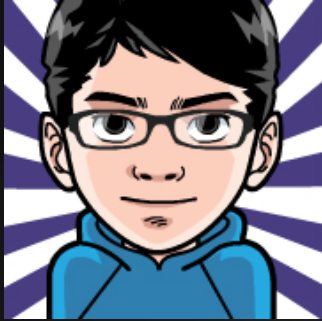


나의 중국 해킹대회 여행기

Belluminar XCTF와 XCTF 참가 후기

진용휘

발표자 소개



진용휘 / jinmo123

- 해킹대회를 4년 반 전부터 참가함
- 팀 내 역할 : 리버싱, 웹, 기타 등등

발표 내용

- 벨루미나 CTF 베이징 (WCTF)
- 제 2회 XCTF Final
 - 소개
 - 여정
 - 인상깊은 두 문제 간략한 설명

Belluminar CTF Beijing

1. 벨루미나 CTF



벨루미나란?

- 참가자들이 문제를 준비해가는 CTF
 - 이번에는 Windows 문제, 자유 문제 1개씩 냄
- 문제 제출은 CFP, 대회는 Geopardy

문제 출제

The screenshot shows a GitHub repository page for 'cykor-belluminar'. The repository is private and has 6 watches, 0 stars, and 0 forks. It has 116 commits, 6 branches, 0 releases, and 5 contributors. The latest commit is '0abcdef' on May 9. The repository contains a directory 'angry_jinmo' with a file 'alarm 시간 넉넉하게', a directory 'puljimara' with a file 'modified writeup', a file '.gitignore' with content 'ring3. writeup.', and a file 'README.md'. The README.md file is selected and shows the text 'cykor-belluminar' and '일하라'.

... / cykor-belluminar Private

Unwatch 6 Star 0 Fork 0

Code Issues 0 Pull requests 0 Pulse Graphs

No description or website provided.

116 commits 6 branches 0 releases 5 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

... Merge pull request #22 from .../angry_jinmo_finish Latest commit 0abcdef on 9 May

angry_jinmo	alarm 시간 넉넉하게	4 months ago
puljimara	modified writeup	4 months ago
.gitignore	ring3. writeup.	4 months ago
README.md		4 months ago

README.md

cykor-belluminar

일하라

CyKor → 벨루미나 베이징

CyKOR



From Korea University, was working together with Lokihardt for a period of time, with rewards of the championship of Trend Micro CTF Asia Pacific & Japan 2015 , HITCON CTF 2015 and HDCON CTF 2015.

Current CTFTIME 2016 Ranking: 31

참여한 팀들



베이징에는 어떻게 갔나요?

비행기표 & 비자 필요

비자가 엄격함 (입출국 날짜, 인원 등등...)

비자 잃어버리지 않기!

벨루미나 일정

~ 5.31

출국
대회 준비

6.1 ~ 6.3

대회
세미나 (문제 발표)

6.4

만리장성 여행
귀국

대회 문제 요약

난이도 ★★★★★

재미 ★★★★★★

운영 ★★★★★

- 문제 하나하나가 각 팀들의 엑기스..
- 어려웠지만 재밌었습니다.

인상 깊은 문제들

1. **BrowserFun** by KeyResolve
2. **blackbox** by HITCON
3. **ahyes** by MSLC

...

인상 깊은 문제 1

KeyResolve: BrowserFun

- 말 그대로 브라우저 공략 문제 (UXSS)
- Chrome 소스 코드에 취약점을 만듦

패치한 부분 (objects.cc)

- 15007 from_javascript -> false

```
15001
15002 Maybe<bool> JSReceiver::SetPrototype(Handle<JSReceiver> object,
15003                                     Handle<Object> value, bool from_javascript,
15004                                     ShouldThrow should_throw) {
15005     if (object->IsJSProxy()) {
15006         return JSPProxy::SetPrototype(Handle<JSProxy>::cast(object), value,
15007                                     from_javascript, should_throw);
15008     }
15009     return JSObject::SetPrototype(Handle<JSObject>::cast(object), value,
15010                                 from_javascript, should_throw);
15011 }
15012
```

이미지는 Chromium 소스 코드 검색 (cs.chromium.org) 캡처

유의사항

- 그 당시에는 `JSObject::SetPrototype`의 `from_javascript` 체크 부분의 `else` 부분이 없었음

공략

1. from_javascript는 JSProxy::SetPrototype을 통해 JSObject::SetPrototype으로 다시 전달됨
2. from_javascript가 false면 Origin 체크를 안하고 prototype을 설정 (그 당시에는 체크가 없었음)
3. 다른 Origin의 Object의 __proto__를 지정 가능

공략 (cont.)

