网络安全专业名词解释

原创

晶晶娃在战斗 已于 2022-03-04 16:04:23 修改 6975 收藏 6

分类专栏： 学习杂记 文章标签： 安全 网络安全 名词解释

于 2022-03-04 16:03:50 首次发布

本文链接：https://blog.csdn.net/qq_40909772/article/details/123279019

学习杂记 专栏收录该内容

14 篇文章 2 订阅

订阅专栏

1. Burp Suite 是一款信息安全从业人员必备的集成型的渗透测试工具，它采用自动测试和半自动测试的方式，通过拦截HTTP/HTTPS的Web数据包，充当浏览器和相关应用程序的中间人，进行拦截、修改、重放数据包进行测试，是Web安全人员的一把必备的瑞士军刀。
2. Bypass就是绕过的意思，渗透测试人员通过特殊语句的构建或者做混淆等进行渗透测试，然后达到绕过WAF的手法。
3. C2全称为Command and Control，命令与控制，常见于APT攻击场景中。作动词解释时理解为恶意软件与攻击者进行交互，作名词解释时理解为攻击者的“基础设施”。
4. CC攻击的原理是通过代理服务器或者大量肉鸡模拟多个用户访问目标网站的动态页面，制造大量的后台数据库查询动作，消耗目标CPU资源，造成拒绝服务。CC不想DDoS可以用硬件防火墙来过滤攻击，CC攻击本身的请求就是正常的请求。
5. CDN，全称“Content Delivery Network”内容分发网络，它能提高用户访问网站的速度，从而提高用户的体验度。它还有一定程度上防DDoS攻击，还能隐藏服务器的真实IP。
6. CISP(Certified Information Security Professional）即注册信息安全专业人员，是经中国信息安全产品测评认证1中心实施的国家认证，对信息安全人员执业资质的认可。该证书是面向信息安全企业、信息安全咨询服务机构、信息安全评测机构等负责信息系统建设、运行维护和管理工作的信息安全专业人员所颁发的专业资质的证书。
7. CISSP(Certification for Information System Security Professional）即信息系统安全专业认证，CISSP认证项目面向从事商业环境安全体系建设、设计、管理或控制的专业人员的技术及知识积累进行测试。
8. CMD一般指命令提示符是在操作系统中，提示进行命令输入的一种工作提示1符。在不同的操作系统环境下，命令提示符各不相同。
9. CMS一般指内容管理系统。CMS是Content Management System的缩写，意为“内容管理系统”，内容管理系统是企业信息化建设和电子政务的新宠，也是一个相对较新的市场。
10. CMS指纹识别，CMS（Content Management System）网站内容管理系统；CMS 是被原理就是得到一些CMS的一些固有特征，通过得到这个特征来判断CMS的类别。
11. CNNVD(China National Vulnerability Database of Information Security）即中国国家信息安全漏洞库，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为我国信息安全保障提供基础服务。
12. CNVD(China National Vulnerability Database）即国家信息安全漏洞共享平台，是由国家计算机网络应急技术处理1协调中

12. CNVD（China National Vulnerability Database）平台是信息安全漏洞共享平台，是由国家计算机网络应急技术处理协调中心（中文简称国家互联应急中心，英文简称CNCERT）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库。
13. Cobalt Strike是用于红队攻击的常见工具，该工具提供了代理服务器、Malleable C2、加密隧道、内置载荷等一系列功能，是红队人员居家必备良品，强大的插件功能使得攻击者可开发自定义功能配合使用。
14. Commando VM是火眼推出的基于Windows平台的渗透测试平台，推出一系列标准化工具套件，包含超过140个开源Windows渗透工具，红队渗透测试和蓝队防御人员均拥有顶级侦查与漏洞利用程序集。
15. Firefox插件，除了用来查看、编辑、创建或插入Cookies，还能看到更多关于Cookies的信息，允许同时修改或备份多个Cookies。
16. CRLF是“回车 + 换行”(\r\n）的简称。在HTTP协议中，HTTP Header与HTTP body是用两个CRLF分隔的，一旦我们能够控制HTTP消息头中的字符，注入一些恶意的换行，这样我们就能注入一些会话Cookies或者HTML代码。
17. 跨站请求伪造（Cross-site request forgery)，通常缩写为CSRF或者XSRF，是一种要挟制用户在当前已登录的Web应用程序上执行非本意的操作的攻击方法。跟跨网站脚本（XSS）相比，XSS利用的是用户对指定网站的信任，CSRF利用的是网站对用户网页浏览器的信任。
18. CVE的全拼是Common Vulnerabilities and Exposures，意思是通用漏洞披露，用来表示一种漏洞的特定编号。CVE就好像是一个字典表，为广泛认同的信息安全漏洞或者已经暴露出来的弱点给出一个公共的名称。
19. CVSS全称是（Common Vulnerability Scoring System）即通用漏洞评分系统。CVSS是一个行业公开标准，其被设计用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度。
20. C段入侵，同网段不同服务器的渗透方案，可能某公司在外网C段中拥有多个IP地址，但是内网却相连着，主目标不存在漏洞通过C段中其他存在漏洞的机器进入内网。
21. 分布式拒绝服务攻击（DDoS:Distributed denial of service）攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。
22. DEFCON（也写作DEF CON，Defcon，or DC）是全球最大的计算机安全会议之一，DEFCON的与会者主要有计算机安全领域的专家、安全研究员、黑客等对安全领域有兴趣的成员，涉及的领域主要有软件安全、计算机架构、无线电窃听、硬件修改和其他容易受到攻击的信息领域。
23. DNS Log，DNS在解析的时候会留下日志，这类工具就是读取多级域名的解析日志，来获取信息，简单来说就是把信息放在多级子域名中，传递到我们自己的服务器中，然后读取日志，获取特定信息，最后根据获取的信息来判断我们渗透测试的动作是否成功运行。
24. DNS域传送漏洞，DNS协议支持使用AXFR类型的记录进行区域传送，用来解决主从同步问题，如果管理员在配置DNS服务器的时候没有限制允许获取记录的来源，将会导致DNS域传送漏洞。
25. Dom型XSS，客户端的脚本程序可以动态地检查和修改页面内容，而不依赖于服务器的数据。例如客户端如从URL中提取数据并在本地执行，如果用户在客户端输入的数据包含了恶意的JavaScript脚本，而这些脚本没有经过适当的过滤，那么应用程序就可能受到DOM-based XSS攻击。
26. DOS命令，计算机术语，是指DOS操作系统的命令，是一种面向磁盘的操作命令，主要包括目录操作类命令、磁盘操作类命令、文件操作类命令和其他命令。
27. 深度包检测技术（即DPI）是一种基于应用层的流量检测和控制技术，当IP数据包、TCP或UDP数据流通过基于DPI技术的带宽管理系统时，通过深入读取IP包载荷的内容来对OSI七层协议中的应用层信息进行重组，得到整个应用程序的内容，按照系统定义的管理策略对流量进行整形操作。
28. 终端防护响应（EDR）工具，运用大数据，为终端抵御未知和零日攻击，应用机器学习和行为分析进行EDR防护。以大数据分析切入EDR（终端防护与响应），应用机器学习算法与行为分析提供精确、全面、实时的防护与响应，能够有效发现未知威胁并减少误报。
29. EL表达式注入漏洞和SpEL、OGNL等表达式注入漏洞是一样的漏洞原理的，即表达式外部可控导致攻击者注入恶意表达式实现任意代码执行。一般的，EL表达式注入漏洞的外部可控点入口都是在Java程序代码中，即Java程序中的EL表达式内容全部或部分是从外部获取的。
30. BetterCap是一个功能强大、模块化、轻便的MiTM框架，可以用来对网络开展各种类型的中间人攻击（Man-In-The-Middle），它也可以帮你实时地操作HTTP和HTTPS流量。BetterCap具有对多主机进行欺骗的能力，包括ARP欺骗

