TEXUGO SCAN: Coletor de Informações Livre para Testes de Intrusão

Anderson Cirilo Valentim[1], **José Gildo de Araújo Júnior**[1]

[1]Universidade Federal Rural do Semi-Árido (UFERSA/Angicos)

anderson2610@live.com, jose.araujo@ufersa.edu.br

Abstract. *This work aims to develop a free tool that unifies in a single project the steps of information gathering and reporting in the ISSAF framework, widely used by information security professionals in the conduct of penetration tests. Although some tools available in the market assist in the collecting information for intrusive tests, many of its functionalities are paid and its source codes are not available for consultation or modification, thus hindering the work of the professionals with scarce financial resources who must to build their own solutions. In this sense, the tool called Texugo Scan, proposed by this work, presents as an alternative that contemplates the paid functionalities and gives the interested community all the necessary services to perform the initial steps of the intrusive tests freely.*

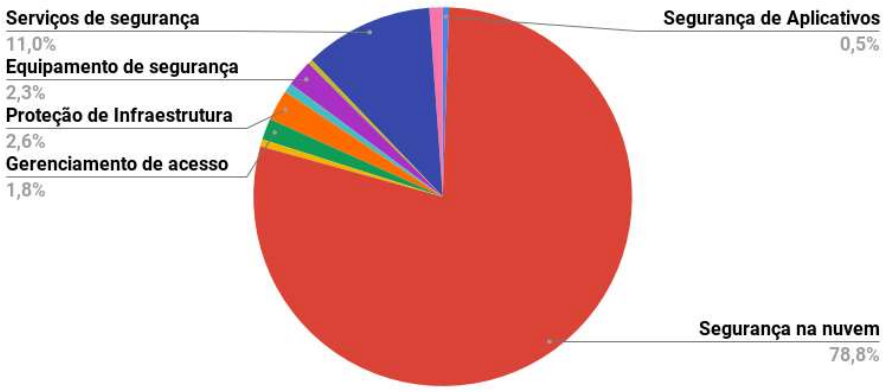
Resumo. *Este trabalho tem por objetivo a proposta de desenvolvimento de uma ferramenta livre que unifica em um único projeto as etapas de coleta de informações e geração de relatórios presentes no framework ISSAF, amplamente utilizado por profissionais de segurança da informação na condução de testes de intrusão. Apesar de algumas ferramentas disponıveis no mercado auxiliarem na etapa de coleta de informação para testes intrusivos, muitas das suas funcionalidades são pagas e seus códigos fonte não estão disponíveis para consulta e modificação, dificultando, assim, o trabalho dos profissionais com escassos recursos financeiros que, então, recorrem às suas próprias soluções. Neste sentido, a ferramenta denominada Texugo Scan, proposta neste trabalho, apresenta-se como uma alternativa que contempla as funcionalidades pagas e oportuniza à comunidade interessada muito dos serviços necessários para a realização das etapas iniciais dos testes intrusivos de forma livre.*

1. Introdução

Segundo dados da [WeAreSocial], cerca de 4 bilhões de pessoas estão conectadas à Internet. Os sistemas de informação atuais com os quais essas pessoas interagem diariamente coletam e armazenam grandes volumes de informações pessoais em suas bases dados. Posteriormente, esses dados são processados com a finalidade de conhecer melhor o público alvo aplicando técnicas de engenharia social visando prestar melhores serviços, aumentar seu poder de influência e consequentemente a lucratividade dessas empresas. O potencial da utilização de dados pessoais é imenso: recomendações mais precisas de produtos e serviços (Google), músicas (Spotify), vídeos (Youtube, Netflix), compras (Amazon, Ebay), ofertas de emprego (LinkedIn) e diversas outras aplicações. Em Uma pesquisa realizada pela [Ernst&Young 2019], com 1.200 executivos da área de

cibersegurança, constatou que apenas 4% das empresas se sentem preparadas para enfrentar ataques cibernéticos. Ainda de acordo com essa pesquisa, 70% dos entrevistados afirmaram que as companhias aumentariam seus investimentos na área caso algum incidente ocorresse e causasse danos significativos aos negócios. Segundo previsão da [Gartner 2019] os investimentos em segurança da informação no ano de 2019 chegarão a US$ 124 bilhões sendo considerando um mercado em franca expansão, a Figura 1 mostra a previsão de gastos mundiais por segmentos na área de segurança no ano de 2019.

