Detecting Brute Force Attacks BY P3NGU1N

Brute Force Attacks

🎯 What is the name of the password cracking method that uses a pre-calculated hash table to crack the password ?

ANSWER: Rainbow table attack

Protocol/Services That Can Be Attacked by Brute Force

🎯 What is the name of the attack that the attackers usually made on the protocol running on port 22 in order to obtain a session on a linux server?

ANSWER: SSH Brute Force

How to Avoid Brute Force Attacks?

🎯 After logging in the username and password, what is the name of the method in which a second verification is made to the user with an additional verification mechanism (SMS, mail, token,push notification, etc.)?

ANSWER: 2FA

Windows Login Brute Force Detection Example

🎯 What is the event id value that indicates that the user is successfully logged in to a Windows system?

ANSWER: 4624

QUIZ:

🎯 **Which of the following tools is used to perform a brute force attack?**

ANSWER: **John the Ripper**

🎯 **Which of the following passwords is difficult for an attacker to crack?**

ANSWER: **eux-1Ac-!dk3-cU0**

🎯 **Which of the following protocols is used in brute force attacks?**

ANSWER: RDP

🎯 **Which of the following pages do attackers use to perform a brute force attack?**

ANSWER: **Login pages**

🎯 **Which of the following tools was created specifically to perform brute force attacks on wireless?**

ANSWER: **Aircrack-ng**

🎯 **Which of the following tools cannot perform an RDP brute force attack?**

ANSWER: **Wfuzz**

🎯 **What is the name of the password cracking method that uses a pre-calculated hash table to crack the password?**

ANSWER: **Rainbow table attack**

🎯 **Using which of the following event IDs can you detect RDP brute force attacks?**

ANSWER: **4624-4625**

🎯 **Which of the following is not used to prevent brute force attacks?**

ANSWER: **Monitoring login activities**

🎯 **What is the purpose of brute force attacks?**

ANSWER: **Gaining unauthorized access**

🎯 **Which of the following is the brute force category in which the attacker cracks the previously captured encrypted or hashed passwords without establishing an active connection with the target system?**

ANSWER: **Offline brute force attacks**

🎯 **Which of the following files does not contain a password hash?**

ANSWER: **/var/log/auth.log.1**

🎯 **In which file SSH brute force logs are kept on Linux?**

ANSWER: **/var/log/auth.log**