Middle人，它也可以帮你实时地操作HTTP和HTTPS流量，BetterCap具有对多主机进行欺骗的能力，包括：ARP欺骗、DNS欺骗以及ICMP双向欺骗。

31. Ettercap是一个基于ARP地址欺骗方式的网络嗅探工具，主要使用于交换局域网络。借助Ettercap攻击者可以检测网络内铭文数据通讯的安全性，及时采取措施，避免敏感数据以明文形式传输。
32. Exp，全称“Exploit”，中文译作利用，可以理解为具体的漏洞的利用，通常是一个漏洞利用的代码，EXP是存在风险的，指利用系统漏洞进行攻击的动作。
33. Exploit-DB是一个面向全世界黑客的漏洞提交平台，该平台会公布最新漏洞的相关情况，这些可以帮助企业改善公司的安全状况，同时也以帮助安全研究员和渗透测试工程师更好的进行安全测试工作。
34. Firefox插件，Firebug是一个好的插件，它集成了Web开发工具。使用这个工具，你可以编辑和调试页面上的HTML，CSS和JavaScript，然后查看任何的更改所带来的影响。它能够帮助我们分析JS文件来发现XSS缺陷。用来发现基于DOM的XSS缺陷，Firebug是相当有用的。
35. Frida是一款轻量级HOOK框架，适用于开发人员，逆向工程人员和安全研究人员的动态仪表工具包。可监听加密API或跟踪私有应用程序代码。
36. FRP是一个高性能的反向代理工具，可以进行内网穿透，对外网提供服务，支持TCP、HTTP、HTTPS等协类型，并且Web服务支持根据域名进行路由转发。
37. Fuzz Seanner，一个主要用于信息搜集的工具集，主要用于对网站子域名、开放端口、端口指纹、C端地址、敏感目录等信息进行批量搜集。
38. Ghidra是由美国国家安全局（NSA）研究部门开发的逆向工程（SRE）套件，是一个软件逆向工程（SRE）框架，包括一套功能齐全的高端软件分析工具，使用户能够在各种平台上分析编译后的代码。功能包括反汇编，汇编，反编译，绘图和脚本，以及数百个其他功能。
39. git信息泄露，当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当，可能会将.git文件夹直接部署到线上环境。这就引起了git泄露漏洞。
40. Goby是基于网络空间映射技术的下一代网络安全工具。它通过为目标网络建立全面的资产库来生成对网络安全事件和漏洞的紧急响应。
41. Google hack 是指使用Google等搜集引擎对某些特定的网络主机漏洞（通常是服务器上的脚本漏洞）进行搜索，已达到快速找到漏洞主机或特定主机的漏洞的目的。
42. GnuPG(GNU Privacy Guard，GPC）是一种加密软件，它是PGP加密软件的满足GPL协议的替代物。GnuPG是用于加密、数字签章及产生非对称匙对的软件。GPG兼容PGP（Pretty Good Privacy）的功能。
43. Firefox插件，主要用于安全审计，例如XSS，SQL的编码/解码，MD5，SH1，Base64，Hexing，Splitting等。
44. 钩子（Hook），是Windows消息处理机制的一个平台，应用程序可以在上面设置程序已监视指定窗口的某种消息，而且所监听的窗口可以是其他进程所创建的。当消息到达后，在目标窗口处理函数之前处理它。钩子机制允许应用程序截获粗粒Windows消息或特定事件。
45. HSTS，HTTP严格传输安全协议，全称：HTTP Strict Transport Security，是一套由互联网工程任务组发布的互联网安全策略机制。网站可以选择使用HSTS策略，让浏览器强制使用HTTPS与网站进行通信，以减少会话劫持风险。
46. HTTP Fox，Firefox插件，用来监测和分析浏览器与Web Server之间的所有HTTP流量。
47. HTTP参数污染，也叫HPP（HTTP Parameter Pollution）。简单地讲就是给一个参数赋上两个或两个以上的值，由于现行的HTTP标准没有提及在遇到多个输入值给相同的参数赋值时应该怎样处理，而且不同的网站后端作出的处理方式是不同的，从而造成解析错误。
48. HTTP报文即数据包，在OSI模型中，网络层及其以上层级，传输的数据单元均为包，即报文。数据链路层传输单元为帧，物理层为比特流。
49. HTTP请求走私是一种干扰网站处理HTTP请求序列方式的技术，使攻击者可以绕过安全控制，未经授权访问敏感数据并直接危害其他应用程序用户。
50. Web程序代码中把用户提交的参数未做过滤就直接输出到HTTP响应头中，攻击者可以利用该漏洞来注入HTTP响应头，可以造成XSS攻击、欺骗用户下载恶意可执行文件等攻击。

51. Hydra是一款爆破神器，可以对多种服务的账号和密码进行爆破，包括Web登录、数据库、SSH、FTP等服务，支持Linux、Windows、Mac平台安装。
52. IDA Pro，为Interactive Disassembler公司的反编译与除错工具的产品，常用于逆向工程。
53. 入侵检测系统（intrusion detection system，简称“IDS”）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处便在于，IDS是一种积极主动的安全防护技术。
54. IMAP (Internet Mail Access Protocol）以前称作交互邮件访问协议（Interactive Mail Access Protocol)，是一个应用层协议。IMAP是斯坦福大学在1986年开发的一种邮件获取协议。它的主要作用是邮件客户端可以通过这种协议从邮件服务器上获取邮件的信息，下载邮件等。
55. IPC$是指共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。
56. 入侵防御系统（IPS: Intrusion Prevention System）是电脑网络安全设施，是对防病毒软件和防火墙的补充。入侵预防系统是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够即时的中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。
57. IP碎片攻击，IP首部有两个字节表示整个IP数据包的长度，所以IP数据包最长只能为0xFFFF，就是65535字节。如果有意发送总长度超过65535的IP碎片，一些老的系统内核在处理的时候就会出现问题，导致崩溃或者拒绝服务。
58. Kali Linux是一个基于Debian的Linux发行版，它预装了14大类近300多个安全测试和渗透软件，Kali Linux预装的这些软件基本包括了黑客会使用到的所有工具。
59. Kill Chain，在网络安全领域，这一概念最早由洛克希德－马丁公司提出，英文名称为Kill Chain，也称作网络攻击生命周期，包括侦查追踪、武器构建、载荷投递、漏洞利用、安装植入、命令控制、目标达成等七个阶段，来识别和防止入侵。
60. LDAP全称：Lightweight Directory Access Protocol，轻型目录访问协议，是一个开放的、中立的工业标准的应用协议，通过IP协议提供访问控制和维护分布式信息的目录信息，常用用途是单点登录，用户可在多个服务中使用同一个密码。
61. LDAP注入是指客户端发送查询请求时，输入的字符串中含有些特殊字符，导致修改了LDAP本来的查询结构，从而使得可以访问更多的未授权数据的一种攻击方式。 类似于SQL注入。
62. MD5一种被广泛使用的密码散列函数，可以产生出一个128位（16字节）的散列值（hash value），用于确保信息传输完整一致。
63. Metasploit是一款开源的渗透测试框架平台， msf 已经内置了数千个已披露的漏洞相关的模块和渗透测试工具，模块使用ruby语言编写，选定需要使用的攻击模块之后，只需要使用简单的命令配置一些参数就能完成针对一个漏洞的测试和利用，将渗透的过程自动化、简单化。
64. Mimikatz为法国人Benjamin Delpy编写的款轻量级的调试工具，在内网渗透过程中，它多数时候是作为一款抓取用户口令的工具。 然而Mimikatz其实并不只有抓取口令这个功能，它还能够创建票证、票证传递、hash 传递、甚至伪造域管理凭证令牌。
65. NCat或者说nc是款功能类似cat的工具，但是用于网络的。它是一款拥有多种功能的 CLI工具，可以用来在网络上读、写以及重定向数据。它被设计成可以被脚本或其他程序调用的可靠的后端工具同时由于它能创建任意所需的连接，因此也是一个很好的网络调试工具。
66. NDay：指已经发布官方补丁的漏洞。通常情况下，此类漏洞的防护只需更新补丁即可，但由于多种原因，导致往往存在大量设备漏洞补丁更新不及时，且漏洞利用方式已经在互联网公开，往往此类漏洞是黑客最常使用的漏洞。
67. Nessus是最受欢迎且功能最强大的漏洞扫描程序之一。它是款用于保护电脑安全，扫描系统漏洞，并及时修复的专业工具，旨在为用户提供完整且有用的网络漏洞扫描方案，可快速轻松地进行补丁、配置以及合规性审核。
68. Netsparker是一款综合型的Web应用安全漏洞扫描工具，它分为专业版和免费版，免费版的功能也比较强大。Netsparker与其他综合性的Web应用安全扫描工具相比的一个特点是它能够更好的检测SQL Injection和Cross site Scripting类型的安全漏洞。
69. Nmap（全称Network Mapper）是一款功能强大、 界面简洁清晰的连接端口扫描软件。Nmap能够轻松扫描确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统，从而帮助用户管理网络以及评估网络系统安全，堪称系统漏洞扫描之王！
70. NTLM(NT LAN Manager）是微软公司开发的一种身份验证机制，从NT4开始就一直使用，主要用于本地的账号管理。

71. Ollydbg通常称作OD，是反汇编工作的常用工具，OD附带了200脱壳脚本和各种插件，功能非常强大，可以过SE, VMP3.0，深受逆向圈内人士的喜爱。
72. OSCP认证，是一个专门针对Kali Linux渗透测试培训课程的专业认证。该认证机构声称，OSCP认证是一个区别于所有其它认证的考试，考试全程采取手动操作的方式，而不设笔试环节。
73. Open Web Application Security Project"表示开放式Web应用程序安全项目，它是一个安全组织，发布了有名的《OWASP Top 10》安全项目，展示了OWASP十大应用安全风险。
74. ZAP则是OWASP里的工具类项目，也是旗舰项目，全称是OWASP Zed attack proxy，是一款web application集成渗透测试和漏洞工具，同样是免费开源跨平台的。
75. Parrot Security OS是个基于Debian的Linux 发行版，专注于计算机安全。它专为渗透测试，漏洞评估和缓解，计算机取证和匿名Web浏览而设计，由Frozenbox团队开发。
76. Payload中文译为，‘有效载荷’，指成功漏洞利用之后，真正在目标系统执行的代码或指令。
77. PoC，全称”Proof of Concept中文译作概念验证。可以理解成为漏洞验证程序。通常是指一段漏洞证明的代码，验证漏洞是否有效，PoC通常是无害的，仅为验证漏洞是否存在。
78. 死亡之Ping（英文： ping of death, POD)，是一种向目标电脑发送错误封包的或恶意的ping指令的攻击方式。通常，一次ping大小为32字节。在当时，大部分电脑无法处理大于IPv4最大封包大小的ping封包。因此发送这样大小的ping可以令目标电脑崩溃。
79. POP3，全名为“Post Office Protocol - Version 3”，即“邮局协议版本3”。是TCP/IP协议族中的一员，由RFC1939定义。本协议主要用于支持使用客户端远程管理在服务器上的电子邮件。
80. Windows PowerShell是微软公司为Windows环境所开发的壳程式（Shell）及脚本语言技术，采用的是命令行界面。这项全新的技术提供了丰富的控制与自动化的系统管理能力。
81. PowerSploit是基于Microsoft Powershell的测试工具集合，可在安全评估所有阶段帮助渗透测试人员，PowerSploit由：CodeExecution、ScriptModification、 Persistence、AntivirusBypass、Exfiltration 等等模块组成。
82. Proxifier软件是一款极其强大的socks5客户端，同时也是款强大的站长工具。Proxifer 支持TCP, UDP 协议，支持Xp, Vista,Win7，支持socks4, socks5, http 代理协议可以让不支持通过代理服务器工作的网络程序能通过HTTPS或SOCKS代理或代理链。
83. RASP即应用运行时自我保护。它是一种新型应用安 全保护技术，它将保护程序像疫苗一样注入到应用程序中，应用程序融为一体，能实时检测和阻断安全攻击，使应用程序具备自我保护能力，当应用程序遭受到实际攻击伤害，就可以自动对其进行防御，而不需要进行人工干预。
84. RCE，全程远程命令执行，由于系统设计实现上存在的漏洞，攻击者可能通过发送特定的请求或数据导致在受影响的系统上执行攻击者指定的任意命令。
85. Rootkit是攻击者用来隐藏自己的行踪和保留root （根权限，可以理解成WINDOWS下的system或者管理员权限）访问权限的工具。
86. Samba是一个能让Linux系统应用Microsoft网络通讯协议的软件，而SMB是ServerMessageBlock的缩写，即为服务器消息块SMB主要是作为Microsoft的网络通讯协议，后来Samba将SMB通信协议应用到了Linux 系统上，就形成了现在的Samba软件。
87. SASE的核心是身份，即身份是访问决策的中心，而不再是企业数据中心。这也与零信任架构和CARTA理念相一致，基于身份的访问决策。
88. SDL的全称为安全开发生命周期，它是由微软最早提出的，在软件工程中实施，是帮助解决软件安全问题的办法，SDL 是一个安全保证的过程，其重点是软件开发，它在开发的所有阶段都引入了安全和隐私的原则。
89. Session：在计算机中，尤其是在网络应用中，称为“会话控制”Session对象存储特定用户会话所需的属性及配置信息。
90. Shell是一种命令执行环境， 比如我们按下键盘上的“开始键+R"时出现“运行”对话框，在里面输入“cmd"会出现一个用于执行命令的黑窗口，这个就是WINDOWS的Shell执行环境。通常我们使用远程溢出程序成功溢出远程电脑后得到的那个用于执行系统命令的环境就是对方的Shell
91. Shellcode是一段用于利用软件漏洞而执行的代码，Shellcode为16进制的机器码，因为经常让攻击者获得shell而得名。

