Tramonto: Uma estratégia de recomendações para Testes de Penetração

Daniel Dalalana Bertoglio[1], **Avelino Francisco Zorzo**[1]

[1]Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Porto Alegre – RS – Brazil

daniel.bertoglio@acad.pucrs.br, avelino.zorzo@pucrs.br

Abstract. *In the past years, a wide variety of contributions for security testing in organizations, networks and systems have been presented. Furthermore, there is a variety of environments that may be the target for those tests, such as networks, systems, databases, web applications, Internet of Things (IoT) or Cloud Computing. Hence, to have a standard for security tests, using methodologies and frameworks, may increase the efficiency and help the tester. Therefore, this work presents Tramonto, a recommendations strategy for Penetration Testing that is based on the main existing security testing methodologies.*

Resumo. *As pesquisas envolvendo técnicas para testes de segurança em organizações, redes e sistemas, têm apresentado grande variedade nas suas contribuições. A diversidade de cenários-alvo nos quais esses testes são executados pode envolver, por exemplo, Redes, Sistemas, Bancos de Dados, Aplicações Web, Internet das Coisas (IoT) ou Computação em Nuvem. A partir disso, a padronização destes testes, através de metodologias e frameworks, pode aumentar a eficácia e ajudar o tester na execução das atividades. Este trabalho apresenta a Tramonto, uma estratégia de recomendações para Testes de Penetração criada a partir das principais metodologias de teste de segurança existentes.*

1. Introdução

Os riscos relacionados com a segurança de informações em empresas, organizações e entidades que trabalham com dados sensíveis, sejam eles públicos ou não, têm obtido certa expressividade nas preocupações de tais instituições [8]. Riscos que não são controlados potencializam ataques a segurança, que por sua vez implicam em perdas consideráveis. O uso de técnicas para testes de segurança, então, é uma alternativa relevante combater e reduzir esses riscos [15].

Dentre esses testes de segurança, uma das técnicas conhecidas é o Teste de Penetração (Pentest). Pentest é a tentativa controlada de penetrar um sistema ou rede a fim de detectar vulnerabilidades, empregando as mesmas técnicas que são utilizadas em um ataque propriamente dito. Essa alternativa permite que sejam tomadas medidas adequadas para eliminar as vulnerabilidades antes que possam ser exploradas por terceiros não autorizados [14].

O processo de um Pentest se divide, normalmente, em atividades como: coleta de informações sobre o sistema alvo; escaneamento do sistema alvo e descoberta dos serviços; identificação de sistemas e aplicações; descoberta de vulnerabilidades e

exploração de vulnerabilidades [4]. Para uma empresa, este processo é aplicado visando objetivos variados, como o natural aumento da segurança dos sistemas, identificação de vulnerabilidades, teste da equipe de segurança da empresa alvo e até mesmo o aumento da segurança organizacional e de pessoas. Ainda nesse sentido, a aplicação do Pentest pode ser classificada em critérios como [14]: base de informações, que trata o nível de conhecimento sobre o alvo; agressividade, representando o nível de profundidade do teste; escopo do teste e, por fim, abordagem e técnica utilizadas.

Testes de penetração, enquanto técnica para avaliação de segurança, são capazes de fornecer um nível de verificação de segurança adequado e com muitos detalhes em respeito as fraquezas do alvo. Ainda assim, pode-se ressaltar que as atividades de um Pentest também possuem, em sua essência, preocupações legais da execução e aplicação do teste, principalmente em virtude das inúmeras formas de aplicação do mesmo e dos cenários-alvo.

Com as variações nas formas e processos de um Pentest, a padronização deste pode ser considerada uma tarefa complexa. As principais metodologias de teste de segurança contém aspectos que não contemplam amplamente essas variações, além do fato de que um teste de penetração também apresenta diferenças em razão do *tester* que o executa. Assim, é toda a experiência e *know-how* do *tester* precisa ser levada em consideração para pontuar essas diferenças.

Dessa forma, a criação de uma estratégia de recomendações de teste é uma maneira relevante para auxiliar as atividades no processo de um teste de penetração. A partir das metodologias de teste de segurança que são consolidadas na comunidade científica, é possível criar fluxos, tarefas e indicações que permitam ao *tester* aplicar as verificações de segurança independente do cenário e da classificação do tipo de teste. Portanto, este trabalho apresenta a Tramonto, uma estratégia de recomendações direcionada a testes de penetração e suas principais concepções. A Seção 2 descreve as principais metodologias de teste de segurança existentes e que são base da Tramonto. Já a Seção 3 apresenta a conceituação e formalização das características da estratégia de recomendações criada. Além disso, é apresentado ainda um comparativo da Tramonto em relação às demais metodologias, envolvendo critérios relevantes no âmbito de modelos de teste. A Seção 4 detém a discussão e as principais contribuições da Tramonto. Por fim, a Seção 5 apresenta as considerações finais deste trabalho.