1. `Object.setPrototypeOf`(

`Proxy(iframe.contentWindow), {a: 1});`

4. 해당 iframe에서는 jQuery를 쓰고 있었음

잘 맞춰주면 그 컨텍스트의 js 개체를 얻어올 수 있음

5. ex) "Function" 함수를 얻어와서 eval처럼 사용

HITCON의 blackbox

- Apache httpd mod_php + mod_jk
- 경로에 ;가 포함될 경우 php/tomcat에서 다르게 처리됨을 이용하는 문제
- Directory Listing -> leak -> ...

MSLC의 ahyes

- Pwnable + Cryptography
- 가장 충격과 공포의 조합
- 직접 보시길 추천합니다

링크: <https://github.com/leetchicken/belluminar/tree/master/ahyes>

대회 결과

KeyResolve 1370 / CyKor 1085 / HITCON 1065
TOOOOOOOOOO CLOSE.....

Rank	Team	Sharing Score	Answer Score	Rule Score	Total Score
1	KeyResolve	660	510	200	1370
2	CyKor	420	483	182	1085
3	HITCON	360	523	182	1065



벨루미나 CTF 후기

- 대우가 친절함
- 상금이 많음 (2천만원)
- 무엇보다도 재밌음 (상당히)

XCTF Finals 2016

https://jinmo123.gitbooks.io/blog/content/xctf_finals_2016.html

2. XCTF Finals

**2016 XCTF全球总决赛**
2016 XCTF Finals

CyKor | 退出

00:00:00

公告栏 / Bulletin 当前为第 180 轮

Web2 IP: 172.16.9.13
Web2 is open!
drawdraw ip: 172.16.9.5
drawdraw is open
Ip Mapping table:http://172.16.4.1/lpMapping.xls
Game

实时信息 / Event Log 00:00:00

07-17 15:55:47 CyKor 攻陷了 NuIL 的 drawdraw gamebox
07-17 15:55:47 CyKor 攻陷了 Shellphish 的 drawdraw gamebox
07-17 15:55:47 CyKor 攻陷了 NSIS 的 drawdraw gamebox
07-17 15:55:47 CyKor 攻陷了 NeSE 的 drawdraw gamebox
07-17 15:55:47 CyKor 攻陷了 NPC 的 drawdraw gamebox
07-17 15:55:47 CyKor 攻陷了 天板 的 drawdraw

本队服务状态 / Gamebox Status

服务正常

服务正常

服务正常

服务正常

未启用

未启用

auction

drawdraw

richman


xhttpd

web1


web2

当前名次	总分	总得分	总失分	与前一队分差	一血数量
1	22508.14	18100.20	1592.06	0.00	2

本队积分曲线图



本队名次曲线图



请在此输入答案 / Flag

提交

积分榜 / Scoreboard

XCTF Finals란?

- 중국 내에서는 XCTF League를 진행, 순위 책정
 - ALICTF, SSCTF, WHCTF, ... (각 대학에서 주최)
- 초청 팀 + 상위권 팀이 XCTF Finals에 초청됨
- 이번 본선은 blue-lotus가 출제함

대회 규칙

- 전형적인 공방전
 - 시스템 / 웹 문제를 풀고 5분마다 인증 (flag가 바뀜)
 - 자신의 바이너리 / 웹 서비스를 패치할 수 있음
- 6시에는 서버를 내림 (대회 막날 제외)
 - 숙소에서 풀면 됨

어떻게 가게 되었나요?

- 데프콘 우승팀으로 초청받음
- CyKor로 나감

XCTF 일정

■ DEF CON 23 통조림이네!

JUNE 1st	8:30-9:30	registration	Group Photo
	9:30	opening	
	10:00-10:30	CTF contest	
	10:30-10:45	Tea break	the contest will not be interrupted.
	10:45-12:00	CTF contest	
	12:00-13:00	Lunch	the server will not be stopped.
	13:00-15:30	CTF contest	
	15:30-15:45	Tea break	the contest will not be interrupted.
	18:00-20:00	Dinner	The serve will be stopped.
JUNE 2nd	9:30-9:40	opening	start the server
	9:40-10:30	CTF contest	
	10:30-10:45	Tea break	the contest will not be interrupted.
	10:45-12:00	CTF contest	
	12:00-13:00	Lunch	the server will not be stopped.
	13:00-15:30	CTF contest	
	15:30-15:45	Tea break	the contest will not be interrupted.
	18:00-20:00	Dinner	The serve will be stopped.

