# Análise e avaliação de Teste de Intrusão para a estratégia de recomendações Tramonto

**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.*** *Nowadays, research on Penetration Testing (Penetration Tests) has new directions in Information Security. Methodologies, techniques and tools have been developed to meet the main challenges of these tests: automation, effectiveness and flexibility. Tramonto is a recommendation strategy designed to assist the tester with these challenges, relating concepts and applications of widely-known methodologies for security testing. This paper discusses the relation of Penetration Tests with Tramonto, analyzing a real test case from the perspective of the proposed strategy.*

***Resumo.*** *Atualmente, as pesquisas sobre Testes de Intrusão (Penetration Tests) apresentam novos rumos para a área de Segurança da Informação. Metodologias, técnicas e ferramentas têm sido desenvolvidas para atender os principais desafios destes testes: automatização, eficácia e flexibilidade. A Tramonto é uma estratégia de recomendações criada para auxiliar o tester com esses desafios, relacionando conceitos e aplicações de metodologias amplamente conhecidas para testes de segurança. Este trabalho discute a relação de Testes de Intrusão com a Tramonto, analisando um caso real de teste sob a ótica da estratégia proposta.*

## 1. Introdução

Atualmente, a informação é considerada o ativo mais valioso para a maioria das empresas. Isso é justificado pelo fato de que o mercado vem emergindo com empresas que possuem um modelo de negócio baseado na informação. Paralelamente, as pesquisas relacionadas com a Segurança da Informação têm procurado soluções para proteger e mitigar o alto número de incidentes de segurança no contexto empresarial. Essas soluções não buscam apenas avaliar a existência de fraquezas e vulnerabilidades nos cenários-alvo, mas sim tratar o impacto dessas brechas na organização, caso algum atacante explore-as e efetue seus ataques.

Tais soluções variam entre mecanismos de defesa, softwares de monitoramento de incidentes, políticas e controles de diretivas e também de procedimentos de avaliação e teste de segurança. Tratando-se de avaliação e teste de segurança, que procuram mensurar, identificar e analisar qual o estado de segurança de um processo, controle, ativo, sistema e até rede, uma das técnicas conhecidas é o Teste de Intrusão (*Pentest*). Segundo [Lam et al. 2004], testes de intrusão aproximam a realidade dos ataques através da simulação do comportamento de um atacante. Em termos gerais, um teste de intrusão

pode ser definido como a tentativa deliberada e controlada de invadir um sistema ou rede com o objetivo de avaliar o estado de segurança do alvo [Bishop 2007].

Testes de intrusão possuem características específicas que variam de acordo com o alvo. Podem ser considerados diferentes aspectos quanto as atividades executadas, divisão de fases, estratégia do teste e até mesmo nas ferramentas utilizadas. Assim, o teste de intrusão permite também que as avaliações possuam objetivos variados, como o aumento da segurança dos sistemas, a identificação de vulnerabilidades, o teste da equipe de segurança da empresa alvo e até mesmo o aumento da segurança organizacional e de pessoas [Henry 2012].

Tantas possibilidades ofertadas por esse tipo de teste de segurança tornam a padronização destes testes de intrusão uma tarefa complexa. Existem metodologias de teste de segurança, posteriormente citadas nesse trabalho, que objetivam tratar esse problema da padronização. Contudo, das metodologias que são mais disseminadas, apenas uma é direcionada para testes de intrusão. A partir disso, a criação de uma estratégia de recomendações de teste é uma possível solução para auxiliar as atividades no processo de um teste de intrusão. Dessa forma, criou-se a Tramonto [Dalalana Bertoglio and Zorzo 2016], uma estratégia de recomendações direcionada a testes de intrusão que objetiva padronizar os testes ao mesmo tempo que procura oferecer flexibilidade ao *tester* e maior eficácia a partir da normatização dos processos. Neste artigo discutimos a relação de um teste de intrusão real com a estratégia de recomendações Tramonto,

Este artigo está organizado da seguinte forma: a Seção 2 descreve os principais conceitos e características de Testes de Intrusão. Já a Seção 3 apresenta a conceituação e formalização das características da estratégia de recomendações Tramonto. A Seção 4 explica detalhadamente o caso real de um teste de intrusão realizado, enquanto a Seção 5 detém a discussão e análise a respeito das principais contribuições da Tramonto direcionadas ao caso apresentado. Por fim, a Seção 6 apresenta as considerações finais deste trabalho.

## 2. Testes de Intrusão

Hoje em dia, proteger sistemas e redes exige um conhecimento amplo das melhores táticas, ferramentas e motivações do atacante. Conhecer a natureza e as técnicas do atacante melhora a capacidade de evitar ataques bem sucedidos, já que auxilia a verificação de quais as vulnerabilidades existentes que o próprio hacker malicioso pode encontrar.

