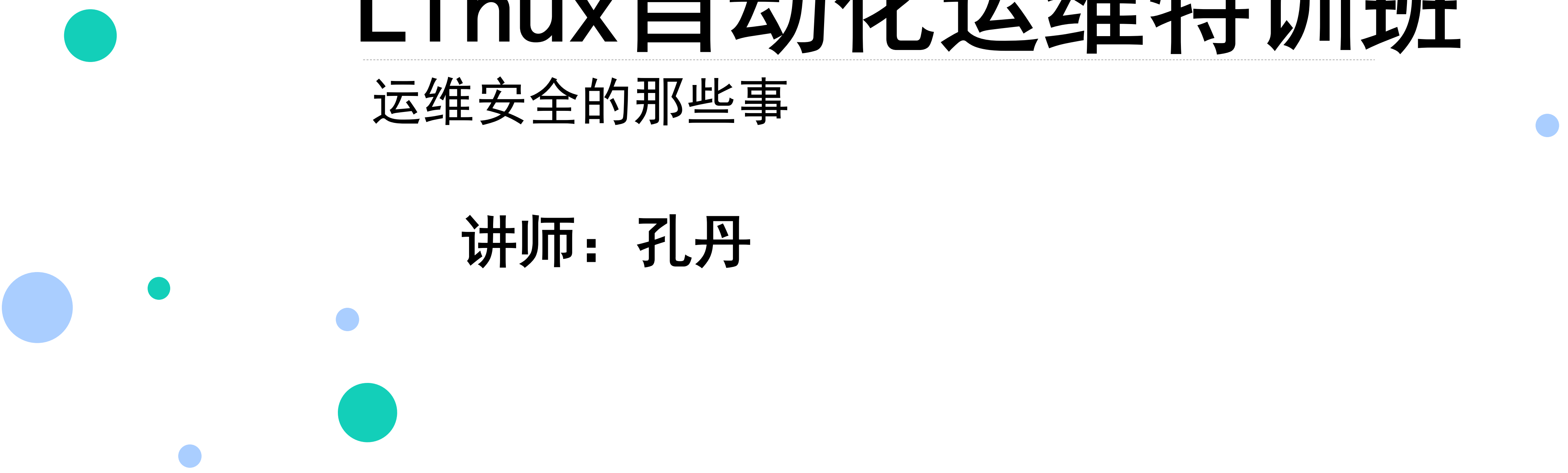


Linux 自动化运维特训班

运维安全的那些事

讲师：孔丹



大纲

- 运维安全简介
- 运维安全威胁
- 运维安全陋习
- 运维安全问题
- 运维安全案例
- 运维安全防范

版权所有，侵权必究

运维安全简介

- 运维安全属于企业安全非常重要的一环。
- 这个环节出现问题，往往会导致非常严重的后果。
- 运维安全研究的是与运维相关的安全问题的发现、分析与阻断：比如操作系统或应用版本漏洞、访问控制漏洞、DDoS攻击等。显然，运维安全立足于运维，从企业架构上讲通常属于运维部门或者基础架构部门，运维安全工程师的专业序列一般属于运维工程师。

为什么重视运维安全

- 近年来，作为互联网基础设施的几大应用相继被爆漏洞或被攻击，例如Struts2远程代码执行漏洞、Openssl心脏滴血、Bash破壳漏洞，以及当时“史上规模最大的DDoS攻击”导致大量.cn和.com.cn域名无法解析等等
- 企业对运维安全投入迅速加大，各种运维安全问题也引起广泛关注。直到今天，运维安全已经成为企业安全建设的重中之重。

