VIT®
BHOPAL
www.vitbhopal.ac.in

CYBERZINE

ANNUAL CYBER SECURITY MAGAZINE

SEPTEMBER 2021

VOLUME III

OUR GUIDING FORCE

DR. G. VISWANATHAN
CHANCELLOR

MR. SANKAR G. VISWANATHAN
VICE PRESIDENT

MS. KADAMBARI S. VISWANATHAN
ASSISTANT VICE PRESIDENT

DR. U. KAMACHI MUDALI
VICE CHANCELLOR

DR. K.K. NAIR
REGISTRAR

DR. MANAS KUMAR MISHRA
DEAN - ACADEMICS

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

DR. S. POONKUNTRAN
DEAN - SCSE

DR. R. RAKESH
PROGRAM CHAIR - B.TECH

DR. R. RAKESH
PROGRAM CHAIR - B.TECH

DR. H. AZATH
PROGRAM CHAIR - INT. M.TECH

DR. PUSHPINDER SINGH PATHEJA
PROGRAM CHAIR - M.TECH

PREFACE

CYBERZINE 2021

Dear Reader,

CyberZine is an attempt by the Department of Cyber Security and Digital Forensics at VIT Bhopal University to bridge the gap between non-technical personnel and cybersecurity professionals. It is a joint effort by cybersecurity students and professionals to present information to the common gentry in an easy-to-understand manner. We aim to arm the non-technical personnel with correct information on what actions lead to these security breaches, thus, preventing them from happening. Despite its simplicity, students and professionals can read it and enhance their knowledge.

The idea behind the magazine is to make cybersecurity more accessible and bring it down to the level of the common gentry while also providing something of value to professionals and students. It covers topics ranging from the latest cybersecurity tools to recent attacks and breaches. The seemingly 'complex jargon' has been broken down into simpler words for a better understanding. We have tried to present this information in small chunks in an attempt to not overwhelm the reader. It results from the constant striving of a dedicated team to present the third edition of CyberZine that you are now reading.

Sincerely,

CyberZine Team.

TABLE OF CONTENTS

TABLE OF CONTENTS

DSCI Excellence Award 2020 for Cyber Security Education

The Data Security Council of India (DSCI) is a not-for-profit data protection industry body set up by NASSCOM® in India, dedicated to making cyberspace safe and trusted by developing cybersecurity and privacy best practices, standards, and initiatives.

On December 17th, 2020, VIT Bhopal University received the prestigious DSCI Excellence Award for Cyber Security Education 2020. It is a national-level award that signifies that VIT Bhopal University's Division of Cyber Security and Digital Forensics is the best in the nation and offers quality cyber education.

Getting Started with Cyber Security and Digital Forensics

There is a myth that cybersecurity is all about hacking, penetration testing, and bug bounty, which is not accurate. Cybersecurity and Digital Forensics are much more than that. Let's explore what it is and find out how to get started.

Here are a few steps every beginner should follow to start or boost their career in this domain. Go through each of them, and you will get an insight to begin or improve your learning. Always remember that knowledge is the key to a successful attack or defense.

1. Cyber Security Mindset: Whenever we do something, we begin by setting a mindset. A mindset to approach, perform, explore, innovate, think smartly, and tackle problems provides the vision to conquer the mission. Following are the few aspects a person should be ready for before getting started:

    - Non-technical: If we plan an ethical

attack or a defense, the first step is information gathering. The same applies to real life as well. Consider a hypothetical scenario where you have to hack a suspect's phone to gather some evidence. The easiest way would be shoulder surfing and getting their password. All you need is social engineering, intelligence, common sense to manipulate them, and mission accomplished.

- Technical: Technologies keep on emerging with exclusive features and hidden vulnerabilities. One should always stay committed to learning about the novel technologies.
- Basic Qualities:
  - Active and aware: It is an essential quality during learning or even after getting a job. Laziness will waste your time, and unawareness will cause mistakes/flaws in your work. Example: In security monitoring, one has to monitor every event. If something is overlooked or neglected, it may lead to a breach.
  - Open to learning: It is a fact that the work efficiency and the results depend on how interested you are. The more you will explore, the more topics and events you will find.
  - Smart-working and consistent: Big dreams require hard work in the right direction. We should not only work hard but should also practice smart working. The only process of mastering any art or skill is by practicing them, focusing on improvements, and doing it consistently.
  - Patience: Good things take time to come, and experience comes with time. Never panic by comparing yourself with others. Everyone has a different goal, approach, and destiny.

2. The Learning Path:
   - Basics of CSE:
     - Computer Hardware: We should start with the identification of hardware. In the cybersecurity domain, we need to know the basics of computer hardware.
     - Computer Architecture: Computer architecture and its basics are essential. One should know about the flow of data, memory allocation, process allocation, etc.
     - Operating Systems: Developers build operating systems on different architectures. As a security professional, knowledge of multiple operating systems is essential.
     - Computer Networks: It defines how hardware and applications communicate. We have different Network Models with different layers, each performing specific functions.
     - Programming Languages: One should learn the required programming languages (C, C++, Bash, PHP, JS), and know the approaches to problem-solving through data structures and algorithms.
   - Architecture basics for cybersecurity:
     - Exploring the cybersecurity hardware architecture: When

we work in cybersecurity, we should learn about the hardware involved in any activity that we perform. Some do's and don'ts related to them, the potential threats to that hardware, how they are vulnerable, corrupted, or exploited.
  - Data and packet flow: When you talk about the digital realm, it's all about the data we store over the cloud or the internet. We send and receive everything in the format of data packets. Understanding how those data packets get sent and received will help one in understanding and manipulating the process.
- Background of cyber laws and policies: Before practicing the technical, one should know about the laws and policies. We should understand the difference between actions we can consider criminal, offensive, threatening, ethical, or legally non-offensive acts. Every country has its laws and policies, as mentioned below.
  - IT Act 2000 and Amendment 2008
  - GDPR
  - PIPA
  - (NIS) Directive 2016/ 2018
  - HIPAA
- These paths are independent of each other, so you can learn them in parallel to save time. Topics will continue to connect with each other's progress. It is the elementary beginning, and it is not limited to just these.

3. To build oneself, one has to work hard on their skills. Both soft and hard skills are critical to proving that you deserve to be selected. These are a few common skills that you should consider a must-have:
   - Hard Skills:
     - Ability to explain technical topics in simpler terms.
     - Computer science fundamentals.
     - Expertise in a sub-field.
     - Knowledge of at least one programming language.
     - Familiarity with the attack tools/techniques in the Mitre attack framework.
     - Ability to track complex engagements and multiple pieces of evidence.
     - Information management and high-risk decision-making.
   - Soft Skills:
     - Active listening, clear verbal and written communication.
     - Attention to detail.
     - Creative and technical problem-solving.
     - Adaptability and a team mindset.
     - Maintaining calm in a stressful situation.
4. Exploring sub-domains, roles, and interests: It's crucial to explore the options before deciding. The domain Cybersecurity and Digital Forensics has over 15 sub-domains.
   - Common
     - Networking
     - Software Development
     - System Engineers
     - Financial and Risk Analysis
     - Security Intelligence
   - Entry-level
     - Cyber Security Specialist/Technician

  - Cyber Crime Analyst/Investigator
  - Incident Management/Analyst/Responder
  - IT Auditor
  - Security Operations Center (SOC)
- Mid-level
  - Cyber Security Analyst
  - Cyber Security Consultant
  - Penetration and Vulnerability Tester
- Advanced level
  - Cyber Security Manager/Administrator
  - Cyber Security Engineer
  - Cyber Security Architect

5. The 4-Point Strategy:
   - Time distribution: It is sometimes challenging to manage time. Mismanagement can lead to progress lags, stress, and a loss of interest. Use your time wisely.
   - Task distribution: One should know the skill of proper task distribution as it can get stressful in hectic and serious situations in this field.
   - Set checkpoints for progress/achievements: Set small goals and checkpoints and try to complete them. It adds value to your working habits, and you can develop the ability to accomplish them in assigned time.
   - Preferred events to take part in: Being selective and prioritizing the events that one wants to take part in is critical for time management and self-growth.
6. Get comfortable with multiple operating systems: In this field, an attitude of sticking to one OS won't help. During the investigation or in security analysis, you may have to deal with different operating systems. There are various operating systems with unique features. Explore each of them and be aware of file directories and their contents. If you plan to work in the security domain, the knowledge of various Linux distributions is essential.
7. Diverse toolset: Keep a set of tools handy, practice with them and use them wisely. Kali Linux, Parrot Security OS, Bugtraq, Blackbox, Martuix, Knoppix are some of the best Operating Systems that contain the best tools for Cyber Security and Digital Forensics. It's not compulsory to know about all of them. But it is necessary to know and understand those which apply to the sub-domain of your interest.
8. Hands-on Practice: Once you have started the learning process and are now ready to practice, here are a few platforms that will help you.
   - TryHackMe
   - Hack The Box
   - Blue Team Labs
   - Hack This Site
   - HellBound Hackers
   - VulnHub
   - PicoCtF
   - CTF101
9. Remain updated with top incidents: Read daily journals, news, and articles to stay updated about the latest technologies and incidents.
10. Prevent Distractions: Last but most important, one should avoid getting distracted.

Importance of Cyber Threat Intelligence in the Organizational Security Framework

Globalization and integration of financial firms with technology have resulted in the assimilation of most businesses and companies into the digital world. The count of active internet users reached almost 4.57 billion in July 2020, comprising 59 percent of the global population. With an ever-increasing user base, the frequency and severity of threats are escalating on the internet. To deal with these advanced and sophisticated cyber-attacks, organizations and individuals need to upgrade their cyber-

security architecture. Global platforms and intelligence exchanges of threat information are necessary for cybersecurity professionals to become more aware of the existing risks and vulnerabilities to security. Also, organizations need to make more informed security decisions for using the security capital efficiently. Cyber Threat Intelligence (CTI) plays an essential role here.

The fundamental aim of security through CTI is to provide an organization-focused outlook to the security team by informing them about the advanced threats and exploits like the zero-day attacks to which they are pretty vulnerable in the current security scenario. It gives a detailed analysis of threats and adversaries and thus facilitates effective intelligence exchange and threat analysis. So, the organizations can outwit the attackers by keeping track of their behavior and predict future attacks by resorting to defensive measures to mitigate them.

Necessity of CTI in the security posture

Most organizations now appoint complex Information Systems (IS) to conduct financial transactions, maintain company records and information infrastructure to handle daily operations. With the increasing cyber-attacks on these systems, the cybersecurity team needs to gather more relevant, timely, and accurate intelligence about the new vulnerabilities, risks, and threats and execute prompt security measures. Henceforth, CTI is an optimal and necessary component of mitigation strategies for all the organizations that function in this developing technical environment and significantly changing the threat landscape.

Threat intelligence should not just be confined to established and well-financed businesses. A recent report on data breach investigations states that small businesses have to face 43% of cyber-attacks. So, even small organizations should gain access to legitimate sources of cyber threat intelligence. To develop an efficient cybersecurity framework, an enterprise needs to be aware of potential cyber threats and understand how threats can affect an organization.

Building an efficient CTI program results in a positive impact on the organization in the following ways:

- Circumvent possible data losses: Data is the most valuable asset and a liability. Protecting and maintaining the confidentiality of data is the utmost priority of a company. So, when malicious domains and IP addresses attempt to gain unauthorized access by connecting with their network to gather critical information, a CTI system safeguards the data. It prohibits such domains and addresses from penetrating the network and stealing confidential data by blocking such activities.
- Lowering costs by preventing financial losses: A recent data breach report by IBM stated that the average total cost of a data breach was USD 3.86 million. Furthermore, the average time to identify and contain a breach was 280 days. After a data breach, an organization not only encounters data loss, but a lot of the company's capital goes into the post-incident response. It has a direct impact on the firm's market image and brand. Cyber threat intelligence plays a vital role in security infrastructure by making well-relevant and timely decisions, mitigating the company's risks of sensitive data theft, device downtime.
- Lowering possible risks: Adversaries and cyber-criminals outsmart the organization's security teams by discover-

ing new and more sophisticated techniques to break into networks and systems to gain unauthorized access and cause further harm to the firm. Organizations need CTI for minimizing risks, preventing data losses, and maintaining the confidentiality of the data.

- Maximizing staffing efficiency: When a data breach or a cyber-attack occurs, it affects the functioning and productivity of the staff. Incorporating the CTI framework increases the yield of an organization's cybersecurity unit. It can prevent the security unit from facing both psychological and technical fatigue.
- Focused security investment and working: A crucial advantage of CTI is that it gives focus and direction to the security department by revealing the essential adversary details like the loopholes in the security posture that they target, the attacker's behavior, their geographical location, et cetera. All this would require more time and investment without threat intelligence. Hence, the company can wisely invest its capital, efforts, and time looking after threats focused on specific areas and the correlated details about the adversaries.
- Threat intelligence exchange platforms: The cyber threat intelligence program integrates loads of threat intelligence feeds into a single feed. It allows coherent analysis and classification of cyber threat incidents, detection of patterns, and developments in an adversary's behavior. Various threat intelligence platforms equip the organization with critical information regarding recent security breaches and cyber-attacks, how adversaries plan to do so, and which set of businesses a specific hacker group targets. If other organizations get relevant information regarding a recent security attack on an organization, they can mitigate it by taking the required security measures.

Future prospects and conclusion

We should integrate threat intelligence with the latest technologies and grow accordingly. It needs to develop with the changing nature of threats, and we must incorporate it with technologies like AI and quantum computing for efficient and accurate working. Hence, the CTI framework needs to strengthen with the changing nature and sophistication of threats.

The Anatomy of an Information Security Audit

It's a systematic and measurable technical assessment of a company's security policies. They provide a way to define and assess the security of a production environment.

There are multiple types of Infosec audits, depending on the security controls used in the organization. An organization can have technical, physical, or administrative audits. The same depends on the rules used in the organization. Information security au-

dits cover several topics across multiple domains of security. These audits help create a security benchmark for the company. Audits identify the strengths and weaknesses of a company while prioritizing the remediation of exposures that present the highest risk. Most audits offer risk mitigation measures in line with industry best practices.

Infosec auditing covers a few fundamentals:

- All critical data and processes.
- An understanding of the threat landscape.
- A proper governance and accounting system.
- Resilience to withstand any attack.
- A strategy to define the security budget allotment.

There are two types of general audits, internal and external. To conduct internal audits, employees use resources available in their work environment. Internal auditors often lack a complete knowledge required to conduct audits. External auditors, however, are skilled professionals with a wide range of tools at their command. External audits are more of a luxury, as the cost can sometimes be higher than the security budget. The success of the audit depends on the level of communication between the sysadmin and the external auditor. An auditor can use multiple software implementations to collect data needed for an infosec audit.

The auditing team designs a list of threats and tests the production infrastructure against them. These threats can include uninformed employees, weak passwords, employee devices, malware, physical theft, natural disasters, insider threats, denial of service attacks, phishing, et cetera.

Auditing is usually a 4-step process:

- Proposing: The audit plans should be very minimal to cover as many aspects as possible. We divide the plot into three parts: the aim, the scope, and the expected outcomes of an audit.
- Investigating: The auditing team will execute the plan in all areas of the business. Thus, having strong communication during the audit process helps move things along faster. This phase involves inspecting the current system for any flaws.
- Concluding: The auditing team will interpret the test results according to the investigation documentation. They determine the conclusion based on the parameters provided by the organizations. Auditors also need to define any deviations from security practices at this stage.
- Reporting: The auditor can deliver the final report verbally or in writing. This report will answer critical questions about the system's security.

While the aforementioned is a general list of auditing responsibilities, the proper roles and responsibilities can vary depending on the organization. Infosec audits require thorough attention to detail. An infosec auditor also has a specialized certification that verifies how good they are at pulling out deficiencies in the security setup.

STEGANOGRAPHY

Aakanksha Priya

1

SUPPOSE THAT RIGBY WANTS TO SEND A MESSAGE TO HIS FRIEND KIRBY. HOWEVER, HE DOES NOT WANT ANYONE ELSE TO READ THE INFORMATION. HOW CAN HE ENSURE THIS? A SIMPLE SOLUTION IS USING CRYPTOGRAPHY.

RIGBY CAN ENCRYPT THE MESSAGE TO MAKE SURE THAT ONLY KIRBY READS THE INFORMATION.

THERE IS A DOWNSIDE TO IT. THOUGH THE TEXT IS NOT READABLE, THE ENCRYPTED TEXT REMAINS VISIBLE. IT CAN LEAD TO SUSPICION. SOMEONE CAN EASILY DECODE THE TEXT.

2

IT IS WHERE STEGANOGRAPHY COMES IN. STEGANOGRAPHY ALLOWS US TO HIDE ANY DIGITAL TEXT, AUDIO, OR VIDEO INSIDE AN ORDINARY FILE OR MESSAGE. WE CAN HIDE THE DATA IN ALMOST ANY KIND OF DIGITAL FILE. WE CAN ALSO ENCRYPT THE DATA BEFORE CONCEALING IT TO STRENGTHEN SECURITY.

THIS COMBINED USE OF ENCRYPTION AND STEGANOGRAPHY OFFERS MORE STEALTH BY HIDING TRACES OF COMMUNICATION.

STEGANOGRAPHY IS NOT A SUBSTITUTE FOR ENCRYPTION. BUT WHEN WE USE IT ALONG WITH ENCRYPTION, IT ENHANCES PRIVACY AND OBSCURES THE EXISTENCE OF DATA. IT IS NEAR AS IF THE COMMUNICATION NEVER HAPPENED.

3

DIGITAL STEGANOGRAPHY CAN HAVE MULTIPLE METHODS. ONE OF THE MOST POPULAR ONES IS TO USE AN IMAGE AS THE CARRIER FILE. SECURE COVER SELECTION IS WHERE THE ATTACKERS COMPARE THE BLOCKS OF CARRIER IMAGES AND THE BLOCKS OF SECRET CODE OR MALWARE. THE LEAST SIGNIFICANT BIT AND PALETTE BASED TECHNIQUES ARE ALSO SUITABLE ALTERNATIVES.

4

GIF FILES ARE SUITABLE FOR THIS PURPOSE. GIFSHUFFLE IS A TOOL THAT ALTERS THE IMAGE'S COLOR MAP AND ENSURES THAT THE ORIGINAL IMAGE IS NOT MODIFIED SIGNIFICANTLY.

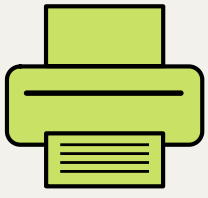
DATA ORDERING IS AN EFFICIENT METHOD AS WELL. AUDIO FILES AS CARRIERS ARE NOT VERY POPULAR BUT QUITE EFFECTIVE. MP3STEGO IS A TOOL USED FOR THIS PURPOSE.

5

STEGANOGRAPHY IS A POPULAR TECHNIQUE AMONG CYBERCRIMINALS. THE ATTACKERS IMPLANT THE ACTUAL SCRIPT OF MALWARE OR TROJAN INTO AN EXCEL FILE OR WORD DOCUMENT. WHEN THE USER OPENS THE DOCUMENT TO READ, THE HIDDEN SCRIPT RUNS AUTOMATICALLY. THE HIDDEN MALWARE THEN INSTALLS A BACKDOOR, WHICH CAN GIVE ENTRY TO UPDATED VERSIONS OF MALWARE.

6

WE CAN UTILIZE STEGANOGRAPHY IN VARIOUS FIELDS. WE CAN USE STEGANOGRAPHY TO STORE WATERMARKS IN A DOCUMENT. MODERN PRINTERS USE STEGANOGRAPHY TO ADD TINY DOTS TO PAGES. THESE DOTS CONTAIN PRINTER SERIAL NUMBERS, DATES, AND TIME STAMPS.



Securing Afterlife Privacy

We are living in a mortal world, and death is inevitable. We are all being followed by the grim reapers all the time. Bad things happen every day. Sometimes, they can happen to you too.

In ancient times, people hid their valuables or life savings for their families to use in case of their demise. They created a map or a secret key to ensure only their loved ones could access it. At the time of their death, they would give it to their family members.

But this is the 21st century, and data is the new gold. Everything is in a digital format, whether it is money or private data. Our digital footprints matter a lot. Nowadays, deaths are more sudden, and sometimes we don't even get the chance to share details such as passwords to our bank and social media accounts, insurance details, and much more with our near ones. It gets hard for them in the coming future to survive, and they have to struggle to claim what is theirs.

Now, three questions arise. First, are we going to lose everything? Do we have any right to control what happens to our online presence, to our social media accounts after death? Can we decide who can have access to our profile or not? This question might seem irrelevant to some people, but

it is not. Because if someone gets unauthorized access to your social media accounts, then that person can pretend to be you and could defame you, which is a direct case of identity theft.

