

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

宋方睿 MaskRay

<https://maskray.me>

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

- 1 Capture the Flag**
- 2 Cyber Grand Challenge**
- 3 CB, Poller, POV, IDS**
- 4 Shellphish 的 CRS**
- 5 DEFCON 24 CTF Finals**
- 6 DEFCON 24 CTF CB**
- 7 References**

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

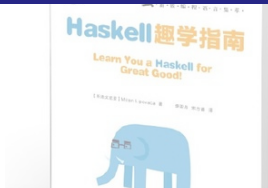
参赛队伍

DEFCON 24
CTF CB

References

MaskRay

■ 过期的算法竞赛 + 超算赛棍



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

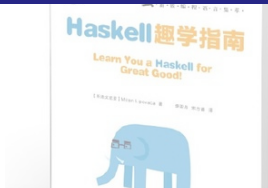
参赛队伍

DEFCON 24
CTF CB

References

MaskRay

- 过期的算法竞赛 + 超算赛棍
- 发霉的运维 + FP 爱好者



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

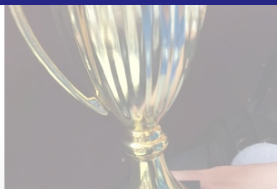
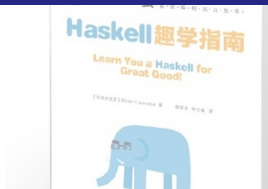
参赛队伍

DEFCON 24
CTF CB

References

MaskRay

- 过期的算法竞赛 + 超算赛棍
- 发霉的运维 + FP 爱好者
- 变质的四届 DEFCON CTF 酱油



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

两个竞赛

- Cyber Grand Challenge (CGC) Final Event, 8 月 4 日
- DEFCON 24 Capture the Flag, 8 月 5~7 日

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Capture the Flag

- 逆向技术, 协议分析, 网络嗅探, 密码破解, 计算机取证, 编程
- Codegate CTF, DEFCON CTF, Hack.lu CTF, Plaid CTF, SECCON CTF
- 0CTF, BCTF, XCTF

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

形式

■ jeopardy, Online Judge

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

形式

- jeopardy, Online Judge
- attack-defense

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

形式

- jeopardy, Online Judge
- attack-defense
- Cyber Grand Challenge

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

宋方睿
MaskRay

Capture the Flag

Cyber Grand Challenge

入围队伍

CB, Poller,
POV, IDS

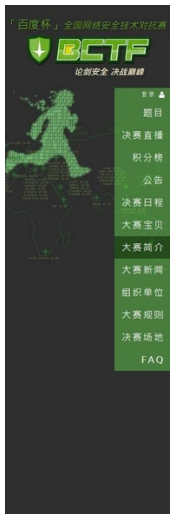
Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



大赛简介

分享到

BCTF“百度杯”全国网络安全技术对抗赛，是由百度公司主办，清华和北大的安全技术专家提供技术支持，紫金江宁，南京赛宇承办，面向全国范围网络安全技术实战竞赛！



大赛三大特色

最具文化的赛事：百度和清华、北大的安全技术人员邀请战队一起重温米特尼克冒险传奇，体验最具神秘色彩的黑客文化和技术！

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Cyber Grand Challenge

- Cyber Reasoning System
- 寻找漏洞
- 修补漏洞
- 分析攻击
- 设置防火墙
- 利用漏洞 (exploit)
- 1280 cores, 16TB ram, 128 TB storage

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

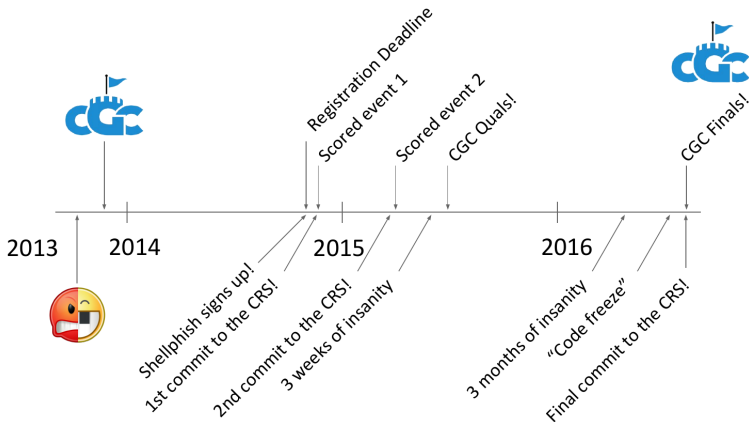
Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