2. Metodologias de Teste

Através da realização de um mapeamento sistemático [1], foi possível identificar as seguintes metodologias, frameworks e modelos de teste de segurança: OSSTMM (*Open Source Security Testing Methodology Manual*) [6][9][12][2], ISSAF (*Information Systems Security Assessment Framework*) [12], PTES (*Penetration Testing Execution Standard*) [9], NIST (*National Institute of Standards and Technology) Guidelines* [12] e OWASP *Testing Guide* [6][9]. As próximas subseções descrevem, resumidamente, cada uma destas metodologias.

2.1. OSSTMM

OSSTMM (*Open Source Security Testing Methodology Manual*) [5] é a metodologia que detém um padrão internacional para testes de segurança, mantida pela ISECOM (*Institute for Security and Open Methodologies*). Suas definições são estabelecidas a partir

do escopo, que representa todo o ambiente de segurança operacional possível para qualquer interação com qualquer ativo. Este escopo é composto por três classes: COMSEC (*Communications Security Channel*), PHYSSEC (*Physical Security Channel*) e SPECSEC (*Spectrum Security Channel*). Essas classes, por sua vez, são divididas em cinco canais antes de serem usados pelo *tester*: Humano, Físico, Sem Fio, Telecomunicações e Redes de Dados.

Com base nas especificações apresentadas nos canais, a metodologia OSSTMM tornou-se uma das mais completas e robustas dentre os modelos de teste de segurança. Um importante diferencial que ela apresenta é a inclusão de fatores humanos como parte dos testes. Por outro lado, pode-se afirmar que a metodologia desconsidera itens como uma avaliação cíclica de vulnerabilidades encontradas e diagramas representando os fluxos do teste. Esses dois itens impactam, respectivamente, em uma diminuição de descobertas alternativas de vulnerabilidades e em um maior trabalho de interpretação dos módulos presentes na metodologia.

2.2. ISSAF

A metodologia ISSAF (*Information Systems Security Assessment Framework*) [3] é um *framework* capaz de modelar os requisitos de controle internos para a segurança da informação, e tem por objetivo avaliar a segurança de redes, sistemas e aplicações. Sua concepção é estruturada em três grandes áreas de execução: planejamento e preparação, avaliação e relatório, limpeza e destruição de artefatos. A fase de Planejamento e Preparação trata os passos necessários para definir o ambiente de teste, ferramentas de teste, contratos e aspectos legais, definição da equipe de trabalho, prazos, requisitos e estrutura dos relatórios finais. Já a fase de Avaliação representa o centro da metodologia, onde o teste de segurança é realmente executado. Esta fase possui nove (9) atividades principais, que seguem o fluxo básico de um ataque (reconhecimento, invasão e pós-invasão).

A metodologia ISSAF possui ampla documentação sobre a sua estrutura, e apresenta como uma das principais vantagens a criação de uma conexão entre as tarefas do teste e as ferramentas utilizadas. Da mesma forma, a ordem na qual a metodologia descreve o teste é otimizada para ajudar o *tester* em um trabalho com fluxo mais claro, evitando erros comumente associados com estratégias de ataques selecionadas aleatoriamente. Como limitações, pode-se ressaltar a falta de melhores orientações na elaboração de relatórios e também o fato de que a ISSAF desconsidera hipóteses que podem melhorar o procedimento do teste.

2.3. PTES

A metodologia PTES (*Penetration Testing Execution Standard*) [11] detalha instruções de como executar as atividades que são requeridas para testar precisamente o estado da segurança em um ambiente. A intenção da metodologia é não estabelecer padrões muito rígidos para um teste de penetração. A comunidade de analistas e profissionais de segurança, responsável por sua criação, trata a ideia de que as diretrizes para o processo de avaliação da segurança de um ambiente devem ser de fácil compreensão para as organizações. Por essa razão, as orientações técnicas ajudam a definir procedimentos a serem seguidos durante um Pentest, fazendo com que a metodologia forneça um estrutura base para iniciar e conduzir um teste de segurança. A estrutura da metodologia

é composta por sete fases: *Pre-engagement interactions*, *Intelligence gathering*, *Threat modeling*, *Vulnerability analysis*, *Exploitation*, *Post-exploitation* e *Reporting*.

Em resumo, PTES é projetado para fornecer às empresas uma linguagem mais comum para a realização de um Pentest. Isso é possível através da utilização de padrões e orientações de como o teste precisa ser realizado. Ao longo de sua descrição, a PTES apresenta esses padrões que, aliado ao fato de que a metodologia considera o conhecimento do *tester* como aspecto primordial, representa a principal vantagem da PTES em relação as demais.

Além disso, a construção da metodologia por parte da comunidade de experts na área de segurança tem atribuição direta com maiores preocupações ligadas aos critérios técnicos de um teste de segurança [7]. Em contraponto, isso impacta na falta de detalhes mais específicos nos aspectos de negócio.