Sounds funny, identity theft after death? Yes, but identity theft is not a joke. That's a serious issue because it can cost the deceased family a lot if someone uses it maliciously. It would all look as if the departed person performed the said malicious activities. To reduce the chances of this happening, tech giants like Facebook and Google have come up with an idea of memorialization.

Facebook calls it Facebook Legacy, wherein your friend or family member whom you have opted as your heir can make choices related to your profile after your death. They can choose to either get the profile deleted or convert your profile to a shrine or memorial. If that person converts your profile into a memorial page, other people can leave comments, poems and share memories on that profile. No one will be able to post or log in to the memorialized account as the deceased.

On Google, there is an inactivity manager. The trusted person (heir) set by you for your account will get a customized text you write during the setup from Google, over the mail, if you remain inactive for a certain period. You can choose to share the data from your emails, drive, photos, et cetera, with them during the setup. They won't receive your google account password. After they get the data, Google will delete the account. No one can get the same username in the future. To ensure that a genuine person receives the data, they will have to verify their identity using the mobile number set up with the email.

So, our online presence and data will remain somewhat secure after our death. But now, the second question arises. What if someone wants to share their last words or private data with their family/friends that they only wanted to share after their demise, like the password to the bank accounts, social security numbers, or a special message? In many cases, a person dies without getting a chance to share the details about their savings or personal things like banking passwords, pins, et cetera, with their family.

The answer to this is renting a legacy locker that keeps your data safe by charging a minimal amount and sharing that data after your demise with the trusted recipients set by you. One of many such legacy lockers is the dead man's switch. They offer two emails with two recipients for free and charge you to increase the limit. Here, you can write the emails and choose the recipients. They will store the emails privately. Then you will have to set a period after which you receive an email from them, asking if you are all right. If they don't receive any response from you within the set period, they will send the emails. In the emails, you can also leave instructions on who is to do what with what. Sometimes, it can also cause you trouble, like, if you forget to respond in time. It will send the emails causing panic to your loved ones - or making your loved ones worry unnecessarily. Otherwise, this could be helpful in tons of ways.

And the very last question, is there a way to remove someone's data from the internet in case of their death? The answer is, in some countries, there is an option of removing their data entirely from the internet. We know it as the right to be forgotten or the right to erasure. It comes under the General Data Protection Regulation (GDPR).

So, you can now make sure that your data and your identity will remain safe even after your demise, and the essential things get shared with your family and friends.

Cyber Diplomacy

Cyber Diplomacy is a new thing that is getting introduced nowadays. Most countries run their foreign policy objectives and narratives through social media platforms, blogs, and websites.

Twitter has brought a revolution in cyber diplomacy. It is connecting the world with international affairs, and the hashtag of Twitter is a weapon in cyber diplomacy. It has democratized the entire diplomatic process. But it also allows unfiltered features. Social media is empowering citizens in making global leaders stand accountable for their policies and statements.

What is cyber diplomacy?

Cyber diplomacy means leveraging the power of the internet to achieve diplomatic targets. Internet, plus other information and communication technologies, act as a medium to strengthen relations, solving foreign policy problems, and showing concern on any matter related to a country by the Foreign ministry and Diplomats.

Cyber diplomacy also allows diplomats to engage directly with the audience. It also works as soft power and increases the participation of general citizens.

The sudden aggressive involvement of Chinese diplomats on Twitter during the initial COVID period, Justin Trudeau's tweets on foreign state matters, The White House following Narendra Modi's account, Republican-Democratic Twitter war, et cetera are examples of cyber diplomacy.

Why is cyber diplomacy dangerous?

Cyber Diplomacy is also a foe. If it is in the wrong hands, then it can provoke people against humanity in the name of religion, culture, and many other narratives. In the wrong hands, it can promote separatism and hate.

Countries that have these social media companies have the advantage of controlling the world. The respective governments can control these companies and force them to work in the way they want.

Cyber diplomacy can set false agendas. It gives a free hand to the diplomats to interfere in internal matters. Cyber diplomacy always has a risk of hacking and data misinterpretation.

Why is cyber diplomacy successful?

Cyber diplomacy is the cheapest means for diplomats to reach people, easily extend their diplomatic networks, and build strategic relationships in real-time.

Cyber diplomacy has increased transparency and accountability. It holds politicians and activists accountable for human rights, environmental and financial problems. It also lets the people know how related the politician or diplomat is to the culture and national interest.

Another advantage of Cyber diplomacy is that it is much cheaper than traditional diplomacy. Diplomats don't need to travel to another country to represent the interest of their country. It is environmentally friendly too. Applications like Skype, Jio meet, Zoom allows them to meet remotely and convey their message or narrative.

Welcome to the Dark Web

The internet was invented with a vision to provide information to all, but it has costed our privacy. While the crowd was in awe of the invention, the US government was worried as they needed a secretive exchange of confidential information through the web. This concern initiated the project known as onion routing. For this, they released a router to the public to maintain decent anonymity. When you browse the web using

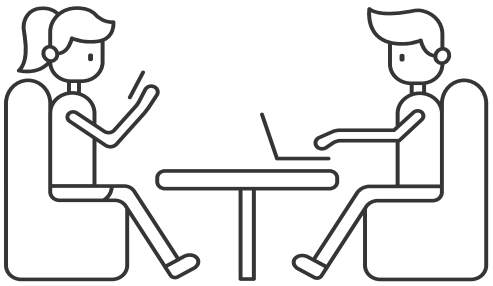
this onion router or TOR, one gains access to the internet's deeper side. This part of the web where some illegal activities happen is called the dark web.

One way that the dark web differs from the web is the domain it uses. The majority of the sites end with the onion domain. Apart from that, the contents heavily contrast. People who have surfed the dark web have confirmed access to buying guns, drugs, hiring hackers, and illicit content. There are rumors that some people commit gruesome torture in online red rooms. No one has ever witnessed such a sight in reality, but horror stories exist. The products are bought via Bitcoins and not using credit cards or other means.

The Silk Road allowed drug exchange with almost 100000 buyers and had generated 600000 Bitcoins. It also provided access to stolen passwords and data. Ross Ulbricht created and operated the site from 2011 until the FBI shut it down in 2013. There were attempts to resurface it.

There are many more websites for the sale of drugs. The wickedest activity prevailing on the dark web is the torture of animals and child pornography. There we can see visuals that would make a person in their right mind sick to their stomach.

Things certainly seem to be pretty bad down there, so one might wonder - why not take the entire platform down?. The existence of such a space was initially not expected. The US NRL (Naval Research Laboratory) started this project to provide ultimate anonymity to the government. The dark web can also perform normal web activities with privacy. Misuses of this benefit are met with punishment occasionally, but it all goes in vain. When one goes down, another pops up months or years later. The only solution is to accept the bad with the good and be fellow humans in the same world, keeping ourselves safe from these things.

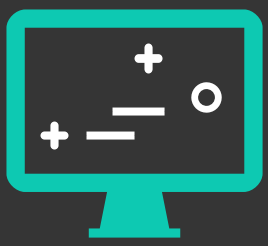


Zero-Day Vulnerabilities

Noel Varghese

What exactly are they?

The vulnerability in question unknowingly exists within the application or software that is released by the developers. Once a weak spot is found, an attack is made. Crucially, it is done before the manufacturer detects the flaw within the software and corrects it.



Who could be at risk?

The first line of attack is upon the software and hardware that gets infected by the vulnerability. The risk then extends, ranging from the typical amateur to the specialized users using the affected service. It depends on the malware unleashed by the attacker, on the software or hardware, hence causing the vulnerability. The miscreant can be driven by targeting financial gain, data theft, or other motives.

How do we identify it?

The chances of detection are rare. That's what makes it a severe threat. However, a few steps can be taken to identify it.

- Live Monitoring - The activity timeline of the software is put on a watch and to detect unusual traces of activities, which raises the flag of vulnerability being exploited.
- Honeypots and Honeynets - Honeypots can be implemented to catch the cracker in the act by analyzing attack patterns and brute force attempts.
- Threat Intelligence - Sourcing information about the supposed threat to generate workable solutions towards nullification.

How do we ensure security?

- Deploy patches to fix the vulnerability.
- Install Patches as soon as they are released.
- Have an emergency response team always on standby.

Data Security: Need of the Hour

Data security, in simple words, can be defined as the security of some private information that a person or an organization, under normal circumstances, is not willing to disclose in public. For instance, you are comfortable telling your name or height to a known person, but not your ATM pin.

Because of the increase in data breaches, companies and governments have become meticulous about data security. If you compare the current scenario with, say, a decade ago, you'll find that things have changed drastically. With more and more people shifting towards the digital world of social media and the Internet, it has become quite difficult for companies and start-ups to store the ever-increasing private data of people while ensuring that we safeguard it from hackers.

With advancements in technology like - faster computers and high-speed internet connections, which are a boon to hackers, the public's data is at stake. Many companies don't even have a planned response mechanism in case of a cyber-attack.

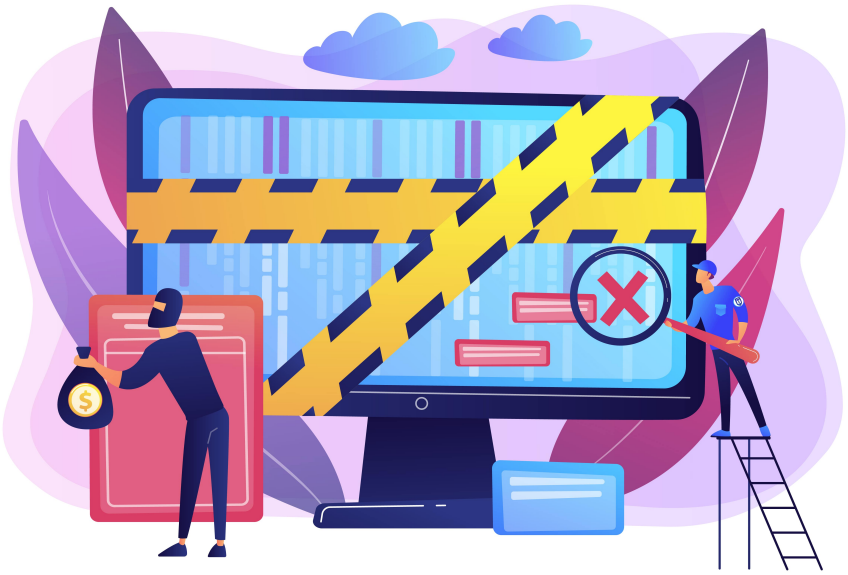
Over the years, more and more people are becoming aware of Data breaches. They are taking steps to protect their private data, though there are some areas where we people need improvements.

In the 21st century, as technology advances, there comes a great deal of risk to your private data. While you might feel safe enough, the reality is far from what you believe.

According to the Information Commissioner's Office (ICO), companies have reported 1500 cyber security incidents that too only in the first quarter of 2020. Though the number of cases has declined since the previous year, people are still falling victim to these cases. According to the Fourth Annual study on the Cyber Resilient Organization, only 23% of the companies have a cyber-attack response plan, which is a tiny percentage.

There are many small things to which we don't pay attention, often falling victim to data breaches as a result. A very primitive measure you can take to protect yourself is setting good authentication keys and passwords.

Introduction to Digital Forensics



Digital Forensics is a sequence of steps that can extract and analyze electronic data using a systematic method. The principal purpose is to replicate the original data and evidence while conducting investigations by collecting, identifying, and verifying digital data to reconstruct past events.

If we try to understand it from the basics, then Forensic Science is a well-established field that plays a critical role in criminal justice systems.

Digital Forensics involves the retrieval and testing of artifacts found on digital devices. The artifacts usually concern cybercrimes. With the emergence of Information and Communications Technology, there have been advancements in social networking, mobile technology, cloud computing, and storage solutions. These things have weakened the security of organizational data. The increasing activity in ICT-focused environments has led to an increase in the misuse of computers and networks.

The field of digital forensics has made rapid developments over the past few years. It is because of the advancements in tools and systems that allow ordinary computer users to look up simple tutorials online. It has led to an increase in demand for forensic tools that can help in gathering digital evidence.

There is a specific procedure for evidence collection. A forensic investigator should follow this procedure in the Court of Law. It focuses on scrutinizing the validity of the process followed in evidence handling before considering its value.

As mentioned above, Digital Forensics is a new milestone in the era of forensics. To this date, researchers have proposed 25 digital forensic models. The most important ones are:

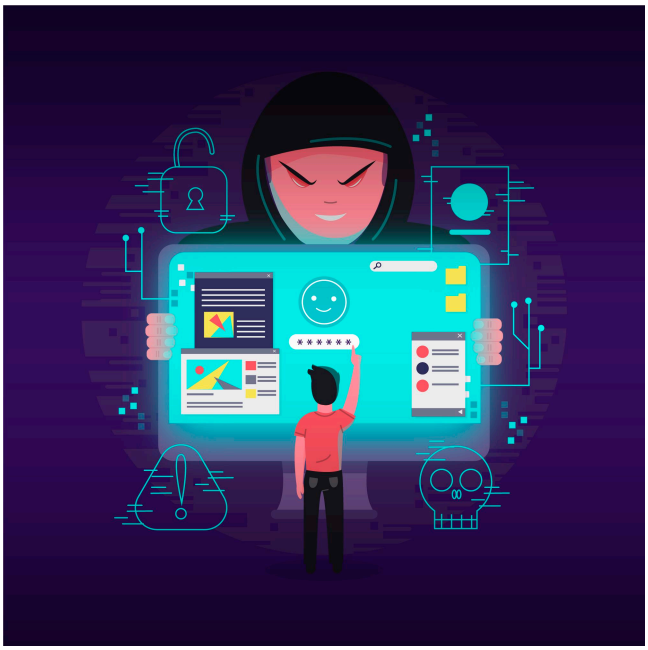
- Electronic Crime Scene Investigation (ECSI)
- Computer Forensic Incident Response Essentials (CFIRE)
- Digital Evidence and Computer Crime (DECC)
- Framework for a Digital Forensic Investigation (FDFI)

If we talk about the norms that a Digital Forensic Investigator should obey, then we can summarise it into two types of norms which are:

- The Investigator should
  - Be honest.
  - Honor property rights, including copyrights and patents.
  - Respect confidentiality and privacy of others.
  - Contribute to society and its individuals.
- The investigator should not
  - Withhold any relevant evidence.
  - Declare any confidence matter or knowledge gained in an investigation without an order from a court of competent jurisdiction or without the client's consent.
  - Express an opinion on the guilt or innocence belonging to any party.
  - Engage or involve themselves in any illegal conduct.
  - Display or falsify education, training, or credentials.

To sum up, Digital Forensics is one of the most effective sciences applicable in criminal investigations. There are many ways how one can go about investigating. Each court will define a standard process that an investigator should follow to the letter.

Phishing



Phishing is a form of cyber-attack which involves stealing the victim's sensitive information by earning their trust. The victim often provides the information themselves. Have you ever received an email titled "This millionaire wants to share his money with you" or "You've won a lottery" and ignored it? If yes, then congratulations, you could evade a phishing attack. It was an example of email phishing, one of the most common forms of phishing attack where the phisher mass mails random people hoping that someone will eventually make a mistake.

Phishers can create fake websites or even clone genuine websites to get people to enter their information. But it is not very difficult to identify these traps. With one look at the website URL, you can tell if it is a fake website or not.

Doesn't it seem like the best they can do, with these kinds of tricks, is to scam the elderly, uneducated people, and that too

rarely, anyone else could tell that the mail or website is fake, right? But then, if you look at the news, you'll realize that's not the case. IT experts, industrialists, and even bankers fall for these attacks often.

Phishing is a socially engineered technique, and the phishers don't even need to be some excellent programmer or hacker. There are plenty of tools online that can create these fake websites and emails for them. That is why it is one of the most used forms of cyberattacks.

The email phishing case we discussed earlier didn't look like there was much preparation behind it. The phisher just used some tools and mass-mailed it to people. These kinds of attacks make people believe that all phishing attacks are just like that, and they don't need to be very cautious of these emails, but what if the phishers come prepared to attack their victims one at a time?

Spear phishing is a targeted, more sophisticated, and well-executed attack carried out using emails. With spear phishing, the phishers gather initial information about their target or victim, mainly using their social media accounts. They then prepare an email that contains information too specific to be a generic phishing email. These emails also give you a feeling of urgency, and the sender can pretend to be someone you know portraying himself as trustworthy, which makes you less cautious about things like checking the link. This entire process can take days or even months of a stalker gathering information on you to find that optimal moment to strike.

Let's consider some scenarios: -

- Suppose you got an email from a senior or boss asking you to join a meeting, with a link immediately. Would you bother checking the link?
- Suppose you got an email from your college asking you to download the attached file and send some documents. Would you not download the file?
- Suppose you get an email from some website that your account security is compromised, and a link is to be used to change your password. Would you not click on it right away?

If your answer to these three questions was yes, then you are on the right track. You should always check the authenticity of these emails first. Sadly, for most people, that's not the case. The sense of urgency and fear can get them to act casually, and in that panicked state, they make mistakes.

How do we protect ourselves from phishing emails?

- A good spam filter can be helpful for phishing emails, especially mass email attacks.
- Avoid emails with too-good-to-be-accurate titles.
- If you get an email with a link to a website, open the website using a browser and not the link.
- Do not open the link or download files sent by an unknown sender
- A good antivirus can easily spot malicious files and fake websites.

Firewall

WHAT IS A FIREWALL?

If anyone tries to invade our country, they'll have to face the Border Security Force (BSF). Similarly, in our digital universe, if someone tries to connect to your computer, they'll have to face the firewall, the primary defense of a computer.

A firewall is an essential part of your computer.It is hardware or software which filters traffic on a network. It allows legitimate traffic and blocks malicious traffic requests, securing your computer from being hacked!

WORKING OF A FIREWALL

The role of a firewall is to block unwanted and malicious traffic requests from connecting with your computer. But how does the firewall know that this request is legitimate and the other one is not? We have ACL for that.

Access Control List has specific criteria listed on it based on which the firewall decides whether to approve the request or deny it. Making the ACL is the most crucial part. A minor error can compromise the security of your computer.

While setting up a firewall, we should program it to block all the traffic and allow only specific traffic. This will decrease the risk of breaching.

Basic types of firewalls

Packet Filtering Firewall

It only inspects basic information of a data packet like its IP address, port number, etc. It is the most basic type of firewall.

Circuit-Level Gateway

It does a TCP (transmission control protocol) handshake to check if the packet is legitimate.

Stateful Inspection Firewall

It inspects the basic information of the packet and performs a TCP handshake.

Proxy Firewall

It performs a deep inspection of the data packet to ensure it has no malware. It directly connects with the source.

Om Sahare

Cyberwarfare and North Korea

North Korea is getting more advanced in Cyber-warfare day by day. Despite the sanctions imposed by the USA and UN, the country continues to reap the benefits of the vulnerabilities in the network system. North Korea can run its Nuclear and Missile programs from the funds collected through its tremendous success in cyber-crimes and the loopholes in the sanctions.

Cyberwarfare is a very cost-effective option for the country. According to South Korea's former Director of National Intelligence Service, Kim Jong Un (Supreme Leader of North Korea) himself marked nuclear capability and cyber warfare as equal on the scale.

