TELNET SCAN

#Ivan Lukman s1967754, #Metin A. Açıkalın s1984853,
#Valentine Legoy s2178192

1. **Introduction**

2. **Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment). For each one:**

   (Do you have comments on these points?)

   1. **Problem Owner.**

      As mentioned in the previous report, the problem owner could be referred to Chief of Information Security Officers (CISOs) and individual network administrators. For this report, the problem owner is focused on the CISOs, because the cyber risk within a company where a CISO is working, is relatively much more significant compared to the risk facing the individual environment.

      a. **Identify one concrete countermeasure that they could take to mitigate the security issue**

         One of the effective ways to improve cybersecurity is by investing in training, as also mentioned in [https://blog.coursera.org/continuous-training-can-close-cybersecurity-skills-gap/]. By having a high standard of security, a company can be more resistant to cyber threats. To illustrate, by taking the highest frequency of appearance in the dataset (static.kpn.net), one of the largest mobile telecommunication company, KPN, can be used as a reference. Although finding the exact information from the internet about periodic training and assessment program, [https://github.com/KPN-CISO/kpn-security-policy/blob/master/Human%20Resource%20Security/ksp-ra-62_-_security-awareness_v1.0_20171211.pdf] and

[https://www.kpn.com/beleef/veiligheid.htm] provides hints that KPN has also introduced a training and assessment plan to mitigate cyber incidents.

In this report, to mitigate the security issue as mentioned in the previous submission, one of the concrete countermeasures is by arranging an annual training and assessment program for the employees, especially for the Information Technology (IT) department. By arranging this program, the employees will acquire a better understanding of the latest threats in cybersecurity. In addition, they will also know the state-of-the-art technology and practices that can mitigate those new cyber threats. Arranging this event will increase the awareness of the employees about cybersecurity, which will make the company less fragile to malicious attacks.

b. Analyze the distribution of costs and benefits (without quantifying) that the deployment of the countermeasure would entail

In brief, the distribution of the cost of organizing an annual training and assessment program can be estimated as follows.

Cost	Ratio
Hiring experts for training	50-65%
Renting logistics and accommodations and paying consumptions for training and assessment	30-45%
Preparing and cleaning up the training and assessment venue	5-10%

On the other hand, the benefits can be estimated as follows.

Benefits	Value	Ratio
Improvement in reputation	Reputation	
Private files are stored more securely	The estimated price of each asset kept private	
Saving of work hours and labour price	Estimated time, human	

(compared to if an incident happens)	resources, and price of conducting maintenance.	

Since the types of values of the benefits are different from one another, it is quite difficult to estimate the distribution of the benefits. Also, the values of some benefits, such as the price of private files, could vary in a wide range.

c. Analyze whether the actors have an incentive to take the countermeasure

By definition, "incentive" is referred to a thing that gives motivations and encouragement to do something. This could be in a form of money, such as prizes or bonuses, or other types of incentives as well, such as appreciation or more-challenging duties, as also mentioned in [http://www.yourarticlelibrary.com/hrm/incentives/incentives-types-financial-and-non-financial-incentives-explained/35360]. In this report, incentives will be referred mostly as the monetary rewards to motivate the actors to countermeasure the security issues. Besides, incentives could be delivered within a company, or from external parties

Since KPN was privatised in the 1990s, the company received no funds from the government. However, there are several ways where the CISOs could still get some incentives, such as:

- Internal incentives
    - Profit sharing. When KPN receive annual profits, some percentage of this could be used to fund the training and assessment program.
- External incentives
    - Certifications and awards received from external parties, such as privacywaarborg [https://privacywaarborg.nl/bedrijven/koninklijke-kpn-b-v/]. Receiving this award, to some extent, could motivate the CISOs

to maintain and improve the cybersecurity of KPN. Also, since some of this kind of awards and certifications will be held annually, these CISOs will be also motivated to win the upcoming editions. This means that the appreciation and the money received from winning the awards could be used to fund the training and assessment program.

d. Briefly reflect on the role of externalities around this security issue

As explained in the video lecture, there are two types of externalities, namely the positive and the negative externalities. In general, having lots of openly-accessible Telnet ports could bring both sides of externalities, because:

- Positive Externalities: create benefits to third parties.

