TU Wien
Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software
Arbeitsgruppe ESSE
http://security.inso.tuwien.ac.at/

CTF Regeln und Informationen

CTF Rules and Information

SS2014

2014-05-28

Inhaltsverzeichnis / Table of Contents

1 CTF-Regeln

(for English version please see section 4 on page 8)

In diesem Kapitel finden Sie die Regeln, die Sie während des CTF-Contests beachten müssen. Sehen Sie sich auch die Informationen zu den Punkten (Kapitel 2 auf Seite 6) an. Dort steht auch mehr zu den Flags, die Sie sammeln können.

1.1 Allgemeines

Dieser CTF-Contest wird im Rahmen der Lehrveranstaltungen *Security for Systems Engineering* und *IT Security in Large IT Infrastructures* abgehalten. Dadurch ist es erforderlich, dass neben der Verteidigung des eigenen Rechners und dem Angriff der Rechner anderer Gruppen auch ein Protokoll verfasst wird.

Die virtuellen Images werden von uns zur Verfügung gestellt. Auf den Hosts, welche diese virtuellen Images hosten, und auf den Images selbst wird es keinen Internetzugang geben.

Falls Sie Hinweise, Kritik oder Wünsche in Bezug auf den CTF-Contest haben, teilen Sie uns diese bitte per e-mail an `lva.security@inso.tuwien.ac.at` mit. Besten Dank!

Die Regeln für diesen CTF-Contest sind zum Teil aus Regeln anderer CTF-Contests angepasst. Dazu gehören die Regeln des da.open(2005), UCSB International Capture The Flag [Vig13], Hack In The Box Conference 2005 CTF [Box05].

1.2 Beurteilung

Die Notengebung für die Lehrveranstaltungen basiert auf dem Gruppenprotokoll, das Sie erstellen müssen. Achten Sie daher darauf, dass dieses detailiert ist. Eine Vorlage für das Protokoll ist vorhanden. Diese Vorlage erhalten Sie während dem CTF-Contest.

1.3 Protokoll

Das Protokoll muss am selben Tag abgegeben werden, an dem auch der CTF-Contest stattfindet. Nach dem Ende des CTF-Contests bleibt Ihnen noch Zeit, um das Protokoll fertigzustellen und im PDF Format in tuwel abzugeben.

Im Protokoll sollen Wege der Verteidigung und der Angriffe zusammen mit einigen technischen Hintergründen beschrieben sein. Der Umfang des Protokolls muss etwa 3.5-4 Seiten sein. Nehmen Sie auch Informationen über Angriffe auf, wenn Sie nicht funktioniert haben, für Sie aber vielversprechend ausgesehen haben. Sollten Sie Advisories (Kapitel 3 auf Seite 7) geschrieben haben, bitte nehmen Sie diese auch in das Abgabeprotokoll mit auf.

1.4 Grundsätzliche Hinweise

- Den Anweisungen der TutorInnen und VU-Mitarbeitern ist Folge zu leisten.
- Regelverstöße können Punkteabzüge bringen. Diese Punkteabzüge können sofort erfolgen oder nach einer Analyse der Angriffe nach dem Ende des CTF-Contests. Dazu wird der gesamte Traffic zentral mitprotokolliert.
- Die Gruppen dürfen nicht miteinander kommunizieren. Die Gruppengröße beträgt zwischen 3-5 Personen und es dürfen keine externen Personen kontaktiert werden.
- Falls Sie denken, dass eine Gruppe unfair handelt, teilen Sie es uns bitte mit.

Die nachfolgenden Regeln sind nicht vollständig. Sie zeigen vielmehr eine Richtung auf, in die gearbeitet werden soll. Der Sinn dieser praktischen Übung ist es, dass gelernt werden kann, wie man Systeme richtig und effektiv absichert. Denken Sie bei Ihren Handlungen an die Fairness und daran, dass es allen TeilnehmerInnen auch eine Freude bereiten soll an dem CTF-Contest teilzunehmen.

1.5 Angriff

- Es dürfen nur die Rechner mit den Images angegriffen werden, welche von uns ausgegeben werden. Angriffe außerhalb der Übungsumgebung oder Angriffe auf Rechner von TeilnehmerInnen sind untersagt. Dies inkludiert natürlich auch Angriffe auf z.B. den Gameserver.
- Nach einem erfolgreichen Angriff muss das gefundene Flag auf dem Gameserver eingetragen werden. Erst dann wird ein Angriff als erfolgreich gewertet und das angreifende Team erhält Punkte.
- DoS Angriffe durch Flooden etc. sind verboten.
- Das Löschen und ändern von Flags wird als unfair angesehen und führt zu Punkteabzug.
- Die gestohlenen Flags müssen gleich eingetragen werden, sie haben nur eine begrenzte Gültigkeitsdauer.

