MITRE

ICCS 2012 January 9 - 12, New York City
International Conference on Cyber Security

Rules for All Challenges

1. You must be a registered attendee of ICCS 2012 to participate in this challenge.

2. Scoring will be done as follows: Let t_s be the start time for question N in seconds since the epoch, t_e be the end time for question N in seconds since the epoch, and M be the maximum point value for question N. If Alice submits an answer to question N at t_q (in seconds since the epoch) then Alice's score for question N can be found by calculating $M - M * \frac{2(t_q - t_s)}{5(t_e - t_s)}$. Therefore, the points earned for each question decreases linearly over time from M if the answer was submitted right at the start to $\frac{M}{5}$ if the answer was submitted right at the end. If no answer is submitted to a question, the contestant will earn 0 points for that question. Each contestant's final score will be the sum of his/her scores from all the questions.

3. To submit an answer, e-mail the answer, and a description of how you arrived at the answer to Dane Smith (ICCS12@mitre.org).
   - The subject line of the e-mail must be of the following format: "ICCS-ANSWER-N" where N is the number of the question.
   - Your answer must contain the answer itself and a description of how you arrived at it.
   - Your answer must be in English.
   - You agree to share your answer with the challenge organizers.

4. You may only submit one answer to each question. In the case multiple submissions are sent, only the first submission will be scored.

5. Questions regarding any of the challenges will be answered only if clarification is deemed necessary. No response is guaranteed, and rapid response cannot be relied on. The challenges were designed to be self-explanatory. To submit a question, e-mail Dane Smith (ICCS12@mitre.org) with the following subject line "ICCS2012QUESTION."

6. MITRE employees and ICCS 2012 staff are not eligible for the prizes.

7. The deadline for submissions is dependent on the challenge. See each challenge for details.

8. The challenges should be treated as confidential during the conference. Sharing them with a non-conference participant will result in disqualification.

9. Winners will be announced by the end of the conference.

10. All decisions are final.

MITRE

ICCS 2012 January 9 - 12, New York City
International Conference on Cyber Security

Day #1 Challenge

Maximum 10 Points

Challenge Statement:
The purpose of this challenge is to recognize when classic cryptography has been used in a digital environment to break it.

Hypothetical Scenario:
You find an odd file on your system. It is not a file that you created, and it definitely isn’t something created by the Operating System or an application. Figure out what is actually contained in the file.

The Challenge is:
Decrypt the file and find the password that has been hidden inside it. Submit the password as your answer. It should be all upper case, and it should start with a “S” and end with a “D”.

Rules Specific to this Challenge:
You may use any numerical or cryptographic software (either online or stand-alone) to solve this challenge.

Deadline:
Submissions must be in by 10:00PM EST on 1/10/2012. Anything submitted after that time will not be considered.

MITRE

ICCS 2012 January 9 - 12, New York City

International Conference on Cyber Security

Day #2 Challenge

Maximum 10 Points

Prerequisite:
You will need the answer from Day # 1 to solve this challenge. It is contained in the day2.zip file under the name day1 solution.txt.

Challenge Statement:
This challenge is meant to illustrate the number of places and ways adversaries can hide information. In this challenge, the purpose is to learn how to spot strange looking images files and search for data hidden within them.

Hypothetical Scenario:
After you found the first encrypted file, you spot an image file that looks decidedly too large for what it should be. Located the data hidden within it.

The Challenge is:
Find the data hidden in the image file. The information you need is contained in that hidden data. Submit the name of the file you should be on the lookout for in the future as your answer. It should start with a “h” and end with an “I”. The case of each letter does matter.

Rules Specific to this Challenge:
Hex editors, image software, and programs you have written are all valid for this challenge.

Deadline:
Submissions must be in by 10:00PM EST on 1/11/2012. Anything submitted after that time will not be considered.

Day #3 Challenge

Maximum 10 Points

Prerequisite:
You will need the answer from Day # 2 to solve this challenge. It is contained in the day3.zip file under the name day2 solution.txt.

Challenge Statement:
The purpose of this challenge is to illustrate ways to look for strange behavior in network traffic.

Hypothetical Scenario:
After you found the strange image, the local network administrators tell you that a large file was transferred off your computer to an unknown source. They provided you with a capture of the network traffic. Find the file that was sent and figure out what was inside it.

The Challenge is:
Locate the file sent over the network. Then locate the stolen information. The key phrase you found yesterday will likely help you locate the information you need. The sensitive data starts with a "P" and ends with a "k". Submit the sensitive data as you answer. The case of each letter does matter.

Rules Specific to this Challenge:
Any network traffic analysis tool, hex editor, or programs you have written can be used for this.

Deadline:
Submissions must be in by 1:00PM EST on 1/12/2012. Anything submitted after that time will not be considered.

MITRE

ICCS 2012 January 9 - 12, New York City
International Conference on Cyber Security

Multi-Day Challenge

Maximum 25 Points

Challenge Statement:

The purpose of this challenge is to recover the private ECDSA key used for sending cryptographically signed data given two signatures.

Hypothetical Scenario:

You are given two ECDSA signatures. Something about them looks strange. Using that, recover the signing (private) key used to generate the signatures.

The Challenge is:

Using the two signatures along with the known public key and parameters, find a way to recover the private key used to generate the signatures. Submit the private key, in hexadecimal, as the answer.

Rules Specific to this Challenge:

You may use numerical software (online or stand-alone) or any program you have written to solve this challenge.

Deadline:

Submissions must be in by 1:00PM EST on 1/12/2012. Anything submitted after that time will not be considered.