Prova A

Segurança Cibernética

Module A1 – Enterprise Security

Criado por:
Thaylon Roberto Muniz da Silva

Table of Contents

Introdução

O conhecimento em cibersegurança está se tornando cada vez mais importante para pessoas que buscam uma carreira de sucesso em qualquer área de TI. Este projeto de teste contém diversos desafios do mundo real, principalmente relacionados à integração de segurança em TI e à terceirização de segurança em TI. Se você conseguir completar este projeto com uma boa pontuação, estará pronto para seguir em frente em sua busca pela excelência.

Descrição do Projeto e das Tarefas

Este projeto de teste é construído com uma variedade de tecnologias de rede com as quais você deve estar familiarizado, tanto da Microsoft quanto da Red Hat. As tarefas estão divididas nas seguintes categorias:

- Configuração da Infraestrutura e Reforço de Segurança
- Autoridade Certificadora e Proteção de Serviços Públicos
- Criptografia
- Reforço do Serviço SSH
- Gestão de Identidades e Acessos (IAM)
- Registro e Segurança dos Logs
- Comunicação Segura

Você deve aplicar o conjunto solicitado de políticas de segurança à infraestrutura existente. A maioria dos serviços já está em operação, mas sua segurança foi negligenciada. Alguns aspectos de segurança são diretos, enquanto outros podem permitir várias opções de implementação. Implemente todos os requisitos da melhor forma possível, seguindo as melhores práticas da indústria (em termos de segurança) e dentro das limitações dos equipamentos.

Instruções para o competidor

1. Antes de prosseguir com qualquer configuração, revise todas as tarefas.
2. Antes de começar o projeto de teste, confirme que todos os dispositivos na sua topologia estão funcionando corretamente. Quando concluir este projeto de teste, garanta que todos os dispositivos sejam acessíveis para a avaliação. Um dispositivo que não esteja acessível para a avaliação não poderá ser marcado e poderá fazer com que você perca pontos substanciais.
3. Salve suas configurações com frequência; acidentes podem e vão acontecer.
4. Quando o período da competição terminar, deixe a máquina ligada e não a desligue. Avaliaremos as máquinas no estado atual.
5. Por favor, escreva todas as suas respostas em um documento do Word, inclua capturas de tela e salve-o com seu nome como nome do arquivo e deixe no desktop da sua máquina local
6. Configuração dos Equipamentos
7. A maioria dos dispositivos e máquinas virtuais já possui nomes de host pré configurados com uma configuração básica. Consulte os diagramas de topologia (Fig. 1.0 e Tabela 1.0).
8. Embora ambos os competidores possam acessar a mesma topologia, eles só podem operar em uma única máquina virtual (VM). (Por exemplo, o competidor 1 está usando um Winserver, então o competidor 2 precisa trabalhar em um LinuxServer).
9. Para as VMs Windows, use as seguintes combinações para fazer login: Skills:P@ssw0rd ou Administrator:P@ssw0rd
10. Para as VMs Linux, use as seguintes combinações para fazer login:Skills:P@ssw0rd ou root/P@ssw0rd

11. As configurações de hostname, endereçamento de IP, Domínio, Instalação de serviços (Se disponíveis nos repositórios), roteamento (Equipamentos de rede ou OS), e demais configurações básicas para realização da prova devem ser feitas pelos competidores.
12. A prova deve ser entregue na área de trabalho com a sigla do DR juntamente com nome e sobrenome do competidor, ex: “AM_João_Ninguem”.

Ctrl + Alt + Shift

Task 1 - Configuração da Infraestrutura e Reforço de Segurança (28 pontos)

Políticas de Login e Senha

1. Implementar a Aplicação da Política de Senhas (14 pontos)

Nota: A política de senhas para o ambiente Windows deve ser implementada por meio da Política de Grupo de Domínio, e para sistemas Linux e dispositivos de rede, deve ser uma política de segurança local. Tanto o WinServer quanto o LinuxServer exigem a conclusão de todas as tarefas.

