Unit 1: Cyber Crimes 1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Types of Cybercrime,
- Hacking,
- Cyberspace and Criminal Behaviour,
- Clarification of Terms,
- Traditional Problems Associated with Computer Crime,
- Introduction to Incident Response,
- Digital Forensics,
- Computer Language,
- Network Language,
- Realms of the Cyber world

1.2 INTRODUCTION

“Cyber-Crime” Computer crime, or cybercrime, is crime that involves a computer and a network. Cyber-crime involves activities like raiding bank accounts and stealing information from companies. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet chat rooms, emails, SMS/MMS, notice boards and groups and mobile phones such crimes may threaten a nation’s security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

1.3 TYPES OF CYBERCRIME

Cybercrime includes a wide range ofactivities generally however it may beclassified into four classes as on theimage

- Crime against individual
- Crime against property
- Crimeagainstorganization
- Crime against society

Crimes against individualsemailspoofing a spoofing mail is theformation of email messages byimpersonatingcorrespondent.

Email spamming spam is amessage also called as junk mail sentwith a web link or business proposalclicking on this link or replying tocommercial offer sent to a phishingwebsite or set up a mall where in yourworkstation the sender's of thiselectronic email are always unidentified.

Crime against Propertycredit card fraud online fraud andcheating are most money spinning tradesthose are raising nowadays in the cyberspace it may have diverse forms some ofthe cases of online fraud and cheatingthat are uncovered are those referred to credit-cardoffences contractual crimes offeringemployment etc.

Intellectual property crimesintellectual property involves a list ofRights any illegal act due to which theowner is deprived entirely or part ofthe his human rights. It is a crime the verycommon form of IPRabuse may be known to be software piracy,copyright infringement, trademark andservice mark violation theft of acomputer source code.The Hyderabad Courthas in a landmark judgment has convictedthree personand sentenced them to six months custodyand fine off rupees 50,000 each forunauthorized copying and sell of piratedsoftware.

Against Organization unauthorized accessthis is generally denoted to and hackingthe intent law has however given adifferent connotation to the termhacking so we will not use the termunauthorized access interchangeably withthe term hacking to preventmisperception.As the term used in the IT Act 2000 of India is much wider thanhacking.

Denial of service attack insimple words denial of service referredthe act by which a user of any website or service denied to use the service orwebsite.In this category of cyber crime offenders in the web server of the websites and flow a large number of requests to that server this causes the use of maximum bandwidth of the website and it goes slow down not available for sometimes.

Virus attack a computer virus is a type of malware that when executed replicates by implanting the replicas of it probably altered into other computer programs data files or the boot sector of the hard drive. When this reproduction proceeds the affected zones are then said to be infected. Viruses frequently do certain type of dangerous activity on infected hosts such as stealing hard disk space or CPU time retrieving, private information corrupting, data displaying radical often emails on the user’s display spamming their links or logging their keystrokes. However not all viruses can have a damaging consignment or effort to hide themselves the describing features of viruses is that they are self-duplicating computer programs which mount themselves without the users approval.

On the other hand computer worm is a separate more than program that copies itself in order to disperse to other computers frequently. It uses a computer network to spread itself depend on security failures on the aim computer to allow it.Unlike a computer virus it does not require to join itself to a prevailing program email bombing. IN email bombing user is sending vast numbers of emails to target address and due to this that email address or mail server crashed. It feels like denial of service impression it says that spamming is a variant of male bonding salami attack.

A salami attack is when minor attacks make up a major attack which becomes untraceable because of its nature. It is also called a salami slicing though salami slicing is frequently used to transport unlawful activities it is only a plan for gaining and benefit over time by collecting it in small increments so it can be used in perfectly legal ways as well the attacker uses an online database to seize the information of customers.i.e.bank credit card details deducted very little amount from every account above a period of time the customers remain unaware of the slicing and hence no complaint is launched thus keeping the hacker away from detection.

Logicbomb

a logic bomb is a piece of code intentionally inserted into a software system that will initiate mischievous features under definite conditions, for example a programmer may hide a part of code that starts initiating deleting files such as salary database. Malicious programs such as viruses and worms often contain logic bombs that execute a certain payload at a predefined time or when some other condition meets.Thistechnique can be used by a virus or wormto gain momentum and spread before beingnoticed.Some viruses attack their wholesystems on particular dates such as,April fool's Day.Trojans thattrigger on certain dates are frequentlyknown as time bomb Trojan horse

a Trojan horse or Trojan in computing is anon-self-duplicating kind of malware program comprising malicious codethatwhen implemented carries out actions determined by the nature of the Trojan Usually causing damage of stealing of data and likely system damage. Theterm is derived from the tale of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece.Becausecomputer trojans often hire a form of social engineering representingthemselves as routine valuable or interesting in order to encourage victims to install them on the computers. A Trojan generally acts as a backdoor communicating a supervisor that can have unlawful access to the affected computer. TheTrojans exit are not themselves easily noticeable but if they carry out substantial computing or communications activity may cause the computer to run noticeably slow data.

1.4 HACKING

- **Why Hackers Hack?**

The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers. They just hack to see what they can hack and what they can't hack, usually by testing their own systems. Many Hackers are the guys who get kicked out of corporate and government IT and security organizations. They try to bring down the status of the organization by attacking or stealing information. The knowledge that malicious hacker's gain and the ego that comes with that knowledge are like an addiction. Some hackers want to make your life miserable, and others simply want to be famous. Some common motives of malicious hackers are revenge, curiosity, boredom, challenge, theft for financial gain, blackmail, extortion, and corporate work pressure. Many hackers say they do not hack to harm or profit through their bad activities, which helps them justify their work. They often do not look for money full of pocket. Just proving a point is often a good enough reward for them.

➢ **Steps Performed By hackers**

1) Reconnaissance
   - Performing Reconnaissance
2) Scanning
   - Scanning and Enumeration
3) Gaining Access
4) Maintaining Access
   - Maintaining access and Placing Backdoors
5) Clearing Tracks
   - Covering tracks or Clearing Logs

- Phase I: Reconnaissance

  Reconnaissance can be described as the pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. The Hacker seeks to find out as much information as possible about the target.

- Phase II: Scanning and Enumeration
  Scanning and enumeration is considered the second pre-attack phase. This phase involves taking the information discovered during reconnaissance and using it to examine the network. Scanning involves steps such as intelligent system port scanning which is used to determine open ports and vulnerable services. In this stage the attacker can use different automated tools to discover system vulnerabilities.

- Phase III: Gaining Access

  This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network, local access to a PC, the Internet, or offline. Gaining access is known in the hacker world as owning the system. During a real security breach it would be this stage where the hacker can utilize simple techniques to cause irreparable damage to the target system.

- Phase IV: Maintaining Access

  Once a Hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, Hackers harden the system from other Hackers or security personnel by securing their exclusive access with Backdoors, Root kits, and Trojans. The attacker can use automated scripts and automated tools for hiding attack evidence and also to create backdoors for further attack.