XCTF 일정

~ 6.30

출국
대회 준비

7.1 ~ 7.2

1박 2일간 대회
브라질리언 바베큐 파티

7.3

귀국

대회 문제 요약

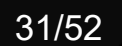
난이도 ★★ ★

재미 ★★ ★★ ★

운영 ★★ ★★ ★

- 무난한 운영, 데프콘보다는 쉬웠던 문제
- HITCON CTF Finals랑 유사함

■ 비주얼



인상 깊었던 점

■ 비주얼 2



인상깊은 문제들

- xhttpd : #1
- drawdraw: #2

#: 품 순서

xhttpd

- HTTP Daemon 컨셉의 문제
- 스레드 간 Stack overflow 문제 (BOF 아님)

xhttpd

- HTTP 파싱하는 곳에서 문자 처리를 재귀호출로 함 (...)
- 파싱 후 처리 함수가 지역변수 크기가 0x1000 이상임
- **1 Thread / 1 Request (pthread)**

xhttpd

■ 스레드 생성

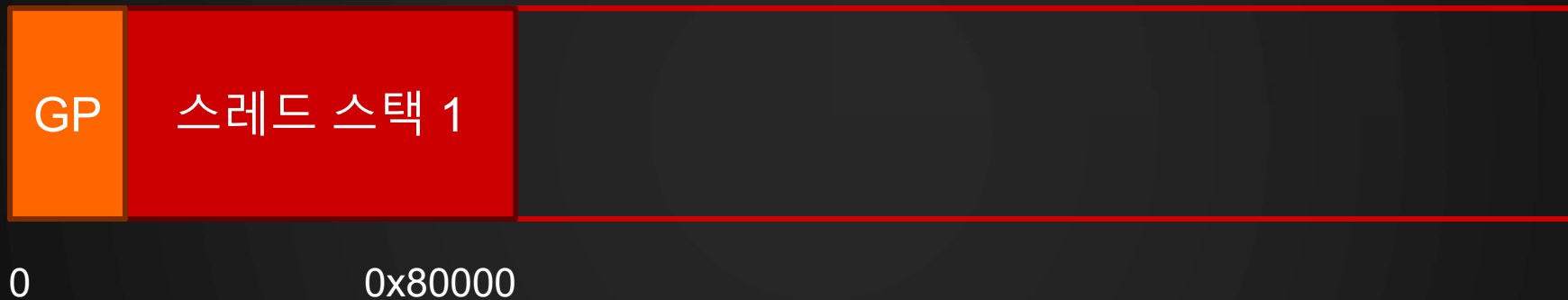
```
if ( pthread_create(&newthread, 0LL, start_routine, (void *)v6) )  
    perror("pthread create");
```

■ 루프

```
void __fastcall on_read(int fd, char *buf, signed int offset)  
{  
    char c; // [sp+Fh] [bp-19h]@1  
  
    c = 0;  
    if ( offset <= 1999 )  
    {  
        recv(fd, &c, 1uLL, 0);  
        if ( c == 13 )  
        {  
            on_read(fd, buf, offset);  
        }  
        else if ( c == 10 )  
        {  
            buf[offset] = '\n';  
            process(fd, (__int64)buf, offset + 1);  
        }  
        else  
        {  
            buf[offset] = c;  
            on_read(fd, buf, offset + 1);  
        }  
    }  
}
```

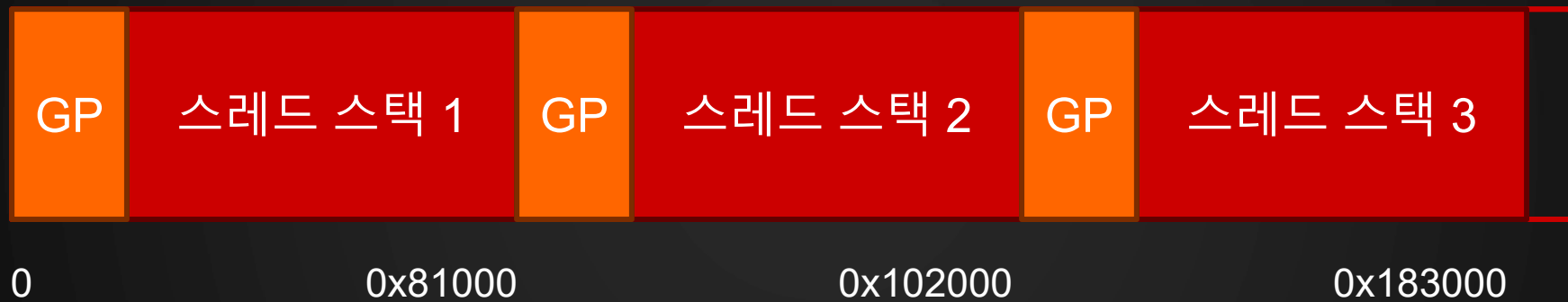
xhttpd

- 스레드 스택은 $0x1000+0x80000$ 크기로
mmap됨 (GP: Guard Page, rwx: ---)



