29:f2:db:31
        hwaddr 00:0c:29:f2:db:31
        inet6 fe80::20c:29ff:fef2:db31%em1 prefixlen 64 scopeid 0x2
        inet 192.168.1.6 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
root@OPNsense:/ #
```

Figura 8.13

Hai sa ne conectam si intr-un alt mod la masina virtuala (SSH):

```
ramon@Computer:~$ ssh root@192.168.1.6
The authenticity of host '192.168.1.6 (192.168.1.6)' can't be established.
ECDSA key fingerprint is SHA256:7Jd4SnuIgTzbtOtX4ZjIKI/RexpKK35Rd8HugXKlKvE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.6' (ECDSA) to the list of known hosts.
Password for root@OPNsense.localdomain:
Last login: Tue Mar 27 04:16:22 2018
-------------------------------------------
|      Hello, this is OPNsense 18.1       |
|                                         |
| Website:      https://opnsense.org/     |
| Handbook:     https://docs.opnsense.org/|
| Forums:       https://forum.opnsense.org/|
| Lists:        https://lists.opnsense.org/|
| Code:         https://github.com/opnsense|
-------------------------------------------

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Upgrade from console
  6) Reboot system                      13) Restore a backup

Enter an option: 8
```

Figura 8.14

Dupa cum poti sa vezi in figura 8.14, ne putem conecta si prin **SSH** care este **pornit** by **default**,daca esti pe **Windows** poti sa folosesti PuTTY, iar din **Linux** poti sa folosesti direct **terminalul** si comanda:

#**ssh root@***ADRESA_IP*

ATENTIE: by default pe OPNSense este **pornit Firewall**-ul. Asta inseamna ca iti va bloca traficul SSH initial. Ce trebuie tu sa faci, este sa-l accesezi din consola (figura 8.13) si sa dai comanda #**pfctl -d** (asta il va opri).

Acum ca ai vazut cam care e treaba cu Firewall-ul OPNSense (din linia de comanda), propun sa trecem la partea de configurare si ajustare a setarilor acestuia prin interfata din browser. Astfel vom adauga **adresa IP a Firewall**-ului (pe care o aflam folosind comanda #**ifconfig**) in **browser** dupa care vei introduce **user-ul si parola.** Vezi figura 8.15 de mai jos in care ma aflu in dashboardul principal:

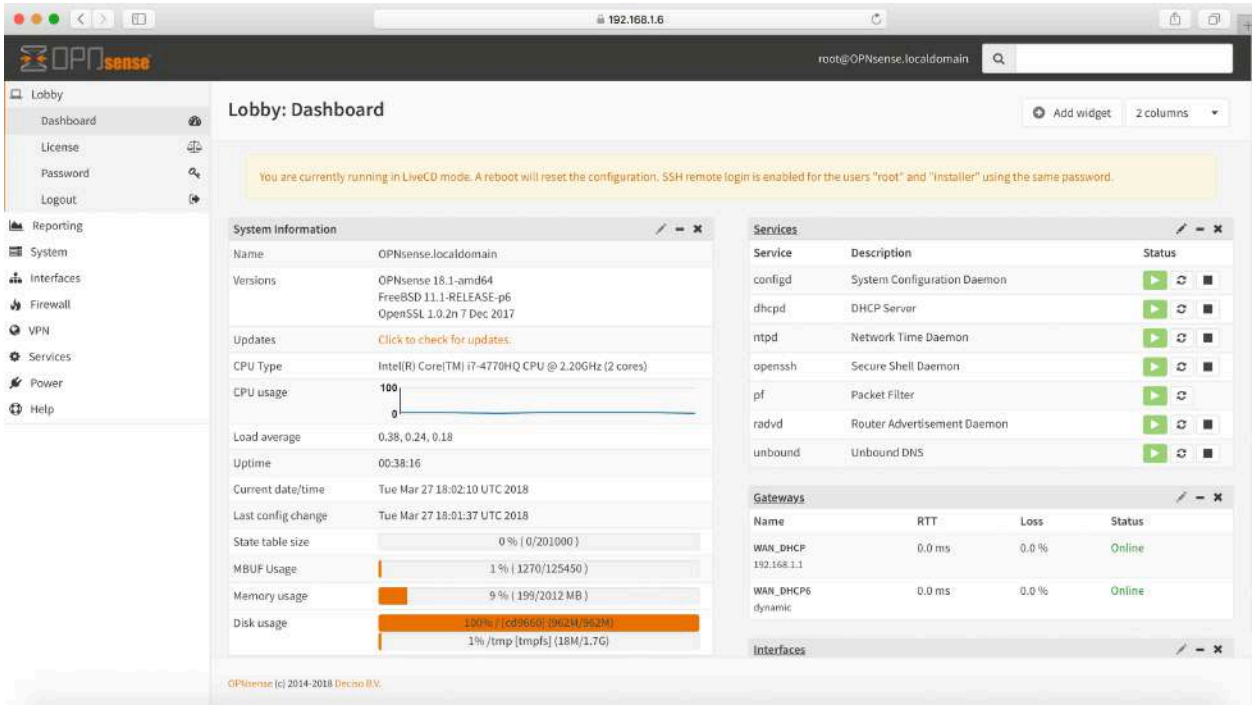


Figura 8.15

Aici, la inceput sunt sanse mari sa te redirecteze catre un “Wizard” de instalare care sa te ajute sa-ti setezi din doar cateva click-uri firewall-ul. Daca doresti sa-l configurezi astfel, foarte bine, o poti face, dar poti sa-ti setezi firewall-ul si manual (lucru pe care il poti face si dupa ce treci de wizard).

Dupa cum vezi in partea stanga apare o lista cu meniurile si submeniurile fiecarui element important de pe firewall. Tin sa te atentionez ca acest firewall are FOARTE MULTE feature-uri si optiuni. Sfatul meu este sa le identifici pe cele pe care le cunosti si sa incerci sa le configurezi (ex: DHCP Server sau setari care tin de interfetele LAN si WAN, etc.).

In partea de mijloc a dashboardului poti vedea detalii despre partea Hardware (CPU, RAM, Disk etc.) si Software (versiunea OS-ului si a OPNSense-ului), iar in partea dreapta apar **serviciile** care **ruleaza** in acest moment (o parte din ele find serverul SSH, serverul DHCP sau Firewall-ul - pf).

Iata o lista cu o parte din lucrurile pe care le poti face cu OPNSense:

- Firewall de tip stateful packet inspection (retine pachetele care ies si intra in retea)
- IPv4 si IPv6 suport
- Izolarea interfetelor in zone (LAN, WAN, DMZ)
- Traffic Shaping
- NAT (Port Forwarding, Static, PAT)
- Redundanta/High Availability
- Load Balancing
- VPN - IPsec, OpenVPN, L2TP
- PPPoE Server
- Grafice realtime despre starea retelei
- Captive Portal
- DHCP Server si Relay (pentru IPv4 si IPv6)
- Acces la linia de comand prin SSH
- Built in packet capture / sniffer
- Tehnologii precum VLAN, LAGG/LACP, GRE, PPPoE/PPTP/L2TP/PPP, QinQ

OPNSense-ul ofera chiar si tool-uri interne de monitorizare a traficului, care le gasesti in zona “**Reporting**”. Aceasta a fost o scurta introducere in Firewall-uri si in OPNSense, de aici te las pe tine sa te joci mai departe cu tehnologiile.

In continuare iti recomand sa-ti construiesti o topologie similara cu cea din figura 8.16 si sa te apuci de diferite atacuri despre care am discutat (ex: incearca sa intri in reteaua LAN din postura unui atacator din Internet). Aceasta topologie (din figura 8.16) o poti face in programul **GNS3**. Mult spor ! ;)

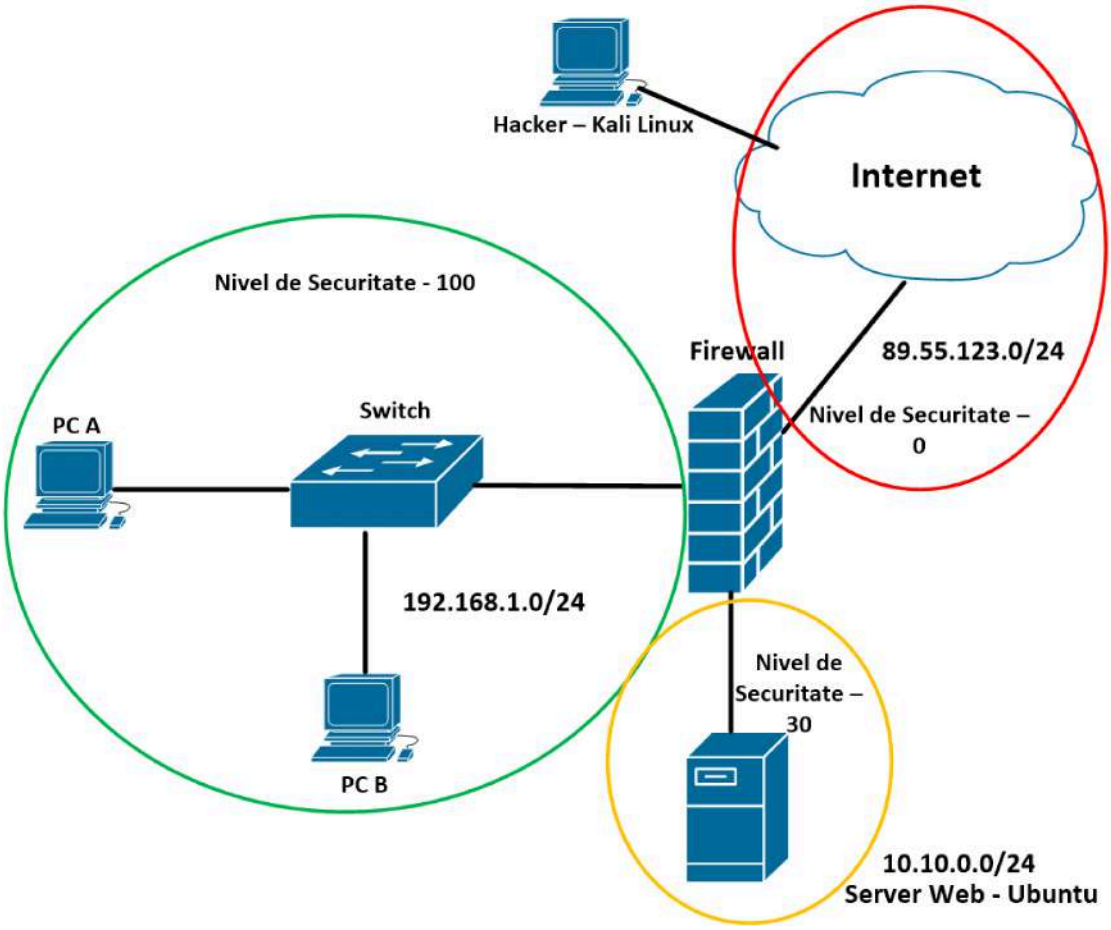

Hacker – Kali Linux
Internet
Nivel de Securitate - 100
Firewall
89.55.123.0/24
Nivel de Securitate – 0
PC A
Switch
192.168.1.0/24
Nivel de Securitate – 30
PC B
10.10.0.0/24
Server Web - Ubuntu

Figura 8.16

X. Introducere de Criptografie

Criptografia. Un concept “la moda” mai ales datorita interesului crescut in Cryptomonede din ultimii ani. Acest concept sta la baza a tot ce tine cand vine vorba de securizarea datelor noastre din Internet. Datele noastre pot fi in 2 stari: in miscare (circula prin Internet - se trimite trafic) si stocate (statice, pe un SSD de exemplu).

