在项目上，漏洞扫描需要注意那些事项

跟客户确认是否充许登录扫描、扫描并发连接数及线程数、

是否充许暴力破\*\*解，什么时间段\*\*扫描、

通知客户备份一下数据，开启业务系统及网站运维监控，以免断机可及时恢复。

谈谈IDS和IPS是什么？有什么作用？

入侵检测：IDS，类似防火墙，主要用于入网流量检测

入侵防御：IPS，对杀软和防火墙的补充，阻止病毒攻击以及点到点应用滥用

态势感知、soc产品的功能

全流量收集、大数据分析、

访问日志展示、攻击日志展示告警、资产管理、大屏展示、

脆弱性识别-弱口令-数据传输未加密-漏洞、

受害主机攻击汇总、内网横向攻击分析、

报表功能

Shiro（rememberme）

550：aes的密钥硬编码在程序中，可以爆破。

721：通过oracle的padding攻击方式爆破出密钥。

Weblogic

如果java应用没有对传入的序列化数据进行安全性检查，我们可以将恶意的TransformedMap序列化后，远程提交给Java应用，如果java应用可以触发变换，就可以成功进行远程命令执行。

反序列化会调用ObjectInputStream类的readObject()方法，如果被反序列化的类重写了readObject()，那么该类在进行反序列化时，java会优先调用重写的readObject()方法。如果某个可序列化的类重写了readObject()的方法，并且在readObject()中对Map类型的变量进行了键值修改操作，并且这个Map变量时可控的，就可以实现攻击链的调用。

Struct2

S2001:当用户提交表单数据并验证失败时，后端会将用户之前提交的参数值使用OGNL表达式%{value}进行解析，然后重新填充到对应的表单数据中。%{1+1}=2

S2005：struts2会将http的每个参数名解析为OGNL语句执行（可理解为java代码）。OGNL表达式通过#来访问struts对象，struts框架通过过滤#字符防止安全问题，然而通过unicode编码（\u0023）或8进制（\43）即绕过了安全限制。

S2007:传递一个非整数给id导致错误，struts2会将用户的输入当作ongl表达式执行，从而导致漏洞。当输入以str的形式提交int时，服务器"’" + value + "’"将对代码进行拼接，然后使用OGNL表达式对其进行解析。我们需要找到一个配置有相似验证规则的表单字段，以产生转换错误。然后，您可以通过注入SQL单引号的方式注入任何OGNL表达式代码。

Fastjson

使用AutoType功能进行序列号的JSON字符会带有一个@type来标记其字符的原始类型，在反序列化的时候会读取这个@type，来试图把JSON内容反序列化到对象，并且会调用这个库的setter或者getter方法，然而，@type的类有可能被恶意构造，只需要合理构造一个JSON，使用@type指定一个想要的攻击类库就可以实现攻击。

脏牛提权

linux内核的子系统在处理写入时复制至产生了竞争条件，恶意用户可利用此漏洞来获取高权限，对只读内存映射进行访问。写时复制的三个步骤不具有原子性，可以被其他线程中断，产生竞争。

Suid提权

SUID是Linux的一种权限机制，具有这种权限的文件会在其执行时，使调用者暂时获得该文件拥有者的权限。如果拥有SUID权限，那么就可以利用系统中的二进制文件和工具来进行root提权。

烂土豆提权

攻击者可以诱骗用户尝试使用NTLM对他的计算机进行身份验证（支持SeImpersonate或者SeAssignPrimaryToken权限、DCOM、支持RPC、能够找到可用的COM对象）

黄金票据：TGT伪造，可以拿着向TGS要ST，可以获取到任何一台电脑的ST。难点：krbtgt的hash

白银票据：ST伪造，，难点：server的hash

委派攻击：委托WEB系统访问文件系统，通过ST委托server访问域内其他主机

Sqlserver提权

Xp\_cmdshell:EXEC master.dbo.xp\_cmdshell 'whoami'

sp\_oacreate:

沙盒提权：启用Ad Hoc Distributed Queries，

执行添加一个管理员 margin 命令，

select \* from openrowset('microsoft.jet.oledb.4.0',';database=c:/windows/system32/ias/ias.mdb','select shell("net user margin margin /add")')

再提升权限。

select \* from openrowset('microsoft.jet.oledb.4.0',';database=c:/windows/system32/ias/ias.mdb','select shell("net localgroup administrators margin /add")')

