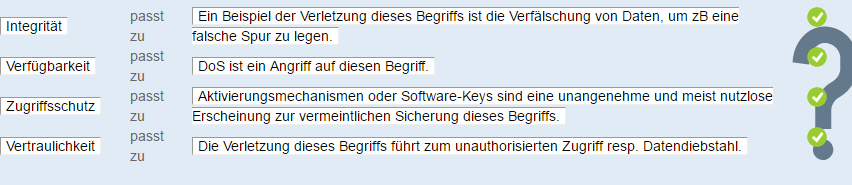
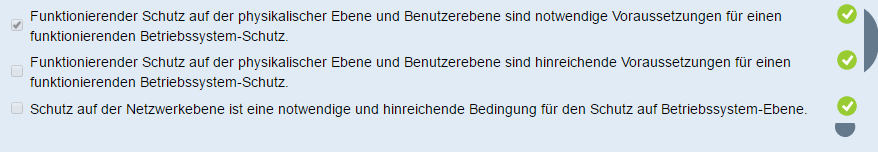
1. Ordne den nachfolgenden Begriffen jeweils die geeignete Aussage zu.



1. Welche der nachfolgenden Aussagen sind korrekt?



1. In Unix wird das setuid-Bit benutzt um Dateien zu schützen bzw. im Bedarfsfall erweiterten Zugriff zu gewähren. Inwiefern bietet das setuid-bit eine Angriffsmöglichkeit?  
   Hinweis: Berücksichtige die Möglichkeit eines Benutzers, beliebige Dateien zu erstellen.

Ein Angreifer kann ein Programm mit SETUID root (Administrator bei Windows) angreifen und mit einer buffer overflow attack Systemaufrufe zu tätigen um ein File (des Angreifers) zu erstellen oder es ins SETUID root zu bringen, damit das "Angriffs-File" mit superuser/Administrator Berechtigungen ausgeführt werden kann.

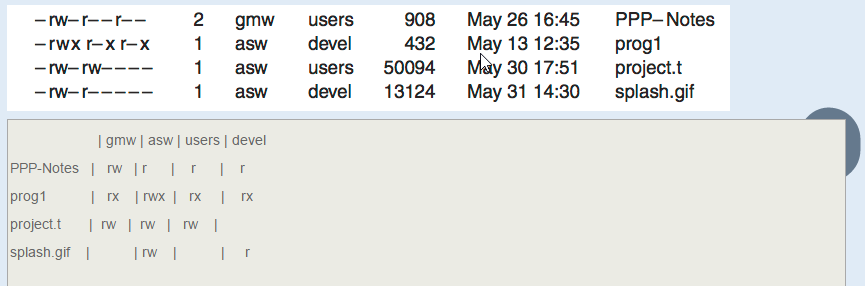
<https://security.stackexchange.com/questions/14520/what-does-it-mean-to-be-setuid-root>

1. Welche Arten von Programmiersprachen sind anfällig für Pufferüberläufe?

Sprachen, die direkten Zugriff auf den Speicher zulassen, keine eingebaute Prüfung der Boundaries haben und nicht starke Typisierung verwendet. Beispiele dafür sind Assembly, C oder C++.

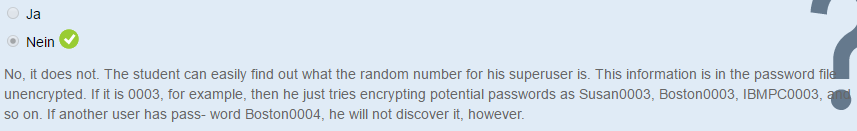
<https://en.wikipedia.org/wiki/Buffer_overflow#Choice_of_programming_language>

1. Repräsentiere die Besitzer und Zugriffsrechte des nachfolgenden UNIX-Directory-Listings als Zugriffsmatrix. asw ist dabei Mitglied der Gruppen users und devel, gmw ist Mitglied von users. Behandle jeden der Benutzer und Gruppen als Domäne. Die Matrix hat also 4 Zeilen (1 pro Domäne) und vier Spalten (1 pro Datei/Objekt).

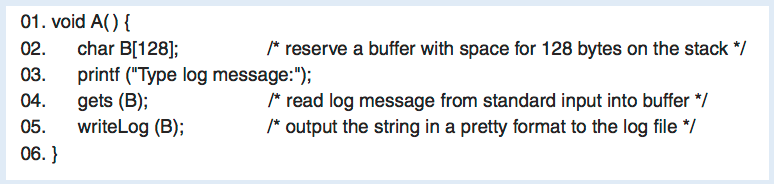


<https://unix.stackexchange.com/questions/103114/what-do-the-fields-in-ls-al-output-mean>

1. Das Morris-Thompson-Verfahren wurde entwickelt, um es einem Angreifer zu erschweren eine grosse Menge an Passwörtern herauszufinden indem er oft benutzte "verschlüsselte" Zeichenfolgen im Voraus berechnet und dann mit einem Passwort-File abgleicht. Bietet das Verfahren Schutz gegen einen Studenten, der versucht das Passwort des Superusers auf seiner Maschine herauszufinden? Man nehme an, das Passwort-File sei allen Benutzern mit Lese-Zugriff zugänglich.



1. Der nachfolgende C-Code bietet eine Angrifssmöglichkeit. Erkläre wieso dies der Fall ist (0.5) und um welche Angriffsmethode es sich handelt (0.5).



Mit Buffer Overflow Attack kann auf ungewollte Speicherorte zugegriffen werden, da B eine fixe Länge hat und keine Prüfung vor dem Schreiben in B vorgenommen wird.