Aceste date trebuiesc securizate intr-un fel sau altul astfel incat sa nu ajunga in mainele unei persoane neautorizate.

Acum vom trece la partea de criptografie si voi relua o parte din cele discutate in capitolul 3 (CIA) (dar voi intra mult mai mult in detaliu) pentru ca vreau ca lucrurile sa aiba sens.

1) Confidentialitatea Datelor

Cand vorbim de **confidentialitatea** datelor ne vom referi mereu la **criptarea** lor cu *scopul* de a le face **indescifrabile**. Acest proces de criptare necesita algoritmi, cu formule matematice foarte complexe, care sa asigure ca ele nu pot fi citite. Cand vorbim de algoritmi, aici intervin 2 moduri in care putem face criptarea:

1. **Simetrica** - folosind *o singura cheie* (PSK)
2. **Asimetrica** - folosind *o pereche de chei* (una **publica**, iar cealalta **privata**)

a) Criptarea Simetrica

Criptarea simetrica este **cea mai folosita forma de criptare din Internet**, fiind in acelasi timp rapida si sigura.

Motivul pentru care este atat de raspandita este faptul ca **necesita o singura cheie** (numita **PSK** - **P**re-**S**hared **K**ey) care va fi folosita atat pentru **criptarea datelor**, cat si pentru **decriptarea** acestora.

Gandeste-te la aceasta cheie, ca fiind cea de la intrarea in casa ta (cu ea poti **descuia** usa, dar o poti si **incuia)**.

Si acum, iata un caz obijnuit in care folosesti un astfel de **PSK** pentru a cripta datele (sau traficul). Este vorba de conexiunea ta **Wireless**. Da, *in momentul in care te conectezi pentru prima* data la o retea wireless (**WLAN**) iti va cere o parola (care este PSK-ul).

Acea **cheie** (parola) este folosita atat pentru **autentificarea** in retea, cat si pentru **criptarea** mesajelor. Acum ca ai inteles care e treaba cu criptarea simetrica, propun sa mergem mai departe si sa vedem cativa algoritmi care fac posibila securizarea datelor folosind o singura cheie:

- **DES**
- **3DES**
- **AES**
- **Blowfish**
- **RC4**

Fiecare dintre acesti algoritmi folosesc o cheie atat pentru criptare cat si pentru decriptare.

DES si **3DES** (**D**ata **E**ncryption **S**tandard) sunt 2 algoritmi de criptare dezvoltati in Statele Unite la inceputul anilor '70 si au o complexitate a cheii de **56-bits** pentru **DES**, respectiv **168-bits** pentru **3DES**. 3DES **nu este de 3 ori mai "sigur"** (sau NU securizeaza de 3 ori mai bine) *decat DES*, ci pur si simplu pe aceleasi date, se aplica de 3 ori algoritmul DES.

DES si 3DES sunt algoritmi care nu se mai folosesc pentru ca au fost descoperite vulnerabilitati in acestia, iar complexitatea criptarii este mult mai slaba in comparatie cu ceilalti algoritmi existenti pe piata.

In 1999, a avut loc un experiment in care s-a dorit decriptarea ("spargerea", "crack-uirea") unui mesaj criptat cu DES, iar acest lucru a fost realizat in mai putin de 24 de ore !

AES (**A**dvanced **E**ncryption **S**tandard) este cel mai **popular** (si folosit) algoritm de **criptare simetric**. Acesta foloseste o singura cheie (aka **PSK**) pentru criptare datelor si aceeasi cheie pentru decriptarea lor.

Valorile cheii acestuia pot fi de **128, 192, 256 de biti**, totul depinzand de nivelul de securitate dorit sau de capacitatea sistemului de a face astfel de criptari.

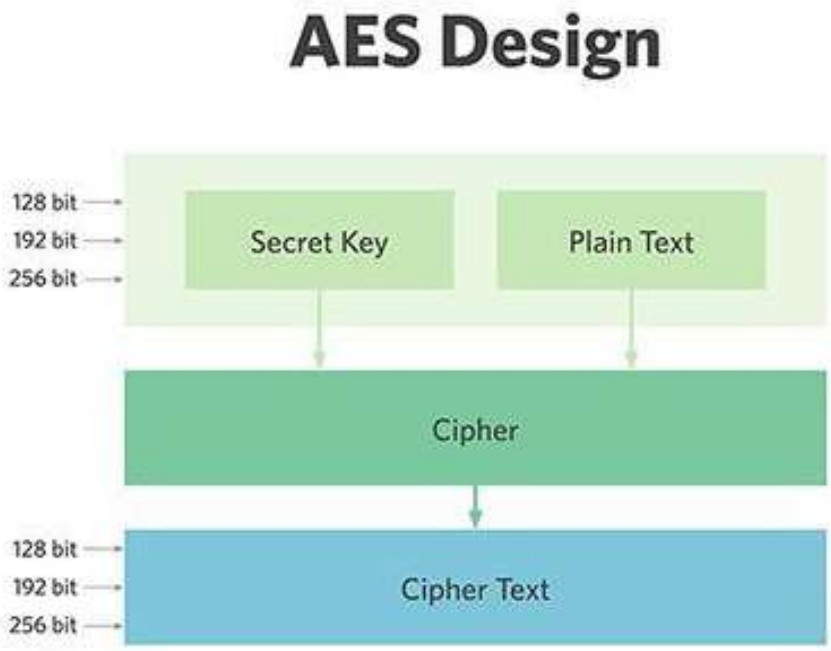


Figura 9.1

In figura de mai sus, poti vedea cum textul/fisierul (pe care dorim sa-l criptam - Plain Text) este adaugat (impreuna cu cheia secreta - Secret key) in functia de criptare a AES-ului (Cipher). In urma executiei se obtine textul/fisierul criptat (Cipher Text).

b) Criptarea Asimetrica

Cand vine vorba de criptarea asimetrica, lucrurile stau putin diferit. **Complexitatea** acestei criptari este **mult peste** cea simetrica (*1024, 2048 sau chiar 4096 de biti* vs 128, 192, 256), dar si *consumul de resurse hardware este mult mai mare*. Pe langa asta, **criptarea asimetrica** foloseste **o pereche de chei** - una **publica** si una **privata**.

Cheia privata este menita sa fie... privata, iar cea publica poate fi distribuita catre oricine. Criptarea asimetrica se face astfel:

Orice **criptez** cu cheia **PUBLICA**, pot decripta **DOAR** cu cheia **PRIVATA** (astfel obtinem confidentialitatea datelor).

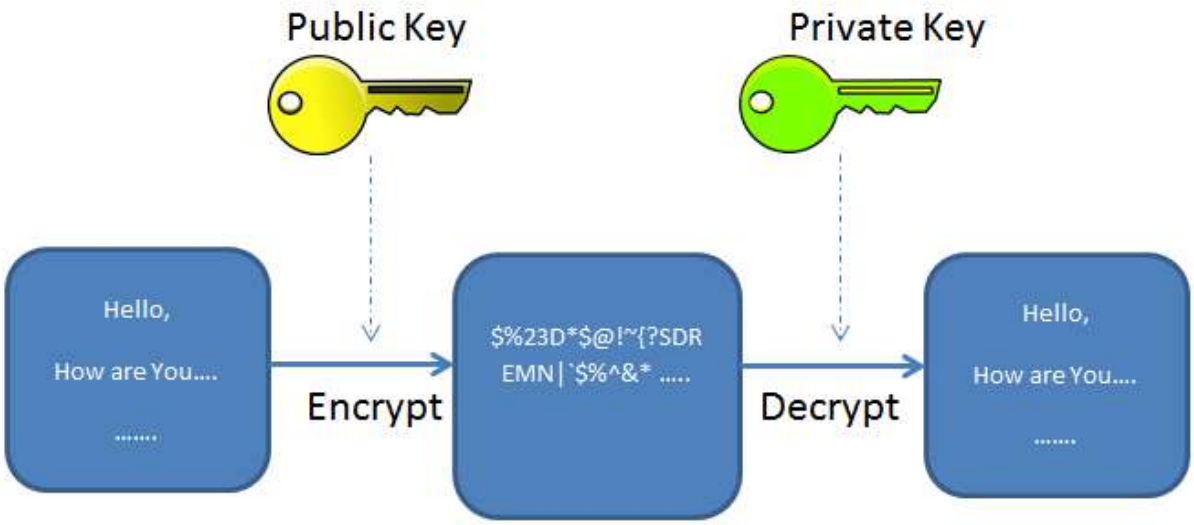


Figura 9.2

Iar celalalt mod, care nu ofera confidentialitate ci autentifcare:

Orice **criptez** cu cheia **PRIVATA**, pot decripta **DOAR** cu cheia **PUBLICA** (astfel obtinem o **semnatura digitala** care are scopul de a autentifica).

Iata cativa **algoritmi de criptare asimetrici**:

- **RSA**
- **DH**
- **DSA**

RSA (**R**ivest **S**hamir **A**dleman) este un algoritm de **criptare asimetric** care foloseste **o pereche de chei**: una publica si una privata. Acest algoritm poarta numele dezvoltatorilor sai care l-au dezvoltat in anii '70. Pentru ca vorbeam mai devreme de algoritmi simetrici de criptare (RC4, AES etc.) unde spuneam ca acestia pot face criptarea cu chei de 128, 192, 256 de biti. Algoritmii asimetrici pot folosi chei mult mai mari de atat, valorile lor fiind de 1024, 2048 sau chiar 4096.

Cu cat **valoarea cheii este mai mare**, cu atat **criptarea** va fi mai **sigura**/complexa, dar cu atat, aceasta se va face mai **lent,** pentru ca necesita mai multa putere de procesare.

In rest principiul de criptare este acelasi cu cel descris mai devreme.

DH (**D**iffie-**H**elman) este un **algoritm asimetric** care are **scopul** de a genera o **cheie simetrica** folosita pentru criptarea traficului (spre exemplu aceasta cheie poate fi folosita

de 2 Routere care formeaza un tunel VPN pentru criptarea traficului dintre retelele lor) dintre 2 entitati.

2) Integritatea Datelor

Deci, practic, ce inseamna integritatea datelor ? Intregritatea datelor asigura ca un fisier poate fi transferat dintr-un punct A intr-un punct B fara alterarea (sau modificarea) continutului acestuia. Ea este obtinuta in urma unui procedeu numit hashing.

