IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Comprehensive Analysis Of Cyber Crimes And Cyber Security Tools

[1]Dr.P.Venkadesh, [2]Dr.S.V.Divya, [3]B.Sudarson, [4]S.Sowmiyan,[5]S.Sebin,[6]N.Vishal
[1,2] Professor, [3,4,5,6] U.G Student
[1]Department of Artificial Intelligence and Data Science,
V.S.B College of Engineering Technical Campus, Coimbatore-642109

Abstract: With the increasing reliance on digital technologies in both personal and professional spheres, cyber security has become crucial than before. Cyber threats continue to evolve, ranging from simple phishing scams to sophisticated hacking techniques. As a result, individuals, organizations, and governments need to stay vigilant and continuously update their cyber security measures to mitigate risks and safeguard their digital assets.Hence numerous cyber tools has been designed to overcome the cyber threats that evolve in and around the globe.In this paper, basic knowledge about cyber crimes, the technologies involved in it , the research gaps and the future directions are reviewed. Moreover, a few cyber tools have been analyzed to highlight their features.

Index Terms - Cyber security, Cyber threats, Risks, Cyber crimes, Cyber tools.

I. INTRODUCTION

Technology in the digital age has brought about unprecedented convenience, connectivity, and innovation, fundamentally changing the way we live, work, and interact with the world around us. With the widespread use of the internet and computer networks, our world has become more interconnected than ever before. However, this digital interconnectedness also brings along new risks and challenges, one of the most significant being cyber crimes. Cyber crimes refer to illegal activities carried out using digital technology and the internet. These offenses encompass a wide range of illicit actions committed by individuals, groups, or even nation-states with malicious intent. The motive behind cyber crimes can vary, including financial gain, political motives, espionage, or even personal vendettas.

The types of cyber crimes are diverse and continually evolving, as perpetrators adapt to exploit new vulnerabilities. Some common examples of cyber crimes include:

Hacking: Unauthorized access to computer systems, networks, or websites to steal sensitive data, disrupt services, or cause harm.

Phishing: Deceptive attempts to acquire sensitive information, such as passwords and financial data, by posing as a trustworthy entity.

Malware: The computer systems were affected by unwanted programs known as malware.

Identity Theft: Illegally obtaining and using someone's personal information for fraudulent purposes.

Distributed Denial of Service (DDoS) Attacks: DDoS stands for Distributed Denial of Service. It's a type of cyberattack where multiple compromised computer systems, often infected with malware, are used to target a single system, website, or network. The goal of a DDoS attack is to overwhelm the targeted system with a flood of incoming traffic, rendering it inaccessible to legitimate users.

Cyber bullying: Using digital platforms to harass, threaten, or intimidate individuals.

Intellectual Property Theft: Unauthorized reproduction or distribution of copyrighted materials and intellectual property.

The impact of these cybercrimes are large such as demolishing entire society as a whole. Victims can suffer financial losses, reputational damage, and emotional distress.

Additionally, cybercrimes can disrupt critical infrastructure, compromise national security, and lead to data breaches with far-reaching implications. Addressing cybercrimes demands a comprehensive strategy involving multiple stakeholders and layers of defense which focuses on firewalls encryption techniques which is employed to mitigate the risks. Moreover, raising awareness about potential threats and educating users about safe online practices are essential in combating cyber crimes.

As technology continues to advance, cyber crimes will remain an ongoing challenge, demanding continuous efforts to stay ahead of malicious actors. Collaborative initiatives between public and private sectors, along with international cooperation, are crucial in developing robust cyber security strategies to protect individuals, businesses, and nations from the growing menace of cyber crimes

II. LITERATURE REVIEW

To protect the confidentiality of information systems, cyber security plays a major concern. The challenges and the vulnerabilities in cyber security [1] were focused.The transition from "Information Security" to cyber security [2] reflects a broader scope and evolving landscape in safeguarding digital assets and systems. While information security primarily focused on protecting data and information assets, cyber security encompasses a wider range of concerns, including protecting digital infrastructure, networks, and systems from cyber threats. The shift in terminology acknowledges the increasing interconnectedness and digitization of systems, highlighting the need for a more holistic approach to security that addresses not only data protection but also the security of the underlying technologies and networks.

Information Security Management System (ISMS) [3] evaluation typically involves assessing various aspects related to assets, threats, and vulnerabilities within an organization's information security framework such as threat assessment, vulnerability assessment,asset identification etc.Understanding and addressing stakeholders' concerns regarding cyber crime [4] involves identifying all relevant parties, such as executives, employees, customers, and regulators, and comprehending their worries about cyber threats. It includes educating stakeholders about cybersecurity risks and best practices, fostering transparent communication channels, implementing robust risk management frameworks, ensuring compliance with regulations, developing effective incident response plans, and continuously improving cybersecurity measures based on feedback and evolving threats. This approach aims to build trust, enhance awareness, and mitigate cyber risks for all stakeholders involved.