Testes de intrusão caracterizam a simulação de um ataque a um sistema, rede ou serviço, com o objetivo de comprovar a vulnerabilidade desse sistema e até mesmo o risco de que o alvo possa sofrer um verdadeiro ataque [Geer and Harthorne 2002]. Dessa forma, proteger as redes corporativas envolve mais do que simplesmente estratégias padrão (como gerenciamento de patches, firewalls, e conscientização de usuários), envolve uma frequente validação de como funciona o "mundo real" [Bishop 2007].

A estruturação de um teste de penetração passa por uma série de critérios que permitem que os testes se diferenciem uns dos outros. Essa diferenciação também implica nas variações dos objetivos do teste e, naturalmente, na eficácia da avaliação proposta. Assim, a aplicação do teste de penetração pode ser classificada em critérios como [Whitaker and Newman 2005]:

- Base de informações. Determina qual o nível de conhecimento que o *tester* possui sobre o alvo antes da execução do teste.
- Agressividade. Critério responsável por definir o quão agressivo age o profissional que está efetuando o teste de intrusão. Em resumo, mensura se o *tester* explora as vulnerabilidades por completo, parcialmente, ou não as explora.
- Escopo. Define o escopo do teste de intrusão, determinando quais os sistemas ou cenários serão testados. O escopo implica diretamente no tempo requerido para a execução do teste.
- Abordagem. Trata o método de execução do teste de intrusão quanto à geração de ruído no ambiente. Em geral, a abordagem pode ser dividida em *covert*, onde os procedimentos do teste não são diretamente identificáveis, e *overt*, onde o teste se assemelha às configurações de uma base de informações *white-box*.
- Técnica: Determina quais as técnicas e metodologias serão usadas no teste de intrusão. Em um teste de intrusão convencional, a técnica é baseada em rede, considerando a ideia de que todos os ataques realizados ao sistema são apenas via rede. Um teste de intrusão baseado em rede simula o típico ataque de um hacker malicioso que atua via protocolo TCP/IP [Fonseca et al. 2010][Jajodia et al. 2005].
- *Starting point*. O ponto onde o *tester* conecta seu equipamento para realizar os ataques do teste pode ser tanto de dentro ou de fora da rede ou ambiente físico do alvo.

## 2.1. Fases

Além dos critérios que diferenciam os testes, existem abordagens diferentes (que geralmente são relacionadas com a metodologia do teste utilizado) em relação às fases pelas quais o teste passa durante a sua aplicação. De maneira abrangente, pode-se delimitar três principais fases para um teste de intrusão: *Pre-Attack phase*, *Attack phase* e *Post-Attack phase*.

### 2.1.1. Fase 1: *Pre-Attack*

A fase *Pre-Attack* consiste em investigar ou explorar o alvo em potencial. Esta fase é basicamente responsável pela tarefa de obtenção de informações e pode ser dividida em reconhecimento passivo e reconhecimento ativo. Reconhecimento passivo envolve a coleta do maior número de informações sobre um alvo em potencial sem o conhecimento da organização, e sabe-se que muitos dados, por exemplo, sobre serviços que executam e até mesmo sobre a topologia da rede, vazam ou são facilmente conseguidos. O tester pode usar essas informações para traçar um mapa do seu alvo e utilizar tal recurso como apoio de decisões estratégicas em relação às possibilidades de ataque. Ainda nesse sentido, informações públicas que são disponíveis sobre o alvo também apoiam efetivamente o sucesso do teste a ser executado. Nesta fase é primordial manter o registro das atividades realizadas e principalmente dos resultados e informações obtidas. O tester precisa garantir e comprovar o seu trabalho através desses registros, além de comunicar os responsáveis da organização a respeito das suas ações (mediante tipo do teste de intrusão, conforme abordado anteriormente). Enquanto a estratégia de ataque é planejada, devem ser correlacionados as escolhas dos vetores de ataque em relação às entradas e saídas provenientes dessa fase. Como possíveis resultados desta fase, é possível obter informações a respeito

de itens como: localização física e lógica do alvo, conexões analógicas, informações pessoais, e informações sobre outras organizações conectadas com o alvo.

### 2.1.2. Fase 2: *Attack*

A fase *Attack* lida basicamente com o comprometimento do alvo, onde o *tester* pode explorar as vulnerabilidades descobertas na fase anterior, de forma a obter acesso ao sistema [Igure and Williams 2008][Sarraute et al. 2011]. As principais atividades nesta fase contemplam o núcleo do teste de intrusão e detém a maior parte do teste. Estas atividades podem ser listadas como: teste de perímetro, teste de firewall, teste de aplicações web, acesso ao alvo e escalada de privilégios. Além disso, há a atividade relacionada ao comprometimento efetivo do alvo alcançado através da execução de códigos arbitrários, cujo objetivo é explorar a extensão na qual a segurança falha.

