بسم الله الرحمن الرحیم

معرفی ۱۰۰ ابزار برتر امنیت و شبکه

ویرایش اولیه .....

1. Nessus

خصوصیات:

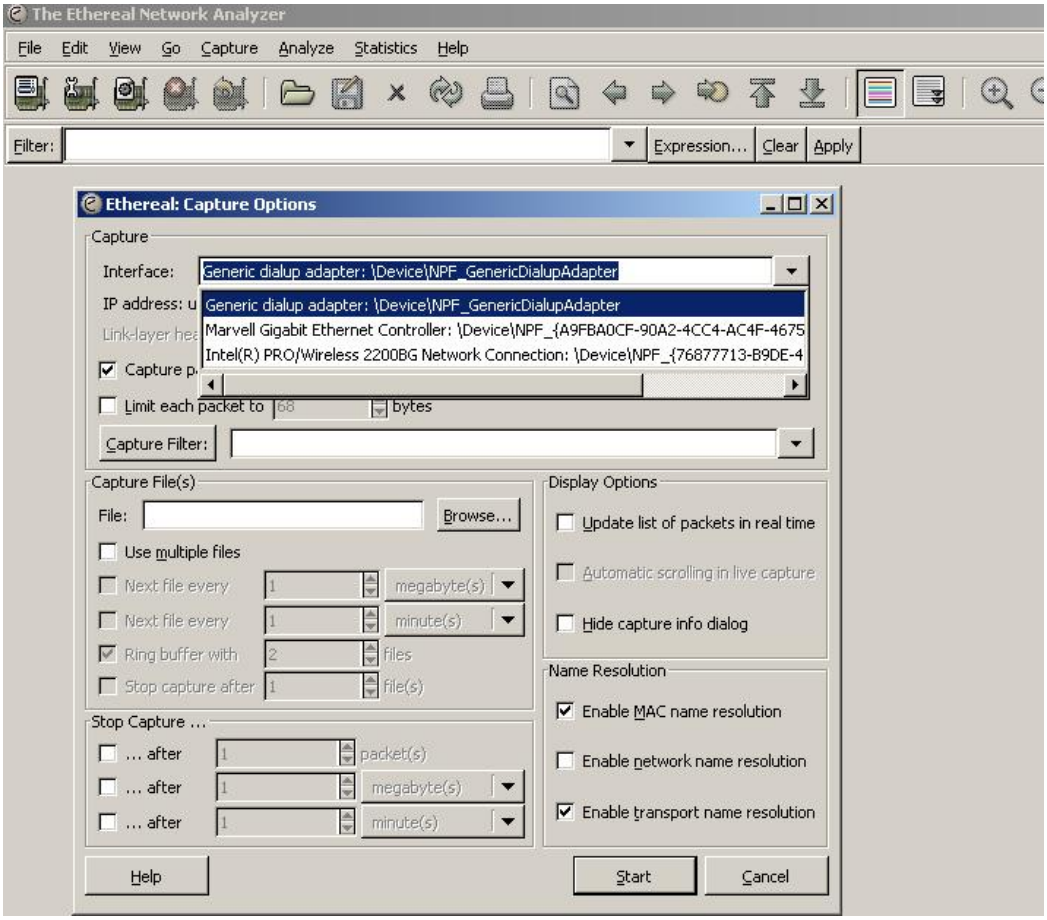
این نرم افزار که به جرأت می توان گفت قوی ترین اسکنر نقاط ضعف امنیتی در شبکه های کامپیوتری است، قابلیت تست حملات گوناگون در لایه های مختلف شبکه به همراه ارائه توضیحات مناسب در مورد حمله کشف شده در شبکه که در زیر نمونه ی آن را مشاهده می کنید از نقاط قوت این اسکنر می باشد.

این اسکنر در حال حاظر حاوی بیش از 11500 تست مختلف امنیتی می باشد، که بررسی تمام این مشکلات، خود دلیلی بر سریع نبودن آن باشد.
از مزایای دیگر این ابزار قوی، قابلیت کار در هر دو صورت Local و کلاینت/سرور می باشد.

2.WinShark(Ethereal)

خصوصیات: 

این ابزار بسیار کارآمدی است که از دسته اسنیفرها و تحلیلگران اطلاعات در حال ردوبدل شدن در شبکه بشمار می آید، کمتر شخصی را در زمینه امنیت می توان یافت که از کار با این نرم افزار ناراضی باشد و ترجیح دهد که کارهای خود را با ابزار دیگری به پیش برد، زیرا که این ابزار به شما این اجازه را می دهد که هرگاه احساس کنید به چیزی در رابطه با تحلیل پروتکل های شبکه احتیاج دارید که در این نرم افزار تعبیه نشده است.
می توانید خود دستبکار شده و ماژول آن را نوشته و به سادگی درون امکانات این ابزار جای دهید. برای آشنایی بیشتر با اینترفیس بسیار کارآمد و User-Friendly آن تصویری از این برنامه را در زیر قرار داده ایم.



Snort .3

خصوصیات:

IDS کدباز مورد علاقه همه!.

از سبکترین سیستم های تشخیص و جلوگیری از حملات است که قابلیت ثبت وقایع در شبکه های مبتنی بر IP می باشد. تحلیل پروتکل و جستجو در وقایع ثبت شده، شناسایی بیش از هزار کرم مخرب، تشخیص پورت اسکن، حمه از طریق برنامه های مخرب و ... از قابلیت های بیشمار این سیستم تشخیص نفوذ می باشد.

NETCat .4

خصوصیات:

نام بردن از این نرم افزار به عنوان چاقوی سویسی شبکه بیهرا ه و اشتباه نیست، زیرا هرگاه به مشکلی برخورد کنید که نرم افزارهای گران قیمت که برای شبکه خود خریداری کرده اید قادر به برطرف کردن آن نباشد، می توانید تا حدود زیادی بر روی این ابزار کارآمد حساب کنید.

می توانید از این نرم افزار به عنوان تست باز بودن پورت، پذیرفتن ارتباط از از محلی دیگر، به گوش بودن بر روی پورت خاص برای دریافت ارتباط و اطلاعات و همچنین قابلت استفاده به عنوان Honey pot و چندین قابلیت دیگر از موارد استفاده این ابزار می باشد.

در زیر قسمت Help این نرم افزار را می بینید:

```
[v1.11 NT www.vulnwatch.org/netcat/]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, background mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

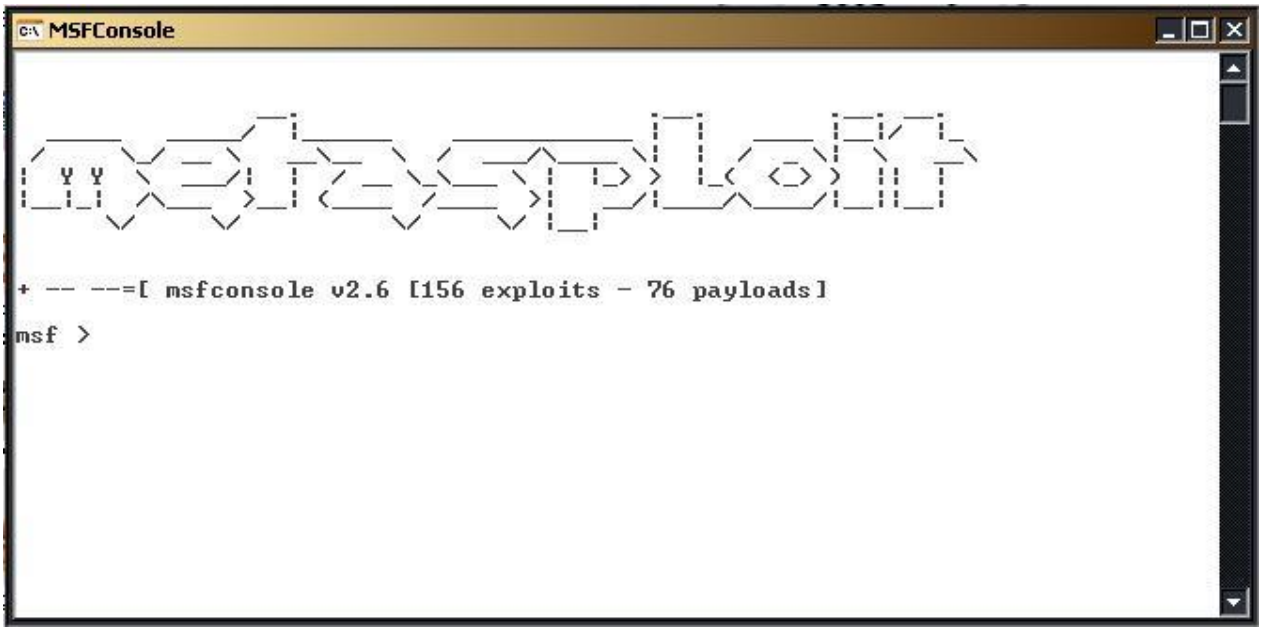
Metasploit Framework .5

خصوصیات:

با استفاده از این برنامه می توانید کدهای مخرب (اکسپلویت) را بر روی سیستم هایی که نقاط ضعف آنها با استفاده از این کدها اجازه دسترسی به سیستم هدف را ایجاد می کند، را اجرا کنید.این نرم افزار را می توان تحت خط فرمان (CMD) و همچنین تحت وب اجرا کرد، که البته بااینکه استفاده از این نرم افزار تحت وب بسیار ساده می باشد اما معمولا کار با این نرم افزار

تحت خط فرمان پاسخ های بهتری را ارئه می کند.نسخه آنلاین این نرم افزار در آدرس http://metasploit.com:55555/ قرار دارد. قابلیت بروز رسانی نیز از جمله امکانات این ابزار برای بروزرسانی کدهای خود می باشد.

تصویر این نرم افزار برای آشنایی شما در زیر آورده شده است.



Hping2 .6

خصوصیات:

با استفاده از قابلیت های این نرم افزار می توانید پکت های ICMP, TCP و UDP را با پارامترهای دلخواه خود ساخته و راهی شبکه و یا سیستم هدف کنید، البته کارایی اصلی این نرم افزار برای تغییر پارمترهای پکت ها به منظور فریب دایواره های آتش می باشد.

این نرم افزار بصورت کدباز قابل دانلود می باشد، جالب است بدانید که در حملات مسوم به Land Attack خود این نرم افزار به تنهایی توانایی انجام اینکار را دارا می باشد و به هیچ ابزار دیگری برای انجام این حمله نیاز ندارید.

در تصویر زیر قسمتی از Help مربوط به این نرم افزار را مشاهده می کنید.

