GOVERNMENT OF INDIA

myGov

Search by #tag or Title...

Indian Space Research Organisation (ISRO)

SEARCH

containing:

इसरो isro
Indian Space Research Organization
Government of India Department of Space
SMART INDIA HACKATHON '17

Indian Space Research Organisation (ISRO)

The Department of Space (DoS) is an Indian government department responsible for administration of the Indian space program. It manages several agencies and institutes related to space exploration and space technologies.The Indian Space Research Organization (ISRO) has been assigned the task of conducting the Smart India Hackathon 2017 on behalf of Department of Space. They have identified 53 problem statements.

Develop a solution for Document tracking within an organization network

#ISR53 Total Submissions : 16

Some of the documents which may be restricted are generally available with multiple persons in an organization. It is essential to keep the trace of such documents for keeping accountability and knowing the

USB and (2) file sharing. Student solution should demonstrate that the file is now available at 3 locations; original as well as 2 destinations.

Student may use Linux machine in place of window if he is more comfortable with the OS.

Sample Data Required: No

PARTICIPATE

Develop a solution for protecting photocopy of Highly Confidential Documents

#ISR52 Total Submissions : 8

We can restrict distribution, copying and printing highly confidential documents but still there remains a possibility of copying information from such documents using external methods such as taking photo of the screen using an external camera while the document is displayed on it. Work out a solution to protect a document in above scenario. Demonstrate a POC to detect such an attempt.

Sample Data: All prerequisite hardware/software required for simulation is to be arranged by participant/organizer

PARTICIPATE

Design a solution to detect Physical Intrusion detection

#ISR51 Total Submissions : 12

PARTICIPATE

Design a solution to restrict usage of public mailing service from government infrastructure

#ISR50 Total Submissions : 9

Usage of public mailing service like gMail, Yahoo, etc. from government infrastructure is prohibited especially when organization provide own email service. There are large number of know mailing service and there could be unlimited unknown mail services. It is easy for anyone to setup his own mail server and start mail service easily using various tools. Google apps is one of such tool.

SMTP ports could be easily blocked using a firewall but accessing mail service through webmail (HTTP/HTTPS) is still is a challenge. There might be unlimited mailing service hence blocking based on domain name is also not possible.

Work out a solution which can detect such an attempt to connect such web mail server using HTTP/HTTPS and block it.

Notes: Simulate a small network or a machine connected to Internet. Demonstrate that it blocks the access of gmail, yahoo mail, etc without blocking the domain or IP.

Sample Data Required: No

PARTICIPATE

Develop a solution to detect backdoors in network routers

#ISR49 Total Submissions : 8

Notes: Simulate a back doored router to demonstrate the solution. For simulation purpose, use a router with known back doored firmware or modify publicly available firmware to create a backdoor and use it in a router for POC purpose.

Sample Data Required: No

PARTICIPATE

Develop a solution to detect backdoors in components of enterprise infrastructure

#ISR48 Total Submissions : 1

Solution should be able to detect backdoors in following components:

Applications and OS.
Desktop/server hardware.
Network switch.
Router.
Modem.
Smartphone.
The solution can be a toolkit comprising of separate solutions for each component.

Notes: The participants can attempt individual parts of the problem if they are not able to address all the components.

Sample Data Required: No

PARTICIPATE

Spear phishing is an email that appears from an individual or business that you know, but it isn’t. The spear phisher thrives on familiarity. The phisher usually knows your name, your email address, and at least a little about you. The salutation on the email message is likely to be personalized: “Hi Bob” instead of “Dear Sir“. This information is usually extracted from social networking sites or your recent online purchases. These factors tempt you to take action specified in the email without being vigilante.

These mails generally contain malicious attachments or URLs which lead to phishing or malicious websites which ask for your credit card/bank details or your passwords in disguised manner. Demonstrate a POC to detect such mails and block them.

Student should configure a email server with 2 users. Student should send a Spear Phishing mail from any external mail server (say gmail) . His solution should be able to detect the same.

Sample Data Required: No

PARTICIPATE

Implement secure data transfer using steganography

#ISR46 Total Submissions : 26

Steganography is a process of concealing file, message, image or video within another file. Often this technique is used to bypass the scanners which look for specific formats or extensions. Design and Implement a novel approach of securely transferring confidential data using this technique.

Sample Data: To be simulated by the participant

Notes: All the servers/services required for POC have to be simulated by the participants

PARTICIPATE

Total Submissions : 12

In an organization working in secure environment, it is necessary to ensure that Internet access is provided to the users with restrictions on data upload. HTTPS provides end to end secured encrypted channel between end user machine and destination server. Similarly, SFTP also provides end to end secured encrypted channel between end user machine and destination FTP server. Since application data is encrypted in these protocols, it is hard to detect the document/data uploading. Work out a solution which can detect the document/data upload through all encrypted data transfer protocols. Solution should also be able to detect the websites providing upload features and subsequently block them.

