QUESTION 6 :

Part a:

1. Players : Max - System and Min - Attacker
   Objectives :

   Max maximizes security and minimizes the damage caused by attacker.
   Max wants to minimize any damage the attacker might cause by making smart, proactive decisions

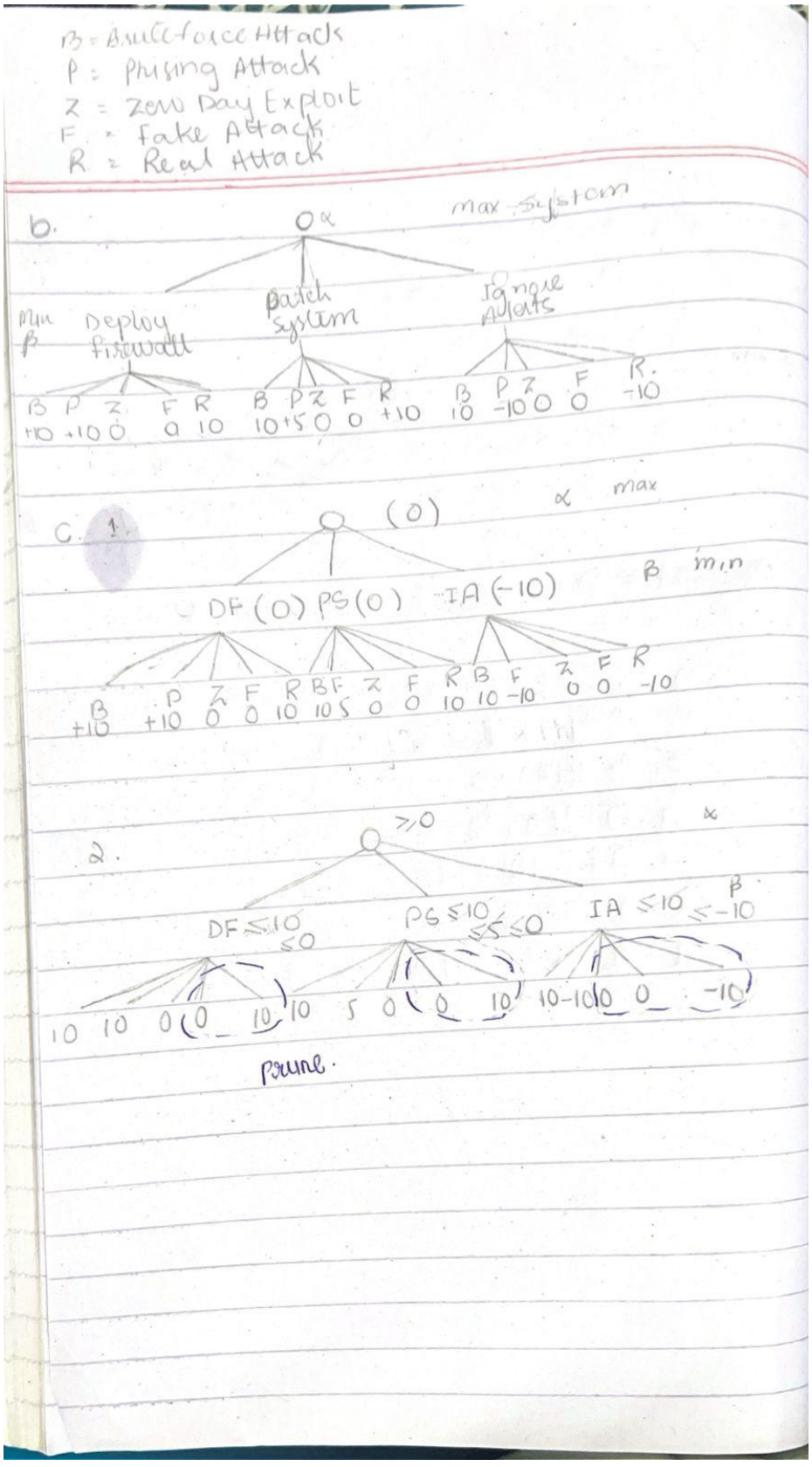
   Min , minimizes the defender's success by selecting attacks that are most likely to succeed.

2. Max (System) : Using algorithms like Minimax, the IDS selects the action that maximizes its utility (security), assuming the attacker will choose the worst-case response.

