HUAWEI

华为云学院

学以致用　云世界大有可为

通过靶场平台演练增强安全攻防意识

华为云 +智能，见未来

www.huaweicloud.com

前言

随着计算机网络技术的快速发展及其在各领域的广泛应用，社会各界也越来越重视信息网络安全问题，不断投入资源进行网络攻防演练和信息安全研究。

目标

- 学完本课程后，您将能够：
  - 知道网络攻防的概念、现实意义等
  - 掌握网络攻击的概念、分类、方式等
  - 学会如何通过靶场平台演练增强安全攻防意识

目录

网络攻防演练的背景

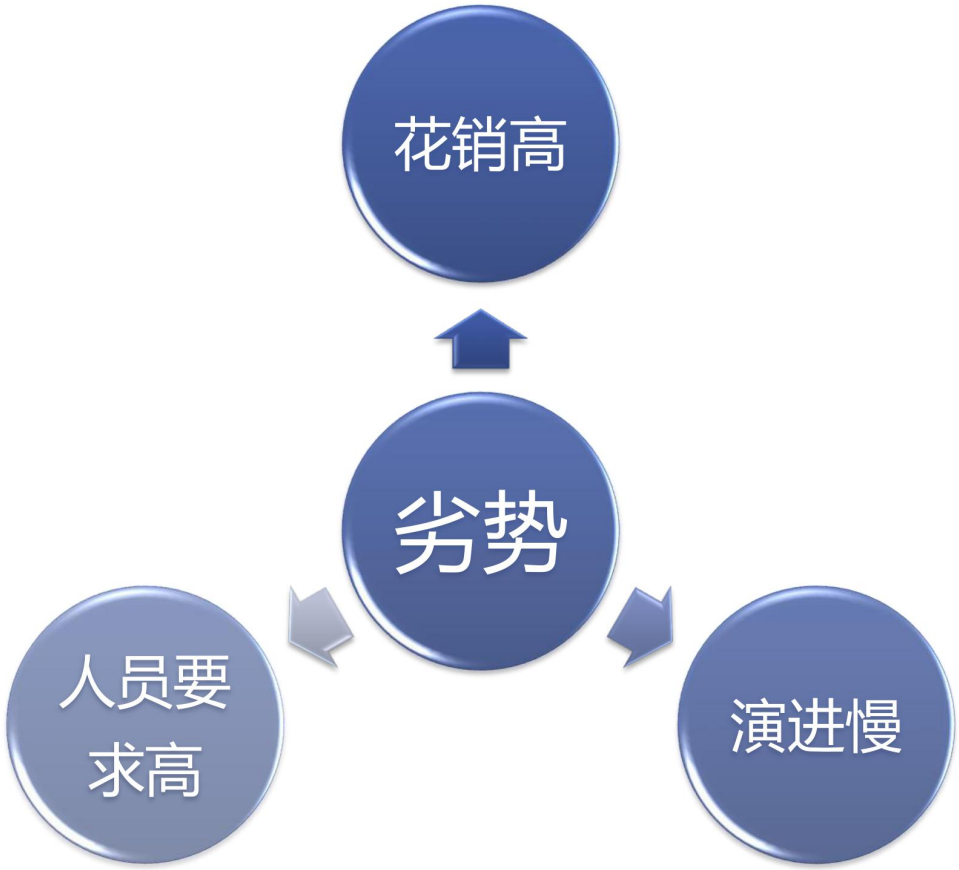
- 随着网络空间安全环境的不断恶化以及以明确政治、经济为目的的攻击事件的不断增多，近年来各级监管部门及企业自身均加强了对于网络安全的实战化要求。
- 对于企业来说，安全演练既是对网络安全建设的一次考核，也是一次发现自身安全建设短板的机会。

网络攻防的概念

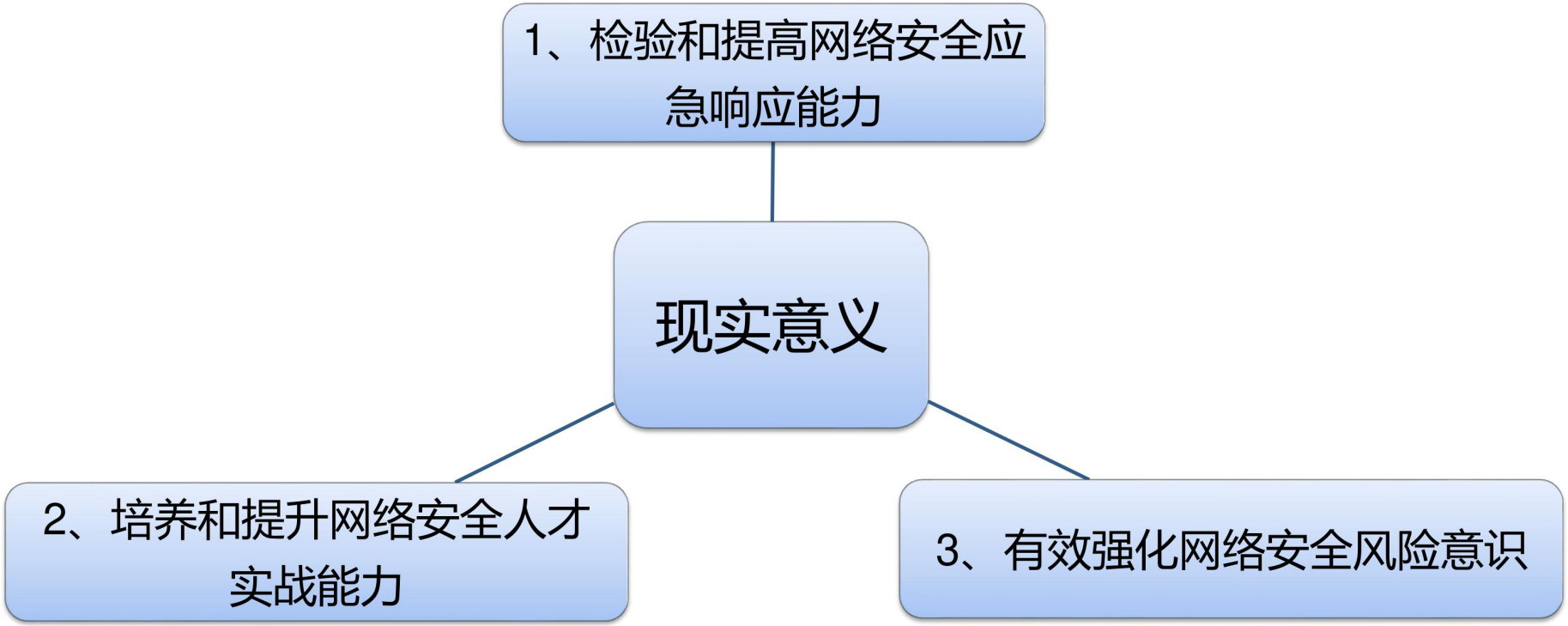
网络攻防，亦称“网络对抗”，网络攻击与网络防护的合称。

- **网络攻击**指综合利用目标网络存在的漏洞和安全缺陷对该网络系统的硬件、软件及其系统中的数据进行攻击。
- **网络防护**指综合利用己方网络系统功能和技术手段保护己方网络和设备，使信息数据在存储和传输过程中不被截获、仿冒、窃取、篡改或消除。