Figura 1. Previsão de Gastos Mundiais com Segurança por Segmento no Ano de 2019.



Fonte: Adaptado de [Gartner 2019]

Garantir a segurança dessas informações é um desafio constante, uma vez que qualquer violação pode comprometer a imagem, a integridade, a confiabilidade e, por fim, o valor de mercado da empresa. Um ataque virtual trouxe prejuízos milionários ao *Facebook*, afetando aproximadamente 50 milhões de usuários, a repercussão foi negativa no mercado financeiro, e as ações do *Facebook* caíram 2,5% em valor de mercado [Estadao 2019].

Um software seguro, é aquele que satisfaz os requisitos implícitos e explícitos de segurança em condições normais de operação e em situações decorrentes de atividade maliciosa do usuário [McGraw 2006, Kissel et al. 2008]. Segundo [Dantas 2011], um sistema de informação seguro necessita garantir três características fundamentais:

- **Integridade:** é a garantia da exatidão e completeza da informação e dos métodos de processamento;
- **Disponibilidade:** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Confidencialidade:** é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

Essas características devem ser preservadas, pois são tidas como princípios da segurança da informação. No intuito de garantir que as três características não sejam violadas, muitas empresas contratam profissionais na área de segurança da informação, conhecidos como *pentesters*, para testar a integridade, a disponibilidade e a confidencialidade de seus sistemas com a intenção de mitigar possíveis falhas que podem resultar

em vulnerabilidades, e, por fim, comprometer tanto as informações do usuário quanto a infraestrutura em que seus sistemas estão inseridos. A execução ideal de um planejamento de testes por parte do *pentester* envolve a utilização de um conjunto variado de técnicas e softwares, parte deles disponíveis apenas em versões pagas, o que inviabiliza o trabalho de *pentesters* iniciantes que não dispõem de recursos suficientes para obtê-los, comprometendo seu trabalho em tempo e qualidade dos resultados.

Este trabalho se propõe a desenvolver e disponibilizar de forma livre uma ferramenta de coleta de informações e geração de relatório, de modo a unificar as recomendações presentes no *framework* ISSAF *(Information Security Assessment Framework)*,de modo a permitir á *pentesters* com poucos recursos disponíveis a possibilidade de executarem à etapa inicial de coleta de informações, tão eficiente quanto as versões pagas disponíveis atualmente.

2. Discussão do Problema

Para a realização de um teste de intrusão, é necessário entender o escopo da organização, rede ou sistema a ser invadido. Para isso, existem metodologias, *frameworks*, e modelos de testes de segurança específicos a serem utilizados para cada cenário. [M. Prandini 2010] comparou-os conforme é apresentado na Tabela 1, onde foram estabelecidos critérios essenciais para comparação das metodologias estudadas.

Tabela 1. Comparação de metodologias para testes de intrusão.

	ISSAF	OSSTM	BHM	GNST
Modelagem	+	=	-	-
Planejamento	+	-	-	-
Flexibilidade	-	-	-	+
Adaptação	=	+	+	=
Relatório	=	=	=	+
Orientação	-	=	-	+
Granularidade	+	=	-	-

Descrição: + Bom, = Médio, - Limitado ou nenhum

Fonte: Adaptado de [M. Prandini 2010]

