Estudo Técnico Preliminar 54/2023

1. Informações Básicas

Número do processo: 03/CCA-BR/2023

2. Descrição da necessidade

A Divisão de Operações (DO) do Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER) tem a necessidade de capacitar seus militares para desempenharem as atividades associadas à Defesa Cibernética, sejam de Proteção, Exploração ou Ataque Cibernético. Os cursos da Offensive Security são internacionalmente reconhecidos e têm as características buscadas pelo Comando da Aeronáutica (COMAER). Em particular, a necessidade identificada para o ano de 2023 foi dos cursos PEN-200, PEN-300, WEB-300.

3. Área requisitante

Área Requisitante	Responsável
Divisão de Operações (DO)	Júlio César Moura de Oliveira - MJ QOENG CMP

4. Descrição dos Requisitos da Contratação

REQUISITOS GERAIS

4.1. Disponibilizar todos os materiais do curso em língua inglesa ou língua portuguesa (Português-Brasil).

4.2. O curso deverá ser realizado na modalidade EAD (Ensino à Distância) por meio de aulas pré-gravadas.

4.3. O voucher terá validade de 12 meses a contar do aceite da nota de empenho.

4.4. A ativação do voucher será feita pela CONTRATANTE.

4.5. Garantir aos militares inscritos o acesso perpétuo às aulas pré-gravadas, por meio da INTERNET, 07 (sete) dias por semana, 24 (vinte e quatro) horas por dia, excluindo os laboratórios após o vencimento do prazo pós-ativação, o qual é de 90 dias.

4.6. Qualquer indisponibilidade de acesso ao curso ou aos laboratórios, referentes a uma licença ativa, que seja causado por falha na infraestrutura da FABRICANTE deverá ter a reposição do tempo de serviço indisponível, sendo este a diferença de tempo entre a notificação da CONTRATANTE sobre a indisponibilidade e a notificação de resolução dela.

4.7. Disponibilizar suporte completo ao ambiente virtual de aprendizagem e tutoria durante todo o período de acesso.

REQUISITOS DE CERTIFICAÇÃO

4.8. Deverá ser fornecido certificado de conclusão do curso, emitido pela CONTRATADA aos militares que concluírem o curso com aproveitamento.

4.9. Deverá ser fornecido certificação oficial da Offensive Security para os militares que forem aprovados na prova de certificação.

REQUISITOS DE NATUREZA DOS SERVIÇOS

4.10. Os serviços pretendidos não possuem natureza continuada, devendo permitir a ativação da licença dos cursos durante período de acesso de 12 meses a contar do aceite da nota de empenho.

5. Levantamento de Mercado

Após pesquisa de mercado, foi constatado que os Cursos da *Offensive Security* são uma referência internacional em treinamento na área de testes de penetração, tendo em vista a profundidade na abordagem do conteúdo, tanto na teoria quanto nos exercícios de laboratório, e possui uma das certificações mais bem avaliadas, pois busca avaliar o aprendizado de forma prática. Eles Provêm uma visão geral sobre o cenário do trabalho de tratamento de incidentes, incluindo os serviços prestados pelo CSIRT, as ameaças dos invasores e a natureza das atividades de respostas a incidentes, buscando identificar e mitigar falhas de segurança.

Sendo assim, após análise das ementas e metodologias dos treinamentos supramencionados, concluiu-se que Cursos da Offensive Security se adequam à necessidade do COMAER.

A empresa Acadi-Ti Consultoria em Informática LTDA é representante autorizada da Offensive Security para ofertas dos cursos descritos como objeto dessa contratação. É considerada uma entidade referência em treinamentos na área de Segurança da Informação, possuindo premiações como a de Melhor Centro de Treinamento EC-Council, empresa considerada como referência internacional em Segurança da Informação.

