FCT Fundação para a Ciência e a Tecnologia
Computação Científica Nacional
FCCN

Modern Honey Network

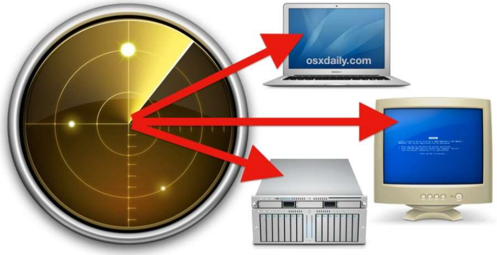
Pedro Esteves
ASA / SEG
20-Nov-2018

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 temporariamente os atacantes dos recursos valiosos
- Monitorização:
  - Atividade anormal na rede interna
  - Scans internos

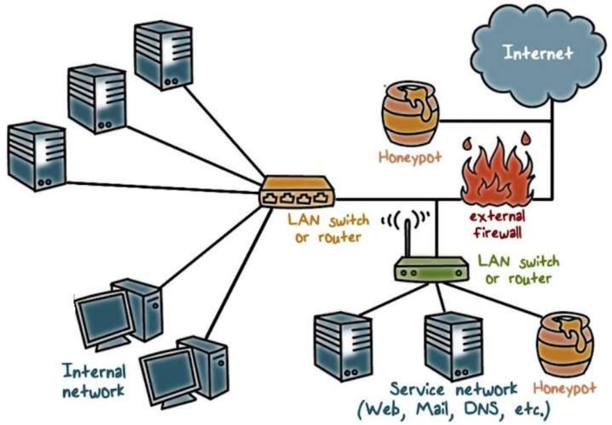


- Facilita o estudo de ataques:
  - Quem ?
  - Como ?
  - Porquê ?

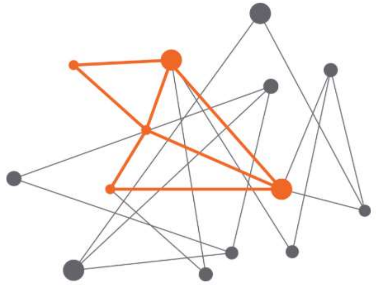
- Criação de feeds de segurança

QUAIS OS TIPOS DE UTILIZAÇÃO ?

- Produção
  - Mecanismo de proteção e monitorização



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



QUAIS OS CUSTOS ?

- Implementação dos honeypots

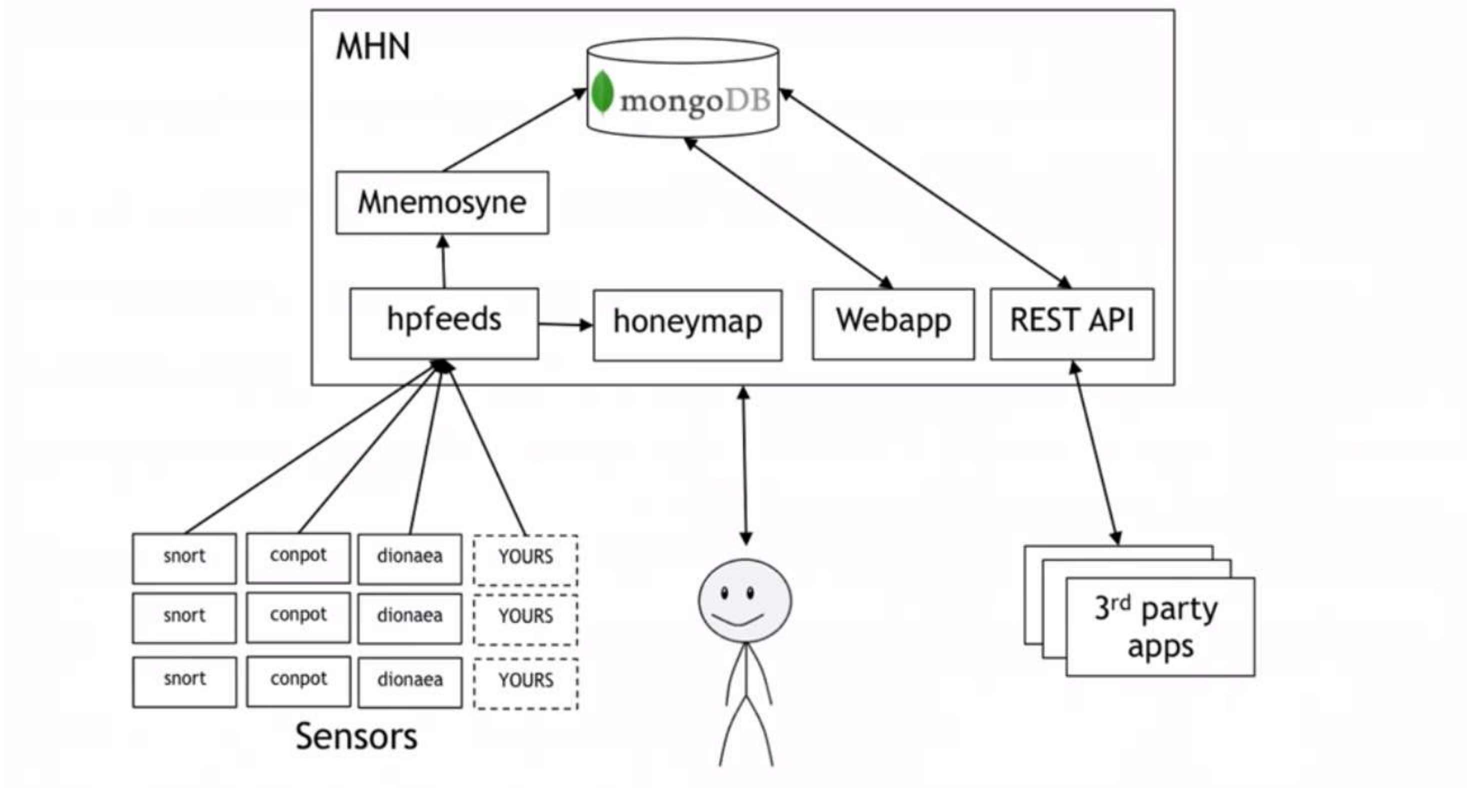
- Gestão dos honeypots e da informação gerada