版权所有，侵权必究

运维安全威胁

- ❑ 漏洞百出的软件供应链
- ❑ struts2远程代码执行漏洞
- ❑ 当年S2漏洞一出，整个互联网一片哀嚎。下面是受影响的企业，几乎没有不认识的吧。

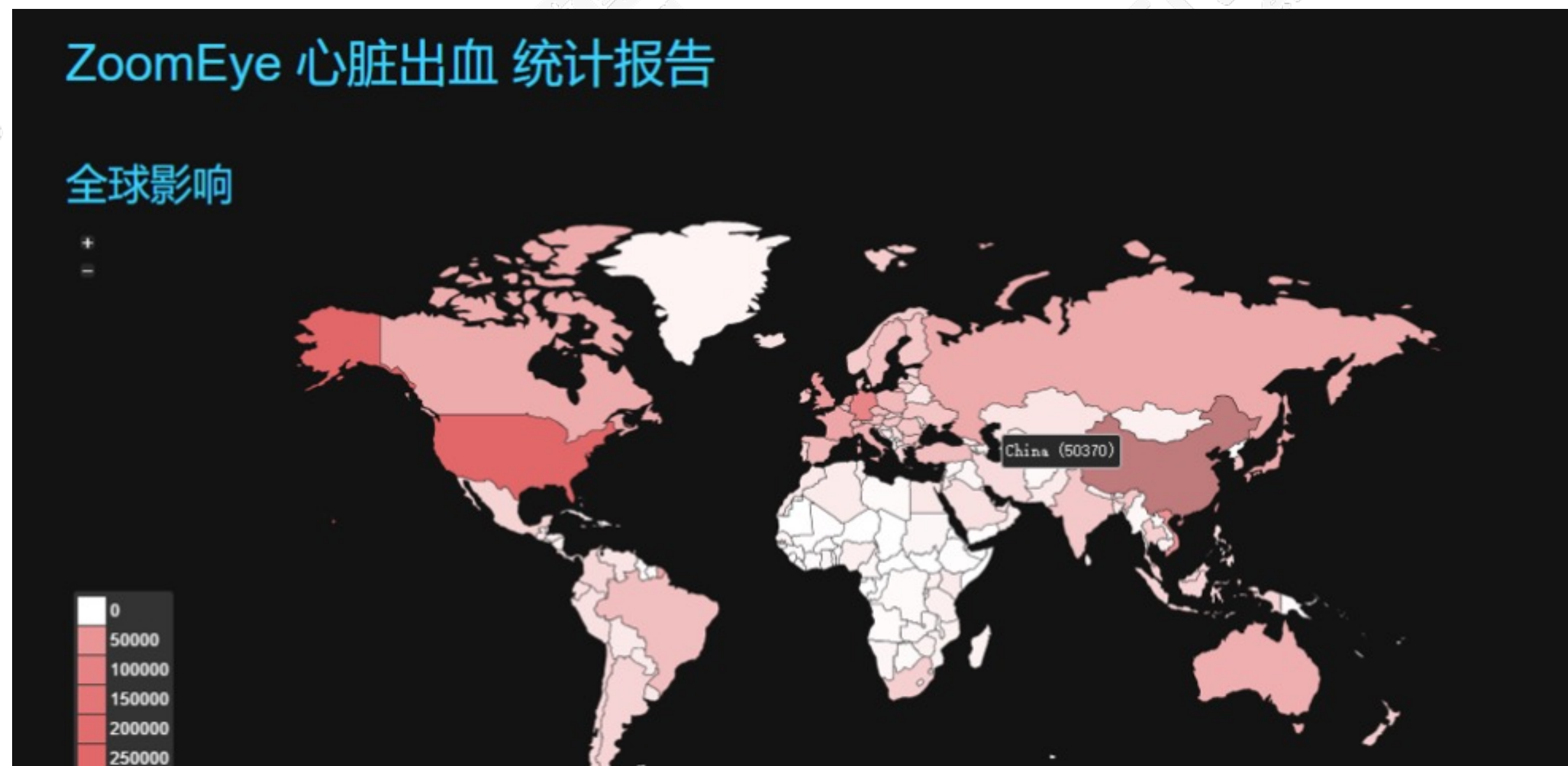
2013年漏洞爆发立刻影响到的企业



版权所有，侵权必究

运维安全威胁

- ❑ 漏洞百出的软件供应链
- ❑ openssl心脏滴血
- ❑ 跟S2漏洞一样，杀伤力极强。



版权所有，侵权必究

运维安全威胁

□ 一次成功的漫游京东内部网络的过程（由一个开发人员失误导致）

1. 首先研发人员将公司的代码发布到第三方代码托管平台，例如GitHub。
2. 其次代码的某些配置里面有发邮件的功能，并且调用了公司的邮箱。
3. 公司的邮箱与VPN的认证是互通的，且VPN没有双因素验证。
4. 恶意用户通过这个账号登陆了企业的VPN，从而达到漫游内网的过程。

