INTERNSHIP REPORT

A report submitted in partial fulfillment of the requirements for the Award of Degree of

BACHELOR OF ENGINEERING
IN
ELECTRONICS AND COMMUNICATION ENGINEERING

by

SIDDHARTHAN R
312418106143

INSTITUTE : AICL

(Duration: 22nd February2021 to 12th March,2021)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
St. JOSEPH'S INSTITUTE OF TECHNOLOGY
OMR, CHENNAI - 600 119

2018-22

AICL
Learning Simplified

TO WHOM IT MAY CONCERN

This is to certify that Mr/Ms SIDDHARTHAN R (312418106143) a student of ST.JOSEPH'S INSTITUTE OF TECHNOLOGY (ECE THIRD YEAR) has successfully completed 15 days (From 22nd February 2021 to 12th March 2021) CYBER SECURITY INTERNSHIP PROGRAM at AICL, CHENNAI.

During the period of his/her internship program with us he/she was found, punctual, hardworking and inquisitive.

We wish his/her every success in life.

Ref: 202103-AICL-CYB6-10035

Date: 19-03-2021

Vice President - Training, AICL

3rd Floor, EA Chambers (Express Avenue) No 49 & 50 L, Whites Road, Royapettah,
Chennai 600014, Tamil Nadu, India.
Ph: 91 95979 40880 Mail: support@aicl.training
URL: www.aicl.training

ACKNOWLEDGEMENT

At the outset, I would like to express my sincere gratitude to our beloved ***Chairman Dr .B. BABUMANOHARAN, M.A., M.B.A., Ph.D.,*** for his constant guidance and support.

I would like to express my sincere thanks to our respected ***Managing Director, Mrs. S.JESSIE PRIYA, M.Com,*** and ***Director, Mr. B.SASHISEKAR, M.Sc.,*** *f*or their kind encouragement and blessings.

I express my sincere gratitude and wholehearted thanks to our Principal ***Dr. P. RAVICHANDRAN, M. Tech., Ph.D.,*** for his encouragement to make this In-Plant Training/Internship a successful one.

I wish to express our truthful thanks and gratitude to our Head of the Department ***Dr. C. GNANA KOUSALYA, M.E., Ph.D.,*** Department of Electronics and Communication Engineering for her constructive criticism throughout my internship.

I have no words to express my heartfelt thanks to ***Ms. R. MONIKA, Scientist, CSIR-CENTRAL ELECTROCHEMICAL RESEARCH INSTITUTE (CSIR-CECRI), KARAIKUDI*** for her guidance, support and encouragement in completing the internship within the stipulated time.

(SIDDHARTHAN R)

ABSTRACT

AICL : We love to inspire and guide you through any subject, develop new skills or upgrade your educational background.**The World is Changing, and** so are Expectations! **of Global Jobs.**

As a student, we must be:

• Aware of rapidly-evolving job profiles

• Tuned in to technology advancements

• Knowledgeable about subject matter that counts

Every student, who has been through the AICL course, can testify to our commitment to their professional growth. Why hear it from us when you can hear it straight from them!

In-plant training includes:

\ **CYBER SECURITY**

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

TABLE OF CONTENTS

OBJECTIVES:

- To learn the principle and applications of CYBER SECURITY
- To learn about the long range and short range technologies
- To understand the function and mechanism of KALI SOFTWARE
- To gain working knowledge of Kali software in Linux

OVERVIEW

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

INTRODUCTION

· Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

· Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

· Information security protects the integrity and privacy of data, both in storage and in transit.

· Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

· Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business

continuity is the plan the organization falls back on while trying to operate without certain resources.

- End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.

2. Cyber-attack often involves politically motivated information gathering.

3. Cyberterrorism is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking

download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

· Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

· Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

· Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

· Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

· Adware: Advertising software which can be used to spread malware.

· Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL

statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.

Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

End-user protection

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft.

In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in primary boot record and are designed to encrypt or wipe data from computer's hard drive.

