Question 1 (10 points)

As we have discussed in class, a sophisticated cyber attack will likely begin with some reconnaissance activity to find the "easiest way in" and to make a compromise most likely. Often this is then followed by a social engineering and spear phishing attack leveraging the information gathered.

The goal of this assignment is to create awareness how much information can be found about you online, and what could be exploited in such an attack. Pretend to be the adversary and search the web and any public databases for information about yourself. What information is available and what kind of profile could someone build about you? Think about your professional life (past schools, work experience), your social life (parents, friends, partners, etc.), skills and interests (which clubs, hobbies, activities you are interested in), political views, where you have been, but also add anything you find important.

As an answer to this question, make a list of things that can be found out about you (1), where you have found this information, and how sensitive you would rate this information.

(1) Note: We don't expect you to reveal this information in your answer, but instead describe it. For example, don't write your girlfriends/boyfriends name, but state that this information could be found and was accurate.

Passive Reconnaissance like *Web Presence, Social Media Profiles of Employees* etc., provide lots of personal information to the adversaries with a simple Google search. **Employee impersonation and Social Engineering Attack** could be done with the details from Linked-in.

I searched for information about myself on the public database “Google” in incognito mode. When I typed “Nivedita Prasad” and my Gmail email-id, I found my Pinterest profile and the pins I have saved publicly available. However, my face-book profile was not visible even after filtering according to school and city. The picture from my twitter account was visible in the images tab of google. Additionally, when I used for my name in Instagram site, my profile was available with the profile picture. The professional details from linked-in including the posts I had shared and liked was readily available when my name was searched. I searched the same using Bing, which gave me more in-depth details stating my previous workplace name – displayed under my name. The Quora website was displaying my profile picture along with the geographical location and the current place of work and bachelor’s college names. Wikipedia did not display any information. I personally found LinkedIn profile gave away the complete information of my location and current education, previously attended schools, summary, my interests and skills in programming skills, the links to previous employees and friends I had added for the potential employers to have a good understanding about me. My profile was available in the Top 25 profiles, making my personal information easily vulnerable to adversaries. A behavior profiling can be made and when the same **usernames are reused** everywhere it really becomes easy to compromise other personal information like bank details or send spam emails using botnet etc.

Question 2 (15 points)

We have discussed in class the concept of port scanning and learned about the volume of attacks on the Internet. In this assignment you will investigate ongoing intrusion attempts against yourself and

analyze information about these perpetrators. On http://honeytrack.cyber-threat-intelligence.com/, download and run the honeytrack client which will forward compromisation attempts to our website. When you go to the website, it gives you a real-time view of who is trying to break into your computer.

Run the honeytrack software for at least 3 days, and analyze the data. How many attempts are recorded, from where do these attackers come from? Do you see any difference by time of day, what can you conclude based on this? You can also download the entire list of events from http://services.cyber-threat-intelligence.com/honeytrack/download
As an answer to this question, summarize your findings, state in your report also the IP where you have collected the data.

If you are running Windows/Mac or don't want to install this, you can also run honeytrack inside a VM. If you have any questions on its use, you can email Sille Kamoen <s.kamoen@student.tudelft.nl>.

Note: I had installed honeytrack using my ubuntu VM and followed all steps. Unfortunately, I could not alter or login as admin into my router as the router are provided by the company my relative works for. Hence, I had mailed Sille after I followed the commands in command prompt as suggested by SIlle.

After I used the Telnet command, Sille mailed me a data set the same afternoon on which I have conducted my analysis.

The destination IP is 145.94.132.155 on which the honeytrack is conducted.

There were 2123 attacks in the span of 3 days with 730 attacks on 12th February and 655 attacks on the 13-Feb-2018 and 737 attacks on 14 th February**.** Additionally, the top 5 source IP from which an attack is launched from different source ports with a time span of 5- 10 seconds gap or sometimes an hour**.** The source ports are selected in random**.** The top 5 IP addresses from which attacks were launched, irrespective of the 3 days that the destination IP was monitored for attacks is displayed below. The country names from the IP addresses are found with the help of the link https://tools.keycdn.com/geo . The time of the day doesn't affect much as there is a gap of 5 seconds or a gap of 2 hours in random.

IP Address	Country	Number of attacks
51.15.193.245	France	63
68.195.111.64	United States-Brooklyn	45
103.234.226.32	Taiwan-Taipei	45
188.166.57.143	Netherlands-Amsterdam	38
85.244.179.228	Portugal-Angra	31

Question 3 (10 points)

Explain two fundamental resources of the IP fragment reassembly process that could be abused in a resource depletion attack.

1. Memory of the host – one or more fragments may overlap

Tear drop attack causes the host to compute the length of the fragments incorrectly which will lead to overlap of the segments, thereby exhausting the entire resources during reassembly and leading to system crash as the data overwriting slows down the system and causes it to crash.

2. The assembly instructions provided by the packets exceed the length of the packet as indicated by the IP header.

In the Ping of Death attack, the insufficient validation of the IP reassembly process that is triggered by any type of protocol delivered through IP. The cause was mismatch between the maximum length of an IP packet which the protocol and the 16 bit packet length is restricted to. During reassembly there is a chance of the fragments exceeding the maximum length. Whether or not an IP implementation would be vulnerable would depend on the process used for reassembly. If a memory region of the maximum permissible packet length was allocated, an unchecked copy could overwrite the other parts of the memory (buffer overflow).As the networking stack is an integral part of the host's operating system, such an overflow has the potential to crash the system.

