worldskills Portugal | CENTRO 2027

47.º CAMPEONATO NACIONAL DAS PROFISSÕES

PROVA REGIONAL

Fase 1

Cyber Security

Profissão 54

CLUSTER

Gestão e Tecnologias da Informação







INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL | worldskills Portugal

Ficha técnica:

TÍTULO

WorldSkills Portugal – **Prova Fase 1 Regional** da Competição de **CyberSecurity**

PROMOTOR E CONCETOR

Instituto do Emprego e Formação Profissional, I.P. - Departamento de Formação Profissional
R. de Xabregas, 52, 1900-003 Lisboa
Tel: (+351) 21 861 41 00
Website: www.iefp.pt
https://worldskillsportugal.iefp.pt
Facebook: www.facebook.com/WorldskillsPortugal

CONCEÇÃO METODOLÓGICA E COORDENAÇÃO GERAL

Gustavo Seia – *WorldSkills* Portugal | Coordenador
Vasco Vaz - *WorldSkills* Portugal | Delegado Técnico

EQUIPA TÉCNICA/CONCETOR

Joaquim Nogueiro - WorldSkills Portugal | Delegado Técnico Assistente
Rui Parente - WorldSkills Portugal | Delegado Técnico Assistente
Sandra Gabadinho - Skills Advisor da WorldSkills Portugal
Rodrigo Lima - WorldSkills Portugal | Presidente de Júri

Nos termos do Regulamento em vigor, esta Prova está aprovada pela *WorldSkill*s Portugal.

[palavras com aplicação em género devem aplicar-se automaticamente também ao outro]

CLUSTER/ÁREA DE ATIVIDADE: Gestão e Tecnologias da Informação

Correspondência com referenciais técnicos nacionais e internacionais	481344 – Técnico/a Especialista em Cibersegurança (Referencial CNQ) 54 - Cyber Security (WorldSkills International)

OBSERVAÇÕES

Portugal, através do Instituto do Emprego e Formação Profissional, I.P. (IEFP), é membro fundador da *WorldSkills International* (WSI) e da *WorldSkills Europe* (WSE), estando representado nos Comités Estratégicos e Técnicos das referidas Organizações. Cabe ao IEFP a promoção, organização e realização de todas as atividades relacionadas com os Campeonatos das Profissões. **A Prova** é o instrumento que **elenca as condições específicas de avaliação das competências dos concorrentes no decurso da competição** contextualizada **no âmbito de uma determinada profissão**.

Índice

1. PROVA 3
2. CRITÉRIOS DE AVALIAÇÃO 4
4. Prova – Módulo 1 5
A. FIREWALLS 5
B. HTTP Hardening 5
C. FTP Hardening 6
5. Prova – Módulo 2 7
A. PASSWORD POLICY 7
B. ACCOUNT LOCKOUT 8

1. PROVA

Apresentação da prova

A. Apresentação e memória descritiva da prova global

A HealthSec é uma start-up, fundada em 2026 por cinco jovens empreendedores recém-saídos da universidade, que se dedica ao desenvolvimento de soluções de software inovadoras para o setor da saúde.

Devido à natureza altamente regulamentada deste setor, à sensibilidade dos dados envolvidos nas operações do seu dia-a-dia e ao aumento da frequência e gravidade dos ataques informáticos nos tempos atuais, a cibersegurança é uma prioridade atual da empresa.

Como tal, a empresa HealthSec contratou os serviços de uma consultora no ramo da cibersegurança. O objetivo desta contratação foi a construção e entrega de um plano de ação que, quando seguido, permita à HealthSec aumentar, de forma faseada, a segurança dos seus colaboradores, equipamentos e soluções.

Neste contexto, os concorrentes irão configurar e aplicar inúmeras medidas que visam aumentar a segurança informática no contexto de sistemas operativos, infraestrutura e rede.

Para executar as tarefas propostas, os concorrentes terão à sua disposição as seguintes máquinas virtuais:

- Servidor Windows Server 2022 (DC) com as seguintes funções:
  - Active Directory Domain Services
  - DNS Server
- Servidor Windows Server 2022 (WINSRV) com as seguintes funções:
  - Web Server
  - FTP Server
- Servidor Linux Ubuntu 24.04 (LINSRV) com as seguintes funções:
  - Web Server
  - FTP Server

Os conjuntos de máquinas são exclusivas a cada concorrente, ou seja, cada concorrente só poderá aceder ao seu conjunto de máquinas.

B. Listagem dos módulos a desenvolver

Neste contexto, no caso da competição em apreço, a estrutura da prova assenta no âmbito dos seguintes 2 módulos de competição.

1) Desenvolvimento de Segurança em Redes
2) Desenvolvimento de Segurança em Sistemas Operativos

Nota: O enunciado dos módulos e respetivos desenhos técnicos (quando existirem) serão apresentados oportunamente de acordo com o calendário da prova.

2. CRITÉRIOS DE AVALIAÇÃO

Será disponibilizado o “Mark summary Form” em anexo.

4. PROVA – MÓDULO 1

A. FIREWALLS

1. Configurar a firewall local do Domain Controller com as seguintes regras:
   a. Permitir pings do servidor LINSRV para o Domain Controller;
   b. Negar todas as conexões de saída para o servidor LINSRV.

