adel piri : mohajem.war@gmail.com inject0r.ir

in the name of allah

adel piri

# آشنایی با حملات مردی در میان

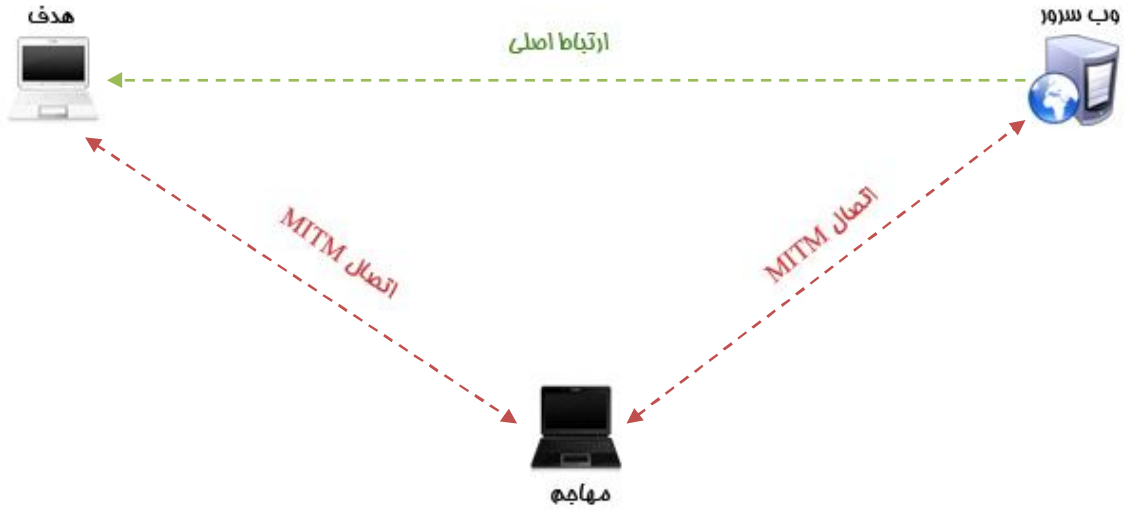
## Introduction to Man-in-the-middle Attacks

## فهرست:

## مقدمه بر MITM:

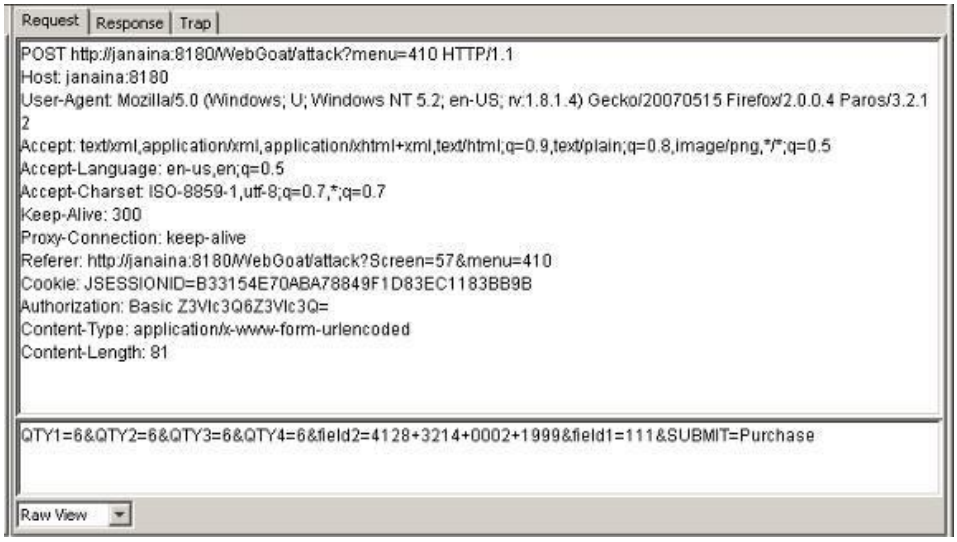
توسط حملات Man-in-the-middle که به اختصار MITM و به فارسی حمله مردی در میان خوانده می شود امکان استراق سمع و تجسس بر اطلاعات رد و بدل شده بین دو سیستم میسر می گردد. برای نمونه هنگام مبادله اطلاعات از نوع HTTP، هدف حمله، ارتباط TCP میان کاربر و سرور است. شخص مهاجم با استفاده از روشهای مختلف، ارتباط TCP اصلی را به دو ارتباط جدید تقسیم می کند.

همان طور که در تصویر ۱ مشخص است، این دو ارتباط شامل ارتباط میان حمله کننده و کاربر و ارتباط میان حمله کننده و سرور می باشد. هنگامیکه ارتباط TCP ردیابی شد، شخص حمله کننده به عنوان یک فیلتر که قادر به خواندن، تغییر و اضافه کردن اطلاعات است عمل می کند.




شکل ۱. نمونه تصویری حمله شخص میانی

از آنجایی که برنامه های http و انتقال داده بر پایه ASCII طراحی شده اند، حملات MITM می تواند بسیار مؤثر باشد. توسط این حملات، امکان مشاهده یا جمع آوری اطلاعات موجود در http و همچنین اطلاعات مبادله شده براحتی میسر می شود. بنابراین، همانطور که در شکل ۲ مشخص است، وقتی بتوان یک کوکی session را که در حال خواندن اطلاعات http می باشد کنترل کرد، پس این امکان نیز وجود خواهد داشت که مثلاً عدد مربوط به مقدار پول را در برنامهٔ تراکنش تغییر داد.




شکل ۲. نمونه تصویری یک بستهٔ http که توسط Paros Proxy ردیابی شده است

با استفاده از روش های مشابه، می توان اقدام به حملهٔ MITM به ارتباطات https نمود. تنها تفاوت این حمله، در نحوه برقراری دو SSL session مستقل در دوسر ارتباط TCP می باشد. در این حالت، مرورگر اینترنت یک ارتباط SSL با فرد حمله کننده ایجاد نموده و شخص حمله کننده نیز یک ارتباط SSL دیگر با سرور برقرار می نماید.

در این هنگام، معمولاً مرورگر اینترنت یک پیغام هشدار دهنده برای کاربر ارسال می کند ولی کاربر به علت عدم آگاهی از وجود تهدید، این پیغام را نادیده می گیرد. در برخی موارد امکان دارد پیغام هشدار برای کاربر ارسال نگردد. به عنوان مثال، هنگامی که تأییده سرور مورد حمله قرار گرفته باشد یا در شرایطی که شخص حمله کننده مورد تأیید یک CA معتمد قرار گرفته باشد که CN آن همان CN وب سایت اصلی باشد.

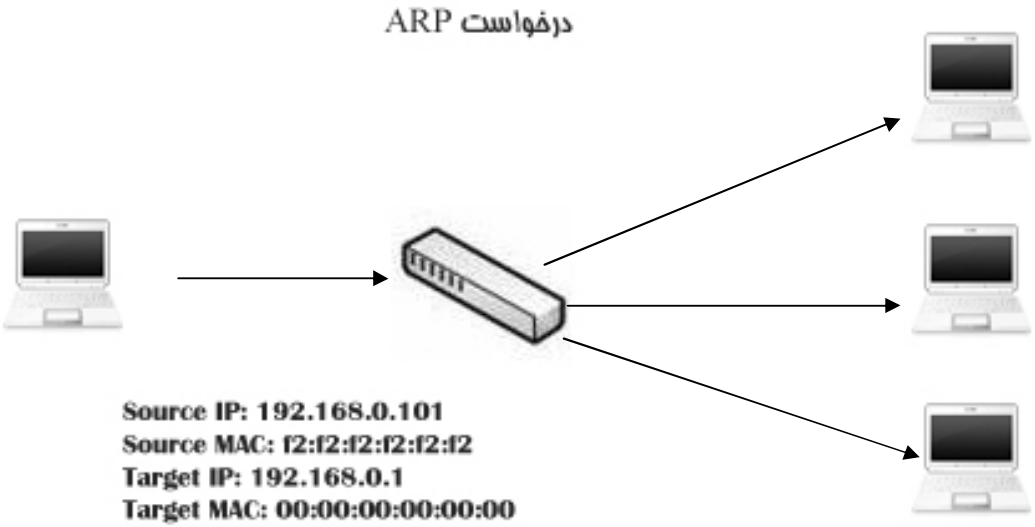
حملات MITM فقط به منظور حمله به سیستم ها در شبکه استفاده نمی شوند، معمولاً از این حملات هنگام اجرای یک برنامهٔ شبکه یا در جهت کمک به آسیب پذیر نمودن شبکه نیز استفاده می گردد.

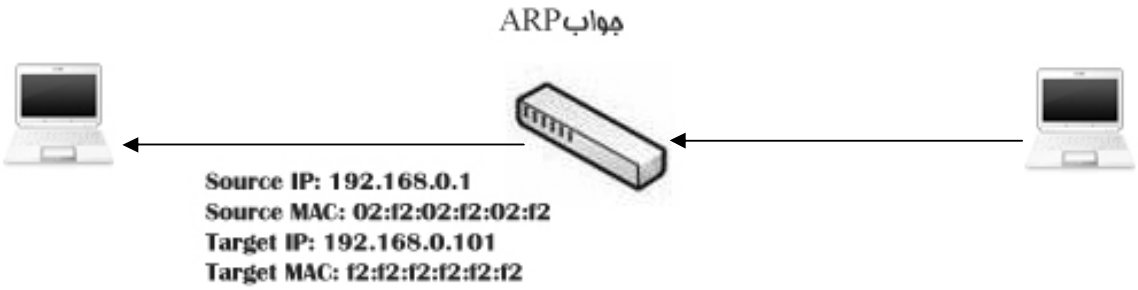
## مسموم سازی حافظهٔ کش ARP :

این روش (که گاهی با نام ردیابی سمی ARP شناخته می شود) به عنوان یکی از قدیمی ترین روش های حملات مدرن MITM شناخته شده است. در این روش به حمله کننده اجازه داده می شود تا در همان زیر شبکه ای که قربانیان در آن قرار دارند به استراق سمع و تجسّس بر تمامی اطلاعات ردوبدل شده بین قربانیان بپردازد ، این حمله یکی از آسانترین و در عین حال مؤثرترین روش های مورد استفادهٔ حمله کنندگان است.

## ارتباطات معمول ARP :

علی‌رغم اینکه نیازی به ابداع سیستم ARP احساس نمی شد، این سیستم جهت تسهیل در فرایند ترجمه آدرس های موجود در میان لایه های دوم و سوم مدل OSI طراحی شد. لایهٔ دوم یا همان لایه اتصال داده ، از آدرس های MAC جهت امکان برقراری ارتباط مستقیم بین دستگاه های سخت افزاری در مقیاس کوچک استفاده می کند. لایهٔ سوم یا لایه شبکه در بیشتر مواقع از آدرس های IP جهت ایجاد شبکه های مقیاس زدنی با قابلیت ارتباط جهانی استفاده می نماید. لایهٔ اتصال داده با دستگاه هایی که مستقیماً به یکدیگر متصل هستند سروکار دارد. در حالیکه، لایهٔ شبکه با دستگاه هایی سرو کار دارد که بطور مستقیم و غیر مستقیم به یکدیگر متصل شده اند. هر لایه فرم آدرسی مخصوص به خود را داشته و برای برقراری ارتباطات شبکه لازم است تمامی این لایه ها به همراه یکدیگر عمل کنند. این حقیقت، پاسخ محکمی برای این سوال است که چرا ARP همیشه به همراه RFC 826 که یک سیستم رزولوشن با آدرس داخلی است، ساخته می شود.