O primeiro critério foi a modelagem, onde somente o *framework* ISSAF ofereceu características para elaboração de um cenário de teste de intrusão específico. No critério planejamento, o ISSAF também apresentou vantagem devido a sua possibilidade de associar a tarefa a ser executada com a técnica a ser utilizada. No critério flexibilidade, o ISSAF apresentou desvantagem por não apresentar subjetividade em como deve ser realizada cada etapa do teste, isso leva o *pentester* a sempre seguir o mesmo roteiro de execução do teste de intrusão, o que pode inviabilizar a descoberta de problemas ao seguir diferentes caminhos. No critério de adaptação, o ISSAF, mostrou-se moderado. A utilização de técnicas bem definidas podem ser executadas em ferramentas diferentes das recomendadas, o que, em situações específicas pode ser mais eficiente do que o recomendado. Em relação aos relatório, o ISSAF apresentou falta de clareza em como deve ser documentado o teste de intrusão. A granularidade é uma das principais características

presente no *framework* ISSAF, devido ao seu detalhamento, o que permite ao *pentester* iniciante entender de forma específica cada atividade executada.

Devido as vantagens apresentadas, o ISSAF foi selecionado como o *framework* base para este trabalho [Rathore et al. 2004]. Este *framework* estabelece objetivos e técnicas a serem utilizados funcionando de forma sequencial. O ISSAF estabelece 3 etapas base para que o teste de intrusão seja executado com êxito, são elas:

- **Planejamento e Preparação:** Esta etapa tem por objetivo definir o ambiente de teste, os softwares a serem utilizados, contratos e aspectos legais, definição da equipe de trabalho, prazos, requisitos e estrutura dos relatórios finais;
- **Avaliação:** Nesta etapa são realizados os testes de intrusão baseados em 9 atividades: coleta de informação, mapeamento de rede, identificação de vulnerabilidades, invasão, acesso e escalação de privilégios, enumeração, comprometimento de usuários remotos, manutenção de acesso, e ofuscamento de rastros;
- **Relatório, Limpeza e Destruição de Artefatos:** Por fim, após a execução das etapas anteriores, é confeccionado pelo profissional de segurança da informação, um relatório decorrente das falhas e vulnerabilidades encontradas e propostas de correção. Também é feita a destruição de artefatos, com finalidade de não deixar nenhum rastro que comprometa a integridade do cliente.

A atividade de coleta de informações proposta no *framework* ISSAF, é a etapa principal para garantir que um teste de intrusão seja bem sucedido, essa atividade consiste em reunir o maior número de informações possíveis do cliente, e, em grande medida, encontra na Internet o meio mais propício para cumprir o seu fim. Contudo, não é trivial analisar e processar os dados da Internet. Para isso existem ferramentas específicas que oferecem funcionalidades relevantes para um teste de intrusão de modo a garantir celeridade nesta etapa. Tanto o **Maltego**[1] quanto o **Netcraft**[2] são ferramenta capazes de coletar informações públicas na Internet e organizá-la de forma simples onde os dados coletados por ele podem ser catalogados e analisados no intuito de montar um vetor de intrusão. Contudo, essas ferramentas só são amplamente úteis em versões pagas. Por exemplo, o número máximo de resultados esperados na versão cliente do Maltego sai de 64.000 na versão paga para apenas 12 na versão gratuita[3], impossibilitando que profissionais com escassos recursos financeiros consigam utilizá-la e tenham que construir suas próprias soluções.

3. Metodologia

Para o desenvolvimento da ferramenta proposta neste trabalho, o passo inicial foi o levantamento dos requisitos de software que se deu por meio da análise das versões pagas das ferramentas Maltego e *Netcraft*. Ambas as ferramentas foram utilizadas para a etapa

[1] A versão do Maltego CE é gratuita, contudo, a quantidade de informações coletadas é limitada. Disponível em: https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php. Acesso em: 13 de maio, 2019.

[2] O Netcraft fornece serviços de segeurança na Internet, além da funcionalidade de coleta de informações de domínios que está disponível no site da empresa. Disponível em: https://www.netcraft.com/. Acesso em: 13 de maio, 2019.

