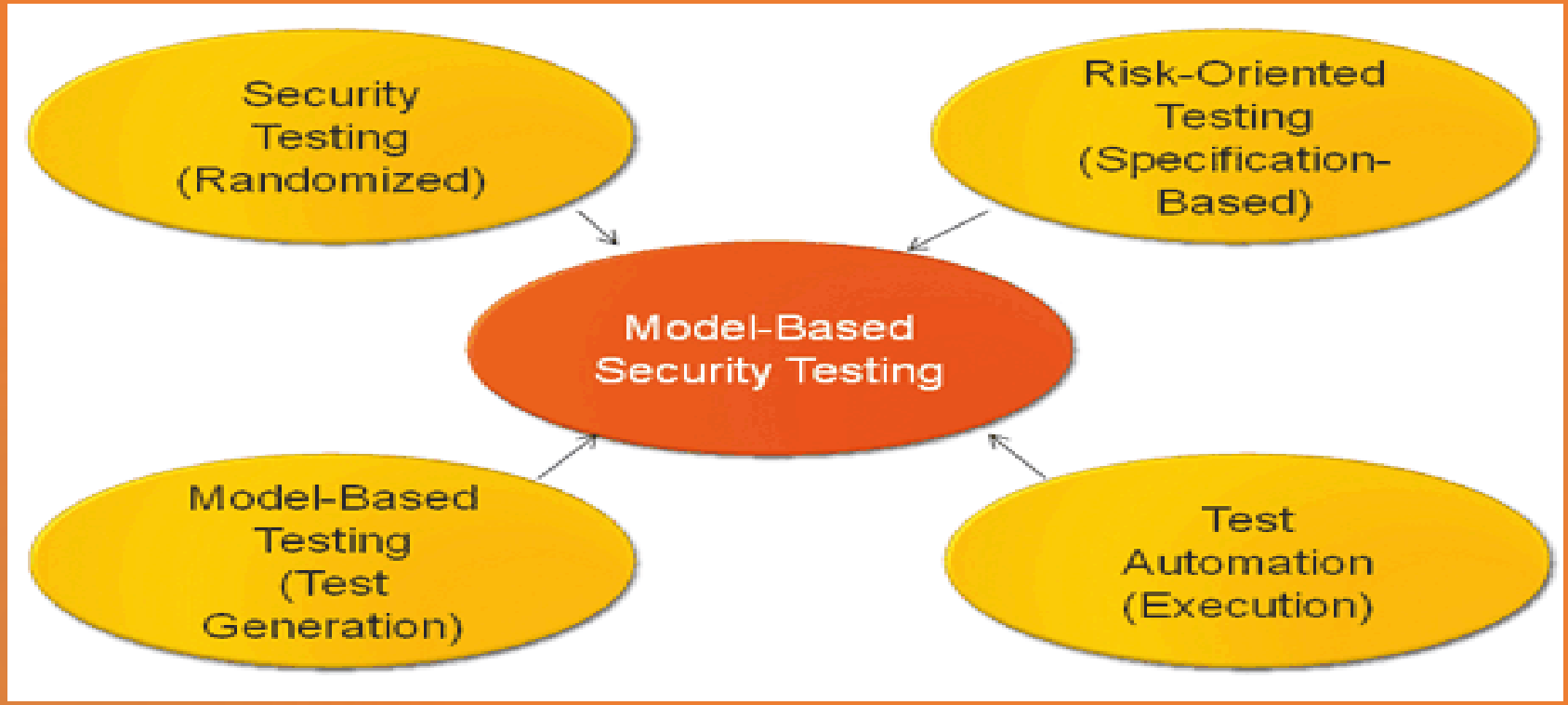
DENIAL OF SERVICE ATTACK (DOS)