- Phase V: Clearing Tracks

  In this phase, once Hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. At present, many successful security breaches are made but never detected. This includes cases where firewalls and vigilant log checking were in place.

The Indian IT Act, 2000 defines and punishes “Hacking” as follows:

Hacking with computer systems

- Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes any information residing in computer resources.

- “Whoever commits hacking shall be punished with imprisonment up to three years, with fine which may extend up to 2 lakh rupees or both”

- Hacking has been very widely defined in the law of Information Technology, which is much wider than the concept of “hacking” as understood in common.i.e. “Breaking into computer systems”.
- “Destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means”

1.5 CYBERSPACE AND CRIMINAL BEHAVIOUR

Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography. The word became popular in the 1990s when the uses of the Internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging. There are no shared definitions of cyberspace at the scientific level and every government uses a different definition. Cyberspace is the national environment in which digitized information is communicated over computer networks.” -Dictionary of Military and Associated A global domain within the information environment consisting of inter dependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems & and embedded processors and controllers.

Cyber security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. Cyber security standards are the specifications which enable organizations to practice safe security techniques to minimize the number of successful cyber-attacks. Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals. Though, cyber security is important for cyberspace.

Traditional Problems Associated with Computer Crime Individuals seeking a crime has always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. Indeed, the law enforcement community has often failed to recognize the criminal potentiality of emerging technologies until it is almost too late. This trend has proven to be true in contemporary society. Fortunately, much computer-related crime involves no specialist users (e.g., child pornographers, narcotics traffickers, and predators). In fact, the earliest computer crimes were characterized as no technological. Theft of computer components and software piracy were particular favourites. Hacking, DDoS attacks, phishing, Botnets, and other technologically complicated computer crimes came later. Although the advent of technology has vastly changed the modus operandi of certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs. As such, the law enforcement community is experiencing unprecedented periods of uncertainty and ineffectiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty. Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to develop investigative techniques without adequate legal foundations. At the same time, the lack of technological knowledge, allocated resources, and administrative apathy traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators and policymakers are ill-equipped to do so.Physicality and Jurisdictional Concerns The physical environment that breeds computer crime is far different from traditional venues. In fact, the intangible nature of computer interaction and subsequent criminality poses significant questions for investigative agents. For example, what forensic tools are available for identifying entry points in data breaking and entering? Certainly, seasoned investigators recognize the utility of prymark analysis in home burglaries.

➢ Cyberspace and Criminal Behavior

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Associate Professor at the Sorbonne Business School), technical expertise and accessibility no longer act as barriers to entry into cybercrime. Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam. Jean-Loup Richet explains that cloud computing could be helpful for a cybercriminal as a way to leverage his attack – brute-forcing a password, improve the reach of a botnet, or facilitating a spamming campaign.

Cyberspace has become an ideal place for criminals to remain anonymous while preying on victims. As the number of cyberspace users increase, so do the opportunities for exploitation and the need of protecting computers, networks, digital applications, programs and data (i.e., sensitive business and personal information) from unintended or unauthorized access, change or destruction. The Department of Homeland Security (DHS) affirms that there is a range of traditional crimes now being perpetrated through cyberspace.

Criminals hide in the net to perpetrate quite effortlessly crimes that, in earlier times, required physical travel and a more direct involvement. As the cyberspace is recognized as a critical domain for conducting everyday distant operations, unfortunately, it has also become a ground for cyber-terrorism and menaces of cyberwar attacks. Cyberterrorists may use various forms of computer-related abuse tactics (e.g., hacking, cracking, phishing, spamming) to accomplish their personal or politically-motivated goals.

However, countries and governments are not the only targets of cyber criminals. Businesses are not safe either; vital corporate data and industrial secrets can be stolen from adversaries, for example, with cyber espionage; in the past, some attempts have come from countries including China and Russia. In fact, the financial sector is one of the most targeted in recent times and has been the theater of attacks that have often captured the interest of the media.

Recent news, for example, report of a large operation conducted in Europe against a multi-national organization operating in Italy, Spain, Poland, Belgium and the UK. Cyber criminals were able to infiltrate malware in the systems of some large European companies and route money to bank accounts they controlled: a $6.8 million business. EC3, the Europol's European Cybercrime Centre, discovered that the organization was operating from Cameroon, Nigeria and Spain through an impressively efficient money laundering system. Cybercrime has really no borders and boundaries.

In recent years, "information warfare," a new form of terrorism, has captured the attention of information security specialists; terrorists might tamper with computers to commit information-based threats to nations, to businesses, and to individuals.

➢ Economic Impact of Cybercrime

Cyberspace is vulnerable to a wide range of risks, affirms the DHS Cyber Security Division, saying it brings substantial human and economic consequences. All computers users are at risk of Internet crime. According to the Norton Cybercrime Report for 2011, "1m+ adults become cybercrime victims every day." As per a study jointly conducted by McAfee and the Center for Strategic and International Studies in June 2014 (Net Losses: Estimating the Global Cost of Cybercrime), computer-related crimes may cause as much as $400 billion in losses annually, while cyberattack-related losses could be as much as 575 billion. However, arriving at an estimate for the financial losses suffered because of cybercrime is difficult because many instances simply go unreported.

Cybercrime can mean incredible losses for businesses, but is a great deal for perpetrators. Trustwave's "2015 Global Security Report" estimated that the average cybercriminal has a 1,425 percent return-on-investment (ROI). These figures can definitely explain the proliferation of attacks.

- **Cybercrime Trends**

In a world where information and communications technology (ICT) that provides the means so people can work with each other electronically in a digital form over great distances, cyber threats are of great concern. Though it is difficult to keep up with the changes as ICT is constantly evolving, an understanding of the concepts and technologies for achieving confidentiality, integrity, authenticity, and privacy protection for information processed across networks is paramount.

Cybercriminals often use ‘bots’ – a network of software robots – to infect and control networks and control them remotely for malicious purposes. From phishing and devious social engineering efforts to using spyware tactics, an invader can carry out an attack on specific targets, exploiting zero-day vulnerabilities, upload malware on certain platforms, if not collect information and gain access to systems for other purposes. In fact, botnets are often used to spread remote code execution malware. Coming familiar with botnet cyber threats (i.e., how they work and spread malicious code infecting each host and then propagate into the network) is vital to preventing the botnets from the beginning.

Examples of botnet attacks are easy to find. The GameOver Zeus botnet (a sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects) that occurred in 2014, according to the FBI, it was believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world.

As per the FBI, “Unlike earlier Zeus variants, GameOver has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin, which means that instructions to the infected computers can come from any of the infected computers, making a takedown of the botnet more difficult. But not impossible.”

The growth of the use of cloud computing and the Internet of Things (IoT) is contributing greatly to the problem. According to Security Expert and bestselling author, Marc Goodman, in fact, the number of devices connected through the Internet is growing exponentially, and security is an issue: the average IoT, he estimates, has over 20 security vulnerabilities, a number that poses serious concerns.

