PA Q1

a)

https://www.theverge.com/news/675702/lexisnexis-data-broker-breach-social-security-numbers

b)

[10] Around December 25th of last year, a breach occurred, compromising LexisNexis's data. The breach was discovered in April of 2025 and revealed that the data of 364 000 people was compromised. This includes personal information such as names, contact details, license numbers, social security numbers and so on. Due to the sensitive nature of the data along with the large quantity of people that were affected by it, the impact of the breach is considered relatively high. With the sensitive data being leaked, this would leave the affected individual in a vulnerable state, with them more prone to id theft and financial fraud

c)

[1] The listed information leaked includes legal names, contact details, license number, social security numbers.

d)

It was stated within the article by the spokesperson name Jennifer Richman that the assailant got in through infiltrating the GitHub account of the firm. And this resulted in data being leaked. This suggests that perhaps an oversight happened, and LexisNexis did not have the security measures for handling personal data.

e)In order to reduce the risk of data leakage happening in the future, I would suggest a few security measurements being put into place. [5] First suggestion is to have some kind of monitoring system or audit log installed. Installing some kind of monitoring system ensures some kind of traceability. This enables authorised members to detect any unauthorised accesses. Second suggestion is to train employees to have better data handling practices. Having employees trained for data handling to reduce the risk of data leakage. The third suggestion is to restrict access to only select few members that the firm can trust. Restricted access means fewer gateways for the assailant to enter.

Q2

a)My advice for developing some kind of teaching content is to inform people and spread awareness about phishing attacks and different variations of it. [8] Being able to be aware of these kinds of attacks would help the people have an easier time recognizing when a phishing attempt is occurring. [2] And teaching different variations, such as whaling, email phishing, smishing, and vishing would reduce the chance of it happening. This is because the mentioned variation of phishing attacks such as whaling, email phishing, smishing, and vishing, are common. And being informed about these variations would help employees be able to recognise it when occurring. I would then provide some kind of example for each variation to help the employees understand what it usually looks like, and how to spot the a phishing attack when encountering one

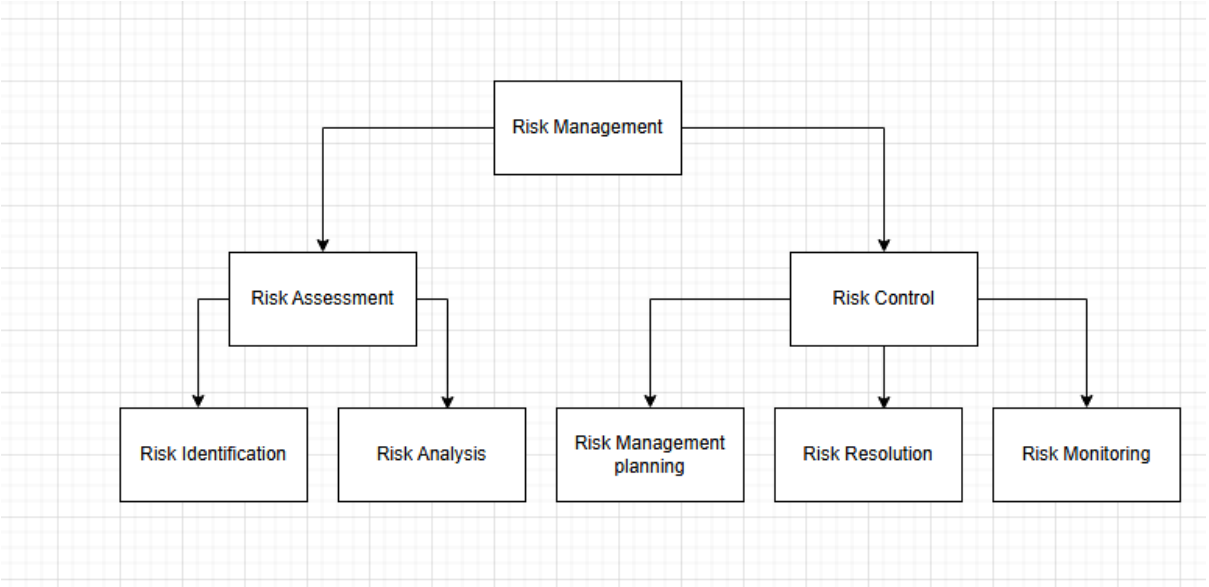
b)

