5.3 Cyber security

Brute force attack

Question

A manager at a company is concerned about a brute-force attack on its employee user accounts.

(a) Describe how a brute-force attack can be used to gain access to the employee user accounts.

[3]

(b) State three aims for carrying out a brute-force attack to gain access to the employee user accounts.

[3]

(c) Give two security solutions that could be used to help prevent a brute-force attack being successful.

[2]

(a) Three from:

- Trial and error to guess a password
- Combinations are repeatedly entered...
- ...until the correct password is found
- Can be carried out manually or automatically by software

(b) Any three from:

- Install malware
- Steal/view/access data
- Delete data
- Change data
- Lock account // Encrypt data
- Damage reputation of a business

(c) Any two from:

- Two-step verification // Two-factor authentication // by example
- Biometrics
- Firewall // Proxy-server
- Strong/complex password // by example
- Setting a limit for login attempts
- Drop-down boxes
- Request for partial entry of password

Question

A finance company is concerned that a hacker may perform a brute-force attack to gain access to an employee's account.

(a) Describe how the hacker would perform the brute-force attack.

[2]

(b) Give three cyber security solutions that could be used to help prevent a brute-force attack from being successful.

[3]

(a) Two from:
Trial and error to guess a password
Combinations are repeatedly entered...
...until the correct password is found

(b) Any three from:
Two-step verification // Two-factor authentication
Biometrics
Strong/complex password
Setting a limit for login attempts
Firewall // Proxy-server

Data interception

Question

(a) Draw and annotate a diagram that demonstrates the cyber security threat of data interception.

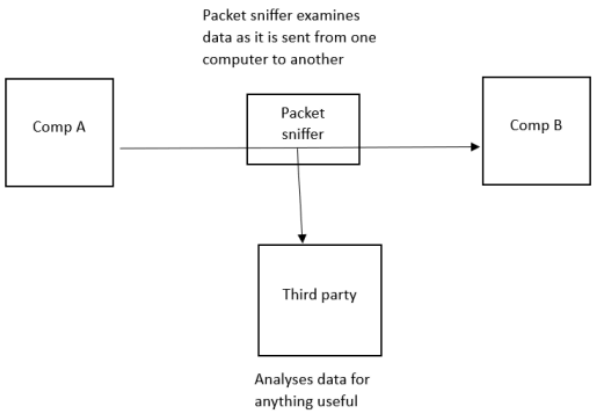
[4]

(b) Identify one security solution that will help keep data safe from data interception and state why it will help keep data safe.

[2]

(a) Four from:

- Data is being sent from one device to another
- **The data is being examined during transmission**
- Packet sniffer is used
- Intercepted data is reported to a third-party during transmission ...
- ... and analysed for anything useful
- Connection hacked to spoof destination address



(b)

- Encryption
- **If the data intercepted, it is meaningless**

DDoS

Question

(a) Draw and annotate a diagram to show the process of DDoS.

[4]

(b) Identify a solution that prevents DDoS from being successful.

[1]

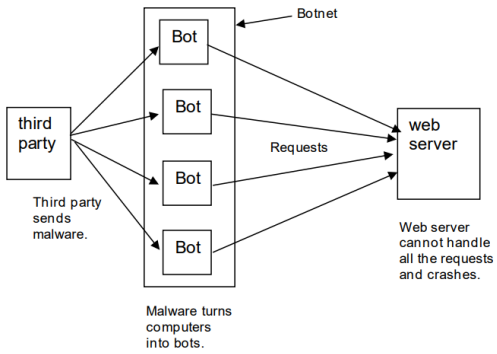
(c) State two aims of a DDoS attack.

[2]

(a) Four from:

- A perpetrator/third party sending malware // user downloads/installs
- Each computer is turned into a bot...
- ... to create a botnet
- Third party initiates the attack
- **All the bots send a request at once to a web server**
- ... crashing the webserver

e.g.



(b) Proxy server // Firewall // Anti-malware

(c) Any two from:

- Revenge
- To damage the company's reputation
- Entertainment value
- To demand a ransom to stop it
- To test a system's resilience

Question

Complete the statements about a distributed denial of service (DDoS) attack. Use the terms from the list: anti-virus, bot, botnet, malware, hacker, spyware, web browser, internet, secondary storage, web server, website.

The attacker encourages people to download ..... onto their computer. This will turn each computer into a ..... , creating a network called a ..... .
When the attacker wants the DDoS to take place, repeated requests are simultaneously sent from the computers to a ..... . This causes it to crash, meaning that users can no longer access the ..... that is stored on this hardware.