Absolutely, the increasing sophistication of cyber threats [5-7] is a significant concern in the realm of cybersecurity. Cybercriminals are indeed leveraging advanced technologies such as artificial intelligence (AI), machine learning (ML), and automation to launch more targeted and sophisticated attacks. These attacks often bypass traditional security measures [8-10], making them challenging to detect and mitigate. As a result, organizations must adopt proactive and adaptive security strategies to defend against these evolving threats.

Another key trend is the rise of ransomware attacks. Ransomware has become a lucrative business for cyber criminals, with attacks targeting organizations of all sizes across various industries. Indeed, one of the increasingly prevalent types of cyber attacks is ransomware. Ransomware attacks involve encrypting critical data or locking users out of their systems and demanding ransom payments, typically in cryptocurrency, in exchange for decryption keys or restored access. This form of attack has become a lucrative business model for cybercriminals, as it allows them to directly monetize their malicious activities. The proliferation of ransomware-as-a-service (RaaS) platforms has made it easier for even novice hackers to launch ransomware attacks, which poses threat to all.

III. CYBERCRIMES :A GLANCE

Cyber crimes, also known as computer crimes or internet crimes, refer to illegal activities conducted through digital technology and the internet. These criminal activities exploit vulnerabilities in computer systems, networks, and digital devices to commit offenses with malicious intent. Cyber crimes encompass a wide range of illicit actions, and they can be committed by individuals, organized groups, or even state-sponsored actors. Due to the tremendous growth of technology has expanded the scope and complexity of cybercrimes, has threatening us to a greater extent.

3.1 Classification of Cybercrimes

Cybercrimes are classified into various categories based on the nature of the offense and the intended target. The following are some common

Hacking: Stealing the confidential data or disrupting the computer systems or causing harm to it by unauthenticated persons.

Phishing: Deceptive attempts to acquire confidential sensitive information, such as passwords and financial data, by posing as a trustworthy entity.

Malware: Malicious software designed to infect and compromise computer systems, including viruses, worms, trojans, and ransomware.

Identity Theft: Illegally obtaining and using someone's personal information for fraudulent purposes, such as making unauthorized transactions or opening accounts in their name.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: Overloading a target's server or network with a flood of traffic, rendering services inaccessible.

Cyber Espionage: Unauthorized access to sensitive information, trade secrets, or intellectual property for the purpose of gaining a competitive advantage or national interests.

Data Breaches: Unauthorized access and disclosure of sensitive information, often resulting in the exposure of personal data or sensitive corporate information.

Online Fraud: Various fraudulent activities conducted over the internet, including online scams, fake auctions, and pyramid schemes.

Cyberbullying and Online Harassment: Using digital platforms to harass, threaten, or intimidate individuals, often leading to emotional distress and harm.

Cyberstalking: Persistent and unwanted surveillance or harassment of individuals through online communication channels.

Online Child Exploitation: The use of the internet to distribute, produce, or possess child pornography or engage in illegal activities involving minors.

Intellectual Property Theft: Unauthorized reproduction, distribution, or use of copyrighted materials, patents, and trade secrets.

Cyber Terrorism: Using cyber techniques to intimidate, coerce, or create fear in individuals, organizations, or governments for ideological, political, or religious purposes.

3.2 Real-world scenarios of cyber attacks

Real-world cyber-attacks were highly affected by individuals, businesses, and governments worldwide. Here are some notable examples of significant cyber-attacks and their consequences:

Stuxnet (2010): Stuxnet is a type of worm which was invented in the year 2010. It is widely considered to be one of the most2 complex malware ever created, notable for its targeted attack . Stuxnet represents a landmark in the history of cyber warfare, demonstrating the capabilities of sophisticated malware to target and disrupt critical infrastructure systems. Its discovery and analysis have led to advancements in cybersecurity practices, particularly in the protection of industrial control systems against cyber threats.

Sony Pictures Hack (2014): In November 2014, a group of hackers believed to be associated with North Korea breached Sony Pictures' computer systems. The attackers leaked confidential documents, emails, and unreleased movies which leads to the economic as well as the financial crises. The incident was allegedly in response to the planned release of the movie "The Interview," which depicted a fictional assassination plot against North Korea's leader.