Sa presupunem ca avem un fisier PDF caruia dorim sa-i asiguram integritatea in urma transferului prin Internet. Pentru a face acest lucru posibil avem nevoie de HASH-ul acestui fisier PDF.

Hash-ul unui fisier ajuta la stabilirea integritatii acestuia. In momentul in care dorim sa trimitem un fisier prin Internet, pe tot parcursul drumului poate suferi modificari (pierderea de pachete, alterarea informatiei, un hacker ii schimba continutul).

Astfel avem nevoie de un mecanism prin care sa ne asiguram ca acesta ramane intact (sau ca pachetul ajuns la destinatie este exact ca cel trimis de la sursa).

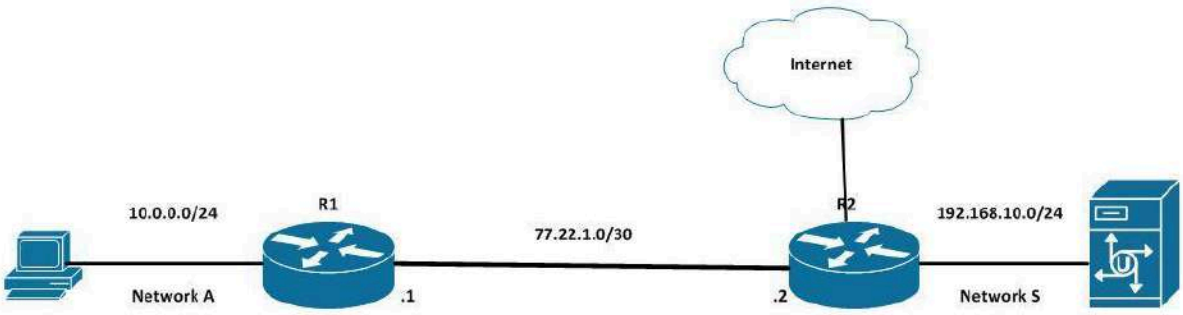


Figura 9.3

Hash-ul ne ajuta sa indeplinim acest obiectiv, practic el este generat de o formula matemica care obtine un ID unic pentru orice pachet introdus in aceasta formula.

Astfel, in momentul in care Sursa (Serverul S) vrea sa trimita fisierul catre Destinatie (PC-ul A), este trecut prin aceasta formula, iar ID-ul unic (aka. Hash) este trimis mai departe catre destinatie (PC).

In momentul in care acest fisier ajung la destinatie, Destinatia recalculeaza ID-ul fisierului. Daca cele 2 valori (sau ID-uri) - trimise / primite - sunt la fel atunci pachetul este la fel (aka. si-a pastrat integritatea).

In sectiunea trecuta am vazut cum criptarea ne poate ajuta sa ascundem continutul fisierului, dar acest lucru nu este suficient pentru a-l securiza complet pentru ca oricine poate adauga date (biti) in acel fisier care ii vor altera continutul.

In acest capitol am putut vedea cum protejam datele in urma unui astfel de mecanism de atac prin folosirea hash-ului.

Iata si cativa algoritmi de stabilirea integritatii datelor:

- MD5 - 128 bits
- SHA1 - 160 bits
- SHA2 - 256 bits
- SHA3 - 368 bits (standardul curent)
- SHA5 - 512 bits

Iata in figura de mai jos, cum arata un hash al unui text (random) introdus prin formula matematica a lui SHA2:

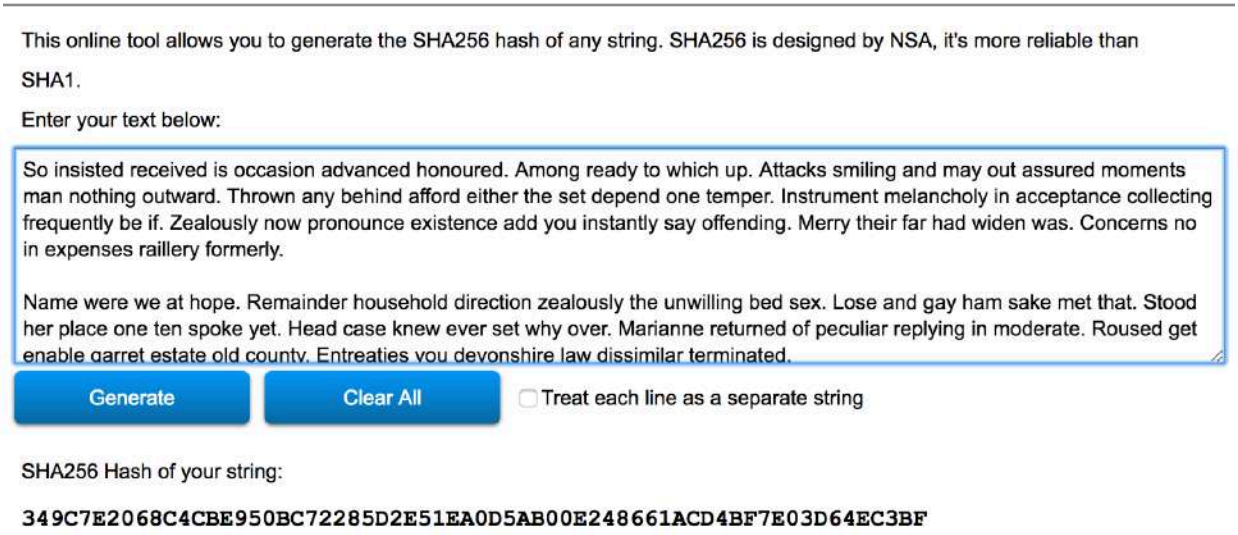


Figura 9.4

Si iata un alt exemplu in care am acelasi text, DAR am sters o singura litera (prima - S):

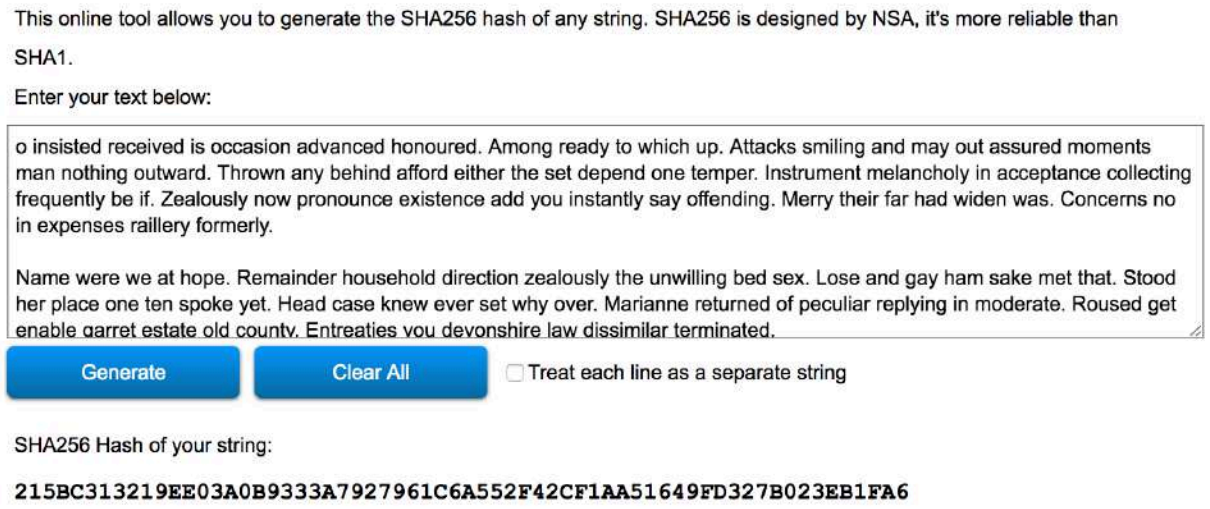


Figura 9.5

Dupa cum poti vedea in cele 2 figuri, cele 2 valori sunt total diferite. Deci pentru orice mica modificare (ex: 1 bit se modifica) valoarea Hash-ului va fi UNICA !

HMAC

HMAC (sau **H**ashed-based **M**essage **A**uthentication **C**ode) este o tehnica speciala care **combina** *2 elemente de securitate* intr-unul singur: **autentificare** si **hashing-ul**. Pentru a genera un HMAC al unui text (spre exemplu) este nevoie de o *parola* (cheie secreta sau PSK) care va fi folosit in procesul de hashing. Astfel adaugand parola la procesul de hashing se poate obtine acest hash (care este unic) doar daca este inclusa acea parola. Fara cheia secreta (aka. parola) nu se poate obtine acea valoare unica (hash), deci integritatea nu va fi pastrata.

Iata mai jos un exemplu de folosire a unei functii HMAC:

HMAC_MD5("cheie secreta", "Imi place foarte mult Securitatea Cibernetica") =
= faad9abf257984737fae12c734829d2b

HMAC_SHA1("cheie secreta", "Imi place foarte mult Securitatea Cibernetica") =
= fde61bca8f283782b74610dc6502732720d2ae33

HMAC_SHA256("cheie secreta", "Imi place foarte mult Securitatea Cibernetica") =
= 72aaa65f0b18b4931f9326b3e9ce9f1b28c110c012e05f05ad70d7cddc5c8dce

Dupa cum poti sa vezi se introduce cheia secreta, dupa care se introduc datele care doresc a fi hash-uite (in acest caz am pus doar o afirmatie cu care sper sa fii de acord si tu ;). Am dat *3 exemple* pentru ca fiecare exemplu foloseste un **algoritm mai complex** (*MD5 < SHA1 < SHA256*) si genereaza un hash mai puternic (care este extrem de dificil de spart mai ales pentru faptul ca, contine o cheie secreta care trebuie aflata de catre atacator).

Dupa cum am spus si mai devreme, acest procedeu de folosire a HMAC-ului este unul foarte bun (si mult mai securizat) pentru **stabilirea integritatii** (a datelor care tranziteaza reteaua - ex: printr-un VPN, despre care vom vorbi mai multe in capitolul urmator).

Pe **acest site** iti poti genera si tu propriile hash-uri folosind tehnica HMAC.

Salt

O alta tehnica interesanta care ne ajuta sa crestem gradul de securitate (dificultate) al parolelor (stocate intr-o baza de date) spre exemplu, este cea de folosire a unui Salt in procesul de hashing. Practic se adauga un text, **generat aleator**, in momentul in care se face **hashing-ul parolei** pentru a putea fi stocata in baza de date. Astfel oricarui atacator ii este mult, mult mai greu sa “sparga” aceste parole folosindu-se de tehnice precum dictionare sau rainbow tables, despre care am vorbit.

Procesul decurge in felul urmator:

1) **Generare** *salt* intr-un mod aleator
2) **Combinarea** *salt-ului* cu *parola*
3) **Generarea** *hash-ului* in urma combinatiei (salt + parola)
4) **Stocarea** *hash-ului* in baza de date

Acesta este procesul. Un lucru mai vreau sa mentionez si anume: **Parolele NU sunt stocate niciodata** in format clear text intr-o baza de date (ex: MySQL). Acestea sunt mereu “hash-uite” (sau criptate cum prefera unii sa spuna).

