مرکز آموزش الکترونیکی

امن کردن سرویس های شبکه های ویندوزی

مهدیه پاک طینت

فهرست

1– **نام موضوع :** امن ساختن شبکه های ویندوزی

2– **توضیح درباره موضوع :**securing windows network services

فرض کنید آخرین service pack و hotfix ها را نصب نموده اید و تقریبا آماده اید که به شبکه متصل شوید. حتی کامپیوتر های Desktop Windows هم انواع زیادی از سرویس های شبکه ای را فراهم می آورد، این سرویس های در ویندوزهای سرور هزاران بار بیشتر است. تنها استفاده از آخرین وصله ها برای شروع به کار کافی نیست، بلکه ما یک سنگر احتیاج داریم. مسلما ما نمی توانیم تمامی اعمال را بلوکه کنیم، اما می توانیم با یک سری پیش بینی های ابتدایی تهدیدات را به میزان قابل توجهی کاهش دهیم.

در این مقاله به روش هایی برای امن تر ساختن شبکه های ویندوزی در حوزه بی سیم، IIS و Remote Desktop می پردازیم.

3– **نام نرم افزارهای مورد استفاده :**

نام نرم‌افزار	نسخه	OS	مشخصه نرم افزار	رایگان	سایت نرم افزار
NetStumbler	0.4.0	win	یابنده و آنالیزور شبکه بی سیم	√	Netstumbler.com stumbler.net
Ethereal	0.99	Win/ Linux /Solrais	آنالیز ترافیک شبکه	√	www.ethereal.com http://ethereal.en.softo /nic.com
Airsnort	0.2.7	Linux/Win	بازیابی رمزنگاری	√	http://airsnort.shmoo.co /m
kismet	2009-06-R1	Linux	شنود و تشخیص دهنده شبکه بی سیم	√	http://www.kismetwir eless.net
Airopeek	NX	Linux	تحلیل گر بسته ها برای شبکه های محلی بی سیم		http://www.wildpackets.c /om
CENif	1.0	Win CE	شنود		

						fer
	http://www.netstumbler.com	√	یابنده و آنالیزور شبکه بی سیم	HPC/ PocketPC /Win Mobile	0.4.0	Minis tumbl er
	http://www.microsoft.Com/technet/security/tools/Locktools.asp	√	بالا بردن امنیت سرور	Win server		IIS Lock down

فهرست تصاویر

چکیده

در این مقاله سعی شده است بر طبق روال قسمت دوم فایل مبنای مقاله، به مباحث امنیت بی سیم، امنیت سرور و کار با Remote Desktop پرداخته شود.

از آن‌جا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست.در این مقاله به رعایت برخی نکات تاکید شده و به این منظور چندین ابزار معرفی گردیده است.

در یک سرور، IIS محلی است که بسیار مورد حمله قرار میگیرد، لذا لازم است در حد امکان از آن ذر برابر تهدیدات محافظت نمود. در این مقاله نکاتی در این باره ذکر شده است که در کنار نرم افزار های معرفی شده می تواند در حد زیادی کمک کننده باشد.

امروزه استفاده از دسترسی از راه دور به یک مقوله همگانی و لازم تبدیل گشته است. برای این منظور لازم است پروتکلی امن وجود داشته باشد که امکان خرابکاری را از این روش غیرممکن سازد. در این مقاله در مورد پروتکل RDP توضیحاتی داده شده است.

امنیت بی سیم:

شبکه های بیسیم به سرعت در حال رشد و توسعه می باشند. در دنیای بی سیم چیزی به عنوان زیر ساخت فیزیکی وجود ندارد تا بتوان با استفاده از این وسائل از دسترسی های غیر مجاز به لایه 2(Media Access) یا لایه 1 (Physical) جلوگیری بعمل آورد. برای دسترسی به منابع شبکه های بیسیم کافی است که یک مهاجم فقط در مجاورت این شبکه قرار گیرد بدون آنکه به محل حفظ اطلاعات مهم سازمان دسترسی فیزیکی داشته باشد و سه ویژگی مهم اطلاعات را از بین ببرد یعنی (Integrity, Confidentiality, Availability). استفاده از شبکه‌های بی سیم مزایای بسیاری دارد اما در کنار آن خطرات مختلفی کاربران را تهدید می کند. با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن است.

برای این منظور رعایت موارد زیر را توصیه میشود:

1- فقط تجهیزات وایرلسی خریداری نمایید که امنیت WPA و یا 802.11i را پشتیبانی کند.

2- اگر از WPA استفاده نمی کنید ، قوی ترین الگوریتم WEP ای که توسط wireless adapter card و Access point شما پشتیبانی می شود را فعال کنید و بلندترین و تصادفی ترین کلید ممکن را استفاده کنید.

3- اگر access point شما اهزار هویت 802.1x را پشتیبانی می کند ، یک سرور RADIUS نصب کنید.

RADIUSبه این معناست: تعیین اعتبار راه دور کاربری که از ارتباط تلفنی استفاده می کند. یک سرور RADIUS به تعیین اعتبار کاربران راه دور و ردیابی انها می پردازد. پیاده سازی RRAS در ویندوز سرور 2003 می تواند اعتبار سنجی کاربران را از طریق RADIUS انجام دهد.

پروتکل RADIUS[1] ، استانداردی برای طراحی و پیاده سازی سرویس دهندگانی است که مسئولیت تائید و مدیریت کاربران را برعهده خواهند گرفت. مشخصات و نحوه عملکرد پروتکل RADIUS در RFC 2865 و RFC 2866تعریف شده است.

پروتکل RADIUS از یک معماری سرویس گیرنده - سرویس دهنده برای تائید و accountingاستفاده می نماید . پروتکل فوق اطلاعات accounting ، پیکربندی ، تائید و مجوزها را بین یک سرویس گیرنده RADIUS و یک سرویس دهنده RADIUS حمل می نماید . سرویس گیرنده RADIUSمی تواند یک سرویس دهنده دستیابی شبکه NAS [2]، و یا هر نوع دستگاه مشابه دیگری باشد که نیازمند تائید و accounting است .

[1] Remote Authentication Dial-In User Service
[2] network access server

همانگونه که اشاره گردید NAS به عنوان یک سرویس گیرنده RADIUS عمل می نماید. سرویس گیرنده مسئول ارسال اطلاعات کاربر برای سرویس دهنده RADIUS است تا بر اساس نتایج برگردانده شده توسط سرویس دهنده ، در خصوص کاربر تعیین تکلیف گردد . سرویس دهندگان RADIUS مسئول دریافت درخواست ارتباط کاربر ، تائید وی و ارسال اطلاعات پیکربندی مورد نیاز برای سرویس گیرنده به منظور عرضه سرویس به کاربر می باشند . یک سرویس دهنده RADIUS می تواند به عنوان یک سرویس گیرنده پراکسی به سایر سرویس دهندگان RADIUS و یا سایر سرویس دهندگان تائید نیز عمل نماید .

سرویس گیرندگان RADIUS از طریق پورت های 1812 و 1813 پروتکل حمل UDP [1] با یک سرویس دهنده RADIUS ارتباط برقرار می نمایند . در نسخه های اولیه پروتکل RADIUS از پورت های 1646 و 1645پروتکل UDP استفاده می گردید . پروتکل RADIUS از پروتکل حمل TCP [2]حمایت نمی نماید .

با استفاده از پروتکل RADIUS می توان دستگاهی نظیر یک NAS را بگونه ای پیکربندی نمود تا یک کاربر را برای استفاده از یک سرویس خاص تائید نماید . به عنوان نمونه ، یک ISP می بایست کاربر یک پورت شبکه dial-inرا تائید نماید تا این اطمینان ایجاد گردد که وی مجاز به استفاده از پورت مورد نظر می باشد . در چنین مواردی لازم است که NAS اطلاعات مورد نیاز برای این ارتباط را دریافت نماید . اطلاعات فوق توسط یک سرویس دهنده RADIUS در اختیار وی گذاشته می شود . پس از ایجاد ارتباط ، دستگاه NAS ممکن است در صورت نیاز اطلاعات accounting را به منظور اهداف مالی و شارژ کاربر تامین و ارائه نماید.

شکل زیر نحوه تعامل بین یک سرویس گیرنده RADIUS (نظیر یک دستگاه NAS) و یک سرویس دهنده RADIUS (نظیر Internet Authentication Service) را نشان می دهد.

شکل 1- سرویس دهنده و سرویس گیرنده RADIUS

در ویندوز 2003 (نسخه های سرویس دهنده) ، IAS (برگرفته شده از Internet Authentication Service) مطابق استاندارد تعریف شده در RFC 2865و RFC 2866 به عنوان یک سرویس دهنده RADIUS و پراکسی پیاده سازی شده است. در نسخه های سرویس دهنده ویندوز 2000 ، شرکت مایکروسافت

[1] User Datagram Protocol
[2] Transmission Control Protocol

صرفا" ویژگی سرویس دهنده RADIUS را پیاده سازی کرده بود. علاوه بر این، در نسخه های سرویس دهنده ویندوز 2003 که بر روی آنها سرویس RRAS (برگرفته شده از Routing and Remote Access service) اجرا شده است را می توان به عنوان یک سرویس گیرنده RADIUS پیکربندی کرد. بدین ترتیب امکان تائید سرویس گیرندگان dial-inو یا VPN (برگرفته شده از Virtual Private Networks) از طریق یک سرویس دهنده RADIUS فراهم می گردد.

عناصر سرویس دهنده RADIUS در IAS قادر به تائید درخواست های سرویس گیرندگان RADIUS از طریق یک بانک اطلاعاتی محلی و یا اکتیو دایرکتوری می باشند. IAS جزئیات اطلاعات accounting ارائه شده توسط سرویس گیرنده RADIUS را در یک فایل متن و یا یک بانک اطلاعاتی رابطه ای ذخیره می نماید. IAS امکان دستیابی به اطلاعات accounting کاربران ، نگهداری شده بر روی سرویس دهنده IAS و یا یک کنترل کننده domain را دارد (در صورتی که سرویس دهنده IAS عضوی از یک domain باشد).

تراکنش های دستیابی و accounting بین سرویس گیرنده و سرویس دهنده با استفاده از یک رمز محرمانه به اشتراک گذاشته شده صورت می پذیرد . رمز فوق هرگز بر روی شبکه ارسال نخواهد شد و از آن به همراه فیلد تائید کننده و به منظور ارائه یک سطح امنیتی مناسب بر روی پیام های RADIUS استفاده می گردد . در صورت نیاز به یک سطح بالاتر امنیتی ، سرویس دهنده و سرویس گیرنده RADIUS می توانند از IPSec برای رمزنگاری پیام های RADIUS استفاده نمایند (این موضوع خارج از حوزه پروتکل RADIUS می باشد).

RADIUS دارای انواع مختلفی است که روی سیستم های عامل شبکه مختلف قابل استفاده اند. می توانید بدون خرید نرم افزار RADIUS تعیین اعتبار راه دور را انجام دهید. خدمات تعیین اعتبار اینترنتی (IAS) را می توان به سرور RADIUS تبدیل کرد. بنابراین همه مشتری های RAS که تقاضای تعیین اعتبار در ناحیه را دارند به سرور IAS ارجاع داده می شوند. IAS در ویندوز سرور 2003 می تواند تا 50 مشتری RADIUS را پشتیبانی کند. مشتری های RADIUS سرورهای دسترسی راه دور شبکه هستندکه برای تعیین اعتبار کاربر از سرور IAS استفاده می کنند.

برای نصب و پیکربندی IAS گامهای زیر رابردارید :

- Start / control panel / add or remove programs

را انتخاب کرده وروی دکمه windows components کلیک کنید .

- در ویزارد این گزینه جزء networking services را انتخاب کرده و روی details کلیک نمایید .

- در جعبه networking services گزینه internet authentication service یا همان IASخودمان را انتخاب کرده و روی OK و next کلیک کنید .
- IAS به سرور اضافه شده است. روی Finish کلیک کنید تا پنجره بسته شود .

پیکربندی خصوصیاتIAS

برای استفاده از سرور IAS بعنوان سرور RADIUS باید سرور IAS را در دایرکتوری فعال ثبت کنید. پس از ثبت آن در دایرکتوری فعال می توانید مشتری هاای RADIUSرا ایجاد کنید .

