12/29/2020

Organization Name: Rills School System

Team Members:

Muhammad Haseeb Ahmad BSE183010

Mohammad Abdul Rafay BSE183009

Muhammad Hamza Tariq BSE183020

Submitted to: Respected Sir Dr. Qamar Mahmood

Dated: 29th December,2020

Link: https://www.youtube.com/watch?v=NHI5qCiHXgY

Contents

Organization Introduction (Rills School System)

Rills school system was found in 1998 by Sir Ahemad, total braches of this org is 350 all across Pakistan and the one we are taking review is in Gujranwala having the student strength of 150+ and employees are more than 200. It's an education Sector teaching the student from grade play group to O-levels.

Questioner

Physical Security

1. Do you have any type of physical security in your organization?
2. If you have any type of physical security, then up to which level is it. If not, then why?
3. Do you have 24/7 guards for your organization?
4. Which type of stake holders are allowed to access the critical nature of data?
5. In how many modes the data is stored in your organization?

Data Security

1. Where the data of your organization is stored?
2. How many data servers do you have?
3. In which form your data is stored?
4. Do your organization fallow any encryption or decryption algorithm?
5. If yes, then which algorithm do you fallow?
6. Do you have and firewall configured in your organization?
7. Which generation firewall is configured in your organization?
8. Do your organization have distributed firewalls?
9. Have your organization faced any type of attack on data?
10. Do you have any type of website/portal where you post the data?
11. Do you perform any type of filtering on data?
12. After how many time your organization discard the data and artifacts?
13. In which form your organization discard the artifacts?

14. Up to which rank of person in your organization is allowed to view, edit and delete the confidential data?
15. Have you installed or configured any type of antivirus software's in the systems of your organization?
16. Do your organization hired people for the data to be secured?

Communicational Security

1. How data is communicated in your organization?
2. Do you fallow any encryption algorithm when data is communicated?
3. If no encryption algorithm is fallowed, then in which form data is communicated?
4. Do your organization check or test the flaws when occur in medium?
5. After how much time your organization test the security medium?

Operational Security

1. How data is communicated in your organization?
2. Do you fallow any encryption algorithm when data is communicated?
3. If no encryption algorithm is fallowed, then in which form data is communicated?
4. Do your organization check or test the flaws when occur in medium?
5. After how much time your organization test the security medium?

Answers from the organization

Physical Security

1. Do you have any type of physical security in your organization?

   Yes, we have guards.

2. If you have any type of physical security, then up to which level is it. If not, then why?

   Medium level security

3. Do you have 24/7 guards for your organization?

   Yes, 2 guards.

4. Which type of stake holders are allowed to access the critical nature of data?

   No stake holders are allowed to access the data of the nature

5. In how many modes the data is stored in your organization?

   Hard disk and cloud server

Data Security

1. Where the data of your organization is stored?

   Laptop and internet and pc

2. How many data servers do you have?

   3 data servers which are interlinked together

3. In which form your data is stored?

   Only in soft copies form

4. Do your organization fallow any encryption or decryption algorithm?

   No but I have my own software developer who does it

5. If yes, then which algorithm do you fallow?

   No but I do follow aes n des

6. Do you have and firewall configured in your organization?

   yes

7. Which generation firewall is configured in your organization?

   Network firewalls

8. Do your organization have distributed firewalls?

   No single firewalls

9. Have your organization faced any type of attack on data?

   No

10. Do you have any type of website/portal where you post the data?

    Yes rills.edu.pk

11. Do you perform any type of filtering on data?

    yes

12. After how many time your organization discard the data and artifacts?

    8 years

13. In which form your organization discard the artifacts?

Print in hard copies and remove it from the servers

14. Up to which rank of person in your organization is allowed to view, edit and delete the confidential data?

    Only Director are allowed

15. Have you installed or configured any type of antivirus software's in the systems of your organization?

    Yes, and avast 2018 version

16. Do your organization hired people for the data to be secured?

    no

Communicational Security

1. How data is communicated in your organization?

   Via email and via phone

2. Do you fallow any encryption algorithm when data is communicated?

   No

3. If no encryption algorithm is fallowed, then in which form data is communicated?

   Like excels sheets and etc.