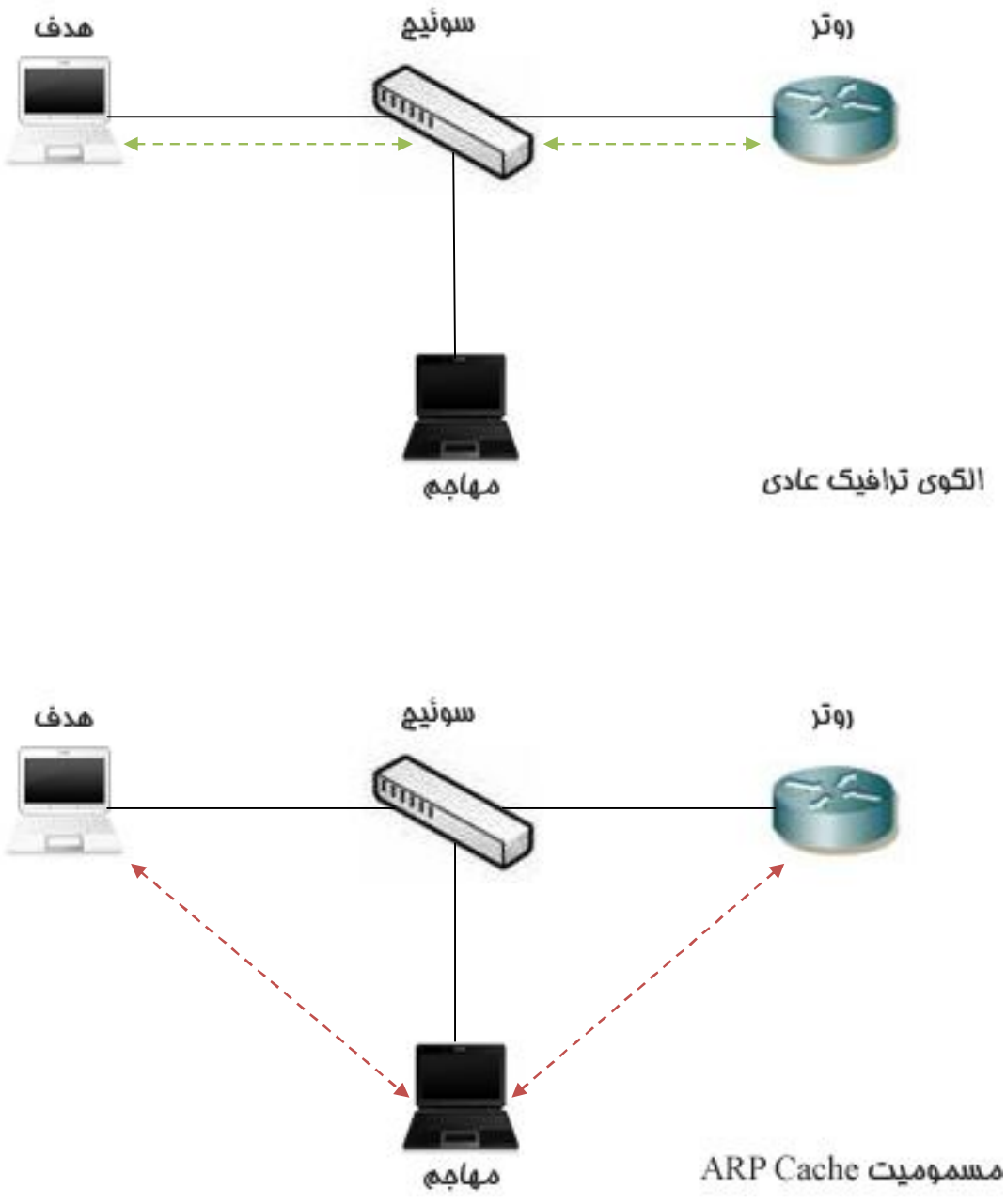

شکل ۳. فرآیند ارتباط ARP

عملکرد زیرکانهٔ ARP حول دو دسته کلی متمرکز شده است : دستهٔ درخواستی ARP و دستهٔ پاسخی ARP. اهداف این دسته ها، پیدا کردن مکان آدرس های MAC می باشد که این آدرس ها، با آدرس IP داده شده ترکیب شده اند . یافتن مکان آدرس های MAC باید طوری صورت پذیرد که در مسیر انتقال داده ها در شبکه خللی وارد نشود. دستهٔ درخواستی به تمامی دستگاه های شبکه فرستاده شده و حاوی این پیام است : "" آهای، آدرس IP من XX:XX:XX:XX و آدرس MAC من XX:XX:XX:XX:XX:XX است. من باید مطلبی را برای شخصی که دارای XX.XX.XX.XX IP می باشد ارسال کنم ولی آدرس سخت افزاری آن شخص را نمی دانم. آیا امکان دارد کسی که این آدرس IP را دارد، با اعلام آدرس MAC خود، به من پاسخ دهد؟"" . پاسخ از طریق دستهٔ پاسخی ARP اعلام شده و حاوی این متن است : "" آهای سیستم انتقال، من همان شخصی هستم که تو به دنبال آن می گردی و آدرس IP من این است : XX.XX.XX.XX و آدرس MAC من هم: XX:XX:XX:XX:XX:XX"". به محض اینکه این روند تکمیل شد، دستگاه انتقال جدول حافظهٔ کش ARD خود را به روز کرده و پس از آن ، هر دو دستگاه قادر به ارتباط با یکدیگر خواهند بود.

## روش مسموم سازی حافظهٔ کش ARP:

روش حمله از طریق مسموم سازی حافظهٔ کش ARP، از طبیعت نا امن سیستم ARP بهره می جوید. بر خلاف سیستم هایی نظیر DNS که به نحوی طراحی می شوند که تنها دارای قابلیت به روز شوندگی دینامیکی امن هستند، دستگاه هایی که از ARP استفاده می کنند، می توانند در هر زمانی به روز شوند. این بدان معنی است که هر دستگاهی در شبکه می تواند یک دستهٔ پاسخی ARP به میزبان فرستاده و آن را مجبور نماید تا حافظهٔ کش ARP خود را مطابق با مقادیر جدید به روز نماید. ارسال یک دستهٔ پاسخی ARP بدون اینکه درخواستی فرستاده شده باشد، فرستاده بلاعوض ARP نامیده می شود. هنگامیکه نیت سوئی توسط حمله کنندگان در حال پیگیری باشد، ارسال چند فرستاده بلاعوض ARP

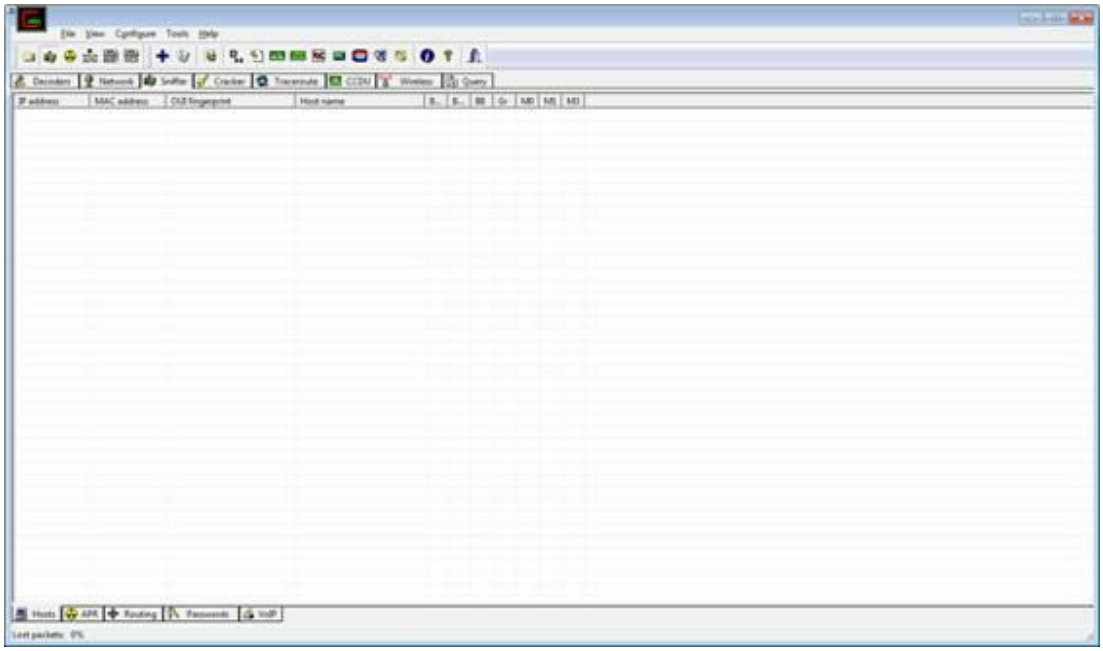
باعث می گردد تا قربانی گمان کند که با یک کامپیوتر میزبان در ارتباط است، در صورتیکه، در واقع آن قربانی در حال تبادل اطلاعات با یک حمله کنندهٔ در حال استراق سمع می باشد.




شکل ۴. الگوی ترافیکی عادی شبکه و سپس مسموم سازی کش ARP

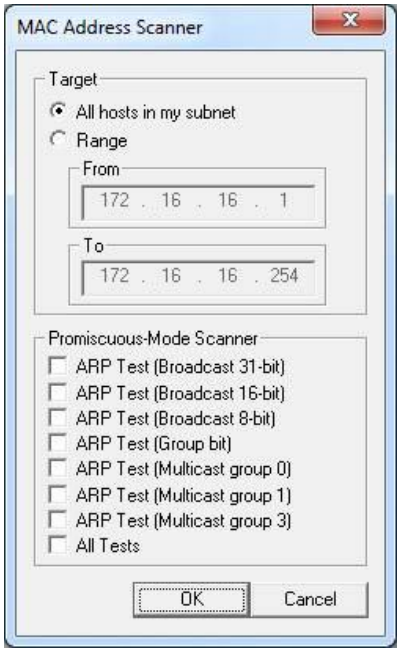
## استفاده از Cain & Able:

نرم افزار Cain & Able قابلیت های فراتر از آنچه ما در اینجا نیاز داریم را داراست، هنگامیکه برای اولین بار نرم افزار را اجرا می کنید، متوجه یک سری دگمه ها در قسمت بالایی پنجره این نرم افزار می شوید. ما از محیط Sniffer (جاسوس) جهت رسیدن به هدف خود استفاده می کنیم. هنگامیکه بر روی دگمه Sniffer کلیک کنید، یک جدول خالی مشاهده خواهید کرد. جهت پارامتر دهی به این جدول، می بایست Sniffer طراحی شده در نرم افزار را فعال ساخته و شبکه خود را جهت استفادهٔ میزبانان اسکن کنید.



شکل ۵. محیط Sniffer نرم افزار

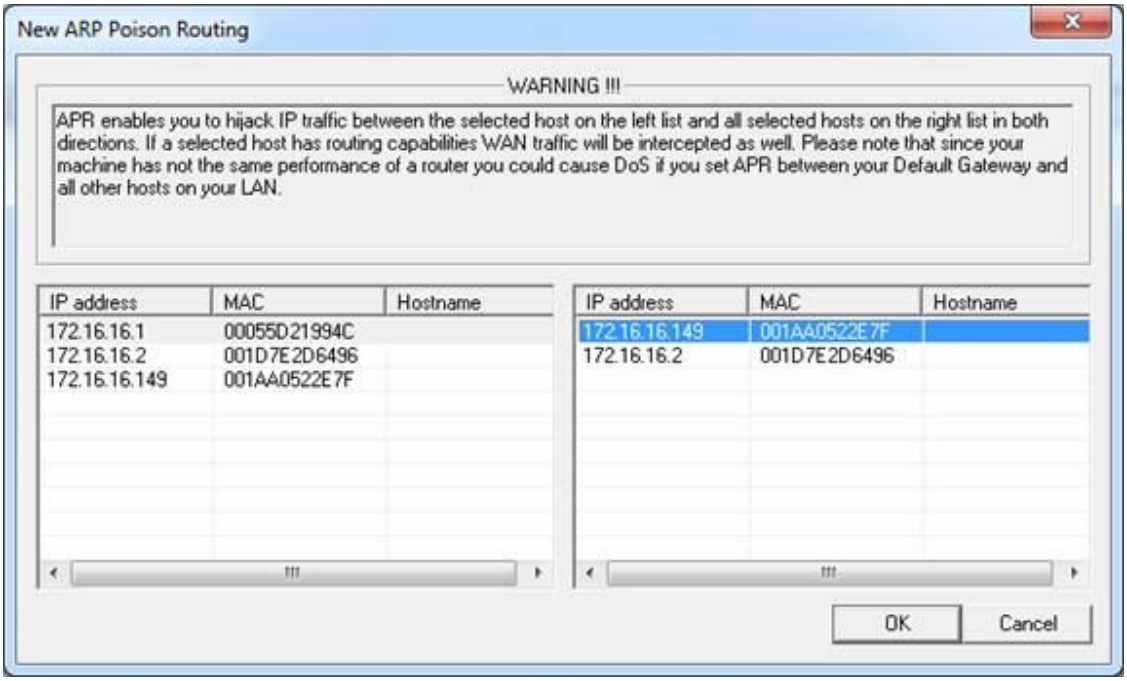
بر روی آیکون دوم در جعبه ابزار نرم افزار کلیک کنید. این آیکون شبیه یک کارت شبکه است. هنگامیکه برای اولین بار بر روی این آیکون کلیک می کنید، از شما خواسته می شود که ترمینالی را که قصد دارید تجسس دارید مشخص نمایید .شما باید ترمینالی را مشخص کنید که به همان شبکه ای متصل است که قصد مسموم سازی آن را دارید. پس از مشخص نمودن ترمینال اتصالی به شبکه، بر روی OK کلیک کنید تا ابزار تجسّسی برنامه فعال گردد. در این زمان می بایست آیکون جعبه ابزار که شبیه یک کارت شبکه است فشرده شده باشد. در صورتیکه این آیکون در وضعیت فشرده شده نباشد، با کلیک بر روی آن، بصورت دستی این آیکون را در وضعیت فشرده قرار دهید. جهت ساختن لیستی از میزبانان موجود در شبکهٔ شما، بر روی آیکون شبیه علامت بعلاوه (+) در جعبه ابزار اصلی کلیک کرده ،سپس بر روی OK کلیک کنید.




شکل ۶. جستجوی شبکه برای پیدا کردن میزبانان

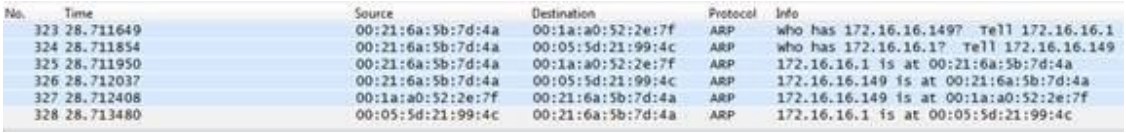
آن جدول که زمانی خالی از پارامتر بود، اکنون می بایست با اطلاعاتی شامل لیست تمامی میزبانان در شبکه به همراه آدرس های MAC و IP آنان و مشخصات ارائه کننده خدمات شبکهٔ میزبانان، پر شده باشد. این همان جدولی است که شما را براساس اطلاعات آن، مسموم سازی حافظهٔ کش ARP انجام می دهید. در پایین پنجرهٔ نرم افزار، شما شاهد سری دگمه هایی می باشید که در صورت کلیک روی آنها ، شما تحت عنوان Sniffer (جاسوس) به پنجره های دیگری هدایت می شوید. حال که شما لیستی از میزبانان تهیه نموده اید، می توانید در محیط APR مشغول به فعالیت شوید.

