Name: _____ Student ID:_____

You will need:
File auth.log.txt on Canvas
Lab Computer

COS30015 IT Security

Lab 7 week 7 (Optional)

In this lab you will watch a tutorial about Password Guessing, Password Spraying and Privilege Escalation Attack, and answer some related questions.

Concepts of Password Guessing, Password Spraying and Privilege Escalation

1. **Password Guessing:**
    - **Concept:** Password guessing is a straightforward attack where an attacker attempts to gain unauthorized access by trying different passwords. This can be done manually or through automated tools. Common targets are accounts where passwords might be weak, default, or commonly used.
    - **Approach:** Attackers might use brute force (trying all possible combinations), or a more refined approach using dictionaries of common passwords.
2. **Password Spraying:**
    - **Concept:** Password spraying takes a different approach by using a few common passwords against a large number of usernames. Unlike password guessing, which focuses on breaking into one account by trying many passwords, password spraying aims to access many accounts by trying only a few commonly used passwords.
    - **Approach:** This type of attack is effective against systems with lockout policies that lock accounts after a few unsuccessful login attempts, as it tries to avoid triggering these security measures.
3. **Privilege Escalation:**
    - **Concept:** Privilege escalation occurs when a user with limited permissions exploits a vulnerability in a system to gain unauthorized access or elevated privileges that they are not entitled to. This can happen after an attacker has gained initial access through other means (like password guessing or spraying).
    - **Approach:** There are two types of privilege escalation: vertical and horizontal. Vertical escalation involves gaining higher-level privileges (e.g., user to admin), while horizontal escalation involves expanding access across accounts at the same privilege level.

4. Differences:

- **Focus and Goal:**
    - **Password Guessing and Spraying:** Both focus on gaining initial access using passwords but differ in strategy—guessing attacks individual accounts intensively, while spraying targets multiple accounts with fewer attempts per account.
    - **Privilege Escalation:** Assumes initial access is already obtained and focuses on gaining broader or higher-level access than initially granted.
- **Methodology:**
    - **Password Guessing:** Often involves intensive effort on a single account.

- **Password Spraying:** Involves minimal effort per account but targets many accounts to increase the likelihood of success.
- **Privilege Escalation:** Utilizes system vulnerabilities, misconfigurations, or software flaws rather than relying on password vulnerabilities.

Understanding these differences is crucial for implementing effective security measures, such as robust password policies, account lockout policies, regular audits of user permissions, and timely patching of known vulnerabilities.

Guidance on interpreting the log structure

```
Feb 10 15:45:09 ubuntu-lts sshd[47341]: Failed password for root from
103.106.189.143 port 60824 ssh2
Feb 10 15:45:11 ubuntu-lts sshd[47341]: Connection closed by
authenticating user root 103.106.189.143 port 60824 [preauth]
Feb 10 15:45:11 ubuntu-lts sshd[47339]: Failed password for root from
180.101.88.228 port 11349 ssh2
Feb 10 15:45:12 ubuntu-lts sshd[47343]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=103.106.189.143  user=root
Feb 10 15:45:14 ubuntu-lts sshd[47339]: Failed password for root from
180.101.88.228 port 11349 ssh2
Feb 10 15:45:14 ubuntu-lts sshd[47343]: Failed password for root from
103.106.189.143 port 33990 ssh2
Feb 10 15:45:16 ubuntu-lts sshd[47343]: Connection closed by
authenticating user root 103.106.189.143 port 33990 [preauth]
Feb 10 15:45:16 ubuntu-lts sshd[47339]: Received disconnect from
180.101.88.228 port 11349:11:  [preauth]
Feb 10 15:45:16 ubuntu-lts sshd[47339]: Disconnected from authenticating
user root 180.101.88.228 port 11349 [preauth]
Feb 10 15:45:16 ubuntu-lts sshd[47339]: PAM 2 more authentication
failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=180.101.88.228
user=root
Feb 10 15:45:18 ubuntu-lts sshd[47345]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=103.106.189.143  user=root
Feb 10 15:45:21 ubuntu-lts sshd[47345]: Failed password for root from
103.106.189.143 port 35180 ssh2
. . .
```

This real-time log stream provides insights into authentication attempts, highlighting failed password entries, successful logins, session disconnections, root privilege escalations, and other significant events. Here is a example slice of a log.