2. Configurar a firewall local (ufw) do servidor LINSRV com as seguintes regras:
   a. Permitir acesso SSH ao servidor LINSRV;
   b. Permitir acesso HTTP e FTP ao servidor LINSRV;
   c. Permitir acesso HTTPS e FTPS ao servidor LINSRV.

Nota: Sendo o servidor LINSRV acedido remotamente, deverão ter em conta a necessidade de não bloquear os protocolos de acesso remoto antes de ativar a firewall local.

B. HTTP HARDENING

3. Criar e proteger um website no servidor web IIS (WINSRV) com os seguintes requisitos:
   a. Gerar e aplicar um certificado *self-signed*;
   b. Todos os pedidos HTTP devem ser redirecionados para HTTPS.
   c. Relativamente aos headers de segurança, deverá ser configurado o header HSTS com as seguintes nuances:
      i. Validade máxima de 1 ano;
      ii. Aplicado também a subdomínios.

4. Criar e proteger um website no servidor web Apache (LINSRV) com os seguintes requisitos:
   a. Gerar e aplicar um certificado *self-signed*;
   b. Todos os pedidos HTTP devem ser redirecionados para HTTPS.
   c. Relativamente aos headers de segurança, deverá ser configurado o header HSTS com as seguintes nuances:
      i. Validade máxima de 1 ano;
      ii. Aplicado também a subdomínios.

Nota: O objetivo do exercício é avaliar a capacidade do concorrente de configurar aspetos de segurança. Como tal, o website deve ser o mais simples possível. Idealmente, apenas uma página estática. O servidor web deverá apenas conter este website.

C. FTP HARDENING

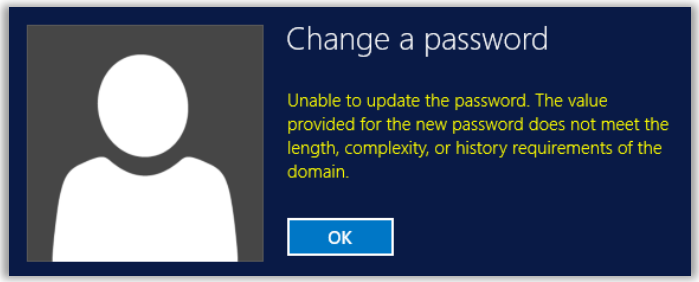
5. Criar e proteger um serviço FTP instalado no servidor WINSRV (via IIS), obedecendo aos seguintes requisitos:
   a. Binding será feito numa porta não comum – a porta 4021;
   b. Gerar e aplicar um certificado self-signed;
   c. Forçar o uso de encriptação durante a autenticação e transmissão de dados.

6. Criar e proteger um serviço FTP instalado no servidor LINSRV (via vsftpd), obedecendo aos seguintes requisitos:
   a. Binding será feito numa porta não comum – a porta 4021;
   b. Gerar e aplicar um certificado self-signed;
   c. Forçar o uso de encriptação durante a autenticação e transmissão de dados.

Nota: O binding de serviços a outras portas poderá requerer a configuração de novas regras de firewall. Um binding configurado corretamente, mas não funcional, irá reduzir a cotação da alínea em 50%.

5. PROVA – MÓDULO 2

A. PASSWORD POLICY



1. Configurar e aplicar uma política de password que obedeça aos requisitos enumerados abaixo, recorrendo às políticas de Active Directory para sistemas Windows. A política deverá ser aplicada a todo o domínio.
    a. O comprimento mínimo da password é de 12 caracteres;
    b. A password tem de obedecer aos requisitos de complexidade; [1]
    c. A password tem uma validade máxima de 3 meses (90 dias);
    d. O histórico de passwords é de 20 passwords.

2. Configurar e aplicar (localmente) uma política de password que obedeça aos requisitos enumerados abaixo, recorrendo à suite PAM do sistema Linux.
    a. O comprimento mínimo da password é de 12 caracteres;
    b. A password tem de obedecer aos requisitos de complexidade; (ver nota 1)
    c. A password tem uma validade máxima de 3 meses (90 dias);
    d. O histórico de passwords é de 20 passwords.

[1] Os requisitos de complexidade determinam que uma password deverá respeitar 3 das seguintes 4 categorias:
1. Conter caracteres maiúsculos;
2. Conter caracteres minúsculos;
3. Conter caracteres especiais;
4. Conter dígitos.

B. ACCOUNT LOCKOUT



3. Configurar e aplicar uma política de *account lockout* que obedeça aos requisitos enumerados abaixo, recorrendo às políticas Active Directory para sistemas em Windows.
    a. A conta deverá ficar impedida de fazer login (isto é, bloqueada) após 5 tentativas falhadas;
    b. A duração do bloqueio de uma conta deverá ser de 15 minutos;
    c. O contador de tentativas de login falhadas deverá voltar ao zero após 15 minutos de uma primeira tentativa falhada;
    d. A política deverá ser aplicada também ao administrador do sistema.

4. Configurar e aplicar (localmente) uma política de *account lockout* que obedeça aos requisitos enumerados abaixo, recorrendo à suite PAM do sistema Linux.
    a. A conta deverá ficar impedida de fazer login (isto é, bloqueada) após 5 tentativas falhadas;
    e. A duração do bloqueio de uma conta deverá ser de 15 minutos;
    f. O contador de tentativas de login falhadas deverá voltar ao zero após 15 minutos de uma primeira tentativa falhada;
    g. A política deverá ser aplicada também ao administrador do sistema.