[3] Existe quatro versões do Maltego disponíveis no mercado, são elas: Maltego XL, Maltego Classic, Maltego CE, Maltego Case File. Disponível em: https://www.paterva.com/web7/buy/maltego-clients.php. Acesso em: 13 de maio, 2019.

de coleta de informações de teste de intrusão em um cenário real seguindo um roteiro de coleta de informações estruturado em conformidade com o *framework* ISSAF. O objetivo dessa etapa foi o de verificar o quão complexo seria executar um teste de intrusão utilizando essas ferramentas e também quais as lacunas deixadas por ambas as ferramentas que poderiam ser resolvidas por meio do Texugo Scan. Futuramente será feita a modelagem UML do sistema, utilizando o software Astah[4] [Astah 2019] de modo a contemplar todas as funcionalidades em comum levantadas. Os artefatos dessa etapa serão os diagrama de caso de uso e classes. O desenvolvimento das funcionalidades levantadas será feito na linguagem de programação python utilizando o *framework* Web Django[5] [Django 2019]. Todo código produzido vem sendo disponibilizado de forma gratuita no Github sob a licença MIT[6].

4. Validação

A validação do Texugo Scan será feita por meio da análise das medidas de tempo de execução, acurácia, precisão e revocação dos resultados obtidos para todas as funcionalidades afins, gerados por cada uma das ferramentas sendo analisadas, seguindo um mesmo roteiro de teste.

5. Resultados Parciais

Para início dos trabalhos, foi elaborado um plano de execução para analisar os resultados obtidos pelas ferramenta Maltego, seguindo as etapas sugeridas na atividade de coleta de informações do *framework* ISSAF, são elas:

- **Investigação DNS**;
- **Identificação da organização**;
- **Identificação de WebServices**.

A ferramenta recebeu como entrada os seguintes domínios:

- **carnaubais.rn.gov.br**
- **assu.rn.gov.br**

Após a execução do Maltego, os seguintes dados foram coletados e organizados,para ambos os domínios como mostram as Figuras 2 e 3.

Figura 2. Dados coletados do Maltego ao analisar o domínio da prefeitura de Carnaubais.

Ferramenta	Alvo	Investigação DNS	Identificação da organização a que pertence.	Enumeração de Subdomínios.	Identificação de WebServices	Identificação de sistema operacional
Maltego	carnaubais.rn.gov.br	Servidores de Registro: ns1.rn.gov.br IP:177.87.96.3 ns2.rn.gov.br IP:177.87.96.4 ns3.rn.gov.br IP:177.87.97.7 Servidores de Hospedagem(NS RECORD): ns1.outboxsistemas.com IP:108.179.192.216 ns2.outboxsistemas.com IP:108.179.192.215	Governo do Estado do Rio Grando do Norte Secretaria de Estado de Tributação	mail.carnaubais.rn.gov.br IP:108.179.192.217 www.carnaubais.rn.gov.br IP:108.179.192.217 webmail.carnaubais.rn.gov.br IP:108.179.192.217 ftp.carnaubais.rn.gov.br IP:108.179.192.217	Nginx 1.14	Null

Fonte: Autoria Própria.

[4]Astah é uma ferramenta de modelagem *UML* desenvolvida na linguagem Java.

[5] Django é um framework para desenvolvimento rápido para web, escrito em Python, que utiliza o padrão *model-template-view*.

[6] Ela é uma licença permissiva utilizada tanto em software livre quanto em software proprietário desenvolvida pelo Instituto de Tecnologia de Massachusett.