```
usage: hping host [options[
- h  --help      show this help
- v  --version   show version
- c  --count     packet count
- i  --interval  wait (mX for X milliseconds, for example -i m10(
--      fast      alias for -i m100 (10 packets for second(
- n  --numeric   numeric output
- q  --quiet     quiet
- I  --interface interface IP (otherwise default routing interface(
- V  --verbose   verbose mode
- D  --debug     debugging info
- z  --bind      bind ctrl+z to ttl          (default to dst port(
- Z  --unbind    unbind ctrl+z
Mode
  default mode     TCP
--  ٠- rawip      RAW IP mode
--  ١- icmp       ICMP mode
--  ٢- udp        UDP mode
--  ٨- scan       SCAN mode.
                Example: hping --scan 1-30,70-90 -S www.target.host
--  ٩- listen     listen mode
IP
- a  --spoof      spoof source address
--  rand-dest      random destination address mode. see the man.
--  rand-source    random source address mode. see the man.
- t  --ttl        ttl (default 64(
- N  --id         id (default random(
- W  --winid      use win* id byte ordering
- r  --rel        relativize id field          (to estimate host traffic(
- f  --frag       split packets in more frag.  (may pass weak acl(
- x  --morefrag   set more fragments flag
- y  --dontfrag   set dont fragment flag
- g  --fragoff    set the fragment offset
```

7. Kismet

خصوصایت:

یکی از قویترین ابزارهای استراق سمع بر روی شبکه های بیسیم تحت پروتکل 802.11 و قابلیت شناسایی، استراق سمع و سیستم تشخیص نفوذ از لایه 2 شبکه می باشد.قابلیت شناسایی شبکه های مخفی بیسیم نیز در این نرم افزار وجود دارد.

8. Tcpdump

خصوصیات:

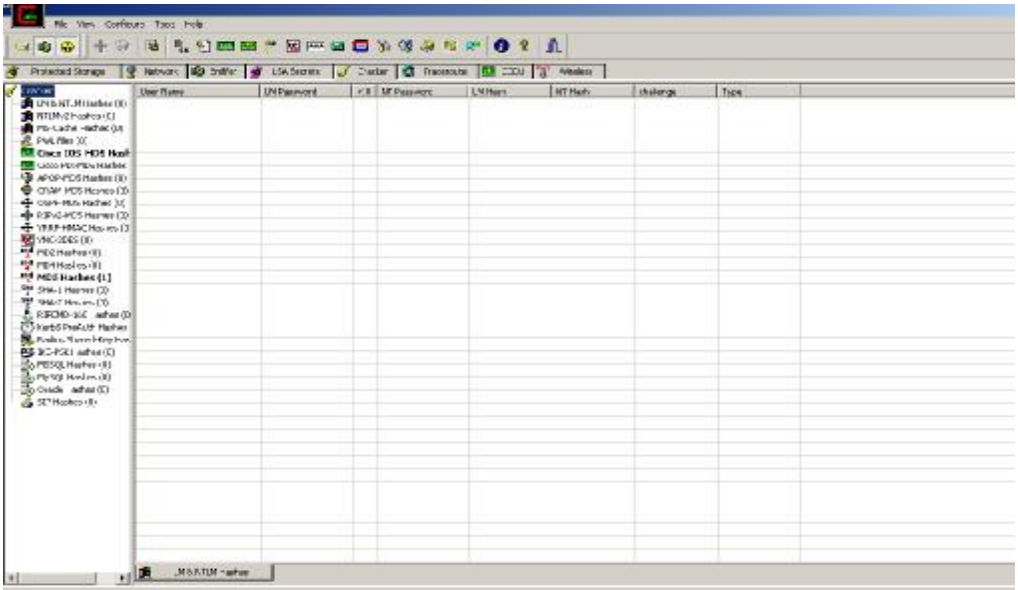
این نرم افزار نیز جزو ابزارهای استراق سمع می باشد، نسبت به Ethereal از قابلیت های کمتری برخوردار است اما به مراتب منابع کمتری از سیستم را به خود اختصاص می دهد.

Cain and Abel.9

خصوصیات:

شاید بتوان این نرم افزار را یکی از کاملترین و جامع ترین نرم افزارهای امنیتی شبکه دانست. به غیر از کشف نقاط آسیب پذیری، کمتر کاری باشد که بخواهید در شبکه انجام دهید که این نرم افزار نتواند از پس آن برآید.

کارهایی مانند: استراق سمع پروتکل های `FTP, Http, Imap,POP3` و چندین پروتکل دیگر، توانایی انجام حملات `ARP` ، استراق سمع `VOIP` ، استراق سمع شبکه های بیسیم و رمزگشایی انواع پسوردهای `MD5` و `Hash` از جمله قابلیت های بیشمار این نرم افزار-البته رایگان- می باشد. رابط گرافیکی این نرم افزار را در زیر مشاهده می کنید:



John the Ripper .10

خصوصیات:

توانایی های این نرم افزار شما را قادر می ساز که انواع رمزنگتری ها مانند:

MD5, HASH, LM, DES, 3DES را رمزگشایی کنید.

تشخیص نوع رمزنگاری در این ابزار بصورت خودکار بوده و با استفاده از الگوهایی که از انواع رمزنگاری ها در اختیار دارد، سریع تر می تواند به کلمه رمزنگاری شده برسد. این نرم افزار قادر است به هر دو صورت دیکشنری و کلمات تصادفی به رمزگشایی اقدام کند. Help نرم افزار را در زیر مشاهده می کنید:

```
John the Ripper password cracker, version 1.7.0.1
Copyright (c) 1996-2006 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john-386 [OPTIONS] [PASSWORD-FILES]
--single                  "single crack" mode
--wordlist=FILE --stdin   wordlist mode, read words from FILE or stdin
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test                    perform a benchmark
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT          load salts with[out] at least COUNT passwords only
--format=NAME             force ciphertext format NAME: DES/BSDI/MD5/BF/AFS/LM
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
```

Ethercap.11

خصوصیات:

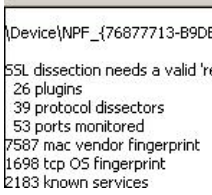
از ابزارهای بسیار کارآمد در حیطه استراق سمع برروی اطلاعات ردوبدل شده در بستر های گوناگون شبکه که توانایی تحلیل و استخراج کلمات عبور پروتکل های مختلف را دارا می باشد.

از نقاط قوت این ابزار می توان به استراق سمع بر روی مودم های دایال آپ و قابلیت استفاده از خط فرمان اشاره کرد. رابط گرافیکی این نرم افزار که تحت ویندوز نیز قابل اجرا می باشد به صورت زیر است.

Nikto .12

خصوصیات:

نرم افزار کدباز برای تست بیش از 3200 نوع آسیب پذیری بر روی بیش از 625 نوع وب سرور می باشد. تنها مشکل آن بروز شدن آن می باشد.



Ping/Telnet/Traceroute/Dig/whois/Netstat .13

خصوصیات:

دستوراتی ابتدایی برای بدست آوردن اطلاعات ابتدایی و مهم از شبکه و یا هدف در شبکه.

خروجی برخی از این نرم افزار ها را در زیر مشاهده می کنید:

