Securitatea rețelelor de calculatoare si a sistemelor de operare

Obiective

Acest laborator își propune studierea aspectelor teoretice si aplicative legate de realizarea atacurilor in rețele de calculatoare si asupra sistemelor de operare.

In acest laborator veți lucra cu sistemul de operare Kali Linux, care poate fi descărcat de la: https://www.kali.org/downloads/

Veti mai lucra cu diferite aplicatii care se instaleaza in Kali Linux (sau vin preinstalate) precum si cu aplicatii independente: Metasploit disponibil la https://www.apachefriends.org/download.html

Introducere

Securitatea reprezintă abilitatea de a evita neplăcerile produse de orice risc, amenințare sau pericol. În practică, acest lucru este imposibil de realizat.

Incident de securitate este un eveniment apărut in cadrul rețelei, provenind din interiorul ori exteriorul rețelei, cu implicații asupra securității unui calculator sau a rețelei.

Se poate introduce un limbaj comun pentru descrierea incidentelor:

Principalul obiect de studiu: ***eveniment*** *(incident legat de securitate)*
- *– consta dintr-o* ***acțiune*** *executata asupra unei* ***ținte***
- *– acțiunea poate fi executata cu o* ***unealta***
- *– exploatând un anumit tip de* ***vulnerabilitate***
- *– cu un anumit* ***rezultat*** *(in mod normal neautorizat)*

Abordarea problemei securității datelor intr-o rețea presupune in primul rând *identificarea cerințelor de funcționare* pentru acea rețea, apoi *identificarea tuturor amenințărilor posibile* (împotriva cărora este necesara protecția). Aceasta analiza consta in principal in trei sub-etape:

- *analiza vulnerabilităților* - identificarea elementelor potențial slabe ale rețelei
- *evaluarea amenințărilor* - determinarea problemelor care pot apărea datorata elementelor slabe ale rețelei si modurile in care aceste probleme interfera cu cerințele de funcționare
- *analiza riscurilor* - posibilele consecințe pe care problemele le pot crea

Următoarea etapa consta in *definirea politicii de securitate*, ceea ce înseamnă sa se decidă:

- care amenințări trebuie eliminate si care se pot tolera
- care resurse trebuie protejate si la ce nivel
- cu ce mijloace poate fi implementata securitatea
- care este prețul (financiar, uman, social etc.) masurilor de securitate care poate fi acceptat

O rețea LAN are un singur administrator si o singura politica de securitate, in vreme ce rețelele WAN au mai mulți administratori si politici de securitate multiple.

Odată stabilite obiectivele politicii de securitate, următoare etapa consta in *selecţia serviciilor de securitate* - funcţiile individuale care sporesc securitatea reţelei. Fiecare serviciu poate fi implementat prin metode (mecanisme de securitate) variate pentru care sunt necesare aşa-numitele funcţii de gestiune a securităţii. Gestiunea securităţii intr-o reţea consta in controlul si distribuţia informaţiilor către toate sistemele deschise ce compun acea reţea in scopul utilizării serviciilor si mecanismelor de securitate si al raportării evenimentelor de securitate ce pot apărea către administratorii de reţea.

Aspecte ale securităţii in reţele de calculatoare:

– ***Identitatea***: va cuprinde elementele de ***autentificare*** şi ***autorizare*** la nivelul reţelei.

– Autenticitatea: presupune ca două entităţi aflate într-un schimb de mesaje se pot identifica una pe cealaltă. În prima fază, la iniţierea conexiunii, acest serviciu asigură că cele două entităţi sunt autentice. În al doilea rând, autenticitatea presupune că transferul de date dintre cele două entităţi nu este interferat astfel încât o a treia entitate poate să se legitimeze ca fiind una din ele.

– Autorizarea: este abilitatea de a limita şi controla accesul în reţea (la sisteme sau aplicaţii). Pentru a realiza acest serviciu, fiecare entitate care încearcă să aibă acces trebuie mai întâi identificată şi apoi verificate drepturile de acces în sistem.

– ***Integritatea***: este o componentă a securităţii care cuprinde infrastructura de securitate (accesul fizic şi logic) precum şi securizarea perimetrului. Ea se referă la asigurarea consistentei informaţiilor, încrederea in date sau resurse (în cazul transmiterii unui mesaj prin reţea, integritatea se referă la protecţia împotriva unor tentative de falsificare a mesajului);

– ***Confidenţialitatea***: asigura faptul că transmisiile de date de-a lungul reţelei au caracter privat. Există numeroase posibilităţi pentru confidenţialitatea informaţiilor de la protecţie fizică până la algoritmi matematici.

– ***Disponibilitatea***: va asigura faptul că toate resursele reţelei sunt disponibile personalului sau proceselor autorizate.

– ***Nerepudierea***: măsură prin care se asigură faptul că, după emiterea/recepţionarea unei informaţii într-un sistem de comunicaţii securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informaţii *Se previne ca nici o entitate să nu refuze să recunoască un serviciu executat. Când un mesaj este trimis, destinatarul poate demonstra că mesajul primit este cel trimis de emiţător. Similar, când un mesaj este primit, emiţătorul poate demonstra că mesajul primit este cel primit de destinatar.*

– ***Auditul***: este necesar pentru monitorizarea şi verificarea securităţii la nivelul firmei

Atacuri in reţele de calculatoare

Atac este un eveniment potenţial distrugător provocat intenţionat de persoane răuvoitoare. Nu toate elementele care afectează o rețea de calculatoare sunt atacuri! Pot exista si:

• Defect =eveniment potenţial distrugător cauzat de deficiente ale sistemului sau ale unui factor de care depinde sistemul (e.g. defecte hard, bug-uri soft, erori ale utilizatorilor)

• Accident =evenimente aleatoare (neprevăzute); exemple: dezastre naturale, căderi de tensiune

Atribute ce trebuie considerate pentru a estima reuşita unui atac (cunoaşterea profilului atacatorului): Resursele disponibile (financiare, tehnice,… + pregătirea in domeniu); Timpul alocat (atacatorii răbdători vor avea mai mult succes); Riscul asumat – depinde de obiective (atacul poate sau nu fi revendicat); Accesul la Internet si calitatea acestuia: tip (dial-up, conexiune satelit,…), mod de alocare a adreselor IP etc.; Obiectivele urmărite (recunoaştere mondiala, denigrarea ţintei, furt de informaţii sau bani etc.)

Niveluri de atac

– ***Oportunist****:* Atacul are un scop "recreational" si nu are obiective/ţinte clar definite. Se utilizează programe disponibile liber pentru a scana sau testa vulnerabilitati uzuale. Nu necesita acces in interiorul sistemului. Cunoştinţe vagi despre sistemul/organizaţia ţinta • Masuri de precauţie: – ziduri de protecţie (firewall-uri) – actualizarea versiunilor de programe

– ***Intermediar*** Obiectiv este conturat, la nivelul organizaţiei. Se efectuează aceleaşi acţiuni ca la atacul "recreational", dar se încearcă ascunderea lor. Atacatorul are mai multa răbdare decât in cazul unui atac oportunist . Cunoştinţe tehnice mai profunde. Probabilitate mai mare de succes, posibil efecte mai puternice

– ***Sofisticat****:*• Obiectiv foarte bine conturat. Ţinta este de cele mai multe ori o organizaţie. Atacurile pot trece peste masurile de prevedere •Atacatorul va avea multa răbdare. Se investeşte timp pentru adunarea de informaţii despre sistemul/organizaţia ţinta • Necesita foarte bune abilitaţi tehnice si are o probabilitate mare de succes.

Prevenirea atacurilor

Modelul de securitate pentru un sistem (un calculator sau o rețea de calculatoare) poate fi văzut ca având mai multe straturi ce reprezintă nivelurile de securitate ce înconjoară subiectul ce trebuie protejat. Fiecare nivel izolează subiectul si il face mai dificil de accesat in alt mod decât cel in care a fost prevăzut.

1. *Securitatea fizica* reprezintă nivelul exterior al modelului de securitate si consta, in general, in încuierea echipamentelor informatice intr-un birou sau intr-o alta incinta precum si asigurarea pazei si a controlului accesului. Aceasta securitate fizica merita o considerație speciala. Una dintre problemele mari o constituie salvările sub forma de copii de rezerva (backup) ale datelor si programelor, precum si siguranța păstrării suportilor de salvare. Rețelele locale sunt, in acest caz, de mare ajutor, copiile de rezerva putându-se face prin retea pe o singura masina ce poate fi mai usor securizata. O alta problema importanta in securitatea unui sistem informatic o constituie pur si simplu sustragerile de echipamente. In plus, celelalte masuri de securitate (parole etc.) devin nesemnificative in cazul accesului fizic neautorizat la echipamente.
2. *Securitatea logica* consta din acele metode logice (software) care asigura controlul accesului la resursele si serviciile sistemului. Ea are, la rândul ei, mai multe niveluri impartite in doua grupe mari : *niveluri de securitate a accesului* si *niveluri de securitate a serviciilor*.
    - *Securitatea accesului* cuprinde:
        - accesul la sistem, care este răspunzător de a determina daca si cand este reteaua accesibila utilizatorilor si in ce conditii. El poate fi raspunzator de asemenea si de gestionarea evidentei accesului. Accesul la sistem poate efectua si deconectarea fortata in anumite cazuri (ex. expirarea contului, ora de varf, ...)

        - accesul la cont care verifica daca utilizatorul ce încearcă sa se conecteze are un nume si o parola valida.
        - drepturile de acces (la fișiere, resurse, servicii etc.) care determina de ce privilegii dispune un utilizator (sau un grup de utilizatori) dat.
    - *Securitatea serviciilor* (care se afla "sub" securitatea accesului) controlează accesul la serviciile unui sistem (mașina, rețea). Din acest nivel fac parte:
        - *controlul serviciilor* care este responsabil cu functiile de avertizare si de raportare a stării serviciilor, precum si de activarea si dezactivarea diverselor servicii oferite de către sistemul respectiv
        - *drepturile la servicii* care determina exact cum folosește un anumit cont un serviciu dat (acces la fișiere, resurse, prioritate,...)

Elaborarea de politici de securitate implica:

– Planificarea cerinţelor de securitate
• Confidenţialitate, integritate, disponibilitate, control
– Evidenţierea riscurilor
– Analiza raportului cost-beneficii
• Costurile prevenirii, refacerii după dezastru etc.
– Stabilirea politicilor de securitate
• Politica generala (naţionala, organizaţionala,…)
• Politici separate pentru diverse domenii protejate
• Standarde & reglementari (recomandări)
• Masurile luate pot fi tehnice si non-tehnice

Supravieţuirea reprezintă capacitatea unui sistem (calculator/reţea) de a-si îndeplini misiunea, in timp util, in prezenta *atacurilor*, *defectelor* sau *accidentelor*

Sistemul trebuie sa-si duca pana la capăt misiunea chiar daca unele componente sau parţi din sistem sunt afectate ori scoase din uz

• Sistemul trebuie sa susţină măcar îndeplinirea funcţiilor vitale:
– Identificarea serviciilor esenţiale
• Proprietati ale sistemului:
– Rezistenta la atacuri
– Recunoaşterea atacurilor si efectelor lor
– Adaptarea la atacuri
• Instrumente sub Linux (Unix):
– Utilitare de reţea: ping, traceroute, netstat, ifconfig, route, host, finger, telnet
– Scanere de porturi: NMAP
– Interceptoare de retea: tcpdump, wireshark
– Testarea securităţii locale: /etc/shadow, Crack, Titan
– Verificări asupra sist. de fisiere: tripwire, showmount
– Salvari de siguranta: tar, dump, amanda

– Verificarea daemonilor: chkconfig
–Protecţia TCP/IP: iptables (firewall), activarea mecanismului SYN cookies in nucleu

Implementare Atacuri

Realizarea unui atac are mai multe etape.