در هنگام فعالیت در پنجرهٔ APR ، دو جدول خالی به شما نشان داده می شود : جدول بالایی و جدول پاینی. با نصب این جداول، جدول بالایی لیست دستگاه هایی که در روند مسموم سازی نقش دارند را نشان می دهد، جدول پایینی تمامی ارتباطات بین کامپیوتر های مسموم شده توسط شما را نشان می دهد. جهت ادامهٔ مسموم سازی، بر روی آیکون شبیه علامت بعلاوه (+) در قسمت جعبه ابزار استاندارد کلیک کنید. پنجرهٔ باز شده، دارای دو ستون کنار هم می باشد. لیست میزبانان موجود در شبکه در ستون چپی قابل رؤیت است. بر روی آدرس IP یکی از قربانیان خود کلیک کنید. این عمل باعث می شود که لیست تمامی میزبانان موجود در شبکه در ستون سمت راستی به نمایش درآمده و آدرسIP انتخاب شده، حذف گردد. بر روی آدرس IP دیگر قربانی در ستون سمت راستی کلیک کرده سپس بر روی OK کلیک کنید.




شکل ۷. انتخاب قربانی ها جهت شروع عملیات مسموم سازی

اکنون می بایست آدرس های IP هر دو کامپیوتر که در جدول بالایی نوشته شده اند قابل رؤیت باشد. جهت تکمیل فرایند مسموم سازی، بر روی نمادی که به شکل اشعهٔ زرد و مشکی در جعبهٔ ابزار وجود داردکلیک نمایید. این عمل باعث فعال سازی امکانات ویژهٔ نرم افزار مسموم سازی می گردد و سیستم آنالیز کنندهٔ شما را قادر می سازد که به عنوان شخص میانی در تمامی ارتباطات دو قربانی عمل کند. در صورتیکه کنجکاو به استراق سمع جریانات پشت پرده باشید، می توانید نرم افزار Wireshark را نصب کرده و هنگام فعال کردن مسموم سازی، اطلاعات رد و بدل شده از ترمینال را مشاهده کنید. در صورت استفاده از این نرم افزار، شما نظاره گر حجم بالایی از اطلاعات ARP که با سرعت بالایی بین دو قربانی ردوبدل می شوند خواهید بود و بلافاصله می توانید ارتباط بین آنها را مشاهده کنید.




شکل ۸. تزریق ترافیک ARP

پس از اتمام کارکافیست دوباره بر روی نمادی که به شکل اشعهٔ زرد و مشکی است کلیک کنید تا به عملیات مسموم سازی حافظهٔ کش ARP خاتمه دهید.

## روش های مقابله در برابر مسموم سازی حافظهٔ کش ARP:

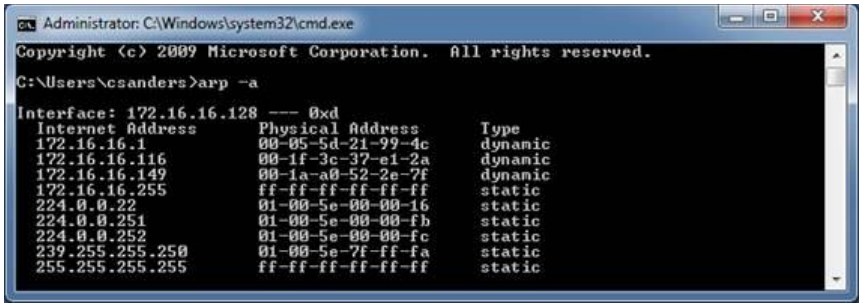
با مشاهدهٔ روش مسموم سازی از دید مقابله کنندگان با این روش در میابیم که قربانیان در شرایط نا مساعدی نسبت به حمله کنندگان قرار دارند. فرایند مسموم سازی ARP در خفا انجام شده و امکان کنترل مستقیم آن توسط ما محدود می باشد. روشی کلی برای مقابله با این حملات وجود ندارد اما در صورت نگرانی از مورد حمله واقع شدن، می توان توسط برخی از اقدامات پیشگیری کننده و واکنشی با این حملات مقابله کرد.

### محافظت از LAN (شبکه محلی):

در یک شبکه محلی، تنها تا زمانی می توان از روش مسموم سازی جهت حمله استفاده کرد که تبادل اطلاعات بین دو قربانی برقرار باشد. با توجه به این موضوع، در یک شبکهٔ محلی، در صورت وقوع یکی از موارد زیر باید نگران امنیت سیستم خود شوید: اگر یک دستگاه در شبکه مورد حمله قرار گرفته باشد، یک کاربر معتمد قصد حمله داشته باشد یا شخصی قصد نصب یک سیستم غیرمطمئن در شبکه را داشته باشد. اگرچه ما اغلب بر حفظ امنیت فضای شبکه تمرکز داریم، ولی با مقابله برابر تهدیدات داخلی و با داشتن وضعیت امنیتی مناسب، می توانیم به از بین بردن نگرانی ها درباره حملات ذکر شده در این مقالات کمک کنیم.

### کدگذاری حافظهٔ کش APR:

یکی از راه های مقابله در برابر طبیعت ناامن و پویای دسته های درخواستی و پاسخیARP، کاهش خاصیت دینامیکی عملکرد این دسته ها می باشد. این روش را می توان به عنوان یک را حل مفید در نظر گرفت زیرا میزبانانی که از سیستم عامل ویندوز استفاده می کنند، اجازه ورود داده های اضافی استاتیک را به حافظهٔ کش خود می دهند. شما می توانید با گشودن یک صفحهٔ دستور و تایپ فرمان arp-a ، حافظهٔ کش ARP ویندوز یک میزبان را مشاهده کنید.




شکل ۹. مشاهده حافظه کش ARP

شما می توانید توسط دستور زیر، ورودی های جدید را به لیست خود اضافه نمایید :

arp –s <IP ADDRESS> <MAC ADDRESS>

در صورتیکه ساختار شبکه شما خیلی به ندرت تغییر می کند، قادر خواهید بود که لیستی از ورودی های استاتیک ARP تهیه کرده و این ورودی ها را توسط متون کامپیوتری اتوماتیک به میزبان ارسال کنید. این اقدام سبب می گردد تا از این موضوع اطمینان حاصل گردد که کامپیوتر های شبکه بجای اعتماد به دسته های درخواستی و پاسخی ARP، همیشه براساس حافظهٔ کش محلی ARP خود عمل می کنند.

## ثبت اطلاعات تبادل شدهٔ ARP توسط یک برنامه ثالث:

آخرین روش مقابله در برابر مسموم سازی حافظهٔ کش ARP، استفاده از یک راه حل واکنشی می باشد. این راه حل، شامل ثبت اطلاعات تبادل شده توسط میزبانان در شبکه می باشد. استفاده از این روش توسط چند سیستم نفوذ یاب مختلف (مانند Snort) یا توسط ابزارهای قابل دانلودی که صرفاً جهت نیل به این هدف طراحی شده اند(مانند xARP) امکان پذیر می باشد. استفاده از این راه حل هنگام تعامل با یک میزبان در شبکه به راحتی امکان پذیر می باشد ولی در صورت مواجه بودن با تمامی بخش های شبکه، بکارگیری این روش کمی دشوار می باشد.

## فریب DNS:

فریب دادن DNS، نوعی دیگر از حملات شخص میانی (MITM) می باشد. توسط این روش، شخص حمله کننده قادر است اطلاعات DNS نادرستی برای کامپیوتر میزبان (کامپیوتر قربانی) ایجاد نماید. بنابراین، زمانیکه شخص قربانی تصمیم دارد وارد سایتی مانند www.bankofamerica.com با آدرس IP : XXX.XX.XX.XX گردد، این شخص در واقع به سایت جعلی و ساختگی www.bankofamerica.com با آدرس IP : YYY.YY.YY.YY فرستاده می شود. این سایت جعلی توسط شخص حمله کننده ساخته شده و هدف این شخص، دزدی اعتبارات بانکی آنلاین و اطلاعات حساب شخص قربانی است، اجرای چنین حمله ای براحتی امکانپذیر است.

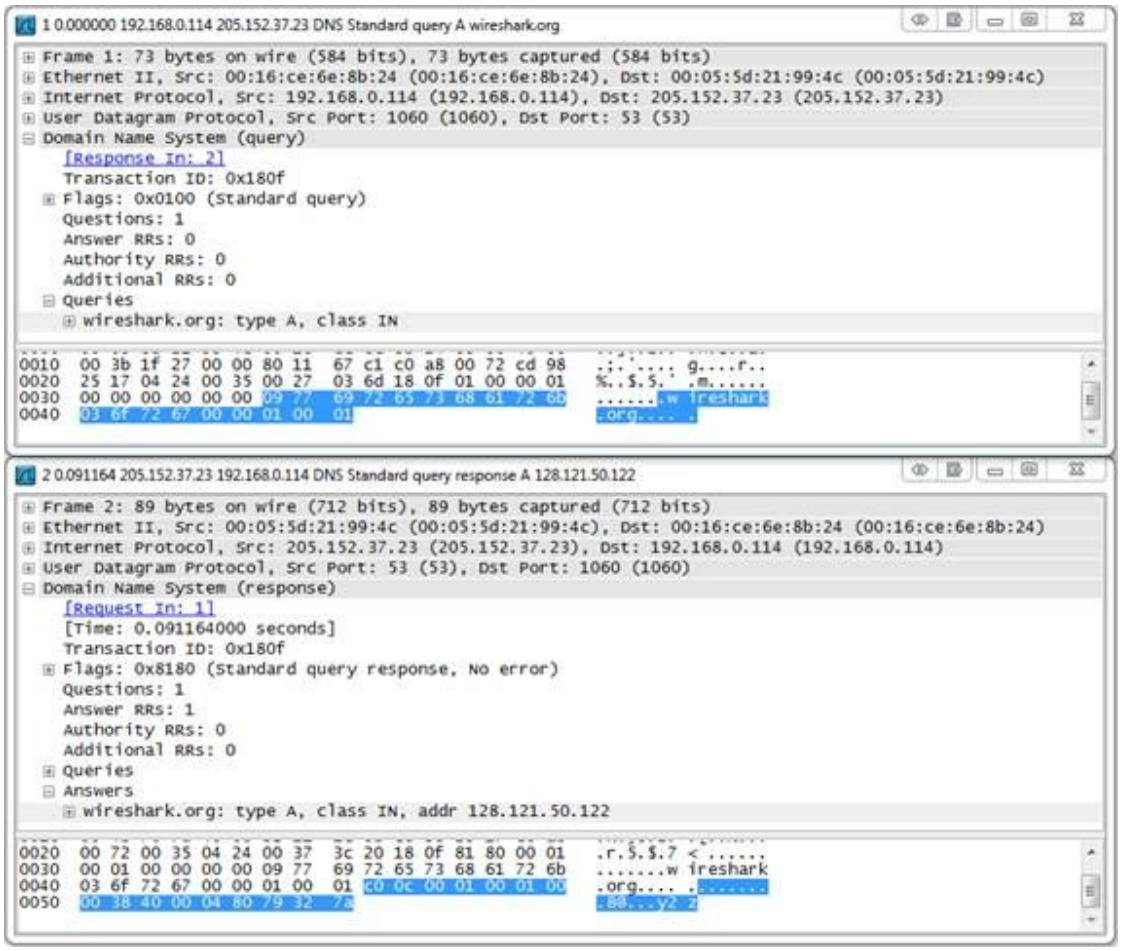
## ارتباط معمول DNS:

طبق تعریف ارائه شده در RFC 1034/1035، پروتکل ""سیستم نامگذاری وب سایت"" یا DNS، مهمترین پروتکل مورد استفاده توسط اینترنت می باشد. زیرا وجود DNS در اینترنت باعث می گردد که به قول معروف:'آجر روی آجر بند شود'. بطور خلاصه می توان گفت هرگاه شما آدرسی مانند http://www.google.com را در صفحهٔ مرورگر تایپ می کنید تا وارد آن سایت شوید، یک درخواست DNS به سرور DNS ارسال می شود تا کامپیوتر شما آدرس IP آن سایت را بدست آورد. به همین علت است که دستگاه های ایجاد کنندهٔ ارتباطات اینترنتی، آدرسی مانند google.com را تشخیص نمی‌دهند. این دستگاه ها، تنها با آدرس IP وب سایت ها (مانند 74.125.95.103) آشنا بوده و براساس آدرس های IP قادر به فعالیت هستند.

مراحل عملکرد یک سرور DNS به این ترتیب می باشد: ذخیرهٔ اطلاعات ورودی مربوط به آدرس های IP (اطلاعات مرجع) در سیستم نامگذاری DNS، تبادل این اطلاعات با کامپیوتر کاربران و تبادل این اطلاعات با سرور های DNS دیگر. ساختار یک سرور DNS در ارتباطات اینترنتی یا بین شرکت ها می تواند تاحدودی پیچیده باشد.


شکل ۱۰. درخواست و پاسخ DNS

پروتکل DNS به صورت درخواستی/ پاسخی عمل می کند. کاربری که قصد دارد وارد وب سایتی با DNS و IP مشخصی گردد، ابتدا درخواستی را به سرور DNS ارسال می کند. سپس، سرور اطلاعات درخواست شده را برای آن کاربر ارسال می نماید. از دیدگاه یک کاربر، تنها همین دو دستهٔ درخواستی و پاسخی در این فرایند وجود دارند.