  Trained professionals in the field of cybersecurity could be benefitted from this security issue. By deploying a large number of systems that can be accessible from anywhere in the world, the CISOs must have also predicted and calculated the possible risks and the worst-case scenarios. And to mitigate these problems, trained professionals, such as cybersecurity specialist or professor, could be employed to conduct security training and assessment programs.

- Negative Externalities: create harm to external companies.

  Having a lot of systems that can be accessed openly from all over the world means that the chance of hackers taking over these devices are higher. Once they gain access to these machines, this could lead to cybercrime acts, such as using the machines as Distributed Denial-of-Service (DDoS) botnets. This means other companies are in danger of being DDoS victims as their services could be inaccessible from legitimate users.

2. Government

As mentioned in the previous report, “governments” are among the actors with a positive impact on the security issue. They are usually represented by agencies created in order to improve network and information security of the country or

grouping of countries they are part of. NIST (National Institute of Standards and Technology) and ENISA (European Union Agency for Network and Information Security) are two examples of organization respectively part of the US government and the EU government.

a. **Identify one concrete countermeasure that they could take to mitigate the security issue**

   If these governmental organizations evaluate various security issues, evaluate the security performance of the countries they represent, their main function is to create policies. The other governmental agencies are supposed to follow those, while private organizations can use them to improve their security performance. The creation of those guidelines is, thus, the main countermeasure they provide.

b. **Analyze the distribution of costs and benefits (without quantifying) among the different actors that the deployment of the countermeasure would entail**

   The costs of the creation of security policies by these governmental agencies mainly lie mainly in the monetary costs those agencies represent. Among those costs can be listed the salaries of the employees or the maintenance of the agency. Costs will vary depending on when those guidelines are developed, for instance, if they are developed as the results of an attack or if they are developed due to a security issue found as part of the agency research. The first instance would cost the brand of those organizations as they were not able to plan these policies or these attacks. In the second case scenario, time could be a significant cost, which could limit the performance of the agency if the focus of too many researchers is on one set of policies for a particular issue.

   The benefits of the creation of guidelines are visible only if they are adopted to a large scale, by the governmental institutions and the private organizations of the countries. The benefits lie in the costs the government would suffer of if the attacks the policies are preventing from were to happen. The main benefits are economic, as a country where all organizations follow good cybersecurity

standards will not suffer from the economic costs of potential attacks. A country with advanced security policy has overall a better branding. A country which seems to be more targeted of cyber attacks is less attractive to companies, which will be more likely to set up themselves in a country where cybersecurity is promoted.

c. **Analyze whether the actors have an incentive to take the countermeasure**

Unless an attack related to telnet scan targets the government, this actor is not directly impacted. However, the fact that some of the companies or private organization might be attacked will have an economic impact on the whole country. Thus it encourages governments to have such agencies creating policies and promote them to those private companies.

The incentive for external organizations and companies to follow these policies created by government officials is mainly the overall security benefit they represent. Those measures are developed by experts who are much more knowledgeable about the security issue and would only benefit from

d. **Briefly reflect on the role of externalities around this security issue**

The creation of these guidelines produces mostly positive externalities, as they are mostly created to improve the security of the organizations. If the application of these policies represents a cost, it cannot be seen as a negative externalities as the benefits is supposed to be superior to it.

3. **Non-profit Organizations**

The telnet scan CSV file was created by Shadowserver which is a non-profit organisation working to understand and help put a stop to high stakes cybercrime in the information age [https://www.shadowserver.org/wiki/]. The organisation is trying to supply timely and relevant information to the security field [https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission]. In their goals, they indicate that Shadowserver wants to work closely with ISPs, Hosting and DNS providers in the identification and mitigation of botnets and malware propagation.

a. **Identify one concrete countermeasure that they could take to mitigate the security issue**

As those kinds of organisations work by volunteering basis, all the participants of those organisations are engaged with the goals of their organisations. In telnet scan, they are already working to provide information to problem owners to inform that they have unsecured telnet ports accessible from the internet. They can move forward to increase the impact of providing security and make a "whois" search on the IP addresses they found to gather information about the owner of the address and send mail about the discovery to inform the problem owners.

b. **Analyze the distribution of costs and benefits (without quantifying) among the different actors that the deployment of the countermeasure would entail**

   As shadow server is a non-profit organisation [https://www.crunchbase.com/organization/the-shadowserver-foundation#section-overview] there will be no costs of deployment for any problem owner or any actor. The only cost will be the labour of volunteer workers of the organisation. By deploying this method, each problem owner's system administrators or CISOs will recognise if they are not aware of the situation. On the other hand, if they know the situation and they are not doing anything with it, this leakage of information might push them to do something with it.