4. Do your organization check or test the flaws when occur in medium?

   yes

5. After how much time your organization test the security medium?

   After every month

Operational Security

1. How data is communicated in your organization?

Via email and via phone

2. Do you fallow any encryption algorithm when data is communicated?

   no

3. If no encryption algorithm is fallowed, then in which form data is communicated?

   Like excels sheets and etc.

4. Do your organization check or test the flaws when occur in medium?

   yes

5. After how much time your organization test the security medium?

   After every month

Reviews of our team

Physical Security

Overall a good physical security is provided in your organization. To increase more security, the organization should fallow the given:

1. You have 24/7 guards and number of guards will be more than 5 that covers all the area of the schools the area includes data server rooms, main blocks, examination hall, Registration areas etc.
2. As you have mentioned in the Questioners above that your data is stored in a hard disk and on cloud server. In our point of view, you should have a data server room where all the information of all the staff and students are stored and is further more equipped with the 24/7 guards and number of guards will be 2 at that point.
3. You should follow the good lock system on the door i.e., biometric lock system, figure print scanner's or a particular type of cards are provided only to those stake holders who are allowed to visit that data server room. If anyone misuses the data in any form only those persons are suing able in this regard.
4. The system's inside the data server room should be provided with the lock system so that everyone is not allowed to access the system and furthermore the hard disks should be equipped with the passwords and that password should be in encrypted form.
5. By applying all these physical security, we have achieved the maximum security in the organization.
6. As security cannot be achieved 100 percent I would be maximum secured over our ends.

Data Security

Data security is one of the major assets of the organization. If it's misused the whole business of the organization could be winded up. Following are the reviews about your data security:

1. As you have only three data servers by concluding all your answers of data security section and by concluding some other answer's we get to the point that some of the data of your branches are stored on the system and on laptops.
2. As you have mentioned in the answer 3 of data security that your data is stored in the soft copies in the branches of your school in difference sections of Pakistan.

3. In our point of view, it's not as much secured because it's quite expensive for the organization to secure each and every system where the data is secured in the organization.
4. As you have only one firewall it's also much dangerous for the confidentially of the data of your organization and it can easily be breached.
5. In our point of view as the solution for the data security of your organization first of all you should have distributed firewalls in your organization.
6. In all the branches of your organization you should have the data section where all the data is stored and should be stored in the encrypted with best algorithms that can never be breached.
7. Only higher hierarchy of the branch should be allowed to access, edit and modify the data with the consent and keeping in view of the directors of the organization.
8. Your organization should have some dummy data servers if anyone is successful in launching the attack on your data server so the only access the dummy data and your organization should take the action against the attacker.
9. Your organization should discard the data by burning it so that no one can further use that information and credentials of your organization.
10. Your organization should try to update the latest versions of the antiviruses by time to time.
11. Your organization should hire the expert people for the security of your data because employees are the assets of every organization.
12. As you have one major data server and two distinct data servers if our view your organization should have more than one major data server because if one is breached the data should be kept secure in other data servers.
13. Multiple firewalls should be configured
14. Proper expert team should be in your organization who manages the website and the credentials of your organization.

Communicational Security

Communicational security is one of the major asset of the organization. If any attacker is advanced in breaching it will be very harmful for the organization. It's possible that attacker may change the data and if the attacker is able to or other perspective is that attacker start creating his

own view's about data after reading the data. By concluding the answers of communicational security we get to point to given the reviews. Our reviews are as following:

1. Overall the communicational security is weak, because this organization don't use any encryption algorithm while communicating with the different departments or within the organization.
2. But if they communication uses the applications like WhatsApp, Gmail and etc. they are end to end encrypted so in that case their communication will be safe in such a way that no of their organization information will be leaked and there will be less amount of packet sniffing and packet spoofing.
3. It is good that they perform the security test on the saved data to check whether the data is being leaked or not to ensure that the data is safe and secure.
4. Although the data is stored in the hard drive and google cloud.