شکل ۱۱. بسته های درخواست و پاسخ DNS

با در نظر گرفتن ارتباطات موجود بین سرور های DNS، فرایند ارسال دسته های درخواستی و پاسخی کمی پیچیده تر می گردد. عملکرد سلسله مراتبی DNS دراینترنت سبب می گردد تا سرور های DNS برای ارسال دستهٔ پاسخی به کاربر، ناچار به ارتباط با یکدیگرگردند. از این گذشته، شاید بتوان از یک سرور DNS داخلی انتظار داشت که نام سرور محلی اینترانت با IP مشخص را بداند، ولی مسلماً نمی توان از چنین سروری انتظار داشت که آدرس های IP مربوط به سایت هایی مانند Google یا Dell را تشخیص دهد. به همین جهت است که ارتباط بین سرور های DNS نقش مهمی در این فرایند بازی می کنند. ارتباط بین سرور های DNS، از طریق ارسال یک دستهٔ پاسخی از یک سرور (از طرف کاربر) به سرور دیگر انجام می گردد. در حقیقت، در این فرایند یک سرور نقش کاربر را بازی می کند (مطابق شکل ۱۲).


شکل ۱۲. ارسال درخواست و پاسخ از مشتری به سرور و از سروری به سرور دیگر

## فریب دادن DNS:

همانطور که به روش های مختلفی می توان صدای یک گربه را تقلید کرد، می توان از روش های متعددی نیز جهت اجرای حمله از نوع ""فریب DNS"" استفاده نمود. ما از روش ""فریب دادن شناسهٔ DNS"" جهت حمله استفاده می کنیم.

هر دستهٔ درخواستی DNS که در شبکه ارسال می شود، دارای شمارهٔ شناسهٔ منحصر به فردی می باشد. این شناسه، جهت امکان شناسایی و متصل نمودن دسته های درخواستی و پاسخی بکار می رود. بنابراین، اگر کامپیوتر حمله کننده قادر به دریافت درخواست DNS ارسال شده از کامپیوتر قربانی باشد، آنگاه کافیست شخص حمله کننده یک دستهٔ پاسخی جعلی که شامل این شناسه باشد بسازد و به کامپیوتر قربانی ارسال کند.

این حمله، با استفاده از یک نرم افزار و توسط اجرای دو مرحله روبرو انجام می گیرد: ابتدا، ما اقدام به مسموم سازی حافظهٔ کش ARP کامپیوتر قربانی نموده تا قادر شویم اطلاعات مبادله شده توسط آن کامپیوتر را منحرف ساخته و در نتیجه دستهٔ درخواستی DNS ارسالی از آن کامپیوتر را دریافت کنیم. سپس، دستهٔ پاسخی جعلی را به کامپیوتر قربانی ارسال می کنیم. هدف از این فرایند این است که کابران (قربانیان) بجای ورود به سایتی که مد نظرشان است، به وب سایت جعلی ما وارد شوند تا ما به اهداف شوم خود برسیم. نمونه ای از این حمله در شکل ۱۳ آمده است.


شکل ۱۳. حمله به روش فریب DNS با استفاده از فریب شناسه DNS

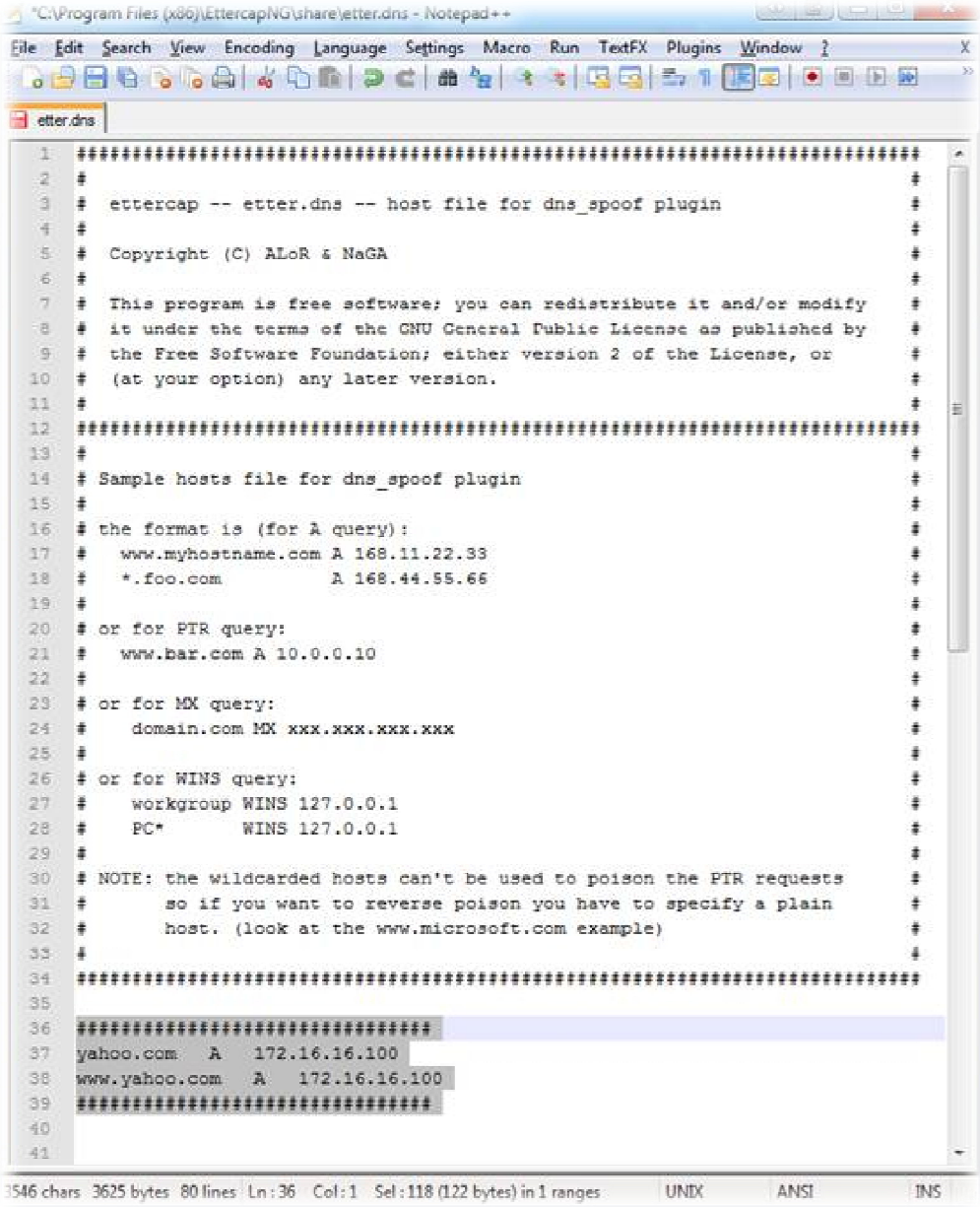
نرم افزار های مختلفی جهت اجرای حمله به روش ""فریب DNS"" وجود دارند. ما از نرم افزار Ettercap به این منظور استفاده می کنیم. این نرم افزار دارای نسخه های قابل اجرا در Windows و Linux می باشد. با تحقیق دربارۀ نرم افزار Ettercap در این وب سایت متوجه می شوید که این نرم افزار دارای قابلیت هایی فراتر از انجام""فریب DNS""بوده و در اکثر حملات شخص میانی (MITM) مورد استفاده قرار می گیرد.

اگر نرم افزار Ettercap را تحت سیستم عامل ویندوز نصب کنید، متوجه می شوید که این نرم افزار دارای یک GUI است، که بخوبی کار می کند. اما در این مثال، ما از ترمینال command-line جهت اجرای حمله استفاده می کنیم. قبل از اجرای نرم افزار Ettercap، نیاز به پیکربندی و انجام برخی تنظیمات می باشد. این نرم افزار در اصل یک وسیلۀ تجسس می باشد که از plug-in های (دوشاخه های) مختلف جهت اجرای حمله استفاده می کند. از آنجاییکه در این مثال، plug-in مربوط به dns_spoof حمله را اجرا می نماید، ما باید پیکر بندی فایل مربوط به این plug-in را اصلاح کنیم. در صورت کار با سیستم عامل ویندوز، این فایل می تواند در آدرس های زیر ذخیره شود:

C:\Program Files (x86)\EttercapNG\share\etter.dns

/usr/share/ettercap/etter.dns

این فایل بسیار ساده بوده و حاوی اطلاعات DNS مورد استفاده در روش ""فریب DNS"" می باشد. هدف ما این است که هر کاربری را که قصد وارد شدن به سایت yahoo.com دارد، به یک سایت میزبان در شبکۀ محلی هدایت و منتقل کنیم تا بتوانیم ورودی مشخص شده در شکل ۱۴ را اضافه نماییم.




شکل ۱۴. اضافه کردن یک ورودی مربوط به DNS فریب داده شده به etter.dns

اساس عملکرد این ورودی ها به اینصورت است: این ورودی ها به plug-in مربوط به dns_spoof دستور می دهند که در صورت مشاهدهٔ یک دستهٔ درخواستی DNS برای yahoo.com یا www.yahoo.com (اطلاعات مرجع کلاس A)، یک دستهٔ پاسخی با آدرس IP : 172.16.16.100 تولید کنند. سپس، کامپیوتر موجود در این آدرس IP، یک سایت جعلی را در معرض نمایش کامپیوتر قربانی می گذارد.

به محض اینکه عملیات پیکربندی فایل به اتمام رسید و این فایل ذخیره شد، ما قادر هستیم دستور اجرایی را صادر نموده و حمله را آغاز کنیم. از موارد زیر برای صدور دستور اجرایی می توان استفاده نمود:

-T کاربرد ترمینال متنی را نشان می دهد

-Q دستورات را در حالت بی سر و صدا اجرا می کند تا دسته های دریافتی به نمایش در نیایند

-P dns_spoof نشان دهنده ی کاربر پلاگین مربوط به آن است

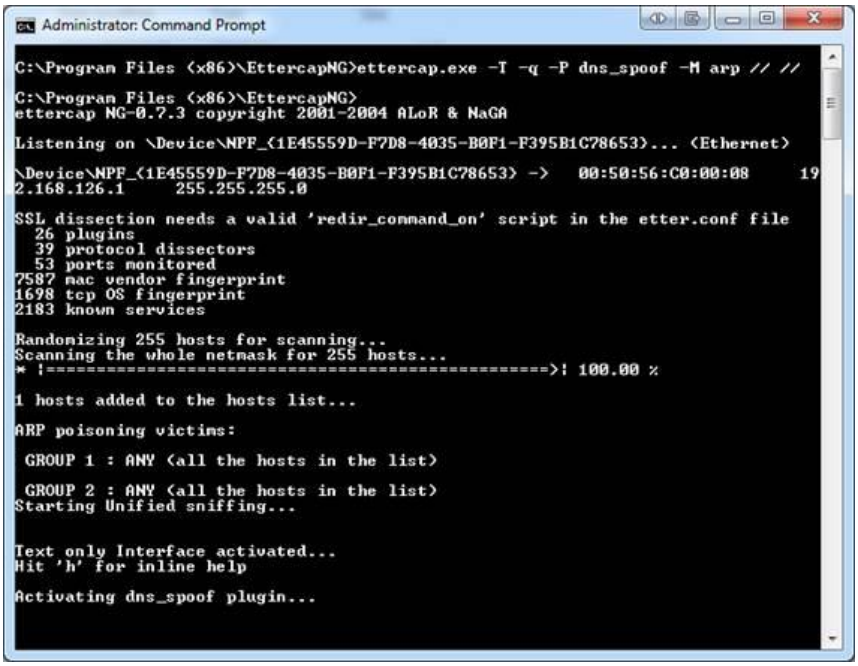
و همچنین دستور M arp– باعث انجام یک حملهٔ ""شخص میانی"" از نوع ""مسموم سازی حافظهٔ کش ARP"" می گردد و در نتیجه امکان دریافت و مشاهدهٔ اطلاعات ردو بدل شده بین قربانی‌ان را فراهم می سازد.

-// // کل شبکه را به عنوان هدف حمله تعیین می کند

دستور زیر، آخرین دستور اجرایی در حملهٔ ما خواهد بود:

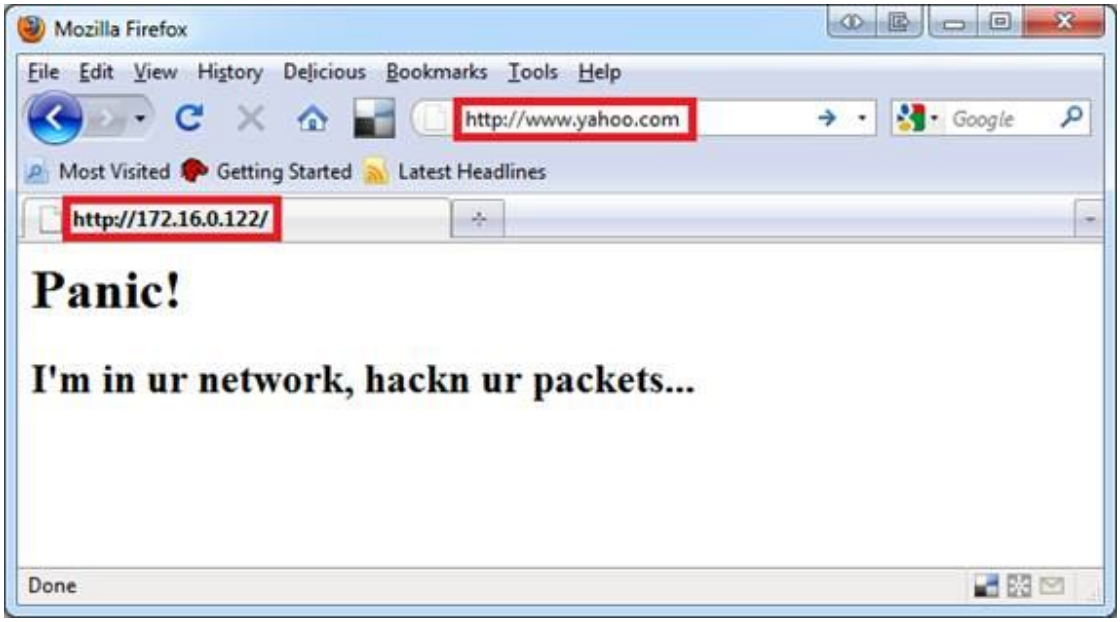
Ettercap.exe –T –q –P dns_spoof –M arp // //

با اجرای دستورات بالا، حمله در دو مرحله انجام می شود: ۱- مسموم سازی حافظهٔ کش ARP کامپی‌وتر قربانیان در شبکه و ۲- انتقال دستهٔ پاسخی جعلی به کامپیوتر قربانیان.




شکل ۱۵. نرم افزار Ettercap دائماً در حال دریافت دسته های درخواستی DNS می باشد

پس از اجرای این دستورات و آغاز حمله، هرکس که قصد ورود به سایت www.yahoo.com را داشته باشد، به سایت جعلی ما هدایت خواهد شد (شکل ۱۶).




شکل ۱۶. نتیجه یک حمله از نوع فریب DNS از دیدگاه قربانی

## روش مقابله در برابر حملات DNS:

از آنجای که این نوع حمله دارای طبیعتی واکنشی می باشد، مقابله در برابر آن بسیار سخت است. قاعدتاً تا زمانیکه شما بطور کامل قربانی این حمله نشده اید، از فریب خوردن DNS خود بی اطلاع باقی می مانید. در صورت انجام چنین حمله ای، شما با وب سایتی مواجه می شوید که کمی با آنچه انتظار داشتید تفاوت دارد. در حملاتی که بطور کامل سازمان دهی شده اند، ممکن است که حتی شما متوجه نشوید که اطلاعات حساب بانکی خود را در یک سایت جعلی وارد کرده اید، تا اینکه از طرف بانک با شما تماس بگیرند و از شما در خصوص کشتی تازه خریداری نموده در سواحل یونان سوال کنند. با این وجود، هنوز اقدامات دفاعی دیگری نیز برای مقابله با این حمله وجود دارند:

کامپیوترهای موجود در شبکهٔ خود را ایمن سازید: چنین حملاتی در اغلب موارد از داخل شبکه صورت می گیرد. اگر کامپیوترهای شبکه شما ایمن باشند، آنگاه احتمال کمتری وجود دارد تا از این کامپیوترها جهت انجام حمله به شما استفاده شود.

به ایمنی DNS اطمینان نکنید: سیستم های مرورگر اینترنت که از حساسیت و ایمنی بالایی برخوردارند، از DNS در عملکرد خود استفاده نمی کنند. شما معمولاً از چنین مرورگرهایی استفاده نمی کنید ولی اگر از نرم افزاری استفاده می نمایید که در عملکرد خود از نام میزبانان در شبکه استفاده می کند، نام این میزبانان را بصورت دستی در فایل میزبانان ذخیره کنید.

از IDS استفاده کنید: در صورت نصب و استفادهٔ صحیح از سیستم تشخیص نفوذ (IDS)، می توان با اکثر حملات ""مسموم سازی حافظهٔ کش ARP"" و ""فریب DNS""مقابله نمود.

از DNSSEC استفاده کنید: DNSSEC نسخهٔ جدید DNS می باشد که از اطلاعات DNS که دارای امضای دیجیتالی می باشند جهت اطمینان از واقعی بودن دسته های پاسخی استفاده می کند. این سیستم هنوز بطور گسترده مورد استفاده قرار نگرفته است ولی به عنوان ""DNS آینده"" مورد قبول همگان قرار گرفته است. این سیستم تا حدی مورد اطمینان می باشد که DOD آمریکا دستور داده است که تمامی وب سایت هایی که دارای پسوند MIL و GOV در آدرس خود هستند می بایست حداکثر تا یک سال دیگر استفاده از DNSSEC را آغاز نموده باشند.

## ربودن جلسه (Session Hijacking):

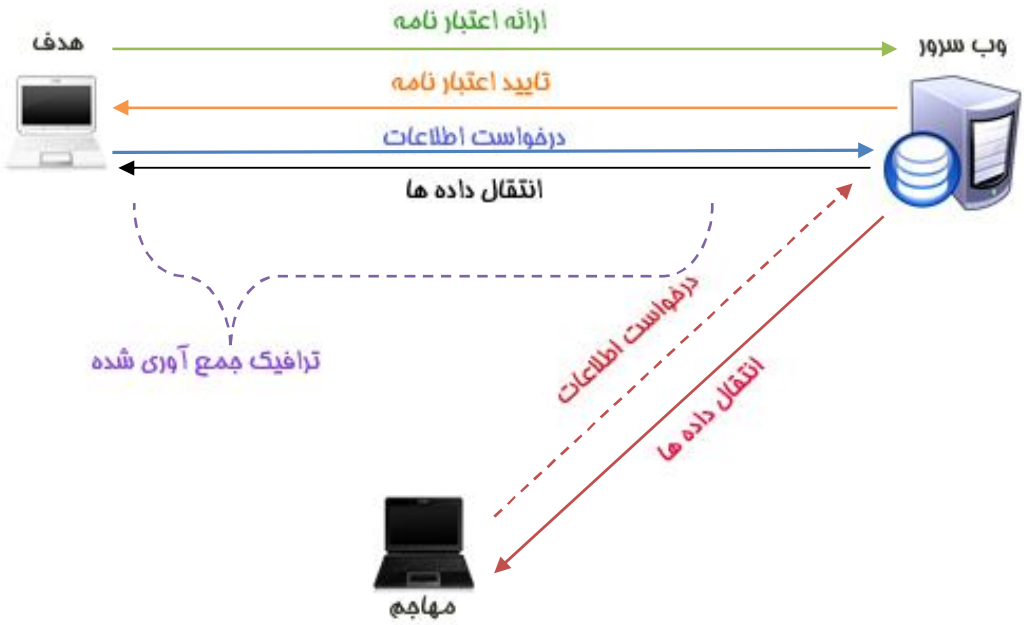
اصطلاح ""ربودن جلسه""، هر از چند گاهی به گوش ما می رسد. این روش، از روش های مختلفی شکل گرفته است. بطور کلی می توان گفت که هر نوع حمله ای که از جلسه و ارتباط جاری بین دو کامپیوتر (قربانی) سوء استفاده نماید، نوعی ""ربودن جلسه"" محسوب می شود. منظور از ""جلسه""، ارتباطی است که در آن اطلاعات رد و بدل می گردد.
به عبارت دیگر، یک جلسه، ارتباطی است که جهت شکل گیری آن، دو کامپیوتر به هم متصل شده، ارتباط برقرار شده و می بایست مراحل مشخصی برای قطع ارتباط انجام پذیرد. اگر از لحاظ تئوری به واژهٔ ""جلسه"" نگاه کنیم، این واژه کمی نامفهوم به نظر می رسد، پس شاید بهتر باشد این واژه را از دیدگاه عملی مورد بررسی قرار دهیم.

در این مقاله، به بررسی روش ""ربودن جلسه"" توسط دزدی cookie ها می پردازیم. در این روش، جلسات HTTP مورد استفاده قرار می گیرند. وب سایت هایی که برای ورود به آنها به username و password نیاز است، مثال های خوبی از ارتباطات جلسه ای هستند. برای برقراری چنین جلسه ای، ابتدا لازم است شما توسط آن وب سایت معتبر شناخته شوید (از طریق usernameو password)، در هنگام برقراری جلسه، آن وب سایت از طریق cookie ها، اتصال دائم شما به وب سایت را چک می کند تا مجوز دسترسی به منابع موجود در آن سایت را برای شما صادر کند. درهنگام پایان جلسه (خروج از وب سایت)، username و password شما پاک شده و جلسه به پایان می رسد. این تنها یک مثال از ارتباطات جلسه ای می باشد. در هنگام فعالیت ما در اینترنت، جلسات بسیاری شکل می گیرند بدون اینکه ما از آنها اطلاعی داشته باشیم و اکثر ارتباطات در اینترنت بر پایهٔ شکل گیری این جلسات انجام می پذیرد.


شکل ۱۷. یک جلسه عادی

همانطور که در حمله از نوع ""فریب DNS "" مشاهده نمودید، اطلاعات رد و بدل شده در اینترنت در امنیت کامل نمی باشند، ارتباطات شکل گرفته در جلسات نیز از این قاعده مستثنی نیستند. قاعدهٔ کلی حملات از نوع ""ربودن جلسه"" این است که اگر شما بتوانید قسمتی از اطلاعات ردوبدل شده در یک جلسه را دریافت کنید، آنگاه قادر خواهید بود که توسط این اطلاعات، خود را بجای یکی از طرفین این جلسه معرفی کنید و در نتیجه به سایر اطلاعات آن جلسه نیز دسترسی

پیدا کنید. در مورد مثال قبلی، می توان گفت که اگر ما قادر به دریافت cookie های مورد استفاده در ایجاد جلسه بین مرورگر و وب سایت مورد نظر گردیم، آنگاه قادر خواهیم بود این cookie ها را به سرور ارائه دهیم و خود را بجای شخص دیگری جا بزنیم. با اینکه ممکن است یک شخص حمله کننده باور نکند که چنین روش آسانی برای حمله وجود دارد، اما چنین حمله ای واقعاً به همین آسانی صورت می گیرد.




شکل ۱۸. ربودن جلسه

اکنون که از تئوری مورد استفاده در این روش اطلاع پیدا نمودیم، به ارائهٔ مثال های عملی می پردازیم.

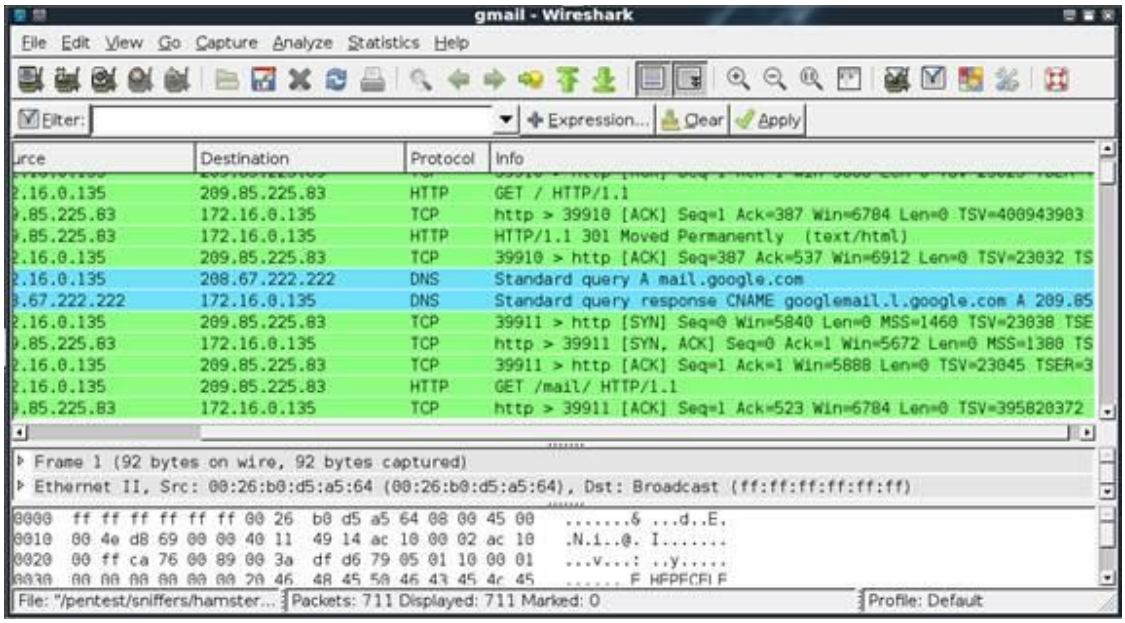
## ربودن cookie ها توسط نرم افزارهای Hamster و Ferret :

در این مثال عملی، به بررسی حملهٔ ""ربودن جلسه"" از طریق ربودن اطلاعات شخصی که در حال دسترسی به آدرس Gmail خود است، می پردازیم. ما با استفاده از این اطلاعات قادر خواهیم بود که خود را بجای آن شخص جا بزنیم و از کامپیوتر خودمان به آدرس Gmail او دسترسی پیدا کنیم.

ما از دو نرم افزار Hamster و Ferret جهت اجرای این حمله استفاده می کنیم.. هر دوی این نرم افزار ها از نوع command-line می باشند تا فولدر Hamster در جایی در کامپیوتر که براحتی قابل دسترسی باشد ذخیره شود.

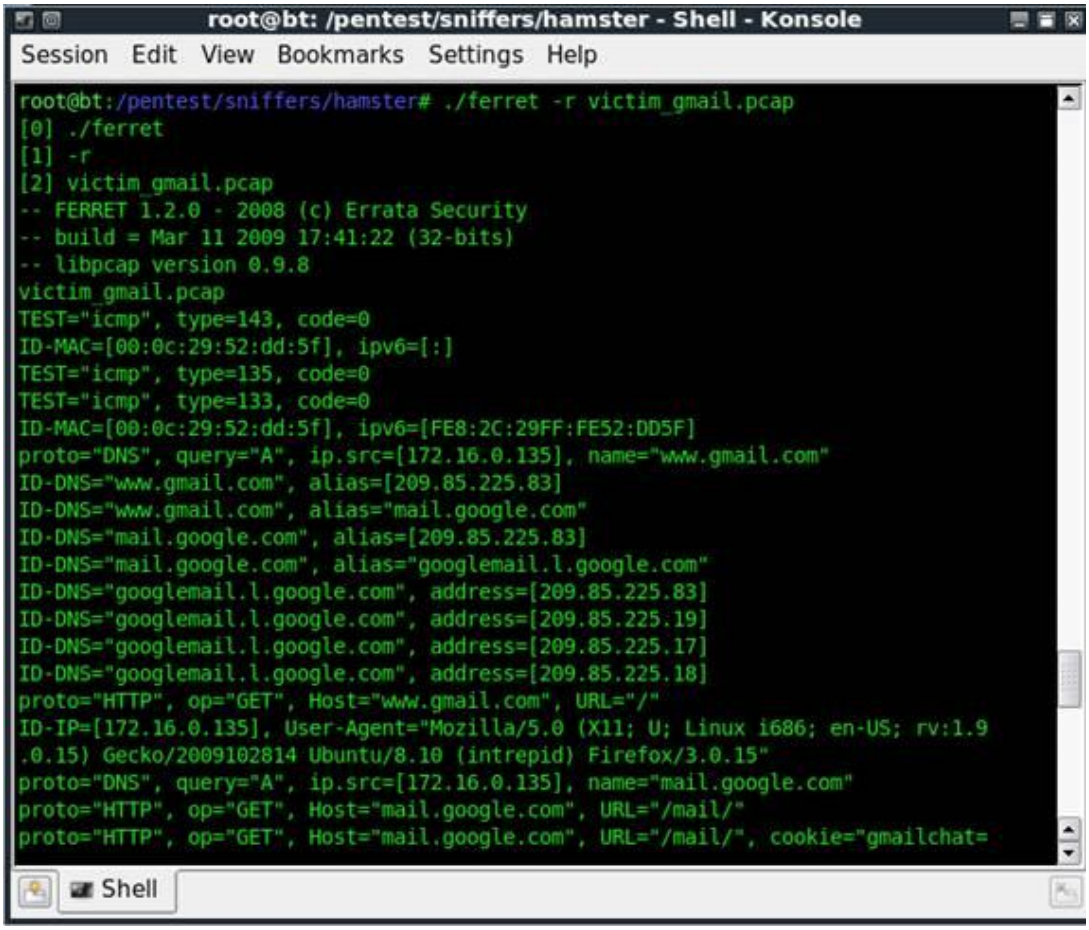
همچنین، شما می توانید برای انجام این حمله، برنامهٔ Backtrack4 را دانلود و اجرا نمایید. این برنامه (BT4)، از محصولات Linux بوده و صرفاً جهت تست و آزمایش هک کردن کامپیوترها تولید شده است. این برنامه حاوی بسیاری از نرم افزارهای از پیش نصب شده بر کامپیوتر از قبیل Hamster و Ferret می باشد. پس از نصب این برنامه، شما می توانید فایل Hamster را در فولدر /pentest/sniffers/hamster بیابید.

اولین قدم در اجرای این نوع حمله از حملات ""ربودن جلسه""، این است که هنگامیکه شخص قربانی تصمیم دارد وارد سایت Facebook شود، اطلاعات مبادله شده توسط او را برباییم. امکان دزدی این اطلاعات توسط هر نرم افزار تجسسی از قبیل TCPDump یا Wireshark امکان پذیر است، اما برای ربودن دسته های اطلاعاتی مناسب، می بایست از روش مسموم سازی حافظهٔ کش ARP استفاده کنیم .



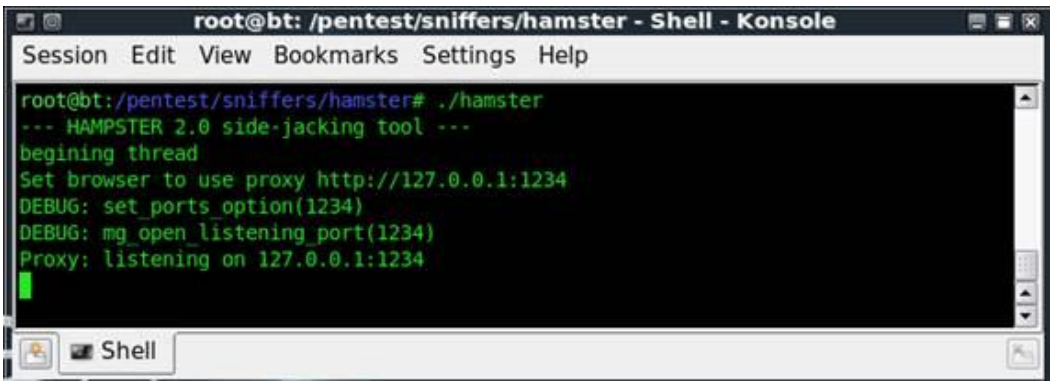

شکل ۱۹. ربودن اطلاعات شخصی که قصد ورود به Gmail خود را دارد

زمانیکه اطلاعات شخصی که می خواهد وارد Gmail خود بشود را ربودید، می بایست آن فایل اطلاعات را در دایرکتوری Hamster ذخیره نمایید. ما فایل مورد استفاده در این مثال را victim_gmail.pcap نام می گذاریم. هنگامیکه این فایل در محل مخصوص خود قرار داشته باشد، از نرم افزار Ferret جهت پردازش این فایل استفاده می کنیم. این کار توسط وارد شدن به فایل Hamster و اجرای دستور ferret-r victim_gmail.pcap انجام می گیرد. برنامهٔ ferret فایل مورد نظر را پردازش نموده و یک فایل hamster.txt تولید می کند. فایل تولید شده می تواند توسط برنامهٔ Hamster هنگام اجرای ""ربودن جلسه"" مورد استفاده قرار بگیرد.



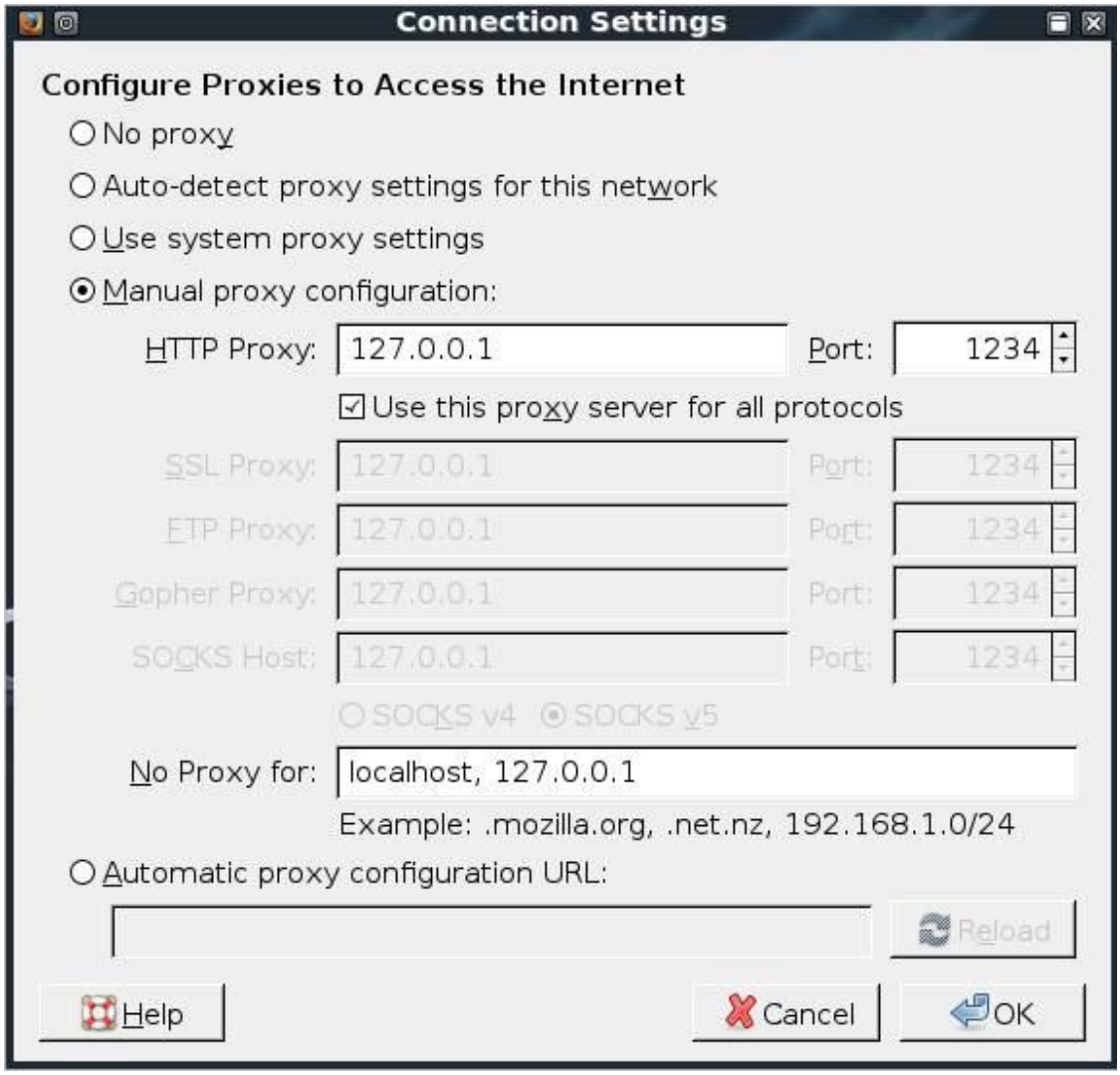

شکل ۲۰. پردازش فایل دزدیده شده توسط Ferret

زمانیکه اطلاعات HTTP را ربوده و در اختیار داشتیم، می توانیم حمله را آغاز کنیم. نرم افزار Hamster، خود همانند یک پراکسی عمل می کند و باعث ایجاد ترمینالی جهت استفاده از cookie ها می گردد. برای اجرای پراکسی Hamster، می توانید این نرم افزار را بدون امکانات و آپشن های command-line اجرا نمایید.




شکل ۲۱. اجرای برنامه Hamster

وقتی این برنامه را اجرا کردید، لازم است تنظیمات پراکسی این نرم افزار را مطابق خروجی های تولیدی توسط برنامهٔ Haster تغییر دهید. به عبارت دیگر، شما می بایست تنظیمات پراکسی خود را طوری تغییر دهید که قادر به استفاده از مسیر برگشتی آدرس 127.0.0.1 در پورت 1234 باشید. می توانید برای تغییر این تنظیمات در Internet Explorer، وارد Tools شده، سپس وارد Internet Options شوید، آنگاه وارد Connections شوید و پس از آن وارد LAN Setting شوید و قسمت Use a proxy server را در LAN box خود تیک بزنید.



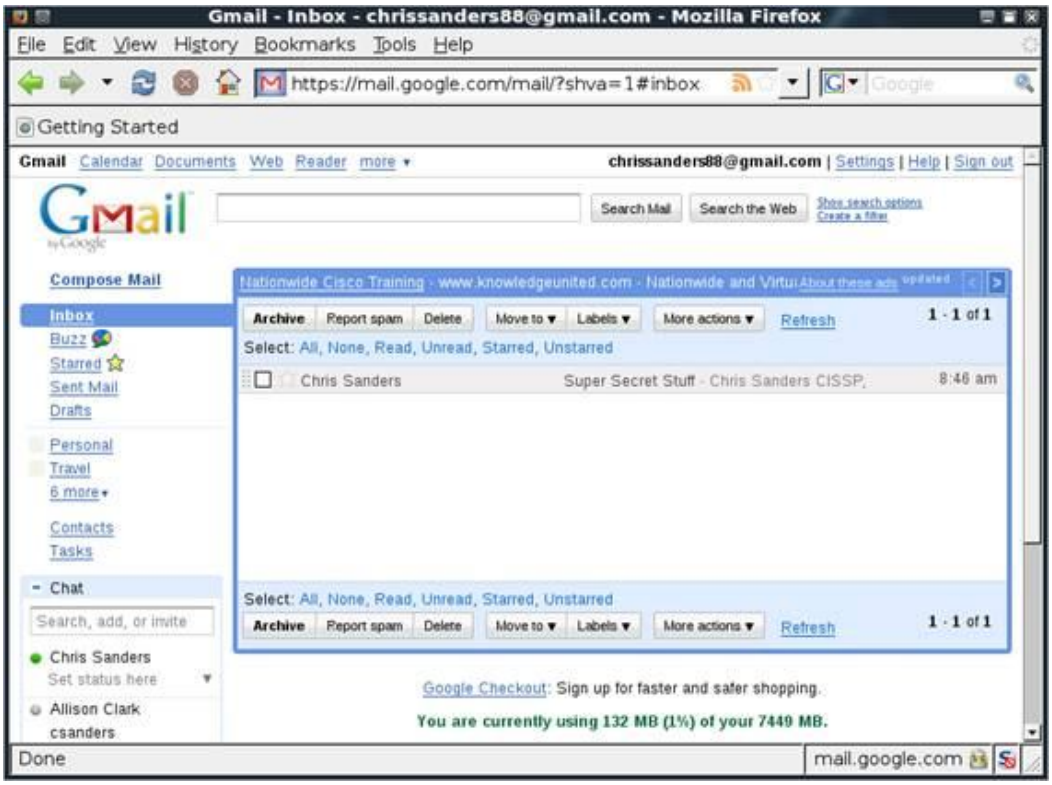

شکل ۲۲. تغییر تنظیمات پراکسی جهت استفاده پراکسی با برنامه Hamster

پس از تغییر تنظیمات پراکسی قادر خواهید بود با رفتن به آدرس http://hamster، به میز فرمان Hamster دسترسی پیدا کنید. نرم افزار Hamster، از فایل تولید شده توسط برنامهٔ Ferret جهت ایجاد لیستی از آدرس های IP مربوط به جلسهٔ دزدیده شده استفاده می کند، سپس این آدرس های IP را در قسمت سمت راست مرورگر نشان می دهد. فایلی

که ما ساخته ایم تنها شامل یک آدرس IP از قربانی می باشد، بنابراین، با کلیک بر روی آن، جلسه های قابل دزدی در قسمت سمت چپ مرورگر به نمایش در می آیند.


