**Homework Assignment #2**

**Mike Pendleton**

**Boralb Mimani**

**West Texas A@M University**

**CIDM-6341 Topics in Cybersecurity SP2022**

**Homework Assignment #2**

**Total Points: 100**

*The purpose of this assignment is to evaluate the ability of identifying the threats posed to information security, the attacks associated with those threats, and assess the used countermeasures. You can work as group/team of MAX FIVE.*

**Q1. [20 points] [ Hints – Ch#4 lecture slides]**

1. What is information security policy and how it is showed in the spheres of security [hints fig 4.1]? List and describe the three guidelines for sound policy, as stated by Bergeron and Bérubé.

Policy is the essential foundation of an effective information security program. In the spheres of security, policy is showed to connect to every layer of the sphere: systems, networks, internet, people, information.

The three guidelines for sound policy are: all policies must contribute to the success of the organization, management must ensure the adequate sharing of responsibility for proper use of information systems, and End users of information systems should be involved in the steps of policy formulation.

1. Describe the bull’s-eye model. What does it say about policy in the InfoSec program?

The bull’s-eye model has four layers:

* 1. Policies: first layer of defense
  2. Networks: threats first met the organization’s network
  3. Systems: computers and manufacturing systems
  4. Applications: all applications systems

Regarding policies the InfoSec program says: Policies are important reference documents for internal audits and for the resolution of legal disputes about management's due diligence [and] policy documents can act as a clear statement of management's intent.

1. List and describe the three types of InfoSec policy as described by NIST SP 800-14.

There are three types of InfoSec policies:

* 1. Program policy
     1. Creates and defines a computer security system
     2. Sets organizational strategic directions
     3. Assign responsibilities to the respective office responsible
     4. Addresses compliance issues regarding meeting requirements to establish the program and specific penalties and disciplinary actions that will be in place
  2. System-specific policy
     1. Focusing and explicitly stating decisions taken by management
     2. Decisions should be made based on technical analysis
     3. Different policies should/will be applied to different systems
     4. Rules should be set regarding whom can use what system and access what data

Issue Specific Policy

1. Should address specific areas relevant to the organization
2. System should be updated frequently
3. It should contain the company’s issue statement.
4. Briefly explain EISP components and ISSP document organization practices with advantages and disadvantages [ Hints: Tables 4.1, 4.4]

There are five components of the EISP:

* 1. Purpose: it identifies the elements of a good security policy, explain the need for information security, specify the different categories of information security, identify the responsibilities and roles, and identify appropriate levels of security through standards and guidelines.
  2. Elements: Defines the whole topic of information security within the organization as well as its critical components.
  3. Need: Justifies the need for an information security program
  4. Roles & Responsibilities: Defines the staffing structure designed to support InfoSec within the organization.
  5. References: Lists other standards that influence and are influenced by this policy document.

There are three ISSP approaches:

1. Individual Policy
   * 1. Advantages: written by individuals with knowledge on the topic and offers clear instructions to the responsible department
     2. Disadvantage: Fails to cover all issues with leads to poor results
2. Comprehensive Policy
   * + 1. Advantages: Well controlled and assures complete topic coverage; provides better procedures
       2. Disadvantages: May be written by individuals with less expertise on the topic leading to an overgeneralization
3. Modular Policy
4. Advantages: Well controlled and assures complete topic coverage, written by individuals with expertise on the matter with clear assignments to the responsible departments
5. Disadvantage: More expensive and more difficult to manage.

**Q2. [20 points] [ Hints – Ch#5 lecture slides]**

* 1. What organizational variables can influence the size and composition of an InfoSec program’s staff? What is the typical size of the security staff in a small organization? [ Example: A medium-sized organization? A large organization? A very large organization?]
* Organizational variables that can influence the size and composition of an InfoSec’s program staff are: organizational culture, size, security personnel budget, and security capital budget.
* Small organization: three members who might be working part time.

Medium organization: four members with at least one member working full-time

Large organization: 17 members with a hierarchy lead by the CISO

Very large organization: 50-65 members with a multilevel hierarchy.

* 1. When developing an awareness program, what priorities should you keep in mind? List the steps in a seven-step methodology for implementing training.

