**单选题：**

1.我国，中央网络安全和信息化领导小组第一次会议于哪一年召开（B）

A.2013年 B.2014年 C.2015年 D.2016年

2.全球的13台根域名服务器由哪个机构统一管理（A）

A.ICANN B.IEEE C.ISO D.CNCERT

3. 永恒之蓝”的攻击工具是从哪个组织泄漏出来？(A)

A.美国NSA B.英国军情五处 C.国内安全公司 D.微软公司

4. 著名的WannaCyr是什么类型恶意代码(D)

A.后门程序 B.挖矿程序 C.APT攻击程序 D.勒索程序

5. 以下哪部法律是我国保障网络安全的基本法？（D）

A.《国家安全法》B.《保密法》C.《治安管理处罚法》D.《中华人民共和国网络安全法》

6. 《中华人民共和国网络安全法》正式实施的日期是以下哪个选项？（C）

A.2016年11月7日 B.2016年12月7日 C.2017年6月1日 D.2017年6日

7. 新浪微博攻击事件是因为（B）

A.撞库攻击 B.XSS C.SQL注入 D.文件上传

8. 以下哪个选项是对TCP/IP模型的传输层（运输层）功能的准确描述？(C)

A,主要负责处理与电缆（或其他任何传输媒介）的物理接口细节

B,主要处理分组在网络中的活动

C,主要为两台主机上的应用程序提供端到端的通信

D.负责处理特定的应用程序细节

9. 以下哪一项不属于HTTP 1.1版本的主要请示方式？(B)

A.GET B.Body C.HEAD D.TRACE

10. 以下哪个选项是询问服务器支持哪些请求方法？(D)

A.GET B.POST C.HEAD D.OPTIONS

11. 以下哪个选项的状态码（数字）代表请求资源的访问被服务器拒绝了。(C)

A.200 B.404 C.403 D.503

12. 以下哪个选项的状态码（数字）类别代表本次请求错误原因主要是由客户端侧引起的(B)

A.3XX B.4XX C.5XX D.1XX

13. HTTP请求报文的请求首部是从客户端往服务器发送请求报文中所使用的字段，以下哪个首部字段的含义代表了客户端操作系统、浏览器等其他信息？(B)

A.Host B.User-agent C.Referer D.Cookie

14. TLS协议协商过程中，客户端向服务端展示可支持的密码套件，是以下哪个阶段？(B)

A.ServerHello B.ClientHello C.ChangeCipherSpec D.ClientKeyExchage

15. 在Kali操作系统中，既属于“数据库评估工具”，又属于“漏洞利用工具”的是（A）

A,Sqlmap B,Nmap C,Wireshark D,Hydra

16. Kali是基于（A）Linux的发行版。

A,Debian B,CentOS C,Fedora D,openSUSE

17. WAMP Server搭建的网站默认情况下只有本地访问权限，如果要开通远程访问权限，则应该将Apache配置文件中<Directory “${INSTALL\_DIR}/www/”>标签下的“Require local”修改成（C）。

A,Require all denied B, Require all accepted

C, Require all granted D, Require all allowed

18. 在Nmap中，可以利用（A）选项指定扫描过程中所用的NSE脚本名称。

A,--script B,--script-name C,--script-args D,--script-file

19. 在Nmap中，用于操作系统侦测的选项是（B）。

A,-T B,-O C,-OS D,-W

20. 在Nmap端口扫描相关的选项中，（D）单独使用时，主要用于探测防火墙是否对目标端口进行了过滤，而无法用于判定端口是否处于开放状态。

A,-sP B,-sS C,-sT D,-sA

21. 当Nmap向目标端口发送TCP SYN报文后，如果收到了目标回复的（D）报文，则可以判定目标端口处于开放状态。

A,TCP ACK B,TCP FIN C,TCP RST+ACK D,TCP SYN+ACK

22. 某用户利用Nmap执行了以下命令： nmap -p 80 -sS 192.168.1.200 那么，Nmap将采用（A）方式对目标机192.168.1.200的TCP 80端口进行扫描。

A,TCP SYN B,TCP connect C,TCP ACK D,TCP FIN

23. 使用-sP或-sn选项扫描跨网段目标主机时，Nmap会默认发送4个报文用于探测，以下哪个选项不属于这4个默认报文之一？（C）

A,发往目标IP的ICMP ECHO请求报文

B,发往目标IP的ICMP TIMESTAMP请求报文

C,发往目标80端口的TCP SYN报文

D,发往目标80端口的TCP ACK报文

24. 在局域网内（即Nmap主机和目标机在同一个局域网中），无论采用哪一种选项，Nmap都是通过（D）报文来进行主机发现的。

A,ICMP ECHO B,TCP SYN C,DHCP D,ARP

25. 以下BurpSuite模块中，（C）模块最适合用于对网站登录凭证实施暴力破解。

A,Proxy B,Repeater C,Intruder D,Sequencer

26. 作为BurpSuite中一款手工验证HTTP消息的测试工具，（B）模块通常用于多次重放请求响应和手工修改请求消息及修改后对服务器端响应的消息分析。

A,Proxty B,Repeater C,Intruder D,Sequencer

27. BurpSuite基于（C）语言开发。

A,Perl B,Python C,Java D,Rudy

28. 以下选项均为Metasploit中meterpreter模块的常用命令，可用于查看当前目标机上运行的进程列表的命令为（B）。

A,getuid B,ps C,shell D,execute

29. ms17-010漏洞，即我们熟知的“永恒之蓝”，从本质上说是一种（C）漏洞。

A,SQL注入 B,XSS C,缓冲区溢出 D,文件解析

30. 在msf终端下，可以用（D）命令查看某模块需要设置哪些参数。

A,display parameters B,show parameters

C,display options D,show options

31. 利用Metasploit进行渗透测试的一般流程 环节包括：①选择一种编码技术（encoders），用来绕过杀毒软件的查杀；②选择并配置一个渗透攻击（漏洞利用）模块（exploits）；③执行渗透攻击；④选择并配置一个攻击载荷模块（payloads）；⑤扫描目标机系统，寻找可用漏洞；⑥后渗透阶段的操作。 下列选项中，流程顺序正确的是（C）。

