

Processo de análise de vulnerabilidades.

Alvo: *Empresa Thousandeyes*

Joelliton Jr. e Manuela Barbosa

1. O processo de análise de vulnerabilidades se deu a princípio da identificação de TI da empresa, isso diz sobre tudo que compõe a infraestrutura dela, como hardwares, softwares e peopleware.

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

thous.cn | thous.com | thous.info | thous.net | thous.org | thous.pl | thous.pw | thous.ro | thous.ua | thous.ru | thous.site | thous.tel | thous8.com | thousa.com | thousa.info | thousa.org | thousa.pl | thousadriver.com | thousad.co.uk | thousad.com | thousad.net |

Registrar Data We will display stored WHOIS data for up to 30 days. [Make Private Now](#)

Registrant Contact Information:

Name	Domain Administrator
Organization	Cisco Technology Inc.
Address	170 W. Tasman Dr.
City	San Jose
State / Province	CA
Postal Code	95134
Country	US
Phone	+1.4085273842
Fax	+1.4085264575
Email	infosec@cisco.com

Administrative Contact Information:

Name	Domain Administrator
Organization	Cisco Technology Inc.
Address	170 W. Tasman Dr.
City	San Jose
State / Province	CA
Postal Code	95134
Country	US
Phone	+1.4085273842
Fax	+1.4085264575
Email	infosec@cisco.com

Technical Contact Information:

Name	Domain Administrator
Organization	Cisco Technology Inc.
Address	170 W. Tasman Dr.
City	San Jose
State / Province	CA
Postal Code	95134
Country	US
Phone	+1.4085273842
Fax	+1.4085264575
Email	infosec@cisco.com

Information Updated: 2022-11-28 22:56:44

Suggested Domains for thousandeyes.com

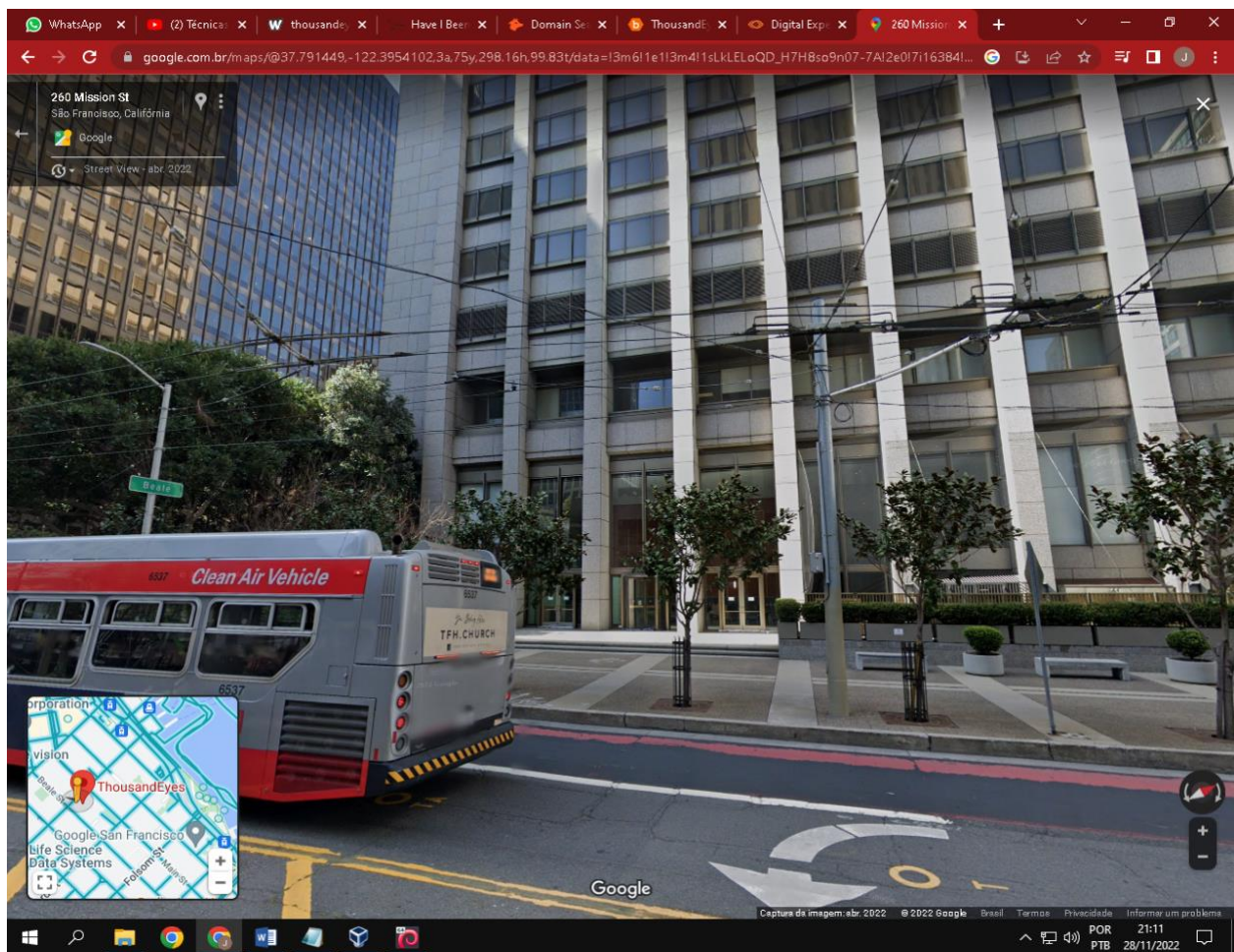
<input type="checkbox"/> thousand-eyes.live	\$2.99
<input type="checkbox"/> thousandeye.live	\$2.99
<input type="checkbox"/> masseyes.live	\$2.99
<input type="checkbox"/> thousandview.live	\$2.99
<input type="checkbox"/> mucheyes.live	\$2.99

