UNITED STATES MILITARY ACADEMY

ASSIGNMENT: Lab 2 Report – Linux Security

CY450: Cyber Security Engineering

SECTION: G1-1

INSTRUCTOR: MAJ ADAM DUBY

By

CADET ZACHARY BOLEN, ’22 HHC

WEST POINT, NEW YORK

DATE 12 JANUARY 2022

\_\_\_\_\_ OUR DOCUMENTATION ATTRIBUTES ALL SOURCES USED AND ASSISTANCE

RECEIVED IN COMPLETING THIS ASSIGNMENT.

\_\_\_\_\_ NO SOURCES WERE USED OR ASSISTANCE RECEIVED IN COMPLETING THIS

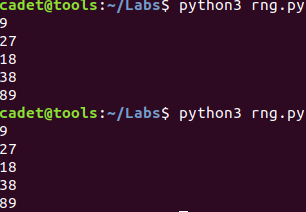
ASSIGNMENT.

SIGNATURES: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Lab 2 Report - Linux Security**

**35 Points**

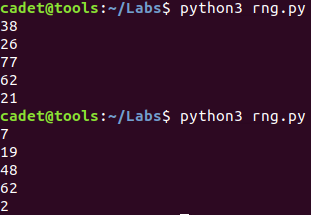
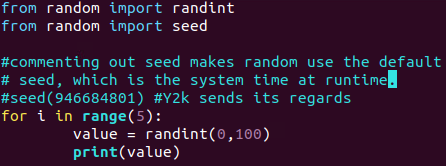
**Question 1 (1 Point)**: What is the output of the program (a screenshot or list of numbers will suffice)?



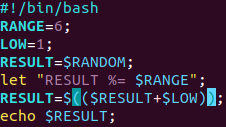
**Question 2 (1 Point)**: Why do we observe the same random numbers each time the program is executed?

We see the same numbers because we manipulated the seed that the random library is referencing when running the script by setting it to 32 instead of the system time.

**Question 3 (1 Point)**: Change the program such that each execution produces a different sequence of numbers. Show a screenshot of your revised code and an output sample.

**Question 4 (1 Point)**: Suppose you want to simulate the roll of a six-sided fair die. Using Bash and $RANDOM, what command can be used to get a positive pseudorandom number less than 7?

 You can do it in code.

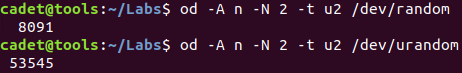
But for a command, you could use shuf I think, or modify something from either /random or /urandom with od.

**Question 5 (1 Point)**: Briefly describe the difference between /dev/random and /dev/urandom.

/dev/random is blocking and guarantees entropy. /dev/urandom is non-blocking and always returns a result even if the randomness (via the entropy pool) is weak/drained.

**Question 6 (1 Point)**: Generate a two-byte random number from /dev/random and /dev/urandom. Attach a screenshot here:

od -A n (None) -N 2 (2 bytes) -t u2 /dev/random (or urandom) 🡪 generates 2-byte random numbers by dumping files in octal.



**Question 7 (1 Point)**: What is the User ID (UID) of the root user?

0

**Question 8 (1 Point)**: Is it possible for another user account to have the same UID as the root user? What would be the implications of having multiple accounts with this UID?

Yes, it is possible to assign the UID 0 to other users. This would give them the same status and access as root, which could be a security risk if those users eventually no longer need that power.

**Question 9 (1 Point)**: What is the User ID of your user account (cadet)?

Name,password,UID,GID (id command)

cadet UID: 1000

**Question 10 (1 Point)**: What is the Group ID of the root account?

0

**Question 11 (1 Point)**: What is the Group ID of your user account (cadet)?

1000

**Question 12 (1 Point)**: What is the logon shell for the user backup and how does this impact this user accessing this machine?

backup is tagged with /usr/sbin/nologin, which means that when a user attempts to access the machine with that username, they won’t be asked or allowed to login.

**Question 13 (1 Point)**: Which user(s) are currently in the adm group?

The only users in adm are syslog and cadet

**Question 14 (1 Point)**: Which user(s) are currently in the sudo group?

The only user in sudo is cadet

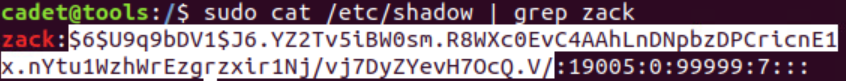
**Question 15 (1 Point)**: What is the output of sudo cat /etc/shadow | grep NAME for the account you just created? (Remember NAME is a variable!) What does the exclamation mark in the output indicate?