WannaCry Ransomware (2017): This ransomware had affected more than 150 countries globally. It exploited a Windows vulnerability and encrypted users' data, demanding a ransom in Bitcoin for its release. The attack impacted critical infrastructure, including hospitals and government organizations, causing operational disruptions and financial losses. It highlighted the potential dangers of unpatched systems and the need for robust cybersecurity measures.

Equifax Data Breach (2017): This event was occurred in 2017 where credit card information of individuals were leaked out. This tends to be the most largest cyber threat happened in those days in US . This tends to be the highest breach which leaks the secret information of about 147 million people.

NotPetya (2017): NotPetya was a destructive malware attack that primarily targeted organizations in Ukraine but quickly spread globally. It used the Eternal Blue exploit, similar to WannaCry, to propagate within networks. The attack affected major multinational companies, disrupting operations and causing financial losses. NotPetya demonstrated the potential for cyber-attacks to have far-reaching economic impacts.

SolarWinds Supply Chain Attack (2020): This targets especially the SolarWinds software company in 2020. The attackers inserted a malicious code into SolarWinds' Orion software updates, compromising thousands of organizations and government agencies, including sensitive U.S. government networks. The attack was attributed to a state-sponsored group and raised concerns about the security of software supply chains.

These examples illustrate the serious implications of cyber-attacks on various sectors, from critical infrastructure to multinational corporations and government entities. They underscore the importance of robust cybersecurity practices, continuous monitoring, and international cooperation in combating cyber threats. As technology continues to evolve, cyber-attacks will remain a persistent challenge, necessitating ongoing efforts to strengthen cyber defenses and raise awareness about potential risks.

IV. THE TACTICS BEHIND CYBER CRIMES

The motivations and tactics behind cybercrimes can vary widely, as they are driven by the diverse objectives and goals of cybercriminals. Understanding these motivations and tactics is essential in developing effective strategies to combat cyber threats. Here are some common motivations and tactics observed in cybercrimes:

4.1 Motivations behind Cybercrimes

Financial Gain: One of the primary motivations for cybercrimes is financial profit. Cyber criminals may target individuals or organizations to steal financial information, conduct fraudulent transactions, or extort money through ransomware attacks. The potential anonymity of the internet makes it an attractive platform for carrying out illegal financial activities.

Espionage and Cyber Warfare: National and International wide actors are widely egaged in illegal activities like stealing sensitive information in areas like military, defense etc. Cyber warfare involves using cyber-attacks as a means of disrupting or disabling an adversary's critical infrastructure or communication networks.

Hacktivism: Hacktivists are motivated by ideological or political reasons and use cyber-attacks to promote a specific cause, protest against social or political issues, or advocate for particular beliefs. Their targets may include government websites, corporations, or other entities they perceive as opponents.

Intellectual Property Theft: Cyber criminals may target organizations to steal intellectual property, trade secrets, and proprietary information. This stolen data can be employed for their personal gain or be sold on the dark web to interested parties.

Data Breaches for Sale: Cyber criminals may infiltrate systems to collect valuable data, such as credit card information, personal identities, or medical records, which they can sell on underground markets to other cyber criminals.

Disruption and Vandalism: Some cyber-attacks are conducted for the sole purpose of causing chaos, disruption, or reputational damage. This can involve defacing websites, disrupting services, or spreading false information.

4.2 Tactics used in cybercrimes

Phishing and Social Engineering: Cyber criminals often use phishing emails, messages, or phone calls to deceive users into exposing user credentials.

Malware and Exploits: Unwanted softwares, such as viruses, worms, ransomware, and trojans, is commonly employed to infiltrate systems, steal data, or disrupt operations.

Advanced Persistent Threats (APTs): APTs are stealthy and sophisticated attacks that target specific organizations for long periods, often remaining undetected while gathering valuable data.

Distributed Denial of Service (DDoS): DDoS attacks overload a target's servers or networks with a flood of traffic, rendering services unavailable to legitimate users.

Zero-Day Exploits: Cybercriminals may exploit previously unknown vulnerabilities (zero-days) in software or systems before developers can patch them.

Insider Threats: Due to the cyber criminals inside the organizations, the confidential information may be leaked.

Supply Chain Attacks: Cyber criminals target software vendors or suppliers to insert malicious code into legitimate software updates, affecting multiple organizations downstream.

Understanding these motivations and tactics is crucial for organizations and individuals to bolster their cybersecurity measures effectively. Implementing robust security practices, raising awareness, and fostering a security-aware culture can help mitigate the risks posed by cybercrimes. Additionally, collaboration between public and private sectors, law enforcement agencies, and international cooperation is vital in combating the evolving landscape of cyber threats.