Another alarming trend, according to Goodman, is the new cybercriminals' profile, who, in most cases, are no longer teenagers looking for glory, but consummate professionals that choose cybercrime as a profession and can sell services. The new breed of malicious hackers is made of more sophisticated criminals who can actually operate within highly organized establishments.

In addition to more specialized hackers, computer software is increasingly been used to perpetrate cybercrime. Crimeware-as-a-service is a new option for criminals without particular technical skills who can carry out their agenda by using off-the-shelves products designed for that purpose. Defending ourselves from this new, decentralized, and pervasive cybercrime is a daunting task.

There is no arguing, "Cybercrime is a global problem." With the ability to connect anything and everything to the Web, cybercriminals exploit the inherent connectivity when and where they like. When it comes to Internet crime, there are all sorts of law-breaking offenses committed that range from identity theft and fraud to unethical hacking, illegal downloading of media, online harassment (e.g., cyberstalking, cyberbullying, to include sexting, child soliciting and abuse), among others. Recurring crimes include sending malicious software to disrupt a network or gain access to a system with the motive to steal sensitive information or data, if not to cause damage to system software. Laws and regulations vary across the country. (See, for example, U.S. state-specific computer crime laws.)

Users are called upon to be the first line of defence and help reduce cyber risks and data compromised by hackers through proper use of their computer, mobile phone and other devices. A Trustwave study showed how 81% of victims they surveyed did not detect breaches in their systems but were notified by external entities. The Verizon's 2015 Data Breach Investigations Report further found that, in 66% of the cases they analysed, it actually took a few months to discover the crime. Situational awareness, then, is one of the key areas of cyber defence and is invaluable when coupled with monitoring and malware analysis from IDS alerts and log files gathered by those in the field. In 60% of the cases, it only took a few minutes for cybercriminals to cause damage to the organizations they attacked, so it is important that everyone in an organization is always looking for anything suspicious in the way their systems behave. Even DHS has created an on going cybersecurity awareness campaign Stop.Think.Connect. launched on October 4, 2010 to help people to understand the risks that come with being online.

Despite IDS/IPS technologies being deployed, only a small percentage of IT decision makers are truly confident that these devices alone will work against a cyber-threat; therefore, they are still seeking alternative solutions, mentioned Tara Seals, US/North America News Reporter, Info security Magazine, in a recent post. Seals explains also the importance of perimeter-based cyber-security models – characterized by a multi-level approach involving firewalls, anti-virus software and powerful analytic tools searching for anomalies in network behaviour

across the enterprise – to protect against threats (or to reduce the damage they can cause), as they continue to evolve rapidly.

- **Cyberspace and Criminal behavior**

Cyberspace may be defined as the indefinite place where individuals transact and communicate. It is the place between places.4 Although originally coined in 1984 by science fiction writer William Gibson, it is hardly a new concept. In fact, traditional electronic communications have always fallen within this existential space. Telephonic conversations, occurring across time and space, were pre-dated by wire exchanges. However, the new medium known as the Internet has monumentally increased the physicality of the virtual world, outpaced only by the exponential growth in the number of users. In 2009, for example, approximately 78 percent of the United States actively used the medium as compared to 10 percent in 1995. In the UK, the growth was even more evident with users of the medium rising from 1.9 percent in 1995 to 83.2 percent in 2009.5Noothermethod of communication converges audio, video, and data entities so effectively. Unlike traditional methods, the Internet combines mail, telephone, and mass media. As stated previously, it exposes individuals to a myriad of new ideas and may serve as a social gathering place, a library, or a place to be alone. As such, the existential nature of the medium does not negate the reality of its consequences. Individual users have married, planned their lives, and stalked our children there. Unfortunately, this virtual world is often perceived as a painless alternative to worldly problems, where individuals shed their worries and become perfect in their profiles. Privacy advocates have often overlooked the negative repercussions of this global medium, arguing zealously that the potentiality of emerging technology precludes governmental interests in monitoring citizens. The organization was co-founded by luminarieslike“TheGratefulDead’s”lyricistJohnBarlowandJohnGilmore,whoistheco-founder/inventorofCygnusSolutions,Cyberpunks,andDESCracker.BothBarlowandGilmorehavebeenmostvocalintheirdefenseofsomeofthemostnotoriouscomputerhackersintheUnitedStatesandhavechampionedtheBillofRights.They argue that the original thrust of the frontier police, directed at ne’er-do-wells intent on compromising the privacy of American citizens, has been refocused on the very individuals that they originally protected. In fact, the two created the electronic Frontier Foundation(EFF)offeringto“fund,conduct,andsupportlegaleffortstodemonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive and unconstitutional.”7 While early actions by the U.S. Secret Service may validate some of these early concerns, the efforts of the EFF have often overlooked the negative potentiality of this global marketplace that has reunited a society that had increasingly removed itself through suburbanization.BeginningwiththeIndustrialRevolution,Americansocietyhaslongbeencharacterized by its distrust of strangers. As media attention increasingly focused on elevated levels of predatory crime perpetrated by non-acquaintances during the 1980s, this fear resulted in a myriad of proactive attempts by both government and citizens to reduce their perceived vulnerability. Among these were admonitions to children to avoid strangers and lock their doors. While such precautionary measures may have been well served in regards to physical crime, the advent of technology has lowered traditional barriers and served as an informal invitation for unknown visitors. Many—such as the victims of theft, stolen privacy, and the like—have recognized only too late the dangers of their inattentiveness, while others, yet to suffer negative consequences, remain blissfully unaware of their own vulnerability. In fact, most individuals, young and old alike, are seduced by the soft hum of a device that appears to be the gateway to worlds that were previously restricted.

Unfortunately, this fascination may be exploited by those we try most to avoid—criminals and predators. As stated previously, technological advancements have historically led to criminal innovations. Just as the Industrial Revolution enhanced threats to national security and created an environment conducive to street/predatory crime through the concentration of the urban population, the information or digital revolution has created a new forum for both terrorist activity and criminal behavior. Indeed, this latest technological era has exacerbated the vulnerabilities of government institutions and personal residences alike. Critical infrastructures, increasingly characterized by tight couplings and interdependency of IT, emergency services, public utilities, banking sectors, food supplies, and transportation systems, have resulted in an interconnectivity inconsistent with traditional security strategies. Such myopia has similarly impacted private citizens who have failed to employ rudimentary measures of cyber protection even as they add additional door locks and alarm systems to insulate themselves from physical attacks. In fact, it may be argued that the Digital or Information Revolution has created a criminogenic environment in which traditional criminals adapt and new criminals emerge.