传统攻防演练的劣势



网络攻防演练的现实意义

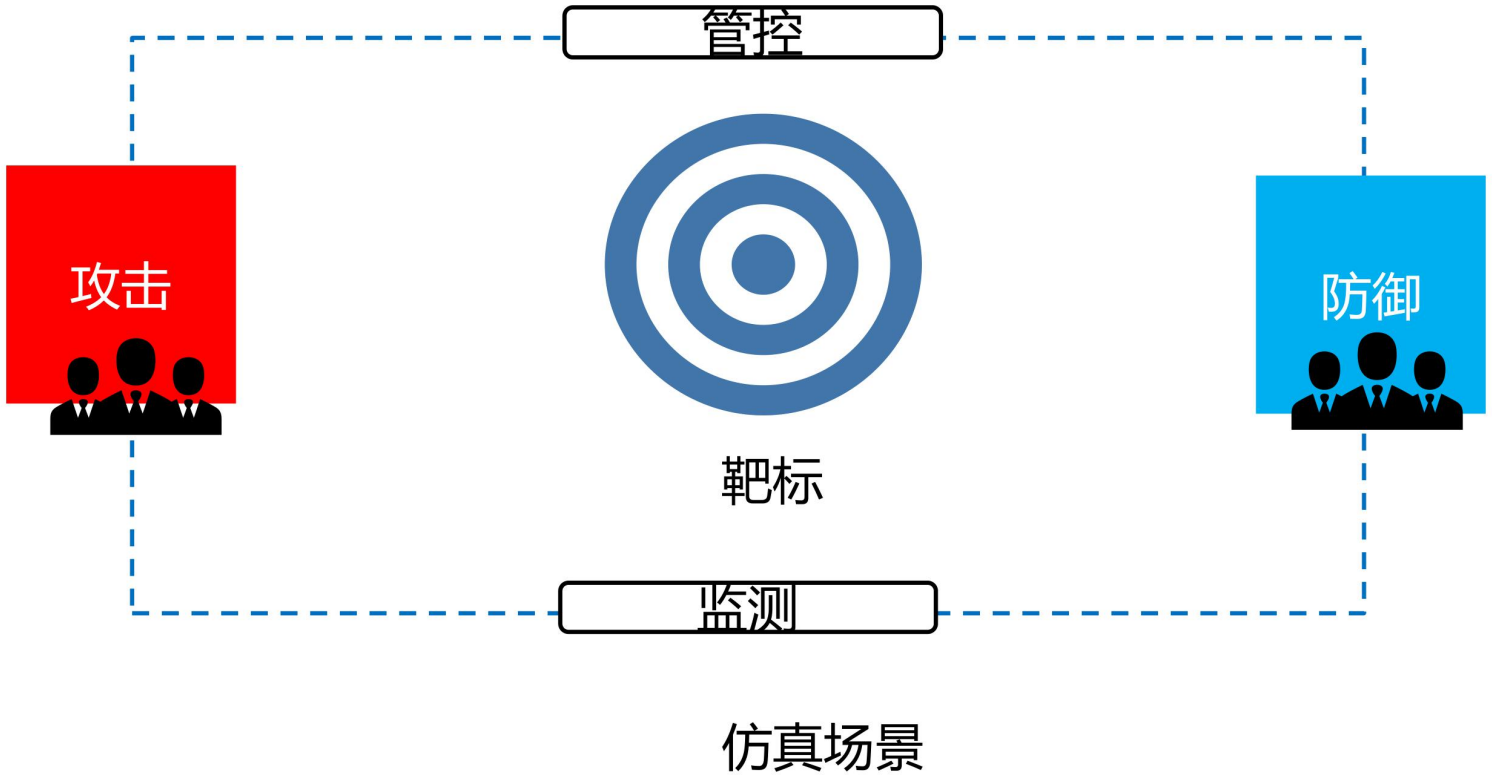


目录

网络靶场的概念

- 网络靶场是一个仿真的网络安全、攻防演练、人员培训的虚拟训练场。
- 网络靶场的价值在于能提供包括进攻（红方）、防御（蓝方）和导演组等多种角色在安全中心、网络中心或者数据中心进行的安全演练。