A,⑤④①②③⑥ B, ⑤①②④③⑥

C,⑤②④①③⑥ D, ⑤②①④③⑥

32. 在msf终端下，选择使用某一模块的命令为（C）。

A,choose B,maintain C,use D,load

33. 用于初始化数据库并启动msf终端的命令是（A）。

A,msfdb init && msfconsole B,msfdb start && msfconsole

C,db init &&msfconsole D,db start && msfconsole

34. Metasploit系统模块中，（D）模块主要用于在渗透攻击取得目标系统远程控制权之后，在受控系统中进行各式各样的后渗透攻击动作，比如获取敏感信息、进一步横向拓展、实施跳板攻击等。

A,auxiliary B,exploits C,evasion D,post

35. Metasploit基本命令行对应的文件是（D）。

A,msfd B,msfdb C,msfrpc D,msfconsole

36. 在Firefox浏览器的插件中，（C）可用于分析目标网站所采用的平台构架、网站环境、服务器配置环境、JavaScript框架、编程语言等参数。

A,FoxyProxy B,Hackbar C,Wappalyzer D,HTTP Header Live

37. 在Firefox浏览器的插件中，（B）可用于改变HTTP头部中的某字段，以实现隐藏（伪装）客户端浏览器信息的目的。

A,FoxyProxy B,User-Agent Switcher C,Hakbar D,HTTP Header Live

38. 在Firefox浏览器的插件中，（A）能够提高Firefox的内置代理的兼容性，可基于URL的参数在一个或多个代理之间进行切换。

A,FoxyProxy B,User-Agent Switcher C,Hakbar D,HTTP Header Live

39. 在Kali终端输入（C）命令即可启动SET。

A,set B,setool C,setoolkit D,setool start

40. SET（Social Engineering Toolkit）是Kali Linux中集成的一款社会工程学工具包，它是一个基于（D）语言的开源社会工程学渗透测试工具。

A,Perl B,PHP C,Java D,Python

41. 利用Crunch生成长度为3的字典集，第一位为数字，第二位为特殊字符，第三位是小写字母，并输出到/usr/pass.txt。应输入以下哪条命令实现？（B）

A,crunch 3 3 -t %@^ -o /usr/pass,txt

B,crunch 3 3 -t %^@ -o /usr/pass,txt

C.crunch 3 3 -t %,^ -o /usr/pass,txt

D.crunch 3 3 -t %^, -o /usr/pass,txt

42. 利用Crunch生成长度为6、以123元素为组合的字典集，并输出到/usr/number.txt。应输入以下哪条命令实现？（C）

A,crunch 6 123 -o /usr/number.txt

B,crunch 123 6 -i /usr/number.txt

C.crunch 6 6 123 -o /usr/number.txt

D.crunch 6 6 123 -i /usr/number.txt

43. 在Hydra中，可以用（D）选项指定用于存储密码的字典。

A,-I B,-L C,-p D,-P

44. 在Hashcat中，（D）文件记录了近期Hashcat破解的所有Hash值和密码明文的对应关

系。

A,hashcat.conf B,hashcat.dictstat2

C,hashcat.crached D,hashcat.potfile

45. 已知目标密码为8位字符串，其中前4位为小写字母，后4位为数字，利用Hashcat对其进行掩码暴力破解时，可以使用下列哪个选项的掩码？（C）

A,?l?l?d?d B,?u?u?d?d

C,?l?l?l?l?d?d?d?d D,?u?u?u?u?d?d?d?d

46. 在Hashcat中，可以用（B）选项指定Hash类型。

A,-c B,-m C,-a D,-o

47. 在Hashcat中，可以用（C）选项指定破解模式。

A,-c B,-m C,-a D,-o

48.OWASP ZAP以架设代理的形式来实现渗透性测试。它将自己置于用户浏览器和服务器中间，充当一个中间人的角色，浏览器与服务器的所有交互都要经过ZAP，这样ZAP就可以获得所有交互的信息，并且可以对它们进行分析、扫描，甚至是改包再发送。从这点上讲，OWASP ZAP与下列哪款工具软件的功能有相似之处？（D）

A,Wireshark B,Nmap C,Metasploit D,Burpsuite

49. Nikto是一款基于（B）语言开发的开源Web扫描评估软件。

A,C B,Perl C,Python D,Java

50. 在AWVS 14中，在（A）菜单下可以设置扫描对象的相关参数，如IP地址、描述信息等。

A,Target B,Vulnerabilities C,Scan D,Reports

51. 微软为安全漏洞设置了4个风险等级，从低到高依次为低危、中危、（ ）和（C）。

A,高危、超危 B,高危、严重 C,重要、严重 D,重要、高危

52. 在网络安全领域，“0day”指的是（D）。

A,未被发现的漏洞 B,刚刚发现的漏洞

C,尚未公布的漏洞 D,被发现但尚未发布补丁的漏洞

53. 如果要利用Weevely生成一个专用木马a.php（连接密码设为1234）并保存至/usr路径下，则需要在Kali终端执行以下哪条命令？（D）

A,weevely /usr/a.php 1234

B,weevely 1234 /usr/a.php

C,weevely generate /usr/a.php 1234

D,weevely generate 1234 /usr/a.php

54. 在渗透测试过程中，“利用Nessus、Nmap等工具对目标系统进行端口及漏洞扫描”事项，应在（B）阶段完成。

A,前期交互 B,信息收集 C,漏洞分析 D,后渗透攻击

55. 在渗透测试过程中，“确定渗透测试的范围和目标”事项，应在（A）阶段完成。

A,前期交互 B,信息收集 C,威胁建模 D,渗透攻击

56. “把测试对象看作一个打开的盒子，测试人员依据测试对象内部逻辑结构相关信息，设计或选择测试用例。”从这段描述中可以看出，渗透测试人员所用的方法为（B）。

A,黑盒测试 B,白盒测试 C,灰盒测试 D,隐秘测试

57. 渗透测试的“后渗透攻击”阶段通常从（D）开始。

A,制定了渗透测试方案并交于客户审核通过后

B,取得了客户对渗透测试的授权之后

C,在客户组织的系统中检测到一些已知的了漏洞之后

D,已经攻陷了客户组织的一些系统或取得域管理员权限之后

58.(C）是一种通过模拟攻击的技术与方法，挫败目标系统的安全控制措施并获得控制访问权的安全测试方法。

A,APT B,功能测试 C,渗透攻击 D,风险测试

59. 以下哪种方式能实现域名到域名的映射功能？（C）

A,A B,AAAA C,CNAME D,TXT

60. 以下哪一项不是子域名信息收集的原因？(C)