91. Shellcode是一段用于利用软件漏洞而执行的代码，Shellcode为16进制的机器码，因为经常让攻击者获得Shell而得名。Shellcode常常使用机器语言编写。可在暂存器eip溢出后，塞入一段可让CPU执行的Shellcode机器码，让电脑可以执行攻击者的任意指令。
92. Shitf后们，其实就是使用了windows系统的粘滞键功能，当连按5次Shift键的时候就会启动粘滞键程序。然后有些后[门]程序会替换掉这个程序，然后通过按5次就来启动后门。
93. Shodan是互联网上最可怕的搜索引擎。Shodan不是在网上搜索网址，而是直接进入互联网的背后通道。Shodan可以说是一款“黑暗”谷歌，一刻不停的在寻找着所有和互联网关联的服务器、摄像头、打印机、路由器等等。每个月Shodan都会在大约5亿个服务器上日夜不停地搜集信息。
94. SMB （全称： Server Message Block）协议即为服务器消息块，SMB主要是作为Microsoft的网络通讯协议，可应用于Web连接和客户端与服务器之间的信息沟通。后来微软又把SMB改名为CIFS，即公共Internet文件系统，并且加入了许多新的功能。
95. SMTP是一种提供可靠且有效的电子邮件传输的协议。SMTP是建立在FTP文件传输服务上的一种邮件服务，主要用于 系统之间的邮件信息传递，并提供有关来信的通知。
96. SPF，即发件人策略框架是一套电子邮件认证机制，可以确认电子邮件确实是由网域授权的邮件服务器寄出，防止有人伪冒身份网络钓鱼或寄出垃圾电邮。SPF 允许管理员设定一个DNS TXT记录或SPF记.录设定发送邮件服务器的IP范围来验证是否为假冒邮件。
97. SPN扫描通过域控制器的LDAP进行服务查询，由于这是Kerberos票据行为的一部分，所以很难被检测到。
98. SQLMap是一个开源渗透测试工具，它可以自动检测和利用SQL注入漏洞并接管数据库服务器。它具有强大的检测引擎，同时有众多功能，包括数据库指纹识别、从数据库中获取数据、访问底层文件系统以及在操作系统上带内连接执行命令。
99. SQL盲注根据注入后页面返回不同情况来得到数据库信息的一-种办法。（例如布尔盲注， 时间盲注等。）
100. SQL注入即是指web应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在事先定义好的查询语句的结尾上添加额外的SQL语句，以此来实现欺骗数据库服务器执行非授权的任意查询，得到相应的数据信息。
101. 漏洞响应平台即SRC，一些企业会通过建立自己的应急响应中心，通过互联网白帽子的力量发掘自身产品的安全问题，并给予-些漏洞挖掘报酬。白帽子可以通过SRC提交你的漏洞换取- - 些钱或者奖励。
102. SSI注入全称Server- Side Includes Injection，即服务端包含注入。Ssl是类似于CGI，用于动态页面的指令。SSI 注入允许远程在Web应用中注入脚本来执行代码。
103. 单点登录（SingleSignOn, SSO） 指一个用户可以通过单一的ID和凭证（密码）访问多个相关但彼此独立的系统。
104. SSRF （服务端请求伪造很多），Web 应用都提供了从其他的服务器上获取数据的功能。使用用户指定的URL, Web应用可以获取图片，下载文件，读取文件内容等。这个功能如果被恶意使用，可以利用存在缺陷的Web应用作为代理攻击远程和本地的服务器，探测内网信息甚至内网入侵。
105. SSTI，服务端模板注入是由于服务端接收了用户的输入，将其作为Web应用模板内容的一部分，在进行目标编译渲染的过程中，执行了用户插入的恶意内容，因而导致了敏感信息泄露、代码执行、GetShell等问题。其影响范围主要取决于模版引擎的复杂性。
106. Apache Struts2是一个基于MVC设计模式的Web应用框架，会对某些标签属性（比如id）的属性值进行二次表达式解析，因此在某些场景下将可能导致远程代码执行。
107. SVN信息泄漏，在使用SVN管理本地代码过程中，会自动生成一个隐藏文件夹，其中包含重要的源代码信息，在发布代码时由于错误操作，直接复制代码文件夹到WEB服务器上，这就使隐藏文件夹被暴露于外网环境，这使得渗透工程师可以借助其中包含版本信息追踪的网站文件，逐步摸清站点结构。
108. 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。
109. Tamper Data, Firefox 插件，这是渗透测试人员最爱的插件之一，经常用来查看修改HTTP/HTTPS头部文件、HTTP 的响应时间或请求时间、POST 参数。
110. TCP四次挥手，由于TCP连接是全双工的，因此每个方向都必须单独进行关闭。TCP有个半关闭状态，假设A.B要释放连接，那么A发送一个释放连接报文给B，B收到后发送确认这个时候A不发数据，但是B如果发数据A还是要接受，这叫半关

闭。然后B还要发给A连接释放报文，然后A发确认，所以是4次。

111. Telegram （非正式简称TG）是跨平台的即时通信软件，其客户端是自由及开放源代码软件，但服务器端是专有软件。用户可以相互交换加密与自毁消息（类似于“阅后即焚”），发送照片、影片等所有类型文件。

112. Token，在计算机身份认证中是令牌（临时）的意思，在词法分析中是标记的意思。一般作为邀请、登录系统使用。

113. 用户账户控制（User Account Control，简写作UAC）是微软公司在其Windows Vista及更高版本操作系统中采用的-种控制机制。其原理是通知用户是否对应用程序使用硬盘驱动器和系统文件授权，以达到帮助阻止恶意程序（有时也称为“恶意软件”）损坏系统的效果。

114. URL编码是–种浏览器用来打包表单输入的格式。浏览器从表单中获取所有的name和其中的值，将它们以name/value参数编码（移去那些不能传送的字符，将数据排行等等）作为URL的一部分或者分离地发给服务器。

115. URL定向钓鱼，通过构建URL，攻击者可以使用户重定向到任意URL，利用这个漏洞可以诱使用户访问某个页面，挂马、密码记录、下载任意文件等，常被用来钓鱼。

116. User Agent Switcher, Firefox 插件，可 以快速添加用户端按钮，可以模拟用户使用不用设备、不同系统的浏览器访问，例如IE,Search Robots，IPhone (IOS)。

117. UTM安全设备的定义是指一体化安全设备，它具备的基本功能包括网络防火墙、网络入侵检测/防御和网关防病毒功能。

118. 虚拟专用网络（VPN）的功能是：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN可通过服务器、硬件、软件等多种方式实现。

119. VPS （即虚拟专用服务器）技术，将一台服务器分割成多个虚拟专享服务器的优质服务。实现VPS的技术分为容器技术，和虚拟化技术在容器或虚拟机中，每个VPS都可选配独立公网IP地址、独立操作系统、实现不同VPS间磁盘空间、内存、CPU资源、进程和系统配置的隔离。

120. 被称为Vanderpool的虚拟技术简称VT，是英特尔公司处理器市场策略之中的一部分，英特尔公司的策略是向用户提供的实用功能而不是增长的性能。VT能够使用户在他们的个人电脑.上建立多套虚拟的运行环境以便能够使同一台个人电脑上能够运行不同的操作系统。