CGC Qualifying Event

- 24 小时分析 126 个 challenge binary (CB)
- 产生让 CB 崩溃的交互
- 修补 CB, 保留功能, 性能也影响分数

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

DECREE 环境

- 修改的 Linux 3.13.0, 32 位 x86
- ELF -> CGC(可执行文件格式)
- allocate(mmap), deallocate(munmap), fdwait(select), random, receive(read), terminate(exit), transmit(write)
- SIGPIPE Ign, SIGSEGV SIGILL SIGBUS Core, 其他 Term
- 禁用 address space layout randomization, 禁用 non-executable stack
- CR4 寄存器禁用 performance monitoring center
- static linking, homebrew libc

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

CodeJitsu

- University of California, Berkeley
- BitBlaze Binary Analysis Platform: Vine(static analysis), TEMU(dynamic analysis), Rudder(symbolic execution)

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

└ Cyber Grand Challenge

└ 入围队伍

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

ForAllSecure

- CMU 教授 David Brumley 發起的 startup, 成员多来自 CyLab
- Binary Analysis Platform
- Plaid Parliament of Pwning 是其 undergraduate computer security research group。

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

└ Cyber Grand Challenge

└ 入围队伍

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

TECHx

- GrammaTech & University of Virginia Technology
- Preventing Exploits of Software of Unknown Provenance

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

CSDS

- University of Idaho
- Jim Alves-Foss, Jia Song

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

└ Cyber Grand Challenge

└ 入围队伍

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

DeepRed

■ Raytheon

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

└ Cyber Grand Challenge

└ 入围队伍

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

disekt

- University Of Georgia
- 2009 年成立 disekt CTF 战队

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Shellphish

- University of California, Santa Barbara
- angr, a python framework for analyzing binaries. It focuses on both static and dynamic symbolic ("concolic") analysis

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

└ Cyber Grand Challenge

└ 入围队伍

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

└ Cyber Grand Challenge

└ 入围队伍

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



CGC Final Event

- 96 轮
- 比赛开始时 CRS 接收 CB，每个 CB 以类似 `socat tcp-l:9999 exec:cb` 的形式提供服务
- 每轮为每个 (*round, team, service*) 产生分数，(***, *team*, ***) 和为该队伍累计分数

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

└ Cyber Grand Challenge

└ 入围队伍

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

(*round, team, service*)

- $score = 100 \times availability \times security \times evaluation$
- $availability \in [0, 1]$, 通过 poller 的比例和内存时间开销
- $security \in \{1, 2\}$, 被其他 CRS 攻击成功?
- $evaluation \in [1, 2]$, 攻击其他 CRS

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

	attack-defense	CGC
题目数量	~6	82 challenge sets(CFE)/ 8(DEFCON CTF)
流量	主办方提供 tcpdump	自行在 1999/udp 接收 (服务编号, 连接号, 流 序号, 消息长度等)
平台	amd64, aarch64, mipsel, ...	DECREE
服务	可 ssh, 替换服务文件	API 提交修补过的
可用性检测	主办方伪装成其他队伍 检测	平台测试提交的 CB
攻击方式	手工, 程序	提交 proof-of- vulnerability
flag	主办方每轮生成, 服务 程序有权限读取的文件	magic page 填充随机值
防火墙	executable wrapper	类 snort 规则

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Challenge binary

- 题目用的可执行文件，特意设置了若干漏洞
- 分析、修补、利用
- API 上传修补后的 CB
- static linking, 手写 libc, 鼓励每道题用不同 libc

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

Poller generator

- 检测 CB 可用性
- finite state automaton
- 每条边指定转移概率
- 每个顶点指定停止概率
- Python 脚本指定各个顶点执行的操作，产生输入或输出等

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

```
nodes:
- name: start
- name: top
- name: endIt
- name: printAirports
- name: addAirport
- name: deleteAirport
- name: findRoutes
```

```
edges:
- start: top
- top: printAirports
- printAirports: top
- top: addAirport
- addAirport: top
- top: deleteAirport
- deleteAirport: top
- top: findRoutes
- findRoutes: top
- top: endIt
  weight: .20
```

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

Proof of vulnerability

- C 编写的 CGC 可执行文件
- 构建方式和 CB 相同
- Type 1 & Type 2

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

Type 1 vulnerability

- 控制 EIP 与 8 个 general purpose register 中任意一个

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

Type 1 vulnerability

- 控制 EIP 与 8 个 general purpose register 中任意一个
- 如果证明能控制?

