

CONSULTA PRÉVIA

N.º 0131- DGCP - 2020

**“Aquisição de testes de penetração por via de plataforma automatizada
através de técnicas de Ethical Hacking”**

CADERNO DE ENCARGOS

CLÁUSULA 1.ª

OBJETO

O presente procedimento tem por objeto a aquisição de testes de penetração por via de plataforma automatizada através de técnicas de Ethical Hacking, de acordo com o Anexo I apenso a este caderno de encargos.

CLÁUSULA 2.ª

PRAZO DE EXECUÇÃO

1. O contrato produz efeitos a partir da data da reunião de Kick-off, que deverá ocorrer no prazo máximo de 10 dias após a assinatura do contrato, e deverá ser executado até 31 de dezembro de 2021.
2. O prazo máximo para o fornecimento da solução proposta, instalação e customização não poderá exceder as 3 semanas.
3. O contrato manter-se-á em vigor até total cumprimento do mesmo, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

CLÁUSULA 3.ª

FORMA E LOCAL DA PRESTAÇÃO DE SERVIÇO

Os serviços a contratar serão executados pela entidade adjudicatária nas instalações da Secretaria-Geral da Economia, sitas na Avenida da República, n.º 79 em Lisboa, ou de forma remota, sempre que a mesma se verifique viável.

CLÁUSULA 4.ª

ESPECIFICAÇÕES TÉCNICAS

A entidade adjudicatária obriga-se à prestação de serviços, de forma a garantir todos os trabalhos especificados no Anexo A, que faz parte integrante do presente caderno de encargos.

CLÁUSULA 5.ª

OBRIGAÇÕES DA ENTIDADE ADJUDICANTE

Constituem obrigações da entidade adjudicante:

1. Pagar, no prazo acordado, a fatura emitida pela entidade adjudicatária, em conformidade com as condições de pagamento estabelecidas no contrato.
2. Monitorizar a prestação do serviço no que respeita às condições acordadas e aplicar as devidas sanções em caso de incumprimento.
3. Designar o gestor de contrato, que terá como função acompanhar permanentemente a execução da presente prestação de serviços.

CLÁUSULA 6.ª

PREÇO BASE

O preço máximo que a Entidade Adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do presente procedimento é de 19.790,00€ (dezanove mil setecentos e noventa euros), ao qual acresce o IVA à taxa legal em vigor.

CLÁUSULA 7.ª

PREÇO CONTRATUAL E CONDIÇÕES DE PAGAMENTO

1. Pela prestação de serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a entidade adjudicante deve pagar à entidade adjudicatária o preço contratual previsto, constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, que não pode ultrapassar o preço base previamente estabelecido.
2. O valor referido no número anterior inclui todos os custos, seguros, encargos e despesas inerentes à prestação de serviços em causa, tais como, encargos decorrentes da utilização de marcas registadas, patentes ou licenças da responsabilidade da entidade adjudicatária.
3. A fatura deverá ser emitida, após a entrega e validação do Full Action Report.
4. A fatura será paga no prazo de 30 dias, após a verificação dos formalismos legais em vigor para o processamento das despesas públicas.
5. A fatura deverá ser emitida em nome da SGE/GAFME, com referência ao número de identificação e ao número de compromisso constantes do contrato, e remetida por meio eletrónico para o endereço de e-mail: Faturacao.DSF@sgeconomia.gov.pt ou via CTT para a Av. da República, nº 79, 1069-218 Lisboa. O envio por outros meios não será considerado. A data de vencimento da fatura será contada a partir da data de receção do mail ou da data de registo de entrada na Secretaria-Geral da Economia.
6. Em caso de discordância por parte da entidade adjudicante, quanto ao valor indicado na fatura, deve esta comunicar à entidade adjudicatária, por escrito, os respetivos fundamentos, ficando a entidade adjudicatária obrigada a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
7. Desde que devidamente emitida e observado o disposto no n.º 1, a fatura será paga através de transferência bancária, após a verificação dos formalismos legais, em vigor, para o processamento das despesas públicas.
8. O atraso no pagamento da fatura confere ao fornecedor o direito de exigir juros de mora, nos termos legais.