[Purchase Selected Domains](#)

Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at **Name.com**

Todos os componentes foram mapeados e registrados para passarem pelas próximas etapas. Por meio dessa etapa crucial foi possível ter uma ideia sobre atividades críticas para serem tratadas posteriormente.



2. Como medida de segundo passo, foi feito um scan de vulnerabilidades. O escaneamento é uma das principais etapas da análise. Para esse processo foi essencial utilizar uma ferramenta scan (**Nmap**), identificando as vulnerabilidades do ambiente.

A screenshot of a Kali Linux desktop environment. On the left, a web browser window shows the WHOIS page for the domain "thousandeyes.com". The page displays registrant contact information for Cisco Technology Inc. On the right, a terminal window shows the execution of an Nmap scan. The terminal output includes the Nmap version, scan time, and results for the target IP 2.17.166.20. The scan identifies an open HTTP port (443/tcp) and a service identified as AkamaiGHost. The terminal also shows a traceroute and OS/service detection results. The system tray at the bottom indicates the date is 28/11/2022.

Assim, foi realizado uma varredura de IP's externos e ativos na rede interna, categorizando as vulnerabilidades pelos seus riscos, identificando e classificando as possíveis brechas de segurança.

As verificações externas identificam as maiores ameaças imediatas, atualizações necessárias de software e firmware, portas, protocolos, entre outros. Enquanto a varredura interna, aprimora as redes do próprio ambiente.