121. WAF即Web Application Firewall, 即Web应用防火墙，是通过执行一系列针对HTTP/HTTPS的安全策略来专门]为Web应用提供保护的一款产品。

122. Web Developer，Firefox 插件，Web Developer是另外一个好的插件，能为浏览器添加很多web开发工具，当然在渗透渗透测试中也能帮上忙。

123. WebShell就是以asp. php. jsp 或者cgi等网页文件形式存在的一种命令执行环境，得到一个命令执行环境，以达到控制网站服务器的目的。可以上传下载文件，查看数据库，执行任意程序命令等。也可以将其称作是一种网页后门。

124. Web容器是一种服务程序，在服务器一个端口就有一个提供相应服务的程序，而这个程序就是处理从客户端发出的请求，如JAVA中的Tomcat容器， ASP的IIS或PWS都是这样的容器。

125. Web应用防火墙，是一款专门提供网站安全服务的产品，集FW.IPS、WAF、 防篡改等功能为- -体，通过 多维度多模块的防御策略防护网站的系统及业务安全。

126. Whois （读作“Whois”，非缩写）是用来查询域名的IP以及所有者等信息的传输协议。简单说，Whois 就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）

127. WinHex （窗口十六进制）是一个德国软件公司X-Ways所开发的十六进制资料编辑处理程序，还可以应用在磁盘资料撤销及资料剖析采证上。WinHex小巧轻快但功能众多，且在此领域已有相当长的历史，第一个公开版本是在1995年。

128. Wireshark是一个非常棒的开源多平台网络协议分析器。它允许检查来自实时网络或磁盘上的捕获文件的数据。您可以以交互方式浏览捕获数据，深入了解所需的数据包详细信息。

129. WMI，是Windows 2K/XP管理系统的核心;对于其他的Win32操作系统，WMI 是一个有用的插件。

130. WriteUp，常指CTF（信息安全夺旗赛）中的解题思路，比赛结束后，通常主办方会要求排名靠前的提交WriteUp，看你是怎么做的。这不仅是为了证明题是你做的，而且由于ctf题目通常一题都是有n种解法的，这样做也可以因此扩展其他选手的知识。

131. XFF，是X-Forwarded-For的缩写，存在于http请求头中，XFF注入是SQL注入的一种，该注入原理是通过修改X-Forwarded-For头对带入系统的dns进行sql注入，从而得到网站的数据库内容。

132. XML注入，服务端解析用户提交的XML文件时未对XML文件引用的外部实体做合适的处理，并且实体的URL支持file:// 和php://等协议，攻击者可以在XML文件中声明URI指向服务器本地的实体造成攻击。

133. Xp_cmd shell,，是SQL Server的一个扩展存储过程，xp_cmd shell扩展存储过程将命令字符串作为操作系统命令shell执行，并以文本行的形式返回所有输出。基于安全考虑，MSSQL2005 及以上版本默认禁用了xp_ cmd shell.

134. 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。

135. Xposed (也被称作Xposed框架），是一个运行于Android操作系统的钩子框架。其通过替换Android系统的关键文件，可以拦截几乎所有Java函数的调用，并允许通过Xposed模块中的自定义代码更改调用这些函数时的行为。因此，Xposed 常被用来修改Android系统和应用程序的功能。

136. 类似于XPath注入，XQuery 注入攻击是指利用XQuery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XQuery查询代码，以获得权限信息的访问权并更改这些信息。

137. XSS是跨站脚本攻击（Cross Site Scripting)， 为不和层叠样式表（Cascading Style Sheets，CSS) 的缩写混淆，故将跨站脚本攻击缩写为XSS。通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序，如劫持用户会话，插入恶意内容、重定向用户等。

138. XXE就是XML外部实体注入（XML External Entity。当允许引用外部实体时，通过构造恶意内容，就可能导致任意文件读取、系统命令执行、内网端口探测、攻击内网网站等危害。

139. 暗链也称黑链，是黑帽SEO的作弊手法之一，目的就是利用高权重网站外链来提升自身站点排名。暗链是由攻击者入侵网站后植入的，且在网页上不可见或者极易被忽略，但是搜索引擎仍然可以通过分析刚页的源代码收录这些链接，以此迅速提高自身网站权重，获得高额流量。

140. 安全加固是指是根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。

141. 安全模式绕过指通过程序相关解析等问题，绕过程序原有的安全保护措施或者模式的一种漏洞类型。

142. 安全审计，指由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。

143. 安全众测，借助众多白帽子的力量，针对目标系统在规定时间内进行漏洞悬赏测试。在收到有效的漏洞后，按漏洞风险等级给予白帽子一定的奖励。通常情况下是按漏洞付费，性价比较高。

144. 暗网（英语： Dark web）是存在于黑暗网络、覆盖网络上的万维网内容，只能用特殊软件、特殊授权或对计算机做特殊设置才能访问，一.些灰色的非法网站将他们]的资源联系到一起形成了一个庞大的网络，这就是暗网。

145. 安卓模拟器是能在个人计算机运行并模拟安卓手机系统的模拟器，并能安装、使用、卸载安卓应用的软件，利用安卓模拟器，用户即使没有手机硬件设备，也能在模拟器中使用移动应用程序。

146. 白盒测试又称结构测试、透明盒测试逻辑驱动测试或基于代码的测试。白盒测试是一种测试用例设计方法，需要全面了解程序内部逻辑结构、对所有逻辑路径进行测试，穷举路径测试。检查程序的内部结构，从检查程序的逻辑着手，得出测试数据。

147. 白帽黑客，一群不被利益趋驱使的文艺黑客。White hat (computersecurity）术语"white"在网络语言中指的是–种道德的电脑黑客，或计算机安全专家，专攻渗透测试和其他测试方法，以确保一个组织的信息系统的安全。

148. 报错注入，顾名思义，报错注入就是通过页面爆出的错误信息，构造合适的语句来获取我们]想要的数据，SQL报错注入就是利用数据库的某些机制，人为地制造错误条件，使得查询结果能够出现在错误信息中。

149. 堡垒机，即在一个特定的网络环境下，为了保障网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动，以便集中报警、及时处理及审计定责。

150. 暴力破解，通过利用大量猜测和穷举的方式来尝试获取用户口令的攻击方式。就是猜口令。攻击者一直枚举进行请求，通过对比数据包的长度可以很好的判断是否爆破成功，因为爆破成功和失败的长度是不一样的，所以可以很好的判断是否爆破成功。

151. 靶机，就是指一个存在漏洞的系统，互联网上所有的网站（系统）都可以说是“靶机”，但是由于存在网络安全法，你是不能直接对人家的未授权的网站（系统）进行测试的。但是，你想做为练手、或者说验证某个漏洞怎么办?现在就有了靶机

的出现，提供测试，验证，学习。

152. 本地文件包含漏洞，由于程序员未对用户可控的变量进行输入检查，导致用户可以控制被包含的文件，成功利用时可以使服务器将特定文件当成服务端脚本执行，从而导致攻击者可获取–定的服务器权限，同时可能导致服务器上的敏感配置文件被攻击者读取。

153. 边界防御，以网络边界为核心的防御模型，以静态规则匹配为基础，强调把所有的安全威胁都挡在外网。

154. 编辑器漏洞，某一些编辑器如FCKEditor、UEditor 以及EWEBeditor等在特定版本存在漏洞如文件上传，命令执行等漏洞。

155. 比特币（Bitcoin） 的概念最初由中本聪在2008年11月1日提出，并于2009年1月3日正式诞生。根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的虚拟的加密数字货币。点对点的传输意味着一个去中心化的支付系统。

156. 彩虹表（Rainbow Tables）就是一个庞大的、针对各种可能的字母组合预先计算好的哈希值的集合，常用来破解md5。

157. 持久化，在攻击者利用漏洞获取到某台机器的控制权限之后，会考虑将该机器作为一个持久化的据点，种植一个具备持久化的后门，从而随时可以连接该被控机器进行深入渗透。

158. 冲击波蠕虫是一种散播于Microsoft操作系统，WindowsXP与Windows 2000的蠕虫病毒，爆发于2003年8月。本蠕虫第一次被注意并如燎原火般散布，是在2003年的8月11日。它不断繁殖并感染，在8月13 日达到高峰，之后借助ISP与网络上散布的治疗 方法阻止了此蠕虫的散布。

159. 垂直越权是指由于后台应用没有做权限控制，或仅仅在菜单、按钮上做了权限控制，导致恶意用户只要猜测其他管理页面的URL或者敏感的参数信息，就可以访问或控制其他角色拥有的数据或页面，达到权限提升的目的。

160. 储存型XSs，攻击者事先将恶意代码上传或储存到漏洞服务器中，只要受害者浏览包含此恶意代码的页面就会执行恶意代码。这就意味着只要访问了这个页面的访客，都有可能会执行这段恶意脚本，因此储存型XSS的危害会更大。

161. 代理： Proxy， 一类程序或系统，接收来自客户计算机的流量，并代表客户与服务器交互。代理能用于过滤应用级别的制定类型的流量或缓存信息以提高性能。许多防火墙依赖代理进行过滤。

162. 代码混淆（Obfuscation） 是将计算机程序的代码转换成功能上等价，但是难于阅读和理解的形式的行为。

163. 代码审计，顾名思义就是检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议。

164. 代码泄露指的是服务器等由于配置不当等原因导致程序源代码可以被攻击者直接访问。

165. 代码执行漏洞是用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许攻击者通过改变SPATH或程序执行环境的其他方面来执行一个恶意构造的代码。

166. 安全网关是各种技术有趣的融合，具有重要且独特的保护作用，其范围从协议级过滤到十分复杂的应用级过滤。设置的目的是防止Internet或外网不安全因素蔓延到自己企业或组织的内部网。

167. 打补丁就好比你的衣服破了个洞需要补漏一样，是对系统的缺陷进行补丁的一种程序包。所谓的补丁就是你安装的这个系统中有些所谓的“漏洞”的修补程序，安装上这些补丁就是把这些“漏洞”补上，以提高安全性或增强性能。

168. 等级保护般指信息安全等级保护。信息安全等级保护，是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的工作。

169. 点击劫持（ClickJacking）也被称为UI覆盖攻击。它是通过覆盖不可见的框架误导受害者点击。虽然受害者点击的是他所看到的网页，但其实他所点击的是被黑客精心构建的另一个置于原网页上面的透明页面。这种攻击利用了HTML中标签的透明属性。

170. 电子取证，数字取证是取证科学的一个分支，它包括计算机取证、网络取证和移动设备取证等，它是一个新兴的领域。

171. 钓鱼网站是指欺骗用户的虚假网站。“钓鱼网站” 的页面与真实网站界面基本致，欺骗消费者或者窃取访问者提交的账号和密码信息。钓鱼网站一般只有一个或几个页面，和真实网站差别细微。

