

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

Computação
Científica Nacional

Honeypots

João Machado



Agenda

- O que é um Honeypot?
- Modern Honey Network



O QUE É UM HONEYPOT?

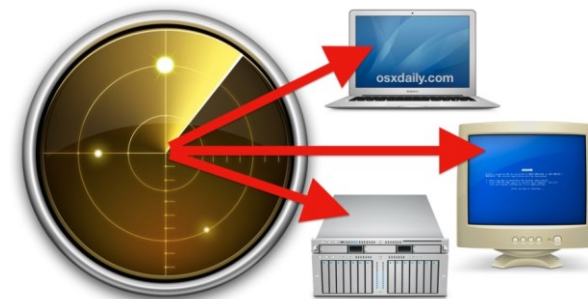
O que é um Honeypot ?

- Máquina que aparenta:
 - Correr um determinado serviço
 - Estar vulnerável a um ou mais ataques
- Regista toda a actividade com a máquina



Qual a finalidade dos Honeypots?

- Desvia atacantes de recursos valiosos
- Monitorização
- Facilita o estudo de ataques:
 - Quem ?
 - Como ?
 - Porquê ?
- Criação de feeds de segurança



Exemplo

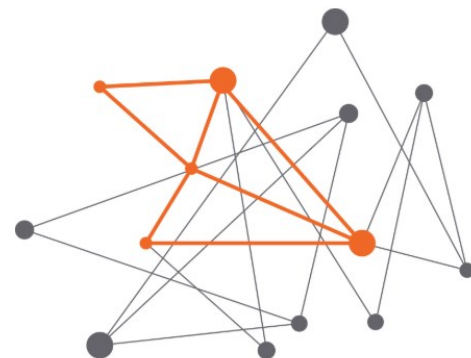
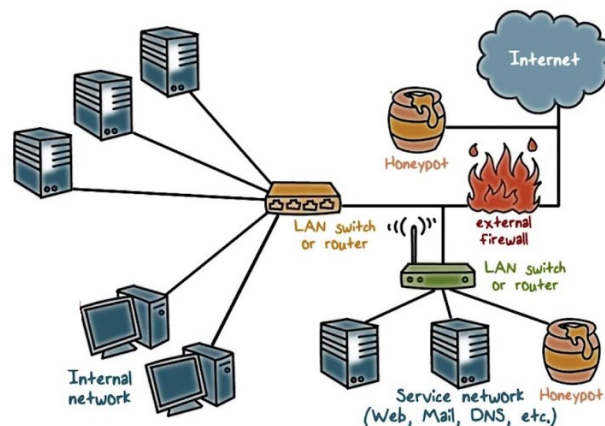
- HoneyTrain
- Infraestrutura
- Resultados



Tipos de Utilização

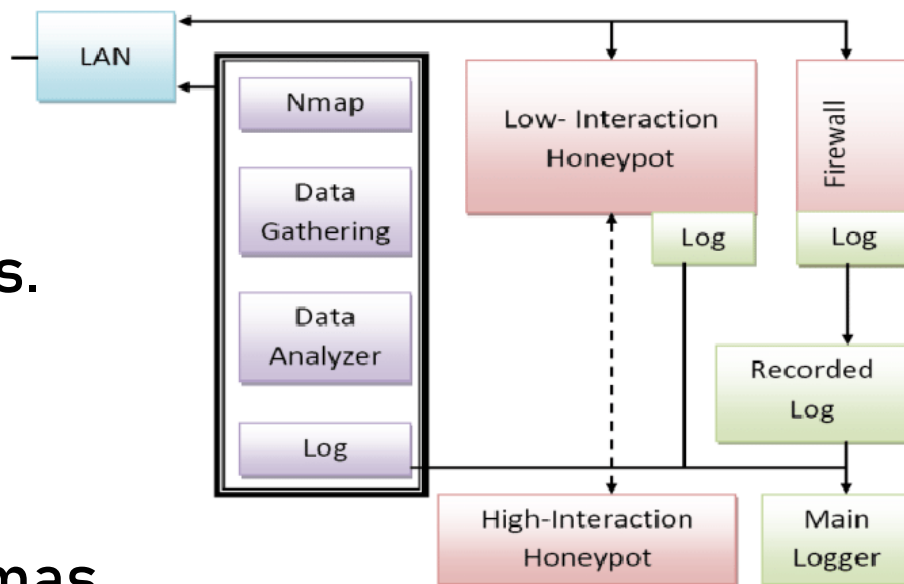
- Produção
 - Mecanismo de proteção e monitorização