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Type 1 vulnerability

- 控制 EIP 与 8 个 general purpose register 中任意一个
- 如果证明能控制？
- Challenge response, POV 程序向平台宣称能控制寄存器的特定 20 bits，平台指定 20 bits 的值

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Type 1 vulnerability

- 控制 EIP 与 8 个 general purpose register 中任意一个
- 如果证明能控制?
- Challenge response, POV 程序向平台宣称能控制寄存器的特定 20 bits, 平台指定 20 bits 的值
- 程序崩溃时两个寄存器的值与 challenge 匹配

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Type 2 vulnerability

- magic page
- CGC 可执行文件执行时, 0x4347c000 处内核分配一页, 填充随机值
- Challenge response, 平台指定要输出 magic page 指定区间内的 4 字节
- POV 程序设法获取

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

Intrusion detection system (IDS)

- 防火墙规则
- 可以阻挡攻击，也可能误伤 poller generator
- domain-specific language

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Proof of vulnerability (POV)

- C 编写的 CGC 可执行文件
- 构建方式和 CB 相同
- Type 1 & Type 2

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

Oracle

- Input: CB, POV, IDS
- Output: score, packet captures, others' CB & IDS
- 可以下载其他队伍的 CB 和 IDS

实现

- <https://github.com/mechaphish>
- angr: binary loader + static analysis (control-flow graph, data-flow analysis, value-set analysis) + symbolic execution
- Driller: fuzzing with selective symbolic execution (American fuzzy lop + angr)
- patcherex: extended malloc, protect indirect call/jmp, return pointer encryption, randomly shift the stack, stack canary, backdoor, ...
- database ORM model, qemu, scheduler, POV simulator, API interaction, ...

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

统计

- 82 Challenge Sets
- 2442 exploits generated
- longest exploit: 3791 lines of C code
- shortest exploit: 226 lines of C code

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

DEFCON 24 CTF Finals

- CTF 届世界杯
- Las Vegas, 8 月 5~7 日

Rise of the Machines: Cyber Grand Challenge 及 DEFCON 24 CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Round 152 | DEF CON CTF 2016

