CTF

转载

渣渣是我 于 2018-05-26 20:44:33 发布 1430 收藏

Defcon CTF：

侧重于计算机底层与系统安全核心能力

- 竞赛环境趋向多CPU指令架构集，多操作系统，多编程语言
- 逆向分析，漏洞挖掘，漏洞利用，漏洞修补加固，网络流量分析，系统安全运维，面向安全的编程调试

服务名称	指令架构	操作系统	编程语言	防御机制	大小
rxc	x86-64	Linux	C++	ASLR/Stack Canary/ NX	192KB
ombdsu	MIPS	Linux	C	ASLR/NX/PIE	19KB
tachikoma	x86-32	Linux	C	ASLR/PIE	188KB
hearye	ARM-64	Android	C		
hackermud	x86-32	Linux	C++	ASLR/NX	184KB
badlogger	ARMv7	Win10	C	ASLR/Stack Canary/ NX	15K
irkd	MIPS	Linux	C	ASLR/NX	713KB

- 多指令集架构：主流CPU指令架构集合 －x86-32/x86-64/armv7/arm-64/MIPS
- 多操作系统：覆盖主流操作系统 －Linux、Win10、Android
- 编程语言：C/C++
- 接近真实环境典型定制服务的逆向工作量：10K－1M

团队合作：

- 类似足球的“442”、“433”、“451”主流阵型
- CB（中卫）：安全加固、系统运维、漏洞修补
- LB/RB（边后卫）：网络流量/日志分析，协助防御和进攻
- CM（中前卫）：逆向分析/漏洞挖掘，组织攻防
- LM/RM（边前卫）：漏洞利用/补丁开发，组织攻防
- ST（前锋）：漏洞利用、攻击实施等
- GK（守门员）：缺失，依赖程序Patch

团队分工详解：

逆向分析 - 对真实环境中典型的定制二进制服务文件的逆向与程序理解

- 文件大小规模：10 KB 至 1MB 之间
- 文件格式：x86/x86-64/ARM/MIPS等指令集，Linux ELF或Windows PE可执行文件
- 编程语言：C/C++/编译型脚本语言等
- 通讯协议：二进制（完全定制或基于成熟协议修改）+ 文本（如命令控制台、Mud等）
- 逆向分析工作量：精通逆向的分析师，超过4-8小时的逆向分析工作量

https://blog.csdn.net/z1592570975

漏洞挖掘 –0day漏洞挖掘和分析能力

- 在逆向分析理解程序逻辑基础上的常见漏洞挖掘
- 漏洞类型：内存破坏类（栈溢出、堆溢出、格式化字符串、整数溢出、UAF）、任意地址读/写、内存信息泄露、逻辑型等等
- 掌握漏洞挖掘方法：动态Fuzzing、静态分析、二进制调试、符号执行等（针对简单服务）

https://blog.csdn.net/z1592570975

漏洞利用 – 成功利用漏洞并突破安全防御机制

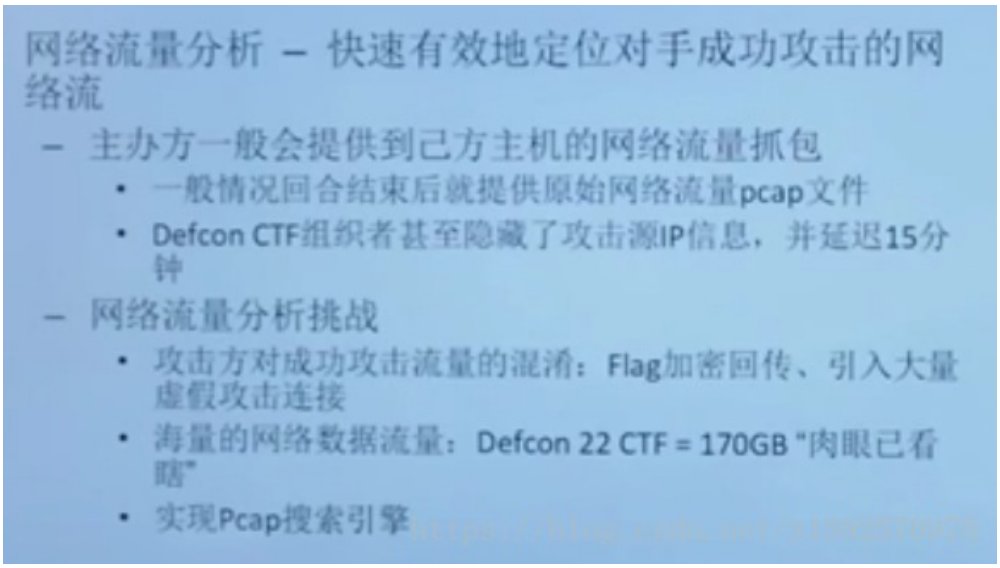
- 漏洞利用后果：控制流劫持、敏感信息泄露、可用性破坏等
- 夺取Flag：控制流劫持并执行Shellcode，获得shell或读flag到socket
- 破坏服务可用性：服务漏洞利用造成服务状态异常
- 安全防御机制：NX（DEP）、PIE、ASLR、Stack Canary...
- 漏洞利用技术：ROP、结合地址泄露漏洞等/brute forcing、SEH Exploit