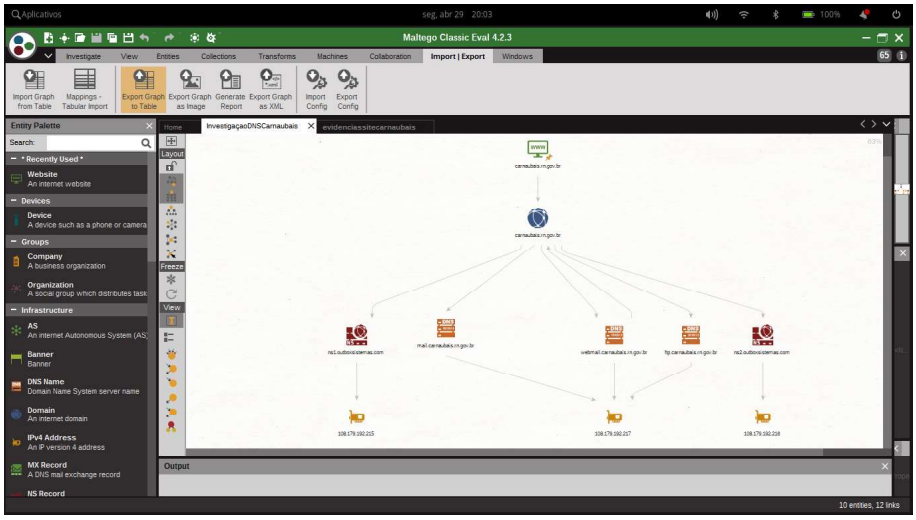
Figura 3. Dados coletados do Maltego ao analisar o domínio da prefeitura de Carnaubais.

Ferramenta	Alvo	Investigação DNS	Identificação da organização a que pertence.	Enumeração de Subdomínios.	Identificação de WebServices	Identificação de sistema operacional
Maltego	assu.rn.gov.br	Servidores de Registro: ns1.rn.gov.br IP:177.87.96.3 ns2.rn.gov.br IP:177.87.96.4 ns3.rn.gov.br IP:177.87.97.7 Servidores de Hospedagem(NS RECORD): ns1.microsysteminfo.com.br IP:187.45.177.142 ns2.microsysteminfo.com.br IP:187.45.177.143	Governo do Estado do Rio Grando do Norte Secretaria de Estado de Tributação	webmail.assu.rn.gov.br IP:187.45.179.194 ftp.assu.rn.gov.br IP:187.45.179.194 mail.assu.rn.gov.br IP:187.45.179.194	Apache	Null

Fonte: Autoria Própria.

A partir dos dados coletados, é possível perceber que a identificação do sistema operacional, não é uma funcionalidade ao qual é contemplada pelo Maltego, o que é extremamente útil para montar um vetor de intrusão. No desenvolvimento do Texugo Scan, uma das principais funcionalidades será a identificação do sistema operacional ao qual o alvo está utilizando. Uma vantagem do Maltego, é a hierarquização dos dados como mostra a figura 4, isso facilita a visualização das entidades geradas para usuário. Contudo, devido a gama de funcionalidades presentes na ferramenta, para cada dado que é solicitado, é necessário fazer uma execução, que no Maltego é chamado de *Transforms*,o que chega a ser incômodo ao usuário, que poderia executar todos os *Transforms* de uma única só vez.

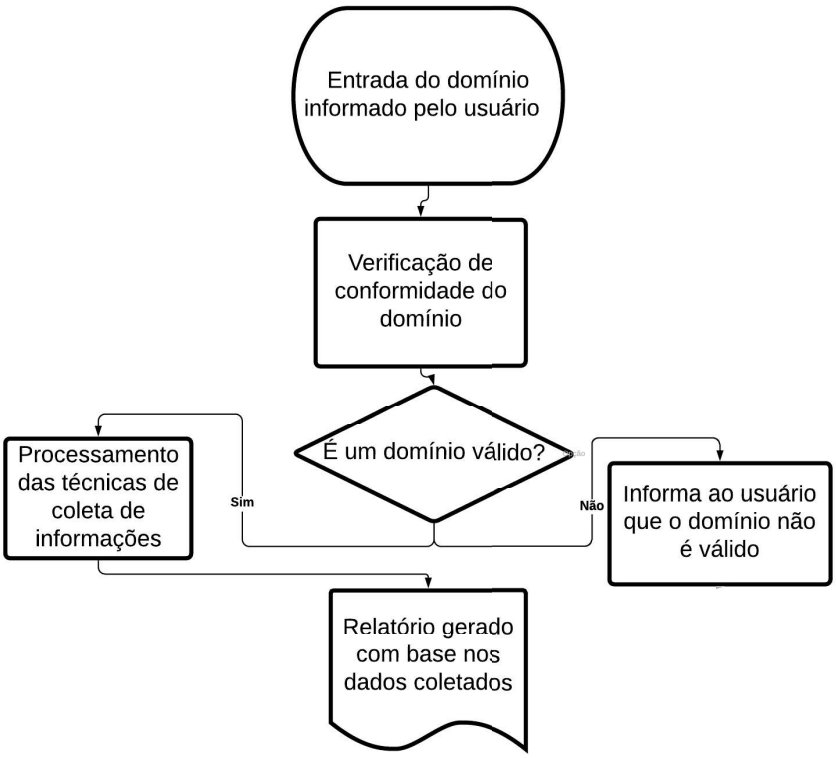
Figura 4. Interface Gráfica do Maltego.