شکل۲۳. GUI مربوط به برنامه Hamster

در قسمت سمت چپ مرورگر، مشاهده می شود که آدرس facebook.com نیز در لیست وجود دارد. با کلیک بر روی آن، وارد صفحهٔ جدیدی می شوید که شما را به صفحات facebook قربانیان هدایت می کند.




شکل۲۴. یک آدرس Gmail که با موفقیت دزدیده شده

## مقابله با حملات ""ربودن جلسه"":

از آنجاییکه روش های مختلفی برای انجام حملاتی از نوع ""ربودن جلسه"" وجود دارد، بنابراین روش های مختلفی نیز جهت مقابله با این حملات وجود خواهد داشت. شناسایی و مقابله با حملاتی از نوع ""ربودن جلسه"" دشوار تر از شناسایی و مقابله با سایر حملاتی که تاکنون بررسی نموده ایم می باشد. علت این امر آن است که این نوع حملات، از بیشترین خاصیت واکنشی در برابر شناسایی و مقابله برخوردارند. اگر شخص حمله کننده، عمل شک برانگیزی را در هنگام حمله انجام ندهد، شما هیچگاه از انجام این حمله اطلاع پیدا نخواهید کرد. در زیر، راه هایی جهت مقابلهٔ بهتر با این حملات ذکر شده است:

عملیات بانکی آنلاین را در منزل انجام دهید: احتمال اینکه شخصی در شبکهٔ خانگی شما به تجسس در اطلاعات مبادله شدهٔ شما بپردازد کمتر از آن است که کسی در محل کار شما به انجام این عمل مبادرت کند. علت این امر آن نیست که کامپیوتر خانگی شما امن تر است زیرا کامپیوتر خانگی شما از امنیت کمتری برخوردار است، بلکه علت آنست که اگر شما یک یا دو کامپیوتر در منزل داشته باشید، تنها خطری که شما را تهدید می کند این است که پسر ۱۴ سالهٔ شما کلیپ های آموزش هک کردن را در YouTube دیده باشد. ولی در شبکهٔ کاری، شما از اتفاقات رخ داد در اتاق های دیگر شرکت یا در شعبه های دیگر شرکت در ۲۰۰ مایلی خود خبر ندارید، بنابراین احتمال اینکه حمله ای به کامپیوتر شما صورت گیرد، چند برابر می شود. یکی از اصلی ترین اهداف حملاتی از نوع ""فریب جلسه""، عملیات بانکی آنلاین می باشد. با این وجود، راه های مقابلهٔ ذکر شده در این مقاله، در مورد تمامی اهداف این حملات کاربرد دارد.

هشیار باشید: حمله کنندگان باهوش، اثری از خود در حساب های بانکی شما باقی نمی گذارند، با این وجود، حتی هکر های حرفه ای نیز گاهی دچار اشتباه می شوند. اگر هنگام کار در سایت هایی که بر مبنای تشکیل جلسات عمل می کنند آگاه و هشیار باشید، ممکن است از وجود هکرها مطلع شوید. به مواردی که عجیب به نظر می رسند دقت کنید، همچنین، به ساعت آخرین ورود خود به وب سایت مورد نظر توجه کنید تا مطمئن شوید موضوع غیر عادی وجود ندارد.

کامپیوترهای موجود در شبکهٔ خود را ایمن سازید: مجدداً تکرار می کنم که در اغلب موارد، چنین حملاتی از داخل شبکه صورت می گیرد. اگر کامپیوترهای شبکه شما ایمن باشند، آنگاه احتمال کمتری وجود دارد تا از این کامپیوترها جهت انجام حمله به شما استفاده شود.

## ربودن SSL:

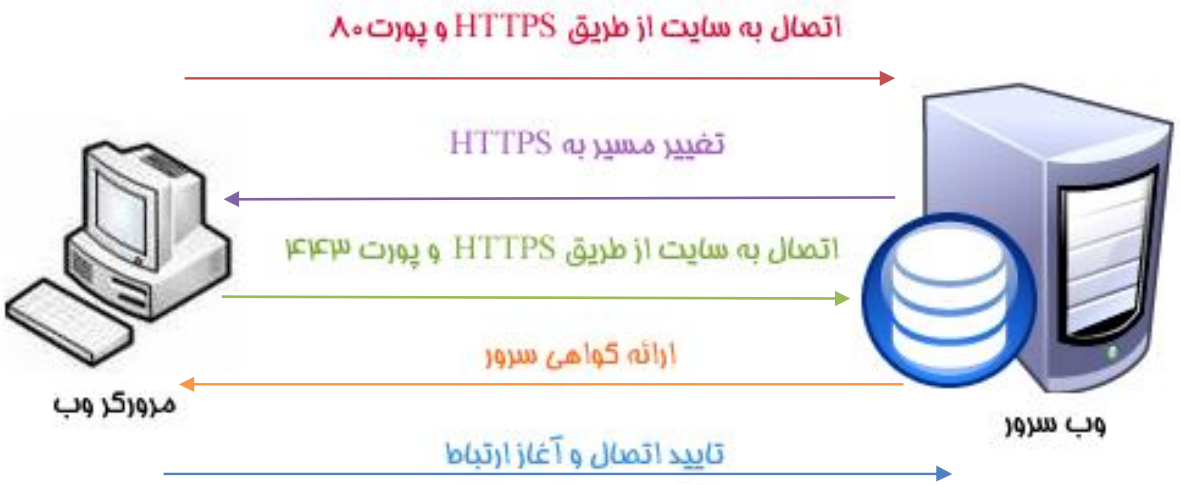
این روش، یکی از قوی ترین حملات شخص میانی محسوب می شود زیرا توسط این روش، امکان سوء استفاده از سرویس ها و خدمات اینترنتی که به گمان مردم امن هستند، فراهم می گردد. این مقاله را با بررسی تئوری های مربوط به ارتباطات SSL آغاز می کنم. همچنین، شرح خواهم داد که چه عللی ایجاد کنندۀ امنیت در این ارتباطات می باشند و پس از آن، نشان خواهم داد که چگونه می توان از این ارتباطات در جهت رسیدن به اهداف شوم خود سوء استفاده کنیم. مطابق همیشه، بخش پایانی این مقاله به روش های شناسایی و مقابله با این نوع حمله اختصاص یافته است.

## SSL و HTTPS:

در مفهوم مدرن، پروتکل تبادل اطلاعات رمز گذاری شده (SSL) یا پروتکل امن انتقال داده (TLS)، پروتکل هایی است که جهت ایجاد امنیت درشبکه طراحی شده اند و توسط رمزگذاری عمل می کنند. در اغلب موارد،این پروتکل بطور مشترک با پروتکل های دیگر (ازقبیل SMTP، IMAPS و HTTPS) عمل می کند تا قادر باشد امنیت را در سرویسی که ارائه میدهد تأمین نماید. هدف نهایی این پروتکل، ایجاد کانالهای امن در شبکه های نا امن می باشد.

با اینکه شما هر روز از HTTPS استفاده می کنید، اما شاید از وجود چنین حملاتی مطلع نگردید. اکثر سرویس های ایمیل و برنامه های آنلاین بانکی از HTTPS جهت اطمینان از رمزدار بودن ارتباطات بین مرورگر شما و خدماتی که این سرویس ها ارائه می دهند استفاده می کنند. اگر HTTPS وجود نداشتند، هرکاربری در شبکه می توانست بوسیلۀ یک برنامۀ تجسس، username و password و اطلاعات مخفی دیگر شما را برباید.

پروسۀ امنیتی مورد استفاده توسط HTTPS ، بر اساس توزیع مجوزهایی بین سرور، کاربر و یک شخص ثالث مورد اطمینان عمل می کند. به عنوان مثال، اگر کاربری قصد ورود به Gmail خود را داشته باشد، می بایست مراحل مشخصی را انجام دهد. این مراحل بطور خلاصه در شکل ۲۵ نشان داده شده است.




شکل ۲۵. پروسه امنیت مورد استفاده در HTTPS

در پروسهٔ نشان داده شده در تصویر بالا، جزئیات عملکرد این پروسه ذکر نشده است. با این وجود، این پروسه شامل مراحل کلی زیر می گردد:

۱. مرورگر کاربر با استفاده از HTTP، به آدرس http://mail.google.com در پورت ۸۰ متصل می شود.
۲. سرور شبکه با استفاده از HTTP code 302، باعث هدایت و انتقال HTTP مورد استفاده توسط کاربر به HTTPS می گردد.
۳. کاربر به آدرس https://mail.google.com در پورت ۴۴۳ متصل می شود.
۴. سرور مجوزی به کاربر ارائه می کند که حاوی امضای دیجیتالی کاربر می باشد. کاربرد این مجوز، اثبات شناسهٔ سایت مورد نظر می باشد.
۵. کاربر این مجوز را دریافت نموده و با دیگر مجوز های صادر شده مقایسه می کند.
۶. ارتباط رمزدار برقرار می گردد.

اگر مراحل بررسی اعتبار این مجوز با شکست روبرو شود، می توان گفت که وب سایت مورد نظر قادر به اثبات شناسهٔ خود نبوده است. در این حالت، پیغام عدم اثبات مجوز برای کاربر صادر می شود. کاربر پس از دریافت این پیغام، می تواند با مسئولیت خود فعالیتش را ادامه دهد، زیرا این احتمال وجود دارد که کاربر در حال تبادل اطلاعات با سایت مورد نظر نباشد.

## شکست HTTPS:

این فرایند تا چند سال پیش بسیارامن و مطمئن شناخته می شد تا اینکه حمله ای انجام گردید که امکان ربودن فرایند ارتباطات را فراهم نمود. این فرایند شامل شکستن SSL نمی گردد بلکه باعث شکستن پل ارتباطی میان ارتباطات رمزدار و غیر رمزی می شود.

آقای Moxie Marlinspike، که در زمینهٔ انجام تحقیقات امنیتی شهرت دارد، این فرضیه را بیان کرده است که یک ارتباط SSL، هیچگاه بصورت مستقیم برقرار نمی شود. به عبارت دیگر، در اغب موارد، یک ارتباط SSL، از طریق HTTP برقرار می شود. علت این امر آن است که کاربران بوسیلهٔ HTTP code 302 به HTTPS هدایت و منتقل می شوند یا اینکه کاربران بر روی لینکی (مانند login) کلیک کرده اند که آنها را به سایت های HTTP منتقل می نماید. این ایده بر این اساس شکل گرفته است که اگر شما به اطلاعات در حال انتقال از یک ارتباط نا امن به ارتباطی امن حمله کنید (در این مثال از HTTP به HTTPS)، در حقیقت شما در به پل ارتباطی حمله نموده اید و قادر خواهید بود یک حملهٔ شخص میانی را در مورد ارتباط SSL اعمال کنید، حتی شما می توانید این حمله را قبل از شکل گیری این ارتباط SSL نیز اجرا کنید. آقای Moxie Marlinspike جهت امکان اجرای مؤثر این روش، اقدام به تولید نرم افزار SSLstrip نموده است. در این بخش ما از وجود این نرم افزار بهره می بریم.

این فرایند بسیار آسان بوده و یادآور برخی از حملات بررسی شده در قسمت های قبلی این مقاله می باشد. این فرایند در شکل ۲۶ نشان داده شده است.


شکل ۲۶. ربودن اطلاعات HTTPS

فرایند نشان داده شده در شکل بالا، به ترتیب زیر عمل می کند:

۱. اطلاعات مبادله شده بین کاربر و سرور ربوده می شود.

۲. زمانیکه URL مربوط به یک HTTP با sslstrip مواجه گردد، آنرا با یک لینک HTTP تعویض نموده و تغییرات انجام شده را در خود ذخیره می کند.

۳. کامپیوتر حمله کننده، مجوز هایی را به سرور شبکه ارائه می کند و خود را بجای کاربر معرفی می کند.

۴. اطلاعات از سایت مورد نظر دریافت شده و به کاربر (قربانی) ارائه می گردد.

این فرایند بسیار خوب عمل می کند، از دیدگاه سرور نیز، اطلاعات SSL مورد نظر در حال دریافت است و سرور تفاوتی را تشخیص نمی دهد. یک کاربر با تجربه یا هشیار ممکن است به HTTP نبودن flag اطلاعات در مرورگر پی برده و متوجه شود که موضوعی غیر عادی است.

