PENTEST

DESCRIÇÃO DO PRODUTO

1. SERVIÇO PENTEST

Trata-se de um serviço de simulação de ataque cibernético, onde um ou mais hackers éticos vão simular um “agente de ameaça”. As organizações podem definir o Pentest por aquilo que pretendem avaliar. Isso inclui todas as redes, aplicativos, dispositivos e componentes de segurança.

Nosso serviço fornece uma avaliação independente e objetiva da segurança da infraestrutura e software, destacando claramente o risco de segurança dos dados corporativos e dos clientes, tanto de vulnerabilidades externas quanto internas. Somente pela emulação de agentes de ameaças da vida real, como hackers externos e invasores cibernéticos, os verdadeiros riscos técnicos inerentes aos sistemas de TI podem ser identificados e, então, é mais fácil identificar os controles de mitigação necessários que precisam ser implementados.

Os testes de intrusão (Pentesting) vão além da análise de vulnerabilidades, sejam elas automáticas ou manuais. Cenários de ataque vetorial e de várias etapas são aplicados para primeiro encontrar vulnerabilidades. Depois, o foco é colocado naquelas vulnerabilidades mais relevantes encontradas para, finalmente, tentar explorá-las com o objetivo de mergulhar na infraestrutura da empresa. Uma vez que é assim que os ataques direcionados avançados funcionam, o teste de penetração fornece visibilidade real do impacto que um ataque pode causar ao explorar configurações incorretas ou vulnerabilidades nos sistemas.

As capacidades dos nossos especialistas não se limitam à execução de scans de segurança e ferramentas que analisam a configuração e descobrem as vulnerabilidades mais comuns dos elementos que compõem os sistemas de informação. Nossos especialistas em segurança coletam essas informações e as usam para atingir níveis que as ferramentas automatizadas não conseguem. A contribuição diferencial de uma equipe humana é a aplicação de inteligência aos testes executados no sistema alvo. Nesse sentido, o serviço analisa a lógica de negócios dos aplicativos do sistema. Essa análise não pode ser implementada por uma ferramenta automatizada, que tenta analisar o desempenho de aplicativos com base em um conjunto finito de testes. Em determinados casos, os testes a implementar podem exigir um conhecimento exaustivo da aplicação analisada.

2. METODOLOGIA DOS TESTES

Na condução dos nossos trabalhos utilizamos a metodologia da Telefónica Tech, que visa testar Aplicativos da web, APIs/Integrações, aplicativos móveis (Android e/ou iOS) e infraestrutura interna. Esta metodologia se baseia nos principais frameworks reconhecidos mundialmente, como PTES (Penetration Testing Execution Standard) para execução da atividade e NIST para métricas de vulnerabilidade, cuja coleção de

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

conhecimento vem sendo sempre aprimorada e tem sido adotada como as mais eficazes no tratamento e identificação de vulnerabilidades virtuais.

As atividades são conduzidas visando os objetivos:

i. Pré-engajamento

Na fase de pré engajamento são realizados os alinhamentos formais e levantamentos de informações relevantes aos próximos passos através de:

- Kick-off interno;
- Questionário de Assessment;
- Kick-off com cliente;
- Envio do TDI e assinatura.

O escopo dos testes não contempla:

- Testes de negação de serviço;
- Testes de carga ou estresse;
- Testes envolvendo uso de phishing.

ii. Mapeamento do ambiente (Footprinting)

Esta seção define uma abordagem de modelagem de ameaças conforme necessário para a execução correta de um teste de penetração.

Avaliar o alvo e identificar serviços de recepção focam a atenção do PENTESTER nas possibilidades de entrada mais promissoras.

Técnicas:

- Pesquisa Passiva utilizando técnicas de OSINT (Shodan, Whois, Google Dorks, Redes Sociais);
- pesquisa Ativa utilizando ferramentas como: ping, hping e nmap;
- Levantamento de vulnerabilidades do ambiente (Serviços desatualizados, portas abertas, erros de Endpoints etc.).

iii. Exploração

Neste ponto já foram coletados dados suficientes para tentar acessar o alvo, normalmente mediante Phishing, envio de cavalos de troia, links. Uma vez aberto comprometidas com exploits de Dia Zero.