1. **Recunoastarea:** Este etapa de inceput in realizarea oricarui atac. De multe ori nici nu este necesara realizarea unui atac complex asupra unui sistem de calcul daca se poate expoata mai usor factorul uman (un email bine scris…). In cazul in care nu se reuseste acest lucru, se trece la pasul urmator.
2. **Utilitare pentru recunoaștere in rețea:** Pentru început este necesara investigarea țintei (recunoaștere) pentru a descoperi caracteristicile acesteia cat si vulnerabilitățile pe care aceasta le are.
3. **Utilitare pentru realizarea atacurilor**: In continuare se va realiza atacul sau o prima etapa a acestuia. Un atac direct este de exemplu cel de negare a accesului la serviciu (DoS). Un atac de tip intermediar este cel Man in the Middle prin care atacatorul obține doar acces la date, urmând sa realizeze un alt atac asupra informațiilor capturate pentru a obține informațiile relevante.
4. **Utilitare pentru extragerea datelor**. Odata obtinute datele acestea trebuie extrase. Daca este o cantitate mare de date acest proces trebuie realizat fara sa atraga atentia. Uneori se cauta in datele capturate doar informatiile utile pentru a reduce cantitatea de date care trebuie trimisa.
5. **Ascunderea urmelor**: Daca se doreste exploatarea ulterioara a tintei, aceasta nu trebuie sa isi dea seama ca a fost atacata, deci se pot ascunde urmele lasate: aplicatii, porturi deschise, etc.

Pentru implementarea atacurilor prezentate mai jos se va descărca Kali Linux pe 64 de biti.

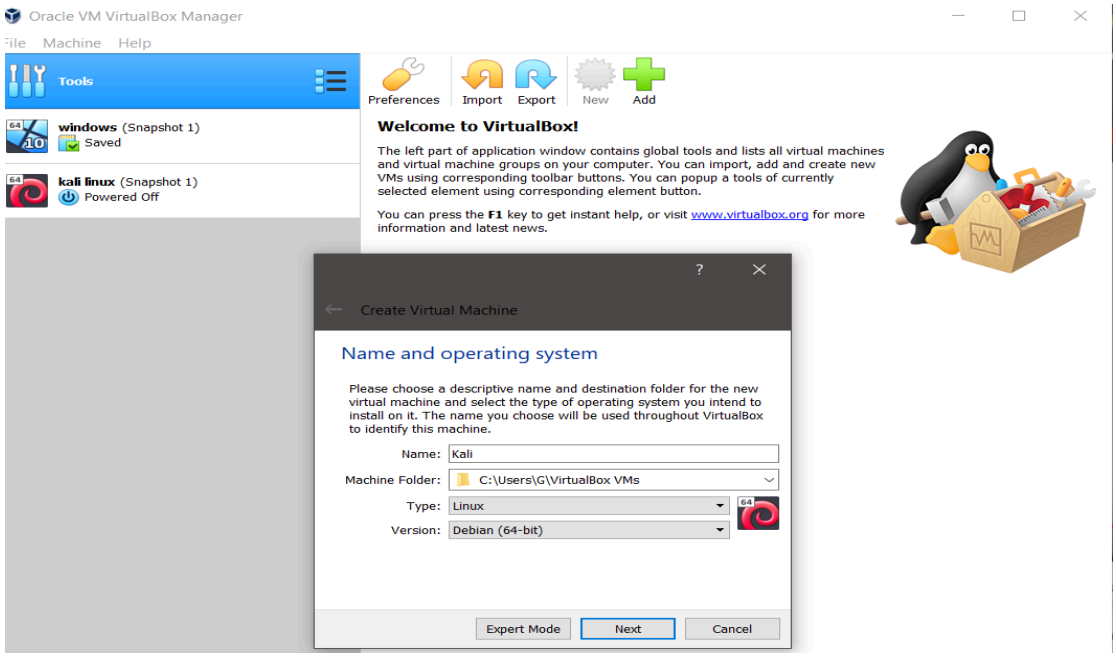
Instalare KALI LINUX (OracleBox)

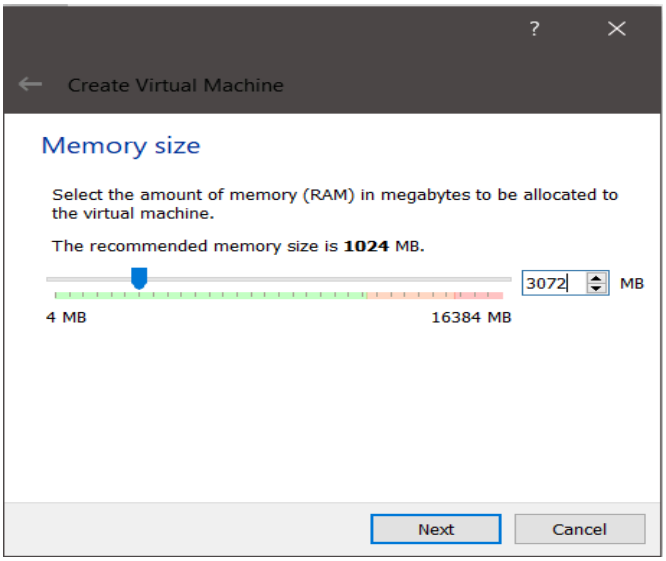
1. Se descarca fisierul Kali Linux ISO Image prin accesarea linkul : https://www.kali.org/downloads/

   Se selecteaza versiunea pe 64 de biti.

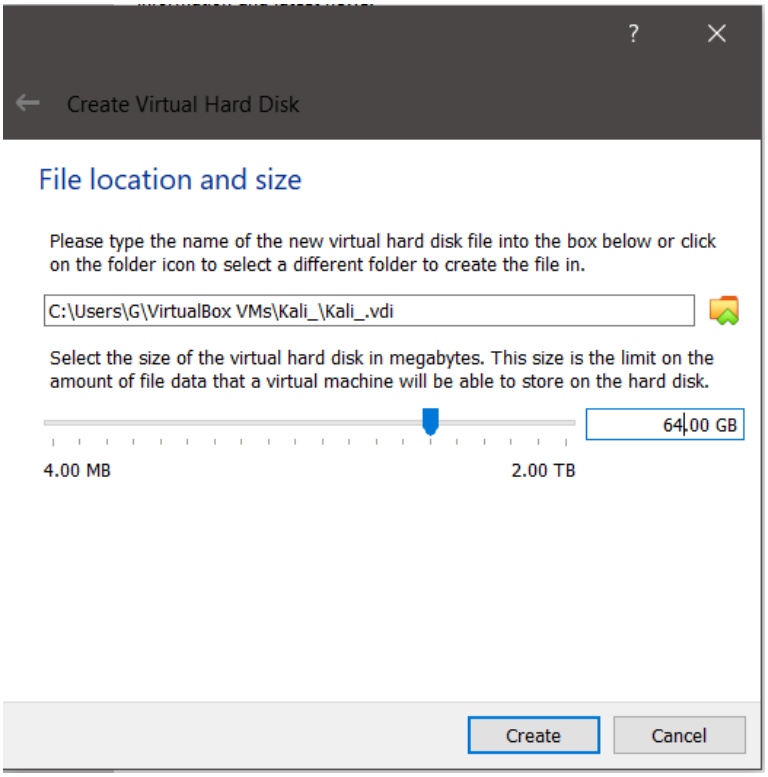
Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit	Torrent	2019.4	2.6G	bad0d602a531b872575e23cc025b45fee475523b51378a035928b733ca395ac5

2. Se creaza o masina virtuala in Oracle VirtualBox cu urmatoarele specificatii:





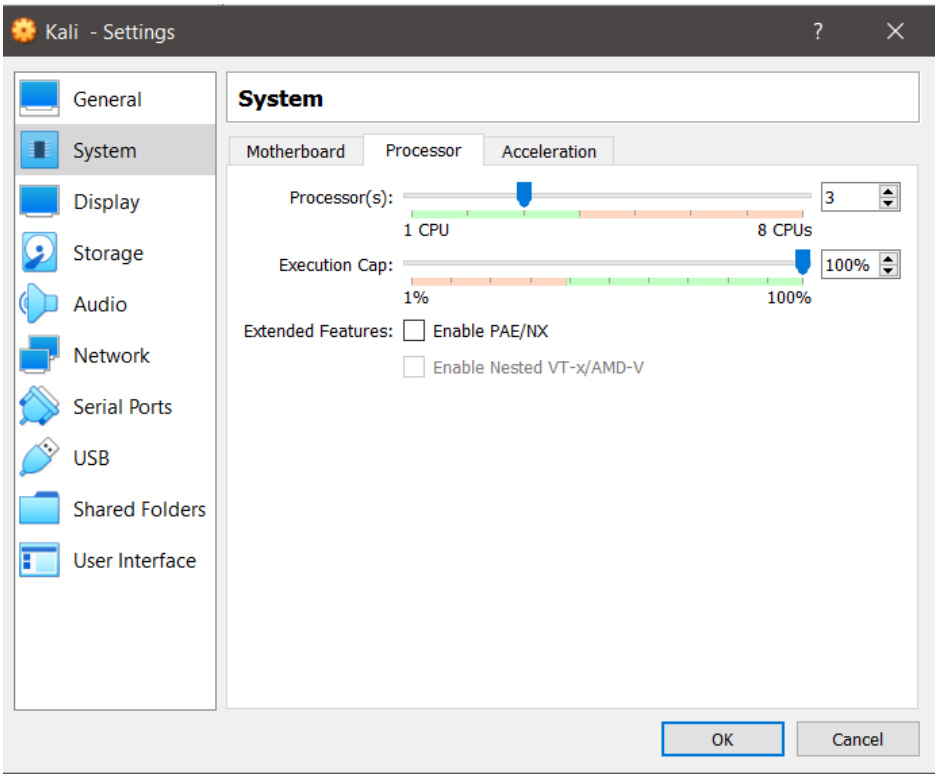
Se continua cu Next Create Next Next .