172. 端口可以认为是设备与外界通讯交流的出口。端口可分为虚拟端口和物理端口，其中虚拟端l指计算机内部或交换机路由器内的端口。例如计算机中的80端口、21 端口、23 端口等。物理端口又称为接口，计算机背板的RJ45网口，交换机路由器集线器等RJ45端口等属于物理接口。

173. 端口复用是指一个端口上建立多个连接，而不是在一个端口上面开放了多个服务而互不干扰。 在一般情况下，一个端口只能被一个程序所占用，如果通过套接字设置了端口复用选项，则该套接字就可以绑定在已经被占用的端口上，同时并没有权限的区分。

174. 端口扫描是指发送一组端口扫描消息，以识别目标端口服务信息、版本信息等。通过了解到的信息探寻攻击弱点，试图以此侵入某台计算机。

175. 端口转发就是将一台主机的网络端口转发到另外一台主机并由另一台主机提供转发的网络服务。

176. 短信轰炸漏洞在网站的一个发送验证码的接口上， 由于未做短信发送限制，可以无限制的请求发送验证码，造成短信资源池浪费，也对被轰炸人造成了严重的影响。

177. 短信劫持，就是在GSM网络下（也就是2G），利用GSM劫持+短信嗅探技术可实时获取使用2G信号的用户手机短信内容，这主要是GSM在制式上存在缺陷，进而利用各大银行、网站、移动支付APP存在的技术漏洞和缺陷，实现信息窃取、资金盗刷和网络诈骗等犯罪。

178. 对称加密采用单钥密码系统的加密方法、同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。

179. 多因子认证，主要区别于单一口令认证的方式，要通过两种以上的认证机制之后，才能得到授权，使用计算机资源：例如，用户要输入PIN码，插入银行卡，最后再经指纹比对，通过这三种认证方式，才能获得授权.这种认证方式可以降低单一口令失窃的风险，提高安全性。

180. 所谓二阶注入是指已存缩（数期库、文件）的用户输入被读取后再次进入到SOL，查询语句中导致的注入

181. 恶意代码Unwanted Code是指没有作用却会带来危险的代码，一个最安全的定义是把所有不必要的代码都看作是恶也的、不必要代码比恶意代码具有更宽泛的含义，包括所有可能与某个组织安全策略相冲突的软件

182. 防爬意为防爬虫，主要是指防止网络爬虫从自身网站中爬取信也网络爬虫是一种按照一定的规则，自动地抓取网络信息的福序或者脚本。

183. 反射型XSS 把用户输入的数据“反射”给浏览器。攻击者往往需要诱使用户“点击”一个恶意链接，于能攻击成功，反射型XSS 也叫做“非持久型XSS”。

184. 反向代理服务器位于用户与目标服务器之间，但是对于用户而言，反向代理服务器就相当于目标服务器，即用户直接访向反向代理服务器就可以获得目标服务器的资源。同时，用户不需要知道目标服务器的地址，也无须在用户端作任何设定。

185. 反序列化漏洞，如果应用对用户输入，即不可信数据做了反序列化处理，那么攻击者可以通过构造恶意输入，让反序列化产生非预期的对象，非预期的对象在产生过程中就有可能带来任意代码执行。

186. 反制，在已知现有的攻击信息对攻击源头采取相应的措施实施反制措施，反制措施是对敌对人物和势力的行为进行回击，包含以血还血、以牙还牙的意思，也是打击和制伏进攻敌人。

187. 非对称加密算法是一种密钥的保密方法。非对称加密算法需要两个密钥：公开密钥（publickey：简称公钥）和私有密钥（privatekey：简称私钥）。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密、

188. 风险端口-1090，是 RMI 服务的默认端门，是远程方法调用。1099端口原本对应的服务为Apache ActiveMQ对JMX的支持，但是由于配置不当，导致攻击者可以通过此端口利用getMBeansFromURL方法来加载一个远端恶意的MBean，即可以远程执行任意代码。

189. 风险端口-11211，是 Memcache服务的默认端口，由于它本身没有权限控制模块，所以对公网开放的 Memcache服务很容易被攻击者扫描发现，攻击者通过命令交互可直接读取 Memcached中的敏感信息

190. 风险端口-1433.是SQL Server默认的端口。SQL Server服务使用两个端口：TCP-1433 UDP-1434。其中1433用于供对外提供服务、1434用于向请求者返回SQL cerver使用了哪个TCP/IP端口。该服务可能存在弱口令，暴力破解等风险。

191. 风险端口-1521, ORACLE数据库系统付用1521端口，ORACLE数据库是美国ORACLE公司（甲骨文）提供的以分布式数据库为核心的一组软件产品，是目前最流行的客户/服务器（CLIENT/SERVER）或B/S体系结构的数据库之一。该数据库可能存在弱口令、暴力破解等风险。

192. 风险端口-161、简单网络管理协议（SNMP）是专门设计用于在IP网络管理网络节点（服务器、工作站、路由器、交换机及HUBS等）的一种标准协议，它是一种应用协议该服务。可能存在弱口令，信息泄露等风险。

193. 风险端-21，主要用于FTP (File Transfer Protocol.文件传输协议）服务。FTP服务主要是为了在两台计算机之间实现文件的

上传与下载，可以采用匿名（anonvmous）登录和授权用户名与密码登录两种方式登录FTP服务器。该服务存在弱口令，暴力破解等风险。

194. 风险端口-2181, Zookeeper服务器的默认端口、分布式的，开放源码的分布式应用程序协调服务。Zookeeper安装部署之后默认情况下不需要任何身份验证，造成攻击者可以远程利用Zookeeper，通过服务器收集敏感信息或者在Zookeeper 集群内进行破坏。

195. 风险端口-22，SSH是传输层和应用层上的安全协议，它只能通过加密连接双方会话的方式来保证连接的安全性。当使用SSH连接成功后，将建立客户端和服务端之间的加密会话。该服务存在弱口令、暴力破解等风险。

196. 风险端口-23，Telnet协议早 TCP/IP协议族中的一员，是Internet远程登录服务的标准协议和主要方式。该服务存在弱口令、暴力破解等风险。

197. 2375是Docker默认端口，当 Docker Daemon把服务暴露在TCP的2375端口上，这样就可以在网络上操作Docker了。Docker 本身没有身份认证的功能，只要网络上能访问到服务端口，就可以操作Docker，可能存在未授权访问等风险。

198. MongoDB是一个基于分布式文件存储的数据库。由CH+语言编写。旨在为WEB应用提供可扩展的高性能数据存储解决方案。该服务可能存在默认口令，弱口令，未授权等风险。

199. MySQL是一种开放源代码的关系型数据库管理系统（RDBMS），使用最常用的数据库管理语言–结构化查询语言（SQL）进行数据库管理。该服务可能存在弱口令，暴力破解等风险。

200. 3389端口是 Windows远程桌面的服务端口，可以通过这个端口，用"远程桌面"等连接工具来连接到远程的服务器。该服务可能存在弱口令，暴力破解，远程命令执行等风险。

201. 风险端口-443，主要是用于 HTTPS服务，是提供加密和通过安全端口传输的另一种HTTP。在一些对安全性要求较高的网站，比如银行、证券等，都采用HTTPS服务，这样在这些网站上的交换信息，其他人抓包获取到的是加密数据，保证了交易的安全性。该服务可能存在SSL心脏滴血等安全风险。

202. 445端口是一个毁誉参半的端口，有了它我们可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机，他们能通过该端口偷偷共享你的硬盘，甚至会在悄无声息中将你的硬盘格式化掉，该端口可能存在永恒之蓝等风险。

203. GlassFish是一款强健的商业兼容应用服务器，达到产品级质量，可免费用于开发、部署和重新分发。该服务部分版本存在弱口令，远程命令执行等风险。

204. 美国Sybase 公司研制的一种关系型数据库系统，IBM DB2是美国IBM 公司开发的一套关系型数据库管理系统。两款数据库在部分版本存在爆破以及注入等风险。

205. 风险端口-5432,PostgreSQL是一种特性非常齐全的自由软件的对象-关系型数据库管理系统（ORDBMS），是以加州大学计算机系开发的POSTGRES,4.2版本为基础的对象关系型数据库管理系统。该服务可能存在弱口令，暴力破解等风险。

206. 风险端口-5900,VNC (Virtual Network Console）是虚拟网络控制台的缩写。它是一款优秀的远程控制工具软件，由著名的AT&T的欧洲研究实验室开发的。该服务可能存在弱口令，暴力破解等风险。

207. 风险端口-5948， Apache CouchDB是一个面向文档的数据库管理系统。它提供以JSON作为数据格式的 REST接口来对其进行操作，并可以通过视图来操纵文档的组织和呈现。该服务部分版本存在未授权导致的任意命令执行风险。

208. 风险端口-6379，是 Redis默认端口，Redis因配置不当可以未授权访问。攻击者无需认证访问到内部数据，可导致敏感信息泄露，也可以恶意执行flushall 来清空所有数据。如果 Redis 以 root身份运行，可以给root账户写入SSH公钥文件，直接通过SSH登录受害服务器。

209. 风险端口-7001，是 Weblogic的默认端口，可能存在java反序列化，Weblogic服务端请求伪造漏洞等。

210. Zabbix是一个基于WEB 界面的提供分布式系统监视以及网络监视功能的企业级的开源解决方案。zabbix能监视各种网络参数，保证服务器系统的安全运营;并提供灵活的通知机制以让系统管理员快速定位/解决存在的各种问题。在部分版本存在SQL注入、未授权、RCE等风险。

211. Rsync(remote synchronize）是一个远程数据同步工具，可通过LAN/WAN快速同步多台主机间的文件，也可以使用 Rsync同步本地硬盘中的不同目录。该服务部分版本存在匿名访问以及文件上传等风险。

212. 风险端口-8888，宝塔面板是一款简单好用的服务器运维面板，简单说来就是一个可视化的面板管理工具，支持一键LAMP/LNMP/集群/监控/网站/FTP/数据库/JAVA等100多项服务器管理功能。部分版本存在信息泄露，数据库未授权等风

