LIVE

INTRAREDE 2022

ATAQUES DE NEGAÇÃO DE SERVIÇO (DoS E DDoS): O QUE FAZER?

16/11 às 10h (UTC-3)

intrarede.nic.br

REALIZAÇÃO

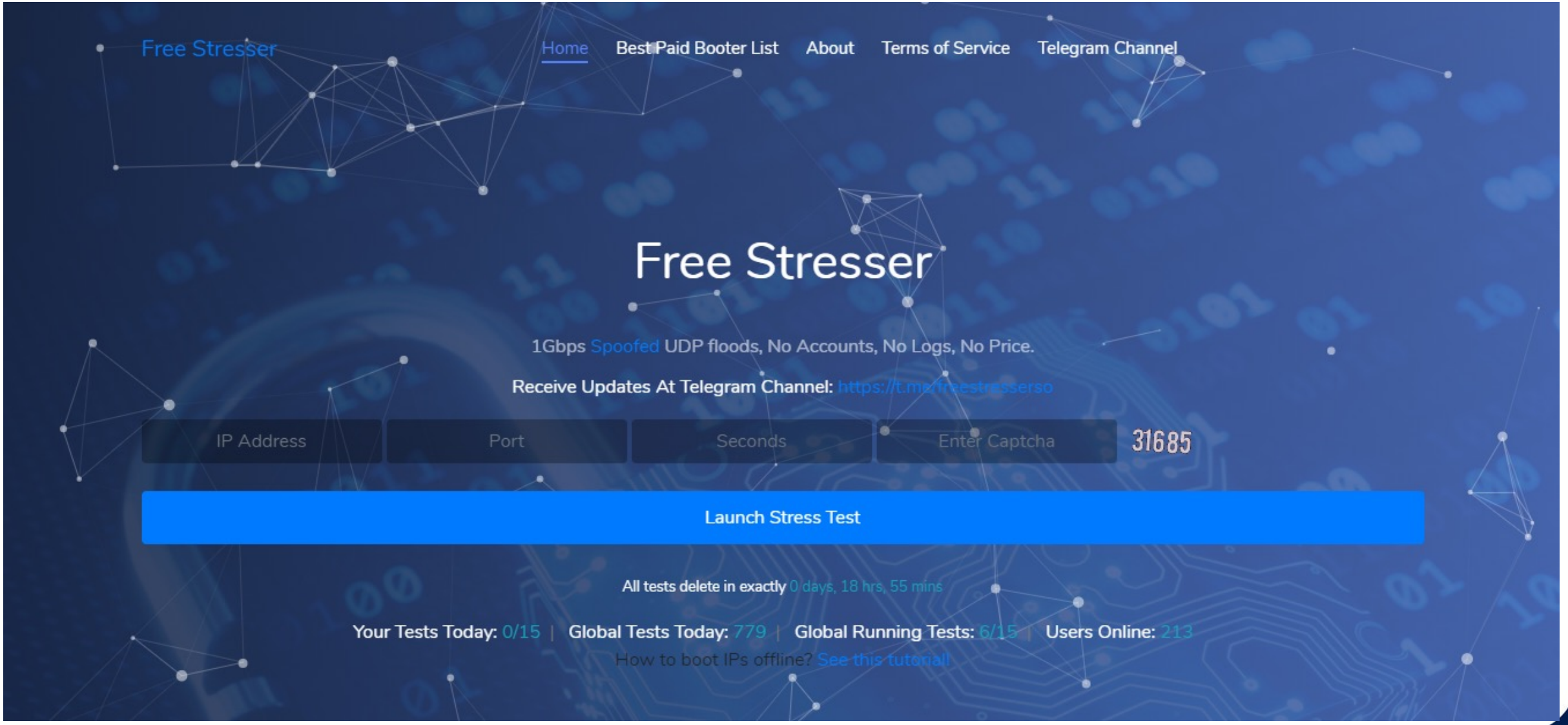
ceptro.br nic.br cgi.br

Profº. Lacier Dias

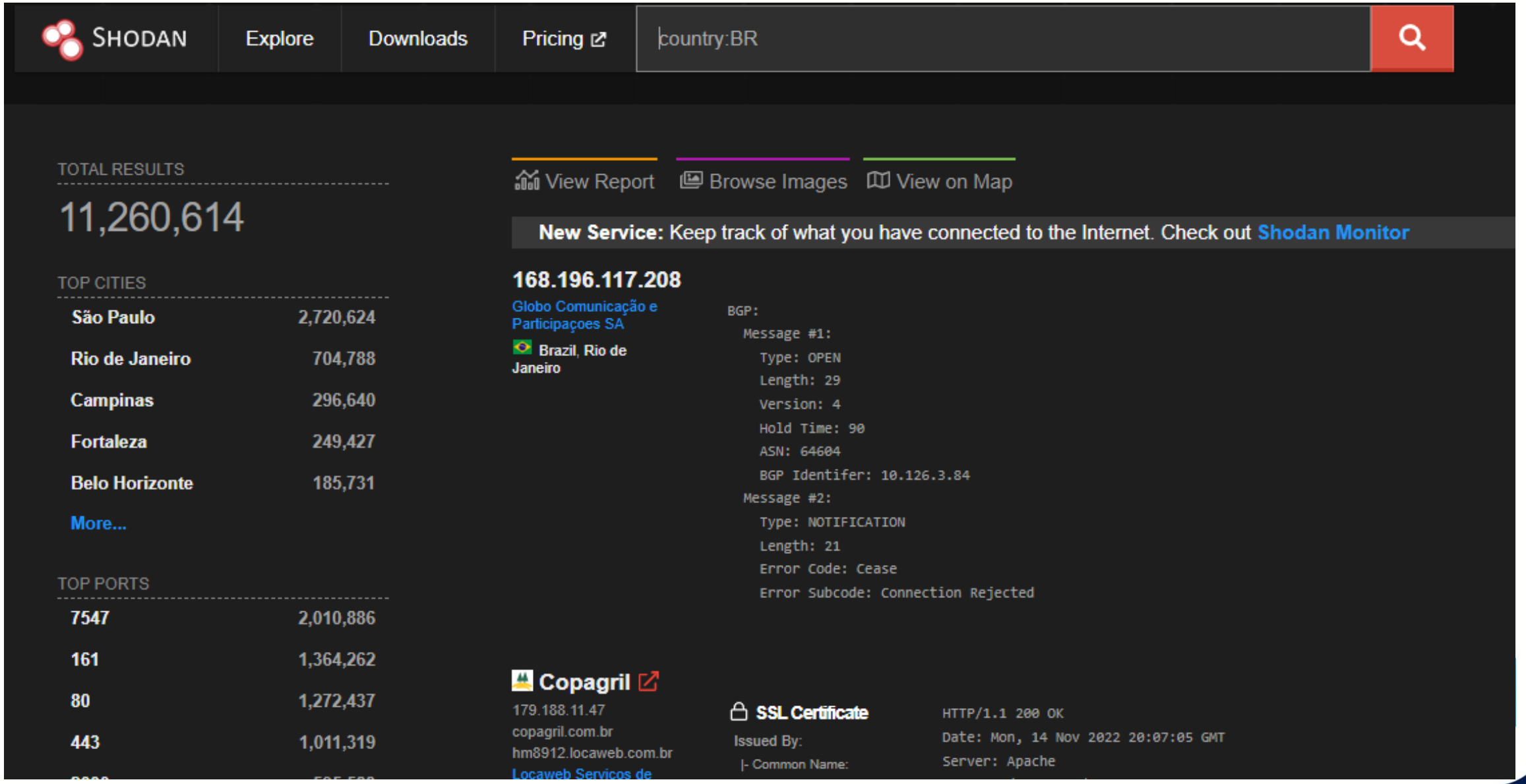
- ✓ Mestrando em Administração - FDC
- ✓ MBA em Gerenciamento de Projetos – FGV
- ✓ Pós-Graduado em Segurança de Rede de Computadores - UNIC

- ✓ Sócio e Diretor na Solintel, MOGA, OPA, TARS e VLSM, coordenando as áreas de Tecnologia e Ciência de Dados, auxiliando na concepção de projetos, produção e aprimoramento dos produtos da organização, com foco em projetar soluções completas para os clientes com base em produtos da organização ou projetando soluções sob medida a partir de projetos especiais.
- ✓ Com 20 anos de experiência no setor de telecom e como Professor de arquitetura, design e roteamento para redes, consultor para provedores de internet e palestrante em eventos do setor e workshops nacionais e internacionais.