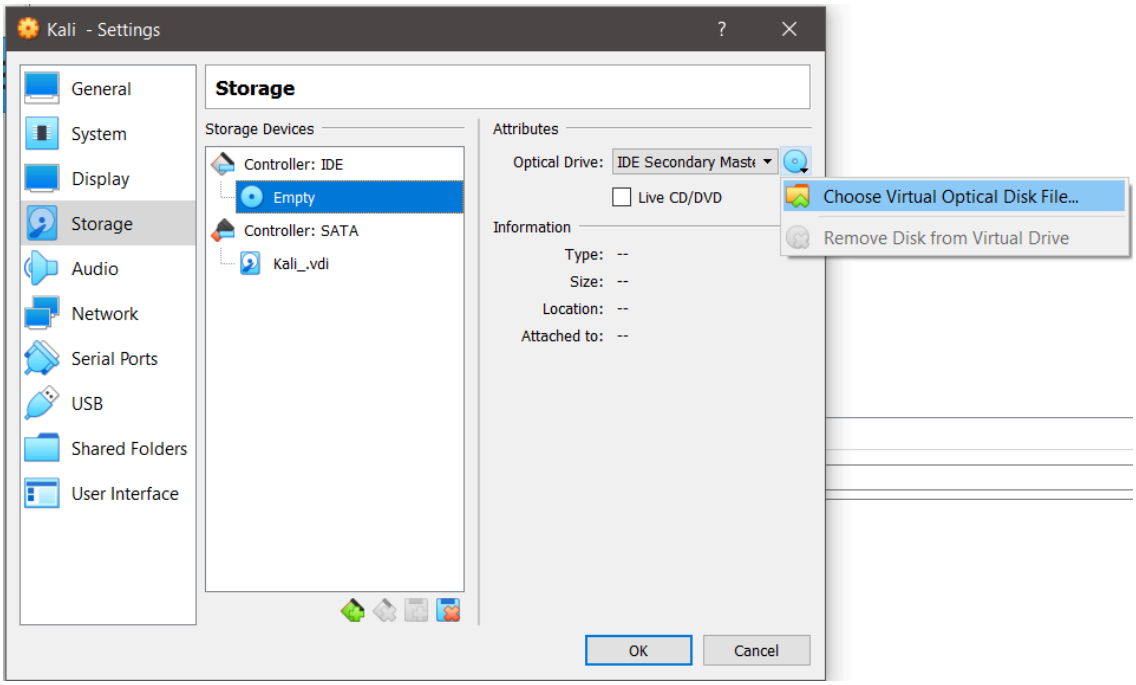
Dupa finalizare , se intra in meniul de **Setari Storage Controller: IDE Empty.**

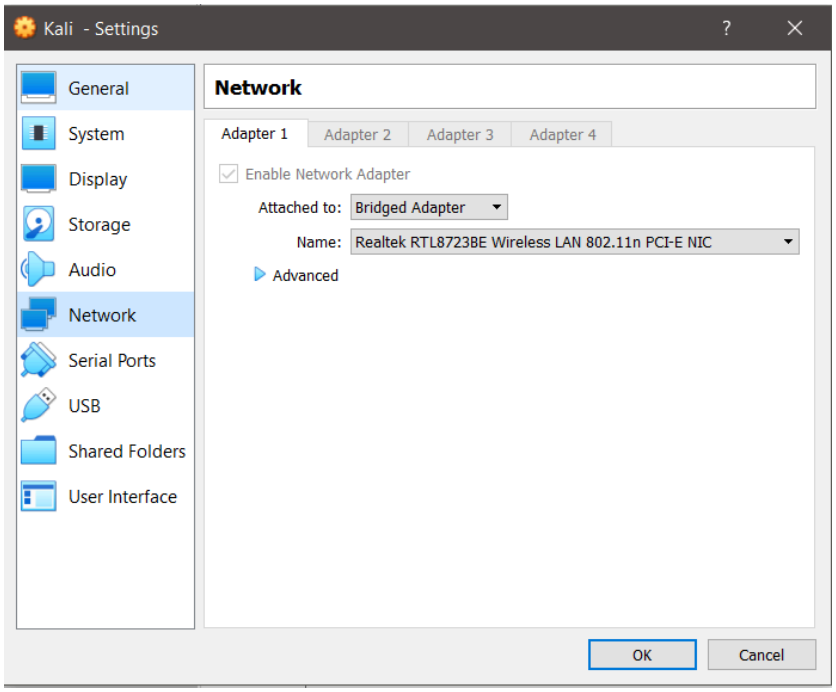
System si adugam inca **2 procesoare**.

Network Bridged Adapter

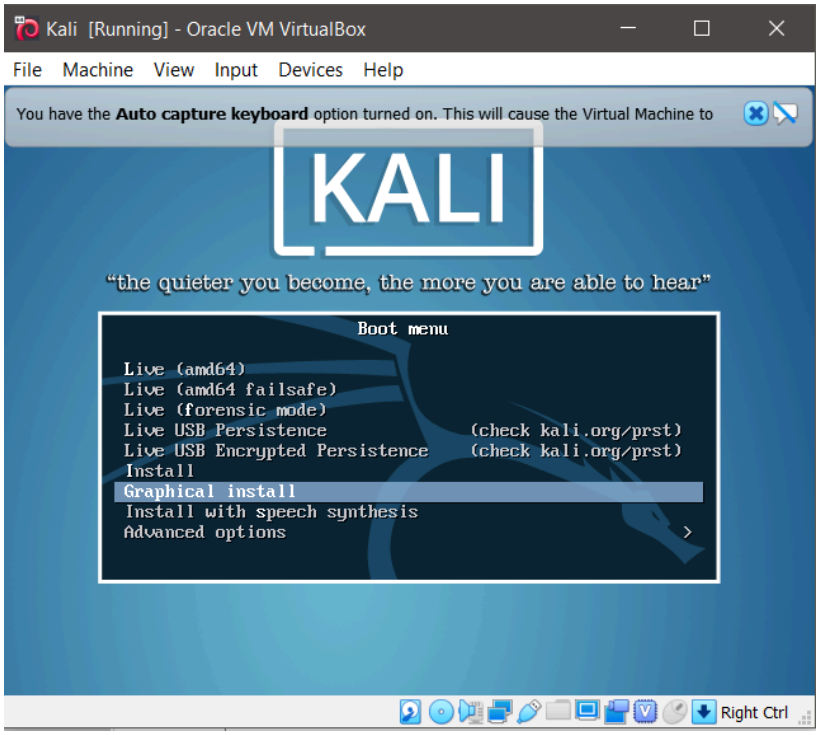


In partea dreapta la **Optical Drive** adaugam fisierul **Kali.ISO** descarcat anterior si apoi se apasa butonul **START** din meniul masinii virtuale.

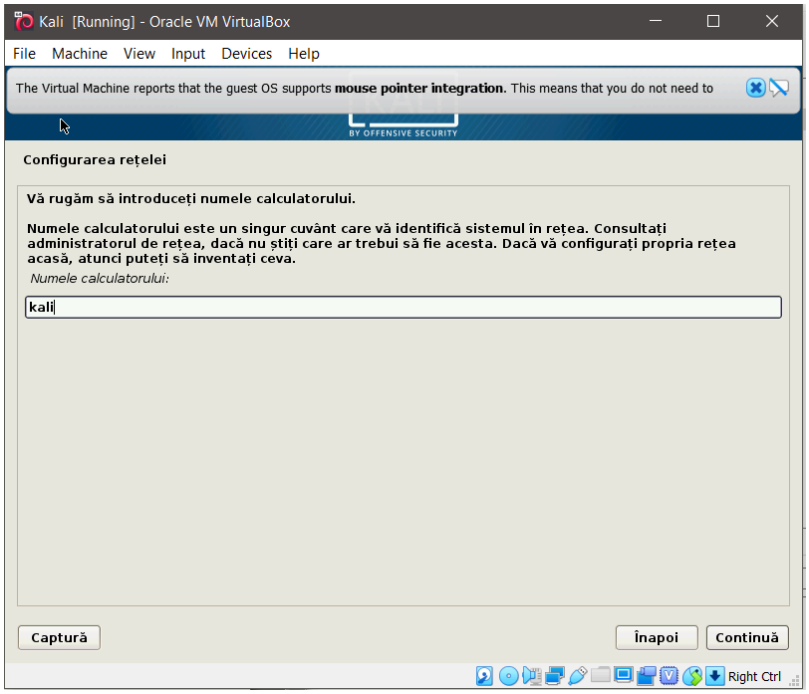




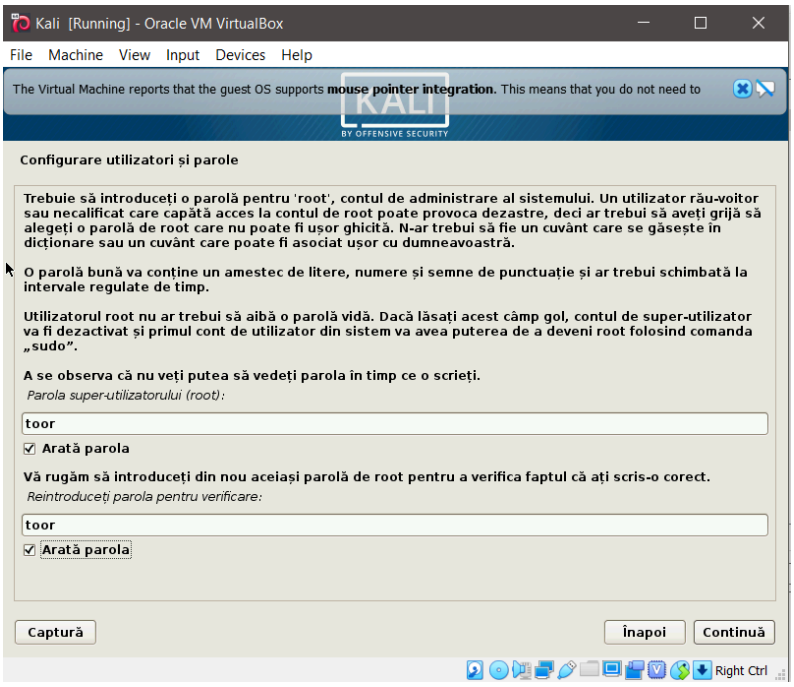
3. In acest moment putem instala KALI Linux



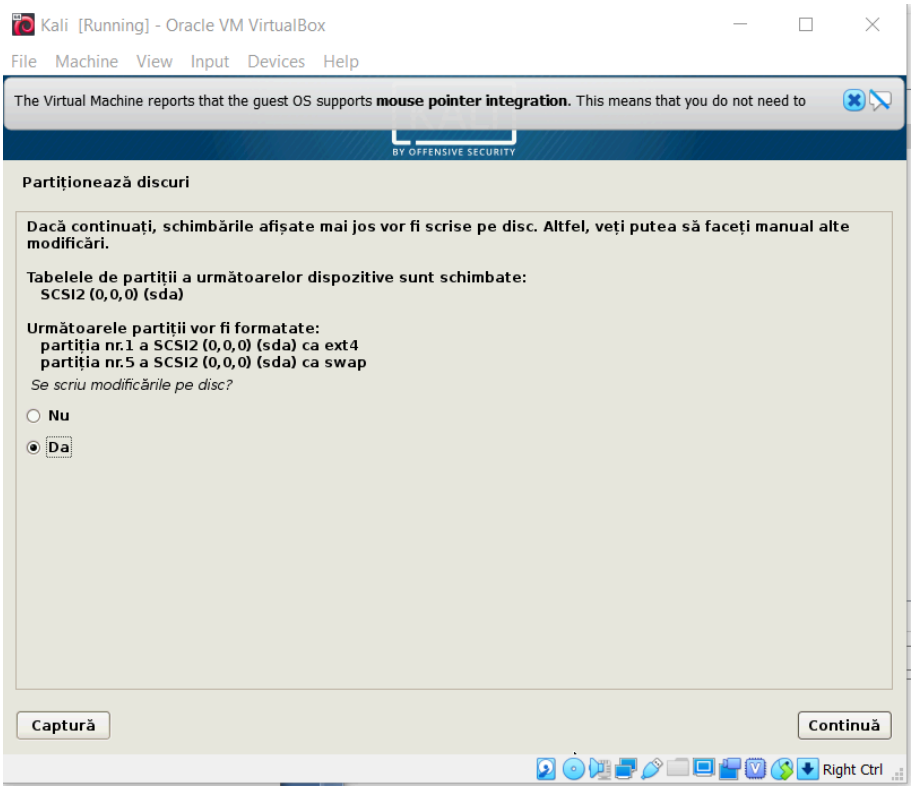
In continuare se selecteaza **limba** si **zona** dorita si se da click pe **Continua** pentru configurari.
Se alege un **nume** al computerului.