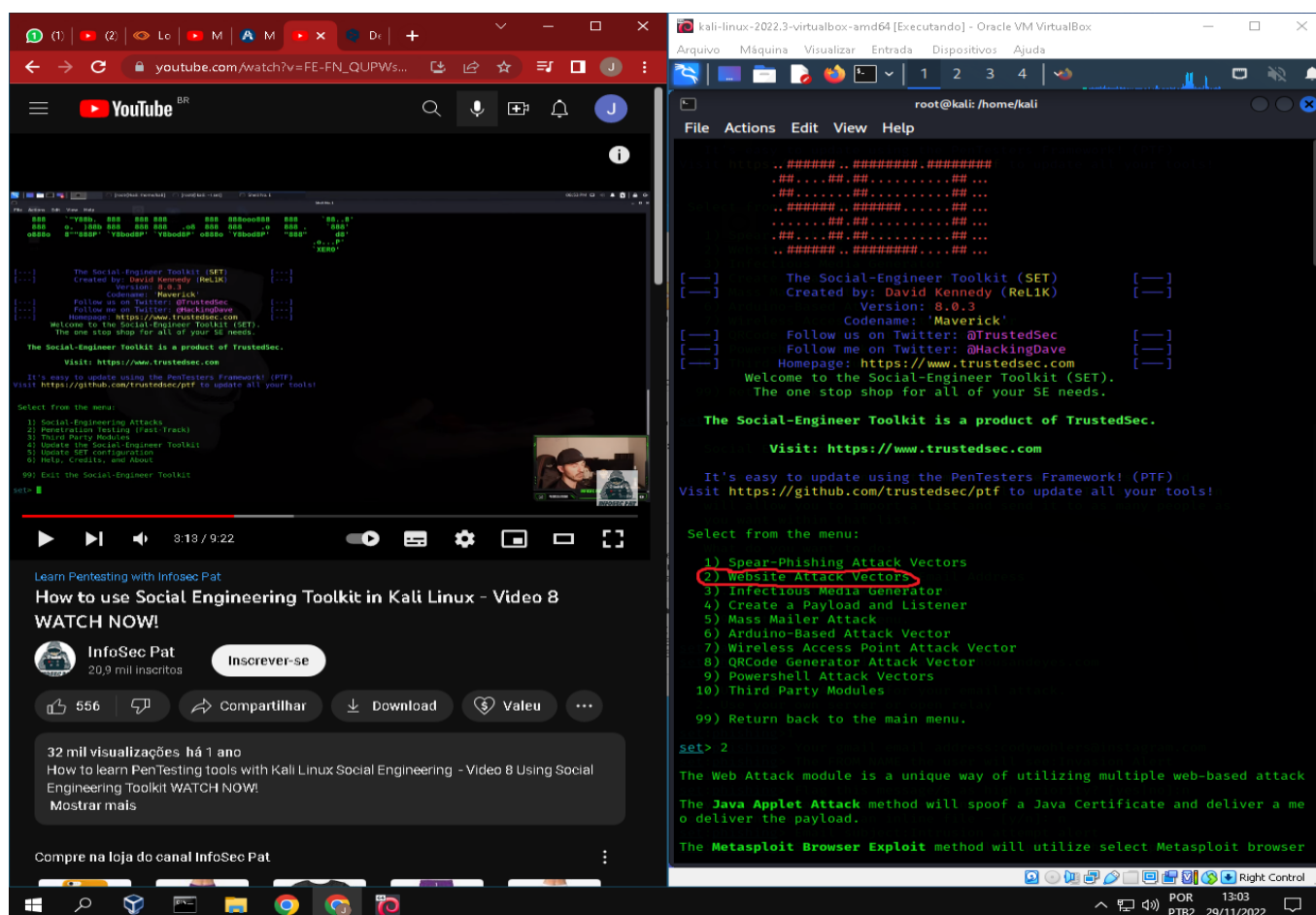
3. Avaliação de vulnerabilidades.

Nessa etapa, as ameaças foram listadas e classificadas a partir dos riscos que ofereceram para a infraestrutura.

Essa avaliação servirá como um guia para a correção e solução que será aplicada em cada brecha encontrada no sistema.

Aqui, foi criado um modelo das principais ameaças em seus ativos e como método foi usado o STRIDE, da Microsoft.

O STRIDE diz sobre os 6 tipos de ameaças, que são Spoofing of identity (roubo de identidade ou falsificação); Tampering with data (violação ou adulteração de dados); Repudiation of transaction (repúdio de transação); Information disclosure (divulgação não autorizada de informação); Denial of service (ataques de negação de serviço); e Elevation of privilege (elevação de privilégio).



4. Avaliação de riscos.

Durante a avaliação foram localizados e classificados os ativos da organização.

Esse processo envolveu relacionar os servidores, estações de trabalho, dispositivos e qualquer mídia que poderia ser alvo de ataque.