2.4. NIST Guidelines

A metodologia proposta pela NIST (*National Institute of Standards and Technology*) [13] foi inicialmente introduzida como GNST (*Guideline on Network Security Testing*), reproduzida na publicação especial 800-42, e a sua última versão continuada é apresentada na publicação especial 800-15 como *Technical Guide to Information Security Testing and Assessment*. Basicamente, sua estrutura segue quatro etapas principais: **planejamento**, onde o sistema é analisado para encontrar os alvos de teste mais interessantes; **descoberta**, onde o *tester* procura as vulnerabilidades no sistema; **ataque**, onde o *tester* verifica se as vulnerabilidades encontradas podem ser exploradas; e **relatório**, onde cada resultado proveniente das ações realizadas na etapa anterior é reportado.

A elaboração deste metodologia é considerada como a primeira que introduz um processo mais detalhado para a escrita de relatórios, assim como o fato de lidar com hipóteses induzidas. De acordo com as melhores práticas, a metodologia sugere escrever um relatório passo-a-passo, onde o *tester* relata suas descobertas depois da fase de planejamento e depois de cada ataque (realizado com sucesso ou não), descrevendo as vulnerabilidades que puderam ou não ser exploradas. Além disso, outro aspecto importante da metodologia é a maneira como são construídos os vetores de vulnerabilidades [13].

2.5. OWASP Testing Guide

A metodologia proposta no OWASP (*Open Web Application Security Project*) *Testing Guide* [10] é um advento consolidado de todos os estudos que a comunidade OWASP realiza. Sua concepção é guiada pela ideia norteadora de tornar softwares seguros uma realidade, e por essa razão percebe-se que suas diretrizes são direcionadas a testes de segurança em softwares e aplicações web. Na grande maioria das organizações voltadas a desenvolvimento de software, as preocupações com segurança não fazem parte do processo de desenvolvimento padrão e, por muitas vezes, também não detém importância para as mesmas. A metodologia, então, idealiza o uso de testes de segurança como forma de conscientização e estrutura-se com base em outros projetos providos pela própria OWASP como o *Code Review Guide* e *Development Guide*.

A metodologia é dividida em três grandes blocos: a etapa introdutória que trata os pré-requisitos para testar as aplicações web e também o escopo do teste, a etapa inter-

mediária que apresenta o *OWASP Testing Framework* e suas tarefas e técnicas relacionadas as diversas fases do ciclo de vida de desenvolvimento de software, e a etapa conclusiva que descreve como as vulnerabilidades são testadas através da inspeção de código e dos testes de penetração.

3. Tramonto

As metodologias de teste de segurança são diferenciadas em diversas questões, como, por exemplo, nas definições sobre planejamento do teste, no tratamento de atividades a serem executadas, nos possíveis cenários-alvo dos testes, e até mesmo no rigor o qual a metodologia lida com a execução do teste.

Aliado com essas diferenças, mensurar e comparar as metodologias de teste de segurança é uma tarefa que requer cuidado. Os principais critérios para essa comparação podem ser considerados: flexibilidade, que diz respeito a forma como a metodologia permite a atuação do *tester* em suas escolhas em contraponto a rigidez do padrão proposto, e eficácia, que está relacionado com aspectos de como metodologia planeja e adequa as suas indicações de modo a atender o objetivo do teste. Baseado nesses critérios, outras características podem ser avaliadas para a comparação entre as metodologias. Algumas dessas características são apresentadas na Seção 3.2 e também dispostas na Tabela 1.

A partir da análise das principais metodologias de teste de segurança, foi criada uma estratégia de recomendações chamada Tramonto. A Tramonto tem como objetivo principal solucionar os problemas relacionados a falta de metodologias voltadas para Pentest, auxiliando o *tester* no processo de intrusão. Contudo, a Tramonto também tem por objetivo adequar atividades, planos, processos e fases de forma a oferecer recursos para um Pentest padronizado, flexível e eficaz.

No que diz respeito aos possíveis cenários-alvo de um Pentest, a Tramonto oferece maiores possibilidades de tratamento, considerando que as metodologias que a constroem ampliam naturalmente essa atuação nos cenários. Tais cenários-alvo foram identificados conforme o mapeamento sistemático disposto em [1], e a Figura 1 apresenta a relação de atuação das metodologias existentes e da própria Tramonto com estes cenários.

3.1. Formalização da Estrutura da Tramonto

Inicialmente, para que fosse possível idealizar soluções e definições prévias da estratégia de recomendações Tramonto, foi necessário estabelecer a estrutura básica que determina as etapas pelos quais as atividades do Pentest estão contidas, conforme apresentado na Figura 2.

Dessa forma, a estrutura da Tramonto é dividida em cinco etapas, que são as seguintes:

- Adequação: etapa responsável por gerenciar todas as escolhas iniciais do *tester* em respeito às informações de escopo, abordagem, dados do alvo, tipo do teste a ser realizado, entre outras. A partir das escolhas e determinações efetuadas, a Tramonto conduzirá o *tester* para os fluxos de trabalho seguintes, fornecendo todas as escolhas possíveis que são categorizadas de acordo com o andamento do teste. Neste ponto, toda experiência e *know-how* do *tester* é levada em conta já que a estratégia irá recomendar as melhores alternativas, não engessando as escolhas caso o profissional venha a decidir por outro caminho de execução.