Operational Security

After Testing and Examine the Faculty has showed us a lot of problem with the operational Security of the Faculty but there is also the possibility to improve the system and secure the data of the organization as well. The review of the system is given bellow:

1. The operational Security of the faculty is okay but too great, the reason behind is that the encryption of text is just too simple and can be easily decrypted as a result a huge loss of data and money to the organization.
2. The transfer of data is not secure, the whole flow of data is out dated and can be improved. Most importantly the mailing system is not secured, most of the mail is done Gmail or Hotmail or outlook, which is not secure and can be easily be hacked as a result all of the data or documents can be lost. There is no proper network in the organization that can encrypt and decrypt the email or document which are sent within the organization.
3. The storing of information or data is not sufficient and it's not a good way to store huge amount of data. First of all, of the data is recording on hard copy them it is transferred on Microsoft Excel (Soft copy) and the all of the file are stored on the Cloud Storage such as Google Drive or One Drive or Drop Box or Mega Drive. After 8 to 10 years the data is

again download and stored as hard copy which is not suitable for this time and data can be destroyed.

4. The data which is stored on Excel sheet are encrypted using simple encryption algorithm but the issue is that excel sheets can be easily decrypted, so there is a room for improving the algorithm to protect the data.
5. The information of each department is enclosed so no other department have access the information about the other department, only the head of the department can access the data on cloud or in the network.

Website

Link: rills.edu.pk

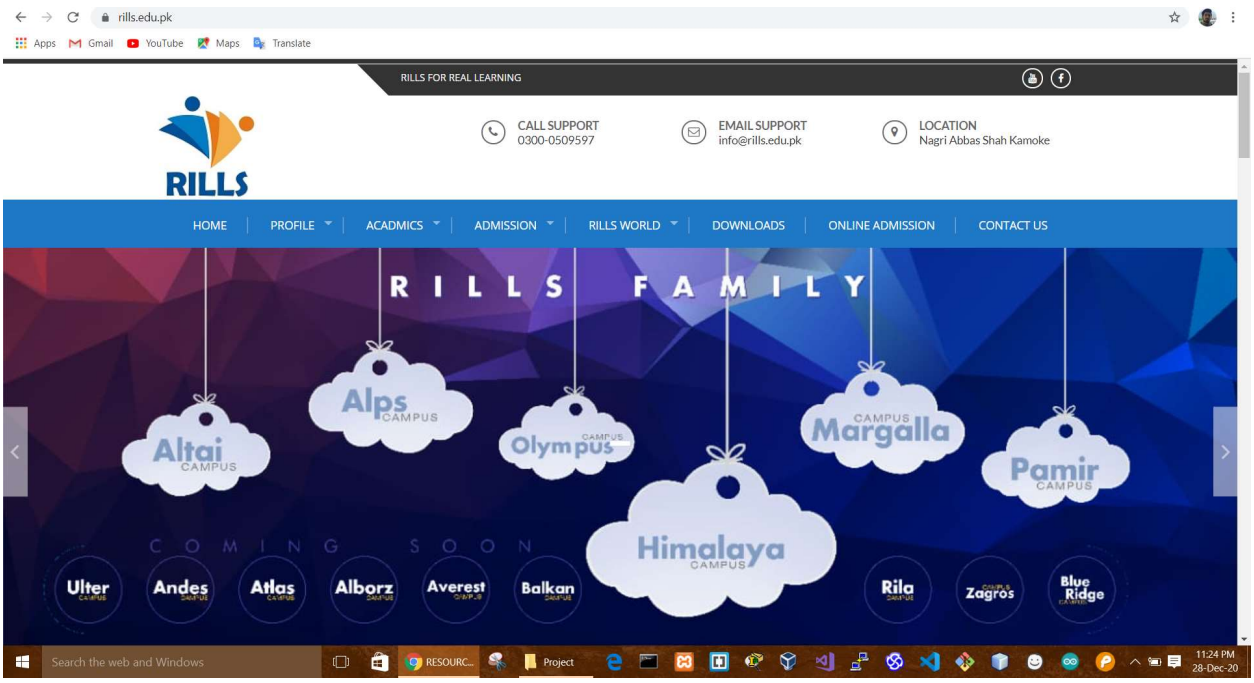

Figure 1Screenshot of website (rills.edu.pk)

Dummy or prototype flow diagram of network

Given below is the dummy flow diagram that for the organization to transmit the data over several branches is Pakistan. So that the data will be securely transmitted. The organization will achieve maximum security. So that the data should be confidential and integrity of data will never be compromised.

