1. intitle: "index of" mp4 - site: "adelaide.edu.au"

2. Defend on multiple levels
   - mechanisms to detect ransomware uploaded as attachments
   - blocking addresses reported to have uploaded / sent ransomwave prior
   - warnings to not run executables in attachments.

3. availability

4. preventive

5. red' <script> alert(1) </script> </div>

6. "'; select t1.id, t1.firstname, t1.lastname, t2.password from t1 inner join t2 on t1.id = t2.id;"

7. ARP poisoning, DNS spoofing

8. - think outside the box - from the perspective of a black hat
   - always try to stay ahead - checks in place stop security issues in the first place

9. Black hat - illegal hacking for personal gain - hacking bank for financial gain
   White hat - preventative measures to stop black hats - stopping bank hackers
   Grey hat - somewhere in the middle of black / white - sometimes doing morally wrong illegal activities for ethical reasons - digital piracy for archival

10. No. Variables declared top down are reversed by the compiler in the stack, so grade actually comes before buff, and therefore a buffer overflow cannot occur. Would be possible if variables were declared in a struct.

11. Yes, it's possible. check comes after buff in the stack and the flags don't stop buff overflow.
    AAAA AAAA AAAA "2019" (hex equivalent)

12. true

13. False.

14. LSB

15. unlikely

16. keep security simple
    fail securely

17 per 100 years – pay 75% of $10 million to replace

= 7,500,000

per year = $\frac{7,500,000}{100}$

= $75,000

18. SIEM – consolidate and organise all log data to make review easier

IDS - simply detect any intrusion attempts

19. WEP

20. all 4

intercept

eavesdrop

impersonate

modify

21. a way to reverse the compile process - convert binary executable back to high level code

-helps to understand how program works

– help to recreate it or exploit it.