1.6 Mögliche Status Meldungen beim Abgeben von Flags am Gameserver

- `Status:scored` Erfolgreicher Angriff.
- `Status:resubmission` Das Flag wurde bereits abgegeben.

- `Status:denied` Das eigene Service funktioniert nicht richtig, Abgabe abgelehnt.
- `Status:expired` Flag ist abgelaufen.
- `Status:error` Fehlerhafte Eingabe. Die genaue Beschreibung wird ausgegeben.

1.7 Verteidigung

- Es ist nicht erlaubt Zugriffe an Hand der IP Adresse via Firewall zu beschränken. Alle notwendigen Services müssen von allen teilnehmenden Rechnern erreichbar sein. Insbesondere ist damit auch gemeint, dass es verboten ist nur Zugriffe vom Gameserver zu erlauben und andere TeilnehmerInnen zu blockieren.
- Es ist nicht erlaubt Zugriffe auf Applikationsebene zu filtern und dadurch z.B. nur die Zugriffe des Gameservers zu erlauben.
- Es dürfen keine Mechanismen aktiviert werden, um Buffer Overflows zu verhindern. Ihre Aufgabe ist es Schwachstellen zu erkennen und diese auszubessern.
- Es dürfen bei Programmen keine auf der Website spezifizierten Funktionen deaktiviert werden, selbst wenn der Gameserver nicht alle Funktionen bei den Zugriffen verwendet.
- Zur Absicherung von Systemen dürfen die Services neu kompiliert oder Scripts angepasst werden. Dabei ist jedoch zu beachten, dass die spezifierten Funktionalitäten erhalten bleiben.

1.8 Abschließende Tipps

- Beachten Sie, dass Sie nach Ende des CTF-Contests ein Protokoll abgeben müssen.
- Denken Sie daran, dass Sie die Funktionalitäten der Services nicht zu sehr einschränken, damit der Gameserver die Wertungen vornehmen kann, indem Flags deponiert und abgefragt werden.
- Planen Sie Ihr Vorgehen. Eventuell sollten Sie schon vorab vereinbaren wer für Angriffe/Verteidigung/Protokoll zuständig ist.
- Überlegen Sie sich, ob Sie Backups der Konfigurationen/Services anfertigen wollen.
- Seien Sie fair!

2 Punkte für den CTF-Contest

Für den CTF-Contest können Sie auf unterschiedliche Arten Punkte sammeln. Dieses Kapitel beschreibt im Detail wie Sie Punkte erhalten. Die ersten 3 Plätze werden nach dem Ende des Bewerbs Preise erhalten.

2.1 Allgemeines

Sie erhalten Punkte sowohl für eine erfolgreiche Verteidigung Ihrer Services, als auch für erfolgreiche Angriffe auf Services anderer Teams. Auch für gute Advisories (Kapitel 3 auf Seite 7) erhalten Sie Zusatzpunkte, die manuell durch die CTF-Contest Leitung vergeben werden.

Bitte beachten Sie dabei immer die Regeln (Kapitel 1 auf Seite 3). Sollten Sie nicht regelkonform am CTF-Contest teilnehmen, werden wir Ihnen Punkte, auch im Nachhinein, aberkennen.

2.2 Verteidigung

Sie erhalten Punkte, wenn Ihr Service als `OK` erkannt wird. Reduzierte Punkte erhalten Sie wenn das Service als `BROKEN` erkannt wird, was bedeutet, dass das Service erreichbar ist aber das Flag nicht erfolgreich abgefragt werden konnte.

Sie können auch nur Angriffspunkte für ein Service sammeln wenn Ihr eigenes Service zum Zeitpunkt des Submit `OK` ist.
Hinweis: Versuchen Sie immer zuerst Ihre eigenen Services zu härten und diese Verfügbar halten.

2.3 Angriffe

Sie greifen andere Services an, indem Sie Sicherheitslücken in den jeweiligen Services ausnützen und dadurch Flags finden, die Sie dann submitten müssen, um Punkte zu erhalten.

Flags sind Strings aus 32 Zeichen (z.B.: `02062011180450NLD3ZL8T6XW1QKSJUU`). Die ersten 14 Zeichen ist ein Java Date Format: `ddMMyyyyHHmmss`). Testweise erzeugte Flags haben `TEST` im String. (z.B.: `02062011180814TESTHY4970VUKCGZIF`)

Sie bekommen pro Service und Team für 4 Flags die volle Punkteanzahl. Danach werden die Punkte für Flags dieser Service-Team Kombination nur mehr zu 20% gezählt.
Hinweis: Sie sollten nun nicht mehr manuell arbeiten, sondern versuchen ein Script zu erstellen.

