TELNET SCAN

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

- **What has been changed according to the feedback of final report of block 2?**

The peer reviews and feedback from the first assignment encouraged us to review our metrics. The metric which was mainly criticized was the " number of telnet sessions that are accessible, grouped by each type of industry", as we were not able to normalize it. As a reminder, the four other metrics evaluated during the previous assignment gave us the following information:

- 77% of the telnet sessions requested log in
- 9% of the attempts of connection to telnet port were rejected
- 17% of the banners grabbed during the scan were giving information about the service
- 1% of the banners gave information about whitelisted ip

The metrics defined during the first assignment might not have been enough to answer the questions of the present assignment, thus we worked again on the definition and evaluation of metrics present in the dataset.

If all the IP from the dataset have been scanned on port 23 or 2323, which are usually used for the telnet protocol, some banners gave us information as to which other protocol the scanned port was assigned. 0.5% are used for FTP. 0.05% are used for SMTP. 5% are used for SSH.

If we did consider evaluating metrics regarding security measure, such as login forms and connection rejection, we did not consider until now the banner giving a warning message, which can be included as a preventive measure. In

the overall scan, over 5% of the banners give out a warning messages to the person trying to access the service.

For the purpose of the second question of this assignment and as a replacement of our previous grouping of telnet sessions by NAICS and SIC, we decided to group the session by hostname[cite h], based on our definition of the problem owner (see question one). The obtained groupment will allow us to normalize the difference between security performance at the second question of this assignment.

We also evaluated the evolution of banner during the 8 months the data were collected to know if the repeated scans on an IP would encourage a change in security[cite i]. A large majority of banners didn't change over the 8 months. Those that did had only a number or a quote modified, supposedly, randomly (see more on question five).

1. **Who is the problem owner of the security issue as measured in your first assignment?**

In this report, "problem owner" is referred to any person, or instances, or organizations, that is responsible of preventing or handling the problems [problem owner]. When dealing with telnetscan data, the problem owners can be said as the executives and the SysAdmins of the company's or individual devices that open the telnet port.

As we have mentioned in the first assignment, there are two security issues that are raised from the given dataset, which is about the telnet scan result.

- Firstly, this dataset gives an example of leakage of systems' critical information. In the given dataset, this is can be seen directly by inspecting the telnet banners. Some records reveal the system's information, such as the Operating System (OS) name and its version, using the telnet sessions' banners. Taking the security perspective, this leakage of

information is very useful for the attackers to find available vulnerabilities, but on the other hand, this is not what the system owners want.

- Secondly, and the more important security problem, is the fact that many computers and networking devices allow remote access from anywhere via telnet. This problem is actually the reason why the dataset was created. There are still a lot number of devices that allow telnet communications from anywhere in the world.

The problem owner of both of the two issues are the executives related to the information security, such as Chief Information Security Officers (CISOs), in the case where the devices belong to a company. If the system that open a telnet port is owned individually, the owner of that device can be said to be the problem owner. SysAdmins, one of the actors that can be related in both cases, can also be blamed, because technically, they are the ones responsible for configuring the devices. If they can enable the telnet services, they should also be able to change the login banners.

These CISOs and SysAdmins should have implemented policies about what should be published into the telnet banners (for the first problem) and from where should the device be accessible (for the second problem). Opening telnet port, to be accessible from anywhere, could be a double-edged sword for the problem owners. On one hand, this may increase the convenience of the SysAdmins because they can configure the device from anywhere. On the other hand, attackers from all around the world can also access the system.

2. <u>What relevant differences in security performance does your metric reveal?</u>

The analysis of the whole dataset show that some security measures were taken, probably local decision makers, in order to make their system more secure. One of those is the presence of a login form when the port is access, before being able to use the service. Logging in is required in 77% of the case

presented in the dataset. However the use of the telnet protocol to send password to a server make the service less secure, as the credentials will not be encrypted and might be sniffed. The dataset doesn't allow us to know if the credentials required are the default ones or not, which could be an additional security issue, as it had been exploited during the Mirai attacks.

The use of a warning message in the banner has been in 5% of the case. It is part of the recommandation to make a secure banner [cite j]. However, this preventive measure might not be discouraging the malicious individuals to attack the service.

Among these five millions of sessions created, a minority of system is likely to a good security performance. 9% of the IP scanned have rejected the telnet connection. In some cases, because of the number of telnet sessions connected were over the limit. In other cases, the IP address from which the scan was done was not whitelisted by the system. The use of SSH on 5% of the ports scanned is the strongest security measure observed, as it is often recommended instead of telnet [cite k].

The fact that 17% of the scanned ports gave information about the system in their banner is worrisome and proof of a low security level. Banner grabbing is one of the issue related to open telnet services. Information gathered from the banners can be used to find vulnerabilities on the system which could be exploited in an attack.