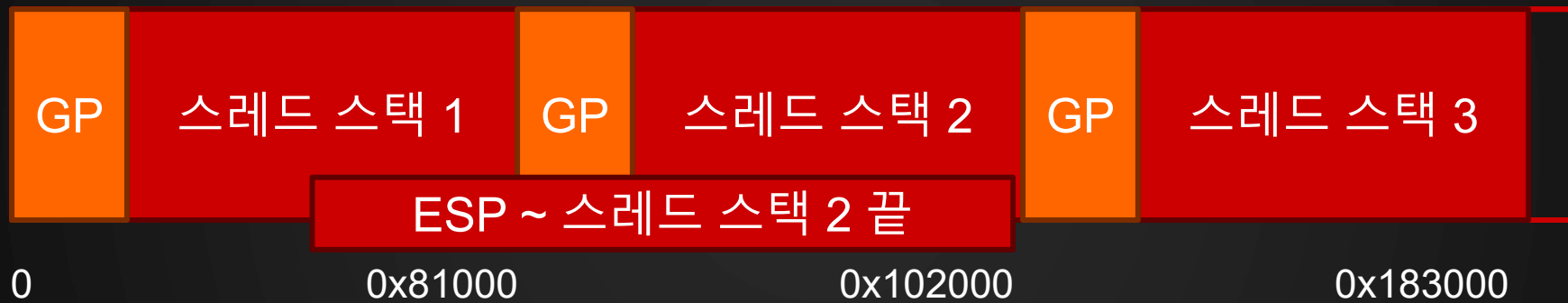
xhttpd

- 여러개 면..



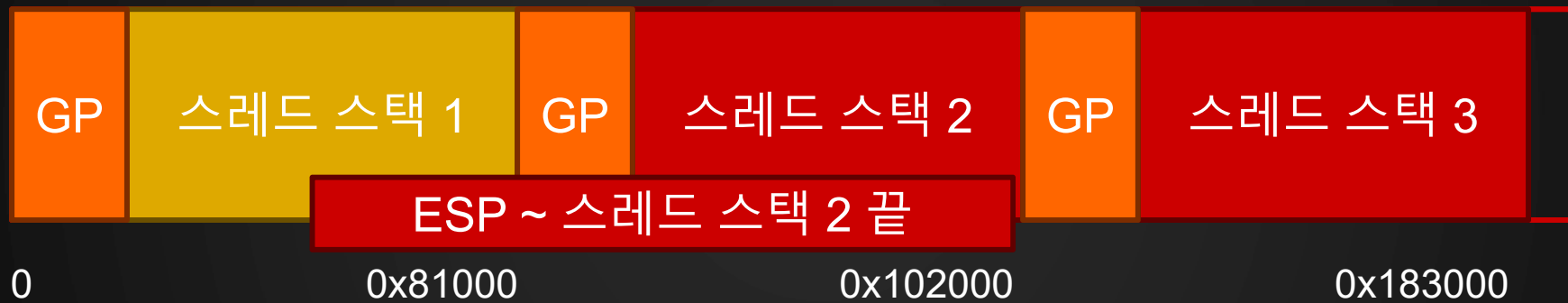
xhttpd

- Q. 만약 이렇게 되면?



