هانی پات
(Honeypot)

Honeypot

- یک سیستم اطلاعاتی است که منابعی را در اختیار می گذارد که هر گونه استفاده از آن منابع نشاندهنده استفاده غیر مجاز و غیر قانونی است.
- هر اطلاعاتی که به Honeypot وارد یا از آن خارج شود، با احتمال زیادی حمله و فعالیت های خرابکارانه است.

وظایف

- تولید امضاء بدافزارها برای آنتی ویروس ها
- تولید امضاء برای ایمیل های اسپم
- شناسایی و از کار اندازی Botnet
- جمع آوری بدافزار و تحلیل آنها

مزایا و معایب

- مزایا
  - کاهش False Positive
  - شناسایی حملات جدید و کاهش False Negative
  - کارایی در تحلیل ترافیک های رمز شده
  - جمع آوری اطلاعات مفید با منابع محدود
- معایب
  - دید محدود
  - ریسک مورد سوء استفاده قرار گرفتن توسط مهاجم

انواع

- Low-interaction
  - سرویس ها، کاربردها و سیستم های عامل را شبیه سازی می کند.
  - ریسک پایینی دارد و به راحتی قابل استفاده و نگهداری است.
  - قادر به جمع آوری اطلاعاتی محدودی است.
- High-interaction
  - سرویس ها، کاربردها و سیستم های عامل واقعی هستند.
  - دارای ریسک بالایی است و زمان زیادی برای نگهداری آن لازم است.
  - قادر به جمع آوری اطلاعات گسترده ای است.

انواع سرورها

- Minimal servers
  - فقط چند پورت باز را فراهم می کند.
  - برای سرویس SMTP، اتصال را با ارسال پیام قطع می کند.
    - "503 Service Unavailable"
- Restricted servers
  - فراهم کننده تراکنش پایه ای
  - سرویس به صورت کامل به نظر می رسد.
  - برای سرویس telnet، کلمه و رمز عبور را از کاربر می گیرد.
    - ولی هیچگونه رمز عبوری معتبری وجود ندارد.

انواع سرورها (ادامه)

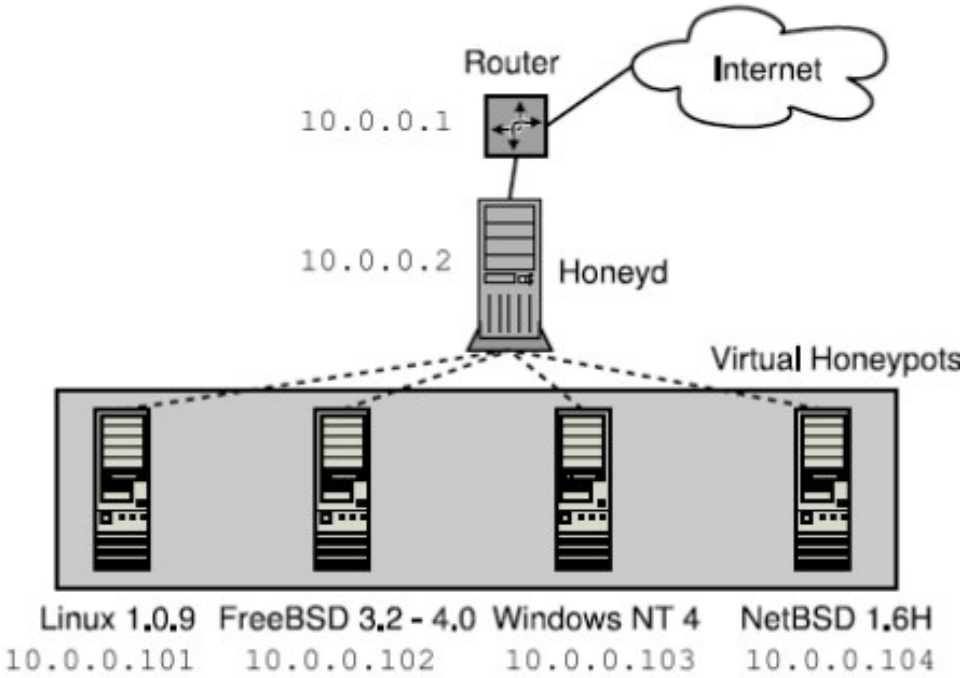
- Simulated servers
  - فراهم کننده تراکنش های پیچیده
  - درخواست ها را دریافت می کند و پاسخ های منطقی تولید می کند.
  - فقط فعالیت ها را ثبت می کند.
- Full servers
  - فراهم کننده کارکرد کامل
  - مهاجم به طور کامل با سرور تماس برقرار می کند و حتی از آن سوء استفاده کند.
  - اجازه برقراری اتصالات محدودی به بیرون شبکه را می دهد.
    - برای جلوگیری از شرکت Honeypot در حملات DDoS