险。

213. 风险端口-9090,Websphere,IBM WebSphere Application Server(WAS）是由IBM 遵照开放标准，例如Java EE、XML及WebServices，开发并发行的一种应用服务器，该服务可能存在Java反序列化以及弱口令等风险。

214. 风险端口-9200/9300, Elasticsearch 是一个分布式、RESTful 风格的搜索和数据分析引擎，能够解决不断涌现出的各种用例。该服务可能存在远程命令执行、文件包含，越权访问等风险。

215. 风险控制是指风险管理者采取各种措施和方法，消灭或减少风险事件发生的各种可能性，或风险控制者减少风险事件发生时造成的损失。

216. 分块传输编码（Chunked transfer encoding）是超文本传输协议（HTTP）中的一种数据传输机制，允许HTTP由网页服务器发送给客户端应用（通常是网页浏览器）的数据可以分成多个部分。分块传输编码只在HTTP协议1.1版本（HTTP/1.1）中提供。

217. 供应链攻击是一种传播间谍软件的方式，一般通过产品软件官网或软件包存储库进行传播。通常来说，黑客会瞄准部署知名软件官网的服务器，篡改服务器上供普通用户下载的软件源代码，将间谍软件传播给前往官网下载软件的用户。

218. 所谓的挂马，就是黑客通过各种手段，获得网站管理员账号，然后登录网站后台，通过漏洞获得一个webshell。利用获得的webshell修改网站页面的内容，向页面中加入恶意转向代码。当你访问被加入恶意代码的页面时，你就会自动的访问被转向的地址或者下载木马病毒。

219. 薅羊毛本是沿袭春晚小品中白云大妈的“游羊毛织毛衣”的做法，被定义为“薅羊毛”。所谓薅羊毛就是指网赚一族利用各种网络金融产品或红包活动推广下线抽成赚钱，又泛指搜集各个银行等金融机构及各类商家的优惠信息，以此实现盈利的目的。这类行为就被称之为薅羊毛。

220. 黑盒测试，在授权的情况下，模拟黑客的攻击方法和思维方式，来评估计算机网络系统可能存在的安全风险。黑盒测试不同于黑客入侵，并不等于黑站。黑盒测试考验的是综合的能力。思路与经验积累往往决定成败，黑盒测试还是传统的渗透测试。

221. 黑帽黑客（black hat hacker）就是人们常说的“黑客”或“骇客”了。他们往往利用自身技术，在网络上窃取别人的资源或破解收费的软件，以达到获利的目的。虽然在他们看来这是因为技术而得到的，但是这种行为却往往破坏了整个市场的秩序，或者泄露了别人的隐私。

222. 黑页，黑客攻击成功后，在网站上留下的黑客入侵成功的页面，用于炫耀攻击成果。

223. 横向移动，横向渗透攻击技术是复杂网络攻击中广泛使用的一种技术，攻击者可以利用这些技术，以被攻陷的系统为跳板，访问其他主机，获取包括邮箱、共享文件夹或者凭证信息在内的敏感资源。攻击者可以利用这些敏感信息，进一步控制其他系统、提升权限或窃取更多有价值的凭证。

224. 宏病毒，宏可能引起宏病毒，它是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行、激活、转移到计算机上，并驻留模板上。所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

225. 红帽黑客，红帽黑客以正义、道德、进步、强大为宗旨，以热爱祖国、坚持正义、开拓进取为精神支柱，红客通常会利用自己掌握的技术去维护国内网络的安全，并对外来的进攻进行还击。

226. 后门，在信息安全领域，后门是指绕过安全控制而获取对程序或系统访问权的方法。后门的最主要目的就是方便以后再次秘密进入或者控制系统。

227. 后渗透，在内网中根据目标的业务经营模式、保护资产形式与安全防御计划的不同特点，自主设计出攻击目标，识别关键基础设施，并寻找客户最具价值的尝试安全防护的信息和资产，最终达成能够对客户造成最重要业务影响的攻击途径。

228. 缓冲区过读是一类程序错误，即程序从缓冲器读出数据时超出了边界，而读取了（或试图读取）相邻的内存。这是有违内存安全的一个例子。

229. 花指令是对抗反汇编的有效手段之一，正常代码添加了花指令之后，可以破坏静态反汇编的过程，使反汇编的结果出现错误。错误的反汇编结果会造成破解者的分析工作大量增加，进而使之不能理解程序的结构和算法，也就很难破解程序，从而达到病毒或软件保护的目的。

230. 活动目录（Active Directory）是面向Windows Server的目录服务，活动目录存储了有关网络对象的信息，并且让管理员和用户可以轻松

231. 查找和使用这些信息。活动目录使用了一种结构化的数据存储方式，并以此作为基础对目录信息进行合乎逻辑的分层组

231. 组织。

232. 加壳，是一种通过一系列数学运算，将可执行程序文件成动态链接库文件的编码进行改变（目前还有一些加壳软件可以压缩、加密驱动序），以达到缩小文件体积或加密程序编码的目的。加壳一般是指保护程序资源的方法。

233. 加密机是通过国家商用密码主管部门整定并批准使用的国内自主开发的主机加密设备，加密机和主机之国使用TCPIP协议通信，所以加密机对主机的类型和主机操作系统无任何特殊的要求。

234. 文件解析漏洞。是指Web容器（Apache、Nginx、IIS等）在解析文件时出现了漏洞，以其他格式执行出脚本格式的效果。从而，黑客可以利用该漏洞实现非法文件的解析。

235. 竞争/并发漏洞，常属于逻辑业务中的漏洞类型，例如攻击者通过并发http/tcp请求而达到多次获奖、多次收获、多次获赠等非正常逻辑所能触发的效果。

236. 进程迁移就是将一个进程从当前位置移动到指定的处理器上。它的基本思想是在进程执行过程中移动它，使得它在另一个计算机上继续存取他的所有资源并继续运行，而且不必知道运行进程或任何与其它相互作用的进程的知识就可以启动进程迁移操作。

237. 近源渗透测试人员靠近或位于测试目标建筑内部，利用各类无线通讯技术、物理接口和智能设备进行渗透测试的总称。

238. 基线检查是针对服务器操作系统、数据库、软件和容器的配置进行安全检测，并提供检测结果说明和加固建议。基线检查功能可以帮您进行系统安全加固，降低入侵风险并满足安全合规要求。

239. 开源，(Open Source）全称为开放酿代码。开源就是要用户利用源代码在其基础上修改和学习的，但开源系统同样也有版权，同样也受到法律保护。

240. 空字符注入也叫零字节注入，是通过添加URL编码的零字节字符来绕过过滤器的一种攻击方式。

241. 跨域资源共享（CORS）是一种放宽同源策略的机制，它允许浏览器向跨源服务器，发出XMLHttpRequest 请求，从而克服了AJAX只能同源使用的限制，以使不同的网站可以跨域获取数据。

242. 垃圾邮件是指未经用户许可（与用户无关）就强行发送到用户邮箱中的电子邮件。

243. 勒索软件是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意软件。勒索软件通常会将用户数据或用户设备进行加密操作或更改配置，使之不可用，然后向用户发出勒索通知，要求用户支付费用以获得解密密码或者获得恢复系统正常运行的方法。

244. 联合查询是可合并多个相似的选择查询的结果集。等同于将一个表追加到另一个表，从而实现将两个表的查询组合到一起，使用谓词为UNION或 UNION ALL。

245. 零信任并不是不信任，而是作为一种新的身份认证和访问授权理念，不再以网络边界来划定可信或者不可信，而是默认不相信任何人、网络以及设备，采取动态认证和授权的方式，把访问者所带来的网络安全风险降到最低。

246. 所谓“流量劫持”，是指利用各种恶意软件修改浏览器、锁定主页或不停弹出新窗口，强制网络用户访问某些网站，从而造成用户流最被迫流向特定网页的情形。

247. 漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

248. 漏洞复测一般指在渗透测试中的漏洞修复阶段，在厂家修复已检测出的安全问题后，检测方对已有问题进行二次检测，检测漏洞是否修复。

249. 漏洞复现是指针对互联网已经暴露出来安全漏洞进行漏洞验证，依据脚本/工具进行漏洞的重现。

250. 漏洞组合拳，引申意为了达到一定目标，采取一连套的措施或实施一整套的步骤来进行，指通过多个漏洞进行组合搭配从而达到预期效果。

251. 逻辑漏洞就是指攻击者利用业务的设计缺陷，获取敏感信息或破坏业务的完整性。一般出现在密码修改、越权访问、密码找回、交易支付金额等功能处。

252. 目录遍历（路径遍历）是由于Web服务器或者Web应用程序对用户输入的文件名称的安全性验证不足而导致的一种安全漏洞，使得攻击者通过利用一些特殊字符就可以绕过服务器的安全限制，访问任意的文件（可以是 Web根目录以外的文件），甚至执行系统命令。

253. 路由劫持是通过欺骗方式更改路由信息，导致用户无法访问正确的目标，或导致用户的访问流量绕行黑客设定的路径，达

到不正当的目的。

254. 免杀技术全称为反杀毒技术Anti Anti-Virus简称“免杀”，它指的是一种能使病毒木马免于被杀毒软件查杀的技术。由于免杀技术的涉猎面非常广，其中包含反汇编、逆向工程、系统漏洞等黑客技术，其内容基本上都是修改病毒、木马的内容改变特征码，从而躲避了杀毒软件的查杀。

255. 绵羊墙（The Wall of Sheep）是在西方举行的各种黑客大会或安全大会上经常出现的趣味活动，源自于黑客大会的鼻祖Defcon。将用户设置的不安全的网络用户名与密码公布在上。

256. Web程序代码中把用户提交的参数未做过滤就直接输出，通过修改参数，攻击者可直接使用Shell，对系统执行命令。

257. 敏感信息/明文传输，网站未使用SSL 证书加密通讯，恶意攻击者如果对网站所在的网段进行嗅探，则当用户登录的时候该攻击者就可以获取到用户的用户名和密码等信息。