A,在测试范围内发现更多的域或子域，增加漏洞发现的概率

B,发现被遗忘的子域名资产存在的安全薄弱面

C,确定子域名是否与私网址对应

D,寻找不同类别资产的共性风险

61. 以下哪一项不是C段信息收集的原因？（D）

A,收集C段内属于测试范围的目标IP地址

B,发现非域名映射的存活网络资产

C,发现更多的网络资产

D,以上选项均不正确

62. 为了防止网络爬虫爬去网站敏感路径，通常采用“网络爬虫排除”协议，在网站根目录下新建一个文档文件，以下哪个选项通常是这个文件的正确明称？（D）

A,reboot.txt B,rebots.txt C,crawler.txt D,robost.txt

63. 以下哪个选项是nmap工具对服务版本探测的配置参数？（B）

A,参数“-sS” B,参数“-sV” C,参数“-Pn” D,参数“-O”

64. 以下哪个选项能精准搜索pdf文件类型的语法？（C）

A,cache:pdf B,info:pdf C,fileype:pdf D,以上选项均不正确

65. Google的搜索语法能实现指定网站进行内容搜索，以下哪个语法字段是实现这一功能的选项？（C）

A,cache B,fileype C,site D,info

66. 下列不属于命令执行漏洞的危害的是（D）

A,反弹shell B,内网穿透 C,读写文件 D,盗取账号

67. 可能造成远程命令执行的函数有（A）

A,eval B,system C,popen D,exec

68. 以下哪种方法不能执行命令（C）

A,system(whoami); B,sysrem(‘whoami’)

C,system(‘eval(whoami);’); D,eval(‘system(whoami);’);

69. MySQL数据库（5.5以上版本）中哪个系统数据库保存着MySQL服务器所维护的所有其他数据库的信息？（D）

A,sys B,performance\_schema C,mysql D,information\_schema

70. 以下哪条指令配合select可用于显示指定条目的数据项？（A）

A,limit B,group by C,order by D,union select

71. 在SQL语法中，用于修改表中某数据项的命令是（C）。

A,alter B,modify C,update D,insert

72. MySQL数据库的默认服务端口号为（C）。

A,1433 B,1521 C,3306 D,5432

73. 以下哪种属于非关系型数据库？（C）

A,MySQL B,SQL Server C,Mongodb D,Oracle

74. 某网站index.php文件中存在下面一段代码： $id=$\_GET['id']; $sql="SELECT \* FROM users WHERE id=('$id') LIMIT 0,1"; 攻击者设置SQL注入payload时，可利用下列哪种符号实现语句闭合？（D）

A,单引号‘ B,双引号“ C,括号) D,单引号+口号’)

75. 某网站index.php文件中存在下面一段代码： $id=$\_GET['id']; $sql="SELECT \* FROM users WHERE id='$id' LIMIT 0,1"; 该网站极有可能存在（B）注入点。

A,数字型 B,字符型 C,搜索型 D,cookie型

76. 以下哪条查询语句将导致“万能密码”登录？（C）

A,select username,password from users where username=’textvalue’ and 1=2

--’and password=’textvalue2’

B,select username,password from users where username=’textvalue’ and password=’textvalue2’and 1=2 –'

--’and password=’textvalue2’

C,select username,password from users where username=’textvalue’or 1=1

--‘and password=’textvalue2’

D,select username,password from users where username=’textvalue’and password=’textvalue2’or 1=1 –’

77. 函数updatexml(p1,p2,p3)中有三个参数p1、p2、p3，利用updatexml进行报错注入时，攻击者可在哪个参数位置设置payload？（B）

A,p1 B,p2 C,p3 D,p1、p2、p3处均可设置payload

78. 假如数据库管理员利用root账户登录MySQL，并执行了下列命令： select extractvalue(1,concat('~',user())); 该条命令的执行结果为（D）。

A,正常显示：“root@localhost“

B,显示错误：You have an error in your SQL suntax;check the manual that corresponds to your MySQL server version for the right syntax to use near ‘~’at line 1

C,显示错误：XPATH syntax error:’root@localhost’

D,显示错误：XPATH syntax error:’~root@localhost’

79. 在MySQL数据库中执行下列命令： select left('a1b2c3',2); 该命令执行后的返回结果是（A）。

A,a1 B,ab C,c3 D,bc

80. 已知某Web服务器存在HTTP头部注入点，正常的HTTP头部字段User-Agent信息为： Mozilla/5.0 Firefox/60.0 后端PHP文件中存在的以下代码： insert into security.uagents ('uagent', 'ip\_address', 'username') values ('$uagent', '$IP', '$uname'); 那么，攻击者通过某种方式将HTTP头部字段User-Agent信息修改为（ ），则可以实现注入，获取网站当前所在数据库的库名。（D）

A,Mozilla/5.0Firefox/60.0 and extractvalue(1,concat(‘~’,(select

database()))),”)

B,Mozilla/5.0Firefox/60.0’ and extractvalue(1,concat(‘~’,(select

database()))),”)#

C,Mozilla/5.0Firefox/60.0 and extractvalue(1,concat(‘~’,(select

database()))),”,”)

D, Mozilla/5.0Firefox/60.0’ and extractvalue(1,concat(‘~’,(select

database()))),”,”)#

81. 假如某Web服务器会对HTTP报文头部某字段内容进行获取，用以验证客户端的身份。那么，该Web服务器最有可能存在以下哪种HTTP头部注入点？（A）

A,Cookie B,Referer C,User-Agent D,XFF

82. 在SQLMAP中，哪个参数可用于从文件（如文本文档）中取出保存的HTTP请求包进行检测？（A）

A,-r B,-u C,-l D,-m

83. 在SQLMap中使用sqlmap -u http://192.168.0.63:8083/show.php?id=33 -D cms --tables命令可达到什么效果？（B）

A,得到该服务器上的数据库名称

B,得到该服务器上cms数据库的表信息

C,得到该服务器上cms表的字段信息

D,得到该服务器上cms字段的内容

84. SQLMAP是用（C）语言开发的自动化SQL注入工具。

A,Perl B,PHP C,Python D,Java

85. 安全运营中心产品，以什么为核心？（C）

A,漏洞 B,管理 C,资产 D,事件

86. SIEM产品不包含下面哪项主要功能（D）

A,安全事件管理 B,安全信息管理 C,日志管理 D,安全态势感知

87. 在安全运营中，数据处理流程是(B)

