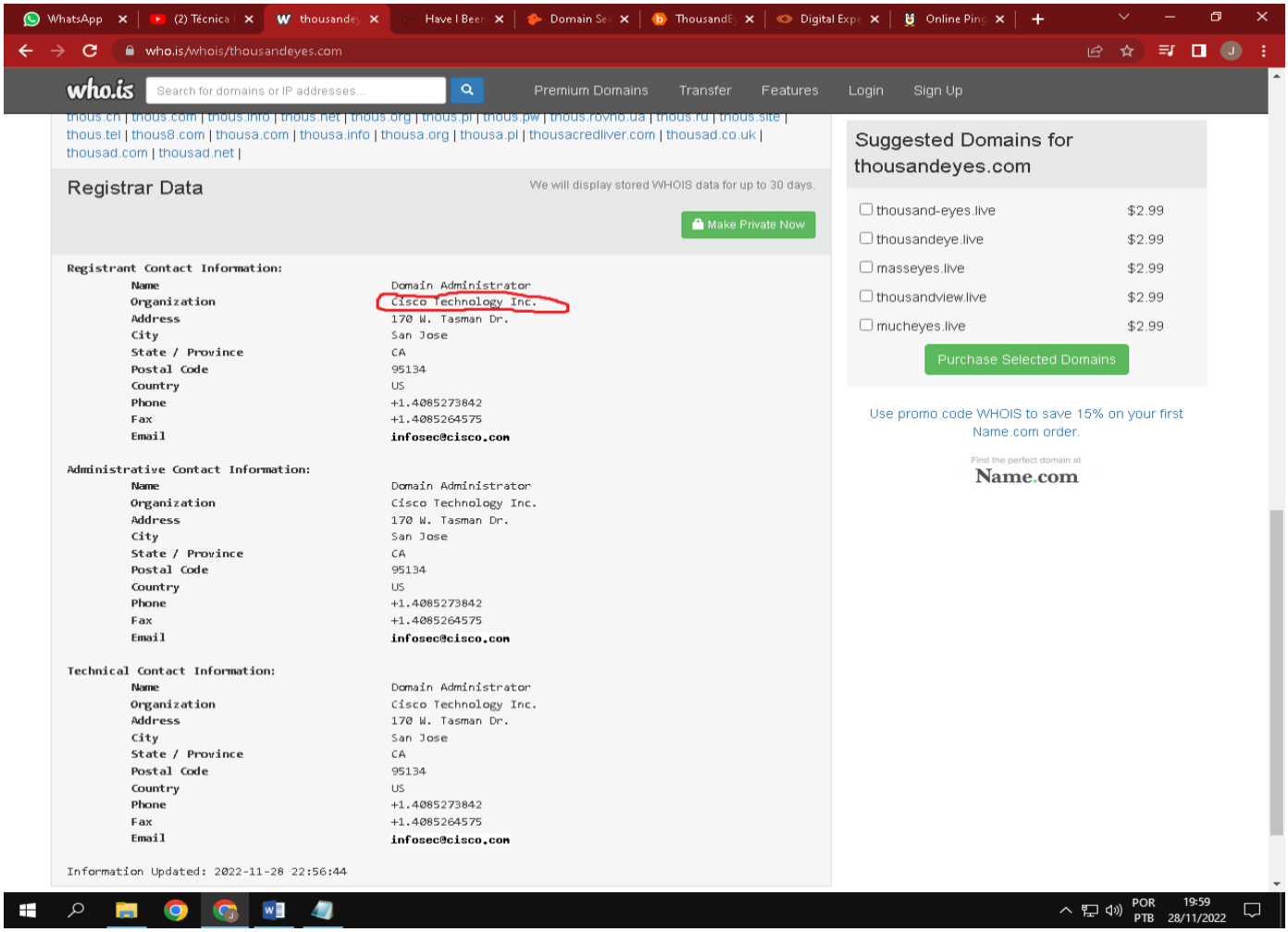
Faculdade Adventista
BAHIA

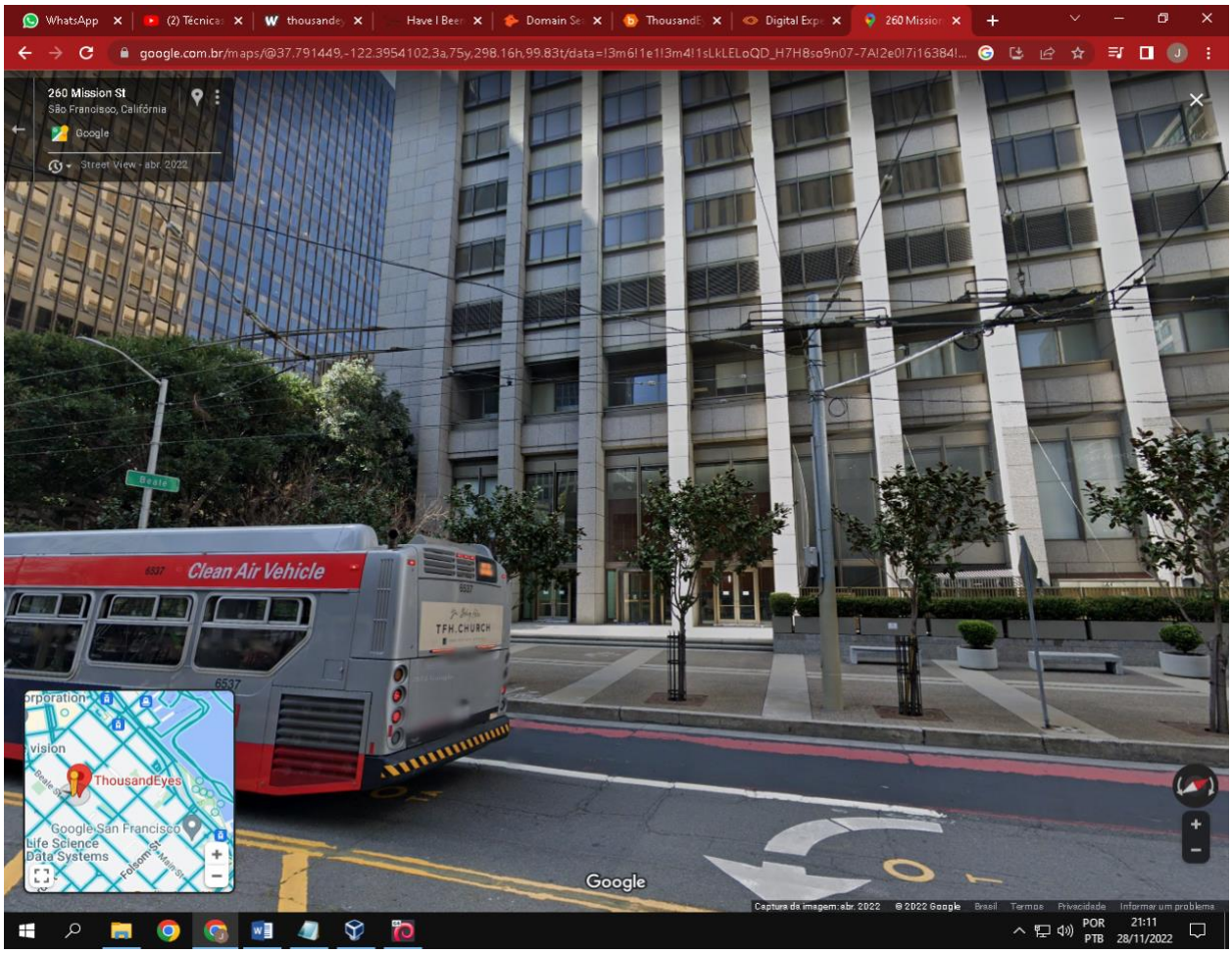
Processo de análise de vulnerabilidades.
Alvo: *Empresa Thousandeyes*