[5]

The attacker encourages people to download **malware** onto their computer.
This will turn each computer into a **bot**, creating a network called a **botnet**.
When the attacker wants the DDoS to take place, repeated requests are simultaneously sent from the computers to a **web server**.
This causes it to crash, meaning that users can no longer access the **website** that is stored on this hardware.

Question

A company has a website that is suffering a distributed denial of service (DDoS) attack.
(a) Describe what is meant by a DDoS attack.

[5]

(b) Identify two solutions to a DDoS attack.

[2]

(a) Five from:

- Multiple computers are used as bots
- Designed to deny people access to a website
- A large number / numerous requests are sent (to a server) …
- … all at the same time
- The server is unable to respond / struggles to respond to all the requests
- The server fails / times out as a result.

(b) Any two from:

- Proxy server
- Firewall
- Users scanning their computers with anti-malware

Malware

Question

Malware can be used to corrupt data stored on a computer.

(a) Tick one box to show which cyber security threat is not a type of malware. Options: Phishing, Ransomware, Virus, Worm.

[1]

(b) Identify one other example of malware than those given in part (a).

[1]

(c) Identify the type of software that is used to find and remove malware from a computer.

[1]

(a) Phishing
(b) Any one from: Trojan horse / Spyware / Adware (not Ransomware, Virus or Worm as in Q)
(c) Anti-malware // anti-virus

Question

One possible aim for carrying out a brute-force attack is to install malware onto the company network. Identify three types of malware that could be installed.

[3]

Any three from:

- Virus
- Worm
- Trojan horse
- Spyware
- Adware
- Ransomware

Question

Identify and describe **three** types of malware.

[6]

One mark for identification. E.g. One mark per bullet for description to max two each.

Virus
- Software/code that replicates
- …when the user runs it // with an active host
- Deletes/damages/corrupts data/files // takes up storage/memory space

Worm
- Software/code that replicates itself on a **network**
- …without user input // without active host
- Takes-up bandwidth
- Deletes/damages/corrupts data/files // takes up storage/memory space
- Opens back doors to computers over the network
- Used to deposit other malware on networked computers

Trojan horse
- Software/code that is hidden within other software // Software that is disguised as authentic software
- …when **downloaded/installed** the other malware/by example it contains is **installed**

Adware
- Software/code that generates/displays (unwanted) adverts on a user's computer
- Some may contain spyware/other malware
- Some when clicked may link to viruses
- Reduces device performance // reduces internet speed
- Redirects internet searches/user to fake websites

Ransomware
- Software/code that stops a user accessing/using their computer/data
- …by encrypting the data/files/computer
- A **fee** has to be paid to decrypt the data // A **fee** has to be paid to 'release' the computer/device/data

Spyware
- Software/code that secretly monitors/records a user's actions/activities
- …such as keystrokes/passwords/browsing history
- Sends the gathered/stolen data to a third party/hacker
- …without the user's knowledge/consent
- Reduces device performance // takes up bandwidth

Pharming

Question

(a) State the aim of pharming.

[1]

(b) Draw and annotate a diagram to represent the process of pharming.

[4]

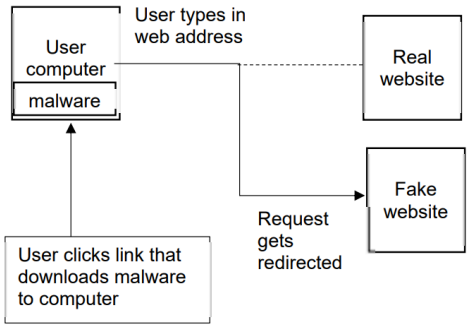
(c) A student is writing a help guide about how to recognise and avoid the cyber-security threat of pharming. Give three appropriate solutions he could include in his guide.

[3]

(a) To obtain personal data

(b) Four from:

- User clicks/opens attachment/link that triggers download
- Malicious software downloaded onto user's computer
- User enters website address
- User is **redirected** to fake website



(c) Any three from:

- Checking the spelling and tone of the email/website
- Checking the URL attached to a link
- Scanning a download with anti-malware
- Only downloading data / software from trusted sources
- Never providing personal details online
- Install a firewall to check if the website is valid

Social engineering

Question

Describe what is meant by social engineering, including one example in your answer.

[3]

- Manipulating/deceiving/tricking people...
- ...to obtain data // to force them to make some error

Any suitable example

- (e.g. Scam call center targeting the elderly to give away their bank account details)

Access levels

Question

Describe what is meant by access levels.

[3]

Any three from:

- Providing users with **different permissions** for the data
- Limiting access to **read** data // limiting the data that can be **viewed**
- Limiting access to **edit** data // limiting the data that can be **deleted** / **changed**
- Normally linked to a username

Question

Cyber security threats are a problem when using the internet.

Explain how access levels are used to help prevent a cyber security attack being successful.