靶场五元组

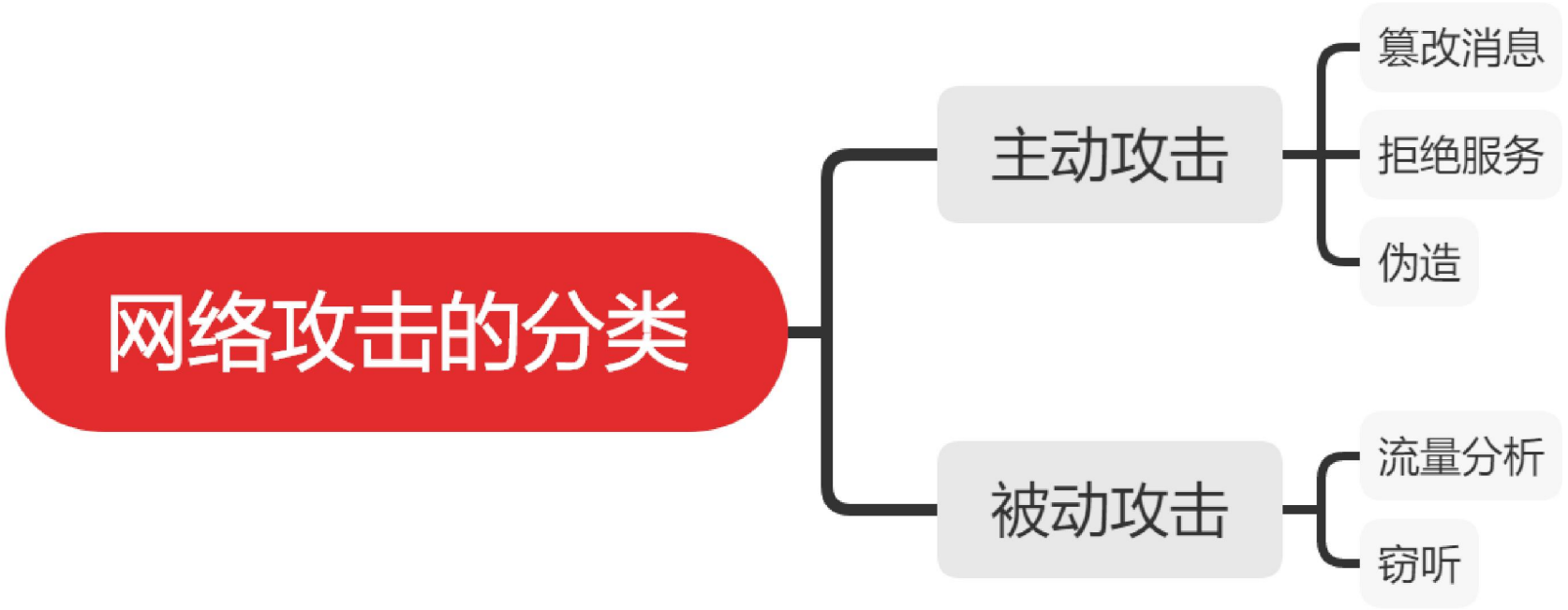


仿真场景

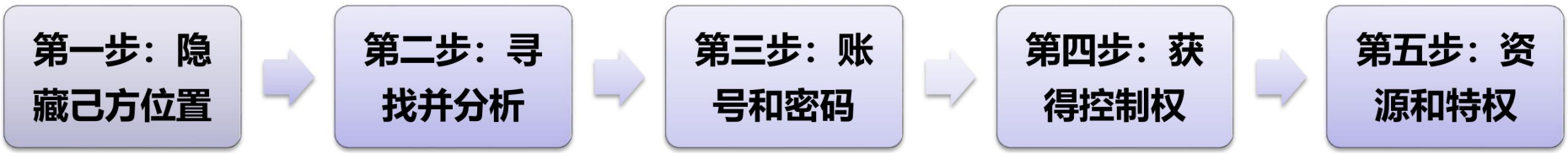
网络攻击的概念

- 网络攻击（Cyber Attacks，也称赛博攻击）是指针对计算机信息系统、基础设施、计算机网络或个人计算机设备的，任何类型的进攻动作。
- 对于计算机和计算机网络来说，破坏、揭露、修改、使软件或服务失去功能、在没有得到授权的情况下偷取或访问任何一计算机的数据，都会被视为于计算机和计算机网络中的攻击。

网络攻击的分类



网络攻击的步骤



网络攻击的方式

DDOS攻击

获取账号和密码

SQL注入

恶意小程序

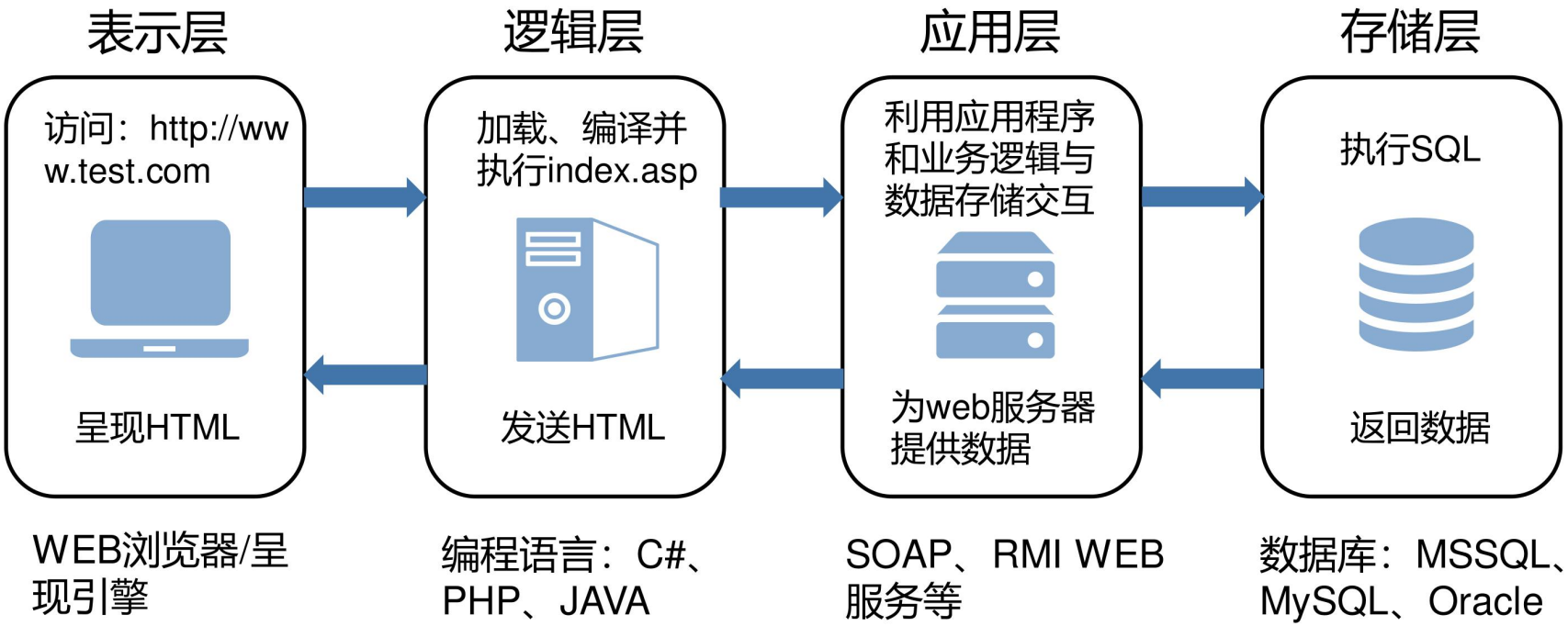
木马植入

SQL注入的概念和特点

SQL是操作数据库数据的结构化查询语言，网页的应用数据和后台数据库中的数据进行交互时会采用SQL。而SQL注入是将Web页面的原URL、表单域或数据包输入的参数，修改拼接成SQL语句，传递给Web服务器，进而传给数据库服务器以执行数据库命令。

广泛性　　隐蔽性　　危害大　　操作方便

SQL注入的原理


表示层
逻辑层
应用层
存储层
访问：http://www.test.com
呈现HTML
加载、编译并执行index.asp
发送HTML
利用应用程序和业务逻辑与数据存储交互
为web服务器提供数据
执行SQL
返回数据
WEB浏览器/呈现引擎
编程语言：C#、PHP、JAVA
SOAP、RMI WEB服务等
数据库：MSSQL、MySQL、Oracle

SQL注入的注入方法

由于编写程序时未对用户输入数据的合理性进行判断，导致攻击者能在SQL Injection的注入点中夹杂代码进行执行，并通过页面返回的提示，获取进行下一步攻击所需的信息。根据输入的参数，可将SQL注入方式大致分为两类：数字型注入、字符型注入。