Joelliton Jr. e Manuela Barbosa

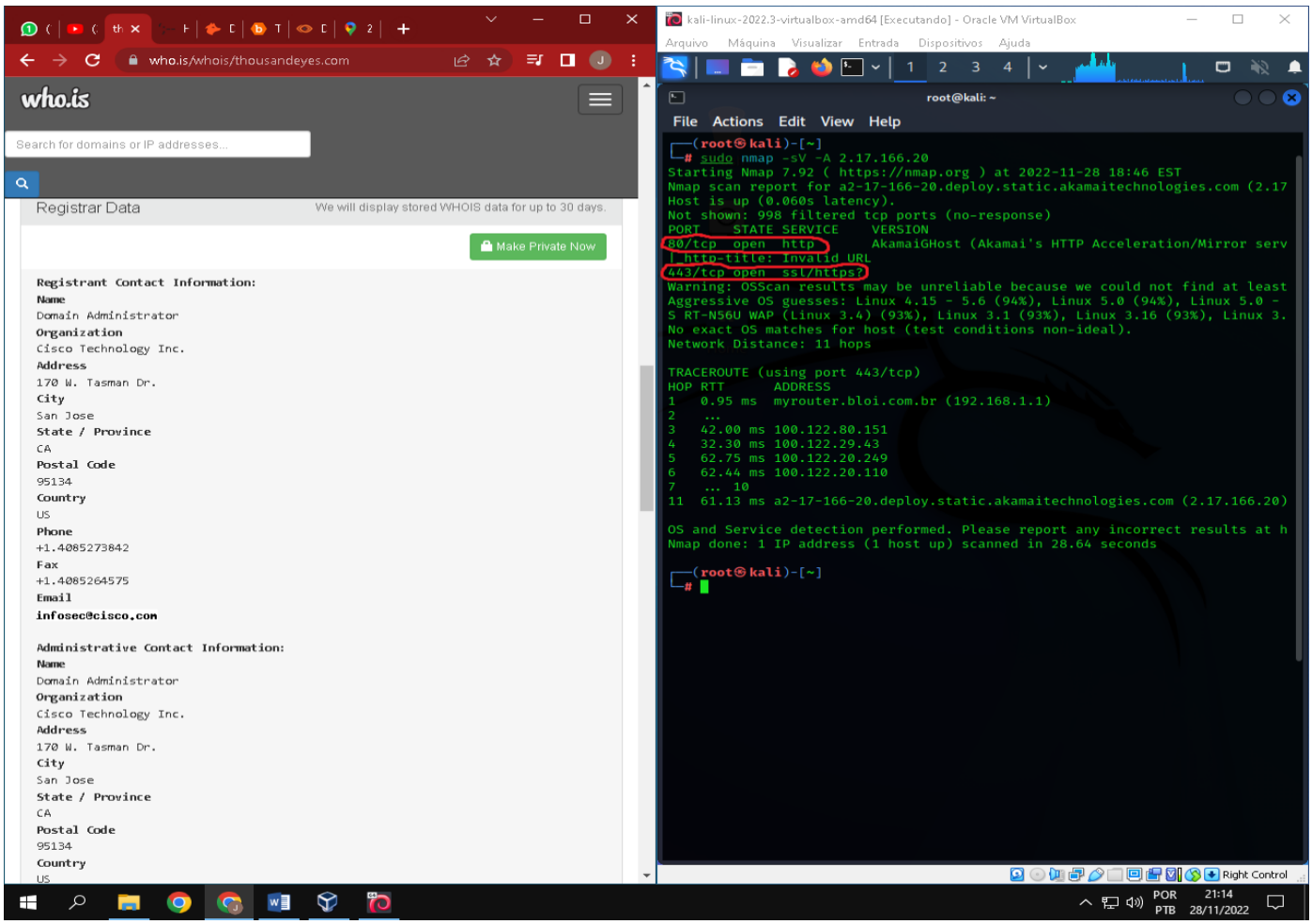
1. O processo de análise de vulnerabilidades se deu a princípio da identificação de TI da empresa, isso diz sobre tudo que compõe a infraestrutura dela, como hardwares, softwares e peopleware.