Wichtig: Wenn Sie den Angriff mittels Script automatisieren, nutzen Sie den Timestamp im Flag um nur die neusten Flags abzugeben. Senden Sie nicht in jeder Runde alle Flags an den Gameserver!

Jene Gruppen, die es schaffen, alle Services mindestens ein Mal erfolgreich zu attackieren, werden mit einem 15% Multiplikator belohnt - der Gesamtscore wird dann automatisch um 15% erhöht.

2.4 Advisories

Für abgegebene Advisories (Kapitel 3 auf Seite 7) bekommen Sie manuell Punkte von der Übungsleitung abhängig von der Qualität des Advisories. Sie können bis zu 100 Punkte für ein Advisory erhalten.

3 Advisories

Im Zuge des CTF-Contests können Sie Advisories verfassen und damit auch Zusatzpunkte erhalten. Die Zusatzpunkte werden manuell während des Spielverlaufs von uns vergeben. Wenn Sie Advisories schreiben, fügen Sie diese bitte auch Ihrem Abgabeprotokoll hinzu, damit diese auch im Zuge der Bewertung von lab2 berücksichtigt werden.
Hinweis: Bitte speichern Sie Ihr Advisory für Ihr Protokoll selbst. Nach der Abgabe des Advisories am Gameserver können Sie nicht mehr über diesen darauf zugreifen.

Ein Advisory ist eine Zusammenfassung einer Sicherheitslücke zusammen mit einem Exploit, der zeigt wie die Sicherheitslücke ausgenutzt werden kann. Gute Advisories beinhalten zudem einen Vorschlag, wie man die gefundene Sicherheitslücke korrigieren kann.

Wir werden abhängig vom Spielverlauf die von Ihnen submitteten Advisories bewerten und eventuell auch am Gameserver veröffentlichen. Sie können beruhigt sein, dass es Ihnen möglich sein wird, Punkte für den Angriff zu sammeln, bevor wir ein Advisory für alle sichtbar veröffentlichen :-).

Advisories werden abhängig vom Einlangen bei uns bewertet, d.h. früher eingelangte Advisories werden in der Bewertung bevorzugt. Die Punkteanzahl für ein Advisory hängt somit vom Zeitpunkt des Eintreffens, vom Detailgrad des Inhalts, der Korrektheit des Security Advisories, insgesamt der Qualität des Security Advisories ab.

Auch unvollständige Security Advisories werden gegebenenfalls von uns bewertet und erhalten Punkte.

4 CTF-Rules

(für die deutsche Version siehe Kapitel 1 auf Seite 3)

In this section you will find rules that must be observed during the CTF contest. Also note the information regarding points (section 5 on page 10), where you will find out more about flags.

4.1 General

This CTF contest will be held in the courses *Security for Systems Engineering* and *IT Security in Large IT Infrastructures*. Thus, it is necessary that in addition to the defense of your own system and the attacks of the other group's systems, a protocol has to be written for the grading of the exercise.

The virtual images are provided by us. On the hosts, which host these virtual images, and the images themselves, there will be no internet access.

If you have any comments, criticisms or requests regarding the CTF contest, please let us know via mail to `lva.security@inso.tuwien.ac.at`. Thank you!

The rules for this CTF contest are partly adapted from rules of other CTF contests. These include the rules of da.open (2005), UCSB International Capture The Flag [Vig13], Hack In The Box Conference 2005 CTF [Box05].

4.2 Grading

The grading for the courses is based on the protocol that you must create as a group. Therefore, make sure that this protocol is detailed. A template for the report exists.

4.3 Protocol

The protocol must be submitted on the same day of the CTF contest. After the end of the CTF contest you still have time to complete your protocol and submit it in PDF format in TUWEL.

The protocol has to include approaches of defense and attacks along with some technical background. The length of the Protocol must be about 3.5-4 pages. Also provide information about attacks, which you did not get to work properly, but have looked promising for you. If you have handed in advisories (section 6 on page 12), please attach them to the protocol.

4.4 Basics

- The instructions of the tutors and VU staff must be obeyed.
- Violations of the rules can bring points deductions. These points deductions can be made immediately or after an analysis of attacks after the end of CTF contest. Thus, all traffic is centrally logged.
- The groups may not communicate with each other. The group size is between 3-5 students and there must be no external persons to be contacted.
- If you think that a group acts unfair, please let us know.

The following rules are not complete. Rather, they point to a direction in which you want to work. The purpose of this practical exercise is to learn how to secure systems properly and effectively. Perform your actions fairly and consider the fact that the contest should be fun to all of the participants.