- Uma rede de honeypots requer:
  - Instalação e configuração dos packages para cada honeypot;
  - 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

THREATSTREAM
Modern Honey Network (MHN)
Open Source Honeynet Management Platform

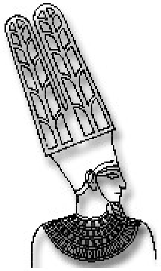
ARQUITECTURA

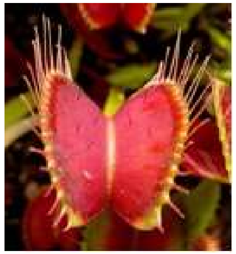


SENSORES

Honeypots

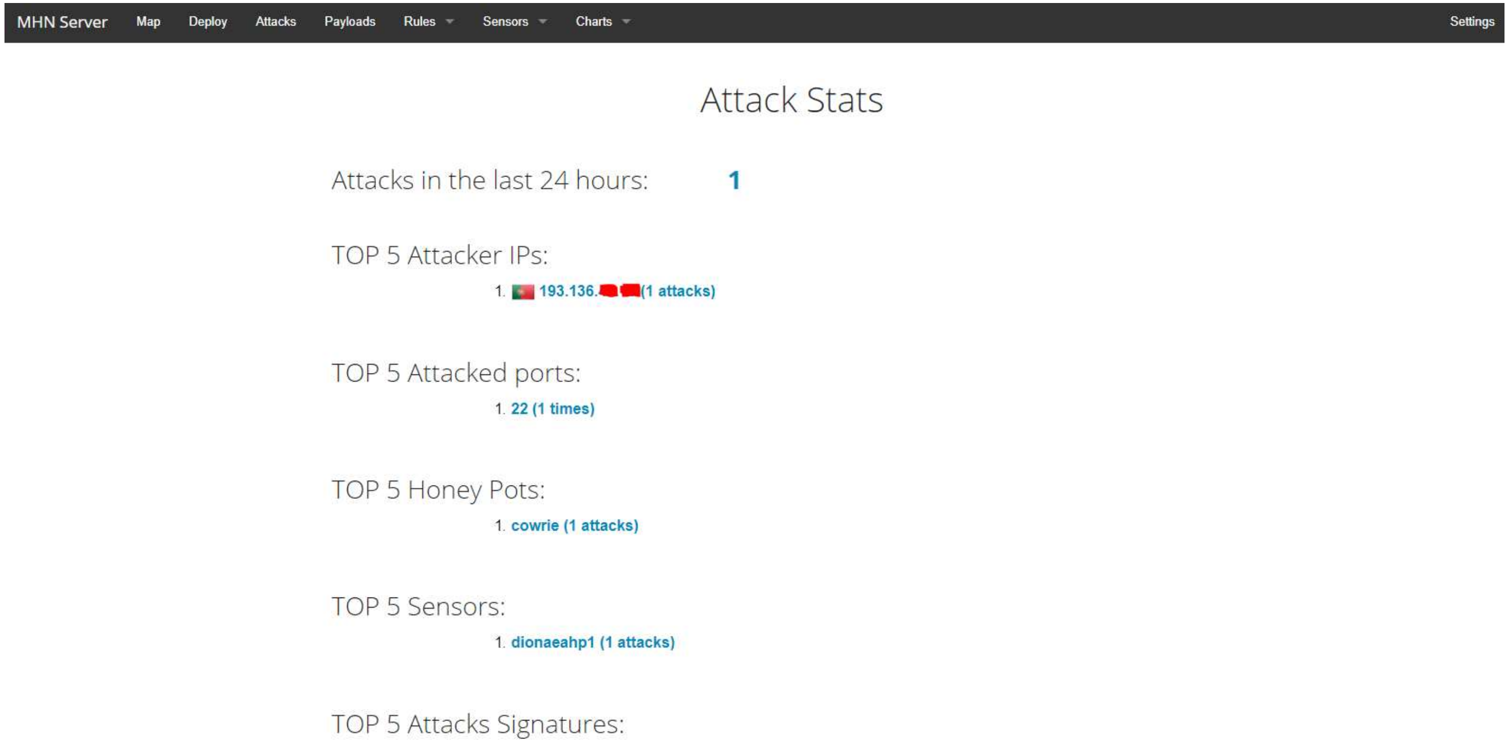
- Amun
- Cowrie
- Conpot
- Dionaea
- ElasticHoney
- Glastopf
- Shockpot
- Wordpot





