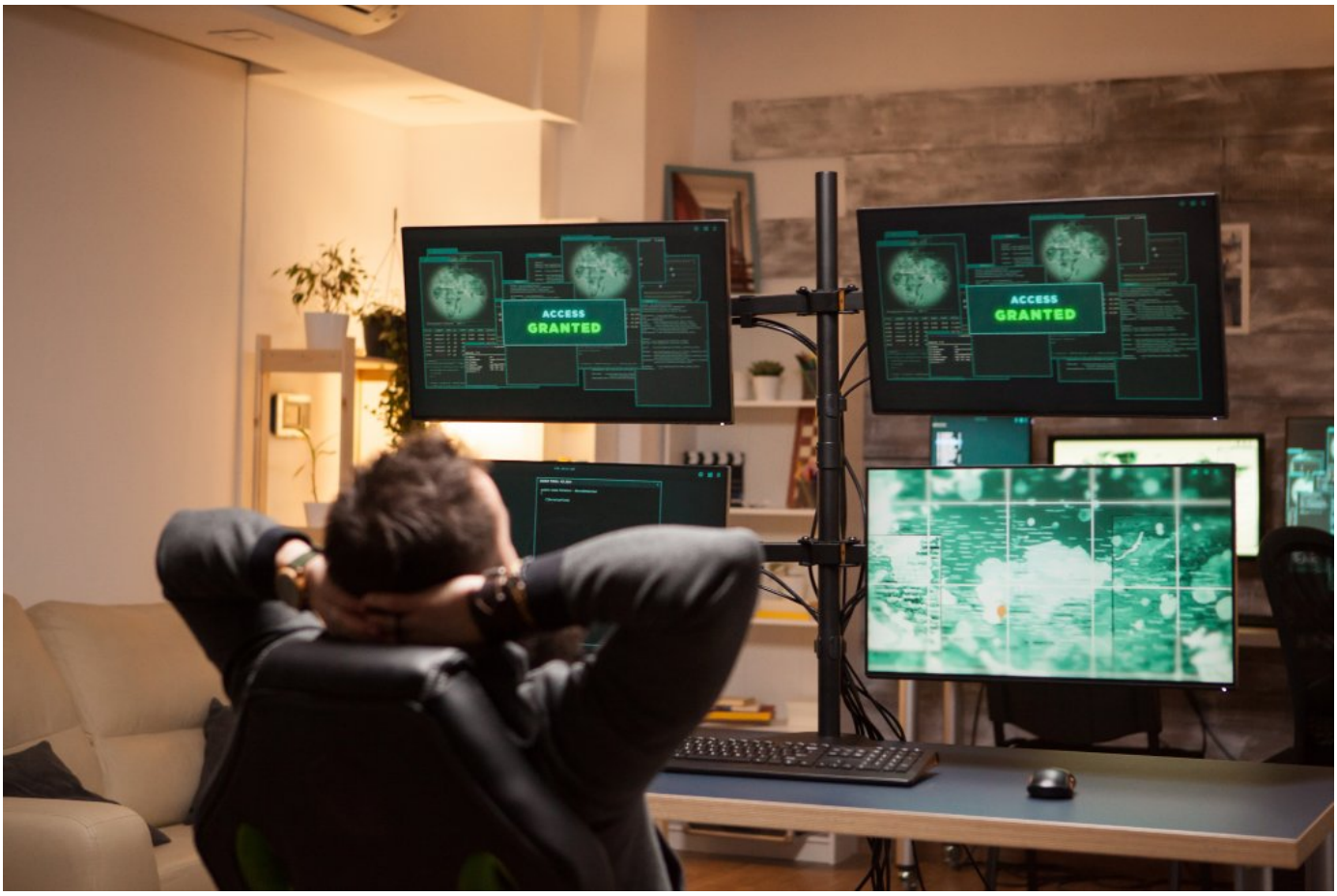
O que é Pentest? Benefícios, tipos e etapas para executá-lo



Pentest — ou Teste de Intrusão — é um método de avaliação que coloca em prática as suas medidas de segurança digitais. E o motivo para isso é simples: atestar que o seu sistema ou rede estão preparados para todo tipo de ataque feito por fontes maliciosas.