CLÁUSULA 8.ª

REVISÃO DE PREÇOS

Não é permitida a revisão dos preços propostos, em circunstância alguma, durante a execução do contrato.

CLÁUSULA 9.ª

DADOS PESSOAIS

1. A entidade adjudicatária obriga-se a efetuar um tratamento lícito, leal e transparente dos dados pessoais.
2. Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, bem como, ser adequados, pertinentes e limitados ao que é necessário, devendo ser apagados, findo o tempo necessário para a finalidade para o qual foram recolhidos, apenas podendo ser comunicados/transmitidos à Direção Superior da entidade adjudicante.

CLÁUSULA 10.ª

GESTOR DO CONTRATO

1. A entidade adjudicante designa como gestor do contrato, o Chefe de Divisão das Estruturas de Comunicações e Segurança, o Eng. João Paulo Camões, que tem a função de acompanhar permanentemente a prestação de serviços objeto da presente prestação de serviços.
2. O gestor do contrato deverá proceder nos termos do disposto no artigo 290.º - A do Código dos Contratos Públicos, de modo a aferir os níveis de desempenho da entidade adjudicatária, a execução financeira, técnica e material do presente contrato.
3. Em caso de desvios, defeitos ou outras anomalias na execução do contrato, deve o gestor do contrato comunicá-los de imediato ao órgão competente, propondo em relatório fundamentado as medidas corretivas que, em cada caso, se revelem adequadas.
4. Antes do início de funções o gestor do contrato irá subscrever a declaração de inexistência de conflitos de interesse, conforme modelo previsto no n.º 7 do artigo 290.º-A do Código dos Contratos Públicos.

CLÁUSULA 11.ª

FISCALIZAÇÃO, CONTROLO E AVALIAÇÃO DO SERVIÇO PRESTADO

A entidade adjudicante tem direito à fiscalização, controlo e avaliação dos serviços prestados, para poder aferir se os mesmos estão a ser prestados de acordo com o contrato a celebrar.

CLÁUSULA 12.ª

SANÇÕES CONTRATUAIS

1. Pelo incumprimento das obrigações previstas no presente caderno de encargos, a entidade adjudicante pode exigir à entidade adjudicatária o pagamento de uma sanção pecuniária, de montante a fixar em função da gravidade do incumprimento e cujo valor poderá ser até 20% do preço contratual.
2. Na determinação da gravidade do incumprimento, a entidade adjudicante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa da entidade adjudicatária e as consequências do incumprimento.
3. Os incumprimentos deverão ser denunciados por escrito no prazo máximo de 48 horas a contar do seu conhecimento, e dados a conhecer à entidade adjudicatária por fax, e-mail ou através de correio em carta registada com aviso de receção.

CLÁUSULA 13.ª

OUTROS ENCARGOS

Todas as despesas derivadas da prestação das cauções e seguros se a eles houver lugar, são da responsabilidade da entidade adjudicatária.

CLÁUSULA 14.ª

CAUÇÃO

Não há lugar à prestação de caução, nos termos do nº 2 do artigo 88º do CCP.

CLÁUSULA 15.ª

PATENTES, LICENÇAS E MARCAS REGISTRADAS

1. A entidade adjudicatária garante que respeita as normas relativas à propriedade intelectual e industrial, designadamente, direitos de autor, licenças, patentes e marcas registadas, relacionadas com o hardware, software e documentação técnica que utilizará no desenvolvimento da sua atividade.
2. A entidade adjudicante, não assume qualquer responsabilidade por infrações cometidas pela entidade adjudicatária, no âmbito da execução do contrato a celebrar, relativamente a direitos de propriedade intelectual e industrial, relacionados com o

hardware, software e documentação técnica por este utilizado, cujos direitos e autorizações legais para o efeito devam por ele ser assegurados.