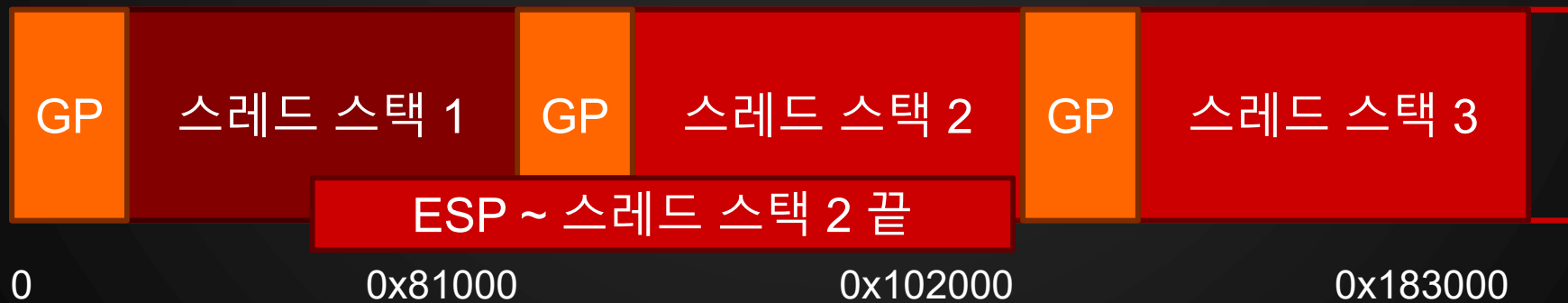
xhttpd

- A. 스레드1 스택 조작가능



xhttpd

1. 스레드 스택 1에서 sleep을 시킴
2. 스레드 2로 스레드 1의 리턴주소 덮음
3. ROP

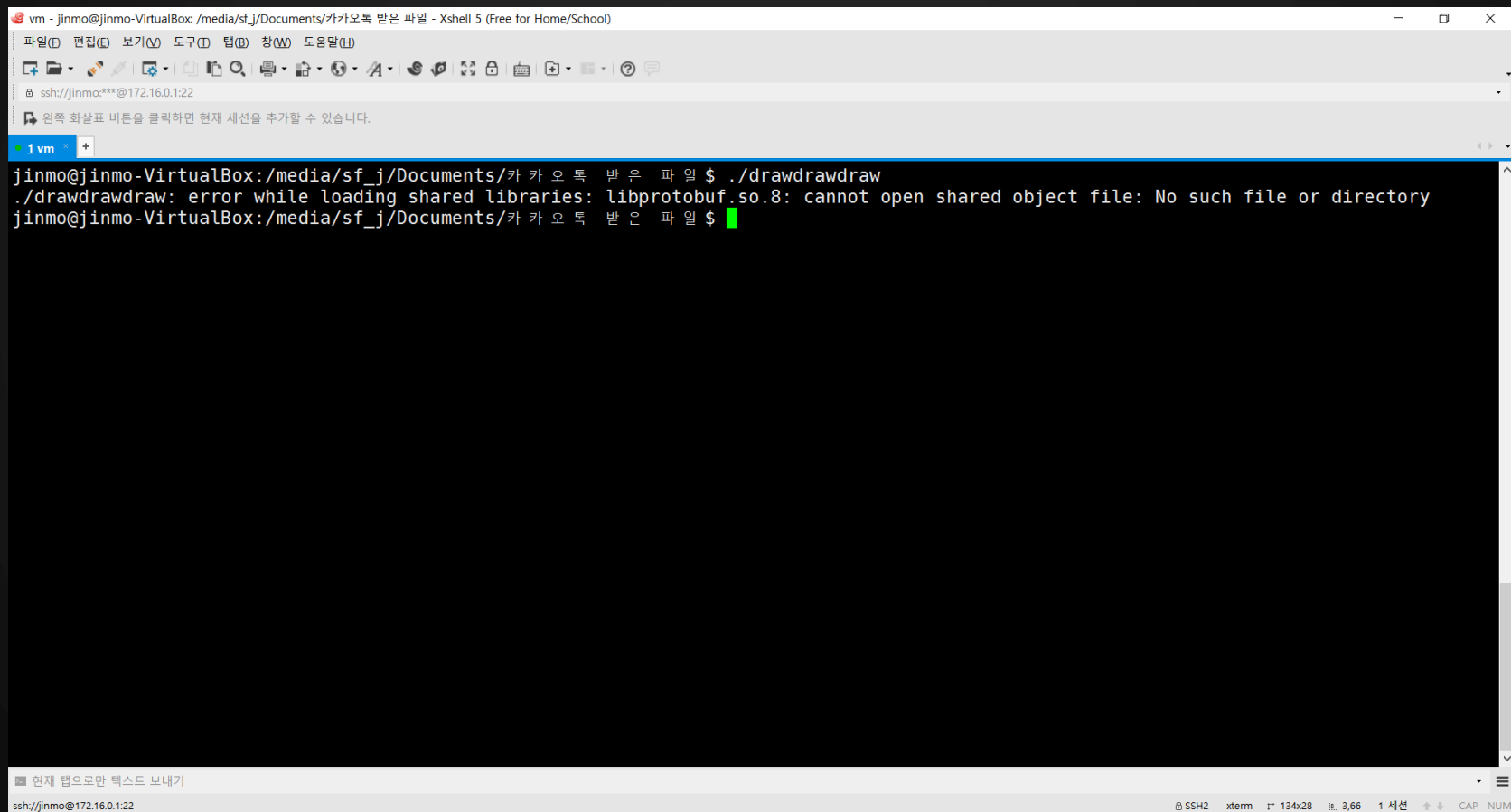


drawdraw

- 바이너리가 strip됨, DH / RSA 암호화
- protobuf reversing w/o .proto file
- protoc는 기본적으로 타입 자체에 대한 protobuf 구조체 정보를 raw data로 파일에 담음
- 그 후로는 OOB read/write