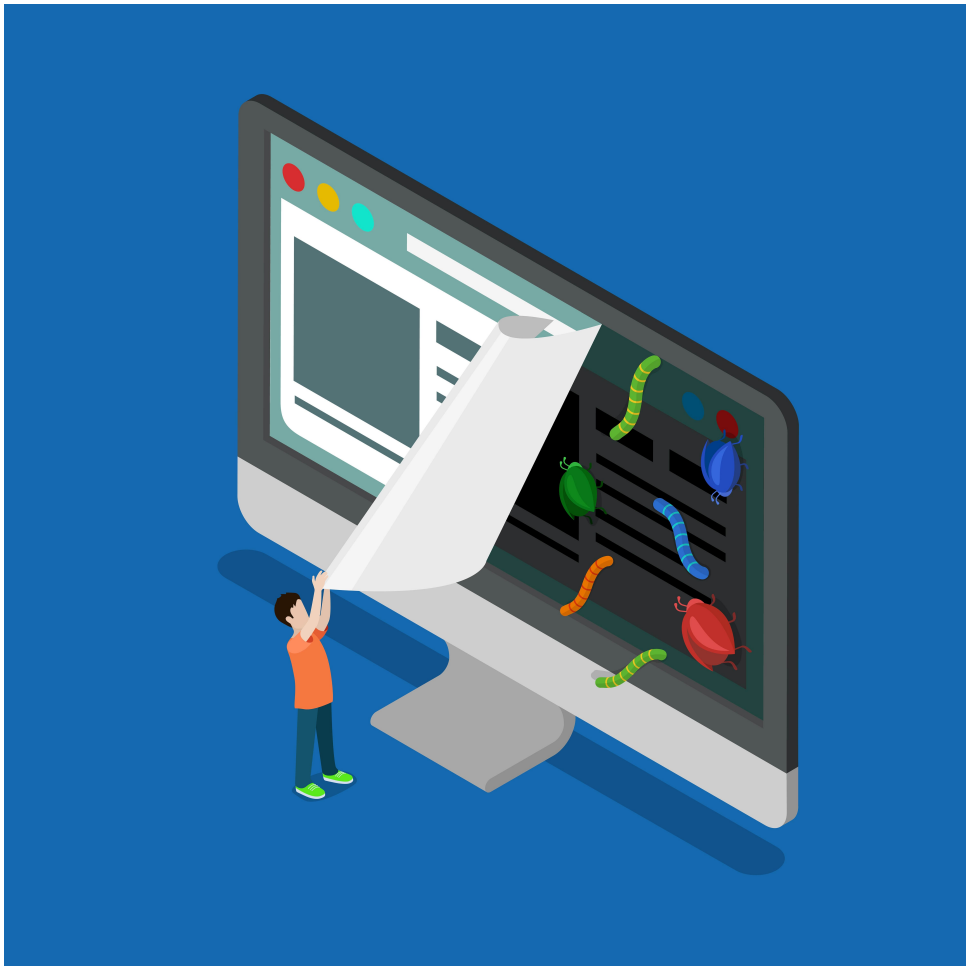
North Korea uses its universities to train its youth in hacking, creating viruses, and finding vulnerabilities. Recently, North Korean state media confirmed the establishment of a Science and Technological University, whose principal motive, according to experts, is to train the youth in cyber warfare and weapon technology.

North Korea did not stop here. According to a US Army report, North Korea has over 5900 agents worldwide. The Lazarus group, which handled the 2017 WannaCry ransomware attack, is one of them.

China is reportedly supporting North Korea indirectly. North Korean students often study in top Chinese technological institutions and get access to top-class technology. The Chinese government continues to support and collaborate with North Korean military institutions, even after knowing the danger it poses for the world. Some experts say that China is giving training to dangerous cyber attackers who are involved in cyber-terrorism.

The world needs to think about new protocols and regulations for cybersecurity and strengthen organizations like the Cybersecurity and Infrastructure Security Agency (CISA) and the Financial Action Task Force (FATF) before it is too late.

The Untraceable Tracing



In the Digital World, technology is all around us. Computers are an inherent part of our lives. As we develop new technologies, cybercriminals apply these technologies to commit crimes. In today's age, the advancement of technology has taken a new turn in the digital realm. Cyber-crimes and attempts to mask fraudulent activity

have increased. Even before people knew about digital forensics, they couldn't have imagined that technology also can cause crimes digitally. Businesses have streamlined their operations by saving millions of dollars in web technologies. Organizations cannot live their life without technology. When a cyber-crime occurs, investigators present the computer evidence in the courts. This evidence can contain fragments or files recovered from storage devices such as emails, personal data, browsing history, photographs, documents. Recovery of deleted files or documents from computers requires special techniques.

While cyber-crimes are intimidating, the digital trail takes us towards the stage of forensic investigation that we had not thought of even a few years ago. So investigators conduct forensics by analyzing, collecting, accessing, and interpreting electronic devices. Digital forensic investigations have a wide range of applications. In the private sector, digital forensics plays an important role. There are forensic investigations in the Military, Corporate Sector, and Law Enforcement.

It is astounding how persuasive the digital world is in the United States. 83% of the households own a computer, 91% of customers check their email at least once, 92% of executives use a mobile device to conduct business. Virtually everyone is a part of the digital world. Sobering statistics about the cost of cyber-crimes comes as no surprise. In 2014, cyber-crime cost us nearly $12.4 million, which was 9% more than the previous year. Globally, cyber-crime leads to a loss of $325 million - $525 million annually. Because of the pervasiveness of desktops and mobile devices, the expense associated with cyber-crimes is on the rise.

One such instance was UniCredit hackers trying to sell employee data on cyber-crime forums. Investigators found that the employee data that went on sale on April 19 included important emails, encrypted passwords, and phone numbers. The attack was likely because of an SQL injection. The attackers sold leaked data based on the number of rows offered to the buyer. The comprehensive package had evaluated 150,000 rows of data to $10,000. It had UniCredit data from late 2018-2019, as reported by Telsey's posting. Large Companies, institutions, and banks have faced cyberattacks that disrupted operations that included customer's private information. Last year, UniCredit discovered a data breach involving three million customers. In 2016, it upgraded its cybersecurity and information technology systems by investing billions of euros to secure its data.

DFI conducts investigations employing a secret weapon to extract almost 90% of the data on mobile devices, laptops, or any digital device used in the private or government sector to secure their data. One such secret weapon used for extracting all the data is Cellebrite Touch Ultimate UFED. UFED provides unimaginable tools and software systems for analyzing the data and speeds up digital forensic investigations.

Cyber Laws in India and The CIA Triad

In the late 90s, after the days of wired communication, the internet developed as the medium for transferring information. Our country has transformed digitally and paved the way for a new period - the Cyber Age! However, uncontrollable dependence on technology encourages the perpetrators to confiscate sensitive data. India observed its first cyber-crime in 1999, wherein the defendant started services similar to those of Yahoo, using the domain name yahooindia.com. Phishing, in which the attacker

falsely impersonates a bank delegate and directs the victim to share his sensitive details, has increased so much that now getting access to someone's personal information has become very easy. Information security aims to defend computers and private data from malicious attacks.

The CIA triad combines three principles- Confidentiality, Integrity, and Availability, all of which function simultaneously. If either of the three does not work, the other two also get thwarted eventually. While dealing with large systems, these fundamentals need administration.

Confidentiality of data refers to the accessibility of information to authorized systems only. It is of enormous concern because of increasing data breaches over the last few years. Integrity means viewers can't change the information circulated by us without notifying us. Availability means if someone owns data, they should be able to access it in the time of need.

It is difficult to figure out what is more unfortunate between the two facts that India stands at third among the most cyber-victimized countries, with over 3000 reported cases, or there are no legitimate cyber laws.

So how are these crimes tackled, or how is the victim granted justice? In October 2000, the Parliament passed the Information Technology Act (ITA). Its focus is to regulate digital signatures and take action against the fraudsters involved in cybercrimes. It also states that they would punish a person of any nationality who tries to defraud any Indian citizen.

These cyber laws have various agendas. These include regulating the use of networks by companies and protecting consumers from online abuse. Some key facets where these laws are strictly required are security, fraud, contracts, copyrights, et cetera.

Cyber frauds have increased over the years to 4000 reported cases per month. Irrespective of the resources, people will always find alternative ways to harass the innocents' safety and privacy. It's high time now that stricter cyber laws get imposed in the country.

Saloni Gupta

Use of Machine Learning in Cyber Security

Machine Learning is the ability of computers to learn and react without being explicitly programmed. You can understand this better with the example of YouTube recommending new videos based on your search and watch history.

Machine learning algorithms are helping detect malicious activities faster and stop attacks before they get started. They can automate manual tasks.

Machine learning is already going mainstream on mobile devices, with voicebased controls such as Siri for Apple, Cortana for Microsoft, and Alexa for Amazon. But now we have an application for it's security, too. Google is analyzing threats against mobile endpoints using ML.

Machine learning is helping human analysts enhance all aspects of their jobs. Let it be detecting malicious attacks, analyzing the network, endpoint protection, or vulnerability assessment. According to research, the attack detection efficiency rate rises by about 85% when using ML.

An advantage of machine learning is automating repetitive tasks so that humans can be free to work on more productive tasks like creating security patches. Some organizations use ML tools to allocate human security resources and track threats. This frees up the workforce for critical tasks.

Word Search

V	I	I	L	C	R	R	G	D	G	R	F	N	R
I	S	S	K	S	O	V	V	O	R	S	W	G	R
R	T	O	L	K	O	C	W	W	H	K	V	N	O
O	C	N	F	U	Z	Z	I	N	G	O	N	I	T
B	L	A	C	K	L	I	S	T	G	G	K	H	O
R	G	T	K	A	P	E	P	N	I	A	Z	S	O
D	A	D	V	L	E	A	O	S	I	O	S	I	O
R	S	S	I	G	Y	K	W	Z	U	U	O	V	T
G	H	E	A	P	O	V	E	R	F	L	O	W	R
G	N	I	N	O	I	S	I	V	O	R	P	E	D
O	W	C	L	I	C	K	J	A	C	K	I	N	G
K	D	I	S	I	V	S	P	A	Y	L	O	A	D
P	A	S	S	W	O	R	D	S	P	R	A	Y	Z
S	A	S	V	A	T	R	R	O	O	T	K	I	T

Hints

- The part of the malware that carries out malicious activities.
- Software containing various malicious tools helpful for an unauthorized user.
- A list of specific unwanted files.
- A single common password that's tried for several usernames.
- The attacker can call any phone number with no toll-charge expense in this attack.
- Removal of access for certain users from software systems.
- A section of memory is written with no bounds checking done on the data.
- Tricking someone to press disguised webpage items.
- The process hopes to trigger an error condition or fault in a target.

Word Search Solutions

V	I	I	L	C	R	R	G	D	G	R	F	N	R
I	S	S	K	S	O	V	V	O	R	S	W	G	R
R	T	O	L	K	O	C	W	W	H	K	V	N	O
O	C	N	F	U	Z	Z	I	N	G	O	N	I	T
B	L	A	C	K	L	I	S	T	G	G	K	H	O
R	G	T	K	A	P	E	P	N	I	A	Z	S	O
D	A	D	V	L	E	A	O	S	I	O	S	I	O
R	S	S	I	G	Y	K	W	Z	U	U	O	V	T
G	H	E	A	P	O	V	E	R	F	L	O	W	R
G	N	I	N	O	I	S	I	V	O	R	P	E	D
O	W	C	L	I	C	K	J	A	C	K	I	N	G
K	D	I	S	I	V	S	P	A	Y	L	O	A	D
P	A	S	S	W	O	R	D	S	P	R	A	Y	Z
S	A	S	V	A	T	R	R	O	O	T	K	I	T

CYBERZINE 2021 | SEPTEMBER 2021

The Division of Cyber Security and Digital Forensics Highlights

REMEDIES FOR FINANCIAL FRAUD AND CYBER SCAMS

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

On 27 April 2020, VIT Bhopal, in partnership with Gujarat Forensic Sciences University, hosted a webinar on Financial Fraud and Cyber Scams Remedies. Dr. Digvijay Singh Rathod, an Associate Professor in the Department of Digital Forensics and Information Security at Gujarat Forensic Sciences University, spoke about Financial Scams and fraud.

A question-and-answer session followed this, clearing further doubts on the subject. Dr. S. O. Junare, Director of Gujarat Forensic Sciences University, then delivered a comprehensive session. He presented his knowledge and experience in Forensic Accounting and Accounting Systems.

Finally, Dr. Haresh Barot, Associate Professor at Gujarat Forensic Sciences University's Institute of Management and Training, demonstrated a presentation on Cyber Security in Internet Financial Services.

Overall, it was an incredible and impressive event that provided many opportunities to learn about being cautious with financial services and accounting online.

CYBER SECURITY AS A SERIOUS CAREER OPPORTUNITY AND NEW AVENUES

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

VIT Bhopal University hosted an expert talk on 4th May by Mr. Shaik J Ahmed on "Cybersecurity as a Serious Career Opportunity and New Avenues". The event started with a strong focus on information security.

Mr. Ahmed stated the increase in demand for cybersecurity and expressed that it is easy to learn as a subject. Further, he mentioned the steps to become cybersecurity professionals. He also elaborated on different cybersecurity roles.

Cyber security skills include networking, software development, system engineering, financial and risk analysis, security intelligence. The event ended with a vote of thanks.

CYVIT 2020

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

CyVIT is the premier annual event of the Department of Cyber Security and Digital Forensics at VIT Bhopal University. On 17th June 2020, the University witnessed the grand virtual inauguration of CyVIT 2020.

Vice-Chancellor Dr. P Gunasekaran, Dean of The School of Computing Science Dr. Manas Kumar Mishra, Division Head of CSDF Dr. Shishir K Shandilya welcomed Dr. Neal Wagner (Chief Guest), Dr. E Khalie Raaj (Guest of Honor), Mr. Maithili Sharan Gupta, Dr. Khalie Raaj, Dr. Vinti Agrawal, and Mr. Ebenezer Stephen, the guests for the day.

The welcome speech of the Vice-Chancellor, VIT Bhopal, Dr. P Gunasekaran, addressed Cyber Security and the events held in CyVIT 2019. He also talked about innovation and achievements in cybersecurity and VIT's rank of being the No.1 institution in cybersecurity. Dr. Manas Kumar Mishra, Dean, School of Computer Science and Engineering, welcomed Dr. Neal Wagner (Expert in Cyber Security and AI), Mr. Maithili Sharan Gupta (IPS officer), and Dr. Khalie Raaj (Additional Director General Nation, Cyber Safety and Security Standards). Dr. Shishir Kumar Shandilya, Division Head of Cyber Security and Digital Forensics, gave a briefing of the event. He mentioned that the event was one of India's largest Cyber Security Conclaves, provided us with valuable insight into different opportunities in cybersecurity, and laid out methods to work within the boundaries of cybersecurity.

Next was a very factual speech by Mr. Maithili Sharan Gupta on the relevance of digital services during the COVID-19 pandemic and the ever-increasing challenges of cybersecurity. He asked the audience to create awareness for cyber-crimes and how fear should be absent while using the internet. He also thanked VIT for associating all resources and appreciated the students and their efforts. Following this, our chief guest, Dr. Neal Wagner, honored the gathering with his insightful words. He spoke on Cyber Kinetic Combat Risk Assessment: A Hierarchical System of Systems Modelling Approach. Cyberattacks are ubiquitous in the government defense industry and critical infrastructure. He gave the example of cyberattacks in the USA in 2016 that had affected their presidential election. He also cited an example of attacks on the defense in 2018 where hackers could take over a navy ship. The lecture continued by assessing risk for cyber defensive mitigation, Microsoft EMET technology, Network segmentation, and a discussion on Markov Process for a network enclave and the Lanchester Model.

At the end of this insightful lecture, Dr. Pushpinder Singh Patheja gave the vote of thanks and invited Dr. Maithili Sharan Gupta to speak about the analogy of cybercrime and the importance of efficient tools and professionals to stop them. Mr. Mihir Haryal then spoke on the relevance of Cyber Security as an inevitable career. His points on the ability to hack the human body while discussing types of hackers were an eye-opener. An interactive question-and-answer round followed this. The fascinating and intellectual event concluded for the day.

The second day of CyVIT started with great zeal and enthusiasm. The event began with the valuable words of Mr. Govil Rajpal from Check Point Software Technology Limited, with his area of expertise including application delivery network, network security, application, and content security. He quoted Freedom of Privacy and Security, describing the need of the situation. He also shed light on the struggles of security and privacy in this digital way of life. He then discussed various viruses and even answered queries. An address by Mr. Rene Benard about blockchain succeeded this. There was a discussion about the dilemma of blockchain adoption in actual life and with enthusiasts about blockchain and cryptography. "Jack of all trades, master of none, but openness is better than master of none" was a fascinating twist to the old saying. It gave us a new perspective on things.

Another provocative speech by Ms. Vinti Agrawal, Associate Professor at Computer science and Information System Department, BITS Pilani, on Cyber Threat Intelligence using machine learning explanation and a case study on COVID lockdown and its effects on cybersecurity followed this.

The event came to a beautiful adjournment with the inauguration of CyberZine's 2nd edition and its aim to spread awareness about cybersecurity and educate people about recent developments in the field.

CYBER WARRIORS CLUB

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

VIT Bhopal University established the Cyber Warriors Club in the summer of 2021 to help students solidify their understanding of cybersecurity through a practical approach.

On the 10th of June, VIT Bhopal university hosted the grand launch of the Cyber Warriors Club's first virtual event, "Bon Hackétit."

On the first day, a webinar was held, which served as the foundation for understanding the crux of cybersecurity. The event kicked off with an introduction to the cyber world and pro insight into it. The driving idea of the event was to give an insight into the challenges, goals, importance, and prerequisite of cybersecurity. It also discussed hackers, their types; and provided a brief idea of defensive, offensive, and research-oriented domains. Speakers objectified the mandatory hard and soft skills required to carry off in the cyber-world. They came up with the elements encompassing the world of cybersecurity. And finally, it stressed the zeal to carry on in the cyber-world.

Furthermore, one of the understudies clarified and gave the possibility of CTF (Capture the Flag). He put forward the idea of CTF and its sort. He likewise referenced the most used tools identified with CTFs and shared valuable resources to practice them. The importance of CTF was also focused, helping in critical thinking, and expanding one's skillset. Finally, he projected on the need for utmost patience and passion while dealing with CTFS. After conducting such an informative session, participants enjoyed some fun events.

On the second day, Virtual Cyber Labs sponsored a six-hour CTF competition was held, including a variety of intriguing challenges for both beginners and intermediates. It was highly favorable for students to acquire new skills and broaden their knowledge base. It enabled them to demonstrate their abilities, enhance them, and earn prizes. The participants exhibited a high level of competence.

In the closing ceremony, they introduced the founding members of the club, who shared their experiences and their journey. A promise to conduct more such events and awareness events in the future was made. Moreover, the prize distribution ceremony commenced, and the winners were awarded free enrolment in the courses offered by virtual cyber labs. The top 3 participants received t-shirts from virtual cyber labs. The event ended with a vote of thanks to Dr. Manas Kumar Mishra, Dr. H. Azath, and Dr. Shishir Kumar Shandilya for their support and guidance to make it a successful event.

FRIGIDSEC

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

"By students, for everyone."

FrigidSec, VIT Bhopal's official CTF community, goes by this thoughtful motto. We incorporated it in August 2020 as part of the School of Computer Science and Engineering's Department of Cybersecurity and Digital Forensics. The official CTF team bears the same moniker. It is possible to exchange and receive knowledge by interacting with numerous other cybersecurity enthusiasts who participate in CTFs, secure coding challenges, conferences, and seminars, among other activities. Joining this club enables you to do that. Apart from that, the topics covered include reverse engineering, cryptography, and open-source intelligence (OSINT).

Furthermore, the FrigidSec CTF team regularly provides practice CTF challenges and solutions, providing ample opportunities for practice and a desire to learn for those who compete.

They have multiple achievements to their name, including landing the top 10 and top 40 spots in PhantomCTF and Arab Security Cyber Wargames, respectively.

VIT Bhopal University on 29th August 2020 witnessed a grand virtual inauguration of the FrigidSec CTF community organized by the CSDF division. The event started with a welcome speech by Dean, School of Computer Science Engineering, Dr. Manas Kumar Mishra, who extended a hearty welcome to all the guests, Vice-Chancellor, VIT Bhopal, Dr. P. Gunasekaran, and others present in the room. Further, Dr. Shishir Shandilya emphasized that CTF competitions are the best way to learn to hack, as they are very challenging and can help one develop many skills. He further explained the two types of CTFs; Jeopardy-style and Attack-Defense style.

Next was an introductory speech by student coordinator Saket Upadhyay for the CTF community. He said that the team is managed by students and guided by teachers and professionals. The community's target is to conduct cybersecurity conferences, tournaments, CTF events, talks, etc. Further, he talked about the community structure, transparent operations, an open-sourced framework, a well-structured collection of member experiences, and collective community knowledge on GitHub. Through this platform, students can spread awareness about cybersecurity to keep themselves safe in a virtual world. After that, he ended his speech with a video featuring all members of the FrigidSec CTF community.

Next was an introductory speech by Dr. Shirish Chandra Pandey, who leads the Red Hat academy at the apex level. He discussed Red Hat, which provides open-source software products to the enterprise community. It provides the curriculum to educational institutes to keep pace with the demand of the industry. Students learn practical skills rather than theoretical skills. After that, he talks about the Red Hat learning community. He also talked about data privacy and open-source software. There are many security concerns with open-source software. Security, and especially cryptography, is hard to implement and review in code.

The Vice-Chancellor's address about the CTF community and how it carries the flag of VIT Bhopal to another height of success followed this. The event ended with a vote of thanks delivered by Dr. Pushpinder Singh Patheja.

WICYS

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

WiCyS women in cybersecurity
VIT BHOPAL UNIVERSITY
STUDENT CHAPTER

WiCyS aims to promote women in the cybersecurity field. Diversity in the workplace is beneficial for any company's growth. Women in senior positions bring new ideas to the table and give a unique perspective on problems. WiCyS aims to bridge the under-representation of women in cybersecurity.