```
Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Documents and Settings\MY-PC>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1110           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5679           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10000          0.0.0.0:0              LISTENING
```

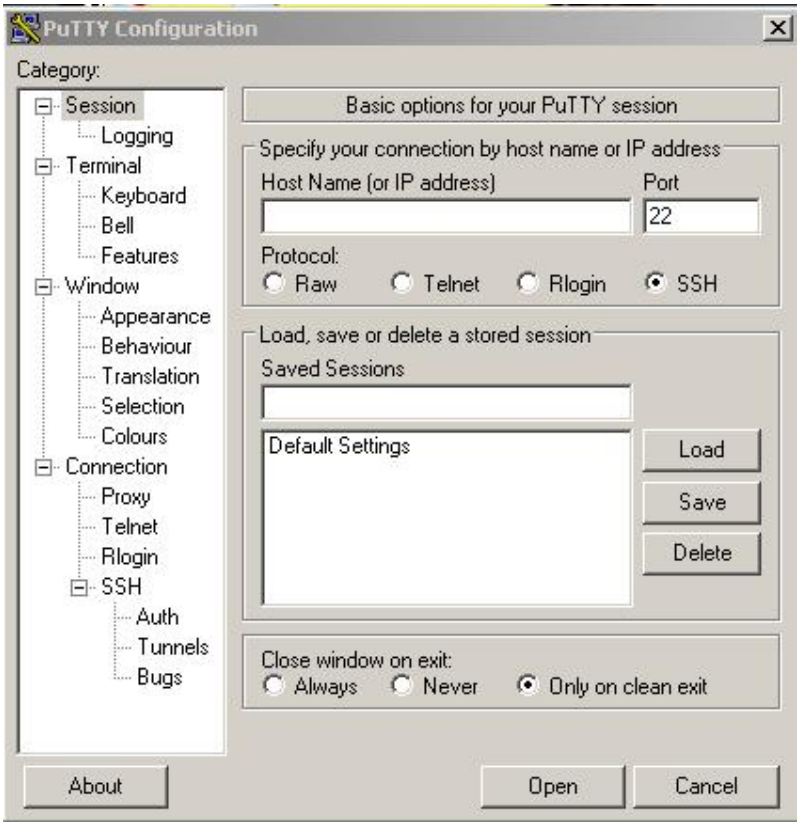
Putty .14

خصوصیات:

استفاده از این نرم افزار کم حجم شما را قادر می سازد که از طریق سیستم عامل ویندوز به SSH سیستم عامل های مبتنی بر لینوکس ارتباط برقرار کرد.

ناگفته نماند که با استفاده از این نرم افزار می توان از بستر پروتکل `Telnet` به پورت های دیگر نیز ارتباط برقرار کرد.

رایگان بودن بهمراه قابلیت ذخیره اطلاعات هریک از ارتباط ها از قابلیت های این نرم افزار می باشد. در زیر تصویر این نرم افزار را مشاهده می کنید:



15. THC Hydra

خصوصیات:

کامل ترین، سریع ترین و معروف ترین نرم افزاری است که توانایی انجام حملات Brute Force بر روی تمامی پروتکل هایی که در برابر این حملات آسیب پذیر می باشند را دارا می باشد.

نسخه اصلی این نرم افزار تحت سیستم عامل لینوکس می باشد، اما چند وقتی است که نسخه تحت ویندوز آن نیز در دسترس می باشد- که البته نسخه لینوکسی آن به نسبت نسخه ویندوزی از سرعت بالاتری برخوردار می باشد-، نکته قابل توجه در مورد این ابزار این است که برای استفاده از تمام امکانات این ابزار به علت فراوانی سوییچ های مشخص کننده ی تنضیمات، دچار دردسر خواهید شد.

16. Paros Proxy

خصوصیات: 

نرم افزار پروکسی تحت جاوا برای تشخیص مشکلات امنیتی برنامه های کاربردی تحت Http و Https به همراه اسکن کردن مشکلات SQL نیز از قابلیت های این نرم افزار می باشد.

17. Dsniff

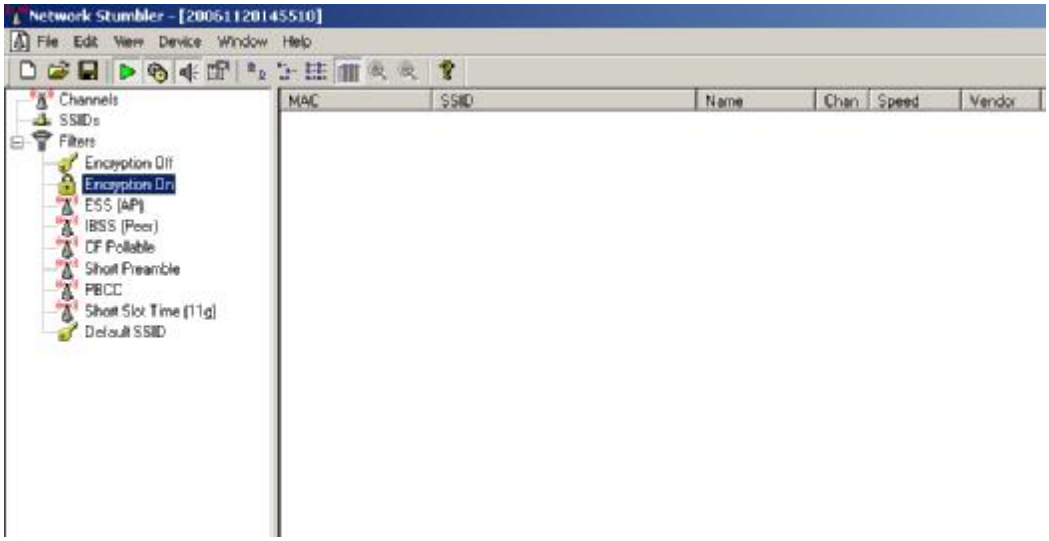
خصوصیات: 

نرم افزار استرق سمع می باشد که قبلیت انجام انواع حملات Spoof را دارا می باشد.

18. NetStumbler

خصوصیات: 

این نرم افزار از آن دسته است که حتما باید آنرا تست کرد تا به توانایی های فوق العاده آن پی برد!، برای دستیابی به تمام اطلاعات شبکه های بیسیم اطراف خود – مجاز و غیرمجاز(استراق سمع)- می توانید تا حدود زیادی بر روی این نرم افزار حساب کنید. از نکات قابل توجه در مورد این ابزار این است که دارای نسخه تحت PDA نیز میباشد، که با استفاده از آن می توانید در خیابان ها به گشت وگذار پرداخته و شبکه های بیسیم را کشف کرده به استراق سمع بر روی آنها بپردازید. نکته دیگر در مورد این ابزار این است که هنگام استفاده از آن نرم افزارهای تنظیم کننده ارتباط بیسیم در سیستم عامل از کارمی افتد. رابط گرافیکی این نرم افزار را در زیر مشاهده می کنید.



THC Amap.19

خصوصیات:

محصول دیگری از گروه THC که مانند محصولات دیگر این گروه به جرات می توان گفت در نوع خود کم نظیر می باشد. این ابزار را می توان به عنوان یک پورت اسکنر هوشمند به حساب آورد، اساس کار این نرم افزار به این صورت می باشد که علاوه بر تست باز و یا بسته بودن پورت های یک سیستم هدف توانایی تشخیص نرم افزار و پروتکلی که بر روی آن پورت در حال فعالیت می باشد را دارا می باشد.

GFI Languard .20

خصوصیات:

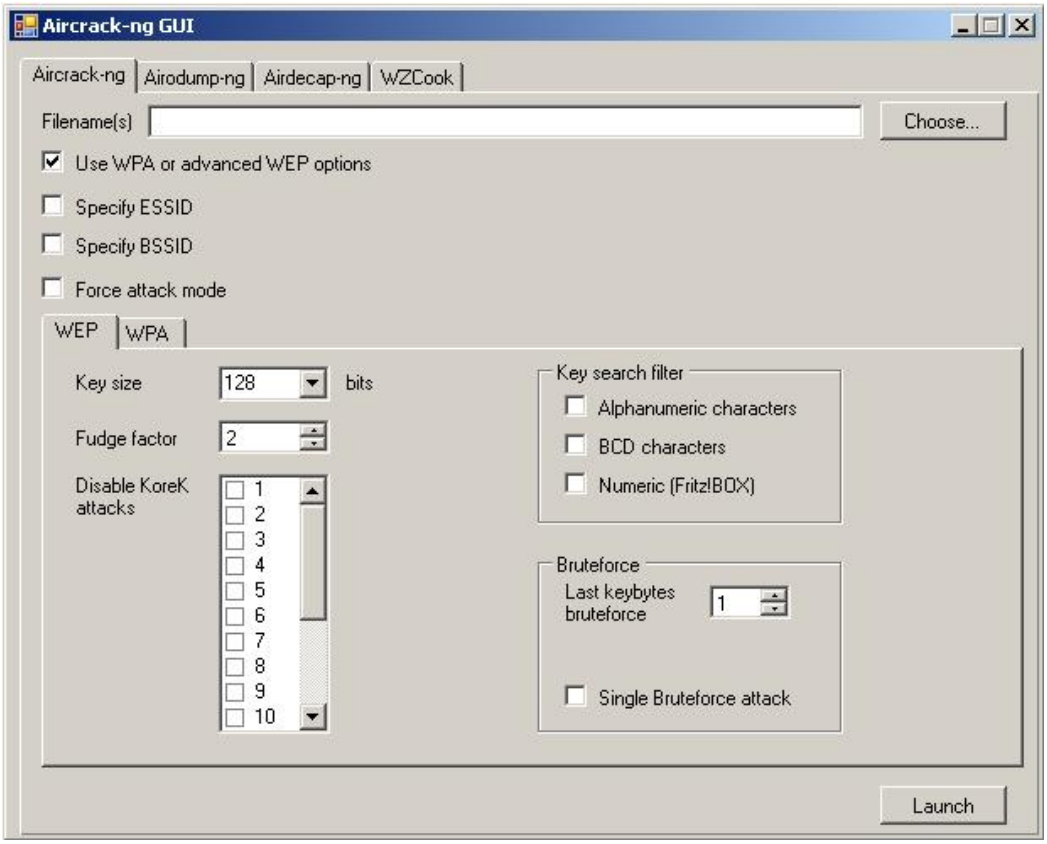
یکی از جامع ترین نرم افزارهای تست امنیتی شبکه و یا یک سیستم خاص که توانایی فرستادن گزارش ها را به پست الکترونیک مدیر سیستم را دارا می باشد. این نرم افزار به تنهایی قادر به شناسایی شبکه های بیسیم ، کشف پسوردهای ضعیف درون شبکه و تشخیص پروتکل ها، پورت ها و سرویس های اجرا شده درون شبکه را دارا می باشد.

مشکل این نرم افزار در این است که برای استفاده از آن باید هزینه آن را پرداخت کنید!. البته نسخه آزمایشی آن تا 30 روز اعتبار دارد و در طول این مدت می توانید به صورت رایگان از امکانات آن بهره گیرید. از دیگر توانایی های این نرم افزار می توان به توانایی تشخیص آپدیت های نصب شده و نشده سیستم ها و سرور های درون شبکه اشاره کرد.

21. AirCrack

خصوصیات: 

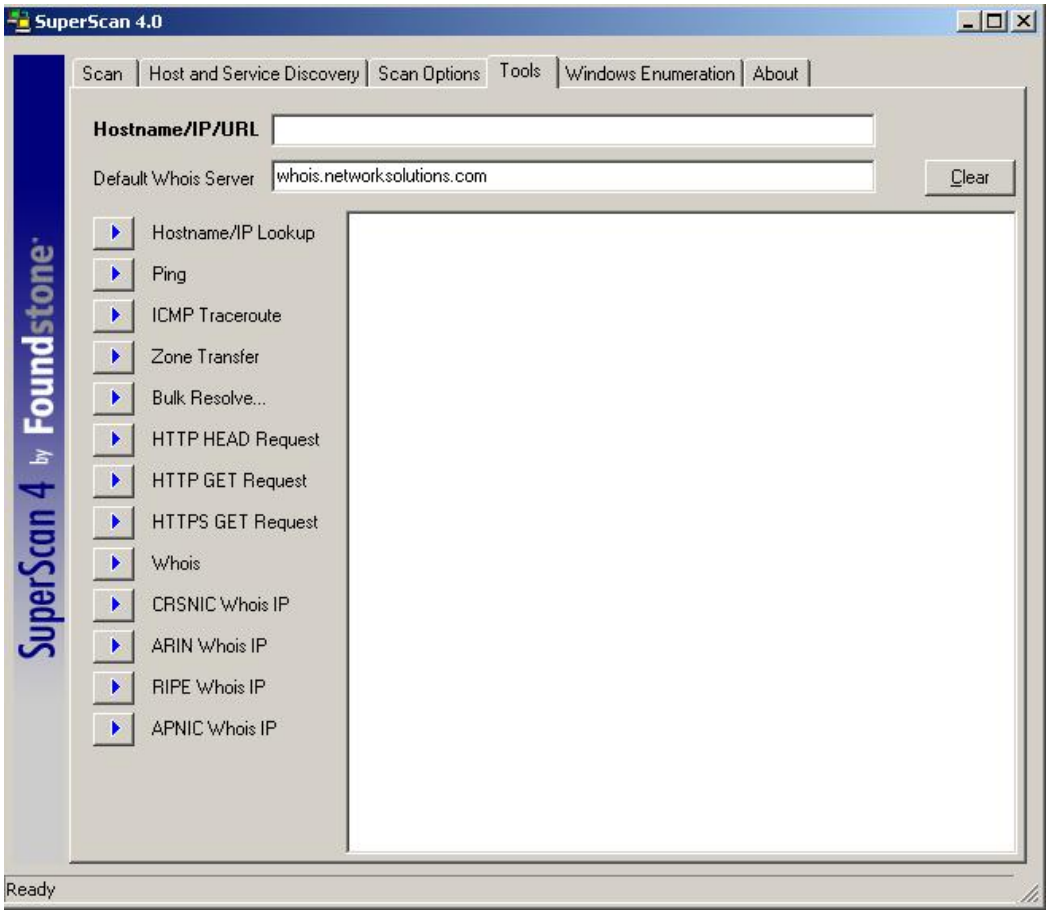
این نرم افزار که نسخه های تحت ویندوز و لینوکس آن در سترس و قابل دانلود می باشد، این توانایی را به شما می دهد که حملاتی را – از قبیل Brute Force- را بر روی پروتکل های WAP یک و دو انجام دهید. همچنین به شما توانایی شکستن و نفوذ به پروتکل های WEP و WAP را می دهد. این نرم افزار تحت خط فرمان نیز قابل استفاده بوده و به صورت کدباز عرضه می شود. اینترفیس این نرم افزار را در زیر مشاهده می کنید.



SuperScan .22

خصوصیات:

این نرم افزار تمامی ابزارهای کوچک مانند `Ping,Trace,Whois` و پورت اسکن و ده ها ابزار کوچک و بزرگ دیگر را در یک نرم افزار گردآوری کرده است. با اینکه این نرم افزار قابلیت خاصی نسبت به دیگر ابزار شبکه ندارد اما گردآوری چندین ابزار کوچک و بزرگ و در عین حال بسیار کارآمد این نرم افزار را جزو ابزارهای برتر امنیت شبکه قرار داده است. رابط گرافیکی این نرم افزار را در زیر مشاهده می کنید.



NetFilter.23

خصوصیات:

قابلیت فیلتر کردن پکت ها و همچنین اجرا کردن سیستم هایی نظیر NAT و NAPT بر روی سیستم عامل لینوکس را دارا می باشد.

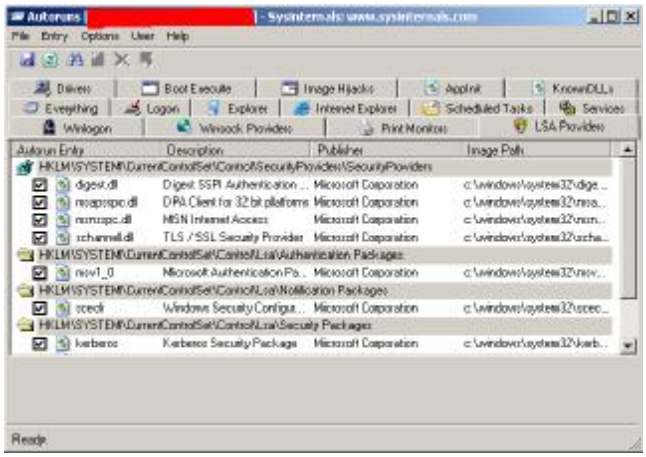
Sysinternal .24

خصوصیات:

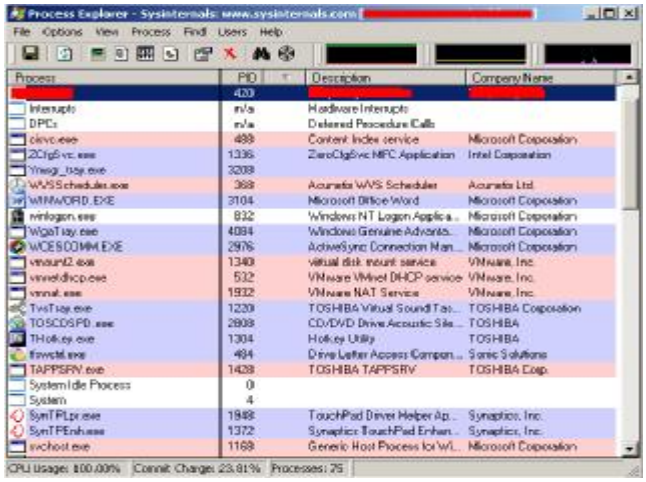
این نام یک مجموعه نرم افزار کوچک می باشد-که چندی پیش شرکت سازنده آن توسط مایکروسافت خریداری شد- که برای گرفتن اطلاعات از سیستم بسیار مفید می باشند.

محصولات مورد نظر ما در اینجا:

AutoRuns.1: این ابزار به لیست تمام فعالیت هایی که در شروع ویندوز به اجرا در می آیند را نمایش می دهد.



ProcessExplorer.2: این نرم افزار تمام فعالیت هایی که در آن موقع در حال اجرا می باشند را به همراه مقدار استفاده آنها از منابع سیستم نمایش داده و به شما اجازه قطع یک فعالیت خاص را می دهد.



و چند نرم افزار دیگر که توضیح تمام آنها در این مقاله باعث طولانی شدن بحث خواهد شد و فقط به ذکر نام آنها اکتفا می کنیم، PsTools و RootkitRevealer و TcpView .

Retina .25

خصوصیات:

نرم افزار اسکنر مشکلات شبکه، همانند Nessus می باشد. با این تفاوت که علاوه بر قیمت بسیار بالا وصله های امنیتی ویندوز را نیز نسب می کند. توجه داشته باشید با این که هیچکس قدرت Nessus را انکار نمی کند اما بسیاری بر این عقیده می باشند که در سیستم عامل ویندوز این نرم افزار به نسبت Nessus از قدرت بیشتری برخوردار می باشد.