- Investigação
 - Criação de threat feeds
 - Estudo de attack trends



Tipos de Distribuições

- Puras
 - Sistemas de produção completos.
- Baixa Interação
 - Serviços limitados com funcionalidades restritas.
- Alta Interação
 - Fornecem mais dados, mas com mais perigos.



Pros & Cons

- Falsos positivos
- Recursos
- Blind spots e ameaças internas
- HoneyWall
- Limitadas
- Podem ser identificadas
- Podem servir de entrada

Quais os custos?

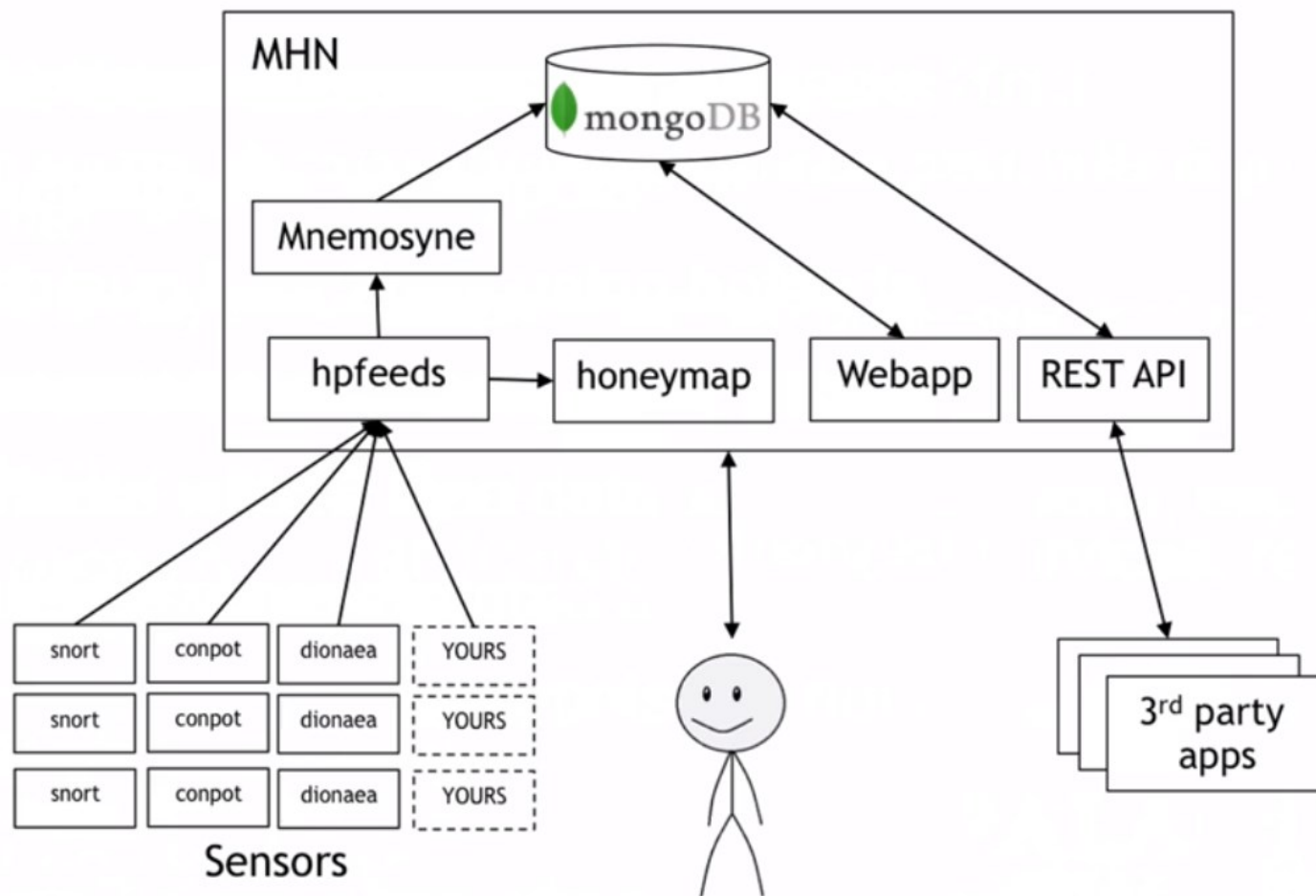
- Implementação
- Gestão
- Uma rede de honeypots requer:
 - Instalação e configuração de packages;
 - Gestão de todos os sensores na rede;
 - Criação de um processo de centralização dos dados recolhidos;
 - Tratamento e análise dos dados recolhidos.