Feb 10 15:45:14 ubuntu-lts sshd[47343]: Failed password for root from 103.106.189.143 port 33990 ssh2

The log provides the "who" root), the "what" (Failed password), the "when" (Feb 10 15:45:14), the "where" (103.106.189.143) and the "how" (ssh2) of the authentication

event. Thanks to these specifics, it is feasible to track trends in login origins, methods, and to pinpoint authentication attacks. The following screenshot is another example that shows the entire log-in and log-out process:

```
Sep 16 16:38:23 xxxxxx sshd[750]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=194.59.249.21  user=root
Sep 16 16:38:25 xxxxxx sshd[750]: Failed password for root from 194.59.249.21 port 49252 ssh2
Sep 16 16:38:29 xxxxxx sshd[750]: Accepted password for root from 194.59.249.21 port 49252 ssh2
Sep 16 16:38:29 xxxxxx sshd[750]: pam_unix(sshd:session): session opened for user root by (uid=0)
.....
Sep 16 18:49:49 xxxxxx sshd[750]: pam_unix(sshd:session): session closed for user root
```

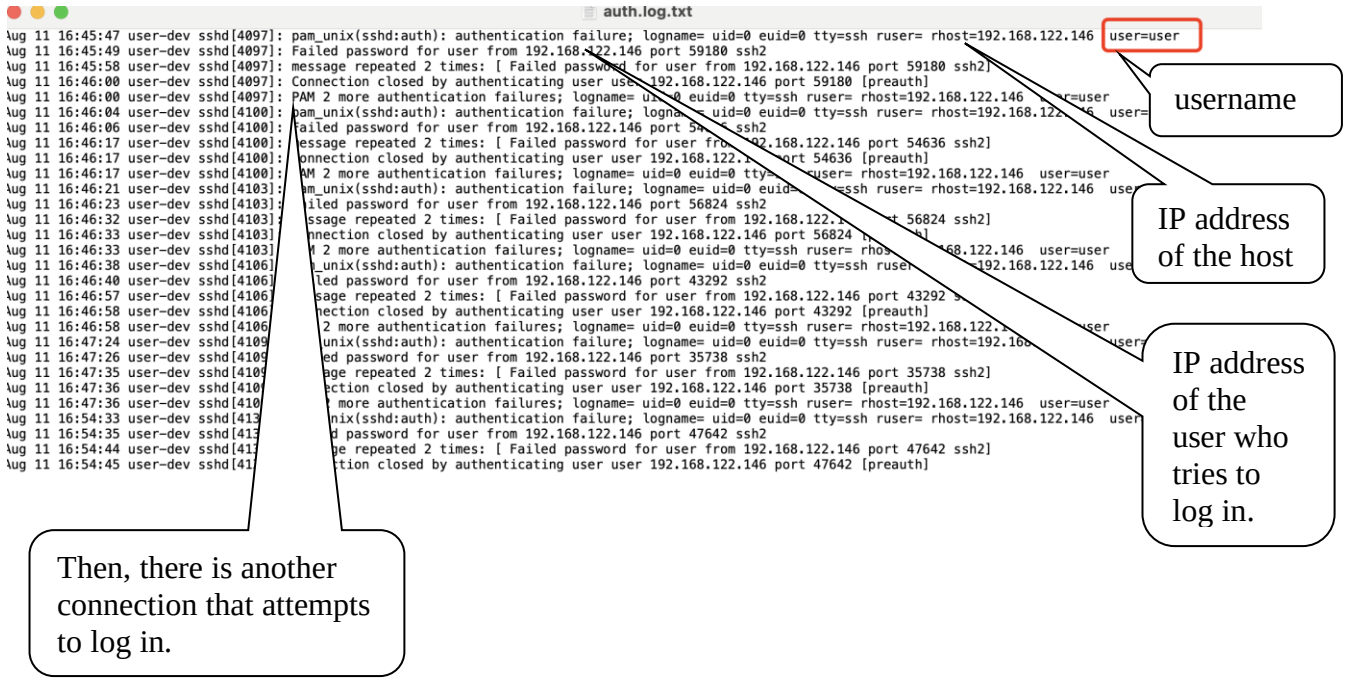
1. Someone tried to log in as the root user at 16:38:23 and failed the password at 16:38:25.
2. 4 seconds later, they type in the correct password and get into the server.
3. 2 hours and 10 minutes later, they log out.