V. CYBER SECURITY

Cyber security is a broad field that encompasses various measures and strategies to protect computer systems, networks, and data from threats and attacks. Here are some common types of cyber security as shown in fig.1.

Data Security: Involves safeguarding data from unauthorized access, loss, or theft. Encryption, access controls, and data backup are essential components.

Network Security: Focuses on protecting the integrity, confidentiality, and availability of data as it travels across networks . This includes IDPS and VPNs.

Application Security: Securing software applications, including web and mobile apps, to prevent vulnerabilities and protect against exploits.

Cloud Security: Addresses the unique security challenges of cloud computing, ensuring the protection of data and resources in cloud environments.

IoT Security: focuses on securing the growing network of connected devices, often referred to as "smart" devices, that make up the IoT ecosystem.

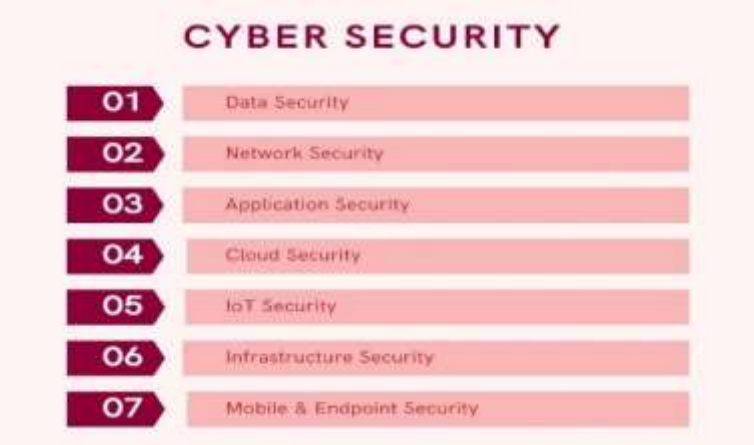

Fig.1 . Types of Cyber Security

Infrastructure Security: Infrastructure security focuses on safeguarding the critical physical and digital assets that form the foundation of an organization's operations, including its IT systems, networks, data centers, and other essential components.

Mobile & Endpoint Security: The former addresses security concerns specific to mobile devices, such as smartphones and tablets while latter involves securing individual devices, such as computers, smartphones, and IoT devices, to prevent unauthorized access and ensure data protection.

VI. CYBER SECURITY TECHNOLOGIES

Cyber security tools and technologies play a critical role in safeguarding computer systems, networks, and data from cyber threats and attacks. These tools are designed to detect, prevent, and respond to various types of security incidents. Here are some essential cyber security tools and technologies commonly used in the field are shown in fig.2.

Fig.2. Cyber Technologies

Antivirus Software: Antivirus software is one of the foundational cybersecurity tools. It scans computer systems and files for known malware signatures and behaviour patterns. When a virus or malware is detected, the antivirus software takes appropriate actions, such as quarantining or deleting the infected files.

Firewalls: Absolutely, firewalls are essential components of network security, acting as a protective barrier between trusted internal networks and potentially malicious external networks like the internet.The network traffic is monitored and filtered by the firewall based on certain metrics like filtering rules thus preventing the unauthorized access. Web Application Firewalls (WAF) provide security for web applications by filtering

and monitoring HTTP requests and responses. They protect against common web-based attacks, such as SQL injection and cross-site scripting (XSS).

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): IDS and IPS are designed to monitor network traffic and detect suspicious or malicious activities. IDS passively analyze network packets, while IPS actively intervene to block or prevent potential threats.

Encryption Tools: To protect the data from unauthorized access, encryption technique is employed. Data can be either at rest (stored on storage devices) or in transit(transmitted over networks).

Multi-Factor Authentication (MFA): Multi-factor authentication (MFA) is a security measure that requires users to provide two or more forms of verification before gaining access to an account or system. It adds an extra layer of security beyond just a username and password, making it significantly more difficult for unauthorized individuals to access sensitive information.

Virtual Private Networks (VPNs): A Virtual Private Network (VPN) is a technology that allows users to establish a secure and encrypted connection over a less secure network, such as the internet. It enables users to access resources and services securely while maintaining privacy and confidentiality.

Threat Intelligence Platforms: Threat intelligence platforms (TIPs) are tools or solutions designed to aggregate, correlate, analyze, and disseminate threat information and intelligence. These platforms help organizations better understand the threats they face, enabling them to make informed decisions about cybersecurity defenses and responses.

