IT SECURITY RESEARCH GROUP

rwthCTF 2011 - Cyberwar the Flag!

RWTH AACHEN UNIVERSITY

Virtual Capture the Flag (CTF) tournaments

Explained using the example of the UMIC rwthCTF 2011, September 30, 2011

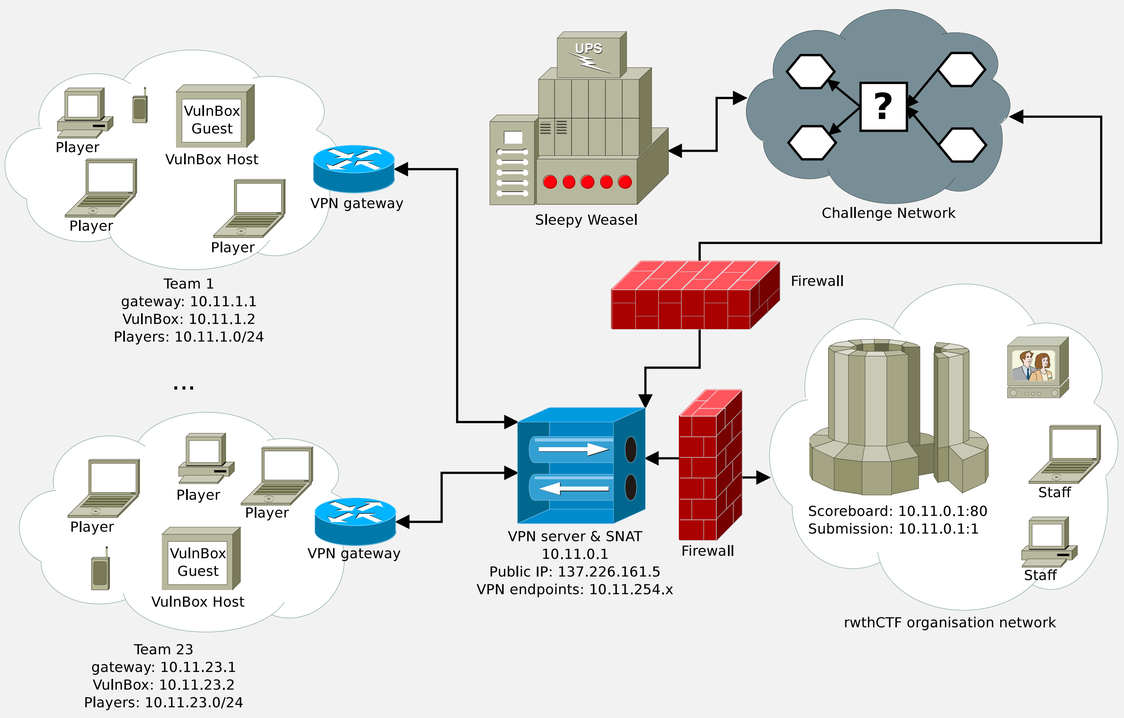
Motivation

Capture the Flag (CTF) tournaments serve the purpose of educating IT security professionals and researchers about hands-on offensive and defensive security. Participants compete as part of a team, defending their own server while attacking other teams. The creative use of technology and knowledge of software problems is encouraged by a relatively loose set of rules.

The *UMIC rwthCTF 2011* was the first CTF organized within the UMIC research cluster by the IT Security Research Group. The UMIC research cluster also sponsored the prize-money for the three winning teams.

The CTF Network

There is a common structure for CTF networks. The teams play within a private Virtual Private Network (VPN), to avoid interferences with any public infrastructure in the Internet or the University. A team cannot distinguish between network traffic originating from the VPN server and from other teams.



The CTF organizers offer basic services to the teams, such as a scoreboard (see below), a server to submit stolen flags and, in the rwthCTF 2011, the Challenge Network.

The Server (VulnBox)

VulnBox Host

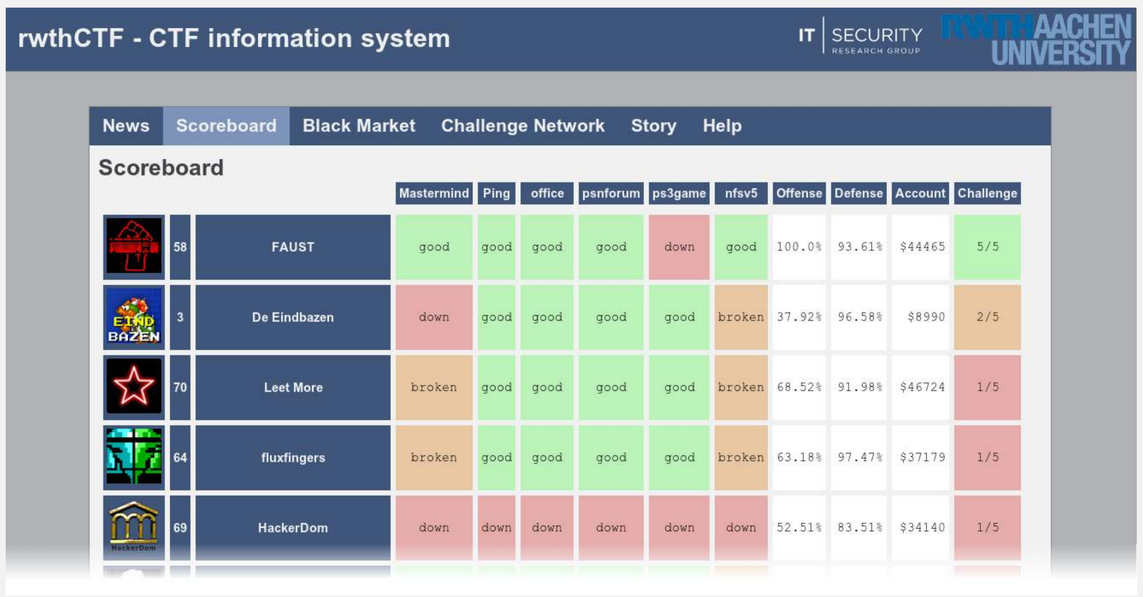
Shortly before the CTF starts, the teams are supplied with a virtual Linux computer image. This image has been carefully prepared by the CTF organizers, and it already contains all of the services which the teams have to run. It has intentional security vulnerabilities which the teams can use to attack other teams and fix them in their own system.