Tools

- P0f
- Snort
- Suricata



Attack Stats

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

TOP 5 Attacker IPs:

1. 193.136.[redacted](1 attacks)

TOP 5 Attacked ports:

1. 22 (1 times)

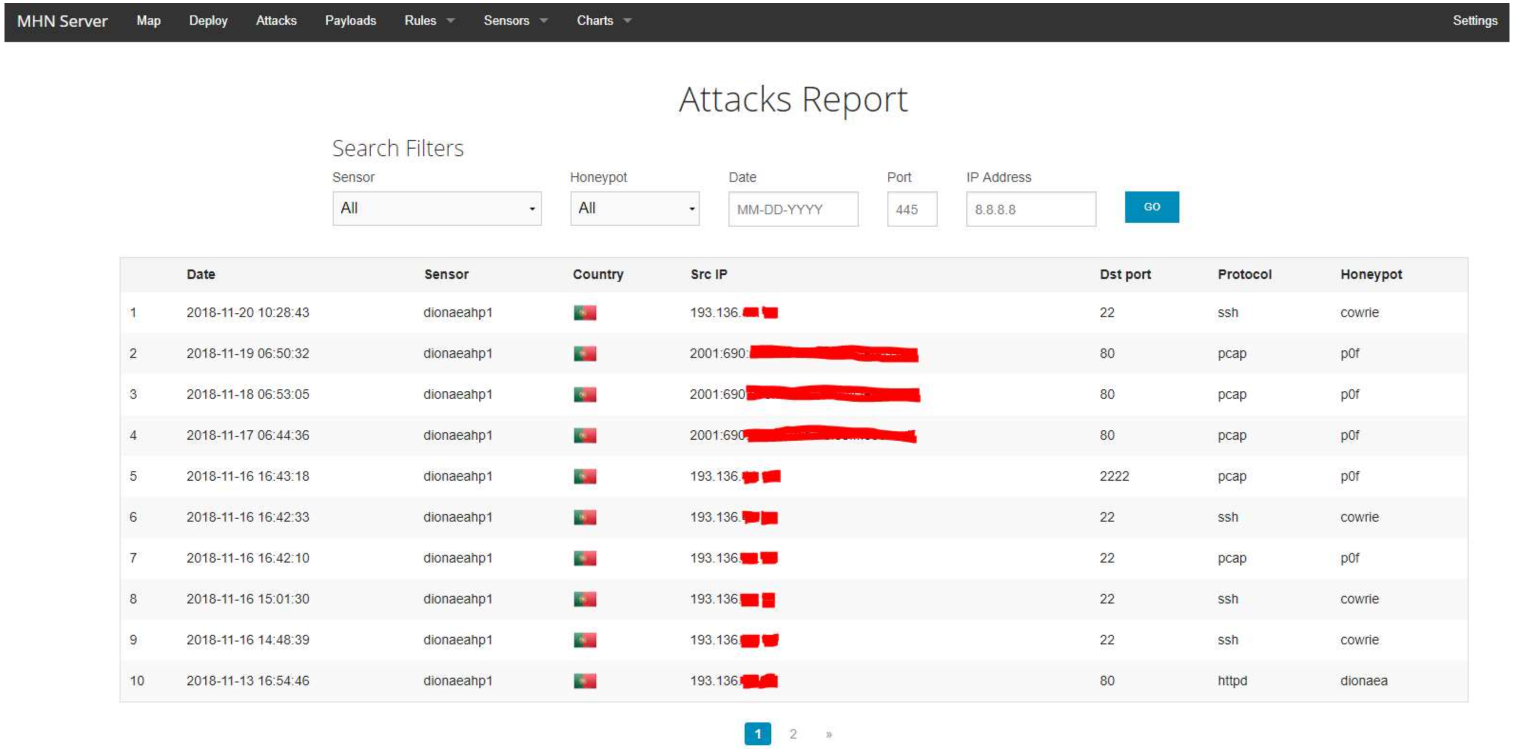
TOP 5 Honey Pots:

1. cowrie (1 attacks)