Modern Honey Network



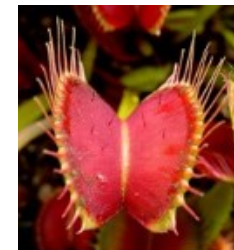
Arquitectura



Sensores

Honeypots

- Amun
- Cowrie
- Conpot
- Dionaea
- ElasticHoney
- Glastopf
- Shockpot
- Wordpot



Tools

- P0f
- Snort
- Suricata



Ataques Detetados

[MHN Server](#)[Map](#)[Deploy](#)[Attacks](#)[Payloads](#)[Rules](#)[Sensors](#)[Charts](#)[Settings](#)

Attack Stats

Attacks in the last 24 hours: **1**

TOP 5 Attacker IPs:

1.  193.136. (1 attacks)

TOP 5 Attacked ports:

1. 22 (1 times)

TOP 5 Honey Pots:

1. cowrie (1 attacks)

TOP 5 Sensors:

1. dionaeahp1 (1 attacks)





TOP 5 Attacks Signatures:

Detalhes dos Ataques

Attacks Report

Search Filters

Sensor:
 Honeypot:
 Date:
 Port:
 IP Address:

| | Date | Sensor | Country | Src IP | Dst port | Protocol | Honeypot |
|----|---------------------|------------|--|--|----------|----------|----------|
| 1 | 2018-11-20 10:28:43 | dionaeahp1 |  | 193.136.  | 22 | ssh | cowrie |
| 2 | 2018-11-19 06:50:32 | dionaeahp1 |  | 2001:690:  | 80 | pcap | p0f |
| 3 | 2018-11-18 06:53:05 | dionaeahp1 |  | 2001:690:  | 80 | pcap | p0f |
| 4 | 2018-11-17 06:44:36 | dionaeahp1 |  | 2001:690:  | 80 | pcap | p0f |
| 5 | 2018-11-16 16:43:18 | dionaeahp1 |  | 193.136.  | 2222 | pcap | p0f |
| 6 | 2018-11-16 16:42:33 | dionaeahp1 |  | 193.136.  | 22 | ssh | cowrie |
| 7 | 2018-11-16 16:42:10 | dionaeahp1 |  | 193.136.  | 22 | pcap | p0f |
| 8 | 2018-11-16 15:01:30 | dionaeahp1 |  | 193.136.  | 22 | ssh | cowrie |
| 9 | 2018-11-16 14:48:39 | dionaeahp1 |  | 193.136.  | 22 | ssh | cowrie |
| 10 | 2018-11-13 16:54:46 | dionaeahp1 |  | 193.136.  | 80 | httpd | dionaea |