برای ثبت سرور IAS نمای فوری IAS را از طریق start / administrative tools / internet authenticationباز کنید، روی IAS کلیک راست کرده و Register server in active directoryرا انتخاب کنید. مرحله دوم پیکربندی IASتعیین نوع رویدادهایی است که در فایل های گزارش IAS ثبت می شوند. این تنظیمات در دو مکان مختلف انجام می شوند: جعبه محاوره ای خصوصیات سرور IAS و پوشه گزارش دسترسی راه دور.(remote access logging)

برای باز کردن جعبه خصوصیات IAS در نمای فوری Internet authentication service کلیک کرده و گزینه properties را انتخاب کنید. بصورت پیش فرض درخواست های تعیین اعتبار پذیرفته شده و رد شده در فایل گزارش دسترسی راه دور ثبت می شوند، می توانید جعبه چک این گزینه ها را غیر فعال کنید، پس از انتخاب گزینه مورد نظر روی ok کلیک کنید. در نمای فوری گزینه remote access logging کلیک کنید تا در صفحه جزئیات روشهای تهیه گزارش نمایش داده شوند. فایل گزارش بصورت پیش فرض در یک فایل متنی ذخیره می شود. همچنین می توانید این فایل را در یک فایل پایگاه داده که روی یک SQL SERVERقرار دارد ذخیره کنید. هم در فایل محلی و هم در فایل پایگاه داده می توان تنظیمات مربوط به رویدادها را انجام داد.

افزودن مشتری های RADIUS

مشتری RADIUSیک سرور دسترسی است که برای تعیین اعتبار از IAS استفاده می کند. مشتری RADIUS در پیاده سازی RRAS ویندوز تعبیه شده و تنها کاری که لازم است انجام دهید اضافه کردن مشتری به پیاده سازی IAS است. برای مشخص کردن مشتری RADIUS از نام DNS یا آدرس IP استفاده کنید. افزودن مشتری RADIUS به سرور IAS طی مراحل زیر انجام می شود:

-در نمای فوری IAS روی پوشه RADIUS clients کلیک راست کرده و از منوی ظاهر شده گزینه new radius clientرا انتخاب کنید .

-نامی برای مشتری انتخاب کنید، همچنین آدرس IP یا نام DNS مشتری را تایپ کنید. اگر نام DNS را وارد می کنید، با استفاده از verify می توانید صحت نام را چک کنید. جعبه محاوره verify client باز می شود .

-روی resolve کلیک کرده و آدرس IP که مشتری از آن استفاده خواهد کرد را وارد کنید و روی OK کلیک کنید تا به جعبه محاوره client new RADIUS برگردید .

-پس از وارد کردن نام و نام DNS یا آدرس IP مشتری روی next کلیک کنید در صفحه بعدی فهرستی از فروشندگان مشتری را مشاهده می کنید. از انجا که از پیاده سازی RRAS مایکروسافت استفاده می کنید گزینه Microsoftرا انتخاب کنید. اگر می خواهید پیامی که بین سرور RADIUS و مشتری RADIUS رد و بدل می شود را رمزگذاری کنیدگزینه request must contain message authenticator را انتخاب کنید. با انتخاب این گزینه و وارد کردن یک رمز عبور محرمانه پیامهایی که بین سرورهای RRAS و IAS رد و بدل می شوندرا رمز گذاری میکنید .

4- اگر می خواهید از یک لایه امنیتی فراتر از WPA/WEP استفاده کنید IPSec را فراموش نکنید (پروتکل IPSEC امنیت ارتباطات IP را توسط عملیات اهراز هویت و رمز نگاری برای هر بسته IP در یک نشست ارتباطی تامین می کند) و فراموش نکنید که NetBIOS را غیر فعال کنید .

فعال و غیر فعال کردن:NetBIOS

روش اول :

برای فعال و یا غیر فعال کردن NetBIOS روی سیستمتان در این روش شما باید به Network Connections رفته و در آنجا Connection مورد نظر خود را انتخاب کنید و سپس به Properties بروید . وقتی که روی این گزینه کلیک کردید باید به سر برگ Networking رفته و گزینه Internet Protocol(TCP/IP) را انتخاب کنید و بعد به قسمت Properties بروید . با کلیک کردن بر روی Properties یک صفحه باز میشود که شما باید روی گزینه Advanced کلیک کنید . حال شما باید در صفحه باز شده به سر برگ WINS رفته و در پایین این صفحه در قسمت NetBIOS setting تنظیمات خود را برای فعال یا غیر فعال کردن نت بیوس اعمال کنید .

روش دوم :

در این روش شما برای فعال یا غیر فعال کردن NetBIOS باید مسیر زیر را دنبال کنید :

Control Panel => Administrative Tools => Local Security Policy

بعد از وارد شدن به Security Policy Local شما باید به قسمت Local Policies و سپس به قسمت Security Options بروید و در آنجا مسیر زیر را دنبال کنید و تغییرات خود را انجام دهید .

1) Network Access: Do not allow anonymous enumeration of SAM accounts
2) Network Access: Do not allow anonymous enumeration of SAM accounts and shares

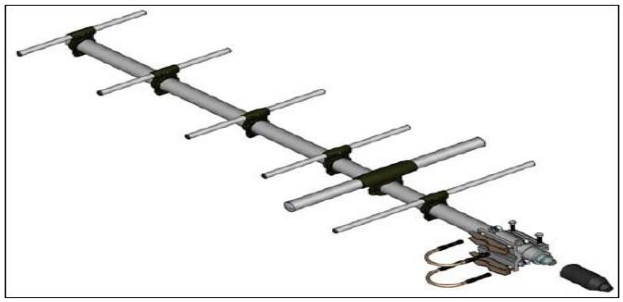
5- SSID پیش فرض کارخانه و کلمه عبور دستگاه wireless را تغییر دهید.

6- از broadcast کردن SSID توسط Access point جلوگیری کنید.

7- یک دیواره اتش شخصی نصب کنید.

8- در صورت امکان APرا پشت یک دیواره آتش داخلی قرار دهید تا جریان بسته ها را تنظیم کند و یک حسگر IDS برای چک کردن بسته ها قرار دهید.

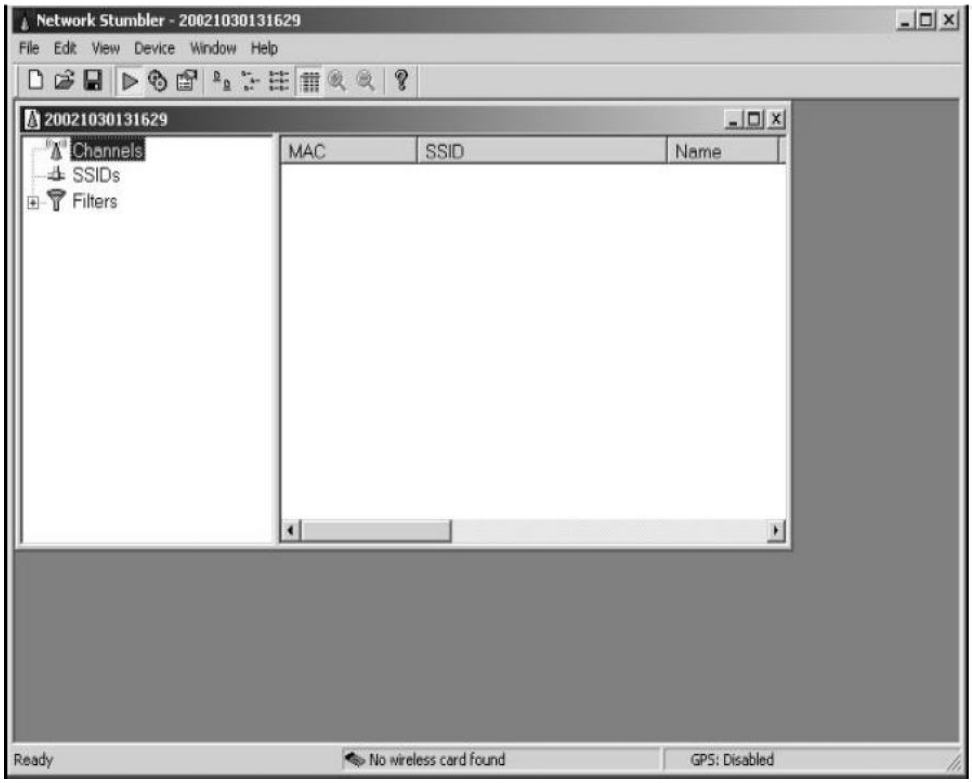
9- به eBay بروید و یک آنتن Yagi با یک کابل تافته (pigtail) برای کارت 802.11 لپ تاپ خود بخرید و یک نرم افزار war driving مثل Netstumbler روی لپ تاپتان نصب کنید (netstumbler.com) سپس اطراف ساختمان را با آن بررسی کنید ببینید آیا AP ناشناخته ای به LAN شما متصل است یا نه. هکرها از این نوع آنتن ها استفاده می کنند.

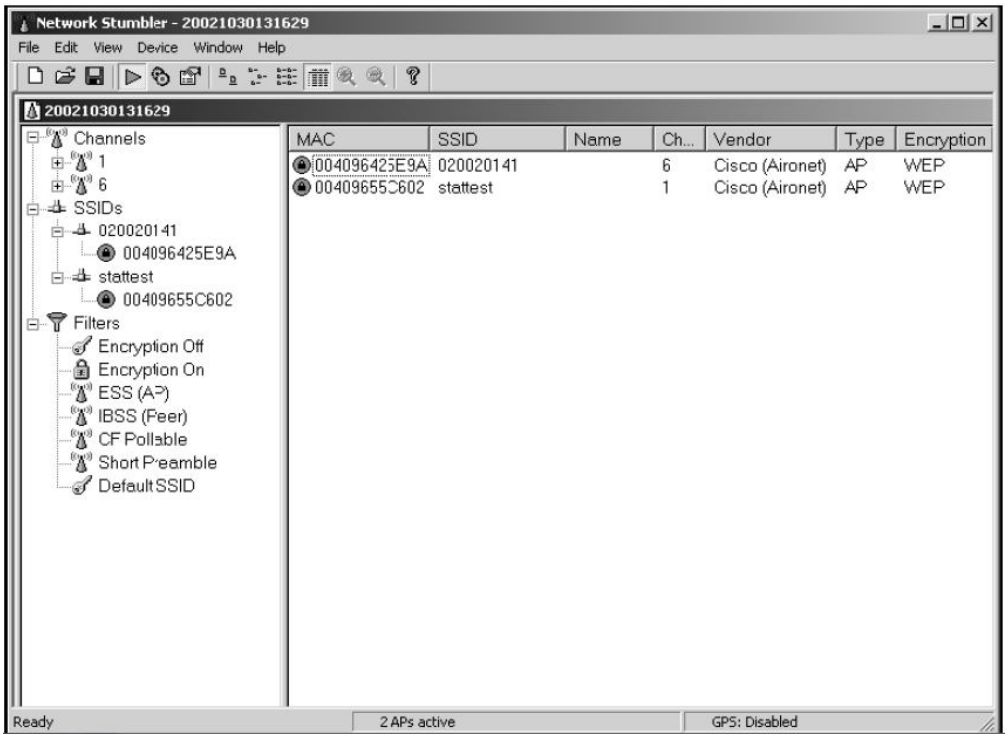


شکل 2- آنتن یاگی

Wardriving : به رانندگی با یک لپ تاپ با قابلیت بی سیم برای یافتن مکان هـایی جهـت دسـت یـابی بـه شبکه های بی سیم بی حفاظ می گویند. گردش در محدوده جغرافیای خاص و پیدا نمـودن شـبکه هـای بـی سـیم برای آمارگیری از این شبکه ها. این آمار در آینده به امنیت شبکه های بی سیم کمک خواهد کرد.

NetStumbler یابنده و آنالیزور شبکه های بی سیم است که شبکه های مبتنی بـر 802.11b و 802.11g را پشتیبانی می کند. این نرم افزار با broadcast نمـودن یـک بسـته در خواسـت، AP هـای نزدیـک بـه خـود را شناسایی می کند. زمانی که AP ها بسته ی درخواست را می گیرند، اطلاعات SSID، آدرس MAC و غیره را بـه نرم افزار ارسال می نمایند. اگرچه بسیاری از آن ها امکان غیر فعال نمودن ایـن ویژگـی را بـه مـدیریت شـبکه مـی دهند. برای آنکه SSID برای NetStumbler ارسال نشود علاوه بر اینکه ویژگی Broadcast ، آنرا غیر فعال مـی کنید باید نام پیش فرض آنرا نیز تغییر دهید.