drawdraw

(부들)

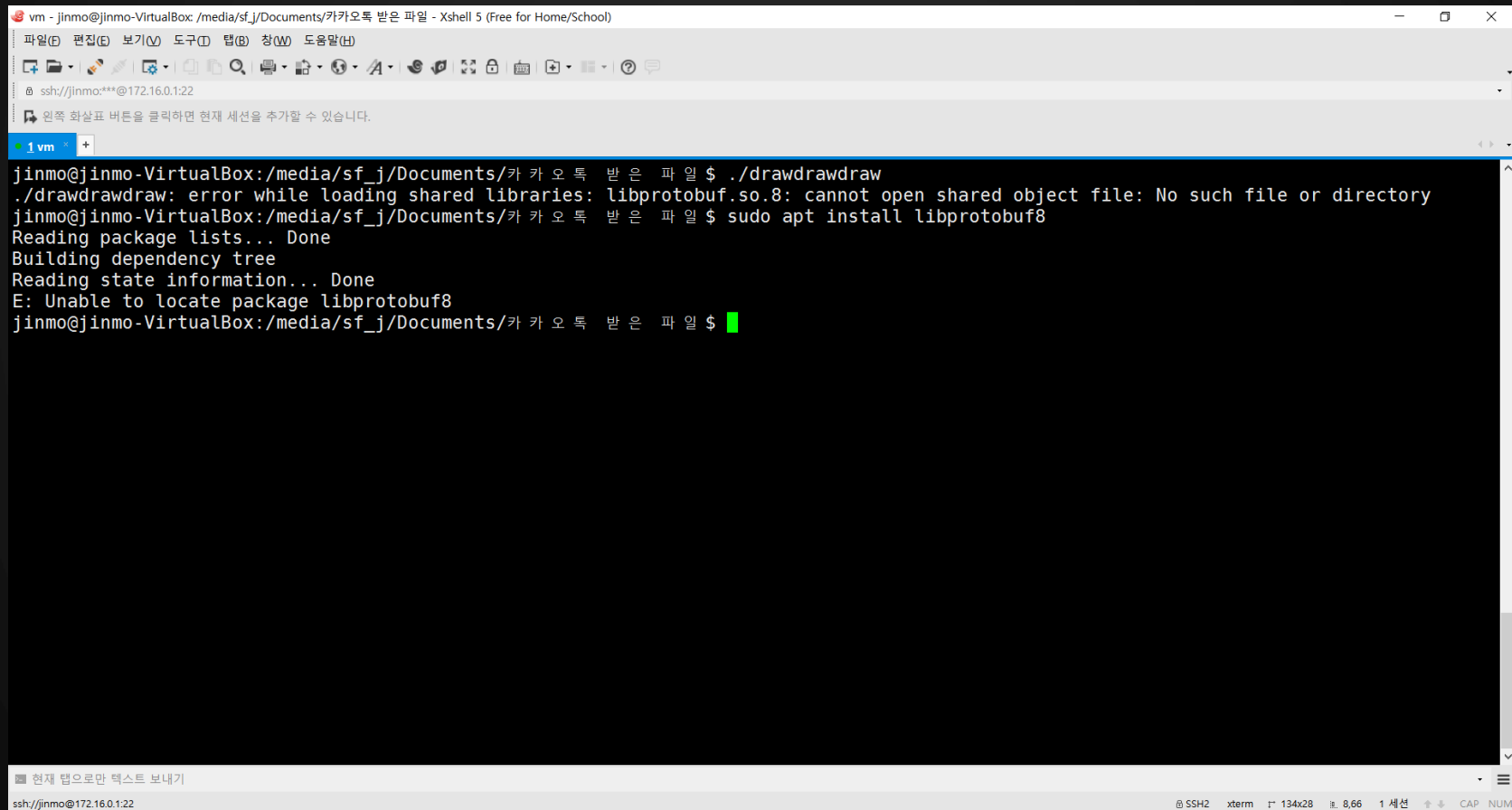


The screenshot shows an Xshell 5 terminal window. The title bar reads "vm - jinmo@jinmo-VirtualBox: /media/sf_j/Documents/카카오톡 받은 파일 - Xshell 5 (Free for Home/School)". The terminal content shows a user running the command `./drawdrawdraw` in the directory `/media/sf_j/Documents/카카오톡 받은 파일`. The command fails with the error: `./drawdrawdraw: error while loading shared libraries: libprotobuf.so.8: cannot open shared object file: No such file or directory`. The terminal status bar at the bottom indicates the session is an SSH2 connection to `ssh://jinmo@172.16.0.122` using xterm, with a resolution of 134x28 and a zoom level of 3.66.

```
vm - jinmo@jinmo-VirtualBox: /media/sf_j/Documents/카카오톡 받은 파일 - Xshell 5 (Free for Home/School)
파일(F) 편집(E) 보기(V) 도구(D) 탭(T) 창(W) 도움말(H)
ssh://jinmo:**@172.16.0.122
왼쪽 화살표 버튼을 클릭하면 현재 세션을 추가할 수 있습니다.
1 vm
jinmo@jinmo-VirtualBox:/media/sf_j/Documents/카카오톡 받은 파일$ ./drawdrawdraw
./drawdrawdraw: error while loading shared libraries: libprotobuf.so.8: cannot open shared object file: No such file or directory
jinmo@jinmo-VirtualBox:/media/sf_j/Documents/카카오톡 받은 파일$
```

drawdraw

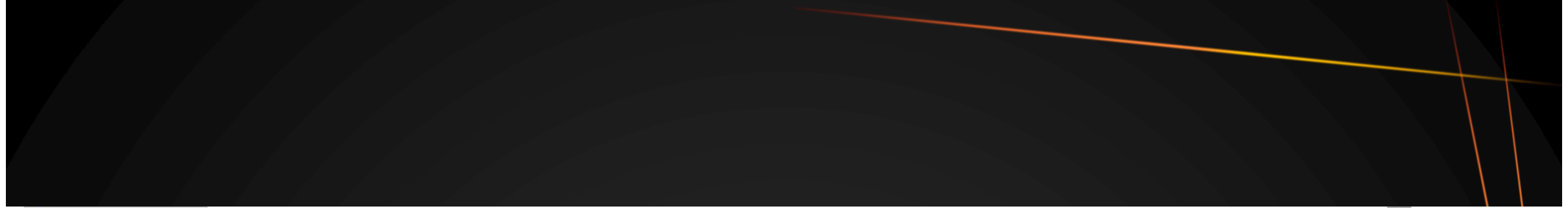
(부들!)



```