26. Perl/Python/Ruby

خصوصیات:

زبان های برنامه نویسی هستند که در عین سادگی در کاربردهای شبکه ای بسیار پرقدرت عمل کرده و بخوبی می توانند با سوکت ها ارتباط برقرار کنند.

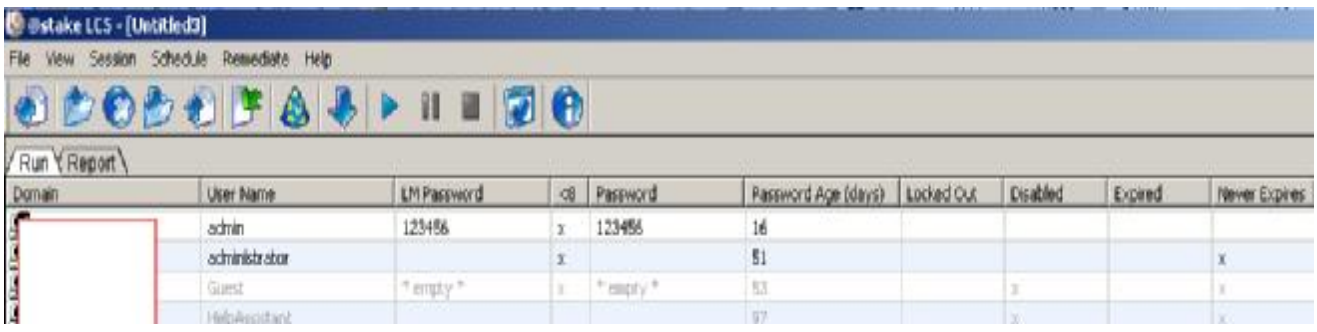
هم اکنون نرم افزارهای در اختیار کاربران قرار گرفته که می توانند در محیط ویندوز از هر سه زبان بهره برند-توجه کنید که در زبان Perl نوشتن برنامه ها برای اجرا در سیستم های لینوکسی و ویندوزی در بعضی اوقات متفاوت از یکدیگر می باشند.

27. L0phtcrack

خصوصیات:

نرم افزاری است برای رمزگشایی پسوردهای رمزنگاری شده، که البته با توجه به قیمت بالای آن و قابلیت های ابزارهایی مانند John و Cain شاید استفاده از این نرم افزار منطقی به نظر نمی رسد، اما با این حال بسیاری این نرم افزار را قدرتمندتر از این دو می پندارند.

همچنین این ابزار قادر است علاوه بر دریافت عبارت های رمزنگاری شده از سیستم ها درون شبکه، خروجی های نرم افزارهای استراق سمع را دریافت کرده و به رمز گشایی آنها بپردازد.



Scapy.28

توضیحات:

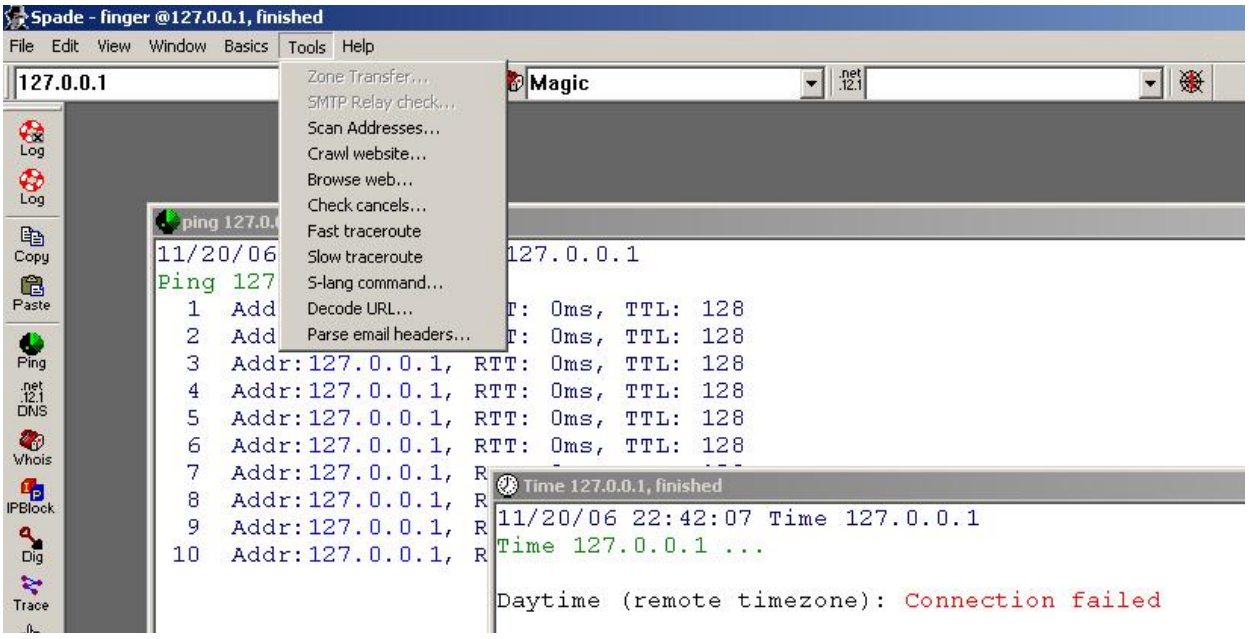
نرم افزاری که برای دستکاری پکت های ردوبدل شده در شبکه ابزاری بسیار مناسب و کارآمد است. با استفاده از زبان برنامه نویسی پیتون تهیه شده و قابلیت های کامل یک اسکنر شبکه را دارا می باشد.

Sam Spade.29

توضیحات:

این نرم افزار نیز اطلاعات اولیه مانند: Ping ، Trace ، Whois ، Finger را از شبکه استخراج کرده و با اینترفس نسبتا مناسب در اختیار کاربر قرار می دهد. استفاده از این نرم افزار در محیط ویندوز در هنگام کند وکاو در شبکه ها احساس خوبی به شما القا خواهد کرد.

در زیر تصویری از رابط گرافیکی این نرم افزار را مشاهده می کنید:



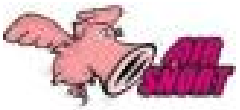
GNuPG/PGP .30

توضیحات:

با استفاده از این نرم افزار که می توان ادعا کرد بهترین در نوع خود است می توانید اطلاعات خود را رمزنگاری کرده و ریسک لو رفتن اطلاعات را به حداقل رساند.

هنگامی که مکاتبات خود در پست الکترونیک با استفاده از این نرم افزار رمزنگاری کنید، در صورتی که صندوق پستی شما مورد نفوذ قرار گیرد اطلاعات که از شما به سرقت می رود به حالت رمزنگاری شده می باشد و در واقع ضرر بسیار کمتری نسبت به هنگامی که اطلاعات رمزنگاری نشده را ذخیره می کنید به شما وارد می شود.

AirSnort .31



توضیحات:

توانایی این نرم افزار در بدست آوردن کلیدهایی که اطلاعات توسط آنها به حالت رمز درآورده می شود را در شبکه های بیسیم دارد.

Backtrack .32

توضیحات:

سیستم عاملی که به صورت Live قابل اجرا می باشد- البته می توان این سیستم عامل را نسب نیز کرد- و بر مبنای سیستم عامل لینوکس تهیه شده است. در این سیستم عامل که بر اساس نیازهای مدیران امنیتی شبکه ها طراحی شده است. به جرأت می تون گفت 60% از ابزارهایی که در این مقاله مورد بررسی قرار گرفته است به صورت پیش فرض در این سیستم عامل قرار داده شده است.

با استفاده از نرم افزارهایی که کامپیوتر را برای شما شبیه سازی می کنند (مانند VMware و Virtual PC) در محیط ویندوز از امکانات این سیستم عامل و ویندوز خود درعین حال استفاده کنید. در حال حاضر نسخه شماره 2 این نرم افزار نیز در دسترس می باشد.

P0f .33

توضیحات:

مفید برای تشخیص دادن نوع سیستم عامل از روی آنالیز کردن پکت های ردوبدل شده در شبکه.

Google .34

Google

توضیحات:

شاید این سوال برای شما که آوردن نام یکی از بهترین موتورهای جستجو در این لیست به چه معنا می تواند باشد!.با استفاده از این موتور جستجو می توانید مورادی همچون پست های الکترونیکی یک سایت و یا صفحاتی از سایت که ممکن است به طور عادی از دید شما پنهان شده باشد. در نظر داشته باشید پیشرفت امکانات جستجو در این موتور به حدی شده است که مباحثی با عنوان گوگل هکینگ را مطرح کرده است.

WebScarab .35

توضیحات:

ابزاری است که برای تجزیه و تحلیل اطلاعات ردوبدل شده تحت پروتکل های Http و Https طراحی شده است. مناسب برای Debug کردن برنامه های تحت وب و مشخص شدن مشکلات امنیتی آنها.

Ntop.36

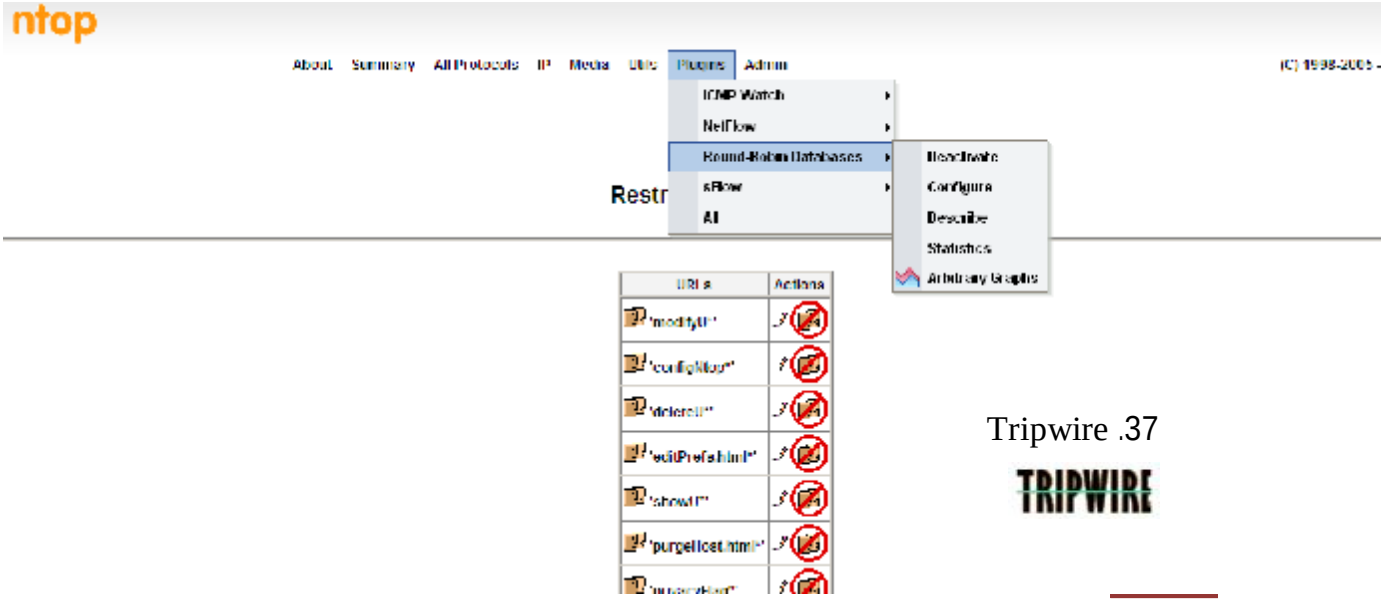
ntop

توضیحات:

نرم افزاری است که تحت وب اجرا شده و به شما امکان می دهد که علاوه بر مدیریت بر روی پهنای باند خود و گزارش گیری دلخواه از آن بر روی نوع پکت ها نیز اعمال مدیریت کرده و ردوبدل شدن آنها را زیر نظر بگیرید.

به طور کل این نرم افزار در دسته ابزار هایی قرار می گیرد که به شما اطلاعاتی در مورد نوع، نحوه و مقدار اطلاعاتی که در زمان های مختلف در شبکه شما ردوبدل شده است را نمایش می دهد.

در تصیر زیر تصویری از این نرم افزار مشاهده می کنید:



Tripwire .37

TRIPWIRE

توضیحات:

قدیمی ترین نرم افزار تست بی عیب بودن فایل ها. هشدار دادن به مدیر شبکه هنگام ایجاد تغییرات غیرمجاز و یا مشکل دار شدن یک فایل و دایرکتوری از امکانات این نرم افزار است.

Ngrep .38

توضیحات:

نرم افزاری با کاربری ساده با قابلیت اجرا تحت خط فرمان که برای تطبیق و نمایش دادن پکت های درون شبکه می تواند مورد استفاده قرار گیرد. این نرم افزار قابلیت تشخیص پروتکل های TCP,UDP,ICMP,PPP,FDDI و چند پروتکل دیگر را دارا می باشد.

گرچه نرم ا فزارهای دیگری که با اینترفیس گرافیکی این کار انجام می دهند – که شاید از قدرت و امکانات بیشتری نیز بر خوردار باشند- اما این ابزار به دلیل داشتن طرفداران فروان در این لیست جای گرفته است. در تصویر زیر سوییچ های که این برنامه برای تنضیمات خود بهره می گیرد را مشاهده می کنید:

Nbtscan .39

توضیحات:

قابلیت های این نرم افزار به شما این امکان را می دهد که تا حد امکان و در صورت باز بودن پروتکل نت بایوس-پورتهای 135و139- اطلاعاتی را از سیستم های مورد نظر خود بدست آورید.

اطلاعاتی نظیر دایرکتوری های به اشتراک گذاشته شده، نام(های) کاربری که در سیستم هدف وجود دارد و اینکه امکان ورود ناشناس وجود دارد یا خیر. ناگفته مشخص است این

ابزار - که تنها قابل اجرا در خط فرمان می باشد - تنها در شبکه های داخلی قابل استفاده می باشد. برای آشنایی بیشتر شما تصویری از این ابزار در زیر قابل مشاهده است.