شکل NetStumbler-3

نصب این نرم افزار مشابه کلیه ی نرم افزار های مبتنی بر ویندوز است. در ابتـدا بایـد بسـته ی نصـب را دانلـود نمایید. برای دریافت این بسته از یکی از دو آدرس زیر استفاده کنید :

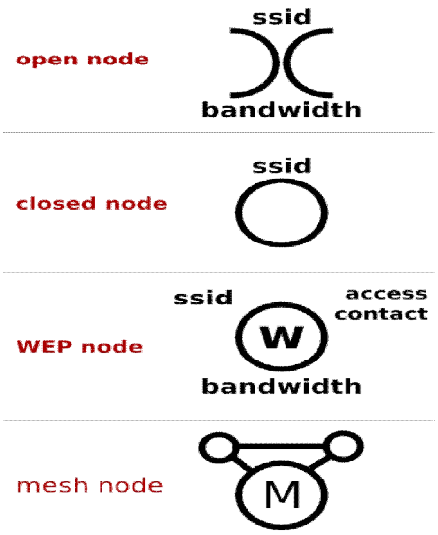
Netstumbler.com
stumbler.net

پس از دانلود بسته نصب، مراحل معمول نصب را با باز نمودن فایل exe ، طی نمایید.

در واقع Wardrivingبه بررسی نقاط ضعف ناشی از وجود ارتباطات بیسیم مـی پـردازد . راهکارهـایی بـرای مقابله با Wardriving و تامین امنیت شبکه بی سیم وجود دارد که عبارتند از:

- کد گذاری داده ها با روش هـای مختلـف مـثلا بـه جـای اسـتفاده از مکـانیزم WEP از WPA و یـا LEAP استفاده کرد تا نفوذ بیگانگان به شبکه را به حداقل رساند
- تنظیمات بهینه مربوط به SSID، SSID Broadcast، Filter By MAC
- استفاده از پروتکل EAP
- و...

10- اگر نمادهای عجیب روی دیوار بیرونی ساختمان شما نوشته شد ، سریع آنها را پاک کنید. این نماد ها warchalking نام دارند[1]. در واقع warchalking علامت گذاری ساختمان ها و پیاده رو ها با گچ برای نشان دادن محلی است که می توان در آن به یک شبکه بی سیم شرکتی بدون حفاظ دسترسی پیدا کرد. این نقاط دستیابی از طریق war driving یافت شده اند.



شکل 4- نمادهای warchalking

11- امنیت بی سیم یک زمینه در حال تغییر است، بنابراین سعی کنید در صدر پیشرفت ها باشید حداقل با ابزارهای رایج و کاربرد آنها برای خود آشنا باشید. برخی از آنها عبارتند از:

Ethereal-Airsnort- Kismet-Airopeek NX- CENiffer- FakeAF-Ministumbler

در اینجا به توضیح تعدادی از آنها می پردازیم:

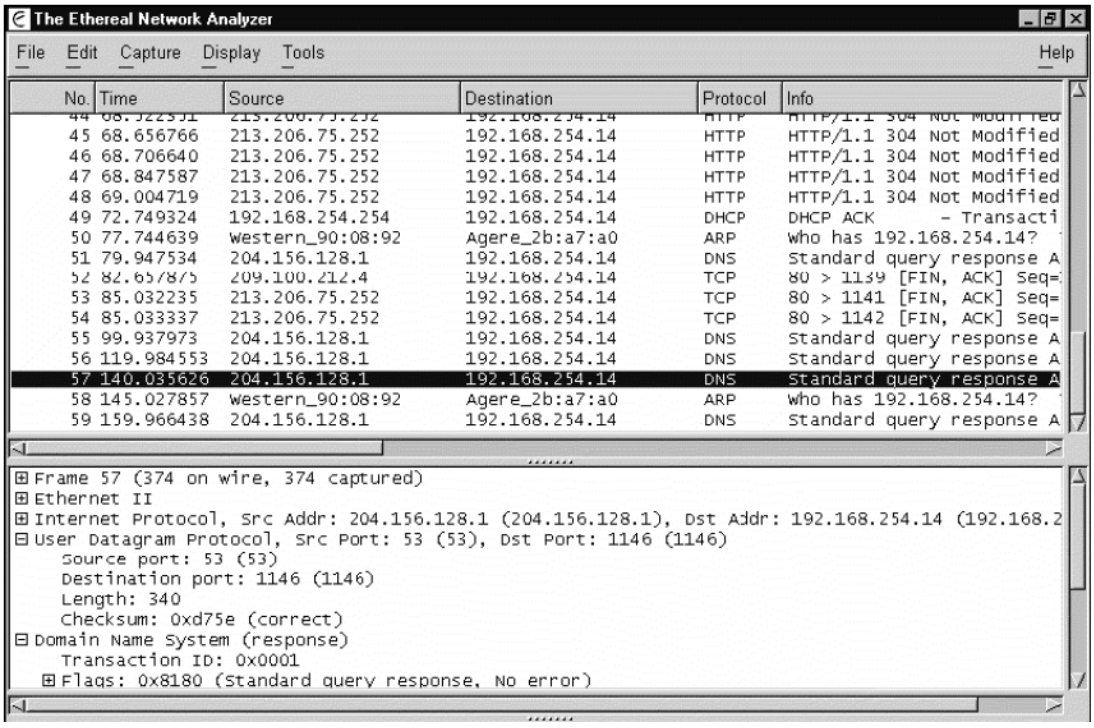
Ethereal: ابزاری کد-باز و رایگان است، که آن‌را می‌توان در دسته‌ی Snifferها جای داد. این نرم‌افزار با توجه به ویژگی‌هایش، یکی از متداول‌ترین ابزارهای آنالیز ترافیک شبکه است.

www.ethereal.com

[1] برای ترجمه نمادها به warchlking .org مراجعه کنید.

این نرم‌افزار نیز مانند WinDump، پس از نصب، از کتابخانه Winpcap برای دریافت اطلاعات بسته‌ها استفاده می‌کند، لذا پیش از نصب Ethereal، آخرین نسخه‌ی نرم‌افزار Winpcap را نصب کنید. همان‌طور که گفته شد این بسته امکان دریافت بسته‌ها و استخراج اطلاعات از آن‌ها را، فراهم می‌کند.

Ethereal، به عنوان نمونه‌ای از یک Sniffer، وظیفه‌ی ثبت رخدادها، اطلاعات و بسته‌های رد و بدل شده بر روی لایه‌های شبکه را بر عهده دارد. با ثبت داده‌های در حال انتقال بر روی شبکه و تجزیه‌ی آنها، می‌توان بسته‌های اطلاعاتی مربوط به پروتکل‌های متفاوت را از یکدیگر تفکیک نمود و ارتباطات مجزا را شناسایی نمود. همان‌گونه که در معرفی این دسته از نرم‌افزارها گفته شد، این قبیل تحلیل‌ها، می‌توانند به شناسایی ارتباطات خطرناک، تلاش‌های پیاپی برای دست‌یابی به منابع شبکه و نفوذ به آن و یا از کار انداختن نرم‌افزارها و سخت‌افزارها فعال بر روی شبکه، بیانجامد. با این وجود از آنجاکه خروجی این دسته از نرم‌افزارها به حدی پیچیده‌اند که کاربران عادی قادر به تحلیل آنها نیستند، لذا این‌گونه نتیجه‌گیری‌ها و تحلیل‌ها عموماً توسط متخصصین شبکه انجام می‌پذیرد.



شکل 5- Ethereal

نرم‌افزار Ethereal بر روی سه بستر اصلی Windows، Linux و Solrais ارایه می‌شود که نسخه‌ای که ما بررسی می‌کنیم، نسخه‌ی تحت Windows آن است.

توانایی‌های این دسته از ابزارها را عموماً می‌توان به بخش‌های زیر تقسیم کرد :

– انواع پروتکل‌ها و انواع رابط‌های شبکه‌ای که توسط ابزار شناسایی شده و تفکیک می‌گردند.

– روش‌ها و قالب‌های ذخیره‌سازی خروجی برداشت و تحلیل اطلاعات شبکه

– امکان بازخوانی اطلاعات ذخیره شده توسط نرم‌افزارهای Sniffer مشابه دیگر

– امکان استفاده از فلیتر برای پروتکل‌های مختلف

– قابلیت نصب بر روی محیط‌ها و سیستم‌های عامل متنوع

البته سادگی کار با نرم‌افزار، به عنوان قابلیت‌های ویژه رابط کاربری، نیز یکی دیگر از قابلیت‌هایی است که اغلب برای کاربران نیمه‌حرفه‌ای و مبتدی اهمیت ویژه‌ای دارد.

قابلیت‌های خاص Ethereal را، با توجه به تقسیم‌بندی فوق، می‌توان به شرح دسته‌بندی نمود :

– شناسایی پروتکل‌ها و رابط‌های شبکه‌ی متنوع

این نرم‌افزار قابلیت شناسایی حدود ۵۰۰ نوع پروتکل مجزا را دارد. تنوع این پروتکل‌ها به این نرم‌افزار قدرتی ویژه بخشیده است.

از باب ارتباطات نیز این نرم‌افزار قابلیت دریافت اطلاعات بسته‌های فعال ارتباطات Ethernet، FDDI، Token-Ring، IEEE 802.11، IP over ATM و رابط‌های loopback را دارد.

– ذخیره‌سازی اطلاعات

Ethereal با ایجاد فایل‌های خروجی قابل ویرایش در قالب‌های (lippcap(tcpdump، Sun snoop، Microsoft Network Monitor و Network Associate Sniffer از نظر ذخیره‌سازی اطلاعات نیز ابزاری قدرت‌مند محسوب می‌شود.

– سازگاری با خروجی نرم‌افزارها و سیستم‌های دیگر

Ethereal قابلیت بازخوانی پرونده‌های اطلاعاتی نرم‌افزارهای مشابه دیگری همچـون TCPDump، NAI's Sniffer & Sniffer Pro، NetXray، MS Network Monitor، Novell LANanalyser، Cisco Secure IDS iplog و غیره را دارد.

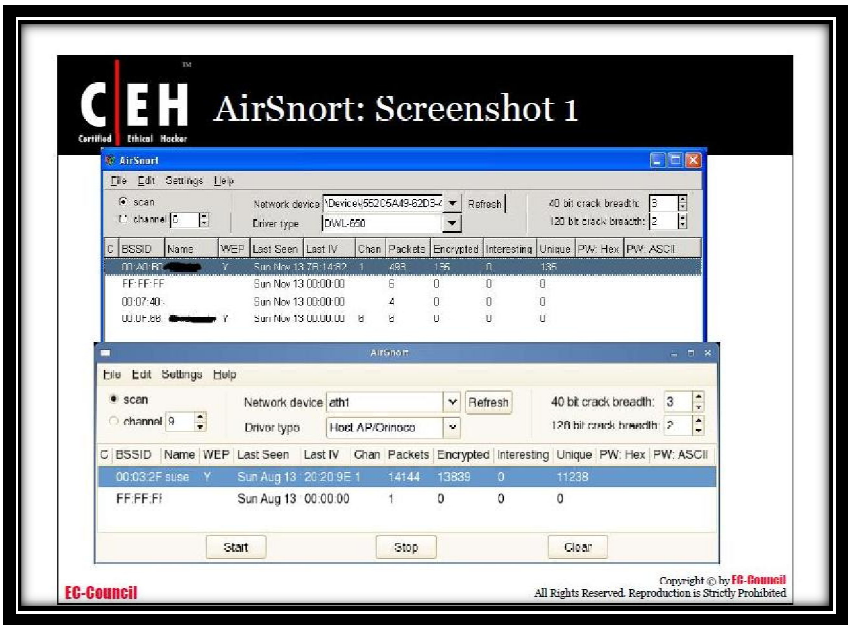
- فیلترها

این ابزار، با محدود سازی روش دریافت و تحلیل اطلاعات جمـع‌آوری شـده از بسـته‌هـا، در بسـیاری از حـالات امکان استفاده از فیلترهای پرقدرتی را به کاربر می‌دهد. در عـین حـال بـا اسـتفاده از ایـن فیلترهـای مـی‌تـوان بـه جست‌وجوی بسته‌ها در میان اطلاعات ذخیره شده نیز پرداخت.

- قابلیت‌های رابط کاربری

رنگ‌های متنوع برای تغییر روش نمایش اطلاعات بسته به فیلتر انتخاب شده، منوهای متنـوع و دیگـر امکانـات رابط کاربری، به تحلیل و شناسایی بسته‌ها کمک شایانی می‌کند.

