# 网络安全实验室CTF—选择题解析 writeup

原创

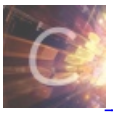
Senimo_ 于 2019-08-04 18:34:50 发布 3622 收藏 26

分类专栏： 网络安全实验室CTF writeup 文章标签： 网络安全实验室 CTF writeup 选择题 解析

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_44037296/article/details/98472247

版权



网络安全实验室CTF writeup 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

## 网络安全实验室CTF—选择题解析 writeup

1.主要用于加密机制的协议是（ ）

2.向有限的空间输入超长的字符串是哪一种攻击手段？（ ）

3.为了防御网络监听，最常用的方法是（ ）

4.使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于什么攻击类型?（ ）

5.用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？( )

6.Windows NT 和Windows Server系统能设置为在几次无效登录后锁定帐号,这可以防止（ ）

7.下列不属于系统安全的技术是（ ）

8.以下关于DOS攻击的描述，哪句话是正确的？（ ）

9.许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么？（ ）

10.下面哪个功能属于操作系统中的日志记录功能（ ）

11.邮件炸弹攻击主要是（ ）

12.故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，将受到（ ）处罚

13.网络物理隔离是指（ ）

14.VPN是指（ ）

15.NAT 是指（ ）

16.局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样，则（ ）

17.一台交换机具有48个10 / 100Mbps端口和2个1000Mbps端口，如果所有端口都工作在全双工状态，那么交换机总带宽应为（ ）

18.IP地址块211.64.0.0 / 11的子网掩码可写为（ ）

19.某企业产品部的IP地址块为211.168.15.192 / 26，市场部的为211.168.15.160 / 27，财务部的为211.168.15.128 / 27，这三个地址块经聚合后的地址为（ ）

20.下列对IPv6地址FF23：0：0：0：0510：0：0：9C5B的简化表示中，错误的是 （ ）

网络安全实验室CTF链接

## 1.主要用于加密机制的协议是（ ）

**A. HTTP**
**B. FTP**
**C. TELNET**
**D. SSL**

**选择：D**
A.超文本传输协议(HTTP)是一种通信协议，它详细规定了浏览器和万维网(WWW = World Wide Web)服务器之间互相通信的规则，由请求和响应构成。
B.文件传输协议（File Transfer Protocol，FTP）是用于在网络上进行文件传输的一套标准协议，FTP允许用户以文件操作的方式（如文件的增、删、改、查、传送等）与另一主机相互通信。
C.Telnet协议是Internet远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。
D.SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。

## 2.向有限的空间输入超长的字符串是哪一种攻击手段？（ ）

**A. 缓冲区溢出**
**B. 网络监听**
**C. 拒绝服务**
**D. IP欺骗**

**选择：A**
A. 缓冲区溢出是一种非常普遍、非常危险的漏洞。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。
B. 网络监听是监视网络状态、数据流程以及网络上信息传输，可以截获网络上所传输的信息。也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其它主机，使用网络监听便可以有效地截获网络上的数据，这是攻击者使用最好的方法。
C. 拒绝服务（英文名称denial of service;DoS）是指通过向服务器发送大量垃圾信息或干扰信息的方式，导致服务器无法向正常用户提供服务的现象。
D. IP欺骗，发送的数据包里面不是真实的IP，取而代之的是伪造的IP地址，这样，看上去包就是由那个IP发出的，如果对方回复这个信息，那么数据将会被发送到伪造的IP上，除非攻击者决定重定向该信息到一个真实的IP上。

## 3.为了防御网络监听，最常用的方法是（ ）

**A. 采用物理传输（非网络）**
**B. 信息加密**
**C. 无线网**
**D. 使用专线传输**

**选择：B**
A. 采用物理传输（非网络）
B. 信息加密技术是利用数学或物理手段，对电子信息在传输过程中和存储体内进行保护，以防止泄漏的技术
C. 无线网（英语：Wireless network）指的是任何型式的无线电计算机网络，普遍和电信网络结合在一起，不需电缆即可在节点之间相互链接。无线电信网络一般被应用在使用电磁波的摇控信息传输系统，像是无线电波作为载波和物理层的网络。
D. 使用专线传输就是一个独立的局域网，例如军事，银行等，让用户的数据传输变得可靠可信，专线的优点就是安全性好，QoS 可以得到保证。不过，专线租用价格也相对比较高，而且管理也需要专业人员。

