

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

| | | | | |
|----|-------|-----------------------------|--|--------|
| | | | 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.

1. Formação dos Grupos e Definição da Organização Fictícia

Passos:

- **Formação dos Grupos:** No início do semestre, os alunos serão organizados em grupos de 4 a 5 integrantes.
- **Escolha da Organização Fictícia:** Cada grupo deverá criar um perfil para uma organização fictícia, definindo seu setor de atuação, porte, infraestrutura de TI e outros detalhes relevantes.

2. Análise de Riscos

Passos:

- **Identificação de Ativos:** Listar todos os ativos críticos da organização, como servidores, bancos de dados, aplicações e informações sensíveis.
- **Identificação de Ameaças e Vulnerabilidades:** Utilizar ferramentas como o **Nmap** para mapear a rede e identificar possíveis vulnerabilidades.
- **Avaliação de Riscos:** Analisar o impacto e a probabilidade de ocorrência de cada ameaça identificada.

3. Desenvolvimento do Plano de Resposta a Incidentes de Segurança da Informação (PRISI)

Passos:

- **Definição de Políticas e Procedimentos:** Estabelecer diretrizes claras para a resposta a diferentes tipos de incidentes.

- **Designação de Responsabilidades:** Atribuir funções específicas a membros da equipe para a gestão de incidentes.
- **Fluxo de Comunicação:** Criar um plano de comunicação para notificar as partes interessadas em caso de incidentes.

4. Implementação de Medidas Preventivas

Passos:

- **Configuração de Ferramentas de Segurança:** Instalar e configurar ferramentas como **iptables** para firewall e **ClamAV** para antivírus.
- **Atualização de Sistemas:** Garantir que todos os sistemas e aplicações estejam atualizados com os patches de segurança mais recentes.
- **Treinamento de Usuários:** Conduzir sessões de conscientização sobre práticas seguras para todos os "funcionários" da organização fictícia.

5. Simulação de Incidentes

Passos:

- **Planejamento de Cenários:** Desenvolver cenários de incidentes comuns, como ataques de phishing ou ransomware.
- **Execução das Simulações:** Utilizar ferramentas como o **Metasploit Framework** para simular ataques, enquanto outras equipes empregam ferramentas de defesa para mitigar os impactos.
- **Avaliação de Respostas:** Analisar a eficácia das respostas e identificar áreas de melhoria.

6. Documentação e Relatório Final

Passos:

- **Coleta de Dados:** Reunir logs, resultados de análises e feedback das simulações.
- **Elaboração do Relatório:** Documentar todas as etapas do projeto, incluindo a análise de riscos, o PRIS desenvolvido, medidas preventivas implementadas, detalhes das simulações e lições aprendidas.
- **Revisão e Submissão:** Revisar o relatório para garantir clareza e precisão antes da submissão final.

Preparação do Ambiente

Passos:

- **Configuração do Ambiente Virtual:** Utilizar plataformas de virtualização para criar redes e sistemas que simulem a infraestrutura da organização fictícia.
- **Instalação de Sistemas Operacionais:** Implementar distribuições Linux, como Debian ou Kali Linux, conforme as necessidades do projeto.
- **Implementação de Ferramentas Necessárias:** Instalar as ferramentas de segurança mencionadas no cronograma semanal, garantindo que todas estejam operacionais para as atividades práticas.

Ferramentas Sugeridas

- **Nmap:** Para mapeamento de rede e descoberta de hosts.
- **Metasploit Framework:** Para simulação de ataques e testes de penetração.
- **iptables:** Para configuração de regras de firewall.
- **ClamAV:** Para detecção e remoção de malwares.
- **Wireshark:** Para análise de tráfego de rede.
- **OpenVPN:** Para criação de redes privadas virtuais seguras.
- **Lynis:** Para auditoria de segurança em sistemas Unix.
- **TheHive e Cortex:** Para gestão e resposta a incidentes.
- **Autopsy e Volatility:** Para análise forense computacional.