c. **Analyze whether the actors have an incentive to take the countermeasure**

   No company works for losing money and more or less each company tries to mitigate the risks of losing money. We can group the incentives in two section as follows;

   - Internal Incentives: In the data that was analysed, there were huge companies such as KPN and Infopact. They have lots of confidential information about their clients. Risking them by leaving a trapdoor to their internal network can be costly in case of an exploit. Thus they have internal incentives to fix openly accessible telnet port issue.
   - External Incentives: When an IP is listed as it has an openly accessible telnet port, this can cause loss of reputation. Especially in the data that

was analysed, the majority of problem owners were companies related with technology. Loss of reputation by a security-related issue might create significant impacts on such companies. Thus, they will be interested to fix it if they see a mail from Shadowserver about the issue.

d. Briefly reflect on the role of externalities around this security issue

- Positive Externalities: As Shadowserver is based on voluntariness, it is an excellent place for a security enthusiast to improve his/her skills. As those kinds of security issues keep existing, it will always create an area of improvement for security specialists.
- Negative Externalities: Disclosure of IP addresses of openly accessible telnet ports may lead more attackers to use this information against problem owners and choose them as one of their targets. However, any IP can be removed from scanning list of shadow server if the owner of the IP sends an e-mail to request his/her IP address to put into the whitelist. By this way, scan excludes that IP address.

3. Identify the type of actor whose security performance is visible in the metric(s) you selected (e.g. ISPs, software vendors, countries). Note that this is not necessarily the problem owner, rather is the unit of analysis in your metric.

To identify the actors where the security performances mentioned in the previous assignment some analysis has done. First of all, for all of the metrics that were discussed, the top 10 hostnames based on the dataset where the security metrics can be applied is listed. Then, the total number of scans based on each hostname rank is calculated from the whole dataset. To normalize the security performance, from the top 10 list for each security metrics, the number of host names that fulfil the security metrics is divided by the total number of scans during the time period of the dataset. Specifically for each security metrics, this can be seen as follows.

a. **Identification of different factors causing the variance in the metric and collection of results for them.**

1. **Security Metrics 1**: Usage of SSH on port 23.

   In [table x1], the data shows the top 10 domain names that was scanned most in the entire dataset. The percentages of ssh usage on port 23, which can be seen in sshPortNb column, are all 0% except kpn.net at 0.65% which is smaller than even 1%. Percentages are calculated as the ratio between banners containing information that SSH is running on port 23 and the total number of scans for each domain name. This reflects the fact that domain names which scanned the most stayed vulnerable because no improvement was done on security performance regarding migrating port to run SSH.

domainname	totalScanNb	sshPortNb
routit.net	438413	0.000000000
kpn.net	413474	0.006563895
ziggozakelijk.nl	282611	0.000000000
ziggo.nl	245564	0.000000000
xenosite.net	213835	0.000000000
solcon.nl	153053	0.000000000
chello.nl	96416	0.000000000
xs4all.nl	90049	0.000000000
infopact.nl	85135	0.000000000
prioritytelecom.net	74903	0.000000000

Table x1: Percentages (sshPortNb) of most scanned domain names which run SSH on port 23

As the domain names that were scanned the most during the entire scan period results were unsatisfying, it was also conducted another analysis in [Table x2]. This time the dataset was first ordered by the domain names that had the maximum number of banners that indicates SSH is running on port 23 and then calculated the ratio between the number of total scans on the domain names and the number of

banners which indicates SSH is running on port 23 to show the security performances. The results were opposite of the results of the previous analysis. This time, top 10 SSH running domain names on port 23, the ratio explained above was 100%. This shows that the companies who are aware of the security issues show a stable security performance.

domainname	totalScanNb	sshPortNb
zeus.pm	1595	1
phpwebhosting.com	1027	1
dnazone.net	975	1
growingminds.nl	910	1
achos.nl	694	1
hostje.nl	618	1
miamo.nl	618	1
coloprovider.nl	603	1
aliensonacid.nl	429	1
pure-isp.eu	421	1

Table x2: Percentages (sshPortNb) of highest SSH usage per domain names.

The differences between the top 10 domain names regarding SSH usage on port 23 might be because of each company's decision of running SSH in their prefered port.

2. **Security Metrics 2**: Rejection of Telnet sessions.