## 4.使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于什么攻击类型？（ ）

**A. 拒绝服务**
**B. 文件共享**
**C. BIND漏洞**
**D. 远程过程调用**

**选择：A**
A. 拒绝服务（英文名称denial of service;DoS）是指通过向服务器发送大量垃圾信息或干扰信息的方式，导致服务器无法向正常用户提供服务的现象。
B. 文件共享是指主动地在网络上共享自己的计算机文件。一般文件共享使用P2P模式，文件本身存在用户本人的个人电脑上。大多数参加文件共享的人也同时下载其他用户提供的共享文件。有时这两个行动是连在一起的。
C. BIND漏洞最早起源于美国DARPA资助研究的一个伯克利大学研究生课题。目前它由因特网软件联合会(Internet Software Consortium)负责进行维护和开发。能够运行在当前大多数系统平台之上。人们可以在网络上自由下载其源代码，进行安装、运行或研究。
D. RPC是远程过程调用（Remote Procedure Call）的缩写形式。SAP系统RPC调用的原理其实很简单，有一些类似于三层构架的C/S系统，第三方的客户程序通过接口调用SAP内部的标准或自定义函数，获得函数返回的数据进行处理后显示或打印。

## 5.用户收到了一封可疑的电子邮件,要求用户提供银行账户及密码,这是属于何种攻击手段？( )

**A. 缓存溢出攻击**
**B. 钓鱼攻击**
**C. 暗门攻击**
**D. DDOS攻击**

**选择：B**
A. 缓存溢出攻击是利用缓冲区溢出漏洞所进行的攻击行动。缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统关机、重新启动等后果。
B. 钓鱼攻击是一种企图从电子通讯中，通过伪装成信誉卓著的法人媒体以获得如用户名、密码和信用卡明细等个人敏感信息的犯罪诈骗过程。这些通信都声称（自己）来自社交网站拍卖网站\网络银行、电子支付网站\或网络管理者，以此来诱骗受害人的轻信。网钓通常是通过e-mail或者即时通讯进行。它常常导引用户到URL与界面外观与真正网站几无二致的假冒网站输入个人数据。就算使用强式加密的SSL服务器认证，要侦测网站是否仿冒实际上仍很困难。
C. 暗门攻击会在特定条件出现时发生。特定条件的一个例子是在一天中的某个时间执行某个命令，另一个可能会发生的例子是当几个命令在同一时间运行的时候，常见的黑客策略是安装一个应用软件，然后，只让它在指定的时间运行。暗门攻击的结果是使系统变得易受攻击。
D. DDOS攻击即分布式拒绝服务攻击，可以使很多的计算机在同一时间遭受到攻击，使攻击的目标无法正常使用，分布式拒绝服务攻击已经出现了很多次，导致很多的大型网站都出现了无法进行操作的情况，这样不仅仅会影响用户的正常使用，同时造成的经济损失也是非常巨大的。

## 6.Windows NT 和Windows Server系统能设置为在几次无效登录后锁定帐号,这可以防止（ ）

**A. 木马**
**B. 暴力攻击**
**C. IP欺骗**
**D. 缓存溢出攻击**

**选择：B**

A. 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、记录键盘和攻击Dos等特殊功能的后门程序。木马病毒其实是攻击者用于远程控制计算机的程序，将控制程序寄生于被控制的计算机系统中，对被感染木马病毒的计算机实施操作，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。

B. 暴力攻击，利用字典等方式破解加密或用户名密码的攻击方式

C. IP欺骗，发送的数据包里面不是真实的IP，取而代之的是伪造的IP地址，这样，看上去包就是由那个IP发出的，如果对方回复这个信息，那么数据将会被发送到伪造的IP上，除非攻击者决定重定向该信息到一个真实的IP上。

D. 缓存溢出攻击是一种非常普遍、非常危险的漏洞。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。

## 7.下列不属于系统安全的技术是（ ）

**A. 防火墙**
**B. 加密狗**
**C. 认证**
**D. 防病毒**

**选择：B**

A. 防火墙技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全性的一种技术。

B. 加密狗是一种插在计算机并行口上的软硬件结合的加密产品。一般都有几十或几百字节的非易失性存储空间可供读写，软件开发者可以在软件中设置多处软件锁，利用软件狗做为钥匙来打开这些锁;如果没插软件狗或软件狗不对应，软件将不能正常执行。

C. 网站认证是指持有“官方网站认证证书”和“官方网站认证标志” 的企业网上身份认证资质，将证书标志悬挂在官网的醒目位置。网站亮证经营是由于网络的虚拟性和开放性，市场主体应当遵循的网站运营规则，既保护网站权益又保障网民利益。

D. 防病毒指用户主动性的防范电脑等电子设备不受病毒入侵，从而避免用户资料泄露、设备程序被破坏等情况的出现。

## 8.以下关于DOS攻击的描述，哪句话是正确的？（ ）

**A. 不需要攻击目标系统**
**B. 以窃取目标系统上的机密信息为目的**
**C. 导致目标系统无法处理正常用户的请求**
**D. 如果目标系统没有漏洞，远程攻击就不可能成功**

**选择：C**

C. 拒绝服务（英文名称denial of service;DoS）是指通过向服务器发送大量垃圾信息或干扰信息的方式，导致服务器无法向正常用户提供服务的现象。

## 9.许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对于这一威胁，最可靠的解决方案是什么？（ ）

**A. 安装防火墙**
**B. 安装入侵检测系统**
**C. 给系统安装最新的补丁**
**D. 安装防病毒软件**

**选择：C**

防火墙、入侵检测系统、防病毒软件无法防御缓冲区溢出的漏洞。

## 10.下面哪个功能属于操作系统中的日志记录功能（ ）

A. 控制用户的作业排序和运行
B. 以合理的方式处理错误事件，而不至于影响其他程序的正常运行
C. 保护系统程序和作业，禁止不合要求的对程序和数据的访问
D. 对计算机用户访问系统和资源的情况进行记录

选择：D
系统日志是记录系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的事件。用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。系统日志包括系统日志、应用程序日志和安全日志。

