Critical Infrastructure for Electronic Information Security and Cyber Defence

Syed Maaz[1*], Garima Sinha[2]

Abstract

This article examined to aware people about cyber security and increase its infrastructure. Here we are attacking a metasploitable-2 machine using kali Linux as attacker machine. Here we are using method of black hat hacker like how they attack in 5 steps like reconnaissance, scanning, gaining access, maintaining access, clearing tracks. First gather as much as information about target this is the first step in hacking also known as reconnaissance where hacker gather all the details about victim or target machine from social media or website name/IP address or using some important hacking tools then scan for open ports and services it's using, after getting all these things we will exploit it using msfconsole in Linux terminal in third step of hacking then next is to maintain access to that victim device until the work is over after it remove all tracks such that no one can catch. We already have so many papers and articles that tell us we have to secure our networks, systems, websites and personal data. Even in some papers we will get a lot of information on networks, internet connected devices (IOT), security architecture, security infrastructure and so on. But in this paper we are going to see a real time Cyber Attack with step by step by knowing this it would be easy for us to secure ourselves in future. Results show that it is really easy to attack if we don't spread awareness about cyber security among people and we must have to improve its infrastructure

Key Words: Cyber Security infrastructure, CSIRM team and risk reduction, Ethical Hacking, Kali Linux, Metasploit, Network infrastructure in cyber security, SCADA system.

DOI Number: 10.14704/nq.2022.20.6.NQ22417 **NeuroQuantology 2022; 20(6):4232-4238**

1. Introduction

First, we will see what is cyber security? Cyber mean online or involving computer networks, and security means securing these computer networks from black hat hackers. As in computer network we used to send data from one PC to another, what if someone will see data while transferring or change data or replace data, even we used to store data in computers, what if someone steal that data, so securing these computers and computer network is one of the main tasks nowadays in this evolving online life. So, this is the meaning of cyber security infrastructure practice of reducing risk such that we are protecting our data, system, hardware, software, and information from people with malicious intent (black hat hacker). In first section we will see the cyber security infrastructure in India where in this section we are discussing about those people who put all their life and money to do something new such that to create their own app, website or to become entrepreneur. What if their app, website or system get hacked they have nothing left to do and in India as it is a developing country if we don't aware about these Cyber Crimes to these people we lose them and it will effect in our developing nation in next section we will see about SCADA systems. Where in nowadays IOT became common and we need good security infrastructure to protect all these connected devices. Then we will see about Network Infrastructure In cyber security. In this section we will see real time example attack how a black hat hacker use Nmap to scan target network and found all the details about the target which Operating System it is using, which service it is running and what ports are open after it we will exploit target using Metasploit as shown in Figure. 7 and get into the System by demonstrating this we are making awareness about Cyber Attacks.

Corresponding author: Syed Maaz
Address: [1]Department of Computer science Engineering (Cyber Security), SET, Jain Deemed to be University, Bangalore, India, [2]Associate Professor, Department of Computer science Engineering , SET, Jain Deemed to be University, Bangalore, India
E-mail: syedmaaz9987@gmail.com[1], mailatgarima@yahoo.co.in[2]

2. Cyber security infrastructure in India

As India is a developing Country we are becoming better every time. So many inventions have been happening. There are so many people who are trying to become entrepreneur. Some are creating their own websites and own apps. So, they are putting their everything in it, money, time, life. What if their website is hacked what if their application is hacked what if their system is hacked. They will lose everything, and it will definitely affect our country growth. Anyway, these risk-taking people are already less if they also get attached and they loss everything we found no one for our country's growth. So, creating a good cyber security infrastructure is necessary today. [1][2]

While protecting data and information we have to put in mind that new vulnerabilities may arise failures may happen and unexpected threats may cause loss in data and information. So, the main thing is we have to update our software every time according to the situation and have to aware this to people. First of all, we have to know how attackers attack systems. They use hacking tools to gain all the information about the target, after getting information, they exploit the system or they may destroy information or change the information. So to protect from these we must have to know all the modern hacking techniques and tools that a black hat hacker may use. Attacks may also happen using Trojan horse in public switched network. Such that if attacker unable to attack main server or main machine, he will attack the new worker or fresher who have access to that website or server, from that attacker goes on to the middle and attack main server, so it's our duty to create awareness about cyber security essentials. Other steps we can follow to improve our security is by seeing developed countries. How their infrastructure is, how they secure their systems, how they treat if any attack has happened and how they recover. [3][4]