SITES DE ATAQUE GRATUITO



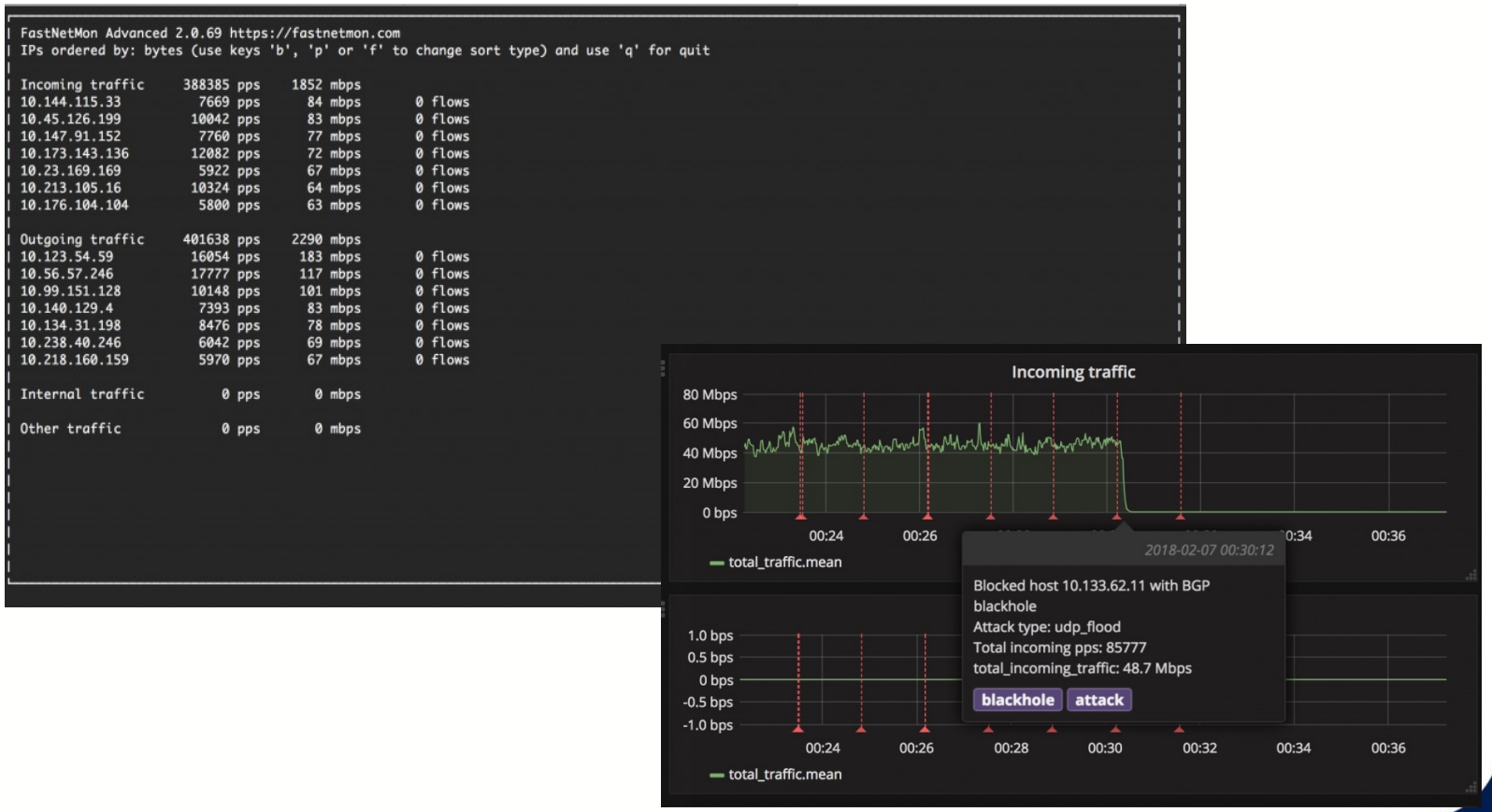
Shodan


SHODAN
Explore
Downloads
Pricing
country:BR
TOTAL RESULTS
11,260,614
TOP CITIES
São Paulo 2,720,624
Rio de Janeiro 704,788
Campinas 296,640
Fortaleza 249,427
Belo Horizonte 185,731
More...
TOP PORTS
7547 2,010,886
161 1,364,262
80 1,272,437
443 1,011,319
View Report
Browse Images
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
168.196.117.208
Globo Comunicação e Participaçoes SA
Brazil, Rio de Janeiro
BGP:
Message #1:
Type: OPEN
Length: 29
Version: 4
Hold Time: 90
ASN: 64604
BGP Identifer: 10.126.3.84
Message #2:
Type: NOTIFICATION
Length: 21
Error Code: Cease
Error Subcode: Connection Rejected
Copagril
179.188.11.47
copagril.com.br
hm8912.locaweb.com.br
Locaweb Servicos de
SSL Certificate
Issued By:
|- Common Name:
HTTP/1.1 200 OK
Date: Mon, 14 Nov 2022 20:07:05 GMT
Server: Apache

FASTNETMON

O fastnetmon é comumente utilizado para identificar anomalias de tráfego e automatizar o processo de blackhole a partir de coletas de netflow, é possível definir alguns parâmetros de análise como:

Número de pps;
mbps;
Flow/s;
Pacotes TCP por segundo;
Pacotes UDP por segundo;
Pacotes ICMP por segundo;
Pacotes TCP SYN por segundo;
TCP mbps;
TCP SYN mbps;
UDP mbps;
ICMP mbps.



MASSCAN

O Masscan é uma ferramenta de scan de portas, embora simples é muito funcional e pode auxiliar na enumeração de vulnerabilidades mais simples de modo ágil.

```
root@ip-10-0-1-12:/home/ubuntu# masscan -p 80,8080,8291,8295,4444,5555,443,22,25,23,21,2222,2323 --max-rate 10000

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2022-11-14 20:03:56 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1024 hosts [13 ports/ho
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 443/tcp on
Discovered open port 23/tcp on 4
Discovered open port 443/tcp on
Discovered open port 8291/tcp or
Discovered open port 80/tcp on 4
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 23/tcp on 4
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 80/tcp on 4
Discovered open port 8291/tcp or
Discovered open port 21/tcp on 4
