2021 — SENAI-SP

Curso Técnico de Desenvolvimento de Sistemas

UC: Hardware e Redes (HARE) – Primeiro Termo

Aula 8 – Segurança

Prof. Douglas Gaspar

Contextualização com o plano de aula

SENAI

2021 — SENAI-SP

Nessa aula será(ão) abordado(s) o(s) seguinte(s) assunto(s) - (Conhecimento(s)):

- Segurança de redes

Relacionados a(os) seguinte(s) Fundamento(s) Técnico(s) e Científico(s):

- Identificar os tipos de serviços disponíveis em redes

Segurança em redes

- Qualquer dispositivo que esteja conectados a uma rede fica, de certa forma, vulnerável a ataques pois há um “caminho” para chegar até esse dispositivo
- O descobrimento do IP de um computador já fornece dados suficientes para começar a procura por brechas no sistema.

Segurança em redes

- A cada dia novas vulnerabilidades são encontradas nos sistemas, são chamadas de Zero Day.
- Há pessoas que pesquisam por essas brechas e revertem esse conhecimento para o bem ajudando empresas a corrigirem falhas
- Mas há pessoas que aproveitam desse conhecimento para ganhar vantagem ou dinheiro

Segurança em redes

- No site da CVE (Common Vulnerabilities and Exposures) há uma lista das vulnerabilidades conhecidas e publicadas bem como quais medidas foram tomadas para a sua correção e orientações
- Atualmente há cerca de 160 mil publicações

Tipos mais comuns de ataques

- DDoS (Distribuited Denial of Service)
  - Acontece quando uma máquina (geralmente um servidor) é o alvo de acesso de diversos dispositivos ao mesmo tempo, isso faz com que o dispositivo não consiga comportar tantas conexões e acabe travando ou ficando inoperante

Tipos mais comuns de ataques

- Port Scanning (busca de portas abertas)
  - Esse tipo de ataque consiste em percorrer todas as portas possíveis de um dispositivo e testar caso haja alguma aberta e assim invadir a rede e roubar dados

Tipos mais comuns de ataques

- Ransonware
  - Muito conhecido ultimamente pois ocorreu em diversos ambientes empresariais e até mesmo na área de saúde (sistemas de hospitais), esse sistema faz a criptografia dos dados de um dispositivo e exige um pagamento para que os dados voltem ao normal

Tipos mais comuns de ataques

- Cavalo de Tróia
  - Assim como o nome diz, tem o mesmo funcionamento do utilizado pelos Gregos. Este ataque tem por finalidade se infiltrar no sistema através de arquivos infectados recebidos via email ou em de sites não seguros e abrir brechas ou monitorar as ações de um usuário.

Tipos mais comuns de ataques

- Força bruta
  - Nesse modo de ataque são realizadas diversas tentativas de acesso a um sistema com senhas padrões ou então com combinações de caracteres em um tamanho específico. Geralmente utilizado para tentar fazer login

Tipos mais comuns de ataques

- Phishing (pescaria)
  - Mais comum de ser encontrado em e-mails falsos quando há requisição para inserção de dados em algum link
  - Os usuários clicam nesse link (isca) e informam os dados geralmente de acesso a banco

Tipos mais comuns de ataques

SENAI

- Cryptojacking
  - Utilizado quando a máquina alvo é infectada por um malware com a intenção de executar programas para mineração de criptomoedas usando a capacidade de processamento do computador

Tipos mais comuns de ataques

- Man-in-the-middle
  - Muito utilizado em redes de wifi públicas onde um computador pode ser configurado para atuar como modem/switch e faz com que os demais computadores da rede enviem os dados para esse computador “no meio do caminho”.
  - Todos os dados podem ser interceptados antes do envio para a internet

Modos de se proteger

- Manter os softwares atualizados
- Possuir um anti-vírus
- Manter o firewall ativado e configurado
- Criar senhas fortes
- Não utilizar sempre a mesma senha
- Fazer backup de arquivos importantes
- Em redes empresariais, bloquear acesso a conteúdos não pertinentes ao escopo da empresa