Além disso, **é uma forma eficaz de identificar falhas e carências** nos seus métodos e nos próprios ambientes digitais. Uma vez que os ataques digitais se atualizam na mesma proporção que novas soluções são lançadas, o Pentest é fundamental para se proteger.

E, ao longo deste post, vamos explicar tudo o que você precisa saber sobre o que é Pentest e também sobre como aplicar esse eficiente teste de vulnerabilidade!

O que é pentest (Teste de Penetração)?

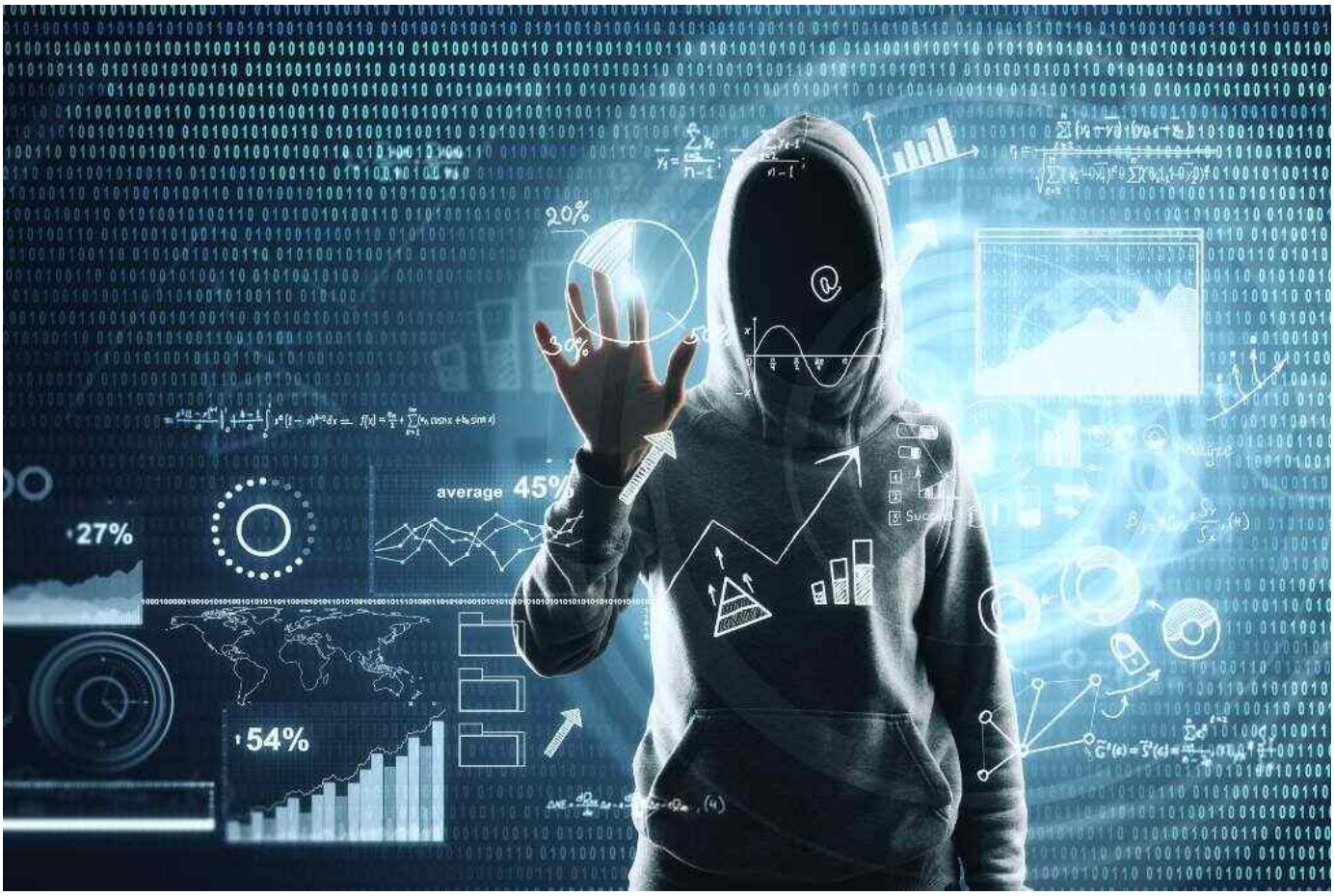
Metade das empresas, ao redor do mundo, utiliza softwares vulneráveis contra cibercriminosos. Ou seja: existe muita brecha a ser usada por fontes maliciosas que podem prejudicar o desenvolvimento da sua organização