TOP 5 Sensors:

1. dionaeahp1 (1 attacks)

TOP 5 Attacks Signatures:

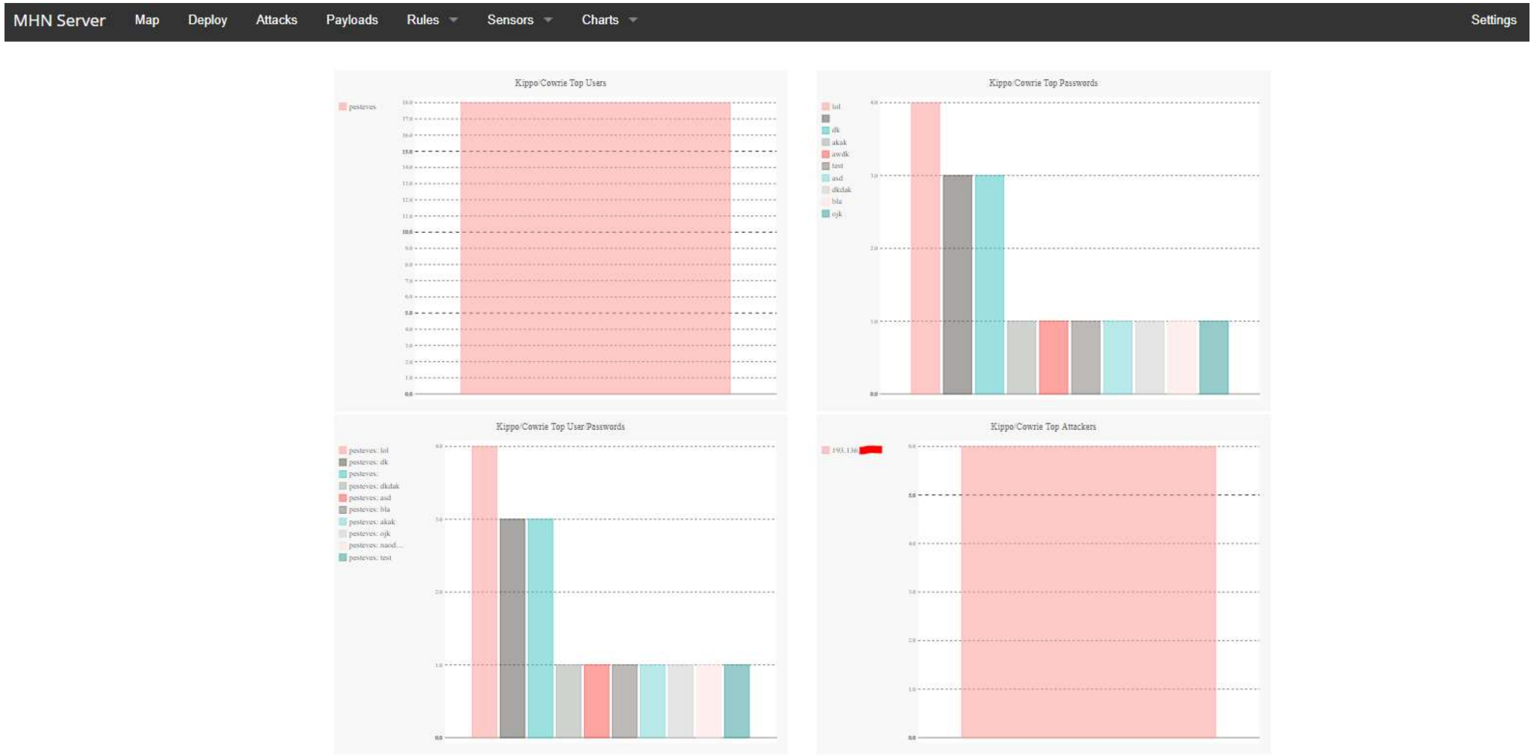


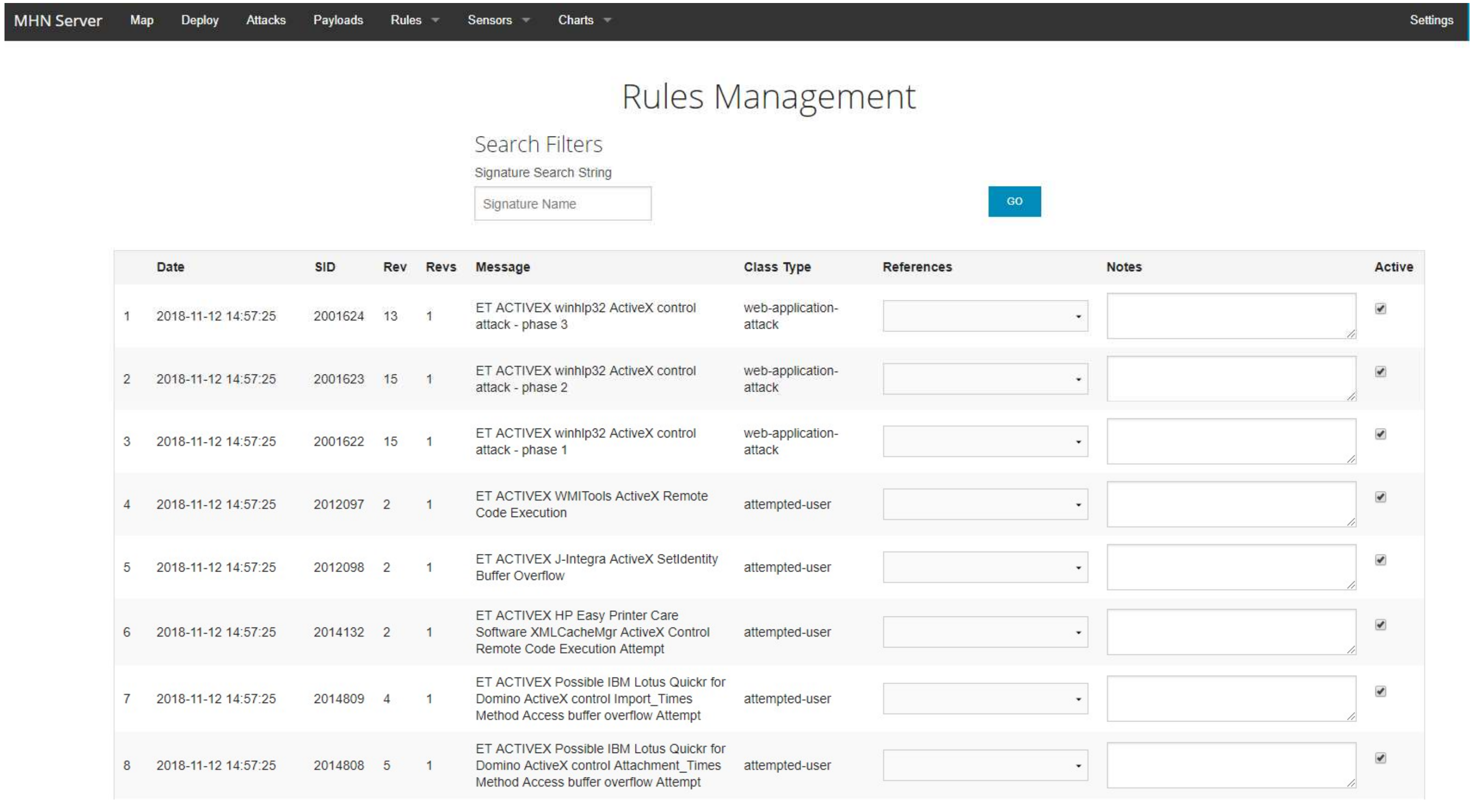
Attacks Report

Search Filters

Sensor	Honeypot	Date	Port	IP Address	
All	All	MM-DD-YYYY	445	8.8.8.8	GO

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


MHN Server
Map
Deploy
Attacks
Payloads
Rules
Sensors
Charts
Settings
Kippo/Cowrie Top Users
pesteves
18.0
17.0
16.0
15.0
14.0
13.0
12.0
11.0
10.0
9.0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
Kippo/Cowrie Top Passwords
lol
dk
akak
awdk
test
asd
dkdak
bla
ojk
4.0
3.0
2.0
1.0
0.0
Kippo/Cowrie Top User/Passwords
pesteves: lol
pesteves: dk
pesteves:
pesteves: dkdak
pesteves: asd
pesteves: bla
pesteves: akak
pesteves: ojk
pesteves: naod...
pesteves: test
4.0
3.0
2.0
1.0
0.0
Kippo/Cowrie Top Attackers
193.136 [redacted]
6.0
5.0
4.0
3.0
2.0
1.0
0.0