[5]

- They **limit/restrict** a user's access to data
- … by giving users **different permissions** // Users can be given read only/read-write/no access/execute/administrator permission
- … so an attacker will only have access to the data that the **user** has access to
- … to stop a **malicious person/attacker deleting/editing/corrupting** data
- Prevents a user/attacker from installing malware (as they don't have administrator permissions)
- Prevents user/attacker from viewing more **confidential/important** data

Guidance

- MP1 – BOD controls access to data
- MP1 – Accept a viable example e.g. a junior employee cannot access customer information
- MP2 – 'different access levels' is TV for different permissions
- MP2 – Accept any reference to a named permission. Just low-level or high-level access is TV.
- MP5 – BOD download in place of install
- MP6 – Accept an example of confidential data e.g. prevents attacker seeing the company financial accounts. Personal data is TV for an example of confidential data.

Firewall

Question

A company owner also installs a firewall to help protect the network from hackers and malware.
(a) Explain how the firewall operates to help protect the network.

[5]

(b) Give two examples of malware that the firewall can help protect the network from.

[2]

(a) Five from:

- **Criteria** can be set (for traffic)
- Such as a **blacklist/whitelist** (of IP addresses)
- It will examine **traffic** coming into the network
- It will check that the traffic meets the set criteria
- It will reject the traffic if it does not meet the criteria
- Certain ports used by hackers can be blocked/closed

(b) Any two from (example):
Virus / Worm / Trojan horse / Spyware / Adware / Ransomware

Proxy server

Question

A company uses a proxy server to help protect the web server and the network from cyber security threats.
(a) Give three cyber security threats that a proxy server can help protect against.

[3]

(b) Identify three functions of the proxy server that can be used to help protect the web server and the network.

[3]

(a) Any three from:

- DDoS // DoS
- Hacking
- Malware // by example
- Brute-force attack

NOTE: three different examples of malware can be awarded.

(b) Any three from:

- **Can limit the number of requests sent to the web server at a time**
- **Can process common requests so they do not need to enter the network**
- Act as a firewall
- Examine incoming data to the webserver/network
- Can have set rules/criteria that data must meet
- Can have a blacklist/whitelist/list of IP addresses to block
- **Blocks traffic that doesn't meet criteria**
- Closing certain ports

Question

Proxy-servers and firewalls have some similar functions.

(a) Identify two similarities between proxy-servers and firewalls.

[2]

(b) Identify two differences between proxy-servers and firewalls.

[2]

(a) One mark for each similarity to max two.
e.g.

- Check incoming and outgoing signals // filter traffic
- Store whitelist/blacklist
- Block incoming/outgoing signals
- Both block unauthorised access
- Keep a log of traffic
- Both can be hardware or software (or both)

(b) One mark for each difference (both sides needed unless clearly and accurately implied).
e.g.

- Proxy can hide user's IP address, firewall does not hide the user's IP address
- Proxy intention is to divert attack from server, firewall is to stop unauthorised access
- Proxy protects a server, firewall protects individual computer
- Proxy examines/processes requests for a website but a firewall does not (checks type of signal) // Proxy **processes** client-side requests whereas firewall **filters** packets
- Proxy transmits website data to the user, but a firewall does not (it allows valid signals)
- Proxy allows faster access to a web page using cache, but a firewall does not (allow faster access or have cache)
- Proxy can hide internal network from internet, but a firewall cannot

Secure socket layer (SSL) protocol

Question

A patient is making a payment through a secure connection. The secure connection is created using the secure socket layer (SSL) protocol. Explain how a secure connection is created using the SSL protocol.

[7]

- **Encrypted connection** established ...
- ... using **asymmetric encryption**
- ... to make any data sent **meaningless**
- The **web browser** asks the **web server** to **identify** itself.
- ... by sending its digital **certificate**.
- The digital certificate is **authenticated/validated** by the **web browser**.
- If the certificate is authenticated/valid, the connection is secure/the transaction can begin.
- If the certificate is not authenticated/invalid, the connection is not secure/the transaction is cancelled/rejected/user is notified.

Question

The data for the web page is transmitted using the secure socket layer (SSL) protocol. Complete the paragraph about the SSL protocol. Use only terms from the list: encrypted, file server, hypertext markup language (HTML), hypertext transfer protocol (HTTP), unencrypted, operating system, URL, web browser, search engine, web server.

The ..... asks the ..... to identify itself. The ..... sends back its digital certificate. The ..... authenticates the digital certificate. If it is authentic, ... data transmission begins.

[5]

The **web browser** asks the **web server** to identify itself.
The **web server** sends back its digital certificate.
The **web browser** authenticates the digital certificate.
If it is authentic, **encrypted** data transmission begins.