In [Table x3], data shows the rejection of connections in the top 10 most scanned domain names. It can be clearly seen from the table that, other than kpn.net which has nearly 1% of rejected connections according to banners, rest has never rejected any connection. This shows, in the entire scan period no improvements on the rejection of connection was done.

domainname	totalScanNb	rejectScanNb	ratio
routit.net	438413	NA	NA
kpn.net	413474	38645	0.093464160
ziggozakelijk.nl	282611	NA	NA
ziggo.nl	245564	NA	NA
xenosite.net	213835	NA	NA
solcon.nl	153053	NA	NA
chello.nl	96416	NA	NA
xs4all.nl	90049	NA	NA
infopact.nl	85135	NA	NA
prioritytelecom.net	74903	NA	NA

Table x3: Top 10 most scanned domain names which reject the telnet port connection.

To be able to further explain the data also for this metric, another analysis was conducted. This time the top 10 domain names which have the most rejection ratio. To be able to obtain this data, some specific keywords were searched in the banner. Afterwards, the ratio between the total number of scan and the scans which have rejection keywords was calculated. The results which can be seen in [Table x4], show that there are 6 hostnames in top 10 hostnames which were scanned significant amount of times and gave more than 78% of rejection. This shows their security performances are improved over time or was already in the highest position for the ones who had 100% rejection.

domainname	totalScanNb	rejectScanNb	ratio
kpn.net	413474	38645	0.093464160
by.pcextreme	2286	1794	0.784776903
tele2.net	1763	1763	1.000000000
weserve.nl	36636	1548	0.042253521
as197156.net	2323	987	0.424881619
nova-ict.nl	977	977	1.000000000
solidbe.nl	819	819	1.000000000
vqbn.com	784	783	0.998724490
colocenter.nl	4153	623	0.150012039
clientshostname.com	578	578	1.000000000

Table x4: Top 10 domain names that have the most telnet connection rejections

The differences between the top 10 domain names in terms of rejection, was because of each company's security approaches.

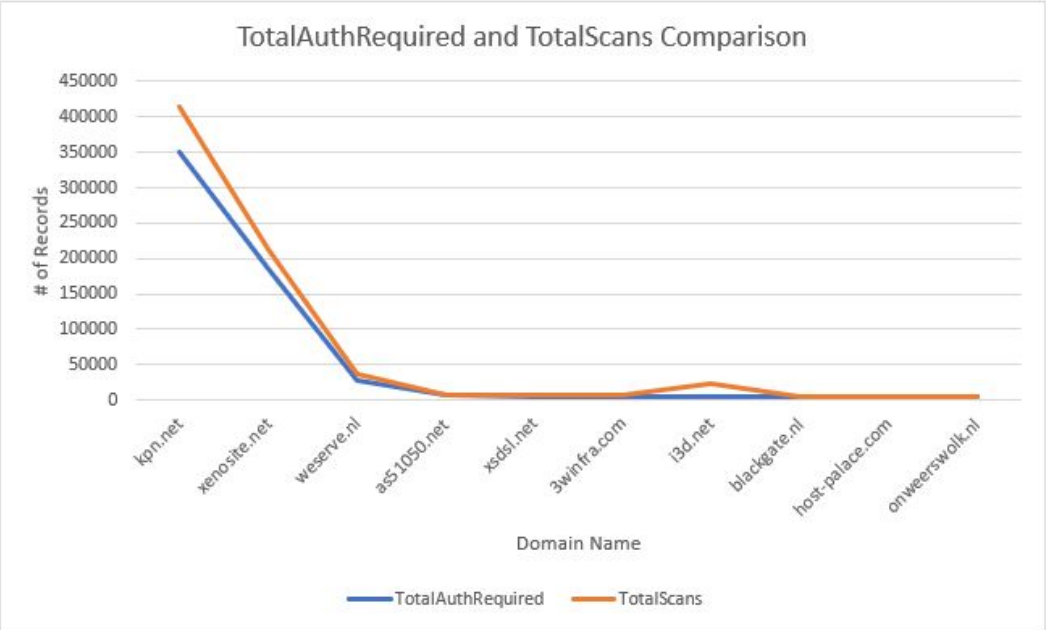
3. **Security Metrics 3:** Authentication banners.