Electronic security protocols also focus on real-time malware detection. Many use heuristic and behavioral analysis to monitor the behavior of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially

malicious programs to a virtual bubble separate from a user's network to analyze their behavior and learn how to better detect new infections.

Security programs continue to evolve new defenses as cyber-security professionals identify new threats and new ways to combat them. To make the most of end-user security software, employees need to be educated about how to use it. Crucially, keeping it running and updating it frequently ensures that it can protect users against the latest cyber threats.

Cyber safety tips - protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1. Update your software and operating system: This means you benefit from the latest security patches.

2. Use anti-virus software: Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.

3. Use strong passwords: Ensure your passwords are not easily guessable.

4. Do not open email attachments from unknown senders: These could be infected with malware.

5. Do not click on links in emails from unknown senders or unfamiliar websites:This is a common way that malware is spread.

6. Avoid using unsecure WiFi networks in public places: Unsecure networks leave you vulnerable to man-in-the-middle attacks.

INTERNSHIP DISCUSSION

Kali Linux is the most popular OS used by Cyber Security experts all over the world. So if you want to get into the world of Cyber Security and Ethical Hacking, Kali Linux Installation is the first step for you. Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools which are geared towards various information security tasks. Such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

Kali Linux and its role in cybersecurity

One of the greatest features of Kali Linux is the fact that is has pre-installed tools which can be used for a tremendous number of cybersecurity-related tasks. There are more than 600 tools included in Kali Linux for penetration testing and cybersecurity purposes, and the Kali distro is continually updated and improved by Offensive Security.

Popular tools of Kali Linux

The pre-installed cybersecurity tools are the major factor in the popularity of Kali Linux. Lets spend a few moments to go over a few of the most popular and useful as an example of what Kali Linux can do for us as cybersecurity professionals.

Metasploit

Metasploit is a penetration testing tool that makes hacking far easier for cyber professionals. It takes processes that used to be manual, such as information gathering, gaining access, and evading detection and automates them. Metasploit is extremely popular and highly used by professionals in the information security field, and it is a great way to test exploits and vulnerabilities.

John the Ripper

John the ripper is a password cracking tool that is customizable and combines numerous cracking modes to suit individual needs. The best part is it can be run against various encrypted password formats, and it can perform password cracking techniques, such as dictionary and brute force attacks.

Netcat

Netcat is a network tool which is used to read and write data across network connections. Netcat includes a list of features from port scanning to transferring files to port listening. Netcat can create almost any kind of connection you would need and is a preferred tool for port scanning.

Wireshark

Wireshark is an open-source packet analyzer and it is used to see and evaluate traffic on a network, which makes it essential for any security professional or systems administrator. When run and analyzed live, it is a real time indicator of what traffic is going across the network, and can even be used for troubleshooting.

The cyber advantage of using Kali Linux

Those were just a few examples of the popular applications that come pre-installed on Kali Linux. While it is true that all of the applications on Kali Linux are free and can be downloaded on other operating systems, Kali Linux makes it a lot easier for the user by doing all of the work for you and compiling them in one operating system distribution.

CONCLUSION

More highly skilled workers in cybersecurity roles would help the nation respond more robustly to the cybersecurity problems it faces. All organizations need to understand their threat environment and the risks they face, address their cybersecurity problems, and hire the most appropriate people to do that work.

With the proper know-how, hacking can be done in any platform — whether it is Linux or Windows. But, Kali Linux — the name itself invokes a strange curiosity, which makes people have a deep look into this OS. From the days of BackTrack to the latest version of Kali, with a plethora of testing tools that allow its users get straight to work, the OS has gained tremendous popularity in the space of penetration testing.

Unlike other OSes, Kali might feel a bit difficult to use, but if you sincerely want to explore the world of cybersecurity, then Kali Linux is the premier choice — it is elegant, clean, and presents a ton of interesting things for you to experience and learn.

Bibliography:

- analyticsindiamag.com
- startacybercareer.com
- www.cybrary.it