Mysql提权

Udf提权：通过into dumpfile函数导入udf.dll进行提权。secure\_file\_priv肯定要设置为空的

启动项提权：中文路径就容易失败

EDR是什么？举例，作用？

终端检测与响应

360天擎、深信服EDR、亚信EDR

通过云端的威胁情报、机器学习、异常行为分析等，主动发现安全威胁，自动化阻止攻击。

随机检测网页是否被篡改

根据设备告警（WEB）如何分析流量

\1. 下载告警pcap数据包，根据告警提示攻击类型，过滤payload信息，定位流量

\2. 判断是否攻击成功，需具体分析攻击请求响应内容或使⽤其payload进⾏攻击测试等

\3. 最终可根据流量分析给出判定类型：扫描、攻击尝试、攻击成功、攻击失败

web中间件加固：tomcat、apache、iis有哪些加固点

web中间件：更改默认端口、低权限运维、降权网站根目录、自定义错误页面、删除自带网页

windows和linux加固？（操作系统加固）

windows：删除无用账号、禁用来宾账号、设置密码复杂度、关闭默认共享、关闭自启

linux：删除无用账号、配置密码策略（复杂度、过期时间）、限制su命令使用、限制ssh远程登陆root、减少命令记录数（.bash\_history）、升级内核版本

mysql加固呢？数据库加固

mysql：使用低权限用户配置网站、启用mysql日志记录、禁用文件导入导出

sql server：使用低权限用户配置网站、关闭xp—cmdshell功能

根据设备告警（内⽹）如何展开排查

定位主要扫描、攻击机器；根据业务情况，进⾏隔离处理；排查主要扫描、攻击机器正在执⾏进程、历史命令，定位攻击者扫描⼯具、扫描结果等；提取攻击者操作信息、攻击样本后，清理查杀攻击者后⻔、⼯具等；根据攻击者扫描结果，对存在的漏洞展开修补⼯作；分析主要扫描、攻击机器如何沦陷，溯源攻击链，展开攻击链修补⼯作

常见洞端口有哪些？

21（FTP）、873（Rsync）、1433（MSSQL）、1521（Oracle）、2181（Zookeeper）、3306（Mysql）、5432（PostgreSQL）、6379（redis）、7001（weblogic）、8161（ActiveMQ ）、9200（elasticsearch ）、27017（Mongodb）、50070，50050（Hadoop）

文件上传加固方法？

后端限制文件上传白名单，头像不允许上传 svg

上传后文件随机重命名，不要输出保存文件位置

图片文件可以二次渲染，使用对象存储 oss

文件目录取消执行权限，PHP 设置 basedir

JAVA内存马如何排查？

**使⽤⼯具进⾏检测查杀**

1、如果是jsp注入，日志中排查可疑jsp的访问请求。

2、如果是代码执行漏洞，排查中间件的error.log，查看是否有可疑的报错，判断注入时间和方法

3、根据业务使用的组件排查是否可能存在java代码执行漏洞以及是否存在过webshell，排查框架漏洞，反序列化漏洞。

4、如果是servlet或者spring的controller类型，根据上报的webshell的url查找日志（日志可能被关闭，不一定有），根据url最早访问时间确定被注入时间。