1.6 CLARIFICATION OF TERMS

Just as debates rage over the appropriate codification of crime committed via electronic means, controversy surrounds the actual semantics associated with the phenomenon. For clarification purposes, then, it is necessary to define the historical usage of terms associated with technological or electronic crimes. Computer crime has been traditionally defined as any criminal act committed via computer. Computer-related crime has been defined as any criminal act in which a computer is involved, even peripherally. Cybercrime has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses. Finally, digital crime, a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. As data may be accessed or stored in a variety of ways and in a variety of locations, digital crime may be characterized as any of the three depending on case characteristics. While computer crime and computer-related crime will be used interchangeably throughout the text, cybercrime will only be used to describe that criminal activity which has been facilitated via the Internet. Additionally, students should be advised that a variety of definitions exist, and that such variations have resulted in confusion among legislators and investigators alike. Some authors, for example, argue that any crime that involves digital evidence may be characterized as a computer crime. This is misleading at best and self-serving at worst. Traditional kidnapping cases in which ransom demands are communicated via telephone will always represent a crime against a person and should not be characterized as a "telecrime." While it is desirable to establish an environment where computers are viewed as potential evidence containers in any case, to redefine traditional predatory crime as cybercrime or computer crime is absurd. Extortion is extortion and will remain such regardless of the method employed to communicate the threat. The result of such hyper-definition is to negate some emerging legislation. This is not to suggest that legislators should cease efforts to specifically criminalize computer-specific criminal activity. Indeed, further legislation should be pursued to enhance prosecutorial toolboxes, not to replace or supplant traditional mechanisms.Just as confusion exists regarding the appropriate terminology for crimes involving computers, the nomenclature of the science developed to investigate such activity lacks universality. For clarification purposes in this text, computer forensic science, computer forensics, and digital forensics may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence.

1.7 TRADITIONAL PROBLEMS ASSOCIATED WITH COMPUTER CRIME

Individuals seeking a crime have always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. Indeed, the law enforcement community has often failed to recognize the criminal potentiality of emerging technologies until it is almost too late. This trend has proven to be true in contemporary society. Fortunately, much computer-related crime involves non specialist users (e.g.,child pornographers, narcotics traffickers, and predators).In fact, the earliest computer crimes were characterized as no technological. Theft of computer components and software piracy were particular favorites. Hacking, DDoS attacks, phishing, Botnets, and other technologically complicated computer crime scame later. Although the advent of technology has vastly changed the modus operandi of certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs. As such, the law enforcement community is experiencing unprecedented periods of uncertainty and ineffectiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty. Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to develop investigative techniques without adequate legal foundations. At the same time, the lack of technological knowledge, allocated resources, and administrative apathy traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators and policymakers are ill-equipped to do so.

1.8 INTRODUCTION TO INCIDENT RESPONSE

Incident handling is a generalized term that refers to the response by a person or organization to an attack. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster. This paper will provide a logical approach to handling two common forms of attack - virus outbreak and system compromise. The method that this article will propose includes the following sequence of steps that should be followed in the case of all types of attack.

1) Preparation

Comprehensively addressing the issue of security includes methods to prevent attack as well as how to respond to a successful one. In order to minimize the potential damage from an attack, some level of preparation is needed. These practices include backup copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. Regularly-scheduled backups minimize the potential loss of data should an attack occur. Monitoring vendors' and security web sites and mailing lists is a good way to keep up to date with the state of the software and patches. It is necessary to update software in order to patch vulnerabilities that are discovered. It is also vital to update anti-virus software in order to keep system protection up-to-date. A documented security policy that outlines the responses to incidents will prove helpful in the event of an attack, as a reliable set of instructions.

2) Identification of Attack

While preparation is vital for minimizing the effects of an attack, the first post-attack step in Incident handling is the identification of an incident. Identification of an incident becomes more difficult as the complexity of the attack grows. One needs to identify several characteristics of an attack before it can be properly contained: the fact that an attack is occurring, its effects on local and remote networks and systems and from where it originates.

3) Containment of Attack

Once an attack has been identified, steps must be taken to minimize the effects of the attack. Containment allows the user or administrator to protect other systems and networks from the attack and limit damage. The response phase details the methods used to stop the attack or virus outbreak. Once the attack has been contained, the final phases are recovery and analysis.

4) Recovery and Analysis

The recovery phase allows users to assess what damage has been incurred, what information has been lost and what the post-attack status of the system is. Once the user can be assured that the attack has been contained, it is helpful to conduct an analysis of the attack. Why did it happen? Was it handled promptly and properly? Could it have been handled better? The analysis phase allows the users and administrators to determine the reason the attack succeeded and the best course of action to protect against future attacks.

- Incident Handling - Viruses
  - Preparation

    Viruses can cause irreparable harm to important files and records. The home and small office user is at even higher risk than larger organizations because the user often works with one computer or stores important information in a single location. Unlike larger organizations that have data spread across many systems in several locations, a virus outbreak in a home or small office could permanently destroy important data. This puts greater emphasis on the need for creating backups of all information. Additionally, backup disks should be kept in a separate location, away from the computer. This ensures that in case of an incident such as fire or theft of hardware that a backup copy of all information is still available.

    The second crucial step in preparing for an attack is to install anti-virus software. Anti-virus software is readily available, easy to install and operate and is affordable. New viruses are created frequently, so it is important to be diligent with anti-virus software maintenance. Almost all anti-virus vendors make updates available on their websites. Users should update their anti-virus software on a regular basis.

  - Identification of Virus Attack

    Viruses are particularly potent and frightening because of their ability to spread quickly to 'friendly' computers. Just think of the public relations nightmare your company could endure if you're the address book in your e-mail program was used to spread a virus to all your suppliers' and your customers' computers.

    Early identification of an incident is crucial to ensuring that the virus does not spread to other computers. It is crucial that users are familiar with the symptoms of a virus attack, such as mass e-mailing, file destruction or other malevolent actions the results of which can be seen immediately. Stealthy viruses require a bit more attention. The user should be aware that periodic anomalous behavior on a system is not always an indicator of a virus attack.

Other factors may cause the erratic behaviour; however, for the sake of security, the user should scan the computer comprehensively to clearly identify the cause. Configuring the anti-virus software to do real-time scanning of files and to periodically do complete system scans helps to both prevent and identify viruses.

- Containment

Containment of the virus is pivotal in limiting the effects. Many viruses spread themselves automatically. If a non-replicating virus infects a single computer, containing the virus is fairly straightforward. The administrator, or user, should disconnect network access including shared directories and other components that may allow the virus to infect files and programs on other machines. Anti-virus software often has a "rescue" component that allows an administrator to scan and clean a system by booting from a specialized floppy disk or CDROM. If available, these tools should be utilized to disinfect the system.

Should the anti-virus software fail to clean the system or lack the features necessary to do the cleansing, it is advisable to try other software packages that may provide more comprehensive coverage. If the system has been altered beyond repair, the last resort is to clear the system entirely and reinstall the operating system and software. If reinstalling, care should be taken to use software that is known to be uninfected and to completely reformat the hard drive to assure the eradication of the virus.