3. SCADA systems in cyber security

Now in this section we will see about SCADA systems. These are the systems which directly interact with devices such as sensors, motors, pumps, values and more HMI software. In this modern era where IOT became so important the need of SCADA systems also increased, because of this security in SCADA is really important. If things are connected to internet they will have an IP address if they have IP then hacking and controlling that device is too easy. This will give us new security challenges. To prevent these attacks we have to work on these kind of attacks which can happen on SCADA and find ways that can prevent these attacks. [5]

4. Network infrastructure in cyber security

Network infrastructure for cyber security applications and protocols are the ones which connect trillions of devices worldwide. They may be having so many vulnerabilities if we discover them we will find many, if a hacker with malicious intent in his mind finds any vulnerability he will destroy the app or network or service fully. [6][7]

To know how they do we will see a short example of it. There are 5 main steps in hacking

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks [8]

Now we will see a simple example how hackers hack a system and gain access.Here we are using kali Linux as attacking machine and Metasploit as target Now we use command called netdiscover to see the IP of different networks that we can attack see Figure. 1. In Figure. 2. we can see all the networks which have been discovered by netdiscover command. There are still so many tools in kali Linux from which a hacker can easily get all the information of target [9]

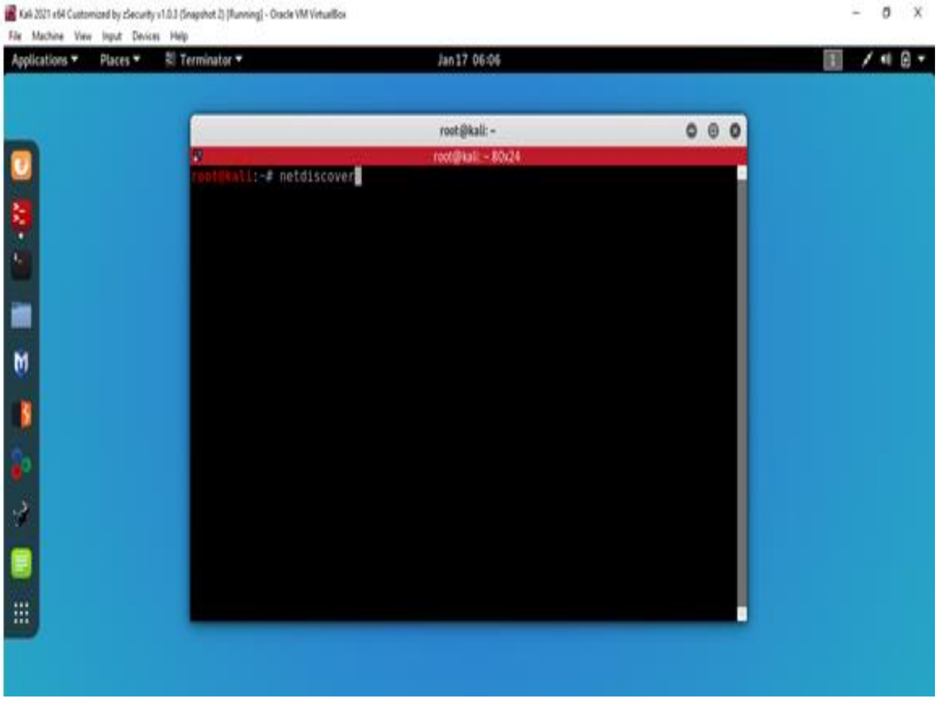

Figure 1. Net discover command

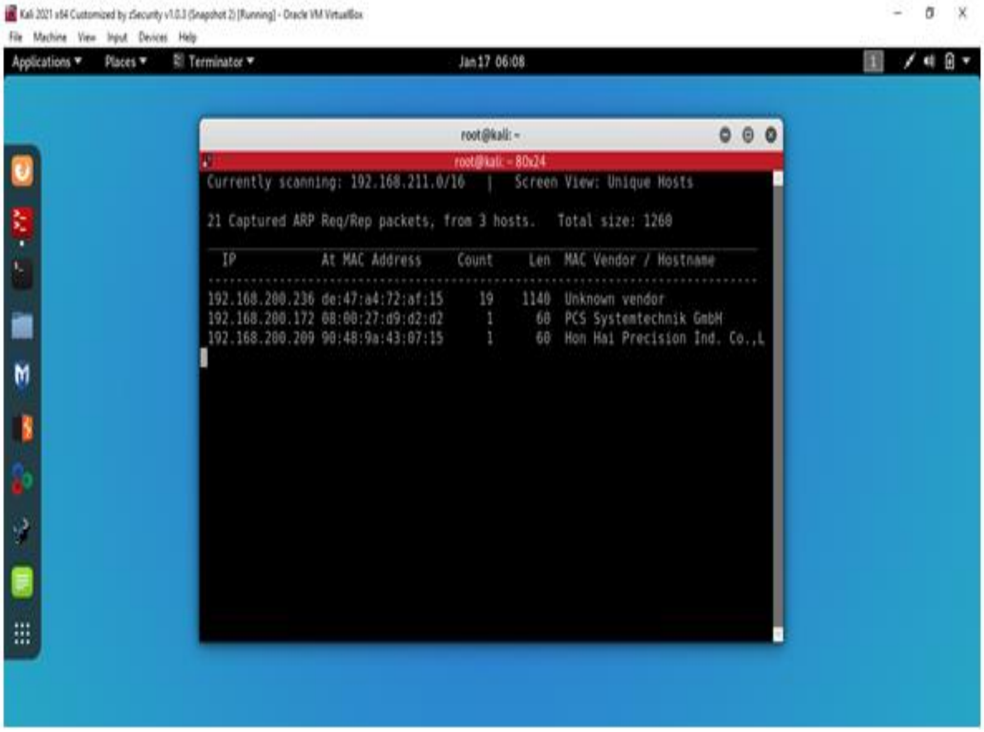

Figure 2. Net discover output

Next step is to see all the open ports and services which the target is running. we can easily find this by using Nmap in command prompt or its GUI Zenmap which is shown is Figure. 3. and Figure. 4. See in figure we are getting all the information of target through its IP. Like services its running and open ports, closed ports and even the host Operating System information [10][11]