Fonte: Autoria Própria.

O Texugo Scan, vem sendo projetado de modo a executar todos os processos com uma única entrada de dados, sem a necessidade de fazer várias execuções para obter um único objetivo, assim executando um fluxo de entrada, processamento e saída, como mostra a figura 5.

Figura 5. Fluxograma de execução do Texugo Scan



Fonte: Autoria Própria.

6. Conclusão

Este trabalho apresenta a proposta de uma ferramenta livre desenvolvida com o propósito de auxiliar a coleta de informações para realização de testes de intrusão uma vez que as principais soluções de softwares disponíveis no mercado atualmente são pagas ou insuficientes.Neste cenário, a ferramenta denominada *Texugo Scan* apresenta-se como alternativa à profissionais que não podem pagar pelas ferramentas disponíveis, e com frequência são forçados à desenvolverem suas próprias soluções. Alguns serviços sendo desenvolvidos inclusive superam versões pagas presentes no mercado. Após as análise descrita em detalhes na seção 5, espera-se, no futuro, consolidar uma ferramenta livre tão ampla e simples quanto as versões em código fechado disponíveis.

7. Reprodutibilidade

Todo o código desenvolvido pode ser encontrado em: https://github.com/andersonvalentim/TexugoScan.

Referências

Astah (2019). Projeto Astah. `http://astah.net/download`. Online; Acesso em: 13 de maio, 2019.

Dantas, M. L. (2011). Segurança da informação: uma abordagem focada em gestão de riscos. *Recife: Livro Rápido-Elógica*.

Django (2019). Projeto Django. https://www.djangoproject.com/. Online; Acesso em: 13 de maio, 2019.

Ernst&Young (2019). Retomada da segurança cibernética: Como se preparar para enfrentar os ataques cibernéticos. https://www.ey.com/Publication/vwLUAssets/EY-GISS-2017//%24File/GISS-2017-Port.pdf. Online; Acesso em: 12 maio, 2019.

Estadao (2019). Falha de segurança no Facebook atinge 50 milhões de usuários. https://link.estadao.com.br/noticias/empresas,hackers-vazam-dados-de-50-milhoes-de-usuarios-diz-facebook,70002523613. Online; Acesso em: 29 abr, 2019.

Gartner (2019). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending- Online; Acesso em: 12 maio, 2019.

Kissel, R. L., Stine, K. M., Scholl, M. A., Rossman, H., Fahlsing, J., and Gulick, J. (2008). Security considerations in the system development life cycle. Technical report.

M. Prandini, M. R. (2010). Towards a practical and effective security testing methodology. *The IEEE symposium on Computers and Communications*.

McGraw, G. (2006). *Software security: building security in*, volume 1. Addison-Wesley Professional.

Rathore, B., Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R., Raman, S., and Chavan, U. (2004). Information systems security assessment framework (issaf). *Draft 0.1, Open Information Systems Security Group*.

WeAreSocial. DIGITAL IN 2018: WORLD'S INTERNET USERS PASS THE 4 BILLION MARK. https://wearesocial.com/blog/2018/01/global-digital-report-2018. Online; Acesso em: 29 abr, 2019.