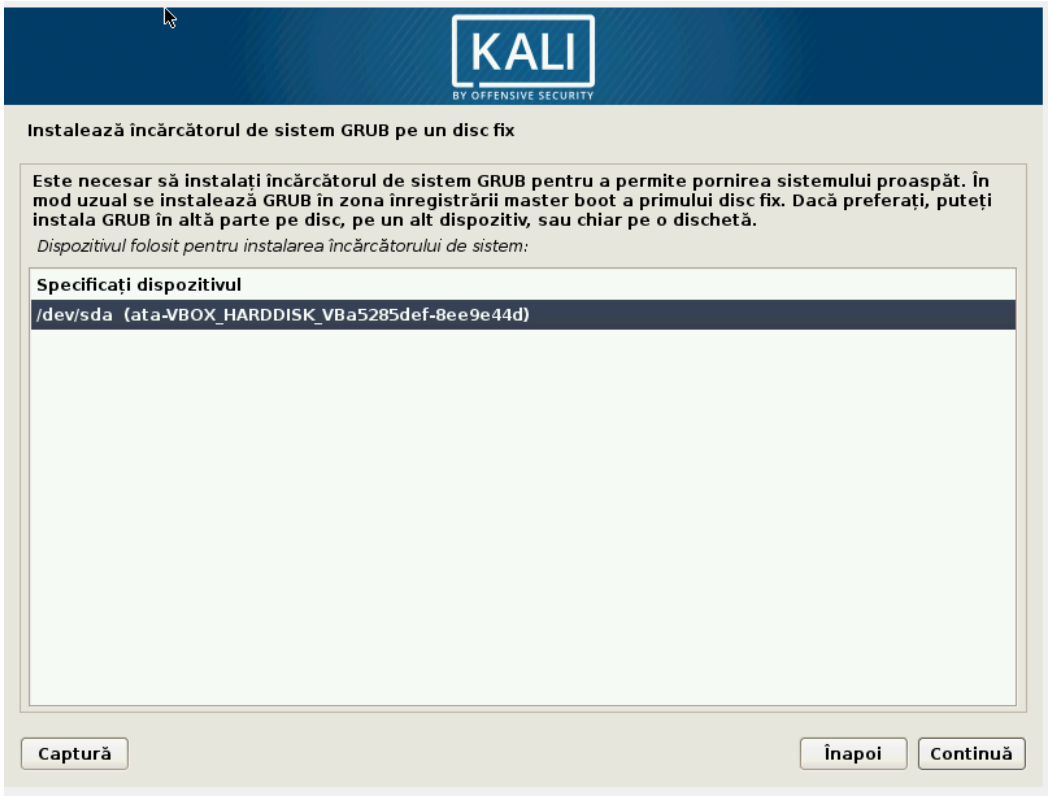
In fereastra de **Nume Domeniu** se lasa **camp gol** iar apoi se seteaza **o parola** .



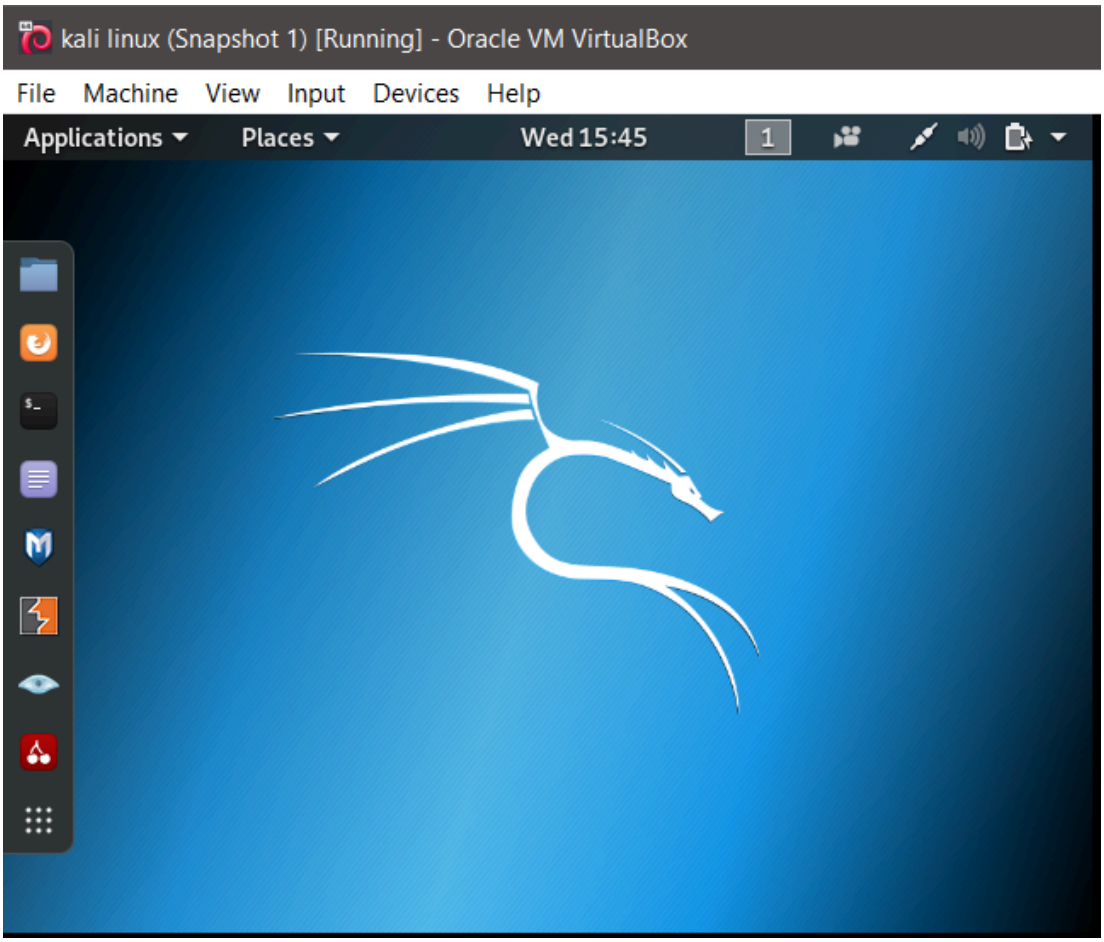
In urmatoarele etape se da click pe **Continua** pana la fereastra cu **Partionare discuri** in care se selecteaza **DA**.



Se mentine cu **Continua** dupa instalare pana la finalizarea procesului de instalare.



Pentru logare introduceti numele de utilizator si parola setate anterior.



După instalare se va verifica faptul ca fisierul **/etc/apt/sources.list** contine linia de mai jos, daca nu aceasta va fi adăugată manual:

deb http://http.kali.org/kali kali-rolling main non-free contrib

Pentru a verifica actualitatea link-urilor catre resursele software se executa ca root:

apt-get update

Daca nu se rulează aceasta comanda, instalarea de aplicații noi din sursele online ale Kali Linux nu va reusi.

Utilitare pentru recunoaștere in rețea

Aceste utilitare realizeaza recoltarea informațiilor despre o anumită rețea, o etapa necesara înaintea începerii unui atac. Se caută orice informație utilă care poate fi folosită în desfășurarea unui

atac ulterior: IP-urile stațiilor dintr-o rețea; Serviciile ce rulează pe fiecare stație; Locația serviciilor în care utilizatorii rețelei au încredere; Vulnerabilități în versiunile serviciilor.

-ping scan

Se va folosi utilitarul **nmap** pentru a scana stațiile prezente in rețea. Comanda următoare trimite un mesaj ICMP echo către calculatoarele din rețea.

nmap –sP 192.168.94.0/24

Informații despre sistemul de operare de pe un anumit calculator se pot obține cu:

nmap –O www.upit.ro

Informații despre porturile deschise se obțin cu:

nmap –sP –p T:20-25,80 192.168.94.0/24

Informatii despre serivicii si versiunea acestora:

nmap –sV 192.168.94.15

sau

nmap –sV www.upit.ro

Utilitare pentru captura de pachete

Utilitarul tcpdump poate fi folosit pentru a captura informații pe o anumita interfața. Pentru a realiza acest lucru se poate folosi comanda:

tcpdump –i eth0 –c 10 dst port 80

Parametri comenzii sunt:

- -i interfata pe care se realizează captura
- -c numarul de pachete care vor fi capturate
- *dst* sau *src* pentru filtrarea in funcție de port

Investigarea informațiilor legate de un domeniu:

whois 8.8.8.8

Investigarea informațiilor legate de serverele de nume:

host –t MX upit.ro

Utilitare pentru scanarea porturilor deschise

Pentru acest atac se folosește aplicația unicornscan:

apt-get install unicornscan

Pentru realizarea scanării unui calculator:

unicornscan 192.168.94.120 –Iv

Pentru a scana intreaga retea petnru conexiuni TCP:

unicornscan -msf -v 192.168.94.1/24

Pentru a scana întreaga rețea pentru servere UDP:

unicornscan –mU –v 192.168.94.1/24

Utilitare pentru realizarea atacurilor

Atacurile de tip Denial of Service (DoS) vizează blocarea accesului la resursele rețelei. Deși serverele funcționează, nici un utilizator nu mai poate accesa aceste resurse. Atacurile sunt realizate prin transmiterea unui numar mare de cereri intr-un interval mic de timp. Serverul nu va putea determina care sunt cereri valide si care fac parte dintr-un atac. Totodată, din cauza încărcării există inclusiv riscul ca aplicația să întâmpine o eroare și să se oprească.

Atacurile de tip DoS se detectata monitorizând traficul curent si comparându-l cu traficul pentru condiții normale. Daca nivelul traficului curent este anormal de mare,

Atac de tip smurf: se realizeaza prin trimitere de Ping-uri către o adresă de broadcast cu o adresă sursă spoofed (impersonata – adică atacatorul completează in câmpul adresei sursa adresa IP a calculatorului). Toate stațiile din rețeaua respectivă vor răspunde către sursă • Dacă rețeaua este mare stația țintă poate să primească mai mult trafic decât poate procesa – Efectul este imposibilitatea folosirii conexiunii la Internet pentru uz normal.

Realizarea atacului: Se trimit pachete ICMP folosind aplicația ping către IP-ul de broadcast al rețelei din care facem parte:

ping 192.168.94.255

Se observa apoi in Wireshark si in Task manager in Windows (sau iptraf in Linux) nivelul traficului recepționat. Pentru un atac catre un anumit PC trebuie modificat câmpul de adresa IP sursa pentru ca atacul sa fie direcționat către acel calculator.

Atac de tip SYN flood: Atacatorul inițiază un număr mare de conexiuni TCP cu un server, fără a termina handshake-ul inițial (conexiuni half-open) • Respectivele conexiuni epuizează resursele serverului si acesta nu mai poate procesa cereri valide.