Honeyd

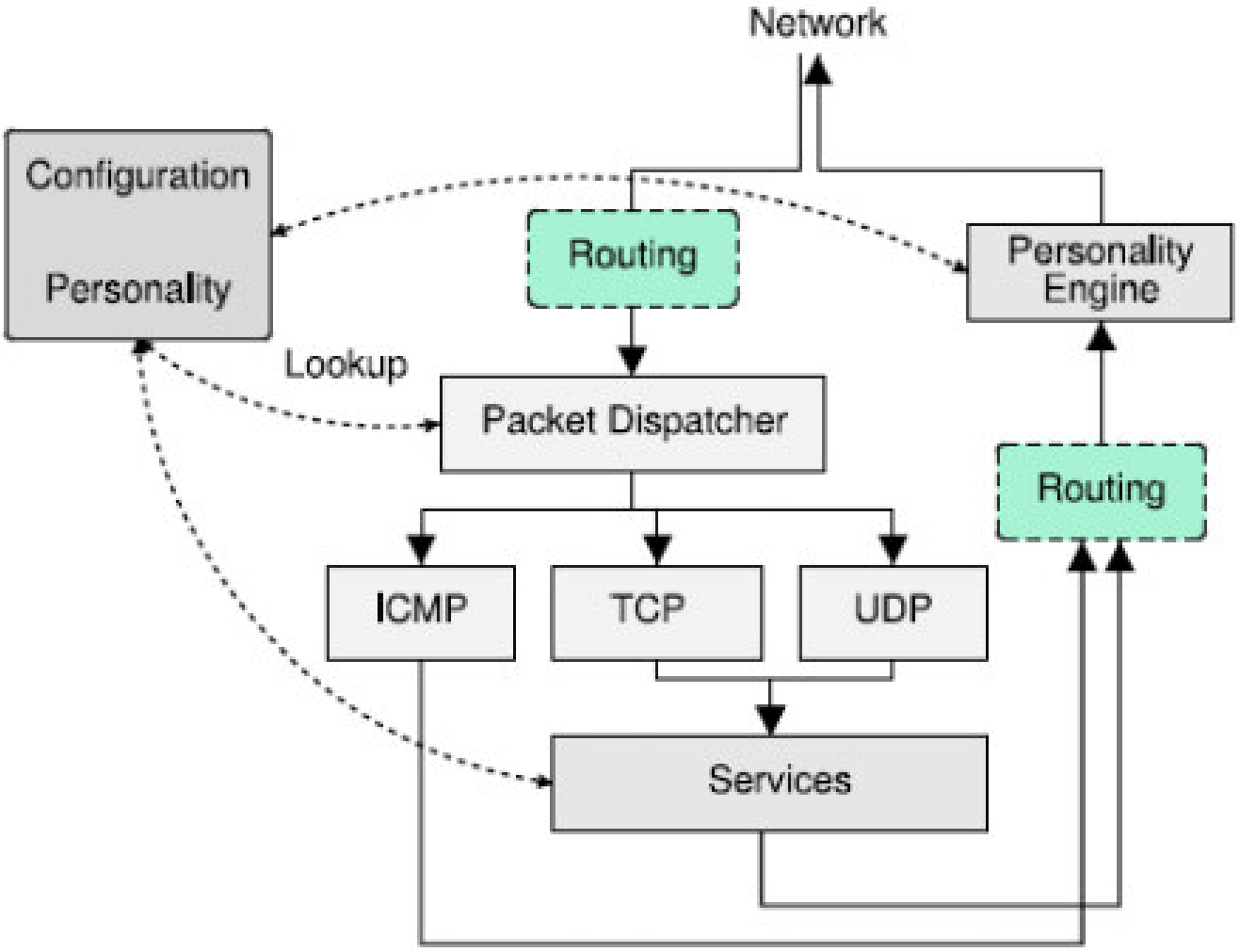
- یک honeypot مجازی low-interaction است.
  - سرویس های مهم TCP/UDP را شبیه سازی می کند.
    - IIS، Telnet، POP3 و ...
  - چندین آدرس IP را پشتیبانی می کند.
    - ۶۵۵۳۶ آدرس IP را همزمان شبیه سازی می کند.
  - پروتکل ICMP را پشتیبانی می کند.
    - ماشین های مجازی به ping و traceroute جواب می دهند.
  - پشتیبانی از ثبت
    - ثبت اتصالات و بسته ها