The purpose of an awareness program is to:

* 1. By building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems
  2. By developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely
  3. By improving awareness of the need to protect system resources

The seven steps for implementing training are:

1. Identify program scope, goals, and objectives
2. Identify training staff
3. Identify target audiences
4. Motivate management and employees
5. Administer the program
6. Maintain the program
7. Evaluate the program
   1. Define “project management.” Why is project management of particular interest in the field of InfoSec?

Project management is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Project management is accomplished through the use of processes such as: initiating, planning, executing, controlling, and closing. Project management is of particular interest to InfoSec because of the benefits it brings:

* + Implementing a methodology ensures that no steps are missed
  + Creating a detailed blueprint of project activities provides a common reference tool and makes all project team members more productive by shortening the learning curve when getting projects underway
  + Identifying specific responsibilities for all the involved personnel reduces ambiguity and also reduces confusion
  + Clearly defining project constraints and minimum quality requirements increases the likelihood that the project will stay within them
  + Establishing performance measures and creating project milestones simplifies project monitoring
  + Identifying deviations in quality, time, or budget early on enables early correction of the problems
  1. What are the 10 areas that make up the component processes of project management? How can security be both a project and a process?

The ten areas that make up the component processes are:

1. Communications: assurance that all project participants communicate effectively.
2. Cost: managing the financial resources committed to the project
3. Humans Resources: managing human capital effectively
4. Integration: Defining, organizing, and controlling pieces and anticipated work
5. Procurement: Acquiring resources needed to complete project task
6. Quality: Assuring that the project meets specifications
7. Risk: Minimizing impact of adverse occurrences
8. Scope: Defining what to be included in the work to be done and what not.
9. Stakeholder: Identifying and cultivating relations with those affected by the project and those that can influence it.
10. Time: Manage the resource of elapsed time as well as time spent by resources.

Security can be both a project and a process because of the magnitude of people, resources, planning it requires which makes it a project and the policies, rules, and steps needed to be taken to complete the project which makes it a process.

**Q3. [20 points] [ Hints – Ch#6 lecture slides]**

1. What is risk management? List and describe the key areas of concern for risk management. Why is identification of risks, through a listing of assets and their vulnerabilities, so important to the risk management process?
   * To discover and asses risks to and environments operations and how to determine that the risks can be controlled or mitigated
2. Who is responsible for risk management in an organization? In risk management strategies, why must periodic reviews be a part of the process?
   * This is broken down into roles for Risk Management
     1. InfoSec
     2. IT
     3. General Management and Users.
   * Periodic reviews must be done in order to improve the program and processes. Gap analysis is a part of the review process where we analyze the current outcomes and the ideal outcomes. This can then be done to determine if any changes need to be made and implemented to the current program.
3. What are vulnerabilities? Describe the TVA worksheet. What is it used for?
   * Specific areas that threat agents can exploit in order to attack an asset(s)
   * The TVA worksheet lists assets according to priority along one axis, and the threats dependent upon priority on the other axis.
   * The worksheet is essential in accessing and controlling risk. Thisi s due ot the risk rating/score representing relative risk for specific vulnerabilities of informational assets.
4. Examine the simplest risk formula presented in this chapter. What are its primary elements?
   * Likelihood
   * Impact
   * The formula calculates the likelihood X Impact.

Q4. [ 20 points] Articles and links

1. Article#3\_1 proposes a method of WiFi penetration testing based on Kali Linux which is divided into four stages: preparation, information collection, simulation attack, and reporting. By using the methods of monitoring, scanning, capturing, data analysis, password cracking, fake wireless access point spoofing, and other methods, the WiFi network penetration testing with Kali Linux is processed in the simulation environment. Please write at least five comments on the proposed approach (example -how good/bad their method is in terms of general security policies and CIAs).
   1. Changing the default password is always a must as the default password is easily obtained in product guides and all router vendors tend to choose the same easy password.
   2. Even though mac addresses can be spoofed, it is always a good idea to turn on the mac filter as this would also increase the amount of time for the crack to complete.
   3. I do not agree with “open network and not connected at will”. This is the opposite of how you gain access to the wireless network. New and existing devices will reach out and attempt to connect to the network. That is the design of 802.11 technology.
   4. Long and extensive passwords are a must in order to best protect access to the network
   5. I strongly agree with hardware appliance implementation such as ids with network supervision. This is a way to detect that access to the network is being attempted. Since password cracking does take a long time to complete, the environment would be able to know that there is an attack and then could implement firewall rules to block the inbound traffic coming from the source ip and ports.
2. Briefly explain National Cybersecurity Framework proposed by NIST.