5、如果是filter或者listener类型，可能会有较多的404但是带有参数的请求，或者大量请求不同url但带有相同的参数，或者页面并不存在但返回200

php内存马如何排查？；使⽤⼯具进⾏检测查杀

php不死马也就是内存马

排查就两点；检测执行文件是否在文件系统真实存在；确认攻击后去重启服务消除内存执行

aspx内存马如何排查？；使⽤⼯具进⾏检测查杀

github有人写了一个排查的aspx脚本，放到网站目录下访问，会返回内存中filter（过滤器0列表，排查未知、可疑的就行

检测执行文件是否在文件系统真实存在；

**日志文件默认位置**

安全日志文件：%systemroot%\system32\config\SecEvent.EVT

系统日志文件：%systemroot%\system32\config\SysEvent.EVT

应用程序日志文件：%systemroot%\system32\config\AppEvent.EVT

Internet信息服务FTP日志默认位置：

%systemroot%\system32\logfiles\msftpsvc1\，默认每天一个日志

1. Internet信息服务WWW日志默认位置：

%systemroot%\system32\logfiles\w3svc1\，默认每天一个日志

Scheduler服务日志默认位置：%systemroot%\schedlgu.txt

Event Viewer/事件查看器

发现一条攻击告警如何判断是否为真实有效攻击事件思路？

分析请求、响应内容，判断是否攻击成功

首先看告警事件名称判断是网络攻击事件还是web攻击事件，

网络攻击事件：定位五元组信息（源IP、目的IP、源端口、目的端口、协议），对整个僵、木、蠕传播链进行分析，以攻击IP作为受害IP进行检索查找攻击源，

WEB攻击事件：通过数据包的请求体、响应体、状态码等。

如何区分扫描流量和手动攻击流量

扫描数据量大，请求有规律

手动攻击流量数据量较少，攻击流量大多和业务关联性较大

如何分析被代理出来的数据流

分析数据包请求头中的 xff、referer、UA 等收集有用的信息

基于网络欺骗与浏览器指纹的WEB攻击溯源

在攻击队变更攻击IP的情况下，如何在流量中找到该攻击者的所有攻击IP？

cookie、ua、session、被利用账号ID等用户特征

如何判断DNS和ICMP（隧道）信道？

dns流量的txt记录比例异常：正常的DNS网络流量中，TXT记录的比例可能只有1%-2%，如果时间窗口内，TXT或者A记录的比例激增，就可能存在异常。

同一来源的ICMP数据包量异常：一个正常的ping命令每秒最多发送两个数据包，而使用ICMP隧道则会在很短时间内产生上千个ICMP数据包，可以检测同一来源的ICMP数据包的数量。

误报怎么判断？比如xxx设备心跳存活过于频繁，误报成攻击。答：心跳检测是有规律的、持续的，与攻击流量区别较大

web日志格式？ip、时间、请求类型、请求url、响应状态、响应大小、UA头

常见的安全工具有哪些？

端口及漏洞扫描：Namp、Masscan；抓包：Wireshark，Burpsuite、Fiddler、HttpCanary；Web自动化安全扫描：Nessus、Awvs、Appscan、Xray；信息收集：Oneforall、hole；漏洞利用：MSF、CS；Webshell 管理：菜刀、蚁剑、冰蝎、哥斯拉

说说Nmap工具的使用？

-sT TCP (全)连接扫描，准确但留下大量日志记录

-sS TCP SYN (半)扫描，速度较快，不会留下日志

-sN null 扫描，标志位全为 0，不适用 Windows

-sF FIN 扫描，标志位 FIN=1，不适用 Windows

-O 查看目标主机系统版本

-sV 探测服务版本

-A 全面扫描

cs shellcode 特征

1、RWX（可读可写可执行）权限的内存空间

2、异或密钥固定，3.x 是 0x69，4.x 是 0x2e

3、命名管道名称字符串

\\.\pipe\MSSE-1676-server

%c%c%c%c%c%c%c%cMSSE-%d-sever

Log4j rce漏洞有了解过？攻击特征是什么？

log4j 是 javaweb 的日志组件，用来记录 web 日志，特征是${jndi:ldap://url}

去指定下载文件的 url 在搜索框或者搜索的 url 里面，加上 {jndi:ldap://127.0.0.1/test} ，log4j 会对这串代码进行表达式解析，给 lookup 传递一个恶意的参数指定，参数指的是比如 ldap 不存在的资源 是会被直接执行的。后面再去指定下载文件的 url，去下载我们的恶意文件。比如是 x.class 下载完成后，并且会执行代码块

修复：升级 Log4j 到最新版本，根据业务判断是否关闭 lookup

新出的office word msdt 漏洞原理？

从Word使用URL协议调用MSDT（微软支持诊断工具），可执行远程网页脚本内容，下载或运行任意命令、程序。

无论是否禁用宏，只要打开word就会中招，但无法正常查看doc内容

WENSHELL流量特征？

菜刀：

1、webshell 为一句话木马

2、ua 头为百度爬虫

3、请求体中存在 eavl，base64

4、响应为明文，格式为 X@Y +内容 + X@Y

蚁剑：

1、webshell 同样有 eval，base64

2、ua 头为蚁剑工具

3、请求体中存在 @ini\_set

4、响应为明文，格式为 随机数+结果 +随机数

冰蝎：

1、webshell 同样有 eavl，base64

2、webshell 中有 md5(密码)前16位

3、2.0 有一次GET请求返回16位的密钥

哥斯拉：

1、webshell 同样有 eavl，base64

2、cookie以分号结尾

3、请求为pass=

常见的未授权访问漏洞有哪些？

Active MQ、Docker、FTP、JBoss、Jupyte、LDAP、MongoDB、Redis、Solr、Spring Boot Actuator、Weblogic 未授权访问