دریافت ترافیک شبکه

- Arpd سرویسی است که به درخواست های Arp مربوط به آدرس های IP آزاد پاسخ می دهد و ترافیک را به سمت honeypotهای مجازی هدایت می کند.



معماری


Network
Configuration
Personality
Routing
Personality
Engine
Lookup
Packet Dispatcher
Routing
ICMP
TCP
UDP
Services

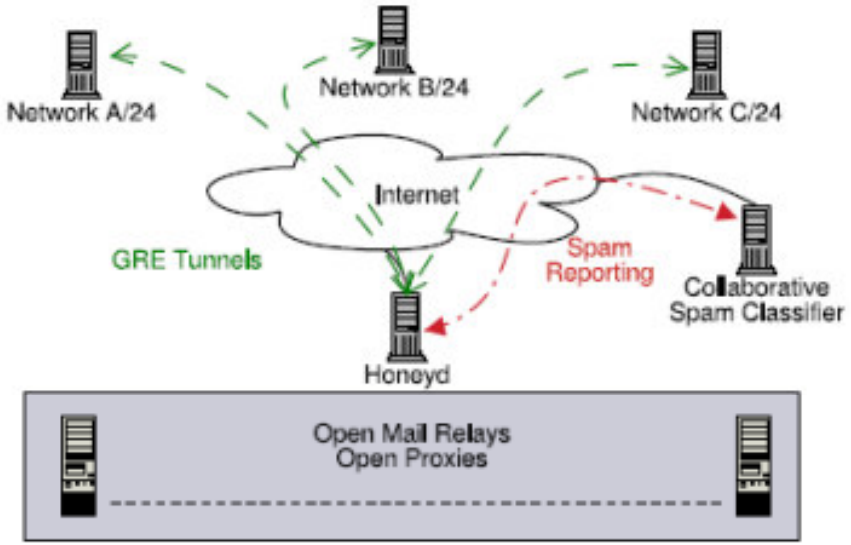
موتور شخصی سازی

- سیستم های عامل مختلف دارای رفتارهای مختلفی در پشته شبکه آن ها وجود دارد.
- مهاجمین از ابزارهایی مثل Nmap برای fingerprint هاست های مورد نظرشان استفاده می کنند.
- موتور شخصی سازی سعی می کند honeypot را به صورت یک سیستم واقعی نشان دهد.
- موتور شخصی سازی بسته های خروجی از honeypot را طوری تغییر می دهد تا در نگاه مهاجم واقعی جلوه کنند.

کاربردها

- Network Decoys
  - استفاده از آدرس های IP آزاد برای گمراه کردن مهاجمین و جلوگیری از اسکن کردن IPهای واقعی توسط مهاجمین
  - در تلفیق با NIDS موجب شناسایی زودتر حملات می شود.
- شناسایی و مقابله با کرم های جدید
  - پیاده سازی زیر سیستم هایی که در مقابل کرم ها آسیب پذیر باشند.
    - OpenSSH

کاربردها (ادامه)