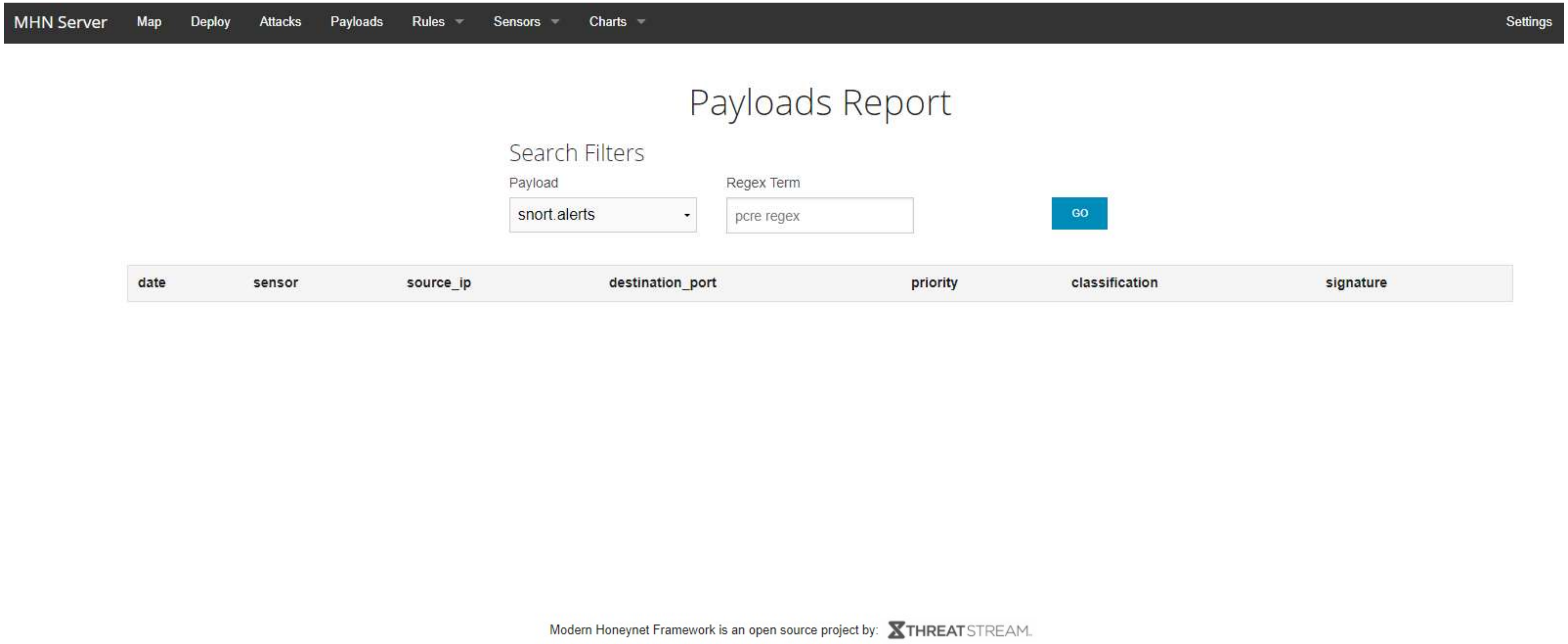
Rules Management

Search Filters

Signature Search String

Signature Name

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



Payloads Report

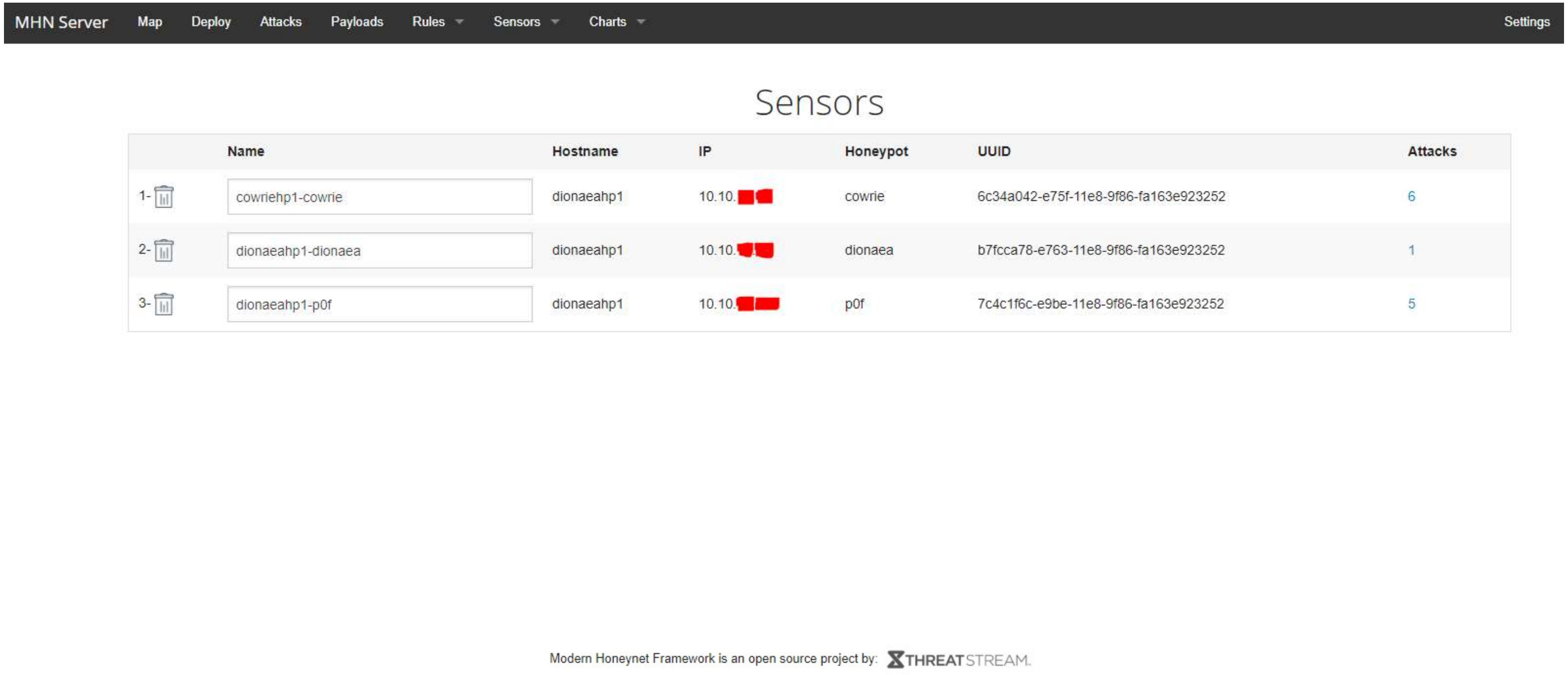
Search Filters