SQL注入的攻击手法

1、基于布尔的盲注

2、基于时间的盲注

3、联合查询注入

4、基于错误信息的注入

SQL注入的防范措施

SQL注入攻击的危害很大，而且防火墙很难对攻击行为进行拦截，主要的SQL注入攻击防范方法，具体有以下几个方面。

1、分级管理
2、参数传值
3、基础过滤与二次过滤
4、使用安全参数
5、漏洞扫描
6、多层验证
7、数据库信息加密

传统的加解密的方法大致可以分为三种：

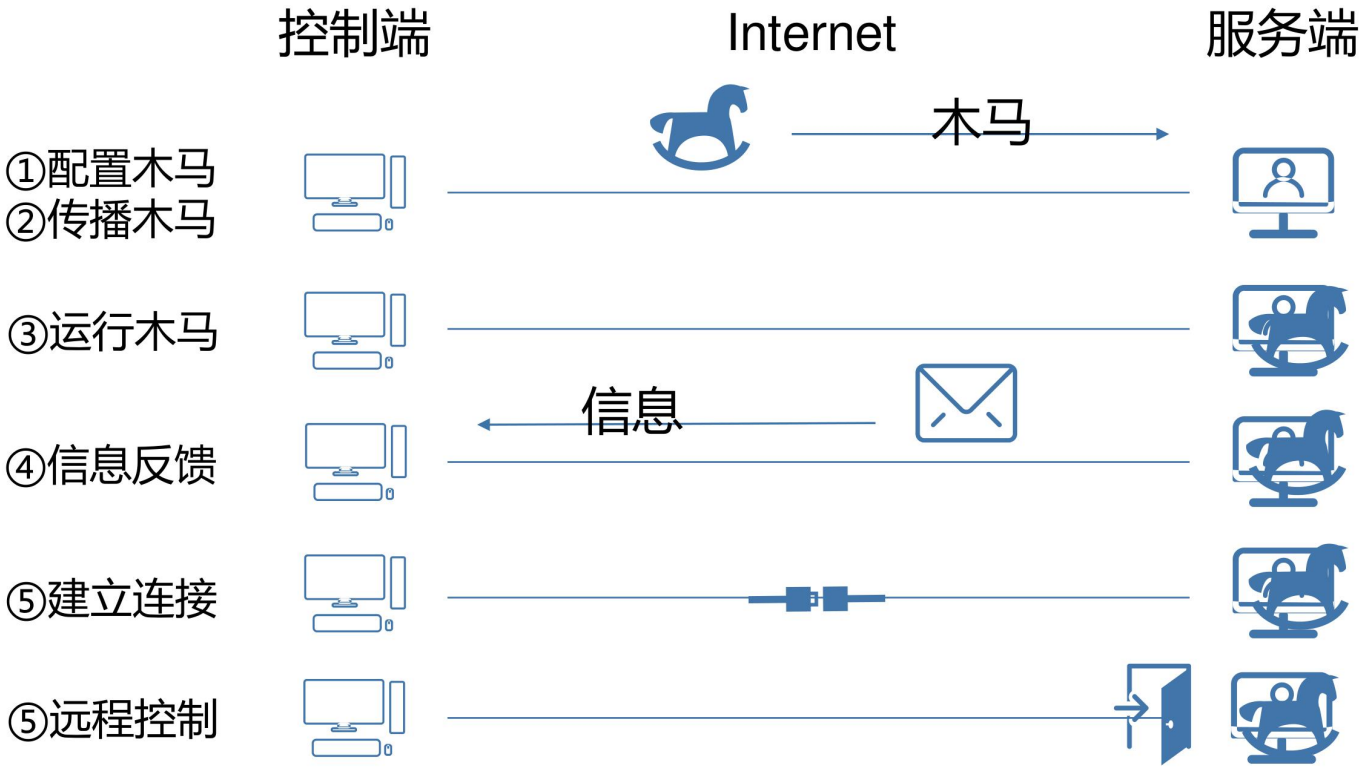
(1)对称加密
(2)非对称加密
(3)不可逆加密

木马病毒的概念特点

木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击Dos等特殊功能的后门程序。

隐蔽性　　欺骗性　　顽固性　　危害性

木马病毒运行的基本原理



木马的危害

木马病毒对计算机的直接破坏方式是改写磁盘，对计算机数据库进行破坏，给用户带来不便。当木马破坏程序后，使得程序无法运行，给计算机的整体运行带来严重的影响。另外一些木马可以通过磁盘的引导区进行，病毒具有强烈的复制功能，把用户程序传递给外部链接者。还可以更改磁盘引导区，造成数据形成通道破坏。病毒也通过大量复制抢占系统资源，对系统运行环境进行干扰，影响计算机系统运行速度。