Additionally, the fact that these service are accessible from the Internet is a proof of a low security level. The Shadowserver, which is the author of this scan, affirmed on their website, that these addresses are not firewalled from the Internet [cite l]. Thus they didn't have to do much effort to have access to the services, proving that any attackers could potentially benefit from the low security performance.

[TODO: comparison of security performance per hostname grouping]

3. **What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?**

When discussing about the strategies to manage the security risk, there are 4 major methods that problem owners can follow. These methods will be explained as follows.

- Risk reduction is one way of tackling the problem. For this phase, problem owners should follow a risk mitigation strategy. For the data that had spoken to, some mitigation methods can be followed to prevent the attackers getting valuable information from the leakage of information about critical running systems. According to Gunderson [cite b], a company should have a policy on the banners they put to openly accessible ports from internet. Agreeing to this, according to Akin (2002), [cite c] a banner message has four goals:
    - 1.0 Be legally sufficient for prosecution of intruders
    - 2.0 Shield administrators from liability
    - 3.0 Warn users about monitoring or recording of system use
    - 4.0 Not leak information that could be useful to an attacker

  By following these guidelines, problem owners can minimize the security threats, at least preventing the attackers from getting the information from the banners.

  Another way problem owners could consider to increase the security of the system which company uses is by moving from unsecured telnet ports to secure SSH ports. Besides, mitigation and prevented losses should be calculated for this purpose to see if the cost of mitigation are worth investing in it. This brings us to second strategy.
- In Risk Acceptance phase, if risk owners' calculations on risk mitigation makes investment infeasible because the mitigation

costs are higher than expected losses, the risk is generally accepted and no mitigation strategy is followed.

- Another strategy that can be followed is the risk avoidance strategy. For the discussed situation, risk owners can choose to shut down the TELNET ports that they are using to access some of their critical systems from the internet if it is too risky for them to keep it on.
- Last strategy that can be used to handle the risk is the Risk Transfer. For the risk transfer phase risk owners transfer the cost of risks to third parties, such as the insurance companies. Even though an exploit can cause loss of reputation for problem owners, sometimes it is the cheaper and more feasible than investing in the risk mitigation strategies.

4. **<u>What other actors can influence the security issue as measured in your first assignment?</u>**

   Following the definition of actors from the previous report, “actors” can be categorized into three groups, namely:

   - Local, which includes SysAdmins and organizational decision makers.
   - National, for example each countries’ ministry of information security.
   - Global, for example, the Internet Society (ISOC).

   In this report, the term “other actors” refers to any person or instances besides the attackers. These actors can influence the security issues positively (preventing/reducing the damages) or negatively (causing worse damages).

   Based on the aforementioned security problems, there are other actors that can influence the security issues, such as:

   1. Non-profit organizations, for instance ISOC, Regional Internet Registry (RIR) Communities, or ShadowServer. There are several ways that these organizations can influence, for example:

a. Arranging a large meeting periodically, together with governments, research institutes, or individuals, to develop new policies to make the Internet more secure. For instance, the discussions held by RIR Communities [nro rir]. During these discussions, basically, all three categories of actors can contribute to make the internet more secure by understanding the latest security threats and technologies. Therefore, these events can impact the security issues positively.
b. Like ShadowServer [shadowserver], the organization can just scan for every kinds of security flaws and report the problems to the corresponding SysAdmins or companies. By doing this, external actors that initially have no relations with the devices owners can affect the security issues positively.
c. Holding a training session about what threats can happen and how to mitigate these vulnerabilities. This can be a positive influence, because more people are aware about how to protect their devices. On the other hand, this can also be a negative influence, as they could also apply the attacks for other active devices in real-world.

2. Governments. In general, governments usually bring positive impacts about the security issues. The information security minister will obviously try to protect the country from cyber attacks. Thus, they will create policies that can improve the security of the devices connected to the internet in their respective regions. The problem is, that these policies are deployed in a different paces. Some countries that are aware of technology threats can impose the laws quicker and more efficiently than other countries.
3. Educational institutions. In general, educational instances, such as universities [cyber schools], could also bring positive impacts in reducing security issues. Introducing the threats and mitigation could increase the awareness of SysAdmins and network configuration staffs. This means,

indirectly, external institutions could bring positive influence positively about the security issues.

5. **Identify the risk strategies that the actors can adopt to tackle the problem:**

   (Notes: "Proactive" and "Reactive" actions?)

   Proactive: Awareness Education Programmes and Trainings.

   a. **are there actors with different strategies? Why?**

      Based on the dataset we were provided, it is difficult to define which strategy each actor have adopted to solve that systems have some of there services on an open telnet port. The evaluation of the dataset show the decision made to make the service more secure at a local level. The majority of the services has a login form to fill in before accessing the service, which in itself is a security measure -- however telnet being a cleartext protocol, it is possible to sniff the credentials, thus making the login process relatively secure. The warning messages included in the banners are a good prevention measure in case someone connect to the service by mistake. It is unlikely that a malicious individual would stop an attack by seeing those messages. The best risk avoidance measure that can be found in the dataset is to assign SSH to port 23 and 2323.