Realizarea atacului:

Se instaleaza aplicatia hping3

sudo apt-get install hping3

Se pornește atacul de inundare cu pachete SYN (parametrul -S) către un anumit IP (in acest caz **192.168.94.12** care poate fi adresa unei masini virtuale) si se trimit 15000 de pachete, fiecare de dimensiune 120 de octeți, cu o dimensiune a ferestrei TCP de 64 . Pachetele vor fi trimise cat de repede este posibil prin precizarea parametrului **flood**

hping3 -c 1500 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.94.12

- **–rand-source:** trimite random adrese IP sursa target-ului
- **–f**: fragmenteaza pachetele, facand mai multe sanse sa treaca prin dispozitive de securitate
- **–S:** trimite pachete SYN pentru a crea conexiuni semi-deschise
- **–flood**: trimite pachete cat mai repede posibil

Detectarea atacului se poate face folosind Wireshark prin vizualizarea nivelului mare de trafic(**Statistics>I/O Graph**) sau aplicarea suplimentara a filtrului in câmpul de filtrare a pachetelor:

tcp.flags.syn == 1 and tcp.flags.ack == 0

Atacurile fork bomb

Un fork bomb este o aplicatie care porneste in scurt timp un numar mare de procese. Acestea vor ocupa memeoria sistemului de calcul si resurse deoarece trebuie sa creeze procesele si s-a cicleze prin ele deoarece sunt mult mai multe decat proceseoarele fizice disponibile pe system.

Pentru a ne proteja impotriva acestui atac putem limita numarul proceseleor din shell.

Utilitarul **ulimit** din Linux are rolul de a scrie/citi valorile limitelor pentru procesul shell. Aplicaţie:

● Folosiţi ulimit pentru a preveni un fork bomb:

❍ Limitaţi numărul de procese din shell-ul vostru **ulimit -u 300**

❍ Verificaţi că aceste valori s-au setat verificând fişierul /proc/$$/limits

❍ Rulaţi, în aceeaşi consolă, următorul program care creează un fork-bomb: **:(){ :|:& };:**

sau

cd Desktop

touch forkbomb.bash

nano forkbomb.bash

scrieti in fisier:

```
:(){
    :|:&
};:
```

rulati din terminal: bash forkbomb.bash

❍ Mai puteţi crea procese în acel terminal?

❍ Afişaţi din altă consolă procesele bash create

Tema: Creati o aplicatie in C care genereaza 50 de procese care asteapta 2 secunde inainte de a se inchide. Executati aplicatia intr-o consola limitata cu ulimit la 10 procese. Ce se intampla?

Atacuri care vizează accesul

Obținerea parolelor folosite in rețea se poate realiza prin sniffing (monitorizarea traficului) pentru serviciile nesecurizate: HTTP, FTP, Telnet.

Parolele cărora li s-a obținut hash-ul pot fi sparte prin:

– Brute force (se încearcă toate combinațiile ce folosesc un set de simboluri)

– Dictionary attack (se încearcă toate cuvintele din dicționar împreună cu permutări simple)

– Cryptanalysis attack (Rainbow tables).

Atacurile Brute force / dictionary attack pot fi aplicate direct pe serviciul de autentificare, fără a avea hash-ul. Ele sunt ușor de blocat prin adăugarea de limitări la autentificare (de exemplu blocarea contului pentru 10 minute la 3 eșuări de autentificare în decurs de un minut).

Rainbow Tables: sunt atacuri de criptanaliză. Parolele nu sunt salvate in sistem in clar (necriptat) si un hash al acestora. La login se compara hash-ul salvat cu hash-ul calculat al parolei introduse. Daca cele doua coincid, userul este autentificat. Pentru spargere se pot folosi tabele de hash-uri precalculate pentru parole cunoscute, deci este necesar mult spațiu insa se reduce considerabil timpul de realizare al unui atac. Rainbow tables mențin punctele de pornire pentru lanțuri de hash-uri. Rainbow tables publice se pot obține de pe Internet – www.freerainbowtables.com (~5 TB)

Metodă de prevenire a atacurilor ce folosesc rainbow tables: Se folosește un segment suplimentar, generat aleator, ce este concatenat la parola utilizatorului înainte de hashing • Segmentul aleator crește dimensiunea tabelelor necesare pentru spargere.

Atac: Spargerea parolei Linux

Se va folosi utilizatorul ***John The Ripper*** pentru a realiza un atac de forta bruta. Acesta poate fi folosit atât pentru parole Linux cat si pentru parole Windows. Exista doua aplicații de acest tip: johnny (cu interfața grafica) si john (fără interfața grafica). Vom folosi aplicația cu interfața grafica:

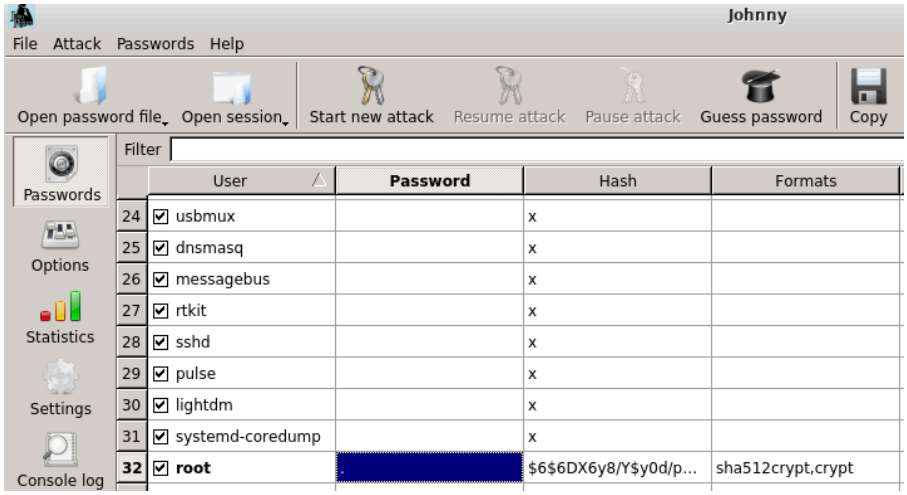
apt-get install johnny

In Linux fișierul care conține datele despre utilizatori este /etc/passwd iar cel care conține parolele in format criptat SHA este /etc/shadow

Se vor combina cele două fișiere intr-un fișier numit crack de pe Desktop:

cat /etc/passwd >> Desktop/crack && cat /etc/shadow >> Desktop/crack

Se pornește aplicația si se încărca fișierul *crack* in aplicație. Aplicația va găsi parola cu atât mai repede cu cât parola este mai simpla.



Atacul se poate realiza si din linie de comanda.

Atacul Man in the Middle (MiM)

Traficul dintre două entități este interceptat și rutat de un atacator, de exemplu traficul între o stație și default gateway.

Atac: Otravire ARP

Se bazează pe faptul că protocolul ARP nu face autentificare – O stație poate minți referitor la adresa sa de nivel 3. Atacul functioneaza doar in reteaua locala. Un exemplu de program pentru ARP Poisoning: Cain and Able. Ghid aici: https://www.youtube.com/watch?v=_pCeEv7d6Sw

Pentru kali linux urmatorul ghid:https://itigic.com/ro/arp-poisoning-attack-how-to-do-it-on-kali-linux/

Social engineering

Se bazează pe extragerea informațiilor confidențiale de la oameni: Parole sau detalii financiare; Atacatorul trebuie să convingă potențialele ținte că este de încredere; Este probabil ca ținta respectivă să nu fie de profil tehnic și să aibă încredere în autoritatea atacatorului. Atacatorul se poate da drept un membru al echipei tehnice. Oamenii nu sunt conștienți de valoarea informației pe care o posedă și vor să ajute. Social engineering poate evita orice tip de securitate

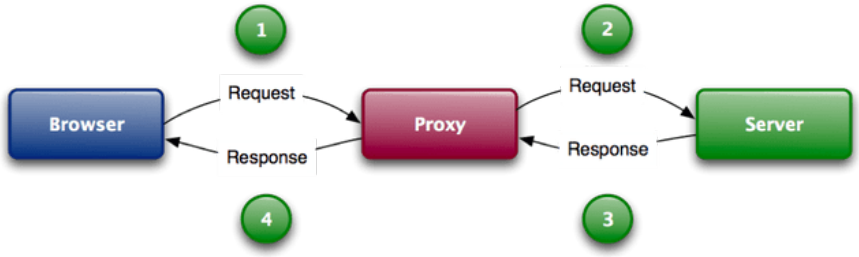
Atac: virusi

Visurii reprezinta cod executabil atașat unui program sau executabil. Codul trebuie să fie rulat de un utilizator pentru a avea efect. Se propagă prin:
– Atașamente de e-mail
– Fișiere descărcate infectate
– Partajări de fișiere în rețeaua locală
– Stick-uri USB
O suita buna pentru a insera cod care permite controlul unui calculator la distanta este Metasploit.

Suite pentru testarea securității

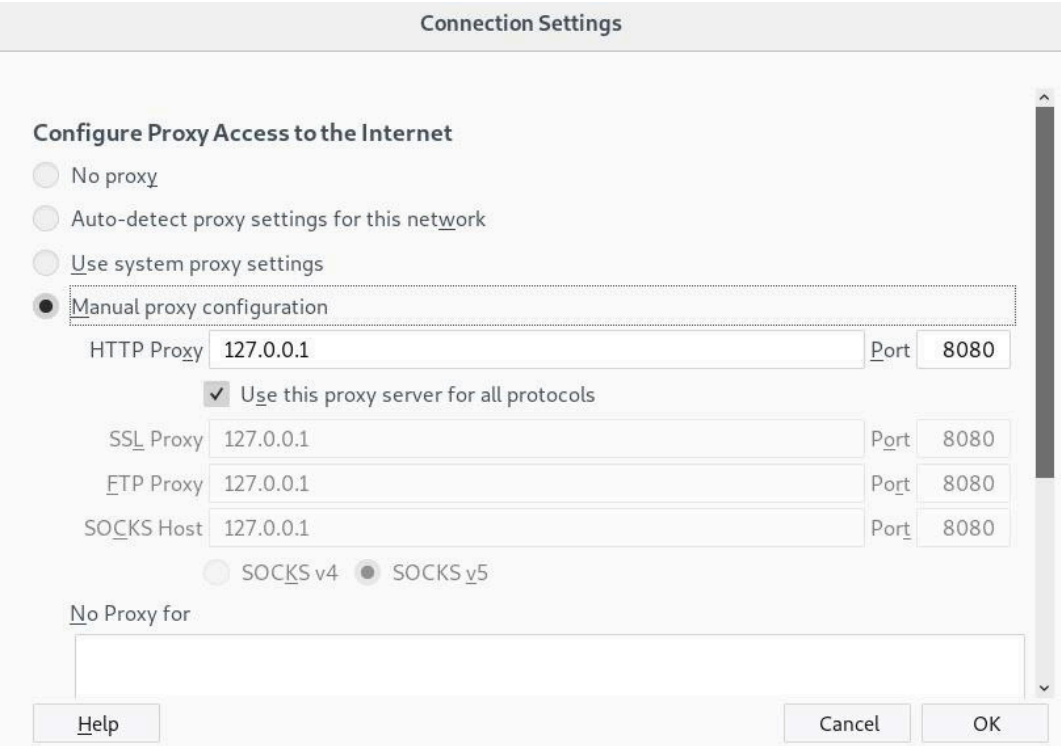
Burp Suite

Pentru testarea securității vom folosi suita Burpsuite care este integrata in Kali Linux (https://tools.kali.org/web-applications/burpsuite). **Burp Suite** este un instrument puternic pentru testarea aplicațiile web pentru vulnerabilități. Burp este folosit ca proxy pentru interceptarea și modificarea cererilor.