		METODOLOGIAS					Tramonto
		OSSTMM	ISSAF	PTES	NIST Guidelines	OWASP Testing Guide	
CENÁRIOS - ALVO	Aplicações Web e Web Services	✖	✖	✖	✖	✓	✓
	Serviços e Protocolos de Rede	✓	✓	✓	✓	✖	✓
	Aplicações e Software	✓	✓	✓	✓	✖	✓
	Físico	✓	✖	◉	✖	✖	✓
	Cloud	✖	✖	◉	✖	✖	◉

Legenda: ✓ - Trata devidamente o cenário; ◉ - Recomenda aspectos de teste no cenário; ✖ - Não trata o cenário.

Figura 1. Cenários-alvo para cada metodologia e Tramonto.

Figura 2. Estrutura da Tramonto.

- Verificação: mediante as alternativas delimitadas na etapa anterior, a etapa de verificação consistirá em efetuar os *checklists* de necessidades, dados, atividades orientadas que foram ou não efetuadas e demais itens relevantes. O intuito dessa etapa é minimizar o número de falhas para a continuidade do teste, de forma com que a Tramonto contribua para que o teste seja o mais detalhista possível, sem retrabalhos.
- Preparação: envolve a escolha das estratégias de teste de penetração a serem efetuadas, bem como a indicação de kits de ferramentas de acordo com os processos anteriores. O processo de preparação idealiza fornecer ao *tester* a análise e detalhamento do planejamento e forma de execução do teste. Nesta etapa a Tramonto permite que as soluções de aplicação do teste de penetração estejam suficientemente elaboradas e com as devidas prescrições mediante os dados provenientes das etapas anteriores.
- Execução: trata o núcleo principal de execução do teste de penetração. Nesta etapa, a Tramonto fornece todo o aparato em relação aos vetores de ataque, que são os possíveis caminhos utilizados pelo *tester* para realizar as intrusões. Os vetores de ataque refletem o planejamento do tipo de ataque que é efetuado, podendo esse ser baseado em computadores (por meios tecnológicos) ou baseado em

pessoas (caracterizados pelo contato direto). Além disso, são listados também os possíveis resultados a serem obtidos de acordo com as ações e demais informações relacionadas. É essencial ressaltar que, nesta etapa, os fluxos oferecidos como alternativas de execução do teste devem estar filtrados de acordo com as informações e verificações das etapas anteriores. Essa funcionalidade permite que o *tester* otimize o tempo do teste mediante suas escolhas anteriores, além de induzir atividades mais precisas sobre o escopo delimitado.

- Finalização: a última etapa proposta na estrutura da Tramonto contempla as ações relacionadas com a elaboração dos relatórios a serem fornecidos ao cliente. Ao mesmo tempo, como característica adicional, a construção de um relatório destinado ao próprio *tester* é um dos itens que a estratégia de recomendações produz ao término do teste, permitindo a criação de um padrão que, posteriormente, pode vir a fornecer as possibilidades de comparação entre os resultados obtidos. Ainda nesse processo são tratadas as atividades de cobertura de rastros, limpeza de registros e controle de estado dos sistemas e aplicações alvo.

É possível ainda descrever um sexto processo que descreve uma avaliação, oferecendo alternativas baseadas no resultado obtido e no resultado desejado inicialmente. Nesse sentido, é estabelecida uma nova funcionalidade específica da Tramonto chamada de Plano Alternativo (PA), responsável por fornecer atividades, fluxos, ferramentas, estratégias e todo o tipo de características iminentes que, dependendo das escolhas e ações do *tester*, trazem novas possibilidades para o fluxo processual do teste de penetração. Dessa forma, cada uma das etapas estabelecidas pode conter planos alternativos que são identificados pelo nome do processo, seguido de um identificador (por exemplo, *PAP1* refere-se a um plano alternativo na etapa de preparação e detém um *ID* 1). Assim, compreende-se que devido a vasta quantidade de informações diferentes contidas nas metodologias analisadas, podem ser criados diversos sub-planos de acordo com as informações iniciais o teste.

3.2. Comparação da Tramonto com as principais metodologias

A Tramonto, conforme descrito anteriormente, é uma estratégia de recomendações destinada exclusivamente para testes de penetração. Nesse sentido, é preciso considerar que a Tramonto não trata-se de uma metodologia, e também que a comparação em relação às suas metodologias base é realizada para compreender quais itens podem ou não ser atendidos pela estratégia.

O fato de ser uma estratégia direcionada para testes de penetração já representa um quesito passível de comparação. Percebe-se que, dentre as metodologias citadas na Seção 2, somente a PTES é específica para testes de penetração, enquanto as demais destinam-se para testes de segurança diversos.

Para estabelecer uma comparação entre as metodologias e a Tramonto, foram consideradas as seguintes características: Abrangência, Flexibilidade, Modelagem, Adaptação, Planejamento e Relatório. Essas características foram definidas a partir dos critérios citados no início desta Seção 3: flexibilidade e eficácia do teste. Características como Abrangência, Modelagem, Adaptação e Planejamento, representam aspectos que contribuem diretamente para ambos os critérios principais. Tais características são explicadas nas subseções 3.2.1, 3.2.3, 3.2.4 e 3.2.5, respectivamente. Além disso, a Flexibilidade (subseção 3.2.2) também é considerada uma característica para comparação,

Tabela 1. Comparativo de características entre as metodologias e a Tramonto.

