# Módulo 15 – Fundamentos de Segurança de Rede

---

## 1. Ameaças e Vulnerabilidades

**Tipos de Ameaças:**

- **Roubo de informações**
- **Manipulação de dados**
- **Roubo de identidade**
- **Interrupção do serviço**

**Tipos de Vulnerabilidades:**

1. **Tecnológicas:** falhas em protocolos, SO ou dispositivos.
2. **De configuração:** senhas fracas, serviços mal configurados.
3. **De políticas:** falta de políticas claras ou mal aplicadas.

**Ameaças físicas:**

- **Hardware:** danos físicos aos equipamentos.
- **Ambientais:** calor, umidade.
- **Elétricas:** quedas de energia, picos de tensão.
- **Manutenção:** cabeamento ruim, peças faltando.

---

## 2. Ataques à Rede

**Tipos de Malware:**

- **Vírus:** se espalha anexando a arquivos.
- **Worms:** se espalham sozinhos, sem ajuda.

- **Cavalos de Tróia:** disfarçados de software legítimo.

**Tipos de Ataques:**

- **Reconhecimento:** mapeamento da rede (nslookup, whois, ping).
- **Acesso:** uso de senhas fracas, exploração de confiança, man-in-the-middle.
- **Negação de Serviço (DoS/DDoS):** consome os recursos até travar o sistema.

---

## 3. Mitigação de Ataques

**Defesa em profundidade:**

Combina vários dispositivos e técnicas:

- **VPN**, **Firewall ASA**, **IPS**, **Servidores AAA**, **WSA/ESA**

**Backup:**

- Fazer backups regulares e armazenar em local seguro.

**Atualizações:**

- Manter sistema, antivírus e patches sempre atualizados.

**AAA (Autenticação, Autorização e Accounting):**

- Controla quem acessa, o que faz e registra tudo.

**Firewall:**

- Filtragem por IP, portas, URLs, SPI (Stateful Packet Inspection).
- Implementar zona desmilitarizada (DMZ) pros serviços públicos.

**Segurança dos endpoints:**

- Antivírus, políticas de uso, controle de acesso à rede (NAC).

---

### 4. Segurança de Dispositivos

**Cisco AutoSecure:**

- Automatiza a aplicação de boas práticas de segurança.

**Boas práticas:**

- Trocar senhas padrão
- Restringir acesso
- Desativar serviços desnecessários

---

### 5. Senhas Fortes

- Mínimo 8 caracteres (melhor: 10+)
- Letras maiúsculas, minúsculas, números, símbolos
- Evite dados pessoais, palavras óbvias

**Frases secretas (passphrases) são melhores que senhas simples.**

---

### 6. Comandos importantes:

```
# Criptografar senhas simples
service password-encryption

# Definir tamanho mínimo da senha
security passwords min-length 10

# Bloquear tentativa de força bruta
login block-for 60 attempts 3 within 30

# Deslogar sessão inativa
exec-timeout 5
```

```
# Criar usuário
username admin secret cisco123

# Gerar chave SSH
crypto key generate rsa general-keys modulus 1024

# Ativar SSH nas VTY
line vty 0 4
 login local
 transport input ssh
```

**Verificar serviços abertos:**

bash
Copiar código

```
# IOS-XE
show ip ports all

# IOS tradicional
show control-plane host open-ports
```