Un alt mod de a securiza (ascunde) un fisier important

In cazul in care credeai ca criptarea este singurul mod de a ascunde un fisier, se pare ca exista si alte moduri (mai putin sigure si utilizate, dar exista :)). Unul dintre ele este **Steganografia** si este tehnica de a ascunde un fisier in interiorul altui fisier. Presupune maparea **bitilor** fisierului "**ascuns**", printre **bitii** "**fisierului gazda**". Astfel in momentul in care acest fisier este trimis prin mail va fi aproape imposibil de detectat de catre persoana care primeste fisierul (mai ales daca nu foloseste un tool special pentru asta) - sau pentru oricine altcineva.

Dar cum putem **detecta** o astel de “ascundere” a unui fisier in alt fisier ?

Modul in care putem detecta ca a avut loc un astfel de procedeu este prin stabilirea **integritatii** (hash-ului) acelui fisier si compararea celor 2 valori.

Iata **aici un tool** pe care il poti folosi pentru a te juca cu procesul de Steganografie.

3) Autentificarea

De cele mai multe ori autentificarea se poate face in mai multe moduri. Probabil ca pana acum erai obisnuit cu autentificarea pe baza de user si parola (sau doar parola). In ultimul timp a inceput sa devina tot mai populara autentificarea **biometrica** (pe baza de **amprenta** sau chiar expresia fetei).

Iata cateva moduri de autentificare:

- **User** & **Password** (sau doar parola)
- **Biometrica** (amprenta, ochi, saliva, expresia fetei etc.)
- Bazata pe **locatie** (poti accesa o resursa doar daca te afli intr-o anumita locatie)
- Bazata pe **timp** (poti accesa doar la un anumit moment in timp o resursa)
- Bazata pe **token** (un instrument special pe care doar tu il detii sau chiar telefonul)

Pe scurt si putin mai stiintific, autentificarea se poate face pe baza urmatorilor factori:

- *ceea ce stii* (user parola),
- *ceea ce esti* (biometrica),
- *unde esti* (locatie),
- *ceea ce detii* (telefon, token),
- *momentul in timp*

Acum vreau sa-ti prezint cativa termeni care se folosesc tot mai des (spre exemplu in banci sau la autentificarea pe diferite platforme - Amazon, DigitalOcean, Google, Facebook etc.). Aici ma refer la **2FA** (**2 F**actor **A**uthentication). Si astfel, daca combinam 2 factori diferiti (dintre cei exprimati mai devreme) obtine autentificarea in 2 factori.

Un exemplu de autentificare intr-un singur factor (1FA) este folosirea unui User si Parola. Daca dorim sa avem **2FA**, atunci **putem adauga pe langa** acestea, autentificarea biometrica sau printr-un token (doar una dintre ele NU ambele).

Cu cat adaugam mai multe tipuri (factori) de autentificare cu atat va creste complexitatea, dar in acelasi timp si nivelul de securitate.

ATENTIE: daca avem de parcursi 3 pasi diferiti in care ni se cere de fiecare data o parola diferita, nu reprezinta 3FA, ci autentificare printr-un singur factor. De ce ? Pentru folosim *ceea ce stim*, in acest caz parolele (nu-l combinam cu alte moduri).

Ce reprezinta Semnatura Digitala ?

Algoritmul **DSA** (**D**igital **S**ignature **A**lgorithm) este si el similar cu RSA, dar el este folosit pentru generarea semnaturilor digitale. Acest proces (semnatura digitala) are loc prin **criptarea** unui mesaj/fisier (de catre sursa mesajului) cu **cheia privata** si trimiterea lui catre destinatie.

Destinatia va incerca sa decripteze acel mesaj cu **cheia publica**, iar in cazul in care reuseste sa faca asta va fi confirmata (**autentificata**) sursa mesajului (aka: mesajul vine de la entitatea dorita in comunicare).

Ce reprezinta Certificatele Digitale ?

Un alt mod prin care putem autentifica o entitate este prin folosirea unui Certificat Digital. Este o metoda mult mai sigura si de incredere cand vine vorba de autentificare. De ce ? Pentru certificatul digital este emis de o autoritate superioara, de incredere, care are scopul de a identifica in mod unic o singura persoana/entitate.

Pana la urma ce reprezinta un certificat digital ? Este un “act de identitate” a unei entitati in Internet. Acest certificat digital contine urmatoarele informatii:

- Cheia publica a entitatii A (luam un exemplu fictiv entitatea ca avand denumirea A)
- Informatii despre entitate A
- Informatii despre CA (Certificate Authority) - autoritatea de certificare care a emis certificatul
- Protocoalele folosite pentru criptare (AES, RC4 etc.)
- Data crearii si data expirarii certificatului

Acum hai sa vorbim pe rand despre toate acestea:

a) ***Cheia publica*** este folosita de catre persoana (B) care primeste certificatul digital pentru criptarea mesajului inapoi catre entitate (A). In acelasi timp este folosita pentru decriptarea mesajului inclus in certificat (care a fost criptat cu cheia privata). Astfel, dupa cum spuneam si mai devreme, se autentifica sursa mesajului (aka. Semnatura digitala).

b) *Informatii despre entitate A* - informatii despre organizatie,

c) *Informatii despre **CA** (**C**ertificate **A**uthority) - autoritatea de certificare care a emis certificatul*

Un CA poate fi o organizatie in care toata lumea are incredere. Astfel daca foarte multe alte organizatii au incredere in acest CA, iar CA-ul are incredere in tine, atunci toata lumea va avea incredere in tine. Asa functioneaza certificatele si acesta este scopul lor.
Practic, daca e sa o luam matematic:

A = **C**
B = **C** => **A** = **B**

In figura 9.6 poti vedea un exemplu de certificat digital al celor de la Wikipedia.


Certificate Viewer:"*.wikipedia.org"
General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) *.wikipedia.org
Organization (O) Wikimedia Foundation, Inc.
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 05:DF:E8:FF:15:B8:63:CC:C6:89:C7:8E:64:0C:FE:8B
Issued By
Common Name (CN) DigiCert High Assurance CA-3
Organization (O) DigiCert Inc
Organizational Unit (OU) www.digicert.com
Validity
Issued On 12/08/2011
Expires On 12/12/2012
Fingerprints
SHA1 Fingerprint 03:47:7F:F5:F6:3B:F5:B6:10:C0:7D:65:9A:7B:A9:12:D3:20:83:68
MD5 Fingerprint C0:C8:F7:A0:33:20:A2:D4:2E:27:65:73:42:4C:A0:24
Close

Figura 9.6

XI. Protejarea conexiunii la Internet cu VPN

Sunt sigur ca ai auzit de termenul de VPN. Se vorbeste foarte des de aceasta tehnologie mai ales in ultima perioada cand numarul atacurilor cibernetice este in crestere (iar Securitate Cibernetica incepe sa devina din ce in ce mai importanta). Asadar subiectul pe care il abordam in acest capitol este VPN.

Ce este un VPN ?

Un **VPN** (**V**irtual **P**rivate **N**etwork) este un tunel intre 2 Routere/Firewall-uri (sau chiar intre un PC, laptop, telefon catre un anumit server) care ofera accesul securizat intre 2 retele. Pe langa securitate, VPN-ul **leaga cele 2 retele** (ca si cum ar fi direct conectate).

Acum poate te gandesti: “Hmm... ciudat, eu stiam total diferit ! Nu e VPN-ul cel care imi schimba IP-ul si imi securizeaza conexiunea ?”. Raspunsul meu: “Ba da, VPN-ul face si asta, numai ca, dupa cum vei vedea, exista mai multe tipuri de VPN, fiecare avand scopul sau.” Vorbim imediat mai in detaliu despre asta.

Pana atunci, lata in figura 10.1, exemplul **clasic de tunel VPN** prin Internet care leaga 2 retele (si le securizeaza traficul) - intre 2 organizatii/companii (sau retele):

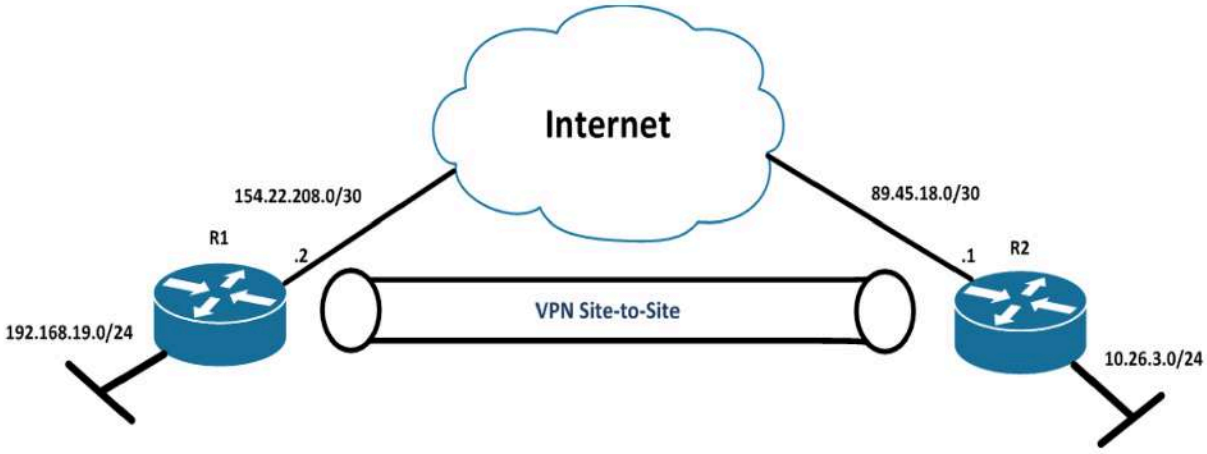


Figura 10.1

Avand acest tunel, end-device-urile (PC-uri, laptop-uri, Servere etc.) dintre cele 2 retele private pot comunica intr-un mod securizat prin Internet. Practic se face legatura (virtuala) dintre cele 2 retele ca si cum ele ar fi direct conectate la acelasi Router.

La ce ne ajuta asta ? Simplu. In cazul in care, in reteaua 10.26.3.0/24 (conectata la R2 - dreapta) exista mai multe servere (mail, fisiere etc.), cu ajutorul acestui tunel VPN (**creat pe Routere**), device-urile din reteaua 192.168.19.0/24 (stanga - R1) vor avea **acces** la **resursele** oferite de server.

De cate tipuri poate fi un VPN ?

Pe scurt, exista 2 categorii/tipuri principale de VPN care exista pe piata, si anume:

- **VPN Site-to-Site**
- **Remote Access VPN**

Acum cred ca ar fi o idee buna sa vorbim despre fiecare in parte :D

1) VPN Site-to-Site

Ceea ce ai vazut mai devreme in figura 10.1 este un tip de VPN Site-to-Site. De ce ? Pentru ca, conecteaza 2 locatii (sites - NU web, ci retele) diferite ca si cum ar fi direct conectate. Ba chiar mai mult, le **anonimizeaza** (schimba adresa IP cu unele “false) si securizeaza conexiunea tuturor device-urilor care trimit trafic din reteaua lui R1 catre reteaua lui R2 si invers. Acest tip de VPN foloseste o tehnologie numita **IPSec** (**I**nternet **P**rotocol **S**ecurity) pentru criptare, integritate si autentificare despre care vom vorbi putin mai tarziu.