```
NBTscan version 1.5.1. Copyright (C) 1999-2003 Alla Bezroutchko.
This is a free software and it comes with absolutely no warranty.
You can use, distribute and modify it under terms of GNU GPL.

Usage:
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator]
 [-m retransmits] (-f filename)|(<scan_range>)
        -v              verbose output. Print all names received
                        from each host
        -d              dump packets. Print whole packet contents.
        -e              Format output in /etc/hosts format.
        -l              Format output in lmhosts format.
                        Cannot be used with -v, -s or -h options.
        -t timeout      wait timeout milliseconds for response.
                        Default 1000.
        -b bandwidth    Output throttling. Slow down output
                        so that it uses no more that bandwidth bps.
                        Useful on slow links, so that ougoing queries
                        don't get dropped.
        -r              use local port 137 for scans. Win95 boxes
                        respond to this only.
                        You need to be root to use this option on Unix.
        -q              Suppress banners and error messages,
        -s separator    Script-friendly output. Don't print
                        column and record headers, separate fields with separato
r.
        -h              Print human-readable names for services.
                        Can only be used with -v option.
        -m retransmits  Number of retransmits. Default 0.
        -f filename     Take IP addresses to scan from file filename.
                        -f - makes nbtscan take IP addresses from stdin.
        <scan_range>    what to scan. Can either be single IP
                        like 192.168.1.1 or
                        range of addresses in one of two forms:
                        xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.
Examples:
        nbtscan -r 192.168.1.0/24
                Scans the whole C-class network.
        nbtscan 192.168.1.25-137
                Scans a range from 192.168.1.25 to 192.168.1.137
        nbtscan -v -s : 192.168.1.0/24
                Scans C-class network. Prints results in script-friendly
                format using colon as field separator.
                Produces output like that:
                192.168.0.1:NT_SERVER:00U
                192.168.0.1:MY_DOMAIN:00G
                192.168.0.1:ADMINISTRATOR:03U
                192.168.0.2:OTHER_BOX:00U
```

40. Webinspect

توضیحات:

اسکنر قدرتمند Application سرورها دارای قابلیت تشخیص حملات Injection و امکان تزریق اسکریپت را دارا می باشد.

41. OpenSSL

توضیحات:

شرح: توانایی رمزنگاری اطلاعات ردوبدل شده با سرور را در محل نصب شده ایجاد می کند. برای اطلاع بیشتر از نحوه عملکرد آن به مقالاتی با همین عنوان مراجعه کنید.

42. Xprobe2

توضیحات: 

شرح: نرم افزای است که به شما توانایی تشخیص سیستم عامل هدف را می بخشد. اساس کا راین نرم افزار مشابه نرم افزار Nmap می باشد، جالب است بدانید تمام توانایی های این نرم افزار با استفاده از پروتکل ICMP حاصل می شود.

43. EtherApe

توضیحات: 

شرح: با استفاده از این ابزار می توانید شبکه خود را به صورت گرافیکی مانیتور کرده و فعالیت های آن را زیر نظر بگیرید. این نرم افزار می تواند از پروتکل های Ethernet, ISDN, Token Ring, FDDI, PPP و چند پروتکل دیگر را پشتیبانی کند.

44. Core Impact

توضیحات: 

شرح: نرم افزاری کاملا خودکار، کامل و بسیار گران!! برای انجام آزمایش و تست نفوذ پذیری شبکه و یا سروری خاص. دارای دیتابیسی فوق العاده از انواع کدهای نفوذپذیری(Exploit) .

IDA Pro .45

توضیحات:

با بهره گیری از توانایی های این نرم افزار می توانید تمامی فعالیت ها و تغیراتی که هنگام نصب برنامه های مختلف و همچنین نصب وصله های امنیتی و . . . شرکت مایکروسافت که در حال وقوع است را زیر نظر داشته و تغییراتی را که در سیستم ایجاد می شود را مورد بررسی خود قرار دهید. این نرم افزار بیشتر مورد استفاده برنامه نویسان می باشد و قابلیت استفاده در مورد تهیه کرک برای برنامه های مختلف را نیز دارا می باشد.

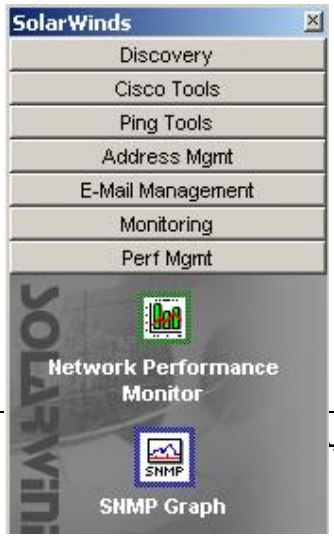
Solar winds .46

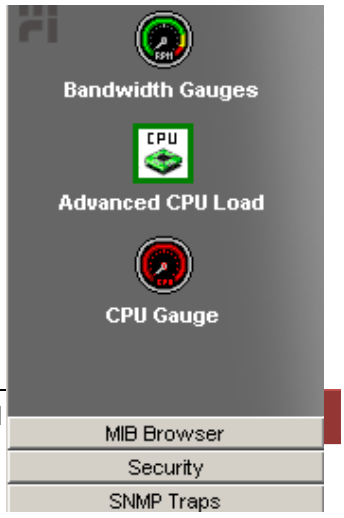
توضیحات:

یکی از کامل و جامع ترین نرم افزارهای مدیریت و بررسی متمرکز شبکه می باشد- که البته قیمت بسیار بالایی نیز دارد- دارای امکانات فراوانی نظیر:

مجموعه برای راهبرد ابزارهای سیسکو در شبکه، ایجاد لیست اسپمرها، ابزار های کاربردی در پروتکلهای دارای ارتباط مستقیم باIP مانندDNS و DHCP، مجموعه ابزارهای کشف سیستم ها و سرویس های در حال کار در شبکه و ابزارهایی جهت بررسی کارآیی شبکه به صورت زنده و قابلیت گزارش گیری جهت استفاده های آینده.

در کل می توان ادعا را داشت که برای راهبرهای امنیتی و از لحاظ کارآیی نرم ا فزار کاملی می باشد. لیست ابزارهای این نرم افزار را در تصویر زیر مشاهده می کنید.





Pwdump .47

توضیحات: 

نرم افزاری است که قابلیت رمزگشایی کلمات عبور سیستم های مبتنی بر سیستم عامل ویندوز را دارا می باشد. از دیگر قابلیت های آن بازیابی کلمات عبور ذخیره شده در سیستم است. گرچه نرم افزارهایی نظیر Cain این کار به خوبی انجام داده وبه صورت ویژوال قابل استفاده است اما اکثرا بر این باور هستند که نرم افزارهای تحت خط فرمان-مانند همین نرم افزار- از قدرت بیشتری نسبت به دیگر نرم افزارها برخوردارند. در تصویر زیر نحوه استفاده از این نرم افزار را مشاهده می کنید:

```
Usage: pwdump [-h][-o output_file][-u user][-p password][-s share] machineName
  where -h prints this usage message and exits
  where -o specifies a file to which to write the output
  where -u specifies the user name used to connect to the target
  where -p specifies the password used to connect to the target
  where -s specifies the share to be used on the target, rather than searching f
or one
  where -n skips password histories
```

LSoF.48

توضیحات: 

شرح: قابلیت نمایش تمام پردازش هایی که توسط فایل های باز شده بر روی سیستم را دارا است. توانایی نمایش فعالیت های سوکت ها یکی دیگر از توانایی های این نرم افزار می باشد.

RainbowCrack .49

توضیحات: 

در اینجا مقصود از ذکر این نام معرفی روشی برای یافتن پسوردهایی رمزنگاری شده به حالت های MD5 و LM می باشد تا معرفی یک نرم افزار. اساس کار این نرم افزار بر این است که در مدت زمان نسبتا طولانی- که به تعداد و نوع کاراکترهای انتخاب شده بین چند ماه تا چندین سال است- تمام احتمالات را ایجاد کرده و پس از آن تنها به جستجو در آن

ها برای یافتن گزینه صحیح می پردازد- درصد صحت بین 99% تا 99.99% قابل تعیین است.

FireWalk .50

توضیحات:

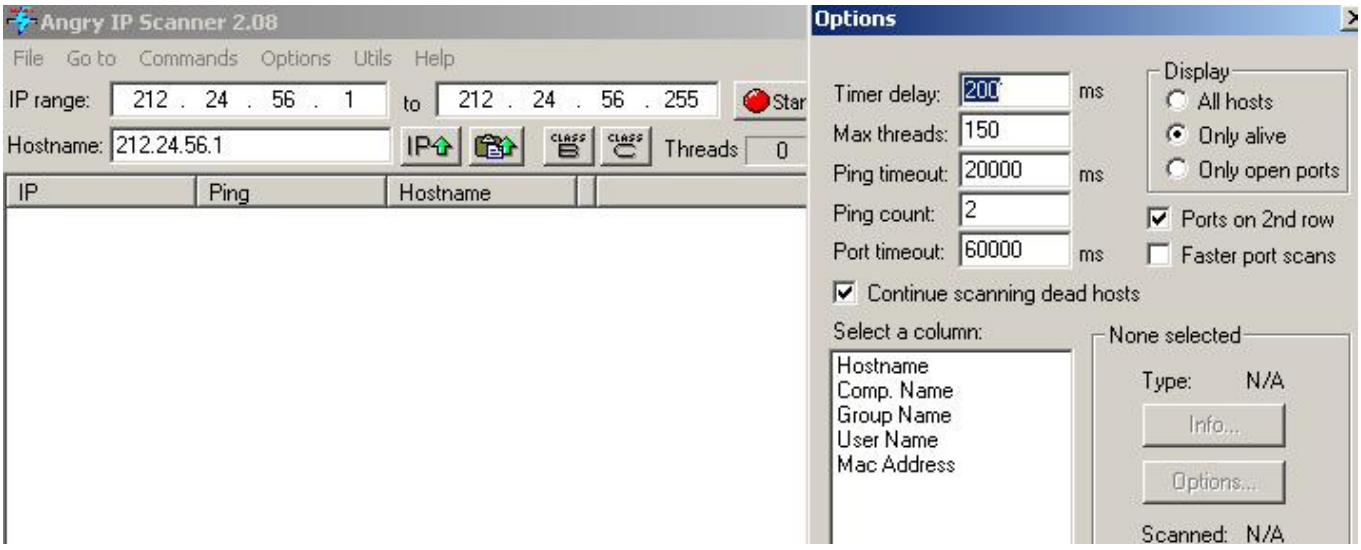
این نرم افزار به عنوان یک ابزار Traceroute حرفه ای با توانایی شناسایی بیشتر انواع دیواره های آتش و سیستم های تشخیص نفوذ سرزده و قابلیت عبور از آنها برای حصول نتایج بهتر. با اینکه نسخه قابل اجرای این نرم افزار تحت سیستم عامل ویندوز نیز در دسترس است اما تجربه نشان داده که نسخه تحت لینوکس آن علاوه بر سرعت نسبتا بالاتر، نتایج بهتری نیز ارائه می دهد.

Angry IP Scanner.51

توضیحات:

نرم افزاری که با اینکه از حجم بسیار کمی برخوردار است، بسیار کارآمد سریع و دقیق می باشد. با استفاده از آن می توانید محدوده های مختلف IP های موردنظر خود را از لحاظ سیستم های در حال کار به همراه پورت هایی که در آنها باز است را مورد بررسی قرار داده و نتایج را برای شما نمایش می دهد.

تصویری از رابط گرافیکی این نرم افزار را در زیر مشاهده می کنید:



PKHunter .52

خصوصیات:

شرح: این نرم افزار که تنها در سیستم های مبتنی بر سیستم عامل یونیکس قابل کار است، توانایی شناسایی Backdoor ها و RootKitها از توانایی های این نرم افزار است.

Ike-Scan .53

توضیحات:

این نرم افزار قابلیت شناسایی ارتباطات VPN بین سرور و کلاینت را دارا می باشد. می تواند پکتهای جعلی و دستکاری شده به سرور ارسال کرده و علاوه بر قابلیت شناسایی VPN شرکت هایی مانند: Checkpoint و Cisco و Microsoft و Nortel و Watchguard باعث فریب دادن سرور VPN می شوند.

ArpWatch .54

توضیحات:

شرح: با استفاده از این نرم افزار می توانید حملات ARP Man-in-the-Middle را در شبکه خود شناسایی کنید. این کار توسط آنالیز کردن پکت های APR انجام می شود.

KisMAC .55


توضیحات:

شرح: با استفاده از این برنامه تحت Mac-OS می توانید تمام قابلیت های نرم افزار Kismet را به شما ارائه کند.

OSSEC HIDS .56


توضیحات:

این نرم افزار با هدف تهیه یک سیستم تشخیص نفوذ سرزده برای یک سیستم خاص و نه برای تمام شبکه است. قابلیت شناسایی اکثر روت کیت ها را دارا می باشد، همچنین این ابزار توانایی بررسی- بصورت زنده- یکپارچگی فایل های سیستم را نیز دارا بوده. نکته قابل توجه در مورد این نرم افزار این است که برای تنظیم درست و صحیح این ابزار حتما به منابع و توضیحات این نرم افزار در اینترنت و یا Help نرم افزار مراجعه کنید.

Openbsd FP .57


توضیحات:

شرح: با استفاده از این نرم افزار که برای سیستم های تحت سیستم عامل یونیکس طراحی شده است می توانید علاوه بر مدیریت بر روی پهنای باند از امکاناتی مانند NAT و اولویت بندی اطلاعات ردوبدل شده آن استفاده کنید.

Nemesis .58


خصوصیات:

می توان گفت این نرم افزار، ابزار ساده شده ی Hping2 می باشد که دارای قابلیت دستکاری پکت های عبوری درون شبکه را دارا می باشد. درای قابلیت تغییر پارمترهای پکت ها به منظور فریب دایواره های آتش می باشد. گرچه استفاده از این ابزار تا حدی ساده تر از `Hping2` می باشد، اما برای افراد حرفه ای کار با `Hping2` به مراتب خوشایندتر و کارا تر می باشد.

TOR .59

خصوصیات:

این نرم افزار توسط گروهی از برنامه نویسان و توسعه دهندگان Fire Fox تهیه گردیده است. این نرم افزار با در اختیار داشتن سرورهای فراوانی که در اینترنت فراهم کرده است، ارتباطات شما را در اینترنت به صورت ناشناس انجام می دهد.

این نرم افزار توانایی انجام این کار را-ناشناس کردن تراکنش ها در شبکه- را برای پروتکل هایی مانند SSh, http, irc وغیره را دارا میباشد.

60. Knoppix

خصوصیات:

این سیستم عامل که بر مبنای لینوکس توسعه پیدا کرده است را می توان جزو اولین سیستم عامل های Live بشمار آورد. این سیستم عامل که با استفاده از ابزارهای شبیه ساز کامپیوتر در سیستم عامل ویندوز نیز قابل اجرا می باشد دارای ابزارهای امنیتی مناسبی برای تست های امنیتی و انجام عملیات های نفوذ در شبکه های مختلف است.

در صورتی که سیستم عامل Back Track توسعه نیافته بود شاید این سیستم جای آن را در لیست به خود اختصاص داده بود.

61. ISS Internet Scanner

توضیحات:

شرح: نرم افزاری که برای ارزیابی امنیتی Application-Server ها طراحی شده است.

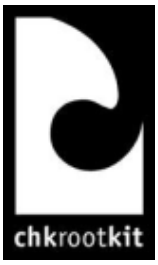
62. Fport

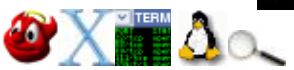
توضیحات:

این نرم افزار قادر است برنامه هایی که پورت هایی را باز کرده اند به همراه شماره پورت به کاربر نمایش می دهد. با توجه به اینکه دستور Netstat در ویندوز نیز کمابیش این کار را انجام می دهد و قابل اجرا بودن این برنامه در خط فرمان، تنها به دلیل مشخص کردن

دقیق برنامه مورد استفاده از پورت در این لیست جای گرفته و کارآیی بخصوص دیگری را دارا نمی باشد.

63. ChkRootkit





توضیحات:

این نرم افزار قادر است اکثر RootKit ها را بر روی سیستم های مبتنی بر سیستم عامل های مبتنی بر یونیکس شناسایی کند. همچنین قادر به شناسایی ماژول های مخرب نیز می باشد.

64. SPIKE Proxy

توضیحات:

این نرم افزار که با استفاده از زبان برنامه نویسی پیتون توسعه پیدا کرده است، جهت تست نفوذ پذیری وب سایت ها طراحی شده است. قابلیت شناسایی حملات SQL Injection و Overflow از توانایی های این نرم افزار است. پس از نصب و انجام تنضیمات برای استفاده از آن می توانید در قسمت تنضیمات پروکسی رفته و با تنظیم آن بترتیب بر روی آدرس و پورت 127.0.0.1 8080 از امکانات این نرم افزار استفاده کنید.

65. Openbsd

توضیحات:

شرح: از امن ترین سیستم عامل ها موجود می باشد!!!.

66. Yersinia

توضیحات:

شرح: با استفاده از این ابزار می توانید حملات سطح پایین شبکه مانند حمله به پروتکل های CDP و HSRP را انجام دهید.

Nagios .67

توضیحات:

شرح: با استفاده از این برنامه می توانید فعالیت اکثر پروتکل های تحت شبکه مانند SMTP, pop3, http, nntp, ping و غیره را علاوه بر تحت نظر گرفتن فعالیت آنها به مانیتور کردن آنها نیز بپردازد.

Fragroute/Fragrouter .68

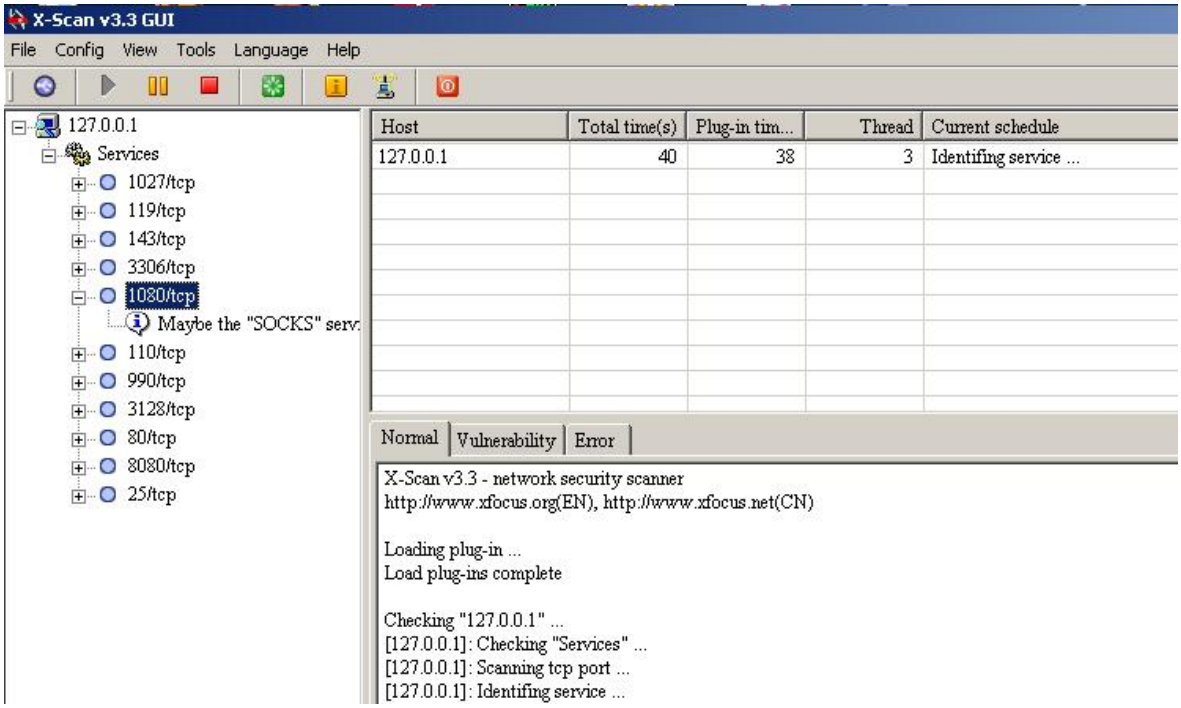
توضیحات:

شرح: این نرم افزار شما را قادر می سازد تا با استفاده از تکنیک های خاصی اطلاعات غیر مجاز خود را از سیستم های تشخیص نفوذ سرزده عبور دهید.

X-scan.69

توضیحات:

اسکنر تقریبا کاملی که اکثر اطلاعاتی را که از شبکه هدف لازم دارید در اختیار شما قرار می دهد. پس از مشخص کردن سیستم و یا شبکه مورد نظر این اسکنر به بررسی پورت ها وسیرویس های آن پرداخته سپس با توجه به نتایج بدست آمده به بررسی نقاط ضعف آن سرویس پرداخته و در صورتی که آن سرویس دارای مرحله تایید هویت (Authentication) باشد به تست کلمات کاربری به همراه کلمات عبور از روی فایل های مشخص شده می پردازد. در پایان نیز با استفاده از ماژول های Nessus که به صورت پیش فرض در آن قرار داده شده است به بررسی آنها درون شبکه پرداخته و نتایج را بصورت جالبی در اختیار شما قرار می دهد.



70. Whisker/Libwhisker

توضیحات:

شرح: نرم افزاری جهت تست نفوذ پذیری از طریق کدهای CGI و یافتن حفره های نفوذ پذیری تحت پروتکل Http.

71. Socat

توضیحات:

شرح: نرم افزاری با کارآیی های شبیه به NETCat می باشد که می توانید با استفاده از آن در سیستم یونیکس می توانید یک ارتباط Shell برقرار کنید.

72. Sara

توضیحات:

ابزاری دیگر برای ارزیابی امنیتی سیستم های مبتنی بر ویندوز و لینوکس که تحت هر دو سیستم عامل قابل اجرا بوده و توانایی اجرا تحت خط فرمان و رابط گرافیکی را نیز دارا می باشد.
نکته مثبت این ابزار، علاوه بر رایگان بودن ارائه دو بسته بروز رسانی در هر 60 روز یکبار می باشد.
گرچه بسیاری از افراد نرم افزارهای دیگر با کارآیی مشابه را مناسب تر و پرقدرت از این نرم افزار می دانند اما همین تعداد رایگان بودن این ابزار را دلیلی کافی برای یکبار امتحان کردن آن می دانند.

QualysGuard .73

توضیحات:

نرم افزاری است که تحت وب به بررسی مشکلات امنیتی می پردازد. این نرم افزار دارای بیش از 5000 هزار تست امنیتی است و دارای سیستم بروزرسانی خودکار نیز می باشد.
نکته جالب در مورد این ابزار آن است که شرکت پشتیبانی کننده از آن تنها یک نام کاربری و یک کلمه عبور مختص به سایت خود در اختیار شما قرار داده و هیچ نرم افزاری به شما تحویل نمی دهد!!.
با استفاده از این دو کد به قسمت تست امنیتی وارد شده و این شرکت با استفاده نرم افزار خود از طریق وب به بررسی و تست نفوذپذیری سایت شما خواهد پرداخت.

ClamAV .74

توضیحات:

این نرم افزار جزو آنتی ویروس ها می باشد، گرچه در لسیت 10 آنتی ویروس برتر نامی از این آنتی ویروس نیست اما قابل اجرا بودن این آنتی ویروس تحت سیستم عامل های

لینوکسی و یونیکسی و همچنین رایگان بودن آن، ما را متقاعد ساخت تا نام این ابزار را در این لیست قرار دهیم.

Cheops .75

Cheops

توضیحات:

شرح: نرم افزاری فوق العاده قدرتمند که تحت سیستم عامل های لینوکسی قابل اجرا بوده و توانایی بسیار زیادی در رسم و تشخیص توپولوژی شبکه ی مورد جستجو از قابلیت های این نرم افزار می باشد.

Brupsuite .76

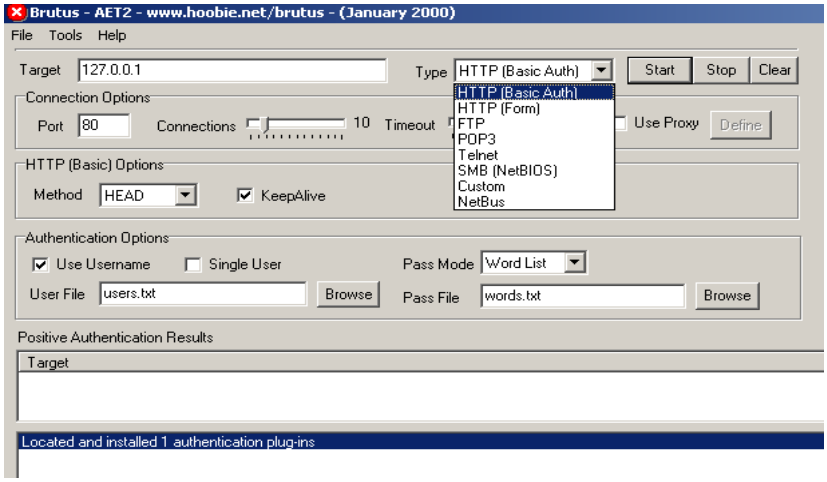
توضیحات:

بابهره گیری از توانایی های این نرم افزار می توانید به صورت دستی و یا اتوماتیک نرم افزارهای تحت وب که توسط کارمندان خود تهیه شده ویا از شرکت دیگری خریداری کرده اید را از نظر امنیتی تست کرده و نتیجه انواع حملات مانند SQL Injection و تزریق انواع اسکریپت ها را بر روی آنها مشاهده کنید.

Brutus.77

توضیحات:

این ابزار از کامل ترین نرم افزارها مختص به حملات موسوم به Brute Force می باشد.
با استفاده از این برنامه می توانید این حمله را بر روی پروتکل هایی نظیر FTP,Http,Telnet,SMB انجام داده و نتایج خوبی را مشاهده کنید. از دیگر نقاط قوت این ابزار قابلت استفاده از لیست کلمات برای انجام این حمله است.
گرچه Hydra ابزار قدرتمندتری نسبت به این نرم افزار به شمار می آید اما بسیاری استفاده از این ابزار را در محیط ویندوز ترجیح می دهند. رابط گرافیکی این نرم افزار را در زیر مشاهده می کنید:



78. Unicornscan

توضیحات:

شرح: این برنامه این توانایی را به شما می دهد که با استفاده از پکت هایی که به سمت سرور خاصی ارسال می کند و با تحلیل پکت های دریافت شده انواع نرم افزارهای نسب شده به همراه خواص گوناگون سیستم عامل را حدس بزند.

79. Stunnel

توضیحات:

این نرم افزار با هدف ایجاد رمزنگاری SSL برای پروتکل های POP3, Imap, NNTP, SMTP و Http تهیه و توسعه یافته است. از مشکلات آن می توان به نداشتن رابط گرافیکی و همچنین نداشتن Help کامل از مشکلات این ابزار می باشد.

تصویر فایل تنظیمات این نرم افزار را در زیر مشاهده می کنید:

```
; Authentication stuff
;verify = 2
; Don't forget to c_rehash CApath
;CApath = certs
; It's often easier to use CAfile
;CAfile = certs.pem
; Don't forget to c_rehash CRLpath
;CRLpath = crls
; Alternatively you can use CRLfile
;CRLfile = crls.pem

; Some debugging stuff useful for troubleshooting
;debug = 7
;output = stunnel.log

; Use it for client mode
;client = yes

; Service-level configuration

[pop3s]
accept  = 995
connect = 110

[imaps]
accept  = 993
connect = 143

[ssmtp]
accept  = 465
connect = 25

;[https]
;accept  = 443
;connect = 80
;TIMEOUTclose = 0

; vim:ft=dosini
```

Honeyd .80

توضیحات:

شرح: با استفاده از این نرم افزار کوچک اما بسیار کارآمد می توانید بر روی یک سیستم چندین گروه مجازی با خاصیت های دلبخواه در شبکه مانند IPو Subnet های گوناگون ایجاد کنید.

Fping .81

توضیحات: 

شرح: این نرم افزار قابلیت تشخیص سیستم هایی که در شبکه در حال فعالیت هستند را با استفاده از پروتکل ICMP تشخیص می دهد.

BASE.82

توضیحات: 

نرم افزاری است که بر اساس زبان PHP تهیه وتوسعه یافته است، با استفاده از اطلاعات خروجی موسوم به Log File که توسط سیستم های تشخیص نفوذ سرزده و دیوارهای آتش ایجاد می شود،به تجزیه و تحلیل این داده های خام پرداخته و امکان در حال انجام بودن یک نوع خاص حمله و محل انجام آن را برای شما نمایش خواهد داد.

Argus .83

توضیحات: 

شرح: با استفاده از این برنامه می توانید تراکنش های انجام شده در شبکه را زیر نظر داشته باشید و کارائی شبکه خود را در زمینه های گوناگون مورد بررسی قرار دهد.

Wikto .84

توضیحات: 

نسخه ویندوزی Nikto همراه با رابط گرافیکی است، البته بسیاری براین عقیده هستند که این ابزار در مقابل با نسخه اصلی از قدرت پایین تری برخوردار می باشد.

Sguil .85

توضیحات: 

شرح: این نرم افزار شبکه شما را از نظر امنیتی مورد تجزیه وتحلیل قرار داده و جزو سیستم های تشخیص نفوذ سرزده به شمار می رود.

86. Scanrand

توضیحات:

شرح: نرم افزاری است که توانایی کشف مشخصات شبکه به همراه حدس ساختار آن (توپولوژی) از خصوصیات آن می باشد. سرعت بسیار بالا و استفاده از روشهای مخفی برای جلوگیری کردن از به دست آوردن اطلاعات از شبکه توسط نفوذگران از خواص این نرم افزار می باشد.

87. IP Filter

توضیحات:

شرح: این نرم افزار شما را قادر می سازد از امکاناتی نظیر NAT و تقریبا تمامی امکانات یک دیواره آتش در آن واحد بهره گیرید.

88. Canvas

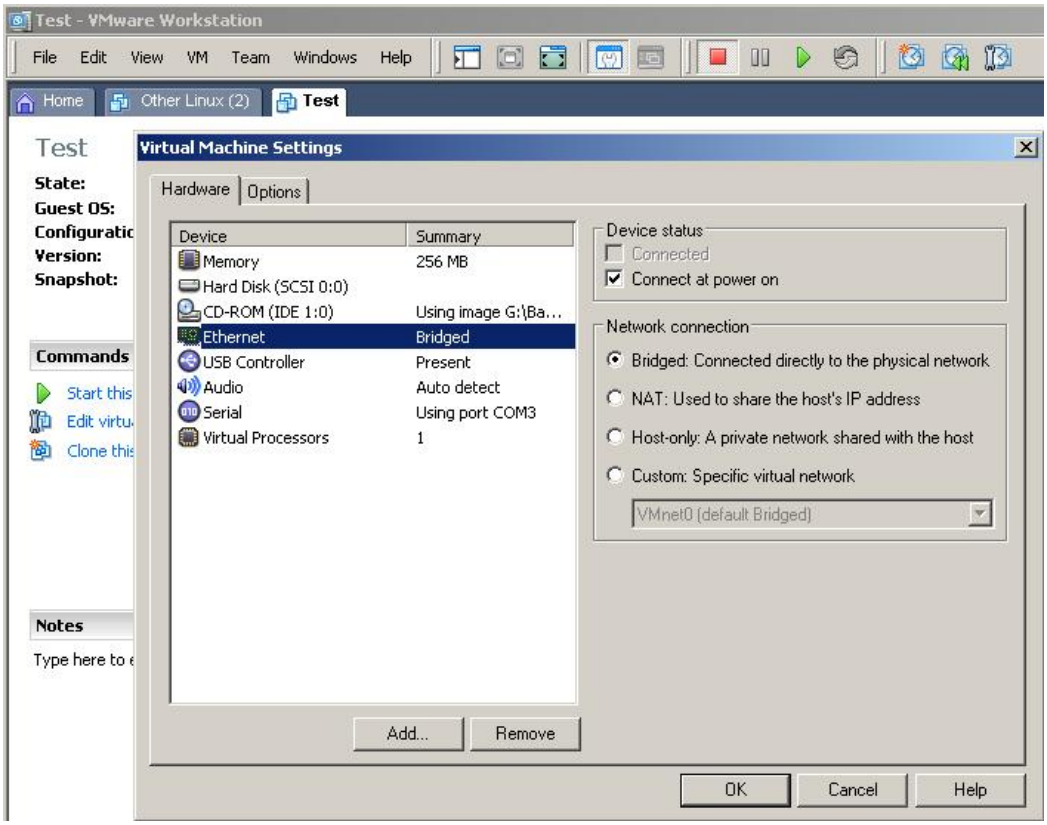
توضیحات:

اساس کار و هدف از تهیه این نرم افزار مشابه Core Impact می باشد اما با آرشیوی در حدود 150 کدمخرب که به مراتب از Core Impact کمتر می باشد. با این حال قیمت این نرم افزار نیز بسیار پایین تر از Core Impact می باشد که این امر سبب جذب بیشتر مشتریان برای این شرکت شده است. شرکت سازنده این نرم افزار ادعا دارد که تمام کدهای مخربی که استفاده کرده است در اصطلاح هکرها 0-day می باشند که به معنی عمومی نبودن این کدها می باشد.

89. VMware

توضیحات:

این نرم افزار که شبیه ساز کامپیوتر می باشد، علاوه بر کاربری های امنیتی دارای کاربردهای آموزشی و حتی صنعتی نیز می باشد. این ابزار تنظیمات بسیاری مانند انتخاب نوع اتصال به شبکه و مقدار رم سیستم و نحوه استفاده از درایوهای نوری سیستم را در اختیار شما قرار. با استفاده از این ابزار می توانید در محیط ویندوز و با تنظیم صحیح آن به شبکه داخلی خود متصل شده و از تمامی امکانات یک سیستم عامل دیگر بهره برده و نیازهای خود را برطرف سازید. در تصویر زیر قسمت تنظیمات این نرم افزار را مشاهده می کنید.



90. TcpTraceroute

توضیحات:

شرح: با استفاده از این نرم افزار می توانید عمل Traceroute را با استفاده از پکت های TCP را انجام دهید. جالب است بدانید که این نرم افزار قابلیت شناسایی و عبور از اکثر دیواره های آتش را دارا می باشد.

91. SAINT

توضیحات:

شرح:نرم افزار جامع مدیریتی امنیت شبکه، مشابه به نرم افزارهای Nessus و Retina.

92. OpenVPN

توضیحات:

این نرم افزار این امکان را برای شما فراهم می سازد که VPN را هم بر روی لایه 3 و هم بر روی لایه 2 شبکه برقرار سازید. گرچه این امکان در ویندوز به صورت پیش فرض قرار دارد، اما استفاده از این ابزار کار شما در شبکه را بیشتر ولی در عوض کلاینت ها را آسوده تر می کند. تمامی قابلیت های یک VPN سرور را دارا می باشد، نکته دیگر در مورد آن استفاده از OpenSSL برای رمزنگاری با طول 2048 بیتی می باشد. توجه داشته باشید که برای درک نصب صحیح حتما باید یکبار به مراجعی که در سایت سازنده قرار داده شده مراجعه کنید.

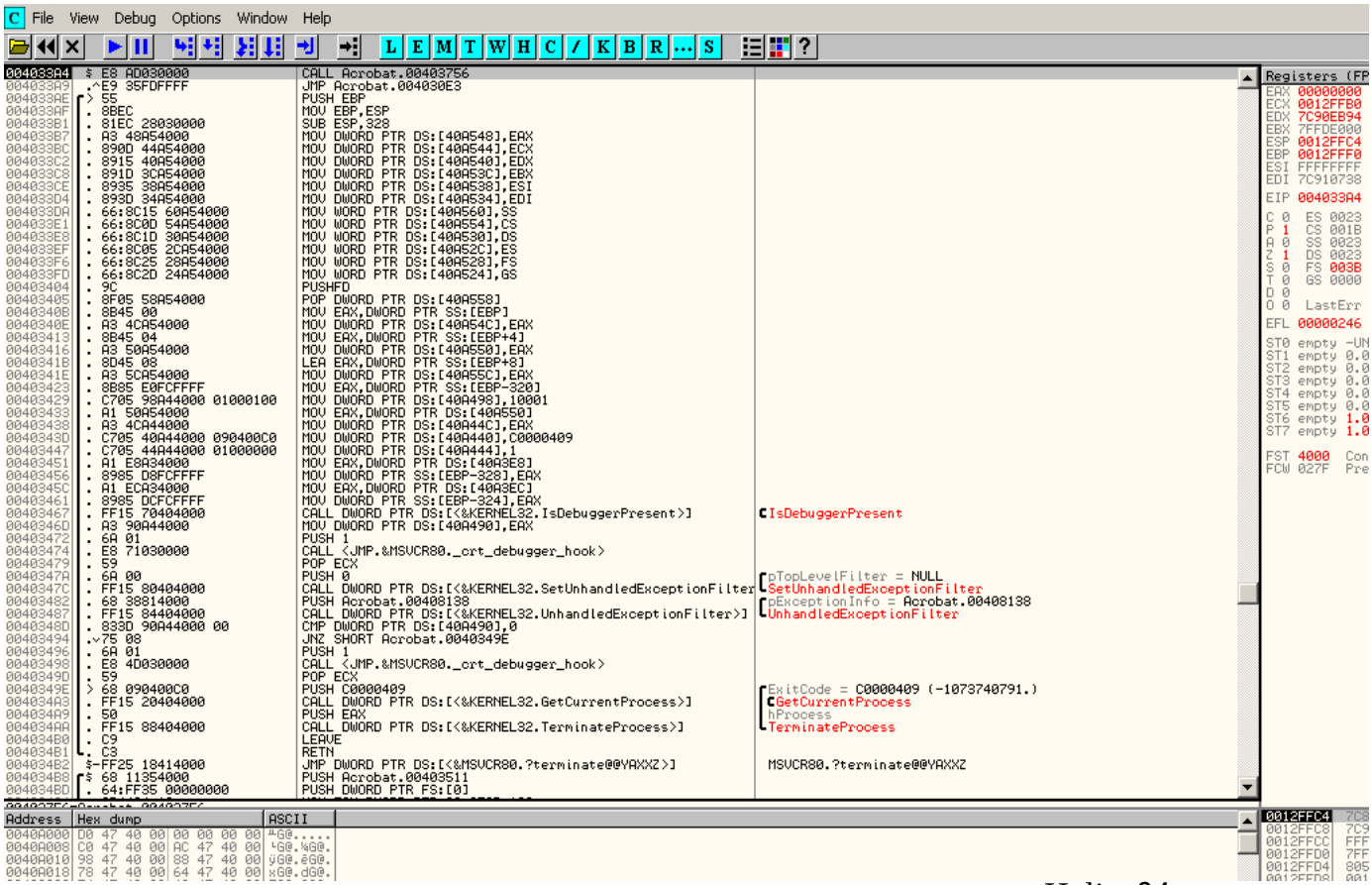
تصویر زیر قسمتی از فایل تنظیمات سرور را نمایش می دهد.