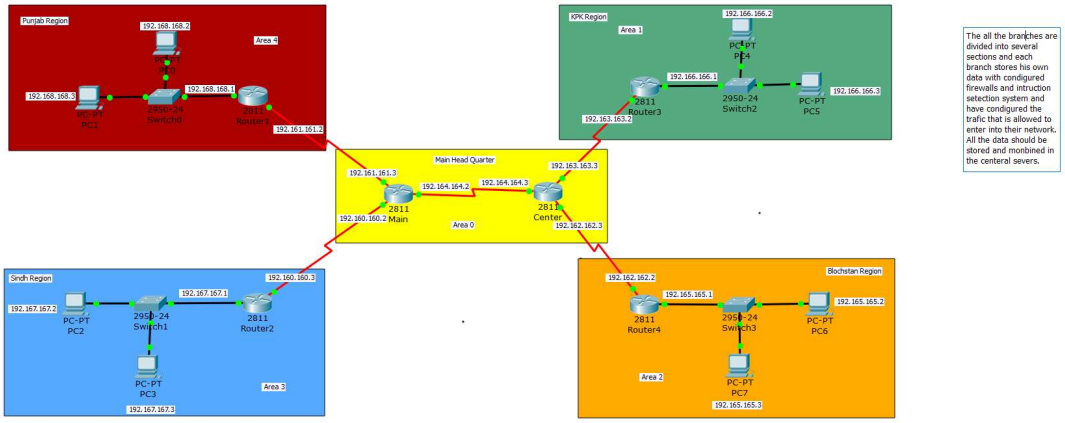

Figure 2Prototype Design

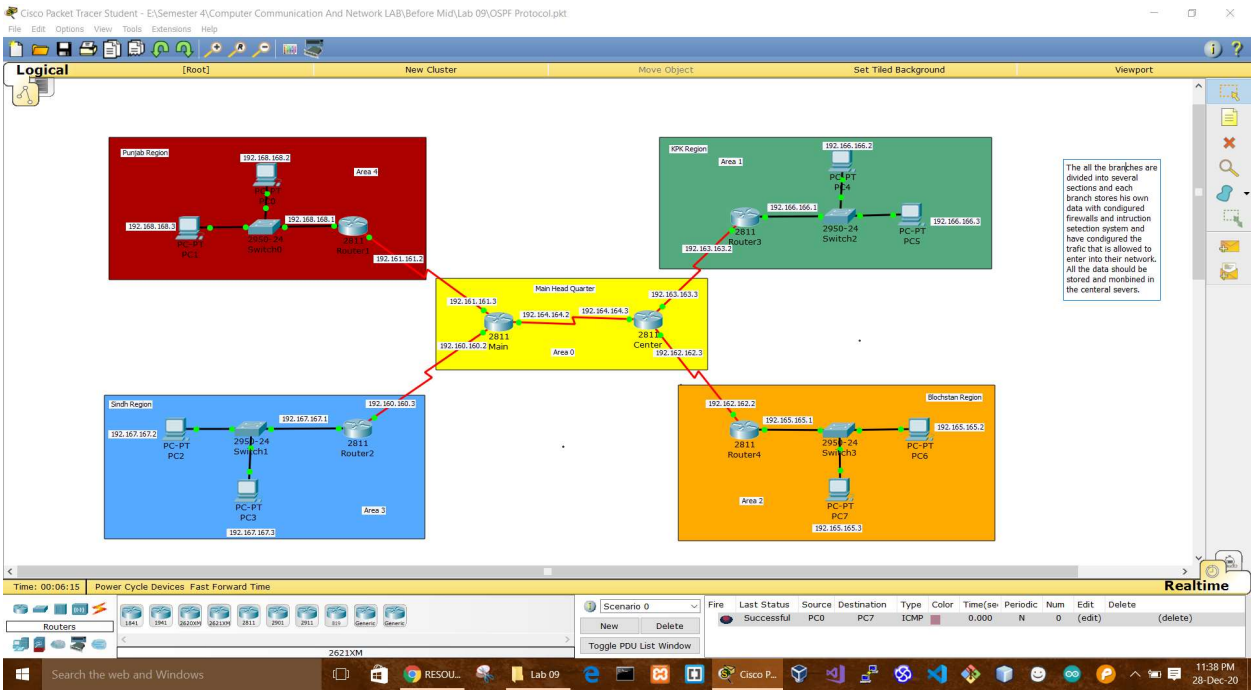

Figure 3Tools screenshot