Com o Pentest, entretanto, você se previne contra as mais populares e também as mais recentes formas de vulnerabilidade digital. Pois, como adiantamos, esse é um verdadeiro teste de vulnerabilidade (ou **hacking ético**) que visa analisar o grau de segurança dos seus sistemas digitais.

Qual é o objetivo do teste de penetração?

O método não é, exatamente, uma novidade. Empresas que comercializam alarmes (residenciais ou corporativos) passam por isso há anos para ter a certeza de que os seus produtos e serviços realmente funcionam.

Até mesmo policiais e profissionais de saúde, entre outros, passam por treinamentos que promovem melhorias no tempo de resposta contra emergências.



E o teste de intrusão atua da mesma maneira — em um contexto inteiramente on-line.

Por meio de abordagens, métodos e aplicações, o Pentest (que é uma abreviação do termo em inglês Penetration Test) busca encontrar vulnerabilidades em potencial.

Assim, **seus analistas e outros especialistas conseguem desenvolver maneiras de proteger seus dados** e prevenir-se contra futuros ataques.

Qual é a importância e benefícios do pentest?

A importância do Pentest é bem clara: periodicamente, seus sistemas de segurança são testados. E o resultado disso se ramifica em ajustes ou substituição de técnicas e tecnologias que não rendem o esperado. E, paralelamente, em novas oportunidades de proteção digital para a empresa.

Os benefícios dessa prática, contudo, se ampliam e diversificam de outras maneiras. Confira, abaixo, as vantagens em implementar o Teste de Penetração:

- avaliação crítica da sua capacidade de segurança cibernética;
- desenvolvimento escalável de fragilidades e carências no seu sistema de segurança;
- trabalho preventivo (e não apenas corretivo) de medidas de segurança contra cibercriminosos;
- **atualização de novas atitudes e medidas de Segurança da Informação**;
- melhor reputação da sua marca (interna e externamente) com relação à sua segurança de dados.

Você deve imaginar, inclusive, que o Teste de Vulnerabilidade oferece um conforto maior para os seus clientes. Em uma época na qual a transformação digital está ligada à Lei Geral de Proteção de Dados (LGPD), o Pentest traz segurança a todos. Inclusive, de acordo com as exigências da lei vigente.

Quais são as aplicações do teste de intrusão?

Existem diversas maneiras de realizar um Pentest. Abaixo, resgatamos algumas das mais populares, embora existam outras que possam fazer mais sentido para as características do seu negócio. Confira:

- análise de rede e portas;
- identificação de sistemas ou de exploits;
- verificação de serviços on-line (como e-mail e servidores, entre outros);
- avaliação de vulnerabilidades;
- verificação de aplicações e/ou d firewall e ACLs;
- revisões diversas (como políticas de segurança, logs e detecção de intrusos);
- números de série;
- política de privacidade;
- análise de cookies ou bugs.

Vulnerabilidades que podem ser identificadas

Quando se realiza algumas das aplicações acima, é possível se deparar com resultados que ligam o sinal de alerta na empresa. E, a seguir, vamos falar melhor sobre as três vulnerabilidades mais comuns que o Pentest pode apontar.