In order to encourage users to learn about different types of phishing attacks. What I would like to do is to gamify it, and introduce a point system similar to duolingo. A study from [9] an article called “The impact of gamification on students’ learning, engagement and behavior based on their personality traits”stated that students yield positive results from a learning environment that encourages fun activity. With that in place, it encourages employees to learn using their drive and competitive spirit. Or perhaps, provide some kind of more hand on learning experience with introducing examples and simulating phishing attempts. This would encourage the users to think and identify the when the attempt is happening

c)
In order to assess the knowledge of the employees, a simple quiz with all of the previous knowledge, can be created. This will encompass general knowledge such as defining what is phishing, identifying different variations of phishing. As well as providing a simulated phishing attempt for employees to work on and identify. General knowledge will test the employees’ information retention, while doing a simulated phishing attempt will test the employees’ reasoning skill and ability to recognize phishing attempts.

Q3
a)
Due to the sensitive nature of hospital records, cybersecurity risk management plans play an important purpose in protecting the information of the patient. The overall role of a cybersecurity risk management plan is to serve as a structured guideline for identifying, assessing, and mitigating risks to information systems. In this context of the hospital, it means to safeguard the data of the patients, and preventing cyber attacks

b)
[6] [7] The cybersecurity risk management plan is structured with two main components: Risk Assessment[4] and Risk Control. Each component serves its own purposes with Risk Assessment help the hospital to identify potential future threats like attacks. And provide an analysis on the likelihood of it happening in the future. Hence it branches out to two different components which is called Risk Identification and Risk Analysis. While Risk Control focuses on implementing appropriate security measures in correspondence to the risk assessment through planning, resolution and monitoring. This kind of structure provides the hospital with an instruction and encourages the hospital to take a more proactive approach in safeguarding their data and ensuring the availability of the services. Making it as an essential piece to securing the data



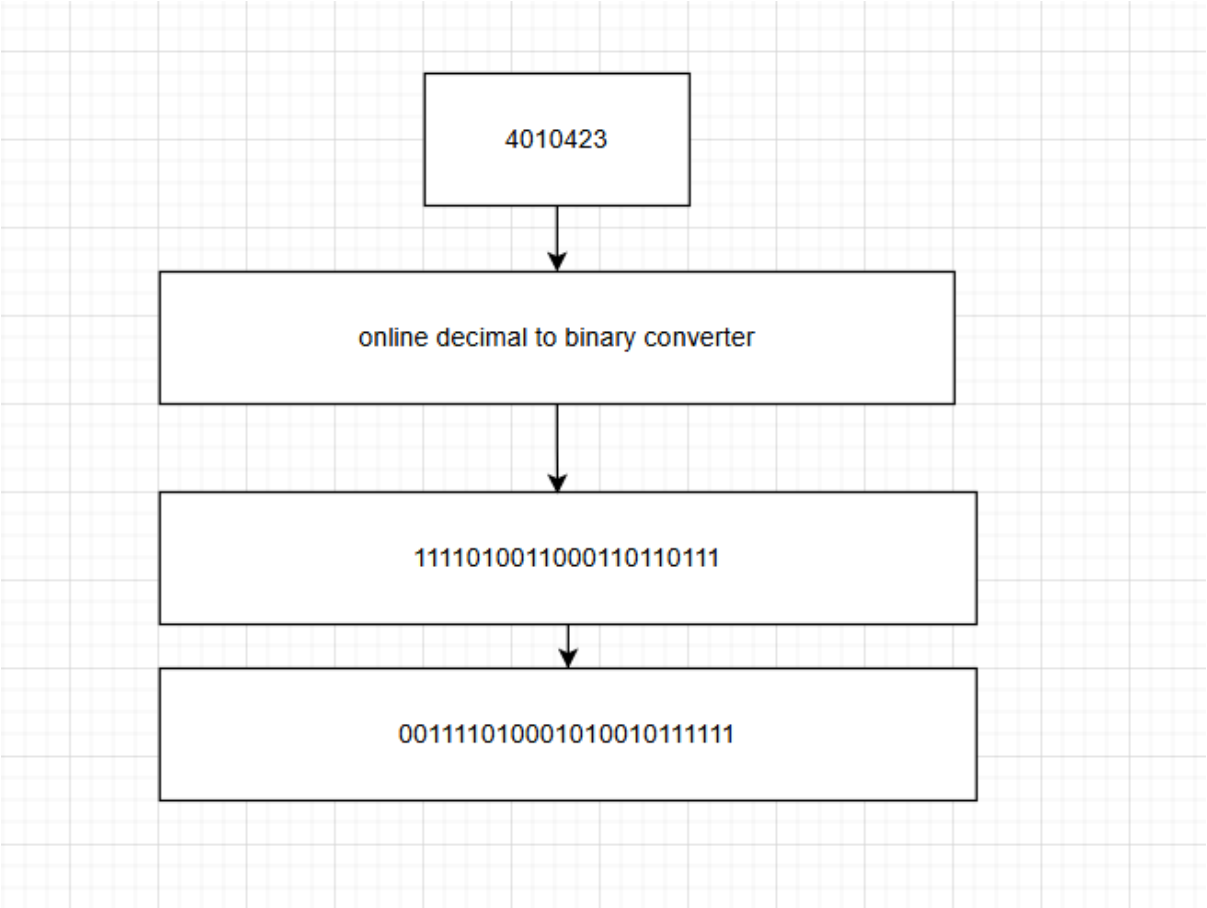
c)
The CIA triad [3] is an acronym for the three core principles of cyber security. These are Confidentiality, integrity, and availability. For example:

- Confidentiality refers to the security and protection of sensitive data from unauthorised access. In the context of the Royal Melbourne Hospital, this means that the health records of patients are safeguarded and remain undisclosed. And only accessible by authorized personnel, like doctors or nurses.

- Integrity refers to the accuracy and consistency of the data, this means that data is guaranteed to be correct and trustworthy as long as it is untampered with. In the context of Royal Melbourne Hospital, what this means is that nurses and doctors can reliably use the data they were given without the fear of incorrect diagnoses.

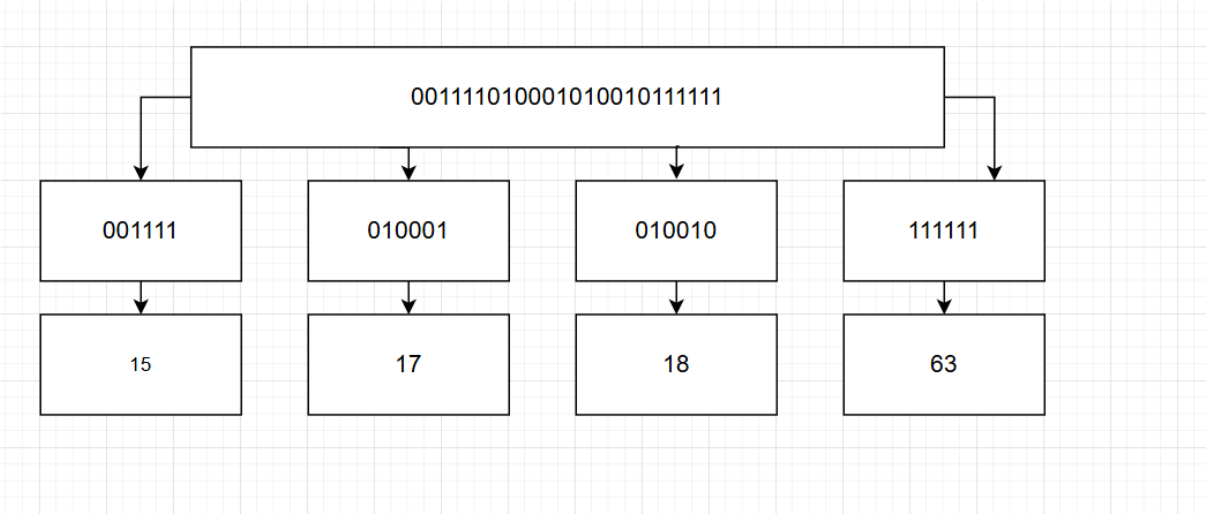
- Availability ensures that the data and services are ready and available at all times. In the context of Royal Melbourne Hospital, what this means is that staff members and doctors are able to access the patient records and the tools that they need freely, especially during emergencies.