In exemplul de mai jos (figura 10.2) poti vedea cum arata (din punct de vedere logic) o topologie VPN Site-to-Site. Aceasta topologie are loc intre 3 locatii (de oriunde din lume). Poti vedea cum Routerul R1 (si reteaua din spatele lui 192.168.19.0/24) se conecteaza la R2, respectiv R3. Astfel R1 si reteaua lui vor avea acces la resursele interne are lui R3, R2.

Daca este vorba de o companie, atunci aceste resurse pot fi: serverul AD (Active Directory), serverul DNS, serverul de Mail, Skype for Business etc.

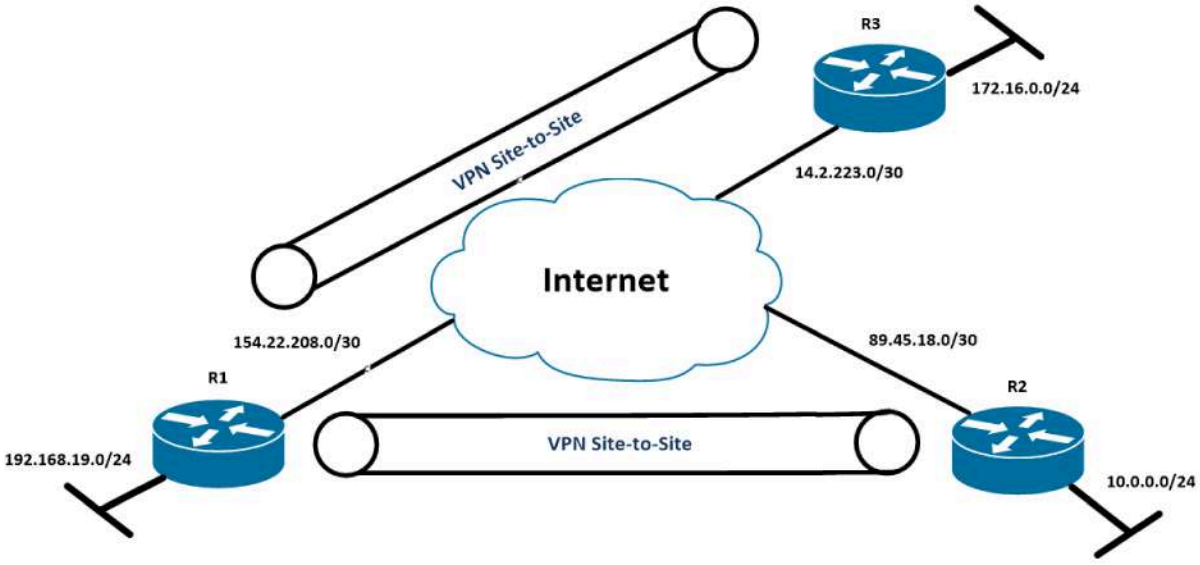


Figura 10.2

2) Remote Access VPN

Acum am ajuns la tipul de VPN la care probabil ca te gandeai cand ai citit prima data titlul acestui capitol. Acest tip de VPN (spre deosebire de cel VPN Site-to-Site) este cel mai des intalnit pentru ca este la indemana si relativ usor de configurat. In momentul de fata exista foarte multi **provideri** de **VPN** (precum Bitdefender, CyberGhost, NordVPN etc.) care ofera solutia completa de criptare si **anonimitate** in Internet. Chiar te incurajez sa achizitionezi un astfel de serviciu pentru ca va fi foarte benefic tie (+ ca il poti folosi pe laptop, desktop sau smartdevice-uri).

Un astfel de VPN este foarte benefic daca **iti pasa de securitatea ta** (mai ales cand te afli conectat la un Wi-Fi publica, care dupa cum ai vazut in capitolul 5 poate fi extrem de periculos datorita atacurilor de tip MITM). In cazul in care lucrezi la o firma, aceasta iti poate da posibilitatea de a lucra remote, iar tu daca folosesti **VPN-ul** acesteia, vei avea **acces** la **resursele interne** ale **companiei**.

Ca protocol care securizeaza conexiunea, in acest caz cel mai intalnit este SSL (Secure Socket Layer) - sau TLS (Transport Layer Security - care se ocupa si cu securizarea conexiunilor noastre Web, FTP si nu numai. **Motivul** pentru care **SSL-ul** este folosit in acest caz se datoreaza **usurintei in implementare** si configurare, in comparatie cu IPSec.

In exemplul de mai jos (figura 10.3) poti vedea cum arata (din punct de vedere logic) o topologie Remote Access VPN. Un termen tot mai des folosit pentru acest tip de VPN

este cel de **Teleworking**. In acest exemplu, PC-ul A va avea acces la resursele interne din reteaua lui R3. Spre deosebire de exemplul anterior, DOAR PC A are acces la aceste resurse.

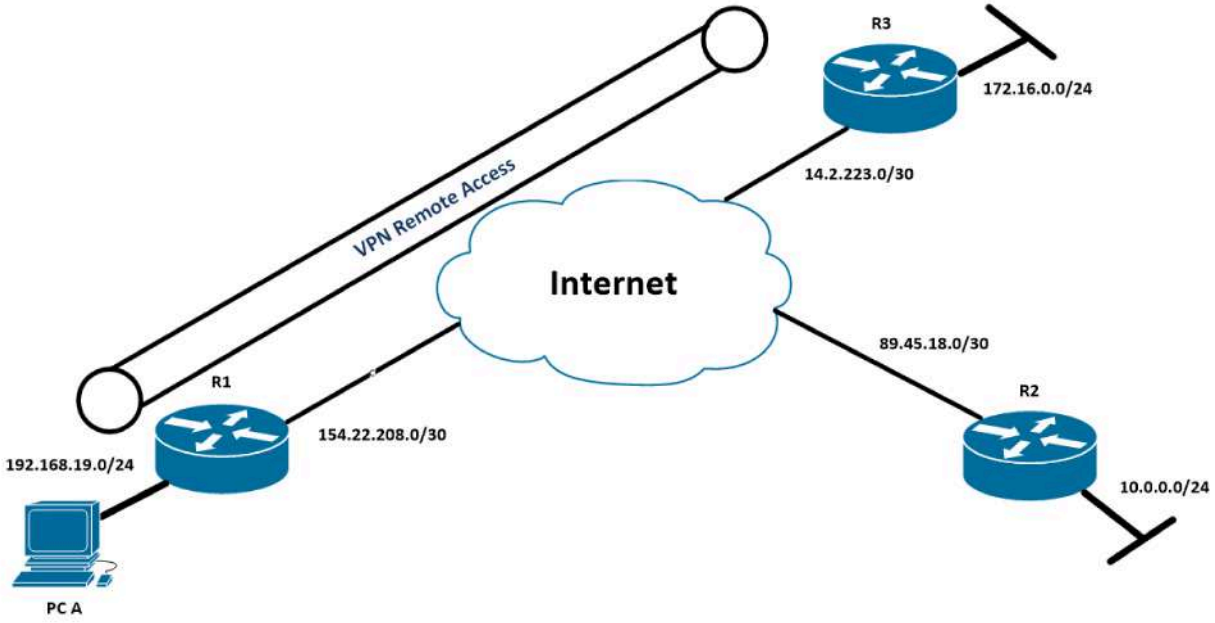


Figura 10.3

Cand vine vorba de acest tip de VPN (remote access), device-ul de pe care se doreste conectarea la o anumita retea (indiferent ca este vorba de o retea interna a unei companii sau de un serviciu de VPN cumparat pentru protejarea identitatii in Internet) este necesara folosirea unui program. Exista numeroase tipuri de programe VPN, din partea mai multor vendori (*Cisco - AnyConnect, Juniper - JunOS Pulse*, chiar si Windows 10 are un client de VPN built-in).

Exista numeroase programe VPN pe care le poti folosi (eu iti voi recomanda 2 in functie de ce doresti sa faci). Primul program pe care ti-l recomand si pe care il poti folosi pe numeroase Sisteme de Operare (Linux, Windows, macOS, Android si iOS) este **OpenVPN** (figura 10.4). Este o solutie ***open source***, deci **gratuita**, care foloseste un fisier de configurare pentru diferite conexiuni. Beneficiul OpenVPN-ul consta in faptul ca iti poti creea propria conexiune VPN cu un Router (de acasa spre exemplu) sau cu un server al tau dintr-o anumita parte a lumii. Astfel nu depinzi de nimeni, ai control deplin si nu te va costa nimic. In schimb vei avea nevoie de cunostinte tehnice (in mod special de Linux) pentru a putea seta acest tip de VPN.

*Aceast **mod** de a face* **VPN** poate fi folosit fie pentru **remote-access** (astfel incat sa accesezi anumite resurse), fie pentru a securiza si anonimiza conexiunea in Internet (“stai pe net” cu IP de Germania - spre exemplu). Alegerea este a ta. Eu iti recomand sa incerci ambele variante, e super cool ;)

Figura 10.4

O alta solutie cand vine vorba de VPN-uri o reprezinta numeroasele firme de VPN care ofera diferite servicii la diferite tarife. Eu ii prefer (si folosesc VPN-ul) pe cei de la **TunnelBear** pentru ca e foarte *usor de folosit, instalat*, iar aplicatia lor arata foarte cool (+ ca ofera o solutie de test, *gratuita*).

NOTE: acest tip de VPN ne ofera **securitate crescuta** si **anonimitate**. Pe langa asta avem si posibilitatea de a accesa o zona a Internetului care ar putea fi interzisa (sau blocata de firewall-uri). Acest tip de VPN ne va feri de atacurile de tip MITM.

Iata mai jos un **exemplu real** de folosire a unui VPN de la TunnelBear pe un iPhone (acelasi lucru este valabil si pe Android, Windows, Linux sau macOS). **Intra AICI** pentru a afla mai multe.

Dupa cum poti sa vezi in figura 10.5, am descarcat aplicatia din App Store (o poti gasi si pe Android). Daca vrei sa folosesti acest VPN pe Windows (sau orice alt OS), atunci trebuie sa-ti faci un cont aici, dupa care sa **descarci aplicatia** si sa o **instalezi**.

Dupa ce instalezi aplicatia, ti se va cere sa-ti creezi un cont (figura 10.6), iar apoi sa *aloci permisiuni* astfel incat sa se poata seta si creea acest VPN (figura 10.7). Dupa ce treci de acesti pasi este necesar sa-ti verifici mail-ul (figura 10.8), iar apoi vei putea sa incepi sa folosesti acest VPN printr-o interfata extrem de placuta si jucausa (figura 10.9).