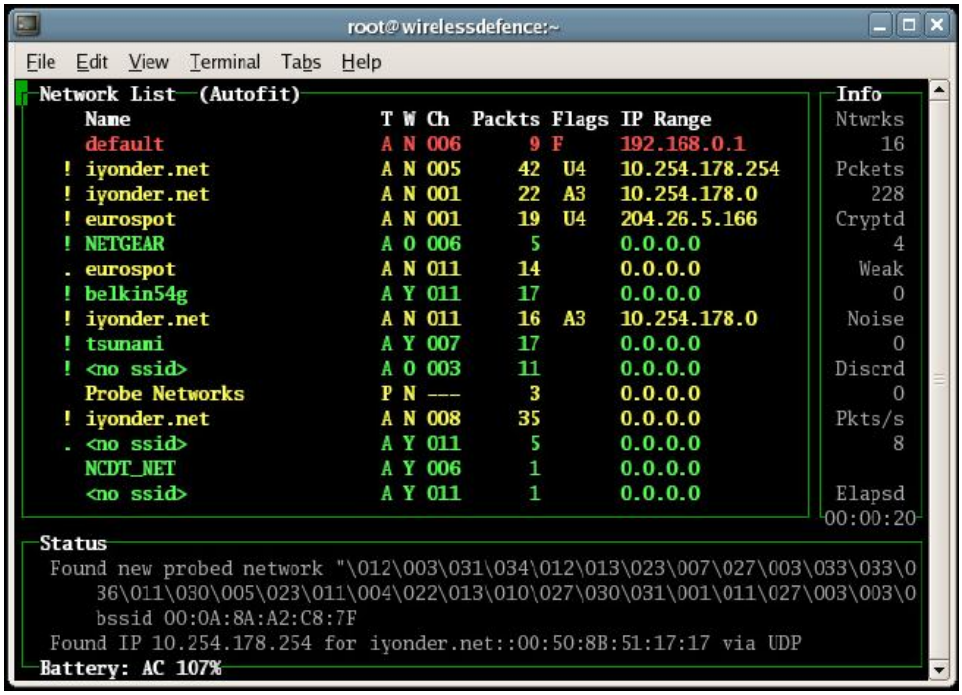
Airsnort : ابزار شبکه LAN و WLAN که کلیه های رمز گذاری را بازیابی می کنـد. ایـن ابـزار بـه طـور منفعلانه انتقالات بی سیم را نظارت کرده و هرگاه به تعداد کافی بسته ها جمع آوری شوند کلیه ی رمـز نگـاری بـه طور اتوماتیک محاسبه می شود.



شکل AirSnort-6

kismet : یک ابزار شنود و تشخیص دهنده شبکه بی سیم 802.11 و همچنین یک سیستم تشخیص نفوذ است. این ابزار با جمع آوری منفعلانه بسته ها، شبکه ها را شناسایی کرده و انواع آنها از شبکه های نامگذاری شده استاندارد تا شبکه های مخفی را تشخیص داده و همچنین با بررسی ترافیک وجود شبکه های non-beaconning را استنتاج می کند. (محیط های Linux و BSD)

http://www.kismetwireless.net



شکل Kismet-7

Airopeek : یک ابزار تحلیل گر بسته ها برای شبکه های محلی بی سیم است که همه پروتکل های لایه های بالایی مانند NetBEUI ، IPX ، Apple talk و TCP/ IP را پشتیبانی می کند.

CENiffer: یکی از ابزار های sniff داده ها در winCEMobile است.

FakeAP: AP های جعلی نقاط دسترسی فریبنده و غیر قابل اعتماد شبیه سازه شده هستند. جعل AP مکانیزمی برای فریب دادن قربانی هاست تا بدون اینکه بدانند به یک AP شبیه سازی وصل شوند و از آن استفاده نمایند.

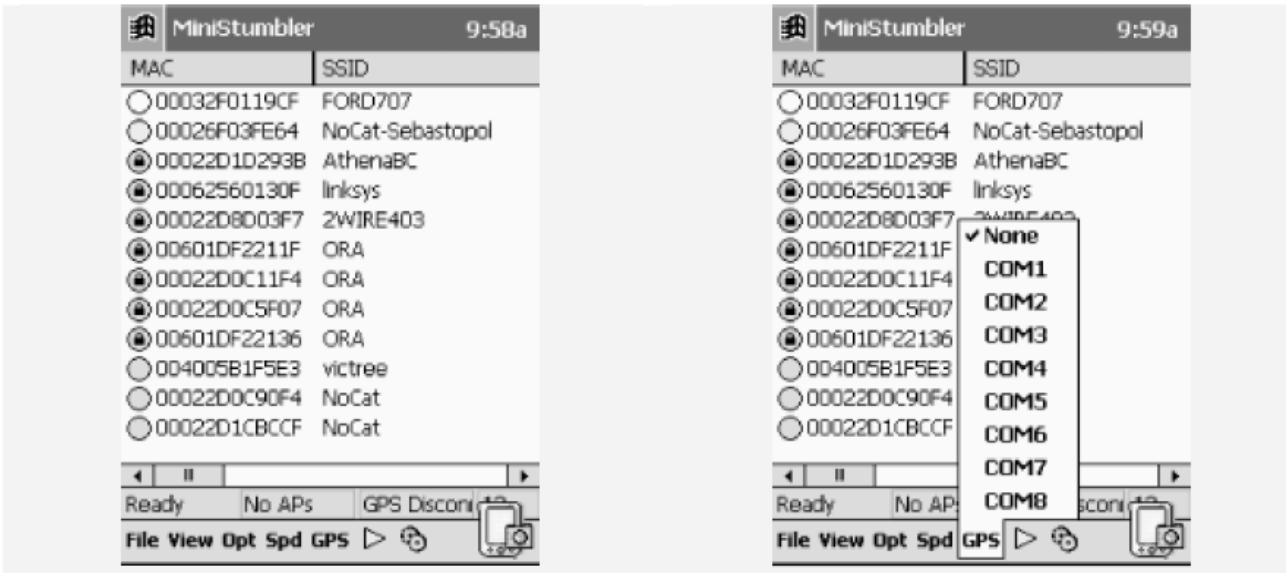
راه انداختن یک AP جعلی، کار ساده‌ای است. با هزینه حدود صد دلار می‌توان یک AP خرید و با اتصال آن به شبکه سیمیLAN ، در شبکه یک backdoor ایجاد نمود. با داشتن یک لپ‌تاپ، لینوکس، (hostap.epitest.fi) و Air Snarf (airsnarf.shmoo.com) به راحتی می‌توان یک AP جعلی ساخت. مهاجمان AP SSID جعلی را با AP های شما همسان در نظر گرفته و اگر کانال کاری آن‌ها را مطابق Access Pointهای شما انتخاب کنند، سرویس‌گیرندگان به آن دستگاهی وصل خواهند شد که سیگنال قوی‌تری داشته

باشد. پس از اتصال سرویس‌گیرنده‌ها، مهاجم می‌تواند تمام ارتباطات و داده‌ها را زیر نظر گرفته و username و passwordکاربران را به سرعت سرقت کند.

برای اجتناب از این خطرات باید به دنبال APهای جعلی بگردید. برای این کار می‌توانید از kismet، wellenreiter یا Airo Peek و Wireless Sniffer استفاده کنید. البته در اصل اولین نقطه مبارزه شما با مهاجمان و هکرها، ایجاد یک محیط مناسب برای شبکه است. علاوه بر بهینه‌سازی مکانAP ها و تهیه نقشه از شبکه خود، کاربران را با ریسک‌های تهدیدکننده و عواقب خرابکاری در شبکه آشنا کنید.

افرادی که در یک قسمت عمومی مثل پارکینگ در شرکت شما به شبکه سیمی دسترسی دارند، به راحتی می‌توانند با یک لپ‌تاپ یک Access Point جعلی بسازند و با Ethereal به دنبال username و passwordهای متنی مبادله شده در شبکه بگردند، با nmap شبکه شما را اسکن کنند و در بهترین حالت با رها کردن آن، به دیگران اجازه استفاده آزاد از آن را بدهند.

Ministumbler: این ابزار نسخه کوچک تری از NetStumbler است که برای کار با pocket pc 3.0 و pocket pc 2000 طراحی شده است. بطور پیش فرض ،اغلب نقاط دسترسی شبکه های بی سیم بطور فراگیر کد شناسایی (SSID) را پخش می کند برای هر کسی که به گوش خواهد بود. این آشوب ناگهانی در شبکه بی سیم توسط ابزار Ministumbler استفاده شده است.این ابزار می تواند به سیستم GPS اتصال پیدا کند .



شکل8 - MiniStumbler

Internet Information server

شـاید Internet Information server (IIs) از محصـولات micro soft بیشـترین میـزان هـک شـدن را داشته باشـد IIS یـک مجموعـه از سـرویس هـایی اسـت کـه مـی تواننـد بـه طـور جداگانـه نصـب شـوند شـامل NNTP,STMP,FTP,HTTP . در اینجا ما فقط به HTTP میپردازیم در این قسمت روی تعـدادی از تغییـرات ساده روی IIS بحث می کنیم که میتواند سطح حمله را کاهش دهد . در حقیقـت IIS مـی توانـد در مقابـل تمـام حمله های شناخته شده مقاوم گردد. IIS سالها یک فضای آزاد شکار خوب برای هکرها بوده است.

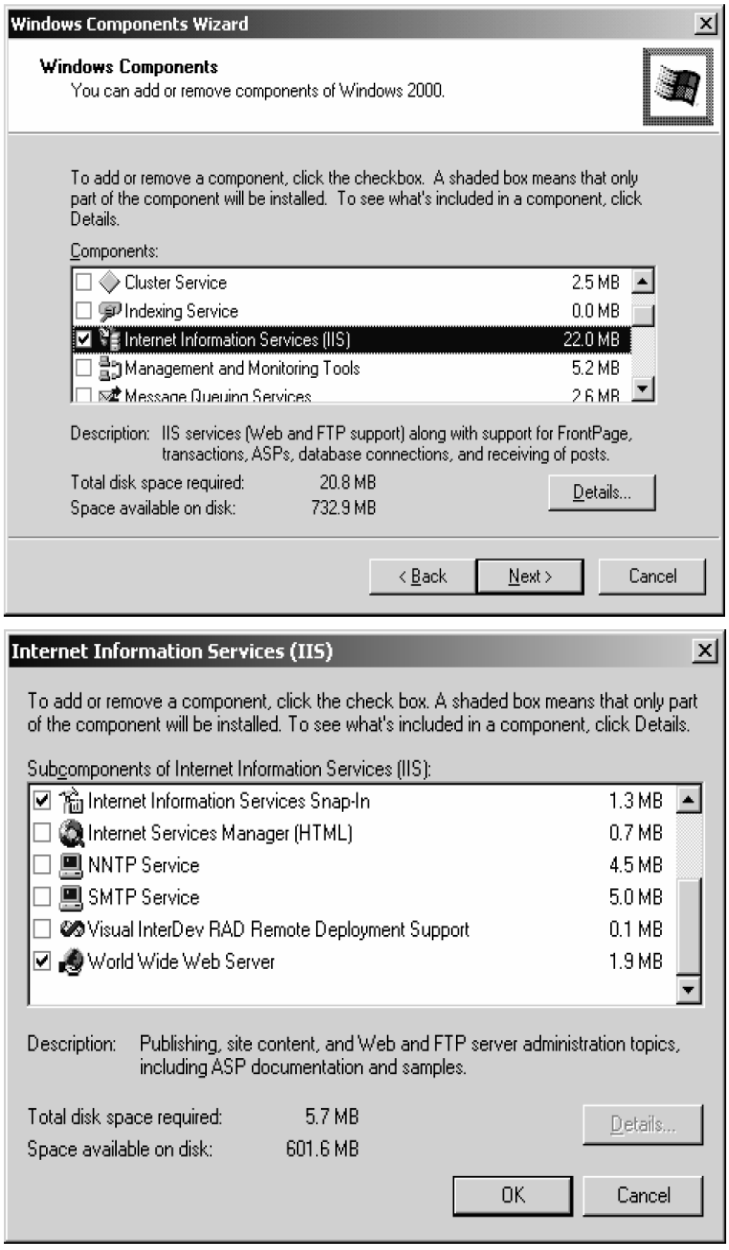
1- IIS6.0 را برگزیند (ویندوز سرور 2003):

ویندوز سرور 2003 به طور پیش فرض IIS6.0 را فعال نمی کند و وقتی که فعال شـود آیـتم هـای کمـی را نصب می نماید IIS 6.0 سریع تر از IIS5.0 نصب شده روی ویندوز سرور 2003 اجرا می شود زیرا از ابتدا برای ASP.Net و سرویس های Netframwork. طراحی شده است و بسیاری از خصوصیات URLScan را بـه طـور پیش فرض یکی کرده اسـت . همچنـین یـک معمـاری «worker process isolation mode» دارد کـه آن را بسیار منعطف تر ساخته است .(در ادامه در مورد URLScan توضیح خواهیم داد)

2- نصب نرم افزار را پاکسازی کنید:

با نصب یک سیستم عامل شروع کنید آخرین Service pack و همه hotfix ها . در حالـت ایـده آل ویـنـدوز شما باید یک سرور مستقل باشد . اگر IIS یک member server است، نباید یکی از اعضای دامین داخلـی اصـلی (main Interal domain) باشد . این دامین IIS باید از دامین داخلی و همه ترافیک firewall ایزوله باشد.