258. 蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机或者网络服务诱使攻击方实施攻击，对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，让防御方清晰地了解他们所面对的安全威胁。

259. 密码嗅探，通过监视或监听网络流量以检索密码数据来收集密码的技术。如果使用非加密的方式传输，一旦数据被截获，就容易被嗅探到传输数据内部的账户密码信息。

260. 蜜网（Honeynet）是在蜜罐技术上逐步发展起来的，蜜网技术实质上还是蜜罐技术，其主要目的是收集黑客的攻击信息。但它又不同于传统的蜜罐技术，它不是单一的系统而是一个网络，即构成了一个诱捕黑客行为的网络体系架构，在这个架构中包含了一个或多个蜜罐。

261. 模糊测试（Fuzzing），是一种通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞的方法。

262. 目录穿越的目的旨在访问存在在网站根目录外面的文件或目录。通过浏览应用，攻击者可以寻找存储在Web 服务器上的其他文件的相对路径。

263. 目录浏览漏洞，Web中间件如果开启了目录浏览功能，当用户访问Web 应用时，Web服务器会将 Web应用的目录结构、文件信息返回给客户端，攻击者可能利用这些敏感信息对Web应用进行攻击，如数据库脚本SQL文件路径泄露、程序备份压缩文件路径泄露等。

264. 木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘等特殊功能的程序。可以对被控计算机实施监控、资料修改等非法操作。木马病毒具有很强的隐蔽性，可以根据黑客意图突然发起攻击。

265. 内存保护是操作系统对电脑上的内存进行访问权限管理的一个机制。内存保护的主要目的是防止某个进程去访问不是操作系统配置给它的寻址空间。

266. 内存取证一般指对计算机及相关智能设备运行时的物理内存中存储的临时数据进行获取与分析，提取相关重要信息。

267. 内网，通俗的讲就是局域网，比如网吧，校园网，公司内部网等都属于此类。查看IP地址如果是在以下三个范围之内的话，就说明我们是处于内网之中的：10.0.0.0—10.255.255.255,172.16.0.0一172.31.255.255，192.168.0.0–192.168.255.255。

268. 内网穿透，构建内网隐蔽通道，从而突破各种安全策略限制，实现对目标服务器的完美控制。

269. 匿名者黑客组织是全球最大的黑客组织，也是全球最大的政治性黑客组织。这里聚集喜欢恶作剧的黑客和游戏玩家。他们支持网络透明，但常有人冒充他们的身份来发表一些虚假视频。“匿名者”是一个体系松散但规模庞大的国际黑客组织，黑客们大多出于对计算机的热爱加入其中。

270. 软件逆向工程又称软件反向工程，是指从可运行的程序系统出发，运用解密、反汇编、系统分析、程序理解等多种计算机技术，对软件的结构、流程、算法、代码等进行逆向拆解和分析，推导出软件产品的源代码、设计原理、结构、算法、处理过程、运行方法及相关文档等。

271. 旁注是最近网络上比较流行的一种入侵方法，在字面上解释就是一“从旁注入"，利用同一主机上面不同网站的漏洞得到webshell，从而利用主机上的程序或者是服务所暴露的用户所在的物理路径进行入侵。

272. 爬虫（又称为网页蜘蛛，网络机器人，更经常的称为网页追逐者），是一种按照一定的规则，自动地抓取万维网信息的程序或者脚本。

273. 票证传递攻击（PtT）是一种使用Kerberos票据代替明文密码或NTLM哈希的方法。PtT最常见的用途可能是使用黄金票证和白银票证

和白银票证。

274. 在访问控制中，票证是对客户端或服务的身份进行身份验证的数据，并与临时加密密钥（会话密钥）一起形成凭据。

275. 全双工通讯方式又称为双向同时通信，即通信的双方可以同时发送和接收信息的信息交互方式。

276. 区块链是一个信息技术领域的术语，从本质上讲，它是一个共享数据库，存储于其中的数据或信息，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征。基于这些特征，区块链技术奠定了坚实的“信任”基础，创造了可靠的“合作”机制，具有广阔的运用前景。

277. 肉鸡也称傀儡机，是指可以被黑客远程控制的机器。比如用"灰鸽子”等诱导客户点击或者电脑被黑客攻破或用户电脑有漏洞被种植了木马，黑客可以随意操纵它并利用它做任何事情。

278. 软件脱壳，顾名思义，就是利用相应的工具，把在软件“外面”起保护作用的“壳”程序去除，还原文件本来面目，这样再修改文件内容或进行分析检测就容易多了。

279. 弱口令，指那些强度不够，容易被猜解的，类似123,abc这样的口令（密码），容易被别人猜测到或被破解工具破解的密码均为弱口令。

280. 蠕虫病毒，它是一类相对独立的恶意代码，利用了互联网系统的开放性特点。通过可远程利用的漏洞自主地进行穿插，受到控制终醋会变成攻击的发起方，尝试感染更多的系统。蠕虫病毒的主要特性有：自我复制能力、很强的传播性、潜伏性、特定的触发性、很大的破坏性。

281. 所谓的“三次握手”：为了对每次发送的数据量进行跟踪与协商，确保数据段的发送和接收同步，根据所接收到的数据量而确认数据发送、接收完毕后何时撤销联系，并建立虚连接。

282. 沙箱是一种用于安全的运行程序的机制。它常常用来执行那些非可信的程序。非可信程序中的恶意代码对系统的影响将会被限制在沙箱内而不会影响到系统的其它部分。

283. 杀猪盘，网络流行词，电信诈骗的一种，是一种阿络交友诱导股票投资、赌博等类型的诈骗方式，“杀猪盘”则是“从业者们”自己起的名字，是指放长线“养猪”诈骗，养得越久，诈骗得越狠。

284. 社工库是黑客与大数据方式进行结合的一种产物，黑客们将泄漏的用户数据整合分析，然后集中归档的一个地方。

285. 社会工程学是黑客米特尼克悔改后在《欺骗的艺术》中所提出的，是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段。

286. 实体化编码，以“&”开头和以“;”结尾的字符串。使用实体代替解释为HTML代码的保留字符（&，<,>,”，不可见字符（如不间断空格）和无法从键盘输入的字符（如@）。

287. 水坑攻击，顾名思义，是在受害者必经之路设置了一个“水坑（陷阱）”。最常见的微法是，黑客分析攻击目标的上网活动规律，寻找攻击目标经常访问的网站的弱点，先将此网站“攻破”并植入攻击代码，一旦攻击目标访问该网站就会“中招”。

288. 水平越权指攻击者尝试访问与他拥有相同权限的用户资源。例如，用户A和用户B属于同一角色，拥有相同的权限等级，他们能获取自己的私有数据（数据A和数据B），但如果系统只验证了能访问数据的角色，而没有对数据做细分或者校验，导致用户A能访问到用户B的数据（数据B）。

289. 数字证书是指在互联网通讯中标志通讯各方身份信息的一个数字认证，人们可以在网上用它来识别对方的身份。因此数字证书又称为数字标识。数字证书对网络用户在计算机网络交流中的信息和数据等以加密或解密的形式保证了信息和数据的完整性和安全性。

290. “撕口子”（又称“打点”）：针对某薄弱环节，尝试通过漏洞利用或社工钓鱼等手段去获取外网系统控制权限。

291. 网络溯源是一种有效的对网络攻击的响应方式。对网络攻击的响应进行网络溯源，找到攻击源进行事故遏制和取证操作，从源头上解决网络攻击。

292. 态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。

293. 探针也叫作网络安全探针或者安全探针，可以简单理解为赛博世界的摄像头，部署在网络拓扑的关键节点上，用于收集和分析流量和日志，发现异常行为，并对可能到来的攻击发出预警。

294. 简称PAM。特权账户往往拥有很高的权限。一日失窃或被滥用会给机构带来非常大的网络安全风险。特权账户管理往往显得十分重要。其主要原则有：杜绝特权凭证共享、为特权使用赋以个人责任、为日常管理实现最小权限访问模型、对这些凭证执行的活动实现审计功能。

295. 跳板攻击是目前黑客进行网络攻击的普遍形式。目前的各类攻击，无论其攻击原理如何，采用何种攻击手法，其攻击过程大多要结合跳板技术，进行攻击源的隐藏。

296. 提权是指提高自己在服务器中的权限，主要针对网站入侵过程中，当入侵某一网站时，通过各种漏洞提升WEBSHELL权限以夺得该服务器权限。

297. 同源策略是一种约定，它是浏览器最核心也是最基本的安全功能，如果缺少了同源策略，则浏览器的正常访问都会受到影响，可以说 web是构建在同源策略的基础之上的，浏览器只是针对同源策略的一种实现。

298. 拖库本来是数据库领域的术语，指从数据库中导出数据。在网络攻击领域，它被用来指网站遭到入侵后，黑客窃取其数据库文件。

299. 外网，直接连入INTERNET（互联网），可以与互联网上的任意一台电脑互相访问，IP地址不是保留IP（内网）地址.。

300. 《中华人民共和国网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的法律。

301. 网络靶场，主要是指通过虚拟环境与真实设备相结合，模拟仿真出真实赛博网络空间攻防作战环境，能够支撑攻防演练、安全教育、网络空间作战能力研究和网络武器装备验证试验平台。

302. 网络钓鱼，攻击者利用欺骗性的电子邮件或伪造的 Web站点等来进行网络诈骗活动。诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，骗取用户的私人信息或邮件账号口令。

303. “网络黑产”即网络黑色产业链，是指利用互联网技术实施网络攻击、窃取信息、勒索诈骗、盗窃钱财、推广黄赌毒等网络违法行为，以及为这些行为提供工具、资源、平台等准备和非法获利变现的渠道与环节。

304. 网络空间测绘，用搜索引擎技术来提供交互，让人们可以方便的搜索到网络空间上的设备。相对于现实中使用的地图，用各种测绘方法描述和标注地理位置，用主动或被动探测的方法，来绘制网络空间上设备的网络节点和网络连接关系图，及各设备的画像。