Part 1: Password Guessing

The following exercises are about Password Guessing Attack.
The goal is to have a good understanding of reading the log to identify the potential attacks.

Open the file auth.log.txt from Canvas.

Here is a part of the file auth.log.txt. Let's the following four pieces of information as an appetiser.



Name: _____ **Student ID:**_____

1. **What is the definition of password guessing? Look it up.**

   Password guessing is a type of cyber attack where an attacker tries to gain unauthorized access to a user account by systematically trying various possible passwords. This method can involve the use of brute force techniques, where all possible combinations are tried, or more commonly, dictionary attacks, which use lists of well-known, previously breached, or simple passwords. The attacker targets a specific user account and tries numerous passwords with the hope that one of them will be correct.

2. **What kind of attack is it for the first connection session? (e.g. password spraying, password guessing and privilege escalation, any of them?)**

   Password Guessing

3. **Identify a series of failed password attempts from a single IP address to a single user account. Provide the IP address and username involved.**

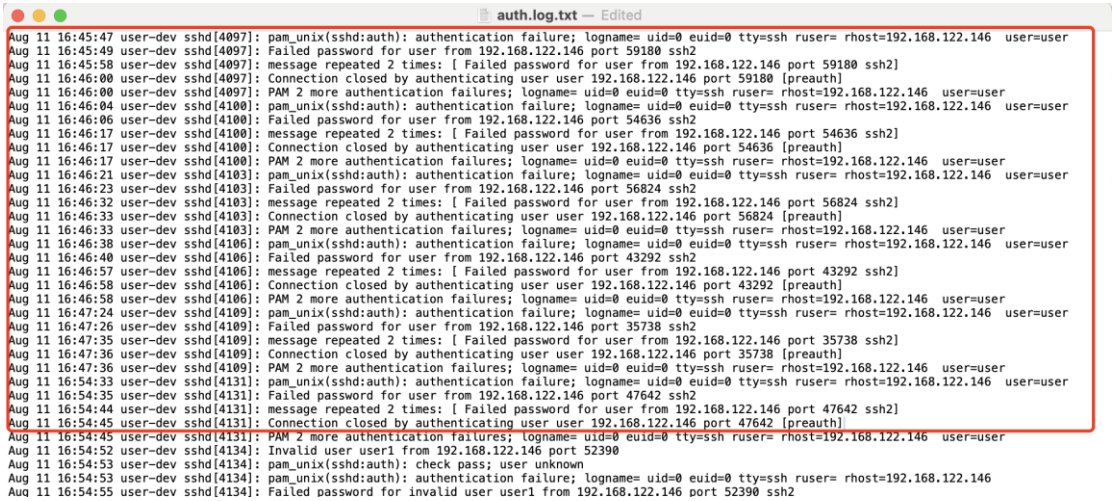
   Answer: *IP 192.168.122.146, User: user*

4. **What time interval do these attempts occur over?**

   About 0-2 seconds

5. **Are there any differences in the server responses to valid vs. invalid users after failed password attempts? Provide examples.**

Response for valid users: "failed password for user" in log.
Response for invalid users: "Failed password for invalid user" in log.



