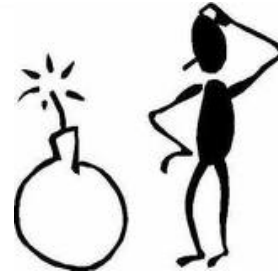




D Deep Guard

- **Dos , DDOS Protection Solution**
- **Web Application Security**

DOS and DDOS Attack ?



- **A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.**
- **DoS/DDoS attacks are a virulent, easy to launch type of Internet attacks, they have caused some biggest web sites on the world -- owned by the most famous E-Commerce companies such as Yahoo, eBay, Amazon -- became inaccessible to customers, partners, and users, sometimes for up to twenty-four hours; some web sites have experienced several days of downtime while trying to restore services.**



- **Although targets of a DoS attack may vary, it generally consists of the concerted efforts of person or persons to prevent an internet site or service from functioning efficiently or at all, temporarily or indefinitely.**
- **DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers .**

Result..... the financial losses are very huge!!!!!!!!!!!!!!!.

- **The term is generally used with regards to computer networks , but is not limited to this field; for example, it is also used in reference to CPU resource management.**



DoS attack forces Dutch bank offline

➤ The outage of Dutch bank Rabobank last weekend was caused by a massive DDoS attack. The perpetrators are still unknown. The bank reports the attack to the police. After two days of mystery surrounding the outage Rabobank gave Dutch IDG-title Webwereld a statement explaining the breakdown of both its website and its e-banking services.

➤ The Dutch bank was hit by a large DDoS attack (Distributed Denial of Service). The outage of Rabobank happened Saturday evening and again Sunday afternoon. The website and e-banking services were inaccessible for desktop and mobile users.

➤ Domino effect

The DDoS attack also caused an outage in the Dutch central payment system iDeal. That alternative to PayPal was flooded with returned transaction messages from the attacked bank. This DoS-'attack' (Denial of Service) caused the payment system to go partially down.

<http://webwereld.nl/nieuws/105785/rabobank-legt-ideal-plat-met-dos-aanval---update.html>



Solution :

Deep Guard Anti-DDOS Software / Hardware Firewall Protection Against ;

- ✓ TCP (syns, syn-acks, acks, fins, fragments)
- ✓ UDP (random port floods, fragments)
- ✓ ICMP (unreachable, echo, fragments)
- ✓ DNS
- ✓ Client Attacks
- ✓ Inactive and total connections
- ✓ HTTP Get flood
- ✓ BGP attacks
- ✓ ARP Spoofing
- ✓ Against Botnet

The logo for Deep Guard, consisting of a blue shield-like icon with a white 'U' shape inside, followed by the text "Deep Guard" in a blue, sans-serif font.





Web applications security: risks and countermeasures

- Reports of vulnerabilities in web applications have risen sharply. Web applications contain vulnerabilities that are easily exploited by attackers to bypass traditional security measures and damage your organization. Because of this, it is essential for organizations to find weaknesses in their Web applications and remediate them. Exploits are easy to develop and targets are easy to find. It is therefore important that we adapt to these threats, when programming and also when we use these applications.
- Web applications are commonly used from a web browser and they cover a range of activities, such as e-banking, webmail, online shopping, community websites, blogs, vlogs, network monitoring and bulletin boards.



- In recent years the development of such applications has been considerable, and today rich internet applications offer complex, real-time interactions with users. For instance, web operating systems such as eyeOS offer many functionalities that were previously available only with traditional operating systems.
- While web applications have become ubiquitous, they also present new security risks. It is important to identify and understand these risks when developing, hosting or simply using these applications.



Deep Guard

Web Application Software / Hardware Firewall Web Application Firewall Solution :

- ✓ XML security
- ✓ Cross Site Scripting (XSS)
- ✓ SQL injection flaws
- ✓ OS command injections
- ✓ Cross-site request forgery
- ✓ Site reconnaissance
- ✓ Session hijacking
- ✓ Application denial of service
- ✓ Malicious probes/crawlers
- ✓ Cookie/session tampering
- ✓ Path traversal
- ✓ Information leakage
- ✓ Buffer overflow

Thank You

