Hardening de Equipamentos

ceptro.br nic.br cgi.br

Licença de uso do material

Esta apresentação está disponível sob a licença

Creative Commons
Atribuição - Sem Derivações 4.0 Internacional (CC BY-ND 4.0)
https://creativecommons.org/licenses/by-nd/4.0/legalcode.pt

Você tem o direito de:

- **Compartilhar -** copiar e redistribuir o **material** em qualquer suporte ou formato para qualquer fim, **mesmo que comercial.**
- *O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.*

De acordo com os termos seguintes:

- **Atribuição** - Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso. Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do **Curso de Boas Práticas Operacionais para Sistemas Autônomos do CEPTRO.br/NIC.br**, e que os originais podem ser obtidos em http://ceptro.br. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.
- **Sem Derivações** - Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

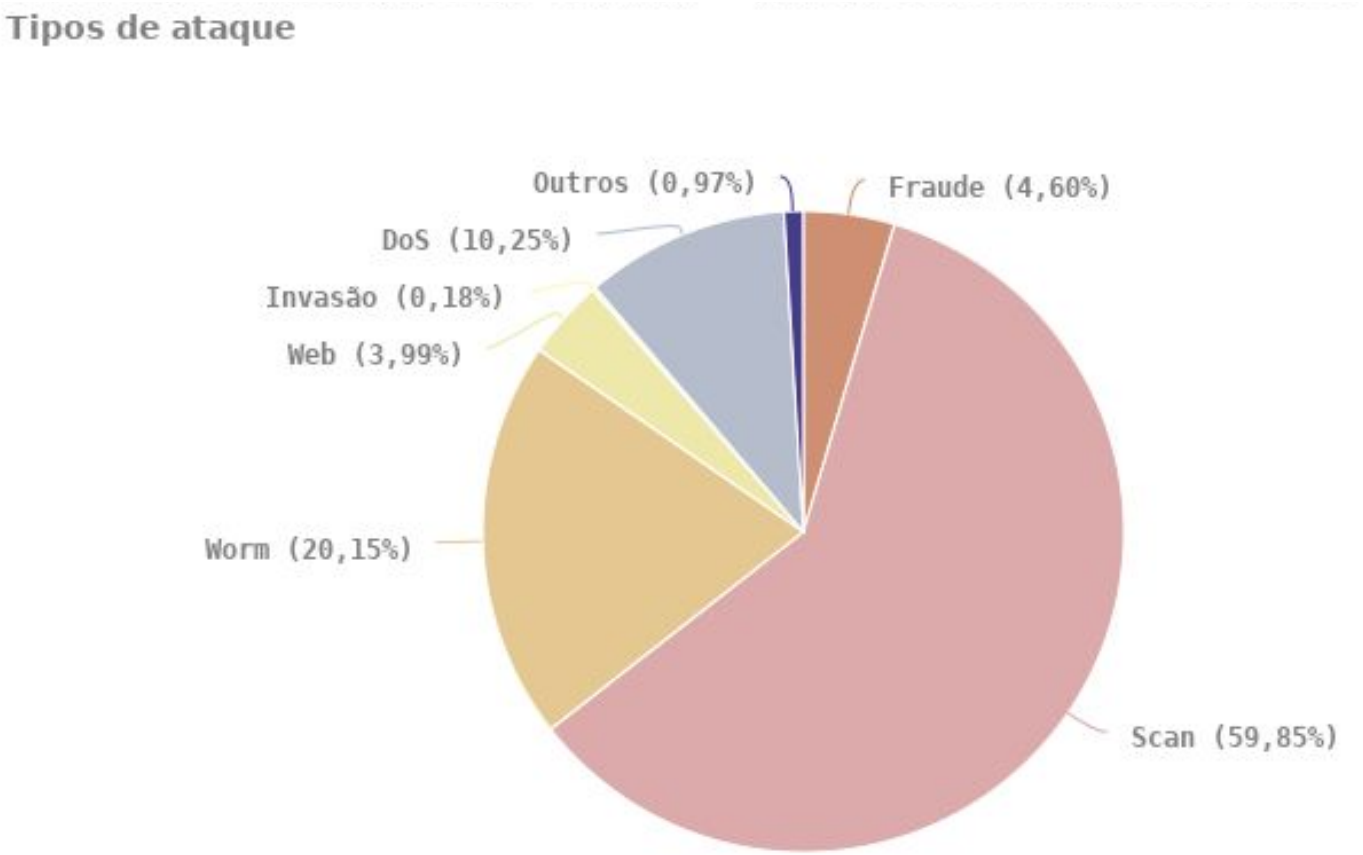
Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