## 11.邮件炸弹攻击主要是（ ）

A. 破坏被攻击者邮件服务器
B. 添满被攻击者邮箱
C. 破坏被攻击者邮件客户端
D. 不清楚

选择：B
邮件炸弹是指电子邮件炸弹，英文是E-Mail Bomb。指的是邮件发送者，利用特殊的电子邮件软件，在很短的时间内连续不断地将邮件邮寄给同一个收信人，在这些数以千万计的大容量信件面前收件箱肯定不堪重负，而最终“爆炸身亡”。

## 12.故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，将受到（ ）处罚

A. 处五年以下有期徒刑或者拘役
B. 拘留
C. 罚款
D. 警告

选择：A
百度百科：网络安全法

## 13.网络物理隔离是指（ ）

A. 两个网络间链路层在任何时刻不能直接通讯
B. 两个网络间网络层在任何时刻不能直接通讯
C. 两个网络间链路层、网络层在任何时刻都不能直接通讯
D. 不清楚

选择：C
物理隔离，是指采用物理方法将内网与外网隔离从而避免入侵或信息泄露的风险的技术手段。物理隔离主要用来解决在那些需要绝对保证安全的保密网，专网和特种网络与互联网进行连接时，为了防止来自互联网的攻击和保证这些高安全性网络的保密性、安全性、完整性、防抵赖和高可用性，几乎全部要求采用物理隔离技术。物理隔离包含隔离网闸技术 、物理隔离卡等。

## 14.VPN是指（ ）

A. 虚拟的专用网络
B. 虚拟的协议网络
C. 虚拟的包过滤网络
D. 不清楚

选择：A
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。

## 15.NAT 是指（ ）

**A. 网络地址传输**
**B. 网络地址转换**
**C. 网络地址跟踪**
**D. 不清楚**

**选择：B**
NAT（Network Address Translation，网络地址转换），当在专用网内部的一些主机本来已经分配到了本地IP地址，但现在又想和因特网上的主机通信时，可使用NAT方法。、

## 16.局域网内如果一个计算机的IP地址与另外一台计算机的IP地址一样，则（ ）

**A. 两台计算机都正常**
**B. 两台计算机都无法通讯**
**C. 一台正常通讯一台无法通讯**
**D. 不清楚**

**选择：B**

## 17.一台交换机具有48个10／100Mbps端口和2个1000Mbps端口，如果所有端口都工作在全双工状态，那么交换机总带宽应为（ ）

**A. 8.8Gbps**
**B. 12.8Gbps**
**C. 13.6Gbps**
**D. 24.8Gbps**

**选择：C**
48*100M*2+2*1000M*2=9.6G+4G=13.6G。其中第一个参数是接口数量，第二个参数是端口速率，第三个参数是双向传输。10/100表示10或100M自适应接口，其上行与下行都可以是10M或100M，并不是一个方向10M，另一个方向100M。

## 18.IP地址块211.64.0.0／11的子网掩码可写为（ ）

**A. 255.192.0.0**
**B. 255.224.0.0**
**C. 255.240.0.0**
**D. 255.248.0.0**

**选择：B**
IP地址块211.64.0.0/11中，网络前缀表示对应11位的网络号是确定的，即IP地址前面的11位为网络号，故其子网掩码为11111111.11100000.00000000.00000000，转化为十进制为255.224.0.0。

## 19.某企业产品部的IP地址块为211.168.15.192／26，市场部的为211.168.15.160／27，财务部的为211.168.15.128／27，这三个地址块经聚合后的地址为（ ）

**A. 211.168.15.0／25**
**B. 211.168.15.0／26**
**C. 211.168.15.128／25**
**D. 211.168.15.128／26**

**选择：C**

三个地址块写成二进制后的前25位是相同的，故选前25位为聚合后的网络前缀，排除B、D两项；前24位不变，第25位为1，其余为0，经过计算得地址为211.168.15.128/25。

## 20.下列对IPv6地址FF23：0：0：0：0510：0：0：9C5B的简化表示中，错误的是（ ）

**A. FF23：：0510：0：0：9C5B**

**B. FF23：0：0：0：0510：：9C5B**

**C. FF23：0：0：0：051：：9C5B**

**D. FF23：：510：0：0：9C5B**

**选择：C**

在使用零压缩法时，不能把一个位段内部的有效0也压缩掉。C项明显不符合前导零压缩法。