

# Especialista em



## Atividades principais

- Projeto e manutenção do esquema de segurança da rede, incluindo a segurança de equipamentos (acesso físico), dos dados (acesso não autorizado) e de sistemas operacionais de clientes e servidores; este profissional propõe, implementa e monitora a política de segurança para múltiplos dispositivos de rede e sistemas operacionais.

## Atividades adicionais

- Configuração e manutenção da segurança de rede;
- Monitoramento constante de aspectos novos relacionados à segurança (novas técnicas de invasão, novos bugs de segurança encontrados em produtos na rede, etc.).





### Pré-requisitos normalmente exigidos

- Profundo conhecimento do protocolo TCP/IP e dos sistemas operacionais de clientes e de servidores existentes na empresa;
- Em algumas empresas, exige-se que o Analista de Segurança também conheça as linguagens de programação utilizadas pela empresa, este profissional é bem mais raro de se encontrar no mercado e seu salário é proporcionalmente maior.
- Profundo conhecimento de configuração e “atualização de regras” em firewalls;
- Conhecimento de protocolos típicos de inter-redes (Frame Relay, X25, ATM, etc.);
- Uso de ferramentas de monitoramento de tráfego de rede, incluindo sniffers.

### Certificações recomendadas

- MCSE (com ênfase nos 3 exames de segurança);
- Certificações de segurança (Cisco, Checkpoint, etc.).



### Cenário atual

- Convergência de Tecnologias;
- Aumento significativo de sistemas e redes de informação;
- Aumento crescente de acessos;
- Avanço das tecnologias de informação e comunicação;
- Ambiente em constante e rápidas mudanças.

### Desafios

- Aumento das ameaças e vulnerabilidades, e, conseqüentemente, a urgência de ações que visem a criação, manutenção e fortalecimento da cultura de segurança.





### Segurança de um computador

➤ Um computador (ou sistema computacional) é dito seguro se atende a três requisitos básicos:

- Confidencialidade;
- Integridade;
- Disponibilidades.

### Ataques

➤ São técnicas utilizadas por hackers para burlar o esquema de segurança, quebrando a confidencialidade, integridades e disponibilidades de algum serviço ou equipamento.



### Ameaças e tipos de ataques

➤ Para que seja possível proteger os sistemas computacionais de ataques e invasões, precisa-se conhecer quem são as pessoas que possuem conhecimentos para comprometer a segurança dos mesmos e quais as tecnologias disponíveis que podem ser utilizadas por elas para atingir seus objetivos. Por isso, surge a necessidade de se classificar essas pessoas (atacantes) e as tecnologias (ataques) usadas por elas.



### Atacantes

➤ Dá-se o nome de atacante à pessoa que realiza um ataque (tentativa de comprometimento ou invasão) a um sistema computacional, obtendo êxito ou não. Esta terminologia é utilizada mais didaticamente, pois o termo conhecido popularmente é Hacker, amplamente usado pela mídia (jornais, revistas, etc.). O termo Hacker possui algumas ramificações, tais como: **Script Kiddies, Crackers, Carders, Cyberpunks, Insiders, Coders, White hats, Black hats** e **Preacker**. Originalmente atribuíam-se o nome Hacker àqueles que utilizavam seus conhecimentos para invadir sistemas, sem o intuito de causar danos, mas como um desafio às suas habilidades [Spy 2001].



### Tipos de Ataques

➤ **Ataque físico** – são roubos de equipamentos, softwares e qualquer outro tipo de ativo que se possa ser levado ou danificado. Pode ser utilizado também, por acesso não autorizado a um terminal com acesso a uma rede corporativa ou sistema, para se obter informações privilegiadas, modificar arquivos importantes, implantar bombas lógicas e outros danos. É um método pouco utilizado, mas nem por isso, menos danoso. Logo requer que a organização mantenha algum tipo de controle de acesso às suas dependências.

➤ **Sniffing** - consiste na captura de informações diretamente do fluxo de pacotes no mesmo segmento de rede onde o atacante instalou o software. Seus alvos preferidos são senhas que trafegam sem criptografia, e-mails e qualquer outro tipo de informação que passe em texto plano.