A,input-output-filter B,input-filter-output

C,filter-input-output D,ourput-filter-input

88. 在安全运营中数据采集的常用手段不包含(D)

A,syslog B,snmp C,agent收集 D,smb共享

89. 下面哪项是IT部门无法为SOC提供的（C）

A,CMDB B,网络拓扑 C,威胁检测 D,补丁管理

90. 在一个7X24小时运行的安全运营中心，建议使用多少人来满足运营的要求（B）

A,5-6人 B,8-12人 C,6-8人 D,12-16人

91. 自动化基线检查的缺点是（A）

A,可能造成未知影响 B,检查速度慢 C,检查时间长 D,检查非常不准确

92. 用户账户控制位于组策略的（A）

A,安全选项 B,用户权限分配 C,审核策略 D,账户策略

93. windows基线自动化检查主要通过（A）

A,注册表 B,控制面版 C,设置 D,组策略

94. windows基线人工配置的主要通过（D）

A,注册表 B,控制面版 C,设置 D,组策略

95. 在基线管理中，Linux路径/etc/passwd的权限默认应配置为哪项合适（C）

A,777 B,666 C,644 D,664

96. 在基线管理中，Linux路径/var/log下的日志文件权限默认应配置为哪项合适(B)

A,400 B,600 C,440 D,660

97. windows操作系统中，使用哪个工具可以看到进程运行的选项（D）

A,任务管理器 B,注册表 C,tasklis命令 D,wmic process命令

98. linux系统中/etc/rc5.d的文件夹的作用是（C）

A,用户模式下的开机启动脚本 B,完全命令行模式下的启动脚本

C,图形模式下的启动脚本 D,所有模式下的启动脚本

99. linux操作系统默认的wheel组的作用是（A）

A,允许用户以sudo执行命令 B,不允许用户以root权限执行命令

C,允许用户修改自己的密码 D,不允许用户修改自己的密码

100. linux系统中last命令的作用是（B）

A,显示运行命令的历史纪录 B,显示用户最后登录时间

C,显示计算机上次关机时间 D,执行上一条命令

101. linux下使用find命令的哪个选项可以查找修改时间小于1天的文件（A）

A,mitme B,ctime C,atime D,dtime

102. linux下使用哪个命令可以查看二进制文件中的字符串(C)

A,cat B,more C,stings D,tali

**多选题：**

1. 我国网络强国战略的近期目标包含（A,B,C,D,E）

A.技术强 B.基础强 C.内容强 D.人才强 E.国际话语强

2. 以下哪些是APT攻击的特征（A,B,C,D,E）

A.潜伏性 B.持续性 C.单点隐蔽性 D.攻击渠道多样性 E.针对特定目标

3. 以下哪些选项是我国网络安全法做了明确规定？（A,B,C,D）

A.国家实行网络安全等级保护制度

B.用户接入网络，实行实名制度

C.对关键信息基础设施的保护

D.数据保护设计个人信息保护、用户信息保护和商业秘密保护等

4. 以下哪些选项是我国网络安全法解决的基础性问题？（A,B,C,D）

A.基本原则：网络空间主权原则、网络安全与信息化发展并重原则、共同治理原则

B.明确了政府各部门的职责权限，完善了网络安全监管体制

C.强化网络运行安全，重点保护关键信息基础设施

D.将监测预警与应急处置措施制度化、法制化

5. 早期Web站点入侵的方式有哪些（A,C）

A.歪曲网站内容 B.脱裤 C.暗链 D.上传脚本

6. 中国黑客的发展经过了哪些时代（A,B,C）

A.启蒙时代 B.黄金时代 C.信息时代 D.黑暗时代

7. 万维网（WWW）由以下哪几项技术主要构成？（A,C,D）

A,超文本标记语言（HTML） B,UDP协议

C,超文本传输协议（HTTP） D,统一资源定位符（URL）

8. 以下哪些选项，是对管线技术正确的描述？(A,B,C)

A.在持久连接技术之上发展而来，之前是发送一个请求，响应后，才能发送下一个请求。

B.管线技术，客户可以一次发送多个请求，同时接收多个响应。

C.管理技术，并发传输，进一步提升了资源的效率，内容显示更快。

D.管线技术在传输层使用协议是UDP协议。

9. 以下哪些选项是HTTP协议常见的请求方式？(A,B,C,D)

A.GET B.POST C.HEAD D.OPTIONS

10. HTTP报文首部有通用首部字段和实体首部字段，以下哪些选项属于实体首部字段？(A,B,C)

A,Allow B,Content-Language C,Content-Length D,Connection

11. TLS协议协商过程（Handshake Protocol）中的服务器会回复客户端一个ServerHello包，以下哪些选项可能是该包包括的内容？(A,B,C,D)

A.服务器的随机数 B.会话ID C.选定的密码套件 D.数据压缩方式

12. 在Kali操作系统中，具有密码破解功能的工具包括（ A,B,D）。

A,John B,Hashcat C,Wireshark D,Ophcrack

13. Kali操作系统中包含的渗透测试或安全审计工具都有哪些功能？（A,B,C,D）

A,信息收集 B,密码攻击 C,逆向工程 D,嗅探欺骗

14. 在终端命令行中输入（B,C）命令，可立即关闭Kali操作系统。

A,shutdown -r now B,shurdown -h now C,init 0 D,init 6

15. PHPstudy是一个PHP调试环境的程序集成包，它包含了以下哪些组件？（A,B,C,D）

A,Apache B,MySQL C,phpMyAdmin D,Pycharm

16. 以下哪些选项属于“Apache+MySQL+PHP”的程序集成包？（B,C）

A,Pycharm B,PHPstudy C,WAMP Server D,phpMyAdmin

17. Nmap支持的主机发现方法包括（A,B,C,D）。

A,TCP ACK B,ICMP ECHO C,TCP SYN D,ICMP TIMESTAMP

18. BurpSuite的Intruder模块支持下列哪些payload类型？（A,B,C,D）

A,简单列表(Simple list) B,自定义迭代器(Cusrom iterator)

C,递归提取(Recurxive grep) D,运行时文件(Runtime file)

19. BurpSuite的Intruder模块，哪些攻击模式可用于“多个攻击位置，多个payload集合”的场景？（C,D）

A,狙击手模式(Sniper) B,攻城锤模式(Battering ram)

C,草叉模式(Pitchfork) D,集束炸弹模式(Cluster bomb)