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.



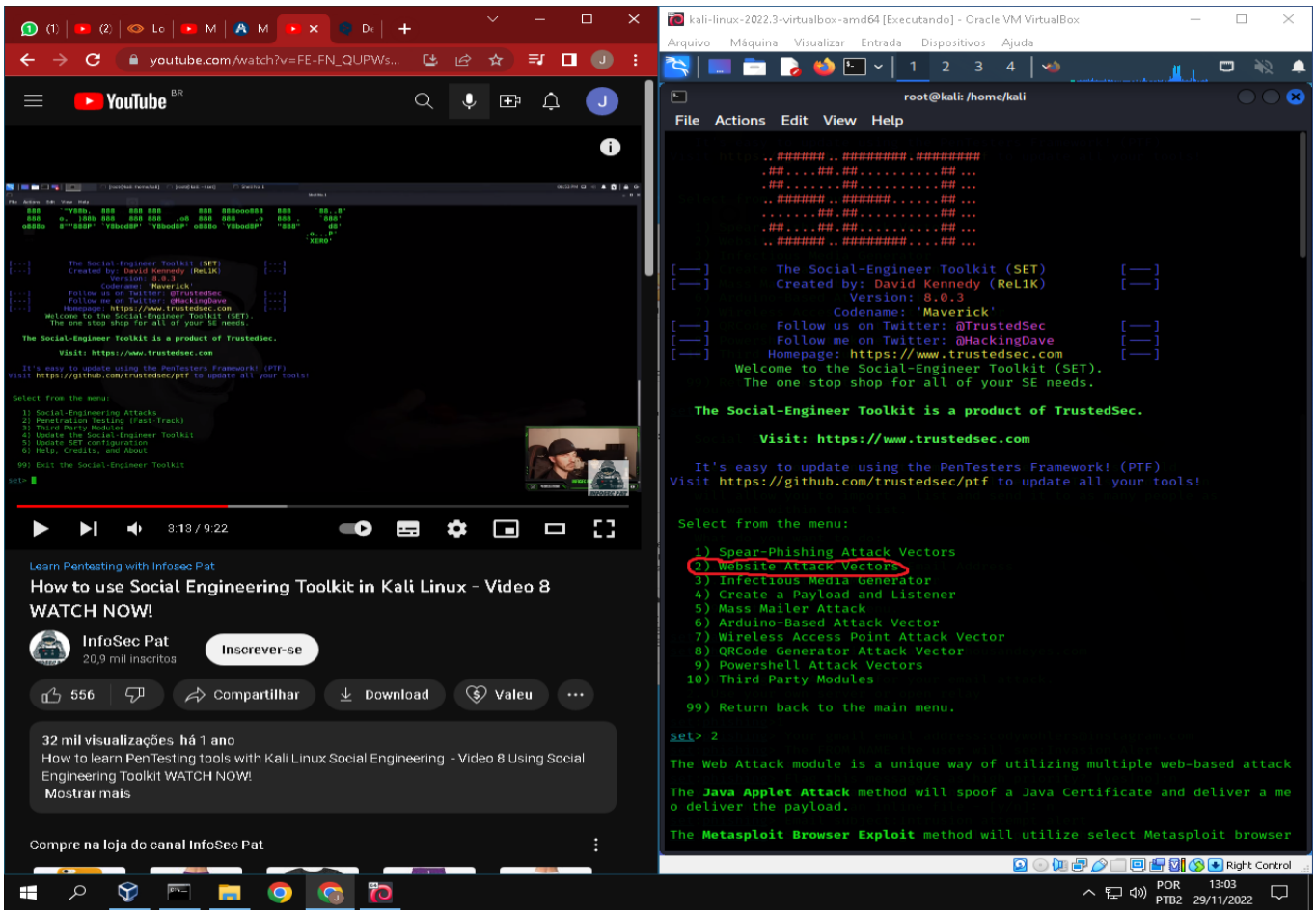
Assim, foi realizado uma varredura de IP's externos e ativos na rede interna, categorizando as vulnerabilidades pelos seus riscos, identificando e classificando as possíveis brechas de segurança.