A Acadi-Ti possui em seus quadros instrutores com certificações internacionalmente reconhecidas (como CEH, OSCP, DCPT) e com experiência de mercado em diversos projetos envolvendo testes de segurança. A instituição possui ainda como clientes empresas privadas como a Netshoes e Nestlé, além de outras instituições públicas como o Centro de Defesa Cibernética do Exército e a Marinha do Brasil.

6. Descrição da solução como um todo

A contratação será de três cursos da formação Offensive Security, na modalidade EAD (Ensino à Distânica) a ser realizado na plataforma da empresa, com aulas pré-gravadas, sendo eles descritos abaixo.

6.1. PEN-200 – O treinamento é realizado em ritmo individualizado. Introduz ferramentas e técnicas de testes de penetração por meio de experências hands-on. Treina não apenas as habilidades, mas também a mentalidade necessária para se tornar um pentester bem-sucedido.

EMENTA:

1. Penetration Testing with Kali Linux: Informações gerais do curso

2. Conhecendo o Kali Linux

2.1. Princípios básicos de linha de comando

2.2. Ferramentas práticas

2.3. Bash Scripting

2.4. Coleta passiva de informações

2.5. Coleta ativa de informações

2.6. Escaneamento de vulnerabilidade

2.7. Ataques de aplicações *web*

3. Introdução a *Buffer Overflow*

4. Buffer Overflows em Windows

5. Buffer Overflows em Linux

6. Ataques *client-side*

7. Localizando *Exploits* Públicas

8. Reparando *Exploits*

9. Transferências de arquivo

10. Evasão de antivírus

11. Escalonamento de privilégios

12. Ataques de senha

13. Redirecionamento de Portas e Tunelamentos

14. Ataques a *Active Directory*

15. O *Framework* Metasploit

16. Agente *Empire* do Powershell

17. Juntando as peças: análise do teste de penetração

18. Explorando arduamente os laboratórios

Ao final do curso e dos laboratórios online do curso PEN-200, o participante estará apto a realizar o exame certificatório para o OSCP, que conta com duas etapas. A primeira etapa é um exame prático vigiado de 23 horas e 45 min, enquanto a segunda etapa é direcionada para a produção de um relatório profissional sobre cada passo da exploração durante o exame, o qual será validado pela equipe de Pentesters da Offensive Security, a ser entregue no período de 24 horas.

6.2. PEN-300 – É o curso avançado de teste de penetração. Baseia-se nos conhecimentos e técnicas ensinados no curso PEN-200, capacitando os alunos a realizar testes avançados de penetração contra organizações maduras com uma função de segurança estabelecida.

EMENTA:

1. Evasion Techniques and Breaching Defenses: Informações gerais do curso

2. Sistema Operacional e Teoria de Programação

3. Execução de código *client-side* com Microsoft Office

4. Execução de código *client-side* com *scripts* executados em *host* Windows

5. Injeção e migração de processos

6. Introdução à evasão de antivírus

7. Evasão avançada de antivírus

8. *Whitelisting* de aplicações

9. *Bypassing* de filtros de rede

10. Pós-exploração em Linux

11. Fuga de *KIOSKs*

12. Credenciais Windows

13. Movimentação lateral em sistemas Windows

14. Movimentação lateral em sistemas Linux

15. Ataques em Microsoft SQL

16. Exploração de *Active Directory*

17. Juntando as peças

18. Tentando arduamente: Os laboratórios

Ao final do curso e dos laboratórios online do curso PEN-300, o participante estará apto a realizar o exame certificatório para o OSEP, que conta com duas etapas. A primeira etapa é um exame prático vigiado de 47 horas e 45 min, enquanto a segunda etapa é direcionada para a produção de um relatório profissional sobre cada passo da exploração durante o exame, o qual será validado pela equipe de Pentesters da Offensive Security, a ser entregue no período de 24 horas.

6.3. WEB-300 – O treinamento foca em métodos de pentest do tipo caixa branca em aplicações WEB. A maior parte da ementa será gasta analisando código-fonte, descompilando Java, realizando debug de DLL's, manipulando requisições, e mais, usando ferramentas como Burp Suite, dnSpy, JD-GUI, Visual Studio e editores de texto confiáveis.