- Recovery and Analysis

Viruses cause varying degrees of destruction- some exist merely to replicate; others attach to and destroy files and programs. Anti-virus programs can generally restore files to their original state, but there are exceptions. If there is doubt to the reliability of the data held within a file, the user should compare the damaged file to a backup copy in order to assess whether or not damage has been sustained.

Once the system or systems have been returned to full operation, analysis should be done to determine where the defenses failed. Does fault lie in the anti-virus software, or the frequency and reliability of updates? Or did some user behaviour - such as opening files from an unknown or untrusted source - allow the system to become infected? Once the attack was identified, were appropriate and sufficient steps taken to minimize the damage that the system sustained? Analysis of the incident allows the user to learn from the unfortunate incident and ensure that it does not happen again.

- ➢ System Compromise
  - Preparation

    System compromise is an attack in which an intruder breaks into a computer and, either sitting directly in front of it or from a remote network, is able to use that computer. The attacker typically has total access to a system and all information contained therein including files, applications and potentially any other system connected to it.

    Managing system compromise is more daunting than managing virus outbreaks. The basic steps to help prepare in case of system compromise are basically the same as are used in preparation for virus outbreaks. All vital information should be backed up on a regular basis. Software updates are also crucial. System compromise often arises due to security vulnerabilities in common software, particularly in operating system software. Users and administrators should be sure to maintain current software patches in order to protect against attacks. Patches are available through vendors' websites. Users can learn about the latest patches by monitoring vendors' web sites, mailing lists and user forums related to the software and to security.

    In order to prevent against unauthorized intrusion into a system, users should implement firewalls. Just as anti-virus software is the cornerstone of a virus prevention strategy, firewalls are extremely important in preventing unauthorized individuals from accessing network services and resources. Like anti-virus software, firewalls are relatively affordable and easy to use - they not only protect against intrusion, but some can be configured to notify the user if an intrusion is being attempted.

  - Identification

Systems compromise attacks are often indicated by missing or modified files, changes to the system configuration and services, greater memory and disk usage and unidentified network connections. Attackers will often seek to hide any indication of the intrusion by replacing files and programs with versions that protect the attacker. Programs that act normally on one occasion and strangely the next, as well as files and programs that have their time, date or size information modified may be indicative of an unauthorized intrusion. Comparison against backup copies may reveal changes to files.

Users and systems administrators can identify potential systems compromise attacks by monitoring network traffic and processes. The new wave of Intrusion Detection Systems (IDS) is extremely helpful in allowing for the monitoring of systems. By actively monitoring the network for known signs of attack and other anomalous conditions, an IDS notifies users as soon as it detects the event. IDS are useful in complex networked environments and where minimal technical staffing is available. By automatically monitoring and notifying users, an IDS can offload some responsibility from an overburdened administrator, making them invaluable resources for users and administrators in small offices and home offices.

- Containment

  Containment of an intrusion involves some effort on the part of the administrator. First, the administrator should freeze the current system as soon as an intrusion is suspected. This includes disconnecting the system from the network, stopping the operating system and disallowing anyone to use the system. As an operating system runs and people use the system files are naturally modified and updated depending on what they are doing. This normal functionality often erases important information that can be used to detect and trace an intrusion, therefore it is very important to stop the system as soon as possible after an attack is discovered. If possible, it is advisable to duplicate the hard disk of the system. This allows the administrator to begin the cleanup process on one disk and to give the other to an expert to determine the exact source and cause of the intrusion.

- Recovery and Analysis

The most devastating but least-effort method of cleaning up a compromised system is to wipe the hard disk clean and re-install the operating system and software allowing a faster return to normal operation. A more painstaking approach is to compare each individual file and program against a copy known to be original in order to determine if any modifications have been made. It is important to do a minimal level of analysis in order to determine the cause of the intrusion. Once a cause is determined, changes to the environment should be made to avoid future attacks by that method. This includes updating affected software, access control methods that allow only certain users, systems and networks to use the services, firewalls and intrusion detection systems. A combination of these changes can provide a safer and more secure working environment.

Analysis of the attack provides several benefits. The user and administrator can determine the shortcomings in existing security policies, installation methods and configurations that allow attacks to succeed. Users and administrators should periodically review existing installations, configurations and security policies. New attacks and security vulnerabilities are found often and updating the existing environment can minimize the threats of future attack.

1.9 DIGITAL FORENSICS

Digital forensics is a key component in Cyber Security. Many people hear the term forensics, or computer forensics, or digital forensics and instantly think, that’s just for law enforcement, but the truth is, digital forensics has a key place on every cyber security team. In fact, without it, chances are your organizations Security posture and maturity will fail to see its full potential.

Digital forensic practices stem from forensic science, the science of collecting and examining evidence or materials. Digital or computer forensics focuses on the digital domain including computer forensics, network forensics, and mobile forensics.

In the event of a cyber-attack or incident, it is critical investigations be carried out in a manner that is forensically sound to preserve evidence in the event of a breach of the law. Far too many cyber-attacks are occurring across the globe where laws are clearly broken and due to improper or non-existent forensic investigations, the cyber criminals go either unidentified, undetected, or are simply not prosecuted.

➢ Malware Forensics

Malware is a type of software intentionally designed with malicious functionalities. The goal of malware forensics is to find out:

- What the malware can do (and what it does in a particular situation)
- To which family it belongs to (ransomware, keyloggers, remote administration tools)
- How it can be detected and blocked, and
- How it can be cleanly removed from an infected system

To achieve these goals, there are two approaches: static analysis and dynamic analysis. Each approach has its own pitfalls and advantages. Static analysis examines the binary without running it. It is the only option when the malware cannot be run, i.e. taken from a partial memory dump, missing pieces, or having an unavailable architecture. It tells the analyst everything the program can do, but this approach is less precise because of the need to reason about the program behavior without actually executing the code. By contrast, it achieves a larger coverage: one can reason about all possible executions at the same time. Dynamic analysis runs the program and observes its behaviour. It tells the analyst exactly what the program does when it is executed in a given environment and with a particular input. It is more precise because it can observe the instructions executed and the values of registers and memory; however, it achieves a smaller coverage because it observes one execution path at the time.

A general approach to malware analysis would be:

1. Set up a controlled, isolated laboratory in which to examine the malware sample
2. Perform behavioral analysis to examine the sample's interactions with its environment
3. Perform static code analysis to further understand the sample's inner workings

4. Perform dynamic code analysis to understand the more difficult aspects of the code
5. If necessary, unpack the sample
6. Repeat steps 2, 3, and 4 (order may vary) until analysis objectives are met
7. Document findings and clean up the laboratory for future analysis

The following section describes each step with the common and popular tools used to achieve the goal.

Examining malicious software involves infecting a system with the malware sample and then using the appropriate behaviour analysis tools to observe its interaction with the system. This requires an isolated laboratory environment that you can infect without affecting your production environment. The most common and flexible way is to use virtualization software (e.g., VMware or VirtualBox).