20. BurpSuite可以使用下列哪些语言编写的扩展插件？（A,C,D）

A,Java B,Perl C,Ruby D,Python

21. BurpSuite的Proxy模块可以对（B,C）协议报文进行拦截、修改和转发。

A,DNS B,HTTP C,HTTPS D,SMTP

22. BurpSuite包含下列哪些功能模块？（A,B）

A,Proxy B,Repeater C,Encorder D,Meterpreter

23. Hackbar V2能够提供以下哪些漏洞的测试攻击payload？（A,B,C,D）

A,XSS B,SQL注入 C,XXE D,本地文件包含

24. SET支持的攻击方法包括（A,B,C,D）。

A,收集网站认证信息 B,E-mail钓鱼攻击 C,二维码攻击 D,Java Applet攻击

25. 常见的社会工程学攻击方式包括（A,B,C,D）。

A,引诱 B,伪装欺骗 C,恐吓 D,恭维

26. Hashcat支持的散列算法包括（A,B,C,D）。

A,LM B,NTLM C,SHA2-224 D,SHA2-256

27. 常用的Hash算法包括（B,D）。

A,AES B,MD5 C,RSA D,SHA1

28. 以下哪些版本的AWVS为Web版？（C,D）

A,AWVS 9 B,AWVS 10 C,AWVS 11 D,AWVS 12

29. CVSS（Common Vulnerability Scoring System，通用漏洞评分系统）是一种行业公开标准，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。CVSS对漏洞的评分标准包括以下哪些指标？（B,C,D）

A,利用难度评估指标 B,基本评估指标

C,时效性评估指标 D,环境评估指标

30. 蚁剑的常用功能包括（A,C,D）。

A,虚拟终端 B,磁盘分区操作 C,数据操作 D,文件管理

31. “蚁剑”程序由两部分组成，分别是（ ）和（ ）。一个是项目核心源码antSword，另一个是加载器（B）

A,控制端，服务端

B,项目核心源码，加载器

C,Webshell生成器，控制端

D,项目核心源码，Webshell生成器

32. 常见的Webshell管理工具包括（A,B,C）。

A,”菜刀” B,“蚁剑” C,“冰歇” D,“灰鸽子”

33. 在渗透测试的“渗透攻击”阶段，针对目标系统实施深入研究和测试的渗透攻击，主要包括（B,C,D）。

A,漏洞扫描 B,检测和防御机制绕过 C,触发攻击响应控制措施 D,渗透代码测试

34. 关于渗透测试和APT的区别，下列说法正确的是（A,B,D）。

A,从目前的上看，渗透测试的目的是评估计算机网络系统的安全性，而APT的目的则是对高价值目标进行有组织、长期持续性的控制

B,从手段方法上看，渗透测试通过被允许的行为模拟黑客攻击来对目标系统进行测试，而APT则利用各种高科技手段进行攻击

C,从执行主体上看，渗透测试一般由个人来实施，而APT则一般由一个组织来实施

D,从结果上看，渗透测试提高了目标系统的安全级别，而APT在达成目的的过程中一般会给目标系统带来严重损失

35. 关于渗透测试的原则，下列说法正确的是（C,D）。

A,应随机选择测试目标

B,应严格控制熟悉范围，秘密实施测试

C,应选择不影响业务系统正常运行的攻击方法

D,应符合测试规范和法律要求

36. 渗透测试标准将渗透测试过程分为七个阶段，以下选项中属于这七个阶段的有（A,B,D）。

A,信息收集阶段 B,渗透攻击阶段 C,清楚痕迹阶段 D,报告阶段

37. 撰写渗透测试报告的主体部分时，有哪些要求？（A,B,D）

A,列举渗透测试过程中发现的所有漏洞

B,列举发现漏洞所使用的工具、payload、exp、影响范围和存在的隐患或危害内容

C,可以直接复制粘贴漏洞扫描器的检测结果

D,必须给出漏洞修复建议

38. 撰写渗透测试报告的内容摘要部分时，有哪些要求？（B,D）

A,尽可能体现渗透测试的细节

B,明确指出客户所要求测试的系统是否安全

C,应列举渗透测试过程中所使用的工具和技术

D,让客户明白渗透测试过程中做了什么，以及接下来要做什么

39. 编写渗透测试报告的两大宗旨及难点是（B,C）。

A.如何复现漏洞

B.如何准确定位问题

C.如何让甲方意识到问题的严重

D.如何运用自己的专业知识

40. 渗透测试报告必须具备的品质包括（A,B,C）。

A,满足甲方需求B,简单明了，直击要害C,尽可能通俗易懂D,尽可能复详细

41. 下列选项中，哪些是信息收集的常见方式？（A,B,C,D）

A,DNS信息收集 B,子域名 C,C段 D,”指纹”识别

42. 以下哪些选项是“钓鱼”攻击的特点？（A,B,C）

A,可通过邮件、连接、办公文件承载体、实现攻击

B,主要的攻击方式由鱼叉和水坑攻击

C,可绕过传统边界设备的防护投机

D,以上答案均不正确

43. 以下哪些选项是DNS支持的常见查询种类？(A,B,C,D)

A,A B,AAAA C,NS D,MX

44. 以下哪些选项可以通过搜索引擎查询子域名？（A,B,C）

A,指定查询网站的site语法（特定搜索引擎）

B,theharvester工具

C,aquatone工具

D,以上选项均不正确

45. 以下哪些选项可能实现子域名信息收集？（A,B,C,D）

A,子域名爆破 B,搜索引擎搜索 C,域传输漏洞 D.域名查询网站

46. 在使用“Nmap –sn –PE -n 192.168.1.1/24 –oX out.xml”命令扫描C段时，以下哪些选项说法正确？（A,B,C）

A,字段“sn”代表不扫描端口

B,字段“PE”代表采用ICMP方式进行探测

C,字段“n”代表不进行DNS解析

D,以上选项均不正确

47. 以下哪些工具可以实现web目录扫描测试?(A,B,C)

A,dirb B,dirbuster C,御剑 D,以上选项均不正确

48. 以下哪些选项是Web目录扫描测试可以实现的？（A,B,C）

A,发现网站后台管理页面B,发现未授权页面C,发现网站隐藏页面D,以上选项均不正确

49. 以下哪些选项可能提取到中间件相关信息（指纹）？（A,B,C）

A,http返回消息中server字段

B,端口服务探测中间件

C,在构造错误的返回界面查看中间件信息

D,以上选项均不正确

50. 以下哪些选项是可以通过网络空间搜索引擎完成搜索的？(A,B,C,D)