Artificial Intelligence (AI) and Machine Learning (ML) in Cybersecurity: Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being integrated into cybersecurity to enhance threat detection, response, and overall security posture.AI and ML technologies play a critical role in augmenting traditional cybersecurity approaches by providing advanced threat detection, rapid response capabilities, and adaptive security measures to defend against increasingly sophisticated cyber threats.

VII CYBER TOOLS

There are numerous cyber security tools and technologies available to defend against cyber threats. Effective cyber security involves deploying a combination of these tools, along with robust security policies, employee training, and proactive incident response planning. Additionally, cyber security professionals continuously monitor the threat landscape and update their defensive strategies to stay ahead of evolving cyber threats. This section explains about the different cyber security tools available. The top most recommended cyber tools are listed below:

1.***NMap:*** NMap is an open source network tool mainly used for discovering hosts, the corresponding services and also used for security auditing and vulnerability assessment. Nmap is a skilled and essential tool for network administrators, security professionals, and penetration testers. Its comprehensive feature set, flexibility, and reliability which focuses on network reconnaissance, security assessment, and threat detection. Host Discovery , service discovery and Port scanning are the important features of Nmap.

2. ***Kali Linux***:Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It comes packed with a variety of tools used for network security assessments, ethical hacking, and computer forensics tasks. Kali Linux provides a robust platform for security professionals and enthusiasts to test and assess the security of networks and systems. It includes tools for information gathering, vulnerability analysis, wireless attacks, web application assessments, password cracking, and much more. Kali Linux is widely used by cybersecurity professionals, researchers, and hobbyists for various security-related tasks and projects.

3.***Burp Suite:*** It is a security testing tool mainly used for testing the web application. It is widely used by security professionals, web developers, and penetration testers to assess the security of web applications. Burp Suite offers a range of features designed to identify vulnerabilities and potential security flaws in web applications. Some of its key features include: Proxy, Spider, Intruder,Repeater etc.Burp Suite is a comprehensive toolset for web application security testing, offering a range of features to identify and mitigate potential vulnerabilities in web applications. However, Burp Suite can automate many aspects of security testing, manual inspection and verification are often necessary for thorough assessment and validation of findings.

4. ***Angry IP Scanner :*** Angry IP Scanner is a popular open-source network scanner designed to scan IP addresses and ports within a network. It is commonly used by network administrators and security professionals to identify active devices, discover open ports, and gather information about the network. Some of its features are: cross-platform compatibility, Fast scanning,Customizable scan parameters etc.Angry IP Scanner is often used for tasks such as network inventory, troubleshooting network connectivity issues, detecting unauthorized devices or services, and assessing network security. However, it's important to note

that while Angry IP Scanner can provide valuable information about a network, it should be used responsibly and ethically, respecting privacy and legal boundaries

5. ***Cain & Abel :*** Cain & Abel is a Windows-based password recovery tool that is primarily used for recovering various types of passwords through different methods. It is developed by Massimiliano Montoro and is widely used by security professionals, penetration testers, and system administrators for legitimate security purposes.Network sniffing, for recovering passwords, wireless network auditing, VoIP recording are some of the features of it. However, it's essential to note that Cain & Abel can also be misused for illegal activities, such as hacking into systems without proper authorization, and therefore its usage should comply with ethical and legal guidelines.

6.***Ettercap :*** Ettercap is a comprehensive suite for man-in-the-middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis. Ettercap is primarily used for network analysis and security auditing. It allows security professionals to monitor network traffic, perform man-in-the-middle attacks, and analyze the security posture of networked systems.

7.***Etherpeek:***Etherpeek is a powerful tool for network administrators, security analysts, and IT professionals who need to monitor, analyze, and troubleshoot network traffic effectively. Its comprehensive features and intuitive interface make it a valuable asset for network management and security operations. It is a network protocol analyzer, offering unparalleled capabilities for capturing, analyzing, and troubleshooting network traffic. With its extensive features, real-time monitoring, and advanced analysis capabilities, Etherpeek remains a cornerstone tool for network management, security analysis, and performance optimization. As organizations continue to rely on robust and secure networks, Etherpeek will continue to serve as an essential asset in ensuring network reliability, security, and performance.

8.***Network Stumbler:*** Network Stumbler, also known as NetStumbler, is a popular Windows-based tool used for discovering wireless networks (Wi-Fi) in the vicinity. It is primarily used for wardriving, which involves driving or walking around with a Wi-Fi-enabled device to detect and map out wireless networks. Network Stumbler is a handy tool for discovering and mapping wireless networks, making it useful for network administrators, security professionals, and enthusiasts interested in Wi-Fi network exploration. However, it's important to note that the tool has not been actively maintained or updated in recent years, and it may not be compatible with newer Wi-Fi standards or operating systems.