To understand the threat associated with the sample, the analyst needs to examine its behaviour in the controlled environment already setup in the previous step. He uses Process Monitor to study the process, network, file, and registry interactions between the malware and the operating system.

Process Monitor is a common tool for capturing the following events:

> Registry: Capture registry keys query, read, and creation operations.
>
> File system: File creation, writing, deletion from local hard drives and network drives.
>
> Network: Show the source and destination of TCP/UDP traffic, but it doesn't show the data.

Analysts use Wireshark to capture data. Packets can be filtered based on source destination IP/port by Process Monitor.

> Process: Shows processes and threads creation and exit, etc.
>
> Profiling: Checks the amount of CPU time used by each process or the malware being studied and the memory use.

- Is the malware a known binary?

To check if the sample is a known binary based on its hash or if it is similar to something already known based on its signature, the analyst could submit it to VirusTotal. VirusTotal is a sandbox tool for malware identification owned by Google. The tool has the biggest repository of malware and known file types around.

Malicious binaries are typically stripped of all symbols, obfuscated and packed. In addition, they implement plenty of anti-debugging and anti-analysis tricks and checks for analysis environments. Packing a program is compressing or encrypting the instructions and data in order to save disk space. It’s widely used by malware writers. Many packers automatically include anti-disassembly, anti-debugging, and anti-VM techniques to further complicate the analysis.

The packer can be identified based on its signature or by using heuristics. PEiD is a popular tool that can identify most common packers, cryptors, and compilers for PE files. It packs more than 600 different signatures in PE files, which make its detection rate higher than that of other similar tools.

There are several heuristic techniques to determine whether a program is packed, including sections with high entropy, weird section names, and few entries in the import table, etc. Mandiant’s Red Curtain tool computes entropy of sections. High entropy means that the program is likely packed or encrypted. The tool also scans for packing signatures and computes a threat score.

There are several approaches to unpacking a program. One first approach could be to manually reverse-engineer the packing stub and write the corresponding unpacking tool, but this is complex and time-consuming. An automatic and dynamic approach could be dumping the binary containing the unpacked program. In a few cases, the program can be unpacked automatically using a tool (e.g., the UPX tool, using –d option). PEiD comes with a set of plugins, including an UPX unpacker.

Disassemblers are among the tools that can be used to statically analyze binary programs and further understand the malware’s inner workings. These tools do not require the analyzed module to operate; it can be safer to use static analysis if it is known that the module under analysis is malicious. A disassembler converts machine language into assembly language. IDAPro is popular tool for doing this job.

In order to determine the higher-level logic of a function, such as loops, switches, and conditions, the malware analyst can use a decompiler. A decompiler converts assembly code into source code in a higher-level language such as C++ or C. Paid versions of IDAPro come with a C/C++ decompiler called Hex-Rays Decompiler. An alternative is to use a similar tool called Snowman.

The last step is to document the findings and analysis results in a report that summarizes the answers to the predefined questions. The analysis report covers, but not limited to, screenshots, notes, and observations.

- Memory Forensics

Memory forensics is the process of investigating a memory dump to locate malicious behaviors. The dump is a snapshot capture of RAM memory at a specific point of time; it can be a full physical memory dump, a crash dump, or a hibernation file.

The investigator extracts useful artifacts from memory, including running processes, URLs, passwords, encryption keys, kernel modules, shared libraries, open sockets, active connections, and open registry keys. That information can be accessed by obtaining and analyzing the target computer’s physical memory dump.

A general approach to memory forensics would acquire and analyze physical memory.

Memory dump acquisition: can be performed using a program installed on the system, such as win32dd, win64dd, dumpit, or dd or by using dedicated hardware such as an internal acquisition card (PCI card), or sniffing direct memory access (DMA) transfer, or using a FireWire port. The difference is that the software may alter the system, in contrast to the use of hardware. However, using hardware may crash the system or lose information, in the case of FireWire. In addition, the hardware must be installed on the machine before an incident occurs.

Memory dump analysis: Many tools offer digital artifacts and analysis facilities. Volatility is the most popular memory forensics framework. It can extract digital artifacts from multiple types of memory (crash dump, core dump, hibernation file, etc). It provides an in-depth visibility into the runtime state of the system. Rekall is an advanced memory analysis solution. It is basically a fork of the Volatility memory analysis framework maintained by Google’s incidence response team.

To start the analysis, summary information of the dump can be viewed. This information includes the operating system version and target architecture (32 or 64 bits). The most commonly used analysis approach then is to list the processes that were running in the system, the loaded kernel modules, and shared libraries to locate malicious modules. The analysis can also cover other data, such as registry keys.

In addition to the active processes, the analyst should keep track of terminated and hidden processes, since they might also load malicious modules.

The analysis may end when malicious files are dumped. Then malicious file analysis comes to play as described in the previous section.

- Email Forensics

Emails are the main channel for worms, phishing, and the transportation of spam. Email forensics involves investigating email content and sources to reveal key information, such as the recipient's identity, the trace path traversed by the message, the application used to compose the email, the timestamp when a message was generated, a unique message ID, etc.

Typically, email forensics consists of the following steps:

- Examining sender's e-mail address
- Examining message initiation protocol (HTTP, SMTP)
- Examining message ID
- Examining sender's IP address

This involves investigation of port scanning metadata and keyword searching.

There are several approaches to email forensics such as header analysis, server investigation, client-side mailer fingerprint, network devices investigation, and bait tactics.

Many tools may assist in the study of source and content of e-mail message so that an attack or the malicious intent of the intrusions may be investigated. The following is a non-exhaustive list of email forensics tools:

- MailXaminer
- Add4Mail
- eMailTrackerPro

- AccessData’s FTK
- Paraben E-Mail Examiner

- Smartphone Forensics

Smartphone devices contain sensitive personal information such as contact lists, SMSs, calls, pictures, etc. This information can be used by attackers to impersonate the owner’s identity, so it is risky if it is lost or stolen. That’s why smartphones become an inevitable source for digital forensics. There are three primary approaches to smartphone forensics which focus on extraction of data that might be rightly challenged in a court of law.

General approaches to smartphone forensics

Manual Acquisition: The investigator browses the smartphone and takes pictures of each screen that contains important information. This technique does not alter the device and no tools are required to perform data acquisition. However, only data visible to the investigator can be recovered since only the user interface is used.

Physical Acquisition: The investigator clones the smartphone storage device and then normal disk forensic techniques are used (see Disk Forensics section).

Logical Acquisition: In this technique, little manual intervention or cloning is required. Here data available on the smartphone is acquired by automated tools for synchronizing the device and PC. With this technique, the investigator can’t acquire deleted data and unallocated spaces.