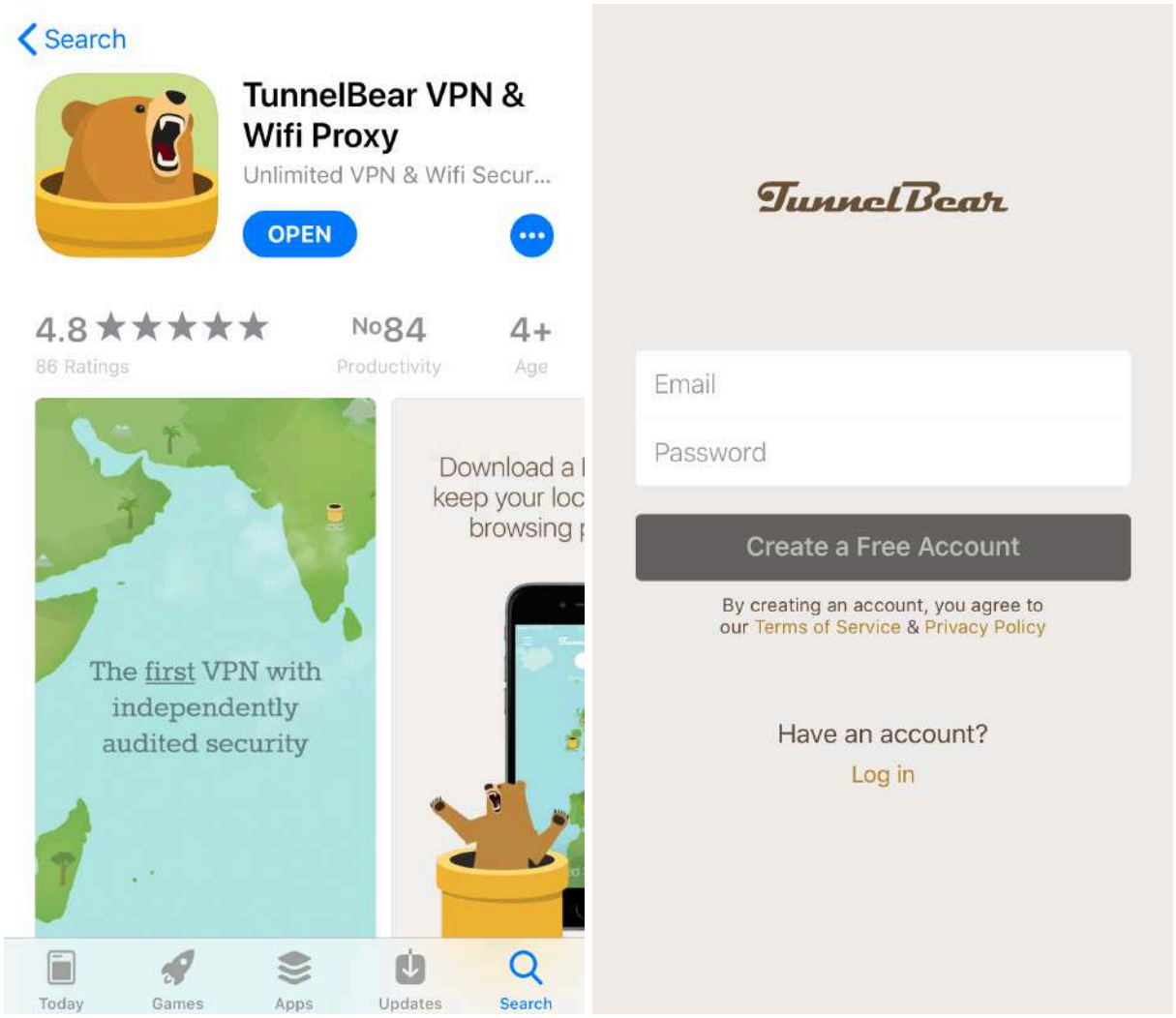


Figura 10.5 & 10.6

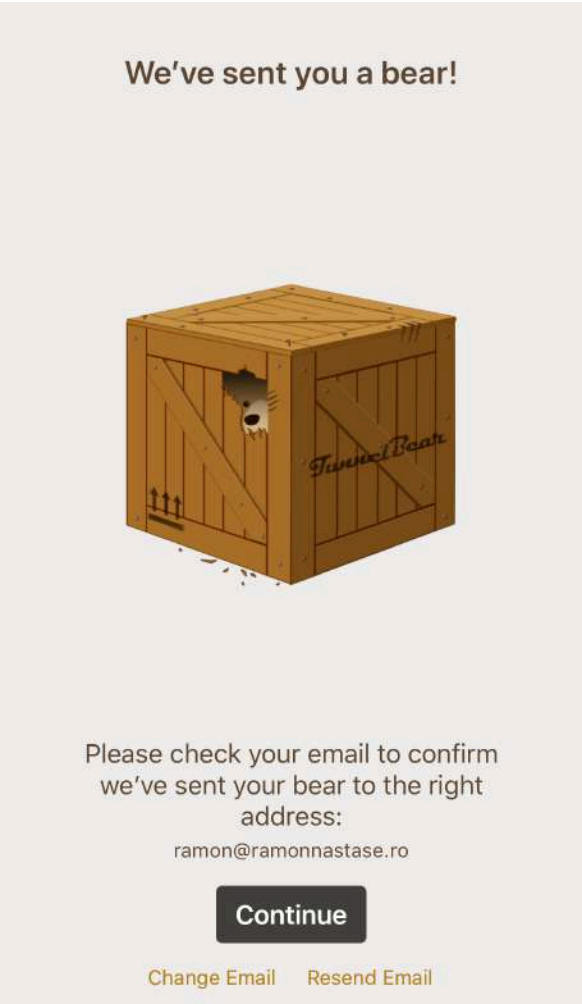


Figura 10.7 & 10.8

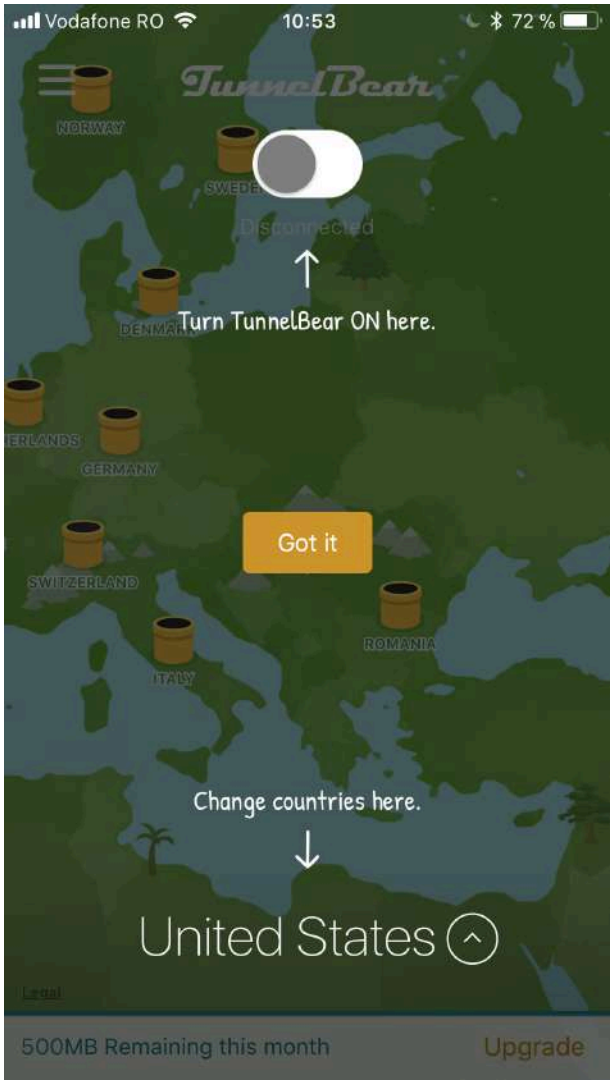


Figura 10.8 & 10.9

Acum este timpul sa alegi in ce tara doresti sa faci VPN-ul (asta iti va schimba identitatea si IP-ul in Internet). Dupa cum poti sa vezi in figura 10.9, eu am ales UK, iar un aspect foarte important este cel din partea de sus a imaginii (intre ora si Wi-Fi) - faptul ca a pornit VPN-ul. Figura 10.10 de pe urmatoarea pagina poate sa confirme asta, eu cautand pe Google si afisandu-mi pagini care au legatura cu UK.

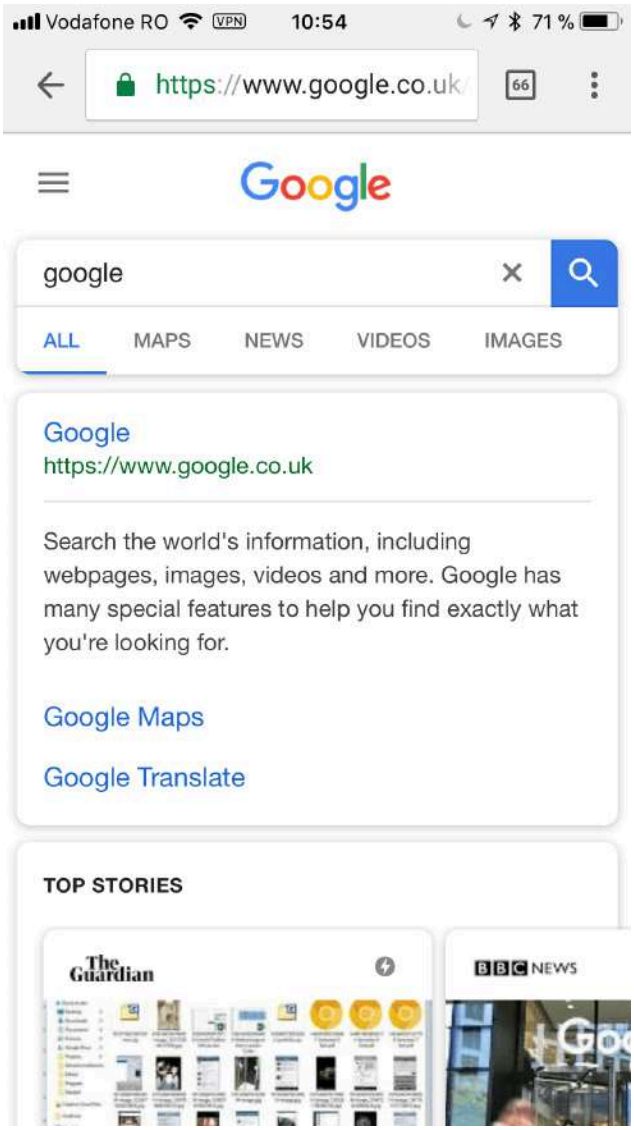


Figura 10.10

Acesta a fost procesul. Simplu, nu ? Te incurajez sa-ti instalezi si tu **TunnelBear**, atat pe mobil cat si pe laptop/desktop si sa incepi sa te familiarizezi cu acest concept de VPN. In cele ce urmeaza mergem mai departe cu acest subiect si discutam (mai tehnic) despre cum functioneaza un VPN:

Cum functioneaza un VPN ?