木马防范

1、检测和寻找木马隐藏的位置

2、防范端口

3、删除可疑程序

4、安装防火墙

5、相关部门加强整治木马产业链，完善相应的法律法规

6、健全网站和网络游戏的管理

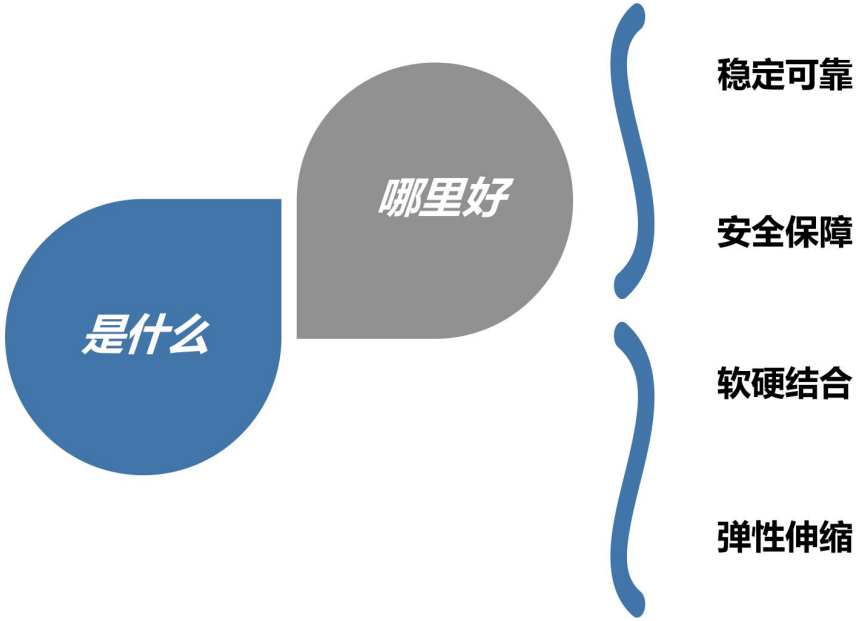
7、增加网民的防范意识

目录

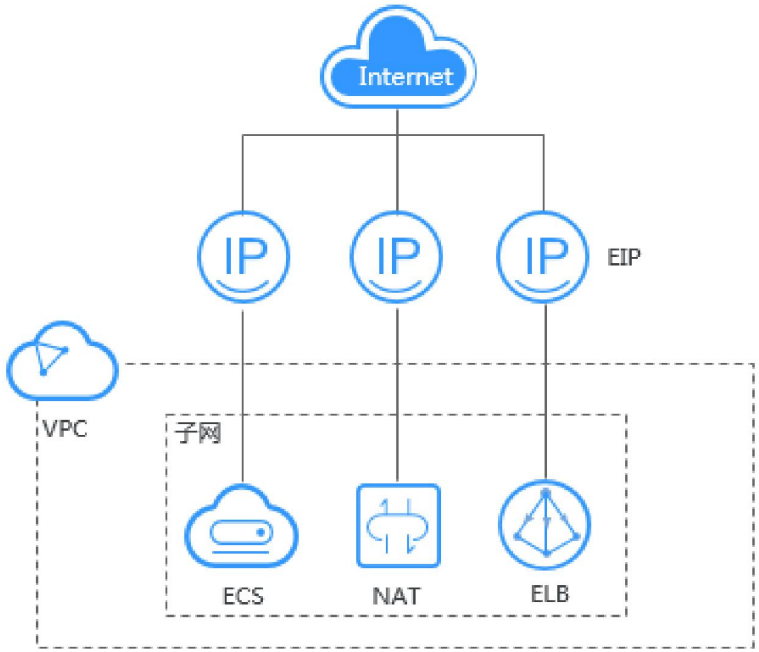
靶场平台攻防演练架构

靶场平台攻防演练架构 - 弹性云服务器

弹性云服务器（Elastic Cloud Server，ECS）是由CPU、内存、操作系统、云硬盘组成的基础的计算组件。弹性云服务器创建成功后，就可以像使用自己的本地PC或物理服务器一样，在云上使用弹性云服务器。

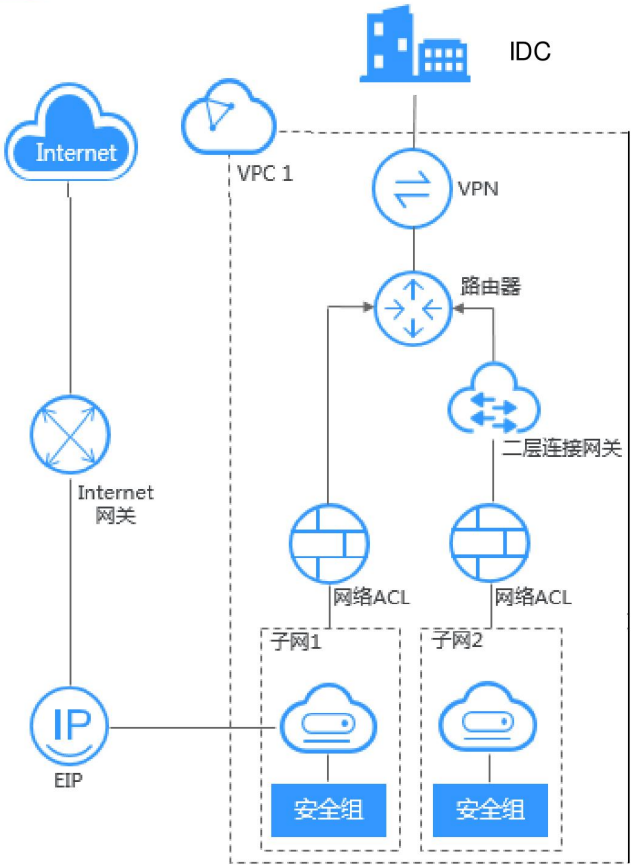


靶场平台攻防演练架构 - 弹性公网IP

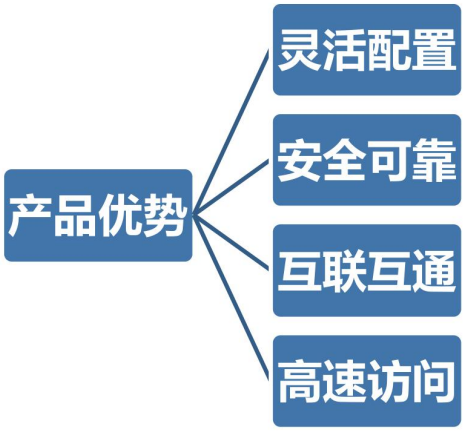


弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。

靶场平台攻防演练架构 - 虚拟私有云



虚拟私有云（Virtual Private Cloud，以下简称VPC），为云服务器、云容器、云数据库等资源构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。

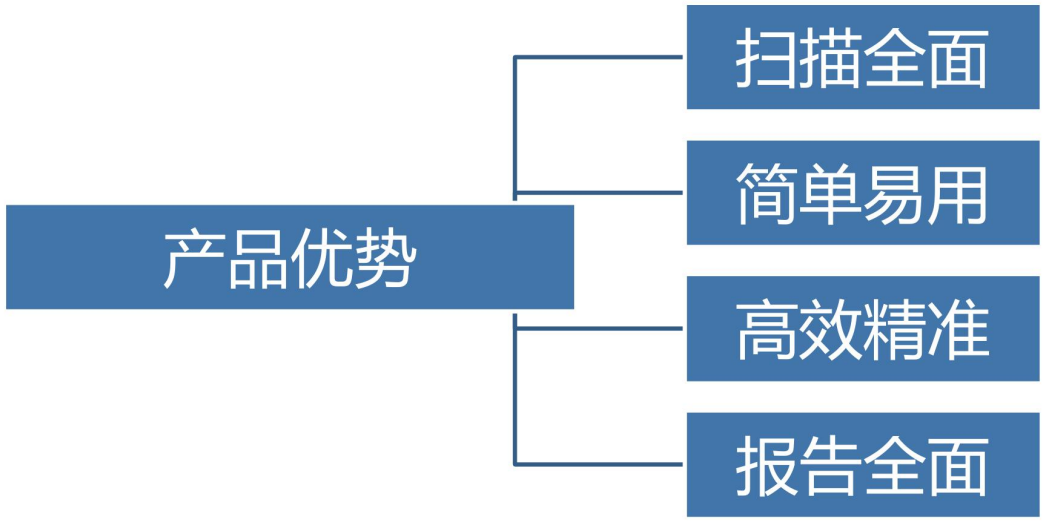


靶场平台攻防演练架构 - 企业主机安全

企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

靶场平台攻防演练架构 - 漏洞扫描服务

漏洞扫描服务（Vulnerability Scan Service，简称VSS）是针对网站进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测、漏洞生命周期管理、自定义扫描多项服务。用户新建任务后，即可人工触发扫描任务，检测出网站的漏洞并给出漏洞修复建议。