6. **From line 1 to line 29, how many times did this type of attack happen?**

6 attempts were made.

7. **What could be inferred about the password strength of the user based on the log data?**

The user likely has a strong password since multiple attempts failed.

8. **Suggest a security measure that could prevent this type of attack.**

Implement account lockout policies after a few unsuccessful login attempts.

Name: _____ **Student ID:**_____

Part 2: Password Spraying.

The following exercises are about Password Spraying Attack.
The goal is to have a good understanding of reading the log to identify the potential attacks.

9. What is password spraying? Look it up.

Password spraying is a form of cyber attack that differs from password guessing by targeting many user accounts with a few commonly used passwords rather than attempting many passwords on a single account. This strategy helps avoid triggering account lockouts that many security systems use to prevent brute force attacks. It relies on the assumption that at least some user accounts will use common, weak passwords, making it more efficient against organizations with basic or default password policies.

10. How does password spraying differ from password guessing based on the log entries?

Password spraying targets multiple accounts with likely common passwords, while password guessing targets one account with multiple password attempts.

11. **From line 30 to line 54 in the screenshot above, Identify evidence of password spraying by showing different usernames being targeted from the same IP address with a common password.?**

Attempts from IP 192.168.122.146 on multiple user accounts (user1, user2, user3, user4) with repeated failed attempts.

12. **List the usernames that were targeted during this spraying attack.**

Usernames user1, user2, user3, user4.

13. **What could be a countermeasure to mitigate the risk of password spraying?**

Use multifactor authentication and enforce complex password policies.

Part 3: Privilege Escalation.

The following exercises are about Privilege Escalation.
After gaining access, attackers might attempt to escalate their privileges to gain broader access to the system's resources.
The goal is to have a good understanding of reading the log to identify the potential Privilege Escalation.

Name: _____ **Student ID:**_____

Let's look at this part of log.

auth.log.txt

```
Aug 11 16:56:20 user-dev sshd[4143]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.122.146  user=user4
Aug 11 16:59:16 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:19 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 16:59:22 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:24 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 16:59:27 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:30 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 16:59:33 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:35 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 16:59:38 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:41 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 16:59:45 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:46 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 16:59:50 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:53 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 16:59:57 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 16:59:59 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 17:00:03 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 17:00:05 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 17:00:09 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 17:00:11 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 17:00:14 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=root
Aug 11 17:00:17 user-dev su: FAILED SU (to root) user on pts/0
Aug 11 17:00:45 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=user2
Aug 11 17:00:47 user-dev su: FAILED SU (to user2) user on pts/0
Aug 11 17:00:53 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=user3
Aug 11 17:00:55 user-dev su: FAILED SU (to user3) user on pts/0
Aug 11 17:01:00 user-dev su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/0 ruser=user rhost=  user=user4
Aug 11 17:01:02 user-dev su: FAILED SU (to user4) user on pts/0
```

14. What is the definition of Privilege Escalation? Look it up.

Privilege escalation occurs when an attacker exploits a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The process allows the attacker to obtain privileges that are not intended for them, ranging from administrative to higher-level permissions than originally granted. Privilege escalation can occur either horizontally (acquiring privileges of a different user of the same level) or vertically (acquiring higher-level privileges), often leading to unauthorized system access, data theft, or control over system functions.

15. Find an instance where a user attempts to switch to a higher privilege account. Identify the usernames and target account.

User user attempts to switch to root.

16. How many attempts were made to escalate privileges to the root user?

11 attempts.

17. What was the result of these privilege escalation attempts?

All attempts failed.

18. What security mechanism seems to be in place to prevent successful privilege escalation?

Authentication failures indicate strong password requirements and possibly limited sudo or su access rights.

19. Suggest an audit or monitoring strategy that could detect such attempts more proactively.

Implement real-time monitoring and alerting for repeated failed login attempts, especially on sensitive accounts like root.