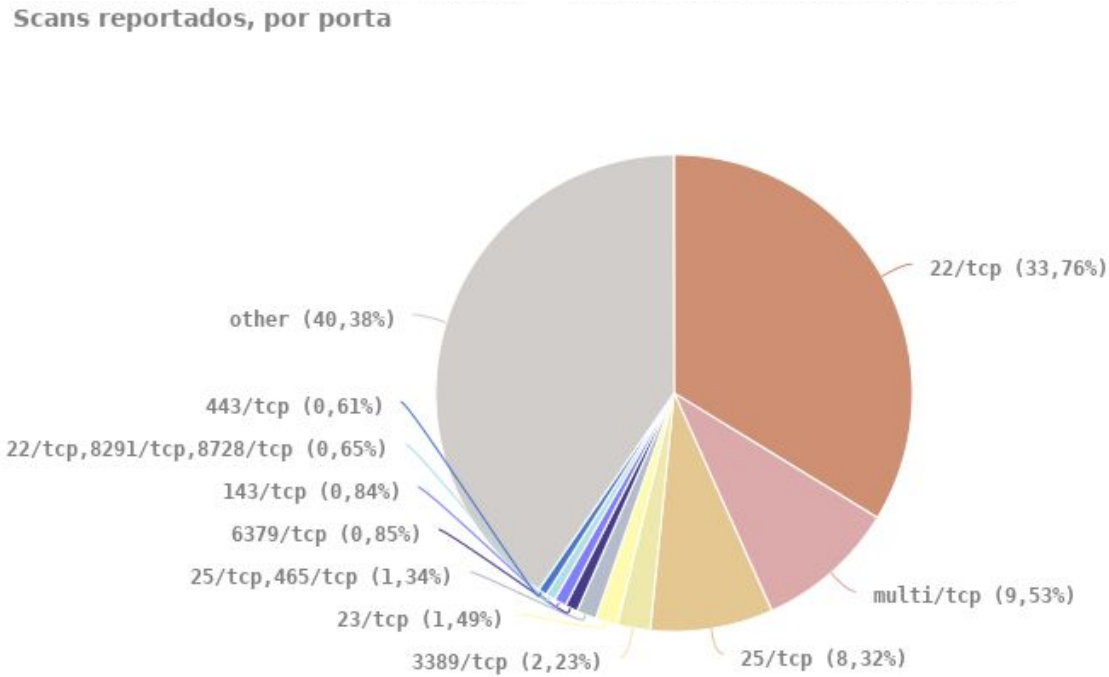
Atividades nos Honeypots Distribuídos

- **Força bruta de senhas (usado por malwares de IoT e para invasão de servidores e roteadores):**
  - Telnet (23/TCP)
  - SSH (22/TCP)
  - Outras TCP (2323, 23231, 2222)
- **Protocolos explorados pela botnet Mirai, na variante para CPEs (roteadores de banda larga)**
  - TCP: 7547, 5555, 37777, 6789, 81, 37215, 52869
- **Busca por protocolos que permitam amplificação**
  - UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

Projeto *Honeypots* Distribuídos
https://honeytarg.cert.br/honeypots/

Ataques dentro da Internet Brasileira





Scan Portas 22 e 23:
Força bruta de senhas de servidores, CPEs e IoT

Fonte: https://stats.cert.br/historico/incidentes/2020-jan-dec/tipos-ataque.html

Alteração de DNS para fraudes

- **Comprometidos**
  - via força bruta de senhas (geralmente via telnet)
  - explorando vulnerabilidades
  - via ataques CSRF, através de iFrames com JavaScripts maliciosos
    - Colocados em sites legítimos comprometidos pelos fraudadores
- **Objetivos dos ataques**
  - **alterar a configuração de DNS para que consultem servidores sob controle dos atacantes**
  - servidores DNS maliciosos hospedados em serviços de hosting/cloud
  - casos com mais de 30 domínios de redes sociais, serviços de e-mail, buscadores, comércio eletrônico, cartões, bancos

O que é Hardening?