Payload: snort.alerts

Regex Term: pcre regex

date	sensor	source_ip	destination_port	priority	classification	signature

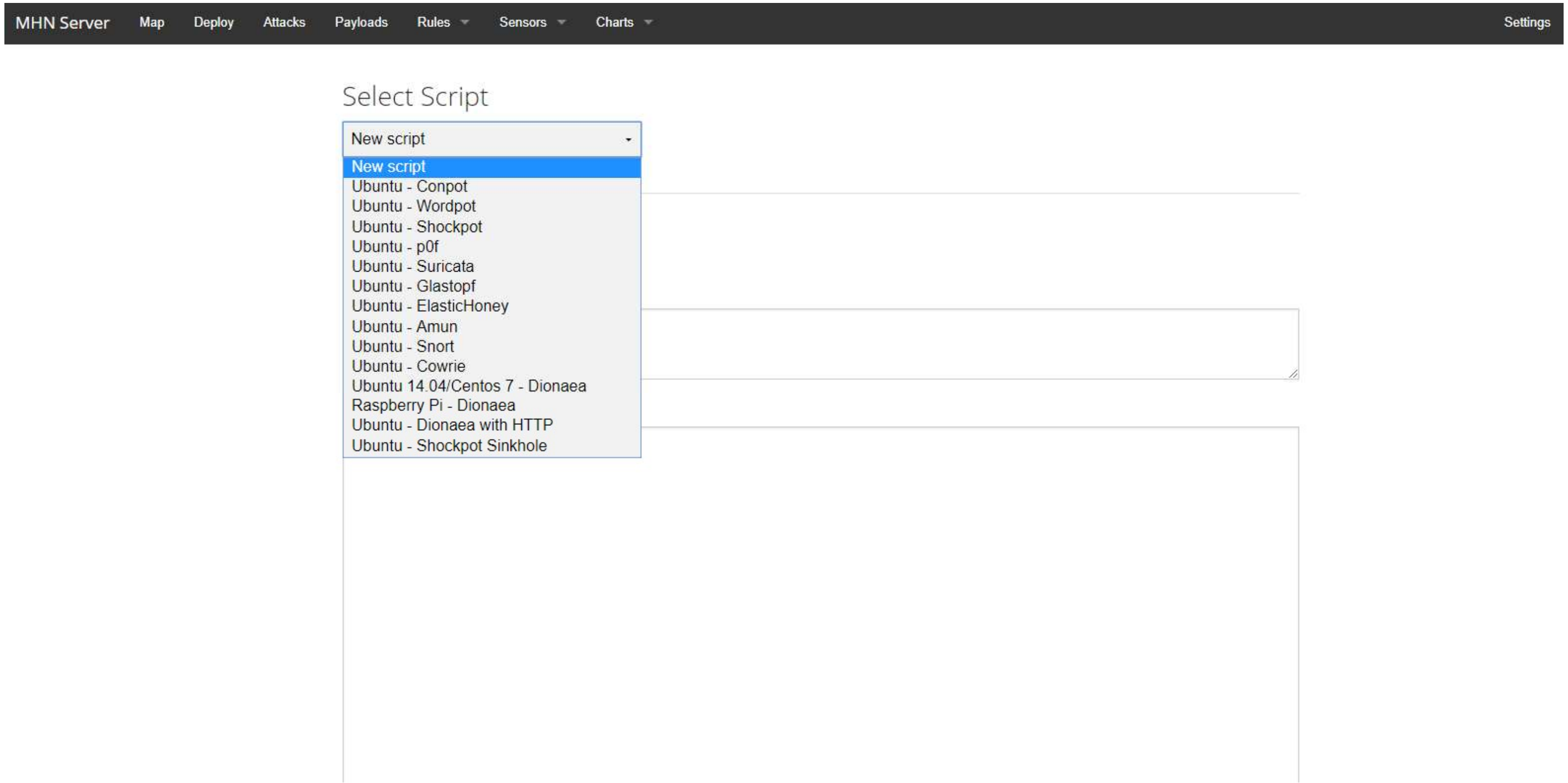
Modern Honeynet Framework is an open source project by: THREATSTREAM.



Sensors

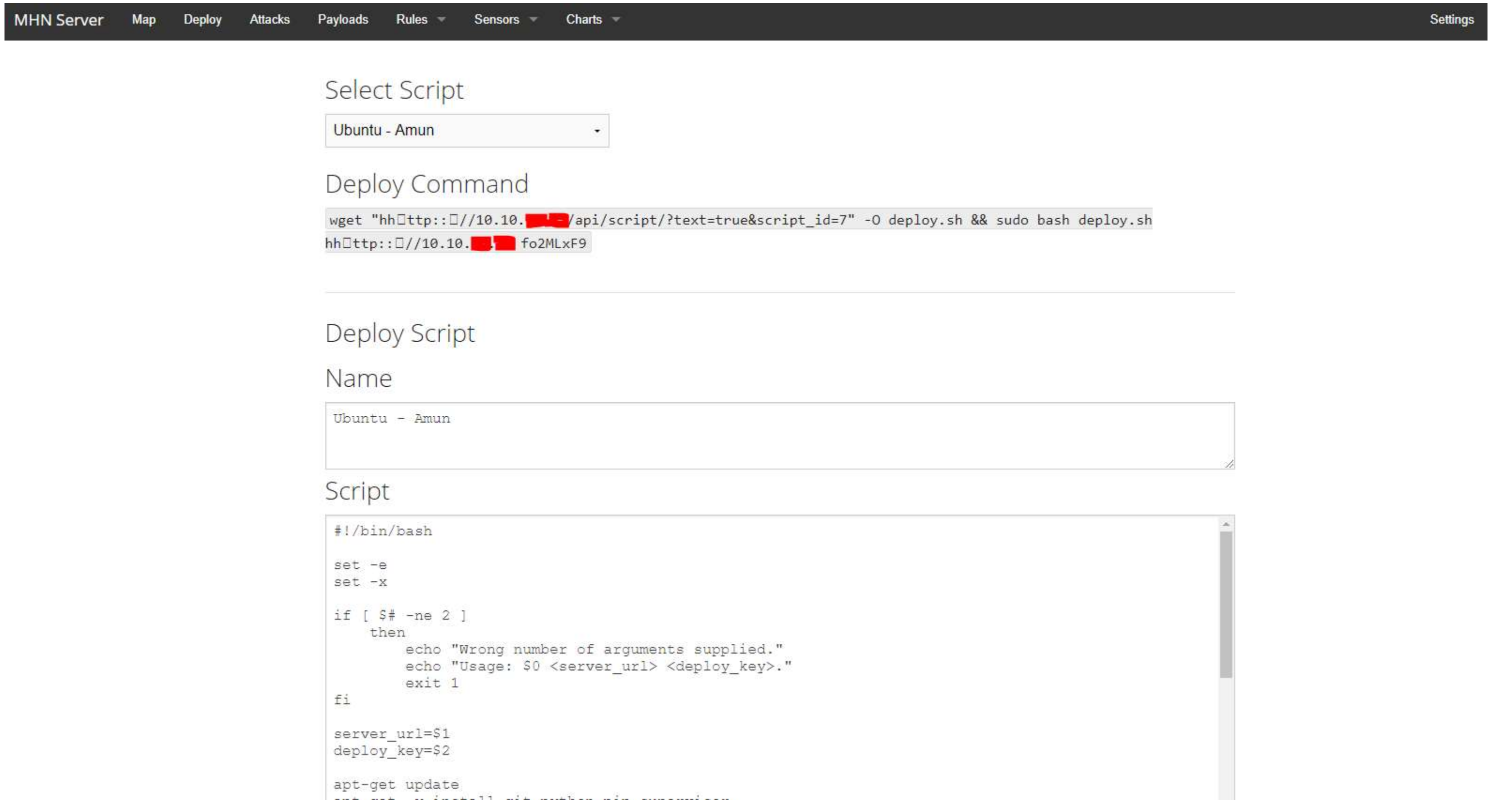
	Name	Hostname	IP	Honeypot	UUID	Attacks
1-	cowriehp1-cowrie	dionaeahp1	10.10.[redacted]	cowrie	6c34a042-e75f-11e8-9f86-fa163e923252	6
2-	dionaeahp1-dionaea	dionaeahp1	10.10.[redacted]	dionaea	b7fcca78-e763-11e8-9f86-fa163e923252	1
3-	dionaeahp1-p0f	dionaeahp1	10.10.[redacted]	p0f	7c4c1f6c-e9be-11e8-9f86-fa163e923252	5

Modern Honeynet Framework is an open source project by: THREATSTREAM.



Select Script

New script



Select Script

Ubuntu - Amun

Deploy Command

```
wget "hhttp:://10.10.[redacted]/api/script/?text=true&script_id=7" -O deploy.sh && sudo bash deploy.sh hhttp:://10.10.[redacted] 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
```

Perguntas

FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Obrigado pela atenção!

info@cert.rcts.pt