



Complete, fold and seal
(see note 2 below)

FORENAME(S): William

12 Pages

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, fold over and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can either ignore illegible script or have it typed and the expense of typing charged to the candidate.
4. Write your answers in ink.
5. Begin each answer on a fresh page. Do all rough work in the answer book and cross it through.
6. No part of this book is to be torn out; it must be handed in complete.
7. If more books than one are used, fasten them together using the tags available from the invigilator(s).
8. **Every book must be handed in. In no circumstances may answer books, used or unused, be taken out of the examination venue.**

[illegible]

(Gweler yr ochr arall am y fersiwn Cymraeg)

41%



1ai Virus life -

Attacker creates virus → Virus becomes accessible online → user downloads virus → Virus relays information to attacker

Virus can attempt to access admin areas on the PC such as windows/system32.

Slows users / System down

Virus clones itself

Anti-virus detects and removes virus. and attempts to hide

~

1aii If a virus infected a computer then it could slow down the system by running malicious code to hog the system resources to prevent the user from doing any tasks.

The virus could be using unwanted network traffic so ~~use~~ using task manager to see what's using the network is a good idea. The best would be using resource monitor to check each application with network permissions that's open.

Too many invalid login attempts such as the virus could be trying to access the local administrator account and using logs this will support the theory.

The virus could cause applications to stop working or locking the users files which would be a clear indication of a virus.

laill

Countermeasures -

Anti-virus - Regular updates turned on.
Weekly Scan of system
Scan new files ~~auto~~ once downloaded.

Firewall - To block ~~network~~ ^{un-trusted} Services
To warn the user if the site is trusted
To ~~detect~~ ^{new} network connections and prompt the user.

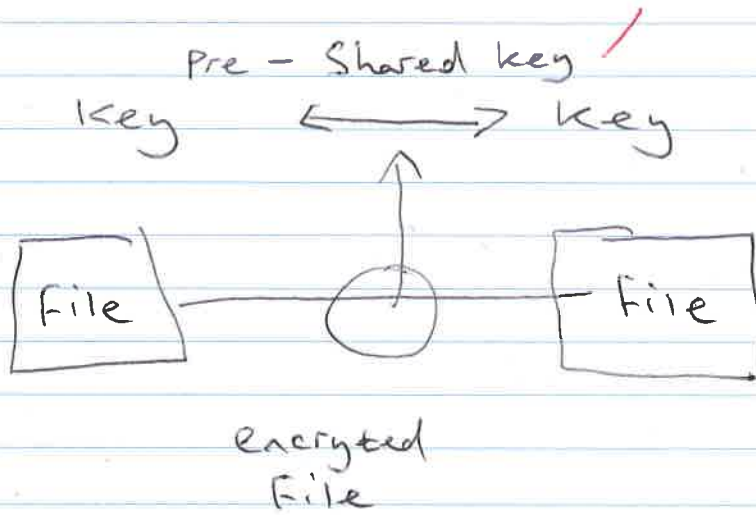
Sandbox - using an application called Sandboxie
Sandbox runs the new application in a boxed off portion on the hard drive so the application cannot access the users files.

Web browser - Chrome has an in-built anti-virus which scans the downloads for you and removes them if it's been reported as a threat. It will even warn the user of phishing sites.



There are online anti-virus sites which allow a user to upload the file before opening it and scan the file against all the top anti-virus software.

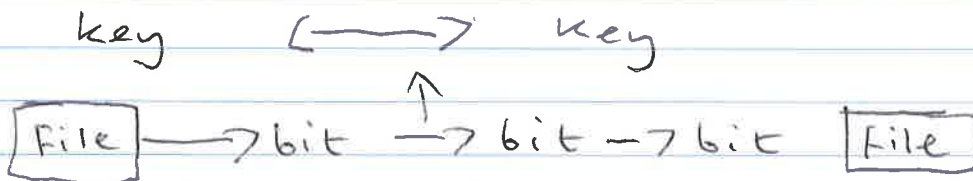
3a Symmetric —



The file is encrypted with a key which is shared with the end user to de-encrypt it.

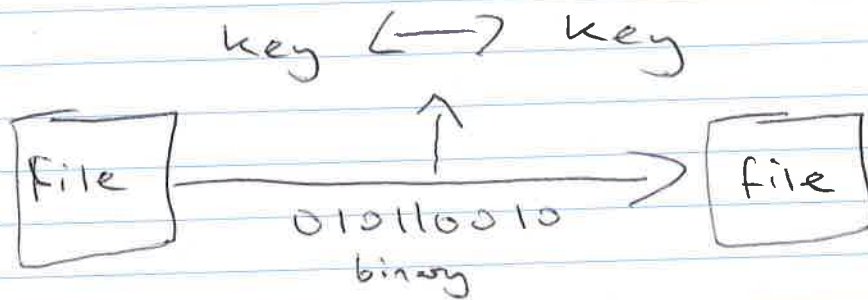
Symmetric uses 80-256 bit encryption and can be found in AES which is used for WiFi.

Asymmetric —
Two forms (block chain or stream)
Block —



Block sends the file in ~~bits~~ blocks.

Stream -



Stream sends the file in bits in 0 and 1.

Asymmetric uses 512-4096 bit encryption.
Example - RSA, used in VPNs

public key - shared online

private key - only known to the file owner.

36

Network Scanning - Searching for open ports
Network mapping
MAC Table
IP Subnet
Network Services
OS on system.

OS - Exploiting the binary of the OS.

Attempting rootkit access.

Exploiting the system if the latest system patches aren't installed.

4a

Android devices use SQLite.

Android is a linux-based OS.

Android can be secured by installing an anti-virus.

Android can perform various attacks.



Android, -

Pros

- Google play policy.
- Anti-virus.
- Encryption.
- Applies to Bgood policy.
- Standard OS.
- Security patches ~~more~~

Cons

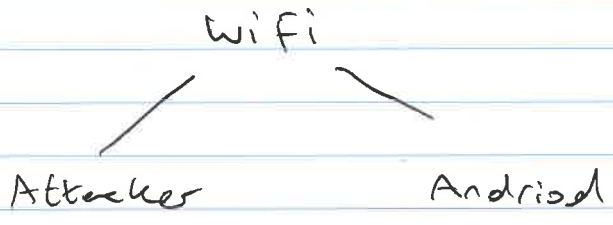
- Root-Access
- Binary changed
- Direct .Apk installed
- low-level encryption
- Bricking device.
- Custom OS/kernel.
- Outdated ~~it~~ - No patches
- Rootkit.
- Firewall requires root
- CAN be used as a network scanner

10

Android is a Google INC OS. ~~It is not~~
A ~~no~~

46

Pen-test



- Network Scan for - Open Ports on devices.
- Android Version.
- Mac address.
- IP information.

Attacker looks up the vendor information from the mac address gathered.

The attacker can research the android version of the device and look for any exploits such as binary, rootkit or security patches.

The attacker would launch an attack on the open port if found and attempt to access the device.

The attacker could or ~~make~~ made a fake APK for the user to download to open a port. The APK would be designated like a common application or an application to best fit that person being attacked.

The APK could launch other attacks if root-access has been giving on the android device giving the attacker more kernel access to the device.