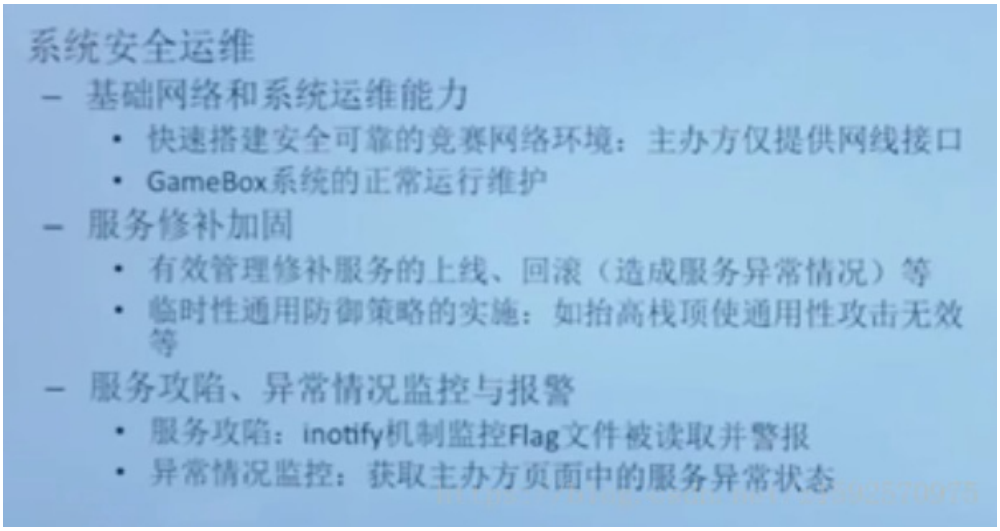
https://blog.csdn.net/z1592570975

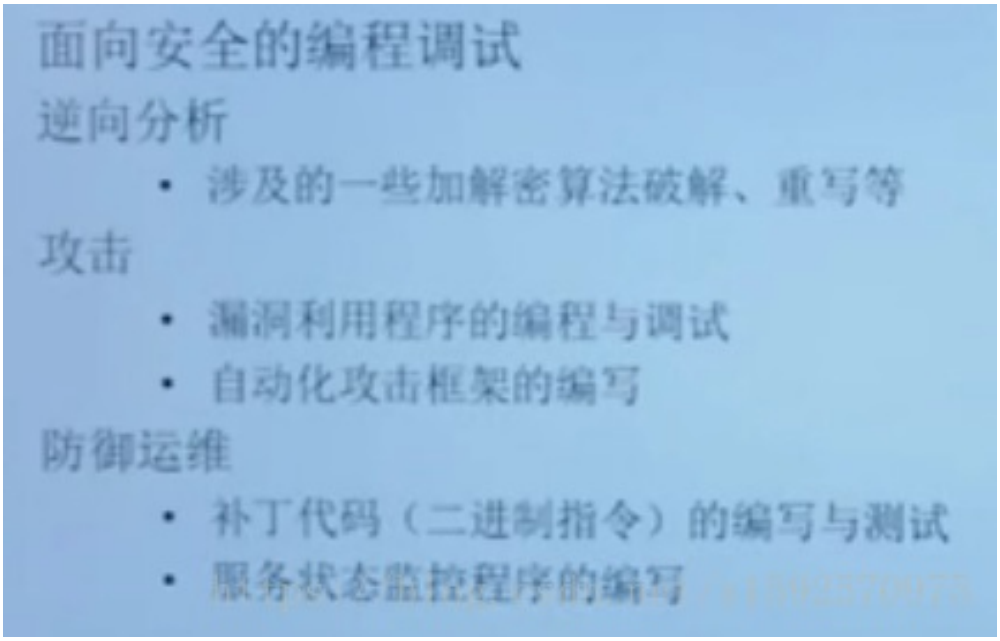
漏洞修补 – 在保障服务业务正常前提下Patch漏洞

- 二进制漏洞修补：二进制程序重写技术
  - 简单难度：修改指令，如修改常数值等，修改条件跳转等
  - 中等难度：附近存在空闲区，增加一段Patch的指令逻辑
  - 高等难度：扩大代码段，执行流首先跳转至扩展代码段增加Patch指令逻辑，再跳转回来；修复程序文件
- 难点
  - 准确理解漏洞机理，精确找出漏洞触发条件并封堵
  - 把握Checker检查业务正常与触发漏洞的临界条件（绕开“坑点”）

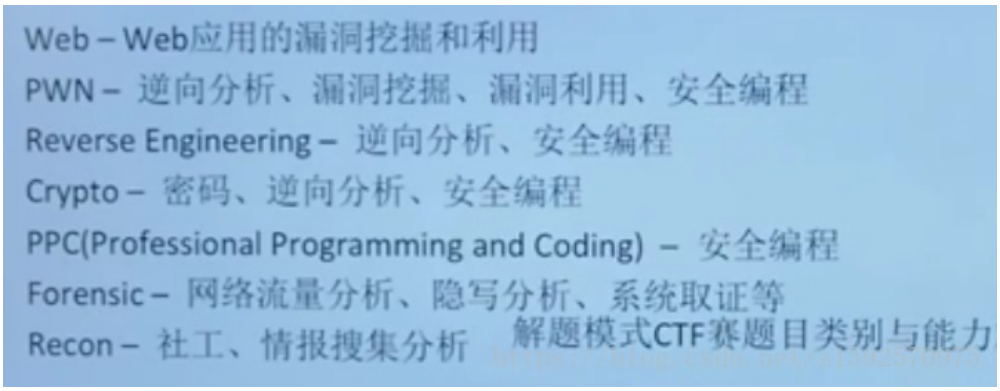
https://blog.csdn.net/z1592570975


网络流量分析 – 快速有效地定位对手成功攻击的网络流
– 主办方一般会提供到己方主机的网络流量抓包
• 一般情况回合结束后就提供原始网络流量pcap文件