目录

关键流程

准备环境

预置环境

登录华为云

知识共享平台SQL注入攻击

开启企业主机安全防护

SQL注入漏洞确认

Sqlmap扫描爆破

企业主机安全病毒木马查杀体验

文件上传获取SHELL

运行第三方恶意程序

恶意程序隔离查杀

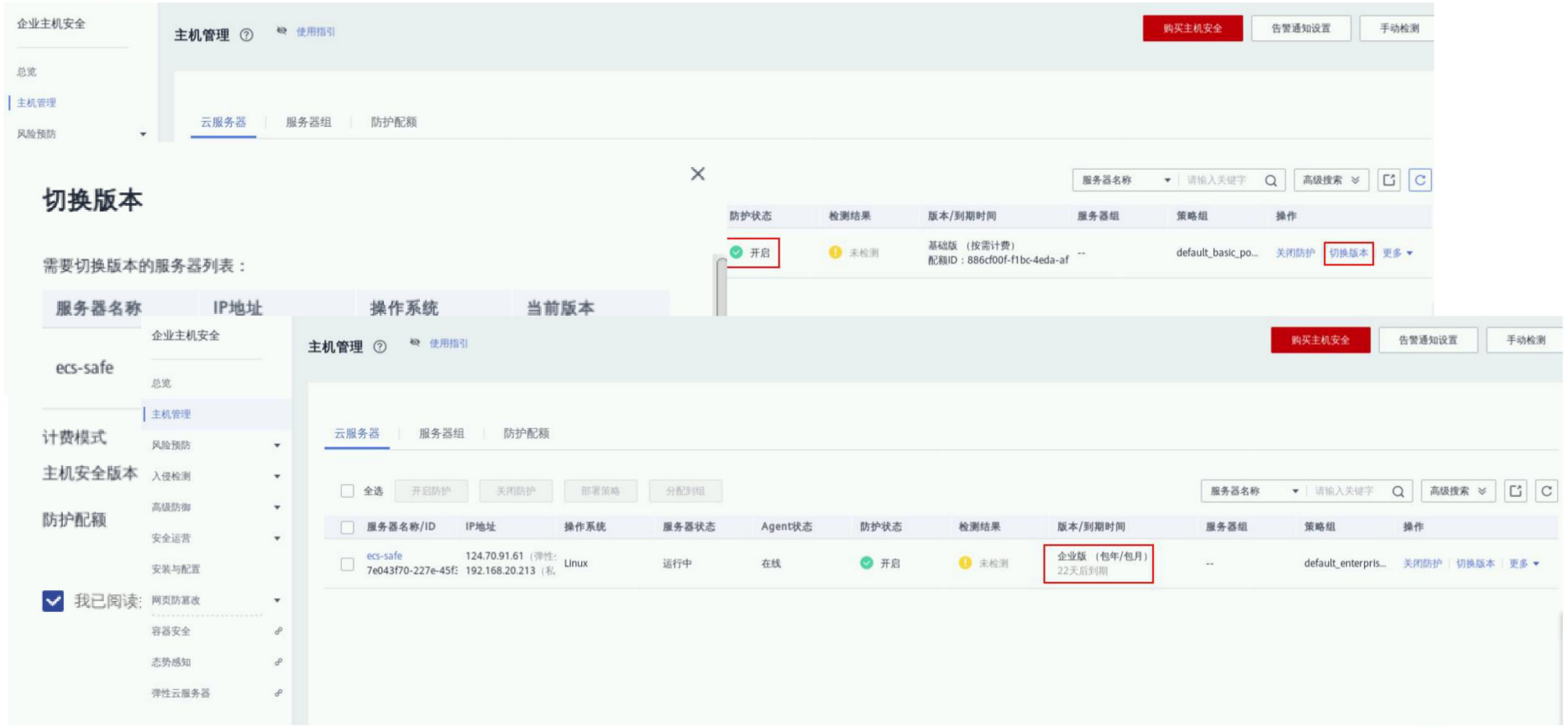
准备环境 - 预置环境

点击上方“预置实验环境”按钮，【约等待3分钟】后预置成功。环境预置成功会生成名称为“ecs-safe”的弹性云服务器ECS，创建配置相关的VPC、弹性公网IP、安全组，默认开启基础安全防护，并在“ecs-safe”上完成搭建攻防演练所需的数据库及知识共享平台应用。

