# 网络攻击与防御

1. 信息安全三原则：

文本

描述已自动生成

1. 在安全漏洞生命周期中，从安全漏洞被发现到厂商发布补丁程序用于修补该漏洞之前的这段时间，被安全社区普遍地称为0day。
2. 国际标准化组织ISO对信息安全定义的建议是：为数据处理系统建立和采取的技术和管理的安全保护。保护计算机的硬件、软件和数据不因偶然的或恶意的原因而受到破坏、更改、泄漏。
3. APT是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。
4. EXP（或Exploit）是一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码，可以使得读者完全了解漏洞的机理以及利用的方法。
5. CVE编号是业界标识该漏洞的标准索引号。
6. 在使用Google搜索时，\*符号用于模糊匹配某些内容。当利用google进行搜索想要只搜某网站的内容时，可以使用site关键字。
7. 国家代码域名支持组织CNNSO：负责国家顶级域名分配，包括.us、.cn、.jp等。
8. 可以使用Whois查询特定域名的详细注册信息。
9. 网络扫描类型及目的:

手机屏幕截图

描述已自动生成

1. TCP/IP三次握手协议过程。
2. 图示

   描述已自动生成
3. TCP ACK Ping主机扫描。

文本

描述已自动生成

1. DHCP协议过程分析：

图形用户界面

低可信度描述已自动生成

No106：本机localhost（10.133.81.229）向DHCP server（10.133.0.1）发送了一个DHCP Release数据包，终止了ip租赁。将本机IP地址清空。

No267：本机localhost向局域网广播一个DHCP Discover包，此时本机localhost的IP地址为0.0.0.0。广播地址为255.255.255.255。本地端口为68，目的端口为67。

No277：Ipv4地址为10.133.0.1的DHCP服务器收到该包后，向本机发送一个DHCP Offer数据包。

No278：DHCP Request包由本机localhost广播，表示本机已经收到DHCP Offer包，对此事进行通告，通告的内容包括预分配给本机的IP地址，本机的MAC地址，本机的计算机名等信息。

No279：DHCP server（10.133.0.1）向本机localhost（10.133.81.229）发送了一个DHCP Ack数据包。确认IP地址，路由、DNS、IP租赁时间、子网掩码等信息。

1. Tracert命令使用IP 生存时间 (TTL)和ICMP 错误消息来确定从一个主机到网络上其他主机的路由。
2. 域名信息探测命令dig有交互式和非交互式两种模式。使用Dig命令查询邮件服务器时所使用的querytype选项是MX。域名信息探测命令：dig @dnsserver name querytype，其中参数querytype有A、AAAA、PTR、MX和ANY五种类型。
3. 用户代理(User-Agent)头字段确定用户使用的Web浏览器。
4. 端口扫描是一种用来确定目标主机TCP端口和UDP端口状态的方法。开放某个端口，意味着提供某种网络服务。
5. Nessus是一款综合型漏洞扫描工具。
6. TCP/UDP 均定义了1-65535端口范围，由ICANN负责分配。MySQL数据库默认的端口号是3306。MSSQL SERVER的默认端口号是1433。SSH的默认端口号是22。phpstudy默认的端口号为80。HTTP服务，默认的端口号为80。
7. Http状态码为404表明无法找到指定位置的资源。
8. SQL语言规定，将单引号解析成代码与数据之间的分界线。
9. MySQL数据库中的注释符有3种，分别是#、/\*\*/、-- 。
10. floor（rand（）\*2）函数返回值为0或者1。
11. UNION 操作符的作用：UNION 操作符用于合并两个或多个 SELECT 语句的结果集。
12. UNION使用要求：UNION 内部的 SELECT 语句必须拥有相同数量的列。列也必须拥有相似的数据类型。同时，每条 SELECT 语句中的列的顺序必须相同。
13. 常用数据库带有很多默认的用户预安装内容，如SQL Server使用sa作为默认的数据库系统管理员账户。
14. 为了安全起见，应保证程序的数据库访问在最低权限模型下运行。
15. SQL的时间延迟漏洞的识别。
16. 利用时间延迟进行数据库长度的猜测：攻击者可以构造and if(length(database())=100,sleep(1),1)# 语句来猜测数据库名的长度是否为100，如果检测到服务器响应时间延迟了1秒钟，则表明猜测正确，否则修改数字4为其他数字，依次猜测。
17. SQL漏洞的防范：
18. 应该使用参数化语句（也称为预处理语句，PHP中使用PDO）而非动态SQL来组装SQL查询。
19. 使用白名单对输入内容进行验证，确保验证应用收到的所有用户控制的输入类型、大小、范围和内容。
20. 确保对包含用户可控制输入的查询进行正确编码，以防止使用单引号或其他字符来修改查询。
21. XSS是一种经常出现在Web应用程序中的计算机安全漏洞，是由于Web应用程序对用户的输入过滤不足而产生的。XSS跨站脚本攻击本身对Web服务器没有直接危害，它借助网站进行传播，使网站的大量用户受到攻击。XSS攻击可分为反射型、存储型和基于Dom的。
22. javaScript用于设置Cookie的函数是setCookie。
23. Cookie，有时也用其复数形式Cookies，指某些网站为了辨别用户身份、进行session跟踪而存储在用户本地终端上的数据（通常经过加密）,它是用户和服务器之间的桥梁。
24. 同源策略，它是由Netscape提出的一个著名的安全策略。所谓同源是指：域名、协议、端口相同。
25. 文本

    描述已自动生成
26. 文本

    描述已自动生成
27. 文本

    描述已自动生成
28. CSRF攻击示例（只针对课件示例，请具体问题具体分析进行使用）：

图形用户界面, 文本

描述已自动生成

1. CSRF攻击代码示例（只针对课件示例，请具体问题具体分析进行使用）：

文本

描述已自动生成

1. 防范CSRF攻击的措施。

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

1. 上传漏洞的识别及绕过。

文本

描述已自动生成

1. MIME检测过滤的绕过：burpsuite抓包，修改content-type的值为白名单中的类型。
2. 暴力破解是一种针对密码或身份认证的破解方法，穷举各种可能，找到突破身份认证的一种攻击方法。Burpsuite 进行暴力破解时，需要把抓取到的包发送到Intruder功能页面。
3. 暴力破解的防御措施：

文本, 信件

描述已自动生成