WiCyS student chapter of VIT Bhopal University perfectly embodies these ideals of WiCyS and is working towards training the upcoming generation of cyber warriors. Recently, the student chapter allowed its members to learn and compete in a secure code competition in collaboration with Secure Code Warrior.

WiCyS members have also taken part in the Mossé Cybersecurity Internship that will allow them to learn and upgrade their skills to industry standards. Apart from enhancing their skills, WiCyS connects learners with mentors who are industry professionals for guidance under the Mentor-Mentee program. These opportunities help promote women in the cybersecurity field and helps create a diverse workforce.

On 9th September 2020, VIT Bhopal University witnessed a grand virtual inauguration program of the Student Chapter of WiCyS. It is the first chapter of WiCyS in India.

Ms. Genie Sugene Gan (Head of public affairs and government relations in Kaspersky, Singapore), Ms. Satyavathi Divadari (Chief Cyber Security Architect and Principal Partner Advisor at Micro Focus, India), and Dr. Vitaly Ford (Director of Chapter Development at WiCys, USA) were the honorable guests of the day.

The event started with the welcome speech of the Dean of the School of Computer Science Engineering. He told how in Yajurveda, they define women as the life of all living beings and humans look up to women for all their solutions and how WiCyS plays a similar role in the world of cybersecurity for everyone.

Next, Dr. Vitaly Ford delivered an introductory speech about WiCyS. He expressed his excitement regarding the first Indian chapter of WiCyS and the career opportunities that WiCyS provides to the students through internships, industrial training, conferences, seminars, industry-level exposure, and even job opportunities to its student members.

"Women support society." These were the words from the Vice-Chancellor of VIT, Bhopal University. He was glad to share that the first batch of cybersecurity division in the college witnessed 25% of girls' admission, which further increased to 35-45% in the second batch.

Next, Miss. Gan expressed her views that men should be equal partners in women's empowerment. Women in cybersecurity cannot succeed without men coming on board. She presented data figures and mentioned that in the Asia-Pacific region's participation of women is below average. She concluded by stating that the sky's the limit, but you determine your sky one should take responsibility for their growth and finally implore oneself regarding what defines them.

Ms. Satyavathi Divadari expressed the need for a female chapter and underlined the importance of providing a platform to minorities in every field and giving them more strength by supporting them. She also threw light upon the increasing number of career opportunities in the field and advised students on working on some projects by teaming up with seniors or someone who knows better about the project to enhance their knowledge.

Finally, Ms. Bhawna Yadav, President of the WiCyS Student Chapter, VIT Bhopal, shared how establishing a WiCyS student chapter in the university came into the picture. After attending her first event, 'Security Free Enemies', of WiCyS organized in collaboration with Google Ethical Hackers, Ms. Bhawna felt so motivated that it was no longer just an organization to her but a place of like-minded people connected with a single string. She emphasized WiCyS is not to be confused as discrimination against men over women, but it is all about establishing an inclusive environment for everyone overcoming gender biases.

Dr. Kanchan Lata Kashyap, Senior Assistant Professor of CSDF division, VIT Bhopal, delivered a vote of thanks to all the guests and faculty who took out their time for the program by making it a success. She also congratulated Ms. Bhawna for her success after six months of hardships.

Thus, it was an exceptional event and an enlightening experience for the students and faculties of the Cyber Security and Digital Forensics division, VIT Bhopal.

Secure Code Warrior

WiCyS VIT Bhopal Student Chapter collaborated with Secure Code Warrior, OWASP Foundation Bangalore Chapter, and InfoSec Girls to conduct a Secure Coding Tournament on November 28th, 2020.

Before the tournament, Secure Code Warrior's Co-Founder and Customer Success Guru, Mr. Jaap Singh, delivered a perceptive and enlightening presentation on Dev to DevSec: Why Security-Aware Developers Are the New Rockstars. In this tournament, developers competed against each other in a series of vulnerability code challenges that included identifying a problem, locating insecure code, and fixing a vulnerability.

It comprised of different levels and gave a real-time experience of fixing the insecure code. The participants had 90 minutes to complete the levels. They provided various hints and related videos on the platform for the reference of the participants. They had the liberty to choose their favorite programming language and framework to complete the challenges.

The program concluded with the declaration of the winners and an appreciation note from Vandana Verma, InfoSec Girls.

This event provided exposure to women in the cybersecurity domain to secure coding and tested the participant's secure coding skills. It gave them a chance to win cool swags and gain real-time experience with secure coding.

Mossé Research Institute: MCSI Remote Internship

WiCyS VIT Bhopal Student Chapter, in collaboration with Mossé Cybersecurity Institute, brought in a remote training and internship opportunity for women who share their passion for Cybersecurity. On the Eighth of December 2020, they introduced the internship to the members alongside Mr. Harris Wassylko, Cyber Security Education Coordinator and Solutions Specialist at MCSI. This remote internship delivers the skills to bridge the gap between knowledge gained from a college or university with the practical skills employers expect their team to possess.

The skills members will learn from completing this remote internship program are:

- Perform network vulnerability scans.
- Exploit vulnerabilities with Metasploit.
- Identify and exploit web application vulnerabilities without tools.
- Write custom offensive security tools to aid Red Teaming operators.
- Assess the security settings of Windows machines and harden them.
- Hunt for malware using YARA.
- Hunt for threat actors on Windows networks using Python.
- Defend web applications against common vulnerabilities.

This internship will equip the students with the skills to become a valued members of any industry technology or security team and provide the rigor to research and deliver technology solutions. The WiCyS VIT Bhopal Student Chapter extends gratitude to Benjamin Mossé, CEO, MCSI, and Harris Wassylko, Education Coordinator, MCSI, for providing us with such a great opportunity.

How To Build Your Cybersecurity Startup

On February 28th, 2021, WiCys VIT Bhopal Student Chapter conducted an interactive session with Ms. Shifa Cyclewala on How to Build Your Cybersecurity Startup. She is the founder of Hacktify Cyber Security, a startup that envisions secure cyberspace.

Ms. Cyclewala explained that the Cybersecurity Job Market Remains Hot despite the COVID-19 downturn. According to her research, there were 261,545 cybersecurity job postings on LinkedIn during the COVID slump. These numbers keep on increasing as ransomware attacks on critical infrastructure like hospitals increase.

In her experience, one must have Strong Fundamental networking skills and programming skills for entry-level jobs in cybersecurity. Internships and certifications like EC Council, CompTIA, e-learn, and Offensive security certifications add to your resume. She also encouraged attendees to practice bug-bounty hunting and resume building.

Commenting on her personal experiences, she believes that as an entrepreneur interested in establishing a cybersecurity startup, strong fundamental networking skills, OS, Mobile, OWASP, SANS, and programming skills are required. But most important is a new idea and a spark to solve a problem. An entrepreneur must have strong communication skills and a like-minded team.

She believes that there is more digitization in India, increasing the need for cybersecurity startups. She also gave details of several government funds for startups. Most of the government documentation for startups is online. In her overall experience, one needs 3-4 years of professional work and certified staff with infosec certifications to get government projects for your startup.

She answered various questions that the attendees had in the question-and-answer session. The attendees learned a lot from her talk, and Ms. Cyclewala addressed their doubts and questions diligently.

Ransomware Attack: How can an organization be prepared for the changing security threat landscape?

On 20th June 2021, the WiCyS VIT Bhopal student chapter organized an online panel discussion event on one of the trending issues in the security space: "Ransomware Attack: How can an organization be prepared for the changing security threat landscape?". The event started at 11:00 AM through the official channel of VIT Bhopal University.

Ms. Aarushi Koolwal, the moderator of the panel discussion, welcomed the audience and the esteemed guests of the event; Ms. Vandana Verma, Security Director at global board OWASP and founder of Infosec Girls; Ms. Genie Sugene Gan, Head of Public Affairs and Government Relations, APAC Kaspersky; Ms. Preeti Bhisikar, Relationship Manager, APAC and MEA, IBM Indian Army Veteran; and Mrs. Sarba Roy, Product Security Consultant, Umpqua bank.

The panel discussion encompassed various solutions, loopholes, and best security practices, considering the ransomware attack on the Colonial Pipeline network in the USA. The experts discussed the importance of general security awareness and how infosec communities help in achieving this goal. They conducted the event under the supervision of Dr. Shishir Kumar Shandilya and Dr. Kanchan Lata Kashyap. Ms. Bhawna Yadav, President, WiCyS VIT Bhopal Student Chapter, delivered a special vote of thanks to the guests towards the end of the event.

WiCyS Social media Campaigns

Apart from the various year-round events, WiCyS also holds various campaigns on its social media pages to commemorate unique international events.

WiCyS VIT Bhopal student chapter organized a “Tell us your warrior story” campaign on International Women’s day, 8th March 2021. They encouraged participants to submit posters, videos, poems, and stories that depicted the warrior that resides in every woman. With 27 submissions, WiCyS brought in a wave of motivation and positivity for all women warriors.

SECURITY STRATEGIES FOR YOUTH IN CYBERSPACE

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

On October 27, the CSDF division of VIT Bhopal University hosted an expert talk by Dr. Varun Kapoor on Security Strategies for Youth in Cyberspace.

The event began with an engaging introduction by Dr. Varun Kapoor, the keynote speaker. He discussed his work experiences in five distinct mainlands.

.

He believes that the virtual world poses a threat to public security. According to him, cybersecurity is achieved through awareness and sound judgment, and the means of achieving that security is you.

He discussed his motivations for establishing the Black Ribbon Initiative's cybercrime awareness strategy.

He also discussed the Internet's applications, the first and most critical being data collection and sharing. It is without a doubt the most popular application, with over 2 trillion people visiting Google each year. The second application is for business management, which primarily entails net banking and online payments. The third category is correspondence, which encompasses telephone calls, text messages, and association. The fourth application that shapes organizations are interpersonal interaction. The fifth application is a diversion that incorporates the time spent on the previous four.

He emphasized the importance of parents monitoring their children's online activity. He discussed the Digital Crimes that affect children and adolescents, including online harassment and cyberbullying, cyberstalking, and online gaming. He used anecdotes and statistics to illustrate the negative impact these activities have on young people's mental health. According to him, phishing is the foundation of all digital crimes.

While concluding, he highlighted the central issues of well-being and security. Aseem Pandya concluded the meeting with a vote of thanks to Dr. Varun Kapoor for educating the students about general security practices.

CYBER4U

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

On 23rd and 24th January 2021, VIT Bhopal conducted a nationwide workshop, “Cyber4U” (Cyber for You), on the theme of “Future Ready Skills” so that the students of technical background can understand current cybersecurity technology used in daily lives.

The workshop was conducted for two days and was free of cost. The workshop included introductions to cybersecurity, digital forensics, and several competitions. The aim of the workshop was twofold. First, to make students aware of the current state of threats to security and privacy. Second, to provide hands-on training on the tools required for cybersecurity. To make it appealing, some challenges related to cybersecurity were also there, and rewards to those who performed best in the challenges.

On the inaugural day of the event, we conducted some informative talks, interactive sessions, and a contest based on digital forensics.

On the second day, a demonstration of the forensic investigation process took place. Afterward, we held a CTF competition based on cybersecurity challenges. Towards the end, we announced the winners for the two contests, followed by a prize distribution ceremony.

CVE TEAM

THE DIVISION OF CYBER SECURITY AND DIGITAL FORENSICS

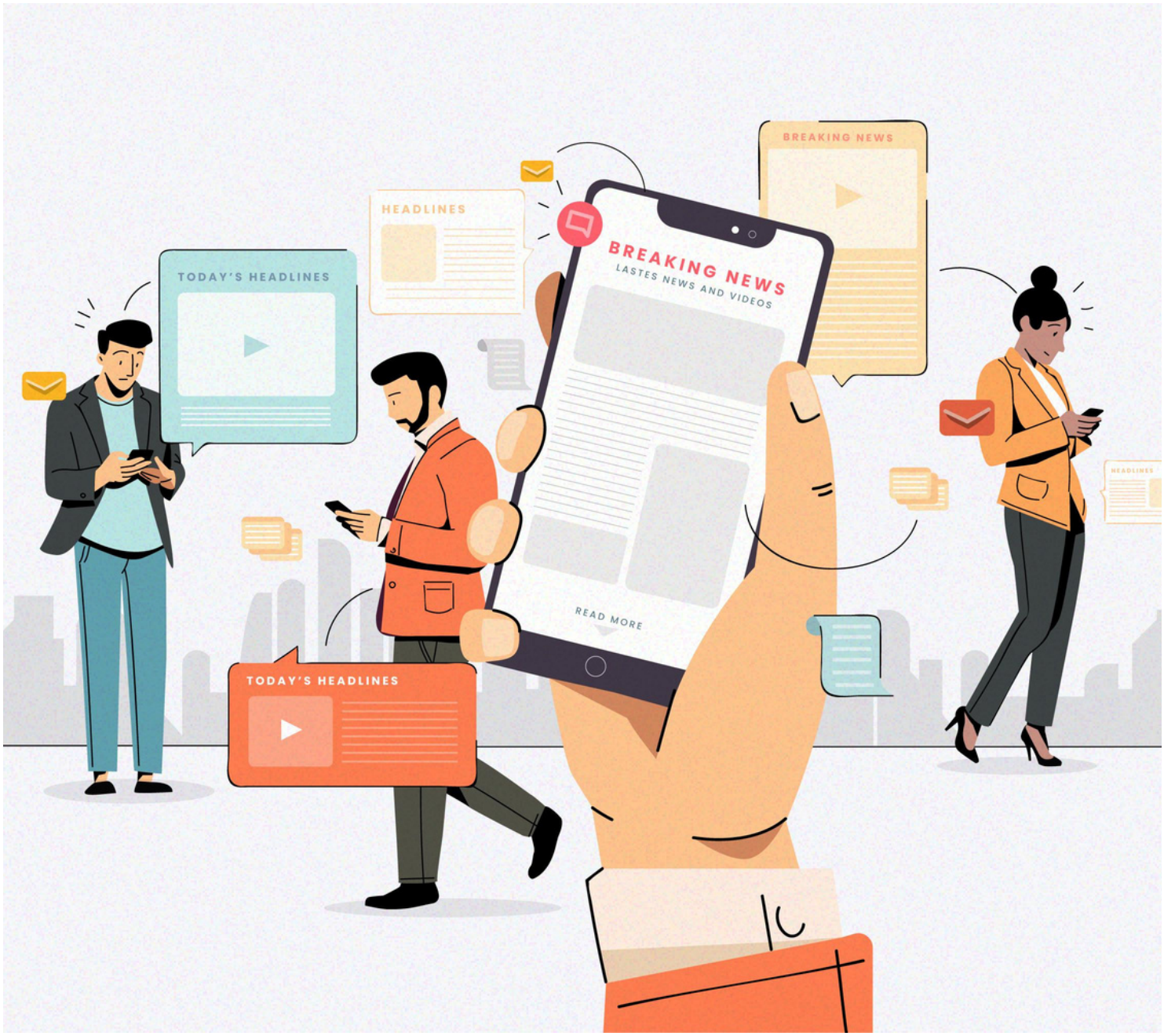
Some organizations maintain a list of computer security flaws in online databases, sometimes open to the public for viewing as a part of global threat intelligence. This list of computer security flaws is known as CVE (Common Vulnerabilities and Exposures), and it is updated regularly. Developed by MITRE in 1999, CVE is a tool for identifying and categorizing software and firmware vulnerabilities. Organizations can benefit from the use of the CVE's free cyber security dictionary. The CVE's mission is to make it easier for organizations to share vulnerability information. They accomplish this by assigning a unique identification number to each vulnerability or exposure.

Several Ethical Hackers and Pen-testers from VIT Bhopal University are on the lookout for security flaws in various computer products. They report these flaws to the appropriate authorities following ethical hacking practices. In the end, the goal is to make the Internet more secure by identifying security flaws and issues in a variety of products and services. After that, they notify the organization of the vulnerability and work together to solve the problem. They then apply for a CVE identification for the specific vulnerabilities so the organizations using that product can be made aware of the issue and secure their system. They discovered three different vulnerabilities in the widely used document management system SeedDMS and were assigned three CVE identifiers (CVE-2021–35343, CVE-2021– 36542, and CVE-2021–36543) within a few days of getting to grips.

CYBERZINE | SEPTEMBER 2021

CYBER ATTACKS

BIGGEST CYBERSECURITY ATTACK HIGHLIGHTS



DÜSSELDORF UNIVERSITY HOSPITAL RANSOMWARE ATTACK

CyberZine | Ghanishth Goyal

The Düsseldorf University Hospital faced the brunt of an unethical hacking, a ransomware attack. The IT system eventually got compromised and affected systems and data access. Because of the attack, the hospital could only take in 50% of cases. Though they could take care of the already admitted patients, the doctors had to postpone surgeries because of the loss of records on the patients. The system failure also costed the life of a 78-year-old critically ill woman. The woman needed urgent admission but had to shift to another hospital around 20 miles away, causing a delay of an hour in her treatment and ultimately her death.

The encrypted message displayed on around 30 servers of the hospital contained the instructions to contact the attackers to discuss ransom terms. However, they were meant for Heinrich Heine University and not the hospital.

The attackers got informed that they misfired and were putting patient's lives at stake, after which they withdrew the ransom condition and provided a decryption key.

AIR INDIA DATA LEAK

CyberZine | Ghanishth Goyal

In a cyber-attack on the data processor of Air India, occurring in February 2021, the data of around 45,00,000 individuals was made public; this included the passengers' personal and financial data. They launched this attack on Air India's SITA PSS data processor.

The targeted processor stored and processed the personal information of passengers. This attack compromised all the data of the past ten years, including the booking history, the personal and financial information (such as credit card details), and frequent flyer data of the customers.

According to an Air India member, the breach involved all information registered between 26 August 2011 and 20 February 2021. But, the security details for credit cards such as CVV or CVC numbers were not stored on the targeted server and are safe.

FLORIDA WATER SYSTEM SECURITY BREACH

CyberZine | Ghanishth Goyal

A hacker breached the security of the Florida Water System by using a remote access software platform, Teamviewer. The attack happened twice in the day, at 8.00 am and 1.30 pm. The malicious attacker tried to poison the water that got supplied to approximately 1500 people.

According to one of the workers present there, the mouse on the screen started moving automatically and started increasing sodium hydroxide and Lye to over 100 times its defined level. Sodium hydroxide, the key ingredient in liquid drain cleaners, is used to control water acidity and remove metals from drinking water.

Furthermore, Lye poisoning can cause burns, vomiting, severe pain, and bleeding. After the attacker exited the computer, the worker returned the Sodium Hydroxide and Lye levels to normal after the whole event was alerted to the officials.

According to Pinellas County Sheriff Bob Gualtieri, the water system had safeguards, which would have stopped the poisoned water from getting released. So, the public was safe.

RANSOMWARE ATTACK

CyberZine | Ghanishth Goyal

The Taiwanese tech giant Acer suffered a ransomware attack suspected to be orchestrated by a hacker group known as REvil. The same group of hackers is also associated with 2020's ransomware attack on Travelex, a London-based foreign exchange company.

The cause of the attack was apparently a vulnerability in the Microsoft Exchange server, which helped the attackers gain access to Acer's back-office network. They also leaked data consisting of financial spreadsheets, bank balances as well as bank communications.

This attack has also made a new record, as the hackers demanded US$50,000,000 in exchange for the decryption key.

After negotiating with the group, the company settled the deal with a 20% reduction. Luckily, the ransom was paid on time. Causing a delay in payment could also have steeped the price from US$50 million to US$100 million.

JUBILANT FOODWORKS DATA LEAK

CyberZine | Ghanishth Goyal

Jubilant FoodWorks, which runs the Domino's Pizza Chain in India, faced a cyber-attack in which around 13 TB of data of nearly 18 crore orders got leaked.

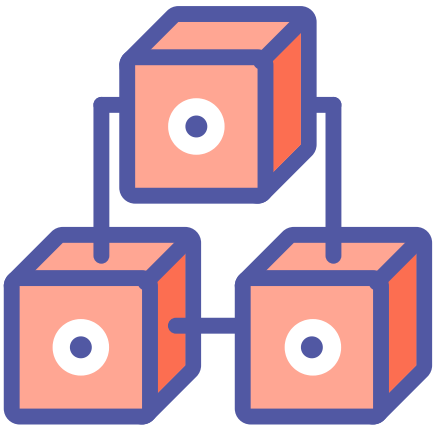
Customer's details, such as name, phone no, order history, and GPS location, were made public on the dark web. According to the company, the attackers didn't leak any financial data.

The official statement by the company's spokesperson was, "As a policy, we do not store financial details or credit card data of our customers. No such information has been compromised.