```
# Generate with:↓
#   openvpn --genkey --secret ta.key↓
#↓
# The server and each client must have↓
# a copy of this key.↓
# The second parameter should be '0'↓
# on the server and '1' on the clients.↓
;tls-auth ta.key 0 # This file is secret↓
↓
# Select a cryptographic cipher.↓
# This config item must be copied to↓
# the client config file as well.↓
;cipher BF-CBC        # Blowfish (default)↓
;cipher AES-128-CBC   # AES↓
;cipher DES-EDE3-CBC  # Triple-DES↓
↓
# Enable compression on the VPN link.↓
# If you enable it here, you must also↓
# enable it in the client config file.↓
comp-lzo↓
↓
# The maximum number of concurrently connected↓
# clients we want to allow.↓
;max-clients 100↓
```

OllyDbg .93

توضیحات:

یک Debugger اسمبلی بسیار مناسب تحت ویندوز. تمام امکاناتی که از یک Debugger انتظار دارید در این نرم افزار وجود دارد. این ابزار بیشتر مورد استفاده برنامه نویسانی است که با هدف بررسی نرم افزارهای گوناگون برای تهیه کرک آنها می باشد. این ابزار برای تهیه کدهای مخرب و نفوذگر نیز قابل استفاده بوده و بسیار کارآمد می باشد. در تصویر زیر نمایی از این برنامه را مشاهده می کنید:



Helix .94

توضیحات:

شرح: سیستم عاملی Live لینوکسی که بر مبنای سیستم عامل Knoppix طراحی شده است. دارای ابزارهای امنیتی گوناگون در زمینه امنیت می باشد.

Bastille .95

توضیحات:

شرح: نرم افزاری است که به تست امنیتی و ارائه راهکار برای برطرف کردن آنها می پردازد. برروی تمامی نسخه های لینوکس قابل نسب و بهره بر داری می باشد.

Acunetix Web Vulnerability Scanner.96

توضیحات:

از ابزارهای تازه طراحی شده برای انجام تست های امنیتی در لایه کاربردی شبکه می باشد، این ابزار که به تازگی محبوبیت فراوانی پیدا کرده است. از نقاط قوت آن می توان به بروزرسانی مناسب و پشتیبانی از تمامی حملات – در لایه کاربردی شبکه- و امکان تغییر پارامترهای حملات گوناگون به صورت دستی نیز اشاره داشت.

امکاناتی نظیر Http Fuzzer و Http Sniffer از دیگر قابلیت های این ابزار هوشمند و کارا می باشد. تصویر زیر لیست ابزارهای این نرم افزار را به خوبی نمایش می دهد.

TrueCrypt 97

توضیحات:

شرح: این نرم افزار این توانایی را به شما می دهد که فایل های درون سیستم خود را به به صورت رمز نگاری شده ذخیره می شود.

Watchfire AppScan .98


توضیحات:

یک اسکنر نقاط ضعف امنیتی کامل، بسیار قوی و قابلیت کار در لایه های مختلف که البته قیمت بسیار زیادی نیز دارد. کامل بودن دیتا بیس حملات و همچنین کدهای مخرب این ابزار نسبت به نرم افزارهای مشابه کامل تر بوده و نتایج حاصل شده را به شیوه بسیار کامل و همچنین ارائه راهکارهایی جهت برطرف سازی این مشکلات در اختیار شما قرار می دهد. توجه داشته باشید که در صورت استفاده از کرک از نصب وصله های ارائه شده توسط شرکت ارائه شده خودداری کنید.

N-Stealth.99

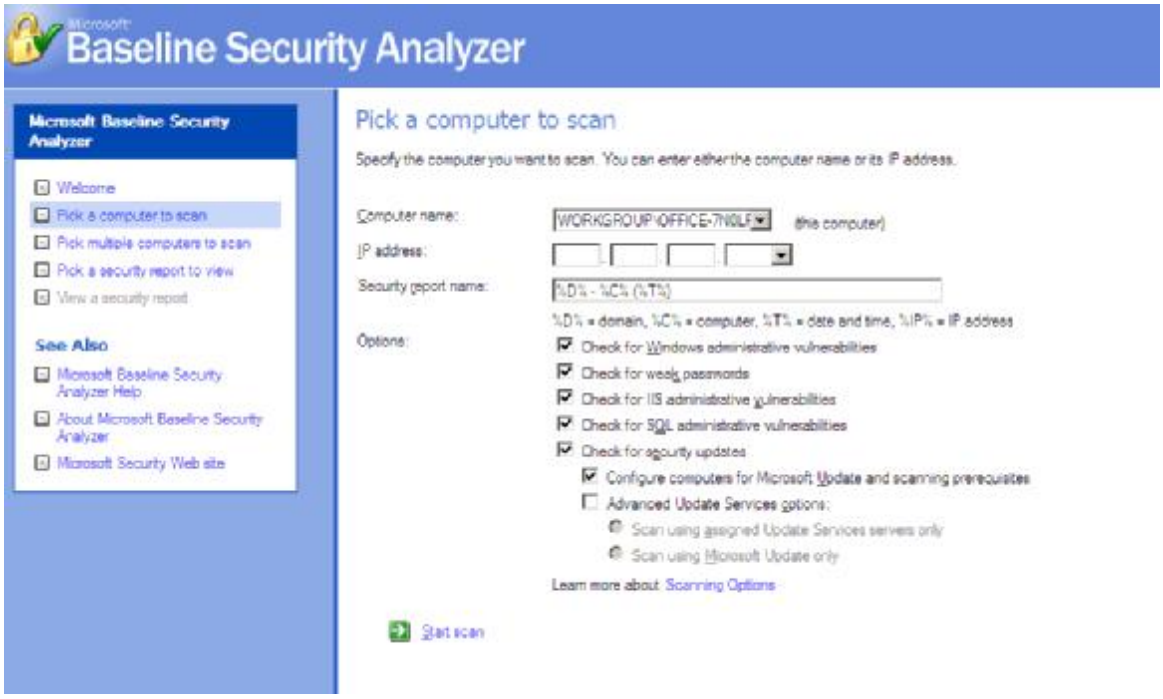

توضیحات:

شرح: اسکنر قوی دیگر که آرشیوی شامل 30000 مشکلی امنیتی است واساس کار آن مانند Nessus و Retina می باشد.

MBSA .100


توضیحات:

شاید دلیل اصلی وجود این نرم افزار در این لیست، نام ماکروسافت باشد- شرکت توسعه دهنده این ابزار- این ابزار پس از نصب به سایت ماکروسافت متصل شده و نکات امنیتی سیستم شما را به شرکت گزارش کرده و راهکارهای برطرف سازی آن را به شما ارائه می کند. در تصویر زیر نمای کلی واسط گرافیکی این نرم افزار را مشاهده می کنید:


Microsoft
Baseline Security Analyzer
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Pick a computer to scan
Specify the computer you want to scan. You can enter either the computer name or its IP address.
Computer name:
WORKGROUP\OFFICE-7N0LF
(this computer)
IP address:
Security report name:
%D% - %C% (%T%)
%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address
Options:
Check for Windows administrative vulnerabilities
Check for weak passwords
Check for IIS administrative vulnerabilities
Check for SQL administrative vulnerabilities
Check for security updates
Configure computers for Microsoft Update and scanning prerequisites
Advanced Update Services options:
Scan using assigned Update Services servers only
Scan using Microsoft Update only
Learn more about Scanning Options
Start scan