9.***ToneLoc :*** ToneLoc stands for Tone Locator "Tone Locator," is a discontinued open-source tool developed by "mudge" (also known as Peiter Zatko) in the 1990s. It was primarily designed for exploring and manipulating the telephone network. ToneLoc was particularly known for its ability to generate and detect various tones used in the telephone system, such as dial tones, ringing tones, and DTMF (Dual-Tone Multi-Frequency) tones.

10.***LC4 :*** LC4, also known as L0phtCrack 4, is a discontinued password auditing and recovery tool developed by the security research group L0pht Heavy Industries. It was designed to assess the strength of passwords used in Windows operating systems and recover lost or forgotten passwords through various methods. LC4 was widely used by security professionals, system administrators, and penetration testers for auditing password security and testing the resilience of user passwords.

11.LANguard Network Security Scanner: LANguard Network Security Scanner, developed by GFI Software (now known as Kerio Control), is a comprehensive network security scanner designed to identify vulnerabilities, security misconfigurations, and potential threats within a network infrastructure. It is primarily used by network administrators, security professionals, and IT teams to assess and improve the security posture of their networks. LANguard Network Security Scanner provides a comprehensive solution for network vulnerability assessment, patch management, and security compliance auditing. Organizations can enhance their overall security posture and mitigate the risk of cyber threats and data breaches by addressing its issues proactively.

12.Wireshark: Wireshark is a widely used network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It is open-source and cross-platform, available for numerous OSs. This tool is used by network administrators, security professionals, developers, and researchers to troubleshoot network issues, analyze network protocols, and investigate security incidents. Its rich feature set and user-friendly interface which is utilized for anyone working with computer networks.

13.Metasploit: Metasploit is a widely used penetration testing framework developed by Rapid7. It provides security professionals, penetration testers, and ethical hackers with a comprehensive set of tools and resources for conducting security assessments, vulnerability testing, and exploit development. Metasploit is a powerful and versatile penetration testing framework that provides security professionals with the tools and resources

needed to assess and improve the security of their systems and networks. It is widely used in the cybersecurity industry for ethical hacking, red teaming, and security research.

14.***NetworkMiner:*** NetworkMiner is a popular network forensic analysis tool that is used for detecting and analyzing network traffic. It runs on Windows and Linux operating systems and is widely utilized by network administrators, security professionals, and researchers for investigating network incidents, analyzing network protocols, and extracting information from captured network traffic. Its intuitive interface, comprehensive features, and support for various network protocols make it a popular choice among security professionals for investigating network incidents and analyzing network traffic.

VIII. RESULTS

In this section, the cyber tools are demonstrated and analyzed their performances.

NMap: The NMap tool can be used for various purposes such as port scanning, TCP scanning, UDP scanning , to detect service running and OS version, state of the ports etc . The fig.3 demonstrates the host IP address 192.168233.129 is scanned and performed ARP ping scan, SYN Stealth Scan,OS detection.

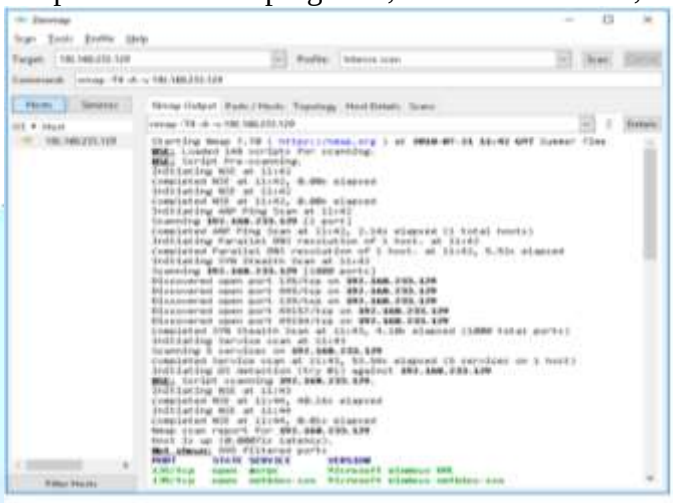

Fig. 3. NMap tool

Wireshark: Wireshark is a powerful network analyzer tool that allow users to capture the live network analyzer in real time. It is widely used by network administrators, security professionals, developers, and researchers to analyze the network protocols, troubleshoot network issues, and detect potential security threats.