[Hints: <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

The framework proposed was based off of an executive order 13636 in which critical infrastructures would be able to maintain security within the cybersecurity space.

The overview is the Framework Core, Framework Implementation Tiers, and The Framework Profile.

The Framework Core represents the standards, guidelines for allowing communication and the potential outcomes that it would expect as a strategic management for information security risk. Framework Tiers is the risk assessment, implementation and execution against potential threats. The Framework Profile is the alignment of the standards practices and guidelines for risk assessment, which is divided into categories and sub categories in order to address the environments risk.

Q5. [20 points] Lab

1. Install Kali Linux, Ubuntu, and Virtual Box binary with extensions. Share your screenshots. [ hints watch the linked video, Lab0, and/or CISCO instructions. Briefly explain a Linux ACL [hints Fig. 4.6]

Task –1: Download Kali Linux virtual box image

Task – 2: Download Virtual Box

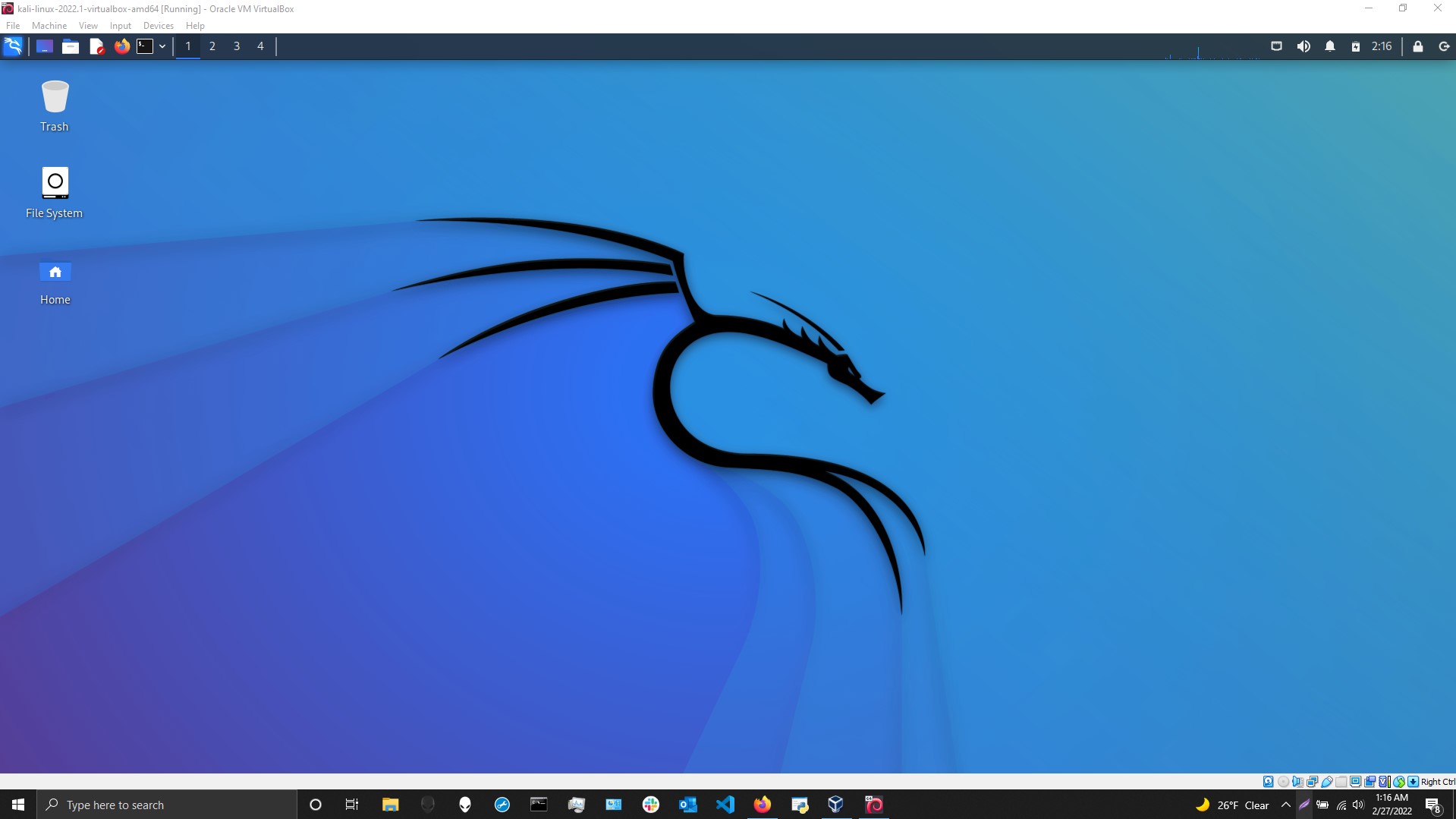
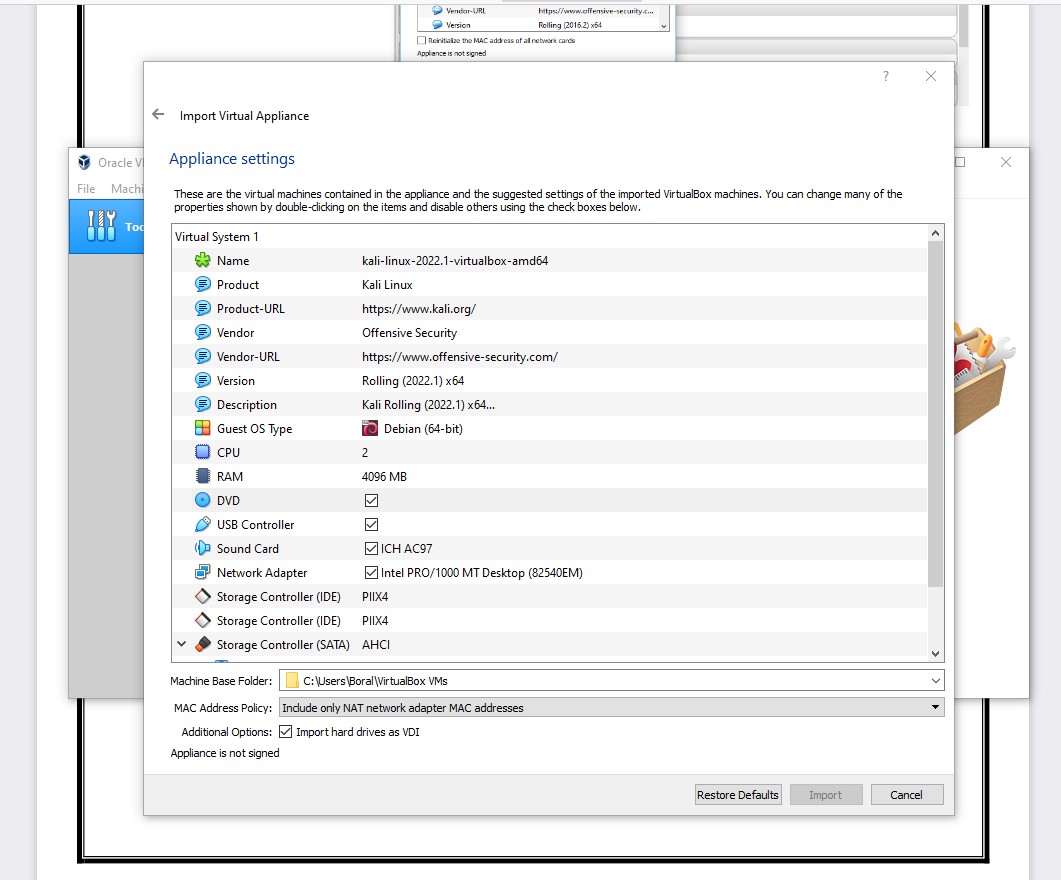
Task – 3: Install Virtual Box