CR
Q1
a)
Plaintext (P) = 4010423 = 001111010001010010111111



b)

P1 = 001111
P2 = 010001
P3 = 010010
P4 = 111111



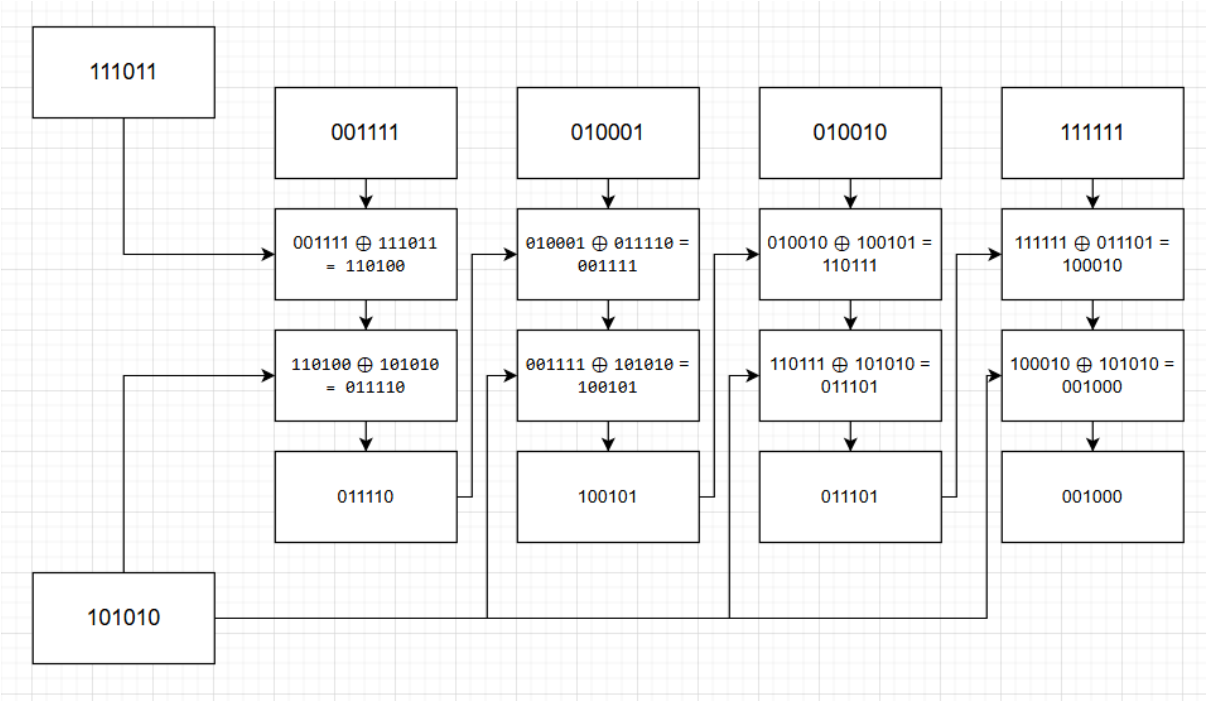
c)
K = 101010

IV = 111011
001111 ⊕ 111011 = 110100
110100 ⊕ 101010 = 011110
C1= 011110

010001 ⊕ 011110 = 001111
001111 ⊕ 101010 = 100101
C2 = 100101

010010 ⊕ 100101 = 110111
110111 ⊕ 101010 = 011101
C3 = 011101

111111 ⊕ 011101 = 100010
100010 ⊕ 101010 = 001000