Requerimento	Aplicado a VM \ dispositivo	Providencie uma captura de tela para cada atividade(📷)
a) Política de Senha - O usuário deve alterar sua senha a cada duas semanas,	Winserver, LinuxServer	

com 3 dias de aviso e 1 dia de uso após a expiração. (lin - Linux | win - Windows) b) Complexidade da Senha ● Configurar a política para um comprimento mínimo de senha de 10 caracteres. (lin - Linux | win - Windows) ● Configurar o limite de 3 para o número máximo de caracteres consecutivos permitidos da mesma classe. (lin - Linux | win - Windows) ● Exigir pelo menos um caractere minúsculo. (lin - Linux | win - Windows) ● Exigir pelo menos um caractere maiúsculo. (lin - Linux | win - Windows) ● Exigir pelo menos um dígito. (lin - Linux | win - Windows)		

Nota: Caso algum novo usuário tenha sido criado, liste abaixo o nome de usuário ea senha correspondente: Nome de Usuário Senha		

2. Configurações de Segurança de Login (14 pontos)

Nota: A política de senha para o ambiente Windows deve ser implementada por meio da Política de Grupo de Domínio. Para sistemas Linux e dispositivos de rede, deve ser uma política de segurança local.

Requerimento	Aplicado a VM \ dispositivo	Providencie uma captura de tela para cada atividade(📷)
a) Configurar o banner de login como abaixo: “TP@IPT – WorldSkills Lyon 2024 "Apenas usuários autorizados" (win)	Winserver, LinuxServer	
b) Configurar uma política de bloqueio de conta para bloquear contas após 3 tentativas de login malsucedidas por uma duração de 25 minutos. (lin | win)		
c) Configurações da Política de Conta • Reusabilidade de Senha – Lembrar das 15 senhas anteriores. (win | lin)		
d) Crie os seguintes usuarios e grupos (Referente a tabela abaixo) e eles devem ser capazes de logar remotamente		

<table><tr><th>Usuarios</th><th>Senha(WinServer)</th><th>Senha(LinuxServer)</th></tr><tr><td>User01</td><td>P@ssw0rd</td><td>P@ssw0rd</td></tr><tr><td>User02</td><td>P@ssw0rd</td><td>P@ssw0rd</td></tr><tr><td>User03</td><td>P@ssw0rd</td><td>P@ssw0rd</td></tr></table> <table><tr><td>Grupos</td><td>developer</td></tr><tr><td></td><td>technical</td></tr></table>		
e) O tempo limite de inatividade não deve ser superior a 20 minutos. (win)		
f) Prevenir que credenciais armazenadas em cache sejam usadas para autenticar usuários em caso de indisponibilidade do controlador de domínio.		

Task 2: Autoridade Certificadora e Proteção de Serviços Públicos (10 pontos)

Você tem um Windows Server em um ambiente de domínio e deseja configurar o ADCS (Active Directory Certificate Services) para emitir certificados. Em seguida, você adquirirá um certificado para um servidor web e configurará esse certificado em um site do Windows usando o IIS (Internet Information Services).

2.1 IIS (Winserver) (6 marks)

Tasks	Respostas
a) Adquirir um certificado de servidor web usando o ADCS.	
b) Adquirir um certificado de cliente usando o ADCS.	
c) Configurar o site padrão com um certificado.	

2.2 FTP (LinuxServer) (4 marks)

Tasks	Respostas

a) Configurar a emissão de certificado do servidor CA (LinuxServer) para proteger o serviço FTP. Configurar o servidor FTP para aceitar apenas conexões SSL/TLS.	
b) O FTP proíbe o login anônimo.	

Task 3: Criptografia (12 pontos)

Tarefa de Trabalho: Servidor Web (LinuxServer)

Você foi designado para configurar um servidor we

b para utilizar um certificado RSA autoassinado de 4096 bits para tráfego HTTP e HTTPS. Além disso, você deve garantir que qualquer acesso via HTTP seja automaticamente redirecionado para a URL HTTPS.