版权所有，侵权必究

运维安全威胁

□ 我是如何拿到高德7个vcenter和漫游内网的

1. 首先研发人员将公司的代码发布到第三方代码托管平台，例如GitHub。
2. 其次代码的某些配置里面有发邮件的功能，并且调用了公司的邮箱。
3. 邮箱没有对通讯录遍历功能进行限制，导致遍历通讯录
4. 对所有的用户进行一次弱口令的洗劫，是用Burpsuite破解（简称：BP）
5. 得到一个运维或者运维组员工的邮箱，在邮件里面找到了明文密码.txt

版权所有，侵权必究

运维安全威胁

□ 百度某站漏洞导致敏感信息泄露Getshell

(涉及至少66W+的用户数据含密码可内网)

1. 上线前没有进行安全检查, .git目录外泄
2. 检出源代码, 得到UC_KEY
3. 利用UC_KEY得到websheII
4. 通过websheII内网

版权所有, 侵权必究

运维安全威胁

□ 搜狐的zabbix, 可导致内网渗透

1. zabbix默认口令 (admin/zabbix)
2. 执行正常命令测试命令执行模块
3. 执行恶意命令使服务器反连到你的机器
4. 得到zabbix权限的shell
5. 提权的提权, 内网的内网

版权所有，侵权必究

运维安全威胁

□ 58同城某业务多个站点存在弱口令导致Getshell

(内网小漫游)

1. Tomcat业务manager模块存在并开启
2. 配置了tomcat-users.xml, 并且存在弱口令
3. 上传war包得到webshell
4. 提权的提权, 内网的内网

版权所有, 侵权必究

运维安全威胁

❑ 顺丰删库跑路

2018年9月，顺丰科技数据中心的一位邓某因误删生产数据库，导致某项服务无法使用并持续590 分钟。



运维安全威胁

□ 腾讯云故障数据丢失

2018年8月5日，北京清博数控科技有限公司（以下简称“前沿数控”）在官方微博发文：《腾讯云给一家创业公司带来的灾难！》。表示，在使用腾讯云服务器8个月后，我们放在云服务器上的数据全部丢失，腾讯云所谓的三备份数据也全部离奇丢失！。

“而灾难就发生在2018年7月20日，我们近千万元级的平台数据全部丢失，包括经过长期推广导流积累起来的精准注册用户以及内容数据，这瞬间将一家创业公司摧毁...”

事件：

当天上午11:57，腾讯云运维人员收到仓库I空间使用率过高告警，准备发起搬迁扩容。

14:05，运维人员从仓库I选择了一批云盘搬迁至新仓库II，为了加速搬迁，手动关闭了迁移过程中的数据校验。

20:27，搬迁完成之后，运维人员将客户的云盘访问切至仓库II，同时为了释放空间，对仓库I中的源数据发起了回收操作。

20:30，监控发现仓库II部分云盘出现IO异常。

运维安全威胁

□ 万豪酒店数据泄露

2018年底，万豪酒店宣布：旗下喜达屋的一个顾客预订数据库被黑客入侵，可能有多达5亿人次预订喜达屋酒店客户的详细个人信息遭到泄露。经过一段时间调查后，万豪集团将遭到信息泄漏的客户数量修正为3.83亿。

万豪酒店因此在美国遭遇集体诉讼，索赔金额高达125亿美元。万豪酒店去年公开的用户信息泄漏一事有了最新结果，这家公司被英国罚款1.24亿美元。

运维安全威胁

□ 阿里云故障

2019年，3月3日早间消息，阿里云深夜出现故障，引发众多网友吐槽，“很多互联网公司的App和网站瘫痪，一大波程序员和运营、运维专员都从被窝爬起来去公司干活了”。