20220day安恒数据大脑 API 网关任意密码重置、360 天擎任意文件上传、万户 OA 文件上传、泛微 OA 文件上传

获得文件读取漏洞，通常会读哪些文件

1、linux

etc/passwd、etc/shadow直接读密码

/etc/hosts # 主机信息

/root/.bashrc # 环境变量

/root/.bash\_history # 还有root外的其他用户

/root/.viminfo # vim 信息

/root/.ssh/id\_rsa # 拿私钥直接ssh

/proc/xxxx/cmdline # 进程状态枚举 xxxx 可以为0000-9999 使用burpsuite

数据库 config 文件

web 日志 access.log, error.log

ssh 日志

bash /root/.ssh/id\_rsa /root/.ssh/id\_rsa.pub /root/.ssh/authorized\_keys /etc/ssh/sshd\_config /var/log/secure /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/syscomfig/network-scripts/ifcfg-eth1

2、windows

C:\boot.ini //查看系统版本

C:\Windows\System32\inetsrv\MetaBase.xml //IIS 配置文件

C:\Windows\repair\sam //存储系统初次安装的密码

C:\Program Files\mysql\my.ini //Mysql 配置

C:\Program Files\mysql\data\mysql\user.MY D //Mysql root

C:\Windows\php.ini //php 配置信息

C:\Windows\my.ini //Mysql 配置信息

主机发生安全事件处置流程

抑制范围：主机断网或者隔离使受害⾯不继续扩⼤；收集信息：收集客户信息和中毒主机信息，包括样本

3、判断类型：判断是否是安全事件，何种安全事件，勒索、挖矿、断网、DoS 等等

4、深入分析：日志分析、进程分析、启动项分析、样本分析方便后期溯源

5、清理处置：杀掉进程，删除文件，打补丁，删除异常系统服务，清除后门账号防止事件扩大，处理完毕后恢复生产

6、产出报告：整理并输出完整的安全事件报告

在Windows靶标站点如何建立隐藏用户？

net user xiaofeng 112233 /add (建立隐藏用户xiaofeng）net localgroup administrators xiaofeng /add （将隐藏用户xiaofeng加入管理员用户组）

Windows被创建影子用户怎么办?

1、可以通过控制面板管理账户查看

2、注册表中查看是否存在影子账户：

（HEKY\_LOCAL\_MACHINE\SAM\SAM\Domains\Account\User）

windows端口进程间怎么关联查找

netstat -ano | findstr “port”查看目前的网络连接，定位可疑的 ESTABLISHED

根据netstat定位出的 pid，再通过tasklist命令进行进程定位tasklist | findstr “PID”

windows怎么查看进程对应的程序位置

任务管理器--选择对应进程--右键打开文件位置运行输入 wmic，cmd界面 输入 process

查看 Windows 服务所对应的端口

%system%/system32/drivers/etc/services（一般 %system% 就是 C:\Windows）

查看windows进程的方法

开始 -- 运行 -- 输入msinfo32 命令，依次点击 "软件环境 -- 正在运行任务" 就可以查看到进程的详细信息，比如进程路径、进程ID、文件创建日期以及启动时间等

打开D盾\_web查杀工具，进程查看，关注没有签名信息的进程

通过微软官方提供的 Process Explorer 等工具进行排查

查看可疑的进程及其子进程。可以通过观察以下内容：

没有签名验证信息的进程

没有描述信息的进程

进程的属主

进程的路径是否合法

CPU 或内存资源占用长时间过高的进程

Windows日志存放位置？

大致是System32的Logs目录下

系统日志：%SystemRoot%\System32\Winevt\Logs\System.evtx

应用程序日志：%SystemRoot%\System32\Winevt\Logs\Application.evtx

安全日志：%SystemRoot%\System32\Winevt\Logs\Security.evtx

windows日志分析工具有哪些

Log Parser、LogParser Lizard、Event Log Explorer、360星图

遇到日志文件量大的时候怎么去分析？

通过正则去匹配日志中的攻击请求

借助腾讯日志分析工具：LogForensics

讲一下Linux机器被攻陷排查思路？

账号排查（/etc/passwd存储用户信息、/etc/shadow存储用户密码信息）

历史命令查看：.bash\_history；检查异常进程：ps aux | grep pid；检查开机启动项：/etc/rc.local；查看定时任务：crontab -l

检查网站目录可疑文件：

Find /var/www/html -name "\*.php" |xargs egrep 'assert|eval|phpinfo()|(base64\_decoolcode|shell\_exec|passthru|file\_put\_contents(.\*$|base64\_decode('

