0x01渗透测试流程

信息收集（IP、子域名、C段、旁站、框架、服务器系统、语言、目录结构、数据库类型、端口、注册人员信息、防护设备）- 漏洞发现（网站功能点测试（上传、越权、目录遍历、注入、XSS、CSRF）、漏扫（Nessus、AWVS）、系统漏洞）- 验证漏洞（Kali、exp、）-出具报告交付-漏洞复测

0x02信息收集都收集什么内容

信息收集（IP、子域名、C段、旁站、框架、服务器系统、语言、目录结构、数据库类型、端口、注册人员信息、防护设备）

0x03收集端口有什么用，常见高危端口

端口的收集可以为进一步的找到对方系统漏洞给出更多的路径，如果找到一些常见的漏洞直接使用exp进行攻击的话甚至能直接获取对方服务器权限

21 ftp、22 ssh、23 Telnet、80/8080/8888、1080 socks、3389 RDP、7001 Weblogic

1521 Oracle、1433 MSSQL、3306 MySQL、5432 PostgreSQL、6379 Redis

139 445 SMB NetBIOS 建立IPC$文件共享

0x04 Sql注入、xss、csrf、文件上传、ssrf漏洞原理（少部分细节，比如SQL盲注、报错注入怎么注）

Mysql报错函数（floor(rand())、updatexml、extractvalue）

Mysql盲注函数Sleep、ascii、mid

写shell函数 dumpfile，ouyfile等

ssrf特征分析 可以看请求包内⼀些绕过姿势 0x01 ⼀些特殊符号 @ [::] 。 0x02 看协议dict gopher file 0x03 短连接 localhost 0x04 ip进制绕过

0x04工具使用（burp、sqlmap等）

Burp模块（Poxy、Intruder、Repeater、Decoder）

Sqlmap（-level 3/5、-r 文件、-u url、--method 提交方式、-cookie 自定义cookie、-tamper 混淆器）

0x07熟悉的中间件及常见漏洞

IIS解析漏洞、RCE / Apache解析漏洞、目录遍历 / Nginx解析漏洞、目录遍历、目录穿越

Shiro、fastjson、weblogic等漏洞（根据6所说的问）

漏洞流量特征 怎么判断漏洞是否攻击成功（如shiro、sql注入等）

Structs2漏洞

016是post数据用defaultactionmapper类的redirecration方法当做ONGL表达式，可以当做代码执行，造成远程代码执行漏洞

045漏洞成因主要是接受contenttype值的时候会对其进行ONGL表达式解析，造成远程代码执行

特征是使用OGNL语法，payload中含有memberaccess字段，相关特征应该在catalina.out日志文件中有体现

fastjson攻击流量

漏洞主要是因为autotype功能，这个功能本身是用于fastjson对JSON字符进行序列化和返序列化的，然后使用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，只需要构造一个JSON字符，使用@type指定一个想要的攻击类库就可以实现攻击

常见的有sun官方提供的一个类，其中有个datasourcename方法支持传入一个rmi的源，只要解析其中的url就会支持远程调用

log4j2的原理及特征

原理:log4j2框架下的lookup服务提供了{}字段解析功能，传进去的值会被直接解析，JNDI服务会请求远程服务来链接本地对象，这时候只用在｛}里面调用JNDI服务即可反弹shell到指定服务器

特征:数据包里有{jndi:ladp//}字段

weblogic

xml反序列化漏洞，wls组件对外提供webserver服务，通过xmldecoder去解析xml导致一个远程代码执行

特征是xml格式的数据到wls，数据内容可能包含bash或者dnslog之类的 开放7001端口

/console控制台弱口令上传部署一个war包，特征是在adminsever.log文件中会有deploy war的字段

原理：

从⽇志查看(⽇志存放位置：/domains/当前域⽬录/servers/AdminServer/logs)

● 弱⼝令利⽤上传war的特征：分析AdminServer.log⽇志查找deploy war字样

● 利⽤T3协议传输反序列化数据特征：AdminServer.log⽇志中，⼀般利⽤的cc链(commoncollections)，因此⽇志⽂件可能有InvokerTransformer、ChainedTransformer等