对此，阿里云官方凌晨向新浪科技回应称，华北2地域可用区C部分ECS服务器等实例出现IO HANG，经紧急排查处理后逐步恢复，此外将根据协议尽快赔偿。

在今日凌晨2点37分，阿里云官网发公告称经紧急排查处理后已全部恢复，并已经全面排查其他地域及可用区，未发现此类情况



版权所有，侵权必究

常见运维安全陋习

□ 运维安全事件频发，一方面固然是因为运维或安全规范空白或者没有落地，另一方面也在于运维人员缺乏强烈的运维安全意识，在日常工作中存在这样那样的安全陋习导致。

1、修改iptables后没有还原配置，甚至清空关闭iptables
出于测试需要临时清空iptables可以理解，但是很多人会忘记还原，也没有设置自动还原机制

iptables -F

版权所有，侵权必究

常见运维安全陋习

□ 常见运维安全陋习

2、脚本没有检查“*”、空格、变量

如果我们认可“不光用户的输入是不可信的，自己的输入也是不可信”，这样的坑就会少踩。

```
rm -rf /var1/var2
```

3、服务启动默认监听全部地址

绝大部分应用默认配置便是如此，在没有有效访问控制的情况下开启监听所有地址，离危险也不远了。

```
bind-address 0.0.0.0
```

版权所有，侵权必究

常见运维安全陋习

□ 常见运维安全陋习

4、给文件开放过大的权限时，任何人都能读写
这个跟phpinfo有点像，能给入侵者推一把。

```
chmod 777 dir || chmod 666 script
```

5、用root启动服务

对于大多数运维人员而言，一上机器就切到root，后面用
root启动服务仿佛一气呵成。

```
#nohup ./server &
```

6、嫌麻烦不配认证，也不配访问控制

这个跟监听任意地址比较像，通常也是默认配置使然，使用
者也没有意识去加固。

```
#requirepass test
```

版权所有，侵权必究

常见运维安全陋习

□ 常见运维安全陋习

7、单机安装docker之后忽略检查iptables，导致docker修改iptables开放外网

docker技术给我们带来的便利自不必言，但是因为docker带来的安全风险却一点也不少。而且，docker daemon默认是能控制宿主iptables的，如果docker daemon使用tcp socket或者启动的容器可被外部访问，则连宿主一同 沦陷也不在话下。比如下面一启动容器则将tcp/443端口对外开放了。

```
docker restart
```

8、sudo授权过大，导致自定义脚本提权
如果攻击者可修改脚本内容则提权易如反掌。

```
sudo script.sh
```

版权所有，侵权必究

常见运维安全陋习

□ 常见运维安全陋习

9、给开发或者QA授权root权限，他搞事你背锅？

一直以来我们强调RBAC，基于角色的访问控制（Role-Based Access Control），但是运维太忙，开发测试人员需求太多时，很多运维人员会直接授权他们root权限，而他们对系统级访问控制不甚了了，因此造成的漏洞非常可观

10、key/token/ssh私钥保存在txt文件里，也有把个人ssh私钥放在服务器的

11、把工作上的代码对外发布

常见运维安全问题

□ 敏感端口对外开放

db或者cache属于敏感应用，通常部署在内网，但是如果部署的机器有内外网ip，且默认监听地址为0.0.0.0的话，则敏感端口会对外开放。如mysql/mongodb/redis/rsync/docker daemon api等端口对外开放。

□ 敏感应用无认证、空口令或者弱口令

同上，如果敏感应用使用默认配置，则不会开启认证，mysql/mongodb/redis/rsync/supervisord rpc/memcache等应用无认证。有时贪图测试方便，配置了弱口令或空口令，则认证形同虚设。

常见运维安全问题

- ❑ 敏感信息泄露，如代码备份、版本跟踪信息、认证信息泄露

web.tar.gz/backup.bak/.svn/.git/config.inc.php/test.sql等信息泄露随处可见，人人知道危险，但是始终时不时会有人会踩坑。

- ❑ 应用默认配置未清除

jenkins script/apache server-status等默认功能未清理，则可直接执行命令。

- ❑ 应用系统打开debug模式

Django debug模式开启暴露uri路径，phpinfo()暴露服务器信息甚至webroot等，之后攻击者便可借此进一步渗透，很多白帽子应当有此同感，发现了sql注入但是写不了webshell，如果能遇上个phpinfo()那是再好不过的事情了。

版权所有，侵权必究

常见运维安全问题

□ 应用漏洞未及时升级

越是通用的应用，就越经常爆出漏洞。有句话说的好：不是因为黑客这个世界才不安全，而是因为不安全才会有了黑客，才会有黑客去揭开那层假象，让我们发现有那么多不安全。于是Struts2、OpenSSL、Apache、Nginx、Flash等等CVE接踵而来。