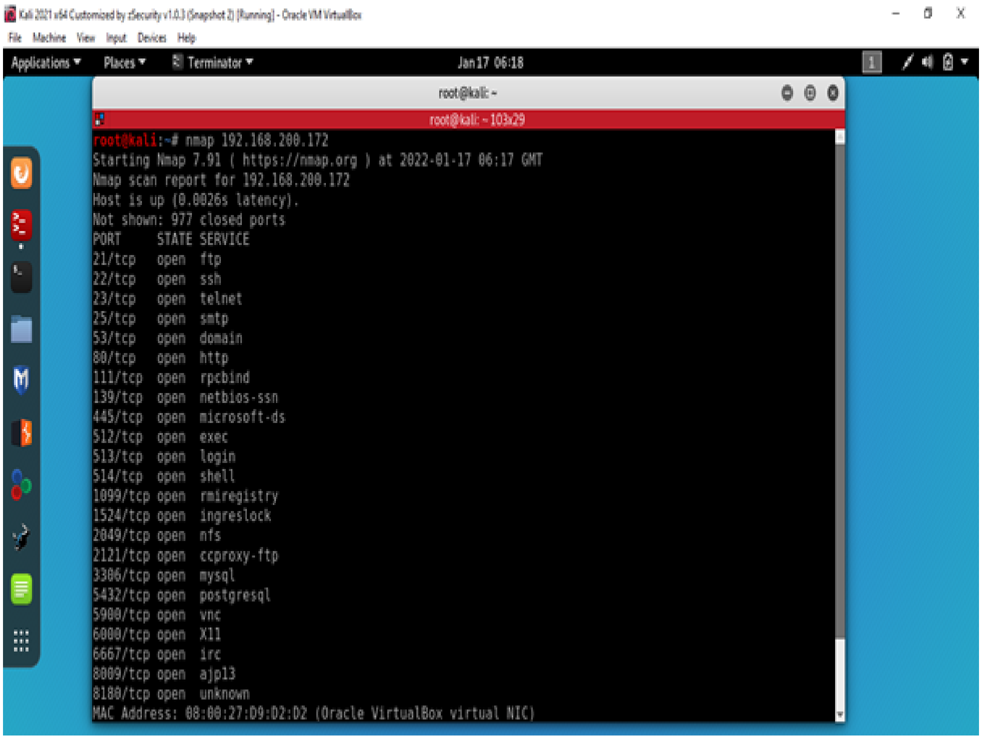

Figure 3. Nmap command

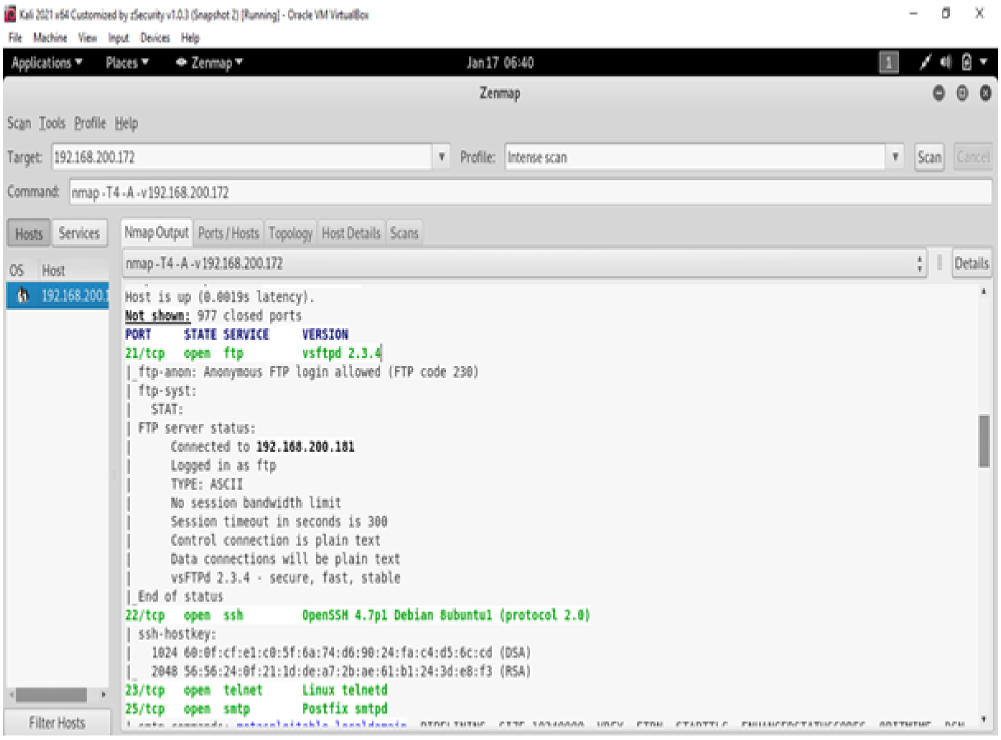

Figure 4. Zenmap command

Next step is after getting its info we will exploit it using attacker machine, here we are using kali Linux as attacker machine. To exploit it we are using msfconsole as shown in Figure. 5.[12]