Técnicas:

- Obtenção de acesso “não autorizado”;
- Obtenção de shell;
- Execução de código malicioso remotamente;
- Roubo de credenciais;

- Roubo de dados sensíveis;
- Execução de SQLI;
- Execução de XSS (Refletido e Armazenado);
- Roubo de cookie de sessão;
- Execução de vetor CSRF;
- Execução Clickjacking.

iv. Pós-exploração

Etapa já foi obtido o acesso nível de usuário, PENTESTER procurará obter controle total do sistema.

Técnicas:

- Persistência (Estabilização de Shell);
- Movimentação lateral;
- Roubo de credenciais administrativas;
- Escalação de privilégio (De usuário normal para System ou Root);
- Comando e controle (C2).

v. Resultados

Etapa onde é comunicado ao cliente dos resultados da metodologia, com o detalhamento das vulnerabilidades identificadas, suas respectivas recomendações e ambiente impactado.

3. ENTREGÁVEIS

Elementos	Alcance
Relatório de teste	Relatório detalhado com os resultados e conclusões dos testes realizados pelo serviço
Revisão e recomendações	1 (uma) reunião remota para apresentar os resultados de cada relatório com orientações acionáveis sobre remediação e proteções

4. PORTFÓLIO DE TESTES DE SEGURANÇA

O portfólio do serviço contempla os seguintes tipos de testes:

1. **Aplicativos da web:** testamos aplicativos da web e sua infraestrutura e serviços de suporte. Nossa equipe de pentesting tem vasta experiência com uma ampla variedade de estruturas e tecnologias de aplicativos da web e está alinhada aos padrões de teste de segurança da web OWASP;
2. **APIs/Integrações:** seguindo as diretrizes do OWASP, realizamos pentest de API para descobrir uma ampla gama de fraquezas em APIs expostas como fraquezas de autenticação, ataques de injeção, controles de API ineficazes e muito mais;

3. **Aplicações móveis:** inclui especialistas em testes de aplicativos móveis nas plataformas iOS e Android. Descubra pontos fracos em APIs de aplicativos móveis e descoberta de vulnerabilidades que podem ser exploradas em um dispositivo comprometido;
4. **Infraestrutura rede interna:** testar ativos tecnológicos de forma rápida na infraestrutura do cliente. Nossa equipe de Pentesting realiza uma varredura pontual para que nosso cliente tenha visibilidade do estado atual de suas vulnerabilidades.

A modalidade oferecida neste contexto, é a do tipo Black Box, a depender da necessidade do cliente. Caso o cliente queira modificar a modalidade, segue abaixo as definições de cada tipo para esclarecimento.

- **White Box:** todas as informações do cliente sobre a rede (servidores, banco de dados e sistemas, informações de acesso que estão inclusos no escopo) e análise de código fonte da aplicação, devem ser fornecidas para que possam ser realizados testes extensivos e com mais abrangência. Necessário apoio da equipe interna do cliente para análises profundas e entendimento das aplicações. Este modelo de análise é frequentemente usado em testes de software e engenharia de software, onde o objetivo é identificar problemas específicos e fornecer soluções precisas e detalhadas;
- **Grey Box:** informação do cliente deve ser recebida, como: dados da infraestrutura da rede ou acesso à determinado serviço web. Geralmente é utilizado em Pentest autenticado em aplicações WEB ou API. Esse modelo é frequentemente usado em testes de segurança, onde o objetivo é identificar vulnerabilidades e pontos fracos no sistema ou processo. Esse tipo de análise pode ser considerado um mix de White Box e Black Box, pois o analista de teste recebe alguma informação do cliente, como: dados da infraestrutura da rede ou acesso a determinado serviço web;

Black Box: este modelo de análise é usado o analista não tem conhecimento do sistema ou processo que está sendo analisado. Neste modelo, o analista não tem acesso ao código fonte, documentação ou outras informações relevantes. Este modelo de análise é frequentemente usado em testes de usabilidade, onde o objetivo é avaliar a experiência do usuário e identificar possíveis problemas ou pontos fracos no sistema ou processo. É o tipo de análise mais próximo de um ataque externo, pois nenhuma informação vinda do cliente é fornecida ao analista de teste. Sendo assim, todo e qualquer tipo de informação para a realização de um teste Black Box é adquirida através de técnicas específicas de hacking sobre os serviços disponíveis do alvo, identificando assim as vulnerabilidades e os possíveis danos causados por um ataque mal-intencionado.

5. ESPECIALISTAS DO SERVIÇO

A nossa equipe de *PENTESTERS* faz parte de uma unidade global especializada na realização de testes de cibersegurança para os mais diversos setores (Financeiro, público, saúde, educação, transportes, energia etc.), para diferentes tipos de organizações e em diferentes tipos de projetos de teste de intrusão.