	OSSTMM	ISSAF	PTES	NIST Guidelines	OWASP Guide	**Tramonto**
Última Atualização	2010	2006	2012	2008	2014	**2016**
Específica para Pentest	Não	Não	Sim	Não	Não	**Sim**
Abrangência	A	AP	A	AP	NA	**A**
Flexibilidade	AP	NA	AP	A	NA	**A**
Modelagem	A	AP	AP	NA	A	**A**
Adaptação	A	AP	NA	AP	AP	**AP**
Planejamento	AP	A	A	AP	A	**A**
Relatório	A	AP	AP	A	AP	**A**

Legenda - A: Atende; AP: Atende Parcialmente; NA: Não Atende.

juntamente com o item Relatório (subseção 3.2.6), que trata a documentação do teste e outros detalhes.

A Tabela 1 apresenta um comparativo dessas características em relação as metodologias. Os valores para essa comparação são categorizados em:

- **Atende** (A): Fornece definições detalhadas para lidar com a característica de maneira apropriada.
- **Atende Parcialmente** (AP): Questões sobre a característica são mencionadas, mas sem o rigor e detalhe necessários.
- **Não Atende** (NA): A metodologia não menciona nada relacionado à característica, ou não contempla as definições da mesma.

Com base na comparação, as subseções a seguir descrevem cada característica e como a Tramonto busca adequar-se para atender os critérios.

3.2.1. Abrangência

Inicialmente, uma das atividades importantes para um teste de segurança é a definição do escopo. Escopo refere-se às preocupações do alcance do teste em relação aos possíveis cenários-alvo. As metodologias OSSTMM, ISSAF, PTES e NIST são facilmente integradas e podem ser adequadas para aplicações e sistemas operacionais, banco de dados, avaliações de segurança física e aplicações web. Contudo, o modelo *OWASP Testing Guide* tem seu foco precisamente definido: serviços e aplicações web. Dessa forma, a abrangência dessa metodologia pode representar uma limitação.

Na Tramonto a abrangência é tratada na fase de Adequação. A principal contribuição da estratégia em relação a este critério se dá através do direcionamento do fluxo das atividades de cada etapa de acordo com o cenário-alvo. Assim, quanto melhor delimitado for o andamento durante a execução do teste, maior será a facilidade no tratamento de possíveis problemas referentes a características do cenário-alvo.

3.2.2. Flexibilidade

A possibilidade de integrar meios, itens e direções adicionais ao teste de segurança a partir dos resultados obtidos em cada etapa ou fase da metodologia, é uma característica importante no contexto atual de verificações de segurança. Nesse sentido, mesmo que uma definição estática dos planos e passos a serem seguidos seja um requisito primordial, a flexibilidade de incluir novos itens torna uma metodologia mais interessante. Para essa característica, o modelo fornecido pela NIST apresenta um aspecto interessante ao permitir que o *tester* tenha maior dinamicidade ao longo do teste, podendo considerar e reavaliar seus artefatos obtidos a cada atividade. Em contraponto, algumas metodologias, como OSSTMM ISSAF e *OWASP Testing Guide*, ao mesmo tempo que são extremamente robustas, limitam tal flexibilidade por tratarem os cenários de execução especificamente.

De forma cíclica e continuada, a Tramonto trata o critério flexibilidade com o intuito de garantir que cada atividade ou passo dentro das etapas seja validada. Nesse sentido, a Tramonto estabelece duas opções possíveis para essa validação: um sistema de notas, para mensurar a capacidade de cada atividade frente ao teste, e uma análise das recomendações, considerando tabelas de ”memória”. O sistema de notas pode balizar o andamento do teste e redirecionar o mesmo de acordo com a satisfação ou não da atividade. Isso é feito de acordo com a nota definida, mecanismo esse que é estabelecido pelo próprio *tester*. Já a tabela de ”memória”consiste em armazenar os conteúdos e experiências relevantes obtidos durante cada atividade para permitir alterações no teste.

3.2.3. Modelagem

Ao definir detalhadamente os aspectos e conceitos norteadores para o processo de teste, a metodologia pode até limitar a flexibilidade, mas incrementa a qualidade da modelagem. Esses conceitos-chave facilitam o *tester* na sua atividade de modelar todo o fluxo de ações do teste, além de modelar o sistema e ambiente alvo. Isso ratifica um ponto crucial em testes de segurança, que é a eliminação de possíveis ambiguidades em relação a cada passo subsequente a ser realizado. Para essa característica, os modelos OSSTMM, *OWASP Testing Guide* e PTES atendem adequadamente, principalmente pela forma com que abordam a etapa de planejamento do seu processo de teste.

