**DNS域传送信息泄露**

Dns是整个互联网公司业务的基础，目前越来越多的互联网公司开始自己搭建DNS服务器做解析服务，同时由于DNS服务是基础性服务非常重要，因此很多公司会对DNS服务器进行主备配置而DNS主备之间的数据同步就会用到dns域传送，但如果配置不当，就会导致任何匿名用户都可以获取DNS服务器某一域的所有记录，将整个企业的基础业务以及网络架构对外暴露从而造成严重的信息泄露，甚至导致企业网络被渗透。

<http://static.hx99.net/static/drops/papers-64.html>

<http://www.lijiejie.com/dns-zone-transfer-1/>

<http://www.lijiejie.com/dns-zone-transfer-2/>

<http://www.lijiejie.com/dns-zone-transfer-3/>

**0x01 成因**

DNS服务器的主备数据同步，使用的是域传送功能。 域传送关键配置项为：

allow-transfer {ipaddress;}; 通过ip限制可进行域传送的服务器

allow-transfer { key transfer; }; 通过key限制可进行域传送的服务器

默认安装完毕后，配置项没有allow-transfer 项。如果直接使用默认配置文件进行配置的话（不手动添加allow-transfer项），就会存在dns 域传送漏洞。

**操作基本的步骤是:**

1) 输入nslookup命令进入交互式shell

2) Server 命令参数设定查询将要使用的DNS服务器

3) Ls命令列出某个域中的所有域名

4) Exit命令退出程序

Nslookup –type=ns 域名。

Server dns服务器

Ls 域名

**攻击者能获取的敏感主要包括：**

1）网络的拓扑结构，服务器集中的IP地址段

2）数据库服务器的IP地址，例如上述nwpudb2.nwpu.edu.cn

3）测试服务器的IP地址，例如test.nwpu.edu.cn

4）VPN服务器地址泄露

5）其他敏感服务器