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
Discovered open port 8291/tcp or
```

SPAMHAUS

A Spamhaus possui diversas ferramentas baseadas em listas de nomes de domínios e IP’s com má reputação. Essas reputações de domínio são calculadas a partir de muitos fatores e mantidas em um banco de dados que, por sua vez, alimenta as ferramentas

NMAP/Zenmap

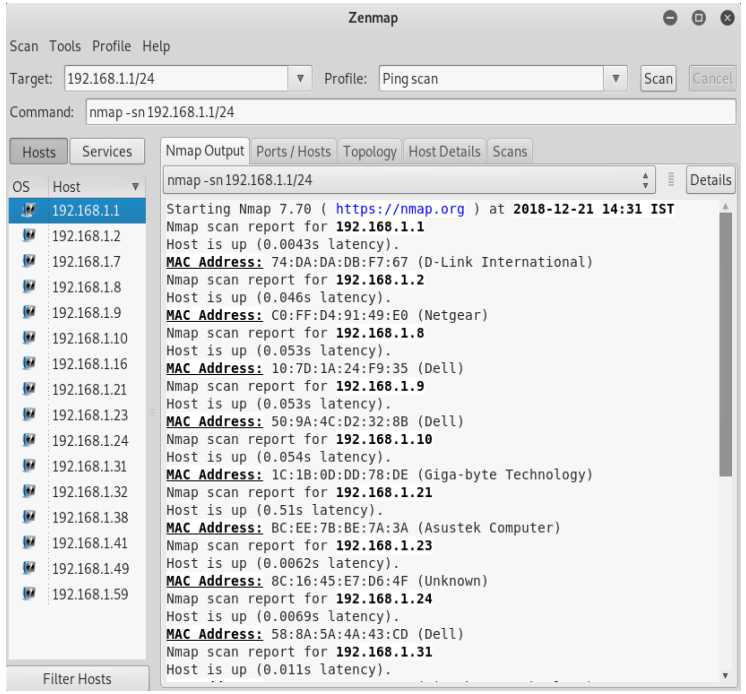
Outra ferramenta normalmente presente no kit de especialistas da área é o nmap.

```
$ nmap -A scanme.nmap.org

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-29 20:02 CET
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_  2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
9929/tcp open  nping-echo Nping echo
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|storage-misc|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (94%), Netgear RAIDiator 4.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.38 cpe:/o:linux:linux_kernel:3 cpe:/o:netgear:raidiator:4 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.38 (94%), Linux 3.0 (92%), Linux 2.6.32 - 3.0 (91%), Linux 2.6.18 (91%), Linux 2.6.39 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 2.6.38
- 3.0 (90%), Linux 2.6.38 - 2.6.39 (89%), Linux 2.6.35 (88%), Linux 2.6.37 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   14.21 ms  151.217.192.1
2   5.27 ms   ae10-0.mx240-iphh.shitty.network (94.45.224.129)
3   13.16 ms  hmb-s2-rou-1102.DE.eurorings.net (134.222.120.121)
4   6.83 ms   blnb-s1-rou-1041.DE.eurorings.net (134.222.229.78)
5   8.30 ms   blnb-s3-rou-1041.DE.eurorings.net (134.222.229.82)
6   9.42 ms   as6939.bcix.de (193.178.185.34)
7   24.56 ms  10ge10-6.core1.ams1.he.net (184.105.213.229)
8   30.60 ms  100ge9-1.core1.lon2.he.net (72.52.92.213)
9   93.54 ms  100ge1-1.core1.nyc4.he.net (72.52.92.166)
10  181.14 ms 10ge9-6.core1.sjc2.he.net (184.105.213.173)
11  169.54 ms 10ge3-2.core3.fmt2.he.net (184.105.222.13)
12  164.58 ms router4-fmt.linode.com (64.71.132.138)
13  164.32 ms scanme.nmap.org (74.207.244.221)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.98 seconds
```



