Auditoria de Sistemas

Prof. Dr. Joseffe Barroso de Oliveira

AULA 05

Softwares de Auditoria de Sistemas

Introdução

A utilização de softwares que podem ser utilizados em uma auditoria ajudam muito ao auditor e as empresas conseguirem informações valiosas e detalhadas sobre toda jornada. A seguir estão alguns dos principais softwares utilizados em auditoria de sistemas, com uma descrição detalhada de cada um e exemplos práticos de uso. Esses softwares ajudam a automatizar processos, identificar vulnerabilidades e garantir a conformidade em várias frentes, desde segurança de TI até auditoria financeira e de conformidade regulatória.

Audit Command Language (ACL)

Descrição do ACL

O ACL é uma ferramenta amplamente usada para auditoria de dados e análise, oferecendo funcionalidades avançadas para extrair, processar e analisar grandes volumes de dados.

Funcionalidades

Ele ajuda a identificar padrões, outliers e irregularidades nos dados, sendo útil em auditorias financeiras e operacionais.

Aplicações em Auditoria

O ACL permite filtrar e identificar transações suspeitas, como duplicidades de faturas, e comparar com os relatórios fiscais oficiais para verificar discrepâncias.

Exemplo Prático de Uso

Em uma auditoria de conformidade fiscal, o auditor pode utilizar o ACL para analisar registros de faturamento de uma empresa.

IDEA (Interactive Data Extraction and Analysis)

Capacidades do IDEA

O IDEA é uma ferramenta poderosa de análise de dados que auxilia auditores a realizar extrações, análises e amostragens em grandes volumes de dados. Ele automatiza o processo de auditoria e oferece relatórios detalhados para investigações de fraudes e conformidade.

Detecção de Fraudes

O IDEA permite identificar padrões fraudulentos em dados, facilitando a detecção de irregularidades e aumentando a eficiência das auditorias.

Exemplo Prático

Uma empresa de seguros pode usar o IDEA para identificar padrões fraudulentos de sinistros, detectando sinistros com valores acima do padrão e repetição de beneficiários em curto período.

Ferramentas de Teste de Penetração

O Nmap realiza varreduras de portas e mapeamento de rede, identificando dispositivos conectados e vulnerabilidades potenciais.

O Nessus detecta vulnerabilidades em sistemas, ajudando a identificar falhas que podem ser exploradas por atacantes.

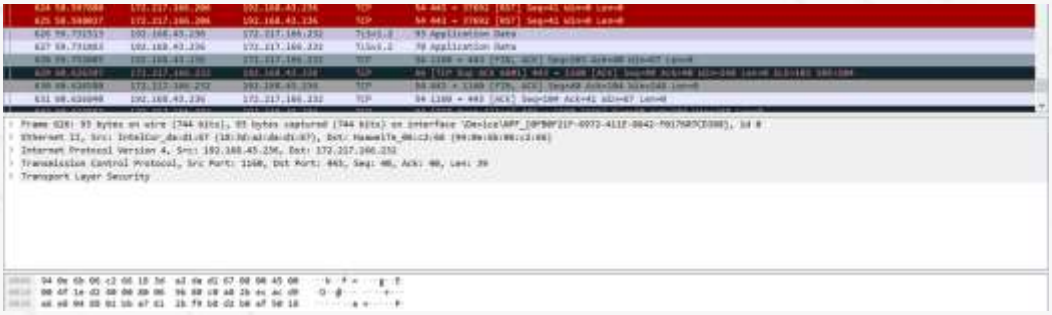
O Metasploit executa ataques simulados para avaliar a segurança do sistema, permitindo testar se as vulnerabilidades podem ser exploradas.

Em uma auditoria de segurança, a equipe pode usar o Nmap para mapear dispositivos conectados à rede e identificar portas abertas, seguido pelo Nessus para detectar falhas.

Wireshark e Análise de Tráfego

Uso do Wireshark em Auditorias de Segurança

- O Wireshark é uma ferramenta de análise de tráfego de rede que permite capturar e examinar pacotes de dados. É amplamente utilizado em auditorias de segurança e diagnóstico de rede, pois possibilita a visualização de comunicações em tempo real e a identificação de anomalias.
- Durante uma auditoria de segurança de rede, um auditor pode usar o Wireshark para capturar e analisar o tráfego da rede corporativa. Se houver comunicação não autorizada ou um ataque man-in-the-middle, o Wireshark pode ajudar a identificar os pacotes suspeitos e determinar a origem da anomalia.
- A capacidade do Wireshark de filtrar e detalhar pacotes permite que auditores identifiquem padrões de tráfego que podem indicar comportamentos maliciosos ou vazamentos de dados, facilitando a resposta a incidentes.



Splunk para Análise de Dados

1

O Splunk é uma plataforma para análise de dados em tempo real, especialmente logs de sistemas e eventos de TI, permitindo insights detalhados para auditorias de segurança.

2

Em auditorias de segurança cibernética, o Splunk pode ser configurado para monitorar eventos críticos, como tentativas de login, e gerar alertas para anomalias.

3

Se houver um aumento incomum no número de tentativas de login com falhas, o sistema pode gerar alertas para investigação imediata, garantindo a conformidade e segurança dos sistemas.

SonarQube e Controle de Qualidade de Código

Verificação de Qualidade e Segurança do Código

- O SonarQube verifica a qualidade e segurança do código-fonte em busca de vulnerabilidades, erros e inconsistências.
- Ele é especialmente útil para auditorias de software, garantindo conformidade com padrões de segurança e desenvolvimento.
- O SonarQube analisa práticas de programação, como manuseio adequado de exceções e uso de autenticação segura.

Exemplo Prático de Uso

- Em uma auditoria de desenvolvimento seguro, o SonarQube pode ser utilizado para revisar o código de um aplicativo web.
- Ele identifica vulnerabilidades como injeção de SQL ou Cross-Site Scripting (XSS).
- O uso do SonarQube assegura que as melhores práticas de programação estão sendo seguidas.