EMENTA:

1. Introdução

2. Ferramentas e metodologias

3. Bypass de autenticação e RCE no *Atutor*

4. Atutor LMS type juggling vulnerability

5. Injeção SQL para RCE em gerenciador de aplicações ManageEngine por meio de AMUserResourcesSyncServlet

6. Vulnerabilidade de injeção arbitrária de JavaScript através do *plugin* Bassmaster de NodeJS

7. RCE através de vulnerabilidade de deserialização de *cookie* do DotNetNuke

8. *Bypass* de autenticação ERPNext e injeção de *template server side*

9. *Bypass* de autenticação openCRX e execução remota de código

10. XSS no openITCOCKPIT e injeção de comando de sistema operacional em testes caixa preta

11. *Bypass* de autenticação do Concord para RCE

12. Falsificação de requisição server-side

13. Poluição de protótipo do Guacamole Lite

14. Conclusão

Ao final do curso e dos laboratórios online do curso WEB-300, o participante estará apto a realizar o exame certificatório para o OSWE, que conta com duas etapas. A primeira etapa é um exame prático vigiado de 47 horas e 45 min, enquanto a segunda etapa é direcionada para a produção de um relatório profissional sobre cada passo da exploração durante o exame, o qual será validado pela equipe de Pentesters da Offensive Security, a ser entregue no período de 24 horas.

O prazo de ativação de todos os cursos será de 12 meses a contar do aceite da nota de emprenho.

Esta Equipe de Planejamento sugere que a contratação seja por inexigibilidade de licitação motivada no art. 74, inciso III, alínea ' f ', da Lei 14.133/2020.

7. Estimativa das Quantidades a serem Contratadas

Id.	Descrição do Bem ou Serviço	CATSER	QTD	Métrica
1	Curso OffSec **PEN-200** - Penetration Testing with Kali Linux	3840	04	un
2	Curso OffSec **PEN-300** - Advanced Evasion Techniques and Breaching Defenses	3840	02	un
3	Curso OffSec **WEB-300** - Advanced Web Attacks and Exploitation	3840	01	un

JUSTIFICATIVA

O quantitativo descrito é estimado com base na quantidade de militares que atuam em atividades relacionadas a Proteção, Exploração ou Ataque Cibernético, que ainda não possuem o treinamento objeto deste processo, seguindo a trilha de capacitação do NuCDCAER para os militares do setor que desempenham as atividades associadas.

8. Estimativa do Valor da Contratação

Valor (R$): 66.290,49

O valor estimado para a contratação é de R$ 66.290,49 (Sessenta e seis mil**,** duzentos e noventa reais e quarenta e nove centavos).

9. Justificativa para o Parcelamento ou não da Solução

Considerando a natureza dos serviços a serem prestados, entende-se que não é viável o parcelamento da solução, por se tratar da contratação de uma empresa de notória especialização para o fornecimento do curso almejado. Para embasar esta decisão, foram considerados a viabilidade técnica e econômica, as eventuais perdas de escala e o aproveitamento do mercado e ampliação da competitividade.

10. Contratações Correlatas e/ou Interdependentes

Não há contratações que guardam relação/afinidade com o objeto da compra/contratação pretendida.

11. Alinhamento entre a Contratação e o Planejamento

Como definido no Art. 1º do Regimento Interno do Centro de Computação da Aeronáutica de Brasília: O Centro de Computação da Aeronáutica de Brasília (CCA-BR), Organização do Comando da Aeronáutica (COMAER), tem por finalidade gerenciar os sistemas e serviços de Tecnologia da Informação (TI), sob sua responsabilidade, a fim de manter a disponibilidade, a confiabilidade e a integridade das informações.