هر نسخه ای از IIS را که نصب می کنید تمام کامپوننت های اختیاری که نمی خواهید از آن استفاده کنیـد را uninstall کنید (مانند Indexing service ,SMTP)



شکل 9- حذف کامپوننت های اختیاری IIS

اگر هر گونه نمونه صفحه web یا IISHelp نصب کرده اید همه آنها را حذف کنید.

3- درایورهای NTFS را با حداقل دسترسی جدا سازی کنید :

سیستم عامل شما باید در یک درایو نصب شود و فایل های وب سایت شما در درایو دیگر قرار گیرند (شاید D) و چیز دیگری در آن قرار نگیرد.

همه درایوها باید با فرمت NTFS باشند برای درایو سیستم عامل [1] قالب امنیتی مناسب به کار گیرید.

[1] boot partition

قسمت های فایل های HTML ، اسکریپت های ASP/CGI و گرافیک شما نباید جز موارد زیر اجازه کار دیگری داشته باشند :

سیستم :کنترل کامل

ادمین : کنترل کامل

سایر افراد : خواندن و اجرا کردن .

نکته مهمی که وجود دارد،دادن اجازه «نوشتن» به Local Administrator ها و جلوگیری از دسترسی «نوشتن » به هر شخص دیگر می باشد .

4- وب سایت های پیش فرض را غیر فعال کنید:

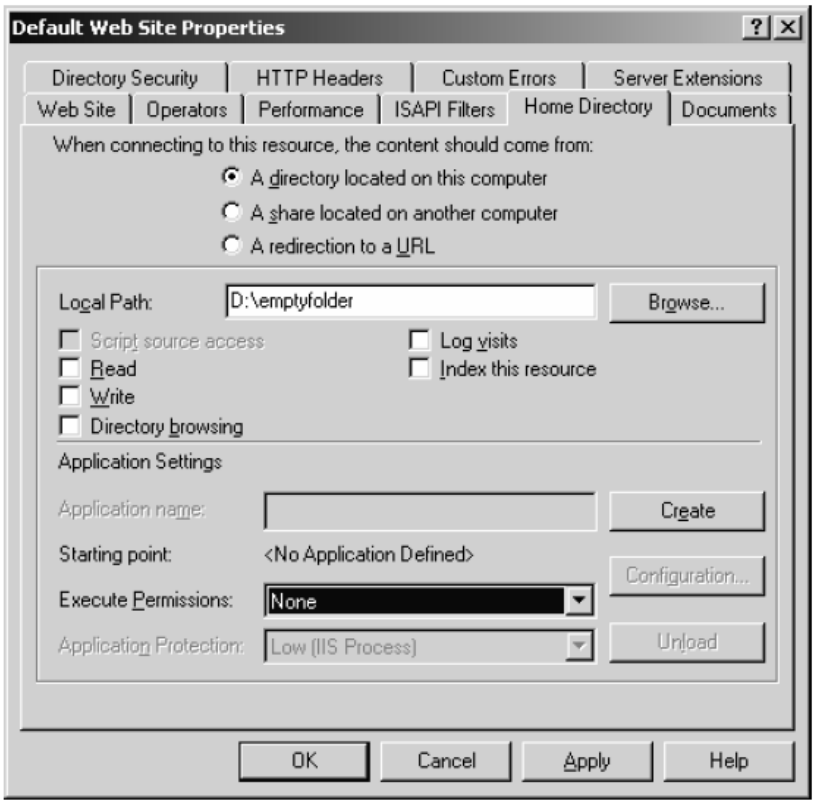
Administrative Tools→snap-in

Right click on your Default website→ properties →Home Directory

پوشه root از وبسایت را به پوشه های top-level تغییر دهید . سپس در هر برگه property از Defualt website ، همه گزینه ها را بر روی restricted /off/disabled و مشابه آن تنظیم کنید.

مطمئن شوید که اجازه اجرا در تب Home Directory روی None قرار گرفته است . روی OK کلیک کنید و تغییرات را ذخیره نمایید.

سپس روی Default website راست کلیک کنید و stop را انتخاب نمایید وب سایت شما کاملاً غیر فعال است .



شکل 10-غیر فعال کردن وبسایت های پیش فرض

5- یک وب سایت جدید بسازید:

یک جعبه IIS به تنهایی می تواند به طور همزمان چندین وب سایت را میزبانی کند. سه راه برای تفکیک وب سایت ها از یکدیگر وجود دارد. 1- اختصاص IP مختلف به هر سایت 2- اختصاص شماره پورت های مختلف به هر سایت 3- اختصاص Host Header مختلف به هر سایت.

یکی از امکاناتی که به Http v1.1 اضافه گردیده ، این است که هدر Http اجازه می دهد چندین سایت روی یک IP و درست روی همان پورت استاندارد TCP (پورت 80) اجرا شوند . پیش از این هر وب سایت برای اجرا شدن به حداقل یک IP اختصاصی و یا یک پورت اختصاصی نیاز داشت . برای این منظور در صورت نیاز به تعریف چندین سایت ناگزیر بودیم یا چند IP داشته باشیم و یا اینکه از پورت ها غیر استاندارد استفاده کنیم. وقتی یک کلاینت همساز با Http v1.1 یک منبع (مثل یک صفحه اچ تی ام ال یا یک تصویر یا یک فایل صوتی) را از سرور درخواست می کند در حقیقت یک آدرس URL شامل نام DNS وب سایت حاوی آن مطلب را به سرور ارسال می کند . این نام را اصطلاحا Host Header می نامیم (مثلا www.yahoo.com) این هاست هدر به سمت سرور می رود و سرور آن را مورد بررسی قرار می دهد تا ببیند آیا با هیچ کدام از هاست هدر های تعریف شده ی خود مطابقت دارد یا خیر . در صورت عدم مطابقت با هیچ کدام ، خطای 404 صادر می کند.

در هنگام تنظیم یک وب سایت در IIS می توانیم یک یا چند ترکیب از IP + PORT TCP + Host Header داشته باشیم . هر یک از این ترکیبات به عنوان یک Identity برای آن وب سایت شناخته می شود. هر وب سایت حداقل یک Identity دارد و البته می توان تعدا بیشتری برایش تعریف کرد . ولی در هر حالتی باید حواسمان باشد که هر یک از Identity ها می بایست یکتا باشد . یعنی آنها را طوری تعریف نکنیم که یک Identityبرای چندین سایت مشترک باشد.

به طور خلاصه می توان گفت هر سایت می تواند چندین Identity داشته باشد ولی هر Identity فقط و فقط متعلق به یک سایت است. در غیر اینصورت IIS نخواهد دانست identity تعریف شده را به کدام وب سایت اختصاص دهد بنابر این خطای 404 صادر می کند.

در هنگام تنظیم identity قرار دادن هاست هدر اختیاری است . علاوه بر این برای آی پی می توان هم آی پی اختصاص داده شده به ماشین سرور مان را ست کنیم و هم می توانیم از گزینه all unsigned استفاده کنیم . در حالت دوم identityتعریف شده تمام درخواست های IP متصل نشده را در بر می گیرد.

وقتی مرورگری به IIS متصل می شود ، سرور می داند که مرورگر به کدام آدرس IP و شماره پورت وصل شده است ، از این رو می داند که کدام سایت را می خواهد . اگر شخصی به سرور IIS متصل شود و تقاضای HTTP آن شامل FQDN [1] وب سایت در هدرش نشود، IIS پروسس را متوقف کرده و به سادگی یک پیغام خطا ارسال می کند.

چرا این کارها را انجام می دهیم ؟ فکر کنید تمام اسکریپت کیدی ها و کرم های IIS بیرون آن هستند ، آنان از host header استفاده نمی کنند . انها فقط توسط یک IP و شماره پورت سرویس HTTP متصل می شوند . وقتی آنها به سرور IIS شما متصل می شوند به چه وبسایتی وصل می شوند؟ وبسایت پیش فرض. اما هیچ چیز قابل هکی آنجا وجود ندارد ! وبسایت پیش فرض توسط شما از بین رفته است.

6- نگاشت های نامستعمل را قطع کنید.

وقتی که یک درخواست HTTP برای یک فایل به IIS میرسد، IIS پسوند فایل مورد تقاضا را چک می کند. (مثلاً ASP. ، GIF. ، HTML. ، PHP . و...) اگر آن پسوند به یک مفسر نگاشت شده باشد، آنگاه آن فایل و

[1] fully Qualified Domain name

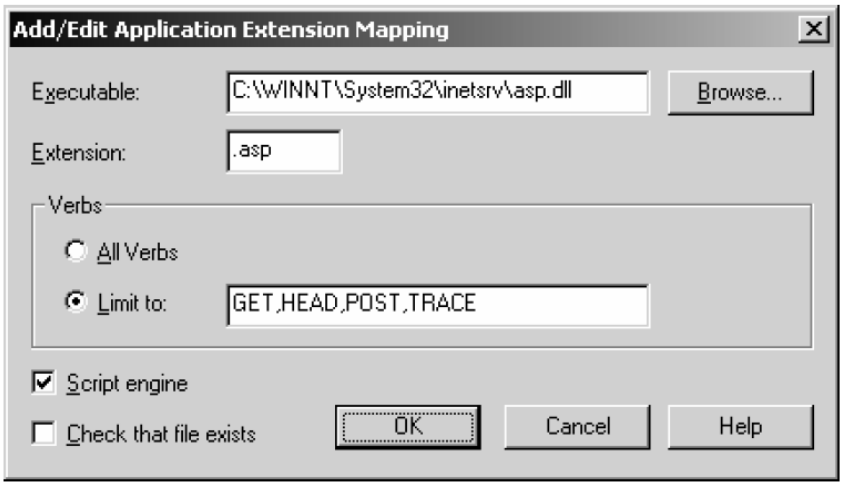
همه ی داده های درخواست، به مفسر تحویل داده می شود. خروجی پروسس، به صورت صفحه وب به مرورگر برگردانده می شود. این روشی است که ASP[1] ها و اسکریپت های CGI اجرا می شوند.

حال، از دیدگاه یک هکر شرایط متفاوت است. برای یک هکر، شما سرورتان را تنظیم کرده اید که به طور مطلق از افراد ناشناخته روی اینترنت ورودی دریافت کند و اجازه می دهید این ورودی ها به مرحله اجرا پاس داده شوند. این فایل های اجرایی معمولاً DLL هایی هستند که در فضای آدرس حافظه وب سرویس بار گذاری می شوند.(مثلا INETINFO. EXE یکی از کامپوننت های IIS است که برای debug کردن پروسس ها مورد استفاده قرار میگیرند.) در نتیجه، همه ی آن چیزی که یک هکر نیاز دارد انجام دهد تکه کردن ورودی به شکل درست برای نفوذ در حافظه، 100٪ کردن CPU utlization ، سرریز کردن بافر، و یک سری تأثیرات جانبی نامطبوع دیگراست.

برای ویرایش نگاشت پسوند به مفسر (extention_ to _ interpreter)، روی وبسایتتان راست کلیک کنید.

properties→Home Directory tab→Configuration button

صفحه property یک لیست از پسوند فایل ها در سمت چپ و مفسرهای متناظر با آنها در میان صفحه نمایش می دهد. خیلی ساده نگاشت هایی که از آن استفاده نمی کنید را حذف نمایید.



شکل 11- ویرایش نگاشت پسوند

برای مثال Code Red worm به نگاشت IDA. نیاز دارد، از شر آن خلاص شوید.

7- پوشه هایی که نباید داشته باشید.

