### COS30015 IT Security

You will need:

File auth.log.txt on Canvas

Lab Computer

### 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.

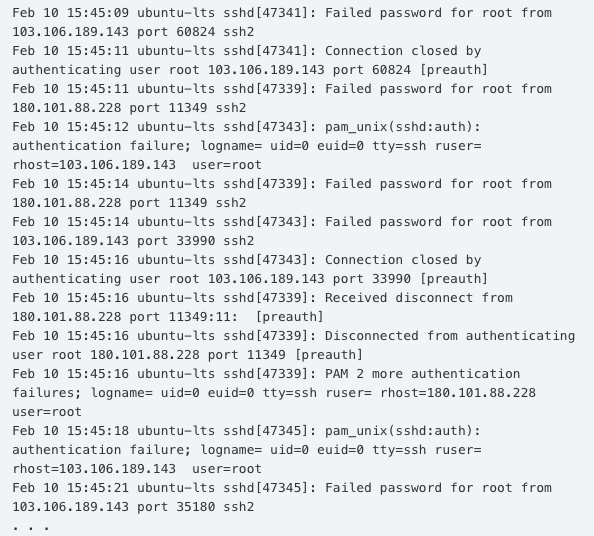
**Concepts of Password Guessing, Password Spraying and Privilege Escalation**

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.

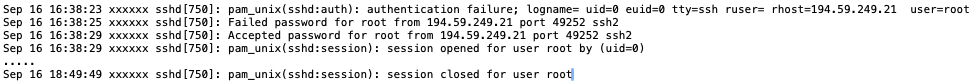
**Guidance on interpreting the log structure**



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:

**

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.

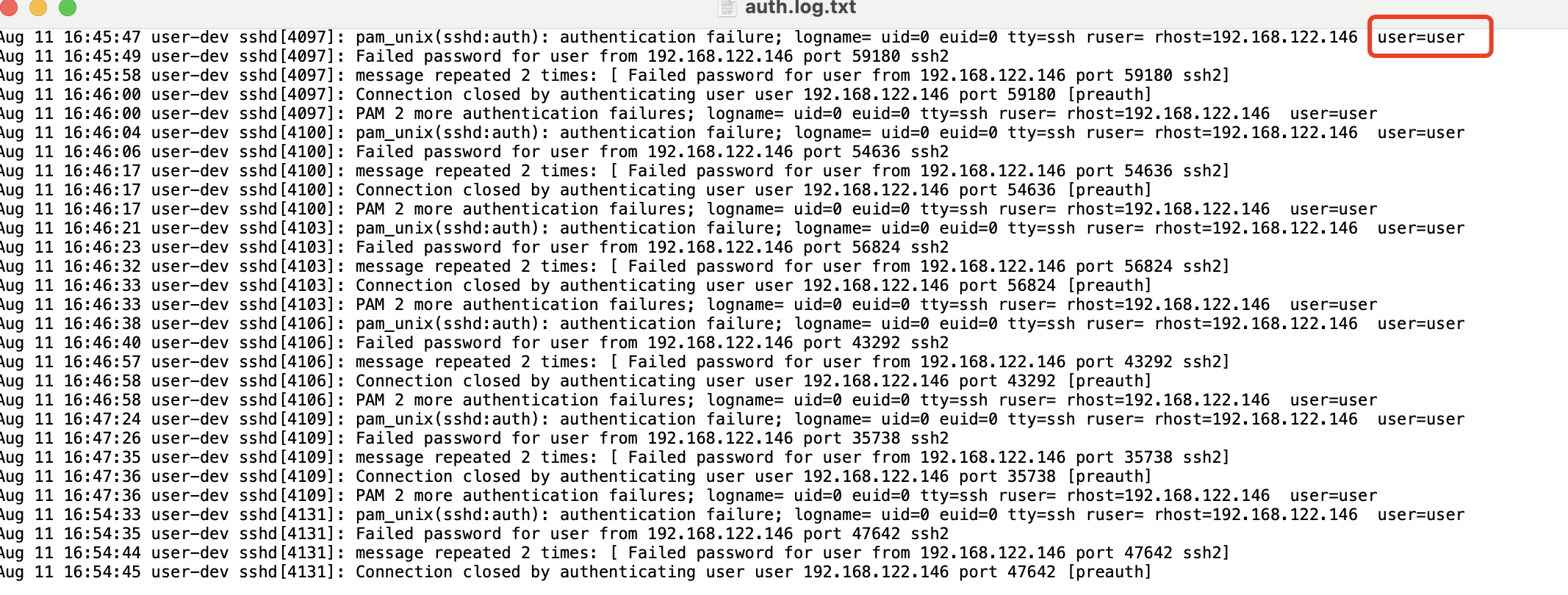
3. 2 hours and 10 minutes later, they log out.

### 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.

****

username

IP address of the user who tries to log in.

IP address of the host

Then, there is another connection that attempts to log in.