### 2.1.3. Fase 3: *Post-Attack*

A fase *Post-Attack* contempla as revisões e atividades finais do teste de intrusão realizado, onde o *tester* atua na reconstrução do ambiente avaliado, bem como a restauração dos sistemas e segmentos que sofreram alterações mediante as explorações feitas. Analisando o fluxo do processo de teste, subentende-se que esta fase trata os devidos encaminhamentos dos resultados e de toda a avaliação de segurança efetuada no alvo, relacionando diretamente com o objetivo proposto inicialmente na concepção do teste. Assim, a apresentação dos resultados é a atividade final desta fase e, consequentemente, do teste de intrusão [Line et al. 2008][Bechtsoudis and Sklavos 2012].

Ao longo desta última fase o *tester* é responsável por remover todos os arquivos provenientes do teste, limpar todos os registros, recuperar todas as modificações realizadas em arquivos e alterar todas as configurações para seu estado original. Em contraponto, essa retomada do ambiente alvo para seu estado original passa também pelo processo de tratamento das vulnerabilidades encontradas, mesmo que essa tarefa só seja realmente efetivada após a documentação, apresentação e análise da aplicação do teste como um todo.

## 2.2. Metodologias

Atualmente, as principais metodologias de teste de segurança são: OSSTMM (*Open Source Security Testing Methodology Manual*), ISSAF (*Information Systems Security Assessment Framework*), PTES (*Penetration Testing Execution Standard*), NIST (*National Institute of Standards and Technology) Guidelines* e OWASP *Testing Guide* [Dalalana Bertoglio and Zorzo 2017].

- **OSSTMM**. OSSTMM (*Open Source Security Testing Methodology Manual*) [Hertzog 2010] é a metodologia que detém um padrão internacional para testes de segurança, mantida pela ISECOM (*Institute for Security and Open Methodologies*). Essa metodologia é basicamente dividida em três classes (COMSEC (*Communications Security Channel*), PHYSSEC (*Physical Security Channel*) e SPECSEC (*Spectrum Security Channel*), que por sua vez, são divididas em cinco canais (Humano, Físico, Sem Fio, Telecomunicações e Redes de Dados).

- **ISSAF**. ISSAF (*Information Systems Security Assessment Framework*) [ISSAF 2006] é um *framework* que gerencia requisitos e diretivas de controle internos para a segurança da informação. É essencialmente constituído de três áreas de execução: planejamento e preparação, avaliação e relatório, limpeza e destruição de artefatos.
- **PTES**. A metodologia PTES (*Penetration Testing Execution Standard*) [Nickerson et al. 2014] é a única direcionada para testes de intrusão e fornece todo o aparato necessário para um *tester*. A estrutura da metodologia é composta por sete fases: *Pre-engagement interactions*, *Intelligence gathering*, *Threat modeling*, *Vulnerability analysis*, *Exploitation*, *Post-exploitation* e *Reporting*.
- **NIST Guidelines**. A metodologia proposta pela NIST (*National Institute of Standards and Technology*) [Stouffer et al. 2008] é apresentada na publicação especial 800-15 como *Technical Guide to Information Security Testing and Assessment* e é construída a partir de 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.
- **OWASP Testing Guide**. A metodologia proposta no OWASP (*Open Web Application Security Project*) *Testing Guide* [Meucci et al. 2008] tem a sua proposta voltada para o contexto web, e objetiva testar a segurança em softwares e aplicações web. São propostas atividades detalhadas para se avaliar diferentes tipos de riscos e vulnerabilidade na web, e tudo com base nas pesquisas e contribuições gerenciadas pela comunidade juntamente com a OWASP.

## 3. Tramonto

A partir das metodologias de teste de segurança citadas na Seção 2.2, e dos desafios que estão contidos nos estudos relacionados aos Testes de Intrusão e suas características, foi criada uma estratégia de recomendações chamada Tramonto [Dalalana Bertoglio and Zorzo 2016]. A Tramonto tem como objetivo principal solucionar os problemas relacionados a falta de metodologias específicas para Testes de Intrusão, auxiliando o *tester* no processo do teste. Adicionalmente, a Tramonto também tem por objetivo adequar atividades, planos, processos e fases de forma a oferecer recursos para um teste padronizado, flexível e eficaz.

Inicialmente, para que fosse possível idealizar soluções e definições da estratégia de recomendações Tramonto, foi necessário estabelecer a estrutura básica que determina as etapas pelos quais as atividades do Teste de Intrusão estão contidas, conforme apresentado na Figura 1.

Assim, a estrutura da estratégia de recomendações Tramonto é dividida basicamente em cinco etapas que descrevem o seu fluxo:

- **Adequação**. A etapa inicial da Tramonto é responsável por gerenciar todas as escolhas iniciais do *tester* em respeito às informações de escopo, abordagem, dados do alvo e tipo do teste a ser realizado. Essas definições iniciais são determinantes para o andamento e execução do teste, e precisam da aprovação do administrador ou responsável pelo ambiente alvo. Assim, é alinhado o máximo de


**Figura 1. Estrutura da Tramonto.**

informações com o intuito de que o plano seja melhor traçado. 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.