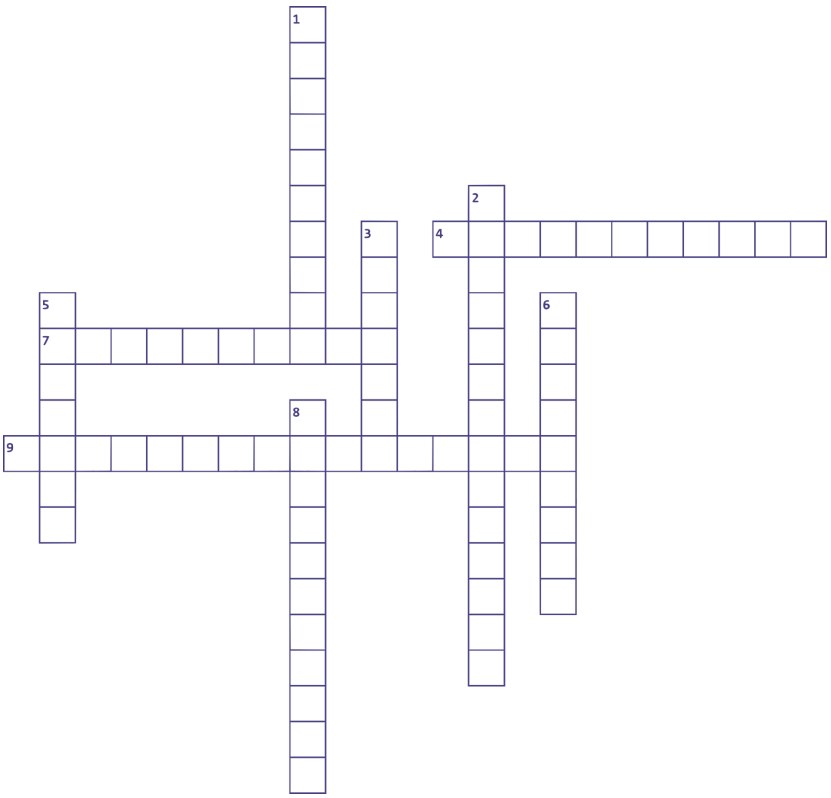
Our team of experts is investigating the matter, and we have taken necessary actions to contain the incident".

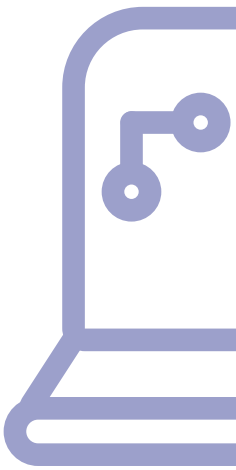
But according to an Israeli cybersecurity expert, the hacker put up data of Domino's India for a sale of $550,000 per buyer. The data included details of Domino's India's customers and employees and sensitive data such as names, emails, phone numbers, and credit card details.

BLOCKCHAIN CROSSWORD



Answer the questions below by filling in the blanks in the puzzle.





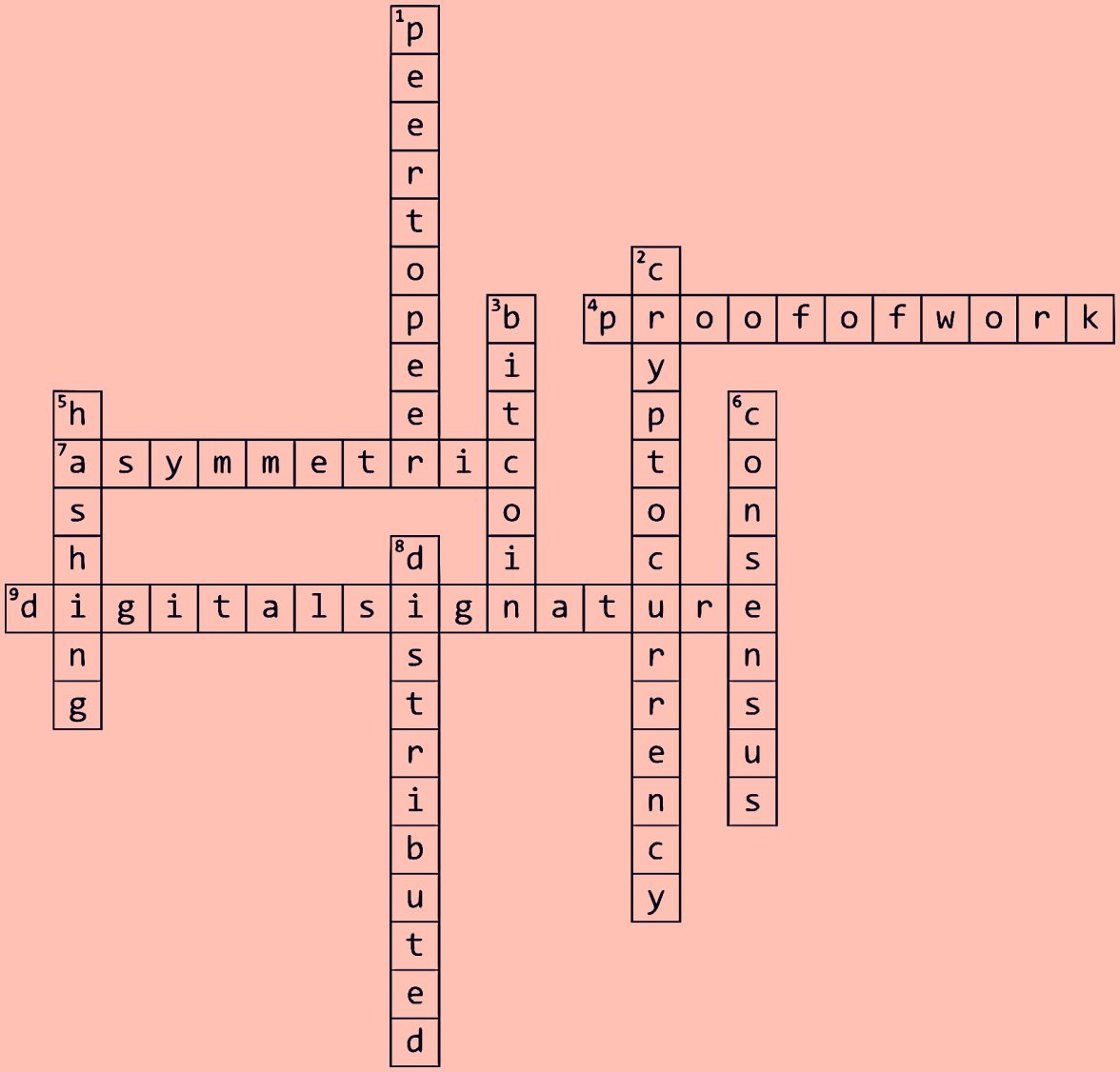
ACROSS

4. I am the proof of computational effort spent for some purpose.
7. I am a type of encryption that doesn't have the same encryption and decryption key.
9. I help overcome fraudulent signatures.

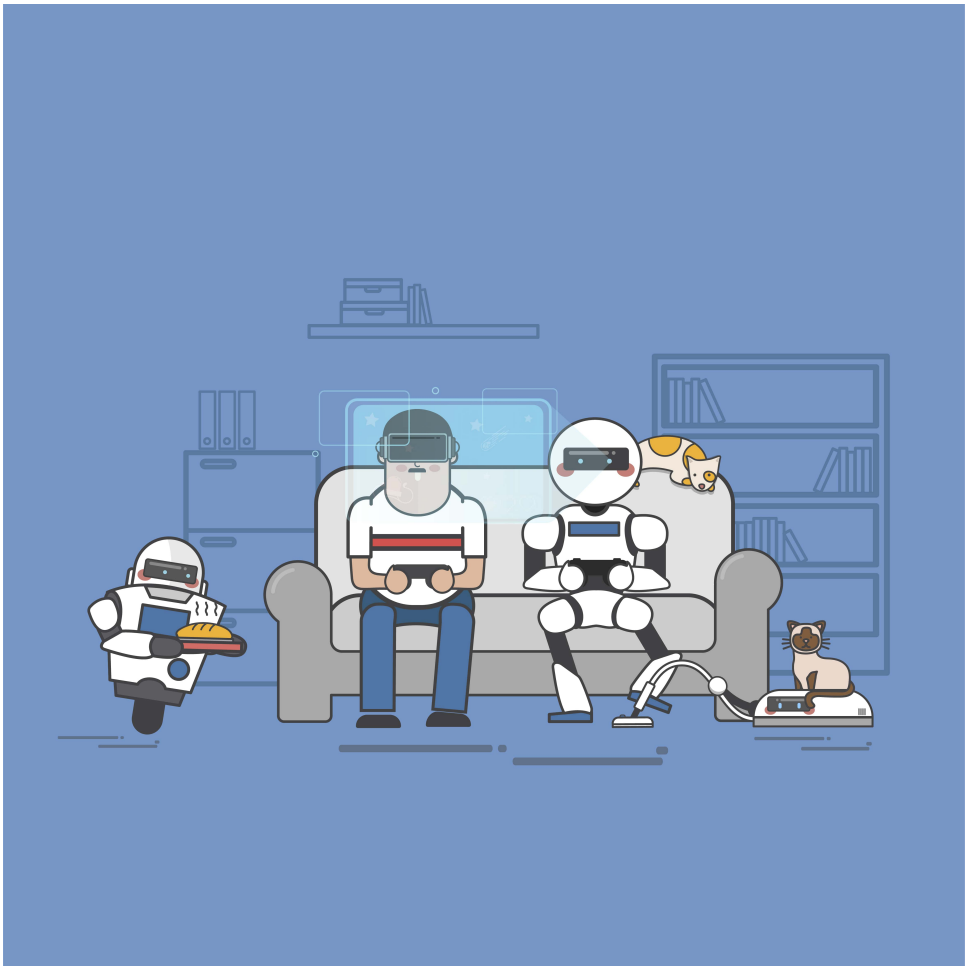
DOWN

1. I am a network. I won't talk to a third party. I will only talk to you directly.
2. I am a virtual currency secured by cryptography.
3. I am the most popular cryptocurrency to date.
5. I show the Avalanche effect and produce unique codes.
6. I am an agreement used for authentication and validation of a value or transaction in a blockchain.
8. I am a decentralized network.

Blockchain Crossword Solution



Foul Play



Gaming has become a significant part of our lives. It can be highly addictive and competitive and is also a growing profession. The gaming industry has reached new heights in terms of technology and quality. Unfortunately, the growth of hackers has been proportional to the industry. They have started exploiting this rising interest and

ambitiousness. Gamers have become an easy target because most of them are ready to buy special weapons, powers, use cheat codes, and even download modified versions of the same game. They usually have a common password which, when compromised, creates a pathway into all their accounts. Firms are consistently under pressure to release new games and levels, giving rise to more security loopholes. All these reasons combined reinforce the hackers.

Hacking and using cheats to win a game has become common. Although it seems harmless, it ruins the gaming experience. It even drives consumers away and decreases the profits of the company. Using hacks in games is like using steroids in the digital world. Although it's difficult to cheat in tournaments because of the strict rules and controls, it's easy to do it when playing at home. There exists an entire market of people who exploit game vulnerabilities and create cheat codes.

This talent is not only being used for winning but for exploiting as well. Gamers have become an easy target for all the black hat hackers. Making people click on an anonymous link has become effortless these days.

We download games from the Google Play Store because we consider them safe, but they aren't. A digital security firm called Avast found that there were several harmful mobile applications targeting gamers. These mobile applications use a method called fleeceware, a new technique of cybercrime. Under this technique, they offer users modifications for a short period of a free trial, and after time passes, fraudsters slowly start charging exorbitant costs. They expect to keep earning money from them. Scams of such nature are harmful to those who do not read the details of every app they download.

Phishing is another such way through which hackers are targeting gamers. They set up false, harmful, and yet, convincing emails and websites related to video games and lure you into giving your login credentials. Knowing how to spot a bogus website is a trick that might come in handy. Such a website might have grammatical mistakes or a false sense of urgency. It will be very general in its way of addressing. We can also check if the email or website has a public presence on social media pages, making it a trusted source. With each year, these false websites have become more and more reliable and persuasive. DDoS attacks and Teslacrypt are some other types of hacking attacks witnessed by this industry.

Being informed is the first and most critical step to safeguard oneself. A few responsible moves can help you. Using strong and different passwords for all your accounts, downloading games from trusted sources after reading its reviews, avoiding clicking on unknown links, especially in multiplayer games, and keeping your system updated with the latest anti-virus systems. As said by Window Snyder, an American security expert, "One single vulnerability is all an attacker needs."

Dark Web, Not Dark Alley

When we use cryptocurrencies for daily transactions, we often look at them as investment instruments. As the COVID-19 crisis is increasing day by day, some are using the darknet for illegal marketing. To people's surprise, darknet activities are low at this point. Darknet users often deal with Bitcoin to complete their transactions for buying illegal goods and drugs. They don't care about the market volatility, and the number of darknet activities has remained the same. But now, the scenario has changed. The reasons cited are that the COVID-19 pandemic has got people thinking more about their health than buying illegal drugs. As European and Asian countries are under complete lockdown, it has affected the overall business.

Looking at several other patterns affected by the pandemic environment, the market has also taken damage. In the present situation, people are purchasing only commodi-

ties. They have halted their activities in countries such as India, where there is a total lockdown, they have suspended operations; online shopping has taken a massive blow.

Why Do Drug Sellers See Internet as Remunerative Protection?

After the demise of the world's first drug crypto market, SILK ROAD, the dark web is the home to thriving trade in illicit drugs. Hundreds of thousands of people are selling drugs, and we refer to them as vendors. The dark web offers vital anonymity to vendors and buyers with the use of Bitcoins for transactions. According to a survey, 13 Darknet drug vendors are supplying illicit drugs to people amid the pandemic for curing people alongside face-masks. The darknet market gives lucidity to vendors and coronavirus scammers who exploit the current crisis to earn a quick buck! Dark web drug dealers have resorted to selling face-masks and fake coronavirus testing kits amid the pandemic. Coronavirus scammers in the UK have pocketed over one and a half million pounds so far through phishing attempts, seeking illegal donations, and exploiting pandemic-related fears by selling daily essentials and cures.

Users who used to market illicit drugs now sell Personal Protective Equipment (PPE), unverified antibody testing kits, and medications instead for £35 each. We see vendors selling medicines despite not involving themselves in the sale of PPE kits.

Illegal drugs smuggled into the UK have dropped in the face of international lockdowns. Earlier, the National Crime Agency warned that the pandemic had led to £1.8 million in fraud. Since the virus outbreak, it shut down six domains to stop cyber-attackers from attempting to steal personal data. Investigators also arrested two men on suspicion of illegally selling COVID-19 testing kits and making false agreements about their efficacy.

On 2nd April 2020, a notable darknet journalist called Eileen Ormsby from Tor-Hosted darknet marketplace stated that the platform reserves the full right to ban any vendor or scammer who promotes fake coronavirus vaccines or cures. Darknet markets experienced an inundation of users ever since people have been staying indoors. Due to complete lockdown, many countries have completely shut off online sales of non-essential items.

According to a Twitter survey, we observed that Bitcoin Ransomware Ryuk is wreaking havoc everywhere in healthcare systems and targets vulnerable hospital management across the US. They have shown no form of mercy amid the pandemic, so some people have come forward to express solidarity to those affected by COVID-19 and discouraging coronavirus scammers from exploiting challenging times to target the helpless.

Thus, hoping that darknet platforms adhere to the rules and regulations set and stand in unity in this uphill battle against the unceasing infection.

Privacy Policy or Controversy: WhatsApp

Facebook has owned WhatsApp since early 2014. Even after the companies combined, the data of Facebook and WhatsApp has always been separate. But now, the companies are thinking of merging their policies. We expect the latest policy update to

come into effect soon, whether or not users agree to it. This policy might also affect the overall popularity of the application. Its July 2020 policy update has already alluded to its complete data is being shared with Facebook. But at that point, after witnessing the reaction of the general people, they made sharing optional. What remains to be analyzed is whether WhatsApp's dedicated users are comfortable enough with such an emerging policy to stay connected with the app or not.

Looking back at the past month, clients did not have any idea about this decision. Some of the personal data that WhatsApp gathers incorporates:

- Client telephone numbers.
- Other telephone numbers are put away in the location guide.
- Profile names.
- Profile pictures.
- A status message, including when a client was last on the web.
- Symptomatic information from the software log.

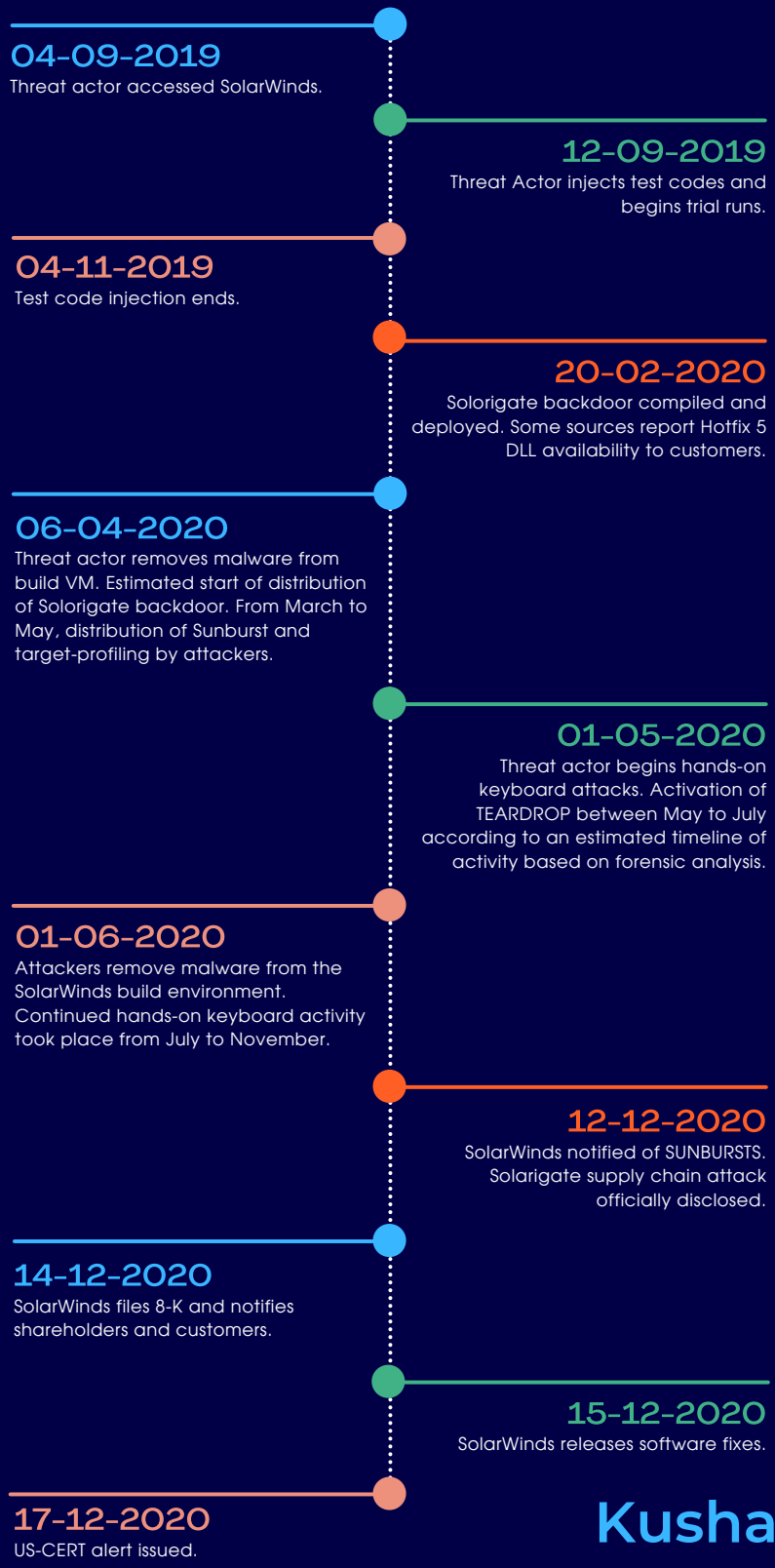
Once, a company like Apple had also altered some of its monitoring policies. But they gave their users the option to not accept the ad tracking on an app basis. Likewise, Facebook will lose benefits because of the new updates. Facebook's advertisement domain is worth more than $70 billion. That is why Facebook omits the advantage they are earning.

As the company's spokesperson stated, changing the policies was crucial for organizations to store and track WhatsApp visits using Facebook's principles. Clients will always have the alternative of not using WhatsApp. The company said there might be no change in how WhatsApp shares personal data with Facebook for non-business purposes. Individuals can always switch to other messengers if they have issues with the new terms and conditions.

SOLARWINDS ATTACK:
A Timeline

SolarWinds Inc. is an American MNC founded in 1999 that makes software for businesses to help manage their IT infrastructure. Their product, Orion, helps monitor the network performance of over 33,000 customers.

The attackers that attacked the Orion software framework did so by inducing a DLL file that remained dormant for a while and ran small test codes which went unnoticed. They remained non-aggressive and moved in a lateral direction, hopping from one server to another without alarming anyone. So, before they even began the full-fledged attack, they were already deep in the network framework of the clients.



Kushagra Pandey

OSINT: Workflows, Benefits, and Challenges

OSINT stands for Open Source Intelligence framework. The intended purpose of OSINT is to gather information from free resources for a relevant cause. For instance, viewing someone's public profile on social media is OSINT. Using their login credentials to get their personal information isn't.

OSINT workflows

Just like every other intelligence, OSINT requires methodologies too. Since OSINT offers a vast amount of information, it is essential to follow a workflow that determines that the result will be sophisticated.OSINT workflow comprises mainly three steps.

The first step is the collection phase, wherein we retrieve publicly available data from relevant open sources.

Second, we filter the data to generate valuable information through in-depth analysis.

At the last stage, we take the purified information as input for sophisticated interface algorithms. This step generates a final report.

Benefits associated with OSINT

OSINT offers an extensive amount of applications. One of the significant advantages is that it is cost-effective. Collecting OSINT is cheaper than any other intelligence. It also contributes a humongous amount of information with a high computing capacity. Besides this, the structure of OSINT is open enough to include data from open-source systems. Machine learning algorithms, along with data analysis and mining, will be pivotal in future OSINT activities.

Challenges associated with OSINT

OSINT offers a tremendous amount of data. It creates a complexity of data management and poses a challenge to handle it effectively.

Structuring a massive amount of information becomes difficult and results in an unorganized collection of data. Though OSINT offers resources, not all of them are reliable. Hence, there might be cases of misinformation linked to OSINT. Since OSINT is a vital means of spotting sensitive information in the public domain, malicious actors can abuse it to compromise data.

After all the information about OSINT, the real question arises; why should we learn OSINT? First, it provides us with a lot of information about organizations, restaurants, solutions to our problems, social media profiles, and whatnot. Second, it supplies us with knowledge about vulnerabilities, software releases, and many more. OSINT can protect citizens, as it applies to criminals, law enforcers, and the government.

OSINT is both a valuable tool for raising security awareness and a technical apparatus for identifying security risks. It's also capable of bringing down the security organizations if exploited by malicious actors. With the rise of social media and the internet, OSINT subsequently gained its relevance and is expected to expand even more.

MITM Attacks

A man-in-the-middle attack is focused on the technical side and doesn't require interaction between the attacker and the victim. A man-in-the-middle attack happens when the attacker eavesdrops on a conversation. This information is for sharing between the client and the website they are visiting. A man-in-the-middle can intercept this connection before it reaches the client. Then the website can make a connection. One of the most common ways is to set up free Wi-Fi without a password and make it seem legitimate. A Wi-Fi network named "Starbucks 5G" looks legitimate if you are at Starbucks, but once you connect with it, the attacker can look at the websites you visit and any sensitive information you enter on a website.

A MITM attack involves intercepting the network, getting the key, decrypting the data, installing the decoded data, re-encrypting it, and finally sending it back. This way, the client and the website get the expected information back. The MITM then receives the

desired information.

A common analogy to understand a MITM attack is to imagine talking to a friend in a crowded place. You might think that no one else would pay attention to you, and you continue talking, but a stalker could sit right next to you, pretending to be busy while noting the tiniest bit of information about you.

Now, suppose you realized that someone could listen to you talk about something sensitive. What would you do? HTTPS extends HTTP, where the S stands for secure. The information shared on websites using HTTPS is encrypted using Transport Layer Security (TLS). A website URL using TLS has a padlock next to it in the chrome browser. A website using HTTP would have ”Not secure” written next to it. Most of the websites nowadays are moving to HTTPS, making MITM attacks ineffective.

Some ways we can still protect ourselves from MITM attacks are: -

- Avoid connecting to public Wi-Fi connections.
- Avoid entering sensitive information into websites over any network other than home.
- Do not use websites that do not use HTTPS
- If there is no other way, then at least use a VPN before connecting to public Wi-Fi or entering a website that does not use HTTPS.

SQL Injection: It's Prevalence and Dominance over other Vulnerabilities

SQL injections have been ubiquitous for decades now because of their extensible nature. Unlike some other vulnerabilities that can be found and patched with an excellent defense mechanism, SQL Injections continue to persist to scourge web development to a large extent. They are an attacker's favorite vector because of their easy implementation and malicious potential.

OWASP defines a SQL injection attack as the

insertion or injection of a SQL query via the input data from the client to the application. Injections have been at the top of OWASP's top 10 list of vulnerabilities since 2013. Injections are more inclusive and cover other arenas like networking hardware, application code, and much more. There must have been some solid reason for its clear dominance over other vulnerabilities for over eight years.

Dependence on traditional SQL databases

Most web pages still run traditional SQL databases like MySQL and Oracle. User-defined data is quite sensitive and may contain confidential information like passwords, contact details, business information, et cetera. It is one of the major causes of SQLi and exposes these web pages to a higher risk.

Outdated code and unpatched applications

Let us take an example of a shopping website that was coded and launched six years ago. Over time, security considerations change, and the classes of vulnerabilities change too. We need to update every web page as per the current security standards. Running patched versions of software plays a crucial role in the security infrastructure.

Blind trust on the user's inputs

Web pages trust the input that is entered by the user as is and store it in their databases. The developers often overlook verification and assurance of the safety of the data entered by the user. It becomes easy for the attacker to break into the web page through the input sections; the search bar, the comment section, or any way users can interact with the website. Hence, validating the user input is as important as sanitizing your hands before eating in the current situation!

Ignorance and low capital investment in the security infrastructure

Security is growing day by day, and hence web pages need an optimal investment in the security infrastructure to prevent possible data breaches and attacks. Securing data should not just be perceived as a wall or a single layer of protection. Layered security is essential here; multiple layers make it harder for adversaries to penetrate the network. A proper security framework requires capital investment in securing the data.

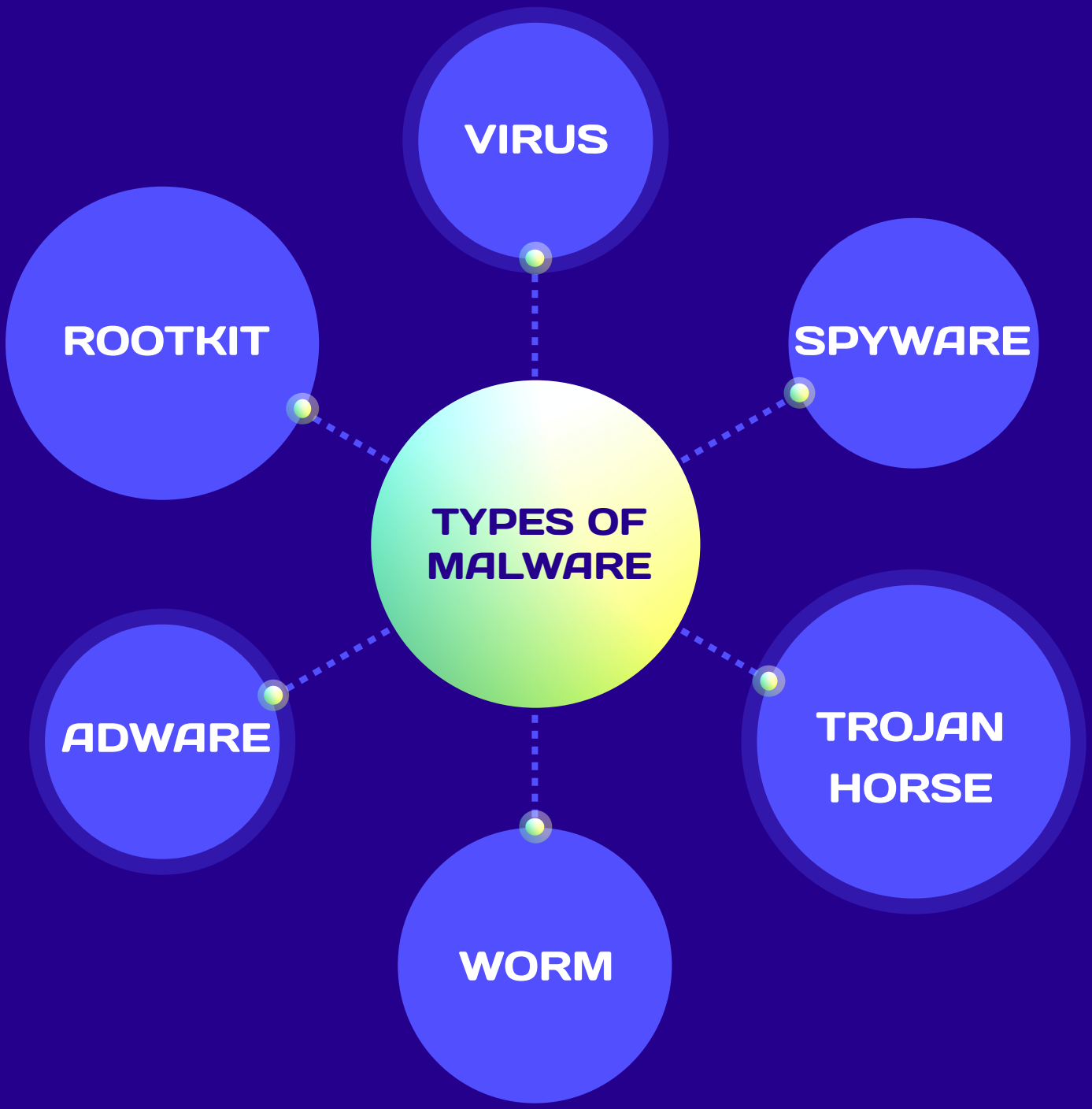
Conclusion

Different SQL injection attacks are prevalent today, as they are easier to find and implement than other exploits and bugs. Adversaries use SQLi to carry out malicious tasks, like retrieving or altering application data, subverting the application layer, fingerprinting a database, and so on. Even though organizations have introduced several security measures to prevent SQL injection, attackers have remained one step ahead.

THE BASICS OF MALWARE ANALYSIS

JAYANT VERMA

Any program that is made for gathering sensitive information or gaining access to computer systems and networks is malware. Malware analysis is the art of detecting malware to grasp how it works and how to defeat or eliminate it.



STATIC ANALYSIS

1

BASIC SCANNING

In Static Analysis, we run an executable through different scanners which can detect malicious content in it. Virustotal is a free online scanner that analyzes files and enables the detection of malicious content in it.

2

HASHING TECHNIQUE

It is used to uniquely identify malware. Each malicious software is run through a hashing program that produces a unique hash for each malware. The MD5 hash function is most commonly used for malware analysis.

3

BINTEXT

It is used to display all the strings within an executable. An executable contains a string if it prints a message, connects to a URL, or copies a file to a specific location. Through these strings, we can get an idea of the working of the executable. If the executable is packed or obfuscated, no useful strings will be seen.

4

DEPENDENCY WALKER

It has built-in tools that can check for dynamically linked lists within an executable. It can list out all the dependencies and libraries in the executable. Identifying the dependencies can sometimes help us recognize what the program does.

5

IDA PRO

IDA Pro is a multi-platform disassembler that can translate assembly-level code into source code. It can display the code as text or as a graph with zoom and mapping capabilities. It can help identify what an executable is doing.

DYNAMIC ANALYSIS

1

MONITORING TOOLS

Using procmon or Process Monitor, we can monitor all system calls made by a process and all resources it uses. Process Monitors can display currently running processes as a graph or a tree, making it easy to monitor.

2

REGSHOT

Regshot is used to take snapshots of the Windows Registry Hive and compare it with other snapshots. Since the Windows Registry contains all the essential system settings and variables, monitoring the registry can help determine traces of malicious activity.

3

NETWORK ACTIVITY MONITOR

For monitoring network activity, we can use Apate DNS and Wireshark. Apate DNS can check all the DNS requests made by an executable. Wireshark is a packet sniffer that can monitor the network activity on a particular network.

4

DEBUGGER

We can examine the execution of malware using a low-level debugger like Ollydbg or Windbg. The main objective of a debugger is to catch bugs. However, we can use a debugger to run a target program under controlled conditions. Debuggers can also allow us to pause the execution of a target executable and examine its current state.

I2P Network:
Is it safer from VPN and TOR?

Darkweb. This word alone is a complete image of what it has on the inside. Most illegal black-market activities happen on the dark web. Given the terrifying image that the Darkweb has, individuals should perceive that anonymous data access may lead to a privacy breach. They should know the consequences and take it on themselves to ensure the freedoms associated with them. One of the most efficient, reliable, and safe tools to do this over the web is I2P.

I2P: Brief Introduction

Invisible Internet Project or I2P is a decentralized anonymous network layer-based router implemented as a mixed network. The I2P network is very similar to the Onion Router. In contrast to TOR, it allows censorship-resistant peer-to-peer communication. They achieve it by encrypting the traffic and directing it towards the volunteer-run network, constituting several

computer systems spread over the world. It also employs Garlic routing rather than Onion Routing.

With I2P, the term Garlic Routing refers to the layering of the encryption process just like in Onion Routing and bundling the unique pieces of information just like a clove. Garlic routing provides the users with the benefit of communicating anonymously with each other. No users, senders, receivers, or any third party can enumerate the IP address of an I2P user.

I2P: Security and Working

To transfer data with the I2P network, users have to turn their systems into nodes with CRIs (Cryptographic Router Identity), for making their data anonymous. The assembled routers form virtual tunnels, and every piece of information is sent over to cryptographic locations. Each participant in the network is free to choose the length of tunnels. In doing so, they often make a trade-off between anonymity, latency, and throughput, depending on their own needs.

Routers and nodes connected to several unidirectional inbound and outbound virtual tunnels make up the I2P network. Each node has a unique CRI that is typically long-lasting. For the first time, when users intend to connect, they have to create a query against a network database. This database is known as a Distributed Hash Table (DHT) and is designed based on the Kademlia algorithm. The routers communicate through transport mechanisms like TCP for transferring various messages. Each application has its Cryptographic Identifier, which allows it to transmit messages. All of this is to check whether the other client's inbound channel works efficiently or not. This entire process helps in the safe transfer of information.

Downloading and Installing I2P

Downloading and Installing I2P involves three key steps. First, if you are not using android, Debian, or Ubuntu, you need to download and install the Java runtime version 7 or 8. The next step is to run the I2P installer in your system. This step remains the same for all the operating systems. The last step is to configure your browser according to the required needs. Without configuring it, the network might not work. I2P works best on the Linux operating system.

Compared to TOR, I2P stands out when it comes to handling man-in-the-middle and timing attacks. Because of the garlic routing protocol, I2P is resistant to such attacks, unlike TOR.

Transfer of files over the I2P network is a quick process. Unlike the TOR network, P2P transfer occurs very efficiently through this network.

Every good thing has some drawbacks as well. The same goes for the I2P network. One of them being, I2Ps' new design. I2P may have some undiscovered issues. Comparing it with TOR or Freenet, I2P might not have proper documentation.

For sharing files on the I2P network, it is necessary to login into the network. Without a login, you might not be able to share your files from one person to another. It means for sharing of data, both the sender and the receiver must remain online. In other networks like Freenet and TOR, this problem never appears.

Last and most important is that through the I2P network, the public web is unsafe to access. It means that this network is not efficient for browsing indexed sites.

Is VPN or TOR more secure than I2P?

Virtual Private Network (VPN) is simply software meant to protect you on the web. It is a secured communication channel over the internet, also known as the public network. In this setup, the communication path is encrypted. Amongst all the solutions to protect online identity, VPNs are the most extensively used. VPN helps the data to reach its endpoint over a shared or open network safely and appropriately.

This process encrypts the whole data, maintaining the confidentiality and integrity of the data. The data remains unreadable without the decryption key. Talking about the user's perspective, we can easily say that the VPN is a point-to-point network between the client system and the server. In VPN, it appears like the information is moving over a dedicated link.

The TOR Browser or the Onion browser is just another web browser. Besides browsing the surface web, TOR provides the facility to access the dark web too. It has an extra level of security for surface web use. This browser can easily bypass the surveillance and censorship applied by the government.

It is open-source software that you can easily download from www.torproject.org. It enables the hidden exchange of data by managing network traffic through a free-of-cost, widely spread, overlayed network. The TOR network consists of thousands of relays to protect a user's browsing data from any organization. Hackers nowadays use TOR as it is more difficult for anyone to trace user activities over the internet. These activities include visiting websites, accessing the dark web and the darknet, instant messaging, posting things over the internet, et cetera.

Just like an onion makes up a set of layers, onion routing encryption works layer-wise. It protects the data of the network protocol stack in the application layer. It starts the encryption with the first layer and proceeds similarly with other layers. Each layer has a particular amount of data in it, concealing communication at every layer of the circuit. In the entire process, the IP address of the user is hidden. The layered encryption format eliminates all points of failure. It makes the users anonymous on the TOR network.

If we compare VPN and I2P networks, a VPN has some similarities to I2P. However, both are poles apart from each other. Both of these are recommended for different purposes. VPN is recommended mainly for anonymously surfing the public web. An I2P network, on the other hand, is used for torrenting or accessing the darknet or Darkweb.

If we compare TOR with the I2P network, we can see that they are used for the same purpose and have their respective pros and cons. On comparing different aspects of security, both have been equally important. TOR is based on the C language, while I2P consists of Java. I2P is much faster than the TOR.

So, we are unable to say which among them is more secure. All the networks have different usage, applications, and benefits. It all depends on the user's requirements.

In-depth analysis of an Intrusion Prevention System

The Intrusion Prevention System (IPS) is an automated network security device. IPS is handy in sensing DDOS attacks, brute force attacks, malware threats, etc.

The IPS sets three criteria for functionality: Detection, Prevention, and Responsiveness.

The role of an IPS is to check transmissions, find suspicious activities, compile logs of relevant transmission information, flag them and report them to the network

administrator or concerned person.

It is more effective than an IDS. While an IDS provides threat detection and nil prevention, IPS provides both detection and rectification of network threats.

How does detection take place?

The IPS device stays on the lookout for malicious activities and brute-force attempts. It inspects each packet transmitted through the network. It then cross-checks the contents with a database of known threats. It allows legitimate transmissions between nodes on the network. Since this system is behind a firewall, we can apply it as a filter to offer an extra layer of security. **In case a packet gets flagged, it enforces the following actions:**

- Stop transmission from the source IP.
- Drop the packets that are transmitted.
- Reset the established connection.
- Disallow the IP from using any resources.

What are the detection methods employed by an IPS?

Detection methods may include:

- Address Matching
- TCP connection analysis
- TCP Port matching

Methods to detect suspicious activity on networks:

- Signature-based detection: For each vulnerability in the network, the IPS records the exploit signature. The IPS tries to match the signature of the exploit with the ones recorded earlier. These signatures are pre-defined and take form in a sequence of bytes.
- Statistical Anomaly Detection: In this method, the network calculates what makes up a regular traffic pattern. We know this as the baseline performance level. The baseline always tries to match the current traffic. In case the traffic is not regular, it aborts the transmission. A reason for abnormal traffic is the illegitimate use of network capacity.
- Policy-based detection: In this method, the network admin sets the IPS rules/protocols. In case a packet in transmission does not follow the specified protocols, the IPS drops the packet. It aborts transmission while raising an alert to the concerned personnel.

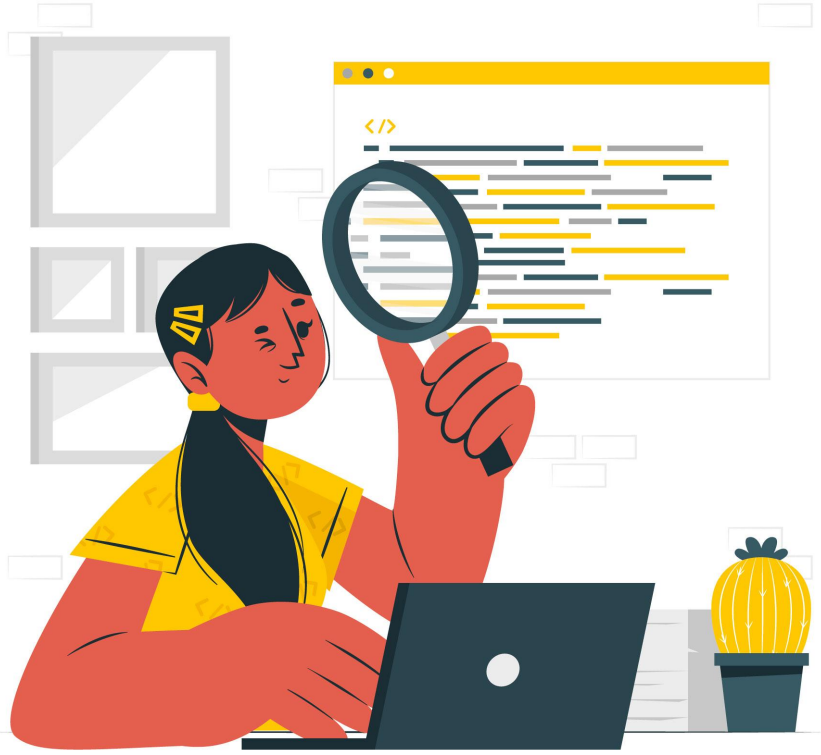
Relative Advantages of an IPS:

- Constant surveillance while supervising traffic flow.
- Threat detection and prevention.
- Network functions with the specified protocols.