Gestão de Regras

MHN Server

Map

Deploy

Attacks

Payloads

Rules ▾

Sensors ▾

Charts ▾

Settings

Rules Management

Search Filters

Signature Search String

Signature Name

GO

| | Date | SID | Rev | Revs | Message | Class Type | References | Notes | Active |
|---|---------------------|---------|-----|------|---|------------------------|----------------------|----------------------|-------------------------------------|
| 1 | 2018-11-12 14:57:25 | 2001624 | 13 | 1 | ET ACTIVEEX winhlp32 ActiveX control attack - phase 3 | web-application-attack | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |
| 2 | 2018-11-12 14:57:25 | 2001623 | 15 | 1 | ET ACTIVEEX winhlp32 ActiveX control attack - phase 2 | web-application-attack | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |
| 3 | 2018-11-12 14:57:25 | 2001622 | 15 | 1 | ET ACTIVEEX winhlp32 ActiveX control attack - phase 1 | web-application-attack | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |
| 4 | 2018-11-12 14:57:25 | 2012097 | 2 | 1 | ET ACTIVEEX WMItools ActiveX Remote Code Execution | attempted-user | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |
| 5 | 2018-11-12 14:57:25 | 2012098 | 2 | 1 | ET ACTIVEEX J-Integra ActiveX Setidentity Buffer Overflow | attempted-user | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |
| 6 | 2018-11-12 14:57:25 | 2014132 | 2 | 1 | ET ACTIVEEX HP Easy Printer Care Software XMLCacheMgr ActiveX Control Remote Code Execution Attempt | attempted-user | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |
| 7 | 2018-11-12 14:57:25 | 2014809 | 4 | 1 | ET ACTIVEEX Possible IBM Lotus Quickr for Domino ActiveX control Import_Times Method Access buffer overflow Attempt | attempted-user | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |
| 8 | 2018-11-12 14:57:25 | 2014808 | 5 | 1 | ET ACTIVEEX Possible IBM Lotus Quickr for Domino ActiveX control Attachment_Times Method Access buffer overflow Attempt | attempted-user | <input type="text"/> | <input type="text"/> | <input checked="" type="checkbox"/> |

Relatório dos Payloads

Payloads Report

Search Filters

Payload

suricata.events

Regex Term

pcre regex

GO

| timestamp | sensor | source_ip | destination_port | proto | signature |
|----------------------------|--------------------------------------|-------------|------------------|-------|---|
| 2021/05/21 17:14:50.378926 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 3306 | TCP | ET SCAN Suspicious inbound to MySQL port 3306 |
| 2021/05/04 10:33:42.919193 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 3306 | TCP | ET SCAN Suspicious inbound to MySQL port 3306 |
| 2020/10/01 15:43:58.757705 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 67 | UDP | ET POLICY Possible Kali Linux hostname in DHCP Request Packet |
| 2020/10/01 15:43:16.396857 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 67 | UDP | ET POLICY Possible Kali Linux hostname in DHCP Request Packet |
| 2020/08/18 17:24:25.852479 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 161 | UDP | GPL SNMP public access udp |
| 2020/08/18 17:23:24.830065 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 161 | UDP | GPL SNMP public access udp |
| 2020/08/18 17:22:50.346947 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 161 | UDP | GPL SNMP public access udp |
| 2020/06/18 14:56:20.881955 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 80 | ICMP | GPL ICMP_INFO PING BayRS Router |
| 2020/06/18 14:55:53.637379 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 80 | ICMP | GPL ICMP_INFO PING BayRS Router |
| 2020/03/12 16:33:20.623249 | 37d34c42-eb76-11e9-a0fb-000c2981ad97 | 192.168.1.1 | 161 | UDP | GPL SNMP public access udp |

Configuração de Sensores

Select Script

Ubuntu - Amun

Deploy Command

```
wget "http://10.10.10.10/api/script/?text=true&script_id=7" -O deploy.sh && sudo bash deploy.sh  
http://10.10.10.10 fo2MLxF9
```

Deploy Script

Name

Ubuntu - Amun

Script

```
#!/bin/bash  
  
set -e  
set -x  
  
if [ $# -ne 2 ]  
then  
    echo "Wrong number of arguments supplied."  
    echo "Usage: $0 <server_url> <deploy_key>."  
    exit 1  
fi  
  
server_url=$1  
deploy_key=$2  
  
apt-get update
```


Em Resumo



Importante para detetar intrusões em redes internas



Baixo custo de instalação e manutenção



Diversidade de serviços “simulados”



Obrigado