Na etapa de Adequação, a Tramonto trata o critério modelagem, onde é inicialmente abordado. Nela são determinadas os meios de abordagem aos conceitos pré-estabelecidos, fazendo com que o *tester* consiga traçar os objetivos do teste e suas subetapas mediante definições *a priori*.

3.2.4. Adaptação

É importante possuir conceitos bem definidos com o intuito de evitar possíveis ambiguidades e, portanto, impactar na adaptação. Além disso, a possibilidade de adaptar a metodologia e suas ações para diferentes ambientes fornece um fluxo do teste mais completo. Entre as possíveis adaptações possíveis estão, por exemplo, a escolha dos tipos de teste, o plano de teste ou a definição de escopo. A partir das metodologias estudadas, por um lado, a OSSTMM é aquela que pode melhor satisfazer esta característica, uma vez

que tem um processo com atividades bem definidas. Por outro lado, a metodologia PTES apresenta algumas limitações por não detalhar concisamente essas adaptações como uma alternativa.

A adaptação para a Tramonto tem uma relação semelhante ao critério abrangência. Contudo, cabe considerar que a Tramonto objetiva fornecer conjuntos pré-definidos de tipos de teste, oferecendo variações em atividades específicas. Em contraponto a isso, também permite que o *tester* consiga alterar alguns desses conjuntos, tornando a execução do teste dinâmica e permissiva.

3.2.5. Planejamento

Todo o conjunto de aspectos definidos em um teste de segurança deve ser devidamente planejado antes de iniciar a execução do teste. Assim, o planejamento é a característica que representa o suporte fornecido ao *tester* para a fase de definição, execução das atividades, pré-requisitos para continuação e andamento do teste, escolha das ferramentas a serem utilizadas e também o retorno esperado para cada atividade dentro do teste. PTES é uma metodologia que fornece esse tipo de característica. Ela descreve, cuidadosamente, todo o planejamento que deve ser definido, além de estabelecer o conjunto de ferramentas, e como operar as mesmas, que serão utilizadas em cada atividade do Pentest. OSSTMM e NIST, uma vez que tentam fornecer maior flexibilidade, não são focadas em prover um planejamento muito detalhado.

Nesse ponto a Tramonto é estritamente vinculada as demais etapas. O planejamento do teste tem inúmeras variações de acordo com a flexibilidade, adaptação e abrangência, fazendo com que cada escolha seja notavelmente acolhida às decisões do *tester*.

3.2.6. Relatório

Por fim, é possível considerar a documentação como parte das características principais da constituição de um Pentest. Todas as metodologias estudadas fornecem como a documentação precisa ser produzida, contendo sugestões e indicações para o preenchimento do relatório final de teste.

Para tal, a Tramonto estabelece uma frequente e assídua documentação de todo o fluxo do teste e com registro dos detalhes considerados mais importantes. Uma contribuição nesse ponto é a possibilidade de constituir um resumo mediante a descrição das atividades e resultados mais relevantes, que pode ser entregue juntamente ao relatório completo.

4. Discussão e Principais Contribuições

O conflito entre padronizar um teste por completo e torná-lo o mais flexível possível a partir das escolhas do *tester* é um problema no qual a Tramonto procura solucionar de uma forma balanceada. Através da criação de uma estratégia de recomendações busca-se indicar soluções para a realização de um teste de penetração que auxilie o *tester* durante toda a execução.

Uma das principais contribuições da Tramonto é permitir alternativas e sugerir, durante as etapas, atividades devidamente planejadas. Essas sugestões, por sua vez, não inibem a atuação do *tester*, já que a Tramonto considera que o seu *know-how* pode implicar diretamente no sucesso do teste. A etapa de Adequação da Tramonto é um exemplo dessa descrição.

Considerando um exemplo da aplicação de um teste de penetração para avaliar a segurança dos servidores de uma instituição de ensino, as discussões da etapa de Adequação da Tramonto ficam em torno de:

1. Informações sobre o alvo: as indicações iniciais do teste são guiadas, essencialmente, pelas informações obtidas em reuniões e/ou repassadas pelo cliente. Por vezes, o cliente pode ser induzido a avaliar o estado de segurança de outros pontos nos quais ele pode não ter considerado. Dessa forma, o *tester* pode sugerir meios que possam contribuir para que o teste seja mais eficaz e, aliado a isso, acabem testando esses pontos que possam interferir na preocupação inicial do cliente. No exemplo de aplicação, o cliente (instituição) passa apenas o desejo de testar a segurança de seus servidores, e fornece os dados sobre os mesmos (nomes, *range* endereços IP e localização física, entre outros). Além disso, o cliente repassa as informações de controles, diretivas e políticas de segurança que estão relacionadas aos servidores. Essas informações são requisitadas pela Tramonto e são recomendações provenientes, principalmente, das metodologias NIST e PTES.
2. Informações gerais do teste: neste ponto da etapa de Adequação são estabelecidas as características gerais do teste, como datas, intervalos de tempo para execução do teste, avaliações e métodos utilizados. Determinar datas e horários para a aplicação do teste é um quesito que a Tramonto recomenda não só com o intuito de assegurar um melhor funcionamento do mesmo, mas também para relacionar com o tipo de Pentest que será efetuado. Caso seja optado por avaliar também a equipe que responde pelos incidentes de segurança, os horários podem ser diferentes dos determinados inicialmente pelo cliente. Ainda nesse sentido, os intervalos para execução do teste também são determinados e discutidos com o cliente para que os cuidados com possíveis interrupções no negócio sejam devidamente tomados. A Tramonto apresenta alguns *checklists* na etapa de Verificação, mas esses são criados a partir dessas informações da etapa de Adequação. Outro aspecto contido nas informações gerais do teste são as escolhas para a avaliação ou não dos controles, políticas e demais aspectos gerenciais anteriormente obtidos com o cliente. Para o caso da avaliação dos servidores, o intervalo de tempo fica aberto ao *tester*, ou seja, sem restrição por parte da instituição. Não são avaliadas as políticas e diretrizes, apenas é considerado o plano de contingência para eventuais problemas de funcionamento dos sistemas armazenados nestes servidores. A Tramonto efetua as recomendações desse item a partir de tópicos tratados pelas metodologias OSSTMM e NIST.
3. Determinações contratuais e implicações legais: antes do início do teste, é requisito obrigatório da Tramonto a atribuição de aspectos contratuais. É necessário delimitar em contrato qual o teste será efetuado, os limites que a penetração não pode ultrapassar ou alcançar (e caso ocorra ou o cliente solicite posteriormente, saber quais as implicações contratuais), o acordo de confidencialidade (em relação à informações sensíveis passíveis de serem descobertas ao longo do teste, por exem-

plo) e por fim, os custos envolvidos em toda a operação. Além disso, existem os cuidados com as implicações legais, envolvendo a violação de controles ou até mesmo a descoberta de registros que possam comprovar atividades maliciosas por parte de colaboradores da empresa cliente. Os prazos de entrega do relatório final e de soluções para mitigação de ataques e correção de vulnerabilidades é outro ponto tratado neste item. No exemplo da aplicação do teste nos servidores da instituição de ensino, não é autorizada a divulgação das informações a respeito desses itens.

4. Estratégias e técnicas do teste: a etapa de Adequação encerra-se listando, a partir das informações coletadas anteriormente, as possibilidades de estratégias e técnicas que o *tester* pode querer utilizar na execução do teste. Essas possibilidades são criadas pela Tramonto com o intuito de facilitar o teste, fazendo com que o *tester* possa indicar suas preferências a partir de soluções pré-determinadas. Contudo, essa pré-determinação é construída com base em duas vertentes: padrões indicados pelas metodologias (como OSSTMM, OWASP e PTES) e testes de penetração efetuados anteriormente. O segundo ponto é um contribuição relevante da Tramonto, já que ao término de cada teste efetuado, é possível atribuir uma avaliação que pode indicar que as escolhas deste teste realizado mostraram-se eficientes para atingir o objetivo proposto. Para o exemplo em questão, as estratégias sugeridas pela Tramonto são duas: teste de segurança a partir da rede interna e teste de segurança física.

Dessa forma, é perceptível que o *tester* possui uma flexilidade relevante utilizando a Tramonto. Assim, conclui-se que o fato do teste não ser completamente padronizado e de que há a interferência do *tester* indica que a Tramonto resolve o problema anteriormente descrito através de uma solução equilibrada que mostra-se interessante para o âmbito de testes de segurança.

A proposta de uma estratégia de recomendações é uma solução nova na área de Testes de Penetração, o que ratifica a relação de nível diferente entre a Tramonto e a demais metodologias de teste de segurança (OSSTMM, por exemplo). Neste ponto, uma limitação da Tramonto é não representar uma metodologia, pois considera-se que criar uma metodologia requer o know-how de muitos especialistas da área e principalmente de um número elevado de avaliações de aplicação da mesma em testes executados. Por outro lado, a Tramonto contempla, além de tarefas, passos, fluxos e conceitos provenientes de cada uma das metodologias, características próprias (como a solução de planos alternativos, por exemplo). Novas funcionalidades aliadas às demais características das metodologias base podem incrementar a qualidade do teste executado, e este ponto representa outra contribuição relevante da Tramonto.

Da mesma forma, a Tramonto apresenta também como contribuições:

- Análise das metodologias base: Cada etapa da Tramonto foi determinada e construída a partir de uma análise detalhada das principais metodologias utilizadas para testes de segurança. Assim, a criação da Tramonto é um processo que contempla uma análise de conteúdo das metodologias, realizada com o viés destinado a Testes de Penetração. A partir disso foi possível identificar características as quais não se encaixam adequadamente em padrões de teste de segurança atuais, como a identificação de vetores de ataque indicada pela ISSAF, por exemplo. Em

contraponto, o fornecimento de *checklists* e outros aspectos que são relacionados a outros tipos de teste de segurança contribuíram para funcionalidades além das triviais de um Pentest.