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.

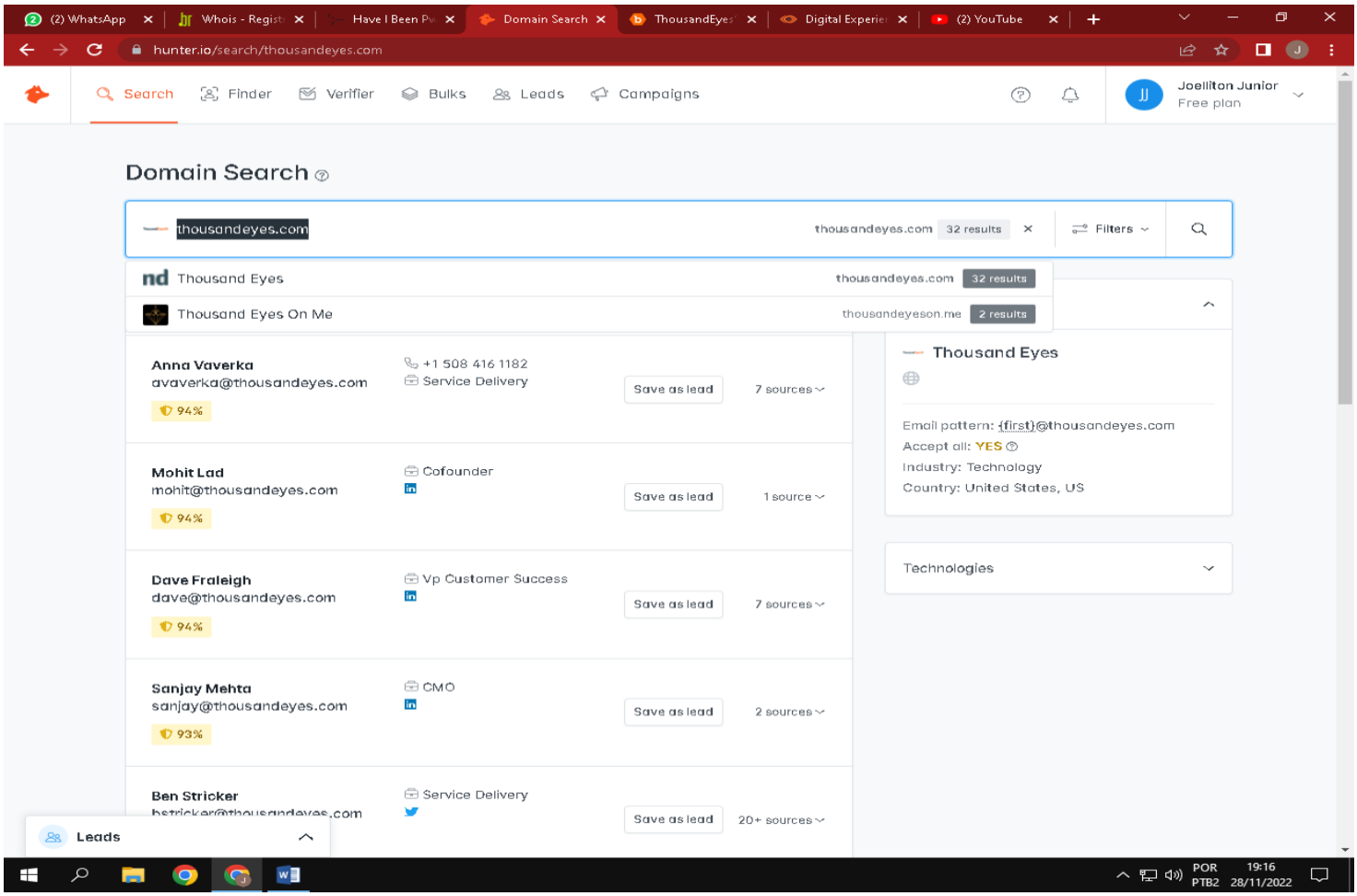
3. Avaliação de vulnerabilidades.
   Nessa etapa, as ameaças foram listadas e classificadas a partir dos riscos que ofereceram para a infraestrutura.
   Essa avaliação servirá como um guia para a correção e solução que será aplicada em cada brecha encontrada no sistema.