## استفاده از SSLStrip:

نرم افزاری که امکان عملکرد های ذکر شده را مهیا می سازد، SSLStrip نام دارد. این نرم افزار تنها تحت Linux اجرا می شود، اگر مایل به مواجه شدن با مراحل دشوار نصب این نرم افزار نیستید، می توانید برنامهٔ Backtrack 4 را دانلود و اجرا کنید زیرا نرم افزار SSLStrip از قبل در این برنامه نصب شده است.

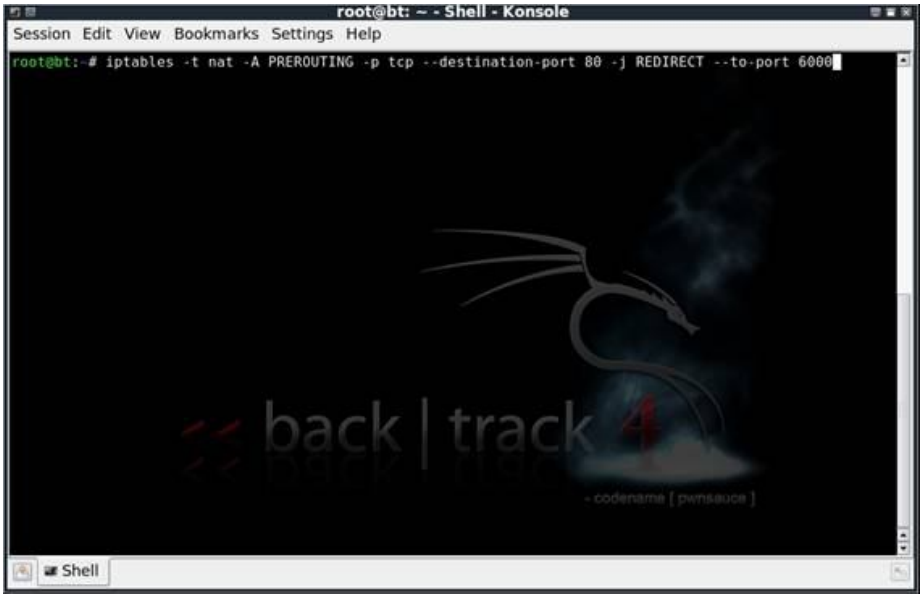
هنگامیکه به SSLStrip دسترسی پیدا کردید، لازم است اقدامات پیش نیازی را انجام دهید. ابتدا می بایست سیستم عامل Linux خود را جهت ارسال آدرس ها IP پیکربندی نمایید. برای انجام این کار باید آدرس زیر را در برنامهٔ واسط (shell) وارد نمایید

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```


شکل ۲۷. فعال نمودن امکان ارسال IP

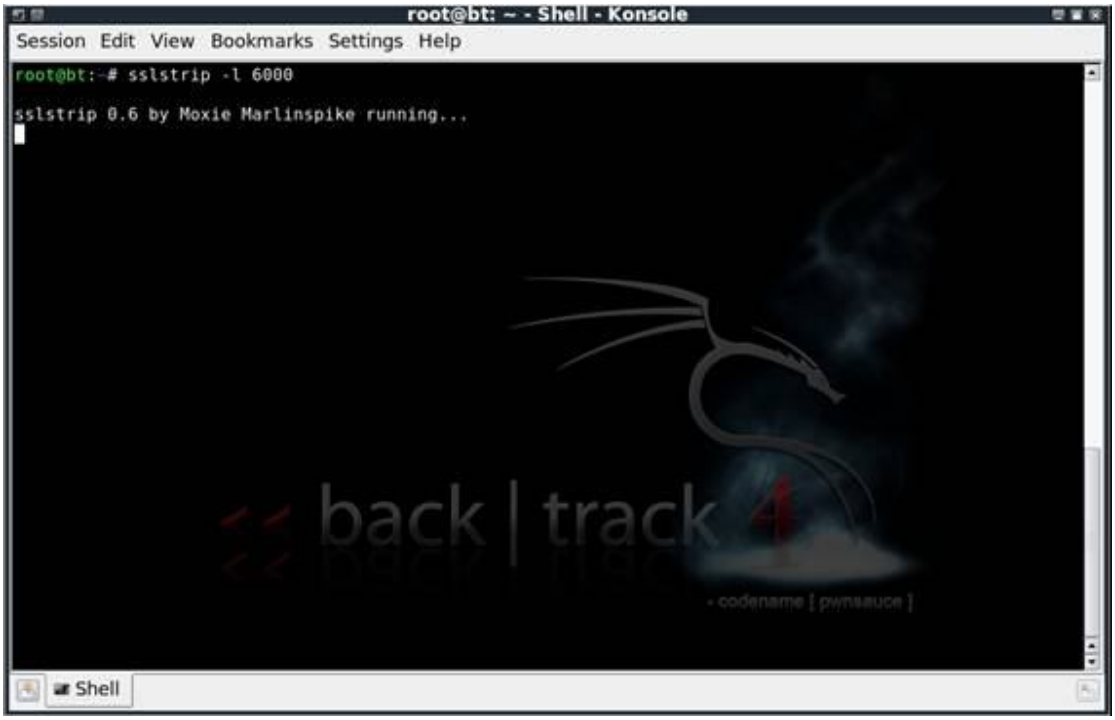
زمانیکه امکان ارسال IP ها را فعال نمودید، می بایست تمامی اطلاعات HTTP ربوده شده را به پورتی که SSLStrip در آن فعال است منتقل کنید. این عمل توسط اصلاح پیکربندی فایروال iptabel ها انجام می گیرد. برای اصلاح این پیکربندی، می بایست دستور زیر را وارد نمایید:

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port <listenPort>.




شکل۲۸. پیکربندی iptable جهت انتقال صحیح اطلاعات HTTP

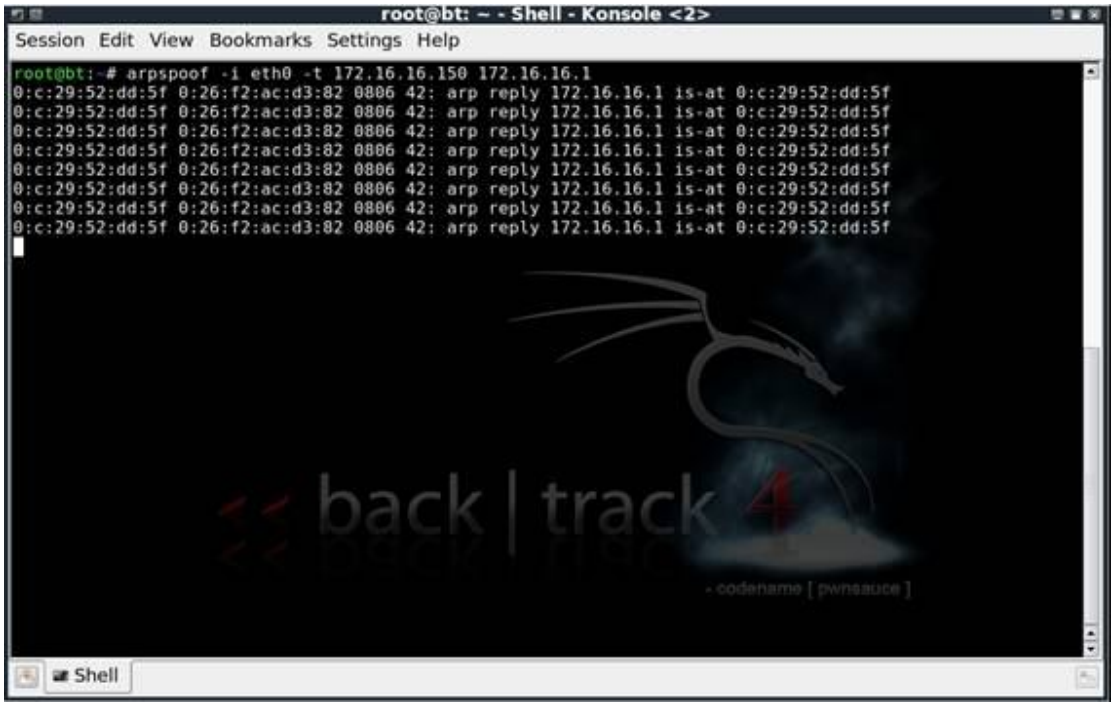
شما با انجام این عمل، <listen port> را با یک پورت تصادفی به انتخاب خودتان تعویض خواهید نمود. پس از پیکربندی این موارد، ما قادر خواهیم بود که sslstrip را اجرانموده و آنرا برای تجسس در پورت مشخص شده توسط دستور sslstrip -l <listenPort> پیکر بندی نماییم.




شکل ۲۹. بکارگیری SSLStrip

آخرین مرحله در این فرایند، پیکربندی "ARP Spoofing" جهت ربودن اطلاعات مبادله شده توسط قربانی می باشد. ما قبلاً در ویندوز و توسط نرم افزار Cain and Abel این کار را انجام داده ایم، اما در اینجا از ابزار arpspoof برای این منظور استفاده می کنیم. این نرم افزار در داخل برنامهٔ Backtrack4 تعبیه شده است. جهت انجام این کار باید دستور زیر را وارد نماییم:

arpspoof -i <interface> -t <targetIP> <gatewayIP>



```
root@bt:~# arpspoof -i eth0 -t 172.16.16.150 172.16.16.1
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
0:c:29:52:dd:5f 0:26:f2:ac:d3:82 0806 42: arp reply 172.16.16.1 is-at 0:c:29:52:dd:5f
```

شکل ۳۰. پیکربندی ARP Spoofing

با استفاده از این دستور، شما <interface> را برای ترمینال شبکه ای که شما این اقدامات را در آن انجام می دهید (eth0، eth1 و غیره) تعویض خواهید نمود. همچنین، <targetIP> را برای آدرس IP شخص قربانی تغییر می دهید و <gatewayIP> را برای آدرس IP دروازهٔ مورد استفادهٔ شخص قربانی عوض خواهید کرد.

پس از تکمیل این فرایند، شما می بایست بطور فعالانه به ربودن ارتباطات برقرارشدهٔ SSL بپردازید. اکنون شما می توانید از یک نرم افزار تجسسی برای دزدی password ها، اطلاعات شناسایی شخصی، شمارهٔ کارت های اعتباری و غیره استفاده کنید.

## روش های مقابله در برابر "ربودن SSL":

همانطور که قبلاً هم به آن اشاره شد، این نوع حمله از حملات ""ربودن SSL""، به هیچ عنوان توسط سرور قابل شناسایی نمی باشد زیرا این تبادل اطلاعات، به عنوان ارتباطات عادی و نرمال کاربر تلقی می شود. یک سرور، نمی تواند تشخیص دهد که از طریق یک پراکسی با کاربر در ارتباط است. خوشبختانه، چند روش برای کمک به کاربران جهت شناسایی و مقابله با این حملات وجود دارد:

از امن بودن اتصالاتی که از HTTPS استفاده می کنند، اطمینان حاصل نمایید: وقتی این نوع حمله را به اجرا در می آید، جنبه های امنیتی ارتباط از بین می رود و این تغییر، در مرورگر کاربر قابل مشاهده است. به عنوان مثال، هنگامیکه شما وارد عملیات بانکی آنلاین خود می شوید و می بینید که تنها یک اتصال عادی HTTP برقرار است، آنگاه می توانید به جریان داشتن چنین حملاتی شک کنید. مستقل از اینکه شما از چه مرورگری استفاده می کنید، باید قادر باشید اتصالات امن را از اتصالات نا امن تشخیص دهید.

عملیات بانکی آنلاین را در منزل انجام دهید: احتمال اینکه شخصی در شبکهٔ خانگی شما به تجسس در اطلاعات مبادله شدهٔ شما بپردازد کمتر از آن است که کسی در محل کار شما به انجام این عمل مبادرت کند. علت این امر آن نیست که کامپیوتر خانگی شما امن تر است زیرا کامپیوتر خانگی شما از امنیت کمتری برخوردار است، بلکه علت آنست که اگر شما یک یا دو کامپیوتر در منزل داشته باشید، تنها خطری که شما را تهدید می کند این است که پسر ۱۴ سالهٔ شما کلیپ های آموزش هک کردن را در YouTube دیده باشد. ولی در شبکهٔ کاری، شما از اتفاقات رخ داد در اتاق های دیگر شرکت یا در شعبه های دیگر شرکت در ۲۰۰ مایلی خود خبر ندارید، بنابراین احتمال اینکه حمله ای به کامپیوتر شما صورت گیرد، چند برابر می شود. یکی از اصلی ترین اهداف حملاتی از نوع ""ربودن SSL""، عملیات بانکی آنلاین است. با این وجود، راه های مقابلهٔ ذکر شده در این مقاله، در مورد تمامی اهداف این حملات کاربرد دارد.

کامپیوترهای موجود در شبکهٔ خود را ایمن سازید: باز هم تکرار می کنم که در اغلب موارد، چنین حملاتی از داخل شبکه صورت می گیرد. اگر کامپیوترهای شبکه شما ایمن باشند، آنگاه احتمال کمتری وجود دارد تا از این کامپیوترها جهت اجرای این حملات علیه شما استفاده شود.

## منابع و مآخذ:

MITM Attack, Chris Sanders

Man-in-the-middle attack, OWASP

adel piri : inject0r.ir

mohajem.war@gmail.com

tnx: Milad_Hacking - arf1372 - shabgard - b3hz4d - n1arash -Und3rground -ehsanc0d3r