شما نباید پوشه های زیر را داشته باشید یا مورد استفاده قرار دهید:

[1] Active server pages

Scripts - Cgibin – MSADC – Printers – IISHelp – IISSamples

اگر آنها را دارید حذف کنید یا تغییر نام دهید زیرا فولدرهایی که مشهور هستند و به طور پیش فرض برای برخی فایل ها ایجاد می شوند به سادگی توسط ابزارها و کرم ها یافت می شوند اما وقتی از نام دیگری استفاده کنید دفعه بعد کرم نمی داند در کجا تکثیر شود زیرا اطلاع ندارد شما فایل هایتان را کجا نگهداری می کنید.

8- پوشه root :

هر وب سایت باید یک root داشته باشد. در صورت امکان، اجازه اجرا در فولدر root را None کنید. برای تنظیم اجازه ی اجرا، روی پوشه راست کلیک کنید:

Properties →Home Directory tab → desired execute permissions.

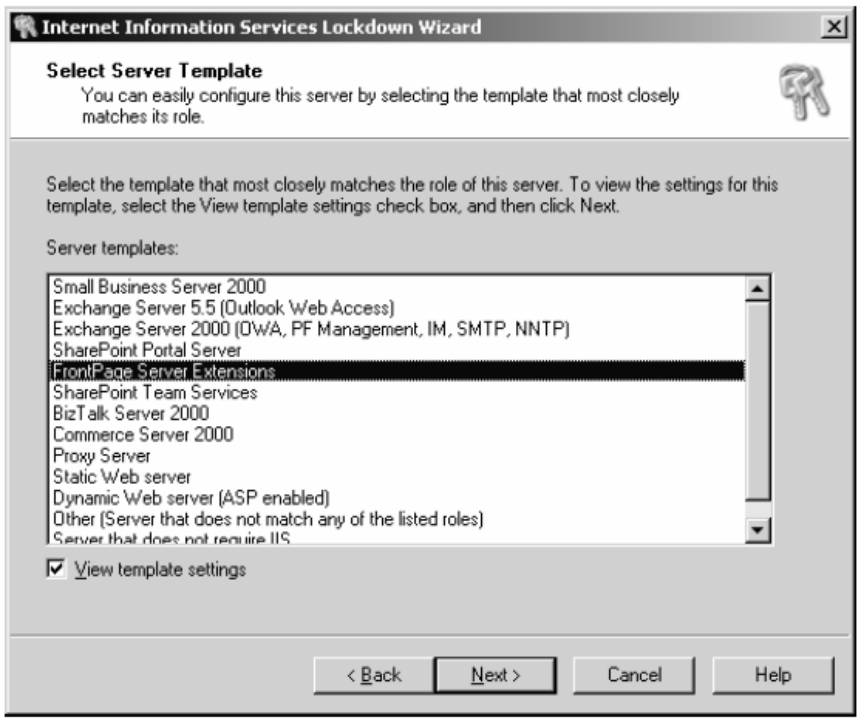
اسکریپت هایتان را در یک پوشه دیگر در پوشه root قرار دهید و اجازه اسکریپت را برای آن زیر پوشه فعال نمایید.

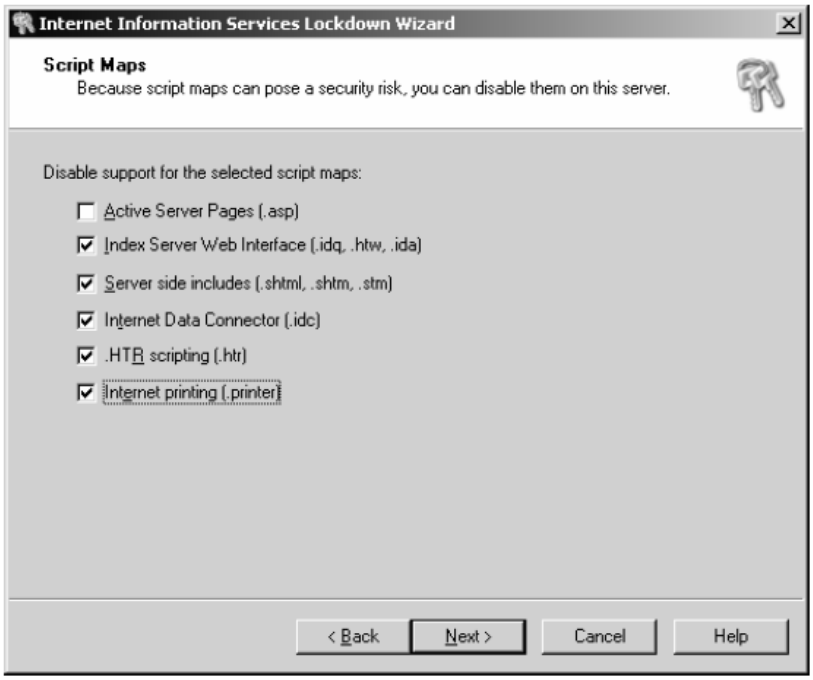
9- ابزار قفل IIS :

ابزار قفل IIS (IIS Lock down) یک ابزار سودمند Microsoft است که بسیاری از تغییرات امنیتی که بیان خواهیم کرد را پیاده سازی می کند. برای دانلود:

http://www.microsoft.Com/technet/security/tools/Locktools.asp

قابل استفاده در windows server 2003 , windows server 2003 Sp1





شکل 12-IIS Lockdown

IISLock Down به ورژن های اولیه IIS با انجام موارد زیر کمک می کند:

- جلوی غیر فعال شدن سرویس WWW را بعد از ارتقاء یافتن به Web Server هایی که اکنون در windows server 2000 و IIS 5.0 اجرا می شوند را می گیرد.

- با غیر فعال یا پاک کردن ویژگی های غیر ضروری که IIS 4.0 و IIS 5.0 ارائه می کند به امن ساختن Web server کمک می کند.

یادداشت: سرویس www بعد از تکمیل مراحل ارتقاء، IIS 4.0 را اجرا می کند.

پیکر بندی سرور با ابزار IIS Lock Down :

ابزار IIS Lock Down ، IIS موجود را با اجرای یک یا چند تراکنش زیر (که توسط کاربر مشخص می شوند) امن می کند:

*فعال یا غیر فعال کردن سرویس ها مانند سرویس www ، سرویس FTP، یا سرویس ساده ارسال ایمیل (SMTP)

*حذف سرویس هایی که غیر فعال شده اند.

*غیرفعال کردن اختیاری کامپوننت ها، شامل:

Index Server web interface
Server – Side includes (SSI)
Internet Data Connector (IDC)
Internet Printing

HTR Scripting
Web Distributed Authoring and Versioning (WebDAV)

*غیر فعال کردن دسترسی کاربران ناشناس به سرور با مسدود کردن موارد زیر:

1- اجازه اجرای DLL ها و فایل های اجرایی در OS

2- اجازه ی نوشتن در دایرکتوری همه ی سایت ها

*حذف دایرکتوری های مجازی غیرضروری، شامل

IIS Samples
Scripts
Microsoft Data Access (MDAC)
IIS Admin

*نصب UrLsean

*غیرفعال کردن Application های ASP فعال روی سرور

10- URL Scan.DLL ، دیواره آتش لایه Application:

URLScan درخواست های HTTP ورودی به وب سرور را بازرسی می کند و هر یک از الگوهای تنظیم شده در URL Scan توسط کاربر را بلوکه می کند. همچنین URL Scan همه ی تقاضاها را غربال می کند و اگر تقاضاها به هر شکل تهدیدآمیز باشند پیغام خطای 404 File Not Found را بر می گرداند.

ضوابط عدم پذیرش:

URL Scan می تواند بر اساس هر یک از ضوابط زیر درخواست های HTTP را رد کند.

- لغات استفاده شده در درخواست مثل : PUT, HEAD, GET و...
- پسوند فایل درخواست شده
- کاراکترهای دوبار کد شده مثل: " 252e % " ← " 2 e % " ← "."
- حضور کاراکترهای غیر اسکی در URL
- وجود تعداد بایت های بسیار زیاد در Header ها

به طور اختیاری، وقتی یک درخواست رد می شود اطلاعات مربوط به درخواست می تواند در یک فایل گزارش نوشته شود. هر ورودی به Log ، موارد تاریخ، ساعت، IP مبدأ، URL و توضیح در مورد علت رد درخواست لیست می شود.

URLScanیک ابزار تولید شده از سوی شرکت مایکروسافت میباشد که امکان کنترل و محدود نمودن انواع درخواستهای ارسالی به IIS را داراست. این ابزار میتواند از درخواستهای ارسالی که میتوانند امکان بالقوه ای برای

ایجاد خطر در سرویس دهنده باشند جلوگیری نماید. در حال حاضر URLScan از IIS نسخه 4 و نسخه های بالاتر پشتیبانی میکند. باید توجه داشت که استفاده از این ابزار بدون توجه و نصب بروزرسانها ، مکمل های امنیتی و سرویس پکهای منتشر شده نمیتواند کمک زیادی در امنیت سرویس دهنده شما داشته باشد.این ابزار شامل 2 فایل میباشد:Urlscan.dll و Urlscan.ini که بصورت فشرده در فایل urlscan.exe قایل دریافت برای نصب در سرویس دهنده میباشد.

برخی از امکاناتی که در حال حاضر در urlscan گنجانده شده است:

-امکان گزارش گیری (logging) از آدرسهای URL طولانی ارسال شده در نسخه های اولیه از این ابزار امکان ثبت آدرسها تنها تا 1024 بایت اولیه آنها فراهم بود ولی در حال حاضر امکان گزارش گیری یک ادرس طولانی تا 128 کیلوبایت فراهم شده است.بدین ترتیب مشکل ثبت آدرسهایی که از کدهای UTF-8 استفاده میکنند و بسیار طولانی میشوند حل شده است.

-کنترل حجم درخواستها

با استفاده از این امکان میتوان اندازه درخواستهای رسیده را کنترل نمود و یک روند عالی برای کنترل URL ها بر اساس حجم انها به بایت تنظیم کرد.

-امکان تغییر در محل ثبت گزارشهایurlscan

شما میتوانید ابزار را به نحوی پیکربندی نمایید تا گزارشات را در محلی که شما میخواهید ذخیره نمایید.

-محدودیت در پسوندهای درخواستی

امکان تعریف ممنوعیت برای پسوندهای مورد نیاز. با استفاده از این قابلیت مدیر سرور قادر به اعمال محدودیت بر روی درخواستهای URL که دارای فایلها با پسوندهای خاصی میباشند ، خواهد بود.

-محدودیت در درخواستهایWebDav

برخی ار کدهای WebDav قادر به انجام افعال خاصی در سرویس دهنده HTTP میباشند. با استفاده از این قابلیت میتوان برروی اعمالی که کاربران با استفاده ار کدهای WebDav قادر به انجام میباشند محدودیت اعمال نمود.

-محدودیت در سرآیندها

برخی از کدهای WebDav قادرند با استافده از سرآیندهای خاص به سرویس دهنده آسیب برسانند. با استفاده از این امکان URLScan میتواند برروی این سرآیندها محدودیت لازم را اعمال کرد.

-مقابله با درخواستهای پی در پی

درخواستهای پی در پی همانند ، یکی از روشهای موجود در حملات بر پایه وب میباشد. کـه بوسـیله ایـن ابـزار براحتی قابل کنترل میباشد.

-کنترل تعداد نقطه ها در آدرس ورودی

بـا اسـتفاده از ایـن امکـان میتـوان تعـداد نقطـه هـا (dot) را در آدرس URL ورودی کنتـرل نمـود.

-حذف سرآیند سرویس دهنده

این امکان اجازه پنهان نمودن سرآیند سرور را میدهد تا کار برای شناسایی نسخه های مـورد اسـتفاده سـختتر گردد.

نحوه نصب و راه اندازی:

بـــرای نصـــب کافیســـت فایـــل ایـــن برنامـــه را دریافـــت و بـــر روی آن 2 بـــار کلیـــک نماییـــد. با اجرای این فایل 3 بخش ایجاد میشود:

urlscan.dllکه باید بصورت زیر دسترسی آن تنظیم گردد:

read , execute : LocalService, IIS_WPG , NetworkService
full control: Administrators, LocalSystem

urlscan.iniکه باید بصورت زیر دسترسی آن تنظیم گردد:

read , execute : LocalService, NetworkService
full control: Administrators, LocalSystem

logsکه باید بصورت زیر دسترسی آن تنظیم گردد:

read , execute : LocalService, IIS_WPG , NetworkService
full control: Administrators, LocalSystem

11- امنیت Web Application :

یک Web Application یک سری از اسکریپت ها و فایل های اجرایی روی وب سرور است که بـا هـم دیگـر یک سرویس را ارائه می دهند مانند خواندن یا ارسال ایمیل، مـدیریت حسـاب بـانکی، خریـد و فـروش سـهام و یـا مدیریت یک بانک اطلاعاتی منابع انسانی در SQL Server

کد گذاری SSL :

کد گذاری Secure Sockets Layer (SSL) می تواند همه ی داده هایی که بین مرورگر و سرور منتقل می شوند را رمز کند. سرور و مرورگر با تکیه به پروتکل SSL یک کانال کد گذاری شده واحدی را جهت یک ارتباط شخصی و محرمانه فراهم می نماید.