C4 = 001000



Q2
param_p = 531
param_g = 13
param_a = 43
param_b = 67

A=g^a mod p
13^43mod531 = 292

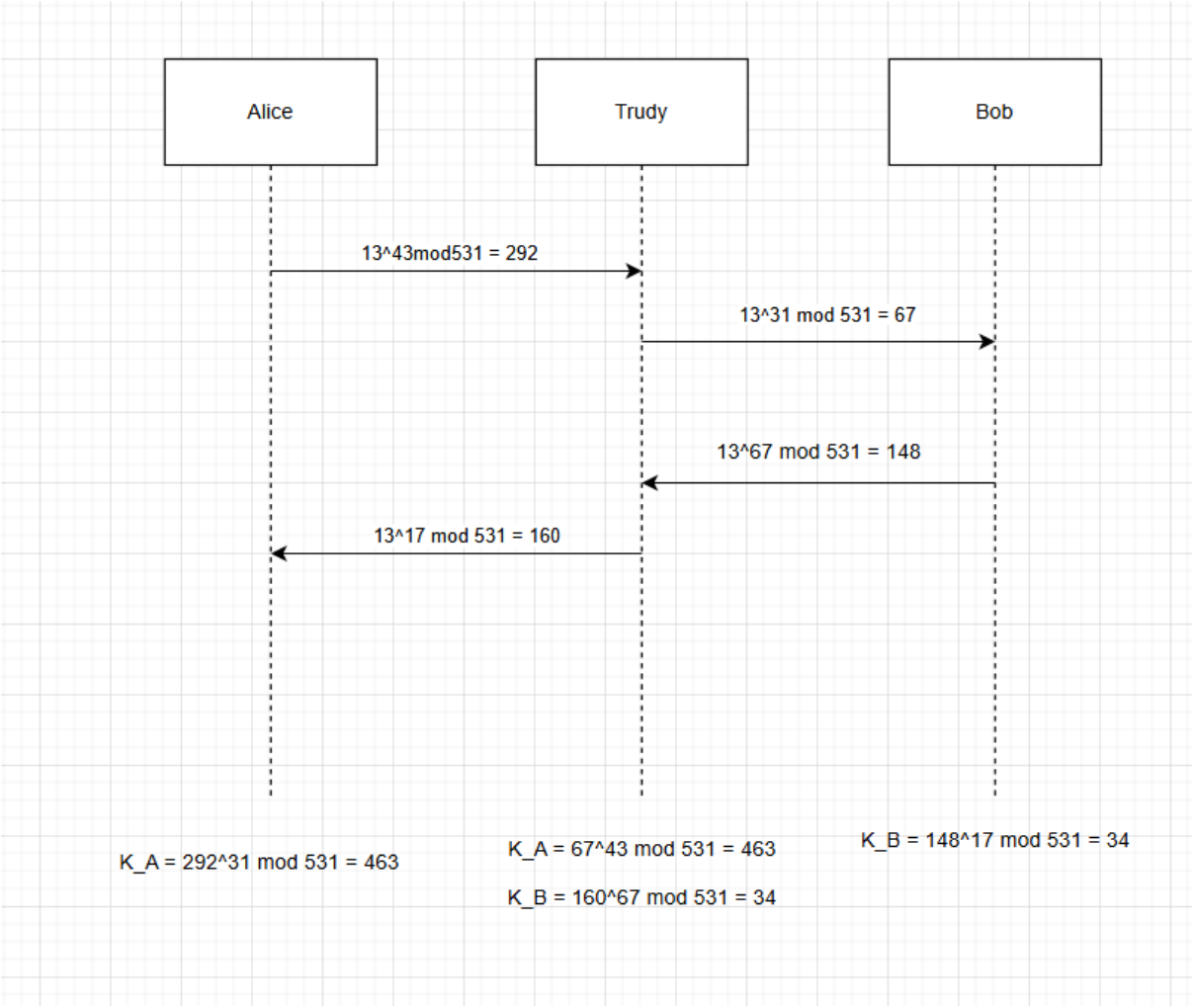
B=g^b mod p
13^67 mod 531 = 148

Trudy impersonating alice and bob
t1=17
t2=31

T1 = 13^17 mod 531 = 160
T2 = 13^31 mod 531 = 67

Alice receives fake public key
K_A = 67^43 mod 531 = 463

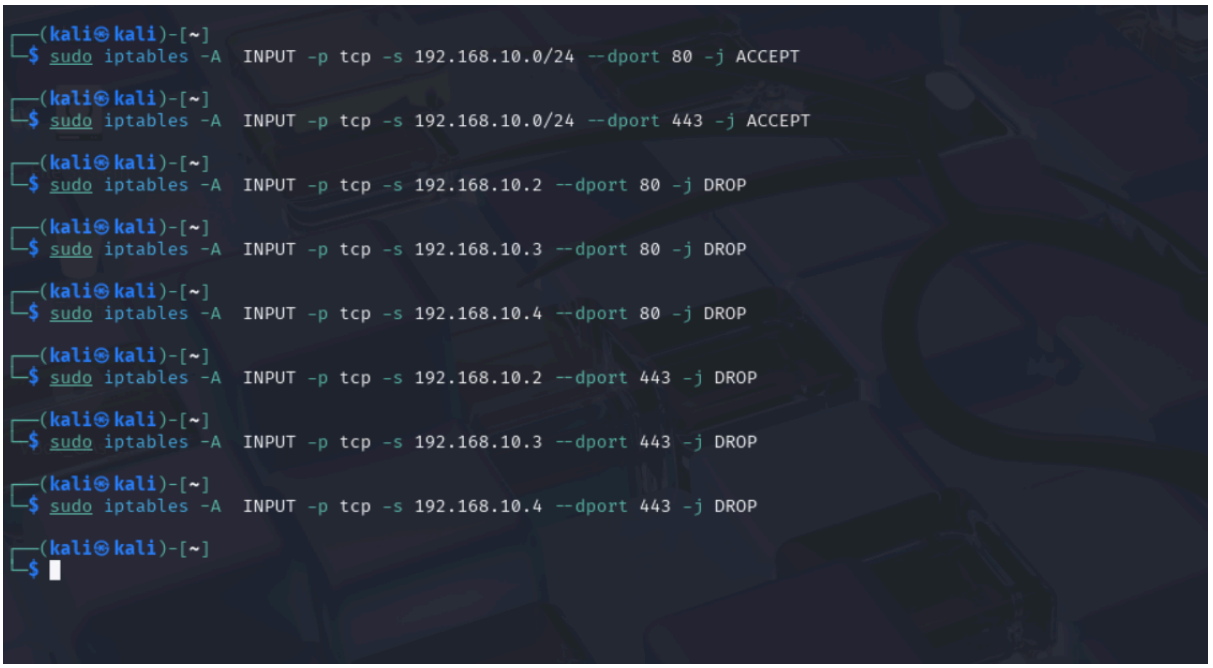
Bob receives fake public key
K_B = 160^67 mod 531 = 34