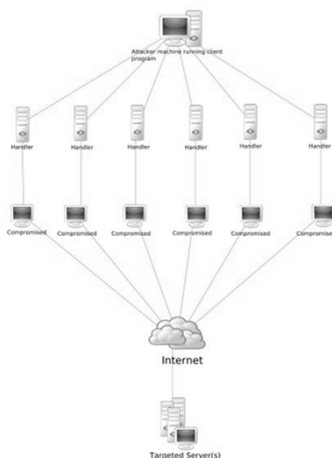


➤ **Port Scanning** - são utilizadas para obtenção de informações referentes aos serviços que são acessíveis e definidas por meio do mapeamento das portas TCP e UDP. Com as informações obtidas com a varredura, evita-se o desperdício de esforços com ataques e serviços inexistentes, de modo que o hacker pode se concentrar em utilizar técnicas que exploram serviços específicos, que podem ser de fato, explorados.

➤ **Denial of Service** - Um Distributed Denial-of-Service ATTACK é uma maneira relativamente simples de derrubar algum *service*. O objetivo aqui é unicamente o de tornar uma página ou processo indisponível para o usuário final.



### ➤ DDoS ATTACK





➤ **Cavalos de Troia, vírus e outros malwares** - Esses programas são normalmente desenvolvidos pelos hackers com o único objetivo de gerar destruição do alvo. Os vírus e worms normalmente se aderem a um sistema de forma que possam inviabilizar o uso de uma máquina ou de uma rede como um todo, e são normalmente disseminados por email ou ficam escondidos dentro de aplicações de interesse do usuário.

➤ **Ataques de Força Bruta** - Essa é a maneira mais famosa que existe para se quebrar senhas. Consiste em tentar todas as combinações possíveis até que o password seja encontrado. Porém, com o crescimento do tamanho das senhas, as combinações possíveis aumentam exponencialmente e, com isso, também aumenta o tempo necessário para serem decifradas.



➤ **Engenharia Social** - é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. A engenharia social é um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. [Mitnick, 2003] Ela é um perigo real e sutil e é fundamental que as organizações assegurem-se que seus usuários sejam atuantes defensores da sua informação e que não sejam facilmente ludibriados por pessoas mal intencionadas e não autorizadas, abrindo assim, o caminho para o acesso a informação.



### Prevenção e Boas Práticas

- **Senhas Fortes** – Usar letras ( a A ), números e caractere especial ( Longa )
- **Antivirus** – Usar versões pagas
- **Anti-Spyware** – Usar versões pagas
- **Anti-Spam** – Usar versões pagas
- **Proxy** - Exige autenticação para uso da rede
- **Atualizações** – Baixar e instalar todas atualizações de segurança
- **Firewall** – Usar hardware dedicado e bem configurado ou UTM
- **Criptografia** – Manter o disco ou suas pastas e arquivos criptografados
- **VPNs** – Usar para comunicação externa
- **Configuração Wifi** – Usar equipamento profissional e bem configurado
- **Proteção por camadas** – A redundância em vários níveis



### A Perícia Forense Computacional

- A perícia forense computacional é definida como a aplicação de conhecimento de informática e técnicas de investigação com a finalidade de obtenção de evidências, além de, ser uma área relativamente nova e em grande ascensão; justamente por isso tornou se uma prática importante nas corporações e polícias, que utilizam resultados científicos e matemáticos estudados na ciência da computação.
- Existem hoje diversas ferramentas que auxiliam no trabalho, quando se trata de verificação de rede.
- Até mesmo a análise de logs do sistemas ajuda e muito nesse tipo de investigação...





- **Unified Threat Management (UTM)**, que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes e vem ganhando notoriedade e se tornou a solução mais procurada na defesa das organizações.
- **VPNs** seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.
- A credencial Microsoft Certified Systems Engineer (**MCSE**) mostra a clientes e empregadores que você pode projetar, implementar e administrar infraestruturas para soluções corporativas baseadas no Microsoft 2000 Windows Server e em outras plataformas de servidor do Windows. As responsabilidades de implementação incluem a instalação, a configuração e a solução de problemas em sistemas de rede.



## PenTest

- O **teste de penetração** 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 envolve 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/software desconhecidas, deficiência no sistema operacional ou técnicas contramedidas.
- BackTrack
- BackBox
- NodeZero
- Blackbuntu







## Trabalho de Informática e Sociedade

- **Tema** : Especialista em Segurança de Redes
- **Professor** : Frederico Sauer
- **Fonte** : Internet ( Diversos sites )

➤ **Grupo** :

- Andrews Santos da Costa
- Denis Fernandes da Silva
- Lucas Souza Tambelini
- Mauricio Rondon
- Mayra Santiago
- Natália Cristina Soares Silva