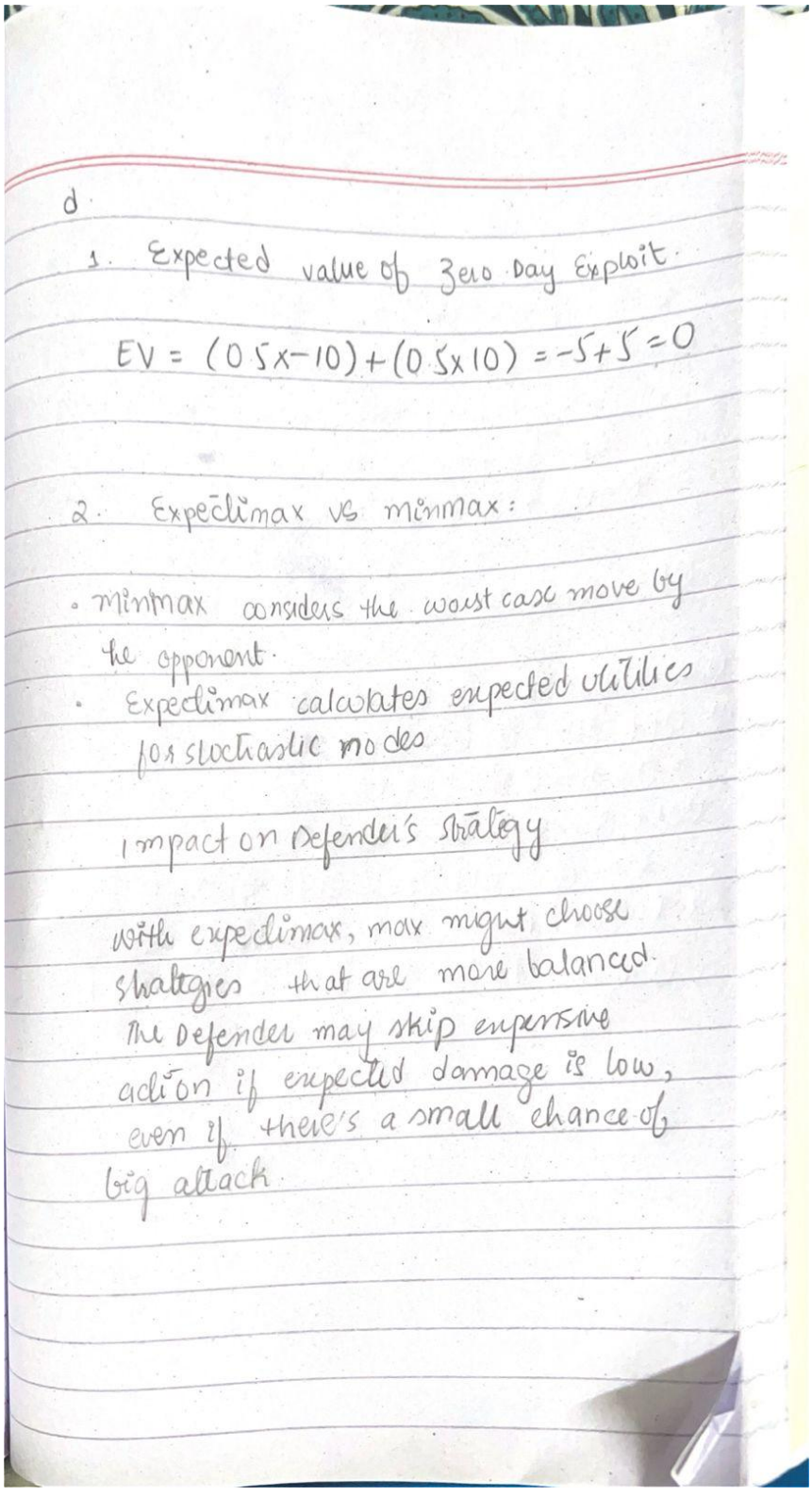
   Min (Attacker) : The attacker chooses the action that yields the lowest utility for the defender, assuming optimal play by the system.

3. Stochastic elements:
   Zero-day exploits introduce uncertainty with a 50% chance of success.
   Impact of defender's strategy:
   The IDS must account for uncertainty by computing expected utilities at chance nodes.
   This uncertainty forces the IDS to balance risk and reward, potentially favoring strategies like patching the system to reduce vulnerabilities, even if zero-day exploits remain possible.

Part b. & c.


B = Brute-force Attacks
P = Phising Attack
Z = Zero Day Exploit
F = Fake Attack
R = Real Attack
b.
max system
Deploy firewall
Patch system
Ignore Alerts
B P Z F R
+10 +10 0 0 10
B P Z F R
10 +5 0 0 +10
B P Z F R
10 -10 0 0 -10
c. 1.
(0)
max
DF (0) PS (0) IA (-10)
min
B P Z F R B F Z F R B F Z F R
+10 +10 0 0 10 10 5 0 0 10 10 -10 0 0 -10
2.
≥0
DF ≤10 ≤0
PS ≤10 ≤5 ≤0
IA ≤10 ≤-10
10 10 0 0 10 10 5 0 0 10 10 -10 0 0 -10
prune.

Part d.



d

1. Expected value of Zero Day Exploit.

$EV = (0.5 \times -10) + (0.5 \times 10) = -5 + 5 = 0$

2. Expectimax vs minmax:

- Minmax considers the worst case move by the opponent.
- Expectimax calculates expected utilities for stochastic nodes

Impact on defender's strategy

With expectimax, max might choose strategies that are more balanced. The defender may skip expensive action if expected damage is low, even if there's a small chance of big attack.