□ 权限管理松散

不遵循最小权限原则，给开发提供root权限或者给业务账号授权admin权限。

□ DDoS攻击

DDoS攻击对于运维人员而言，是再熟悉不过的安全问题了。我们都知道通过占满带宽、耗尽资源等方式可让服务器无法响应正常请求，说到底资源对抗的一种攻击方式。如果仅依赖服务器资源去抗，去过滤，在大流量、高并发之下，只会引来雪崩。加上DDoS攻击平台大量存在，而且价格低廉，这就让DDoS攻击成为打压竞争对手、报复、勒索等阴谋诡计者首选方式了。

常见运维安全问题

□ 流量劫持

还记得2015年小米、腾讯、微博、今日头条等六家公司联合发表声明呼吁电信运营商打击流量劫持的报告吗？即便如此，现今的互联网江湖仍是暗流滚滚。下面介绍三种常见的流量劫持方式，这也是困扰运维安全人员多年的痼疾。

arp劫持：ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行。基于ARP协议的这一工作特性，黑客向对方计算机不断发送有欺诈性质的ARP数据包，假冒目标IP进行ARP响应，从而实现中间人攻击。

域名劫持：通过劫持掉域名的DNS解析结果，将HTTP请求劫持到特定IP上，使得客户端和攻击者的服务器建立TCP连接，而非和目标服务器直接连接。

HTTP劫持/直接流量修改：在数据通路上对页面进行固定的内容插入，比如广告弹窗等。

运维安全案例

❑ svn

部署web代码时误将. svn目录上传

使用rsync上传代码时没有exclude掉. svn目录，svn仓库也没有使用svn propedit svn:ignore <目录或文件>的方式ignore掉不应当上传的文件或目录。