b1o0p

started round 153

Dashboard Scoreboard

Help

Round 152

all rounds

Started at 16 minutes ago

Finished at 7 minutes ago

Replacements

cbid team digest size actions

LEGIT 00000 defcon (2) ua6d584b 442452 download details

Poll Feedbacks

statuses performance

csat success timeout functionality connect bad time memory

5 294 0 0 0 0 0.988 1.239

2 374 0 0 0 0 0.864 1.008

1 301 0 0 0 0 0.856 1.133

4 329 0 0 0 0 17.476 1.0

0 106 0 0 0 0 1.086 1.0

CB Feedbacks

csat cb signal timestamp

LEGIT 00004 LEGIT 00004 11 1470572205

LEGIT 00004 LEGIT 00004 11 1470572222

LEGIT 00004 LEGIT 00004 11 1470572265

LEGIT 00004 LEGIT 00004 11 1470572222

LEGIT 00004 LEGIT 00004 11 1470572191

LEGIT 00004 LEGIT 00004 11 1470572189

LEGIT 00004 LEGIT 00004 11 1470572186

LEGIT 00004 LEGIT 00004 11 1470572207

LEGIT 00004 LEGIT 00004 11 1470572208

LEGIT 00004 LEGIT 00004 11 1470572196

LEGIT 00004 LEGIT 00004 11 1470572196

LEGIT 00004 LEGIT 00004 11 1470572196

LEGIT 00004 LEGIT 00004 11 1470572196

LEGIT 00004 LEGIT 00004 11 1470572169

LEGIT 00004 LEGIT 00004 11 1470572159

LEGIT 00004 LEGIT 00004 11 1470572159

LEGIT 00004 LEGIT 00004 11 1470572159

LEGIT 00004 LEGIT 00004 11 1470572154

LEGIT 00004 LEGIT 00004 11 1470572154

LEGIT 00004 LEGIT 00004 11 1470572153

LEGIT 00004 LEGIT 00004 11 1470572145

LEGIT 00004 LEGIT 00004 11 1470572145

LEGIT 00004 LEGIT 00004 11 1470572114

LEGIT 00004 LEGIT 00004 11 1470572135

LEGIT 00004 LEGIT 00004 11 1470572135

LEGIT 00004 LEGIT 00004 11 1470572101

LEGIT 00004 LEGIT 00004 11 1470572115

LEGIT 00004 LEGIT 00004 11 1470572117

LEGIT 00004 LEGIT 00004 11 1470572157

LEGIT 00004 LEGIT 00004 11 1470572173

LEGIT 00004 LEGIT 00004 11 1470572169

LEGIT 00004 LEGIT 00004 11 1470572169

LEGIT 00004 LEGIT 00004 11 1470572065

LEGIT 00004 LEGIT 00004 11 1470572065

LEGIT 00004 LEGIT 00004 11 1470572087

LEGIT 00004 LEGIT 00004 11 1470572081

LEGIT 00004 LEGIT 00004 11 1470572102

LEGIT 00004 LEGIT 00004 11 1470572070

PoV Feedbacks

csat target

LEGIT 00000 samurai (9)

LEGIT 00000 defcon (2)

LEGIT 00000 ppp (8)

LEGIT 00000 blinja (12)

LEGIT 00000 ppp (8)

LEGIT 00000 dragonsector (14)

LEGIT 00000 dragonsector (14)

LEGIT 00000 dragonsector (14)

LEGIT 00000 hitcon (6)

LEGIT 00000 ppp (8)

LEGIT 00000 shellphish (13)

LEGIT 00000 shellphish (13)

LEGIT 00000 ppp (8)

LEGIT 00000 samurai (9)

LEGIT 00000 team047 (18)

LEGIT 00000 lche (7)

LEGIT 00000 ppp (8)

LEGIT 00000 dragonsector (14)

LEGIT 00000 shellphish (13)

LEGIT 00000 shellphish (13)

LEGIT 00000 blinja (12)

LEGIT 00000 pasten (8)

LEGIT 00000 defcon (2)

LEGIT 00000 dragonsector (14)

LEGIT 00000 dragonsector (14)

LEGIT 00000 hitcon (6)

LEGIT 00000 shellphish (13)

LEGIT 00000 team047 (18)

LEGIT 00000 kalchackon (11)

LEGIT 00000 lche (7)

LEGIT 00000 dragonsector (14)

LEGIT 00000 hitcon (6)

LEGIT 00000 extelsooppetrepeat (3)

PoV throw success

5147725027 1 false

514772506 1 false

514772517 1 false

514772517 1 false

514772518 1 false

514772518 1 false

514772518 2 false

514772518 0 false

514772518 1 false

514772518 2 false

514772518 0 false

514772518 2 false

514772518 1 true

514772518 1 false

514772518 1 false

514772518 2 true

514772518 2 false

514772518 4 false

514772518 1 false

514772518 0 false

514772518 5 false

514772518 4 false

514772518 0 false

514772518 0 false

514772518 5 false

514772518 1 false

514772518 1 false

514772518 2 false

514772518 1 false

514772518 1 false

514772518 2 false

514772518 1 false

514772518 2 false

514772517 1 false

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

b1o0p

- $\text{blue-lotus} + \text{0ops} = \text{b1o0p}$
- blue-lotus 成立于清华大学网络与信息安全实验室，是中国首支入围 DEFCON CTF 全球决赛的战队
- 上海交通大学 0ops 成立于 2013 年，成员主要来自于计算机系密码学与计算机安全实验室、信息安全工程学院等，大陆首支国际 CTF 赛事冠军战队，2015 年 ctftime 排名第 3。