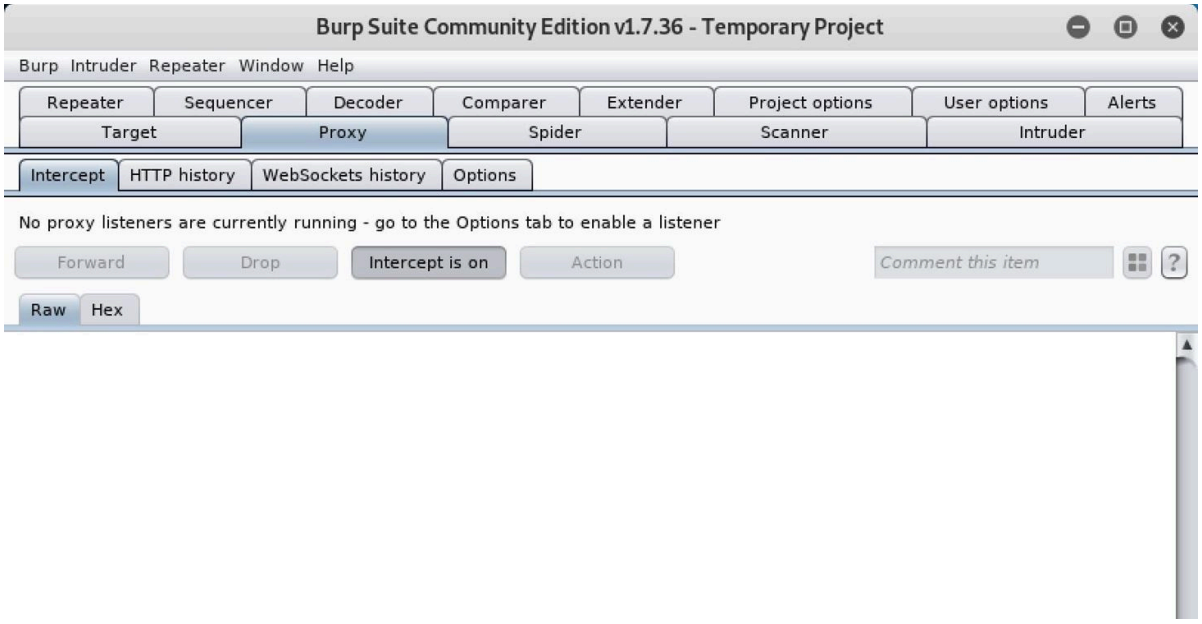


Pentru inceput trebuie să configurați browserul pentru a lucra cu Burp.

În Firefox, accesați "Preferințe" și derulați până la secțiunea intitulată Network Proxy . Setări"→ "Configurare manuală proxy" și introduceți 127.0.0.1 ca *proxy HTTP* și 8080 ca port . Acum, bifați "Utilizați acest server proxy pentru toate protocoalele" și asigurați-vă că este gol în *No Proxy for* .



În cele din urmă, dați clic pe "OK" și totul trebuie configurat corect. Apoi, puteți porni Burp Suite și puteți începe un nou proiect. Navigați la fila "Proxy" și asigurați-vă că este apăsat butonul "***Intercept is on***". Acest lucru ne va permite să modificăm cererea pentru atacurile XSS



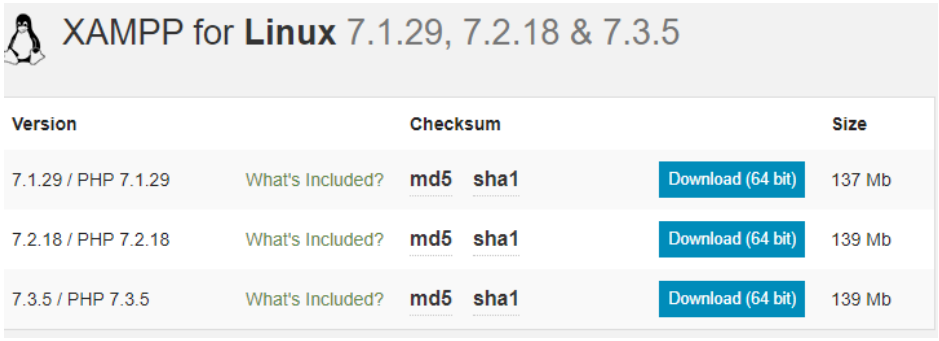
Mutillidae

Ținta atacului trebuie sa fie un site care are vulnerabilitati. **Fuzzing** este o tehnică utilizată pentru a testa aplicațiile defectelor de securitate într-un mod automat. Fuzzerul, un software conceput pentru a testa aceste defecte, oferind date defectuoase sau aleatorii ca intrări în cadrul unui program pentru a găsi erori. Aceste date eronate de obicei conduc la vulnerabilități în contextul securității. Intrările generate pot fi statice, cum ar fi valori încărcate dintr-o listă sau aleatoare, sau date dinamice generate de algoritmi.

Vom folosi drept ținta a atacului ***Mutillidae***, o aplicație web creata sa fie vulnerabilă, pentru a testa atacurile in condiții cunoscute. Instalarea Mutillidae necesita prezenta XAMPP (server web, MySQL, etc.). In aplicațiile reale, vulnerabilitățile unui sistem de operare sau ale unui site trebuie detectate in prealabil.

Instalare Mutillidae Linux

Pentru a instala XAMPP se vizitează https://www.apachefriends.org/download.html si se descarcă versiunea pentru Linux.



In acest caz se descarcă versiunea 7.3.5.

Se da instalerului XAMPP permisiunea de execuție.

sudo chmod +x xampp-linux-x64-7.3.5-0-installer.run

apoi se lanseaza in executie aplicatia

sudo ./xampp-linux-x64-7.3.5-0-installer.run

La întrebările care apar in timpul instalării se va răspunde afirmativ cu Y. Instalarea XAMPP va începe si se va finaliza. In timpul instalării este evidențiat faptul ca LAMPP este instalat in /opt/lampp.

Se va descărca in continuare Mutillidae de pe site-ul de mai jos, după care se va dezarhiva in **/opt/lampp/htdocs** in asa fel incat sa se regaseasca continutul in **/opt/lampp/htdocs/mutillidae**:

https://github.com/webpwnized/mutillidae

In continuare se porneşte XAMPP din folderul /opt/lampp prin executarea comenzii:

./xampp start

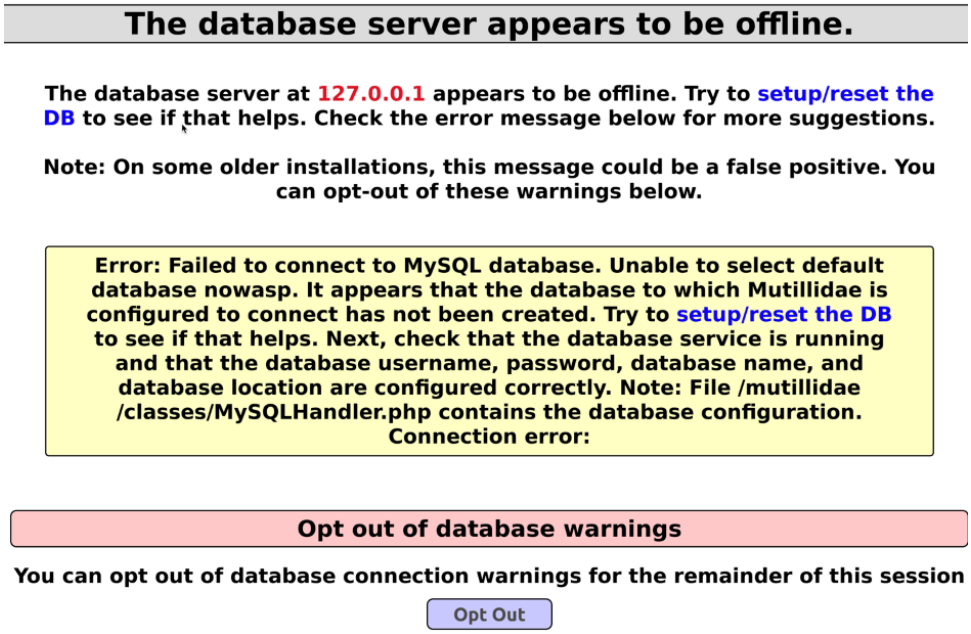
Daca este necesar, panoul control grafic XAMPP este pornit din folderul /opt/lampp cu:

./manager-linbux-x64.run

Se deschide browserul si se verifica faptul ca se paote accesa site-ul la adresa:

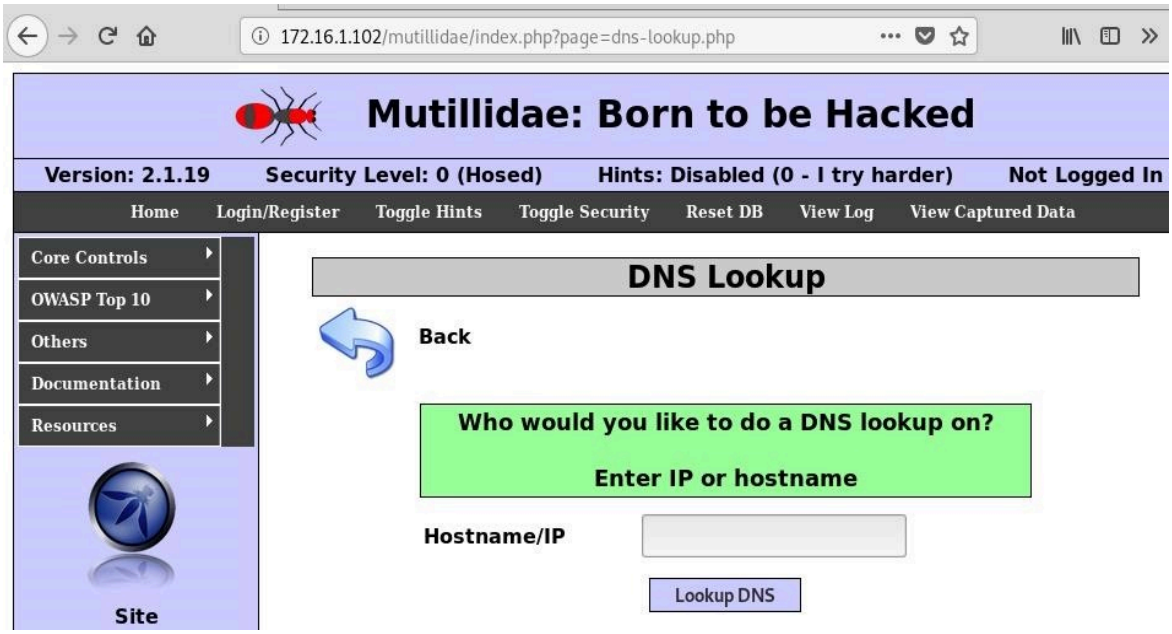
http://127.0.0.1/mutillidae

Site-ul va indica o eroare deoarece nu este configurat.