Sample Data: Not required

Notes: The solution should be able to detect data upload by monitoring network traffic from the machines and must be capable of blocking it. The participants can also use any other approach like agent based solution blocking upload on the end point itself, but users should not able to bypass it by killing the agent or some other methods.

PARTICIPATE

Data leakage detection and prevention of confidential documents

#ISR44 Total Submissions : 8

A major requirements for all the organizations is securing the confidential documents. In current era, there are multiple ways in which data is regularly transferred from an organization. Hence it is necessary to have a mechanism for checking transmission of unauthorized/restricted data. Implement a solution which:

1.Flags any confidential document sent outside organization via email.

2.Flags any confidential document being uploaded on Internet Website

Sample Data: To be simulated by the participant

Notes: All the servers/services required for POC have to be simulated by the participants

PARTICIPATE

Implement a solution which preserves Secret and Top Secret Documents

#ISR43 Total Submissions : 14

Secret and top secret documents are not at all shared. As per old procedure, such documents are printed and ensured that the softcopy is destroyed. In today digital world there is need to work out solution to protect such digital documents.

Problem 1: Since server and storage admins have unrestricted access over the system and its file system, the restricted document is accessible to them even if not shared. Workout solution to protect such document even from server and storage admins.

Problem 2: In event of physical breach to the servers, the documents must be protected. Workout solution to protect such document cannot be accessed even after stealing the storage hardware. Please suggest a solution other than encryption.

Student is expected to declare/protect a file as confidential and store it at a location on server. The specified file should not be accessible even with the root access of the server.

The student should mount the storage (hard disk) where the file is stored on another server/system and the file shouldn’t be accessible.

Sample Data: To be simulated by the participant.

Secure distribution of restricted documents outside the organization

#ISR42 Total Submissions : 9

Organization have variety of documents out of which some documents are very sensitive. Such documents are required to be protected. The Sensitive documents are classified as restricted and Confidential. Implement a solution to cater the following problems:

End users require sharing the document with others to achieve desired goal. Existing freeware, PDF writer, Word, etc provide document security features for password protection, disabling cut, paste, copy, save, print, etc. This security can be bypassed easily by experts. Workout solution to provide high level of document security to ensure that document is neither viewed by unauthorized person nor copied partial/fully.

Student should declare a doc file as confidential. This file should be not be accessible to unauthorized persons. It should be deleted on 3 unauthorized attempts.

PARTICIPATE

Building Trusted Execution Environment for Linux

#ISR41 Total Submissions : 2

Trusted execution (TE) includes a group of features which can verify the integrity of files in an OS like Linux. It can thus block any attempts to execute malicious code that is not part of the trusted database. Hence, developments for Linux OS are needed such that

Hashed signature for following types of files can be generated for Linux OS any time
- Kernels and kernel extensions
- All setuid root programs, All setgid root programs

Any change in Hash signature database shall be effective only after reboot of OS.
Sample Data Required: No

PARTICIPATE

[Develop a cloud based centralized repository for distribution, management and updating of cyber security tools for government organisations.]

#ISR40 Total Submissions : 1

This aims at creation of a secure centralized repository security tools viz., anti-virus, anti-malware, IPS, IDS etc., for an organization.
The repository shall have the provision for on-the-fly updating from reliable sources on the Internet
The end-user system shall be dynamically updated so that zero-day attacks are addressed effectively.
System administration shall be alerted for the surge of threats in the Internet so that stringent monitoring of the organization can be effected.
This infrastructure shall have a proactive mechanism to alert the government agencies using the fastest mode of communication so that the government agencies can adopt the countermeasures to mitigate the cyber security threats.
Notes: Participate should manage cloud based resources to demonstrate the approach

Sample Data Required: No

PARTICIPATE

Detecting Virus Spread through Network Connection

same). Advanced Viruses have self-spreading capabilities. Such Virus scans the machines connected on network to find out vulnerabilities of the remote machines. It will propagate by exploiting the vulnerabilities. An agent based solution is to be worked out to detect such propagation. Agent will run on all the machines. It will send abnormal behaviour or detected anomaly to the server for further automatic analysis to arrive upon conclusion.

Notes: Simulate a small network of 3 machines to demonstrate the virus spread. Use machines without any anti-virus installed and infect it with a self-propagating virus. At least one machine on the network should have vulnerabilities exploitable by the virus. Run agent-based solution on all the machines. The solution should be able to generate alerts about the virus infection/propagation.

Sample Data Required: No

PARTICIPATE

Simulate Virus Spread through Network Connection

#ISR38 Total Submissions : 8

If an organization is infected by ZERO-day virus attack, their antivirus solutions would not be able to detect the same. (Antivirus solutions depends on the virus signature and behavior which could be obtained only after their teams know about it. Zero-day attack is the first attack and hence Antivirus teams are not aware about the same). Advanced Viruses have self-spreading capabilities. Such Virus scans the machines connected on network to find out vulnerabilities of the remote machines. It will propagate by exploiting the vulnerabilities.