The Flag

In this example, the Gameserver stores a flag with one service of Team 5. It then waits for a few minutes before trying to retrieve the flag. If the flag is still there and has not already been copied and submitted (i.e. stolen) by another team, Team 5 receives defense points. Stealing another team's flag is rewarded with offense points.

The Scoreboard

During the CTF, teams can access the Scoreboard to check the current score and the state of the services of each team. The virtual Black Market is also part of this interface.

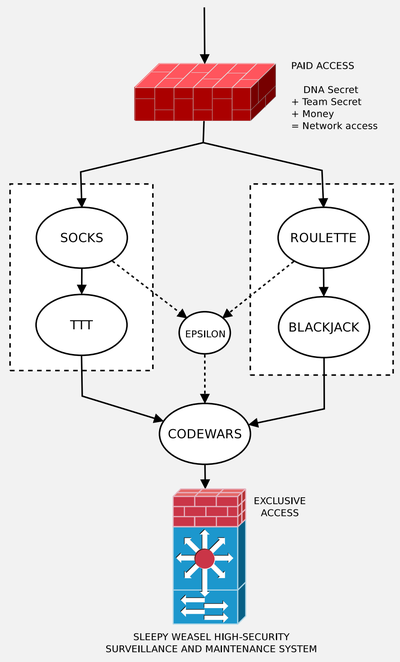


		Mastermind	Ping	office	psnforum	ps3game	nfsv5	Offense	Defense	Account	Challenge
58	FAUST	good	good	good	good	down	good	100.0%	93.61%	$44465	5/5
3	De Eindbazen	down	good	good	good	good	broken	37.92%	96.58%	$8990	2/5
70	Leet More	broken	good	good	good	good	broken	68.52%	91.98%	$46724	1/5
64	fluxfingers	broken	good	good	good	good	broken	63.18%	97.47%	$37179	1/5
69	HackerDom	down	down	down	down	down	down	52.51%	83.51%	$34140	1/5

Advisories

Advisories on how to exploit and fix security vulnerabilities can be written and submitted during the tournament. These advisories enter a virtual black market, where they are reviewed and can subsequently be sold to interested teams. In the real world, well written advisories about high-profile security vulnerabilities are regularly traded for high rewards. Criminals and software vendors are equally interested in learning about unpublished security vulnerabilities.

The Challenge Network



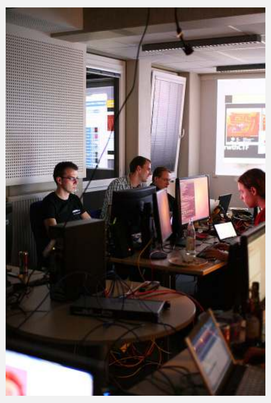
The Challenge Network is a layered riddle. On each layer, at least one riddle or challenge has to be solved to advance to the next layer.

The differences between these challenges and the services are twofold. The challenges do not hide the fact that they were fabricated with the intention to be solved. Furthermore, they also include problems which are of a theoretical or very playful nature.

In the rwthCTF 2011 Challenge Network, there were binary exploitation challenges, an Android cellphone challenge, cryptographic challenges, and the CodeWars game, which is about computer programs that fight against each other.

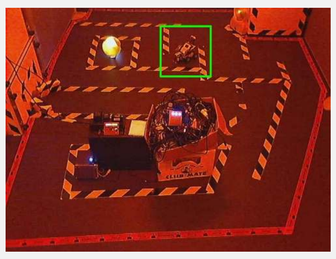
Teams which successfully completed all of the stages of the network would gain access to the robot control, a simple command-line interface and a webcam to steer a small LEGO robot through a maze and win the rwthCTF 2011.

Infrastructure



rwthCTF HQ

The rwthCTF 2011 team headquarters were set up in the seminar room of the Research Group IT Security in the UMIC building. The servers needed for the tournament were running in the ITSec lab room.



The robot control

The robot was located in an adjacent storage room and could remotely be controlled through a wireless connection.

The current progress of the CTF could be monitored on two projectors with real-time reporting.

UMIC rwthCTF 2011 Team

UMIC rwthCTF 2011 team (students and faculty of the Research Group IT Security)

The rwthCTF 2011 team (in alphabetical order):

Cornelius Aschermann (CodeWars challenge, Office service), **Johannes Barnickel** (Communication, Documentation), **Jó Ágila Bitsch Link** (DNA Challenge, ComSys), **André Egners** (Communication), **Felix Glaser** (CodeWars challenge), **Johannes Gilger** (Scoreboard, Press), **Tobias Jarmuzek** (Homepage, Robot), **Marián Kühnel** (Crypto challenge), **Elvin Mehmedagic** (Android challenge), **Ulrike Meyer** (Head of Research Group), **Georg Neugebauer** (Crypto challenge, Robot control), **Mark Schlösser** (Network, DB, NFSv5 service), **Florian Weingarten** (Mastermind service), **Georg Wicherski** (Binary Exploitation, ps3game service)

References

- CIPHER CTF - http://www.cipher-ctf.org/ (old CTF organized by i4 RWTH)
- UMIC rwthCTF 2011 - http://ctf.itsec.rwth-aachen.de