Cross Site Scripting (XSS)

Por meio de um Teste de Penetração, você consegue avaliar as validações dos parâmetros de entrada e também a resposta do servidor.

Um exemplo disso pode ser observado em fóruns on-line. Sem os filtros adequados, ações maliciosas têm a capacidade de executar tarefas que podem gerar a violação de dados.

Isso aconteceu, um tempo atrás, com o WordPress. Um tema na plataforma estava vulnerável, e isso possibilitou que comentários maliciosos fossem postados;

Se um administrador clicasse neles, ativaria um script que poderia modificar o código ou mesmo configuraçó do site.

Cross Site Request Forgery (CSRF)

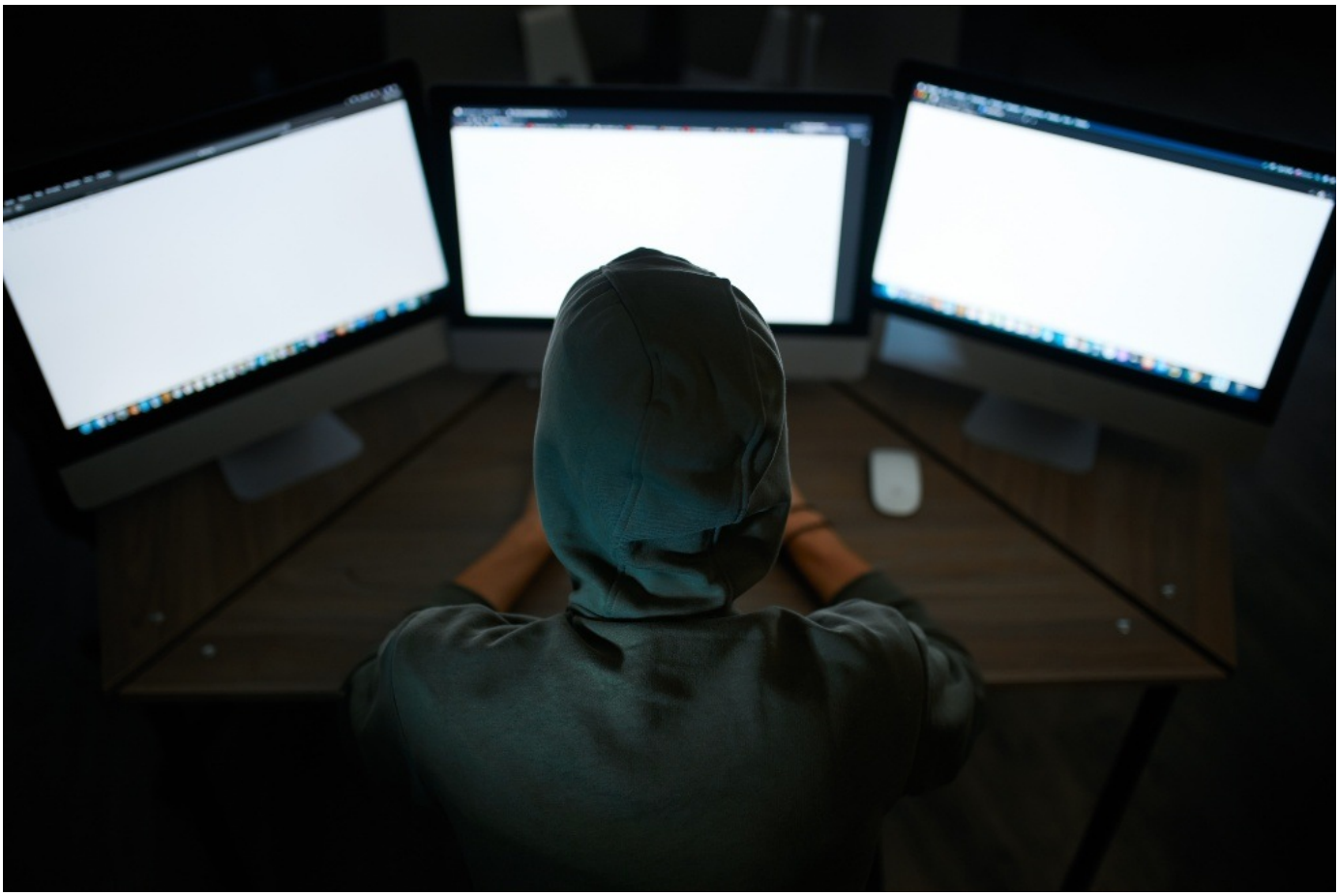
Um tipo de golpe bastante comum: **esse pode ser traduzido a partir do clique em links encaminhados via e-mail**, por exemplo, gerando ações indesejadas pelo usuário.

