网站安全：底层平台的安全-DDos，扫描，ARP，暴力破解，恶意篡改，针对服务攻击；网站程序安全—注入攻击，代码漏洞，欺骗攻击。

DDos通过正常或非正常迫使服务器资源耗尽，洪泛攻击方式

扫描是对攻击进行的准备，用来获取服务器的详细信息，有什么服务，是用什么软件，有什么端口号；

暴力破解：使用穷举法尝试用户的密码；

篡改配置：攻入系统后修改配置文件或其他设置。

Iptables是linux内置的防火墙，对于网站安全来说，它是比较方便的一种，只允许特定的流量通过，禁用其他流量；1:允许ssh流量，2：允许dns流量，3：允许业务流量，4：禁用其他流量；

Iptables –A INPUT –p tcp –dport 22 –j ACCEPT;

Iptables –I INPUT 1 –p tcp –sport 53 –j ACCEPT;

Iptables –I INPUT 1 –p udp –sport 53 –j ACCEPT

Iptables –I INPUT 1 –p tcp –dport 80 –j ACCEPT

Iptables –A INPUT –j DROP;

阻止攻击流量：监控日志或netstat信息。

使用AIDE入侵检测：advanced intrusion detection environment，使用aide对文件的完整性进行检测，aide的配置文件在/etc，我们可以修改配置，1：初始化aide数据库aide --init，改变文件名，2：通过aide –check检查；3：更新aide数据库aide –update，4：周期性的将检查发送到邮箱。