حملاته پروتوکل DNS

(Attacking DNS Protocol)

فهرست مطالب:

گفته های نویسنده 1
مقدمه..... 1-2-3
انواعه حملاته DSN Server 4
Cache Poisoning DNS Transaction ID Prediction 4-5

گفته های نویسنده :

شما در حال خواندن چاپ اول مقاله حملات پروتوکل DNS هستید در چاپ اول نویسنده سعی خود را بر این داشته که بتواند خواننده را با خود سرویسDNS آشنا سازد , در صورته دیدن کم و کاستی در این مقاله و دادن نظر در مورد مقاله با ای میل نویسنده تماس حاصل فرمایید از توجه شما ممنونیم .

مقدمه :

DNS (Domain Name System)

کار یک DNS Server مبدل یا MAP کردنه Host Name ها به IP Address ها و بر عکس است .

به عمل مبدل شدن یک هاست نیم به آی پی در اصطلاح میگویند:
Forward Look Up Zone (Forward Look UP Query)
وبه عمل مبدل شدن آی پی به هاست نیم در اصطلاح میگویند :
Reverse Look UP Zone (Reverse LookUP Query)

یک DNS Server برایه جستجو در Name Resolution ها (Forward LookUP Zone) بر رویه پورته UDP 53 و برایZone Transfer ها (Reverse LookUP Zone) بر رویه پورته TCP 53به صورته Listen قرار میگیرد .

ساختار اصلی یک DNS SERVER از چهار قسمت تشکیل شده است :

ROOT DOMAIN -1
TOP-LEVEL DOMAINS -2
SECOND-LEVEL DOMAINS -3
HOST NAMES -4

Copyright © 2004
www.PersianHacker.NET

Root Domain

در بالا ترین قسمت یک DNS یک دامنه هست به نام ROOT DOMAIN , بطوریکه روت دامین نماینده کل دامین است

Top-Level Domains

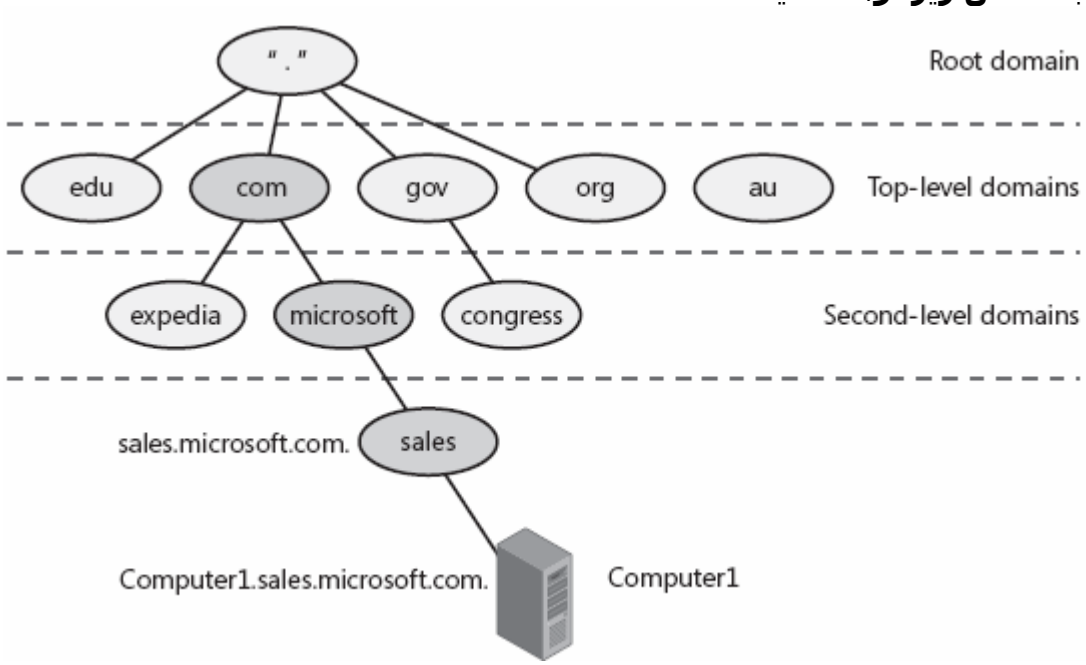
در این قسمت نام پسوندی دامنه قرار میگیرد که از دو , سه یا چهار کارکتر درست شده است
اصولاً TOP-LEVEL DOMAIN ها گروهایی هستند که بیان گر نوع سازمان یا محل جغرافیایی دامنه میباشند.
TOP-LEVEL DOMAIN ها توسط Internet Architecture Board (IAB) کنترل و ثبط میشوند به مثالهای زیر توجه کنید :