Students should simulate a small network of 3 Windows-7 or 10 to demonstrate the virus spread. Use machines without any anti-virus installed. Develop a small program pretending as Virus. It should be able to find out vulnerability of other machines connected on network and spread itself of other machines.

Sample Data Required: No

Develop a solution for protecting App distribution

#ISR37 Total Submissions : 10

Web based model for distributing the smart phone app among the authorized persons is very popular. Although web site provides a level of protection against the app copying and forging, it is not enough. Work out a solution which ensures integrity, proper installation, and usage of an app.

Sample Data Required: No

PARTICIPATE

Develop an Add-on for any popular open-source VPN solution for improving the security of authentication

#ISR36 Total Submissions : 8

VPN is one of the most widely used solution for implementing secure communications outside the periphery of the organization. However, the password based authentication remains a point of failure in such scenarios. There is a need to add additional authentication factors in the solution. Due to widely used standard solutions, it is preferable to use existing solutions with such an add-on. Customize any popular open-source VPN solution to enable secure authentication using additional authentication methods such as asymmetric key cryptography, biometric or OTP methods. Apart from username and password, it should have 2 more authentication mechanism.

Note: Users can use widely popular open source VPN solutions such as OpenVPN.

Sample Data Required: None

PARTICIPATE

Keystroke dynamics uses the manner and rhythm in which an individual types characters on a keyboard. It is used for behavioral biometrics wherein an identity of person is determined or verified based on the patterns and timings of the key strokes. Develop a solution which implements key strokes dynamics as an authentication/verification mechanism minimizing the false positives

Sample Data Required: Simulate sample data for demonstration

PARTICIPATE

Design a Network level Application Layer Firewall

#ISR34 Total Submissions : 1

Demonstrate a POC of an application layer firewall that works on network traffic passing through the gateway. The firewall should have the capability of analyzing traffic of all protocols at the application layer. Subsequently, it should allow application layer traffic from a customized application layer protocol and block all other protocols.

Notes: Simulate a small network to demonstrate the approach

Sample Data Required: No

PARTICIPATE

Work out novel approach to implement honey pot/net/service/app in real live surfing environment to detect attack or/and machine compromise.

#ISR33 Total Submissions : 7

Student should implement a live server (website or webmail) and honeypot/honey net along with it. Student should simulate some known attacks on the server and the solution should be able to detect the attack and redirect the attacker to honeypot/honey net and record his activities, path, his machines details and footprint.

Sample Data Required: No

PARTICIPATE

Develop a solution to detect payloads generated by tools like veil-evasion

#ISR32 Total Submissions : 5

Tools like veil-evasion have come up in recent times that are capable of bypassing anti-virus solutions. These tools use a lot of advanced evasion techniques, generates polymorphic payloads to avoid signature detection. Following techniques are used to evade detection:

Randomization of variable names and methods
Encryption of source
Native stagers (shellcode-less)
Method nops (randomizing program’s call tree via dummy methods)
Obfuscated loaders
Figure out solutions for better detection of each of these payloads.

Notes: For demonstration generate payloads using veil-evasion which is open source.

Sample Data Required: No

PARTICIPATE

A exploit kit is a software kit designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it, and discovering and exploiting vulnerabilities in it to execute malicious code on client. Exploit kits are modular, allowing easy addition and removal of vulnerabilities and provides a user interface to control the settings, thereby automating the entire process of compromising a client. The exploit kit uses known available browser vulnerabilities and as soon as a client request reaches the web server running exploit kit (through traffic redirection), exploit kit checks the client browser for vulnerabilities and exploits it if the browser is found vulnerable and provides a remote shell of victim machine to control it. The participants are required to develop such a exploit-kit with a GUI

Students should form a small network of 2-3 computers with popular browser (chrome/firefox) installed. They should perform the exploitation on the browser using the developed kit from the other computer in the network and demonstrate the comprising and thereafter controlling the target machine.

Sample Data Required: No

PARTICIPATE

Design a solution to detect Arp-spoofing attacks originating within a network

#ISR30 Total Submissions : 9

ARP Attacks aims at poisoning the ARP records of a machine so as to silently eavesdrop or manipulate all the data that is sent over the network. ARP spoofing is done so as to carry out MAN IN THE MIDDLE attacks where all traffic from client machine to a server is directed through an attacker’s machine. ARP attacks can only be carried out within a LAN. A security application is required that is capable of detecting ARP-based attacks originating within the network. Work out new approach to detect such attacks. The solution could use active/passive approaches to detect arp records tampering. The solution could be agent based which could be run on all machines on a network or a solution that could be run on network devices like switch/routers etc.

GOVERNMENT OF INDIA

PARTICIPATE

Home

Terms & Conditions

Sitemap

Associate with Mygov

Contact Us

About Us

Feedback

FAQ

Link to Us

NATIONAL INFORMATICS CENTRE

Last Updated:February 8, 2017 at 10:44 am -- innov-web-sp-83-145.mygov.in

SWACHH BHARAT | eGreetings | india

Power To Empower | Open Government Data (OGD) Platform India | india | MeitY