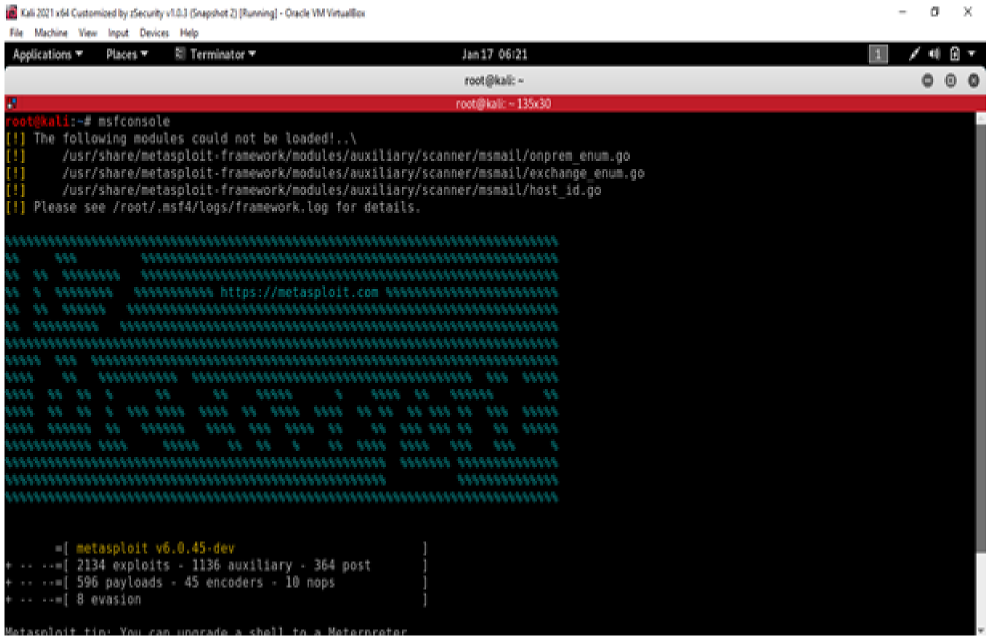

Figure 5. Msfconsole

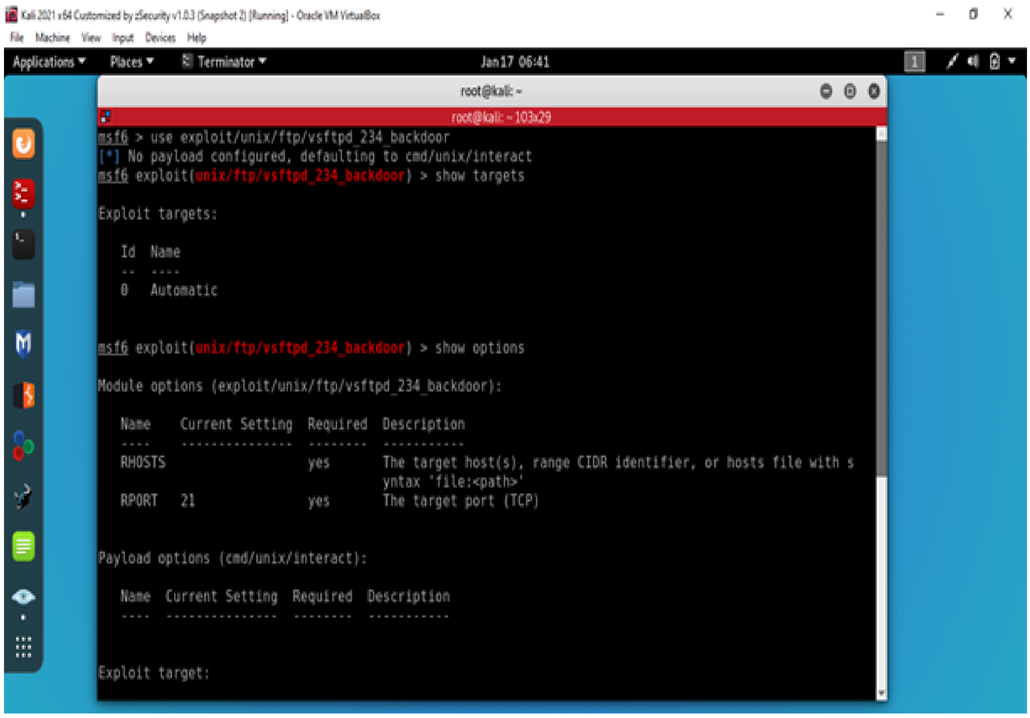

Figure 6. Setting options

After running msfconsole use exploit/unix/ftp/vsftpd_234_backdoor then as shown in Figure. 6. we will set options such that we will set the port number to the running port number and we will set the rhost to the target machine then we run exploit commands shown in Figure. 7. as we can see in Figure. 7. session 1 is opened means we attacked the target. In Figure. 8. we are running all the shell commands like it's our own machine [13]

