SYMMETRY

PENTEST – Teste de Intrusão

Qual é a sua eficácia?

Symmetry

RECURSOS INCRÍVEIS PARA TECNOLOGIA

Presente no mercado desde 1996 ocupa posição de destaque entre as principais integradoras e provedoras de soluções de Tecnologia da Informação do país.

Áreas de atuação:

Infraestrutura de LAN e Wi-Fi

Segurança da Informação

Alta Disponibilidade

Backup e Storage

Telefonia IP

Network Analytics
Análise, Site Survey e indicadores de desempenho em tempo real

A Symmetry traz uma visão inovadora, voltada a aumentar a eficiência da TI nos mais diversos tipos de ambientes.

Flexibilidade para seu negócio

Segundo publicação do anuário INFORMÁTICA HOJE:

Eleita como a "Integradora Mais Eficiente do País"

CONFIRA NOSSOS PARCEIROS

FORTINET · aruba NETWORKS · COMMVAULT · SOPHOS · Aerohive NETWORKS · IS Decisions · peplink · Hewlett Packard Enterprise

SOLUÇÕES CUSTOMIZADAS

Soluções como serviço (IaaS)

Serviços gerenciados de Segurança

Serviços gerenciados de Infraestrutura

Operação (Parcial ou Full)

Outsourcing

GESTÃO E MONITORAMENTO

A melhor equipe **focada na sua solução**

Profissionais certificados nas tecnologias que melhor se ajustam às necessidades do seu negócio

Você pode contar com nosso **NOC** que realiza monitoramento remoto em tempo real dos seus serviços e aplicações

TREINAMENTO HANDS-ON

Através da **Symmetry Academy** ofertamos diversos cursos e treinamentos de forma prática e extensiva para profissionais que necessitem de qualificação técnica para se diferenciar no mercado de TI.

Teste de Intrusão: Qual é a sua eficácia?

A utilização de softwares na prevenção de intrusão nas redes de computadores deve fazer parte da política de segurança das organizações que prezam pela segurança e sigilo das informações. A organização que não tem a preocupação com suas informações se torna um alvo fácil para que seus dados sejam roubados e utilizados por terceiros. Este estudo tem por finalidade demonstrar a utilização de uma ferramenta de grande utilidade na coleta de informações que servem para prevenção de ataques as redes de computadores, com um estudo de caso e, fazendo uso de um software para esse fim. Conclui-se que a utilização dessa ferramenta atingiu o objetivo proposto, pois o retorno obtido pelo software expôs informações que poderiam deixar o sistema vulnerável.

Com o uso crescente da rede mundial as organizações tem se preocupado com a integridade, confiabilidade e segurança dos dados. Manter um firewall ativado e bem configurado, o uso da criptografia, software antivírus e outros métodos de segurança tornam-se necessários, mas nem sempre eficientes e eficazes contra os ataques a que a rede está sujeita. As organizações estão sujeitas a riscos, os ataques são executados em data e hora não estipulados, os métodos utilizados, as técnicas e ferramentas utilizadas pelos atacantes são das mais diversas. Cuidados devem ser tomados para que as atividades e negócios das organizações não sejam interrompidos.

Método

O Teste de Intrusão ou Teste de Penetração (do inglês “Penetration Test” ou pentest) é um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa. O processo pontua uma análise nas atividades do sistema, que envolvem a busca de alguma vulnerabilidade em potencial que possa ser resultado de uma má configuração do sistema, falhas em hardwares ou softwares desconhecidas, deficiência no sistema operacional ou técnicas de contramedidas. Todas as análises submetidas pelos testes escolhidos são apresentadas no sistema, junto com uma avaliação do seu impacto e muitas vezes com uma proposta de resolução ou de uma solução técnica.

Objetivo

Pode ser classificado como um método de auditoria de segurança relizado por Administradores de Redes, Analistas de Testes ou até mesmo os Pentesters (que são profissionais especializados em realizar o Teste de Intrusão). Nele são simulados ataques com o intuito de mensurar o impacto da varredura caso seja bem sucedida, onde se descobrem falhas ou bugs. Desta forma é possível descobrir o conjunto de vetores de ataques, vulnerabilidade de alto e baixo risco, identificar os que podem ser difíceis ou impossíveis de detectar, os impactos operacionais, testar a capacidade defensiva da rede e identificar a reação do sistema aos ataques. Dentre vários motivos pra realizar ataques a software, se destacam as invasões por questões financeiras, pessoais, cometer fraudes, sabotagem ou espionagem. O invasor é uma pessoa com alto nível de conhecimento técnico, seus ataques são minuciosamente planejados, portanto é importante que haja o estudo do comportamento do alvo, assim

procurando uma brecha na segurança dando início ao seu objetivo depois de passar por várias etapas ou fases.

