24-S1-Q3

Q (a) brute, dictionary, rainbow, MFA

(i) 102, 8, 8×10^9, time?

(ii) compare: biometrics & password
in security

(b) vulnerabilities of IOT → botnets

(i) DDOS: 5×10^6 10×10^9 64k

(ii) Botnet.

Solution (a) password attacks and MFA

① Brute Force: Systematically trying all possible combinations

② Dictionary Attacks: Trying common words or phrases, often with slight modifications.

③ Rainbow Tables: Using large precomputed table mapping hashes back to candidate

④ Multi-Factor Authentication (MFA) mitigate password attacks by requiring not just something you know, e.g. password, but alse something you have, e.g. smartphone, or something you are, e.g. biometrics. Even if the password is cracked. an attacker lacks the additional factor

(i) crack password

$$t = \frac{102^8}{8 \times 10^9} = 1464574.226 \ s$$

$1464574.226 \div 60 \div 60 \div 24 \div 365$

$= 0.04644$ year

(ii) Password -Based

① Relies on a user remembering and securely managing a secret string

② Vulnerable to brute-force, phishing, password reuse and social engineering

③ Simple to implement but can be less secure, especially if users pick week passwords.

Password - Less

① Difficult to Hack

Biometric systems are incredibly difficalt to hack as it can't be guessed or cracked like passwords. Generally more resistant to remote attacks and phishing

② Convenient: faster and reduces reliance on user momory and caution

③ user might authenticate with a biometric. ike fingerprint, facial recognition, iris, retinal and so on, or a physical device.

④ Implementation can be more complex and has potiential privacy concerns, such as storing or transmitting bio metric data

⑤ Complacency: It can lead to reklessness when logging in.

⑥ High Risk: You can change passwords, but you can't change your biometric details If your biometric data is stolen or lost, it coub be permanetly compromised

⑦ Duplication / Cloning is easy.

(b) IoT vulnerabilities

① IOT Devices Vulnerable to compleee tacKover

② Many IOT devices ship with default credentials, rarely receive firmware updates, and often lack robust patching mechanisms

③ Attacker Scan the internet to locate IoT then infect them with malware to form large botnets.

④ A single IoT is relatively weak, but millions of these compromised bots can collectively overwhelm high-capacity targets.

(i) DDOS

$$\text{packets} = \frac{10\times10^{9}}{64\times1024\times8}$$

$$= 19073.4863$$

So, about 19074 packets per second will fill up a 10 Gbit/s link.

(ii) ① Recruitment of Devices

(1) Attackers scan the in~~ter~~net for vulnerable IoT devices

(2) Once the device is compromised, often via weak/default passwords or unpatched firmware, malware is upload.

(3) the device becomes a "bot" awaiting commands from the attacker command and control server

② Centralized Control

(1) the tacker can use program to

simultaneouly instruct millions of compromised devices to send traffic to a target

(2) Because the traffic sources are globally distributed, it is much harder to block than a single origin

③ coordinate attack

(1) Botnets can generate enormous amount. of traffic, such as HTTP request UDP packets. TCP SYN floods, etc to exhaust a victim's bandwidth or CPU

(2) This flood the target's network, leading to denial of service for legitimate.