   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.

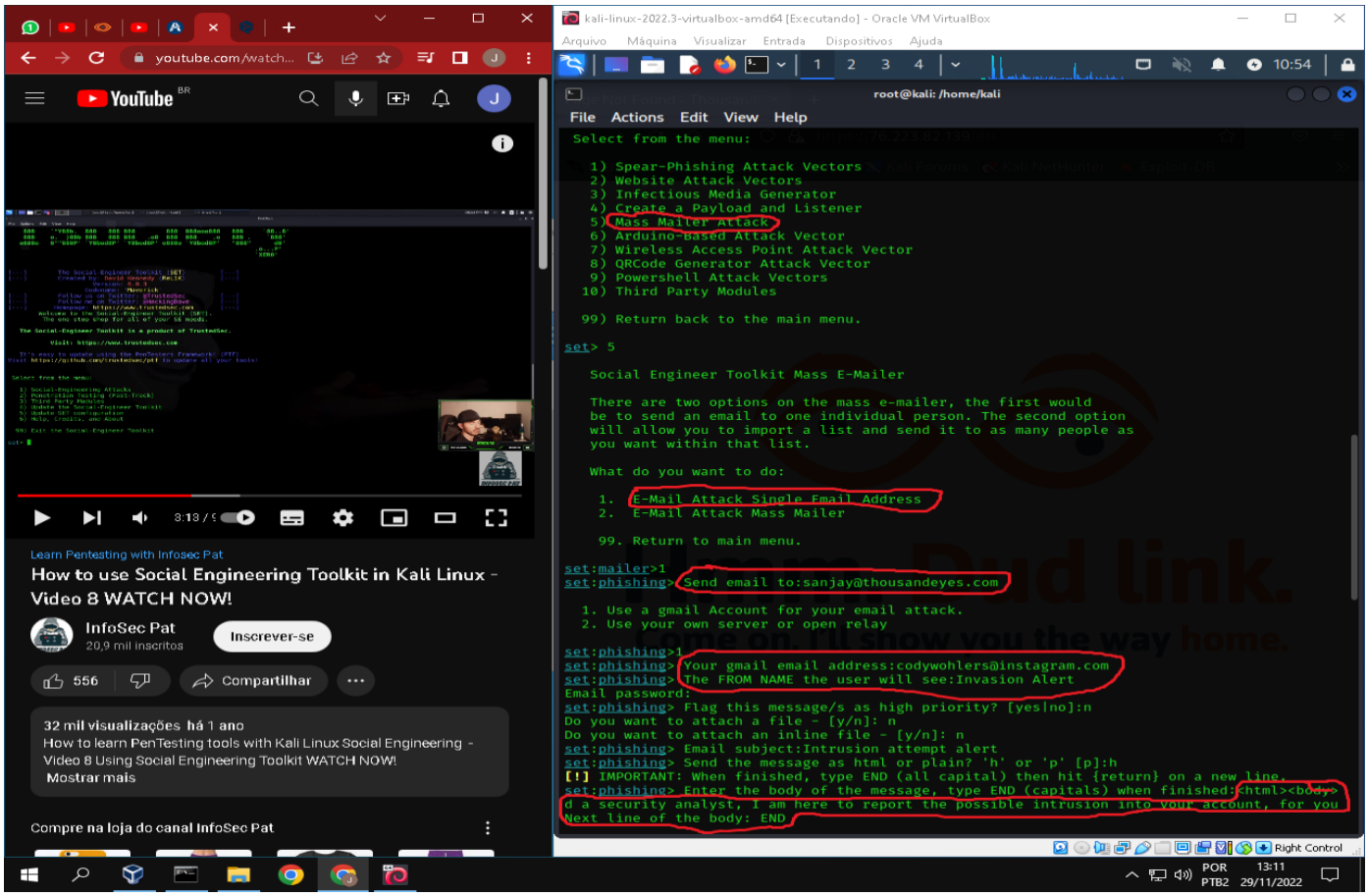


Após a avaliação, foi classificado cada um quanto ao tipo de informação que carregam utilizando uma escala de 1 a 5, que diz sobre:

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;