- **Verificação**. Mediante as alternativas delimitadas na etapa anterior, a etapa de verificação consiste em efetuar os *checklists* de necessidades, dados, atividades orientadas que foram ou não efetuadas e demais itens relevantes. Essa etapa assemelha-se ao processo de auditoria, considerado também um teste de avaliação de segurança. Nesse sentido, validar as entradas e necessidades do teste permite também que o *tester* avalie suas decisões tomadas na etapa anterior e verifique se as escolhas tomadas inicialmente, aliadas aos checklists gerados, fornecem a base essencial para avaliação do estado de segurança do alvo. Assim, 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. Da mesma forma, a etapa de Verificação também objetiva que o teste seja feito sem gerar retrabalhos, o que não significa que o *tester* não possa retomar as suas decisões feitas na etapa de Adequação e modificá-las para um melhor andamento.
- **Preparação**. Envolve a escolha das estratégias de teste de intrusão a serem efetuadas, bem como a indicação de kits de ferramentas de acordo com os processos anteriores. Os kits de ferramentas são um conjunto de soluções e aplicações que são utilizadas nas diversas etapas do teste. Oferecer diferentes possibilidades neste ponto pode permitir ao *tester* experimentar outras ferramentas que não aquelas que o mesmo utiliza trivialmente. A indicação desses kits é baseada em sugestões e opiniões de profissionais de segurança e pesquisas relacionadas. 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 intrusão 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 intrusão. 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 relaci-

onadas. 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 intrusão. 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 do teste.

Para o processo do teste, de acordo com a estrutura da Tramonto, cada uma das etapas requer uma ou mais entradas e gera uma ou mais saídas. A partir disso, os planos alternativos podem ser melhor determinados, uma vez que a estratégia controla e lista as entradas e saídas. Na etapa de Adequação, os artefatos de saída são determinantes para a construção da etapa seguinte, de Verificação. São gerados os documentos comprobatórios do teste e o levantamento de requisitos estipulados no planejamento realizado na Adequação. Para a etapa de Verificação, diante dessa entrada, a saída é a enumeração e listagem de todos os itens que necessitam ser verificados para que o teste ocorra da forma prevista. Na etapa de Preparação os artefatos de saída são relacionados com aspectos mais técnicos, considerando que são esperadas as estratégias e técnicas cabíveis para a execucação do teste requerido. A etapa de Execução, por sua vez, retrata a maior quantidade de artefatos em sua saída por lidar com o núcleo do teste. Isso também é ressaltado pelo fato de que as vulnerabilidades encontradas podem gerar novos vetores de ataque, e isso mantém a ideia do fluxo contínuo do teste, com frequente reavaliação do que foi testado. Por fim, a etapa de Finalização, mediante entrada de todos os artefatos obtidos nas etapas anteriores, gera de saída os relatórios, tanto para o cliente como para o *tester*.

## 4. Caso de Teste de Intrusão

Para a análise de um teste de intrusão a partir da estratégia de recomendações Tramonto, esta seção apresenta um caso real de teste aplicado a um cenário organizacional. Informações sensíveis e identificáveis estão omitidas, conforme orientação do acordo de

confidencialidade (NDA - *Non-disclosure Agreement*) determinado juntamente ao *tester* responsável pela aplicação deste teste. A apresentação do teste segue nas próximas subseções com a divisão entre: sumário executivo, narrativa das ações de intrusão e análise/recomendações.

### 4.1. Sumário Executivo

A aplicação do teste de intrusão na empresa alvo foi determinada para avaliar sua exposição a um ataque direcionado, considerando a ação de um ataque externo e simulando o comportamento de um atacante. O teste busca identificar se o atacante, de maneira remota, consegue invadir e ultrapassar as defesas da empresa alvo, além de determinar o impacto de violações de segurança relacionadas a confidencialidade dos dados privados da empresa e também a infra-estrutura interna/disponibilidade dos sistemas de informação.

As atividades executadas ao longo do teste foram focadas principalmente na identificação e exploração das deficiências de segurança que poderiam permitir ao atacante remoto obter acesso não autorizado a dados organizacionais. Os ataques foram conduzidos com o nível de acesso que um usuário comum da Internet teria. O processo do teste de intrusão e da avaliação de segurança seguiu com metodologias NIST e OSSTMM, com todos os testes e ações sendo conduzidos em condições controladas.

### 4.2. Narrativa das Ações de Intrusão

Para o início do teste de intrusão, a empresa forneceu o mínimo de informações a respeito da mesma, apenas o nome do domínio. Para não atingir sistemas terceirizados ou que simplesmente não fazem parte da propriedade da empresa, todos os ativos identificados foram submetidos para verificação de propriedade antes que quaisquer ataques fossem realizados.