(Na raiz de ambos os sites deve ser criado os arquivos “index.html” e “backup.bak”)

Task	Resposta

• site.wsc.local deve exibir uma página "Hello World". • files.wsc.local deve exibir uma lista simples de diretórios (VsFTPD).	
Crie um certificado autoassinado RSA de 4096 bits para o servidor web. Configure esse certificado para que o Server Name Indicator (SNI) responda corretamente a uma URI que inclua o endereço IP do host. Detalhe quais evidências foram fornecidas.	
Configure a autenticação .htaccess em files.wsc.local com as credenciais usuário: pwd123.	
Permitir tráfego HTTP e HTTPS através do firewall	
Modificar os arquivos de configuração do servidor web para responder tanto em HTTP quanto em HTTPS.	
Garantir que qualquer acesso via HTTP seja redirecionado para a URL HTTPS.	

Desabilitar a listagem de diretórios para evitar que atacantes naveguem pela estrutura de diretórios do seu site.	
Alterar o usuário e o grupo sob os quais o Apache é executado para um usuário que não seja o root.	
Habilitar o HSTS (HTTP Strict Transport Security)	
Todas as solicitações para arquivos com a extensão '.bak' devem retornar erro 403. Observe que os usuários ainda devem sercapazes de usar '.bak' em outras partes da URL, como parâmetros de consulta.	

Task 4: Reforço do Serviço SSH (10 pontos)

Requerimentos	Aplicado a VM \ dispositivo	Providencie uma captura de tela de cada atividade(📷)
a) Quando um usuário tentar fazer login via SSH, exibir uma mensagem legal:	LinuxServer	

“acesso não autorizado a este sistema não permitido”.		
b) Configurar logoff automático após 20 minutos de inatividade e exibir banners de segurança “Você não está ativo” para sessões SSH.		
c) Aplicar diferentes configurações do SSH com base no usuário ou grupo. Usuário: User02 Grupo: developer		
d) Configurar logging mais detalhado (verbose).		
e)Configurar outras configurações de segurança diversas, incluindo: ● Desabilitar o encaminhamento X11. ● Desabilitar o tunelamento SSH.		

f) Configurar controle de acesso usando TCP Wrappers para permitir apenas o host: 192.168.10.5.		
g) O SSH deve escutar na porta 22222 em vez da porta padrão. Fornecer evidências de que é possível se conectar ao servidor usando a porta 22222. Dica: Certifique-se de configurar as regras do firewall para que isso funcione.		
h) Você deseja desabilitar o login SSH usando nome de usuário/senha e permitir apenas autenticação baseada em chave.		
i) Você deseja aprimorar a segurança impedindo o login direto do root via SSH.		
j) Você deseja configurar login SSH sem senha usando pares de chaves.		

Task 5: IAM (10 marks)

Você foi designado para proteger um servidor FTP (vsFtpd) em execução no LinuxServer usando SELinux.

Task	Resposta
a) Habilitar o SELinux no servidor LinuxServer.	
b) Verificar o status atual do SELinux.	
c) Permitir que o servidor FTP escute na porta padrão do FTP (21) através do SELinux. (Se necessário)	
d) Configurar o vsftpd para usar um diretório específico para uploads via FTP.	

e) Definir o contexto SELinux para o diretório de upload do FTP.	
f) Permitir que os usuários do FTP leiam/gravem arquivos no diretório de upload.	
g) Permitir que os usuários do FTP façam login com o SELinux habilitado.	
h) Monitorar regularmente os logs de auditoria do SELinux para qualquer negação relacionada ao FTP e ajustar as políticas do SELinux conforme necessário.	

Task 6: Logging and Log Security (10 pontos)

Você tem um servidor CentOS Stream 9 atuando como um servidor de logs centralizado, denominado *Log Server*. Você deseja configurar este servidor para receber logs de diversas fontes.