Wireshark Tool Screenshots

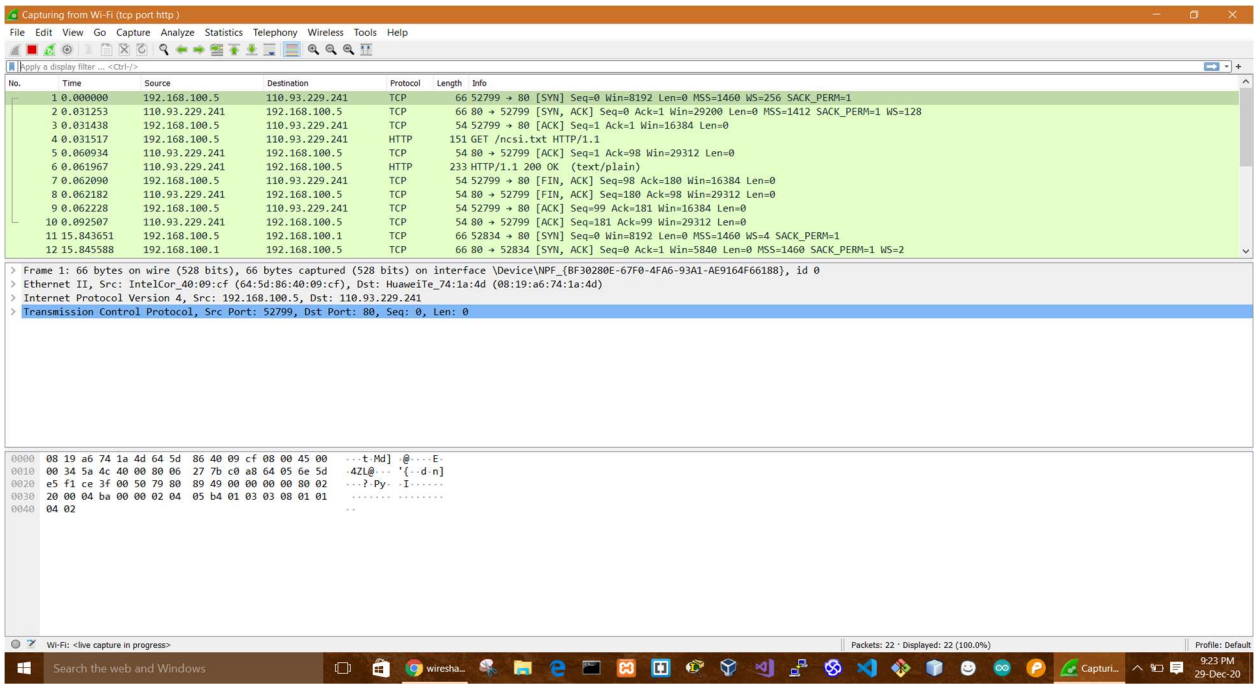

Figure 4Wireshark Tool Screenshot