A,摄像头设备 B,打印机设备 C,路由器设备 D,红绿灯设备

51. 以下哪些选项是常见的网络空间搜索引擎？（A,B,C）

A,shodan B,zoomeye C,fofa D,bing

52. 下列属于文件包含函数的是（A,B,C,D）

A,include B,include\_once C,require D,require\_once

53. 命令执行常见的场景有哪些（A,B,C,D）

A,ping主机 B,DNS请求 C,Office文档 D,框架缺陷

54. 以下属于XSS漏洞的危害的是（A,B,D）

A,盗取账号 B,劫持会话 C,脱裤 D,刷流量

55. 以下常用于XSS漏洞验证的弹窗语句是（A,B,C）

A,alert B,confirm C,prompt D,console.log

56. 在MySQL中，已知非空表users有4个字段id、name、passwd和address；非空表result有3个字段id、name和score。数据库管理员想通过联合查询的方式同时查看users表的name、passwd和result表的score字段内容，以下哪些命令可以达到预期的效果？（C,D）

A,select \* from users union select \* from result

B,select name,passwd from users union select \* from result

C,select 1,name,passwd from users union select \* from result

D,select name,passwd from users union select 1,score from result

57. 在MySQL中，已知非空表users有4个字段，按顺序分别为id、name、passwd和address，数据库管理员执行了以下命令： select id,name,passwd from users order by N; 其中N为正整数，当N为下列哪些值时，上述命令能够正常执行（不报错）？（A,B）

A,2 B,3 C,4 D,5

58. 假如MySQL数据库的登录用户名为root，密码为pass123，在本地用命令行方式连接MySQL数据库的命令为（B,C）。

A,mysql -h 127.0.0.1 -u root -p pass123

B,mysql -h 127.0.0.1 -u root -p

C,mysql -h 127.0.0.1 -uroot -ppass123

D,mysql -h 127.0.0.1 -u -p

59. 如果POST参数处存在SQL注入点，则可以通过下列哪些方式修改POST数据包实现注入？（B,C）

A,在浏览器导航栏中修改POST数据包

B,利用Hackebar插件修改POST数据包

C,利用Burpsuite工具拦截和修改POST数据包

D,利用HTTP Header Live插件修改POST数据包

60. 已知某网站后台数据库为MySQL，页面http://www.testweb.com/user.php?id=8存在数字型注入点，查询字段数为3，且有3个回显位。如果攻击者直接通过在浏览器地址栏中调整参数对网站进行注入，那么他可以利用下列哪些语句获取网站当前的数据库库名？（A,C）

A,http://www.testweb.com/user.php?id=8 and 1=2 union select 1,2,database()

B, http://www.testweb.com/user.php?id=8‘and 1=2 union select 1,2,database()

--+

C, http://www.testweb.com/user.php?id=8 and 1=2 and extractvalue(1,concat

(‘~’,(select database())))

D, http://www.testweb.com/user.php?id=8 and 1=2 and extractvalue(1,concat

(‘~’,(select database())))--+

61. 在MySQL数据库中，以下哪些函数具有报错功能？（A,D）

A,exp B,benchmark C,substr D,name\_const

62. 已知某网站后台数据库为MySQL，攻击者向网站服务器提交了3条payload： （1）http://www.testweb.com/user.php?id=8' and if((length(database())>3),sleep(5),1)--+，执行后页面有明显的延迟； （2）http://www.testweb.com/user.php?id=8' and if(((select substr(database(),2,1))='a'),sleep(5),1)--+，执行后页面没有延迟； （3）http://www.testweb.com/user.php?id=8' and if(((select substr(database(),4))='e'),sleep(5),1)--+，执行后页面有明显的延迟。 那么，网站当前数据库的库名可能是下列哪些选项？（B,C）

A,date B,like C,note D,money

63. 已知某网站后台数据库为MySQL，且对于任何输入，Web页面仅仅返回类似True或False的两种结果。攻击者向网站服务器提交了3条payload： （1）http://www.testweb.com/user.php?id=8'--+（2）http://www.testweb.com/user.php?id=8' and length(database())>3--+ （3）http://www.testweb.com/user.php?id=8' and (select substr(database(),2,1))='a'--+ 发现，三者返回的页面显示结果均为True。那么，网站当前数据库的库名可能是下列哪些选项？（B,C）