Requerimento	Aplicado a VM \ dispositivo	Providencie uma captura de tela para cada atividade(📷)
a) Configurar o sistema para deixar apenas 7 dias de logs.	LinuxServer	

b) Configurar uma rotação diária de logs comprimidos para um mês de logs, usando arquivos nomeados com a data.		
c) Fazer com que todos os processos executados pelo usuário Doe sejam executados com uma prioridade baixa e os executados pelo usuário John sejam executados com uma prioridade mais alta (+/- 10).		
d) Configurar o rsyslog para receber logs remotos e configurar o firewall para permitir o tráfego Syslog.		
e) Suponha que você tenha um servidor web (WebServer) executando httpd. Você configurará o httpd para enviar seus logs de acesso para o LogServer (staff1). • O rsyslog deve receber os logs de acesso do httpd. • O rsyslog deve receber os logs do pfSense.		
f) Configurar a sincronização de horário contra o servidor NTP:		

pool 2.centos.pool.ntp.org com sincronização rápida.		
g) Fornecer serviços de servidor NTP para a sub-rede 10.8.8.0/24 apenas.		

Task 7: Comunicação Segura (20 pontos)

Você tem dois escritórios, Escritório 1 e Escritório 2, cada um protegido por um firewall pfSense (FW1 e FW2, respectivamente). Você deseja estabelecer um túnel VPN Site-to-Site seguro entre esses dois escritórios para permitir comunicação normal entre as redes atrás do FW1 e do FW2. Além disso, você deseja permitir que usuários remotos se conectem de forma segura à rede no Escritório 1 (FW1) usando o OpenVPN, com autenticação baseada em certificado.

7.1 Site-to-Site VPN (10 pontos)

Tasks	Resposta

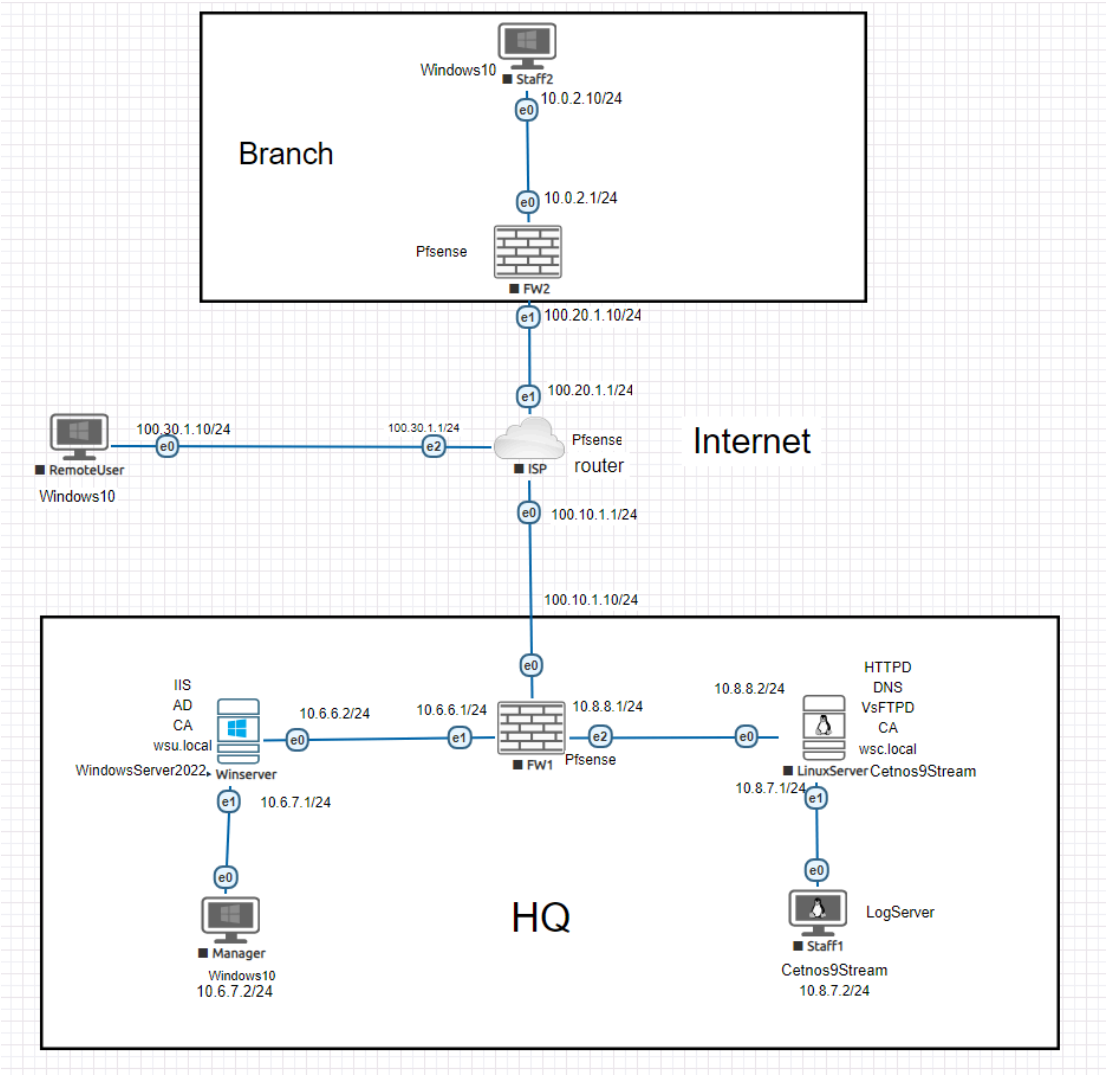
1. Construir um túnel VPN utilizando pfSense para comunicação normal entre o FW1 e FW2 usando a estratégia IKEv2 para o túnel IPsec na VPN.	
2. VPN Site-to-Site IPsec com Autenticação por Certificado. Os certificados devem ser assinados pela CA do WinServer.	

