Reg.No: IT15156952
Name: S.Benjamine
Question 01

1. A. The date : September 22nd 2016
   B. a. Source: Trinidad and Tobago, Destination: Poland
      b. For 31 minutes. (Sep 22 2016, 15:55 – Sep 22 2016, 16:26)
      c. How the attack been pulled off?

         This attack pulled off by the Volumetric (ICMP flood). Volumetric attack is a common type of the DDoS attack by using UDP floods and ICMP floods. Here ICMP flood is mentioned as the way of attack. ICMP is a protocol which is used by the network devices to send their error messages (e.g. Service not available). ICMP flood occurs by making flooded spoofed ICMP echo request from the infected botnet systems (botnet contain many zombie computers and those zombie computers can replicate by infecting the other computers). Generally botnet contain multiple computers. When these ICMP echo messages redirected towards a target server that server will overload and it cannot be able to process the valid ICMP messages from the legitimate users.

   C. United States
2. A. The date: July 17th 2016
   B. a. Source: Colombia, Destination: Czech Republic
      b. For 7 minutes. (Jul 17 2016, 21:30 – Jul 17 2016, 21:37)
      c. How the attack been pulled off?

         This DDoS attack is based on the fragmentation. IP fragmentation is a process of breaking the IP packets into smaller units which can be acceptable to transmit to avoid traffic (MTU). Attackers sends IP which exceeds the maximum allowable size through the ping command (e.g. IP datagram of 65535 bytes which MTU is 1500). If many exceeded size packets reached to the server at the same time (transmission process will automatically break them into small fragmented packets) it is difficult to handle. If it is large then fragmentations also many. By this act the server needs to wait till the last/all fragmented packet arrive. So server cannot be able to provide it service until it clear its traffic.

   C. Czech Republic

3. A. The date: 2013 11th December
   B. a. Source: Unknown, Destination: United States
      b. For 20 days and 2 hours 45 minutes. (Dec 11th 2013, 10:23 to Dec 31st 2013, 13:08)
      c. How the attack been pulled off?

         The attack pulled off by TCP Connection (TCP SYN). TCP SYN flood is a type of DDoS attack that exploits part of the normal TCP three way handshake to consume resources on the targeted service and render it unresponsive. Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation. In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server,

unaware of the attack, receives multiple, apparently legitimate request to establish communication. It responds to each attempt with a SYN-ACK packet from each open port. The malicious client either does not send the expected ACK, or if the IP address is spoofed never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet.

C. United States

Question 02

A. u-Torrent Forums Hacked.

What Happened?

Basically if we are a hacker and if we want to hack something then we need some vulnerabilities. As like that u-Torrent which is a part of the Bit-Torrent had some vulnerabilities. Those vulnerabilities were not originated from their forums, but that vulnerability originated from the vendor's client. Usually this kind of website organizations are having many vendors to provide their services to their customers and at the same time vendors are also having some clients for their resources. The hacker/intruder make use of the vulnerability in the client to move inside up-to the database of the u-Torrent. Generally these kind of Organizations will not say their vulnerabilities to the outside world.

u-Torrent having 150million of active users per month and ten thousand visitors per day and 388000 registered members. So, the hacker gaining the access of the user database is a huge issue for them. Mainly the organization cannot able to identify the attack because their vendors and vendor's clients are not directly under their controls. If a attack occurred they cannot be sure what information was compromised.

How they informed their customers?

u-Torrent team was alerted/informed by the issue occurred by the vendor(vendor who had the vulnerability). Vendors are out of their boundary so they did not expect the attack which was indirectly compromised. After they identified the attack and they informed their legitimate users to change their passwords again through another site for the precaution. By using their blogger page announcement they informed to their customers.

u-Torrent vendor make some actions and changes to mitigate the attack but the hashed passwords are compromised. Hacker gain nearly 100000 user details with their hash passwords. Here the hashing mechanism reduce the risk rate level for the u-Torrent.

Snap-chat Hacked

What happened?

Before move into the attack we need to know this attack is done by the hacktivist/gray hat hackers. Gray hat attacks are not to gain advantage but just find the vulnerability and exploit it and reveal that to the outside world. As hacktivist

they are doing these things for a purpose. This Snap-chat attack is also having a purpose that was making revenge on the statement which was delivered by the CEO of Snap-chat. “We don’t have any plane to expand the business to poor countries like India, and this app was only meant for rich people”. Snap-chat was hacked by the Anonymous Indian hacker group which consist with top bug bounty hunters. They hacked the 1.7 million Snap-chat users details and published on the dark net. Snap-chat is a social media where people can share their news, photos and videos. This kind of of attacks makes the social medias as untrusted things and their trusting rating also will be down. Reports are saying Snap-chat rating move to one star from the 5 stars (maximum) in the Apple’s App Store.

How they informed their customers?
In their case, before to inform their customers they are pulled to ask the sorry from the Indians. Snap-chat CEO said “This is ridiculous. Obviously Snap-chat is for everyone! Its available worldwide to download for free”. After this attack customer boycott and unistall the Snap-chat App.

B. u-Torrent –

It is a Bit-Torrent site. Bit-Torrent is having a good internal security measures auditing as well as testings. But Bit-Torrent sites are mostly illegal and they are not under the governments. When its comes to a system which is having more users they have need to strength their security level to prevent hacking/security attacks. In the Bit-Torrent sites there are some addwares can be available. These addwares are obstructing the legitimate customers. When we are seeing the above mentioned u-Torrent Forum, that forum uses Invension Power Board software and that software is not capable to provide sufficient security may as the vulnerability for that attack.

Snap-chat –

When its come to social media networks they will have user authentication and CIA (confidentiality, integrity and availability) on their information and resources. Here the weaken security and less security architecture were the vulnerability. Because they kept the user details that can be easily accessible when its attacked. The details wants to be under authorized access and in encrypted format which make the risk rate lower. Release of the key metrics of the Snap-chat is also cause to its fall.

C. It can be both based on the consequence.

Because in generally small business and start up business are not having much capital to run their business. They don’t have any security policies and separate departments/division for the risk assessment. If the consequence can be affordable they can afford it with their effort (when it comes to risk we want to accept/mitigate the risk/transfer it to 3rd party/ignore). The consequence which is unexpectedly coasting then it cannot be affordable for the business.

Question 03

1. What is confidentiality?

   Uses encryption algorithms to encrypt and hide data.
2. What is integrity?

   Uses hashing algorithms to ensure that data is unaltered during any operation.
3. What is availability?

   Assures that data is accessible. This is guaranteed network hardening mechanisms and backup systems.
4. What is a Denial of Service attack?

   DoS attacks are highly publicized network attack. A DoS attack results in some sort of interruption of service to users, devices, or application.
5. What is a virus?

   A virus is malicious code that is attached to executable files which are often legitimate programs.
6. What is a trojan?

   A Trojan horse is malware that carries out malicious operations under the guise of a desired function.
7. What is a botnet?

   A hacker build a network of infected machine. A network of infected host is called a botnet.
8. What is a zero day?

   This is newest cyber attack. The world never seen before.
9. What is a n-day?

   This is oldest cyber attack. The world seen before.
10. Is a bug the same as a vulnerability?

    Yes
11. What is a weakness?

    Loop hole of system.
12. Name 4 ways an attacker can act anonymously online

    Reconnaissance Attacks

    Access Attacks

    Social Engineering Attacks

    DoS Attacks