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

结果

■ PPP 第一, b1o0p 第二, DEFKOR 第三

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

结果

- PPP 第一, b1o0p 第二, DEFKOR 第三
- 奖品 = null

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

结果

- PPP 第一, b1o0p 第二, DEFKOR 第三
- 奖品 = null
- 不是我军无能, 而是敌人太狡猾

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

我军

- neoni, BinDiff, 找出修补 CB 与原 CB 差异
- azure.kdays.cn, F.L.I.R.T signatures、executable loader
- hen, 反汇编工具
- 小花椒, 可执行文件修补工具、流量分析重放
- ...
- libmaru, 网络环境、主办方平台监控发送到 slack
- yu4fn、firesun、BrieflyX 等, team interface 网站
- MaskRay, PCAP 搜索、packet captures、POV 检测

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Mayhem

■ ForAllSecure 的 Cyber Reasoning System

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Mayhem

- ForAllSecure 的 Cyber Reasoning System
- DEFCON CTF 与 CGC 平台不一致，比赛前两天收到的流量有问题

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Mayhem

- ForAllSecure 的 Cyber Reasoning System
- DEFCON CTF 与 CGC 平台不一致，比赛前两天收到的流量有问题
- 没能公平的较量实属遗憾

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

Mayhem

- ForAllSecure 的 Cyber Reasoning System
- DEFCON CTF 与 CGC 平台不一致，比赛前两天收到的流量有问题
- 没能公平的较量实属遗憾
- 8 题做出 7 题应该不实，一题往往藏有数个漏洞。所有可执行文件都经过 binary recompiler，MaskRay 喵逆向不来

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

PPP

- DEFCON 21,22,24 CTF 第一, 2011、2013、2015 ctftime 第一

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

PPP

- DEFCON 21,22,24 CTF 第一, 2011、2013、2015 ctftime 第一
- geohot 和 Ricky Zhou 为代表的 Pwn 机

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

PPP

- DEFCON 21,22,24 CTF 第一, 2011、2013、2015 ctftime 第一
- geohot 和 Ricky Zhou 为代表的 Pwn 机
- 参与 Mayhem 开发的 ForAllSecure 成员

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

PPP

- DEFCON 21,22,24 CTF 第一, 2011、2013、2015 ctftime 第一
- geohot 和 Ricky Zhou 为代表的 Pwn 机
- 参与 Mayhem 开发的 ForAllSecure 成员
- binary recompiler, Shellphish、binja 等也有

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References



Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

DEFKOR

■ 韩国梦之队, Best of Best 计划学生

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

DEFKOR

- 韩国梦之队, Best of Best 计划学生
- Jung Hoon Lee(lokihardt), Pwn2Own 2015 攻破 IE 11 Chrome Safari

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

DEFKOR

- 韩国梦之队, Best of Best 计划学生
- Jung Hoon Lee(lokihardt), Pwn2Own 2015 攻破 IE 11 Chrome Safari
- DEFCON 23 CTF 第一

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

LC BC

- 俄罗斯, Yellowstone Yachtsclub of Yawning

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

LC BC

- 俄罗斯, Yellowstone Yachtsclub of Yawning
- OpenCTF 2016, 0CTF 2016 第一

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals
参赛队伍

DEFCON 24
CTF CB

References

HITCON

■ 大量 ICPC 选手: peter50216, Shik, seanwu, david942j

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

HITCON

- 大量 ICPC 选手: peter50216, Shik, seanwu, david942j
- Orange Tsai, 找出过 Facebook, Uber, Yahoo 多家大厂漏洞

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 决赛介绍

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge

入围队伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

参赛队伍

DEFCON 24
CTF CB

References

实战

Rise of the
Machines:
Cyber Grand
Challenge 及
DEFCON 24
CTF 決賽介紹

宋方睿
MaskRay

Capture the
Flag

Cyber Grand
Challenge
入圍隊伍

CB, Poller,
POV, IDS

Shellphish 的
CRS

DEFCON 24
CTF Finals

參賽隊伍

DEFCON 24
CTF CB

References

References

- Cyber Grand Challenge 簡介
- 從 HITCON 駭客戰隊挑戰美國 CGC 天網機器人探討自動攻防技術發展
- Cyber Grand Shellphish
- A Dozen Years of Shellphish From DEFCON to the Cyber Grand Challenge
- 机器的黎明-第 24 届 DEF CON CTF 总决赛亚军队员访谈