Como primeira ação no teste, foram identificados os *name servers* do domínio através do *nslookup*. A partir disso, foi realizada uma tentativa de transferência de zona, efetuada com sucesso no *name server* 2 que era vulnerável. Assim, foi possível obter uma lista de hosts e endereços IP associados.

Antes da avaliação dos hosts identificados, a lista desses hosts foi verificada juntamente a empresa alvo para permitir e incluir os IPs no escopo de avaliação. Foram realizadas varreduras nos hosts para enumerar os serviços e determinar a potencial exposição desses serviços a um ataque direcionado. Através de uma combinação de outras técnicas de enumeração de DNS e demais varreduras realizadas na rede, foi possível idealizar a topologia e a infra-estrutura da empresa alvo, conforme apresentado na Figura 2.

Um dos vetores de ataque determinado a partir das varreduras foi a tentativa de intrusão do servidor web Apache na porta 80. Acessando a URL do endereço do servidor, e através da enumeração do sistema procurando diretórios e arquivos comuns, foi identificado o endereço **/portaladmin** que exigia a autenticação. Assim, para passar a autenticação foi efetuado um ataque de força bruta que utilizou uma *wordlist* criada especificamente para o alvo, envolvendo a combinação de palavras e termos relacionados com a empresa (totalizando 14.214 palavras). A senha foi descoberta com sucesso e o acesso a parte administrativa do site permitiu também o acesso ao gerenciador do banco de dados. Após esta etapa do teste, a interface forneceu acesso direto aos dados e a capacidade de extrair uma lista de usuários no sistema com os valores de hash de senha associados.

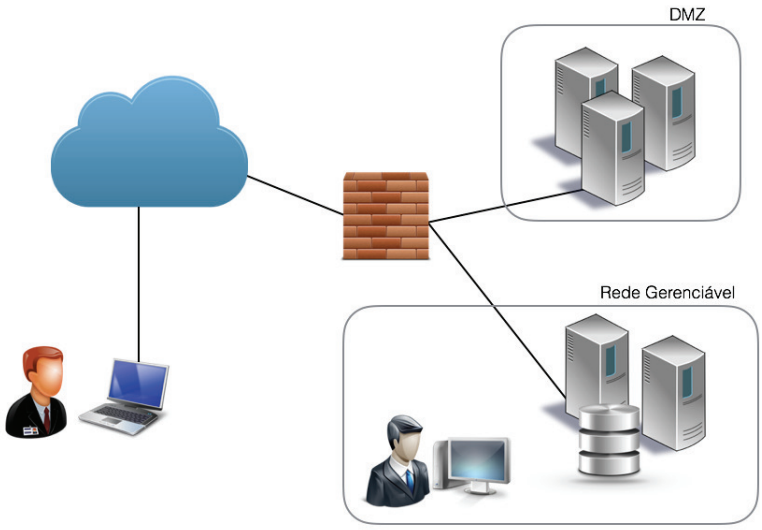


**Figura 2. Topologia reconstituída a partir do teste.**

Considerando o gerenciador de banco de dados vulnerável a injeção de código, a exploração bem-sucedida resultou em acesso de *shell* ao sistema alternativo relacionado ao usuário do servidor web. Através do uso de um exploit público, foi possível obter acesso remoto ao domínio **admin** do servidor web.

Com o acesso remoto obtido, o teste buscou a escalada de privilégios ao nível administrativo. Através de um novo exploit, o sistema mostrou-se vulnerável e foi possível obter as credenciais de administrador. Com a capacidade de obter acesso administrativo completo, uma parte mal-intencionada poderia utilizar este sistema vulnerável para ataques contra a própria empresa e até ataques contra os clientes relacionados.

De posse do acesso administrativo ao sistema, descobriu-se uma seção privada do site da empresa que fornece um serviço específico a um subconjunto de usuários internos. Dessa forma, foi possível estabelecer um caminho para chegar a esses usuários internos. Para tal, a aplicação de uma técnica de engenharia social, como *phishing*, foi a atividade determinada para simular esse serviço específico e manipular os usuários para que interagissem com o mesmo.

Como resultado dessa manipulação e do vetor de ataque, o acesso foi limitado ao nível de um usuário padrão. Para analisar realmente o impacto do ataque, foi necessário buscar o acesso ao nível de administrador de domínio. Em um primeiro momento foi necessário, através das diretivas de grupos no sistema operacional, conseguir acesso como administrador local.

Uma vez como administrador local, foram realizadas tentativas de conexão de sessões utilizando SSH, que foram efetuadas com sucesso. Neste sentido, o perímetro externo da rede da empresa estava totalmente comprometido. Por fim, o acesso como administrador de domínio foi alcançado via acesso ao servidor de posse das credenciais de administrador local.