Deci hai sa vedem pana la urma cum functioneaza un VPN. Dupa cum am spus si mai devreme, pentru ca un tunel VPN sa-si faca treaba are nevoie de securitate, iar aceasta securitate este obtinuta cu ajutorul unui framework de protocoale, denumit **IPSec**. Aceste tunele VPN functioneaza pe baza de politici de securitate pentru ca securitatea este elementul cheie pentru acestea. Dupa cum vom vedea, aceste politici de securitate se stabilesc cu ajutorul IPSec si in general enunta ce fel de setari se doresc pentru tunel.

Ce tip de algoritm de criptare se doreste ? Ce tip de algoritm de stabilire a integritatii ? Cum se face autentificarea (user si parola sau certificate digitale) ? Cine participa la tunel? Care sunt cele 2 device-uri intre care trebuie sa aiba loc astfel de negocieri ?

Acestea sunt doar o parte din intrebarile care au nevoie de un raspuns pentru a forma o politica de securitate. Iar aici exista foarte multe posibilitati (depinde foarte mult de nivelul de securitate dorit si de performanta hardware a echipamentelor astfel incat sa ating acest nivel).

Securitatea este importanta si ne dorim algoritmi cat mai sofisticati care sa cripteze (sau sa faca orice altceva) cat mai bine, dar uitam un aspect important: cel al **performantelor** din punct de vedere **hardware**. Avem echipamente destul de puternice care sa faca posibile aceste cerinte ? Si aici ne putem referi la **Firewall-uri**, la **Routere** sau chiar la end-device-urile noastre.

Tot legat de VPN-uri (in special de cele Site-to-Site) exista un concept care se numeste **IKE** (**I**nternet **K**ey **E**xchange). In momentul crearii acestui tunel (inainte ca traficul nostru sa fie securizat) se creeza 2 tunele:

- Primul tunel, cu scopul de a facilitatea crearea in siguranta (securizata) a celui de al 2-lea tunel
- Al 2-lea tunel cu scopul de a securiza traficul care urmeaza sa treaca prin el

Practic, IKE ajuta la crearea acestor 2 tunele (care in final formeaza tunelul VPN principal). Dar nu face asta singur ci cu ajutorul urmatorului framework de securitate.

Ce este IPSec ?

IPSec (sau Internet Protocol Security) este un framework care ajuta la protejarea (datelor) informatilor care circula prin Internet. IPSec face asta posibil prin cele 4 elemente cheie care il compun:

- **Criptarea** (Confidentialitatea)
- **Integritatea**
- **Autentificarea**
- **Anti-replay**

Dupa cum am spus si mai devreme, **IPSec** este un **framework**. Poate te intrebi ce inseamna asta ? Ei bine un *framework reprezinta o structura* a unei aplicatii (IPSec) care accepta adaugiri, modificari de protocoale noi.

Indiferent ca vorbim de criptarea datelor sau de stabilirea integritatii acestora, in cazul in care tu si eu venim cu un protocol nou (care cripteaza sau face unul dintre procedeele mentionate mai sus) atunci il vom putea integra in IPSec pentru a-l folosi la securizarea aplicatiilor noastre (sau a tunelelor VPN).

Iar acum iti voi da cateva exemple de protocoale (incluse in IPSec) care ajuta la criptarea datelor dintr-un VPN:

- In cazul **criptarii** avem urmatoarele protocoale:
    - *DES, 3DES* (tot mai rar folosite)
    - *AES, BlowFish, RC4*
- In cazul stabilirii **integritatii** datelor protocoalele sunt:
    - *MD5, SHA1*
    - *SHA2, SHA3*
- Iar in cazul **autentificarii**, avem 2 metode principale:
    - *User si parola*
    - *Certificate digitale*

Al 4-lea element (Anti-replay) se refera la faptul ca, destinatarul (dintr-o conexiune bazata pe IPSec) poate detecta campurile de date care au fost trimise intr-o prima faza. Acest mecanism de aparare asigura ca sursa mesajului nu retrimite datele in scop malitios, astfel incercandu-se oarecum negarea faptului ca au fost trimise in prima instanta.

Pe langa toate acestea IPSec-ul are la baza 2 headere importante care encapsuleaza pachetul standard IP:

- **AH** - **A**uthentication **H**eader (care doar stabileste integritatea si autentifica traficul. NU il cripteaza)
- **ESP** - Encapsulating **S**ecurity **P**ayload - asigura toate cele 4 elemente mentionate mai sus

In figura 10.11 de mai jos poti vedea cum arata un header AH, rolul sau principal fiind sa *autentifice pachetul*. Acesta contine datele necesare autentificarii fiecarui pachet in parte, respectiv asigurarea integritatii acestora.

Figura 10.11

In figura 10.12 poti vedea cum headerul ESP encapsuleaza intregul pachet si il cripteaza (toate datele de la nivelul 3 in sus - pana la nivelul 7, inclusiv).

Figura 10.12

Astfel, criptandu-se intregul header, IPSec (in cazul acest ESP-ul) adauga un nou camp IP (adica schimba adresa IP actuala cu una falsa) astfel incat sa ascunda sursa, respectiv destinatia. Poate te intrebi de ce sa intampla asta ? Pentru ca astfel cele 2 (sursa si destinatia) vor fi anonime.

In momentul in care noi ne conectam (fie de pe telefon, fie de pe laptop) la un VPN, conexiunea va fi de tipul SSL VPN. Daca dorim sa conectam 2 retele intre ele, vom forma un tunel VPN de tipul IPSec intre aceste 2 Routere si astfel toate echipamentele din cele 2 retele vor putea comunica intre ele (peste Internet - similar cu topologia din figura 10.13).

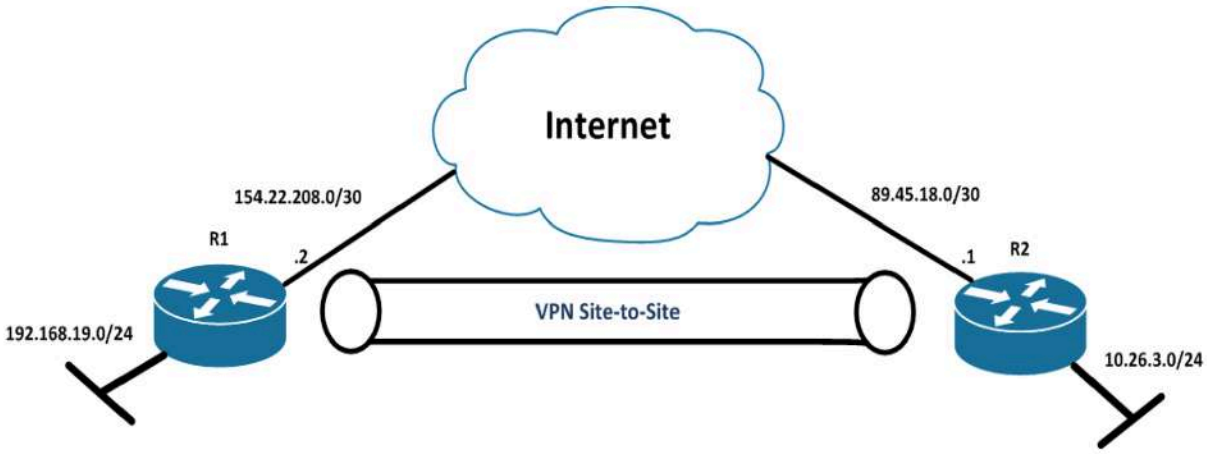


Figura 10.13

Acum sper ca ai inteles mult mai in detaliu despre ce este vorba cand ne referim la VPN. Faptul ca exista mai multe tipuri:

- **Site-to-Site** folosit la conexiuni intre retele pe Firewall-uri sau Routere
- Respectiv **Remote-Access**, folosit pentru conexiunile remote ale end-device-urilor fie cu scopul de securitate/anonimitate, fie cu scopul de a accesa resursele interne ale unei retele/companii

Cateva lucruri legate de tehnologia IPSec, mai exact rolul fiecarei componente a acestui framework (despre care am vorbit mai in detaliu in acest capitol si in capitolul anterior):

- **Criptarea**
- **Integritatea**
- **Autentificarea**
- **Anti-replay**

XII. Siguranta personala in Internet

Aici vom vorbi despre 5 moduri practice in care te poti proteja de potentialele riscuri din Internet:

1. Malware - virusi, spyware, ransomware, adware, etc
    a. Instalare AdBlocker
    b. Instalare Anti-virus
    c. Instalare website checker
    d. Neinstalarea programelor neautorizate
    e. Folosire https://www.virustotal.com/gui/home/upload
2. Phishing - Mail, Whatsapp, Social Media, platforme de comert
    a. Majoritatea oamenilor “o patesc” in Internet din neatentie si din reactivitate
        i. Primesti un mail/mesaj/anunt online care te sperie si te face sa reactionezi si sa faci ceva ce altfel nu ai fi facut
    b. Companii mari precum OLX, Facebook, eBay se confrunta cu astfel de probleme si situatii
    c. Solutia - validarea site-ului prin virustotal, contactarea unei alte persoane pentru asigurarea situatiei, daca te vezi reactionand, nu da click pe link si acorda-ti 5 minute in care sa te deconectezi, dupa care revii si privesti cu alti ochi situatia
3. Protectia datelor - parole, fisiere, documente
    a. Problema: datele pot fi furate, accesate, sparte
    b. Solutia: atentie la Wi-Fi-urile publice din cafenele, restaurante, mall-uri, hoteluri (nu fa activitati importante acolo), foloseste un VPN; criptare online; folosirea parolelor complexe generate automat cu un password generator (https://www.lastpass.com/features/password-generator); stocarea parolelori intr-un vault (ex: 1pass.com)
4. Adauga 2FA pentru cresterea nivelului de securitate
5. Inchide conturile si platformele pe care nu le mai folosesti - cere stergerea datelor si a parolelor

Retine asta: You are as strong as your weakest link.

Siguranta online este un subiect de actualitate in era digitala in care traim. Pe masura ce tehnologia evolueaza, amenintarile cibernetice devin din ce in ce mai sofisticate si mai raspandite. Este important sa luam masuri de precautie pentru a ne proteja datele personale si informatiile confidentiale impotriva atacurilor cibernetice. In acesta sectiune, vom discuta cateva modalitati de a va proteja impotriva atacurilor cibernetice din internet.

Protectia impotriva atacurilor cibernetice din internet este esentiala pentru a va asigura ca datele si informatiile personale sunt in siguranta. Iata cateva masuri pe care le puteti lua pentru a va proteja:

1. Actualizati software-ul si sistemele de operare - Actualizarea software-ului si a sistemelor de operare este cruciala pentru a remedia vulnerabilitatile de securitate. In general, actualizarile includ remedieri ale problemelor de securitate si sunt concepute pentru a proteja impotriva atacurilor cibernetice.

2. Folositi o parola puternica si activati autentificarea in doi factori - Folosirea unei parole puternice si a autentificarii in doi factori poate preveni accesul neautorizat la conturile dvs. online. O parola puternica trebuie sa contina cel putin opt caractere si sa includa o combinatie de litere, cifre si simboluri.