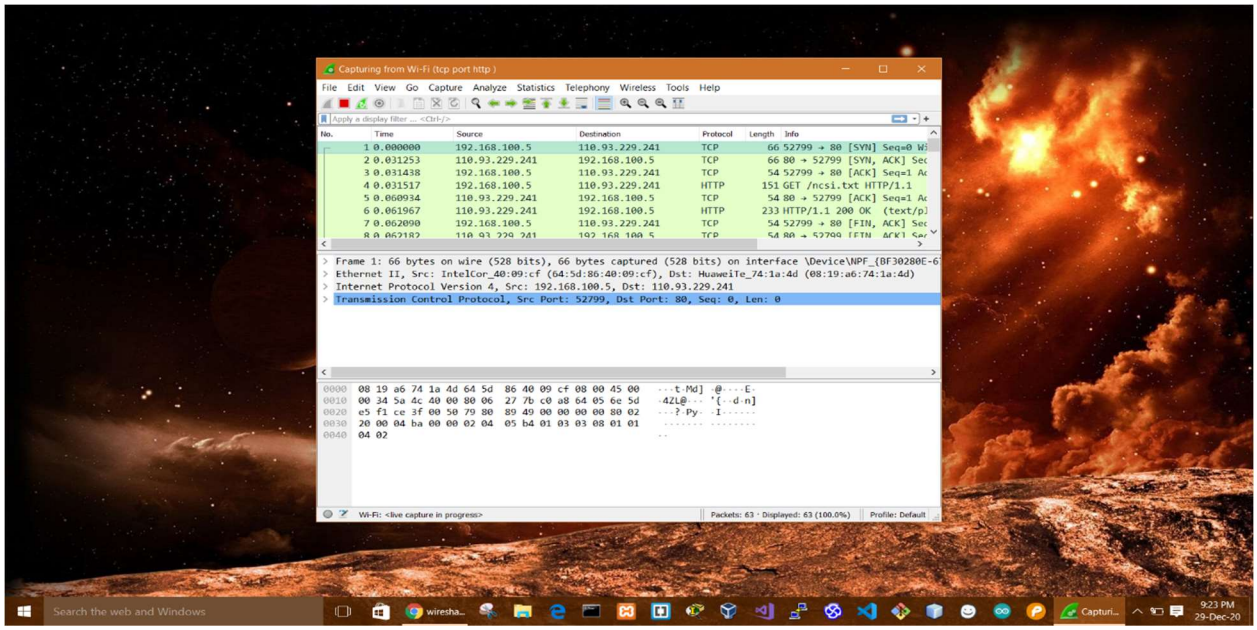

Figure 5Wireshark Tool Screenshot

Kali Linux Screenshots

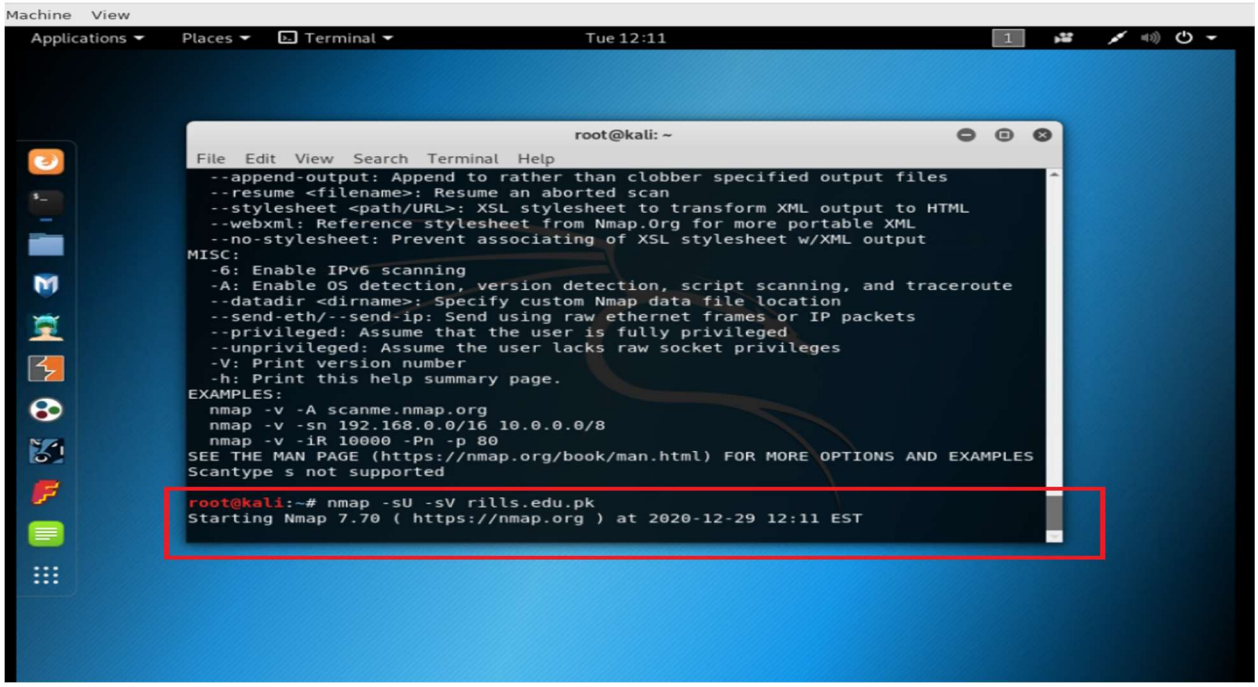