Task – 4: Import Kali Linux virtual image using virtual box

Task – 5: Enabling Virtualization (For windows 8, 8.1 and 10 users)

Task – 6: Download required tools for the labs]

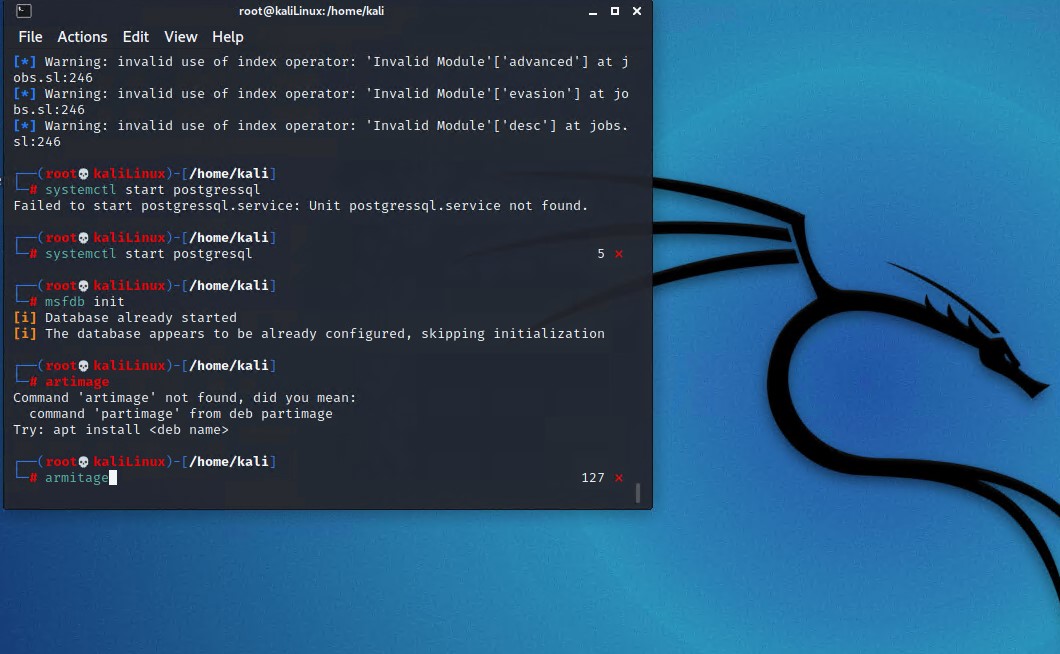
ACLs enable administrations to restrict access according to user, computer, time, duration, or even a particular file by allowing the administrator to apply a more specific set of permissions to a file or directory without (necessarily) changing the base ownership and permissions The common user privileges used are: read, write, execute, and delete.