DI
Q1
a)

sudo iptables -F remove firewall rules
sudo iptables -P INPUT DROP sets default policy to drop
sudo iptables -P FORWARD DROP blocks forwarded packets
sudo iptables -P OUTPUT ACCEPT allows outgoing traffic

b



sudo iptables -A INPUT -p tcp -s 192.168.10.0/24 --dport 80 -j ACCEPT allow hosts to access web over HTTP
sudo iptables -A INPUT -p tcp -s 192.168.10.0/24 --dport 443 -j ACCEPT allow hosts to access web over HTTPS

Sudo iptables -A INPUT -p tcp -s 192.168.10.x -dport 80 -j DROP block HTTP access
Sudo iptables -A INPUT -p tcp -s 192.168.10.x -dport 443 -j DROP block HTTPS access

c)

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A  INPUT -p tcp --dport 8080 -m iprange --src-range 192.168.10.11-192.168.10.30 -j ACCEPT
```

Allow finance team to access port number 8080

d)

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A  OUTPUT -p tcp -d 142.250.64.110 --dport 443 -j ACCEPT
```

Allows HTTPS traffic to YouTube

e)

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -F

┌──(kali㉿kali)-[~]
└─$ sudo iptables -P INPUT DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -p FORWARD DROP
iptables v1.8.11 (nf_tables): unknown protocol "forward" specified
Try `iptables -h' or 'iptables --help' for more information.

┌──(kali㉿kali)-[~]
└─$ sudo iptables -P FORWARD DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -P OUTPUT ACCEPT
```

Removing all rules

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

Block all income ssh connection

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A OUTPUT -p tcp --sport 22 -j DROP
```

Block all outgoing ssh connection

[1]E. Roth, “LexisNexis leaked social security numbers and other personal data of over 364,000 people,” The Verge, May 28, 2025. https://www.theverge.com/news/675702/lexisnexis-data-broker-breach-social-security-numbers

[2]“What Is Phishing? | Microsoft Security,” www.microsoft.com. https://www.microsoft.com/en-au/security/business/security-101/what-is-phishing

[3] Instructure.com, 2025. https://rmit.instructure.com/courses/144018/pages/week-1-lecture?module_item_id=7199165

[4] NIST, “Guide for Conducting Risk Assessments,” NIST Special Publication 800-30 Rev. 1, 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[5] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” NIST Special Publication 800-94, Feb. 2007. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[6] Instructure.com, 2025. https://rmit.instructure.com/courses/144018/pages/week-8-lecture-2?module_item_id=7199179

[7] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” National Institute of Standards and Technology, Version 1.1, Apr. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[8]CISA, “Teach employees to avoid phishing,” www.cisa.gov, 2024. https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing

[9]R. Smiderle, S. J. Rigo, L. B. Marques, J. A. Peçanha de Miranda Coelho, and P. A. Jaques, “The impact of gamification on students’ learning, engagement and behavior based on their personality traits,” Smart Learning Environments, vol. 7, no. 1, pp. 1–11, Jan. 2020, doi: https://doi.org/10.1186/s40561-019-0098-x.

[10]Z. Whittaker, “Data broker giant LexisNexis says breach exposed personal information of over 364,000 people | TechCrunch,” TechCrunch, May 28, 2025. https://techcrunch.com/2025/05/28/data-broker-giant-lexisnexis-says-breach-exposed-personal-information-of-over-364000-people/