• Defcon CTF组织者甚至隐藏了攻击源IP信息，并延迟15分钟
– 网络流量分析挑战
• 攻击方对成功攻击流量的混淆：Flag加密回传、引入大量虚假攻击连接
• 海量的网络数据流量：Defcon 22 CTF = 170GB "肉眼已看瞎"
• 实现Pcap搜索引擎


系统安全运维
– 基础网络和系统运维能力
• 快速搭建安全可靠的竞赛网络环境：主办方仅提供网线接口
• GameBox系统的正常运行维护
– 服务修补加固
• 有效管理修补服务的上线、回滚（造成服务异常情况）等
• 临时性通用防御策略的实施：如抬高栈顶使通用性攻击无效等
– 服务攻陷、异常情况监控与报警
• 服务攻陷：inotify机制监控Flag文件被读取并警报
• 异常情况监控：获取主办方页面中的服务异常状态


面向安全的编程调试
逆向分析
• 涉及的一些加解密算法破解、重写等
攻击
• 漏洞利用程序的编程与调试
• 自动化攻击框架的编写
防御运维
• 补丁代码（二进制指令）的编写与测试
• 服务状态监控程序的编写

题目类型：



未来：

人工智能，机器人对手

CGC：机器人CTF赛

不忘初心，方得始终

CTFTIME