4.5 Offense

- You may only perform attacks via the provided images. Attacks outside the lab environment or attacks on computers of participants are prohibited. Of course, this includes attacks on the gameserver.
- After a successful attack, the flag found must be entered on the gameserver. Only then an attack is rated as a success and the attacking team gets points.
- DoS attacks by Flooding, etc. are prohibited.
- Deletion or alteration of flags is considered as unfair and leads to deduction of points.
- The stolen flags must be entered immediately, as they have a limited validity.

4.6 Possible status messages when handing in flags on the gameserver

- `Status:scored` Successful attack.
- `Status:resubmission` The flag has been submitted already.
- `Status:denied` Your own service does not work properly. No score.
- `Status:expired` Flag has expired.
- `Status:error` Incorrect input. The detailed description is given.

4.7 Defense

- It is not allowed to restrict accesses via firewall based on their IP. All necessary services must be accessible from all participating machines. In particular, it is forbidden to allow access from the gameserver only and to block other participants.
- It is not allowed to filter accesses on the application level and thus e.g. allow accesses by the gameserver only.
- It is not allowed to activate mechanisms to prevent buffer overflows. Your task is to identify vulnerabilities and to fix them.
- It is not allowed to disable any functions of the services specified on the website, even if the gameserver does not access all of the functions.
- For the protection of your systems, the services may be recompiled and scripts may be adapted. However, it is important that the specified functionalities retain working.

4.8 Final Hints

- Note that you have to submit a protocol after the end of the CTF contest.
- Remember that the gameserver deposits and queries flags on your services to evaluate their functionality.
- Plan your strategy. You may want to arrange in advance who is responsible for offense, defense and protocol.
- Think about whether you want to make backups of your configurations and services.
- Be fair!

5 Points for the CTF Contest

There are several ways to collect points for the CTF contest. This page describes how to obtain points in detail. The top three teams will receive prizes after the end of the contest.

5.1 General

You get points for both a successful defense of your services, as well as for successful attacks on services of other teams. Additionally, you will receive points for good advisories (section 6 on page 12) - these points will be assigned manually by the CTF administration.

Please always observe the rules (section 4 on page 8). If you do not act compliant to the rules, we will deduct points, even in hindsight.

5.2 Defense

You get points if your service is recognized as `OK`. You get reduced points if the service is recognized as `BROKEN`, meaning that the service indeed is available, but the flag could not be queried successfully.

Keep in mind, that you can collect offense points for attacking a service only if your own respective service is `OK` at the moment of submission.
Hint: Before attacking other services, try to harden your own services and keep them available.

5.3 Attacks

You attack other services by exploiting vulnerabilities in the respective services and thus find flags, which you have to submit to earn points.

Flags are strings of 32 characters (e.g., `02062011180450NLD3ZL8T6XW1QKSJUU`). The first 14 characters are a Java Date format: `ddMMyyyyHHmmss`). Flags for testing purposes contain the characters `TEST`. (e.g., `02062011180814TESTHY4970VUKCGZIF`)

You will get full points for the first 4 submitted flags per service/team combination. Afterwards, the additional offense points for flags of this service/team combination are only counted for 20%.
Hint: You should now no longer work manually, but try to create a script, which automatises your attacks.

Those teams, who manage to successfully attack all services at least once, will be rewarded with a 15% multiplicator, i.e., your total score will then be increased by 15% automatically.

5.4 Advisories

If you hand in advisories (section 6 on page 12), you will get points manually from the CTF administration. You can receive up to 100 points for an advisory, depending on its quality.

6 Advisories

As part of the CTF contests you can hand in advisories and thus earn extra points. The additional points are awarded manually during the game by the CTF administration. If you create advisories, please make sure to add them to your protocol so we can take them into account for the evaluation of lab2.
Note: Please make sure to save your advisories before submission yourself, as you wont be able to access them after submission any more.

An advisory is a summary of a vulnerability with an exploit that shows how the vulnerability can be exploited. Good advisories also include a suggestion of how to fix these vulnerabilities.

We will evaluate your submitted advisories and - depending on the course of the game - also publish them on the gameserver for other teams. You can be assured that you will be able to earn enough attacking points before we publish an advisory :-).

The score of your advisories depends on the time of submission, i.e. the earlier you hand it in, the more points you will earn. Furthermore, the level of detail of the content, the correctness and the overall quality of the security advisories are taken into account at evaluation.

Incomplete advisories will be evaluated too and may score points.

Literatur

[Box05] Hack In The Box. *HITBSecConf2005*. [Online; abgerufen am 2013-06-06]. 2005. URL: http://conference.hitb.org/hitbsecconf2005kl/?p=35.

[Vig13] Giovanni Vigna. *The 2007 UCSB International Capture The Flag*. [Online; abgerufen am 2013-06-06]. 2013. URL: http://ictf.cs.ucsb.edu/archive/iCTF_2007/index.html.