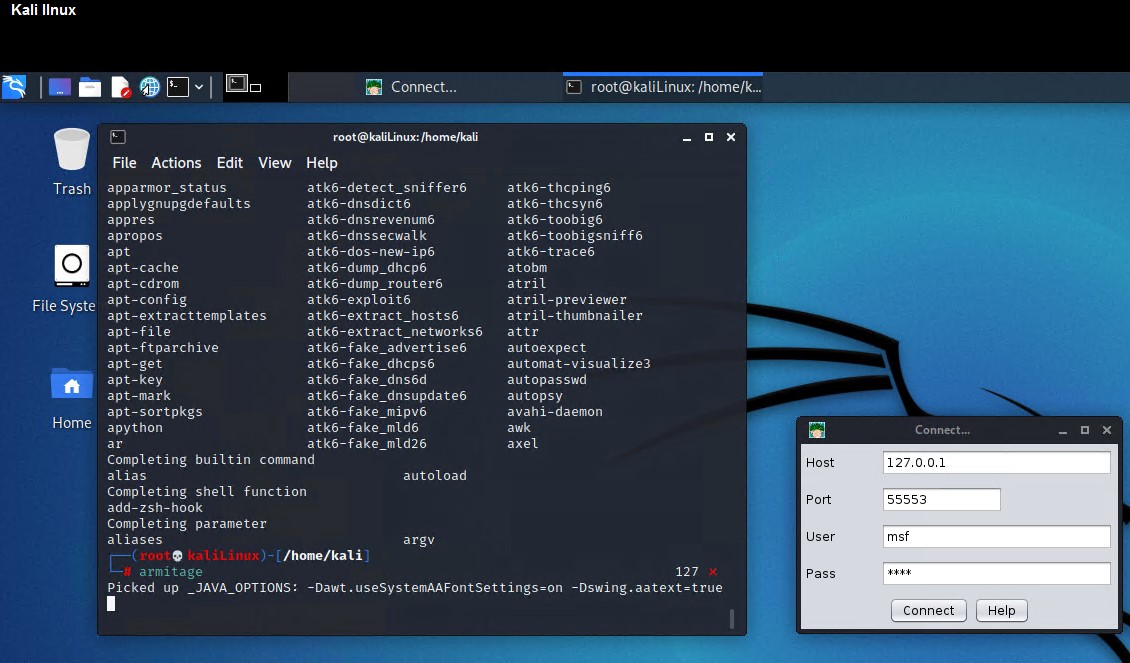
1. What do you mean by Armitage Package? How can we run Armitage on Kali Linux? Why is Armitage not displaying hosts from the Database? How do you secure a server? [ Hints see Lect#6]
   1. Armitage is a postgresql database application that runs scans on hosts. The tool can also find exploits and complete attacks, runs port scans and more. Since this is a database, it can also be used to share with other hackers what exploits they have been successful with on environments with other hackers.
   2. In order to start/run Armitage:
      1. systemctl start postgresql
      2. msfdb init
      3. Armitage
      4. Below are screen shots on how to start Armitage

* 1. Why is there no hosts ?
     1. There are no hosts by default, so you will either add manually if you know them, or search the environment.
  2. How do you secure a server?
     1. Utilize secure protocols like sftp, ssh and not telnet.
     2. Implement secure and encrypted email connections
     3. All browsing traffic should only use https
     4. Connect to the network via vpn
     5. Firewalls should be enabled on all endpoints and all operating systems. This includes clients and servers both virtual and physical.

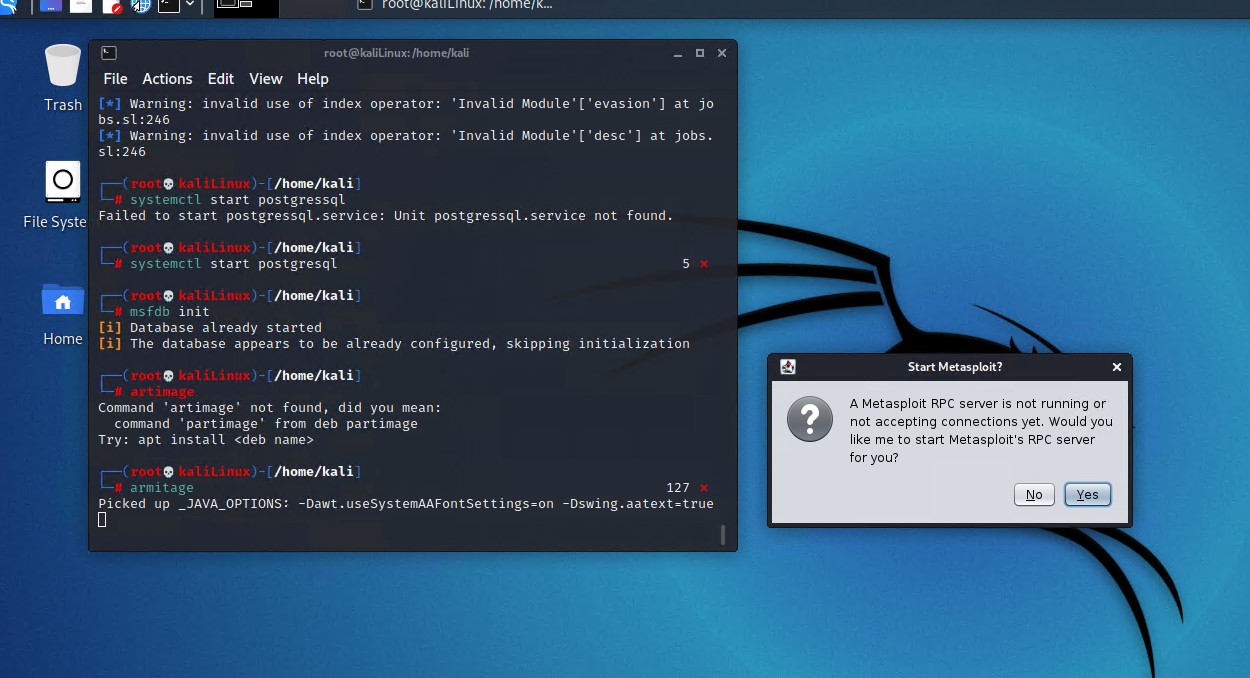
Screen shots on startup:



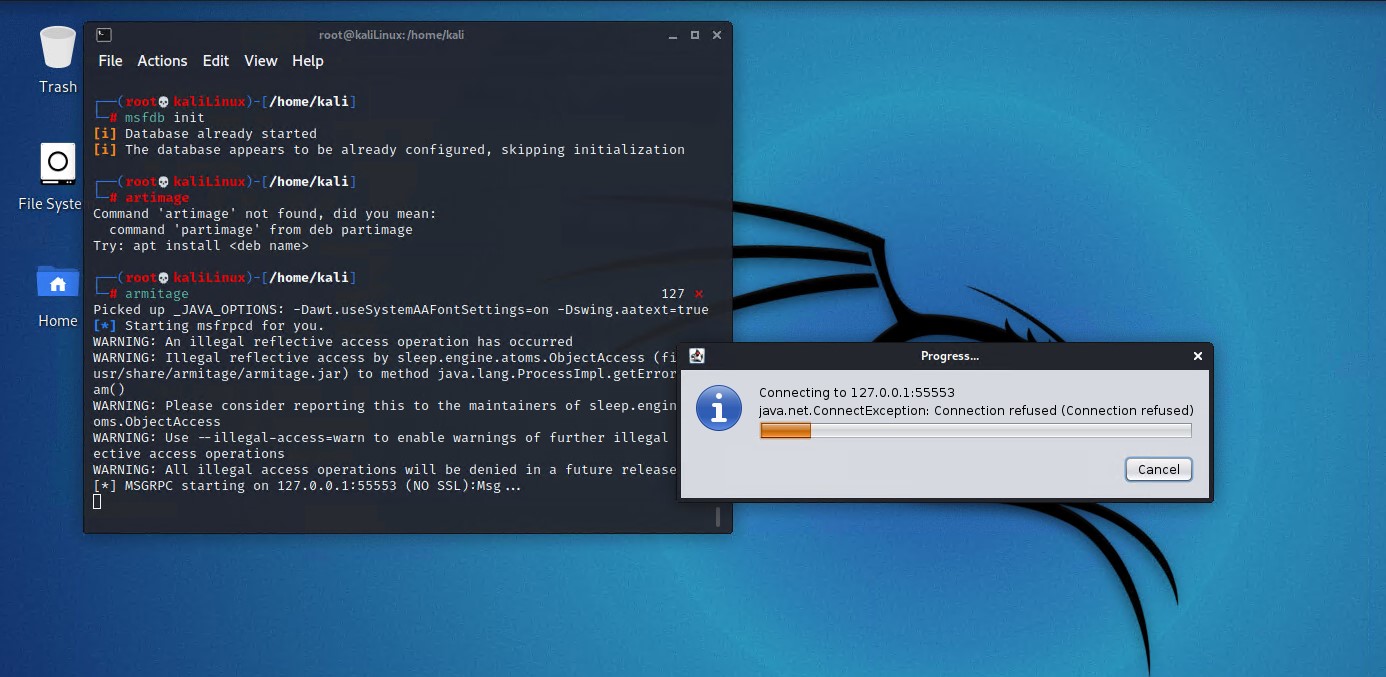
Now we will need to connect to the database, by clicking on connect



We will need to start the rpc server if it is not running by clicking on yes.



This is connecting to the server



Armitage is now up and running and you can start adding hosts.