Normalmente, esse tipo de ação se configura no envio de e-mails falsos, em nome de uma empresa popular, por exemplo, estimulando o clique do usuário. Essa ação direciona-o a um site fraudulento e tem, entre os objetivos, roubar informações privilegiadas, como dados pessoais dos usuários.

Injeção de SQL

O Pentest também pode ser considerado para encontrar uma vulnerabilidade na injeção de SQL. Nesse tipo de ataque, existe a possibilidade de ter a tabela do banco de dados deletada. Ou, ainda, realizar o roubo de senhas registradas nesse local.

Em 2021, por exemplo, 25% das empresas nacionais foram vítimas de crimes virtuais. E a injeção SQL está entre as ações mais populares dos cibercriminosos.



Quais são os tipos de pentest?

Você pode fazer uso do Pentest em diversos serviços e produtos. Falamos, anteriormente, das aplicações desse conjunto de técnicas e abordagens, inclusive.

Mas dá para entender melhor isso a partir do conhecimento das principais modalidades do Teste de Intrusão. Veja quais são!

White Box

Conhecido por alguns especialistas como um Pentest completo, o White Box (ou White Box Penetration Testing) **consiste na realização de uma análise integral**.

Ou seja: investigando toda a infraestrutura da sua rede.

Nele, o pentester (que é o hacker ético, responsável pelo Teste de Penetração) "ataca" a empresa por meio d
todas as suas informações essenciais. Isso inclui:

- topografia;
- senhas;
- IPs;
- logins;
- dados que direta ou indiretamente se relacionam à rede, aos servidores e toda a estrutura digital da organização.

A partir daí, o resultado do Pentest ajuda a direcionar o que deve ser trabalhado para corrigir e implementar e, assim, aumentar a segurança.

Black Box

O Black Box — ou Teste Cego — não oferece os dados, como acontece com o White Box. Aqui, **o Pentest é feito como um elemento surpresa de ataque** para realmente testar as possíveis vulnerabilidades da segurança da empresa.

Gray Box

A "área cinzenta do Pentests é conhecida como Gray Box, e **envolve uma ação híbrida entre o White Bo e o Black Box**.

Para isso, o pentester vai contar com algumas informações, apenas, para direcionar os ataques simulados. A quantidade de dados, entretanto, é baixa.

Só que esse tipo de Pentest é mais indicado porque permite combinações variadas para testar o grau de segurança dos seus sistemas. O que permite, também, ações mais precisas para fortalecer a segurança de dados na sua empresa.

Como funciona e quais são as etapas do pentest?

Independentemente do tipo de Pentest aplicado, é possível seguir um fluxo específico de processos e atividades. E, assim, extrair as melhores análises para tornar os seus ambientes digitais continuamente mais seguros.

Veja, abaixo, cada etapa para um eficiente Teste de Intrusão.

1. Planejamento do teste

O conceito sugere exatamente o que seu nome implica: **é o momento de sentar à mesa e definir os objetivos, os riscos e as potenciais ameaças** que o Pentest vai lidar.

Todo o mapeamento da atividade deve passar pelo planejamento. Assim, você sabe, exatamente, o que procurar e como mensurar os resultados, posteriormente.