305. 远程文件包含，(RFI）是一种黑客攻击，主要发生在网站上。如果管理员或网站建设者没有进行正确的验证，并且任何想要的人都可以将一个文件潜入系统，则会发生这种攻击。通过这种攻击，黑客将远程文件注入服务器，文件的内容会根据黑客的编码在服务器上造成严重破坏。

306. 网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

307. 网页仿冒是通过构造与某一目标网站高度相似的页面诱骗用户的攻击方式。钓鱼网站是网页仿胃的一种常见形式，常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式传播，用户访问钓鱼网站后可能泄露账号、密码等个人隐私。

308. 网页木马就是表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。

309. 网闸是使用带有多种控制功能的固态开关读写介质，连接两个独立主机系统的信息安全设备。由于两个独立的主机系统通过网闸进行隔离，使系统间不存在通信的物理连接、逻辑连接及信息传输协议，不存在依据协议进行的信息交换，而只有以数据文件形式进行的无协议摆渡。

310. 万能密码，通过在用户名或者密码处输入闭合SQL.语句的SQL字符串，拼接成一个结果为True的SQ1语句，从而绕过登陆限制。

311. 挖矿是对加密货币（比如比特币 Bitcoin）开采的一个俗称。开采比特币就像是求解一道数学题，最先得到答案，就获得相应的奖励。也指非法利用其他的电脑进行构建区块，间接为其生产虚拟货币。

312. “伪基站”即假基站，设备一般由主机和笔记本电脑或手机组成，通过短信群发器、短信发信机等相关设备能够搜取以其为中心、一定半径范围内的手机卡信息，利用2G移动通信的缺陷，通过伪装成运营商的基站，冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。

313. 未授权访问，顾名思义不进行请求授权的情况下对需要权限的功能进行访问执行。通常是由于认证页面存在缺陷，无认证，安全配置不当导致。常见于服务端口，接口无限制开放，网页功能通过链接无限制用户访问，低权限用户越权访问高权限功能。

314. 威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于资产相关主体对威胁或危害的响应或处理决策提供信息支持。根据使用对象的不同，威胁情报主要分为人读情报和机读情报。

315. 伪协议是为关联应用程序而使用的在标准协议(http://,https://.,ftp://）之外的一种协议。例如:file:///协议。

316. 文件上传漏洞是指未对上传文件的格式内容进行校验，恶意攻击者通过上传包含恶意代码的文件，从而攻击利用获得服务器的权限。

317. 物联网（IoT,Internet of things）即“万物相连的互联网”，是互联网基础上的延伸和扩展的网络，将各种信息传感设备与互联网结合起来而形成的一个巨大网络，实现在任何时间、任何地点，人、机、物的互联互通。

318. “无文件攻击”不代表真的没有文件，只是一种攻击策略，其出发点就是避免将恶意文件放在磁盘上，以逃避安全检测。所说的无文件，也未必是攻击全程无文件，而是其中的一部分采用了无文件攻击。

319. 信息泄露，泄露的系统信息或者调试信息可以帮助攻击者了解系统和制定攻击计划。信息泄露一般发生在程序使用输出或者日志功能的时候。

320. 心脏血漏洞是一个出现在加密程序库OpenSSL的安全漏洞，该程序库广泛用于实现互联网的传输层安全（TLS）协议。它于2012年被引入了软件中，2014年4月首次向公众披露。只要使用的是存在缺陷的OpensSSL实例，无论是服务器还是客户端，都可能因此而受到攻击。

321. 熊猫烧香是一种经过多次变种的计算机蠕虫病毒，2006年10月16日由25岁的中国湖北武汉新洲区人李俊编写，2007年1月初肆虐中国大陆网络，它主要透过网络下载的文件植入计算机系统。

322. 虚拟化简单讲，就是把一台物理计算机虚拟成多台理辑计算机，每个逻辑计算机里面可以运行不同的操作系统，相互不受影响，这样就可以充分利用硬件资源。

323. 所谓虚拟机逃递（Escape Exploit），指的是突破虚拟机的限制，实现与宿主机操作系统交互的一个过程，攻击者可以通过虚拟机逃逸感染宿主机或者在宿主机上运行恶意软件。

324. 羊毛党，网络流行语，源于1999年央视春晚小品《昨天·今天·明天》。薅羊毛，指利用规则漏洞或者通过钻研规则，在规则之内获取一些小利益，俗称占便宜。羊毛党便是对薅羊毛用户的戏称。

325. 延时注入属于盲注技术的一种，它是一种基于时间差异的注入技术，根据页面返回时同的长短进行判断数据库的信息。

326. 验证码绕过是指在认证过程中跳过验证码直接访问需要的界面内容，通常有以下几种方式，如响应包含验证码信息导致验证码绕过，验证码前段校验导致验证码绕过等等。

327. 应急响应是指在发生安全事件时对安全事件紧急排查、修复并对攻击进行溯源分析。

328. 影子账户是内部账户和外部账户的形式，主要起备查及处理不方便放在外部账户的费用的功能。“影子用户”一种指在网络应用中将网卡的MAC,IP地址修改为与别人的一模一样，然后接在同一个交换机的认证口下的终端用户。另一种指操作系统中影子账户。

329. 隐蔽通道是一种回避或进攻手段，用隐匿、未授权或非法方式来传输信息。互联网隐敲通道就像是一个带有秘密夹层的数字公文包，间谍会使用它来瞒过保安，将敏感文件放入安全设施，或从安全设施取出敏感文件。

330. 隐写，将信息地藏在多种载体中，如：视频、硬盘和图像，将需要隐藏的信息通过特殊的方式嵌入到载体中，而又不损害载体原来信息的表达。

331. 溢出，确切的讲，应该是“缓冲区溢出”。简单的解释就是程序对接受的输入数据没有执行有效的检测而导致错误，后果可能是造成程序崩溃或者是执行攻击者的命令。大致可以分为两类：堆溢出，栈溢出。

332. 一句话木马是一种基于BS结构的简短脚本，通过这个脚本，执行POST 来的任意参数语句，可以提交任意内容，黑客借此进行SQL注入或拿到SHELL写入大马或截取网站私密信息，达到注入非法信息等的目的。

333. 永恒之蓝（Eternal Blue）被影子经纪人公布到互联网上，一经发布便被多款恶意软件利用。包括肆虐的WannaCry,SMB虫EternalRocks 等。EternalBlue是在Windows的SMB服务处理SMB v1请求时发生的漏洞、这个漏洞导致攻击者在目标系统上可以执行任意代码。

334. 邮件网关是专门为邮箱打造的安全产品。邮件网关通过对邮件多维度信息的综合分析，可迅速识别APT 攻击邮件、钓鱼邮件、病毒木马附件、漏洞利用附件等威胁，有效防范邮件安全风险，保护企业免受数据和财产损失。

335. 远程文件包含，简称RFI，指服务利用程序文件包含函数包含远程文件，过滤不严导致可以包含服务器外的文件而导致问题产生。

336. 服务器端对用户提出的数据操作请求过分信任，忽略了对该用户操作权限的判定，导致恶意攻击者账号拥有了其他账户的增删改查功能。

337. 云计算（Cloud Computing）是分布式计算的一种，指的是通过网络“云”将巨大的数据计算处理程序分解成无数个小程序，然后，通过多部服务器组成的系统进行处理和分析这些小程序得到结果并返回给用户。

338. 预编译是指在创建数据库对象时就将指定的SOL 语句编译完成，这时SQL语句已经被数据库解析、审查，可有效防止SQL注入，因为预编译时预先已经将SOL的结构确定，在执行SQL语句时，结构也不会发生改变。

339. 鱼叉攻击是将用鱼叉捕鱼形象的引入到了网络攻击中，主要是指可以使欺骗性电子邮件看起来更加可信的网络钓鱼攻击，具有更高的成功可能性。不同于撒网式的网络钓鱼，鱼叉攻击往往更加具备针对性，攻击者往往“见鱼而使叉”。

340. 域控制器（Domain Controller，简称DC）是指在“域”模式下，至少有一台服务器负责每一台入网的电脑和用户的验证工作，相当于一个单位的门卫一样， DC是活动目录的存储位置，安装了活动目录的计算机称为域控制器。

341. 网域服务器缓存污染（DNS cache pollution）, 又称域名服务器缓存投毒（DNS cache poisoning） DNS 缓存投毒，是指一些刻意制造或无意中制造出来的域名服务器数据包，把域名指往不正确的P地址。

342. 域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假IP地址或使用户的请求失败。

343. 正向代理，意思是一个位于客户端和原始耶务器（Origin Server）之间的服务器，为了从原始服务器取得内容客户端向代理发送一个请求并指定目标（原始服务器）然后代理向原始服务器转交请求并将获得的内容返回给客户端。客户端才能使用正向代理。

344. 震网病毒又名Stuxnet 病毒、是个席卷全球工业界的病毒。作为世界上首个网络“超级破坏性武器”, Stuxnet 的计算机病毒已经感染了全球超过45000个网络，伊朗遭到的攻击最为严重，60%的个人电脑感染了这种病毒。

345. 中国蚁剑是一款开源的路平台网站管理工具，它主要面向于合法授权的渗透测试安全人品以及进行常规操作的网站管理员。是一款非常优秀的Webshell管理工具。

346. 中间件是介于应用系统和系统软件之间的一类软件，它使用系统软件所提供的基础服务（功能），衔接网络上应用系统的各个部分或不同的应用，能够达到资源共享、功能共享的目的。

347. 中间人攻击是一种“间接”的入侵攻击，这种攻击方式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，通过拦截正常的网络通信数据，并进行数据篡改和嗅探，而这台计算机就称为“中间人”。

348. 撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户。很多用户在不同网站使用的是相同的账号密码，因此黑客可以通过获取用户在A网站的账户从而尝试登录B网址，这就可以理解为撞库攻击。

349. 子域名（或子域英语：Subdomain）是在域名系统等级中，属于更高一层域的域。比如mail.example.com和calendar.example.com是example.com的两个子域，而example.com则是顶级域.com的子域。