A,cat B,case C,raise D,better

64. 在盲注中，攻击者根据其返回页面的不同来判断信息。一般情况下，盲注可分为两类，即（B,D）。

A,基于联合查询的盲注B,基于布尔的盲注C,基于错误的盲注D,基于时间的盲注

65. 常见的SQL注入点都是通过针对select语句来实现的，除了select语句之外，还可以针对以下哪些SQL语句实现注入？（A,B,C,D）

A,create B,insert C,delete D,update

66. 如果某Web服务器存在HTTP头部注入点，则可以通过下列哪些方式修改头部信息实现注入？（B,C）

A,在浏览器导航栏中修改HTTP头部信息

B,利用Hackbar插件定制HTTP头部信息

C,利用Burpsuite工具拦截和修改HTTP头部信息

D,利用HTTP　Header　Live　插件修改ＨＴＴＰ头部信息

67. 常见的HTTP头部注入类型包括（Ａ，Ｂ，Ｃ，Ｄ）。

A,Cookie注入 B,Referer注入 C,User-Agent注入 D,XFF注入

68. SQLMAP支持的数据库类型包括（A,D）。

A,SQL Server B,Mongodb C,Redis D,Access

69. 下列属于文件上传漏洞危害的是（A,B,C）

A,上传恶意脚本 B,网站沦陷 C,服务器沦陷 D,刷流量

70. 造成文件上传漏洞的成因有哪些（A,B,D）

A,对上传文件没有进行足够的限制 B,操作系统的特性

C,危险函数 D,web服务器解析漏洞

71. 下列属于文件上传客户端检测绕过方法的是（A,C,D）

A,删除浏览器事件 B,添加头文件

C,利用Bp抓包修改后缀名 D,伪造上传表单

72. 访问控制包含哪些要素（A,B,C）

A,主体 B,客体 C,控制策略 D,系统

73. 我们提出网络安全运营的概念，是因为当下的网络安全存在哪些问题（A,B,D）

A,安全运维工作量大 B,安全人员不足

C,安全成本太高 D,安全运维效率低下

74. MDR服务主要提供哪些服务（B,C,D）

A.完整的合规报告 B.威胁分析 C.专家服务 D.威胁发现与检测

75. MSSP服务主要提供哪些服务（A,B）

A,漏洞管理 B,安全设备日志分析 C,操作系统日志分析 D,操作系统性能管理

76. 态势感知产品中使用的关键技术有（A,C,D）

A,UEBA B,网络虚拟化 C,大量关联分析 D,SOAR

77. ATT&CK是以下哪三项的结合（A,C,D）

A,战术 B,人员 C,流程 D,技术

78. Elasticserach的特点有?（A,B,C,D）

A,高扩散 B,分布式 C,快速存储 D,快速检索

79. 技术有效的安全运营包含下面哪些（A,B,C,D）

A,漏洞管理 B,威胁管理 C,事件管理 D,运营可视

80. MSS服务漏洞管理的工作包含（A,B,C）

A,漏洞分析 B,弱口令分析 C,新漏洞预警 D,漏洞的修复补丁发布

81. 构建SOC时，组织不应该包外下面哪些业务（A,C,D）

A,组织高度自定义的业务 B,易于独有的业务

C,组织独有的业务 D,依赖于组织流程的业务

82. 在构建SOC时，我们需谨记SOC是哪些部分融合的？（A,B,D）

A,技术 B,人员 C,设备 D,流程

83. 以下哪些是常用的SOC运营的衡量维度（A,C,D）

A,警告时间线度量 B,分析师处理的事件数量

C,事件警告 D,监测用例

84. 下面哪些属于SOC工具中的分析类（A.B.D）

A,SIEM B,UEBA C,EDR D,沙箱

85. 下面哪些属于SOC工具中的威胁可见性类（A,B,C,D）

A,EDR B,NTA C,VA D,CASB

86. SOC中的工具可以分为三大类，分别是(B,C,D)

A,MSS服务 B,分析 C,行管和管理 D,威胁可见性

87. 自动化基线检查的方式有（A,C,D）

A,安装agent检查 B,使用VNC远程检查

C,使用脚本检查 D,提供账号，由扫描平台检查

88. 下面哪些属于基线管理的访问控制维度检查（A,B,D）

A,用户口令复杂度 B,访问控制颗粒度 C,账号自动锁定 D,用户权限分离

89. 基线检查的维度通常包含（A,B,D,E）

A,访问控制 B,授权管理 C,失陷管理 D,日志审计 E,入侵防范

90. 常见的基线标准可以参照（A,B,C,D）

A,CLS B,OWASP C,等级保护制度 D,厂商基线

91. windows基线检查的账户策略包含（A,B）

A,密码策略 B,账户锁定策略 C,审计策略 D,用户权限分配

92. 通过/etc/ssh/sshd\_config可以配置(B,C,D)

A,SSH登录的密码复杂度 B,是否允许root登录SSH

C,SSH登录失败次数 D,SSH会话的最大连接数

93. linux安全配置原则有（A,B,C,D）

A,最小安装 B,不影响业务可用 C,职责分离 D,审计记录

94. 在应急响应的恢复阶段，恢复的优先级应当参照（A,B）

A,业务影响分析 B,服务器级别协议（SLA） C,IT工程师建议 D,业务人员建业

95. 在应急响应的检测和分析阶段，分析主要为了（B,C,D）

A,确定事件性质 B,将事件分级分类 C,找到攻击源头 D,确定事件原因

96. 在应急响应的准备阶段，要完成的事有（A,B,C,D）

A,风险评估 B,业务影响分析 C,系统恢复能力等级设定 D,恢复目标确定

97. 通常，应急响应中心服务的内容有（A,B,C）

A,安全事件响应 B,信息发布 C,安全事件分析 D,安全事件预防

98. windows应急响应主要包含下面哪些维度（A,B,C,D,E）

A,账户排查 B,网络排查 C,进程排查 D,注册排查 E,内存排查

**判断题：**

1.网络空间不是虚拟空间，而是人类现实活动空间的人为、自然延时，是人类崭新的存在方式和形态。[√]

2.美国在《保护网络空间的国家战略》中指出了Cyberspace的含义：一个由信息基础设施组成的相互依赖的网络。[√]

3.《中华人民共和国网络安全法》中不涉及人才培养相关规定。[✗]

4.网络安全法对个人信息保护方面，规定了个人信息主体不拥有删除权（保护使用不当）和更正权（有误）[✗]

5.动态网页可以实现客户端与服务端之间信息的双向传递。[√]

6.cms和ThinkPHP没有区别。[✗]

7.在目前的网络犯罪中，造成主要破环的是脚本小子[√]

8.统一资源标识符（URI）中涉及字段包括;协议、服务器地址、文件路径等，但不包括登录认证字段[✗]

9.HTTP协议会保存请求和响应的通信状态，具有持久化处理。[✗]

10.HTTP客户端发出请求，告知服务端需要执行不同类型的请求命令，这些命令被称为HTTP方法。[√]

11.HTTP响应状态码是由3位数字和原因短语共同组成。[√]

12. HTTP报文由报文首部、空行、报文主体3部分共同构成。[√]

13. HTTP协议正式传输文件内容前，需先同服务器建立TCP连接，传输完毕后，再关闭该TCP连接。[√]

14、访问某WEB链接时，首先是和服务器建立连接，然后再由DNS解析Url地址。[✗]

15、HTTP协议不面向连接，所以传输层使用的是UDP协议。[✗]

16. HTTPS是由HTTP协议和SSL/TLS协议共同构成，实现HTTP内容的密文传输。[√]

17. DVWA是一款开源的渗透测试漏洞练习平台，基于Apache+MySQL+PHP运行，包含了XSS、SQL注入、文件上传、文件包含、CSRF、暴力破解等各个难度的测试环境。[√]

18. 管理员可通过修改Apache的配置文件，设定网站的根目录和默认服务端口。[√]

19. Nmap向目标端口发送TCP FIN报文，对于Windows系统的目标机，如果目标机未响应，则说明目标端口处于开放状态或被防火墙屏蔽；如果目标机返回TCP RST+ACK报文，则说明目标端口处于关闭状态。[✗]

20. 在Nmap中，可以用-p选项指定扫描的目标端口，默认情况下，Nmap会扫描由-p选项指定的全部TCP和UDP端口。[✗]