Pentru configurare se apasa pe link-ul din pagina de **setup/reset DB**. Dupa configurare conexiue la DB, se poate accesa siteul pentru teste.

Pentru a începe, deschideți Mutillidae, iar în stânga navigați la "OWASP Top 10", apoi "Cross Site Scripting", urmat de "Reflected", și în cele din urmă "DNS Lookup". Acesta va fi punctul nostru de intrare pentru XSS fuzzing.

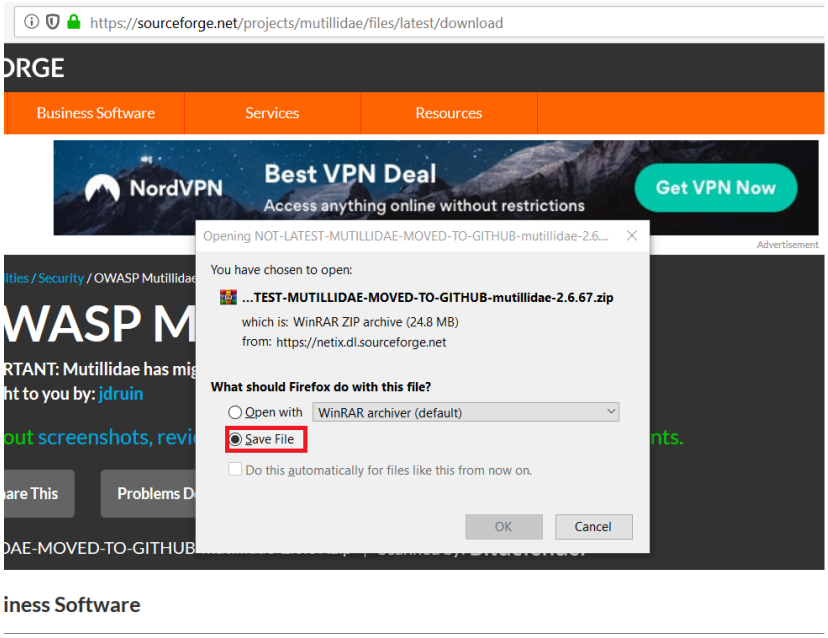


Instalare Mutillidae pe Windows 10 (Oracle VM VirtualBox)

Pasul 1. Se descarcă aplicația Mutillidae accesând link-ul de mai jos , se apasă butonul verde de **Download** si se deschide documentul prin **Save File**.

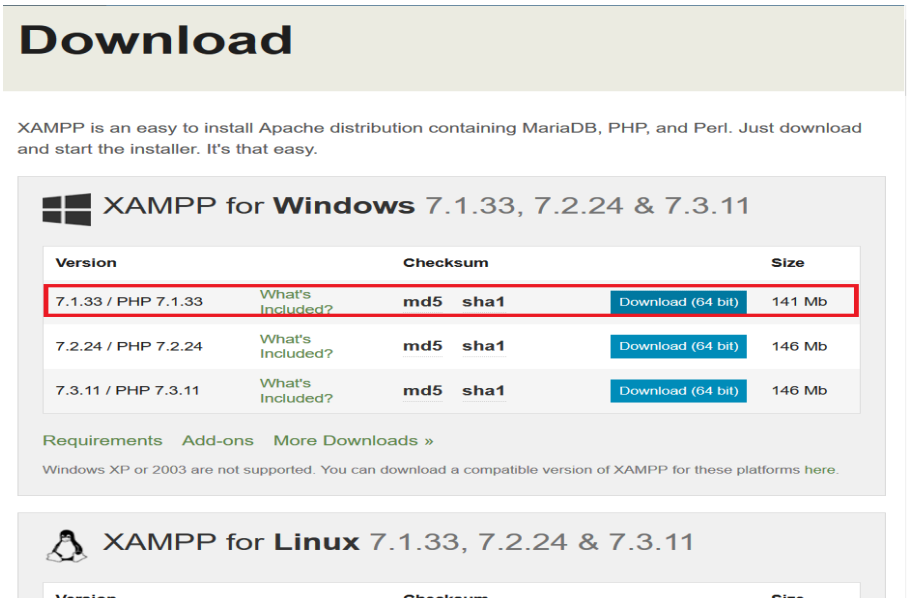
https://sourceforge.net/projects/mutillidae/

Se extrag fișierele din arhiva in același fișier.



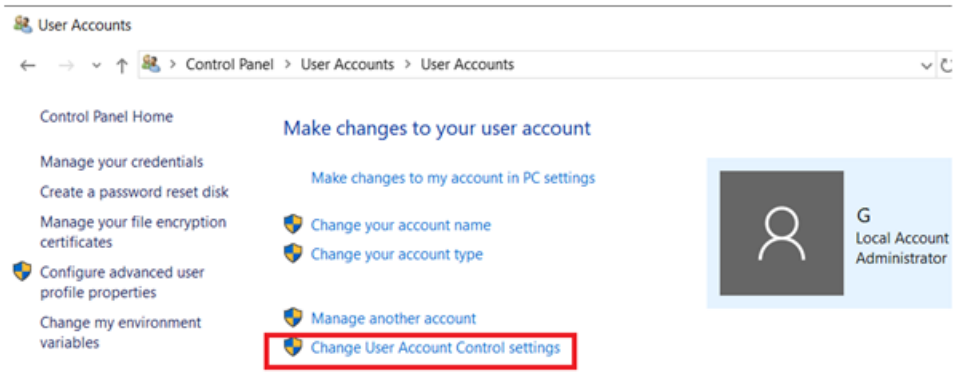
Pasul 2. Se descarcă si se instalează **XAMPP,** alegând ultima versiune din lista , in cazul meu fiind 7.1.33.

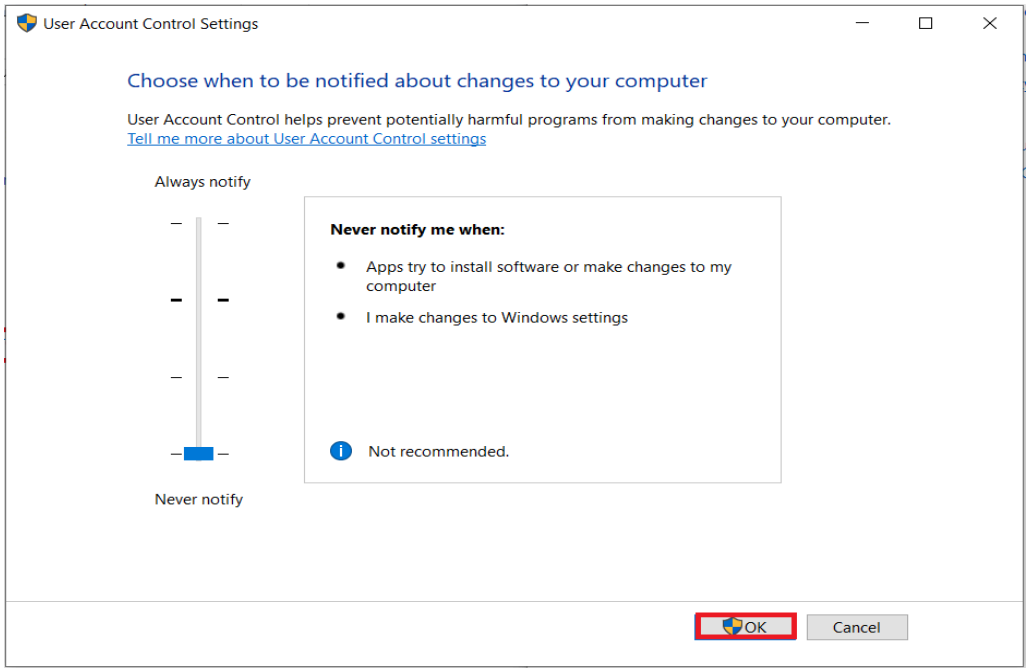
https://www.apachefriends.org/download.html



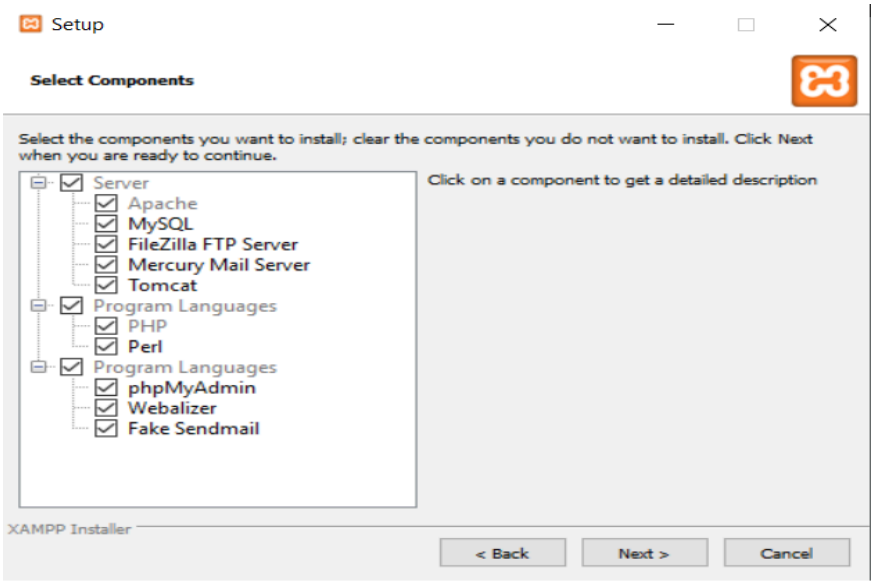
Înainte de a instala XAMPP, se va face o modificare pentru setările Windows User Account Control, astfel: se deschide CONTROL PANEL USER ACCOUNTS CHANGE USER ACCOUNT CONTROL

In noua fereastra este nevoie sa trageți glisorul complet in jos si sa apăsați **OK** pentru a salva modificarea.