- **É um procedimento para:**
  - Analisar vulnerabilidades.
  - Mapear as ameaças.
  - Minimizar/Mitigar riscos.
  - Aplicar medidas corretivas.
- **Proteger**
  - Ataques vindos de terceiros
  - Seus equipamentos façam ataques em outros.

Recomendações para Autenticação

- **Básico**
  - **Criar um usuário para cada funcionário.**
    - Desative contas antigas e inutilizadas.
  - **Não deixe os funcionários utilizarem a mesma conta padrão de administração do sistema!!!**
    - Guarde o acesso padrão somente para backup e emergências.

Recomendações para Autenticação

- **Básico**
  - **Não permita senhas fracas de acesso!**
    - O CERT.br possui fascículo sobre recomendações de senhas!
  - **Não armazena sua senhas em texto puro!**
    - Use uma função hash (PBKDF2, Bcrypt, Scrypt e Argon2)

https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf

Recomendações para Autenticação

- **Avançado**
  - Aplique técnicas de **autenticação em 2 fatores.**
    - Coisas que eu **sei**!
      - Ex: Senhas.
    - Coisas que eu **sou**!
      - Ex: Biometria.
    - Coisas que eu **possuo**!
      - Ex: Chave.
  - **Usar 2 coisas do mesmo tipo não caracteriza autenticação em 2 fatores.**
  - O CERT.br possui fascículo com **recomendações sobre o assunto**.

Recomendações para Autorização

- **Básico**
  - **Cada usuário deve ter permissão para acessar o roteador de acordo com o seu trabalho.**
    - Não forneça acesso administrador para todos o seus usuários.
    - Pense no que seu estagiário/agente malicioso poderia fazer no seu sistema.
  - **Em alguns sistemas pode se criar grupos de privilégios.**
  - **Em alguns sistemas é possível escalar privilégios.**

Recomendações para Auditoria

- **Básico**
  - Manter um **registro de cada usuário com suas respectivas permissões**.
  - **Registrar as ações** de cada usuário no sistema.
  - Operar com **nível de criticidade** nos registros.
    - Informativo
    - Aviso
    - Crítico
  - Tipos de registros
    - Documentos
    - Logs
    - Backups de configuração
  - É **importante** guardar a informação com a **data e hora certa**!

Recomendações para Acesso

- **Básico**
  - **Não utilize protocolos inseguros** para acesso.
    - Exemplos:

  - **Desative-os se eles estiverem operando.**

  - **Se for o único meio** de acesso a máquina, **restrinja** o alcance para somente ser utilizada pela **interface de gerencia** (uma rede apartada e protegida).

Recomendações para Acesso

- **Básico**
  - Utilize preferencialmente protocolos com mensagens **criptografadas!**
    - Exemplos:

Winbox
(secure mode)

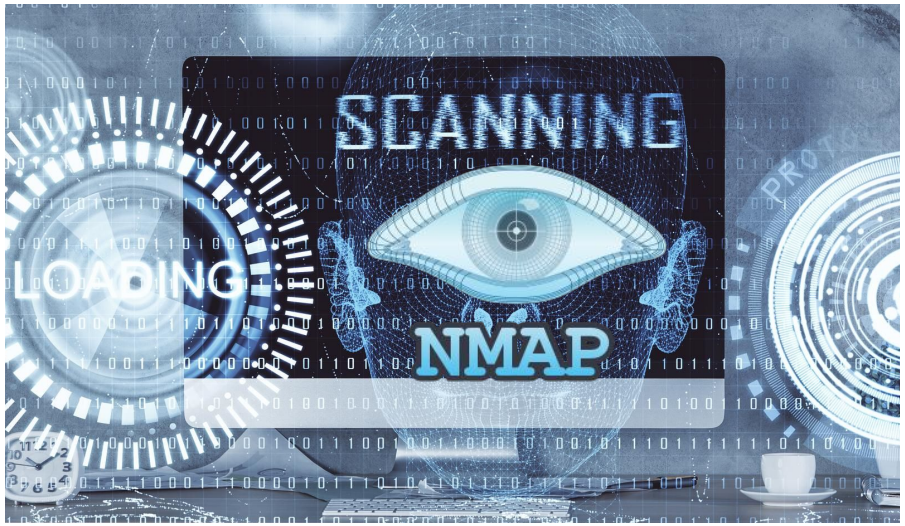
  - Lembre-se de utilizar a última versão estável disponível.
    - SSH v2 com strong crypto