GVM (OpenVas)

- OpenVAS (Open Vulnerability Assessment System), em português Sistema Aberto de Avaliação de Vulnerabilidade, é um framework de vários serviços e ferramentas que oferece uma solução de varredura e gerenciamento de vulnerabilidade.

Pontos de destaque

- Usa o Greenbone Community Feed para executar mais de 50.000 testes de vulnerabilidade;
- Código aberto;
- Desenvolvido e mantido gratuitamente pela Greenbone Networks;
- Suporta mais de 44.000 CVEs.

GVM (OpenVas)

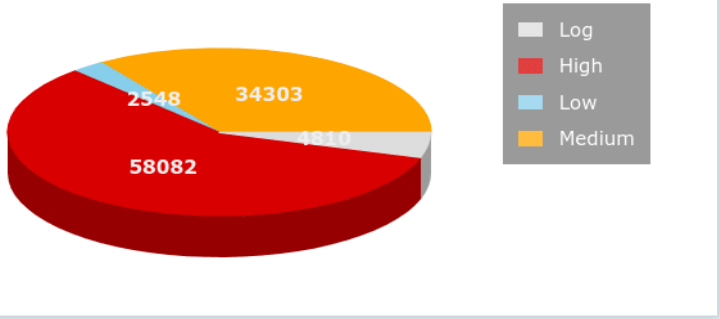
Greenbone Security Assistant

Dashboards | Scans | Assets | Resilience | SecInfo | Configuration | Administration | Help

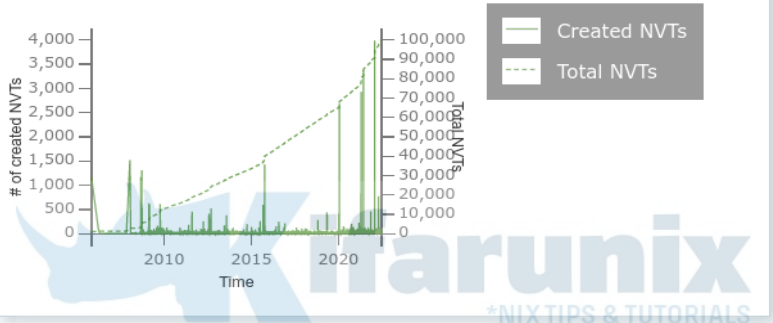
Filter --

NVTs 99743 of 99743

NVTs by Severity Class (Total: 99743)



NVTs by Creation Time

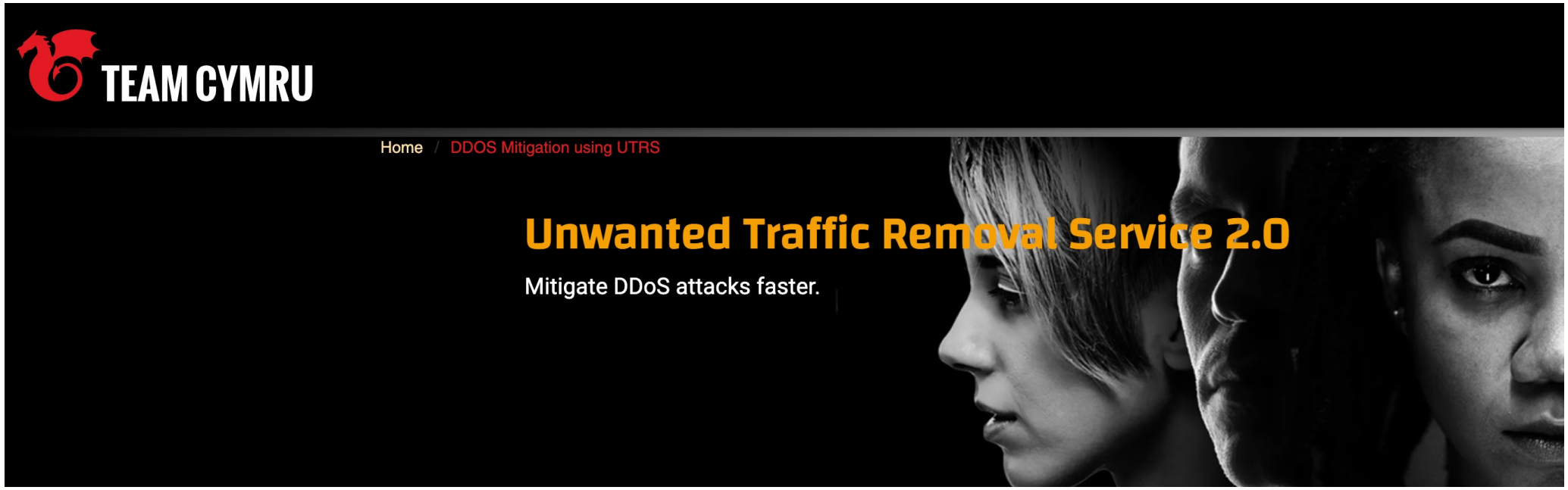


NVTs by Family (Total: 99743)