Concerned people are always in the loop, with real-time alerts provided by IPS.

In conclusion, it is always wise to have a shield on your network, whether private or public. With the technology boom, we have a basket of options to choose from to enforce network security, be it a firewall or authentication system, from the outside threats. Fortunately, implementing an IPS solves that dilemma.

Reverse Engineering: A Tech Rampart



Reverse Engineering is the deconstruction or breaking down of individual components of products. One can break a piece of the software, redesign machines to rediscover the formula, and update them.

Comprehending this through an example gets easier. So, let us suppose a company manufactures a car model. Reverse engineers then examine this model to identify any technical flaws. They fix the flaws and redesign the machine before introducing it to the market.

Reverse Engineering in Cybersecurity

How is it related to the cybersecurity profession?

Well, Reverse Engineering is the best weapon to fight against cyber-attacks. Reverse engineering is like traveling back in time and retracing the constructed hardware/software to detect any bug and fix it!

With the help of reverse engineering, one can find system vulnerabilities, search for malware and viruses, restore core software algorithms that can help deter theft even more. Reverse engineering treads a thin line in intellectual property law since it may reassemble source code.

Using this skill, security experts can advise how to make things more difficult for a potential hacker. The cybersecurity team can uncover inefficiencies and weaknesses in data storage, encryption, and decryption key storage processes by reverse-engineering them. They may then enhance their solutions and add more levels of protection.

Compared to other ways of security, reverse engineering is preferable since it not only detects and removes malware but also serves as a risk assessment tool. It could be possible to backpedal malware to dope what makes it tick.

As more of our lives and companies migrate online, data security will become increasingly more critical. Cyber security teams must grow smarter than online criminals. Reverse engineering is at the heart of some of the most effective cybersecurity efforts, and it will continue to do so in the future.

Reverse Engineering - An after attack mechanism?

Reverse Engineering is not only limited to security purposes but also is an after-attack mechanism.

Suppose a plane crash happens, now what?

A team of forensic examiners approach the scene and examine how the crash happened. Something similar occurs after a cyber-attack! This tedious process is Reverse Engineering.

Cybercriminals break into computers with malicious intent. They hack into a system with a selfish and harmful aim. Here, Reverse Engineering aids us in identifying their techniques to prevent the system from such attacks in the future. Plenty of tools are available for reverse engineering.

Fate of Reverse Engineering

As more of the world migrates online, data security becomes onerous. White-hat cybersecurity teams must become wiser than online offenders. Reverse engineering is one of the most vital cybersecurity forces, and it will continue to grow more in the future!

CAN BLOCKCHAIN BE HACKED?

SCENARIOS WHERE BLOCKCHAIN CAN BE HACKED

SYBIL ATTACK

An attacker can attack and control most nodes on the network, commanding the network.

51% ATTACK

An attacker can gain over 51% of the mining power on the network, opening the door to fraud and double-spending.

DOS ATTACK

An attacker can flood a node with bad transactions, slowing down the network.

BLOCKCHAIN PROTOCOL BUGS

An attacker can exploit bugs in the blockchain protocol and use them to their advantage.

ROUTING ATTACK

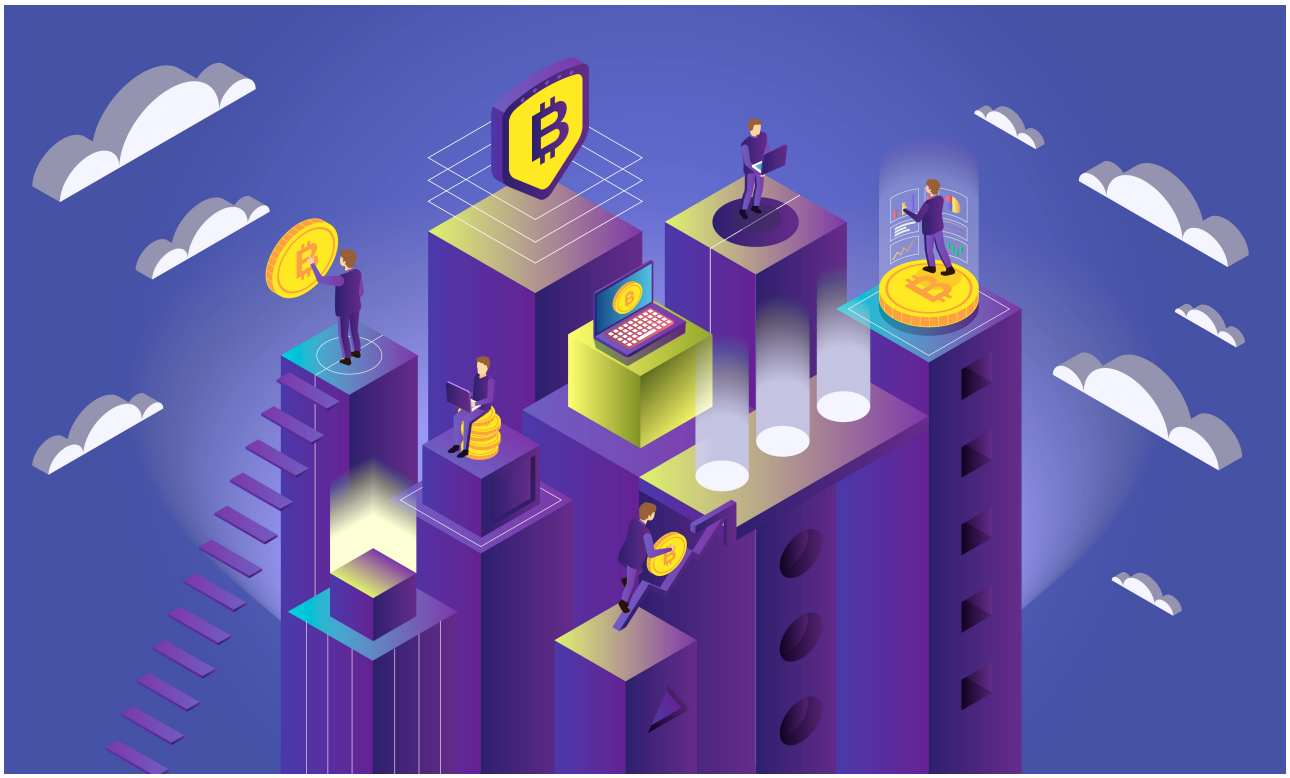
An attacker can compromise the blockchain by compromising the network routing services.

CAN THE HACKER BE DEFEATED?

- Smart contract codes should be tested laboriously to avoid loopholes.
- Do not use weak passwords and do not use unknown devices to log into your accounts.
- All platforms should have a monitoring system to detect any abnormal activity.
- Developers should make sure that the consensus protocol is protected.
- Keep a track of private keys and make sure that they are not lost.
- Keep your security protocols up to date.

ANMOL SINGH

The Cybersecurity Aspect of Cryptocurrency



The hot topic of cryptocurrency and Bitcoin has gained prodigious attention in these recent years. It's a virtual currency and a successor to the global sovereign coinage.

Mainly five cryptocurrencies are ruling the domain; Bitcoin, Ethereum, Litecoin, XRP, and Stellar. These cryptocurrencies have a noticeable impact on various cyber-attacks, hacktivism, cyber-warfare, cyber-crime, and cyber-espionage. It also affects varied spheres of our society, mainly the government, industrial, and finance sectors.

The entire cryptocurrency exchange is vulnerable to cyber-attacks, an imme-

diate consequence of obscurity and anonymity resulting from eminently encrypted blockchain technology.

Increasing security threats

The entire process of transaction relies on a real-time ledger, i.e., Blockchain. One can get bitcoin or any other form of cryptocurrency by decoding an encrypted, unique ID manufactured by the bitcoin formula. And we call the list of records for the same blocks. Every block points to the previous one using a block pointer, and this chain is Blockchain.

Criminals use cryptocurrencies in illicit internet transactions, and its nature of being highly volatile attracts cyber-attacks. Also, the insufficient legal regulation of where the currency is going can be another reason for an increasing number of cyberattacks in this realm.

Risks associated while dealing with cryptocurrencies

According to a research study, 33% of bitcoin trading platforms have been hacked and exploited for profit. Now, one can guess how easy it is for hackers to attack and capitalize on the involved gains.

Recent activity shows that the decentralization of cryptocurrency is what cybercriminals exploit.

With the rise of cryptocurrency, cyber-crime is also rising across the business world. The cyber-crimes involving cryptocurrencies are usually untraceable. It helps criminals use digital assets to hide their illicit activities inconspicuously.

With the growing demand and use of IoT devices, hackers can easily use them as a medium to peep into your system, get unauthorized access and steal your data. Digital transactions use a private key. A private key is a cryptographic algorithm that allows users easy access to their digital platform. If stolen, a cybercriminal can make an extensive monetary profit without being obscure and without ever being caught.

Crypto-jacking, another tactic used by hackers to mine cryptocurrencies using someone else's computer, has also seen a rise. Hackers use poisoned website links to load crypto mining code on your computer. It could be done by either using phishing methods or by injecting a script into a website.

While we can consider cryptocurrency as a new chapter for the finance sector, the attacks associated with it come in many forms ranging from email scams to trading of your compromised personal information to third-party in the black market for profit.

Crypto exchange: Worth the risk?

The cryptocurrency market is not stable and accurately looked into with legal aspects. Many experienced people advise not to affiliate with the market because of the potential cyber risks involved.

An exchange, once completed, cannot be reversed. And this factor makes digital currency exchange more stressful and prone to phishing attacks.

Need of the hour: Sophisticated evolution in cryptocurrency security

Despite the growing clientele of cryptos, the principal concerns of people investing in cryptos are confidence and the entire process of its authentication and authorization.

Thus, the global shift to the concept of making cryptocurrencies the mainstream currency will not be possible until crypto communities develop a robust infrastructure for regulation.

But the onus for protecting one's data in the world of a crypto exchange is on the account holder. The crypto-owner should follow a crucial practice while dealing with volatile currencies, and that is to have both hot and cold wallets.

Meanwhile, cold wallets are hardware devices that store cryptocurrency. It is the most crucial security precaution and is the best possible way to keep your digital assets safe. But again, to access digital currency, one needs to connect these hardware devices to a computer, thus compromising it through an internet connection. It attracts potential cyber-attacks.

The CryptoCurrency Security Standard lays down the practices and strategies to deal with security to make transactions safer. Systems that were non-compliant with CCSS experienced more security breaches. Strengthening these security standards can prevent unrecoverable loss because of a lack of security while making a financial transaction.

With potential attacks increasing, the consumer demand for the currency also depreciates. It is clear now that hackers today can spend millions to target billions. So, there is a need for a proper infrastructure that can safeguard the cryptosystem.

Coin Mining as a Career

With the coming advent of cryptocurrencies and their growing popularity in the global markets, coin mining has become a highly profitable and ideal job to look for in the 21st century.

How do miners get paid?

We must first know that a cryptocurrency runs on a decentralized blockchain network, which requires miners to validate transactions, mine the blocks, and complete the blockchain. Users get paid in tokens for mining blocks.

What do we mean by decentralized system?

Decentralized Systems do not have any central governing body to control and regulate them. It is one of the biggest reasons for cryptocurrencies to succeed in the global market. They are uncontrolled and unregulated by any central body. It provides the

users the authority to validate and authenticate the transactions and payments made in the network. It makes the web more secure and transpicuous for its users and increases their trust in the network.

How exactly does a miner earn themselves a token?

To understand this, we shall take the case of the most eminent cryptocurrency, Bitcoin. For understanding the process of bitcoin mining, we must get a brief about the same. Bitcoin was first introduced in 2009 by Satoshi Nakamoto. In a bitcoin network, there are two ways for possessing a bitcoin, either mining the bitcoins or buying the already mined bitcoins. The reward (token) awarded for successfully mining a block also decreases every four years. A bitcoin mining in 2009 would yield the miner 50 BTCs. In 2012 it was 25 BTCs. In 2016, it was 12.5 BTCs, and the latest halved in November 2020 to 6.25 BTCs.

Now talking about the foremost thing, what does a miner do to mine a bitcoin? In the simplest of terms, a miner must undergo the following tasks:

- Verifying transactions worth 1MB.
- Being the first miner to arrive at the correct or closest answer to the numeric problem.

The first task may sound cumbersome, but it is a straightforward task. The second task is colossal as well. The miner solves a numerical problem involving advanced mathematics or large computations. The miners are supposed to produce an equivalent hash as demanded by the question. They need to be the fastest or first to generate the most accurate hash to earn the reward.

It is a sort of guesswork to predict the most appropriate hash for a specific problem. It has trillions of plausible options to guess out of, making the entire task vexatious. To deal with this problem, the miner uses high-power computers that possess the hash rates of Mega hashes per second (MH/s), Giga hashes per second (GH/s), or even Tera hashes per second (TH/s). The return on the mining rewards is going to be uncertain. It is common in the bitcoin network for a miner not to get rewarded despite validating multiple bytes of transactions. It happens because of the constraints of the hash values.

Despite all this, miners have been making millions out of the bitcoin network. Already about 18 million bitcoins have been mined just in the past ten years. It has become even harder than ever before.

Cryptocurrency is the future of modern trade, so try to capitalize on it most from this very point to get ahead of others. Crypto is not a game of roses. Be very cautious while entering this high-risk game. Take all decisions responsibly and with a well-thought-out strategy.

SQL Injection

Injections cause discomfort not just to your arm but to your computers too. SQL Injection is a malicious code injected into an SQL query to change the results according to the attacker. SQLI attack is a web-application based attack where the attacker manipulates the SQL query to return the output as 'true' even if the login credentials are un-

known. This technique exploits databases by injecting malicious SQL queries into the site inputs or site URL. This exploit targets those web applications which use back-end database servers. Building web applications used to be straightforward, but as technology has advanced, it has become more complex and vulnerable to cyber-attacks. The method used in building a web application plays a crucial role in its vulnerability to SQL Injection.

To confirm a SQL Injection vulnerability, put the apostrophe symbol after the input portion. An error shows that a SQL vulnerability exists that is exploitable by using SQL Injection. The attacker uses OR logic to exploit as it returns the result as 'true', even if at least one value is 'true'. Consider this example: X is a hacker who wants to use SQL Injection to attack a web application. For a successful login, the site requires a username and password.

The original SQL query is:

$sql: select * from users where username='admin' and password='admin';

Since X does not know the login credentials, they will use OR logic to access the database. The exploited query will be:

$sql: select * from users where, username='meenal' or 1=1;– and password='garg';

Here 1=1 is always 'true', so the result returned will always be 'true'.

As the site is vulnerable to SQL Injection, hacker X will get access. Keywords like ORDER BY, GROUP BY, UNION, CONCAT are used to navigate the databases and tables to access vulnerable databases, their versions, and current users. It can attain user details like username, password, email, address, phone number, bank details (credit card number, pin, etc.), shopping carts, histories, SSN, and many more. In the end, if the exploit is successful, the hacker will have complete access to the data. Besides accessing the data, the hacker can insert, edit, modify and delete it. Some tools used for SQL Injection are SQLMap, jSQL Injection, BBQSQL, NoSQLMap, and many more.

Many cyber-attacks exist in the current world, yet SQL Injection remains the second most common attack after CSRF. Various reports in the last few years show that SQL Injection is responsible for almost 65.1% of all web application-based attacks. A little while back, the Flaticon website was under SQL Injection attack, and 8.3 million Freepik and Flaticon user's emails and password hashes were compromised. Whether it is a problem in life or a vulnerability in a web application, the most important thing is to find an efficient solution and implement it. The following are some of the single-layer defense tactics that can prevent SQL Injection:

- Input validation: This method validates the input to ensure that only a particular type, length, and format is accepted. It aids in the nullification of malicious commands sent as the input.
- Parameterized queries: This technique pre-compiles a SQL query to execute it with just arguments/parameters. It stops malicious operations from running since the database can distinguish between authorized input and malicious code. Bind parameters are required to forward data to the database.
- Stored procedures: It is a way of storing the procedures or queries into a logical unit, the Relational Database Management System, to prevent direct access to the database. Statements are automatically parameterized at runtime,

prohibiting SQL Injection and providing advantages like data encapsulation, Strong input validation, and speedier execution. Stored procedures can help protect static SQL queries from code injection.

- Escaping: Character escaping functions can inform the system to handle specific characters differently to avoid confusion in the database between the malicious commands and the authentic input.
- Avoiding Administrative Privileges: Avoid providing unnecessary access to the web application. Use the principle of least privilege to assign permissions.

Because of advancements in cyber-attack practices, these techniques are not enough to keep websites secure. So adding more security, multi-layer defense tactics are used. Host-based WAF and edge-sided WAF may also be helpful. It strengthens database security. A WAF keeps track of the server's incoming and outgoing traffic to check for threats. It creates a barrier between the web application and the internet, hence blocking any malicious activity. Given rising digitalization, we must exercise caution and take preventive measures over the threats of the cyber-world.

How Secure is Cryptocurrency?

AAYUSHI SHRIVASTAVA

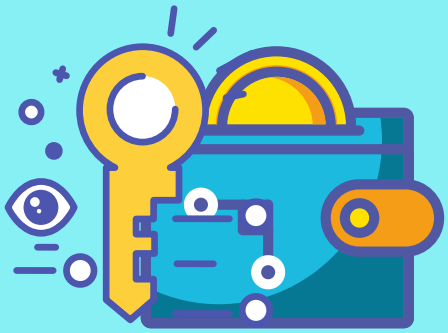
Cryptocurrency, the emerging trend of the future, often said to be the upcoming digital currency, has been in the limelight recently. As the name suggests, cryptocurrency uses cryptography, an advanced coding and encryption technique to store data between wallets, encrypt, record, and monitor transactions. It uses blockchain technology, which comprises a vast network of computers and miners, to check whether a transaction is legitimate.

Cryptocurrency is not a physical currency; it is a fully digital code that exists electronically. It is fully decentralized, which means no central authority, government agency, or bank monitors the transactions. Usage of cryptocurrency in place of traditional money saves us from malicious activities and cybercrimes like double-spending, i.e., using the same amount of currency to pay at different places to pay more than once. To comprehend this technology well, we need to inspect and understand the cybersecurity system operating behind it.

When a cryptocurrency transaction is executed, similar to a bank account book, crypto uses ledgers that store the details and amounts of each transaction made. They place the transaction of sending a coin from one person to another in a virtual block. There is a series of all such blocks comprising nodes that are interconnected. When a payment is made, every computer on the network checks whether the transaction is legitimate. If even a single node is rejected, all the other computers will reject it to show that the transaction is illegal. Once the transactions are deemed safe, the block is added to the chain, providing a transparent record of the transaction. Validating transactions on the block is called mining. Miners get paid a reward (some number of bitcoins) for every successful block they validate.

Despite how dreamy and perfect it may seem, crypto does not rely on trust between the parties involved in the transaction. The payments made are irreversible and highly volatile; the prices keep fluctuating. Here are a few places cryptocurrencies are weak.

- The user might save passwords and files related to crypto on their system. Hackers can manipulate or program these devices to gain access to them and rob you of confidential data and financial assets.
- The transactions via cryptocurrency are immutable. Payment once made accidentally cannot be reverted.
- If the crypto exchange you are trading on gets hacked, or your username/password is compromised, your coins are lost.
- If you store your coins on a laptop and a hacker breaks in and steals them, they cannot be retrieved back.
- If you are running a trading operation and an unscrupulous trader moves coins into their wallet, there is little you can do to get them back.



Due to all these reasons, security in this domain is of utmost importance. As we have seen so far, crypto is a high-risk deal. The ownership, management, and regulation are within the hands of the trader. There is no mediation like a government authority, agency, or the bank acting as a regulator to prevent or report a theft or fraud. So, one should take apt precautions. One must create and store currencies with sufficient balance offline in cold storage and take necessary precautions. The number of attacks reported every day in exchanges is mind-boggling. Here's how cybersecurity in this domain can protect you from fraud.