CLÁUSULA 16.ª

DEVER DE SIGILO

A entidade adjudicatária obriga-se a manter sigilo, inclusive após a cessação do contrato, sobre toda a informação de que venha a tomar conhecimento, por via direta ou indireta, no âmbito da prestação de serviço em causa e vincula-se a não utilizar essa informação para outros fins que não aqueles destinados direta e exclusivamente à execução do contrato.

CLÁUSULA 17.ª

CONTAGEM DOS PRAZOS

Os prazos previstos no contrato são contínuos correndo em sábados, domingos e dias feriados.

CLÁUSULA 18.ª

NOTIFICAÇÕES E COMUNICAÇÕES

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma das partes, indicados no contrato a celebrar.
2. Qualquer alteração dos elementos de contacto deve ser comunicada à outra parte.

CLÁUSULA 19.ª

FORO COMPETENTE

Para resolução de todos os litígios decorrentes do contrato a celebrar fica estipulada a competência do Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

CLÁUSULA 20.ª

LEGISLAÇÃO APLICÁVEL

Em tudo o que for omissivo e que suscite dúvidas no presente contrato, reger-se-á pela lei geral aplicável aos contratos administrativos, bem como ao regime jurídico do Código dos Contratos Públicos e demais legislação aplicável em razão da matéria.

ANEXO A

Especificações Técnicas

I. Serviços a adquirir

A solução que se pretende adquirir deve ser uma ferramenta automatizada de testes de penetração com gestão de vulnerabilidades que imitará o comportamento, as operações e as técnicas utilizadas por um atacante, deve executar cenários de testes de penetração e permitir explorar as vulnerabilidades através de explorações baseadas em automatismos sem existir interferência na operação da rede e na continuidade do serviço. Como resultado dos testes a realizar deverão ser produzidos relatórios detalhados de acordo com o plano de cenários de testes e as configurações realizadas, assim como deverão ser indicadas as ações corretivas e de remediação a realizar.

Como as infraestruturas tecnológicas podem ter falhas de segurança, vulnerabilidades, resultantes de erros de desenho e de desenvolvimento de hardware e de software, adicionalmente, as configurações incorretas e erros de codificação podem permitir o acesso indevido a sistemas.

Atendendo a estas vulnerabilidades, para se diminuir a superfície de ataques de cibersegurança, devem se verificar constantemente os controlos e meios de proteção de ameaças e incidentes. Com recurso à solução que se pretende adquirir será possível garantir os objetivos desse pressuposto.

A solução deverá ainda permitir explorar e mapear a gama de IP's dentro do intervalo definido pela SGE na infraestrutura tecnológica, enumerando os sistemas, equipamentos e dispositivos que sejam identificados, vulnerabilidades em software (sistema operativo, aplicações, serviços) e hardware.

A solução deverá também de obedecer às seguintes especificações técnicas detalhadas:

- O pentesting será realizado com ligação via ethernet sem quaisquer credenciais e acessos privilegiados, como um hacker faria (sendo necessário garantir a atribuição de um IP);
- A solução tem de ser (Plug & Play), apenas necessita de estar instalada numa máquina que cumpra os requisitos mínimos de hardware/software;
- Deverá ser de uma solução "Agentless", não realizando qualquer deployment de agentes na infraestrutura;