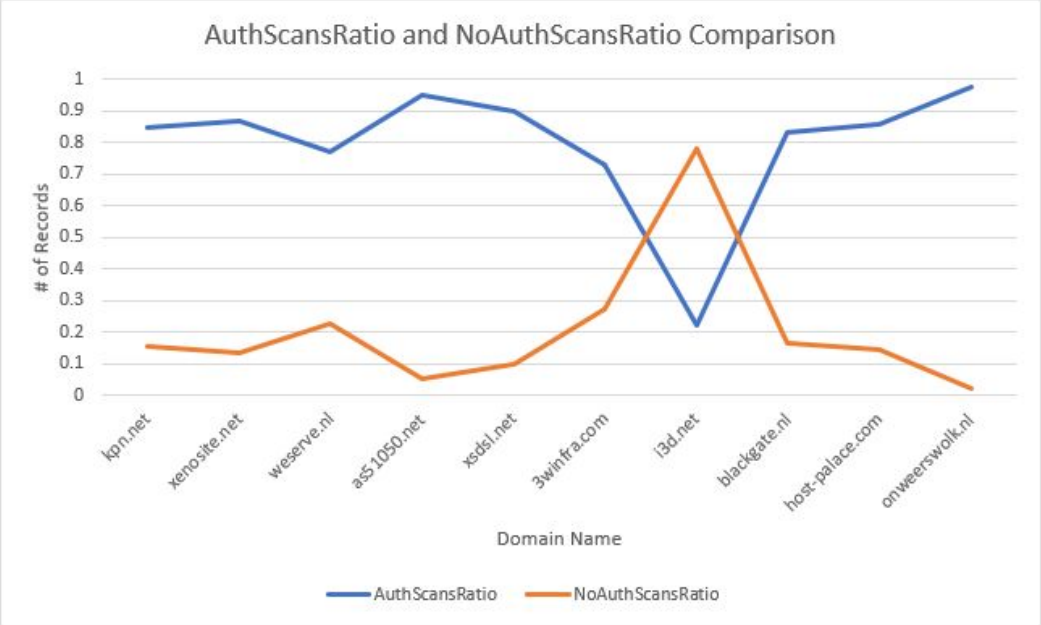
   The result of evaluating this metric can be seen at the figure below.

Domain Names	TotalAuthRequired	TotalScans	AuthScansRatio	NoAuthScansRatio
kpn.net	349672	413474	0.8456928	0.15430716
xenosite.net	185334	213835	0.8667150	0.13328501
weserve.nl	28270	36636	0.7716454	0.22835462
as51050.net	6630	6988	0.9487693	0.05123068
xsdsl.net	5689	6319	0.9003007	0.09969932
3winfra.com	5373	7372	0.7288388	0.27116115
i3d.net	5292	24062	0.2199318	0.78006816
blackgate.nl	4772	5723	0.8338284	0.16617159
host-palace.com	4051	4720	0.8582627	0.14173729
onweerswolk.nl	3937	4025	0.9781366	0.02186335

   The table is sorted by the number of records that requires authentication (TotalAuthRequired) in a decreasing order. In this table, column TotalAuthRequired shows the number of records from the dataset that requires authentication, based on each domain name. TotalScans shows the total number of scans based on the domain names from the dataset. AuthScansRation is computed by dividing TotalAuthRequired with TotalScans per domain names. NoAuthScansRatio is the opposite of AuthScansRatio, and computed as 1 - AuthScansRatio.

   Visually, this statistics can be visualized in two line charts as shown below.





The type of actors based on the top-10 list (based on the total number of authentication required) can be seen at the table below.

Domain Name	Type of actor
kpn.net	Internet Service Provider

xenosite.net	Internet Service Provider
weserve.nl	Internet Service Provider
as51050.net	-
xsdsl.net	Internet Service Provider (has relationship with xenosite.net)
3winfra.com	Hosting company
i3d.net	Hosting company
blackgate.nl	Internet Service Provider
host-palace.com	Hosting company
onweerswolk.nl	-

Based on the table, this metrics is essential for Internet Service Provider companies. The higher value of NoAuthScansRatio means that to some extent, the security of that system is better because based on the dataset, these records that contain no authentication requirements are stating that the telnet connections were rejected.