3. Too many fragments came in and exceed the buffer space the receiver has set aside until reassembly

Rose attack is where the adversary will fill the buffer with a flood of packets all indicating more frames to follow that are never completed. This does not crash the system but denies connections made.

4. The fragments do not reassemble to a complete packet and some data is missing.

The New Dawn attack exhausts the host's CPU cycles rather than exhausting the buffer by making some fragments of the data are deliberately missing.

Question 4 (10 points)

Initiate DNS queries to a public DNS server for a number of well known websites and record the size of the request and response packets. What is the difference in query and response for typical DNS queries such as the lookup of an IP address, subdomain or mail server address? Based on your knowledge of DNS, describe which type of requests will generate a higher amplification factor. Provide a few examples you could find.

DNS amplification attacks:

To avoid DNS resolver being abused in DoS attacks against other parties, DNS servers should not provide recursive lookups as a public service without reason. This issue begins with software engineering principles with software engineers setting safe defaults. Recently many DNS software

packages allow recursive resolving by default. We can solve this by limiting the queries to the IP ranges the DNS serves such as allow-query.

Here the query for www.google.nl is a recursive query / lookup.

Initiating DNS queries to a public DNS server (UDP and destination port 53):

I have used the Wireshark software to initiate the DNS queries to a public DNS server. A example of the public server I queried for is **www.google.nl** , the request time was "0.017010 seconds" and the response time was "0.033596000 seconds" . The details are from wire shark for the www.google.nl , (IPV6 address)**source IP**: fe80::88d6:ceaf:5f85:bbf1 , **Destination IP:** fe80::7ac1:a7ff:fe10:826f **Protocol:** DNS**, Packet length** is 93, Flags: 0x0100 and the **information** is "Standard query 0x4024 AAAA www.google.nl".

Another public server I queries for is **www.overleaf.com** . The request time is "83.664558 seconds" and the response time is 0.033596000 seconds. The details are from wire shark for the www.overleaf.com ,(IPv4 address) **source IP**: fe80::88d6:ceaf:5f85:bbf1, **Destination IP:** fe80::7ac1:a7ff:fe10:826f **Protocol:** DNS**, Packet length** is 96, Flags: 0x0100 and the **information** is "0x0100 Standard query 0x3b17 A www.overleaf.com ".

www.google.nl - difference in time between the request and response is 0.016586 seconds.

www.overleaf.com - difference in time between the request and response is 83.649884 seconds

Further details for www.google.com is:

Flags: 0x0100 Standard query

0... .... = **Response: Message is a query**

.000 0... .... = Opcode: Standard query (0)

.... ..0. .... = Truncated: Message is not truncated

....1 .... = Recursion desired: Do query recursively

.... .0.. .... = Z: reserved (0)

....0 .... = Non-authenticated data: Unacceptable

Domain Name System (response)

[Request In: 28]

[Time: 0.033596000 seconds]

Transaction ID: 0x4024

Flags: 0x8180 Standard query response, No error

1... .... = **Response: Message is a response**

.000 0... .... = Opcode: Standard query (0)

Queries

www.google.nl: type AAAA, class IN

Name: www.google.nl

[Name Length: 13]

[Label Count: 3]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Question 5 (10 points)

An organization wishes to strictly regulate the use of applications within their network, clients may for example only use web and e-mail applications but not instant messaging services. To accomplish this, the company deploys a proxy gateway setup and requires all clients to authenticate against the bastion host. Critique their solution.

Instead of the company deploying a proxy gateway setup and requiring all clients to authenticate against the bastion host which is not an ideal solution, an alternative design that balances the implementation of strict trust boundaries with maintainability and usability using different controls is a good solution. The organization's work place can be located in the same trust zone and the mechanisms such as VLAN's or 802.1X provide each host dynamic access based on the user's(emloyee's) role and privileges. This allows flexible work places and access via a trusted connection from the outside. The internal servers are decoupled from the company's users and may be concentrated into one secure location under tighter access control.

Question 6 (10 points)

`

In the "classical" network design of access, distribution and core layer, there are typically no security measures such as firewalls deployed in the core. Discuss whether this is a "wise" design. Since the core connects everything, this should be a prime location to enforce security policies?

The design of the network's core layer is centered around one task: Provide High-Speed and resilient connectivity between ta network's geographically different locations. With the core devices focused on fast packet forwarding, typically no packet manipulation or filtering happens within the core after the processing in the distribution layer. core devices are highly interconnected to provide a comparable network diameter for any routes passing though the core, and thus consistent and predictable packet experience between any path across the network core layer.

Hence the firewalls should not be deployed in the core as high speed is important and the firewalls will slow it down. Hence it should be designed and placed outside the core.

The network security and design considerations should be implemented with organizational requirements in core, distribution and access blocks of the network. Hence the core is routed instead of switched, to make more efficient use of the band width and introduce separate broadcast domains. Switching is restricted to the leaf parts of the network. Applications and data only accessible to the internal network are located directly off the core, to provide the highest speed and the consistent performance from all points in the organization.