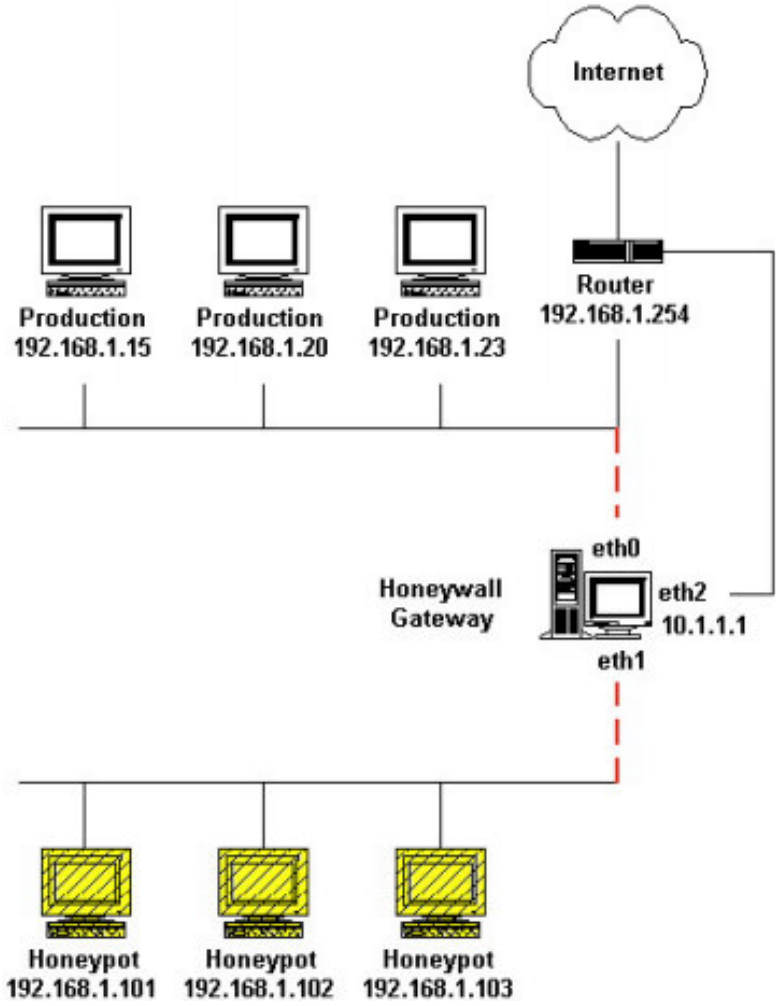
- جلوگیری از اسپم
  - زیر ساخت spammers
    - Proxy Servers
    - Open Mail Relays

Using the Honeyd framework, it is possible to instrument networks to automatically capture spam and submit it to collaborative filtering systems.

Honeynets

- یک high-interaction honeypot است که برای جمع آوری اطلاعات دقیق طراحی شده اند.
- ترافیک های ورودی و خروجی مشکوک هستند.
- یک شبکه بسیار کنترل شده که تمام بسته های ورودی و خروجی گرفته و بررسی می شود.
  - کنترل داده
  - گرفتن داده
  - تحلیل داده