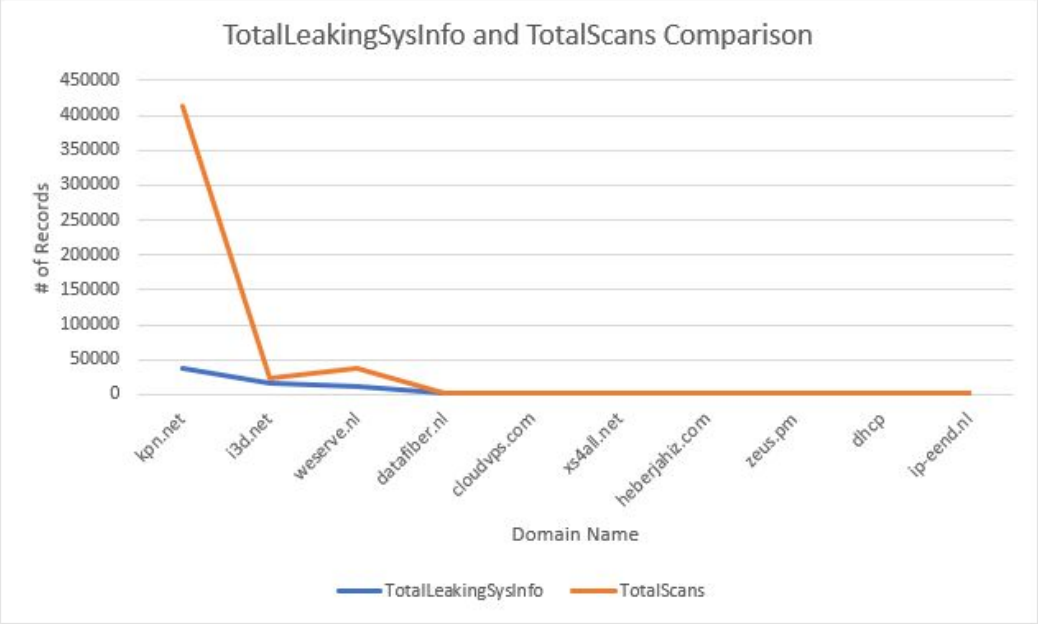
The variance within the top 10 domain names that requires authentication is mostly caused by the different limit of telnet sessions each company allows. Even within an organization, the telnet limitation could differ due to different purposes of each systems. For instance, this is visible for “leaseweb” company, whereby there are different total number of authentication in the telnet banners for the host names.

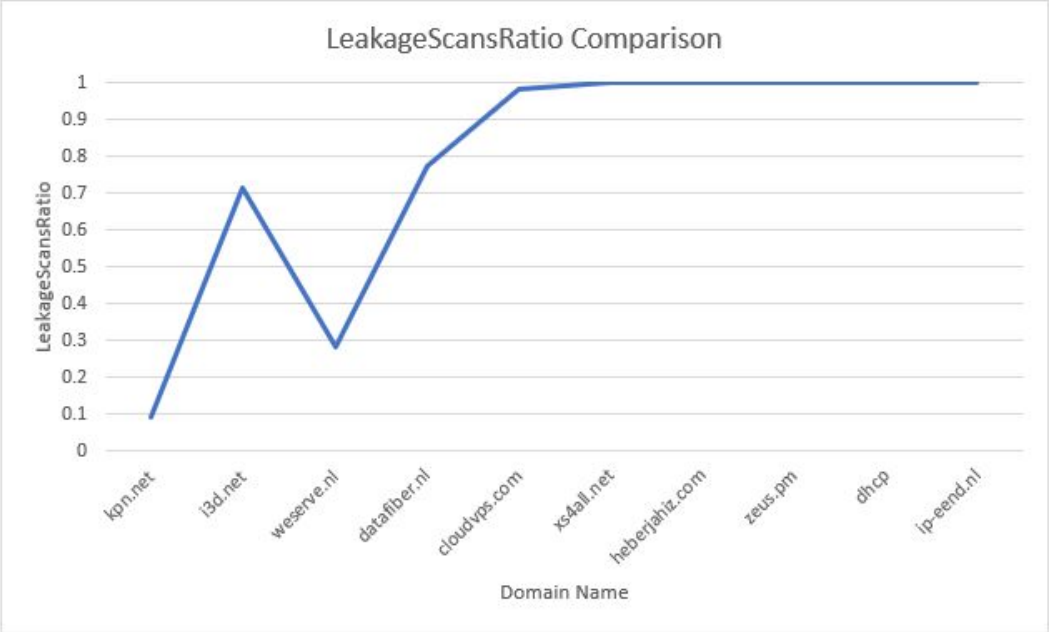
4. **Security Metrics 4:** System information leakage from the banners.