The following is a list of the popular tools available for smartphone forensics:

- Andriller
- XRY
- Oxygen Forensic
- Ufed Touch
- Droidspotter
- Mobiledit Forensic

- Disk Forensics

The goal of disk forensics is to acquire a copy of data resident on hard drives and USB memory sticks, analyzing it to extract digital evidence. The acquisition can be performed at the file level or the sector level. At the file level, the investigator can't acquire deleted files and unallocated spaces. At the sector level, however, the investigator can acquire an exact copy of the device storage. If the storage is corrupt or damaged, then the investigator relies on file carving, which may recover data if the files' metadata are lost. The most popular tools are the Sleuth Kit, Digital Forensic Framework, FTK, and EnCase.

- Cloud Forensics

Cloud forensics involves inspecting cloud components, which include logs, virtual machine disk images, volatile memory dumps, console logs, and network captures. Cloud forensic tools collect data from the cloud, image the instances, and recover data from cloud instances. FROST is a forensics tool for OpenStack.

- Log Forensics

Logs generated by the operating systems and applications are segregated and parsed to generate useful information. Correlation mechanisms are applied to find relationships between logs and external or internal events.

1.10 COMPUTER LANGUAGE

Programming languages for Web Hacking and Pentesting

If you're interested in web hacking and pentesting, then you must learn learn below mentioned languages at-least basic and intermediate level.

1. HTML

   Always begin with basics and HTML — HyperTextMarkup Language — should be the first one you should learn as a beginner. HTML is the building blocks of the internet and an ethical hacker should know it very well to understand web action, response, structure, and logic. Also, learning HTML is not at all that tough.

2. JavaScript

   JavaScript — JavaScript is the most used as client-side programming and for web development is also the best programming language for hacking web applications.

In fact, it is the best programming language for hackers and security experts for developing cross-site scripting hacking programs.

You should learn it on high priority mode. Understanding JavaScript code logic can help you find the web-apps flaws and it is the best one to manipulate both front-end and back-end web components.

3. SQL

   SQL — Structured Query Language — is a database programming language used to query and fetch information from databases. All big and small websites and web apps are using databases to store data like login credentials and other valuable inventories — it is the most sensitive part of the Web. So a hacker must learn SQL to communicate with databases and to develop hacking programs based on SQL injection.

4. PHP

   PHP is the most popular dynamic programming language, used mainly by websites build upon popular CMS like WordPress. So knowing PHP will help you to find vulnerabilities in such network and take down a personal website or blog. Hackers use PHP mainly for developing server hacking programs as it is a server-side scripting language. So, if you are into web hacking then deeper knowledge in PHP is necessary.

5. Perl

   Perl is an important programming language for hacking to compromise old machines since many old systems still use Perl. Perl is worth learning for practical reasons — it’s very widely used for active web pages and system administration, best available language for manipulating text files on Unix systems and integration with popular web-databases. So that even if you never write Perl you should learn to read it.

Programming Languages for writing Exploits

Exploit writing is an advance part of hacking. It requires a higher level of programming language. Every professional hacker must know to exploit writing. It can be done in any programming language like C, C++, Ruby, Python, etc.

6. C

The mother of all programming language, C is the most important programming language used in creation for Linux and Windows. So learning C programming will help an ethical hacker to understand the way of working of these systems — like how CPU and memory interact with each other.

However, it is the best programming language for exploit writing and development. The low-level nature of C benefits security experts to develop hacking programs to access and manipulate system hardware and lower level resources.

7. C++

C++ is one of the best programming languages for hacking software comes under a proprietary license and require paid activation. Like C, C++ also gives the low-level of access to the system and helps to analyze the machine code and bypass such activation schemes. Also, many modern hacking programs are built on C++.

8. Python

Unlike any other programming language listed here, Python is the easiest one to learn. It is the most used language for exploit writing as Python is the easiest programming language to write automation scripts because of pre-built libraries with some powerful functionality.

Also “run without compilation” nature of Python makes its an essential programming language for hackers to take down web servers. It is highly recommended you to learn Python Socket Programming because it helps lot learning exploit creation.

9. Ruby

Ruby is a simple but complicated object-oriented programming language used in web development. Ruby is very useful in exploit writing. It is used for meterpreter scripting and do you know Metasploit Framework itself programmed in Ruby.

10. Java

Java is the most widely used programming language in the coding community. Java was originally released with the slogan “write once, run anywhere,” which was intended to underscore its cross-platform capabilities. Because of that Java is the perfect programming language for hacking PC, mobile devices and web servers.

You can make tools using Java and it can also be used to create backdoor exploits as well as exploits that can kill a computer. Once you write your hacking programs with Java, you can run them on any platform that supports Java.

11. LISP

Lisp is the second-oldest high-level programming language in widespread use today. LISP is absolutely wide open, flexible and totally machine independent makes it hacker’s favorite. You can define your own syntax and create any sort of programming paradigm you like and include it in your programs.

Programming languages for Reverse Engineering

Reverse engineering, also called back engineering, is the processes of extracting knowledge or design information from anything man-made and reproducing it or reproducing anything based on the extracted information. Reverse engineering is also beneficial in crime prevention, where suspected malware is reverse engineered to understand what it does, and how to detect and remove it, and to allow computers and devices to work together. Reverse engineering can also be used to “crack” software and media to remove their copy protection.

12. Assembly Language

Assembly is low level programming language but very complicated. One can instruct a machine hardware or software using Assembly language. Reverse Engineers uses Assembly language, and if you want to learn Reverse Eng, you must need to learn Assembly language.

Finally one more thing, programming languages for hacking also depends upon what program you want to hack, for example; if a web-app in coded in ASP.NET then you can’t hack it using PHP knowledge, although you can understand logic but it will be harder, so always make sure what you wanna hack and in which programming the app is coded.

Also hacking is a skill and only talented well-trained could become a better security expert. So learn these programming languages to its core and hard-train your abilities to solve different coding problems.

1.11 NETWORK LANGUAGE

Network security is an integration of multiple layers of defenses in the network and at the network. Policies and controls are implemented by each network security layer. Access to networks is gained by authorized users, whereas, malicious actors are indeed blocked from executing threats and exploits.

Our world has presently been transformed by digitization, resulting in changes in almost all our daily activities. It is essential for all organizations to protect their networks if they aim at delivering the services demanded by employees and customers. This eventually protects the reputation of your organization. With hackers increasing and becoming smarter day by day, the need to utilize network security tool becomes more and more impotent.

Types of Network Security

1) Antivirus and Antimalware Software
2) Application Security
3) Behavioral Analytics
4) Data Loss Prevention (DLP)
5) Email Security
6) Firewalls
7) Intrusion Prevention System (IPS)
8) Mobile Device Security
9) Network Segmentation
10) Security Information and Event Management (SIEM)
11) Virtual Private Network (VPN)
12) Web Security
13) Wireless Security
14) Endpoint Security
15) Network Access Control (NAC)

1) Antivirus and Antimalware Software : This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses. Malware can also become very dangerous as it can infect a network and then remain calm for days or even weeks. This software handles this threat by scanning for malware entry and regularly tracks files afterward in order to detect anomalies, remove malware, and fix damage.