- Check infrastructure resistance to attacks.
- Create strong passwords and stop visiting illicit, unsanctioned websites.
- Audit application source code and smart contracts for the exchange system.
- When you create a crypto wallet, they ask you for a passphrase, ensure there is no API call or key logger installed in your system to check the passphrase.
- Make duplicates of e-wallets and take a security assessment of your crypto e-wallet application.
- Do not fall prey to phishing attacks by clicking on suspicious links or share details of your account.

Some Useful Tools

⚠ Disclaimer: The following excerpt contains a description of tools that can be mishandled easily. Neither the magazine nor the author is responsible for any damages that may occur from misusing these tools.

Ok Cancel

Breacher

Breacher is a tool used to find out admin console panels. Or, we can say, login input places on a website. It means any page where one can log in to a particular website, this tool can sniff it out.

Prerequisites

Ok Cancel

Terminal

```
user@cyberzine:~$ git clone https://github.com/s0md3v/Breacher.git
Cloning into 'Breacher'...

user@cyberzine:~$ cd Breacher

user@cyberzine:~/Breacher$ python breacher.py -h
Usage:
python breacher.py -u [URL] (Options)
--fast: Enable Multi-threading
--type: Set page type, e.g.: html, php, etc.
--path: Point the tool to a specific directory or path

user@cyberzine:~/Breacher$
```

Fardeen Ahmed

HashCat

HashCat is a fast, easy-to-use, and most advanced password recovery tool. It supports CPUs, GPUs, and other hardware accelerators on Linux, Windows, and OSX. It enables us to crack multiple types of hashes.

Terminal

```
user@cyberzine:~$ wget https://hashcat.net/files/hashcat-x.x.x.7z
'hashcat-x.x.x.7z'-saved (20000000 bytes)

user@cyberzine:~$ p7zip -d hashcat-x.x.x.7z

user@cyberzine:~$ cd hashcat-x.x.x

user@cyberzine:~/hashcat-x.x.x$  cp hashcat-cli64.bin /usr/bin/

user@cyberzine:~/hashcat-x.x.x$ hashcat --help
Usage:
hashcat [Arguments] (Options)
-m: Set the type of hash
-a: Set the type of attack

user@cyberzine:~/hashcat-x.x.x$
```

John The Ripper

This tool is for cracking the hashes and passwords. John the ripper not only runs on 15 different platforms. It can auto-detect the hash type and includes a customizable cracker. This tool also offers brute-force mode. The tool uses a word list that can also be called a dictionary. It compares the hashes of the words present in the dictionary with the password hash.

Terminal

```
user@cyberzine:~$ wget https://www.openwall.com/john-x.x.x.tar.xz
'john-x.x.x.tar.xz'-saved (20000000 bytes)

user@cyberzine:~$ tar -xzf john-x.x.x.tar.xz

user@cyberzine:~$ cd john-x.x.x

user@cyberzine:~/john-x.x.x$  john --help
Usage:
john [hash file] (Options)
--wordlist: Include a word list to enhance the cracking speed

user@cyberzine:~/john-x.x.x$
```

Anant Chouhan

Nmap

When we plan to attack a target, it is crucial to know every aspect of its network. The more knowledge you'll have about the target, the more attack vectors will be available to you. It's also important to know what services are running in the target, like a web server or Windows Active Directory domain controller. Now the first approach is the construction of a map of this landscape by port scanning. There are many scanning tools available, but the best is nmap.

Terminal

```
user@cyberzine:~$ sudo apt install nmap
'nmap' installed successfully...

user@cyberzine:~$ nmap -h
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all
probes)
OS DETECTION:
  -O: Enable OS detection
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt
kIddi3,
     and Grepable format, respectively, to the given filename.
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning,
and traceroute

user@cyberzine:~/$
```

Mahendra Kumar

GNU Privacy Guard

There are several ways by which one can ensure that their data will remain sheltered from the prying eyes of duplicitous hackers. However, the unsurpassed and most preferred method is by introducing encryption technology that is the parts of privacy systems, collectively called PGP and GPG.

PGP is an acronym for PRETTY GOOD PRIVACY. This program uses several encryption technologies, like hashing, data compression, and public/private PGP keys to protect an organization's critical information. However, we can say that this particular encryption program is the propriety of Symantec, the developers of Norton antivirus.

Fortunately, an open-source standard called the OpenPGP is typically free to the public. GnuPG or GPG stands for GNU Privacy Guard. GPG is a different implementation of the Open PGP standard and a well-built alternative to Symantec's official PGP software.

Terminal

```
user@cyberzine:~$ sudo apt install gnupg
'gnupg' installed successfully...

user@cyberzine:~/$ gpg -help
Usage:
gpg [Arguments] (options)
--full-generate-key: Generate a new key pair
--list-keys: View all generated keys
--encrypt: Encrypt data
--decrypt: Decrypt data

user@cyberzine:~$ gpg --full-generate-key
Key Type:
(1) RSA, RSA (Default)
...
: 1
Key Size: 64
Expiration Date (enter 0 for no expiry): 0
Input Password: ********************
...
Key Generation Successful...

user@cyberzine:~$ gpg --encrypt file
The operation completed successfully...

user@cyberzine:~$ gpg --decrypt file
The operation completed successfully...

user@cyberzine:~$
```

Saket Upadhyay

Jewels in the crown of The Division of Cyber Security and Digital Forensics

VIT®
BHOPAL
www.vitbhopal.ac.in

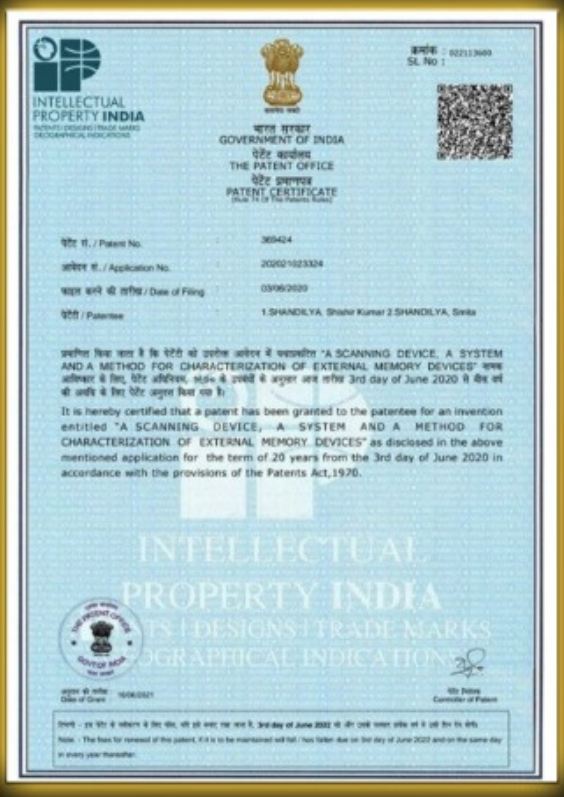
Congratulations!

VIT BHOPAL UNIVERSITY
The Division of Cyber Security and Digital Forensics

PATENT GRANTED by Govt. of India

Title: A SCANNING DEVICE, A SYSTEM AND A METHOD FOR CHARACTERIZATION OF EXTERNAL MEMORY DEVICES

Grantee: Dr. Shishir Kumar Shandilya et. al


INTELLECTUAL PROPERTY INDIA

भारत सरकार
GOVERNMENT OF INDIA
पेटेंट कार्यालय
THE PATENT OFFICE
पेटेंट प्रमाणपत्र
PATENT CERTIFICATE

पेटेंट सं. / Patent No. 369424

आवेदन सं. / Application No. 202021023324

फाइल करने की तारीख / Date of Filing 03/06/2020

पेटेंटी / Patentee 1.SHANDILYA, Shishir Kumar 2.SHANDILYA, Smita

It is hereby certified that a patent has been granted to the patentee for an invention entitled "A SCANNING DEVICE, A SYSTEM AND A METHOD FOR CHARACTERIZATION OF EXTERNAL MEMORY DEVICES" as disclosed in the above mentioned application for the term of 20 years from the 3rd day of June 2020 in accordance with the provisions of the Patents Act,1970.

About the Invention: The invention has intelligence to identify the malware and has a capability of camouflaging the host computer information, making it nearly impossible for the malicious code to attack. Due to ever-evolving cyber attacks, nature-inspired defensive mechanisms hardware security are the future.

Inventors:
Shishir Kumar Shandilya, AK Nagar, VB Gupta, Saket Upadhyay, Shahana Gajala Qureshi, Lokesh Giripunje, Durgesh M Sharma

VIT BHOPAL - RECIPIENT OF DSCI Excellence Award for Cyber Security Education

Shayak Sarkar

2018 Batch

Super Dream Placement - Microsoft

VIT Bhopal University helps get the best out of everyone. The opportunities it provides to its students to showcase their talent are unmatched, especially in cyber security.

Harshit Kulshreshtha

2018 Batch

Super Dream Placement - Walmart

I am proud to be a part of VIT Bhopal University and grateful for the multitudinous opportunities provided by the University to showcase one's talents and skills.

Tanmay Shelat

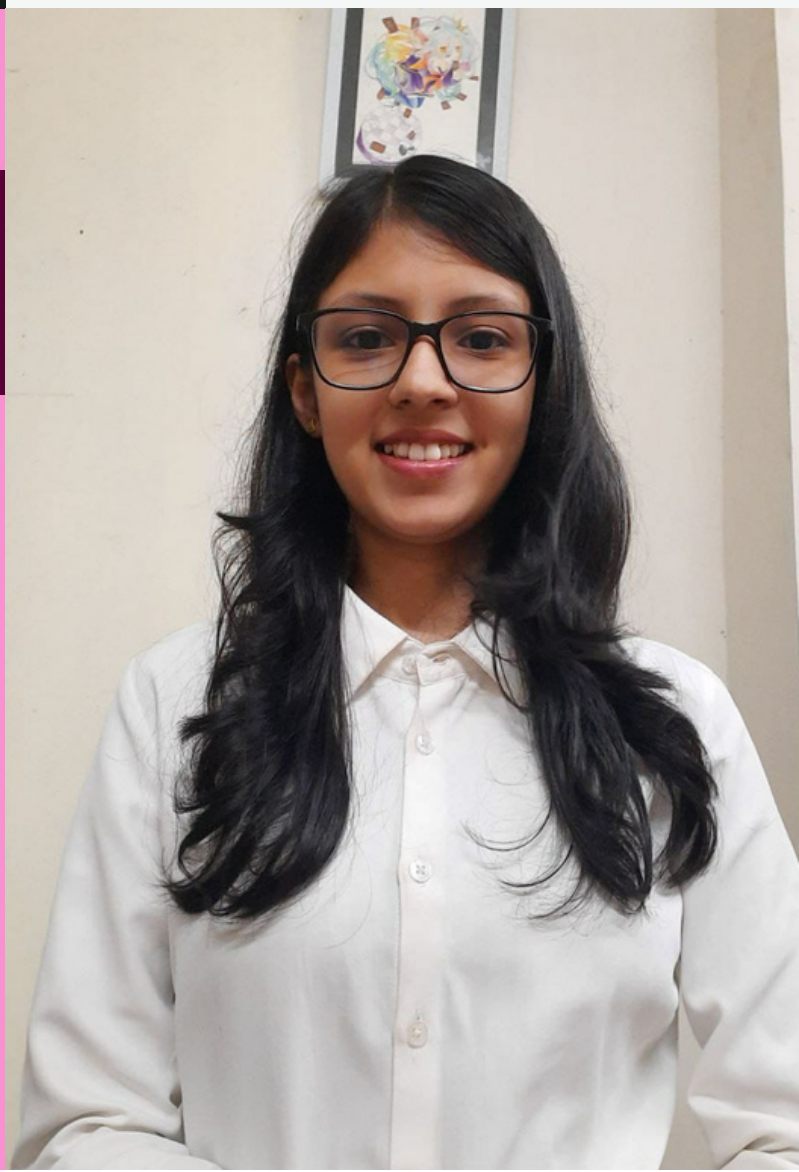
2018 Batch
Super Dream Placement - Bank of America

VIT Bhopal provided me a flexible environment where I could learn and grow in my field of passion. I feel joyous and proud that I finally got my dream job in cyber security.

Pragya Singh

2018 Batch
Super Dream Placement - Providence

Potential is a priceless treasure, like gold. All of us have gold hidden within, but we have to dig to get it out. VIT Bhopal brings out your inner potential and helps you succeed in life.



Divyansh Bhatia

2018 Batch
Super Dream Internship - American Express

While anyone can tell you what is principally required in the placement season, your uniqueness matters the most. VIT Bhopal will provide you with tons of opportunities to build your uniqueness.

Bhawna Yadav

2018 Batch
Super Dream Internship - HP Enterprise

The numerous opportunities for growth at VIT Bhopal help shape you up as a person. It makes me proud to see myself have grown so much.

Adhira Gera

2018 Batch
Super Dream Internship - Trademarkia

VIT Bhopal has always helped me sharpen my skills by challenging me with new tasks and opportunities every day.

Alkesh Gupta

2018 Batch
Super Dream Placement - Bank of America

VIT Bhopal has provided me with everything essential for my future. Journey since the first day of the college itself charged me up with excitement for the present day. Faculties and the PAT team constantly helped me build my learning and personality.

Tejshree Suresh

2018 Batch
Super Dream Placement -
Bank of America

At VIT Bhopal, amidst highly intellectual, experienced, and supportive faculties, I have witnessed my skill and competence rising to a zenith. The learner-centric environment crafted here trained me in academic proficiencies and motivated me to achieve my dreams.

Antara Sinha

2018 Batch
Super Dream Placement -
Bank of America

VIT Bhopal university allowed me to go beyond the regular curriculum, where teachers act more like mentors and coaches in bringing the best out of you. It was a very enriching and fulfilling journey at the campus that I will always cherish in my life.

Jasleen Kaur

2019 Batch
Super Dream Internship - Microsoft

From being an average CS student to getting an internship at Microsoft, the journey has been excellent. VIT Bhopal has played a crucial role in my journey. It has allowed me to meet different people and learn an array of skills.

Muskaan Singh

2019 Batch
Super Dream Internship - Microsoft

VIT Bhopal provided us with an excellent platform for learning and enriching our knowledge. Our faculty put in immense effort to guide us in theoretical, aptitude, and technical skills, which helped us in our interviews. They encouraged us at every step of the way.

Student Achievements

Abhishek Motlani

Cleared Certified Ethical Hacker v10 from EC Council.

Adhira Gera

Scored 90 percentile in Cyber Forensics, Cyber Crimes, Cyber Security and Cyber Law (Gold Expert) organized by International Forensic Sciences (IFS).

Aseem Pandya

Cleared Certified Ethical Hacker v10 from EC Council.

Bhawna Yadav

Achieved 2nd World Rank, Secur'IT Cup, By Kaspersky, 2020 International level. Achieved 3rd Rank, Smart India Hackathon National Level By MHRD, Government of India, 2020. Achieved 3469th Rank in Google Code Jam to I/O Women 2021 Coding Competition.

Debosmita Sinha

Cleared Certified Cyber Forensics Expert (CCFE) from International Forensic Sciences.

Divyansh Bhatia

Cleared Certified Ethical Hacker v10 from EC Council.

Meeraj Mahendra Gawde

Cleared Certified Ethical Hacker v10 from EC Council. Selected for the 6 months ITTCP Development Phase at Siemens Healthineers.

Puneet Bokka

Certified for ECSA by EC-COUNCIL. ECSA certification is a program that builds on previous programs like the Certified Ethical Hacker (CEH) certification. It's a certification that teaches advanced security techniques and Licensed Penetration Tester (LPT) methodologies to cybersecurity professionals.

Student Achievements

Ghanishth Goyal

Achieved 27th Rank in Google organised 0x0G 2021 CTF.

Saloni Gupta

Certified for Google IT Support Professional.

Vipul Jaiswal

Won 3 out of 4 Technical Quizzes at the Asia Innovation Summit.

Navaldeep Singh Chhabra

Certified for Microsoft Technology Associate Security Fundamentals.

Rupesh Kumar

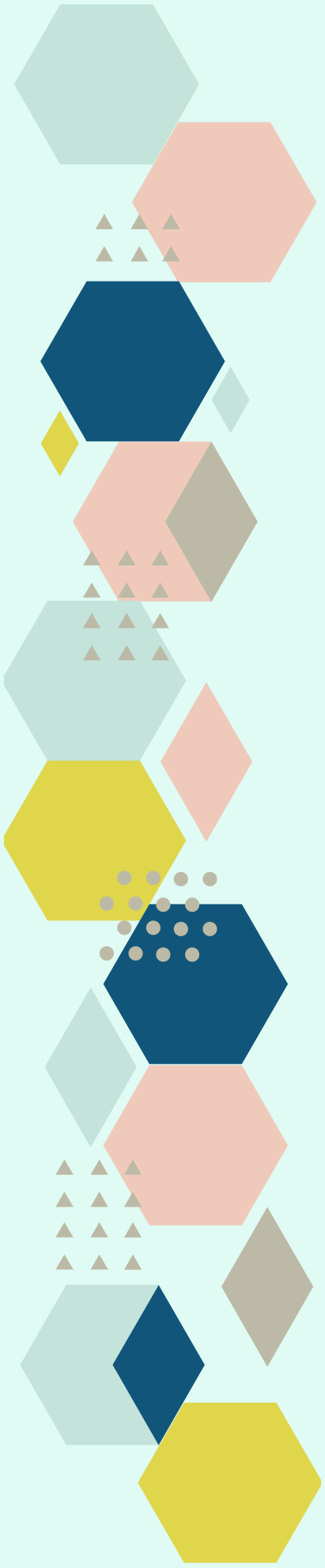
Awarded with one year membership of Australian Information Security Association (AISA). Achieved Cyber Threat hunting level-1 through attending hands-on training by Active Countermeasures. Received the SOC challenge badge by Rangeforce for completing the activities of phishing and other social engineering techniques. Selected as a volunteer in cybersecurity Gatebreakers Foundation in the core cybersecurity team.

Tuhin Bose

Ethically hacked and secured Google, National Cyber Security Centre(Netherlands), ISC2(Top 25), MasterCard, Dell, Unilever(Top 25), Pinterest, Underarmour, JISC, NCIIPC(Hacked 20+ times), Zoho, SeedDMS, Achmea, Pon, SIDN, E-Goi(Hacked 15 times), Flywire, Contacts+, napi.hu, SpaceX, Electroneum, Indodax, Cynical Technology, OMG Nepal(Top 5) and many other private programs. Listed in Top 30 Hackers at BugV.

Vinayak Agrawal

Earned the eJPT Certification from E-Learn Security. Achieved under 300 rank in Try Hack Me.



MEET THE TEAM

EDITORS

DIVYANSH BHATIA
EDITOR - IN - CHIEF

ANIRUDH AGARWAL
MANAGING EDITOR

SOUMYA TIWARI
MANAGING EDITOR

OORJA RUNGTA
MANAGING EDITOR

ANAMIKA MITTAL
EDITOR

ADITI KURUTALA
EDITOR

ARUNDHATI MENON
EDITOR

SHIVYANSHI SHUKLA
EDITOR

DESIGNERS

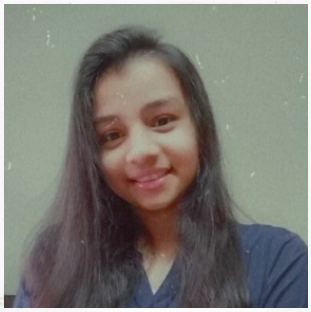
GHANISHTH GOYAL
MANAGING DESIGNER

SANCHIT BAJAJ
DESIGNER

MEET THE TEAM

COLUMNISTS

AARUSHI KOOLWAL
HEAD COLUMNIST



KHUSHI GARG
COLUMNIST

MANSI BAKHSHI
COLUMNIST

EXTERNAL AFFAIRS

SANDEEP KUMAR
HEAD - EXTERNAL AFFAIRS

FARDEEN AHMED
EXTERNAL AFFAIRS

SAKET UPADHYAY
EXTERNAL AFFAIRS

ABOUT US

VIT Bhopal University, an acclaimed institution across the nation, envisaged an idealistic viewpoint of making its students conditioned individuals and technically equipped with the ability to pay their share to the world. It aims the futuristic curriculum at nurturing young minds, giving them a broader perspective of the new avenues open to them. Our aim also is to make our students quality human beings and focus on overall development. We believe that education for the 21st century and centuries to come must be bolder and broader.

In this endeavor, we aim to recognize the true potential of our students by giving them a global platform, instilling in them inquisitiveness to know more, igniting minds to develop into earnest professionals, ready to fight the challenges that may come their way.

UNIVERSITY ADDRESS

VIT Bhopal
Bhopal - Indore Highway
Kothrikalan, Sehore
Madhya Pradesh - 466114

CONTACT: +91 7560254500/ 501 / 502