- Profundo conhecimento técnico sobre riscos e tendências de compliance;
- Atualizado diariamente, com acesso à mais recente inteligência de ameaças;
- Colaboradores ativos em fóruns e comunidades especializadas;
- Participantes regulares em conferências ao redor do mundo;
- Mais de 10 anos trabalhando com grandes empresas e multinacionais.

Essa experiência diversificada e o alcance global de nossa equipe de *PENTESTERS* facilitam a adaptação ao contexto e ambiente específico do cliente e a realização de um teste de intrusão abrangente, com base em metodologias comprovadas. Os profissionais de segurança que participam do serviço são especializados nas diversas áreas da segurança da informação e possuem conhecimentos respaldados com diversas certificações.

6. SERVIÇOS ADICIONAIS - RETESTE

O reteste é uma etapa importante nas avaliações de teste de segurança porque valida se as etapas de correção propostas por nossos especialistas foram implementadas pelo cliente.
Nossos especialistas confirmarão se as vulnerabilidades descobertas foram corrigidas ou ao menos mitigadas. Em até 90 dias após o primeiro ciclo de Pentest, nossos especialistas repetem todo o teste inicial para verificar se as alterações, indicadas por nossos especialistas e realizadas pelo cliente foram efetivas, como correção de configurações incorretas ou ainda, se as alterações introduziram novos problemas com novas vulnerabilidades.

7. ENTREGÁVEIS DO SERVIÇO

As notificações serão enviadas por e-mail para as pessoas autorizadas do cliente. O serviço inclui as seguintes entregas:

Notificação de serviço de início e término

- O início do serviço incluindo a data e o calendário das sessões de trabalho;
- O término do serviço uma vez terminado o período de suporte pós-contratação dos últimos testes de segurança, caso não seja acordada entre as partes qualquer renovação ou prorrogação do contrato.

Relatório do Teste

O relatório será entregue por meio seguro, contendo o resultado da avaliação realizada nos ambientes e as vulnerabilidades identificadas durante o teste. Faz parte do relatório apresentar os seguintes conteúdos:

Relatório de Pentesting

O relatório é baseado na apresentação de evidências relacionado com as atividades compreendidas na anatomia do Pentest, apresentando o quadro de riscos (alto, médio e baixo) a serem mitigados pelo cliente, finalizando a entrega do serviço de Pentest. A seguinte estrutura geral está incluída neste tipo de relatório:

- **Descrição:** inclui as motivações dos clientes para realizar o teste (por exemplo, nova vulnerabilidade lançada, mudança de rede / aplicativo, programa VM, após uma quebra ou vazamento, regulamentos de conformidade etc.) e a descrição do tipo de análise;
- **Objetivo:** inclui os objetivos acordados com o cliente que avaliam o exercício de Pentesting e indicará uma medida da postura de segurança do cliente;

- **Escopo:** uma definição do escopo analisado dentro do período contratado avaliando o perímetro da infraestrutura e quaisquer sistemas críticos que possam impactar a segurança do ambiente (rede, sistemas, aplicativos) e o cronograma de testes;
- **Metodologia:** detalhamento da sucessão das ações e ferramentas utilizadas para realizar os testes;
- **Resumo executivo:** resumo do conteúdo do relatório em formato não técnico. Em um nível mais executivo, o processo, os resultados e as recomendações gerais são cobertos para fornecer uma revisão geral do resultado do Pentesting;
- **Conclusões resumidas:** pretende fornecer aos executivos e pessoas um pouco mais técnicas uma melhor compreensão de algumas das descobertas específicas. Os resultados incluem alguns com maior risco (se houver), bem como algumas menções valiosas de controles de segurança positivos descobertos. Cada descoberta listada aqui inclui gravidade, facilidade / tempo para implementar a medida de correção e ganho de segurança associado considerando uma perspectiva baseada em risco;
- **Recomendações gerais:** inclui as sugestões de mitigação que precisam ser tratadas. As recomendações fornecidas servem para abordar as vulnerabilidades atuais. Observe que as tarefas de limpeza pós-engajamento também são mencionadas para ajudar a restaurar o ambiente de destino;
- **Processo de Pentesting:** traz detalhes sobre o andamento dos testes, o método adotado pelo PENTESTER, a descrição dos achados, a demonstração do passo a passo da exploração, bem como as medidas de mitigação;
- **Referências padrão da indústria:** informações sobre as referências (OWASP, OSSTMM, SANS, CVSS, CVE, CAPEC, CWE, MITRE, NIST) e nomenclatura usada.