پس از برقراری اتصال امن، SSL اطلاعات را به وسیله دو کلید رمز نگاری می کند، کلید عمومی برای اشخاص سوم شخص قابل خواندن است اما کلید دوم تنها توسط ارسال کننده و دریافت کننده داده قابل استفاده است. کلید عمومی جهت رمز گذاری اطلاعات و کلید شخصی جهت کشف رمز مورد استفاده قرار می گیرند. زمانی که یک مرورگر به یک دامنه امن انتقال پیدا می کند سطحی از رمز گذاری بر اساس نوع گواهی SSL و به همان اندازه گنجایش سرور و سیستم عامل، دایر می گردد.

کد گذاری قدرتمند 128 بیت، مرتبه توانایی محاسبه بیشتری نسبت به ترکیبی از کدگذاری 40 بیت دارد یعنی بیش از یک ترلیون ترلیون مرتبه قویتر.

با سرعت کنونی کامپیوترها، یک هکری که از ابزارها و انگیزه های مناسب برخوردار است به بیش از یک ترلیون سال زمان برای شکستن بخش حمایت شده توسط گواهی SGC فعال شده، نیاز دارد.

گواهی نامه رانندگی، پاسپورت، کارت ملی و ... شناسنامه هایی برای احراز هویت می باشد. گواهی های SSL، شناسنامه ای در دنیای آنلاین می باشند که منحصراً برای یک دامنه ویژه یا وب سایت از سوی صادر کننده گواهی SSL، صادر می گردد زمانی که یک مرورگر با سرور اتصال برقرار می کند، سرور اطلاعات هویتی را برای مرورگر ارسال می نماید برای دیدن شناسنامه مراحل زیر را طی نمایید.

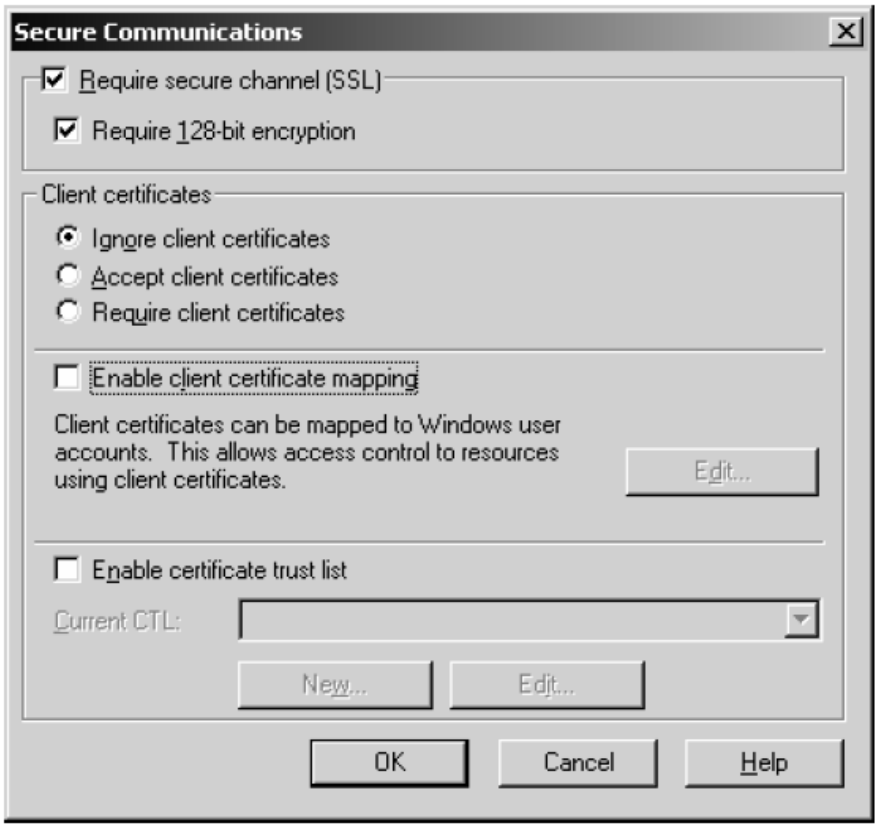
- ♦ بر روی قفل امنیتی در پنجره مروگر کلیک کنید.
- ♦ به دنبال نشان امنیتی در وب سایت بگردید و بر روی آن کلیک کنید.
- ♦ به منطقه سبز رنگ در آدرس بار توجه نمایید.

تنها گواهی های SSL با درجه امنیت بالا و اعتبار سازی توسعه یافته، نام سازمان شما را در قسمت سبز رنگ آدرس بار به نمایش می گذارد.

بعد از نصب یک گواهی نامه دیجیتال می توانید کد SSL را روی هر فایل یا پوشه قرار دهید . برای این کار روی آن آیتم راست کلیلک کنید :

properties→security tab→Bottom Edit batton

باکس Require Secure channel را چک دار کنید و دوبار OK کنید.



شکل 13-تنظیمات گواهی نامه دیجیتال

هر گاه اهراز هویت نیاز باشد SSL باید استفاده شود . همچنین SSL باید برای ارسال هر نوع اطلاعات شخصی استفاده شود مثل شماره کارت اعتباری یا تاریخ تولد.

نکات ایمنی برای SQL Server 2000

بسیاری از وب سرورها از چشم پایگاه داده SQL Server پشت آنها ، front –end به نظر می رسند.

- از نصب SQL روی IIS بپرهیزید SQL Server را پشت فایروال و یا در یک زیر شبکه جدا قرار دهید همه دسترسی های خارجی به سرور پایگاه داده را بلوکه کنید، مخصوصاً پورت های 1433,1434.
- برای ورود به ادمین SQL Server یک کلمه عبور طولانی و تصادفی انتخاب کنید.
- از اهراز هویت Integrated windows استفاده کنید .

- به IIS اجازه ندهید که دستورات SQL را به صورت خام به سرور پایگاه داده ارسال کند.

- روی SQL Server تان یک اسکنر هشدار دهنده آسیب پذیری نصب کنید مانند Microsoft Baseline Security Analyzer، که ضعف ها را مشخص و تصحیح کند.

Microsoft Baseline Security Analyzer (MBSA) یک ابزار ساده برای کمک به کسب و کارهای کوچک و متوسط است تا بتوانند براساس پیشنهادات امنیتی مایکروسافت ، سطح امنیت خود را تعیین نمایند.

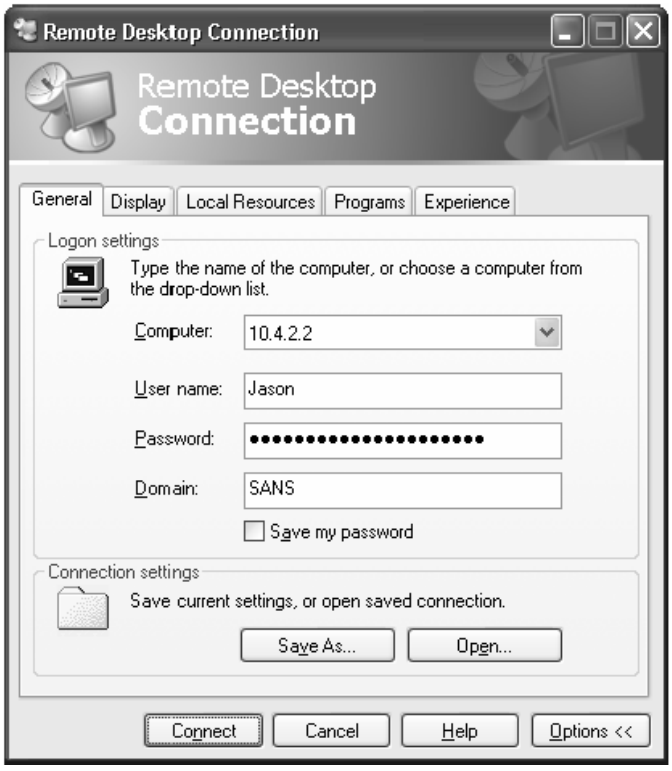
کاربرانی که محصولات زیر را دارند می توانند برای دست یافتن به امنیت کامل از MBSA استفاده نمایند:

-Office 2000
-ISA server2000
-front page server Extensions 2000/2002
-visual studio.Net2002/2003
-SQL server 7.0/2000

سرویس های پایانه ای(terminal) و Remote Desktop

سـرویس هـای ترمینـال امکـان دسترسـی از راه دور بـه Virtual desktop اجـرا شـده روی ویـنـدوزهای 2003,xp,2000 را فـراهم مـی آورنـد. ایـن شـبیه بـه symantec pc Anywhere یـا VNC (Virtual Network Computing) می باشد که یک کامپیوتر راه دور را روی یک پنجره Application شما ظـاهر مـی سازد. با این تفاوت که شما به خود کامپیوتر متصل نمیشوید بلکه به یک کـامپیوتر مجـازی کـه در حافظـه RAM سرور مخفی شده است وصل می شوید.

www.realvnc.com
www.symantec.com/pcanywhere



شکل Remote Desktop-14

VNC امکان اتصال به دسکتاپ گرافیکی را توسـط پروتکـل TCP/IP ، پروتکـل اسـتاندارد اینترنـت، فـراهم می‌کند. VNCاز دو بخش تشکیل شده است :

سرور و بخش ناظر(viewer) . سرور روی ماشینی که از راه‌دور به آن متصل می‌شوید نصب شده‌است و بخـش ناظر نیز روی سیستمی که دسترسی توسط آن صورت خواهد گرفت، نصب مـی‌شـود. RealVNC بخـش سـرور را برای ویندوز و یونیکس تهیه کرده است؛ سرور برای سایر سکوها. برای مثال MAC OSتوسط شرکت‌های دیگری ساخته شده است.

به‌رغم آن‌که VNC رایگان احراز هویت ابتدایی را انجام می‌دهد، ارتباط میان کلاینت و سرور بدون رمزگذاری برقرار می‌شود. اما می‌توانید ارتباط میان آن‌ها را با برنامه‌هایی نظیر SSH که در اصل با تغییر مسیر (یا تونل زدن) به صورت واسطی بین کلاینت و سرور عمل می‌کند، رمزگذاری کنید .

در واقع به‌جای آن‌که به صورت مستقیم به برقراری ارتباط با سرور بپردازید، ناظر VNC با کلاینت SSH محلی ارتباط برقرار می‌کند، SSHمحلی نیز با سرور راه‌دور ارتباط برقرار می‌نماید و پیام را به آن می‌رساند. دست آخر SSH سرور ارتباط را با VNC سرور برقرار می‌نماید. برای انجام‌دادن این فرایند به یک کلاینت و سرور SSH نیاز دارید. MAC OS براساس یک هسته یونیکس ساخته شده است (بر پایهBSD)

قابل توجه است که VNC یک جلسه (Session)جداگانه برای کاربر نمی‌گشاید، بلکه در واقع اجازه کنترل هر آنچه روی دسکتاپ / صفحه نمایش در حال اجرا باشد را از راه‌دور به شما می‌دهد.

- سرویس های ترمینال روی ویندوز سرور 2003/2000

وقتی که سرویس های ترمینال نصب شد، شما باید licensing mode آن را انتخاب نمایید : remote administration یا application sever. اگر application sever را انتخاب نماید هر یوزر می تواند متصل شود اما یک گواهی مخصوص از مایکروسافت نیاز دارد. اگر remote administrator را انتخاب نماید نیازی ندارید هیچ گواهی دیگری بخرید ، اما فقط ادمین می تواند وصل شود .

دستیابی به سخت افزار از راه دور:

با پیدایش و آغاز به کار ترمینال سرویس ها در ویندوز NT به دلایلی چون عدم پشتیبانی شبکه های آن دوران از برنامه های کاربردی پرترافیک و همچنین عدم وجود سرورهای قدرتمند، امکان اجرای چندین نشست (Session)به صورت همزمان وجود نداشت. اما امروزه با قدرتمند تر شدن سرور ها و قابلیت اجرای همزمان چندین سیستم عامل و سرعت بالا در شبکه ها، می توانند به خوبی از عهده میزبانی نشست های ترمینال سرویس بر آیند.