      [TODO: detail potential strategy from the different actors based on literature and not the dataset]

   b. **have the strategies changed significantly over time in a way that reduces or increases risks?**

      To be able to gather this from the dataset provided, a filtering according to unique IP scan count, which identifies how many times each unique IP was scanned in entire time period, and the number of banner changes in each unique IP addresses has been done. The results will be shared in detail in the final report. Preliminary results show that there was no significant change in the banners that can affect the security in a

positive or negative way. Before concluding in this decision, the data from the first filtered data has been reduced through the following criterias;

- ➢ If the number of scans is equal to the number of banners, these data were removed because those are generally the banners that include a quote of the day or exact timestamp. Therefore, even if they are unique, they never change the behaviour that can affect the security of the device.
- ➢ If there is only one unique banner, these data were all the same during the entire scan period.

IMPORTANT NOTE & LIMITS: While evaluating this, we looked in detail some IPs in the original dataset which had significant difference between how many times the scan has been done on them and how many times they displayed unique banners to be able to see and analyse the change. By this way it was planned to gather the information if they were affecting the security. It has been discovered that for some IPs after a specific time period there is no more entry. To be precise, for instance, IP address 145.130.38.249's scan started on 18 February 2018 and ended on 22 April 2018. If the reason of this cut off in the scan (considering the scan was done from 1st of January 2018 until 30th of August 2018) was because telnet port of this IP was turned off, then it means that there was a significant security change in lots of IP addresses. On the other hand, if it is removed from the scan list upon request of the IP address holder then there still may not be any difference. Unfortunately, for this discussion, we need more information about the methods ShadowServer used to collect this data which is not displayed in their website or online.

6. **Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy, for example:**

(Notes: This section is still a draft. We would like to receive your feedbacks, whether what we are currently doing is correct or not.)

The risk strategy selected for this approximation is {deploying a security awareness program in every universities or companies}.

a. Estimate the costs involved in following that strategy

   The costs of conducting the risk strategy is around {1.5 million euros}.

b. Estimate the benefits of following that strategy (assume a particular loss distribution)

- Financially / the number of mitigated risks
  - Identify the assets
    - The devices (easier to quantify: calculate the number of unique IP addresses from the dataset: 125915)
      - The number of routers/switches: 37104 unique IPs
      - The number of computers: 13647 unique IPs
    - Telecommunication networks using the routers/switches (impossible to calculate precisely. For example, including the damages caused by DDoS)
  - Research for the costs estimation (direct/indirect expenditure)
    - Average price for
      - the routers/switches: around 60 euros in amazon.
      - the computers: around 550 euro in 2018 [computer price].
  - Apply the security measure to the assets
    - Create assumptions of the values of the losses and investments.

- Assumptions of security measures success: {40%}, which means, the number of vulnerability can be reduced by {40%}.

The ROSI can then be estimated as follows.

- Risk Exposure = 37104*60+13647*550 = 9.7 million euros
- Risk Mitigated = 40%.
- Solution Cost = 1.5 Million euros.
- ROSI = $\frac{(Risk\ Exposure \bullet \%\ Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost}$

  ROSI = $\frac{(9.7 \bullet 0.4) - 1.5}{1.5} \bullet 100\% =$ 159%.

Based on the computed ROSI, investing in {education} seems to be beneficial for the problem owners, since the ROSI is larger than the cost of the {education program}.

7. References
   a. [problem owner] - https://www.visioline.ee/itup/itup/roles/problem_owner_3556C72.html
   b. http://minds.wisconsin.edu/bitstream/handle/1793/40423/2002gundersonr.pdf?sequence=1
   c. Akin, Thomas. (2002). Hardening Cisco Routers. California: O'Reilly & Associates.
   d. [nro rir] - https://www.nro.net/about-the-nro/regional-internet-registries/
   e. [shadowserver] - https://www.shadowserver.org/wiki/
   f. [cyber schools] - https://www.cyberdegrees.org/listings/top-schools/
   g. [computer price] - https://www.statista.com/statistics/722992/worldwide-personal-computers-average-selling-price/
   h. https://drive.google.com/file/d/1Yx5-cFW_LciP1TxS9yMnVKhqJgia_DcW/view?usp=sharing

i. https://drive.google.com/file/d/1HgxE5LH6gD9i_WsKO4WKNtf-_u6IHilb/view?usp=sharing
j. https://docstore.mik.ua/manuals/hp-ux/en/5992-3387/ch02s10.html
k. https://nvd.nist.gov/vuln/detail/CVE-1999-0619
l. https://telnetscan.shadowserver.org/