### 4.3. Resumo dos Resultados

O reconhecimento inicial da rede da empresa resultou na descoberta de um servidor DNS mal configurado que permitia uma transferência de zona DNS. Os resultados listaram uma ordem de hosts específicos que foram alvos do teste. A partir de uma avaliação desses hosts foi possível identificar uma interface administrativa do webserver. Na tentativa de intrusão do webserver, foi criada uma *wordlist* com palavras e termos relacionados ao contexto da empresa alvo, para a realização de um ataque de quebra de senha por meio de força bruta.

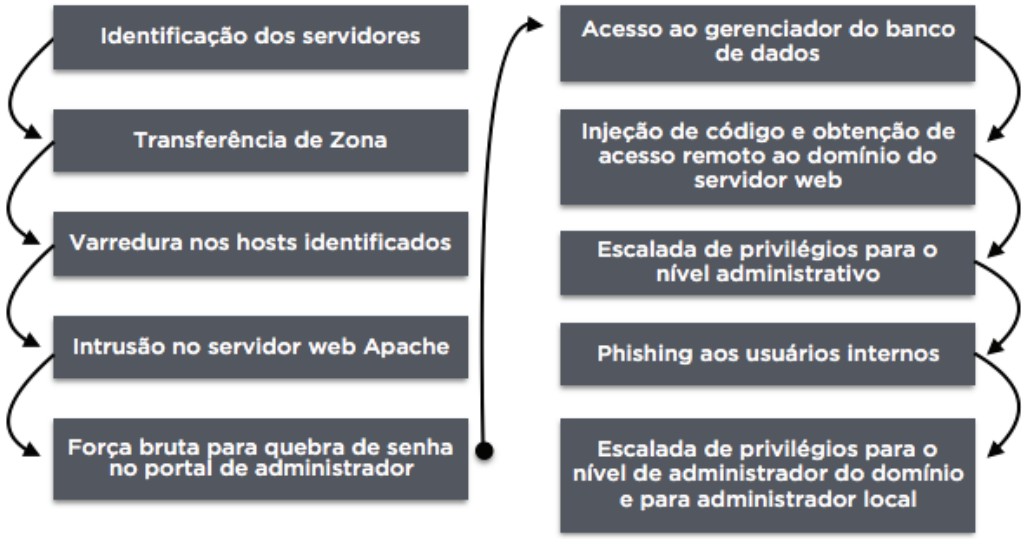


**Figura 3. Resumo do teste de intrusão efetuado.**

Após a obtenção da senha, uma análise da interface administrativa permitiu a identificação de vulnerabilidades de injeção de código remoto. Essa técnica de injeção foi utilizada para obter acesso a um sistema de produção conectado a esse webserver. Após isso, foi escalado o privilégio para um acesso como administrador em virtude da falta de atualizações desse sistema.

Uma vez com o acesso de administrador e dentro do servidor web, foi possível recuperar diversos usuários e senhas e alcançar recursos internos a partir desse acesso, que inicialmente era limitado. Com base nisso, o teste resultou no acesso como administrador local de hosts internos, ao completo comprometimento de um servidor de acesso remoto e também ao controle administrativo completo da infraestrutura do *Active Directory*.

### 4.4. Análises e Principais Recomendações

Baseado no teste de intrusão realizado, as principais análises e recomendações estão voltadas a dois grandes tópicos:

- Adoção de procedimentos padrão: é necessário, naturalmente, estar atento ao uso de credenciais fortes em todo o contexto organizacional. A intrusão realizada na empresa alvo apresentou relação diretada com o uso de senhas fracas e da falta de diferentes ações e níveis de segurança. Além disso, a empresa poderia, como parte do gerenciamento dos seus riscos, manter um controle sobre as avaliações e testes de segurança realizados com o intuito de padronizar e verificar constantemente o estado de segurança do seu ambiente.

- Implementação de recursos adicionais de segurança: estabelecer limites de confiança e acesso na rede interna, evitando efeito cascata quando do comprometimento da rede ou sistema por parte de um atacante. Da mesma forma, a implementação de controles e verificações de mudança nos principais sistemas, permitindo gerenciar erros de configuração e demais problemas direcionados a falta de tratamento correto. Por fim, implementar também uma organização para gerenciar atualizações e patches em geral, de acordo com alguma metodologia específica. Esses fatores são essenciais para atenuar e mitigar potenciais ataques como o que foi simulado pelo teste de intrusão realizado.

## 5. Tramonto x Caso de Teste de Intrusão

Após a compreensão da descrição geral da Tramonto e também do caso de Teste de Intrusão, esta seção confronta os itens vistos com o intuito de verificar a ligação entre ambos e analisar as ações realizadas no teste de acordo com o que a Tramonto propõe.

### 5.1. Organização

A estrutura do teste de intrusão apresentado na seção anterior segue, de forma sucinta, o processo padrão desse tipo de teste: coleta de informações, reconhecimento, exploração e pós-exploração. É importante ressaltar também que o caso cita que seu processo de teste foi baseado em duas metodologias, NIST e OSSTMM. Contudo, não há uma apresentação detalhada do que ocorre ao longo do teste em confronto com as definições fornecidas por essas metodologias.