Top-Level Domain	Description
gov	Government organizations
com	Commercial organizations
edu	Educational institutions
org	Noncommercial organizations
au	Country code of Australia

Second-Level Domains

در این قسمت نام رحیستر شده دامنه قرار میگیرد

به شکل زیر نوجه کنید :



Copyright © 2004
www.PersianHacker.NET

BIND (Berkley Internet Name Domain)

سرویسه BIND بیشتر برایه DNS Server هایی که در اینترنت است استفاده میشود , به طوره نمونه BIND بر رویه انواعه سیستم عاملهایه مبتنی بر UNIX طراحی و استفاده میشود , که در هنگامه خارج کردنه اطلاعات (مخصوصه Domain) DNS Server یه کپی رو هم در خود ذخیره میکند .

DNS Client ها بر رویه سرویسی به نامه Resolve طراحی و به کار انداخته شده اند, در حقیقت Revolver درخواسته تجزیه و Resolve هاستها به IP ها را به سویه DNS Server میدهد, که جوابه آنها توسط Record هایه درون DNS داده میشود.

Record ها تعداده زیادی دارند که در مقاله به تعدادی از آنها اشاره میشود :

Value	Description
A	Specifies a computer's IP address.
ANY	Specifies all types of data.
CNAME	Specifies a canonical name for an alias.
GID	Specifies a group identifier of a group name.
HINFO	Specifies a computer's CPU and type of operating system.
MB	Specifies a mailbox domain name.
MG	Specifies a mail group member.
MINFO	Specifies mailbox or mail list information.
MR	Specifies the mail rename domain name.
MX	Specifies the mail exchanger.
NS	Specifies a DNS name server for the named zone.
PTR	Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information.
SOA	Specifies the start-of-authority for a DNS zone.
TXT	Specifies the text information.
UID	Specifies the user identifier.
UINFO	Specifies the user information.
WKS	Describes a well-known service.

Copyright © 2004
www.PersianHacker.NET

در آخر Client خودش قادر به برخورد و ارتباط با DNS Server به وسیله Resolve یک Name است . وقتی که Client با DNS Server ارتباط برقرار میکند Client قادر به افزودنه Query های مبتنی بر مرجع جوابها برایه سرور است .

Typical DNS Attack's:

DNS Server دارایه حملاته زیادی است که در این مقاله به بعضی از آنها اشاره میشود :

1- Buffer Overflow Attack

این حمله به وسیله Command Level Access بر رویه DNS Server و یا اصلاح کردنه Zone فایلها صورت میگیرید .

2- Information Disclosure Attacks

این اطلاعات شامله Zone Transfer و اطلاعات راجع به DNS Server , Version است .

3- Cache Poisoning Attacks

به وسیله این حمله میتوان DNS , Cache ها رو آلوده کرد که در این حمله از روش زیر استفاده میشود :

DNS Transaction ID Predication یا Recursive Queries

(در این مقاله بیشتر برروبه این نوع حمله بحث میشود)

Cache Poisoning DNS Transaction ID Prediction:

هنگامی که Client ی در دامینه www.Yahoo.com درخواسته Resolve دامینه www.Microsoft.com را به DNS Server میفرستد به طور نمونه چنین مراحلی طی میشود :

