Part C

Brute force

Intrusion prevention tools like fail2ban and denyhosts are subject to log based attacks. IPtables can stop ssh brute force attacks. The iptables rules are relatively simple. This rule will block an IP if it attempts more than 3 connections per minute to SSH.

Password guessing

The most common type of attack is password guessing. Weak passwords can be easily guessed. It is a good idea to have a strong password. An attacker needs to find only one weak password to gain access to a network

Password Resetting

Many password cracking programs are actually password resetters. Most password resetters contain a bootable version of Linux that can mount NTFS volumes and can help you locate and reset the Administrator's password.

Password Cracking

Password cracking is the process of taking a captured password hash and converting it to its plaintext original. Pwdump4 is the most used hash extractor. It is done by generating some guesses for the password, then hashing the guesses and comparing those hashes with the extracted hash.

References

Grimes, R. (2017). *Types of Password Attacks*. [online] IT Pro. Available at: http://www.itprotoday.com/security/types-password-attacks [Accessed 1 Dec. 2017].