معماری Honeynet

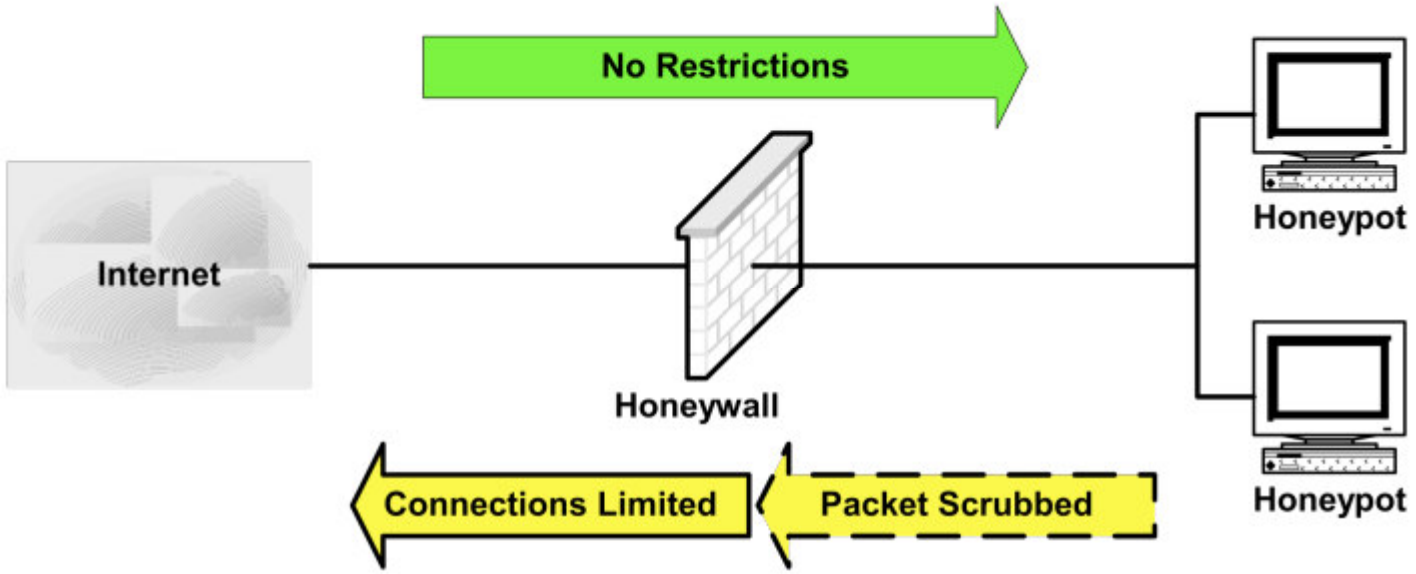


کنترل داده

- جلوگیری از مورد سوء استفاده قرار گرفتن honeynet برای حمله به سیستم های غیر honeynet
  - شمردن اتصالات برونسو و محدود کردن تعداد آن ها
  - IPS
  - کنترل پهنای باند

عدم کنترل داده

کنترل داده


No Restrictions
Internet
Honeypot
Honeywall
Honeypot
Connections Limited
Packet Scrubbed