1 - 10 of 99743

Name	Family	Created ▼	Modified	CVE	Severity	QoD
Jenkins < 2.356, < 2.332.4 LTS Information Disclosure Vulnerability (SECURITY-2566) - Windows	Web application abuses	Fri, Jun 24, 2022 6:58 AM UTC	Fri, Jun 24, 2022 6:58 AM UTC	CVE-2022-34174	5.0 (Medium)	80 %
Jenkins < 2.356, < 2.332.4 LTS Information Disclosure Vulnerability (SECURITY-2566) - Linux	Web application abuses	Fri, Jun 24, 2022 6:51 AM UTC	Fri, Jun 24, 2022 6:56 AM UTC	CVE-2022-34174	5.0 (Medium)	30 %
Jenkins 2.335 < 2.356 Information Disclosure Vulnerability (SECURITY-2777) - Windows	Web application abuses	Fri, Jun 24, 2022 6:48 AM UTC	Fri, Jun 24, 2022 6:49 AM UTC	CVE-2022-34175	4.0 (Medium)	80 %
Jenkins 2.335 < 2.356 Information Disclosure Vulnerability (SECURITY-2777) - Linux	Web application abuses	Fri, Jun 24, 2022 6:41 AM UTC	Fri, Jun 24, 2022 6:47 AM UTC	CVE-2022-34175	4.0 (Medium)	30 %
Jenkins 2.340 < 2.356 Multiple Vulnerabilities (SECURITY-2776, SECURITY-2780) - Windows	Web application abuses	Fri, Jun 24, 2022 6:39 AM UTC	Fri, Jun 24, 2022 6:40 AM UTC	CVE-2022-34172 CVE-2022-34173	4.9 (Medium)	80 %
Jenkins 2.340 < 2.356 Multiple Vulnerabilities (SECURITY-2776, SECURITY-2780) - Linux	Web application abuses	Fri, Jun 24, 2022 6:01 AM UTC	Fri, Jun 24, 2022 6:37 AM UTC	CVE-2022-34172 CVE-2022-34173	4.9 (Medium)	30 %
Jenkins 2.321 < 2.356, 2.332.1 LTS < 2.332.4 LTS XSS Vulnerability (SECURITY-2761) - Windows	Web application abuses	Fri, Jun 24, 2022 5:52 AM UTC	Fri, Jun 24, 2022 5:53 AM UTC	CVE-2022-34171	4.3 (Medium)	80 %

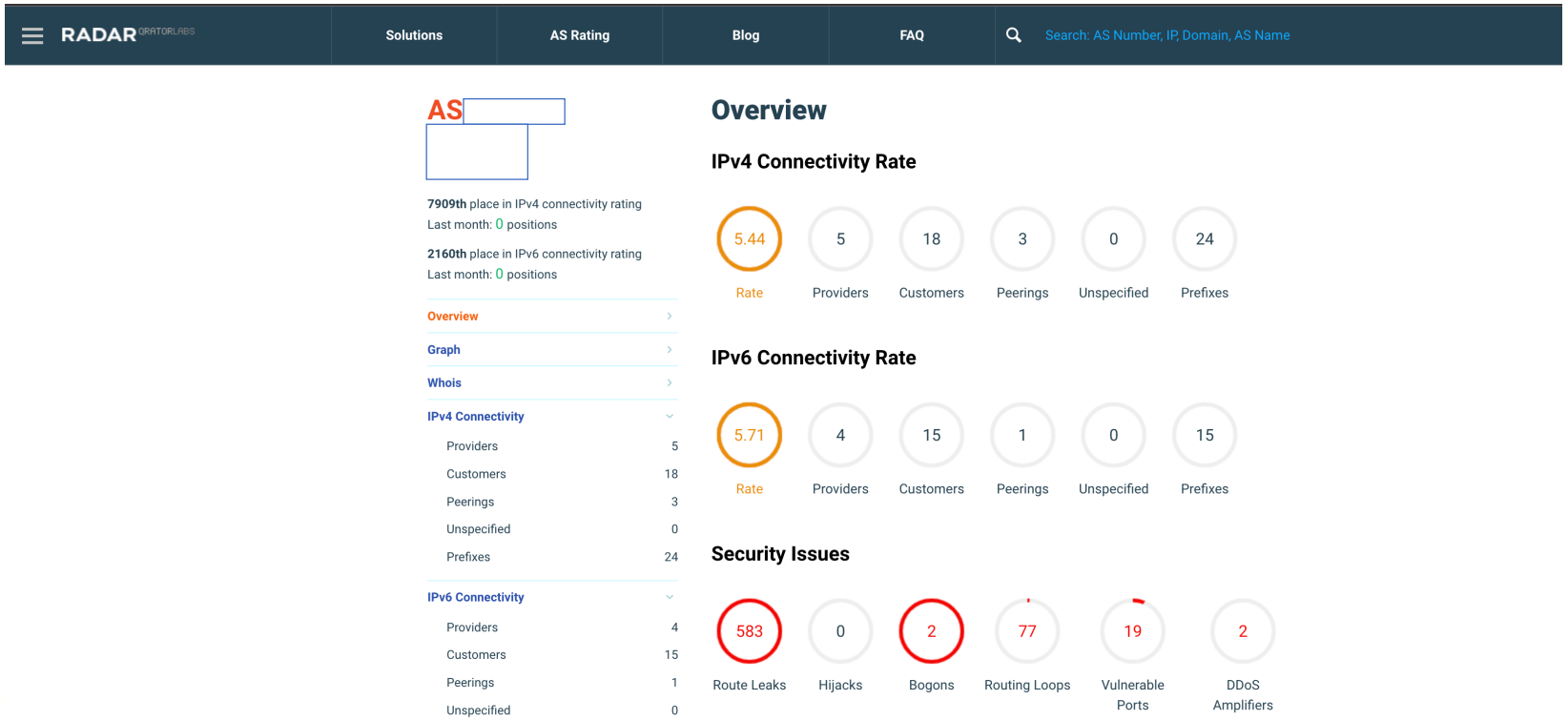
UTRS - Unwanted Traffic Removal Service



UTRS 2.0, é um serviço baseado em BGP que é uma ferramenta para ajudar a mitigar ataques DDoS, exclusivamente para proprietários de ASN globalmente exclusivo, o UTRS 2.0 adiciona suporte para FlowSpec, IPv6, aumenta os tamanhos de anúncio de IPv4 e IPv6, confiabilidade aprimorada com sessões de emparelhamento redundantes e ROA's são honrados.