Nota: O prazo para envio do relatório é de até 5 dias úteis após a conclusão dos testes. Revisão das descobertas e recomendações.
No final do projeto será agendada uma reunião remota com o cliente para apresentação das vulnerabilidades descobertas, juntamente com orientações práticas sobre medidas corretivas a implementar e salvaguardas para o futuro além de mencionarmos se os critérios de sucesso ou a meta e o processo seguido foram alcançados.

Se forem encontradas vulnerabilidades críticas, o cliente será imediatamente notificado e receberá informações com instruções para mitigação do risco, incluindo uma prova de conceito (PoC), caso necessário, sendo opcional.

8. TERMOS E CONDIÇÕES DO SERVIÇO

Duração

Este serviço terá uma duração associada ao cumprimento dos dias de trabalho contratados em função do número e tipo de testes de segurança incluídos no âmbito acordado.
Qualquer renovação deverá ser previamente acordada por ambas as partes, pelo que não haverá renovações automáticas do contrato deste serviço. A Vivo Empresas não será responsável pelos atrasos que possam ocorrer se estes forem devidos a qualquer causa alheia ao seu controle.

Provisão e configuração

Para garantir a melhor prestação do serviço, será necessário que o cliente esteja envolvido neste processo de levantamento de informação. Para uma entrega ideal do serviço, um membro designado da Vivo Empresas entrará em contato com o cliente para organizar a reunião inicial, na qual:

- A Vivo Empresas explicará ao cliente a planificação das atividades a serem realizadas para a correta execução do serviço contratado;
- O cliente fornecerá à Vivo Empresas todas as informações relevantes e necessárias para a prestação do serviço de acordo com o escopo contratado, bem como a identificação dos temas de maior relevância e / ou impacto para o cliente.

Todas as informações solicitadas ao cliente serão registradas no Documento de Requisitos de Informação a ser fornecido pela Vivo Empresas.

Uma vez concluídas as fases de provisão e configuração, o serviço entrará em operação e será prestado de acordo com o escopo definido no contrato do cliente. A Vivo Empresas comunicará ao cliente pelos canais acordados (por exemplo, e-mail) o seguinte:

- A disponibilização do serviço contratado, para proceder a partir desse momento o faturamento dele;
- O calendário das sessões de trabalho de acordo com os requisitos do cliente e o escopo dos testes de segurança contratados.

9. ESCALONAMENTO E SUPORTE

O cliente pode enviar solicitações relacionadas a:

- Dúvidas sobre o escopo do serviço e testes de segurança contratados;
- Agendar sessões de trabalho de testes de segurança;
- Dúvidas e esclarecimentos sobre os resultados fornecidos nas entregas do serviço;
- Mudanças no escopo dos testes de segurança que não impliquem em modificações no contrato.

As solicitações devem ser sempre comunicadas à Vivo Empresas pelo contato autorizado do cliente para tais fins, e pelos canais estabelecidos. Portanto, nenhuma consulta ou incidência que não seja devidamente solicitada será administrada.

Os pontos de contato para essas solicitações são descritos a seguir:

- A equipe de segurança tratará das incidências e solicitações 8x5, dependendo da gravidade, via e-mail e / ou telefone.

10. OBJETIVOS DE NÍVEL DE SERVIÇO (SLOs)

Os principais objetivos de Nível de Serviço são os seguintes:

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

- Assegurar o devido entendimento do escopo do serviço prestado;
- Garantir o acesso às informações de segurança fornecidas pelo serviço.

Os SLOs aqui fornecidos são os seguintes:

SLO	Alcance	Valor Aceitável
Provisão e configuração	Prazo desde que a Vivo Empresas valida e dá o de acordo ao Documento de Requisitos de Provisão fornecido pelo cliente até a primeira data em que a Vivo Empresas indica que está pronta para iniciar a execução dos testes.	< 4 semanas

11. RESPONSABILIDADES

Responsabilidades da Vivo Empresas serão:

- Nomear um representante para atuar como o único contato da Vivo Empresas;
- Dirigir, organizar e gerir a implementação do serviço;
- Participar das reuniões de trabalho desta proposta;
- Manter a equipe do cliente informada sobre as ações e resultados das atividades;
- Assegurar a confidencialidade dos dados fornecidos pelo cliente para o desenvolvimento da atividade;
- Garantir a qualidade do serviço e disponibilizar as instalações e recursos humanos necessários à realização das atividades indicadas;
- Prover instruções sobre como a limpeza pós-teste deve ser realizada e como verificar se os controles de segurança foram restaurados.