Snort-Inline

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53
(msg:"DNS EXPLOIT named";flags: A+; content:"|
CD80 E8D7 FFFFFF|/bin/sh";
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53
(msg:"DNS EXPLOIT named";flags: A+; content:"|
CD80 E8D7 FFFFFF|/bin/sh"; replace:"|0000 E8D7
FFFFFF|/ben/sh";)
```

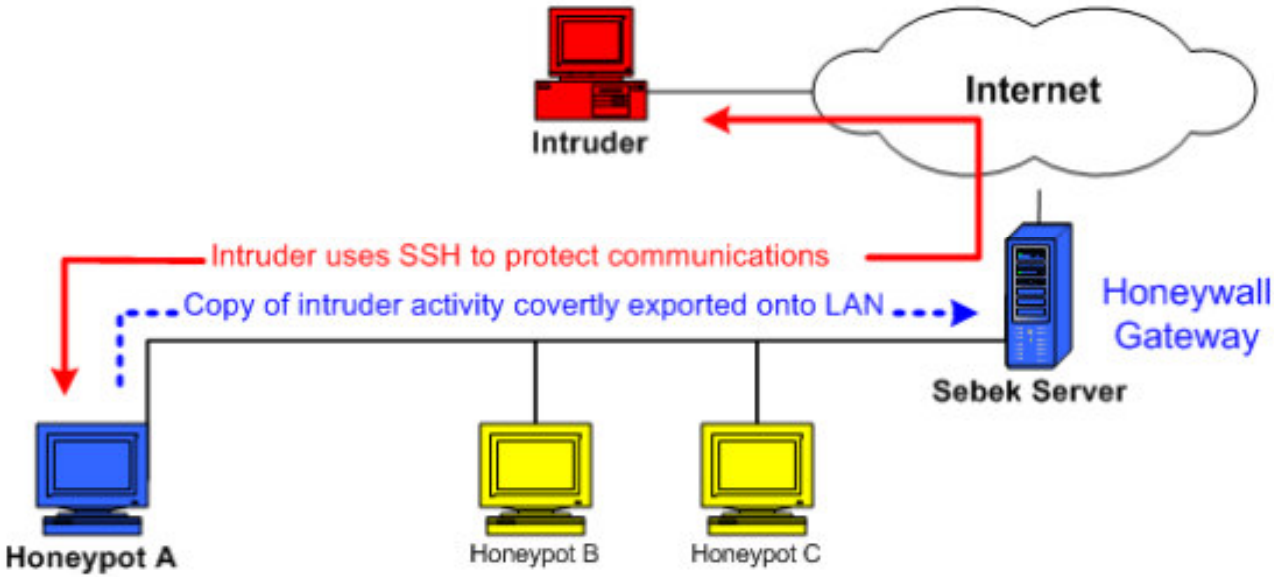
گرفتن داده

- گرفتن تمام فعالیت ها در لایه های مختلف
  - فعالیت های شبکه
  - فعالیت های کاربردها
  - فعالیت سیستمی

Sebek

- یک ماژول کرنل است که تمام فعالیت های هاست را گرفته و ثبت می کند.
- اطلاعات گرفته شده را روی شبکه قرار می دهد.
- مهاجم قادر به sniff کردن بسته های تولید شده توسط Sebek را ندارد.

معماری Sebek



حمله به Honeypot

- سوء استفاده
  - Honeypotها اصولاً در شبکه های محلی جدا و مجاور شبکه های مهم قرار دارند و بهترین سکو برای حملات به داخل شبکه است.
- مسموم کردن
  - مهاجم اطلاعات اشتباه و اطلاعات مهم را تحت الشعاع قرار می دهد.
- جاسوسی
  - هک کردن honeypot
  - شناسایی اطلاعات شخصی
  - شناسایی ساختار شبکه داخل سازمان

شناسایی Honeypot

- مشخصات فنی Honeypot
  - زمان پاسخ، banners، اطلاعات رجیستری، ناسازگاری پارامترها
- عدم تراکنش با کاربر
  - عدم ساخت و دسترسی فایل روی سرور برای مدت طولانی
- جستجوی درپای VMware
- جستجوی ردپای ابزارهای honeypot
  - پوشه های temp، ماژول های کرنل

مشخصات پشته TCP/IP در سیستم های عامل مختلف

OS	Platform	Vendor	Device/System	Default TTL	WINDOW SIZE	ID	DF bit
AIX 4.2.1	R6000	IBM	n/a	60	16384	+	Y
AIX 5.2	R6000	IBM	n/a	60	16384	+	N
FreeBSD 4.7	Intel	FreeBSD	n/a	64	57344	+	Y
Linux 2.4.20	Intel	Gentoo	n/a	64	32767	0	Y
Linux 2.4.20	Intel	Debian	n/a	64	5840	0	Y
Linux 2.4.21	Intel	SuSE	n/a	64	0	+	Y
Linux 2.4.21	Intel	RedHat	n/a	64	5840	+	Y
OS/400 5.1	Intel	?	n/a	64	8192	+	Y
Solaris 2.5.1	Sparc	Sun	n/a	255	9112	+	Y
Solaris 2.6	Sparc	Sun	n/a	255	9112	+	Y
Solaris 2.7	Sparc	Sun	n/a	255	9112	+	Y
Solaris 2.7	Sparc	Sun	n/a	255	9112	+	Y
Solaris 2.8	Sparc	Sun	n/a	255	24656	+	Y
Solaris 2.9	Intel	Sun	n/a	60	65392	+	Y
Windows 2000 Professional SP3	Intel	Microsoft	n/a	128	64512	+	Y
Windows 2000 Professional SP3	Intel	Microsoft	n/a	128	64240	+	Y
Windows 2000 Server SP4	Intel	Microsoft	n/a	128	65535	+	Y
Windows 2003 Server Standard	Intel	Microsoft	n/a	128	16616	+	Y
PIX 6.2.2	?	Cisco	n/a	257	4096	+	N
FreeBSD 4.9	Intel	FreeBSD	n/a	64	57344	+	Y
D-Link DWL-900+ Wireless AP	?	D-Link	Wireless AP	127	8192	+	N
Linux 2.4.24	Intel	Kernel.org	n/a	64	5840	0	Y
Solaris 2.8	Intel	Sun	n/a	60	65392	+	Y
Fiberline Broadband Router	?	Fiberline	Broadband Router	60	4096	+	N