- Fornecer aos executores dos testes uma alternativa de padronização mais intuitiva e principalmente flexível, considerando que a Tramonto busca determinar um processo que se aproxime da melhor solução na relação inversamente proporcional entre modelos com passos e fluxos fechados e as escolhas pessoais dos próprios executores do teste, como afirmado anteriormente.
- A utilização de uma aplicação que auxilie o *tester* a seguir as recomendações da Tramonto e que, paralelamente, registra as atividades e resultados de cada etapa da estratégia. Neste ponto existe a proposta de uma solução de elaboração de relatório de um teste a partir das indicações feitas na aplicação. Esse fator também permite que a aplicação possa fornecer, a partir da extração de conhecimento dos dados de testes já executados, padrões de solução de testes de penetração realizados com a Tramonto.

5. Considerações Finais

O uso de testes de penetração como método para avaliação da segurança de sistemas e demais cenários-alvo mostra-se uma solução interessante para organizações e empresas. Isso se deve ao fato da forma como o teste é executado, simulando intrusões e comportamentos de atacantes maliciosos, fornecendo assim uma percepção próxima da realidade dos ataques reais que, por sua vez, vêm tomando uma proporção exponencial em quantidade e efetividade. Para o tratamento desses ataques e o uso dos testes de segurança é essencial a atuação da comunidade de profissionais de segurança e das pesquisas relacionadas a esse contexto, pois a partir desse movimento, surgem padrões e soluções que auxiliam a área. As metodologias analisadas neste trabalho possuem ampla consolidação em estudo e uso, porém com objetivos e características variadas. Isso motivou a construção da estratégia de recomendações Tramonto, contribuindo para uma solução destinada a testes de penetração com base nas principais metodologias de teste de segurança. No cenário de Pentest, a Tramonto apresenta-se como uma alternativa única no que diz respeito ao desenvolvimento de recomendações, avaliando cuidadosamente o processo de Pentest e propondo funcionalidades para aumentar a eficácia e auxiliar o *tester* em suas atividades. Nesse sentido, a Tramonto é norteada pelo objetivo de atender os critérios de eficácia e flexibilidade do teste, sabendo que atualmente grande parte dos *testers* utiliza metodologia própria ou alguma que não é destinada exclusivamente para Pentest, implicando em não conseguir mensurar devidamente esses critérios. Assim, acredita-se que a Tramonto pode futuramente ser aprimorada para incluir os diferentes cenários de aplicação de testes de penetração, aprimorando o nível de detalhe e idealizando a criação de padrões de teste que possam oferecer soluções e avaliações mais rápidas e eficazes.

Referências

[1] D. D. Bertoglio and A. F. Zorzo. Um mapeamento sistemático sobre testes de penetração. Technical Report TR 084, Faculdade de Informática, Programa de Pós-Graduação em Ciência da Computação, Pontifíca Universidade Católica do Rio Grande do Sul (PUCRS), Porto Alegre, Rio Grande do Sul, 2015.

[2] T. Dimkov, A. van Cleeff, W. Pieters, and P. Hartel. Two methodologies for physical penetration testing using social engineering. In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pages 399–408, New York, NY, USA, 2010. ACM.

[3] O. I. S. S. Group. *Information Systems Security Assessment Framework*. Open Information Systems Security Group, 2006.

[4] K. M. Henry. *Penetration Testing: Protecting Networks and Systems*. IT Governance Publishing, 2012.

[5] P. Hertzog. *OSSTMM - Open Source Security Testing Methodology Manual*. Institute for Security and Open Methodologies (ISECOM), 2010.

[6] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta. Effective penetration testing with metasploit framework and methodologies. In *Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on*, pages 237–242, Nov 2014.

[7] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni. *Metasploit: The Penetration Tester's Guide*. No Starch Press, San Francisco, CA, USA, 1st edition, 2011.

[8] K. Lam, D. LeBlanc, and B. i. Smith. *Assessing network security*. Redmond, Wash. Microsoft Press, 2004.

[9] B. Liu, L. Shi, Z. Cai, and M. Li. Software vulnerability discovery techniques: A survey. In *Proceedings of the 2012 Fourth International Conference on Multimedia Information Networking and Security*, MINES '12, pages 152–156, Washington, DC, USA, 2012. IEEE Computer Society.

[10] M. Meucci, E. Keary, and D. Cuthbert. *OWASP Testing Guide v.3*. OWASP Foundation, 2008.

[11] C. Nickerson, D. Kennedy, E. Smith, A. Rabie, S. Friedli, J. Searle, B. Knight, C. Gates, and J. McCray. *Penetration Testing Execution Standard*. PTES, 2014.

[12] M. Prandini and M. Ramilli. Towards a practical and effective security testing methodology. In *Computers and Communications (ISCC), 2010 IEEE Symposium on*, pages 320–325, June 2010.

[13] K. Stouffer, J. Falco, and K. Scarfone. *NIST SP 800-115: Technical Guide to Information Security Testing and Assessment*. National Institute of Standards and Technology, 2008.

[14] A. Whitaker and D. Newman. *Penetration Testing and Cisco Network Defense*. Cisco Press, 2005.

[15] J. J. Zhao, S. Y. Zhao, and S. Y. Zhao. Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, 27(1):49 – 56, 2010.