● 利⽤socket连接特征：base\_domain.log或AdminServer.log⽇志中，会有socket字样

● ⽂件操作：base\_domain.log中会有FileOutputStream字样

T3 cc链的利用，T3协议加上java反序列化，特征adminserver.log中有invoketransformer和chainedtransformer字段，T3CC利用原理好像是weblogic调用rmi服务传递对象时对参数没过滤完全，而中间T3协议对传递的字符串只能增加黑名单

socket登录就会有socket字段

文件操作的话会有fileoutputname字段

特征:数据内包含t3字段，类似：t3 12.2.1\nAS:255\nHL:19\nMS:10000000\nPU:t3://us-lbreens:7001\n\

shiro 550 721区别

漏洞成因是因为有一个remeberme的方法，它可以对cookie进行加密后存储，下次访问就不需要登录了，生成方法是对cookie先进行序列化，aes加密，base64加密

550就是aes它是使用固定的key进行加密，所以就可以直接构造cookie利用

721的话是使用aes128cbc加密，可以不固定，可以使用padding oracle attack的工具进行利用，好像还需要提供一个有效的cookie，以及需要明确对方的操作系统

0x08 应急流程

首先收集客户机器信息以及样本，做好文件备份

然后判断安全事件的类型，是系统层面的，如挖矿病毒、后门木马，还是网络应用层面的，如webshell，或者是网络层面，如断网、DDOS等，之后隔离机器

日志、用户、进程、启动项、样本，看到可疑的就杀掉，删文件，打补丁，溯源

最后产出一份安全事件报告

0x09 Linux排查常见命令

Linux ps -aux 查看进程 netstat -antlp 查看端⼝ top查看 cpu使⽤情况

Windows tasklist 查看进程 netstat -an 查看端⼝

0x10 Linux怎么看ssh登录日志

/var/log/secure

/var/log/utmp

/var/log/wtmp

/var/log/lastlog

0x11 Linux查看定时任务 怎么删除定时任务

Crontab -l / /var/spool/cron/ 查看

/etc/cron 这个目录下面一堆

Crontab -r / Crontab -e 删除整个/编辑文件一条一条删

0x12 Windows查看rdp登录日志 登陆成功的事件id

eventvwr.exe事件查看器/windows/system32/winevt/Logs

登录成功事件ID4624

登录失败事件ID4625

0x13 Windows查找隐藏用户

lusrmgr.msc(本地用户和组)查看账号信息，排查是否含有新增账户，检查注册表判断是否存在隐藏账户、克隆账号等

防御：在正式的对抗之前备份注册表中

HKEY\_LOCAL\_MACHINE/SAM/SAM/Domain/Account/Group的键值，再将其删除，这样服务器就不再允许创建其他账号或者删除账号，可以有效防范影子账户的创建，在需要创建用户或者删除用户的时候，在导入该键值

HKEY\_LOCAL\_MACHINE\SAM\SAM\Domains\Account\Users\Names

0x14 项目经验，有没有参加过hw，负责什么岗位，工作内容是啥，结合工作内容问一点

之前是在xx单位驻场（安服/渗透），主要负责单位的APP、内部系统、公网系统版本更新前的安全测试任务，工作内容主要就是开发更新了功能点或者什么其他的新地方，提交了一个安全测试到内部平台上，然后小组长分发任务，在版本更新日期前做完安全测试并且提交漏洞定级，并且跟踪复测漏洞，出具安全测试报告，来不及修的就让开发延期，定期会有内部的攻防演练，之前是请奇安信的红队来对抗

有过hw经验，在监控组，主要负责看安全设备，也做一部分研判工作，看SIP态势感知、WAF、IPS/IDS，微步查一下恶意IP，封堵IP，配点进出网规则。

0x15结合安全设备问一下策略或使用方面的问题 熟悉哪些设备

天融信的IDS，深信服的IPS，深信服的SIP

策略个锤子，很少开放新的策略，除非是客户这边让设置一个策略啥的

0x16 漏洞流量特征 怎么判断漏洞是否攻击成功（如shiro、sql注入等）

请求包响应包 拉流量出来分析 看他的数据包有哪些漏洞攻击的特征 看看响应包的状态及响应体