vm - jinmo@jinmo-VirtualBox: /media/sf_j/Documents/카카오톡 받은 파일 - Xshell 5 (Free for Home/School)
파일(F) 편집(E) 보기(V) 도구(D) 탭(B) 창(W) 도움말(H)
ssh://jinmo:**@172.16.0.122
왼쪽 화살표 버튼을 클릭하면 현재 세션을 추가할 수 있습니다.
1 vm
jinmo@jinmo-VirtualBox:/media/sf_j/Documents/카카오톡 받은 파일$ ./drawdrawdraw
./drawdrawdraw: error while loading shared libraries: libprotobuf.so.8: cannot open shared object file: No such file or directory
jinmo@jinmo-VirtualBox:/media/sf_j/Documents/카카오톡 받은 파일$ sudo apt install libprotobuf8
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package libprotobuf8
jinmo@jinmo-VirtualBox:/media/sf_j/Documents/카카오톡 받은 파일$
```

현재 탭으로만 텍스트 보내기

ssh://jinmo@172.16.0.122 @ SSH2 xterm 134x28 8.66 1 세션 CAP NUM



百度一下, 你就知道

www.baidu.com/s?ie=utf-8&f=8&rsrv_bp=0&rsrv_idx=1&tn=baidu&wd=libprotobuf.so.8&rsrv_pq=cf6c03c20000997f&rsrv_t=03f9X4WVJG4Bo7gssSoFdwXFV54wf25BiyIv9LKSjirHqqquNaloN42KnhM&rqlq

Baidu 百度

libprotobuf.so.8

百度一下

百度首页 设置 登录

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约62,000个

搜索工具

[proto buffer 安装 及 调用 - dofound的日志 - 网易博客](#)
2013年6月24日 - proto buffer 安装 及 调用,dofound的网易博客,日进 月斗,http://... protoc:
error while loading shared libraries: libprotobuf.so.8: cannot open...
[dofound.blog.163.com/b...](#) - 百度快照 - 700条评价