Considerando a estrutura da Tramonto, as atividades descritas na Seção 4 podem ser divididas da seguinte forma:

- Adequação: Estabelecimento das informações iniciais (apenas o nome do domínio) e preocupação em não atingir sistemas terceirizados ou que simplesmente não fazem parte da propriedade da empresa.
- Verificação: Confirmação dos sistemas que não poderiam ser atingidos e da lista de hosts que foi obtida após o processo de enumeração.
- Preparação: Não foram listadas informações que se encaixam nessa etapa.
- Execução: Processo de enumeração dos *name servers* do domínio através do *nslookup*, transferência de zona e varreduras nos hosts para enumerar os serviços. Além disso, todos as intrusões, vetores de ataque e descobertas realizadas, contando também o ataque de força bruta para descobrir as senhas.
- Finalização: As recomendações e análises feitas para mitigar e adicionar controles a partir do teste efetuado, além do resumo do que foi realizado ao longo do teste.
- Avaliação: Basicamente, a alternância de vetores de ataque conforme os artefatos que iam surgindo com exploração realizada com sucesso. Não seria possível avaliar o impacto real de um ataque no caso de teste proposto se não houvesse uma continuidade de exploração por parte do *tester*.

### 5.2. Limitações

É necessário considerar a omissão de informações como os estabelecimentos contratuais inicias realizados juntamente a empresa alvo. Isso impacta diretamente em uma avaliação não tão completa sob a ótica da Tramonto. De qualquer maneira, o fato da empresa ter

informado apenas o nome do domínio fornece o entendimento essencial para a etapa de Adequação da Tramonto.

Da mesma forma, a falta de uma explicação detalhada sobre as ferramentas utilizadas no teste também limitam o confronto com a Tramonto. Contudo, pode-se considerar isto como uma vantagem da Tramonto em relação ao caso de teste apresentado, uma vez que a estratégia se preocupa em apresentar claramente o kit de ferramentas idealizado para o cenário.

Por mais que o teste tenha seguido uma parte das metodologias NIST e OSSTMM, conforme informado pelo *tester*, há uma falta de padronização para o prosseguimento do fluxo do teste, no qual aparece quando não existe um planejamento prévio do caminho executado no caso em questão. O conflito entre padronizar um teste por completo e permitir uma atuação autônoma do *tester* é um problema no qual a Tramonto, desde sua idealização, procura resolver.

### 5.3. Principais contribuições da Tramonto para o Caso de Teste

Inicialmente, é possível discutir a atuação da Tramonto a partir da apresentação do caso. Os relatórios que a Tramonto propõe como saída final dos testes apresentam um resumo geral de cada detalhe da avaliação de segurança executada: ferramentas, técnicas, soluções e alvos definidos. Além disso, a contribuição de oferecer um relatório com aspecto mais técnico para o *tester* que efetuou o teste de intrusão também é um item a ser considerado de maneira relevante.

Ao início do teste de intrusão realizado, não há determinação dos rumos possíveis que o mesmo pode deter a partir do que é informado pela empresa. Mesmo que isso possa ser refutado em virtude do estabelecimento de um teste do tipo *black-box* (foi fornecido apenas o nome do domínio), seria interessante possibilitar ao *tester* as principais tarefas iniciais a serem realizadas. Como se sabe, uma das principais contribuições da Tramonto é permitir alternativas e sugerir, durante as etapas, atividades devidamente planejadas.

Em determinado momento do teste, mesmo que em caráter de tipo *black-box*, o *tester* ratifica com o responsável da empresa uma lista de hosts que foram identificados. Esse processo de verificação se encaixa diretamente em uma das etapas da Tramonto, e poderia ter sido feito com melhor organização, gerando uma saída para a etapa seguinte e conteúdo direto para o relatório final. O escopo, mesmo que bem definido, poderia ter indicado ao *tester* que alguns procedimentos implementados fossem previamente verificados para tornar o teste melhor constituído. Assim, quando da enumeração e da obtenção de informações, a estratégia permitiria um controle maior do *tester* sobre suas ações.

Não há, no caso apresentado, uma discussão sobre a conformidade do teste e seus aspectos legais. A Tramonto, antes do início do teste, exige a listagem de aspectos contratuais, sendo necessário delimitar em contrato qual o teste será efetuado, os limites que a intrusão não pode ultrapassar ou alcançar (há uma breve afirmação de que sistemas de terceiros não podem ser atingidos no caso), o acordo de confidencialidade e por fim, os custos envolvidos em toda a operação.