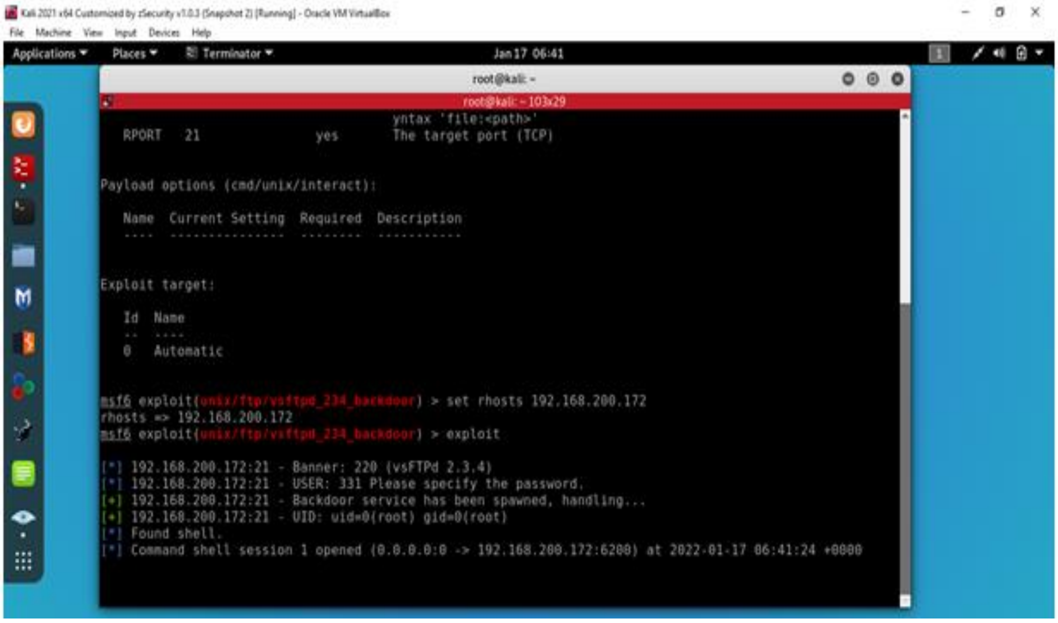

Figure 7. Exploit

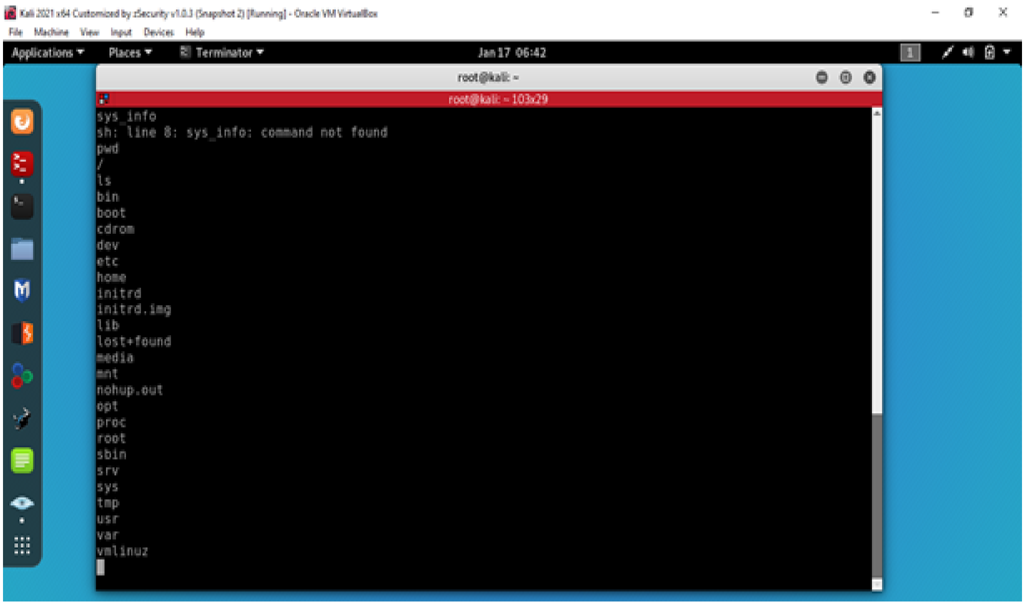

Figure 8. Into the victim machine

5. Cyber security information sharing and risk reduction

Now in this section we will see what to do if the attack has happened. Remember whatever we do attack will happen as there are trillions of devices in the internet if by mistake we forgot to close a port or while updating if hacker finds any vulnerability he will exploit it. And if that happens what to do how to stop them and how to recover the lost files at this time we need a CSIRM team.[14]

To deal with this we will be having a CSIRM team. These are the professionals who knows incidents, threats, vulnerabilities, mitigation, situational awareness. Here what they do is they see the situation and take steps. They see the symptoms and get that what type of attack has happened how can we recover files how can we catch the attacker. [15]

6. Conclusion

We just saw how fast everything is becoming online and security is really important for this it will play a very important role in development of our country. Even we have to spread awareness about cyber security basics among people who are working in large companies that have high market value and even among people who are linked to internet our simple awareness can save a life or a company.

Reference

Chaturvedi1M. M. C., Gupta1 M., and J. Bhattacharya, "Cyber Security Infrastructure in India: A Study." Department of Management Studies, Indian Institute of Technology Delhi, Hauz Khas, New Delhi 110016, India, pp. 70-82, 2008.

Patrascu, Alecsandru. (2012). Cyber security evaluation of critical infrastructures system. In book: Autonomous hybrid vehicles. Intelligent transport systems and automotive technologies (pp.73-91)