21. BurpSuite中的Repeater模块可以与Proxy模块进行联动，传递和共享HTTP报文。[√]

22. 利用BurpSuite对目标网站进行重放攻击时，可直接利用Repeater模块拦截并手工修改HTTP请求报文。[✗]

23. 在Metasploit中，auxiliary模块主要用于执行扫描、嗅探、指纹识别等相关功能以辅助渗透测试，必须和payloads模块联合使用。[✗]

24. Metasploit是一款开源的安全漏洞检测工具，其核心代码中绝大部分由Ruby语言实现。[√]

25. 利用Hackbar插件，可以对攻击payload中的字符串进行16进制编码。[√]

26. SET可用于端口扫描和漏洞检测。[✗]

27. Hash加盐法可在一定程度上抵御字典及彩虹表攻击。[√]

28. OWASP ZAP具有Web安全漏洞模糊测试功能。[√]

29. OWASP ZAP可用于检测和修复Web应用程序中的安全漏洞。[✗]

30. Nikto可以用于扫描目标的Web类型、主机名、指定目录、特定CGI漏洞、返回主机允许的HTTP模式等。[√]

31. Weevely可用于管理由ASP语言编写的Webshell。[✗]

32. 渗透测试过程中主要以检测常规漏洞为主，一般不会用0day漏洞作为攻击手段。[√]

33. 通过互联网向客户传输渗透测试报告时，应尽可能选择明文方式发送，方便客户接收和查阅。[✗]

34. DNS主要是完成域名和IP地址对应，提供解析服务，“根”域名服务器能完成所有域名到IP的解析工作。[✗]

35. DNS协议在传输层仅用到了UDP协议进行承载。[✗]

36. whois是一种传输协议，时常用于域名相关注册信息查询，它通常采用的的协议端口是TCP协议的43号端口。[√]

37. Masscan扫描工具在扫描时，指定的IP段只能全部扫描，不能排除指定IP或IP段不进行扫描作业。[√]

38. sqlmap工具能实现对数据库注入的自动化探测，但无法实现防火墙的探测。[✗]

39. google只能对指定的域名进行查询，不能对IP地址类进行指定查询，比如C段。[✗]

40. 网络空间搜索引擎shodan不能实现指定图标的搜索功能。[✗]

41. 文件包含漏洞在利用时无视后缀名，任何扩展名都可以被PHP解析[√]

42. 文件包含漏洞在PHP中比较多，其他语言中不存在[✗]

43. Windows中管道符"|"在前面命令错误后面命令正确时，后面命令正常执行[✗]

44. 利用代码执行漏洞可以Getshell[√]

45. eval函数与assert函数用法相同[✗]

46. exec函数执行命令后可以获取全部数据[✗]

47. 反引号"`"可能造成系统命令执行[√]

48. 只要用户输入的地方都存在XSS漏洞[✗]

49. 在MySQL数据库中，可以对默认的管理员账户root进行账户名修改和降权。[✗]

50. 在MySQL数据库中执行下列命令： select concat('1','2','3'); 该条命令执行成功后返回的结果是6。[✗]

51. 基于联合查询的注入，指的是可以同时执行多条语句的注入。[✗]

52. 只要网站有报错机制，就一定可以通过union select的方式进行联合查询注入。[✗]

53. 在SQL盲注过程中，可以借助二分法来提高注入的效率。[√]

54. 作为自动化SQL注入工具，SQLMAP不能与BurpSuite联动实现注入。[✗]

55. 恶意上传行为可能导致网站甚至整个服务器被控制[√]

56. 点、空格、::$DATA等特殊文件名在Windows和Linux下都是不被允许的[✗]

57. 文件上传客户端做过滤限制后服务端不需要再做了[✗]

58. 网络中，身份不仅可以标识人，也可以标识机器或者物体，但是不能标记虚拟的东西[✗]

59. 一般的安全设备无法防御逻辑漏洞[√]

60. 强制访问控制中安全策略高于一切[√]

61. 访问是主体和客体之间的信息流动[√]

62. 成熟的安全运营中心需要购买大量成熟工作，直接使用，而不是自定义工具[✗]

63. 在实现安全运营时，我们可以重点参考ISO 20000中的信息系统服务管理标准[✗]

64. SOC的全称是安全运营中心，仅仅表示一个安全的产品[✗]

65. 网络安全运营是网络安全运维的升级版，仍然是强调突发性的运维工作[✗]

66. SOAR的主要作用是定义标准化工作流，便于自动化的响应[√]

67. 安全事件响应四步法是1、应急预案，2、检测及分析，3、控制、根除和恢复，4、总结优化[√]

68. MSS服务中针对威胁的处置流程通常是威胁上报、威胁研判、安全通告、远程排查、溯源分析、闭环总结六个步骤[√]

69. MSS服务的流程可以分为运营准备和持续运营两个阶段[√]

70. 组织建立安全运营中心通常是希望改善安全状况，侧重于威胁检测[√]

71. 通过调查，我们发现企业建设安全运营中心时，人员的应用比流程和技术更为关键[√]

72. 在优秀的SOC中，引入欺骗技术（蜜罐）主要是为了溯源攻击者[✗]

73. 在一个优秀的SOC展示中，告警不再是展示的主机，而应该是不同实体的威胁评分[√]

74. 我们可以发起模拟攻击来对SOC是否完成其工作进行测试[√]

75. SOC中行动和管理的核心工具是统一通信工具[✗]

76. 安全运营中心的核心功能是围绕检测和监控来进行[√]

77. 基线检查的前提是将资产清单整理完成，否则整个基线检测工作会失去意义[√]

78. 基线表达了最基本的需要满足的安全要求[√]

79. 系统审核策略是属于组策略的“用户配置”[✗]

80. PAM模块是Linux中的认证管理模块，所有认证相关可以PAM管理[√]

81. apache通过编辑配置文件，加入requestreadtimeout选项来防止http的高并发会话攻击[✗]

82. apache可以通过安装ModSecurity模块来实现WAF的功能[√]

83. apache的.htaccess文件可以控制当前目录的配置选项[√]

84.为了保证系统安全，apache网站目录下的文件所有者有应设为root[√]

85.为了保证系统安全，apache服务应该以root的身份来运行[✗]

86. 应急响应不仅是技术层面的响应，也包含管理行动[√]

87. 通过分析windows操作系统的内存文件，我们可以发现系统被hook的API函数[√]

88. windows操作系统中，使用tasklist命令，查看任务管理器[✗]

89. windows在应急响应时，可以使用net user命令查看隐藏账户[✗]