The screenshot displays the Hunter.io Domain Search results for the domain thousandeyes.com. The main table lists the following employees:

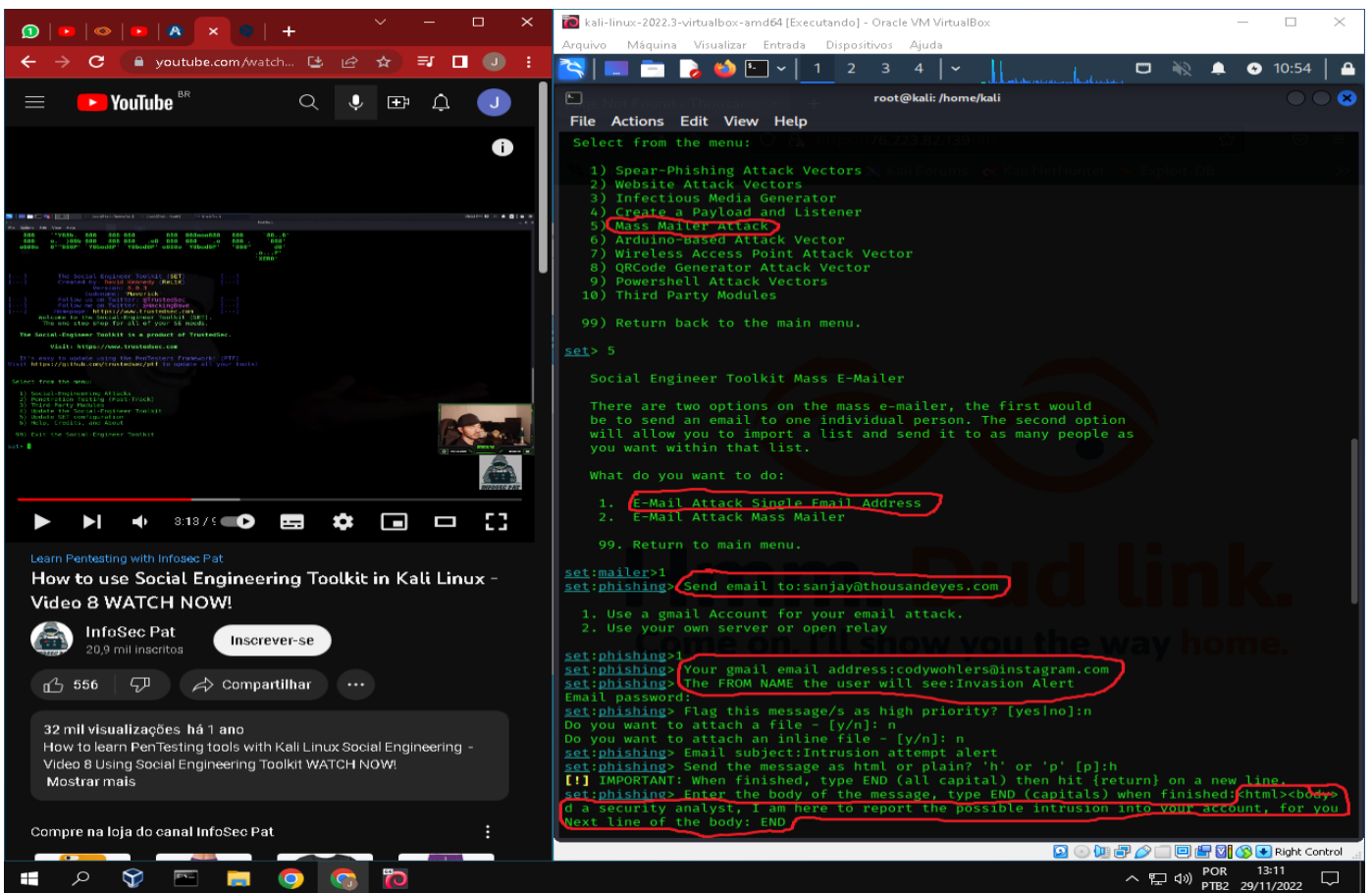
Name	Email	Phone	Job Title	Save as lead	Sources
Anna Vaverka	avaverka@thousandeyes.com	+1 508 416 1182	Service Delivery	Save as lead	7 sources
Mohit Lad	mohit@thousandeyes.com		Cofounder	Save as lead	1 source
Dave Fraleigh	dave@thousandeyes.com		Vp Customer Success	Save as lead	7 sources
Sanjay Mehta	sanjay@thousandeyes.com		CMO	Save as lead	2 sources
Ben Stricker	bstricker@thousandeyes.com		Service Delivery	Save as lead	20+ sources