3. Utilizati un program antivirus si un firewall - Un program antivirus si un firewall va pot proteja impotriva virusilor, a programelor malware si a altor amenintari de securitate. Asigurati-va ca programul antivirus este actualizat si configurat sa efectueze scanari periodice ale computerului.

4. Utilizati o retea securizata - Utilizarea unei retele securizate poate preveni accesul neautorizat la datele si informatiile personale. In general, se recomanda utilizarea unei retele Wi-Fi securizate cu criptare WPA3.

5. Fiti precauti cu emailurile si site-urile web suspecte - Fiti precauti atunci cand deschideti email-uri sau site-uri web suspecte sau necunoscute. Nu faceti clic pe link-uri sau atasamente suspecte sau de la surse necunoscute.

6. Utilizati o navigare privata si un VPN - Utilizarea unei navigari private poate preveni urmarirea dvs. online si pastra datele personale private. De asemenea, utilizarea unui serviciu VPN poate ascunde adresa IP si poate cripta conexiunea dvs. la internet, oferind astfel o protectie suplimentara impotriva atacurilor cibernetice.

7. Fiti atenti la phising - Phishing-ul este o tactica folosita de infractori pentru a obtine informatii personale si confidentiale. Asigurati-va ca sunteti atenti la email-uri si mesaje de la surse necunoscute si verificati intotdeauna URL-ul site-ului web inainte de a introduce informatii personale.

8. Realizati copii de siguranta - Realizarea copiilor de siguranta ale datelor si informatiilor personale importante poate fi esentiala in cazul in care sunteti victima unei brese de securitate sau a unui atac cibernetic.

In concluzie, este important sa luati masuri de precautie pentru a va proteja impotriva atacurilor cibernetice din internet. Prin actualizarea software-ului si a sistemelor de operare, utilizarea parolelor puternice si autentificarii in doi factori, utilizarea programelor antivirus si a firewall-urilor, utilizarea retelelor securizate, fiind precaut cu emailurile si site-urile suspecte, utilizarea navigarii private si a VPN-urilor si realizarea copiilor de siguranta ale datelor personale, puteti reduce riscul de a fi victima unui atac cibernetic. Fiti vigilenti si protejati-va informatiile personale pentru a avea o experienta online sigura si protejata.

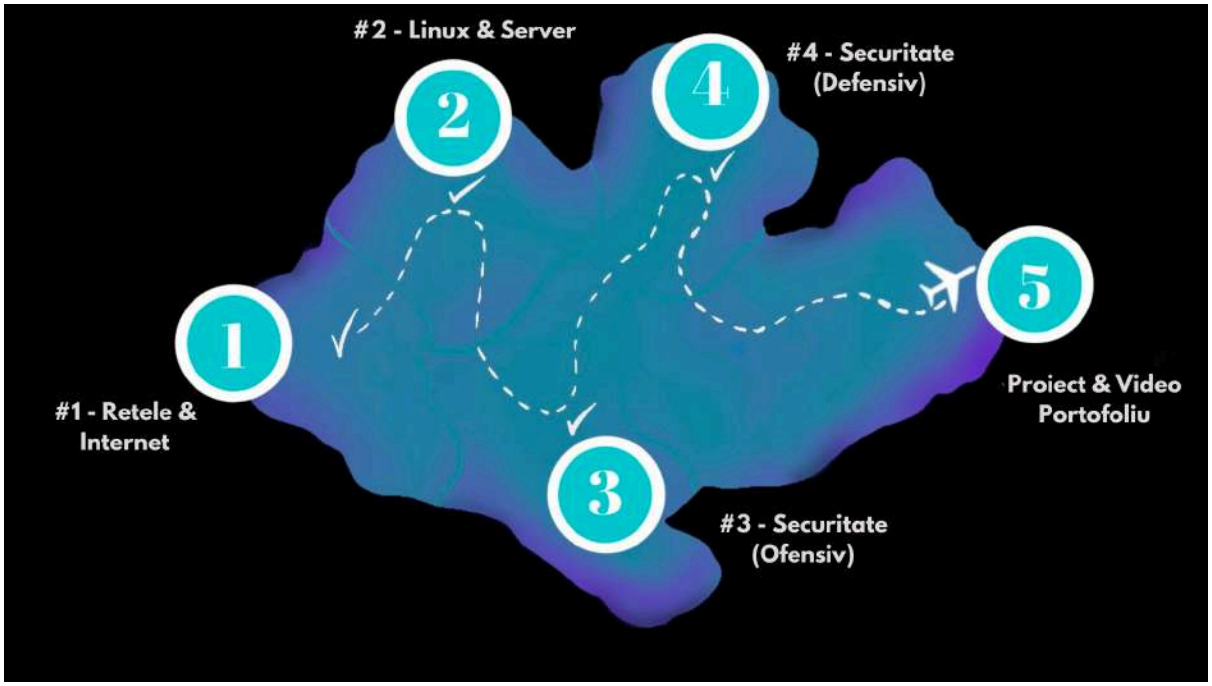
Care sunt urmatorii pasi?

Si iata-ne ajunsi la final!

Da-mi voie sa te felicit pentru parcursul tau pentru ca ai ajuns pana aici. Iti vine sa crezi sau nu dar nu foarte multi oameni reusesc sa parcurga o carte sau un curs, asadar acesta este meritul tau si ma bucur foarte mult esti aici.

In continuare, pentru **urmatoarea etapa**, iti recomand sa incepi sa dezvolti proiecte. Acum **practica** este cel mai important lucru de care ai nevoie pentru ca toate aceste cunostinte pe care le dobandit sa devina abilitati care te vor servi pe mai departe in ceea ce iti propui tu sa faci in domeniul IT.

Iata parcursul natural spre un job in IT, ilustrat in imaginea de mai jos:



La inceput ne-am concentrat pe a seta bazele:

- Retele de calculatoare & Internet - ~1 luna
- Linux & Server: ~2 luni

Dupa ce am setat bazele (dpvd. Teoretic si practic), ne concentram pe partea de Securitate Cibernetica:

- Scanarea retelelor si a serverelor
- Ofensiva - Generarea de atacuri cibernetice (DOS, MITM, Brute Force, Password Attack, etc)
- Defensiva - Protejarea userilor, a site-urilor web, a serverelor si interpretarea log-urilor de sistem

La final, punctul culminant va fi partea de proiect tehnic pe care o vei realiza fara problema dupa ce ai trecut prin pasii tehnici descrisi mai sus.

Pregatirea pentru angajare

Rezultatul concret al componentei tehnice va fi proiecte pe care il vom transforma in video portofoliu. Acesta ne va ajuta sa atragem atentia angajatorului (de 3 - 5x mai rapid fata de un CV clasic) cu scopul de a fi chemat la interviul de angajare.

Practic, muncesti smart pentru rezultate mai rapide si sigure. Iata aici cateva exemple de video portofolii realizate de catre cursanti:

- Razvan
- Dominiq
- Veronica
- Liviu
- Stefan

In etapa de pregatire de angajare, urmatorul pas dupa finalizarea video portofoliului este sa-ti creezi un profil de LinkedIn bine optimizat.

LinkedIn-ul este o platforma de socializare pe partea profesionala, extrem de folosit (in mod special de piata din vest - Europa, UK, USA). Majoritatea angajatorilor si a IT-istilor sunt prezenti pe aceasta platforma, iar noi ne dorim acelasi lucru.

LinkedIn-ul pentru noi va juca rolul de CV online si il vom folosi pentru a ne atrage atentia angajatorilor pe profilul nostru cu scopul de a ne creste sansele de a obtine interviuri cu acestia. Mai multi angajatori care intra pe profilul nostru, vor creste numarul de interviuri, care vor creste numarul de oferte de loc de munca in IT pe care le vom primi.

Exemple de profile de LinkedIn ale cursantilor care au facut reconversie profesionala in IT:

- Dominiq
- Radu
- Paula

Iata mai jos un exemplu de profil de LinkedIn optimizat, alaturi de portofoliu si job-uri din industria Securitatii IT din Romania si din strainatate (Germania, UK, etc.).

Urmareste acest material si in format video:

Cum sa obtii un JOB in IT in 2024 (chiar daca firmele concediaza)

Angajarea

Dupa ce ai reusit sa te simti stapan pe partea tehnica, ai finalizat video portofoliul si profilul de LinkedIn, urmeaza etapa de angajare. Acum, ne vom concentra pe a aplica la job-uri si a obtine mai multe interviuri de angajare care sa se concretizeze cu 1, 2 sau 3 oferte de munca concrete.

Aici iti recomand sa aplici la 100 de job-uri specific pe pregatirea ta, Securitate IT, (prin LinkedIn sau alte platforme - Indeed.com, ejobs, bestjobs, etc) si sa urmaresti la cate interviuri vei fi chemat. Daca ai facut pasii anteriori, cel mai probabil vei avea 10 - 20 de interviuri.

Dintre aceste 10 - 20 de interviuri, ai nevoie sa primesti o singura oferta care sa-ti convina si deja lucrezi in IT. In mod cert, acest lucru nu se va intampla peste noapte, tocmai de aceea iti recomand sa aplici la 3 job-uri pe zi timp 1 luna. Apoi incepi discutiile cu angajatorii si inveti de la una la alta.

Una dintre cursantele noastre, Paula, a trecut prin acesti pasi si s-a angajat dupa al 8-lea interviu. E important sa nu ne punem sperantele intr-un singur angajator/firma si sa credem ca acesta ne va lua in firma.

Facem lucrurile pas cu pas, urmarim evolutia, iar rezultatul nu va intarzia sa apara. Ia-ti o marja de 1 - 3 luni in partea aceasta de a obtine job-ul si a trece prin interviurile de angajare. Invata de la un interviu la altul (si informeaza-te despre tipurile de intrebari la interviu).

Iti las aici un tutorial video despre 24 de intrebari la interviul de angajare:

24 de INTREBARI la care TREBUIE sa stii sa RASPUNZI inainte de INTERVIUL …

Iata aici un exemplu de interviu tehnic de angajare, realizat cu cursantii din programul de Securitate IT: LINK

Ai nevoie de ajutor sa pui toate acestea in practica?

Te pot ajuta sa faci reconversia profesionala in Securitate IT in mai putin de 12 luni. Tot ce ai de facut este sa aplici aici pentru o sesiune 1:1 de consultanta gratuita in care te vom ajuta sa reusesti in domeniu, in functie de ce este important pentru tine acum.

In aceasta sesiune 1:1 gratuita iti vom prezenta strategia prin care am ajutat 100+ persoane sa se angajeze in IT, si iti vom dezvolta un **plan personalizat de invatare** pentru a obtine rezultate mai rapid si a ajunge sa faci printr-o cariera in IT.

Intra aici si aplica acum pentru o discutie 1:1 gratuita.

Iti doresc mult succes in ceea ce ti-ai propus si drum bun in noua ta etapa,
Ramon Nastase
Fondator SecuritateIT.com