Ademais, a Tramonto poderia contribuir também através da explicação e indicação de estratégias e técnicas para o teste de intrusão, atividade que ocorre na primeira etapa da Tramonto. Essas possibilidades são criadas com o intuito de auxiliar o teste, permitindo

que o *tester* possa relatar suas preferências. Contudo, cabe ressaltar que essas estratégias e técnicas, para a Tramonto, são determinadas não só pelos padrões indicados pelas metodologias que constituem a Tramonto, mas também através de testes de intrusão anteriores. É importante considerar, neste ponto, que não há informações de outros testes realizados pelo mesmo *tester* do caso relatado. Com base nisso, seria possível que avaliações de técnicas de segurança a partir da rede interna e de teste de segurança físico fossem consideradas para o caso, já que ao término no mesmo percebeu-se as ações como usuário da rede interna, por exemplo.

## 6. Considerações Finais

A execução de testes de intrusão apresenta particularidades e detalhes que fazem com que esse tipo de teste promova uma série de desafios tanto para quem o executa (*tester*) como para o alvo. Inicialmente, percebe-se que os inúmeros cenários, controles e recursos que podem ser estabelecidos como alvos permitem uma ampla variação nas atividades que são desenvolvidas no teste de intrusão. Além disso, sabe-se que a tentativa de padronização dessas atividades tem sido discutida e encarada como uma problemática nas pesquisas recentes envolvendo a área de testes de segurança. A Tramonto, desde a sua concepção, é uma estratégia de recomendações que procura atender os requisitos necessários para a aplicação de testes de intrusão mas também idealiza, e objetiva, a flexibilidade do *tester*. Esse quesito é um aspecto essencial para a autonomia do teste, ao mesmo tempo em que são fornecidos procedimentos e atividades padrão para os diversos alvos possíveis. No estudo de caso previamente discutido nesse trabalho, alguns traços normatizam o plano do teste de intrusão, mas há uma carência na formatação desse teste. É possível afirmar que esse estudo de caso discute detalhes que comumente são vistos em grande parte dos testes de intrusão: falta de detalhamento técnico dos procedimentos, discussão superficial sobre os vetores de ataque encontrados e novas possibilidades de extração de conhecimento a partir do teste efetuado. A partir da análise deste estudo de caso surgem novas possibilidades para os trabalhos futuros, envolvendo outros casos específicos de cenários pré-determinados que representem as principais vulnerabilidades em algum recurso e/ou ativo. Assim, a Tramonto procura, dentre outros objetivos, tratar as problemáticas relacionadas aos testes de intrusão e seus demais aspectos.

## Referências

Bechtsoudis, A. and Sklavos, N. (2012). Aiming at higher network security through extensive penetration tests. *IEEE Latin America Transactions*, 10(3):1752–1756.

Bishop, M. (2007). About penetration testing. *IEEE Security & Privacy*, 5(6):84–87.

Dalalana Bertoglio, D. and Zorzo, A. F. (2016). Tramonto: Uma estratégia de recomendações para testes de penetração. In *Simpósio Brasileiro de Segurança de Sistemas*, SBSeg, pages 366–379. SBC.

Dalalana Bertoglio, D. and Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, 23(1):1–16.

Fonseca, J., Vieira, M., and Madeira, H. (2010). The web attacker perspective - a field study. In *2010 IEEE 21st International Symposium on Software Reliability Engineering*, pages 299–308.

Geer, D. and Harthorne, J. (2002). Penetration testing: a duet. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, pages 185–195.

Henry, K. M. (2012). *Penetration Testing: Protecting Networks and Systems*. IT Governance Publishing, UK.

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

Igure, V. M. and Williams, R. D. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys Tutorials*, 10(1):6–19.

ISSAF (2006). Information systems security assessment framework.

Jajodia, S., Noel, S., and O'Berry, B. (2005). *Managing Cyber Threats: Issues, Approaches, and Challenges*, chapter Topological Analysis of Network Attack Vulnerability, pages 247–266. Springer US, Boston, MA.

Lam, K., LeBlanc, D., and Smith, B. i. (2004). *Assessing network security*. Redmond, Wash. Microsoft Press, Washington, USA.

Line, M. B., Jaatun, M. G., Cheah, Z. B., Faruk, A. B. M. O., Garnes, H. H., and Wedum, P. (2008). *Ubiquitous Intelligence and Computing: 5th International Conference, UIC 2008, Oslo, Norway, June 23-25, 2008 Proceedings*, chapter Penetration Testing of OPC as Part of Process Control Systems, pages 271–283. Springer Berlin Heidelberg, Berlin, Heidelberg.

Meucci, M., Keary, E., and Cuthbert, D. (2008). *OWASP Testing Guide v.3*. OWASP Foundation.

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

Sarraute, C., Richarte, G., and Lucángeli Obes, J. (2011). An algorithm to find optimal attack paths in nondeterministic scenarios. In *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, AISec '11, pages 71–80, New York, NY, USA. ACM.

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

Whitaker, A. and Newman, D. (2005). *Penetration Testing and Cisco Network Defense*. Cisco Press, Indianapolis, USA.