‘code:!:19005:0:99999:7:::’

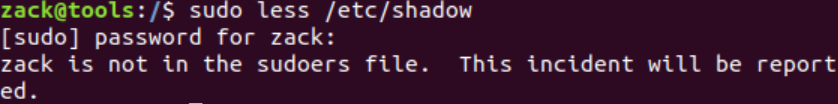
The exclamation mark means that the password is “locked” or hidden from non-root users.

**Question 16 (1 Point)**: Set a password for the new user using: sudo passwd NAME. What is the updated password hash and user ID for the account you just created?

The uid for ‘zack’ is 1006, and the password hash is below (hard to copy out of VM)

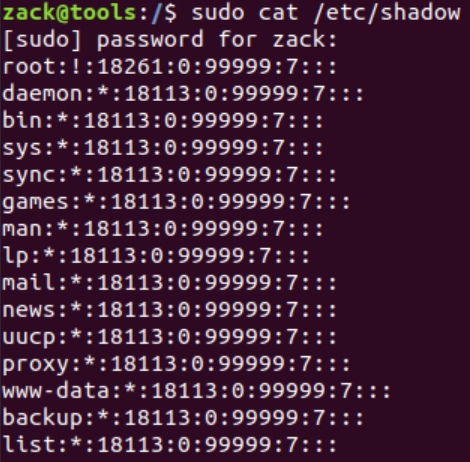


**Question 17 (1 Point)**: Use su to assume the identity of the account you just created then enter sudo less /etc/shadow. Why did you get that result from trying to view the shadow files as your new user?



[It gets reported to the highest arbiter of moral character.](https://www.explainxkcd.com/wiki/index.php/838:_Incident) ‘zack’ doesn’t have permission to view that file (not in super user group) and subsequently gets blocked from opening it.

**Question 18 (1 Point)**: Take a screenshot of all the members of the sudo group, which should include your newly created user. Use su to assume the identity of your new user. Confirm that you are acting as the new user using whoami and that you can now view the contents of /etc/shadow .

 as proof. 

**Question 19 (1 Point)**: Based on the contents of /etc/shadow, what hash algorithm is being used? (MD5, SHA256, or SHA512).

Linux uses MD5 to hash the data in/etc/shadow.

**Question 20 (1 Point)**: Briefly describe a rainbow table attack.

Rainbow table attacks work by constructing a table of the hashes for all characters in the input alphabet (or a set of standard password examples) and then comparing a database of stored passwords to those precomputed hashes.

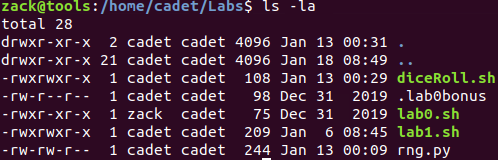
**Question 21 (2 Points)**: Briefly describe how cryptographic salt values enhance password security.

Salts enhance security by preventing attackers from being able to link input strings with stored/precomputed hashes.

**Question 22 (1 Point)**: What are all r/w/x permissions of the /home/cadet/Labs/lab0.sh file? Hint: The answer should begin with -r.

-rwxr-xr-x

**Question 23 (1 Point)**: Take a screenshot of the lab0.sh file in its new location with its new permissions and owner using ls -l.



**Question 24 (2 Points)**: Look at the listening TCP ports using the command netstat -plnt. What ports are currently in a LISTEN state? What programs are associated with those ports? Look up what well-known protocols are associated with those ports. Use the provided table to fill in your answers:

|  |  |  |
| --- | --- | --- |
| Service Name | Protocol | Port |
| DNS | tcp | 53 |
| SSH | tcp | 22 |
| Telnet | tcp | 23 |
| HTTP | Tcp6 | 80 |

**Question 25 (2 Points)**: Take a screenshot of your current active ports using netstat -plnt after you have minimized your attack surface.

**Question 26 (1 Point)**: What is the date, time, and message of the first (so the oldest) entry in the syslog (see note below)? Hint: The current log is syslog , the next most recent is syslog.1 . The older system logs are compressed and have the extension .gz with the oldest having the highest number. As such, tail of syslog (with no integer) is the newest syslog information and head of syslog.X where X is the highest integer is the oldest syslog file.

**Question 27 (1 Point)**: For compressed log files you can use the zcat command to display them without unzipping. Use zgrep on the oldest authentication log file (the one with the highest number) to output the date and time that an authentication failure event occurred. Take a screenshot of your command and the output of the oldest event.

**Question 28 (1 Point)**: Which access control policy do most Linux distros depend upon? Hint: See Chapter 25 from the text.

**Question 29 (5 Points) - Application of Security Primitives Reflection Discussion**:

Take any step executed in this lab and explain it in a short paragraph as it relates to at least two of the terms from the three basic security primitives discussed in lesson 2 (CIA+ Triad, 4 Elements of Defensible Systems, and the 13 Security Design Principles).