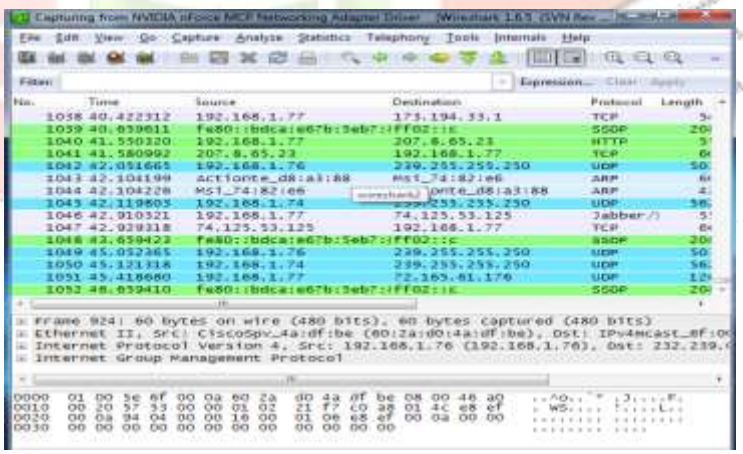

Fig. 4. Wireshark capturing live packets

Fig.4. shows the wireshark captures the live traffic including the IP version, number of packets captured, source address and the destination address etc.

Ophcrack:Ophcrack is a free and open-source Windows password cracker that utilizes rainbow tables to recover passwords from Windows operating systems. It is primarily used for recovering lost or forgotten passwords by analyzing password hashes stored in the Windows SAM (Security Account Manager) database as shown in fig.5. It's important to note that while Ophcrack can be effective for recovering simple or weak passwords, it may struggle with complex or strong passwords that are resistant to rainbow table attacks. Additionally, Ophcrack cannot recover passwords that are not present in its rainbow tables. Therefore, its effectiveness depends on the quality and coverage of the rainbow tables used.

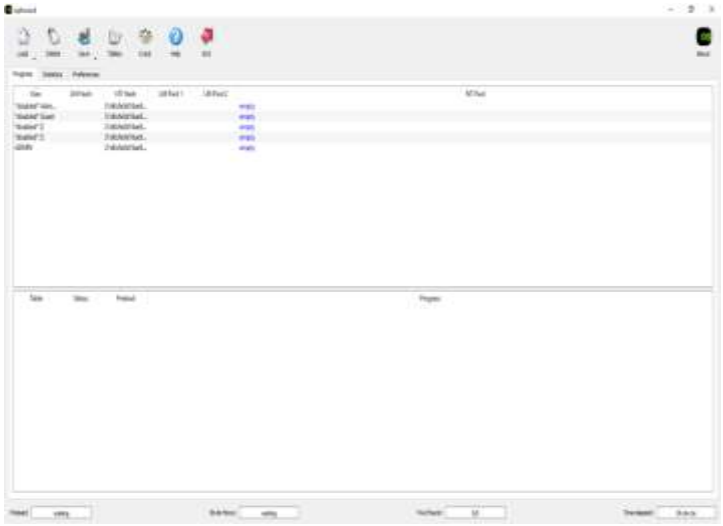

Fig. 5. Password cracking using Ophcrack

SmartSniff: For capturing and viewing the TCP/IP packets which pass through the network adapter, SmartsSniff is used. However, for analyzing the network traffic, for troubleshooting and for debugging purposes it is highly recommended. As shown in fig.6, the source and the destination address along with its port number are anlayzed.

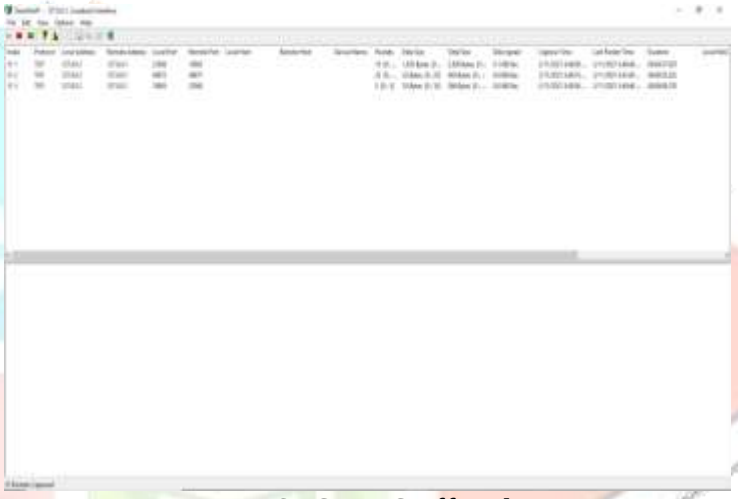

Fig.6. SmartSniff tool

NetworkMiner: NetworkMiner is a popular network forensic analysis tool . It is primarily used by network administrators, security professionals, and forensic investigators to monitor and investigate network activity, detect security incidents, and extract information from captured network traffic. NetworkMiner is a powerful and versatile network analysis tool that provides valuable insights into network traffic, facilitates network forensics investigations, and helps detect and respond to security incidents effectively. Its intuitive interface, comprehensive features, and support for various network protocols make it a valuable asset for network security professionals.