[Linux 下使用protobuf 几点细节 - 七夜狐的专栏 - 博客频道 - ...](#)
2010年12月22日 - 安装之后,运行protoc,提示找不到两个库:libprotobuf.so,libprotoc.so. 原因是
因为这两个库安装在/usr /local/lib下,但是ubunut的lib路径为/usr/lib...
[blog.csdn.net/sky_cn19...](#) - 百度快照 - 1533条评价

[proto buffer 安装 及 调用 五月jks_gyS_新浪博客](#)
2013年8月12日 - [root@F2C-1 protobuf-2.5.0]# protoc --version protoc: error while loading
shared libraries: libprotobuf.so.8: cannot open shared object file...
[blog.sina.com.cn/s/blo...](#) - 百度快照 - 3895条评价

[ubuntu下编译protobuf - xocoder's coding life - 博客频道 - ...](#)
2013年6月23日 - protoc: error while loading shared libraries: libprotoc.so.8: cannot open
shared 错误原因: protobuf的默认安装路径是/usr/local/lib,而/usr/loc...
[blog.csdn.net/xocoder/...](#) - 百度快照 - 1533条评价

[Centos6.4下安装protobuf-c问题及解决办法 - Anker's Blog - 博客园](#)
2013年10月4日 - protobuf是Google提供的结构持久化工具,类型XML,但要比XML更加灵活,效
率要高。protobuf当初支持C++、JAVA和Python,后来有了支持C语言的Protobuf-c。失...
[www.cnblogs.com/Anker/...](#) - 百度快照 - 835条评价

[LINUX下编译安装PROTOBUF - shanshu12的专栏 - 博客频道 - CSDN.NET](#)
2011年12月23日 - protoc: error while loading shared libraries: libprotobuf.so.0: cannot
open...Java EE SSH(8) Java 开发(5) linux(26) 信息检索(2) 数据库(6...
[blog.csdn.net/shanshu1...](#) - 百度快照 - 1533条评价

[linux下安装protobuf教程+示例\(详细\) - colorful - C++博客](#)

其他人还搜

展开



163
网易公司网
聚人的力量



网易
中国领先的
互联网公司



ctags
方便代码阅
读的工具



node.js
JavaScript工
具包

相关软件



memcached
分布式对象
缓存系统



wxwidgets
C构架库fra
mework



centos
综合社区企
业操作系统



apache
Web服务器

计算机术语



动态链接库
共享数据和
资源



g++
执行编译工
作



动态链接
使模块形成
独立的文件

给百度提建议

45/52

- 자세한 것은 직접 보면 압니다.

drawdraw

- 그림판 컨셉의 문제
- 기능: 점 찍기 / 패턴 그리기 / 저장 / 비우기
- 패턴 저장 / 그리기에서 패턴 번호 지정 가능
- 패턴 버퍼는 스택에 있었고 번호에서 OOB

인상깊었던 점

- 첫날 나온 문제 첫 날 밤에 다 풀었습니다.
 - web1 - CodeIgniter with MANY 1days
 - web2 - Command Injection (Obfuscated code, backdoor)
 - drawdraw - OOB r/w on stack (protobuf reversing)
 - xhttpd - Stack overflow on multithreaded program
 - richman - Uninitialized variable on stack

XCTF 후기

- 전형적인 공격-방어 대회구나
 - DEF CON 23 CTF 본선, HITCON CTF 2015 본선 등
- 대회 타이틀이 아주 거창했는데..
 - 문제들이 술술 풀려서 아주 약간 당황함
 - 1박 2일이므로 적절함

XCTF 후기

- 1등해서 기분 좋았음
- LCBC팀은 유쾌하구나!

积分榜 / Scoreboard			
总分		得分	失分
1	 CyKor	22508.14	
2	 LCBC	12435.64	
3	 Oops	9670.83	
4	 217	7519.97	
5	 forx	7380.61	
6	 FlappyPig	6008.18	
7	 *****	5838.15	
8	 Nu1L	5393.39	
9	 WildWolf	5192.00	
10	 NeSE	3980.58	
11	 Shellphish	3839.27	
12	 ROIS	3240.73	
13	 Dcua	3214.70	

후기

- 이제 점점 CTF 팀들이 익숙해집니다.
- 보기만 해도 기분이 좋아지더군요.
- 대회덕분에 해외여행다니는 기분입니다.

Q&A