攻击者利用svn信息泄露利用工具Svn-Tool或者svn-extractor还原代码

❑ rsync

rsync使用root用户启动，模块没有配置认证，还对外开放默认端口873

攻击者利用rsync写crontab任务成功反弹shell，并种上了挖矿木马

运维安全案例

❑ redis

redis使用root用户启动，没有配置认证，还对外开放默认端口6379

攻击者利用redis写ssh公钥到root用户的.ssh目录成功登上机器
一般部署redis的机器都有内网ip，攻击者可借此进行内网漫游了

❑ kubernetes

k8s的api对外开放，同时未开启认证

攻击者调用api创建容器，将容器文件系统根目录挂载在宿主根目录，攻击者利用写crontab任务成功反弹shell，并在宿主种上了挖矿木马

有时候容器里跑着未编译的代码或者在沦陷的机器上可以拉到私有docker镜像仓库的任意镜像，后果将难以想象，如下面k8s的api，调用起来则非常简单。

如何做好运维安全

□ 培养良好的运维安全习惯

1、端口开放

默认监听内网或者本地

如需监听全部外网，iptables、password和acl能加都加上

2、iptables

在cmdb为机器或者服务设计好iptables规则，同时结合同步机制：

部署服务时使用cmdb生成的iptables同意更新

测试时一旦清空iptables后使用自动或者手工方式刷回标准

iptables

3、权限管理

采用puppet、ansible或者saltstack等集群管理工具统一管理操作系统权限

遇到临时需要高级权限时手工后添加定时回收，量大时采用自动化方式配置

如何做好运维安全

□ 培养良好的运维安全习惯

4、脚本安全

校验变量，特别是高危操作

原则上不给脚本授权sudo密码或者授予666的权限位

5、密钥管理

不要让ssh私钥离开你的办公电脑

定期修改你的corp或者域密码

配置与代码分离的一个理由是：账号密码不能写在代码里

6、服务管理

能不用root启动最好不要用root

不要把服务根目录放到你的home目录

如何做好运维安全

□ 培养良好的运维安全习惯

7、代码管理

跟工作相关的代码禁止上传github!!!
仔细学习git/svn等版本管理工具的使用姿势
定义好你的.gitignore，特别是删除你的.DS_Store

8、应用选型

安全性是应用选型的一个重要考虑点
对漏洞修复和安全编码不怎么积极的开源软件，再好用都不要用

9、关注应用安全配置文档

一般应用程序的官方说明文档会包含安全配置的章节，在部署时需要循序渐进，按照最佳实践配置安全部分，而不是嫌麻烦直接跳过。

如何做好运维安全

□ 企业级运维安全体系

安全体系，是一套很大的概念。从流程规范，到技术架构，不是本文所能解释清楚。因此，下面所探讨的企业级运维安全体系，会大体介绍一下，涉及到其中的部分。

首先，整套运维安全体系，其实属于企业安全体系的一部分，所以大体上思路不会相差太多。其次，运维安全，更关注的是“运维”，所以像业务风控、反欺诈、app反编译则不在考虑范围之内。

流程规范

运维规范如同法律，这套规范，不仅是约束、指引运维人员，也是约束、指引开发测试人员，以及围绕生产活动的所有参与者。

如何做好运维安全

□ 企业级运维安全体系 流程规范

1、培训

此处的培训 是只面向运维人员的意识与技术培训。就比如本文前面的安全陋习和安全习惯，就可作为意识培训的蓝本。而后面所讲的技术体系，则可作为技术培训的基础。

2、审批+审核+评估

首先，审核或者审批，不是为了阻碍业务发展，更不是为了没事找事，而是希望通过流程去减少或者避免人的因素导致忽略安全。所以权限申请要上级审批、功能开放要安全人员或者同组同事审核、功能上线要安全人员评估测试。当然，实现的方式可以灵活多样，比如默认通过，可以根据产品或者业务需要开启审批、审核机制，然后把评估机制放在业务上线流程中，只有通过评估才能上线。在安全部门比较强势或者相对重视安全的企业，相信以上机制都落实的比较到位。

如何做好运维安全

□ 企业级运维安全体系

3、安全报表

安全可视化、数据化非常重要，是体现安全价值的形式之一，因此通过与企业SRC或者安全部的对接，可以获取运维相关的漏洞、安全事件统计数据，然后根据内部需求进行二次处理，然后通过定期报表的形式发给运维人员或者部门领导甚至技术负责人查看，一方面让他们了解运维安全态势，这种通常能看到安全不足，从而让大家从数据得到警示，或者获得上级关注，从而为获得更多的资源或者实现自上而下推动安全规范落地走向可能。

如何做好运维安全

□ 企业级运维安全体系

技术体系

1、访问控制

1>安全域划分下的网络隔离

网络层：192.168分为办公区、办公服务区与开发机网，部分隔离；10.x分为IDC物理内网、IDC虚拟内网与公有云虚拟内网，通过IGP互通，可申请端口映射外网；公网IP仅用于业务外网，开发测试环境禁止使用公网环境！

系统层：装机镜像默认开启防火墙，仅开放ssh、rdp管理端口。ssh一律采用公钥登陆，禁止启用密码认证；按角色授权系统权限。

应用层：数据库、缓存类应用部署在内网IP，管理接口禁止对外开放，按最小权限原则授权

如何做好运维安全

□ 企业级运维安全体系 技术体系

2>统一出入口级访问控制

建设IDC级别统一入口，结合NAT网关实现出入向访问控制。

目前BATJ都有自己的企业级GW作为统一应用层入口，同时使用NAT网关走出向流量。GW的实现开源方式不少，一旦作为企业级GW仍需自研。而NAT网关，则可采购具备API功能的分布式硬件防火墙或者自研NAT网关，解决IDC内网出向流量RS直接回外网时无外网IP的问题，或者服务器直接对外发起请求的情况，然后再采用统一系统管理。目前业界多有分享，相关思路不难找到。

3>敏感端口访问控制

一旦有了统一的出入口，整个生产网就像办公网一样，可以对外屏蔽敏感端口访问，对内限制出向流量，在风险缓解和攻击阻断上行之有效。

版权所有，侵权必究

如何做好运维安全

□ 企业级运维安全体系

技术体系

2、应用层访问控制

通过WAF防刷、限流是一种通用方案，如果没有WAF的可以应用的acl自行进行控制，比如nginx的limit_rate或者haproxy的acl。

1>堡垒机与VPN

使用堡垒机可实现运维入口统一化，也能做到集中访问控制和审计。

在登陆堡垒机时也需要拨入VPN，目前应用比较广泛的有IPSecVPN以及SSLVPN，像openvpn则部署维护简单、服务端较为灵活以及客户端支持丰富等优势目前被广泛应用。

