Projeto Integrado de Segurança Cibernética: Desenvolvimento e Implementação de um Plano de Resposta a Incidentes

Objetivo Geral: Capacitar os alunos a elaborar e implementar um Plano de Resposta a Incidentes de Segurança da Informação (PRISI) para uma organização fictícia, aplicando os conhecimentos adquiridos ao longo do semestre.

Descrição do Projeto: Os alunos serão divididos em grupos e cada grupo assumirá o papel de uma equipe de segurança cibernética dentro de uma organização fictícia. Ao longo do semestre, os grupos deverão:

1. **Análise de Riscos:** Identificar e avaliar possíveis ameaças e vulnerabilidades nos sistemas da organização.
2. **Desenvolvimento do PRISI:** Criar um plano detalhado que inclua políticas, procedimentos e responsabilidades para responder a diferentes tipos de incidentes de segurança.
3. **Implementação de Medidas Preventivas:** Propor e, se possível, implementar soluções técnicas e administrativas para mitigar os riscos identificados.
4. **Simulação de Incidentes:** Conduzir exercícios simulados para testar a eficácia do PRISI e a prontidão da equipe.
5. **Documentação e Relatório Final:** Elaborar um relatório abrangente que descreva todo o processo, desafios enfrentados, soluções adotadas e lições aprendidas.

Cronograma Sugerido:

- **Semanas 1-4:** Formação dos grupos, escolha da organização fictícia e início da análise de riscos.
- **Semanas 5-8:** Desenvolvimento do PRISI com base nos riscos identificados.
- **Semanas 9-12:** Implementação das medidas preventivas propostas.
- **Semanas 13-15:** Condução das simulações de incidentes e ajustes no PRISI conforme necessário.
- **Semanas 16-18:** Preparação e submissão do relatório final.

Recursos e Referências:

- **Guia de Aperfeiçoamento da Segurança Cibernética para Infraestruturas Críticas**: Este documento fornece uma estrutura flexível para gerenciar riscos de segurança cibernética e pode servir como referência para o desenvolvimento do PRISI.
- **OWASP (Open Web Application Security Project)**: Uma comunidade online que oferece artigos, metodologias e ferramentas gratuitas no campo da segurança de aplicações web.

- **CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)**: Fornece materiais e cursos relacionados à segurança da informação e resposta a incidentes.

Avaliação: A avaliação do projeto considerará a qualidade e a profundidade da análise de riscos, a eficácia e a clareza do PRISI desenvolvido, a implementação adequada das medidas preventivas, a condução realista das simulações de incidentes e a qualidade do relatório final, incluindo a documentação de todo o processo e as lições aprendidas.

Este projeto integrador permitirá que os alunos apliquem na prática os conceitos teóricos abordados durante o curso, desenvolvendo habilidades essenciais para a atuação na área de segurança cibernética.

Cronograma Semanal de Ferramentas e Cenários

Semana	Data	Tema da Aula	Ferramenta(s)	Cenário(s)
1	03/02	Introdução à Segurança Cibernética	-	-
2	10/02	Valor da Informação e Alinhamento Estratégico	-	-
3	17/02	Plano de Cibersegurança	-	-
4	24/02	Ameaças e Vulnerabilidades	-	-
5	03/03	Interceptação de Tráfego & Mapeamento de Redes	**Wireshark**: Analisador de pacotes de rede.	Atacante/Defesa
			Nmap: Scanner de rede para descoberta de hosts e serviços.	Atacante/Defesa
6	10/03	Ataques e Vulnerabilidades em Aplicações Web	**OWASP ZAP**: Scanner de segurança para aplicações web.	Atacante
			Burp Suite Community Edition: Plataforma para testes de segurança em aplicações web.	Atacante
7	17/03	Códigos Maliciosos e Wireless Hacking	**Aircrack-ng**: Conjunto de ferramentas para avaliação de segurança em redes sem fio.	Atacante
			ClamAV: Antivírus de código aberto para detecção de malwares.	Defesa
8	24/03	OWASP: Principais Vulnerabilidades	**OWASP ZAP**: Scanner de segurança para aplicações web.	Atacante

			SQLMap: Ferramenta para detecção e exploração de vulnerabilidades de injeção SQL.	Atacante
9	31/03	Atividade Prática Supervisionada	**Metasploit Framework**: Plataforma para desenvolvimento e execução de exploits.	Atacante
			Snort: Sistema de detecção de intrusões em rede.	Defesa
10	07/04	Segurança em Redes	**iptables**: Ferramenta de filtragem de pacotes e firewall.	Defesa
			OpenVPN: Solução de VPN para conexões seguras.	Defesa/Cliente
11	14/04	Segurança em Protocolos	**Wireshark**: Analisador de pacotes para inspeção de protocolos.	Defesa
			tcpdump: Ferramenta de captura de pacotes de rede.	Defesa
12	21/04	Segurança em Ambientes Linux e Windows	**Lynis**: Ferramenta de auditoria de segurança para sistemas Unix.	Defesa
			OSSEC: Sistema de detecção de intrusões baseado em host.	Defesa
13	28/04	Segurança em Redes sem Fio & IoT	**Kismet**: Detector de redes sem fio e sniffer.	Defesa
			Wireshark: Analisador de pacotes para inspeção de tráfego IoT.	Defesa
14	05/05	Resposta a Incidentes e Correções de Vulnerabilidades	**TheHive**: Plataforma de resposta a incidentes.	Defesa
			Cortex: Motor de análise e resposta a incidentes.	Defesa
15	12/05	Análise Forense Computacional	**Autopsy**: Interface gráfica para o Sleuth Kit, usada em investigações forenses.	Defesa
			Volatility: Framework para análise de memória RAM.	Defesa
16	19/05	Plano de Recuperação de Desastres	**Rsync**: Ferramenta para sincronização e backup de dados.	Defesa/Cliente

			Bacula: Solução de backup e recuperação de dados.	Defesa
17	26/05	Revisão Geral e Casos Reais	-	-
18	02/06	Prova/Atividade Avaliativa	-	-
19	09/06	Prova/Atividade Avaliativa	-	-
20	16/06	Encerramento e Feedbacks	-	-

Descrição dos Cenários

- **Atacante:** Ferramentas utilizadas para simular ataques e identificar vulnerabilidades em sistemas e redes.
- **Defesa:** Ferramentas empregadas para proteger, monitorar e responder a incidentes de segurança, fortalecendo a postura defensiva da infraestrutura.
- **Cliente:** Ferramentas ou configurações aplicadas no ambiente do usuário final, visando garantir a segurança dos dados e comunicações.