The sidebar on the right shows company details for Thousand Eyes:

- Email pattern: {first}@thousandeyes.com
- Accept all: YES
- Industry: Technology
- Country: United States, US
- Technologies: [Dropdown menu]

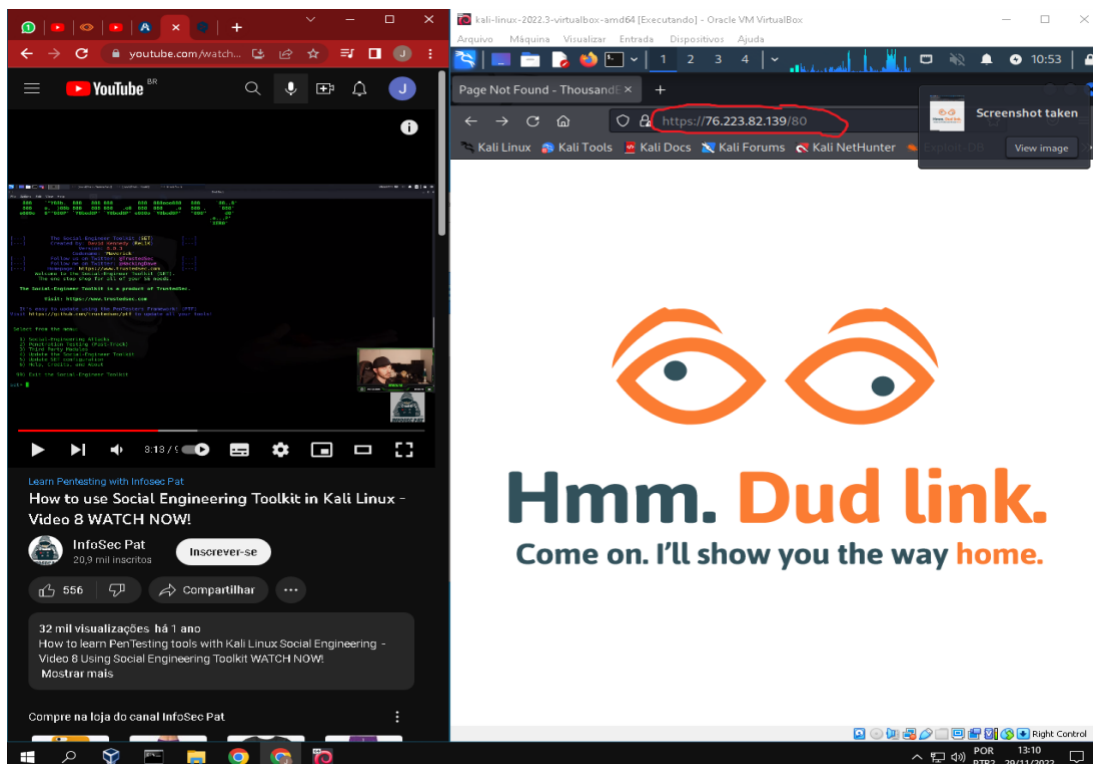
Após a avaliação, foi classificado cada um quanto ao tipo de informação que carregam utilizando uma escala de 1 a 5, que diz sobre:

1. Diz respeito às informações públicas sobre a organização;
 2. Os dados internos, mas que não são confidenciais;
 3. Informações sensíveis, como plano de negócios;
 4. Dados que não podem ser vistos nem mesmo por todos os funcionários;
 5. Todas as informações confidenciais;
5. Teste de invasão.
- Foi utilizado como ferramenta complementar do escaneamento de vulnerabilidade a ferramenta de teste de invasão SET (social engineering toolkit), simulando ações de infiltrações criminosas a estrutura de TI.



6. Considerações finais.

Após realizar toda estrutura analítica de vulnerabilidades, foram descartados de forma ética, todas as informações da empresa para não serem usadas posteriormente para outros fins.



Realizar análise de vulnerabilidades pode levar uma série de vantagens para a empresa e trata-se de uma ferramenta preventiva e corretiva, afinal, além de identificar brechas, acusa alterações dos sistemas e dá insumos para o tratamento dos riscos.