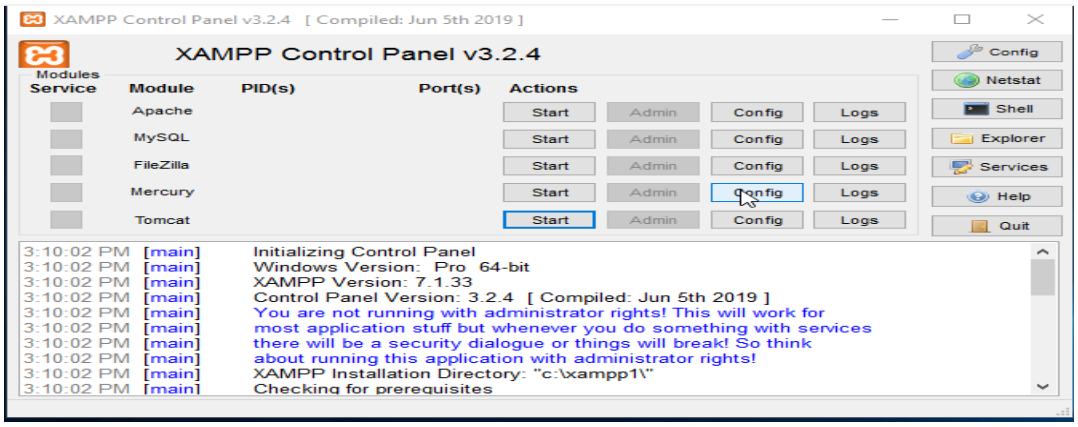


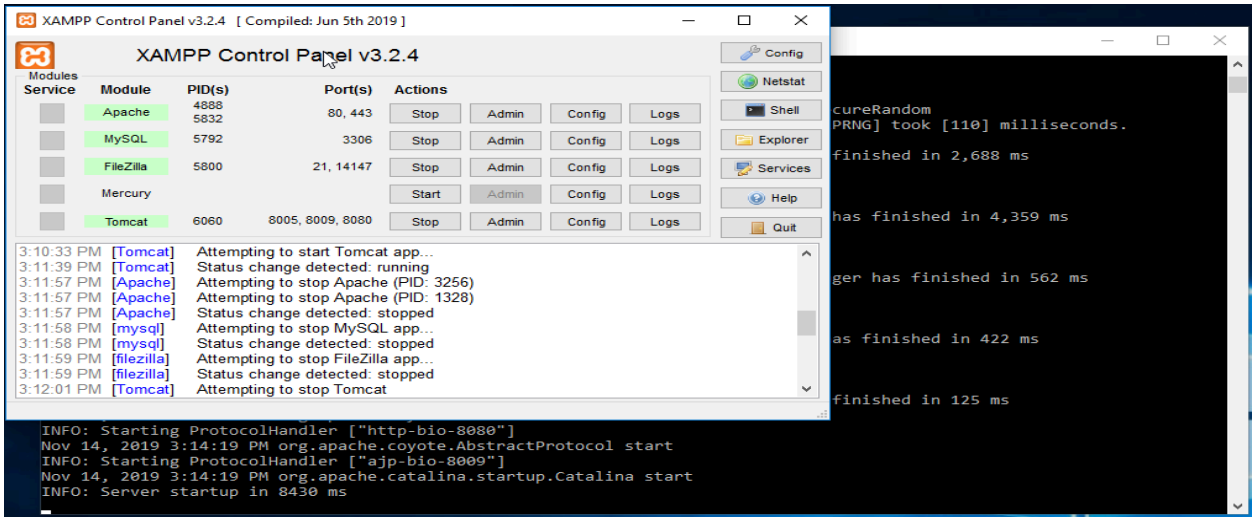


Pentru a instala XAMPP se va executa fișierul descărcat pentru a începe procesul de instalare si pentru prima fereastra se apasă butonul **Next** ca si in următorii pași.



Dupa finalizarea instalarii, se ruleaza **XAMPP CONTROL PANEL** si se apasa butonul de **Start** pentru APACHE, MySQL, FileZilla, Tomcat.





Se copiaza folderul extras Mutillidae in folderul **C:\xamp\htdocs.**

Se deschide un browser si se tasteaza **http://[localhost IP]/mutillidae .**

Pentru configurare se apasa pe link-ul din pagina de **setup/reset DB**. Dupa configurare conexiune la DB, se poate accesa siteul pentru teste.

Warning: mysqli::__construct(): (HY000/1045): Access denied for user 'root'@'localhost' (using password: YES) in **C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php** on line **248**

Warning: mysqli::__construct(): (HY000/1045): Access denied for user 'root'@'localhost' (using password: YES) in **C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php** on line **250**

The database server appears to be offline.

The database server at 127.0.0.1 appears to be offline.

1. Be sure the username and password to MySQL is the same as configured in includes/database-config.inc
2. Be aware that MySQL disables password authentication for root user upon installation or update in some systems. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/database-config.inc
3. Try to **setup/reset the DB** to see if that helps
4. A **video is available** to help reset MySQL root password
5. The commands vary by system and version, but may be something similar to the following
   - mysql -u root
   - use mysql;
   - update user set authentication_string=PASSWORD('mutillidae') where user='root';
   - update user set plugin='mysql_native_password' where user='root';
   - flush privileges;
   - quit;
6. Check the error message below for more hints
7. If you think this message is a false-positive, you can opt-out of these warnings below

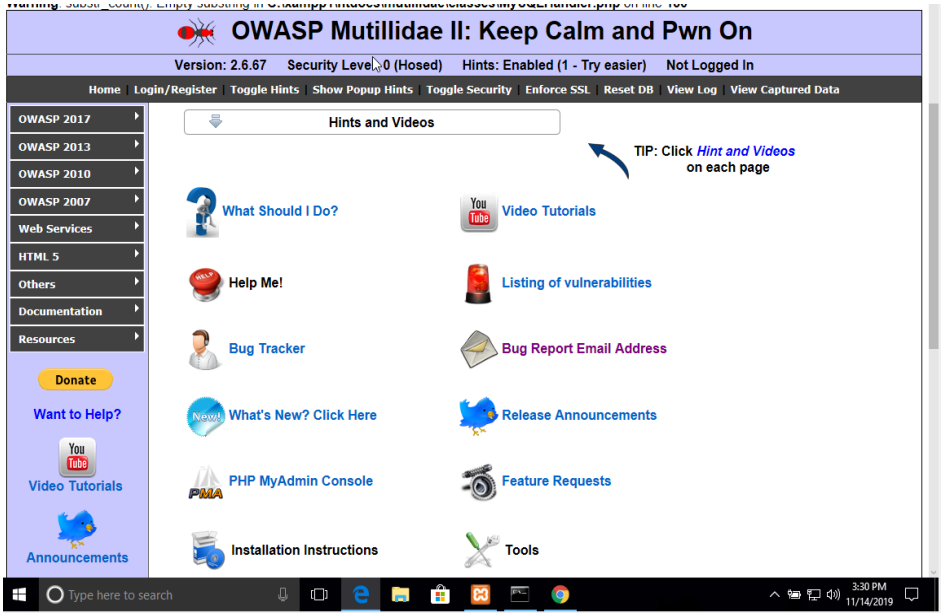
Error Message

Error: Failed to connect to MySQL database. Error connecting to MySQL database First, try to reset the database (ResetDB button on menu). Next, check that the database service is running and that the database username, password, database name, and database location are configured correctly in includes/database-config.php Connection error:

Opt out of database warnings

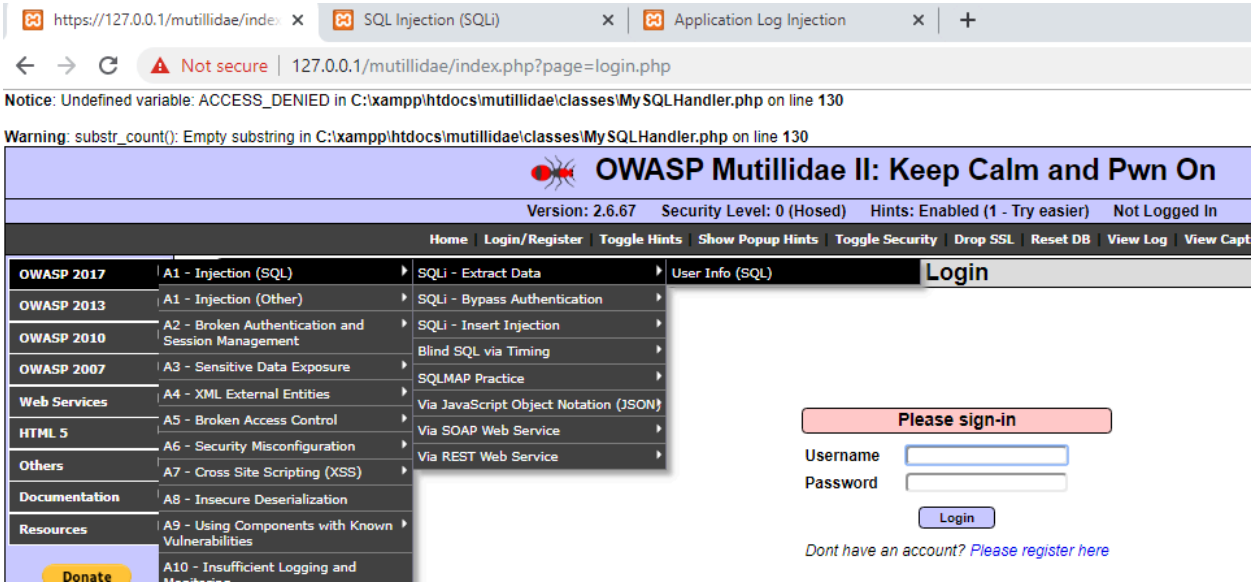
You can opt out of database connection warnings for the remainder of this session

Opt Out



Pentru configurare se apasa pe link-ul din pagina de **setup/reset DB**. Dupa configurare conexiue la DB, se poate accesa siteul pentru teste.

Exemplu atac simplu asupra Mutillidae



Se introduce in campul de username:

```
' or 1=1 --
```

Obs . Atentie la sfarsitul comenzii de mai sus , dupa `--` se adauga un spatiu.

In acest moment loginul se va finalize desi nu a fost introdus nici un nume de utilizator.

Acest lucru se intampla deoarece a fost rulata o comanda SQL de tipul:

select * from Users where Username = ‘valoare din campul username’ and Password=’valoare introdusa la campul parola’

in care ‘valoare din campul username’ a fost introdusa neprocesata (parsing). Rezultatul va fi ca se vor returna datele deoarece testul de parola dupa -- va fi comentat, iar conditia din **where** va fi mereu adevarata datorita testului **1=1**:

select * from Users where Username = ‘`' or 1=1 --` *and Password=’valoare introdusa la campul parola’*

Atacuri care exploateaza vulnerabilitati hardware

Rowhammer

„Rowhammer” se bazeaza pe o problemă cu modulele DRAM recente în care accesarea repetată a unui rând de memorie poate provoca inversarea biților în rândurile adiacente. In acest mod se pot realiza modificari ale datelor in alte procese sau se pot modifica permisiunile unei aplicatii.

O implementare se gaseste aici: https://github.com/google/rowhammer-test

Meltdown si Spectre

Meltdown și Specter exploatează vulnerabilitățile critice ale procesoarelor moderne. Aceste vulnerabilități hardware permit programelor să fure date care sunt procesate în acel moment pe computer. Deși programele nu sunt autorizate să citească date din alte programe, un program dăunător poate exploata Meltdown și Spectre pentru a pune stăpânire pe secretele stocate în memoria altor programe care rulează. Acest lucru poate include parolele stocate într-un manager de parole sau browser, e-mailuri, mesaje instantanee și chiar documente critice pentru afaceri.

Meltdown și Spectre funcționează pe computere personale, dispozitive mobile și în cloud. În funcție de infrastructura furnizorului de cloud, este posibil să furi date de la alți clienți care rulteaza masini virtuale pe acelasi sistem de calcul.

O implementare se gaseste aici: https://github.com/IAIK/meltdown

EternalBlue

Aceasta vulnerabilitate exploateaza implementarea incorecta a protocolului Server Message Block (SMB) utilizat in retelele Windows pentru partajarea de fisiere folosind Network Neighborhood. Aceasta a aparut deoarece unele versiuni de Microsoft Windows manipulează pachete special concepute de la atacatorii de la distanță, permițându-le să execute cod arbitrar pe computerul țintă.

O implementare a unui atac exista in Kali Linux si este documentata aici:

https://null-byte.wonderhowto.com/how-to/manually-exploit-eternalblue-windows-server-using-ms17-010-python-exploit-0195414/