Etapas

As etapas de estudo se dividem em:

1. Coletar Informações: Toda e qualquer informação sobre a empresa a ser atacada é indispensável, como o ramo de atuação, se existem filiais ou empresas coligadas, endereços de e-mails, nomes dos principais cargos. Com esses dados é possível descobrir se a empresa utiliza VPN (Virtual Private Network) e coletar endereços dos servidores DNS (Domain Name Service).

2. Mapeamento de Rede: Através do DNS é possível descobrir a topologia da rede, IP e a quantidade de computadores na rede interna.

3. Enumeração de Serviços: Depois de conhecer as maquinas da rede, essa etapa consiste em descobrir os serviços que estão sendo executados em uma determinada porta utilizando um programa que monitora atrás das conexões. Na porta 80, por exemplo, a conexão é com o servidor web.

4. Busca de Vulnerabilidade: É fase em que o software é examinado com intuito de encontrar alguma vulnerabilidade e se é explorável.

5. Exploração das Vulnerabilidades: Após o estudo das vulnerabilidades é realizado a invasão ao software, podendo interromper o serviço, atacar o SQL ou dar início a execução de outro programa que recebe comandos remotamente.

6. Implantação de Backdoors e Rootkits: O invasor deixa instalado um programa que facilita o seu retorno ao software. Esses tipos de programas são chamados de Backdoors (do inglês “Portas dos Fundos” que deixam uma porta disponível para o acesso do invasor) e Rootkits (que se mantém do núcleo do sistema operacional e é difícil de ser localizado).

7. Eliminação de Vestígios: As invasões são registradas através do histórico (logs) ou de arquivos temporários. Para apagar os rastros o invasor terá que apagar esses registros, podendo tornar impossível a sua identificação.

Testes

Os testes de intrusão podem ser realizados de várias maneiras. A diferença mais comum entre eles é a quantidade de detalhes da implementação do sistema a ser testado, que estão disponíveis para os testadores.

O teste da caixa preta assume que não existe qualquer conhecimento prévio da infraestrutura a ser testada. Sendo que o primeiro teste deve determinar a localização e extensão dos sistemas antes de iniciar a análise.

O teste da caixa branca assume que o testador possui total conhecimento da infraestrutura a ser testada, incluindo o diagrama da rede, endereçamento IP e qualquer informação complementar.

Testes de caixa preta simulam um ataque de alguém que esteja familiarizado com o sistema, enquanto um teste de caixa branca simula o que pode acontecer durante o expediente de trabalho ou depois de um "vazamento" de informações, em que o invasor tenha acesso ao código fonte, esquemas de rede e, possivelmente, até mesmo de algumas senhas.

Aplicações

Os serviços oferecidos por empresas contratadas para usar o teste de intrusão, podem ser uma simples varredura dos endereços IP na organização, abrir e fechar portas ou fazer uma auditoria completa no escopo da rede em busca de vulnerabilidade.

Segundo a página “Software Livre Brasil”, existem vinte e um passos para se realizar Teste de Segurança, são eles:

1. Análise da rede
2. Análise de portas
3. Identificação de sistemas
4. Provas de debilidades em sistemas sem fios (dependendo segundo o caso)
5. Verificação de serviços (Site, correio, servidor de nomes, documentos visíveis, vírus e trojanos)
6. Determinação de vulnerabilidades
7. Identificação de exploits
8. Verificação manual de vulnerabilidades
9. Verificação de aplicações
10. Verificação de firewall e ACL
11. Revisão das políticas de segurança
12. Revisão de sistemas de detecção de intrusos
13. Revisão de sistemas de telefonia (dependendo segundo o caso)
14. Obtenção de informação (serviços de notícias, notas de imprensa, informações facilitadas pela própria empresa), ofertas de trabalho, newsgroups, xracks, números de série e “underground”, FTP, Site, P2P
15. Engenharia social
16. Verificação de sistemas “confiáveis”
17. Análise de fortaleza de senhas
18. Negação de serviço
19. Revisão da política de privacidade.
20. Análise de cookies e bugs no Site
21. Revisão de arquivos de anotações cronológicas (logs)

O primeiro passo para a prevenção é o Firewall ativo na rede para controlar e impedir acessos suspeitos, com todas as configurações e atualização dos serviços web realizadas, além de se fazer o monitoramento constante da rede e gerar um relatório com registros de todas anomalias detectadas.