Progress and Research in Cybersecurity: Supporting A Resilient and Trustworthy System for The Uk Issued: July 2016 Des3800 Isbn: 978-1-78252-215-7

Reddy, G. Nikhita, and G. J. Reddy. "A study of cyber security challenges and its emerging trends on latest technologies." arXiv preprint arXiv:1402.1842 (2014).

L. A. Maglaras, "Cyber security of critical infrastructures." ICT Express, vol. 4, no. 1, pp. 42-45, 2018, doi: 10.1016/j.icte.2018.02.001.

L. G. Nikolov and V. O. Slavyanov, "NETWORK INFRASTRUCTURE FOR CYBERSECURITY ANALYSIS." Proceedings of International Scientific Conference "Defense Technologies", pp. 191-195.

M. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech, pp. 1-10, Aug. 2018.

A. Gupta and A. Anand, "Ethical Hacking and Hacking Attacks." International Journal Of Engineering And Computer Science, vol. 6, no. 4, pp. 21042-21050, Apr. 2017, doi: 10.18535/ijecs/v6i4.42.

K. Chowdappa, P. Kumar C, and S. Lakshmi, "Ethical Hacking Techniques with Penetration Testing." K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 3389-3393, 2014.

"Nmap: the Network Mapper - Free Security Scanner." nmap.org. https://nmap.org/ (accessed: Dec. 22, 2021).

"Nmap - TryHackMe." tryhackme. https://tryhackme.com/room/furthernmap (accessed: Dec. 26, 2021).

Z. Sabhi. "zSecurity – Ethical Hacking Courses, Tutorials, News, Products and .." zsecurity. https://zsecurity.org/ (accessed: Jan. 11, 2022).

"VSFTPD v2.3.4 Backdoor Command Execution." www.rapid7.com. https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/ (accessed: Jan. 06, 2022).

Goodwin, Cristin, et al. "A framework for cybersecurity information sharing and risk reduction." Microsoft (2015).

Scarfone, Karen, Tim Grance, and Kelly Masone. "Computer security incident handling guide." NIST Special Publication, VOL. 800, No 61, pp.38, 2008