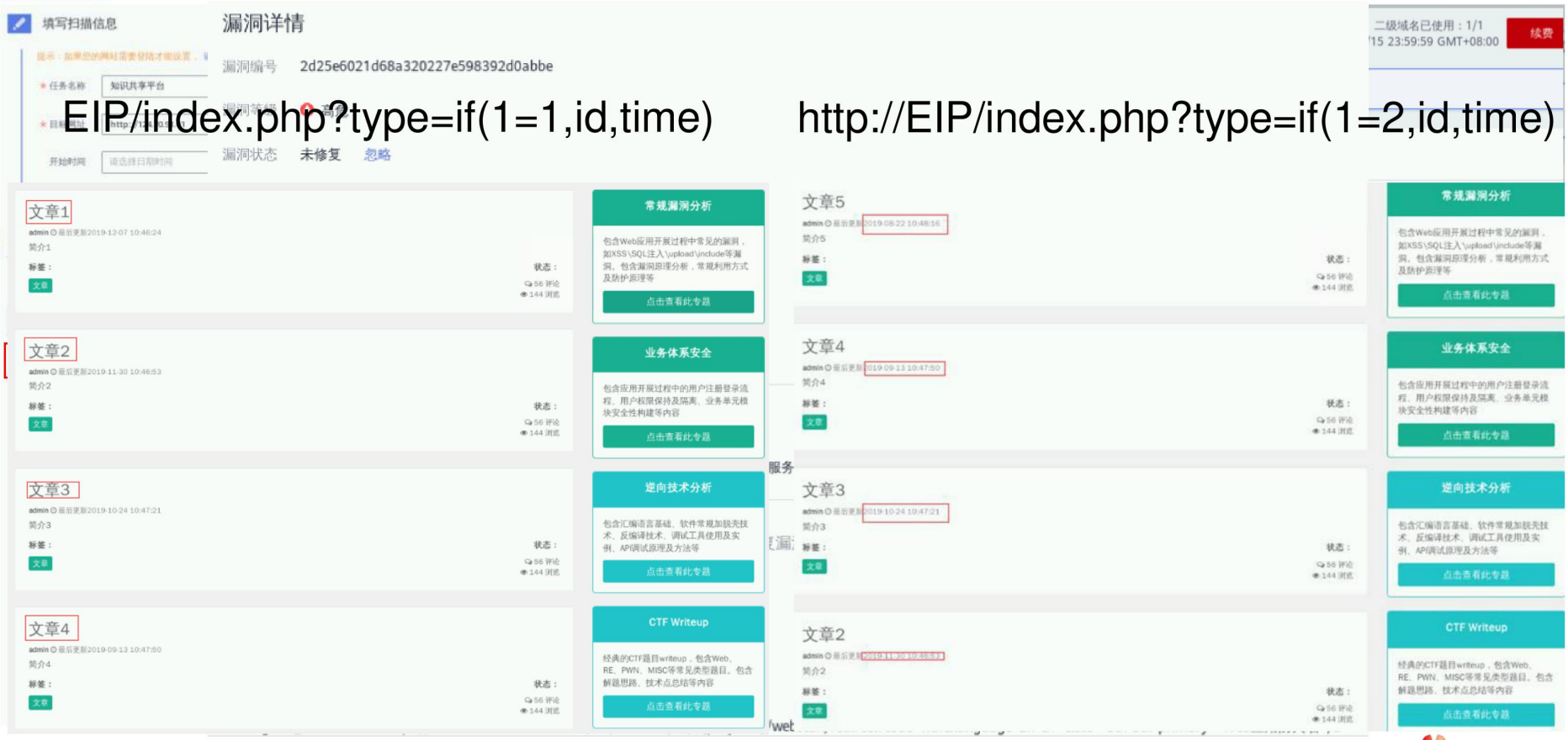
准备环境 - 登录华为云


扫码登录
密码登录
华为帐号登录
手机号/邮件地址/帐号名/原华为云帐号
密码
登录
注册
忘记密码
华为帐号服务在登录过程中会使用到您的帐号和网络信息提升您的登录体验，了解更多。点击"登录"表示您同意上述内容。
其他登录方式：IAM用户 华为官网帐号 | 华为企业合作伙伴 | 华为云帐号
扫码登录
密码登录
IAM用户登录
Sanfb
Sandb
登录
忘记密码
其他登录方式： 华为帐号