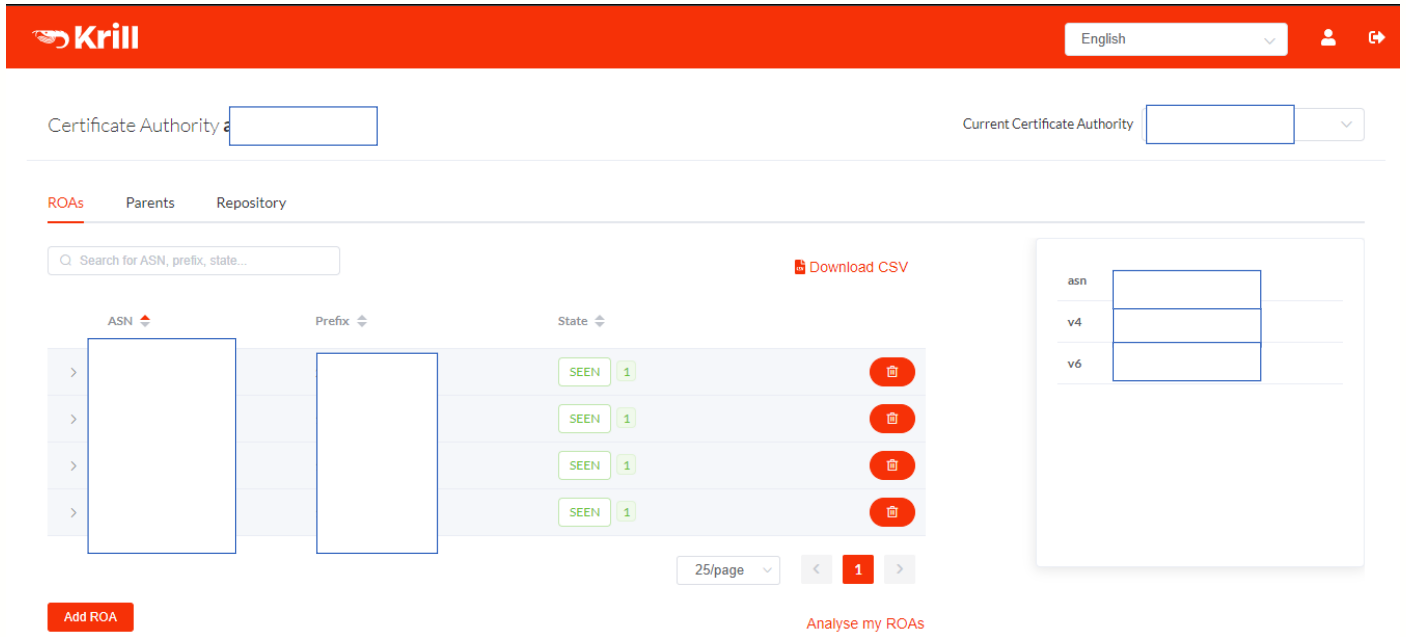
Reduza os ataques DDoS como uma comunidade:
O UTRS v2.0 usa técnicas como buracos negros acionados remotamente (RTBH),
mas globalmente. Juntos, permitimos que você se proteja enquanto ajudamos a proteger a Internet.
Você ajuda seu próximo e ele te ajuda.

Radar Qrator



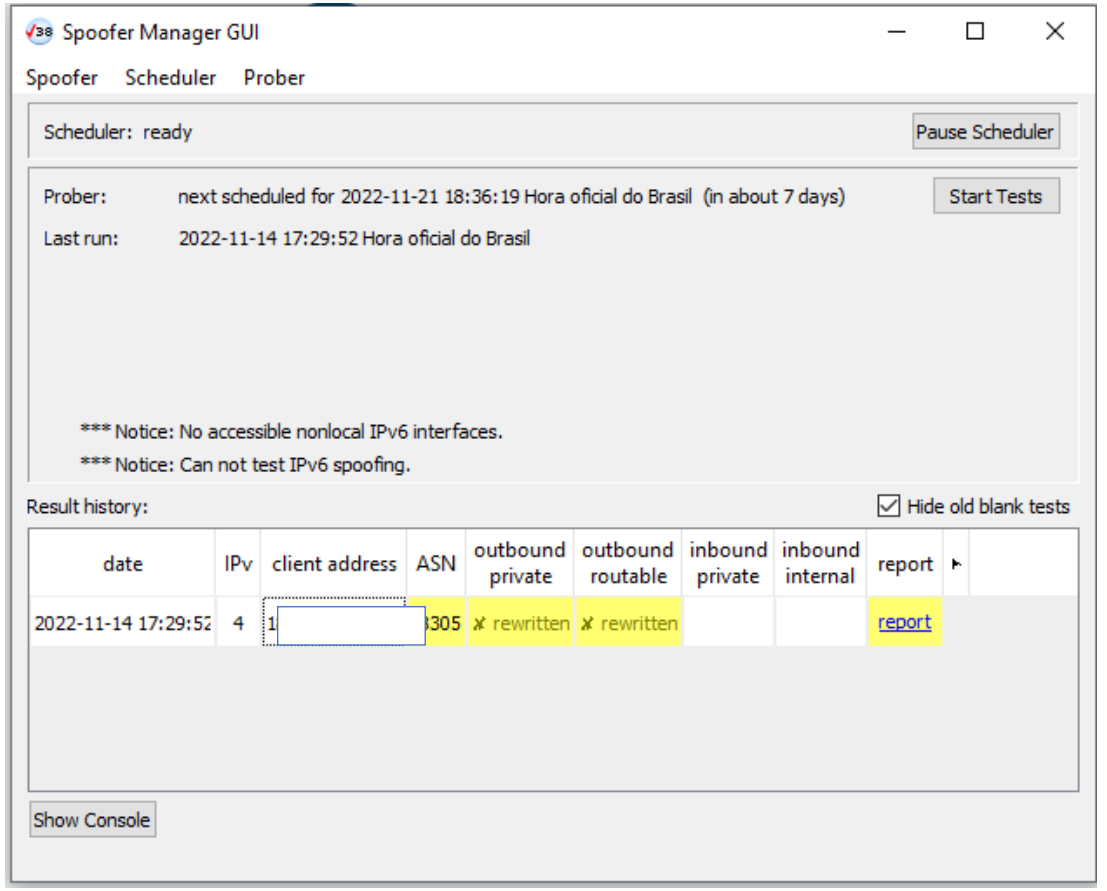
Krill (RPKI)