As responsabilidades do cliente serão:

- Designar os seus representantes na equipe do projeto, com a disponibilidade necessária para participar de todas as atividades previstas no plano de trabalho;
- Manter total confidencialidade em relação às técnicas, instrumentos e metodologias aplicados pela Vivo Empresas na prestação dos serviços objeto desta proposta;
- Para a condução do teste White box (quando aplicável), o cliente deve fornecer informações sobre a infraestrutura de rede e aplicações, incluindo topologias, endereçamento IP, credenciais de acesso, entre outras;
- Atrasos provocados na contratação de fornecedores e soluções e/ou no fornecimento e/ou implementações, correções etc., provocados por terceiros ou a própria CONTRATANTE não poderão onerar o tempo de contratação, ficando a Vivo Empresas isenta de responsabilização por tais atrasos;
- Mudanças nos sistemas e ferramentas de TI, equipes internas e/ou nas atividades da CONTRATANTE que porventura venham a ocorrer serão objeto de negociação complementar entre as partes, sempre que estas mudanças demandarem carga horária complementar relacionadas com a revisão das atividades e da documentação já elaborados e apresentados à CONTRATANTE.

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

12. LIMITAÇÕES

Não fazem parte do escopo do trabalho aqui proposto:

- Configuração e/ou manipulação de equipamentos, hardware de propriedades da CONTRATANTE, salvo em atividade de contratação, acordada e autorizada para a execução de Pentests;
- Desenvolvimento e correção de código de software, arquiteturas de bancos de dados como entregas de projeto, entre outros; • Responsabilização para a Vivo Empresas em processo de seleção de empresas. A indicação de empresas prestadoras e fornecedores de solução é um serviço de consultoria com vistas facilitação e aconselhamento nos trabalhos a serem executados. A responsabilidade pelo processo de requerimento por proposta para empresas indicadas ou não, seleção e compra de solução ficam reservado, única e exclusivamente ao CONTRATANTE, seus profissionais e seus processos internos;
- Elaboração de Normas específicas de segurança da informação e/ou procedimentos de segurança de qualquer natureza não ligados ao ambiente da proposta;
- Atualizações de sistemas operacionais e correção de vulnerabilidades encontradas durante a realização dos trabalhos;
- Explorações fora do escopo durante o projeto alinhadas previamente no kick-off ou além da metodologia de Pentest;
- Implementação ou manipulação de regras em firewall, IPS, IDS, roteadores, switches e/ou sistemas de informação e segurança de qualquer natureza;
- Análise de segurança lógica em outros sistemas de computadores e redes de comunicação não destacados no escopo;
- O teste será 100% remoto, executado entre a CONTRATANTE e CONTRATADA, logo, não está previsto atuação presencial no ambiente da CONTRATANTE;
- Análises de segurança de aplicações corporativas, suas especificações e suas funcionalidades fora do âmbito do escopo;
- Análise de segurança dos bancos de dados nos aspectos de modelagem e estruturação de seus databases de aplicação;
- Avaliação, fornecimento e implementação de ferramentas que eventualmente sejam recomendadas pela análise de vulnerabilidades, nem de outras ferramentas que venham a ser necessárias;
- Atendimento a demandas que envolvam trabalho fora do horário comercial. Se surgirem necessidades deste tipo, a Vivo Empresas deverá ser formalmente comunicada, a fim de que um plano de trabalho possa ser avaliado e aprovado pelas partes, atendendo assim a legislação trabalhista vigente;
- Qualquer aumento subsequente no número de dias de trabalho que possa impactar o escopo definido. Caso isso aconteça, uma proposta comercial separada será avaliada pela Vivo Empresas e apresentada ao Cliente;
- Viagens fora do local de trabalho, exceto aquelas indicadas no escopo. Qualquer outra viagem deve ser cotada de forma independente;
- O serviço será realizado impreterivelmente em horário comercial, no formato 8x5;
- Os materiais de conscientização ou treinamento não estão incluídos no orçamento e serão orçados de forma independente, se solicitado pelo Cliente;

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

- Atrasos ou falha nas entregas causadas por terceiros ou por inexatidão / falta de informação;
- Qualquer outro tipo de serviço que não esteja descrito neste documento.