DNS Hacking Technique:

هک کردن DNS سرور ها روشهای مختلفی دارد که قبل از هرگونه توضیح ابتدا باید نحوه کار کرد DNSسرور مورد بررسی قرار گیرد.

کار اصلی DNS فوروارد کردن و یا Map کردن هاست نیم به Ip وبالعکس می باشد که این کار به دو حالت زیر انجام می شود

Forward LookUp Zone (Forward Lookup Query)

به عمل مبدل شدن یک هاست نیم به ip گویند

Reverse Lookup Zone (Revers Lookup Query)

به عمل مبدل شدن یک ip به هاست نیم گویند.

که DNS سرور برای جستجو بر روی Forward Lookup Zone بر روی پورت udp53 و برای جستجو بر روی Reverse Lookup Zone بر روی پورت Tcp 53یه حالت Listen قرار می گیرد.

DNS به دو صورت full , incremental ترنسفر میشه.
که هر کدام در مورد نحوه ترنسفر و ارتباطش با DNS Server الگوریتم متفاوتی داره.
خوب در full و Incremental در واقع برای نشان دادن رکورد های DNS دیتابیس را می خونند
در وافع وقتی مشکل DNS Zone Transfer باشه این دیتابیس ترنسفر میشه به Client هکر و هکر می تونه تمام Record ها را ببینه. که این دیتابیس در سرور وجود دارد به عنوان مثال securehost.ir در مسیر

/var/named/securehost.ir.db

قرار دارد.

Typical DNS Attack's:

حملاتی که بر روی DNS انجام می پذیرد عمدتا 3 روش زیر می باشد

1 - Buffer Overflow Attack
2 - Information Disclosure Attacks
3 - Cache Poisoning Attacks

از روش های گفته شده روش 3 خطرناکترین حمله می باشد.

موضوع مورد بحث روش 2 می باشد که به DNS Zone Transfer نیز معروف می باشد.

در واقع این روش ، روش جمع آوری اطلاعات از DNS Server و رکورد های مربوط به DNS استخراج می شود .

به عنوان مثال در عکس زیر با استفاده از مشکل DNS Zone توانسته ایم تمام Recordهای وب سایت shabgard.org را استخراج نماییم.

```
root@linux [~]# clear
root@linux [~]# dig @shabgard.org shabgard.org AXFR

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> @shabgard.org shabgard.org AXFR
; (1 server found)
;; global options:  printcmd
shabgard.org.           604800  IN      SOA     shabgard.org. info.shabgard.org. 2007
011501 7200 120 2419200 604800
shabgard.org.           604800  IN      NS      ns1.shabgard.org.
shabgard.org.           604800  IN      NS      ns2.shabgard.org.
shabgard.org.           604800  IN      MX      10 mail.shabgard.org.
shabgard.org.           604800  IN      A       78.129.220.112
\\www.shabgard.org.     604800  IN      CNAME   shabgard.org.
magic.shabgard.org.     604800  IN      CNAME   shabgard.org.
mail.shabgard.org.      604800  IN      A       78.129.220.112
ns1.shabgard.org.       604800  IN      A       78.129.220.112
ns2.shabgard.org.       604800  IN      A       78.129.220.112
www.shabgard.org.       604800  IN      A       78.129.220.112
shabgard.org.           604800  IN      SOA     shabgard.org. info.shabgard.org. 2007
011501 7200 120 2419200 604800
;; Query time: 84 msec
;; SERVER: 78.129.220.112#53(78.129.220.112)
;; WHEN: Sat May 15 16:17:03 2010
;; XFR size: 12 records (messages 1)
```

که به وسیله این اطلاعات می توان روش 3 را که خطرناکترین روش می باشد را پیاده سازی نمود.

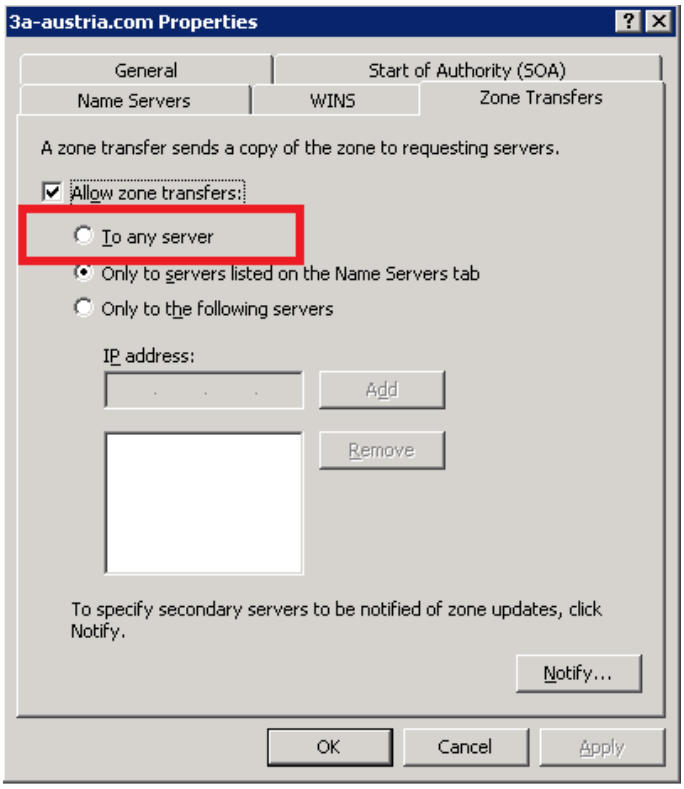
نحوه سکیور کردن :

از مسیر /etc/named.conf در Named.conf باید مقدار زیر را قرار دهید.

```
allow-transfer {none;};
```

و یا می توان یک ip خاص را در این قسمت اضافه نمود.

و در سروهای ویندوز نیز باید در تنظیمات مربوط به DNS در سرویس DNS در قسمت properties باید بررسی شود که عبارت to any server فعال نباشد.



تهیه تنظیم : **حامد مسافر**

ایمیل : Pen-Test[at]SecureHost.ir

وب سایت : http://SecureHost.ir

Author **: Hamed Mosafer**

Email : Pen-Test[at]SecureHost.ir

Web : http://SecureHost.ir