A **poison packet** triggers a bug in the system’s network handling software causing it to crash and the  
system can no longer communicate over the network until this software is reloaded.

In a **DNS amplification** attack the attacker creates a series of DNS requests containing the spoofed source  
address for the target system.

Given sufficiently privileged access to the network handling code on a computer system, it is difficult  
to create packets with a forged source address. **False**

When a DoS attack is detected, the first step is to **identify the attack**.

In both direct flooding attacks and **SYN spoofing attacks** the use of spoofed source addresses results in response packets being scattered across the Internet and thus detectable.

A characteristic of reflection attacks is the lack of **backscatter** traffic.

A **network-based IDS** monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a  
legitimate user in ways that can be quantified. **True**

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible  
on a system. **True**

The IDS component responsible for collecting data is the user interface. **False**

**Insider attacks** are among the most difficult to detect and prevent.

The **analyzer** is responsible for determining if an intrusion has occurred.

A **VPN** consists of a set of computers that interconnect by means of a relatively unsecure  
network and makes use of encryption and special protocols to provide security.  
   
**Direction** control determines the direction in which particular service requests may be initiated and  
allowed to flow through the firewall.  
   
**Service** control determines the types of Internet services that can be accessed, inbound or outbound.  
   
The firewall may be a single computer system or a set of two or more systems that cooperate to perform  
the firewall function. **True**  
   
**Stateful matching** scans for attack signatures in the context of a traffic stream rather than individual packets.  
   
A prime disadvantage of an application-level gateway is the additional processing overhead on each  
connection. **True**

**Run-time** defenses involve changes to the memory management of the virtual address space of  
processes that act to either alter the properties of regions of memory or to make predicting the location  
of target buffers sufficiently difficult to thwart many types of attacks.  
   
Buffer overflows can be found in a wide variety of programs. **True**  
   
21 An essential component of many buffer overflow attacks is the transfer of execution to code, known as  
**shellcode**, supplied by the attacker and often saved in the buffer being overflowed.  
   
A **stack frame** is a structure where data are usually saved on the stack.  
   
In 2004 the  **Sasser Worm** exploited a buffer overflow in Microsoft Windows 2000/XP Local Security  
Authority Subsystem Service.  
   
The x86 Assembly Language Instruction NOP means **no operation or do nothing instruction** .  
   
Programmers often make assumptions about the type of inputs a program will receive. **True**  
   
Many computer security vulnerabilities result from poor programming practices. **True**  
   
The correct implementation in the case of an atomic operation is to test separately for the presence of  
the lockfile and to not always attempt to create it. **False**  
   
**Environment variables** are a collection of string values inherited by each process from its parent that can affect the way a running process behaves.  
   
A **command injection** attack occurs when the input is used in the construction of a command that is subsequently executed by the system with the privileges of the Web server.  
   
Software security is closely related to software quality and reliability. **True**  
  
The **mail submission agent** accepts the message submitted by a message user agent and enforces the policies of the hosting domain and the requirements of Internet standards.  
  
IPsec can assure that **a router advertisement comes from an authorized router, a routing update is not forged, a redirect message comes from the router to which the initial packet was sent**  
   
33 An ADMD is an Internet e-mail provider. **True**  
   
The **MDA** is responsible for transferring the message from the MHS to the MS.  
   
35 At its most fundamental level the Internet mail architecture consists of a user world in the form of **MUA**  
   
36 ESP supports two modes of use: transport and **tunnel**.  
  
The ticket-granting ticket is not reusable. **False**  
The ticket-granting ticket is encrypted with a secret key known only to the AS and the TGS. **True**  
   
**Kerberos** requires that a user prove his or her identity for each service invoked and, optionally,  
requires servers to prove their identity to clients.  
  
CMP, defined in RFC 2510, is designed to be a flexible protocol able to accommodate a variety of  
technical, operational, and business models. **True**  
   
Federated identity management makes use of a number of standards that provide the building blocks  
for secure identity information exchange across different domains or heterogeneous systems. **True**  
   
A principal element of an identity management system is  **workflow automation, delegated administration, and authentication**.  
   
Initialization begins the process of enrolling in a PKI. **False**  
   
Company wireless LANs or wireless access points to wired LANs in close proximity may create overlapping transmission ranges. **True**  
   
A wireless access point is a **cell tower, Wi-Fi hot spot, wireless access point to a LAN or WAN**

A **pre-shared key** is a secret key shared by the AP and a STA and installed in some fashion outside the  
scope of IEEE 802.11i.  
   
The smallest building block of a wireless LAN is a **BSS**.  
   
The MPDU exchange for distributing pairwise keys is known as the **4-way handshake**.  
   
The MAC service data unit contains any protocol control information needed for the functioning of the  
MAC protocol. **False**  
   
Any device that contains an IEEE 802.11 conformant MAC and physical layer is a basic service set. **False**