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

After the first attempt to log in, there are two other attempts too.

1. **What kind of attack is it for the first connection session? ( e.g. password spraying, password guessing and privilege escalation, any of them?)**
2. **Identify a series of failed password attempts from a single IP address to a single user account. Provide the IP address and username involved.**
3. **What time interval do these attempts occur over?**
4. **Are there any differences in the server responses to valid vs. invalid users after failed password attempts? Provide examples.**

***A screenshot of a computer

Description automatically generated***

1. **From line 1 to line 29, how many times did this type of attack happen?**
2. **What could be inferred about the password strength of the user based on the log data?**
3. **Suggest a security measure that could prevent this type of attack.**

### 

### 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.

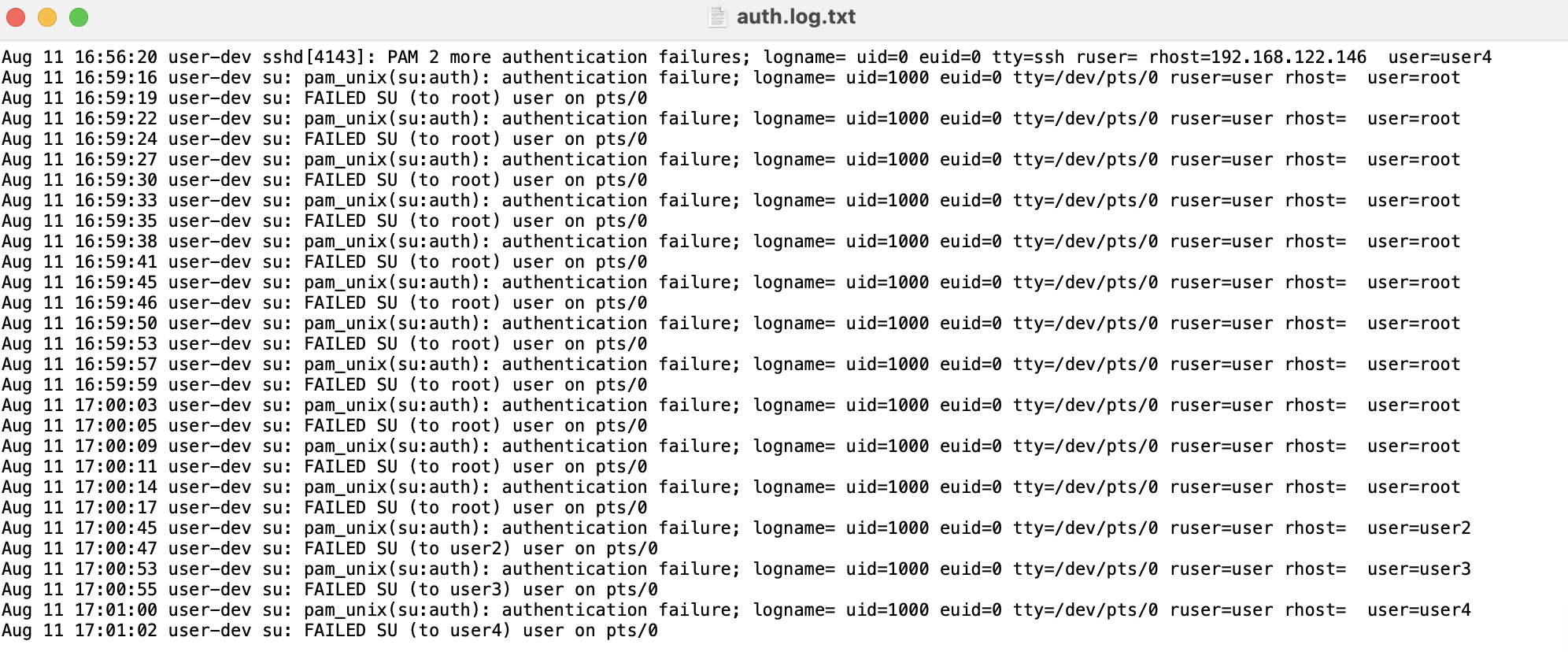
1. **What is password spraying? Look it up.**
2. **How does password spraying differ from password guessing based on the log entries?**
3. **From line 30 to line 54 in the screenshot above, Identify evidence of password spraying by showing different usernames being targeted from the same IP address with a common password.?**
4. **List the usernames that were targeted during this spraying attack.**
5. **What could be a countermeasure to mitigate the risk of password spraying?**

### 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.

**Let’s look at this part of log.**

****

1. **What is the definition of Privilege Escalation? Look it up.**
2. **Find an instance where a user attempts to switch to a higher privilege account. Identify the usernames and target account.**
3. **How many attempts were made to escalate privileges to the root user?**
4. **What was the result of these privilege escalation attempts?**
5. **What security mechanism seems to be in place to prevent successful privilege escalation?**
6. **Suggest an audit or monitoring strategy that could detect such attempts more proactively.**