مجازی سازی دسکتاپ (DVI) درWindows Server 2008 R2

ویندوز سرور 2008 امکان مجازی سازی کامل دسکتاپ (DVI) را برای مدیران سازمان ها ایجاد کرده است. به این معنی که ترمینال سرور می تواند به منظور میزبانی از دسکتاپ های مجازی، پیکربندی شود. در این حالت زمانی که کاربران از سرور log off می کنند، هارد مجازی سرور به حالت اولیه و دست نخورده بر می گردد و برای استفاده توسط کاربر بعدی آماده می شود.

امکان ایجاد دسکتاپ های مجازی اختصاص یافته

به طور کلی یکی از راهکارهای اختصاص ماشین های مجازی به کاربران نهایی، طراحی مخزنی از دسکتاپ های مجازی (Virtual desktop pool) می باشد که در آن به ازای هر کاربر یک دسکتاپ مجازی (یکسان با دیگر کاربران) ساخته می شود و هر کدام به صورت موقت به یک ماشین مجازی (Virtual Machine) مرتبط می شوند. از آنجایی که در این راهکار کاربران اجازه اعمال تغییرات در دسکتاپ مجازی را ندارند، بعد از هر جلسه DVI، ماشین مجازی بدون ذخیره تغییرات، به مخزن بر می گردد و آماده استفاده توسط کاربر دیگری می شود. اگر چه این یک روش کارآمد است، اما وجود نیازهای تجاری سازمان ها، ایجاب می کنند که اجازه اعمال تغییرات معینی روی دسکتاپ مجازی به برخی کاربران داده شود. در چنین مواقعی ویندوز سرور 2008 R2 قابلیت ارائه یک دسکتاپ مجازی اختصاصی (Dedicated) به کاربران را به منظور اعمال تغییرات مورد نیاز در دسکتاپ مجازی خود، فراهم آورده است.

امکان میزبانی از برنامه های کاربردی اختصاص یافته به جای کل دسکتاپ مجازی

یکی از خصوصیات پر کاربرد ویندوز سرور 2008، برنامه کاربردی از راه دور (RemoteApp) می باشد. بدین ترتیب که به جای مجازی سازی کل دسکتاپ، برنامه کاربردی اختصاص یافته را مجازی می کنید. نه تنها با این روش، منابع کمتری از سرور اشغال می شود، بلکه به مدیران اجازه می دهد که بدون وابستگی به محیط کلاینت به مدیریت برنامه های کاربردی بپردازد.

افزایش طول عمر سخت افزار دسکتاپ

سازمان ها می توانند با ترمینال سرویس ها، طول عمر کامپیوتر های رومیزی خود را افزایش دهند. از آنجایی که همه پردازش ها در پایانه سرور رخ می دهد، اصولا دسکتاپ ها نقش ترمینال های غیر هوشمند را دارند و این بدین معنی است که با استفاده این چنینی از دسکتاپ ها، طول عمر آنها نسبت به اجرای برنامه ها به صورت محلی در آنها، بیشتر و با دوام تر خواهد بود. به همین ترتیب با اجرای برنامه ها روی یک ترمینال سرور، با خریداری حداقل سخت افزار، نسبت به حالتی که ترمینال سرور وجود ندارد؛ هزینه ها به مقدار زیادی کاهش می یابد.

امکان دسترسی کاربران به " کامپیوتر کاری " خود از هر مکانی

پشتیبانی از کاربرانی که مجبورند خارج از محیط کاری خود فعالیت کنند، امر تازه ای نیست، اما می دانیم که نگهداری و به روزکردن کامپیوتر های سیار چالش برانگیز است. به همین خاطر با پیاده سازی یک محیط ترمینال سرویس، کاربران از راه دور و صرف نظر از اینکه داخل شرکت هستند یا در سفر، می توانند وظیفه شغلی خود را بدون هیچ مشکلی به انجام رسانند. در واقع با استفاده از کامپیوترهای داخل و خارج از محیط کار، می توانند تجربه و عملکرد یکسانی داشته باشند.

آسان تر شدن تعمیر، نگهداری و به روز رسانی برنامه ها

در محیط ترمینال سرویس، برنامه ها، به جای نصب روی کامپیوتر های شخصی افراد، روی یک ترمینال سرور نصب می شوند. در نتیجه به دلیل اینکه تنها یک کپی از نرم افزار وجود دارد، ترمیم و به روز رسانی برنامه ها بسیار آسان تر و روی ترمینال سرور انجام می شود و مجبور نیستید که روی تک تک کامپیوتر های شخصی تغییرات لازم را اعمال کنید.

امنیت بالای کامپیوتر های شخصی رومیزی

چون ترمینال سرویس ها میزبان برنامه های کاربردی یا نشست های دسکتاپ مجازی هستند، هیچ نیازی به نصب برنامه ها روی کامپیوتر های شخصی نمی باشد و همه برنامه های کاربردی یا نشست ها روی سرور قابل اجرا است، به همین علت کامپیوتر های شخصی افراد کمتر در معرض خطر و حمله قرار می گیرد.

آسان تر شدن تامین و نگهداری دسکتاپ

وقتی که یک سازمان با ترمینال سرویس ها سازگار شده است، کامپیوتر ها به کمترین تنظیمات برای پیکربندی نیاز دارند..همین امر فرآیند تامین و نگهداری دسکتاپ را ساده تر می کند. به عنوان مثال فایل های عکس کوچکتر می شوند و نیازی به تست سازگاری برنامه ها روی دسکتاپ نمی باشد.

فراهم شدن امکان حذف نرم افزار مدیریت دسکتاپ

نمونه های زیادی از سازمان هایی را در دنیای واقعی می توان سراغ گرفت که بعد از پیاده سازی سرویس های ترمینال، تصمیم به حذف نرم افزار مدیریت دسکتاپ خود گرفته اند. آنها در ابتدا به منظور نگهداری از موجودی سخت افزار و نرم افزار در سازمان خود، اقدام به خریداری نرم افزار مدیریت دسکتاپ کرده اند. و چون فروشنده متعهد به پشتیبانی و نگهداری سالیانه است، استفاده از نرم افزار باعث صرف هزینه های ثابت و مداوم سازمان می شدند. با پیاده سازی محیط ترمینال سرویس ها، نیاز به نرم افزار مدیریت دسکتاپ از بین رفت. بنابراین حذف نرم افزار مدیریت دسکتاپ، کاهش هزینه های سازمان را به دنبال دارد.

پروتکل Remote desktop(RDP)

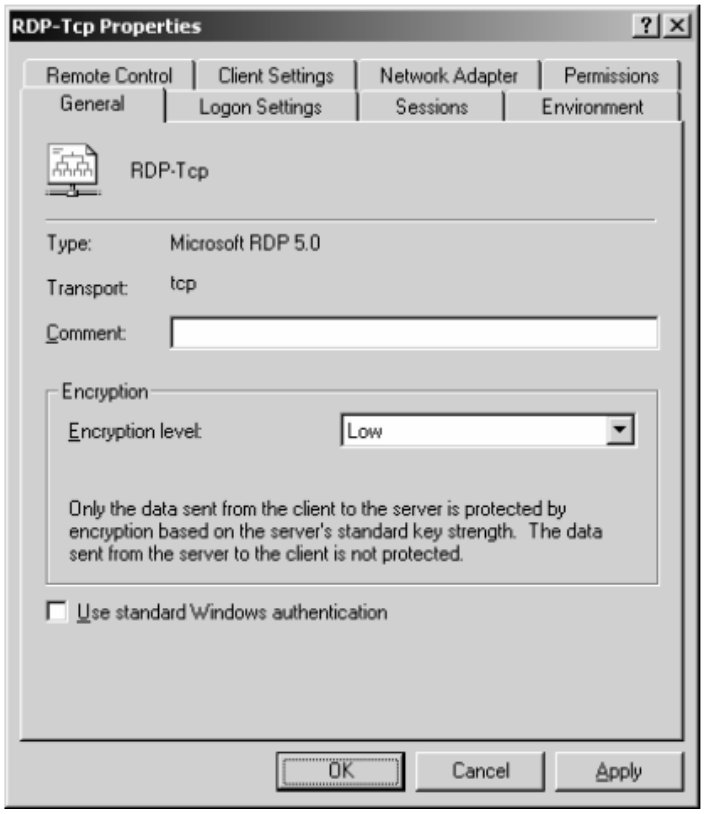
سرویس های ترمینال و Remote desktop هر دو از پروتکل Remote Desktop روی پورت 3389 TCP استفاده می کنند. سرویس های ترمینال در ویندوز سرور 2003و2000 باید کد گذاری سنگینی مورد استفاده قرار دهند . سه نوع تنظیمات روی سرور ممکن است :

1- کم : کدگذاری 56 بیتی RC4 روی اطلاعات فرستاده شده به سرور ترمینال شامل کلمه های عبور

2- متوسط (پیش فرض): کد گذاری 56 بیتی RC4 روی همه اطلاعات

3- زیاد : کد گذاری 128 بیتی RC4 روی همه اطلاعات

بصورت پیش فرض پروتکل RDP پکت های رد و بدل شده بین کلاینت و سرور را رمزنگاری می کند. این رمزنگاری بر مبنای RC4 بنا نهاده شده است. رمزنگاری که در این پروتکل جا داده شده است قوی و قابل اطمینان می باشد .



شکل 15-تنظیمات RDP

اما این پروتکل یک ضعف عمده دارد. در صورتی که هکری خود را در بین دو سیستمی قرار دهد که می خواهند RDP برقرار کنند می تواند ترافیک رد و بدل شده بین دو سیستم را بخواند. چون در این سناریو هکر به کلاینت می قبولاند که سرور است. در نسخه های قبلی RDP هیچ راهی وجود نداشت که بتوان هویت سرور را تایید کرد. تا زمانی که RDP 6.0 به همراه ویندوز ویستا ارائه شد از Network Level Authentication و TLS 1.0پشتیبانی کرد. در این حالت کلاینت و سرور قبل از اینکه ارتباطی را برقرار کنند یکدیگر را Authenticate می کنند. این باعث می شود که فرآیند استفاده از RDP بسیار امن تر شود.

این قابلیت ها در RDP 7.0 که به همراه ویندوز ۲۰۰۸ R2 و ویندوز ۷ ارائه شد نیز پشتیبانی می شود.

در صورتی که شما از سرور های ۲۰۰۸ به بالا در ساختار خود استفاده کنید احتمالا در هنگام remote کـردن به آن سرور این پیام را زیاد دیده اید:

The identity of the remote computer cannot be verified. Do you want to connect anyway?

در این قسمت بـه شـما اعـلام مـی کنـد کـه سیسـتم شـما نمـی توانـد کـامپیوتری را کـه بـه آن وصـل مـی شوید Authenticate کند.

اساس این Authentication بر PKI یا Publick Key Infrastructure پیاده سازی شده اسـت. در ایـن روش کلاینت می تواند ارتباط خود را بر اساس TLS و certificateارائه شده از طرف سرور برقرار کند. چون این certificateاز محل معتبری صادر شده است هویت سرور را نیز تایید می کند.

برای تنظیم کردن این قابلیت کافی است که از CA سروری که راه اندازی کرده ایـد یـک certificate بـرای کامپیوتر خود دریافت کنید. حال کافی است که سرور و کلاینتی که می خواهند وصل شوند به ایـن CA Server اعتماد داشته باشند.

بهبود کارایی RDP:

1- آخرین سرویس پک ها و hotfix ها را به کار گیرند.

2-ترافیک ناخواسته روی پورت TCP/3389 را درفایروال بلوکه کنید.

3-در سرور از کد گذاری 128 بیتی RDP استفاده کنید.

4-وقتی اطلاعات حساس است به جای کدگذاری RDP از IPSec یا یک VPN استفاده کنید.

5-برای دعوت نامه Remote Assistance از کلمه عبور و TTL کوتاه استفاده کنید.

منابع

1- Securing windows network services , SECBK_55_1203

2- http://www.mrfi.ir/

3- http://www.ircert.com

4- http://technet.microsoft.com/en-us/library/cc738967(v=ws.10).aspx

5- http://esecurity.ir/index.php

6- http://www.srco.ir

7- Wireless Hacking, Mohammad Mosafer2005-2006

8- http://msdn.microsoft.com/library/default.aspx