A execução dessa iniciativa pelo CCA-BR possui alinhamento com o Plano Diretor de Tecnologia da Informação da Aeronáutica (PCA 11-320 – PDTIC 23-26) atendendo por meio de projetos e ações de capacitação desenvolvidos pelo CCA, conforme apresentado a seguir:

ALINHAMENTO AO PDTIC (23-26) - Anexo B			
PROTIFÓLIO	**PROGRAMA**	**EMPREENDIMENTO**	**ATIVIDADE**
DEFESA CIBERNÉTICA	DEFESA ATIVA	SEGURANÇA CIBERNÉTICA	CAPACITAR MILITARES PARA DESEMPENHO DAS ATIVIDADES DE DEFESA CIBERNÉTICA.

ALINHAMENTO AO PTA-CCABR (2023)			
ITEM	CÓDIGO	PERÍODO	TAREFA
7.10	23SCO012	2023	Capacitar os militares do CCA-BR e do NuCDCAER para as atividades técnicas de TIC.

12. Benefícios a serem alcançados com a contratação

12.1. Continuidade da capacitação de recursos humanos envolvidos nesta contratação, sem a interrupção dos serviços em andamento.

12.2. Garantir o aprimoramento e a boa utilização dos recursos computacionais no que tange à aplicação de boas práticas nos testes de segurança.

12.3. Cumprimento das medidas previstas no Plano Diretor de Tecnologia da Informação e Comunicação da Aeronáutica (PDTIC) do COMAER.

13. Providências a serem Adotadas

Não há providências a serem adotadas pela administração previamente.

14. Possíveis Impactos Ambientais

Em conformidade com o art. 11, inciso IV, da Lei 14.133/2020 a CONTRATADA deve seguir as normas ambientais vigentes através do Guia Nacional de Contratações Sustentável, 5ª edição de agosto de 2022, bem como as normas porventura criadas/alteradas durante o período de vigência do contrato, bem como o eventual ônus e adaptações a normas ambientais futuras.

15. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

15.1. Justificativa da Viabilidade

A partir dos presentes estudos preliminares e em atendimento ao art.6°, inciso XX, da Lei 14.133/2020 a Equipe de Planejamento declara a contratação pretendida viável, devendo prosseguir com a tramitação prevista.

16. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

JÚLIO CÉSAR MOURA DE OLIVEIRA - MJ QOENG CMP

Integrante Requisitante

LOURENÇO BRUNO DA CUNHA NETO - 1T QOENG CMP

Integrante Técnico

VANESSA SMARZARO MAIA DAS CHAGAS - CAP QOINT NTE

Integrante Administrativo

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO

Documento:	ETP DIGITAL
Data/Hora de Criação:	19/07/2023 14:29:37
Páginas do Documento:	7
Páginas Totais (Doc. + Ass.)	8
Hash MD5:	ab3ff5a05fd8bd3929949715aac826c5
Verificação de Autenticidade:	https://autenticidade-documento.sti.fab.mil.br/assinatura

Este documento foi assinado e conferido eletronicamente com fundamento no artigo 6º, do Decreto nº 8.539 de 08/10/2015 da Presidência da República pelos assinantes abaixo:

Assinado via ASSINATURA CADASTRAL por Major JÚLIO CÉSAR MOURA DE OLIVEIRA no dia 31/07/2023 às 15:00:16 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por 1º Ten LOURENÇO BRUNO DA CUNHA NETO no dia 01/08/2023 às 10:51:33 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Cap VANESSA SMARZARO CHAGAS DE TOLEDO no dia 01/08/2023 às 15:42:53 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Cap RODRIGO MARTIN MARQUES LOUZADA no dia 04/08/2023 às 10:22:16 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por 1º Ten MARCO AURÉLIO LEITE DE PAULA no dia 07/08/2023 às 09:59:44 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Cel WAGNER OLIVEIRA DA SILVA no dia 07/08/2023 às 11: 00:59 no horário oficial de Brasília.

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO