|  |  |
| --- | --- |
| Cd ~ | Go back to Home directory |
| Cd / | Root directory |
| ls | List directory content |
| ls -l | List with extra information |
| ls -la | List with extra information incl. hidden stuff |
| sudo | Get higher user permissions |
| apt | program |
| sudo apt install xyz | Install new software called xyz |
| sudo apt update | List of software that need update |
| sudo apt upgrade | Install all updated software |
| file xyz | Type of file |
| cat | Look at inside a file |
| more | Look at inside a file |
| strings | Print sequence of a file |
| rm xyzfile | Remove a file from a folder not delete |
| rmdir xyzfolder | Remove a folder/directory |
| rm -rf | Forceful removal |
| ping IPxyz | Ip address information |
| curl http --output filename | Download from internet |
| wget http | download |
| mkdir | Make a folder/directory |
| pwd | Current directory/path |
| Ln | Linking files |
| chmod | Change file mode |
| cut |  |
| sort |  |
| which | locate a program file in the user's path |
| grep | file pattern searcher |
| whereis | locate programs path |
| finger | displays information about the system users |
| W | display who is logged in and what they are doing |
| who | display who is logged in |
| whoami | display effective user id |
| last | indicate last logins of users and ttys |
| top | display and update sorted information about processes |
| ps | process status |
| nice | ecute a utility with an altered scheduling priority -20 to +20 |
| Nohup | invoke a utility immune to hangups |
| kill | terminate |
| Less |  |
| More |  |
| ifconfig | assign an address to a network interface and/or configure network interface parameters |
| arp | displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol (arp(4)) |
| nslookup | program to query Internet domain name servers |
| uname | Print operating system name |
| netstat | show network status |
| traceroute | print the route packets take to network host |
| dig | DNS lookup utility |
| lsof | list open files |
| whois | Internet domain name and network number directory service |
| crontab | maintain crontab files for individual users (V3) |
| NC | arbitrary TCP and UDP connections and listens |
| uniq | report or filter out repeated lines in a file |
| id | return user identity |
| groups | show group memberships |
| df | display free disk space |
| Du | display disk usage statistics |
| Dd | convert and copy a file |
| openssl | OpenSSL command line tool |
| tar | manipulate tape archives |
| touch | change file access and modification times |
| shred | to [overwrite](https://www.computerhope.com/jargon/o/overwrit.htm) a file to hide its contents, and optionally delete it |
| history | view the previously executed command |
| umask | allows you to view or to set the file mode creation mask, which determines the permissions bits for newly created files or directories |
| signal |  |
| find ~ -name "LaptopLikeYou.mp3” find ~ -name "Laptop\*mp3"  find ~ -name "\*mp3" | find a file or similar items |
| wc -w "Essay.txt" | count lines, words and characters |

1  
As a student at Tufts, you have agreed to abide by the Student [Code of Conduct] ([http://students.tufts.edu/student-affairs/student-code-conductLinks to an external site.](http://students.tufts.edu/student-affairs/student-code-conduct)), which prohibits all forms of academic misconduct, including cheating, plagiarism, inappropriate collaboration, academic dishonesty, and facilitating the academic misconduct of another.

By entering your name below in lieu of your signature, you acknowledge that you have read the instructions for the exam, and you pledge again to adhere to the Tufts Student Code of Conduct during and after the exam.  
  
 [\_\_\_\_]

2  
Transport Layer Security (TLS) uses

Both symmetric and asymmetric encryption

Asymmetric encryption

Neither symmetric nor asymmetric encryption

Symmetric encryption

3 [\_\_\_\_] attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites.

Cross-Site Scripting (XSS)

4 [\_\_\_\_] is a formal dictionary of common software weaknesses that is based in part on the 74,000+ CVE Identifiers on the CVE List.

**Common Weakness** Enumeration (CWE™)

5 A virus needs to attach itself to another file.

True

False

6 A worm needs to attach itself to another file.

True

False

7 Dynamic analysis has full (100%) coverage of the code, whether or not the source is available.

True

False

8 A command-line tool for searching text is an example of a static analysis tool.

True

False

9 A worm infects a network by using techniques including...

* Email: Carried inside files sent as email attachments
* Internet: Via links to infected websites; generally hidden in the website’s HTML, so the infection is triggered when the page loads
* Downloads & FTP Servers: May initially start in downloaded files or individual FTP files, but if not detected, can spread to the server and thus all outbound FTP transmissions
* Instant Messages (IM): Transmitted through mobile and desktop messaging apps, generally as external links, including native SMS apps, WhatsApp, Facebook messenger, or any other type of ICQ or IRC message
* P2P/Filesharing: Spread via P2P file sharing networks, as well as any other shared drive or files, such as a USB stick or network server
* Networks: Often hidden in [network packets](https://www.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer); though they can spread and self-propagate through shared access to any device, drive or file across the network

10 A [\_\_\_\_\_] is random data that is used as an additional input to a one-way function that hashes a password or passphrase.  It is used to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow table attacks.

salt

11 [\_\_\_\_] is an international organization dedicated to web application security.

Open **Web Application Security** Project® (OWASP)

12 The principle of [\_\_\_\_] is the practice of giving a user or system access only to the components that it requires to do its work and no more.

**Least Privilege (POLP)**

13 [\_\_\_\_] is a way to prevent SQL injection; they takes the form of a template into which certain constant values are substituted during each execution. It does not mix code and data.

Prepared statements

14 A [\_\_\_\_] is software that allows form data to be modified after submission and to bypass restrictions on input choices.

15 [\_\_\_\_] is the key defense mechanism against Cross-Site Scripting, SQL injection, Cross-Site Request Forgery, and most web application vulnerabilities.

16 CVE is a [\_\_\_\_] of common names for publicly known cyber security vulnerabilities

dictionary

17 Static analysis can prove findings are actual vulnerabilities.

T  
F

18 Briefly explain why a vulnerability assessment that reports no security vulnerabilities in a system does not mean that the system is secure. Give one example.  
anti-virus on a personal computer that look for vulnerability will look at the current publicly available dictionary of threats. Usually these threats are historically that have been recorded and if there is new threat, the anti-virus software will not catch it and this new threat can negatively affect the personal computer.

19 Recently, someone was able to bypass PayPal’s two factor authentication within minutes.  While the person had Internet access, there was no phone signal so the person could not receive a two factor authentication token on his/her mobile phone.  After successfully entering password, the person was presented with two security questions that he/she could not remember the answers to (we've all been there).  However, there was a weakness in the system: the security questions were part of the HTTP POST data: Briefly explain how can one bypass PayPal’s two factor authentication given the weakness as illustrated in the picture above.  
  
There must be another way when user isn’t able to use two factor authentication via mobile phone. You can identify yourself another way via secondary form of authentication. In this picture, it was via answering security questions, the questions and the submitted answers were inside URL for logging in. The authentication could have been approved by removing the questions and the answers from the URL altogether

20 A [\_\_\_\_\_] is malware that bypasses authentication and enables a remote attacker to have access to or send commands to a compromised computer.

Trojan

21 Consider the following real scenario below:

In early 2008, the RIAA website (http://www.riaa.com) was compromised.  While visitors could still access the website, it hardly displayed any relevant content, other than the header and footer of the site.

What attack most likely occurred?

SQL injection attack

22 Consider the following real scenario below:

In early 2008, the RIAA website (http://www.riaa.com) was compromised.  While visitors could still access the website, it hardly displayed any relevant content, other than the header and footer of the site.

Give two ways to defend or prevent this attack.

Sanitize Data By Limiting Special Characters

Enforce Prepared Statements

23 This is a real incident from 2010.  Consider the following screenshot:

What vulnerability on Amazon is responsible for this defacement?  
  
The XSS attack happened on product title and the input was not a sanitized.

int main() {  
    char str1[] = "Who lives in a pineapple under the sea?";  
    char str2[15];  
  
    strcpy(str2, str1);  
}

24 Consider the following code example, in C:

Where is the vulnerability?

25 Consider the following code example, in C:

int main() {  
    char str1[] = "Who lives in a pineapple under the sea?";  
    char str2[15];  
  
    strcpy(str2, str1);  
}

Briefly describe how to fix the vulnerability.

26 Consider the following working program written in Java (i.e., compiles with no errors):

import java.sql.\*;  
  
  
  
  
public class TwitterTest {  
  
  private static final String username = "root";  
  
  private static final String password = "SpongebobSquarepantsWasATerribleCartoon";  
  
  
  
  
  public static void main(String args[]) {  
  
    try {  
  
      Class.forName("com.mysql.jdbc.Driver");  
  
      Connection conn = DriverManager.getConnection("jdbc:mysql://192.168.1.10:3306/twitter", username, password);  
  
      Statement stmt = conn.createStatement();  
  
      String theQuery = "SELECT tweet\_text FROM tweets WHERE tweet\_text = '" + args[0] + "'";  
  
      ResultSet rs = stmt.executeQuery(theQuery);  
  
      while (rs.next()) {  
  
        System.out.println(rs.getString(2));  
  
      }  
  
    }  
  
    catch (Exception e) {  
  
      System.out.println("Whoops, something went terribly wrong! " + e.toString());  
  
    }  
  
  }  
  
}  
  
// 1. Compile via `javac TwitterTest.java`  
  
// 2. Run via `java -classpath .:mysql-connector-java-5.1.40-bin.jar TwitterTest`

Identify the vulnerabilities in the source code.

27 In static analysis, the program will be executed.  
T  
F