2) Application Security: It is important to have an application security since no app is created perfectly. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.

3) Behavioral Analytics: In order to detect abnormal network behaviour, you will have to know what normal behavior looks like. Behavioral analytics tools are capable of automatically discerning activities that deviate from the norm. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

4) Data Loss Prevention (DLP): Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures, that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner.

5) Email Security: Email gateways are considered to be the number one threat vector for a security breach. Attackers use social engineering tactics and personal information in order to build refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application is capable of blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.

6) Firewalls: Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A set of defined rules are employed

to block or allow traffic. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online.

7) Intrusion Prevention System (IPS): An IPS is a network security capable of scanning network traffic in order to actively block attacks. The IPS Setting interface permits the administrator to configure the ruleset updates for Snort. It is possible to schedule the ruleset updates allowing them to automatically run at particular intervals and these updates can be run manually on demand.
8) Mobile Device Security: Mobile devices and apps are increasingly being targeted by cybercriminals. 90% of IT organizations could very soon support corporate applications on personal mobile devices. There is indeed the necessity for you to control which devices can access your network. It is also necessary to configure their connections in order to keep network traffic private.

9) Network Segmentation: Software-defined segmentation places network traffic into varied classifications and makes enforcing security policies a lot easier. The classifications are ideally based on endpoint identity, not just IP addresses. Rights can be accessed based on location, role, and more so that the right people get the correct level of access and suspicious devices are thus contained and remediated.

10) Security Information and Event Management (SIEM): SIEM products bring together all the information needed by your security staff in order to identify and respond to threats. These products are available in different forms, including virtual and physical appliances and server software.

11) Virtual Private Network (VPN): A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mostly over the Internet. A remote-access VPN typically uses IPsec or Secure Sockets Layer in order to authenticate the communication between network and device.

12) Web Security: A perfect web security solution will help in controlling your staff's web use, denying access to malicious websites, and blocking

13) Wireless Security: The mobile office movement is presently gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones and this makes way for hackers to enter. It is thus essential for the wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used in order to prevent an exploit from taking place.

14) Endpoint Security: Endpoint Security, also known Network Protection or Network Security, is a methodology used for protecting corporate networks when accessed through remote devices such as laptops or several other wireless devices and mobile devices. For instance, Comodo Advanced Endpoint Protection software presents seven layers of defense that include viruscope, file reputation, auto-sandbox, host intrusion prevention, web URL filtering, firewall, and antivirus software. All this is offered under a single offering in order to protect them from both unknown and known threats.

15) Network Access Control (NAC): This network security process helps you to control who can access your network. It is essential to recognize each device and user in order to keep out potential attackers. This indeed will help you to enforce your security policies. Noncompliant endpoint devices can be given only limited access or just blocked.

- Technical Network Protection: Technical Network Protection is used to protect data within the network. Technical network protection guards both stored and in-transit data from malicious software and from unauthorized persons.
- Physical Network Protection: Physical Network Protection, or Physical Network Security, is a network security measure designed to prevent

unauthorized people from physically interfering with network components. Door locks and ID passes are essential components of physical network protection.

- Administrative Network Protection: Administrative Network Protection is a security method that control a user's network behaviour and access. It also provides a standard operating procedure for IT officers when executing changes in the IT infrastructure. Company policies and procedures are forms of Administrative network protection.

1.12 REALMS OF THE CYBER WORLD

The need for information security has ceased to be a subject of debate in technology circles. The expectations, the context and the need probably differ, however one sees a consensus on the need to secure and protect information. In the technology landscape, where jargon and acronyms occur as frequently as the tides that wash ashore, the term cyber security has grabbed a lot of attention. International Telecommunication Union (ITU) refers to cyber security as – 'Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.' Professionals, enterprises and even nations seem to focus on cyber security today. While the people at large may not ponder much, for IT professionals it may raise a few questions. Some of them are likely to be -are the terms information security and cyber security synonyms, if not what's the difference? Is cyber security is a sub set of information security or are the two entirely different? Multiple definitions that allude to the different views on cyber security are likely to be available. However it is important that we understand the core behind cyber security than get hindered by the definitions. The focus on threats, risks and controls relevant to the cyber world is the realm of cyber security. This does not mean that security in the cyber world was not addressed in the information security legacy that we inherited and that has developed over the years. The footprint of the 'cyber' aspect though, was rather limited. This limited focus was not deliberate but merely reflected the reality of the day where connectivity to cyber space was less extensive and controlled. Hence the risks posed by the cyber world were not as extensive as they are today.

Changes in the environment triggered a focus on cyber security. The changes have been varied and extensive. The changes have not been unidimensional but have encompassed a wide landscape. The traditional view about architecture, technology, its delivery and utilization have all changed. The holy grail of technology available to a few qualified professionals is now available to the world at large. Within a short span of time, innovative and unthinkable concepts like Bring Your Own Device (BYOD) and Mobility, Cloud Computing, Social Networks, Internet of Things (IoT) have become reality of the day. This imperative has been embraced for sure–in some instances with open arms and in few other cases grudgingly. The underlying enabler for the change is connectivity that has been provided by the cyber world. The innovative and diverse leveraging of the cyber world has increased the number of cyber citizens and also the traffic flows. The perimeter has traditionally been the frontier that separated the trusted internal network from the un-trusted external network. The gatekeepers in the form of layer 3-4 firewalls provided the much needed assurance and resilience to protect from external threats. In some instances it was complemented by Intrusion Detection/Prevention Systems. The ‘internal’ elements with patched end points and antivirus software fortified the network. Alas this simplistic model, though essential

Even today no longer provides the level of assurance it provided earlier. The BYOD program saw an influx of personal devices with a variety of operating systems. The enterprise no longer owned and controlled all the end points. The devices that traditionally were outside the trusted perimeter were now connected to the internal network. These devices tip toed inside the perimeter due to their physical proximity; however some devices even when physically remote became part of the trusted network. Virtualized servers hosted by IaaS and PaaS providers and applications provided by SaaS that are physically away from the perimeter need to be part of the trusted network. The traditional firewalls that had no visibility on the application layer were not much useful in regulating traffic to the cloud since IP addresses changed at irregular intervals.

Check Your Progress :

1. Define term Cyber Crime.

2. Explain the classification of Cyber Crime.

3. Short note on Hacking.

4. Define tem Cyber Space.

5. Describe Criminal behavior.

6. List out Traditional problems with Computer crimes.

7. Explain realms of Cyber world.

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Refer the Topic no 1.2.

2. Refer the Topic no 1.3.

3. Refer the Topic no 1.4.

4. Refer the Topic no 1.5.

5. Refer the Topic no 1.5.

6. Refer the Topic no 1.7.

7. Refer the Topic no 1.12.

1.14 FURTHER READING

- Read the Cyber Crime topic related book.