2. Escaneamento

Por meio de ferramentas e soluções de escaneamento, o Pentest é colocado em prática. É aqui, inclusive, que soluções tecnológicas são aplicadas para verificar e diagnosticar as possíveis ameaças.

É uma etapa do Pentest de caráter preliminar, portanto, que visa percorrer os processos e sistemas possivelmente vulneráveis aos ataques virtuais.

3. Explorar vulnerabilidades

Nessa etapa do Pentest, a inspeção de aplicações e dados específicos é maior. E isso ajuda a obter uma avaliação melhor do comportamento do sistema diante de ataques.

O resultado disso é ter ainda mais parâmetros e informações para uma tomada de decisão assertiva para combater futuros ataques reais.

E, assim, você tem tudo o que mais importa para ir à etapa seguinte do Pentest: dados confiáveis.

4. Análise dos resultados e risco

A inspeção, aqui, ocorre em tempo real, garantindo que os dados sejam monitorados e os melhores planos d resolução sejam definidos.

Depois do teste de intrusão, as ações cabíveis vão ser desenhadas e implementadas. E, com isso, um ciclo se encerra, mas o planejamento já pode ser considerado novamente.

Afinal de contas, o Pentest não é uma atividade que só vai acontecer uma vez. Pelo contrário: deve ser algo a ser considerado com certa curiosidade.

E muita gente se pergunta, justamente, **a frequência entre um Pentest e outro**.

A verdade é que não existe uma resposta direta. Isso vai variar de acordo com os objetivos e as necessidades da sua empresa. Mas uma periodicidade anual é bem-vinda.

Acima disso, somente se você enxergar oportunidades e carências que devem ser constantemente monitoradas e testadas. E, também, se:

- você pretende investir em novas aplicações ou infraestrutura de rede;
- houve uma aplicação de patches de segurança;
- sua empresa mudou de endereço e uma nova configuração de rede vai ser aplicada.

Por meio dessas informações, é possível ter em mente uma frequência personalizada e eficiente para planejar o próximo Pentest.

Conclusão

A Transformação Digital é um caminho sem volta. Afinal de contas, seus benefícios se acumulam e multiplicam no dia a dia de qualquer empresa.

Entretanto, também existem os pontos de atenção porque muita gente consegue transformar os benefícios da Era Digital em ameaças em potencial.

Isso significa que a sua empresa deve se antecipar. Primeiro, por meio da capacitação de suas equipes, da parceria com empresas especialistas e do investimento em infraestrutura.

Mas também com um olhar atento em oportunidades de mercado para construir um ambiente digital ágil, automatizado e seguro, acima de tudo.

Nesse sentido, a Yssy pode ser uma grande ajuda para o desenvolvimento sustentável da sua marca.

Por meio do **Yssy Cyber Diagnosis**, você pode contar com uma solução que atua em todas as frentes, fases e processos de um sistema de segurança cibernética.

E isso vai diretamente de encontro com o que falamos ao longo de todo o artigo: essa solução se torna uma ferramenta indispensável para o seu Pentest. Tudo ocorre a partir de uma profunda análise de infraestrutura e detecção de eventuais problemas — de maneira preventiva e sem causar prejuízos e danos ao seu negócio.

Inclusive, realizamos o Pentests de três maneiras. Todas elas, já discutidas acima, neste artigo. São elas:

- White Box, um método de Teste de Intrusão no qual temos todas as informações para testar sua segurança com total acesso;
- Black Box, que simulamos ataques sem nenhum conhecimento prévio dos seus dados;
- Gray Box, em que realizamos um Pentest híbrido com características do White Box do Black Box.

Você pode contar conosco, então, para avaliar as melhores estratégias e abordagens de Pentest para o seu negócio. Assim, fica mais fácil ter uma empresa moderna, competitiva e muito bem protegida contra as atuais ameaças e as futuras tendências em crimes virtuais.

Para saber mais a respeito das nossas soluções em Pentest, **acesse a página da Yssy Cyber Diagnosis e entenda em detalhes tudo o que podemos fazer pelo seu negócio**!