7.2 Remote access (10 marks)

(Para a criação da VPN Remote Access deve ser usado o usuário “Skills” com a senha “P@ssw0rd”)

Tasks	Resposta
1. Usuário remoto utiliza OpenVPN para acessar o LinuxServer.	
2. Usuário remoto utiliza certificados para autenticação do OpenVPN.	

Topology



VM name	IP address	Username	Password
HQ			
Winserver	10.6.6.2/24 10.6.7.1/24 mana	Administrator	P@ssw0rd
Manager(Windows 10)	10.6.7.2/24	Skills	P@ssw0rd
LinuxServer	10.8.7.1/24 10.8.8.2/24	root	P@ssw0rd
Staff1 (Centos9stream)	10.8.7.2/24	Skills	P@ssw0rd
FW1(Pfsense)	10.8.8.1/24 (Linux LAN) 10.6.6.1/24 (WIN LAN) 100.10.1.10/24 (WAN) Note: To gain access to the FW1, log in to Winserver and browse to http://10.6.6.1	admin	pfsense
Branch			
FW2(Pfsense)	100.20.1.10/24 (WAN) 10.0.2.1/24 (Branch LAN) Note: To gain access to the FW2, log in to staff2 and browse to http://10.0.2.1	admin	pfsense
Staff2(Windows 10)	10.0.2.10/24	Skills	P@ssw0rd
Internet			
ISP	100.10.1.1/24 (HQ) 100.20.1.1/24 (Branch) 100.30.1.1/24 (RemoteUser)		

RemoteUser(Windows 10)	100.30.1.10/24	Skills	P@ssw0rd

Table 1.0

Mark Summary Form

ID	Description	Mark Summary	Awarded marks
Task 1	Infrastructure Setup and Security Hardening	28.00	
Task 2	Certificate Authority and Public service protection	10.00	
Task 3	Cryptography	12.00	
Task 4	SSH service hardening	10.00	
Task 5	IAM	10.00	
Task 6	Logging and Log security	10.00	
Task 7	Secure communication	20.00	
	Total	100.00	