Recomendações para Acesso

- **Básico**
  - Adicione uma **mensagem de login**.
  - **Existem governos que exigem** essas mensagens para o **âmbito legal**.
  - **Exemplo:**
    - “Roteador pertencente a empresa X, acessos não autorizados serão monitorados, investigados e entregues às autoridades responsáveis”

Recomendações para Acesso

- **Básico**
  - Mudar a porta padrão do serviço de acesso.
  - Bloquear acesso a porta padrão.
  - Não é bem uma proteção mas pode ajudar contra um ataque simples que procura portas padrão.



Recomendações para Acesso

- **Básico**
  - Armazene informações para auditoria
    - Log de ações
      - Identifica comandos indevidos
    - Log de tentativas de acesso.
      - Identifica ataque de força bruta
      - Identifica ataque de negação de serviço
      - Identifica tentativa de roubo de informações

  - Crie políticas de mitigação de ataque
      - Filtros
      - Blackhole

Recomendações para Acesso

- **Básico**
  - Utilize a hora legal brasileira com ntp.br

Recomendações para Acesso

- **Básico**
  - Não permita acesso por todas as interfaces dos equipamentos.
  - Escolha uma interface de loopback para os seus serviços:
    - São mais estáveis
    - Não sofrem com variações no link
    - Caso uma interface física fique indisponível os protocolos de roteamento procuram um novo caminho.
  - Faça essa interface parte da sua rede de gerência.

Recomendações para Acesso

- **Básico**
  - Forçar o logout depois de um tempo de inatividade.
    - Isso evita que alguém use sua máquina em seu período ausente.
    - Isso evita que um atacante monitore o seu tempo de inatividade para tomar controle da máquina.

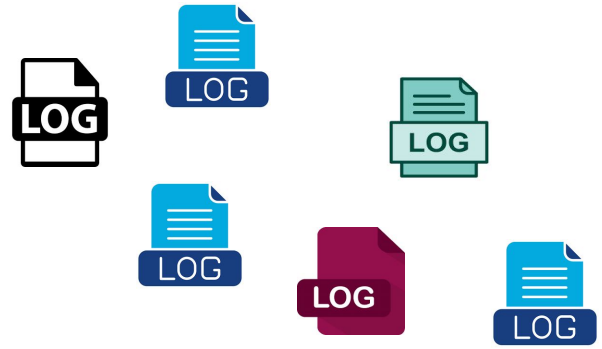
  - Forçar o logout depois de se desconectar o cabo.
    - Isso evita que alguém reconecte o cabo e use o seu login.

Recomendações para Acesso

- **Avançado**
  - **Port Knocking**
    - Nenhuma porta aparece aberta no scan
    - Diminui a superfície de ataques
    - Para acessar um serviço
      - Testar uma sequência de portas fechadas.
      - Configurar a mudança de regras de firewall dinamicamente.
      - Conectar na porta desejada.

Recomendações para Logs

- **Básico**
  - Configure logs com diferentes níveis de criticidade.
  - Evite gerenciar logs dentro dos roteadores.
    - Quanto mais funções o roteador tiver que fazer, menos processamento será utilizado para rotear pacotes.
  - Envie de maneira segura os logs para uma outra máquina.
    - Algum agente malicioso pode interceptá-los.
  - Guarde de maneira segura seus logs.
    - Eles podem te ajudar num processo judicial.
  - Mantenha a hora correta com NTP.