- Deverão ser realizadas explorações reais sem interrupções no serviço;
- As etapas do vetor de ataque deverão ser apresentadas em detalhe para documentar a vulnerabilidade e/ou mitigar o ataque;
- O técnico de segurança deverá poder controlar o nível de intrusão do ataque e selecionar uma fragilidade ou aplicação específica a analisar;
- A solução deverá poder executar a descoberta e enumeração automáticas de servidores e aplicações web. A descoberta deve ser realizada automaticamente em todos os hosts ativos definidos no intervalo de IP do cenário de teste;
- A identificação e consulta automatizadas a Domain Controllers da Active Directory, em ambientes com Active Directory, a solução deve emular o comportamento do invasor, identificando automaticamente o(s) controlador(es) de domínio e realizando consultas LDAP e ataques de retransmissão de credenciais (incluindo criação de utilizador administrador de domínio);
- O acesso direto a toda a WIKI, com instruções de remediação e mitigação, este recurso em simultâneo com o suporte multi-utilizador o acesso completo à lista de vulnerabilidades, aos relatórios e à Wiki tem de ser garantido;
- A solução deverá permitir a exploração do cenário "pior dos dois mundos", que é um vetor de ataque muito sofisticado e que permite que os invasores obtenham a execução remota de código como SYSTEM em computadores Windows nos domínios pertencentes à Active Directory, sem credenciais. Esta exploração deverá utilizar uma combinação de técnicas de delegação de NTLM e de delegação Kerberos para alcançar esse objetivo;
- A solução automática deverá fornecer um mecanismo para garantir que todos os resíduos de tarefas sejam limpos no final do PenTest;
- Deverá ser elaborado um resumo claro das etapas críticas de correção a serem executadas com base nas prioridades voltadas para ameaças que são relevantes para a rede organizacional e seus ativos críticos;
- A solução deverá exibir a hierarquia de ação completa nos relatórios e permitir que a visualização das etapas da ação seja realizada de maneira hierárquica, permitindo que utilizadores tenham melhor visibilidade sobre o fluxo de ataques em ações complexas, como execução remota de código; Para além disso, nas etapas de ação executadas em vários hosts (como nas etapas de descoberta e enumeração) também deverão ser exibidas agrupadas, para facilitar a visualização e análise das etapas de ataque subsequentes.

A solução deverá dispor dos seguintes modos de operação e funcionalidades:

- Scan e Avaliação das Vulnerabilidades:
 - O sistema realiza scan e análise de vulnerabilidades, fornecendo relatórios priorizados de scan de vulnerabilidades com base nos níveis de gravidade padrão da indústria.
- Teste de Penetração (Black-Box Basic):
 - Pen-testing com configurações padrões (basta definir intervalos de IP's e duração).
- Teste de penetração (Black-Box Advanced):
 - Pen-testing com recursos avançados e configurações adicionais permitindo, na exploração de vulnerabilidades "críticas" solicitar a aprovação do técnico de segurança para a execução das mesmas.
- Teste de Penetração (Gray Box, Advanced Targeted Start-Point/End-Goal):
 - Permite a definição granular de cenários avançados de pentesting com definição de ponto inicial e definição de serviço/dados de meta final (por exemplo, comece com credenciais/sistema de utilizador da área de Recursos Humanos, verifique se é possível obter acesso a dados financeiros críticos (cartão de crédito/outras informações confidenciais).
- Tarefas de ação única:
 - Permite a criação de tarefas com âmbito de teste específicos para identificar metas de ação "a la carte", não um "pentesting" completo.

Operações a ser realizadas pela solução:

- Criação de cenários de testes de "pentesting";
- Representação visual dos vetores de ataque;
- Visibilidade gradual sobre as explorações atingidas;
- Varrimento à rede;
- Enumeração dos sistemas/equipamentos/dispositivos;
- Verificação e categorização das vulnerabilidades;
- Exploração e mapeamento;
- Exploração dos endpoints;
- Movimentos laterais;
- Descoberta de contas/credenciais de utilizador;
- Ataques Man-in-the-Middle;
- Escalonamento de contas privilegiadas;
- Ataque de "brute force" a aplicações/serviços sem afetar o processamento local;

- Bypass de segmentos de rede;
- Definição de cenários de teste;
- Identificação de dispositivos não autorizados;
- Condições what-if do teste de penetração;
- Extração de dados sensíveis;
- Exploração proveniente do fator humano;
- Detecção de serviços mal configurados;
- Relatórios de vulnerabilidades existentes com priorização e nível de severidade;
- Lista de ações de remediação priorizadas.

De modo a garantir o bom funcionamento da solução, nomeadamente na componente de “Ethical Hacking” é necessário que o técnico que irá configurar e conduzir o Pentest Automatizado tenha o certificado da PCYSYS de Profissional de “Penetration Power of Knowledge Training”.

II. Entregáveis

Deverão ser entregues 3 tipos de reports:

- Executive Report (em pdf);
- Summary Report (em pdf);
- Full Action Report em pdf ou csv.