Codificação de Segurança da informação

Prof. Me. Gabriel Caixeta Silva

Por que não estamos seguros?

- Configurações malfeitas
- Softwares com falhas
- Redes desprotegidas
- Proteções ineficazes
- Falta de atualizações
- Fator humano

Vulnerabilidade

Configurações malfeitas

- senha muito fácil
- permissão excessiva
- máquinas que podem ser acessadas por qualquer usuário
- roteadores ou switches com contas de usuário-padrão
- portas de serviços sem proteção adequada

softwares com falhas

- sistema operacional
- calculadora
- tocador de mp3
- leitor de pdf
- editor de texto
- etc

https://www.cvedetails.com/

Redes desprotegidas

- Falta de criptografia
  - uso de serviços como HTTP, FTP, DNS; ao invés de HTTPS com SSL, SFTP e DNSSEC
- Redirecionamento de tráfego
  - ARP POISONING, DHCP SPOOFING, ICMP REDIRECT ou PORT STEALING, fazem com que máquinas da rede envie o tráfego local
- Spoofing
  - IP Spoofing, permite falsificar o endereço de origem;
  - DNS Spoofing envia respostas dns falsas;

Proteções ineficazes

- antivírus
- filtro de pacotes
- proxys
- firewalls

Falta de atualizações

- atualizações não automáticas
- patches de segurança podem abrir novas falhas
- software muito antigos (windows 98, xp)

Fator humano

Engenharia social

- usuário roda um cavalo de tróia sem saber
- informações privilegiadas
- vazamento de especificações de um novo produto

Termos

Hacker

- termo para designar ‘fuçadores’ e a mídia o popularizou para os invasores digitais
- Kevin Mitnick é o mais famoso ‘hacker do mal’

Termos

Hacker white-hat

- ‘hacker do bem’
- normalmente realizada testes de intrusão dentro da empresa de modo preventivo;
- não usa o seu conhecimento de forma banal e irresponsável.

Termos

Hacker black-hat

- ‘hacker do mal
- usa seus conhecimentos para roubar senhas, documentos, causar danos a terceiros ou até mesmo realizar espionagem industrial

Termos

cracker

- o mesmo que hacker black-hat

Termos

Engenheiro social

- utiliza meios não técnicos para obter informações privilegiadas

Termos

Scammer

- fraudador que utiliza falhas em programas e um pouco de engenharia social para enviar sites falsos, idêntico ao original, a usuários leigos

Termos

Script kiddie

- invasor que não tem um conhecimento profundo nem alvos definidos;
- não sabe programar e usa ‘receitas de bolo’ para fazer seus ataques;
- o que importa é a quantidade e não a qualidade dos ataques

Termos

Defacer

- Script Kiddie que só se preocupa em substituir a página principal de algum website

Termos

Lammer

- Script Kiddie possui pouco conhecimento e se faz passar por um ‘guru da tecnologia’

Termos

Lammer

- Script Kiddie possui pouco conhecimento e se faz passar por um ‘guru da tecnologia’

TCP/IP básico

APLICAÇÃO

TRANSPORTE

INTERNET

REDE

Camada da Aplicação

- Contém os protocolos de alto nível
- operações e propriedades, sessões e controle de diálogos dos protocolos
- SMTP
- POP
- FTP
- HTTP
- SNMP
- DNS
- TELNET
- SSL
- SSH

Camada de Transporte

- controla o fluxo, confiabilidade e possível correção de erros na entrega de dados
- TCP
- UDP
- PORTAS
  - 21 TCP FTP
  - 69 UDP TFTP
  - 22 TCP SSH
  - 443 TCP HTTPS

Camada da Internet

- Assegura que os dados cheguem ao seu destino, independente do caminho
- Protocolos
  - IP
    - endereço do host
    - máscara de rede
    - porção da rede
    - endereço de rede
    - endereço de broadcast
  - ICMP
    - envia pacotes avisando de possíveis erros ou informações (ping)
  - ARP - converte um endereço IP em endereço físico (MAC)

Camada de Rede

- camada que se relaciona a tudo que um capote IP precisa para realmente estabelecer um link físico;
- LAN, WAN
- todos os detalhes nas camadas físicas e enlace do OSI

Tipos de transmissão de dados

- Unicast
  - um computador envia os dados para o cliente que o requisitou, nenhum outro computador da rede recebe os dados.
- Broadcast
  - os dados são enviados uma vez, mas para toda a rede.
- Multicast
  - mistura os dois anteriores