- O Krill é utilizado para gerenciar e manter as ROAs (Routing origin authorization) publicadas de forma correta, auxiliando no processo de validação de origem dos blocos IP.



Spoofer Caida

- O Spoofer é utilizado para validação da correta aplicação da política de anti-spoofing.



WalledGarden.Global

O Walled Garden coloca no seu roteador de BGP milhares de rotas de lixo IPv4 e IPv6, central de controle, vírus, route leaks, bots usados para DDOS, phishing dentre outros.

Um ferramenta eficaz para ajudar a prevenir e mitigar ataques DDoS.

WalledGarden.Global

Pedir proteção Ajuda

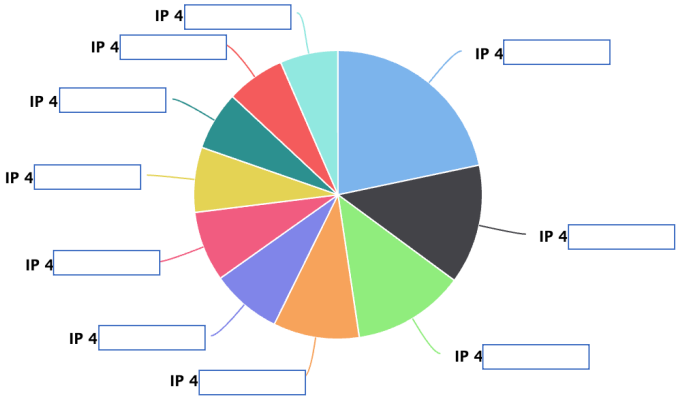
Selecione o seu AS

2

Data/Hora	Alerta	Proto	IP origem	Porta origem	IP destino	Porta destino
16/11/2022 10:39:42	bruteforce	TCP	4	60695	1	445
16/11/2022 10:39:42	scanner	TCP	4	4899	1	36830
16/11/2022 10:39:38	bruteforce	TCP		23	1	40206
16/11/2022 10:39:38	honeypot	TCP		23	1	55265
16/11/2022 10:39:31	honeypot	TCP	12	23634	4	23
16/11/2022 10:39:28	bruteforce	TCP	4	62406	4	23
16/11/2022 10:39:27	honeypot	TCP	14	50634	4	23
16/11/2022 10:39:25	scanner	TCP	4	8014	1	45636
16/11/2022 10:39:24	honeypot	ICMP	4	0	7	0
16/11/2022 10:39:23	scanner	TCP	4	23	5	43807
16/11/2022 10:39:21	bruteforce	TCP	1	56355	4	23
16/11/2022 10:39:21	controller-http_post	TCP	1	443	4	56636

Meus IPs que estão realizando ataques

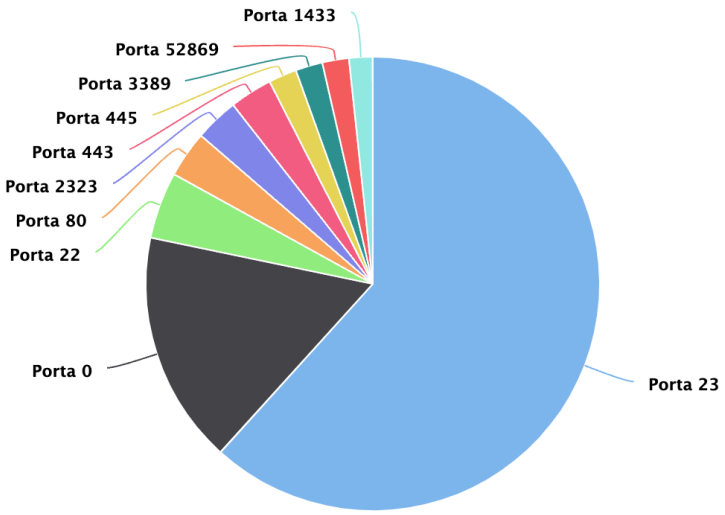
Apenas os 10 IPs que realizaram mais ataques



WalledGarden.Global

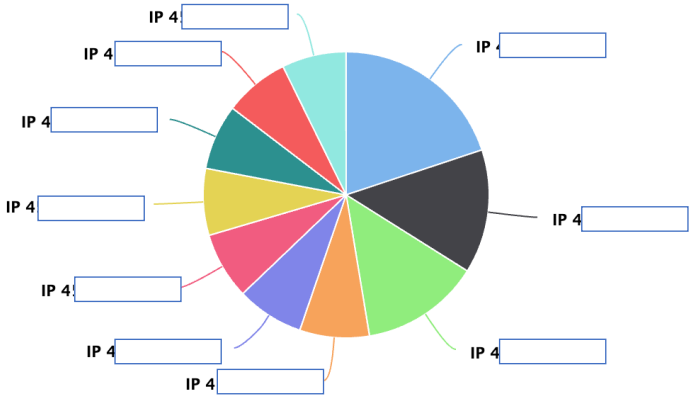
Minhas portas que estão realizando ataques