Figure 6Kali Linux Tool Screenshots

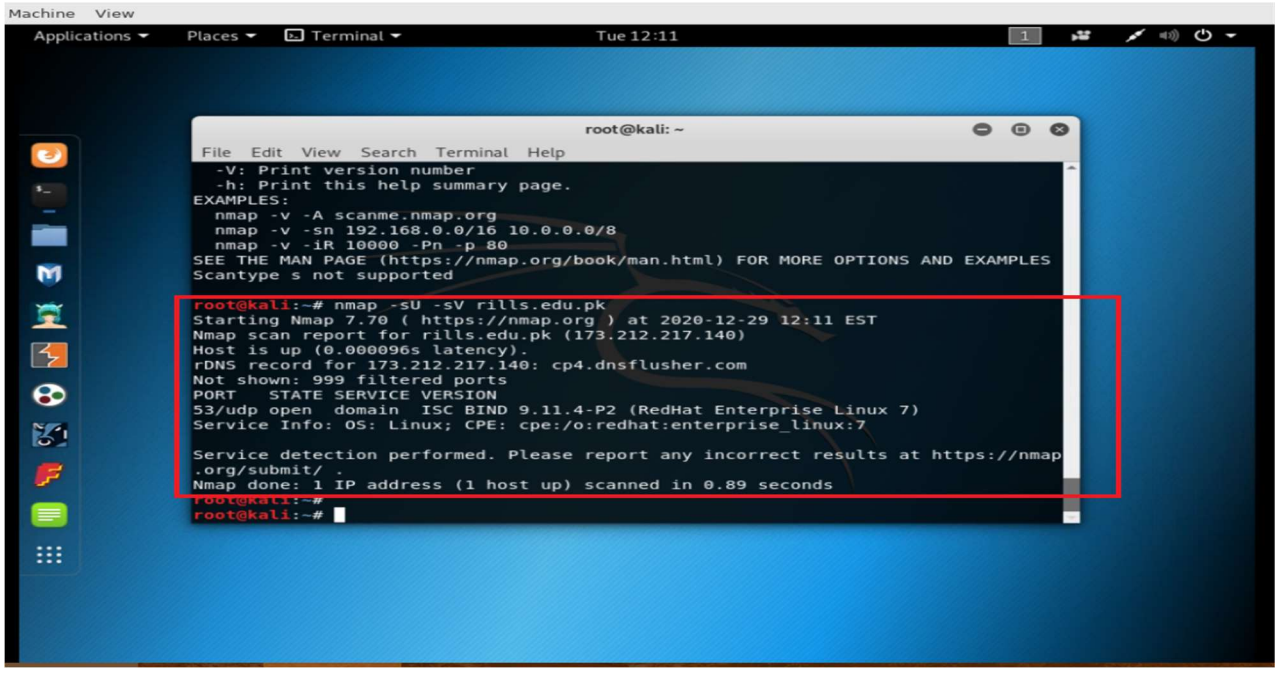

Figure 7Kali Linux Tool Screenshots