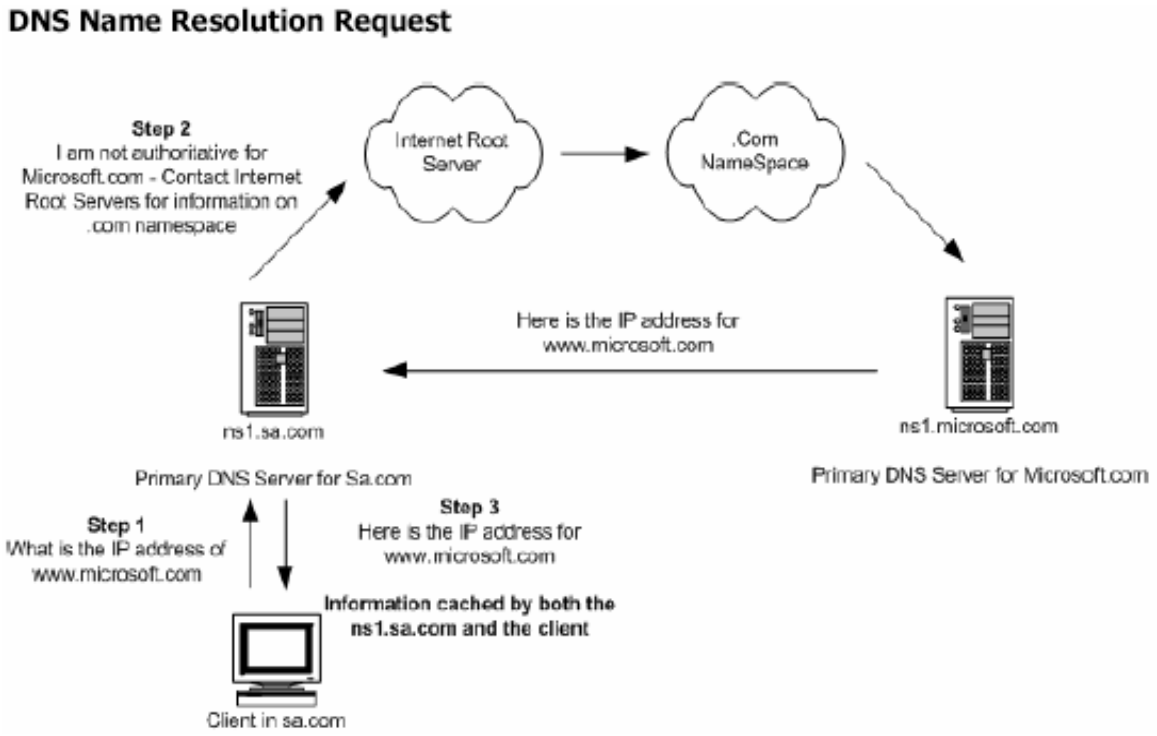
1- Client درخواسته برقراری ارتباط با DNS Server پیکر بندی شده و همچنین راجع به Resolve دامینه www.Microsoft.com را میدهد بسته ای که در این مرحله کلینت به سویه DNS Server میفرستد شامله : Source UDP Port, IP Address و DNS Transaction ID است.

2- DNS Server بعد از گرفتنه دامینه درخواستی Client (www.Microsoft.com) , اگر دامین برایه DNS Server معتبر یا Authoritative نباشد DNS Server با Root-DNS سرورهایی که با دامینه www.Microsoft.com در ارتباط است ارتباط برقرار میکند (به وسیله Query هایی که میفرستد) و ار آنها جواب را دریافت میکند .

3- جستجو (Query) با موفقیت انجام میشود و جواب به دسته DNS Server میرسد و بعد DNS Server اطلاعاته راجع به دامینه www.Micrsooft.com را به Client میدهد و این اطلاعات در DNS Server به صورته Cache ذخیره میشود .

Copyright © 2004
www.PersianHacker.NET

مانند شکل زیر :



پایان چاپ اول :

امیدوارم این مقاله برای شما مفید و مورد علاقه تان قرار گرفته باشد , منتظره چاپ دوم این مقاله باشید و همچنین مارو از نظرات مفید خود بهره مند کنید تا بتوانیم در راه بهتر شدن و بر طرف کردن کاسنی های این مقاله کوشا باشیم , موفق و پیروز باشید .

شناسنامه:

نویسنده **Ilov3ccie**
ای میل ..... **Ilov3ccie at Yahoo Dot Com**
منبع ..... PersianHacker.NET

Digitally signed by Amir Torabi
DN: CN = Amir Torabi, C = IR, O = PersianHacker
Reason: I am the author of this document
Location: In The World

هر گونه کپی برداری و استفاده از مطالب این مقاله با ذکر نام منبع و نویسنده آن بلامانع است
برای کسب اطلاع بیشتر در این باره اینجا را کلیک کنید.

Copyright © 2004
www.PersianHacker.NET