Recomendações para o Sistema

- **Básico**
  - Desative todas as interfaces não utilizadas.
    - Interfaces que não possuem cabos conectados.

  - Desative todas os serviços não utilizadas, inseguros e que podem ser utilizados para ataques de amplificação.
    - Testador de banda
    - DNS recursivo
    - Servidor NTP
  - Remova ou desative os pacotes de funções extras não utilizados.
    - Pacote wireless

Recomendações para o Sistema

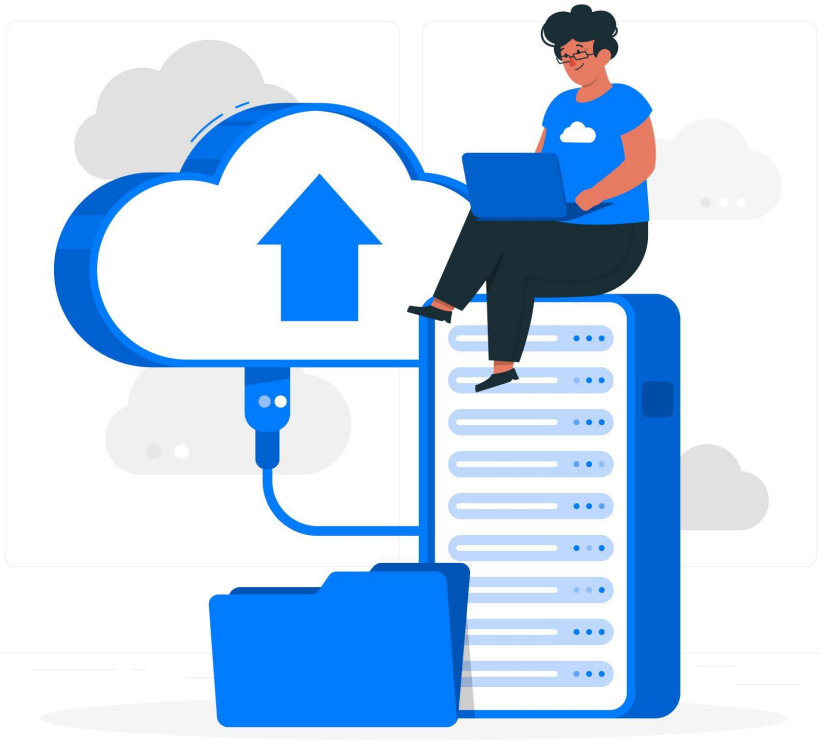
- **Básico**
  - Desabilite protocolos de descoberta de vizinhança:
    - CDP
    - MNDP
    - LLDP
  - Facilita para o atacante descobrir o tipo do seu roteador.
  - Inundam a rede com mensagens desnecessárias.
  - Tome cuidado com o IPV6:
    - Descoberta de vizinhança é essencial.
    - Sem ela, nada funciona.

Recomendações para o Sistema

- **Básico**
  - Mantenha o sistema sempre atualizado na versão estável.
    - Incluindo seus pacotes.
  - Aplique todos os patches de segurança.
  - Procure testar as atualizações, antes de aplicar em produção, num ambiente controlado.
    - Emulador.
    - Simulador.

Recomendações para Configurações

- **Básico**
  - Mantenha sempre um backup atualizado das configurações atuais.
  - Envie de maneira segura esse backup para uma outra máquina.
    - Email criptografado
    - SCP
    - SFTP
  - Lembre, o operacional da sua empresa está guardado lá!
    - Hashes de senhas podem ser quebrados!



Recomendações para Configurações

- **Básico**
  - Mantenha um script de hardening de roteadores.
  - Assim ao comprar um novo roteador, você saberá as políticas mínimas de segurança que precisam ser aplicadas.
  - Mantenha esse script atualizado. Cada nova política precisa ser agregada ao script.

Dúvidas?

Patrocínio Super Like

Apoio de Mídia

Obrigado!

CEPTRO.br Cursos: cursosceptro@nic.br
CEPTRO.br IPv6: ipv6@nic.br

@comunicbr
@nicbr
@NICbrvideos

nic.br cgi.br

www.nic.br | www.cgi.br