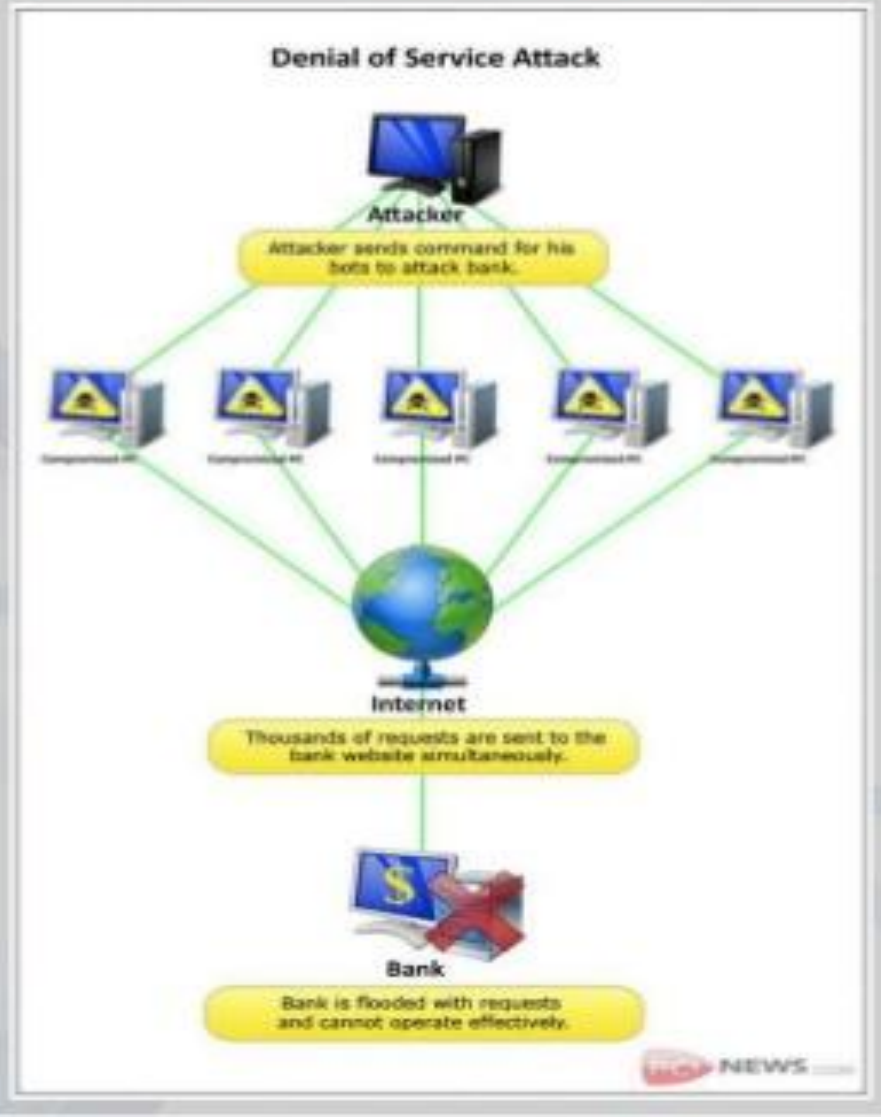


Present by :- Rahul kumar jha

What is "DOS ATTACK"

- A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.
- DOS = When a single host attack.
- DDOS = when multiple hosts attack simultaneously.

TYPES OF DOS ATTACKS



TYPE OF "DOS ATTACK"

- **Volume Based Attacks :-**

Imperva counters these attacks by absorbing them with a global network of scrubbing centers that scale, on demand, to counter multi-gigabyte DDoS attacks.

Protocol Attacks :-

Imperva mitigates this type of attack by blocking "bad" traffic before it even reaches the site, leveraging visitor identification technology that differentiates between legitimate website visitors (humans, search engines etc.) and automated or malicious clients.

Application Layer Attacks :-

Imperva mitigates Application Layer attacks by monitoring visitor behavior, blocking known bad bots, and challenging suspicious or unrecognized entities with JS test, Cookie challenge, and even CAPTCHAs.

HOW TO DEFEND

- During a DDoS attack, an effective defense will include:
- On-premises gear automatically detects the attack and activates mitigation procedures.
- The incident response team is automatically alerted when the attack escalates to a certain level without being successfully mitigated.
- The incident response team engages by verifying that a real attack is taking place (rather than a false positive), analyzing the attack, providing mitigation guidance and recommending cloud swing when needed.
- A diversion signal is sent to the cloud, along with details about the attack.
- The cloud team diverts traffic for scrubbing, usually using the Border Gateway Protocol (BGP) or the Domain Name System (DNS).
- When the attack is over, traffic is restored to its normal path through the ISP.

CONCLUSION

- Role of international bounderies –consoles located across international border, law-enforcement problem.
- In the past , as the present , DDoS has been more a nuisance activity conducted by cyber vandas than an activity with specify scioeconomic aims.
- In the future , DDos may be used as a disruptive force , with brod destabilizatio as its aim instead of targeetin of specific target.
- Destabilization has a high (ROI) return on investment when compared to targeted attacks.

THANK YOU