   The result of evaluating these metrics can be seen at the figure below. The table is sorted by the number of records that leaks the system information (TotalLeakingSysInfo) in a decreasing order. In this table, column TotalLeakingSysInfo shows the number of records from the dataset that reveals the system information, based on each domain name. TotalScans shows the total number of scans based on the domain names from the dataset. LeakageScansRatio is computed by dividing TotalLeakingSysInfo with TotalScans per domain names.

Domain Names	TotalLeakingSysInfo	TotalScans	LeakageScansRatio
kpn.net	38391	413474	0.09284985
i3d.net	17171	24062	0.71361483
weserve.nl	10474	36636	0.28589366
datafiber.nl	2242	2896	0.77417127
cloudvps.com	2065	2099	0.98380181
xs4all.net	2012	2012	1.00000000
heberjahiz.com	1881	1881	1.00000000
zeus.pm	1595	1595	1.00000000
dhcp	1567	1567	1.00000000
ip-eend.nl	1559	1559	1.00000000

Visually, this statistics can be visualized in two line charts as shown below.





The type of actors based on the top-10 list, ordered by the total number of systems that reveals the system information, can be seen at the table below.

Domain Name	Type of actor
kpn.net	Internet Service Provider
i3d.net	Hosting company
weserve.nl	Internet Service Provider
datafiber.nl	Internet Service Provider
cloudvps.com	Hosting company
xs4all.net	Internet Service Provider
heberjahiz.com	Hosting company
zeus.pm	Internet Service Provider
dhcp	-
ip-eend.nl	-

Based on the table, this metrics is important for Internet Service Providers in the Netherlands. To be able to mitigate the security issues, the value of TotalLeakingSysInfo should be minimized.

One of the factors that makes the top 10 domain names leaks the system information differently is the different devices that each companies use. Taking the example from the dataset, domain name “kpn.net” has 24287 unique banners. Many of those reveal system information, such as Wandy and MikroTik version numbers. This fact also applies for other domain names.

b. Statistical analysis to explore the impact of the factors on the metric

Please note that we would like feedback on this section in particular. We detail here the processes we went through up to now for this part, but also some questions to which we would like answers. This part will be developed based on the given comments

For this statistical analysis, we decided to use pearson’s χ^2. For each domain name, we identified the number of rows in the original dataset with a banner which let us believe security measures were implemented, either because it indicated that SSH was running on the port 23 or 2323, or that because it rejected the telnet connection. These numbers were collected in the first column. The second column represents the number of other rows in the original dataset, which did not indicate the use of any security measures. This led us to have a table of 2 columns and 1832 rows, for which we were not able to find a contingency table large enough in order evaluate our χ^2. We ended up obtain a χ^2 of 871645,70644798 and Cramer’s V of 0,4858865941. Our χ^2 is probably this large because two third of the first column is equal to 0. From understanding of the χ^2, we studied here the relation between the domain name and the implementation of the security measures.

The main problem we have for our dataset is that there are no clear indication of the security performance for each domain name (which are supposed to represent our security issue’s owner). Thus we had to define the security performance of each

owner based on what we could analysed from the banner. For instance, if the banner gave information about the system, it represented a potential lack of implementation of security measure, as this information might help potential attackers to find vulnerability to exploit on the owner's system. On another hand, other banners would indicate that the connection was rejected for various reason (session timeout, too many session connected to the service, wrong sender's IP address) or that SSH was used on port 23 or 2323 (only ports scanned in our dataset), which, for us, was a proof of better security performance.

The only other possible way we could have potentially defined the security performance would have been based on the number of IP addresses scanned per ASN, which can be defined from our dataset, compared to the number of IP addresses available for each ASN, which can be found on the Internet. Of course, this would have required to change the security owner. However, we cannot be sure the IP addresses, which are not present in our dataset, were not whitelisted by ShadowServer, because the companies to which they belong have requested it.

In this regard, is our way of defining security performance correct or not?

Because we defined the "security performance" of the actors based on factors defined on our own, we are not sure how to do the statistical analysis, here. *Should we correlate the numbers of scans which we define as having security measures implemented, or not, with the different factors explained in the part 3.a?*

4. **Conclusion & limitations**

   (*This is to be discussed for the final submission*).

5. **References**

   a. (*This is to be discussed for the final submission*).