知识共享平台SQL注入攻击 - 开启企业主机安全防护



知识共享平台SQL注入攻击 - SQL注入漏洞确认

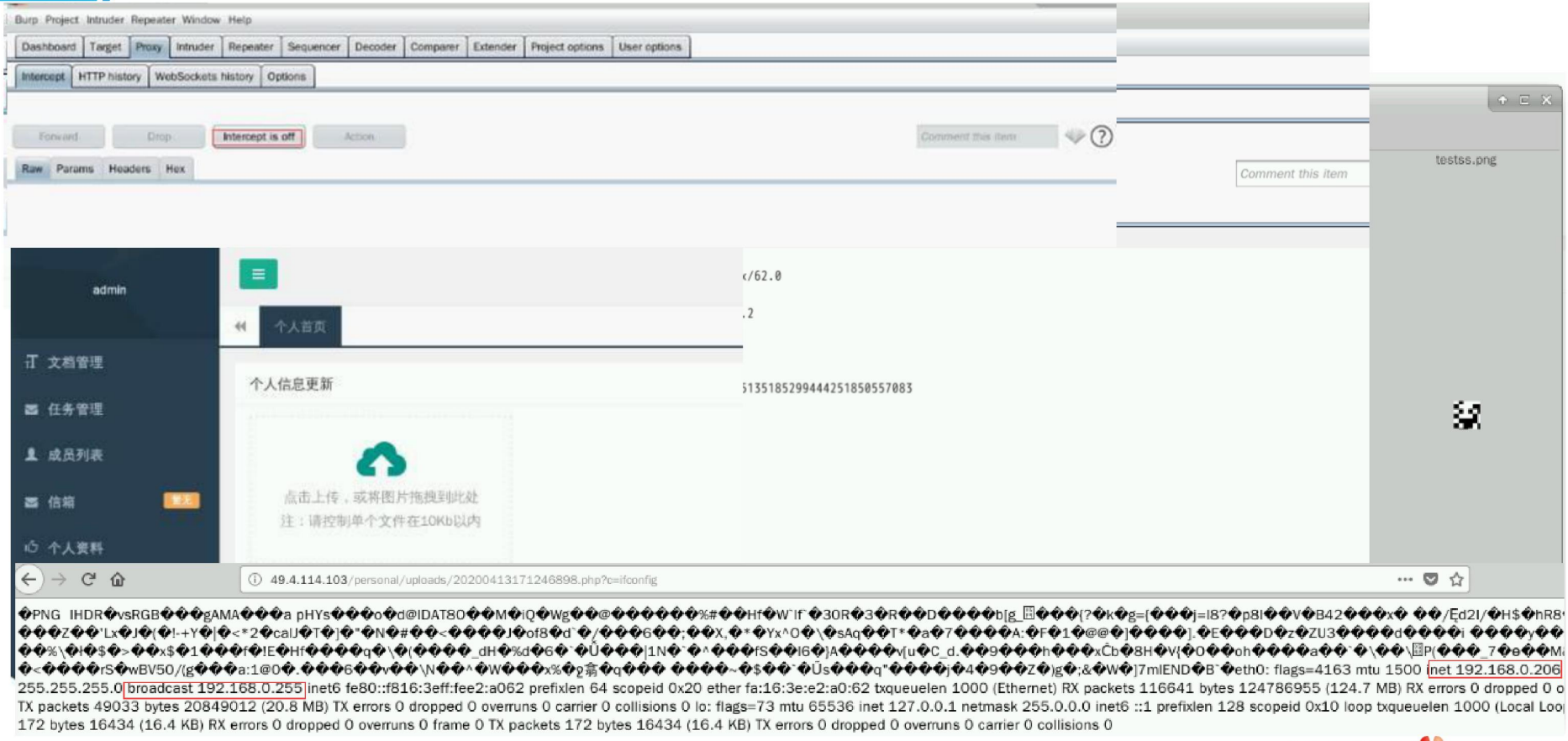


知识共享平台SQL注入攻击 - Sqlmap扫描爆破

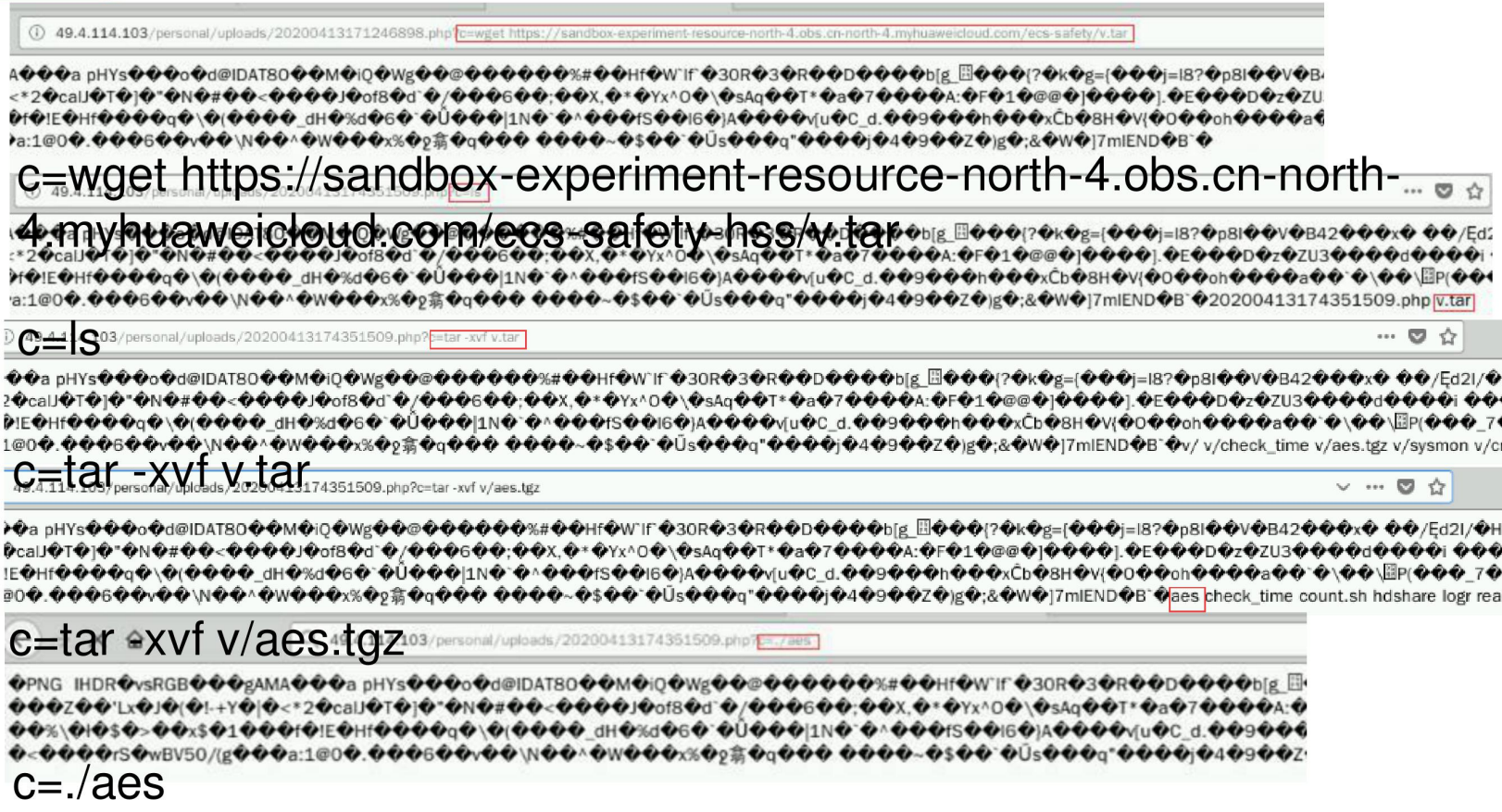
1、进行漏洞扫描：

./sqlmap.py -u http://EIP/index.php?type=1 -D webuser -T articleinfo -dump

企业主机安全病毒木马查杀体验 - 文件上传获取SHELL



企业主机安全病毒木马查杀体验 - 运行第三方恶意程序

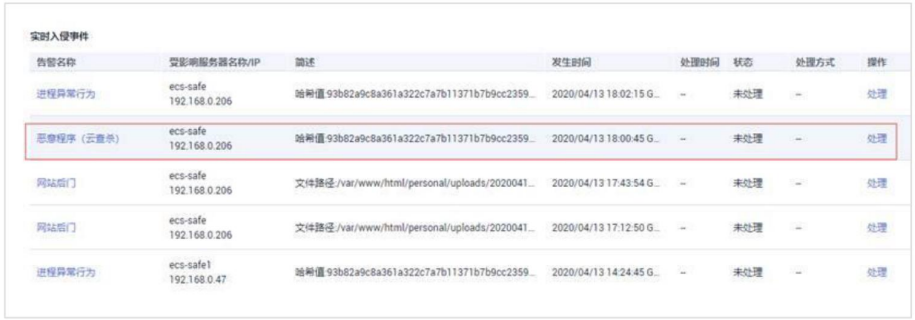


企业主机安全病毒木马查杀体验 - 恶意程序隔离查杀

top

```
top - 18:05:57 up  3:23,  2 users,  load average: 1.00, 0.67, 0.30
Tasks: 101 total,   1 running,  63 sleeping,   0 stopped,   1 zombie
%Cpu(s): 99.7 us,  0.3 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1008684 total,   290748 free,   356112 used,   361824 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   497760 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
13850 www-data  20   0  232168   3620   1592 S 99.7  0.4   5:20.26 aes
 2278 root      20   0  792076  19424  14920 S  0.3  1.9   0:17.60 hostguard
    1 root      20   0  225548   9316   6704 S  0.0  0.9   0:02.75 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    4 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kworker/0:0H
    6 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 mm_percpu_wq
    7 root      20   0       0      0      0 S  0.0  0.0   0:00.19 ksoftirqd/0
```




```
Tasks:  99 total,   1 running,  62 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  0.0 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1008684 total,   292296 free,   353096 used,   363292 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   500736 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 2278 root      20   0  792076  19464  14920 S  0.3  1.9   0:19.04 hostguard
    1 root      20   0  225548   9316   6704 S  0.0  0.9   0:02.78 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    4 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kworker/0:0H
    6 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 mm_percpu_wq
    7 root      20   0       0      0      0 S  0.0  0.0   0:00.21 ksoftirqd/0
    8 root      20   0       0      0      0 I  0.0  0.0   0:00.55 rcu_sched
    9 root      20   0       0      0      0 I  0.0  0.0   0:00.00 rcu_bh
   10 root      rt   0       0      0      0 S  0.0  0.0   0:00.00 migration/0
   11 root      rt   0       0      0      0 S  0.0  0.0   0:00.01 watchdog/0
```

本章总结

- 网络攻防是什么、步骤以及方式
- HSS、VSS、VPC等的使用
- 怎样通过靶场平台演练增强安全攻防意识

学习推荐

- 华为云官方网站
  - https://www.huaweicloud.com/
- 华为云帮助中心
  - https://support.huaweicloud.com/index.html
- 华为云学院
  - https://edu.huaweicloud.com/

HUAWEI

华为云学院

学以致用　云世界大有可为

Thank You.

华为云 +智能, 见未来

www.huaweicloud.com