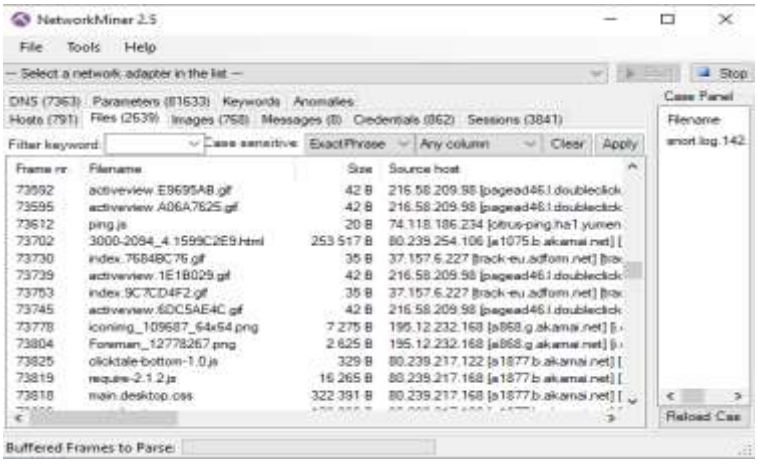

Fig.7 Network Miner

Figure.7 shows the Network miner tool analyzing the frame number along with the filename, size and the source host.

IX RESEARCH GAPS

Among the various cyber tools exists only some have been analyzed here and observed that all these tools cant be applied to gain its benefits thoroughly. This section highlights some of the research gaps faced by these tools.

- Lack of automated vulnerability detection in dynamic environments.
- Lack of automated incident response system.
- Inability to identify the user behavioral analytics.
- Lack of advanced tools to offer high end security in cloud and resource constrained IoT devices.

X CONCLUSION AND FUTURE DIRECTIONS

Here, numerous cyber tools and their outputs were demonstrated. However effective cyber security also requires a combination of technical solutions, user education, and proactive risk management strategies. It's not just about deploying the latest security tools but also fostering a security-aware culture where everyone understands their role in protecting sensitive information and maintaining cyber security hygiene.To overcome the existing research gaps, the current cyber tools need to be incorporated with the latest technologies such as : Artitifical Intelligence, Machine Learning, Intelligent Systems, Cloud Computing , Quantum Computing and Super Computing etc.

REFERENCES

[1] Wasyihun Sema Admass , Yirga Yayeh Munaye , Abebe Abeshu Diro, "Cyber security: State of the art, challenges and future directions",Cyber Security and Applications,vol.24,2024.

[2] Rossouw von Solms, Johan van Niekerk, "From information security to cyber security",Computers and Security,vol.38, 2013.

[3] Kwo-Jean Farn, Shu-Kuo Lin , Andrew Ren-Wei Fung, "A study on information security management system evaluation—assets, threat and vulnerability", Computer Standards and Interfaces,vol.26, no.6,2004.

[4] Nigel Martin, John Rice, "Cyber crime: Understanding and addressing the concerns of stakeholders",Computers and Security, vol.30, No.8, 2011.

[5] Jagpreet Kaur, K .R. Ramkumar, "The recent trends in cyber security: A review",vol.34,no.8,2022.

[6] R. Sharma, "Study of latest emerging trends on cyber security and its challenges to society", International Journal of Scientific & Engineering ,vol.3.no.6,2012.

[7] J. Jang-Jaccard, S. Nepal, "A survey of emerging threats in cyber security", Journal of Computer and System Sciences,vol.80,no.5,2014.

[8] lSeong Oun Hwang, Taekyoung Kwon, Wei-Chuen Yau, DaeHun Nyang"Special Issue on Cyber Security and AI", ETRI Journal,2019.

[9] G.D. Rodosek, M. Golling, "Cyber security: challenges and application areas",Supply Chain Safety Management,Springer-Verlag Berlin Heidelberg,2013.

[10] P Venkadesh, JPM Dhas, SV Divya, "Techniques to enhance security in SCTP for multi-homed networks", Global Conference on Communication Technologies (GCCT), 468-473,2015.