服务器ssh端口或者业务管理后台也可只对堡垒机与VPN Server开放白名单

2>基线审计与入侵检测

基线审计与入侵检测是两个不同的概念，前者在于事后审计，看合不合格，后者在于事前预防与事中检测响应。在具体落地上，基线审计通常依赖堡垒机，入侵检测通常依赖安全agent。

如何做好运维安全

□ 企业级运维安全体系

技术体系

2、应用层访问控制

3>堡垒机

通常堡垒机有访问控制、日志审计、操作行为审计、数据上传下载审计以及权限管理等功能。但是，系统补丁更新与应用版本更新等操作，则不是堡垒机所能覆盖。

对于堡垒机的落地，采购设备倒是其次，重点在于整合整套运维体系，对于有些年头的企业改造成本太大，而且大家也担心其性能与可用性。

4>漏洞扫描

漏洞扫描器也可以结合机器学习或者大数据分析，根据扫描日志或者已有的经验，做策略的自动生成，实现扫描规则的轻量化与精准化。

版权所有，侵权必究

如何做好运维安全

□ 企业级运维安全体系

技术体系

2、应用层访问控制

5>CI/CD安全

CI/CD是运维的重要一环。在CI/CD上出现的安全漏洞也多如牛毛。下面我们从如何安全的发布和应用部署来讨论。

敏感信息泄露

我们都知道发布代码应排除：源码文件和临时文件，如.py、.cc、*.swp(vim临时文件)，上传版本管理相关的信息文件(如.svn/.git)，以及打包/备份文件(如.gz/.bak)。这看起来更像是一种规范，其实不然，通过在代码分发系统增加钩子或者过滤模块，是可以提前发现敏感信息的上传的。比如代码提交了ssh私钥或者账号密码配置文件，只需要一个webhook就能检测到。实现上的成本与出问题付出的代价相比，其实不算什么。

版权所有，侵权必究

如何做好运维安全

□ 企业级运维安全体系

技术体系

2、应用层访问控制

5>CI/CD安全

CI/CD是运维的重要一环。在CI/CD上出现的安全漏洞也多如牛毛。下面我们从如何安全的发布和应用部署来讨论。

代码或镜像的安全审计

随着docker容器技术的广泛应用，CI/CD安全的落地更加充满希望。我们都知道，使用docker容器需要经历编写dockerfile/docker-compose文件，docker build之后才有镜像，然后再docker pull、docker run部署服务，实际上可以结合jenkins等CI/CD工具调用CoreOS官方的Clair镜像安全审计工具进行漏洞扫描。此外，当然还有RASP等Runtime机制的动态检测机制，也有foritity或者Cobra等或商用或开源的代码审计工具，也可以结合使用。

版权所有，侵权必究

如何做好运维安全

□ 企业级运维安全体系

技术体系

3、认证授权

SSH不允许用密码登陆，必须用公钥登陆

建立个人帐号的概念，必须做到一人一个帐号，不允许多个人共用一个个人帐号

公共帐号要和个人帐号分开，不允许直接登陆

口令安全需要注意复杂度校验

无法通过网络层或应用层进行访问控制的，应增加认证授权机制

RBAC：根据角色授权

最小权限原则：禁止给业务配置root/admin级别的数据库账号，根据业务需求授权相应权限。

白名单机制：同时限制root/admin级别的数据库账号仅能通过白名单ip访问。如存在默认账号密码应同时删除。

认证信息管理：说到docker容器这块，目前kubernetes提供了ConfigMap，可以用于传递认证配置路径或者其他间接变量，用于计算认证信息。也可以用Hashicorp Vault进行认证信息管理