Linux日志存放位置？

日志默认存放位置：/var/log/

查看日志配置情况：more /etc/rsyslog.conf

一台主机在内网进行横向攻击，怎么处理？

确定攻击来源，是不是员工内部误操作，比如询问运维是否有自动化轮训脚本

如果没有，确定是攻击，结合时间点，根据设备信息，看一下安全事件，进程，流量

找到问题主机，开始应急响应流程：准备、检测、遏制、根除、恢复、跟踪，具体的操作要交给现场运维去处理

HW期间发现在野0day利用怎么处置？

首先确认0day影响产品，危害程度；下线应用；排查应用日志查找是否有攻击请求；更新官方发布的最新补丁或者升级版本

如何发现钓鱼邮件

邮件系统异常登录告警、员工上报、异常行为告警、邮件蜜饵告警

推荐接入微步或奇安信的情报数据。

对邮件内容出现的 URL 做扫描，可以发现大量的异常链接

遇到钓鱼邮件如何处置？

1、第一时间隔离被钓鱼的主机

2、\*\*通过第三方联系方式对攻击进行预警，防止其他员工再次上钩\*\*

3、对钓鱼邮件中的样本进行取样，分析溯源

4、HW前期针对安全意识进行培训

说说钓鱼邮件处置实际操作

屏蔽办公区域对钓鱼邮件内容涉及站点、URL 访问

根据办公环境实际情况可以在上网行为管理、路由器、交换机上进行屏蔽

邮件内容涉及域名、IP 均都应该进行屏蔽

对访问钓鱼网站的内网 IP 进行记录，以便后续排查溯源可能的后果

屏蔽钓鱼邮件；屏蔽钓鱼邮件来源邮箱域名；屏蔽钓鱼邮件来源 IP；有条件的可以根据邮件内容进行屏蔽

删除还在邮件服务器未被客户端收取钓鱼邮件；处理接收到钓鱼邮件的用户；根据钓鱼邮件发件人进行日志回溯

此处除了需要排查有多少人接收到钓鱼邮件之外，还需要排查是否公司通讯录泄露。

通知已接收钓鱼邮件的用户进行处理

删除钓鱼邮件；系统改密；全盘扫毒

后续：溯源、员工培训提升安全意识

溯源反制手段有哪些？

根据流量溯源反制：筛选攻击IP、域名，扫描端⼝服务，或通过威胁情报分析，对攻击者VPS进⾏溯源分析

蜜罐平台反制：模拟SSL VPN等平台，诱导攻击者下载应⽤软件及安装使⽤，上线攻击者主机

钓⻥反制：根据蜜罐捕获信息，通过社交软件平台、⼿机短信、邮件等⽅式进⾏钓⻥

说一下你的溯源思路？

蜜罐是怎么获取攻击者社交账号信息的？怎么防

浏览器信息读取

利用jsonp，跨域访问社交平台接口，提取包含的个人信息

使用浏览器隐私模式，或虚拟机内实施攻击操作

常见溯源方法（溯源思路）有哪些？

1、通过恶意样本文件特征进行溯源渠道（github、网盘、博客、论坛等等）

2、域名、IP反查目标个人信息

3、微信、支付宝、淘宝等平台查找姓氏

4、蜜罐：浏览器指纹技术、网络欺骗技术

对攻击者进行身份画像有哪些？

虚拟身份：ID、昵称、网名

真实身份：姓名、物理位置

联系方式：手机号、qq/微信、邮箱

组织情况：单位名称、职位信息

HW期间没发现有效攻击事件如何得分？

可以通过对非法攻击溯源反制得分

可以通过提交灰黑产线索进行得分

获取到钓鱼邮件exe如何分析？

看创建日期，看备注信息

ida看调试信息，可能有个人id、网名

上传查杀、威胁检测平台，分析行为特征，获取内部url、ip地址等

各大威胁平台结果判断木马生成时间，是否已知

溯源收集目标邮箱对有什么用？

搜索引擎，查论坛，查博客，推测职业

社工库、第三方直接查个人信息

通过手机号后怎么获取攻击者信息？

各大社交平台

百度、谷歌搜索

各种app，如csdn、支付宝、钉钉、脉脉等，qq、微信好友

通过域名、ip怎么确认攻击者身份？

云平台域名、ip找回账号方式，获取手机号部分信息

搜索引擎查ip现有服务，历史服务，有无攻击特征

威胁情报、沙箱获取信息

百度贴吧、个人博客、技术论坛、网站备案等

通过哪些工具、网站获取攻击者信息？

自行总结

微步情报查询、埃文科技网站定位ip地址等