Trabalho Prático 1

CET 8493 | UFCD 9196 - Cibersegurança Ativa | Formador: Paulo Vaz

Formando: João Rodrigo Mota da Costa

1. Qual é a diferença entre IPS, IDS e SIEM?

IPS significa "Sistema de Prevenção de Intrusão", IDS significa "Sistema de Detecção de Intrusão" e SIEM significa "Gestão de Eventos e Informação de Segurança". IPS e IDS são sistemas de segurança que monitorizam o tráfego de rede em tempo real para detetar e prevenir intrusões e ataques cibernéticos. SIEM é uma plataforma que recolhe e analisa dados de segurança de vários sistemas e dispositivos para identificar ameaças de segurança e gerir incidentes.

2. Como funcionam os sistemas IPS e IDS?

Os sistemas IPS e IDS funcionam através da monitorização do tráfego de rede em busca de padrões de atividade maliciosos. O IDS deteta e alerta quando ocorre uma atividade suspeita, enquanto o IPS pode bloquear automaticamente essa atividade maliciosa.

3. Quais são alguns tipos comuns de ataques que os sistemas IPS e IDS podem detetar e prevenir?

Alguns tipos comuns de ataques que os sistemas IPS e IDS podem detetar e prevenir incluem ataques de negação de serviço, intrusões em sistemas, ataques de malware e ataques de phishing.

4. Quais são os benefícios de usar um sistema SIEM?

Os benefícios de usar um sistema SIEM incluem a capacidade de detetar e responder rapidamente a ameaças de segurança, melhorar a visibilidade da segurança e fornecer informações para conformidade regulamentar.

5. Quais são algumas das principais funcionalidades de um sistema SIEM?

Algumas das principais funcionalidades de um sistema SIEM incluem a recolha de dados de vários sistemas e dispositivos, a correlação de eventos de segurança, a análise de dados para identificar ameaças e a capacidade de gerir incidentes de segurança.

6. Como é que os sistemas SIEM ajudam as organizações a cumprir os requisitos regulamentares e os padrões de segurança?

Os sistemas SIEM ajudam as organizações a cumprir os requisitos regulamentares e os padrões de segurança, fornecendo uma visão abrangente das atividades de segurança em toda a empresa e ajudando a identificar ameaças de segurança em tempo real.

7. Quais são os desafios associados à implementação e gestão de sistemas IPS, IDS e SIEM?

Os desafios associados à implementação e gestão de sistemas IPS, IDS e SIEM incluem a necessidade de recursos especializados, o custo de hardware e software e a necessidade de manter esses sistemas atualizados e configurados corretamente.

8. Quais são as melhores práticas para configurar e ajustar os sistemas IPS, IDS e SIEM para maximizar a sua eficácia?

Algumas das melhores práticas para configurar e ajustar os sistemas IPS, IDS e SIEM incluem a implementação de políticas de segurança robustas, a monitorização regular de logs de segurança e a realização de testes regulares para garantir que esses sistemas estejam a funcionar corretamente.

9. Como é que as organizações podem garantir que os seus sistemas IPS, IDS e SIEM estão integrados e funcionam de forma eficaz?

As organizações podem garantir que os seus sistemas IPS, IDS e SIEM estão integrados e funcionam de forma eficaz através da implementação de um plano de gestão de segurança abrangente, da formação de pessoal especializado e da monitorização regular da atividade de segurança.

10. Quais são as tendências emergentes na tecnologia IPS, IDS e SIEM e como é que estão a impactar o panorama da Cibersegurança?

Algumas das tendências emergentes na tecnologia IPS, IDS e SIEM incluem a utilização de inteligência artificial e aprendizagem automática para melhorar a deteção de ameaças e a automatização de processos de segurança para reduzir o tempo de resposta a incidentes. Essas tendências estão a impactar o panorama da cibersegurança, tornando a proteção contra ameaças cada vez mais avançadas e sofisticadas.