Minhas portas que estão realizando ataques



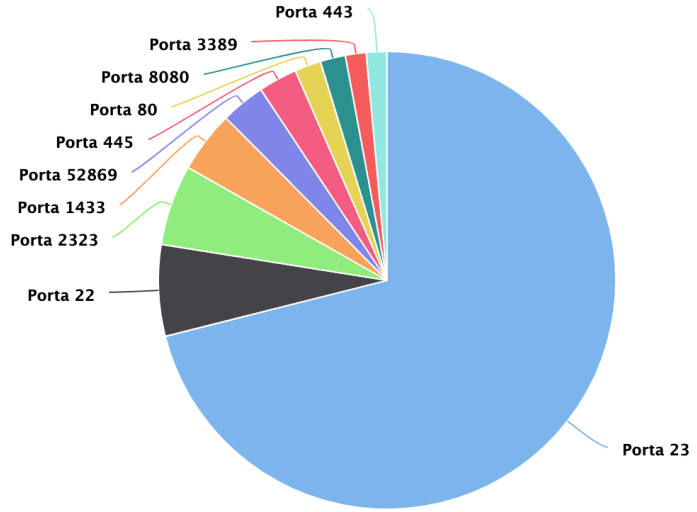
Meus IPs que estão sofrendo ataques

Apenas os 10 IPs que sofreram mais ataques



Minhas portas que estão sofrendo ataques

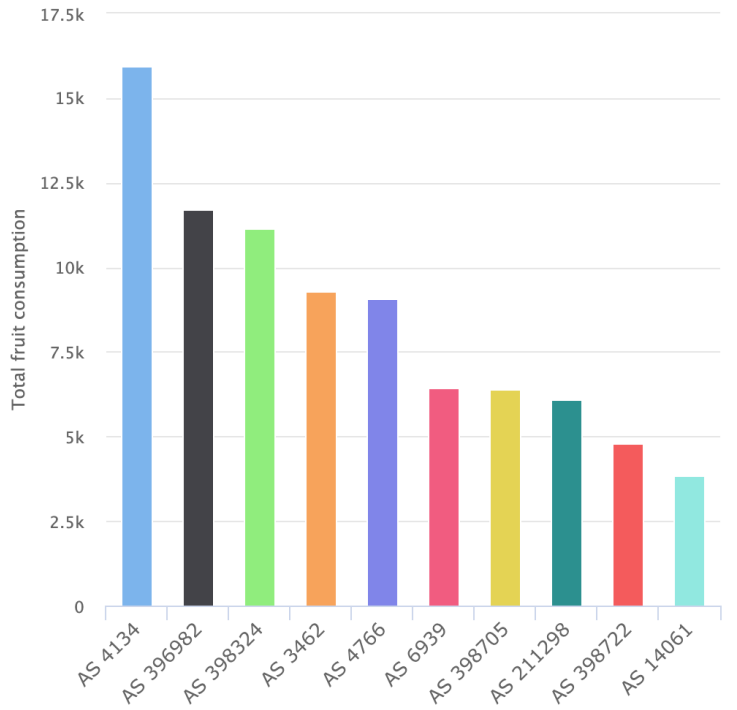
Apenas as 10 portas que sofreram mais ataques



WalledGarden.Global

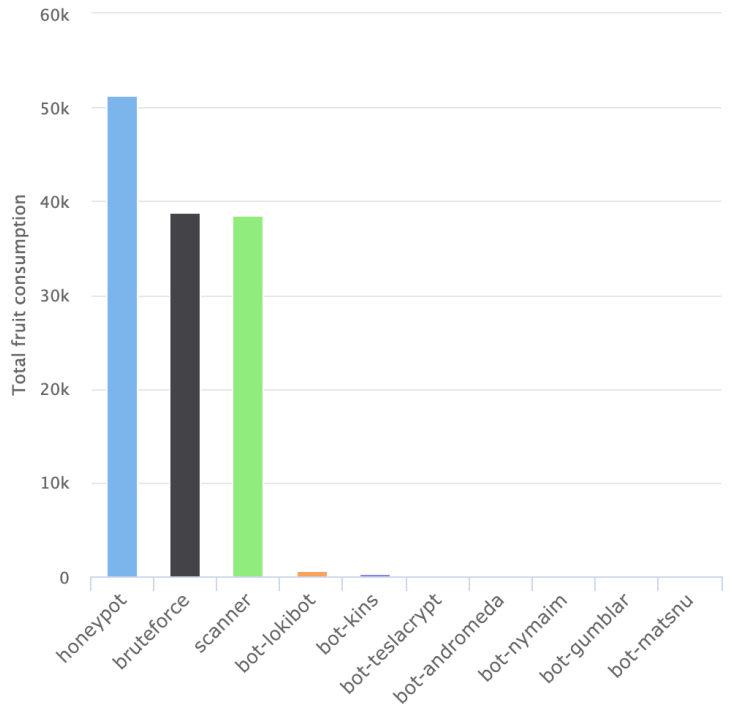
Top alerta de ASs atacantes

Top 10 dos ASs que estão me atacando



Assinatura dos alertas

Distribuição das assinaturas dos alertas



Pensar fora da Caixa...

Easter morning 1900: 5th Ave, New York City. Spot the automobile.

Source: US National Archives.

Pensar fora da Caixa...

Easter morning 1913: 5th Ave, New York City.
Spot the horse.

Source: George Grantham Bain Collection.

Conclusão....

- Teste sua rede com equipes sérias.
- Prevenção é sempre a melhor solução.

Dúvidas?????


Solintel
VLSM
MOGA
>TARS
OPA!
conectados
coworking
telcont
telefonarnet

Obrigado

Prof. Lacier Dias
lacier@solintel.com.br
(043) 99185-5550
https://www.linkedin.com/in/lacierdias
https://www.facebook.com/lacier.dias
https://www.instagram.com/lacierdias/