如何做好运维安全

□ 企业级运维安全体系

技术体系

4、数据安全

数据安全层面，最好是和开发、业务安全联合规划设计方案。通常运维安全所能覆盖的是访问控制、认证授权、备份、加密等。

访问控制：区分数据敏感程度，实行不同程度的访问控制。但是应当严格按照db放置于内网的原则。

认证授权：基于RBAC进行授权。如果是比较成熟的db或者大数据集群，还可以使用动态计算权限、动态下发权限的方式，做到有需才授权、用完就回收。

备份：本地备份与远程备份，视业务需要决定是否加密备份。

如何做好运维安全

□ 企业级运维安全体系

技术体系

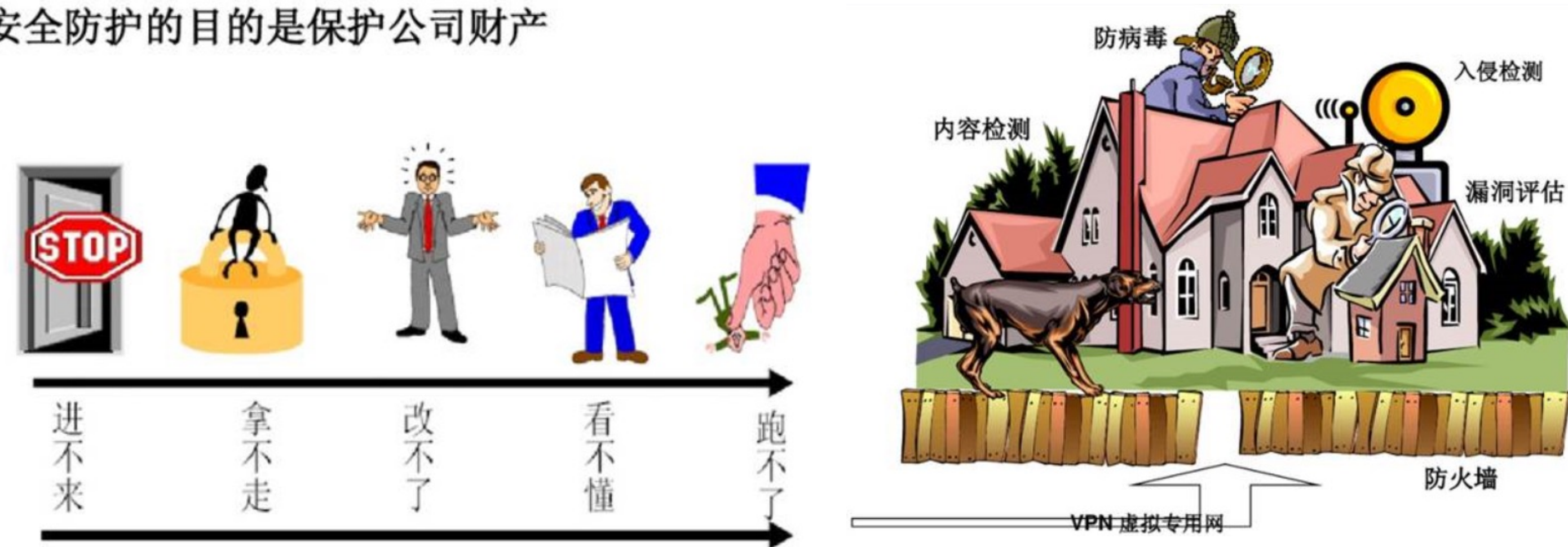
5、外部合作

运维安全，首先是运维。日常工作中与IT、安全和网络部门关系都十分密切，保持与兄弟部门的良好沟通和信息共享非常重要。

版权所有，侵权必究

安全防护

安全防护的目的是保护公司财产



安全防护体系需要采用多层、堡垒式防护策略

需要从多个层面解决安全问题（物理、通信、网络、系统、应用、人员、组织和管理）

分层安全防护成倍地增加了黑客攻击的成本和难度

有效地降级被攻击的危险，达到安全防护的目标

防火墙类似于护城河——只允许己方的队伍通过；

防病毒产品类似于城堡中的将士——想方设法把发现的敌人消灭；

入侵检测系统类似于城堡中的瞭望哨——监视有无敌方或其他误入城堡的人出现；

VPN类似于城堡内的安全通道——有时城堡周围遍布敌军而内外需要联络

漏洞评估类似于巡逻——检测城堡是否坚固以及是否存在安全隐患

总结

- 运维安全简介
- 运维安全威胁
- 运维安全陋习
- 运维安全问题
- 运维安全案例
- 运维安全防范

版权所有，侵权必究



谢谢观看

更多好课，请关注万门大学APP