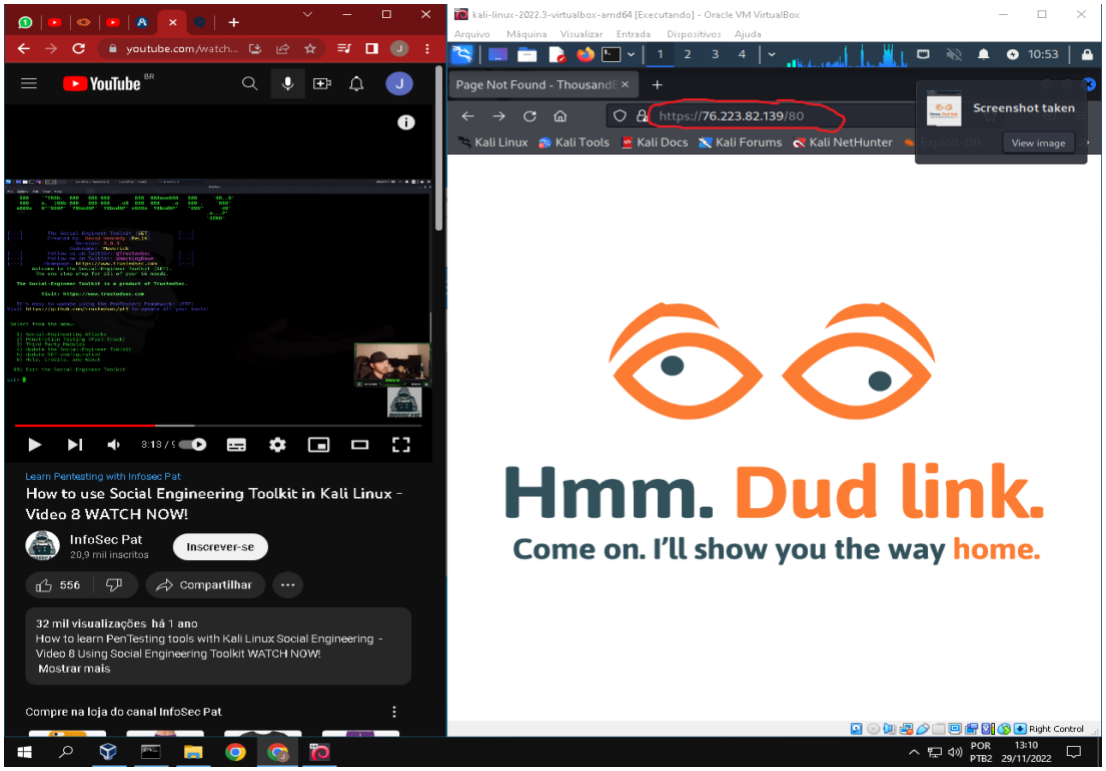
5. Teste de invasão.

Foi utilizado como ferramenta complementar do escaneamento de vulnerabilidade a ferramenta de teste de invasão SET (social enginering 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.